



Configurar o acesso do S3 a uma SVM

ONTAP 9

NetApp
January 17, 2025

Índice

- Configurar o acesso do S3 a uma SVM 1
 - Criar um SVM para ONTAP S3 1
 - Crie e instale um certificado de CA em um SVM habilitado para ONTAP S3 4
 - Crie a política de dados de serviço do ONTAP S3 7
 - Criar LIFs de dados para o ONTAP S3 8
 - Criar LIFs entre clusters para disposição remota de FabricPool em camadas com o ONTAP S3 11
 - Crie o servidor de armazenamento de objetos ONTAP S3 14

Configurar o acesso do S3 a uma SVM

Criar um SVM para ONTAP S3

Embora o S3 possa coexistir com outros protocolos em um SVM, você pode querer criar um novo SVM para isolar o namespace e a carga de trabalho.

Sobre esta tarefa

Se você estiver fornecendo apenas um storage de objetos S3 a partir de uma SVM, o servidor S3 não exigirá nenhuma configuração DNS. No entanto, você pode querer configurar o DNS no SVM se outros protocolos forem usados.

Ao configurar o acesso S3 a uma nova VM de armazenamento usando o System Manager, você será solicitado a inserir informações de certificado e rede, e a VM de armazenamento e o servidor de armazenamento de objetos S3 são criados em uma única operação.

Exemplo 1. Passos

System Manager

Você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN do servidor S3 não deve começar com um nome de bucket.

Você deve estar preparado para inserir endereços IP para dados de função de interface.

Se você estiver usando um certificado assinado de CA externo, será solicitado que o insira durante este procedimento; você também terá a opção de usar um certificado gerado pelo sistema.

1. Habilite o S3 em uma VM de storage.
 - a. Adicionar uma nova VM de armazenamento: Clique em **armazenamento > armazenamento de VMs** e, em seguida, clique em **Adicionar**.

Se este for um novo sistema sem VMs de armazenamento existentes: Clique em **Dashboard > Configure Protocols**.

Se estiver adicionando um servidor S3 a uma VM de armazenamento existente: Clique em **armazenamento > armazenamento de VMs**, selecione uma VM de armazenamento, clique em **Configurações** e, em seguida, clique em  **S3**.

- a. Clique em **Ativar S3** e, em seguida, introduza o nome do servidor S3.
- b. Selecione o tipo de certificado.

Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.

- c. Introduza as interfaces de rede.

2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
 - A chave secreta não será exibida novamente.
 - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Verifique se o S3 está licenciado no cluster:

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

Se não estiver, contacte o seu representante de vendas.

2. Criar um 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>
```

- Utilize a definição UNIX para a `-rootvolume-security-style` opção.
- Utilize a opção C.UTF-8 predefinida `-language`.
- A `ipspace` definição é opcional.

3. Verifique a configuração e o status do SVM recém-criado:

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

O `Vserver Operational State` campo tem de apresentar o `running` estado. Se ele exibir `initializing` o estado, isso significa que alguma operação intermediária, como criação de volume raiz, falhou e você deve excluir o SVM e recriá-lo.

Exemplos

O comando a seguir cria um SVM para acesso a dados no `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
```

O comando a seguir mostra que um SVM foi criado com um volume raiz de 1 GB, que foi iniciado automaticamente e está `running` no estado. O volume raiz tem uma política de exportação padrão que não inclui nenhuma regra, portanto, o volume raiz não é exportado após a criação. Por padrão, a conta de usuário `vsadmin` é criada e está no `locked` estado. A função `vsadmin` é atribuída à conta de usuário padrão `vsadmin`.

```

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

```

Crie e instale um certificado de CA em um SVM habilitado para ONTAP S3

Um certificado de autoridade de certificação (CA) é necessário para habilitar o tráfego HTTPS de clientes S3 para o SVM habilitado para S3. O uso de certificados de CA cria uma relação confiável entre aplicativos clientes e o servidor de armazenamento de objetos ONTAP. Um certificado de CA deve ser instalado no ONTAP antes de usá-lo como um armazenamento de objetos acessível a clientes remotos.

Sobre esta tarefa

Embora seja possível configurar um servidor S3 para usar apenas HTTP, e embora seja possível configurar clientes sem um requisito de certificado de CA, é uma prática recomendada proteger o tráfego HTTPS para servidores ONTAP S3 com um certificado de CA.

Um certificado de CA não é necessário para um caso de uso local de disposição em camadas, em que o tráfego IP está passando apenas pelas LIFs de cluster.

As instruções neste procedimento irão criar e instalar um certificado auto-assinado ONTAP. Embora o ONTAP possa gerar certificados autoassinados, o uso de certificados assinados de uma autoridade de certificação de

terceiros é a prática recomendada.; consulte a documentação de autenticação do administrador para obter mais informações.

"Autenticação de administrador e RBAC"

Consulte as `security certificate` páginas man para obter opções de configuração adicionais.

Passos

1. Crie um certificado digital autoassinado:

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

A `-type root-ca` opção cria e instala um certificado digital autoassinado para assinar outros certificados agindo como autoridade de certificação (CA).

A `-common-name` opção cria o nome da Autoridade de Certificação (CA) do SVM e será usada ao gerar o nome completo do certificado.

O tamanho padrão do certificado é de 2048 bits.

Exemplo

```
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 o nome gerado do certificado for exibido; certifique-se de salvá-lo para etapas posteriores neste procedimento.

2. Gerar uma solicitação de assinatura de certificado:

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

O `-common-name` parâmetro para a solicitação de assinatura deve ser o nome do servidor S3 (FQDN).

Você pode fornecer a localização e outras informações detalhadas sobre o SVM, se desejado.

Você será solicitado a manter uma cópia da solicitação de certificado e da chave privada para referência futura.

3. Assine a CSR usando SVM_CA para gerar o certificado do S3 Server:

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

Insira as opções de comando que você usou nas etapas anteriores:

- `-ca` — o nome comum da CA que você inseriu na Etapa 1.

- `-ca-serial` — o número de série da CA a partir do passo 1. Por exemplo, se o nome do certificado CA for `svm1_CA_159D1587CE21E9D4_svm1_CA`, o número de série será `159D1587CE21E9D4`.

Por padrão, o certificado assinado expirará em 365 dias. Você pode selecionar outro valor e especificar outros detalhes de assinatura.

Quando solicitado, copie e insira a string de solicitação de certificado que você salvou na Etapa 2.

Um certificado assinado é exibido; salve-o para uso posterior.

4. Instale o certificado assinado no SVM habilitado para S3:

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

Quando solicitado, insira o certificado e a chave privada.

Você tem a opção de inserir certificados intermediários se uma cadeia de certificados for desejada.

Quando a chave privada e o certificado digital assinado pela CA forem exibidos, salve-os para referência futura.

5. Obtenha o certificado de chave pública:

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

Salve o certificado de chave pública para uma configuração posterior do lado do cliente.

Exemplo


```

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

                Name of Vserver: svml.example.com
      FQDN or Custom Common Name: svml_ca
Serial Number of Certificate: 159D1587CE21E9D4
      Certificate Authority: svml_ca
      Type of Certificate: root-ca
(DEPRECATED)-Certificate Subtype: -
      Unique Certificate Name: svml_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

```

Crie a política de dados de serviço do ONTAP S3

Você pode criar políticas de serviço para dados e serviços de gerenciamento do S3. É necessária uma política de dados de serviço S3 para permitir o tráfego de dados S3 nos LIFs.

Sobre esta tarefa

Uma política de dados de serviço S3 é necessária se você estiver usando LIFs de dados e LIFs entre clusters. Não é necessário se você estiver usando LIFs de cluster para o caso de uso de disposição em camadas local.

Quando uma política de serviço é especificada para um LIF, a política é usada para criar uma função padrão, política de failover e lista de protocolos de dados para o LIF.

Embora vários protocolos possam ser configurados para SVMs e LIFs, é uma prática recomendada para S3 ser o único protocolo ao fornecer dados de objetos.

Passos

1. Altere a configuração de privilégios para avançado:

```
set -privilege advanced
```

2. Criar uma política de dados de serviço:

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

Os `data-core` serviços e `data-s3-server` são os únicos necessários para habilitar o ONTAP S3, embora outros serviços possam ser incluídos conforme necessário.

Criar LIFs de dados para o ONTAP S3

Se você criou um novo SVM, as LIFs dedicadas que você cria para o acesso S3 devem ser LIFs de dados.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.
- Se você estiver planejando usar um nome de sub-rede para alocar o endereço IP e o valor de máscara de rede para um LIF, a sub-rede já deve existir.

As sub-redes contêm um conjunto de endereços IP que pertencem à mesma sub-rede da camada 3. Eles são criados usando o `network subnet create` comando.

- A política de serviço LIF já deve existir.
- Como prática recomendada, os LIFs usados para acesso a dados (`data-S3-server`) e LIFs usados para operações de gerenciamento (`Management-https`) devem ser separados. Ambos os serviços não devem ser ativados no mesmo LIF.
- Os Registros DNS devem ter apenas endereços IP dos LIFs que têm `dados-S3-server` associados a eles. Se endereços IP de outros LIFs forem especificados no Registro DNS, as solicitações do ONTAP S3 podem ser atendidas por outros servidores, resultando em respostas inesperadas ou perda de dados.

Sobre esta tarefa

- Você pode criar LIFs IPv4 e IPv6 na mesma porta de rede.
- Se você tiver um grande número de LIFs no cluster, poderá verificar a capacidade de LIF suportada no cluster usando o `network interface capacity show` comando e a capacidade de LIF suportada em cada nó usando o `network interface capacity details show` comando (no nível de privilégio avançado).
- Se você habilitar a disposição em camadas remota de capacidade FabricPool (nuvem), também deverá configurar LIFs entre clusters.

Passos

1. Criar um 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` É o nó para o qual o LIF retorna quando o `network interface revert` comando é

executado no LIF.

Você também pode especificar se o LIF deve reverter automaticamente para o nó inicial e porta inicial com a `-auto-revert` opção.

- `-home-port` É a porta física ou lógica para a qual o LIF retorna quando o `network interface revert` comando é executado no LIF.
- Pode especificar um endereço IP com `-address` as opções e `-netmask` ou ativar a atribuição a partir de uma sub-rede com a `-subnet_name` opção.
- Ao usar uma sub-rede para fornecer o endereço IP e a máscara de rede, se a sub-rede foi definida com um gateway, uma rota padrão para esse gateway é adicionada automaticamente ao SVM quando um LIF é criado usando essa sub-rede.
- Se você atribuir endereços IP manualmente (sem usar uma sub-rede), talvez seja necessário configurar uma rota padrão para um gateway se houver clientes ou controladores de domínio em uma sub-rede IP diferente. A `network route create` página man contém informações sobre a criação de uma rota estática dentro de um SVM.
- Para a `-firewall-policy` opção, use o mesmo padrão `data` que a função LIF.

Você pode criar e adicionar uma política de firewall personalizada mais tarde, se desejado.



A partir do ONTAP 9.10,1, as políticas de firewall são obsoletas e totalmente substituídas por políticas de serviço LIF. Para obter mais informações, "[Configurar políticas de firewall para LIFs](#)" consulte .

- `-auto-revert` Permite especificar se um LIF de dados é automaticamente revertido para o seu nó inicial em circunstâncias como inicialização, alterações no status do banco de dados de gerenciamento ou quando a conexão de rede é feita. A configuração padrão é `false`, mas você pode defini-la como `false` dependendo das políticas de gerenciamento de rede em seu ambiente.
- A `-service-policy` opção especifica a política de dados e serviços de gerenciamento que você criou e quaisquer outras políticas necessárias.

2. Se você quiser atribuir um endereço IPv6 na `-address` opção:

- a. Use o `network ndp prefix show` comando para visualizar a lista de prefixos RA aprendidos em várias interfaces.

O `network ndp prefix show` comando está disponível no nível de privilégio avançado.

- b. Use o formato `prefix:id` para construir o endereço IPv6 manualmente.

`prefix` é o prefixo aprendido em várias interfaces.

Para derivar o `id`, escolha um número hexadecimal aleatório de 64 bits.

3. Verifique se o LIF foi criado com sucesso usando o `network interface show` comando.
4. Verifique se o endereço IP configurado está acessível:

Para verificar um...	Utilizar...
Endereço IPv4	<code>network ping</code>
Endereço IPv6	<code>network ping6</code>

Exemplos

O comando a seguir mostra como criar um LIF de dados S3 atribuído com a `my-S3-policy` política de serviço:

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

O comando a seguir mostra todas as LIFs no cluster-1. Os LIFs de dados `datalif1` e `datalif3` são configurados com endereços IPv4 e o `datalif4` é configurado com um endereço IPv6:

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

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

Criar LIFs entre clusters para disposição remota de FabricPool em camadas com o ONTAP S3

Se você estiver habilitando a disposição em camadas remota de capacidade FabricPool (nuvem) usando o ONTAP S3, configure LIFs entre clusters. Você pode configurar LIFs entre clusters em portas compartilhadas com a rede de dados. Isso reduz o número de portas de que você precisa para redes entre clusters.

Antes de começar

- A porta de rede física ou lógica subjacente deve ter sido configurada para o status administrativo `up`.

- A política de serviço LIF já deve existir.

Sobre esta tarefa

Os LIFs não são necessários para a disposição em camadas do pool de malha local ou para servir aplicações S3 externas.

Passos

1. Liste as portas no cluster:

```
network port show
```

O exemplo a seguir mostra as portas de rede no `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. Criar LIFs entre clusters no sistema:

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

O exemplo a seguir cria LIFs entre clusters `cluster01_ic101` e `cluster01_ic102`:

```

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. Verifique se as LIFs entre clusters foram criadas:

```
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	Port
Home					
-----	-----	-----	-----	-----	-----
-----	-----	-----	-----	-----	-----
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. Verifique se as LIFs entre clusters são redundantes:

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

O exemplo a seguir mostra que os LIFs entre clusters `cluster01_icl01` e `cluster01_icl02` na `e0c` porta irão falhar para a `e0d` porta.

```

cluster01::> network interface show -service-policy default-intercluster
-failover
          Logical          Home          Failover          Failover
Vserver  Interface            Node:Port      Policy            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

```

Crie o servidor de armazenamento de objetos ONTAP S3

O servidor de armazenamento de objetos ONTAP gerencia dados como objetos S3, em vez de armazenamento de arquivos ou blocos fornecido pelos servidores ONTAP nas e SAN.

Antes de começar

Você deve estar preparado para inserir o nome do servidor S3 como um nome de domínio totalmente qualificado (FQDN), que os clientes usarão para o acesso S3. O FQDN não deve começar com um nome de intervalo. Ao acessar buckets usando o estilo virtual hospedado, o nome do servidor será usado como `mydomain.com`. Por exemplo, `bucketname.mydomain.com`.

Você deve ter um certificado de CA autoassinado (criado em etapas anteriores) ou um certificado assinado por um fornecedor de CA externo. Um certificado de CA não é necessário para um caso de uso local de disposição em camadas, em que o tráfego IP está passando apenas pelas LIFs de cluster.

Sobre esta tarefa

Quando um servidor de armazenamento de objetos é criado, um usuário raiz com UID 0 é criado. Nenhuma chave de acesso ou chave secreta é gerada para este usuário raiz. O administrador do ONTAP deve executar o `object-store-server users regenerate-keys` comando para definir a chave de acesso e a chave secreta para esse usuário.



Como uma prática recomendada do NetApp, não use esse usuário root. Qualquer aplicativo cliente que use a chave de acesso ou chave secreta do usuário raiz tem acesso total a todos os buckets e objetos no armazenamento de objetos.


Consulte as `vserver object-store-server` páginas de manual para obter opções adicionais de configuração e exibição.

Exemplo 2. Passos

System Manager

Use este procedimento se estiver adicionando um servidor S3 a uma VM de armazenamento existente. Para adicionar um servidor S3 a uma nova VM de armazenamento, "[Criar um SVM de storage em S3](#)" consulte .

Você deve estar preparado para inserir endereços IP para dados de função de interface.

1. Habilite o S3 em uma VM de storage existente.
 - a. Selecione a VM de armazenamento: Clique em **Storage > Storage VMs**, selecione uma VM de armazenamento, clique em **Settings** e, em seguida, clique em  **S3**.
 - b. Clique em **Ativar S3** e, em seguida, introduza o nome do servidor S3.
 - c. Selecione o tipo de certificado.

Se você selecionar um certificado gerado pelo sistema ou um de seu, ele será necessário para acesso ao cliente.
 - d. Introduza as interfaces de rede.
2. Se você selecionou o certificado gerado pelo sistema, as informações do certificado serão exibidas quando a nova criação da VM de armazenamento for confirmada. Clique em **Download** e salve-o para acesso ao cliente.
 - A chave secreta não será exibida novamente.
 - Se você precisar das informações do certificado novamente: Clique em **armazenamento > armazenamento de VMs**, selecione a VM de armazenamento e clique em **Configurações**.

CLI

1. Crie o servidor S3:

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

Você pode especificar opções adicionais ao criar o servidor S3 ou a qualquer momento mais tarde.

- Se você estiver configurando a disposição em categorias locais, o nome do SVM pode ser um nome de data SVM ou SVM do sistema (cluster).
- O nome do certificado deve ser o nome do certificado do servidor (usuário final ou certificado de folha) e não o certificado de CA do servidor (certificado de CA intermediário ou raiz).
- O HTTPS é ativado por padrão na porta 443. Pode alterar o número da porta com a `-secure -listener-port` opção.

Quando o HTTPS está ativado, os certificados de CA são necessários para a integração correta com SSL/TLS. A partir do ONTAP 9.15.1, o TLS 1,3 é compatível com armazenamento de objetos S3.

- O HTTP está desativado por padrão. Quando ativado, o servidor escuta na porta 80. Você pode ativá-lo com a `-is-http-enabled` opção ou alterar o número da porta com a `-listener -port` opção.

Quando o HTTP está ativado, a solicitação e as respostas são enviadas pela rede em texto não criptografado.

2. Verifique se o S3 está configurado:

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

Exemplo

Este comando verifica os valores de configuração de todos os servidores de armazenamento de objetos:

```
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
```

Informações sobre direitos autorais

Copyright © 2025 NetApp, Inc. Todos os direitos reservados. Impresso nos EUA. Nenhuma parte deste documento protegida por direitos autorais pode ser reproduzida de qualquer forma ou por qualquer meio — gráfico, eletrônico ou mecânico, incluindo fotocópia, gravação, gravação em fita ou storage em um sistema de recuperação eletrônica — sem permissão prévia, por escrito, do proprietário dos direitos autorais.

O software derivado do material da NetApp protegido por direitos autorais está sujeito à seguinte licença e isenção de responsabilidade:

ESTE SOFTWARE É FORNECIDO PELA NETAPP "NO PRESENTE ESTADO" E SEM QUAISQUER GARANTIAS EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÕES, GARANTIAS IMPLÍCITAS DE COMERCIALIZAÇÃO E ADEQUAÇÃO A UM DETERMINADO PROPÓSITO, CONFORME A ISENÇÃO DE RESPONSABILIDADE DESTES DOCUMENTOS. EM HIPÓTESE ALGUMA A NETAPP SERÁ RESPONSÁVEL POR QUALQUER DANO DIRETO, INDIRETO, INCIDENTAL, ESPECIAL, EXEMPLAR OU CONSEQUENCIAL (INCLUINDO, SEM LIMITAÇÕES, AQUISIÇÃO DE PRODUTOS OU SERVIÇOS SOBRESSALIENTES; PERDA DE USO, DADOS OU LUCROS; OU INTERRUPÇÃO DOS NEGÓCIOS), INDEPENDENTEMENTE DA CAUSA E DO PRINCÍPIO DE RESPONSABILIDADE, SEJA EM CONTRATO, POR RESPONSABILIDADE OBJETIVA OU PREJUÍZO (INCLUINDO NEGLIGÊNCIA OU DE OUTRO MODO), RESULTANTE DO USO DESTES SOFTWARES, MESMO SE ADVERTIDA DA RESPONSABILIDADE DE TAL DANO.

A NetApp reserva-se o direito de alterar quaisquer produtos descritos neste documento, a qualquer momento e sem aviso. A NetApp não assume nenhuma responsabilidade nem obrigação decorrentes do uso dos produtos descritos neste documento, exceto conforme expressamente acordado por escrito pela NetApp. O uso ou a compra deste produto não representam uma licença sob quaisquer direitos de patente, direitos de marca comercial ou quaisquer outros direitos de propriedade intelectual da NetApp.

O produto descrito neste manual pode estar protegido por uma ou mais patentes dos EUA, patentes estrangeiras ou pedidos pendentes.

LEGENDA DE DIREITOS LIMITADOS: o uso, a duplicação ou a divulgação pelo governo estão sujeitos a restrições conforme estabelecido no subparágrafo (b)(3) dos Direitos em Dados Técnicos - Itens Não Comerciais no DFARS 252.227-7013 (fevereiro de 2014) e no FAR 52.227- 19 (dezembro de 2007).

Os dados aqui contidos pertencem a um produto comercial e/ou serviço comercial (conforme definido no FAR 2.101) e são de propriedade da NetApp, Inc. Todos os dados técnicos e software de computador da NetApp fornecidos sob este Contrato são de natureza comercial e desenvolvidos exclusivamente com despesas privadas. O Governo dos EUA tem uma licença mundial limitada, irrevogável, não exclusiva, intransferível e não sublicenciável para usar os Dados que estão relacionados apenas com o suporte e para cumprir os contratos governamentais desse país que determinam o fornecimento de tais Dados. Salvo disposição em contrário no presente documento, não é permitido usar, divulgar, reproduzir, modificar, executar ou exibir os dados sem a aprovação prévia por escrito da NetApp, Inc. Os direitos de licença pertencentes ao governo dos Estados Unidos para o Departamento de Defesa estão limitados aos direitos identificados na cláusula 252.227-7015(b) (fevereiro de 2014) do DFARS.

Informações sobre marcas comerciais

NETAPP, o logotipo NETAPP e as marcas listadas em <http://www.netapp.com/TM> são marcas comerciais da NetApp, Inc. Outros nomes de produtos e empresas podem ser marcas comerciais de seus respectivos proprietários.