Release Notes

SPHiNX™

Release: Version 9.6
January 2019

This document applies to version Version 9.6 of SPHiNX™, and this release includes changes made to SPHiNX since the 9.5-33 release. Before beginning, be aware of the following:

- Registration — You must register with ETI\SPHiNX to download software, obtain license keys, view product documentation, and access the SPHiNX knowledge base. To register, log in to registration site at https://register.etinet.com/ and follow the instructions on the site.
- Product documentation — Use your support credentials to download SPHiNX Software and Documentation from https://sftp.etinet.com under the SPHiNX folder. If you don't have access to your credentials, contact support-sphinx@etinet.com :
- Support — If necessary, you can contact your authorized Technical Support organization for additional information or assistance. Be sure to refer to the tracking number when inquiring about an issue. You can also refer to the following web page for Support information: https://etinet.atlassian.net/servicedesk/customer/portal.

Here are the sections included in these release notes:

New features, changes, security vulnerability fixes, and decommissioned features

The 9.6 release includes changes made to SPHiNX since the 9.5 release. For information about features and enhancements included in all past releases, refer to the *Release Notes* for each version, which are available on the registration site.

The issue tracking number is provided (between brackets) - if available - to identify the related support case; each tracking number is a unique identifier, not a counter.

New features and changes

- **Manage Virtual Tapes** page has been improved and changed as follows:

1. the multi-action drop-down list has been moved to the left side of the panel
2. the layout of the **Manage Virtual Tapes** page has been modified to show icons for single action operations (mount and unmount action icons) next to each cartridge listed in the table
3. the display of the **Filter By Location** options has been changed to show under **Libraries** all the library names to choose from
4. the field "Show Cartridges In" has been changed to "Filter by Location" with multiple-choice options in a drop-down list
5. the mount/unmount button color theme has been changed to indicate the state of the operation
6. the mount dialog displays only the standalone VTDs, if cartridges are filtered by Shelf. If cartridges are filtered by library, the mount dialog displays the libraries.

- The **Dump Tables** page has been decommissioned. These tables will not be displayed anymore on the User Interface.
- New action button available to re-certify an expired certificate.
- New feature allowing to mount/ unmount a virtual cartridge in the tape drive of a library. This new feature is available only on the **Manage Virtual Tapes** page, not on the **Advanced Media Actions** page.
- If no VTL configured on SPHiNX, the **Manage Virtual Tapes** page, in the **Actions** drop-down list (under **View Drives**), will not display the **Library Operations** option.
- Non-required kernels get cleaned up when upgrading to a new kernel.
- Improved the Clear Cache feature to create and update data faster and to support NFS vaults.
- The minimum quota value for ZFS DATAxx and VAULTxx is 1000Mb/1Gb.
- RAIDZ-1 and RAIDZ-2 setup for ZFS storage at manufacturing has been modified based on the

number of disks.

- New feature that allows bulk deletion on the **Manage Jobs** page.

Resolved defects

- Fixed an error message typo ("Error updating schedule").
- The quota field on the **ZFS Vaults** page has been modified to accept only numeric values.
- The quota field on the **ZFS Vaults** page generates an error message when the quota value is lower than "1G".
- Fixed a bug that prevented the correct ZFS quota value to be displayed in the **System Status** page.
- Resolved an issue related to the **Delete** dialog box on the **Manage External Data** page.
- Improved the behavior of the **Disk Storage** page to handle the error message 'No zpool found" when adding a disk and no zpool is being found to add the disk to.
- Resolved a defect of Data Encryption key that couldn't be found when the certificate was expired [SPHXSUPP-1228].
- Fixed a bug that prevented the **Cached At** info to be displayed on the **Virtual Tape** page.
- Improved log files cleanup feature.
- The `hsmdelete.pl` script doesn't work as designed [SPHXSUPP-1741].
- Fixed a compression error running on autoload pools.
- Resolved a defect that prevented a backup to finish/abend because of a full virtual cartrige filemark table.
- Resolved an issue that increased the number of parameters "vtsisc_delay=" in vts.conf each time the EMS configuration is saved.
- Change the Linux clock source to HPET to prevent appliance to be feezing.

Security vulnerability fixes

All the following support cases have been fixed with the vulnerability fixes listed below:

- CESA-2018:0469 Important CentOS 6 dhcp Security Update

  https://access.redhat.com/errata/RHSA-2018:0469

  CVE-2018-5732, CVE-2018-5733

- CEBA-2018:0513 CentOS 6 gcc BugFix Update

  https://access.redhat.com/errata/RHBA-2018:0513

  Reduce overhead of mitigating Spectre Variant 2 attacks described in CVE-2017-5715.

  No CVE.

- CEBA-2018:0514 CentOS 6 irqbalance BugFix Update

  https://access.redhat.com/errata/RHBA-2018:0514

  No CVE.

- CEBA-2018:0510 CentOS 6 sssd BugFix Update

  https://access.redhat.com/errata/RHBA-2018:0510

  No CVE.

- CEBA-2018:0511 CentOS 6 ksh BugFix Update

  https://access.redhat.com/errata/RHBA-2018:0511

  No CVE.

- CESA-2018:0512 Important CentOS 6 kernel Security Update

  https://access.redhat.com/errata/RHSA-2018:0512

  CVE-2017-5715, CVE-2017-5753, CVE-2017-5754

- CESA-2018:0169 Kernel security and bug fix update.

  https://access.redhat.com/errata/RHSA-2018:0169

  CVE-2017-7542 - kernel: Integer overflow in ip6_find_1stfragopt() causes infinite loop

  CVE-2017-9074 - kernel: net: IPv6 fragmentation implementation of nexthdr field may be associated with an invalid option

  CVE-2017-11176 - kernel: Use-after-free in sys_mq_notify()

- CESA-2018:0199 CentOS 6 patch Security Update

  https://access.redhat.com/errata/RHSA-2018:1199

  CVE-2018-1000156

- CESA - 2018: 1124 Critical: python-paramiko security update

  https://access.redhat.com/errata/RHSA-2018:1124

  CVE-2018-7750

- CESA-2018:1319 Important CentOS 6 kernel Security Update

  https://access.redhat.com/errata/RHSA-2018:1319

  CVE-2017-7645, CVE-2017-8824, CVE-2017-13166,

  CVE-2017-18017, CVE-2017-1000410, CVE-2018-8897

- CEBA-2018:1339 CentOS 6 tzdata BugFix Update

  https://access.redhat.com/errata/RHBA-2018:1339

  No CVE

- CESA- 2018: 1454 Critical CentOS 6 dhcp Security Update

  https://access.redhat.com/errata/RHSA-2018:1454

  CVE-2018-1111

- CESA-2018:1651 Important CentOS 6 kernel Security Update kernel-2.6.32-696.30.1

  https://access.redhat.com/errata/RHSA-2018:1651

  CVE-2018-3639

- CEBA-2018:0597 CentOS 6 tzdata BugFix Update

  https://access.redhat.com/errata/RHBA-2018:0597

  No CVE

- CESA-2018:0649 Important CentOS 6 libvorbis Security Update

  https://access.redhat.com/security/cve/cve-2018-5146

  CVE-2018:5146

- CESA-2018:2180 Important CentOS 6 gnupg2 Security Update

  https://access.redhat.com/errata/RHBA-2018:2180

  CVE-2018-12020

- CESA-2018:2164 Important CentOS 6 kernel Security Update

  https://access.redhat.com/errata/RHSA-2018:2164

  CVE-2018-3639, CVE-2018-3665, CVE-2018-10675, CVE-2018-10872

- CEBA-2018:2163 CentOS 6 dhcp BugFix Update

https://access.redhat.com/errata/RHBA-2018:2163

No CVE

- SPHiNX has been upgraded from CentOS 6.9 to 6.10.

  The follwing updates are included in the new CentOS:

  CEBA-2018:1914 yum-utils BugFix Update

  CEBA-2018:1899 xorg-x11-server BugFix Update

  CEBA-2018:1899 xorg-x11-drv-mga BugFix Update

  CEBA-2018:1899 xorg-x11-drv-ati BugFix Update

  CEBA-2018:1903 upstart BugFix Update

  CEBA-2018:1864 systemtap BugFix Update

  CESA-2018:1877 Moderate sssd Security Update (CVE-2017-12173)

  CEBA-2018:1920 sos BugFix Update

  CEBA-2018:1872 sg3_utils BugFix Update

  CEBA-2018:1871 selinux-policy BugFix Update

  CESA-2018:1883 Low samba4 Security Update (CVE-2018-1050)

  CEBA-2018:1863 rsyslog BugFix Update

  CEBA-2018:1909 rpm BugFix Update

  CEBA-2018:1901 rpcbind BugFix Update

  CEBA-2018:1925 python-dmidecode BugFix Update

  CEEA-2018:1865 nss-util Enhancement Update

  CEEA-2018:1865 nss Enhancement Update

  CEEA-2018:1865 nspr Enhancement Update

  CEBA-2018:1855 nfs-utils BugFix Update

  CEEA-2018:1934 microcode_ctl Enhancement Update

  CEBA-2018:1887 microcode_ctl BugFix Update

  CEBA-2018:1889 man-pages-overrides BugFix Update

  CESA-2018:1929 Low libvirt Security Update (CVE-2018-1064, CVE-2018-5748)

  CEBA-2018:1876 libtirpc BugFix Update

  CEBA-2018:1892 libreport BugFix Update

  CEBA-2018:1904 libnih BugFix Update

  CEBA-2018:1861 libcgroup BugFix Update

  CEBA-2018:1895 kexec-tools BugFix Update

CESA-2018:1854 Important kernel Security Update (CVE-2012-6701, CVE-2015-8830, CVE-2016-8650, CVE-2017-2671, CVE-2017-6001, CVE-2017-7308, CVE-2017-7616, CVE-2017-7889, CVE-2017-8890, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-12190, CVE-2017-15121, CVE-2017-18203, CVE-2018-1130, CVE-2018-3639, CVE-2018-5803)

CEBA-2018:1873 jasper BugFix Update

CEBA-2018:1896 irqbalance BugFix Update

CEBA-2018:1859 iptables BugFix Update

CEBA-2018:1867 iproute BugFix Update

CEBA-2018:1908 initscripts BugFix Update

CEBA-2018:1911 hwdata BugFix Update

CEBA-2018:1891 httpd BugFix Update

CEBA-2018:1868 gnutls BugFix Update

CEBA-2018:1905 gmp BugFix Update

CESA-2018:1879 Moderate glibc Security Update (CVE-2017-15670, CVE-2017-15804)

CEBA-2018:1898 glib2 BugFix Update

CEBA-2018:1890 gcc-libraries BugFix Update

CEBA-2018:1921 e2fsprogs BugFix Update

CEBA-2018:1910 dracut BugFix Update

CEBA-2018:1884 dhcp BugFix Update

CEBA-2018:1913 device-mapper-persistent-data BugFix

CEBA-2018:1893 device-mapper-multipath BugFix Update

CEBA-2018:1928 dbus BugFix Update

CEBA-2018:1875 cups BugFix Update

CEBA-2018:1930 crash BugFix Update

CEBA-2018:1869 corosync BugFix Update

CEBA-2018:1862 coreutils BugFix Update

CEEA-2018:1922 ca-certificates Enhancement Update

CEBA-2018:1858 binutils BugFix Update

CEBA-2018:1866 bind BugFix Update

CEBA-2018:1892 abrt BugFix Update

CEBA-2018:1917 autofs BugFix Update

- CESA-2018:2390 Important CentOS 6 kernel Security Update

  https://access.redhat.com/errata/RHSA-2018:2390

CVE-2017-0861, CVE-2017-15265, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10901, CVE-2018-1000004

- CEEA-2018:2300 CentOS 6 microcode_ctl Enhancement Update

  https://access.redhat.com/errata/RHEA-2018:2300

  No CVE

- CESA-2018:2284 Important CentOS 6 yum-utils Security Update

  https://access.redhat.com/errata/RHSA-2018:2284

  CVE-2018-10897

- CEBA-2018:3454 CentOS 6 tzdata BugFix Update

  CentOS Errata and Bugfix Advisory 2018:3454

  https://access.redhat.com/errata/RHBA-2018:3454

  No CVE

- CESA-2018:3406 Critical CentOS 6 python-paramiko Security Update

  CentOS Errata and Security Advisory 2018:3406 Critical

  https://access.redhat.com/errata/RHSA-2018:3406

  CVE-2018-1000805

- CEBA-2018:2901 CentOS 6 device-mapper-multipath BugFix Update

  CentOS Errata and Bugfix Advisory 2018:2901

  https://access.redhat.com/errata/RHBA-2018:2901

  No CVE

- CEBA-2018:2895 CentOS 6 libcgroup BugFix Update

  CentOS Errata and Bugfix Advisory 2018:2895

  https://access.redhat.com/errata/RHBA-2018:2895

  No CVE

- CEBA-2018:2894 CentOS 6 mailx BugFix Update

  CentOS Errata and Bugfix Advisory 2018:2894

  https://access.redhat.com/errata/RHBA-2018:2894

No CVE

- CEBA-2018:2896 CentOS 6 nfs-utils BugFix Update

  CentOS Errata and Bugfix Advisory 2018:2896

  https://access.redhat.com/errata/RHBA-2018:2896

  No CVE

- CESA-2018:2892 Moderate CentOS 6 glusterfs Security Update

  CentOS Errata and Security Advisory 2018:2892 Moderate

  https://access.redhat.com/errata/RHSA-2018:2892

  CVE-2018-10911

- CEBA-2018:2900 CentOS 6 dhcp BugFix Update

  CentOS Errata and Bugfix Advisory 2018:2900

  https://access.redhat.com/errata/RHBA-2018:2900

  No CVE

- CESA-2018:2898 Moderate CentOS 6 nss Security Update

  CentOS Errata and Security Advisory 2018:2898 Moderate

  https://access.redhat.com/errata/RHSA-2018:2898

  CVE-2018-12384

- CESA-2018:2846 Important CentOS 6 kernel Security Update

  CentOS Errata and Security Advisory 2018:2846 Important

  https://access.redhat.com/errata/RHSA-2018:2846

  CVE-2018-5391, CVE-2018-14634

Known issues

- 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 empy file. Note that the pool and all its virtual tapes have been successfully moved to the new VAULT.
- In the **Virtual Tapes** table, the values in "Cached At" column are not sorted.
- The **Data Size** section is not sorted by the size in the **External Data** page.

- When editing or creating a new pool, using the browser's auto-complete to fill numerical values might cause out-of-range values to be accepted.
- When network interface bonding is configured, the netconfig command will return error when attempting to configure network settings for eth0 or eth1.

Compatibility

This section describes interoperability of 9.6-18 with third-party hardware and software.

Host server support

The following host servers were tested with SPHiNX for this release:

- HPE Integrity NonStop H-series and NS-series
- HPE NonStop BladeSystems (J-series)
- IBM® iSeries (AS/400) and Power System servers running IBM i v6r1, v7r1, and v7r2
- IBM AIX 6.1, and 7 on Power6, Power7, and Power8
- Windows Server 2003, 2008, and 2012 (for VTLs emulating MSL6000s and HPE MSL G3s)
- CentOS 6.x

Note SAS host connectivity is not supported for HPE hosts.

Host bus adapter support

These host bus adapters (HBAs) were tested for use with SPHiNX and IBM Power System servers:

- For use with Power8:

Feature code (FC)	CCIN	Description
5901	57B3	PCIe Dual x4 SAS Adapter
5273	577D	PCIe LP 8 Gb 2-Port Fibre Channel Adapter
577F	EN0A	PCIe2 16 Gb 2-port Fibre Channel Adapter
EJ10	57B4	PCIe3 4 x8 SAS Port Adapter

- For use with Power7:

Feature code (FC)	CCIN	Description
5901	57B3	PCIe Dual x4 SAS Adapter
5900 and 5912	572A	PCI-X266 Ext Dual-x4 3Gb SAS Adapter
0647, 1912, 5736, 5775	571A	PCI-X DDR Dual Channel Ultra320 SCSI Adapter
5749	576B	4 Gigabit PCI-X2 Dual Port Fibre Channel Adapter
5774	5774	4 Gigabit PCI Express Dual Port Fibre Channel Adapter
5735	577D	8 Gigabit PCI-E Dual Port Fibre Channel Adapter

- For use with Power6:

Feature code (FC)	CCIN	Description
2765	2765	2 Gigabit Fibre Channel Adapter
1905, 5758, 5760, 5761	280D	Single-port 4 Gigabit Fibre Channel PCI-X 2.0 DDR Adapter
5702	5702	PCI-X Ultra Tape Controller (Ultra SCSI LVD Controller)
0647, 1912, 5736, 5775	571A	PCI-X DDR Dual Channel Ultra320 SCSI Adapter
5774	5774	IOPless 4 Gigabit PCI Express Dual Port Fibre Channel Adapter

Library and standalone drive support

Libraries tested with Stacked Export jobs

- Dell PV132-T with LTO-3 drives - FC
- HPE MSL6000 with HPE Ultrium 2 drives - SCSI
- HPE MSL6000 with LTO-4 drives - FC, SCSI
- HPE MSL2024 with LTO-3 drives - SCSI
- HPE MSL5000 with Ultrium 1 and Ultrium 2 drives - SCSI
- HPE MSL6000 with Ultrium 2 drives - FC
- IBM TS3100 with LTO-4 and LTO-5 drives - FC
- IBM TS3580 with LTO-3 drives - FC

Standalone drives tested with Tape-to-tape Export jobs (host-native and virtual formats)

Note Worm media is supported on LTO-3, LTO-4, and LTO-5 drives.

- HPE Storageworks 960 Ultrium3 - SCSI
- HPE Storageworks 960 Ultrium3 - FC
- IBM 3580-HH4 - FC

Storage array support

SPHiNX supports any SAN-attached storage array that is supported by CentOS 6.7.

Note Path failover is supported for Fibre Channel disk array controllers only; failover is not supported for SAS controllers.

Virtual device emulation

SPHiNX allows multiple hosts to perform simultaneous backups to the SPHiNX server. However, the number of simultaneous backups affects performance of each backup, so it is recommended to limit the number of simultaneous backups.

Note Only the first channel of each SAS port is used for VTD and VTL creation when the port is configured as a virtual (target) mode port. If the port is configured as a physical (initiator) mode port, all four channels in the port are available.

Tape drive emulation

SPHiNX supports up to 32 virtual tape drives (VTDs) in any combination of SCSI, Fibre Channel, or SAS port. Due to system performance, a maximum of eight VTDs per Fibre Channel port, a maximum of three VTDs per SCSI port, and a maximum of three VTDs per SAS port is recommended.

Note Virtual tape drives support up to 256KB (262144 byte) blocks.

Tape library emulation

Multiple virtual tape libraries (VTLs) are supported per SPHiNX system. Again, the number of simultaneous backups affects the performance of each backup, so it is recommended to limit the number of simultaneous backups per VTL.

SPHiNX supports one VTL per Fibre Channel, SCSI, or SAS port with a maximum of 16 VTLs per system (limited by the number of available ports on the system). It is recommended that a maximum of eight VTDs per Fibre Channel VTL and a maximum of three VTDs per SCSI or SAS VTL is configured.

The following library types are supported, including the drive types supported within each:

- HPE MSL6000
  - Quantum SDLT320
  - Quantum DLT7000
  - HPE Ultrium 1
  - HPE Ultrium 3
- HPE MSL G3
  - HPE Ultrium 5
- IBM TS3500 (3584)
  - IBM ULT3580-TD1
  - IBM ULT3580-TD3
  - IBM ULT3580-TD4
  - IBM ULT3580-TD5
  - IBM ULT3580-TD6
- IBM TS3100
  - ULT3580-HH5
  - ULT3580-TD5
  - ULT3580-TD6

Note The IBM TS3100 is the only VTL supported for SAS IBM iSeries or Power System hosts, and it is only supported on IBM i v6r1, v7r1, and v7r2 SAS connected hosts. If using an IBM FC EJ10 SAS HBA in a Power8 server, only two LUNs per port are supported. Use the IBM FC 5901 SAS HBA if more than two LUNs are required.

Standalone drive emulation

The following standalone drive types are supported:

- Compaq Network Services Division 5257
- Tandem 519X
- Quantum SDLT320

- Quantum DLT7000
- IBM 3490
- HPE Ultrium (1)
- HPE Ultrium 3
- HPE Ultrium 5
- HPE M8701A
- HPE M8801A
- IBM ULT3580-TD1
- IBM ULT3580-TD3
- IBM ULT3580-TD4
- IBM ULT3580-TD5
- IBM ULT3580-HH5
- IBM ULT3580-TD6
- ALP-LTO-4

Note If using an IBM FC EJ10 SAS HBA in a Power8 server, only two LUNs per port are supported. Use the IBM FC 5901 SAS HBA if more than two LUNs are required.

Backup management application support

IBM Tivoli Storage Manager version 5.5.5 was tested use on the SPHiNX.

Note NetBackup Server is no longer supported on the SPHiNX because NetBackup Server 7.5 is only supported on CentOS 6 as a client. The role of Master server is not supported on CentOS 6.

Host connections were tested with the following backup management applications:

- From Windows Server 2012 R2 hosts:
  - Symantec Veritas NetBackup 7.6
  - Symantec Backup Exec 2014
  - CommVault Simpana 9.0
- From Windows Server 2008 R2 hosts:
  - Symantec Veritas NetBackup 7.5
  - Symantec Backup Exec 12.5
  - EMC (Legato) NetWorker 8.2.1
  - CommVault Simpana 8.0
  - Veeam® Backup & Replication v7
- From IBM AIX hosts:
  - IBM Tivoli Storage Manager 6.2 and 7.0

- From IBM iSeries (AS/400) hosts:
    - IBM Backup Recovery & Media Services (BRMS) V6R1 and V7R1
    - Help/Systems Robot/SAVE 11.0
- From RedHat hosts:
    - Symantec Veritas NetBackup 7.5

Diagnostic tools

- PuTTY
- Virtual Network Computing (VNC)
- On HPE models only:
    - HPE Integrated Lights-Out (iLO), HPE Integrated Lights-Out 2, or HPE Integrated Lights-Out Advanced Pack
    - HPE Systems Insight Manager (SIM) (on HPE models only)

Refer to the *Configuration Guide* for details.

Browser support

SPHiNX has been tested with the following versions of web browsers:

- Microsoft® Internet Explorer® 11.786.15063.0
- Microsoft Edge 40.15063.674.0
- Mozilla® Firefox® 57.0.4
- Google® Chrome 63.0.3239.132
- Apple® Safari 11.0.2

Notes

- SPHiNX might work with some older versions of the browsers listed above.
- SPHiNX version 9.3 and older used to work with only Microsoft® Internet Explorer®. However, since Microsoft® Windows® 10 update version 1709, Microsoft® Internet Explorer® cannot connect to these olderSPHiNX versions. If you have problem accessing your old SPHiNX in a browser, follow the procedure described in section SSL Protocols and Ciphers.

Clearing the web browser cache

- Microsoft® Internet Explorer® : press Ctrl-Shift-Delete (make sure to select **Temporary Internet files and website files**).
- Microsoft Edge: https://support.microsoft.com/en-us/help/10607/microsoft-edge-view-delete-browser-history

- Mozilla® Firefox®: https://support.mozilla.org/en-US/kb/how-clear-firefox-cache
- Google® Chrome: press Ctrl-Shift-Delete (make sure to select **Cached images files**)
- Apple® Safari: http://osxdaily.com/2016/01/17/empty-cache-safari-mac-os-x/

SSL Protocols and Ciphers

In order to avoid problems with web browsers, when you use SPHiNX version 9.1.2-4 or 9.3-25, you will need to change two (2) lines in the file `/etc/httpd/conf.d/ssl.conf`.

Locate both lines starting respectively with `SLProtocol` and `SSLCipherSuite`, make sure they are exactly as below:

```
SLProtocol ALL -SSLv2 -SSLv3
SSLCipherSuite
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:RSA+AESGCM:R
SA+AES:!aNULL:!MD5:!DSS
```

Upgrade and downgrade

Note If deploying SPHiNX for the first time, refer to the *Quick Start Guide* and then the *Configuration Guide*. This section is provided for customers who are upgrading existing installations.

After completing these steps, refer to the *Configuration Guide* for complete configuration information. For technical assistance, visit the ETI\SPHiNX website at ETI\SPHiNX for additional contact and support information.

Known issues

- If the downgrade fails for any reason, /VAULT00/ old root folder may be created but not removed. If so, manually remove this folder before reattempting to downgrade.

Upgrading SPHiNX

You can upgrade from version 9.1.2-4, 9.3-25, 9.4-2, 9.5-32, or 9.5-33 to 9.6-18. In case you are upgrading from 8.4-13, you need firstly to upgrade to 9.1.2-4 and then from this version on to 9.6-18.

During the upgrade, a backup of root filesystem is created, the upgrade is performed, and new system RPMs are installed along with the SPHiNX software. After the upgrade completes, you can view the upgrade logs from the Manage Logs page of the web interface.

WARNING:

- Upgrading from version 9.1.2-4 to 9.6-18 cannot be rolled-back. In case of a problem with the upgrade, you cannot use the downgrade menu from the UI. If that is the case and you have problems upgrading, you need to reinstall your previous version from the DVD and then restore your previously created system image from the UI.
- If you upgrade from 9.1.2-4 make sure to follow the procedure described in section SSL Protocols and Ciphers, then upgrade to version 9.6-18.

- If you are using clustering with version 8.4-13, you cannot upgrade to 9.6-189.6-18.
- If you are using clustering with any version 9.x, please contact support before upgrading.

The upgrade to version 9.6-18 should be expected to take approximately 30 minutes.

Before upgrading

1. Before upgrading, make sure the pubring.gpg file is not altered. Using ssh log in as bill:

   ```
   # cd ~/.gnupg
   # ls -lrt
   ```

   If pubring.gpg is not present or its size is 0, restore it:

   ```
   # cp pubring.gpg~ pubring.gpg
   ```

2. For the SecureVTS make sure to have saved a backup of your key manager before the upgrade. At the beginning, always upgrade the key manager server and only after that the other remote clients.
3. Download the self-extract file SPHiNX-x.x-xx-SelfExtract.exe and run it on your Windows station to get the `.upg` file.

To upgrade the SPHiNX server

1. Verify that at least 1GB of free disk space is available on the root partition of the SPHiNX server before upgrading.
2. If an IBM iSeries (AS/400) host server is connected to the SPHiNX server, vary off the tape drives before upgrading. Also, it is recommended that you place the AS/400 server in IOP reset using the AS/400 command line System Service Tools (SST):

   ```
   strsst->1,7,2,1,IOP->reset
   ```

3. Log in to the SPHiNX web interface. Click the **Log In** button at the top of the page and enter a username and password.
4. To ensure that the filesystem is clean, reboot the system prior to the upgrade. Click **Administration > System Tasks > Reboot the System**.

   Note Pay attention to **Reboot the System** page in case filesystem checks are required. If they are required, it is recommended to not postpone the filesystem check. Note the filesystem checking process might take long time.

5. Log back in to the SPHiNX web interface.
6. Click **Support > System Updates** on the navigation pane and then click **Create a System Restore Image**. Create the system restore image as described in the Help.

7. Upgrade the system:
    a. Click **Support > System Updates** on the navigation pane and then click **Upgrade System**.
    b. Select **From Uploaded File** and then click **Browse** to navigate to the file on the network, or type in the full path of the location.
    c. Click **UPGRADE**.
    d. Click OK to continue.

    Note Upgrading may take a while. Do not navigate away from the page until the upgrade completes.

    e. Confirm that the following message is displayed:

```
Completing Upgrade...
Revision Update Successful!
System must now be rebooted.
```

    f. Click **REBOOT** to complete the update.
8. Restart the web browser and launch the web interface.
9. Clear the web browser's cache (see section Clearing the web browser cache).
10. Navigate to the **System Status** page to verify if the version was installed.

After the upgrade completes, the virtual tape cache is generated and may take a considerable amount of time to complete.

Contact Support if the upgrade fails.

Downgrading SPHiNX

WARNING:

- You can downgrade to any previously installed version, except to 9.1.2-4. If you need to downgrade to 9.1.2-4, you have to reinstall your previous version from the DVD and then restore your previously created system image from the UI.

Complete the following steps if you want to downgrade SPHiNX to the previously installed version. The following is performed by the downgrade process:

- Backup of root filesystem is restored
- SPHiNX
- Backup of root filesystem is deleted

Note It is recommended to downgrade all appliances in your SPHiNX environment.

To downgrade:

1. Verify that at least 1GB of free disk space is available on the root partition of the SPHiNX appliance before downgrading.

2. If connected to an IBM iSeries (AS/400) host server over SAS, disconnect SPHiNX from the host server before downgrading.
3. If possible, locate the system restore image that was created before the system was upgraded. The version of the system restore image should match the version to which you will be downgrading.
4. If necessary, log in to the SPHiNX web interface. Click the **Log In** button at the top of the page and enter a username and password.
5. Click **Administration > System Tasks** on the web interface and then stop all SPHiNX services by clicking the appropriate links on the System Tasks page.
6. Click **Support > System Updates** on the navigation pane and then click **Downgrade System**.
7. Click **REVERT**. A dialog is displayed indicating you are about to revert SPHiNX to the previously installed version.
8. Click **OK** to continue.
9. Reboot SPHiNX.
10. Reconnect SPHiNX to the host server, if necessary.
11. Restart the web browser, launch the web interface, and then navigate to the System Status page to verify that the version was uninstalled.

Known issues

The following known issues apply to all 9.x versions. The issue tracking number is provided (in parentheses) to enable you to identify an issue if making inquiries to Technical Support. The tracking number is a unique identifier, not a counter.

Hardware, configuration, and hardware replacement

- The selected menu item does not correspond to the displayed page when the browser Back or Forward button is used. If you use the Back or Forward button on the browser to navigate to web interface pages, the previously viewed menu item is displayed but the highlighted menu item does not go back or forward to the corresponding menu item. (TL-0570)

Web interface

- "Port configuration has changed.." message is displayed if a change was made to the port configuration after a system restore image is saved and then an old system restore image is applied. For example, if ports are set to virtual, a system restore image is created, a port is changed to either physical, and then the old system restore image is applied, the message is displayed. (TL-9715)

  WORKAROUND: Click the Submit button on the Virtual Devices >Port configuration page.

- When restarting Tapeserver using the web interface, it may fail to restart. (TL-8781)

  WORKAROUND: Reboot SPHiNX.

- Cannot view another page if System Status page is refreshing. If you attempt to view another page while on the System Status page, the request to display the other page may be canceled because the System Status page is refreshing itself. (TL-8722)

  WORKAROUND: Wait until the System Status page refreshes itself (every minute), or go to a different page that will load more quicker, such as the About page, and then navigate to the desired page.

- The status of tapes shown in the Virtual Tapes page may not be current. When tape operations occur outside the Virtual Tapes page, the tapes shown in the Virtual Tapes page may be out of date. Removing a large number of Virtual Tapes can also result in out of date information. (TL-7996, TL-8026)

  WORKAROUND: A manual refresh for a single tape or clear cache for the entire page will update the cartridge information to the latest available.

- Pools may appear empty on the Manage Virtual Tapes page while the virtual tape cache is being built or rebuilt. Populating the virtual tape cache when there is a large number of virtual tapes on the system can take some time. This can result in some pools showing as empty because they have not been processed yet. It may appear that virtual tapes have been removed until all pools have been processed. (TL-7632)
- Clear Cache on a system under heavy load will cause the wrong tapes to be displayed. Under heavy load, virtual tape information may take longer to refresh. (TL-7406)

  WORKAROUND: Wait for system load to reduce and click Clear Cache again.
- Cartridge Status pop-up dialog is not updated while a cartridge is mounted. If you display the Cartridge pop-up dialog by clicking a link in the size (MB) column of the Configure Tapes and Pools page and then the cartridge is mounted, the data is not updated on the pop-up. (TL-2350)

  WORKAROUND: View this information when the cartridge is not mounted.
- Performance slows and the web interface becomes unresponsive if you close the browser during a pool move. After the pool is moved, the web interface becomes responsive again. The popup dialog box should indicate not to close the window or tab while the pool move is in progress. (TL-4956)
- Changing the port on a VTD after it has been created results in duplicate serial numbers. (TL-6429)

  WORKAROUND: Delete the VTD before changing ports, then recreate it on the correct port.
- Cannot re-log in to the web interface using the Log In button. If you are logged in as a non-administrative user, you must close the browser window and log in again as an administrator. The Log In button on the interface will not log you in as another user. (TL-1033)

VTL

- VTL is not updated after ejecting a tape. When removing media from a VTL, you must clear the page cache to update the cached information on the location of the media that has been removed. (TL-7333)

  WORKAROUND: Click Clear Cache on the Manage Virtual Tapes page.
- Incorrect serial numbers used for shared Fibre Channel VTLs. If a short serial number is used when creating a VTL (less than 10 digits), the serial number may be truncated and not displayed correctly. The tape type may also be affected. (TL-6263)

  WORKAROUND: Use at least 10 digits when manually entering a serial number.
- VTL cannot be deleted if /VAULT becomes unavailable. (TL-5882)

WORKAROUND: Click Manage Virtual Devices > Advanced > Manage Virtual Library Configurations > Edit virtual library magazines. Choose the library you wish to delete. Click Update (with no virtual tape loaded).

- One VTL created if the same target is used when creating multiple SCSI VTLs using AS/400. If multiple SCSI VTLs are created using the same target (but on different busses), all VTDs are associated to one VTL. The BTLIs are correct but there is only one VTL shown and all VTDs are associated to this. (TL-3874)

  WORKAROUND: Use a different target for the SCSI libraries on the different ports.

Data Encryption (SecureVTS)

- Erasing an encrypted virtual tape requires the encryption key. If the system does not have the key, the erase will fail and the virtual tape will remain locked. (TL-6606)

  WORKAROUND: Use the Mounts and Lock page or restart Tapeserver to remove the locks.

Scan/Cleanup

- Scan/Cleanup cannot erase cartridges in VTLs. When running Scan/Cleanup, locked cartridges in a VTL will not be erased after migration even though they meet the criteria to be erased. (TL-4326)

  WORKAROUND: Disable the VTL or remove the virtual tape from the VTL.

Tape-to-tape export and import (native export and import)

- Tape-to-tape export does not detect supported block size or set block mode. A tape-to-tape export writes a standard 256K variable block size. If the tape drive does not support this, you cannot use the tape drive for tape-to-tape export (Virtual Tape Format). (TL-6279)

Migration and stacked export and import

- Unable to unmigrate a pool. You cannot unmigrate the cartridges in a pool by selecting the pool; you must select individual cartridges. (TL-0386, TL-8114, TL-5997, TL-7586)

Backup management application support

- A backup may fail when using Netbackup with a VTL consisting of a MSL6000 and Ultrium 1 drives. The VTL will mount the drive but data is never written to the tape. (TL-4533)

  WORKAROUND: Change the tape drive to another drive type supported by MSL6000 (ex: SDLT, DLT7000, or Ultrium3).

- Backup Exec tape capacity is not correct with MSL6000 and SDLT drive. Backup Exec reports the wrong tape capacity when connected MSL6000 and SDLT drive. An Ultrium 3 drive should be used in the MSL6000 if Backup Exec is used on the initiating server. (TL-7940)
- Backup Exec 2012 incorrectly reports VT sizes for SDLT and DLT7000. Backup Exec 2012 incorrectly reports VT sizes for SDLT and DLT7000 tapes. Blank VTs show up with 16MB of free space. Tapes with data report the wrong amount of space left and space used. (TL-8063)

  WORKAROUND: Use the Ultrium, or Ultrium 3-SCSI drive types for correct tape usage.
- Restoring a backup using ARCServe succeeds, but restoring individual files fail. Restoring an entire backup consisting of a multi-tape spanned backup succeeds, but restoring individual files fail. The error reported is “Invalid file signature 0c00000000”. (TL-7725, TL-6517)

  WORKAROUND: Restore the entire backup to obtain the single file.
- TSM running on a host system fails to label tapes when the VTDs are Ultrium. Though the drives are detected and associated with the library, when it tries to load the tapes for labeling, an error is displayed indicating it cannot label the volume. (TL-4670)

AutoCopy, Instant DR, and Replication

- Stop on error for import does not stop on failure. When the first error occurs for a cartridge within a VTL, the job should fail and no other cartridges should be processed. (TL-5982)

  WORKAROUND: To avoid this issue, import one cartridge at a time.
- Unlabeled cartridges are not copied to target server. Cartridges that are unlabeled and written to from the host server are not copied to the target server during AutoCopy. (TL-4286)

EMS

- EMS restart function fails to function if the host name in the EMS messages and the host name as configured in the EMS Configuration page are not identical (including case). For example, if the host name as sent by the host is 'DEV4' but the host name as configured in the EMS Configuration page is 'dev4', the loss of EMS keep-alive messages will not be detected and the EMS restart function will fail to work. (TL-6110)

  WORKAROUND: Ascertain that the host name as configured in the EMS Configuration page is identical to the host name sent from the host (normally all uppercase).
- Enable Keep Alive and Enable Host Notifications must be selected to enable keep-alive messaging. You must enable both options to enable EMS keep-alive messages. Use the EMS Configuration page to set these options. (TL-3152)
- If ems_keep_alive_interval is set too small, a “keep-alive lost!” message is generated. If the ems_keep_alive_interval is set too small, a very large number of Event Monitoring System (EMS)

messages may be queued. This could result in a “keep-alive lost!” message being generated. (TL-8124)

WORKAROUND: To avoid this keep the value of the ems_keep_alive_interval parameter just smaller than the timeout value for telnet or SSH depending on which is being used for EMS.

Clustering

- Policies will work on the node in the cluster on which they were created, but will not work on other nodes within the cluster. Simple policies such as erase, encrypt or decrypt may work on other nodes, but should not be considered reliable. (TL-8507)
- Cannot resolve the hostname in a clustered environment without a DNS server. Currently, you cannot configure VTS in a clustered environment to use a fully qualified domain name without the use of DNS. (TL-6874)
- One or more GFS cluster nodes may receive a "Call Trace" message if communication is lost between one or more nodes. (TL-9211)

  WORKAROUND: Reboot all GFS cluster nodes at the same time.

Troubleshooting

This section includes information about how to troubleshoot problems and notes about items that may need clarification.

Hardware, configuration, and hardware replacement

- Starting a VTD on the NonStop results in two errors logged to debug.log. Immediately after the NonStop command “SCF START TAPE $VTAPE00” is issued to start a virtual tape device, one or more of the following messages may appear on the VTS server in /usr/local/tape/log/debug.log:

  ```
  Mon Jun 23 14:31:33 2008: [cli_tape 0x05000007] read ERROR on message
  rc = 1
  ```

  These messages are benign and may be ignored. (TL-1802)

- After rebooting a node in a GFS cluster, the node may not rejoin the cluster. (TL-9316)

  WORKAROUND: Use the luci High Availability Management utility to have the node rejoin the cluster.

- Fibre Channel ports do not initiate link status and lasers are off if ports are set to target mode and VTDs are not defined. When a Fibre Channel port is enabled for target mode, the port will not initiate link status until a VTD has been defined on that port and the lasers will be off. The port will appear to be disconnected unless a VTD has been defined. Likewise, when TapeServer is stopped, the Fibre

Channel ports will drop link status, to emulate the function of a physical tape drive with the power turned off. (TL-2641)

- Must run /usr/local/tape/bin/grub-serial.bash to access GRUB from the console. When VTS boots, you must press a key when prompted if you wish to see the GRUB menu. The /usr/local/tape/bin/grub-serial.bash command will modify the system boot configuration to provide serial console access to the GRUB boot menu. This command must be run as root. In some cases, it may cause the system boot time to be greatly increased, although the normal boot time is only expected to increase by 10 seconds after running this command. (TL-2255)
- I/O fails to resume after Fibre Channel cable is disconnected and HBA times out. If you disconnect the Fibre Channel cable to the VTS for a time period that exceeds the VTS FC HBA driver timeout value, I/O is interrupted and will not recover. (TL-1886)

  WORKAROUND: Rediscover the Fibre Channel devices on the initiator or reboot the initiator.

General operations

- In 9.1+, VTS checks that any VTD to be used is online from the NonStop system using the MEDIACOM STATUS command. As a result, you may see the following behavior:
  - Previously, the NonStop userid created for use by VTS was used to start an EMSDIST process and set SAFEGUARD security. MEDIACOM is secured for SUPER group EXECUTE access only. By granting the VTS userid READ and EXECUTE access to MEDIACOM, this is resolved but the VTS userid is elevated to 'privileged' status.
  - VTS does not distinguish between two NonStop systems when running the MEDIACOM STATUS command where only one system is configured with Ethernet access. While VTS will start two EMSDIST processes to which it has an Ethernet connection, one opens the local $0 and the other opens the second system's $0 over EXPAND. This enables VTS to see the mount messages for both systems, though it is aware they are separate systems. VTS does not distinguish between two NonStop systems when running the MEDIACOM STATUS command and does not consider the second system's VTDs to be online. Each system should be configured to use its own Ethernet connection for EMS messages.
- If a cartridge contains the maximum amount of data, encrypting the cartridge will cause the cartridge limit to be exceeded. However, no error is given to indicate this situation. The cartridge can be exported but if it is imported to a cartridge of the original cartridge limit size, the import will fail. (TL-1168)

  WORKAROUND: Import the cartridge to a cartridge whose size is larger than the original cartridge limit size.
- Kernel call trace is displayed on console if cluster data is included in a troubleshooting package. When generating a troubleshooting package, if the "Include Cluster data" checkbox is selected, a

kernel call trace will be displayed on the console. This is normal behavior and does not affect system operations. (TL-5111)

- Rerun job in process if power is lost to system. If power is lost while an export is in-progress, re-run the job to ensure that data is written to storage as expected. (TL-4607)
- Must use the rewinding name of a drive for import_export_drive_exclude parameter in vts.conf. When specifying devices to be excluded from imports or exports using the import_export_drive_ exclude parameter in vts.conf, be sure to use the rewinding name of the drive rather than the non-rewinding name. That is, use '/dev/st0', not '/dev/nst0'. (TL-1962)

Web interface

- Virtual tapes cannot be renamed. You cannot rename a virtual tape. (TL-4414, EAR- 6411)

  WORKAROUND: Create new virtual tapes with the desired name using the Advanced Media Actions option on the Manage Virtual Tapes page.

- Changing tape library settings could cause the drives to be unusable. When a tape library was changed from random access mode to auto loader mode, the Physical Device settings could become confused. This caused the changer to be disconnected and the drive entries could not be edited from the Physical Drives page. This can be avoided if the settings in the Manage Settings page are first changed to “Disabled” for the device and saved, followed by the device being changed to auto loader mode. (TL-7812)
- Adding a new certificate does not display the new certificate page. If the browser recognizes the uploaded certificate's authority as a verified authority, no warnings are generated. Firefox and IE will not generate a warning for a signed certificate if the chain follows to a trusted authority. On Firefox and IE, installed SSL certificates information can be obtained directly from the browser's address bar. (TL-6598)
- Logging in to web interface on localhost does not redirect to secure page. When accessing the web interface from the localhost, HTTPS is not needed because data is not transmitted. (TL-3643)
- Browser may display old data or errors if not refreshed. If an unexpected error occurs or data appears to be old, refresh the browser. Old data is cached and may need to be cleared. (TL-1662)
- File size of a mounted tape being written may not be updated. If a virtual tape is mounted and being written to, the size shown on the page may not be updated until the tape is dismounted. Normally, this value will be updated when file marks are written to the tape, so usually this is not an issue for most users. (TL-0881)

VTL

- Must remove reservations before disabling a VTL. If you cannot disable a VTL though no virtual tapes are loaded in the VTDs, make sure no reservations exist for one of the VTDs in the VTL. For AS/400,

this can be done by “varying off” the MLB device or de-allocating the TAP devices. (TL-3837)

- Multiple tape device types may not be supported in a VTL. Using mixed tape devices within the VTL will only function as well as the host backup software functions in that environment. Typically, this can cause the host software to confuse tape types and drive types. It is recommended that all tape drives are of the same type. (TL-3844)

Data Encryption (SecureVTS)

- Tape library must be configured for encryption to support export of encrypted tapes. The external tape library must be correctly configured to allow VTS to manage encryption. Refer to the library documentation for instructions. (TL-6435)
- When encrypting or decrypting a cartridge and TapeServer stops, temporary directory and file are not deleted. Do not stop TapeServer or restart VTS unless the system is quiesced. (TL-3071)

Tape-to-Tape export

- Tape-to-Tape export fails when library is moved to a different port. All devices that are not attached when TapeServer starts must be manually discovered using rescan-scsi-bus.sh. (TL-5698)
- Bus, target, LUN, and device number replaced by friendly name for tape-to-tape exports. In prior releases, when performing a tape-to-tape export job, the drives presented included Bus, Target, LUN, and /dev/nst# as well as the make and model. With the addition of the friendly names to the web interface in 6.04.05, all of this information has been replaced with the friendly name as it's configured in the Physical Drives section of the Manage Settings page. (TL-5844, TL-5155)
- Cartridge remains locked after failed tape-to-tape export from Manage Virtual Tapes page. Tape-to-Tape export performed from the Manage Virtual Tapes page on a cartridge in a pool (not in a VTL) fails and the cartridge is not unlocked after the failure. If the export is done from the Configure Tapes and Pools page, the cartridge is unlocked after the failure. (TL-4536)

Migration and stacked export

- After installing EMC (Legato) NetWorker, the web interface may display the following errors:

  ```
  FATAL: Ident authentication failed for user "postgres" (PGError)
  ```

  This is because NetWorker adds an entry for the IPv6 localhost address in the **/etc/hosts** file. This prevents PostgreSQL from working properly. (TL-9353)

  WORKAROUND: Change the METHOD field for the ipv6 localhost(::1/128) entry in **/var/lib/pgsql/data/pg_hba.conf** from "ident" to "trust" as shown below:

  host all all ::1/128 trust

- Export relies on the capabilities of the backup management agent. The agent will retry the backup repeatedly until it determines file change has not occurred. This could mean that an empty virtual tape is backed up if a virtual tape is erased after the stacked export has begun but before it has completed. (TL-4922)

VTSPolicy

- Memory issues occur when too many concurrent VTSPolicy migrations are attempted. At most, one migrate per physical tape drive should occur at any one time. (TL-6135, EAR-7280)
- Incremental backup backs up all cartridges. Any incremental backup backs up all cartridges, even unchanged cartridges, within the requested file space. This problem is due to the fact that a virtual cartridge contains user data and metadata. VTS often updates the metadata even when the user data has not changed, causing the change time (ctime) on the file to be updated; this is what causes the file to be backed up even if the user data is unchanged. (TL-2155, EAR-4456)

Utilities and services

- CLIM does not see more than 8 LUNs after changing the tape type. This occurs if VTS is started after device discovery. (TL-6777)

  WORKAROUND: Device discovery on the CLIM can be best accomplished by first starting VTS, then connecting the CLIM. Done this way, devices should be discovered correctly. Finally, the device may be mapped with the CLIM to the NonStop.

- EMSDIST service does not start after upgrading comForte SSH to a new version of \dev3. Two issues were found with comForte SSH version 0100b:
  1. SSH fails if uppercase “TACL” is used but it works for lowercase.
  2. New SSH notice - there is no "Last Logon:" output.

  WORKAROUND: From the EMS Configuration page of the web interface, make the following changes:

  - Set **Service Answer** to **tacl** (lowercase)
  - Set **Login Successful** to **/TACL /**
- CLIM device discovery is fragile. Best practice is to set up and connect VTS to the CLIM. When VTS is configured and ready, reboot the CLIM. All LUNs will be viewable after this CLIM restart, and then map the LUNs. This is only necessary for the initial configuration and setup of the CLIM. (TL-5582)
- /usr/local/tape/bin executables cannot be run as root. The programs in /usr/local/tape/bin must not be run as root unless otherwise specified. If this is done inadvertently, check the ownership of the files in /home/bill/.gnupg and ensure that they are owned by the 'bill' account and have group ownership of 'bill' as well. Failure to observe this precaution may cause a number of operational problems including failure to properly process mount requests. (TL-2367)