Extreme Networks SIEM High Availability Guide

9034876

Published July 2015

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks/

Support

For product support, including documentation, visit: www.extremenetworks.com/documentation/

For information, contact:
Extreme Networks, Inc.
145 Rio Robles
San Jose, California 95134
USA

Table of Contents

Introduction to Extreme Security high-availability deployments

Administrators can protect Extreme Networks Security Analytics data by implementing a high-availability (HA) solution.

Intended audience

Extreme SIEM administrators who are responsible for installing and deploying the product must know their corporate network infrastructure, the Linux™ operating system, and networking technologies.

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. Extreme Networks® systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. EXTREME NETWORKS DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Note

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. Extreme Networks Security Analytics may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of Extreme Networks Security Analytics.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that are used throughout this guide.

Table 1: Notice Icons

Icon	Notice Type	Alerts you to...
👉	Tip	Helpful tips for using the product.
📌	Note	Important features or instructions.
⚠	Caution	Risk of personal injury, system damage, or loss of data.
⚠	Warning	Risk of severe personal injury.
New	New	This command or section is new for this release.

Table 2: Text Conventions

Convention	Description
`Screen displays`	This typeface indicates command syntax, or represents information as it appears on the screen.
The words **enter** and **type**	When you see the word "enter" in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says "type."
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del]
Words in italicized type	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.

Terminology

When features, functionality, or operation is specific to a switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the "switch."

Providing Feedback to Us

We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team about this document, please contact us using our short online feedback form. You can also email us directly at InternalInfoDev@extremenetworks.com.

Getting Help

If you require assistance, contact Extreme Networks Global Technical Assistance Center using one of the following methods:

Web	www.extremenetworks.com/support
Phone	1-800-872-8440 (toll-free in U.S. and Canada) or 1-603-952-5000 For the Extreme Networks support phone number in your country: www.extremenetworks.com/support/contact
Email	support@extremenetworks.com To expedite your message, enter the product name or model number in the subject line.

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number
- A description of the failure
- A description of any action(s) already taken to resolve the problem (for example, changing mode switches or rebooting the unit)
- The serial and revision numbers of all involved Extreme Networks products in the network
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load and frame size at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any previous Return Material Authorization (RMA) numbers

Related Publications

The Extreme Security product documentation listed below can be downloaded from http://documentation.extremenetworks.com.

Extreme Security Analytics Threat Protection

- *Extreme Networks Security API Reference Guide*
- *Extreme Networks Security Application Configuration Guide*
- *Extreme Networks Security Ariel Query Language Guide*
- *Extreme Networks Security DSM Configuration Guide*
- *Extreme Security DSM Configuration Guide Addendum*
- *Extreme Networks Security Hardware Guide*
- *Extreme Networks Security Installation Guide*
- *Extreme Networks Security Juniper NSM Plug-in User Guide*
- *Extreme Networks Security Log Manager Administration Guide*

- *Extreme Networks Security Log Sources User Guide*
- *Extreme Networks Security Managing Log Sources Guide*
- *Extreme Networks Security Offboard Storage Guide*
- *Extreme Security Release Notes*
- *Extreme Networks Security Risk Manager Adapter Configuration Guide*
- *Extreme Networks Security Risk Manager Getting Started Guide*
- *Extreme Networks Security Risk Manager Installation Guide*
- *Extreme Networks Security Risk Manager Migration Guide*
- *Extreme Networks Security Risk Manager User Guide*
- *Extreme Networks Security Troubleshooting System Notifications Guide*
- *Extreme Networks Security Upgrade Guide*
- *Extreme Networks Security Vulnerability Manager Release Notes*
- *Extreme Networks Security Vulnerability Manager User Guide*
- *Extreme Networks Security WinCollect User Guide*
- *Extreme Networks SIEM Administration Guide*
- *Extreme Networks SIEM Getting Started Guide*
- *Extreme Networks SIEM High Availability Guide*
- *Extreme Networks SIEM Troubleshooting Guide*
- *Extreme Networks SIEM Tuning Guide*
- *Extreme Networks SIEM Users Guide*
- *Migrating Extreme Security Log Manager to Extreme SIEM*

Extreme Security Threat Protection

- *Extreme Security Intrusion Prevention System Hardware Replacement Guide*
- *Extreme Security Threat Protection Release Notes*

1 HA overview

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

To enable HA, Extreme Security 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.

For more information about using shared external storage with HA, for example iSCSI, Fibre Channel, or NFS, see the *Extreme Networks Security Offboard Storage Guide*.

Unless otherwise noted, all references to Extreme Security refer to Extreme SIEM and Extreme Networks Security Log Manager.

Related Links

HA clusters on page 10
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

Data consistency for HA on page 8
When an HA failover occurs, Extreme Networks Security Analytics ensures the consistency of your data.

Data consistency for HA

When an HA failover occurs, Extreme Networks Security Analytics 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 or Fibre Channel external storage device. See Offboard storage requirements for HA on page 19.

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

DRBD is not enabled by default for an Extreme Networks Security QFlow Collector. To synchronize Extreme Security QFlow data, you must configure an HA cluster by using the console or managed host that is collecting Extreme Security QFlow data.

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.

Related Links

HA overview on page 8

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

Link bandwidth and latency on page 18

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

Status of HA hosts on page 20

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

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 by using DRBD.

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.

Related Links

Status of HA hosts on page 20

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

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. The HA host uses Distributed Replicated Block Device (DRBD).

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 before it can become the active host. Disk replication with the secondary HA host is enabled while the primary HA host remains offline.

When the primary HA host is restored, 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.

Related Links

Setting an HA host online on page 26

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

HA clusters

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

Primary HA host

The primary HA host is any console or managed host in your Extreme SIEM deployment that requires protection from data loss in the event of 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.

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.

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 has a valid HA activation key.
- 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 Links

HA overview on page 8

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

Creating an HA cluster on page 22

Primary HA host failure on page 11

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

Status of HA hosts on page 20

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

Creating an HA cluster on page 22

IP addressing and subnets on page 18

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

Failovers

When a primary or secondary high-availability (HA) host fails, Extreme Networks Security Analytics 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.
- A management interface failure on the primary HA host.

Primary HA host failure

If the secondary high-availability (HA) host detects a primary 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.

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

Related Links

HA clusters on page 10

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

Switching a primary HA host to active on page 27

Secondary HA host failure

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

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

Non-failover scenarios

HA failover does not occur when Extreme Networks Security Analytics detects software errors or disk capacity issues.

The following issues do not cause an automatic HA failover:

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

HA failover event sequence

Extreme Networks Security Analytics 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 *Extreme Networks Security 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 Extreme Security services are started.
5 The secondary HA host connects to the console and downloads configuration files.

Network connectivity tests

To test network connectivity, the primary high-availability (HA) host automatically pings all existing managed hosts in your Extreme Networks Security Analytics deployment.

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

Related Links

Creating an HA cluster on page 22

Creating an HA cluster on page 22

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.

Related Links

Creating an HA cluster on page 22

Creating an HA cluster on page 22

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.

Related Links

Status of HA hosts on page 20

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

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.

Hardware maintenance on a primary and secondary HA host is conducted while the secondary HA host is in standby. Set the secondary HA host offline and power off the primary HA host. If the primary and secondary HA hosts are synchronizing, power off the primary.

For more information about manual failovers, see *Setting an HA host offline.*

Do not manually force a failover on a primary HA host when you install patches or install software upgrades. For more information, see the *Extreme Networks Security Upgrade Guide*.

Related Links

Setting an HA host offline on page 26

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

2 HA deployment planning

Plan your high-availability deployment.

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

Appliance requirements

Before you add a secondary host to your Extreme Networks SIEM Console, 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 Console 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.

/Store partition requirements

- The file system of the `/store` partition must match between your primary and secondary host.

  Example
  If the `/store` partition on the primary uses ext-3 as the file system, then your secondary must also use ext-3 for `/store`. A mismatch of the file system for the `/store` partition is not allowed.

- The size of the `/store` partition on the secondary must be equal to or larger than the `/store` partition of the primary.

For example, do not pair a primary host that uses a 3 TB `/store` partition to a secondary host that has a 2 TB `/store` 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.
- 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 eth0, for example, as the management interface, the secondary HA host must also use eth0.
- 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 Extreme Security 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 Extreme Security 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.
- Ensure that the secondary host has a valid HA activation key.

Software and virtual appliance requirements

If you install Extreme SIEM software on your own hardware or use virtual appliances, review the following requirements before you attempt to configure High-availability (HA).

System requirements for virtual appliances

To ensure that Extreme Networks Security Analytics works correctly, ensure that virtual appliance that you use meets the minimum software and hardware requirements.

Before you install your virtual appliance, ensure that the following minimum requirements are met:

Table 3: Requirements for virtual appliances

Requirement	Description
VMware client	VMWare ESX 5.0 VMWare ESX 5.1 VMWare ESX 5.5 For more information about VMWare clients, see the VMware website (www.vmware.com)
Virtual disk size on VFlow Collector, Extreme Security Event Collector, Extreme Security Event Processor, Extreme Security Flow Processor, Extreme Security All-in-One, and Log Manager appliances	Minimum: 256 GB Important For optimal performance, ensure that an extra 2-3 times of the minimum disk space is available.
Virtual disk size for QFlow Collector appliances	Minimum: 70 GB
Virtual disk size for Risk Manager appliances	Suggested virtual disk size for implementation with up to 10000 configuration sources: 1 TB.
Virtual disk size for Extreme Security Vulnerability Manager processor appliances	50000 IPs - 500 GB 150000 IPs - 750 GB 300000 IPs - 1 TB
Virtual disk size for Extreme Security Vulnerability Manager scanner appliances	20000 IPs - 150 GB

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

Table 4: Minimum and optional memory requirements for Extreme Security virtual appliances

Appliance	Minimum memory requirement	Suggested memory requirement
VFlow Collector 1299	6 GB	6 GB
Event Collector Virtual 1599	12 GB	16 GB
Extreme SIEM Event Processor Virtual 1699	12 GB	48 GB
Extreme SIEM Flow Processor Virtual 1799	12 GB	48 GB
Extreme SIEM All-in-One Virtual 3199	24 GB	48 GB
Log Manager Virtual 8090	24 GB	48 GB
Risk Manager	24 GB	48 GB
Extreme Security Vulnerability Manager Processor	8 GB	16 GB
Extreme Security Vulnerability Manager Scanner	2 GB	4 GB

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 Links

HA clusters on page 10

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

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 Links

Data consistency for HA on page 8

When an HA failover occurs, Extreme Networks Security Analytics ensures the consistency of your data.

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 *Extreme Networks SIEM Administration Guide*

Offboard storage requirements for HA

You can implement high-availability (HA) when the Extreme Networks Security Analytics `/store` partition is mounted to an external storage solution, such as an iSCSI or Fibre Channel device.

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 Extreme Networks Security Analytics *Extreme Networks Security 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*.
- Ensure that there is at least a 1 Gbps connection between each HA host and your external device.

Important
During an upgrade to Extreme Security, you must reconfigure the external storage device connections to the hosts in your HA cluster. For more information, see the *Reconfiguring offboard storage during a QRadar® upgrade technical note*.

3 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 Extreme SIEM 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 5: 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. 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.
Failed	Specifies that the primary or secondary host failed. If the primary HA host displays Failed, the secondary HA host assumes the responsibilities of the primary HA host and displays the Active status. If the secondary HA host displays Failed, the primary HA host remains active, but is not protected by HA. 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. 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. When an appliance indicates a status of offline: Data replication is functioning between the active and offline HA hosts. Services that process events, flows, offenses, and heartbeat ping tests are stopped for the offline HA host. 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 39.
Needs License	Specifies that a license key is required for the HA cluster. In this state, no processes are running. For more information about applying a license key, see your *Administration Guide*.
Setting Offline	Specifies that an administrator is changing the status of an HA host to offline.
Setting Online	Specifies that an administrator is changing the status of an HA host to online

Table 5: HA status descriptions (continued)

Status	Description
Needs Upgrade	Specifies that the secondary HA host requires a software upgrade. 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. 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. 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. Only a secondary HA host can display an Upgrading status.

Related Links

Real-time data synchronization on page 9

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 by using DRBD.

HA clusters on page 10

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

Primary disk failure on page 13

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

Verifying the status of primary and secondary hosts on page 39

Data consistency for HA on page 8

When an HA failover occurs, Extreme Networks Security Analytics ensures the consistency of your data.

Viewing HA cluster IP addresses

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

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration**.
3. Click the **System and License Management** icon.
4. Identify the Extreme Security primary console.
5. Hover your mouse over the **host name** field.

Creating an HA cluster

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

If a primary HA host has external storage configured, you must also configure the secondary HA host to use the same external storage options. For more information, see the Extreme Security *Extreme Networks Security Offboard Storage Guide*.

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.

1 Click the Admin tab.
2 On the navigation menu, click System Configuration.
3 Click the System and License Management icon.
4 Select the host for which you want to configure HA.
5 From the Actions menu, select Add HA Host and click OK.
6 Read the introductory text. Click Next.
7 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. The new primary HA host IP address must be on the same subnet as the virtual host IP address. For IPv6, if you selected Yes to auto-configure Extreme Security for IPv6 during the installation, enter the IP address that you recorded.
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.

8 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. For more information about heartbeat pings, see Heartbeat ping tests on page 13.
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.
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 Extreme Security deployment. For more information about network connectivity testing, see Network connectivity tests on page 12.
Disk Synchronization Rate (`MB/s`)	The disk synchronization rate. The default is 100 `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 Extreme Security to isolate the replication traffic from all other Extreme Security traffic, such as events, flows, and queries.
Crossover Interface	Select the interfaces that you want to connect to the primary HA host. Only interfaces with an active link appear in the list.
Crossover Advanced Options	Select **Show Crossover Advanced Options** to enter, edit, or view the property values.

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

Important
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.

Related Links

HA clusters on page 10
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

HA clusters on page 10
A high-availability (HA) cluster consists of a primary HA host, a secondary HA host, and cluster virtual IP address.

Network connectivity tests on page 12
To test network connectivity, the primary high-availability (HA) host automatically pings all existing managed hosts in your Extreme Networks Security Analytics deployment.

Heartbeat ping tests on page 13

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

Heartbeat ping tests on page 13

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

Network connectivity tests on page 12

To test network connectivity, the primary high-availability (HA) host automatically pings all existing managed hosts in your Extreme Networks Security Analytics deployment.

Recovering a secondary HA console or non-console on page 29

Recovering Extreme Networks Security Analytics on a failed primary HA console or non-console on page 34

Disconnecting an HA cluster

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 25.

1 Click the **Admin** tab.
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

Before you disconnect a Fibre Channel HA cluster, you must modify the `/store` and `/store/tmp` 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 Extreme Security host as the root user:
2 Modify the `etc/fstab` file.
   a Locate the existing mount information for the `/store` and `/store/tmp` file systems.
   b Remove the **noauto** option for the `/store` and `/store/tmp` file systems.
3 Save and close the file.

Disconnecting an HA cluster on page 25.

Editing an HA cluster

You can edit the advanced options for your HA cluster.

1 Click the Admin tab.
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.

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 Click the Admin tab.
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 Links

Manual failovers on page 13

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

Setting an HA host online

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

1 Click the Admin tab.
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* or *Restoring a failed primary HA host*.

Related Links

Post-failover data synchronization on page 9

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. The HA host uses Distributed Replicated Block Device (DRBD).

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. Click the Admin tab.
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 primary HA host.
5. From the toolbar, select High Availability > Set System Offline.

   Note
   Your Extreme SIEM user interface might be inaccessible during this time.

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

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 Links

Primary HA host failure on page 11

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

4 Recovery options for HA appliances

You can reinstall or recover Extreme Networks Security Analytics high-availability (HA) appliances.

If your HA cluster uses shared storage, manually configure your external storage device. For more information, see the Extreme Networks Security Analytics *Extreme Networks Security Offboard Storage Guide*.

Notebook hyperterminal connections

During the recovery of a Extreme Networks Security Analytics appliance, you can use a notebook to monitor the progress of the installation.

If you use HyperTerminal to monitor a Extreme Security reinstallation or recovery, choose from the connection parameters that are listed in the following table.

Hyper terminal connection parameters

Table 6: Hyper terminal connection parameters

Parameter	Description
Connect Using	Select the appropriate COM port of the serial connector.
Bits per second	Type 9600
Stop Bits	Type 1
Data bits	Type 8
Type 8	Type None

Related Links

Recovering a secondary HA console or non-console on page 29

Network connections

During the recovery or reinstallation of a Extreme Networks Security Analytics appliance, you can specify the network connection settings.

Use the information in the following table when you recover or reinstall a Extreme Security appliance:

Extreme Security network setting parameters

Table 7: Extreme Security network setting parameters

Parameter	Description
Hostname	Type a fully qualified domain name as the system host name.
IP Address	Type the IP address of the system. Note If you are recovering an HA appliance, the IP address is the primary HA host IP address. You can identify the IP address in the **System and License Management** window.
Network Mask	Type the network mask address for the system.
Gateway	Optional Type the **Public IP address** of the server. The **Public IP address** is a secondary IP address that is used to access the server. Access is usually from a different network or the Internet, and is managed by your network administrator. The **Public IP address** is often configured by using Network Address Translation (NAT) services or firewall settings on your network.
Email Server	Type the email server. If you do not have an email server, type `localhost` in this field.

Recovering a secondary HA console or non-console

You can install or recover a secondary high-availability (HA) Extreme Networks Security Analytics or non-console (managed host) appliance.

To recover a primary or secondary console or non-console HA console or reinstall Extreme Security software, you must have a valid activation key.

The activation key is a 24-digit, 4-part, alphanumeric value. You can find the activation key:

- Printed on a sticker and physically placed on your console.
- Included with the packing slip. All consoles are listed along with their associated keys.

> Note
> The letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

The build version of the primary HA host must be the same as the Extreme Security build version installed on the secondary HA host.

The secondary or primary HA host must be patched to the correct build version before you configure an HA cluster.

1 Prepare your appliance.

   a Install all necessary hardware.

   b Connect a notebook to the serial port on the rear of the appliance, or connect a keyboard and monitor to their respective ports.

   For more information on your Extreme Security appliance or appliance ports, see the *Extreme Networks Security Hardware Guide*.

   c Turn on the system and log in as **Username:** `root`

   > Note
   > The user name is case-sensitive.

   d Press Enter.

   e Press the Spacebar to advance each window then type yes to accept the agreement and press **Enter**.

   f Type your activation key and press Enter.

2 Follow the instructions in the wizard.

3 Configure the Extreme Security network settings.

4 Select **Next** and press Enter.

> Note
> If you are changing network settings with `qchange_netsetup`, select **Finish** and press Enter. For more information about changing network settings, see the *Extreme Networks Security Installation Guide* or the *Log Manager Installation Guide*.

5 Configure the Extreme Security root password:

   a Type your password, then select **Next** and press Enter.

   b Retype your new password. Select **Finish** and press Enter.

   > Note
   > This process can take several minutes.

   c Press Enter to select OK.

6 Log in to the Extreme Security user interface.

Configure the HA Cluster.

Related Links

Notebook hyperterminal connections on page 28

During the recovery of a Extreme Networks Security Analytics appliance, you can use a notebook to monitor the progress of the installation.

Creating an HA cluster on page 22

Recovering a failed primary HA host

You can recover a failed primary high-availability (HA) Extreme Networks Security Analytics host.

If you need to reinstall Extreme Security on a failed primary high-availability (HA) host, you must consider the build version of the secondary HA host.

To recover a primary or secondary console or non-console HA console or reinstall Extreme Security software, you must have a valid activation key.

The activation key is a 24-digit, 4-part, alphanumeric value. You can find the activation key:

- Printed on a sticker and physically placed on your console.
- Included with the packing slip. All consoles are listed along with their associated keys.

Note
The letter I and the number 1 (one) are treated the same, as are the letter O and the number 0 (zero).

The build version of the primary HA host must be the same as the Extreme Security build version installed on the secondary HA host.

The secondary or primary HA host must be patched to the correct build version before you configure an HA cluster.

1 Install all necessary hardware.
2 Choose one of the following options:
   - Connect a notebook to the serial port on the rear of the appliance. For more information, see Notebook hyperterminal connections on page 28.
   - Connect a keyboard and monitor to their respective ports.
3 Turn on the system and login: **Username**: `root`
4 Press Enter.
5 Press the Spacebar to advance each window then type `yes` to accept the agreement and press Enter.
6 Type your activation key and press Enter.
7 Select **HA Recovery Setup** Select **Next** and press Enter.
8 Follow the instructions in the wizard.
9 Configure the Extreme Security network settings.
10 Select **Next** and press Enter.
11 Configure the Extreme Security root password.
12 Log in to the Extreme Security user interface.
13 Restore the failed primary HA host. For more information, see Verifying the status of primary and secondary hosts on page 39.

Recovering a failed secondary HA host to Extreme SIEM 7.1

You can recover a failed secondary high-availability (HA) host to Extreme SIEM v7.1.

When you recover a failed secondary HA host that used a previous Extreme Security version, you can install Extreme Security 7.1 from an updated recovery partition.

The installer repartitions and reformats the hard disk, installs the Operating System, then reinstalls Extreme Security. Wait for the flatten process to complete. This process can take several minutes.

For more information on installing your secondary HA host, see the *Extreme Networks Security Installation Guide* or the *Extreme Networks Security Log Manager Administration Guide*.

1 Using SSH, log in to the secondary HA host as the root user:

   a Username:`root`

   b Password:`<password>`

2 Obtain the Extreme Security software from the following location: https://www.ibm.com/support

3 Copy the Extreme Security 7.1 ISO to the secondary HA host by typing the following command: `scp <iso file name> root@<ip_address>:/root`

> Important
> If you are installing Extreme Security 7.0 and above, Step 4 through Step 5 are not necessary. The recovery script is placed in `/opt/qradar/bin` during the installation.

4 Mount the ISO by typing the following command: `mount -o loop <iso_file_name> /media/cdrom/`

5 Copy the recovery script into the root directory by typing the following command: `cp /media/cdrom/post/recovery.py /root`

6 Unmount the ISO by typing the following command: `umount /media/cdrom/`

7 If the host is a non-console, to stop the IPTables service to allow secure copy (SCP), type the following command:

```
service iptables stop
```

8 Start the extracted recovery script by typing the following command: `./recovery.py -r --default --reboot <iso_file_name>`

9 When prompted, press Enter to restart the appliance.

10 When prompted, type `flatten` and press Enter.

11 When the installation completes, type SETUP and log in to the system as the root user.

Recovering a failed secondary HA host to Extreme SIEM 7.1 (MR2)

When you recover a failed secondary high-availability (HA) host that used a previous Extreme SIEM version, you can install Extreme Security 7.1 from an updated recovery partition.

1 Using SSH, log in to the secondary HA host as the root user:

   a Username:`root`

   b Password:`<password>`

2 Obtain the Extreme Security software from the following location: https://www.ibm.com/support

3 Copy the Extreme Security 7.1 ISO to the secondary HA host by typing the following command: `scp <iso file name> root@<ip_address>:/root`

4 If the host is a non-console, to stop the IPTables service to allow secure copy (SCP), type the following command.

```
service iptables stop
```

5 Start the extracted recovery script by typing the following command: `./recovery.py -r --default --reboot <iso_file_name>`

6. When prompted, press Enter to restart the appliance.
7. When prompted, type `flatten` and press Enter.

The installer repartitions and reformats the hard disk, installs the Operating System, and then reinstalls Extreme SIEM. Wait for the flatten process to complete. This process can take up to several minutes, depending on your system. When this process is complete, the normal installation process proceeds.

Recovering a failed primary high-availability (HA) QFlow appliance

You can recover a failed primary high-availability (HA) Extreme Networks Security QFlow Collector.

1. Install all necessary hardware.
2. Choose one of the following options:
   - Connect a notebook to the serial port on the rear of the appliance. For more information, see Notebook hyperterminal connections on page 28.
   - Connect a keyboard and monitor to their respective ports.
3. Turn on the system and login: Username: `root`
4. Press Enter.
5. Press the Spacebar to advance each window then type `yes` to accept the agreement and press Enter.
6. Type your activation key and press Enter.
7. Select HA Recovery Setup. Select Next and press Enter.
8. Select your time zone continent or area. Select Next and press Enter.
9. Select your time zone region. Select Next and press Enter.
10. Select IPv4. Select Next and press Enter.

    Note
    Each interface with a physical link is denoted with a plus (+) symbol.

11. Select the management interface. Select Next and press Enter.
12. Type the Cluster Virtual IP address, then select Next and press Enter. For more information, see Viewing HA cluster IP addresses on page 22.
13. Configure the Extreme Security network settings. .
14. Select Next and press Enter.
15. Configure the Extreme Security root password.
16. Log in to the Extreme Security user interface.
17. Restore the failed primary HA host. For more information about restoring a failed primary HA host, see Verifying the status of primary and secondary hosts on page 39.

Recovering Extreme Security on a secondary high-availability HA console or non-console system

You can install or recover Extreme Security Console or non-console (managed host) software on your secondary high-availability (HA) system.

These instructions are applicable to the installation or recovery of a Extreme Security Console and non-console. You must choose different options according to the appliance you are installing or recovering.

Ensure that you have a Extreme Security activation key. For more information, see Extreme Security activation keys.

1 Install the necessary hardware.
2 Obtain the Red Hat Enterprise Linux™ operating system and install it on your hardware.

> Note
> For instructions on how to install and configure the Red Hat Enterprise Linux™ operating system, see the *Extreme Networks Security Installation Guide*.

3 Log in as root.
4 Create the `/media/cdrom` directory by typing the following command: `mkdir /media/cdrom`
5 Obtain the Extreme Security software from the following location: https://www.ibm.com/support
6 Mount the Extreme Security ISO by typing the following command:`mount -o loop <path to the QRadar ISO> /media/cdrom`
7 Begin the installation by typing the following command: `/media/cdrom/setup`
8 Press the Spacebar to advance each window then type yes to accept the agreement and press Enter.
9 Type your activation key and press Enter.
10 Follow the instructions in the wizard.
11 Configure the Extreme Security network settings.
12 Select Next and press Enter.

> Note
> If you are changing network settings by using `qchange_netsetup`, select Finish and press Enter. For more information, see the *Extreme Networks Security Installation Guide*.

13 Configure the Extreme Security root password.
14 Log in to the Extreme Security user interface.

Configure the HA cluster.

Recovering Extreme Networks Security Analytics on a failed primary HA console or non-console

You can recover Extreme Networks Security Analytics console or non-console (managed host) software on your failed primary HA host.

These instructions are applicable to the installation or recovery of Extreme Security on a primary console and non-console. You must choose different options according to the appliance you are installing or recovering.

Ensure that you have a Extreme Security activation key. For more information, see Extreme Security activation keys.

1 Install the necessary hardware.

2 Obtain the Red Hat Enterprise Linux™ operating system and install it on your hardware.

> Note
> For instructions on how to install and configure the Red Hat Enterprise Linux™ operating system, see the *Extreme Networks Security Installation Guide*.

3 Log in as root.
4 Create the `/media/cdrom` directory by typing the following command: `mkdir /media/cdrom`
5 Obtain the Extreme Security software from the following location: https://www.ibm.com/support
6 Mount the Extreme Security ISO by typing the following command: `mount -o loop <path to the QRadar ISO> /media/cdrom`
7 Begin the installation by typing the following command: `/media/cdrom/setup`

> Note
> Extreme Security verifies the integrity of the media before installation by checking the MD5 sum. If a warning message is displayed, that the MD5 checksum failed, redownload Extreme Security. For further assistance, contact Customer Support.

8 Press the Spacebar to advance each window then type `yes` to accept the agreement and press Enter.
9 Type your activation key and press Enter.
10 Follow the instructions in the wizard.
11 Configure the Extreme Security network settings.
12 Select Next and press Enter.
13 Configure the Extreme Security root password.
14 Log in to Extreme Security.

Restore the failed primary HA host. See Verifying the status of primary and secondary hosts on page 39.

Related Links

Creating an HA cluster on page 22

Recovering a secondary HA host to a previous version or factory default

You can recover an Extreme Networks Security Analytics secondary high-availability (HA) host to a previous version or factory default.

You can recover a failed Extreme Security 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 recover the failed secondary HA host, all data is removed and the factory default configuration is restored on the host.

1 Using SSH, log in to the Console as the root user.

2. Using SmartCloud Provisioning, copy the `recovery.py` script from the Console to the failed secondary HA host.

   Note

   By default, the `recovery.py` script is downloaded to the `/root` directory if you do not specify a location.

3. Obtain the Extreme Security ISO from the following location: https://www.ibm.com./support
4. Use secure copy (SCP) to copy the ISO file to the target Extreme Security host.

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

5. Using SSH, 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 Extreme Security. 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.

5 Troubleshooting Extreme Security HA deployments

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.

System and license management window host statuses

Table 8: 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 38.
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 38.
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.
Offline	Active	To set the primary host online, see Set the primary HA host online.

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:

```
cat /proc/drbd
```

2 Review the following line: in the output:

```
0: cs:Connected ro:Primary/Secondary ds:UpToDate/UpToDate
```

- If the line does not display the following text, `cs:Connected`, determine the most recent active HA host in the HA cluster.
- If the output displays the following text, `Secondary/Primary`, the secondary HA Host is the active system.
- If the output displays the following text, `ro:Primary/Secondary`, the primary HA Host is the active system.

3 If the line displays `ro:Secondary/Secondary`, review the following line in the output:

```
0: cs:Connected ro:Secondary/Secondary
```

- If the output displays the following text, `ds:< >/UpToDate`, the secondary HA Host is the active system.
- If the output displays the following text, `ds:UpToDate/< >`, the primary HA Host is the active system.
- If the output displays the following text, `ds:< >/< >`, determine the most recent active HA host in your HA cluster.
- If the output displays the following text, `ds:UpToDate/UpToDate`, determine the most recent active HA host in your HA cluster.

Restoring a failed secondary HA host

You can restore a failed secondary HA host.

1 Click the Admin tab.
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 Links

Verifying the status of primary and secondary hosts on page 39

Restoring a failed primary HA host

You can restore a failed primary HA host.

1 Click the Admin tab.
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 Links

Setting the status of the primary HA host to online on page 39

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 Extreme Security. For more information, see the *Extreme Networks Security Troubleshooting System Notifications 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 Links

Status of HA hosts on page 20

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

Verifying the status of primary and secondary hosts on page 39

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 Click the Admin tab.

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 Links

Restoring a failed primary HA host on page 38