JUNIPER NETWORKS | Engineering Simplicity

Juniper Secure Analytics Risk Manager Installation Guide

Published
2022-05-09

RELEASE
7.5.0

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

Juniper Secure Analytics Risk Manager Installation Guide
7.5.0

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 This Guide

Use this guide to install JSA Risk Manager appliance as a managed host on your JSA console.

1
CHAPTER

JSA Risk Manager Installation Overview

JSA Risk Manager Installation Overview

IN THIS SECTION

You install an JSA Risk Manager appliance as a managed host on your JSA console. Only one JSA Risk Manager can exist on a JSA console.

JSA console and JSA Risk Manager use the same installation process and ISO image. After you install the JSA Console and JSA Risk Manager, you add JSA Risk Manager as a managed host by using the **System and License Management** tool on the **Admin** tab. A JSA Risk Manager appliance is preinstalled with the JSA Risk Manager software and a Red Hat Enterprise Linux operating system.

JSA Risk Manager and JSA Vulnerability Manager Licenses

JSA Vulnerability Manager and JSA Risk Manager are combined into one offering and both are enabled through a single base license. The combined offering provides an integrated network scanning and vulnerability management workflow. With the base license, you are entitled to use JSA Vulnerability Manager to scan up to 256 assets. You can integrate JSA Risk Manager with up to 50 standard configuration sources. If you are entitled to either JSA Vulnerability Manager or JSA Risk Manager, you are automatically entitled to the base license allowance for the other product. You require extra licenses to scan more than 256 assets or to integrate with more than 50 configuration sources.

2
CHAPTER

JSA Risk Manager Installation Prerequisites

JSA Risk Manager Installation Prerequisites

IN THIS SECTION

You must complete the installation process for an JSA console before you install JSA Risk Manager. It is a good practice to install JSA and JSA Risk Manager on the same network switch.

For information about installing JSA, including hardware and software requirements, see the *Juniper Secure Analytics Administration Guide*.

Since JSA Risk Manager is a 64-bit appliance, make sure that you download the correct installation software for your operating system.

Network Settings

Gather the following information for your network settings:

- Hostname
- IP address
- Network mask address
- Subnet mask
- Default gateway address
- Primary Domain Name System (DNS) server address
- Secondary DNS server (optional) address
- Public IP address for networks that use Network Address Translation (NAT) email server name
- Email server name

- Network Time Protocol (NTP) server (Console only) or time server name

Port Requirements

Ensure that any firewall located between the JSA Console and JSA Risk Manager allows traffic on the following ports:

- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Time)

Unsupported Features

The following features are not supported in JSA Risk Manager:

- High availability (HA)
- Dynamic Routing for Border Gateway Protocol (BGP)
- Non-contiguous network masks
- Load-balanced routes

CHAPTER 3

System Requirements for JSA Risk Manager

System Requirements for JSA Risk Manager

IN THIS SECTION

Before you install JSA Risk Manager, ensure that your system meets the minimum hardware and software requirements.

Additional Hardware Requirements

Before you install JSA Risk Manager systems, you need access to the following hardware components:

- Monitor and keyboard
- Uninterrupted Power Supply (UPS)

Protect your JSA Risk Manager installations that store data by using an Uninterrupted Power Supply (UPS). Using a UPS ensures that your JSA Risk Manager data, such as the data that is stored on consoles, event processors, and flow processors, is preserved during a power failure.

Additional Software Requirements

The following software must be installed on the desktop system that you use to access JSA Risk Manager:

- Java Runtime Environment

Memory Requirements

The minimum memory requirement for JSA Risk Manager is 24 GB. The suggested memory requirement for optimal performance is 48 GB.

For more information about JSA system requirements, see the *Juniper Secure Analytics Installation Guide*.

Processor Requirements

The minimum and suggested CPU requirements for JSA Risk Manager are 8 CPU cores.

For more information about JSA system requirements, see the *Juniper Secure Analytics Installation Guide*.

4

CHAPTER

Installing JSA Risk Manager

Installing JSA Risk Manager

A JSA Risk Manager deployment includes a JSA Console and JSA Risk Manager appliance as a managed host.

1. Select normal for the type of setup. Select **Next** and press Enter.
2. Select your time zone continent or area. Select **Next** and press Enter.
3. Select your time zone region. Select **Next** and press Enter.
4. Select an Internet Protocol version. Select **Next** and press Enter.
5. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
6. Type your host name, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server.

   Network information for Internet Protocol version 4 (IPv4) network settings is required.

   The Public IP network setting is optional. This secondary IP address is used to access the server, usually from a different network or the internet, and is managed by your network administrator. The Public IP address is often configured by using the Network Address Translation (NAT) services on your network or firewall settings on your network. NAT translates an IP address in one network to a different IP address in another network.
7. Select **Next** and press Enter.
8. Type a password to configure the JSA Risk Manager root password.
9. Select **Next** and press Enter.
10. Retype your new password to confirm. Select **Finish** and press Enter.

    This process typically takes several minutes.

RELATED DOCUMENTATION

Adding JSA Risk Manager to JSA Console | 10

Clearing Web Browser Cache | 12

Adding JSA Risk Manager to JSA Console

If you want to enable compression, then the minimum version for each managed host must be JSA console 2014.1 or JSA Risk Manager 2014.1.

To add a managed host that is not NATed to your deployment where the Console is NATed, you must change the JSA console to a NATed host. You must change the console before you add the managed host to your deployment. For more information, see the *Juniper Secure Analytics Administration Guide*.

You must add JSA Risk Manager as a managed host to JSA console.

1. Open your web browser.
2. Type the URL, **https://<*IP Address*>**, where <*IP Address*> is the IP address of the JSA console.
3. Type your user name and password.
4. Click the **Admin** tab.
5. In the **System Configuration** pane, click **System and License Management**.
6. In the **System and License Management** window, click **Deployment Actions**, and then select **Add Host**.
7. Enter values for the following parameters:

Option	Description
Host IP	The IP address of JSA Risk Manager.
Host Password	The root password for the host.
Confirm Host Password	Confirmation for your password.
Encrypt Host Connections	Creates an SSH encryption tunnel for the host. To enable encryption between two managed hosts, each managed host must be running JSA console 2014.1 or JSA Risk Manager 2014.1.
Encryption Compression	Enables data compression between 2 managed hosts.
Network Address Translation	To enable NAT for a managed host, the NATed network must be using static NAT translation. For more information, see the *Juniper Secure Analytics Administration Guide*.

8. If you select the **Network Address Translation** check box, then you must enter values for the NAT parameters:

Option	Description
NAT Group	The network that you want this managed host to use. If the managed host is on the same subnet as the JSA console, select the console of the NATed network. If the managed host is not on the same subnet as the JSA console, select the managed host of the NATed network.
Public IP	The public IP address of the managed host. The managed host uses this IP address to communicate with other managed hosts in different networks that use NAT.

9. Click **Add**.

   This process can take several minutes to complete. If your deployment includes changes, then you must deploy all changes.

10. From the **Admin** tab, click **Advanced >Deploy Full Configuration**.

Clear your web browser cache and then log in to JSA console. The **Risks** tab is now available.

RELATED DOCUMENTATION

Clearing Web Browser Cache | 12

Installing JSA Risk Manager | 10

Clearing Web Browser Cache

Ensure that only one web browser is open. If you have multiple browsers open, the cache can fail to clear properly.

If you are using a Mozilla Firefox web browser, you must clear the cache in your Microsoft Internet Explorer web browser too.

You must clear the web browser cache before you can access the **Risks** tab in JSA console.

1. Open your web browser.
2. Clear your web browser cache. For instructions, see your web browser documentation.

RELATED DOCUMENTATION

Installing JSA Risk Manager | 10

Adding JSA Risk Manager to JSA Console | 10

5
CHAPTER

Install JSA Virtual Risk Manager Appliances

Creating Your Virtual Machine

To install a virtual appliance, you must first use VMWare ESXi to create a virtual machine.

1. From the VMware vSphere Client, click **File > New > Virtual Machine**.
2. Add the **Name and Location**, and select the **Datastore** for the new virtual machine.
3. Use the following steps to guide you through the choices:
   a. In the **Configuration** pane of the Create New Virtual Machine window, select **Custom**.
   b. In the **Virtual Machine Version** pane, select a virtual machine hardware version 13. For more information about VMWare ESXi and hardware versions, see ESXi/ESX hosts and compatible virtual machine hardware versions list (https://kb.vmware.com/s/article/2007240).
   c. For the **Operating System (OS)**, select **Linux**, and select **Red Hat Enterprise Linux 7 (64-bit)**.
   d. On the **CPUs** page, configure the number of virtual processors that you want for the virtual machine.
   e. In the **Memory Size** field, type or select the RAM required for your deployment.
   f. Use the following table to configure your network connections.

      Table 1: Descriptions for Network Configuration Parameters

Parameter	Description
How many NICs do you want to connect?	You must add at least one Network Interface Controller (NIC)
Adapter	VMXNET3

   g. In the **SCSI controller** pane, select **VMware Paravirtual**.
   h. In the **Disk** pane, select **Create a new virtual disk** and use the following table to configure the virtual disk parameters.

Table 2: Settings for the Virtual Disk Size and Provisioning Policy Parameters

Parameter	Description
Capacity	256 or higher (GB) for the installation. Your storage capacity depends on your event rate, the average size of your events, and your retention requirements.
Disk Provisioning	Thin provision
Advanced options	Do not configure

4. On the **Ready to Complete** page, review the settings and click **Finish**.

RELATED DOCUMENTATION

Installing JSA Software on a Virtual Machine | 16

Adding Your Virtual Appliance to Your Deployment | 18

Installing JSA Software on a Virtual Machine

You must complete the "Creating Your Virtual Machine" on page 15 before you install JSA software on the virtual machine.

1. In the left navigation pane of your VMware vSphere Client, select your virtual machine.
2. In the right pane, click the **Summary** tab.
3. In the **Commands** pane, click **Edit Settings**.
4. In the left pane of the **Virtual Machine Properties** window, click **CD/DVD Drive 1**.
5. In the **Device Type** pane, select **DataStore ISO File**.
6. In the **Device Status** pane, select the **Connect at power on** check box.
7. In the **Device Type** pane, click **Browse**.
8. In the Browse Datastores window, locate and select the JSA product ISO file, click **Open** and then click **OK**.
9. After the JSA product ISO image is installed, right-click your virtual machine and click **Power > Power On**.
10. Log in to the virtual machine by typing root for the user name. The user name is case-sensitive.

11. Accept the End User License Agreement.
12. Select the appliance type:
    - **Non-Software Appliance**
    - **Software Appliance**
13. Select the appliance assignment, and then select **Next**.
14. If you selected an appliance for high-availability (HA), select whether the appliance is a console.
15. For the type of setup, select **Normal Setup (default)** or **HA Recovery Setup**, and set up the time.
16. If you selected **HA Recovery Setup**, enter the cluster virtual IP address.
17. Select the Internet Protocol version:
    - Select **ipv4** or **ipv6**.
18. If you selected **ipv6**, select **manual** or **auto** for the **Configuration type**.
19. Select the bonded interface setup, if required.
20. Select the management interface.
21. In the wizard, enter a fully qualified domain name in the **Hostname** field.
22. In the **IP address** field, enter a static IP address, or use the assigned IP address.

    NOTE: If you are configuring this host as a primary host for a high availability (HA) cluster, and you selected Yes for auto-configure, you must record the automatically-generated IP address. The generated IP address is entered during HA configuration.

    For more information, see the *Juniper Secure Analytics High Availability Guide*.
23. If you do not have an email server, enter `localhost` in the **Email server name** field.
24. Enter `root` and `admin` passwords that meet the following criteria:
    - Contains at least 5 characters
    - Contains no spaces
    - Can include the following special characters: @, #, ^, and *.
25. Click **Finish**.
26. Follow the instructions in the installation wizard to complete the installation.

    The installation process might take several minutes.
27. Apply your license key.
    a. Log in to JSA.

       The default user name is admin. The password is the password of the root user account.

    b. Click **Login To JSA**.

c. Click the **Admin** tab.

d. In the navigation pane, click **System Configuration**.

e. Click the **System and License Management** icon.

f. From the **Display** list box, select **Licenses**, and upload your license key.

g. Select the unallocated license and click **Allocate System to License**.

h. From the list of systems, select a system, and click **Allocate System to License**.

RELATED DOCUMENTATION

Adding Your Virtual Appliance to Your Deployment | 18

Creating Your Virtual Machine | 15

Adding Your Virtual Appliance to Your Deployment

You can add your virtual appliance to your deployment after you install JSA software on a virtual machine.

1. Log in to the JSA Console.
2. On the **Admin** tab, click the **Deployment Editor** icon.
3. In the **Event Components** pane on the **Event View** page, select the virtual appliance component that you want to add.
4. On the first page of the **Adding a New Component** task assistant, type a unique name for the virtual appliance.

   The name that you assign to the virtual appliance can be up to 20 characters in length and can include underscores or hyphens.
5. Complete the steps in the task assistant.
6. From the **Deployment Editor** menu, click **File > Save to staging**.
7. On the **Admin** tab menu, click **Deploy Changes**.
8. Apply your license key.

   a. Log in to JSA:

      The default user name is admin. The password is the password of the root user account.

   b. Click **Login To JSA**.

c. Click the **Admin** tab.

d. In the navigation pane, click **System Configuration**.

e. Click the **System and License Management** icon.

f. From the **Display** list box, select **Licenses**, and upload your license key.

g. Select the unallocated license and click **Allocate System to License**.

h. From the list of systems, select a system, and click **Allocate System to License**.

RELATED DOCUMENTATION

Creating Your Virtual Machine | 15

Installing JSA Software on a Virtual Machine | 16

CHAPTER 6

Assigning the Risk Manager User Role

Assigning the Risk Manager User Role

You must assign the Risk Manager user role and a security profile for users that require access to the **Risks** tab.

Before you allow users in your organization to have access to JSA Risk Manager functions, you must assign the appropriate user role permissions. By default, JSA Console provides a default administrative role, which provides access to all areas of JSA Risk Manager.

For information about creating and managing user roles, see the *Juniper Secure Analytics Administration Guide*.

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. In the **User Management** pane, click the **User Roles** icon.
4. Click the **Edit** icon next to the user role you want to edit.
5. Select the **Risk Manager** check box.
6. Click **Next**.

   If you add Risk Manager to a user role that has Log Activity permission, then you must define the log sources that the user role can access. You can add an entire log source group by clicking the **Add** icon in the **Log Source Group** pane. You can select multiple log sources by holding the Ctrl key while you select each log source you want to add.
7. Click **Return**.
8. From the **Admin** tab menu, click **Deploy Changes**.

RELATED DOCUMENTATION

Risk Manager User Role

Troubleshoot the Risks Tab | 23

Removing a Managed Host | 23

7

CHAPTER

Troubleshoot the Risks Tab

Troubleshoot the Risks Tab

You can troubleshoot if the **Risks** tab does not display properly or is inaccessible.

When the Risks tab is not displaying properly or is inaccessible, you "Removing a Managed Host" on page 30 and "Re-adding JSA Risk Manager As a Managed Host" on page 25 JSA Risk Manager as a managed host.

Removing a Managed Host

You can remove your JSA Risk Manager managed host from JSA console to change network settings or if there is a problem with the **Risks** tab.

1. Log in to JSA console as an administrator:

   https:// ***IP_Address_JSA***

   The default user name is admin. The password is the password of the root user account that was entered during the installation.
2. Click the **Admin** tab.
3. In the **System Configuration** pane, click **System and License Management**.
4. From the host table, click the JSA Risk Manager host that you want to remove, and click **Deployment Actions >Remove Host**.
5. From the **Admin** tab menu bar, click **Deploy Changes**.
6. Refresh your web browser.

RELATED DOCUMENTATION

8
CHAPTER

Re-adding JSA Risk Manager As a Managed Host

Re-adding JSA Risk Manager As a Managed Host

You can re-add JSA Risk Manager as a managed host after it is removed.

1. Click **Admin** tab.
2. Click **System and License Management >Deployment Actions >Add Host**.
3. Enter the host IP address and password.
4. Click **Add**.

   You must wait several minutes while the managed host is added.
5. Close the **System and License Management** window.
6. On the **Admin** tab toolbar, click **Advanced >Deploy Full Configuration**.
7. Click **OK**.

   NOTE: When you remove a JSA Risk Manager managed host and then re-add a JSA Risk Manager managed host by using a different IP address, you must restart the hostcontext and tomcat services.

   Use SSH to log in to the JSA console as the root user and type the following commands to restart these services:

   systemctl start tomcat -rm

   systemctl start hostcontext
8. Optional: To view pre-existing benchmark scan profiles in the **Monitor Question Results** window after the JSA Risk Manager license is re-added, you must reactivate the benchmark scan profiles.
   a. Click **Vulnerabilities >Administrative >Scan Profiles > Details** tab.
   b. Select the **Active** check box.
   c. Click **Save**.

RELATED DOCUMENTATION

Removing a Managed Host | 30

Changing Network Settings | 31

9

CHAPTER

Reinstall JSA Risk Manager from the Recovery Partition

Reinstall JSA Risk Manager from the Recovery Partition

When you reinstall JSA Risk Manager from the JSA console ISO on the recovery partition, your system is restored back to factory default configuration. This means that your current configuration and data files are overwritten.

This information applies to new JSA Risk Manager installations or upgrades from new JSA Risk Manager on JSA Risk Manager appliances. When you install JSA Risk Manager, the installer (JSA console ISO) is copied into the recovery partition. From this partition, you can reinstall JSA Risk Manager, which restores JSA Risk Manager to factory defaults.

NOTE: If you upgrade your software after you install JSA Risk Manager, then the ISO file is replaced with the newer version.

When you reboot your JSA Risk Manager appliance, you are presented with the option to reinstall the software. Since JSA console and JSA Risk Manager use the same ISO installation file, the JSA console ISO name displays.

If you do not respond to the prompt after 5 seconds, the system reboots as normal, which maintains your configuration and data files. If you choose to reinstall JSA console ISO, a warning message is displayed and you must confirm that you want to reinstall the software. After confirmation, the installer runs and you can follow the prompts through the installation process.

After a hard disk failure, you cannot reinstall from the recovery partition because it is no longer available. If you experience a hard disk failure, contact Juniper Customer Support for assistance.

Reinstalling JSA Risk Manager by Using Factory Re-install

You can restart and reinstall your JSA Risk Manager appliance by using the factory installation option.

1. Reboot your JSA Risk Manager appliance.
2. Select **Factory re-install**.
3. Type **flatten** to continue.

The hard disk is partitioned and reformatted, the OS is installed, and then JSA Risk Manager is reinstalled. You must wait for the flatten process to complete. This process can take up to several minutes, depending on your system.

4. Type **SETUP**.
5. Log in to JSA Risk Manager as the root user.
6. Read the information in the window. Press the Space bar to advance each window until you reach the end of the document. Type **yes** to accept the agreement, and then press **Enter**.
7. Follow the instructions in the wizard.

   This process typically takes several minutes.
8. Press **Enter** to select **OK**.

RELATED DOCUMENTATION

Reinstall JSA Risk Manager from the Recovery Partition | 27

Change Network Settings | 30

10
CHAPTER

Change Network Settings

Change Network Settings

You can change the network settings of an JSA Risk Manager appliance that is attached to an JSA console.

If you need to change the network settings, then you must complete these tasks in the following order:

1. "Removing a Managed Host" on page 30.
2. "Re-adding JSA Risk Manager As a Managed Host" on page 25.
3. "Changing Network Settings" on page 31

Removing a Managed Host

You can remove your JSA Risk Manager managed host from JSA console to change network settings or if there is a problem with the **Risks** tab.

1. Log in to JSA console as an administrator:

   https://*IP_Address_JSA*

   The default user name is admin. The password is the password of the root user account that was entered during the installation.
2. Click the **Admin** tab.
3. In the **System Configuration** pane, click **System and License Management**.
4. From the host table, click the JSA Risk Manager host that you want to remove, and click **Deployment Actions >Remove Host**.
5. From the **Admin** tab menu bar, click **Deploy Changes**.
6. Refresh your web browser.

RELATED DOCUMENTATION

Changing Network Settings | 31

Re-adding JSA Risk Manager As a Managed Host | 25

Changing Network Settings

You must remove the JSA Risk Manager managed host from JSA console before you change the network settings.

You can change the network settings of an JSA Risk Manager appliance that is attached to an JSA console.

NOTE: Verify all external storage which is not **/store/ariel** or **/store** is not mounted.

1. Using SSH, log in to JSA Risk Manager as the root user.
2. Type the command, **qchange_netsetup**.
3. Select an Internet Protocol version. Select **Next** and press Enter. Depending on your hardware configuration, the window displays up to a maximum of four interfaces. Each interface with a physical link is denoted with a plus (+) symbol.
4. Select the interface that you want to specify as the management interface. Select **Next** and press Enter.
5. Enter information for your host name, IP address, network mask, gateway, primary DNS, secondary DNS, public IP, and email server.
6. Type your password to configure the JSA Risk Manager root password.
7. Select **Next** and press Enter.
8. Retype your new password to confirm. Select **Finish** and press Enter.

   This process typically takes several minutes.

RELATED DOCUMENTATION

Re-adding JSA Risk Manager As a Managed Host | 25

Removing a Managed Host | 30

Re-adding JSA Risk Manager As a Managed Host

You can re-add JSA Risk Manager as a managed host after it is removed.

1. Click **Admin** tab.

2. Click **System and License Management >Deployment Actions >Add Host**.
3. Enter the host IP address and password.
4. Click **Add**.

   You must wait several minutes while the managed host is added.
5. Close the **System and License Management** window.
6. On the **Admin** tab toolbar, click **Advanced >Deploy Full Configuration**.
7. Click **OK**.

> **NOTE**: When you remove a JSA Risk Manager managed host and then re-add a JSA Risk Manager managed host by using a different IP address, you must restart the hostcontext and tomcat services.
>
> Use SSH to log in to the JSA console as the root user and type the following commands to restart these services:
>
> **systemctl start tomcat -rm**
>
> **systemctl start hostcontext**

8. Optional: To view pre-existing benchmark scan profiles in the **Monitor Question Results** window after the JSA Risk Manager license is re-added, you must reactivate the benchmark scan profiles.
   a. Click **Vulnerabilities >Administrative >Scan Profiles > Details** tab.
   b. Select the **Active** check box.
   c. Click **Save**.

RELATED DOCUMENTATION

Removing a Managed Host | 30

Changing Network Settings | 31

11

CHAPTER

Data Back Up and Restore

Data Back Up and Restore

You can use a command-line interface (CLI) script to back up data that is stored on JSA console managed hosts.

You can use the CLI script to restore JSA Risk Manager after a data failure or hardware failure on the appliance.

A backup script is included in JSA Risk Manager, which can be scheduled by using crontab. The script automatically creates a daily archive of JSA Risk Manager data at 3:00 AM. By default, JSA Risk Manager keeps the last five backups. If you have network or attached storage, you must create a cron job to copy JSA Risk Manager back archives to a network storage location.

The backup archive includes the following data:

- JSA Risk Manager device configurations
- Connection data
- Topology data
- Policy Monitor questions
- JSA Risk Manager database tables

Prerequisites for Backing Up and Restoring Data

IN THIS SECTION

You must understand how data is backed up, stored, and archived before you back up and restore your data.

Data Backup Location

Data is backed up in the **/store/qrm_backups** local directory. Your system might include a mount **/store/backup** from an external SAN or NAS service. External services provide long-term offline retention of data. Long-term storage might be required for compliance regulations, such as Payment Card Industry (PCI) standards.

Appliance Version

The version of the appliance that created the backup in the archive is stored. A backup can be restored only in an JSA Risk Manager appliance if it is the same version.

Data Backup Frequency and Archival Information

Daily data backups are created at 3:00 AM. Only the last five backup files are stored. A backup archive is created if there is enough free space on JSA Risk Manager.

Format Of Backup Files

Use the following format to save backup files:

```
backup-<target date>-<timestamp>.tgz
```

Where, `<target date>` is the date that the backup file was created.

The format of the target date is `<day>_<month>_<year>`. `<timestamp>` is the time that the backup file was created.

The format of the time stamp is `<hour>_<minute>_<second>`.

RELATED DOCUMENTATION

Backing Up Your Data | 36

Restoring Data | 36

Backing Up Your Data

Automatic backup occurs daily, at 3:00 AM, or you can start the backup process manually.

1. Using SSH, log in your JSA console as the root user.
2. Using SSH from the JSA console, log in to JSA Risk Manager as the root user.
3. Start a JSA Risk Manager backup by typing the following command:

   /opt/qradar/bin/dbmaint/risk_manager_backup.sh

The script that is used to start the backup process might take several minutes to start.

The following message is an example of the output that is displayed, after the script completes the backup process:

Fri Sep 11 10:14:41 EDT 2015 - Risk Manager Backup complete, wrote /store/qrm_backups/backup-2015-09-11-10-14-39.tgz

RELATED DOCUMENTATION

Restoring Data | 36

Prerequisites for Backing Up and Restoring Data | 34

Restoring Data

The JSA Risk Manager appliance and the backup archive must be the same version of JSA Risk Manager. If the script detects a version difference between the archive and the JSA Risk Manager managed host, an error is displayed.

You can use a restore script to restore data from a JSA Risk Manager backup.

Use the restore script to specify the archive that you are restoring to JSA Risk Manager. This process requires you to stop services on JSA Risk Manager. Stopping services logs off all JSA Risk Manager users and stops multiple processes.

The following table describes the parameters that you can use to restore a backup archive.

Table 3: Parameters Used to Restore a Backup Archive to JSA Risk Manager

Option	Description
-f	Overwrites any existing JSA Risk Manager data on your system with the data in the restore file. Selecting this parameter allows the script to overwrite any existing device configurations in Configuration Source Management with the device configurations from the backup file.
-w	Do not delete directories before you restore JSA Risk Manager data.
-h	The help for the restore script.

1. Using SSH, log in your JSA console as the root user.
2. Using SSH from the JSA console, log in to JSA Risk Manager as the root user.
3. Stop **hostcontext** by typing **systemctl stop hostcontext**.
4. Type the following command to restore a backup archive to JSA Risk Manager:
   /opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<backup>.

   Where **<backup>** is the JSA Risk Manager

   archive that you want to restore.

   For example, **backup-2012-09-11-10-14-39.tgz**.
5. Start **hostcontext** by typing **systemctl start hostcontext**.

RELATED DOCUMENTATION

Prerequisites for Backing Up and Restoring Data | 34

Backing Up Your Data | 36