Technical Note

Dell EMC NetWorker

Version 9.2

Differences between NetWorker 9.2 and previous releases

302-003-795
REV 01
July 28, 2017

This document identifies the most significant enhancements to the NetWorker software since the NetWorker 8.2.x release, including changes implemented in the NetWorker 9.0.x, 9.1.x, and 9.2 releases. Where the version is identified for when a new feature or enhancement was introduced, the change is considered applicable to that specific release and all subsequent releases. The NetWorker core documentation set provides more information on these changes.

Table 1 Revision history

Revision	Date	Description
01	July 28, 2017	First release of this document for NetWorker 9.2.

DELL EMC

NetWorker installation changes

NetWorker 9.2 features separate packages for installation. When you install NetWorker, you can choose to install the full package, Base Client package, or Extended Client package, depending on which software and features you plan to use.

The core NetWorker software consists of the following packages:

- The NetWorker full installation package (for example, `NetWorker-9.2.0.1.exe` on Windows) installs the client, server, and NMC software. You have the option to install only the client from this installer, but it is recommended that you use `lgtoclnt-9.2.0.1.exe` when you only need to install the base client. NetWorker no longer uses the InstallSheild `setup.exe` file.
- The Base Client package (for example, `lgtoclnt-9.2.0.1.exe`) provides you with the ability to perform file system backup and recovery operations. These must be installed on each NetWorker client, except for NDMP Clients.
- The Extended Client package (for example, `lgtoxtdclnt-9.2.0.1.exe`) provides additional feature support for NetWorker clients, such as snapshot backup support, command line utility support including server reporting and administration, cloning and staging support, and so on. This package is also required if using the NMDA, NMMedi or SCVMM modules. When you install the NetWorker server or storage node software on Windows, the installation process automatically installs the Extended Client package. You should install the Extended Client package when upgrading a NetWorker client to ensure that functionality that was available with the previously installed NetWorker version is available.

The following sections provide more information about other installation changes.

NetWorker Authentication Service installation

NetWorker uses the NetWorker Authentication Service to authenticate NMC and command prompt users.

The *NetWorker Security Configuration Guide* and *NetWorker Installation Guide* provide more information.

The NetWorker server installation process automatically installs the NetWorker Authentication Service software on the NetWorker host.

The NetWorker Authentication Service requires a minimum Java version of 64-bit Java 8 update 60. If the installation process does not detect a minimum of this version on the host, the installation process will not continue. It is recommended that you use the latest version of Java 8 on the host.

EMC License Server installation

After you complete the NetWorker install, you must install the EMC License Server package whether you plan to continue using the traditional enabler-based method of licensing or want to use the new EMC Licensing Solution with capacity entitlement. You can download install packages for the License Server in the same location as the NetWorker software. Separate packages are available for Windows and Linux.

The *NetWorker Licensing Guide* provides more information about the new licensing model.

Supported Java versions

Java is not included with the NetWorker install. When installing the Console server software, you must install the minimum required Java version. You cannot start NMC until the appropriate JRE version is installed.

The minimum required version for NetWorker 9.2 is 64-bit Java 8 update 60.

On Windows, the NetWorker server installation processes performs a check to ensure that the minimum required Java version is installed on the host. If you complete the installation without the minimum required Java version installed, NetWorker daemons will not start correctly.

It is recommended that you install the latest version of the 64-bit Java 8 software on the NetWorker server host before you install the NetWorker server or NetWorker Authentication Service software. Ensure that you stop NMC and the NetWorker server daemons prior to updating Java.

Changes to platforms supported

NetWorker features the following platform changes:

- NetWorker no longer supports the Linux ia64 platform.
- The NMC server software package can only be installed on a Linux or Microsoft Windows 64-bit host. The NMC server software requires the NetWorker client software.

EMC Licensing Solution

NetWorker 9.0 and later releases feature the EMC Licensing Solution with capacity entitlement, which uses a License Server and a license file.

NetWorker 8.2.x and earlier
The traditional licensing model and the capacity licensing model are both available to permanently license the NetWorker software, but only one method can be used per NetWorker server or datazone.

With traditional licensing, you can use features of products once you purchased a base enabler.

With capacity licensing, you can deploy unlimited quantities of the NetWorker options and modules to protect, up to the amount of licensed capacity you purchased.

NetWorker 9.0 and later
The EMC Licensing Solution introduced in NetWorker 9.0 stores the licenses for all installed products in one file. This file must reside on a platform that is accessible to NetWorker and runs the EMC License Server. The License Server must be installed along with the NetWorker software installation.

The license file can contain one of two types of licenses — a single capacity license, which enables all data zones in an installation, and an update license, if updating from a previous NetWorker release.

For new installations of NetWorker 9.1, you can only use the EMC Licensing Solution with capacity entitlement. When you upgrade from a NetWorker 8.2.x or earlier release, you can continue to use the traditional or legacy capacity model, or use the EMC Licensing Solution with capacity entitlement. If you previously used the capacity model, any unused storage is added to the capacity purchased for use of the EMC Licensing Solution.

Licensing solution requirements for new and upgraded installations

New and upgraded installations of NetWorker 9.2 must fulfill the following requirements to use the EMC Licensing Solution.

New installation of NetWorker 9.2

All new NetWorker 9.2 installations use the EMC Licensing Solution with capacity entitlement, which requires the following setup:

1. Install the EMC License Server.
2. Obtain the license file, which contains the capacity entitlement called NETWORKER_CAPACITY.
3. Set up the license file on the License Server host:
   - On Linux, copy the file to the `/opt/emc/licenses/` directory.
   - On Windows, copy the file to the `C:\Program Files\EMC License Server\elms\licenses` folder.
4. On the NetWorker server, launch the NMC **Administration** window, and then right-click the server and select **Properties** from the drop down. In the **Licensing** tab of the **Server Properties** window, browse to and select the license file to populate the **CLP license text** field.

Upgrading to NetWorker 9.2

When you upgrade to NetWorker 9.2 from a NetWorker 8.2.x release, you have the following two options:

- Use the EMC Licensing Solution with the capacity entitlement.
- Continue to use the traditional enabler-based licensing model from the previous NetWorker version.

If you decide to use the EMC Licensing Solution with the capacity entitlement after you upgrade to NetWorker 9.2, you must take the following actions:

1. Install the EMC License Server. Without a connection to the EMC License Server, NetWorker 9.2 runs in evaluation mode for 90 days. Install the License Server before the end of the evaluation period.
2. Obtain the license file, which contains a capacity entitlement that is called NETWORKER_CAPACITY or an update entitlement called NETWORKER_UPDATE.
3. Set up the license file on the License Server host:
   - On Linux, copy the file to the`/opt/emc/licenses/` directory.
   - On Windows, copy the file to the `C:\Program Files\EMC License Server\elms\licenses` folder.
4. On the NetWorker server, launch the NMC **Administration** window, and then right-click the server and select **Properties** from the list. In the **Licensing** tab of the **Server Properties** window, browse to and select the license file to populate the **CLP license text** field.

Note

When you choose the capacity entitlement option, contact a Dell EMC sales representative to perform the conversion from the traditional enabler-based licensing model to the EMC Licensing Solution with the capacity entitlement.

If you decide to continue using the traditional enabler-based licensing model, you must take the following actions before upgrading to NetWorker 9.2:

1. Install the EMC License Server. Without a connection to the EMC License Server, NetWorker 9.2 runs in evaluation mode for 90 days. Install the License Server before the end of the evaluation period.
2. Obtain the license file, which should contain only an update entitlement called NETWORKER_UPDATE.

   Note

   When you apply an update entitlement, a notification that indicates that `NETWORKER_CAPACITY entitlement is not present in the license file` might display. If you are not using the NETWORKER_CAPACITY entitlement, you can ignore this message.
3. Set up the license file on the License Server host:
   - On Linux, copy the file to the `/opt/emc/licenses/` directory.
   - On Windows, copy the file to the `C:\Program Files\EMC License Server\elms\licenses` folder.
4. On the NetWorker server, launch the NMC **Administration** window, and then right-click the server and then select **Properties** from the list. In the **Licensing** tab of the **Server Properties** window, browse to and select the license file to populate the **CLP license text** field.

Quick Start: Activate the EMC Licensing Solution

The following section provides an overview of the steps that are required to activate the EMC Licensing Solution in a new installation of NetWorker. For more details, see subsequent sections of the *NetWorker Licensing Guide* and the *License Server Installation and Administration Guide*.

Before you begin

Obtain the license file from EMC Licensing. For a new installation of NetWorker, this file contains a capacity entitlement. You can obtain the file after you provide EMC Licensing with the License Server host/IP information and the required capacity. If you cannot use the default 27000 port for communication between NetWorker and the License Server, you must also provide the port number. EMC Licensing requires this information to create the license file.

Procedure

1. Download the License Server package for the appropriate platform from the same location that you downloaded the NetWorker software from.
2. Install the Windows or Linux 64-bit License Server package. You can install the License Server in the same location as the NetWorker Server. The following table provides the package name for each OS version.

OS	Package name
Windows	`EMC_LicenseServer_3.4.0_x64 installer.msi`
RHEL 5 and SuSE 11	`emclicenseserver-3.4.1-2.x86_64_lsb.rpm`
RHEL 6, 7 and SuSE 12	`emclicenseserver-3.5.0-1.x86_64_lsb.rpm`

3. In the location that you installed the License Server, copy the license file to the following directory:

   Note

   Do not rename the license file.

   - On Windows: `C:\Program Files\EMC License Server\elms\licenses`
   - On Linux: `/opt/emc/licenses`

   Note

   On Linux, you might be required to complete this step before you install the License Server package.

4. Complete the License Server configuration, and then start the License Server:
   - On Windows, use **LMTOOLS** or the command-line interface.
     An icon for **LMTOOLS** appears on the desktop after the License Server installation.
   - On Linux, use the `lmgrd` command-line utility.

5. On the NetWorker server, launch the NMC **Administration** window, right-click the server, and then select **Properties** from the list. The **Server Properties** window appears.
   a. Select the **Licensing** tab.
   b. In the **CLP license text** field, click **Browse**.
   c. Navigate to the location of the file, and select the license file.
   d. Click **Validate license**. The **Validate license** button will be disabled until the contents are validated. You can check the status by using the `nsrlic -C` command.
6. In the **Server Properties** window, on the **Licensing** tab, ensure that the following fields have the correct values, and then click **OK**.
   - CLP license server
   - CLP License Server Port
   - Solution ID
   - CLP SWID

   Note

   CLP refers to the EMC License Server.

7. In the NMC **Administration** window, click **Server**, and then select **Registrations**. Confirm that the right pane displays an entry for CLP Capacity License that indicates the **Authorized -No expiration date**.

NetWorker Authentication Service

NetWorker introduces a new authentication and authorization model, the Authentication Service, which is designed to improve NetWorker security by using token-based authentication and single sign on (SSO) support.

Token-based authentication enables users to securely connect to the NMC server, the NetWorker server, and to perform secure backup and recover operations.

NetWorker 8.2 and earlier

In versions of NetWorker up to NetWorker 8.2.x, user authentication is handled in one of two ways:

- By specifying privileges through NSR usergroup resources, or by using the NSR resource Administrators list, for operating system usernames, <user>@<host>, groups, and so on. Also, NMC maintained its own list of users and those users would be granted privileges by specifying "<user>@<NMC Server>."
- By using an external authority (LDAP or AD) to authenticate users. You configured the NetWorker and NMC servers to access the LDAP or AD server directly, and authenticate users against the server. LDAP or AD groups were specified in the **External Roles** field of NSR usergroup resources.

NetWorker 9.0 and later

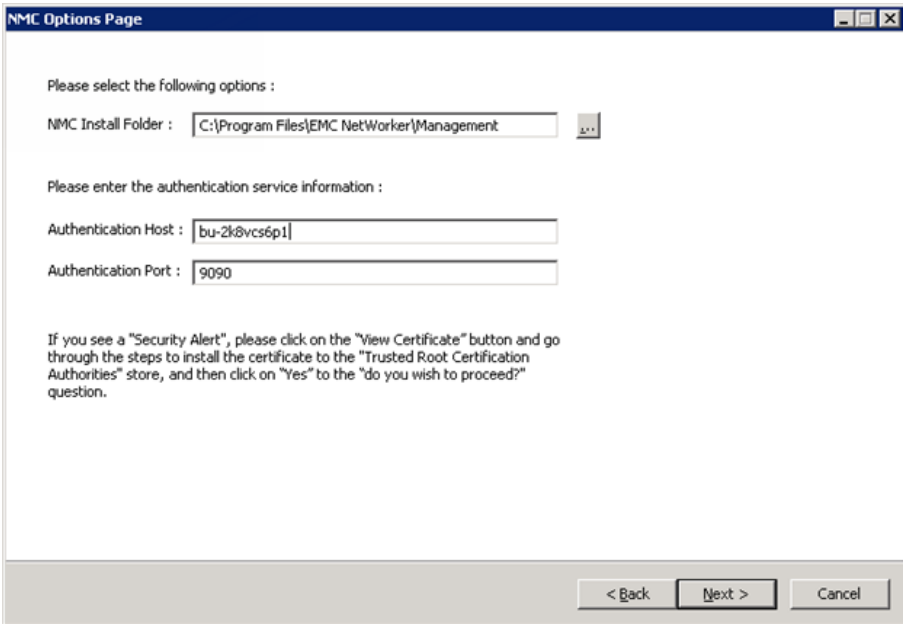
In NetWorker 9.0 and later, installation and configuration of an authentication server allows you to authenticate all users for NMC and the command line interface. The authentication server maintains its own local database of users and groups independent from the operating system users and groups. The authentication server gets installed with the NetWorker server software.

A wizard guides you through authentication server setup. During the installation, the **Configure the NetWorker Authentication Service** page may appear under certain conditions, along with a new Java truststor password requirement. The *NetWorker Updating from a Previous Release Guide* provides more information.

After the **Configure NetWorker Authentication Service Keystore** and **NetWorker Authentication Service - Service Options** pages, the **NMC Options Page** window appears, where you type the name of the authentication host (the local hostname), and the authentication port that you selected during the authentication server install.

The following figure shows the **NMC Options Page** window.

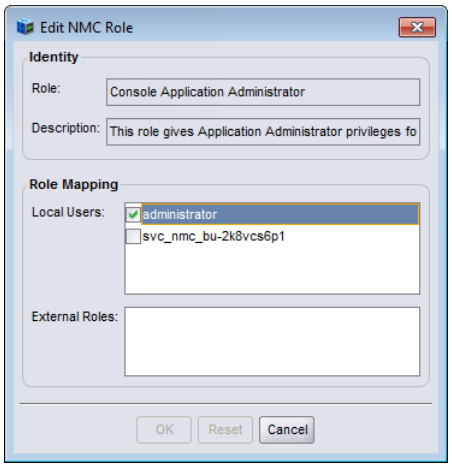
Figure 1 NMC Options



To complete the wizard, fill out the **NMC Database Options** page and the **NMC migration** page, and then click **Install** to display the **Complete the Setup** page. After completing the wizard, you can launch NMC.

Upon launching NMC and completing the **Console Configuration** wizard, you can create additional users and groups in the authentication server local database by using the **Edit Roles** dialog box, as shown in the following figure.

Figure 2 Edit Roles dialog box



Note

You can still configure NetWorker to authenticate based on an operating system user.

The *NetWorker Security Configuration Guide* provides complete details for installing and configuring the NetWorker Authentication Service.

Changes to resources between NetWorker releases

Due to changes introduced in NetWorker 9.0 and NetWorker 9.1, there are differences in functionality and the location of certain resources between NetWorker 9.0 and previous releases.

The following table provides information about functionality in the NetWorker Management Console's **Administration** window and command line programs that has changed, been removed, or been replaced since NetWorker 9.0.

Table 2 Changes to properties since NetWorker 9.0

Category	Previous to NetWorker 9.0	NetWorker 9.0 and later
Group	Group: A logical group of clients which you can run to perform backup, clone, snapshot, bootstrap, and index backups. VMware backups are not supported.	Protection Group: Logical group of clients/virtual machines/NAS devices/Save sets/Dynamic Save-set Query/Dynamic client. You can associate to a workflow.
Group	You can run a group, which consists of backup properties (and clients) used to start or manage backups.	You cannot run a group. A group can be a logical group of NetWorker clients, a query to produce save sets, or a query based on tags to produce clients. Group should be associated with workflow for protection.
Group > Probe	Used to configure Probe before backup.	Create Probe Action and Backup Action in a workflow. Probe resources are retained and must be associated to clients as-is. Probe properties moved to probe action definition.
Group > Clone	Configure clone after backup as Immediate clone and concurrent immediate clone. Not all save sets can be cloned as soon as the backup completes.	Chain a clone action to a backup action and set the clone action to run concurrently with the backup action.
Group > Bootstrap and index backups	Bootstrap and index backups are performed as the last steps for a Group run.	Server protection policy is created by default with Server database action and expiration action. Tune this policy to add Clone Action, turn off index backups, specify certain clients for index backups, and so on. Client's backup and server protection are independent of each other.

Table 2 Changes to properties since NetWorker 9.0 (continued)

Category	Previous to NetWorker 9.0	NetWorker 9.0 and later
Group > Snapshot backup	Take snapshot backups using snapshot policy.	Create a workflow with snapshot backup action. NSR Snapshot policy resource is deprecated.
Group > Schedule	Specify a schedule from existing schedule resources.	Schedule resource cannot be used in policy. Schedule activity is part of backup action definition.
Group > Backup levels	Specify level of a backup to be performed by this group.	Level should be specified as schedule activity in backup action definition.
Group > Browse policy	Determines how long files are maintained in the client's file index on the NetWorker server, after which the entry for that file is deleted.	No longer supported. Browse retention will be same as save set's retention.
Archiving	Performed from the **Administration** window.	Only available using the `nsrarchive` command.
Retention policy	Retention policy can be specified in various places such as Client resource, Group resource and Pool resource.	Defined in the Policy Action properties in the **Protection** window.
Group	Other properties in Group resource such as start time, interval, and so on.	Moved to workflow definition and backup action definition in the **Protection** window.
Client	Properties in **Configuration** window.	Properties in **Protection** window.
Client Push	Upgrade using the Software Distribution wizard in the **Configuration** window.	Upgrade using Package Manager in the **Hosts** window. Does not support NMM.
Clone	You can use a scheduled clone to query the save sets/ specify the save sets.	To achieve scheduled clone functionality, create a workflow with a clone action and associate a Group with save set query/save sets.
	Clone volumes in the **Media** window. You can also clone save sets by using the **Media** window.	Use `nsrclone` to clone volumes. Use a clone action in the policy workflow of the **Protection** window.
	You can use `nsrclone` command on the NetWorker client and server.	You can only use the `nsrclone` command on the NetWorker server.

Table 2 Changes to properties since NetWorker 9.0 (continued)

Category	Previous to NetWorker 9.0	NetWorker 9.0 and later
	FORCE_REQ_AFFINITY variable for clone operation to determine a read source storage node.	The *FORCE_REQ_AFFINITY* variable is removed.
Notification	Configured through Notification resource.	A property of policy, workflow, and action.
Schedules	Used in clients and groups.	Used in clients only. Policy cannot use schedule resource. Defined in the Policy Action wizard.
Time policy	Used in clients and groups.	Used in clients only. Cannot be used in policy.
VMware Protection Policies	Used to create VMware policies for backup, clone, checkpoint discovery, and checkpoint backup in **Configuration** window.	Create a workflow with VMware Backup action and Clone action in the **Protection** window. Associate with a virtual machine (virtual machine/ VMDK) protection group. You cannot perform backups to internal storage.
NAS Device	Used to create NAS Device resource to discover and index NAS snapshots.	Create NAS Device protection group. Create a workflow with discovery and index action.
Directives	Under **Configuration** window.	Under **Server** window.
Lockboxes	Under **Configuration** window.	Under **Server** window.
Notification	Under **Configuration** window.	Under **Server** window.
Registration	Under **Configuration** window.	Under **Server** window.
RDZ	Under **Configuration** window.	Under **Server** window.
Security Audit log	Under **Configuration** window.	Under **Server** window.
Time Policy	Under **Configuration** window.	Under **Server** window.
User Group	Under **Configuration** window.	Under **Server** window.

Table 2 Changes to properties since NetWorker 9.0 (continued)

Category	Previous to NetWorker 9.0	NetWorker 9.0 and later
Tools	Use `nsradmin` on all resources.	It is recommended that you use `nsrpolicy` for policy and group management.
Backup Levels	Use levels 1–9.	Can use level 1 only, levels 2–9 levels removed.
Media Pool	Save set, retention, client, level, and group can be set in Pool resource.	All 5 properties in Group resource removed.
Destination Pool	Client, Group.	Defined in the Policy Action wizard of the **Protection** window.
Backup commands	The `savegrp -g Default` command.	The `nsrpolicy start -p <policy name> -w 'FS'` or `nsrworkflow -p <policy name> -w 'FS'` commands.
Save sets	Client in **Configuration** window.	Under **Protection** window.
Cluster	NetWorker Server and Client.	NetWorker Client only.
`Nsrsgrpcomp`	Command line program that allows you to retrieve job information by querying information that is stored in the jobsdb and the `savegrp` log files.	This option is no longer available. Use `nsrpolicy` with the monitor option to retrieve job information and monitor policy activities.
`Savegrp`	Command line utility for performing backups, sending completion reports.	You can no longer run from the command line, only by using policy framework. The `nsrpolicy` command line utility replaces the `savegrp` command functionality. `Savegrp` no longer sends completion report, policy framework sends notification email messages.
Pre and post commands	`Savepnpc` used to execute pre and post commands.	Use NetWorker pre and post commands within the NetWorker client (NMC Client Properties Apps & Modules tab).

Configuring Force Backup Level

NetWorker 8.1.x and 8.2.x provided the **Force incremental** option in the Group resource. The option provided you with the ability to schedule multiple backups for clients in a 24 hours period, but limit the number of full backups to the first scheduled backup. Each subsequent backup in the 24 hour period is an incremental backup. NetWorker 9.2.x provides you with the ability to define a backup level for a backup action that differs from the scheduled level. NetWorker 9.2.x does not migrate the value in the **Force incremental** option to the action resource.

For workflows that have more than one scheduled backup within a 24-hour period, use the **Force Backup Level** attribute to allow more than one backup to occur at two different backup levels in a 24-hour period. When you select a backup level in the **Force Backup Level** attribute, the first backup is performed at the scheduled backup level. Each subsequent occurrence of the backup action in the next 24 hours occurs at the level defined in the **Force Backup Level** attribute. For example, if the level defined by the schedule is Full and the **Force Backup Level** attribute is set to Incr, the first backup started by the action occurs at a level full and subsequent backups, within 24 hours of the start of the full backup are incremental. By default this option is cleared, which means that if the action runs multiple backup operations in a 24 period, all the backups occur at the scheduled backup level.

To define a level for multiple backups that occur in a 24 hour period, perform the following steps:

Procedure

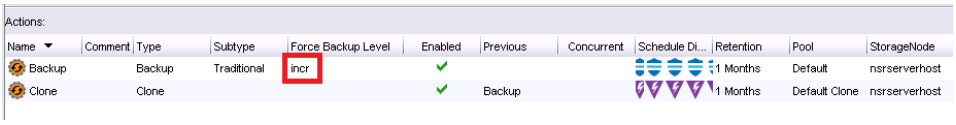
1. In the **Administration** window, click **Protection**.
2. In left pane, expand **Policies**.
3. Expand the policy and then select the workflow.
4. In the **Actions** pane, right click the action that is schedule to run multiple times in a 24 hour period, and then select **Properties**.

   The **Specify the Action Information** window in the **Policy Actions** wizard appears.
5. From the **Force Backup Level** list select a backup level.
6. Click **Next** on each subsequent window, and then click **Configure**.

Results

The level that you chose appears in the **Force Backup Level** column for the action, in the **Action** pane. The following figure provides an example of the Action pane, where the **Force Backup Level** attribute is set to Incr for the backup action.

Figure 3 Force Backup Level attribute



Customizing backups with the pre and post commands

Starting in NetWorker 9.0, the `savepnpc` command is no longer supported. However, you can customize backup behavior by running preprocessing and postprocessing

commands. These commands should only be run once during the client backup, instead of once for each save set.

Preprocessing and postprocessing scripts can be useful if the client is running a database or another program that should be stopped before the client is backed up, and then restarted after the backup has completed.

To set the preprocessing and postprocessing command attributes in the client resource and configure the scripts for use, perform the following in NMC's **Administration** window.

Procedure

1. In the **Administration** window, click **Protection**.
2. In the expanded left pane, select **Clients**.
3. Right-click the Client resource and select **Modify Client Properties**.

   The **Client Properties** dialog box appears.
4. On the **Apps and Modules** tab, in the **Pre command** attribute, specify the name of the script file that you require NetWorker to run before a backup.

   Note

   Do not specify the path to the file.
5. Optionally, in the **Post command** attribute, specify the name of the script file that you require NetWorker to run after a backup of all the save sets for the client completes.

   Note

   Do not specify the path to the file.
6. Click **OK**.

Results

The customized instructions are applied the next time that the client is backed up.

Jobs database changes

Improvements to the jobsdb were made in NetWorker 9.0 and later, and the format of the jobsdb changed. Also, the default retention period of jobsdb is now 72 hours. You can modify the retention period by editing the variable *Jobsdb retention in hours*.

Previous versions of the jobsdb (NetWorker 8.2.x and earlier) are not compatible with NetWorker 9.0 and later, and the update process does not migrate the jobsdb data. When you update from a NetWorker 8.2.x release to NetWorker 9.2, the updating process renames the jobsdb and the NetWorker server uses a new database.

Note

After you update the NetWorker server, all policy, workflow, and action resources will report a status of *never run*. This status also displays after a workflow has expired.

NMC database changes

In NetWorker 9.0 and later, NMC uses a PostgreSQL database instead of Sybase. As a result, you must migrate existing databases if performing an upgrade.

Migrating the database is a two-step process:

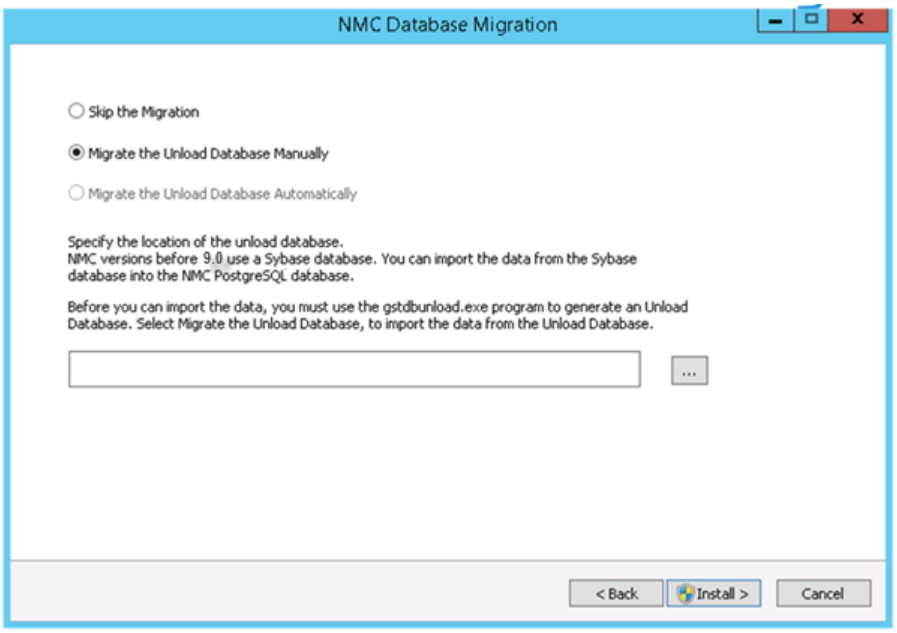
1. Unload the Sybase database before upgrading or uninstalling the previous version. You can unload the database manually by running the `gstdbunload` tool, or automatically.
2. Upgrade and then reload the SQL database to import the date from the Sybase database into the new PostreSQL database. You can perform this automatically, or you can manually reload the database by running the `gstdbupgrade` tool.

The upgrade on Linux platforms requires you to copy `gstdbunload` to the `/opt/lgtonmc/bin` directory before the upgrade, and then run `gstdbunload <path to unload directory>`. You can then install the NMC for NetWorker rpm.

When you update a Windows NMC server, it is recommended that you allow the migration process to handle the database migration. If your 8.2.x NMC server is on a Windows operating system that NetWorker 9.1.x does not support, you must use the `gstdbunload` utility included with the NetWorker 9.1.x software package to convert the NMC database into a platform independent format. After you convert the database, you must copy the converted files to the Windows or Linux host that will become the new NMC server.

The following figure shows the **NMC Database Migration** window.

Figure 4 NMC database migration on Windows platforms



NetWorker 9.0 and later drops NMC support for AIX and Solaris. If you upgrade from one of those platforms you must copy `gstdbunload` from the package to a location on the NetWorker 8.2.x server, run the command, generate the conversion files, and then copy the conversion files to the new NMC server.

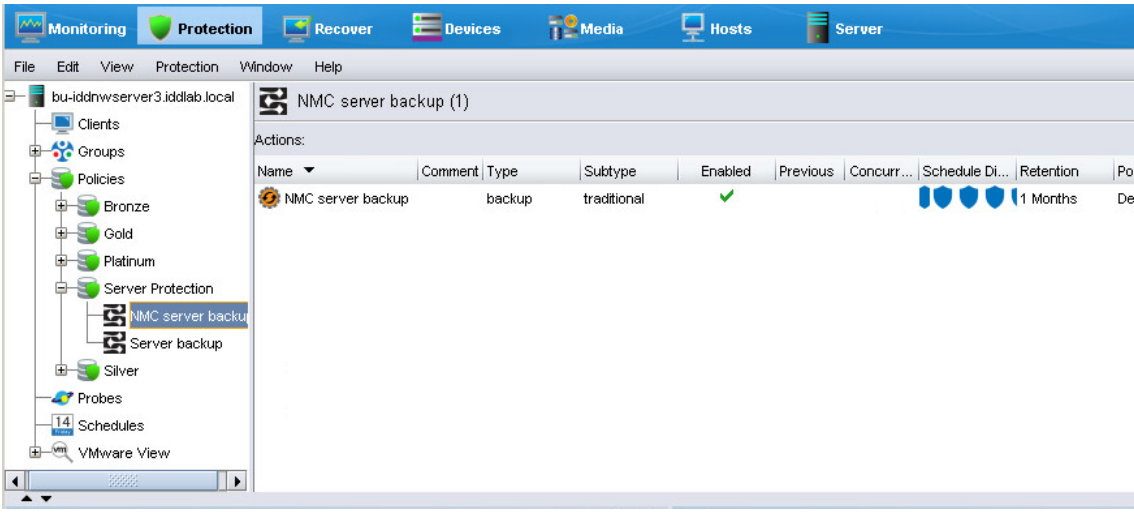
Database reloading typically takes less than 90 minutes but can take longer depending on several factors, including the number of NetWorker servers managed by NMC, and

the size of the database. After database reloading, a prompt appears to specify an account for the new database server.

The NMC database now gets replicated to a staging area and backed up as part of the default Server Protection policy in NMC.

The following figure shows the NMC database in the Server Protection Policy in NMC.

Figure 5 NMC database in Server Protection Policy



Media database changes

In NetWorker 9.0 and later, SQLlite replaces WiSS as the media database.

The new database features the following advantages:

- Object caching—A targeted cache facility that operates independently of file system or database caching to maintain recently used objects in memory for subsequent requests.
- Parallel request processing or multi-threading—The database in previous versions of NetWorker was single-threaded, which means it could handle only one database request at a time. As a result, long transactions could delay the performance of any other transactions, such as an operational request having to wait until the bootstrap was completed. With multi-threading, the database can handle requests in parallel, so that the operational request would be picked up and handled immediately without requiring completion of the bootstrap.
- Request handling—Any request that takes multiple seconds gets logged. You can choose to log all requests by setting `dbgcommand` to level 1 or higher in debug mode.
- Bootstrap compatibility—The mechanism being used for SQLlite is the same as for the WiSS database. If a problem occurs after upgrading, you can use a bootstrap taken from the previous system and recover that information directly into the SQL database. If you must temporarily downgrade NetWorker but already performed backups using NetWorker 9.0 and later that you want to maintain, you can perform a bootstrap and recover the media database into NetWorker 8.2, and that data will be recovered into the WiSS database.

The `nsrmmdbd` process handles the migration automatically during NetWorker startup after the upgrade. The database migration does not require any user intervention, and occurs in three stages: clients, volumes, and then save set records, with the daemon log indicating the beginning of each stage and logging any errors that occur. Once all

data has been moved to the new database, NetWorker performs a cross check to verify the success of the migration. The migration process typically takes between 1-3 minutes but can take longer for very large databases of 1 GB or greater.

On successful migration, the `/nsr/mm/mmvolume6` directory gets appended with a timestamp to indicate that the directory is no longer active. You can keep this directory if you do not have a current bootstrap backup, otherwise it can be removed. The `mmvolrel` directory gets used as the new directory for the SQLlite database.

If the database migration does not complete, `nsrmmdbd` notifies you that migration has failed and the legacy WiSS database continues to run to process jobs until the migration is successful.

Note

It is recommended that you do not host a media database on a remote file system, for example, an NFS file system. Not all systems handle file locking correctly, which can introduce access latency that degrades performance.

NetWorker Server and resource migration

After upgrading from NetWorker 8.1.x and 8.2.x to NetWorker 9.2.x, when you start the NetWorker processes on the NetWorker Server, the process converts NetWorker 8.1.x and 8.2.x resources to the new NetWorker 9.2.x policy-based resources.

The following NetWorker 8.1.x and 8.2.x resource types do not exist in NetWorker 9.2.x:

- Group, also referred to as the savegroup or save group
- Schedule clone
- VMware policy
- NAS Device

NetWorker migrates the configuration information for each resource into new resources, which support the NetWorker Data Protection Policy framework.

The migration process creates log files on the NetWorker Server, which provide information about the status of resource conversions. The log files are located in the `/nsr/logs/migration` folder on LINUX and the `C:\Program Files\EMC NetWorker\nsr\logs\migration` directory on Windows.

The following table describes the files thatNetWorker creates during the resource migration process.

Table 3 Migration log files

File name	Purpose
`migration_summary_`*`date`*`.log`	Provides a summary of the resource conversion status.
`group_`*`groupname`*`.raw`	Provides detailed information about the migration of attributes in an 8.1.x and 8.2.x Group resource, including the following information: • A summary of NetWorker 8.1.x and 8.2.x attribute settings. • A list of NetWorker 8.1.x and 8.2.x attributes that are deprecated in 9.2.x and are not converted.

Table 3 Migration log files (continued)

File name	Purpose
	• A summary of attributes with defined values that override the equivalent attribute in the Client resource.
clone_*groupname*.raw	Provides detailed information about the migration of attributes in an NetWorker 8.1.x and 8.2.x scheduled Clone resource, including the following information: • A summary of NetWorker 8.1.x and 8.2.x attribute settings. • A list of NetWorker 8.1.x and 8.2.x attributes that are deprecated in 9.2.x and are not converted.
NAS_device_*groupname*.raw	Provides detailed information about the migration of attributes in an NetWorker 8.1.x and 8.2.x scheduled NAS Device resource, including the following information: • A summary of NetWorker 8.1.x and 8.2.x attribute settings. • A list of NetWorker 8.1.x and 8.2.x attributes that are deprecated in 9.2.x and are not converted.
VMWare_Policy_*groupname*.raw	Provides detailed information about the migration of attributes in an NetWorker 8.1.x and 8.2.x VMware Policy resource, including the following information: • A summary of NetWorker 8.1.x and 8.2.x attribute settings. • A list of NetWorker 8.1.x and 8.2.x attributes that are deprecated in 9.2.x and are not converted.

Backup Group resource migration

During the migration process, NetWorker creates resources to replace each Group resource, and then migrates configuration attributes from the NetWorker 8.1.x and 8.2.x resources to the new NetWorker 9.2 resources.

Resource migration for Group resources when Snapshot is not enabled

This section summarizes the group attribute values that migrate to 9.2 resources attributes, when the group is not Snapshot enabled.

Table 4 Migration of Group attributes

9.2 Resource type	9.2 Resource name	Migration process overview Attribute values migrated from Group resource	Attribute values migrated from Group resource
Policy	Backup	One policy resource that is called Backup appears and contains all migrated information for all NetWorker group resources that back up file system and NetWorker Module for Microsoft (NMM) data.	Not applicable
Protection Group	Name of the Group resource	One Protection Group resource appears for each migrated Group resource. Each Protection Group contains the same client resources that were associated with the pre-9.2 group resource.	Comment

Table 4 Migration of Group attributes (continued)

9.2 Resource type	9.2 Resource name	Migration process overview Attribute values migrated from Group resource	Attribute values migrated from Group resource
Workflow	Name of the Group resource	One Workflow resource appears for each migrated Group resource. Each Workflow resource is associated with the Protection Group resource that was created for the migrated Group resource.	• Autostart • Start Time • Next Start • Interval • Restart Window • End Time attribute value is set to Start Time+(Interval*(n-1)) • Probe Interval—To the Interval attribute • Probe Start Time—To the Start Time attribute • Probe End Time—To the End Time attribute
Probe	Probe	The Probe action resource appears when the Probe based group attribute was enabled in the pre-9.2 migrated group.	Not applicable
Action—Traditional backup	Backup	The Traditional Backup action appears for a Group resource that does not have the Snapshot attribute enabled.	• Parallelism • Retries • Retry delay • Success Threshold • Option attributes: ▪ No save, Verbose, Estimate, Verify Synthetic Full, Revert to full when Synthetic Full fails • Schedule • Schedule Time • Retention policy • Inactivity Timeout • Soft Runtime Limit—To Soft Limit • Hard Runtime Limit—To Hard Limit • File Inactivity Threshold—To Inactivity Threshold • File Inactivity Alert Threshold —To Inactivity Alert Threshold

Table 4 Migration of Group attributes (continued)

9.2 Resource type	9.2 Resource name	Migration process overview Attribute values migrated from Group resource	Attribute values migrated from Group resource
			• Min expiration = (1440/(backups per day/retain count))-10 • If Retain snapshot=0, then Backup snapshots attribute is set to ALL
Action—Clone	Clone	The Clone action resource appears when the Clone attribute was enabled in the Group resource.	Clone Pool—To the Destination Pool attribute

Scheduled Clone migration

The migration process creates one **Clone** policy for all the **Scheduled Clone** resources.

Table 5 Migration of Scheduled Clone attributes

9.2 resource type	9.2 Resource name	Migration process overview	Attribute values migrated from the Scheduled Clone resource
Policy	Clone	One Policy resource appears for all migrated Scheduled Clone resources.	Not applicable
Protection Group	Clone_*Name_of_Scheduled_Clone_resource*	One Protection Group appears for each migrated scheduled Clone resource. Each Protection Group contains the same save set list that was associated with the pre-9.2 Scheduled Clone resource.	Comment
Workflow	Name of the Scheduled Clone resource	One Workflow resource appears for each migrated Scheduled Clone resource. Each Scheduled Clone workflow is associated with the Protection Group resource that is created by the migrated Scheduled Clone resource.	• Comment • Start Time • Interval
Action	Clone	The Clone action appears for a Schedule Clone resource.	• Retention Policy • Destination Pool • Source Storage Node

The *NetWorker VMware Integration Guide* provides detailed information about VMware resource migrations.

The *NetWorker Snapshot Management Integration Guide* provides detailed information about Snapshot resource migrations.

The NMM documentation provides detailed information about NMM resource migrations.

Changes to the Client and Pool resources after migration

NetWorker uses a number of attributes that are defined in multiple resources to determine which pool receives the data that is generated by an action task, and how NetWorker backs up the data. The migration process preserves the values that are defined for the attributes and introduces new attributes in the Action resource.

NetWorker provides the following attributes, which work together to determine how NetWorker manages a backup and determines which device to use to receive the backup data:

- Client resource—**Pools**, **Retention**, **Save set**, and **Level** attributes on the **General** tab of the **Client Properties** window. The migration process retains the values in these legacy attributes.

  Note

  The **Modify Client** wizard does not display the **Pools**, **Retention**, **Save set**, and **Level** attributes.

- Action resource—**Destination Pool** and **Retention** attributes on the **Specify the Backup Options** and **Specify the Clone Options** wizard windows. The backup levels are defined for the action schedule on the **Specify the Action Information** wizard window.
- Pool resource—**Clients**, **Save sets**, and **Retention policy** attributes on the **Legacy** tab. The values that appear in these attributes were defined in NetWorker 8.1.x and 8.2.x. After the migration completes, the NetWorker 9.2 server retains the values and these legacy attributes become read-only. You cannot modify the values in these fields after migration.

The Action resource includes an attribute that is called **Client Override Behavior**. The value that is selected for this attribute determines which resource attribute has precedence over the attributes in other resources that determine the same behavior. By default, the migration process enables **Legacy Backup Rules** on an Action resource. **Legacy Backup Rules** allow NetWorker to use the values during the pool selection criteria process.

Note

By default, the **NetWorker Administration** window does not show the legacy attributes. To view the legacy attributes in the **Client Properties** window, go to the **View** menu and select **Diagnostic Mode**.

Client resource overrides

NetWorker 9.2.x enables you to define a schedule, destination pool, retention policy, and destination storage node for each backup action that you configure.

NetWorker 8.1.x and 8.2.x allowed you to define a schedule, destination pool, retention policy, and destination storage node value for each Group and Client resource.

When you assigned a value to any of these attributes in the Group resource, that value was applied to all data generated by each client in the group.

When you assigned a value to any of these attributes in the Client resource, that value was applied to all data generated by the client and took precedence over the value that was defined in the equivalent Group resource attribute.

The updating process retains these Client resource values but sets the attributes values to read-only.

The Client resource has the following attributes in common with the Action resource:

- **Schedule**
- **Pool**
- **Retention**
- **Storage Node**

The NetWorker 9.2.x **Action** wizard provides you with the ability to define which resource attribute takes precedence, the value that is defined in the Action resource or the value that is defined in a Client resource. The selection that you make in the **Client Override Behavior** list determines which attribute values take precedence. The following table summarizes each option.

Table 6 Client override behaviors

Option	Behavior
Client Can Override	The values in the Client resource for **Schedule**, **Pool**, **Retention policy**, and the **Storage Node** attributes take precedence over the values that are defined in the equivalent Action resource attributes.
Client Cannot Override	The values in the Action resource for the **Schedule**, **Destination Pool**, **Destination Storage Node**, and the **Retention** attributes take precedence over the values that are defined in the equivalent Client resource attributes.
Legacy Backup Rules	This value only appears in actions that are created by the migration process. The updating process sets the **Client Override Behavior** for the migrated backup actions to **Legacy Backup Rules**. This value handles the Schedule, Pool, Retention, and Storage Node values in the following way: • If a value is defined in the **Retention Policy** attribute of the Group resource, then the value that is defined in the **Retention** attribute of the Action resource takes precedence. If a value is not defined in the Group resource, then the attribute that is defined in the Client resource takes precedence. • If a value is defined in the **Schedule** attribute of the Group resource, then the value that is defined in the **Schedule** attribute of the Action resource takes precedence. If a value is not defined in the Group resource, then the attribute that is defined in the Client resource takes precedence. • If a value is defined in the **Pool** attribute of the Client resource, the value that is defined in the Client resource is used. If a value is not defined in the Client resource, then the action sends the data to a pool that best matches the pool selection criteria. **Note** You can edit the Action resource and change the **Client Override Behaviour** attribute to **Client Can Override** or **Client Cannot Override**, but after you save the change to the Action resource, you cannot set the attribute back to **Legacy Backup Rules**.

Changes to the schedule resource and levels

NetWorker allows you to configure attributes in the Action resource that define the schedule for the task, and for a backup or clone task, the level.

When you configure an Action resource in NetWorker 9.2.x, the **Action** wizard provides you with the ability to define the schedule, schedule overrides, and level for the data that is generated by the task.

In NetWorker 8.1.x and 8.2.x, you assigned a pre-configured or user-configured backup schedule to the Group and Client resources. When you assigned the schedule or a level to the Group resource, the values were applied to all the backup and clone data generated by each client in the group. When you assigned the schedule or level to the Client resource, the values were applied to all the backup and clone data generated by the client and took precedence over the values that were defined in the Group resource.

The updating process migrates existing values in the Schedule and Level attributes in the Group resource to the Action resource. NetWorker 9.2.x does not support backup levels 2–9. When the update process encounters a schedule with a backup level 2–9, NetWorker changes the level to 1. The update process retains the level and schedule attributes that were defined in the Client resource.

The Client resource overrides section describes how NetWorker 9.2.x determines the schedule that a task uses when an action is performed on a client and both the Client resource and Action resource define a schedule.

Changes to save set policies

NetWorker 9.2.x does not separate the length of the browse time for a save set from the length of the retention time for a save set. Information about a backup or clone save set remains in the client file index and media database for the length of time that is defined by the retention policy.

When you configure an Action resource in NetWorker 9.2.x, the Action wizard provides you with the ability to define the retention policy for the data that is generated by the task.

In NetWorker 8.1.x and 8.2.x, you assigned a browse and retention policy to the Group and Client resources. When you assigned a browse or retention policy to the Group resource, the value that is applied to all the data that is generated by each client in the group. When you assigned a policy to the Client resource, the value that is applied to all the data that is generated by the client.

The updating process performs the following tasks:

- Migrates the existing value in the Retention Policy attribute in the Group resource to the Action resource.
- Modifies the browse time for all save sets in the media database to match the retention time.
- Modifies the Browse policy in the Client resource to match the existing value in the Retention Policy attribute, and make the attribute read-only.
- Retains the value that is defined in the Retention Policy attribute that was defined in the Client resource.
  The Client resource overrides section describes how NetWorker 9.2.x determines the retention policy that a task uses when an action is performed on a client and both the Client resource and Action resource define a retention policy.

Changes to the save set expiration process

NetWorker 9.2.x expires save set information in the media database and client file index as a separate action, in the Server backup workflow, which is part of the Server Protection policy.

In NetWorker 8.1.x and 8.2.x, the NetWorker server ran an `nsrim` process once every 24 hours to remove information about eligible save sets from the client file index and mark eligible save sets as recoverable or recyclable in the media database.

NetWorker 9.2.x creates a Policy resource that is called the Server Protection policy. The Server Protection Policy contains the Server Protection group. The Server Protection group is associated with the Server backup workflow, which starts the Expiration action daily at 10 a.m.

Expiration
The expiration action expires save sets in the media database based on retention time of the save set. When the retention time of the save set has been reached, NetWorker uses the `nsrim` process to expire the save set. When a save set expires, the `nsrim` process performs the following actions:

- Removes information about the save set from the client file index.
- If the save set data resides on an AFTD, removes the save set information from the media database and removes the save set data from the AFTD.
- If the save set data resides on a tape device, the `nsrim` process marks the save set as recyclable in the media database. When all save sets on a tape volume have expired, the volume is eligible for reuse.

An expiration action is created automatically in the Server maintenance workflow of the Server Protection policy. An expiration action only supports Execute and Skip backup levels.

Changes to bootstrap and index backups

NetWorker 9.2.x performs a bootstrap and index backup as separate backup action in the Server backup workflow, which is part of the Server Protection policy.

In NetWorker 8.1.x and 8.2.x, NetWorker performs a bootstrap backup when the operations in a group that contains the NetWorker server completes. If the NetWorker server Client resource does not appear in an active Group resource, the bootstrap backup every time a group completes, even when the backup level is set to skip.

NetWorker 9.2.x creates a policy resource that is called the Server Protection policy. The Server Protection Policy contains the Server Protection group. The Server Protection group is associated with the Server backup workflow, which starts the Server database backup action daily at 10 a.m.

Server database backup
A server database backup action performs a bootstrap backup and can also include the client file indexes.

A bootstrap backup contains the following NetWorker server components:

- Media database
- Server resource files. For example, the resource (res) database and the Package Manager database (nsrcpd)
- NetWorker Authentication Service database

NetWorker automatically creates a server backup action in the Server Backup workflow of the Server Protection policy. By default, a full backup of the media

database, resource files, and the NetWorker Authentication Service database occurs daily. A full backup of the client file indexes occur on the first day of the month. An incremental backup of the client file indexes occur on the remaining days of the month. The default retention policy for the server database backup is one month.

The migration process may not assign the bootstrap backup to the pool that was configured in NetWorker 8.1.x and 8.2.x. You can edit the Server database action in the NetWorker Administration window and change the destination pool value or use the `nsrpolicy` command to update the pool. For example:

```
nsrpolicy action update server-backup -p "Server Protection" -w
"Server backup" -A "Server db backup" --destination_pool pool_name
```

Changes to the NMC database backup

NetWorker 9.2.x performs an NMC database backup as separate backup action in the NMC Server backup workflow, which is part of the Server Protection policy. The NMC database backup action creates a staging directory for the database files, performs a backup of the staging directory, and then deletes the contents of the staging directory.

In NetWorker 8.1.x and 8.2.x, the NMC server configuration process created a Client resource for NMC database backups on the NetWorker server. The Client resource contained the following value in the **Save set** attribute:

NMCASA:/gst_on_*server_name*/lgto_gst

where *server_name* is the short name of the NMC server host.

When the update process detects a Client resource for the NMC backup, NetWorker migrates the Client resource, but does not add it to the Protection Group associated with NetWorker 8.1.x and 8.2.x Group resource that contained the NMC Client resource. The migration process makes the following attribute changes to the Client resource for the NMC server database backup:

- Updates the value in the **Save set** attribute. The **Save set** field for the client contains the path to the database staging directory. By default, the staging directory is in `C:\Program Files\EMC NetWorker\Management \nmcdb_stage` on Windows and `/opt/lgtonmc/nmcdb` on Linux.

  Note

  The file system that contains the staging directory must have free disk space that is a least equal to the size of the current NMC database. The *NetWorker Administration Guide* describes how to change the staging directory

- Clears the values in the **Level** and **Retention** attributes.

When you log in to the NMC server for the first time after an update, the configuration wizard prompts you to define the NetWorker server that will backup the NMC database. When you configure the NMC database backup, the NetWorker server performs the following actions:

- Creates a group called NMC server.
- Adds the Client resource to the NMC server group.
- Creates a workflow that is called NMC server backup in the Server Protection policy. The workflow contains the NMC server backup action, which performs a full backup of the NMC server database every day at 2 P.M.

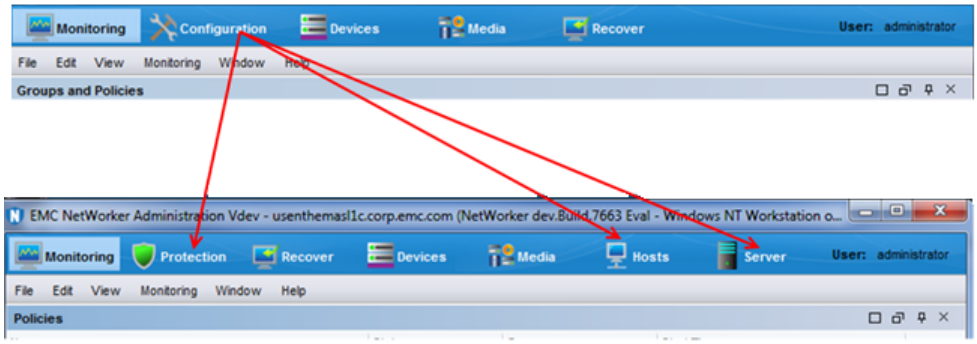
- Adds the NMC server group to the NMC server backup workflow.

Visual representation of NMC's Administration window

In NetWorker 9.0 and later releases, the NetWorker Management Console's (NMC) **Administration** window features three new windows, including the **Protection**, **Hosts**, and **Server** windows, which replace the **Configuration** window from previous versions.

The following graphic shows the visual difference between the **Administration** window options for NetWorker 8.2.x and NetWorker 9.1.

Figure 6 Visual changes to Administration window between NetWorker 8.2.x and NetWorker 9.1



The three additional windows contain functionality and resources that were previously managed under the **Configuration** window:

- Protection—The main function of the **Protection** window is to create and manage policies that protect all the data in the environment. The data protection policy replaces the client backup configuration previously available from the **Configuration** window.
- Hosts—The **Hosts** window allows you to manage local host activities with easily visible repository and inventory details, and to manage all installed NetWorker packages across hosts, replacing the previous **Software Administration** wizard.
- Server—The **Server** window contains all resources (for example, User Groups information) that previously appeared in the **Configuration** window.

Data Protection Policies and the Protection window in NMC

NetWorker introduces a new method for protecting data in the environment—the creation of policies, which you can perform from the **Protection** window in the NetWorker Management Console's **Administration** window, or by using the `nsrpolicy` command.

NetWorker 8.2 and earlier

NetWorker 8.2 and previous releases require you to create and configure Client and Group resources to perform backups, clones, and so on, using the **Configuration** window or by running `savegroup`.

NetWorker 9.0 and later

Instead of creating a backup by using the **Client Backup Configuration** wizard under the Client tab, the **Protection** window allows you to create data protection policies

and assign those policies to clients, virtual machines, and so on, across the environment.

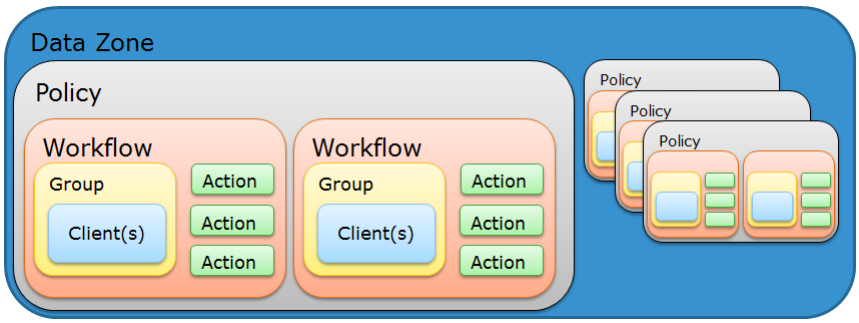
Policies are made up of actions (such as backup and cloning operations) that you can configure using action wizards in the **Administration** window, or by using the new command line tool `nsrpolicy`.

Setting up a policy includes creating the following resources:

- Client resource—Allows you to define the backup data for a host. By default, when you install NetWorker, the installation process creates two Client resources -- one to backup all local file systems on a NetWorker Server, and one to backup the NetWorker and NMC server databases.
- Policy resource—Provides a container for the workflows, actions, and groups that support and define the backup, management, and system maintenance actions that you want to perform.
- Workflow resource—Allows you to define the order of actions, concurrently or in sequence, and when to start the sequence. You can create multiple workflows in a single policy. However, each workflow can belong to only one policy.
- Group resource—Allows you to group a set of clients, virtual machines, and so on, for a specific workflow, which is based on the type of actions you plan to perform. You create one group for each workflow. You can create the group before you create the workflow, or you can create the group after you create the workflow and then assign the group to the workflow later.
- Action resource—Allows you to define a specific task, and specify how and when to run the task. Actions include backup operations, cloning operations, or user-defined actions. You can create multiple actions for a single workflow. However, each action applies only to a single workflow and policy.

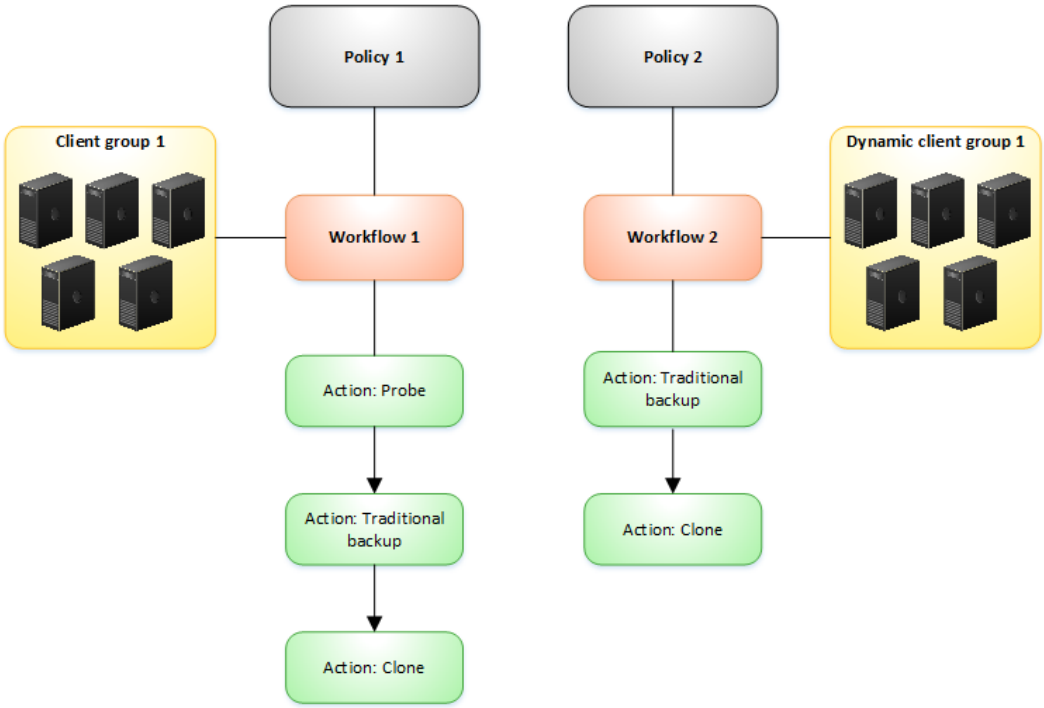
The following diagram shows how the policy acts as a container for the workflows, groups, and their associated actions.

Figure 7 Policy as a container



The following figure illustrates a policy with two different workflows. Workflow 1 performs a probe and then a backup of the Client resources in Client group 1, and then clones the save sets from the backups. Workflow 2 performs a backup of the Client resources in Dynamic client group 1, and then clones the save sets from the backups.

Figure 8 Data protection policy example



Setting up a policy in NMC GUI's Administration window

The following section describes how to set up a basic policy container in the NMC GUI's **Administration** window.

Before you begin

Performing these steps requires a working knowledge of NMC and the **Administration** window.

It is recommended that you use the following order of operations within the **Administration** window for policy creation:

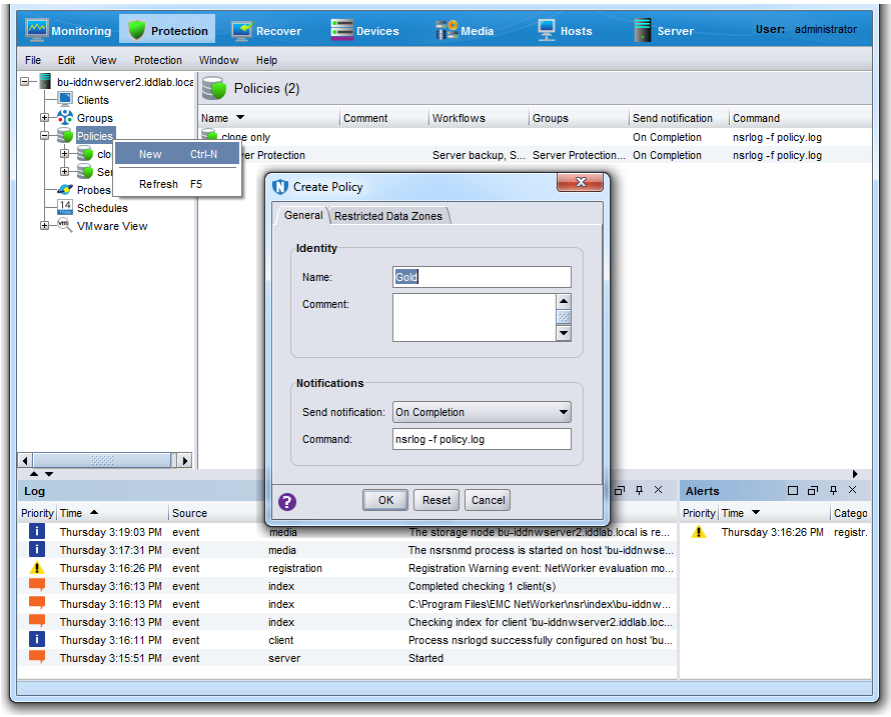
- Create a new policy (**Policies** > **New**)
- Create a new workflow using the **New Workflow** wizard. You can create multiple workflows per policy, however, each workflow should contain only one group.
- Create a group (**Groups** > **New**) .
- Create the actions for the workflow, for example, backup, clone, and so on, using the **Policy Action** wizard.
- Assign the clients or save sets that you want to protect to the group. The clients that you assign to the group should fit the type of actions you want to perform.

Procedure

1. In the **Administration** window, select **Protection**.
2. On the left navigation pane, right-click **Policies** and select **New**.

   The **Create Policy** window appears, where you specify a name for the policy, and then click **OK**.

Figure 9 Policy setup - creating the policy



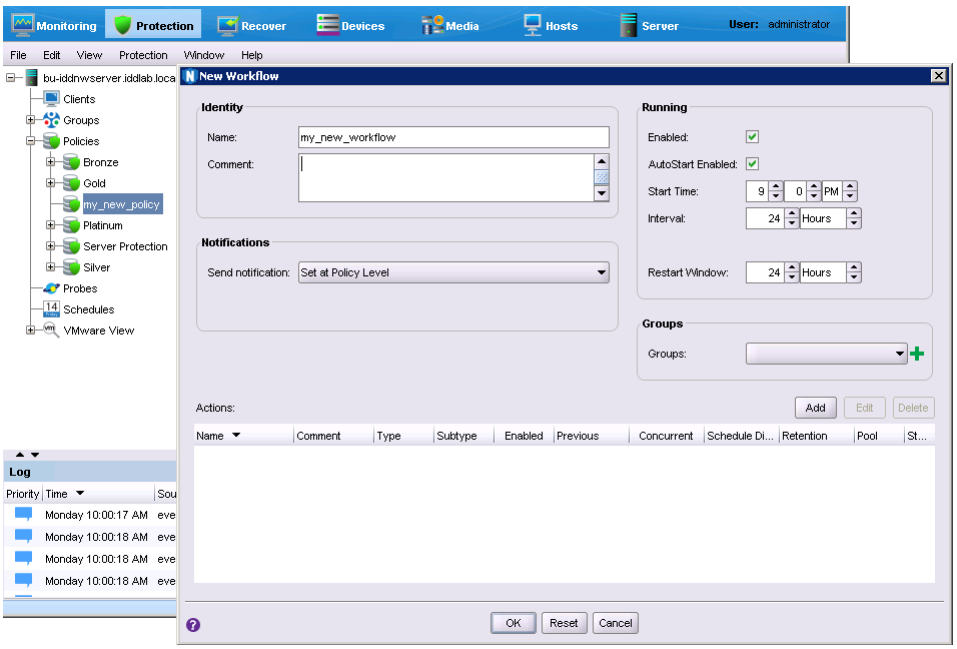
3. In the left navigation pane, expand **Policies** and then select the policy that you created.

   In the right pane, the option to create a workflow appears.

4. With the policy selected, go to **File** > **New** to start the new workflow, or select **Create a New Workflow** in the right pane.

   The **New Workflow** window appears. Specify a name for the workflow that reflects the type of protection.

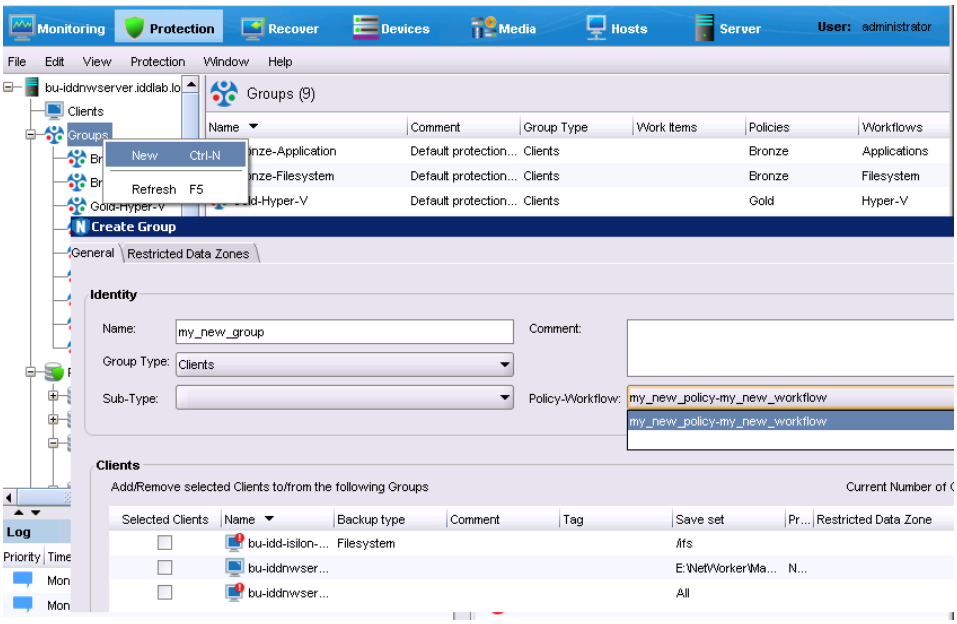
Figure 10 Policy setup - creating the workflow



5. On the left navigation pane, right-click **Groups** and select **New**.

   The **Create Group** window appears. Specify a name for the group, select the name of the workflow, and then click **OK**.

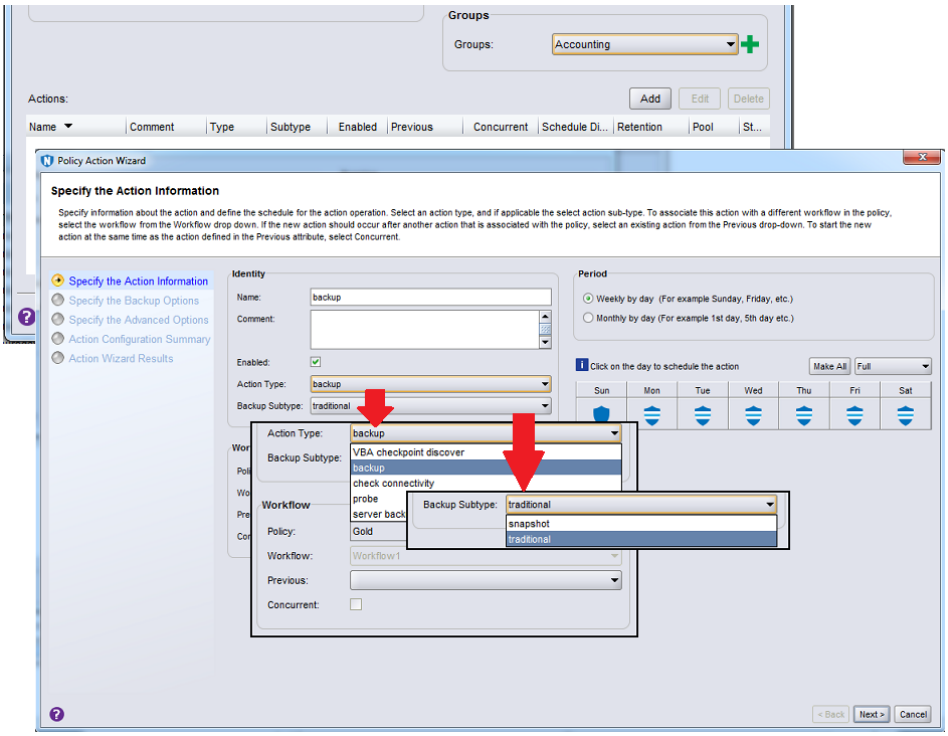
   Figure 11 Policy setup - creating a group and adding client(s)



6. On the left navigation pane, select the new workflow, and then select **Create a new action**.

   The **Policy Action** wizard opens. Specify a name and action type (for example, backup, traditional) for the action and then continue through the wizard.

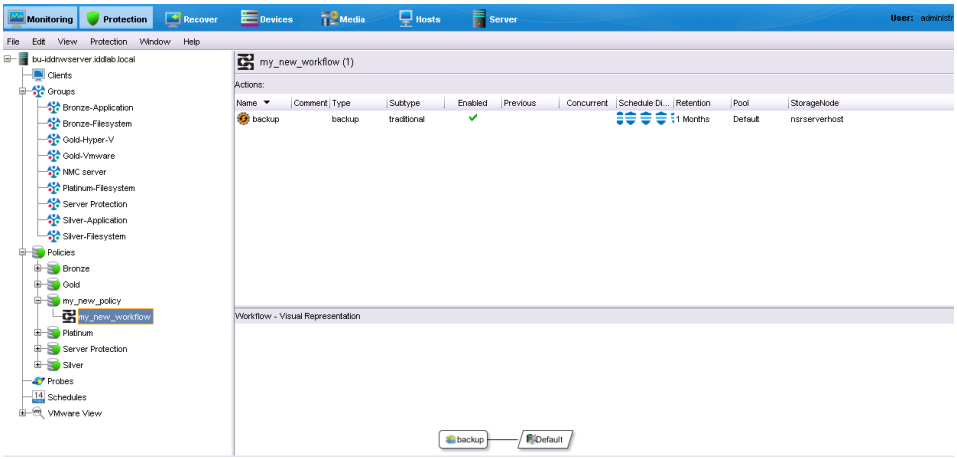
   Figure 12 Policy setup - creating the actions



7. In the **Action Wizard Summary** window, click **Configure**.

The **New Workflow** window appears with the new action, and a visual representation of the Workflow appears in the **Workflow - Visual Representation** pane.

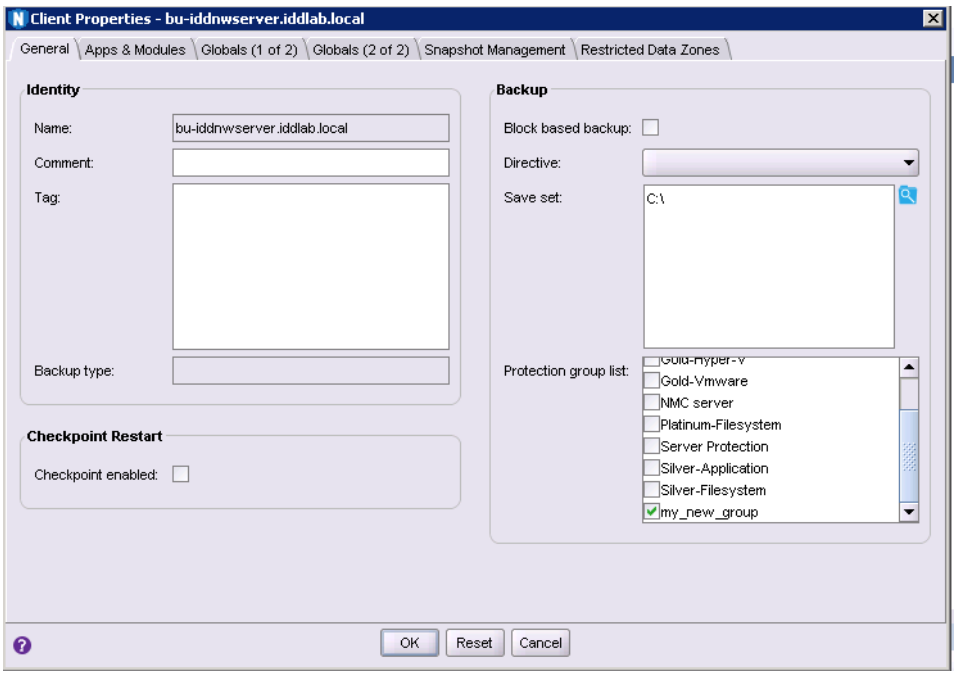
Figure 13 Policy setup - configuring workflow actions



8. Right-click the workflow and select **New** to start the **Policy Action wizard** to create additional actions, such as clone actions.
9. On the left navigation pane, select **Clients**.

   The Client resources for the NetWorker Server appear in the **Clients** window.
10. Right-click the client instance that contains the Save set All and select **Modify Client Properties**.
11. In the **Save set** field, click the **Browse** icon. Unselect the server and expand the browse tree, and then select a directory. Click **OK**.
12. In the **Groups** field, select the new group. Click **OK**.

Figure 14 Policy setup - adding client to group



13. In the **Monitoring** window, right-click the policy in the Policies pane and select **Start**.

Setting up a policy from the command line

In addition to configuring data protection policies from the NMC GUI's **Administration** window, you can also use the command line tool `nsrpolicy` to perform the same functionality. The workflow for policy creation is very similar to the order used in the **Administration** window.

Procedure

1. Create a protection group and add clients to the group:

   `nsrpolicy group create client -C` *networker client* `-g` *group name*

2. Create a policy:

   `nsrpolicy policy create -p` *policy name* `-c` *policy comment*

3. Create a workflow, and assign the group created in step one, policy created in step two, and a schedule, to the workflow:

   `nsrpolicy workflow create -p` *policy name* `-w` *workflow name* `-c` *workflow comment* `-S` *schedule* `-g` *group name*

4. Create actions. For example, backup and clone actions:

   `nsrpolicy action create backup traditional -p` *policy name* `-w` *workflow name* `-c` *action comment* `-A clone-`*workflow name*`-backup-action -b traditional -o` *backup pool*

Results

When you complete the policy setup, you can choose options to display the policy (`nsrpolicy policy display -p` *policy name*), run the policy (`nsrpolicy start -p` *policy name* `-w` *workflow name*), and monitor the policy progress (`nsrpolicy monitor -p` *policy name* `-w` *workflow name*).

Server Protection policy and workflows

When you install or upgrade the NetWorker server, the installation or upgrade process creates a Server Protection policy with default workflows to support NetWorker and NMC backup and maintenance activities.

The Server Protection policy includes the following default workflows:

Server backup
The workflow performs two actions:

- Expiration—An expire action to mark expired save sets as recyclable.
- Server database backup—A backup of the NetWorker server media database, authentication service database, and the client file indexes. The data in this backup, also called a bootstrap backup, enables you to perform a disaster recovery of the NetWorker server.

The workflow is scheduled to start daily at 10 a.m. The workflow is assigned to the default Server Protection group, which contains a dynamically generated list of the Client resources for the NetWorker server.

NMC server backup

The workflow performs a traditional backup of the NMC database. The workflow is scheduled to start a full backup daily at 2 p.m. The workflow is assigned to the default NMC server group, which contains the NMC server.

Hosts window in the NMC GUI's Administration window

NetWorker 9.0 features a dedicated **Hosts** window for the management of NetWorker packages and local host activities.

NetWorker releases previous to NetWorker 9.0 and later

In NetWorker releases previous to NetWorker 9.0 and later, NMC provides a wizard for managing packages across hosts. From the **Configuration** window, you can launch the **Software Administration** wizard and choose a certain operation (for example, inventory of all local hosts), and continue to go through the wizard for each required operation.

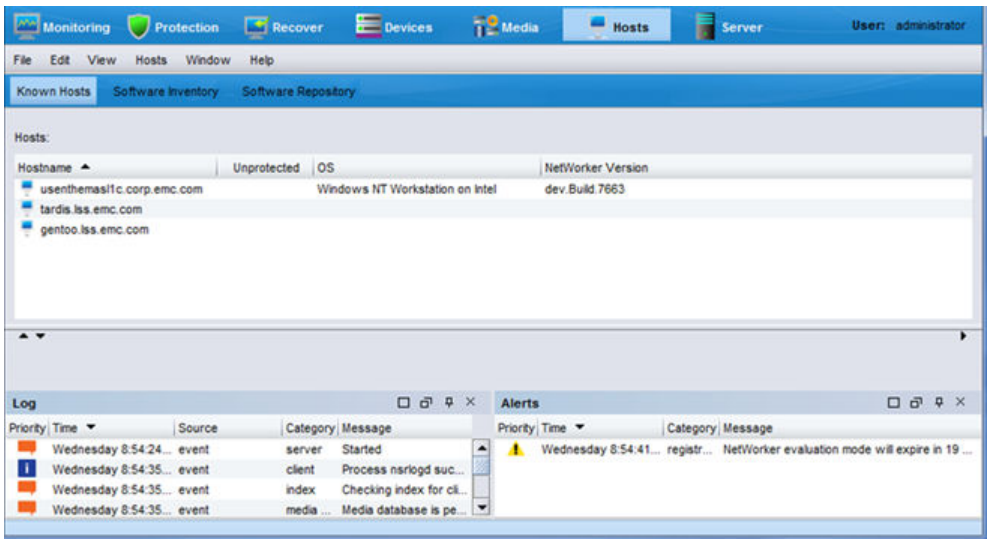
NetWorker 9.0 and later

In NetWorker 9.0 and later, you can perform package management by using the **Hosts** window, which provides you with the ability to easily view the host, the version of the software, and if the host is eligible for an upgrade.

The **Hosts** window is divided into three sub-tasks:

- Known Hosts—Provides information about the configured hosts and their certificates, NetWorker version, operating system, and performed software operations. You can also determine whether the host is eligible for an upgrade.
- Software Inventory—Displays information about the software packages that are installed on the host, and provides the option to upgrade the software and monitor the upgrade in the Software Operations pane.
- Software Repository—Displays a view of the NetWorker server's repository, providing version information for all products that are installed on the NetWorker host. You can also add to the repository from this view.

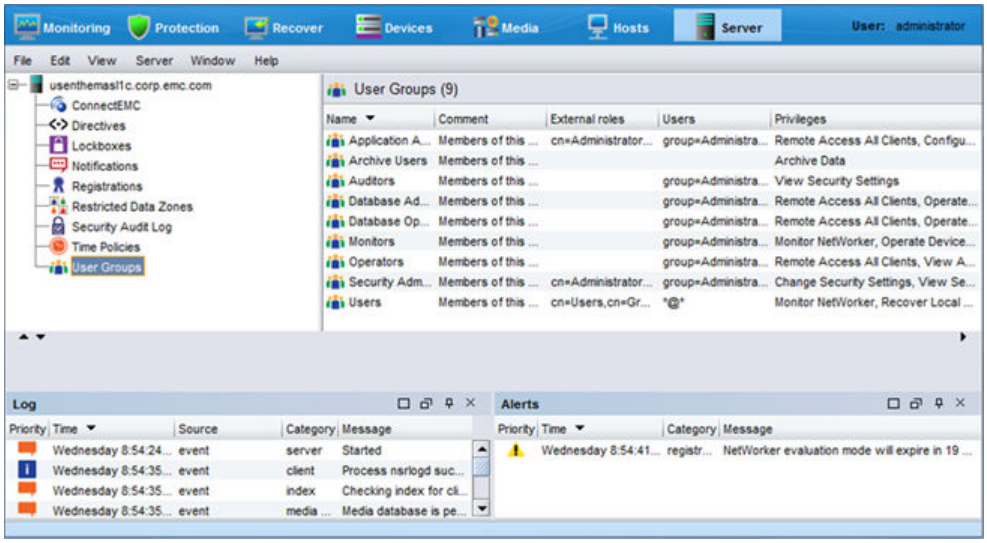
Figure 15 Hosts window



Server window in the NMC GUI's Administration window

The **Administration** window in NetWorker 9.0 and later features a **Server** window, which contains most of the resources that were previously located under the **Configuration** window, such as **Directives**, **Notifications**, and **User Groups**.

Figure 16 Server window



Changes to NetWorker VMware Protection

NetWorker 9.1.x and 9.2 releases feature a vProxy appliance, or NVP, for virtual machine protection. NetWorker 8.2.x and 9.0.x releases feature a VMware Backup appliance, or VBA, for virtual machine protection. Similar to VBA in NetWorker 9.0, NVP in NetWorker 9.1 features the integration of VMware Protection Policies within the main policy workflow of NMC, an interface for the **EMC Data Protection Restore Client** for file-level restore, and the use of a plug-in within the **vSphere Web Client** to run virtual machine backup and recovery.

NetWorker 8.2.x

Upon deployment of the VMware Backup Appliance in NetWorker 8.2 SP1 and earlier, two resources appear in the left pane of the **Configuration** window in NMC:

- A default protection policy, which is created after NetWorker registers the first VMware Backup Appliance.
- A default device, which is based on the media type AFTD, to backup to the VMware Backup Appliance's internal storage.

NetWorker 9.0.x

In NetWorker 9.0.x, further integration of VMware protection policies within the data protection policy framework of NMC means that you no longer require a separate window to run policies for the VMware Backup Appliance. Access to the same functionality is available in the NMC **Administration** window, under the **Protection** window. Expanding **Policies** in the left pane of the **Protection** window displays all existing protection policies. You can protect virtual machines and VMDKs at the group level by specifying the group type as **VMware**, and associate the group with a workflow and policy.

To view the available VMware Backup Appliances, select the **Devices** window. When you select **VMware Backup Appliances**, the deployed appliances appear in the right pane, which also allows you to monitor the state of the appliance.

VMware View remains the same, as well as the visual representation, which are now provided in the **Protection** window.

The new interface for the **EMC Data Protection Restore Client** allows you to perform file-level recoveries in two modes:

- User, which allows a local user to restore folders or files to the original virtual machine.
- Admin, which allows an administrator to restore folders or files from a different virtual machine to any available destination client.

NetWorker 9.1

NetWorker VMware Protection with the vProxy appliance (NVP) is a new solution available in NetWorker 9.1 and later releases for virtual machine backup and recovery. With NVP, NetWorker directly manages the vProxy appliances without the use of an external node for proxy management. New installations of NetWorker 9.1 and later use NVP.

NVP has the following benefits:

- Uses standalone data mover proxy appliances, or vProxy appliances to backup and restore virtual machines that run in a virtualizated infrastructure.
- NetWorker directly manages the vProxy appliances without the use of an external node for proxy management and load balancing.
- Stores the virtual machine backups as raw VMDKs on the Data Domain device, which reduces overhead. NetWorker does not convert the backup to any backup streaming formats.
- Provides the ability to clone virtual machine backups. When you use streaming devices such as tape, NetWorker converts the save set directories format (SSDF) to Common Data Storage Format (CDSF) during a clone operation, and converts back to SSDF on Data Domain for recovery from streaming devices.
- Provides user interfaces to perform image-level recovery by using the **NMC Recovery** wizard or the **VM Backup and Recovery** plug-in within the **vSphere Web Client**, and file-level recovery by using the **NMC Recovery** wizard or the **EMC Data Protection Restore Client**.

Note

If upgrading from a NetWorker 9.0 and earlier release to NetWorker 9.1 and later, you can choose to migrate VBA policies and workflows to the NVP solution, or you can continue to use the VMware Backup appliance to run existing VBA protection policies and recover from VBA backups. Note, however, you will not be able to create any new policies using the VMware Backup Appliance, and you cannot recover backups performed with the VMware Backup appliance by using the vProxy appliance.

NetWorker 9.2

NetWorker 9.2 features the addition of advanced application-consistent data protection for the purposes of backup and recovery of SQL databases, instances, and transaction logs as part of a NetWorker VMware Protection workflow.

For SQL application-consistent data protection, a separate policy is created within NMC, where the Policy Action wizard allows you to select the advanced application-consistent backup option, as well as enabling transaction log backups.

Microsoft VM App Agent for SQL Server application-consistent protection

The Microsoft Virtual Machine Application Agent (MSVMAPPAGENT) is a new component of the vProxy data protection solution that is bundled with the vProxy appliance OVA for NetWorker 9.2. **MSVMAPPAGENT** is automatically deployed by the vProxy during a virtual machine application-consistent backup and, if required, when restoring Midrosoft SQL databases and SQL instances to running virtual machines. After installation, the **MSVMAPPAGENT** package appears in the Windows installer Add-Remove programs list.

The **MSVMAPPAGENT** allows for advanced application data protection of workloads residing on a VMware ESXi server. In NetWorker 9.2, this includes adding SQL virtual machines to an application-consistent protection policy to perform the following operations:

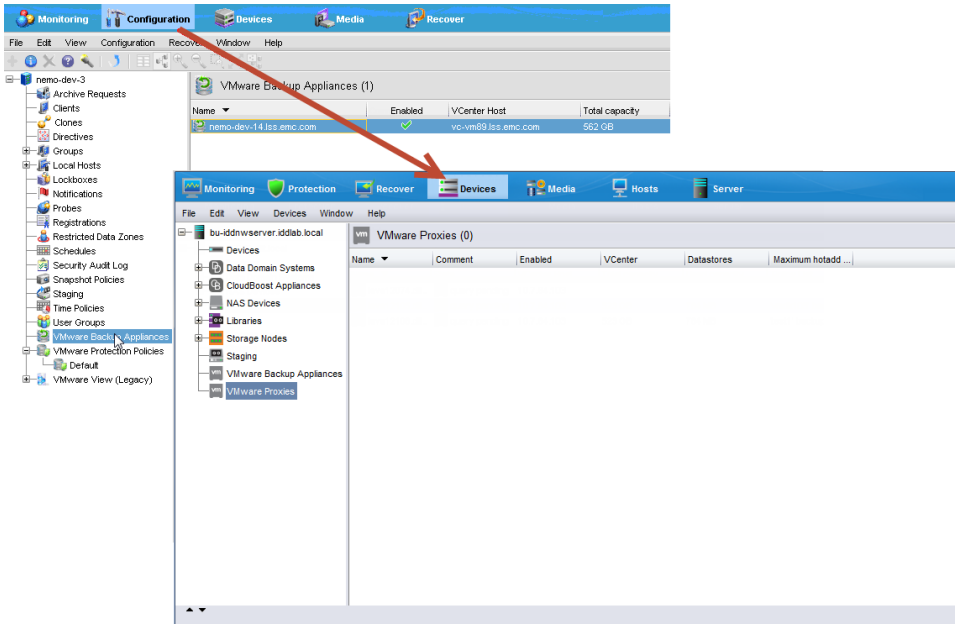
- SQL Server FULL backup to Data Domain—Configure a NetWorker policy's VMware backup action with the Advanced Application Consistency option to perform SQL Server FULL backup to a Data Domain device. The SQL Server FULL backup is performed during the in-guest quiesce by VMware Tools. After running the policy, the catalog and index information for the SQL server backup is stored on the Data Domain device. The SQL data files are backed up as part of the VMDKs during the vProxy image backup.
- Transaction log backup—When configuring a NetWorker policy's workflow and VMware backup action with the Advanced Application Consistency option, select Transaction log backup to enable transaction log backups for SQL Instances running in the virtual machine, and set the Interval attribute in the backup policies workflow properties to specify the frequency of backups. Backups are written directly to Data Domain under the SDSF backup folder that was created by the NetWorker save set session. Transaction log backup is only performed for databases in the proper state, otherwise databases are skipped.
- Restore of SQL Server instance or individual SQL Server databases—The **Dell EMC Data Protection Restore Client** includes an App mode that allows you to restore an entire SQL Server instance or individual SQL Server databases to the original database on the original virtual machine, with roll-forward of transaction log backups.

Visual differences for VMware Protection

The following diagrams show the visual differences in the handling of VMware Protection policies between NetWorker 8.2.x and NetWorker 9.1 in the NMC **Administration** window

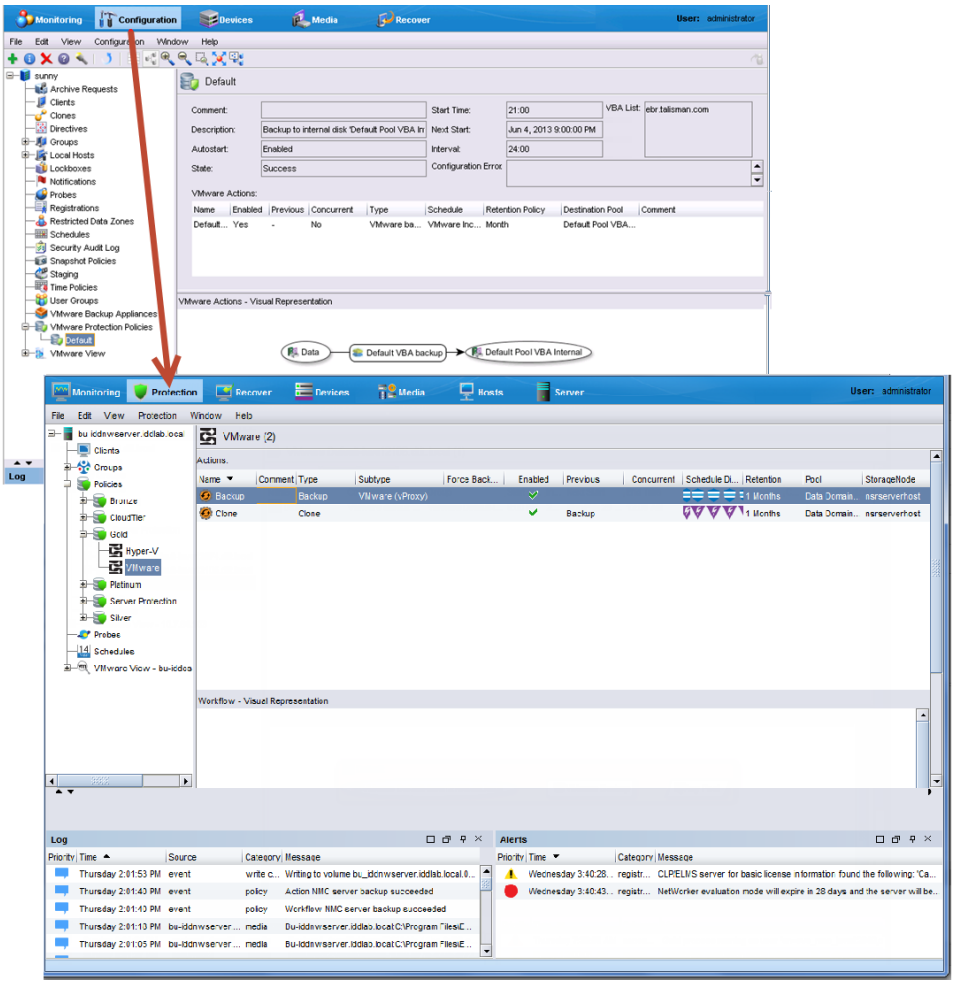
Information about the deployed VMware Backup Appliance changes from the **Configuration** window to the **Devices** window.

Figure 17 Changes to VMware Backup Appliance monitoring in the Devices window



VMware Protection Policy creation changes from the **Configuration** window to the **Protection** window.

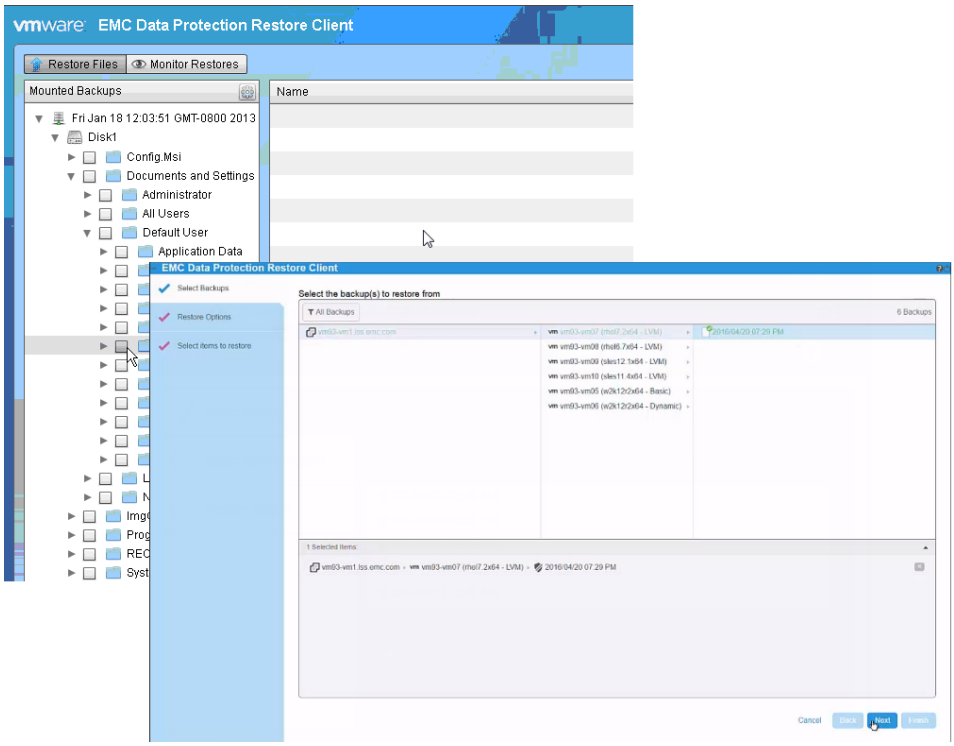
Figure 18 Changes to VMware Protection policies in the Protection window



The process for creating a VMware policy, workflow, group, and actions is similar to the process described in the topic Sample policy setup, and is provided in detail in the *NetWorker VMware Integration Guide*.

The **Dell EMC Data Protection Restore Client** also contains some visual differences. In NetWorker 9.1, the **Dell EMC Data Protection Restore Client** functions like a wizard, where you complete steps to perform file-level recoveries.

Figure 19 Changes to the EMC Data Protection Restore Client



Migrating policies from VMware Backup appliance to vProxy appliance

New installations of NetWorker 9.2 use the NetWorker VMware Protection solution with the vProxy appliance. When you upgrade from a NetWorker 9.0.x and earlier release, you can continue to use the VMware Backup appliance, migrate to use only the vProxy appliance, or use a combination of the VMware Backup appliance and vProxy appliance. If you choose to use the vProxy appliance only, workflow migration is required to convert existing VMware Backup appliance policies to vProxy appliance policies.

This migration involves two stages—a check that occurs prior to migration to ensure all the compatibility prerequisites are satisfied, and then the actual migration to convert existing VMware Backup appliance protection groups and policies to the vProxy appliance. You can initiate the policy migration by using the command line or NMC.

Note

NetWorker does not support the migration of workflows and policies from a VMware Backup appliance deployed in a NetWorker release previous to NetWorker 9.0 that uses GSAN internal storage.

Migration pre-requisites

When you migrate a VMware Backup appliance policy to a vProxy policy, a pre-check occurs automatically to determine that compatibility requirements are met.

These requirements include verification of the following items:

- The Data Domain OS (DD-OS) is DDOS version 5.7, 6.0.0.30, 6.0.1-10, or 6.1. Note that use of the DD Retention Lock feature on vProxy backup and clone actions requires DDOS 6.1.
- The NetWorker server and storage node version is NetWorker 9.2.
- The vProxy is available on the vCenter server and is version 2.1.0.17 for NetWorker 9.2.
- The vCenter server is a minimum of version 5.5.

If this check discovers any compatibility issues that can cause problems migrating all policies, the issues are reported and migration is cancelled. If using the command line to migrate policies, you can specify a force flag (-f) to ignore these errors and proceed with the migration to correct any issues afterwards, however it is recommended that the pre-check requirements be met prior to proceeding with the migration. Issues discovered during the pre-check will be logged and displayed even when using the force flag.

Additionally, if you used IPv6 only or dual stack (IPv4 and IPv6) for the VMware Backup appliance and are migrating to use the vProxy appliance, ensure that you switch to IPv4 only. The vProxy appliance does not support either IPv6 or dual stack (IPv4 and IPv6), and so the migration from the VMware Backup appliance to the vProxy appliance will not work with these configurations. If you previously used IPv4 only, no configuration change is necessary.

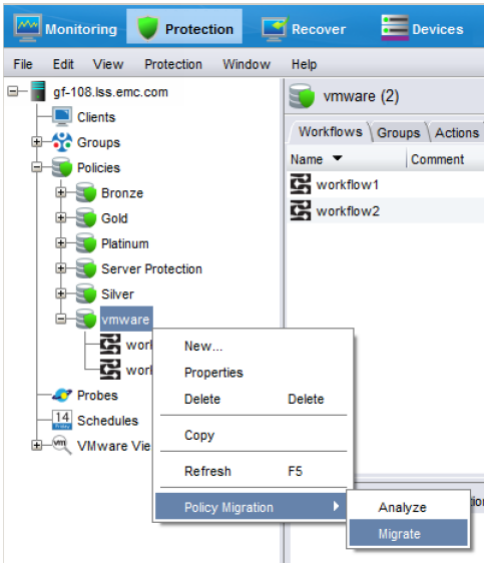
Policy migration to vProxy by using NMC

You can use the NetWorker Management Console (NMC) Administration window to migrate VMware Backup appliance policies and workflows to vProxy, or perform a pre-check before migrating.

Procedure

1. In the NMC **Administration** window, click **Protection**.
2. In the left pane, expand **Policies** to view the VMware policy.
3. (Optional) Right-click the **vmware** policy and select **Policy Migration** > **Analyze** from the drop-down if you want to perform a compatibility pre-check before migration.
4. Right-click the **vmware** policy and select **Policy Migration** > **Migrate** to start the migration.

Figure 20 Migrating a VMware Backup appliance policy to vProxy in NMC



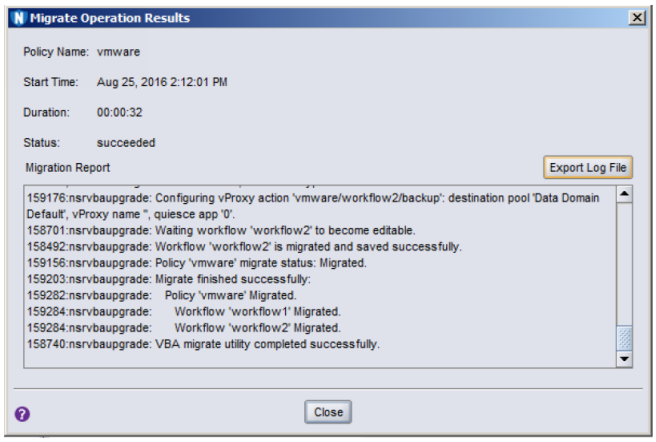
Note

If a pre-check failure occurs upon initiating the migration, a prompt appears to confirm that you want to ignore the errors and proceed. It is recommended that you resolve any pre-check errors, including unsupported software versions, before completing the migration in order for backups to complete successfully.

Results

A **Migrate Operation Results** dialog box opens which provides a real-time report of the analyzation and the migration until the process completes. You can then choose to export a log of the analyzation or migration as a report by clicking **Export Log File**.

Figure 21 Migrate Operation Results dialog



Policy migration to vProxy by using the command line

You can also migrate VMware Backup appliance policies and workflows to vProxy by using the `nsrvbaupgrade` command line utility, which additionally allows you to

perform a pre-migration check before migrating. The command line supports multiple policies for each run.

Before you begin

To perform a pre-check only before migrating, run `nsrvbaupgrade -c`. It is recommended that you resolve any pre-check errors, including unsupported software versions, before completing the migration in order for backups to complete successfully.

Procedure

1. Open a command prompt.
2. Specify the `nsrvbaupgrade` command in the following format:

   `nsrvbaupgrade -p` *policy* `[-c] [-f] [-v]` where:

   - -p *policy* specifies one or more policies to migrate
   - -c runs the pre-check only
   - -f forces the migration to ignore a pre-check failure
   - -v specifies verbose mode

Co-existence of the VMware Backup appliance and vProxy appliance

After upgrading to a NetWorker 9.1.x or 9.2 release and migrating from the VMware Backup appliance to the vProxy appliance, you might still require the VMware Backup appliance. For example, if you want to recover from a backup performed with the VMware Backup appliance that has not expired, you must keep the VMware Backup appliance and at least one of the VMware Backup appliance's external proxies.

If you plan to continue using the VMware Backup appliance, make note of the following information:

- NetWorker 9.1 and later releases require the same version of the VMware Backup appliance as NetWorker 9.0.1, which is 1.5.1.7. If you are upgrading from NetWorker 9.0.1, you do not need to upgrade the VMware Backup appliance version. If you are upgrading from an earlier release, for example, from NetWorker 8.2.3 with version 1.1.3.7, you will need to upgrade the VMware Backup appliance version to 1.5.1.7 after upgrading the NetWorker server to 9.1 and later.
- Backups run with VMware Backup appliance policies cannot be recovered using the vProxy appliance. These backups must be recovered with the VMware Backup appliance.
- You cannot create new policies with the VMware Backup appliance. You can only run or edit existing policies.
- You cannot run policies with VMware Backup appliance GSAN internal storage.
- Different plug-ins are available in the vSphere Web Client for VMware Backup appliance policies and vProxy appliance policies. For the VMware Backup appliance, this is the **EMC Backup and Recovery** plug-in. For the vProxy appliance, this is the **VM Backup and Recovery** plug-in. The two plug-ins can co-exist on the same vCenter.

It is recommended to migrate all VMware Backup appliance policies to the vProxy appliance. Note that you can still use the **EMC Backup and Recovery** plug-in within the **vSphere Web Client** for operations that are related to the backup of still-to-be migrated VMware Backup appliance policies, or for image-level recovery of any backups performed with the VMware Backup appliance. However, after a policy has been migrated to the vProxy appliance, it is no longer accessible from the VMware

Backup appliance. You must manage all such migrated policies as native NetWorker vProxy policies from NMC, or by using the **VM Backup and Recovery** plug-in within the **vSphere Web Client** for NetWorker 9.1 and later vProxy-based policies.

Additionally, for file-level recovery in the **EMC Data Protection Restore Client**, you must use vProxy appliance backups after migrating. Recovery from older backups that were created using the VMware Backup appliance can still be performed using the **EMC Backup and Recovery** plug-in, but you must retain at least one external proxy node.

The following table provides a list of supported and unsupported VMware Backup appliance operations in an upgraded NetWorker 9.1 and later environment.

Table 7 Supported and unsupported VMware Backup appliance operations in a NetWorker 9.1 and later environment

Supported operations	Unsupported operations
• Scheduled backups of VMware Backup appliance policies that were created before upgrading to NetWorker 9.1 or 9.2 • On demand (adhoc) backups of virtual machines protected by a VMware Backup appliance from NMC's **Protection** window • On demand (adhoc) backups of virtual machines protected by a VMware Backup appliance from the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Edit existing VMware Backup appliance protection policies (for example, to modify an existing action to point to a different VMware Backup appliance) • Modify the VMware Backup appliance protection group to add virtual machines to an existing group or remove virtual machines from an existing group • Image-level recovery (to a new virtual machine, revert, VMDK-level and instant access) from VMware Backup appliance backups run before or after the upgrade by using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • File-level recovery from VMware Backup appliance backups run before or after the upgrade by using the **Dell EMC Data Protection Restore Client** (VBA) • Emergency restore from VMware Backup appliance backups run before or after the upgrade • Create checkpoints after the upgrade by running an integrity check using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Rollback to a desired checkpoint (to checkpoints taken after the upgrade) • Deploy and manage VMware Backup appliance external proxies after the upgrade by selecting a desired VMware Backup appliance	• Create new VMware Backup appliance protection policies • Image-level recovery of VMware Backup appliance backups by using the **VM Backup and Recovery** plug-in in the **vSphere Web Client** • Image-level recovery of VMware Backup appliance backups by using the NMC **Recovery** wizard • File-level recovery from VMware Backup appliance backups by using the NMC **Recovery** wizard • File-level recovery from VMware Backup appliance backups by using the **Dell EMC Data Protection Restore Client** (vProxy) • Manage VMware Backup appliance policies by using the **VM Backup and Recovery** plug-in in the **vSphere Web Client** • Manage vProxy policies by using the **VM Backup and Recovery** plug-in in the **vSphere Web Client**

Table 7 Supported and unsupported VMware Backup appliance operations in a NetWorker 9.1 and later environment

Supported operations	Unsupported operations
• Resurrect VMware Backup appliance backups run before or after the upgrade by using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Disaster recovery of VMware Backup appliance in case of a VMware Backup appliance failure • Restore to the same vCenter with a newly deployed VMware Backup appliance by using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client** • Recovery of VMware Backup appliance backups from a secondary site (restore to a different vCenter) with a newly deployed VMware Backup appliance by using the **EMC Backup and Recovery** plug-in in the **vSphere Web Client**	

NetWorker support for CloudBoost 2.2

A NetWorker with CloudBoost environment can extend onsite data protection to the cloud with the following solutions:

- Backup to the cloud.
- Backup to cloud directly with NetWorker Linux 64-bit and Windows x64-bit client.
- External storage node configuration support for NetWorker Linux 64-bit and Windows x64-bit clients.
- Backup in the cloud by using Amazon EC2 and Amazon S3.
- Backup in the cloud by using Microsoft Azure and Microsoft Azure Blob Storage.

Direct back up to the cloud with Linux and Windows clients

This use case is intended for when you have onsite infrastructure and want to use object storage for all backup workloads, including short-term backups for operational recovery and long-term backups for compliance.

The optional site cache reduces the impact of long-distance connectivity. The optional site cache also meets recovery-time objectives more quickly, because the most frequently used data is cached locally.

Direct backup to the cloud is recommended for the following use cases:

- Where a high bandwidth pipe to the object store is required.
- When backing up to a local ECS.
- When backing up non-critical applications that can tolerate a higher SLA for backup and restore operations.

This figure displays Linux and Windows clients that are directly backed up to the cloud.

Figure 22 Clients backed up directly to the cloud

For clients that cannot back up directly to the cloud, you can send backups through the CloudBoost appliance or an external NetWorker storage node to the cloud. However, routing through either the CloudBoost appliance or the NetWorker storage node limits performance. Having the data path go directly from the client to the cloud is the most scalable, efficient, and optimal performance deployment model.

Backup a Microsoft Azure virtual machine data to Azure blob storage

This use case is intended for workloads that run in the public cloud and use Microsoft Azure blob storage for backups, including short-term backups for operational recovery and long-term retention backups for compliance.

You use the same NetWorker tools to manage both onsite and cloud-based data protection processes.

The following figure displays back up Microsoft Azure blob storage.

Figure 23 Back up to Microsoft Azure

The optional site cache service is unavailable when you deploy the appliance within Microsoft Azure.

CloudBoost Virtual appliance on Amazon Web Services

NetWorker features support for the CloudBoost Virtual appliance on Amazon Web Services to backup and clone data.

By utilizing a virtual machine that is Amazon Machine Image (AMI) compatible, the CloudBoost Virtual appliance supports both long-term retention and backup to cloud, allowing you to benefit from Amazon's Simple Storage Service (S3) deduplication.

Backup Amazon EC2 data to Amazon S3 storage

This use case is intended for workloads that run in public clouds and use S3 cloud object storage for backups, including short term backups for operational recovery and long term retention backups for compliance.

The following figure displays back up in Amazon EC2 to Amazon S3 storage.

Figure 24 Back up in Amazon EC2 to Amazon S3 storage

The optional site cache service is unavailable when you deploy the appliance within Amazon EC2.

Enhancements to Data Domain support

NetWorker includes the following Data Domain related enhancements.

Data Domain Retention Lock

The Data Domain Retention Lock (DD Retention Lock) feature within NetWorker allows you to efficiently manage and store different types of data backed up by NetWorker to a single Data Domain system by securely locking the data on that system, preventing accidental deletion of save sets.

When you enable a DD Boost device Mtree with DD Retention Lock in the NetWorker Management Console (NMC) **NetWorker Administration** window, and apply the DD Retention Lock to the data protection policy action, the save sets backed up by the NetWorker policy cannot be overwritten, modified, or deleted for the duration of the retention period, up to a maximum of 70 years. Additionally, the device cannot be removed or relabeled at any time during the retention period, though the device that contains the retention lock save sets can be mounted and unmounted. The secure

locking of data occurs at an individual file level, and locked files can co-exist with unlocked files on the same Data Domain system.

With DD Retention Lock, you can set the retention time to meet the requirements driven by governance policies. The **DD Retention Lock Time** specified at the save set level must fall within the range of the minimum and maximum retention times configured on the DD Boost Mtree during device creation.

You can enable DD Retention Lock on the DD Boost Mtree during device configuration, or by modifying the device properties after configuration. If using the NMC **Device Configuration** wizard for the first instance of Data Domain device configuration, ensure that you populate the Data Domain device management credentials (Management host, Management user name, management password and management port).

When you enable DD Retention Lock at the device level, you must additionally apply DD Retention Lock to the data protection policy action so that data is backed up with retention lock set.

After successful backup, save set queries in the **Media** window of **NetWorker Administration** displays **DD Retention Lock Period** and **DD Retention Lock Type** columns to indicate which save sets have retention lock enabled and provide the retention lock expiry date and time. If these columns are not initially visible, you can customize the view to include this information. This information is also available within the **NMC Enterprise Reports** window, under **Policy Statistics** > **Save Set Details**. Similarly, if these columns are not initially visible, you can customize the view to include this information.

Backup direct to Data Domain Virtual Edition

NetWorker 9.2 supports backup direct to Data Domain Virtual Edition (DDVE), allowing you to deploy DDVE in Amazon Web Services (AWS) for Windows and Linux instances.

Data Domain Cloud Tier

The Data Domain Cloud Tier (DD Cloud Tier) is a long term data retention solution that enables the movement of data from an Data Domain Active Tier (DD Active Tier) device to a DD Cloud Tier device, and then to an external Cloud Provider.

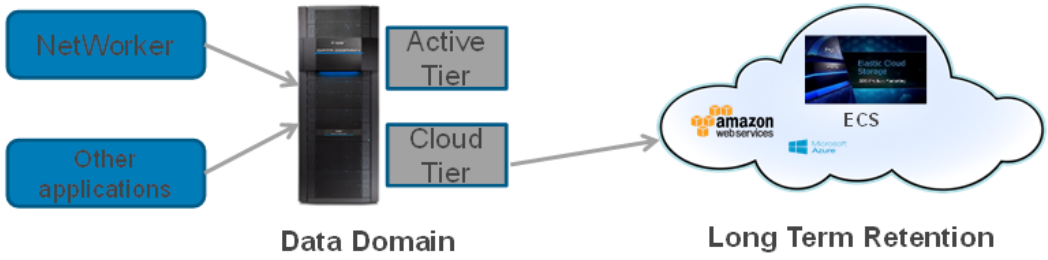
The NetWorker integration with the DD Cloud Tier provides a Data Protection Administrator with the ability to perform the following functions:

- Ability to clone data from a DD Active Tier device to a DD Cloud Tier device.
- Track individual client data that is stored in the cloud or on-premise.
- Recover data to a client from the cloud, including FLR/GLR recoveries.

NetWorker supports the following Cloud services, for long term retention in this release: Amazon web services (AWS), Elastic Cloud Storage™ (ECS™), and Microsoft® Azure®

The following diagram provides an overview of the DD Cloud Tier solution.

Figure 25 DD Cloud Tier solution



Data Domain High Availability support

NetWorker 9.1 and later supports highly available Data Domain systems.

To configure alerts for the following Data Domain high availability events, during Data Domain device setup, select the following options from the **Device Configuration Wizard** > **SNMP Monitoring Options** page:

- HA Setup Degraded
- HA Setup Offline
- HA Setup Out-of-Sync

When a highly available Data Domain system fails over to its standby highly available Data Domain system, NMC displays event messages. All in-progress NetWorker operations including backup, clone, and recover operations are unaffected, except for a temporary freeze of operations for a few minutes. However, during unusually long freezes, for example over ten minutes, some NetWorker operations might fail but are automatically retried. Some failed NetWorker operations might require a manual restart.

If interrupted by a failover NFS, VTL, and CIFS jobs fail. You must configure NetWorker policies to restart or resume the failed jobs. You can manually restart the failed jobs as soon as the failover completes. The failed jobs will not restart or resume on their own.

Note

To view events in NMC, clear all alerts on the Data Domain system. For example, in the Data Domain UI, select **Alerts** > **Current Alerts** > **Select All** > **Clear**.

Improved performance of NetWorker Clone Controlled Replication (CCR) for Data Domain due to Automated Multi-streaming

The Automated Multi-streaming (AMS) feature improves cloning performance for large save sets when you use high bandwidth networks. Previously when you replicated save sets between two Data Domain devices on different machines, the replication process used to take longer in NetWorker. AMS significantly speeds up replication between DDRs by splitting up large files (files whose sizes are roughly greater than 3.5 GB) into multiple smaller 2 GB slices, replicating the slices individually, and finally re-creating the original large file on the destination DDR using those slices.

NetWorker features enhancements to clone controlled replication (CCR), also known as DD to DD Managed File Replication. Also, enhancements to load balancing so that the load (save sets to clone) is spread evenly across the multi-threaded `nsrclone`

process were implemented. By default, the AMS feature is disabled. You can turn on the feature by changing the command to *ams_enabled=yes*.

DDOS version 5.7.x high availability failover capabilities

NetWorker allows you to make use of the Data Domain failover capabilities available in DDOS 5.7.x for both DD Boost and non-Boost devices, introducing the following enhancements:

- View status information and reports from NMC's **Monitoring** window.
- In the result of a failover, perform an unscheduled shutdown of the primary Data Domain device to ensure that NetWorker operations in progress (including backup, recovery and configuration options) are not interrupted.

Note

If you run an `inquire` during a Data Domain failover, the VTL output does not display. There is, however, no impact to the backup.

Support for DD Boost Fibre Channel on Solaris 10 and 11

DD Boost Fibre Channel now supports Solaris versions 10 and 11 for the File System Client.

Enhancements to Snapshot management

NetWorker includes the following snapshot management related enhancements.

SmartSnap for centralized snapshot management

NetWorker 9.1 allows you to backup and restore VMAX devices using a device worldwide name (WWN).

The SmartSnap feature enables centralized snapshot management and snapshot support for operating system platforms where traditional NetWorker Snapshot Management (NSM) is not supported. The backup component of this feature is supported by the NMC Client Configuration wizard when you select the **SmartSnap** option from the **Available applications**, and then select the **Snapshot** checkbox. Restore is supported at the array device level.

Rollback to an alternate location

NetWorker 9.1 allows you to perform an array level restore (rollback) of a snapshot to an alternate set of devices.

You can pre-select the device. The devices should be of the same size or larger than the original source devices and should be visible to an alternate host. You must create the same file systems that were on the source devices.

ProtectPoint

NetWorker introduces support for the ProtectPoint solution, which allows for Data Domain vDisk snapshot creation within NetWorker's policy workflow. You can specify a snapshot backup type ProtectPoint Snapshot, where NetWorker creates the

snapshot of specified files on the application host and retains the snapshot on the Data Domain system only.

The ProtectPoint solution integrates primary storage on an VMAX3 array and protection storage for backups on a Data Domain system. ProtectPoint provides block movement of the data on application source LUNs to encapsulated Data Domain LUNs for full and incremental backups.

ProtectPoint operations require the following:

- Both IP network (LAN or WAN) and Fibre Channel (FC) storage area network (SAN) connectivity.
- A VMAX3 array with SnapVX and Federated Tiered Storage (FTS) software features enabled.
- Solutions Enabler 8.0.1 installed on the application host, data mover, optionally the recovery host and in some configurations on the NetWorker server.
- Data Domain systems (DD4500, DD7200, DD990) with the Data Domain Operating System (DDOS) 5.6 installed, with Vdisk service and DD Boost service enabled.

Note

NetWorker supports the backup of Oracle, SAP oracle, and DB2 databases using the ProtectPoint Workflow. Backup of file systems is not supported.

The *NetWorker Snapshot Management Integration Guide* provides details for configuring ProtectPoint.

NetWorker support in the vRealize Data Protection Extension

The vRealize Data Protection Extension version 4.0 features support for data protection (backup and recovery operations) on NetWorker 9.1. In previous releases, data protection was only available for Avamar systems.

vRealize data protection for NetWorker consists of the following:

- Image level data protection, which backups virtual machines at the disk level.
- Image level recovery, to recover virtual machines to the original location or a new location.
- File level restore using the Data Protection Restore Client.

The following limitations apply to NetWorker data protection support:

- Restore from a deleted virtual machine is not supported.
- Networker does not support multi-tenancy for VMware data protection. Multi-tenancy can be supported with vRA by assigning/dedicating one Networker instance per tenant.

Note

With the vRealize Data Protection Extension, the management of data protection is integrated into the standard vRealize Automation workflow. Service Level Agreements (SLAs) seamlessly enable data protection in the cloud. The applications are protected automatically when you enable data protection.

Enhancements to parallel save streams and client parallelism settings

NetWorker enhancements to parallel save streams (PSS) provide additional backup performance gains for concurrent backup that is compared to previous NetWorker releases.

In NetWorker 9.0 and later, the NetWorker server starts a single save process per PSS-enabled client, with all client save sets passed to the single process for processing optimizations. Enhancements to PSS in NetWorker include:

- Four parallel streams started per save set, subject to any client parallelism limitations that might prevent all save sets from starting simultaneously.

  Note

  PSS and non-PSS backups currently ignore the policy workflow action's parallelism, previously known as the savegrp parallelism, and use the client parallelism value instead.

- The ability to modify the number of parallel streams per save set by defining the new **PSS:streams_per_ss** option in the selected Client resource's **save operations** attribute.
- Automatic stream reclaiming, which dynamically increases the number of active streams for an already running save set backup to maximize utilization of limited client parallelism conditions, also known as Dynamic PSS (or DPSS).

  Note

  The term DPSS can also refer to the overall enhancements to PSS in NetWorker 9.0 and later.

- Performance gains for environments with a limited client parallelism, multiple save sets for concurrent backup, and significantly unbalanced save set sizes. A save set is a save point such as a Windows volume, UNIX file system mount point directory, or a Windows or UNIX directory.

Due to differences in the handling of save streams, the recommended value for client parallelism in NetWorker 9.0 and later has changed.

In NetWorker 8.2.x and earlier, PSS requires a sufficiently high client parallelism value due to the up-front static division of client parallelism among the client's save points which all get started at the same time.

In NetWorker 9.0 and later the save points are scheduled at four parallel save streams each by default, and handled in batches according to the client parallelism value. Therefore, you do not require a high value for client parallelism. For a single save set, you can obtain the best backup throughput at a configurable 4-8 parallel streams per save set.

Note

PSS is not supported for checkpoint restart backups in NetWorker 9.1.

Block based backup on Linux platforms

Block based backup (BBB) is a NetWorker solution that facilitates the backup of data by scanning a volume or a disk in a file system, and backing up all the blocks that are in use in the file system.

BBB uses the Change Block Tracking (CBT) driver to identify the changed blocks, and back up only the changed blocks. Previously, this backup option was only available on Windows. In NetWorker 9.0 and later, Linux platforms can also use BBB.

On a Windows host, the NetWorker client software includes support for BBB. On Linux hosts, install the BBB software package to provide a NetWorker client with BBB support. The BBB software package for installation is `lgtobbb-9.1.x86_64.rpm`.

NetWorker Virtual Edition

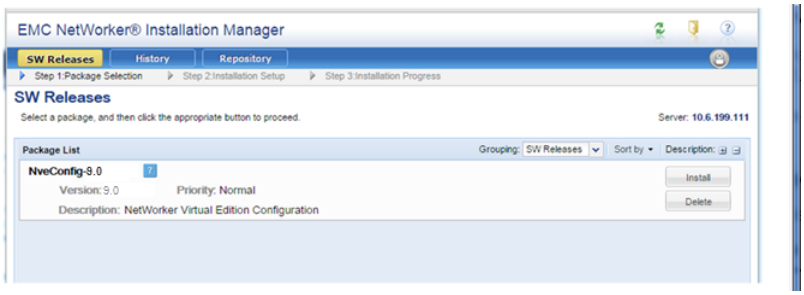
The NetWorker Virtual Edition (NVE), introduced in NetWorker 9.0, is a self-contained virtual appliance for VMware that integrates the latest version of the NetWorker server software with SUSE Linux as a VMware virtual machine.

The NVE appliance, compatible with vSphere versions 5.1 and later, is delivered as an OVA file that you deploy through the vCenter server.

After deployment and completing the configuration, run the **NetWorker Installation Manager** from a web browser to complete the NVE setup. To access the **NetWorker Installation Manager**, type a link in the following format:

`https://<NVE_address>:7543/avi/avigui.html`

Figure 26 NetWorker Installation Manager



The *NetWorker Virtual Edition Installation Guide* provides more information.

NOTICE

Only new installations of NetWorker 9.0 and later can use NVE. If you upgrade to NetWorker 9.0 and later from a NetWorker 8.2.x and earlier release, NVE will not be available.

Restricted Data Zone changes

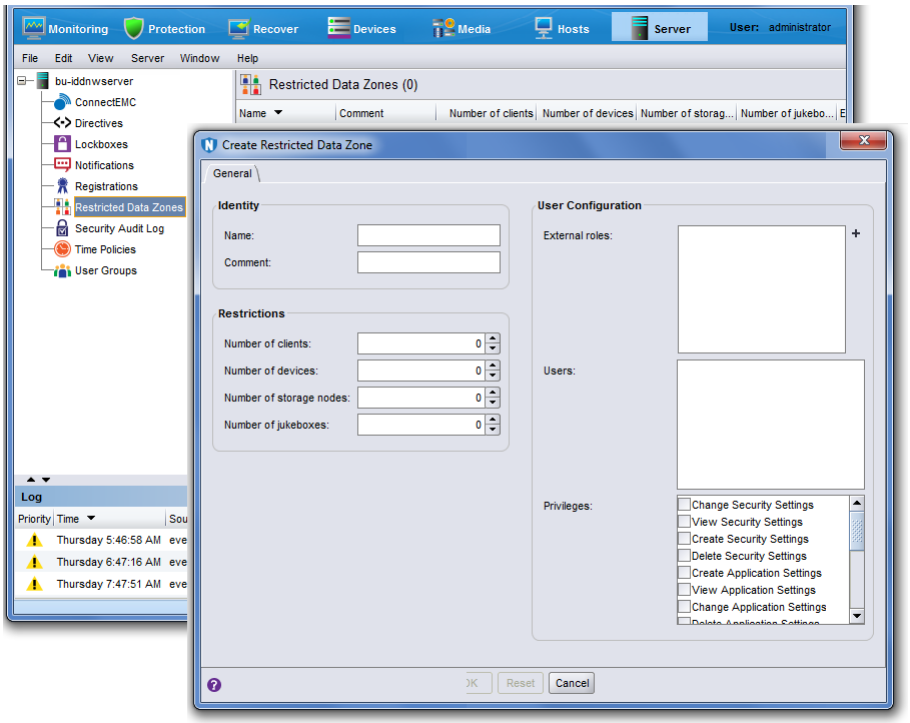
The Restricted Data Zone (RDZ) feature provides NetWorker administrators with an additional layer of privilege control that allows you to isolate access to resources, and separate these resources into specific groups.

NetWorker 9.0 and later releases feature the following changes to RDZ:

- You can now associate an RDZ resource to an individual resource (for example, to a client, protection policy, protection group, and so on) from the resource itself. As a result, RDZ resources can no longer affect resource associations directly.
- Non-default resources that are previously associated to the global zone, and therefore unusable by an RDZ, are now shared resources that can be used by an RDZ. Although, these resources cannot be modified by restricted administrators.

Also, RDZ setup in the NMC GUI's **Administration** window is now located under the **Server** window, as shown in the following:

Figure 27 Create Restricted Data Zone in the Server window



Changes to NetWorker and Avamar integration

Beginning with NetWorker version 9.0, Avamar integration support is deprecated for new clients. However, older integrations continue to be supported, with the following considerations.

Considerations for installing the Avamar Client in NetWorker 9.0 and later

You can continue to install the Avamar client with NetWorker 9.0 and later. Installation of the Avamar client is not required until you want to recover data from backups performed to Avamar deduplication nodes. You can use either of the following methods to install the Avamar client:

- Install the Avamar client as part of the update to NetWorker 9.0 and later by using the WIX installer or UNIX package deployment.

Note

As of NetWorker 9.0.1, the Avamar client is no longer selected by default during the NetWorker install or upgrade. You must manually select the Avamar client in the Wizard options (WIX installer), or manually install the RPM package appropriate to your platform.

- After upgrading to NetWorker 9.0 and later, install the Avamar client package. The package names are `AvamarClient-windows-x86_64-7.2.100-401.msi` on Windows, `AvamarClient-linux-sles11-x86_64-7.2.100-401.rpm` on SuSE Linux Enterprise Server (SLES) version 11, `AvamarClient-linux-rhel4-x86_64-7.2.100-401.rpm` on Red Heat Enterprise Linux, and `AvamarClient-debian4.0-x86_64-7.2.100-401.deb` on Debian.

  Note

  The NetWorker client no longer supports RedHat 4.0. You can still install Avamar 7.0 on RedHat 4.0, but if you install the NetWorker 9.0 and later client package on an Avamar server that is on RedHat 4.0, the installation fails. In this case, leave the current NetWorker client version as is. You can still upgrade the NetWorker server and NetWorker deduplication client to NetWorker 9.0 and later and continue performing backup and recovery using the Avamar server with a pre-NetWorker 9.0 client package installed.

When you install the Avamar client using either of these methods, make note of the following considerations:

- If you install the Avamar client during an upgrade to NetWorker 9.0 and later, you must activate the Avamar client with the Avamar server/deduplication node to ensure that the Avamar server can communicate with the Avamar client.
- After you upgrade the NetWorker server to version 9.0 and later, Avamar clients previous to NetWorker 9.0 can continue to perform deduplication backup and recovery.
- If the NetWorker server and the NetWorker client are the same hosts, and you upgrade to NetWorker 9.0 and later, then install the Avamar client to perform deduplication backups and recoveries.
- After you upgrade the NetWorker server to version 9.0 and later, you cannot configure a new Avamar deduplication node. As a result, you cannot configure any new NetWorker clients with deduplication enabled.
- Install the NetWorker client rpm on the Avamar server node. Do not install the Avamar client package on the Avamar node.
- This solution does not support IPv6.
- Avamar version 7.2 uses an encrypted port 29000 as the default port, as a result, the NetWorker and Avamar deduplication backup fails. Set the port to an unencrypted port 27000, for the NetWorker and Avamar deduplication to backup correctly. To make this port change, perform the following steps:

  1. On the Avamar server, create a file that is named `gsan-port` under the directory `/usr/local/avamar/lib/admin/security/` with the content as follows:

     ```
     <avamar server hostname>:~/#: cat /usr/local/avamar/lib/admin/
     security/gsan-port GSAN_PLAIN_TEXT="27000,"
     ```

  2. Type the following command to restart the Avamar firewall:

     ```
     service avfirewall stop
     service avfirewall start
     ```

  3. Type the following command to restart NetWorker:

     ```
     /etc/init.d/networker stop
     /etc/init.d/networker start
     ```

Existing users of this feature

Existing customers using this feature can continue to refer to the *NetWorker and Avamar Integration Guide* version 8.2 Service Pack 1.

The NetWorker software installation packages includes the Avamar client software. The Avamar client software only provides support to NetWorker hosts that used an Avamar system as a data protection target with a previous release of NetWorker. You can only install the Avamar client software when you upgrade a NetWorker 8.2.x and earlier host. The *NetWorker Updating from a Previous Release Guide* provides more information.

Copyright © 2015-2017 Dell Inc. and its subsidiaries. All rights reserved.

Published July 28, 2017

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be the property of their respective owners. Published in the USA.