Luna HSM Cluster Node Setup

Document Information

Namn	Luna HSM Cluster Node Setup
Version	1.0
Editor	Leif Johansson
Date	2014-11-28

Purpose and scope

This procedure ensures that a new Luna HSM is setup as part of a cluster.

Governing policies

This procedure is governed by the following policies:

- SUNET Key Management Policy (SUNET KMP)
- SUNET Asymmetric HSM Service Key Management Practice Statement (SUNET HSM KMPS)

Roles

Number of Persons	Role Name	Responsibilities
1	KCO	Note taking and driving the process (optional)
2	SO	Authenticate to HSM and cloning domain

Summary

This process is related to the “Luna HSM Initialization” process which initializes a Luna HSM along with a set of Blue HSM and Red Cloning Domain PED keys. This process is meant to be run when adding another Luna HSM to the same trust set (eg for the purpose of setting up a HA Group). At the end of the process the HSM is ready to be added to a cluster group. If no KCO is present one of the SOs is responsible for taking notes.

Procedure Steps

Role	Description
KCO	Preparation 1. Boot the appliance and perform basic network configuration to make the appliance ready for setup. 2. (Optionally) register any clients needed to setup the HA Groups.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	**Description**
SO	HSM Initialization Login to HSM appliance. Connect a PED terminal to the PED port (or use a remote PED). Issue the following command at the HSM appliance prompt: **# hsm init -label <name of hsm>** Follow the directions in the PED display. Use the following answers for the Blue and Red PED keyset prompts: **Reuse existing keyset: Yes** **Duplicate keyset: No** When prompted at the PED, insert two blue PED key of the Primary keychain of the two SOs. After this is done choose not to duplicate the keyset. At this point proceed to creating the cloning domain. The cloning domain is created using the same process: first insert each primary Red SO and then choose not to duplicate the keyset. After completing this the HSM terminal prompt should indicate success.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

Role	**Description**
SO	HSM Partition Duplication (optional) For each partition currently in use that is to be member of the cluster, run the following commands **# partition create –partition <name>** **# partition changePw –partition <name> -oldpw <pw> -newpw <newpw>** Do this once for each partition. During partition creation the Black PED key associated with each partition must be used to authenticate to the partition. After each partition is created, change the password to match the password of each partition to match the current password. Remember to set partition policy to allow auto activation and to activate the partitions as appropriate. Record the partitions below. After this step, the new Luna HSM should have a set of duplicated partitions each with the same password as the matching partition in other parts of the cluster. Finally record the serial numbers of the partitions for use when setting up a HA Group (use **partition show** to display serial numbers). Note that clients need to be registered and assigned to partitions before HA Group setup can be completed.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**

<table>
<tr><td><b>Role</b></td><td><b>Description</b></td></tr>
<tr><td>SO</td><td>PED Keyset Safe Deposit
Each SO deposits the primary and backup in separate tamper-evident bags. Each bag is deposited in the SO personal safe storage. Record the serial numbers of each bag below:</td></tr>
<tr><td><b>Completed (yes/no)</b></td><td><b>Notes</b></td></tr>
<tr><td></td><td>SO tamper-evident bag serials
<table><tr><th>SO Name</th><th>Tamper Bag Serial</th></tr><tr><td></td><td></td></tr><tr><td></td><td></td></tr></table></td></tr>
<tr><td><b>Time &Date</b></td><td><b>Signature/Initial</b></td></tr>
<tr><td></td><td></td></tr>
</table>

Role	**Description**
KCO	Finish up Ensure all safe deposit boxes are closed. Close safe, logout from HSM appliance.
Completed (yes/no)	**Notes**
Time &Date	**Signature/Initial**