



Configurez l'accès S3 à un SVM

ONTAP 9

NetApp
April 24, 2024

Sommaire

- Configurez l'accès S3 à un SVM 1
 - Création d'un SVM pour S3 1
 - Créer et installer un certificat d'autorité de certification sur le SVM. 4
 - Création d'une règle de données de service S3 7
 - Création de LIF de données. 8
 - Création des LIFs intercluster pour le Tiering distant des FabricPool 11
 - Créez le serveur de magasin d'objets S3 13

Configurez l'accès S3 à un SVM

Création d'un SVM pour S3

Bien que S3 puisse coexister avec d'autres protocoles dans un SVM, il peut être nécessaire de créer un nouveau SVM afin d'isoler le namespace et les workloads.

Description de la tâche

Si vous fournissez uniquement le stockage objet S3 à partir d'un SVM, le serveur S3 ne nécessite aucune configuration DNS. Toutefois, il peut être nécessaire de configurer le DNS sur le SVM si d'autres protocoles sont utilisés.

Lorsque vous configurez l'accès S3 à une nouvelle machine virtuelle de stockage à l'aide de System Manager, vous êtes invité à saisir des informations de certificat et de mise en réseau, et la machine virtuelle de stockage et le serveur de stockage objet S3 sont créés en une seule opération.

Exemple 1. Étapes

System Manager

Vous devez préparer à saisir le nom du serveur S3 en tant que nom de domaine complet (FQDN) que les clients utiliseront pour l'accès S3. Le FQDN du serveur S3 ne doit pas commencer par un nom de compartiment.


Vous devez être prêt à saisir des adresses IP pour les données de rôle d'interface.

Si vous utilisez un certificat signé par une autorité de certification externe, vous serez invité à le saisir au cours de cette procédure ; vous avez également la possibilité d'utiliser un certificat généré par le système.

1. Activez S3 sur une VM de stockage.

- a. Ajouter une nouvelle machine virtuelle de stockage : cliquez sur **stockage > machines virtuelles de stockage**, puis sur **Ajouter**.

S'il s'agit d'un nouveau système sans machines virtuelles de stockage existantes : cliquez sur **Tableau de bord > configurer les protocoles**.

Si vous ajoutez un serveur S3 à une machine virtuelle de stockage existante : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sur  Sous **S3**.

- a. Cliquez sur **Activer S3**, puis entrez le nom du serveur S3.
- b. Sélectionnez le type de certificat.

Que vous sélectionniez un certificat généré par le système ou l'un de vos propres certificats, il sera nécessaire d'accéder au client.

- c. Saisissez les interfaces réseau.

2. Si vous avez sélectionné le certificat généré par le système, les informations de certificat s'affichent lorsque la création de la nouvelle machine virtuelle de stockage est confirmée. Cliquez sur **Download** et enregistrez-le pour accéder au client.

- La clé secrète ne s'affiche plus.
- Si vous avez besoin de nouveau des informations de certificat : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.

CLI

1. Vérifiez que la licence S3 est disponible sur votre cluster :

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

Si ce n'est pas le cas, contactez votre représentant commercial.

2. Création d'un 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>
```

- Utilisez le paramètre UNIX pour le `-rootvolume-security-style` option.
- Utilisez le paramètre par défaut C.UTF-8 `-language` option.
- Le `ipSPACE` le paramètre est facultatif.

3. Vérifier la configuration et le statut du nouveau SVM :

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

Le `Vserver Operational State` le champ doit afficher `running` état. S'il affiche le `initializing` État, cela signifie qu'une opération intermédiaire telle que la création du volume root a échoué, et vous devez supprimer la SVM et la recréer.

Exemples

La commande suivante crée un SVM pour l'accès aux données dans l'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
```

La commande suivante montre qu'un SVM a été créé avec un volume root de 1 Go, il a été démarré automatiquement et qu'il est en `running` état. Le volume root dispose d'une export policy par défaut qui n'inclut aucune règle et qui ne précise donc pas l'exportation du volume root au moment de sa création. Par défaut, le compte utilisateur `vsadmin` est créé et est dans le `locked` état. Le rôle `vsadmin` est attribué au compte utilisateur par défaut `vsadmin`.

```

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

```

Créer et installer un certificat d'autorité de certification sur le SVM

Un certificat d'autorité de certification (CA) est nécessaire pour activer le trafic HTTPS des clients S3 vers le SVM compatible avec S3.

Description de la tâche

Bien qu'il soit possible de configurer un serveur S3 pour utiliser uniquement le protocole HTTP, et bien qu'il soit possible de configurer des clients sans exigence de certificat d'autorité de certification, il est recommandé de sécuriser le trafic HTTPS vers des serveurs ONTAP S3 avec un certificat d'autorité de certification.

Un certificat CA n'est pas nécessaire pour une utilisation de hiérarchisation locale, où le trafic IP transite uniquement par les LIFs de cluster.

Les instructions de cette procédure créent et installent un certificat auto-signé ONTAP. Les certificats CA de fournisseurs tiers sont également pris en charge ; consultez la documentation relative à l'authentification de l'administrateur pour plus d'informations.

["Authentification de l'administrateur et RBAC"](#)

Voir la `security certificate` pages de manuel pour les options de configuration supplémentaires.

Étapes

1. Créer un certificat numérique auto-signé :

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

Le `-type root-ca` Option crée et installe un certificat numérique auto-signé pour signer d'autres certificats en agissant comme autorité de certification (CA).

Le `-common-name` Option crée le nom de l'autorité de certification du SVM et sera utilisé lors de la génération du nom complet du certificat.

La taille du certificat par défaut est de 2048 bits.

Exemple

```
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
```

Lorsque le nom généré du certificat est affiché, veuillez à l'enregistrer pour les étapes ultérieures de cette procédure.

2. Générer une demande de signature de certificat :

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

Le `-common-name` Le paramètre de la demande de signature doit être le nom de serveur S3 (FQDN).

Vous pouvez fournir l'emplacement et d'autres informations détaillées sur la SVM si nécessaire.

Vous êtes invité à conserver une copie de votre demande de certificat et de votre clé privée pour référence ultérieure.

3. Signer la RSC à l'aide de SVM_CA pour générer le certificat du serveur S3 :

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

Entrez les options de commande que vous avez utilisées aux étapes précédentes :

- `-ca` — le nom commun de l'autorité de certification que vous avez saisi à l'étape 1.
- `-ca-serial` — le numéro de série CA de l'étape 1. Par exemple, si le nom du certificat de l'autorité de certification est `svm1_CA_159D1587CE21E9D4_svm1_ca`, le numéro de série est `159D1587CE2E9D4`.

Par défaut, le certificat signé expirera dans 365 jours. Vous pouvez sélectionner une autre valeur et spécifier d'autres détails de signature.

Lorsque vous y êtes invité, copiez et entrez la chaîne de demande de certificat que vous avez enregistrée à l'étape 2.

Un certificat signé s'affiche ; enregistrez-le pour une utilisation ultérieure.

4. Installez le certificat signé sur le SVM compatible S3 :

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

Lorsque vous y êtes invité, entrez le certificat et la clé privée.

Vous avez la possibilité de saisir des certificats intermédiaires si une chaîne de certificats est souhaitée.

Lorsque la clé privée et le certificat numérique signé par l'autorité de certification sont affichés, enregistrez-les pour référence ultérieure.

5. Obtenir le certificat de clé publique :

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

Enregistrez le certificat de clé publique pour une configuration client ultérieure.

Exemple


```

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

```

Création d'une règle de données de service S3

Vous pouvez créer des règles de service pour les données S3 et les services de gestion. Une règle de données de service S3 est nécessaire pour activer le trafic de données S3 sur les LIF.

Description de la tâche

Une politique de données de service S3 est requise si vous utilisez des LIF de données et des LIF intercluster. Il n'est pas nécessaire d'utiliser des LIF de cluster pour la hiérarchisation locale.

Lorsqu'une politique de services est spécifiée pour une LIF, cette règle est utilisée pour construire un rôle par défaut, une politique de basculement et une liste de protocoles de données pour la LIF.

Bien que plusieurs protocoles puissent être configurés pour les SVM et les LIF, il est recommandé de configurer S3 comme le seul protocole lors du service des données d'objet.

Étapes

1. Modifiez le paramètre de privilège sur avancé :

```
set -privilege advanced
```

2. Création d'une règle de données de service :

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

Le *data-core* et *data-s3-server* Les services sont les seuls requis pour activer ONTAP S3, bien que d'autres services puissent être inclus si nécessaire.

Création de LIF de données

Si vous avez créé un nouveau SVM, les LIF dédiées que vous créez pour accéder à S3 doivent être des LIF de données.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur up état.
- Si vous prévoyez d'utiliser un nom de sous-réseau pour allouer la valeur de l'adresse IP et du masque de réseau à une LIF, le sous-réseau doit déjà exister.

Les sous-réseaux contiennent un pool d'adresses IP qui appartiennent au même sous-réseau de couche 3. Ils sont créés à l'aide du `network subnet create` commande.

- La politique de service LIF doit déjà exister.

Description de la tâche

- Vous pouvez créer des LIF IPv4 et IPv6 sur le même port réseau.
- Si vous disposez d'un grand nombre de LIF dans le cluster, vous pouvez vérifier la capacité LIF prise en charge sur le cluster à l'aide de `network interface capacity show` Et la capacité LIF prise en charge sur chaque nœud à l'aide de `network interface capacity details show` commande (au niveau de privilège avancé).
- Si vous activez la hiérarchisation distante de la capacité FabricPool (cloud), vous devez également configurer les LIF intercluster.

Étapes

1. Créer une 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` Est le nœud vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

Vous pouvez également indiquer si la LIF doit revenir automatiquement au nœud home et au port home-port avec le `-auto-revert` option.

- `-home-port` Est le port physique ou logique vers lequel la LIF renvoie lorsque `network interface revert` La commande est exécutée sur le LIF.

- Vous pouvez spécifier une adresse IP avec le `-address` et `-netmask` ou vous activez l'allocation à partir d'un sous-réseau avec le `-subnet_name` option.
- Lors de l'utilisation d'un sous-réseau pour fournir l'adresse IP et le masque de réseau, si le sous-réseau a été défini avec une passerelle, une route par défaut vers cette passerelle est ajoutée automatiquement au SVM lorsqu'une LIF est créée à l'aide de ce sous-réseau.
- Si vous attribuez des adresses IP manuellement (sans utiliser de sous-réseau), vous devrez peut-être configurer une route par défaut vers une passerelle si des clients ou des contrôleurs de domaine se trouvent sur un autre sous-réseau IP. Le `network route create` La page man contient des informations sur la création d'une route statique au sein d'un SVM.
- Pour le `-firewall-policy` utilisez la même option par défaut `data` Comme le rôle LIF.

Vous pouvez créer et ajouter une stratégie de pare-feu personnalisée ultérieurement si vous le souhaitez.



Depuis ONTAP 9.10.1, les politiques de pare-feu sont obsolètes et intégralement remplacées par les politiques de service de LIF. Pour plus d'informations, voir "[Configuration des politiques de pare-feu pour les LIF](#)".

- `-auto-revert` Vous permet de spécifier si une LIF de données est automatiquement rétablie sur le nœud de rattachement en cas de démarrage, de modifications du statut de la base de données de gestion ou lors de la connexion réseau. Le paramètre par défaut est `false`, mais vous pouvez le définir sur `false` selon les stratégies de gestion de réseau de votre environnement.
- Le `-service-policy` spécifie la stratégie de données et de services de gestion que vous avez créée ainsi que les autres règles dont vous avez besoin.

2. Si vous souhaitez attribuer une adresse IPv6 dans `-address` option :

- Utilisez le `network ndp prefix show` Commande permettant d'afficher la liste des préfixes de RA apprises sur diverses interfaces.

Le `network ndp prefix show` la commande est disponible au niveau de privilège avancé.

- Utiliser le format `prefix:id` Pour construire l'adresse IPv6 manuellement.

`prefix` est le préfixe utilisé sur les différentes interfaces.

Pour calculer le `id`, choisissez un nombre hexadécimal 64 bits aléatoire.

- Vérifier que le LIF a été créé avec succès en utilisant le `network interface show` commande.
- Vérifiez que l'adresse IP configurée est accessible :

Pour vérifier...	Utiliser...
Adresse IPv4	<code>network ping</code>
Adresse IPv6	<code>network ping6</code>

Exemples

La commande suivante montre comment créer une LIF de données S3 attribuée avec le my-S3-policy règle de service :

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

La commande suivante affiche toutes les LIFs du cluster-1. Les LIF de données datalif1 et datalif3 sont configurées avec des adresses IPv4 et le datalif4 est configuré avec une adresse 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.

Création des LIFs intercluster pour le Tiering distant des FabricPool

Si vous activez le Tiering FabricPool à distance (cloud) à l'aide de ONTAP S3, vous devez configurer les LIF intercluster. Vous pouvez configurer les LIFs intercluster sur des ports partagés avec le réseau de données. Cela réduit le nombre de ports nécessaires pour la mise en réseau intercluster.

Avant de commencer

- Le port réseau physique ou logique sous-jacent doit avoir été configuré sur l'administrateur up état.
- La politique de service LIF doit déjà exister.

Description de la tâche

Les LIF intercluster ne sont pas nécessaires pour la hiérarchisation locale des pools de structure ni pour le traitement d'applications S3 externes.

Étapes

1. Lister les ports dans le cluster :

```
network port show
```

L'exemple suivant montre les ports réseau dans cluster01:

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

						Speed
(Mbps)						
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. Création des LIFs intercluster sur le SVM système :

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

L'exemple suivant illustre la création de LIFs intercluster cluster01_icl01 et 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. Vérifier que les LIFs intercluster ont été créés :

```
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. Vérifier que les LIFs intercluster sont redondants :

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

L'exemple suivant indique que les LIFs intercluster cluster01_icl01 et cluster01_icl02 sur le e0c le port basculera vers le e0d port.

```
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		

Créez le serveur de magasin d'objets S3

Le serveur de magasin d'objets ONTAP gère les données sous forme d'objets S3 au lieu du stockage de fichiers ou de blocs fourni par les serveurs NAS et SAN ONTAP.

Avant de commencer

Vous devez préparer à saisir le nom du serveur S3 en tant que nom de domaine complet (FQDN) que les clients utiliseront pour l'accès S3. Le FQDN ne doit pas commencer par un nom de compartiment.

Vous devez disposer d'un certificat d'autorité de certification auto-signé (créé aux étapes précédentes) ou d'un certificat signé par un fournisseur d'autorité de certification externe. Un certificat CA n'est pas nécessaire pour une utilisation de hiérarchisation locale, où le trafic IP transite uniquement par les LIFs de cluster.

Description de la tâche

Lorsqu'un serveur de magasin d'objets est créé, un utilisateur root avec UID 0 est créé. Aucune clé d'accès ou clé secrète n'est générée pour cet utilisateur root. L'administrateur ONTAP doit exécuter le `object-store-server users regenerate-keys` commande permettant de définir la clé d'accès et la clé secrète pour cet utilisateur.



Dans le cadre de nos bonnes pratiques, ne pas utiliser cet utilisateur root. Toute application client qui utilise la clé d'accès ou la clé secrète de l'utilisateur root dispose d'un accès complet à tous les compartiments et objets du magasin d'objets.


Voir la `vserver object-store-server` pages de manuel pour des options de configuration et d'affichage supplémentaires.

Exemple 2. Étapes

System Manager

Suivez cette procédure si vous ajoutez un serveur S3 à une machine virtuelle de stockage existante. Pour ajouter un serveur S3 à une nouvelle machine virtuelle de stockage, voir "[Création d'un SVM de stockage pour S3](#)".

Vous devez être prêt à saisir des adresses IP pour les données de rôle d'interface.

1. Activez S3 sur une machine virtuelle de stockage existante.
 - a. Sélectionnez la VM de stockage : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez une VM de stockage, cliquez sur **Paramètres**, puis cliquez sur  Sous **S3**.
 - b. Cliquez sur **Activer S3**, puis entrez le nom du serveur S3.
 - c. Sélectionnez le type de certificat.

Que vous sélectionniez un certificat généré par le système ou l'un de vos propres certificats, il sera nécessaire d'accéder au client.
 - d. Saisissez les interfaces réseau.
2. Si vous avez sélectionné le certificat généré par le système, les informations de certificat s'affichent lorsque la création de la nouvelle machine virtuelle de stockage est confirmée. Cliquez sur **Download** et enregistrez-le pour accéder au client.
 - La clé secrète ne s'affiche plus.
 - Si vous avez besoin de nouveau des informations de certificat : cliquez sur **stockage > machines virtuelles de stockage**, sélectionnez la machine virtuelle de stockage, puis cliquez sur **Paramètres**.

CLI

1. Création du serveur S3 :

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

Vous pouvez spécifier des options supplémentaires lors de la création du serveur S3 ou à tout moment ultérieurement.

- Si vous configurez une hiérarchisation locale, le nom du SVM peut être un SVM de données ou un nom de SVM système (cluster).
- Le nom du certificat doit être le nom du certificat du serveur (certificat d'utilisateur final ou de serveur) et non le certificat de l'autorité de certification du serveur (certificat de l'autorité de certification intermédiaire ou racine).
- HTTPS est activé par défaut sur le port 443. Vous pouvez modifier le numéro de port à l'aide du `-secure-listener-port` option.

Lorsque HTTPS est activé, des certificats CA sont requis pour une intégration correcte avec SSL/TLS.

- HTTP est désactivé par défaut. Lorsqu'il est activé, le serveur écoute sur le port 80. Vous pouvez l'activer avec le `-is-http-enabled` ou modifiez le numéro de port avec le `-listener-port`

option.

Lorsque HTTP est activé, la requête et les réponses sont envoyées sur le réseau en texte clair.

2. Vérifier que S3 est configuré :

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

Exemple

Cette commande vérifie les valeurs de configuration de tous les serveurs de stockage objet :

```
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: svml_ca
      Comment: Server comment
```

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.