Product Bulletin 26

Product	StorNext versions 2.8, 3.0 and 3.1
Summary	Under some circumstances, Windows security descriptors can become corrupted, causing files to become inaccessible on SNFS Windows clients.
Date	May 2008

Problem

Due to an issue in flushing cached entries of security descriptors on SNFS clients, the security descriptor for a file can be corrupted, causing invalid data to be stored in the metadata portion of the file system. This corruption is interpreted by the Windows access system calls to not allow access.

Workarounds

1. Increase the SNFS buffer cache by 2 times the current size. This reduces the likelihood of encountering the buffer cache flushing issue, but will not correct existing corruption.
2. From a Linux or other non-Windows client, identify the files that have the corrupted security descriptors, and then perform the following procedure:
   a. Copy the file to <filename>_old. This creates a new inode and uses the parent folder's security descriptor.
   b. Move <filename>_old to <filename>.

Note: This workaround does NOT remove the corrupted security descriptors, and there is a chance the corrupted security descriptors could be used on new files or directories.

Fixes

Follow the procedure that applies to your version of StorNext.

For StorNext 2.8

Install StorNext 2.8.0 build 50 or greater, and then follow step 2 in the Workarounds section to correct the invalid security descriptors. **See the previous Note about corrupted security descriptors potentially affecting new files or directories.**

For StorNext 3.0

Install StorNext 3.0.3 build 59 or greater, and then follow step 2 in the Workarounds section to correct the invalid security descriptors. **See the previous Note about corrupted security descriptors potentially affecting new files or directories.**

For StorNext 3.1

Install StorNext 3.1.0 build 20 or greater, and then run `cvfsck` with the `-S` option on the file system. This will find all of the corrupted security descriptors and files associated with the invalid descriptors, and then reset their security descriptors to the parent directory. **This fix is the ONLY complete solution and should be used if at all possible.**

Support Information

For further assistance, contact Quantum Global Services.

North America	1+800-284-5101
UK, France, Germany	00800 4 QUANTUM
EMEA	+44 1256 848 766
Online	www.quantum.com/ServiceandSupport