



Extreme Networks Security Offboard Storage Guide

Copyright © 2012–2015 All rights reserved.

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 offboard storage devices for Extreme Security products.....	4
Conventions.....	4
Providing Feedback to Us.....	5
Getting Help.....	6
Related Publications.....	6
Chapter 1: Offboard storage overview.....	8
File system options for offboard storage.....	9
External storage options.....	10
Chapter 2: iSCSI external storage device.....	12
iSCSI configuration options in an HA environment.....	12
Secondary network interfaces.....	13
iSCSI configuration in standard Extreme Security deployments.....	13
Configuring the iSCSI volumes.....	14
Mounting the iSCSI volume automatically.....	18
Configuring iSCSI in an HA deployment.....	18
Configuring control of secondary interfaces in HA deployments.....	20
Verifying iSCSI connections.....	21
Chapter 3: Fibre Channel storage.....	24
Configuration overview for Fibre Channel storage.....	24
Chapter 4: NFS offboard storage device.....	33
Moving backups to an NFS.....	33
Configuring a new backup location.....	35
Configuring a mount point for a secondary HA host.....	35
Index.....	36

Introduction to offboard storage devices for Extreme Security products

This guide provides information about how to move the `/store` or `/store/ariel` file systems to an external storage device for Extreme Networks Security Analytics products.

Intended audience

System administrators responsible for configuring offboard storage devices must have administrative access to Extreme Security systems and to network devices and firewalls. The system administrator must know the corporate network 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	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]
<i>Words in italicized type</i>	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 Offboard storage overview

File system options for offboard storage External storage options

To increase the amount of storage space on your appliance, you can move your data to an offboard storage device. You can move your `/store`, `/store/ariel`, or `/store/backup` file systems to an iSCSI, Fibre Channel, or Network File System (NFS) external storage solution.

You can implement an offboard storage solution by using a standard Extreme Networks Security Analytics primary console or in a high-availability (HA) environment. When you use iSCSI or Fibre Channel with HA, the external storage device ensures data consistency if your primary HA host fails.

To move a Extreme Security file system to an external storage device, you must configure your iSCSI, Fibre Channel, or NFS external storage devices. If you implement external storage with HA, you must configure these devices on the primary HA host and the secondary HA host.

Before you implement an offboard storage solution, consider your local storage options, existing hardware infrastructure, and your data retention and fault tolerance requirements.

Local storage

The disk on your Extreme Security appliance is faster than external storage and supports up to 16 TB of data. When possible, use local storage as an alternative to an external storage device.

Multiple appliances

Use multiple appliances if larger storage capacity is required for your Extreme Security deployment.

When multiple appliances are not feasible, or an existing deployment can increase capacity by using available external storage, then external storage might be appropriate for your deployment.

Hardware and infrastructure

Your existing infrastructure and experience with storage area networks are important factors in deciding whether to use an offboard storage solution.

Certain offboard devices require less configuration and might be able to use existing network infrastructures. For example, iSCSI uses existing Ethernet networking, while Fibre Channel uses more specialized hardware.

Data retention and fault tolerance

Your Extreme Security data retention policy is important in considering an offboard storage solution. If your data retention settings exceed the capacity of existing storage or your are planning to expand the retention of existing deployed appliances, you might require an offboard storage solution.

An offboard storage solution can be used to improve your fault tolerance and disaster recovery capabilities.

File system options for offboard storage

Use an offboard storage solution to move the `/store` file system or specific subdirectories, such as the `/store/ariel` directory.

You can move the `/store` file system when you want to increase the fault tolerance levels in your Extreme Networks Security Analytics deployment. Each option impacts Extreme Security performance.

Moving the `/store` file system to an external device can provide an alternative to implementing a high-availability system.

The `/store/ariel` directory is most common file system that is moved to an offboard storage solution. By moving the `/store/ariel` file system, you can move collected log and network activity data to external storage. The local disk remains used for the PostgreSQL database and temporary search results.

Administrators can move the following types of Extreme Security data to offboard storage devices:

- PostgreSQL metadata and configuration information
- Log activity, payloads (raw data), normalized data, and indexes
- Network activity, payloads, normalized data, and indexes
- Time series graphs (global views and aggregates)

Performance impact of offboard storage solutions

Moving the `/store` file system to an external device might affect Extreme Security performance.

After migration, all data I/O to the `/store` file system is no longer done on the local disk. Before you move your Extreme Security data to an external storage device you must consider the following information:

- Maintain your log and network activity searches on your local disk by mounting the `/store/transient` file system to the unused `/store` file partition.
- Searches that are marked as saved are also in the `/store/transient` directory. If you experience a local disk failure, these searches are not saved.

Storage expansion

By creating multiple volumes and mounting `/store/ariel/events` and `/store/ariel/flows`, you can expand your storage capabilities past the 16 TB file system limit that is supported by Extreme Security.

Any subdirectory in the `/store` file system can be used as a mount point for your external storage device.

If you want to move dedicated event or flow data, you might configure more specific mount points. For example, you can configure `/store/ariel/events/records` and `/store/ariel/events/`

payloads as mount points. Specific mount points can provide up to 32 TB of storage for the **Log Activity** or **Network Activity** data.

External storage options

You can use iSCSI, Fibre Channel, or NFS to provide an offboard storage solution.

Onboard disks provide a faster solution than offboard storage devices. Local disk storage on appliances supports Extreme Networks Security Analytics read speeds of 200 - 400 MBps and write speeds of almost 200 MBps. When multiple appliances are deployed, performance and capacity scale at the same rate.

Fibre Channel	<p>Fibre Channel provides the fastest offboard performance by using storage area network (SAN) speeds of 200 MBps to 3200 MBps, depending on your network configuration.</p> <p>Fibre Channel performance might be impacted by factors within the SAN implementation, such as the following factors:</p> <ul style="list-style-type: none"> • Disk or spindle counts per volume • Number of concurrent sessions. • Cache capacity in the SAN controllers.
iSCSI	<p>iSCSI uses a dedicated storage channel over standard Ethernet infrastructure, rather than a dedicated SAN network. For this reason, iSCSI can be the easiest to implement, most cost effective, and most readily available.</p> <p>If you implement an iSCSI solution, then network capacity is shared between external storage access and management interface I/O. In this situation, you can configure a secondary network interface on a separate storage network.</p> <p>Using a dedicated interface, you are limited to 1 Gbps and might experience only 200 MBps to 400 MBps. Your iSCSI storage device might provide only 25 MBps to 50 MBps I/O performance.</p>
NFS	<p>A Network File System (NFS) solution must not be used to store active Extreme Security data. You can move the <code>/store/backup</code> file system to an external NFS.</p> <p>If the <code>/store</code> file system is mounted to an NFS solution, PostgreSQL data can be corrupted. If the <code>/store/ariel</code> file system is mounted to NFS, Extreme Security experiences performance issues.</p> <p>Use NFS for tasks during off-peak times, tasks that involve batch file writes, and tasks that involve a limited volume of file I/O. For example, use NFS for daily configuration and data backups.</p> <p>NFS storage operates over existing management Ethernet networks and is limited to performance levels of 20 MBps to 50 MBps. The NFS protocol might affect performance for file access, locking, and network permissions. Remediate the performance impact by using a dedicated network interface.</p> <p>If NFS is used only for backups, the same NFS share can be used for each host. The backup files contain the system host name, which enables the identification of each backup file. If you are storing a long period of data on your NFS shares, consider a separate share or export for each appliance in your deployment.</p>

External storage limitations

Multiple systems cannot access the same block device in an Extreme Networks Security Analytics deployment.

If you configure iSCSI in an HA environment, do not mount the iSCSI or Fibre Channel volumes on the secondary host while the primary host is accessing the volumes.

An external storage device must be able to provide consistent read and write capacity of 100 MBps to 200 MBps. When consistent read and write capacity is not available, the following issues might occur:

- Data write performance is impacted.
- Search performance is impacted.

If performance continues to degrade, then the processing pipeline can become blocked and Extreme Security might display warning messages and drop events and flows.

Offboard storage in HA environments

If you choose to move the `/store` file system in a high-availability (HA) environment, the `/store` file system is not replicated by using Disk Replication Block Device (DRBD).

If you move the `/store/ariel` file system to an offboard storage device and maintain the `/store` file system on local disk, the `/store` file system is synchronized with the secondary HA host by using DRBD. By default, when your environment is configured for HA, DRBD is enabled.

2 iSCSI external storage device

iSCSI configuration options in an HA environment
Secondary network interfaces
iSCSI configuration in standard Extreme Security deployments
Configuring the iSCSI volumes
Mounting the iSCSI volume automatically
Configuring iSCSI in an HA deployment
Configuring control of secondary interfaces in HA deployments
Verifying iSCSI connections

Administrators can configure an iSCSI storage device in a standard or high-availability (HA) Extreme Networks Security Analytics deployment.

When you configure an iSCSI external storage device, you must migrate the Extreme Security data that is maintained on your `/store` or `/store/ariel` file system and then mount the `/store` or `/store/ariel` file system to a partition on the iSCSI device volume.

Depending on your device configuration, you might be required to create a partition on the volume of your Fibre Channel disk.

If you configure iSCSI in an HA deployment and your primary HA host fails, your iSCSI device can be used to maintain data consistency with your secondary HA host.

iSCSI configuration options in an HA environment

iSCSI configurations are different for a primary HA host and secondary HA host. To configure iSCSI you must ensure that the primary HA host and secondary HA host are not connected in an HA cluster.

In HA environments, review the `/var/log/messages` file for errors in your iSCSI storage configuration.

Ensure that you use a different *initiatorname* on the primary HA host and secondary HA host. Your iSCSI device must be configured to enable each *initiatorname* to access the same volume on the iSCSI device.

You configure the *initiatorname* in the `/etc/iscsi/initiatorname.iscsi` file and is used by Extreme Security to identify the volume on the iSCSI device where the `/store` or `/store/ariel` file system is mounted.

Related Links

[Configuring iSCSI in an HA deployment](#) on page 18

To use an iSCSI device in an HA environment, you must configure the primary high-availability (HA) host and secondary HA host to use the same iSCSI external storage device.

Secondary network interfaces

You can configure a secondary network interface with a private IP address to connect to an iSCSI storage area network (SAN).

You use secondary network interface to improve performance. If you configure a secondary network interface, you require address information from your SAN network manager. For more information about configuring a network interface, see your *Administration Guide*.

HA systems in iSCSI deployments

For dedicated access to the iSCSI storage network, use the following order to set up high availability (HA), iSCSI, and a network interface:

- 1 Configure the primary and secondary appliances.
- 2 Set up external iSCSI storage on both hosts
- 3 Configure HA on the primary and secondary hosts.

The HA process for Extreme Networks Security Analytics controls the all network interfaces. When an HA appliance is in active mode, the HA process enables the interfaces. When HA is in standby mode, the HA process disables the interfaces. If the dedicated network interface for storage is disabled and the HA system goes into failover, the standby host tries to go into active mode. If the HA system is in standby mode, you cannot access the iSCSI storage system. Access issues are caused during the transition of the HA node from standby to active. The HA process brings the secondary interface online, but when the iSCSI system is mounted, the networking is not available and the failover process fails. The standby HA host cannot change to active mode.

To resolve the issue, you must remove control of the iSCSI network interface from the HA system to ensure that network interface is always active. Remove any dependencies that the network interface has on the status of the HA node. The HA primary and secondary hosts must have unique IP addresses on these secondary network interfaces.

Related Links

[Configuring control of secondary interfaces in HA deployments](#) on page 20

If you use iSCSI and a dedicated network interface in a high-availability (HA) deployment, you must ensure that the secondary interface is not managed by the HA process. Configure the management of the secondary interface to ensure that in the event of a failover to the secondary HA host, the interface always remains active.

iSCSI configuration in standard Extreme Security deployments

Use Extreme Security Console to configure iSCSI in a standard deployment.

Administrators must perform the following tasks in sequence:

- 1 [Configure iSCSI volumes](#)
- 2 Migrate the file system to an iSCSI storage solution.

- Move the `/store/ariel` file system to an iSCSI storage solution.
 - Move the `/store` file system to an iSCSI storage solution.
 - Mount the iSCSI volume automatically
- 3 Verify iSCSI connections.

Configuring the iSCSI volumes

You can configure iSCSI for a stand-alone Extreme Security Console or a Extreme Security Console that is the primary high-availability (HA) host in an HA deployment.

Optionally, you can create a partition on the volume of the external iSCSI storage device.

Extreme Networks Security Analytics V7.2.1 and later uses the XFS file system. You can create the partition on your iSCSI device with either an ext4 or XFS file system.

Disk partitions are created by using GUID Partition Table (GPT). You can use a new device partition as the mount point for the file system, such as `/store` or `/store/ariel` that you migrate.

Important



If you created an iSCSI or Fibre Channel device partition on your external device and Extreme Security data is stored, then you cannot create a partition or reformat the partition on the volume.

- 1 Using SSH, log in to the Extreme Security Console as the root user.
- 2 Edit the `/etc/iscsi/initiatorname.iscsi` file to include the iSCSI qualified name for your host.

```
InitiatorName=iqn.yyyy-mm.{reversed domain name}:hostname
```

Example

```
InitiatorName=iqn.2014-11.com.qradar:pl13
```

- 3 Open a session to the iSCSI server by typing the following command: `service iscsi restart`.
- 4 To detect volumes on the iSCSI server, type the following command:

```
iscsiadm -m discovery --type sendtargets --portal IP address:[port]
```

The `IP address` option is the IP address of the iSCSI server. The `port` is optional. Record the initiator name.

- 5 To log in to the iSCSI server, type the following command:

```
iscsiadm -m node --targetname <Initiator name from step 4> --portal <IP address:[port]> --login
```

- 6 To find the iSCSI device volume name, type the following command:

```
dmesg | grep "Attached SCSI disk"
```

- 7 To create a partition, use the GNU parted command:

```
parted /dev/volume
```

- 8 Configure the partition label to use GPT by typing the following command:

```
mklabel gpt
```

- 9 If the following message is displayed, type **Yes**.

```
Warning: The existing disk label on /dev/volume will be destroyed and all data
on this disk will be lost. Do you want to continue?
```

- 10 Create a partition on the iSCSI disk volume.

- a To create the partition, type the following command:

```
mkpart primary 0% 100%
```

- b Set the default units to TB by typing the following command:

```
unit TB
```

- c Verify that the partition is created by typing the following command:

```
print
```

- d Exit from GNU parted by typing the following command:

```
quit
```

- e Update the kernel with the new partition data by typing the following command:

```
partprobe /dev/volume
```

You might be prompted to restart the appliance.

- f To verify that the partition is created, type the following command:

```
cat /proc/partitions
```

- 11 Reformat the partition and make a file system.

- To create an XFS file system, type the following command: `mkfs.xfs -f /dev/partition`
- For an ext4 files system, type the following command: `mkfs.ext4 /dev/partition`

See [Moving the /store/ariel file system to an iSCSI storage solution](#) on page 15 or [Moving the /store file system to an iSCSI storage solution](#) on page 16.

Related Links

[Troubleshooting iSCSI issues](#) on page 22

Moving the /store/ariel file system to an iSCSI storage solution

You can migrate the Extreme Networks Security Analytics data that is maintained in the `/store/ariel` file system and mount the `/store/ariel` file system to an iSCSI device partition.

Configure iSCSI volumes.

- 1 Stop the hostcontext service by typing the following command:

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```

- 2 Move the existing mount point by typing the following commands:

```
cd /store
mv ariel ariel_old
```

- 3 Verify the Universally Unique Identifier (UUID) of the iSCSI device partition by typing the following command:


```
blkid /dev/partition
```
- 4 Add the mount point for the `/store/ariel` file system by adding the following text to the `/etc/fstab` file:
 - If the file system is ext4, add the following text


```
UUID=uuid /store/ariel ext4 noatime,noauto,nobarrier 0 0
```
 - If the file system is XFS, copy the following text into a text editor, remove the line break, and paste as a single line:


```
UUID=uuid /store/ariel xfs inode64,logbsize=256k,noatime,  
noauto,nobarrier 0 0
```
- 5 Create the ariel directory for the mount point by typing the following command:


```
mkdir ariel
```
- 6 Mount `/store/ariel` to the iSCSI device partition by typing the following command:


```
mount /store/ariel
```
- 7 Verify that `/store/ariel` is correctly mounted by typing the following command:


```
df -h
```
- 8 Move the data from the local disk to the iSCSI storage device by typing the following command:


```
mv /store/ariel_old/* /store/ariel
```
- 9 Remove the `/store/ariel_old` directory by typing the following command:


```
rmdir /store/ariel_old
```
- 10 Start the hostcontext service by typing the following command:


```
service crond start  
service systemStabMon start  
service hostservices start  
service tomcat start  
service hostcontext start
```

See [Mounting the iSCSI volume automatically](#) on page 18.

Related Links

[Moving the /store file system to an iSCSI storage solution](#) on page 16

Moving the /store file system to an iSCSI storage solution

You can migrate the Extreme Networks Security Analytics data that is maintained in the `/store` file system and mount the `/store` file system to an iSCSI device partition.

Migrating the `/store` files system to your offboard storage device can take an extended period of time.

[Configure iSCSI volumes..](#)

- 1 Stop the hostcontext service by typing the following command:

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```

- 2 Unmount the file systems by typing the following commands:

```
umount /store/tmp
umount /store/transient
umount /store
```

- 3 Create the `/store_old` directory by typing the following command:

```
mkdir /store_old
```

- 4 Derive the iSCSI device partition universal unique identifier (UUID) by typing the following command:

```
blkid /dev/partition
```

- 5 Edit the `/etc/fstab` file to update the existing `/store` file system mount point to `/store_old`.

- 6 Add a new mount point for the `/store` file system by adding the following text to the `/etc/fstab` file:

- If the file system is ext4, add the following text:

```
UUID=uuid /store ext4 noatime,noauto,nobarrier 0 0
```

- If the file system is XFS, add the following text:

```
UUID=uuid /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- a Modify the `/store/tmp` mount line to use the following file system options:

```
noatime,noauto,nobarrier 0 0
```

- b If `/store/transient` is listed in the `fstab` file, then type the following file system options:

```
xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- c Save and close the file.

- 7 Mount the `/store` file system to the iSCSI device partition by typing the following command:

```
mount /store
```

- 8 Mount the `/store_old` file system to the local disk by typing the following command:

```
mount /store_old
```

- 9 Move the data from the local disk to the iSCSI storage device by typing the following command:

```
mv -f /store_old/* /store
```

- 10 Re-mount the file systems by typing the following commands:

```
mount /store/tmp
mount /store/transient
```

- 11 Unmount `/store_old` by typing the following command:

```
umount /store_old
```

- 12 Remove the `/store_old` directory from the `/etc/fstab` file by typing the following command:

```
rmdir /store_old
```

13 Start the hostcontext service by typing the following command:

```
service crond start
service systemStabMon start
service hostservices start
service tomcat start
service hostcontext start
```

See [Mounting the iSCSI volume automatically](#) on page 18.

Related Links

[Moving the /store/ariel file system to an iSCSI storage solution](#) on page 15

You can migrate the Extreme Networks Security Analytics data that is maintained in the `/store/ariel` file system and mount the `/store/ariel` file system to an iSCSI device partition.

Mounting the iSCSI volume automatically

You must configure Extreme Networks Security Analytics to automatically mount the iSCSI volume.

Ensure that you moved the `/store/ariel` and `/store` file systems to an iSCSI storage solution.

1 Add the iSCSI script to the startup information by typing the following commands:

```
chkconfig --add iscsi
chkconfig --level 345 iscsi on
```

2 Create a symbolic link to the script that mounts the iSCSI storage solution by typing the following command:

```
ln -s /opt/qradar/init/iscsi-mount /etc/init.d
```

3 Add the mount script to the startup information by typing the following commands:

```
chkconfig --add iscsi
chkconfig --level 345 iscsi on
```

4 Verify that the iSCSI device is correctly mounted by restarting your system.

- a Restart the system by typing the following command: `reboot`
- b Ensure that the iSCSI mount point is retained by typing the following command: `df -h`

If you are configuring a high-availability (HA) environment, you must set up your secondary HA host by using the same iSCSI connections that you used for your primary HA host. For more information, see [Configuring iSCSI in an HA deployment](#) on page 18.

Related Links

[Configuring iSCSI in an HA deployment](#) on page 18

To use an iSCSI device in an HA environment, you must configure the primary high-availability (HA) host and secondary HA host to use the same iSCSI external storage device.

Configuring iSCSI in an HA deployment

To use an iSCSI device in an HA environment, you must configure the primary high-availability (HA) host and secondary HA host to use the same iSCSI external storage device.

- 1 Using SSH, log in to the secondary HA host as the root user.
- 2 To configure your HA secondary host to identify the iSCSI device volume, add the iSCSI qualified name for your host to the `/etc/iscsi/initiatorname.iscsi` file.

```
Initiatorname=iqn.yyyy-mm.{reversed domain name}:hostname
```

Example

```
InitiatorName=iqn.2008-11.com.qradar:pl13
```

- 3 Restart the iSCSI service to open a session to the server by typing the following command:

```
service iscsi restart
```

- 4 To detect the volume on the iSCSI server, type the following command:

```
iscsiadm -m discovery --type sendtargets --portal IP address:[port]
```



Note

The `port` is optional.

- 5 Verify the login to your iSCSI server by typing the following command:

```
iscsiadm -m node -l
```

- 6 To find the iSCSI device volume name, type the following command:

```
dmesg | grep "Attached SCSI disk"
```

- 7 To create a partition, use the GNU parted command:

```
parted /dev/volume
```

- 8 Configure the mount point for the secondary HA host.

- a To unmount the file systems, type the following commands:

```
umount /store/tmp
umount /store/transient
umount /store
```

- b Identify the UUID of the iSCSI device partition by typing the following command:

```
blkid /dev/partition
```

- c If you are moving the `/store` file system, edit the file settings in the `/etc/fstab` file to be the same as the mount points that are listed in the `/etc/fstab` file on the HA primary host:

- `/store`
- `/store/temp`
- `/store/transient`

- d If you are moving the `/store/ariel` file system, edit the settings in the `/etc/fstab` file to be the same as the mount point that is listed in the `/etc/fstab` file on the HA primary host for `/store/ariel`.

- 9 Configure the secondary HA host to automatically mount the iSCSI volume.

- a Add the iSCSI script to the startup information by typing the following commands:

```
chkconfig --add iscsi
chkconfig --level 345 iscsi on
```

- b Create a symbolic link to the mount script by typing the following command:

```
ln -s /opt/qradar/init/iscsi-mount /etc/init.d
```

- c Add the mount script to the startup information by typing the following commands:

```
chkconfig --add iscsi-mount
chkconfig --level 345 iscsi-mount on
```

See [Verifying iSCSI connections](#) on page 21.

Related Links

[iSCSI configuration options in an HA environment](#) on page 12

iSCSI configurations are different for a primary HA host and secondary HA host. To configure iSCSI you must ensure that the primary HA host and secondary HA host are not connected in an HA cluster.

Configuring control of secondary interfaces in HA deployments

If you use iSCSI and a dedicated network interface in a high-availability (HA) deployment, you must ensure that the secondary interface is not managed by the HA process. Configure the management of the secondary interface to ensure that in the event of a failover to the secondary HA host, the interface always remains active.

Ensure that the following conditions are met:

- Separate IP addresses for the dedicated iSCSI network interface on each of the HA servers

Separate IP addresses prevent IP address conflicts when the network interfaces are active on both HA hosts at the same time. The iSCSI software and drivers can access the external storage at startup and during the HA failover. Also, the external volume can be successfully mounted when the HA node switches from standby to active.

- The primary and secondary appliances are configured.

For more information, see the *Extreme Networks SIEM High Availability Guide*

- iSCSI storage is configured.
 - 1 On the primary host, use SSH to log in to the Extreme Security Console as the root user.
 - 2 Disable the Extreme Security HA service control of network interface.
 - a Go to the `/opt/qradar/ha/interfaces/` directory

The directory contains a list of files that are named `ifcfg-ethN`. One file exists for each interface that is controlled by Extreme Security HA processes.
 - b Delete the file that is used to access your iSCSI storage network.

Deleting the file removes control of the interface from the HA processes.
 - 3 Re-enable operating system-level control of the network interfaces.
 - a Go to the `/etc/sysconfig/network-scripts/ifcfg-ethN` directory.
 - b Open the `ifcfg-ethN` file for the interface that connects to your iSCSI network.
 - c To ensure that the network interface is always active, change the value for the `ONBOOT` parameter to `ONBOOT=yes`.
 - 4 To restart the iSCSI services, type the following command:


```
/etc/init.d/iscsid restart
```
 - 5 Repeat these steps for the HA secondary appliance.

- 6 To test access to your iSCSI storage from your secondary appliance, use the ping command:

```
ping iscsi_server_ip_address
```

Related Links

[Secondary network interfaces](#) on page 13

You can configure a secondary network interface with a private IP address to connect to an iSCSI storage area network (SAN).

Verifying iSCSI connections

Verify that the connections between a primary HA host or secondary HA host and an iSCSI device are operational

- 1 Using SSH, log in to the primary or secondary HA host as the root user.
- 2 To test the connection to your iSCSI storage device, type the following command:

```
ping iSCSI_Storage_IP_Address
```

- 3 Verify the iSCSI service is running and that the iSCSI port is available by typing the following command:

```
telnet iSCSI_Storage_IP_Address 3260
```



Note

The default port is 3260.

- 4 Verify that the connection to the iSCSI device is operational by typing the following command:

```
iscsiadm -m node
```

To verify that the iSCSI device is correctly configured, you must ensure that the output that is displayed for the primary HA host matches the output that is displayed for the secondary HA host.

If the connection to your iSCSI volume is not operational, the following message is displayed:

```
iscsiadm: No records found
```

- 5 If the connection to your iSCSI volume is not operational, then review the following troubleshooting options:
 - Verify that the external iSCSI storage device is operational.
 - Access and review the `/var/log/messages` file for specific errors with your iSCSI storage configuration.
 - Ensure that the iSCSI `initiatornames` values are correctly configured by using the `/etc/iscsi/initiatornames.iscsi` file.
 - If you cannot locate errors in the error log, and your iSCSI connections remain disabled, then contact your Network Administrator to confirm that your iSCSI server is functional or to identify network configuration changes.
 - If your network configuration has changed, you must reconfigure your iSCSI connections.

Establish an HA cluster. You must connect your primary HA host with your secondary HA host by using the Extreme Security user interface. For more information about creating an HA cluster, see the *Extreme Networks SIEM High Availability Guide*.

Troubleshooting iSCSI issues

To prevent iSCSI disk and communication issues, you must connect Extreme Security, the iSCSI server, and your network switches to a uninterruptible power supply (UPS). Power failure in a network switch might result in your iSCSI volume reporting disk errors or remaining in a read-only state.

In a high-availability (HA) environment, if your primary host fails, you must restore your iSCSI configuration to the primary host. In this situation, the `/store` or `/store/ariel` data is already migrated to the iSCSI shared external storage device. Therefore, to restore the primary host iSCSI configuration, ensure that you configure a secondary HA host. For more information see, [Configuring iSCSI in an HA deployment](#) on page 18.

- 1 Determine whether there is a disk error.
 - a Using SSH, log in to Extreme Security Console as the root user.
 - b Create an empty file named `filename.txt` on your iSCSI volume by typing one of the following command:
 - `touch /store/ariel/filename.txt`
 - `touch /store/filename.txt`

If your iSCSI volume is mounted correctly and you have write permissions to the volume, the touch command creates an empty file named `filename.txt` on your iSCSI volume.

If you see an error message, unmount and remount the iSCSI volume.

- 2 Stop the Extreme Networks Security Analytics services.
 - If you migrated the `/store` file system, type the following commands in the specified order:
 - `service hostcontext stop`
 - `service tomcat stop`
 - `service hostservices stop`
 - `service systemStabMon stop`
 - `service crond stop`
 - If you migrated the `/store/ariel` file system, type the following command:

```
service hostcontext stop
```

- 3 Unmount the iSCSI volume.
 - If you migrated the `/store` file system, type the following commands:
 - `umount /store/tmp`
 - `umount /store`
 - If you migrated the `/store/ariel` file system, type the following command:

```
umount /store/ariel
```

- 4 Mount the iSCSI volume.
 - If you migrated the `/store` file system, type the following commands:
 - `moumt /store`
 - `moumt /store/tmp`
 - If you migrated the `/store/ariel` file system, type the following command:

```
mount /store/ariel
```

5 Test the mount points.

- If you migrated the `/store` file system, type the following command:

```
touch /store/filename.txt
```

- If you migrated the `/store/ariel` file system, type the following command:

```
mount /store/ariel/filename.txt
```

If you continue to receive a read-only error messages after remounting the disk, then reconfigure your iSCSI volume.

Alternatively, you can unmount the file system again and run a manual file system check with the following command: `fsck /dev/partition`.

6 Start the Extreme Security services.

- If you migrated the `/store` file system, type the following commands in the specified order:
 - `service crond start`
 - `service systemStabMon start`
 - `service hostservices start`
 - `service tomcat start`
 - `service hostcontext start`
- If you migrated the `/store/ariel` file system, type the following command: `service hostcontext start`

Related Links

[Configuring the iSCSI volumes](#) on page 14

You can configure iSCSI for a stand-alone Extreme Security Console or a Extreme Security Console that is the primary high-availability (HA) host in an HA deployment.

3 Fibre Channel storage

Configuration overview for Fibre Channel storage

You can configure Fibre Channel (FC) in a standard Extreme Security deployment or in a high-availability (HA) environment. You can also configure FC multipath to provide redundancy if your FC switch fails.

When you configure an FC device, you can move the Extreme Networks Security Analytics data in your `/store` or `/store/ariel` file system. Then, mount the `/store` or `/store/ariel` file system to a partition on the FC device.

Depending on your device configuration, you might be required to create a partition on the volume of your FC disk.

If you configure FC in an HA deployment and your primary HA host fails, your FC device can be used to maintain data consistency with your secondary HA host. For more information about data consistency and shared storage in an HA environment, see the *Extreme Networks SIEM High Availability Guide*.

Configuration overview for Fibre Channel storage

Configuring Fibre Channel (FC) is different for a primary high-availability (HA) host than the secondary HA host. To configure FC, you must ensure that the primary HA host and secondary HA host are not connected in an HA cluster.

Frequently searched data must be moved to a faster disk. For example, move recent data or data that is used for security incident investigations. However, deploying high performance offboard disk storage might be costly. Where possible, use lower performance and less expensive offboard storage for activities such as moving older data, archiving, or for reporting purposes.

If you are using FC only for archive purposes, then use the same mount point for every appliance and configure these mount points to correspond with each unique FC volume.

In deployments that use multiple appliances, ensure that each appliance is configured to use a separate FC volume. Failure to use separate volumes can result in two devices that mount the same block device, which can corrupt the block device file system.

Verifying your Emulex adapter installation

You must verify that an Emulex LPe12002 Host Bus adapter is attached and installed with the correct firmware and driver versions.

To use the Fibre Channel protocol, you must install an Emulex LPe12002 Host Bus adapter on your Extreme Networks Security Analytics appliance. In a high-availability (HA) deployment, you must install an Emulex LPe12002 card on the primary and secondary HA host.

The Emulex LPe Host Bus adapter must use the following driver and firmware versions:

- Driver version: 8.3.5.68.5p
- Firmware version: 1.10A5(U3D1.10A5),sli-3

- 1 Using SSH, log in to your Extreme Security host as the root user:
- 2 Verify that an Emulex LPe12002 card is attached by typing the following command:

```
hbacmd listhbas
```

If no result is displayed, then contact your system administrator.

- 3 Verify that the Emulex card is using the correct firmware and driver versions by typing the following command:

```
hbacmd HBAAattrib
```

device id is the Port WWN that is displayed in the preceding step.

Related Links

[Verifying the Fibre Channel connections](#) on page 25

You must identify the disk volume on the external Fibre Channel device. If required, you must also create a partition on the volume.

Verifying the Fibre Channel connections

You must identify the disk volume on the external Fibre Channel device. If required, you must also create a partition on the volume.

[Verify your Emulex adapter installation.](#)

- 1 Using SSH, log in to your Extreme Security Console as the root user.
- 2 Identify the Fibre Channel volume by typing the following command:

```
ls -l /dev/disk/by-path/*-fc-*
```

If multiple Fibre Channel devices are attached and you cannot identify the correct Fibre Channel volume, contact your system administrator.

- 3 If there is no partition on the Fibre Channel volume, then create a partition on the Fibre Channel device volume.

- a To create a partition, use the GNU parted command:

```
parted /dev/volume
```

- b Configure the partition label to use GPT by typing the following command:

```
mklabel gpt
```

- c If the following message is displayed, type **Yes**.

```
Warning: The existing disk label on /dev/volume will be destroyed and all
data on this disk will be lost. Do you want to continue?
```

- d To create the partition, type the following command:

```
mkpart primary 0% 100%
```

- e Set the default units to TB by typing the following command:

```
unit TB
```

- f Verify that the partition is created by typing the following command:

```
print
```

- g Exit from GNU parted by typing the following command:

```
quit
```

- h Update the kernel with the new partition data by typing the following command:

```
partprobe /dev/volume
```

You might be prompted to restart the appliance.

- i To verify that the partition is created, type the following command:

```
cat /proc/partitions
```

- 4 Reformat the partition and make a file system.

- To create an XFS file system, type the following command: `mkfs.xfs -f /dev/partition`
- For an ext4 files system, type the following command: `mkfs.ext4 /dev/partition`

Related Links

[Verifying your Emulex adapter installation](#) on page 24

You must verify that an Emulex LPe12002 Host Bus adapter is attached and installed with the correct firmware and driver versions.

Moving the /store file system to a Fibre Channel solution

You can move the Extreme Networks Security Analytics data that is maintained in the `/store` file system and mount the `/store` file system to a Fibre Channel (FC) device partition.

[Verifying the Fibre Channel connections](#) on page 25

- 1 Stop the `hostcontext` service by typing the following command:

```
service hostcontext stop
service tomcat stop
service hostservices stop
service systemStabMon stop
service crond stop
```

- 2 Unmount the file systems by typing the following commands:

```
umount /store/tmp
umount /store/transient
umount /store
```

The `/store/transient` file system is mounted only when the `/store` file system is XFS.

- 3 Create the `/store_old` directory by typing the following command:

```
mkdir /store_old
```

- 4 Derive the device partition universal unique identifier (UUID) by typing the following command:

```
blkid /dev/partition
```

- 5 Edit the `/etc/fstab` file to update the existing `/store` file system mount point to `/store_old`.
- 6 Add a mount point for the `/store` file system by adding the following text to the `/etc/fstab` file:

- If the file system is ext4, add the following text

```
UUID=uuid /store ext4 noatime,noauto,nobarrier 0 0
```

,

- If the file system is XFS, add the following text:

```
UUID=uuid /store xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- a Modify the `/store/tmp` mount line to use the following file system options:

```
noatime,noauto,nobarrier 0 0
```

- b If `/store/transient` is listed in the `fstab` file, then type the following file system options:

```
xfs inode64,logbsize=256k,noatime,noauto,nobarrier 0 0
```

- c Save and close the file.

- 7 Mount the `/store` file system to the FC device partition by typing the following command:

```
mount /store
```

- 8 Mount the `/store_old` file system to the local disk by typing the following command:

```
mount /store_old
```

- 9 Copy the data to the Fibre Channel partition by typing the following command:

```
cp -af /store_old/* /store
```

- 10 Mount the file systems by typing the following commands:

```
mount /store/tmp
mount /store/transient
```

The `/store/transient` file system is mounted only when the `/store` file system is XFS.

- 11 Unmount `/store_old` by typing the following command:

```
umount /store_old
```

- 12 Remove the `/store_old` directory from the `/etc/fstab` file.

- 13 Start the `hostcontext` service by typing the following command:

```
service crond start
service systemStabMon start
service hostservices start
service tomcat start
service hostcontext start
```

See [Verifying the Fibre Channel mount point](#) on page 29.

Related Links

[Moving the `/store/ariel` file system to a Fibre Channel storage solution](#) on page 28

You can move the Extreme Networks Security Analytics data that is maintained in the `/store/ariel` file system and mount the `/store/ariel` file system to a Fibre Channel (FC) device partition.

Moving the /store/ariel file system to a Fibre Channel storage solution

You can move the Extreme Networks Security Analytics data that is maintained in the `/store/ariel` file system and mount the `/store/ariel` file system to a Fibre Channel (FC) device partition.

See [Verifying the Fibre Channel connections](#) on page 25.

- 1 After the Extreme Security installation, connect Extreme Security with fibre channel and restart.
- 2 Stop the Extreme Security services by typing the following commands:

```
service systemStabMon stop
service hostcontext stop
service tomcat stop
service hostservices stop
service crond stop
```

- 3 Create a temporary directory by typing the following command:

```
mkdir /tmp/fcdata
```

- 4 Mount the Fibre Channel storage partition to the temporary directory by typing the following command:

```
mount /dev/<partition> /tmp/fcdata
```

Where `<partition>` is the name of the device partition. For example: `sdb1`.

- 5 Copy the data to the Fibre Channel device by typing the following command:

```
cp -af /store/ariel/* /tmp/fcdata
```

- 6 Unmount the Fibre Channel partition by typing the following command:

```
umount /tmp/fcdata
```

- 7 Verify the Universally Unique Identifier (UUID) of the iSCSI device partition by typing the following command:

```
blkid /dev/<partition>
```

Where `<partition>` is the name of the device partition. For example: `sdb1`.

- 8 Edit the `fstab` file by typing the following command:

```
vi /etc/fstab
```

- 9 Add the mount point for the `/store/ariel` file system by adding the following text to the `/etc/fstab` file.

If the file system is ext4:

```
UUID=<uuid> /store/ariel ext4 defaults,noatime,nobarrier 1 2
```

If the file system is XFS:

```
UUID=<uuid> /store/ariel xfs inode64,logbsize=256k,noatime,nobarrier 0
0
```

Where `<uuid>` is the UUID of the fibre channel device partition.

- 10 Save and close the file.

- 11 Mount the `/store/ariel` file system to the FC device partition by typing the following command:

```
mount /store/ariel
```

12 Start the Extreme Security services by typing the following commands:

```
service crond start
service hostservices start
service tomcat start
service hostcontext start
service systemStabMon start
```

[Verifying the Fibre Channel mount point](#) on page 29.

Related Links

[Moving the /store file system to a Fibre Channel solution](#) on page 26

Verifying the Fibre Channel mount point

On the primary host, verify that the file system that you moved is correctly mounted to Fibre Channel device partition.

1 Type the following command:

```
df -h
```

2 Verify that the `/store` or `/store/ariel` file system is correctly mounted to the Fibre Channel device partition.

Configuring Fibre Channel in a standard Extreme Security deployment

In Extreme Networks Security Analytics, you can implement multipath Fibre Channel. If you experience a storage area network or SAN switch issue, multipath provides extra redundancy to prevent disruption to flow and event data.

Ensure that you completed the following tasks:

- [Verify your Emulex adapter installation.](#)
- [Verify the Fibre Channel connections.](#)

1 On your Extreme Security Console appliance, attach both Fibre Channel cables to the Emulex LPe12002 Host Bus adapter.

2 Using SSH, log in to your Extreme Security Console as the root user:

3 Identify a storage area network (SAN) partition by typing the following command:

```
blkid -o list
```

4 Format the partition.

- If your file system is ext4, then type the command: `mkfs.ext4 -L multiPath /dev/partition`
- If your file system is XFS, then type the command: `mkfs.xfs -L multiPath /dev/partition`

5 Stop the Extreme Security services by typing the following commands in the order specified:

```
service systemStabMon stop
service hostcontext stop
service tomcat stop
```

```
service imq stop
service postgresql stop
service hostservices stop
```

- 6 Unmount the file systems by typing the following commands:

```
umount /store/tmp
umount /store/transient
umount /store
```

- 7 Create a `/store_old` directory by typing the following command:

```
mkdir /store_old
```

- 8 Determine the Universally Unique Identifier (UUID) of the device partition by typing the following command:

```
blkid /dev/partition
```

- 9 Edit the `/etc/fstab` file.

- a Replace the existing `/store` file system entry to `/store_old` system.
- b If your file system is ext4, add the following text:

```
UUID=uuid/store ext4 defaults,noatime,nobarrier 1 2
```

- c If your file system is XFS, add the following text:

```
UUID=uuid/store xfs defaults,noatime,nobarrier 1 2
```

- 10 Mount the file systems and copy the data to your device by typing the following commands:

```
mount /store
mount /store_old
cp -af /store_old/* /store
mount /store/tmp
umount /store_old
```

- 11 Start Extreme Security services by typing the following commands in the order specified:

```
service hostservices restart
service postgresql restart
service imq restart
service tomcat restart
service hostcontext restart
service systemStabMon restart
```

- 12 Enable Fibre Channel multipath by typing the following command:

```
mpathconf --enable
```

- 13 Start the multipath daemon by typing the following command:

```
service multipathd start
```

- 14 Restart the system by typing the following command:

```
reboot
```

Configuring Fibre Channel in an HA deployment

To use Fibre Channel storage, or multipath, in a high-availability (HA) environment, administrators must configure the primary HA host and the secondary HA host to use the same storage partition.



Important

You must configure multipath on both the primary and secondary HA hosts before you initiate HA syncing.

- 1 Verify that the correct Fibre Channel hardware is installed on your secondary HA. For more information, see [Verifying your Emulex adapter installation](#) on page 24
- 2 Configure Fibre Channel on your primary HA host. For more information, [Configuring Fibre Channel in a standard Extreme Security deployment](#) on page 29
- 3 Verify the HA Fibre Channel connections. For more information, see [Verifying the Fibre Channel connections](#) on page 25
- 4 Configure the file system mount point for the secondary HA host.
- 5 Enable Fibre Channel multipath service if the fibre channel is configured with multipath. For more information, see [Configuring Fibre Channel in a standard Extreme Security deployment](#) on page 29.

Configuring the mount point for the secondary HA host

You must configure the mount point on the secondary high-availability (HA) host for the file system that is moved to a Fibre Channel storage device.

- 1 Using SSH, log in to the secondary HA host as the root user.
- 2 Derive the UUID by typing the following command:


```
blkid /dev/partition
```
- 3 Update the kernel with the Fibre Channel partition data by typing the following command:


```
partprobe
```

Troubleshoot

If you see a warning error message that the kernel cannot read the partition table, type the following command: `ls -l /dev/disk/by-uuid/partition`. If no output is displayed, then restart the secondary HA host by typing `reboot`.

- 4 Unmount the file systems by typing the following commands:

```
umount /store/tmp
umount /store/transient
umount /store
```

The `/store/transient` file system is mounted only when the `/store` file system is XFS.

- 5 If you redirected the `/store` file system to an offboard device, then choose one of the following options:; edit the `/etc/fstab` file.
 - If the `/store` file system is an XFS file system, update the following lines. For each line, copy the text into a text editor, remove any line breaks, and paste as a single line.

```
UUID=uuid/store xfs inode64,logbsize=256k,noatime,
noauto,nobarrier 0 0
```

```
UUID=uuid/store/transient xfs inode64,logbsize=256k,noatime
```

```
,noauto,nobarrier 0 0
```

```
UUID=uuid/store/tmp ext4 noatime,noauto,nobarrier 0 0
```

- If the `/store` file system is ext4, update the following line:

```
UUID=uuid/store ext4 defaults,noatime,noauto,nobarrier 1 2
```

- 6 If you are moving the `/store/ariel` file system to an offboard device, choose one of the following options to edit the `/etc/fstab` file

- If the `/store/ariel` file system is an XFS file system, update the following lines. For each line, copy the text into a text editor, remove any line breaks, and paste as a single line.

```
UUID=uuid/store/ariel xfs inode64,logbsize=256k,noatime,  
noauto,nobarrier 0 0
```

```
UUID=uuid/store/transient xfs inode64,logbsize=256k,noatime  
,noauto,nobarrier 0 0
```

- If the `/store/ariel` file system is ext4, update the following line:

```
UUID=uuid/store/ariel ext4 defaults,noatime,noauto,nobarrier 1 2
```

Create an HA cluster. For more information, see *Extreme Networks SIEM High Availability Guide*.

4 NFS offboard storage device

Moving backups to an NFS
Configuring a new backup location
Configuring a mount point for a secondary HA host

You can back up the Extreme Networks Security Analytics data to an external Network File System (NFS).

You cannot use NFS for storing active data, which includes the PostgreSQL and ariel databases. If you do use NFS, it might cause database corruption or performance issues.

Depending on your high-availability (HA) deployment, you might be required to change the location of your Extreme Security backup files and configure your NFS share with this new location.

You can move backup files to NFS from a stand-alone Extreme Security Console, configure a new HA deployment, and move backup files to NFS or move backup files from an existing Extreme Security HA deployment.

Moving backups to an NFS

You can configure Network File System (NFS) for a stand-alone Extreme Security Console, new Extreme Security HA deployments, or existing Extreme Security HA deployments.

You must enable the connections to your NFS server for any of the following situations:

- You migrate the `/store/backup` file system to NFS from a stand-alone Extreme Security Console
- You have new and existing HA deployments

You must configure your NFS mounts for any of the following situations:

- If you are migrating the `/store/backup` file system to NFS from a stand-alone Extreme Security Console.
- If you are configuring an HA deployment for the first time, then you must configure an NFS mount point for the `/store/backup` file system on your primary and secondary HA hosts.

To use NFS storage in an HA environment, you must configure the primary HA host and the secondary HA host with the same NFS configurations.

- 1 Using SSH, log in to Extreme Security as the root user.
- 2 Add your NFS server to the `/etc/hosts` file:
`IP address hostname`
- 3 Add the following line to the `/opt/qradar/conf/iptables.pre` file:
`-A INPUT -i interface -s IP address -j ACCEPT`

If you have a dedicated NFS network, `interface` is `ETH0` or `ETH1`

`IP address` is the IP address of your NFS server.

- 4 To update the firewall settings, type the following command:

```
/opt/gradar/bin/iptables_update.pl
```

- 5 Add NFS to be part of the startup routine by typing the following commands:

```
cd /etc/rc3.d
chkconfig --level 3 nfs on
chkconfig --level 3 nfslock on
```

- 6 Start NFS services by typing the following commands:

```
service nfslock start
service nfs start
```

- 7 Add the following line to the `/etc/fstab` file.

```
hostname:shared_directory/store/backup nfs
soft,intr,rw,clientaddr=IP address 0 0
```

You might need to adjust the settings for the NFS mount point to accommodate your configuration.

Example

```
hostname:shared_directory/store/backup
nfs soft,intr,rw,noac 0 0
```

- 8 Move your backup files from the existing directory to a temporary location by typing the following commands:

```
cd /store/
mv backup backup.local
```

- 9 Create a new backup directory by typing the following command:

```
mkdir /store/backup
```

- 10 Set the permissions for the NFS volume by typing the following command:

```
chown nobody:nobody /store/backup
```

- 11 Mount the NFS volume by typing the following command:

```
mount /store/backup
```

The root user must have read and write access to the mounted NFS volume because the `hostcontext` process runs as root user.

- 12 Verify that `/store/backup` is mounted by typing the following command:

```
df- h
```

- 13 Move the backup files from the temporary location to the NFS volume by typing the following command:

```
mv /store/backup.local/* /store/backup
```

- 14 Remove the `backup.local` directory by typing the following commands:

```
cd /store
rm -rf backup.local
```

Configuring a new backup location

If you have an existing high-availability cluster, then you must change the Extreme Networks Security Analytics backup location on your primary HA host.

- 1 Using SSH, log in to the Extreme Security Console as the root user.
- 2 Create a file location to store your Extreme Security backups.



Restriction

Do not create your new backup location under the `/store` file system.

- 3 Add the following line to the `/etc/fstab` file.

```
hostname:shared_directory backup location nfs
soft,intr,rw,clientaddr=IP address 0 0
```

- 4 Mount the new backup file location to the NFS share by typing the following command:

```
mount backup location
```

- 5 Copy the existing backup data to the NFS share by typing the following command:

```
mv /store/backup/* backup location
```

- 6 Log in to Extreme Security
- 7 Click the **Admin** tab.
- 8 On the navigation menu, click **System Configuration**.
- 9 Click **Backup and Recovery**.
- 10 On the toolbar, click **Configure**.
- 11 In the **Backup Repository Path** field, type the location where you want to store your Extreme Security V7.2.5 backup files and click **Save**.
- 12 On the **Admin** tab menu, click **Deploy Changes**.

Configuring a mount point for a secondary HA host

On your existing secondary high-availability (HA) host, you must configure an NFS mount point for the alternative Extreme Networks Security Analytics backup file location.

- 1 Using SSH, log in to the Extreme Security secondary HA host as the root user:
- 2 Create a backup file location that matches the backup file location on your primary HA host.
For more information, see [Configuring a new backup location](#) on page 35.



Restriction

Do not create your new backup location under the `/store` file system.

- 3 Add the following line to the `/etc/fstab` file:

```
hostname:shared_directory backup location nfs
soft,intr,rw,clientaddr=IP address 0 0
```

- 4 Mount the new Extreme Security backup file location by typing the following command:

```
mount backup location
```

Index

Specials

/store file system
moving to iSCSI storage solution 16

C

conventions, guide
notice icons 4
text 5

E

Emulex adapter
installing 24

F

Fibre Channel
configuration overview 24
HA deployment overview 31
overview 24
verifying connections 25
verifying mount points 29
file systems
moving to iSCSI storage solution 15
moving to offboard storage 9

H

HA
offboard storage options 11
HA deployments
configuring mount point 35
Fibre Channel 31

I

iSCSI
configuration options in HA environment 12
configuring standard deployments 13
configuring volumes 14
mounting 18
moving /store/ariel files systems 28
offboard storage options 12
troubleshooting 22
verifying connections 21

M

migration, see moving

N

Network File System, see NFS
network interfaces
secondary 13

NFS
configuring a new backup location 35

P

performance
impact 9

S

secondary network interfaces
overview 13
standard deployments
configuring iSCSI 13
Fibre Channel configuration 29
storage
expansion 9
limitations 10
options 10

T

troubleshooting
iSCSI issues 22