



配置对 **SVM** 的 **S3** 访问 ONTAP 9

NetApp
April 24, 2024

目录

- 配置对 SVM 的 S3 访问 1
 - 为 S3 创建 SVM 1
 - 在 SVM 上创建并安装 CA 证书 4
 - 创建 S3 服务数据策略 7
 - 创建数据 LIF : 7
 - 为远程 FabricPool 分层创建集群间 LIF 10
 - 创建 S3 对象存储服务器 13

配置对 SVM 的 S3 访问

为 S3 创建 SVM

虽然S3可以与SVM中的其他协议共存、但您可能需要创建一个新的SVM来隔离命名空间和工作负载。

关于此任务

如果您仅从SVM提供S3对象存储、则S3服务器不需要任何DNS配置。但是，如果使用其他协议，则可能需要在SVM上配置DNS。

在使用System Manager配置对新Storage VM的S3访问时、系统会提示您输入证书和网络信息、并在一次操作中创建Storage VM和S3对象存储服务器。

示例 1. 步骤

System Manager

您应准备好将S3服务器名称输入为完全限定域名(FQDN)、客户端将使用该域名进行S3访问。S3服务器FQDN不能以分段名称开头。


您应准备为接口角色数据输入IP地址。

如果您使用的是外部 CA 签名证书，则在此操作步骤期间，系统将提示您输入此证书；您也可以选择使用系统生成的证书。

1. 在 Storage VM 上启用 S3 。

- a. 添加新的Storage VM：单击*存储> Storage VM*、然后单击*添加*。

如果这是一个没有现有Storage VM的新系统：单击*信息板>配置协议*。

如果要将S3服务器添加到现有Storage VM：单击*存储> Storage VM*、选择一个Storage VM、单击*设置*、然后单击  在 * S3 下。

- a. 单击 * 启用 S3* ，然后输入 S3 服务器名称。
- b. 选择证书类型。

无论选择系统生成的证书还是您自己的证书之一，客户端访问都需要此证书。

- c. 输入网络接口。

2. 如果选择了系统生成的证书，则在确认创建新 Storage VM 后，您将看到证书信息。单击 * 下载 * 并保存以供客户端访问。

- 不会再显示此机密密钥。
- 如果您再次需要证书信息：单击*存储>存储VM*、选择Storage VM、然后单击*设置*。

命令行界面

1. 验证 S3 是否已在集群上获得许可：

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

如果不是，请联系您的销售代表。

2. 创建 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>
```

- 对使用UNIX设置 -rootvolume-security-style 选项

- 使用默认C.UTF-8 -language 选项

- ipspace 设置是可选的。

3. 验证新创建的 SVM 的配置和状态：

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

。 Vserver Operational State 字段必须显示 running 状态。如果显示 initializing 状态、表示某些中间操作(如创建根卷)失败、您必须删除SVM并重新创建它。

示例

以下命令将在 IP 空间 ipspaceA 中创建用于数据访问的 SVM：

```
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
```

以下命令显示已创建根卷为1 GB的SVM、并且此SVM已自动启动并位于中 running 状态。根卷具有一个默认导出策略，该策略不包含任何规则，因此根卷在创建时不会导出。默认情况下、vsadmin用户帐户会创建在中 locked 状态。vsadmin 角色将分配给默认 vsadmin 用户帐户。

```

cluster-1::> vservers show -vservers 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

```

在 SVM 上创建并安装 CA 证书

要启用从 S3 客户端到启用了 S3 的 SVM 的 HTTPS 流量，需要证书颁发机构（CA）证书。

关于此任务

虽然可以将 S3 服务器配置为仅使用 HTTP，并且可以在不要求 CA 证书的情况下配置客户端，但最佳做法是使用 CA 证书保护发送到 ONTAP S3 服务器的 HTTPS 流量。

在本地分层使用情形中，IP 流量仅通过集群 LIF 时，不需要 CA 证书。

此操作步骤中的说明将创建并安装 ONTAP 自签名证书。此外，还支持来自第三方供应商的 CA 证书；有关详细信息，请参见管理员身份验证文档。

"管理员身份验证和 RBAC"

请参见 `security certificate` 其他配置选项的手册页。

步骤

1. 创建自签名数字证书：

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

。 -type root-ca 选项用于创建并安装自签名数字证书、以便通过充当证书颁发机构(CA)对其他证书进行签名。

。 -common-name 选项将创建SVM的证书颁发机构(Certificate Authority、CA)名称、并在生成证书的完整名称时使用。

默认证书大小为 2048 位。

示例

```
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
```

显示证书的生成名称时，请务必保存此证书，以供此操作步骤中稍后的步骤使用。

2. 生成证书签名请求：

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

。 -common-name 签名请求的参数必须是S3服务器名称(FQDN)。

如果需要，您可以提供 SVM 的位置和其他详细信息。

系统会提示您保留证书请求和私钥的副本，以供日后参考。

3. 使用 SVM_CA 对 CSR 签名以生成 S3 服务器的证书：

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

输入您在先前步骤中使用的命令选项：

- 。 -ca --您在步骤1中输入的CA的公用名。
- 。 -ca-serial --步骤1中的CA序列号。例如，如果 CA 证书名称为 svm1_ca_159D1587CE21E9D4_svm1_ca ，则序列号为 159D1587CE21E9d4 。

默认情况下，签名证书将在 365 天后过期。您可以选择其他值并指定其他签名详细信息。

出现提示时，复制并输入您在步骤 2 中保存的证书请求字符串。

此时将显示一个签名证书；请保存此证书以供日后使用。

4. 在启用了 S3 的 SVM 上安装签名证书:

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

出现提示时, 输入证书和专用密钥。

如果需要证书链, 您可以选择输入中间证书。

显示私钥和 CA 签名的数字证书时, 请保存它们以供将来参考。

5. 获取公有密钥证书:

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

保存公有密钥证书以供稍后的客户端配置使用。

示例

```
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
```


创建 S3 服务数据策略

您可以为 S3 数据和管理服务创建服务策略。要在 LIF 上启用 S3 数据流量，需要使用 S3 服务数据策略。

关于此任务

如果使用的是数据 LIF 和集群间 LIF，则需要使用 S3 服务数据策略。如果在本地分层使用情形中使用集群 LIF，则不需要此功能。

为 LIF 指定服务策略时，将使用该策略为 LIF 构建默认角色，故障转移策略和数据协议列表。

虽然可以为 SVM 和 LIF 配置多个协议，但最好将 S3 作为提供对象数据的唯一协议。

步骤

1. 将权限设置更改为高级：

```
set -privilege advanced
```

2. 创建服务数据策略：

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

。data-core 和 data-s3-server 服务是启用 ONTAP S3 所需的唯一服务、但也可以根据需要包括其他服务。

创建数据 LIF：

如果创建了新的 SVM，则为 S3 访问创建的专用 LIF 应为数据 LIF。

开始之前

- 底层物理或逻辑网络端口必须已配置为管理端口 up 状态。
- 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，则此子网必须已存在。

子网包含属于同一第 3 层子网的 IP 地址池。它们是使用创建的 `network subnet create` 命令：

- LIF 服务策略必须已存在。

关于此任务

- 您可以在同一网络端口上创建 IPv4 和 IPv6 LIF。
- 如果集群中有大量 LIF、则可以使用验证集群上支持的 LIF 容量 `network interface capacity show` 命令以及每个节点上支持的 LIF 容量 `network interface capacity details show` 命令(在高级权限级别)。
- 如果要启用远程 FabricPool 容量（云）分层，则还必须配置集群间 LIF。

步骤

1. 创建 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 是LIF返回到的节点 network interface revert 命令将在LIF上运行。

您还可以使用指定LIF是否应自动还原到主节点和主端口 -auto-revert 选项

- -home-port 是LIF返回到的物理或逻辑端口 network interface revert 命令将在LIF上运行。
- 您可以使用指定IP地址 -address 和 -netmask 选项、或者使用启用从子网分配 -subnet_name 选项
- 使用子网提供 IP 地址和网络掩码时，如果使用网关定义了子网，则在使用该子网创建 LIF 时，系统会自动向 SVM 添加指向该网关的默认路由。
- 如果您手动分配 IP 地址（而不使用子网），则在其他 IP 子网上存在客户端或域控制器时，可能需要配置指向网关的默认路由。。 network route create 手册页包含有关在SVM中创建静态路由的信息。
- 。 -firewall-policy 选项中、使用相同的默认值 data 作为LIF角色。

如果需要，您可以稍后创建和添加自定义防火墙策略。



从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 ["为 LIF 配置防火墙策略"](#)。

- -auto-revert 用于指定在启动、更改管理数据库状态或建立网络连接等情况下、数据LIF是否自动还原到其主节点。默认设置为 false，但您可以将其设置为 false 具体取决于您环境中的网络管理策略。
- 。 -service-policy 选项用于指定您创建的数据和管理服务策略以及所需的任何其他策略。

2. 如果要在中分配IPv6地址 -address 选项：

- a. 使用 network ndp prefix show 命令以查看在各种接口上获取的RA前缀列表。
 - network ndp prefix show 命令可在高级权限级别下使用。
- b. 使用格式 prefix:id 手动构建IPv6地址。

prefix 是在各种接口上获取的前缀。

用于派生 `id` 下，选择一个随机的64位十六进制数。

- 3. 使用验证是否已成功创建LIF network interface show 命令：
- 4. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	network ping

要验证 ...	使用 ...
IPv6地址	network ping6

示例

以下命令显示如何创建分配给S3数据LIF my-S3-policy 服务策略：

```
network interface create -vserver svm1.example.com -lif lif2 -home-node  
node2 -homeport e0d -service-policy my-S3-policy -subnet-name ipspace1
```

以下命令显示 cluster-1 中的所有 LIF 。数据 LIF datalif1 和 datalif3 配置了 IPv4 地址，而 datalif4 配置了 IPv6 地址：

```
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.

为远程 FabricPool 分层创建集群间 LIF

如果要使用 ONTAP S3 启用远程 FabricPool 容量（云）分层，则必须配置集群间 LIF。您可以在与数据网络共享的端口上配置集群间 LIF。这样可以减少集群间网络连接所需的端口数量。

开始之前

- 底层物理或逻辑网络端口必须已配置为管理端口 up 状态。
- LIF 服务策略必须已存在。

关于此任务

本地 Fabric Pool 分层或提供外部 S3 应用程序不需要集群间 LIF 。

步骤

- 1. 列出集群中的端口：

```
network port show
```

以下示例显示了中的网络端口 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. 在系统 SVM 上创建集群间 LIF ：

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

以下示例将创建集群间生命周期 cluster01_icl01 和 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. 验证是否已创建集群间 LIF :

```
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. 验证集群间 LIF 是否冗余:

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

以下示例显示了集群间的生命周期 cluster01_icl01 和 cluster01_icl02 在上 e0c 端口将故障转移到 e0d 端口。

```
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	

创建 S3 对象存储服务器

ONTAP 对象存储服务器将数据作为 S3 对象进行管理，而不是由 ONTAP NAS 和 SAN 服务器提供的文件或块存储。

开始之前

您应准备好将 S3 服务器名称输入为完全限定域名(FQDN)、客户端将使用该域名进行 S3 访问。FQDN 不能以分段名称开头。

您应具有自签名 CA 证书（在先前步骤中创建）或由外部 CA 供应商签名的证书。在本地分层使用情形中，IP 流量仅通过集群 LIF 时，不需要 CA 证书。

关于此任务

创建对象存储服务器时，将创建 UID 为 0 的 root 用户。不会为此 root 用户生成访问密钥或机密密钥。ONTAP 管理员必须运行 `object-store-server users regenerate-keys` 命令以设置此用户的访问密钥和机密密钥。



作为 NetApp 最佳实践，请勿使用此 root 用户。使用 root 用户的访问密钥或机密密钥的任何客户端应用程序都可以完全访问对象存储中的所有分段和对象。


请参见 `vserver object-store-server` 有关其他配置和显示选项的手册页。

System Manager

如果要将S3服务器添加到现有Storage VM、请使用此操作步骤。要将S3服务器添加到新的Storage VM、请参见 ["为S3创建存储SVM"](#)。

您应准备为接口角色数据输入IP地址。

1. 在现有Storage VM上启用S3。

- 选择Storage VM：单击*存储> Storage VM*、选择一个Storage VM、单击*设置*、然后单击  在 * S3 下。
- 单击 * 启用 S3* ，然后输入 S3 服务器名称。
- 选择证书类型。

无论选择系统生成的证书还是您自己的证书之一，客户端访问都需要此证书。

d. 输入网络接口。

2. 如果选择了系统生成的证书，则在确认创建新 Storage VM 后，您将看到证书信息。单击 * 下载 * 并保存以供客户端访问。

- 不会再显示此机密密钥。
- 如果您再次需要证书信息：单击 * 存储 > 存储 VM* ，选择 Storage VM ，然后单击 * 设置 * 。

命令行界面

1. 创建 S3 服务器：

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

您可以在创建 S3 服务器时或以后任何时间指定其他选项。

- 如果要配置本地分层、则SVM名称可以是数据SVM或系统SVM (集群)名称。
- 证书名称应是服务器证书的名称(最终用户证书或叶证书)、而不是服务器CA证书(中间CA证书或根CA证书)。
- 默认情况下，HTTPS 在端口 443 上处于启用状态。您可以使用更改端口号 `-secure-listener -port` 选项

启用HTTPS后、要与SSL/TLS正确集成、需要CA证书。

- 默认情况下、HTTP处于禁用状态。启用后、服务器将侦听端口80。您可以使用启用它 `-is-http -enabled` 选项、或者使用更改端口号 `-listener-port` 选项

启用HTTP后、请求和响应将以明文形式通过网络发送。

2. 验证是否已配置S3：

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


示例

此命令将验证所有对象存储服务器的配置值：

```
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
```

版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。