



Setting up Unified Manager for high availability

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

This PDF was generated from <https://docs.netapp.com/us-en/oncommand-unified-manager-95/install/concept-requirements-for-unified-manager-in-vcs.html> on October 23, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Setting up Unified Manager for high availability 1
 - Requirements for Unified Manager in VCS 1
 - Installing Unified Manager on VCS 2
 - Configuring Unified Manager with VCS using configuration scripts 2
 - Unified Manager service resources for VCS configuration 4
 - Updating an existing Unified Manager setup for high availability 4

Setting up Unified Manager for high availability

You can create a high-availability setup by using the Veritas Cluster Server (VCS). The high-availability setup provides failover capability and helps in disaster recovery.

In a high-availability setup, only one node remains active at a time. When one node fails, VCS service recognizes this event and immediately transfers control to the other node. The second node in the setup becomes active and starts providing services. The failover process is automatic.

A VCS cluster configured with the Unified Manager server consists of two nodes, with each node running the same version of the Unified Manager. All of the Unified Manager server data must be configured for access from a shared data disk.

After you install Unified Manager in VCS, you must configure Unified Manager to work in the VCS environment. You can use configuration scripts to set up Unified Manager to work in VCS environments.

Requirements for Unified Manager in VCS

Before installing Unified Manager in a Veritas Cluster Server (VCS) environment, you must ensure that the cluster nodes are properly configured to support Unified Manager.

You must ensure that the VCS configuration meets the following requirements:

- Both the cluster nodes must be running a supported operating system version.
- The same version of Unified Manager must be installed using the same path on both the cluster nodes.
- The MySQL user on both the nodes must have the same user ID and group ID.
- Native ext3, ext4 file systems, and Logical Volume Manager (LVM) must be used.
- Unified Manager must be connected to the storage system through Fibre Channel (FC) or iSCSI.

You must also ensure that the FC link is active and that the LUNs created on the storage systems are accessible to both the cluster nodes.

- The shared data disk must have enough space (minimum 80 GB) for the Unified Manager database, reports, certificates, and script plug-in folders.
- A minimum of two network interfaces must be set up on each system: one for node-to-node communication and the other for node-to-client communication.

The name of the network interface used for node-to-client communication must be the same on both the systems.

- A separate heartbeat link must be established between the cluster nodes; otherwise, the network interface is used to communicate between the cluster nodes.
- Optional: SnapDrive for UNIX should be used to create a shared location that is accessible to both the nodes in a high availability setup.

See the *SnapDrive for UNIX Installation and Administration Guide* for information about installing and creating a shared location. You can also manage LUNs using SnapDrive or the storage system command-line interface. See the SnapDrive for UNIX compatibility matrix for more information.

- Additional RAM must be available for the SnapDrive and VCS applications.

Installing Unified Manager on VCS

For configuring high availability, you must install Unified Manager on both the cluster nodes of VCS.

Before you begin

- VCS must be installed and configured on both the nodes of the cluster.

See the instructions provided in the *Veritas Cluster Server 6.2.1 Installation Guide* for more information about installing VCS.

- You must have clear root privileges to log in to the Unified Manager server console.

About this task

You must configure both the instances of Unified Manager to use the same database and to monitor the same set of nodes.

Steps

1. Log in to the first node of the cluster.
2. Install Unified Manager on the first node.

[Installing Unified Manager on Red Hat Enterprise Linux or CentOS](#)

3. Repeat Steps 1 and 2 on the second node of the cluster.
4. On the second instance of Unified Manager, log in as the root user to the Red Hat Enterprise Linux or CentOS server and enter the same `umadmin` password as you defined on the first instance of Unified Manager.
`passwd umadmin`

Configuring Unified Manager with VCS using configuration scripts

You can configure Unified Manager with Veritas Cluster Server (VCS) using configuration scripts.

Before you begin

- Unified Manager must be installed on both the nodes in the VCS setup.
- The XML::LibXML module must be bundled with Perl for VCS scripts to work.
- You must have created a shared LUN with sufficient size to accommodate the source Unified Manager data.
- You must have specified the absolute mount path for the script to work.

The script will not work if you create a folder inside the mount path.

- You must have downloaded the `ha_setup.pl` script at `/opt/netapp/ocum/scripts`.

About this task

In the VCS setup, the node for which the virtual IP interface and mount point are active is the first node. The other node is the second node.

Steps

1. Log in to the first node of the cluster.

You must have stopped all the Unified Manager services on the second node in the high availability setup.


2. Add the VCS installation directory `/opt/VRTSvcs/bin` to the `PATH` environmental variable.
3. If you are configuring an existing Unified Manager setup, create a Unified Manager backup and generate the support bundle.
4. Run the `ha_setup.pl` script: `perl ha_setup.pl --first -t vcs -g group_name -e eth_name -i cluster_ip -m net_mask -n fully_qualified_cluster_name -f mount_path -v volume_group -d disk_group -l install_dir -u user_name -p password`

```
perl \ha_setup.pl --first -t vcs -g umgroup -e eth0 -i 10.11.12.13 -m 255.255.255.0 -n cluster.eng.company.com -f /mnt/ocumdb -v ocumdb_SdHv -d ocumdb_SdDg -l /opt/netapp/ -u admin -p wx17yz
```

5. Use the Veritas Operation Manager web console or VCS Cluster Manager to verify that a failover group is created, and that the Unified Manager server services, mount point, virtual IP, network interface card (NIC), and volume group are added to the cluster group.
6. Manually move the Unified Manager service group to the secondary node and verify that cluster failover is working.
7. Verify that VCS has switched over to the second node of the cluster.

You must verify that the data mount, virtual IP, volume group, and NIC are online on the second node of the cluster.

8. Stop Unified Manager using Veritas Operation Manager.
9. Run the `perl ha_setup.pl --join -t vcs -f``mount_path` command on the second node of the cluster so that the Unified Manager server data points to the LUN.
10. Verify that the Unified Manager server services are starting properly on the second node of the cluster.
11. Regenerate the Unified Manager certificate after running the configuration scripts to obtain the global IP address.

- a. In the toolbar, click , and then click **HTTPS Certificate** from the **Setup** menu.
- b. Click **Regenerate HTTPS Certificate**.

The regenerated certificate provides only the cluster IP address, not the fully qualified domain name (FQDN). You must use the global IP address to set up Unified Manager for high-availability.

12. Access the Unified Manager UI using the following: `https://<FQDN of Global IP>`

After you finish

You must create a shared backup location after high availability is configured. The shared location is required for containing the backups that you create before and after failover. Both the nodes in the high-availability setup must be able to access the shared location.

Unified Manager service resources for VCS configuration

You must add the cluster service resources of Unified Manager to Veritas Cluster Server (VCS). These cluster service resources are used for various purposes, such as monitoring storage systems, scheduling jobs, processing events, and monitoring all the other Unified Manager services.

The following table lists the category of all the Unified Manager services:

Category	Services
Storage resource	<ul style="list-style-type: none">• vol• mount
Database resource	<ul style="list-style-type: none">• mysqld
Network resource	<ul style="list-style-type: none">• nic• vip
Unified Manager resource	<ul style="list-style-type: none">• ocie• ocieau

Updating an existing Unified Manager setup for high availability

You can update your existing Unified Manager installation and configure your setup environment for high availability.

Before you begin

- You must have created a backup and support bundle of your existing data.
- You must have the OnCommand Administrator or Storage Administrator role.
- You must have added a second node to your cluster and installed Veritas Cluster Server (VCS) on the second node.

See the *Veritas Cluster Server 6.2.1 Installation Guide*.

- The newly added node must be configured to access the same shared location as that of the existing node in the high-availability setup.

Steps

1. Log in to the new node of the cluster.
2. Install Unified Manager on the node.

[Installing Unified Manager on Red Hat Enterprise Linux or CentOS](#)

3. Configure the Unified Manager server using configuration scripts on the existing node with data.
4. Initiate manual fail over to the second node.
5. Run the `perl ha_setup.pl --join -t vcs -f ``mount_path` command on the second node of the cluster so that the Unified Manager server data points to the shared LUN.
6. If OnCommand Workflow Automation (WFA) is configured for Unified Manager, disable and then reconfigure the WFA connection.
7. If SnapProtect is configured with Unified Manager, reconfigure SnapProtect with a new cluster IP address and the existing storage policies.
8. Regenerate the custom reports and add these reports to Unified Manager with the new cluster IP address.

Copyright information

Copyright © 2024 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.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, 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) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.