Customer Advisory for HPE Workload Aware Security for Linux (WASL)

Sep-2019
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Advisory</td>
<td>3</td>
</tr>
<tr>
<td>Recommendation</td>
<td>4</td>
</tr>
<tr>
<td>Detailed Description</td>
<td>4</td>
</tr>
<tr>
<td>Removing the changes done by WASL on SAP HANA Database:</td>
<td>6</td>
</tr>
<tr>
<td>Removing the Encryption related rules from WASL policies:</td>
<td>7</td>
</tr>
</tbody>
</table>
NOTICE
The information in this document, including products and software versions, is current as of the Release Date. This document is subject to change without notice.

Customer Advisory

1. To eliminate the possibility of data loss in SAP HANA database, backup the encryption root keys.

Release Date: 27-Sep-2019

Last Updated: 27-Sep-2019

The HPE Workload Aware Security for Linux (WASL) SAP HANA database policies has rules to protect data at rest and backup. The rules include:

1. Enabling encryption of Data, Redo Logs and backup for System Database (SystemDB) and newly created tenant databases. Following rules are related to this:
   a. Data at rest is encrypted (Rule ID: xccdf_com.hpe.wasl.data_mpersistence_1)
   b. PERSISTENCE_ENCRYPTION_KEYS should be within timeout (Rule ID: xccdf_com.hpe.wasl.data_mpersistence_2)
   c. Redo logs should be encrypted (Rule ID: xccdf_com.hpe.wasl.data_redolog_enable_encryption)
   d. Backup encryption should be enable (Rule ID: xccdf_com.hpe.wasl.data_backup_enable_encryption)
   e. Ensure that initial database data volume encryption is enabled (Rule ID: xccdf_com.hpe.wasl.database_initial_persistence_encryption)
   f. Ensure that initial database redolog encryption is enabled (Rule ID: xccdf_com.hpe.wasl.database_initial_log_encryption)
   g. Ensure that initial database backup encryption is enabled (Rule ID: xccdf_com.hpe.wasl.database_initial_backup_encryption)

2. Checking if the root keys for “Data, Redo Logs, Application and backup” needs to be changed as they might be old or might be initial default root keys set by the vendor. WASL does not remediate these rules i.e. WASL will not create new root keys directly here but expects the SAP HANA Database administrator to create new root keys. Following rules are related to this:
   a. REDO Logs root encryption keys should be changed periodically (Rule ID: xccdf_com.hpe.wasl.data_redolog_root_key_timeout)
   b. Data volume encryption root keys should be changed in regular intervals (Rule ID: xccdf_com.hpe.wasl.data_root_key_datavolume_timeout)
   c. Internal application encryption root keys should be changed in regular intervals (Rule ID: xccdf_com.hpe.wasl.data_root_key_application_timeout)
   d. Backup root encryption keys should be changed periodically (Rule ID: xccdf_com.hpe.wasl.data_backup_root_key_timeout)
   e. Data volume encryption root keys set during installation should be changed (Rule ID: xccdf_com.hpe.wasl.data_root_key_datavolume_default)
   f. Internal application encryption root keys set during installation should be changed (Rule ID: xccdf_com.hpe.wasl.data_root_key_application_default)
   g. Redo logs encryption root keys set during installation should be changed (Rule ID: xccdf_com.hpe.wasl.data_root_key_redologs_default)
   h. Backup encryption root keys set during installation should be changed (Rule ID: xccdf_com.hpe.wasl.data_root_key_backup_default)

3. Checking if master keys of Instance Secure Store in the File System (SSFS) and System PKI (Public Key Infrastructure) SSFS needs to be changed as they might be old or might be initial default master keys set by the vendor. WASL does not remediate this i.e. WASL will not change the master keys but expects the SAP HANA Database administrator to set new master keys. Following rules are related to this:
a. Master Keys set during installation is changed (Rule ID: xccdf_com.hpe.wasl.data_ssfs_master_2)
b. Change SSFS master key periodically (Rule ID: xccdf_com.hpe.wasl.data_ssfs_master_3)
c. Initial default master key that protects the system PKI SSFS is changed (Rule ID:
   xccdf_com.hpe.wasl.data_ssfs_pki_2)
d. Change PKI SSFS master key periodically (Rule ID: xccdf_com.hpe.wasl.data_ssfs_pki_3)

**Recommendation**

The encryption root keys for both the system database and all the tenant databases should be backed up during initial installation and every time there is a change or addition of root keys.

The change or addition of the root keys can happen, under scenarios like creation of new tenant database, manually changing the root keys, etc;

**Note:** It is recommended to test the encryption settings in the SAP HANA test environments before enabling in production. Testing is highly recommended for backup and recovery operations (on two different systems) as well as testing disaster recovery capability.

**Detailed Description**

The above mentioned rules refers to following sections of SAP HANA Security or Administrator guides. Refer to these guides on SAP HANA portal for more details on each rule and necessary actions:

- **SAP HANA Security Guide**
  - Data and Log Volume Encryption
  - Backup Encryption

- **SAP HANA Administrator Guide**
  - Managing Data Encryption in SAP HANA
  - SAP HANA Backup Encryption
  - Change Encryption Root Keys
  - Change the SSFS Master Keys

As explained in these sections, it is critical to perform a regular backup of all the encryption root keys (BACKUP, PERSISTENCE, LOG, DPAPI/APPLICATION keys). The backup of all the root keys is critical in the recovery of a SAP HANA database, incase of a database failure. This requirement becomes more critical when the encryption features of SAP HANA are enabled, as there is a chance of data becoming irrecoverable unless you have a root keys backup. The encryption root keys for both the system database and all the tenant databases should be backed up during initial installation and every time there is a change or addition of root keys. The change or addition of the root keys can happen, under scenarios like creation of new tenant database, manually changing the root keys, etc;

**SAP HANA 2.0**

On SAP HANA 2.0 version, the sections “Change Encryption Root Keys”, “Back Up Root Keys”; and “Set the Root Key Backup Password” of “SAP HANA Administrator Guide” provides the detailed steps to perform the root key backup. The steps include:

a. Identify the database IDs (dbid) of the systemDB and the tenant databases

b. Set the “Root Key Backup Password” by the “ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD <passphrase>” SQL statement on the systemDB and all the tenant databases.

**Note:** These root keys backup passwords need to be remembered and should be provided during the restoration of the database.

c. Perform a backup of the root keys for all types of root keys of all databases (SystemDB and all tenant databases) by running command "./hdbnsutil -backupRootKeys <filename>.rkb --dbid=dbid --type=ALL" multiple times for each database (Here dbid is the database ID and <filename>.rkb is the destination file name having backed up root keys).

**Example:**
d. Securely store all the root keys backup files, so that they are available in a disaster recovery situation. Also ensure that all the "Root Key Backup Password" of each of the databases is remembered, which are needed during the restoration.

e. You can also verify all the root key backed up files by running the command:

```
./hdbnsutil -validateRootKeysBackup <filename> [--password=<passphrase>] -printMetaData
```

Example:

```
seqadm@linux-system:/usr/sap/SEQ/HDB00/exe> ./hdbnsutil -validateRootKeysBackup
/usr/sap/SEQ/home/SampleSystemDB.rkb --password=sample12345_ABC --printMetaData
Backup Version: 1 Backup Creation Date: -------------------
Printing Root Key Metadata for dbid: 1

<table>
<thead>
<tr>
<th>Key Purpose</th>
<th>Key Version</th>
<th>Key State</th>
<th>Key Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKUP</td>
<td>0</td>
<td>Deactivated</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>BACKUP</td>
<td>1</td>
<td>Deactivated</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>BACKUP</td>
<td>2</td>
<td>Active</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>BACKUP</td>
<td>3</td>
<td>Preactive</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>DPAPI</td>
<td>0</td>
<td>Active</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>Active</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
<tr>
<td>PERSISTENCE</td>
<td>0</td>
<td>Active</td>
<td>0000000000000000000000000000000000000000000000000000000000000000</td>
</tr>
</tbody>
</table>

Total number of Root Keys in backup file: 7
Successfully validated the backup file /usr/sap/SEQ/home/SampleSystemDB.rkb done.
```

f. You can also compare by printing the contents of the current Root keys in instance SSFS by running the command from time to time:
Example:

```
$hdbnutil -printHashedRootKeys --dbid=<dbid> --verbose
```

Example:

```
seqadm@linux-system:/usr/sap/SEQ/HDB00/exe> ./hdbnutil -printHashedRootKeys --dbid=1 --verbose
Printing all Key(s) for DBID: 1

<table>
<thead>
<tr>
<th>Key Purpose</th>
<th>Key Version</th>
<th>Key State</th>
<th>Key Hash</th>
</tr>
</thead>
<tbody>
<tr>
<td>BACKUP</td>
<td>0</td>
<td>Deactivated</td>
<td>b56e8df45048a22d37b769bf77ceb98124e14bf71db7e6000199ba6f36dc5b</td>
</tr>
<tr>
<td>BACKUP</td>
<td>1</td>
<td>Deactivated</td>
<td>078d24d3428da50358ec5cc87560d0aba32e6f568146e06f55560759bc208b46</td>
</tr>
<tr>
<td>BACKUP</td>
<td>2</td>
<td>Active</td>
<td>8d93e7d35c556b28a33699cff1c220c7ba75566c2fba84637c2730636b121191</td>
</tr>
<tr>
<td>BACKUP</td>
<td>3</td>
<td>Preactive</td>
<td>06988410ab567a22df1c08696bd5c39f21760cee2b30fd436bf8eac04f80095a</td>
</tr>
<tr>
<td>DAPI</td>
<td>0</td>
<td>Active</td>
<td>1bf0a2b1c8f71fe3fccc4f3d2eb8b85fc25f74a86de3994b0c31078374954a1</td>
</tr>
<tr>
<td>LOG</td>
<td>0</td>
<td>Active</td>
<td>eb8ba427cb48dce5652807f551bec4f2c6102c52d03b83a8d5307dd216df4fb2</td>
</tr>
<tr>
<td>PERSISTENCE</td>
<td>0</td>
<td>Active</td>
<td>14743ca6d6737082937796e44b46d3f54b076dd7dadae1d82b2b401da6b79bd</td>
</tr>
</tbody>
</table>
```

done.

g. You can refer to the above mentioned sections in the SAP HANA Security and Administrator guides and also SAP Note “2444090 - FAQ: SAP HANA Backup Encryption” to get more information.

**SAP HANA 1.0**
On SAP HANA 1.0 version, the commands mentioned above will not work. For backing up the root keys you can take a backup of the SSFS file and key file directly. Refer to SAP Note: “2524649 - Backup Encryption Root Key” for details.

**Note:** It is also recommended to test the encryption settings in your SAP HANA test environments before moving to production. Testing is highly recommended for backup and recovery (into different system) operations as well as testing disaster recovery capability.

**Removing the changes done by WASL on SAP HANA Database:**
In case, you wish to remove the changes done by WASL remediation on the SAP HANA Database, you can perform the following steps:
a. Take a backup of encryption root keys and remember the “Root Key Backup Password” as explained in the earlier sections of this document

b. Take a complete backup of the SAP HANA Database

c. Perform a rollback of the Workload in WASL using the WASL SAP HANA policy you have used to perform a remediation earlier. The “Rollback last Remediation operation on Workload” section in “WASL User Guide” (https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=WASL) has information and screenshots on how to do this.

d. If you are using “SAP HANA 2.0 SPS03” version of the database and the WASL SAP policies used for remediation is based on “SAP HANA 2.0 DB Security Level 1 - update 1” or “SAP HANA 2.0 DB Security Level 2 - update 1”, then any new Tenant database created after remediation will have Data, Redo Log and Backup encryption enabled. This encryption will not be disabled by the rollback of the Workload in WASL. To disable the Data, Redo Log and Backup encryption of these Tenant databases follow the “Disable Data Encryption” section in SAP HANA Administrator Guide.

e. Disabling/Enabling the “Data Volume” encryption will take time and you can monitor the progress in SAP HANA Studio.

f. Perform a complete backup of the SAP HANA Database, as some of the delta backups and log backups might still be encrypted.

Removing the Encryption related rules from WASL policies:

In case, the encryption rules for data, log and backup need to be disabled, custom SAP HANA policies can be created from the default policies and deployed in the environment in the place of the default policy. You can use the customized policy for the subsequent WASL operations.

Note 1: Taking a backup of your encryption root keys and remembering the “Root Key Backup Password” as explained in the earlier sections of this document is still recommended even if Data Encryption related rules are removed in your WASL policy.

Note 2: Removing the Encryption related rules from WASL policies will not decrypt or change settings on a SAP HANA Database. If an earlier remediation was performed using WASL SAP HANA policies, you can revert it back by following the steps in “Removing the changes done by WASL on SAP HANA Database” section above.

Following are the steps to create custom policy and remove Data Encryption related rules:

a. Customize the Policy which you are using:


2. While editing the Tailoring file using a text editor, identify the following rules in the tailoring file:
   - xccdf_com.hpe.wasl.data_mpersistence_1
   - xccdf_com.hpe.wasl.data_mpersistence_2
   - xccdf_com.hpe.wasl.data_redolog_enable_encryption
   - xccdf_com.hpe.wasl.data_backup_enable_encryption
   - xccdf_com.hpe.wasl.database_initial_persistence_encryption
   - xccdf_com.hpe.wasl.database_initial_log_encryption
   - xccdf_com.hpe.wasl.database_initial_backup_encryption
   - xccdf_com.hpe.wasl.data_redolog_root_key_timeout
   - xccdf_com.hpe.wasl.data_root_key_datavolume_timeout
3. For every rule that is identified, change the ‘selected’ attribute from selected="true" to selected="false". A sample to disable "xccdf_com.hpe.wasl.data_mpersistence_1" is as follows:

   Change:
   
   <refine-rule idref="xccdf_com.hpe.wasl.data_mpersistence_1" weight="1" />
   <select idref="xccdf_com.hpe.wasl.data_mpersistence_1" selected="true" />

   To:
   
   <refine-rule idref="xccdf_com.hpe.wasl.data_mpersistence_1" weight="1" />
   <select idref="xccdf_com.hpe.wasl.data_mpersistence_1" selected="false" />

4. After editing the tailoring file, reload the custom policy in WASL SMS GUI and enable the policy (Screen shots are provided in WASL “User Guide”).

b. Undeploy your current SAP HANA Database policy and deploy the new customized policy on all the SAP HANA workload instances.


Other Information:
In For information related to support and other Information, refer to the “Support and other resources” section of WASL Release notes at https://h20392.www2.hpe.com/portal/swdepot/displayProductInfo.do?productNumber=WASL.