



Autenticazione e controllo dell'accesso

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/it-it/ontap/concept_authentication_access_control_overview.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommario

- Autenticazione e controllo dell'accesso 1
 - Panoramica dell'autenticazione e del controllo degli accessi 1
 - Gestire l'autenticazione dell'amministratore e RBAC. 1
 - Autenticazione e autorizzazione utilizzando OAuth 2,0 84
 - Configurare l'autenticazione SAML 106
 - Gestire i servizi Web. 113
 - Verificare l'identità dei server remoti utilizzando i certificati 123
 - Autenticare reciprocamente il cluster e un server KMIP 126

Autenticazione e controllo dell'accesso

Panoramica dell'autenticazione e del controllo degli accessi

Puoi gestire l'autenticazione del cluster ONTAP e il controllo dell'accesso ai servizi web ONTAP.

Con System Manager o la CLI puoi controllare e proteggere l'accesso client e amministratore al cluster e allo storage.

Se si utilizza la gestione di sistema classica (disponibile solo in ONTAP 9.7 e versioni precedenti), fare riferimento a. ["System Manager Classic \(ONTAP da 9.0 a 9.7\)"](#)

Autenticazione e autorizzazione del client

ONTAP autentica un computer client e un utente verificando la propria identità con un'origine attendibile.

ONTAP autorizza un utente ad accedere a un file o a una directory confrontando le credenziali dell'utente con le autorizzazioni configurate nel file o nella directory.

Autenticazione amministratore e RBAC

Gli amministratori utilizzano account di accesso locali o remoti per autenticarsi sulla VM del cluster e dello storage. RBAC (Role-Based Access Control) determina i comandi a cui un amministratore ha accesso.

Gestire l'autenticazione dell'amministratore e RBAC

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

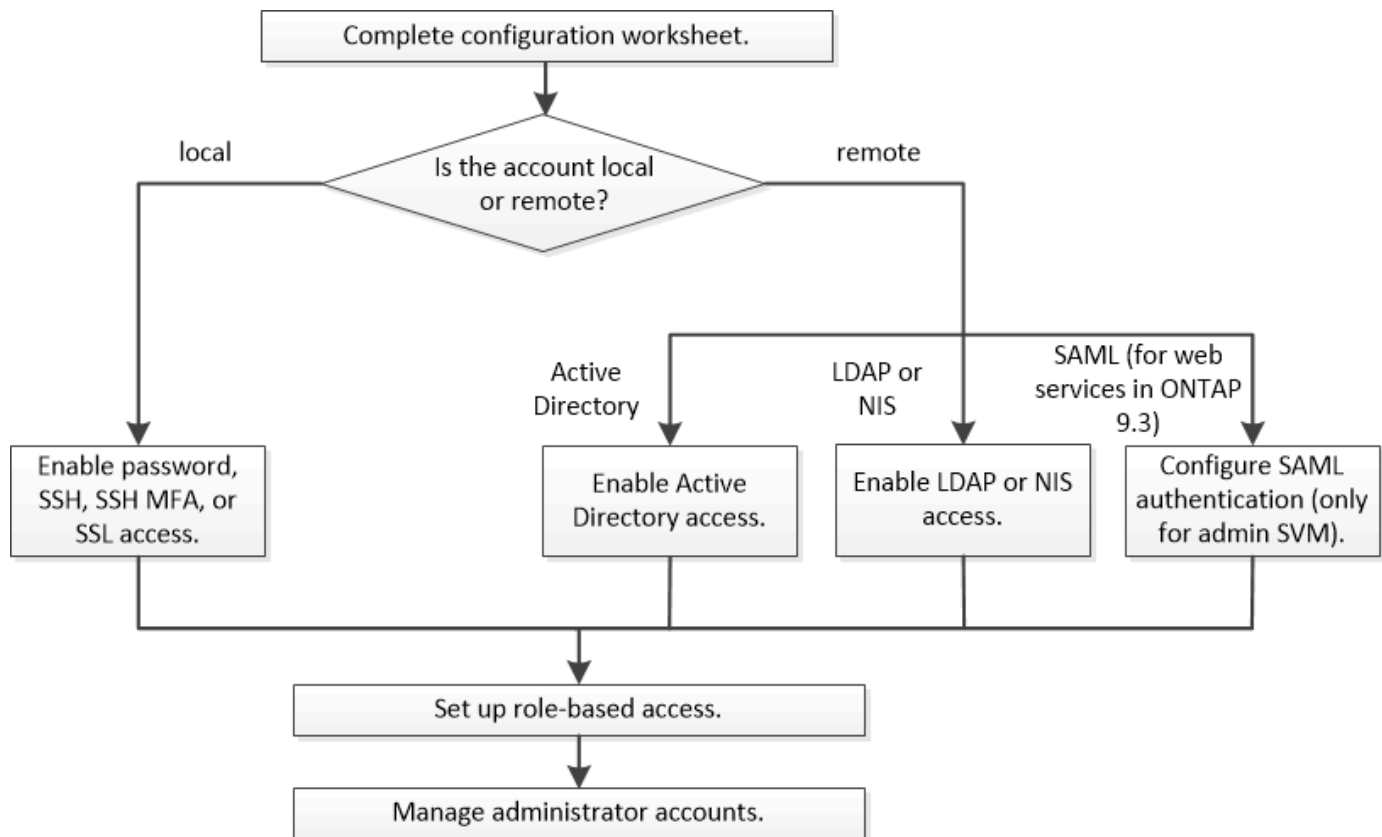
È possibile abilitare gli account di accesso per gli amministratori del cluster ONTAP e per gli amministratori delle macchine virtuali di storage (SVM). È inoltre possibile utilizzare RBAC (role-based access control) per definire le funzionalità degli amministratori.

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.	
<code>-user-or-group-name</code>	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.	
<code>-application</code>	Applicazione utilizzata per accedere alla VM di storage: <ul style="list-style-type: none">• <code>http</code>• <code>ontapi</code>• <code>snmp</code>• <code>ssh</code>	

-authmethod	<p>Il metodo utilizzato per autenticare l'account:</p> <ul style="list-style-type: none"> • <code>cert</code> Per l'autenticazione del certificato SSL • <code>domain</code> Per l'autenticazione di Active Directory • <code>nsswitch</code> Per l'autenticazione LDAP o NIS • <code>password</code> per l'autenticazione della password dell'utente • <code>publickey</code> per l'autenticazione a chiave pubblica • <code>community</code> Per le stringhe di comunità SNMP • <code>usm</code> Per il modello di sicurezza dell'utente SNMP • <code>saml</code> Per l'autenticazione SAML (Security Assertion Markup Language) 	
-remote-switch-ipaddress	<p>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>.</p>	
-role	<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>. 	
-comment	<p>(Facoltativo) testo descrittivo per l'account. Racchiudere il testo tra virgolette doppie (").</p>	

-is-ns-switch-group	Se l'account è un account di gruppo LDAP o NIS (yes oppure no).	
-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
-------	-------------	---------------

<code>-vserver</code>	La VM di storage (denominata vserver nell'interfaccia CLI di ONTAP) a cui si applicano le impostazioni di autenticazione Duo.	
<code>-integration-key</code>	La chiave di integrazione, ottenuta durante la registrazione dell'applicazione SSH con Duo.	
<code>-secret-key</code>	La chiave segreta, ottenuta durante la registrazione dell'applicazione SSH con Duo.	
<code>-api-host</code>	<p>Il nome host API, ottenuto durante la registrazione dell'applicazione SSH con Duo. Ad esempio:</p> <pre>api- <HOSTNAME>.duosecurity.com</pre>	
<code>-fail-mode</code>	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.	
<code>-http-proxy</code>	<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>	

-enabled	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
-vserver	(Opzionale) il nome della VM di storage (chiamato vserver nella CLI di ONTAP) associata al ruolo.	
-role	Il nome del ruolo.	
-cmddirname	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 (").	

-x509-certificate	<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
-common-name	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.	

<code>-type</code>	<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
<code>-vserver</code>	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
<code>-vserver</code>	Il nome della VM di storage per cui si desidera creare un account di computer Active Directory.	
<code>-account-name</code>	Il nome NetBIOS dell'account del computer.	
<code>-domain</code>	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 aggiungere 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)

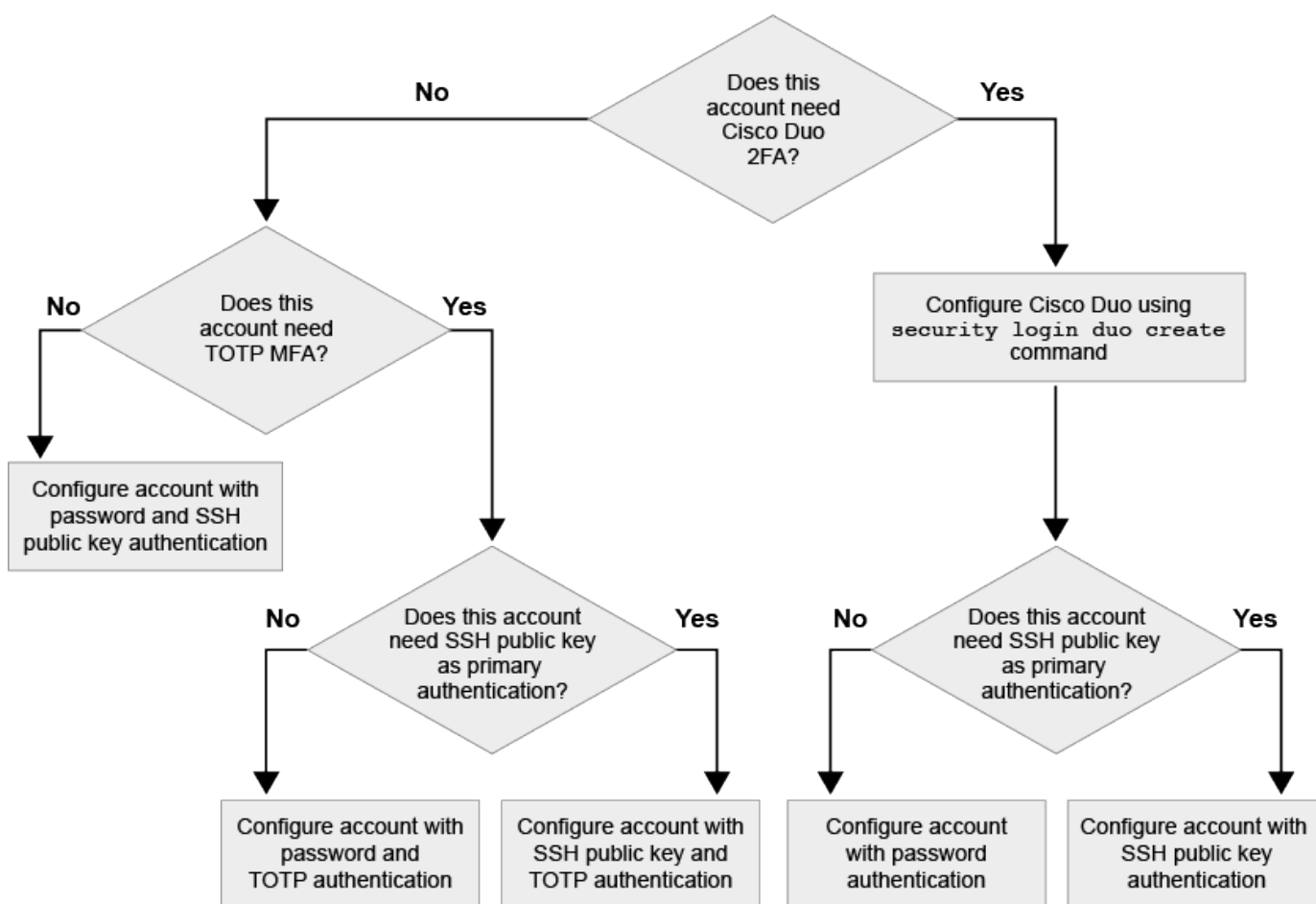
Panoramica dell'autenticazione a più fattori

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>

Versione di ONTAP	Autenticazione primaria	Autenticazione secondaria	Comando
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>
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 `quest2` con il predefinito backup Ruolo di accesso alla SVM amministrativa `engCluster`.

```
cluster1::>security login create -vserver engCluster -user-or-group-name
quest2 -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) • security login rest-role • security login role
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 "server1.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
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBChUAA0EA6EagLfso5+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
AMQ8wDQYJKoZIhvcNAQkBFgAwXDANBgkqhkiG9w0BAQEFAANLADBIAAkEAYXrK2sry
-----END CERTIFICATE-----
```

```
Please enter Private Key: Press <Enter> when done
-----BEGIN RSA PRIVATE KEY-----
MIIBPAIBAAJBAMl6ytrK8nQj82UsWeHOeT8gk0BPX+Y5MLyCsUdXA7hXhumHNpvF
C6lX2G32Sx8VEalth94tx+vOEzq+UaqHlt0CAwEAAQJBAMZjDWlgmlm3qIr/n8VT
PFnnZnbVcXVM70tbUsgPKw+QCCh9dF1jmuQKeDr+wUMWkn1DeGrfhILpzfJGHRlJ
z7UCIQDr8d3gOG7lUyX+BbFmo/N0uAKjS2cvUU+Y8a8pDxGLLwIhANqa99SuS18U
DiPvdaKTj6+EcGuXfCXz+G0rfgTZK8uzAiEArlmnrfYC8KwE9k7A0ylRzBLdUwK9
AvuJDn+/z+H1Bd0CIQDD93P/xpaJETNz53Au49VE5Jba/Jugckrbosd/lSd7nQIg
aEMAzt6qHHT4mndi8Bo8sDGedG2SKx6Qbn2IpuNZ7rc=
-----END RSA PRIVATE KEY-----
```

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

```
Please enter Intermediate Certificate: Press <Enter> when done
-----BEGIN CERTIFICATE-----
MIIE+zCCBGSGAwIBAgICAQ0wDQYJKoZIhvcNAQEFBQAwwgbsxJDAiBgNVBAcTG1Zh
bGlDZXJ0IFZhbGlkYXRpb24gTmV0d29yazEXMBUGA1UEChMOVmFsaUNlcnQsIElu
Yy4xNTAzBgNVBAsTTFZhbGlDZXJ0IENsYXNzIDIGUG9saWN5IFZhbGlkYXRpb24g
QXV0aG9yaXR5MSEwHwYDVQQDEwExd3d3LnZhbGljZXJ0LmNvbS8xIDAe
BgkqhkiG9w0BCQEWEluZm9AdmFsaWNlcnQuY29tMB4XDTA0MDYyOTE3MDYyMFoX
DTI0MDYyOTE3MDYyMFowYzELMAkGA1UEBhMCVVMxITAfBgNVBAoTGFROZSBHbyBE
YWRkeSBHcm91cCwgSW5jLjExMC8GA1UECzMOR28gRGFkZkhkgQ2xhc3MgMiBDZXJ0
-----END CERTIFICATE-----
```

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

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

```
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 .
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 .
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 group1[,group2...] [- required-approvers nn] -enabled true [-execution-expiry [nnh][nm][nns]] [-approval-expiry [nnh][nm][nns]]</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 group1 [,group2...]] [-required-approvers nn] [-execution-expiry [nnh][nm][nns]] [-approval-expiry [nnh][nm][nns]]</pre>
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>

Se si desidera...	Immettere questo comando
Disattivare la funzionalità MAV (richiede l'approvazione MAV)	<code>security multi-admin-verify modify -enabled false</code>

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.

<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>

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	<pre>security multi-admin-verify rule create -operation "protected_operation" [- query operation_subset] [parameters]</pre>
Modificare le credenziali degli amministratori correnti	<pre>security login modify <parameters></pre> <p>Esempio: La seguente regola richiede l'approvazione per eliminare il volume root.</p> <pre>security multi-admin-verify rule create -operation "volume delete" -query "- vserver vs0"</pre>
Modificare una regola	<pre>security multi-admin-verify rule modify -operation "protected_operation" [parameters]</pre>

Se si desidera...	Immettere questo comando
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 sospenso
- (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 voll1_" 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 field1[,field2...]	[-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: -
```

Autenticazione e autorizzazione utilizzando OAuth 2,0

Panoramica dell'implementazione di ONTAP OAuth 2,0

A partire da ONTAP 9,14, puoi controllare l'accesso ai tuoi cluster ONTAP utilizzando il framework Open Authorization (OAuth 2,0). Puoi configurare questa funzionalità utilizzando qualsiasi interfaccia amministrativa di ONTAP, inclusi l'interfaccia a riga di comando di ONTAP, System Manager e l'API REST. Tuttavia, le decisioni relative all'autorizzazione e al controllo dell'accesso OAuth 2,0 possono essere applicate solo quando un client accede a ONTAP utilizzando l'API REST.



Il supporto di OAuth 2,0 è stato introdotto per la prima volta con ONTAP 9.14.0, pertanto la sua disponibilità dipende dalla versione di ONTAP in uso. Vedere ["Note di rilascio di ONTAP"](#) per ulteriori informazioni.

Caratteristiche e vantaggi

Di seguito sono descritte le principali caratteristiche e i vantaggi dell'utilizzo di OAuth 2,0 con ONTAP.

Supporto per lo standard OAuth 2,0

OAuth 2,0 è il quadro di autorizzazione standard del settore. Viene utilizzato per limitare e controllare l'accesso alle risorse protette utilizzando token di accesso firmati. L'utilizzo di OAuth 2,0 offre diversi vantaggi:

- Molte opzioni per la configurazione dell'autorizzazione
- Non rivelare mai le credenziali del client, incluse le password
- I token possono essere impostati in modo che scadano in base alla configurazione
- Ideale per l'uso con API REST

Testato con diversi server di autorizzazione più diffusi

L'implementazione di ONTAP è progettata per essere compatibile con qualsiasi server di autorizzazione conforme a OAuth 2,0. È stato testato con i seguenti server o servizi comuni, tra cui:

- Auth0
- Active Directory Federation Service (ADFS)
- Keycloak

Supporto per più server di autorizzazione simultanei

È possibile definire fino a otto server di autorizzazione per un singolo cluster ONTAP. Ciò offre la flessibilità necessaria per soddisfare le esigenze dei diversi ambienti di sicurezza.

Integrazione con i ruoli REST

Le decisioni di autorizzazione ONTAP si basano in ultima analisi sui ruoli REST assegnati a utenti o gruppi. Questi ruoli vengono riportati nel token di accesso come ambiti indipendenti o in base alle definizioni ONTAP locali insieme ai gruppi Active Directory o LDAP.

Opzione per utilizzare token di accesso con restrizioni del mittente

È possibile configurare ONTAP e i server di autorizzazione per utilizzare Mutual Transport Layer Security (mTLS) che rafforza l'autenticazione client. Garantisce che i token di accesso OAuth 2,0 siano utilizzati solo dai client ai quali sono stati originariamente rilasciati. Questa funzionalità supporta e si allinea con diverse raccomandazioni di protezione note, incluse quelle stabilite da FAPI e MITER.

Implementazione e configurazione

A un livello elevato, ci sono diversi aspetti di un'implementazione e configurazione di OAuth 2,0 che è necessario considerare quando si inizia.

OAuth 2,0 entità all'interno di ONTAP

Il framework di autorizzazione OAuth 2,0 definisce diverse entità che possono essere mappate ad elementi reali o virtuali all'interno del data center o della rete. Le entità OAuth 2,0 e il loro adattamento a ONTAP sono presentati nella tabella seguente.

Entità OAuth 2,0	Descrizione
Risorsa	Gli endpoint delle API REST che forniscono accesso alle risorse ONTAP tramite comandi ONTAP interni.
Proprietario della risorsa	L'utente del cluster ONTAP che ha creato la risorsa protetta o la possiede per impostazione predefinita.
Server delle risorse	L'host per le risorse protette, ovvero il cluster ONTAP.
Client	Un'applicazione che richiede l'accesso a un endpoint API REST per conto o con l'autorizzazione del proprietario della risorsa.
Server di autorizzazione	In genere, un server dedicato responsabile dell'emissione dei token di accesso e dell'applicazione dei criteri amministrativi.

Configurazione core ONTAP

È necessario configurare il cluster ONTAP per abilitare e utilizzare OAuth 2,0. Ciò include la creazione di una connessione al server di autorizzazione e la definizione della configurazione di autorizzazione ONTAP richiesta. È possibile eseguire questa configurazione utilizzando una qualsiasi delle interfacce amministrative, tra cui:

- Interfaccia a riga di comando di ONTAP
- System Manager
- API REST di ONTAP

Ambiente e servizi di supporto

Oltre alle definizioni di ONTAP, è necessario configurare anche i server di autorizzazione. Se si utilizza la mappatura da gruppo a ruolo, è necessario configurare anche i gruppi Active Directory o l'equivalente LDAP.

Client ONTAP supportati

A partire da ONTAP 9,14, un client API REST può accedere a ONTAP utilizzando OAuth 2,0. Prima di eseguire una chiamata API REST, è necessario ottenere un token di accesso dal server di autorizzazione. Il client passa quindi questo token al cluster ONTAP come *bearer token* utilizzando l'intestazione della richiesta di autorizzazione HTTP. A seconda del livello di protezione necessario, è anche possibile creare e installare un certificato nel client per utilizzare token con vincoli di mittente basati su mTLS.

Terminologia selezionata

Quando si inizia a esaminare la distribuzione di OAuth 2,0 con ONTAP, è utile acquisire familiarità con alcune parti della terminologia. Vedere ["Risorse aggiuntive"](#) Per collegamenti a ulteriori informazioni su OAuth 2,0.

Token di accesso

Token emesso da un server di autorizzazione e utilizzato da un'applicazione client OAuth 2,0 per effettuare richieste di accesso alle risorse protette.

Token Web JSON

Lo standard utilizzato per formattare i token di accesso. JSON viene utilizzato per rappresentare le rivendicazioni OAuth 2,0 in formato compatto con le rivendicazioni disposte in tre sezioni principali.

Token di accesso vincolato dal mittente

Funzione opzionale basata sul protocollo mTLS (Mutual Transport Layer Security). Utilizzando un'ulteriore richiesta di conferma nel token, questo garantisce che il token di accesso venga utilizzato solo dal client al quale è stato originariamente emesso.

Set di chiavi Web JSON

Un JWKS è un insieme di chiavi pubbliche utilizzate da ONTAP per verificare i token JWT presentati dai clienti. I set di chiavi sono generalmente disponibili sul server di autorizzazione tramite un URI dedicato.

Scopo

Gli ambiti forniscono un modo per limitare o controllare l'accesso di un'applicazione alle risorse protette come l'API REST ONTAP. Sono rappresentate come stringhe nel token di accesso.

Ruolo REST di ONTAP

I ruoli REST sono stati introdotti con ONTAP 9,6 e costituiscono una parte fondamentale del framework RBAC di ONTAP. Questi ruoli sono diversi dai ruoli tradizionali precedenti che sono ancora supportati da ONTAP. L'implementazione di OAuth 2,0 in ONTAP supporta solo i ruoli REST.

Intestazione autorizzazione HTTP

Intestazione inclusa nella richiesta HTTP per identificare il client e le autorizzazioni associate come parte di una chiamata API REST. Sono disponibili diverse varianti o implementazioni a seconda della modalità di autenticazione e autorizzazione. Quando si presenta un token di accesso OAuth 2,0 a ONTAP, il token viene identificato come *token bearer*.

Autenticazione di base HTTP

Una tecnica di autenticazione HTTP avanzata ancora supportata da ONTAP. Le credenziali in testo normale (nome utente e password) sono concatenate con due punti e codificate in base64. La stringa viene inserita nell'intestazione della richiesta di autorizzazione e inviata al server.

FAPI

Un gruppo di lavoro della OpenID Foundation che fornisce protocolli, schemi di dati e raccomandazioni sulla sicurezza per il settore finanziario. L'API era originariamente nota come API di livello finanziario.

MITRA

Un'azienda privata senza scopo di lucro che fornisce una guida tecnica e di sicurezza all'aeronautica militare degli Stati Uniti e al governo degli Stati Uniti.

Risorse aggiuntive

Di seguito sono riportate diverse risorse aggiuntive. Dovreste rivedere questi luoghi per ottenere più informazioni su OAuth 2,0 e sugli standard relativi.

Protocolli e standard

- ["RFC 6749: Framework di autorizzazione OAuth 2,0"](#)
- ["RFC 7519: Token Web JSON \(JWT\)"](#)
- ["RFC 7523: Profilo JSON Web Token \(JWT\) per l'autenticazione client OAuth 2,0 e le concessioni di autorizzazione"](#)
- ["RFC 7662: Introspezione token OAuth 2,0"](#)
- ["RFC 7800: Chiave di prova del possesso per JWT"](#)
- ["RFC 8705: Autenticazione client OAuth 2,0 Mutual-TLS e token di accesso con associazione a certificati"](#)

Governativi

- ["Fondazione OpenID"](#)
- ["Gruppo di lavoro FAPI"](#)

- ["MITRA"](#)
- ["IANA - JWT"](#)

Prodotti e servizi

- ["Auth0"](#)
- ["Panoramica di ADFS"](#)
- ["Keycloak"](#)

Strumenti e utilità aggiuntivi

- ["JWT entro il Auth0"](#)
- ["OpenSSL"](#)

Documentazione e risorse di NetApp

- ["Automazione ONTAP"](#) documentazione

Concetti

Server di autorizzazione e token di accesso

I server di autorizzazione svolgono diverse funzioni importanti come componente centrale all'interno del framework OAuth 2,0 Authorization.

Server di autorizzazione OAuth 2,0

I server di autorizzazione sono principalmente responsabili della creazione e della firma dei token di accesso. Questi token contengono informazioni di identità e autorizzazione che consentono a un'applicazione client di accedere in modo selettivo alle risorse protette. I server sono generalmente isolati l'uno dall'altro e possono essere implementati in diversi modi, incluso come server dedicato standalone o come parte di un prodotto di gestione delle identità e degli accessi più ampio.



A volte è possibile utilizzare una terminologia diversa per un server di autorizzazione, specialmente quando la funzionalità OAuth 2,0 è inclusa in un prodotto o una soluzione di gestione delle identità e degli accessi più ampia. Ad esempio, il termine **provider di identità (IdP)** viene spesso utilizzato in modo intercambiabile con **server di autorizzazione**.

Amministrazione

Oltre all'emissione di token di accesso, i server di autorizzazione forniscono anche servizi amministrativi correlati, in genere tramite un'interfaccia utente Web. Ad esempio, è possibile definire e amministrare:

- Autenticazione degli utenti e degli utenti
- Ambiti
- Segregazione amministrativa attraverso locatari e regni
- Applicazione delle policy
- Collegamento a vari servizi esterni
- Supporto per altri protocolli di identità (come SAML)

ONTAP è compatibile con i server di autorizzazione conformi allo standard OAuth 2,0.

Definizione di ONTAP

È necessario definire uno o più server di autorizzazione in ONTAP. ONTAP comunica in modo sicuro con ciascun server per verificare i token ed eseguire altre attività correlate a supporto delle applicazioni client.

Di seguito sono illustrati gli aspetti principali della configurazione di ONTAP. Vedere anche ["Scenari di distribuzione di OAuth 2,0"](#) per ulteriori informazioni.

Come e dove vengono convalidati i token di accesso

Sono disponibili due opzioni per la convalida dei token di accesso.

- Convalida locale

ONTAP può convalidare i token di accesso localmente in base alle informazioni fornite dal server di autorizzazione che ha emesso il token. Le informazioni recuperate dal server di autorizzazione vengono memorizzate nella cache da ONTAP e aggiornate a intervalli regolari.

- Introspezione remota

È inoltre possibile utilizzare l'introspezione remota per convalidare i token nel server di autorizzazione. Introspezione è un protocollo che consente alle parti autorizzate di interrogare un server di autorizzazione su un token di accesso. Fornisce a ONTAP un modo per estrarre determinati metadati da un token di accesso e convalidare il token. ONTAP memorizza nella cache alcuni dati per motivi di prestazioni.

Posizione di rete

ONTAP potrebbe essere protetto da un firewall. In questo caso, è necessario identificare un proxy come parte della configurazione.

Come vengono definiti i server di autorizzazione

Puoi definire un server di autorizzazione per ONTAP utilizzando qualsiasi interfaccia amministrativa, inclusa CLI, System Manager o API REST. Ad esempio, con l'interfaccia CLI si utilizza il comando `security oauth2 client create`.

Numero di server di autorizzazione

È possibile definire fino a otto server di autorizzazione per un singolo cluster ONTAP. Lo stesso server di autorizzazione può essere definito più di una volta nello stesso cluster ONTAP, purché le attestazioni dell'emittente o dell'emittente/pubblico siano univoche. Per esempio, con Keycloak questo sarà sempre il caso quando si usano reami diversi.

Utilizzo dei token di accesso OAuth 2,0

I token di accesso OAuth 2,0 emessi dai server di autorizzazione vengono verificati da ONTAP e utilizzati per prendere decisioni di accesso basate sui ruoli per le richieste dei client API REST.

Acquisizione di un token di accesso

È necessario acquisire un token di accesso da un server di autorizzazione definito nel cluster ONTAP in cui si utilizza l'API REST. Per acquisire un token, è necessario contattare direttamente il server di autorizzazione.



ONTAP non rilascia token di accesso o reindirizza le richieste dai client ai server di autorizzazione.

Il modo in cui si richiede un token dipende da diversi fattori, tra cui:

- Server di autorizzazione e relative opzioni di configurazione
- Tipo di concessione OAuth 2,0
- Client o strumento software utilizzato per emettere la richiesta

Tipi di sovvenzione

Un *grant* è un processo ben definito, che include un insieme di flussi di rete, utilizzato per richiedere e ricevere un token di accesso OAuth 2,0. A seconda dei requisiti del client, dell'ambiente e della protezione, è possibile utilizzare diversi tipi di concessione. Un elenco dei tipi di sovvenzione più comuni è presentato nella tabella seguente.

Tipo di concessione	Descrizione
Credenziali client	Tipo di concessione comune basato sull'utilizzo di credenziali (come ID e segreto condiviso). Si presuppone che il client abbia una stretta relazione di trust con il proprietario della risorsa.
Password	È possibile utilizzare il tipo di concessione delle credenziali della password del proprietario della risorsa nei casi in cui il proprietario della risorsa abbia una relazione di trust stabilita con il client. Può essere utile anche per la migrazione di client HTTP legacy a OAuth 2,0.
Codice di autorizzazione	Si tratta di un tipo di sovvenzione ideale per i client riservati e si basa su un flusso basato sul reindirizzamento. Può essere utilizzato per ottenere sia un token di accesso che un token di aggiornamento.

Contenuti JWT

Un token di accesso OAuth 2,0 è formattato come JWT. Il contenuto viene creato dal server di autorizzazione in base alla configurazione. Tuttavia, i token sono opachi per le applicazioni client. Un cliente non ha motivo di ispezionare un token o di essere a conoscenza del contenuto.

Ogni token di accesso JWT contiene una serie di attestazioni. Le attestazioni descrivono le caratteristiche dell'emittente e l'autorizzazione basata sulle definizioni amministrative del server di autorizzazione. Alcuni dei reclami registrati con la norma sono descritti nella tabella seguente. Tutte le stringhe rilevano la distinzione tra maiuscole e minuscole.

Reclamo	Parola chiave	Descrizione
Emittente	iss	Identifica l'entità che ha emesso il token. L'elaborazione della richiesta di rimborso è specifica per l'applicazione.
Soggetto	sub	L'oggetto o l'utente del token. Il nome è considerato univoco a livello globale o locale.
Pubblico	aud	I destinatari a cui è destinato il token. Implementato come array di stringhe.
Scadenza	scad	Il tempo dopo il quale il token scade e deve essere rifiutato.

Vedere ["RFC 7519: Token Web JSON"](#) per ulteriori informazioni.

Opzioni per l'autorizzazione client ONTAP

Sono disponibili diverse opzioni per personalizzare l'autorizzazione del client ONTAP. Le

decisioni di autorizzazione si basano, in ultima analisi, sui ruoli REST ONTAP contenuti o derivati dai token di accesso.



È possibile utilizzare solo **"Ruoli REST di ONTAP"** Quando si configura l'autorizzazione per OAuth 2,0. I ruoli tradizionali ONTAP precedenti non sono supportati.

Introduzione

L'implementazione di OAuth 2,0 all'interno di ONTAP è progettata per essere flessibile e robusta, fornendo le opzioni necessarie per proteggere l'ambiente ONTAP. A un livello elevato, esistono tre categorie di configurazione principali per la definizione dell'autorizzazione del client ONTAP. Queste opzioni di configurazione si escludono a vicenda.

ONTAP applica la singola opzione più appropriata in base alla configurazione scelta. Vedere ["Modalità con cui ONTAP determina l'accesso"](#) Per ulteriori informazioni su come ONTAP elabora le definizioni di configurazione per prendere decisioni sugli accessi.

Oscilloscopi indipendenti OAuth 2,0

Questi ambiti contengono uno o più ruoli REST personalizzati, ciascuno incapsulato in una singola stringa. Sono indipendenti dalle definizioni dei ruoli ONTAP. È necessario definire queste stringhe di ambito nel server di autorizzazione.

Ruoli e utenti REST locali specifici di ONTAP

In base alla configurazione, è possibile utilizzare le definizioni di identità ONTAP locali per prendere decisioni di accesso. Le opzioni includono:

- Singolo ruolo REST denominato
- Corrispondenza del nome utente con un utente ONTAP locale

La sintassi dell'ambito per un ruolo denominato è **ontap-role-`<URL-encoded-ONTAP-role-name>`**. Ad esempio, se il ruolo è "admin" la stringa dell'ambito sarà "ontap-role-admin".

Active Directory o gruppi LDAP

Se vengono esaminate le definizioni ONTAP locali ma non è possibile prendere alcuna decisione di accesso, vengono utilizzati i gruppi Active Directory ("dominio") o LDAP ("nsswitch"). Le informazioni sul gruppo possono essere specificate in due modi:

- Stringa OAuth 2,0 Scope

Supporta le applicazioni riservate utilizzando il flusso di credenziali client in cui non vi è alcun utente con appartenenza a un gruppo. L'ambito deve essere denominato **ontap-group-`<URL-encoded-ONTAP-group-name>`**. Ad esempio, se il gruppo è "sviluppo" la stringa dell'ambito sarà "ontap-group-development".

- Nella richiesta di "gruppo"

Questa funzione è destinata ai token di accesso emessi da ADFS utilizzando il flusso proprietario della risorsa (concessione password).

Oscilloscopi OAuth 2,0 autonomi

Gli scope autonomi sono stringhe trasportate nel token di accesso. Ognuno di essi costituisce una definizione completa e personalizzata del ruolo e include tutto ciò che ONTAP ha bisogno per prendere una decisione di accesso. L'ambito è separato e distinto dai ruoli REST definiti all'interno di ONTAP stesso.

Formato della stringa Scope

A livello base, l'ambito è rappresentato come una stringa contigua e composta da sei valori separati da due punti. I parametri utilizzati nella stringa Scope sono descritti di seguito.

Letterale di ONTAP

L'ambito deve iniziare con il valore letterale `ontap` in minuscolo. Questo identifica l'ambito come specifico di ONTAP.

Cluster

Definisce il cluster ONTAP a cui si applica l'ambito. I valori possono includere:

- UUID cluster

Identificazione di un singolo cluster.

- Asterisco (*)

Indica che l'ambito si applica a tutti i cluster.

È possibile utilizzare il comando CLI di ONTAP `cluster identity show` Per visualizzare l'UUID del cluster. Se non specificato, l'ambito si applica a tutti i cluster.

Ruolo

Il nome del ruolo di RIPOSO contenuto nell'ambito autonomo. Questo valore non viene esaminato da ONTAP o abbinato a ruoli REST esistenti definiti in ONTAP. Il nome viene utilizzato per la registrazione.

Livello di accesso

Questo valore indica il livello di accesso applicato all'applicazione client quando si utilizza l'endpoint API nell'ambito. Sono disponibili sei valori, come descritto nella tabella seguente.

Livello di accesso	Descrizione
nessuno	Nega tutti gli accessi all'endpoint specificato.
readonly	Consente solo l'accesso in lettura utilizzando GET.
read_create	Consente l'accesso in lettura e la creazione di nuove istanze di risorse utilizzando POST.
read_modify	Consente l'accesso in lettura e la possibilità di aggiornare le risorse esistenti utilizzando PATCH.
read_create_modify	Consente tutti gli accessi ad eccezione dell'eliminazione. Le operazioni consentite includono GET (lettura), POST (creazione) e PATCH (aggiornamento).
tutto	Consente l'accesso completo.

SVM

Nome della SVM all'interno del cluster a cui si applica l'ambito. Utilizzare il valore * (asterisco) per indicare tutte le SVM.



Questa funzione non è completamente supportata con ONTAP 9.14.1. È possibile ignorare il parametro SVM e utilizzare un asterisco come segnaposto. Esaminare ["Note di rilascio di ONTAP"](#) Per verificare il supporto SVM futuro.

URI API REST

Percorso completo o parziale di una risorsa o di una serie di risorse correlate. La stringa deve iniziare con `/api`. Se non si specifica un valore, l'ambito si applica a tutti gli endpoint API nel cluster ONTAP.

Esempi di ambito

Di seguito sono riportati alcuni esempi di ambiti auto-contenuti.

`ontap*:joes-role:read_create_modify:*/api/cluster`

Fornisce all'utente assegnato a questo ruolo l'accesso di lettura, creazione e modifica al `/cluster` endpoint.

Strumento di amministrazione CLI

Per rendere più semplice e meno incline agli errori l'amministrazione degli ambiti autonomi, ONTAP fornisce il comando CLI `security oauth2 scope` per generare stringhe di ambito in base ai parametri di input.

Il comando `security oauth2 scope` ha due casi d'utilizzo sulla base delle tue indicazioni:

- Parametri CLI per la stringa di ambito

È possibile utilizzare questa versione del comando per generare una stringa di ambito in base ai parametri di input.

- Stringa di ambito per i parametri CLI

È possibile utilizzare questa versione del comando per generare i parametri del comando in base alla stringa dell'ambito di input.

Esempio

Nell'esempio seguente viene generata una stringa di scope con l'output incluso dopo l'esempio di comando riportato di seguito. La definizione si applica a tutti i cluster.

```
security oauth2 scope cli-to-scope -role joes-role -access readonly -api
/api/cluster
```

```
ontap*:joes-role:readonly:*/api/cluster
```

Modalità con cui ONTAP determina l'accesso

Per progettare e implementare correttamente OAuth 2.0, è necessario comprendere in che modo la configurazione delle autorizzazioni viene utilizzata da ONTAP per prendere decisioni di accesso per i client.

Fase 1: Oscilloscopi autonomi

Se il token di accesso contiene ambiti indipendenti, ONTAP esamina prima tali ambiti. Se non sono presenti oscilloscopi autonomi, passare al punto 2.

Con uno o più ambiti auto-contenuti presenti, ONTAP applica ogni ambito fino a quando non può essere presa una decisione esplicita **ALLOW** o **DENY**. Se viene presa una decisione esplicita, l'elaborazione termina.

Se ONTAP non è in grado di prendere una decisione di accesso esplicita, continuare con il passaggio 2.

Passaggio 2: Controllare il flag dei ruoli locali

ONTAP esamina il valore del flag `use-local-roles-if-present`. Il valore di questo indicatore viene impostato separatamente per ogni server di autorizzazione definito su ONTAP.

- Se il valore è `true` passare alla fase 3.
- Se il valore è `false` l'elaborazione termina e l'accesso è negato.

Passaggio 3: Ruolo REST di Named ONTAP

Se il token di accesso contiene un ruolo REST denominato, ONTAP utilizza il ruolo per prendere la decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se non è presente alcun ruolo REST denominato o se il ruolo non è stato trovato, passare al punto 4.

Fase 4: Utenti ONTAP locali

Estrarre il nome utente dal token di accesso e tentare di associarlo a un utente ONTAP locale.

Se un utente ONTAP locale viene associato, ONTAP utilizza il ruolo definito per l'utente per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se un utente ONTAP locale non corrisponde o se non è presente alcun nome utente nel token di accesso, passare al punto 5.

Fase 5: Mappatura da gruppo a ruolo

Estrarre il gruppo dal token di accesso e tentare di associarlo a un gruppo. I gruppi vengono definiti utilizzando Active Directory o un server LDAP equivalente.

Se esiste una corrispondenza di gruppo, ONTAP utilizza il ruolo definito per il gruppo per prendere una decisione di accesso. Ciò comporta sempre una decisione **ALLOW** o **DENY** e l'elaborazione termina.

Se non è presente alcuna corrispondenza di gruppo o se non è presente alcun gruppo nel token di accesso, l'accesso viene negato e l'elaborazione termina.

Scenari di distribuzione di OAuth 2,0

Quando si definisce un server di autorizzazione per ONTAP, sono disponibili diverse opzioni di configurazione. In base a queste opzioni, è possibile creare un server di autorizzazione appropriato per l'ambiente di distribuzione.

Riepilogo dei parametri di configurazione

Quando si definisce un server di autorizzazione per ONTAP, sono disponibili diversi parametri di configurazione. Questi parametri sono generalmente supportati in tutte le interfacce amministrative.

I nomi dei parametri possono variare leggermente a seconda dell'interfaccia amministrativa di ONTAP. Ad esempio, quando si configura l'introspezione remota, l'endpoint viene identificato utilizzando il parametro del comando CLI `-introspection-endpoint`. Con System Manager, il campo equivalente è *Authorization server token introspection URI*. Per soddisfare tutte le interfacce amministrative di ONTAP, viene fornita una descrizione generale dei parametri. Il parametro o il campo esatto dovrebbe essere ovvio in base al contesto.

Parametro	Descrizione
Nome	Il nome del server di autorizzazione così come è noto a ONTAP.
Applicazione	L'applicazione interna ONTAP a cui si applica la definizione. Deve essere http .
URI emittente	FQDN con percorso che identifica il sito o l'organizzazione che emette i token.
Provider JWKS URI	L'FQDN con percorso e nome file in cui ONTAP ottiene i set di chiavi Web JSON utilizzati per convalidare i token di accesso.
Intervallo di aggiornamento JWKS	L'intervallo di tempo che determina la frequenza con cui ONTAP aggiorna le informazioni del certificato dall'URI JWKS del provider. Il valore è specificato in formato ISO-8601.
Endpoint introspezione	L'FQDN con percorso utilizzato da ONTAP per eseguire la convalida dei token remoti tramite introspezione.
ID client	Il nome del client come definito nel server di autorizzazione. Quando questo valore è incluso, è necessario anche fornire il segreto client associato in base all'interfaccia.
Proxy in uscita	In questo modo viene fornito l'accesso al server di autorizzazione quando ONTAP è protetto da un firewall. L'URI deve essere in formato Curl.
Utilizzare i ruoli locali, se presenti	Un flag booleano che determina se vengono utilizzate le definizioni ONTAP locali, inclusi un ruolo REST denominato e gli utenti locali.
Rimuovere la richiesta di rimborso dell'utente	Un nome alternativo utilizzato da ONTAP per associare gli utenti locali. Utilizzare <code>sub</code> nel token di accesso in modo che corrisponda al nome utente locale.

Scenari di distribuzione

Di seguito vengono presentati diversi scenari di distribuzione comuni. Sono organizzati in base al fatto che la convalida dei token venga eseguita localmente da ONTAP o in remoto dal server di autorizzazione. Ogni scenario include un elenco delle opzioni di configurazione richieste. Vedere ["Implementa OAuth 2,0 in ONTAP"](#) per esempi dei comandi di configurazione.



Dopo aver definito un server di autorizzazione, è possibile visualizzarne la configurazione tramite l'interfaccia amministrativa di ONTAP. Ad esempio, utilizzare il comando `security oauth2 client show` Con l'interfaccia a riga di comando di ONTAP.

Convalida locale

I seguenti scenari di distribuzione si basano su ONTAP che esegue la convalida dei token localmente.

Utilizzare gli oscilloscopi autonomi senza proxy

Questa è l'implementazione più semplice che utilizza solo gli oscilloscopi indipendenti OAuth 2,0. Nessuna delle definizioni di identità ONTAP locali viene utilizzata. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- URI emittente

È inoltre necessario aggiungere gli ambiti al server di autorizzazione.

Utilizzare gli oscilloscopi autonomi con un proxy

Questo scenario di distribuzione utilizza gli oscilloscopi indipendenti OAuth 2.0. Nessuna delle definizioni di identità ONTAP locali viene utilizzata. Ma il server di autorizzazione è protetto da un firewall e quindi è necessario configurare un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Proxy in uscita
- URI emittente
- Pubblico

È inoltre necessario aggiungere gli ambiti al server di autorizzazione.

Utilizzare ruoli utente locali e associazione nome utente predefinita con un proxy

Questo scenario di distribuzione utilizza ruoli utente locali con mappatura dei nomi predefinita. La richiesta di rimborso dell'utente remoto utilizza il valore predefinito di `sub` quindi questo campo nel token di accesso viene utilizzato per corrispondere al nome utente locale. Il nome utente deve contenere al massimo 40 caratteri. Il server di autorizzazione è protetto da un firewall, quindi è necessario configurare anche un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Utilizzare i ruoli locali, se presenti (`true`)
- Proxy in uscita
- Emittente

È necessario assicurarsi che l'utente locale sia definito su ONTAP.

Utilizzare ruoli utente locali e mapping nome utente alternativo con un proxy

Questo scenario di distribuzione utilizza ruoli utente locali con un nome utente alternativo utilizzato per associare un utente ONTAP locale. Il server di autorizzazione è protetto da un firewall, quindi è necessario configurare un proxy. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Provider JWKS URI
- Utilizzare i ruoli locali, se presenti (`true`)
- Richiesta di rimborso per utenti remoti
- Proxy in uscita
- URI emittente
- Pubblico

È necessario assicurarsi che l'utente locale sia definito su ONTAP.

Introspezione remota

Le seguenti configurazioni di distribuzione si basano su ONTAP che esegue la convalida dei token in modalità remota tramite introspezione.

Utilizzare gli oscilloscopi autonomi senza proxy

Si tratta di una semplice implementazione basata sull'utilizzo degli oscilloscopi indipendenti OAuth 2,0. Nessuna delle definizioni di identità ONTAP viene utilizzata. È necessario includere i seguenti parametri:

- Nome
- Applicazione (http)
- Endpoint introspezione
- ID client
- URI emittente

È necessario definire gli ambiti, nonché il segreto client e client nel server di autorizzazione.

Autenticazione client mediante TLS reciproco

A seconda delle esigenze di protezione, è possibile configurare il protocollo mTLS (Mutual TLS) per implementare l'autenticazione client avanzata. Quando viene utilizzato con ONTAP come parte di una distribuzione OAuth 2,0, mTLS garantisce che i token di accesso vengano utilizzati solo dai client ai quali sono stati originariamente emessi.

TLS reciproco con OAuth 2,0

Transport Layer Security (TLS) viene utilizzato per stabilire un canale di comunicazione sicuro tra due applicazioni, in genere un browser client e un server Web. Il TLS reciproco estende questa funzione fornendo una solida identificazione del client tramite un certificato client. Quando viene utilizzata in un cluster ONTAP con OAuth 2,0, la funzionalità mTLS di base viene estesa creando e utilizzando token di accesso con vincoli di mittente.

Un token di accesso vincolato dal mittente può essere utilizzato solo dal client al quale è stato originariamente emesso. Per supportare questa funzione, è necessario presentare una nuova richiesta di conferma (cnf) è inserito nel token. Il campo contiene proprietà `x5t#S256` che contiene un digest del certificato client utilizzato quando si richiede il token di accesso. Questo valore viene verificato da ONTAP come parte della convalida del token. I token di accesso emessi dai server di autorizzazione che non sono vincolati dal mittente non includono la richiesta di conferma aggiuntiva.

È necessario configurare ONTAP in modo che utilizzi mTLS separatamente per ogni server di autorizzazione. Ad esempio, il comando CLI `security oauth2 client include` il parametro `use-mutual-tls`. Per controllare l'elaborazione mTLS in base a tre valori, come mostrato nella tabella seguente.



In ogni configurazione, il risultato e l'azione intrapresi da ONTAP dipendono dal valore del parametro di configurazione, dal contenuto del token di accesso e dal certificato client. I parametri nella tabella sono organizzati dal minimo al più restrittivo.

Parametro	Descrizione
nessuno	L'autenticazione TLS reciproca OAuth 2,0 è completamente disattivata per il server di autorizzazione. ONTAP non eseguirà l'autenticazione del certificato client mTLS anche se la richiesta di conferma è presente nel token o se viene fornito un certificato client con la connessione TLS.
richiesta	L'autenticazione reciproca TLS OAuth 2,0 viene applicata se il client presenta un token di accesso con restrizioni del mittente. Vale a dire, mTLS viene applicato solo se la richiesta di conferma (con proprietà <code>x5t#S256</code>) è presente nel token di accesso. Questa è l'impostazione predefinita.
obbligatorio	L'autenticazione TLS reciproca OAuth 2,0 viene applicata per tutti i token di accesso emessi dal server di autorizzazione. Pertanto, tutti i token di accesso devono essere vincolati dal mittente. L'autenticazione e la richiesta dell'API REST non riescono se la richiesta di conferma non è presente nel token di accesso o se è presente un certificato client non valido.

Flusso di implementazione di alto livello

Di seguito vengono illustrati i passaggi tipici richiesti quando si utilizza mTLS con OAuth 2,0 in un ambiente ONTAP. Vedere ["RFC 8705: Autenticazione client OAuth 2,0 Mutual-TLS e token di accesso con associazione a certificati"](#) per ulteriori dettagli.

Passaggio 1: Creare e installare un certificato client

La definizione dell'identità del client si basa sulla prova della conoscenza di una chiave privata del client. La chiave pubblica corrispondente viene inserita in un certificato X.509 firmato presentato dal cliente. A un livello elevato, i passaggi necessari per la creazione del certificato client includono:

1. Generare una coppia di chiavi pubbliche e private
2. Creare una richiesta di firma del certificato
3. Inviare il file CSR a una CA nota
4. CA verifica la richiesta ed emette il certificato firmato

In genere è possibile installare il certificato client nel sistema operativo locale o utilizzarlo direttamente con un'utilità comune, ad esempio curl.

Passaggio 2: Configurare ONTAP per l'utilizzo di mTLS

È necessario configurare ONTAP per utilizzare mTLS. Questa configurazione viene eseguita separatamente per ogni server di autorizzazione. Ad esempio, con il CLI il comando `security oauth2 client` viene utilizzato con il parametro opzionale `use-mutual-tls`. Vedere ["Implementa OAuth 2,0 in ONTAP"](#) per ulteriori informazioni.

Passaggio 3: Il client richiede un token di accesso

Il client deve richiedere un token di accesso dal server di autorizzazione configurato su ONTAP. L'applicazione client deve utilizzare mTLS con il certificato creato e installato nel passaggio 1.

Passaggio 4: Il server di autorizzazione genera il token di accesso

Il server di autorizzazione verifica la richiesta del client e genera un token di accesso. Come parte di ciò, crea un riepilogo del messaggio del certificato client che è incluso nel token come richiesta di conferma (campo `cnf`).

Passaggio 5: L'applicazione client presenta il token di accesso a ONTAP

L'applicazione client effettua una chiamata API REST al cluster ONTAP e include il token di accesso nell'intestazione della richiesta di autorizzazione come token **bearer**. Il client deve utilizzare mTLS con lo stesso certificato utilizzato per richiedere il token di accesso.

Passaggio 6: ONTAP verifica client e token.

ONTAP riceve il token di accesso in una richiesta HTTP e il certificato client utilizzato come parte dell'elaborazione mTLS. ONTAP prima convalida la firma nel token di accesso. In base alla configurazione, ONTAP genera un riepilogo dei messaggi del certificato client e lo confronta con l'attestazione di conferma **cnf** nel token. Se i due valori corrispondono, ONTAP ha confermato che il client che effettua la richiesta API è lo stesso client a cui è stato originariamente emesso il token di accesso.

Configurazione e implementazione

Preparati a implementare OAuth 2,0 con ONTAP

Prima di configurare OAuth 2,0 in un ambiente ONTAP, è necessario prepararsi per la distribuzione. Di seguito è riportato un riepilogo delle principali attività e decisioni. La disposizione delle sezioni è generalmente allineata con l'ordine da seguire. Tuttavia, sebbene sia applicabile per la maggior parte delle implementazioni, è consigliabile adattarlo all'ambiente in base alle esigenze. È inoltre opportuno prendere in considerazione la creazione di un piano di distribuzione formale.



In base all'ambiente in uso, è possibile selezionare la configurazione per i server di autorizzazione definiti in ONTAP. Sono inclusi i valori dei parametri da specificare per ogni tipo di distribuzione. Vedere "[Scenari di distribuzione di OAuth 2,0](#)" per ulteriori informazioni.

Risorse protette e applicazioni client

OAuth 2,0 è un framework di autorizzazione per controllare l'accesso alle risorse protette. In questo caso, un primo passo importante per qualsiasi distribuzione consiste nel determinare quali sono le risorse disponibili e quali client devono accedervi.

Identificare le applicazioni client

È necessario decidere quali client utilizzeranno OAuth 2,0 per l'emissione di chiamate API REST e a quali endpoint API devono accedere.

Esaminare i ruoli REST ONTAP esistenti e gli utenti locali

È necessario esaminare le definizioni di identità ONTAP esistenti, inclusi i ruoli REST e gli utenti locali. A seconda della configurazione di OAuth 2,0, queste definizioni possono essere utilizzate per prendere decisioni sugli accessi.

Transizione globale a OAuth 2,0

Sebbene sia possibile implementare l'autorizzazione OAuth 2,0 gradualmente, è anche possibile spostare immediatamente tutti i client API REST in OAuth 2,0 impostando un flag globale per ogni server di autorizzazione. In questo modo, è possibile prendere decisioni di accesso in base alla configurazione ONTAP esistente senza dover creare ambiti autonomi.

Server di autorizzazione

I server di autorizzazione svolgono un ruolo importante nella distribuzione di OAuth 2,0 rilasciando token di accesso e applicando criteri amministrativi.

Selezionare e installare il server di autorizzazione

È necessario selezionare e installare uno o più server di autorizzazione. È importante acquisire familiarità con le opzioni di configurazione e le procedure dei provider di identità, incluse le modalità di definizione degli ambiti.

Determinare se è necessario installare il certificato CA principale di autorizzazione

ONTAP utilizza il certificato del server di autorizzazione per convalidare i token di accesso firmati presentati dai client. A tale scopo, ONTAP necessita del certificato della CA principale e di eventuali certificati intermedi. Questi potrebbero essere preinstallati con ONTAP. In caso contrario, è necessario installarli.

Valutare la posizione e la configurazione della rete

Se il server di autorizzazione è protetto da un firewall, ONTAP deve essere configurato per utilizzare un server proxy.

Autenticazione e autorizzazione del client

È necessario prendere in considerazione diversi aspetti dell'autenticazione e dell'autorizzazione dei client.

Ambiti indipendenti o definizioni di identità ONTAP locali

A un livello elevato, è possibile definire ambiti indipendenti definiti nel server di autorizzazione o fare affidamento sulle definizioni di identità ONTAP locali esistenti, inclusi ruoli e utenti.

Opzioni con elaborazione ONTAP locale

Se si utilizzano le definizioni di identità ONTAP, è necessario decidere quale applicare, tra cui:

- Ruolo REST denominato
- Far corrispondere gli utenti locali
- Active Directory o gruppi LDAP

Convalida locale o introspezione remota

È necessario decidere se i token di accesso verranno convalidati localmente da ONTAP o dal server di autorizzazione tramite introspezione. Ci sono anche diversi valori correlati da prendere in considerazione, come l'intervallo di aggiornamento.

Token di accesso con restrizioni del mittente

Per gli ambienti che richiedono un alto livello di protezione, è possibile utilizzare token di accesso con limitazioni di invio basati su mTLS. Questo richiede un certificato per ciascun client.

Interfaccia amministrativa

È possibile eseguire l'amministrazione di OAuth 2,0 tramite una qualsiasi delle interfacce ONTAP, tra cui:

- Interfaccia della riga di comando
- System Manager
- API REST

Modalità con cui i client richiedono i token di accesso

Le applicazioni client devono richiedere i token di accesso direttamente dal server di autorizzazione. È necessario decidere in che modo eseguire questa operazione, incluso il tipo di concessione.

Configure ONTAP (Configura SNMP)

È necessario eseguire diverse attività di configurazione di ONTAP.

Definire i ruoli REST e gli utenti locali

In base alla configurazione dell'autorizzazione, è possibile utilizzare l'elaborazione dell'identificazione ONTAP locale. In questo caso, è necessario rivedere e definire i ruoli REST e le definizioni utente.

Configurazione di base

Per eseguire la configurazione di base di ONTAP sono necessari tre passaggi principali, tra cui:

- Se si desidera, installare il certificato di origine (e qualsiasi certificato intermedio) per la CA che ha firmato il certificato del server di autorizzazione.
- Definire il server di autorizzazione.
- Abilitare l'elaborazione OAuth 2,0 per il cluster.

Implementa OAuth 2,0 in ONTAP

L'implementazione della funzionalità principale di OAuth 2,0 richiede tre fasi principali.

Prima di iniziare

È necessario prepararsi per la distribuzione di OAuth 2,0 prima di configurare ONTAP. Ad esempio, è necessario valutare il server di autorizzazione, incluso il modo in cui il certificato è stato firmato e se è protetto da un firewall. Vedere ["Preparati a implementare OAuth 2,0 con ONTAP"](#) per ulteriori informazioni.

Passaggio 1: Installazione del certificato del server di autenticazione

ONTAP include un gran numero di certificati CA principali preinstallati. Pertanto, in molti casi, il certificato per il server di autorizzazione verrà immediatamente riconosciuto da ONTAP senza ulteriori configurazioni. Tuttavia, a seconda di come è stato firmato il certificato del server di autorizzazione, potrebbe essere necessario installare un certificato della CA principale e qualsiasi certificato intermedio.

Seguire le istruzioni fornite di seguito per installare il certificato, se necessario. È necessario installare tutti i certificati richiesti a livello di cluster.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP.

Esempio 1. Fasi

System Manager

1. In System Manager, selezionare **Cluster > Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su → accanto a **certificati**.
4. Nella scheda **autorità di certificazione attendibili** fare clic su **Aggiungi**.
5. Fare clic su **Importa** e selezionare il file del certificato.
6. Completare i parametri di configurazione dell'ambiente.
7. Fare clic su **Aggiungi**.

CLI

1. Avviare l'installazione:

```
security certificate install -type server-ca
```

2. Cercare il seguente messaggio della console:

```
Please enter Certificate: Press <Enter> when done
```

3. Aprire il file del certificato con un editor di testo.
4. Copiare l'intero certificato, incluse le seguenti righe:

```
-----BEGIN CERTIFICATE-----  
  
-----END CERTIFICATE-----
```

5. Incollare il certificato nel terminale dopo il prompt dei comandi.
6. Premere **Invio** per completare l'installazione.
7. Verificare che il certificato sia installato utilizzando una delle seguenti opzioni:

```
security certificate show-user-installed  
  
security certificate show
```

Passaggio 2: Configurare il server di autorizzazione

È necessario definire almeno un server di autorizzazione per ONTAP. È necessario scegliere i valori dei parametri in base alla configurazione e al piano di distribuzione. Revisione ["OAuth2 scenari di distribuzione"](#) per determinare i parametri esatti necessari per la configurazione.



Per modificare la definizione di un server di autorizzazione, è possibile eliminare la definizione esistente e crearne una nuova.

L'esempio fornito di seguito si basa sul primo semplice scenario di distribuzione all'indirizzo ["Convalida locale"](#). Gli oscilloscopi autonomi vengono utilizzati senza proxy.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP. La procedura CLI utilizza variabili

simboliche che è necessario sostituire prima di eseguire il comando.

Esempio 2. Fasi

System Manager

1. In System Manager, selezionare **Cluster > Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su **+** accanto a **autorizzazione OAuth 2,0**.
4. Selezionare **altre opzioni**.
5. Fornire i valori richiesti per la distribuzione, ad esempio:
 - Nome
 - Applicazione (http)
 - Provider JWKS URI
 - URI emittente
6. Fare clic su **Aggiungi**.

CLI

1. Creare nuovamente la definizione:

```
security oauth2 client create -config-name <NAME> -provider-jwks-uri  
<URI_JWKS> -application http -issuer <URI_ISSUER>
```

Ad esempio:

```
security oauth2 client create \  
-config-name auth0 \  
-provider-jwks-uri https://superzap.dev.netapp.com:8443/realms/my-  
realm/protocol/openid-connect/certs \  
-application http \  
-issuer https://superzap.dev.netapp.com:8443/realms/my-realm
```

Fase 3: Abilitare OAuth 2,0

Il passaggio finale consiste nell'abilitare OAuth 2,0. Si tratta di un'impostazione globale per il cluster ONTAP.



Non attivare l'elaborazione OAuth 2,0 finché non si conferma che ONTAP, i server di autorizzazione e gli eventuali servizi di supporto sono stati configurati correttamente.

Scegliere la procedura corretta in base alla modalità di accesso a ONTAP.

Esempio 3. Fasi

System Manager

1. In System Manager, selezionare **Cluster > Impostazioni**.
2. Scorrere fino alla sezione **protezione**.
3. Fare clic su → accanto a **autorizzazione OAuth 2,0**.
4. Abilita **autorizzazione OAuth 2,0**.

CLI

1. Abilita OAuth 2,0:

```
security oauth2 modify -enabled true
```

2. Confermare che OAuth 2,0 sia abilitato:

```
security oauth2 show  
Is OAuth 2.0 Enabled: true
```

Eseguire una chiamata API REST utilizzando OAuth 2,0

L'implementazione di OAuth 2,0 in ONTAP supporta le applicazioni client API REST. È possibile eseguire una semplice chiamata API REST utilizzando curl per iniziare a utilizzare OAuth 2,0. L'esempio presentato di seguito recupera la versione del cluster ONTAP.

Prima di iniziare

È necessario configurare e abilitare la funzione OAuth 2,0 per il cluster ONTAP. Ciò include la definizione di un server di autorizzazione.

Fase 1: Acquisire un token di accesso

È necessario acquisire un token di accesso da utilizzare con la chiamata API REST. La richiesta token viene eseguita al di fuori di ONTAP e la procedura esatta dipende dal server di autorizzazione e dalla relativa configurazione. È possibile richiedere il token tramite un browser Web, con un comando curl o utilizzando un linguaggio di programmazione.

A scopo illustrativo, di seguito viene presentato un esempio di come un token di accesso può essere richiesto da Keycloak usando curl.

Esempio Keycloak

```
curl --request POST \  
--location  
'https://superzap.dev.netapp.com:8443/realms/peterson/protocol/openid-  
connect/token' \  
--header 'Content-Type: application/x-www-form-urlencoded' \  
--data-urlencode 'client_id=dp-client-1' \  
--data-urlencode 'grant_type=client_credentials' \  
--data-urlencode 'client_secret=5iTUf9QKLGxAoYaliR33v1D5A2xq09V7'
```

Copiare e salvare il token restituito.

Passaggio 2: Eseguire la chiamata API REST

Dopo avere un token di accesso valido, è possibile utilizzare un comando curl con il token di accesso per eseguire una chiamata API REST.

Parametri e variabili

Le due variabili nell'esempio dell'arricciatura sono descritte nella tabella seguente.

Variabile	Descrizione
\$FQDN_IP	Il nome di dominio o l'indirizzo IP pienamente qualificato della LIF di gestione ONTAP.
\$ACCESS_TOKEN	Token di accesso OAuth 2,0 emesso dal server di autorizzazione.

Prima di eseguire l'esempio Curl, è necessario impostare queste variabili nell'ambiente della shell Bash. Ad esempio, nella CLI di Linux digitare il seguente comando per impostare e visualizzare la variabile FQDN:

```
FQDN_IP=172.14.31.224  
echo $FQDN_IP  
172.14.31.224
```

Dopo aver definito entrambe le variabili nella shell Bash locale, è possibile copiare il comando curl e incollarlo nella CLI. Premere **Invio** per sostituire le variabili ed eseguire il comando.

Esempio di arricciamento

```
curl --request GET \  
--location "https://$FQDN_IP/api/cluster?fields=version" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Bearer $ACCESS_TOKEN"
```

Configurare l'autenticazione SAML

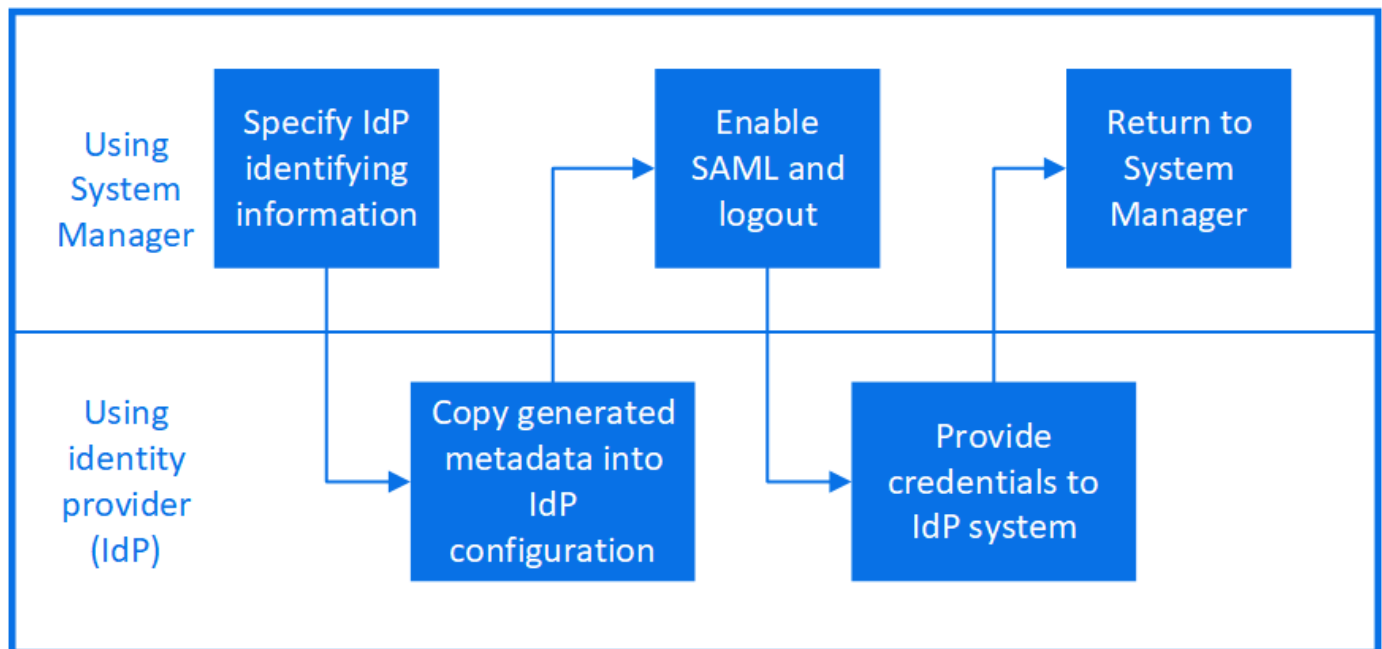
A partire da ONTAP 9.3, è possibile configurare l'autenticazione SAML (Security Assertion Markup Language) per i servizi Web. Quando l'autenticazione SAML è configurata e abilitata, gli utenti vengono autenticati da un provider di identità esterno (IdP) invece che dai provider di servizi di directory come Active Directory e LDAP.

Abilitare l'autenticazione SAML

Per attivare l'autenticazione SAML con System Manager o con la CLI, attenersi alla seguente procedura. Se il cluster esegue ONTAP 9,7 o versione precedente, la procedura indicata è diversa da quella illustrata in System Manager. Fare riferimento alla guida in linea di System Manager disponibile sul sistema.



Dopo aver attivato l'autenticazione SAML, solo gli utenti remoti possono accedere alla GUI di System Manager. Gli utenti locali non possono accedere alla GUI di System Manager dopo l'attivazione dell'autenticazione SAML.



Prima di iniziare

- È necessario configurare l'IdP che si intende utilizzare per l'autenticazione remota.



Consultare la documentazione fornita dall'IdP configurato.

- È necessario disporre dell'URI dell'IdP.

A proposito di questa attività

- L'autenticazione SAML si applica solo a `http e. ontapi` applicazioni.

Il `http e. ontapi` Le applicazioni vengono utilizzate dai seguenti servizi Web: Infrastruttura del processore di servizi, API ONTAP o Gestore di sistema.

- L'autenticazione SAML è applicabile solo per l'accesso alla SVM amministrativa.


I seguenti IDP sono stati convalidati con System Manager:

- Servizi di federazione di Active Directory
- Cisco DUO (compatibile con le seguenti versioni di ONTAP:)
 - 9.7P21 e versioni successive 9,7 (fare riferimento a. ["Documentazione di System Manager Classic"](#))
 - 9.8P17 e versioni successive 9,8
 - 9,9.1P13 e versioni successive 9,9
 - 9.10.1P9 e versioni successive 9,10
 - 9.11.1P4 e versioni successive 9,11
 - 9.12.1 e versioni successive
- Shibboleth

A seconda dell'ambiente in uso, effettuare le seguenti operazioni:

Esempio 4. Fasi

System Manager

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. Accanto a **SAML Authentication**, fare clic su .
3. Verificare che la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML) sia selezionata.
4. Inserire l'URL dell'URI IdP (incluso "[- 5. Modificare l'indirizzo del sistema host, se necessario.
- 6. Assicurarsi di utilizzare il certificato corretto:
 - Se il sistema è stato mappato con un solo certificato di tipo "server", il certificato viene considerato predefinito e non viene visualizzato.
 - Se il sistema è stato mappato con più certificati come tipo "server", viene visualizzato uno dei certificati. Per selezionare un certificato diverso, fare clic su **Cambia**.
- 7. Fare clic su **Save** \(Salva\). Una finestra di conferma visualizza le informazioni sui metadati, che sono state copiate automaticamente negli Appunti.
- 8. Accedere al sistema IdP specificato e copiare i metadati dagli Appunti per aggiornare i metadati del sistema.
- 9. Tornare alla finestra di conferma \(in System Manager\) e selezionare la casella di controllo **ho configurato IdP con l'URI host o i metadati**.
- 10. Fare clic su **Logout** per attivare l'autenticazione basata su SAML. Il sistema IdP visualizza una schermata di autenticazione.
- 11. Nel sistema IdP, immettere le credenziali basate su SAML. Una volta verificate le credenziali, viene visualizzata la home page di System Manager.](https://\)

CLI

1. Creare una configurazione SAML in modo che ONTAP possa accedere ai metadati IdP:

```
security saml-sp create -idp-uri idp_uri -sp-host ontap_host_name
```

`idp_uri` È l'indirizzo FTP o HTTP dell'host IdP da cui è possibile scaricare i metadati IdP.

`ontap_host_name` È il nome host o l'indirizzo IP dell'host del provider di servizi SAML, che in questo caso è il sistema ONTAP. Per impostazione predefinita, viene utilizzato l'indirizzo IP della LIF di gestione del cluster.

È possibile fornire le informazioni sul certificato del server ONTAP. Per impostazione predefinita, vengono utilizzate le informazioni del certificato del server Web ONTAP.

```
cluster_12::> security saml-sp create -idp-uri  
https://example.url.net/idp/shibboleth
```

Warning: This restarts the web server. Any HTTP/S connections that are active

will be disrupted.

Do you want to continue? {y|n}: y

[Job 179] Job succeeded: Access the SAML SP metadata using the URL:
https://10.0.0.1/saml-sp/Metadata

Configure the IdP and Data ONTAP users for the same directory server domain to ensure that users are the same for different authentication methods. See the "security login show" command for the Data ONTAP user configuration.

Viene visualizzato l'URL per accedere ai metadati dell'host ONTAP.

2. Dall'host IdP, configurare IdP con i metadati dell'host ONTAP.

Per ulteriori informazioni sulla configurazione di IdP, consultare la documentazione di IdP.

3. Abilitare la configurazione SAML:

```
security saml-sp modify -is-enabled true
```

Qualsiasi utente esistente che accede a `http` oppure `ontapi` L'applicazione viene configurata automaticamente per l'autenticazione SAML.

4. Se si desidera creare utenti per `http` oppure `ontapi` Applicazione dopo aver configurato SAML, specificare SAML come metodo di autenticazione per i nuovi utenti.

- a. Creare un metodo di accesso per i nuovi utenti con autenticazione SAML:

```
security login create -user-or-group-name user_name -application [http |  
ontapi] -authentication-method saml -vserver svm_name
```

```
cluster_12::> security login create -user-or-group-name admin1  
-application http -authentication-method saml -vserver  
cluster_12
```

- b. Verificare che la voce utente sia stata creata:

```
security login show
```

```
cluster_12::> security login show
```

```
Vserver: cluster_12
```

```
Second
```

User/Group	Authentication	Acct
Name	Application Method	Role Name
Method		Locked
admin	console	password
none		admin
admin	http	password
none		admin
admin	http	saml
none		admin
admin	ontapi	password
none		admin
admin	ontapi	saml
none		admin
admin	service-processor	password
none		admin
admin	ssh	password
none		admin
admin1	http	password
none		backup
**admin1	http	saml
none**		backup


Disattiva l'autenticazione SAML

È possibile disattivare l'autenticazione SAML quando si desidera interrompere l'autenticazione degli utenti Web utilizzando un provider di identità (IdP) esterno. Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati come Active Directory e LDAP vengono utilizzati per l'autenticazione.

A seconda dell'ambiente in uso, effettuare le seguenti operazioni:

Esempio 5. Fasi

System Manager

1. Fare clic su **Cluster > Settings** (Cluster > Impostazioni).
2. In **SAML Authentication**, fare clic sul pulsante di commutazione **Enabled**.
3. *Opzionale:* È anche possibile fare clic su  Accanto a **SAML Authentication**, quindi deselezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).

CLI

1. Disattiva autenticazione SAML:

```
security saml-sp modify -is-enabled false
```

2. Se non si desidera più utilizzare l'autenticazione SAML o se si desidera modificare IdP, eliminare la configurazione SAML:

```
security saml-sp delete
```

Risolvere i problemi relativi alla configurazione SAML

Se la configurazione dell'autenticazione SAML (Security Assertion Markup Language) non riesce, è possibile riparare manualmente ogni nodo su cui la configurazione SAML ha avuto esito negativo e ripristinarlo in caso di errore. Durante il processo di riparazione, il server Web viene riavviato e tutte le connessioni HTTP o HTTPS attive vengono interrompute.

A proposito di questa attività

Quando si configura l'autenticazione SAML, ONTAP applica la configurazione SAML per nodo. Quando si attiva l'autenticazione SAML, ONTAP tenta automaticamente di riparare ogni nodo in caso di problemi di configurazione. In caso di problemi con la configurazione SAML su qualsiasi nodo, è possibile disattivare l'autenticazione SAML e riattivarla. Possono verificarsi situazioni in cui la configurazione SAML non viene applicata a uno o più nodi anche dopo aver riattivato l'autenticazione SAML. È possibile identificare il nodo su cui si è verificato un errore nella configurazione SAML e quindi riparare manualmente tale nodo.

Fasi

1. Accedere al livello di privilegio avanzato:

```
set -privilege advanced
```

2. Identificare il nodo su cui la configurazione SAML non ha avuto esito positivo:

```
security saml-sp status show -instance
```

```
cluster_12::*> security saml-sp status show -instance

Node: node1
Update Status: config-success
Database Epoch: 9
Database Transaction Count: 997
Error Text:
SAML Service Provider Enabled: false
ID of SAML Config Job: 179

Node: node2
Update Status: config-failed
Database Epoch: 9
Database Transaction Count: 997
Error Text: SAML job failed, Reason: Internal error.
Failed to receive the SAML IDP Metadata file.
SAML Service Provider Enabled: false
ID of SAML Config Job: 180
2 entries were displayed.
```

3. Riparare la configurazione SAML sul nodo guasto:

security saml-sp repair -node *node_name*

```
cluster_12::*> security saml-sp repair -node node2

Warning: This restarts the web server. Any HTTP/S connections that are
active
        will be disrupted.
Do you want to continue? {y|n}: y
[Job 181] Job is running.
[Job 181] Job success.
```

Il server Web viene riavviato e tutte le connessioni HTTP o HTTPS attive vengono interrompute.

4. Verificare che SAML sia configurato correttamente su tutti i nodi:

security saml-sp status show -instance

```
cluster_12::*> security saml-sp status show -instance
```

```

                Node: node1
        Update Status: config-success
    Database Epoch: 9
Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 179

                Node: node2
        Update Status: **config-success**
    Database Epoch: 9
Database Transaction Count: 997
        Error Text:
SAML Service Provider Enabled: false
        ID of SAML Config Job: 180
2 entries were displayed.
```

Informazioni correlate

["Comandi di ONTAP 9"](#)

Gestire i servizi Web

Panoramica sulla gestione dei servizi Web

È possibile attivare o disattivare un servizio Web per il cluster o una macchina virtuale di storage (SVM), visualizzare le impostazioni per i servizi Web e controllare se gli utenti di un ruolo possono accedere a un servizio Web.

È possibile gestire i servizi Web per il cluster o una SVM nei seguenti modi:

- Attivazione o disattivazione di un servizio Web specifico
- Specifica se l'accesso a un servizio Web è limitato solo a HTTP (SSL) crittografato
- Visualizzazione della disponibilità dei servizi Web
- Consentire o negare agli utenti di un ruolo di accedere a un servizio Web
- Visualizzazione dei ruoli autorizzati ad accedere a un servizio Web

Affinché un utente possa accedere a un servizio Web, devono essere soddisfatte tutte le seguenti condizioni:

- L'utente deve essere autenticato.

Ad esempio, un servizio Web potrebbe richiedere un nome utente e una password. La risposta dell'utente deve corrispondere a un account valido.

- L'utente deve essere configurato con il metodo di accesso corretto.

L'autenticazione ha successo solo per gli utenti con il metodo di accesso corretto per il servizio Web specificato. Per il servizio Web API di ONTAP (`ontapi`), gli utenti devono disporre di `ontapi` metodo di accesso. Per tutti gli altri servizi Web, gli utenti devono disporre di `http` metodo di accesso.



Si utilizza `security login` comandi per gestire i metodi di accesso e di autenticazione degli utenti.

- Il servizio Web deve essere configurato in modo da consentire il ruolo di controllo degli accessi dell'utente.



Si utilizza `vserver services web access` comandi per controllare l'accesso di un ruolo a un servizio web.

Se un firewall è attivato, il criterio firewall per l'utilizzo della LIF per i servizi Web deve essere impostato in modo da consentire HTTP o HTTPS.

Se si utilizza HTTPS per l'accesso al servizio Web, è necessario attivare anche SSL per il cluster o SVM che offre il servizio Web e fornire un certificato digitale per il cluster o SVM.

Gestire l'accesso ai servizi Web

Un servizio Web è un'applicazione a cui gli utenti possono accedere utilizzando HTTP o HTTPS. L'amministratore del cluster può configurare il motore del protocollo Web, configurare SSL, abilitare un servizio Web e consentire agli utenti di un ruolo di accedere a un servizio Web.

A partire da ONTAP 9.6, sono supportati i seguenti servizi Web:

- Infrastruttura del Service Processor (`spi`)

Questo servizio rende disponibili i file di log, core dump e MIB di un nodo per l'accesso HTTP o HTTPS attraverso la LIF di gestione del cluster o una LIF di gestione dei nodi. L'impostazione predefinita è `enabled`.

Su richiesta di accesso ai file di log o ai file core dump di un nodo, il `spi` il servizio web crea automaticamente un punto di montaggio da un nodo al volume root di un altro nodo in cui risiedono i file. Non è necessario creare manualmente il punto di montaggio.

- API ONTAP (`ontapi`)

Questo servizio consente di eseguire API ONTAP per eseguire funzioni amministrative con un programma remoto. L'impostazione predefinita è `enabled`.

Questo servizio potrebbe essere richiesto per alcuni strumenti di gestione esterni. Ad esempio, se si utilizza System Manager, lasciare attivato questo servizio.

- Rilevamento Data ONTAP (`disco`)

Questo servizio consente alle applicazioni di gestione off-box di rilevare il cluster nella rete. L'impostazione predefinita è `enabled`.

- Diagnostica di supporto (`supdiag`)

Questo servizio controlla l'accesso a un ambiente privilegiato sul sistema per facilitare l'analisi e la risoluzione dei problemi. L'impostazione predefinita è `disabled`. Attivare questo servizio solo se richiesto dal supporto tecnico.

- System Manager (`sysmgr`)

Questo servizio controlla la disponibilità di Gestore di sistema, incluso in ONTAP. L'impostazione predefinita è `enabled`. Questo servizio è supportato solo sul cluster.

- Aggiornamento del firmware Baseboard Management Controller (BMC) (`FW_BMC`)

Questo servizio consente di scaricare i file del firmware BMC. L'impostazione predefinita è `enabled`.

- Documentazione ONTAP (`docs`)

Questo servizio consente di accedere alla documentazione di ONTAP. L'impostazione predefinita è `enabled`.

- API RESTful di ONTAP (`docs_api`)

Questo servizio fornisce l'accesso alla documentazione dell'API RESTful di ONTAP. L'impostazione predefinita è `enabled`.

- Caricamento e download del file (`fud`)

Questo servizio offre il caricamento e il download dei file. L'impostazione predefinita è `enabled`.

- Messaggi ONTAP (`ontapmsg`)

Questo servizio supporta un'interfaccia di pubblicazione e sottoscrizione che consente di iscriversi agli eventi. L'impostazione predefinita è `enabled`.

- Portale ONTAP (`portal`)

Questo servizio implementa il gateway in un server virtuale. L'impostazione predefinita è `enabled`.

- Interfaccia RESTful di ONTAP (`rest`)

Questo servizio supporta un'interfaccia RESTful utilizzata per gestire in remoto tutti gli elementi dell'infrastruttura cluster. L'impostazione predefinita è `enabled`.

- Security Assertion Markup Language (SAML) Service Provider Support (`saml`)

Questo servizio fornisce risorse per supportare il provider di servizi SAML. L'impostazione predefinita è `enabled`.

- Provider di servizi SAML (`saml-sp`)

Questo servizio offre servizi come i metadati SP e il servizio di asserzione per i clienti al provider di servizi. L'impostazione predefinita è `enabled`.

A partire da ONTAP 9.7, sono supportati i seguenti servizi aggiuntivi:

- File di backup della configurazione (`backups`)

Questo servizio consente di scaricare i file di backup della configurazione. L'impostazione predefinita è `enabled`.

- Sicurezza ONTAP (`security`)

Questo servizio supporta la gestione dei token CSRF per un'autenticazione avanzata. L'impostazione predefinita è `enabled`.

Gestire il motore dei protocolli Web

È possibile configurare il motore dei protocolli Web sul cluster per controllare se l'accesso Web è consentito e quali versioni SSL possono essere utilizzate. È inoltre possibile visualizzare le impostazioni di configurazione del motore dei protocolli Web.

È possibile gestire il motore dei protocolli Web a livello di cluster nei seguenti modi:

- È possibile specificare se i client remoti possono utilizzare HTTP o HTTPS per accedere al contenuto del servizio Web utilizzando `system services web modify` con il `-external` parametro.
- È possibile specificare se utilizzare SSLv3 per un accesso web sicuro utilizzando `security config modify` con il `-supported-protocol` parametro. Per impostazione predefinita, SSLv3 è disattivato. Transport Layer Security 1.0 (TLSv1.0) è attivato e può essere disattivato se necessario.
- È possibile attivare la modalità di conformità FIPS (Federal Information Processing Standard) 140-2 per le interfacce dei servizi Web del piano di controllo a livello di cluster.



Per impostazione predefinita, la modalità di conformità FIPS 140-2 è disattivata.

- **Quando la modalità di compliance FIPS 140-2 è disattivata**, è possibile attivare la modalità di compliance FIPS 140-2 impostando `is-fips-enabled` parametro a `true` per `security config modify` e quindi utilizzando il comando `security config show` per confermare lo stato online.
- **Quando è attivata la modalità di conformità FIPS 140-2**
 - A partire da ONTAP 9.11.1, TLSv1, TLSv1.1 e SSLv3 sono disattivati e solo TLSv1.2 e TLSv1.3 rimangono attivati. Riguarda altri sistemi e comunicazioni interni ed esterni a ONTAP 9. Se si attiva la modalità di conformità FIPS 140-2 e successivamente si disattiva, TLSv1, TLSv1.1 e SSLv3 rimangono disattivati. TLSv1 o TLSv1.3 resteranno abilitati a seconda della configurazione precedente.
 - Per le versioni di ONTAP precedenti alla 9.11.1, TLSv1 e SSLv3 sono disattivati e solo TLSv1.1 e TLSv1.2 rimangono attivati. ONTAP impedisce di abilitare sia TLSv1 che SSLv3 quando è attivata la modalità di conformità FIPS 140-2. Se si attiva la modalità di conformità FIPS 140-2 e successivamente la si disattiva, TLSv1 e SSLv3 rimangono disattivati, ma TLSv1.2 o TLSv1.1 e TLSv1.2 vengono attivati a seconda della configurazione precedente.
- È possibile visualizzare la configurazione della sicurezza a livello di cluster utilizzando `system security config show` comando.

Se il firewall è attivato, il criterio firewall per l'interfaccia logica (LIF) da utilizzare per i servizi Web deve essere impostato in modo da consentire l'accesso HTTP o HTTPS.

Se si utilizza HTTPS per l'accesso al servizio Web, è necessario attivare anche SSL per il cluster o la macchina virtuale di storage (SVM) che offre il servizio Web e fornire un certificato digitale per il cluster o la SVM.

Nelle configurazioni MetroCluster, le modifiche apportate alle impostazioni per il motore del protocollo Web su un cluster non vengono replicate sul cluster partner.

Comandi per la gestione del motore dei protocolli web

Si utilizza `system services web` comandi per gestire il motore dei protocolli web. Si utilizza `system services firewall policy create` e `network interface modify` comandi per consentire alle richieste di accesso web di passare attraverso il firewall.

Se si desidera...	Utilizzare questo comando...
Configurare il motore del protocollo Web a livello di cluster: <ul style="list-style-type: none">• Attivare o disattivare il motore dei protocolli Web per il cluster• Attivare o disattivare SSLv3 per il cluster• Attivazione o disattivazione della conformità FIPS 140-2 per servizi Web sicuri (HTTPS)	<code>system services web modify</code>
Visualizzare la configurazione del motore dei protocolli Web a livello di cluster, determinare se i protocolli Web sono funzionanti in tutto il cluster e visualizzare se la conformità FIPS 140-2 è attivata e online	<code>system services web show</code>
Visualizzare la configurazione del motore dei protocolli Web a livello di nodo e l'attività di gestione dei servizi Web per i nodi nel cluster	<code>system services web node show</code>
Creare una policy firewall o aggiungere il servizio del protocollo HTTP o HTTPS a una policy firewall esistente per consentire alle richieste di accesso Web di passare attraverso il firewall	<code>system services firewall policy create</code> Impostazione di <code>-service</code> parametro a <code>http</code> oppure <code>https</code> consente alle richieste di accesso web di passare attraverso il firewall.
Associare una policy firewall a una LIF	<code>network interface modify</code> È possibile utilizzare <code>-firewall-policy</code> Parametro per modificare la policy firewall di una LIF.

Configurare l'accesso ai servizi Web

La configurazione dell'accesso ai servizi Web consente agli utenti autorizzati di utilizzare

HTTP o HTTPS per accedere al contenuto del servizio sul cluster o su una macchina virtuale di storage (SVM).

Fasi

1. Se è attivato un firewall, assicurarsi che l'accesso HTTP o HTTPS sia impostato nel criterio del firewall per la LIF che verrà utilizzata per i servizi Web:



È possibile verificare se un firewall è attivato utilizzando `system services firewall show` comando.

- a. Per verificare che HTTP o HTTPS sia impostato nel criterio firewall, utilizzare `system services firewall policy show` comando.

Impostare `-service` del parametro `system services firewall policy create` comando a `http` oppure `https` per consentire al criterio di supportare l'accesso web.

- b. Per verificare che il criterio firewall che supporta HTTP o HTTPS sia associato al LIF che fornisce servizi Web, utilizzare `network interface show` con il `-firewall-policy` parametro.

Si utilizza `network interface modify` con il `-firewall-policy` Parametro per attivare la policy firewall per una LIF.

2. Per configurare il motore del protocollo Web a livello di cluster e rendere accessibile il contenuto del servizio Web, utilizzare `system services web modify` comando.
3. Se si prevede di utilizzare servizi web sicuri (HTTPS), abilitare SSL e fornire informazioni sul certificato digitale per il cluster o SVM utilizzando `security ssl modify` comando.
4. Per attivare un servizio Web per il cluster o SVM, utilizzare `vserver services web modify` comando.

Ripetere questo passaggio per ogni servizio che si desidera attivare per il cluster o SVM.

5. Per autorizzare un ruolo ad accedere ai servizi Web sul cluster o SVM, utilizzare `vserver services web access create` comando.

Il ruolo a cui si concede l'accesso deve già esistere. È possibile visualizzare i ruoli esistenti utilizzando `security login role show` o creare nuovi ruoli utilizzando `security login role create` comando.

6. Per un ruolo autorizzato ad accedere a un servizio Web, verificare che anche i relativi utenti siano configurati con il metodo di accesso corretto controllando l'output di `security login show` comando.

Per accedere al servizio Web API di ONTAP (`ontapi`), un utente deve essere configurato con `ontapi` metodo di accesso. Per accedere a tutti gli altri servizi Web, è necessario configurare un utente con `http` metodo di accesso.



Si utilizza `security login create` per aggiungere un metodo di accesso per un utente.

Comandi per la gestione dei servizi Web

Si utilizza `vserver services web` Comandi per gestire la disponibilità dei servizi Web

per il cluster o una macchina virtuale di storage (SVM). Si utilizza `vserver services web access` comandi per controllare l'accesso di un ruolo a un servizio web.

Se si desidera...	Utilizzare questo comando...
Configurare un servizio Web per il cluster o anSVM: <ul style="list-style-type: none">• Attivare o disattivare un servizio Web• Specificare se è possibile utilizzare solo HTTPS per accedere a un servizio Web	<code>vserver services web modify</code>
Visualizzare la configurazione e la disponibilità dei servizi Web per il cluster o anSVM	<code>vserver services web show</code>
Autorizzare un ruolo ad accedere a un servizio Web sul cluster o su una SVM	<code>vserver services web access create</code>
Visualizzare i ruoli autorizzati ad accedere ai servizi Web sul cluster o su una SVM	<code>vserver services web access show</code>
Impedire a un ruolo di accedere a un servizio Web sul cluster o su una SVM	<code>vserver services web access delete</code>

Informazioni correlate

["Comandi di ONTAP 9"](#)

Comandi per la gestione dei punti di montaggio sui nodi

Il `spi` il servizio web crea automaticamente un punto di montaggio da un nodo al volume root di un altro nodo su richiesta di accesso ai file di log o ai file core del nodo. Sebbene non sia necessario gestire manualmente i punti di montaggio, è possibile farlo utilizzando `system node root-mount` comandi.

Se si desidera...	Utilizzare questo comando...
Creare manualmente un punto di montaggio da un nodo al volume root di un altro nodo	<code>system node root-mount create</code> Può esistere un solo punto di montaggio da un nodo all'altro.
Visualizzare i punti di montaggio esistenti sui nodi del cluster, incluso l'ora in cui è stato creato un punto di montaggio e il relativo stato corrente	<code>system node root-mount show</code>
Eliminare un punto di montaggio da un nodo al volume root di un altro nodo e forzare la chiusura delle connessioni al punto di montaggio	<code>system node root-mount delete</code>

Informazioni correlate

Gestire SSL

Il protocollo SSL migliora la sicurezza dell'accesso web utilizzando un certificato digitale per stabilire una connessione crittografata tra un server web e un browser.

È possibile gestire SSL per il cluster o una macchina virtuale di storage (SVM) nei seguenti modi:

- Abilitazione di SSL
- Generazione e installazione di un certificato digitale e associazione con il cluster o SVM
- Visualizzazione della configurazione SSL per verificare se SSL è stato attivato e, se disponibile, il nome del certificato SSL
- Impostazione di policy firewall per il cluster o SVM, in modo che le richieste di accesso Web possano essere inoltrate
- Definizione delle versioni SSL utilizzabili
- Limitazione dell'accesso solo alle richieste HTTPS per un servizio Web

Comandi per la gestione di SSL




Si utilizza `security ssl` Comandi per gestire il protocollo SSL per la cluster ora storage virtual machine (SVM).


Se si desidera...	Utilizzare questo comando...
Abilitare SSL per il cluster oranSVM e associare un certificato digitale	<code>security ssl modify</code>
Visualizzare la configurazione SSL e il nome del certificato per il cluster oranSVM	<code>security ssl show</code>


Risolvere i problemi di accesso al servizio Web

Gli errori di configurazione causano problemi di accesso al servizio Web. È possibile risolvere gli errori assicurandosi che LIF, policy firewall, motore del protocollo web, servizi web, certificati digitali, e l'autorizzazione all'accesso dell'utente sono tutte configurate correttamente.

La seguente tabella consente di identificare e risolvere gli errori di configurazione del servizio Web:

Questo problema di accesso...	Si verifica a causa di questo errore di configurazione...	Per risolvere l'errore...
<p>Il browser Web restituisce un <code>unable to connect</code> oppure <code>failure to establish a connection</code> errore quando si tenta di accedere a un servizio web.</p>	<p>La LIF potrebbe non essere configurata correttamente.</p>	<p>Assicurarsi di poter eseguire il ping della LIF che fornisce il servizio Web.</p> <div data-bbox="1166 331 1469 653">  <p>Si utilizza <code>network ping</code> Comando per eseguire il ping di una LIF. Per informazioni sulla configurazione di rete, consultare la <i>Guida alla gestione di rete</i>.</p> </div>
<p>Il firewall potrebbe non essere configurato correttamente.</p>	<p>Assicurarsi che un criterio firewall sia impostato per supportare HTTP o HTTPS e che il criterio sia assegnato alla LIF che fornisce il servizio Web.</p> <div data-bbox="621 1104 1000 1346">  <p>Si utilizza <code>system services firewall policy</code> comandi per gestire le policy firewall. Si utilizza <code>network interface modify</code> con il <code>-firewall -policy</code> Parametro per associare un criterio a un LIF.</p> </div>	<p>Il motore del protocollo Web potrebbe essere disattivato.</p>
<p>Assicurarsi che il motore dei protocolli Web sia abilitato in modo da poter accedere ai servizi Web.</p> <div data-bbox="167 1623 532 1759">  <p>Si utilizza <code>system services web</code> comandi per gestire il motore del protocollo web per il cluster.</p> </div>	<p>Il browser Web restituisce un <code>not found</code> errore quando si tenta di accedere a un servizio web.</p>	<p>Il servizio Web potrebbe essere disattivato.</p>

Questo problema di accesso...	Si verifica a causa di questo errore di configurazione...	Per risolvere l'errore...
<p>Assicurarsi che ogni servizio Web a cui si desidera consentire l'accesso sia attivato singolarmente.</p> <div data-bbox="167 394 220 451">  </div> <p>Si utilizza <code>vserver services web modify</code> per abilitare un servizio web per l'accesso.</p>	<p>Il browser Web non riesce ad accedere a un servizio Web con il nome account e la password dell'utente.</p>	<p>L'utente non può essere autenticato, il metodo di accesso non è corretto o non è autorizzato ad accedere al servizio Web.</p>
<p>Assicurarsi che l'account utente esista e sia configurato con il metodo di accesso e di autenticazione corretti. Inoltre, assicurarsi che il ruolo dell'utente sia autorizzato ad accedere al servizio Web.</p> <div data-bbox="167 1192 220 1249">  </div> <p>Si utilizza <code>security login</code> comandi per gestire gli account utente, i relativi metodi di accesso e i metodi di autenticazione. L'accesso al servizio Web API di ONTAP richiede <code>ontapi</code> metodo di accesso. L'accesso a tutti gli altri servizi Web richiede <code>http</code> metodo di accesso. Si utilizza <code>vserver services web access</code> comandi per gestire l'accesso di un ruolo a un servizio web.</p>	<p>Si effettua la connessione al servizio Web con HTTPS e il browser Web indica che la connessione è stata interrotta.</p>	<p>È possibile che SSL non sia abilitato sul cluster o sulla SVM (Storage Virtual Machine) che fornisce il servizio Web.</p>

Questo problema di accesso...	Si verifica a causa di questo errore di configurazione...	Per risolvere l'errore...
<p>Assicurarsi che il cluster o la SVM abbia abilitato SSL e che il certificato digitale sia valido.</p> <div>  <p>Si utilizza <code>security ssl</code> Comandi per gestire la configurazione SSL per i server HTTP e il <code>security certificate show</code> per visualizzare le informazioni del certificato digitale.</p> </div>	<p>La connessione al servizio Web viene stabilita con HTTPS e il browser Web indica che la connessione non è attendibile.</p>	<p>È possibile che si stia utilizzando un certificato digitale autofirmato.</p>

Verificare l'identità dei server remoti utilizzando i certificati

Verificare l'identità dei server remoti utilizzando la panoramica dei certificati

ONTAP supporta le funzionalità dei certificati di sicurezza per verificare l'identità dei server remoti.

Il software ONTAP consente connessioni sicure utilizzando le seguenti funzionalità e protocolli di certificazione digitale:

- Il protocollo OCSP (Online Certificate Status Protocol) convalida lo stato delle richieste di certificati digitali dai servizi ONTAP utilizzando connessioni SSL e TLS (Transport Layer Security). Questa funzione è disattivata per impostazione predefinita.
- Il software ONTAP include un set predefinito di certificati root attendibili.
- I certificati KMIP (Key Management Interoperability Protocol) consentono l'autenticazione reciproca di un cluster e di un server KMIP.

Verificare che i certificati digitali siano validi utilizzando OCSP

A partire da ONTAP 9.2, il protocollo OCSP (Online Certificate Status Protocol) consente alle applicazioni ONTAP che utilizzano le comunicazioni TLS (Transport Layer Security) di ricevere lo stato del certificato digitale quando OCSP è attivato. È possibile attivare o disattivare i controlli dello stato dei certificati OCSP per applicazioni specifiche in qualsiasi momento. Per impostazione predefinita, il controllo dello stato del certificato OCSP è disattivato.

Di cosa hai bisogno

Per eseguire questa attività, è necessario disporre di un accesso avanzato a livello di privilegi.

A proposito di questa attività

OCSP supporta le seguenti applicazioni:

- AutoSupport
- Sistema di gestione degli eventi (EMS)
- LDAP su TLS
- Protocollo KMIP (Key Management Interoperability Protocol)
- Registrazione dell'audit
- FabricPool
- SSH (a partire da ONTAP 9.13.1)

Fasi

1. Impostare il livello di privilegio su Advanced (avanzato): `set -privilege advanced`.
2. Per attivare o disattivare i controlli dello stato dei certificati OCSP per applicazioni ONTAP specifiche, utilizzare il comando appropriato.

Se si desidera che lo stato del certificato OCSP verifichi che alcune applicazioni siano...	Utilizzare il comando...
Attivato	<code>security config ocsp enable -app app name</code>
Disattivato	<code>security config ocsp disable -app app name</code>

Il seguente comando abilita il supporto OCSP per AutoSupport e EMS.

```
cluster::*> security config ocsp enable -app asup,ems
```

Quando OCSP è attivato, l'applicazione riceve una delle seguenti risposte:

- Buono - il certificato è valido e la comunicazione procede.
 - Revocato - il certificato viene considerato permanentemente come non attendibile dall'autorità di certificazione di emissione e la comunicazione non riesce.
 - Sconosciuto - il server non dispone di informazioni sullo stato del certificato e la comunicazione non riesce.
 - Le informazioni del server OCSP non sono presenti nel certificato - il server agisce come se OCSP sia disattivato e continui con la comunicazione TLS, ma non si verifica alcun controllo dello stato.
 - Nessuna risposta dal server OCSP - l'applicazione non riesce a procedere.
3. Per attivare o disattivare i controlli dello stato dei certificati OCSP per tutte le applicazioni che utilizzano le comunicazioni TLS, utilizzare il comando appropriato.

Se si desidera che lo stato del certificato OCSP verifichi che tutte le applicazioni siano...	Utilizzare il comando...
Attivato	<pre>security config ocsf enable</pre> <pre>-app all</pre>
Disattivato	<pre>security config ocsf disable</pre> <pre>-app all</pre>

Quando questa opzione è attivata, tutte le applicazioni ricevono una risposta firmata che indica che il certificato specificato è valido, revocato o sconosciuto. In caso di certificato revocato, l'applicazione non potrà procedere. Se l'applicazione non riesce a ricevere una risposta dal server OCSP o se il server non è raggiungibile, l'applicazione non potrà procedere.

4. Utilizzare `security config ocsf show` Per visualizzare tutte le applicazioni che supportano OCSP e il relativo stato di supporto.

```
cluster::*> security config ocsf show
Application                                OCSP Enabled?
-----
autosupport                                false
audit_log                                  false
fabricpool                                 false
ems                                         false
kmip                                        false
ldap_ad                                    true
ldap_nis_namemap                           true
ssh                                         true

8 entries were displayed.
```

Visualizza i certificati predefiniti per le applicazioni basate su TLS

A partire da ONTAP 9.2, ONTAP fornisce un set predefinito di certificati root attendibili per le applicazioni ONTAP che utilizzano TLS (Transport Layer Security).

Di cosa hai bisogno

I certificati predefiniti vengono installati solo sulla SVM amministrativa durante la creazione o durante un aggiornamento a ONTAP 9.2.

A proposito di questa attività

Le applicazioni correnti che agiscono come client e richiedono la convalida dei certificati sono AutoSupport, EMS, LDAP, registrazione degli audit, FabricPool, E KMIP.

Quando i certificati scadono, viene richiamato un messaggio EMS che richiede all'utente di eliminarli. I

certificati predefiniti possono essere eliminati solo al livello di privilegio avanzato.



L'eliminazione dei certificati predefiniti potrebbe causare il mancato funzionamento di alcune applicazioni ONTAP (ad esempio, AutoSupport e registrazione audit).

Fase

1. È possibile visualizzare i certificati predefiniti installati sulla SVM amministrativa utilizzando il comando `show` del certificato di protezione:

`security certificate show -vserver -type server-ca`

```
fas2552-2n-abc-3::*> security certificate show -vserver fas2552-2n-abc-3
-type server-ca
Vserver      Serial Number  Common Name                                     Type
-----
fas2552-2n-abc-3
              01              AAACertificateServices
server-ca
Certificate Authority: AAA Certificate Services
Expiration Date: Sun Dec 31 18:59:59 2028
```

Autenticare reciprocamente il cluster e un server KMIP

Autenticazione reciproca del cluster e panoramica di un server KMIP

L'autenticazione reciproca del cluster e di un gestore di chiavi esterno, ad esempio un server KMIP (Key Management Interoperability Protocol), consente al gestore di chiavi di comunicare con il cluster utilizzando KMIP su SSL. Ciò avviene quando un'applicazione o una determinata funzionalità (ad esempio, la funzionalità Storage Encryption) richiede chiavi sicure per fornire un accesso sicuro ai dati.

Generare una richiesta di firma del certificato per il cluster

È possibile utilizzare il certificato di protezione `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.

Di cosa hai bisogno

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
```

Per la sintassi completa dei comandi, vedere le pagine man.

Il seguente comando crea una CSR con una chiave privata a 2,048 bit generata dalla funzione di hashing SHA256 per l'utilizzo da parte del gruppo Software nel reparto IT di una società il cui nome comune personalizzato è server1.companyname.com, con sede a Sunnyvale, California, USA. L'indirizzo e-mail dell'amministratore del contatto SVM è web@example.com. Il sistema visualizza la CSR e la chiave privata nell'output.

```
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  
CSqGSIB3DQEJARYAMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAPXFanNoJApt1nzS  
xOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJbmXuj6U3alwoUsb13wfEvQnHVFNCi  
2ninsJ8CAwEAAaAAMA0GCSqGSIB3DQEBCwUAA0EA6EagLfso5+4g+ejiRKKTUPQO  
UqOUEoKuvxhOvPC2w7b//fNSFsFHvXloqEOhYECn/NX9h8mbphCoM5YZ4OfnKw==  
-----END CERTIFICATE REQUEST-----  
Private Key :  
24 | Administrator Authentication and RBAC  
-----BEGIN RSA PRIVATE KEY-----  
MIIBOwIBAAJBAPXFanNoJApt1nzSxOcxixqImRRGZCR7tVmTYyqPSuTvfVtWdJb  
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, quindi 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 per il cluster

Per consentire a un server SSL di autenticare la macchina virtuale del cluster o dello

storage (SVM) come client SSL, installare un certificato digitale con il tipo di client sul cluster o SVM. Quindi, fornire il certificato client-ca all'amministratore del server SSL per l'installazione sul server.

Di cosa hai bisogno

È necessario aver già installato il certificato root del server SSL sul cluster o SVM con `server-ca` tipo di certificato.

Fasi

1. Per utilizzare un certificato digitale autofirmato per l'autenticazione del client, utilizzare `security certificate create` con il `type client` parametro.
2. Per utilizzare un certificato digitale con firma CA per l'autenticazione del client, attenersi alla seguente procedura:
 - a. Generare una richiesta di firma del certificato digitale (CSR) utilizzando il certificato di sicurezza `generate-csr` comando.

ONTAP visualizza l'output CSR, che include una richiesta di certificato e una chiave privata, e ricorda di copiare l'output in un file per riferimenti futuri.
 - b. Inviare la richiesta di certificato dall'output CSR in un formato elettronico (ad esempio un'e-mail) a una CA attendibile per la firma.

Conservare una copia della chiave privata e del certificato firmato dalla CA per riferimenti futuri.

Una volta elaborata la richiesta, la CA invia il certificato digitale firmato.

- a. Installare il certificato firmato dalla CA utilizzando `security certificate install` con il `-type client` parametro.
- b. Quando richiesto, immettere il certificato e la chiave privata, quindi premere **Invio**.
- c. Quando richiesto, immettere eventuali certificati root o intermedi aggiuntivi, quindi premere **Invio**.

Se una catena di certificati che inizia dalla CA principale attendibile e termina con il certificato SSL emesso, non dispone dei certificati intermedi, è necessario installare un certificato intermedio sul cluster o sulla SVM. Un certificato intermedio è un certificato subordinato emesso dalla radice attendibile in modo specifico per il rilascio di certificati server di entità finale. Il risultato è una catena di certificati che inizia dalla CA principale attendibile, passa attraverso il certificato intermedio e termina con il certificato SSL emesso.

3. Fornire il `client-ca` Certificato del cluster o SVM all'amministratore del server SSL per l'installazione sul server.

Il comando `show` del certificato di protezione con `-instance e. -type client-ca parameters` (parametri): visualizza `client-ca` informazioni sul certificato.

Installare un certificato client firmato dalla CA per il server KMIP

Il sottotipo di certificato del protocollo KMIP (Key Management Interoperability Protocol) (il parametro `-subtype kmip-cert`), insieme ai tipi `client` e `server-ca`, specifica che il certificato viene utilizzato per l'autenticazione reciproca del cluster e di un gestore di

chiavi esterno, ad esempio un server KMIP.

A proposito di questa attività

Installare un certificato KMIP per autenticare un server KMIP come server SSL nel cluster.

Fasi

1. Utilizzare `security certificate install` con il `-type server-ca` e `-subtype kmip-cert` Parametri per installare un certificato KMIP per il server KMIP.
2. Quando richiesto, immettere il certificato, quindi premere Invio.

ONTAP ricorda di conservare una copia del certificato per riferimenti futuri.

```
cluster1::> security certificate install -type server-ca -subtype kmip-  
cert  
-vserver cluster1
```

Please enter Certificate: Press <Enter> when done

-----BEGIN CERTIFICATE-----

```
MIICPDCCAaUCEDyRMcsf9tAbDpq40ES/Er4wDQYJKoZIhvcNAQEFBQAwXzELMAkG  
2JhucwNhkcV8sEVAbkSdjbCxlRhLQ2pRdKkkirWmnWXbj9T/UWZYB2oK0z5XqcJ  
2HUw19JlYDln1khVdWk/kfVIC0dpImmClr7JyDiGSnoscxlIaU5rfGW/D/xwzoiQ
```

...

-----END CERTIFICATE-----

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

```
cluster1::>
```

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.