Set up NAS path failover with the CLI

ONTAP 9

NetApp
April 18, 2023

Table of Contents

Set up NAS path failover with the CLI

ONTAP 9.8 and later

About NAS path failover for ONTAP 9.8 and later CLI

This workflow guides you through the networking configuration steps to set up NAS path failover for ONTAP 9.8 and later. This workflow assumes the following:

- You want to use NAS path failover best practices in a workflow that simplifies network configuration.
- You want to use the CLI, not System Manager.
- You are configuring networking on a new system running ONTAP 9.8 or later.

If you are running an ONTAP release earlier than 9.8, you should use the following NAS path failover procedure for ONTAP 9.0 to 9.7:

- ONTAP 9.0-9.7 NAS path failover workflow

If you want network management details, you should use the network management reference material:

- Network management overview

Workflow NAS path failover

Overview

If you are already familiar with basic networking concepts, you might be able to save time setting up your network by reviewing this "hands on" workflow for NAS path failover configuration.

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. You can rely on the ONTAP defaults to manage path failover.

A SAN LIF does not migrate (unless you move it manually after the link failure). Instead, multipathing technology on the host diverts traffic to a different LIF. For more information, see SAN administration.

Worksheet for NAS path failover configuration for ONTAP 9.8 and later

You should complete all sections of the worksheet before configuring NAS path failover.

IPspace configuration

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Information	Required?	Your values
IPspace name The unique identifier of the IPspace.	Yes	

Broadcast domain configuration

A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports.

Broadcast domains are assigned to an IPspace. An IPspace can contain one or more broadcast domains.

The port to which a LIF fails over must be a member of the failover group for the LIF. For each broadcast domain created by ONTAP, a failover group with the same name is also created that contains all the ports in the broadcast domain.

Information	Required?	Your values
IPspace name The IPspace to which the broadcast domain is assigned. This IPspace must exist.	Yes	
Broadcast domain name The name of the broadcast domain. This name must be unique in the IPspace.	Yes	
MTU The maximum transmission unit value for the broadcast domain, commonly set to either **1500** or **9000**. The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain. The MTU value should match all the devices connected to that network. Note that the e0M port handling management and service processor traffic should have the MTU set to no more than 1500 bytes.	Yes	

Ports Ports are assigned to broadcast domains based on reachability. After port assignment is complete, check reachability by running the `network port reachability show` command. These ports can be physical ports, VLANs, or interface groups.	Yes	

Subnet configuration

A subnet contains pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing in the IPspace.

- When creating a LIF on an SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.
- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in a separate step when creating an SVM.
- A broadcast domain can contain one or more subnets.
- You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace's broadcast domain.
- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets in the same IPspace.
- You can assign specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet.

Information	Required?	Your values
IPspace name The IPspace to which the subnet will be assigned. This IPspace must exist.	Yes	
Subnet name The name of the subnet. This name must be unique in the IPspace.	Yes	
Broadcast domain name The broadcast domain to which the subnet will be assigned. This broadcast domain must reside in the specified IPspace.	Yes	

Subnet name and mask The subnet and mask in which the IP addresses reside.	Yes	
Gateway You can specify a default gateway for the subnet. If you do not assign a gateway when you create the subnet, you can assign one later.	No	
IP address ranges You can specify a range of IP addresses or specific IP addresses. For example, you can specify a range such as: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign to LIFs.	No	
Force update of LIF associations Specifies whether to force the update of existing LIF associations. By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided. Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.	No	

SVM configuration

You use SVMs to serve data to clients and hosts.

The values you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the Fabric-attached MetroCluster Installation and Configuration Guide or the Stretch MetroCluster Installation and Configuration Guide.

Information	Required?	Your values

SVM name The fully qualified domain name (FQDN) of the SVM. This name must be unique across cluster leagues.	Yes	
Root volume name The name of the SVM root volume.	Yes	
Aggregate name The name of the aggregate that holds the SVM root volume. This aggregate must exist.	Yes	
Security style The security style for the SVM root volume. Possible values are **ntfs**, **unix**, and **mixed**.	Yes	
IPspace name The IPspace to which the SVM is assigned. This IPspace must exist.	No	
SVM language setting The default language to use for the SVM and its volumes. If you do not specify a default language, the default SVM language is set to **C.UTF-8**. The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. You can modify The language after the SVM is created.	No	

LIF configuration

An SVM serves data to clients and hosts through one or more network logical interfaces (LIFs).

Information	Required?	Your values
SVM name The name of the SVM for the LIF.	Yes	

LIF name The name of the LIF. You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports. To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes. **Important:** If you are configuring a SMB server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the SVM must have at least one data LIF on every node in the cluster.	Yes	
Service policy Service policy for the LIF. The service policy defines which network services can use the LIF. Built-in services and service policies are available for managing data and management traffic on both data and system SVMs.	Yes	
Allowed protocols IP-based LIFs do not require allowed protocols, use the service policy row instead. Specify allowed protocols for SAN LIFs on FibreChannel ports. These are the protocols that can use that LIF. The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.	No	
Home node The node to which the LIF returns when the LIF is reverted to its home port. You should record a home node for each data LIF.	Yes	

Home port or broadcast domain Chose one of the following: **Port**: Specify the port to which the logical interface returns when the LIF is reverted to its home port. This is only done for the first LIF in the subnet of an IPspace, otherwise it is not required. **Broadcast Domain**: Specify the broadcast domain, and the system will select the appropriate port to which the logical interface returns when the LIF is reverted to its home port.	Yes	
Subnet name The subnet to assign to the SVM. All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.	Yes (if using a subnet)	

DNS configuration

You must configure DNS on the SVM before creating an NFS or SMB server.

Information	Required?	Your values
SVM name The name of the SVM on which you want to create an NFS or SMB server.	Yes	
DNS domain name A list of domain names to append to a host name when performing host- to-IP name resolution. List the local domain first, followed by the domain names for which DNS queries are most often made.	Yes	

IP addresses of the DNS servers List of IP addresses for the DNS servers that will provide name resolution for the NFS or SMB server. The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the SMB server will join. The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. SMB server creation fails if ONTAP cannot obtain the service location records through local DNS queries. The simplest way to ensure that ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers. You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers. For information about the Active Directory-integrated SRV records, see the topic How DNS Support for Active Directory Works on Microsoft TechNet.	Yes	

Dynamic DNS configuration

Before you can use dynamic DNS to automatically add DNS entries to your Active Directory- integrated DNS servers, you must configure dynamic DNS (DDNS) on the SVM.

DNS records are created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load-balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round- robin fashion.

Information	Required?	Your values
SVM name The SVM on which you want to create an NFS or SMB server.	Yes	
Whether to use DDNS Specifies whether to use DDNS. The DNS servers configured on the SVM must support DDNS. By default, DDNS is disabled.	Yes	

Whether to use secure DDNS Secure DDNS is supported only with Active Directory-integrated DNS. If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be true. By default, secure DDNS is disabled. Secure DDNS can be enabled only after a SMB server or an Active Directory account has been created for the SVM.	No	
FQDN of the DNS domain The FQDN of the DNS domain. You must use the same domain name configured for DNS name services on the SVM.	No	

Create IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Before you begin

You must be a cluster administrator to perform this task.

Step

Create an IPspace.

```
network ipspace create -ipspace ipspace1

network ipspace show
```

```
IPspace             Vserver List          Broadcast Domains
------------------- --------------------- ----------------------------
Cluster             Cluster               Cluster
Default             Cluster1              Default
ipspace1            ipspace1              -
```

The IPspace is created, along with the system SVM for the IPspace. The system SVM carries management traffic.

Move broadcast domains into IPspaces

Move the broadcast domains that the system created based on layer 2 reachability into the IPspaces you created.

Before you move the broadcast domain, you must verify the reachability of the ports in your broadcast domains.

The automatic scanning of ports can determine which ports can reach each other and place them in the same broadcast domain, but this scanning is unable to determine the appropriate IPspace. If the broadcast domain belongs in a non-default IPspace, then you must move it manually using the steps in this section.

Before you begin

Broadcast domains are automatically configured as part of cluster create and join operations. ONTAP defines the "Default" broadcast domain to be the set of ports that have layer 2 connectivity to the home port of the management interface on the first node created in the cluster. Other broadcast domains are created, if necessary, and are named **Default-1**, **Default-2**, and so forth.

When a node joins an existing cluster, their network ports automatically join existing broadcast domains based on their layer 2 reachability. If they do not have reachability to an existing broadcast domain, the ports are placed into one or more new broadcast domains.

About this task

- Ports with cluster LIFs are automatically placed into the "Cluster" IPspace.
- Ports with reachability to the home port of the node-management LIF are placed into the "Default" broadcast domain.
- Other broadcast domains are created by ONTAP automatically as part of the cluster create or join operation.
- As you add VLANs and interface groups, they are automatically placed into the appropriate broadcast domain about a minute after they are created.

Steps

1. Verify the reachability of the ports in your broadcast domains. ONTAP automatically monitors layer 2 reachability. Use the following command to verify each port has been added to a broadcast domain and has "ok" reachability.

   ```
   network port reachability show -detail
   ```

2. If necessary, move broadcast domains into other IPspaces:

   ```
   network port broadcast-domain move
   ```

   For example, if you want to move a broadcast domain from "Default" to "ips1":

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

Repair port reachability

Broadcast domains are automatically created. However, if a port is recabled, or the switch configuration changes, a port might need to be repaired into a different broadcast domain (new or existing).

Before you begin

You must be a cluster administrator to perform this task.

About this task

A command is available to automatically repair the broadcast domain configuration for a port based on the layer 2 reachability detected by ONTAP.

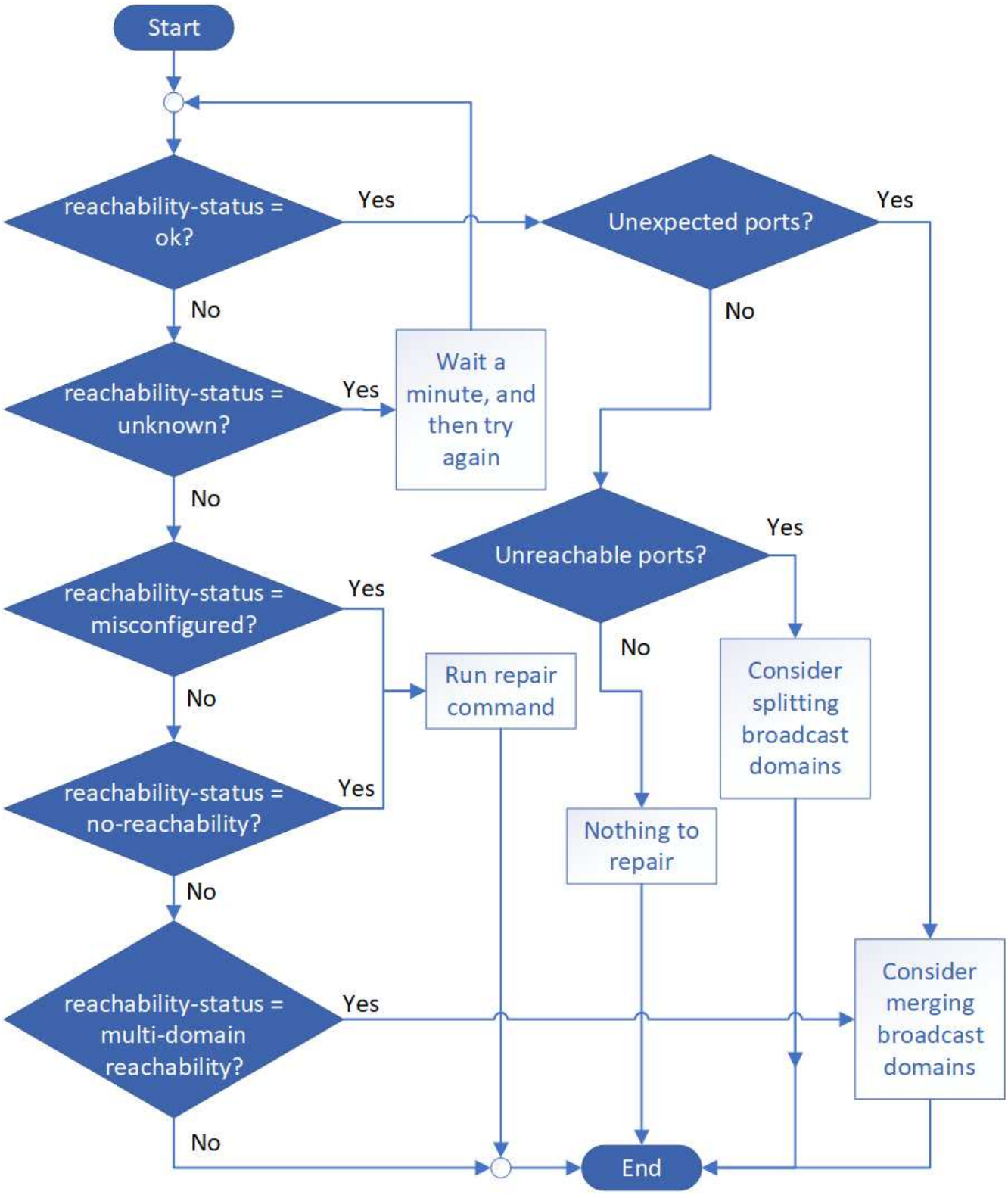
Steps

1. Check your switch configuration and cabling.
2. Check the reachability of the port:

   ```
   network port reachability show -detail -node -port
   ```

   The command output contains reachability results.

3. Use the following decision tree and table to understand the reachability results and determine what, if anything, to do next.



Reachability-status	Description

ok	The port has layer 2 reachability to its assigned broadcast domain. If the reachability-status is "ok", but there are "unexpected ports", consider merging one or more broadcast domains. For more information, see the following *Unexpected ports* row. If the reachability-status is "ok", but there are "unreachable ports", consider splitting one or more broadcast domains. For more information, see the following *Unreachable ports* row. If the reachability-status is "ok", and there are no unexpected or unreachable ports, your configuration is correct.
Unexpected ports	The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain. Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains. For more information, see Merge broadcast domains.
Unreachable ports	If a single broadcast domain has become partitioned into two different reachability sets, you can split a broadcast domain to synchronize the ONTAP configuration with the physical network topology. Typically, the list of unreachable ports defines the set of ports that should be split into another broadcast domain after you have verified that the physical and switch configuration is accurate. For more information, see Split broadcast domains.
misconfigured-reachability	The port does not have layer 2 reachability to its assigned broadcast domain; however, the port does have layer 2 reachability to a different broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to the broadcast domain to which it has reachability: `network port reachability repair -node -port`
no-reachability	The port does not have layer 2 reachability to any existing broadcast domain. You can repair the port reachability. When you run the following command, the system will assign the port to a new automatically created broadcast domain in the Default IPspace: `network port reachability repair -node -port`

multi-domain-reachability	The port has layer 2 reachability to its assigned broadcast domain; however, it also has layer 2 reachability to at least one other broadcast domain. Examine the physical connectivity and switch configuration to determine if it is incorrect or if the port's assigned broadcast domain needs to be merged with one or more broadcast domains. For more information, see Merge broadcast domains.
unknown	If the reachability-status is "unknown", then wait a few minutes and try the command again.

After you repair a port, check for displaced LIFs and VLANs. If the port was part of an interface group, you also need to understand what happened to that interface group.

LIFs

When a port is repaired and moved into a different broadcast domain, any LIFs that were configured on the repaired port will be automatically assigned a new home port. That home port is selected from the same broadcast domain on the same node, if possible. Alternatively, a home port from another node is selected, or, if no suitable home ports exist, the home port will be cleared.

If a LIF's home port is moved to another node, or is cleared, then the LIF is considered to have been "displaced". You can view these displaced LIFs with the following command:

```
displaced-interface show
```

If there are any displaced LIFs, you must either:

- Restore the home of the displaced LIF:

  ```
  displaced-interface restore
  ```

- Set the home of the LIF manually:

  ```
  network interface modify -home-port -home-node
  ```

- Remove the entry from the "displaced-interface" table if you are satisfied with the LIF's currently configured home:

  ```
  displaced-interface delete
  ```

VLANs

If the repaired port had VLANs, those VLANs are automatically deleted but are also recorded as having been "displaced". You can view these displaced VLANs:

```
displaced-vlans show
```

If there are any displaced VLANs, you must either:

- Restore the VLANs to another port:

```
displaced-vlans restore
```

- Remove the entry from the "displaced-vlans" table:

```
displaced-vlans delete
```

Interface groups

If the repaired port was part of an interface group, it is removed from that interface group. If it was the only member port assigned to the interface group, the interface group itself is removed.

Related topics

Verify your network configuration after upgrading

Monitor the reachability of network ports

Create SVMs

You must create an SVM to serve data to clients.

Before you begin

- You must be a cluster administrator to perform this task.
- You must know which security style the SVM root volume will have.

  If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

System Manager

You can use System Manager to create a storage VM.

Steps

1. Select **Storage VMs**.
2. Click + Add to create a storage VM.
3. Name the storage VM.
4. Select the access protocol:
   - SMB/CIFS, NFS
   - iSCSI
   - FC
   - NVMe
     a. If you select **Enable SMB/CIFS**, complete the following configuration:

Field or check box	Description
Administrator Name	Specify the administrator user name for the SMB/CIFS storage VM.
Password	Specify the administrator password for the SMB/CIFS storage VM.
Server Name	Specify the server name for the SMB/CIFS storage VM.
Active Directory Domain	Specify the active directory domain to provide user authentication for the SMB/CIFS storage VM.
Organizational Unit	Specify the organizational unit within the Active Directory domain associated with the SMB/CIFS server. "CN=Computers" is the default value, which can be modified.
Encrypts data while accessing the shares in the storage VM	Select this check box to encrypt data using SMB 3.0 to prevent unauthorized file access on the shares in the SMB/CIFS storage VM.
Domains	Add, remove, or reorder the domains listed for the SMB/CIFS storage VM.
Name Servers	Add, remove, or reorder the name servers for the SMB/CIFS storage VM.

Default Language	Specifies the default language-encoding setting for the storage VM and its volumes. Use the CLI to change the settings for individual volumes within a storage VM.
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

b. If you select **Enable NFS**, complete the following configuration:

Field or check box	Description
Allow NFS client access check box	Select this check box when all volumes created on the NFS storage VM should use the root volume path "/" to mount and traverse. Add rules to the export policy "default" to allow uninterrupted mount traversal.

Rules	Click + Add to create rules. • Client Specification: Specify the host names, IP addresses, netgroups, or domains. • Access Protocols: Select a combination of the following options: ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Access Details: For each type of user, specify the level of access, either read-only, read/writer, or superuser. User types include: ◦ All ◦ All (as anonymous user) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM Save the rule.
Default Language	Specifies the default language-encoding setting for the storage VM and its volumes. Use the CLI to change the settings for individual volumes within a storage VM.
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

c. If you select **Enable iSCSI**, complete the following configuration:

Field or check box	Description
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

d. If you select **Enable FC**, complete the following configuration:

Field or check box	Description
Configure FC Ports	Select the network interfaces on the nodes you want to include in the storage VM. Two network interfaces per node are recommended.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

e. If you select **Enable NVMe/FC**, complete the following configuration:

Field or check box	Description
Configure FC Ports	Select the network interfaces on the nodes you want to include in the storage VM. Two network interfaces per node are recommended.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

f. If you select **Enable NVMe/TCP**, complete the following configuration:

Field or check box	Description
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

5. Save your changes.

CLI

Use the ONTAP CLI to create a subnet.

Steps

1. Determine which aggregates are candidates for containing the SVM root volume.

   ```
   storage aggregate show -has-mroot false
   ```

   You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra free space on the root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.

   If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.
3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

   ```
   vserver create -language ?
   ```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the Snapshot policy you want to use:

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver vserver_name
```

6. Create an SVM:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Verify that the SVM configuration is correct.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.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, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In this example, the command creates the SVM named "vs1" in IPspace "ipspace1". The root volume is named "vs1_root" and is created on aggr3 with NTFS security style.

Create LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data.

Before you begin

You must be a cluster administrator to perform this task.

About this task

Beginning with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

You should not configure LIFs that carry SMB traffic to automatically revert to their home nodes. This recommendation is mandatory if the SMB server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.

Steps

1. Determine which broadcast domain ports you want to use for the LIF.

   `network port broadcast-domain show -ipspace` *`ipspace1`*

   ```
   IPspace     Broadcast                         Update
   Name        Domain name   MTU   Port List     Status Details
   ipspace1
               default       1500
                                   node1:e0d     complete
                                   node1:e0e     complete
                                   node2:e0d     complete
                                   node2:e0e     complete
   ```

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

   `network subnet show -ipspace` *`ipspace1`*

3. Create one or more LIFs on the ports you want to use to access data.

   `network interface create -vserver` *`vs1`* `-lif` *`lif1`* `-home-node` *`node1`* `-home-port` *`e0d`* `-service-policy` *`default-data-files`* `-subnet-name` *`ipspace1`*

4. Verify that the LIF interface configuration is correct.

   `network interface show -vserver vs1`

```
           Logical    Status     Network          Current   Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node      Port    Home
---------- ---------- ---------- ---------------- --------- ------- ----
vs1
            lif1       up/up      10.0.0.128/24   node1     e0d     true
```

5. Verify that the failover group configuration is as desired.

   `network interface show -failover -vserver vs1`

```
          Logical    Home       Failover        Failover
Vserver   interface  Node:Port  Policy          Group
--------- ---------- ---------  ---------       --------
vs1
          lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

Configure DNS services

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are files and dns.

You must ensure that dns is one of the sources before you create the SMB server.

> To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

Steps

1. Determine what the current configuration is for the hosts name services database. In this example, the hosts name service database uses the default settings.

   `vserver services name-service ns-switch show -vserver vs1 -database hosts`

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. Perform the following actions, if required.
   a. Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

      In this example, the hosts database is configured to use DNS and local files in that order.

      `vserver services name-service ns-switch modify -vserver vs1 -database hosts -sources dns,files`

   b. Verify that the name services configuration is correct.

      `vserver services name-service ns-switch show -vserver vs1 -database hosts`

      ```
      Vserver: vs1
      Name Service Switch Database: hosts
      Name Service Source Order: dns, files
      ```

3. Configure DNS services.

   `vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51`

   > The vserver services name-service dns create command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

   ```
   Vserver: vs1
   Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
   Enable/Disable DNS: enabled Timeout (secs): 2
   Maximum Attempts: 1
   ```

5. Validate the status of the name servers.

   `vserver services name-service dns check -vserver vs1`

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified fully qualified domain name (FQDN) must be unique:

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                        Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                             Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see RFC 1123.

Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates

vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

ONTAP 9.7 and earlier

Set up NAS path failover with the CLI (ONTAP 9.0-9.7)

This workflow guides you through the networking configuration steps to set up NAS path failover for ONTAP 9.0 - 9.7. This workflow assumes the following:

- You want to use NAS path failover best practices that simplify network configuration.
- You want to use the CLI, not System Manager.
- You are configuring networking on a new system running ONTAP 9.0 to 9.7.

If you are running an ONTAP release later than 9.7, you should use the NAS path failover procedure for ONTAP 9.8 or later:

- ONTAP 9.8 and later NAS path failover workflow

If you want details about network components and management, you should use the network management reference material:

- Network management overview

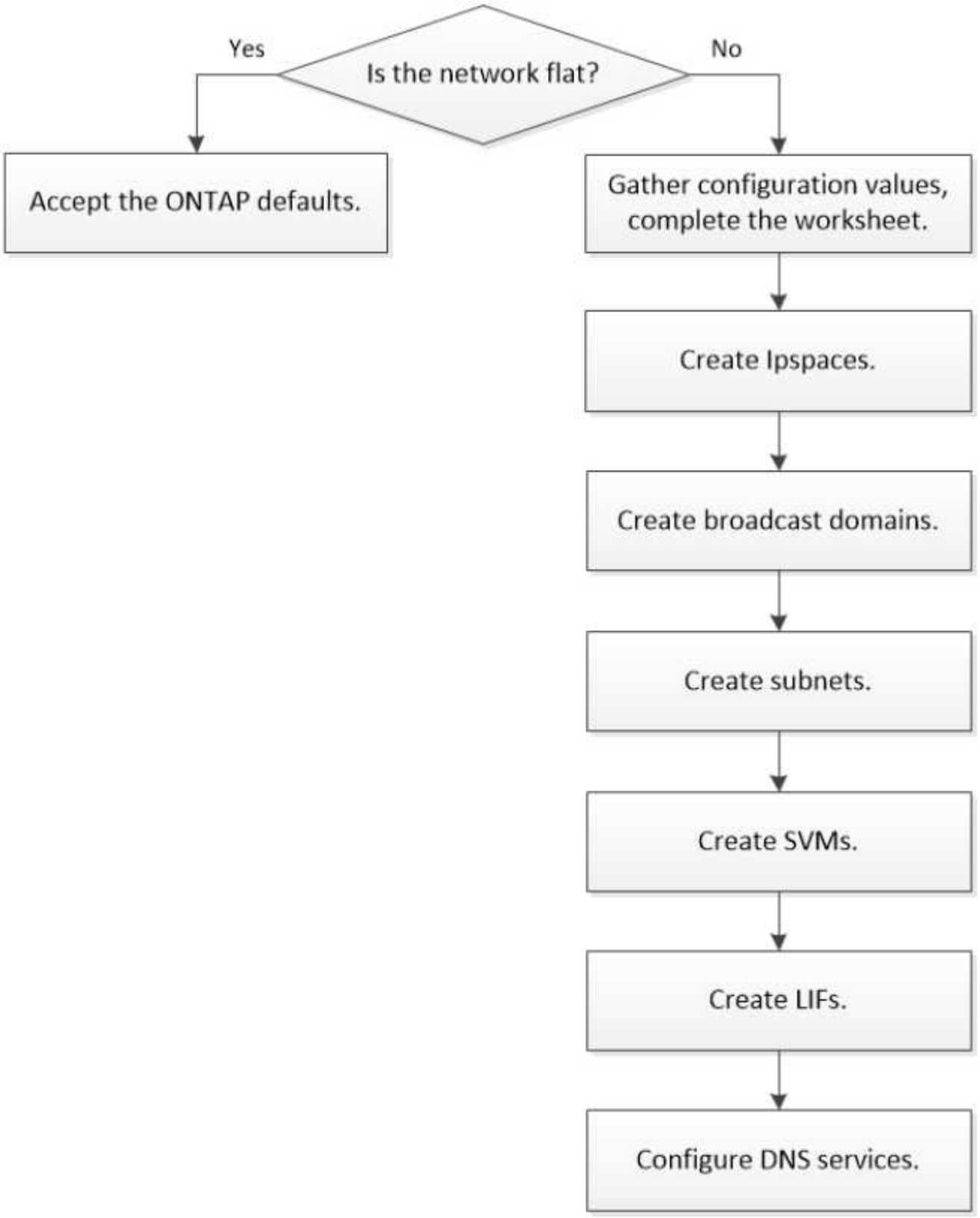
Workflow NAS path failover

Overview

If you are already familiar with basic networking concepts, you might be able to save time setting up your network by reviewing this "hands on" workflow for NAS path failover configuration.

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. If your network is flat, you can rely on the ONTAP defaults to manage path failover. Otherwise, you should configure

path failover following the steps in this workflow.



A SAN LIF does not migrate (unless you move it manually after the link failure). Instead, multipathing technology on the host diverts traffic to a different LIF. For more information, see SAN administration.

Worksheet for NAS path failover configuration for ONTAP 9.0 - 9.7

You should complete all sections of the worksheet before configuring NAS path failover.

IPspace configuration

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Information	Required?	Your values
IPspace name • The name of the IPspace. • The name must be unique in the cluster.	Yes	

Broadcast domain configuration

A broadcast domain groups ports that belong in the same Layer 2 network and sets the MTU for the broadcast domain ports.

Broadcast domains are assigned to an IPspace. An IPspace can contain one or more broadcast domains.

The port to which a LIF fails over must be a member of the failover group for the LIF. When you create a broadcast domain, ONTAP automatically creates a failover group with the same name. The failover group contains all the ports assigned to the broadcast domain.

Information	Required?	Your values
IPspace name • The IPspace to which the broadcast domain is assigned. • The IPspace must exist.	Yes	
Broadcast domain name • The name of the broadcast domain. • This name must be unique in the IPspace.	Yes	

MTU • The MTU of the broadcast domain. • Commonly set to either **1500** or **9000**. • The MTU value is applied to all ports in the broadcast domain and to any ports that are later added to the broadcast domain. The MTU value should match all the devices connected to that network. Note that the e0M port handling management and service processor traffic should have the MTU set to no more than 1500 bytes.	Yes	
Ports • The network ports to add to the broadcast domain. • The ports assigned to the broadcast domain can be physical ports, VLANs, or interface groups (ifgroups). • If a port is in another broadcast domain, it must be removed before it can be added to the broadcast domain. • Ports are assigned by specifying both the node name and port: for example, node1:e0d.	Yes	

Subnet configuration

A subnet contains pools of IP addresses and a default gateway that can be assigned to LIFs used by SVMs residing in the IPspace.

- When creating a LIF on an SVM, you can specify the name of the subnet instead of supplying an IP address and a subnet.
- Since a subnet can be configured with a default gateway, you do not have to create the default gateway in a separate step when creating an SVM.

- A broadcast domain can contain one or more subnets.
  You can configure SVM LIFs that are on different subnets by associating more than one subnet with the IPspace's broadcast domain.
- Each subnet must contain IP addresses that do not overlap with IP addresses assigned to other subnets in the same IPspace.
- You can assign specific IP addresses to SVM data LIFs and create a default gateway for the SVM instead of using a subnet.

Information	Required?	Your values
IPspace name • The IPspace to which the subnet will be assigned. • The IPspace must exist.	Yes	
Subnet name • The name of the subnet. • The name must be unique in the IPspace.	Yes	
Broadcast domain name • The broadcast domain to which the subnet will be assigned. • The broadcast domain must reside in the specified IPspace.	Yes	
Subnet name and mask • The subnet and mask in which the IP addresses reside.	Yes	
Gateway • You can specify a default gateway for the subnet. • If you do not assign a gateway when you create the subnet, you can assign one to the subnet at any time.	No	

IP address ranges • You can specify a range of IP addresses or specific IP addresses. For example, you can specify a range such as: `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` • If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign to LIFs.	No	
Force update of LIF associations • Specifies whether to force the update of existing LIF associations. • By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided. • Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.	No	

SVM configuration

You use SVMs to serve data to clients and hosts.

The values you record are for creating a default data SVM. If you are creating a MetroCluster source SVM, see the Install a fabric-attached MetroCluster or the Install a stretch MetroCluster.

Information	Required?	Your values
SVM name • The name of the SVM. • You should use a fully qualified domain name (FQDN) to ensure unique SVM names across cluster leagues.	Yes	

Root volume name • The name of the SVM root volume.	Yes	
Aggregate name • The name of the aggregate that holds the SVM root volume. • This aggregate must exist.	Yes	
Security style • The security style for the SVM root volume. • Possible values are **ntfs**, **unix**, and **mixed**.	Yes	
IPspace name • The IPspace to which the SVM is assigned. • This IPspace must exist.	No	
SVM language setting • The default language to use for the SVM and its volumes. • If you do not specify a default language, the default SVM language is set to **C.UTF-8**. • The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM. You can modify The language after the SVM is created.	No	

LIF configuration

An SVM serves data to clients and hosts through one or more network logical interfaces (LIFs).

Information	Required?	Your values
SVM name • The name of the SVM for the LIF.	Yes	

LIF name • The name of the LIF. • You can assign multiple data LIFs per node, and you can assign LIFs to any node in the cluster, provided that the node has available data ports. • To provide redundancy, you should create at least two data LIFs for each data subnet, and the LIFs assigned to a particular subnet should be assigned home ports on different nodes. **Important:** If you are configuring a SMB server to host Hyper-V or SQL Server over SMB for nondisruptive operation solutions, the SVM must have at least one data LIF on every node in the cluster.	Yes	
LIF role • The role of the LIF. • Data LIFs are assigned the data role.	Yes Deprecated from ONTAP 9.6	data
Service policy Service policy for the LIF. The service policy defines which network services can use the LIF. Built-in services and service policies are available for managing data and management traffic on both data and system SVMs.	Yes Beginning with ONTAP 9.6	

Allowed protocols • The protocols that can use the LIF. • By default, SMB, NFS, and FlexCache are allowed. The FlexCache protocol enables a volume to be used as an origin volume for a FlexCache volume on a system running Data ONTAP operating in 7-Mode. The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.	No	
Home node • The node to which the LIF returns when the LIF is reverted to its home port. • You should record a home node for each data LIF.	Yes	
Home port or broadcast domain • The port to which the logical interface returns when the LIF is reverted to its home port. • You should record a home port for each data LIF.	Yes	
Subnet name • The subnet to assign to the SVM. • All data LIFs used to create continuously available SMB connections to application servers must be on the same subnet.	Yes (if using a subnet)	

DNS configuration

You must configure DNS on the SVM before creating an NFS or SMB server.

Information	Required?	Your values
SVM name • The name of the SVM on which you want to create an NFS or SMB server.	Yes	
DNS domain name • A list of domain names to append to a host name when performing host- to-IP name resolution. • List the local domain first, followed by the domain names for which DNS queries are most often made.	Yes	

IP addresses of the DNS servers * List of IP addresses for the DNS servers that will provide name resolution for the NFS or SMB server. * The listed DNS servers must contain the service location records (SRV) needed to locate the Active Directory LDAP servers and domain controllers for the domain that the SMB server will join. The SRV record is used to map the name of a service to the DNS computer name of a server that offers that service. SMB server creation fails if ONTAP cannot obtain the service location records through local DNS queries. The simplest way to ensure that ONTAP can locate the Active Directory SRV records is to configure Active Directory-integrated DNS servers as the SVM DNS servers. You can use non-Active Directory-integrated DNS servers provided that the DNS administrator has manually added the SRV records to the DNS zone that contains information about the Active Directory domain controllers. * For information about the Active Directory-integrated SRV records, see the topic How DNS Support for Active Directory Works on Microsoft TechNet.	Yes	

Dynamic DNS configuration

Before you can use dynamic DNS to automatically add DNS entries to your Active Directory- integrated DNS servers, you must configure dynamic DNS (DDNS) on the SVM.

DNS records are created for every data LIF on the SVM. By creating multiple data LIFS on the SVM, you can load-balance client connections to the assigned data IP addresses. DNS load balances connections that are made using the host name to the assigned IP addresses in a round- robin fashion.

Information	Required?	Your values
SVM name • The SVM on which you want to create an NFS or SMB server.	Yes	

Whether to use DDNS • Specifies whether to use DDNS. • The DNS servers configured on the SVM must support DDNS. By default, DDNS is disabled.	Yes	
Whether to use secure DDNS • Secure DDNS is supported only with Active Directory-integrated DNS. • If your Active Directory-integrated DNS allows only secure DDNS updates, the value for this parameter must be true. • By default, secure DDNS is disabled. • Secure DDNS can be enabled only after a SMB server or an Active Directory account has been created for the SVM.	No	
FQDN of the DNS domain • The FQDN of the DNS domain. • You must use the same domain name configured for DNS name services on the SVM.	No	

Create IPspaces

You can use an IPspace to create a distinct IP address space for each SVM in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

Before you begin

You must be a cluster administrator to perform this task.

Step

Create an IPspace.

```
network ipspace create -ipspace ipspace1

network ipspace show
```

```
IPspace              Vserver List          Broadcast Domains
-------------------- --------------------- ----------------------------
Cluster              Cluster               Cluster
Default              Cluster1              Default
ipspace1             ipspace1              -
```

The IPspace is created, along with the system SVM for the IPspace. The system SVM carries management traffic.

Determining which ports can be used for a broadcast domain

Before you can configure a broadcast domain to add to the new IPspace, you must determine what ports are available for the broadcast domain.

This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

Before you begin

You must be a cluster administrator to perform this task.

About this task

- Ports can be physical ports, VLANs, or interface groups (ifgroups).
- The ports that you want to add to the new broadcast domain cannot be assigned to an existing broadcast domain.
- If the ports that you want to add to the broadcast domain are already in another broadcast domain (for example, the Default broadcast domain in the Default IPspace), you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.
- Ports that have LIFs assigned to them cannot be removed from a broadcast domain.
- Because the cluster management and node management LIFs are assigned to the Default broadcast domain in the Default IPspace, the ports assigned to these LIFs cannot be removed from the Default broadcast domain.

Steps

1. Determine the current port assignments.

   ```
   network port show
   ```

```
Node   Port IPspace  Broadcast Domain Link   MTU  Admin/Oper
------ ---- -------  ---------------- ----- ----  ------------
node1
       e0a  Cluster  Cluster          up    9000  auto/1000
       e0b  Cluster  Cluster          up    9000  auto/1000
       e0c  Default  Default          up    1500  auto/1000
       e0d  Default  Default          up    1500  auto/1000
       e0e  Default  Default          up    1500  auto/1000
       e0f  Default  Default          up    1500  auto/1000
       e0g  Default  Default          up    1500  auto/1000
node2
       e0a  Cluster  Cluster          up    9000  auto/1000
       e0b  Cluster  Cluster          up    9000  auto/1000
       e0c  Default  Default          up    1500  auto/1000
       e0d  Default  Default          up    1500  auto/1000
       e0e  Default  Default          up    1500  auto/1000
       e0f  Default  Default          up    1500  auto/1000
       e0g  Default  Default          up    1500  auto/1000
```

In this example, the output from the command provides the following information:

- Ports `e0c`, `e0d`, `e0e`, `e0f`, and `e0g` on each node are assigned to the Default broadcast domain.
- These ports are potentially available to use in the broadcast domain of the IPspace that you want to create.

2. Determine which ports in the Default broadcast domain are assigned to LIF interfaces, and therefore cannot be moved to a new broadcast domain.

   `network interface show`

```
         Logical      Status     Network          Current   Current Is
Vserver  Interface    Admin/Oper Address/Mask     Node      Port    Home
-------  ----------   ---------- ------------   --------- -------  ----
Cluster
         node1_clus1  up/up       10.0.2.40/24   node1     e0a     true
         node1_clus2  up/up       10.0.2.41/24   node1     e0b     true
         node2_clus1  up/up       10.0.2.42/24   node2     e0a     true
         node2_clus2  up/up       10.0.2.43/24   node2     e0b     true

cluster1
         cluster_mgmt up/up       10.0.1.41/24   node1     e0c     true
         node1_mgmt   up/up       10.0.1.42/24   node1     e0c     true
         node2_mgmt   up/up       10.0.1.43/24   node2     e0c     true
```

In the following example, the output from the command provides the following information:

- The node ports are assigned to port `e0c` on each node and the cluster administrative LIF's home node is on `e0c` on `node1`.
- Ports `e0d`, `e0e`, `e0f`, and `e0g` on each node are not hosting LIFs and can be removed from the Default broadcast domain and then added to a new broadcast domain for the new IPspace.

Remove ports from a broadcast domain

If the ports that you want to add to the new broadcast domain are already in another broadcast domain, you must remove the ports from that broadcast domain before assigning them to the new broadcast domain.

This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

Before you begin

You must be a cluster administrator to perform this task.

Steps

1. Remove ports from the broadcast domain specifying the following:
   - IPspace, `Default` in the following sample.
   - Broadcast domain, `Default` in the following sample.
   - Ports, using the node and port syntax, `node1:e0d,node1:e0e,node2:e0d,node2:e0e` in the following sample.

   ```
   network port broadcast-domain remove-ports -ipspace Default
   -broadcast-domain Default -ports
   node1:e0d,node1:e0e,node2:e0d,node2:e0e
   ```

2. Verify that the ports were removed from the broadcast domain:

   ```
   network port show
   ```

Create a broadcast domain

You must create a broadcast domain for a custom IPspace. The SVMs created in the IPspace use the ports in the broadcast domain.

This task is relevant for ONTAP 9.0 - 9.7, not ONTAP 9.8.

Before you begin

You must be a cluster administrator to perform this task.

About this task

The port to which a LIF fails over must be a member of the failover group for the LIF. When you create a broadcast domain, ONTAP automatically creates a failover group with the same name. The failover group contains all the ports assigned to the broadcast domain.

Steps

1. Create a broadcast domain.

```
network port broadcast-domain create -ipspace ipspace1 -broadcast-domain
-ipspace1 -mtu 1500 -ports node1:e0d,node1:e0e,node2:e0d,node2:e0e
```

2. Verify that the broadcast domain configuration is correct.
   a. Verify the broadcast domain is correct:

      ```
      network port broadcast-domain show
      ```

   b. Verify the network port is correct:

      ```
      network port show
      ```

   c. Verify the failover group names and failover targets are correct:

      ```
      network interface failover-groups show
      ```

Create a subnet

You can create a subnet to allocate specific blocks of IPv4 or IPv6 addresses to be used later when you create LIFs for the SVM.

This enables you to create LIFs more easily by specifying a subnet name instead of having to specify IP address and network mask values for each LIF.

Before you begin

You must be a cluster administrator to perform this task.

Procedure

The procedure you follow depends on the interface that you use—System Manager or the CLI:

System Manager

Beginning with ONTAP 9.12.0, you can use System Manager to create a subnet.

Steps

1. Select **Network > Overview > Subnets**.
2. Click + Add to create a subnet.
3. Name the subnet.
4. Specify the subnet IP address.
5. Set the subnet mask.
6. Define the range of IP addresses that comprise the subnet.
7. If useful, specify a gateway.
8. Select the broadcast domain to which the subnet belongs.
9. Save your changes.
   a. If the IP address or range entered is already used by an interface, the following message is displayed:
   `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. When you click **OK**, the existing LIF will be associated with the subnet.

CLI

Use the CLI to create a subnet.

Steps

1. Create a subnet.

   ```
   network subnet create -broadcast-domain ipspace1 -ipspace ipspace1 -subnet
   -name ipspace1 -subnet 10.0.0.0/24 -gateway 10.0.0.1 -ip-ranges
   "10.0.0.128-10.0.0.130,10.0.0.132"
   ```

   The subnet name can be either a subnet IP value such as `192.0.2.0/24` or a string such as `ipspace1` like the one used in this example.

2. Verify that the subnet configuration is correct.

   The output from this example shows information about the subnet named ipspace1 in the ipspace1 IPspace. The subnet belongs to the broadcast domain name ipspace1. You can assign the IP addresses in this subnet to data LIFs for SVMs created in the ipspace1 IPspace.

   ```
   network subnet show -ipspace ipspace1
   ```

Create SVMs

You must create an SVM to serve data to clients.

Before you begin

- You must be a cluster administrator to perform this task.
- You must know which security style the SVM root volume will have.

  If you plan to implement a Hyper-V or SQL Server over SMB solution on this SVM, you should use NTFS security style for the root volume. Volumes that contain Hyper-V files or SQL database files must be set to NTFS security at the time they are created. By setting the root volume security style to NTFS, you ensure that you do not inadvertently create UNIX or mixed security-style data volumes.

System Manager

You can use System Manager to create a storage VM.

Steps

1. Select **Storage VMs**.
2. Click + Add to create a storage VM.
3. Name the storage VM.
4. Select the access protocol:
   - SMB/CIFS, NFS
   - iSCSI
   - FC
   - NVMe
     a. If you select **Enable SMB/CIFS**, complete the following configuration:

Field or check box	Description
Administrator Name	Specify the administrator user name for the SMB/CIFS storage VM.
Password	Specify the administrator password for the SMB/CIFS storage VM.
Server Name	Specify the server name for the SMB/CIFS storage VM.
Active Directory Domain	Specify the active directory domain to provide user authentication for the SMB/CIFS storage VM.
Organizational Unit	Specify the organizational unit within the Active Directory domain associated with the SMB/CIFS server. "CN=Computers" is the default value, which can be modified.
Encrypts data while accessing the shares in the storage VM	Select this check box to encrypt data using SMB 3.0 to prevent unauthorized file access on the shares in the SMB/CIFS storage VM.
Domains	Add, remove, or reorder the domains listed for the SMB/CIFS storage VM.
Name Servers	Add, remove, or reorder the name servers for the SMB/CIFS storage VM.

Default Language	Specifies the default language-encoding setting for the storage VM and its volumes. Use the CLI to change the settings for individual volumes within a storage VM.
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

b. If you select **Enable NFS**, complete the following configuration:

Field or check box	Description
Allow NFS client access check box	Select this check box when all volumes created on the NFS storage VM should use the root volume path "/" to mount and traverse. Add rules to the export policy "default" to allow uninterrupted mount traversal.

Rules	Click + Add to create rules. • Client Specification: Specify the host names, IP addresses, netgroups, or domains. • Access Protocols: Select a combination of the following options: ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • Access Details: For each type of user, specify the level of access, either read-only, read/writer, or superuser. User types include: ◦ All ◦ All (as anonymous user) ◦ UNIX ◦ Kerberos 5 ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM Save the rule.
Default Language	Specifies the default language-encoding setting for the storage VM and its volumes. Use the CLI to change the settings for individual volumes within a storage VM.
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

c. If you select **Enable iSCSI**, complete the following configuration:

Field or check box	Description
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

d. If you select **Enable FC**, complete the following configuration:

Field or check box	Description
Configure FC Ports	Select the network interfaces on the nodes you want to include in the storage VM. Two network interfaces per node are recommended.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

e. If you select **Enable NVMe/FC**, complete the following configuration:

Field or check box	Description
Configure FC Ports	Select the network interfaces on the nodes you want to include in the storage VM. Two network interfaces per node are recommended.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

f. If you select **Enable NVMe/TCP**, complete the following configuration:

Field or check box	Description
Network Interface	For each network interface you configure for the storage VM, select an existing subnet (if at least one exists) or specify **Without a subnet** and complete the **IP Address** and **Subnet Mask** fields. If useful, select the **Use the same subnet mask and gateway for all of the following interfaces** check box. You can allow the system to automatically select the home port, or manually select the one you want to use from the list.
Manage administrator account	Select this check box if you want to manage the storage VM administrator account. When selected, specify the user name, password, confirm the password, and indicate if you want to add a network interface for storage VM management.

5. Save your changes.

CLI

Use the ONTAP CLI to create a subnet.

Steps

1. Determine which aggregates are candidates for containing the SVM root volume.

   ```
   storage aggregate show -has-mroot false
   ```

   You must choose an aggregate that has at least 1 GB of free space to contain the root volume. If you intend to configure NAS auditing on the SVM, you must have a minimum of 3 GB of extra free space on the root aggregate, with the extra space being used to create the auditing staging volume when auditing is enabled.

   If NAS auditing is already enabled on an existing SVM, the aggregate's staging volume is created immediately after aggregate creation is successfully completed.

2. Record the name of the aggregate on which you want to create the SVM root volume.
3. If you plan on specifying a language when you create the SVM and do not know the value to use, identify and record the value of the language you want to specify:

   ```
   vserver create -language ?
   ```

4. If you plan on specifying a Snapshot policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the Snapshot policy you want to use:

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. If you plan on specifying a quota policy when you create the SVM and do not know the name of the policy, list the available policies and identify and record the name of the quota policy you want to use:

```
volume quota policy show -vserver vserver_name
```

6. Create an SVM:

```
vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
IPspace_name] [-language <language>] [-snapshot-policy
snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
```

```
vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
-rootvolume-security-style ntfs -ipspace ipspace1 -language
en_US.UTF-8
```

```
[Job 72] Job succeeded: Vserver creation completed
```

7. Verify that the SVM configuration is correct.

```
vserver show -vserver vs1
```

```
Vserver: vs1
Vserver Type: data
Vserver Subtype: default
Vserver UUID: 11111111-1111-1111-1111-111111111111
Root Volume: vs1_root
Aggregate: aggr3
NIS Domain: -
Root Volume Security Style: ntfs
LDAP Client: -
Default Volume Language Code: en_US.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, ndmp
Disallowed Protocols: fcp, iscsi
QoS Policy Group: -
Config Lock: false
IPspace Name: ipspace1
Is Vserver Protected: false
```

In this example, the command creates the SVM named "vs1" in IPspace "ipspace1". The root volume is named "vs1_root" and is created on aggr3 with NTFS security style.

Create LIFs

An SVM serves data to clients through one or more network logical interfaces (LIFs). You must create LIFs on the ports you want to use to access data.

Before you begin

You must be a cluster administrator to perform this task.

About this task

Beginning with ONTAP 9.7, ONTAP automatically chooses the home port of a LIF, as long as at least one LIF already exists in the same subnet in that IPspace. ONTAP chooses a home-port in the same broadcast domain as other LIFs in that subnet. You can still specify a home port, but it is no longer required (unless no LIFs yet exist in that subnet in the specified IPspace).

You should not configure LIFs that carry SMB traffic to automatically revert to their home nodes. This recommendation is mandatory if the SMB server is to host a solution for nondisruptive operations with Hyper-V or SQL Server over SMB.

Steps

1. Determine which broadcast domain ports you want to use for the LIF.

   `network port broadcast-domain show -ipspace` *`ipspace1`*

   ```
   IPspace     Broadcast                         Update
   Name        Domain name   MTU   Port List     Status Details
   ipspace1
               default       1500
                                   node1:e0d     complete
                                   node1:e0e     complete
                                   node2:e0d     complete
                                   node2:e0e     complete
   ```

2. Verify that the subnet you want to use for the LIFs contains sufficient unused IP addresses.

   `network subnet show -ipspace` *`ipspace1`*

3. Create one or more LIFs on the ports you want to use to access data.

   `network interface create -vserver` *`vs1`* `-lif` *`lif1`* `-home-node` *`node1`* `-home-port` *`e0d`* `-service-policy` *`default-data-files`* `-subnet-name` *`ipspace1`*

4. Verify that the LIF interface configuration is correct.

   `network interface show -vserver vs1`

```
           Logical    Status     Network          Current   Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node      Port    Home
---------- ---------- ---------- ---------------- --------- ------- ----
vs1
            lif1       up/up      10.0.0.128/24   node1     e0d     true
```

5. Verify that the failover group configuration is as desired.

   `network interface show -failover -vserver vs1`

```
          Logical    Home       Failover        Failover
Vserver   interface  Node:Port  Policy          Group
--------- ---------- ---------  ---------       --------
vs1
          lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

Configure DNS services

You must configure DNS services for the SVM before creating an NFS or SMB server. Generally, the DNS name servers are the Active Directory-integrated DNS servers for the domain that the NFS or SMB server will join.

About this task

Active Directory-integrated DNS servers contain the service location records (SRV) for the domain LDAP and domain controller servers. If the SVM cannot find the Active Directory LDAP servers and domain controllers, NFS or SMB server setup fails.

SVMs use the hosts name services ns-switch database to determine which name services to use and in which order when looking up information about hosts. The two supported name services for the hosts database are `files` and `dns`.

You must ensure that `dns` is one of the sources before you create the SMB server.

> To view the statistics for DNS name services for the mgwd process and SecD process, use the Statistics UI.

Steps

1. Determine what the current configuration is for the `hosts` name services database.

   In this example, the hosts name service database uses the default settings.

   `vserver services name-service ns-switch show -vserver vs1 -database hosts`

```
                    Vserver: vs1
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

2. Perform the following actions, if required.
   a. Add the DNS name service to the hosts name service database in the desired order, or reorder the sources.

      In this example, the hosts database is configured to use DNS and local files in that order.

      `vserver services name-service ns-switch modify -vserver vs1 -database hosts -sources dns,files`

   b. Verify that the name services configuration is correct.

      `vserver services name-service ns-switch show -vserver vs1 -database hosts`

3. Configure DNS services.

   `vserver services name-service dns create -vserver vs1 -domains example.com,example2.com -name-servers 10.0.0.50,10.0.0.51`

   > The vserver services `name-service dns create` command performs an automatic configuration validation and reports an error message if ONTAP is unable to contact the name server.

4. Verify that the DNS configuration is correct and that the service is enabled.

```
           Vserver: vs1
           Domains: example.com, example2.com Name
           Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
  Maximum Attempts: 1
```

5. Validate the status of the name servers.

   `vserver services name-service dns check -vserver vs1`

```
Vserver  Name Server  Status  Status Details
-------  -----------  ------  ----------------------
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

Configure dynamic DNS on the SVM

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified fully qualified domain name (FQDN) must be unique:

- For NFS, the value specified in `-vserver-fqdn` as part of the `vserver services name-service dns dynamic-update` command becomes the registered FQDN for the LIFs.
- For SMB, the values specified as the CIFS server NetBIOS name and the CIFS server fully qualified domain name become the registered FQDN for the LIFs. This is not configurable in ONTAP. In the following scenario, the LIF FQDN is "CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                               Authentication Style: domain
                  CIFS Server Administrative Status: up
                             CIFS Server Description:
                             List of NetBIOS Aliases: -
```

To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant. For more information, see RFC 1123.

Steps

1. Configure DDNS on the SVM:

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Configure dynamic DNS services

If you want the Active Directory-integrated DNS server to dynamically register the DNS records of an NFS or SMB server in DNS, you must configure dynamic DNS (DDNS) on the SVM.

Before you begin

DNS name services must be configured on the SVM. If you are using secure DDNS, you must use Active Directory-integrated DNS name servers and you must have created either an NFS or SMB server or an Active Directory account for the SVM.

About this task

The specified FQDN must be unique.

> To avoid a configuration failure of an SVM FQDN that is not compliant to RFC rules for DDNS updates, use an FQDN name that is RFC compliant.

Steps

1. Configure DDNS on the SVM:

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates

vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

   Asterisks cannot be used as part of the customized FQDN. For example, `*.netapp.com` is not valid.

2. Verify that the DDNS configuration is correct:

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

Copyright information

Trademark information