# CONTENTS

<table>
<thead>
<tr>
<th>Figures</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td>7</td>
</tr>
<tr>
<td>Chapter 1</td>
<td><strong>Introduction</strong></td>
</tr>
<tr>
<td></td>
<td>Overview of NetWorker Virtual Edition</td>
</tr>
<tr>
<td>Chapter 2</td>
<td><strong>Deployment and Update</strong></td>
</tr>
<tr>
<td></td>
<td>Predeployment requirements and best practices</td>
</tr>
<tr>
<td></td>
<td>System requirements</td>
</tr>
<tr>
<td></td>
<td>Verifying the DNS configuration</td>
</tr>
<tr>
<td></td>
<td>NVE virtual disk requirements</td>
</tr>
<tr>
<td></td>
<td>Network requirements</td>
</tr>
<tr>
<td></td>
<td>Virtual disk configuration best practices</td>
</tr>
<tr>
<td></td>
<td>Deployment</td>
</tr>
<tr>
<td></td>
<td>Deploying the appliance</td>
</tr>
<tr>
<td></td>
<td>Setting up the NetWorker software on NVE</td>
</tr>
<tr>
<td></td>
<td>Starting the NMC server GUI for the first time</td>
</tr>
<tr>
<td></td>
<td>About the EMC Licensing Solution</td>
</tr>
<tr>
<td></td>
<td>Configuring sendmail and NetWorker notifications</td>
</tr>
<tr>
<td></td>
<td>Upgrading</td>
</tr>
<tr>
<td>Chapter 3</td>
<td><strong>Maintenance</strong></td>
</tr>
<tr>
<td></td>
<td>Password maintenance</td>
</tr>
<tr>
<td></td>
<td>Reviewing password policies</td>
</tr>
<tr>
<td></td>
<td>Modifying passwords</td>
</tr>
</tbody>
</table>
## FIGURES

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Select source page</td>
<td>16</td>
</tr>
<tr>
<td>2</td>
<td>Review details page</td>
<td>17</td>
</tr>
<tr>
<td>3</td>
<td>End User License Agreement page</td>
<td>17</td>
</tr>
<tr>
<td>4</td>
<td>Name and Location page</td>
<td>18</td>
</tr>
<tr>
<td>5</td>
<td>Select a resource page</td>
<td>18</td>
</tr>
<tr>
<td>6</td>
<td>Select storage page</td>
<td>19</td>
</tr>
<tr>
<td>7</td>
<td>Setup networks page</td>
<td>19</td>
</tr>
<tr>
<td>8</td>
<td>Customize templates page</td>
<td>20</td>
</tr>
<tr>
<td>9</td>
<td>Recent Tasks</td>
<td>20</td>
</tr>
<tr>
<td>10</td>
<td>Associating a jnlp file with Java (TM) web Start Launcher for Mozilla Firefox</td>
<td>25</td>
</tr>
</tbody>
</table>
As part of an effort to improve its product lines, EMC periodically releases revisions of its software and hardware. Therefore, some functions described in this document might not be supported by all versions of the software or hardware currently in use. The product release notes provide the most up-to-date information on product features.

Contact your EMC technical support professional if a product does not function properly or does not function as described in this document.

Note
This document was accurate at publication time. Go to EMC Online Support (https://support.emc.com) to ensure that you are using the latest version of this document.

Purpose
This document describes how to set up NetWorker Virtual Edition in a NetWorker environment.

Audience
This guide is part of the NetWorker documentation set, and is intended for use by system administrators during the installation and setup of the NetWorker software.

Revision history
The following table presents the revision history of this document.

Table 1 Revision history

<table>
<thead>
<tr>
<th>Revision</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>September 24, 2015</td>
<td>First release of this document for EMC NetWorker 9.0</td>
</tr>
<tr>
<td>02</td>
<td>October 23, 2015</td>
<td>Revised section Network requirements to indicate ports that are required for communication with the EMC License Server</td>
</tr>
<tr>
<td>03</td>
<td>November 12, 2015</td>
<td>Updates to the sections Preparing the virtual machine and Setting up the NetWorker software on NVE</td>
</tr>
<tr>
<td>04</td>
<td>December 16, 2015</td>
<td>Updates to the section Setting up the NetWorker software on NVE</td>
</tr>
<tr>
<td>05</td>
<td>April 15, 2016</td>
<td>Updates to the Updating section</td>
</tr>
<tr>
<td>06</td>
<td>June 29, 2016</td>
<td>Updates to include information about the NetWorker 9.0.1 release</td>
</tr>
<tr>
<td>07</td>
<td>November 10, 2016</td>
<td>Various updates to the guide including updates to the installation and configuration sections, information about how to configure sendmail and details about the licensing sever.</td>
</tr>
</tbody>
</table>

Related documentation
The NetWorker documentation set includes the following publications, available on EMC Online Support:
- **EMC NetWorker Online Software Compatibility Guide**  
  Provides a list of client, server, and storage node operating systems supported by the EMC information protection software versions. You can access the guide at [https://support.emc.com](https://support.emc.com). From the Support by Product pages, search for NetWorker using "Find a Product", and then select the Install, License, and Configure link.

- **EMC NetWorker Administration Guide**  
  Describes how to configure and maintain the NetWorker software.

- **EMC NetWorker Network Data Management Protocol (NDMP) User Guide**  
  Describes how to use the NetWorker software to provide data protection for NDMP filers.

- **EMC NetWorker Cluster Integration Guide**  
  Contains information related to configuring NetWorker software on cluster servers and clients.

- **EMC NetWorker Installation Guide**  
  Provides information on how to install, uninstall, and update the NetWorker software for clients, storage nodes, and servers on all supported operating systems.

- **EMC NetWorker Updating from a Previous Release Guide**  
  Describes how to update the NetWorker software from a previously installed release.

- **EMC NetWorker Release Notes**  
  Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.

- **EMC NetWorker Command Reference Guide**  
  Provides reference information for NetWorker commands and options.

- **EMC NetWorker Data Domain Boost Integration Guide**  
  Provides planning and configuration information on the use of Data Domain devices for data deduplication backup and storage in a NetWorker environment.

- **EMC NetWorker Performance Optimization Planning Guide**  
  Contains basic performance tuning information for NetWorker.

- **EMC NetWorker Server Disaster Recovery and Availability Best Practices Guide**  
  Describes how to design and plan for a NetWorker disaster recovery. However, it does not provide detailed disaster recovery instructions. The Disaster Recovery section of the NetWorker Procedure Generator (NPG) provides step-by-step disaster recovery instructions.

- **EMC NetWorker Snapshot Management Integration Guide**  
  Describes the ability to catalog and manage snapshot copies of production data that are created by using mirror technologies on EMC storage arrays.

- **EMC NetWorker Snapshot Management for NAS Devices Integration Guide**  
  Describes how to catalog and manage snapshot copies of production data that are created by using replication technologies on NAS devices.

- **EMC NetWorker VMware Integration Guide**  
  Provides planning and configuration information on the use of VMware in a NetWorker environment.

- **EMC NetWorker Error Message Guide**  
  Provides information on common NetWorker error messages.

- **EMC NetWorker Licensing Guide**  
  Provides information about licensing NetWorker products and features.
EMC NetWorker REST API Getting Started Guide
Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.

EMC NetWorker REST API Reference Guide
Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.

EMC NetWorker Management Console Online Help
Describes the day-to-day administration tasks performed in the NetWorker Management Console and the NetWorker Administration window. To view the online help, click Help in the main menu.

EMC NetWorker User Online Help
Describes how to use the NetWorker User program, which is the Windows client interface, to connect to a NetWorker server to back up, recover, archive, and retrieve files over a network.

Special notice conventions that are used in this document
EMC uses the following conventions for special notices:

**NOTICE**
Identifies content that warns of potential business or data loss.

---

**Note**
Contains information that is incidental, but not essential, to the topic.

Typographical conventions
EMC uses the following type style conventions in this document:

**Table 2 Style conventions**

**Bold**
Used for names of interface elements, such as names of buttons, fields, tab names, and menu paths (what the user specifically selects or clicks)

**Italic**
Used for full titles of publications that are referenced in text

**Monospace**
Used for:
- System code
- System output, such as an error message or script
- Pathnames, file names, prompts, and syntax
- Commands and options

**Monospace italic**
Used for variables

**Monospace bold**
Used for user input

[ ]
Square brackets enclose optional values

| |
Vertical bar indicates alternate selections - the bar means “or”

{} 
Braces enclose content that the user must specify, such as x or y or z

...
Ellipses indicate non-essential information that is omitted from the example
Where to get help
EMC support, product, and licensing information can be obtained as follows:

Product information
For documentation, release notes, software updates, or information about EMC products, go to EMC Online Support at https://support.emc.com.

Technical support
Go to EMC Online Support and click Service Center. Several options for contacting EMC Technical Support appear on the site. Note that to open a service request, you must have a valid support agreement. Contact your EMC sales representative for details about obtaining a valid support agreement or with questions about your account.

Online communities
Go to EMC Community Network at https://community.emc.com for peer contacts, conversations, and content on product support and solutions. Interactively engage online with customers, partners, and certified professionals for all EMC products.

Your comments
Your suggestions help to improve the accuracy, organization, and overall quality of the user publications. Send your opinions of this document to DPAD.Doc.Feedback@emc.com.
CHAPTER 1

Introduction

This chapter includes the following topics:

- Overview of NetWorker Virtual Edition

12
Overview of NetWorker Virtual Edition

EMC® NetWorker® Virtual Edition (NVE) is a NetWorker server that runs as a virtual machine in a VMware environment. NVE integrates the latest version of the NetWorker software with SUSE Linux as a VMware virtual machine. NVE is available as a 250 GB virtual appliance.

Note

Only new installations of NetWorker 9.0.x can use NVE. If you upgrade to NetWorker 9.0.x from an 8.2.x or earlier NetWorker release, NVE will not be available.
CHAPTER 2

Deployment and Update

This chapter includes the following topics:

- Predeployment requirements and best practices ................................................ 14
- Deployment ........................................................................................................ 15
- Upgrading ........................................................................................................... 33
Predeployment requirements and best practices

Before you deploy an NVE virtual machine, review the predeployment requirements and best practices in the following sections.

**Note**

NVE does not support migration of data from another instance of NetWorker.

System requirements

Networker Virtual Edition (NVE) is supported on VMware ESXi 5.1/5.5/5.5u2/6.0. The following table defines the minimum system requirements for each size of NVE.

**Table 3 Minimum requirements for NVE**

<table>
<thead>
<tr>
<th>System object</th>
<th>250 GB NVE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processors</td>
<td>Minimum four 2 GHz processors</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>Disk space</td>
<td>600 GB</td>
</tr>
<tr>
<td>Network connection</td>
<td>1 GbE connection</td>
</tr>
</tbody>
</table>

Verifying the DNS configuration

Before you deploy the NVE, ensure that name resolution is properly configured. Failure to have DNS set up properly can cause runtime or configuration issues.

**Procedure**

1. Open a command prompt on the vCenter Server and type the following command:
   
   `nslookup NVE_IP_address DNS_Server_IP_address`

   When name resolution is properly configured, the `nslookup` command will return the FQDN for NVE.

2. Type the following command:
   
   `nslookup NVE_FQDN DNS_Server_IP_address`

   When name resolution is properly configured, the `nslookup` command will return the IP address for NVE.

3. Type the following command:
   
   `nslookup FQDN_of_vCenter DNS_Server_IP_address`

   When name resolution is properly configured, the `nslookup` command returns the IP address of the vCenter Server.

4. If the `nslookup` commands returned the proper information, close the command prompt. If the `nslookup` commands do not return proper information, resolve the DNS configuration before you install NVE.
NVE virtual disk requirements

The NVE disk layout comprises one operating system disk (256 GB) and one storage partition (250 GB).

Network requirements

Before you deploy NVE, gather the following information:

- Hostnames and IP addresses for the NVE virtual machine and the DNS Server
- Gateway, netmask, and domain of the NVE virtual machine
- Firewall openings, if applicable. NetWorker requires ports 27000, 27010, and 51000 to communicate with the EMC License Server. Ensure that these ports remain open only for this purpose. *EMC NetWorker Security Configuration Guide* provides more information about firewall port requirements

Virtual disk configuration best practices

ESXi supports multiple disk formats. For NVE virtual machines, the initial configuration is Thick Provision Lazy Zeroed.

- NVE does not support thin provisioning.

After the initial installation, if you configure the virtual disks for the Thick Provision Eager Zeroed, the customer will get better initial performance because the first write to the disk will require less operations.

- See the VMware documentation for information on converting Lazy zeroed virtual disks to Eager zeroed virtual disks. Converting a disk from Thick Provisioned Lazy Zeroed to Thick Provisioned Eager Zeroed is time consuming and can consume a significant number of storage I/O processes.

- A virtual machine running NVE aggressively uses disk I/O and is almost never idle. VMware’s recommendations for appropriate resources for high-performance database virtual machines are generally applicable to an NVE virtual machine. In particular, a storage pool allocated from a group of dedicated physical disks in a RAID 1 (mirror) or RAID 10 (combines RAID 0 with RAID 1) configuration provides the best performance.

Deployment

The following sections describe how to deploy and set up an NVE virtual machine.

- NVE does not support migration of data from another instance of NetWorker.
Deploying the appliance

Perform the following steps from a host that has network access to the vCenter server that will host the NVE appliance.

**Before you begin**

Download and install the vSphere Web Integration Client Plug-in.

---

**Note**

The following procedure and screen shots are specific to vCenter 6.0. Other vCenter server versions might display the information in the deployment screens differently.

---

**Procedure**

1. Download the NVE virtual appliance OVA file.
2. Use VMware vSphere Web Client to connect to the vCenter server with a user that has administrative rights.
3. Right-click the vCenter server and select **Deploy OVF template**.
   
   The **Deploy OVF Template** window appears.
4. In the **Select source** page, choose one of the following options, and then click **Next**.
   
   a. **URL**—Specify the path to the OVA file.
   
   b. **Local file**—Click **Browse** and then search for the OVA file.
   
   The following figure provides an example of the **Select source page**.

   ![Select source page](image)

5. In the **Review details** page, review the details about the template, and then click **Next**.
   
   The following figure provides an example of the **Review details page**.
6. In the **End User License Agreement** page, if you agree to the license terms, click **Accept** and then click **Next**.

The following figure provides an example of the **End User License Agreement** page.

**Figure 3** End User License Agreement page

7. In the **Name and Location** page, type a descriptive name for the NVE, select the inventory location, and then click **Next**.

The following figure provides an example of the **Name and Location** page with a Datacenter named Burlington IDD lab selected.
8. In the **Select a resource** page, select the ESXi host, cluster, vApp, or resource pool on which to run the deployed template, and then click **Next**.

   The following figure provides an example of the **Select a resource** page with an ESXi host selected.

   **Figure 5 Select a resource page**

9. In the **Select storage** page, perform the following configuration tasks:
   a. In the **Select virtual disk format** field, leave the default selection **Thick Provisioned Lazy Zeroed**.
      
      Thin provisioning is not supported with NVE.
   b. In the **VM storage policy**, select a storage policy.
   c. In the **Storage** table, select the datastore for NVE.
   d. Click **Next**

   The following figure provides an example of the **Select storage** page with a VNX datastore selected.
10. In the Setup networks page, select the destination network and click Next.

The following figure provides an example of the Setup networks page.

**Figure 7 Setup networks page**

11. In the Customize template page, perform the following configuration tasks, and then click Next:

   a. In the IP Address field, type the IPv4 address for the NVE appliance.
   
   b. In the Netmask field, type the netmask address for the NVE appliance.
   
   c. In the Default Gateway, type the address of the gateway host.
   
   d. In the FQDN field, type the fully qualified domain name (FQDN) for the NVE appliance.
   
   e. In the DNS field, type the IP address of up to three DNS servers, separated by commas.

The following figure provides an example of the Customize templates page.
12. On the Ready to complete page, confirm that the deployment settings, select Power on after deployment, and then click Finish.

The deployment might take several minutes. When the deployment completes, in the Recent tasks section of the vSphere Web Client, the status of the Deploy OVF template task appears as Completed. The following figure provides an example of the Recent Tasks window when the deployment completes.

**Figure 8 Customize templates page**

![Customize templates page](image)

13. In the vSphere Web Client, browse to the Hosts window and select the NVE virtual machine. Open the Virtual Console to monitor installation progress.

14. On the Summary tab, verify that the status for VMware Tools changes to Running or Unmanaged.

**Setting up the NetWorker software on NVE**

To set up the NetWorker software on a new NVE virtual machine, complete the following procedure:

**Procedure**

1. Connect to the NVE, and perform the following tasks:

   If you connect by using the vSphere client to open a VM Console session, you can log in to the NVE with the root or admin account. If you connect by using SSH, you must log in as admin and then use the `su` command to change to the
root account. The default password for the root and admin accounts is `changeme`.

a. Edit the `/etc/hosts` file.

b. Add an entry for the EMC Licensing server.

c. Optional, if you will use a Data Domain system, add an entry for the Data Domain system.

d. Save the file.

2. On a host that has access to the NVE virtual machine, open a web browser and type the following URL:

   `https://NVE_VM`  
   where `NVE_VM` is the hostname or IP address of the NVE virtual machine.

   The **EMC NetWorker Installation Manager** login page appears.

3. When you use Internet Explorer, if any security messages appear, click **Continue**. When you use Firefox, if any connection warnings appear, select **I understand the risks**, and then add an exception for the website.

   The **EMC NetWorker Installation Manager** dialog box appears.

4. In the **User** field, type `root`.

5. In the **Password** field, type `changeme`.

   Note: The default password expiration policy on the NVE is once every 60 days. If the password that you specified has expired, a message similar to the following appears: "Login failed. The password has already expired or is within the warning period. You must change and verify the password expiration date." To resolve this issue, change the passwords assigned to the root and admin users. Modifying passwords provides more information.

6. Click **Login**.

7. On the **SW Releases** tab, click the **Install** button in the upper right corner of the dialog page, to install the NveConfig package.

8. On the **Authc Settings** tab, specify the following attributes:

   a. In the **Tomcat KeyStore password** field, type a password for the keystore file that the NetWorker Authentication Service uses to store data.

      Specify a password that contains at least six characters and does not contain dictionary words.

   b. In the **Tomcat KeyStore password (confirm)** field, type the password for the keystore file.

   c. In the **Authc Password** field, type the a password the NetWorker Authentication Service administrator.

      Ensure the password complies with the following minimum requirements:

      - Nine characters
      - One uppercase letter
      - One lowercase letter
      - One special character
- One numeric character

Note

You will use the administrator account to log in to the NMC Server.

d. In the Authc Password (confirm) field, confirm and type the password for the NetWorker Authentication Service administrator.

e. Click Save.

9. (Optional) To use Data Domain devices in the NetWorker datazone, on the Data Domain Settings tab, check the box in the Value column, and then specify the following configuration attributes:

a. In the Data Domain Address field, type the IP address or the FQDN of the Data Domain system.

b. In the Data Domain Administrator Name field, type the username for an Data Domain Administrator account.

c. In the Data Domain Administrator Password field, type the password for the Data Domain Administrator account.

d. In the Data Domain Storage Folder field, type a new existing name for a folder on the Data Domain system that you will use for DD Boost storage.

e. Optionally, select DDBooost create new login account to create a new DDBooost account.

f. In the Data Domain Login field, type the account for the DD Boost user.

g. In the DDBooost Login Password field, type the password for the DDBooost user that you specified in the Data Domain Login field.

h. In the DDBooost Login Password Confirm field, type the password for the DDBooost user that you specified in the Data Domain Login field.

i. Click Save.

10. On the Passwords tab, and specify the OS admin user and OS root user passwords, and then click Save.

Ensure that you specify a password that meets the following requirements:

- Between 9-40 characters in length
- Contains one upper case letter
- Contains one lower case letter
- Contains one number
- Contains one special character

11. (Optional) On the Security Settings tab, select Show advanced settings, and then check the box in the Value column, to install or upgrade password hardening package. Click Save.

12. (Optional) On the NetWorker Settings tab, enable Show advanced settings and specify the following options:

a. From the Additional Language Pack drop-down, select the desired language pack to install on the NetWorker server.

b. For Data Domain systems only, in the SNMP Community String field, type the SNMP Community String used to monitor the Data Domain system.
The default SNMP Community String on a Data Domain system is *Public.*

13. On the **Server Settings** tab, select the appropriate time zone, and then click **Save.**

14. Click **Continue.**

The **Installation Progress** page appears and displays information about the status of the installation actions.

**Results**

The EMC NetWorker Installation Manager installs the NetWorker and NMC server software on the NVE appliance.

### Starting the NMC server GUI for the first time

The NMC server is a Java web-based application that manages NetWorker server operations. An NMC client is a host that connects to the NMC server through a supported web browser, to display the NMC server GUI.

The following sections outline how to prepare the NMC client and how to connect to the NMC server GUI.

#### Preparing to connect to the NMC server

NetWorker 9.0.1 does not support using a browser on the following operating systems to connect to the NMC GUI:

- AIX
- HP-UX
- Solaris

Before you try to connect to the NMC server from a supported host, ensure that JRE is correctly configured.

**Enabling temporary internet file caching**

Enable the **Temporary internet file caching** attribute in the **Java Control Panel** of the Console client. When you do not enable this option in JRE, **Java WebStart** fails to start.

For Windows Console clients:

1. Browse to **Control Panel** > **Java** > **General** > **Temporary Internet Files** > **Settings**.
2. Ensure that the option **Keep temporary files on my computer** is selected.

For UNIX Console clients:

1. Start the Java web Start Application Manager, `javaws`.
2. Select **Enable temporary internet file caching.**

#### Windows only, confirming JRE version

For Windows hosts only, ensure that you install the correct JRE program for the installed version of Microsoft Internet Explorer.

- For the 32-bit version of Microsoft Internet Explorer, install the 32-bit version of JRE.
- For the 64-bit version of Microsoft Internet Explorer, install the 64-bit version of JRE.
Use the following procedure to determine the Microsoft Internet Explorer version on the Windows Console client.

**Procedure**

1. Right click the Microsoft Internet Explorer shortcut and select **Properties**.
2. Review the **Target Location** field.
   
   The Target Location is:
   
   - C:\Program Files (x86)\Internet Explorer\ for the 32-bit version of Microsoft Internet Explorer.
   - C:\Program Files\Internet Explorer\ for the 64-bit version of Microsoft Internet Explorer.

**Adding the NMC server to Exception Site list**

Java security settings block the NMC server application.

Therefore, you must add the NMC server address to the JRE Exception site list.

**Procedure**

1. Open the **Java Control Panel**.
2. On the **Security** tab, select **Edit Site list**.
3. Click **Add**.
4. In the **Location** field, specify the URL to the NMC server in the format `http://server_name:9000`
   where `server_name` is the hostname of the NMC server.

**Note**

If you connect to the NMC server by using the IP address of the NMC server, add an entry for the IP address in the following format:

```
http://ip_address:9000
```

5. Click **OK**.
6. In the **Security Warning** window, click **Continue**.
7. Click **OK**.

**Launching the Networker Console**

Complete the following procedure to connect to the NMC Server GUI from an NMC client. By default, the NetWorker Authentication Service uses the local user database for user authentication. Specify the NetWorker Authentication Service administrator account to log in to the NMC Server. The *EMC NetWorker Security Configuration Guide* describes how to configure the NetWorker Authentication Service to use LDAP or AD for user authentication.

**Procedure**

1. From a supported web browser session, type the URL of the NMC Server:

   `http://server_name:http_service_port`
   
   where:
• \textit{server\_name} is the name of the NMC Server.

• \textit{http\_service\_port} is the port for the embedded HTTP server. The default HTTP port is 9000.

For example: http://houston:9000

The \texttt{gconsole.jnlp} file downloads to the host. When the download completes, open the file.

2. When you use Mozilla Firefox on Windows, and the \texttt{jnlp} extension is not associated with Java, you are prompted to choose the program that opens the \texttt{jnlp} file. Select \texttt{Java (TM) Web Start Launcher}. If this application does not appear, browse to the Java 7 folder and select the \texttt{javaws.exe} file.

The following figure provides an example of the file association window that appears with the Mozilla Firefox browser.

\textbf{Figure 10 Associating a jnlp file with Java (TM) web Start Launcher for Mozilla Firefox}

3. In the \textbf{Welcome} page, click \textbf{Start}.

\textbf{Note}

If the \textbf{Start} button does not appear but you see a warning message, which states that Java Runtime Environment cannot be detected, click the \texttt{here} hyperlink.

4. For Internet Explorer only, if a security warning appears, select \texttt{I accept the risks and want to run this application}, then click \texttt{Run}.

5. In the \textbf{Log in} page, specify the NetWorker Authentication Service administrator username and password, and then click \texttt{OK}.

6. In the \textbf{Licensing Agreement} page, select \textbf{Accept}.

7. If you did not install a support version of JRE on the host, then a prompt to install JRE appears. Cancel the installation, install JRE, and then re-run the installation.

8. In the \textbf{Welcome to the NMC Server Configuration Wizard} page, click \textbf{Next}.
9. In the **Specify a list of managed NetWorker Servers** page:
   a. Specify the names of the NetWorker Server that the NMC Server will manage, one name per line.

   **Note**
   If the NMC Server is also the NetWorker Server, specify the name of the NetWorker Server.

   b. Leave the default options **Capture Events** and **Gather Reporting Data** enabled.

   Consider the following:
   - Enable the **Capture Events** option to allow the NMC Server to monitor and record alerts for events that occur on the NetWorker Server.
   - Enable the **Gather Reporting Data** option to allow the NMC Server to collect data about the NetWorker Server and generate reports.

10. Click **Finish**. The installation starts the default web browser and connects to the NMC server. The **NetWorker Management Console** window and the **Getting Started** window appear.

11. In the **Enterprise** window, right-click the NetWorker Server, and then select **Launch Application**.

   **Note**
   If you do not specify any NetWorker Servers in the **Specify a list of managed NetWorker servers** window, then the NMC **Enterprise** window does not display any NetWorker Servers. To add a host, right-click **Enterprise** in the left navigation pane and select **New > Host**. The **Add New Host** wizard appears.

**After you finish**

After launching the NVE appliance, refer to the standard NetWorker documentation for any additional configuration.

**About the EMC Licensing Solution**

The EMC Licensing Solution introduced in NetWorker 9.0, is an EMC licensing standard that stores all licensing information for the environment in one license file, which is stored on both the NetWorker server and an EMC License Server. All new installations of NetWorker 9.0 and later use the EMC Licensing Solution.

The following section provides an overview of the various components that are required to set up the EMC Licensing Solution. These components include the following:

- **EMC License Server**
- **License file**
- **Management of the License Server through LMTOOLS (Windows) or lmgrd (Linux).**

The *EMC NetWorker Licensing Guide* provides more information about the EMC License Solution.
EMC License Server

After installing NetWorker 9.0.1, install the Windows or Linux 64-bit License server package if you do not already have the License Server installed. The License Server is responsible for managing the EMC licenses and capacity allocation.

NetWorker supports installation of the License Server on the following 64-bit platforms.

Table 4 Supported License Server platforms

<table>
<thead>
<tr>
<th>Platform</th>
<th>Versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Linux</td>
<td>Red Hat Enterprise Linux 6.x, SuSE Linux Enterprise Server 10.x, 11.x</td>
</tr>
</tbody>
</table>

Once you install the License Server, you must obtain the license file from EMC Licensing. This file contains the host and port information of the License Server. The License Server is expected to use a default or specific TCP/IP port number. For NetWorker, this default port is 27000. If a specific (non-default) port is used, it must match the port number in the license file. You can set the License Server to listen to an available TCP/IP port, typically in the range of 27000 to 27009.

You can start the License Server by using the LMTOOLS application (on Windows) or the `lmgrd` command (on Linux).

**Note**

EMC does not recommend running the NetWorker Server and the License Server on the same host. If you do run both on the same host, ensure that you start the NetWorker server before you start the `lmgrd` process.

License file

The EMC Licensing Solution relies on a license file to indicate the NetWorker features and capacity you purchased, or options made available for the purposes of evaluating NetWorker.

When you download the NetWorker software and the EMC License Server software, you must also obtain a license file from EMC Licensing. This file must reside both on a platform that runs the License Server, and is accessible to NetWorker. Therefore, you must store a copy of the file in the License server folder, and in the `/nsr/lic` directory on the NetWorker server. When you copy the license file to this directory on the NetWorker server, you must change the file name to `dpa.lic` if this is not the file name already. The license file is an ASCII text file for which the content is encrypted to prevent tampering or changes.

The license file can contain two types of entitlements -- an update entitlement, if updating from a previous NetWorker release, and a single capacity entitlement, which you can share across two datazones if you do not exceed the capacity purchased. All datazones can point to a single License Server to request capacity.

Management of the EMC License Server

After you install the License Server, a management application is placed on an accessible server. Complete the setup and configuration of the EMC Licensing
Solution by using the License Server management application appropriate to your platform.

On Windows, use the LMTOOLS application. On Linux, use the command line utility lmgrd.

The application should be running constantly to serve licenses to NetWorker. To accomplish this, the application requires the existence of a running vendor daemon, EMCLM, which delivers license features to NetWorker and keeps track of counted features. The application automatically manages EMCLM by starting, restarting, and stopping the daemon as required. It will also write to the License Server’s troubleshoot log file lmgrd.log to report errors and license feature activity. The lmgrd, EMCLM, license, and troubleshoot log files are located in the same directory.

Note

Use the *EMC License Server Installation and Administration Guide* for complete EMC License Server management instructions.

Quick Start: Activating 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 9.0, as outlined in more detail in subsequent sections of the *EMC NetWorker Licensing Guide* and the *EMC License Server Installation and Administration Guide*.

Procedure

1. Download the License Server package for the platform from the same location you downloaded the NetWorker software.
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.
   - On Windows, the package is `EMC_LicenseServer_3.4.0_x64 installer.msi`.
   - On Linux, the package is `emclicenseserver-3.4.1-2.x86_64_lsb.rpm`
3. Obtain the license file from EMC Licensing. For a new installation of NetWorker 9.0, this file contains a capacity entitlement.
   
   You can obtain the file once you provide EMC Licensing with the License Server host/IP information, the required capacity, and the port to use for communication between NetWorker and the License Server if you cannot use the default port 27000. EMC requires this information to create the license file.
4. In the location you installed the License Server:
   a. Create a directory.
   b. Copy the license file to this directory.
   c. Do not rename the license file.

   For example, on the License Server, create the following directories:
   - On Windows: `C:\Program Files\EMC License Server\elms\licenses`
   - On Linux: `/opt/emc/licenses`
Note
On Linux, you may be required to complete this step before installing the License Server package.

5. On the NetWorker server:
   a. Copy the license file to the following locations:
      - On Windows: C:\Program Files\EMC NetWorker\nsr\lic
      - On Linux: /nsr/lic
   b. Rename the file to dpa.lic if this is not already the file name.

6. Complete the configuration of the License Server and then start the License Server:
   a. On Windows, use LMTOOLS or the command line interface.
      An icon for LMTOOLS appears on the desktop after the License Server installation.
   b. On Linux, use lmgrd.

7. In the NMC Administration window:
   a. Right-click the server.
   b. Select Properties.

8. In the Server Properties window:
   a. Change the CLP Refresh field to Yes.
   b. Ensure that the following fields are populated correctly:
      - CLP license server
      - CLP License Server Port
      - Solution ID
      - CLP SWID
   c. Click Ok.

Note
CLP refers to the EMC License Server.

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

Configuring sendmail and NetWorker notifications
Review this section to configure the sendmail application and modify NetWorker email notifications.

The EMC NetWorker Administration Guide provides more information about server notifications and how to configure notifications while creating the Policy, Workflow and Action resources.
Configuring sendmail

The sendmail application is automatically installed on the NVE. To configure the NetWorker server to send notifications, configure sendmail.

Before you begin

The environment requires an SMTP relay host.

Procedure

1. Connect to the NVE.
   
   If you connect by using the vSphere client to open a VM Console session, you can log in to the NVE with the root or admin account. If you connect by using SSH, you must log in as admin and then use the su command to change to the root account. The default password for the root and admin accounts is changeme.

2. Create the /etc/rc.conf file, and then add the following line:

   ```
   sendmail_enable="YES"
   ```

3. Save the file.

4. Edit the /etc/sysconfig/sendmail.conf file, and change the line `SENDMAIL_SMARTHOST=" "` to include the hostname of the SMTP relay host.

   For example:

   ```
   SENDMAIL_SMARTHOST=" mysmtp_relay.emc.com"
   ```

5. Restart the sendmail appliance by typing the following command:

   ```
   service sendmail restart
   ```

6. Test the connection to the SMTP relay host.

   For example:

   ```
   echo "Subject: sendmail test" | sendmail -v debbied@email.com
   ```

   Output similar to the following appears when the test succeeds:

   ```
   debbied@email.com... Connecting to [127.0.0.1] port 25 via relay...
   SuSE Linux 0.8; Mon, 3 Oct 2016 10:36:58 -0400
   >>> EHLO bu-idd-nve.iddlab.local
   250-bu-idd-nve.iddlab.local Hello localhost.localdomain
   [127.0.0.1], pleased to meet you
   250-ENHANCEDSTATUSCODES
   250-PIPELINING
   250-8BITMIME
   250-DNS
   250-ETRN
   250-AUTH GSSAPI
   250-DELIVERBY
   250 HELP
   >>> MAIL From:<root@bu-idd-nve.iddlab.local> SIZE=23
   AUTH=root@bu-idd-nve.iddlab.local
   250 2.1.0 <root@bu-idd-nve.iddlab.local>... Sender ok
   ```
Configuring email notifications

Perform the following steps to modify existing notification configurations in NetWorker.

Before you begin
- Enable and configure the sendmail application.

Procedure

1. Click the Enterprise button on the taskbar.
2. Highlight a host in the navigation tree, right-click NetWorker and select Launch Application. The NetWorker Administration window appears.
3. On the main toolbar, click Server, and then from the left navigation pane, select Notifications.
4. Right-click a notification and select Properties.
5. Edit the Action field, and then specify the sendmail command in the following format:

   `/usr/sbin/sendmail -v recipient_email "subject_text"`

   where:
   - `recipient_email` is the email address for the recipient of the notification.
   - `subject_text` is the subject of the email address, enclosed in quotation marks.

   For example, to edit the Bus/Device Reset action, type:

   `/usr/sbin/sendmail -v debbied@emc.com "host <bu-iddnwserv.iddlab.local>: Bus/Device reset detected"`

Editing policy notifications

Perform the following steps to modify the notification configuration for an existing policy resource, when the Send notification option is set to On Completion or On Failure.

Before you begin
- Enable and configure the sendmail application.

Procedure

1. Click the Enterprise button on the taskbar.
2. Highlight a host in the navigation tree, right-click NetWorker and select Launch Application. The NetWorker Administration window appears.
3. In the **NetWorker Administration** window, click **Protection**.

4. In the left navigation pane, expand **Policies**, right click the policy, and then select **Properties**.

5. Edit the **Command** field, and then specify the `sendmail` command in the following format:

   ```
   /usr/sbin/sendmail -v recipient_email "subject_text"
   ```

   where:
   - `recipient_email` is the email address for the recipient of the notification.
   - `subject_text` is the subject of the email address, enclosed in quotation marks.

6. Click **OK**.

### Editing workflow notifications

Perform the following steps to modify a workflow notification, when the **Send notification** option is set to **On Completion** or **On Failure**.

**Before you begin**

Enable and configure the `sendmail` application.

**Procedure**

1. Click the **Enterprise** button on the taskbar.
2. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
3. In the **NetWorker Administration** window, click **Protection**.
4. In the left navigation pane, expand **Policies**, and then expand the policy that contains the workflow.
5. Right-click the workflow and select **Properties**.
6. In the **Command** field, type the `sendmail` command in the following format:

   ```
   /usr/sbin/sendmail -v recipient_email "subject_text"
   ```

   where:
   - `recipient_email` is the email address for the recipient of the notification.
   - `subject_text` is the subject of the email address, enclosed in quotation marks.

7. Click **OK**.

### Editing action notifications

Perform the following steps to modify an action notification, when the **Send notification** option is set to **On Completion** or **On Failure**.

**Before you begin**

Enable and configure the `sendmail` application.

**Procedure**

1. Click the **Enterprise** button on the taskbar.
2. Highlight a host in the navigation tree, right-click **NetWorker** and select **Launch Application**. The **NetWorker Administration** window appears.
3. In the **NetWorker Administration** window, click **Protection**.
4. In the left navigation pane, expand **Policies**, and then expand the policy that contains the workflow.
5. Select the workflow. On the **Workflow** pane, click the **Action** tab.
6. Right-click the action, and then select **Properties**.
7. In the Policy Action wizard, browse to the **Specify the Action Information** window.
8. In the **Command** field, type the `sendmail` command in the following format:
   
   ```
   /usr/sbin/sendmail -v recipient_email "subject_text"
   ```
   
   where:
   * `recipient_email` is the email address for the recipient of the notification.
   * `subject_text` is the subject of the email address, enclosed in quotation marks.
9. Click **OK**.

---

**Upgrading**

The following sections describe how to upgrade an NVE virtual appliance.

**Procedure**

1. Download the NVE virtual appliance upgrade file (*NVEUpgrade*.avp) to a host that has access to the NVE virtual appliance.
2. Log in to the NVE virtual appliance as the root user.
3. Copy the AVP file to the `/data01/avamar/repo/packages` folder on the NVE virtual appliance.
   
   For example, to use `scp` application to copy the file to the NVE virtual appliance, perform the following steps:
   
   a. Start the `ssh` daemon: `/etc/init.d/sshd`.
   b. Edit the `/etc/ssh/sshd_config` file and then uncomment the line:
      
      ```
      PermitRootLogin yes
      ```
   c. Use the `scp` application on the host that contains the AVP file, and connect to the NVE virtual appliance with the root account.
4. Open a web browser and type the following URL:
   
   ```
   https://NVE_address
   ```
   
   Where `NVE_address` is the hostname or IP address of the NVE virtual appliance.
   
   The **EMC NetWorker Installation Manager** login page appears.
5. When you use Internet Explorer, if any security messages appear, click **Continue**. When you use Firefox, if any connection warnings appear, select **I understand the risks**, and then add an exception for the website.
   
   The **EMC NetWorker Installation Manager** dialog box appears.
6. In the **User** field, type `root`.
7. In the **Password** field, type the password for the root account.
8. On the SW Releases tab, click the Install button in the upper right corner of the dialog page, to install the NveConfig package.

The Installation Setup page appears.

9. Click Continue.

10. When the upgrade completes, click Launch NMC to connect to the NMC server.
CHAPTER 3

Maintenance

This chapter includes the following topic:

- Password maintenance ........................................................................................................... 36
Password maintenance

This section describes how to manage the root and admin passwords.

Reviewing password policies

Use the `chage` command to review password policy configuration for an OS user.

Procedure

1. Connect to the NVE.
   
   If you connect by using the vSphere client to open a VM Console session, you can log in to the NVE with the root or admin account. If you connect by using SSH, you must log in as admin and then use the `su` command to change to the root account. The default password for the root and admin accounts is `changeme`.

2. Use the `chage` command to determine the password expiration policy and the scheduled expiration date for a user account.
   
   For example, to determine the policy assigned to the root user account, and the password expiration date, type:

   ```
   chage -l root
   ```

   Output similar to the following appears:

   ```
   Minimum: 1
   Maximum: 60
   Warning: 7
   Inactive: -1
   Last Change: Dec 07, 2015
   Password Expires: Feb 05, 2016
   Password Inactive: Never
   Account Expires: Never
   ```

   The following table provides more information about the `chage` output.

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum</td>
<td>Defines the minimum numbers of days that are allowed between password changes. When this value is 0, a user can change the password at any time.</td>
</tr>
<tr>
<td>Maximum</td>
<td>Defines the maximum numbers of days that a password remains valid, before a password change is required.</td>
</tr>
<tr>
<td>Inactive</td>
<td>Defines the number of days that a user account can remain inactive after the password has expired, before the user account is locked out of the system. When this value is -1, the inactive feature is disabled.</td>
</tr>
</tbody>
</table>
Table 5 chage output (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last change</td>
<td>Display the date that the password was last changed.</td>
</tr>
<tr>
<td>Password expires</td>
<td>Defines the date that the current password will expire.</td>
</tr>
<tr>
<td>Password inactive</td>
<td>Defines the date that the current password will become inactive.</td>
</tr>
<tr>
<td>Account expires</td>
<td>Defines the date that the user account will expire.</td>
</tr>
</tbody>
</table>

**Modifying passwords**

By default, the password expiration policy for the admin and root user accounts is every 60 days.

Perform the following steps to determine the password expiration policy, to determine the scheduled expiration date for a password, and to change passwords.

**Procedure**

1. Connect to the NVE.
   
   If you connect by using the vSphere client to open a VM Console session, you can log in to the NVE with the root or admin account. If you connect by using SSH, you must log in as admin and then use the `su` command to change to the root account. The default password for the root and admin accounts is `changeme`.

2. Use the `passwd` command to change the password for an OS user account.

   For example, to change the password for the root account, type:

   `passwd root`