



Configuring backup and restore operations

Active IQ Unified Manager 9.7

NetApp
October 22, 2024

This PDF was generated from <https://docs.netapp.com/us-en/active-iq-unified-manager-97/health-checker/concept-backup-and-restore-using-a-mysql-database-dump.html> on October 22, 2024. Always check docs.netapp.com for the latest.

Table of Contents

- Configuring backup and restore operations 1
 - What a database backup is 1
 - Configuring database backup settings 2
 - What a database restore is 2
- Virtual appliance backup and restore process overview 3
- Restoring a database backup on a virtual machine 3
- Restoring a database backup on a Linux system 4
- Restoring a database backup on Windows 6
- Migrating a Unified Manager virtual appliance to a Linux system 7

Configuring backup and restore operations

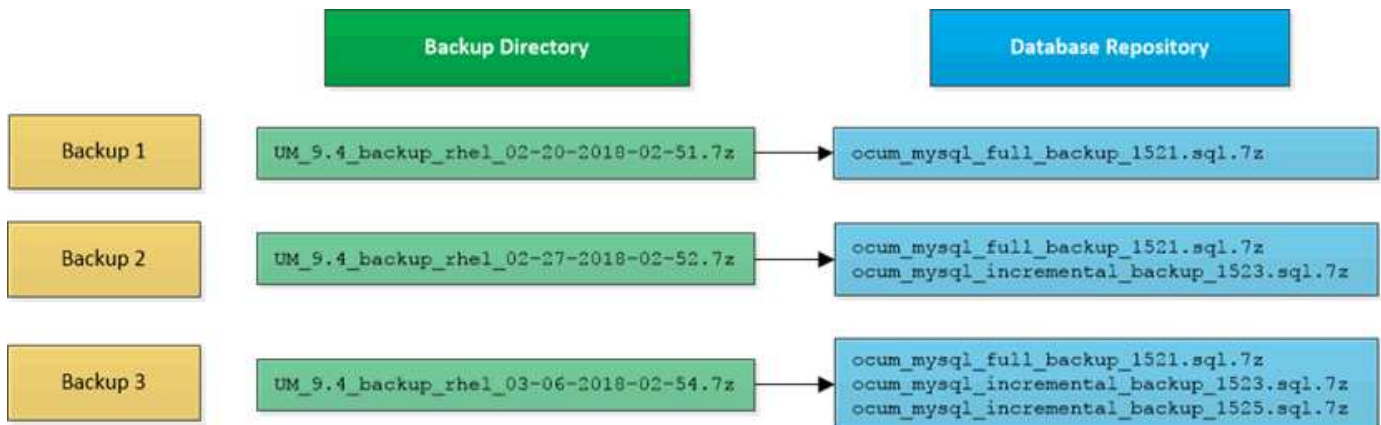
You can create backups of Unified Manager and use the restore feature to restore the backup to the same (local) system or a new (remote) system in case of a system failure or data loss.

What a database backup is

A backup is a copy of the Unified Manager database and configuration files that you can use in case of a system failure or data loss. You can schedule a backup to be written to a local destination or to a remote destination. It is highly recommended that you define a remote location that is external to the Unified Manager host system.

A backup consists of a single file in the backup directory and one or more files in the database repository directory. The file in the backup directory is very small because it contains only a pointer to the files located in the database repository directory that are required to recreate the backup.

The first time you generate a backup a single file is created in the backup directory and a full backup file is created in the database repository directory. The next time you generate a backup a single file is created in the backup directory and an incremental backup file is created in the database repository directory that contains the differences from the full backup file. This process continues as you create additional backups, up to the maximum retention setting, as shown in the following figure.



Do not rename or remove any of the backup files in these two directories or any subsequent restore operation will fail.

If you write your backup files to the local system, you should initiate a process to copy the backup files to a remote location so they will be available in case you have a system issue that requires a complete restore.

Before beginning a backup operation, Unified Manager performs an integrity check to verify that all the required backup files and backup directories exist and are writable. It also checks that there is enough space on the system to create the backup file.

Note that you can restore a backup only on the same version of Unified Manager. For example, if you created a backup on Unified Manager 9.4, the backup can be restored only on Unified Manager 9.4 systems.

Configuring database backup settings

You can configure the Unified Manager database backup settings to set the database backup path, retention count, and backup schedules. You can enable daily or weekly scheduled backups. By default, scheduled backups are disabled.

Before you begin

- You must have the Operator, Application Administrator, or Storage Administrator role.
- You must have a minimum of 150 GB of space available in the location you define as the backup path.

It is recommended that you use a remote location that is external to the Unified Manager host system.

- When Unified Manager is installed on a Linux system, verify that the “jboss” user has write permissions to the backup directory.
- You should not schedule backup operations to occur immediately after a new cluster has been added while Unified Manager is collecting 15 days of historical performance data.

About this task

More time is required the first time a backup is performed than for subsequent backups because the first backup is a full backup. A full backup can be over 1 GB and can take three to four hours. Subsequent backups are incremental and require less time.

Steps

1. In the left navigation pane, click **General > Database Backup**.
2. In the **Database Backup** page, click **Backup Settings**.
3. Configure the appropriate values for a backup path, retention count, and schedule.

The default value for retention count is 10; you can use 0 for creating unlimited backups.

4. Select the **Scheduled Daily** or **Scheduled Weekly** button, and then specify the schedule details.
5. Click **Apply**.

What a database restore is

Database restore is the process of restoring an existing Unified Manager backup file to the same or a different Unified Manager server. You perform the restore operation from the Unified Manager console.

If you are performing a restore operation on the same (local) system, and the backup files are all stored locally, you can run the restore command using the default location. If you are performing a restore operation on a different Unified Manager system (a remote system), you must copy the backup file, or files, from secondary storage to the local disk before running the restore command.

During the restore process, you are logged out of Unified Manager. You can log in to the system after the restore process is complete.

The restore feature is version-specific and platform-specific. You can restore a Unified Manager backup only on the same version of Unified Manager. Unified Manager supports backup and restore in the following platform scenarios:

- Virtual appliance to virtual appliance
- Virtual appliance to Red Hat Enterprise Linux or CentOS
- Red Hat Enterprise Linux to Red Hat Enterprise Linux or CentOS
- Windows to Windows

If you are restoring the backup image to a new server, after the restore operation completes you need to generate a new HTTPS security certificate and restart the Unified Manager server. You will also need to reconfigure SAML authentication settings, if they are required, when restoring the backup image to a new server.



Old backup files cannot be used to restore an image after Unified Manager has been upgraded to a newer version of software. To save space, all old backup files, except the newest file, are removed automatically when you upgrade Unified Manager.

Virtual appliance backup and restore process overview

The backup and restore model for Unified Manager when installed on a virtual appliance is to capture and restore an image of the full virtual application.

Because the Unified Manager backup operation on the virtual appliance does not provide a way to move the backup file from the vApp, the following tasks enable you to complete a backup of the virtual appliance:

1. Power off the VM and take a VMware snapshot of the Unified Manager virtual appliance.
2. Make a NetApp Snapshot copy on the datastore to capture the VMware snapshot.

If the datastore is not hosted on a system running ONTAP software, follow the storage vendor guidelines to create a backup of the VMware snapshot.

3. Replicate the NetApp Snapshot copy, or snapshot equivalent, to alternate storage.
4. Delete the VMware snapshot.

You should implement a backup schedule using these tasks to ensure that the Unified Manager virtual appliance is protected if issues arise.

To restore the VM, you can use the VMware snapshot you created to restore the VM to the backup point-in-time state.

Restoring a database backup on a virtual machine

In case of data loss or data corruption, you can use the restore feature to restore Unified Manager to the previous stable state with minimal loss. You can restore the Unified Manager database on a virtual machine by using the Unified Manager maintenance console.

Before you begin

- You must have the maintenance user credentials.
- The Unified Manager backup files must be on the local system.
- The backup files must be of .7z type.

About this task

Backup compatibility is platform and version dependent. You can restore a backup from a virtual appliance to another virtual appliance, or from a virtual appliance to a Red Hat Enterprise Linux or CentOS system.



When performing a restore operation on a different virtual appliance than the system from which the original backup file was created, the maintenance user name and password on the new vApp must be the same as the credentials from the original vApp.

Steps

1. In the vSphere client, locate the Unified Manager virtual machine, and then select the **Console** tab.
2. Click in the console window, and then log in to the maintenance console using your user name and password.
3. In the **Main Menu**, enter the number for the **System Configuration** option.
4. In the **System Configuration Menu**, enter the number for the **Restore from a Unified Manager Backup** option.
5. When prompted, enter the absolute path of the backup file.

```
Bundle to restore from: opt/netapp/data/ocum-  
backup/UM_9.4.N151112.0947_backup_unix_02-25-2018-11-41.7z
```

After the restore operation is complete, you can log in to Unified Manager.

After you finish

After you restore the backup, if the OnCommand Workflow Automation server does not work, perform the following steps:

1. On the Workflow Automation server, change the IP address of the Unified Manager server to point to the latest machine.
2. On the Unified Manager server, reset the database password if the acquisition fails in step 1.

Restoring a database backup on a Linux system

If data loss or data corruption occurs, you can restore Unified Manager to the previous stable state with minimum loss of data. You can restore the Unified Manager database to a local or remote Red Hat Enterprise Linux or CentOS system by using the Unified Manager maintenance console.

Before you begin

- You must have Unified Manager installed on a server.
- You must have the root user credentials for the Linux host on which Unified Manager is installed.
- You must have copied the Unified Manager backup file and the contents of the database repository directory to the system on which you will perform the restore operation.

It is recommended that you copy the backup file to the default directory `/data/ocum-backup`. The database repository files must be copied to the `/database-dumps-repo` subdirectory under the `/ocum-backup` directory.

- The backup files must be of `.7z` type.

About this task

The restore feature is platform-specific and version-specific. You can restore a Unified Manager backup only on the same version of Unified Manager. You can restore a Linux backup file or a virtual appliance backup file to a Red Hat Enterprise Linux or CentOS system.



If the backup folder name contains a space, you must include the absolute path or relative path in double quotation marks.

Steps

1. If you are performing a restore onto a new server, after installing Unified Manager do not launch the UI or configure any clusters, users, or authentication settings when the installation is complete. The backup file populates this information during the restore process.
2. Using Secure Shell, connect to the IP address or fully qualified domain name of the Unified Manager system.
3. Log in to the system with the maintenance user (`umadmin`) name and password.
4. Enter the command `maintenance_console` and press Enter.
5. In the maintenance console **Main Menu**, enter the number for the **System Configuration** option.
6. In the **System Configuration Menu**, enter the number for the **Restore from a Unified Manager Backup** option.
7. When prompted, enter the absolute path of the backup file.

```
Bundle to restore from: /data/ocum-  
backup/UM_9.4.N151113.1348_backup_rhel_02-20-2018-04-45.7z
```

After the restore operation is complete, you can log in to Unified Manager.

After you finish

After you restore the backup, if the OnCommand Workflow Automation server does not work, perform the following steps:

1. On the Workflow Automation server, change the IP address of the Unified Manager server to point to the latest machine.
2. On the Unified Manager server, reset the database password if the acquisition fails in step 1.

Restoring a database backup on Windows

In case of data loss or data corruption, you can use the restore feature to restore Unified Manager to the previous stable state with minimal loss. You can restore the Unified Manager database to a local Windows system or a remote Windows system by using the Unified Manager maintenance console.

Before you begin

- You must have Unified Manager installed on a server.
- You must have Windows administrator privileges.
- You must have copied the Unified Manager backup file and the contents of the database repository directory to the system on which you will perform the restore operation.

It is recommended that you copy the backup file to the default directory `\ProgramData\NetApp\OnCommandAppData\ocum\backup`. The database repository files must be copied to the `\database_dumps_repo` subdirectory under the `\backup` directory.

- The backup files must be of `.7z` type.

About this task

The restore feature is platform-specific and version-specific. You can restore a Unified Manager backup only on the same version of Unified Manager, and a Windows backup can be restored only on a Windows platform.



If the folder names contain a space, you must include the absolute path or relative path of the backup file in double quotation marks.

Steps

1. If you are performing a restore onto a new server, after installing Unified Manager do not launch the UI or configure any clusters, users, or authentication settings when the installation is complete. The backup file populates this information during the restore process.
2. Log in to the Unified Manager system with administrator credentials.
3. Launch PowerShell as a Windows administrator.
4. Enter the command `maintenance_console` and press Enter.
5. In the **Main Menu**, enter the number for the **System Configuration** option.
6. In the **System Configuration Menu**, enter the number for the **Restore from a Unified Manager Backup** option.
7. When prompted, enter the absolute path of the backup file.


```
Bundle to restore from:
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.4.N151118.2300_bac
kup_windows_02-20-2018-02-51.7z
```

After the restore operation is complete, you can log in to Unified Manager.

After you finish

After you restore the backup, if the OnCommand Workflow Automation server does not work, perform the following steps:

1. On the Workflow Automation server, change the IP address of the Unified Manager server to point to the latest machine.
2. On the Unified Manager server, reset the database password if the acquisition fails in step 1.

Migrating a Unified Manager virtual appliance to a Linux system

You can restore a Unified Manager database backup from a virtual appliance to a Red Hat Enterprise Linux or CentOS Linux system if you want to change the host operating system on which Unified Manager is running.


Before you begin

- On the virtual appliance:
 - You must have the Operator, Administrator, or Storage Administrator role to create the backup.
 - You must know the name of the Unified Manager maintenance user for the restore operation.
- On the Linux system:
 - You must have installed Unified Manager on a RHEL or CentOS server following the instructions in the Installation Guide.
 - The version of Unified Manager on this server must be the same as the version on the virtual appliance from which you are using the backup file.
 - Do not launch the UI or configure any clusters, users, or authentication settings on the Linux system after installation. The backup file populates this information during the restore process.
 - You must have the root user credentials for the Linux host.

About this task

These steps describe how to create a backup file on the virtual appliance, copy the backup files to the Red Hat Enterprise Linux or CentOS system, and then restore the database backup to the new system.

Steps

1. On the virtual appliance, in the toolbar click , and then click **Management > Database Backup**.
2. In the **Database Backup** page, click **Actions > Database Backup Settings**.

3. Change the backup path to `/jail/support`.
4. In the **Schedule Frequency** section, select the **Enable** checkbox, select **Daily**, and enter a time a few minutes past the current time so that the backup is created shortly.
5. Click **Save and Close**.
6. Wait a few hours for the backup to be generated.

A full backup can be over 1 GB and can take three to four hours to complete.

7. Log in as the root user to the Linux host on which Unified Manager is installed and copy the backup files from `/support` on the virtual appliance using SCP.
`root@<rhel_server>:/# scp -r admin@<vapp_server_ip_address>:/support/* .`

```
root@ocum_rhel-21:/# scp -r admin@10.10.10.10:/support/* .
```

Make sure you have copied the `.7z` backup file and all the `.7z` repository files in the `/database-dumps-repo` subdirectory.

8. At the command prompt, restore the backup: `um backup restore -f /<backup_file_path>/<backup_file_name>`

```
um backup restore -f /UM_9.4.N151113.1348_backup_unix_02-12-2018-04-16.7z
```

9. After the restore operation completes, log in to the Unified Manager web UI.

After you finish

You should perform the following tasks:

- Generate a new HTTPS security certificate and restart the Unified Manager server.
- Change the backup path to the default setting for your Linux system (`/data/ocum-backup`), or to a new path of your choice, because there is no `/jail/support` path on the Linux system.
- Reconfigure both sides of your Workflow Automation connection, if WFA is being used.
- Reconfigure SAML authentication settings, if you are using SAML.

After you have verified that everything is running as expected on your Linux system, you can shut down and remove the Unified Manager virtual appliance.

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.