SafeNet Network HSM 5.3.15

TECHNICAL NOTE

Feature Updates

Contents

007-013432-005 Rev. A Copyright 2001-2017 Gemalto All rights reserved.

Release Description

This appliance software release introduces a fix to correct the representation of partition serial numbers.

Note: Release 5.3.15 accumulates all changes since release 5.3.10, including the features and fixes described below.
This list includes both the new items for 5.3.15 and the features for 5.3.13 and fixes for 5.3.14, because you could be updating from any of version 5.3.10 or version 5.3.13 or version 5.3.14.

Note: If your appliance is not already at version 5.3.10, it must be updated to that version before you can update to this version (5.3.15).

5.3.15

This fix ensures that the representation of partition serial numbers on the Network HSM appliance harmonizes with PKCS #11 and matches the output of the Client-side tools (such as lunacm), and functions with SNMP.

Previously, it was not possible to use client-side scripts to operate against network HSM partitions, based on partition serial numbers obtained from lunash command outputs, when the HSM contained large numbers of managed objects.

The current fix affects the following lunash commands:

- partition list
- partition show
- partition showContents
- partition showPolicies
- hsm supportInfo .
- sysconf appliance reboot
- sysconf appliance poweroff

In addition, for SNMP the partition serial number for Partition table reports the correct value.

As well, the issue is addressed in the application audit log output.

A note about audit log file handling

The Network HSM appliance is not designed for long-term, permanent storage of audit logs. Audit logs from the HSM that accumulate on the file-system should be archived (with command **audit log tarlogs**), and the resulting archive files (audit.tgz) moved off to dedicated storage, elsewhere in your network (use **scp** or **pscp**).

The local copies (on the Network HSM appliance) should then be cleared (with command **audit log clear**) to ensure that the HSM can continue to write log entries to the system's hard disk.

Notwithstanding the fixes from release 5.3.14 (included in 5.3.15), you must ensure that the disk partition that accepts HSM audit logs does not become overfull. If this occurs, log rotation on the HSM can cease, and when the limited space inside the HSM fills, audit logging stops. Whenever the appliance audit log partition usage reaches 79% of the available space, the appliance issues a warning each time a user logs in (admin, audit, etc.) so you know to take action as described above. Pay special attention after you have made any changes to logging behavior (like changing the types of events that are logged), as this can affect the rate at which audit records accumulate.

 Copyright 2001-2017 Gemalto All rights reserved.

Previous (5.3.14)

Log rotation fixes

Several fixes are introduced, relating to the log rotation from the HSM onto the local HSM appliance. The logs were filling the HSM because log rotation was not working.

- Previously, (releases 5.3.9, 5.3.10, and 5.3.13) the upgrade process overwrote a logrotate configuration that pointed to the log file destination. Without a destination, the rotation failed and the log inside the HSM continued to grow. The update process was modified for release 5.3.14 to spare the existing configuration. Log rotation now functions properly, maintaining a small log footprint within the HSM.
- Changes to **audit log logappliance** <set | unset> include:
  - As of release 5.3.14, configuration changes take effect when the "set" or "unset" option is used, with no need to specify "-restart".
  - Previously, it was possible to set multiple log-rotation periods, resulting in confusing behavior. This is now prevented.
- Previously, running **audit log clear** could introduce a state that would prevent logging to the local appliance. This is also fixed.

Signature verification fix.

A separate issue concerning signature verification was discovered and fixed at the same time as the rotation problem.

Previous (5.3.13)

These features from release 5.3.13 are also included in 5.3.14 and 5.3.15, and are listed here in case you are updating directly from version 5.3.10.

NTLS Shutdown on Critical HSM Errors

Error handling is enhanced for HSM failures due to critical conditions. Real-time monitoring ensures that if the HSM (one member of an HA group) experiences a critical error state, NTLS is shut down, causing the affected HSM to exit cleanly from the group. This triggers an HA fail-over condition, allowing the remaining group to resume HA redundancy and load-balancing without penalty. The affected HSM can be serviced off-line when convenient.

Disk Full Errors

Errors related to disk space full are tracked. This includes audit logs and system level logs.This error condition covers both an appliance log full error and firmware log full error. When either condition is met, NTLS is shutdown at the appliance resulting in an HA fail-over for the next cryptographic operation request. We actively monitor for disk full errors returned by the firmware when the audit log full condition is triggered.

Firmware Halted Error

All firmware shutdown/halt errors are monitored. When one is encountered, an NTLS shutdown is triggered. This results in an HA fail-over.

Request Timeout Error

This occurs when the HSM is not handling requests, and is treated similarly to the Critical HSM Device Errors.

 Copyright 2001-2017 Gemalto All rights reserved.

Applicable Products

- SafeNet Network HSM 5.3.15

Upgrade Procedure

Upgrade Paths

The following table demonstrates the supported upgrade paths. If your software or firmware is at a version lower than the indicated starting versions, you must first upgrade them to an indicated version before applying the patch.

Table 1: Upgrade from (path)

Starting Appliance Software and Firmware Version	End Software and Firmware Version
5.3.10 with f/w 6.10.9	5.3.15 with f/w 6.10.9
5.3.10 with f/w 6.20.2	5.3.15 with f/w 6.20.2
5.3.13 with f/w 6.10.9	5.3.15 with f/w 6.10.9
5.3.13 with f/w 6.20.2	5.3.15 with f/w 6.20.2
5.3.14 with f/w 6.10.9	5.3.15 with f/w 6.10.9
5.3.14 with f/w 6.20.2	5.3.15 with f/w 6.20.2

Note: If your appliance is not already at version 5.3.10, it must be updated to that version before you can update to this version (5.3.15).

Upgrade Outcomes

The following table shows how the appliance behaves with different sequences of upgrade and configuration

Start appliance version	Action	Action	End appliance version	Result
5.3.9	Configure local/remote ntls audit logging	Update to 5.3.10 and immediately update to 5.3.15	5.3.15	Remote audit logging works; local logging must be reconfigured
5.3.10	Configure	Update to 5.3.13 and	5.3.15	Local and remote

 Copyright 2001-2017 Gemalto All rights reserved.

Start appliance version	Action	Action	End appliance version	Result
	local/remote ntls audit logging	immediately update to 5.3.15 (*)		logging both work, right away
5.3.10	Configure local/remote ntls audit logging	Update to 5.3.15	5.3.15	Local and remote logging both work, right away
5.3.13	Configure local/remote ntls audit logging	Update to 5.3.15	5.3.15	Local and remote logging both work, right away

(* If local audit logging was configured and working at appliance version 5.3.10, or at 5.3.13 then it continues to work properly after update to 5.3.14 or 5.3.15. Attempting to use previously configured local audit logging after updating to appliance version 5.3.13 causes local logging to fail until reconfigured. So if you configured at 5.3.10 and updated to 5.3.13, then avoid starting local logging until you update again to 5.3.14 or 5.3.15 and it will work properly without reconfiguring.)

Note: The update from 5.3.9 to 5.3.10 interrupts logging only if logging was already configured while the appliance was at 5.3.9.

If you have logging configured and upgrade to version 5.3.10, you can use command **sysconf config factoryreset –service syslog** and then configure local/remote ntls audit logging "fresh" and it will work in 5.3.10.

If you want to avoid the reset, then perform the update to 5.3.10 and the update to 5.3.15 (which fixes the problem by including 5.3.14 fixes) in quick succession.

Future upgrades

Earlier update 5.3.10 installed a modified operating system kernel to the HSM appliance. You will be able to update from this version to any future 5.3.x versions, as they will all include, and require, the newer kernel. Contact Gemalto Support to ensure that any upgrade outside that range is - or can be made - compatible, and has been explicitly tested as an upgrade target. Versions 5.4.0 through early version 6.x appliance software do not include the newer kernel and therefore are not possible upgrade targets without extensive modification and testing.

Preparing your HSMs for Upgrade

Perform the following tasks to prepare your HSM for the upgrade:

1. Ensure that your appliance software, and firmware are at a starting version listed in the "Upgrade Paths" section above.
2. Connect your HSM appliance or host computer to an uninterruptible power supply (UPS), if available. Although this is not a requirement, use of a UPS is strongly recommended to ensure successful completion of all upgrade activities.
3. If the Secure Recovery Key (SRK) on the HSM is enabled, it must be disabled before you can upgrade the HSM firmware. The SRK is an external split of the HSM's Master Tamper Key (MTK) that is imprinted on the purple PED key. When you disable the SRK, the SRV (Secure Recovery Vector) portion of the MTK is returned to the HSM, so that the SRV is no longer external to the HSM. It is only in this state that you can upgrade the HSM firmware. After

 Copyright 2001-2017 Gemalto All rights reserved.

you upgrade the firmware, you can re-enable SRK, if desired, to re-imprint a purple PED key with the SRV.

4. Backup the content of your HSM or HSM partitions to SafeNet Network HSM Backup HSMs (if you have the Backup option).
5. Use your favorite archiving program to untar the archive.
6. Stop all applications and services that are using the HSM.

Upgrading SafeNet Network HSM Software

To upgrade the Luna SA Appliance software to Luna HSM 5.3.15

1. Copy the Luna HSM 5.3.15 appliance package file (.spkg) to the Luna SA appliance you want to upgrade:

Windows	**pscp** <path>\<partnum>**.spkg admin**@<LunaSA_hostname>
Unix/Linux	**scp** <path>/<partnum>**.spkg admin**@<LunaSA_hostname>

2. Stop all client applications that are connected to the Luna SA.

3. At the console, log in to the Luna SA appliance using an admin-level account (the default account is admin).

4. Log in to the Luna SA HSM as the HSM admin user:

   ```
   lunash :> hsm login
   ```

   For Luna SA with PED authentication, the blue PED Key is required.For Luna SA with Password Authentication, you are prompted for the HSM Admin (SO) password.

5. Verify that the upgrade package file that you copied is present (optional):

   ```
   lunash :> package listfile
   ```

6. Verify the upgrade package (optional):

   ```
   lunash :> package verify <partnum>.spkg -authcode <authorization_code>
   ```

   The verification process requires approximately 90 seconds.

7. Install the upgrade package:

   ```
   lunash :> package update <partnum>.spkg -authcode <authorization_code>
   ```

   The installation/upgrade process takes approximately 90 seconds. During that time, a series of messages are displayed that detail the progress of the upgrade. At the end of this process, a message “Software upgrade completed!” is displayed.

8. Restart the Network HSM appliance:

   ```
   lunash :> sysconf appliance reboot
   ```

9. Verify that the upgrade package has been installed:

   ```
   lunash :> hsm show
   ```

 Copyright 2001-2017 Gemalto All rights reserved.

Contact Information

Contact method	Contact	
Phone (Subject to change. An up-to-date list is maintained on the Technical Support Customer Portal)	Global	+1 410-931-7520
	Australia	1800.020.183
	India	000.800.100.4290
	Netherlands	0800.022.2996
	New Zealand	0800.440.359
	Portugal	800.863.499
	Singapore	800.1302.029
	Spain	900.938.717
	Sweden	020.791.028
	Switzerland	0800.564.849
	United Kingdom	0800.056.3158
	United States	(800) 545-6608
Web	https://safenet.gemalto.com	
Technical Support Customer Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Knowledge Base. To create a new account, click the "Register" link at the top of the page. You will need your Customer Identifier number.	

 Copyright 2001-2017 Gemalto All rights reserved.

Appendix

The following is some additional information about the issues and fixes.

The **audit log logappliance** feature logs HSM activity to the appliance file system. This feature processes logs directly, with much less computational expense than the record-verifying **audit log** functions.

Configure Appliance Audit Logging

This example assumes that the HSM Audit role is already enabled.

1. Log into the Network HSM appliance Luna Shell as the appliance "audit" user.

2. Use the **audit log logappliance set** command to enable local and remote logging. If you wish to log locally on the Network HSM file system, include the "-local" option; if you wish to log to a remote system, add include the "-ip" option along with that remote system's IP address.

   For example :

   a. Enable local logging only

   ```
   lunash:>audit log logappliance set -local
   ```

   b. Enable remote logging only

   ```
   lunash:>audit log logappliance set -ip <ip address>
   ```

   c. Enable both local and remote logging

   ```
   lunash:>audit log logappliance set -local -ip <ip address>
   ```

3. Set the desired log rotation period for local logging, for example:

   ```
   lunash:>audit log logappliance rotation -weekly
   ```

4. Display detailed appliance logging setup information, for example where both local and remote logging have been setup and rotation has been set to weekly:

   ```
   lunash:>audit log logappliance show

   Logging to appliance is enabled

   Using Weekly rotation
   Log Forwarding is enabled to
   <ip address>

   Command Result : 0 (Success)
   ```

5. You can use **audit log logappliance unset** command to disable local logging and turn off the remote logging. For example:

   ```
   lunash:>audit log logappliance unset -local
   ```

> **Note:** Using the "set" or "unset" commands triggers a restart of the service. If at least one of the options is in state 'set' after the command completes, it resumes automatically.

 Copyright 2001-2017 Gemalto All rights reserved.

About Remote Logging from the Appliance

Remote log sending from the appliance uses UDP on port 514.

Modifying the protocol or the port is not supported at this time.

Therefore, ensure that port 514 is open in the remote host and that UDP protocol is set by the host.

The format of the log can be modified by the receiving host. Be sure to restart the rsyslog service after the changes have been made.

Use your audit logs

Here is an example of using an applog file that is saved from the HSM into the appliance file system.

- In Luna Shell (lunash):
  - audit log tarlogs
- At the client:

1. Download the SafeNet HSM appliance audit log file, for example:

   ```
   # scp audit@mylunasa:audit-151234.tgz  <location_to_place_file_on_local_computer>
   ```

2. Extract the appliance logs tar file (audit-<serial num>.tgz),

   ```
   # tar -xzvf audit-151234.tgz
   ```

3. Change to the location of the extracted file.

   ```
   # cd 151234/applog_backups
   ```

4. Untar this file and identify the specific applog file that you wish to verify.

5. The applog file is compressed. Gunzip this file

   ```
   # gunzip applog-2017-04-21-1442829661.gz
   ```

6. Use your own log-parsing tools to examine the log for events or anomalies.

Verify the logs

Here is an example of verifying the signature of an applog file.

- In Luna Shell (lunash):
  - audit log tarlogs
- At the client:

1. Download the SafeNet HSM appliance audit log file, for example:

   ```
   # scp audit@mylunasa:audit-151234.tgz  <location_to_place_file_on_local_computer>
   ```

2. Extract the appliance logs tar file (audit-<serial num>.tgz),

   ```
   # tar -xzvf audit-151234.tgz
   ```

3. Change to the location of the extracted file.

   ```
   # cd 151234/applog_backups
   ```

 Copyright 2001-2017 Gemalto All rights reserved.

4. Download the SafeNet HSM appliance NTLS certificate file, for example:

```
# scp admin@mylunasa:server.pem <location_to_place_file_on_local_computer>
```

5. Identify the specific applog file that you wish to verify.

6. The applog file is compressed. Gunzip this file

```
# gunzip applog-2015-09-21-1442829661.gz
```

7. Extract the public key from the NTLS certficate file

```
# openssl x509 -in server.pem -pubkey -noout > pubkey.pem
```

8. Verify the signature of the applog file.

```
# openssl dgst -sha256 -verify pubkey.pem -signature
     applog-2017-04-21-1442829661.sig applog-2017-04-21-1442829661
```

When the last step is performed, to verify the signature, the result is either “Verification OK” or “Verification Failure”. A bug exists for logs created in appliance software versions 5.3.9, 5.3.10, and 5.3.13, where the output can be “Verification Failure”, even when the log is valid. The “Verification Failure” is especially likely if the appliance experiences heavy loads (such as constant high volume of crypto operations). This bug is fixed for logs created in appliance software version 5.3.14 or 5.3.15.

Note: After upgrading to 5.3.15, if logs remain that were created in 5.3.9, 5.3.10, and 5.3.13, signature creation on those logs might still fail, though new logs created on 5.3.15 will pass signature verification.

007-013432-005 Rev. A Copyright 2001-2017 Gemalto All rights reserved.