2nd Modification

**128 bit Blowfish Encryption Algorithm outperforms 256 bit AES (Rijndael)**

**Submitted: 3/24/2009 11:19:18 PM**

**Release: All**

**Category: Galaxy AFP**

**Description:**

Software based encryption is a CPU intensive operation as the encryption algorithm process is managed at the processor level for the server that is completing the encryption process.

Blowfish was rated on performance based on the number of megabytes encrypted per second in a Windows environment with the CommServe® software. Blowfish scored 10 on a scale of 1-10, with 10 being the fastest on a Test system with 1GHz single CPU system, 1GB RAM and Windows 2003. Only one single backup stream with encryption options enabled was used for testing (Your results will vary depending on your testing environment).

Blowfish 128 keys --> 85.74 Megabits per second

AES 256 -------> 27.1 Megabits per second

Blowfish 128 keys ---> 37.68 Gigabyte per hour

AES 256 -----> 11.91 GB/hour

CommVault recommends selecting specific data for encryption rather than completing ‘bulk’ encryption operations for client server systems. It is not recommended to encrypt Windows executables, programs and similar object types.