

Release Notes for the Cisco NSS3000 Series Network Storage System Version 1.15

February, 2009

These release notes contain important information about the initial release of the NSS3000 Series Network Storage System and any limitations, restrictions, and caveats that apply to this product.

Contents

This information is in the release notes:

- **Compatibility**
- **Limitations and Restrictions**
- **Open Caveats**

Compatibility

When the NSS is joined to the Windows Server 2008 domain and multiple users are sharing the same file, these are the compatibility issues that can occur:

- When accessing a database file (such as a Microsoft Access file), files opened by the user automatically obtain an exclusive lock, blocking other users from opening the files, even in read-only mode.
- In other applications, when multiple users access the same file, each user has read-write access privileges. This can cause the file to be overwritten and can lead to data loss. If this occurs, no user warning message appears.

Although this feature is working, Cisco does not fully support joining the NSS to the Windows Active Directory Server (ADS) in a Windows Server 2008 environment. This workaround is to enforce file access by one user at a time. (CSCsw88123)

Limitations and Restrictions

This is the known limitation for this release:

The maximum transmission unit (MTU) size that this firmware release supports is 2000 bytes. There is no workaround. (CSCsw85950)

Open Caveats

These are the open caveats for this release.

- CSCsw83249

When creating a RAID1, RAID1+Spare, or a RAID5 array using the Initial Setup wizard, the total disk space usage is less than the available disk capacity.

The workaround is to delete the existing array built by the Initial Setup and recreate it manually by using the **Storage ➔ RAID** page in the Configuration GUI.

- CSCsw85340

When the NSS is running over a network that is on a different subnet, a user cannot mount a CIFS connection by using a hostname.

The workaround is to mount the CIFS connection by using an IP address.

- CSCsw85367

When the Network Access Filter is set to Policy=DropTraffic and Filter=AllowAll or Policy=Drop and Filter=AllowCIFS, the CIFS mount does not work properly.

The workaround is to set the Network Access Filter to the default settings by using the Configuration GUI.

- CSCsw85370

When the Network Access Filter is set to Filter=AllowHTTPS and Filter=DropFTPS, you cannot add Network Access from the Configuration GUI.

The workaround is to set the Network Access Filter to the default settings in the Configuration GUI.

- CSCsw85385

When an unexpected power cycle occurs on the NSS, the time might be corrupted on the NSS. This only applies if the time is set manually, not by using NTP.

When this occurs, a pop-up alert window appears when you access the Configuration GUI after the unexpected shutdown.

The workaround is to manually check the time by clicking **Admin ➔ Time** in the Configuration GUI and to correct the time if necessary.

- CSCsw85433

When writing simultaneously to the same file by using NFS and FTP, or by using NFS and CIFS, the NSS file locking mechanism does not work properly.

There is no workaround.

- CSCsw85463

If a data write operation is in progress, and the system power is interrupted, data stored in a degraded RAID1 or RAID5 array might become inaccessible. This is common to all NSS systems using software RAID implementations.

These are the workarounds:

- Replace the failed drives in the degraded arrays as soon as possible, as failed RAID arrays can result in complete loss of all user data.
- Use the degraded mode management feature to limit the amount of time that a RAID array will run in the degraded state.
- Implement a backup power strategy by using a UPS or RPSU backup power system.

- CSCsw85469

When a RAID0 array failure occurs, an alert (SNMP trap, email or system alert) is not triggered.

When this occurs, the Drive Error LED (on the disk that caused the array failure) does not light up.

There is no workaround.

- CSCsw85475

When you create a share by using the Initial Setup wizard and enable NFS, users are assigned root privilege access.

The workaround is to not enable NFS in the Initial Setup wizard. If NFS is required, you can enable it at a later time by using the Configuration GUI.

- CSCsw85493

The **Network ➔ Identification** page in the Configuration GUI does not accept domain controller hostnames that begin with a digit.

The workaround is to enter the IP address of domain controller instead of the hostname.

- CSCsw85481

When rebuilding a RAID1 spare device, the rebuilding does not resume after the NSS reboots. After reboot, the array might be falsely marked as clean and the drive falsely marked as synced. This does not affect the initial rebuild of an array following a RAID creation.

The workaround is to not reboot the NSS during the RAID rebuild.

- CSCsw85488

If power is interrupted when rebuilding a RAID array (RAID1, RAID5 or RAID10), the rebuild does not restart automatically after the system is powered up again.

When this occurs, the array remains in the degraded state and the rebuilt drive is ejected from the array.

The workaround is to manually restart the rebuild by adding the ejected drive back to the array by using the Configuration GUI.

- CSCsw85517

When the RAID global spares option is enabled in the Configuration GUI, the RAID spares are not shared during the RAID array rebuild.

For example: If RAID A has a hot spare and RAID B does not, if RAID B is degraded while RAID A is rebuilding, the spare will not transfer to RAID B until after RAID A completes the rebuild.

There is no workaround.

- CSCsw85643

When replacing and rebuilding a drive in a 2-disk RAID1 array, both drive LED's stay lit.

The workaround is to reboot the NSS after the RAID rebuilt completes,

- CSCsw85780

When a Seagate 1 terabyte (TB) hard drive (model ST31000340AS) is installed in the NSS, it is not detected by the system on bootup or when hot plugging the drive.

There is no workaround.

- CSCsw85800

When Seagate hard drives are installed in the NSS, they can take about 30 seconds to be detected on bootup.

This problem occurs because pin 11 of the SATA power connector is not connected in the NSS backplane design.

There is no workaround.

- CSCsw85923

When the Default Network Policy filter is set to Drop Traffic, no automatic Allow Filter is created for the default gateway.

When this occurs, all traffic from the default gateway is dropped and all traffic sent from other subnets through a router is not forwarded to the NSS.

The workaround is to manually create an AllowAll Network Access Filter for the default gateway IP address by using the Configuration GUI.

- CSCsw86022

If a user was granted write access to a share and the write access was revoked, the user can still write to subfolders by using FTP.

This problem only occurs under these conditions:

- The user has write privileges to the subfolder (either because the user is the owner, or was granted access by the owner).
- The user has read privileges to the share (by having explicit share read-only access).

There is no workaround.

- CSCsw85454

If a user was granted write access to a share and the write access was revoked, the user can still write to subfolders by using NFS.

This problem only occurs under these conditions:

- The user has write privileges to the subfolder (either because the user is the owner, or was granted access by the owner).
- The user has read privileges to the share (by having explicit share read-only access).

The workaround is to not enable NFS (which is disabled by default), if NFS is not being used.

- CSCsw85502

When the NSS sends out a broadcast message to discover an NIS server, the broadcast is only sent to the physical interface, not over any VLANs that are defined in the system.

The workaround is to not use the NSS in networks where NIS servers are only accessible over VLANs.