NetApp

Setup ONTAP

ONTAP 9

NetApp
April 15, 2022

Table of Contents

Setup ONTAP

Decide whether to use System Manager or the ONTAP CLI for cluster setup

While you can set up new clusters with the ONTAP CLI, NetApp recommends that you use System Manager whenever possible to simplify the cluster setup process. Use these procedures only if your version of System Manager does not support initial cluster setup for your planned ONTAP deployment.

You should be aware of the following System Manager support requirements:

- Cluster setup is supported only for single nodes and HA pairs

- When you set up node management manually using the CLI, System Manager supports only IPv4 and does not support IPv6. However, if you launch System Manager after completing your hardware setup using DHCP with an auto assigned IP address and with Windows discovery, System Manager can configure an IPv6 management address.

  In ONTAP 9.6 and earlier, System Manager does not support deployments that require IPv6 networking.

- MetroCluster setup support is for MetroCluster IP configurations with two nodes at each site.

  In ONTAP 9.7 and earlier, System Manager does not support new cluster setup for MetroCluster configurations.

If you are configuring a FlexArray on non-NetApp disks, you need to use the ONTAP CLI to configure root volumes on the array LUNs, and then use the Cluster Setup wizard to set up your cluster. For more information, see the FlexArray Virtualization installation and requirements documentation.

Before completing any of these procedures, you should have installed, cabled and powered on your new storage system according to the installation and setup instructions for your platform model. See the AFF and FAS documentation.

Configure ONTAP on a new cluster

System Manager provides a simple and easy workflow for setting up a new cluster and configuring your storage.

In some cases, such as certain MetroCluster deployments or clusters that require IPv6 network addressing, you might need to use the ONTAP CLI to set up a new cluster. Click here for more details about these requirements, as well as steps for cluster setup with the ONTAP CLI.

Whether you use System Manager or the CLI for your setup, your system should already be installed and cabled according to the Installation and Setup Instructions that came with the system. Also, cluster network interfaces should be configured on each node of the cluster for intra-cluster communication.

Assign a node-management IP address

Windows System

You should connect your Windows computer to the same subnet as the controllers. This will automatically assign a node-management IP address to your system.

Step

1. From the Windows system, open the **Network** drive to discover the nodes.
2. Double-click the node to launch the cluster setup wizard.

Other systems

You should configure the node-management IP address for one of the nodes in your cluster. You can use this node-management IP address to launch the cluster set up wizard.

See Creating the cluster on the first node for information about assigning a node-management IP address.

Initialize the cluster

You initialize the cluster by setting an administrative password for the cluster and setting up the cluster management and node management networks. You can also configure services like a DNS server to resolve host names and an NTP server to synchronize time.

Steps

1. On a web browser, enter the node-management IP address that you have configured: "https://node-management-IP"

   System Manager automatically discovers the remaining nodes in the cluster.

2. Initialize the storage system by configuring the cluster management network and node management IP addresses for all the nodes.

Create your local tier

Create local tiers from the available disks or SSDs in your nodes. System Manager automatically calculates the best tier configuration based on your hardware.

Steps

1. Click **Dashboard** and then click **Prepare Storage**.

   Accept the storage recommendation for your local tier.

Configure protocols

Depending on the licenses enabled on your cluster, you can enable the desired protocols on your cluster. You then create network interfaces using which you can access the storage.

Steps

1. Click **Dashboard** and then click **Configure Protocols**.
   - Enable iSCSI or FC for SAN access.
   - Enable NFS or SMB for NAS access.
   - Enable NVMe for FC-NVMe access.

Provision Storage

You can now provision storage. The options you see depends on the licenses that are installed.

Steps

1. Click **Dashboard** and then click **Provision Storage**.
   - To provision SAN access, click **Add LUNs**.
   - To provision NAS access, click **Add Volumes**.
   - To provision NVMe storage, click **Add Namespaces**.

Configure ONTAP on a new cluster video

Set up the cluster with the ONTAP CLI

Setting up the cluster involves gathering the information needed to configure setting up

each node, creating the cluster on the first node, and joining any remaining nodes to the cluster.

Get started by gathering all the relevant information in the cluster setup worksheets.

Cluster setup worksheets

The cluster setup worksheet enables you to record the values that you need during the cluster setup process. If a default value is provided, you can use that value or else enter your own.

System defaults

The system defaults are the default values for the private cluster network. It is best to use these default values. However, if they do not meet your requirements, you can use the table to record your own values.

> (i) For clusters configured to use network switches, each cluster switch must use the 9000 MTU size.

Types of information	Your values
Private cluster network ports	
Cluster network netmask	
Cluster interface IP addresses (for each cluster network port on each node) The IP addresses for each node must be on the same subnet.	

Cluster information

Types of information	Your values
Cluster name The name must begin with a letter, and it must be fewer than 44 characters. The name can include the following special characters: . - _	

Feature license keys

You can find license keys for your initial or add-on software orders at the NetApp Support Site under **My Support** > **Software Licenses**.

Types of information	Your values
Feature license keys	

Admin storage virtual machine (SVM)

Types of information	Your values
Cluster administrator password The password for the admin account that the cluster requires before granting cluster administrator access to the console or through a secure protocol. ⓘ For security purposes, recording passwords in this worksheet is not recommended. The default rules for passwords are as follows: • A password must be at least eight characters long. • A password must contain at least one letter and one number.	
Cluster management interface port The physical port that is connected to the data network and enables the cluster administrator to manage the cluster.	
Cluster management interface IP address A unique IPv4 or IPv6 address for the cluster management interface. The cluster administrator uses this address to access the admin SVM and manage the cluster. Typically, this address should be on the data network. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization. Example: 192.0.2.66	
Cluster management interface netmask (IPv4) The subnet mask that defines the range of valid IPv4 addresses on the cluster management network. Example: 255.255.255.0	

Types of information	Your values
Cluster management interface netmask length (IPv6) If the cluster management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the cluster management network. Example: 64	
Cluster management interface default gateway The IP address for the router on the cluster management network.	
DNS domain name The name of your network's DNS domain. The domain name must consist of alphanumeric characters. To enter multiple DNS domain names, separate each name with either a comma or a space.	
Name server IP addresses The IP addresses of the DNS name servers. Separate each address with either a comma or a space.	

Node information (for each node in the cluster)

Types of information	Your values
Physical location of the controller (optional) A description of the physical location of the controller. Use a description that identifies where to find this node in the cluster (for example, "Lab 5, Row 7, Rack B").	
Node management interface port The physical port that is connected to the node management network and enables the cluster administrator to manage the node.	

Types of information	Your values
Node management interface IP address A unique IPv4 or IPv6 address for the node management interface on the management network. If you defined the node management interface port to be a data port, then this IP address should be a unique IP address on the data network. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization. Example: 192.0.2.66	
Node management interface netmask (IPv4) The subnet mask that defines the range of valid IP addresses on the node management network. If you defined the node management interface port to be a data port, then the netmask should be the subnet mask for the data network. Example: 255.255.255.0	
Node management interface netmask length (IPv6) If the node management interface uses an IPv6 address, then this value represents the prefix length that defines the range of valid IPv6 addresses on the node management network. Example: 64	
Node management interface default gateway The IP address for the router on the node management network.	

NTP server information

Types of information	Your values
NTP server addresses The IP addresses of the Network Time Protocol (NTP) servers at your site. These servers are used to synchronize the time across the cluster.	

Create the cluster on the first node

You use the Cluster Setup wizard to create the cluster on the first node. The wizard helps you to configure the cluster network that connects the nodes, create the cluster admin storage virtual machine (SVM), add feature license keys, and create the node management interface for the first node.

1. Power on all the nodes you are adding to the cluster. This is required to enable discovery for your cluster setup.

2. Connect to the console of the first node.

    The node boots, and then the Cluster Setup wizard starts on the console.

    ```
    Welcome to the cluster setup wizard....
    ```

3. Acknowledge the AutoSupport statement.

    ```
    Type yes to confirm and continue {yes}: yes
    ```

    ⓘ   AutoSupport is enabled by default.

4. Follow the instructions on the screen to assign an IP address to the node.

5. If you are using the GUI wizard to perform setup, follow the instructions to complete setup in your web browser. If you are using the CLI wizard to perform setup, press Enter to continue.

    ```
    Use your web browser to complete cluster setup by accessing
    https://10.63.11.29

    Otherwise, press Enter to complete cluster setup using the
    command line interface:

    Do you want to create a new cluster or join an existing cluster?
    {create, join}:
    ```

6. Create a new cluster: `create`

7. Accept the system defaults or enter your own values.

8. After setup is completed, log in to the cluster and verify that the cluster is active and the first node is healthy by entering the ONTAP CLI command: `cluster show`

    The following example shows a cluster in which the first node (cluster1-01) is healthy and eligible to participate:

```
cluster1::> cluster show
Node                    Health  Eligibility
--------------------    -------  ------------
cluster1-01             true     true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the `cluster setup` command.

Join remaining nodes to the cluster

After creating a new cluster, you use the Cluster Setup wizard to join each remaining node to the cluster one at a time. The wizard helps you to configure each node's node management interface.

When you join two nodes in a cluster, you are creating a high availability (HA) pair. If you join 4 nodes, you create two HA pairs. To learn more about HA, see Learn about HA.

You can only join one node to the cluster at a time. When you start to join a node to the cluster, you must complete the join operation for that node, and the node must be part of the cluster before you can start to join the next node.

Best Practice: If you have a FAS2720 with 24 or fewer NL-SAS drives, you should verify that the storage configuration default is set to active/passive to optimize performance.
For more information, see Setting up an active-passive configuration on nodes using root-data partitioning

1. Log in to the node you plan to join in the cluster.

   Cluster Setup wizard starts on the console.

   ```
   Welcome to the cluster setup wizard....
   ```

2. Acknowledge the AutoSupport statement.

   (i)   AutoSupport is enabled by default.

   ```
   Type yes to confirm and continue {yes}: yes
   ```

3. Follow the instructions on the screen to assign an IP address to the node.

4. Join the node to the cluster: `join`

5. Follow the instructions on the screen to set up the node and join it to the cluster.

6. After setup is completed, verify that the node is healthy and eligible to participate in the cluster: `cluster show`

   The following example shows a cluster after the second node (cluster1-02) has been joined to the cluster:

```
cluster1::> cluster show
Node                   Health  Eligibility
---------------------  ------- ------------
cluster1-01            true    true
cluster1-02            true    true
```

You can access the Cluster Setup wizard to change any of the values you entered for the admin SVM or node SVM by using the cluster setup command.

7. Repeat this task for each remaining node.

Check your cluster with Active IQ Config Advisor

After you have joined all the nodes to your new cluster, you should run Active IQ Config Advisor to validate your configuration and check for common configuration errors.

Config Advisor is a web-based application that you install on your laptop, virtual machine or a server, and works across Windows, Linux, and Mac platforms.

Config Advisor runs a series of commands to validate your installation and check the overall health of the configuration, including the cluster and storage switches.

1. Download and install Active IQ Config Advisor.

   Active IQ Config Advisor

2. Launch Active IQ, and set up a passphrase when prompted.

3. Review your settings and click **Save**.

4. On the **Objectives** page, click **ONTAP Post-Deployment Validation**.

5. Choose either Guided or Expert mode.

   If you choose Guided mode, connected switches are discovered automatically.

6. Enter the cluster credentials.

7. (Optional) Click **Form Validate**.

8. To begin collecting data, click **Save & Evaluate**.

9. After data collection is complete, under **Job Monitor > Actions**, view the data collected by clicking **Data View** icon, and view the results by clicking the **Results** icon.

10. Resolve the issues identified by Config Advisor.

Synchronize the system time across the cluster

Synchronizing the time ensures that every node in the cluster has the same time, and prevents CIFS and Kerberos failures.

A Network Time Protocol (NTP) server should be set up at your site. Beginning with ONTAP 9.5, you can set up your NTP server with symmetric authentication.
For more information, see Managing the cluster time (cluster administrators only).

You synchronize the time across the cluster by associating the cluster with one or more NTP servers.

1. Verify that the system time and time zone is set correctly for each node.

    All nodes in the cluster should be set to the same time zone.

    a. Use the cluster date show command to display the current date, time, and time zone for each node.

    ```
    cluster1::> cluster date show
    Node         Date                  Time zone
    -----------  --------------------  -----------------
    cluster1-01  01/06/2015 09:35:15   America/New_York
    cluster1-02  01/06/2015 09:35:15   America/New_York
    cluster1-03  01/06/2015 09:35:15   America/New_York
    cluster1-04  01/06/2015 09:35:15   America/New_York
    4 entries were displayed.
    ```

    b. Use the cluster date modify command to change the date or time zone for all of the nodes.

    This example changes the time zone for the cluster to be GMT:

    ```
    cluster1::> cluster date modify -timezone GMT
    ```

2. Use the cluster time-service ntp server create command to associate the cluster with your NTP server.

    ◦ To set up your NTP server without symmetric authentication enter the following command: `cluster time-service ntp server create -server server_name`

    ◦ To set up your NTP server with symmetric authentication, enter the following command: `cluster time-service ntp server create -server server_ip_address -key-id key_id`

    (i) Symmetric authentication is available Beginning with ONTAP 9.5. It is not available in ONTAP 9.4 or earlier.

    This example assumes that DNS has been configured for the cluster. If you have not configured DNS, you must specify the IP address of the NTP server:

    ```
    cluster1::> cluster time-service ntp server create -server
    ntp1.example.com
    ```

3. Verify that the cluster is associated with an NTP server: `cluster time-service ntp server show`

    ```
    cluster1::> cluster time-service ntp server show
    Server                Version
    --------------------  -----------
    ntp1.example.com      auto
    ```

Commands for managing symmetric authentication on NTP servers

Beginning with ONTAP 9.5, Network Time Protocol (NTP) version 3 is supported. NTPv3 includes symmetric authentication using SHA-1 keys which increases network security.

To do this…	Use this command…
Configure an NTP server without symmetric authentication	`cluster time-service ntp server create -server server_name`
Configure an NTP server with symmetric authentication	`cluster time-service ntp server create -server server_ip_address -key-id key_id`
Enable symmetric authentication for an existing NTP server An existing NTP server can be modified to enable authentication by adding the required key-id.	`cluster time-service ntp server modify -server server_name -key-id key_id`
Configure a shared NTP key	`cluster time-service ntp key create -id shared_key_id -type shared_key_type -value shared_key_value` **Note:** Shared keys are referred to by an ID. The ID, its type, and value must be identical on both the node and the NTP server
Configure an NTP server with an unknown key ID	`cluster time-service ntp server create -server server_name -key-id key_id`
Configure a server with a key ID not configured on the NTP server.	`cluster time-service ntp server create -server server_name -key-id key_id` **Note:** The key ID, type, and value must be identical to the key ID, type, and value configured on the NTP server.
Disable symmetric authentication	`cluster time-service ntp server modify -server server_name -authentication disabled`

Additional system configuration tasks to complete

After setting up a cluster, you can use either System Manager or the ONTAP command-

line interface (CLI) to continue configuring the cluster.

System configuration task	Resource
Configure networking: • Create broadcast domains • Create subnets • Create IP spaces	Setting up the network
Set up the Service Processor	System administration
Lay out your aggregates	Disk and aggregate management
Create and configure data storage virtual machines (SVMs)	NFS configuration SMB configuration SAN administration
Configure event notifications	EMS configuration

All SAN Array Software Configuration

Use the following procedures to configure an All SAN Array using System Manager.

Supported ALL SAN Array configurations

The NetApp All SAN Arrays (ASAs) are all-flash SAN-only solutions built on proven AFF NetApp platforms.

The ASA platforms are available in two-node switched or switchless clusters, can be configured for FC or iSCSI, and use symmetric active-active for multipathing. All paths are active/optimized so in the event of a storage failover, the host does not need to wait for the ALUA transition of the failover paths to resume I/O. This reduces time to failover.

> ⓘ With ONTAP 9.9.1, customers can now scale AFF ASA configurations up to 12 nodes. ASAs are supported in ONTAP 9.7 and later. Supported configurations are listed in the NetApp Interoperability Matrix Tool.

Related information

NetApp Technical Report 4515: ONTAP AFF All SAN Array Systems
NetApp Technical Report 4080: Best Practices for Scalable SAN ONTAP 9

Set up an ASA

All SAN Arrays (ASAs) follow the same setup procedure as non-ASA systems.

System Manager guides you through the procedures necessary to initialize your cluster, create a local tier, configure protocols, and provision storage for your ASA. See the steps to Configure ONTAP.

ASA limitations and restrictions

You need to be aware of the limitations and restrictions for using AFF All SAN Array (ASA) controllers, prior to ONTAP 9.9.1.

ASAs do not support NVMe-oF protocol.

> ⓘ | With ONTAP 9.9.1, NVMe-oF protocol support is now available with an AFF ASA system.

You should use the tested and supported maximum configuration limits established for the AFF All SAN Array (ASA) controllers. For reliable operations, you should not exceed the current tested and supported limits listed in NetApp Hardware Universe.

Note: With ONTAP 9.9.1, customers can now scale AFF ASA configurations up to 12 nodes. Customers can also now deploy 8-node MCC IP configurations on AFF platforms that support ASA.

Support for persistent ports

Beginning with ONTAP 9.8, persistent ports are enabled by default on All SAN Arrays (ASAs) that are configured to use the FC protocol. Persistent ports are only available for FC and require zone membership identified by World Wide Port Name (WWPN).

Persistent ports reduce the impact of takeovers by creating a shadow LIF on the corresponding physical port of the HA partner. When a node is taken over, the shadow LIF on the partner node assumes the identity of the original LIF, including the WWPNe. Before the status of path to the taken over node is changed to faulty, the shadow LIF appears as an Active/Optimized path to the host MPIO stack, and I/O is shifted. This reduces I/O disruption because the host always sees the same number of paths to the target, even during storage failover operations.

For persistent ports, the following FCP port characteristics should be identical within the HA pair:

- FCP port counts
- FCP port names
- FCP port speeds
- FCP LIF WWPN-based zoning

If any of these characteristics are not identical within the HA pair, the following EMS message is generated:

```
EMS : scsiblade.lif.persistent.ports.fcp.init.error
```

For more information on persistent ports, see NetApp Technical Report 4080: Best Practices for Scalable SAN ONTAP 9.

ASA host settings and utilities

Host settings for setting up All SAN Arrays (ASAs) are the same as those for all other SAN hosts.

You can download the NetApp Host Utilities software for your specific hosts from the support site.

Ways to identify an ASA system

You can identify an ASA system using System Manager or using the ONTAP command line interface (CLI).

From the System Manager dashboard, click **Cluster > Overview** and then select the system node. The **PERSONALITY** is displayed as **All SAN Array**.

From the CLI, you can use san config show command. The "All SAN Array" value returns as true for ASA systems.