Cisco Storage Media Encryption Key Migration from Cisco Key Management Center to RSA Key Manager

What You Will Learn

Cisco® Storage Media Encryption (SME) provides encryption of data at rest for tape drives and virtual tape libraries. The integrated Cisco Key Manager Center (KMC) offers a basic set of key management features. Additionally, Cisco SME offers an option to use an enterprise-class key management solution: RSA Key Manager (RKM) for the Data Center.

Customers can start using RKM at the time of Cisco SME installation, or they can choose to deploy Cisco SME with the integrated Cisco KMC later. If RKM is deployed after Cisco KMC has been used alone, it is necessary to perform an explicit key migration procedure before using RKM with Cisoc SME.

This document describes the procedure for migrating encryption keys, wrap keys, and encryption policy information from Cisco KMC to RKM.

Migration Procedure

Follow the step-by-step procedure below to migrate keys from the Cisco KMC to RKM.

The migration procedure is slightly different if Cisco KMC is using the PostgresSQL database or the Oracle Express database for the key catalog. The documentation clearly states the differences where applicable.

1. Suspend any backup applications and jobs.

   The migration procedure temporarily suspends access to keys, so the execution of backup operations must be suspended until the migration is completed.

2. Back up the key database.

   It is a good practice to back up the key database before performing the migration. The backup procedure should have been previously tested to help ensure the correct restoration of the keys in case any problems arise during migration.

3. Export all volume group keys in the cluster. Each volume group export will generate a separate password-protected file.

   The password-protected files contain the keys to be imported in RKM.

4. Shut down the Cisco Fabric Manager and consequently the Cisco KMC.

   This step prevents any key operation from being performed during migration.

5. Run the appropriate database script from the database administrative console as shown here. These scripts are packaged in Cisco Fabric Manager CD starting SAN-OS Software Release 4.1(1).

   - Key catalog on PostgresSQL:
     - Script: **postgres-kmc-rkm-pre-migrate.sql**
   - Key catalog on Oracle Express:
     - Script: **oracle-kmc-rkm-pre-migrate.sql**

6. Install RKM on the computer allocated for this purpose.

   RKM can be installed and configured separately. RKM should be ready prior to the start of the migration to decrease downtime.

7. Refer to the "Cisco MDS 9000 Family Storage Media Encryption Configuration Guide" to configure the certificates for RKM and identify the two certificate files:
   - sme_rkm_client.jks
   - sme_rkm_trust.jks

8. Copy these two certificate files on the Cisco Fabric Manager Server computer.

   Copy the two files in the certificate store directory. The actual directory is displayed on the Cisco Fabric Manager web client (on the SME tab, choose Key Manager Settings).

Note: The default certificate store (Windows) is at C:\Program Files\Cisco Systems\MDS 9000\conf\cert\.

9. Start Cisco Fabric Manager and consequently Cisco KMC.
10. Specify the new key manager on the Cisco Fabric Manager web client (on the SME tab, choose Key Manager Settings.

    Select RSA as the key manager and configure the IP address and port for RKM.

11. Using the Cisco Fabric Manager web client, monitor the Cisco SME log until the message "Synchronization Complete for Cluster" is displayed.
12. Create and import all volume group keys from the password-protected files.
13. Run the post-migration scripts to delete the keys in the Cisco KMC key database. These scripts are packaged in Cisco Fabric Manager CD starting SAN-OS Software Release 4.1(1).
    - Key catalog previously on PostgresSQL:
      - Script: **postgres-kmc-rkm-post-migrate.sql**
    - Key catalog previously on Oracle Express:
      - Script: **oracle-kmc-rkm-post-migrate.sql**
14. Restart any backup applications and jobs that were deactivated or suspended before the migration.

Migration from Cisco KMC to RKM is now complete.

Note that in Cisco MDS 9000 SAN-OS Software Releases 3.2(3a) and 3.3(1a), import of the volume group leaves all the keys in a deactivated (archived) state, which implies that, after the migration, the tapes can be restored but cannot be used for active encryption.

Cisco MDS 9000 SAN-OS Software Release 4.1(1b) offers a stateful export procedure, and consequently the keys will be restored in the same state (active or archived) as before the migration.

For More Information

For more information about Cisco SME solution, please visit http://www.cisco.com/en/US/products/ps8502/index.html.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Printed in USA C11-508589-00 11/08