Monitor performance

ONTAP 9

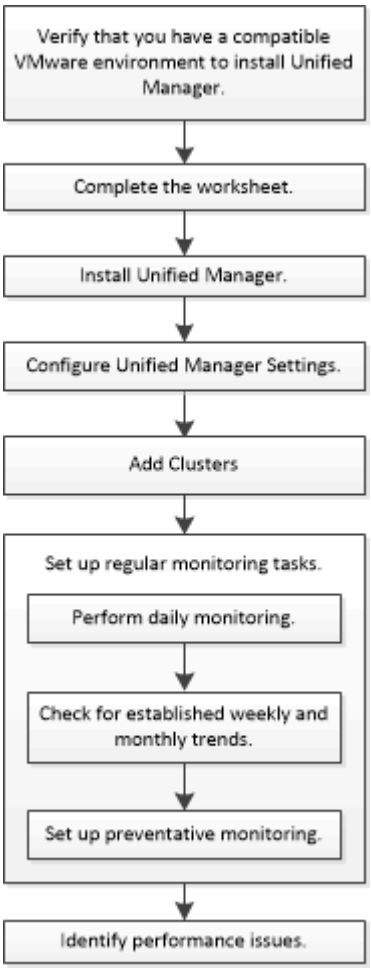
NetApp
January 13, 2023

Table of Contents

Monitor performance

Performance monitoring and maintenance workflow overview

Monitoring and maintaining cluster performance involves installing Active IQ Unified Manager software, setting up basic monitoring tasks, identifying performance issues, and making adjustments as needed.



Verify that your VMware environment is supported

To successful install Active IQ Unified Manager, you must verify that your VMware environment meets the necessary requirements.

Steps

1. Verify that your VMware infrastructure meets the sizing requirements for the installation of Unified Manager.
2. Go to the Interoperability Matrix to verify that you have a supported combination of the following components:

    - ONTAP version

- ESXi operating system version
- VMware vCenter Server version
- VMware Tools version
- Browser type and version

The Interoperability Matrix lists the supported configurations for Unified Manager.

3. Click the configuration name for the selected configuration.

   Details for that configuration are displayed in the Configuration Details window.

4. Review the information in the following tabs:
   - Notes

     Lists important alerts and information that are specific to your configuration.

   - Policies and Guidelines

     Provides general guidelines for all configurations.

Active IQ Unified Manager worksheet

Before you install, configure, and connect Active IQ Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

Unified Manager installation information

Virtual machine on which software is deployed	Your value
ESXi server IP address	
Host fully qualified domain name	
Host IP address	
Network mask	
Gateway IP address	
Primary DNS address	
Secondary DNS address	
Search domains	
Maintenance user name	

Maintenance user password	

Unified Manager configuration information

Setting	Your value
Maintenance user email address	
NTP server	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP default port	25 (Default value)
Email from which alert notifications are sent	
LDAP bind distinguished name	
LDAP bind password	
Active Directory administrator name	
Active Directory password	
Authentication server base distinguished name	
Authentication server host name or IP address	

Cluster information

Capture the following information for each cluster on Unified Manager.

Cluster 1 of N	Your value
Host name or cluster-management IP address	
ONTAP administrator user name The administrator must have been assigned the "admin" role.	

ONTAP administrator password	
Protocol (HTTP or HTTPS)	

Related information

Administrator authentication and RBAC

Install Active IQ Unified Manager

Download and deploy Active IQ Unified Manager

To install the software, you must download the virtual appliance (VA) installation file and then use a VMware vSphere Client to deploy the file to a VMware ESXi server. The VA is available in an OVA file.

Steps

1. Go to the **NetApp Support Site Software Download** page and locate Active IQ Unified Manager.

   https://mysupport.netapp.com/products/index.html

2. Select **VMware vSphere** in the **Select Platform** drop-down menu and click **Go!**
3. Save the “OVA” file to a local or network location that is accessible to your VMware vSphere Client.
4. In VMware vSphere Client, click **File** > **Deploy OVF Template**.
5. Locate the “OVA” file and use the wizard to deploy the virtual appliance on the ESXi server.

   You can use the **Properties** tab in the wizard to enter your static configuration information.

6. Power on the VM.
7. Click the **Console** tab to view the initial boot process.
8. Follow the prompt to install VMware Tools on the VM.
9. Configure the time zone.
10. Enter a maintenance user name and password.
11. Go to the URL displayed by the VM console.

Configure initial Active IQ Unified Manager settings

The Active IQ Unified Manager Initial Setup dialog box appears when you first access the web UI, which enables you to configure some initial settings and to add clusters.

Steps

1. Accept the default AutoSupport enabled setting.
2. Enter the NTP server details, the maintenance user email address, the SMTP server host name, and additional SMTP options, and then click **Save**.

After you finish

When the initial setup is complete, the Cluster Data Sources page is displayed where you can add the cluster

details.

Specify the clusters to be monitored

You must add a cluster to an Active IQ Unified Manager server to monitor the cluster, view the cluster discovery status, and monitor its performance.

What you'll need

- You must have the following information:
  - Host name or cluster-management IP address

    The host name is the fully qualified domain name (FQDN) or short name that Unified Manager uses to connect to the cluster. This host name must resolve to the cluster-management IP address.

    The cluster-management IP address must be the cluster-management LIF of the administrative storage virtual machine (SVM). If you use a node-management LIF, the operation fails.

  - ONTAP administrator user name and password
  - Type of protocol (HTTP or HTTPS) that can be configured on the cluster and the port number of the cluster
- You must have the Application Administrator or Storage Administrator role.
- The ONTAP administrator must have the ONTAPI and SSH administrator roles.
- The Unified Manager FQDN must be able to ping ONTAP.

  You can verify this by using the ONTAP command `ping -node` *`node_name`* `-destination` *`Unified_Manager_FQDN`*.

About this task

For a MetroCluster configuration, you must add both the local and remote clusters, and the clusters must be configured correctly.

Steps

1. Click **Configuration** > **Cluster Data Sources**.
2. From the Clusters page, click **Add**.
3. In the **Add Cluster** dialog box, specify the required values, such as the host name or IP address (IPv4 or IPv6) of the cluster, user name, password, protocol for communication, and port number.

   By default, the HTTPS protocol is selected.

   You can change the cluster-management IP address from IPv6 to IPv4 or from IPv4 to IPv6. The new IP address is reflected in the cluster grid and the cluster configuration page after the next monitoring cycle finishes.

4. Click **Add**.
5. If HTTPS is selected, perform the following steps:
   a. In the **Authorize Host** dialog box, click **View Certificate** to view the certificate information about the cluster.
   b. Click **Yes**.

Unified Manager checks the certificate only when the cluster is initially added, but does not check it for each API call to ONTAP.

If the certificate has expired, you cannot add the cluster. You must renew the SSL certificate and then add the cluster.

6. **Optional**: View the cluster discovery status:

   a. Review the cluster discovery status from the **Cluster Setup** page.

   The cluster is added to the Unified Manager database after the default monitoring interval of approximately 15 minutes.

Set up basic monitoring tasks

Perform daily monitoring

You can perform daily monitoring to ensure that you do not have any immediate performance issues that require attention.

Steps

1. From the Active IQ Unified Manager UI, go to the **Event Inventory** page to view all current and obsolete events.
2. From the **View** option, select `Active Performance Events` and determine what action is required.

Use weekly and monthly performance trends to identify performance issues

Identifying performance trends can assist you in identifying whether the cluster is being overused or underused by analyzing volume latency. You can use similar steps to identify CPU, network, or other system bottlenecks.

Steps

1. Locate the volume that you suspect is being underused or overused.
2. On the **Volume Details** tab, click **30 d** to display the historical data.
3. In the "Break down data by" drop-down menu, select **Latency**, and then click **Submit**.
4. Deselect **Aggregate** in the cluster components comparison chart, and then compare the cluster latency with the volume latency chart.
5. Select **Aggregate** and deselect all other components in the cluster components comparison chart, and then compare the aggregate latency with the volume latency chart.
6. Compare the reads/writes latency chart to the volume latency chart.
7. Determine whether client application loads have caused a workload contention and rebalance workloads as needed.
8. Determine whether the aggregate is overused and causing contention and rebalance workloads as needed.

Use performance thresholds to generate event notifications

Events are notifications that the Active IQ Unified Manager generates automatically when a predefined condition occurs, or when a performance counter value crosses a threshold. Events help you identify performance issues in the clusters you are monitoring. You can configure alerts to send email notification automatically when events of certain severity types occur.

Set performance thresholds

You can set performance thresholds to monitor critical performance issues. User-defined thresholds trigger a warning or a critical event notification when the system approaches or exceeds the defined threshold.

Steps

1. Create the Warning and Critical event thresholds:
   a. Select **Configuration** > **Performance Thresholds**.
   b. Click **Create**.
   c. Select the object type and specify a name and description of the policy.
   d. Select the object counter condition and specify the limit values that define Warning and Critical events.
   e. Select the duration of time that the limit values must be breached for an event to be sent, and then click **Save**.
2. Assign the threshold policy to the storage object.
   a. Go to the Inventory page for the same cluster object type that you previously selected and choose the **Performance** from the View option.
   b. Select the object to which you want to assign the threshold policy, and then click **Assign Threshold Policy**.
   c. Select the policy you previously created, and then click **Assign Policy**.

Example

You can set user-defined thresholds to learn about critical performance issues. For example, if you have a Microsoft Exchange Server and you know that it crashes if volume latency exceeds 20 milliseconds, you can set a warning threshold at 12 milliseconds and a critical threshold at 15 milliseconds. With this threshold setting, you can receive notifications when the volume latency exceeds the limit.

Add alerts

You can configure alerts to notify you when a particular event is generated. You can configure alerts for a single resource, for a group of resources, or for events of a particular severity type. You can specify the frequency with which you want to be notified and associate a script to the alert.

What you'll need

- You must have configured notification settings such as the user email address, SMTP server, and SNMP trap host to enable the Active IQ Unified Manager server to use these settings to send notifications to users when an event is generated.
- You must know the resources and events for which you want to trigger the alert, and the user names or email addresses of the users that you want to notify.
- If you want to have a script execute based on the event, you must have added the script to Unified Manager by using the Scripts page.
- You must have the Application Administrator or Storage Administrator role.

About this task

You can create an alert directly from the Event details page after receiving an event in addition to creating an alert from the Alert Setup page, as described here.

Steps

1. In the left navigation pane, click **Storage Management** > **Alert Setup**.
2. In the **Alert Setup** page, click **Add**.
3. In the **Add Alert** dialog box, click **Name**, and enter a name and description for the alert.
4. Click **Resources**, and select the resources to be included in or excluded from the alert.

   You can set a filter by specifying a text string in the **Name contains** field to select a group of resources. Based on the text string that you specify, the list of available resources displays only those resources that match the filter rule. The text string that you specify is case-sensitive.

   If a resource conforms to both the include and exclude rules that you have specified, the exclude rule takes precedence over the include rule, and the alert is not generated for events related to the excluded resource.

5. Click **Events**, and select the events based on the event name or event severity type for which you want to trigger an alert.

   To select more than one event, press the Ctrl key while you make your selections.

6. Click **Actions**, and select the users that you want to notify, choose the notification frequency, choose whether an SNMP trap will be sent to the trap receiver, and assign a script to be executed when an alert is generated.

   If you modify the email address that is specified for the user and reopen the alert for editing, the Name field appears blank because the modified email address is no longer mapped to the user that was previously selected. Also, if you modified the email address of the selected user from the Users page, the modified email address is not updated for the selected user.

   You can also choose to notify users through SNMP traps.

7. Click **Save**.

Example of adding an alert

This example shows how to create an alert that meets the following requirements:

- Alert name: HealthTest
- Resources: includes all volumes whose name contains "abc" and excludes all volumes whose name

contains "xyz"

- Events: includes all critical health events
- Actions: includes "sample@domain.com", a "Test" script, and the user has to be notified every 15 minutes

Perform the following steps in the Add Alert dialog box:

1. Click **Name**, and enter `HealthTest` in the **Alert Name** field.
2. Click **Resources**, and in the Include tab, select **Volumes** from the drop-down list.
   a. Enter `abc` in the **Name contains** field to display the volumes whose name contains "abc".
   b. Select **<<All Volumes whose name contains 'abc'>>** from the Available Resources area, and move it to the Selected Resources area.
   c. Click **Exclude**, and enter `xyz` in the **Name contains** field, and then click **Add**.
3. Click **Events**, and select **Critical** from the Event Severity field.
4. Select **All Critical Events** from the Matching Events area, and move it to the Selected Events area.
5. Click **Actions**, and enter `sample@domain.com` in the Alert these users field.
6. Select **Remind every 15 minutes** to notify the user every 15 minutes.

   You can configure an alert to repeatedly send notifications to the recipients for a specified time. You should determine the time from which the event notification is active for the alert.
7. In the Select Script to Execute menu, select **Test** script.
8. Click **Save**.

Configure alert settings

You can specify which events from Active IQ Unified Manager trigger alerts, the email recipients for those alerts, and the frequency for the alerts.

What you'll need

You must have the Application Administrator role.

About this task

You can configure unique alert settings for the following types of performance events:

- Critical events triggered by breaches of user-defined thresholds
- Warning events triggered by breaches of user-defined thresholds, system-defined thresholds, or dynamic thresholds

By default, email alerts are sent to Unified Manager admin users for all new events. You can have email alerts sent to other users by adding those users' email addresses.

> To disable alerts from being sent for certain types of events, you must clear all of the check boxes in an event category. This action does not stop events from appearing in the user interface.

Steps

1. In the left navigation pane, select **Storage Management** > **Alert Setup**.

The Alert Setup page is displayed.

2. Click **Add** and configure the appropriate settings for each of the event types.

   To have email alerts sent to multiple users, enter a comma between each email address.

3. Click **Save**.

Identify performance issues in Active IQ Unified Manager

If a performance event occurs, you can locate the source of the issue within Active IQ Unified Manager and use other tools to fix it. You might receive an email notification of an event or notice the event during daily monitoring.

Steps

1. Click the link in the email notification, which takes you directly to the storage object having a performance event.

If you…	Then…
Receive an email notification of an event	Click the link to go directly to the event details page.
Notice the event while analyzing the Event Inventory page	Select the event to go directly to the event details page.

2. If the event has crossed a system-defined threshold, follow the suggested actions in the UI to troubleshoot the issue.
3. If the event has crossed a user-defined threshold, analyze the event to determine if you need to take action.
4. If the issue persists, check the following settings:
   - Protocol settings on the storage system
   - Network settings on any Ethernet or fabric switches
   - Network settings on the storage system
   - Disk layout and aggregate metrics on the storage system
5. If the issue persists, contact technical support for assistance.

Copyright information

Trademark information