Troubleshooting

Active IQ Unified Manager 9.8

NetApp
February 20, 2023

Table of Contents

Troubleshooting

Troubleshooting information helps you to identify and resolve issues you encounter when using Unified Manager.

Changing the Unified Manager host name

At some point, you might want to change the host name of the system on which you have installed Unified Manager. For example, you might want to rename the host to more easily identify your Unified Manager servers by type, workgroup, or monitored cluster group.

The steps required to change the host name are different depending on whether Unified Manager is running on a VMware ESXi server, on a Red Hat or CentOS Linux server, or on a Microsoft Windows server.

Changing the Unified Manager virtual appliance host name

The network host is assigned a name when the Unified Manager virtual appliance is first deployed. You can change the host name after deployment. If you change the host name, you must also regenerate the HTTPS certificate.

Before you begin

You must be logged in to Unified Manager as the maintenance user, or have the Application Administrator role assigned to you to perform these tasks.

About this task

You can use the host name (or the host IP address) to access the Unified Manager web UI. If you configured a static IP address for your network during deployment, then you would have designated a name for the network host. If you configured the network using DHCP, the host name should be taken from the DNS. If DHCP or DNS is not properly configured, the host name “Unified Manager” is automatically assigned and associated with the security certificate.

Regardless of how the host name was assigned, if you change the host name, and intend to use the new host name to access the Unified Manager web UI, you must generate a new security certificate.

If you access the web UI by using the server’s IP address instead of the host name, you do not have to generate a new certificate if you change the host name. However, it is the best practice to update the certificate so that the host name in the certificate matches the actual host name.

If you change the host name in Unified Manager, you must manually update the host name in OnCommand Workflow Automation (WFA). The host name is not updated automatically in WFA.

The new certificate does not take effect until the Unified Manager virtual machine is restarted.

Steps

1. Generate an HTTPS security certificate

   If you want to use the new host name to access the Unified Manager web UI, you must regenerate the

HTTPS certificate to associate it with the new host name.

2. Restart the Unified Manager virtual machine

   After you regenerate the HTTPS certificate, you must restart the Unified Manager virtual machine.

Changing the Unified Manager host name on Linux systems

At some point, you might want to change the host name of the Red Hat Enterprise Linux or CentOS machine on which you have installed Unified Manager. For example, you might want to rename the host to more easily identify your Unified Manager servers by type, workgroup, or monitored cluster group when you list your Linux machines.

Before you begin

You must have root user access to the Linux system on which Unified Manager is installed.

About this task

You can use the host name (or the host IP address) to access the Unified Manager web UI. If you configured a static IP address for your network during deployment, then you would have designated a name for the network host. If you configured the network using DHCP, the host name should be taken from the DNS server.

Regardless of how the host name was assigned, if you change the host name and intend to use the new host name to access the Unified Manager web UI, you must generate a new security certificate.

If you access the web UI by using the server's IP address instead of the host name, you do not have to generate a new certificate if you change the host name. However, it is the best practice to update the certificate, so that the host name in the certificate matches the actual host name. The new certificate does not take effect until the Linux machine is restarted.

If you change the host name in Unified Manager, you must manually update the host name in OnCommand Workflow Automation (WFA). The host name is not updated automatically in WFA.

Steps

1. Log in as the root user to the Unified Manager system that you want to modify.
2. Stop the Unified Manager software and the associated MySQL software by entering the following command: `systemctl stop ocieau ocie mysqld`
3. Change the host name using the Linux `hostnamectl` command: `hostnamectl set-hostname new_FQDN`

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Regenerate the HTTPS certificate for the server: `/opt/netapp/essentials/bin/cert.sh create`
5. Restart the network service: `service network restart`
6. After the service is restarted, verify whether the new host name is able to ping itself: `ping new_hostname`

   ```
   ping nuhost
   ```

This command should return the same IP address that was set earlier for the original host name.

7. After you complete and verify your host name change, restart Unified Manager by entering the following command: `systemctl start mysqld ocie ocieau`

Adding disk space to the Unified Manager database directory

The Unified Manager database directory contains all of the health and performance data collected from ONTAP systems. Some circumstances may require that you increase the size of the database directory.

For example, the database directory may get full if Unified Manager is collecting data from a large number of clusters where each cluster has many nodes. You will receive a warning event when the database directory is 90% full, and a critical event when the directory is 95% full.

No additional data is collected from clusters after the directory reaches 95% full.

The steps required to add capacity to the data directory are different depending on whether Unified Manager is running on a VMware ESXi server, on a Red Hat or CentOS Linux server, or on a Microsoft Windows server.

Adding space to the data disk of the VMware virtual machine

If you need to increase the amount of space on the data disk for the Unified Manager database, you can add capacity after installation by increasing disk space using the Unified Manager maintenance console.

Before you begin

- You must have access to the vSphere Client.
- The virtual machine must have no snapshots stored locally.
- You must have the maintenance user credentials.

About this task

We recommend that you back up your virtual machine before increasing the size of virtual disks.

Steps

1. In the vSphere client, select the Unified Manager virtual machine, and then add more disk capacity to data `disk 3`. See the VMware documentation for details.

   In some rare cases the Unified Manager deployment uses “Hard Disk 2” for the data disk instead of “Hard Disk 3”. If this has occurred in your deployment, increase the space of whichever disk is larger. The data disk will always have more space than the other disk.

2. In the vSphere client, select the Unified Manager virtual machine, and then select the **Console** tab.
3. Click in the console window, and then log in to the maintenance console using your user name and password.

4. In the **Main Menu**, enter the number for the **System Configuration** option.
5. In the **System Configuration Menu**, enter the number for the **Increase Data Disk Size** option.

Adding space to the data directory of the Linux host

If you allotted insufficient disk space to the `/opt/netapp/data` directory to support Unified Manager when you originally set up the Linux host and then installed Unified Manager, you can add disk space after installation by increasing disk space on the `/opt/netapp/data` directory.

Before you begin

You must have root user access to the Red Hat Enterprise Linux or CentOS Linux machine on which Unified Manager is installed.

About this task

We recommend that you back up the Unified Manager database before increasing the size of the data directory.

Steps

1. Log in as root user to the Linux machine on which you want to add disk space.
2. Stop the Unified Manager service and the associated MySQL software in the order shown: `systemctl stop ocieau ocie mysqld`
3. Create a temporary backup folder (for example, `/backup-data`) with sufficient disk space to contain the data in the current `/opt/netapp/data` directory.
4. Copy the content and privilege configuration of the existing `/opt/netapp/data` directory to the backup data directory: `cp -arp /opt/netapp/data/* /backup-data`
5. If SE Linux is enabled:
   a. Get the SE Linux type for folders on existing `/opt/netapp/data` folder:

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}'| awk -F: '{print $3}'|
      head -1
      ```

      The system returns a confirmation similar to the following:

      ```
      echo $se_type
      mysqld_db_t
      ```

   b. Run the `chcon` command to set the SE Linux type for the backup directory: `chcon -R --type=mysqld_db_t /backup-data`
6. Remove the contents of the `/opt/netapp/data` directory:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`

7. Expand the size of the `/opt/netapp/data` directory to a minimum of 750 GB through LVM commands or by adding extra disks.

   Mounting the `/opt/netapp/data` directory on an NFS or CIFS share is not supported.

8. Confirm that the `/opt/netapp/data` directory owner (mysql) and group (root) are unchanged: `ls -ltr /opt/netapp/ | grep data`

   The system returns a confirmation similar to the following:

   ```
   drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
   ```

9. If SE Linux is enabled, confirm that the context for the `/opt/netapp/data` directory is still set to mysqld_db_t:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      The system returns a confirmation similar to the following:

      ```
      -rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
      /opt/netapp/data/abc
      ```

10. Delete the file `abc` so that this extraneous file does not cause a database error in the future.
11. Copy the contents from `backup-data` back to the expanded `/opt/netapp/data` directory: `cp -arp /backup-data/* /opt/netapp/data/`
12. If SE Linux is enabled, run the following command: `chcon -R --type=mysqld_db_t /opt/netapp/data`
13. Start the MySQL service: `systemctl start mysqld`
14. After the MySQL service is started, start the ocie and ocieau services in the order shown: `systemctl start ocie ocieau`
15. After all of the services are started, delete the backup folder `/backup-data`: `rm -rf /backup-data`

Adding space to the logical drive of the Microsoft Windows server

If you need to increase the amount of disk space for the Unified Manager database, you can add capacity to the logical drive on which Unified Manager is installed.

Before you begin

You must have Windows administrator privileges.

About this task

We recommend that you back up the Unified Manager database before adding disk space.

Steps

1. Log in as administrator to the Windows server on which you want to add disk space.
2. Follow the step that corresponds to method you want to use to add more space:

Option	Description
On a physical server, add capacity to the logical drive on which the Unified Manager server is installed.	Follow the steps in the Microsoft topic: Extend a Basic Volume
On a physical server, add a hard disk drive.	Follow the steps in the Microsoft topic: Adding Hard Disk Drives
On a virtual machine, increase the size of a disk partition.	Follow the steps in the VMware topic: Increasing the size of a disk partition

Changing the performance statistics collection interval

The default collection interval for performance statistics is 5 minutes. You can change this interval to 10 or 15 minutes if you find that collections from large clusters are not finishing within the default time. This setting affects the collection of statistics from all clusters that this instance of Unified Manager is monitoring.

Before you begin

You must have a user ID and password authorized to log in to the maintenance console of the Unified Manager server.

About this task

The issue of performance statistics collections not finishing on time is indicated by the banner messages `Unable to consistently collect from cluster <cluster_name>` or `Data collection is taking too long on cluster <cluster_name>`.

You should change the collection interval only when required because of a statistics collections issue. Do not change this setting for any other reason.

> Changing this value from the default setting of 5 minutes can affect the number and frequency of performance events that Unified Manager reports. For example, system-defined performance thresholds trigger events when the policy is exceeded for 30 minutes. When using 5-minute collections, the policy must be exceeded for six consecutive collections. For 15-minute collections the policy must be exceeded for only two collection periods.

A message at the bottom of the Cluster Setup page indicates the current statistical data collection interval.

Steps

1. Log in using SSH as the maintenance user to the Unified Manager host.

   The Unified Managermaintenance console prompts are displayed.

2. Type the number of the menu option labeled **Performance Polling Interval Configuration**, and then press Enter.
3. If prompted, enter the maintenance user password again.
4. Type the number for the new polling interval that you want to set, and then press Enter.

After you finish

If you changed the Unified Manager collection interval to 10 or 15 minutes, and you have a current connection to an external data provider (such as Graphite), you must change the data provider transmit interval so that it is equal to, or greater, than the Unified Manager collection interval.

Changing the length of time Unified Manager retains event and performance data

By default, Unified Manager stores event data and performance data for 6 months for all monitored clusters. After this time, older data is automatically deleted to make room for new data. This default timeframe works well for most configurations, but very large configurations with many clusters and nodes may need to reduce the retention period so that Unified Manager operates optimally.

Before you begin

You must have the Application Administrator role.

About this task

You can change the retention periods for these two types of data in the Data Retention page. These settings affect the retention of data from all clusters that this instance of Unified Manager is monitoring.

Unified Manager collects performance statistics every 5 minutes. Each day the 5-minute statistics are summarized into hourly performance statistics. It retains 30 days of 5-minute historical performance data and 6 months of hourly summarized performance data (by default).

You should reduce the retention period only if you are running out of space or if backup and other operations are taking a very long time to complete. Reducing the retention period has the following effects:

- Old performance data is deleted from the Unified Manager database after midnight.
- Old event data is deleted from the Unified Manager database immediately.
- Events prior to the retention period will no longer be available to view in the user interface.
- Locations in the UI where hourly performance statistics are displayed will be blank prior to the retention period.
- If the event retention period exceeds the performance data retention period, a message will be displayed

under the performance slider warning that older performance events may not have backing data in their associated charts.

Steps

1. In the left navigation pane, click **Policies** > **Data Retention**.
2. In the **Data Retention** page, select the slider tool in the Event Retention or Performance Data Retention area and move it to the number of months that data should be retained, and click **Save**.

Enabling periodic AutoSupport

You can choose to have specific, predefined AutoSupport messages sent automatically from Unified Manager to technical support to ensure correct operation of your environment, and to assist you in maintaining the integrity of your environment. AutoSupport is enabled by default, and it must not be disabled in order for you to receive the benefits of NetAppActive IQ.

Before you begin

You must be logged in as the maintenance user.

About this task

Active IQ is a web-based application hosted on the NetApp Support Site that you can access using a browser. Your system must have AutoSupport enabled and configured so that it sends data back to NetApp.

NetApp Active IQ

Steps

1. In the left navigation pane, click **General** > **AutoSupport**.
2. Select the **Enable Sending AutoSupport Data Periodically to Active IQ** check box.
3. If required, define the name, port, and authentication information for the HTTP proxy server.
4. Click **Save**.

Sending on-demand AutoSupport messages

You can send Unified Manager system information to technical support for assistance with troubleshooting issues. The AutoSupport message contains diagnostic system information and detailed data about the Unified Manager server.

Before you begin

You must be logged in as the maintenance user.

Steps

1. In the left navigation pane, click **General** > **AutoSupport**.

2. Perform one or both of the following actions:

If you want to send the AutoSupport message to…	Do this…
Technical support	Select the **Send to Technical Support** check box.
A specific email recipient	Select the **Send to Email Recipient** check box, and enter the email address of the recipient.

3. If required, define the name, port, and authentication information for the HTTP proxy server, and click **Save**.
4. Click **Generate and Send AutoSupport**.

AutoSupport page

The AutoSupport page enables you to enable periodic AutoSupport, or to send an on-demand AutoSupport message to NetAppActive IQ. AutoSupport is enabled by default.

Information area

- **System ID**

  Displays the system ID for this Unified Manager server.

On-Demand AutoSupport area

You can generate and send an on-demand message to technical support, a specified email recipient, or both:

- **Send to Technical Support**

  Indicates that you want to send an on-demand message to technical support for any issues that have occurred.

- **Send to Email Recipient**

  Indicates that you want to send an on-demand message to a specified recipient for any issues that have occurred.

- **Generate and Send AutoSupport**

  Generates and sends an on-demand message to technical support, a specified email recipient, or both for any issues that have occurred.

Periodic AutoSupport area

Enables you to have specific, predefined messages to technical support for issue diagnosis and resolution periodically generated.

- **Enable Sending AutoSupport Data Periodically to Active IQ**

Indicates that you want to enable the periodic AutoSupport functionality. This functionality is enabled by default.

HTTP Proxy area

You can designate a proxy to provide Internet access in order to send AutoSupport content to support if your environment does not provide direct access from the Unified Manager server.

- **Use HTTP proxy**

  Check this box to identify the server being used as the HTTP proxy.

  Enter the host name or IP address of the proxy server, and the port number used to connect to the server.

- **Use authentication**

  Check this box if you need to provide authentication information to access the server being used as the HTTP proxy.

  Enter the user name and the password required to authenticate with the HTTP proxy.

HTTP proxies that provide only Basic Authentication are not supported.

Unknown authentication error

- **Issue**

  When you are performing an authentication-related operation such as adding, editing, deleting, or testing remote users or groups, the following error message might be displayed: `Unknown authentication error`.

- **Cause**

  This problem can occur if you have set an incorrect value for the following options:

  - Administrator Name of the Active Directory authentication service
  - Bind Distinguished Name of the OpenLDAP authentication service

- **Corrective action**

  a. In the left navigation pane, click **General** > **Remote Authentication**.

  b. Based on the authentication service that you have selected, enter the appropriate information for Administrator Name or Bind Distinguished Name.

  c. Click **Test Authentication** to test the authentication with the details that you specified.

  d. Click **Save**.

User not found

- **Issue**

  When you are performing an authentication-related operation such as adding, editing, deleting, or testing

remote users or groups, the following error message is displayed: `User not found`.

- **Cause**

  This problem can occur if the user exists in the AD server or LDAP server, and if you have set the base distinguished name to an incorrect value.

- **Corrective action**

  a. In the left navigation pane, click **General** > **Remote Authentication**.

  b. Enter the appropriate information for base distinguished name.

  c. Click **Save**.

Issue with adding LDAP using Other authentication services

- **Issue**

  When you select Others as the Authentication service, the user and groupObjectClass retain the values from the previously selected template. If the LDAP server does not use the same values, the operation might fail.

- **Cause**

  The users are not configured correctly in OpenLDAP.

- **Corrective action**

  You can manually fix this issue by using one of the following workarounds.

  If your LDAP user object class and group object class are user and group, respectively, perform the following steps:

  a. In the left navigation pane, click**General** > **Remote Authentication**.

  b. In the **Authentication Service** drop-down menu, select **Active Directory**, and then select **Others**.

  c. Complete the text fields. If your LDAP user object class and group object class are posixAccount and posixGroup, respectively, perform the following steps:

  d. In the left navigation pane, click**General** > **Remote Authentication**.

  e. In the **Authentication Service** drop-down menu, select **OpenLDAP**, and then select **Others**.

  f. Complete the text fields. If the first two workarounds do not apply, call the `option-set` API, and set the `auth.ldap.userObjectClass` and `auth.ldap.groupObjectClass` options to the correct values.

Copyright information

Trademark information