Juniper Networks | Engineering Simplicity

# Juniper Secure Analytics High Availability Guide

Published
2022-05-04

RELEASE
7.5.0

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



*Juniper Secure Analytics High Availability 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 understand how you can protect your JSA data by implementing a HA solution.

1
CHAPTER

# High Availability Overview

# High Availability Overview

If your hardware or network fails, JSA can continue to collect, store, and process event and flow data by using high-availability (HA) appliances.

To enable HA, JSA connects a primary HA host with a secondary HA host to create an HA cluster.

If a primary HA host fails, then the secondary HA host maintains access to the same data as the primary by using data synchronization or shared external storage.

The secondary HA host inherits the license from the primary HA host. There is no need to apply a separate license to the secondary host.

For more information about using shared external storage with HA, for example iSCSI, or NFS, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.

You can use HA on hardware or virtual appliances, and with either appliance or software installations, if you meet the HA requirements. Security Technical Implementation Guide (STIG) is not supported in JSA high-availability (HA) deployments.

RELATED DOCUMENTATION



# Data Consistency for HA

IN THIS SECTION



When an HA failover occurs, JSA ensures the consistency of your data.

The type of storage that you use determines how HA data consistency is maintained. If you configure HA with external storage, data consistency is maintained by using a component such as an iSCSI external storage device. See "Offboard Storage Requirements for HA" on page 20.

If you do not use external storage devices, then JSA HA maintains data consistency between a primary and secondary HA host by using Distributed Replicated Block Device (DRBD).

Data synchronization occurs in the following situations in an HA environment:

- When you initially configure an HA cluster.
- When a primary HA host is restored after a failover.
- During normal HA operation, data is synchronized in real time between the primary and secondary host.

## Real-time Data Synchronization

When you configure an HA cluster, the **/store** file system on the primary HA host is automatically synchronized with the **/store** partition on the secondary HA host.

If the primary HA host fails over, the **/store** file system on the secondary HA host is automatically mounted to its local disk, where it continues to read from and write to the data received by the primary HA host before the failover.

After synchronization is complete, the secondary HA host assumes a status of standby.

Depending on the size of the primary **/store** partition and performance, disk synchronization can take an extended time period. Ensure that the connection between the primary and secondary HA host has a minimum bandwidth of 1 Gbps.

## Post-failover Data Synchronization

Data that is collected by a primary high-availability (HA) host, up to the point of failover, is maintained virtually, in real time, by the secondary HA host.

When the primary HA host is restored after a failure, only the data that is collected by the secondary HA host in the intervening period is synchronized with the primary HA host. Therefore, post-failover disk synchronization is faster than initial disk synchronization, unless the disk on the primary HA host was replaced or reformatted when the host was manually repaired.

When restored from a failover, the status of the primary HA host becomes offline. You must set the primary HA host to an online state, and set the secondary host to an offline state, before it can become the active host. Disk replication with the secondary HA host is enabled while the primary HA host remains offline.

RELATED DOCUMENTATION

High-availability Clusters | 4

Failovers | 6

# High-availability Clusters

IN THIS SECTION



A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

**NOTE**: You must purchase a separate HA license to set up high availability. However, the license should not be allocated to the secondary console or the secondary managed host.

## Primary HA Host

The primary HA host is any console or managed host in your JSA deployment that requires protection from data loss if there is a failure.

When you create an HA cluster, the IP address of the primary HA host is automatically reassigned to a cluster virtual IP address. Therefore, you must assign an unused IP address to the primary HA host.

When you create an HA cluster, the original host name of your primary HA host becomes the virtual hostname for the HA cluster, and "-primary" is appended to the host name of your primary HA host. You can't change the host name of a host in an HA cluster.

The primary HA host can act as a standby system for the secondary HA host. For example, if the primary HA host is repaired after a failover, the status changes to standby.

## Secondary HA Host

The secondary HA host is the standby system for the primary HA host.

If the primary HA host fails, the secondary HA host automatically takes over all the responsibilities of the primary HA host.

When you create an HA cluster, the host name of your secondary HA host is changed to *<cluster_host_name>*-secondary. You can't change the host name of a host in an HA cluster.

## Virtual IP Address

When you create an HA cluster, the cluster virtual IP address takes the IP address of the primary HA host.

## Configuring the Cluster

Use the HA wizard to configure the primary host, secondary host, and cluster virtual IP address.

The following items are validated when you configure by using the HA wizard:

- The secondary HA host is not part of another HA cluster.
- The software versions on the primary and secondary HA hosts are the same.
- If the primary HA host is configured with an external storage device, the secondary HA host is configured to access the same external storage device.
- The primary and secondary HA hosts support the same Device Support Module (DSM), scanner, and protocol RPMs.

RELATED DOCUMENTATION

Failovers | 6

Data Consistency for HA | 2

# Failovers

IN THIS SECTION



When a primary or secondary high-availability (HA) host fails, JSA maintains data consistency.

The following scenarios cause failover:

- A power supply failure.
- A network failure that is detected by network connectivity tests.
- An operating system malfunction that delays or stops the heartbeat ping tests.
- A complete Redundant Array of Independent Disks (RAID) failure on the primary HA host.
- A manual failover.
- NFS volumes that become read-only or not writable.

The following scenarios do not cause an automatic HA failover:

- If a JSA process develops an error, stops functioning, or exits with an error.
- If a disk on your primary HA host reaches 95% capacity, JSA data collection stops, but the primary HA host continues to function.

## Primary HA Host Failure

If the secondary high-availability (HA) host detects a primary host failure, it automatically takes over the responsibilities of the primary HA host and becomes the active system.

When a primary HA host is recovered from a failover, it does not automatically take over the active status in the HA cluster. Instead, the secondary HA host remains the active system and the primary host acts as the standby system.

**NOTE**: You must switch the primary back to the active status after successfully recovering from a primary failure.

## Secondary HA Host Failure

If the primary high-availability (HA) host detects a secondary host failure, it automatically assumes the responsibilities of the secondary HA host and becomes the active system.

## HA Failover Event Sequence

JSA initiates a sequence of events when a primary high-availability (HA) host fails.

During failover, the secondary HA host assumes the responsibilities of the primary HA host. The following actions in sequence are completed in sequence:

1. If configured, external shared storage devices are detected and the file systems are mounted. For more information, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.
2. A management interface network alias is created, for example, the network alias for eth0 is eth0:0.
3. The cluster virtual IP address is assigned to the network alias.
4. All JSA services are started.
5. The secondary HA host connects to the console and downloads configuration files.

## Network Connectivity Tests

To test network connectivity, the JSA Console automatically pings all existing managed hosts in your JSA deployment.

If the primary HA JSA console loses network connectivity to a managed host, but the connection to the secondary HA console remains intact, the HA secondary JSA console completes another network connectivity test with the managed hosts. If the test succeeds, the primary HA console completes a controlled failover to the secondary HA console. If the test fails, HA failover is not completed because the secondary HA console might also be experiencing network connectivity problems.

## Heartbeat Ping Tests

You can test the operation of the primary high-availability (HA) host by configuring the time interval of heartbeat ping tests.

If the secondary HA host does not receive a response from the primary HA host within a preconfigured time period, automatic failover to the secondary HA host is completed.

## Primary Disk Failure

If RAID completely fails and all disks are unavailable, the primary HA host completes a shutdown and fails over to the secondary HA host.

After a failover, the primary HA host assumes a status of **Failed**.

## Manual Failovers

You can manually force a failover from a primary high-availability (HA) host to a secondary HA host.

Manually forcing a failover is useful for planned hardware maintenance on a console or managed host. Ensure the following before you conduct a manual failover:

- The primary and secondary HA hosts are synchronized.
- The secondary HA host has a status of standby.

To perform a manual failover on the primary HA host, set the primary system to offline to make the secondary HA host active. After the secondary host becomes active, you can perform maintenance on the primary host.

To perform a manual failover on the secondary HA host, set the secondary system to offline. After the primary host becomes active, you can perform maintenance on the secondary host.

Do not manually force a failover on a primary HA host when you install patches or install software upgrades. For more information, see the *Upgrading Juniper Secure Analytics to 7.5.0*.

## RELATED DOCUMENTATION

Data Consistency for HA | 2

High-availability Clusters | 4

2

CHAPTER

# HA Deployment Planning

# HA Deployment Planning

Plan your high-availability deployment.

Before you implement high-availability (HA), review all the requirements to understand and prepare your JSA deployment.

# Appliance Requirements

**IN THIS SECTION**



Before you add a secondary appliance to your JSA host, you must review the hardware configuration differences between your primary and secondary appliances.

Appliances that you order as primary and secondary HA pairs are matched to ensure compatibility. However, replacing an appliance or adding HA to an older host with a different hardware configuration can lead to data replication issues. Data replication issues can occur when you replace end-of-life hardware or create primary and secondary HA pairs that have appliances from different manufacturers.

## Partition requirements for /store

The combined size of the **/store** and **/transient** partitions on the secondary host must be equal to or larger than the /store partition on the primary host.

For example, do not pair a primary host that uses a 4 TB **/store** partition to a secondary host that has a 2 TB **/store** partition and a 1 TB **/transient** partition.

## Storage Requirements

Follow these storage requirements when you replace an appliance:

- Ensure that the replacement appliance includes storage capacity that is equal to or greater than the original hardware you replace, and be at least 130 gigabytes (GB).
- Secondary replacement appliances can have larger storage capacity than the primary appliance. If so, partitions on the secondary are resized to match the storage capacity of the primary appliance when you configure the HA pair.
- Primary replacement appliances can have larger storage capacity than the secondary appliance. If so, partitions on the primary are resized to match the storage capacity of the secondary appliance when you configure the HA pair.
- If you replace both primary and secondary appliances, then the system resizes the storage partition that is based on the appliance with the smallest capacity.

## Managed Interfaces

- The primary host does not contain more physical interfaces than the secondary.

  If there is a failover, the network configuration of the primary is replicated to the secondary host. If the primary is configured with more interfaces, any additional interfaces cannot be replicated to the secondary during a failover.
- The secondary host must use the same management interface as the primary HA host.

  If the primary HA host uses ens192, for example, as the management interface, the secondary HA host must also use ens192.
- The management interface supports one cluster virtual IP address.
- TCP port 7789 must be open and allow communication between the primary and secondary for Distributed Replicated Block Device (DRBD) traffic.

  DRBD traffic is responsible for disk replication and is bidirectional between the primary and secondary host.
- You must ensure the JSA software version is identical between the primary and secondary host before you pair a primary to a secondary appliance for the first time.

  If the JSA version between your primary and secondary differ, you must patch either the primary or secondary appliance to ensure both appliances use the same software version.

After the primary and secondary appliances are paired together, disk replication ensures that any additional software updates are also applied to the secondary.

## Software and Virtual Appliance Requirements

If you use JSA software on virtual appliances, review the following requirements before you attempt to configure High-availability (HA).

### System Requirements for Virtual Appliances

To ensure that JSA works correctly, ensure that virtual appliance that you use meets the minimum software and hardware requirements.

Your virtual appliance must have at least 256 GB of storage available.

The following table describes the minimum memory requirements for virtual appliances.

**Table 1: Minimum and Suggested Memory Requirements for JSA Virtual Appliances**

| Appliance | Minimum memory requirement | Suggested memory requirement |
|---|---|---|
| JSA Flow Processor Virtual 1299 | 6 GB | 6 GB |
| JSA Flow Processor Virtual | 16 GB | 64 GB |
| JSA Event Collector Virtual | 12 GB | 16 GB |
| JSA Event Processor Virtual<br>up to 20,000 EPS | 16 GB | 64 GB |
| JSA Event Processor Virtual 1699<br>20,000 EPS or higher | 128 GB | 128 GB |

**Table 1: Minimum and Suggested Memory Requirements for JSA Virtual Appliances *(Continued)***

| Appliance | Minimum memory requirement | Suggested memory requirement |
|---|---|---|
| JSA Flow Processor Virtual 1799<br>up to 1,200,000 FPM | 16 GB | 64 GB |
| JSA Flow Processor Virtual 1799<br>1,200,000 FPM or higher | 128 GB | 128 GB |
| JSA Event and Flow Processor Combo<br>5,000 EPS or less<br>200,000 FPM or less | 16 GB | 64 GB |
| JSA Event and Flow Processor Combo<br>30,000 EPS or less<br>1,000,000 FPM or less | 128 GB | 128 GB |
| Virtual JSA All-in-One or Virtual JSA Console<br>5,000 EPS or less<br>200,000 FPM or less | 32 GB | 64 GB |
| Virtual JSA All-in-One or Virtual JSA Console<br>30,000 EPS or less<br>1,000,000 FPM or less | 64 GB | 128 GB |
| Virtual JSA Log Manager | 24 GB | 48 GB |

**Table 1: Minimum and Suggested Memory Requirements for JSA Virtual Appliances *(Continued)***

| Appliance | Minimum memory requirement | Suggested memory requirement |
|---|---|---|
| JSA Risk Manager | 24 GB | 48 GB |
| JSA Vulnerability Manager Processor | 32 GB | 32 GB |
| JSA Vulnerability Manager Scanner | 16 GB | 16 GB |
| JSA App Host | 12 GB | 64 GB or more for a medium sized App Host<br>128 GB or more for a large sized App Host |

The following table describes the minimum CPU requirements for virtual appliances.

**Table 2: CPU Requirements for JSA Virtual Appliances**

| Appliance | Threshold | Minimum number of CPU cores | Suggested number of CPU cores |
|---|---|---|---|
| JSA Flow Processor Virtual 1299 | 10,000 FPM or less | 4 | 4 |
| JSA Event Collector Virtual 1599 | 5,000 EPS or less | 8 | 16 |
| | 20,000 EPS or less | 19 | 19 |
| JSA Event Processor Virtual 1699 | 5,000 EPS or less | 8 | 24 |
| | 20,000 EPS or less | 16 | 32 |
| | 40,000 EPS or less | 40 | 48 |

**Table 2: CPU Requirements for JSA Virtual Appliances *(Continued)***

| Appliance | Threshold | Minimum number of CPU cores | Suggested number of CPU cores |
|---|---|---|---|
| | 80,000 EPS or less | 56 | 80 |
| JSA Flow Processor Virtual 1799 | 150,000 FPM or less | 4 | 24 |
| | 300,000 FPM or less | 8 | 24 |
| | 1,200,000 FPM or less | 16 | 32 |
| | 2,400,000 FPM or less | 40 | 48 |
| | 3,600,000 FPM or less | 56 | 80 |
| JSA Event and Flow Processor Combo | 200,000 FPM or less<br>5,000 EPS or less | 16 | 32 |
| | 300,000 FPM or less<br>15,000 EPS or less | 40 | 48 |
| | 1,200,000 FPM or less<br>30,000 EPS or less | 56 | 80 |
| Virtual JSA All-in-One or Virtual JSA Console | 25,000 FPM or less<br>500 EPS or less | 4 | 24 |
| | 50,000 FPM or less<br>1,000 EPS or less | 8 | 24 |

**Table 2: CPU Requirements for JSA Virtual Appliances *(Continued)***

| Appliance | Threshold | Minimum number of CPU cores | Suggested number of CPU cores |
|---|---|---|---|
| | 100,000 FPM or less<br>1,000 EPS or less | 12 | 24 |
| | 200,000 FPM or less<br>5,000 EPS or less | 16 | 32 |
| | 300,000 FPM or less<br>15,000 EPS or less | 40 | 48 |
| | 1,200,000 FPM or less<br>30,000 EPS or less | 56 | 80 |
| Virtual JSA Log Manager | 2,500 EPS or less | 4 | 16 |
| | 5,000 EPS or less | 8 | 16 |
| JSA Vulnerability Manager Processor | | 4 | 4 |
| JSA Vulnerability Manager Scanner | | 4 | 4 |
| JSA Risk Manager | | 8 | 8 |
| JSA Flow Processor Virtual | | 4 | 16 |

**Table 2: CPU Requirements for JSA Virtual Appliances *(Continued)***

| Appliance | Threshold | Minimum number of CPU cores | Suggested number of CPU cores |
|---|---|---|---|
| JSA App Host | | 4 | 12 or more for a medium sized App Host<br><br>24 or more for a requirements for virtual appliances large sized App Host |

RELATED DOCUMENTATION


- IP Addressing and Subnets | **18**
- Link Bandwidth and Latency | **19**
- Data Backup Requirements | **19**


# IP Addressing and Subnets

To configure high-availability (HA), you must consider the subnet that is used by the secondary HA host and the virtual IP address.

Administrators must ensure that the following conditions are met:

- The secondary host is in the same subnet as the primary host.
- When the IP address of the primary host is reassigned as a cluster virtual IP, the new IP address that you assign must be in the same subnet.
- The secondary HA host that you want to add to the HA cluster is not a component in another HA cluster.

RELATED DOCUMENTATION


- Link Bandwidth and Latency | **19**
- Data Backup Requirements | **19**

Offboard Storage Requirements for HA | 20

# Link Bandwidth and Latency

To configure high-availability (HA), you must consider the bandwidth and latency between the primary and secondary HA hosts.

If your HA cluster is using disk synchronization, the following conditions must be met:

- The connection between the primary and secondary HA host has a minimum bandwidth of 1 gigabits per second (Gbps).
- The latency between the primary and secondary HA host is less than 2 milliseconds (ms).

**NOTE**: If your HA solution uses a wide area network (WAN) to geographically distribute the hosts in your cluster, latency increases with distance. If latency rises above 2 ms, then system performance is affected.

RELATED DOCUMENTATION

Data Backup Requirements | 19
Offboard Storage Requirements for HA | 20
IP Addressing and Subnets | 18

# Data Backup Requirements

There are items to consider for data backup before you configure hosts for High-availability (HA).

If a backup archive originates on an HA cluster, click **Deploy Full Configuration** to restore the HA cluster configuration after the restore is complete. If disk replication is enabled, the secondary HA host immediately synchronizes data after the system is restored.

If the secondary HA host is removed from the deployment after a backup is completed, the secondary HA host displays a **Failed** status on the **System and License Management** window.

For more information about restoring backup archives in an HA environment, see the *Juniper Secure Analytics Administration Guide*.

RELATED DOCUMENTATION

Offboard Storage Requirements for HA | 20
IP Addressing and Subnets | 18
Link Bandwidth and Latency | 19

# Offboard Storage Requirements for HA

You can implement high-availability (HA) when the JSA **/store** partition is mounted to an external storage solution, such as an iSCSI.

If you implement an external storage solution, the data that is received by the primary HA host is automatically moved to the external device. It remains accessible for searching and reporting.

If a failover occurs, the **/store** partition on the secondary HA host is automatically mounted to the external device. On the external device, it continues to read and write to the data received by the primary HA host before the failover.

For more information about configuring shared external storage with HA, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.

Administrators must review the following HA requirements before you implement an offboard storage device:

- The primary HA host must be configured to communicate with the external device. The data in the **/store** partition of the local disk must be moved to the external storage device.
- The secondary HA host must be configured to communicate with the external device. In doing so, when a primary HA host fails over, the secondary HA host can detect the external storage device.
- You must create an HA cluster only after the secondary HA host is configured to access the same external storage device.
- If you must reconfigure your external storage device or HA cluster settings, you must remove the HA cluster between the primary and secondary HA host. For more information, see "Disconnecting an HA Cluster" on page 29.
- Ensure that there is at least a 1 Gbps connection between each HA host and your external device.

**NOTE**: During an upgrade to JSA, you must reconfigure the external storage device connections to the hosts in your HA cluster. For more information, see the *Juniper Secure Configuring Offboard Storage Guide*.

## RELATED DOCUMENTATION

IP Addressing and Subnets | **18**

Link Bandwidth and Latency | **19**

Data Backup Requirements | **19**

3

CHAPTER

# HA Management

# HA Management

If you are required to tune, troubleshoot, or update your high-availability (HA) settings, use the **System and License Management** window on the JSA**Admin** tab.

Administrators can use the **System and License management** window to complete the following HA tasks:

- Monitor the state of an HA cluster.
- Force the manual failover of a primary HA host to complete maintenance on the primary host.
- Disconnect an HA cluster to alter the partitions of the primary and secondary HA hosts.
- Configure the ping test time period after which automatic failover to a secondary HA host occurs.
- Modify the HA cluster settings that are used to control network connectivity testing.

# Status Of HA Hosts

You can review the status of the primary and secondary host in your high-availability (HA) cluster.

The following table describes the status of each host that is displayed in the **System and License Management** window:

**Table 3: HA Status Descriptions**

| Status | Description |
|---|---|
| Active | Specifies that the host is the active system and that all services are running normally. The primary or secondary HA host can display the active status.<br><br>**NOTE**: If the secondary HA host displays the active status, the primary HA host failed. |
| Standby | Specifies that the host is acting as the standby system. In the standby state, no services are running but data is synchronized if disk replication is enabled. If the primary or secondary HA host fails, the standby system automatically becomes the active system. |

**Table 3: HA Status Descriptions *(Continued)***

| Status | Description |
|---|---|
| Failed | Specifies that the primary or secondary host failed.<br><br>If the primary HA host displays Failed, the secondary HA host assumes the responsibilities of the primary HA host and displays the Active status.<br><br>If the secondary HA host displays Failed, the primary HA host remains active, but is not protected by HA.<br><br>A system in a failed state must be manually repaired or replaced, and then restored. If the network fails, you might need access to the physical appliance. |
| Synchronizing | Specifies that data is synchronizing between hosts.<br><br>**NOTE**: This status is displayed only when disk replication is enabled. |
| Online | Specifies that the host is online. |
| Offline | Specifies that an administrator manually set the HA host offline. Offline mode indicates a state that is typically used to complete appliance maintenance.<br><br>When an appliance indicates a status of offline:<br><br>Data replication is functioning between the active and offline HA hosts.<br><br>Services that process events, flows, offenses, and heartbeat ping tests are stopped for the offline HA host.<br><br>Failover cannot occur until the administrator sets the HA host online. |
| Restoring | Specifies that the host is restoring. For more information, see "Verifying the Status Of Primary and Secondary Hosts" on page 44. |
| Needs License | Specifies that a license key is required for the HA cluster. In this state, no processes are running.<br><br>For more information about applying a license key, see your *Juniper Secure Analytics Administration Guide*. |
| Setting Offline | Specifies that an administrator is changing the status of an HA host to offline. |

**Table 3: HA Status Descriptions *(Continued)***

| Status | Description |
|---|---|
| Setting Online | Specifies that an administrator is changing the status of an HA host to online |
| Needs Upgrade | Specifies that the secondary HA host requires a software upgrade.<br><br>When the **Needs Upgrade** status is displayed, the primary remains active, but is not protected against failover. Disk replication of events and flows continues between the primary and the secondary HA hosts. |
| Upgrading | Specifies that the secondary HA host is being upgraded by the primary HA host.<br><br>If the secondary HA host displays the Upgrading status, the primary HA host remains active, but is not protected by HA. Heartbeat monitoring and disk replication, if enabled, continue to function.<br><br>After DSMs or protocols are installed and deployed on a Console, the Console replicates the DSM and protocol updates to its managed hosts. When primary and secondary HA hosts are synchronized, the DSM and protocols updates are installed on the secondary HA host.<br><br>Only a secondary HA host can display an Upgrading status. |

RELATED DOCUMENTATION

Viewing HA Cluster IP Addresses | 25

Creating an HA Cluster | 26

Disconnecting an HA Cluster | 29

# Viewing HA Cluster IP Addresses

You can display the IP addresses of all the components in your High-availability (HA) cluster.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.

4. Identify the JSA primary console.
5. Hover your mouse over the **host name** field.

RELATED DOCUMENTATION

Creating an HA Cluster | 26

Disconnecting an HA Cluster | 29

Editing an HA Cluster | 30

# Creating an HA Cluster

Pairing a primary host, secondary high-availability (HA) host, and a virtual IP address using JSA creates an HA cluster.

- If external storage is configured for a primary HA host, you must also configure the secondary HA host to use the same external storage options. For more information, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.
- Ensure that no undeployed changes exist before you create an HA cluster.

If disk synchronization is enabled, it might take 24 hours or more for the data in the **/store** partition on the primary HA host **/store** partition to initially synchronize with the secondary HA host.

If the primary HA host fails and the secondary HA host becomes active, the Cluster Virtual IP address is assigned to the secondary HA host.

In an HA deployment, the interfaces on both the primary and secondary HA hosts can become saturated. If performance is impacted, you can use a second pair of interfaces on the primary and secondary HA hosts to manage HA and data replication. Use a crossover cable to connect the interfaces.

**NOTE**: You can enable a crossover connection during and after the creation of an HA cluster and this does not cause any event collection downtime.

1. On the navigation menu, click **Admin**.
2. Click **System and License Management**.
3. Select the host for which you want to configure HA.
4. From the **Actions** menu, select **Add HA Host** and click **OK**.
5. Read the introductory text. Click **Next**.

6. Type values for the parameters:

| Option | Description |
|---|---|
| Primary Host IP address | A new primary HA host IP address. The new IP address replaces the previous IP address. The current IP address of the primary HA host becomes the Cluster Virtual IP address.<br><br>The new primary HA host IP address must be on the same subnet as the virtual host IP address. |
| Secondary HA host IP address | The IP address of the secondary HA host. The secondary HA host must be on the same subnet as the primary HA host. |
| Enter the root password of the host | The root password for the secondary HA host. The password must not include special characters. |
| Confirm the root password of the host | The root password for the secondary HA host again for confirmation. |

7. To configure advanced parameters, click the arrow beside **Show Advanced Options** and type values for the parameters.

| Option | Description |
|---|---|
| Heartbeat Interval (seconds) | The time, in seconds, that you want to elapse between heartbeat pings. The default is 10 seconds.<br><br>For more information about heartbeat pings, see "Heartbeat Ping Tests" on page 8. |
| Heartbeat Timeout (seconds) | The time, in seconds, that you want to elapse before the primary HA host is considered unavailable if no heartbeat is detected. The default is 30 seconds. |

*(Continued)*

| Option | Description |
|---|---|
| Network Connectivity Test List peer IP addresses (comma delimited) | The IP addresses of the hosts that you want the secondary HA host to ping. The default is to ping all other managed hosts in the JSA deployment.<br><br>For more information about network connectivity testing, see "Network Connectivity Tests" on page 8. |
| Disk Synchronization Rate (**MB/s**) | The disk synchronization rate. The default is 100 MB/s.<br><br>Increase this value to 1100 MB/s when you are using 10 G crossover cables.<br><br>**NOTE**: Do not exceed your system's capacity. The limit for Distributed Replicated Block Devices is 4096 MB/ s. |
| Disable Disk Replication | This option is displayed only when you are configuring an HA cluster by using a managed host. |
| Configure Crossover Cable | Crossover cables allow JSA to isolate the replication traffic from all other JSA traffic, such as events, flows, and queries.<br><br>You can use crossover cables for connections between 10 Gbps ports, but not the management interface. |
| Crossover Interface | Select the interfaces that you want to connect to the primary HA host.<br><br>**NOTE**: All interfaces with an established link, or an undetermined link, appear in the list. Select interfaces with established links only. |
| Crossover Advanced Options | Select **Show Crossover Advanced Options** to enter, edit, or view the property values. |

8. Click **Next**, and then click **Finish**.

> **NOTE**: When an HA cluster is configured, you can display the IP addresses that are used in the HA cluster. Hover your mouse over the **Host Name** field on the **System and License Management** window.

9. On the navigation menu, click **Admin**.
10. Click **Admin >Advanced >Deploy Full Configuration** to enable network connectivity tests.

RELATED DOCUMENTATION


- Disconnecting an HA Cluster | 29
- Editing an HA Cluster | 30
- Setting an HA Host Offline | 31


# Disconnecting an HA Cluster

IN THIS SECTION



By disconnecting an HA cluster, the data on your primary HA console or managed host is not protected against network or hardware failure.

If you migrated the **/store** file system to a Fibre Channel device, you must modify the **/etc/fstab** file before you disconnect the HA cluster. For more information, see "Updating the /etc/fstab File" on page 30.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the HA host that you want to remove.
5. From the toolbar, select **High Availability** > **Remove HA Host**.

6. Click **OK**.

> **NOTE**: When you remove an HA host from a cluster, the host restarts.

- "Updating the /etc/fstab File" on page 30
  Before you disconnect a Fibre Channel HA cluster, you must modify the **/store** and **/storetmp** mount information in the **/etc/fstab** file.

## Updating the /etc/fstab File

Before you disconnect a Fibre Channel HA cluster, you must modify the **/store** and **/storetmp** mount information in the **/etc/fstab** file.

You must update the **/etc/fstab** file on the primary HA host and the secondary HA host.

1. Use SSH to log in to your JSA host as the root user:
2. Modify the **etc/fstab** file.
   a. Locate the existing mount information for the **/store** and **/storetmp** file systems.
   b. Remove the **noauto** option for the **/store** and **/storetmp** file systems.
3. Save and close the file.

RELATED DOCUMENTATION

Editing an HA Cluster | 30
Setting an HA Host Offline | 31

# Editing an HA Cluster

You can edit the advanced options for your HA cluster.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.

4. Select the row for the HA cluster that you want to edit.
5. From the toolbar, select **High Availability >Edit HA Host**.
6. Edit the parameters in the table in the advanced options section.
7. Click **Next**.
8. Review the information.
9. Click **Finish**.

RELATED DOCUMENTATION


- Setting an HA Host Offline | 31
- Setting an HA Host Online | 32
- Switching a Primary HA Host to Active | 32


# Setting an HA Host Offline

You can set the primary or secondary high-availability (HA) host to **Offline** from the **Active** or **Standby** state.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the HA host that you want to set to offline.
5. From the toolbar, select **High Availability >Set System Offline**.

RELATED DOCUMENTATION


- Setting an HA Host Online | 32
- Switching a Primary HA Host to Active | 32
- Editing an HA Cluster | 30

# Setting an HA Host Online

You can set the primary or secondary HA host to Online.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Select the offline HA host that you want to set to Online.
5. From the toolbar, select **High Availability >Set System Online**.

On the **System and License Management** window, verify the status of the HA host. Choose from one of the following options:

- If the primary HA host displays a status of **Active**, HA host is restored.
- If you experience a problem, restore the primary or secondary HA host. For more information, see "Restoring a Failed Secondary HA Host" on page 42 or "Restoring a Failed Primary HA Host" on page 43.

RELATED DOCUMENTATION

Switching a Primary HA Host to Active | 32
Editing an HA Cluster | 30
Setting an HA Host Offline | 31

# Switching a Primary HA Host to Active

You can set the primary high-availability (HA) host to be the active system.

The primary HA host must be the standby system and the secondary HA host must be the active system.

If your primary host is recovered from a failure, it is automatically assigned as the standby system in your HA cluster. You must manually switch the primary HA host to be the active system and the secondary HA host to be the standby system.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.

3. Click the **System and License Management** icon.
4. In the **System and License Management** window, select the **secondary HA host**.
5. From the toolbar, select **High Availability >Set System Offline**.

   Your primary HA host is automatically switched to be the Active HA host.

   **NOTE**: Your JSA user interface might be inaccessible during this time. To return the secondary HA host to standby and return the primary HA host to active run either of the following commands:

   - From the active host run:

     **/opt/qradar/ha/bin/ha giveback**

     The host that was active is now the standby host and the standby host is now the active host.

   - From the standby host run:

     **/opt/qradar/ha/bin/ha takeover**

     The host that was on standby is now the active host and the host that was the active host is now the standby host.

6. In the **System and License Management** window, select the **secondary HA host**.
7. From the toolbar, select **High Availability >Set System Online.**

   Your secondary HA host is now the standby system.

When you can access the **System and License Management** window, check the **status** column. Ensure that the primary HA host is the active system and the secondary HA host is the standby system.

## RELATED DOCUMENTATION

Editing an HA Cluster | 30

Setting an HA Host Offline | 31

Setting an HA Host Online | 32

4

CHAPTER

# Recovery Options for HA Appliances

# Recovery Options for HA Appliances

You can reinstall or recover JSA high-availability (HA) appliances.

If your HA cluster uses shared storage, manually configure your external storage device. For more information, see the *Juniper Secure Analytics Configuring Offboard Storage Guide*.

RELATED DOCUMENTATION



# Recovering a Failed Primary HA Host

You can recover a failed primary high-availability (HA) JSA host if the build version of the primary HA host is the same as the JSA build version installed on the secondary HA host.

Ensure that the following requirements are met:

- The required hardware is installed.
- You need the cluster virtual IP address and the primary HA host IP address. You can identify the IP address in the System and License Management window. For more information, see "Viewing HA Cluster IP Addresses" on page 25.
- A keyboard and monitor are connected by using the VGA connection.

1. Type root at the login prompt to start the installation wizard.
2. Accept the End User License Agreement.
3. Select the appliance type:
   - Appliance Install
   - Software Install

> **NOTE**: You must choose the same appliance type as the failed primary. Do not chose an HA standby appliance.

4. In the Type of Setup window, select **HA Recovery Setup**.
5. Follow the instructions in the wizard.
6. Configure the JSA network settings.
   a. In the Cluster Virtual IP Address Setup window, enter the cluster virtual IP address.
   b. In the Network Information Setup window, enter the original hostname and the IP address of the primary HA host.

> **NOTE**: When an HA cluster is created, "-primary" is appended to the original hostname of the primary HA host. Do not include "-primary" when you enter the original hostname in the Network Information Setup window.

7. Configure the JSA root password.
8. Review your software version. If your secondary HA host patch version is newer than the software on this appliance, download and install the SFS from Juniper Support website to upgrade this appliance to match the software version.
9. Log in to the JSA user interface.
10. Select **Main menu** > **Admin** > **System and License Management** > **Systems**.
11. Highlight the primary HA host that you are restoring and select **High Availability** > **Restore System**.

RELATED DOCUMENTATION


- Recovering a Failed Secondary HA Host | 36
- Restoring a Primary HA Host to a Previous Version or Factory Default | 37
- Restoring a Secondary HA Host to a Previous Version or Factory Default | 38


# Recovering a Failed Secondary HA Host

You can recover a failed secondary high-availability (HA) JSA host if the build version of the secondary HA host must be the same as the JSA build version installed on the primary HA host.

Ensure that the following requirements are met:

- The required hardware is installed.
- You need the secondary HA host IP address. You can identify the IP address in the **System and License Management** window.
- A keyboard and monitor are connected by using the VGA connection.

1. Type `root` at the login prompt to start the installation wizard.
2. Accept the End User License Agreement.
3. Select the appliance type: **High Availability Appliance**.
4. Follow the instructions in the wizard.
5. Configure the JSA root password.
6. Review your software version. If your secondary HA host patch version is newer than the software on this appliance, download and install the SFS (software fix/patch) from Juniper Support website to upgrade this appliance to match the software version.
7. Log in to the JSA user interface.
8. Select **Main menu** > **Admin** > **System and License Management** > **Systems**.
9. Highlight the secondary HA host that you are restoring and select **High Availability** > **Restore System**.

RELATED DOCUMENTATION

Recovering a Failed Primary HA Host | 35

Restoring a Primary HA Host to a Previous Version or Factory Default | 37

Restoring a Secondary HA Host to a Previous Version or Factory Default | 38

# Restoring a Primary HA Host to a Previous Version or Factory Default

Restore the JSA primary high-availability (HA) host to a previous version or factory default. You can restore a failed JSA primary HA host that does not include a recovery partition or a USB port to a previous version. You can also restore the system to factory defaults. When you restore the failed primary HA host, all data is removed and the factory default configuration is restored on the host.

1. Use SSH to log in to the console as the root user.

2. Copy the recovery.py script from the console to the failed primary HA host.

```
scp recovery.py root@<TargetIP_address>:/root
```

3. Obtain the JSA ISO from the following location: Juniper Support website
4. Copy the ISO file to the target JSA host.

```
scp <iso_file_name> root@<TargetIP_address>:/root
```

5. Use SSH to log in to the primary HA host.
6. Type the following commands:

```
chmod 755 recovery.py
./recovery.py -r --default --reboot <iso_file_name>
```

7. Press Enter when prompted to restart the system.
8. When prompted, type flatten and press Enter.

The installer repartitions and reformats the hard disk, installs the operating system, and then installs JSA. Wait for the flatten process to complete. This process can take up to several minutes. After the process is complete, the normal installation process continues.

RELATED DOCUMENTATION


- Recovering a Failed Primary HA Host | 35
- Recovering a Failed Secondary HA Host | 36
- Restoring a Secondary HA Host to a Previous Version or Factory Default | 38


# Restoring a Secondary HA Host to a Previous Version or Factory Default

Restore the JSA secondary high-availability (HA) host to a previous version or factory default. You can restore a failed JSA secondary HA host that does not include a recovery partition or a USB port to a previous version. You can also restore the system to factory defaults. When you restore the failed secondary HA host, all data is removed and the factory default configuration is restored on the host.

1. Use SSH to log in to the console as the root user.
2. Copy the recovery.py script from the console to the failed secondary HA host.

```
scp recovery.py root@<TargetIP_address>:/root
```

3. Obtain the JSA ISO from the following location: Juniper Support website
4. Copy the ISO file to the target JSA host.

```
scp <iso_file_name> root@<TargetIP_address>:/root
```

5. Use SSH to log in to the secondary HA host.
6. Type the following commands:

```
chmod 755 recovery.py
./recovery.py -r --default --reboot <iso_file_name>
```

7. Press Enter when prompted to restart the system.
8. When prompted, type flatten and press Enter.

The installer repartitions and reformats the hard disk, installs the operating system, and then installs JSA. Wait for the flatten process to complete. This process can take up to several minutes. After the process is complete, the normal installation process continues.

## RELATED DOCUMENTATION

Recovering a Failed Primary HA Host | 35

Recovering a Failed Secondary HA Host | 36

Restoring a Primary HA Host to a Previous Version or Factory Default | 37

5
CHAPTER

# Troubleshooting JSA HA Deployments

# Troubleshooting JSA HA Deployments

IN THIS SECTION



Use the status of the HA hosts in the **System and License Management** window to help you troubleshoot.

## Status Combinations and Possible Resolutions

The following table describes the possible status settings for primary and secondary HA hosts. Each status combination requires a different troubleshooting approach.

**Table 4: System and License Management Window Host Statuses**

| Primary HA host status | Secondary HA host status | Possible action |
|---|---|---|
| Active | Failed or Unknown | Ensure that the secondary host is on, and that you can log on to it as a root user by using SSH. If you can connect, see "Restoring a Failed Secondary HA Host" on page 42. |
| Failed or Unknown | Active | Ensure that the primary host is on, and that you can log on to it as a root user by using SSH. If you can connect, see "Restoring a Failed Primary HA Host" on page 43. |
| Unknown | Unknown | If you cannot connect to the primary or secondary HA host by using SSH, ensure that your network and hardware configuration is operational. |

**Table 4: System and License Management Window Host Statuses *(Continued)***

| Primary HA host status | Secondary HA host status | Possible action |
|---|---|---|
| Offline | Active | To set the primary host online, see "Restoring a Failed Primary HA Host" on page 43. |

## Identifying Active Hosts

You can identify the most recent active host in your HA cluster by using SSH.

1. To display the HA cluster configuration, type the following command:

   **/opt/qradar/ha/bin/ha cstate**

2. Review the following line: in the output:

   **Local: R:PRIMARY S:ACTIVE/ONLINE CS:NONE P:1:0 HBT:UP RTT:2 1:0 SI:4105589 Remote: R:SECONDARY S:STANDBY/ONLINE CS:NONE P:1.0 HBC:UP RTT:2 I:11753 SI:1382557**

   - If the output displays `Local: R:PRIMARY S:ACTIVE/`, the primary HA Host is the active system.
   - If the output displays `Remote: R:SECONDARYS:ACTIVE/ONLINE`, the secondary HA Host is the active system.

# Restoring a Failed Secondary HA Host

You can restore a failed secondary HA host.

**NOTE**: Restore only a failed secondary host, or a secondary host with unknown status. If you reinstall the HA secondary host, the state changes to standby.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click **System and License Management**.

4. Select the secondary HA host that you want to restore.
5. From the **High Availability** menu, click **Restore System**.
6. If the secondary HA host displays a status of **Failed** or **Unknown** in the **System and License Management** window, use SSH to log in to the secondary HA host as the root user to ensure that the host is operational.
7. Restart the secondary HA host by typing **reboot**.
8. After the system is restarted, if the secondary HA host displays a status of **Failed** or **Unknown**, from the **High Availability** menu, click **Restore System**.

RELATED DOCUMENTATION

Restoring a Failed Primary HA Host | 43

Verifying the Status Of Primary and Secondary Hosts | 44

Setting the Status Of the Primary HA Host to Online | 44

# Restoring a Failed Primary HA Host

You can restore a failed primary HA host.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click **System and License Management**.
4. Select the primary HA host that you want to restore.
5. From the **High Availability** menu, click **Restore System**.
6. Verify the status of the primary HA host.
7. If the primary HA host displays a status of **Offline**, in the **System and License Management** window, click **High Availability >Set System Online**.
8. If the primary HA host displays a status of **Failed** or **Unknown** in the **System and License Management** window, use SSH to log in to the primary HA host as the root user to ensure that the host is operational.
9. Restart the primary HA host by typing the following command: **reboot**

RELATED DOCUMENTATION

Verifying the Status Of Primary and Secondary Hosts | 44

Setting the Status Of the Primary HA Host to Online | 44

Restoring a Failed Secondary HA Host | 42

# Verifying the Status Of Primary and Secondary Hosts

You must verify that the primary and secondary HA hosts are operational.

1. Identify whether the primary HA host was configured as a console or managed host.
2. If the primary HA host is configured as a console, use SSH to log in to the Cluster Virtual IP address as the root user:
   - If you can connect to the Cluster Virtual IP address, restore access to the JSA. For more information, see the *Juniper Secure Analytics Troubleshooting Guide*.
   - If you cannot connect to the Cluster Virtual IP address, use SSH to log in to the secondary HA host as the root user to ensure that it is operational.
3. If your secondary host is configured as a managed host, use SSH to log in to the secondary HA host as the root user.
   - If you cannot connect to the primary or secondary HA host by using SSH, ensure that your network and hardware configuration is operational.
   - If you can connect to the primary and secondary HA host, identify the most recently active HA host in your HA cluster.

RELATED DOCUMENTATION

Setting the Status Of the Primary HA Host to Online | 44

Restoring a Failed Secondary HA Host | 42

Restoring a Failed Primary HA Host | 43

# Setting the Status Of the Primary HA Host to Online

If the primary HA host displays a status of offline, you can reset the status to online.

1. On the navigation menu, click **Admin**.
2. On the navigation menu, click **System Configuration**.
3. Click **System and License Management**.
4. Select the primary HA host that you want to restore.
5. In the **System and License Management** window, if the primary HA host displays a status of **Offline**, your must restore the primary HA host.

## RELATED DOCUMENTATION


- Restoring a Failed Secondary HA Host | 42
- Restoring a Failed Primary HA Host | 43
- Verifying the Status Of Primary and Secondary Hosts | 44

CHAPTER 6

# Recovery Solution for JSA Deployments

# Recovery Solution for JSA Deployments

IN THIS SECTION



Maintaining data redundancy is crucial to resiliency and recovery from data loss. There are a wide variety of solutions that are currently deployed in the field to prevent and recover from data loss, and vary greatly in terms of complexity, cost, and effectiveness. JSA provides the QRadar Data Synchronization app as a solution to maintain your configuration and data during a failure of you main site.

## QRadar Data Synchronization App

The QRadar Data Synchronization app mirrors your data to another identical system. It is possible to maintain configurations and data when you have two identical JSA systems in separate geographic environments that are a mirror of each other. Data is collected at both sites and ensures operations can continue to function as normally as possible in scenarios when your main site fails.

QRadar Data Synchronization forwards live data, for example, flows and events from the main site's JSA to a parallel destination site. You can set up data synchronization with deployments that are in different geographical locations.

To use the QRadar Data Synchronization app, the main site and destination site deployments must be running JSA 7.4.0 FixPack 3 or later. The destination site must be a fully duplicated deployment (1:1 host ratio) for hosts that contain or collect Ariel (event and flow) data. This includes Event Processors, Flow Processors, All in one Event Processors and Flow Processors, Event Collectors, Flow Processors, consoles, and data nodes. However, JSA Risk Manager, JSA Vulnerability Manager, and QRadar App Host do not require 1:1 mapping.

A high-availability (HA) cluster is considered one host and the Data Synchronization app supports a HA cluster that is paired with a non-HA host.

**NOTE**: App data backup is currently not available using the Data Synchronization app.