Configuration Guide

Release: 9.6

January 2019

ETI\SPHiNX Inc.
505 Maisonneuve West, Suite 400
Montreal, QC H3A 3C2, Canada
https://www.etinet.com

Contents

Preface

Welcome to the *Configuration Guide*. SPHiNX offers complete disaster recovery capabilities. As a primary repository for data center backups, SPHiNX can also be used as secondary tiered storage for replicated data to meet disaster recovery requirements.

About this guide

The *Configuration Guide* is designed to help you configure SPHiNX and then accomplish the necessary tasks for using virtual media to store and retrieve data. This guide provides procedures for all tasks you must perform to start using SPHiNX.

Note Upgrade, update, and downgrade information is now located in the *SPHiNX Release Notes*.

Audience

SPHiNX is designed for use by a storage area network (SAN) administrator or IT professional who typically works with large data centers and is responsible for ensuring that data backups occur in the organization. This document is designed for personnel who install or maintain SPHiNX. The audience should be familiar with configuring backup applications, Ethernet and Fibre Channel networks, email servers, and tape libraries.

Typographical conventions

This guide uses the following typographical conventions:

Convention	Description
Bold	Used for file names, field names, URLs, interface elements that are clicked/selected, and information that must be used literally.
Bold Italic	Represents variables within file names, command syntax, URLs, or other literal text.
Italics	Used for emphasis, book titles, and variables.
`Monospace`	Used for text that is displayed on-screen, command names and arguments (syntax), code, and command-line text.
`Monospace Italic`	Represents variables within command syntax, code, or command-line text.
Blue Text	Used for cross-references.

 *This icon notes the user who is responsible for performing the procedure that follows.*

Related documentation

The following documentation is provided for SPHiNX:

- *Quick Start Guide*, which provides instructions for installing the hardware and configuring SPHiNX on the network.
- *Configuration Guide*, which describes how to configure SPHiNX and how to use the SPHiNX web interface to manage SPHiNX.
- Help, which provides detailed instructions for working with the web interface
- *Release Notes*, which provides information about system support, known issues, upgrade and downgrade instructions, and other information about the current release.

All documentation is available on the **About** page of the web interface.

Support

For technical assistance, email your inquiries to support@etinet.com. You may also visit the ETINET website at https://etinet.atlassian.net/servicedesk/customer/portal for additional contact and support information.

For the fastest possible resolution, have the following information available:

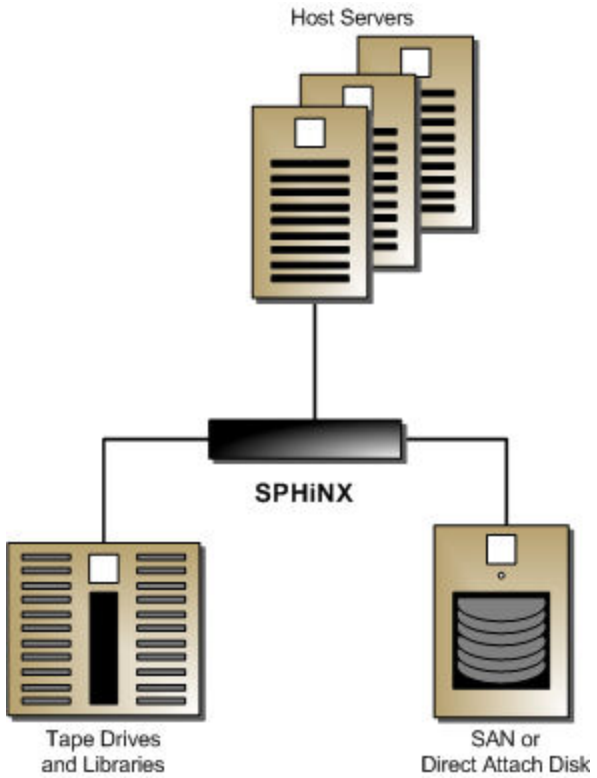
- Your company's name
- SPHiNX hardware platform
- Serial number of your equipment
- Hardware configuration
- Software configuration
- The "Software version" value, including the date created, from the System Status page on the SPHiNX web interface
- A detailed description of the problem you are having with the equipment
- Your name, telephone number, email address, and company address

You may also consider gathering the output of the get VTS_dbginfo utility, which is provided on the SPHiNX server, or you can generate a troubleshooting package from the web interface. The utility and troubleshooting package collects log files and system information. Refer to "Troubleshooting" on page 157 for more information.

1 Introduction

Tape remains the most practical solution for removable storage, and it is often required by regulatory agencies to be archived and stored offsite. However, as the cost of commodity disk storage has decreased, many enterprises view disk-based backup solutions as a feasible alternative to tape-based backup. Disk-based backup, or virtual tape storage, can significantly improve performance, allows users to plan backup and archiving strategies, and enables users to manage data retention and disaster recovery operations.

SPHiNX is a fully integrated virtual tape hardware and software solution. SPHiNX allows host systems to read from and write to a local or SAN-attached file system. Data is automatically exported to a tape device based on job schedules or manually migrated to physical tape for archival storage or disaster recovery, if long-term backup copies are required. The integrated support for backup management application software provides a mechanism for writing to physical tape drives and libraries. If the Clustered Option (implemented through the use of GFS) is enabled in your environment, multiple SPHiNX servers can access a shared set of pools and virtual tapes stored on the same storage array.

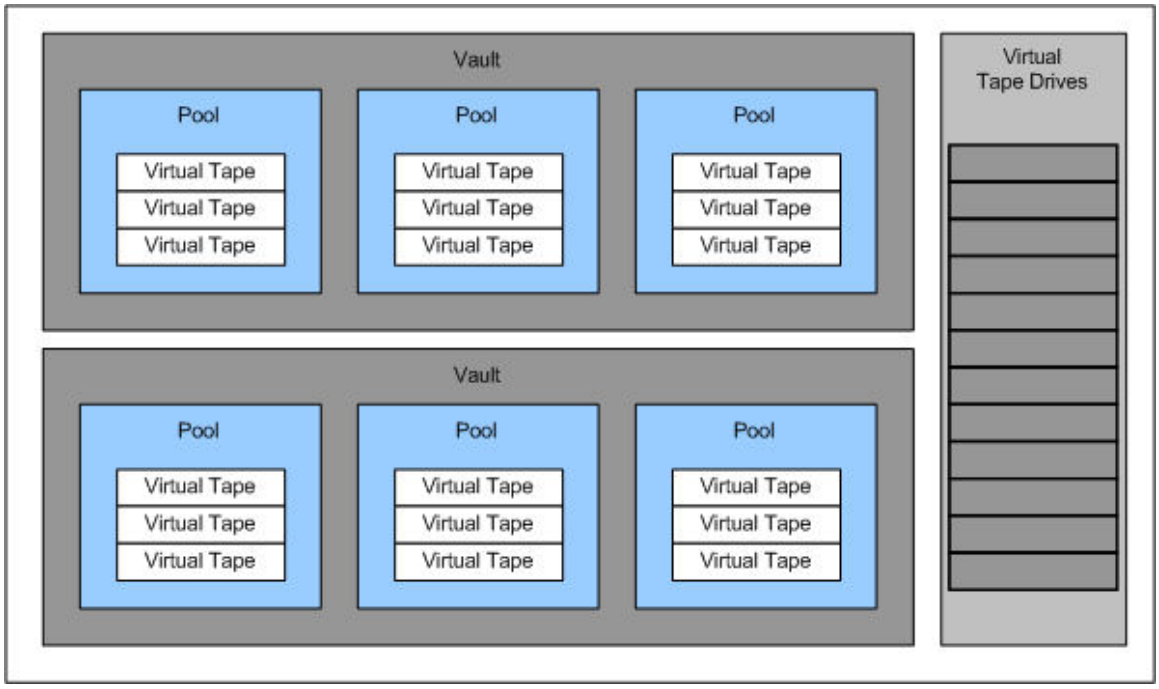


For every host connection to SPHiNX, the host system “sees” one or more tape drives; the virtual tape drive emulates the type of tape drive specified during the initial installation and setup process. Virtual tape drives behave just like real tape drives without the problems generally associated with real tape drives.

SPHiNX delivers reliable, scalable, and high performance virtual tape for backup, restore, archive, and data recovery operations. You can deploy SPHiNX to simplify and streamline traditional tape operations, reduce costs for storage hardware and tape media, automate backup and restore operations, and increase flexibility in managing backed-up data.

The virtual environment

The building blocks of SPHiNX are vaults, pools, virtual tape drives, and virtual tapes. SPHiNX can support multiple virtual tape drives that respond to tape commands just as physical drives would.



Virtual pools are organized into vaults, which correspond to areas of the file system that are configured according to user needs. Defining several vaults is a convenient way to separate data for different applications or users.

Note Vaults are used for storing pools only; SPHiNX uses vaults for virtual tapes and VTD components exclusively. Files and applications should be installed in other storage locations, such as the root partition.

Virtual tapes are “stored” in pools, which are the equivalent to magazines of cartridges used in tape drive libraries. A pool can contain as many virtual tapes as necessary for a given application, which provides a great advantage over cartridge magazines that have physical limits to the number of cartridges they can contain. A pool is synonymous with a directory on a file system.

Note The SPHiNX web interface refers to virtual tapes as “cartridges.” Note that these terms are synonymous in SPHiNX.

Virtual tape drives respond to mount, write, rewind, read, and unload commands from standard backup management applications. Virtual tape drives require virtual tape media, and SPHiNX enables you to create an unlimited number of virtual tapes. A virtual tape is the logical equivalent to a physical tape. However, unlike physical tape media, virtual tapes can be created in any size because the data is pooled on low-cost disk storage. A virtual tape contains only the data written to it, with no wasted space. When a virtual tape is no longer needed, it can be discarded just like a physical tape. A virtual tape is synonymous with a file in a directory.

Overview of features

The heart of SPHiNX is a middleware tape emulation engine that enables SPHiNX to emulate tape storage to host servers and provides backup storage for the data on industry standard, low-cost disk arrays. Data stored in SPHiNX can later be copied to real tape media for archival storage or disaster recovery if long-term backup copies are required. The advantages of this approach include the following:

- Access to data in SPHiNX is almost immediate, and there is no tape to mount or rewind and no searching through tape volumes for data files.
- Dynamic Data Reduction, which allows SPHiNX to compress files as they are written to disk storage devices. Its use can provide up to 12 times the available storage capacity and reduce the amount of associated storage costs. This feature uses an “on-the-fly” compression algorithm that creates little processor overhead and can increase performance and throughput by decreasing the volume of data written to disk.
- Tape-to-Tape Export, which enables you to export data on a virtual tape to a physical tape in an external tape drive or library. This provides a one-to-one mapping of virtual to physical tape. When creating the tape-to-tape export job, you can choose whether the data remains in virtual tape format or host format. This allows application-aware exports because you have the ability to name the virtual tapes such that they are the same as a pool of physical tape cartridges. This then ensures that DR reports created by backup applications are accurate when a virtual tape has been written to physical tape.
- Stacked Tape Export, which enables you to export a virtual tape to one or more physical tapes in an external tape library or drive. The entire virtual tape, including its header information (metadata), is exported by a backup management application. This is also referred to as “migrating” a virtual tape.

  Note This is an optional feature which must be licensed separately. Refer to the Release Notes to find out if your model comes with this feature.
- Dynamic Import provides the ability to dynamically import data from pre-existing physical tapes in a physical tape device. This enables you to use older tape formats and restore them to a host. Or, you can convert older physical tapes by importing them and then exporting the virtual tapes to newer physical tapes. For example, you can import DLT7000 tapes into SPHiNX; when you import physical tapes, the data on those tapes is stored on virtual tapes. Then, to convert the data to LTO-4 format, you could mount each virtual tapes in a VTD that emulates an IBM TD4 drive and restore them to a host.
- Scan/Cleanup, which enables SPHiNX to scan pools and virtual tapes to identify virtual tapes that are past their retention period. Scan/Cleanup can erase old virtual tapes to recover disk space. You can also schedule virtual tape erasures when the overall disk space falls below a specified threshold. Finally, Scan/Cleanup can erase tapes after they are exported to physical tape.

The following SPHiNX features enable you to simplify and streamline tape operations from the host server, reduce costs for storage, automate backup and restore operations, and increase flexibility in managing backed-up data:

- Flexible and extendable, enabling you to create any number of virtual tape pools that “contain” any number of virtual tapes
- Compatibility with IBM Backup, Recovery, and Media Services (BRMS)
- Integration with Help/system’s Robot/SAVE® without disruption to current policies
- Support for migration through the use of IBM Tivoli Storage Manager

Optional features that further enhance the benefits of SPHiNX include the following:

- Clustered Option — Offers enhanced access to shared vaults and eliminates single points of failure by deploying multiple SPHiNX systems into a set of clustered nodes. In the event of a failure, the Clustered Option (implemented through the use of GFS) enables any active SPHiNX system in the cluster to have access to the data, ensuring uninterrupted service to host systems.
- WAN Acceleration — Provides 300Mb and 1Gb options to overcome bottlenecks associated with TCP and to enable replication and data synchronization over the WAN regardless of distance and network conditions. WAN Acceleration enables end-to-end data transfers at near maximum bandwidths, ensuring scalability, network efficiency, security, and bandwidth control when replicating data between sites and SPHiNX systems. This feature is for use with Data Replication and Remote Export.
- Data Replication — Enables the creation of a disaster recovery plan by efficiently copying or synchronizing backup data between a local SPHiNX server and one or more remote SPHiNX sites. This allows for maintaining one or more copies of backup data at a remote site. After the initial backup is copied to one or more remote locations, only that portion of the backup data that has changed since the last backup is transmitted from the local site to the remote site.
- Data Encryption— Encrypts and decrypts backup data written on disk from one or more host servers. Compliance regulations and organizations highly recommend the encryption of valuable data; Data Encryption provides a robust encryption solution that deploys on existing hardware. Industry-standard 256-bit AES symmetric key encryption is used.

Accessing the SPHiNX web interface

SPHiNX is managed through a standard web browser interface. To access the web interface, launch a supported web browser that is on the same internal network as SPHiNX and then enter the following URL:

https://*ip_address*

where *ip_address* is the management network interface address.

Or, if the Domain Name System (DNS) is configured on the network, enter the following:

https://*hostname*

where *hostname* is the hostname of the SPHiNX server.

If SPHiNX is configured to use a self-signed certificate to secure communication between your browser and the SPHiNX web application server, the certificate may cause the browser to display a warning page and certificate errors. You can accept the certificate or add an exception (depending on your browser) and continue to the web interface.

Links on the navigation pane on the left side of the page enable you to navigate through SPHiNX functions.

Overview of Tasks

After completing the procedures provided in the *SPHiNX Quick Start Guide*, you can continue the initial configuration of the SPHiNX server. Then, you can use SPHiNX to manage your virtual media.

The following outlines the general tasks that you must complete to configure SPHiNX and perform day-to-day tasks to maintain SPHiNX. Many of these procedures for the tasks are now provided in the online help.

To configure the SPHiNX server:

1. If necessary, upgrade or update the SPHiNX software as described in the *SPHiNX Release Notes*.
2. Validate or change the standard vault layout as described in "Reconfiguring Vaults" on page 18.
3. Configure licensing for managed capacity, standalone virtual tape drives (VTDs), Data Encryption, and WAN Acceleration (used by Replication and Remote Export) as described in Enabling Licensed Features.
4. Configure target and initiator ports, so that you can create virtual tape libraries (VTLs) and virtual tape drives (VTDs) and attach physical devices. See Configuring Ports.
5. Create VTLs as described in "Managing VTLs" on page 34. If necessary, you can also create VTDs as described in "Managing standalone VTDs" on page 39.
6. Enable and configure virtual tape exports:
   - Tape-to-tape exports enable you to export data on virtual tapes to a physical tapes in an external tape drive or library, providing a one-to-one mapping of virtual to physical tape, and you can choose whether the data remains in virtual tape format or host format. See "Enabling and Performing Tape-to-tape Exports" on page 45
   - Stacked exports enable SPHiNX to export, or "migrate", virtual tapes to physical tapes in non-native format through the use of a backup management application. When a virtual tape is exported this way, all data on the virtual tape is written to physical tape, including the header information (metadata), and a virtual tape may span multiple physical tapes. Stacked exports allow for better use of the disk space on the storage array. See "Enabling and Performing Stacked Exports" on page 51 for more information.
   - Remote exports enable you to export virtual tapes to a remote SPHiNX server; this is also referred to as "role swapping". The exported tapes are stored in vaults (/VAULTxx) on the remote server. See "Enabling and Configuring Remote Export" on page 70 for details.
7. If desired, configure Data Replication, which enables you to create and schedule replicate jobs that export virtual tapes to a remote SPHiNX server, for redundancy or disaster recovery purposes. Exported tapes are stored in data partitions (/DATAxx) on the remote server. See "Enabling and Configuring Data Replication" on page 60.

8. If licensed, configure Data Encryption, which enables SPHiNX to encrypt data that is stored on virtual tape. See "Enabling and Configuring Data Encryption" on page 87.
9. Enable and configure Scan/Cleanup, which erases old virtual tapes to recover disk space. See "Enabling and Configuring Scan/Cleanup" on page 115 for more information.
10. Configure access control to grant or limit access to specific SPHiNX functions. See "Configuring User Accounts" on page 118.
11. Configure the user interface as described in "Configuring Web Interface Preferences" on page 135.
12. Write labels to the virtual tapes from the host server as described in "To label virtual tapes" on page 99.
13. The SPHiNX server provides an Intelligent Platform Management Interface (IPMI) card, which has a dedicated Ethernet port for hardware management. It also uses a MegaRaid controller that can notify users of hardware problems. If you wish to use these features, see "Configuring Alerts" on page 138 for more information.
14. Back up the database and configuration files as described in "Backing up the SPHiNX server" on page 149.

To maintain SPHiNX

- Manage the virtual tape libraries (VTLs) and virtual tape drives (VTDs) as necessary, such as renaming VTDs according to your chosen naming convention. Also, create and manage pools and tapes as necessary. See "Creating and Managing Virtual Media" on page 93.
- View and save log files. See "Log files" on page 164 for more information.
- Start and stop processes, including the main TapeServer process, from the Manage System Tasks page.
- Power on and off the SPHiNX system as described in "Powering up and down" on page 153.
- Maintain the file system (run a file system check) and view file system (vault) status from the System Status page. See "Maintaining the file system" on page 153.
- Monitor backups and restores from the Manage Virtual Tapes page.

3 Reconfiguring Vaults

By default, vault storage is preconfigured on most SPHiNX servers. Prior to using this storage, you may want to review and change the configuration. For example, you may want to define additional vaults, which provide a convenient way to separate data for different applications or users. You may want to reconfigure vault storage before creating virtual tape drives (VTDs) or using SPHiNX, though you can use SPHiNX without reconfiguring vaults. Or you may want to add internal or external storage if your appliance supports this.

Note Vaults are used for storing pools only; SPHiNX uses vaults for virtual tapes and VTD components exclusively. Files and applications should be installed in other storage locations, such as the root partition. In addition, customer data should not be stored on VAULT00, which provides a small amount of space needed for system maintenance.

Prior to using SPHiNX, you may want to shrink the size of VAULT01 or reconfigure the layout of the additional internal storage, possibly creating more vaults.

Installing internal storage

You should add internal storage before changing vault storage if additional disk packs were purchased. These appliances provide two mirrored internal SSDs where the operating system is located, and they provide an internal drive bay with up to 16 drives that can be used for storing user data. The drives are formatted using the Z File System (ZFS) as one or more RAIDZ sets instead of physical RAID arrays. This section can be used to add additional disk packs, which increases the additional space to /VAULT01.

If you would like to learn more about ZFS, see https://en.wikipedia.org/wiki/ZFS. To view your current disk storage configuration, go to **Configuration > System > Edit System Settings > Disk Storage** on the SPHiNX web interface.

To install a disk pack and configure the ZFS RAID set

1. Access the SPHiNX web interface and log in as the **admin** user.
2. Each ZFS RAID set consists of four (4), five (5) or eight (8) internal drives, depending on the model. To view the current RAID set, click **Configuration > System > Edit System Settings > Disk Storage**. The internal disks that are used for virtual media storage are shown in these columns:
    - For the vault (if one has been created), these columns are displayed:
        - Pool — The name of the storage pool (also referred to as a "ZFS dataset" or "vault").
        - Label — The name of the disk label
        - Mount Point — The mount point of the storage pool

- Raid Set — The name of the RAID set to which the disk belongs
- Model — The manufacturer and model name of the disk
- Serial Number — The serial number of the disk; click on the serial number to view detailed information about the disk
- Transport — The protocol used by the disk
- Status — The status of the disk (OK, Failed, Predictive Failure)
- Capacity — The size of the disk
- Device Name — The devices that were created on the disk
- ID — The disk's World Wide Name (WWN)

3. Before inserting the new disk pack in to the chassis, make note of the serial number information on the disk pack. The following picture shows where to look on the drive. You will need this information when selecting the correct drives to add to the ZFS RAID set later in this procedure.

4. Add the disk pack to the appliance:
   a. Open the drive bay door on the SPHiNX chassis.
   b. On the CS or ES model, remove the bezel.
   c. Insert the disk pack into an empty slot.

Refer to the *Quick Start Guide* for illustrations of the appliances and their slots.

5. After inserting the new disk pack into the empty slot, verify that a green or blue LED is illuminated. The LED will blink and then will become solid as the drives are ready.
6. Go to the **Disk Storage** section of the **Manage Settings** page again to view the newly added disks. They are listed without an associated pool.
7. Make note of the WWNs associated with the new disks (and ignore any external storage).
8. Add the new disks to current pool:
   a. In the Internal disks attached section of the **Disk Storage** tab on the **Manage Settings** page, select at least four (4), five (5) or eight (8) disks depending on your RAIDZ configuration. Click in all their checkboxes on the right side of the table.

      Note You must select disks in multiples of four, five, or eight depending on your Sphinx version and configuration.

   b. Click  to add the disks as a single ZFS dataset (or "storage pool").
9. Confirm that a new RAID (**raidz2-*x*** or **raidz1-*x*** with the new disks in the ONLINE state is listed.
10. Navigate to the **System Status** page and verify that the new storage capacity for /VAULT01 increased.
11. Repeat these steps as necessary for additional disk packs.

Changing vault storage on an ext3 or ext4 file system

For the SPHiNX 1U-s, 2U-s, 3U-s, and 3U-ns appliances, you must use a Linux partition editor, such as **parted** or **druid**, to review the current configuration

Then, before changing the vault configuration, consider the following recommendations:

- Do not resize any vault on the operating system partition(s) (/dev/sda), and VAULT00 cannot be used to store user data.
- The minimum partition size is 1TB.
- The maximum supported partition size is 16TB.
- All data on a partition that is resized will be lost.

Keep in mind that performance and system operations will be slow when vaults are at maximum capacity.

To view your current disk storage configuration, go to **Configuration > System > Edit System Settings > Disk Storage** on the SPHiNX web interface.

Note For information about reconfiguring a vault on ZFS, see "Changing vault storage on a ZFS dataset" on page 24.

Reviewing the vault layout

To view the current vault configuration

1. Log in to the SPHiNX server as the root user.
2. Use the **df** command to view the current disk utilization:

   ```
   df -H
   ```

   Here is an example of the output. The bolded lines indicate partitions that are eligible for configuration:

   ```
   Filesystem            Size  Used Avail Use% Mounted on
   /dev/sda2              19G  7.1G   11G  40% /
   /dev/sda4              76G  184M   72G   1% /VAULT00
   /dev/sda1              99M   23M   71M  25% /boot
   tmpfs                 2.0G     0  2.0G   0% /dev/shm
   /dev/sdb1             3.3T  535G  2.6T  17% /VAULT01
   ```

3. Use **parted** to display the current partition layout for all disks.

   ```
   parted /dev/sdb print
   ```

   Here is an example of the output:

   ```
   Model: AMCC 9650SE-16M DISK (scsi)
   Disk /dev/sdb: 3643GB
   Sector size (logical/physical): 512B/512B
   Partition Table: gpt

   Number  Start   End     Size    Type     File system Flags
   1       17.4kB  3643GB  3643GB  primary ext3
   ```

Modifying the vault layout

To change the vault configuration

Note You can perform this procedure multiple times, if necessary.

1. Identify the partition to modify. This example will modify VAULT01 (sdb1).
2. Unmount the file system.

   ```
   umount /VAULT01
   ```

3. Create partitions on the disk.
   a. Erase the first 1MB of the disk by writing zeros to it:

      ```
      dd if=/dev/zero of=/dev/sdb bs=1024 count=1024
      ```

   b. Create a GPT disk label, which is a GUID partition table:

      ```
      parted -a optimal /dev/sdb mklabel gpt
      ```

   c. Create a primary partition that will span the entire disk:

      ```
      parted -a optimal /dev/sdb mkpart primary ext4 0% 100%
      ```

Or, create multiple partitions to consume all disk space with each spanning 50%:

```
parted -a optimal /dev/sdb mkpart primary ext4 0% 50%

parted -a optimal /dev/sdb mkpart primary ext4 51% 100%
```

Or, you can specify the size in TB:

```
parted –a optimal /dev/sdb mkpart primary ext4 0TB 16TB
```

d. Review the layout by entering the following command:

```
parted /dev/sdb print
```

Here is an example of the output (for a 14.9TB partition):

```
Model: LSI MR9280-16i4e (scsi)
Disk /dev/sdb: 14.9TB
Sector size (logical/physical): 512B/512B
Partition Table: gpt
Number  Start   End     Size    File system  Name     Flags
1       1049kB  14.9TB  14.9TB               primary
```

4. Create file systems on the newly created partitions. Format the disk partition by entering the following command:

```
mkfs.ext4 -L /VAULT01 /dev/sdb1
```

When specifying a vault name, use this format: **VAULT*xx***, where *xx* indicates a number.

Repeat this command, incrementing *xx* for each new vault.

Note You can move existing pools to the new vault, if necessary (after completing this procedure). Refer to the online help for details.

5. Update the file-system table to reflect the new disks. Using a text editor, add the following lines to the **/etc/fstab** file for each vault created above:

```
LABEL=/VAULT01 /VAULT01 ext4 defaults 1 2
```

Repeat this command for each vault.

6. Create the mount directories by using the **mkdir** command for each of the vaults that were created above. Here is an example of the command to create the mount directory for VAULT01:

```
mkdir /VAULT01
```

Repeat this command for each vault.

7. Mount the new vault and set permissions. Here are example commands:

```
mount /VAULT01

chown bill.root /VAULT01

chmod 750 /VAULT01
```

Repeat these commands for each vault.

8. Verify the new configuration by entering the following command:

   ```
   df -H
   ```

Renaming vaults

You may need to rename a vault on an ext3 or ext4 file system.

Note When renaming vaults, some existing policies could break. To avoid breaking them, either disable the policies before renaming the vaults or edit them afterwards.

For information about renaming a vault on a replication target (renaming a VAULT file system to a DATA file system), see "Configure a data partition on a target server" on page 62.

To rename a vault

1. Click **Administration > System Tasks** on the navigation pane and then click **Stop TapeServer**.
2. Log in to the server as **root**.
3. Review the existing vault layout and identify the device to rename. Use the **df** command to view the current disk utilization:

   ```
   df -h
   ```

   Here is an example of the output:

   ```
   Filesystem      Size    Used    Avail   Use%    Mounted on
   /dev/sda2       11G     3.7G    6.3G    37%     /
   /dev/sda4       92G     50G     38G     57%     /VAULT00
   /dev/sda1       104M    16M     83M     16%     /boot
   /dev/sdb1       4.9T    229M    4.7T    1%      /VAULT01
   /dev/sdb2       4.9T    868G    3.8T    19%     /VAULT02
   /dev/sdc1       7.9T    1.6T    5.9T    22%     /VAULT03
   /dev/sdd1       4.0T    1.2G    3.8T    1%      /VAULT04
   tmpfs   2.1G            0       2.1G    0%      /dev/shm
   ```

4. Unmount the file system:

   ```
   umount /VAULT03
   ```

5. Copy the **/etc/fstab** file to a backup file:

   ```
   cp /etc/fstab /etc/fstab.backup
   ```

6. Relabel the device, using the file system name from step 3:

   ```
   e2label /dev/sdc1 /VAULT05
   ```

7. Edit **/etc/fstab** and replace the old vault name with the new vault name.
8. Rename the mount point:

   ```
   mv /VAULT03 /VAULT05
   ```

9. Mount the file system and set permissions:

   ```
   mount /VAULT05
   chown bill.root /VAULT05
   chmod 750 /VAULT05
   ```

10. Verify that it mounted correctly by running the **df** command again.
11. Click **Administration > System Tasks** on the navigation pane and then click **Start TapeServer**.

Changing vault storage on a ZFS dataset

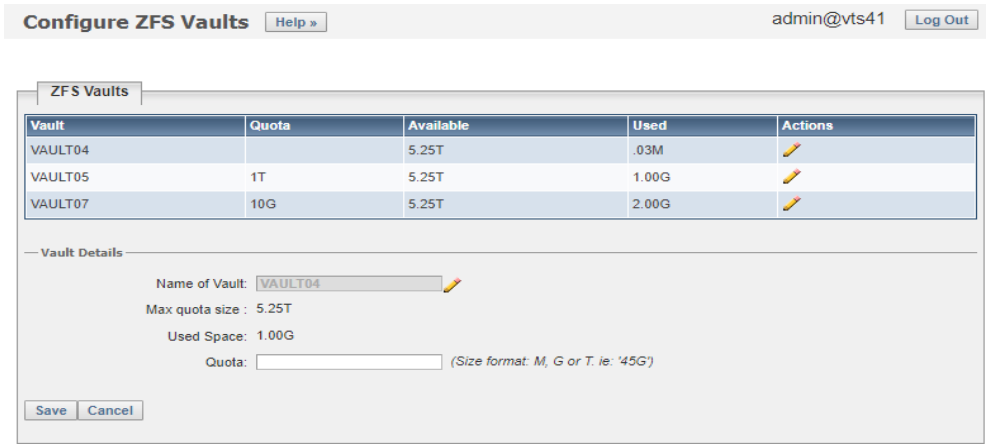
You can change the vault layout by creating additional vaults (as ZFS datasets) or by renaming an existing vault. For NS appliances, the vault layout can be changed only if internal storage has been added subsequently.

ZFS is more than a simple file system. It provides the facilities of a logical volume manager (LVM), which allow you to create a pool of storage and then divide it into datasets (VAULTs) as needed. The initial configuration of a SPHiNX system provides ZFS pool named “storage” and all internal disks are assigned to this pool. If more disks were added to the system, as described in "Installing internal storage" on page 18, the disks were added to this “storage” pool.

Creating a ZFS dataset on internal storage

To create an additional vault

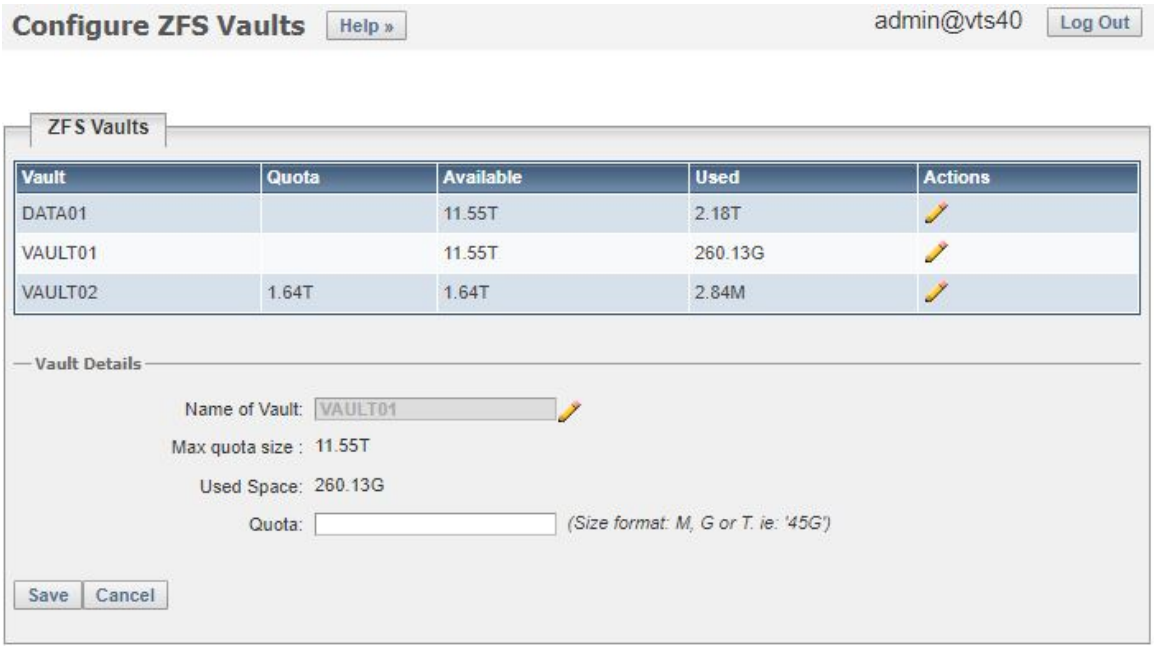
The page allows configuring (add and modify) ZFS Vaults.
To access the page select on the left-hand panel **Configuration** > **ZFS Vaults**.



The main page lists all the existing vaults with their names and assigned quotas.
In the **Actions** column - next to the vault - the edit button allows modifying the vault's configuration.

To add a Vault

1. Click **Configuration > ZFS Vaults** on the navigation pane.
2. Click **Add Vault** on the bottom of the page.
3. In the **Vault Details** section, name the Vault following the *VAULTxx* or *DATAxx* format, where *xx* are digits.
4. Fill in the quota field, giving it a value corresponding to a size defined in MegaBytes (M), GigaBytes (G) or TeraBytes (T).
5. **Save** the new Vault's configuration.



Note If the value of the Vault quota is lower than 1000Mb/1Gb, an error (red tagged) message will state that the vault cannot be created.

Renaming and editing ZFS datasets on internal storage

To edit a Vault

1. On the ZFS Vaults page, in the **Actions** column of the vault that you want to change click the edit button .
2. Modify the name by clicking on the edit button next to the Vault Name field. By default, this field is grayed out (if the Vault has already a name assigned) to avoid stopping the Tape Server by accident. Renaming a vault stops the Tape Server. Click **OK** if you want to keep renaming the vault or the close button if you want to review the running actions before stopping the Tape Server.

3. Change or input a quota value for the vault in MegaBytes (M), GigaBytes (G) or TeraBytes (T).
4. **Save** the change(s). **Cancel** if you dont want to save the changes.

Adding vaults on external storage devices

If an external storage device is connected to SPHiNX, you can use it to configure additional vaults. Up to 100 vaults are supported per SPHiNX server. Refer to the *Quick Start Guide* for cabling instructions if you want to attach a new device.

Note If the Clustered Option (GFS) is used in your SPHiNX environment, see "Installing GFS for SPHiNX" on page 172 for instructions to create vaults.

Before configuring the vault, consider the following recommendations:

- The minimum partition size is 1TB.
- The maximum supported partition size is 16TB.
- All data on a partition that is resized will be lost.

Keep in mind that performance and system operations will be slow when vaults are at maximum capacity.

To add a vault to SPHiNX

1. If you attached a new storage device to SPHiNX, make sure that the cable is plugged in and the link light is illuminated (for Fibre Channel) on the SPHiNX server. The port to which the external storage device is attached must be set to “physical”. See Configuring Ports for more information.
2. Set up a partition on the external storage device (if necessary, ask your storage area network administrator for assistance). The maximum size supported by SPHiNX is 16TB.
3. Identify the disks.
   a. Log in to the SPHiNX server.
   b. Become root (using the **su** command).
   c. Enter the following command to determine the disk partitions:

      ```
      parted -l
      ```

      Output similar to the following is displayed:

      ```
      Model: LSI MR9280-16i4e (scsi)
      Disk /dev/sda: 107GB
      Sector size (logical/physical): 512B/512B
      Partition Table: msdos

      Number  Start   End     Size    Type     File system     Flags
       1      1049kB  525MB   524MB   primary  ext4            boot
       2      525MB   21.5GB  21.0GB  primary  ext4
       3      21.5GB  23.6GB  2147MB  primary  linux-swap(v1)
       4      23.6GB  107GB   83.7GB  primary  ext4

      Model: LSI MR9280-16i4e (scsi)
      Disk /dev/sdb: 14.9TB
      Sector size (logical/physical): 512B/512B
      Partition Table: gpt
      ```

```
Number  Start   End     Size    File system  Name     Flags
1      1049kB  14.9TB  14.9TB  ext4         primary

Model: LSI MR9280-16i4e (scsi)
Disk /dev/sdc: 12.0TB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start   End     Size    File system  Name     Flags
1      1049kB  5000GB  5000GB  ext3         primary

Model: LSI MR9280-16i4e (scsi)
Disk /dev/sdd: 12.0TB
Sector size (logical/physical): 512B/512B
Partition Table: gpt

Number  Start  End  Size  File system  Name  Flags
```

d. If the partition is not visible, enter the following command to scan the SCSI connections and detect new hardware:

```
/usr/local/tape/bin/rescan-scsi-bus.sh -l -c -r -w
```

Output similar to the following is displayed:

```
1 new device(s) found.
```

If you cannot see the partition after rescanning the SCSI connections, reboot the SPHiNX server.

4. Complete these steps to configure the disk partition:
   a. Erase the first 1MB of the disk by writing zeros to it:

```
dd if=/dev/zero of=/dev/sdb bs=1024 count=1024
```

   b. Create a GPT disk label, which is a GUID partition table:

```
parted /dev/sdb mklabel gpt
```

   c. Create a primary partition that will span the entire disk:

```
parted -a optimal /dev/sdb mkpart primary ext4 0% 100%
```

Or, you can create multiple partitions that use all disk space with each partition using 50% of the disk:

```
parted -a optimal /dev/sdb mkpart primary ext4 0% 50%
parted -a optimal /dev/sdb mkpart primary ext4 51% 100%
```

Or, you can specify the size in TB:

```
parted –a optimal /dev/sdb mkpart primary ext4 0TB 16TB
```

5. Format the disk partition by entering the following command:

```
mkfs.ext4 -L /VAULT01 /dev/sdb1
```

When specifying a vault name, use the following format: **VAULT*xx***, where *xx* indicates a number. Repeat this command, incrementing *xx* for each new vault. Replace **/dev/sdb1** with each new partition name and so on, as in these examples:

```
mkfs.ext4 -L /VAULT02 /dev/sdb2
mkfs.ext4 -L /VAULT03 /dev/sdc1
```

By convention:

- VAULT00 remains unchanged as it's assigned to the system
- VAULT01 to VAULT09 are assinged to local storage
- VAULT10 to VAULT49 are assigned to external SAN storage
- VAULT50+ should be used for external NAS storage

6. Create the mount directories by using the **mkdir** command for each of the vaults that were created above. Here is an example of the command to create the mount directory for VAULT01:

   ```
   mkdir /VAULT01
   ```

   Repeat this command for each new vault.

7. Update the file-system table to reflect the new disks. Using a text editor, add the following lines to the **/etc/fstab** file for each vault created above:

   ```
   LABEL=/VAULT01 /VAULT01 ext4 defaults 1 2
   ```

   Repeat this command for each new vault.

8. Mount the newly created disks by entering the following command:

   ```
   mount /VAULT01
   ```

   Repeat this command for each new vault.

9. Assign access rights to the newly created vaults by completing the following steps:
   a. Change the ownership of the vaults by entering the following command:

      ```
      chown bill.root /VAULT*
      ```

   b. Change the rights of the vaults by entering the following command:

      ```
      chmod 750 /VAULT*
      ```

   c. Change the rights of the **lost+found** directories by entering the following command:

      ```
      chmod 750 /VAULT*/lost+found
      ```

How to connect a NAS to your appliance

This section explains how to configure NFS on a SPHiNX appliance in order to connect it to a NAS (Network Attached Storage).

You can connect your NAS through a dedicated network or through a regular network.

1. In order to configure the dedicated network, your SPHiNX has to be equipped with an additional network card that is paired with the card attached to the NAS.

2. For the regular network, neither SPHiNX nor NAS need a special configuration or card.

Pre-requirement: at least one container on the NAS that has been created and configured to share with the SPHiNX appliance. When configuring the container of NAS, make sure that the access protocol is NFS selected. Also, it is recommended to enter the FQDN or IP Address of the SPHiNX to restrict access to that container. For more information, refer to the specific NAS documentation.

When connected to SPHiNX, the NAS container is accessed via NFS through a VAULT. The VAULT needs to be configured manually at the command line. Below are the necessary steps to configure a VAULTxx - replace xx with digits, for example VAULT03. Replace <NasIP> with the NAS IP address and replace <NasContainer> with the name of the NAS container. If necessary, repeat the steps below for each NAS container you want to access through a VAULT.

1. Log in to the SPHiNX server as root user.
2. Make sure that the SPHiNX appliance sees the NAS container through NFS: `showmount -e <NasIP>`. If you don't see the container or if an error is listed, stop here and refer to the documentation of your NAS to fix this issue.
3. Append the following line for each NFS mount point in the file `/etc/fstab`

```
<NasIP>:/<NasContainer>/VAULTxx       nfs
soft,timeo=100,retry=1 0
0
```

example:

```
192.168.99.20:/containers/ShareA2/VAULT03         nfs
soft,timeo=100,retry=1 0
0
```

4. Create the mount point for the new VAULTxx by using the `mkdir` command:

```
mkdir /VAULTxx
```

5. Mount the new VAULTxx and set permissions:

```
mount /VAULTxx
chown bill.root /VAULTxx
chmod 750 /VAULTxx
```

6. Verify the new configuration by entering the following command:

```
df -H
```

7. Open the SPHiNX UI and go to the **System Status** page. Make sure the new VAULTxx appears in the **Storage** section of the page. Note that it is normal to see **N/A** for Size, Used and Available, since this information is provided by your NAS and not by the SPHiNX appliance.

Securing your NAS

When SPHiNX connects to a NAS, the NAS storage becomes available to SPHiNX via NFS.

To secure your NAS, it is recommended to:

- Connect your SPHiNX to your NAS either directly or on a secured private LAN where everything connected to the switch is trusted
- Configure your NAS containers in such a way that only your SPHiNX has access rights.

Note Networking NFS through firewalls is not recommended, because the NFS ports are randomly assigned after each re-boot session.

Note In case NFS looses the connection to the NAS and the Notification Email is set (**Raid Alerts** option checked in the notifications panel), an email notification will be sent to indicate the condition. For more details, see the *Configuring notification settings* in the HelpSet Guide.

Enabling Licensed Features

Before you can use SPHiNX, you must enable licensing. You can enable licensing for the following:

- Managed capacity, which includes licensing for virtual tape libraries (VTLs)
- Standalone virtual tape drives (VTDs) and compression, if included
- Data Encryption
- 300Mb and 1Gb WAN Acceleration (for use with Data Replication and Remote Export)

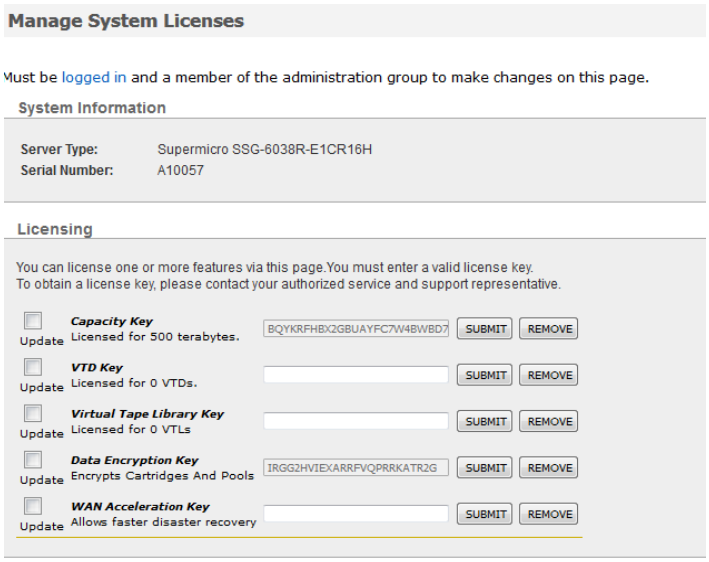
To obtain license keys:

Log in to https://register.etinet.com and follow the instructions on the site. License keys are generated based on the serial number of the SPHiNX server, so any server hardware replacement or upgrade that occurs at a customer site will require new license keys. Obtain a set of license keys for each SPHiNX server in your environment.

To add a license key:

 *Requires Administration group membership*

1. Click **Configuration > System** on the navigation pane.
2. Click **Manage System Licenses**. The following page is displayed:



3. a. To enable SPHiNX to store data (managed capacity), including VTLs and VTDs, type or paste the license key in the **Capacity Key** field and then click **SUBMIT**. On the pop-up dialog, click **OK** to confirm that you want to add the key.

   If this is the first time you are entering a capacity license key, you are prompted to accept the end-user license agreement. Read the agreement and click **ACCEPT**. If you do not accept the agreement, you cannot use the SPHiNX server.

   b. In the **VTD Key** field, type or paste the license key, if VTDs are licensed by number and then click **SUBMIT**. On the pop-up dialog, click **OK** to confirm that you want to add the key.

   c. If Data Encryption is licensed, type or paste the license key in the **Data Encryption Key** field and then click **SUBMIT**. On the pop-up dialog, click **OK** to confirm that you want to add the key.

   d. If WAN Acceleration is licensed, for use during replication or remote exports, type or paste the license key in the **WAN Acceleration Key** field and then click **SUBMIT**. On the pop-up dialog, click **OK** to confirm that you want to add the key.

   e. Restart the TapeServer service. Click **Administration > System Tasks** on the navigation pane. Then, click **Stop TapeServer** and then click **Start TapeServer**.

4. Submitting a valid license key enables you to perform all other installation and configuration tasks. Submitting a valid license key for Data Encryption adds the localhost as the key server that generates keys; you can now add a key database backup host. If a key is not valid, an error message is displayed and the key is not accepted.

   After licensing is initially enabled for one or more features, you can update a license key. For example, you can add to or subtract capacity. You can also remove a licensed feature. Refer to the online help for instructions. If necessary, obtain the license key from your Sales representative.

4 Configuring Ports

After cabling the host server(s) and external devices to the SPHiNX server, you must configure the ports to enable SPHiNX to communicate properly with each device (target or initiator). Or, if you attach a physical tape drive or storage device to the server after initial configuration, you must define the port as physical. Ports connected to host servers must be defined as virtual.

To configure ports

Requires the View/Manage Configuration access right

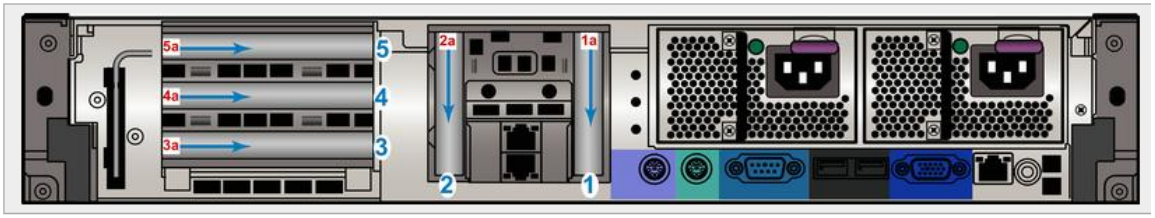
1. Click **Configuration > Virtual Devices** on the navigation pane.
2. Click **Toggle View Port Layout** in the MANAGE PORT CONFIGURATION section of the page to view a diagram of the back of your server, for reference during this procedure. The example below is an image of the DL380 G63U server.

MANAGE PORT CONFIGURATION

Name	Ports	Type
PCI Slot 01		RAID bus controller: Hewlett-Packard Company Smart Array Controller
PCI Slot 02		
PCI Slot 03		
PCI Slot 04	4a: virtual 4b: physical	Fibre Channel: QLogic Corp. ISP2312-based 2Gb Fibre Channel to PCI-X HBA
PCI Slot 05	5a: virtual 5b: physical	SCSI storage controller: Adaptec AHA-3960D / AIC-7899A U160/m

Submit Cancel

VIEW PORT LAYOUT



3. Configure each port that is used to attach SPHiNX to a host server. From the drop-down list for the port attached to the host server, select **virtual**.
4. Configure each port that is used to attach SPHiNX to an external storage device (tape drive, library, or disk array). From the drop-down list for the port attached to the device, select **physical**.
5. Click **Submit**.

6. When prompted, click **OK** to confirm that you want to reboot the server.
7. On the Reboot The System - Confirmation page, click **REBOOT**.
8. If one or more 2Gb Fibre Channel ports on the SPHiNX server are connected directly to an IBM i host server, the host server may not be able to discover virtual devices on the port(s). To force the host server to discover the virtual devices, you can set the **2Gb FC Direct Connect ports** option. (This parameter is not used for the 1Gb or 4Gb Fibre Channel ports.)
    a. For each port that is connected directly to the host server, note the port number(s) in the VIRTUAL TAPE DRIVES or VIRTUAL TAPE LIBRARIES section of the Configure Virtual Devices page.
    b. Click **Configuration > System** on the navigation pane of the SPHiNX interface.
    c. Click **Edit Configuration**.
    d. Expand the **Miscellaneous parameters** section of the page.
    e. Set the **2Gb FC Direct Connect port** option to the port number noted in step a. If multiple ports are directly connected, separate the port numbers using commas. Example: 1a,3b,4a
    f. Click **Apply**.
    g. Expand the **Configuration File** section of the page and then click **Save Changes**.
    h. Restart the TapeServer process. Click **Administration > System Tasks** on the navigation pane, click **Stop TapeServer** (under Processes), and then click **Start TapeServer**.

If problems arise:

- Make sure there are no bus conflicts with a physical drive or library on a virtual port or with a host server on a virtual port.
- Note that you can set the mode of supported HBAs only.

5 Creating and Managing VTLs and VTDs

After SPHiNX is deployed, you can create virtual tape libraries (VTLs). A VTL emulates the functionality of a tape library, which contains one or more tape drives, magazines that hold tape cartridges, a barcode reader to identify tape cartridges, and a media changer for loading and unloading tape cartridges. The virtual changers move virtual cartridges to and from virtual tape drives (VTDs) as instructed by standard host software, backup management applications, and utilities.

If applicable, a VTL can accept these commands from multiple hosts over Fibre Channel.

Note If multiple host servers will share a VTL, ensure that each host server's operating system supports device sharing, such as through the use of reservations.

If necessary, you can add a vault for VTL and VTD storage as described in "Adding vaults on external storage devices" on page 26.

You can also create standalone VTDs.

It is recommended that you back up the SPHiNX database before and after modifying the SPHiNX configuration. See "Backing up the SPHiNX server" on page 149 for more information.

This chapter describes how to create and modify VTLs and standalone VTDs.

Managing VTLs

A virtual tape library (VTL) emulates the functionality of a physical tape library, which contains tape drives, magazines that hold tape cartridges, a barcode reader to identify tapes, and a SCSI media changer for loading and unloading tape cartridges. The VTL's virtual changer moves virtual tapes to and from virtual tape drives (VTDs) as instructed by standard host software, backup management applications, and utilities. A VTL can accept these commands from multiple hosts over Fibre Channel.

Note IPL is not supported from a VTL; you must create a standalone VTD to IPL to an IBM iSeries host.

The Configure Virtual Devices page enables you to create and modify VTLs. The Manage Virtual Tapes page enables you to manage the virtual tapes in VTLs.

Creating a VTL

When you create a VTL, the following are also created:

- The specified number of virtual tape drives (VTDs)
- One virtual tape magazine (VTM), which defines the list of virtual tapes that are present in the VTL

A naming convention is used when the components of the VTL are created. The VTL name is specified by the user. All other names are automatically assigned by SPHiNX.

Example

If the following are specified when creating the VTL:

- VTL name: **1vtl_25**
- Number of slots: **287**
- Number of drives (VTDs): **2**

The following names are used for the VTL components:

- VTL name: **1vtl_25**
- VTD names: **1vtl_25_1** and **1vtl_25_2**

If a naming conflict occurs when SPHiNX tries to create the VTL components, a message is displayed on the Configure Virtual Devices page. You must then manually create the components.

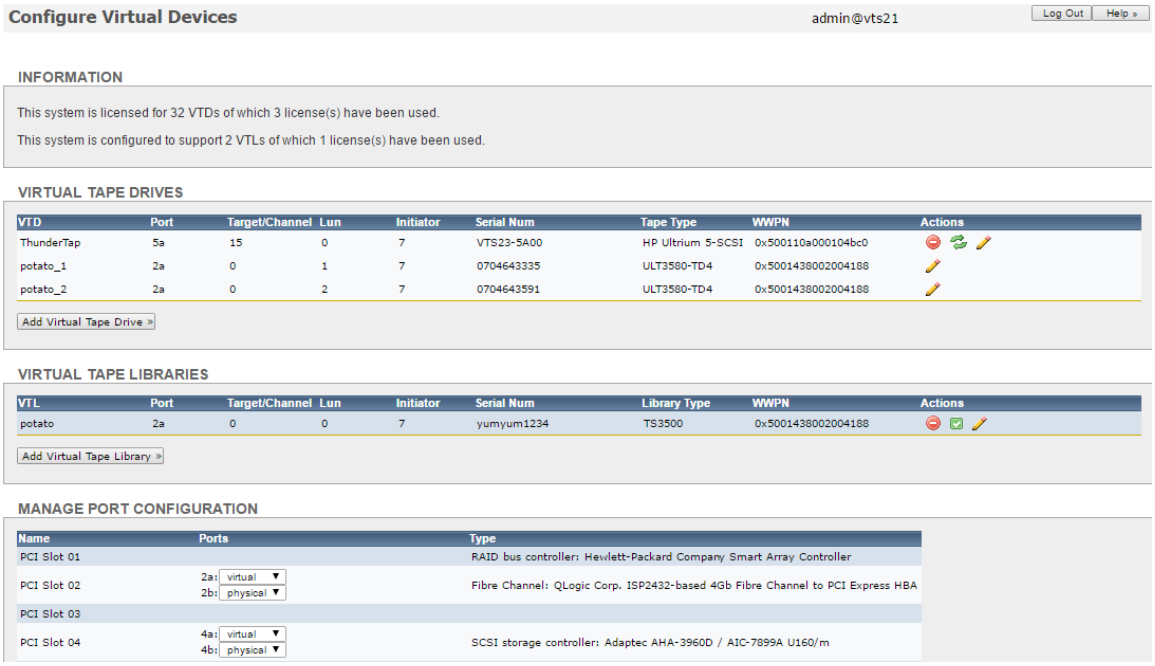
You must manually create pools and virtual tapes to populate the VTL and VTDs. To create virtual tapes and add them to the VTL, see Adding a virtual tape to a VTL.

Before beginning:

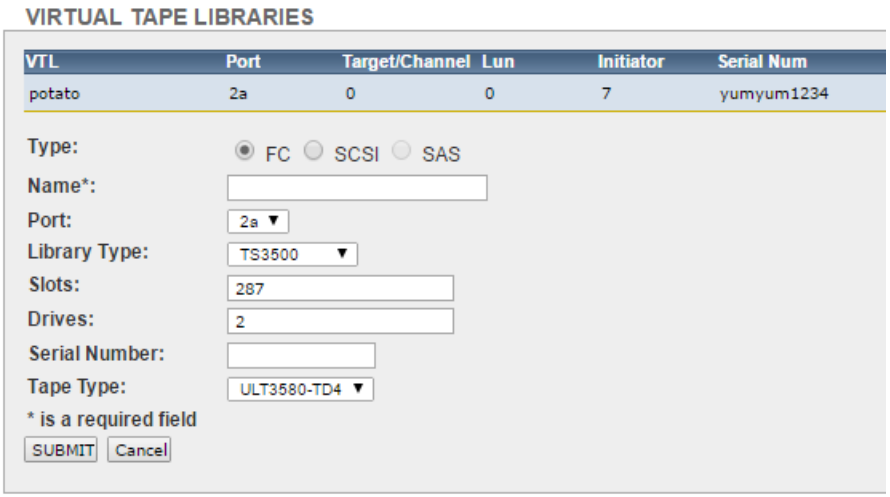
- VTL licenses are provided as part of the capacity license. Enable licensing as described in Enabling Licensed Features, if necessary.
- Verify that a vault is available for storing data; you must select a vault during VTL creation. Customer data should not be stored on VAULT00, which provides a small amount of space needed for system maintenance. If VAULT00 is the only vault available, it is recommended that you attach an external storage device for use in storing data. See the *Quick Start Guide* for cabling instructions and then refer to "Adding vaults on external storage devices" on page 26 the vaults chapter of the *Configuration Guide* for configuration details.

To create a virtual tape library:

1. If necessary, log in to the web interface.
2. Click **Configuration > Virtual Devices** on the navigation pane. The following page is displayed:



3. Click **Add Virtual Tape Library** in the VIRTUAL TAPE LIBRARIES section of the page. The following is displayed:



4. Select the **Type** option that corresponds to the connection type of the port (Fibre Channel or SCSI) to which the host is connected.

   Note SPHiNX assigns ID 6 to the SCSI cards because SPHiNX acts as a SCSI target for virtual devices. Using ID 6 instead of 7, which is the industry standard, avoids SCSI ID conflicts with SCSI hosts. You may need to modify settings on the host server or attached physical devices accordingly.

5. In the **Name** field, specify a name for the VTL. This name is for use in the interface only; it is not presented to the host.

   Note Be sure to specify a unique name for the VTL. If multiple VTLs are created with same first three characters in the name, a naming conflict may occur when SPHiNX attempts to create the VTDs.

6. From the **Port** drop-down list, select the port ID to which the host is connected.

   Note The port must be set to virtual, and only one VTL can be assigned to a port.

7. Select the type of library that the VTL will emulate from the **Library Type** drop-down list.
   - For Fibre Channel VTLs, the TS3500, MSL6000, and HPE MSL G3 options are provided by SPHiNX.
   - For SAS VTLs, the TS3100, TS3500, MSL6000, and HPE MSL G3 options are provided.

   The Slots and Drives fields are populated based on the selected library type, and the library type determines the tape types for the VTDs.

8. In the **Slots** field, specify the number of slots to create in the VTL. This also determines the number of virtual tapes created. Up to 999 slots can be created (depending on library type; the MSL6000 supports up to 416 slots).

   Note If you change the number of slots, a custom library type will be created when the VTL is created. This indicates that the VTL emulation deviates from the default (standard) library definition.

9. In the **Drives** field, specify the number of drives (VTDs) that will be created in the VTL.

   Note If you change the number of drives, a custom library type will be created when the VTL is created. This indicates that the VTL emulation deviates from the default (standard) library definition.

10. In the **Serial Number** field, specify the serial number of your virtual library. You may want to verify that the host server will recognize and accept the specified serial number. If you do not specify a serial number, it is automatically generated.

11. Select the drive type for the virtual tapes from the **Tape Type** drop-down list. Only tape types supported by the chosen library type are displayed.

12. Click **Submit** to create the VTL.

The VTDs are listed in the VIRTUAL TAPE DRIVES section of the Configure Virtual Devices page. Be sure that no errors are displayed on the web interface, and if problems arise, verify vault permissions.

After creating a VTL, you should:

- create pools, which organize and set properties on all tapes in a pool
- add virtual tapes to the pools
- insert virtual tapes into the VTL

See "Managing virtual tapes" on page 97 for more information.

Managing and using VTLs

You can perform the following to manage and use VTLs in your environment:

- Modify VTLs, including adding and removing slots and VTDs
- Modify VTDs in a VTL
- Manage virtual tapes in a VTL, including inserting and replacing virtual tapes
- Delete VTLs

These procedures are provided in the help, which can be viewed by clicking the **Help** button at the top of any page.

To view a list of VTLs

Click **Configuration > Virtual Devices** on the navigation pane.

- VIRTUAL TAPE DRIVES section – Lists the VTDs (standalone and those in VTLs) on the server. The VTD names that are associated with VTLs are similar to the VTL names.
- VIRTUAL TAPE LIBRARIES section – Lists all VTLs on the server. Here is an explanation of the columns in the section:
    - VTL - The name of the VTL.
    - Port - The port to which the host server is connected.
    - Target/Channel - The SCSI ID on which the VTL will respond.
    - Lun - The logical unit number, which identifies the sub-ID on the port (bus).
    - Initiator - The SCSI ID of the host port to which SPHiNX is connected.
    - Serial Num - The serial number of the VTL.
    - Library Type - The type of library that the VTL emulates.
    - WWPN - The World Wide Port Name, which uniquely identifies a port on the device (for Fibre Channel only).
    - Actions - The possible actions are: Delete Library Connection / Disable Virtual Device / Edit Library Connection

To view the contents of VTLs

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. From the **Show Cartridges In** list, select an option:
    - To view virtual tapes on the shelf only, select Shelf from the Show Cartridges In drop-down list.
    - To view virtual tapes in a VTL, select the VTL name from the Show Cartridges In drop-down list. VTL details are displayed at the top of the page and its virtual tapes are listed in the table.
    - To view all virtual tapes in all VTLs and on the shelf, select All from the Show Cartridges In drop-down list.
    - To view virtual tapes in a pool, select All from the Show Cartridges In drop-down list and then select the pool name from the Filter By Pool drop-down list.

The VTL properties are displayed at the top of the page and the virtual tapes in the VTL are listed.

Managing standalone VTDs

A standalone virtual tape drive (VTD) emulates the behavior of a physical tape drive. The Configure Virtual Devices page enables you to create and modify VTDs. The Virtual Media - Operation page enables you to view the contents of VTDs.Up to 32 VTDs are supported per SPHiNX server. Your licensing determines how many VTDs you can create.

Note If you need to IPL to an IBM iSeries host, you must create a standalone VTD; you cannot IPL from a VTL.

You can create standalone VTDs, and then you can modify or delete VTDs as needed.

Creating a standalone VTD

The following table describes the properties that you must set when defining a standalone VTD. For each property, this table provides a description and whether each property is presented to the host server when SPHiNX responds to a host's query:

Property	Description	Presented to Host?
Name	A user-friendly name for the VTD.	Yes
Tape type	The type of tape that the VTD emulates.	Yes
Port ID	The ID of the port on the SPHiNX server to which the host is connected. This ID is not presented directly to the host; the host will see this port numbered according to its numbering scheme. If the connection is over Fibre Channel, the port ID is associated with a port WWN that is used by the host to identify the SPHiNX server. If the connection is over SCSI, the port ID on the SPHiNX server has no significance to the host.	Indirectly
Target ID	The SCSI ID on which the VTD responds. This ID is not presented to the host if the connection is over Fibre Channel.	Yes, for SCSI only
Logical unit number (LUN)	The sub-ID on the port. This ID is used by the host for SCSI and Fibre Channel connections.	Yes
Serial number	The serial number or other string describing the VTD. Only alphanumeric characters should be used (10-digit numeric serial numbers are required for IBM i hosts).	Yes

The port ID, target ID, LUN, and initiator ID (not shown) are collectively referred to as the PTLI. The PTLI enables the host server to precisely identify the VTD; it provides an exact address of the VTD on the port. Remember that the host is connected to SPHiNX by a single cable. The PTLI thereby enables you to multiplex the cable to identify multiple VTDs over a single cable (for Fibre Channel VTDs).

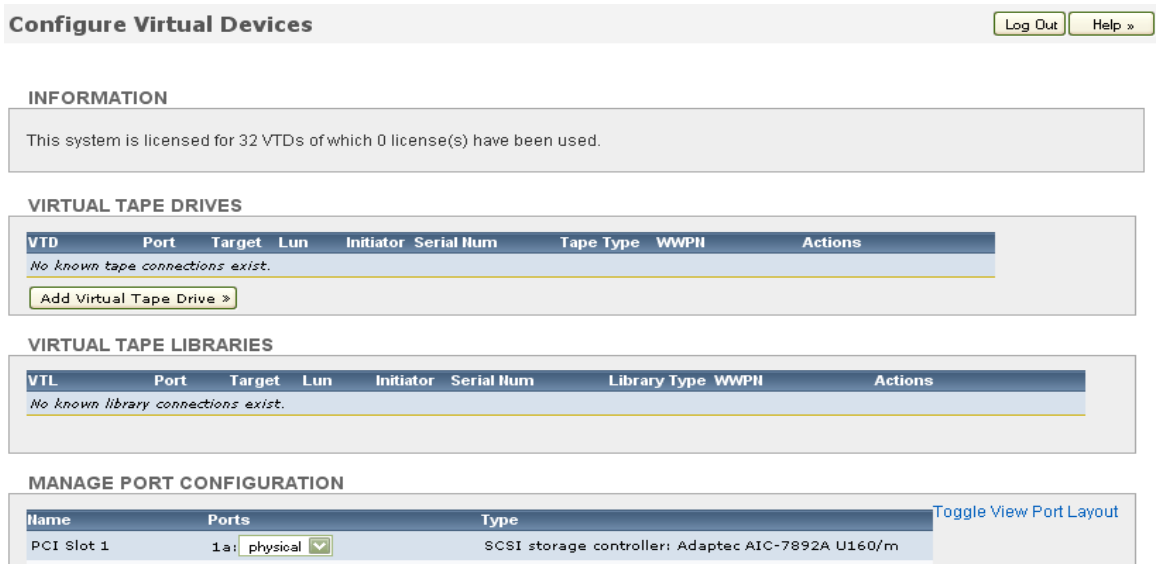
Before beginning:

- Enable Managed Capacity or VTD licensing as described in Enabling Licensed Features, if necessary.
- Verify that at least one port is set to Virtual (target) mode on the Configure Virtual Devices page. Ports should have been configured as described in Configuring Ports.
- You may want to stop VTDs that use the same port as the one you will create. Creating a VTD may interrupt the activities of other VTDs on the same port.
- Back up the SPHiNX database before modifying the SPHiNX configuration. See "Backing up the SPHiNX server" on page 149 for more information.

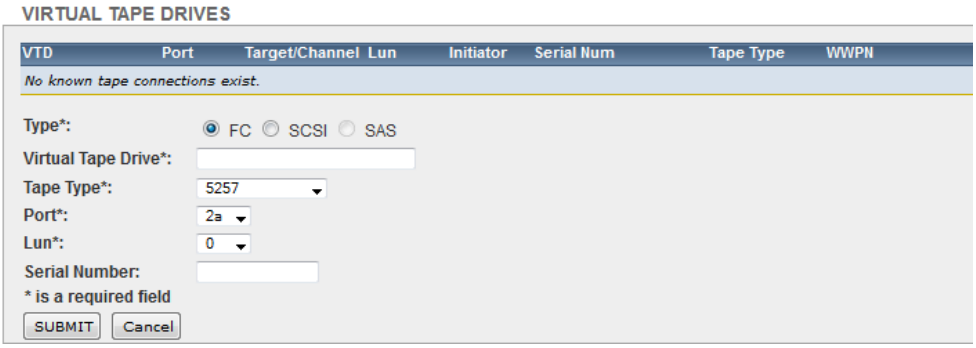
To create a VTD:

 *Requires the View/Manage Configuration access right*

1. If necessary, log in to the web interface as a user who has the View/Manage Configuration access right.
2. Click **Configuration > Virtual Devices** on the navigation pane. The following page is displayed:



3. Click **Add Virtual Tape Drive** in the VIRTUAL TAPE DRIVES section of the Configure Virtual Devices page. The following is displayed:



4. Select the connection type: **FC**, **SCSI**, or **SAS**.

   Note SPHiNX assigns ID 6 to the SCSI cards because SPHiNX acts as a SCSI target for virtual devices. Using ID 6 instead of 7, which is the industry standard, avoids SCSI ID conflicts with SCSI hosts. You may need to modify settings on the host server or attached physical devices accordingly.

5. In the **Virtual Tape Drive** field, specify a name for the VTD. This name is for use in the interface and by EMS, and it is presented to the host server. It is also noted in the configuration file. The name is case-sensitive.

6. Select the drive type from the **Tape Type** drop-down list. This property defines the type of tape drive that the VTD emulates.

7. From the **Port** drop-down list, select the ID of the port to which the host server is connected. This ID is not presented directly to the host; the host will see this port numbered according to its own numbering scheme. If the connection is over Fibre Channel, the port ID is associated with a port WWN that is used by the host to identify the SPHiNX server. If the connection is over SCSI, the port ID on the SPHiNX server has no significance to the host.

- If you are creating a SCSI VTD, select the ID on which the VTD will respond from the **Target** drop-down list. This is the ID that the host uses to identify its target. For SAS VTDs, set this value to 0.

  Note SCSI devices use target-based addressing. Fibre Channel devices use LUN-based addressing. For Fibre Channel devices, the LUN determines the unique address of the device on the port, so you cannot assign a LUN value more than once per port.

  The appropriate target ID value depends on the host server:

  NonStop G-series and S-series servers IDs 4 and 5 are reserved for tape devices, while other IDs are reserved for other device types. NonStop S servers default to target ID 5 for tape drives, therefore it is recommended that you set the target to 5. You can set the target to 4 but you must configure the NonStop S server by specifying "DEVICEID 4" with the SCF ADD TAPE command. (Refer to the NonStop S server documentation for more information.)

  NonStop Integrity (NS) and BladeSystem servers In general, you can assign values 0-15 to the target ID. (Integrity servers support Fibre Channel ports only.) Best practices encourage you to assign value 5 to the target ID.

  UNIX servers In general, any ID greater than 0 can be used for the target ID. The backup management application determines the ID and typically assigns 0 to the robot in a tape library. Refer to backup management application documentation and host server to determine the target ID.
  If the Fibre Channel is configured for the Arbitrated Loop topology, use the Loop ID as the target ID

here. To find the Loop ID, boot SPHiNX while connected to the Fibre Channel network. Then, after the startup is complete, access the SPHiNX web interface. Click **Support > Logs** on the navigation pane, click **Examine the system log file**, and search for "Loop id." The ID is typically set to 0 or 1 but it can be set as high as 255.

IBM i servers Check your current hardware and operating system documentation for supported target addresses.

Windows Server Values 0-15 are acceptable.

- NonStop G-series and S-series servers
  IDs 4 and 5 are reserved for tape devices, while other IDs are reserved for other device types. NonStop S servers default to target ID 5 for tape drives, therefore it is recommended that you set the target to 5. You can set the target to 4 but you must configure the NonStop S server by specifying "DEVICEID 4" with the SCF ADD TAPE command. (Refer to the NonStop S server documentation for more information.)
- NonStop Integrity (NS) and BladeSystem servers
  In general, you can assign values 0-15 to the target ID. (Integrity servers support Fibre Channel ports only.) Best practices encourage you to assign value 5 to the target ID.
- UNIX servers
  In general, any ID greater than 0 can be used for the target ID. The backup management application determines the ID and typically assigns 0 to the robot in a tape library. Refer to backup management application documentation and host server to determine the target ID.

  If the Fibre Channel is configured for the Arbitrated Loop topology, use the Loop ID as the target ID here. To find the Loop ID, boot SPHiNX while connected to the Fibre Channel network. Then, after the startup is complete, access the SPHiNX web interface. Click **Support > Logs** on the navigation pane, click **Examine the system log file**, and search for "Loop id." The ID is typically set to 0 or 1 but it can be set as high as 255.
- IBM i servers
  Check your current hardware and operating system documentation for supported target addresses.
- Windows Server
  Values 0-15 are acceptable.

8. From the **Lun** drop-down list, select the logical unit number. This number identifies the sub-ID on the port, and this ID typically ranges from 0-255. For SCSI connections, this ID is typically 0.

   Note SCSI devices use target-based addressing. Fibre Channel devices use LUN-based addressing. For Fibre Channel devices, the LUN determines the unique address of the device on the port, so you cannot assign a LUN value more than once per port.

   For Fibre Channel, the appropriate LUN value depends on the host server:

   NonStop G-series and S-series servers. Set the LUN to 0. 0 is the only value supported by NonStop S servers, which support SCSI ports only and ignore the LUN.

   NonStop Integrity (NS) and BladeSystem servers. Up to four tape devices are supported per port, therefore you can assign values 0-3 to the LUN. 0 is typically assigned to the LUN for the first tape device, 1 is typically assigned for the second tape device, 2 for the third, and 3 for the fourth.

UNIX servers. In general, set the LUN to any value between 0 and 7. Begin with 0 and increment the LUN for each additional VTD that is added on a port. The backup management application determines the ID. Refer to backup management application documentation and host server to determine the LUN.

Windows Server. Set the LUN to any value between 0 and 7. Begin with 0 and increment the LUN for each additional VTD that is added on a port. The backup management application determines the ID. Refer to backup management application documentation and host server to determine the LUN.

IBM i servers. LUN 0 is required. If more than one VTD is created, begin with 0 and increment the LUN for each additional VTD that is added on a port.

- NonStop G-series and S-series servers
  Set the LUN to 0. 0 is the only value supported by NonStop S servers, which support SCSI ports only and ignore the LUN.
- NonStop Integrity (NS) and BladeSystem servers
  Up to four tape devices are supported per port, therefore you can assign values 0-3 to the LUN. 0 is typically assigned to the LUN for the first tape device, 1 is typically assigned for the second tape device, 2 for the third, and 3 for the fourth.
- UNIX servers
  In general, set the LUN to any value between 0 and 7. Begin with 0 and increment the LUN for each additional VTD that is added on a port. The backup management application determines the ID. Refer to backup management application documentation and host server to determine the LUN.
- Windows Server
  Set the LUN to any value between 0 and 7. Begin with 0 and increment the LUN for each additional VTD that is added on a port. The backup management application determines the ID. Refer to backup management application documentation and host server to determine the LUN.
- IBM i servers
  LUN 0 is required. If more than one VTD is created, begin with 0 and increment the LUN for each additional VTD that is added on a port.

9. In the **Serial Number** field, specify the serial number of the VTD. You can specify up to 10 alphanumeric characters. On IBM i hosts, 10-digit numeric serial numbers are required (non-numeric characters are not allowed). This string is presented to the host and should be unique (across all SPHiNX servers and VTDs in the environment). If you do not specify a serial number, it is automatically generated.
10. Click **Submit**.

It is recommended that you back up the SPHiNX database after modifying the SPHiNX configuration. See "Backing up the SPHiNX server" on page 149 for more information.

After creating a VTD, you should:

- create virtual tapes
- create pools, which organize and set properties on the tapes
- mount a virtual tape in the VTD

See "Managing virtual tapes" on page 97 for more information.

Viewing standalone VTDs

To view standalone VTDs on the server:

Click **Configuration > Virtual Devices** on the navigation pane. A list of VTDs is provided in the VIRTUAL TAPE DRIVES section of the page. Here is an explanation of the columns:

- VTD - The name of the VTD.
- Port - The SPHiNX port to which the host server is connected.
- Target - The SCSI ID on which the VTD will respond.
- Lun - The logical unit number, which identifies the sub-ID on the port (bus).
- Initiator - The SCSI ID of the host port to which SPHiNX is connected.
- Serial Num - The serial number of the VTD.
- Tape Type - The type of tape drive that the VTD emulates.
- WWPN - The World Wide Port Name, which uniquely identifies a port on the device.

Note To identify VTDs in VTLs, note the name of the VTD; it is similar to the name of its associated VTL. Also, you cannot delete VTDs that are associated with a VTL.

To view all VTDs from the Manage Drives page

Click **Administration > Virtual Drives** on the navigation pane. The Manage Drives page is displayed.

Here is a description of the columns on this page:

- Drive - The name of the drive (VTD).
- Cartridge Name - The name (or barcode) of the virtual tape that is currently loaded in the drive.
- Pool - The pool that contains the virtual tape.
- Vault - The vault that contains the pool.
- Actions - The allowed actions to be preformed on that specific drive.

The page is not updated in real-time. Click **Refresh Drives** to update the page.

7 Enabling and Performing Tape-to-tape Exports

You can export data on a virtual tape to a physical tape in an external tape drive or library. This provides a one-to-one mapping of virtual to physical tape. When creating the tape-to-tape export job, you can choose whether the data remains in virtual tape format or host format. This allows application-aware exports because you have the ability to name the virtual tapes such that they are the same as a pool of physical tape cartridges. This then ensures that DR reports created by backup applications are accurate when a virtual tape has been written to physical tape.

Note You can also export a virtual tape to physical tape using a stacked export job, though this requires backup management application integration. See "Enabling and Performing Stacked Exports" on page 51 for more information.

Steps to enable, configure, and use tape-to-tape exports

1. Connect the tape drive or library to SPHiNX. Refer to the *Quick Start Guide* for cabling instructions.

   Note By default, the SPHiNX port that is used to connect to the drive or library is set to physical (to support external devices).

2. If you want data to be compressed during export, verify that compression is enabled on the target drive.

3. Configure the physical drive or library for use with tape-to-tape export jobs. You can also configure SPHiNX to export encrypted data, if Data Encryption is licensed and all drives in the library support encryption.

4. Format and label a cartridge so that its label matches the barcode of the virtual tape you will export. Also, ensure that a cartridge is loaded in the external tape drive or library.

5. If you want to send email notifications for completed or failed jobs, configure SMTP settings as described in the help.

6. If exporting a tape to a drive (if Tape-to-Tape to Drive was selected on the Manage Physical Devices page), you must manually mount the tape cartridge before exporting the virtual tape. (Do not manually mount a cartridge if Tape-to-Tape to Library was selected; the library will mount the cartridge.)

7. Export virtual tapes by creating tape-to-tape export jobs using the web interface. If necessary, you can also import exported tapes.

Considerations

- To encrypt data that is exported:
  - Enable Data Encryption and select an encrypted virtual tape for tape-to-tape export (in virtual tape format). The tape is exported as-is if the target library supports encryption on all

of its drives.

- Enable drive-level encryption and export an unencrypted virtual tape using virtual tape format.

If you choose to export an encrypted tape in host format, the tape is decrypted before it is exported.

- When a tape-to-tape export job completes, the tape is rewound and ejected from the drive.
- SPHiNX cannot export virtual tapes with barcodes that include more than six characters. If you attempt to export a tape with an eight -character barcode (which includes a two-character density, such as L4 or L5), SPHiNX truncates the barcode, using only the first six characters.
- The tape-to-tape export job will fail:
  - If the SPHiNX server is rebooted while a tape-to-tape export job is in progress
  - If a virtual tape does not reside in a VTL and the virtual tape is locked at the time of the export
  - If the library is moved to a different port; you can manually discover the library using rescan-scsi-bus.sh
  - If a physical cartridge with a matching barcode is not found in the library (the job.log will state “No tape in the library that has a barcode of *barcode*”)
  - If the cartridge reached "End of Life" date or it is write-protected
  - If the virtual tape is mounted or locked
  - If the connection to the physical tape is disrupted; this may require a reboot of SPHiNX
  - If the export is too big to fit on the physical tape; SPHiNX will not span tapes
- To restore a virtual tape that was exported by a tape-to-tape export job, you can import the virtual tape using the Manage External Data page of the web interface. This restores the virtual tape to SPHiNX so that a host server can then use the tape. Refer to the help for importing instructions.

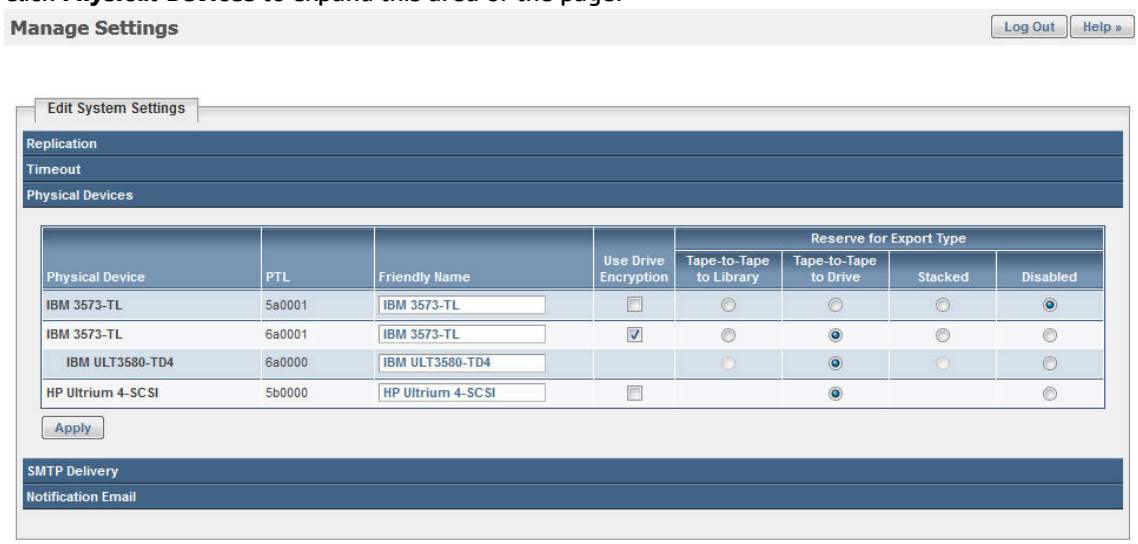
Configuring the physical drive or library

After attaching a physical drive or library to SPHiNX but before creating a tape-to-tape export job, you must assign a user-friendly name to a drive or library, and then you must dedicate a drive or library for tape-to-tape exports.

To assign a user-friendly name to a physical library or drive

Requires the System Maintenance Functions and View/Manage Configuration access rights

1. Click **Configuration > System** on the navigation pane.
2. Click **Edit System Settings**.
3. Click **Physical Devices** to expand this area of the page.



4. To specify a user-friendly name or short description of the drive or library, type a name in a drive or library's **Friendly Name** column. This name will be used when selecting a drive or library on other pages in the web interface.

5. Click **Apply**.

To assign a user-friendly name to a physical library or drive

1. Click **Configuration** > **System** on the navigation pane.
2. Click **Edit System Setting**s.
3. Click **Physical Devices** to expand this area of the page.
4. To dedicate a library for use by tape-to-tape jobs, seclect **Tape-to-Tape to Library** option for the library. The library mounts the tape cartrige as needed.

   Note: After selecting this option, you cannot select individual drives in the library during job creation. Also, if you manually mount the cartrige, the tape-to-tape export job will fail.

5. To dedicate a drive for use by tape-to-tape jobs, select the **Tape-to-Tape to Drive** option for the drive. The drive is then available for selction during job creation, and you must manually mount the tape cartrige in the library or drive before running the tape-to-tape export job.
6. Click **Apply**.

Exporting a virtual tape or pool

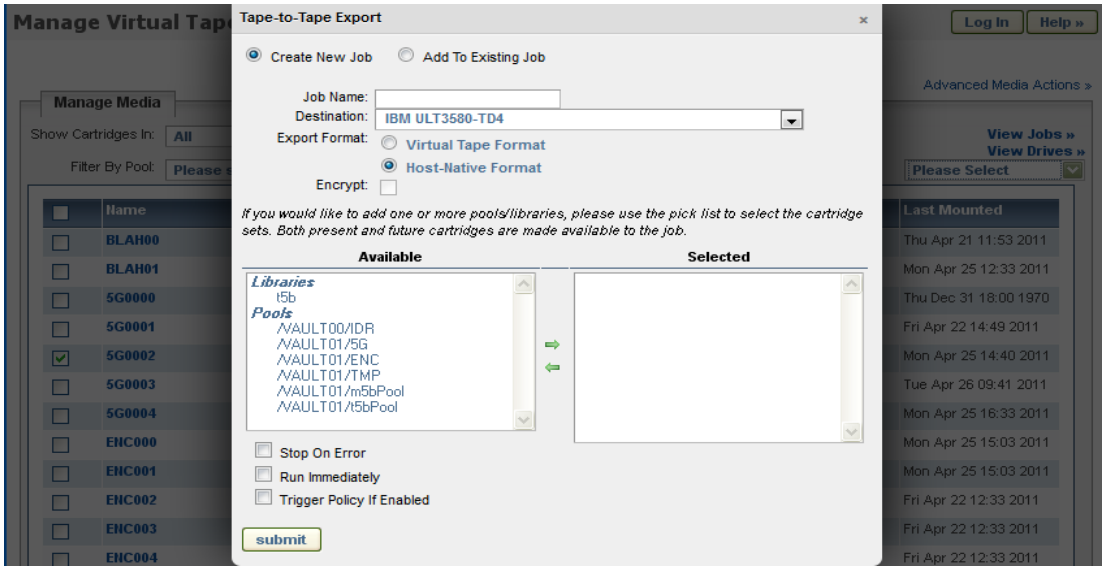
You can export one virtual tape to one physical tape using a tape-to-tape export job, and you can choose whether the data remains in virtual tape format or host format.

To export a virtual tape or pool

Requires the Virtual Tape Import and Export, Vault Access, and Access to all Vaults access rights

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Select **All**, **Shelf**, or a VTL name from the **Show Cartridges In** drop-down list.
3. Choose one or more virtual tapes to export. (In a later step, you can also choose virtual tapes in VTLs or pools.)

   Note If the physical cartridge's label does not match the barcode of the virtual tape to export, another virtual tape may be overwritten if the data is imported from the cartridge. For example, if virtual tape 00000 is written to physical tape 00001, data will be written to virtual tape 00001 when the physical tape is imported. Therefore, before exporting, be sure that the physical tape's label matches the virtual tape's barcode.
4. Select **Tape-to-Tape Export** from the Please Select drop-down list above the table, on the right side of the page. The following is displayed:



5. On the pop-up dialog, select the **Create New Job** option.
6. Specify a job name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed.

7. Select a drive or library from the **Destination** drop-down list.

   Note Disconnected tape drives or libraries can be selected, though the job will fail if the drive or library remains disconnected when the job runs.

8. Select an **Export Format** option:
   - If you choose **Virtual Tape Format**, the tape is exported as-is and cannot be read by the host server. If the virtual tape is encrypted, SPHiNX is enabled for drive-level encryption, and all drives in the target library support encryption, the tape remains encrypted when it is exported.
   - If you choose **Host-Native Format**, the tape is exported in a format that can be used by the host server. If the virtual tape is encrypted, the tape is decrypted before it is exported in host-native format.

9. If Virtual Tape Format is selected and drive-level encryption is enabled, you can select the **Encrypt** option to encrypt the virtual tape when it is written to physical tape.

10. To choose virtual tapes or pools to export or replicate (in addition to those selected on the Manage Virtual Tapes page), move tapes or pools from the **Available** list to the **Selected** list. Or, remove tapes or pools by moving them from the **Selected** list to the **Available** list. Use the  and  buttons to move items to and from the lists.

11. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to export all virtual tapes.

12. Select the **Run Immediately** option to run the job immediately after it is created. Do not select this option if you want to create a schedule for the job.

13. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.

14. Click **submit**.

15. To schedule the tape-to-tape export job, create a schedule that is associated with the job.
    a. Click **Administration > Jobs** on the navigation pane.

    b. On the Manage Jobs page, click  next to the job you want to schedule. The Manage Schedules page is displayed.

    c. Click **Add Schedule**.

    d. In the Create Schedule area, select how often you want the job to occur:
       - One time — Runs the job once. You must select a start date and time.
       - Weekly/Daily — Runs on the days you select. You must select the days and a start date and time.
       - Monthly — Runs on a specific date each month. Select a date and start time.

       If you specify a date that does not exist in a month, the job will run on the last day of the month.

    e. Click **Save**.

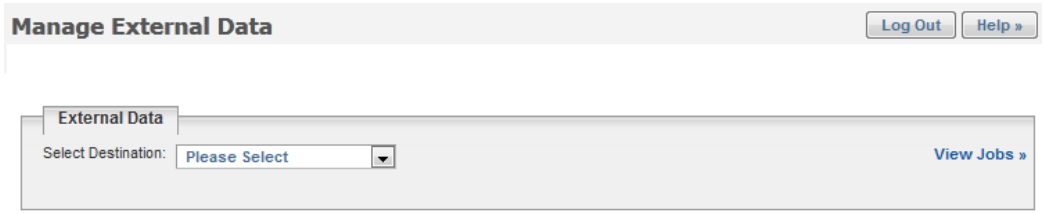
    After the job runs, you can return to the Managed Schedules page for its status. If a problem occurred, the Last Run column will display “Failed”.

Importing data from a physical library or drive

To import data from an external tape device

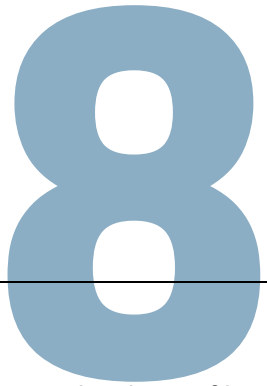
Requires the Virtual Tape Import and Export, Vault Access, and Access to all Vaults access rights

1. Click **Administration > External Data** on the navigation pane.



2. If necessary, log in using an account that has the access rights listed above. Click the **Log In** button at the top of the page and enter a username and password.
3. If necessary, log in using an account that has the Virtual Tape Import and Export, Vault Access, and Access to all Vaults access rights. Click the **Log In** button at the top of the page and enter the credentials to log in.
4. From the **Select Destination** drop-down list, select the library or drive from which the data or tape will be imported. (For a description of the columns that are displayed, see Managing external data.)
5. To name the restore job, enter a name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed. (A name is generated if you do not specify one.)
6. If you wish to stop the import operation if an error occurs, select **Stop on Error** (above the table). If an error occurs, the import job fails. If you do not select this option, the import operation will skip tapes that caused an error and finish importing the selected tapes.
   Note If an import fails, tapes that were imported before the failure are not "rolled back". They remain imported.
7. Select one or more tapes to import from the list. You can also select all tapes by selecting the check-box in the table header.
8. If importing from a pre-existing tape (that was not written to by SPHiNX), select the virtual tape where the imported data will be stored from drop-down list in the **Source Vault/Pool** column.
9. Select **Import** from the drop-down list above the table on the right side of the page.
10. When prompted, confirm that you want to import the tape(s). A library import job is created and run immediately.

Enabling and Performing Stacked Exports



Through integration with a backup management application (BMA) server, you can read and write files to and from SPHiNX (SPHiNX). You can create stacked export jobs on SPHiNX to export, or “migrate”, virtual tapes to physical tapes using an attached external tape device. The entire virtual tape is exported, and a virtual tape may span multiple physical tapes. Stacked exports allow for better use of the disk space on the storage array. For instance, if a virtual tape needs to be saved for seven years for legal purposes, you could automatically export the virtual tape to physical tape. In the unlikely event that the virtual tape is needed, SPHiNX can restore it from physical tape.

Note To install IBM Tivoli Storage Manager (TSM) on the SPHiNX server you need to purchase a license through your Sales Represenative.

When a virtual tape is exported to physical tape, all data on the virtual tape is written to physical tape, including the header information (metadata). To restore a virtual tape that was exported, the tape must first be restored on SPHiNX before restoring it on the host server. Host servers cannot read physical tapes that were created through stacked exports because the tape is formatted for use by SPHiNX only. After the data is restored as a virtual tape in SPHiNX, the host server can then restore the data.

Note You can also export a virtual tape to physical tape using a tape-to-tape export job, which does not require backup management application integration. See "Enabling and Performing Tape-to-tape Exports" on page 45 for more information.

If Scan/Cleanup is enabled, you can configure SPHiNX to automatically erase virtual tapes after they are exported to tape by a stacked export job. See "Enabling and Configuring Scan/Cleanup" on page 115 for more information about enabling and configuring Scan/Cleanup.

Steps to enable, configure, and use stacked exports

1. Connect the library or drive to SPHiNX. Refer to the *Quick Start Guide* for cabling instructions.
2. Configure the BMA that will perform stacked export operations. Refer to the Release Notes to find out if your Sphinx model comes with the BMA.
3. If using a NonStop host server, configure the Event Management Service (EMS) on SPHiNX as described in Configuring EMS Communication.
4. If using a BMA other than TSM that is installed on the SPHiNX server, configure a system account for use by the BMA as described in this chapter, so that it can communicate with SPHiNX and perform stacked exports.
5. Insert labeled tapes into the tape drive(s). Tapes should be labeled to match the barcode.
6. Export virtual tapes by creating stacked export jobs using the web interface as described in this chapter. If necessary, you can also import exported tapes.

This chapter provides information for performing the steps above unless another document is cited.

Considerations

- If Data Encryption is enabled and an encrypted virtual tape is selected for stacked export, the tape is exported as-is. That is, the data remains encrypted when it is exported to physical tape.
- If Scan/Cleanup is enabled, you can configure SPHiNX to automatically erase virtual tapes after they are exported or after their retention periods expire. Refer to the *Configuration Guide* for more information about Scan/Cleanup.
- If a virtual tape does not reside in a VTL, the stacked export job will fail if the virtual tape is locked at the time of the export.
- If a stacked export job fails, you may need to
  - Remove old media from the library and mark as scratch
  - Increase the storage pool
  - Verify the TSM password and login
- To restore a virtual tape that was exported by a stacked export job, you can import the virtual tape using the UnMigrate button on the **Virtual Media - Operation** page of the web interface: **Administration** > **Virtual Tapes** > **Advanced Media Actions**. This restores the virtual tape to SPHiNX so that a host server can then use the tape. Refer to the help for importing instructions.

Configuring IBM Tivoli Storage Manager on SPHiNX

If you intend to use TSM, you must configure first SPHiNX to use TSM and then configure TSM to use a library that is attached after initial configuration.

After completing the steps in this section, refer to the Administration > Managing the TSM Library section of the online help for additional information that you will find useful after configuring TSM.

To configure TSM on the SPHiNX server

Note During configuration, if you are using an IBM library or IBM drive, you may receive an email notification stating that devices have been disconnected or connected. You can ignore this notification.

1. If you are using a SCSI library, you must enable SAN discovery for TSM as follows:
   a. On the SPHiNX system, open the **/opt/tivoli/tsm/server/bin/dsmserv.opt** file for editing. Here is an example of the file:

```
*** IBM TSM Server options file
*** Refer to dsmserv.opt.smp for other options
COMMMETHOD TCPIP
TCPPORT 1500
DEVCONFIG devcnfg.out
VOLUMEHISTORY volhistory.out
```

   b. Add the following line to the end of this file:

```
SANDISCOVERY PASSIVE
```

   c. Save and close the file.

2. Configure SPHiNX to use TSM:
    a. Log in to the web interface.
    b. Click **Configuration > System** on the navigation pane.
    c. Click **Edit Configuration**.
    d. Expand the **Backup Management Application (BMA)** section of the page.
    e. Select **Tivoli Storage Manager** from the **BMA to use** drop-down list and then click **Apply**.
    f. Expand the **Configuration File** section of the page and then click **Save Changes**.
3. Perform initial configuration of TSM:
    a. Log in to the SPHiNX server from the command line.
    b. Become root:

        ```
        su -
        ```

    c. Enter the following command to initialize TSM:

        ```
        bmaconfig -c tsm
        ```

        Here is an example of the output:

        ```
        BMACONFIG starting.
        set_hsm_pswd: set v-30000D
        doing initial TSM configuration ...
        dsmserv lic file built ...
        TSM licenses installed ...
        dsmserv.opt setup ...
        dsmserv config file built ...
        dsmserv configured ...
        enable tivoli logging: true
        Tivoli TSM logging enabled ...
        Status of dsmserv: stopped
        Status of dsmserv: running
        TSM service started ...
        file dsm.sys setup ...
        file dsm.opt setup ...
        VTS Configuration file setup ...
        TSM activity log management setup ...
        (If the BMA prompts for user id, enter 'admin', and subsequently
        admin's password.)
        ```

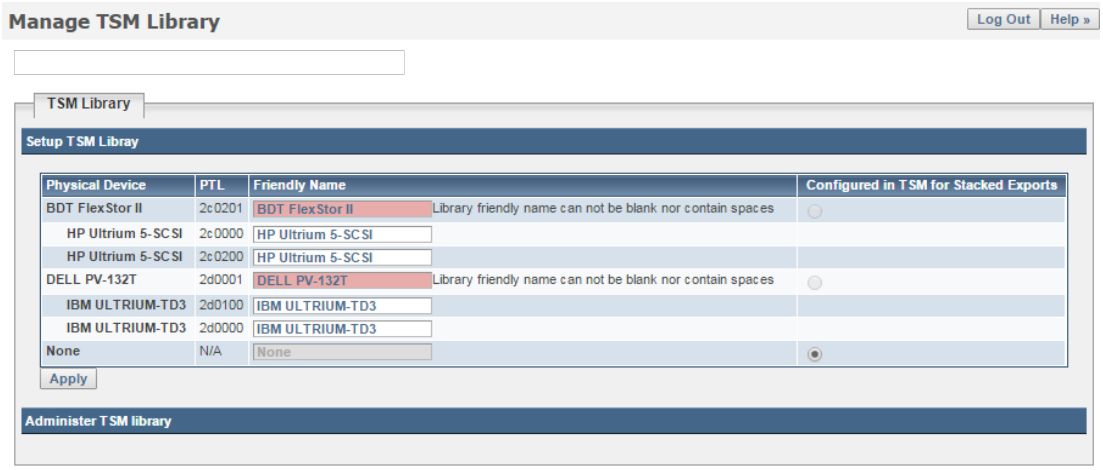
    d. When prompted, enter **admin** as the user ID and then enter the password, which is ***v-serial#_in_reverse*** (such as v-7500D if the serial number is D0057). The serial number of your appliance is available on the System Status page.

        Here is an example of the output that is displayed:

        ```
        IBM Tivoli Storage Manager
        Command Line Backup/Archive Client Interface
           Client Version 5, Release 5, Level 2.7
           Client date/time: 10/15/15   10:22:03
        ```

```
(c) Copyright by IBM Corporation and other(s) 1990, 2009. All
Rights Reserved.

Node Name: VTS31
Session established with server VTS31: Linux/x86_64
   Server Version 5, Release 5, Level 5.2
   Server date/time: 10/15/15   10:22:03  Last access: 10/15/15
10:22:03

TSM Server Connection Information

Server Name.............: VTS31
Server Type.............: Linux/x86_64
Archive Retain Protect..: "No"
Server Version..........: Ver. 5, Rel. 5, Lev. 5.2
Last Access Date........: 10/15/15   10:22:03
Delete Backup Files.....: "No"
Delete Archive Files....: "Yes"

Node Name...............: VTS31
User Name...............: root

  99 char cmdline =/opt/tivoli/tsm/client/ba/bin/dsmadmc -
id=admin -pa=* 'update node * PASSExp=0 MAXNUMMP=250'
IBM Tivoli Storage Manager
Command Line Administrative Interface - Version 5, Release 5,
Level 2.7
(c) Copyright by IBM Corporation and other(s) 1990, 2009. All
Rights Reserved.

Session established with server VTS31: Linux/x86_64
   Server Version 5, Release 5, Level 5.2
   Server date/time: 10/15/15   10:23:31  Last access: 10/15/15
10:22:03

ANS8000I Server command: 'update node * PASSExp=0 MAXNUMMP=250'
ANR2063I Node CLIENT updated.
ANR2063I Node VTS31 updated.

ANS8002I Highest return code was 0.
```

4. Configure TSM to use the physical library and drives, complete these steps:
   a. Click **Administration > TSM Library** on the navigation pane. All libraries that are attached to SPHiNX are listed on the Manage TSM Library page.



Note If your library is connected but not listed, check connections to the appliance and library or restart the TapeServer service.

b. If a library's friendly name is not valid because it contains a space or is blank, it is highlighted red. You must edit the name in the **Friendly Name** field (but do not press Enter).

c. Select the library to use for stacked exports by clicking on its radio button in the **Configured in TSM for Stacked Exports** column.

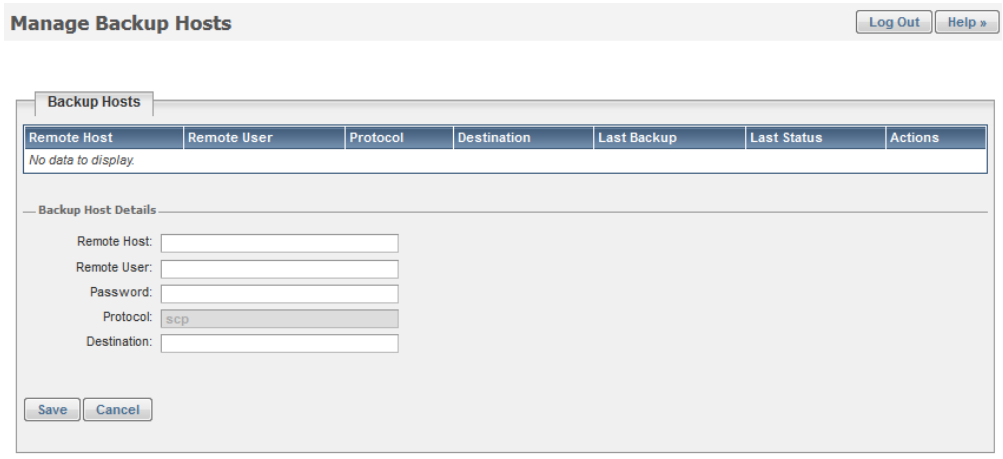
d. Click **Apply**.

5. Create a database backup host, which is a remote host that will be used to backup the stacked-export database. This ensures that you can restore exported tapes in the event of a system failure.

6. a. Click **Configuration > System** on the navigation pane.

b. Click **Manage Backup Hosts**.

c. Click the **Add Backup Host** button. The following is displayed:



d. In the **Remote Host** field, type the hostname or IP address of a server that SPHiNX will use as a backup host.

e. In the **Remote User** field, type the username of a user account that can access the SCP program on the specified server.

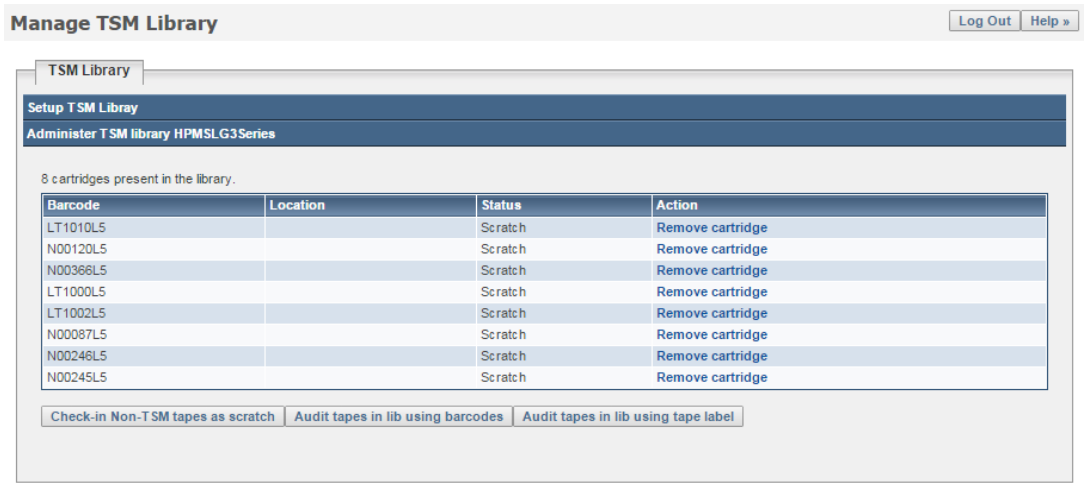
f. Type the password of the user account in the **Password** field.

g. In the **Destination** field, type a path and file name where SPHiNX will store the database files. The file is archived and compressed (using gzip), though no extension is added if a file name is specified. If you do not specify a fully qualified path, the file is stored in the specified user's home directory. Example: /home/bill/tsmbackupfile

h. Click **Save**.

7. Check in tapes for use by stacked export jobs:
   a. Insert one or more tapes into the library, if necessary. To do this, add the physical tape to the I/O slot in the physical library and then move the tape from the I/O slot into a regular slot using the library's control panel.

   b. Check one or more tapes in by clicking **Administration > TSM Library** on the navigation pane and then expanding the **Administer TSM Library** section of the page. Here is an example of the page:



   Perform one of these steps:

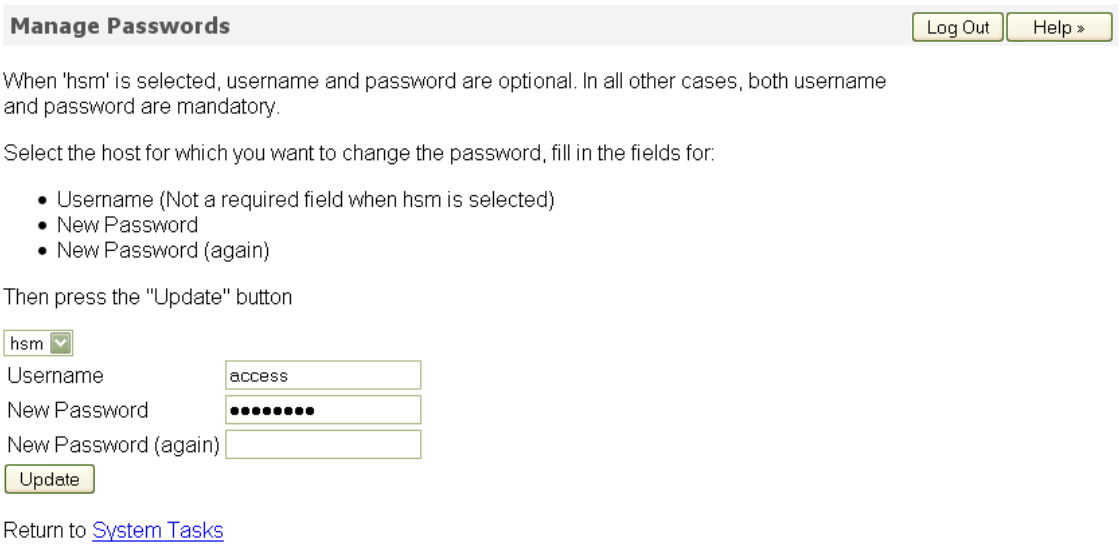
   - If a tape was inserted that had been used previously for a stacked export, click **Remove cartridge** (in the Action column) for each tape you want to use
   - If adding a scratch tape, click **Add cartridge** next to the tape
   - To add all scratch tapes listed on the page, click the **Check-in Non-TSM tapes as scratch** button below the table of tapes. (This may take a while to complete.)
   - To synchronize the TSM inventory with the library inventory, click **Audit tapes in lib using barcodes** or **Audit tapes in lib using tape label**. This is necessary after tapes are added to the physical library. The first button performs the action faster and executes the **dsmadmc audit library checklabel=barcode** command. The second executes a full audit using the **dsmadmc audit library checklabel=yes** command.

Setting the backup management application password

If you are using a BMA other than TSM installed on the SPHiNX server, you can configure a system account for use by backup management applications (for stacked exports).

To configure a system user account

1. Click **Security > Passwords** on the navigation pane of the SPHiNX web interface. A page similar to the following is displayed:



2. Select **hsm** from the drop-down list.
3. Type the username and password that is required to log in to the backup management application and then click **Update**.

For more information, view the help on the Manage Passwords page. Click the **Help** button at the top of the page.

Exporting virtual tapes

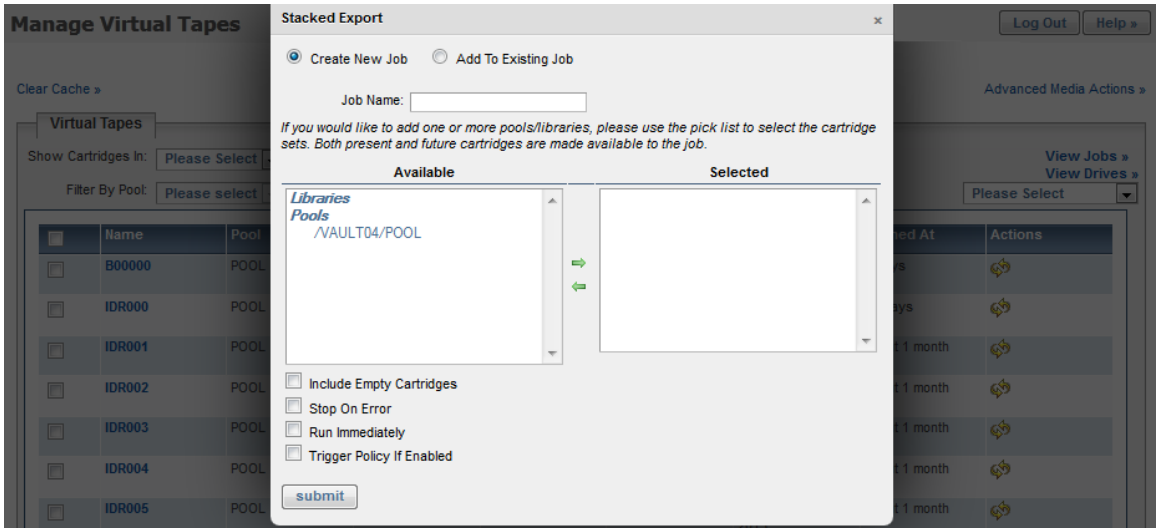
To export a virtual tape to physical tape, you must create and run a stacked export job. If Data Encryption is enabled and an encrypted virtual tape is selected for stacked export, the tape is migrated as-is. That is, the data remains encrypted when it is exported to physical tape. See "Enabling and Configuring Data Encryption" on page 87 for more information about this feature.

To create and run a stacked export job

Requires the HSM Migration access right

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Select **All**, **Shelf**, or a VTL name from the **Show Cartridges In** drop-down list.

3. Choose one or more virtual tapes to export. (In a later step, you can also choose virtual tapes in VTLs or pools.)
4. Select **Stacked Export** from the Please Select drop-down list above the table, on the right side of the page. The following is displayed:



5. On the pop-up dialog, select the **Create New Job** option.
6. Specify a job name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed. If you leave this field blank, a name is generated for you.
7. To choose virtual tape libraries or pools to export (in addition to those selected on the Manage Virtual Tapes page), move libraries or pools from the **Available** list to the **Selected** list. Or, remove tapes or pools by moving them from the **Selected** list to the **Available** list. Use the ➡ and ⬅ buttons to move items to and from the lists.
8. If empty tapes are included in those selected above, you can select the **Include Empty Cartridges** option to export these tapes as well as those with data. If you do not select this option, empty tapes are not exported (they are skipped).
9. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to export all virtual tapes.
10. Select the **Run Immediately** option to run the job immediately after it is created. Do not select this option if you want to create a schedule for the job.
11. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.
12. Click **submit**.
13. To schedule the stacked export job, you must create a schedule that is associated with the job.
    a. Click **Administration > Jobs** on the navigation pane.
    b. On the Manage Jobs page, click next to the job you want to schedule. The Manage Schedules page is displayed.

c. Click **Add Schedule**.

d. In the Create Schedule area, select how often you want the job to occur:
   - One time — Runs the job once. You must select a start date and time.
   - Weekly/Daily — Runs on the days you select. You must select the days and a start date and time.
   - Monthly — Runs on a specific date each month. Select a date and start time.

   If you specify a date that does not exist in a month, the job will run on the last day of the month.

e. Click **Save**.

After the job runs, you can return to the Managed Schedules page for its status. If a problem occurred, the Last Run column will display “Failed”.

After exporting virtual tapes, you can view the Export Reports page to verify that the backup was successful. See the online help for more information.

Importing data from a physical library or drive

To import data from an external tape device

This procedure enables you to import a virtual tape that was exported by a stacked export job to a physical tape device (library or drive).

 *Requires the Virtual Tape Import and Export, Vault Access, and Access to all Vaults access rights*

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Click the **Advanced Media Actions** link in the upper right corner of the page. The Virtual Media - Operation page is displayed.
3. Expand a pool and select a virtual tape in the **cartridge** column.
4. Click the **UnMigrate** button at the top of the page.
5. When prompted, confirm the action.

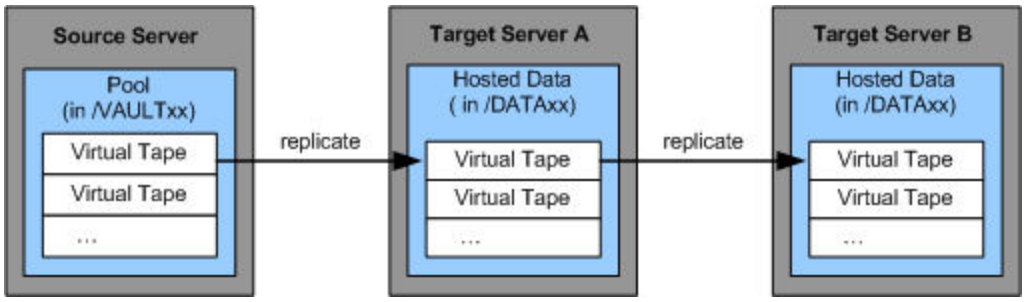
9 Enabling and Configuring Data Replication

You can configure SPHiNX to replicate virtual tapes to a remote SPHiNX server. Using replicate jobs, you can export data as part of your disaster recovery solution or to enable multiple SPHiNX servers to back up virtual tapes to a single remote server. The SPHiNX web interface enables you to view ownership of the virtual tapes that are replicated, and the source server is the only server that can access those tapes. Replicated tapes are stored in data partitions (/DATAxx) on the remote server.

Note See "Enabling and Configuring Remote Export" on page 70 for instructions to configure and use remote export jobs.

To use replicate jobs, you must define a source server where the job originates and one or more target servers, where the replicated data is hosted. The source server ensures that the virtual tape to be replicated contains data. If the virtual tape was erased and has a label only (or no label), it cannot be replicated. Each target server must be configured to accept replication requests from each of the defined source servers. You must also configure the vaults that will be used on target servers to store replication data.

You can also replicate data from one target server to another. If a target server is also configured as a source server, it can then replicate the data to other servers:



Steps to enable, configure, and use replicate jobs

1. Enable the WAN Acceleration license key, if purchased, using the SPHiNX web interface as described in Enabling Licensed Features.

   Note Multiple, optional license keys are available for this feature, based on the desired transfer speed (WAN Acceleration). If the licensed transfer speeds do not match on the source and target systems, the lowest speed is used during replication.

2. Verify that the network servers (firewall, VPN, and so on) between the source and target servers are configured to allow replication traffic; ports 22, 443, and 4567 are required.

3. Configure data partitions on the remote (target) servers as described in the Data Replication chapter of the *Configuration Guide*.
4. Configure source and target settings as described in "Configuring replication settings" help topic.
5. If you want to send email notifications for completed or failed jobs, or after replicated tapes are restored, configure SMTP settings as described in the help.
6. Replicate data to remote servers by creating and running replicate jobs as described in this chapter.

Considerations

- The replicate job will fail if:
  - a virtual tape does not reside in a VTL and the virtual tape is locked at the time of the export
  - there is not enough room on the target; clear space on the target or consider increasing the available capacity on the target system
- If an error occurs during replication, the replicate job is retried once every 30 seconds. The retry is attempted up to 10 times.
- If you notice that replication performance is slow, you may need to adjust the bandwidth limit (when configuring the target server).
- To recover data from a target server, you can restore virtual tapes using the Manage External Data page of the web interface. You can then select the target server and list of virtual tapes to restore. Refer to the help for more information.
- The speed and performance of remote export jobs is determined by the following:
  - If a WAN or Acceleration license is enabled on the source and target servers, WAN acceleration is used to transfer tapes to the target server using the UDP protocol
  - If no WAN Acceleration license is enabled data is transferred to the target server over the network using normal transfer speeds using rsync (TCP).

Configure a data partition on a target server

To dedicate one or more data partitions on a target server for use in replication, you can

- rename an existing vault partition, or
- create a new data partition

The procedures to perform these tasks differ based on the file system type of your appliance (ext3, ext4, or ZFS).

Renaming an existing vault partition

For the SPHiNX 1U-s, 2U-s, 3U-s, and 3U-ns appliances,you can convert existing storage (an existing vault partition) to a data partition using this procedure. Make sure to delete or edit policies on the vault being renamed.

Note For the SPHiNX appliances using ZFS for their VAULT01 file systems, there is no need to rename the existing VAULT01. Instead, you can configure a destination for replicated data by creating a new DATA file system in the ZFS “storage” pool, as described in "Adding a data partition on ZFS" below.

To rename existing vault space

1. Remove or erase virtual tapes and pools on the vault partition that will be used as the data partition. (Data currently residing on a vault partition will no longer be accessible to host systems.)
2. Rename an existing partition. In these steps, you will move (rename) the vault mount point to the new data mount point. A data partition must be labeled **DATAxx**, where *xx* is a two-digit number following the name. Partitions do not need to be numbered sequentially.
   a. Use the **df** command to view the current disk utilization:

      ```
      df -H
      ```

      Here is an example of the output. The bolded lines indicate partitions that are eligible for configuration:

      ```
      Filesystem            Size  Used Avail Use% Mounted on
      /dev/sda2              19G  7.1G   11G  40% /
      /dev/sda4              76G  184M   72G   1% /VAULT00
      /dev/sda1              99M   23M   71M  25% /boot
      tmpfs                 2.0G     0  2.0G   0% /dev/shm
      /dev/sdb1             3.3T  535G  2.6T  17% /VAULT01
      ```

   b. Unmount the vault partition:

      ```
      umount /VAULT01
      ```

   c. Copy the **/etc/fstab** file to a backup file:

      ```
      cp /etc/fstab /etc/fstab.backup
      ```

   d. Relabel the device for the partition in the file, using the new partition name:

      ```
      e2label /dev/sdb1 /DATA01
      ```

e. Edit **/etc/fstab** and replace the old "VAULT*xx*" name with the new "DATA*xx*" name. For example, change this line:

```
LABEL=/VAULT01          /VAULT01                ext4    defaults
      1 2
```

to this:

```
LABEL=/DATA01          /DATA01                ext4    defaults
    1 2
```

f. Rename the mount point:

```
mv /VAULT01 /DATA01
```

g. Mount the partition and set permissions:

```
mount /DATA01
chown bill.replicators /DATA01
chmod 750 /DATA01
```

3. Repeat these steps for each partition you wish to rename.

Creating a new data partition

You can create a new data partition on internal storage or an existing external storage device. You can also attach a new external storage device as described in the *Quick Start Guide*, and then create a data partition.

Adding a data partition on an ext3 or ext4 file system

If using internal storage on a SPHiNX 1U-s, 2U-s, 3U-s, or 3U-ns appliance, or if adding a partition on an external device, you can add a data partition using the following steps:

To add a new data partition

Complete all of the steps from "Adding vaults on external storage devices" on page 26 with the following caveats:

- Use /DATA*xx* instead of /VAULT*xx*
- Use this **chown** command to change the ownership and file system mode of the new data partition: **chown bill.replicators /DATA*xx***

Adding a data partition on ZFS

If using internal storage on a SPHiNX appliance, you can add a data partition using the following steps.

To add a new ZFS dataset for replication

1. To review the current vault layout, click **Configuration > ZFS Vaults** on the web interface.
2. Click on **Add Vault**. In the Vault Details section, name the vault that you want to create. The name t has to be **VAULTxx** or **DATAxx** format; where **xx** are digits.
3. Set a quota for the vault: Size format: M, G or T. ie: **45G**. Click **Save** to save the details for the vault or **Cancel** if you want to cancel the vault creation.

The vault name and mount point is changed; the storage pool name stays the same.

Configuring source and target settings

The “source” server is the SPHiNX server where the original virtual tapes reside. This server replicates tapes to remote (“target”) servers, which store the replicated tapes in a designated directory on a /DATAxx partition. You can also configure a server to be an “intermediate” server, which will host replicated tapes and then replicate them to other remote servers.

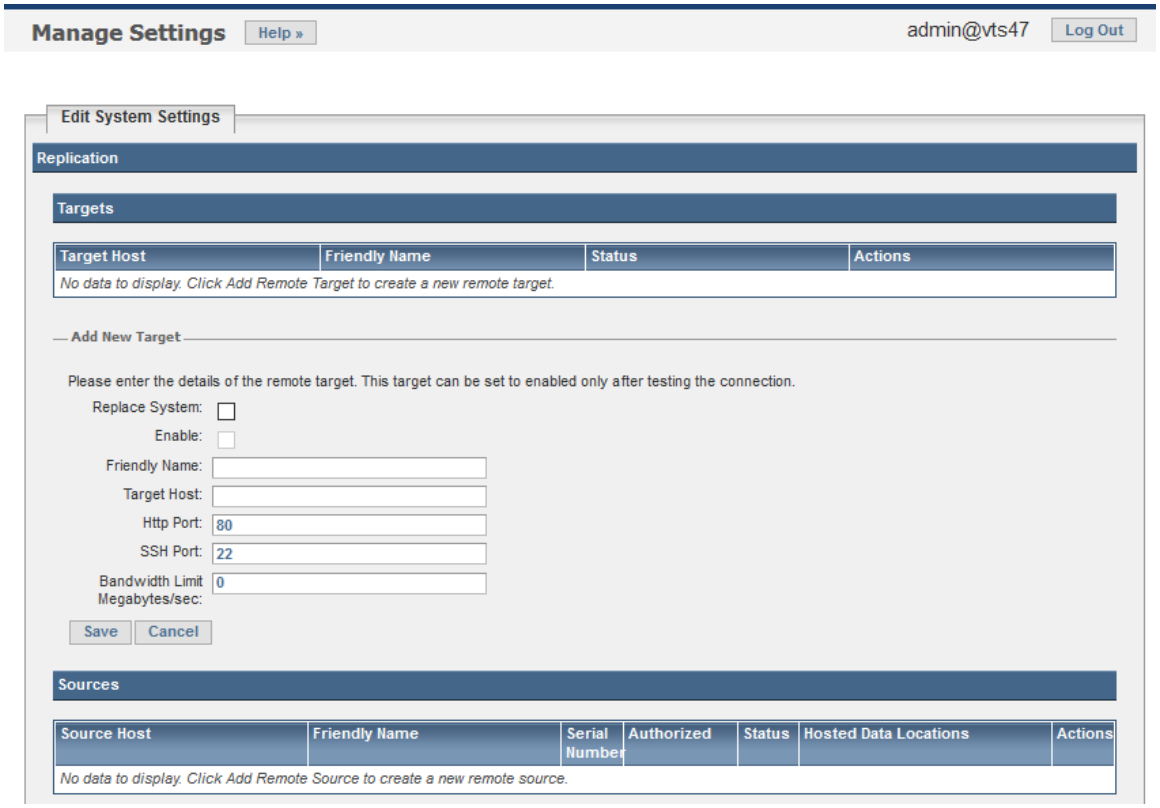
Use the web interface to configure source and target settings, and refer to the online help, which provides in-depth information about each required step in the process.

To add a target server

Requires Administration group membership

Complete these steps using the source server's web interface:

1. Click **Configuration > System** on the navigation pane.
2. Click **Edit System Settings**.
3. Click **Replication** to expand this area of the page.
4. Click the **Add Target Host** button. The following is displayed:



5. If the local (source) server was replaced, you need to notify the target server so that it can update its source server information:

a. Select the **Replace System** checkbox.

b. In the **Previous Serial Number** field, type the serial number of the old source server.

6. In the **Friendly Name** field, type a name for the target server.
7. In the **Target Host** field, type the fully qualified hostname or IP address of the target server.

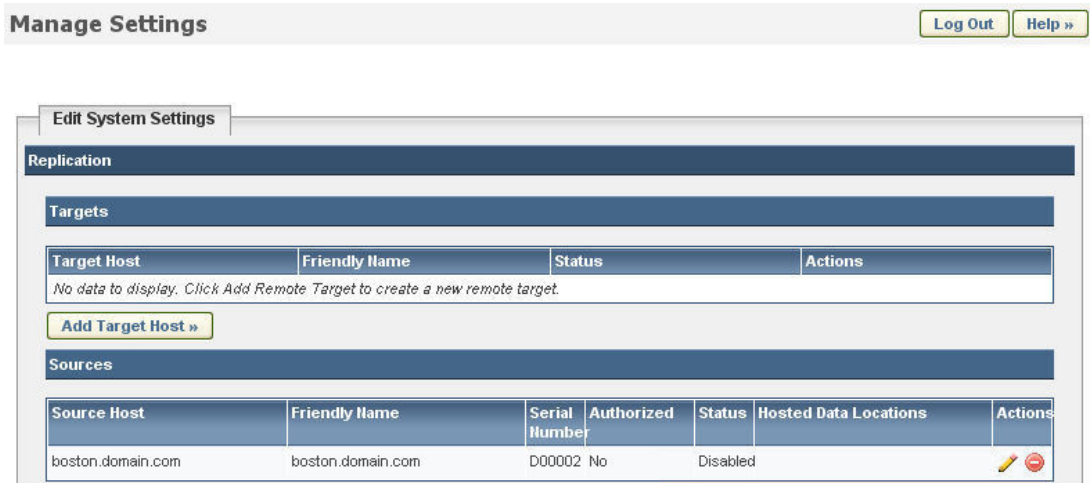
   Note It is recommended that you provide a hostname, if DNS is configured on your network. If you provide an IP address instead of a hostname and then the IP address of the source or target server changes, you must delete the target server and then complete all configuration procedures again.

8. In the **Http Port** field, type the port number used for accessing the web interface on the target system. Typically, this port is set to 80 but it may be set to another number if, for example, the server is behind a firewall. Contact your firewall or system administrator for this port number.
9. In the **Ssh Port** field, type the port number used to access SSH on the target server. Again, if the server uses a non-standard port, contact your firewall or system administrator.
10. In the **Bandwidth Limit** field, type the number of Megabytes per second (**Megabytes/sec**) that the source server can use to send data. If you specify 0, no limit is set.
11. Click **Save**.

To authorize and enable a source server

Complete these steps using the target server's web interface:

1. Click **Configuration > System** on the navigation pane.
2. Click **Edit System Settings**.
3. Click **Replication Settings** to expand this area of the page. The following is displayed:



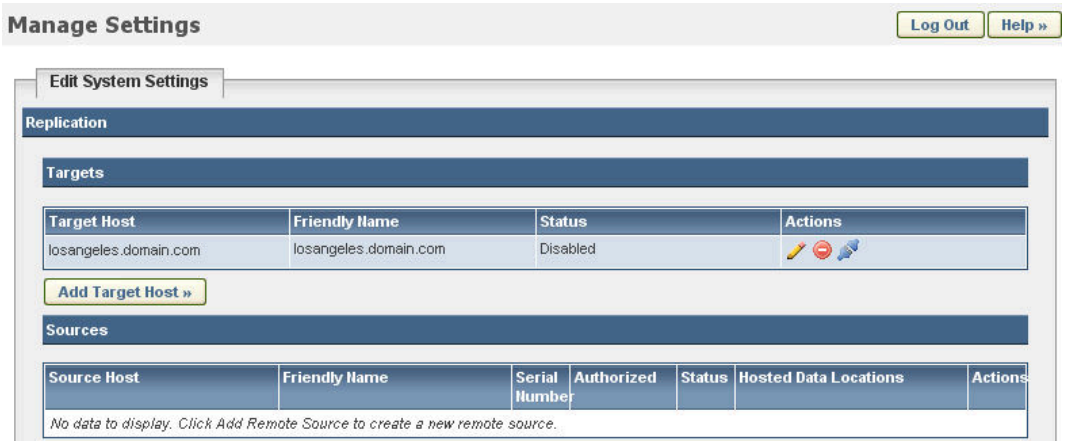
4. Click ✎ next to the source server you want to authorize and enable.
5. Select the **Authorized** checkbox to verify that the source credentials are valid and expected.

6. Select the **Enabled** checkbox to enable the source server, thereby allowing it to use the local (target) system as a replication target. (You cannot select this checkbox if the Authorized checkbox is not selected.)
7. In the **Friendly Name** field, type a name for the source server.
8. Using the **Map To** lists, map mount points (data volumes) on the local (target) server to the source server. This determines where replicated tapes are stored on the local server when sent from this source server. Use the  and  buttons to move mount points to and from the lists.
9. From the **Allowed Streams** drop-down list, set the number of data streams that the source may use when transferring data to this target.
10. If you need to confirm the SSH server key that is seen by the source when this target connects, review the **Fingerprint** value. You can copy and paste the fingerprint and send it to the administrator on the source system, if necessary. This fingerprint is used in the Test Target Connection section of the Edit System Settings page when the source connects to the target.
11. Click **Save**.

To complete the connection and enable the target server

After the target authorizes and enables this source, complete these steps using the source server's web interface:

1. Click **Configuration > System** on the navigation pane.
2. Click **Edit System Settings**.
3. Click **Replication Settings** to expand this area of the page. The following is displayed:



4. Test the connection to the target server. Click  in the Actions column next to the target server.
5. In the Test Target Connection section of the page, select **Yes** to continue the connection and then click **Submit**.
6. Enable the target server by clicking  next to the target server and then selecting the **Enable** checkbox. Then, click **Save**. The server will then be available for selection during replicate job creation.

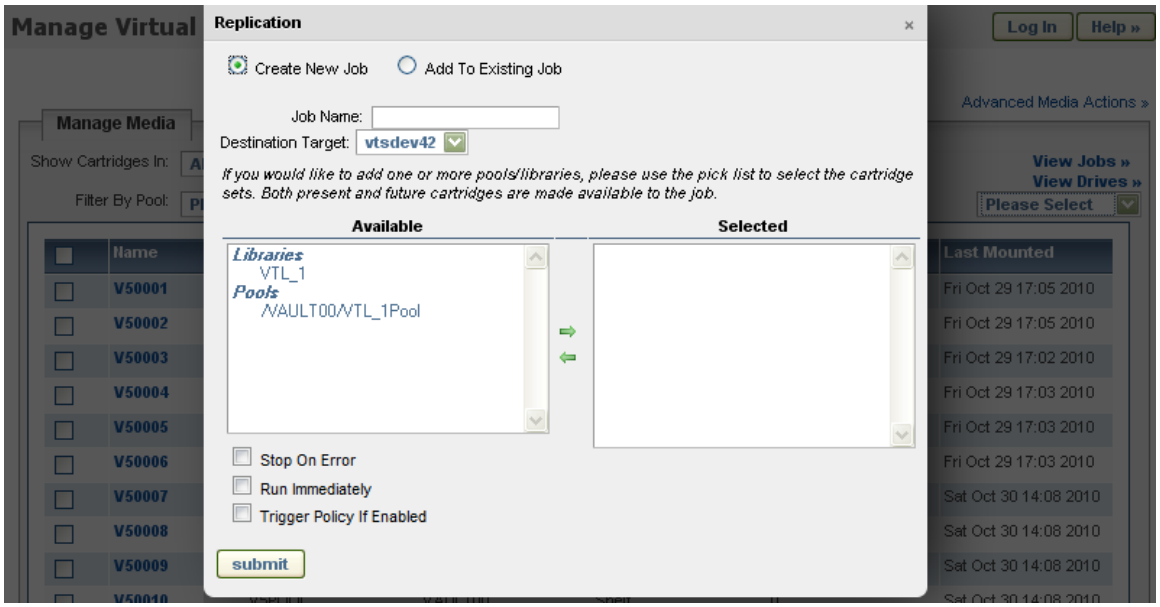
Replicating data to remote servers

To replicate data to remote servers, you must create and run a replicate job.

To create and run a replicate job

Requires the Virtual Tape Import and Export, Vault Access, and Access to all Vaults access rights

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Select **All**, **Shelf**, or a VTL name from the **Show Cartridges In** drop-down list.
3. Choose one or more virtual tapes to replicate. (In a later step, you can also choose virtual tapes in VTLs or pools.)
4. Select **Replicate** from the Please Select drop-down list above the table, on the right side of the page.



5. On the pop-up dialog, select the **Create New Job** option.
6. Specify a job name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed.
7. Select a remote server from the **Destination Target** drop-down list.
8. To choose virtual tape libraries or pools to replicate (in addition to those selected on the Manage Virtual Tapes page), move tapes or pools from the **Available** list to the **Selected** list. Or, remove tapes or pools by moving them from the **Selected** list to the **Available** list. Use the ➡ and ⬅ buttons to move items to and from the lists.
9. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to export all virtual tapes.
10. Select the **Run Immediately** option to run the job immediately after it is created.

11. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.
12. Click **submit**.
13. To schedule the replicate job, you must create a schedule that is associated with the job.
    a. Click **Administration > Jobs** on the navigation pane.
    b. On the Manage Jobs page, click next to the job you want to schedule. The Manage Schedules page is displayed.
    c. Click **Add Schedule**.
    d. In the Create Schedule area, select how often you want the job to occur:
        - One time — Runs the job once. You must select a start date and time.
        - Weekly/Daily — Runs on the days you select. You must select the days and a start date and time.
        - Monthly — Runs on a specific date each month. Select a date and start time.

        If you specify a date that does not exist in a month, the job will run on the last day of the month.
    e. Click **Save**.

    After the job runs, you can return to the Managed Schedules page for its status. If a problem occurred, the Last Run column will display “Failed”.

Restoring a virtual tape from a replication target

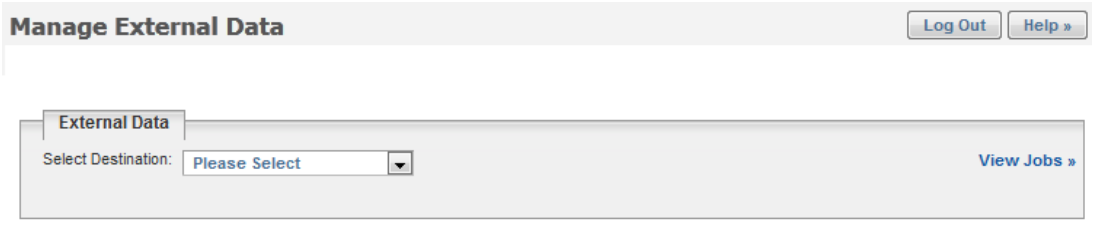
You can restore virtual tapes that were replicated to remote SPHiNX servers (by replicate jobs).

Note A virtual tape will be locked (on the remote server) when it is imported. Therefore, the virtual tape cannot reside in an active library. If necessary, move the tape to the shelf on the remote server before importing it on the local server.

To restore exported virtual tapes as part of disaster recovery (if the source SPHiNX server is unavailable), you can convert a target server to a source server to access the exported virtual tapes. Refer to "Reinstalling and Restoring SPHiNX" on page 188 for instructions.

To restore replicated tapes

1. Click **Administration > External Data** on the navigation pane.



2. Select a remote host from the Replication Destinations section of the **Select Destination** drop-down list. A list of replicated tapes that reside on the remote host are listed.

3. Select one or more virtual tapes to restore and then select **Import** from the Please Select drop-down list above the table on the right.

   Note If the virtual tape has moved from its original location on the source (local) server,  is displayed next to the physical tape and the new location is displayed in the **Source Vault/Pool** column. If you import a physical tape whose virtual tape has moved, the contents of the virtual tape in the new location are overwritten. You can also choose not to import the tape, move the source virtual tape to its original location, and then attempt to import the physical tape again.

4. To name the restore job, enter a name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed.

5. If you wish to stop the restore operation if an error occurs, select **Stop on Error** (above the table). If an error occurs, the restore job fails. If you do not select this option, the restore operation will skip tapes that caused an error and finish importing the selected tapes.

6. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.

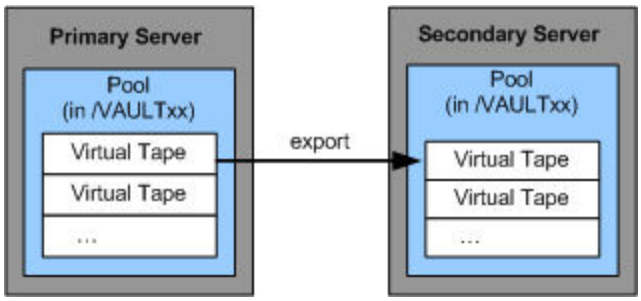
7. If the virtual tape is no longer on the source (local) server, select a location where the imported tape will be created. You can select a vault and pool from the drop-down list that is displayed in the **Source Vault/Pool** column.

8. Click **submit**. A import job is created and run immediately.

Note Replicate jobs write to temporary files and can be resumed if you retry the job within 25 hours of the original job run.

10 Enabling and Configuring Remote Export

Remote export jobs enable you to mirror data on a remote server. Virtual tapes that are exported this way are copied to the remote (also referred to as "target") server over a wide area network (WAN) TCP/IP connection and stored in vault partitions (/VAULTxx) on the remote server.



You can use remote export jobs to ensure high availability of data across sites or to set up “role swapping” of primary and secondary SPHiNX servers in your environment, for disaster-recovery purposes.

This chapter describes how to enable and configure SPHiNX for remote export jobs. See "Enabling and Configuring Data Replication" on page 60 for instructions to configure and use replicate jobs.

Before configuring remote export jobs, be aware of the following:

- SPHiNX does not determine if virtual tapes are synchronized across servers. There is no way to inform the administrator of either system that virtual tapes are synchronized or which system last modified a virtual tape.
- Ownership of virtual tapes is not stored, so there is no way to inform the administrator on either system of the originator (source) of the virtual tape.
- Remote export jobs push virtual tapes from one system to another. If using these jobs for role swapping, it is your responsibility to disable the remote export jobs on the current source server (at the production site) and enable them on the secondary server. If you do not disable all jobs on the production site, data may be overwritten.
- The export will fail if a virtual tape with the same name exists on the target server (in a different pool).
- If a virtual tape does not reside in a VTL, the remote export will fail if the virtual tape is locked at the time of the export.
- The speed and performance of remote export jobs is determined by the following:
    - If a WAN or Acceleration license is enabled on the source and target servers, WAN acceleration is used to transfer tapes to the target server using the UDP protocol

- If no WAN Acceleration license is enabled data is transferred to the target server over the network using normal transfer speeds using rsync (TCP).

How to configure servers for remote export

This section describes the steps that need to be performed to configure SPHiNX to perform remote export jobs for two use cases:

- Copying data to a remote server, for high availability purposes
- "Role swapping" of primary and secondary SPHiNX servers, for disaster recovery purposes

If you are using remote export jobs for role swapping, there are two scenarios that dictate the steps you can perform:

- The primary (source) server becomes unavailable and the secondary (target) server must assume production responsibilities. Eventually, the primary server will resume production responsibilities. This may be the case if you must take a site offline for maintenance or if you are testing DR procedures.
- The primary server or site becomes permanently unavailable.

Configuring SPHiNX to mirror data on a remote server

1. Configure network settings and TCP/IP security as described in Configuring network settings. This step includes configuration of the source server and target server.
2. If you want to send email notifications for completed or failed remote export jobs, configure SMTP settings on the source server as described in the online help.
3. Configure the source server:
   a. Enable the WAN Acceleration license key on the source server, if purchased, using the SPHiNX web interface as described in Enabling Licensed Features.
   b. Configure the Remote Export options as described in Configuring settings for remote export jobs. This includes pairing the source and target servers.
4. Configure the target server:
   a. Enable the WAN Acceleration license key on the target server, if purchased, using the SPHiNX web interface as described in .
   b. Identify the source server on the target server. This is also described in Configuring settings for remote export jobs.
   c. If Data Encryption is licensed, it is recommended that you configure the target server to use the source server as its key generator.
5. Export virtual tapes to the target server by creating and running remote export jobs (on the source server). This is described in Replicating a virtual tape using a remote export job.

   If virtual tapes are exported to the target server after the source server has been in production, new remote export jobs may take a long time to complete.

Configuring SPHiNX for role swapping

The following procedures provide an overview of the steps you must perform for each role swapping scenario. The primary server is referred to as "Server A" and the secondary server is referred to as "Server

B" for simplicity.

Note Some steps in the following procedures are provided in section of this chapter. However, some steps are provided in the *Quick Start Guide* and online help. It is recommended that you display and review this documentation before beginning.

To configure servers and swap roles

1. Configure network settings and TCP/IP security as described in "Configuring network settings" on page 73. This step includes configuration of the primary server (Server A) and secondary server (Server B).
2. If you want to send email notifications for completed or failed remote export jobs, configure SMTP settings on Server A as described in the online help.
3. Configure Server A to export data to Server B:
    a. Enable the WAN Acceleration license key on Server A, if purchased, using the SPHiNX web interface as described in Enabling Licensed Features.
    b. Configure the Remote Export options as described in "Configuring settings for remote export jobs" on page 77.
    c. Export virtual tapes to Server B by creating and running remote export jobs. This is described in "Exporting a virtual tape using a remote export job" on page 79.

    If virtual tapes are exported to Server B after the Server A has been in production, new remote export jobs may take a long time to complete.
4. Configure Server B in preparation for role swapping:
    a. Enable the WAN Acceleration license key on Server B, if purchased, using the SPHiNX web interface as described in .
    b. Make sure ports on Server B are set to virtual for ports to be connected to host servers. (Host servers will use these ports to write data to VTLs and VTDs.) See Configuring Ports for more information.
    c. Connect the host servers to Server B. Refer to the *Quick Start Guide* for cabling instructions.
    d. Identify the source server (Server A) on Server B. This is also described in "Configuring settings for remote export jobs" on page 77.
    e. Configure VTLs and VTDs to match those on Server A. See "Creating and Managing VTLs and VTDs" on page 34 for more information.
    f. Remove virtual tapes from the newly created VTLs, if VTLs were created. These virtual tapes are created automatically but cannot be used to store data that is exported by the remote export jobs. Refer to the online help for instructions.
    g. Recreate and schedule all of Server A's jobs on Server B, including the remote export jobs (whose target should be Server A). Be sure to disable these jobs; they should not run until after the roles of the servers have been swapped. Refer to the online help for instructions.
    h. If Data Encryption is licensed, it is recommended that you configure Server B to use Server A as its key generator.

5. To swap roles:
    a. If Server A is available:
        - Stop all backup operations to Server A.
        - Disable all jobs on Server A, including the remote export jobs that export data to Server B. See the “Modifying a job” help topic in the online help.
        - Remove virtual tapes from all VTLs on Server A, if VTLs are used. See the “Removing a virtual tape from a VTL” help topic for details.

    b. Load virtual tapes that were exported from Server A into VTLs on Server B, if VTLs are used. These virtual tapes are needed by the host servers, to back up data on Server B. See the “Adding a virtual tape to a VTL” help topic for details.

    c. Enable jobs on Server B.

    d. If Data Encryption is used in the environment and Server A was the key generator, you do not need to perform additional steps to continue to use Data Encryption after swapping roles. However, if Server A is not available, you can restore a backup of Server A’s key database from a remote host. Then, you can configure Server B to be the key generator. See the Managing Data Encryption help topics in the online help for details.

    e. Back up data from host servers to Server B as needed.

At this point, Server B has become the primary server.

To restore roles

1. Cease production on Server B:
    - Stop all backup operations to Server B.
    - Disable all jobs on Server B, including the remote export jobs that export data to Server A. See the “Modifying a job” help topic in the online help.
    - Remove virtual tapes from all VTLs on Server B. See the “Removing a virtual tape from a VTL” help topic for details.
2. Load virtual tapes that were exported from Server B in VTLs on Server A. These virtual tapes are needed by the host servers, to back up data on Server A. See the “Adding a virtual tape to a VTL” help topic for details.
3. Enable jobs on Server A.
4. Back up data from host servers to Server A as needed.

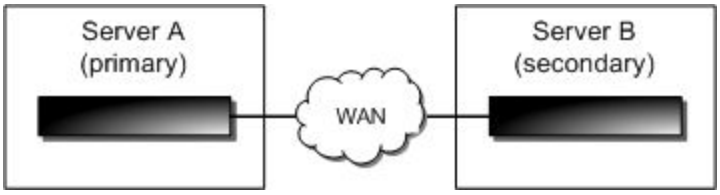
Configuring network settings

You must configure network settings for all SPHiNX locations. To configure the local system, you must attach a monitor, keyboard, and mouse to the SPHiNX server. To configure remote systems, you must use a remote-access application to access those systems, or perform the steps at each site. The IP address, which will differ for each SPHiNX server, must be configured at the local and remote sites. Consult your network administrator to determine the gateway and subnet mask to use for each system.

In addition, you should be familiar with networking concepts to complete the steps in this section. Obtain the following information before beginning this procedure:

- Root access to the SPHiNX system; see "Managing operating system accounts" on page 118 of the default accounts provided on the server
- IP address, subnet mask, and gateway of each SPHiNX server

The following steps use two sites as an example of enabling Data Replication between two sites, Boston and Los Angeles, connected by a wide area network (WAN):



To configure network settings

1. Verify that the hostname, IP address, and gateway are configured on each SPHiNX server in the environment. Refer to the *Quick Start Guide* for more information.
2. If DNS or DHCP is not configured in your environment and you want the servers to communicate using hostnames, set up the **/etc/hosts** file to configure aliases for each SPHiNX server in the environment. Perform this step on the target server for each source SPHiNX server.
   a. At the command prompt, log in.
   b. Become root:

      ```
      su -
      ```

   c. Be sure the file contains the IP address, hostname, and alias for the local SPHiNX server and the remote server(s). Here is an example of the file on the losangeles server:

      ```
      # Do not remove the following line, or various programs
      # that require network functionality will fail.

      127.0.0.1       localhost.localdomain   localhost
      10.10.2.144     losangeles.domain.com   losangeles
      10.10.2.145     boston.domain.com       boston
      ```

      Here is an example of the file on the boston server:

      ```
      # Do not remove the following line, or various programs
      # that require network functionality will fail.

      127.0.0.1       localhost.localdomain   localhost
      10.10.2.145     boston.domain.com       boston
      10.10.2.144     losangeles.domain.com   losangeles
      ```

3. Test connectivity by pinging the network connections. At the prompt, enter **ping hostname**. For example, to ping the Boston server, enter **ping boston**. Output similar to the following is displayed:

   ```
   64 bytes from boston (10.10.2.145): icmp_seq=0 ttl=64 time=0.053 ms
   64 bytes from boston (10.10.2.145): icmp_seq=1 ttl=64 time=0.053 ms
   64 bytes from boston (10.10.2.145): icmp_seq=2 ttl=64 time=0.053 ms
   64 bytes from boston (10.10.2.145): icmp_seq=3 ttl=64 time=0.053 ms
   ```

   Press CTRL-C to stop the ping process.

If you receive a timeout error, check cabling or contact a network administrator for assistance. If you receive an unknown host error, check the **/etc/hosts** file and make sure everything is correct. Note that the hostnames in this file are case-sensitive.

4. Set up and authorize secure shell (SSH):
   a. At the command prompt, become bill:

      ```
      su - bill
      ```

   b. Generate an authorization key for SSH for the target server, to authorize remote access for the bill user:

      ```
      ssh-keygen -t rsa
      ```

   c. Press ENTER to save the file in the default location. This step creates the **/home/bill/.ssh/** directory.

   d. Press ENTER to skip the pass phrase.

   e. Press ENTER to verify skipping the pass phrase.

   f. Copy the generated authorization key to the target server (boston):

      ```
      ssh-copy-id -i /home/bill/.ssh/id_rsa.pub bill@boston
      ```

   g. When prompted, enter **yes**.

   h. Enter the password for the bill user at the target server.

   If problems arise when using SSH with the target server, you can remove the **/home/bill/.ssh/known_hosts** and **/home/bill/.ssh/authorized_keys** files from the target and source servers and repeat the steps above.

5. If you configured SSH and access to the bill account is restricted on the SPHiNX servers, you must grant SSH access to the bill user for each SPHiNX server. To do this, become root (enter **su - root**) and then edit **/etc/ssh/sshd_config** to add this line:

   ```
   AllowUsers bill@source_svr
   ```

   where *source_svr* is the IP address or hostname of the SPHiNX server where the AutoCopy operation is originating. For example, if the AutoCopy operation will originated on the losangeles server, you must log in to the boston server and edit the file to allow access from the losangeles server. To specify multiple servers, use wildcard characters in the specified IP address or hostname, or specify a list of servers separated by spaces.

   Also, if the following line is listed in the file, be sure to remove it:

   ```
   DenyUsers bill
   ```

6. Check the SSH connection, if you configured SSH.
   a. At the command prompt, log in.

   b. Become bill:

      ```
      su - bill
      ```

   c. At the command prompt, enter **ssh user@server uptime**. For example, on the Boston server, enter **ssh bill@boston uptime**.

      The first time you enter an ssh command, a message similar to the following is displayed:

```
The authenticity of host 'server_name (IP_addr)' can't be
established.

RSA key fingerprint is
5f:10:3c:47:78:8f:e3:28:9d:ab:6b:34:ed:d1:e4:08.

Are you sure you want to continue connecting (yes/no)?
```

Enter **yes**.

d. Repeat these steps on each SPHiNX server.

Note SSH can be setup for one direction or multiple directions. If multiple directions are configured, these steps should be executed from the other direction.

Configuring settings for remote export jobs

To configure remote export settings

 *Requires the Edit Configuration File and Factory Setup Activities access rights*

1. Enable WAN Acceleration licensing, if purchased, as described in "Enabling Licensed Features" on page 30.
2. On the source server, complete these steps:
   a. Configure source server settings by clicking **Configuration > System > Edit Configuration > Remote Export** (you may need to click ✎ next to **vts.conf** to see the Remote Export section of the page). Then, provide settings for these parameters:

Parameter	Description	Values	Example
Remote Export source parameters			
Destination hosts	Specifies a list of hosts or IP addresses that can be chosen as destinations. This parameter is required.	SPHiNX server name (s)	vts11, vts21
# streams to break the files into	Specifies the number of streams used to transmit each file. That is, the file is split into chunks and sent in parallel. This option should be used over high-latency, high bandwidth networks. This parameter is optional.	Integer	2
Temp directory on destination	Specifies the staging area of the chunks if # streams to break the files into is specified. Ensure enough space is available to hold the sum of the sizes of largest files to be sent at one time. This parameter is required if the # streams to break the files into parameter is set to a value greater than 1.	Full path to a directory	/VAULT10/.TMP
Temp directory on source	Specifies the list of entries	Full path to a directory,	vts11:/VAULT01/TMP, vts21:/VAULT00

Parameter	Description	Values	Example
	in the form host:/dir where the remote-side chunks are stored during transmission. This parameter is required if # streams to break the files into is set to a value greater than 1.	including the target server's name	
Remote Export target parameter	Specifies		
Bandwidth limit Megabytes/sec	Allows configuring the bandwidth limit (in Megabytes/sec) for replication and auto-copy.	Numerical values only	
rsync override parameter			
Disable delta differencing	By default, delta differencing is used to determine the content that is exported to remote servers after the initial export if WAN Acceleration is not licensed, select this option.		

b. Click **Apply**.

c. Expand the **Configuration File** section of the page and then click **Save Changes**.

d. Restart the TapeServer process on the Manage System Tasks page.

3. On the target servers, configure the source server(s), as follows:
   a. Click **Configuration > System** on the navigation pane.

   b. Click **Edit Configuration**.

   c. Expand the **Remote Export** section of the page.

   d. In the **Source hosts** field, specify a list of authorized source (originating) servers. The list of target locations cannot be generated unless the source server is listed.

   e. Click **Apply**.

   f. Expand the **Configuration File** section of the page and then click **Save Changes**.

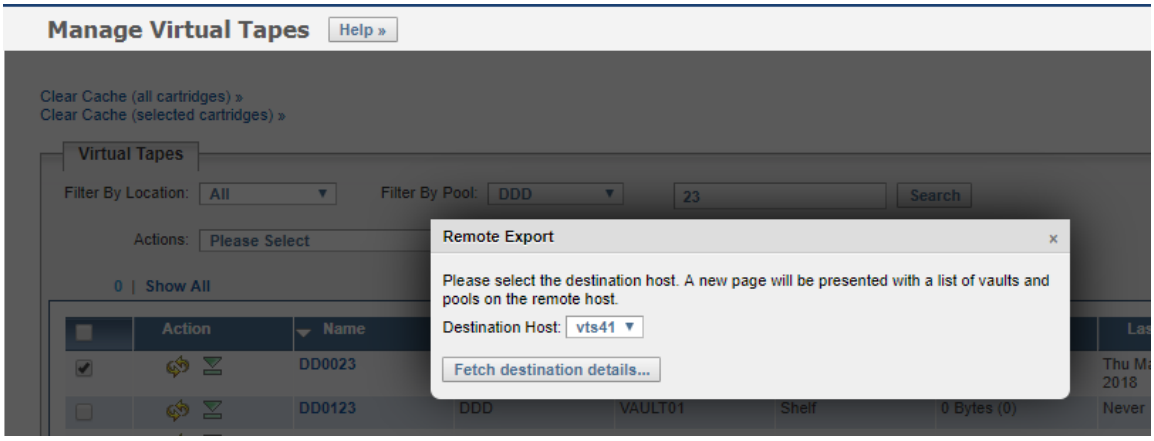
   g. Restart the TapeServer process on the Manage System Tasks page.

Exporting a virtual tape using a remote export job

To create a remote export job

Requires the Virtual Tape Instant DR access right

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Select **All**, **Shelf**, or a VTL name from the **Filter By Location** drop-down list.
3. Choose one or more virtual tapes to export.
4. Select **Remote Export** from the **Actions** drop-down list above the table, on the left side of the page. The following dialog is displayed:



5. Select a target server from the **Destination Host** drop-down list.
6. Click **Fetch destination details**. A list of virtual tapes to be exported is then listed on the **Manage Virtual Tapes** page.
7. If necessary, exclude virtual tapes from the remote export job. If the name of a selected virtual tape exists on the destination host, the existing path will be used and cannot be changed. Therefore, you can exclude the virtual tape from export if you do not wish to overwrite the destination virtual tape.
8. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to export all virtual tapes.
9. Click **Remote Export**.
10. To schedule the remote export job, you must create a schedule that is associated with the job.
    a. Click **Administration > Jobs** on the navigation pane.
    b. On the Manage Jobs page, click next to the job you want to schedule. The Manage Schedules page is displayed.
    c. Click **Add Schedule**.

d. In the Create Schedule area, select how often you want the job to occur:
   - One time — Runs the job once. You must select a start date and time.
   - Weekly/Daily — Runs on the days you select. You must select the days and a start date and time.
   - Monthly — Runs on a specific date each month. Select a date and start time.

   If you specify a date that does not exist in a month, the job will run on the last day of the month.

e. Click **Save**.

After the job runs, you can return to the Managed Schedules page for its status. If a problem occurred, the Last Run column will display “Failed”.

12 Configuring EMS Communication

To automate the process of mounting and dismounting virtual tapes on a NonStop host server, you must configure the Event Management System (EMS) on SPHiNX. The EMS service for host servers starts the EMS distributor on the host server by issuing a Tandem Advanced Command Language (TACL) command. The distributor notifies the SPHiNX EMS service when an EMS message is posted on the host server. These EMS messages relate to mount requests, VTSPolicy commands, heartbeat messages, and critical and error event messages.

Perform the following steps for *each* NonStop host server to which SPHiNX will send messages.

Before beginning:

- Create a user account on the host server that can be used by the EMS distributor.

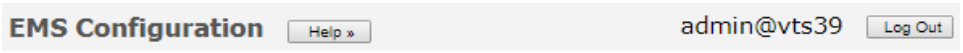
To configure EMS:

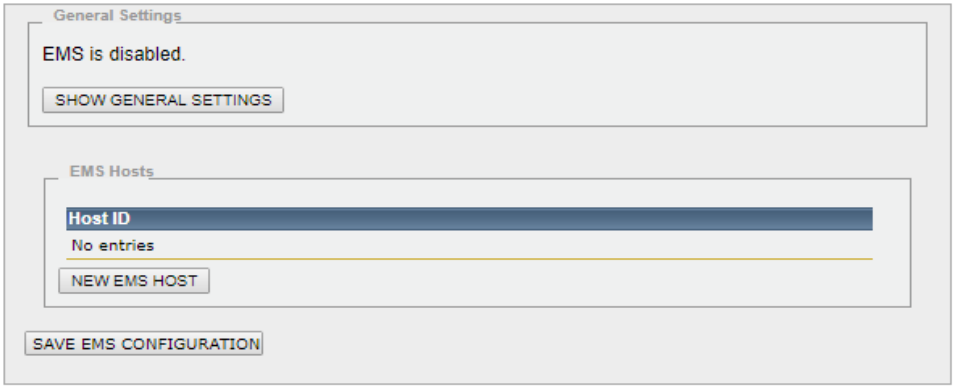
Requires the Edit Configuration File access right to edit the EMS settings, and System Maintenance Functions or Virtual Tape Mounts and Locks access right to restart the EMS service

1. Enable EMS and configure the general settings, as follows:

a. Click **Configuration > System** on the navigation pane.

b. Click the **Edit EMS Configuration** link. The EMS Configuration page is displayed.





c. Click **Show General Settings**.

d. To enable EMS, select the **Enable EMS** check-box.

e. To configure SPHiNX to generate EMS messages for notifications, set the following:
   - To enable SPHiNX to send notification messages back to the host from EMS messages, select **Enable Host Notifications**.
   - If you enabled notifications, set the notification level from the **Notification Level** drop-down list. This enables EMS to acknowledge certain EMS messages and generate completion status (success or failure) messages. You can select multiple levels by pressing CTRL and clicking on the levels in the list. To deselect a selected notification level, press CTRL and click a selected item.

f. To configure keep-alive messaging, set the following:
   - Select **Enable Host Notifications**.
   - Select the **Enable Keep Alive** checkbox to enable keep-alive messaging, which configures SPHiNX to send EMS messages to the host so that the Telnet or SSH session does not time out. Once enabled, EMS processing on the host can be increased because the Telnet or SSH connection between the SPHiNX server and the host stays alive.
   - In the **Keep Alive Interval** field, specify the number of seconds between EMS messages that are sent from SPHiNX to the host.

g. If GFS is implemented, define SPHiNX servers with which the current SPHiNX server will coordinate mount processing. Intersystem communication is primarily used to cancel pending mounts on other SPHiNX systems that have simultaneous access to the same vaults mounted by GFS. (If GFS is not used in the environment, ignore this setting.)

Select **Enable Intersystem Communication**. Then, in the Intersystem Communications Hosts section of the page, click **New** and specify a hostname or IP address in the **Host** field. Then, click **Add**. Repeat this step for each host you want to add.

h. Click the **Save EMS Configuration button** (at the bottom of the page) to save the settings.

2. Define the EMS hosts that identify the host servers for which a Telnet or SSH session will be established.
   a. Click the **New EMS Host** button.
   b. Specify a name for the host in the **Host ID** field. This is used for display purposes only.
   c. In the **Host Name or IP** field, specify a hostname or IP address of the host server for which a Telnet or SSH session will be established.
   d. Select the protocol to use for the session from the **Protocol** drop-down list.
   e. In the **Host Port** field, specify the target Telnet or SSH port on the host server. By default, SSH runs on port 22. To identify the SSH port on the host server, refer to the PORT parameter in the SCF IN file that defines the SSH process.
   f. To define the service settings, set the following:
      - *For Telnet only*
        Specify the service selection prompt to which the EMS login process responds and begins in the **Service Prompt** field. Specify any search pattern as a Perl regular expression, and the %username% and %password% values may be used as placeholders that will be replaced with values defined on the Manage Passwords page later.

Example: `/^Enter Choice>\s*$/i`

- In the **Service Answer** field, specify the service response.

  Example: `TACL`

g. To define the login settings, configure the following:
   - *For Telnet only*
     Specify the user prompt that will be used during the login process in the **Login User Prompt** field.

     Examples:

     TACL: `/TACL 1>\s*$/`

     TACLS: `/login:\s*$/i`

     XYGATE: `/TACL 1>\s*$/`

     SAFEGUARD: `/TACL 1>\s*$/`

   - *For Telnet only*
     Specify the user response that will be shown during the login process in the **Login User Answer** field.

     Examples:

     TACL: `logon %username%`

     TACLS: `%username%`

     XYGATE: `logon %username%`

     SAFEGUARD: `logon %username%`

   - In the **Login Password Prompt** field, specify the password prompt that will be returned by the host server in response to the Telnet or SSH connection.

     Examples:

     TACL: `/Password:\s*$/i`

     TACLS: `/Password:\s*$/i`

     XYGATE: `/Password:\s*$/i`

     SAFEGUARD: `/Password:\s*$/i`

   - In the **Login Password Answer** field, specify the password response that will be shown during the login process.

     Example: `%password%`

   - In the **Login Successful** field, specify a command string to send after a successful login.

     Example: `/Last Logon:/`

   - In the Login Command text box, specify the command that will initiate the EMS Distributor on the host server. Each line entered in the text box will be sent as a

separate line to the host. If more than one SPHiNX server is deployed in the environment, each SPHiNX server must specify a unique name (for the NAME parameter) that is up to six characters in length (including the $). Here is an example: (for TACL):

```
#SET #INFORMAT TACL
EMSDIST /CPU 0, PRI 100, NAME $VTMS1, TERM $ZHOME/ BACKUP 1,
TYPE P, COLLECTOR $0, TEXTOUT [#MYTERM]
```

h. In the **Notify Wait Timeout** field, specify the number of seconds to allow the host to process commands before SPHiNX expects to prompt for another command. Typically, this should be 2-3 seconds but it causes no harm to allow more time for the host.

i. In the **Notify Logout Timeout** field, specify the number of seconds to wait after issuing the LOGOUT command and before closing the socket connection.

j. In the **Response Timeout** field, specify the timeout value (in seconds) used to wait for each response during the EMS login process.

k. In the **Host and Virtual Devices** section of the page, add the tape devices that are configured on the host server and connected to SPHiNX. Each host device corresponds to a virtual device, which defines the virtual tape drive known to the host server for the host device. You must define at least one host device.

   Click **New** and specify a name in the **Host Device** field. Then, specify a name in the **Virtual Device** field. Then, click **Add**. Repeat this step for each host device you want to add.

l. In the **Vaults** section of the page, specify the vaults that should be accessed by SPHiNX. If a vault is not listed here, it cannot be accessed. If this section is left blank, all vaults are available to SPHiNX.

   Click **New** and specify a name in the **Vault** field. You do not need to specify the leading slash in the vault name. Then, click **Add**. Repeat this step for each vault you want to add.

m. In the **Reset Devices** section of the page, define the list of tape names as known to the host system for which SPHiNX will issue a reset before each mount.

   Click **New** and specify a name in the **Reset Device** field. Then, click **Add**. Repeat this step for each device you want to add.

n. Click **Add**.

   Note Clicking the Add button does not save the settings. You must click the Save EMS Configuration button to save host settings.

Repeat these steps for each EMS host you want to add.

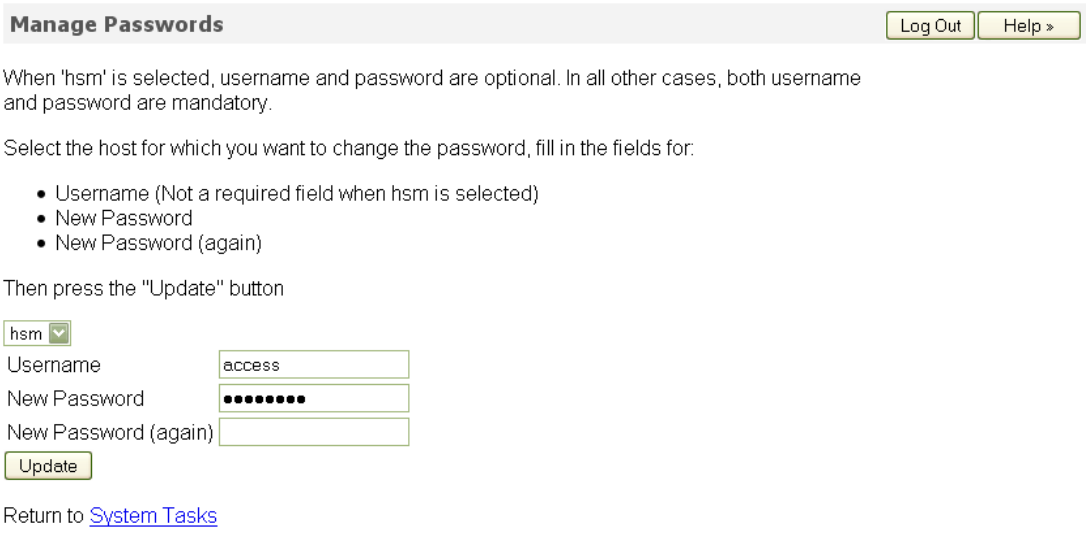
3. Click **Save EMS Configuration** to save the settings.

4. *If using EMC NetWorker (formerly Legato NetWorker) client:*
   After the EMC NetWorker client is installed, IPV6 entries are added to the **/etc/hosts** file. This is required for NetWorker to work properly, though this prevents the host from being listed as a configured EMS host on the web interface. To fix this, edit the **/etc/hosts** file to change the IPv^ entry to look like this:

   ```
   ::1 localhost6.localdomain loopback
   ```

5. Set the username and password for each EMS host:

   a. Click **Security > Passwords** on the navigation pane. The following page is displayed:



   b. Configure a password for each EMS host. Click **Help** for complete instructions.

6. If you configured EMS to use SSH, you must log in to each host server to verify and accept the fingerprint. When the fingerprint is accepted, the host server's key is stored in **/home/bill/.ssh/known_ hosts** on the SPHiNX server and used to authenticate the key during subsequent logins.

   Be careful when accepting keys from remote hosts, to prevent security breaches. A key mismatch can occur because the key has been changed on the host server or because a "man in the middle" exploit is being attempted, which could be used to obtain login credentials. If the key does not match, EMS will not log in.

   Complete these steps to accept the fingerprint:

   a. Log in to the SPHiNX server as the bill user.

   b. Log in to the host server using the bill account:

      ```
      ssh bill@host_server
      ```

      The following message is displayed:

      ```
      The authenticity of host 'host (ip_address)' can't be
      established.
      DSA key fingerprint is <fingerprint>.
      Are you sure you want to continue connecting (yes/no)?
      ```

   c. Enter **yes** to accept the fingerprint.

   d. Exit by pressing CTRL+C.

   If a mismatch occurs after accepting the fingerprint, you can edit the /home/bill/.ssh/known_hosts file to remove lines for host server whose key has changed. Then, after the obsolete key has been removed, repeat this step to accept the new key.

7. Click **Stop EMS Service** and then click **Start EMS Service** on the Manage System Tasks page to restart the EMS service. You must start or restart the service to enable SPHiNX to reread the configuration file.
8. To send notifications to the NonStop server, you must configure several parameters in the configuration file, as follows:
    a. Click **Configuration > System** on the navigation pane.
    b. Click **Edit Configuration**.
    c. Expand the Scan/Cleanup section of the page and set the **Threshold percentage for need cleanup message** option. This indicates the threshold after which a cleanup is initiated, if Scan/Cleanup is enabled. When the SPHiNX file system reaches this threshold (a percentage), virtual tapes can be scheduled for erasure if this parameter is set. This parameter also instructs SPHiNX to send a notification to the NonStop server. Click **Apply** when done.
    d. Expand the **Miscellaneous parameters** section of the page and set these parameters.

Parameter	Description
Send notification on low free space	Enables notification on low vault space; a message is sent to the NonStop host server (the **Send EMS status** option must also be enabled on the Backup Management Application (BMA) page).
% space used before notify	Sets the percentage for the **/VAULTxx** file system usage; if this usage is exceeded, a message is sent to the NonStop server (and an alert is displayed on the Virtual Media - Operation page of the web interface).

    Then, click the **Apply** button.
    e. Expand the **Configuration File** section of the page and then click **Save Change**.

If problems arise, check the **ems.log** file to confirm that the login to the host server and the prompt response are correct.

13 Enabling and Configuring Data Encryption

Data Encryption is an optional SPHiNX licensed feature that enables SPHiNX to encrypt data that is stored on virtual tape. Note that Data Encryption protects data at rest. It does not protect or secure the SPHiNX server.

Here is how Data Encryption affects tape operations:

- When an encrypted tape is mounted, the data that is written to the tape is encrypted. You can also instruct SPHiNX to encrypt data that is already stored on a virtual tape if the tape is not encrypted.
- When SPHiNX exports an encrypted virtual tape to a physical tape using tape-to-tape export, the data remains encrypted if SPHiNX is configured for this and all drives in the physical library support encryption. Otherwise, SPHiNX decrypts the data before it is exported.
- When data is imported (restored) from a physical tape, the data is encrypted if the target virtual tape is encrypted.
- When SPHiNX migrates an encrypted virtual tape to a physical tape (through the use of Stacked Exports), the data remains encrypted as it is migrated.

Note If you need to restore Data Encryption as part of disaster recovery, see "Reinstalling and Restoring SPHiNX" on page 188 for details.

Steps to enable, configure, and use Data Encryption

1. Enable Data Encryption licensing as described in "Enabling Licensed Features" on page 30.
2. Add a key server as described in this chapter.
3. Add a remote key database backup host as described in this chapter.
4. Encrypt virtual tapes as described in "Encrypting and decrypting virtual tapes" on page 103. Then, write data to virtual tapes from the host server.

Decrypt virtual tapes as described in "Encrypting and decrypting virtual tapes" on page 103. Also, data is decrypted as it is read by the host server. You can also restore a key database or restore all Data Encryption settings from a Disaster Recovery site as described in "Recovering SPHiNX configuration data and settings" on page 190.

Overview of Data Encryption

When Data Encryption is enabled on a SPHiNX server, the embedded key server can be configured to generate keys for encrypting virtual tapes. SPHiNX uses symmetric key encryption to secure data written to tape. This encryption is based on Advanced Encryption Standard-Cipher Block Chaining (AES-CBC) and uses 256-bit keys provided by a random number generator. When a key is generated, its key ID is stored with the encrypted virtual tape. The key is stored in a key database on the server that generated it, and each key is encrypted multiple times before being stored. When data on a virtual tape must be decrypted, SPHiNX uses the key ID to retrieve the key from the key database. Storing the key ID with the tape and the key in the database ensures that the key will not be compromised and that it resides in a central, secure location with all other keys.

The key database is backed up on the key server and on at least one other remote server to ensure that a backup of the keys is always available in case the key server is damaged or destroyed. The backup must complete successfully on the localhost and backup host before the keys are available for use by SPHiNX. This ensures that keys are backed up before data is encrypted. (Refer to the "Restoring a key database" help topic for instructions to restore the key database if the key server is no longer available.)

Encryption and decryption during virtual tape operations

A virtual tape can be encrypted in several ways:

- It can be encrypted when it is created.
- It can be manually encrypted after it is created.
- It can be automatically encrypted when it is added to a pool that is designated as encrypted.
- It can be encrypted if the pool in which it resides is designated as encrypted.

Similarly, a virtual tape can be decrypted manually or when its pool is decrypted.

Data Encryption affects other tape operations as well:

- Mounting, reading, and writing to an encrypted virtual tape

  When an encrypted tape is mounted, SPHiNX retrieves the key ID from the tape and uses the ID to request the key from the key server that generated it. The key is then used to decrypt the data as it is read from the tape. (The data remains encrypted on the tape.) Also, SPHiNX cannot read or write to the tape without the key.

- Exporting a virtual tape (tape-to-tape export)

  An encrypted virtual tape is exported as-is if SPHiNX is configured for encryption and the tape is exported in virtual tape format. If you export a pool, the virtual tapes remain intact and encrypted. If the physical drive supports encryption, an unencrypted virtual tape can be encrypted by the drive.

- Migrating a virtual tape (stacked export)

  An encrypted virtual tape is migrated as-is; that is, the data remains encrypted when it is migrated to physical tape.

- Compressing data

  If enabled, data compression occurs before encryption.

- Updating metadata, timestamps, and file sizes

  Every virtual tape stores header information called metadata, which is used by SPHiNX to retain an audit trail of information about the tape. When a tape is encrypted, the metadata is not encrypted. The following timestamps are associated with virtual tapes: modify, access, and change. The modify timestamp is not updated when a tape is encrypted or decrypted. However, the access and change timestamps are updated when a tape is encrypted or decrypted.

  Finally, when a virtual tape is encrypted, its file size changes because the key ID and other encryption metadata is added to the virtual tape.

The **SecureVTS.log** file, which resides in **/usr/local/tape/log/**, stores an audit trail of all encryption operations.

Multi-server considerations

Keep the following in mind when configuring and using Data Encryption in an environment with multiple SPHiNX servers, such as if the Clustered Option (GFS) or Data Replication is configured:

- Server configuration

  When configuring key servers and backup hosts for Data Encryption, it is *highly* recommended that you configure only one key generator for the environment. You must also configure at least one other server in the environment that can serve as the backup host for the key database. See "Adding a key server" on page 90 and "Adding a key database backup host" on page 91 for more information.

  If virtual tapes are stored on a remote server, such as through the use of Data Replication, and you need to access the data on tapes, Data Encryption must be enabled on the remote server. This will enable the remote server to decrypt encrypted tapes when necessary. Otherwise, the remote server cannot retrieve the key from the key server that encrypted the tape.

- Tape operations performed on encrypted virtual tapes

  SPHiNX attempts to decrypt an encrypted tape when a tape operation, such as mounting the tape, is performed on that tape. If Data Encryption is not enabled or the key server that was used to encrypt the tape is not configured on the server where the encrypted tape resides, the tape operation will fail and an error message will be displayed indicating that the operation failed. See "Data Encryption and failed tape operations" on page 163 for an explanation of the possible failures.

- Upgraded installations

  Beware of using Data Encryption in an environment where some SPHiNX servers are upgraded and others are not. *It is highly recommended that you* ***do not use Data Encryption in a mixed environment****.*

Configuring Data Encryption

This section provides the procedures needed to configure Data Encryption.

Prerequisites for configuration

Before you begin, ensure the connection between the host and SPHiNX servers is secure. Then, ensure that the connection between the SPHiNX server and the physical drive or library is secure if you want to export

encrypted virtual tapes. You may also want to gather the following information to expedite the configuration process:

- Username and password of a SPHiNX user account that belongs to the Administration group.
- If multiple SPHiNX servers are installed, gather the following:
  - Hostname or IP address, username, and password of the SPHiNX server that will be configured as the key generator, which will generate keys when virtual tapes and pools need to be encrypted and decrypted.
  - Hostname or IP address, port, username, and password for configuring a backup host that will be used by the key generator to store a backup of the key database; this host must support the Secure Copy (SCP) protocol, through the use of the scp or scp2 program.

Adding a key server

A key server is embedded in every SPHiNX server and, by default, each SPHiNX server is configured to generate keys. This type of key server is referred to as a “key generator”. When a key is generated, the key ID is stored with the encrypted virtual tape and the key is stored in a key database on the key generator.

If a key generator is reconfigured to no longer generate keys, it is then referred to as a “non-key generator”. The key database remains on the non-key generator, but that server no longer creates keys.

When a virtual tape needs to be decrypted, SPHiNX retrieves the encryption key from the key server that generated the key. If the key generator was reconfigured as a non-key generator, SPHiNX must still have access to that key server.

If there are multiple SPHiNX servers in your environment, you must designate only one server as the key generator. For a detailed procedure see section To add a key server.

Any time a key is stored in the key database, the database is backed up locally and on a backup host, which must be configured as described in Adding a key database backup host. In general, the key database (and its backup) remains small, typically around 10MB when storing thousands of keys.

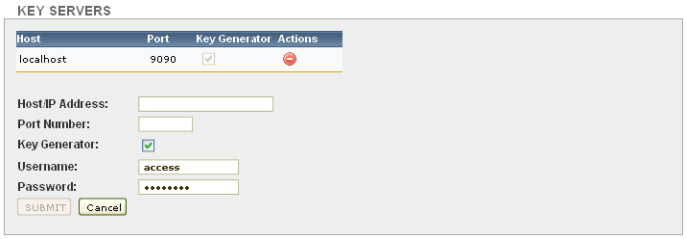
Note You cannot modify a key server after it is added. To change the settings, you must delete the key server and then add it again.

To add a key server

 *Requires Administration group membership*

1. Click **Configuration > Data Encryption** on the navigation pane.
2. If necessary, log in using an account that is a member of the Administration group. Click the **Log In** button at the top of the page and enter a username and password.

3. Click **ADD NEW SERVER** in the KEY SERVERS section of the page. The following is displayed:



4. In the **Host/IP Address** field, type the hostname or IP address of a SPHiNX server in your environment that you would like to designate as a key server. If there is no tape encrypted with that localhost, simply delete the local host entry.
5. In the **Port Number** field, type the port number of the key server, which is 9090 by default.
6. Select the **Key Generator** checkbox to enable the key server to generate keys. If you do not select this checkbox, the key server can only be used to return keys from its database that were previously used to encrypt virtual tapes.
7. In the **Username** field, type the username of the account that can access the SPHiNX server. By default, the bill user is configured on each SPHiNX server.
8. Type the password of the specified user in the **Password** field.
9. Click **SUBMIT**.

After you add a key generator and a key database backup host (other than localhost), allow **five minutes** for the key generator to create the first set of keys and key IDs. Key IDs may not be available until after this initial time period.

Modifying Data Encryption in a multi-server environment

If you need to change or reconfigure the key server and there are multiple SPHiNX servers in your environment, contact ETI\SPHiNX support.

Adding a key database backup host

By default, each SPHiNX server is configured as its own backup host. You must configure at least one other backup host on the key generator. The key server backs up the key database to the localhost and all defined backup hosts every time a new key is generated. (Keys are not available for use until the key database is successfully backed up to the localhost and at least one other backup host.)

It is highly recommended that you configure at least one other backup host that is not in the SPHiNX environment. An off-site backup host ensures that data is safe in case of unrecoverable failures in the SPHiNX environment.

Note You cannot modify a key database backup host after it is added. To change the settings of a backup host, you must delete it and then add it again, specifying the correct parameters. See Deleting a key database backup host for instructions on deleting a backup host.

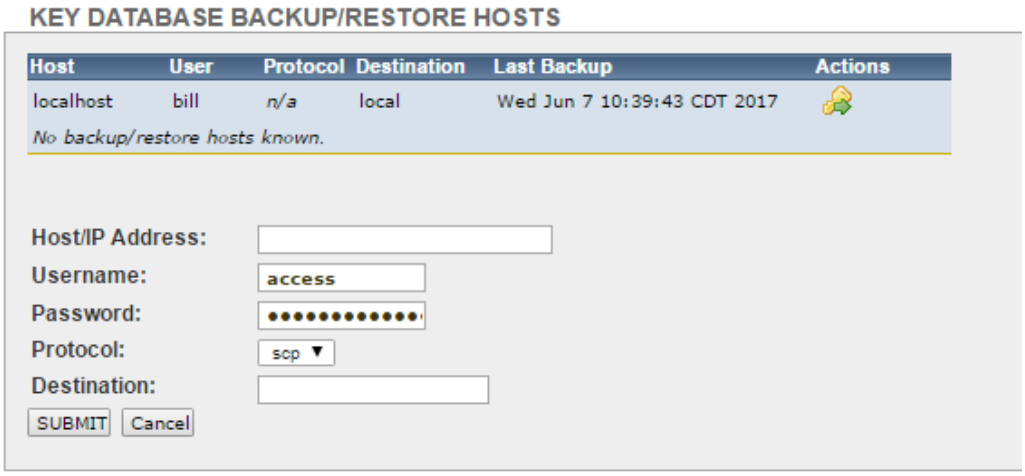
Before beginning

To configure a server as a backup host, the server must support SCP, either through the use of the scp or scp2 program. The scp program is installed on every SPHiNX server. If you use a non-SPHiNX server as a backup host, make sure SCP is supported.

To add a backup host

Requires Administration group membership

1. Click **Configuration > Data Encryption** on the navigation pane.
2. If necessary, log in using an account that is a member of the Administration group. Click the **Log In** button at the top of the page and enter a username and password.
3. Click **ADD NEW HOST** in the KEY DATABASE BACKUP/RESTORE HOSTS section of the page. The following is displayed:



4. In the **Host/IP Address** field, type the hostname or IP address of a server that SPHiNX will use as a backup host for the key database.
5. In the **Username** field, type the username of a user account that can access the SCP program on the specified server.
6. Type the password of the user account in the **Password** field.
7. Select a protocol from the **Protocol** drop-down list.
8. In the **Destination** field, type a path and file name to the file that will store the key database. If the file does not exist, SPHiNX will create it. If you do not specify a fully qualified path, the path and file are created in the specified user's home directory.
9. Click **SUBMIT**.

When you add a backup host, SPHiNX immediately sends a copy of the local key database to the host. This tests the connection to the host and validates the host parameters that you specified. If a copy of the key database exists on the target host, it is overwritten.

14 Creating and Managing Virtual Media

SPHiNX organizes data in vaults, which are defined for you. Vaults contain pools, and pools contain virtual tapes. You can create, modify, and delete pools. You can perform the following on virtual tapes:

- Mount and unmount
- Encrypt and decrypt, if Data Encryption is licensed
- Export to physical tape (tape-to-tape export and stacked tape export)
- Replicate or export to a remote host, if Data Replication is configured
- Import from physical tape, from a remote host, a physical tape drive, or a physical library
- Erase
- Delete

You can also manage virtual tape locks. And, of course, you can backup and restore virtual tapes from the host server, though these procedures are not provided here.

This chapter describes how to manage and use pools and virtual tapes.

Note Be sure to display the online help; click **About** on the navigation pane of the web interface and then click the **Help Set** link in the Product Documentation section of the About page. Full details are provided in the help and are necessary to complete the procedures in this chapter.

Creating a pool

Pools enable you to group virtual tapes and then set attributes on all tapes in the pool, such as policy, encryption, autoloading, and size limits. When you create a new pool, a directory of the same name is created in the chosen vault (/VAULT0*x*/*pool_name*) and all associated virtual tapes are stored in the directory.

After you create pools, you can view them in their respective vaults in the Storage Report.

Note Vaults are used for storing pools only; SPHiNX uses vaults for virtual tapes and VTD components exclusively. Files and applications should be installed in other storage locations, such as the root partition.

Before beginning

- Verify that a vault is available for storing data. Customer data should not be stored on VAULT00, which should be reserved for system maintenance. If VAULT00 is the only vault available, it is

recommended that you attach an external storage device for use in storing data. See the *Quick Start Guide* for cabling instructions and then refer to "Reconfiguring Vaults" on page 18.

To create a pool

Requires Administration, Operations, or Supervisor group membership

Now, you should create virtual tapes in the pool and define policies for the pool.

To rename a pool:

1. Click **Configuration > Tapes and Pools** on the navigation pane.

2. In the Actions column of the pool you want to rename, click on the to edit its properties. Change the name of the pool by entering a new name in the appropriate field.

To move a pool to anew vault:

You may need to move a pool to a new vault. (View the Storage Report for a list of pools in each vault.)

1. Click **Configuration >Tapes and Pools** on the navigation pane.
2. Click next to the pool you want to move.
3. Select a new vault from the **Vault** drop-down list.
4. Click **Save**.

Note: When moving a pool from one VAULT to another and the source VAULT is NFS type, it is possible that the source VAULT would temporarily keep an empty file with the name of the moved pool. Delete the empty file. Note that the pool and all its virtual tapes have been successfully moved to the new VAULT.

Related Topics

Administering virtual media
Managing virtual tapes and pools
Managing virtual tapes

Configuring policy

Policies enable you to configure automation. For example, you can replicate and export a tape after it is unmounted using policy. In this scenario, you would apply two policies to the pool that contains the tape: one that performs a replication after the tape is successfully unmounted and one that performs a stacked export after the tape is successfully replicated.

The Configure Policies page enables you to create, edit, and delete policies. After creating a policy, you can edit it to change the pools to which it is applied and to enable or disable it as needed.

Keep the following in mind when creating policies:

- Each policy is applied to one or more pools, so the policy action is performed on all virtual tapes within the pools associated with the policy (after the specified event completes successfully).
- You must set the Trigger Policy If Enabled option when configuring jobs; jobs are responsible for performing policy actions. For example, a replication jobs and a stacked export job must exist and the Trigger Policy If Enabled option must be set on the jobs to accomplish the scenario described above.
- You cannot create multiple policies that are initiated by the same event *for the same pool*. For example, you cannot replicate and export a tape in PoolA after the tape is unmounted.
- You cannot define different policy attributes if multiple policies trigger the same action *for the same pool*. For example, you cannot replicate to HostA and HostB after tapes in PoolA are unmounted.
- Be careful not to create "circular" policies, such as if PolicyA triggers a stacked export after replication and PolicyB triggers replication after a stacked export. These policies will trigger each other indefinitely.
- If a policy is disabled, it cannot trigger actions. You must enable a policy to allow SPHiNX to perform an action after the specified event occurs.

Events that trigger policy actions

- export (by tape-to-tape or stacked export job)
- replication
- import (from a tape device or replication target)
- encryption
- decryption
- unmount

Note that an event must complete successfully to trigger a policy action.

Actions that can be triggered

- stacked export
- tape-to-tape export
- replication to a target

- remote export
- mount
- insert into VTL
- encryption
- erasure
- import from a tape device
- import from a replication target

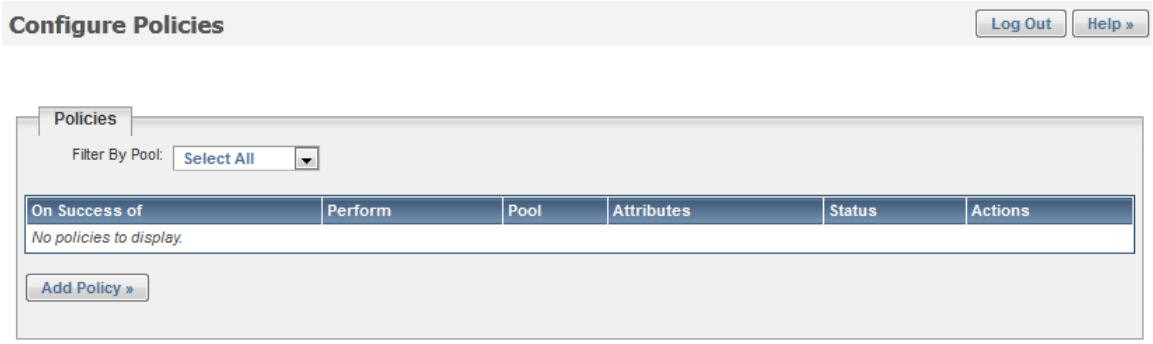
Before beginning

- Create one or more pools to which the policy can be applied.

To create a policy

Requires Administration, Operations, or Supervisor group membership

1. Click **Configuration > Policies** on the navigation pane. The Configure Policies page is displayed.



2. Click **Add Policy**.
3. From the **On Success Of** drop-down list, select the event that must complete successfully to trigger the policy action.
4. Select the policy action from the **Perform** drop-down list.
5. Choose the pools to which this policy applies from the **Pool Selection** list.
6. For most policy actions, you must configure attributes in the **Policy Attributes** section of the page:
   - If you chose Tape-to-Tape Out, select the library or drive to which the tape will be exported, the export format (SPHiNX or host-native), and whether the tape will be encrypted when exported.
   - If you chose Remote, select the remote server to which the tape will be exported. If you select the Skip If Unchanged option, the virtual tapes are not exported if their contents have not changed. (Stated differently, the virtual tapes are exported only if their contents have changed when the unmount occurs, if this option is selected.)
   - If you chose Replicate (export), select the remote server to which the tape will be replicated.

- If you chose Tape-to-Tape In, select the library or drive from which the data or tape will be imported.
- If you chose Replicate (import), select the remote server from which the tape will be imported.
- If you chose Mount, select the standalone VTD where the tape will be mounted and whether the tape will be mounted as read-only.
- If you chose VTL-Insert, select the target VTL.

Be careful when defining attributes if multiple policies trigger the same action for the same pool. Attributes for existing policies *are overwritten* (for policies that trigger the same action for the same pool.)

7. Enable the policy if you want SPHiNX to begin evaluating events and trigger policy actions. You can leave the **Enable** checkbox unchecked if you want to leave the policy disabled for now.
8. Click the **Save** button.

Now, verify that jobs are configured and the Trigger Policy If Enabled attribute is set.

Managing virtual tapes

This section describes how to perform actions on virtual tapes:

- Creating virtual tapes
- Inserting virtual tapes into a VTL
- Mounting and unmounting virtual tapes
- Encrypting and decrypting virtual tapes
- Exporting virtual tapes
- Restoring data
- Erasing and deleting virtual tapes
- Managing locks on virtual tapes

Note If an unexpected power loss or shutdown occurs, data may not be written to virtual tapes that were mounted. It is recommended that you rerun jobs for virtual tapes that were mounted during the power loss or shutdown, to ensure that data is written to the virtual tapes as expected.

Creating virtual tapes

You must create a virtual tape before the host server can mount and write data to it. When you create a virtual tape, a file is created on the SPHiNX server's disk. The file is empty except for up to 27MB of header information (metadata), which is used by SPHiNX to retain an audit trail of information, including the following:

- Tape label information, such as the volume label
- When the virtual tape was created, written to, updated, mounted, unmounted, or erased
- If and when the virtual tape was exported, imported, migrated, or restored

- How long the virtual tape has been retained
- The ID of the key used to encrypt the tape, if Data Encryption is enabled and the tape is encrypted

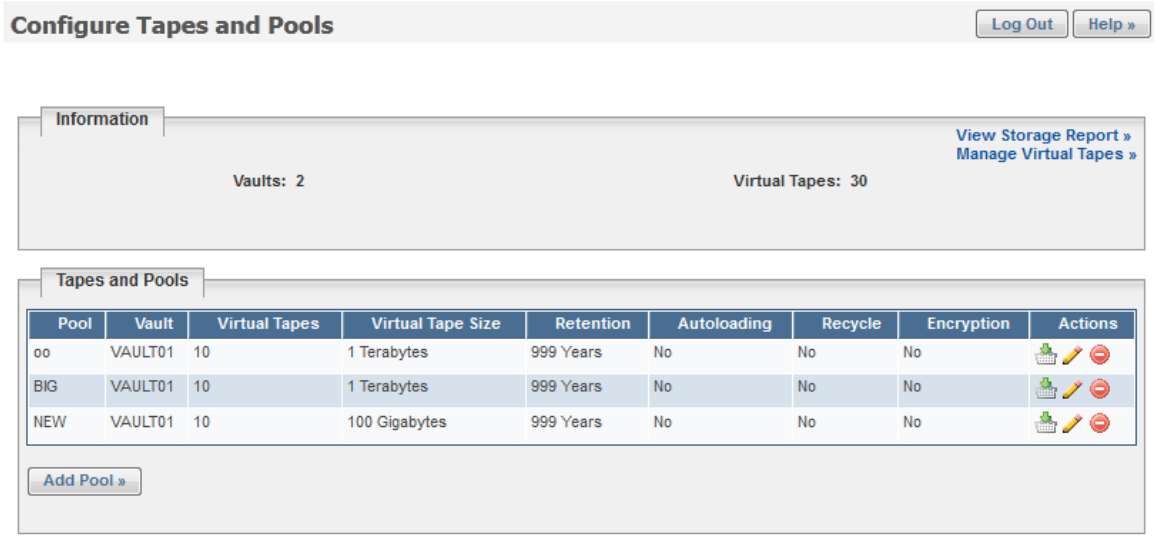
Before beginning

- Verify the name(s) of the tape(s) on the host server. It is recommended to use consistent naming on the SPHiNX and host servers. For example, specify VTAPE1 on the SPHiNX server if the tape is named TAPE1 on the host server.
- Be sure that virtual tape names are unique across all pools on the SPHiNX server and all SPHiNX servers in the environment. (Think of virtual tape names as you would physical tape barcodes; duplicates are not supported.)
- If you intend to export a tape to a physical tape in an external drive or library (tape-to-tape export), be sure the barcode of the virtual tape does not include more than six characters. If you attempt to export a tape with an eight-character barcode (which includes a two-character density, such as L4 or L5), SPHiNX truncates the barcode, using only the first six characters.
- Create a pool in which the virtual tape(s) will reside. See "Creating a pool" on page 93 for details.

To create one or more virtual tapes within a pool

 *Requires Administration, Operations, or Supervisor group membership*

1. Click **Configuration > Tapes and Pools** on the navigation pane. The Configure Tapes and Pools page is displayed.



2. Click  next to the pool in which the virtual tape(s) will be created.
3. In the **Virtual Tape Name/Prefix** field, type the name for the virtual tape or, if creating multiple tapes, type a string that will be used as the base of the tape names. The name on the virtual tape should match the name used the host server if the tape will be used in a VTL. This is because SPHiNX will use the tape name as the barcode. Virtual tape names can be up to 6 characters in length (total).

Note The names applied to virtual tapes are not tape labels. They are equivalent to the stick-on labels applied to physical tapes. Also, be aware that you cannot change a virtual tape's name after it is created.

4. In the **How Many?** field, type the number of tapes to create.
5. In the **Start At** field, indicate where numbering begins. For example, if you enter **VT** in the Prefix field and enter **2** here, the first tape created is named VT0002.
6. Click **Save**.

To label virtual tapes

After creating pools and virtual tapes, you may need to label the virtual tapes if required by the host server. Refer to the host server documentation for complete labeling instructions.

1. Configure SPHiNX to automatically load and unload virtual tapes as they are used, from the first to the last virtual tape in the pool. See the help topic and select the **Autoloading** checkbox.
2. Manually mount the first tape in the pool as described in "Mounting and unmounting virtual tapes" on page 100.
3. On the host server, label the virtual tape.

   Some hosts have a method for sequentially labeling tapes. If your host server has this ability, a sequence can be labeled consecutively, thereby allowing SPHiNX to progress through the tapes in the pool. The host server will unload the tape after labeling it, and SPHiNX will load the next tape in the pool. If you label all tapes in the pool, the host server will unload the last tape that was labeled.
4. Modify the pool again to disable autoloading.

To verify virtual tapes are available to the host server

To verify that a tape is available on SPHiNX, check the Data Size on the Manage Virtual Tapes page. This column indicates whether a tape is unlabeled (empty) and indicates the data capacity that is used after a backup runs. (If a labeled tape is erased, the value in this column returns to 0.) If you click the name of the virtual tape (link), a pop-up dialog box is displayed listing tape data.

Inserting virtual tapes into a VTL

You can move virtual tapes from the shelf, where they are placed after creation, to a VTL. (The shelf contains virtual tapes that are not associated with a VTL.)

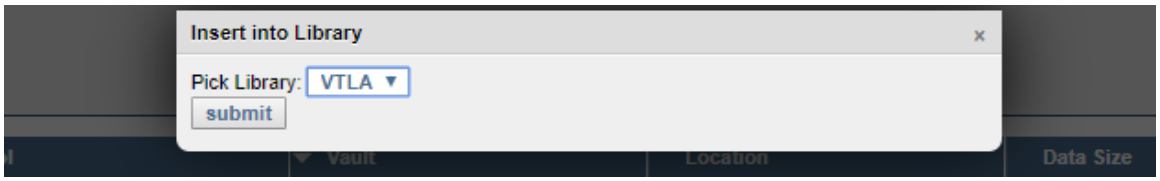
Before beginning

- Make sure empty slots are available in the VTL.
- Be aware that you must insert the tapes in the order they should be rotated. If all tapes are inserted at once, they are placed in alphabetical order.

To add virtual tapes to a VTL

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. From the **Filter By Location** drop-down list, select **Shelf**.
3. Choose the virtual tapes you want to add to the VTL by selecting/ check-marking them in the table.

4. Select **Insert into library** from the **Bulk Actions** drop-down list above the table, on the left side of the page.



5. Select the target VTL.
6. Click **submit**.

Mounting and unmounting virtual tapes

To mount a virtual tape in a standalone VTD, you must create a mount job. You can run the job immediately after creating it, or you can schedule a mount job, such as if a VTD is currently reserved but will be available at a future time. Then, to backup to the mounted virtual tape, use the backup software you normally use to perform a backup to the mounted VTD.

Note You can automate mounting using the Event Management System; see Configuring EMS Communication.

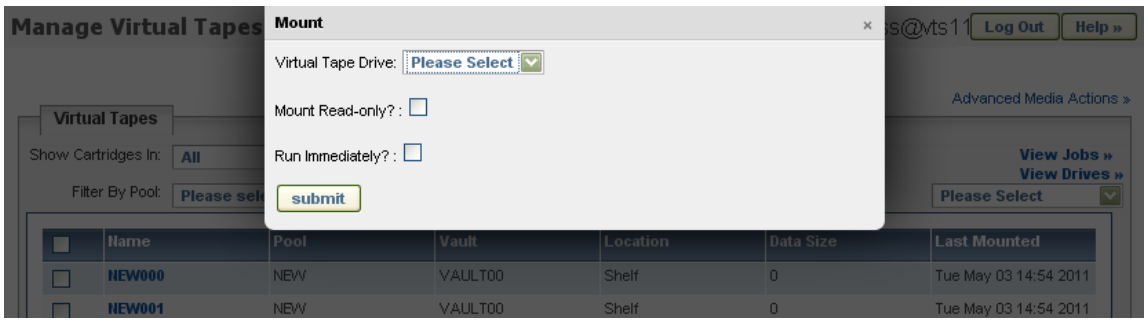
When you mount a virtual tape, keep the following in mind:

- The virtual tape's modification date is not updated; the ctime (inode change time) is updated.
- If Data Encryption is enabled and the virtual tape is encrypted, the data on the tape is decrypted when it is read. The data on the virtual tape remains encrypted. Refer to "Enabling and Configuring Data Encryption" on page 87 for more information about this feature.

To mount a virtual tape

Requires the Mount Cartridges, Vault Access, and Access to all Vaults access rights

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Click, in the **Action** column, on the mount button next to the tape(s) you want to mount.



3. When prompted, select a VTD from the **Virtual Tape Drive** drop-down list. Only available drives are listed, though the drive must be available when the job runs (if it is scheduled).
4. If you want to mount the tape for read-only purposes, select the **Mount Read-only?** option.
5. To mount the virtual tape immediately after creating the job, select **Run Immediately?**.

6. Click **submit**.
7. Schedule the job, if necessary.

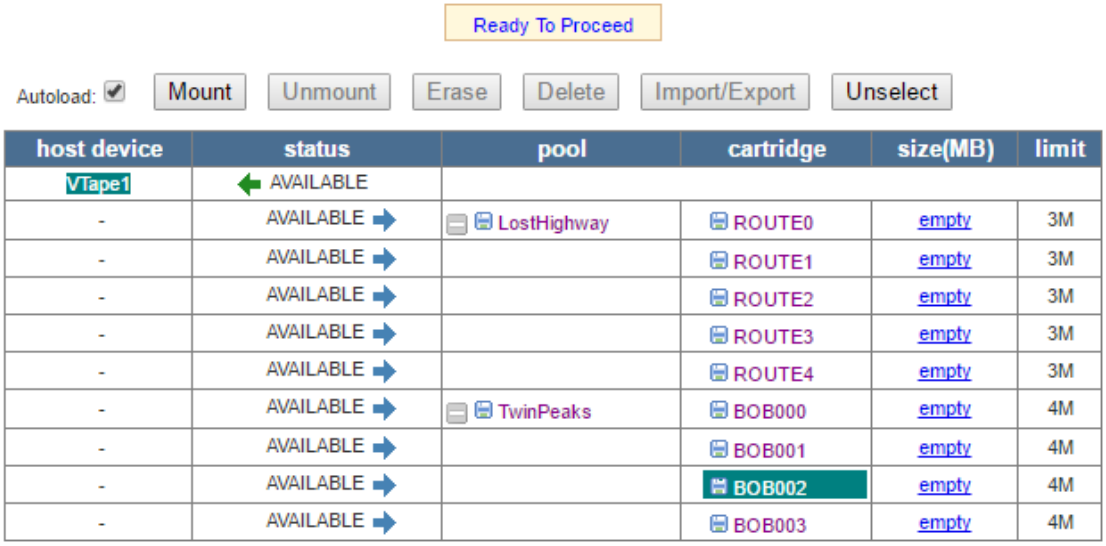
To verify that the tape was mounted, view the Manage Drives page. Navigate to the System Status page to verify that data is being written to the tape. After the data is written, view the Manage Virtual Tapes page again to verify the data size. You can also unmount a virtual tape from a standalone VTD.

If you cannot mount an encrypted tape, it may be that the certificate used by the Encryption feature has expired. See Regenerating a key server's certificate for more information.

To mount a virtual tape and monitor the progress of a backup

Use this procedure if a VTD license is enabled on the server.

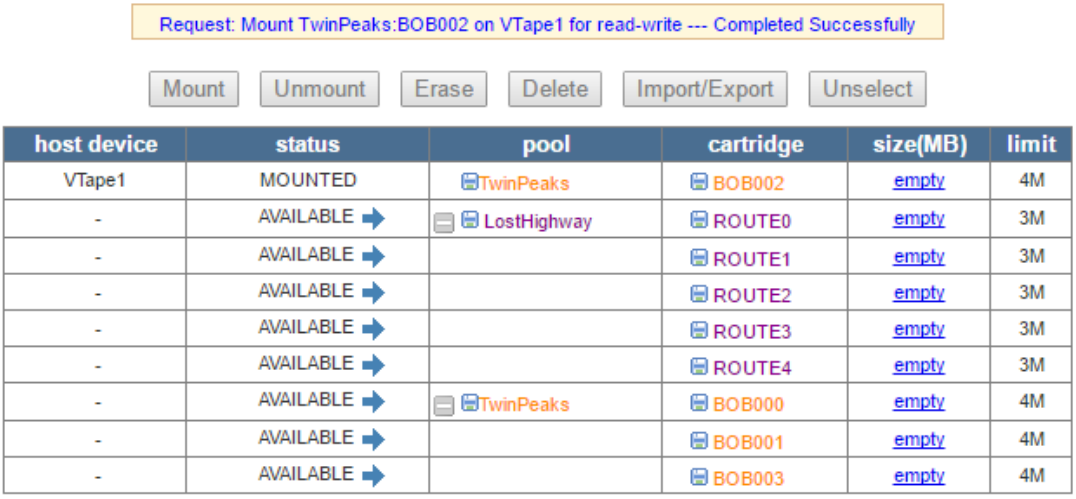
1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Click the **Advanced Media Actions** link on the upper right side of the page.
3. Select the host device (in the respective column) where the virtual tape will be mounted. If you select a host device on which a virtual tape is mounted, the currently loaded virtual tape is unmounted.
4. Select the virtual tape to mount. In the following screen shot, the DF0000 virtual tape will be mounted on the VF40500 host device:



5. Click **Mount**.

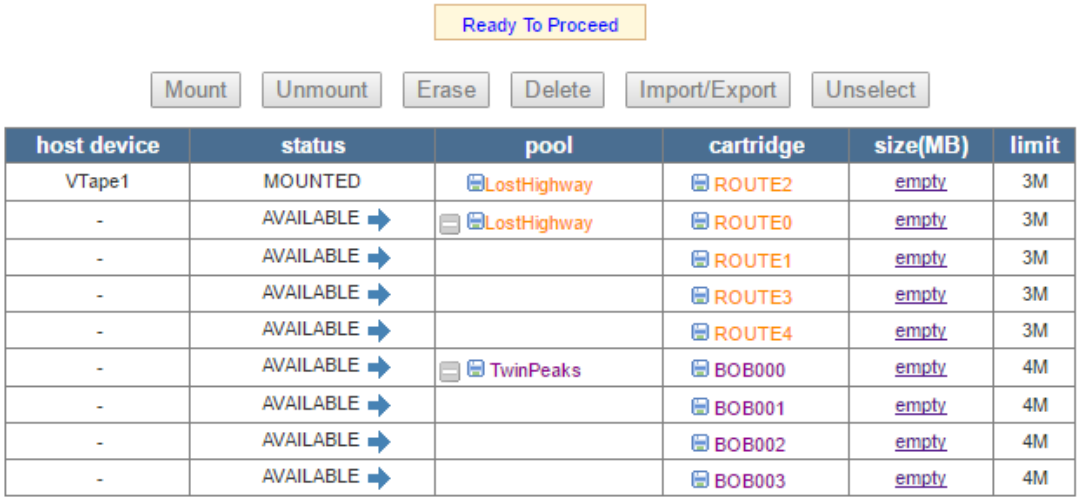
   Note If the Mount button is not displayed, see "Configuring Web Interface Preferences" on page 135 for information about displaying this button. Also, if you cannot click the Mount button, maximize your browser; this should display an arrow cursor and enable you to click the button. See the Release Notes for more information.

6. On the pop-up dialog, click **Read/Write** to mount the virtual tape for read and write operations, or click **Read Only** to mount the tape for read operations only. SPHiNX mounts the virtual tape on the selected virtual tape drive.



If the mount fails, see "Managing locks on virtual tapes" on page 113 for more information.

7. After the backup begins, you can monitor the progress from the Virtual Media - Operation page. In the kb/sec and size(MB) columns, you can see the megabytes that have been backed up and the backup rate.



After the backup completes, you can verify that the size of the virtual tape has changed. You can also monitor progress from the System Status page, which shows the current transfer rate (if enabled).

When the backup is finished, SPHiNX unloads the virtual tape. If the pool was configured to autoload virtual tapes, it mounts the next virtual tape (in alphabetical order) in the pool.

Viewing mounts

If EMS was enabled, the process of mounting virtual tapes is automated; the NonStop server can initiate mounts and dismounts. (For details, see Configuring EMS Communication.) When SPHiNX detects a mount

request, it checks to see if the requested virtual tape resides on a RAID array connected to SPHiNX. If it does, that virtual tape is mounted on the device specified by the mount request. If no device is specified in the backup command, the first available virtual tape drive connected to that host is used. After the virtual tape is mounted, the backup proceeds automatically.

The Virtual Media - Mounts and Locks page enables you to monitor mount activity.

Unmounting virtual tapes

To unmount a virtual tape

 *Requires the Mount Cartridges, Vault Access, and Access to all Vaults access rights*

Use this procedure if a capacity license is enabled on the server.

1. Click **Administration > Virtual Drives** on the navigation pane.
2. Click ⏏ next to the drive that contains the virtual tape you want to unmount.

Use this procedure if a VTD license is enabled on the server.

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. Click the Advanced Media Actions link in the upper right corner of the page.
3. Select the host device where the virtual tape is mounted.
4. Click **Unmount**.

Encrypting and decrypting virtual tapes

You can encrypt virtual tapes individually or you can encrypt a pool, which instructs SPHiNX to automatically encrypt virtual tapes when they are added to the pool.If you encrypt a pool, all virtual tapes in the pool are encrypted when they are created. If virtual tapes exist in the pool when the pool is configured for encryption, you can specify whether they should also be encrypted.If virtual tapes exist in a pool before the pool is encrypted, you can choose whether to encrypt the existing virtual tapes.

You can also decrypt virtual tapes after they are encrypted.

Encrypting virtual tapes

Before beginning

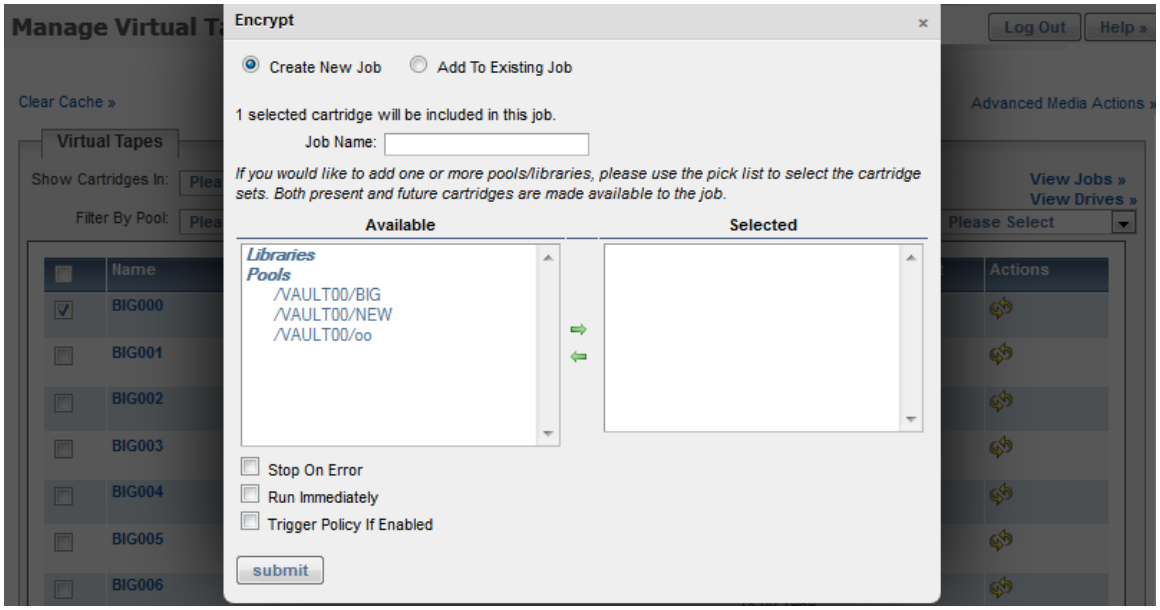
- Refer to "Enabling and Configuring Data Encryption" on page 87 in the *Configuration Guide* to enable and configure this feature.
- If a virtual tape contains the maximum amount of data, encrypting the tape will cause the tape limit to be exceeded. Make sure there is space on the tape before encrypting it.

To encrypt one or more virtual tapes

 *Requires Administration group membership*

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. From the **Filter by Location** drop-down list, select **Shelf** or **All**. Or simply choose the virtual tapes you want to encrypt by selecting them in the table.

3. Select **Encrypt** from the **Bulk Actions** drop-down list above the table, on the left side of the page. If the **Encrypt** option is not available in the list, you have to enable and configure data encryption feature. Refer to "Enabling and Configuring Data Encryption" on page 87 in the *Configuration Guide* to enable and configure this feature. The following is displayed:



4. On the pop-up dialog, select the **Create New Job** option.
5. Specify a job name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed. If you leave this field blank, a name is generated for you.
6. To choose pools to encrypt (in addition to those selected on the Manage Virtual Tapes page), move pools from the **Available** list to the **Selected** list. Or, remove tapes or pools by moving them from the **Selected** list to the **Available** list. Use the ➡ and ⬅ buttons to move items to and from the lists.
7. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to encrypt all virtual tapes.
8. Select the **Run Immediately?** option to run the job immediately after it is created. Do not select this option if you want to create a schedule for the job.
9. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.
10. Click **submit**.
11. Create a schedule for the job, if necessary.
12. To schedule the Encrypt job, you must create a schedule that is associated with the job.
    a. Click **Administration > Jobs** on the navigation pane.
    b. On the Manage Jobs page, click next to the job you want to schedule. The Manage Schedules page is displayed.

c. Click **Add Schedule**.

d. In the Create Schedule area, select how often you want the job to occur:
   - One time — Runs the job once. You must select a start date and time.
   - Weekly/Daily — Runs on the days you select. You must select the days and a start date and time.
   - Monthly — Runs on a specific date each month. Select a date and start time.

   If you specify a date that does not exist in a month, the job will run on the last day of the month.

e. Click **Save**.

After the job runs, you can return to the Managed Schedules page for its status. If a problem occurred, the Last Run column will display “Failed”.

If data is stored on the virtual tape, it is encrypted. If the virtual tape is empty, data will be encrypted as it is written to the virtual tape.  is displayed next to the tape name on the Manage Virtual Tapes page after the virtual tape is encrypted.

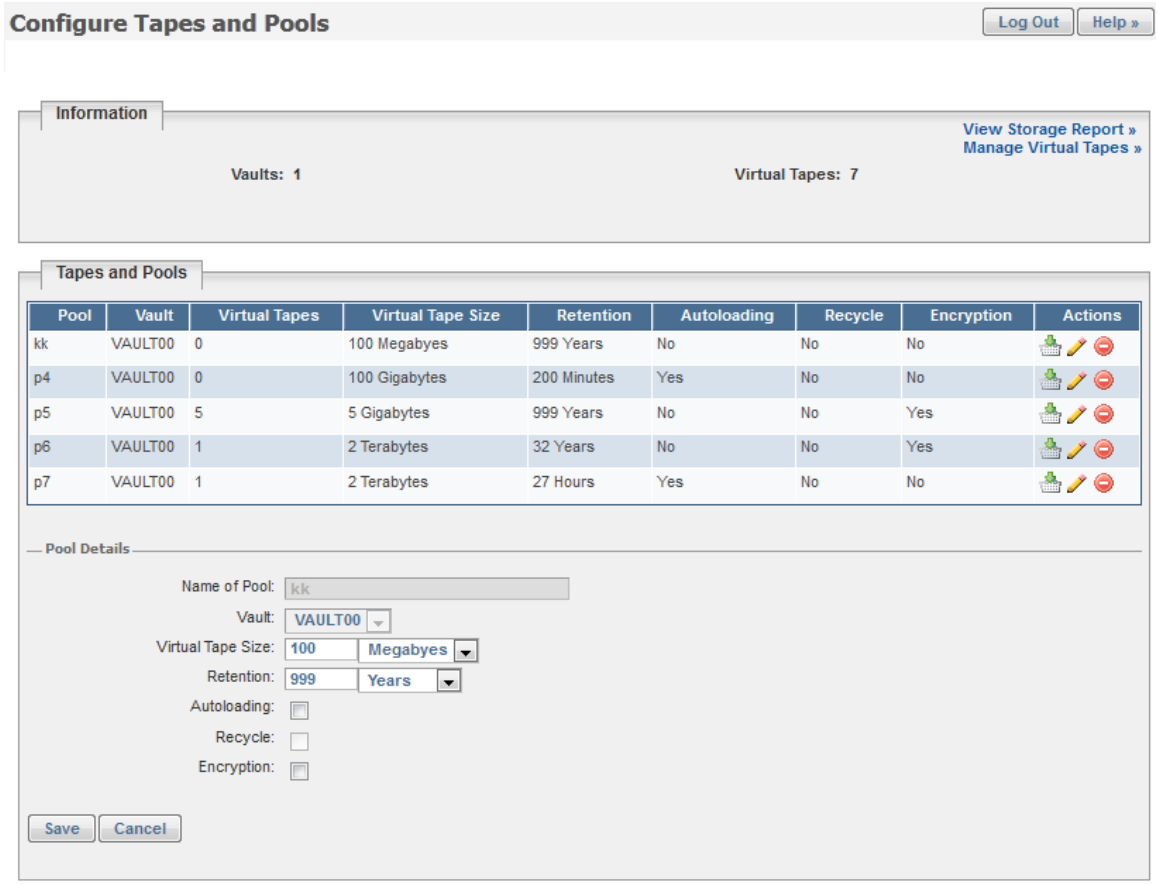
To encrypt all virtual tapes in a pool

 *Requires Administration, Operations, or Supervisor group membership*

If a pool contains virtual tapes and then you edit the pool to encrypt tapes in the pool, SPHiNX creates a job to encrypt the existing tapes.

Note To encrypt a pool when it is created, see "Creating a pool".

1. Click **Configuration > Tapes and Pools** on the navigation pane.
2. Click ✎ next to the pool you want to encrypt. The following is displayed:



3. Select the **Encryption** checkbox. (This option is not available if you have not enabled Data Encryption or if you have not logged in.)
4. Click **Save** .

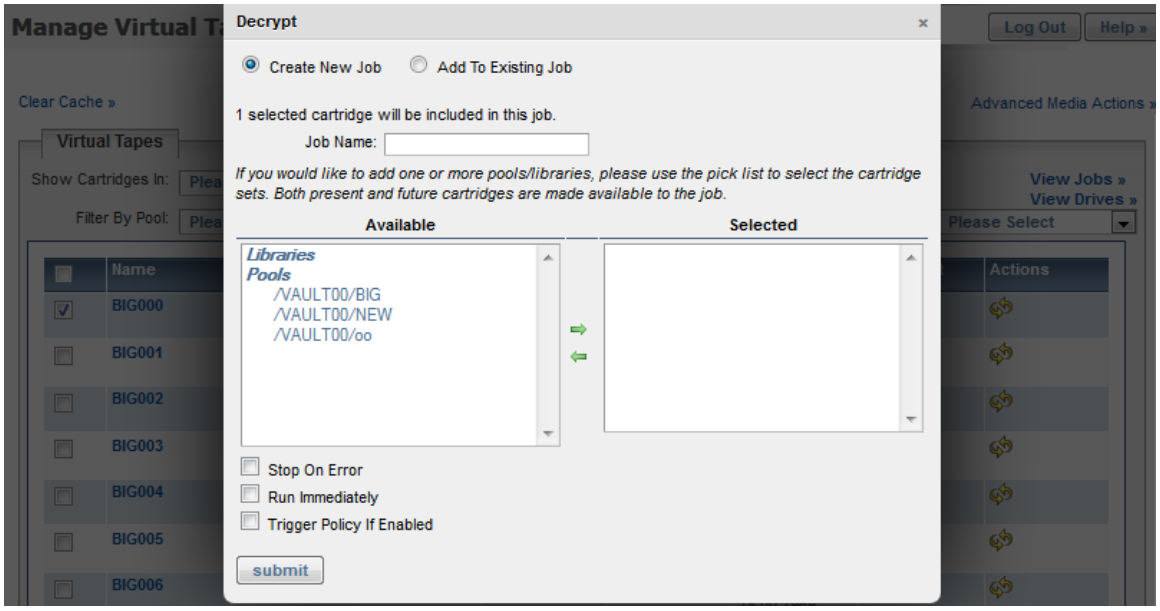
is displayed next to the virtual tape names on the Manage Virtual Tapes page after the virtual tapes are encrypted.

Decrypting virtual tapes

To decrypt one or more virtual tapes

Requires Administration group membership

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. From the **Filter By Location** drop-down list, select **Shelf** or **All**. Or simply choose the virtual tapes you want to decrypt by selecting them in the table.
3. Select **Decrypt** from the **Bulk Actions** drop-down list above the table, on the left side of the page. The following is displayed:



4. On the pop-up dialog, select the **Create New Job** option.
5. Specify a job name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed. If you leave this field blank, a name is generated for you.
6. To choose virtual tape libraries or pools to decrypt (in addition to those selected on the Manage Virtual Tapes page), move libraries or pools from the **Available** list to the **Selected** list. Or, remove tapes or pools by moving them from the **Selected** list to the **Available** list. Use the and buttons to move items to and from the lists.
7. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to decrypt all virtual tapes.
8. Select the **Run Immediately?** option to run the job immediately after it is created. Do not select this option if you want to create a schedule for the job.
9. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.
10. Click **submit**.
11. Create a schedule for the job, if necessary.
12. To schedule the Decrypt job, you must create a schedule that is associated with the job.
    a. Click **Administration > Jobs** on the navigation pane.
    b. On the Manage Jobs page, click next to the job you want to schedule. The Manage Schedules page is displayed.
    c. Click **Add Schedule**.

d. In the Create Schedule area, select how often you want the job to occur:
   - One time — Runs the job once. You must select a start date and time.
   - Weekly/Daily — Runs on the days you select. You must select the days and a start date and time.
   - Monthly — Runs on a specific date each month. Select a date and start time.

   If you specify a date that does not exist in a month, the job will run on the last day of the month.

e. Click **Save**.

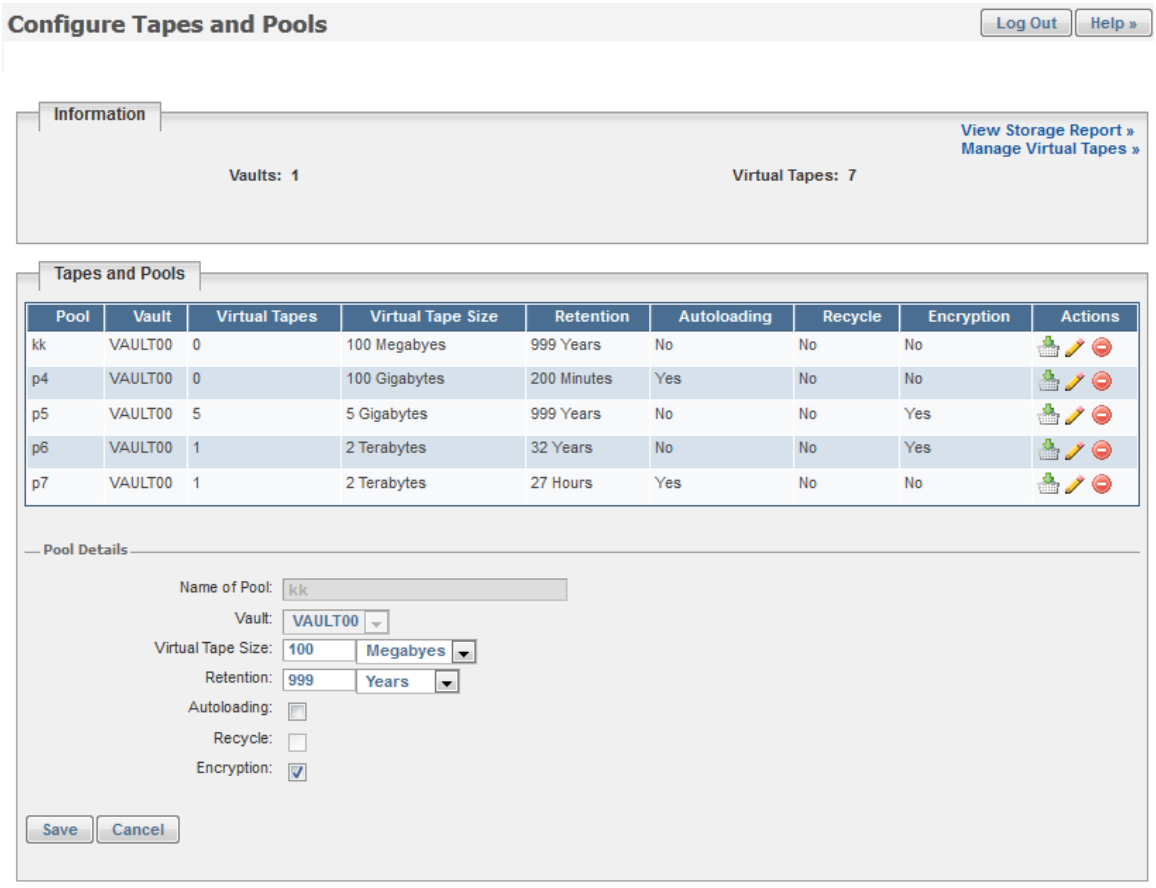
After the job runs, you can return to the Managed Schedules page for its status. If a problem occurred, the Last Run column will display “Failed”.

To decrypt all virtual tapes in a pool

Requires Administration, Operations, or Supervisor group membership

If a pool contains virtual tapes and then you edit the pool to disable encryption, SPHiNX creates a job to decrypt the existing tapes.

1. Click **Configuration > Tapes and Pools** on the navigation pane.
2. Click ✎ next to the pool you want to decrypt. The following is displayed:



3. Select the **Encryption** check-box to remove the checkmark.
4. Click **Save** .

Exporting virtual tapes

You can export data in the following ways:

- Export to a physical library or tape drive using a tape-to-tape export job to an external tape library or standalone drive. .
- Export a virtual tape to one or more physical tapes using a stacked export job. See "Enabling and Performing Stacked Exports" on page 51 for details.
- Export a virtual tape to a remote host (replication target) using a replicate job; the source server is the only server that can access the replicated tapes, and the replicated tapes are stored in data partitions (/DATAxx) on the remote server. See "Enabling and Configuring Data Replication" on page 60 for details.
- Exports a virtual tape to a remote SPHiNX server; the exported tapes are stored in vaults (/VAULTxx) on the remote server. See "Enabling and Configuring Remote Export" on page 70 for details.

Restoring data

You can restore data in the following ways:

- Import from a physical library; this is the reverse of a tape-to-tape export job to an external tape library and can be performed from the Manage External Data page of the web interface.

  or

  Import from a physical tape drive; this is the reverse of a tape-to-tape export to a standalone drive and can be performed from the Manage External Data page.

  Refer to "Enabling and Performing Tape-to-tape Exports" on page 45 for more information.
- Import from a physical library or drive, to import pre-existing tapes (dynamic import); perform this operation from the Manage External Data page. Refer to the online help for instructions.
- Import a virtual tape that was exported to one or more physical tapes; this is the reverse of a stacked export job and can be performed from the Configure Tapes and Pools page. See "Enabling and Performing Stacked Exports" on page 51 for details.
- Import a virtual tape on a remote host (replication target); this is the reverse of a replicate job and can be performed from the Manage External Data page. See "Enabling and Configuring Data Replication" on page 60 for details.

Erasing and deleting virtual tapes

Deleting a virtual tape removes it altogether and its data cannot be recovered. Be careful when deleting a virtual tape; its contents will no longer be available. To delete one or more virtual tapes, you must create a Delete job. The job runs immediately after it is created.

You can erase the contents of a virtual tape but leaves the metadata and ANSI label of the virtual tape file intact. When you erase a virtual tape, its modification date is not updated; the ctime (inode change time) associated with the virtual tape file is updated. To erase one or more virtual tapes, you must create an Erase job. The job runs immediately after it is created.

If Scan/Cleanup is enabled, you can configure SPHiNX to automatically erase virtual tapes after they are exported to tape by a stacked export job or after their retention periods expire. See "Enabling and Configuring Scan/Cleanup" on page 115 for more information about enabling and configuring Scan/Cleanup; using Scan/Cleanup is described below. See "Creating a pool" on page 93 for more information about setting retention periods.

Manually erasing a virtual tape using the web interface

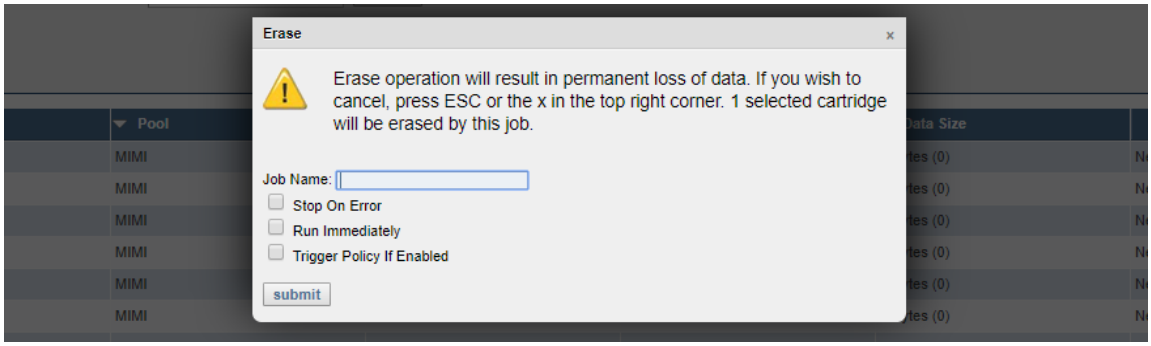
Before beginning

- Remove the virtual tape from the VTL, if necessary. Or, unmount the virtual tape, if it is mounted.

To erase a virtual tape

To erase an unencrypted virtual tape: Requires the Erase Cartridges, Vault Access, and Access to all Vaults access rights; also, requires Administration group membership if erasing an encrypted tape

1. Click **Administration > Virtual Tapes** on the navigation pane.
2. From the **Filter by Location** drop-down list, select **Shelf** or **All**. Or simply choose the virtual tapes you want to erase by selecting them in the table.
3. Select **Erase** from the **Bulk Actions** drop-down list above the table, on the left side of the page. The following is displayed:



4. Specify a job name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed.
5. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to erase all selected virtual tapes.
6. Select the **Run Immediately** option to run the job immediately after it is created.
7. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.
8. Click **submit** to create and run the Erase job.

Manually deleting a virtual tape using the web interface

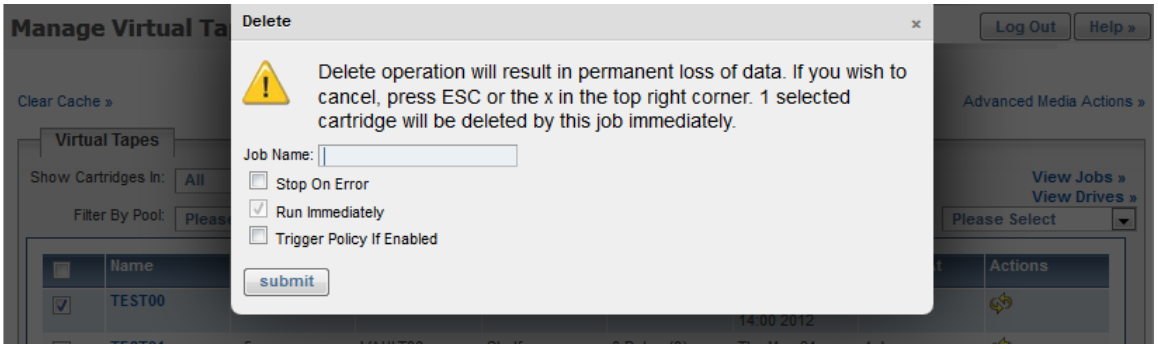
Before beginning

- If the virtual tape resides in a VTL, you must remove it from the VTL before you can delete it.

To delete a virtual tape

To delete an unencrypted virtual tape: Requires the Delete Cartridges, Vault Access, and Access to all Vaults access rights; also, requires Administration group membership if deleting an encrypted tape

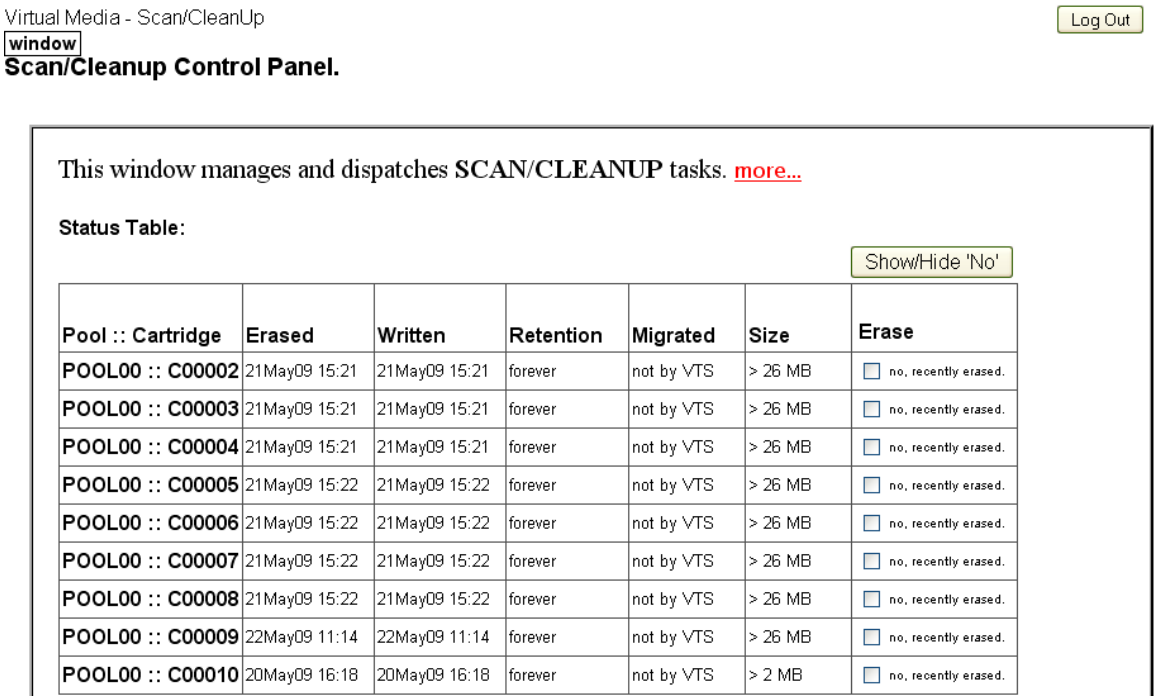
1. Click **Administration > Virtual Tapes** on the navigation pane.
2. From the **Filter by Location** drop-down list, select **Shelf** or **All**. Or simply choose the virtual tapes you want to delete by selecting them in the table.
3. Select **Delete** from the **Bulk Actions** drop-down list above the table, on the left side of the page. The following is displayed:



4. Specify a job name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed.
5. Select the **Stop on Error** option if you want to stop the job if an error occurs. Otherwise, the job will continue until SPHiNX has attempted to delete all selected virtual tapes.
6. Select the **Run Immediately** option to run the job immediately after it is created.
7. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.
8. Click **submit** to create and run the Delete job.

Automatically erasing a virtual tape using Scan/Cleanup

After you enable and configure Scan/Cleanup as described in "Enabling and Configuring Scan/Cleanup" on page 115, through the web interface, the Scan/Cleanup feature will be shown under **Configuration > Scan Cleanup** on the navigation pane. Click the **Show/Hide 'No'** button to display the cartridges:



To view the Status table

This table lists all virtual tapes on the system and their Scan/Cleanup status. The following is a description of each column:

Pool :: Cartridge — Displays the name of the pool and virtual tape.

Erased — Displays the timestamp when the virtual tape was erased.

Written — Displays the timestamp when data was last written to the virtual tape.

Retention — Specifies how long the virtual tape will be retained. A retention period specifies an expiration date and time, which governs when vault space can be reclaimed.

Migrated — Displays the timestamp when the virtual tape was backed up (typically to physical tape) by a backup management application. If the virtual tape was migrated by another application, **n/a** or **not by SPHiNX** is displayed.

Size — Displays the size of the virtual tape (in bytes). This reflects the size of the tape data; it excludes the size of the metadata (up to 27MB).

Erase — Indicates whether the virtual tape is selected for erasure or not. This column also provides an explanation of the business rule that is controlling the erasure status.

In the following example, virtual tape X00001 was erased on 13Feb05 15:43, last written on 17Feb05 14:49, will be retained for two weeks, and has never been migrated. The business rules indicate “no, not past retention,” which means the virtual tape is not scheduled for erasure because it is not past the retention time.

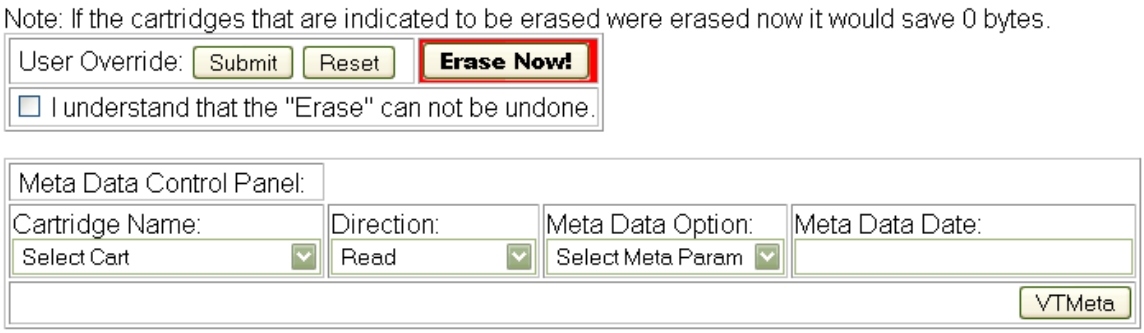
Pool :: Cartridge	Erased	Written	Retention	Migrated	Erase
TEST :: X00001	13Feb05 15:43	17Feb05 14:49	2 weeks	not by SPHiNX	no, not past retention

In the following example, there are two virtual tapes, N00014 and N00015, which were erased on 13Feb05 15:43 and last written on 17Feb05 14:49. Their retention time is 2 weeks and they never have been migrated by SPHiNX. However, the user has elected to override the business rules and has indicated that N00014 is to be erased and that N00015 will not be erased.

Pool :: Cartridge	Erased	Written	Retention	Migrated	Erase
FTP :: N00014	13Feb05 15:43	17Feb05 14:49	2 weeks	not by SPHiNX	yes, user authorized
FTP :: N00015	13Feb05 15:43	17Feb05 14:49	2 weeks	not by SPHiNX	no, not user authorized

To erase a virtual tape

At the bottom of the Scan/Cleanup page, the following is displayed:



Scan/Cleanup is designed to run as a periodic job. However, buttons are provided to enable you to control the virtual tape erase process.

Submit — Use this button with the Erase column checkboxes in the Status table. You can change that erasure status by selecting or clearing the checkbox and clicking Submit.

Reset — Use this button to remove any user-defined (override) controls and revert to the business rules.

Erase Now! — Use this button to erase the selected virtual tapes or schedule tapes for erasure immediately.

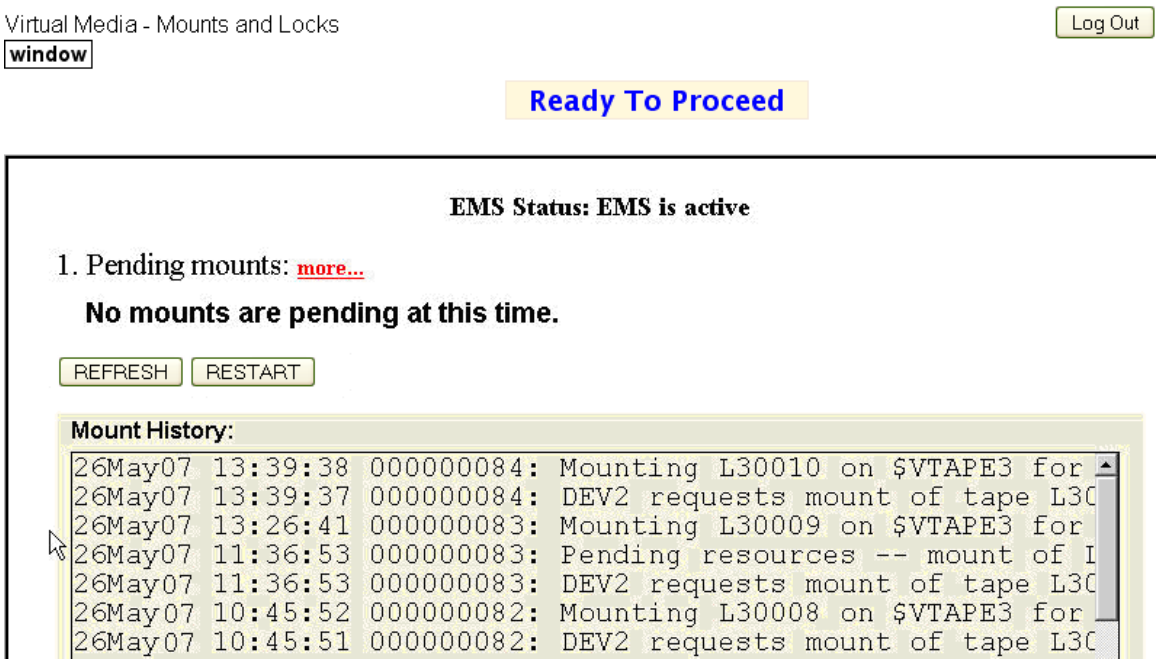
Managing locks on virtual tapes

Pools are locked when SPHiNX needs uninterrupted access to any of the cartridges in a pool. The Virtual Media - Mounts and Locks page enables you to view current locks on pools and virtual tapes. Under normal conditions, manual lock maintenance is not necessary; these locks are created and deleted by the SPHiNX processes. Removing a lock here should only be done if a SPHiNX process terminated abnormally.

To view locks

Requires the Virtual Tape Mounts and Locks access right

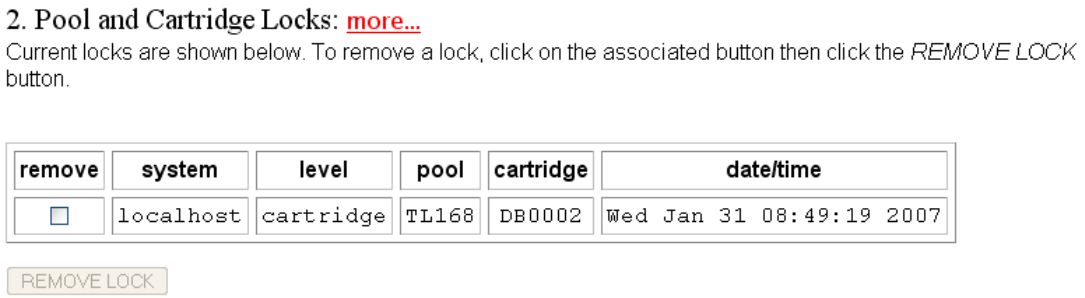
Click **Administration > Mounts and Locks** on the navigation pane.



The bottom of the page shows the current locks, which ensure that virtual tapes are only accessed by one process at a time.

To remove a lock

1. Click **Administration > Mounts and Locks** on the navigation pane.



2. Select the pool or virtual tape to unlock at the bottom of the page.
3. Click **REMOVE LOCK**.

14 Enabling and Configuring Scan/Cleanup

Scan/Cleanup is a SPHiNX (VTS) feature that is designed to help you maintain SPHiNX. It scans pools and virtual tapes to identify virtual tapes that are past their retention period. Scan/Cleanup can erase old virtual tapes to recover disk space. You can also schedule virtual tape erasures when the overall disk space falls below a specified threshold. Scan/Cleanup can be used to erase tapes after they are exported to physical tape using stacked export jobs. See "Enabling and Performing Stacked Exports" on page 51 for more information about migration. Refer to "Exporting virtual tapes" on page 109 for more information about manually erasing virtual tapes using Scan/Cleanup.

Here is a description of the general Scan/Cleanup functionality and the erase process:

- A virtual tape that is locked cannot be erased. Virtual tapes can be individually locked, locked by pool, or locked by autoloading. The locked status must be manually changed to erase a locked virtual tape.
- For the erase process, the following rules are applied to identify the virtual tapes to be erased.
  - Do not schedule erasure of virtual tapes that have not been migrated by SPHiNX.
  - Do not schedule erasure of a virtual tape that is smaller than a minimum file size.
  - Schedule erasure of a virtual tape if its retention time has expired. (The retention period is set when the pool is created or modified.)
  - Schedule erasure of virtual tapes that exceed a specified percent of usage.

  Each time Scan/Cleanup runs, it scans all virtual tapes and applies these business rules. If a virtual tape meets the criteria, it is identified for erasure. Once a virtual tape is erased, it cannot be recovered.
- The erase process can be manual or automated. To enable and configure Scan/Cleanup, select options on the **Configuration > System > Edit Configuration > Scan/Cleanup** page.
- You can force an erasure or block an erasure by using the checkboxes on the Scan/Cleanup page. However, when an erase process completes (either auto-erase or erase-now), these overrides are removed.
- When Scan/Cleanup erases a virtual tape, the header information (metadata) remains stored on SPHiNX.
- Scan/Cleanup does not affect a virtual tape's encryption setting.

At a glance, here is how to enable, configure, and use Scan/Cleanup:

- To enable and configure:
  Configure the Scan/Cleanup parameters in the configuration file as described in this chapter.

- To use:
  Use the Virtual Media - Scan/Cleanup page as described in "Automatically erasing a virtual tape using Scan/Cleanup" on page 111.

This chapter describes how to enable and configure Scan/Cleanup.

To configure Scan/Cleanup

 *Requires the Edit Configuration File access right*

1. Click **Configuration > System** on the navigation pane.
2. Click **Edit Configuration**.
3. Expand the **Scan/Cleanup** section of the page.
4. Configure the following parameters:

Parameter	Description
Enable Scan/Cleanup	Enables Scan/Cleanup. When disabled, the Scan/Cleanup page indicates that this feature is disabled. You must also select the Enable Auto Erase option to enable automated Scan/Cleanup.
Enable Auto Erase	Enables Scan/Cleanup and controls the automated erase process. When disabled, Scan/Cleanup is disabled and the Scan/Cleanup page displays the erasure cleaning status of each virtual tape but no virtual tapes are erased without further configuration. If you want to automate virtual tape erasures, enable this option and set the HH:MM to start automatic scan and erasure and Interval(hrs) to run auto erase options. Once enabled, the start time and interval are used to determine how many times per day the erasure process runs.
HH:MM to start automatic scan and erasure	Specifies when the automated scan and erasure should run (in the 24-hour format; values between and including 00:05 and 23:50 are allowed). A typical setting would be 04:30, which indicates to run at 4:30AM. To avoid scheduling problems, set this option greater than 00:04 and less than 23:51. Specify 00:00 to disable this feature. Scheduling this once or twice a day should be frequent enough to manage disk space utilization.
Interval(hrs) to run auto erase	Controls how often (in hours) the feature should run. A typical setting would be 24, which indicates to run once a day. 24 must be divisible by the specified value; thus, the following values are supported: 1, 2, 3, 4, 6, 8, 12, and 24. If the HH:MM to start automatic scan and erasure option is

Parameter	Description
	set to 04:30 and Interval(hrs) to run auto erase is set to 6, Scan/Cleanup will run at 4:30AM, 10:30AM, 4:30PM and 10:30PM daily. If you specify 0, the feature is disabled.
Erase non-Migrated	Indicates to erase virtual tapes that have not been migrated. Migration is used to move data from SPHiNX to permanent storage.
Threshold percentage for need cleanup message	Indicates the threshold after which a cleanup is initiated, if Scan/Cleanup is enabled. When the SPHiNX file system reaches this threshold (a percentage), virtual tapes can be scheduled for erasure if this parameter is set. This parameter also instructs SPHiNX to send a notification to the NonStop server.
Ignore files smaller than this number of MB	Define which files to ignore based on size. The specified value is used to set the minimum file size to erase. Some installations have many small virtual tapes and do not require that they be erased.
Enable Scan/Cleanup page	Determines whether the Scan/Cleanup page is available, which also enables the Scan/Cleanup option on the Configuration menu.
SC Erase	Shows or hides the Erase meta data column in the Status Table. The date of the last erasure may not be important to a particular installation of SPHiNX. However, this information may easily be viewed by enabling this feature.
SC No Erase	Controls whether SPHiNX should display the NO rows on the Scan/Cleanup page. Many of the virtual tapes will not be scheduled for erasure. To make the display smaller and simpler, the NO rows are suppressed. When this parameter is set to NO, a small button is shown that permits the user to temporarily override this parameter and show the NO rows.
SC Control File	Displays Scan/Cleanup files that are used to implement the Scan/Cleanup erasure process. This is typically disabled and may be enabled to help diagnose a system problem, if indicated.
SC Size	Shows or hides the Size column in the Status Table.

5. Click **Apply** to save all changes.
6. Expand the **Configuration File** section of the page and then click **Save Changes**.

15 Configuring User Accounts

This chapter describes how to manage and use the operating system and web interface accounts on the SPHiNX server.

Managing operating system accounts

By default, the following user accounts are provided for the SPHiNX operating system (Linux):

- root — the superuser of the system, who has all rights or permissions (to all files and programs) on the system; in general, it is not recommended that you use this account unless specifically directed to do so
- bill — the administrative user of the system, which was created to enable you to manage all SPHiNX functions

The first time you log in to the SPHiNX operating system using one of these usernames, you are prompted to change the password. An acceptable password must comprise eight characters, including at least one numeric character, one uppercase character, one lowercase character, and one other (non-alphanumeric) character. Note that if you use an uppercase character as the first character in the password or if you use a numeric character as the last, you must provide these character types in other positions in the new password.

If you wish to reset the root and bill accounts to the default settings, you can run the following script (as root): **/usr/local/tape/bin/ResetDefaultPasswords.bash**. After running this script, you must change the password the next time each username is used to log in.

In general, keep the following in mind when logging in to SPHiNX:

- After five failed login attempts, the user is locked out for 60 seconds. The count is reset when a password is successfully entered.
- Idle shell sessions terminate after two hours.

Adding accounts

To create an account

1. Log in to the SPHiNX server.
2. Become the root user:

```
su -
```

3. Enter the following command to create the user account:

   `useradd -n username`

4. Enter the following command to set the password for the new account:

   `passwd user_acct`

   The password must comprise eight characters, including one numeric character, one uppercase character, one lowercase character, and one other (non-alphanumeric) character. The password expires after 90 days.

Changing a user's password

To change the current user's password

1. Log in to the SPHiNX server.
2. Enter the following command to set the password for the new account:

   `passwd`

3. When prompted, enter the current password, and then enter a new password (twice). The password must comprise eight characters, including one numeric character, one uppercase character, one lowercase character, and one other (non-alphanumeric) character. Note that if you use an uppercase character as the first character in the password or if you use a numeric character as the last, you must provide these character types in other positions in the new password.

   The password expires after 90 days.

Expiring passwords

By default, account passwords expire in 90 days (this does not apply to the bill or root accounts).

To change account expiration

1. Log in to the SPHiNX server.
2. Enter the following command:

   `chage -M days user_acct`

   where *days* specifies the number of days after which the password expires, and *user_acct* specifies the user account.

   You can also use the following commands:

   `chage -l user_acct` — Lists expiration information

   `chage -M -1 user_acct` — Removes expiration from an account

Restricting access to bill

The bill account has the same access rights as the root account. You can restrict access of the bill account, thereby forcing users to use another account and denying access to functions that may present security vulnerabilities.

To restrict access to bill

1. Log in to the SPHiNX server as root.
2. Edit the **/etc/ssh/sshd_config** file to add this line:

   ```
   DenyUsers bill
   ```

   Or, if a remote export job is configured in your environment, add this line:

   ```
   AllowUsers bill@source_svr
   ```

   where *source_svr* is the IP address or hostname of the SPHiNX server where the replication operation is originating.
3. Restart the SSH service by entering this command:

   ```
   service sshd restart
   ```

Managing web interface accounts

Here is a list of the default user accounts provided for accessing the SPHiNX web interface:

Username	Default Password	Group	Privileges
operator	tapelabs	Operations	Can view system status, including vaults.
tapelabs	tapelabs	Supervisor	Can perform all SPHiNX functions but cannot administer access control, edit the SPHiNX configuration file, restore the Linux configuration, or view and manage configurations.
admin	virtual	Administration	Can access all SPHiNX functions

If you have system administrator privileges, you can configure access control to grant or limit access to specific SPHiNX functions. Each login ID belongs to a group and each group has a unique set of privileges.

Note SPHiNX provides a user that has administrator privileges. You can log in as **admin** if no other administrative user is created on the system. The default password for this user is **virtual**.

By default, SPHiNX is a closed system, which means that users are required to authenticate before they can access the web interface. Access control enables you to establish rights for specific users or classes of users. You can fine tune control of SPHiNX system resources on a group-by-group basis. A closed system requires authentication to access resources assigned to a particular group. You can enable or disable individual rights to resources.

Note In the following procedures, if the Users and Groups and Rights sections of the Manage Access Control page are not available, you must enable a closed system. These sections are not displayed if the system is configured as open access.

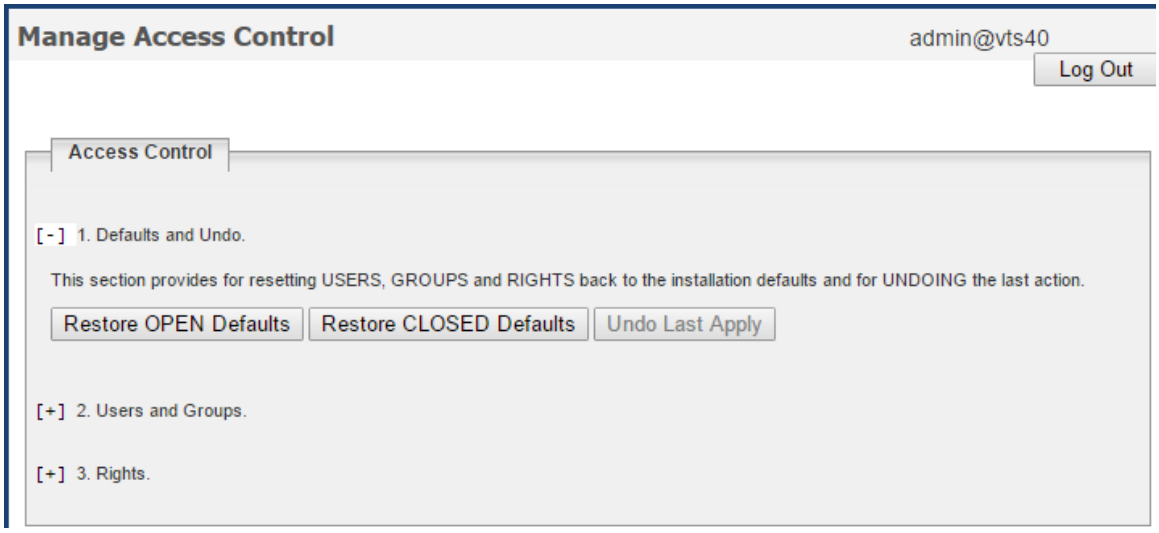
Enabling a closed system using default users and groups

You can enable a closed system to require authentication. The user can access only the resources assigned to a particular group. You can enable or disable individual rights to resources.

To enable a closed system


Requires the System Access Controls access right

1. Click **Security > Access Control** on the navigation pane.
2. If prompted, log in. After logging in, the Manage Access Control page is displayed.



3. Under Defaults and Undo, click the **Restore CLOSED Defaults** button, which restores all default users, groups, and rights.
4. Click **OK** on the pop-up dialog box to confirm that you want to restore closed defaults.

Below are closed system defaults:

- Users — The following users are defined.

Username	Group
admin	Administration
operator	Operations
tapelabs	Supervisor

- Groups — The following rights are assigned to the groups.

  Note The rights are organized in categories. If you grant access to a category, all rights in the subcategories are granted by default, though you can remove individual rights in the subcategories.

Rights	Administration Group	Operations Group	Supervisor Group	Description
Supervisory Functions	X		X	Grants access to the System administration and configuration pages
Access	X			Grants access to the Manage Access

Rights	Administration Group	Operations Group	Supervisor Group	Description
Administration				Control page
System Access Controls	X			Enables the user to administer groups and rights within Access Control
User Access Controls	X			Enables the user to change his or her password only within Access Control
Block and Unblock TapeServer	X		X	Displays the Block/Unblock TapeServer Startup link on Manage System Tasks page, which enables the user to block and unblock SPHiNX functions
Database Download	X		X	Enables the user to create a system restore image from the Manage System Updates page
Database Upload	X			Enables the user to restore a system restore image from the Manage System Updates page
Edit VTS Configuration File	X			Enables the user to edit the SPHiNX configuration file from the Manage System Configuration page
Halt and Reboot TapeServer	X		X	Enables the user to halt and reboot SPHiNX from the Manage System Tasks page
Manage Scheduled Jobs	X		X	Obsolete; do not assign this access right
Server Certificate Maintenance	X		X	Enables the user to manage certificates
System Maintenance Functions	X		X	Enables the user to stop and start the Inter- Systems Communication (ISC) services from the Manage System Tasks page, enables licensing, and displays the Edit System Settings, the File System Check Status, and the Generate Troubleshooting Package links
System Upgrade/Update Functions	X		X	Enables the user to apply revision updates and apply customized code changes
Turn Compression On or Off	X		X	Enables the user to enable or disable compression from the Manage System Configuration page

Rights	Administration Group	Operations Group	Supervisor Group	Description
VPD Upload	X			Enables the user to upload the VPD file
VTS/Linux Configuration Backup	X		X	Obsolete; do not assign this access right
VTS/Linux Configuration Restore	X			Obsolete; do not assign this access right
View log files	X		X	Enables the user to view log files from the Logs page
View/Manage Configuration	X			Grants access to the Configure Virtual Devices page
Virtual Tape Operations	X	X	X	Grants access to the Configure Tapes and Pools page
Scan and Cleanup Control Panel	X		X	Grants access to the Virtual Media - Scan/Cleanup page
Virtual Tape Cartridge Maintenance	X		X	Grants access to the Virtual Media - Cartridge Maintenance page
Delete Cartridges	X		X	Enables the user to delete virtual tapes from the Configure Tapes and Pools and Virtual Media - Cartridge Maintenance pages
Virtual Tape Import and Export	X		X	Grants access to the Virtual Media - Import/Export page
Virtual Tape Instant DR	X		X	Grants access to the Virtual Media - Instant DR page
Virtual Tape Mounts and Locks	X		X	Grants access to the Virtual Media - Mounts and Locks page
Virtual Tape Pool Maintenance	X		X	Grants access to the Virtual Media - Pool Maintenance page
Erase Cartridges	X		X	Enables the user to erase virtual tapes from the Configure Tapes and Pools and Virtual Media - Cartridge Maintenance pages
HSM Migration	X		X	Enables the user to migrate virtual tapes using the Migrate button on the Configure Tapes and Pools page

Rights	Administration Group	Operations Group	Supervisor Group	Description
Mount Cartridges	X		X	Enables the user to manually mount virtual tapes using the Mount button on the Configure Tapes and Pools page
Unmount Cartridges	X		X	Enables the user to unmount virtual tapes using the Unmount button on the Configure Tapes and Pools page
Access to secure vts	X			Grant access to secure vts (to the encyrption features).
Factory Setup Activities	X			Enables the user to manage disk storage.
View System Status	X	X	X	Grants access to the System Status page
Stop and Start TapeServer	X	X	X	Enables the user to start and stop SPHiNX from the Manage System Tasks page
Vault Access	X	X	X	Provides access to vaults.
Access to All Vaults	X	X	X	Provides access to any vault and vault contents.

Enabling closed access and restricting access to virtual tapes

If you want to create an account that does not have access to virtual tapes, complete this procedure.

To restrict access to virtual tapes

1. Log in using the admin account.
2. Enable a closed system as described in "Enabling a closed system using default users and groups" on page 121.
3. Add a user as described in "Creating a user" on page 126.
4. Add a group:
   a. Click **+** to expand Users and Groups.
   b. Click **ADD** next to Groups.
   c. In the **add group** field, type a name for the group.
   d. Click **APPLY**.
5. Add the user to the group:
   a. Deselect the new user in the **Users** drop-down list and select it again to enable the CHANGE GROUP button.

b. Click **CHANGE GROUP**.

c. Select the group from the **in Group** drop-down list.

d. Click **APPLY**.

6. Assign rights to the group:
   a. Expand **+** to expand Rights.

   b. Select the **1.3 Virtual Tape Operations** access right only.

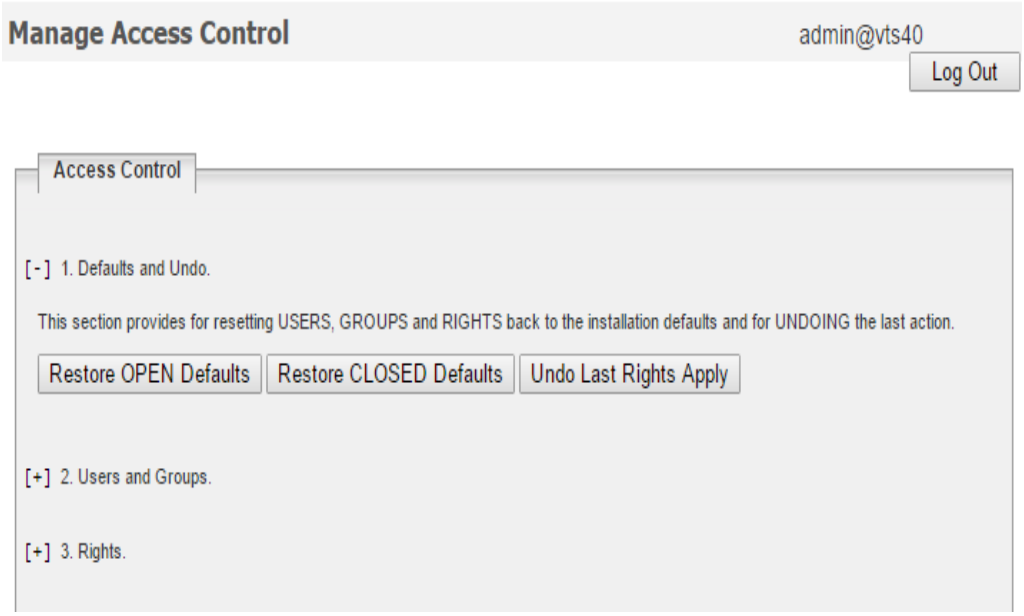
   c. Click **APPLY**.

Creating a user

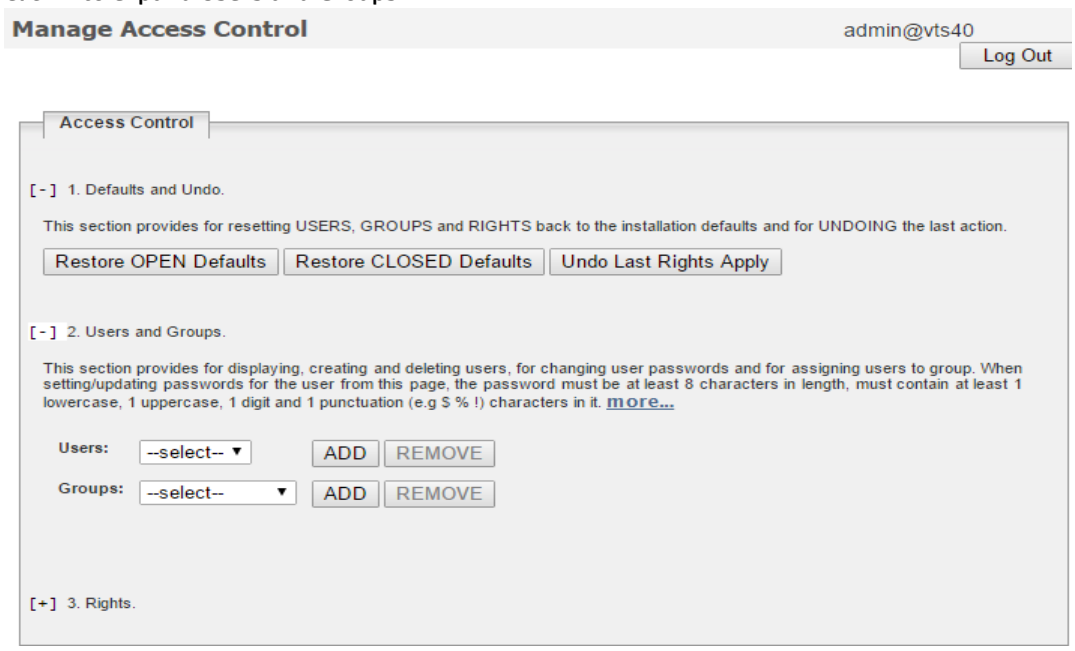
To create a user

Requires the System Access Controls access right

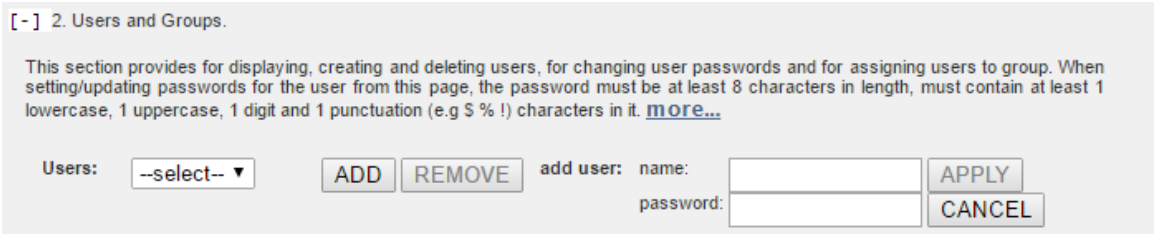
1. Click **Security > Access Control** on the navigation pane.
2. If prompted, log in. After logging in, the Manage Access Control page is displayed.



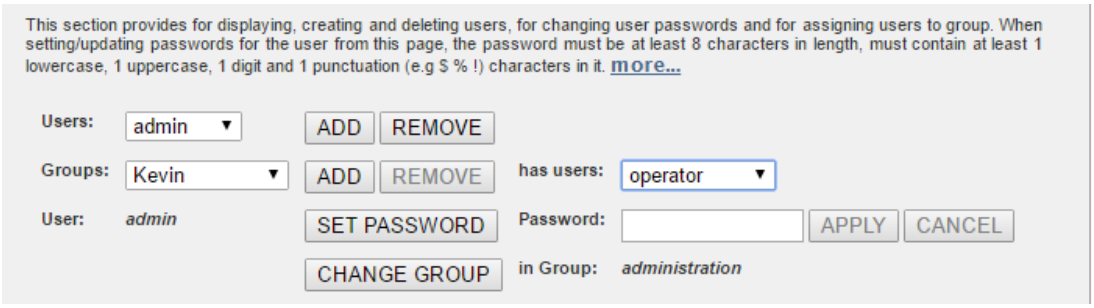
3. Click **+** to expand Users and Groups.



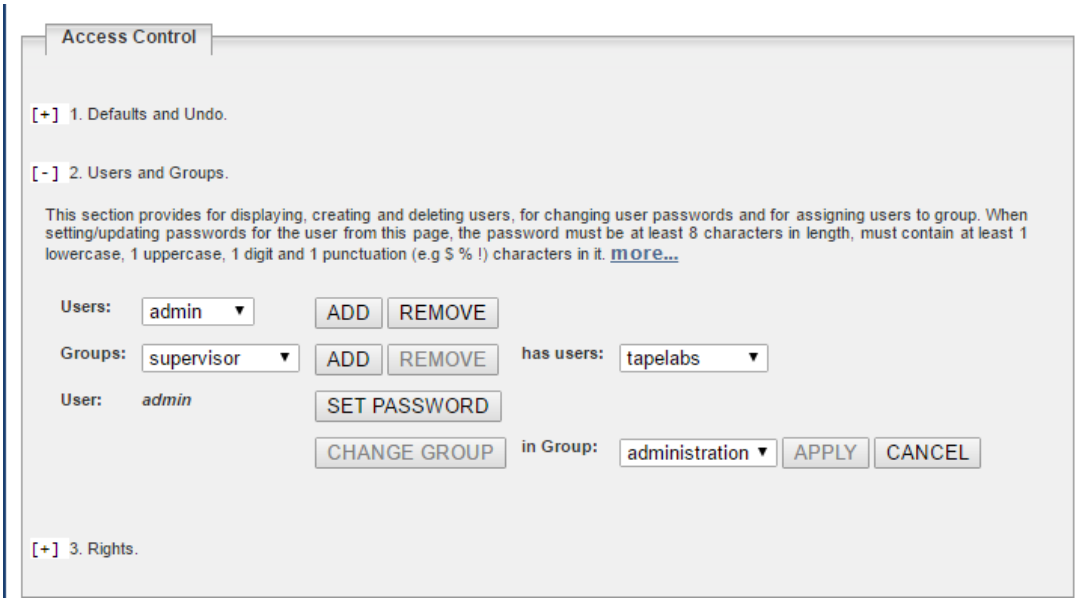
4. Click **ADD** next to Users. The name and password fields are displayed.



5. Type a username in the **name** field. Usernames cannot contain spaces and cannot duplicate existing usernames, group names, or reserved names. Also, they must be alphanumeric, though they can include an _ (underscore) character.
6. Type a password in the **password** field.
7. Click **APPLY**. The user is added and additional buttons are displayed.



8. To assign the user to a group, click **CHANGE GROUP**. The Group drop-down list is displayed.



9. Select a group from the drop-down list and click **APPLY**.

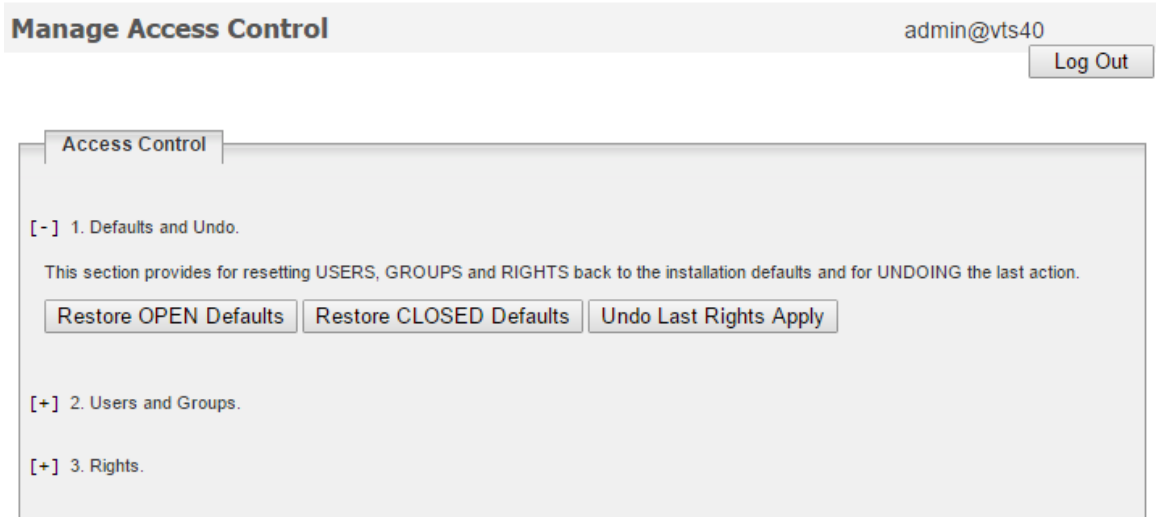
Changing any user's password

It is *highly* recommended that you change the passwords of the default users.

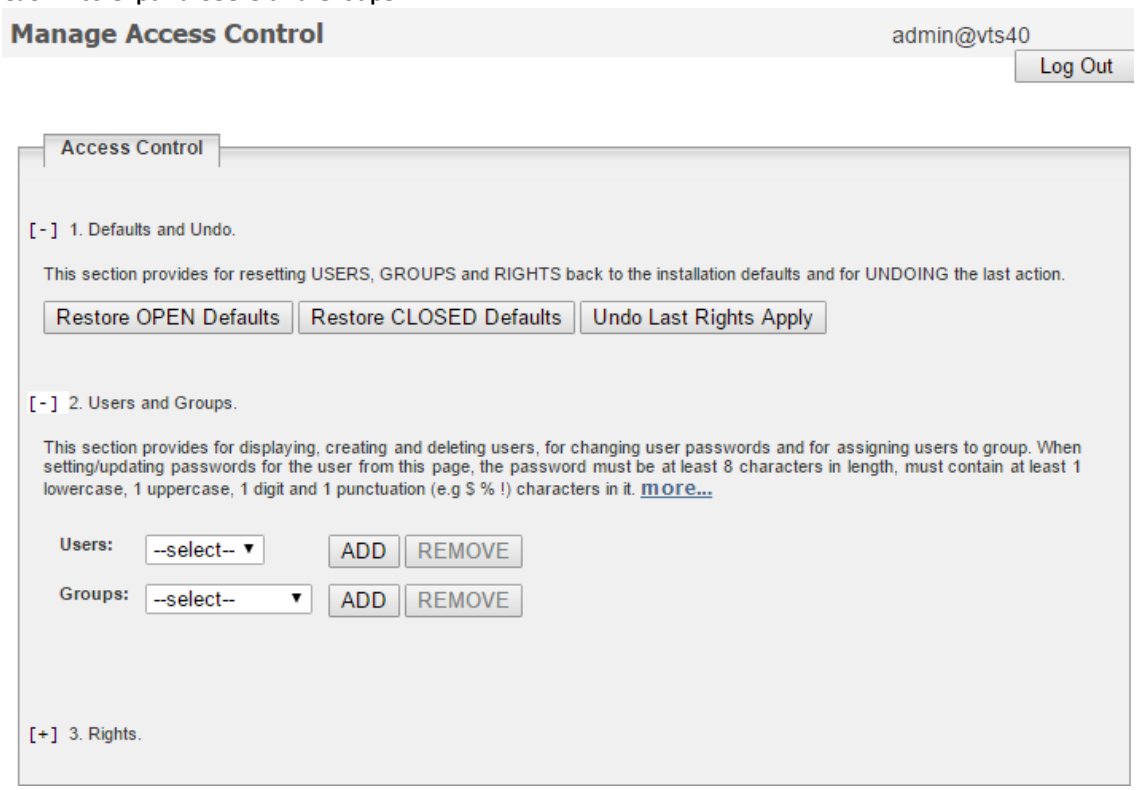
To change a user's password

Requires the System Access Controls access right to change any user's password

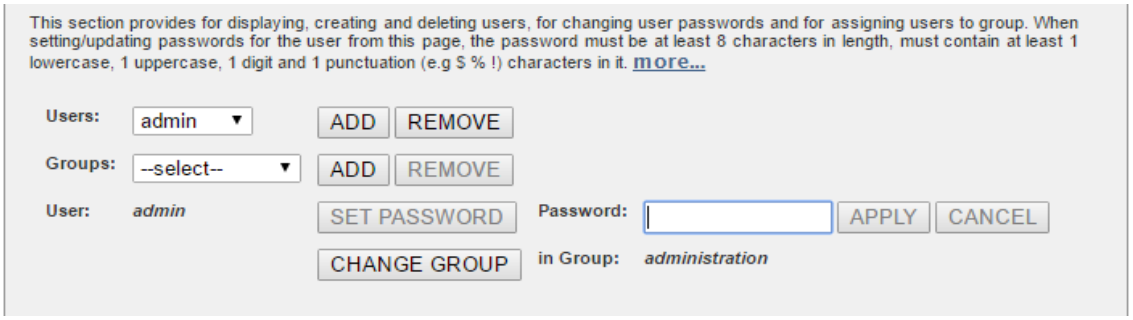
1. Click **Security > Access Control** on the navigation pane.
2. If prompted, log in. After logging in, the Manage Access Control page is displayed.



3. Click **+** to expand Users and Groups.



4. Select the user from the **Users** drop-down list.
5. Click **SET PASSWORD**. The Password field is displayed.



6. Type a new password in the field.
7. Click **APPLY**.

Configuring groups

Groups define the access rights that are assigned to users. Three groups are provided:

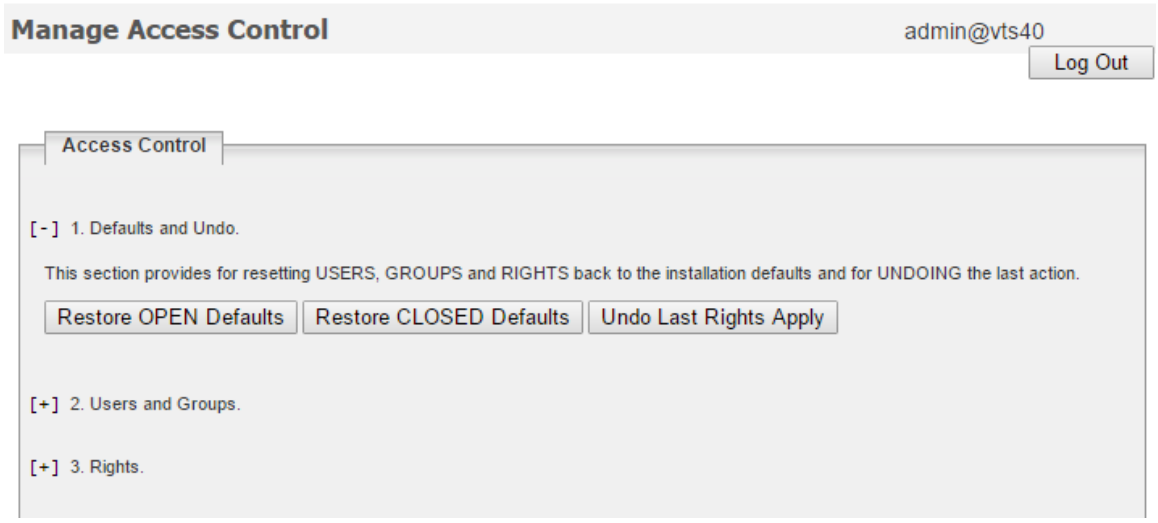
- Administration
- Operations
- Supervisor

For a list of the default rights assigned to these groups, see 122. You can modify the access rights that are assigned to these groups. You can also save your changes as a set of custom defaults, which can be restored later if necessary.

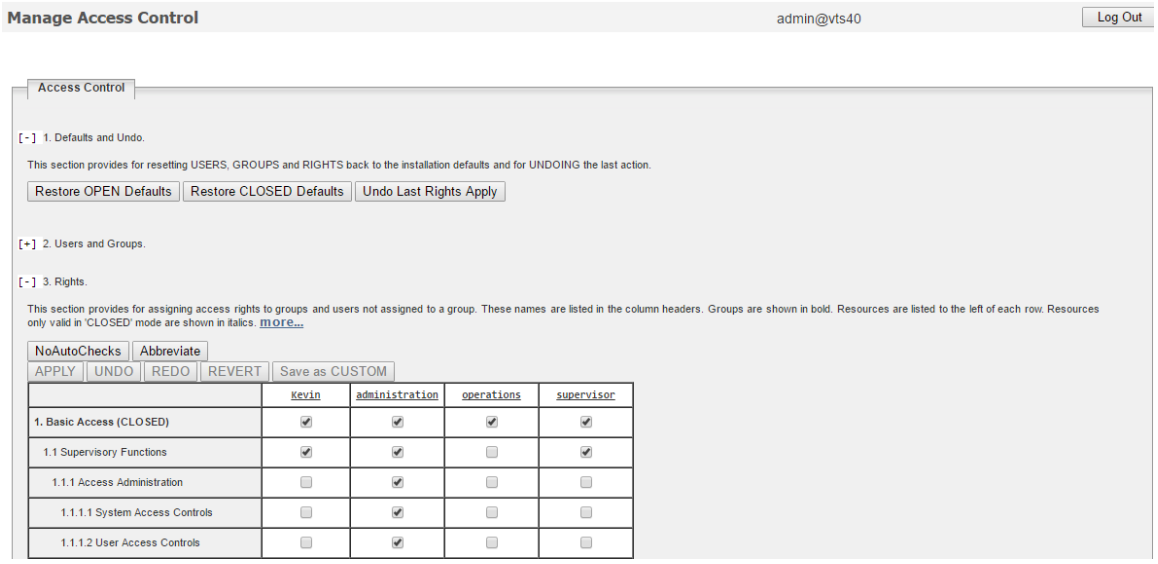
To modify access rights assigned to the Administration, Operations, and Supervisor groups

Requires the System Access Controls access right

1. Click **Security > Access Control** on the navigation pane.
2. If prompted, log in. After logging in, the Manage Access Control page is displayed.



3. Click **+** to expand Rights.



4. To modify access rights assigned to the Administration group, select the checkbox next to each access right in the Administration column.

Note The rights are organized in categories. If you grant access to a category, all rights in the subcategories are granted by default, though you can remove individual rights in the subcategories.

Here is a description of each access right:

Right	Description
Supervisory Functions	Grants access to the System administration and configuration pages
Access Administration	Grants access to the Manage Access Control page
System Access Controls	Enables the user to administer groups and rights within Access Control
User Access Controls	Enables the user to change his or her password only within Access Control
Block and Unblock TapeServer	Displays the Block/Unblock TapeServer Startup link on Manage System Tasks page, which enables the user to block and unblock SPHiNX functions
Database Download	Enables the user to create a system restore image from the Manage System Updates page
Database Upload	Enables the user to restore a system restore image from the Manage System Updates page
Edit Configuration File	Enables the user to edit the SPHiNX configuration file from the Manage System Configuration page
Halt and Reboot TapeServer	Enables the user to halt and reboot SPHiNX from the Manage System Tasks page
Manage Scheduled Jobs	Obsolete; do not assign this access right
Server Certificate Maintenance	Enables the user to manage certificates
System Maintenance Functions	Enables the user to stop and start the Inter-Systems Communication (ISC) services from the Manage System Tasks page, enables licensing, and displays the Edit System Settings, the File System Check Status, and the Generate Troubleshooting Package links
System Upgrade/Update Functions	Enables the user to apply revision updates and apply customized code changes
Turn Compression On or Off	Enables the user to enable or disable compression

Right	Description
	from the Manage System Configuration page
Upload Encryption Keys	Obsolete; do not assign this access right
Upload VPD	Enables the user to upload the VPD file
Configuration Backup	Obsolete; do not assign this access right
Configuration Restore	Obsolete; do not assign this access right
View log files	Enables the user to view log files from the Logs page
View/Manage Configuration	Grants access to the Configure Virtual Devices page
Virtual Tape Operations	Grants access to the Configure Tapes and Pools page
Scan and Cleanup Control Panel	Grants access to the Virtual Media - Scan/Cleanup page
Virtual Tape Cartridge Maintenance	Grants access to the Virtual Media - Cartridge Maintenance page
Delete Cartridges	Enables the user to delete virtual tapes from the Configure Tapes and Pools and Virtual Media - Cartridge Maintenance pages
Virtual Tape Import and Export	Grants access to the Virtual Media - Import/Export page
Virtual Tape Instant DR	Grants access to the Virtual Media - Instant DR page
Virtual Tape Mounts and Locks	Grants access to the Virtual Media - Mounts and Locks page
Virtual Tape Pool Maintenance	Grants access to the Virtual Media - Pool Maintenance page
Erase Cartridges	Enables the user to erase virtual tapes from the Configure Tapes and Pools and Virtual Media - Cartridge Maintenance pages
HSM Migration	Enables the user to migrate virtual tapes using the Migrate button on the Configure Tapes and Pools page

Right	Description
Mount Cartridges	Enables the user to manually mount virtual tapes using the Mount button on the Configure Tapes and Pools page
Unmount Cartridges	Enables the user to unmount virtual tapes using the Unmount button on the Configure Tapes and Pools page
View System Status	Grants access to the System Status page
Change Refresh Rate	Enables the user to change the refresh rate of the System Status page from the System Status page
Stop and Start TapeServer	Enables the user to start and stop SPHiNX from the Manage System Tasks page
Vault Access	Provides access to vaults.
Access to All Vaults	Provides access to any vault and vault contents.

5. To modify access rights assigned to the Operations group, select the checkbox next to each access right in the Operations column. See the previous step for a description of each right.
6. To modify access rights assigned to the Supervisor group, select the checkbox next to each access right in the Supervisor column. See step 4 for a description of each right.
7. Click **APPLY** above the table to save your changes.

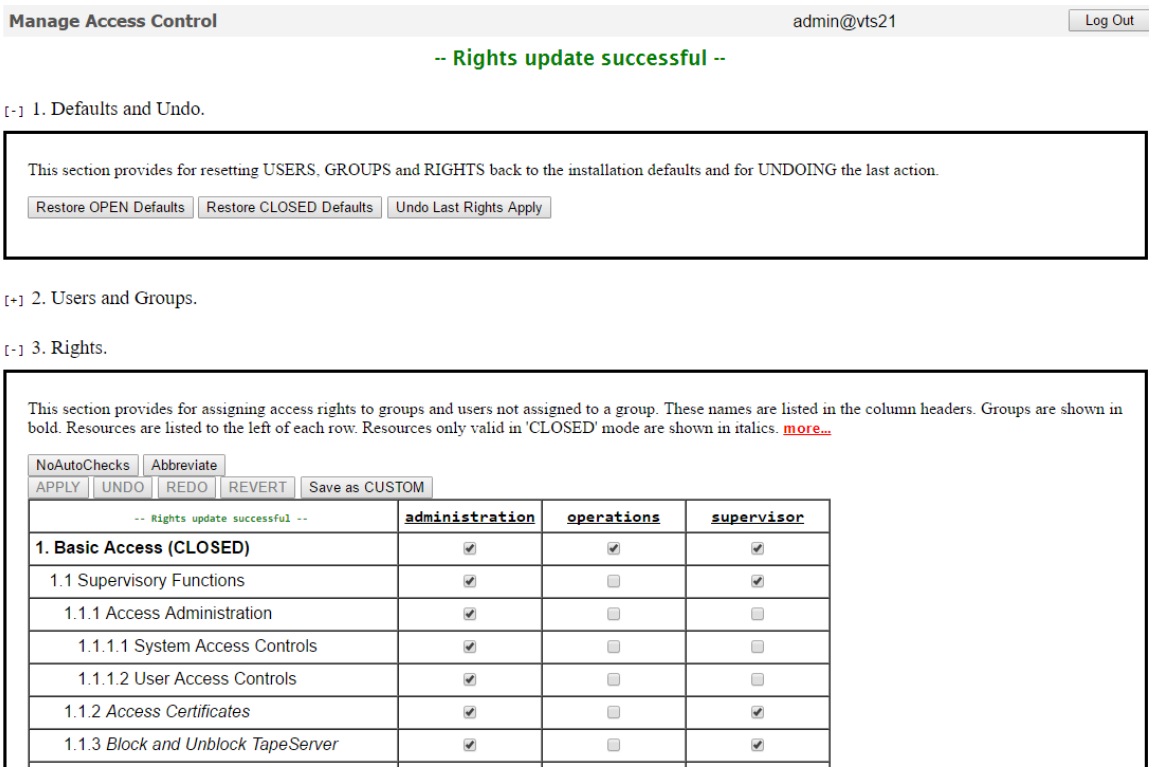
Saving and restoring custom defaults

After configuring users and group rights, you can save all settings as a custom configuration. Later, you can restore these settings by simply clicking the Restore CUSTOM Defaults button in the Defaults and Undo section of the page. This button becomes available after you save a custom configuration.

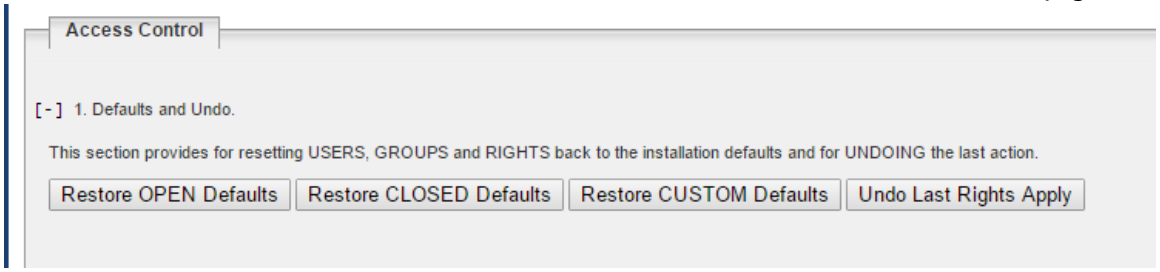
To save custom default settings

 *These procedures require the System Access Controls access right*

1. Click the **Save as CUSTOM** button above the access rights table.



2. When prompted, click **OK** to confirm that you want to save the settings as the custom defaults. The Restore CUSTOM Defaults button becomes available in the Defaults and Undo section of the page.



To restore the custom default settings

Click the **Restore CUSTOM Defaults** button to restore the custom configuration and discard changes made since the custom defaults were last saved.

16 Configuring Web Interface Preferences

This chapter describes how to configure web interface preferences. You can set a number of parameters in the SPHiNX configuration to specify the following:

- Whether and how often to display status messages at the top of the page.
- Whether and when to display a notification regarding low vault space.
- Whether to display the free space by vault on the System Status page.
- Whether to display the buttons and features on the Configure Tapes and Pools page, which can be displayed by clicking Advanced Media Actions at the top of the Manage Virtual Tapes page.

You must modify the SPHiNX configuration to configure these features.

To configure web interface preferences

 *Requires the Edit Configuration File access right*

Note A default configuration file is defined for each SPHiNX server. To override the default settings, you must define settings as described below.

1. Click **Configuration > System** on the navigation pane.
2. Click **Edit Configuration**.
3. Expand the **Web Interface** section of the page.
4. Configure these parameters (under **Adjust which buttons and/or columns are shown:**), as necessary:

Parameter	Description
Allow Auto Refresh	Whether to allow auto-refresh on the Virtual Media - Operation page. This also displays the kb/sec column on the page.
Delete	Displays the Delete button on the Virtual Media - Operation page.
Export/Import	Displays the Import/Export button on the Virtual Media - Operation page.

Parameter	Description
UnMigrate	Displays the UnMigrate button on the Advanced Virtual Media - Operation page.
UnMount	Displays the Unmount button on the Virtual Media - Operation page.
Compression Ratio	Displays the compression ratio (c/ratio) column on the Virtual Media - Operation page.
Size Limits	Displays pool size limits on the Virtual Media - Operation page.
Cartridge selection menu on Cart Maint	Displays the cartridge selection drop-down menu on the Cartridge Maintenance Operations page.
Block Mark Conversion	Displays the blockmark conversion button on the Virtual Media - Operation page.
Erase	Displays the Erase button on the Virtual Media - Operation page.
Migrate	Displays the Migrate button on the Virtual Media - Operation page. Note that a BMA must be selected on the Configuration > System > Edit Configuration > Backup Management Application (BMA) page to display the button.
Mount	Displays the Mount button on the Virtual Media - Operation page.
Cartridge Version	Displays the cartridge version on the Virtual Media - Operation page.
Last Written	Displays the last written column on the Virtual Media - Operation page.
ReadOnly	Displays the read-only flag column, which indicates whether the virtual tape is set to read-only or read/write, on the Virtual Media - Operation page. When a virtual tape is loaded in a VTD, the column indicates “ro” for read-only or “rw” for read-write. Otherwise, the read-only flag column is blank for all virtual tapes in every pool.
Show VAULT free space table on System Status page	Specifies whether to display the Free Space information (for each vault) on the System Status page.

5. Click the **Apply** button.

6. Expand the **Configuration File** section of the page and then click **Save Changes**.
7. Expand the **Miscellaneous parameters** section of the page.
8. Configure these parameters as necessary:

Parameter	Description
% space used before notify	Sets the percentage for the **/VAULT xx** file system usage alert on the Virtual Media - Operation page. Set this parameter to a value greater than 0, or set it to 0 to disable the feature. If EMS is enabled, a message is also sent to the NonStop host server.
Send notification on low free space	Enables notification on low vault space. If EMS is enabled, a message is also sent to the NonStop host server (the **Enable Host Notifications** option must also be enabled on the EMS Configuration page).

9. Click the **Apply** button.
10. Expand the **Configuration File** section of the page and then click **Save Changes**.

17 Configuring Alerts

The SPHiNX server provides an Intelligent Platform Management Interface (IPMI) card, which has a dedicated Ethernet port for management use and provides the following features:

- Temperature monitoring
- Fan speed monitoring
- Voltage monitoring
- Power status monitoring
- Chassis intrusion monitoring
- Remote power control to power-on, power-off, or reboot the server
- Remote access to text- or graphic-based system information, including BIOS configurations and OS operation information (KVM)
- Remote management of utility/software applications

In addition, the SPHiNX appliance ships with a RAID controller, which monitors for hardware problems (on an hourly basis). Specifically, the RAID controller checks the status of the cache battery backup, HBA operation, physical disks, and logical disks.

This chapter describes how to configure the IPMI card and SPHiNX system to send alerts.

Configuring the IPMI card

This section provides steps for configuring the IPMI card on the 2U server and 3U servers, which differ.

Configuring the IPMI card on the SPHiNX 2U-s

Before beginning

- Connect to and configure the IPMI port as described in the *Quick Start Guide*.
- Download the *Supermicro AOC-SIMLP-B+ User's Manual* for more information about using this web interface. Specifically, refer to chapter 3, "Software Application and Usage".

  http://www.supermicro.com/manuals/other/AOC-SIMLP.pdf

Accessing the web interface of the IPMI card

Complete the following steps to connect to the web interface of the IPMI card.

To access the IPMICFG Utility

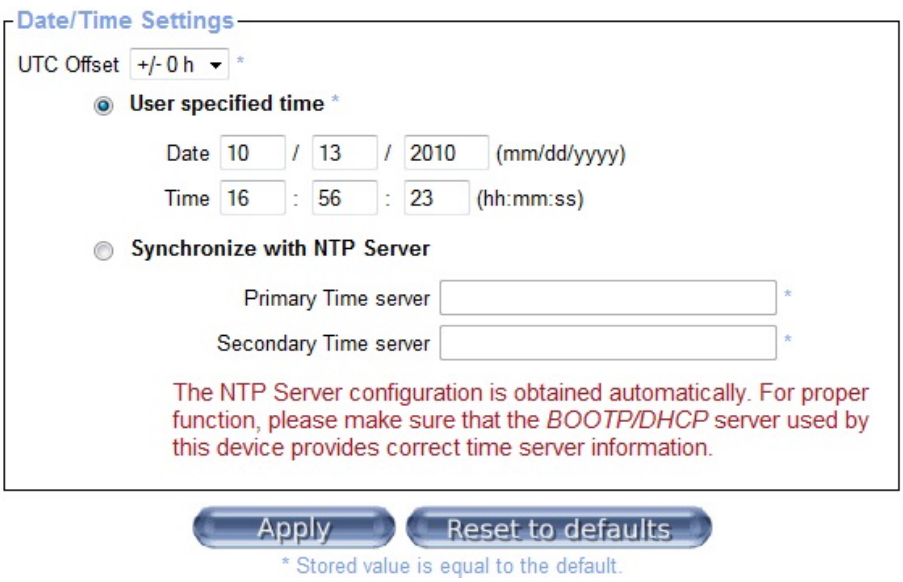
1. On a computer that is connected to the same network as SPHiNX, launch a web browser.
2. Enter the hostname or IP address of the IPMI card in the address field. If the card is configured to use DHCP, you can enter **netconfig** from the serial console to determine the currently assigned IP address (you must log in as root to use this command). Refer to the *Quick Start Guide* for information about connecting to and using the serial console and **netconfig** command.
3. On the login page, type **ADMIN** in the **USERNAME** field.
4. Type **ADMIN** in the **PASSWORD** field.
5. Click the **LOGIN** button.

Setting the IPMI clock

Before you can define alerts, you must set the clock on the IPMI card. You can set the date and time or use NTP. You can also set a timezone or use Coordinated Universal Time (UTC).

To configure the clock

1. Log in to the IPMICFG web interface.
2. Select **Device Settings > Date/Time** from the navigation pane. The Date/Time Settings page is displayed:



3. From the **UTC Offset** drop-down list, select an offset, which is the time offset from UTC. It is recommended that you select **+/- 0 h**, thereby using UTC. Otherwise, set the offset so it coordinates with your timezone.
4. Set the time using the **User specified time** fields, or choose **Synchronize with NTP Server** and then specify IP addresses or hostnames for a primary and secondary NTP server.
5. Click **Apply** to save your settings.

Defining alerts

You may find it useful to set up email alerts based on sensors readings. To do this, create an alert filter, an alert policy, and a LAN destination with your email address

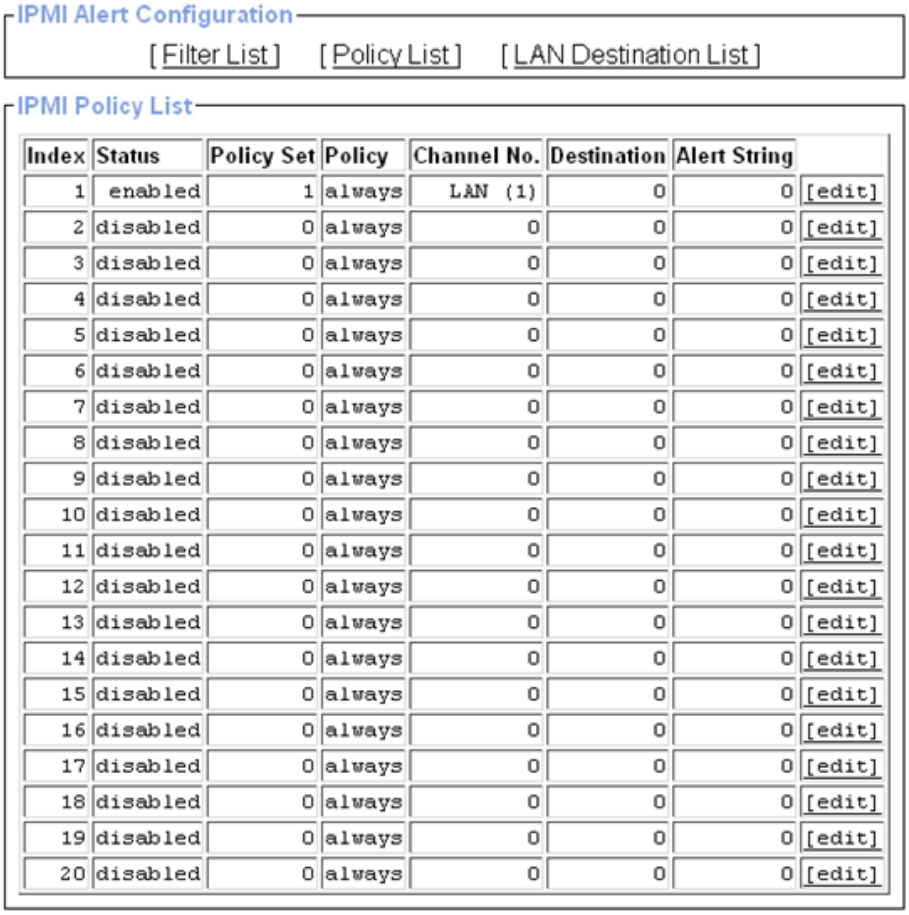
To configure alerts based on sensors

1. Log in to the IPMICFG web interface.
2. Select **System Health > Alert Settings** from the navigation pane.
3. Edit the first IPMI filter (Index 1) by clicking **edit** on the right side of the filter list.
4. In the edit dialog, set the following options:
   - Set **Status** to **enable**.
   - From the **Action** list, set the actions that will occur when this alert is generated.
   - Assign the policy ID to the filter in the **Alert Policy** field.
   - Set the sensor type and number in the **Sensor Type** and **Sensor Number** fields. Refer to "Sensor types and numbers" on page 142 for a list.

   Here is an example:

   Then, click **Apply**.

5. Enable a policy for the alert by selecting the **Policy List** link in the IPMI Alert Configuration section and then clicking **edit** next to Index 1.



IPMI Alert Configuration

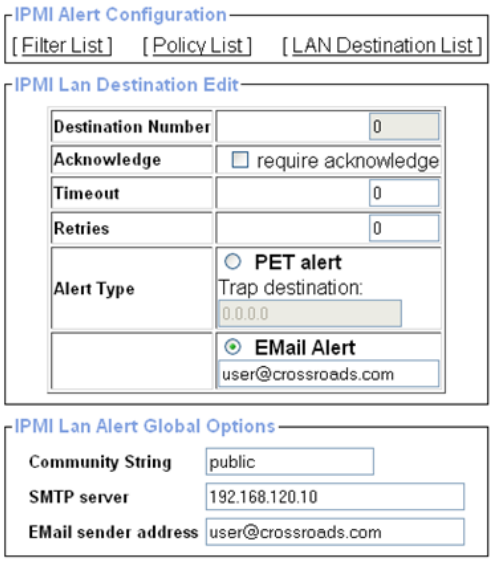
[Filter List] [Policy List] [LAN Destination List]

IPMI Policy List

Index	Status	Policy Set	Policy	Channel No.	Destination	Alert String	
1	enabled	1	always	LAN (1)	0	0	[edit]
2	disabled	0	always	0	0	0	[edit]
3	disabled	0	always	0	0	0	[edit]
4	disabled	0	always	0	0	0	[edit]
5	disabled	0	always	0	0	0	[edit]
6	disabled	0	always	0	0	0	[edit]
7	disabled	0	always	0	0	0	[edit]
8	disabled	0	always	0	0	0	[edit]
9	disabled	0	always	0	0	0	[edit]
10	disabled	0	always	0	0	0	[edit]
11	disabled	0	always	0	0	0	[edit]
12	disabled	0	always	0	0	0	[edit]
13	disabled	0	always	0	0	0	[edit]
14	disabled	0	always	0	0	0	[edit]
15	disabled	0	always	0	0	0	[edit]
16	disabled	0	always	0	0	0	[edit]
17	disabled	0	always	0	0	0	[edit]
18	disabled	0	always	0	0	0	[edit]
19	disabled	0	always	0	0	0	[edit]
20	disabled	0	always	0	0	0	[edit]

6. Configure these settings for the policy:
   - Policy Set entry — Type the number of the alert policy in the IPMI Filter List (1, in this example).
   - Destination — Type the number of the destination, which you will configure next.
   - Channel No. — Type the number of the LAN channel.

   Then, click **Apply**.
7. Configure the LAN destination assigned to the policy by clicking the **LAN Destination List** link in the IPMI Alert Configuration section, and then click **edit** next to the ID you assigned.
8. Select **EMail Alert** and enter the email address to which the alert will be sent. Specify the SMTP settings of the SMTP server in the IPMI Lan Alert Global Options section of the page.



Then, click **Apply**.

9. Repeat these steps for each additional alert you want to add.

Sensor types and numbers

Sensor type codes

Sensor Type	Type Code
reserved	00h
Temperature	01h
Voltage	02h
Current	03h
Fan	04h
Physical Security (Chassis Intrusion)	05h
Platform Security Violation Attempt	06h
Processor	07h
Power Supply	08h
Power Unit	09h
Cooling Device	0Ah

Sensor Type	Type Code
Other Units-based Sensor	0Bh
Memory	0Ch
Drive Slot (Bay)	0Dh
POST Memory Resize	0Eh
System Firmware Progress	0Fh
Event Logging Disabled	10h
Watchdog 1	11h
System Event	12h
Critical Interrupt	13h
Button / Switch	14h
Module / Board	15h
Microcontroller / Coprocessor	16h
Add-in Card	17h
Chassis	18h
Chip Set	19h
Other FRU	1Ah
Cable / Interconnect	1Bh
Terminator	1Ch
System Boot / Restart Initiated	1Dh
Boot Error	1Eh
OS Boot	1Fh
OS Stop / Shutdown	20h
Slot / Connector	21h
System ACPI Power State	22h

Sensor Type	Type Code
Watchdog 2	23h
Platform Alert	24h
Entity Presence	25h
Monitor ASIC / IC	26h
LAN	27h
Management Subsystem Health	28h
Battery	29h
Session Audit	2Ah
FRU State	2Ch

Sensor numbers

Sensor Type	Sensor #	
CPU1 Temp	00h	
CPU2 Temp	01h	
Sys Temp	02h	Temperature = Data
CPU1 Vcore	03h	Voltage = Data* 0.008
CPU2 Vcore	04h	Voltage = Data* 0.008
3.3V	05h	Voltage = Data* 0.016
5V	06h	Voltage = Data* 0.024
12V	07h	Voltage = Data* 0.096
-12V	08h	Voltage = Data* 0.148 - 16.92
1.5V	09h	Voltage = Data* 0.016
5VSB	0Ah	Voltage = Data* 0.024
VBAT	0Bh	Voltage = Data* 0.016

Sensor Type	Sensor #	
Fan1	0Ch	RPM = 1350000/Data
Fan2	0Dh	RPM = 1350000/Data
Fan3	0Eh	RPM = 1350000/Data
Fan4	0Fh	RPM = 1350000/Data
Fan5	10h	RPM = 1350000/Data
Fan6	11h	RPM = 1350000/Data
Fan7/CPU1	12h	RPM = 1350000/Data
Fan8/CPU2	13h	RPM = 1350000/Data
Intrusion	44H	
Power Supply	14H	

Configuring the IPMI card on the SPHiNX 3U-s

Before beginning

- Connect to and configure the IPMI port as described in the *Quick Start Guide*.
- Download the *Supermicro Embedded BMC/IPMI User's Guide* for complete information:

  http://www.supermicro.com/manuals/other/Embedded_BMC_IPMI.pdf

Accessing the web interface of the IPMI card

Complete the following steps to connect to the web interface of the IPMI card.

To access the IPMICFG Utility

1. On a computer that is connected to the same network as SPHiNX, launch a web browser.
2. Enter the hostname or IP address of the IPMI card in the address field. If the card is configured to use DHCP, you can enter **netconfig** from the serial console to determine the currently assigned IP address (you must log in as root to use this command). Refer to the *Quick Start Guide* for information about connecting to and using the serial console and **netconfig** command.
3. On the login page, type **ADMIN** in the **USERNAME** field.
4. Type **ADMIN** in the **PASSWORD** field.
5. Click the **LOGIN** button.

Configuring clock, alert, and SMTP settings

To use the IPMI card to alert users about hardware problems, you must configure the card. Complete instructions are detailed in chapter 2 of the *Supermicro Embedded BMC/IPMI User's Guide*. Be sure to

download this guide before proceeding.

To configure the IPMI card

1. Configure time and date settings on the IPMI card.
2. Define alerts. Alerts enable you to send notifications based on the information gathered by the IPMI card.
3. Configure SMTP settings.

Configuring the 3ware agent on legacy hardware

If you upgrade to the current release, you can configure the 3ware agent to send email alerts based on hardware problems, you must define email alerts using the 3DM 2 web application. (A 3ware RAID controller shipped in the SPHiNX 6.04.x and 8.0 appliances.)

To log in to the 3DM 2 web application

1. On a computer that is connected to the same network as SPHiNX, launch a web browser.
2. Enter the following URL in the address field:

   https://*hostname*:888/

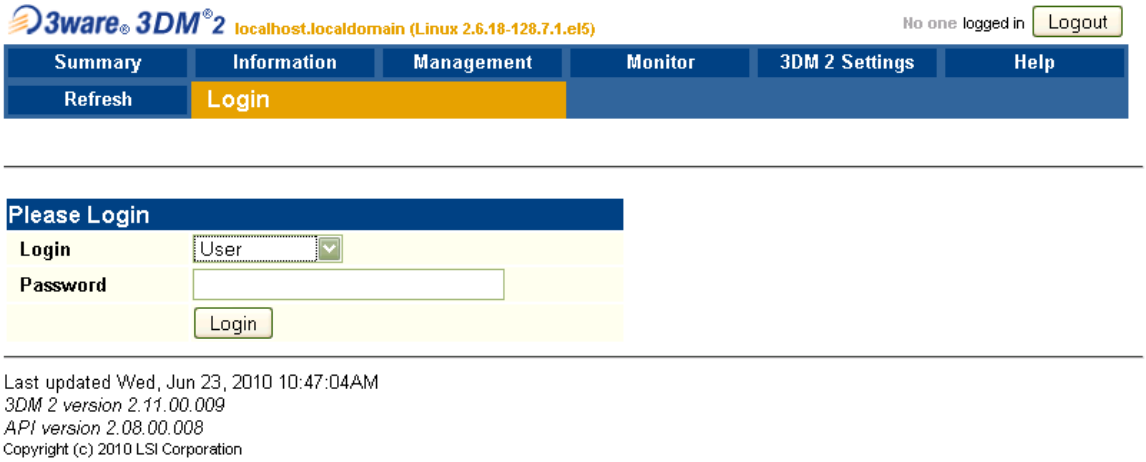
   where *hostname* is the hostname or IP address of the SPHiNX server.

   Your browser may display a warning page and certificate errors. SPHiNX ships with a self-signed certificate that is used to establish a secure communication channel between your browser and the SPHiNX web application server, through Secure Sockets Layer (SSL). This self-signed certificate may cause your browser to display a certificate warning for the following reasons:

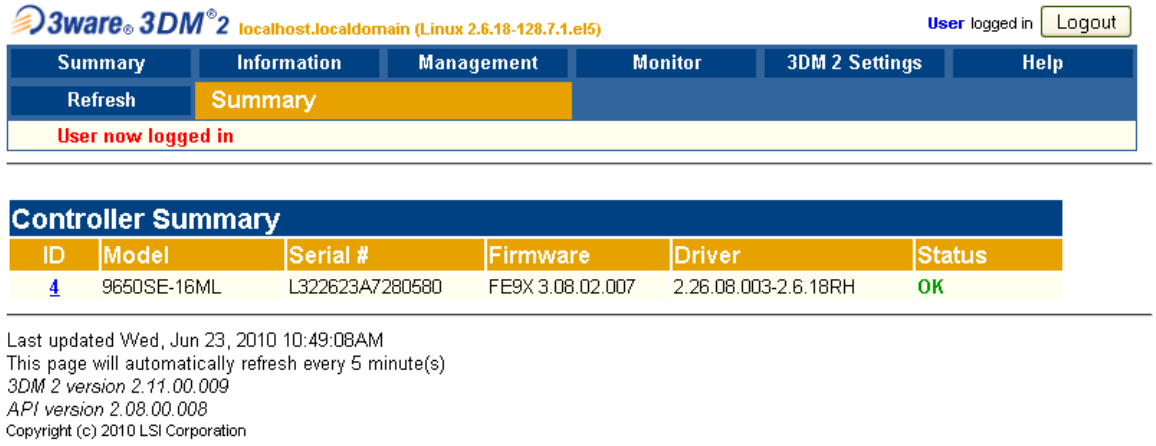
   - Many browsers warn you when a web application employs a self-signed certificate. These certificates are not considered as secure as a certificate signed by a Certificate Authority.
   - When the SPHiNX default self-signed certificate is created, a temporary hostname is used for the appliance. During deployment, this hostname most likely changed. Many browsers warn you when the hostname on the certificate and the hostname on the appliance do not match.

   When the browser displays this warning, accept the certificate or add an exception (depending on your browser) and continue to the web interface. Refer to the browser help for more information.

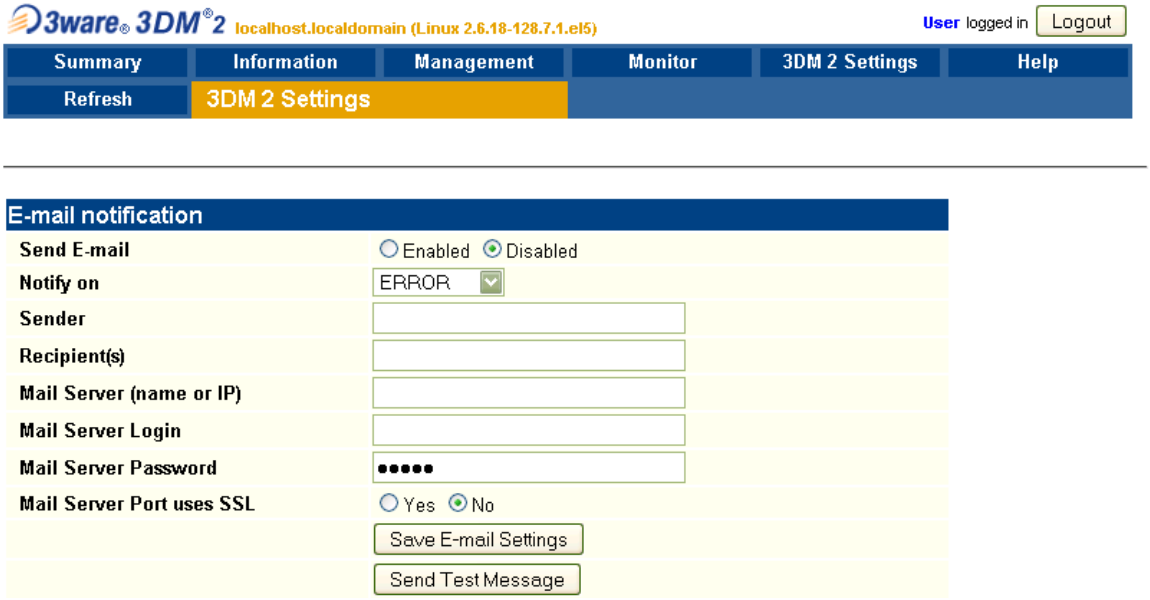
   Then, this page is displayed:



3. From the **Login** drop-down list, select **User** or **Administrator**. Users can check the status of the controller, units, and attached drives. Administrators can check status of, configure, and maintain the units and drives on the 3ware controller.
4. In the **Password** field, type **3ware**, which is the default password for both accounts.
5. Click **Login**. The following page is displayed:



6. To configure email alerts, click 3DM 2 Settings at the top of the page:



Define email settings in the E-mail notification section of the page. For more information, click **Help** at the top of the page.

18 Managing the SPHiNX Server

This chapter describes several tasks that are performed from time-to-time as needed. For more information about system tasks, refer to the online help.

Backing up the SPHiNX server

It is recommended that you back up the SPHiNX server before and after any major operation, such as an upgrade. This section describes how to create a system restore image, to save

- All configuration databases
- root and bill home directories
- Some contents of the **/etc** and **/usr/local/tape/etc** directories
- Virtual tapes (this is optional and only the tapes and their locations are backed up, not the data on the tapes)
- IBM Tivoli Storage Manager catalog and configuration information, for stacked exports

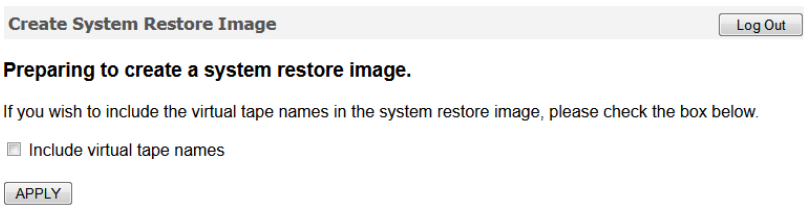
Note that a system restore image does not include virtual tape data.

To restore a system image, see "Recovering SPHiNX configuration data and settings" on page 190.

To create a system restore image

The procedure describes how to create a system restore image using the SPHiNX web interface. The system restore image contains a vital file, and if the file cannot be recovered, you may have loss of service for several days.

1. Make sure SPHiNX is not in use and that no virtual tapes are mounted.
2. Click **Support > System Updates** on the navigation pane.
3. Click **Create system restore image**. The Creating System Restore Image page is displayed.



4. Select the **Include virtual tape names** option if you want to back up virtual tape names (including vault and pool locations); data on the tapes is not backed up.
5. Click **APPLY**.
6. When prompted, choose to save the .tgz file.
7. Move the system restore image (.tgz file) to another server, so that it is not erased during re-installation.
8. If encryption is used in your environment, back up the most current backup of the key database:
    a. Click **Configuration** > **Data Encryption** on the navigation pane.
    b. Under the host table in the KEY DATABASE BACKUP/RESTORE HOSTS section of the page, click **Backup to All**.

    A message should be displayed at the top of the page indicating whether the backup was successful.

    IMPORTANT:

a. Note the currently configured key server's hostname, port and key generator.

b. Note the backup locations defined for all remote backup hosts. You MUST make a copy of each remote file backup. Te restorign process may send an empty copy of the local key database to the host, thereby overwriting the copy of the database on that host.

Note If no backup hosts are listed in the TSM DB Backup Hosts table, you must add a backup host by clicking **Add Backup Host**. Refer to the help for details. Then, complete the steps here.

9. If using stacked export jobs to migrate data to physical tapes, back up the stacked-export database (also referred to as the "TSM database").
    a. Click **Configuration > System** on the navigation pane.
    b. Click **Manage Backup Hosts** in the list.
    c. On the Manage Backup Hosts page, click the **Backup To All Hosts** button.

If Data Encryption is enabled, back up the most current key database by completing these steps:

1. Log in to the SPHiNX server.
2. Use the **su** command to change to the bill user:

    ```
    su - bill
    ```

3. Determine the location of the most recent backup file by entering the following command:

    ```
    psql -d database -c "SELECT last_local_backup FROM ks_backup_config"
    ```

    Here is an example of the output from this command:

    ```
    last_local_backup
    ------------------------------------------
    /VAULT00/.ks_backups/LocalKSBackup.tar.gz(1 row)
    ```

4. Copy the .gz file to a remote system, for safe keeping.
5. Enter **exit**.
6. Log out of the server.

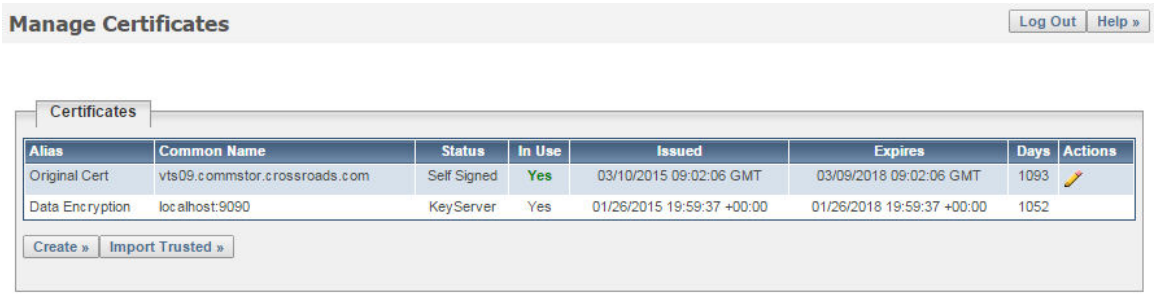
Managing certificates

SPHiNX uses X.509 certificate-based Secure Sockets Layer (SSL) communication between the user's browser and the SPHiNX web server. When SPHiNX initially starts up, it automatically generates a self-signed certificate. If you decide not to use a certificate approved by a Certificate Authority, no further action is required.

If you use a self-signed certificate for SSL, your browser may display a certificate warning when you access SPHiNX. To prevent this warning, use a certificate signed by a Certificate Authority (CA).

To create and manage certificates

1. Click **Security > Certificates**. The following page is displayed:



2. Create a certificate as described in the online help. To view help, click **Help** at the top of the page.

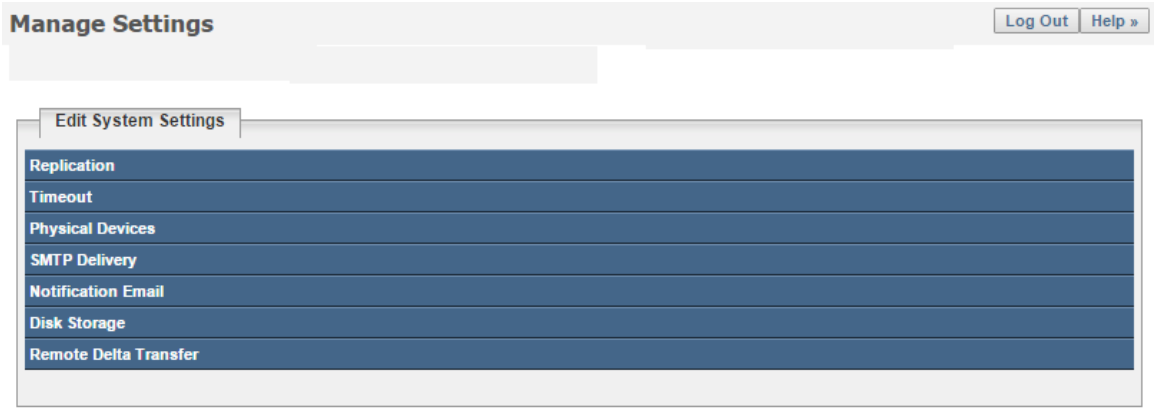
Configuring system settings

You can configure the following settings for the SPHiNX server:

- Session timeouts, to allow inactive browser and command line sessions to time out
- SMTP settings, to define the email host and port that will use to send email notifications
- Notification settings, to define email addresses that will notifications about disk and capacity usage

To configure system settings

1. Click **Configuration > System** on the navigation pane.
2. Click **Edit System Settings**. The following page is displayed:



3. Configure the settings as described in the online help. To view the help, click the **Help** button at the top of the page.

Powering up and down

Perform these procedures to power up the system and start services and to power down (halt and shut down) the system.

To power up

1. Press the power button located on the front panel of the SPHiNX server module. The power button on the front panel changes from yellow to green, and the server module self-boots.

   Allow the SPHiNX server to completely boot before proceeding. The console will display a login prompt when it is ready to proceed.

To power down

1. Power down the SCSI converter using the power switch on the rear panel, if necessary.
2. Execute the halt command by clicking **Administration > System Tasks** on the navigation pane of the web interface and then clicking **Halt the System**.

   Allow the SPHiNX server to completely shut down before proceeding. The SPHiNX server's console will indicate "System Halted".
3. Press the power button located on the front panel of the SPHiNX server module. The button light changes from green to yellow.

Maintaining the file system

The file system of the SPHiNX server requires maintenance for optimal performance.

Performing a file system check

Several utilities are provided to check a file system's integrity, depending on the file system type:

- For ext3 and ext4 file systems, the **fsck** utility checks the consistency of the SPHiNX file systems. ext3 and ext 4 are in use on all partitions (root and data) of the SPHiNX 1U-s, 2U-s, 3U-s, and 3U-ns appliances.
- For ZFS, the **zpool scrub** utility is used to check data integrity.

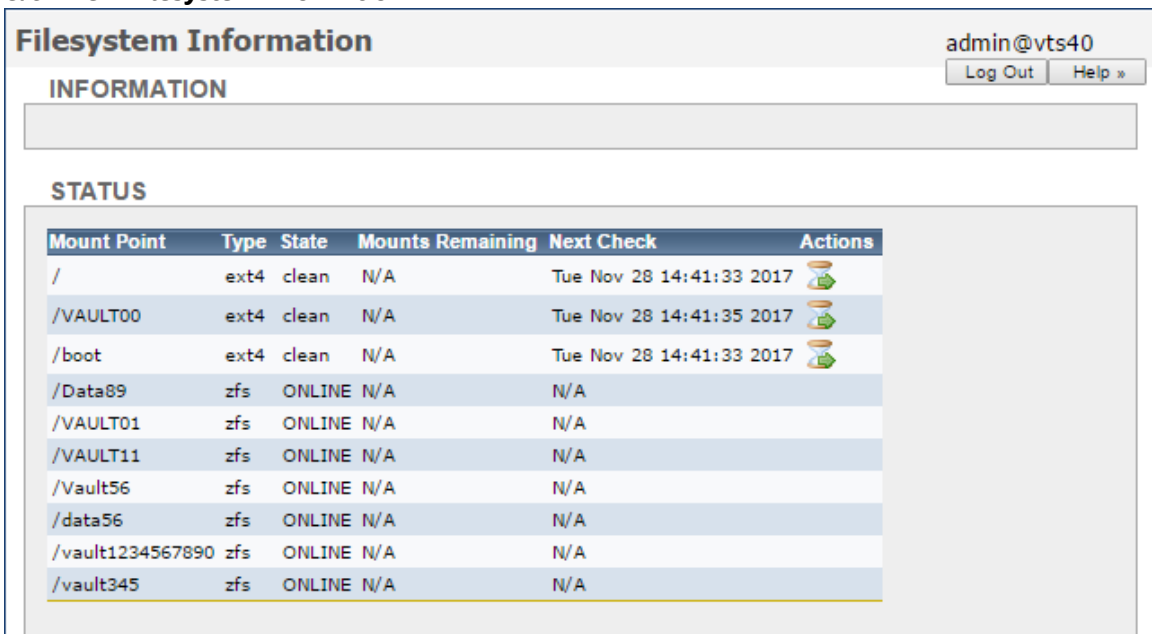
On ext3 and ext4 file systems, fsck may run automatically after a reboot and can take several hours to complete. On ZFS, the scrub utility runs at 9AM on the first Tuesday of every month. SPHiNX enables you to control when a file system check runs; you can postpone it once, thereby allowing you to schedule downtime to run the file system check.

You can use the Filesystem Information page to view fsck status for mounted file systems and postpone a file system check, if necessary. Be aware that this page does *not* list the last check nor the next check for GFS volumes.

Note It is highly recommended that you run fsck on all disk subsystems, to maintain disk consistency and health.

To review file system status

1. Click **Administration > System Tasks** on the navigation pane of the SPHiNX web interface.
2. Click **View Filesystem Information**.



Mount Point	Type	State	Mounts Remaining	Next Check	Actions
/	ext4	clean	N/A	Tue Nov 28 14:41:33 2017	
/VAULT00	ext4	clean	N/A	Tue Nov 28 14:41:35 2017	
/boot	ext4	clean	N/A	Tue Nov 28 14:41:33 2017	
/Data89	zfs	ONLINE	N/A	N/A	
/VAULT01	zfs	ONLINE	N/A	N/A	
/VAULT11	zfs	ONLINE	N/A	N/A	
/Vault56	zfs	ONLINE	N/A	N/A	
/data56	zfs	ONLINE	N/A	N/A	
/vault1234567890	zfs	ONLINE	N/A	N/A	
/vault345	zfs	ONLINE	N/A	N/A	

Here is a description of the columns in the STATUS section of the Filesystem Information page:

Mount Point — Lists each file system defined on the SPHiNX system. Note that no mount point is listed for unmounted file systems.

Type — Displays the type of file system installed (ext3, ext4, ZFS, and so on).

State — Provides the result of the last file system check. The "clean" state indicates that there are no outstanding journal transactions and the file system was correctly unmounted at last reboot. The "not clean" state indicates that the file system requires checking because of a problem, such as a system crash, file system panic, or incomplete journal transaction.

Mounts Remaining — Provides the number of mounts remaining before the fsck utility will run (after the next boot). The number is displayed in red if less than three mounts remain. N/A is displayed if mount-based checks are not enabled for the file system.

Next Check — Provides the date and time when the fsck utility will run (after the next boot). The date and time are displayed in red if the file system check will run in the next 24 hours or is past due. N/A is displayed if time-based checks are not enabled for the file system.

Actions — Provides buttons for the actions you can perform for each file system.

The STATUS table is also displayed on the Reboot the System - Confirmation page, though you cannot postpone a file system check from that page.

For more information, see the online help. To view help, click the **Help** button at the top of the page.

To run a file system check manually

On ext3 and ext4 file systems, you can run the **fsck** command manually instead of waiting for it to run automatically:

1. Ensure no I/O is running on the system.
2. Log in to a console as the **root** user. Or, log in and change to the **root** user using the **su** command.
3. Use the **blkid** command to determine where the partition to be checked is mounted. In the example output below, /VAULT01 is mounted on /dev/sdc1.

```
/dev/sda1: UUID="b0fdddc4-bfd4-4f3d-84b6-d1c5e1e05e54" TYPE="ext4"
/dev/sda2: UUID="a1eed5a0-7196-41ed-836f-3b7fad7aa402" TYPE="ext4"
/dev/sda3: UUID="9f0657dc-3e42-4f72-86f0-bf6e109df835" TYPE="swap"
/dev/sda4: LABEL="/VAULT00" UUID="656bf2d0-4746-4a7b-b26a-
ae5b21d45466" TYPE="ext3"
/dev/sdc1: LABEL="/VAULT01" UUID="87df71fc-fb90-47f2-a9d4-
5d39904e57d8" SEC_TYPE="ext2" TYPE="ext3"
/dev/disk/by-path/pci-0000:04:00.0-scsi-0:0:0:0-part1: UUID="b0fdddc4-
bfd4-4f3d-84b6-d1c5e1e05e54" TYPE="ext4"
/dev/disk/by-path/pci-0000:04:00.0-scsi-0:0:0:0-part2: UUID="a1eed5a0-
7196-41ed-836f-3b7fad7aa402" TYPE="ext4"
/dev/disk/by-path/pci-0000:04:00.0-scsi-0:0:0:0-part3: UUID="9f0657dc-
3e42-4f72-86f0-bf6e109df835" TYPE="swap"
/dev/disk/by-path/pci-0000:04:00.0-scsi-0:0:0:0-part4:
LABEL="/VAULT00" UUID="656bf2d0-4746-4a7b-b26a-ae5b21d45466"
TYPE="ext3"
/dev/disk/by-path/pci-0000:0c:00.1-fc-0x500508b3009079f1-lun-2-part1:
LABEL="/VAULT01" UUID="87df71fc-fb90-47f2-a9d4-5d39904e57d8"
TYPE="ext3"
```

4. Unmount the vault to be checked using the **umount** command.

```
umount vault
```

5. Run the **fsck** command on the vault. Note that this may take a long time.

```
fsck -y partition
```

Example output:

```
fsck from util-linux-ng 2.17.2
e2fsck 1.41.12 (17-May-2010)
/VAULT01: clean, 1199/183123968 files, 73436527/366247853 blocks
```

6. Remount the vault when complete:

```
mount partition        vault
```

Monitoring files and directories

The following files and directories should be monitored. Remove old data as needed.

Several directories store files that are generated on a regular basis. Files may accumulate in the following directories:

/tmp — Used for temporary files, this directory contains a variety of items including files, fifos, and directories

/var/log — Contains system log files

/usr/local/tape/log — Contains SPHiNX log files

/usr/local/tape/trace — Contains trace logs generated by some programs

/var/spool/mail — Contains user mail folders.

/var/spool/mqueue — Contains outbound mail

/var/spool/clientmqueue — Contains outbound mail not yet processed by the host's MTA.

It is recommended that you monitor these directories and archive (or purge) old files as needed. You can use several commands to help manage the directories:

- To view the size of a directory, run the following command (as root):

  `du -sh /dir_path`

- To see the oldest files in the directory and their sizes, run this command (as root):

  `ls -alth /dir_path`

The system facility, which is called logrotate, is used to rotate log files on a daily basis. The configuration files for logrotate are located in **/etc/logrotate.d**. You can tune the settings in this file to rotate and overwrite files as needed.

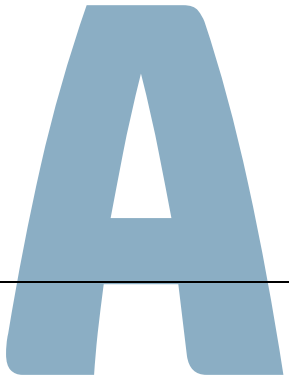
Several scripts are available that clean up after files that were created and abandoned due to system or application errors. These include the following:

- **rmoldbylist**
- **rmoldsync**
- **rmoldfilelist.pl**

In addition, errors in processes such as cron can cause mail messages to accumulate in the mail directories. If a mail transfer agent is configured and running on the SPHiNX server but forwarding for the root and bill accounts is not configured, mail can accumulate in the mail folders.

Finally, if Data Encryption is enabled, the **/var/log/te-server** directory can accumulate files.

Troubleshooting



This chapter provides information to assist you in addressing problems you may encounter while installing and using SPHiNX. If you cannot solve an issue using this information or if you must contact Support, gather the following information:

- SPHiNX hardware platform or model number
- The operating system and firmware versions of the SPHiNX server
- The version of SPHiNX, which can be found on the System Status page
- Whether external storage is attached to SPHiNX (disk array, network attached storage, and so on)
- The symptom of the problem
- The last time SPHiNX functioned properly
- The task (backup, restore, export, and so on) that was occurring at the point of failure

You can also run the getVTS_dbginfo utility, which is provided on the SPHiNX server. This utility collects log files and system information that can used to troubleshoot SPHiNX issues. To run getVTS_dbginfo, log in to the SPHiNX server, change to the root user (using the **su** command), and enter the following command:

```
/usr/local/tape/bin/getVTS_dbginfo
```

To collect GFS information, enter this command:

```
/usr/local/tape/bin/getVTS_dbginfo -g
```

A zipped archive file named **VTStimestamp.zip** is created in the **/usr/local/tape/troubleshooting/** directory. After the file is created, send it to Support.

Finally, you can generate a troubleshooting package from the web interface. Click **Support > Troubleshooting** on the navigation pane. Refer to the online help for more information.

Diagnostic techniques

For diagnosing problems, the following tools may be helpful.

PuTTY (Telnet/SSH client)

This is a GUI-based application to issue Telnet, SSH, and other connection commands to a host server. You can download PuTTY from http://www.chiark.greenend.org.uk/~sgtatham/putty/.

Virtual Network Computing remote control software

VNC software enables you to remotely access the console of a UNIX server. VNC must be configured on the host server before you can use it from a client. You can download VNC from http://www.vnc.com/.

Intelligent Platform Management Interface card and 3ware RAID controller

The SPHiNX server provides an Intelligent Platform Management Interface (IPMI) card, which has a dedicated Ethernet port for management use. Also, the server uses a 3ware RAID controller that can be configured to notify users of hardware problems. See "Configuring Alerts" on page 138 for more information.

HPE health monitoring utilities

You can use HPE health monitoring utilities to manage HPE systems, to maximize system uptime and health. The agent package integrates with HPE Systems Insight Manager (SIM), Insight Manager Console, HPE Services Essential Remote Support Pack, and HPE NonStop Cluster Essentials. It monitors all serviceable system components (drives, fans, power supplies, and so on).

To use these utilities, you must configure them. Refer to *HPE Systems Insight Manager Installation and Configuration Guide for Linux* for your appropriate HPE SIM version.

If you want to use HPE SIM, you must install it on SPHiNX. Be aware of the following:

- You must install the net-snmp package before installing HPE SIM.
- Installing HPE SIM overwrites the **/etc/ld.so.conf** file by adding the **/opt/hpsmdb/lib** path. This causes the Tapeserver process to fail startup because it cannot connect to the database. To workaround this issue, run the following commands to prepend the standard linker path *after HPE SIM is installed*:

```
sed -i '1i/usr/lib64' /etc/ld.so.conf
ldconfig
reboot
```

Configuration of HPE systems health is out of this document's scope. Please refer to appropriate HPE documentation for HPE system health tools configuration.

Note To monitor MSA2000 and P2000 storage arrays using HPE SIM, you must install and configure SIM on a system other than SPHiNX.

Then, after installing HPE SIM, SNMP must be enabled to use HPE Insight Manager; SNMP is disabled by default for security reasons. As the root user, enter this command:

```
chkconfig snmpd on
```

Common issues

The following sections provide general information to diagnose hardware components and software features of the SPHiNX system.

IBM i server

If there are problems using the drive, perform the following:

- Using the STRSST command, ensure that the IOA and the associated tape devices are “Operational”.
- Using the WRKCFGSTS *DEV *TAP command, ensure that the tape device is “Available to use” or “VARIED ON”.

If the drives are operational but errors are encountered while accessing the data, check the media class, or density, setting for that cartridge using the DSPTAP command. The currently recommended media classes supported by IBM i with SPHiNX are the following:

- 3580-TD1
- 3580-TD3
- 3580-TD4

Windows Server

If problems arise, you may need to rescan the devices using the Device Manager. To launch the Device Mapper, enter **devmgmt.msc** on the command line of the server. Select any component in the hostname tree, right- click on any component, and select **Scan for hardware changes**. This should discover new VTDs.

If devices do not show up after a rescan, if VTDs show up as Unrecognized devices or tape devices, or if VTLs show up as Medium Changer devices, verify that the correct port on the SPHiNX server is connected to the host. Or, reboot the SPHiNX server to reset the Fibre Channel card, if it’s connected to the host.

Finally, the backup management application may not work well with the driver on the Windows Server system. You may need to update the driver installed on the Windows system.

SPHiNX server module

You can troubleshoot various areas of the SPHiNX server module.

Host server

Verify the following:

- Is the server powered on?
- Are the lights on?
- Are all of the cables secured tightly?
- Are any pins bent on any of the cables?
- Are all of the PCI cards seated properly? Is the plastic clip secured for each?
- Are messages present in the Power On Self Test (POST)?

If necessary, reseat the PCI cards. Halt SPHiNX from the web interface, power down the server, unplug the power cord, and then remove cables and reseat the PCI cards.

Hard drives

Verify the following:

- Are the hard drives seated properly?
- What is the color of the drive LED?

A green LED indicates normal operation; amber indicates failure. You can also remove all hard drives and reseat them individually. Be sure to properly shut down SPHiNX before performing this operation.

SCSI controllers

You can rescan all SCSI controllers to list devices. Be sure to stop the tape drives in SCF on the host server before initiating the scan. Run these commands (as root) to rescan the SCSI controllers:

```
cd /usr/local/tape/bin./rescan-scsi-bus.sh -l -c -r -w
```

Output is listed on screen and in the **/usr/local/tape/log/rescan.txt** file. The SPHiNX application must be restarted when a new physical tape device is found and must be used. If the new devices were not detected, you can unplug the Fibre Channel connection to the SPHiNX server for two minutes or reboot the system.

File system

Verify the following:

- Has anything changed?
- Is performance slow?
- Is GFS running on the system?
- Is the problem occurring for a particular vault or all vaults? Is the problematic vault on internal or external disk storage?
- What is the result of the last vault check on the external storage?

You can check for file system check messages in the system log and the result of the last vault check. If GFS is running, check connectivity between the systems by pinging the systems from the command line of the operating system.

To diagnose file system problems, the following commands are useful:

`df` — Shows disk utilization

`top` — Shows CPU utilization, swap space, zombie processes, and so on

`top -b -n 10 > output.txt` — Runs `top` in batchmode

`du` — Shows file space usage

`ps -xaf` — Lists running processes

`tail -f -n 24 filename` — Displays a real-time file listing

`grep filename` — Searches for a string in a file

`man` — Displays help for a program

`more` *`filename`* — Lists a file

`reset` — Resets the current terminal

Following a hard (unclean) shutdown of SPHiNX (such as a system crash or loss of power), the system may be left in an inconsistent state. Many services running on the server use PID files to tell the system that a service is running. When a service is started, the PID file is created. When a service is shutdown, the PID file is deleted. If SPHiNX is shutdown uncleanly, the PID files will not be deleted. When the system comes back up, it assumes that the service is running and does not try to restart the service. This will cause SPHiNX to function incorrectly or not at all. Here is an example of a service failing to start due to a stale PID file that resulted from a crashed server, in /var/log/messages.

```
Nov 6 12:29:18 ProdVTS rhdb: Starting PostgreSQL - Red Hat Edition service:
failed
```

To address this issue, reboot the server twice. This will allow the server to clean up the PID files as the server shuts down and allows all of the necessary services to start properly when the server boots up.

Control-Alt-Delete

To avoid rebooting the system by **Control-Alt-Delete** activate the script that overrides the command. To do so, follow the procedure described below:

1. Log into CLI as root.
2. Rename the file **/etc/init/control-alt-delete.override.SP-1242** to **/etc/init/control-alt-delete.override**.

Note: No system reboot is required.

Web interface

If the web interface stops responding, verify the following:

- Access the interface from a different workstation.
- Ping the address.
- Check the Ethernet cable.
- Check Ethernet connectivity and activity LEDs.

The Apache web server is responsible for running the SPHiNX web interface. To verify that Apache is running:

```
/etc/init.d/httpd status
```

A message similar to the following should be displayed:

```
httpd (pid 25380 25015 25014 25013 25012 25011) is running...
```

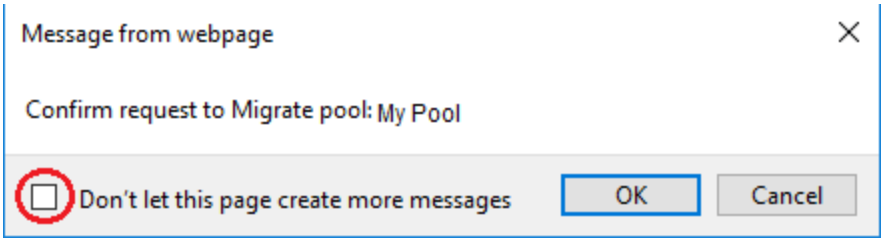
You can reboot SPHiNX to attempt to solve the problem.

If you can ping the system but the web interface is not accessible, verify the **/etc/hosts** file; the SPHiNX server may not be listed (so the httpd service will not start). Add the hostname and address to the file and then restart the httpd service to fix this problem.

Browser

If you use Firefox or Internet Explorer as browser(s) you could get pop-up messages asking to confirm the operation that you want to perform (Import/Export, Migrate, Erase, Unselect, ect.). If you cancel the operation a second pop-up will ask you to re-confirm.

To avoid freezing the User Interface, either leave the check-box of the second pop-up unchecked or press Ctrl+Shift+R. If the issue keeps occuring change the web browser.



External storage or the SAN

Verify the following:

- Is the storage array powered on?
- Are the lights on?
- Are all of the cables secured tightly?
- Are any cables broken?
- Is the link LED on? What is the color of the LED?

A green LED indicates normal operation; amber indicates failure.

Virtual tape operations

If you are unable to manually mount a virtual tape, perform the following:

- Check the color of the virtual tape label. Gray indicates the virtual tape is in use by Import/Export or is remotely mounted.
- Verify that the autoloading pool containing the virtual tape is not in use.
- Verify that Data Encryption is enabled and configured properly in a cluster environment. The mount will fail, for example, if the key server is not configured on all servers.

If virtual tapes are mounted as read-only or write failures occur, verify that licensing has not been exceeded (for the VTD or Capacity license).

If you cannot import a physical tape, perform the following:

- Check the tape drive for power.
- Check the tape drive for tape ready indicators.
- Check the SCSI cable to the tape drive.
- Check file system Free (Pct).

If you cannot export a virtual tape or an export failed, perform the following:

- Check the tape drive for power.
- Check the tape drive for tape ready indicators.
- Check the SCSI cable to tape drive.
- Check that the tape is in the drive.
- Check the media write-protection.

If you cannot access a virtual tape because it is locked, perform the following:

- Check other SPHiNX systems for remotely mounted virtual tapes.
- Reboot SPHiNX to clear all local file locks.

If an autoloading pool did not recycle, verify that Autoloading or Recycle is selected on the Pool Maintenance page. If virtual tape operations failed to a remote server, verify that licensing has not been exceeded (for VTD or Capacity licenses).

Data Replication

If you can no longer replication virtual tapes, verify that the network settings are configured correctly for the target servers. For example, if you move a target SPHiNX server to another network (thus changing the IP address of the target), replication will not work. It is recommended that you use hostnames when configuring replication, if DNS is configured on your network. If you provide IP addresses instead of hostnames and then the IP address of the source or target server changes, you must delete the target server(s) and then complete all configuration procedures again.

Refer to the “Configuring replication settings” help topic for information about specifying replication settings.

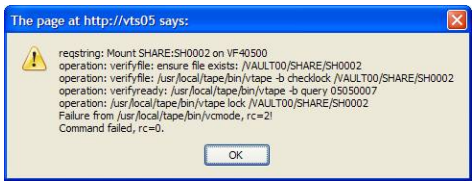
If you need to restore exported virtual tapes as part of disaster recovery, refer to the help for details.

Data Encryption and failed tape operations

If SPHiNX attempts to perform an operation on an encrypted virtual tape, Data Encryption must be enabled and the key server that was used to encrypt the tape must be configured on the server where the tape resides. If not, the tape operation will fail and an error message is displayed indicating that the operation failed. This section provides an overview of the error messages that are displayed. See "Enabling and Configuring Data Encryption" on page 87 for instructions on enabling Data Encryption and configuring a key server.

- Mounting an encrypted tape

  An error similar to the following is displayed:

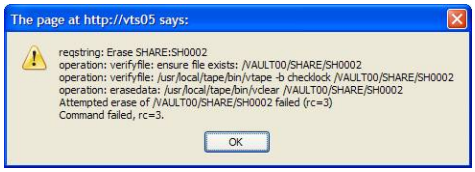


  Also, a message similar to the following is displayed on the web interface:

```
Request: Mount SHARE:SH0002 on VF40500 for read-write --- Failed!
```

- Erasing an encrypted tape:

  An error similar to the following is displayed:

  Also, a message similar to the following is displayed on the web interface:

  ```
  Request: Erase SHARE:SH0000 --- Failed!
  ```

- Exporting an encrypted tape:

  A message similar to the following is displayed on the web interface:

  ```
  Thu 2008-01-17 09:49:31: SHARE:SH0000 Export data transfer failed,
  rc=3
  ```

- Erasing all virtual tapes in a pool on the Cartridge Maintenance page:

  A message similar to the following is displayed on the web interface:

  ```
  Erased 1 cartridge; Erasure of cartridge SH0002 in pool SHARE failed!
  ```

- Setting the virtual tape size on the Pool Maintenance page:

  A message similar to the following is displayed on the web interface:

  ```
  Unable to set size limit on SHARE:SH0001, rc=2. Operation aborted!
  ```

  After the operation aborts for the encrypted tape, any tapes for which this operation is attempted will also fail.

You can also check **/usr/local/tape/log/SecureVTS.log**, which logs all tape operations associated with encryption. Go to the bottom of the log to look for problems.

Log files

SPHiNX provides many log files for troubleshooting issues with various functions of the system. For example, the event log lists an error if a password is invalid or an IP address does not connect.

To access logs from the SPHiNX web interface

Click **Support > Logs** on the navigation pane and then click a link to examine logs.

This section provides in-depth information about several of the logs. Refer to the online help for information about using the web interface to view and download log files.

Event log

The event log file is an especially useful log that is generated by SPHiNX. It records information about system events, such as the creation and deletion of virtual tapes, failures of processes and services, and the status of jobs and policies. The messages include information about the time and date of the event as well as the name of the user who initiated the event. Use the messages in this file to detect problems,

track down the source of faults, and audit users. In addition, information in the system event log can be retrieved by third-party applications, for notification purposes.

Log format

Each entry in the event log follows the same format, as shown in the following example:

```
2006-08-28 16:25:18|WARNING|440002|5900-E|
127.0.0.1|Tapeserver01|administrator||Access Control RESTORE OPEN defaults
have been restored
```

Messages are up to 255 characters in length; each message field has a character limit. The attributes that have a variable length are automatically compressed to the available space. Here is a description of each message field:

Attribute	Format Example	Character Limit	Description
Timestamp	2006-08-28 16:25:18	19	Time and date when the message originated, in a format that is specific to the locale.
Severity	WARNING	8	The degree of impact or seriousness of the event reported by the message. (See "Message severity" on page 166.)
Message ID	440002	6	A unique six-digit identifier. All message IDs contain the severity, subsystem, and message ID. The unique ID falls within a numerical range of 0-999999. (See "Message IDs" on page 166.)
System ID	5900-E	7	The make and model of SPHiNX on which the message was generated.
IP address	127.0.0.1	15	The IP address of the user or client that initiates a function on a page of SPHiNX.
Server name	Tapeserver01	15	The Domain Name Server (DNS) name of the computer that hosts the server instance.
User	administrator	15	The user ID under which the associated event was executed.
Program		None	The name of the program that generated the message. This field is often omitted, such as when the web interface generates the message.
Message text	Access Control	177	A description of the event or condition.

Attribute	Format Example	Character Limit	Description
	RESTORE OPEN defaults have been restored		

Message severity

The severity attribute indicates the potential impact of the event or condition that the message reports.

Note Though you can change the debug level on the Set Debug Level page, the debug level is reset to Error every time SPHiNX is restarted.

The following table lists the severity levels for log messages, starting from the lowest level of impact to the highest.

Severity ID	Severity Level	Description
2	Info	A normal operation.
4	Warning	A suspicious operation or configuration that might not affect normal operation.
6	Error	A user error that the system or application can handle with no interruption and limited degradation of service.
8	Critical	A system or service error from which the system can recover, although there might be a momentary loss or permanent degradation of service.

Message IDs

Each six-digit message ID is made up of the following:

- The first digit represents the severity ID (see "Message severity" on page 166)
- The second and third digits represent the subsystem ID
- The final three digits represent the event ID

The following provides a list of subsystem IDs:

ID	Subsystem
21	Cartridge maintenance
22	Pool maintenance

ID	Subsystem
24	Data Replication
26	Scan/Cleanup
27	Import
28	Export
33	Utilities
35	Services
40	Factory setup
51	Tape connections
52	Logical tapes
53	Virtual tapes
61	Access Control defaults
62	Access Control users
63	Access Control groups
64	Access Control rights
65	Secure password management
71	Erase by list
72	Delete by list
81	Crumb
91	System status

Export log

This log provides information about all export operations. If a problem occurs, a return code is listed in the log file, such as in this example:

```
000000016: Fri Jun 11 10:45:02 2010: NSPOOL:V16009 Rewind failed!
/dev/nst2, rc=1
```

Here is an explanation of the return codes that may be displayed in this log:

Return Code	Possible Cause(s)	Corrective Action(s)
-1	• File is empty on export • Rewind failed • Parameters incorrect or missing (internal error)	• Retry with a non-empty file • Load tape in drive • Make sure tape drive is on and properly configured • Check cabling
1	Could not allocate buffer (malloc)	N/A
2	Could not lock memory (mlock)	N/A
3	• Could not open data source file • Invalid data source file specified or file not found	Specify a valid source file
4	Could not open physical tape drive; usually due to a configuration error	• Make sure tape drive is on and properly configured • Check cabling
5	Could not load and rewind tape before copy	• Load tape in drive • Make sure tape drive is on and properly configured • Check cabling
6	Could not rewind tape after copy	• Make sure tape drive is on and properly configured • Check cabling
7	Could not issue SCSI write command, possible because of too much data for physical tape	• Use larger tape or less data • Verify configuration • Check cabling
8	SCSI write command failed Too much data for physical tape	• Use larger tape or less data • Verify configuration • Check cabling.
254	Incorrect file ownership	Change ownership to bill.bill

Scan/Cleanup log files

While the Scan/Cleanup is running, a log file is created in **/usr/local/tape/log**. The file is named **erasebylist.date.log**, such as **erasebylist.12Mar06.log**. The format of the information written to the file is

as follows:

```
02Mar05 14:41:factory:erase-by-list

Wed, 02 Mar 2005 14:41:25 -0800
/VAULT00/BILL/Q00001 erased
/VAULT00/BILL/Q00002 erased
/VAULT00/BILL/Q00003 erased

Total Freed: 0
Total Erased: 3
Total Errors: 0
```

If the freed space is negative, a virtual tape that had no metadata associated with it was erased and the metadata was added. Thus, the virtual tape disk file size actually increased slightly. Typically, you would erase a virtual tape that was never written or erased.

The log files are created as needed on a daily basis and are relatively small.

Other log files

The following log files are generated and saved in various directories on the SPHiNX server.

Operating system logs:

- **/var/log/messages**
- **/var/log/cron**
- **/var/log/boot.log**

Apache web server logs:

- **/var/log/httpd/error_log**
- **/var/log/httpd/access_log**

SPHiNX function logs:

- **/usr/local/tape/log/debug.*** (available from the SPHiNX web interface)
- **/usr/local/tape/log/mount.log**
- **/usr/local/tape/log/export.log** (available from the SPHiNX web interface)
- **/usr/local/tape/log/event.log** (available from the SPHiNX web interface; see 164 for more information)
- **/usr/local/tape/log/scanat.log**
- **/usr/local/tape/log/vtape.log**
- **/usr/local/tape/log/upgrade.log**
- **/usr/local/tape/log/rescan.txt**
- **/usr/local/tape/log/SecureVTS.log**

Note Though you can change the log level of these files, the log level is reset to the default every time SPHiNX is rebooted.

To view log files, the following commands are useful:

`view logfile` — To search the file

`tail -f -n 35 logfile` — To list the file in real-time

`grep -ni string logfile` — To search for a specific string

`less logfile` — To search a file by paging through it

Compressed log files can be searched and viewed by using **zgrep** and **zless**.

Logwatch reports

Daily Logwatch reports enable you to view significant events that occurred on the system in the last 24 hours. The reports are generated by parsing events in the Linux log directory (**/var/log**) and SPHiNX log directory (**/usr/local/tape/log**). A report is generated every day at 4AM before SPHiNX log files are rotated. Each Logwatch reports is deleted after 120 days. These reports are generated by an implementation of the logwatch system monitoring system; see http://www.logwatch.org/index.html for more information.

The VTS Events section of the logwatch report consists of topic headings followed by subject lines. Each subject line begins with a message ID (see "Message IDs" on page 166), is followed by a message explanation and ends with the count of such messages in the **event.log** file for the previous day.

To view a Logwatch report

 *Requires the View log files access right*

1. Click **Support > Logs** on the navigation pane.
2. Click **Examine Logwatch Output** in the Log Files section of the page. The VTS Server Logwatch Reports page provides a list of reports, and the newest report is listed first.
3. Click the name of a TXT file to view its contents.

Remote logging of audit log records

If necessary, you can enable remote logging of auditd log records. This is done using the rsyslogd facility provided with the SPHiNX operating system (Linux).

Note Log files are sent to the remote server in the clear text. Because the log files may contain audit data, be careful to evaluate the safety of remote logging.

To enable remote logging

1. Log in to the SPHiNX server as bill.
2. Use the **su** command to change to the root user:

   ```
   su -
   ```

3. Edit **/etc/rsyslog.conf** and add a line for the remote host. The following line is an example that logs kernel messages.

   ```
   kern.* @remote.log.host.domain.com:514
   ```

where **kern.*** specifies to log all kernel messages and *remote.log.host.domain.com* specifies the hostname or IP address of the remote host that will log messages for the target host. To log other messages, refer to the auditd, rsyslogd, and rsyslog.conf man pages.

4. Run the following commands:

```
chkconfig auditd off
service auditd stop
service rsyslog restart
```

These commands stop local logging through the auditd process and force audit records to be logged through rsyslogd. The rsyslogd facility will send log messages to the remote system.

5. Log out of the SPHiNX server.
6. If necessary, enable the remote system to receive the log messages.

The following steps describes how to configure rsyslogd on a remote Linux server.

a. On the target (remote) system, log in.

b. Become root:

```
su -
```

c. Modifying the **/etc/rsyslog.conf** file and uncomment the following lines:

```
# $ModLoad imudp
# $UDPServerRun 514
```

d. Restart the rsyslogd daemon by entering this command:

```
service rsyslog restart
```

e. On the local system, verify that messages are being logged in the remote system. For example, use the logger utility:

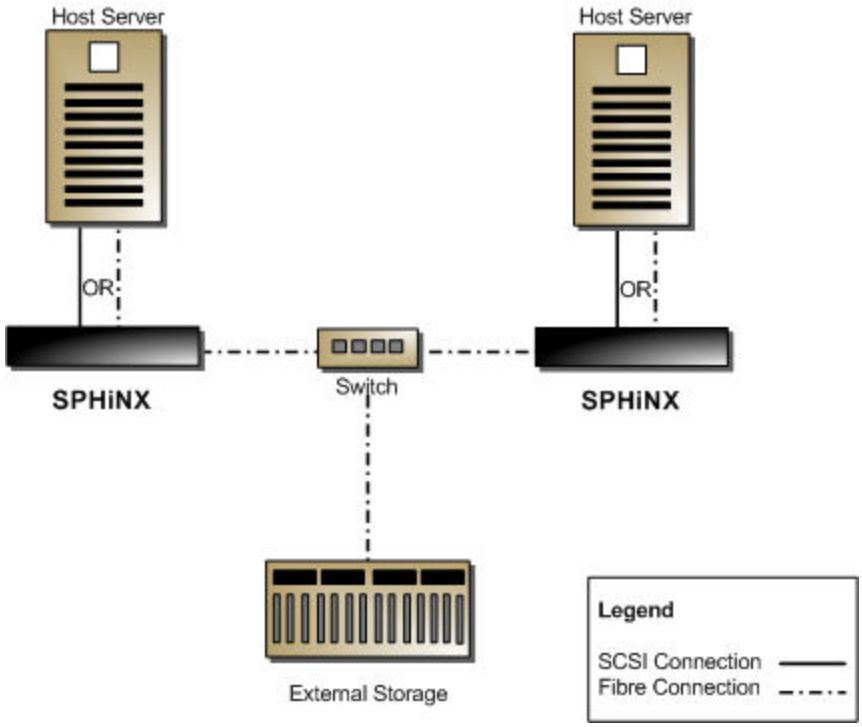
```
logger -p kern.info test message
```

This should result in an entry such as “Jun 29 15:29:51 vtsdev24 bill: test message” appearing in the remote system's **/var/log/messages** file.

Note The **rsyslog.conf** file on the remote system will determine if and where the message is logged. Use "man rsyslog.conf" for more information.

Installing GFS for SPHiNX

The Clustered Option is an advanced feature that allows Linux servers to simultaneously read and write files on a single shared file system on a SAN. SPHiNX is based on Linux, and clustering (through the use of GFS) enables multiple SPHiNX servers to access a shared set of pools and virtual tapes. Here is an example GFS configuration:



With GFS, all SPHiNX servers connect to each other over Fibre Channel to the same storage array, and GFS allows each SPHiNX to access all vaults at the same time. If a server becomes unavailable, other servers can still access the vaults.

This appendix provides instructions to install GFS. To upgrade GFS in your environment, refer to the *Release Notes*.

To maintain GFS and manage clusters, refer to these documents for more information:

- GFS2 — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/5/html/Global_File_System_2/index.html

- Cluster management — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Cluster_Administration/index.html
- Conga (luci and ricci) overview — Chapters 3 and 4 of this guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Cluster_Administration/index.html
- Fencing overview — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/High_Availability_Add-On_Overview/ch-fencing.html
- Configuring fencing devices with Conga (luci and ricci) — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Cluster_Administration/ch-config-conga-CA.html
- All other Red Hat documentation — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/index.html

Installing GFS

This section provides steps to install GFS for the first time or to reinstall GFS and remove all volume data. If you want to upgrade GFS and keep volume data from a previous installation, refer to the upgrade procedure in the *Release Notes*.

During the installation of GFS, you must configure a fencing method for the cluster. You can configure Fibre Channel switch fencing if the external storage device is connected over Fibre Channel (for example, if the HP StorageWorks Modular SAN Array provides a built-in Fibre Channel switch). Or, you can configure HP Integrated Lights-Out (iLO) to handle fencing. Refer to the following for more information about fencing:

- Fencing overview — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/High_Availability_Add-On_Overview/ch-fencing.html
- Conga (luci and ricci) overview —Chapters 3 and 4 of this guide: https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Cluster_Administration/index.html
- Configuring fencing devices with Conga (luci and ricci) — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/html/Cluster_Administration/ch-config-conga-CA.html
- All other Red Hat documentation — https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/6/index.html

  Also, if you encounter problems while installing GFS, you may need to delete a cluster. The URLs listed here provide this information as well.

Before beginning

- Verify that physical cabling of the servers and storage is complete and connectivity has been established.

  Note When connecting to the Fibre Channel switch, ensure that multiple paths to SPHiNX are not configured if zoning is configured.

- Be aware that GFS requires system hostnames to be specified using all lowercase letters. If the hostname includes uppercase and lowercase letters or all uppercase letters, change the hostname

to use all lowercase letters before beginning installation. Failure to make the change will result in GFS cluster communication failures and ultimately a failure to start the GFS cluster.

- Make sure that NTP is configured on all nodes that will be included in the cluster so that all node times are the same.
- It is recommended that you use a static IP address for each node.

To install GFS

1. On each node (SPHiNX server) that will be included in the cluster, log in to the operating system and become root:

   ```
   su -
   ```

2. On each node, enter the following command to disable clustering services that are included with the GFS but not used by SPHiNX. Failure to disable these can cause the system to hang.

   ```
   chkconfig saslauthd off && service saslauthd stop
   ```

   If this command returns a failure, it is not an error. It indicates that the process was not running.

3. On one node, choose your device(s) to be used for GFS by partitioning the disk. You can use the **parted -l** command to list devices and note the partition information. If a partition is not listed, check connections to storage. Or, the storage may need to be configured; refer to the storage documentation for details.

   The same LUN presented by the storage device needs to be visible to all nodes through a Fibre Channel switch. You can verify that all nodes see the same LUN by using the following command on each host. This command returns a unique ID that can be seen by all nodes, though the /dev/sd*x* device names may be different. For example:

   ```
   scsi_id -g /dev/sdc
   ```

   may return 3600508b300908250f482e980860a002e.

   This command:

   ```
   scsi_id -g /dev/sdg
   ```

   may return 3600508b300908250f482e980860a002e.

   Finally, this command:

   ```
   scsi_id -g /dev/sde
   ```

   may return 3600508b300908250f482e980860a002e.

   Although the /dev/sd*x* device names are different, they all correspond to the same LUN in the storage array. Once a LUN is visible by all nodes, continue on with the partitioning the LUN using the **parted** command.

   SPHiNX assumes an empty, unpartitioned disk, and further disk partitioning is not performed. Cluster members will mount devices based on LVM names, not SCSI device names, and these GFS devices will not use disk labels.

   Complete these steps to partition the disk, where *x* is the partition number:

a. Erase the first 1MB of the disk by writing zeros to it:

```
dd if=/dev/zero of=/dev/sdx bs=1024 count=1024
```

b. Start the partition editor, which is an interactive program similar to fdisk:

```
parted -a optimal /dev/sdx mklabel gpt
```

c. Create a primary partition that will span the entire disk:

```
parted /dev/sdx mkpart primary 0% 100%
```

4. On one node, perform LVM initialization of the device.
   a. If GFS was previously installed and you want to remove all volume data, enter the following commands to remove the logical volume (lv1) and wipe labels from the physical volume (sd*x*1):

```
lvremove -f /dev/gfsvg1/lv1 gfsvg1
```

```
pvremove /dev/sdx1 -ff
```

When prompted, enter **y** to confirm.

   b. Create the physical volume by entering the following command:

```
pvcreate /dev/sdx1
```

You may need to use the **-ff** option to force creation.

   c. Create the volume group by entering the following (this example creates the **gfsvg1** group):

```
vgcreate gfsvg1 /dev/sdx1
```

   d. Create the logical volume by entering the following command. The **-l 100%FREE** option creates a logical volume using the entire volume group. Note that the **-l** flag below is a lowercase L, not the number 1. Similarly, **lv1** is lowercase L, v, and then number 1.

```
lvcreate -l 100%FREE -n lv1 gfsvg1
```

   e. Enter the following command to confirm the physical volume:

```
pvscan
```

Here is an example of the output:

```
PV /dev/sde1   VG gfsvg1   lvm2 [17.14 GB / 0    free]
Total: 1 [17.14 GB] / in use: 1 [17.14 GB] / in no VG: 0 [0   ]
```

   f. Enter the following command to confirm the volume group:

```
vgscan
```

Here is an example of the output:

```
Reading all physical volumes. This may take a while...
Found volume group "gfsvg1" using metadata type lvm2
```

   g. Enter the following to display details about the physical volume:

```
pvdisplay
```

Here is an example of the output:

```
--- Physical volume ---
PV Name               /dev/sde1
VG Name               gfsvg1
PV Size               17.14 GB / not usable 3.37 MB
Allocatable           yes (but full)
PE Size (KByte)       4096
Total PE              4388
Free PE               0
Allocated PE          4388
PV UUID               tTHBFt-6pqc-ILIY-Uis5-L8Yn-bvBu-SCN3MV
```

h. Enter the following to view details about the volume group:

```
vgdisplay
```

Here is an example of the output:

```
--- Volume group ---
VG Name               gfsvg1
System ID
Format                lvm2
Metadata Areas        1
Metadata Sequence No  2
VG Access             read/write
VG Status             resizable
MAX LV                0
Cur LV                1
Open LV               1
Max PV                0
Cur PV                1
Act PV                1
VG Size               17.14 GB
PE Size               4.00 MB
Total PE              4388
Alloc PE / Size       4388 / 17.14 GB
Free  PE / Size       0 / 0
VG UUID               lm4cH7-4wgq-s1VR-VNwc-pFC6-i54u-h5tKxk
```

i. Enter the following command to view details about the logical volume:

```
lvdisplay
```

Here is an example of the output:

```
--- Logical volume ---
LV Name                /dev/gfsvg1/lv1
VG Name                gfsvg1
LV UUID                VQUsmh-LI1E-rBIm-3tCe-9o6K-cjlp-ah8e4j
LV Write Access        read/write
LV Status              available# open                 0
LV Size                17.14 GB
Current LE             4388
Segments               1
```

```
Allocation              inherit
Read ahead sectors      0
Block device            253:0
```

5. On one node, create the GFS file system:
    a. Enter the following command. Note that any data that resides on the specified logical volume is destroyed.

    ```
    mkfs.gfs2 -p lock_dlm -t cluster_name:gfs01 -j journals
        logical_volume_path
    ```

    where

    -p lock_dlm sets the lock manager to DLM

    -t *cluster_name* specifies the cluster name; restrict the cluster name length to 15 characters or less

    -j *journals* specifies the number of journals to create, which should be the number of nodes plus two

    logical_volume_path specifies the path to the device (file system)

    Here is an example:

    ```
    mkfs.gfs2 -p lock_dlm -t sphinxdev:gfs01 -j 5 /dev/gfsvg1/lv1
    ```

    (The last part of the logical volume path is lv1: lowercase L, lowercase V, number one.)

    b. When prompted, enter **y** to proceed. Output similar to the following is displayed:

    ```
    Device:                    /dev/gfsvg1/lv1
    Blocksize:                 4096
    Device Size                1397.11 GB (366242816 blocks)
    Filesystem Size:           1397.11 GB (366242816 blocks)
    Journals:                  5
    Resource Groups:           5589
    Locking Protocol:          "lock_dlm"
    Lock Table:                "sphinxdev:gfs01"
    UUID:                      e042be76-bf6d-ec1a-0cfc-a95b4ec983fe
    ```

6. If you are creating multiple vaults, you must repeat steps 3-5 (on one node) for each GFS file system that will be used for vault storage.

7. Start ricci and luci.
    a. On each node to be included in the cluster, make sure that the luci system has a proper **/etc/hosts** file. Here is an example command to confirm the contents of the file:

    ```
    cat /etc/hosts
    ```

    Here is an example of the file for a two-node cluster:

    ```
    # Do not remove the following line, or various programs
    # that require network functionality will fail.
    127.0.0.1       localhost.localdomain   localhost
    192.168.80.115  vts15.domain.com   vts15
    192.168.80.135  vts35.domain.com   vts35
    ```

The file should list all cluster nodes. The localhost entry (including IP address and node name) is for the system you are using and the other entries are for the cluster nodes.

b. On each node, set the password and then start ricci:

```
passwd ricci
```

When prompted, enter a new password. Then, enter these commands:

```
chkconfig ricci on
service ricci start
```

To confirm that ricci is running, enter the following:

```
service ricci status
```

c. On one (and only one) of the nodes, start and configure the luci service. Red Hat recommends configuring luci on a non-cluster node. It will function properly on a cluster node, though web connectivity is lost while the system is rebooting. If the luci node goes down, the cluster cannot be administered with luci.

```
service luci restart
```

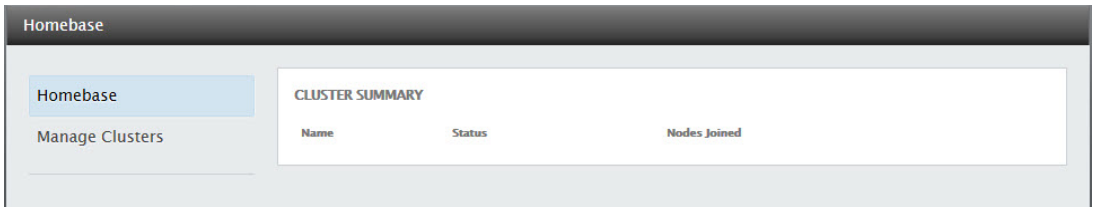
Here is an example of the output:

```
Adding following auto-detected host IDs (IP addresses/domain names), corresponding to `vtsdev10.domain.com' address, to the configuration of self-managed certificate `/var/lib/luci/etc/cacert.config' (you can change them by editing `/var/lib/luci/etc/cacert.config', removing the generated certificate `/var/lib/luci/certs/host.pem' and restarting luci):

(none suitable found, you can still do it manually as mentioned above)

Generating a 2048 bit RSA private key

writing new private key to '/var/lib/luci/certs/host.pem'

Start luci...                                              [  OK  ]

Point your web browser to https://vtsdev10.domain.com:8084 (or equivalent) to access luci
```

Note the URL given in the output; you will access it in the next step.

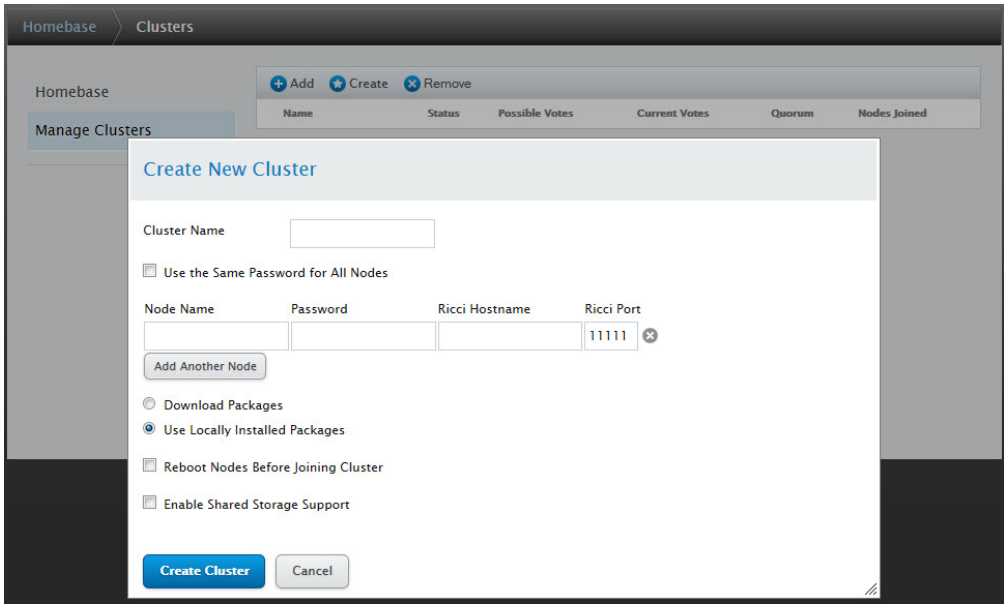
8. On one node, configure the cluster using the luci web interface. These steps create the cluster, configure fencing, and add GFS storage to the cluster.
   a. Access the web interface by loading the URL given in the previous step in a web browser.
   b. When prompted, accept the certificate(s) permanently.
   c. Log in as **root** and enter the SPHiNX password.
   d. Click **OK** if a certificate domain mismatch warning is displayed.

e. Click **OK** to dismiss the warning message. A page similar to the following is displayed:



f. Create the cluster:

i. Click **Manage Clusters** and then click **Create**.



ii. In the **Cluster Name** field, enter the same cluster name that you used when creating the GFS file system (step 5a).

iii. If desired, select the **Use the Same Password for All Nodes** option.

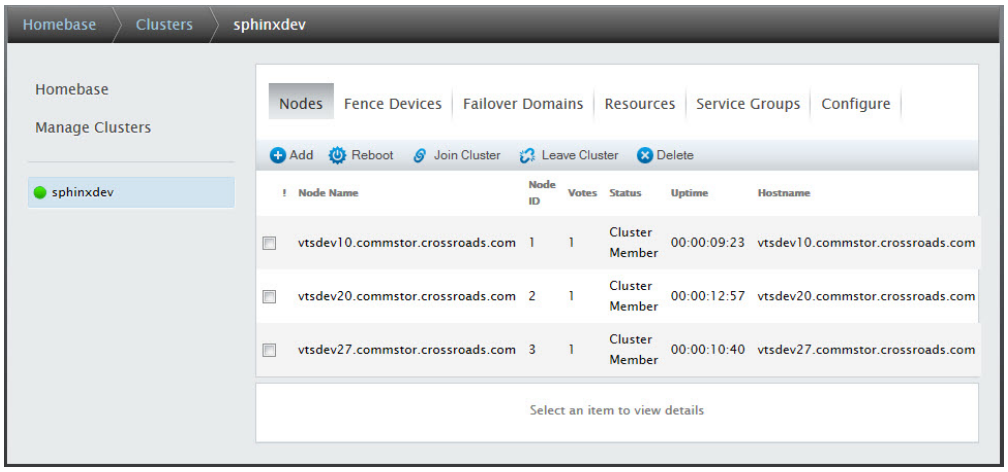
iv. In the Node Name field, enter the first node's ***fully qualified*** domain name or IP address, and enter the node's root password in the **Password** field.

v. Click **Add Another Node** and repeat the previous step for each node in the cluster.

vi. Select **Use Locally Installed Packages**.

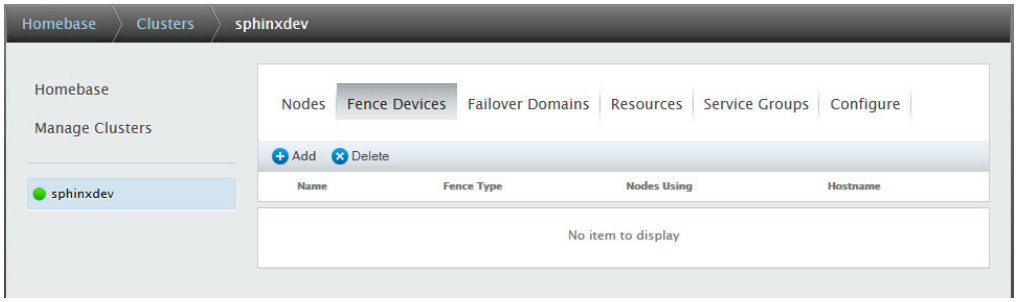
vii. Select **Enable Shared Storage Support**.

viii. Click **Create Cluster**. The nodes in the cluster are listed.

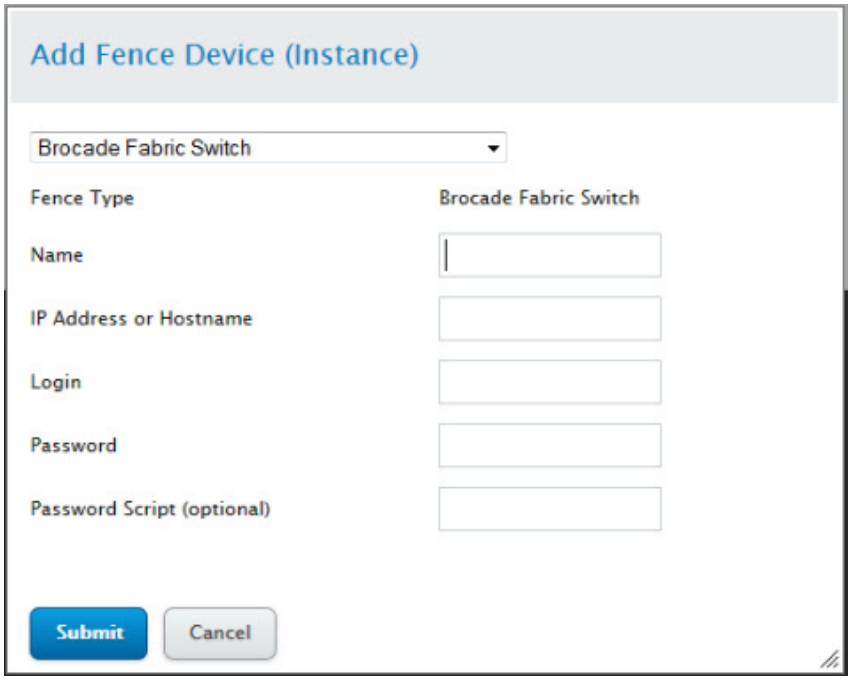


g. Configure fencing:

i. Click the **Fencing Devices** tab and then click **Add**.



ii. From the Add Fence Device (Instance) dialog, select a device from the drop-down list and click **Submit**. This dialog is displayed:



iii. Enter the name of the device in the **Name** filed.

iv. Enter the hostname or IP address of the switch. Consult your SAN administrator for this information.

v. Enter the username in the **Login** field (for accessing the switch). Consult your SAN administrator for this information.

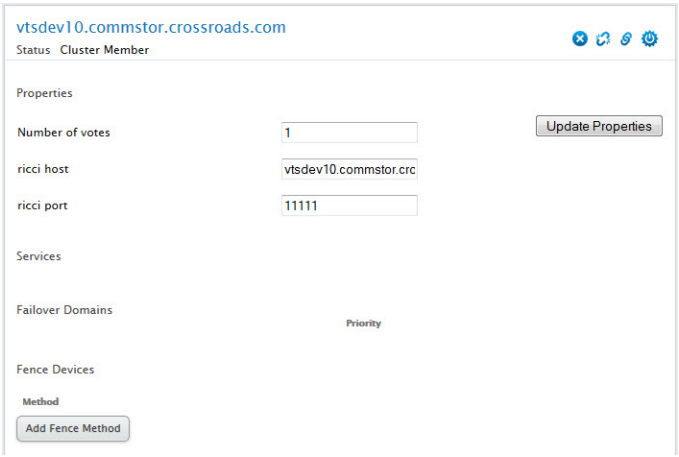
vi. Enter the corresponding password in the **Password** field. Consult your SAN administrator for this information.

vii. Click **Submit**.

viii. Click on the **Nodes** tab again.

ix. Click a node name to view its properties.

x. In the Fence Devices section, click **Add Fence Method**.



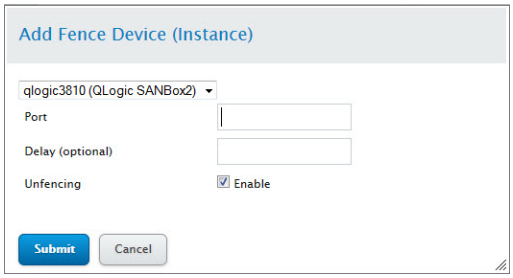
xi. Specify a name for the method when prompted.

xii. In the Fence Devices section, click **Add Fence Instance**.

Note Fencing may not work using deprecated fence devices.

xiii. Select the fencing device you created on the Fence Devices tab.

xiv. In the **Port** field, enter the port number of the port to which the node is connected (on the switch).

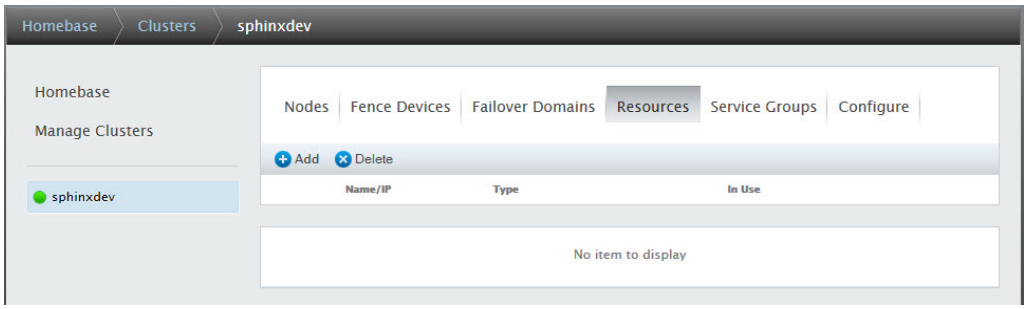


xv. Uncheck the **Enable** checkbox; you need to disable unfencing.

xvi. Click **Submit**.

xvii. Repeat steps xi - xvii for each node in the cluster.

h. Add GFS storage to the cluster:
   i. Click the **Resources** tab.



   ii. Click **Add**.

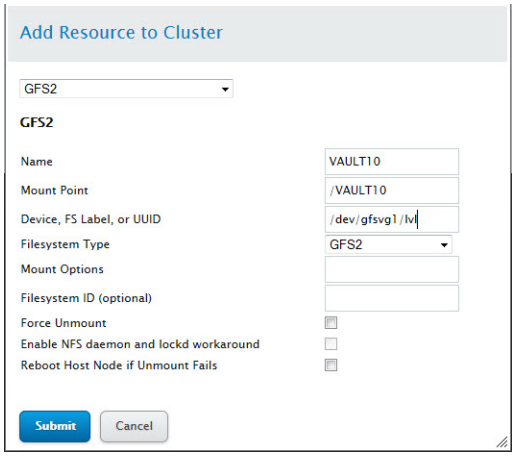
   iii. Select **GFS2**.

   iv. For the name, enter the vault name (for example, **VAULT10**).

   v. For the mount point, enter the location where you want the vault to appear (for example, **/VAULT10**).

   vi. For the device, enter the name of the device that you used when creating the GFS file system (step 5a).

   vii. Leave the options and file system ID blank.



   viii. Click **Submit**.

   ix. If you created multiple vaults, repeat these steps for each vault.

9. If GFS was previously installed, you may need to rediscover the previous GFS volume by running these commands:

```
pvscan
lvscan
vgscan
```

10. Complete the following steps on each cluster node to verify that all cluster nodes can access the GFS volumes, mount them, and access files written by other nodes. In the following steps, **VAULT10**

is used as the name of the vault.

a. Configure the **/etc/fstab** file to automatically mount the file system when SPHiNX restarts. Add a line to the file that is similar to the following:

```
/dev/gfsvg1/lv1 /VAULT10 gfs2 defaults 0 0
```

b. Enter the following commands on the console of the node:

```
mkdir /VAULT10

mount -a -t gfs2

chown bill.root /VAULT10

chmod 755 /VAULT10

ls -al /VAULT10
```

The following is an example of output for the **ls** command:

```
total 12
drwxr-xr-x 2 root root 3864 May 15 15:24 .
drwxr-xr-x 4 root root 4096 May 15 17:59 ..
```

Note If an error occurs on a node that states "invalid device path /dev/gfsvg1/lv1", you may need to reboot the node using the luci interface.

c. Enter the following command to verify that there is free space on the mounted GFS file system.

```
df -H /VAULT10
```

Here is an example of the output:

```
Filesystem      Size    Used    Avail   Use%    Mounted on
/dev/mapper/gfsvg1-lv1  17G     36K     17G     1%      /VAULT10
```

d. Enter the following command to verify that you can write to the mounted GFS file system.

```
touch /VAULT10/`hostname`
```

e. Verify that files written by other SPHiNX servers are visible by entering the following command:

```
ls -al /VAULT10
```

Here is an example of the output:

```
total 28
drwxr-xr-x 2 root root 3864 May 16 11:32 .
drwxr-xr-x 4 root root 4096 May 15 17:59 ..
-rw-r--r-- 1 root root 0 May 16 11:32   vtsdev27.domain.com
```

After completing these steps on each node, this output lists each system's hostname in the vault directory. Be sure to delete these files after completing this installation procedure.

11. Verify fencing.

Note These steps verify Brocade Fibre Channel fencing only. Use the command that matches your fence device instance.

a. Before performing these steps, make sure you are not logged into the switch through Telnet. If you are logged in, the brocade fencing script will fails with an error similar to the following:

```
/usr/sbin/fence_brocade -a ip_addr -l username -n switch_port# -p
password -o disable
pattern match read eof at ./fence_brocade line 138
# echo $?
255
```

where *ip_addr*, *username*, and *password* is that of the Ethernet switch. Consult your SAN administrator for this information.

b. To verify the fencing method, enter the following commands:

```
/usr/sbin/fence_brocade -a ip_addr -l username -n switch_port# -p
password -o disable
```

```
/usr/sbin/fence_brocade -a ip_addr -l username -n switch_port# -p
password -o enable
```

c. In a separate window, enter the following command to view for fencing messages in the system log file:

```
tail -f /var/log/messages
```

Here is an example of the messages:

```
May 15 19:10:25 SPHiNX_svr fenced[10804]: SPHiNX_svr2 not a
cluster member after 0 sec post_fail_delay
May 15 19:10:25 SPHiNX_svr fenced[10804]: fencing node "SPHiNX_
svr2"
May 15 19:10:26 SPHiNX_svr fenced[10804]: fence "SPHiNX_svr2"
success
```

To power up a GFS cluster after installation, see below.

Troubleshooting

This section describes how to verify the installation and troubleshoot any issues.

1. Verify that the appropriate services are enabled and started by entering the following commands:

   ```
   chkconfig cman on && service cman restart

   chkconfig clvmd on && service clvmd restart

   chkconfig ricci on && service ricci restart
   ```

   Note that these commands also restart fencing and deactivate the cluster.

2. Verify that logical volumes cannot be seen by attempting to mount a logical volume (**/dev/gfsvg1/gfslv1** and **VAULT10** are example values):

   ```
   mount /dev/gfsvg1/gfslv1 /VAULT10
   ```

   Here is an example of the output if the logical volume is not visible:

   ```
   mount: special device /dev/gfsvg1/gfslv1 does not exist
   ```

3. Verify that the volume is active:

   ```
   ls /VAULT10
   ```

4. Using the luci web interface, ensure that nodes are not fenced.

5. Enter the following command to activate all known volume groups in the system:

   ```
   vgchange -ay
   ```

   Here is an example of the output:

   ```
    1 logical volume(s) in volume group "gfsvg1" now active
   ```

6. Mount the vault by entering this command:

   ```
   mount /dev/gfsvg1/gfslv1 /VAULT10
   ```

7. If you have trouble mounting the GFS volume, add the following to **/etc/cluster/cluster.conf**:

   ```
   <cman broadcast="yes" expected_votes="1" two_node="1"/>
   ```

   Here is an example of the file:

   ```
   <?xml version="1.0"?>
   <cluster config_version="4" name="XYRATEX1">
     <clusternodes>
       <clusternode name="vts29.yourdomain.com" nodeid="2"/>
       <clusternode name="vts32.yourdomain.com" nodeid="3"/>
     </clusternodes>
     <rm>
       <resources>
         <clusterfs device="/dev/gfsvg1/lv1" fsid="52342" fstype="gfs2"
             mountpoint="/VAULT10" name="VAULT10"/>
   ```

```
    </resources>
  </rm>
  <cman broadcast="yes" expected_votes="1" two_node="1"/>
</cluster>
```

8. If luci will not start or restart, enter the following:

   ```
   service luci start
   ```

   or

   ```
   service luci restart
   ```

   If luci can see a node but indicates that ricci is not running, but the node shows ricci is running, output to the similar is displayed:

   ```
   luci[15356]: Unable to establish an SSL connection to
   192.168.80.2:11111: ricci's certificate is not trusted
   ```

   Enter the following commands to remove luci:

   ```
   rpm -e luci
   ```

   ```
   rm -rf /var/lib/luci
   ```

   You may need to reinstall luci or re-import the cluster. Enter the following command to install luci:

   ```
   rpm -ivh /media/cdrom/vts-6.04-gfs-install/luci*.rpm
   ```

To review the cluster status, enter the following command:

```
cman_tool status
```

Here is an example of the output:

```
Version: 6.0.1
Config Version: 5
Cluster Name: cma
Cluster Id: 711
Cluster Member: Yes
Cluster Generation: 64
Membership state: Cluster-Member
Nodes: 2
Expected votes: 1
Total votes: 2
Quorum: 1
Active subsystems: 7
Flags: 2node
Ports Bound: 0 11
Node name: 192.168.80.2
Node ID: 2
Multicast addresses: 239.192.2.201
Node addresses: 192.168.80.2
```

Reinstalling and Restoring SPHiNX

This appendix describes how to:

- reinstall the operating system and SPHiNX system
- recover the SPHiNX configuration and data, after reinstalling the server or as part of disaster recovery
- restore data stored on virtual tapes
- restore the stacked-export database from a backup server to the replacement server
- convert a target SPHiNX server (to which virtual tapes were replicated) to a source server

If you must reformat the vaults, refer to "Reconfiguring Vaults" on page 18 for instructions. If clustering (GFS) is configured in your environment, you may want to contact your authorized support representative before reinstalling or restoring settings.

Note The following procedures are intended for Linux system administrators. If you are not proficient in Linux administration and if you do not have expert knowledge of the SPHiNX hardware, you could irrevocably damage the system. You are strongly advised to contact your authorized support representative for assistance.

Reinstalling the SPHiNX server

This procedure describes how to

- back up the server, thereby creating a system restore image
- back up the key database, if Data Encryption is in use
- back up the stacked-export database, if using stacked exports to export data to physical tapes
- reinstall the operating system and SPHiNX software, thereby restoring the SPHiNX server to the factory defaults

Be aware of the following before proceeding:

- Version 9.*x* is installed on the first available disk. If you are reinstalling SPHiNX on a server that was upgraded, make sure that the first available disk does not store data that you want to preserve; the disk is erased before re-installation. Back up data and restore it to another disk after re-installation.

- VAULT00 is erased during re-installation. Customer data should not be stored on this vault; if there is data on VAULT00, you must move it or delete it. (You can use the web interface; see the "Moving a pool to a new vault" help topic.)
- If you want to preserve internal storage, contact your SPHiNX support representative for assistance.

To reinstall a SPHiNX server

Read the entire procedure before beginning!

1. Create a system restore image using the SPHiNX web interface refer to the sub-section To create a system restore image.
2. Contact your authorized support representative to obtain the installation media (DVD), which will enable you to reinstall the server.
3. If SPHiNX is connected to one or more host servers, clear any host reservations by varying off the host's device connection and then disconnect the cable(s) from the SPHiNX server.
4. Power off the SPHiNX server:
   a. Halt the system by clicking **Administration > System Tasks** on the navigation pane of the web interface and then clicking **Halt the System**. Allow the SPHiNX server to completely shut down before proceeding.

   b. Verify that the system is halted by looking at the LEDs on the front of the system and verify that there is no activity. The power LED will turn from green to yellow.
5. If necessary, disconnect any external storage devices that are connected to the SPHiNX server.
6. Power on the SPHiNX server.
7. Immediately after powering on the server, insert the installation DVD.
8. At the Linux prompt, enter **reinstall**. The installation process begins.
9. To confirm that you want to reinstall SPHiNX on the displayed device name, navigate to Yes and press ENTER.

   Note During the re-installation process, a warning may be displayed that asks you to verify that you want to reinitialize the device (erasing ALL DATA). You must select Yes to continue. You cannot cancel the re-installation at this point.
10. Recreate the mount points for any vaults and data partitions that previously existed:
    a. Create the mount directories by using the **mkdir** command for each of the vaults and data partitions. Here is an example of the command to create the mount directory for VAULT01:

       ```
       mkdir /VAULT01
       ```

       Repeat this command for each vault and data partition.

    b. Update the file-system table for the vaults and data partitions. Using a text editor, add the following lines to the **/etc/fstab** file for each vault created above:

       ```
       LABEL=/VAULT01 /VAULT01 ext4 defaults 1 2
       ```

       Repeat this command for each vault and data partition.

c. Mount the vaults and data partitions by entering the following command:

```
mount /VAULT01
```

Repeat this command for each vault and data partition.

d. Assign access rights to the vaults and data partitions by completing the following steps:
   a. Change the ownership of the vaults by entering the following command:

```
chown bill.root /VAULT*
```

   b. Change the ownership of data partitions by entering the following command:

```
chown bill.replicators /DATA*
```

   c. Change the rights of the vaults and data partitions by entering the following command:

```
chmod 750 /VAULT*
chmod 750 /DATA*
```

   d. Change the rights of the **lost+found** directories by entering the following command:

```
chmod 750 /VAULT*/lost+found
```

11. If necessary, reconnect any external storage devices to the SPHiNX server.
12. Reconnect the SAS cable(s) to the SPHiNX server, if necessary.

If you want to recover data from a backup, continue with the next procedure.

Recovering SPHiNX configuration data and settings

The steps in this section can be performed after reinstalling the SPHiNX server or as part of disaster recovery. This procedure describes how to:

- restore a system restore image, which includes
  - all configuration databases except for the key database and stacked-export database.
  - root and bill home directories.
  - some contents of the **/etc** and **/usr/local/tape/etc** directories.
  - virtual tapes, if they were backed up and the original vault is present. Only the tape names are restored; data on the tapes was not backed up. If the original vault is not present, virtual tapes are not restored.
  - policies, if the pool exists after the system is restored. Policy attributes are reset to those that were configured when the restore image was created, and deleted policies are restored if they were deleted after the restore image was created. Policies created after the system restore image will exist on the system but attributes are lost and the policies are disabled.
- restore the key database, if Data Encryption was in use
- restore the stacked-export database (also referred to as the "TSM database"), if stacked export jobs were in use
- restore replication tapes from a remote (target) server, if Replication was in use

To recover the SPHiNX server

1. If you have not done so, back up the SPHiNX server as described in "Backing up the SPHiNX server" on page 149. This includes creating a system restore image, backing up the key database (if Data Encryption is in use), and backing up the stacked-export database (if stacked exports are in use).

   Note If you are recovering data settings after reinstalling the server, you performed this step in the previous procedure and can skip to the next step.

2. If path failover was configured in the SPHiNX environment, log in to the SPHiNX operating system, change to the root user (using the **su** command), and enter the following commands:

   ```
   chkconfig multipathd on

   multipathd -v0
   ```

3. If necessary, upload and install the VPD file on the server:
   a. If necessary, contact your authorized service and support representative to obtain the VPD file.

   b. Using the web interface, click **Configuration > System > Upload Vital Product Data (VPD) File**.

   c. Locate the file by clicking **Choose File**.

   d. Click **UPLOAD**.

4. Enable license keys:

   a. Click **Configuration > System** on the navigation pane.

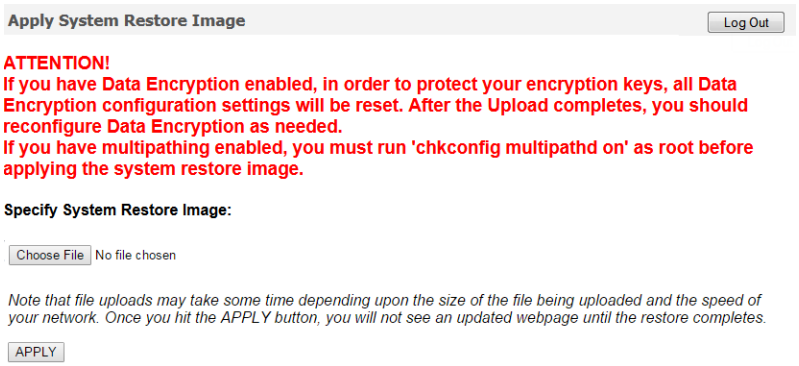
   b. Click **Manage System Licenses**.

   c. For each license key you need to enable, type or paste the license key in the corresponding field and then click **SUBMIT**. On the pop-up dialog, click **OK** to confirm that you want to add the key.

   d. Restart the TapeServer service. Click **Administration > System Tasks** on the navigation pane. Then, click **Stop TapeServer** and then click **Start TapeServer**.

5. Restore the system restore image:
   a. Using the SPHiNX web interface, click **Support > System Updates** on the navigation pane.

   b. Click **Restore a System Restore Image**. The Apply System Restore Image page is displayed.



c. Click **Choose File** to browse to and select the system restore image.
d. Check the file size of the system restore image. If the system restore image is larger than 1GB, this step may fail. Contact Support for assistance if necessary.
e. Select the **Set hostname and machine ID from image (override current settings)?** option to set the hostname and machine ID according to those specified in the restore image. This overrides the current system settings.
f. Click **APPLY**.

(Do not reboot SPHiNX yet.)

6. Modify the user privileges on the SPHiNX system:
   - If the system is in an OPEN state, navigate to the Manage Access Control page of the SPHiNX web interface and click **Restore OPEN Defaults**.
   - If the system is in a CLOSED state, navigate to the Manage Access Control page and click **Rights** to display the list of privileges. Select the **System Upgrade/Update Functions** access right for each of the appropriate users.
7. If Data Encryption is licensed, restore the key database from a remote host:
   a. Re-enable Data Encryption by removing the current license key and reinstalling the Data Encryption license key. Contact your authorized service and support representative to obtain a license key, if necessary. Use the **Configuration > System > Manage System Licenses** page of the web interface to remove and install license keys.
   b. Remove all key-servers (both localhost and remote key-servers). Remove all backup key-servers on local server (new key-server).
   c. Go to **Configuration** > **System** > **Manage System Licenses** to copy and remove the Data Encryption License(s).
   d. Go back to re-apply the Data Encryption License: **Configuration** > **System** > **Manage System Licenses**.

      Note This will create a new key server as localhost.

   e. Go to **Configuration** > **Data Encryption** to delete the localhost key-server .

      Note When a new license is applied, the old localhost key-server has to be deleted.

   f. On the same page, click on **Restore from Disaster Recovery Site**. Enter all information required and the source path where you recovering from.

      Note The permission of the backup keys you are importing should have ownership: bill.bill, permission:644.

   g. Add a key-server as localhost, port number 9090, key generator box checked, with username and password.
   h. Add the backup server to complete the configuration.

      Note Not the same path as the orginal recovery path as in step f.

   i. Verify if the size of the tapes has changed from 0 Bytes to the actual sizes. If the size hasn't changed, call support.
8. If using stacked export jobs to migrate data to physical tape, restore the stacked-export database (TSM) to enable the SPHiNX server to resume stacked exports:
   a. Launch a command line utility and log in as **bill** and then use the **su** command to change to the **root** user.

b. If connected to an IBM library, start the driver that is installed on the SPHiNX server by entering these commands:

```
chkconfig lin_tape on
service lin_tape start
```

c. Configure TSM:

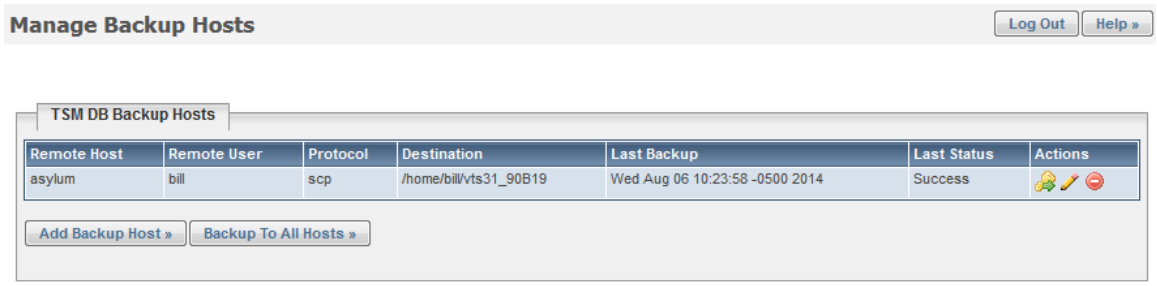
```
bmaconfig -c tsm
```

Here is an example of the output (for a library):

```
doing initial TSM configuration ...
dsmserv lic file built ...
TSM licenses installed ...
dsmserv.opt setup ...
dsmserv config file built ...
dsmserv configured ...
enable tivoli logging: trueTivoli TSM logging enabled ...
Status of dsmserv: stopped
Status of dsmserv: running
TSM service started ...
file dsm.sys setup ...
file dsm.opt setup ...
file vts.conf setup ...
TSM activity log management setup ...
```

d. Using the web interface, click **Configuration > System** on the navigation pane.

e. Click **Manage Backup Hosts** in the list.



f. On the Manage Backup Hosts page, click next to the backup host.

g. From the command line, rename the directory where the backup file resides. Log in to the SPHiNX operating system, change to the root user (using the **su** command), and enter the following commands:

```
mv /usr/local/tape/var/restore /usr/local/tape/var/bmadb
chown bill.bill /usr/local/tape/var/bmadb
chmod 755 /usr/local/tape/var/bmadb
```

h. Restore the TSM database:

```
bmaconfig -b tsm -r /usr/local/tape/var/bmadb
```

i. Log in to the TSM administrative client and update the TSM password by entering this command:

```
/opt/tivoli/tsm/client/ba/bin/dsmc q sched
```

When prompted, enter **admin** as the username and **v-*serial#_in_reverse*** as the password (such as v-75001A if the serial number is A10057).

To exit the administrative client, enter **quit**.

9. If Replication will be used, you must reconfigure Replication on the server. Then, you can restore virtual tapes that were replicated to remote SPHiNX servers (by replicate jobs):

   a. Delete any remote target servers that were previously configured:

      a. Click **Configuration > System** on the navigation pane.

      b. Click **Edit System Settings**.

      c. Click **Replication Settings** to expand this area of the page.

      d. Click  next to the server you want to delete.

      e. When prompted, click **Yes**.

   b. Add target servers, which exchanges SSH keys between the servers:

      ### To add a target server

       *Requires Administration group membership*

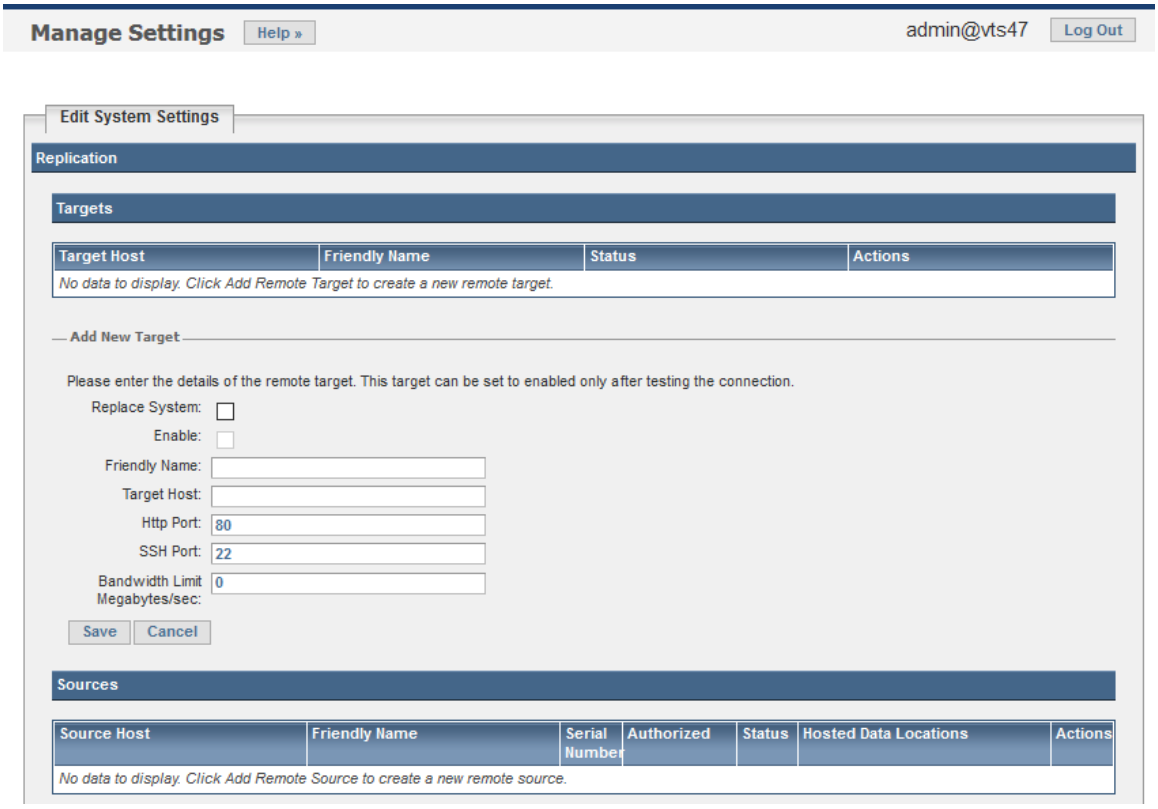
      Complete these steps using the source server's web interface:

      a. Click **Configuration > System** on the navigation pane.

      b. Click **Edit System Settings**.

      c. Click **Replication** to expand this area of the page.

      d. Click the **Add Target Host** button. The following is displayed:



e. If the local (source) server was replaced, you need to notify the target server so that it can update its source server information:
   a. Select the **Replace System** checkbox.
   b. In the **Previous Serial Number** field, type the serial number of the old source server.

f. In the **Friendly Name** field, type a name for the target server.

g. In the **Target Host** field, type the fully qualified hostname or IP address of the target server.

   Note It is recommended that you provide a hostname, if DNS is configured on your network. If you provide an IP address instead of a hostname and then the IP address of the source or target server changes, you must delete the target server and then complete all configuration procedures again.

h. In the **Http Port** field, type the port number used for accessing the web interface on the target system. Typically, this port is set to 80 but it may be set to another number if, for example, the server is behind a firewall. Contact your firewall or system administrator for this port number.

i. In the **Ssh Port** field, type the port number used to access SSH on the target server. Again, if the server uses a non-standard port, contact your firewall or system administrator.

j. In the **Bandwidth Limit** field, type the number of Megabytes per second (**Megabytes/sec**) that the source server can use to send data. If you specify 0, no limit is set.

k. Click **Save**.

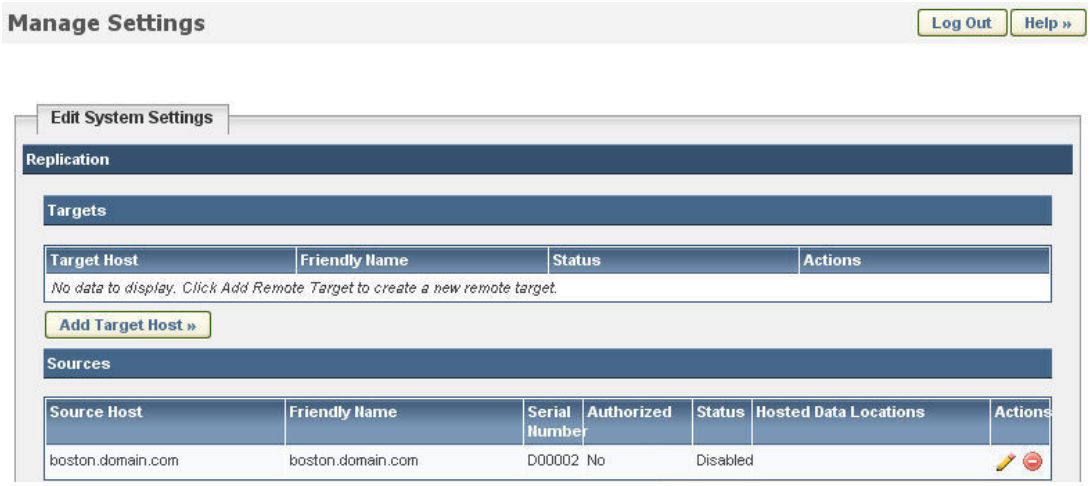
To authorize and enable a source server

Complete these steps using the target server's web interface:

a. Click **Configuration > System** on the navigation pane.

b. Click **Edit System Settings**.

c. Click **Replication Settings** to expand this area of the page. The following is displayed:



d. Click ✎ next to the source server you want to authorize and enable.

e. Select the **Authorized** checkbox to verify that the source credentials are valid and expected.

f. Select the **Enabled** checkbox to enable the source server, thereby allowing it to use the local (target) system as a replication target. (You cannot select this checkbox if the Authorized checkbox is not selected.)

g. In the **Friendly Name** field, type a name for the source server.

h. Using the **Map To** lists, map mount points (data volumes) on the local (target) server to the source server. This determines where replicated tapes are stored on the local server when sent from this source server. Use the ➡ and ⬅ buttons to move mount points to and from the lists.

i. From the **Allowed Streams** drop-down list, set the number of data streams that the source may use when transferring data to this target.

j. If you need to confirm the SSH server key that is seen by the source when this target connects, review the **Fingerprint** value. You can copy and paste the fingerprint and send it to the administrator on the source system, if necessary. This fingerprint is used in the Test Target Connection section of the Edit System Settings page when the

source connects to the target.

k. Click **Save**.

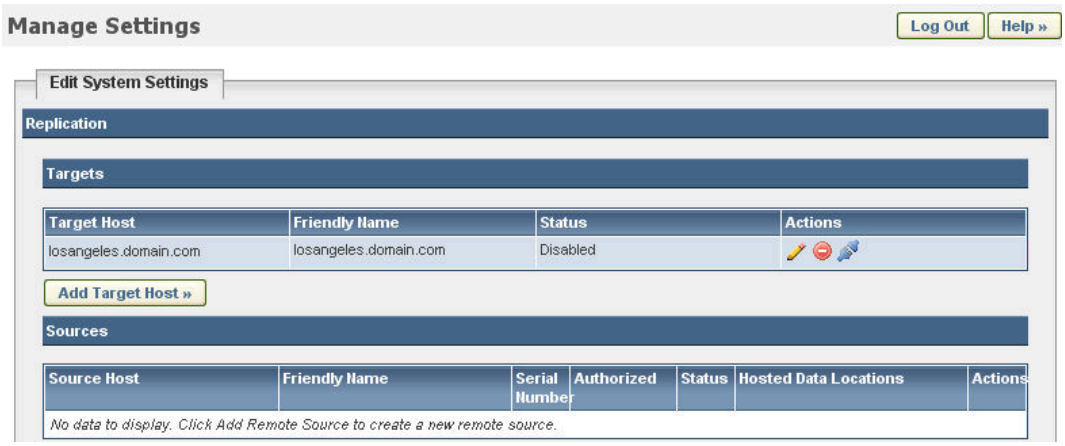
To complete the connection and enable the target server

After the target authorizes and enables this source, complete these steps using the source server's web interface:

a. Click **Configuration > System** on the navigation pane.

b. Click **Edit System Settings**.

c. Click **Replication Settings** to expand this area of the page. The following is displayed:



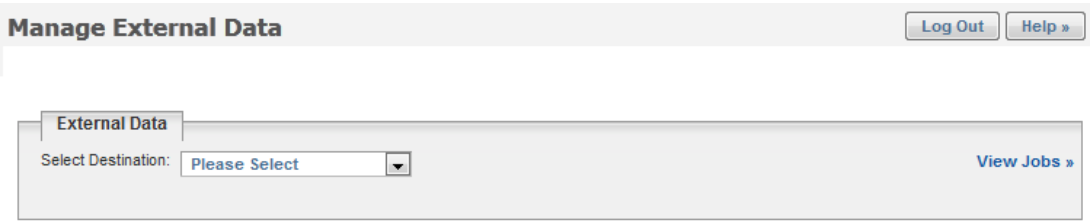
d. Test the connection to the target server. Click  in the Actions column next to the target server.

e. In the Test Target Connection section of the page, select **Yes** to continue the connection and then click **Submit**.

f. Enable the target server by clicking next to the target server and then selecting the **Enable** checkbox. Then, click **Save**. The server will then be available for selection during replicate job creation.

c. Restore virtual tapes that were replicated to remote SPHiNX servers (by replicate jobs):

a. Click **Administration > External Data** on the navigation pane.



b. Select a remote host from the Replication Destinations section of the **Select Destination** drop-down list. A list of replicated tapes that reside on the remote host are listed.

c. Select one or more virtual tapes to restore and then select **Import** from the Please Select drop-down list above the table on the right.

Note If the virtual tape has moved from its original location on the source (local) server,  is displayed next to the physical tape and the new location is displayed in the **Source Vault/Pool** column. If you import a physical tape whose virtual tape has moved, the contents of the virtual tape in the new location are overwritten. You can also choose not to import the tape, move the source virtual tape to its original location, and then attempt to import the physical tape again.

d. To name the restore job, enter a name in the **Job Name** field. Include only alphanumeric characters in a job name; spaces and special characters are not allowed.

e. If you wish to stop the restore operation if an error occurs, select **Stop on Error** (above the table). If an error occurs, the restore job fails. If you do not select this option, the restore operation will skip tapes that caused an error and finish importing the selected tapes.

f. Select **Trigger Policy If Enabled** if you want to initiate actions defined in policies associated with the selected virtual tapes. Policies apply to pools, so this option triggers policies that are defined for pools in which the selected virtual tapes reside.

g. If the virtual tape is no longer on the source (local) server, select a location where the imported tape will be created. You can select a vault and pool from the drop-down list that is displayed in the **Source Vault/Pool** column.

h. Click **submit**. A import job is created and run immediately.

10. If the system image was restored on a system that is different than the one used to create the image, you must manually delete the old MACHINEID file in **/boot**. Log in to the SPHiNX operating system, change to the root user (using the **su** command), and delete the file.

11. Reboot SPHiNX by clicking **Administration > System Tasks > Reboot the System**.

Recovering customer data on virtual tapes from SAN

If you reinstall the SPHiNX server and restore a system image, data stored on virtual tapes is not restored. If the data is intact on the storage area network (SAN), you can perform the following steps to reinstate data.

Note If you have already reinstalled the SPHiNX server and restored the system image, you can begin this procedure at step 4.

1. Disconnect the SPHiNX server from the SAN.

2. Reinstall SPHiNX as described in "Reinstalling the SPHiNX server" on page 188.

3. Restore the SPHiNX system image, which restores configuration settings, as described in "Recovering SPHiNX configuration data and settings" on page 190.

4. On the SPHiNX server, edit the **fstab** file to include the SAN vaults. Here is an example entry for a vault:

```
LABEL=/VAULT04   /VAULT04        ext3    defaults         1 2
```

5. Reconnect SPHiNX to the SAN.
6. Reboot SPHiNX by clicking **Administration > System Tasks > Reboot the System**.

Restoring the stacked-export database on a replacement server

If the SPHiNX server was configured to back up the stacked-export database to a backup host, you can restore the database and then import tapes that were exported. The following procedure restores the stacked-export database from the backup server (Host1) to the replacement server (Host2).

Note To restore the stacked-export database after reinstallation, see "Recovering SPHiNX configuration data and settings" on page 190.

Before beginning

- Note the serial number of your SPHiNX appliance, which is provided on a label on the back of the server.

To restore the stacked-export database

1. From the command line of the replacement or reinstalled server (Host2), log in as root. Or, you can log in as bill and then enter the **su** command to become root.
2. Create the **/usr/local/tape/var/bmadb** directory. This is where the database backup from the backup server (Host1) will reside before it is restored.
3. Copy the backup file from Host1 to Host2. This file resides in the path specified in the Destination field for the backup server. If no path was specified, the file resides in user's home directory.
4. On Host2, extract the contents of the backup file, which is archived and compressed (using gzip), using the **tar -xzf** command. Extract the contents to the **/usr/local/tape/var/bmadb** directory.

   The contents of the **.tar.gz** file include files similar to these:

   - 96582894.dbb
   - datetime.txt
   - devcnfg.out
   - dsmserv.opt
   - log.dsm
   - volhistory.out
5. Change the ownership of the extracted files by entering these commands:

   ```
   chown bill.bill /usr/local/tape/var/bmadb/*
   chown bill.bill /usr/local/tape/var/bmadb
   ```
6. Physically remove the tape cartridge from the library connected to Host1 and insert it into the new library connected to Host2.

7. From Host2, complete these steps:
    a. Configure TSM to use the new library by running these commands:

    ```
    bmaconfig -c tsm
    bmaconfig -b tsm -n library_name -l changer
    ```

    Refer to the "Enabling and Performing Stacked Exports" on page 51 for detailed information about these commands.

    b. Create the **/tmp/scratch** directory, which will store a database backup of Host2. The purpose of this backup is to add information to the **devcnfg.out** file, which is needed to restore the stacked-export database from Host1.

    ```
    bmaconfig -b tsm -k /tmp/scratch
    ```

    c. Restore the backup from Host1 to Host2; specify the directory to which the backed up files were copied from Host1:

    ```
    bmaconfig -b tsm -r /usr/local/tape/var/bmadb
    ```

    d. Log in to the TSM administrative client by running the **dsmadmc** command:

    ```
    /opt/tivoli/tsm/client/ba/bin/dsmadmc
    ```

    When prompted, enter **admin** as the username and **v-*serial#_in_reverse*** as the password (if the serial number is A10057, enter **v-75001A**). The serial number of your SPHiNX appliance is provided on a label on the back of the server.

    e. Query the library paths:

    ```
    q path
    ```

    f. Delete the paths for the drives and libraries; repeat these commands for each path listed by the query command. Because you are performing these steps on a replacement server, the TSM server name is now incorrect. Thus, these commands rename the configured library and drives.

    If the destination type is a drive, use this command:

    ```
    delete path source_name destination_name srctype=source_type
    desttype=drive library=library_name
    ```

    If the destination type is a library, use this command:

    ```
    delete path source_name destination_name srctype=source_type
    desttype=library
    ```

    g. Query the drives:

    ```
    q drive
    ```

    h. Delete all drives; repeat this command for each drive listed in the query:

    ```
    delete drive library_name drive_name
    ```

    i. Query the libraries:

    ```
    q library
    ```

j. Delete all libraries; repeat this command for each library listed in the query:

```
delete library library_name
```

k. Rename the node:

```
rename node Host1 Host2
```

l. Quit **dsmadmc** by entering **quit**.

m. Configure TSM and configure TSM to use the new library:

```
bmaconfig -c tsm
bmaconfig -b tsm -n library_name -l changer -d drive_name,drive_
name,...
```

Again, refer to the "Enabling and Performing Stacked Exports" on page 51 for detailed information about these commands.

Note that command failed error is displayed, which can be ignored:
`/opt/tivoli/tsm/server/bin/dsmserv runfile /tmp/dsmservcfg.txt.`

n. Run the short archive test:

```
bmaconfig -t library_name
```

When prompted, enter admin as the username and **v-*serial#_in_reverse*** as the password.

o. Within 60 minutes of supplying credentials for the archive test, check in the tape:

```
bmamanage insert -n library_name -t tape_barcode -p -r
```

The tape is checked in and the archive test should succeed.

p. Log in to the web interface.

q. Click **Administration > Virtual Tapes**, click the **Advanced Media Actions** link, and then select the desired virtual tape on the Virtual Media - Operation page and click the **UnMigrate** button. Refer to the Importing section of "Creating and Managing Virtual Media" on page 93 for more information.

r. In the HSM Put log (**hsmput.log** file), verify that the files were retrieved and have been unmigrated to the virtual tape. To access logs from the web interface, click **Support > Logs** on the navigation pane and then click a link in the Log Files section of the page.

Converting a target replication server to a source server

You can access replicated virtual tapes on a target replication server as part of disaster recovery, if the source SPHiNX server becomes unavailable. This procedure converts a target SPHiNX server (to which the virtual tapes were replicated) to a source server. (If you need to restore replicated virtual tapes from a target server, you can import the tapes as described in "Recovering SPHiNX configuration data and settings" on page 190.)

After connecting a host server to the target SPHiNX server as described in the *Quick Start Guide*, complete these steps, which are performed from the command line.

Note Virtual tape names must be unique across all pools on the SPHiNX server and all SPHiNX servers in the environment. If you are restoring tapes from multiple servers, it is recommended that you restore tapes from one host at a time to avoid duplicate names.

To restore virtual tapes

1. From the command line of the SPHiNX server, log in as the root user.
2. Use the **mount** command to list the devices mounted on the **/DATAxx** partition, where DATA*xx* is the data partition designated for storing exported tapes:

   ```
   mount
   ```

   Here is an example of this command's output. In this example, /dev/sdb1 is mounted on DATA01.

   ```
   /dev/sda2 on / type ext3 (rw)
   proc on /proc type proc (rw)
   sysfs on /sys type sysfs (rw)
   devpts on /dev/pts type devpts  (rw,gid=5,mode=620)
   /dev/sda1 on /boot type ext3 (rw)
   /dev/sda4 on /VAULT00 type ext3 (rw)
   tmpfs on /dev/shm type tmpfs (rw)
   none on /proc/sys/fs/binfmt_misc type binfmt_misc  (rw)
   sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs  (rw)
   192.168.60.40:/TEST/TEST on /TEST type nfs
   (rw,soft,addr=192.168.60.40)
   /dev/sdb1 on /DATA01 type  ext3 (rw)
   ```

3. Unmount the data partition. For this example, unmount DATA01:

   ```
   umount /DATA01
   ```

4. Update the file-system table to comment out the data partition. Using a text editor, insert a pound sign (#) in front of the following line of the /etc/fstab file:

   ```
   # LABEL=/DATA01 /DATA01 ext3    defaults         1 2
   ```

5. Mount the device on a /VAULT and set permissions. For this example, /dev/sdb1 is mounted on /VAULT01:

   ```
   mount /dev/sdb1 /VAULT01
   chown bill.root /VAULT01
   chmod 750 /VAULT01
   ```

6. Verify the new configuration by entering the following command:

   ```
   df -H
   ```

Now, you can create VTDs or VTLs and use the host server to restore the data. Because the data is now in a vault location, it can change and be manipulated by the host server. After the data is restored, you can unmount the device from the vault (/dev/sdb1 in this scenario) and remount it back to /DATA01. Replication will continue as normal.

Attaching External Devices after Initial Deployment

You can attach an external tape device, such as a tape drive or robotic library, to SPHiNX after initial deployment. You can then export to physical tapes loaded in the device if stacked export or tape-to-tape export is enabled. Or, if you must replace the external tape device that was initially attached and configured for use in stacked exports, you can reconfigure SPHiNX after initial deployment.

To use an external disk drive for vault and pool storage, see "Adding vaults on external storage devices" on page 26.

Attaching an external tape device

To add an external tape device to the SPHiNX server


Requires the View/Manage Configuration and Halt and Reboot TapeServer access rights

1. If a virtual tape drive (VTD) is already defined on the port, complete the following steps to remove the drive:
   a. Delete the VTD that uses the target port. Click **Configuration > Virtual Devices** on the navigation pane. If necessary, log in. Then, click  next to the VTD you want to remove. A dialog box is displayed indicating that VTD operations will be interrupted if you modify the VTD. Click **OK** to confirm the deletion.

   b. Change the system limits for the target port.

   c. In the MANAGE PORT CONFIGURATION section of the Configure Virtual Devices page, select **physical** from the drop-down list that corresponds to the target port and then click **Submit**. Confirm that you want to reboot the server.

2. For SCSI ports only
   Power down the SPHiNX server and then cable the physical tape device (through the SCSI converter as necessary) to the SPHiNX server. Then, power on the physical tape device, SCSI converter, and SPHiNX server. Refer to the *SPHiNX Quick Start Guide* for hardware diagrams and information.

3. To confirm that the physical tape device was created and is communicating with the operating system, go to the Linux text console and enter the following command:

   ```
   sg_map -x
   ```

   Here is an example of the output from this command:

   ```
   /dev/sg0  0 0 3 0  1  /dev/nst0
   /dev/sg1  6 0 0 0  5  /dev/scd0
   /dev/sg2  6 0 0 1  5  /dev/scd1
   ```

```
/dev/sg3  6 0 0 2  5  /dev/scd2
/dev/sg4  6 0 0 3  5  /dev/scd3
/dev/sg5  6 0 0 4  5  /dev/scd4
/dev/sg6  6 0 0 5  5  /dev/scd5
/dev/sg7  6 0 0 6  5  /dev/scd6
```

Then, find the nst0 entry (tape drive) attached and then enter this command:

```
sg_inq /dev/sgn
```

where *sgn* is the number that matches the **/dev/nst*n*** device. For the output listed above, you would enter **sg_inq /dev/sg0**. Here is an example of the output from this command:

```
standard INQUIRY:
PQual=0  Device_type=1  RMB=1  [ANSI_version=4]  version=0x04
[AERC=0]  [TrmTsk=0]  NormACA=0  HiSUP=0  Resp_data_format=2
SCCS=0  ACC=0  ALUA=0  3PC=0  Protect=0
BQue=0  EncServ=0  MultiP=0  MChngr=0  [ACKREQQ=0]  Addr16=1
[RelAdr=0]  WBus16=1  Sync=1  Linked=0  [TranDis=0]  CmdQue=0
Clocking=0x3  QAS=0  IUS=0
length=74 (0x4a)   Peripheral device type: tape
Vendor identification: CERTANCE
Product identification: ULTRIUM 3
Product revision level: 1770
Product serial number: JD006D2
```

Repeat for each tape drive that was added.

Reconfiguring TSM to use a new library

After connecting the library to SPHiNX as described in the *Quick Start Guide*, complete these steps to assign the library to TSM.

Note Perform these steps *before* removing the configured library from the SAN.

To reconfigure TSM using the web interface

1. Configure TSM to use the newly attached library:
    a. Click **Administration > TSM Library** on the navigation pane. All libraries that are attached to SPHiNX are listed on the Manage TSM Library page.

    b. If a library's friendly name is not valid because it contains a space or is blank, it is highlighted red. You must edit the name in the **Friendly Name** field (but do not press Enter).

    c. Select the library to use for stacked exports by clicking on its radio button in the **Configured in TSM for Stacked Exports** column.

    d. Click **Apply**.

2. Check in tapes for use by stacked export jobs:
    a. Insert one or more tapes into the library, if necessary. To do this, add the physical tape to the I/O slot in the physical library and then move the tape from the I/O slot into a regular slot using the library's control panel.

    b. Check one or more tapes in by expanding the **Administer TSM Library** section of the page and then doing this:
        - If a tape was inserted that had been used previously for a stacked export, click **Return cartridge** (in the Action column) for each tape you want to use
        - If adding a scratch tape, click **Add cartridge** next to the tape
        - To add all scratch tapes listed on the page, click the **Check-in Non-TSM tapes as scratch** button below the table of tapes. (This may take a while to complete.)

To reconfigure TSM using the command line

1. Log in to the SPHiNX server.
2. Become root:

    ```
    su -
    ```

3. If connected to an IBM library, start the driver that is installed on the SPHiNX server by entering this command:

    ```
    chkconfig lin_tape on
    service lin_tape start
    ```

4. Configure TSM:

    ```
    bmaconfig -c tsm
    ```

    Here is an example of the output (for a library):

    ```
    doing initial TSM configuration ...
    dsmserv lic file built ...
    ```

```
TSM licenses installed ...
dsmserv.opt setup ...
dsmserv config file built ...
dsmserv configured ...
enable tivoli logging: trueTivoli TSM logging enabled ...
Status of dsmserv: stopped
Status of dsmserv: running
TSM service started ...
file dsm.sys setup ...
file dsm.opt setup ...
file vts.conf setup ...
TSM activity log management setup ...
```

5. Remove the library and associated drives from the TSM configuration by entering this command:

   ```
   bmaconfig -b tsm -n libname -x /dev/changerpath
   ```

   Here is are examples of this command:

   ```
   bmaconfig -b tsm -n lib35 -x /dev/sg0
   ```

   ```
   bmaconfig -b tsm -n lib35 -x /dev/IBMchanger0
   ```

6. Reconfigure the SAN.
7. Configure the new library as described in "Configuring IBM Tivoli Storage Manager on SPHiNX" on page 52.

TCP/IP Ports and Protocols

This appendix describes the ports and protocols that are used by SPHiNX.

Note Not all ports are used on all SPHiNX servers; port use varies according to the SPHiNX configuration. All ports other than those listed here are disabled and inactive on the server.

Port	Protocol	Comment
	ICMP Type 8	Used by ping and tracert on Windows, for remote testing and SPHiNX networking.
21	TCP, UDP, FTP	This port and other ephemeral ports are used if the client is configured for passive (PASV) mode.
22	TCP, SSH	Used by SCP, which is used by Data Replication and Data Encryption if these services are configured.
23	TCP, TELNET	Used for Telnet remote access.
80	TCP, HTTP	Used by the SPHiNX web interface (HTTP).
111	TCP, UDP	Used by SPHiNX when using NFS services.
123	TCP, UDP	Used to synchronize the SPHiNX clock (NTP).
443	TCP	Used by the SPHiNX web interface (HTTPS) and Data Replication.
449	TCP	Used by TapeMountServer (TMS).
514	TCP	Used for remote command execution (RSH).
873	TCP, UDP	Used by rsync, which enables Data Replication to transfer files, if these services are configured.
2049	TCP, UDP	Used for NFS file sharing.
4567	TCP	Used by Data Replication.
5404, 5405	UDP	Used by cman service if GFS is installed in your environment.

Port	Protocol	Comment
5432	TCP, UDP	Used by the internal (Postgres) database
7295	TCP	Used by TMS.
7297	TCP	
8080	TCP	Used by the Eruces encryption provider (te-server) for Data Encryption.
8888	TCP	
9090	TCP	
9999	TCP	
11111	TCP	Used by ricci service if GFS is installed in your environment.
14567	TCP	Used by gndb service if GFS is installed in your environment.
16851	TCP	Used by modclusterd service if GFS is installed in your environment.
21064	TCP	Used by dim service if GFS is installed in your environment.
33434-33534	UDP	Used by traceroute, which is a diagnostic utility delivered with SPHiNX but not essential to its functioning
50006, 50008, 50009	TCP	Used by ccsd service if GFS is installed in your environment.
50007	UDP	

NFS lockd (the lock manager) is also required for NFS and can have its ports set manually in /etc/sysconfig/nfs by adding the following:

- For quotas:

  `RQUOTAD_PORT=`*`port_number`*

- For the lock daemon:

  `LOCKD_TCPPORT=`*`port_number`*

  `LOCKD_UDPPORT=`*`port_number`*

- For the mount daemon:

  `MOUNTD_PORT=`*`port_number`*

- For the stat daemon:

  `STATD_PORT=`*`port_number`*

Index