

# Using the HP StorageWorks EBS Data Encryption Solution with the NeoScale CryptoStor Tape Appliance and HP OpenView Storage Data Protector



- Solution overview ..... 2
- Components ..... 2
- About the CryptoStor Tape appliance ..... 3
- CryptoStor Tape appliance configuration ..... 4
- Taking advantage of ETLA with CryptoStor ..... 7
- Creating custom maps ..... 11
- Test configuration ..... 12
- Configuring Data Protector ..... 14
- Test observations ..... 15
- Conclusion ..... 16
- For more information ..... 16

## Solution overview

Protection of data, in the form of backups, has been a part of corporate strategy for years. However, the sensitive nature of corporate data has forced many companies to go to greater lengths to protect their data more stringently. Simply backing up data to tape and storing it offsite is not sufficient. If the tape falls into the wrong hands, a company can be liable if sensitive information is leaked.

As a result, data encryption has come to the forefront as a necessary component of data protection. However, simply incorporating data encryption doesn't solve the problem. In fact, it can cause other headaches, especially when the procedure greatly increases backup windows. The best solution is one in which companies can encrypt the necessary data while inserting the process seamlessly into their current data protection scheme, without adding extra overhead.

The HP StorageWorks Enterprise Backup Solution (EBS) Data Encryption Solution with NeoScale CryptoStor® provides that ability with an easy-to-install, easy-to-manage appliance that encrypts the data as it is written to tape. The appliance can be inserted into an EBS data protection environment with minimal configuration required. The backup application functions without even knowing that the data is being encrypted during backup and decrypted upon restore. All of this is done without impacting data transfer rates to tape, so there is no effect on current backup windows.

All encryption key management is safely maintained via the CryptoStor device, and allows for redundancy as well as disaster recovery. When combined with an HP Enterprise Backup Solution environment running HP OpenView Storage Data Protector™ and including HP tape libraries featuring the Enterprise Tape Library Architecture, customers can take advantage of a well-tested, proven encryption solution to more fully protect their data.

## Components

The HP EBS Data Encryption Solution was tested with the following components:

- HP ProLiant server running Windows 2003
- HP PA-RISC server running HP-UX 11.23
- HP ProLiant Server running RedHat Enterprise Linux 4 (Update 1)
- HP StorageWorks EML E-series tape library with LTO-3 tape drives
- HP StorageWorks Command View for Tape Libraries Software (Command View TL) for EML administration
- EBS-supported SAN infrastructure (B-series 2GB switch fabric, supported HBAs)
- HP OpenView Storage Data Protector 5.5
- NeoScale CryptoStor Tape 700-series encryption devices (System version: fc-2.1.0-Build 12)
- HP StorageWorks EVA5000 and EVA8000 storage arrays (for backup data)
- HP StorageWorks Secure Manager Tape Library Software advanced feature option (recommended)

For this solution, Windows, HP-UX, and RHEL 4 are the supported operating systems.

The key to successfully integrating the CryptoStor device into an EBS data protection environment is the use of the Enterprise Tape Library Architecture (ETLA) features that allow selective LUN presentation via the Command View TL administration interface. Using the Secure Manager feature within Command View TL, individual tape drives within a library can be presented to different backup servers on the SAN, or whole sections of the library can be partitioned, with each partition presented separately. This allows for integration of an encryption solution to certain servers while preserving non-encrypted backup activity in those instances when encryption is unnecessary. This provides flexibility, as well as the ability to integrate additional encryption as needed over time. For more information on the EBS components and their features, visit the HP EBS website at <http://www.hp.com/go/ebs>.

## About the CryptoStor Tape appliance

The NeoScale CryptoStor Tape 700-series appliance compresses, encrypts, and digitally signs data as it is transferred to tape media or virtual tape, without disrupting backup processes. The appliance actually presents the library robot and tape device LUNs to any hosts that would use the library on the SAN, residing between the hosts and the library. The encryption is secured by a key management strategy that allows options for maintaining the encryption keys used to protect the data. Two types of encryption algorithm strategies are recommended:

- **AES256**—the 256-bit Advanced Encryption Standard algorithm (the strongest available and the one recommended for use with this solution)
- **AES128**—the 128-bit AES version

---

**NOTE:**

3DES is an option, but it is not supported with this solution.

---

Keys can either be static (one key is used for all tapes) or dynamic (a new key is generated for each tape), and they can be stored in a catalog on the appliance or can be written to each tape in encrypted form. No keys are transmitted outside the appliance without being encrypted themselves using the system key; therefore, the CryptoStor clustering function can transmit key information between the appliances, and the keys can move to tape fully protected. The system key itself can be protected and backed up in several ways: 1) written to a smart card that comes with the appliance, 2) saved within the appliance itself, or 3) saved to a PC as an encrypted file. This provides the ability to rebuild an appliance and access previously written data. As previously mentioned, a clustered scenario is available for redundancy of the key management and the encryption rules. In lieu of clustering, NeoScale provides a software tool that can decrypt data restored from tape while a replacement is readied. For more information on the appliance and its functionality, refer to the CryptoStor Tape documentation found at <http://www.neoscale.com>.

## CryptoStor Tape appliance configuration

The CryptoStor Tape appliances are configured in a clustered format, which provides redundancy and consistency in terms of encryption rules. The clustering function automatically shares tape keys and policy data to minimize operational impact to restores and to ensure the integrity of data encryption/decryption in the event of appliance failure. If an appliance is unavailable for any reason, a replacement can be quickly authenticated and synchronized as it is added to the existing cluster. In the interim, data paths to tape can be reconfigured through remaining cluster members.

---

**NOTE:**

The clustering capability is not meant to be used as a tape path failover or multi-path-to-tape with this solution. EBS does not support multiple paths to tape devices in its solution configurations.

---

CryptoStor is configured using a browser interface, as shown in Figure 1.

Figure 1: System summary page

The screenshot shows a web browser window displaying the 'CryptoStor™ for Tape Management Console' interface. The browser title is 'CryptoStor for Tape (isis150) - Microsoft Internet Explorer provided by NeoScale'. The address bar shows 'https://192.168.20.150/cgi-bin/nscg'. The page features a navigation menu with tabs for 'Summary', 'General', 'Time', 'FC config', and 'Cluster'. The 'Summary' tab is active, showing 'System Summary (isis150)'. On the left, there is a sidebar with buttons for 'System', 'Storage', 'Keys', 'Users', 'Logs', and 'Config Files'. The main content area displays the following system information:

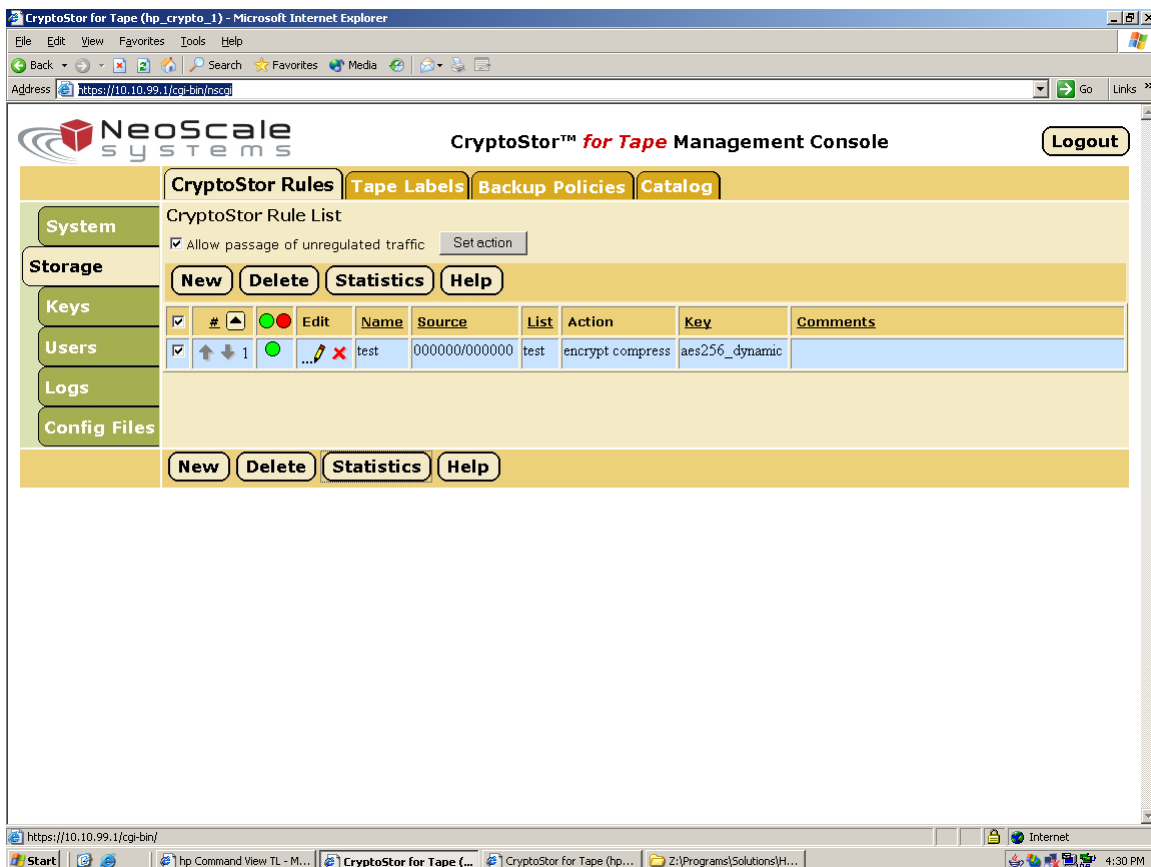
- System**
  - System version: fc-2.1.1-Build1-dev
  - Previous version: fc-2.1.0-Build12-dev
  - Last upgrade: Thu Nov 3 07:58:55 2005
  - User: nsadmin
  - Role: Administrator
  - Security Officer
  - Date and time: Thu Nov 10 15:22:19 2005
  - Time zone: Pacific
  - Uptime: 1 days, 1 hours, 54 minutes, 37 seconds
- FIPS mode of operation:** no
  - Log file capacity: Log file is 0% full
  - Audit file capacity: Audit file is 4% full
- Appliance World Wide Names**
  - Host port WWN: 21:01:00:e0:8b:32:b5:8f
  - Host node WWN: 20:01:00:e0:8b:32:b5:8f
  - Tape port WWN: 21:00:00:e0:8b:12:b5:8f
  - Tape node WWN: 20:00:00:e0:8b:12:b5:8f
- Hardware**
  - Enclosure: OK
  - Fan: OK
  - Top Power Supply: OK
  - Bottom Power Supply: OK
  - Temperature: OK
  - Battery: Battery charged.

At the bottom of the page, there are four buttons: 'Show Targets', 'Restart System', 'Halt System', and 'Help'.

Figure 1 shows the System Summary page, which provides the basic information about the appliance. The Show Targets button, located at the bottom of the screen, allows the user to see a list of the devices currently available to the appliance. This is useful when troubleshooting device discovery issues.

Under the Storage section is the CryptoStor Rules tab, as shown in Figure 2.

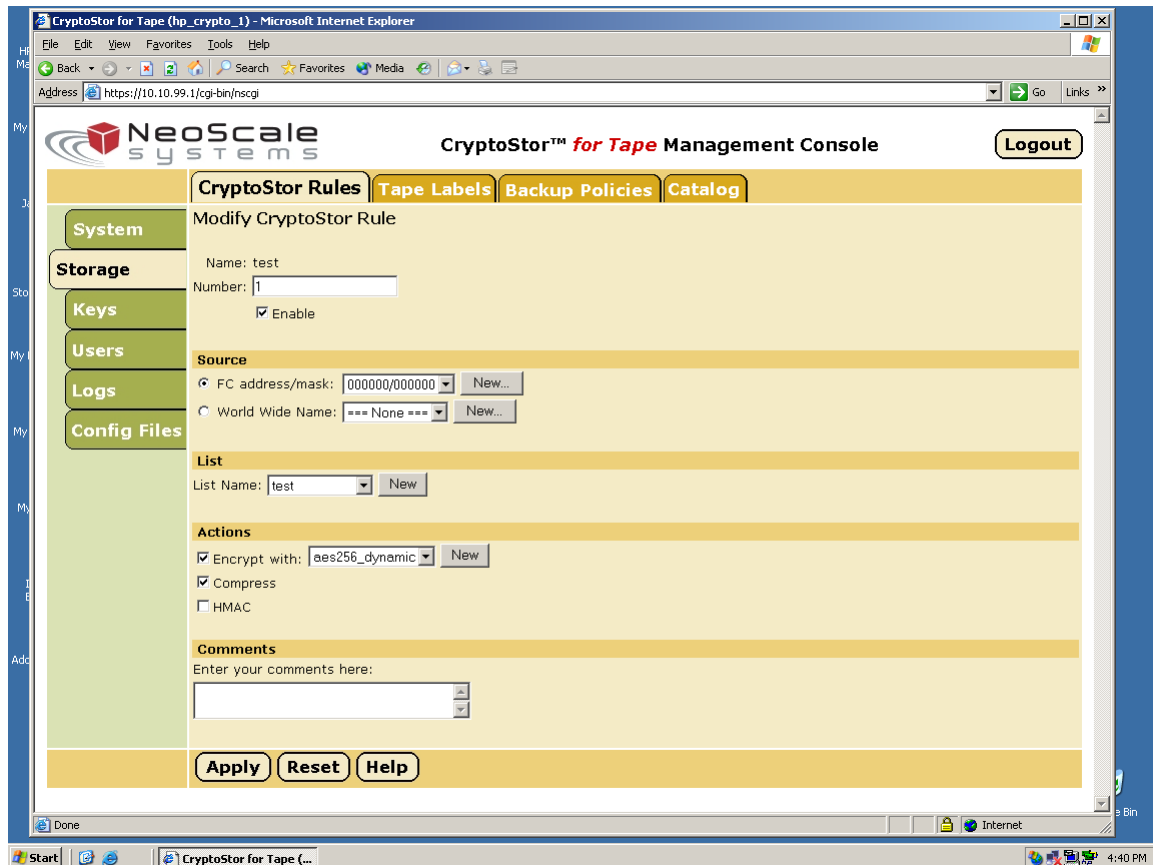
Figure 2: CryptoStor rules tab



The Rules tab is where the encryption rules are created. The **Statistics** button can be used to monitor data throughput statistics, such as read/write speed, compression ratio, and total bytes written to tape or restored from tape. This function is also useful to verify that backup jobs are indeed passing through the CryptoStor Tape appliance and that the data is being protected.

To create an encryption rule, click the **New** button. Figure 3 shows the screen for creating or modifying an encryption rule. From here, the authorized user can enable or disable the rule, designate a particular host (via FC address or World Wide Name) to which this rule will apply, designate a particular destination tape list, and define the actions to be enforced on the data. A CryptoStor user account's ability to perform such tasks is dependent upon its allocated permissions. Different user accounts can be created for different levels of access. For more information, refer to the *CryptoStor Tape Administration Guide*.

Figure 3: Creating or modifying an encryption rule



## Taking advantage of ETLA with CryptoStor

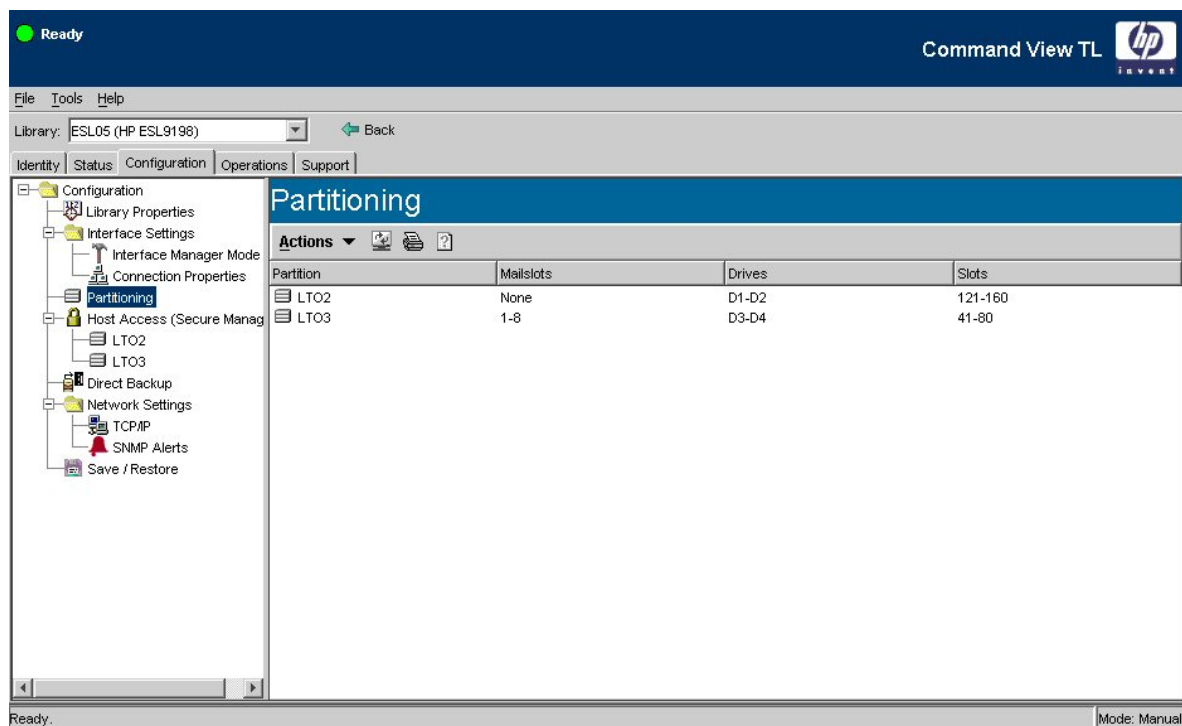
The capabilities provided by the HP StorageWorks Extended Tape Library Architecture (ETLA) via the Command View TL interface are a key feature of this solution with the CryptoStor appliance. The following is an example of how an HP StorageWorks library can have some of its drives segmented for use only through the CryptoStor, while the rest can be reserved for normal data protection. In this scenario, the HP StorageWorks Secure Manager Tape Library Software advanced feature option is required in order to present drives individually.

This configuration requires that the robot and two LTO3 drives be presented to each backup server. The library contains 4 drives: two are LTO2 and two are LTO3. First, partitions must be created within Command View TL to separate the LTO2 and LTO3 drives. To do this:

1. From the CV-TL browser interface, select the library to be managed and click the Configuration tab.

2. Select the *Partitioning* item in the tree view to access the Partitioning screen.
3. Select **Actions > Add Partition**. Two partitions are created: one for the LTO2 drives (named LTO2) and one for the LTO3 drives (named LTO3). The mailslots are assigned to the LTO3 partition, and each partition receives a section of library tape slots.

Figure 4: Partitioning screen



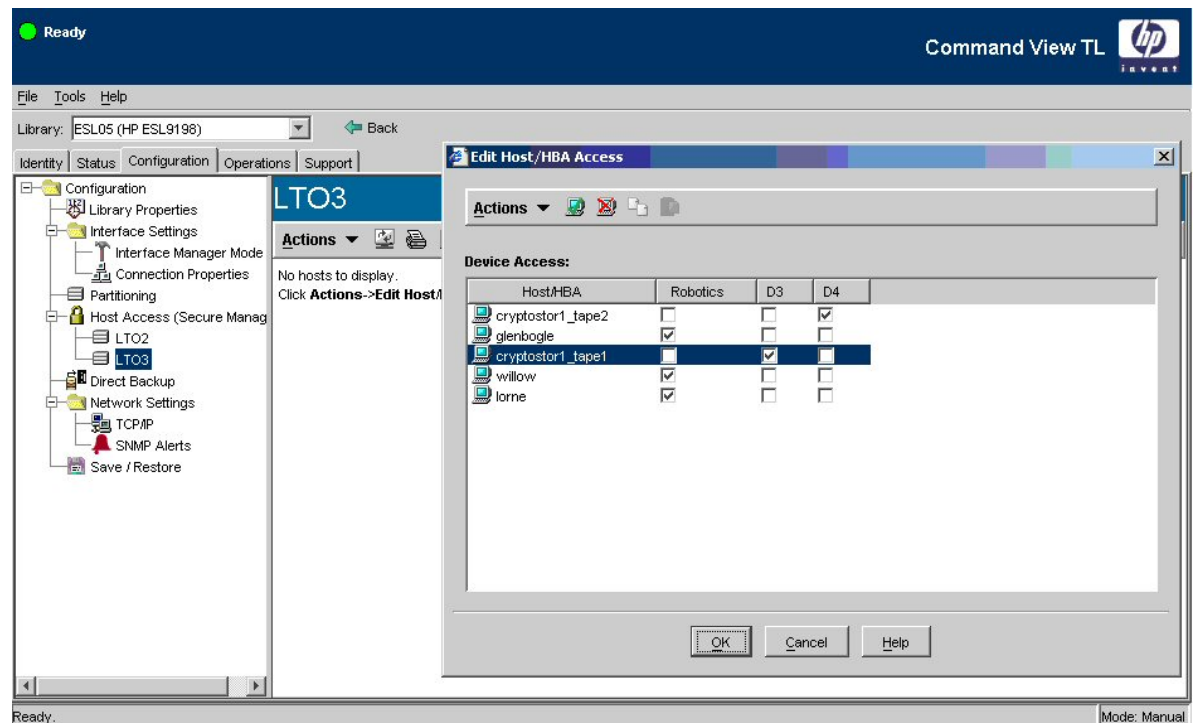
The SAN fabric zoning necessary to present the library devices to hosts and the CryptoStor should now be created. This solution is only supported in a SAN fabric that employs zoning. A separate zone should be created for each CryptoStor tape port, including the tape port World Wide Name (WWN) and the WWNs for the appropriate interface controller ports. In this configuration, each of the LTO3 drives is to be presented out its own interface controller port. Therefore, the first tape port zone will have the WWN of the first CryptoStor tape port and the first interface controller port, while the second tape port zone will have the WWN of the second tape port and second interface controller port.

In addition, zones should be created for the backup hosts that include the WWNs for the host HBAs and the appropriate CryptoStor host ports, as well as the interface controller port on the library through which the robot will be presented. In this case, two 2GB HBAs will be used per server, with each HBA having its own zone with its own CryptoStor host port. This is necessary to preserve maximum available bandwidth in order to take advantage of the LTO3 streaming capabilities. One of the two host zones for each backup host will have the WWN of the interface controller port for the robot. After the zones are established, an HBA rescan should be done on the hosts, and the CryptoStor appliance should be rebooted so that Command View TL will recognize all the appropriate WWNs.

With the two partitions now established, use the Host Access (Secure Manager) section of Command View TL to present the library devices to the SAN as follows:

1. Select the LTO3 partition on the Configuration tab under the Host Access (Secure Manager) section. The Host/HBA Access screen is displayed for that partition.
2. Select **Actions > Edit Host/HBA Access** to open the Edit Host/HBA Access window.
3. In the Edit Host/HBA Access window, select **Actions > Add Known Host/HBA**. The host HBAs and the CryptoStor tape ports should all have WWNs represented in this list.
4. Assign the robot to each host WWN by clicking the Robotics box for each.
5. Assign the first LTO3 drive to the first CryptoStor WWN and the second drive to the second CryptoStor WWN by clicking the appropriate drive box for each.

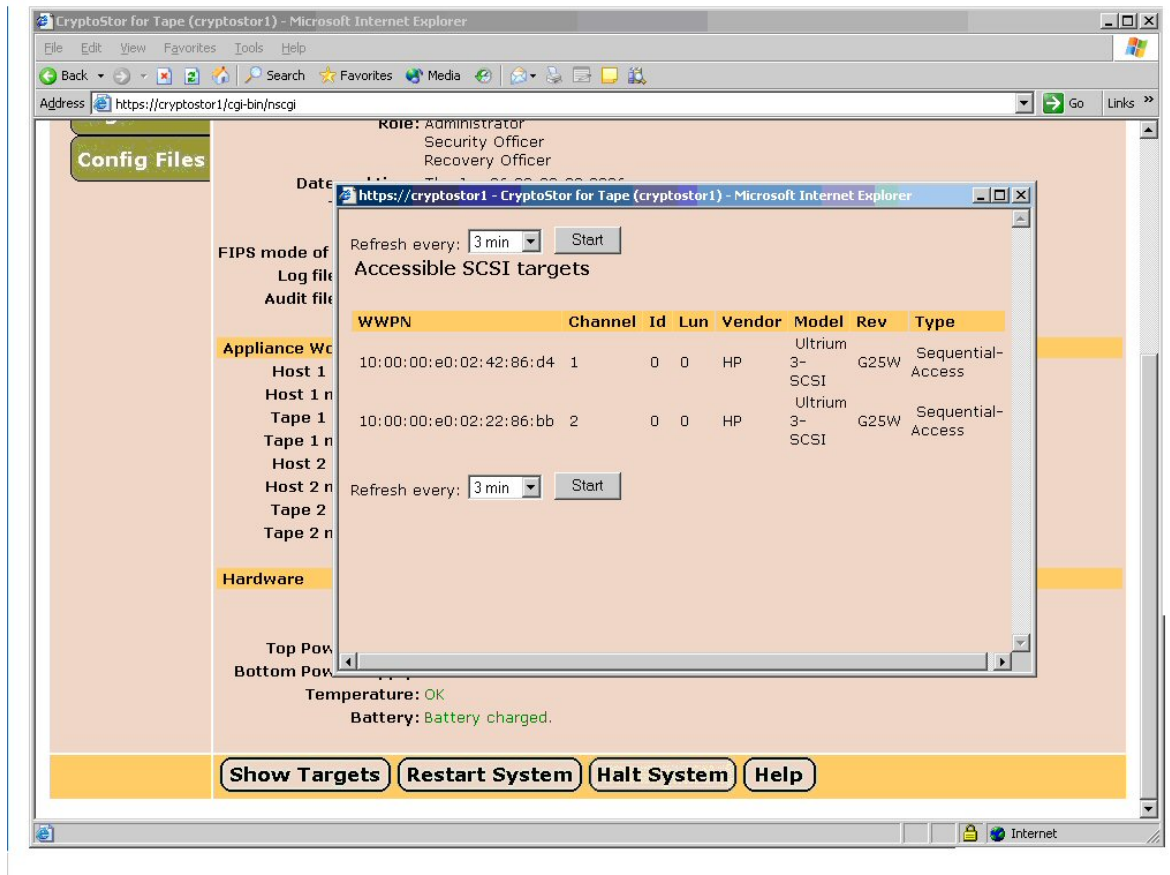
Figure 5: Edit host/HBA access window



At this point, it is necessary to verify that the drives are being presented through separate interface controller ports. To do this:

1. Right-click each of the CryptoStor tape port listings in the Host Access (Secure Manager) window and choose **Edit Custom Device Map**. In this scenario, the first drive is being presented out port 1 on the first interface controller in the library and the second drive is presented out port 0 on the second interface controller. Therefore, in this instance, no custom mapping is necessary.
2. Click **Cancel** at the bottom of the Edit Custom Device Map window to exit without changes.
3. Reboot the CryptoStor appliance and log in to the browser interface.
4. Click **Show Targets** at the bottom of the window to view how the library devices are recognized. If the drives are not presented sequentially, that is, if the drive sequence is interrupted by, for example, a LUN for the interface controller, a custom map or maps must be created in Command View TL to rectify this. See Creating custom maps for more information.
5. Rescan the backup host HBAs to discover the newly available targets.

Figure 6: SCSI targets

**NOTE:**

When configuring an HP StorageWorks tape library using the Command View TL interface, it may be necessary to create a custom device map to present the tape drives to the CryptoStor appliance. Library devices must be presented sequentially to CryptoStor for the backup configuration to function properly. With the default map, the appliance may recognize library interface controllers as LUNs between drive LUNs, which can cause inconsistent backup behavior.

## Creating custom maps

As noted earlier, library devices presented to the CryptoStor appliance must be in order and uninterrupted by other LUNs. If, for example, an interface controller LUN is presented in the middle of the drive LUNs, then a custom map must be created to remove the controller LUN from the listing. Make a note of the LUN for the interface controller for use when the custom map is created.

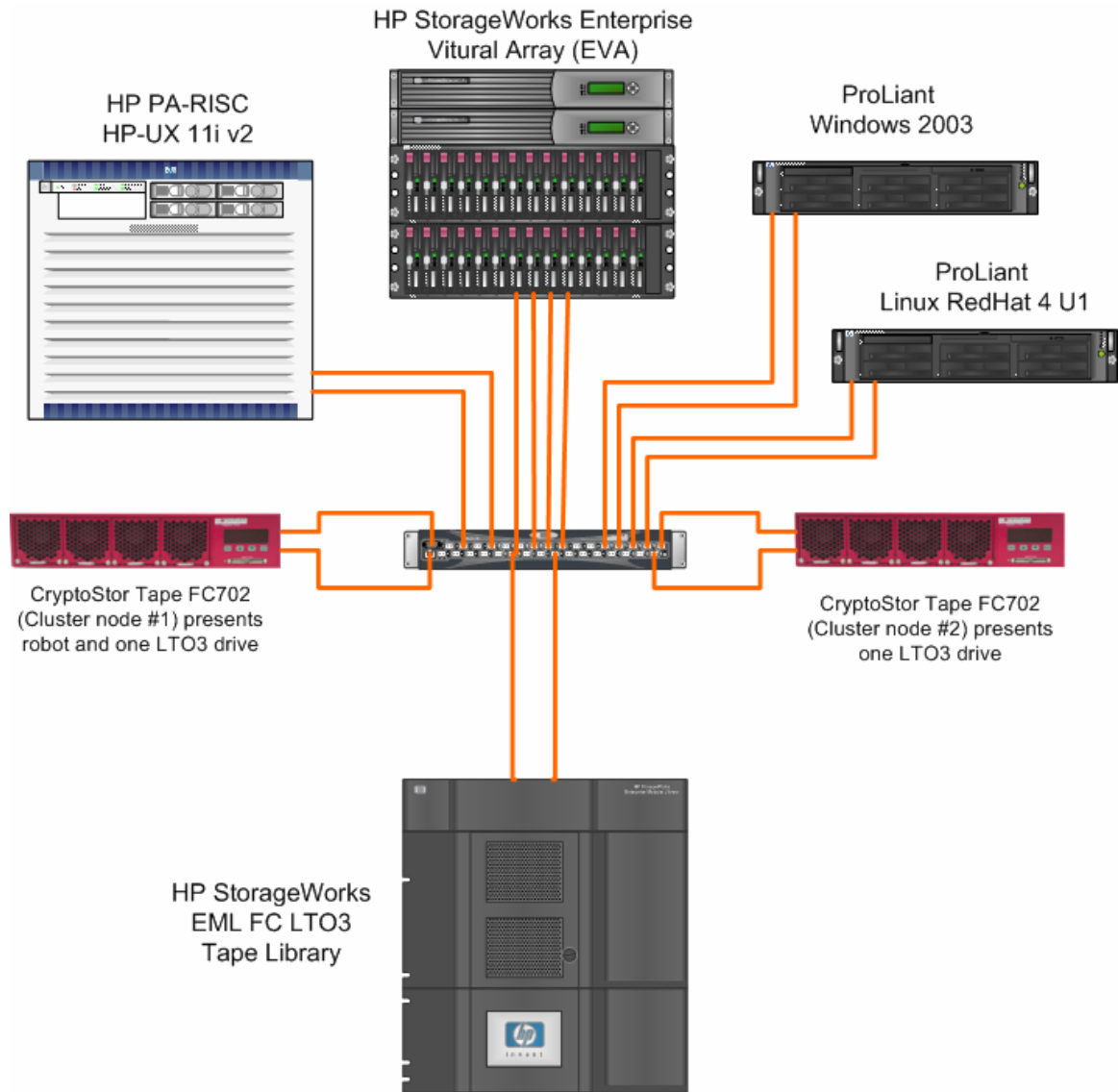
The ability to create a custom map and present it to a specific HBA is a feature of the Advanced Secure Manager and requires additional licensing. The Basic Secure Manager allows a custom map, but it must be presented to all HBAs that access the tape library.

To create a custom map:

1. In the Command View TL browser interface on the Configuration tab, open the Host Access (Secure Manager) window.
2. Select **Actions > Edit Host/HBA Access** and enable access to the CryptoStor World Wide Port Name.
3. Right-click the newly-created CryptoStor listing and select **Edit Custom Device Map**.
4. Alter the LUN listings as necessary to ensure that the interface controller LUN no longer appears between drive LUNs on the CryptoStor interface.
5. Reboot the CryptoStor appliance.

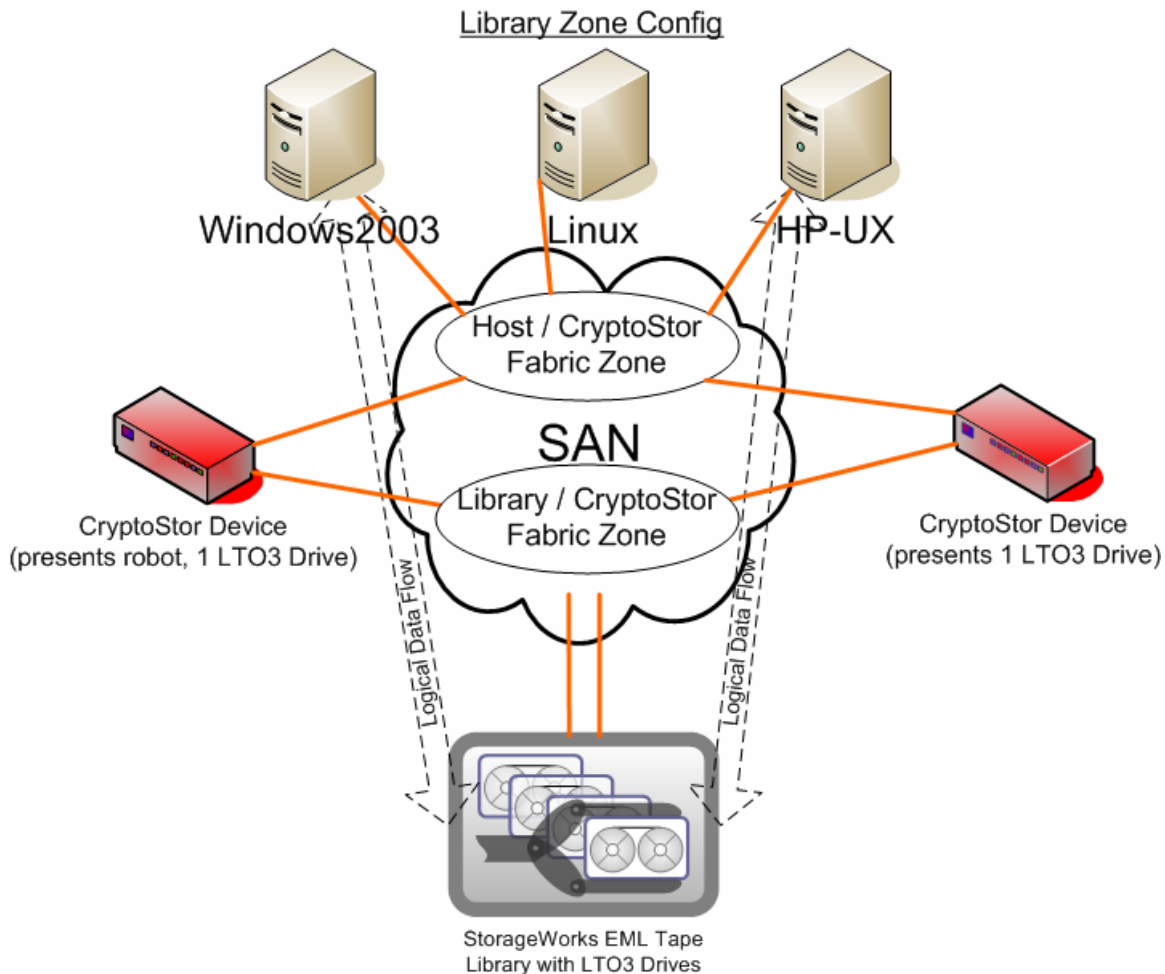
## Test configuration

Figure 7: Test configuration



For test purposes, two NeoScale CryptoStor Tape appliances were used—one for each of the two tape devices in the EML library. The appliances were configured in a clustered format using the CryptoStor clustering function. Each appliance had two Fibre Channel ports: one to be zoned to the backup hosts, and the other to be zoned to the library. The CryptoStor devices reside between the library and the hosts in the SAN, and actually present LUNs to the hosts that represent the robot and drives. With the EML library, Command View TL was used to provide library access to the appliances. The Secure Manager feature of Command View TL was used to present the library robot and one LTO3 drive to one appliance; the other LTO3 drive was presented to the other appliance. In turn, the appliances presented robot and drive LUNs to the Data Protector servers in the backup host fabric zone. Figure 8 shows the zoning configuration used.

Figure 8: Library zone configuration



A single encryption rule was created for use by all servers. The rule designated AES256 as the encryption algorithm, and had both compression and HMAC enabled. When HMAC (*HashMAC*), is enabled, a hash signature is applied to the data stored on tape. This provides an authenticated data integrity check, to ensure that the data written to tape has not been altered.

Data Protector was installed on all three servers, with the Windows server functioning as the Cell Manager. The HP-UX and RHEL 4 servers shared library access using the MultiPath functionality in Data Protector. Each server had data stored on a volume mounted from an HP StorageWorks EVA storage array—either an EVA5000 or an EVA8000. All backup jobs were done using data on these EVA volumes.

## Configuring Data Protector

From within the Data Protector Manager interface, the Autoconfigure Wizard was accessed and set to run for all three servers. The wizard correctly detected the device files for each server. Once the library definitions had been completed, each drive was accessed in order to optimize the settings for better performance. Each drive was configured as follows:

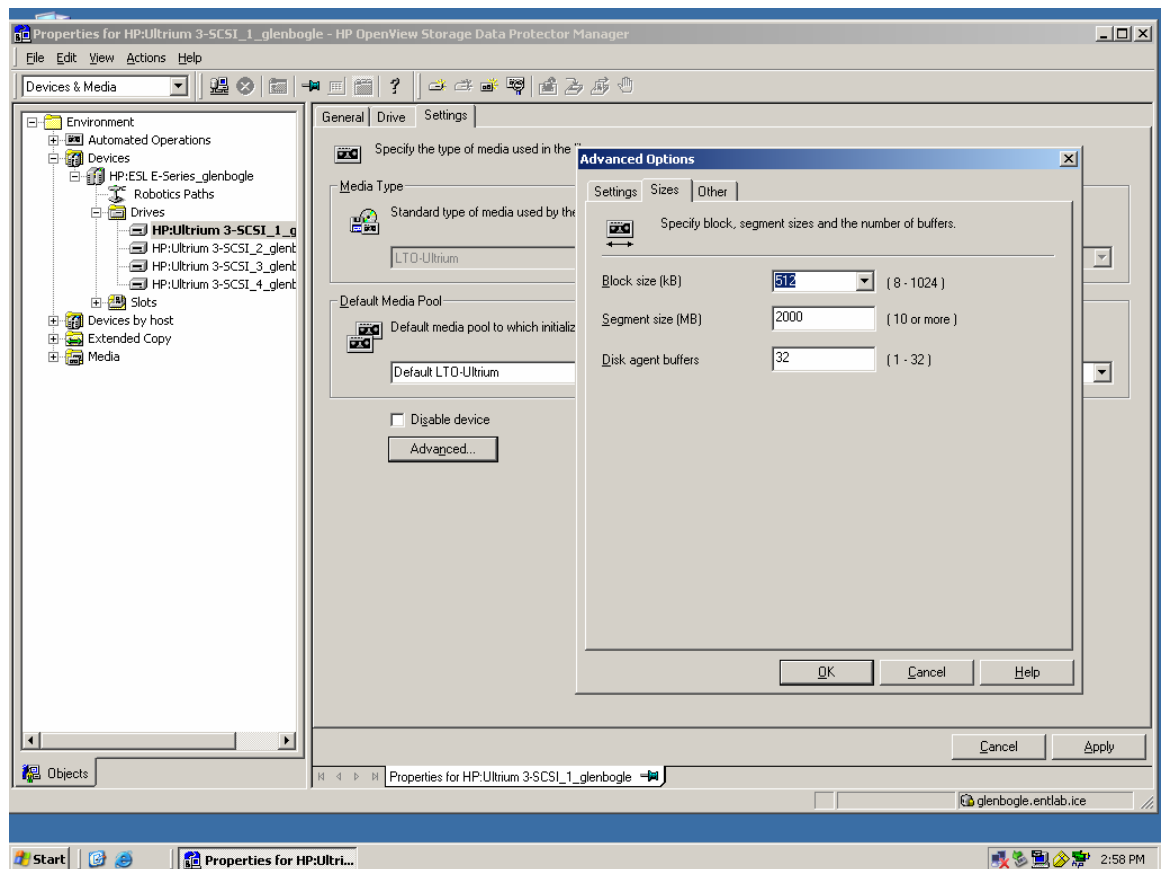
1. In the properties for each drive, click on the Settings tab.
2. Click on the **Advanced** button and then choose the Sizes tab.

The following settings were used:

Block size (KB): 512 (Note: this figure must be manually typed in the window—it is not included in the drop-down list.)

Disk agent buffers: 32

Figure 9 Configuring data protector



The block size was set to match the maximum setting available on the CryptoStor appliance. Both the block size and buffer settings can be adjusted on the appliance by logging into it via SSH with the same security-manager-level user name and password used at the GUI. To show the current settings, enter the following command:

```
sh tapeconfig
```

To change the current block size and/or buffer count, enter the `set tapeconfig` command as follows:

```
set tapeconfig blocksize 524288
set tapeconfig writebuf 32
```

At this point, the library can be inventoried, the tapes labeled, and the backup specifications configured as usual in Data Protector.

---

**NOTE:**

When setting block sizes, be aware of the capacity of the server HBA to handle larger data blocks. Consult the documentation for your HBA and/or the HP StorageWorks EBS Design Guide for further information.

---

## Test observations

One of the key requirements of this solution was the need for simplicity in implementation. The setup of the test configuration confirmed that the CryptoStor appliance could be inserted into an existing Data Protector configuration seamlessly. After the fabric zoning of all the components was complete and the library was presented to the appliances via Command View TL, a simple restart of the appliances was necessary to present the library LUNs to the hosts. After the operating systems were able to create devices for the LUNs, the Data Protector Autoconfiguration Wizard had no problems defining the library and drives for use. At no time were any special accommodations necessary within Data Protector to make use of the library via the CryptoStor Tape appliance.

---

**NOTE**

It is necessary to note that the CryptoStor appliances do not handle dynamic LUN reassignments in the event of a change in device presentation on the SAN. If, for some reason, an event occurs which would alter the presentation order to the OS, a restart of the appliance is required to newly present the changed LUNs. Subsequently, a rescan of the available SCSI devices (using Device Manager in Windows or the `ioscan` command in HP-UX), plus a re-run of the Data Protector Autoconfiguration Wizard, should also be performed.

---

Multiple tests were performed to measure the difference in streaming performance between encrypted and non-encrypted data transfer jobs. In each backup instance, there was no significant difference in transfer rates. In addition, with the encryption process taking place outside the backup server, the processing capability of the server is unaffected.

Restores of encrypted data through the appliance, however, showed a decrease in performance as compared to unencrypted data restores. When planning restore windows, it may be necessary to consider this aspect, along with other factors that affect performance including SAN infrastructure, tape technologies, and data structure.

The compression ability of the appliance was also measured against the compression ability of the tape device. In each test instance, identical 2:1 compressible data compressed equally when done by either the appliance or a tape device outside the encryption configuration.

The CryptoStor appliance has the option to enable or disable compression before encryption. Use the browser interface to set this option. When enabled, the appliance analyzes the incoming data and determines whether or not to compress it before encrypting it. Although HP LTO tape drives are able to detect incoming compressed data and automatically disable compression, the CryptoStor appliance is in front of the drives and automatically disables compression on all drives. This prevents dual compression, which frequently results in data sizes that are larger than the original data.

This solution can be easily inserted into an already existing backup configuration, as the CryptoStor appliance allows for the passing of non-encrypted data. Tapes that have been used previously for non-encrypted backup jobs can be restored through the appliance by checking the Allow passage of unregulated traffic option on the CryptoStor Rules tab.

## Conclusion

The HP StorageWorks EBS Data Encryption Solution provides customers with the ability to implement an encryption policy in a HP Data Protector environment quickly and easily. The NeoScale CryptoStor appliance, in a supported HP EBS data protection configuration, allows implementation without needing to maintain separate equipment for restore of non-encrypted data. Backup windows are unaffected by the encryption process; however, restore performance may be impacted. Furthermore, the investment that customers have already made in library management with Command View TL remains fully available. In fact, the ETLA Secure Manager feature of Command View TL is critical for its ability to separate encrypted and non-encrypted backup environments. Finally, because no alterations or additional administration are required within Data Protector to function with the CryptoStor appliance, customers can enjoy the added security of data encryption without adding to the time and effort necessary to administer their current configurations.

## For more information

<http://www.hp.com/go/ebs>