JUNIPER NETWORKS | Engineering Simplicity

Upgrading Juniper Secure Analytics to 7.3.1

Published
2021-04-07

Release
7.3.1

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Upgrading Juniper Secure Analytics to 7.3.1
7.3.1

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement (“EULA”) posted at https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About the Documentation

IN THIS SECTION

Use this guide to upgrade JSA from earlier version to the current version.

Documentation and Release Notes

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at https://www.juniper.net/documentation/.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at https://www.juniper.net/books.

Documentation Conventions

Table 1 on page vi defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.
	Tip	Indicates helpful information.
	Best practice	Alerts you to a recommended use or implementation.

Table 2 on page vi defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the **configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`
Italic text like this	• Introduces or emphasizes important new terms. • Identifies guide names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS CLI User Guide* • RFC 1997, *BGP Communities Attribute*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# **set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Encloses optional keywords or variables.	**stub <default-metric *metric*>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(*string1* | *string2* | *string3*)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Encloses a variable for which you can substitute one or more values.	**community name members [*community-ids*]**

Indention and braces ({ })	Identifies a level in the configuration hierarchy.	[edit]
		routing-options {
		  static {
		  route default {
		  nexthop *address*;
		  retain;
		  }
		  }
		}

; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		

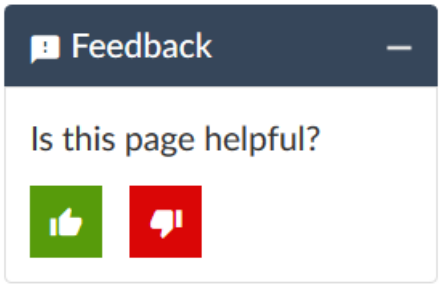
Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback so that we can improve our documentation. You can use either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:



  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active Juniper Care or Partner Support Services support contract, or are

covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf.
- Product warranties—For product warranty information, visit https://www.juniper.net/support/warranty/.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: https://www.juniper.net/customers/support/
- Search for known bugs: https://prsearch.juniper.net/
- Find product documentation: https://www.juniper.net/documentation/
- Find solutions and answer questions using our Knowledge Base: https://kb.juniper.net/
- Download the latest versions of software and review release notes: https://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: https://www.juniper.net/company/communities/
- Create a service request online: https://myjuniper.juniper.net

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://entitlementsearch.juniper.net/entitlementsearch/

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit https://myjuniper.juniper.net.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see https://support.juniper.net/support/requesting-support/.

1
CHAPTER

Preparing for the Upgrade

Preparing for the Upgrade

To successfully upgrade an JSA system, verify your upgrade path, especially when you upgrade from older versions that require intermediate steps. You must also review the software, hardware, and high availability (HA) requirements.

NOTE: When you upgrade to JSA 2014.6 or later, the SSH keys on every managed host are replaced. If you are connecting to or from a JSA managed host and you are using key-based authentication, do not remove or alter the SSH keys. Removing or altering the keys might disrupt communication between the JSA Console and the managed hosts, and result in lost data.

RELATED DOCUMENTATION

Software Version Requirements for Upgrades | 11

Memory and Disk Space Requirements | 12

Backing Up Third-party Data | 13

Software Version Requirements for Upgrades

To ensure that JSA upgrades without errors, ensure that you use only the supported versions of JSA software:

- Ensure that JSA 2014.8.r2 and later is installed.
- Check the software version in the software by clicking **Help >About**.

NOTE: Software versions for all JSA appliances in a deployment must be the same version and build. Deployments that use different JSA versions of software are not supported.

NOTE: For a managed WinCollect deployment, you must use WinCollect V7.2.5 or later. If you are on an earlier version of WinCollect, you must upgrade to WinCollect V7.2.5 before you can apply the JSA 7.3.1 upgrade.

RELATED DOCUMENTATION

Memory and Disk Space Requirements | 12
Backing Up Third-party Data | 13
Upgrade Sequence in Distributed Deployments | 14

Memory and Disk Space Requirements

Before you upgrade, ensure that JSA meets the minimum or suggested memory and disk space requirements.

JSA Memory Requirements

The following table describes the minimum and suggested memory requirements for JSA appliances. The minimum memory requirement defines the amount of memory that is required by the software features. The suggested memory requirements include the amount of memory that is required by the current software features and extra memory for possible future capabilities. Appliances that have less than the suggested appliance memory might experience performance issues during periods of excessive event and flow traffic.

Table 3: Minimum and Optional Memory Requirements for JSA Appliances

Appliance	Minimum memory requirement	Suggested memory requirement
Flow Collector Virtual without JSA Vulnerability Scanner	2 GB	2 GB
Flow Collector Virtual with JSA Vulnerability Scanner	6 GB	6 GB
JSA Event Collector/ Processor Virtual	12 GB	48 GB

Table 3: Minimum and Optional Memory Requirements for JSA Appliances *(continued)*

Appliance	Minimum memory requirement	Suggested memory requirement
JSA Flow Processor Virtual	12 GB	48 GB
JSA SIEM Virtual	24 GB	48 GB

Other Memory Requirements

If the following conditions are met, extra memory requirements might be required:

- If you plan to enable payload indexing, your system requires a minimum of 24 GB of memory. However, 48 GB of memory is suggested.

Disk Space Requirements

Before you upgrade to JSA 7.3.1, ensure that the total size of the primary disk is at least 130 gigabytes (GB).

The upgrade pretest determines whether a partition includes enough free space to complete an upgrade. Before you can upgrade, you must free up sufficient disk space on the partition that is defined in the pretest error message.

RELATED DOCUMENTATION

Backing Up Third-party Data | 13
Upgrade Sequence in Distributed Deployments | 14
Precautions for Upgrading Appliances | 15

Backing Up Third-party Data

Before you upgrade, ensure that you back up all third-party data on the system.

All third-party data on the system is removed during the OS upgrade portion of the JSA upgrade. Only data stored in the **/store** partition will be preserved. We recommend that you back up any such data before performing the upgrade such as:

- Any third-party user accounts and data
- Any static route files for network interfaces
- Any files, scripts, or data in **/root**

RELATED DOCUMENTATION

Upgrade Sequence in Distributed Deployments | 14
Upgrading High-availability Deployments | 15
Precautions for Upgrading Appliances | 15

Upgrade Sequence in Distributed Deployments

When you upgrade JSA systems, you must complete the upgrade process on your JSA Console first. You must be able to access the user interface on your desktop system before you upgrade your secondary JSA Console and managed hosts.

Upgrade your JSA systems in the following order:

1. Console
2. The following JSA systems can be upgraded concurrently:
   - Event Processors/ Collectors
   - Flow Processors

RELATED DOCUMENTATION

Upgrading High-availability Deployments | 15
Precautions for Upgrading Appliances | 15
Backing Up Third-party Data | 13

Upgrading High-availability Deployments

Before you upgrade the JSA in a high-availability (HA) deployment, the primary host must be the active system in your deployment. The primary host must be upgraded before you manually upgrade the secondary host.

If the HA cluster is disconnected, or you want to add a new secondary HA host, you must reinstall JSA on the secondary HA. For more information about reinstalling software, see the *Juniper Secure Analytics Installation Guide* for your system. After you reinstall the secondary HA host, log in to the user interface to reconnect or to create a new HA cluster.

Before you upgrade a disconnected HA cluster, copy the following file from the primary to the secondary HA host to ensure that the management interfaces match between the two hosts after the upgrade finishes:

scp /opt/qradar/conf/capabilities/map_localhost_interfaces.txt.bak root@<secondary_ip>:/opt/qradar/ha/map_localhost_interfaces.txt

> **NOTE:** Disk replication and failover are unavailable until the primary and secondary hosts synchronize and the **needs upgrade** or **failed** status is cleared from the secondary host.

After you upgrade the secondary host, you might need to restore the configuration of the secondary host. For more information about restoring a failed host, see the *Administration Guide* for your product.

RELATED DOCUMENTATION

Precautions for Upgrading Appliances | 15

Backing Up Third-party Data | 13

Upgrade Sequence in Distributed Deployments | 14

Precautions for Upgrading Appliances

Follow certain precautions before upgrading JSA appliances.

Ensure that you take the following precautions:

- Back up your data, and confirm that backups are complete before you begin the upgrade.

  For more information about backup and recovery, see the *Juniper Secure Analytics Administration Guide* for your product.

- Ensure that you either have a JSA Console connected to your hardware or have a remote connection to the management port (often called an out of band management setup). This is important because, if you encounter a problem while you are reinstalling RHEL, you will need to access the server through one of these connections.

- Upgrade all managed hosts before you deploy changes.

- Close all open JSA sessions to avoid excess errors in your log file.

- Confirm that your appliance meets the minimum requirements for JSA. For more information about system requirements, see "Memory and Disk Space Requirements" on page 12.

- Disconnect high availability (HA) hosts before the upgrade if the entire **/store** directory is mounted on offboard storage. For more information about disconnecting an HA cluster, see the *Juniper Secure Analytics High Availability Guide*.

- Ensure that the order of mount points in the **/etc/fstab** file matches on both the primary and secondary HA host:

  - **/store**
  - **/store/tmp**
  - **/store/transient**
  - Any subdirectory of **/store** if the partition is mounted on offboard storage

  Restart the system after any updates to the **/etc/fstab** file.

- If the entire **/store** directory is mounted on offboard storage, run the following command to prepare the system for the upgrade:

  /media/cdrom/post/prepare_offboard_storage_upgrade.sh

- If you are not prompted to remount your offboard storage solution during the upgrade, remount the storage when the upgrade finishes.

  For additional upgrade steps for iSCSI l offboard storage solutions, and for information about remounting offboard storage, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.

- For more information about managing licenses, see the *Juniper Secure Analytics Administration Guide*.

RELATED DOCUMENTATION

Backing Up Third-party Data | 13

Upgrade Sequence in Distributed Deployments | 14

2
CHAPTER

Upgrading JSA

Upgrading JSA Appliances

You must upgrade all of the JSA products in your deployment to the same version. During the upgrade, the version of Red Hat Enterprise Linux is upgraded to V7.3.

> **NOTE:** You must have JSA 2014.8.r2 path and later installed before you can upgrade to JSA 7.3.1. Click **Help >About** to view the JSA version.

Upgrade your JSA Console first, and then upgrade each managed host. In high-availablity (HA) deployments, upgrade the HA primary host first, and then upgrade the HA secondary host.

> **NOTE:** Upgrading the JSA Console to 7.3.1 should take approximately 3 hours. Upgrading managed hosts should take approximately 1 ½ hours. If you experience extended upgrade times, contact support to review the progress of the upgrade.

1. If you are not on JSA 2014.8.r2 or later, perform the following steps to update to the minimum JSA software version patch required for the JSA 7.3.1 upgrade. Otherwise, skip to step 2.

   > **NOTE:** Ensure that the console is upgraded before upgrading any attached managed hosts or HA secondary appliances.

   a. Download the <*JSA_patchupdate*>.*sfs* file from Juniper Customer Support (https://www.juniper.net/support/downloads).

   b. Use SSH to log in to your system as the root user.

   c. Copy the patch file to the **/tmp** directory or to another location that has sufficient disk space.

      > **NOTE:** Do not copy the file to an existing JSA system directory, such as **/store** or **/root**.

   d. To create the **/media/updates** directory, type the following command:

      mkdir -p /media/updates

   e. Change to the directory where you copied the patch file.

   f. Unzip the patch file using the bunzip utility:

bunzip2 <patchfilename>.bz2

g. To mount the patch file to the **/media/updates** directory, type the following command:

mount -o loop -t squashfs <jsa_patchupdate>.sfs /media/updates/

h. To run the patch installer, type the following command:

/media/updates/installer

> **TIP:** The first time that you run the patch installer script, there might be a delay before the first patch installer menu is displayed.

i. Provide answers to the pre-patch questions based on your JSA deployment.

j. Using the patch installer, upgrade all systems in your deployment.

The patch installer menu lists the following options.

- Console
- All

If you select *All*, the patch is applied to the JSA Console first, and then to all managed hosts. If you select Console, the patch is applied only to the JSA Console. After the patch is applied to the JSA Console, the menu lists the remaining managed hosts, and the *All* option.

If your SSH session is disconnected while the patching is in progress, the patching continues. When you reopen your SSH session and rerun the installer, the installation resumes.

k. After the patch is complete, unmount the software update by using the following command:

umount /media/updates

l. Now that you have updated to the minimum patch required for 2014.8, use the following sequence to upgrade to JSA 7.3.1.

2. To upgrade, download the *<JSA>.iso* file from Juniper Customer Support (https://www.juniper.net/support/downloads).

a. Use SSH to log in to your system as the root user.

b. Copy the ISO file to the **/tmp** directory or to another location that has sufficient disk space.

> **NOTE:** Don't copy the file to an existing JSA system directory, such as **/store** or **/root**.

c. To create the **/media/cdrom** directory, type the following command:

mkdir -p /media/cdrom

d. Change to the directory where you copied the ISO file.

e. To mount the ISO file to the **/media/cdrom** directory, type the following command:

mount -o loop <*JSA*>.iso /media/cdrom/

f. Pretest the installation by typing the following command:

/media/cdrom/setup -t

g. Review the pretest output and, if your deployment fails any pretests, take any of the suggested actions.

h. To run the installer, type the following command:

/media/cdrom/setup

> **NOTE:** The SSH connection pauses for 20 minutes because the system restarts. Monitor the console screen to confirm when the SSH becomes available after the system restart.

i. If your deployment includes offboard storage, see the *Juniper Secure Analytics Configuring Offboard Storage Guide* for steps to reconnect and remount offboard storage types.

1. Perform an automatic update to ensure that your configuration files contain the latest network security information. For more information, see the *Juniper Secure Analytics Administration Guide*.
2. Delete the patch file to free up space on the partition.
3. Clear your web browser cache. After you upgrade JSA, the **Vulnerabilities** tab might not be displayed. To use JSA Vulnerability Manager after you upgrade, you must upload and allocate a valid license key. For more information, see the *Juniper Secure Analytics Administration Guide* for your product.

RELATED DOCUMENTATION

Clearing the Web Browser Cache After Upgrades | **21**

Clearing the Web Browser Cache After Upgrades

After you upgrade, clear the web browser cache before you log in to JSA.

1. To clear your web browser cache, ensure that you have only one instance of your web browser open, and then clear the cache.

2. Log in to JSA by typing the IP address of the JSA system into a web browser:

   https://*IP Address*

   The default user name is admin.

RELATED DOCUMENTATION

Upgrading JSA Appliances | **19**

3

CHAPTER

Upgrading JSA Software Installations

Upgrading JSA Software Installations

Upgrade JSA to 7.3.1 on your own appliance with a JSA software installation. A software installation includes custom Red Hat Enterprise Linux (RHEL) partitions that are already configured.

> **NOTE:** You must have JSA 2014.8.r2 and later installed before you can upgrade to JSA 7.3.1. Click **Help >About** to view the JSA version.

You must complete these tasks to upgrade JSA with customer RHEL partitions:

1. Copy the required files to your appliance and start the upgrade.
2. Install RHEL V7.3 and configure partitions.
3. Follow the installation wizard to complete the JSA installation.

> **NOTE:** Upgrading the JSA Console to 7.3.1 should take approximately 3 hours. Upgrading managed hosts should take approximately 1 ½ hours. If you experience extended upgrade times, contact support to review the progress of the upgrade.

RELATED DOCUMENTATION

Copying the Required Files | 24

Partition Requirements and Recommendations | 26

Copying the Required Files

Copy the files to the host where you want to upgrade JSA, and begin the setup process.

- Download the JSA release ISO file from Juniper Customer Support (https://www.juniper.net/support/downloads).
- Obtain the Red Hat Enterprise Linux V7.3 ISO.
- Confirm that your appliance meets the minimum requirements for JSA. For more information about system requirements, see “Memory and Disk Space Requirements” on page 12.

- Upgrade all managed hosts before you deploy changes.
- Disconnect high-availablity (HA) hosts before the upgrade if the entire **/store** directory is mounted on offboard storage. For more information about disconnecting an HA cluster, see the *Juniper Secure Analytics High Availability Guide*.
- Ensure that the order of mount points in the **/etc/fstab** file matches on both the primary and secondary HA host:
  - **/store**
  - **/store/tmp**
  - **/store/transient**
  - Any subdirectory of **/store** if the partition is mounted on offboard storage

  Restart the system after any updates to the **/etc/fstab** file.
- If the entire **/store** directory is mounted on offboard storage, run the following command to prepare the system for the upgrade:

  /media/cdrom/post/prepare_offboard_storage_upgrade.sh
- If you are not prompted to remount your offboard storage solution during the upgrade, remount the storage when the upgrade finishes.

  For additional upgrade steps for iSCSI offboard storage solutions, and for information about remounting offboard storage, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.

1. Copy the Red Hat Enterprise Linux operating system DVD ISO to one of the following portable storage devices:
   - Digital Versatile Disk (DVD)
   - Bootable USB flash drive
2. Using a Secure File Transfer Protocol (SFTP) program, such as WinSCP, copy the JSA ISO to the host where you want to install JSA.
3. Use SSH to log in to the system as the root user.
4. Create the installation directory by typing the following command:

   mkdir -p /media/cdrom
5. Mount the JSA ISO by typing the following command:

   mount -o loop <*JSA_ISO*> /media/cdrom
6. Start the JSA setup by typing the following command:

   /media/cdrom/setup

RELATED DOCUMENTATION

Partition Requirements and Recommendations | 26
Completing the JSA Installation | 28

Partition Requirements and Recommendations

During the upgrade process, partition requirements and recommendations are generated. If those instructions don not work, you can configure the partition manually.

The following partitions must be preserved and must not be reformatted:

Table 4: Requirements (preserve and do Not Reformat These Partitions).

Partition	Description
/store	Stores data files.
/storetmp	Stores configuration files.
/transient	Stores saved searches.

Table 5: Requirements (minimum Partition Sizes for Red Hat V7.3 & JSA 7.3.1 Upgrade)

Partition	Size(MiB)	Device Type	Volume Group	File System Type
/boot	100 MiB **NOTE:** Suggested size is at least 200 MiB. Ideal size is 1024 MiB.	Standard Partition	N/A	XFS
/	5000 MiB (Normally 1000 MiB, but /store requires 4000 MiB.) **NOTE:** **/store** needs to be unmounted when you are installing JSA 7.3.1 for the upgrade, so the requirement falls to **/**.	LVM	rootrhel	XFS

Table 5: Requirements (minimum Partition Sizes for Red Hat V7.3 & JSA 7.3.1 Upgrade) *(continued)*

Partition	Size(MiB)	Device Type	Volume Group	File System Type
/opt	6000 MiB	LVM	rootrhel	XFS
/var	500 MiB	LVM	rootrhel	XFS
/home	1 MiB	LVM	rootrhel	XFS
/tmp	500 MiB	LVM	rootrhel	XFS
/var/log	1000 MiB	LVM	varlogrhel	XFS
/var/log/audit	1000 MiB	LVM	varlogrhel	XFS

RELATED DOCUMENTATION

Completing the JSA Installation | 28

Copying the Required Files | 24

Installing RHEL V7.3 and Configuring Partitions

When you initiate an JSA upgrade on a host that has custom RHEL partitions configured, a message appears stating that a RHEL Software Installation exists. Copy the recommendations for sizing your existing partitions for RHEL V7.3 to use later in the procedure.

1. Insert the portable storage device into your appliance and restart your appliance.

2. From the starting menu, select one of the following options:
   - Select the USB or DVD drive as the boot option.
   - To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in legacy mode.
3. Follow the instructions in the installation wizard to begin the installation:
   a. Select your language.
   b. Click **Date & Time** and set the time for your deployment.
   c. Click **Installation Destination** and select the **I will configure partitioning** option, and then click **Done**.

4. Adjust the partition sizes according to the recommendations for your deployment that is listed in the installation window.

5. Click **Done** on the **Manual Partitioning** window.

6. Follow the instructions in the wizard to complete the installation:
   a. Click **Network & Host Name**.
   b. Enter the host name for your appliance.
   c. Select the interface in the list, move the switch to the **ON** position, and click **Configure**.
   d. On the **General** tab, select the **Automatically connect to this network when it is available** option.
   e. On the **IPv4 Settings** tab, in the **Method** list, select **Manual**.
   f. Click **Add** to enter the IP address, Netmask, and Gateway for the appliance in the **Addresses** field.
   g. Add two DNS servers.
   h. Click **Save**, click **Done**, and then click **Begin Installation**.
7. Set the root password, and then click **Finish configuration**.

8. Restart the host after the RHEL V7.3 installation finishes.

RELATED DOCUMENTATION

Completing the JSA Installation | 28
Copying the Required Files | 24
Partition Requirements and Recommendations | 26

Completing the JSA Installation

After you configure RHEL V7.3, complete the JSA installation by preparing for the JSA installation wizard.

1. Use SSH to log in to the system as a root user.

2. Modify the **SELINUX** value in the **/etc/sysconfig/selinux** file to **SELINUX=disabled**, and restart the host.

3. Use SSH to log back in to the system as the root user.

4. Confirm that the **/store** partition is not mounted by typing the following command:

   mount

   If the **/store** partition is mounted, unmount the partition by typing the following command:

   umount /store

5. Confirm that the **/storetmp** partition is mounted by typing the following command:

   mount /storetmp

6. Create the **/media/cdrom** directory by typing the following command:

   mkdir -p /media/cdrom

7. Mount the JSA ISO by typing the following command:

   mount /storetmp/730/<*JSA_ISO_name*> /media/cdrom

8. Type the following command to begin the JSA upgrade:

   /media/cdrom/setup

9. After the installation finishes, clear your browser cache. For more information, see "Clearing the Web Browser Cache After Upgrades" on page 21.

RELATED DOCUMENTATION

Copying the Required Files | **24**

Partition Requirements and Recommendations | **26**