NetBackup Encryption Options

Click to edit Master subtitle style
Why Encrypt Backups?

- Concentrated amount of data on highly portable backup tapes
- Backup / tape service providers can and do lose data
- Lost backup tapes and potential fraudulent activity have real financial costs
- Public disclosure of data loss impacts your company

---

- The Cost of a Data Breach is 16X than the cost of encryption*
  Gartner analyst Avivah Litan said in a June 2006 research note that data protection is cheaper than a data breach.
  
NetBackup Encryption Option Overview

Integrated with NetBackup

- No additional software, hardware, or training
- Easy to deploy based on existing policies

Encryption applied at source (client) or media server

- Protect heterogeneous clients, applications, or databases
- Mitigates risk at other storage and hardware points

Multiple bit levels and ciphers for encryption

Choose appropriate level of encryption for your needs
Choice Of Encryption Points

Client

LAN

Media Server

SAN

Tape Drive/ Appliance

Choice Of Encryption Points

Client

LAN

Media Server

SAN

Tape Drive/ Appliance

Enterprise Data Protection
NetBackup Encryption Options

**Client Encryption Option (CEO) if…**
- Require data to be encrypted at the source for maximum security
- Have a specific requirement for encrypting a small number of dedicated clients/applications
- Are able to accommodate the performance impact typical with client-based encryption
- Are able to manually track encryption keys
- Require data to be encrypted to disk or tape
- Require encryption strengths other than AES 128-bit or AES 256-bit

**Media Server Encryption Option (MSEO) if …**
- Needs a cost-effective approach to encrypting data that is integrated within the NetBackup policy
- Requires flexibility with both compression and encryption strengths to best customize for environment
- Needs “set it & forget it” key management
- Unable to accommodate client performance impact
## NetBackup Encryption Options

<table>
<thead>
<tr>
<th></th>
<th>Client Encryption Option (CEO)</th>
<th>Media Server Encryption Option (MSEO)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Encryption Strength</strong></td>
<td>DES: 40, 56 &amp; 112 (2 Triple Key DES); AES: 128 &amp; 256; Blowfish 128</td>
<td>AES: 128 &amp; 256</td>
</tr>
<tr>
<td><strong>Compression Option</strong></td>
<td>Uses NetBackup client compression feature</td>
<td>Selectable options: LZRW3, LZO1X &amp; TXT85.ENG</td>
</tr>
<tr>
<td><strong>Encryption Source</strong></td>
<td>Client</td>
<td>Media Server</td>
</tr>
<tr>
<td><strong>Encryption Target</strong></td>
<td>Disk or Tape</td>
<td>Tape</td>
</tr>
<tr>
<td><strong>Management</strong></td>
<td>Administer within NetBackup</td>
<td>Administer within NetBackup</td>
</tr>
<tr>
<td><strong>Key Management</strong></td>
<td>Manual</td>
<td>Automated &amp; Centralized</td>
</tr>
<tr>
<td><strong>Scalability</strong></td>
<td>No logical limit, simply add additional client licenses</td>
<td>Centralized across multiple NetBackup domains, no logical limit</td>
</tr>
<tr>
<td><strong>NetBackup Support</strong></td>
<td>v. 5.1 and v.6.0</td>
<td>v. 5.1 and v.6.0</td>
</tr>
<tr>
<td><strong>Platform Support</strong></td>
<td>Heterogeneous (same as NetBackup)</td>
<td>Heterogeneous (same as NetBackup)</td>
</tr>
</tbody>
</table>
The NetBackup Advantage

• Most Complete
  – Secure data whether at the client or media server
  – Support for hardware alternatives

• Lowest Cost to Buy and Operate
  – Data center components seamlessly integrated into NetBackup and require no backup or recovery process changes
  – Cost efficient data center solution scales without need of separate hardware encryption devices
  – Data can be compressed prior to encryption reducing media consumption and storage costs

• Most Flexible Deployment and Recovery
  – No special purpose hardware required
  – Perfect for multiple DR locations and scenarios
Summary

• **Backup tapes are mobile and therefore vulnerable as they stolen or lost**
• **One backup tape can contain large amounts of proprietary company and customer information**
• **Encrypting backups is quickly becoming a hard requirement**
• **NetBackup provides the most comprehensive approach to protecting backup tapes**
  - Use NetBackup Client Encryption Option for maximum security (encrypts at the source)
  - Use NetBackup’s new Media Server Encryption Option for viable and cost-effective encryption point with “set it and forget it” key management
What is NetBackup Media Server Encryption Option?

- Encryption occurs at the media server
- Integrated within the NetBackup policy
- High-performance parallelized encryption with minimal client impact
- Centrally managed key store for “set it and forget it” key management
- Choice of compression algorithms and encryption strengths
- Supports most common backup configurations

Encryption Strength Options:
- AES 128-bit
- AES 256-bit
Why NetBackup Media Server Encryption Option?

• Simplified Management
  – Administer encryption process within the NetBackup policy
  – No change to backup processes
  – Actively select compression and encryption where it makes sense
  – Centralized across multiple NetBackup domains

• Minimal Performance Impact
  – Parallelized encryption and compression
  – The media server typically has extra CPU cycles
  – Minimal client impact

• Cost Efficient
  – Scales to accommodate complex combinations of media servers
  – No need to procure or support separate hardware encryption devices
  – ~50% cost of appliance solution

• Highly Secure
  – Standards based security
  – Centralized key management
  – Hierarchical key security
  – FIPS compliance
Media Server Encryption Option Architecture

- Master Server
  - NetBackup
  - Store
  - Catalog

- Media Server
  - NetBackup
  - Compression/Encryption Driver
  - Tape Driver

- Tape
MSEO Key Management

- Centralized, No-touch Key Management
  - “Set it and forget it”
  - No need to manually track which key was used for which tape – it’s automatically tracked for you

- Centralized Key Protection
  - Key store backups can be performed with catalog backups
  - Key store backups can be performed separately
Recovery & Disaster Recovery

• Ease of Recovery
  – Encrypted data recovery process is transparent to the end user
  – Encrypted tapes can be imported

• Key Store Protection and Recovery at the DR Site
  – Enables recovery of encrypted backups
  – Cluster and replication support via VCS, SRDF, VVR, etc. (same as NetBackup catalog)

• Software Encryption Provides Flexibility
  – Removes requirement to deploy inline hardware to all recovery sites
MSEO Performance Assumptions

- Encryption will impose system overhead
- To best maintain performance and capacity it is critical to compress data before encrypting
- Because data is encrypted at the media server, client impact negligible
- Media server more I/O bound than CPU-bound
- Minimal impact to backup window