# **■** NetApp

# Workflow NAS path failover

ONTAP 9

NetApp April 18, 2023

# **Table of Contents**

Workflow NAS path failover	1
Overview	1
Worksheet for NAS path failover configuration for ONTAP 9.0 - 9.7	3
Create IPspaces	12
Determining which ports can be used for a broadcast domain	13
Remove ports from a broadcast domain	15
Create a broadcast domain	15
Create a subnet	16
Create SVMs	17
Create LIFs.	25
Configure DNS services	26
Configure dynamic DNS services	29

# **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.



(i)

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	Yes	
<ul><li>The name of the IPspace.</li><li>The name must be unique in the cluster.</li></ul>		

### **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
<ul> <li>Pspace name</li> <li>The IPspace to which the broadcast domain is assigned.</li> <li>The IPspace must exist.</li> </ul>	Yes	
<ul> <li>Broadcast domain name</li> <li>The name of the broadcast domain.</li> <li>This name must be unique in the IPspace.</li> </ul>	Yes	

MTU		Yes	
The Momain domain	ITU of the broadcast in.		
• Comn 9000.	nonly set to either <b>1500</b> or		
ports i	ITU value is applied to all in the broadcast domain any ports that are later to the broadcast domain.		
i	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.		
Ports		Yes	
	etwork ports to add to the cast domain.		
broad physic	orts assigned to the cast domain can be cal ports, VLANs, or ace groups (ifgroups).		
doma before	ort is in another broadcast in, it must be removed e it can be added to the cast domain.		
specif	are assigned by fying both the node name ort: for example, l:e0d.		

# **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
<ul><li> The IPspace to which the subnet will be assigned.</li><li> The IPspace must exist.</li></ul>	Yes	
<ul><li>Subnet name</li><li>The name of the subnet.</li><li>The name must be unique in the IPspace.</li></ul>	Yes	
<ul> <li>The broadcast domain to which the subnet will be assigned.</li> <li>The broadcast domain must reside in the specified IPspace.</li> </ul>	Yes	
Subnet name and mask     The subnet and mask in which the IP addresses reside.	Yes	
<ul> <li>You can specify a default gateway for the subnet.</li> <li>If you do not assign a gateway when you create the subnet, you can assign one to the subnet at any time.</li> </ul>	No	

IP address ranges	No	
<ul> <li>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</li> <li>If you do not specify an IP address range, the entire range of IP addresses in the specified subnet are available to assign</li> </ul>		
to LIFs.		
Force update of LIF associations	No	
<ul> <li>Specifies whether to force the update of existing LIF associations.</li> </ul>		
<ul> <li>By default, subnet creation fails if any service processor interfaces or network interfaces are using the IP addresses in the ranges provided.</li> </ul>		
<ul> <li>Using this parameter associates any manually addressed interfaces with the subnet and allows the command to succeed.</li> </ul>		

# **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	Yes	
The name of the SVM.		
<ul> <li>You should use a fully qualified domain name (FQDN) to ensure unique SVM names across cluster leagues.</li> </ul>		

The name of the SVM root volume.	Yes	
<ul> <li>Aggregate name</li> <li>The name of the aggregate that holds the SVM root volume.</li> <li>This aggregate must exist.</li> </ul>	Yes	
<ul> <li>Security style</li> <li>The security style for the SVM root volume.</li> <li>Possible values are ntfs, unix, and mixed.</li> </ul>	Yes	
<ul><li>IPspace name</li><li>The IPspace to which the SVM is assigned.</li><li>This IPspace must exist.</li></ul>	No	
<ul> <li>The default language to use for the SVM and its volumes.</li> <li>If you do not specify a default language, the default SVM language is set to C.UTF-8.</li> <li>The SVM language setting determines the character set used to display file names and data for all NAS volumes in the SVM.</li> <li>You can modify The language after the SVM is created.</li> </ul>	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	Yes	
The name of the SVM for the LIF.		
LIF name	Yes	
The name of the LIF.		
<ul> <li>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.</li> </ul>		
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.		
<ul><li> The role of the LIF.</li><li> Data LIFs are assigned the data role.</li></ul>	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 p	rotocols	No	
The pr LIF.	rotocols that can use the		
FlexCa The Flenable as an FlexCa	fault, SMB, NFS, and ache are allowed. lexCache protocol es a volume to be used origin volume for a ache volume on a system g Data ONTAP operating ode.		
i	The protocols that use the LIF cannot be modified after the LIF is created. You should specify all protocols when you configure the LIF.		
Home nod	le	Yes	
return: reverte	ode to which the LIF s when the LIF is ed to its home port.		
	nould record a home for each data LIF.		
Home por	t or broadcast domain	Yes	
interfa	ort to which the logical ce returns when the LIF erted to its home port.		
	nould record a home port ch data LIF.		
Subnet na	ime	Yes (if using a subnet)	
• The su SVM.	ubnet to assign to the		
contin conne	a LIFs used to create uously available SMB ctions to application is must be on the same t.		

# **DNS** configuration

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

Yes	
Yes	

IP addresses of the DNS servers Yes \* 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 Directoryintegrated DNS servers as the SVM DNS servers. You can use non-Active Directoryintegrated 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.

### **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
The SVM on which you want to create an NFS or SMB server.	Yes	

Yes	
No	
No	
	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
ode1							
	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
	eOf	Default	Default		up	1500	auto/1000
	e0g	Default	Default		up	1500	auto/1000
de2							
	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
	eOf	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

Vserver	Logical Interface	Status Admin/Oper	Network Address/Mask	Current Node	Current Port	Is 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
  - $\circ$  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.
	<ul> <li>Access Protocols: Select a combination of the following options:</li> </ul>
	∘ SMB/CIFS
	∘ FlexCache
	· NFS
	■ NFSv3
	■ NFSv4
	<ul> <li>Access Details: For each type of user, specify the level of access, either read-only, read/writer, or superuser. User types include:</li> </ul>
	· All
	<ul> <li>All (as anonymous user)</li> </ul>
	· UNIX
	Kerberos 5
	· Kerberos 5i
	<ul> <li>Kerberos 5p</li> </ul>
	· 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
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 ipspace1	Domain name	MTU	Port List	Status Details
1 1	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
```

Vserver	Logical Interface		Network Address/Mask	Current Node	Current Port	Is 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

vsl 10.0.0.50 up Response time (msec): 2

vsl 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
```

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

-enabled true - use-secure true -vserver-fqdn vs1.example.com

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

#### 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 <a href="http://www.netapp.com/TM">http://www.netapp.com/TM</a> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.