12.8.6 Restrictions

The following restrictions apply to encryption:

- Image mode volumes cannot be in encrypted pools.
- You cannot add external non self-encrypting MDisks to encrypted pools unless all control enclosures in the system support encryption.

12.9 Rekeying an encryption-enabled system

Changing the master access key is a security requirement. *Rekeying* is the process of replacing current master access key with a newly generated one. The rekey operation works whether encrypted objects exist. The rekeying operation requires access to a valid copy of the original master access key on an encryption key provider that you plan to rekey. Use the rekey operation according to the schedule defined in your organization's security policy and whenever you suspect that the key might have been compromised.

If you have both USB and key server enabled, rekeying is done separately for each of the providers.

Important: Before you create a master access key, ensure that all nodes are online and that the current master access key is accessible.

No method is available to directly change data encryption keys. If you must change the data encryption key that is used to encrypt data, the only available method is to migrate that data to a new encrypted object (for example, an encrypted child pool). Because the data encryption keys are defined per encrypted object, such migration forces a change of the key that is used to encrypt that data.

12.9.1 Rekeying using a key server

Ensure that all the configured key servers can be reached by the system and that service IPs are configured on all your nodes.

To rekey the master access key kept on the key server provider, complete the following steps:

1. Click **Settings** → **Security** → **Encryption**. Ensure that Encryption Keys shows that all configured SKLM servers are reported as **Accessible**, as shown in Figure 12-82 on page 666. Click **Key Servers** to expand the section.