



Gestire l'autenticazione dell'amministratore e RBAC

ONTAP 9

NetApp
April 24, 2024

Sommario

- Gestire l'autenticazione dell'amministratore e RBAC..... 1
 - Panoramica dell'autenticazione dell'amministratore e RBAC con la CLI..... 1
 - Autenticazione dell'amministratore e workflow RBAC..... 1
 - Fogli di lavoro per l'autenticazione dell'amministratore e la configurazione RBAC..... 2
 - Creare account di accesso..... 17
 - Gestire i ruoli di controllo degli accessi..... 32
 - Gestire gli account amministratore..... 39
 - Gestire la verifica multi-admin..... 64

Gestire l'autenticazione dell'amministratore e RBAC

Panoramica dell'autenticazione dell'amministratore e RBAC con la CLI

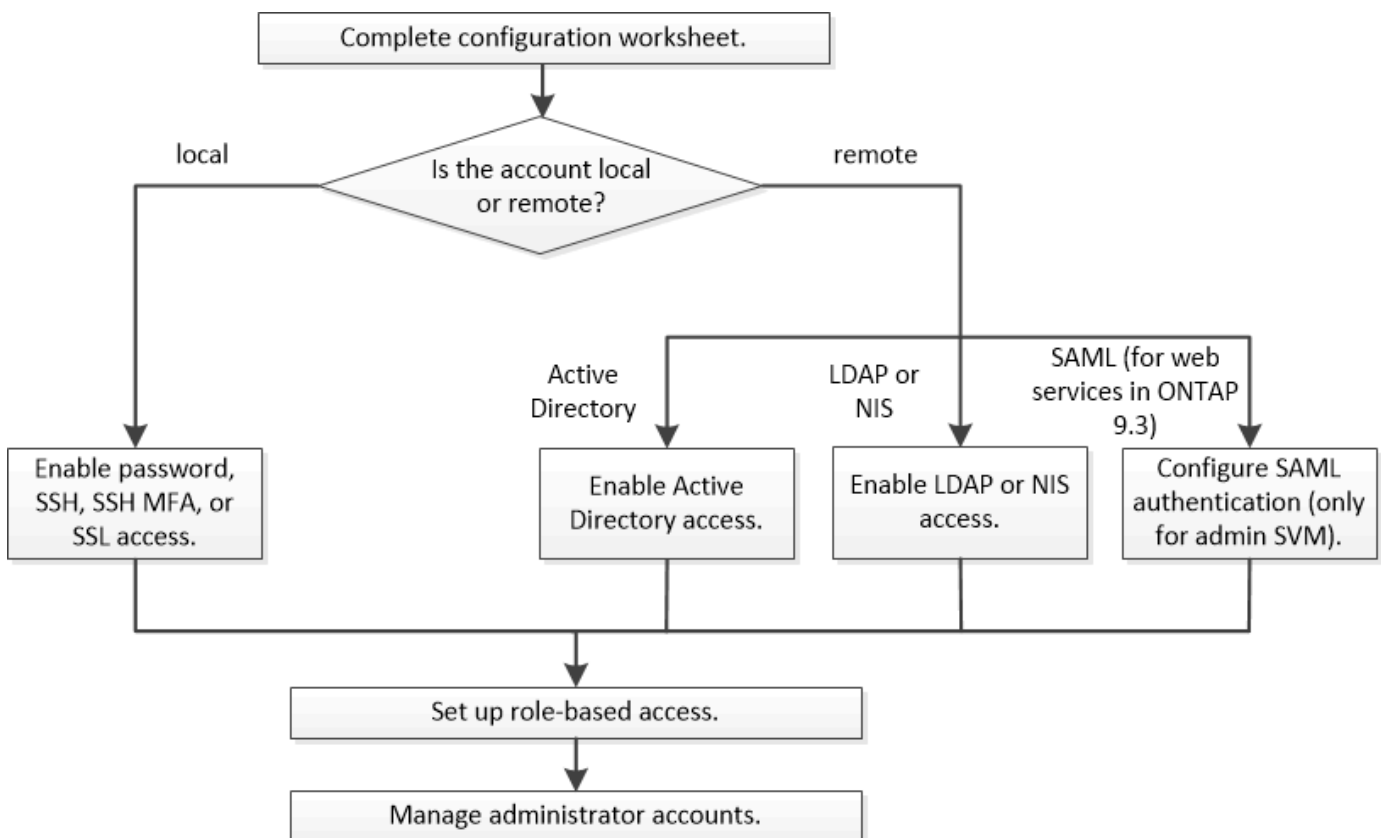
È possibile abilitare gli account di accesso per gli amministratori del cluster ONTAP e per gli amministratori delle macchine virtuali di storage (SVM). È inoltre possibile utilizzare RBAC (role-based access control) per definire le funzionalità degli amministratori.

È possibile abilitare gli account di accesso e RBAC nei seguenti modi:

- Si desidera utilizzare l'interfaccia della riga di comando (CLI) di ONTAP, non Gestione di sistema o uno strumento di scripting automatico.
- Si desidera utilizzare le Best practice, non esplorare tutte le opzioni disponibili.
- Non si utilizza SNMP per raccogliere informazioni sul cluster.

Autenticazione dell'amministratore e workflow RBAC

È possibile attivare l'autenticazione per gli account amministratore locali o per gli account amministratore remoti. Le informazioni dell'account per un account locale risiedono nel sistema di storage e le informazioni dell'account per un account remoto risiedono altrove. Ogni account può avere un ruolo predefinito o personalizzato.



È possibile consentire agli account amministratore locali di accedere a una SVM (Storage Virtual Machine) o a una SVM dati con i seguenti tipi di autenticazione:

- Password
- Chiave pubblica SSH
- Certificato SSL
- Autenticazione multifattore SSH (MFA)

A partire da ONTAP 9.3, è supportata l'autenticazione con password e chiave pubblica.

È possibile consentire agli account amministratore remoto di accedere a una SVM amministrativa o a una SVM dati con i seguenti tipi di autenticazione:

- Active Directory
- Autenticazione SAML (solo per SVM admin)

A partire da ONTAP 9.3, l'autenticazione SAML (Security Assertion Markup Language) può essere utilizzata per accedere alla SVM amministrativa utilizzando uno dei seguenti servizi Web: Infrastruttura del processore di servizi, API ONTAP o Gestore di sistema.

- A partire da ONTAP 9.4, SSH MFA può essere utilizzato per utenti remoti su server LDAP o NIS. È supportata l'autenticazione con nsswitch e chiave pubblica.

Fogli di lavoro per l'autenticazione dell'amministratore e la configurazione RBAC

Prima di creare account di accesso e impostare RBAC (role-based access control), è necessario raccogliere informazioni per ciascun elemento nei fogli di lavoro di configurazione.

Creare o modificare gli account di accesso

Questi valori vengono forniti con `security login create` Comando quando abiliti gli account di accesso per accedere a una VM di storage. Vengono forniti gli stessi valori con `security login modify` Comando quando si modifica il modo in cui un account accede a una VM storage.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della VM di storage a cui accede l'account. Il valore predefinito è il nome della VM storage di amministrazione per il cluster.	

-user-or-group-name	Il nome utente o il nome del gruppo dell'account. Specificando un nome di gruppo, è possibile accedere a ciascun utente del gruppo. È possibile associare un nome utente o un nome di gruppo a più applicazioni.	
-application	<p>Applicazione utilizzata per accedere alla VM di storage:</p> <ul style="list-style-type: none"> • http • ontapi • snmp • ssh 	
-authmethod	<p>Il metodo utilizzato per autenticare l'account:</p> <ul style="list-style-type: none"> • cert Per l'autenticazione del certificato SSL • domain Per l'autenticazione di Active Directory • nsswitch Per l'autenticazione LDAP o NIS • password per l'autenticazione della password dell'utente • publickey per l'autenticazione a chiave pubblica • community Per le stringhe di comunità SNMP • usm Per il modello di sicurezza dell'utente SNMP • saml Per l'autenticazione SAML (Security Assertion Markup Language) 	

<code>-remote-switch-ipaddress</code>	L'indirizzo IP dello switch remoto. Lo switch remoto può essere uno switch del cluster monitorato dal monitor di stato dello switch del cluster (CSHM) o uno switch Fibre Channel (FC) monitorato dal monitor di stato MetroCluster (MCC-HM). Questa opzione è applicabile solo quando l'applicazione è <code>snmp</code> e il metodo di autenticazione è <code>usm</code> .	
<code>-role</code>	<p>Il ruolo di controllo degli accessi assegnato all'account:</p> <ul style="list-style-type: none"> • Per il cluster (la VM di storage di amministrazione), il valore predefinito è <code>admin</code>. • Per una macchina virtuale per lo storage dei dati, il valore predefinito è <code>vsadmin</code>. 	
<code>-comment</code>	(Facoltativo) testo descrittivo per l'account. Racchiudere il testo tra virgolette doppie (").	
<code>-is-ns-switch-group</code>	Se l'account è un account di gruppo LDAP o NIS (<code>yes</code> oppure <code>no</code>).	

-second-authentication-method	<p>Secondo metodo di autenticazione in caso di autenticazione multifattore:</p> <ul style="list-style-type: none"> • none se non si utilizza l'autenticazione a più fattori, valore predefinito • publickey per l'autenticazione a chiave pubblica quando authmethod è password o nsswitch • password per l'autenticazione della password utente quando authmethod è chiave pubblica • nsswitch per l'autenticazione della password utente quando il metodo authmethod è publickey <p>L'ordine di autenticazione è sempre la chiave pubblica seguita dalla password.</p>	
-is-ldap-fastbind	<p>A partire da ONTAP 9.11.1, se impostato su true, attiva il binding rapido LDAP per l'autenticazione nsswitch; l'impostazione predefinita è false. Per utilizzare l'associazione rapida LDAP, il -authentication-method il valore deve essere impostato su nsswitch. "Scopri di più su LDAP fastbind per l'autenticazione nsswitch."</p>	

Configurare le informazioni di protezione di Cisco Duo

Questi valori vengono forniti con `security login duo create` Comando quando si attiva l'autenticazione a due fattori Cisco Duo con gli accessi SSH per una VM di storage.

Campo	Descrizione	Il tuo valore
-vserver	La VM di storage (denominata vserver nell'interfaccia CLI di ONTAP) a cui si applicano le impostazioni di autenticazione Duo.	

-integration-key	La chiave di integrazione, ottenuta durante la registrazione dell'applicazione SSH con Duo.	
-secret-key	La chiave segreta, ottenuta durante la registrazione dell'applicazione SSH con Duo.	
-api-host	<p>Il nome host API, ottenuto durante la registrazione dell'applicazione SSH con Duo. Ad esempio:</p> <pre>api- <HOSTNAME>.duosecurity.com</pre>	
-fail-mode	<p>In caso di errori di configurazione o di servizio che impediscono l'autenticazione Duo, non viene eseguita correttamente <code>safe</code> (consentire l'accesso) o. <code>secure</code> (negare l'accesso). L'impostazione predefinita è <code>safe</code>, il che significa che l'autenticazione Duo viene ignorata se non riesce a causa di errori quali il server Duo API non è accessibile.</p>	
-http-proxy	<p>Utilizzare il proxy HTTP specificato. Se il proxy HTTP richiede l'autenticazione, includere le credenziali nell'URL del proxy. Ad esempio:</p> <pre>http- proxy=http://username :password@proxy.example.org:8080</pre>	

-autopush	<p>Entrambi <code>true</code> oppure <code>false</code>. Il valore predefinito è <code>false</code>. Se <code>true</code>, Duo invia automaticamente una richiesta di accesso push al telefono dell'utente, tornando a una chiamata telefonica se non è disponibile il push. Si noti che in questo modo l'autenticazione con codice di accesso viene disattivata. Se <code>false</code>, all'utente viene richiesto di scegliere un metodo di autenticazione.</p> <p>Se configurato con <code>autopush = true</code>, si consiglia l'impostazione <code>max-prompts = 1</code>.</p>	
-max-prompts	<p>Se un utente non riesce ad autenticarsi con un secondo fattore, Duo richiede all'utente di eseguire nuovamente l'autenticazione. Questa opzione consente di impostare il numero massimo di richieste visualizzate da Duo prima di negare l'accesso. Deve essere 1, 2, o 3. Il valore predefinito è 1.</p> <p>Ad esempio, quando <code>max-prompts = 1</code>, l'utente deve eseguire correttamente l'autenticazione al primo prompt, mentre se <code>max-prompts = 2</code>, se l'utente immette informazioni errate al prompt iniziale, gli verrà richiesto di eseguire nuovamente l'autenticazione.</p> <p>Se configurato con <code>autopush = true</code>, si consiglia l'impostazione <code>max-prompts = 1</code>.</p> <p>Per una migliore esperienza, un utente con solo autenticazione a chiave pubblica avrà sempre <code>max-prompts</code> impostare su 1.</p>	

<code>-enabled</code>	Attiva l'autenticazione a due fattori Duo. Impostare su <code>true</code> per impostazione predefinita. Quando questa opzione è attivata, l'autenticazione Duo a due fattori viene applicata durante il login SSH in base ai parametri configurati. Quando Duo è disattivato (impostato su <code>false</code>), l'autenticazione Duo viene ignorata.	
-----------------------	---	--

Definire ruoli personalizzati

Questi valori vengono forniti con `security login role create` quando si definisce un ruolo personalizzato.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	(Opzionale) il nome della VM di storage (chiamato <code>vserver</code> nella CLI di ONTAP) associata al ruolo.	
<code>-role</code>	Il nome del ruolo.	
<code>-cmddirname</code>	La directory di comando a cui il ruolo dà accesso. I nomi delle sottodirectory dei comandi devono essere racimati tra virgolette doppie ("). Ad esempio, " <code>volume snapshot</code> ". È necessario immettere <code>DEFAULT</code> per specificare tutte le directory dei comandi.	

-access	<p>(Facoltativo) il livello di accesso per il ruolo. Per le directory dei comandi:</p> <ul style="list-style-type: none"> • <code>none</code> (il valore predefinito per i ruoli personalizzati) nega l'accesso ai comandi nella directory dei comandi • <code>readonly</code> concede l'accesso a <code>show</code> comandi nella directory dei comandi e nelle relative sottodirectory • <code>all</code> concede l'accesso a tutti i comandi nella directory dei comandi e alle relative sottodirectory <p>Per <i>comandi non intrinseci</i> (comandi che non finiscono in <code>create</code>, <code>modify</code>, <code>delete</code>, o <code>show</code>):</p> <ul style="list-style-type: none"> • <code>none</code> (il valore predefinito per i ruoli personalizzati) nega l'accesso al comando • <code>readonly</code> non applicabile • <code>all</code> concede l'accesso al comando <p>Per concedere o negare l'accesso ai comandi intrinseci, è necessario specificare la directory dei comandi.</p>	
-query	<p>(Facoltativo) oggetto query utilizzato per filtrare il livello di accesso, specificato sotto forma di un'opzione valida per il comando o per un comando nella directory dei comandi. Racchiudere l'oggetto di query tra virgolette doppie ("). Ad esempio, se la directory dei comandi è <code>volume</code>, l'oggetto query <code>"-aggr aggr0"</code> consentirebbe l'accesso a <code>aggr0</code> solo aggregato.</p>	

Associare una chiave pubblica a un account utente

Questi valori vengono forniti con `security login publickey create` Quando si associa una chiave pubblica SSH a un account utente.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	(Facoltativo) il nome della VM di storage a cui l'account accede.	
<code>-username</code>	Il nome utente dell'account. Il valore predefinito, <code>admin</code> , che è il nome predefinito dell'amministratore del cluster.	
<code>-index</code>	Il numero di indice della chiave pubblica. Il valore predefinito è 0 se la chiave è la prima chiave creata per l'account; in caso contrario, il valore predefinito è uno più del numero di indice più alto esistente per l'account.	
<code>-publickey</code>	La chiave pubblica OpenSSH. Racchiudere la chiave tra virgolette doppie (").	
<code>-role</code>	Il ruolo di controllo degli accessi assegnato all'account.	
<code>-comment</code>	(Facoltativo) testo descrittivo per la chiave pubblica. Racchiudere il testo tra virgolette doppie (").	

<code>-x509-certificate</code>	<p>(Facoltativo) a partire da ONTAP 9.13.1, consente di gestire l'associazione del certificato X.509 con la chiave pubblica SSH.</p> <p>Quando si associa un certificato X.509 alla chiave pubblica SSH, ONTAP verifica la validità del certificato al momento dell'accesso SSH. Se è scaduto o è stato revocato, l'accesso non è consentito e la chiave pubblica SSH associata è disattivata. Valori possibili:</p> <ul style="list-style-type: none"> • <code>install</code>: Installare il certificato X.509 con codifica PEM specificato e associarlo alla chiave pubblica SSH. Includere il testo completo del certificato che si desidera installare. • <code>modify</code>: Aggiornare il certificato X.509 con codifica PEM esistente con il certificato specificato e associarlo alla chiave pubblica SSH. Includere il testo completo del nuovo certificato. • <code>delete</code>: Rimuovere l'associazione esistente del certificato X.509 con la chiave pubblica SSH. 	
--------------------------------	---	--

Installare un certificato digitale del server firmato dalla CA

Questi valori vengono forniti con `security certificate generate-csr` Comando quando si genera una richiesta di firma digitale del certificato (CSR) da utilizzare per l'autenticazione di una VM di storage come server SSL.

Campo	Descrizione	Il tuo valore
<code>-common-name</code>	Il nome del certificato, ovvero un nome di dominio completo (FQDN) o un nome comune personalizzato.	

-size	Il numero di bit nella chiave privata. Maggiore è il valore, maggiore sarà la sicurezza della chiave. Il valore predefinito è 2048. I valori possibili sono 512, 1024, 1536, e. 2048.	
-country	Il paese della macchina virtuale di archiviazione, in un codice di due lettere. Il valore predefinito è US. Consultare le pagine man per un elenco di codici.	
-state	Lo stato o la provincia della macchina virtuale di storage.	
-locality	La località della macchina virtuale storage.	
-organization	L'organizzazione della macchina virtuale di storage.	
-unit	L'unità nell'organizzazione della VM di storage.	
-email-addr	L'indirizzo e-mail dell'amministratore del contatto per la VM di storage.	
-hash-function	Funzione di hashing crittografico per la firma del certificato. Il valore predefinito è SHA256. I valori possibili sono SHA1, SHA256, e. MD5.	

Questi valori vengono forniti con `security certificate install` Comando quando si installa un certificato digitale con firma CA da utilizzare per l'autenticazione del cluster o della VM di storage come server SSL. Nella tabella seguente sono riportate solo le opzioni relative alla configurazione dell'account.

Campo	Descrizione	Il tuo valore
-vserver	Il nome della VM di archiviazione su cui deve essere installato il certificato.	

-type	<p>Il tipo di certificato:</p> <ul style="list-style-type: none"> • <code>server</code> per i certificati server e intermedi • <code>client-ca</code> Per il certificato a chiave pubblica della CA principale del client SSL • <code>server-ca</code> Per il certificato a chiave pubblica della CA principale del server SSL di cui ONTAP è un client • <code>client</code> Per un certificato digitale autofirmato o firmato da CA e una chiave privata per ONTAP come client SSL 	
-------	--	--

Configurare l'accesso al controller di dominio Active Directory

Questi valori vengono forniti con `security login domain-tunnel create` Comando quando è già stato configurato un server SMB per una macchina virtuale per lo storage dei dati e si desidera configurare la macchina virtuale per lo storage come gateway o *tunnel* per l'accesso al cluster da parte del controller di dominio Active Directory.

Campo	Descrizione	Il tuo valore
-vserver	Nome della VM di storage per cui è stato configurato il server SMB.	

Questi valori vengono forniti con `vserver active-directory create` Comando quando non è stato configurato un server SMB e si desidera creare un account di un computer VM di archiviazione nel dominio Active Directory.


Campo	Descrizione	Il tuo valore
-vserver	Il nome della VM di storage per cui si desidera creare un account di computer Active Directory.	
-account-name	Il nome NetBIOS dell'account del computer.	
-domain	Il nome di dominio completo (FQDN).	

-ou	L'unità organizzativa nel dominio. Il valore predefinito è CN=Computers. ONTAP aggiunge questo valore al nome di dominio per produrre il nome distinto di Active Directory.	
-----	---	--

Configurare l'accesso al server LDAP o NIS

Questi valori vengono forniti con `vserver services name-service ldap client create` Comando quando si crea una configurazione del client LDAP per la VM di storage.

Nella seguente tabella sono riportate solo le opzioni relative alla configurazione dell'account:

Campo	Descrizione	Il tuo valore
-vserver	Nome della VM di storage per la configurazione client.	
-client-config	Il nome della configurazione del client.	
-ldap-servers	Elenco separato da virgole di indirizzi IP e nomi host per i server LDAP a cui si connette il client.	
-schema	Lo schema utilizzato dal client per eseguire query LDAP.	
-use-start-tls	<p>Se il client utilizza Start TLS per crittografare la comunicazione con il server LDAP (<code>true</code> oppure <code>false</code>).</p> <div>  <p>Start TLS è supportato solo per l'accesso alle macchine virtuali storage dei dati. Non è supportato per l'accesso alle VM di amministrazione dello storage.</p> </div>	

Questi valori vengono forniti con `vserver services name-service ldap create` Comando quando si associa una configurazione client LDAP alla VM di storage.

Campo	Descrizione	Il tuo valore
-------	-------------	---------------

<code>-vserver</code>	Nome della VM di storage a cui deve essere associata la configurazione client.	
<code>-client-config</code>	Il nome della configurazione del client.	
<code>-client-enabled</code>	Se la VM di storage può utilizzare la configurazione del client LDAP (true oppure false).	

Questi valori vengono forniti con `vserver services name-service nis-domain create` Quando crei una configurazione di dominio NIS su una VM di storage.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Nome della VM di storage su cui deve essere creata la configurazione del dominio.	
<code>-domain</code>	Il nome del dominio.	
<code>-active</code>	Se il dominio è attivo (true oppure false).	
<code>-servers</code>	ONTAP 9.0, 9.1: Un elenco separato da virgole di indirizzi IP per i server NIS utilizzati dalla configurazione del dominio.	
<code>-nis-servers</code>	Elenco separato da virgole di indirizzi IP e nomi host per i server NIS utilizzati dalla configurazione di dominio.	

Questi valori vengono forniti con `vserver services name-service ns-switch create` quando si specifica l'ordine di ricerca per le origini del servizio nome.

Campo	Descrizione	Il tuo valore
<code>-vserver</code>	Il nome della VM di storage su cui deve essere configurato l'ordine di ricerca del servizio dei nomi.	

-database	<p>Il database name service:</p> <ul style="list-style-type: none"> • <code>hosts</code> Per file e servizi di nomi DNS • <code>group</code> Per file, LDAP e NIS name service • <code>passwd</code> Per file, LDAP e NIS name service • <code>netgroup</code> Per file, LDAP e NIS name service • <code>namemap</code> Per file e servizi di nomi LDAP 	
-sources	<p>L'ordine in cui cercare le origini del servizio dei nomi (in un elenco separato da virgole):</p> <ul style="list-style-type: none"> • <code>files</code> • <code>dns</code> • <code>ldap</code> • <code>nis</code> 	

Configurare l'accesso SAML

A partire da ONTAP 9.3, si forniscono questi valori con `security saml-sp create` Comando per configurare l'autenticazione SAML.

Campo	Descrizione	Il tuo valore
-idp-uri	L'indirizzo FTP o HTTP dell'host IdP (Identity Provider) da cui è possibile scaricare i metadati IdP.	
-sp-host	Il nome host o l'indirizzo IP dell'host del provider di servizi SAML (sistema ONTAP). Per impostazione predefinita, viene utilizzato l'indirizzo IP della LIF di gestione del cluster.	

<code>-cert-ca e. -cert-serial, o. -cert-common-name</code>	I dettagli del certificato del server dell'host del provider di servizi (sistema ONTAP). È possibile immettere l'autorità di certificazione (CA) di emissione del certificato del provider di servizi e il numero di serie del certificato oppure il nome comune del certificato del server.	
<code>-verify-metadata-server</code>	Se l'identità del server di metadati IdP deve essere convalidata <code>true</code> oppure <code>false</code>). La procedura consigliata consiste nell'impostare sempre questo valore su <code>true</code> .	

Creare account di accesso

Panoramica sulla creazione degli account di accesso

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

Attiva la panoramica dell'accesso all'account 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. È possibile utilizzare `security login create` Comando per consentire agli account locali di accedere a un amministratore o a una SVM di dati.

Abilitare l'accesso all'account password

È possibile utilizzare `security login create` Comando per consentire agli account amministratore di accedere a un 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 sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiornare il ruolo in un secondo momento.

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
```

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

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
```

Abilitare gli account a chiave pubblica SSH

È possibile utilizzare `security login create` Comando per consentire agli account amministratore di accedere a una SVM amministrativa o di 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 sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

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
```

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

Il seguente comando attiva l'account amministratore SVM `svmadmin1` con il predefinito `vsadmin-volume` Ruolo per accedere a `SVMengData1` Utilizzando una chiave pubblica SSH:

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

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)

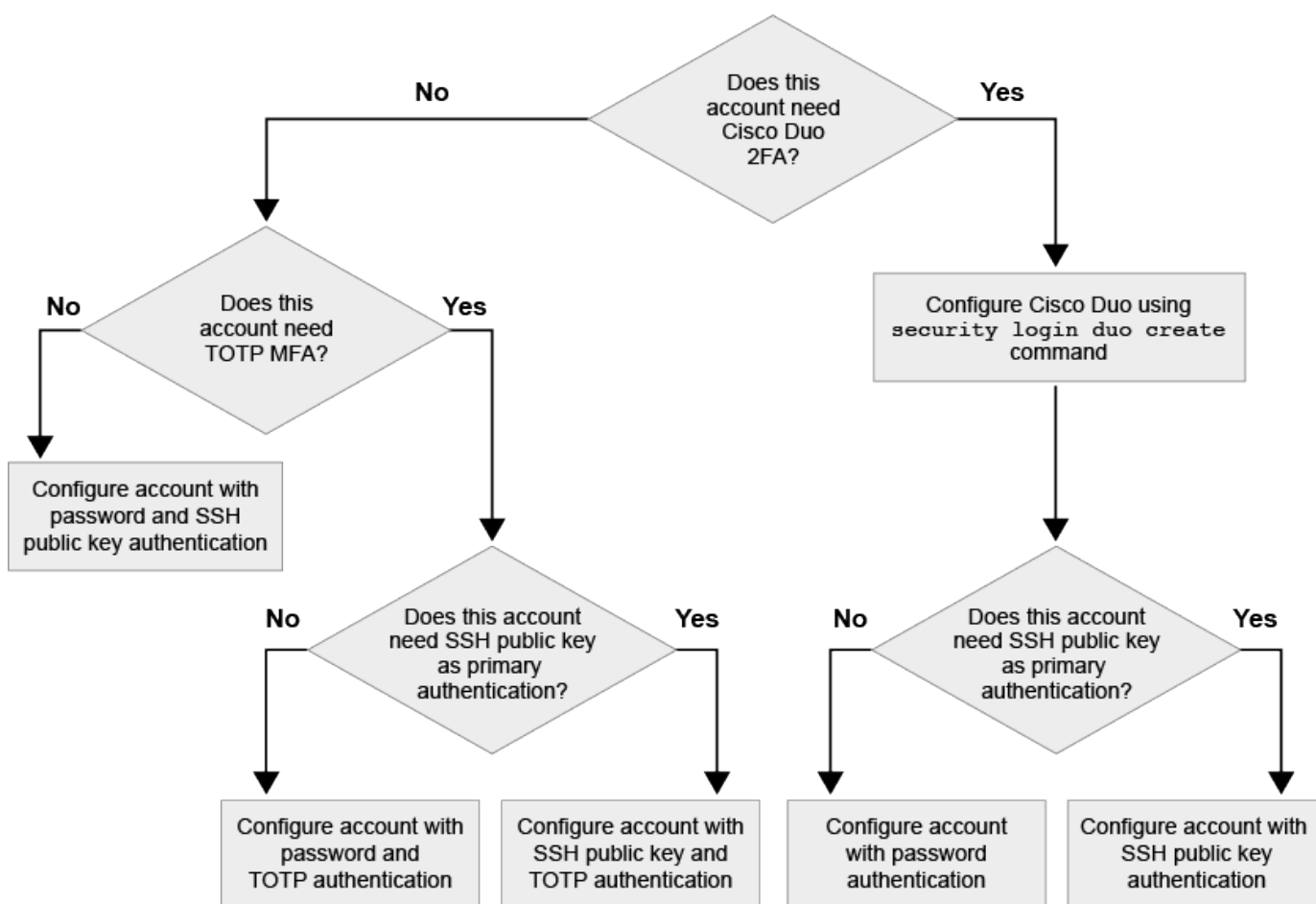
Panoramica dell'autenticazione a più fattori

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.



Abilitare l'autenticazione a più fattori

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 sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

"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 `SVMengData1` 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".

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>
```

2. Verificare che MFA con TOTP sia attivato:

```
security login show
```

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

Scopri di più ["Autenticazione multifattore in ONTAP 9 \(TR-4647\)"](#).

Configurare l'account utente locale per MFA con TOTP

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

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.

TOTP è supportato da diverse applicazioni di autenticazione come Google Authenticator.

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>"
```

Reimpostare la chiave segreta TOTP

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>
```

Disattiva la chiave segreta TOTP per l'account locale

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 delete -vserver "<svm_name>" -username  
"<account_username>"
```

Abilitare gli account dei certificati SSL

È possibile utilizzare `security login create` Comando per consentire agli account amministratore di accedere a un 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
```

Per la sintassi completa dei comandi, vedere ["Man page di ONTAP per release"](#).

Il seguente comando attiva l'account amministratore SVM `svmadmin2` con l'impostazione predefinita `vsadmin` Ruolo per accedere a `SVMengData2` Utilizzando un certificato digitale SSL.

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

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](#)

Abilitare l'accesso all'account Active Directory

È possibile utilizzare `security login create` Comando per abilitare gli account utente o di gruppo Active Directory (ad) per accedere 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 ["LDAP fast bind per l'autenticazione nsswitch"](#) Se supportato dal server LDAP ad.
- Se non si è sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

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

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
9.0 e versioni successive	Dominio	Nessuno	<pre>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]</pre>

Per gruppi ad:

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
9.0 e versioni successive	Dominio	Nessuno	<pre>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]</pre>

Per la sintassi completa dei comandi, vedere ["Fogli di lavoro per l'autenticazione dell'amministratore e la configurazione RBAC"](#)

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](#)

Abilitare l'accesso all'account LDAP o NIS

È possibile utilizzare `security login create` Comando per abilitare gli account utente LDAP o NIS per accedere a un SVM di amministrazione o 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 sicuri del ruolo di controllo degli accessi che si desidera assegnare all'account di accesso, è possibile utilizzare `security login modify` per aggiungere il ruolo in un secondo momento.

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 "[LDAP fast bind per l'autenticazione nsswitch](#)" Se 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]
```

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

"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
```

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](#)

Gestire i ruoli di controllo degli accessi

Panoramica sui ruoli di controllo degli accessi

Il ruolo assegnato a un amministratore determina i comandi a cui l'amministratore ha accesso. Il ruolo viene assegnato quando si crea l'account per l'amministratore. È possibile assegnare un ruolo diverso o definire ruoli personalizzati in base alle esigenze.

Modificare il ruolo assegnato a un amministratore

È possibile utilizzare `security login modify` Comando per modificare il ruolo di un account di amministratore di cluster o SVM. È possibile assegnare un ruolo predefinito o personalizzato.

Prima di iniziare

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

Fase

1. Modificare il ruolo di un amministratore di cluster o SVM:

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

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

"Creazione o modifica degli account di accesso"

Il seguente comando modifica il ruolo dell'account amministratore del cluster ad `DOMAIN1\guest1` al predefinito `readonly` ruolo.

```
cluster1::>security login modify -vserver engCluster -user-or-group-name  
DOMAIN1\guest1 -application ssh -authmethod domain -role readonly
```

Il seguente comando modifica il ruolo degli account amministratore SVM nell'account di gruppo ad `DOMAIN1\adgroup` al personalizzato `vol_role` ruolo.

```
cluster1::>security login modify -vserver engData -user-or-group-name  
DOMAIN1\adgroup -application ssh -authmethod domain -role vol_role
```

Definire ruoli personalizzati

È possibile utilizzare `security login role create` per definire un ruolo personalizzato. È possibile eseguire il comando tutte le volte necessarie per ottenere la combinazione esatta di funzionalità che si desidera associare al ruolo.

A proposito di questa attività

- Un ruolo, predefinito o personalizzato, concede o nega l'accesso ai comandi ONTAP o alle directory dei comandi.

Una directory di comandi (`volume`, ad esempio) è un gruppo di sottodirectory di comandi e comandi correlati. Ad eccezione di quanto descritto in questa procedura, la concessione o il rifiuto dell'accesso a una directory di comandi concede o nega l'accesso a ciascun comando nella directory e nelle relative sottodirectory.

- L'accesso a comandi o sottodirectory specifici sovrascrive l'accesso alla directory principale.

Se un ruolo viene definito con una directory di comandi e quindi viene definito nuovamente con un livello di accesso diverso per un comando specifico o per una sottodirectory della directory principale, il livello di accesso specificato per il comando o la sottodirectory sovrascrive quello della directory principale.



Non è possibile assegnare a un amministratore SVM un ruolo che dia accesso a una directory di comandi o comandi disponibile solo per `admin` amministratore del cluster, ad esempio `security directory` dei comandi.

Prima di iniziare

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

Fase

1. Definire un ruolo personalizzato:

```
security login role create -vserver SVM_name -role role -cmddirname  
command_or_directory_name -access access_level -query query
```

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

I seguenti comandi assegnano a `vol_role` accesso completo ai comandi in `volume` directory dei comandi e accesso in sola lettura ai comandi in `volume snapshot` sottodirectory.

```
cluster1::>security login role create -role vol_role -cmddirname  
"volume" -access all
```

```
cluster1::>security login role create -role vol_role -cmddirname "volume  
snapshot" -access readonly
```

I seguenti comandi assegnano a `SVM_storage` accesso in sola lettura ai comandi in `storage directory` dei comandi, nessun accesso ai comandi in `storage encryption sottodirectory` e accesso completo a `storage aggregate plex offline` comando non intrinseco.

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage" -access readonly
```

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage encryption" -access none
```

```
cluster1::>security login role create -role SVM_storage -cmddirname  
"storage aggregate plex offline" -access all
```

Ruoli predefiniti per gli amministratori del cluster

I ruoli predefiniti per gli amministratori dei cluster devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore del cluster viene assegnato il valore predefinito `admin` ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori del cluster:

Questo ruolo...	Dispone di questo livello di accesso...	Alle seguenti directory di comandi o comandi
amministratore	tutto	Tutte le directory dei comandi (DEFAULT)
admin-no-fsa (disponibile a partire da ONTAP 9.12.1)	Lettura/scrittura	<ul style="list-style-type: none">• Tutte le directory dei comandi (DEFAULT)• <code>security login rest-role</code>• <code>security login role</code>

Di sola lettura	<ul style="list-style-type: none"> • security login rest-role create • security login rest-role delete • security login rest-role modify • security login rest-role show • security login role create • security login role create • security login role delete • security login role modify • security login role show • volume activity-tracking • volume analytics 	Nessuno
volume file show-disk-usage	AutoSupport	tutto
<ul style="list-style-type: none"> • set • system node autosupport 	nessuno	Tutte le altre directory di comando (DEFAULT)
backup	tutto	vserver services ndmp
readonly	volume	nessuno
Tutte le altre directory di comando (DEFAULT)	readonly	tutto

<ul style="list-style-type: none"> • security login password <p>Solo per la gestione della password locale del proprio account utente e delle informazioni sulle chiavi</p> <ul style="list-style-type: none"> • set 	nessuno	security
readonly	Tutte le altre directory di comando (DEFAULT)	nessuno



Il autosupport il ruolo viene assegnato al predefinito autosupport Account, utilizzato da AutoSupport OnDemand. ONTAP impedisce di modificare o eliminare autosupport account. ONTAP impedisce inoltre l'assegnazione di autosupport ruolo per altri account utente.

Ruoli predefiniti per gli amministratori SVM

I ruoli predefiniti per gli amministratori SVM devono soddisfare la maggior parte delle esigenze. È possibile creare ruoli personalizzati in base alle necessità. Per impostazione predefinita, a un amministratore SVM viene assegnato il valore predefinito `vsadmin` ruolo.

La seguente tabella elenca i ruoli predefiniti per gli amministratori SVM:

Nome del ruolo	Funzionalità
vsadmin	<ul style="list-style-type: none"> • Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, ad eccezione degli spostamenti dei volumi • Gestione di quote, qtree, copie Snapshot e file • Gestione delle LUN • Esecuzione delle operazioni SnapLock, ad eccezione dell'eliminazione con privilegi • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitoraggio delle connessioni di rete e dell'interfaccia di rete • Monitoraggio dello stato di salute di SVM

volume vsadmin	<ul style="list-style-type: none"> • Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, compresi gli spostamenti dei volumi • Gestione di quote, qtree, copie Snapshot e file • Gestione delle LUN • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Interfaccia di rete di monitoraggio • Monitoraggio dello stato di salute di SVM
protocollo vsadmin	<ul style="list-style-type: none"> • Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Configurazione dei protocolli: NFS, SMB, iSCSI, FC, FCoE, NVMe/FC e NVMe/TCP • Configurazione dei servizi: DNS, LDAP e NIS • Gestione delle LUN • Interfaccia di rete di monitoraggio • Monitoraggio dello stato di salute di SVM
vsadmin-backup	<ul style="list-style-type: none"> • Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione delle operazioni NDMP • Creazione di un volume ripristinato in lettura/scrittura • Gestione delle relazioni SnapMirror e delle copie Snapshot • Visualizzazione di volumi e informazioni di rete

vsadmin-snaplock	<ul style="list-style-type: none"> • Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Gestione dei volumi, ad eccezione degli spostamenti dei volumi • Gestione di quote, qtree, copie Snapshot e file • Esecuzione di operazioni SnapLock, inclusa l'eliminazione con privilegi • Configurazione dei protocolli: NFS e SMB • Configurazione dei servizi: DNS, LDAP e NIS • Monitoraggio dei lavori • Monitoraggio delle connessioni di rete e dell'interfaccia di rete
vsadmin-readonly	<ul style="list-style-type: none"> • Gestione delle informazioni relative alla password locale e alle chiavi del proprio account utente • Monitoraggio dello stato di salute di SVM • Interfaccia di rete di monitoraggio • Visualizzazione di volumi e LUN • Visualizzazione di servizi e protocolli

Controllare l'accesso dell'amministratore

Il ruolo assegnato a un amministratore determina le funzioni che l'amministratore può eseguire con System Manager. System Manager fornisce ruoli predefiniti per gli amministratori dei cluster e gli amministratori delle macchine virtuali dello storage. Il ruolo viene assegnato quando si crea l'account dell'amministratore oppure è possibile assegnarlo in un secondo momento.

A seconda di come è stato attivato l'accesso all'account, potrebbe essere necessario eseguire una delle seguenti operazioni:

- Associare una chiave pubblica a un account locale.
- Installare un certificato digitale del server firmato dalla CA.
- Configurare l'accesso ad, LDAP o NIS.

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

Assegnazione di un ruolo a un amministratore

Assegnare un ruolo a un amministratore, come indicato di seguito:

Fasi


1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare ➔ Accanto a **utenti e ruoli**.

3. Selezionare **+ Add** Sotto **utenti**.
4. Specificare un nome utente e selezionare un ruolo nel menu a discesa per **ruolo**.
5. Specificare un metodo di accesso e una password per l'utente.

Modifica del ruolo di amministratore

Modificare il ruolo di amministratore, come segue:

Fasi

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Selezionare il nome dell'utente di cui si desidera modificare il ruolo, quindi fare clic su  visualizzato accanto al nome utente.
3. Fare clic su **Edit** (Modifica).
4. Selezionare un ruolo nel menu a discesa per **ruolo**.

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 svmin2 Per SVM engData2. Alla chiave pubblica viene assegnato il numero di indice 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>
```

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 svmin2 Per SVM engData2 al numero di indice 6.

```
cluster1::> security login publickey modify -vserver engData2 -username svmin2 -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 "erver1.companyname.com", con sede a Sunnyvale, California, USA. L'indirizzo e-mail dell'amministratore del contatto della SVM è "[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
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUA0EA6EagLfso5+4g+ejiRKKTUPQO
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==
-----END CERTIFICATE REQUEST-----
```

Private Key :

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

```
MIIBOwIBAAJBAPXFanNoJApTlnzSxOcxixqImRRGZCR7tVmTYyqPSuTvfhVtwDJb
mXuj6U3alwoUsb13wfEvQnHVFNCi2ninsJ8CAwEAAQJAWt2AO+bW3FKezEuIrQlu
KoMyRYK455wtMk8BrOyJfhYsB20B28eifjJvRWdTOBEav99M7cEzgPv+p5kaZTTM
gQIhAPsp+j1hrUXSRj979LIJJY0sNez397i7ViFXWQScx/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
AMQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAyXrK2sry
-----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
QXV0aG9yaXR5MSEwHwYDVQQDEwExd3d3LnZhbG1jZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm9lcCwgSW5jLjExMC8GA1UECzMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----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.

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...
Autorità di certificazione attendibili	<ul style="list-style-type: none"> • [install-trusted-cert] • Eliminare un'autorità di certificazione attendibile • Rinnovare un'autorità di certificazione attendibile
Certificati client/server	<ul style="list-style-type: none"> • [install-cs-cert] • [gen-cs-cert] • [delete-cs-cert] • [renew-cs-cert]
Autorità locali di certificazione	<ul style="list-style-type: none"> • Creare una nuova autorità di certificazione locale • Firmare un certificato utilizzando un'autorità di certificazione locale • Eliminare un'autorità di certificazione locale • Rinnovare un'autorità di certificazione locale

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.

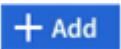
Fasi

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.

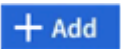
Fasi

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 `SVMvs1.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 `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.

Gestire la verifica multi-admin

Panoramica sulla verifica multi-admin

A partire da ONTAP 9.11.1, è possibile utilizzare la verifica multi-admin (MAV) per garantire che determinate operazioni, come l'eliminazione di volumi o copie Snapshot, possano essere eseguite solo dopo l'approvazione da parte degli amministratori designati. In questo modo si evita che gli amministratori compromessi, dannosi o inesperti apportino modifiche indesiderate o eliminino dati.

La configurazione della verifica multi-admin comprende:

- "Creazione di uno o più gruppi di approvazione dell'amministratore."
- "Abilitazione della funzionalità di verifica multi-admin."

- ["Aggiunta o modifica di regole."](#)

Dopo la configurazione iniziale, questi elementi possono essere modificati solo dagli amministratori di un gruppo di approvazione MAV (amministratori MAV).

Quando la verifica multi-admin è attivata, il completamento di ogni operazione protetta richiede tre passaggi:

- Quando un utente avvia l'operazione, un ["la richiesta viene generata."](#)
- Prima che possa essere eseguito, almeno uno ["L'amministratore MAV deve approvare."](#)
- Dopo l'approvazione, l'utente completa l'operazione.

La verifica multi-admin non è prevista per l'utilizzo con volumi o flussi di lavoro che comportano un'elevata automazione, perché ogni attività automatizzata richiederebbe l'approvazione prima che l'operazione possa essere completata. Se si desidera utilizzare l'automazione e MAV insieme, si consiglia di utilizzare le query per specifiche operazioni MAV. Ad esempio, è possibile fare domanda `volume delete`. Le regole MAV si applicano solo ai volumi in cui l'automazione non è coinvolta ed è possibile designare tali volumi con uno schema di denominazione specifico.



Se è necessario disattivare la funzionalità di verifica multi-admin senza l'approvazione dell'amministratore MAV, contattare il supporto NetApp e citare il seguente articolo della Knowledge base: ["Come disattivare la verifica multi-amministratore se MAV admin non è disponibile"](#).

Come funziona la verifica multi-admin

La verifica multi-admin consiste in:

- Un gruppo di uno o più amministratori con poteri di approvazione e veto.
- Un insieme di operazioni o comandi protetti in una *tabella di regole*.
- Un *motore di regole* per identificare e controllare l'esecuzione di operazioni protette.

Le regole MAV vengono valutate in base alle regole RBAC (role-based access control). Pertanto, gli amministratori che eseguono o approvano operazioni protette devono già disporre dei privilegi RBAC minimi per tali operazioni. ["Scopri di più su RBAC."](#)

Regole definite dal sistema

Quando la verifica multi-admin è attivata, le regole definite dal sistema (note anche come regole *guard-rail*) stabiliscono un insieme di operazioni MAV per contenere il rischio di aggirare il processo MAV stesso. Queste operazioni non possono essere rimosse dalla tabella delle regole. Una volta abilitato MAV, le operazioni contrassegnate da un asterisco (*) devono essere approvate da uno o più amministratori prima dell'esecuzione, ad eccezione dei comandi **show**.

- `security multi-admin-verify modify funzionamento*`

Controlla la configurazione della funzionalità di verifica multi-admin.

- `security multi-admin-verify approval-group operazioni*`

Controlla l'appartenenza all'insieme di amministratori con credenziali di verifica multi-admin.

- `security multi-admin-verify rule operazioni*`

Controlla il set di comandi che richiedono la verifica multi-admin.

- `security multi-admin-verify request` operazioni

Controllare il processo di approvazione.

Comandi protetti da regole

Oltre ai comandi definiti dal sistema, i seguenti comandi sono protetti per impostazione predefinita quando è attivata la verifica multi-admin, ma è possibile modificare le regole per rimuovere la protezione per questi comandi.

- `security login password`
- `security login unlock`
- `set`

I seguenti comandi possono essere protetti in ONTAP 9.11.1 e versioni successive.

<code>cluster peer delete</code>	<code>volume snapshot autodelete modify</code>
<code>event config modify</code>	<code>volume snapshot delete</code>
<code>security login create</code>	<code>volume snapshot policy add-schedule</code>
<code>security login delete</code>	<code>volume snapshot policy create</code>
<code>security login modify</code>	<code>volume snapshot policy delete</code>
<code>system node run</code>	<code>volume snapshot policy modify</code>
<code>system node systemshell</code>	<code>volume snapshot policy modify-schedule</code>
<code>volume delete</code>	<code>volume snapshot policy remove-schedule</code>
<code>volume flexcache delete</code>	<code>volume snapshot restore</code>
	<code>vserver peer delete</code>

I seguenti comandi possono essere protetti a partire da ONTAP 9.13.1:

- `volume snaplock modify`
- `security anti-ransomware volume attack clear-suspect`
- `security anti-ransomware volume disable`
- `security anti-ransomware volume pause`

I seguenti comandi possono essere protetti a partire da ONTAP 9.14.1:

- `volume recovery-queue modify`

- `volume recovery-queue purge`
- `volume recovery-queue purge-all`
- `vserver modify`

Come funziona l'approvazione multi-admin

Ogni volta che un'operazione protetta viene inserita in un cluster protetto da MAV, una richiesta di esecuzione dell'operazione viene inviata al gruppo di amministratori MAV designato.

È possibile configurare:

- I nomi, le informazioni di contatto e il numero di amministratori nel gruppo MAV.

Un amministratore MAV deve avere un ruolo RBAC con privilegi di amministratore del cluster.

- Il numero di gruppi di amministratori MAV.
 - Viene assegnato un gruppo MAV per ogni regola operativa protetta.
 - Per più gruppi MAV, è possibile configurare quale gruppo MAV approva una data regola.
- Il numero di approvazioni MAV richieste per eseguire un'operazione protetta.
- Un periodo di *scadenza dell'approvazione* entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione.
- Un periodo di *scadenza dell'esecuzione* entro il quale l'amministratore richiedente deve completare l'operazione.

Una volta configurati questi parametri, è necessaria l'approvazione MAV per modificarli.

Gli amministratori MAV non possono approvare le proprie richieste di esecuzione di operazioni protette. Pertanto:

- MAV non deve essere abilitato sui cluster con un solo amministratore.
- Se nel gruppo MAV è presente una sola persona, l'amministratore MAV non può inserire operazioni protette; gli amministratori regolari devono inserirle e l'amministratore MAV può solo approvarle.
- Se si desidera che gli amministratori MAV siano in grado di eseguire operazioni protette, il numero di amministratori MAV deve essere maggiore di uno rispetto al numero di approvazioni richieste. Ad esempio, se sono necessarie due approvazioni per un'operazione protetta e si desidera che gli amministratori MAV le eseguano, devono essere presenti tre persone nel gruppo di amministratori MAV.

Gli amministratori MAV possono ricevere richieste di approvazione in avvisi e-mail (tramite EMS) oppure interrogare la coda delle richieste. Quando ricevono una richiesta, possono intraprendere una delle tre azioni seguenti:

- Approvare
- Rifiuto (veto)
- Ignora (nessuna azione)

Le notifiche e-mail vengono inviate a tutti i responsabili dell'approvazione associati a una regola MAV quando:

- Viene creata una richiesta.
- Una richiesta viene approvata o vetoata.

- Viene eseguita una richiesta approvata.

Se il richiedente si trova nello stesso gruppo di approvazione per l'operazione, riceverà un'e-mail quando la richiesta verrà approvata.

Nota: Un richiedente non può approvare le proprie richieste, anche se si trova nel gruppo di approvazione. Ma possono ricevere le notifiche via email. I richiedenti che non fanno parte di gruppi di approvazione (vale a dire, che non sono amministratori MAV) non ricevono notifiche via email.

Come funziona l'esecuzione di operazioni protette

Se l'esecuzione viene approvata per un'operazione protetta, l'utente richiedente continua con l'operazione quando richiesto. Se l'operazione è vetoed, l'utente richiedente deve eliminare la richiesta prima di procedere.

Le regole MAV vengono valutate dopo le autorizzazioni RBAC. Di conseguenza, un utente senza autorizzazioni RBAC sufficienti per l'esecuzione dell'operazione non può avviare il processo di richiesta MAV.

Gestire i gruppi di approvazione degli amministratori

Prima di attivare la verifica multi-amministratore (MAV), è necessario creare un gruppo di approvazione amministratore contenente uno o più amministratori a cui concedere l'autorizzazione di approvazione o veto. Una volta attivata la verifica multi-admin, qualsiasi modifica all'appartenenza al gruppo di approvazione richiede l'approvazione di uno degli amministratori qualificati esistenti.

A proposito di questa attività

È possibile aggiungere amministratori esistenti a un gruppo MAV o creare nuovi amministratori.



La funzionalità MAV rispetta le impostazioni RBAC (role-based access control) esistenti. I potenziali amministratori MAV devono disporre di privilegi sufficienti per eseguire operazioni protette prima di aggiungerli ai gruppi di amministratori MAV. ["Scopri di più su RBAC."](#)

È possibile configurare MAV per avvisare gli amministratori MAV che le richieste di approvazione sono in sospeso. A tale scopo, è necessario configurare le notifiche e-mail, in particolare i Mail From e Mail Server parametri—oppure è possibile cancellare questi parametri per disattivare la notifica. Senza avvisi via email, gli amministratori MAV devono controllare manualmente la coda di approvazione.



Procedura di System Manager

Se si desidera creare un gruppo di approvazione MAV per la prima volta, consultare la procedura di System Manager in ["attiva la verifica multi-admin."](#)

Per modificare un gruppo di approvazione esistente o creare un gruppo di approvazione aggiuntivo:

1. Identificare gli amministratori per ricevere la verifica multi-admin.
 - a. Fare clic su **Cluster > Settings**.
 - b. Fare clic su  Accanto a **utenti e ruoli**.
 - c. Fare clic su  **Add** Sotto **utenti**.
 - d. Modificare il registro in base alle esigenze.

Per ulteriori informazioni, vedere ["Controllare l'accesso dell'amministratore."](#)

2. Creare o modificare il gruppo di approvazione MAV:
 - a. Fare clic su **Cluster > Settings**.
 - b. Fare clic su  Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**. (Viene visualizzata la  Se MAV non è ancora configurato).
 - Name (Nome): Immettere un nome di gruppo.
 - Responsabili dell'approvazione: Selezionare i responsabili dell'approvazione da un elenco di utenti.
 - Email address (Indirizzo email): Inserire gli indirizzi email.
 - Default group (Gruppo predefinito): Selezionare un gruppo.

L'approvazione MAV è necessaria per modificare una configurazione esistente una volta abilitato MAV.

Procedura CLI

1. Verificare che siano stati impostati i valori per Mail From e Mail Server parametri. Inserire:

```
event config show
```

Il display dovrebbe essere simile a quanto segue:

```
cluster01::> event config show
                        Mail From:  admin@localhost
                        Mail Server: localhost
                        Proxy URL:  -
                        Proxy User:  -
                        Publish/Subscribe Messaging Enabled: true
```

Per configurare questi parametri, immettere:

```
event config modify -mail-from email_address -mail-server server_name
```

2. Identificare gli amministratori per ricevere la verifica multi-admin

Se si desidera...	Immettere questo comando
Visualizza gli amministratori correnti	<code>security login show</code>
Modificare le credenziali degli amministratori correnti	<code>security login modify <parameters></code>
Creare nuovi account amministratore	<code>security login create -user-or-group -name <i>admin_name</i> -application ssh -authentication-method password</code>

3. Creare il gruppo di approvazione MAV:

```
security multi-admin-verify approval-group create [ -vserver svm_name] -name group_name -approvers approver1 [, approver2...] [[-email address1], address1...]
```

- `-vserver` - Solo la SVM amministrativa è supportata in questa versione.
- `-name` - Il nome del gruppo MAV, composto da un massimo di 64 caratteri.
- `-approvers` - L'elenco di uno o più responsabili dell'approvazione.
- `-email` - Uno o più indirizzi e-mail che vengono notificati quando una richiesta viene creata, approvata, sottoposta a veto o eseguita.

Esempio: il seguente comando crea un gruppo MAV con due membri e indirizzi e-mail associati.

```
cluster-1::> security multi-admin-verify approval-group create -name
mav-grp1 -approvers pavan,julia -email pavan@myfirm.com,julia@myfirm.com
```

4. Verificare la creazione e l'appartenenza del gruppo:

```
security multi-admin-verify approval-group show
```

Esempio:

```
cluster-1::> security multi-admin-verify approval-group show
Vserver   Name           Approvers      Email
-----
-----
svm-1     mav-grp1      pavan,julia    email
pavan@myfirm.com,julia@myfirm.com
```

Utilizzare questi comandi per modificare la configurazione iniziale del gruppo MAV.

Nota: tutti richiedono l'approvazione dell'amministratore MAV prima dell'esecuzione.

Se si desidera...	Immettere questo comando
Modificare le caratteristiche del gruppo o le informazioni sui membri esistenti	<code>security multi-admin-verify approval-group modify [parameters]</code>
Aggiungere o rimuovere membri	<code>security multi-admin-verify approval-group replace [-vserver svm_name] -name group_name [-approvers-to-add approver1[,approver2...]] [-approvers-to-remove approver1[,approver2...]]</code>
Eliminare un gruppo	<code>security multi-admin-verify approval-group delete [-vserver svm_name] -name group_name</code>

Attiva e disattiva la verifica multi-admin

La verifica multi-admin (MAV) deve essere attivata esplicitamente. Una volta attivata la verifica multi-admin, l'approvazione da parte degli amministratori di un gruppo di approvazione MAV (amministratori MAV) è necessaria per eliminarla.

A proposito di questa attività

Una volta attivato MAV, la modifica o la disattivazione di MAV richiede l'approvazione dell'amministratore MAV.



Se è necessario disattivare la funzionalità di verifica multi-admin senza l'approvazione dell'amministratore MAV, contattare il supporto NetApp e citare il seguente articolo della Knowledge base: "[Come disattivare la verifica multi-amministratore se MAV admin non è disponibile](#)".

Quando si attiva MAV, è possibile specificare globalmente i seguenti parametri.

Gruppi di approvazione

Un elenco di gruppi di approvazione globali. Per abilitare la funzionalità MAV è necessario almeno un gruppo.



Se si utilizza MAV con la protezione ransomware autonoma (ARP), definire un gruppo di approvazione nuovo o esistente responsabile dell'approvazione della pausa, della disattivazione e dell'eliminazione delle richieste sospette di ARP.

Responsabili dell'approvazione richiesti

Il numero di responsabili dell'approvazione necessari per eseguire un'operazione protetta. Il numero predefinito e minimo è 1.



Il numero richiesto di responsabili dell'approvazione deve essere inferiore al numero totale di responsabili dell'approvazione univoci nei gruppi di approvazione predefiniti.

Scadenza approvazione (ore, minuti, secondi)

Periodo entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione. Il valore predefinito è un'ora (1h), il valore minimo supportato è un secondo (1s) e il valore massimo supportato è 14 giorni (14d).

Scadenza dell'esecuzione (ore, minuti, secondi)



Il periodo entro il quale l'amministratore richiedente deve completare l'operazione:: Il valore predefinito è un'ora (1h), il valore minimo supportato è un secondo (1s) e il valore massimo supportato è 14 giorni (14d).

È inoltre possibile eseguire l'override di uno qualsiasi di questi parametri per specifici "[regole operative](#)."

Procedura di System Manager

1. Identificare gli amministratori per ricevere la verifica multi-admin.
 - a. Fare clic su **Cluster > Settings**.
 - b. Fare clic su [→](#) Accanto a **utenti e ruoli**.
 - c. Fare clic su [+](#) **Add** Sotto **utenti**.
 - d. Modificare il registro in base alle esigenze.


Per ulteriori informazioni, vedere ["Controllare l'accesso dell'amministratore."](#)

2. Abilitare la verifica multi-admin creando almeno un gruppo di approvazione e aggiungendo almeno una regola.
 - a. Fare clic su **Cluster > Settings**.
 - b. Fare clic su  Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**.
 - c. Fare clic su  **Add** per aggiungere almeno un gruppo di approvazione.
 - Name (Nome): Immettere il nome di un gruppo.
 - Responsabili dell'approvazione: Selezionare i responsabili dell'approvazione da un elenco di utenti.
 - Email address (Indirizzo e-mail) – inserire gli indirizzi e-mail.
 - Default group (Gruppo predefinito) – selezionare un gruppo.
 - d. Aggiungere almeno una regola.
 - Operation (funzionamento) – selezionare un comando supportato dall'elenco.
 - Query - immettere le opzioni e i valori dei comandi desiderati.
 - Parametri facoltativi; lasciare vuoto per applicare le impostazioni globali o assegnare un valore diverso per regole specifiche per sostituire le impostazioni globali.
 - Numero richiesto di responsabili dell'approvazione
 - Gruppi di approvazione
 - e. Fare clic su **Advanced Settings** (Impostazioni avanzate) per visualizzare o modificare le impostazioni predefinite.
 - Numero richiesto di responsabili dell'approvazione (impostazione predefinita: 1)
 - Scadenza richiesta di esecuzione (impostazione predefinita: 1 ora)
 - Scadenza richiesta di approvazione (impostazione predefinita: 1 ora)
 - Server di posta*
 - Da indirizzo email*

*Questi aggiornano le impostazioni e-mail gestite in "Gestione notifiche". Se non sono ancora stati configurati, viene richiesto di impostarli.
 - f. Fare clic su **Enable** (attiva) per completare la configurazione iniziale MAV.

Dopo la configurazione iniziale, lo stato MAV corrente viene visualizzato nel riquadro **Multi-Admin Approval**.

- Stato (attivato o meno)
- Operazioni attive per le quali sono richieste approvazioni
- Numero di richieste aperte in stato di attesa

È possibile visualizzare una configurazione esistente facendo clic su . L'approvazione MAV è necessaria per modificare una configurazione esistente.

Per disattivare la verifica multi-admin:

1. Fare clic su **Cluster > Settings**.
2. Fare clic su  Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**.

3. Fare clic sul pulsante di attivazione/disattivazione.

Per completare questa operazione è richiesta l'approvazione MAV.

Procedura CLI

Prima di attivare la funzionalità MAV nella CLI, almeno una "[Gruppo di amministratori MAV](#)" deve essere stato creato.

Se si desidera...	Immettere questo comando
Abilitare la funzionalità MAV	<pre>security multi-admin-verify modify -approval-groups <i>group1</i> [, <i>group2</i>...] [- required-approvers <i>nn</i>] -enabled true [-execution-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]] [-approval-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]]</pre> <p>Esempio: Il seguente comando abilita MAV con 1 gruppo di approvazione, 2 responsabili dell'approvazione richiesti e periodi di scadenza predefiniti.</p> <pre>cluster-1::> security multi-admin- verify modify -approval-groups mav-grp1 -required-approvers 2 -enabled true</pre> <p>Completare la configurazione iniziale aggiungendone almeno una "regola operativa."</p>
Modifica di una configurazione MAV (richiede l'approvazione MAV)	<pre>security multi-admin-verify approval- group modify [-approval-groups <i>group1</i> [, <i>group2</i>...]] [-required-approvers <i>nn</i>] [-execution-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]] [-approval-expiry [<i>nnh</i>][<i>nnm</i>][<i>nns</i>]]</pre>

Se si desidera...	Immettere questo comando
Verificare la funzionalità MAV	<pre>security multi-admin-verify show</pre> <p>Esempio:</p> <pre>cluster-1::> security multi-admin-verify show Is Required Execution Approval Approval Enabled Approvers Expiry Expiry Groups ----- true 2 1h 1h mav-grp1</pre>
Disattivare la funzionalità MAV (richiede l'approvazione MAV)	<pre>security multi-admin-verify modify -enabled false</pre>

Gestire le regole operative protette

Si creano regole di verifica multi-amministratore (MAV) per designare le operazioni che richiedono l'approvazione. Ogni volta che viene avviata un'operazione, le operazioni protette vengono intercettate e viene generata una richiesta di approvazione.

Le regole possono essere create prima di abilitare MAV da qualsiasi amministratore con funzionalità RBAC appropriate, ma una volta attivata la MAV, qualsiasi modifica al set di regole richiede l'approvazione MAV.

È possibile creare una sola regola MAV per operazione; ad esempio, non è possibile creare più regole `volume-snapshot-delete` regole. Tutti i vincoli di regola desiderati devono essere contenuti all'interno di una regola.

Comandi protetti da regole

È possibile creare regole per proteggere i seguenti comandi, a partire da ONTAP 9.11.1.

cluster peer delete	volume snapshot autodelete modify
event config modify	volume snapshot delete
security login create	volume snapshot policy add-schedule
security login delete	volume snapshot policy create
security login modify	volume snapshot policy delete
system node run	volume snapshot policy modify
system node systemshell	volume snapshot policy modify-schedule
volume delete	volume snapshot policy remove-schedule
volume flexcache delete	volume snapshot restore
	vserver peer delete

È possibile creare regole per proteggere i seguenti comandi a partire da ONTAP 9.13.1:

- volume snaplock modify
- security anti-ransomware volume attack clear-suspect
- security anti-ransomware volume disable
- security anti-ransomware volume pause

È possibile creare regole per proteggere i seguenti comandi a partire da ONTAP 9.14.1:

- volume recovery-queue modify
- volume recovery-queue purge
- volume recovery-queue purge-all
- vserver modify

Le regole per i comandi MAV di default del sistema, il security multi-admin-verify "**comandi**", non può essere modificato.

Oltre ai comandi definiti dal sistema, i seguenti comandi sono protetti per impostazione predefinita quando è attivata la verifica multi-admin, ma è possibile modificare le regole per rimuovere la protezione per questi comandi.

- security login password
- security login unlock
- set

Vincoli della regola

Quando si crea una regola, è possibile specificare il `-query` opzione per limitare la richiesta a un sottoinsieme della funzionalità del comando. Il `-query` Può essere utilizzata anche per limitare gli elementi di configurazione, come SVM, volume e nomi delle Snapshot.

Ad esempio, in volume snapshot delete comando, `-query` può essere impostato su `-snapshot !hourly*,!daily*,!weekly*`, Ovvero, le istantanee del volume con attributi orari, giornalieri o settimanali sono escluse dalle protezioni MAV.

```
smci-vs1m20::> security multi-admin-verify rule show
```

		Required	Approval
Vserver	Operation	Approvers	Groups
vs01	volume snapshot delete	-	-
	Query: -snapshot !hourly*,!daily*,!weekly*		



Tutti gli elementi di configurazione esclusi non sono protetti da MAV e qualsiasi amministratore può eliminarli o rinominarli.

Per impostazione predefinita, le regole specificano un corrispondente `security multi-admin-verify request create "protected_operation"` il comando viene generato automaticamente quando si inserisce un'operazione protetta. È possibile modificare questa impostazione predefinita in modo che richieda `request create` il comando deve essere immesso separatamente.



Per impostazione predefinita, le regole ereditano le seguenti impostazioni MAV globali, anche se è possibile specificare eccezioni specifiche della regola:

- Numero richiesto di approvatori
- Gruppi di approvazione
- Periodo di scadenza dell'approvazione
- Periodo di scadenza dell'esecuzione

Procedura di System Manager

Se si desidera aggiungere una regola operativa protetta per la prima volta, consultare la procedura di System Manager in ["attiva la verifica multi-admin."](#)

Per modificare il set di regole esistente:

1. Selezionare **Cluster > Settings** (cluster > Impostazioni).
2. Selezionare  Accanto a **approvazione multi-amministratore** nella sezione **sicurezza**.
3. Selezionare  **Add** per aggiungere almeno una regola, è anche possibile modificare o eliminare le regole esistenti.
 - Operation (funzionamento) – selezionare un comando supportato dall'elenco.
 - Query - immettere le opzioni e i valori dei comandi desiderati.
 - Parametri facoltativi: Lasciare vuoto per applicare le impostazioni globali o assegnare un valore diverso per regole specifiche per sostituire le impostazioni globali.

- Numero richiesto di responsabili dell'approvazione
- Gruppi di approvazione

Procedura CLI



Tutto `security multi-admin-verify rule` I comandi richiedono l'approvazione dell'amministratore MAV prima dell'esecuzione tranne `security multi-admin-verify rule show`.

Se si desidera...	Immettere questo comando
Creare una regola	<code>security multi-admin-verify rule create -operation "protected_operation" [-query operation_subset] [parameters]</code>
Modificare le credenziali degli amministratori correnti	<code>security login modify <parameters></code> Esempio: La seguente regola richiede l'approvazione per eliminare il volume root. <code>security multi-admin-verify rule create -operation "volume delete" -query "-vserver vs0"</code>
Modificare una regola	<code>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</code>
Eliminare una regola	<code>security multi-admin-verify rule delete -operation "protected_operation"</code>
Mostra regole	<code>security multi-admin-verify rule show</code>

Per informazioni dettagliate sulla sintassi dei comandi, vedere `security multi-admin-verify rule` pagine man.

Richiedere l'esecuzione di operazioni protette

Quando si avvia un'operazione o un comando protetto su un cluster abilitato per la verifica multi-admin (MAV), ONTAP intercetta automaticamente l'operazione e chiede di generare una richiesta, che deve essere approvata da uno o più amministratori in un gruppo di approvazione MAV (amministratori MAV). In alternativa, è possibile creare una richiesta MAV senza la finestra di dialogo.

Se approvata, è necessario rispondere alla richiesta per completare l'operazione entro il periodo di scadenza della richiesta. In caso di veto o di superamento dei termini di richiesta o scadenza, è necessario eliminare la richiesta e reinviarla.

La funzionalità MAV rispetta le impostazioni RBAC esistenti. In altri termini, il ruolo di amministratore deve disporre di privilegi sufficienti per eseguire un'operazione protetta, indipendentemente dalle impostazioni MAV. ["Scopri di più su RBAC"](#).

Se sei un amministratore MAV, le tue richieste di eseguire operazioni protette devono essere approvate anche da un amministratore MAV.

Procedura di System Manager

Quando un utente fa clic su una voce di menu per avviare un'operazione e l'operazione è protetta, viene generata una richiesta di approvazione e l'utente riceve una notifica simile a quanto segue:

```
Approval request to delete the volume was sent.  
Track the request ID 356 from Events & Jobs > Multi-Admin Requests.
```

La finestra **Richieste multi-amministratore** è disponibile quando MAV è attivato, mostrando le richieste in sospeso in base all'ID di accesso dell'utente e al ruolo MAV (approvatore o meno). Per ogni richiesta in sospeso, vengono visualizzati i seguenti campi:

- Operazione
- Indice (numero)
- Stato (in sospeso, approvato, rifiutato, eseguito o scaduto)

Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

- Query (qualsiasi parametro o valore per l'operazione richiesta)
- Utente richiedente
- La richiesta scade il
- (Numero di) approvatori in sospeso
- (Numero di) potenziali responsabili dell'approvazione

Una volta approvata la richiesta, l'utente richiedente può riprovare l'operazione entro il periodo di scadenza.

Se l'utente tenta di eseguire nuovamente l'operazione senza approvazione, viene visualizzata una notifica simile alla seguente:

```
Request to perform delete operation is pending approval.  
Retry the operation after request is approved.
```

Procedura CLI

1. Inserire l'operazione protetta direttamente o utilizzando il comando di richiesta MAV.

Esempi – per eliminare un volume, immettere uno dei seguenti comandi:

```
° volume delete
```



```
cluster-1::*> volume delete -volume voll -vserver vs0
```

```
Warning: This operation requires multi-admin verification. To create  
a
```

```
    verification request use "security multi-admin-verify  
request  
    create".
```

```
    Would you like to create a request for this operation?  
    {y|n}: y
```

```
Error: command failed: The security multi-admin-verify request (index  
3) is  
    auto-generated and requires approval.
```

```
° security multi-admin-verify request create "volume delete"
```

```
Error: command failed: The security multi-admin-verify request (index  
3)  
    requires approval.
```

2. Controllare lo stato della richiesta e rispondere all'avviso MAV.

a. Se la richiesta viene approvata, rispondere al messaggio CLI per completare l'operazione.

Esempio:

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: approved
Required Approvers: 1
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

Info: Volume "voll1" in Vserver "vs0" will be marked as deleted and placed in the volume recovery queue. The space used by the volume will be recovered only after the retention period of 12 hours has completed. To recover the space immediately, get the volume name using (privilege:advanced) "volume recovery-queue show voll_*" and then "volume recovery-queue purge -vserver vs0 -volume <volume_name>" command. To recover the volume use the (privilege:advanced) "volume recovery-queue recover -vserver vs0 -volume <volume_name>" command.

Warning: Are you sure you want to delete volume "voll1" in Vserver "vs0" ?
{y|n}: y

- b. Se la richiesta è stata vetoata o il periodo di scadenza è scaduto, eliminarla e reinviarla o contattare l'amministratore MAV.

Esempio:

```
cluster-1::> security multi-admin-verify request show 3
```

```
Request Index: 3
  Operation: volume delete
    Query: -vserver vs0 -volume voll1
    State: vetoed
Required Approvers: 1
Pending Approvers: 1
  Approval Expiry: 2/25/2022 14:38:47
  Execution Expiry: -
    Approvals: -
    User Vetoed: admin2
    Vserver: cluster-1
User Requested: admin
  Time Created: 2/25/2022 13:38:47
  Time Approved: -
    Comment: -
Users Permitted: -
```

```
cluster-1::*> volume delete -volume voll1 -vserver vs0
```

```
Error: command failed: The security multi-admin-verify request (index 3)
hasbeen vetoed. You must delete it and create a new verification
request.
To delete, run "security multi-admin-verify request delete 3".
```

Gestire le richieste di operazioni protette

Quando gli amministratori di un gruppo di approvazione MAV (amministratori MAV) ricevono una notifica di una richiesta di esecuzione dell'operazione in sospeso, devono rispondere con un messaggio di approvazione o veto entro un periodo di tempo fisso (scadenza dell'approvazione). Se non si riceve un numero sufficiente di approvazioni, il richiedente deve eliminare la richiesta ed effettuare un'altra.

A proposito di questa attività

Le richieste di approvazione sono identificate con numeri di indice, inclusi nei messaggi e-mail e nelle visualizzazioni della coda di richiesta.

È possibile visualizzare le seguenti informazioni dalla coda di richiesta:

Operazione

Operazione protetta per la quale viene creata la richiesta.

Query

Oggetto (o oggetti) su cui l'utente desidera applicare l'operazione.

Stato

Lo stato corrente della richiesta: In sospeso, approvato, rifiutato, scaduto, eseguito. Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

Responsabili dell'approvazione richiesti

Il numero di amministratori MAV necessari per approvare la richiesta. Un utente può impostare il parametro `required-approvers` per la regola dell'operazione. Se un utente non imposta i responsabili dell'approvazione richiesti sulla regola, vengono applicati i responsabili dell'approvazione richiesti dall'impostazione globale.

Responsabili dell'approvazione in sospeso

Il numero di amministratori MAV che sono ancora necessari per approvare la richiesta per essere contrassegnati come approvati.

Scadenza approvazione

Periodo entro il quale un amministratore MAV deve rispondere a una richiesta di approvazione. Qualsiasi utente autorizzato può impostare la scadenza dell'approvazione per una regola dell'operazione. Se la regola non è impostata su approvazione-scadenza, viene applicata l'approvazione-scadenza dall'impostazione globale.

Scadenza dell'esecuzione

Il periodo entro il quale l'amministratore richiedente deve completare l'operazione. Qualsiasi utente autorizzato può impostare la scadenza dell'esecuzione per una regola dell'operazione. Se la regola non è impostata su `execution-expiry`, viene applicata l'impostazione di `execution-expiry` dall'impostazione globale.

Approvati dagli utenti

Gli amministratori MAV che hanno approvato la richiesta.

Veto dell'utente

Gli amministratori MAV che hanno posto il veto alla richiesta.

Storage VM (vserver)

SVM a cui è associata la richiesta. Solo la SVM amministrativa è supportata in questa release.

Richiesto dall'utente

Il nome utente dell'utente che ha creato la richiesta.

Ora di creazione

L'ora in cui viene creata la richiesta.

Tempo approvato

L'ora in cui lo stato della richiesta è cambiato in approvato.

Commento

Eventuali commenti associati alla richiesta.

Utenti consentiti

L'elenco degli utenti autorizzati a eseguire l'operazione protetta per cui la richiesta è approvata. Se `users-permitted` è vuoto, quindi qualsiasi utente con autorizzazioni appropriate può eseguire l'operazione.

Tutte le richieste scadute o eseguite vengono eliminate quando viene raggiunto un limite di 1000 richieste o quando il tempo di scadenza è superiore a 8 ore per le richieste scadute. Le richieste vetoed vengono

eliminate una volta contrassegnate come scadute.

Procedura di System Manager

Gli amministratori MAV ricevono messaggi e-mail con i dettagli della richiesta di approvazione, il periodo di scadenza della richiesta e un link per approvare o rifiutare la richiesta. È possibile accedere a una finestra di dialogo di approvazione facendo clic sul collegamento nell'e-mail o accedendo a **Eventi e lavori > Richieste** in System Manager.

La finestra **Requests** (Richieste) è disponibile quando è attivata la verifica multi-admin, mostrando le richieste in sospeso in base all'ID di accesso dell'utente e al ruolo MAV (approvatore o meno).

- Operazione
- Indice (numero)
- Stato (in sospeso, approvato, rifiutato, eseguito o scaduto)

Se una richiesta viene respinta da un responsabile dell'approvazione, non sono possibili ulteriori azioni.

- Query (qualsiasi parametro o valore per l'operazione richiesta)
- Utente richiedente
- La richiesta scade il
- (Numero di) approvatori in sospeso
- (Numero di) potenziali responsabili dell'approvazione

Gli amministratori MAV dispongono di controlli aggiuntivi in questa finestra; possono approvare, rifiutare o eliminare singole operazioni o gruppi di operazioni selezionati. Tuttavia, se l'amministratore MAV è l'utente richiedente, non può approvare, rifiutare o eliminare le proprie richieste.

Procedura CLI

1. Quando viene inviata una notifica via email delle richieste in sospeso, annotare il numero di indice della richiesta e il periodo di scadenza dell'approvazione. Il numero dell'indice può essere visualizzato anche utilizzando le opzioni **show** o **show-pending** indicate di seguito.
2. Approvare o veto la richiesta.

Se si desidera...	Immettere questo comando
Approvare una richiesta	<code>security multi-admin-verify request approve nn</code>
Veto di una richiesta	<code>security multi-admin-verify request veto nn</code>
Mostra tutte le richieste, le richieste in sospeso o una singola richiesta	<code>`security multi-admin-verify request { show</code>

Se si desidera...	Immettere questo comando
show-pending } [nn] { -fields <i>field1</i> [, <i>field2</i> ...]	[-instance] }` È possibile visualizzare tutte le richieste nella coda o solo quelle in sospeso. Se si inserisce il numero di indice, vengono visualizzate solo le informazioni relative a tale valore. È possibile visualizzare informazioni su campi specifici utilizzando -fields o su tutti i campi (utilizzando il -instance parametro).
Eliminare una richiesta	security multi-admin-verify request delete nn

Esempio:

La seguente sequenza approva una richiesta dopo che l'amministratore MAV ha ricevuto l'email di richiesta con il numero di indice 3, che ha già un'approvazione.

```

cluster1::> security multi-admin-verify request show-pending
                                Pending
Index Operation      Query State  Approvers Requestor
-----
   3 volume delete  -    pending 1      julia

cluster-1::> security multi-admin-verify request approve 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: approved
Required Approvers: 2
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
Execution Expiry: 2/25/2022 14:35:36
    Approvals: mav-admin2
    User Vetoed: -
      Vserver: cluster-1
User Requested: julia
  Time Created: 2/25/2022 13:32:03
Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -

```

Esempio:

La seguente sequenza veto una richiesta dopo che l'amministratore MAV ha ricevuto l'email di richiesta con il numero di indice 3, che ha già un'approvazione.

```
cluster1::> security multi-admin-verify request show-pending
                                     Pending
Index Operation      Query State  Approvers Requestor
-----
3 volume delete    -    pending 1      pavan

cluster-1::> security multi-admin-verify request veto 3

cluster-1::> security multi-admin-verify request show 3

Request Index: 3
  Operation: volume delete
    Query: -
    State: vetoed
Required Approvers: 2
Pending Approvers: 0
  Approval Expiry: 2/25/2022 14:32:03
  Execution Expiry: 2/25/2022 14:35:36
    Approvals: mav-admin1
    User Vetoed: mav-admin2
    Vserver: cluster-1
User Requested: pavan
  Time Created: 2/25/2022 13:32:03
  Time Approved: 2/25/2022 13:35:36
    Comment: -
Users Permitted: -
```

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.