

Dell EMC NetWorker

Version 19.1

Virtual Edition Deployment Guide

302-005-708

REV 01

Copyright © 1990-2019 Dell Inc. or its subsidiaries. All rights reserved.

Published May, 2019

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.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

Figures		5
Preface		7
Chapter 1	Overview of NetWorker Virtual Edition	11
	Overview of NetWorker Virtual Edition.....	12
Chapter 2	Deploying NetWorker Virtual Edition in VMware vSphere	13
	Predeployment requirements and best practices.....	14
	Solution requirements.....	14
	Virtual disk configuration best practices.....	15
	Preconfiguration checklist.....	16
	Verify the DNS configuration.....	16
	Deploying the NVE appliance.....	17
Chapter 3	Deploying the NetWorker Virtual Edition in Amazon EC2	25
	Deploying the NetWorker Virtual Edition Appliance in Amazon EC2.....	26
	Deploy NVE from the AWS Marketplace.....	26
	Deploying the NVE Virtual Machine from AWS Marketplace.....	26
Chapter 4	Deploying the NetWorker Virtual Edition with Microsoft Azure Resource Manager	29
	Deploying the NetWorker Virtual Edition Appliance in Microsoft Azure Resource Manager.....	30
	Deploying the NVE Virtual Machine from Azure Marketplace.....	30
Chapter 5	Deploying NetWorker Virtual Edition in VMware Cloud Marketplace	33
	Deploying the NetWorker Virtual Edition On VMC.....	34
Chapter 6	Configuring the NetWorker Virtual Edition	37
	Setting up the NetWorker software on NVE.....	38
	Launching the NetWorker Management Web UI.....	40
	Starting the NMC server GUI for the first time.....	41
	Preparing to connect to the NMC server.....	41
	Launching the NetWorker Management Console	43
	Configuring sendmail and NetWorker notifications.....	45
	Configure the sendmail application.....	46
	Configuring NetWorker to send operation notifications by email... ..	47
	Edit policy notifications.....	47
	Edit workflow notifications.....	48
	Edit action notifications.....	48
	Upgrade the NVE appliance using GUI.....	49

	Upgrading the NVE using CLI	50
Chapter 7	Maintenance	53
	Performing NVE appliance Security Rollup Update.....	54
	Password maintenance.....	54
	Review password policies.....	55
	Modify passwords.....	56
	Change the storage disk configuration.....	56
Chapter 8	Configuring Firewall	61
	NetWorker Virtual Edition firewall.....	62
	Editing the Firewall in NVE.....	62
	Configuring the NVE firewall.....	63
	Opening a firewall port.....	63
	Closing a firewall port.....	66
	Removing a custom firewall rule.....	69
	Configuring service port ranges on firewall.....	70
Chapter 9	Troubleshooting and Best Practices	71
	Best Practices and Recommendations.....	72
	Accessing NetWorker Virtual Edition using SSH.....	72
	Enable SSH for root.....	72
	Enable SSH for root for NVE running in Cloud.....	73
	Support for NVE in Dual NIC configuration with different Subnets.....	74
	Binding to LDAP server error.....	74
	NVE installation log files.....	75

FIGURES

1	Select source page.....	18
2	Review details page.....	18
3	End User License Agreements page.....	19
4	Select a name and folder page.....	19
5	Select a resource page.....	20
6	Select storage page.....	20
7	Setup networks page.....	21
8	Customize template page.....	22
9	Recent Tasks.....	22
10	Summary tab	23
11	Welcome to the NMC Server Configuration Wizard page.....	44
12	Specify a list of managed NetWorker servers page.....	45
13	Deleting a disk device.....	58
14	Deleting the old VMDK file.....	60
15	NetWorker in Dual NIC configuration.....	74

FIGURES

Preface

As part of an effort to improve product lines, periodic revisions of software and hardware are released. Therefore, all versions of the software or hardware currently in use might not support some functions that are described in this document. The product release notes provide the most up-to-date information on product features.

If a product does not function correctly or does not function as described in this document, contact a technical support professional.

Note

This document was accurate at publication time. To ensure that you are using the latest version of this document, go to the Support website <https://www.dell.com/support>.

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

Revision	Date	Description
01	May 20, 2019	First release of this document for NetWorker 19.1.

Related documentation

The NetWorker documentation set includes the following publications, available on the Support website:

- *NetWorker E-LAB Navigator*
Provides compatibility information, including specific software and hardware configurations that NetWorker supports. To access E-LAB Navigator, go to <https://elabnavigator.emc.com/eln/elhome>.
- *NetWorker Administration Guide*
Describes how to configure and maintain the NetWorker software.
- *NetWorker Network Data Management Protocol (NDMP) User Guide*
Describes how to use the NetWorker software to provide data protection for NDMP filers.
- *NetWorker Cluster Integration Guide*
Contains information related to configuring NetWorker software on cluster servers and clients.
- *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.

- *NetWorker Updating from a Previous Release Guide*
Describes how to update the NetWorker software from a previously installed release.
- *NetWorker Release Notes*
Contains information on new features and changes, fixed problems, known limitations, environment and system requirements for the latest NetWorker software release.
- *NetWorker Command Reference Guide*
Provides reference information for NetWorker commands and options.
- *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.
- *NetWorker Performance Optimization Planning Guide*
Contains basic performance tuning information for NetWorker.
- *NetWorker Server Disaster Recovery and Availability Best Practices Guide*
Describes how to design, plan for, and perform a step-by-step NetWorker disaster recovery.
- *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 storage arrays.
- *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.
- *NetWorker Security Configuration Guide*
Provides an overview of security configuration settings available in NetWorker, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- *NetWorker VMware Integration Guide*
Provides planning and configuration information on the use of VMware in a NetWorker environment.
- *NetWorker Error Message Guide*
Provides information on common NetWorker error messages.
- *NetWorker Licensing Guide*
Provides information about licensing NetWorker products and features.
- *NetWorker REST API Getting Started Guide*
Describes how to configure and use the NetWorker REST API to create programmatic interfaces to the NetWorker server.
- *NetWorker REST API Reference Guide*
Provides the NetWorker REST API specification used to create programmatic interfaces to the NetWorker server.
- *NetWorker 19.1 with CloudBoost 19.1 Integration Guide*
Describes the integration of NetWorker with CloudBoost.
- *NetWorker 19.1 with CloudBoost 19.1 Security Configuration Guide*
Provides an overview of security configuration settings available in NetWorker and Cloud Boost, secure deployment, and physical security controls needed to ensure the secure operation of the product.
- **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.

- **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

The following conventions are used 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

The following type style conventions are used in this document:

Table 2 Style conventions

Bold	Used for interface elements that a user specifically selects or clicks, for example, names of buttons, fields, tab names, and menu paths. Also used for the name of a dialog box, page, pane, screen area with title, table label, and window.
<i>Italic</i>	Used for full titles of publications that are referenced in text.
Monospace	Used for: <ul style="list-style-type: none"> • System code • System output, such as an error message or script • Pathnames, file names, file name extensions, prompts, and syntax • Commands and options
<i>Monospace italic</i>	Used for variables.
Monospace bold	Used for user input.
[]	Square brackets enclose optional values.
	Vertical line indicates alternate selections. The vertical line means or for the alternate selections.
{ }	Braces enclose content that the user must specify, such as x, y, or z.
...	Ellipses indicate non-essential information that is omitted from the example.

You can use the following resources to find more information about this product, obtain support, and provide feedback.

Where to find product documentation

- <https://www.dell.com/support>
- <https://community.emc.com>

Where to get support

The Support website <https://www.dell.com/support> provides access to product licensing, documentation, advisories, downloads, and how-to and troubleshooting

information. The information can enable you to resolve a product issue before you contact Support.

To access a product-specific page:

1. Go to <https://www.dell.com/support>.
2. In the search box, type a product name, and then from the list that appears, select the product.

Knowledgebase

The Knowledgebase contains applicable solutions that you can search for either by solution number (for example, KB000xxxxxx) or by keyword.

To search the Knowledgebase:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Knowledge Base**.
3. In the search box, type either the solution number or keywords. Optionally, you can limit the search to specific products by typing a product name in the search box, and then selecting the product from the list that appears.

Live chat

To participate in a live interactive chat with a support agent:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Contact Support**.
3. On the **Contact Information** page, click the relevant support, and then proceed.

Service requests

To obtain in-depth help from Licensing, submit a service request. To submit a service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.

Note

To create a service request, you must have a valid support agreement. For details about either an account or obtaining a valid support agreement, contact a sales representative. To get the details of a service request, in the *Service Request Number* field, type the service request number, and then click the right arrow.

To review an open service request:

1. Go to <https://www.dell.com/support>.
2. On the **Support** tab, click **Service Requests**.
3. On the **Service Requests** page, under **Manage Your Service Requests**, click **View All Dell Service Requests**.

Online communities

For peer contacts, conversations, and content on product support and solutions, go to the Community Network <https://community.emc.com>. Interactively engage with customers, partners, and certified professionals online.

How to provide feedback

Feedback helps to improve the accuracy, organization, and overall quality of publications. You can send feedback to DPAD.Doc.Feedback@emc.com.

CHAPTER 1

Overview of NetWorker Virtual Edition

This chapter includes the following topic:

- [Overview of NetWorker Virtual Edition](#)..... 12

Overview of NetWorker Virtual Edition

NetWorker® Virtual Edition (NVE) is a NetWorker Server that runs as a virtual machine in VMware and cloud environment. NVE integrates the latest version of the NetWorker software with SuSE Linux as a VMware virtual machine.

Note

You cannot update a NetWorker Server that resides on a physical host to an NVE appliance.

CHAPTER 2

Deploying NetWorker Virtual Edition in VMware vSphere

This chapter includes the following topics:

- [Predeployment requirements and best practices](#)..... 14
- [Deploying the NVE appliance](#)..... 17

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 data migration from another instance of NetWorker.

Solution requirements

This section outlines the solution requirements for the NetWorker Virtual Edition in the following environments.

- VMware vSphere
- Amazon Web Services (AWS) EC2
- Microsoft Azure

WAN requirements

The following points provide the WAN requirements for the NetWorker Virtual Edition.

- Greater than or equal to 100 Mb/s bandwidth
- Less than or equal to 100 ms RTT latency

System requirements

The following table defines the minimum system requirements for each size of NVE. When creating the Azure or AWS instance, you should select the appropriate instance type for the minimum system requirements for the NVE.

Table 3 Minimum requirements for vSphere, Azure and AWS

	Small workload	Medium workload	High workload
NVE root disk space	126 GB	126 GB	126 GB
Data disk space	600 GB	1200 GB	2400 GB
Azure instance	D4S_V3 Standard	D4S_V3 Standard	D8S_V3 Standard
AWS instance	m4.xlarge	m4.xlarge	m4.2xlarge
vSphere	-	-	-
Number of jobs performed per day	Up to ten thousand	Up to fifty thousand	Up to one hundred thousand

Note

For information related to IOPS, memory, cores, network and disk sizing, refer to *NetWorker Performance and Optimization planning guide*

VMware ESX System Requirements

NetWorker Virtual Edition (NVE) supports the following VMware versions:

- VMware vCenter 5.5, 5.5u2, 6.0, and 6.5
- ESXi 5.5, 5.5u2, 6.0, and 6.5

Port requirements

As with all networked software solutions, adhering to best practices for security is encouraged to protect the deployment. If the ports in the following table are not configured before you configure the NetWorker Virtual Edition appliance, restart the NetWorker Virtual Edition appliance.

The following table outlines the port requirements.

Table 4 Port requirements

Out	In	TCP port	Description
Administrator workstation	NetWorker Virtual Edition appliance	22	SSH for maintenance and troubleshooting
Administrator workstation	NetWorker Virtual Edition appliance	23	Optional for Telnet
Administrator workstation	NetWorker Virtual Edition appliance	443	HTTPS to local appliance administration page that is used by support for troubleshooting

For information about NetWorker Server port requirement, refer to the *NetWorker Security Configuration Guide*.

Virtual disk configuration best practices

ESXi supports multiple disk formats. For NVE virtual machines, the initial configuration is thick provision lazy zeroed.

Note

NVE does not support thin provisioning.

After the initial deployment, if you configure the virtual disks for the thick provision eager zeroed, you will get better initial performance because the first write to the disk will require fewer operations.

Note

VMware documentation provides information about 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 that runs NVE aggressively uses disk I/O and is almost never idle. VMware recommendations for appropriate resources for high-performance database virtual machines are generally applicable to an NVE virtual machine. In particular, a storage pool that is 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.

Preconfiguration checklist

Before you deploy the NVE appliance, gather the following information.

Table 5 Preconfiguration checklist

Completed?	Information
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>Network configuration details:</p> <ul style="list-style-type: none"> • Additional DNS search domains: • DNS servers: • Hostname FQDN: • IPv4 or IPv6 Address and Mask/Prefix: • IPv4 or IPv6 Default Gateway: • NTP Servers:
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>Ensure that the following firewall ports are open between the NetWorker Server and the Dell EMC License Server:</p> <ul style="list-style-type: none"> • 27000 • 27010 • 51000 <hr/> <p>Note</p> <p>These ports are not required for NetWorker Virtual Edition running with unserved license</p>
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<p>Data Domain system information (when DD Boost devices are used):</p> <ul style="list-style-type: none"> • IP address of the Data Domain system: • Administrator account name: • Password of the administrator account: • Storage folder location: • DDBoost user username: • Password of the DDBoost user: • SNMP community string:

Verify the DNS configuration

Before you deploy the NVE, ensure that the DNS server is configured correctly for the hostname and IP address of the vCenter server and the NVE appliance. Incorrect name resolution results in runtime errors and configuration issues.

From a command prompt on the vCenter server, type the following commands:

Procedure

1. To perform a reverse DNS lookup of the IP address of the NVE, type the following command:

```
nslookup NVE_IP_address DNS_Server_IP_address
```

The IP address configuration is correct when the `nslookup` command returns the fully qualified domain name (FQDN) of the NVE.

2. To perform a forward DNS lookup of the FQDN of the NVE, type the following command:

```
nslookup NVE_FQDN DNS_Server_IP_address
```

The FQDN configuration is correct when the `nslookup` command returns the correct IP address of the NVE.

3. To perform a reverse DNS lookup of the IP address of the vCenter server, type the following command:

```
nslookup vCenter_IP_Address DNS_Server_IP_address
```

The IP address configuration is correct when the `nslookup` command returns the FQDN of the vCenter server.

4. To perform a forward DNS lookup of the FQDN of the vCenter server, type the following command:

```
nslookup FQDN_of_vCenter DNS_Server_IP_address
```

The FQDN configuration is correct when the `nslookup` command returns the correct IP address of the vCenter Server.

Results

If the `nslookup` commands return the proper information, close the command prompt. If the `nslookup` commands do not return the correct information, before you install NVE, resolve the DNS configuration.

Deploying the NVE appliance

NVE uses an open virtualization format template (OVF Template) to deploy and configure the appliance. The OVF template is distributed as an open virtual appliance (OVA) package.

Before you begin

Download and install the vSphere Web Integration Client Plug-in on a host that has network access to the vCenter server that manages the NVE appliance.

Perform the following steps from a host that has the vSphere Web Integration Client Plug-in and network access to the vCenter server.

Note

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

Procedure

1. Download the NVE OVA package from <http://support.emc.com>.
2. Connect to the vCenter server, by using the VMware vSphere Web Client. On the Login screen, specify a user account that has administrative rights.

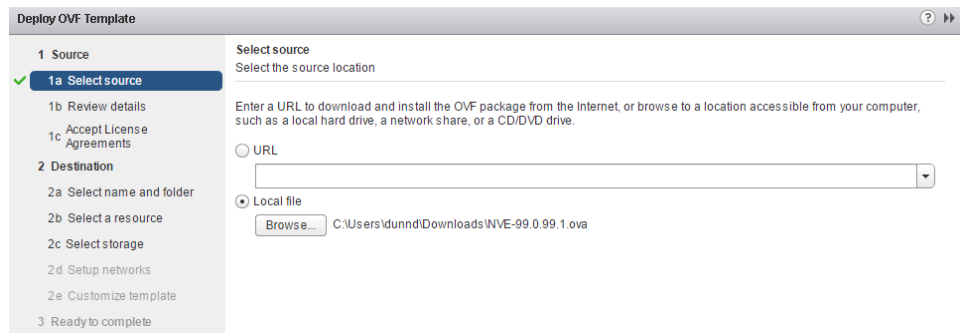
3. In the vCenter server console, browse to **vCenter > vCenter server**.
4. Right-click the vCenter server that manages the NVE appliance and select **Deploy OVF template**.

The **Deploy OVF Template** wizard is displayed.

5. On the **Select source** page, select one of the following options, and then click **Next**.
 - **URL**—Type the path to the OVA file.
 - **Local file**—Click **Browse**, and then search for the OVA file.

The following figure provides an example of the **Select source** page.

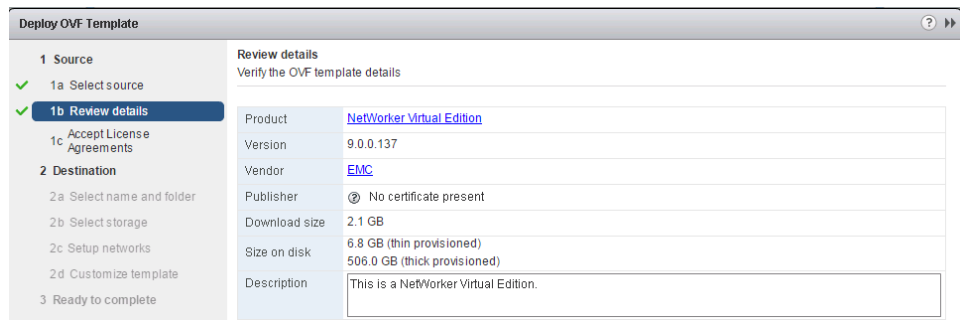
Figure 1 Select source page



6. On the **Review details** page, verify the details about the template, and then click **Next**.

The following figure provides an example of the **Review details** page.

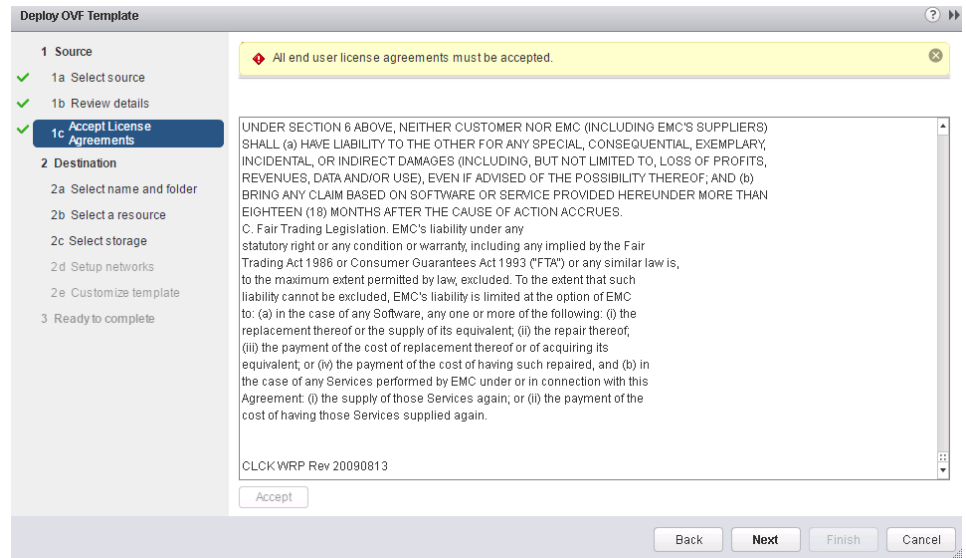
Figure 2 Review details page



7. On 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 **Accept License Agreements** page.

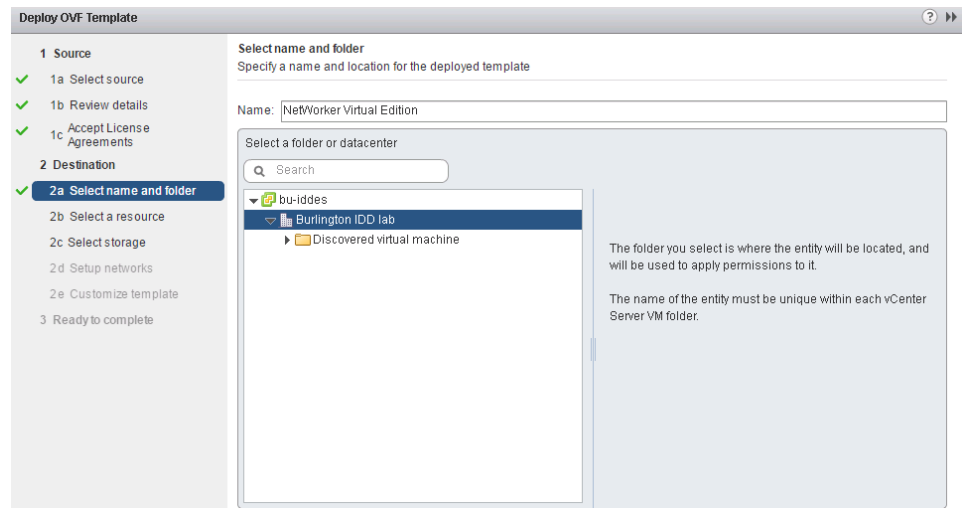
Figure 3 End User License Agreements page



8. On the **Select a name and folder page** page, type a descriptive name for the NVE, select the inventory location, and then click **Next**.

The following figure provides an example of the **Select a name and folder page** with a Datacenter named Burlington IDD lab selected.

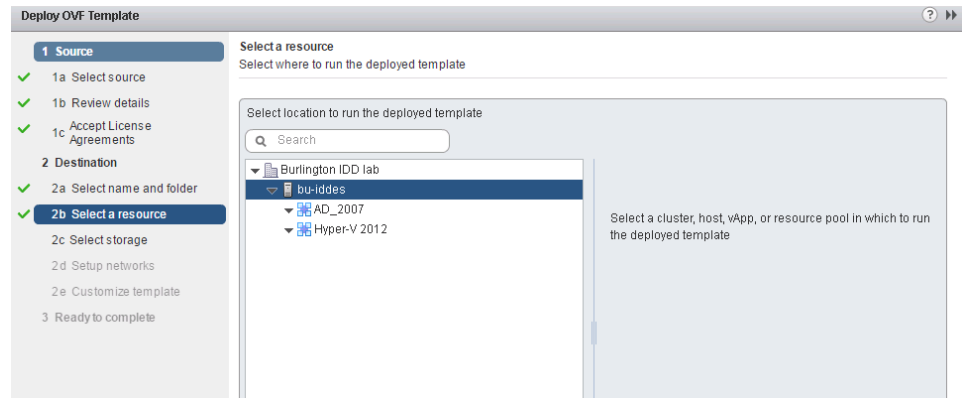
Figure 4 Select a name and folder page



9. On 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



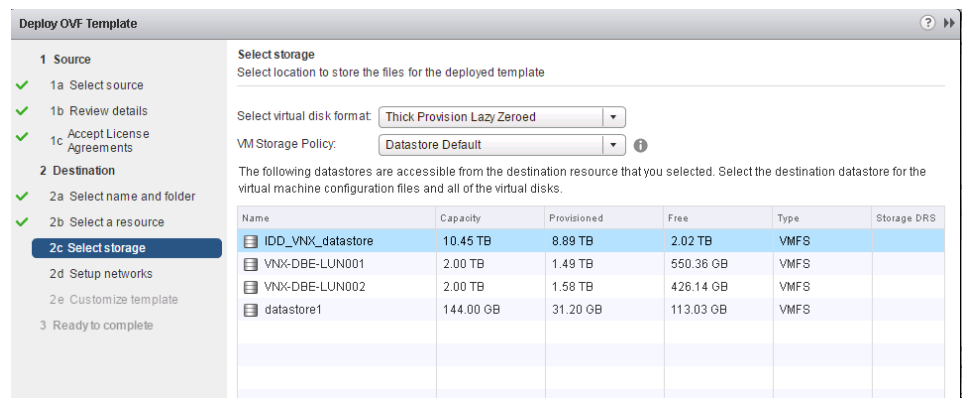
10. On the **Select storage** page, perform the following configuration tasks:
 - a. In the **Select virtual disk format** field, leave the default selection **Thick Provisioned Lazy Zeroed**.
Thin provisioning is not supported with NVE.
 - b. In the **VM Storage Policy** field, select a storage policy.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

Note

[System requirements](#) on page 14 contains details about the disk requirements.

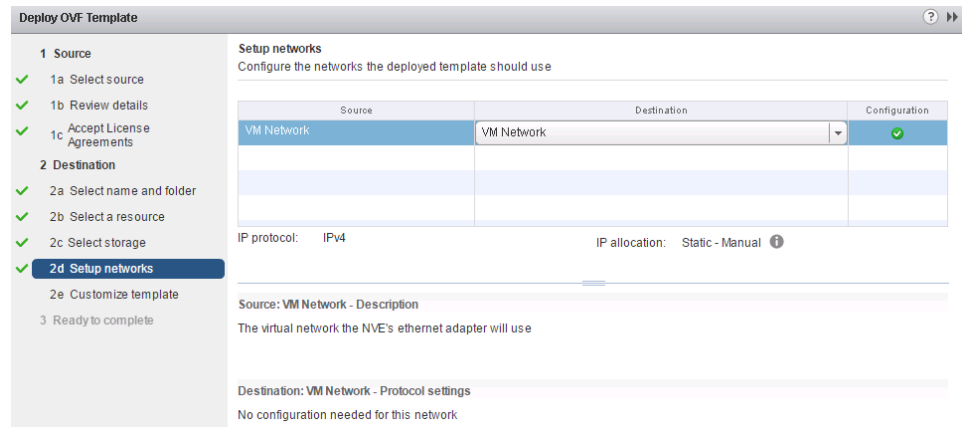
The following figure provides an example of the **Select storage** page with a **VNX** datastore selected.

Figure 6 Select storage page



11. On the **Setup networks** page, select the destination network, and then click **Next**.

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

Figure 7 Setup networks page

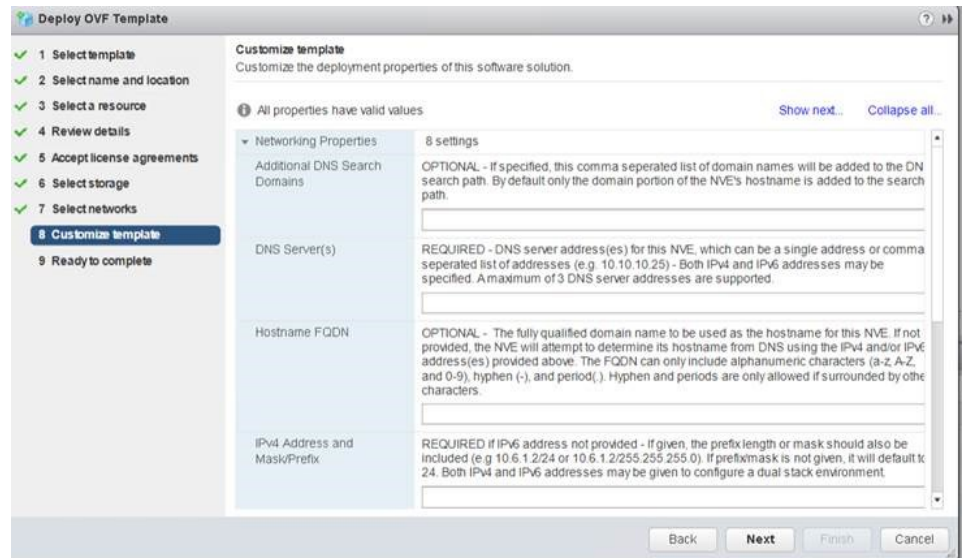
12. On the **Customize template** page, perform the following configuration tasks, and then click **Next**:
- In the **Additional DNS Search Domains** field, type additional DNS search domains, which are comma separated.
 - In the **DNS Server(s)** field, type the IP address of up to three DNS servers, which are comma separated.
 - In the **Hostname FQDN** field, type the fully qualified domain name (FQDN) for the NVE appliance.
 - In the **IPv4 Address and Mask/Prefix** field, type the IPv4 address and netmask for the NVE appliance.
 - In the **IPv4 Default Gateway** field, type the IPv4 address of the gateway host.
 - If deployed in IPv6 environment, in the **IPv6 Address and Prefix** field, type the IPv6 address and netmask for the NVE appliance.
 - If deployed in IPv6 environment, in the **IPv6 Default Gateway** field, type the IPv4 address of the gateway host.
 - In the **NTP Server(s)** field, type the NTP server name, which are comma separated.

Note

In the VMware deployment, ignore the VMC specific fields.

The following figure provides an example of the **Customize template** page.

Figure 8 Customize template page



13. On the **Ready to complete** page, confirm the deployment settings, select **Power on after deployment**, and then click **Finish**.

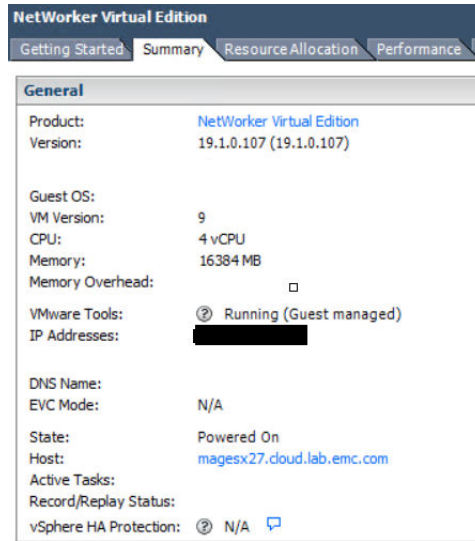
The deployment might take several minutes. After the deployment completes, the **Recent tasks** section of the vSphere Web Client displays the status of the **Deploy OVF template** task as **Completed**. The following figure provides an example of the **Recent Tasks** window after the deployment completes.

Figure 9 Recent Tasks

Recent Tasks		
Task Name	Target	Status
Deploy OVF template	NetWorker Virtual E...	✓ Completed
Initialize OVF deployment	bu-iddes	✓ Completed

14. In the vCenter console, browse to the **Hosts** window and select the NVE virtual machine. To monitor the progress of the installation, open the **Virtual Console**.
15. On the **Summary** tab, verify that the status for **VMware Tools** changes to **Running** or **Unmanaged**.

The following figure provides an example of the **Summary** tab where the status of **VMware Tools** is displayed as **Running**.

Figure 10 Summary tab**After you finish**

For information on configuring the NetWorker Virtual Edition, see the topic [Configuring the NetWorker Virtual Edition](#) on page 37

CHAPTER 3

Deploying the NetWorker Virtual Edition in Amazon EC2

This chapter includes the following topics:

- [Deploying the NetWorker Virtual Edition Appliance in Amazon EC2](#).....26

Deploying the NetWorker Virtual Edition Appliance in Amazon EC2

You can deploy the NetWorker Virtual Edition Appliance in Amazon EC2 By using the NVE Amazon Machine Image (AMI) image in the AWS marketplace.

Deploy NVE from the AWS Marketplace

The following topics describe how to deploy an NVE virtual machine by using the AMI image in the AWS Marketplace, and then prepare the virtual machine for NetWorker Virtual Edition software installation. This method saves time by eliminating the need to upload and convert an NVE virtual appliance file.

Before you can use the AMI image in the AWS Marketplace, you must subscribe to NVE and accept the software terms. Subsequent launches omit these steps.

The [AWS documentation](#) provides more information about subscribing to software and the different methods of deploying virtual machine instances.

Deploying the NVE Virtual Machine from AWS Marketplace

If you have already subscribed to the NVE marketplace image in the AWS Marketplace, the following instructions launch an instance of the NVE virtual machine from the EC2 dashboard.

Procedure

1. Open the [AWS EC2 Console](#) and select the correct region.
2. From the EC2 console dashboard, click **Launch Instance**.

The **Choose an Amazon Machine Image (AMI)** page appears.

3. Select the **AWS Marketplace** category.
4. Search the AWS Marketplace for `NetWorker Virtual Edition`, and then locate **NetWorker Virtual Edition 19.1**.
5. Click **Select**.

The **Choose an Instance Type** page appears.

6. For **Step 2: Choose an Instance Type**, select the correct instance type.

For more information on system requirement, see [System requirements](#) on page 14

7. Click **Add Storage** from the ribbon bar at the top of the page.
8. Click **Add New Volume**.

- For **Size**, type the size as per your requirement. [System requirements](#) on page 14 provides information about the required disk size.
- For **Volume Type**, because SSD volumes have better performance than volumes other volume types, NVE recommends **SSD** for all volumes. However, SSD volumes incur a larger cost to the customer. Customers should balance performance and budget when selecting the volume type.

Repeat this step for all required volumes.

9. Click **Step 6: Configure Security Group**. Create or select a security group.

Note

[Port requirements](#) on page 15 contains information about the required settings for security groups that are used with NVE on AWS.

10. Complete the rest wizard as appropriate. At **Step 7: Review Instance Launch**, select the key pair that you created in a previous step, then click **Launch Instance**.
 11. Before you can connect to the NetWorker Virtual Edition appliance, you must download the private key.
-

Note

Save the private key in a secure and accessible location. After the private key is created, you will be unable to download the private key again.

The NetWorker Virtual Edition appliance starts in Amazon EC2.

12. Change the NVE hostname from AWS assigned DNS to a custom DNS.
By configuring a custom DNS in AWS cloud, you can control the length of the NVE hostname. For best practices and recommendation on configuring DNS, see [Best Practices and Recommendations](#) on page 72
 - a. Login to the NVE using an SSH as an *admin* user.
-

Note

The default password is *the private ip* address of the NVE.

- b. Switch to super user by entering the command `sudo su`.
 - c. Update the `/etc/hosts` file with the custom FQDN and shortname.
 - d. Update the `/etc/resolve.conf` file with the Name Server and custom search DNS.
 - e. Update the `/etc/HOSTNAME` with new FQDN.
 - f. Restart the NVE using by the `reboot` command.
-

Note

You must run this procedure before taking the backup.

After you finish

Configure the NetWorker Virtual Edition. To configure NetWorker Virtual Edition, refer [Configuring the NetWorker Virtual Edition](#) on page 37

CHAPTER 4

Deploying the NetWorker Virtual Edition with Microsoft Azure Resource Manager

Use the procedures in this section to deploy NetWorker Virtual Edition with Microsoft Azure Resource Manager (ARM).

- [Deploying the NetWorker Virtual Edition Appliance in Microsoft Azure Resource Manager](#)30

Deploying the NetWorker Virtual Edition Appliance in Microsoft Azure Resource Manager

You can deploy the NetWorker Virtual Edition (NVE) from the Microsoft Azure marketplace.

Deploying the NVE Virtual Machine from Azure Marketplace

The NetWorker Virtual Edition (NVE) software is available in the Microsoft Azure marketplace.

Note

For security considerations, deploy NVE in a private network and configure a secure gateway from which you can install, configure, and manage the NetWorker server.

Procedure

1. Open the Azure portal at <https://portal.azure.com> and log in to the Azure account.
2. In the Azure Marketplace, search for NetWorker Virtual Edition and click the Dell EMC NetWorker Virtual Edition 19.1.
3. To start the NetWorker Virtual Edition Deployment wizard, click **Create**.
4. Configure the basic setting for the virtual machine:
 - a. In the **Name** field, type a name for the virtual machine.
 - b. In the **VM disk type** field, select **HDD**.
 - c. In the **User name** field, type a username.
 - d. In the **Authentication** type field, select one of the following options:
 - In the **SSH Public Key** field, type the public key.
 - In the **Password** field, type the password.
 - e. Verify the subscription information.
 - f. In the **Resource Group**, perform one of the following steps:
 - To create a resource group, click **Create new**.
 - To select a resource group, click **Use existing** and then select the resource group that you would like to use.
 - g. In the **Location** field, select a location to deploy the virtual machine.
 - h. Click **OK** to continue.
5. Choose the size of the virtual machine:
 - a. Select the **VM** size that you would like to deploy.
Refer to the [System requirements](#).
 - b. Click **Select** to continue.
6. Configure settings for the virtual machine.

- a. In the **Availability set** field, keep the default setting of **None**.
- b. In the **Storage** field, keep the default setting of **Yes**.
- c. In the **Virtual network** field, select an existing or create a new virtual network.
- d. In the **Subnet** field, select a subnet.
- e. In the **Public IP address** field, keep the default settings to create a Public IP address.
- f. In the **Network security group (firewall)** field, click **Advanced**, and select the Network security group to add inbound and outbound rules.

Table 6 Required inbound and outbound ports for NVE

Type	Priority	Name	Port	Protocol	Source	Destination	Action
Inbound	1000	TCP_inbound_rule_1	9000–9001	TCP	Any	Any	Allow
Inbound	1010	TCP_inbound_rule_2	8080	TCP	Any	Any	Allow
Inbound	1030	TCP_inbound_rule_3	22	TCP	Any	Any	Allow
Inbound	1060	TCP_inbound_rule_4	9090	TCP	Any	Any	Allow
Inbound	1100	TCP_inbound_rule_5	443	TCP	Any	Any	Allow
Inbound	1150	TCP_inbound_rule_6	7937–7954	TCP	Any	Any	Allow
Inbound	65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
Inbound	65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	Allow
Inbound	65500	DenyAllInBound	Any	Any	Any	Any	Deny
Outbound	1000	HTTPS	443	TCP	Any	Any	Allow
Outbound	65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
Outbound	65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
Outbound	65500	DenyAllOutBound	Any	Any	Any	Any	Deny

- g. In the **Extensions** field, keep the default setting of **No extensions**.
 - h. In the **Enable auto-shutdown** field, keep the default setting of **Off**.
 - i. In the **Boot diagnostics** field, keep the default setting of **Enabled**.
 - j. In the **Guest OS diagnostics** field, keep the default setting of **Disabled**.
 - k. In the **Diagnostics storage account** field, select an existing or create a storage account.
 - l. In the **Managed service identity** field, keep the default setting of **No**.
 - m. Click **OK** to continue.
7. Review the summary for the NetWorker Virtual Edition (NVE) and then click **Create**.

After launching the instance, the NVE initializes and restarts automatically. This process takes 15–25 minutes. You cannot configure NVE until this process is

complete because the NVE installation package, **NVE-config**, is not available. SSH is also unavailable during this time.

8. Create the data disks for NVE by performing the following steps:
 - a. From the disks configuration page for the virtual machine, click **Add data disk**.
 - b. In the **Name** drop-down list, click **Create new**.
 - c. Type a name for the data disk.
 - d. Select **Use existing** for **Resource Group** and select the resource group that you created in the previous step.
 - e. Select **Standard HDD** for **Account type**.
 - f. Select **None(empty disk)** for **Source type**.
 - g. Type the disk size according to the workload.

For more information about disk size, refer to the [System requirements](#)

9. Change the NVE hostname from Azure assigned DNS to a custom DNS.

By configuring a custom DNS in Azure cloud, you can control the length of the NVE hostname. For best practices and recommendation on configuring DNS, see [Best Practices and Recommendations](#) on page 72

- a. Login to the NVE using an SSH as an *admin* user.

Note

The default password is *the private ip* address of the NVE.

- b. Switch to super user by entering the command `sudo su`.
- c. Update the `/etc/hosts` file with the custom FQDN and shortname.
- d. Update the `/etc/resolve.conf` file with the Name Server and custom search DNS.
- e. Update the `/etc/HOSTNAME` with new FQDN.
- f. Restart the NVE using by the `reboot` command.

After you finish

Configure the NetWorker Virtual Edition. To configure NetWorker Virtual Edition, refer [Configuring the NetWorker Virtual Edition](#) on page 37

CHAPTER 5

Deploying NetWorker Virtual Edition in VMware Cloud Marketplace

This chapter includes the following topics:

- [Deploying the NetWorker Virtual Edition On VMC.....](#) 34

Deploying the NetWorker Virtual Edition On VMC

You can deploy the NetWorker Virtual Edition in the VMware Cloud Marketplace (VMC) by using the NVE image in the VMC.

Before you begin

You must have an account in the VMC.

Procedure

1. Right-click the Resource pool where you want to deploy the NVE appliance and select **Deploy OVF template**.

The **Deploy OVF Template** wizard is displayed.

2. On the **Select source** page, select one of the following options, and then click **Next**.
 - **URL**—Type the path to the OVA file.
 - **Local file**—Click **Browse**, and then search for the OVA file.
3. On the **Select a name and folder page** page, type a descriptive name for the NVE, select the inventory location, and then click **Next**.
4. On the **Review details** page, verify the details about the template, and then click **Next**.
5. On the **End User License Agreement** page, if you agree to the license terms, click **Accept**, and then click **Next**.
6. On 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** field, select a storage policy.
 - c. In the **Storage** table, select the datastore for NVE.
 - d. Click **Next**

Note

[System requirements](#) on page 14 contains details about the disk requirements.

7. On the **Setup networks** page, select the destination network, and then click **Next**.
8. On the **Customize template** page, perform the following configuration tasks, and then click **Next**:
 - a. In the **Additional DNS Search Domains** field, type additional DNS search domains, which are separated by commas.
 - b. In the **DNS Server(s)** field, type the IP address of up to three DNS servers, which are separated by commas.
 - c. In the **Hostname FQDN** field, type the fully qualified domain name (FQDN) for the NVE appliance.

- d. In the **IPv4 Address and Mask/Prefix** field, type the IPv4 address and netmask for the NVE appliance.
 - e. In the **IPv4 Default Gateway** field, type the IPv4 address of the gateway host.
 - f. If deployed in IPv6 environment, in the **IPv6 Address and Prefix** field, type the IPv6 address and netmask for the NVE appliance.
 - g. If deployed in IPv6 environment, in the **IPv6 Default Gateway** field, type the IPv4 address of the gateway host.
 - h. In the **NTP Server(s)** field, type the NTP server name, which are separated by commas.
 - i. In the **NVE Timezone** field, select the NVE timezone. UTC is selected by default.
 - j. In the **DD IP Address** field, type the IP address of a working Data Domain.
 - k. In the **DDBoost use existing username** field, select **yes** if you are using an existing DDBoost username. By default, **No** is selected
 - l. In the **DDBoost username** field, type an unique or existing username for the Data Domain.
 - m. In the **vCenter FQDN** field, type the FQDN or IP address of a working vCenter.
 - n. In the **vCenter username** field, type an unique or existing username for the Data Domain and click **Next** .
9. On the **Ready to complete** page, confirm the deployment settings, and then click **Finish**.

After you finish

For information on configuring the NetWorker Virtual Edition, see the topic [Configuring the NetWorker Virtual Edition](#) on page 37

CHAPTER 6

Configuring the NetWorker Virtual Edition

This chapter includes the following topics:

- [Setting up the NetWorker software on NVE](#)..... 38
- [Launching the NetWorker Management Web UI](#)..... 40
- [Starting the NMC server GUI for the first time](#).....41
- [Configuring sendmail and NetWorker notifications](#)..... 45
- [Upgrade the NVE appliance using GUI](#)..... 49
- [Upgrading the NVE using CLI](#)50

Setting up the NetWorker software on NVE

The NVE appliance includes an installation manager that prompts you for environment-specific information, such as passwords, and then automatically installs of the NetWorker server software.

Before you begin

For Azure and AWS instances, you must know the private IP address of the NVE appliance.

To set up the NetWorker software on a new NVE appliance, perform the following steps:

Procedure

1. On a host that has network 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 appliance.

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 **NetWorker Installation Manager** login page appears.

2. In the **User** field, type `root`.
3. In the **Password** field, type the default password.

Note

- The default password for NVE running on
 - a. VMware vSphere is *changeme*
 - b. Azure or AWS is the *private ip* address of the NVE
 - The default password expiration policy on the NVE is once every 60 days. If the password that you specify has expired, a messages similar to the following appears: `Error "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.
-

4. Click **Login**.
5. On the **SW upgrades** tab, to the right of the NveConfig package, click **Install**.
The installation initialization begins. The initialization extracts files from the package and prepares the environment for the installation. The process can take a few minutes. After the initialization completes, the **Installation Setup** page appears.
6. On the **Authc Settings** tab, specify the following attributes:
 - a. In the **Tomcat KeyStore Password** and **Tomcat KeyStore password (Confirm)** fields, 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 **Authc Password** and **Authc Password (confirm)** fields, type a password for the NetWorker Authentication Service administrator account.

Ensure the password complies with the following minimum requirements:

- Nine characters long
- 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.

- c. Click **Save**.

7. (Optional) To install additional language packs, on the **NetWorker Settings** tab, from the **Value** list, select the language pack, and then click **Save**.
8. On the **Passwords** tab, and specify the OS admin user and OS root user passwords, and then click **Save**.

Ensure that the passwords comply with the following minimum requirements:

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

9. On the **Server Settings** tab, from the **Value** list, select the time zone for the appliance, and then click **Save**.
10. (Optional) To configure Data Domain devices in the NetWorker datazone, on the **Data Domain Settings** tab, select 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 a 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 or existing name for a folder that you want to use for DD Boost storage.

The installation process automatically creates a Storage Unit (SU) and folder for the appliance in the hidden mount point folder, `/data/col1`. Do not modify this folder structure, which all NetWorker server hosts use.

- e. (Optional) To create a DD Boost account, select **DDBoost create new login account**.

- f. In the **Data Domain Login** field, type the account for the DD Boost user.
 - g. In the **DDBoost Login Password** field, type the password for the DD Boost user that you specified in the **Data Domain Login** field.
-

Note

The DD Boost user that you specify must have an assigned role that is not *none*.

- h. In the **DDBoost Login Password Confirm** field, type the password for the DD Boost user that you specified in the **Data Domain Login** field.
- i. Click **Save**.
- j. To specify the SNMP community string to monitor the Data Domain system, on the **NetWorker Settings** tab, in the **SNMP Community String** field, type the string value. Click **Save**.

The default SNMP Community String on a Data Domain system is *Public*.

11. (Optional) To install or upgrade the password hardening package, on the **Security Settings** tab, select **Show advanced settings**, and then select the box in the **Value** column. Click **Save**.
12. Click **Continue**.

The **Installation Progress** window appears and displays information about the status of the installation actions. The **Information Log** pane displays messages about the status of each task. To generate a file that contains each message, click **Export**, and then select **Excel** to export the information to an Excel spreadsheet or select **PDF** to export the information to a PDF file.

Results

The EMC NetWorker Installation Manager installs the NetWorker, NMC server software and the NetWorker Management Web UI on the NVE appliance.

After you finish

Install and configure the Dell EMC License Server on a host in the datazone that the NetWorker server can access. *NetWorker Licensing Guide* provides more information.

Launching the NetWorker Management Web UI

The NetWorker Management Web UI, introduced in NetWorker 18.2, is a web-based management interface that provides support for the following NetWorker VMware-integrated operations:

- Managing VMware vCenter servers
- Managing VMware Proxies
- Installing the vCenter Plugin
- Recovering virtual machines
- Monitoring recovery operations

The following table provides more information on the functionality available in the NetWorker Management Web UI.

Table 7 Supported operations in the NetWorker Management Web UI

Operation	Description
Protection	VMware vCenter servers <ul style="list-style-type: none"> • Manage vCenter servers. • Refresh and view the vCenter inventory. • View properties of entities in the vCenter Inventory tree.
	VMware vProxies <ul style="list-style-type: none"> • Manage vproxies. • Monitor progress of vProxy registration.
Recovery	Recover virtual machines. Supports both image-level and file-level recovery.
Monitoring	<ul style="list-style-type: none"> • View and monitor the progress of virtual machine recovery; includes the list of completed and currently running recover jobs. • View recover logs.

You can log in to the NetWorker Management Web UI by using following link:

[https:// <IP_address_or_hostname>.9090/nwui](https://<IP_address_or_hostname>.9090/nwui)

The *NetWorker VMware Integration Guide* provides more information on how to use the NetWorker Management Web UI to perform the supported tasks.

Supported browsers

The NetWorker Management Web UI supports the following browsers:

- Microsoft Internet Explorer 11
- Google Chrome
- Microsoft Edge
- Mozilla Firefox

Starting the NMC server GUI for the first time

The NMC server is a web-based Java 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

You cannot connect to the NMC GUI with any of the following, previously supported, operating systems:

- AIX
- HP-UX

- Solaris

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

Note

Post-upgrade, the maximum heap memory configuration resets to default minimum value of the NetWorker. For information on configuration for the scaled setup, see the *Performance Optimization Planning Guide*.

Enable temporary internet file caching

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

For Windows NMC clients:

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

For UNIX NMC clients:

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

Confirm JRE and Internet Explorer compatibility (Windows only)

For Windows hosts only, ensure that you install the 64-bit JRE program for the 64-bit version of Microsoft Internet Explorer (IE).

To determine the Microsoft Internet Explorer version on the Windows NMC client, perform the following steps.

Procedure

1. Right-click the Microsoft Internet Explorer shortcut and select **Properties**.
2. Review the **Target Location** field.

The **Target Location** is the following path:

64-bit IE—`C:\Program Files\Internet Explorer\`

Add 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.

Note

These changes are not required if you are using NMC Launcher. For more information on installing NMC launcher, see *NetWorker Runtime Environment Readme Guide*

Procedure

1. Open the **Java Control Panel**.
2. On the **Security** tab, click **Edit Site list**.
3. Click **Add**.

- In the **Location** field, specify the URL to the NMC server in the format `https://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:

```
https://ip_address:9000
```

- Click **OK**.
- In the **Security Warning** window, click **Continue**.
- Click **OK**.

Launching the NetWorker Management 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 *NetWorker Security Configuration Guide* describes how to configure the NetWorker Authentication Service to use LDAP or AD for user authentication.

Procedure

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

```
https://server_name:https_service_port
```

where:

- server_name* is the name of the NMC Server.
- https_service_port* is the port for the embedded HTTP server. The default https port is 9000.

For example: `https://houston:9000`

The `gconsole.jnlp` file downloads to the host. When the download completes, open the file.

- Optional, associate the `jnlp` file with a program.

When you use Mozilla Firefox on Windows, and the `jnlp` extension is not associated with Java, you are prompted to choose the program that opens the `jnlp` file. In the dialog box that appears, select **Open with**, and then select `Java (TM) Web Start Launcher`. If this application does not appear, browse to the Java folder and select the `javaws.exe` file.

- On the **Welcome** page, click **Start**.

Note

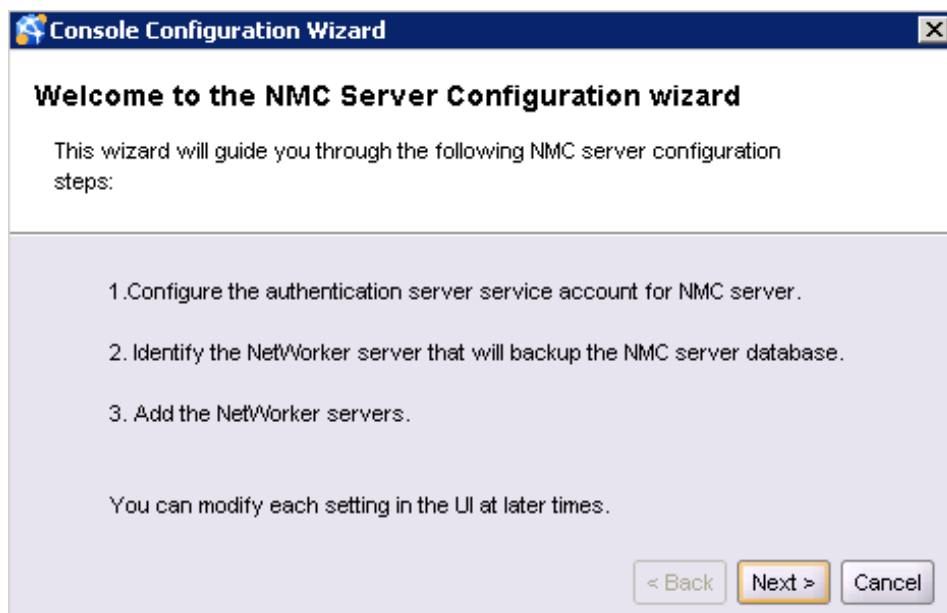
If the **Start** button does not appear but you see a warning message that states that Java Runtime Environment cannot be detected, click the **here** hyperlink.

- For Internet Explorer only, if a security warning appears, select **I accept the risks and want to run this application**, and then click **Run**.

5. On the **Log in** page, specify the NetWorker Authentication Service administrator username and password, and then click **OK**.
6. On the **Licensing Agreement** page, select **Accept**.
7. If you did not install a supported version of JRE on the host, then a dialog box that prompts you to install JRE appears. Cancel the application installation, install JRE, and then rerun the application installation.
8. On the **Welcome to the NMC Server Configuration Wizard** page, click **Next**.

The following figure shows the **Welcome to the NMC Server Configuration Wizard** page.

Figure 11 Welcome to the NMC Server Configuration Wizard page



9. On the **Specify a list of managed NetWorker Servers** page:
 - a. Specify the names of the NetWorker Servers that the NMC Server will manage, one name per line.

Note

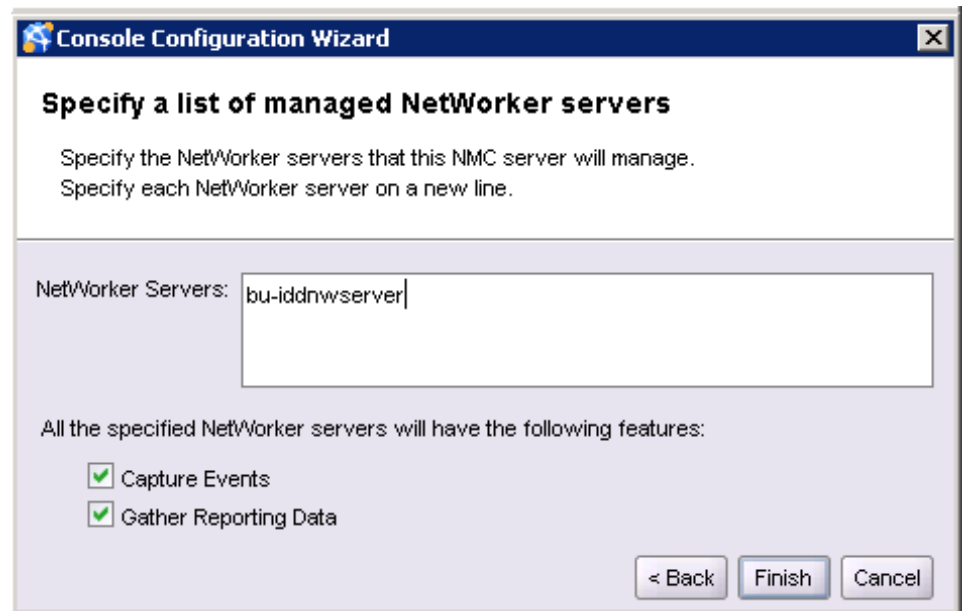
If the NMC Server is also the NetWorker Server, specify the name of the NetWorker Server.

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

Consider the following options:

- To allow the NMC Server to monitor and record alerts for events that occur on the NetWorker Server, select **Capture Events**.
- To allow the NMC Server to collect data about the NetWorker Server and generate reports, select **Gather Reporting Data**.

The following figure shows the **Specify a list of managed NetWorker servers** page.

Figure 12 Specify a list of managed NetWorker servers page

10. Click **Finish**. The installation starts the default web browser and connects to the NMC server. The **NetWorker Management Console** and **Getting Started** windows 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** page, the NMC **Enterprise** window does not display any NetWorker Servers. To add a host, in the left navigation pane, right-click **Enterprise**, and then click **New > Host**. The **Add New Host** wizard appears.

After you finish

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

Configuring sendmail and NetWorker notifications

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

The *NetWorker Administration Guide* provides more information about server notifications and how to configure notifications when you create the Policy, Workflow and Action resources.

Configure the sendmail application

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

Before you begin

The `sendmail` application is an SMTP Mail Transfer Agent, not an SMTP server. To use the `sendmail` application, the environment must have a configured SMTP relay host, which the NVE will use to send email messages.

Procedure

1. Connect to the NVE.

If you connect by using the vSphere client to open a VM Console session, 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` file, and change the line `SENDMAIL_SMARTHOST=""` to include the hostname of the SMTP relay host.

For example:

```
SENDMAIL_SMARTHOST="mysmtp_relay.corp.com"
```

5. Restart the `sendmail` service. At the command prompt, type the following command:

```
service sendmail restart
```

6. Test the connection to the SMTP relay host.

For example, at the command prompt, type the following command:

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

When the test succeeds, output similar to the following example appears:

```
debbied@email.com... Connecting to [127.0.0.1] port 25 via
relay...
220 bu-idd-nve.iddlab.local ESMTP Sendmail 8.14.3/8.14.3/
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-SIZE
250-DSN
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
>>> RCPT To:<debbied@email.com>
>>> DATA
250 2.1.5 <debbied@email.com>... Recipient ok
354 Enter mail, end with "." on a line by itself
>>> .
250 2.0.0 u93Eaws2014693 Message accepted for delivery
debbied@email.com... Sent (u93Eaws2014693 Message accepted
for delivery)
Closing connection to [127.0.0.1]
>>> QUIT
221 2.0.0 bu-idd-nve.iddlab.local closing connection


```

Configuring NetWorker to send operation notifications by email

By default, NetWorker writes operation notifications to log files.

To configure NetWorker to send system notifications to email recipients, perform the following steps:

Procedure

1. On the taskbar, click the **Enterprise** icon .
2. In the navigation tree, highlight a host:
 - a. Right-click **NetWorker**.
 - b. 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. In the **Action** field, specify the `mail` command in the following format:

```

/usr/bin/mail -s "subject_text" recipient_email
where:

```

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

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

```


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

```

Edit policy notifications

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

Procedure

1. On the taskbar, click the **Enterprise** icon .
2. In the navigation tree, highlight a host:

- a. Right-click **NetWorker**.
- b. 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 type the `mail` command in the following format:


```
/usr/bin/mail -s "subject_text" recipient_email
```

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

Edit workflow notifications

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

Procedure

1. On the taskbar, click the **Enterprise** icon .
2. In the navigation tree, highlight a host:
 - a. Right-click **NetWorker**.
 - b. 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 then select **Properties**.
6. In the **Command** field, type the `mail` command in the following format:

```
/usr/bin/mail -s "subject_text" recipient_email
```

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

Edit action notifications

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

Procedure

1. On the taskbar, click the **Enterprise** icon .

2. In the navigation tree, highlight a host:
 - a. Right-click **NetWorker**.
 - b. 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. In 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** page.
8. In the **Command** field, type the `mail` command in the following format:


```
/usr/bin/mail -s "subject_text" recipient_email
```

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

Upgrade the NVE appliance using GUI

The installation manager automates the upgrade process on an NVE appliance.

Before you begin

NVE appliance should updated with the latest security update. For more information, see [Performing NVE appliance Security Rollup Update](#) on page 54

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

Procedure

1. Download the NetWorker 9.1 Virtual Edition Upgrade file (*.avp) from <http://support.emc.com>.

Note

For NVE version 9.x, use a file transfer program to copy the AVP file to the `/data01/avamar/repo/packages` folder on the NVE appliance.

For more information on enabling SSH for root, refer the topic [Enable SSH for root](#)

2. Open a web browser and type the following URL:

```
https://NVE_address
```

Where *NVE_address* is the hostname or IP address of the NVE appliance.

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 **NetWorker Installation Manager** login page appears.

3. In the **User** field, type `root`.
4. In the **Password** field, type the password for the root account.
If you are upgrading from NVE version 9.x, then skip to [Step 6](#)
5. On the **Repository tab**, in the **Package upload** field, upload the AVP file.
The NVE upgrade package is listed in the **Packages in Repository** section.
6. On the **SW upgrades** tab, to the right of the NveConfig package, click **Install**.
The **Installation Setup** page appears.
7. Click **Continue**.
8. When the upgrade completes, to connect to the NMC server, click **Launch NMC**.

After you finish

- After upgrading the NVE, you should revert the changes made to the `ssh_config` file.
- When you upgrade NVE running on Microsoft Azure to the latest version, the Azure Linux agent version remains unchanged. You must manually update the Azure Linux agent.

Upgrading the NVE using CLI

You can upgrade the NetWorker Virtual Edition(NVE) by using the command line interface.

Before you begin

NVE appliance should updated with the latest security update. For more information, see [Performing NVE appliance Security Rollup Update](#) on page 54

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

Procedure

1. Download the NetWorker 19.1 Virtual Edition Upgrade file (*.avp) from <http://support.emc.com>.
2. Use a file transfer program to copy the AVP file to the `/data01/avamar/repo/packages/` folder on the NVE appliance.

For more information on enabling SSH for root, refer the topic [Enable SSH for root](#)

3. List the software package by running the command `avi-cli <server_ipaddress> --password <password> -- supportkey <supportkey> -- listcategories <"SW Upgrades">`
4. Run the command `avi-cli <server_ipaddress> --password <password> --install <package>`

The following command upgrades the NVE to NVE 19.x:

```
avi-cli 10.x.x.10 --password Root_Password --install NveUpgrade-19.x
```

After you finish

- After upgrading the NVE, you should revert the changes made to the `ssh_config` file.
- When you upgrade NVE running on Microsoft Azure to the latest version, the Azure Linux agent version remains unchanged. You must manually update the Azure Linux agent.

CHAPTER 7

Maintenance

This chapter includes the following topics:

- [Performing NVE appliance Security Rollup Update](#)..... 54
- [Password maintenance](#)..... 54
- [Change the storage disk configuration](#)..... 56

Performing NVE appliance Security Rollup Update

The installation manager automates the operating system rollup update an NVE appliance.

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

Procedure

1. Download the NVE platform OS Security Rollup package from <http://support.emc.com>.

Note

For NVE version 9.x, use a file transfer program to copy the AVP file to the `/data01/avamar/repo/packages` folder on the NVE appliance.

For more information on enabling SSH for root, refer the topic [Enable SSH for root](#)

2. Open a web browser and type the following URL:

`https://NVE_address`

Where *NVE_address* is the hostname or IP address of the NVE appliance.

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 **NetWorker Installation Manager** login page appears.

3. In the **User** field, type `root`.
4. In the **Password** field, type the password for the root account.
If you are upgrading from NVE version 9.x, then skip to [Step 6](#)
5. On the **Repository** tab, in the **Package upload** field, upload the AVP file.
The NVE Platform OS Security Rollup package is listed in the **Packages in Repository** section.
6. On the **SW Updates** tab, to the right of the NVE OS rollup package, click **Install**.

The installation initialization begins. The initialization extracts files from the package and prepares the environment for the installation. The process can take a few minutes. After the initialization completes, the **Installation Setup** page appears. In the **Password** field, type the password for the root account.

7. Click **Continue**.

Password maintenance

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

Review password policies

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

Procedure

1. Connect to the NVE, and perform the following tasks from a prompt.

Note

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 example 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 8 chage output

Option	Definition
Minimum	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.
Maximum	Defines the maximum numbers of days that a password remains valid, after which a password change is required.
Inactive	Defines the number of days that a user account can remain inactive after the password has expired and before the user account is locked out of the system. When this value is -1, the inactive feature is disabled.
Last change	Displays the date that the password was last changed.

Table 8 chage output (continued)

Option	Definition
Password expires	Defines the date that the current password will expire.
Password inactive	Defines the date that the current password will become inactive.
Account expires	Defines the date that the user account will expire.

Modify passwords

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

Perform the following steps to change the passwords.

Procedure

1. Connect to the NVE, and perform the following tasks from a prompt.

Note

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
```

Change the storage disk configuration

Perform the following steps to configure the NVE to support higher-performing and larger capacity datastores.

Procedure

1. From the virtual machine console of the NVE appliance, perform the following configuration tasks:

- a. Use the `su` command to change to the root account.

- b. Stop the NetWorker and NMC daemons:

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

- c. Confirm that the NetWorker daemons are not running:

```
/etc/init.d/networker status
```


Output similar to the following example appears when the daemons are not running:

```
nsr_shutdown: There are currently no running NetWorker processes.
```

d. Disable NetWorker:

```
chkconfig gst off networker off
```

2. In the Vsphere Web Client, perform the following configuration tasks:

- a. Right-click the appliance and select **Edit Settings**.
- b. From the **New Device** list, select **New Hard Disk**, and then click **Add**.
- c. Expand **New Hard disk**.
- d. In the **Size** field, type the size of the disk.
- e. In the **Disk Provisioning** field, leave **Thick provision lazy zero**.
- f. In the **Disk Mode** list, select **Independent - Persistent**.
- g. Click **OK**.

3. From the virtual machine console of the NVE appliance, perform the following configuration tasks:

a. Rescan the SCSI devices, by typing the following command:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
```

b. Verify that the new `/dev/sdc` disk appears on the system, by typing the following command:

```
ls /dev/sd*
```

Output similar to the following example appears:

```
/dev/sda /dev/sda1 /dev/sda2 /dev/sda3 /dev/sda4 /dev/sda5 /dev/sda6 /dev/sda7 /dev/sda8 /dev/sdb /dev/sdb1 /dev/sdc
```

c. Partition the new disk.

For example, type the following command:

```
parted -a minimal -s -- /dev/sdc mklabel msdos mkpart p ext3
ls -ls
```

d. Rescan the partition table, by typing the following command:

```
partprobe
```

e. Confirm that the new disk partition `/dev/sdc1` appears, by typing the following command:

```
ls /dev/sd*
```

Output similar to the following appears:

```
dev/sda /dev/sda1 /dev/sda2 /dev/sda3 /dev/sda4 /dev/sda5 /dev/sda6 /dev/sda7 /dev/sda8 /dev/sdb /dev/sdb1 /dev/sdc /dev/sdc1
```

f. Create a file system on the `/dev/sdc1` partition, by typing the following command:

```
mkfs.ext3 /dev/sdc1
```

- g. Mount `/dev/sdc1`, by typing the following command:

```
mkdir /tmpmnt mount/dev/sdc1 /tmpmnt
```

- h. Stop the `avinstaller`, by typing the following command

```
avinstaller.pl --stop
```

- i. Copy the contents from the old disk to the new disk, by typing the following command:

```
cp -rfp /data01/* /tmpmnt/
```

- j. Relabel the old and new disks, by typing the following command:

```
e2label /dev/sdb1 dataold
e2label /dev/sdc1 data01
```

- k. Power off the NVE, by typing the following command:

```
poweroff
```

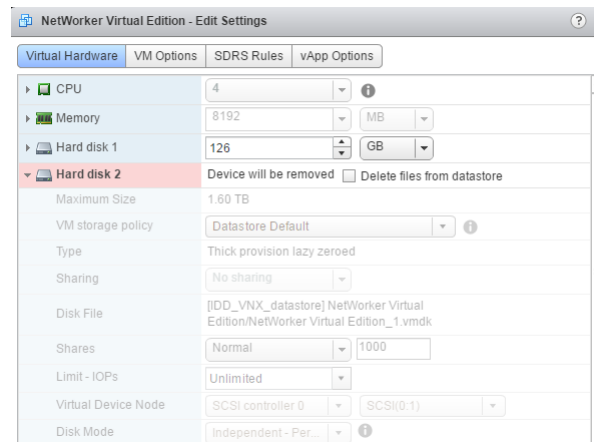
4. After the NVE power off completes, use the vSphere Web Client to perform the following configuration tasks:

- a. Right-click the appliance, and then select **Edit Settings**.

- b. Hover over Hard disk 2, and then click **X**, do not select **Delete files from datastore**. Click **OK**.

The following figure shows the **Edit Settings** screen, when the system deletes the disk device.

Figure 13 Deleting a disk device



- c. Right-click the virtual machine and select **Power > Power On**.

5. From the VM console of the NVE appliance, perform the following configuration tasks:

- a. Type `mount` and verify that disk `/dev/sdc1` is mounted on `/data01`.

For example, the `mount` output would include the following line:

```
/dev/sdc1 on /data01 type ext3 (rw,noatime)
```

- b. Confirm that the `avinstaller` is started:

```
avinstaller.pl --test
```

Output similar to the following example appears when the `avinstaller` has started:

```
Avistart process: 3311
```

- c. Enable NetWorker and NMC, by typing the following commands:

```
chkconfig networker on
chkconfig gstd on
```

- d. Start the NetWorker and NMC daemons, by typing the following commands:

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

- e. Confirm that the NetWorker daemons have started, by typing the command below, based on the initialization system running on your Linux machine: `/etc/init.d/networker status`

Note

Before you run this command, wait several minutes for the daemons to start.

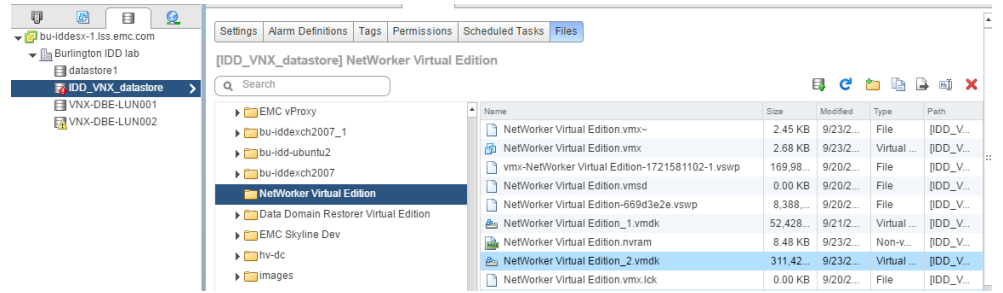
For a NetWorker server, the `nsrctld` daemon starts. The `nsrctld` daemon starts other processes that the NetWorker server requires. Output similar to the following example appears when the daemons are started:

```
+--o nsrctld (29021)
  +--o epmd (29029)
  +--o rabbitmq-server (29034)
    +--o beam (29038)
      +--o inet_gethost (29144)
        +--o inet_gethost (29145)
  +--o jsvc (29108)
    +--o jsvc (29114)
  +--o nsrd (29123)
    +--o java (29135)
    +--o nsrmdbd (29828)
    +--o nsrindexd (29842)
    +--o nsrdispd (29853)
    +--o nsrjobd (29860)
    +--o nsrvmsd (29968)
  +--o eventservice.ru (29154)
    +--o jsvc (29158)
      +--o jsvc (29159)
  +--o java (29838)
    +--o node-linux-x64- (29885)
+--o nsrexecd (29004)
  +--o nsrlogd (29899)
  +--o nsrsnmd (30038)
```

6. Perform a backup and recovery operation. If NetWorker operations succeed, use the vSphere Web Client to delete the old VMDK file:
- Browse to the datastore that contains the VM files and expand the NVE folder.
 - Select the VMDK file, `VM_name_2.vmdk`, and then click **X**.

The following figure provides an example of the expanded NVE folder with the old VMDK file selected.

Figure 14 Deleting the old VMDK file



CHAPTER 8

Configuring Firewall

This chapter includes the following topic:

- [NetWorker Virtual Edition firewall](#)..... 62
- [Editing the Firewall in NVE](#)..... 62
- [Configuring the NVE firewall](#)..... 63

NetWorker Virtual Edition firewall

The host level firewall can be configured in NetWorker Virtual Edition using a firewall daemon called `entfirewall`.

The firewall controls the access to all inbound and outbound ports in NVE. When a change is made to the firewall rule, restart `entfirewall` to load the new configuration.

The NetWorker firewall daemon uses the rules in `/etc/entfirewall.base`.

Editing the Firewall in NVE

Edit the status of the NVE firewall.

Firewall edit functionality allows the user to open and close nondependent ports for customized data transfer and to modify associated rules. Rules and ports can be initiated, edited, and terminated through manual configuration of a designated text file, executing those changes, and then restarting the firewall on the NVE server. Editing the firewall is essentially understanding the content of the config file, editing that content, and then executing those changes.

Procedure

1. Log in as root.
Type the password.
2. Change the working directory to the following: `/usr/local/avamar/lib/admin/security`.
3. Open `entfwb_custom_config.txt` in a plain text editor.
See section below for config file example and how to edit the file.
4. Save and close the file.
5. Run the following command: `sh ent-manage-custom-rules.sh --execute-rules`.
This command applies the new firewall rules to the system and restarts the firewall.
6. Exit the command session.

The firewall customization lines that you add to the `entfwb_custom_config.txt` file must be structured in a pipe-delimited fashion such as the following:

Source IP | Source Port | Destination IP | Destination Port | Protocol | ICMP-type | Target | Chain | Run Order

where:

Table 9 Firewall customization

Section	Description
Source IP	Source specification - address can be a network IPv4 or IPv6 address (with or without /mask) .

Table 9 Firewall customization (continued)

Section	Description
Source Port	Port of origin for traffic.
Destination IP	IP address of destination machine.
Destination Port	Destination port or port range specification.
Protocol	TCP, UDP, or ICMP.
ICMP-type	If ICMP is entered for Protocol, enter the type.
Target	ACCEPT, REJECT, DROP, or LOGDROP.
Chain	INPUT, OUTPUT, or LOGDROP
Run Order	<ul style="list-style-type: none"> • A - Append: It the default behavior of the Run Order. It can also be a blank, with or without the “ ” • i - Insert: Inserts the rule before the Run Order.

If a field does not apply, leave the field blank.

Miscellaneous information

To delete all firewall rules, delete the rules in `entfwb_custom_config.txt` and run `sh ent-manage-custom-rules.sh --execute-rules` again.

For diagnostic purposes, the log file is located in `/var/log/custom-firewall`.

To view the current state of the firewall iptable on the utility node or a single-node server, run the following command: `iptables -L -4` (for ipv4) or `iptables -L - 6` (for ipv6).

Configuring the NVE firewall

Use the following instructions to open or close particular ports in the nve firewall, or restrict access to a particular IP address.

Users should be familiar with the operation of `iptables`, including order of precedence, before creating custom firewall rules.

Opening a firewall port

If the NVE server is a dual-stack configuration, repeat this task to create rules for both addressing systems.

Procedure

1. Open a command shell:
 - a. Log in as the Admin.
 - b. Switch user to root by typing `su -`.
2. Change directory by typing the following command:

```
cd /usr/local/avamar/lib/admin/security
```

3. Run the firewall rules script by typing the following command:

```
sh ent-edit-firewall-rules.sh
```

The following output appears:

```
Choose an Action
-----
1) Add a custom rule
2) Remove a custom rule
3) List Current Custom Rules
4) Exit
5) Save Changes
Enter desired action:
```

4. Type **1** to add a custom rule and press **Enter**.

The following output appears:

```
Firewall Rule Types
-----
1) IPv4 Rule
2) IPv6 Rule
Enter Firewall Rule Type:
```

5. Type the number that corresponds to the addressing system in use and press **Enter**.

The following output appears:

```
Firewall Chains
-----
1) OUTPUT
2) INPUT
3) LOGDROP
4) FORWARD
Select Chain:
```

6. Type **1** to add an output rule or **2** to add an input rule and press **Enter**.

The following output appears:

```
Protocol
-----
1) TCP
2) UDP
3) ICMP
Enter Protocol:
```

7. Type the number that corresponds to the required protocol and press **Enter**.

The following output appears:

```
Enter source IP (leave blank for none):
```

8. For outbound connections, perform the following substeps:

- a. Type the IP address of this NVE server and press **Enter**.

The following output appears:

```
Enter source port (leave blank for none):
```

- b. Type the number of the port to open and press **Enter**.

The following output appears:

```
Enter Destination IP Address (leave blank for none):
```

- c. Leave this field blank and press **Enter**.

If you want to restrict connections to a particular IP address, type the IP address instead and press **Enter**.

The following output appears:


```
Enter Destination Port (leave blank for none):
```

- d. Leave this field blank and press **Enter**.

The following output appears:

```
Targets
-----
1) ACCEPT
2) REJECT
3) DROP
4) LOGDROP
Select Target:
```

9. For inbound connections, perform the following substeps:

- a. Leave this field blank and press **Enter**.

If you want to restrict connections to a particular IP address, type the IP address instead and press **Enter**.

The following output appears:

```
Enter source port (leave blank for none):
```

- b. Leave this field blank and press **Enter**.

The following output appears:

```
Enter Destination IP Address (leave blank for none):
```

- c. Type the IP address of this NVE server and press **Enter**.

The following output appears:

```
Enter Destination Port (leave blank for none):
```

- d. Type the number of the port to open and press **Enter**.

The following output appears:

```
Targets
-----
1) ACCEPT
2) REJECT
3) DROP
4) LOGDROP
Select Target:
```

10. Type **1** to allow packets for the specified port and press **Enter**.

The following output appears:

```
Run Order
-----
I) Insert (Inserts rule before default AV Firewall rules are
applied)

A) Append (Standard behavior. Rule is appended, with default AV
Firewall rules taking precedent)

Select run order for this rule [A]:
```

11. Type the number that corresponds to the Run order and press **Enter**.

Unless otherwise indicated by the tables in this appendix, most ports only require the utility node.

Output similar to the following appears:

```
Add rule <IP Address>|Port Number|<IP Address>|Port Number|tcp|
ACCEPT|OUTPUT|A
to custom rules file? (Y/N):
```

12. Type **y** to save the new rule and press **Enter**.

The script writes the new rule to `entfwb_custom_config.txt`.

Output similar to the following appears:

```
Adding <IP Address>|Port Number|<IP Address>|Port Number|tcp||
ACCEPT|OUTPUT|A
to pending actions...
Add another firewall rule? (Y/N):
```

13. If you require more rules, type **y** and press **Enter**. Otherwise, type **n** and press **Enter**.

The following output appears:

```
Return to main menu? (Y/N):
```

14. Type **n** and press **Enter**.

The following output appears:

```
Save and execute rules now? (Y/N):
```

15. Type **y** to save the new firewall rules and press **Enter**.

The script saves the new rules to the system firewall tables and automatically restarts the NVE firewall, then exits.

Output similar to the following appears:

```
Rules have been saved to /usr/local/avamar/lib/admin/security/
entfwb_custom_config.txt

Applying rule /usr/sbin/iptables -A OUTPUT -p tcp -s <IP
Address> -d <IP Address> --dport 11
-j ACCEPT
```

Closing a firewall port

If the NVE server is a dual-stack configuration, repeat this task to create rules for both addressing systems.

Procedure

1. Open a command shell:
 - a. Log in as the Admin.
 - b. Switch user to root by typing `su -`.
2. Change directory by typing the following command:


```
cd /usr/local/avamar/lib/admin/security
```
3. Run the firewall rules script by typing the following command:

```
sh ent-edit-firewall-rules.sh
```

The following output appears:

```
Choose an Action
-----
1) Add a custom rule
2) Remove a custom rule
3) List Current Custom Rules
4) Exit
5) Save Changes
Enter desired action:
```

4. Type **1** to add a custom rule and press **Enter**.

The following output appears:

```
Firewall Rule Types
```

```
-----
1) IPv4 Rule
2) IPv6 Rule
Enter Firewall Rule Type:
```

5. Type the number that corresponds to the addressing system in use and press **Enter**.

The following output appears:

```
Firewall Chains
```

```
-----
1) OUTPUT
2) INPUT
3) LOGDROP
4) FORWARD
Select Chain:
```

6. Type **1** to add an output rule or **2** to add an input rule and press **Enter**.

The following output appears:

```
Protocol
```

```
-----
1) TCP
2) UDP
3) ICMP
Enter Protocol:
```

7. Type the number that corresponds to the required protocol and press **Enter**.

The following output appears:

```
Enter source IP (leave blank for none):
```

8. For outbound connections, perform the following substeps:

- a. Leave this field blank and press **Enter**.

The following output appears:

```
Enter source port (leave blank for none):
```

- b. Type the number of the port to close and press **Enter**.

The following output appears:

```
Enter Destination IP Address (leave blank for none):
```

- c. Leave this field blank and press **Enter**.

If you want to block connections to a particular IP address, type the IP address instead and press **Enter**.

The following output appears:

```
Enter Destination Port (leave blank for none):
```

- d. Leave this field blank and press **Enter**.

The following output appears:

```
Targets
```

```
-----
1) ACCEPT
2) REJECT
3) DROP
4) LOGDROP
Select Target:
```

9. For inbound connections, perform the following substeps:

- a. Leave this field blank and press **Enter**.

If you want to block connections from a particular IP address, type the IP address instead and press **Enter**.

The following output appears:

```
Enter source port (leave blank for none):
```

- b. Leave this field blank and press **Enter**.

The following output appears:

```
Enter Destination IP Address (leave blank for none):
```

- c. Type the IP address of this NVE server and press **Enter**.

The following output appears:

```
Enter Destination Port (leave blank for none):
```

- d. Type the number of the port to close and press **Enter**.

The following output appears:

```
Targets
-----
1) ACCEPT
2) REJECT
3) DROP
4) LOGDROP
Select Target:
```

10. Type 2 to reject packets for the specified port, or 3 to drop packets for the specified port, and press **Enter**.

The following output appears:

```
Run Order
-----
I) Insert (Inserts rule before default AV Firewall rules are
applied)
A) Append (Standard behavior. Rule is appended, with default AV
Firewall rules taking precedent)
Select run order for this rule [A]:
```

11. Type the number that corresponds to the node type and press **Enter**.

Unless otherwise indicated by the tables in this appendix, most ports only require the utility node.

Output similar to the following appears:

```
Add rule |80||66|tcp||REJECT|OUTPUT|A to custom rules file? (Y/
N):
```

12. Type **y** to save the new rule and press **Enter**.

The script writes the new rule to `avfwb_custom_config.txt`.

Output similar to the following appears:

```
Adding |80||66|tcp||REJECT|OUTPUT|A to pending actions...
Add another firewall rule? (Y/N):
```

13. If you require more rules, type **y** and press **Enter**. Otherwise, type **n** and press **Enter**.

The following output appears:

```
Return to main menu? (Y/N):
```

14. Type **n** and press **Enter**.

The following output appears:

```
Save and execute rules now? (Y/N):
```

15. Type `x` to save the new firewall rules and press **Enter**.

The script saves the new rules to the system firewall tables and automatically restarts the NVE firewall, then exits.

Output similar to the following appears:

```
Rules have been saved to /usr/local/avamar/lib/admin/security/
entfwb_custom_config.txt

Applying /usr/sbin/iptables -A OUTPUT -p tcp --sport 80 --dport
66 -j REJECT...
```

Removing a custom firewall rule

You can remove a custom firewall rule by updating the `entfwb_custom_config.txt` file.

Procedure

1. Open a command shell:
 - a. Log in as the Admin.
 - b. Switch user to root by typing `su -`.
2. Change directory by typing the following command:


```
cd /usr/local/avamar/lib/admin/security
```
3. Run the firewall rules script by typing the following command:

```
sh ent-edit-firewall-rules.sh
```

The following output appears:

```
Choose an Action
-----
1) Add a custom rule
2) Remove a custom rule
3) List Current Custom Rules
4) Exit
5) Save Changes
Enter desired action:
```

4. Type `2` to remove custom rules and press **Enter**.

Output similar to the following appears:

```
Rules in configuration file:
  1 <IP Address>|22|<IP Address>|11|tcp||ACCEPT|OUTPUT|A

  2 |80||66|tcp||REJECT|OUTPUT|A

Select line to remove (ENTER to go back):
```

5. Type the number of the line that corresponds to the custom rule and then press **Enter**.

Output similar to the following appears:

```
Line |80||66|tcp||REJECT|OUTPUT|A will be flagged for removal
from custom configuration file.
```

The script returns to the main menu.

```
Choose an Action
-----
1) Add a custom rule
2) Remove a custom rule
3) List Current Custom Rules
4) Exit
```

```
5) Save Changes
Enter desired action:
```

6. If you want to remove additional custom rules, repeat the previous steps. Otherwise, type 5 to save changes and press **Enter**.

The following output appears:

```
Rules have been saved to /usr/local/avamar/lib/admin/security/
entfwb_custom_config.txt
Return to main menu? (Y/N):
```

7. Type **n** and press **Enter**.

The following output appears:

```
Save and execute rules now? (Y/N):
```

8. Type **y** and press **Enter**.

The script removes the custom firewall rules from the system firewall tables, automatically restarts the NVE firewall, and then exits.

The following output appears:

```
Rules have been saved to /usr/local/avamar/lib/admin/security/
entfwb_custom_config.txt

Applying rule /usr/sbin/iptables -A OUTPUT -p tcp -s <IP
Address> -d <IP Address>
--dport 11 -j ACCEPT
```

Configuring service port ranges on firewall

You can change the default service port range of 7937-9936 to another by configuring the port range on the firewall.

Procedure

1. Open a command shell:
 - a. Log in as the Admin.
 - b. Switch user to root by typing `su -`.
2. Change directory by typing the following command:


```
cd /usr/local/avamar/lib/admin/security
```
3. Open `customized_pre_rules` in a plain text editor.
4. Reassign the variable `NW_UPPER_PORT`.

```
NW_UPPER_PORT=<PORT>
```

where, <PORT> is the value of the upper port number.

5. Save and close the file.
6. Restart firewall daemon by using the command: `service entfirewall restart`

CHAPTER 9

Troubleshooting and Best Practices

This chapter contains the following topics:

- [Best Practices and Recommendations](#)..... 72
- [Accessing NetWorker Virtual Edition using SSH](#).....72
- [Enable SSH for root](#)..... 72
- [Enable SSH for root for NVE running in Cloud](#).....73
- [Support for NVE in Dual NIC configuration with different Subnets](#)..... 74
- [Binding to LDAP server error](#).....74
- [NVE installation log files](#)..... 75

Best Practices and Recommendations.

Changing the default NVE hostname from Azure or AWS DNS to custom DNS

The default DNS of Microsoft Azure or AWS, limits the FQDN to 51 characters. It is recommended to use a short NVE hostname. A short NVE hostname prevents the FQDN name from exceeding 64 characters, that the NetWorker server name allows. The default resources of the NetWorker server such as, label template, pools uses the NetWorker server name from its configuration database (resource DB). If the NetWorker server name is of 64 characters, then the default resources creation might fail because the overall characters in the pool or the label template name might exceed 64 characters limit.

To use longer FQDN and host name it is recommended to use a custom DNS when configuring the NVE in Azure or AWS cloud. However, if no custom domain is available, then use a short NVE name (up to 4 char), to ensure that the creation of default resources is not impacted.

Accessing NetWorker Virtual Edition using SSH

You can access NVE using an SSH client.

Before you begin

- You should have an SSH client installed on the system.
- You should have the private or public IP address of the NVE.

Procedure

1. Connect to NVE using the private or public IP address from an SSH client.

The user is admin and the default password is *the private ip* address of the NVE

Enable SSH for root

By default, you cannot use SSH to log in to the NVE appliance with the root account. Enable SSH to allow root to transfer log files from the NVE appliance for troubleshooting.

Procedure

1. From a vSphere client, launch the console window for the NVE appliance.
2. Log in to the NVE as the root user.
3. Edit the `/etc/ssh/sshd_config` file.

For example, type the following command to edit the file with the vim application:

```
vim /etc/ssh/sshd.config
```

4. In the **Authentication** section, remove the `#` from the beginning of the line `PermitRootLogin yes`

For example, the **Authentication** section will appear similar to the following:

```
#Authentication:
#LoginGraceTime 2m
PermitRootLogin yes
```



```
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10
```

5. Save the file.
6. Restart the SSH service, by typing the following command:

```
service sshd restart
```

Enable SSH for root for NVE running in Cloud

Before you begin

By default, you cannot use SSH to log in to the NVE appliance with the root account. Enable SSH to allow root to transfer log files from the NVE appliance for troubleshooting.

Procedure

1. Edit the `/etc/ssh/sshd_config` file.

type the following command to edit the file with the vim application:

```
vim /etc/ssh/sshd.config
```

2. Add the `#` to the beginning of the line and IP address of the workstation from where you want to login as shown in the following example:

```
## disable root login if not access from self
# Match User root Address *,!::1,!127.0.0.1,!10.13.144.188
# ForceCommand echo'Please login as the user admin rather
than the user root.';sleep 5
# Match all
## Permit local root login
Match Address ::
1,127.0.0.1,127.0.0.1,127.0.0.2,::1,10.13.144.188,fe80::ee
:beff:fe36:cde8,<IP Address of workstation>
PermitRootLogin yes
Match all
LogLevel INFO
PermitRootLogin no
```

3. Save the file.
4. Restart the SSH service, by typing the following command:

```
service sshd restart
```

5. To download the NVE logs to workstation, run the following command
 - If you are running NVE on AWS, use the `scp` command with the option `-i`
 - If you are running NVE on Azure use the `scp` command

NVE running on AWS:

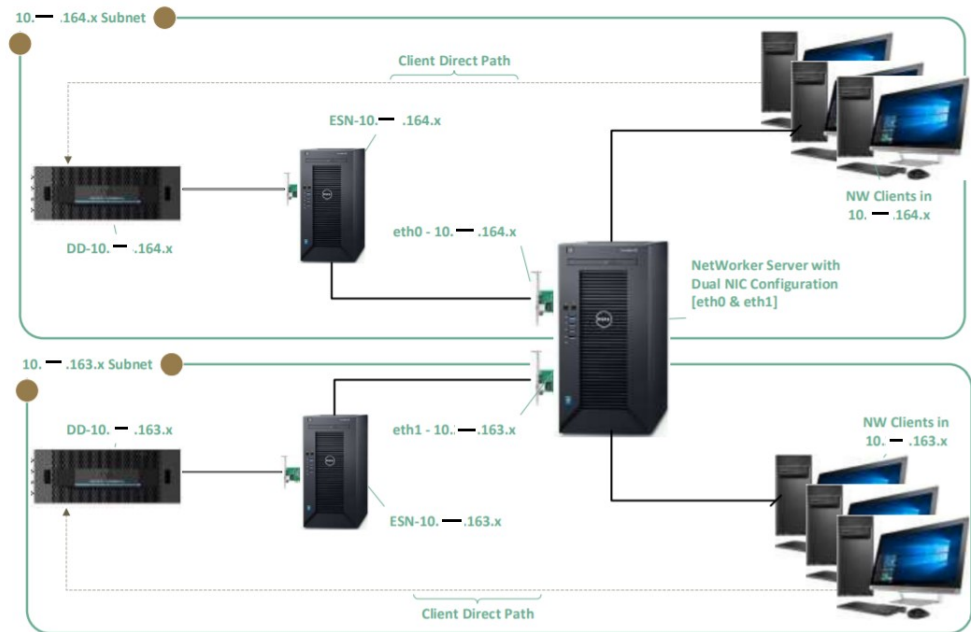
```
[root@ip-<AWS work station> ec2-user]#scp -i aws_key.pem
root@<NVE Address>:/etc/hosts /root/tmp
```

NVE running on Azure:[root@ip-<Azure work station>]#scp
root@<NVE Address>:/etc/hosts /root/tmp

Support for NVE in Dual NIC configuration with different Subnets

If the secondary Network interface card is on a different subnet, then the NetWorker Virtual Edition does not route traffic to that Network Interface card. You can route the traffic by including an additional storage node in the respective subnets.

Figure 15 NetWorker in Dual NIC configuration



Binding to LDAP server error

The Name service switch (nsswitch.conf) provides a mechanism to identify sources of network information such as username, password, LDAP and DNS. It also provides an order in which these sources are to be consulted during a network information look up.

By default, the nsswitch.conf file in NetWorker Virtual Edition is not configured to support LDAP. When you configure an LDAP client on a NetWorker Virtual Edition, it fails with an error "failed to bind to LDAP server". The error messages are logged under /var/messages To prevent this issue, you must perform the following steps:

Procedure

1. Open the /etc/nsswitch.conf file for editing.
2. Change the order of entries from "ldap files" to "files ldap"

```
Existing nsswitch file
passwd: ldap files
```

```
group: ldap files
shadow: ldap files
```

Updated nsswitch file

```
passwd: files ldap
group: files ldap
shadow: files ldap
```

NVE installation log files

The following table provides a summary of log files on the NVE that are related to installation.

Table 10 NVE installation log files

Log file	Purpose
/usr/local/avamar/var/avi/server_log/ avinstaller.log.0	Installation log file
/data01/avamar/repo/temp/****/tmp/ workflow.log	Installation log file

