



Configurare l'accesso S3 a una SVM

ONTAP 9

NetApp
April 24, 2024

Sommario

- Configurare l'accesso S3 a una SVM. 1
 - Creare una SVM per S3. 1
 - Creare e installare un certificato CA sulla SVM 4
 - Creare una policy sui dati del servizio S3 7
 - Creazione di LIF di dati 8
 - Creazione di LIF intercluster per tiering FabricPool remoto. 10
 - Creare il server archivio oggetti S3 13

Configurare l'accesso S3 a una SVM

Creare una SVM per S3

Sebbene S3 possa coesistere con altri protocolli in una SVM, potrebbe essere necessario creare una nuova SVM per isolare lo spazio dei nomi e il carico di lavoro.

A proposito di questa attività

Se si fornisce solo lo storage a oggetti S3 da una SVM, il server S3 non richiede alcuna configurazione DNS. Tuttavia, se si utilizzano altri protocolli, è possibile configurare il DNS sulla SVM.

Quando si configura l'accesso S3 a una nuova macchina virtuale di storage utilizzando System Manager, viene richiesto di inserire le informazioni relative a certificato e rete e di creare la macchina virtuale di storage e il server di storage a oggetti S3 in una singola operazione.

Esempio 1. Fasi

System Manager

Si consiglia di immettere il nome del server S3 come FQDN (Fully Qualified Domain Name), utilizzato dai client per l'accesso S3. L'FQDN del server S3 non deve iniziare con un nome bucket.

Si consiglia di inserire gli indirizzi IP per i dati del ruolo dell'interfaccia.

Se si utilizza un certificato firmato da una CA esterna, viene richiesto di inserirlo durante questa procedura; è inoltre possibile utilizzare un certificato generato dal sistema.

1. Abilitare S3 su una VM di storage.

- a. Aggiungere una nuova VM di storage: Fare clic su **Storage > Storage VMS**, quindi fare clic su **Add** (Aggiungi).

Se si tratta di un nuovo sistema senza macchine virtuali di storage esistenti, fare clic su **Dashboard > Configure Protocols** (Configura protocolli).

Se si aggiunge un server S3 a una VM di storage esistente: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings** (Impostazioni), quindi fare clic su  Sotto **S3**.

- a. Fare clic su **Enable S3** (attiva S3), quindi immettere il nome del server S3.
- b. Selezionare il tipo di certificato.

Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.

- c. Inserire le interfacce di rete.

2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.
- La chiave segreta non viene visualizzata di nuovo.
 - Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

CLI

1. Verificare che S3 sia concesso in licenza sul cluster:

```
system license show -package s3
```

In caso contrario, contattare il rappresentante commerciale.

2. Creare una SVM:

```
vserver create -vserver <svm_name> -subtype default -rootvolume  
<root_volume_name> -aggregate <aggregate_name> -rootvolume-security  
-style unix -language C.UTF-8 -data-services <data-s3-server>  
-ipSPACE <ipSPACE_name>
```

- Utilizzare l'impostazione UNIX per `-rootvolume-security-style` opzione.
- Utilizzare il C.UTF-8 predefinito `-language` opzione.
- Il `ipSPACE` l'impostazione è facoltativa.

3. Verificare la configurazione e lo stato della SVM appena creata:

```
vserver show -vserver <svm_name>
```

Il `Vserver Operational State` il campo deve visualizzare `running` stato. Se viene visualizzato il `initializing` indica che alcune operazioni intermedie, ad esempio la creazione del volume root, non sono riuscite ed è necessario eliminare la SVM e ricrearla.

Esempi

Il seguente comando crea una SVM per l'accesso ai dati in IPSPACE `ipSPACEA`:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -data-services _data-s3-server_ -ipSPACE ipSPACEA
```

```
[Job 2059] Job succeeded:  
Vserver creation completed
```

Il seguente comando indica che è stata creata una SVM con un volume root di 1 GB, che è stata avviata automaticamente e si trova in `running` stato. Il volume root dispone di un criterio di esportazione predefinito che non include alcuna regola, pertanto il volume root non viene esportato al momento della creazione. Per impostazione predefinita, l'account utente `vsadmin` viene creato e si trova in `locked` stato. Il ruolo `vsadmin` viene assegnato all'account utente `vsadmin` predefinito.

```

cluster-1::> vserver show -vserver svm1.example.com
                                Vserver: svm1.example.com
                                Vserver Type: data
                                Vserver Subtype: default
                                Vserver UUID: b8375669-19b0-11e5-b9d1-
00a0983d9736

                                Root Volume: root_svm1
                                Aggregate: aggr1
                                NIS Domain: -
                                Root Volume Security Style: unix
                                LDAP Client: -
                                Default Volume Language Code: C.UTF-8
                                Snapshot Policy: default
                                Comment:
                                Quota Policy: default
                                List of Aggregates Assigned: -
                                Limit on Maximum Number of Volumes allowed: unlimited
                                Vserver Admin State: running
                                Vserver Operational State: running
                                Vserver Operational State Stopped Reason: -
                                Allowed Protocols: nfs, cifs
                                Disallowed Protocols: -
                                QoS Policy Group: -
                                Config Lock: false
                                IPspace Name: ipspaceA

```

Creare e installare un certificato CA sulla SVM

Per abilitare il traffico HTTPS dai client S3 alla SVM abilitata per S3, è necessario un certificato CA (Certificate Authority).

A proposito di questa attività

Sebbene sia possibile configurare un server S3 in modo che utilizzi solo HTTP e sebbene sia possibile configurare i client senza un requisito di certificato CA, è consigliabile proteggere il traffico HTTPS ai server ONTAP S3 con un certificato CA.

Un certificato CA non è necessario per un caso di utilizzo del tiering locale, in cui il traffico IP passa solo attraverso le LIF del cluster.

Le istruzioni di questa procedura consentono di creare e installare un certificato autofirmato ONTAP. Sono supportati anche i certificati CA di fornitori terzi; per ulteriori informazioni, consultare la documentazione di autenticazione dell'amministratore.

["Autenticazione amministratore e RBAC"](#)

Vedere `security certificate` pagine man per ulteriori opzioni di configurazione.

Fasi

1. Creare un certificato digitale autofirmato:

```
security certificate create -vserver svm_name -type root-ca -common-name  
ca_cert_name
```

Il `-type root-ca` L'opzione crea e installa un certificato digitale autofirmato per firmare altri certificati agendo come autorità di certificazione (CA).

Il `-common-name` L'opzione crea il nome dell'autorità di certificazione (CA) di SVM e verrà utilizzata per generare il nome completo del certificato.

La dimensione predefinita del certificato è 2048 bit.

Esempio

```
cluster-1::> security certificate create -vserver svm1.example.com -type  
root-ca -common-name svm1_ca
```

The certificate's generated name for reference:
svm1_ca_159D1587CE21E9D4_svm1_ca

Quando viene visualizzato il nome generato del certificato, assicurarsi di salvarlo per i passaggi successivi di questa procedura.

2. Generare una richiesta di firma del certificato:

```
security certificate generate-csr -common-name s3_server_name  
[additional_options]
```

Il `-common-name` Il parametro per la richiesta di firma deve essere il nome del server S3 (FQDN).

Se lo si desidera, è possibile fornire la posizione e altre informazioni dettagliate sulla SVM.

Viene richiesto di conservare una copia della richiesta di certificato e della chiave privata per riferimenti futuri.

3. Firmare la CSR utilizzando SVM_CA per generare il certificato del server S3:

```
security certificate sign -vserver svm_name -ca ca_cert_name -ca-serial  
ca_cert_serial_number [additional_options]
```

Immettere le opzioni di comando utilizzate nei passaggi precedenti:

- `-ca` — il nome comune della CA immesso nel passaggio 1.
- `-ca-serial` — il numero di serie della CA dal punto 1. Ad esempio, se il nome del certificato CA è svm1_ca_159D1587CE21E9D4_svm1_ca, il numero di serie è 159D1587CE21E9D4.

Per impostazione predefinita, il certificato firmato scadrà tra 365 giorni. È possibile selezionare un altro valore e specificare altri dettagli della firma.

Quando richiesto, copiare e inserire la stringa di richiesta del certificato salvata nel passaggio 2.

Viene visualizzato un certificato firmato; salvarlo per un utilizzo successivo.

4. Installare il certificato firmato sulla SVM abilitata per S3:

```
security certificate install -type server -vserver svm_name
```

Quando richiesto, inserire il certificato e la chiave privata.

Se si desidera inserire una catena di certificati, è possibile immettere i certificati intermedi.

Quando vengono visualizzate la chiave privata e il certificato digitale firmato dalla CA, salvarle per riferimenti futuri.

5. Ottenere il certificato della chiave pubblica:

```
security certificate show -vserver svm_name -common-name ca_cert_name -type  
root-ca -instance
```

Salvare il certificato della chiave pubblica per una configurazione successiva lato client.

Esempio


```

cluster-1::> security certificate show -vserver svm1.example.com -common
-name svm1_ca -type root-ca -instance

                Name of Vserver: svm1.example.com
                FQDN or Custom Common Name: svm1_ca
                Serial Number of Certificate: 159D1587CE21E9D4
                Certificate Authority: svm1_ca
                Type of Certificate: root-ca
                (DEPRECATED)-Certificate Subtype: -
                Unique Certificate Name: svm1_ca_159D1587CE21E9D4_svm1_ca
Size of Requested Certificate in Bits: 2048
                Certificate Start Date: Thu May 09 10:58:39 2020
                Certificate Expiration Date: Fri May 08 10:58:39 2021
                Public Key Certificate: -----BEGIN CERTIFICATE-----
MIIDZ ...==
-----END CERTIFICATE-----

                Country Name: US
                State or Province Name:
                Locality Name:
                Organization Name:
                Organization Unit:
Contact Administrator's Email Address:
                Protocol: SSL
                Hashing Function: SHA256
                Self-Signed Certificate: true
                Is System Internal Certificate: false

```

Creare una policy sui dati del servizio S3

È possibile creare policy di servizio per i dati S3 e i servizi di gestione. Per abilitare il traffico dati S3 su LIF, è necessaria una policy dei dati del servizio S3.

A proposito di questa attività

Se si utilizzano LIF di dati e LIF di intercluster, è necessaria una policy sui dati di servizio S3. Non è necessario se si utilizzano le LIF del cluster per il caso di utilizzo del tiering locale.

Quando viene specificata una policy di servizio per una LIF, questa viene utilizzata per creare un ruolo predefinito, una policy di failover e un elenco di protocolli dati per la LIF.

Sebbene sia possibile configurare più protocolli per SVM e LIFF, è consigliabile che S3 sia l'unico protocollo per la fornitura di dati a oggetti.

Fasi

1. Impostare i privilegi su Advanced (avanzato):

```
set -privilege advanced
```

2. Creare una policy sui dati del servizio:

```
network interface service-policy create -vserver svm_name -policy policy_name  
-services data-core,data-s3-server
```

Il data-core e. data-s3-server I servizi sono gli unici necessari per abilitare ONTAP S3, anche se è possibile includere altri servizi in base alle esigenze.

Creazione di LIF di dati

Se hai creato una nuova SVM, le LIF dedicate create per l'accesso S3 dovrebbero essere le LIF dei dati.

Prima di iniziare

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore up stato.
- Se si intende utilizzare un nome di subnet per assegnare l'indirizzo IP e il valore della maschera di rete per un LIF, la subnet deve già esistere.

Le subnet contengono un pool di indirizzi IP appartenenti alla stessa subnet Layer 3. Vengono creati utilizzando `network subnet create` comando.

- La politica di servizio LIF deve già esistere.

A proposito di questa attività

- È possibile creare LIF IPv4 e IPv6 sulla stessa porta di rete.
- Se nel cluster è presente un numero elevato di LIF, è possibile verificare la capacità LIF supportata dal cluster utilizzando `network interface capacity show` E la capacità LIF supportata su ciascun nodo utilizzando `network interface capacity details show` (a livello di privilegi avanzati).
- Se si abilita il tiering remoto della capacità FabricPool (cloud), è necessario configurare anche le LIF intercluster.

Fasi

1. Creare una LIF:

```
network interface create -vserver svm_name -lif lif_name -service-policy  
service_policy_names -home-node node_name -home-port port_name {-address  
IP_address -netmask IP_address | -subnet-name subnet_name} -firewall-policy  
data -auto-revert {true|false}
```

- -home-node È il nodo a cui la LIF restituisce quando `network interface revert` Viene eseguito sul LIF.

È inoltre possibile specificare se il LIF deve ripristinare automaticamente il nodo home e la porta home con `-auto-revert` opzione.

- -home-port È la porta fisica o logica a cui LIF restituisce quando `network interface revert` Viene eseguito sul LIF.
- È possibile specificare un indirizzo IP con `-address` e. `-netmask` oppure attivare l'allocazione da una subnet con `-subnet_name` opzione.

- Quando si utilizza una subnet per fornire l'indirizzo IP e la maschera di rete, se la subnet è stata definita con un gateway, quando viene creata una LIF che utilizza tale subnet viene automaticamente aggiunto un percorso predefinito a tale gateway.
- Se si assegnano gli indirizzi IP manualmente (senza utilizzare una subnet), potrebbe essere necessario configurare un percorso predefinito a un gateway se sono presenti client o controller di dominio su una subnet IP diversa. Il `network route create` La pagina man contiene informazioni sulla creazione di un percorso statico all'interno di una SVM.
- Per `-firewall-policy` utilizzare lo stesso valore predefinito `data` Come ruolo LIF.

Se lo si desidera, è possibile creare e aggiungere un criterio firewall personalizzato in un secondo momento.



A partire da ONTAP 9.10.1, le policy firewall sono obsolete e completamente sostituite con le policy di servizio LIF. Per ulteriori informazioni, vedere ["Configurare le policy firewall per le LIF"](#).

- `-auto-revert` Consente di specificare se un LIF dati viene automaticamente reimpostato sul proprio nodo principale in circostanze come l'avvio, le modifiche allo stato del database di gestione o quando viene stabilita la connessione di rete. L'impostazione predefinita è `false`, ma è possibile impostarlo su `false` in base alle policy di gestione della rete nel proprio ambiente.
- Il `-service-policy` l'opzione specifica la policy creata per i dati e i servizi di gestione e qualsiasi altra policy necessaria.

2. Se si desidera assegnare un indirizzo IPv6 in `-address` opzione:

- Utilizzare `network ndp prefix show` Per visualizzare l'elenco dei prefissi RA appresi su varie interfacce.

Il `network ndp prefix show` il comando è disponibile a livello di privilegio avanzato.

- Utilizzare il formato `prefix:id` Per costruire manualmente l'indirizzo IPv6.

`prefix` è il prefisso appreso sulle varie interfacce.

Per derivare il `id`, scegliere un numero esadecimale casuale a 64 bit.

- Verificare che la LIF sia stata creata correttamente utilizzando `network interface show` comando.
- Verificare che l'indirizzo IP configurato sia raggiungibile:

Per verificare un...	Utilizzare...
Indirizzo IPv4	<code>network ping</code>
Indirizzo IPv6	<code>network ping6</code>

Esempi

Il comando seguente mostra come creare una LIF di dati S3 assegnata a `my-S3-policy` politica di servizio:

```
network interface create -vserver svml.example.com -lif lif2 -home-node
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

Il seguente comando mostra tutti i LIF nel cluster-1. Data LIF datalif1 e datalif3 sono configurati con indirizzi IPv4 e datalif4 è configurato con un indirizzo IPv6:

```
cluster-1::> network interface show
```

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Is Port
Home					
-----	-----	-----	-----	-----	-----

cluster-1					
	cluster_mgmt	up/up	192.0.2.3/24	node-1	e1a
true					
node-1					
	clus1	up/up	192.0.2.12/24	node-1	e0a
true					
	clus2	up/up	192.0.2.13/24	node-1	e0b
true					
	mgmt1	up/up	192.0.2.68/24	node-1	e1a
true					
node-2					
	clus1	up/up	192.0.2.14/24	node-2	e0a
true					
	clus2	up/up	192.0.2.15/24	node-2	e0b
true					
	mgmt1	up/up	192.0.2.69/24	node-2	e1a
true					
vs1.example.com					
	datalif1	up/down	192.0.2.145/30	node-1	e1c
true					
vs3.example.com					
	datalif3	up/up	192.0.2.146/30	node-2	e0c
true					
	datalif4	up/up	2001::2/64	node-2	e0c
true					

5 entries were displayed.

Creazione di LIF intercluster per tiering FabricPool remoto

Se si abilita il tiering della capacità FabricPool remota (cloud) utilizzando ONTAP S3, è necessario configurare le LIF tra cluster. È possibile configurare le LIF di intercluster sulle

porte condivise con la rete dati. In questo modo si riduce il numero di porte necessarie per la rete tra cluster.

Prima di iniziare

- La porta di rete fisica o logica sottostante deve essere stata configurata per l'amministratore `up` stato.
- La politica di servizio LIF deve già esistere.

A proposito di questa attività

Le LIF intercluster non sono richieste per il tiering del pool di fabric locale o per la fornitura di applicazioni S3 esterne.

Fasi

1. Elencare le porte nel cluster:

```
network port show
```

L'esempio seguente mostra le porte di rete in `cluster01`:

```
cluster01::> network port show
```

(Mbps)					Speed	
Node	Port	IPspace	Broadcast Domain	Link	MTU	Admin/Oper

cluster01-01						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000
cluster01-02						
	e0a	Cluster	Cluster	up	1500	auto/1000
	e0b	Cluster	Cluster	up	1500	auto/1000
	e0c	Default	Default	up	1500	auto/1000
	e0d	Default	Default	up	1500	auto/1000

2. Creazione di LIF intercluster sulla SVM di sistema:

```
network interface create -vserver Cluster -lif LIF_name -service-policy  
default-intercluster -home-node node -home-port port -address port_IP -netmask  
netmask
```

Nell'esempio seguente vengono create le LIF tra cluster `cluster01_icl01` e `cluster01_icl02`:

```
cluster01::> network interface create -vserver Cluster -lif
cluster01_icl01 -service-
policy default-intercluster -home-node cluster01-01 -home-port e0c
-address 192.168.1.201
-netmask 255.255.255.0

cluster01::> network interface create -vserver Cluster -lif
cluster01_icl02 -service-
policy default-intercluster -home-node cluster01-02 -home-port e0c
-address 192.168.1.202
-netmask 255.255.255.0
```

3. Verificare che le LIF dell'intercluster siano state create:

```
network interface show -service-policy default-intercluster
```

```
cluster01::> network interface show -service-policy default-intercluster
```

Current Is	Logical	Status	Network	Current
Vserver	Interface	Admin/Oper	Address/Mask	Node
Home				Port
-----	-----	-----	-----	-----
-----	-----	-----	-----	-----
cluster01	cluster01_icl01	up/up	192.168.1.201/24	cluster01-01 e0c
true	cluster01_icl02	up/up	192.168.1.202/24	cluster01-02 e0c
true				

4. Verificare che le LIF dell'intercluster siano ridondanti:

```
network interface show -service-policy default-intercluster -failover
```

L'esempio seguente mostra che le LIF dell'intercluster cluster01_icl01 e cluster01_icl02 su e0c viene eseguito il failover della porta su e0d porta.

```
cluster01::> network interface show -service-policy default-intercluster
-failover
```

Vserver	Logical Interface	Home Node:Port	Failover Policy	Failover Group
cluster01				
	cluster01_icl01	cluster01-01:e0c	local-only	
192.168.1.201/24				
			Failover Targets: cluster01-01:e0c,	
			cluster01-01:e0d	
	cluster01_icl02	cluster01-02:e0c	local-only	
192.168.1.201/24				
			Failover Targets: cluster01-02:e0c,	
			cluster01-02:e0d	

Creare il server archivio oggetti S3

Il server di archiviazione a oggetti ONTAP gestisce i dati come oggetti S3, invece dello storage a blocchi o file fornito dai server NAS e SAN ONTAP.

Prima di iniziare

Si consiglia di immettere il nome del server S3 come FQDN (Fully Qualified Domain Name), utilizzato dai client per l'accesso S3. L'FQDN non deve iniziare con un nome bucket.

È necessario disporre di un certificato CA autofirmato (creato nei passaggi precedenti) o di un certificato firmato da un vendor CA esterno. Un certificato CA non è necessario per un caso di utilizzo del tiering locale, in cui il traffico IP passa solo attraverso le LIF del cluster.

A proposito di questa attività

Quando viene creato un server archivio oggetti, viene creato un utente root con UID 0. Per questo utente root non viene generata alcuna chiave di accesso o chiave segreta. L'amministratore di ONTAP deve eseguire `object-store-server users regenerate-keys` per impostare la chiave di accesso e la chiave segreta per questo utente.



Come Best practice NetApp, non utilizzare questo utente root. Qualsiasi applicazione client che utilizza la chiave di accesso o la chiave segreta dell'utente root ha accesso completo a tutti i bucket e gli oggetti nell'archivio di oggetti.

Vedere `vserver object-store-server` pagine man per ulteriori opzioni di configurazione e visualizzazione.


Esempio 2. Fasi

System Manager

Utilizzare questa procedura se si aggiunge un server S3 a una VM di storage esistente. Per aggiungere un server S3 a una nuova VM di storage, vedere ["Creare una SVM di storage per S3"](#).

Si consiglia di inserire gli indirizzi IP per i dati del ruolo dell'interfaccia.

1. Abilitare S3 su una VM di storage esistente.

- Selezionare la VM di storage: Fare clic su **Storage > Storage VM**, selezionare una VM di storage, fare clic su **Settings**, quindi fare clic su  Sotto **S3**.
- Fare clic su **Enable S3** (attiva S3), quindi immettere il nome del server S3.
- Selezionare il tipo di certificato.

Se si seleziona un certificato generato dal sistema o uno dei propri, questo sarà necessario per l'accesso del client.

d. Inserire le interfacce di rete.

2. Se è stato selezionato il certificato generato dal sistema, le informazioni del certificato vengono visualizzate quando viene confermata la creazione della nuova VM di storage. Fare clic su **Download** e salvarlo per accedere al client.

- La chiave segreta non viene visualizzata di nuovo.
- Se sono necessarie nuovamente le informazioni del certificato: Fare clic su **Storage > Storage VMS**, selezionare la VM di storage e fare clic su **Settings** (Impostazioni).

CLI

1. Creare il server S3:

```
vserver object-store-server create -vserver svm_name -object-store-server  
s3_server_fqdn -certificate-name server_certificate_name -comment text  
[additional_options]
```

È possibile specificare opzioni aggiuntive durante la creazione del server S3 o in qualsiasi momento successivo.

- In caso di configurazione del tiering locale, il nome della SVM può essere un nome di una SVM dati o di una SVM di sistema (cluster).
- Il nome del certificato deve essere il nome del certificato del server (certificato dell'utente finale o del foglio) e non il certificato della CA del server (certificato della CA intermedia o di origine).
- HTTPS è attivato per impostazione predefinita sulla porta 443. È possibile modificare il numero di porta con `-secure-listener-port` opzione.

Quando HTTPS è attivato, i certificati CA sono necessari per la corretta integrazione con SSL/TLS.

- HTTP è disattivato per impostazione predefinita. Quando questa opzione è attivata, il server è in attesa sulla porta 80. È possibile attivarlo con `-is-http-enabled` oppure modificare il numero di porta con il `-listener-port` opzione.

Quando HTTP è attivato, la richiesta e le risposte vengono inviate in rete in formato non

crittografato.

2. Verificare che S3 sia configurato:

```
vserver object-store-server show
```

Esempio

Questo comando verifica i valori di configurazione di tutti i server di storage a oggetti:

```
cluster1::> vserver object-store-server show
```

```
Vserver: vs1
```

```
Object Store Server Name: s3.example.com
```

```
Administrative State: up
```

```
Listener Port For HTTP: 80
```

```
Secure Listener Port For HTTPS: 443
```

```
HTTP Enabled: false
```

```
HTTPS Enabled: true
```

```
Certificate for HTTPS Connections: svm1_ca
```

```
Comment: Server comment
```

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.