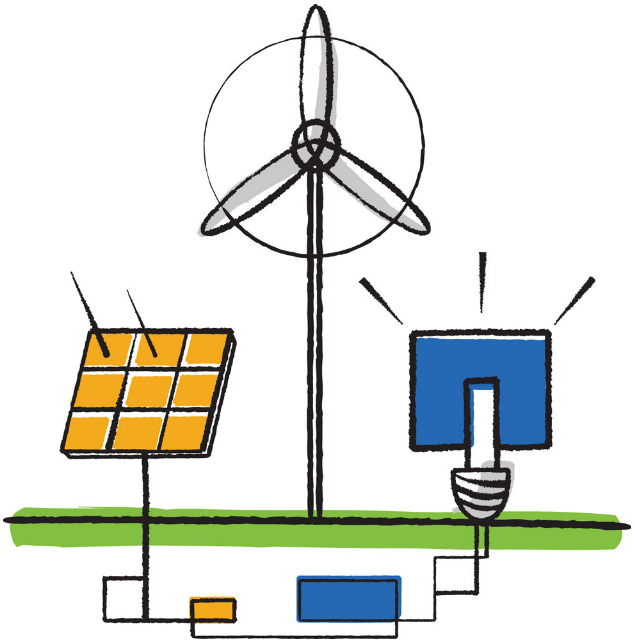
Updated for 8.3.1

Clustered Data ONTAP® 8.3

Performance Monitoring Power Guide



NetApp, Inc.
495 East Java Drive
Sunnyvale, CA 94089
U.S.

Telephone: +1 (408) 822-6000
Fax: +1 (408) 822-4501
Support telephone: +1 (888) 463-8277
Web: www.netapp.com
Feedback: doccomments@netapp.com

Part number: 215-10424_A0
September 2015

Contents

Deciding whether to use this guide

This guide describes how to install and configure both OnCommand Unified Manager and OnCommand Performance Manager, how to set up basic performance management tasks, and how to identify and resolve common performance issues.

You should use this guide if you want to monitor cluster performance in the following way:

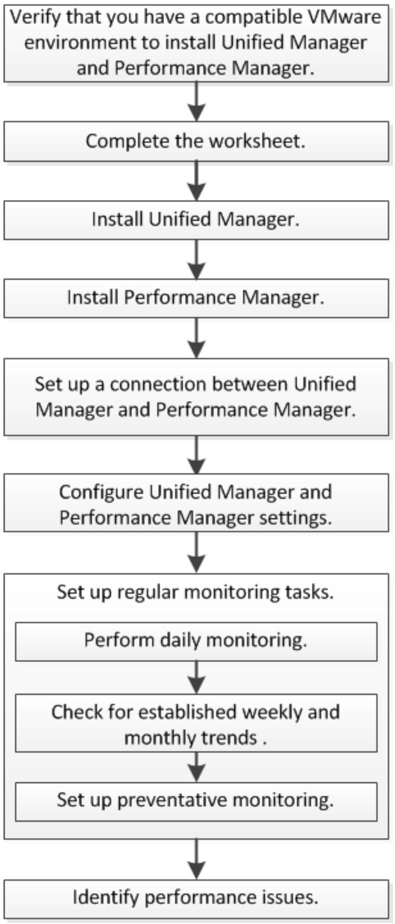
- You want to use best practices, not explore every available option.
- You do not want to read a lot of conceptual background.
- You want to display system status and alerts using Unified Manager 6.3 or later, in addition to the Data ONTAP command-line interface.
- You want to monitor cluster performance and perform root-cause analysis using Performance Manager 2.0 or later, in addition to the Data ONTAP command-line interface.
- You want to install the performance software using a virtual appliance, instead of a Linux or Windows-based installation.
- You want to use a static configuration rather than DHCP to install the software.
- You want to connect one instance of Performance Manager to Unified Manager.
- You can access Data ONTAP commands at the advanced privilege level.
- You have determined that the cause of the performance issue is storage-related.
- You have ruled out any client-side protocol and network issues.

If these assumptions are not correct for your situation, you should see the following resources:

- *OnCommand Unified Manager 6.3 Installation and Setup Guide for VMware Virtual Appliances*
- *OnCommand Performance Manager 2.0 Installation and Administration Guide for VMware Virtual Appliances*
- *Clustered Data ONTAP 8.3 System Administration Guide*
- *Data ONTAP 8.3.1 Performance Monitoring Express Guide*

Performance monitoring workflow

Monitoring cluster performance involves installing software, setting up basic monitoring tasks, and identifying performance issues.


Verify that you have a compatible VMware environment to install Unified Manager and Performance Manager.
Complete the worksheet.
Install Unified Manager.
Install Performance Manager.
Set up a connection between Unified Manager and Performance Manager.
Configure Unified Manager and Performance Manager settings.
Set up regular monitoring tasks.
Perform daily monitoring.
Check for established weekly and monthly trends .
Set up preventative monitoring.
Identify performance issues.

Steps

1. Verifying that your environment is supported on page 6
   To ensure successful installation, you must verify that your VMware environment meets the necessary requirements. The Interoperability Matrix lists the supported configurations for both OnCommand Unified Manager and OnCommand Performance Manager.
2. Completing the worksheet on page 6
   Before you install, configure, and connect Unified Manager and Performance Manager, you should have specific information about your environment readily available.
3. Installing Unified Manager on page 8
   This guide assumes that you will install Unified Manager before installing Performance Manager and monitoring cluster performance.
4. Installing Performance Manager on page 9
   You must install Performance Manager before you can monitor cluster performance.
5. Setting up the connection between Performance Manager and Unified Manager on page 10
   This guide assumes that before monitoring cluster performance, you will connect Performance Manager to Unified Manager.

6. **Configuring Unified Manager and Performance Manager** on page 11
   To be notified of events, you must configure Unified Manager to send alert notifications and configure Performance Manager to export events to Unified Manager.
7. **Setting up basic monitoring tasks** on page 13
   You can monitor your systems for performance issues by checking them daily and thereby establishing weekly and monthly performance trends. You can also create thresholds to prevent critical performance issues.

Verifying that your environment is supported

To ensure successful installation, you must verify that your VMware environment meets the necessary requirements. The Interoperability Matrix lists the supported configurations for both OnCommand Unified Manager and OnCommand Performance Manager.

Steps

1. Verify that your VMware infrastructure meets the sizing requirements for installation of both Unified Manager and Performance Manager.
2. Go to the *NetApp Interoperability Matrix Tool* to verify that you have a supported combination of the following components:
   - Data ONTAP version
   - ESXi operating system version
   - VMware vCenter Server version
   - VMware Tools version
   - Browser type and version
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.

Completing the worksheet

Before you install, configure, and connect Unified Manager and Performance Manager, you should have specific information about your environment readily available.

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	

Virtual machine on which software is deployed	Your value
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	
Default port	25 (Default value)
Username for user with Event Publisher role	
Password for user with Event Publisher role	
Email from which alert notifications are sent	
Active Directory administrator name	
Active Directory password	
Base distinguished name	
Active Directory server host name or IP address	

Performance Manager installation information

Virtual machine on which software is deployed	Your value
Host fully qualified domain name	
IP address	
Network mask	
Gateway IP address	
DNS address	
Maintenance user name	
Maintenance user password	

Performance Manager configuration information

Setting	Your value
Email from which alert notifications are sent	
SMTP server host name or IP address	
SMTP user name	
SMTP password	
Default port	25 (Default value)
Active Directory administrator name	
Active Directory password	
Base distinguished name	
Active Directory server host name or IP address	

Cluster information

Cluster	Your value
Host name or cluster-management IP address	
Data ONTAP administrator user name	
Data ONTAP administrator password	
Protocol (HTTP or HTTPS)	

Installing Unified Manager

This guide assumes that you will install Unified Manager before installing Performance Manager and monitoring cluster performance.

Downloading and deploying 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 OnCommand Unified Manager for Clustered Data ONTAP.

   NetApp Downloads: Software

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.

Configuring initial Unified Manager settings

The OnCommand Unified Manager Initial SetupUnified Manager dialog box appears when you first access the web UI and enables you to configure some initial settings and to add clusters.

Steps

1. Enable AutoSupport.
2. Enter the NTP server, the maintenance user email address, the SMTP server host name and additional SMTP options, and click **Save**.
3. Click **Add Cluster** and add all of your clusters for monitoring.

Installing Performance Manager

You must install Performance Manager before you can monitor cluster performance.

Downloading and deploying Performance 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 OnCommand Performance Manager (Unified Manager Performance Pkg).

   NetApp Downloads: Software
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.
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 VM.
   a. Enter the time zone information.
   b. Enter the fully qualified domain name.
   c. Enter the IP address and netmask.

   d. Enter the DNS server IP address.
   e. Enter the gateway IP address.
   f. Enter the maintenance user name and password.
   g. Enter the OnCommand login.

Configuring initial Performance Manager settings

The setup wizard enables you to configure some initial settings and to add clusters for monitoring.

Steps

1. Log in to the web UI with your maintenance user name and password.
2. Specify where to send email alerts.
3. Enable AutoSupport.
4. Change the maintenance user password.
5. Add clusters.
   a. Go to **Administration > Data Sources**.
   b. Click **Add** and specify the required values.
      All clusters that you add in Performance Manager must also be added in Unified Manager.

Setting up the connection between Performance Manager and Unified Manager

This guide assumes that before monitoring cluster performance, you will connect Performance Manager to Unified Manager.

Creating a user that has Event Publisher privileges

Before setting up the connection, you must create a local user in Unified Manager that has the Event Publisher role and privileges. This user receives the performance incident notifications.

Steps

1. In the Unified Manager UI, click **Administration > Manage Users**.
2. Click **Add**.
3. Select **Local User** as the type and **Event Publisher** as the role.
4. Finish entering the information in the dialog box and click **Add**.

Setting up the connection between Performance Manager and Unified Manager

Before you can see performance issues in the Unified Manager web UI, you must configure the connection between the Performance Manager server and Unified Manager.

Steps

1. Log in to the Performance Manager maintenance console.

2. Select **Add/Modify Unified Manager Server Connection**.
3. Type the Unified Manager server name or IP address.
4. Type **443** for the Unified Manager server port.
5. Enter the Event Publisher user name and password.

Configuring Unified Manager and Performance Manager

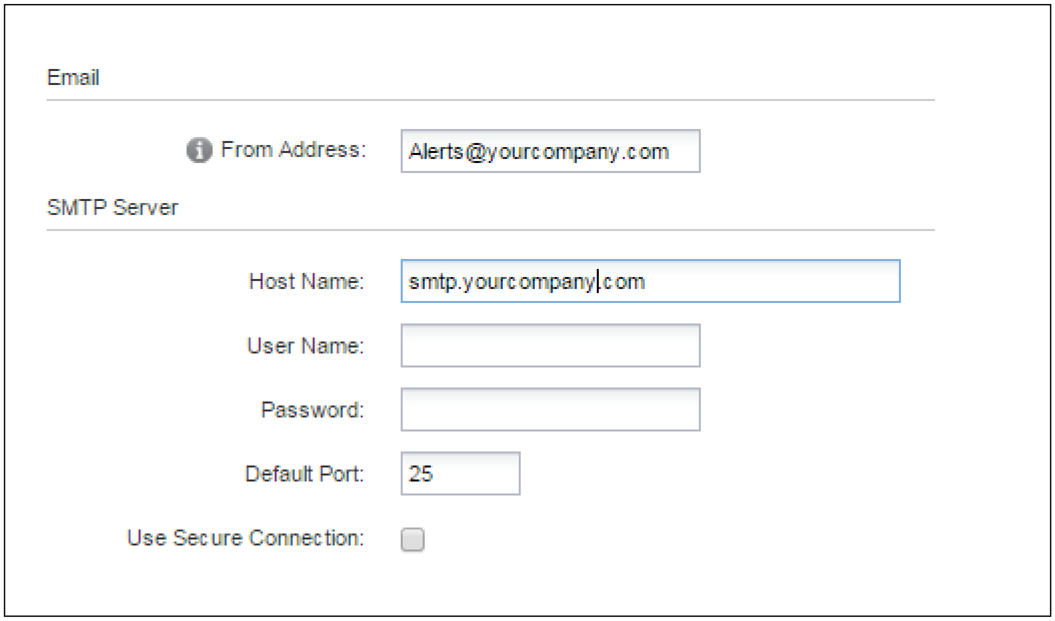
To be notified of events, you must configure Unified Manager to send alert notifications and configure Performance Manager to export events to Unified Manager.

Configuring alert notifications

Configuring email alert notifications enables Unified Manager to notify you if an alert occurs. While you can also configure alert notifications in Performance Manager, doing so means that you receive duplicate emails about the same alerts.

Steps

1. Click **Administration** > **Setup Options** > **General Settings** > **Notification**.
2. Specify the email address from which Unified Manager sends the alert notifications.
3. Specify the SMTP server host name, user name, password, and default port.



Email

From Address: Alerts@yourcompany.com

SMTP Server

Host Name: smtp.yourcompany.com

User Name:

Password:

Default Port: 25

Use Secure Connection: ☐

Exporting performance events to Unified Manager

To see performance events in the Unified Manager dashboard, you must export them from Performance Manager.

Steps

1. In the Performance Manager web UI, select **Configuration** > **Event Handling**.
2. For user-defined threshold policies, check **Export these events to OnCommand Unified Manager as...** to export as critical and warning events.

3. For system-defined threshold policies, check **Export these events to OnCommand Unified Manager as...** to export as warning events.
4. For dynamic threshold policies, check **Export these events to OnCommand Unified Manager as...** to export as warning events.

Enabling remote authentication in Unified Manager

Using Active Directory enables your management servers to communicate with the authentication servers, so that remote users or groups can manage storage object performance.

Steps

1. Click **Administration > Setup Options**.
2. Click **Management Server > Authentication**.
3. Select **Enable Remote Authentication**.
4. Select **Active Directory** as the authentication service.
5. Enter the administrator name.

   The following formats are supported:

   - domainname\username
   - username@domainname
   - Bind Distinguished Name, using the appropriate LDAP notation
6. Enter the administrator password.
7. Enter the base distinguished name of the authentication server.

   #### Example

   For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is dc=ou, dc=domain, dc=com.
8. Add authentication servers:
   a. In the **Servers** area, click **Add**.
   b. Enter the host name or IP address and the port information.
   c. Click **Add**.
9. If applicable, add partner authentication servers.
10. Test the authentication servers.

Enabling remote authentication in Performance Manager

Using Active Directory enables your management servers to communicate with the authentication servers, so that remote users or groups can manage cluster performance.

Steps

1. Click **Administration > Authentication**.
2. Select **Enable Remote Authentication**.
3. Select **Active Directory** as the authentication service.

4. Enter the administrator name.

   The following formats are supported:

   - domainname\username
   - username@domainname
   - Bind Distinguished Name, using the appropriate LDAP notation

5. Enter the administrator password.
6. Enter the base distinguished name of the authentication server.

   Example

   For example, if the domain name of the authentication server is ou@domain.com, then the base distinguished name is dc=ou, dc=domain, dc=com.

7. Add authentication servers:
   a. In the **Servers** area, click **Add**.
   b. Enter the host name or IP address and the port information.
   c. Click **Submit**.
8. If applicable, add partner authentication servers.
9. Test the authentication servers.

Setting up basic monitoring tasks

You can monitor your systems for performance issues by checking them daily and thereby establishing weekly and monthly performance trends. You can also create thresholds to prevent critical performance issues.

Performing 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 Performance Manager UI, go to the **Event Inventory** page and view all current and obsolete events.
2. Click on the new Critical or Warning events and determine what action is required.

Using 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 you suspect is being underused or overused.
2. On the **Details** tab, click **30 days** to display the historical data.

3. In the “Break down data by” drop-down menu, select **Latency** and click **Submit**.
4. Deselect Aggregate in the Compare the Cluster Components chart and compare with the Latency chart.
5. Select Aggregate and deselect all other components in the Compare the Cluster Components chart and compare with the Latency chart.
6. Compare the reads/writes latency chart to the Latency chart.
7. Determine if client application loads have caused a workload contention and rebalance workloads as needed.
8. Determine if the aggregate is overused and causing contention and rebalance workloads as needed.

Preventing performance issues

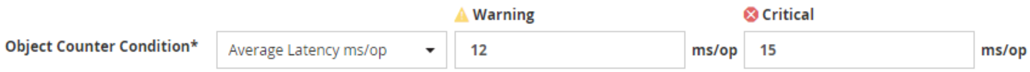
You can set user-defined thresholds to prevent performance issues from being critical. For example, if you have a Microsoft Exchange Server and you know that it will crash if volume latency goes above 20 milliseconds, you can set warning and critical thresholds to keep the server from crashing.

Steps

1. Create the Warning and Critical event thresholds:
   a. Select **Configuration** > **Threshold Policies**.
   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 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.
   b. Select the object to which you want to assign the threshold policy and click **Assign Threshold Policy**.
   c. Select the policy you previously created and click **Assign Policy**.

Example

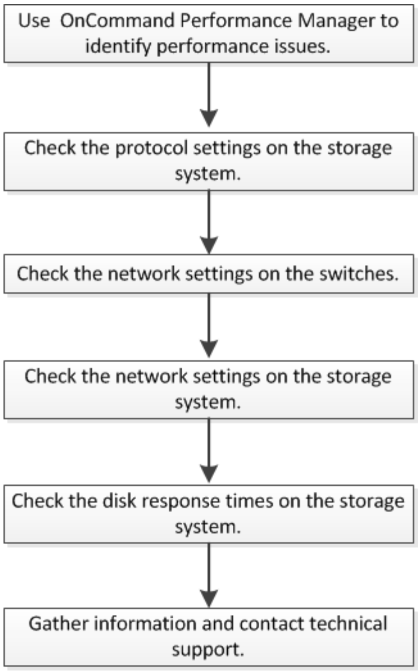
You want to prevent your Microsoft Exchange Server from crashing due to average volume latency exceeding 20 milliseconds. The following example displays the Warning threshold set to 12 milliseconds and the Critical threshold to 15 milliseconds.



		Warning		Critical	
Object Counter Condition*	Average Latency ms/op	12	ms/op	15	ms/op

Identifying and resolving performance issues workflow

Identifying and resolving performance issues includes using Performance Manager to troubleshoot the issue, and then checking network and protocol settings to locate the source of the performance issue.


Use OnCommand Performance Manager to identify performance issues.
Check the protocol settings on the storage system.
Check the network settings on the switches.
Check the network settings on the storage system.
Check the disk response times on the storage system.
Gather information and contact technical support.

Steps

1. Using Performance Manager to identify performance issues on page 16
   If you receive an email notification or someone otherwise notifies you that there is a performance issue, you can locate the source of the issue within Performance Manager and potentially resolve it by using other tools. If the issue is not resolved using the remediation in Performance Manager, you can perform other checks to identify the source of the issue and resolve it.
2. Checking protocol settings on the storage system on page 16
   You can check that a performance issue is not related to protocol settings on your storage system. If the settings are the issue, you can take corrective action and then verify that the performance issue is resolved.
3. Checking the network settings on the data switches on page 18
   You must maintain the same network settings on your clients, storage systems, and switches to ensure that performance is not impacted. All components in the network must have the same MTU setting for best performance.
4. Checking the MTU network setting on the storage system on page 19
   You can change the network settings on the storage system if they are not the same as on the client or data switches. Whereas the management network MTU setting is set to 1500, the data network MTU size should be 9000.
5. Checking the disk response times on page 19
   You can check to see what the disk response times are, and whether the aggregate I/O workload is sequential or random, to assist you in troubleshooting.

6. Contacting technical support on page 20
   If a performance issue remains, you should contact technical support for additional help.

Using Performance Manager to identify performance issues

If you receive an email notification or someone otherwise notifies you that there is a performance issue, you can locate the source of the issue within Performance Manager and potentially resolve it by using other tools. If the issue is not resolved using the remediation in Performance Manager, you can perform other checks to identify the source of the issue and resolve it.

About this task

You might need to use a combination of tools, like Unified Manager or the CLI, to resolve the issue.

Steps

1. Click the link in the email notification, which takes you directly to the **Event Details** page.
2. If the performance issue is due to a system-defined threshold event, perform the suggested actions in the UI.
3. Verify in the Performance Manager **Events Summary** page that the issue has been resolved.

Checking protocol settings on the storage system

You can check that a performance issue is not related to protocol settings on your storage system. If the settings are the issue, you can take corrective action and then verify that the performance issue is resolved.

Checking the NFS TCP read/write size

For NFS, you can check the TCP read/write size to determine if the size setting is creating a performance issue. If the size is the source of an issue, you can correct it.

About this task

Advanced privilege level commands are required for this task.

Steps

1. For NFS, check the TCP receive window size:

   ```
   vserver nfs show -vserver vserver_name -instance
   ```

2. Change the TCP maximum read size:

   ```
   vserver nfs modify -vserver vserver_name -v3-tcp-max-read-size integer
   ```

3. Change the TCP maximum write size:

   ```
   vserver nfs modify -vserver vserver_name -v3-tcp-max-write-size integer
   ```

   Example

   The following example changes the maximum read and write size of vs1 to 1048576:

```
cluster1::*> vserver nfs modify -vserver vs1 -v3-tcp-max-read-size
1048576  -v3-tcp-max-write-size 1048576
```

Related information

Clustered Data ONTAP 8.3.1 man page: vserver nfs modify - Modify the NFS configuration of a Vserver

Checking the iSCSI TCP read/write size

For iSCSI, you can check the TCP read/write size to determine if the size setting is creating a performance issue. If the size is the source of an issue, you can correct it.

About this task

Advanced privilege level commands are required for this task.

Steps

1. Check the TCP window size setting:

   ```
   vserver iscsi show -vserver vserver_name -instance
   ```

2. Modify the TCP window size setting:

   ```
   vserver iscsi modify -vserver vserver_name -tcp-window-size integer
   ```

Example

The following example changes the TCP window size of vs1 to 131,400 bytes:

```
cluster1::*> vserver iscsi modify -vserver vs1 -tcp-window-size
131400
```

Related information

Clustered Data ONTAP 8.3.1 man page: vserver iscsi modify - Modify a Vserver's iSCSI service

Checking the CIFS multiplex settings

If slow CIFS network performance causes a performance issue, you can modify the multiplex settings to improve and correct it.

Steps

1. Check the CIFS multiplex setting:

   ```
   vserver cifs options show -vserver -vserver_name -instance
   ```

2. Modify the CIFS multiplex setting:

   ```
   vserver cifs options modify –vserver -vserver_name –max-mpx integer
   ```

Example

The following example changes the maximum multiplex count on SVM1 to 255:

```
cluster1::> vserver cifs options modify -vserver SVM1 -max-mpx 255
```

Checking the FC adapter port speed

The adapter target port speed should match the speed of the device to which it connects, to optimize performance. If the port is set to autonegotiation, it can take longer to reconnect after a takeover and giveback or other interruption.

Before you begin

All LIFs that use this adapter as their home port must be offline.

Steps

1. Take the adapter offline:

   `network fcp adapter modify -node` ***`nodename`*** **`-adapter`** ***`adapter`*** **`-state`** ***`down`***

2. Check the maximum speed of the port adapter:

   `fcp adapter show -instance`

3. Change the port speed, if necessary:

   `network fcp adapter modify -node` ***`nodename`*** **`-adapter`** ***`adapter`*** **`-speed {`*****`1`*****`|`*****`2`*****`|`*****`4`*****`|`*****`8`*****`|`*****`10`*****`|`*****`16`*****`|`*****`auto`*****`}`**

4. Bring the adapter online:

   `network fcp adapter modify -node` ***`nodename`*** **`-adapter`** ***`adapter`*** **`-state`** ***`up`***

5. Bring all the LIFs on the adapter online:

   `network interface modify -vserver * -lif * { -home-node node1 -home-port e0c } -status-admin up`

Example

The following example changes the port speed of adapter 0d on node1 to 2 Gbps:

```
cluster1::> network fcp adapter modify -node node1 -adapter 0d -
speed 2
```

Checking the network settings on the data switches

You must maintain the same network settings on your clients, storage systems, and switches to ensure that performance is not impacted. All components in the network must have the same MTU setting for best performance.

Step

1. For data switches, check that the MTU size is set to 9000.

   For more information, see the switch vendor documentation.

Checking the MTU network setting on the storage system

You can change the network settings on the storage system if they are not the same as on the client or data switches. Whereas the management network MTU setting is set to 1500, the data network MTU size should be 9000.

Steps

1. Check the MTU port settings on the storage system:

   `network port show -instance`

2. Change the MTU port settings to 9000:

   `network port modify -node` ***`nodename`*** **`-port`** ***`port`*** **`-mtu`** ***`9000`***

Checking the disk response times

You can check to see what the disk response times are, and whether the aggregate I/O workload is sequential or random, to assist you in troubleshooting.

About this task

Advanced privilege level commands are required for this task.

Step

1. Check the disk throughput and latency metrics:

   `statistics disk show -sort-key latency`

Example

The following example displays the totals in each user read or write operation for node2 on cluster1:

```
::*> statistics disk show -sort-key latency
cluster1 : 8/24/2015 12:44:15
                    Busy Total Read  Write  Read    Write
*Latency
  Disk       Node  (%)   Ops   Ops   Ops   (Bps)    (Bps)
(us)
------------ ----   ---- ----   ----- ----- ------   -----    -----

1.10.20      node2     4    5       3     2  95232  367616    23806
1.10.8       node2     4    5       3     2 138240  386048    22113

1.10.6       node2     3    4       2     2  48128  371712    19113
1.10.19      node2     4    6       3     2 102400  443392    19106

1.10.11      node2     4    4       2     2 122880  408576    17713
```

Related information

Clustered Data ONTAP 8.3.1 man page: statistics disk show - Disk throughput and latency metrics

Contacting technical support

If a performance issue remains, you should contact technical support for additional help.

Step

1. Contact technical support.

Where to find additional information

After you have successfully installed and configured Unified Manager and Performance Manager and set up monitoring tasks, you can perform more advanced tasks.

- *OnCommand Unified Manager 6.3 Installation and Setup Guide for VMware Virtual Appliances*
  Provides instructions for installing the Unified Manager appliance on a VMware ESXi server.
- *OnCommand Unified Manager 6.3 Administration Guide*
  Provides information about performing Unified Manager tasks and troubleshooting.
- *OnCommand Performance Manager 2.0 Installation and Administration Guide for VMware Virtual Appliances*
  Provides instructions for installing the Performance Manager appliance on a VMware ESXi server.
- *OnCommand Performance Manager 2.0 User Guide*
  Explains how to use Performance Manager.
- *Clustered Data ONTAP 8.3 System Administration Guide*
  Describes general system administration for storage systems running clustered Data ONTAP.
- *NetApp Technical Report 4211: NetApp Storage Performance Primer for Clustered Data ONTAP 8.3*
  Describes the basic performance concepts in clustered Data ONTAP, how different processes can impact performance, and how to observe cluster performance.
- *NetApp Technical Report 4448: OnCommand Performance Manager Best Practices (OnCommand Performance Manager Version 2.0)*
  Describes some best practices when using Performance Manager to manage storage systems running clustered Data ONTAP.

Copyright information

Trademark information

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email to *doccomments@netapp.com*. To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

- NetApp, Inc., 495 East Java Drive, Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277

Index