Customer Bulletin

Product Model Name: Archive Appliance
Date: November 2007
Reference ECO No: NA

Reason for Bulletin

To detail best practices for archiving data to the Archive Appliance in order to help mitigate the risk of data loss or corruption.

Background

The Archive Appliance provides permanent storage of archived data on UDO media. The Archive Appliance uses a multistep process to archive data and confirm the write process has completed and thus the file is protected. Plasmon has found that some customer's applications are not properly verifying that data has been written to the UDO Archive Appliance prior to deleting archived files from their production data store. This unnecessarily exposes their data to loss or corruption.

The "Archive Bit/Attribute"

In Windows there is a binary flag associated with every file called the archive bit. The basic idea behind the archive bit is that it can tell an application whether or not a file is protected via a backup or archive process.   When a file is first created the archive bit is set to 1. Anytime a file is later modified the archive bit is set to 1. The only time the archive bit is set to 0 is if some program specifically tells Windows to reset it. The Archive Appliance's implementation of the archive bit works the same way and enables Windows applications to check that the data has been written securely to UDO media before removing or moving the original data.

Archive Appliance and the Archive Bit

The first stop for a file ingested into the Archive Appliance is the internal RAID cache. This cache serves two purposes. First it allows the Archive Appliance to ingest files at NAS-like speed. Second it serves as a buffer or work space for the HSM component. When a file is ingested into the Archive Appliance's file system the archive bit for the file is set to 1. At this point in time the file is classified as dirty since it is not yet written to permanent media.

The second step is when, by policy, the file is written to UDO media. The UDO drive performs a write verify process, meaning that the file is written to the UDO media and then the file is verified to ensure that the file was written correctly. Once this has been done, the third step is to change the archive bit to 0 in the file system. The fourth step is to flush the file from the RAID cache; once again this is done according to policy. At this point in time there is a file stub in the Archive Appliance's file system and the archive bit is set to 0, indicating that the file is properly archived.

Best practices would dictate that the client applications perform the following two additional steps prior to deleting the file from the client's production data store:

1. Check the Archive Appliance and verify that the file's archive bit has been set to 0 and
2. Recall the file and verify that the archived version is the same and the original.

Once these two steps have been done the client application can be sure that the data it sent to the Archive Appliance has been properly archived for long term storage.

NOTE

In non-Windows environments there is an API that can be used in a similar manner. For information on the API please contact your technical support team.

Contact Information for Technical Questions:

Americas and Asia Pacific

Plasmon Technical Support Team
United States Calls: 1-877-585-6793
International Calls: 1-719-593-4437
Fax: 1-719-593-4192
Email: tech.support@plasmon.com
Internet: www.plasmon.com

Europe, Africa, and Middle East

Plasmon Technical Support Team
International Calls: +44 (0) 1763 262 963
Fax: +44 (0) 1763 264 407
Email: support@plasmon.co.uk
Internet: www.plasmon.com