Welcome!

Easy Encryption for Data-At-Rest

January 22, 2016

Mark Grumblatt
Nimble Senior Engineer
Email: mgrumblatt@syssrc.com

Chris Riley
System Source – Director
Email: criley@syssrc.com
During the Webinar…

- Audio – In Presentation Mode until End
- Control Panel
- Grab Tab:
  - Hide The Control Panel
  - Audio Pane:
    - Mute Yourself
    - Switch between Phone and Mic & Speakers
  - View Webinar in Full Screen Mode
- Question Pane
  - Submit written questions
  - Open Q & A at the end
    (please mute when not speaking)
We Hope You are Enjoying Your ‘Virtual’ Lunch Today!

THANKS for your Understanding & Flexibility!

If you DID NOT receive your e-GiftCard – Please Contact Tracey Maranto:
tmaranto@syssrc.com OR 410-771-5544 x4355
System Source & Nimble Storage:

- Nimble Storage Partner since 2011
- 80+ Nimble SAN installations
- Nimble Storage beneficial for:
  - Server Virtualization
  - VDI - Virtual Desktop Infrastructure
  - Microsoft Applications: Exchange, SQL Server & SharePoint
  - Applications requiring high IOPS at lower price point
  - Offsite Backup / Replication
  - Keep storage and applications up and running with frequent snapshots and consistent backups, fast restores, and efficient replication for disaster recovery
Welcome to the System Source – Nimble **Lunch Webinar**

**Today’s Agenda**

- Nimble Data Encryption for IT Compliance
- Technical Details – How it works
- Live Product Demonstration
Nimble SmartSecure
Software Based Encryption

Mark Grumblatt
Sr. Sales Engineer
January 22, 2016
Nimble Data Encryption for IT Compliance
Nimble Data Encryption for IT Compliance

What is SmartSecure?

- Ensures the secrecy of data “at rest” with encryption
  - Uses AES-256-XTS cipher for cryptographic protection of data
  - FIPS 140-2 level 1 certified

- Protects against data threats
  - Theft of entire storage array
  - Theft of disks (HDDs or SSDs)

- Transparent host access to encrypted volumes
  - Data is encrypted at write time when entering the array
  - Data is decrypted at read time when exiting the array
Nimble Data Encryption for IT Compliance

SmartSecure Protects Data at Rest AND Data Transferred During Replication

- Data at Rest Protection
  - Ensures theft or disposal of drives or an entire array does not expose data
  - Protects against data center physical security breach
  - Protects when shipping or transporting an array to a new location
  - Protects data on failed/returned HDD or SSD

- Meets Requirements for data to be encrypted on disk
  - Government Compliance
  - Healthcare Compliance
  - Volume keys are deleted when an encrypted volume is deleted

- Ensures data secrecy on replication streams over a WAN
During the Webinar…

- Audio – In Presentation Mode until End
- Control Panel
- Grab Tab:
  - Hide The Control Panel
  - Audio Pane:
    - Mute Yourself
    - Switch between Phone and Mic & Speakers
  - View Webinar in Full Screen Mode
- Question Pane
  - Submit written questions
  - Open Q & A at the end (please mute when not speaking)
THANKS for your Understanding & Flexibility!

We Hope You are Enjoying Your ‘Virtual’ Lunch Today!

If you DID NOT receive your e-GiftCard – Please Contact Tracey Maranto:

  tmaranto@syssrc.com  OR 410-771-5544 x4355
Great Business Value – Nimble SmartSecure Encryption Benefits:

- No additional cost - Nimble Storage software encryption is included at no charge
- Simple, non-disruptive software upgrade to Nimble OS version 2.3 to enable feature
- Supported on all Nimble Storage arrays
  - Leverages the Intel AES-NI instruction set
  - Best performance on later model CS series arrays (CS300, CS500, CS700)
  - 10 ~ 15% CPU overhead on CS200 series arrays
- Data is encrypted on both HDDs and SSDs
- Nimble Data compression is not affected by encryption (still get data compression)
- Easy to administer & manage
Technical Details – How it works
Technical Details – How it works

- Two Levels of Encryption:
  - Master Passphrase Keys – One time procedure
    ‘combination to the safe'
  - Volume Keys – Automatic when enabled
    ‘individual keys to safe deposit boxes'
Master Passphrase – One Time Procedure – Passphrase is Encrypted

- The Passphrase…
  » In Secure Mode the passphrase must be entered after an array restart or power on
    • In “Secure Mode”, encrypted volumes remain offline and cannot be accessed until the passphrase is entered
    • If the passphrase is not available, the data in the encrypted volumes can’t be accessed
      note: Nimble is working on a feature to allow data to be retrieved if the master passphrase is lost
  » In Available Mode the passphrase may be required
    • If controllers are being swapped during an upgrade process
    • In the rare scenario involving NVRAM loss

- Do not lose the passphrase!
  » The array user must keep track of and maintain the passphrase
  » The passphrase is never stored on disk or SSD within the Nimble Storage array
  » The passphrase is not managed or transmitted to Nimble Storage Technical Support
  » The passphrase is not copied into Email Alerts, SNMP, or Syslog
Technical Data Points

- Master key generation – One-time feature initialization

1) User inputs a passphrase

![Diagram showing the process of master key generation]

- User inputs passphrase
- Passphrase hashed with SHA-256
- 8-64 Character Passphrase
- SHA-256 HASH Generator
- SHA-256 HASH
- 256-Bit Random Data
- OpenSSL Random Number Generator
- 256-Bit Pseudo Random Data
- 256-Bit Master Encryption Key
- AES-256 KeyWrap
- Encrypted Master Key
Technical Details – How it works

Technical Data Points

- Master key generation – One-time feature initialization

1) User inputs a passphrase
2) Generate SHA-256 hash

- 8-64 Character Passphrase
- SHA-256 HASH Generator
- SHA-256 HASH
- 256-Bit Pseudo Random Data
- OpenSSL Random Number Generator
- Encrypted Master Key
Technical Details – How it works

Technical Data Points

- Master key generation – One-time feature initialization

1) User inputs a passphrase
2) Generate SHA-256 hash
3) Seed OpenSSL Random Number Generator
Technical Data Points

- Master key generation – One-time feature initialization

1) User inputs a passphrase
2) Generate SHA-256 hash
3) Seed OpenSSL Random Number Generator
4) Resulting Master Key
Technical Details – How it works

Technical Data Points

- Master key generation – One-time feature initialization

1) User inputs a passphrase
2) Generate SHA-256 hash
3) Seed OpenSSL Random Number Generator
4) Resulting Master Key
5) Encrypt Master Key with AES-256-KeyWrap
Technical Details – How it works

Technical Data Points

- Master key generation – One-time feature initialization

1) User inputs a passphrase
2) Generate SHA-256 hash
3) Seed OpenSSL Random Number Generator
4) Resulting Master Key
5) Encrypt Master Key with AES-256-KeyWrap
6) Encrypted Master Key
Technical Data Points

- Volume Keys – Uses Master Passphrase Key to Encrypt the Volume Keys
  - The encrypted state of a volume is defined at volume creation time
    - Encrypted volumes cannot be “converted” to unencrypted volumes
    - Unencrypted volumes cannot be “converted” to encrypted volumes
  - New encrypted volumes cannot be “converted” to encrypted volumes
  - 256 bits in length
  - Encrypted by the master key using AES-256-KeyWrap
  - Stored in the key table
  - Clones get their own new volume key
  - But also have access to their ancestor’s key to read shared blocks
Technical Data Points

- Volume Key Retrieval

1) Volume keys stored encrypted with AES-256-KeyWrap

<table>
<thead>
<tr>
<th>ID</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Encrypted 256 Bit Key</td>
</tr>
<tr>
<td>8</td>
<td>Encrypted 256 Bit Key</td>
</tr>
<tr>
<td>9</td>
<td>Encrypted 256 Bit Key</td>
</tr>
</tbody>
</table>
Technical Details – How it works

Technical Data Points

- Volume Key Retrieval

1) Volume keys stored encrypted with AES-256-KeyWrap

2) Volume key unencrypted with clear text master key

### Key Table

<table>
<thead>
<tr>
<th>ID</th>
<th>Key</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Encrypted 256 Bit Key</td>
</tr>
<tr>
<td>8</td>
<td>Encrypted 256 Bit Key</td>
</tr>
<tr>
<td>9</td>
<td>Encrypted 256 Bit Key</td>
</tr>
</tbody>
</table>
Technical Data Points

- Volume Key Retrieval

1) Volume keys stored encrypted with AES-256-KeyWrap
2) Volume key unencrypted with clear text master key
3) Clear text volume key used to encrypt writes and to decrypt reads
SmartSecure Live Demonstration
Phone Lines Now Open!

(please ‘mute’ if you are not speaking! Thanks!

Thanks for Participating in Today’s Webinar!

Look for a Survey via Email at 2p today
Fill it Out & We will Send You a
$10 Amazon Gift Card!