



Integrating Bus-Tech Mainframe Appliance for Storage (MAS), Decru DataFort™, and NetApp Storage

Proof of Concept

Mark Hayakawa, Toby Creek, Network Appliance, Inc.

Warren Jew, Decru

October, 2005 | TR-3433



ABSTRACT

Encryption of data in place is becoming an important capability for financial institutions and other organizations that hold sensitive data. The Bus-Tech, Decru, NetApp solution gives companies the ability to transparently encrypt data at rest and in place using virtual tape media.

TABLE OF CONTENTS

Encryption of Data at Rest for Tape Applications..... 3

In-line Encryption of Data at Rest Residing on MAS Managed Storage..... 3

NetApp BusTech Decru Mainframe Encryption Solution 3

 Decru DataFort 3

 BusTech MAS 3

 NetApp Storage 3

Key Elements of Business Challenge 4

Demonstration Environment..... 4

 Test Objectives 5

Demonstration Configuration 5

 DataFort Setup 5

 MAS Setup..... 5

 NetApp Storage Setup 6

 z/OS Setup 6

Demonstrate Data Encryption between the MAS and NetApp Storage Using DataFort 6

Demonstrate a Simple Hot Site Recovery Using SnapMirror..... 6

Integrating a DataFort into an Existing MAS Virtual Tape Configuration 7

Conclusion 7

ENCRYPTION OF DATA AT REST FOR TAPE APPLICATIONS

Security has become an increasingly important concern in data processing. The horror stories of missing tapes with critical customer data are prominent in the news. Additional government and business regulations now require the encryption of sensitive data. Data residing on any medium may require encryption for security purposes.

IN-LINE ENCRYPTION OF DATA AT REST RESIDING ON MAS MANAGED STORAGE

Currently there is no data encryption solution that will provide for the in-line encryption of virtual MAS tape data. Data must be encrypted on z/OS prior to placing it on a MAS virtual tape. The decryption of the data would require the reading system to have the appropriate decryption keys and decryption software installed. This activity will take CPU cycles from MVS processing and may affect the total workload of the system.

NETAPP, BUS-TECH, DECRU MAINFRAME ENCRYPTION SOLUTION

Decru DataFort

Decru secures networked storage by protecting data both in transit and stored on disk. Decru DataFort storage security appliances use wire-speed encryption, granular access controls, strong authentication, and cryptographically signed auditing to protect stored data. Decru DataFort appliances can be deployed transparently in SAN, NAS, DAS, or tape backup environments, with no changes to servers, desktops, applications, or user workflow. Built specifically to secure data storage, Decru DataFort combines custom, high-performance hardware with comprehensive key management, creating a powerful, yet manageable security solution. DataFort is application independent and vendor agnostic and fits seamlessly into the existing network infrastructure. With Decru DataFort, enterprises and government organizations can fully leverage the benefits of networked storage, confident that their data assets are secure.

The Decru DataFort encryption technology is implemented in-line on the data path and can be used with Fibre Channel Protocol (FCP), Ethernet, or SCSI.

The E-Series DataFort that supports Ethernet was selected for this demonstration.

Bus-Tech MAS

The Bus-Tech MAS is an appliance that connects to IBM compatible mainframes via Enterprise Systems Connection (ESCON) or IBM Fiber Connection (FICON). The MAS emulates mainframe 3480 or 3490 controllers with the capability of virtualizing up to 256 tape transport devices. The MAS has the capability to attach different kinds of open systems storage. Virtual tapes can be defined on the MAS up to 256GB in size. The default size is 2GB. These virtual tapes are stored on a NetApp FAServer® volume. The tape volume serial (volser) is the file name in the MAS tapelib directory. The hierarchical directory structure of the MAS lends itself to the linear growth of the number of virtual tape volumes that it can manage. The MAS also incorporates integrated load balancing and dynamic failover.

The MAS can be configured to use NAS, SAN, or content addressable storage (CAS). For data to be shared between MAS devices, NAS or CAS has to be utilized. For CAS access, a separate database has to be maintained at the local site and synchronized with the remote site to provide C-Clip and blob relationships to tape volsers for the remote site MAS.

For this demonstration, the MAS was connected with Gigabit Ethernet (GbE) through the Decru DataFort to the NetApp FAS3050. All connections were done using NAS NFS.

NetApp Storage

NetApp storage can be connected to the MAS with either FCP or GbE. Tape images are stored on NetApp volumes as files. NetApp volumes can currently hold 12TB of usable space, which is equivalent to 6000 default 2GB tape volumes. Each new FAServer volume can be exported and mounted to one or more MAS

as a subdirectory off the main or tapelib directory. Utilizing NFS, multiple MAS can share the data residing on one FAServer volume. This provides for seamless failover in the event of a MAS failure.

NetApp SnapMirror® allows for the synchronous, semi-synchronous, or asynchronous transfer of data at the volume level. Asynchronous mirroring can be bandwidth throttled to efficiently use available bandwidth between sites. This mirroring ability is available for compliance or noncompliance volumes.

KEY ELEMENTS OF BUSINESS CHALLENGE

Decru DataFort is designed to provide enterprise customers the security of data encryption as well as the ability to implement the role of a security officer separate from the systems management role. This enables customers to secure their data at rest and in transit to avoid exposure to litigation due to information loss and regulatory noncompliance.

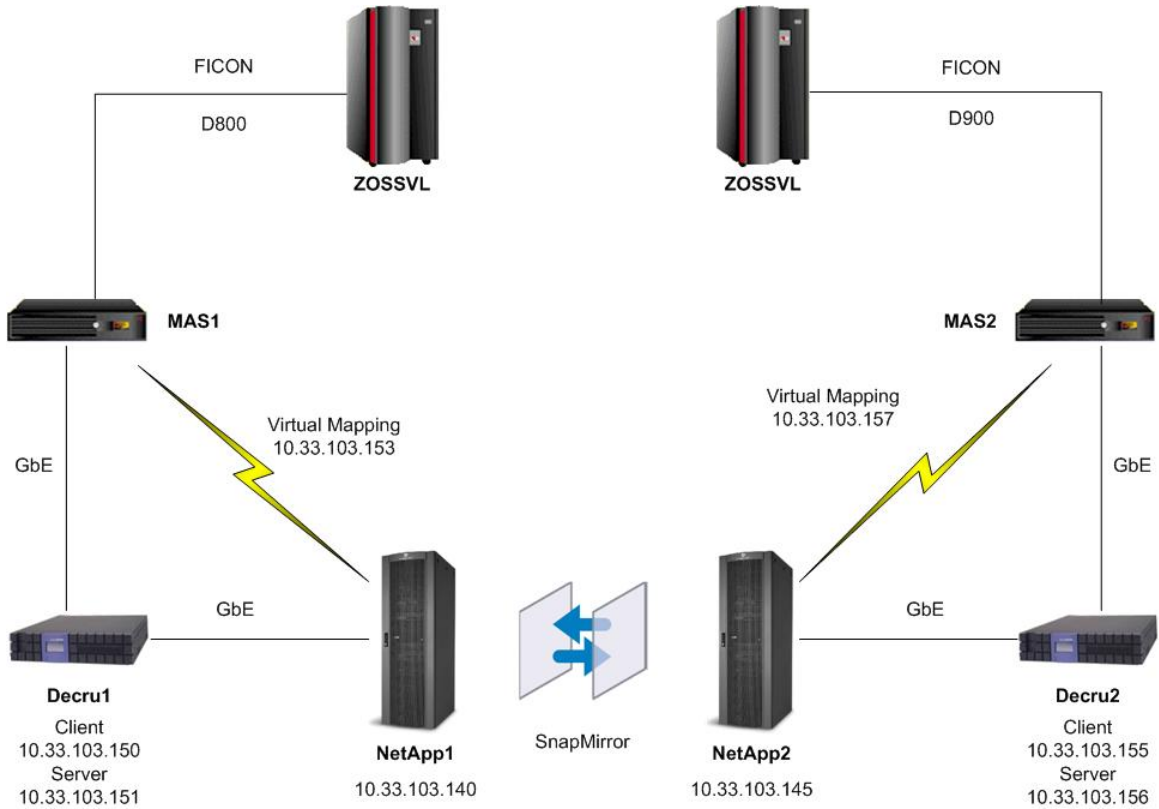


Figure 1) Testing topology

DEMONSTRATION ENVIRONMENT

The demonstration environment attempts to simulate a basic configuration that contains the MAS, NetApp storage, and the DataFort appliance. Additionally, the configuration also simulates a remote site that has a MAS, NetApp storage and a DataFort appliance for hot site backup.

Test Objectives

- Demonstrate that the MAS, NetApp storage, and DataFort configuration is viable.
- Demonstrate a simple hot site recovery using SnapMirror.
- Demonstrate data encryption between the MAS and NetApp storage using Decru DataFort.

DEMONSTRATION CONFIGURATION

DataFort Setup

IP Address Configuration

The Decru DataFort appliance requires at least three IP addresses. The addresses are identified by their connection to the adjacent object. The server-side address facilitates connectivity to the NetApp storage. The client-side address connects the DataFort appliance to the MAS. Finally, the virtual IP (VIP) address is the address that the MAS uses for storage connectivity. The VIP is associated with a virtual host, which can present one or more Cryptainer™ storage vaults, hosted on the NetApp storage system and accessed via NFS.

DataFort Clustering and Key Sharing Options

Decru DataFort appliances can be configured as standalone devices or clustered. In a cluster arrangement, the appliances maintain a heartbeat between them using the client-side storage interfaces. Members of a cluster share keys via an IP Security (IPSec) or Secure Sockets Layer (SSL) tunnel to ensure that unencrypted key material is never passed over an insecure medium. The cluster can be set up in an active-active configuration with each DataFort appliance hosting one or more virtual hosts with their associated IP addresses and Cryptainer storage vaults. Each virtual host is assigned a preferred DataFort appliance to provide some load balancing. If one device fails, all of its virtual hosts will be serviced by the cluster partner.

DataFort appliances can also be cloned, where the entire configuration and keys are transferred manually between devices. The source and destination DataFort appliances do not have to have the same cluster status (clustered vs. nonclustered). This is particularly useful if a small disaster recovery site is maintained with only a single standby DataFort appliance.

Decru Lifetime Key Management™ (LKM) software will assist the security officer in automating key management and configuration storage. LKM is recommended when multiple sites or multiple DataFort clusters are in use.

MAS Setup

New MAS Setup Procedures

The recently announced MAS 2.0 has an updated motherboard with two processors; a new version of the Linux® operating system kernel; a new, easier MAS device setup applet; and an easier method of creating tapelib subdirectories.

The new MAS device setup applet has fewer parameters than the previous version. Also the tedious process of defining a template before adding virtual drive definitions has been streamlined, reducing the amount of time required to set up large numbers of virtual devices.

The creation of subdirectories to the tapelib directory has been automated with a desktop applet that is invoked from the MAS SUSE 9.0 Linux desktop. The applet ensures that a proper naming case standard is enforced and the permissions are properly set.

The MAS was configured with NAS for this test.

An additional Bus-Tech application for the MAS exploits the SnapLock® capabilities of the NetApp FAServer product. This application was not implemented for this test, but can provide WORM capabilities to virtual tape volsers stored on a FAServer volume.

NetApp Storage Setup

There are a few important things to remember when setting up the NetApp volume export permissions. The MAS uses UID 88 and GID 88 for access permissions. The export of the FAServer volume should contain the system and UID for the MAS as added security. Once the export security has been set, only the UID of 88 (TAPE) of the MAS at a certain IP address will be able to access the data on the exported volume.

Volume size is also important. There is no one-to-one correspondence of a tape volser to a FAServer volume. Many tape volsers can reside on an individual FAServer volume. Tape volsers should be associated with specific FAServer volumes that have similar replication requirements. For example, tape volsers that are weekly backups of volumes should be placed on a separate FAServer volume that is mirrored on a weekly schedule, corresponding to the weekly backups. Tape volsers that have a compliance retention period, should be placed on SnapLock volumes for compliance adherence.

The SnapLock feature was not enabled for this demonstration, but can provide compliance-capable volumes on the same FAServer as the regular volumes.

z/OS Setup

The z/OS system the test was performed on already had 3490 tape attached to it. The test MAS devices had FICON adapters installed. The hardware configuration definition (HCD) application would not allow FICON-attached 3480 devices. The simplest solution was to use 3480 format on setup, requiring the use of the Bus-Tech Unit Information Module (UIM). The UIM provides a special control unit definition that will support the virtual drives as 3480 format. The installation of the UIM was very simple and required copying the two Bus-Tech modules to be placed in SYS1.NUCLEUS. No IPL was required.

The HCD control unit definition has a one-byte control unit address. This address is used to identify the control unit in the MAS device setup applet. The IODF created in HCD can be dynamically activated, saving an IPL.

DEMONSTRATE DATA ENCRYPTION BETWEEN THE MAS AND NETAPP STORAGE USING DECRU DATAFORT APPLIANCE

To validate that data was being encrypted between the MAS and FAS3050 using the DataFort appliance, a simple test was performed using multiple IP addresses on the MAS mapped to different mount points. One IP address was the IP address of the FAS3050. The other IP address was the virtual mapping address of the DataFort appliance. The FAS3050 volume was mapped to both mount points.

A test was run that wrote data to the FAS3050 volume mapped to the MAS tapelib encrypted mount point. The data was read from the unencrypted mount point. The data was unreadable. When the data was read from the encrypted mount point, the data was readable.

DEMONSTRATE A SIMPLE HOT SITE RECOVERY USING SNAPMIRROR

A PDS containing text members was written to the MAS using IEBCOPY. The data was encrypted through the DataFort appliance and placed in a virtual tape file residing on the FAS3050. The volume on the FAS3050 was mirrored to a similar volume on the remote FAS3050. Another job was run requesting a mount of the same tape volser from the remote MAS. The data was read in and the text members could be read. Since the mirrored volume is normally read-only while it is in a mirroring state, no overt action on the remote FAS3050 was required. This successfully demonstrated that the DataFort/MAS/FAS3050 combination was capable of encrypting data in place and successfully retrieving and decrypting that same data at a mirrored remote site.

INTEGRATING A DATAFORT APPLIANCE INTO AN EXISTING MAS VIRTUAL TAPE CONFIGURATION

The transparent nature of the DataFort appliance extends to the encryption of existing data. A DataFort appliance can be deployed into existing MAS configurations with very little service interruption to secure existing data. During configuration of the Cryptainer storage vaults for existing NFS-exported directories, the administrator can select the Initial Encryption option, which will encrypt the existing contents of the directory in the Cryptainer storage vault. This encryption job runs as a background process encrypting individual files while all data remains accessible through the DataFort appliance. Once the job is complete, all data in the Cryptainer storage vault is secured, and will be decrypted as required by authorized clients—in this case, the MAS.

CONCLUSION

The Decru DataFort appliance, Bus-Tech MAS, and NetApp FAServer combination provides a simple yet elegant solution for encrypting data at rest. The Decru DataFort appliance seamlessly and transparently encrypts data on the fly, ensuring that the data directed to the MAS from the mainframe tape operation is encrypted on the NetApp FAServer. Because the MAS does not have to rely on a database to identify tape volser objects, the additional overhead of database synchronization between sites is eliminated. The remote MAS simply reads the directory tree to find the desired volser. Additionally, the SnapLock feature of the NetApp FAServer device can provide regulatory compliance for data retention.

