



SME Best Practices

This chapter describes SME best practices. You can avoid problems when configuring SME if you observe the best practices described in this chapter.

Overview of Best Practices

Best practices are the recommended steps you should take to ensure the proper operation of SME. We recommend the following best practices for SME configurations:

- [General Practices, page 10-155](#)
- [SME Configuration Practices, page 10-155](#)
- [SME Disk and VAAI or Thin Provisioning Support, page 10-156](#)
- [KMC Practices, page 10-156](#)
- [Fabric Management Practices, page 10-156](#)

General Practices

- Maintain a consistent Cisco NX-OS release across all your Cisco MDS switches.
- Refer to the [“Planning For SME Installation”](#) appendix for preconfiguration information and procedures.
- Enable system message logging. For information on system messages, refer to the *Cisco MDS 9000 Family Troubleshooting Guide*.
- Refer to the release notes for your Cisco SAN-OS or NX-OS release for the latest features, limitations, and caveats.

SME Configuration Practices

- Troubleshoot any new configuration changes after implementing the change.
- Save all configuration changes on all switches in the cluster for correct cluster operation.
- When designing your backup environment, consider that Cisco SAN-OS or NX-OS supports one cluster per switch.

- All IT-nexuses that host paths between the server and storage must be added to the configuration or else the data integrity is at risk.
- For configuration changes to SME tape groups, it is recommended that the backup application is quiesced during the configuration change.
- Refer to the *Cisco Storage Media Encryption Design Guide* for guidelines on sizing and placements of SME interfaces.

SME Disk and VAAI or Thin Provisioning Support

For the SME configuration, VAAI commands and thin provisioning are not supported.

The following VAAI commands are not supported by SME:

- Extended Copy
- Compare and Swap
- Compare and Write
- Write Same
- Unmap

KMC Practices

- As your data storage grows, the number of tape keys will also grow over time. This is especially the case when you select the unique key mode. It is a good practice to store only active keys in the Cisco KMC database.
- To ensure redundancy and availability, it is important to back up your Cisco KMC database regularly.
- The Cisco KMC listens for key updates and retrieves requests from switches on a TCP port. The default port is 8800; however, the port number can be modified in the smeserver.properties file.



Note

For more information, refer to the *Storage Media Encryption Key Management White Paper*.

Fabric Management Practices

Use DCNM-SAN and Device Manager to proactively manage your fabric and detect possible problems before they become critical.



Note

For details on SME sizing and topology guidelines and case studies, refer to the *Cisco Storage Media Encryption Design Guide*.
