Performance Monitoring Express Guide
Deciding whether to use the Performance Monitoring Express Guide

This guide describes how to quickly install and configure OnCommand Unified Manager, how to perform basic monitoring tasks, and how to identify performance issues.

You should use this guide if you want to monitor cluster performance, and the following assumptions apply to your situation:

• 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 install Unified Manager by using a virtual appliance, instead of a Linux or Windows-based installation.
• You're willing to use a static configuration rather than DHCP to install the software.
• You are a cluster administrator with the “admin” role.

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

• OnCommand Unified Manager 9.4 Installation and Setup Guide
• System administration
Monitoring cluster performance involves installing software, setting up basic monitoring tasks, and identifying performance issues.

Steps

1. **Verifying that your VMware environment is supported** on page 6
   For successful installation of Unified Manager, you must verify that your VMware environment meets the necessary requirements.

2. **Unified Manager worksheet** on page 6
   Before you install, configure, and connect Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

3. **Installing Unified Manager** on page 7
   To install Unified Manager to monitor cluster performance, follow these procedures.

4. **Specifying the clusters to be monitored** on page 8
   You must add a cluster to a Unified Manager server to monitor the cluster, view the cluster discovery status, and monitor its performance.

5. **Setting up basic monitoring tasks** on page 10
   You can monitor your systems for performance issues by checking the systems daily, by establishing weekly and monthly performance trends, and by specifying thresholds for receipt of notifications about potential performance issues.

6. **Identifying performance issues in Unified Manager** on page 12
If a performance event occurs, you can locate the source of the issue within 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.

**Verifying that your VMware environment is supported**

For successful installation of 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 available at mysupport.netapp.com/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

   **Note:** 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.

**Unified Manager worksheet**

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

**Unified Manager installation information**

<table>
<thead>
<tr>
<th>Virtual machine on which software is deployed</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESXi server IP address</td>
<td></td>
</tr>
<tr>
<td>Host fully qualified domain name</td>
<td></td>
</tr>
<tr>
<td>Host IP address</td>
<td></td>
</tr>
<tr>
<td>Network mask</td>
<td></td>
</tr>
<tr>
<td>Gateway IP address</td>
<td></td>
</tr>
<tr>
<td>Virtual machine on which software is deployed</td>
<td>Your value</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>Primary DNS address</td>
<td></td>
</tr>
<tr>
<td>Secondary DNS address</td>
<td></td>
</tr>
<tr>
<td>Search domains</td>
<td></td>
</tr>
<tr>
<td>Maintenance user name</td>
<td></td>
</tr>
<tr>
<td>Maintenance user password</td>
<td></td>
</tr>
</tbody>
</table>

### Unified Manager configuration information

<table>
<thead>
<tr>
<th>Setting</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maintenance user email address</td>
<td></td>
</tr>
<tr>
<td>NTP server</td>
<td></td>
</tr>
<tr>
<td>SMTP server host name or IP address</td>
<td></td>
</tr>
<tr>
<td>SMTP user name</td>
<td></td>
</tr>
<tr>
<td>SMTP password</td>
<td></td>
</tr>
<tr>
<td>SMTP default port</td>
<td>25 (Default value)</td>
</tr>
<tr>
<td>Email from which alert notifications are sent</td>
<td></td>
</tr>
<tr>
<td>LDAP bind distinguished name</td>
<td></td>
</tr>
<tr>
<td>LDAP bind password</td>
<td></td>
</tr>
</tbody>
</table>

### Cluster information

Capture the following information for each cluster on Unified Manager.

<table>
<thead>
<tr>
<th>Cluster 1 of N</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host name or cluster-management IP address</td>
<td></td>
</tr>
<tr>
<td>ONTAP administrator user name</td>
<td></td>
</tr>
<tr>
<td><strong>Note:</strong> The administrator must have been assigned the “admin” role.</td>
<td></td>
</tr>
<tr>
<td>ONTAP administrator password</td>
<td></td>
</tr>
<tr>
<td>Protocol (HTTP or HTTPS)</td>
<td></td>
</tr>
</tbody>
</table>

### Related information

*Administrator authentication and RBAC*

### Installing Unified Manager

To install Unified Manager to monitor cluster performance, follow these procedures.
**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**


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 OnCommand Unified Manager settings**

The OnCommand 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.

**Specifying the clusters to be monitored**

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

**Before you begin**

- 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 OnCommand 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 Configuration/Cluster Data Sources page.

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

You can monitor your systems for performance issues by checking the systems daily, by establishing weekly and monthly performance trends, and by specifying thresholds for receipt of notifications about potential 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 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.

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 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.

Using performance thresholds to generate event notifications

Events are notifications that the 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.
Setting 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.
   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.

```
<table>
<thead>
<tr>
<th>Object Counter Condition</th>
<th>Warning</th>
<th>Critical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average Latency ms/op</td>
<td>12</td>
<td>15</td>
</tr>
</tbody>
</table>
```

Configuring alert settings

You can specify which events from Unified Manager trigger alerts, the email recipients for those alerts, and whether the events should be reported to Unified Manager.

**Before you begin**

You must have the OnCommand 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 choose to send the alerts as Critical, Error, Warning, or Information events. You can have email alerts sent to other users by adding those users' email addresses.

**Note:** 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 **Configuration > Alerting**. The Performance Alerting page is displayed.

2. In the **Performance Alerting** page, 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**.

**Identifying performance issues in Unified Manager**

If a performance event occurs, you can locate the source of the issue within 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.

<table>
<thead>
<tr>
<th>If you...</th>
<th>Then...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive an email notification of an event</td>
<td>Click the link to go directly to the event details page.</td>
</tr>
<tr>
<td>Notice the event while analyzing the Event Inventory page</td>
<td>Select the event to go directly to the event details page.</td>
</tr>
</tbody>
</table>

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.
Where to find additional information

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

- **OnCommand Unified Manager 9.4 Installation and Setup Guide**
  Provides instructions for installing the Unified Manager appliance on a VMware ESXi server.

- **OnCommand Unified Manager 9.4 Workflow Guide for Managing Cluster Performance**
  Provides information about performing Unified Manager tasks and troubleshooting.

- **System administration**
  Describes general system administration for storage systems running ONTAP.

- **NetApp Technical Report 4211: Storage Performance Primer**
  Describes the basic performance concepts in ONTAP, how different processes can impact performance, and how to observe cluster performance.
Copyright information

Copyright © 2018 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).
Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

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.

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., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.
- Telephone: +1 (408) 822-6000
- Fax: +1 (408) 822-4501
- Support telephone: +1 (888) 463-8277
Index

A
adding
   clusters 8
alerts
   configuring Unified Manager settings for 11
AutoSupport
   enabling in Unified Manager 8

C
clusters
   adding 8
   adding in Unified Manager 8
   requirements for using the Performance Monitoring Express Guide to monitor 4
   viewing discovery status 8
comments
   how to send feedback about documentation 16
configuration
   pre-installation worksheet for Unified Manager 6
   verifying that your environment is supported 6

D
daily monitoring
   performing in Unified Manager 10
documentation
   additional information about performance monitoring 13
   how to receive automatic notification of changes to 16
   how to send feedback about 16

E
email notifications
   configuring Unified Manager settings for 11
event notifications
   introduction to using performance thresholds to generate 10
events
   performing daily monitoring in Unified Manager 10
   troubleshooting performance issues 12
express guides
   additional documentation 13
Express Guides
   requirements for using the Performance Monitoring Express Guide 4

F
feedback
   how to send comments about documentation 16
flowcharts
   performance monitoring 5

I
information
   how to send feedback about improving documentation 16
installation
   Unified Manager 8
Interoperability Matrix
   using to verify that your environment is supported 6
issues
   performance event troubleshooting 12
   using weekly and monthly performance trends to identify 10

M
-monitoring
cluster performance 8

N
notifications
   troubleshooting performance issues 12

O
OnCommand Unified Manager
   configuring initial settings 8
ONTAP systems
   See clusters

P
performance
   monitoring for clusters 8
   monitoring for clusters
   performance issues 12
   troubleshooting
   requirements for using the Performance Monitoring Express Guide 4
   workflow 5
performance monitoring tasks
   introduction to 10
performance thresholds
   introduction to using to generate event notifications 10
   setting 11
performance trends
   using weekly and monthly trends to identify performance issues 10
physical storage
   adding clusters 8

S
setting up
   basic monitoring tasks, introduction to 10
storage objects
applying thresholds to 11
using weekly and monthly trends to identify
performance issues 10

suggestions
how to send feedback about documentation 16

T
technical reports
additional information about performance monitoring 13
troubleshooting
performance issues 12
performing daily monitoring in Unified Manager 10
using weekly and monthly trends to identify
performance issues 10

Twitter
how to receive automatic notification of documentation changes 16

U
Unified Manager

configuring alert settings for 11
downloading and deploying 8
pre-installation worksheet 6
verifying that your configuration is supported 6

V
viewing
discovery status of clusters 8
virtual appliances
installing Unified Manager 8

W
workflows
performance monitoring 5
worksheet
for Unified Manager 6