Managing clusters

Active IQ Unified Manager 9.14

NetApp
November 11, 2024

Table of Contents

Managing clusters

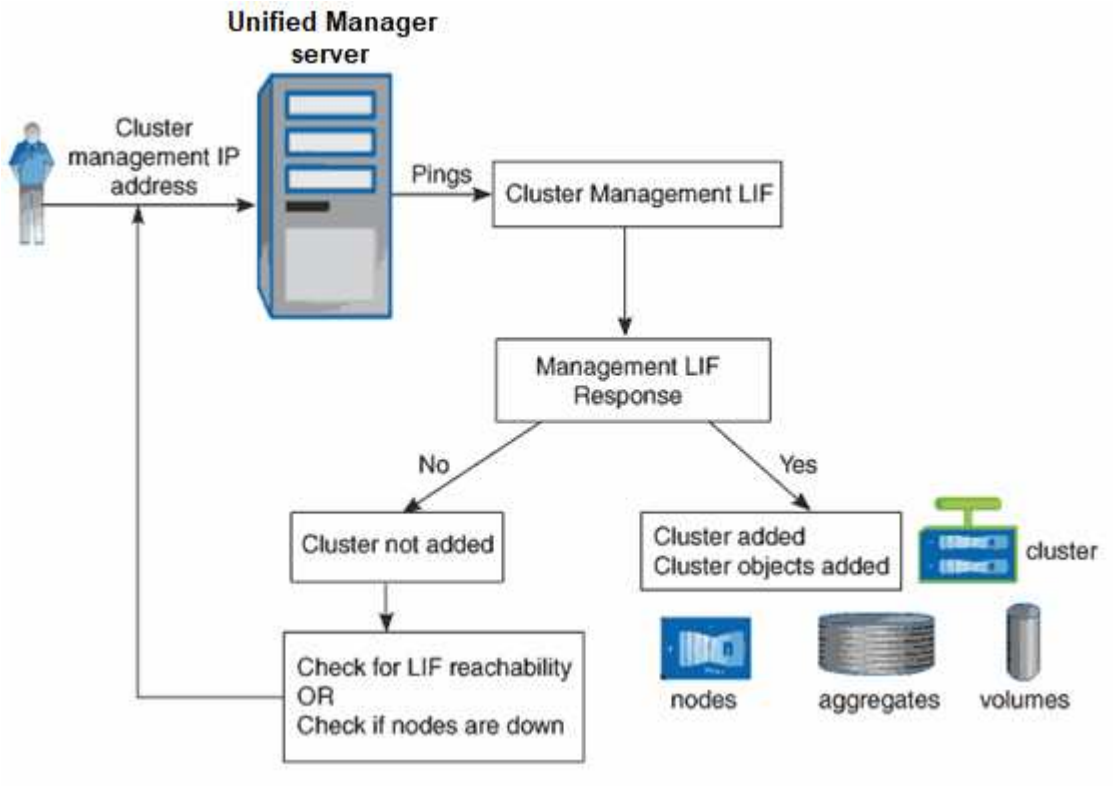
You can manage the ONTAP clusters by using Unified Manager to monitor, add, edit, and remove clusters.

How the cluster discovery process works

After you have added a cluster to Unified Manager, the server discovers the cluster objects and adds them to its database. Understanding how the discovery process works helps you to manage your organization's clusters and their objects.

The monitoring interval for collecting cluster configuration information is 15 minutes. For example, after you have added a cluster, it takes 15 minutes to display the cluster objects in the Unified Manager UI. This time frame is also true when making changes to a cluster. For example, if you add two new volumes to an SVM in a cluster, you see those new objects in the UI after the next polling interval, which could be up to 15 minutes.

The following image illustrates the discovery process:



After all the objects for a new cluster are discovered, Unified Manager starts to gather historical performance data for the previous 15 days. These statistics are collected using the data continuity collection functionality. This feature provides you with over two weeks of performance information for a cluster immediately after it is added. After the data continuity collection cycle is completed, real-time cluster performance data is collected, by default, every five minutes.

Because the collection of 15 days of performance data is CPU intensive, it is suggested that you stagger the addition of new clusters so that data continuity collection polls are not running on too many clusters at the same time.

Viewing the list of monitored clusters

You can use the Cluster Setup page to view your inventory of clusters. You can view details about the clusters, such as their name or IP address and communication status.

What you'll need

You must have the Operator, Application Administrator, or Storage Administrator role.

Step

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.

   All the clusters in your storage environment managed by Unified Manager are displayed.The list of clusters is sorted by the collection state severity level column. You can click a column header to sort the clusters by different columns.

Adding clusters

You can add a cluster to Active IQ Unified Manager so that you can monitor the cluster. This includes the ability to obtain cluster information such as the health, capacity, performance, and configuration of the cluster so that you can find and resolve any issues that might occur.

What you'll need

- You must have the Application Administrator role or the Storage Administrator role.
- You must have the following information:
  - Unified Manager supports on-premises ONTAP clusters, ONTAP Select, Cloud Volumes ONTAP.
  - You must have the host name or cluster management IP address (IPv4 or IPv6) for the cluster.

    When using the host name, it must resolve to the cluster management IP address for the cluster management LIF. If you use a node management LIF, the operation fails.

  - You must have the user name and password to access the cluster.

    This account must have the *admin* role with Application access set to *ontapi*, *console*, and *http*.

  - You must know the port number to connect to the cluster using the HTTPS protocol (typically port 443).
  - The cluster must be running ONTAP version 9.1 software or greater.
  - You must have adequate space on the Unified Manager server. You are prevented from adding a cluster to the server when greater than 90% of space is already consumed.
  - You have the required certificates:

    SSL (HTTPS) certificate: This certificate is owned by Unified Manager. A default self-signed SSL (HTTPS) certificate is generated with a fresh installation of Unified Manager. NetApp recommends that you upgrade it to CA-signed certificate for better security. If the server certificate expires, you should regenerate it and restart Unified Manager for the services to incorporate the new certificate. For more information about regenerating SSL certificate, see Generating an HTTPS security certificate.

EMS certificate: This certificate is owned by Unified Manager. It is used during authentication for EMS notifications received from ONTAP.

Certificates for Mutual TLS communication: Used during Mutual TLS communication between Unified Manager and ONTAP. The certificate-based authentication is enabled for a cluster, based on the ONTAP version. If the cluster running the ONTAP version is lower than the 9.5, certificate-based authentication is not enabled.

Certificate-based authentication is not enabled automatically for a cluster, if you are updating an older version of Unified Manager. However, you can enable it by modifying and saving the cluster details. If the certificate expires, you should regenerate it to incorporate the new certificate. For more information about viewing and regenerating the certificate, see Editing clusters.

- You can add a cluster from the web UI, and certificate-based authentication is automatically enabled.
- You can add a cluster through Unified Manager CLI, the certificate-based authentication is not enabled by default. If you add a cluster using Unified Manager CLI, it is required to edit the cluster using Unified Manager UI. You can see Supported Unified Manager CLI commands to add a cluster using Unified Manager CLI.
- If certificate-based authentication is enabled for a cluster, and you take the backup of Unified Manager from a server and restore to another Unified Manager server where hostname or IP address is changed, then monitoring of the cluster can fail. To avoid the failure, edit and save the cluster details. For more information about editing cluster details, see Editing clusters.
- On the cluster level, the Active IQ interface adds two new user group entries for the authentication method "cert".

Cluster certificates: This certificate is owned by ONTAP. You cannot add a cluster to Unified Manager with an expired certificate and if the certificate has already expired, you should regenerate it before adding the cluster. For information about certificate generation, see the knowledge base (KB) article How to renew an ONTAP self-signed certificate in System Manager user interface.

- A single instance of Unified Manager can support a specific number of nodes. If you need to monitor an environment that exceeds the supported node count, you must install an additional instance of Unified Manager to monitor some of the clusters. To view the list of supported node count, see the Unified Manager Best Practices Guide.

Steps

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.
2. On the Cluster Setup page, click **Add**.
3. In the Add Cluster dialog box, specify the values as required, and then click **Submit**.
4. In the Authorize Host dialog box, click **View Certificate** to view the certificate information about the cluster.
5. Click **Yes**.

   After saving the cluster details, you can see the certificate for Mutual TLS communication for a cluster.

   If the certificate-based authentication is not enabled, Unified Manager checks the certificate only when the cluster is added initially. Unified Manager does not check the certificate for each API call to ONTAP.

After all the objects for a new cluster are discovered, Unified Manager starts to gather historical performance

data for the previous 15 days. These statistics are collected using the data continuity collection functionality. This feature provides you with over two weeks of performance information for a cluster immediately after it is added. After the data continuity collection cycle is completed, real-time cluster performance data is collected, by default, every five minutes.

Because the collection of 15 days of performance data is CPU intensive, it is suggested that you stagger the addition of new clusters so that data continuity collection polls are not running on too many clusters at the same time. Additionally, if you restart Unified Manager during the data continuity collection period, the collection will be halted and you will see gaps in the performance charts for the missing timeframe.

If you receive an error message that you cannot add the cluster, check to see if the following issues exist:

- If the clocks on the two systems are not synchronized and the Unified Manager HTTPS certificate start date is later than the date on the cluster. You must ensure that the clocks are synchronized using NTP or a similar service.
- If the cluster has reached the maximum number of EMS notification destinations the Unified Manager address cannot be added. By default only 20 EMS notification destinations can be defined on the cluster.

Related information

Adding users

Viewing the cluster list and details

Installing a CA signed and returned HTTPS certificate

Editing clusters

You can modify the settings of an existing cluster, such as the host name or IP address, user name, password, and port, by using the Edit Cluster dialog box.

What you'll need

You must have the Application Administrator role or the Storage Administrator role.

Starting with Unified Manager 9.7, clusters can be added using HTTPS only.

Steps

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.
2. On the **Cluster Setup** page, select the cluster you want to edit, and then click **Edit**.
3. In the **Edit Cluster** dialog box, modify the values as required.
   If you have modified the details for a cluster added to Unified Manager, you can view the certificate details for Mutual TLS communication, based on the ONTAP version. For more information about ONTAP version, see Certificates for Mutual TLS communication.
   You can view the certificate details by clicking **Certificate Details**. If the certificate is expired, click the **Regenerate** button to incorporate the new certificate.
4. Click **Submit**.

5. In the Authorize Host dialog box, click **View Certificate** to view the certificate information about the cluster.
6. Click **Yes**.

Related information

Adding users

Viewing the cluster list and details

Removing clusters

You can remove a cluster from Unified Manager by using the Cluster Setup page. For example, you can remove a cluster if cluster discovery fails, or when you want to decommission a storage system.

What you'll need

You must have the Application Administrator role or the Storage Administrator role.

This task removes the selected cluster from Unified Manager. After a cluster is removed, it is no longer monitored. The instance of Unified Manager registered with the removed cluster is also unregistered from the cluster.

Removing a cluster also deletes all its storage objects, historical data, storage services, and all associated events from Unified Manager. These changes are reflected on the inventory pages and the details pages after the next data collection cycle.

Steps

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.
2. On the Cluster Setup page, select the cluster that you want to remove and click **Remove**.
3. In the **Remove Data Source** message dialog, click **Remove** to confirm the remove request.

Related information

Adding users

Viewing the cluster list and details

Rediscovering clusters

You can manually rediscover a cluster from the Cluster Setup page in order to obtain the latest information about the health, monitoring status, and performance status of the cluster.

You can manually rediscover a cluster when you want to update the cluster—such as by increasing the size of an aggregate when there is insufficient space—and you want Unified Manager to discover the changes that you make.

When Unified Manager is paired with OnCommand Workflow Automation (WFA), the pairing triggers the reacquisition of the data cached by WFA.

Steps

1. In the left navigation pane, click **Storage Management** > **Cluster Setup**.
2. On the **Cluster Setup** page, click **Rediscover**.

   Unified Manager rediscovers the selected cluster and displays the latest health and performance status.

Related information

Viewing the cluster list and details

Copyright information

Trademark information