



Configure S3 access to an SVM

ONTAP 9

NetApp
February 07, 2023

Table of Contents

- Configure S3 access to an SVM 1
 - Create an SVM for S3 1
 - Create and install a CA certificate on the SVM 4
 - Create an S3 service data policy 6
 - Create data LIFs 7
 - Create intercluster LIFs for remote FabricPool tiering 9
 - Create the S3 object store server 12

Configure S3 access to an SVM

Create an SVM for S3

Although S3 can coexist with other protocols in an SVM, you might want to create a new SVM to isolate the namespace and workload.

About this task

If you are only providing S3 object storage from an SVM, the S3 server does not require any DNS configuration. However, you might want to configure DNS on the SVM if other protocols are used.

When you configure S3 access to a new storage VM using System Manager, you are prompted to enter certificate and networking information, and the storage VM and S3 object storage server are created in a single operation.

Example 1. Steps

CLI

1. Verify that S3 is licensed on your cluster:

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

If it is not, contact your sales representative.

2. Create an SVM:

```
vserver create -vserver svm_name -rootvolume root_volume_name -aggregate  
aggregate_name -rootvolume-security-style unix -language C.UTF-8 -ipspace  
ipspace_name
```

- Use the UNIX setting for the `-rootvolume-security-style` option.
- Use the default C.UTF-8 `-language` option.
- The `ipspace` setting is optional.

3. Verify the configuration and status of the newly created SVM:

```
vserver show -vserver svm_name
```

The Vserver Operational State field must display the running state. If it displays the initializing state, it means that some intermediate operation such as root volume creation failed, and you must delete the SVM and re-create it.

Examples

The following command creates an SVM for data access in the IPspace `ipspaceA`:

```
cluster-1::> vserver create -vserver svm1.example.com -rootvolume  
root_svm1 -aggregate aggr1 -rootvolume-security-style unix -language  
C.UTF-8 -ipspace ipspaceA
```

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

The following command shows that an SVM was created with a root volume of 1 GB, and it was started automatically and is in `running` state. The root volume has a default export policy that does not include any rules, so the root volume is not exported upon creation. By default, the `vsadmin` user account is created and is in the `locked` state. The `vsadmin` role is assigned to the default `vsadmin` user account.

```

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

```

System Manager

You should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The S3 server FQDN must not begin with a bucket name.

You should be prepared to enter IP addresses for interface role Data.

If you are using an external-CA signed certificate, you will be prompted to enter it during this procedure; you also have the option to use a system-generated certificate.

1. Enable S3 on a storage VM.

- a. Add a new storage VM: Click **Storage > Storage VMs**, then click **Add**.

If this is a new system with no existing storage VMs: Click **Dashboard > Configure Protocols**.

If you are adding an S3 server to an existing storage VM: Click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **S3**.

- b. Click **Enable S3**, then enter the S3 Server Name.

- c. Select the certificate type.

Whether you select system-generated certificate or one of your own, it will be required for client access.

- d. Enter the network interfaces.
2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.
 - The secret key will not be displayed again.
 - If you need the certificate information again: Click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

Create and install a CA certificate on the SVM

A Certificate Authority (CA) certificate is required to enable HTTPS traffic from S3 clients to the S3-enabled SVM.

About this task

Although it is possible to configure an S3 server to use HTTP only, and although it is possible to configure clients without a CA certificate requirement, it is a best practice to secure HTTPS traffic to ONTAP S3 servers with a CA certificate.

A CA certificate is not necessary for a local tiering use case, where IP traffic is going over cluster LIFs only.

The instructions in this procedure will create and install an ONTAP self-signed certificate. CA certificates from third-party vendors are also supported; see the administrator authentication documentation for more information.

Administrator authentication and RBAC

See the `security certificate` man pages for additional configuration options.

Steps

1. Create a self-signed digital certificate:

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

The `-type root-ca` option creates and installs a self-signed digital certificate to sign other certificates by acting as a certificate authority (CA).

The `-common-name` option creates the SVM's Certificate Authority (CA) name and will be used when generating the certificate's complete name.

The default certificate size is 2048 bits.

Example

```
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

When the certificate's generated name is displayed; be sure to save it for later steps in this procedure.

2. Generate a certificate signing request:

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

The `-common-name` parameter for the signing request must be the S3 server name (FQDN).

You can provide the location and other detailed information about the SVM if desired.

You are prompted to keep a copy of your certificate request and private key for future reference.

3. Sign the CSR using SVM_CA to generate S3 Server's certificate:

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

Enter the command options that you used in previous steps:

- `-ca` — the common name of the CA that you entered in Step 1.
- `-ca-serial` — the CA serial number from Step 1. For example, if the CA certificate name is `svm1_ca_159D1587CE21E9D4_svm1_ca`, the serial number is `159D1587CE21E9D4`.

By default, the signed certificate will expire in 365 days. You can select another value, and specify other signing details.

When prompted, copy and enter the certificate request string you saved in Step 2.

A signed certificate is displayed; save it for later use.

4. Install the signed certificate on the S3-enabled SVM:

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

When prompted, enter the certificate and private key.

You have the option to enter intermediate certificates if a certificate chain is desired.

When the private key and the CA-signed digital certificate are displayed; save them for future reference.

5. Get the public key certificate:

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

Save the public key certificate for later client-side configuration.

Example

```

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

```

Create an S3 service data policy

You can create service policies for S3 data and management services. An S3 service data policy is required to enable S3 data traffic on LIFs.

About this task

An S3 service data policy is required if you are using data LIFs and intercluster LIFs. It is not required if you are using cluster LIFs for the local tiering use case.

When a service policy is specified for a LIF, the policy is used to construct a default role, failover policy, and data protocol list for the LIF.

Although multiple protocols can be configured for SVMs and LIFs, it is a best practice for S3 to be the only protocol when serving object data.

Steps

1. Change the privilege setting to advanced:

```
set -privilege advanced
```


2. Create a service data policy:

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

The `data-core` and `data-s3-server` services are the only ones required to enable ONTAP S3, although other services can be included as needed.

Create data LIFs

If you created a new SVM, the dedicated LIFs you create for S3 access should be data LIFs.

What you'll need

- The underlying physical or logical network port must have been configured to the administrative `up` status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.

Subnets contain a pool of IP addresses that belong to the same layer 3 subnet. They are created using the `network subnet create` command.

- The LIF service policy must already exist.

About this task

- You can create both IPv4 and IPv6 LIFs on the same network port.
- If you have a large number of LIFs in your cluster, you can verify the LIF capacity supported on the cluster by using the `network interface capacity show` command and the LIF capacity supported on each node by using the `network interface capacity details show` command (at the advanced privilege level).
- If you are enabling remote FabricPool capacity (cloud) tiering, you must also configure intercluster LIFs.

Steps

1. Create a 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` is the node to which the LIF returns when the `network interface revert` command is run on the LIF.

You can also specify whether the LIF should automatically revert to the home-node and home-port with the `-auto-revert` option.

- `-home-port` is the physical or logical port to which the LIF returns when the `network interface revert` command is run on the LIF.
- You can specify an IP address with the `-address` and `-netmask` options, or you enable allocation from a subnet with the `-subnet_name` option.

- When using a subnet to supply the IP address and network mask, if the subnet was defined with a gateway, a default route to that gateway is added automatically to the SVM when a LIF is created using that subnet.
- If you assign IP addresses manually (without using a subnet), you might need to configure a default route to a gateway if there are clients or domain controllers on a different IP subnet. The `network route create man` page contains information about creating a static route within an SVM.
- For the `-firewall-policy` option, use the same default data as the LIF role.

You can create and add a custom firewall policy later if desired.



Beginning with ONTAP 9.10.1, firewall policies are deprecated and wholly replaced with LIF service policies. For more information, see [Configure firewall policies for LIFs](#).

- `-auto-revert` allows you to specify whether a data LIF is automatically reverted to its home node under circumstances such as startup, changes to the status of the management database, or when the network connection is made. The default setting is `false`, but you can set it to `false` depending on network management policies in your environment.
- The `-service-policy` option specifies the data and management services policy you created and any other policies you need.

2. If you want to assign an IPv6 address in the `-address` option:

- Use the `network ndp prefix show` command to view the list of RA prefixes learned on various interfaces.

The `network ndp prefix show` command is available at the advanced privilege level.

- Use the format `prefix:id` to construct the IPv6 address manually.

`prefix` is the prefix learned on various interfaces.

For deriving the `id`, choose a random 64-bit hexadecimal number.

3. Verify that the LIF was created successfully by using the `network interface show` command.

4. Verify that the configured IP address is reachable:

| To verify an... | Use... |
|-----------------|----------------------------|
| IPv4 address | <code>network ping</code> |
| IPv6 address | <code>network ping6</code> |

Examples

The following command shows how to create an S3 data LIF that is assigned with the `my-S3-policy` service policy:

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

The following command shows all the LIFs in cluster-1. Data LIFs datalif1 and datalif3 are configured with IPv4 addresses, and datalif4 is configured with an IPv6 address:

```
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.

Create intercluster LIFs for remote FabricPool tiering

If you are enabling remote FabricPool capacity (cloud) tiering using ONTAP S3, you must configure intercluster LIFs. You can configure intercluster LIFs on ports shared with the data network. Doing so reduces the number of ports you need for intercluster networking.

What you'll need

- The underlying physical or logical network port must have been configured to the administrative up status.

- The LIF service policy must already exist.

About this task

Intercluster LIFs are not required for local Fabric pool tiering or for serving external S3 apps.

Steps

1. List the ports in the cluster:

```
network port show
```

The following example shows the network ports in `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. Create intercluster LIFs on the system SVM:

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

The following example creates intercluster LIFs `cluster01_icl01` and `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. Verify that the intercluster LIFs were created:

```
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. Verify that the intercluster LIFs are redundant:

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

The following example shows that the intercluster LIFs cluster01_icl01 and cluster01_icl02 on the e0c port will fail over to the 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 | |

Create the S3 object store server

The ONTAP object store server manages data as S3 objects, as opposed to file or block storage provided by ONTAP NAS and SAN servers.

What you'll need

You should be prepared to enter the S3 server name as a Fully Qualified Domain Name (FQDN), which clients will use for S3 access. The FQDN must not begin with a bucket name.

You should have a self-signed CA certificate (created in previous steps) or a certificate signed by an external CA vendor. A CA certificate is not necessary for a local tiering use case, where IP traffic is going over cluster LIFs only.

About this task

When an object store server is created, a root user with UID 0 is created. No access key or secret key is generated for this root user. The ONTAP administrator must run the `object-store-server users regenerate-keys` command to set the access key and secret key for this user.



As a NetApp best practice, do not use this root user. Any client application that uses the access key or secret key of the root user has full access to all buckets and objects in the object store.

See the `vserver object-store-server` man pages for additional configuration and display options.

Example 2. Steps

CLI

1. Create the S3 server:

```
vserver object-store-server create -vserver svm_name -object-store-server  
s3_server_fqdn -certificate-name s3_server_name -comment text  
[additional_options]
```

You can specify additional options when creating the S3 server or at any time later.

- The SVM name can be either a data SVM or `Cluster` (the system SVM name) if you are configuring local tiering.
- HTTPS is enabled by default on port 443. You can change the port number with the `-secure -listener-port` option.

When HTTPS is enabled, CA certificates are required for proper integration with SSL/TLS.

- HTTP is disabled by default; when enabled, the server listens on port 80. You can enable it with the `-is-http-enabled` option or change the port number with the `-listener-port` option.

When HTTP is enabled, all the request and responses are sent over the network in clear text.

2. Verify that S3 is configured as desired:

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

Example

The following command verifies the configuration values of all object storage servers:

```
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
```

System Manager

Use this procedure if you are adding an S3 server to an existing storage VM. To add an S3 server to a new storage VM, see [Create a storage SVM for S3](#).

You should be prepared to enter IP addresses for interface role Data.

1. Enable S3 on an existing storage VM.

- a. Select the storage VM: click **Storage > Storage VMs**, select a storage VM, click **Settings**, and then click  under **S3**.
- b. Click **Enable S3**, then enter the S3 Server Name.
- c. Select the certificate type.

Whether you select system-generated certificate or one of your own, it will be required for client access.

- d. Enter the network interfaces.

2. If you selected the system-generated certificate, you see the certificate information when the new storage VM creation is confirmed. Click **Download** and save it for client access.

- The secret key will not be displayed again.
- If you need the certificate information again: click **Storage > Storage VMs**, select the storage VM, and click **Settings**.

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.