Configure ONTAP

ONTAP 9

NetApp
June 21, 2021

Table of Contents

Configure ONTAP

Decide whether to use the ONTAP CLI for cluster setup

While you can set up new clusters with the ONTAP CLI, NetApp recommends that you use ONTAP System Manager whenever possible to simplify the cluster setup process. Use these procedures only if your version of ONTAP 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 Reference.

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 Center.

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.

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.

   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 in 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`

   > Symmetric authentication is available beginning in 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
   ```

Related information

System administration

Commands for managing symmetric authentication on NTP servers

Beginning in 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`

Decide where to send important event notifications

Before you configure important EMS event notifications, you need to decide whether to

send the notifications to an email address, a syslog server, or an SNMP traphost.

If your environment already contains a syslog server for aggregating the logged events from other systems, such as servers and applications, then it is easier to use that syslog server also for important event notifications from storage systems.

If your environment does not already contain a syslog server, then it is easier to use email for important event notifications.

If you already forward event notifications to an SNMP traphost, then you might want to monitor that traphost for important events.

- Set EMS to send event notifications.

If you want…	Refer to this…
The EMS to send important event notifications to an email address	Configuring important EMS events to send email notifications
The EMS to forward important event notifications to a syslog server	Configuring important EMS events to forward notifications to a syslog server
If you want the EMS to forward event notifications to an SNMP traphost	Configuring SNMP traphosts to receive event notifications

Configure important EMS events to send email notifications

To receive email notifications for the most important events, you must configure the EMS to send email messages for events that signal important activity.

DNS must be configured on the cluster to resolve the email addresses.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

1. Configure the event SMTP mail server settings:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from cluster_admin@your_domain
   ```

2. Create an email destination for event notifications:

   ```
   event notification destination create -name storage-admins -email your_email@your_domain
   ```

3. Configure the important events to send email notifications:

   ```
   event notification create -filter-name important-events -destinations storage_admins
   ```

Configure important EMS events to forward notifications to a syslog server

To log notifications of the most severe events on a syslog server, you must configure the EMS to forward notifications for events that signal important activity.

DNS must be configured on the cluster to resolve the syslog server name.

If your environment does not already contain a syslog server for event notifications, you must first create one. If your environment already contains a syslog server for logging events from other systems, then you might want to use that one for important event notifications.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

1. Create a syslog server destination for important events:

   ```
   event notification destination create -name syslog-ems -syslog syslog-server-address
   ```

2. Configure the important events to forward notifications to the syslog server:

   ```
   event notification create -filter-name important-events -destinations syslog-ems
   ```

Configure SNMP traphosts to receive event notifications

To receive event notifications on an SNMP traphost, you must configure a traphost.

- SNMP and SNMP traps must be enabled on the cluster.

  SNMP and SNMP traps are enabled by default.

- DNS must be configured on the cluster to resolve the traphost names.

If you do not already have an SNMP traphost configured to receive event notifications (SNMP traps), you must add one.

You can perform this task any time the cluster is running by entering the commands on the ONTAP command line.

1. If your environment does not already have an SNMP traphost configured to receive event notifications, add one: `system snmp traphost add -peer-address snmp_traphost_name`

   All event notifications that are supported by SNMP by default are forwarded to the SNMP traphost.

Additional system configuration tasks to complete

After setting up a cluster, you can use either ONTAP 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)	Cluster management using System Manager NFS configuration SMB/CIFS management SAN administration