

[SAP Community](#) > [Products and Technology](#) > [Technology](#) > [Technology Blogs by Members](#)> [SAP HANA Database Encryption](#)

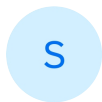
Technology Blogs by Members

Explore a vibrant mix of technical expertise, industry insights, and tech buzz in member blogs covering SAP products, technology, and events. Get in the mix!

Blog

*What are you looking for today?*

SAP HANA Database Encryption

**saroopreddy88**

Explorer



2022 Nov 18 8:26 PM



9 Kudos

41,749

SAP Managed Tags: SAP HANA, platform edition

SAP HANA ENCRYPTION

INTRODUCTION

9.5

SAP HANA provides full support for data-at-rest encryption to secure your data.

SAP HANA is an in-memory database, and most of the data is in the main memory for maximum performance. This helps in processing large data at a very high speed with less administrative effort. However, data is automatically saved from memory to disk at regularly to ensure that the database can be restored to its most recent committed state. Here, all data changes are also captured in redo log entries.

DATA VOLUME ENCRYPTION 9.7

Data volume encryption is available from SAP HANA 1.0 SP12. This protects the data area on the disk, i.e., all the data that resides under /hana/data/<SID>

This encryption uses AES-256-CBC Algorithm and 256-bit page encryption keys to

encrypt and decrypt the data.

As shown here, data is encrypted while it is being saved on to the disk, and it is decrypted when it is being loaded into the memory.



LOG VOLUME ENCRYPTION

9.7

Redo log encryption protects the log area i.e., the logs that are created under `/hana/log/SID`.

This feature is available only from HANA 2.0 SP00.

Like data volume encryption, log volume encryption also uses AES-256-CBC Algorithm and 256-bit page encryption keys.

BACKUP ENCRYPTION

9.8

This feature is available from HANA 2.0 SP01. Backup encryption protects the contents of data backup, log backups and delta/ differential backups which includes snapshot backups as well. Backup encryption can be enabled for both backups written to the file system or backup written to the third-party backup tool through backint for SAP HANA interface.

9.8

A third-party backup tool can also be used, in this case, you have a choice between SAP HANA Encryption or tool-side backup encryption. If full protection in the persistence layer is required, SAP recommends that you use all the three backups.

KEYS USED IN SAP HANA ENCRYPTION

1. Instance SSFS Master Key
2. PKI SSFS Key.
3. Data Volume Root Key

4. Log Volume Root Key

5. Backup Volume Root Key

HOW TO ENABLE AND DISABLE ENCRYPTION?

There are two ways in which you can enable and disable encryption, one is through SAP HANA Studio by use of various SQL commands or statements. The other option is to do it through SAP HANA COCKPIT.

Enable and Disable Encryption using SAP HANA Studio

Stop your HANA DB.

SAP HANA provides two keys with installation which are

1. SSFS Keys à These keys reside in `/hana/shared/<SID>/global/hdb/security/ssfs`. These instance SSFS keys helps in protecting the root keys used for all data-at-rest encryption services and the internal application encryption service.
2. PKI SSFS à system PKI SSFS helps protect system-internal root certificates required for secure internal communication. These keys can be found under `/usr/sap/<SID>/SYS/global/security/rsecssfs/`.

If your HANA DB is pre-installed or delivered by any partner, then SAP recommends to change the master keys that are created during installation.

1. Encrypt SSFS Keys:

Take a backup of existing SSFS keys which will be at `/hana/shared/<SID>/global/hdb/security`

```
root@hana1:~# HDB:saradm /usr/sap/SAR/SYS/global/hdb/security 8> ls -ltr
total 8
drwx----- 2 saradm sapsys 4096 Jul 17 13:23 vsi
drwx----- 2 saradm sapsys 4096 Jul 17 13:29 ssfs
```

Switch to sidadm at OS level and execute below commands

```
export RSEC_SSFS_DATAPATH=/usr/sap/SAR/SYS/global/hdb/security/ssfs
```

```
export RSEC_SSFS_KEYPATH=/usr/sap/SAR/SYS/global/hdb/security/ssfs
```

```
paradm@US11TC041133:/usr/sap/SAR/HDB00> export RSEC_SSFS_DATAPATH=/usr/sap/SAR/SYS/global/hdb/security/ssfs
paradm@US11TC041133:/usr/sap/SAR/HDB00> export RSEC_SSFS_KEYPATH=/usr/sap/SAR/SYS/global/hdb/security/ssfs
```

```
rsecssfx changekey $(rsecssfx generatekey -getPlainValueToConsole)
```

```
paradm@US11TC041133:/usr/sap/SAR/HDB00> rsecssfx changekey $(rsecssfx generatekey -getPlainValueToConsole)
Record Statistics
=====
Encrypted and readable           : 8
Encrypted and not readable      : 0
Plaintext                       : 8
Removed by compacting           : 0
```

Go to path /usr/sap/SAR/SYS/global/hdb/custom/config and add below lines in global.ini file.

```
ssfs_key_file_path = /usr/sap/SAR/SYS/global/hdb/security/ssfs
```

```
paradm@US11TC041133:/usr/sap/SAR/SYS/global/hdb/custom/config> more global.ini

[system_information]
usage=test

[multidb]
mode=multidb
database_isolation=low

[persistence]
basepath_datavolumes=/hana/data/SAR
basepath_logvolumes=/hana/log/SAR

[cryptography]
ssfs_key_file_path = /usr/sap/SAR/SYS/global/hdb/security/ssfs
```

Encrypt PKI SSFS Keys:

```
export RSEC_SSFS_DATAPATH=/usr/sap/SAR/SYS/global/security/rsecssfs/data
```

```
export RSEC_SSFS_KEYPATH=/usr/sap/SAR/SYS/global/security/rsecssfs/key
```

```
rsecssfx changekey $(rsecssfx generatekey -getPlainValueToConsole)
```

```
paradm@US11TC041133:/usr/sap/SAR/SYS/global/security/rsecssfs> export RSEC_SSFS_DATAPATH=/usr/sap/SAR/SYS/global/security/rsecssfs/data
paradm@US11TC041133:/usr/sap/SAR/SYS/global/security/rsecssfs> export RSEC_SSFS_KEYPATH=/usr/sap/SAR/SYS/global/security/rsecssfs/key
paradm@US11TC041133:/usr/sap/SAR/SYS/global/security/rsecssfs> rsecssfx changekey $(rsecssfx generatekey -getPlainValueToConsole)
Record Statistics
=====
Encrypted and readable           : 3
Encrypted and not readable      : 0
Plaintext                       : 0
Removed by compacting           : 0
paradm@US11TC041133:/usr/sap/SAR/SYS/global/security/rsecssfs>
```

Now start your HANA DB and give system privilege ENCRYPTION ROOT KEY ADMIN to user and run below SQL command.

Whenever HANA DB is installed or a tenant DB is created, unique keys will be created, and encryption will be disabled.

From HANA studio, To check Initial Keys ***select * from ENCRYPTION_ROOT_KEYS;***

```
select * from ENCRYPTION_ROOT_KEYS
```

	ROOT_KEY_TYPE	ROOT_KEY_VERSION	CREATE_TIMESTAMP	IS_CONSISTENT	RESET_COUNT	IS_USED	ROOT_KEY_STATUS	ROOT_KEY_HASH	
1	PERSISTENCE	0	Jun 17, 2021 5:42:33.0 PM	TRUE	0	FALSE	ACTIVE	ccc1a2c280d7e3b560c214f372204caca0d1615f0d1f4c66fb53f233073d...	IN
2	DPAPI	0	Jun 17, 2021 5:42:43.0 PM	TRUE	0	TRUE	ACTIVE	951c5e941d916e91b35473ac51ca114d69f065028be44099146e2a824e86...	FA
3	LOG	0	Jun 17, 2021 5:43:02.0 PM	TRUE	0	FALSE	ACTIVE	b1913d0d8376b4f13b73fd9a7d9280d0378a8dee7b6d4187f793ec862e3...	FA
4	BACKUP	0	Jun 17, 2021 5:42:52.0 PM	TRUE	0	?	ACTIVE	80e87e5f8969556ad75dd91d4122048c4c80d79fbf992653c8e277aa0d7c...	FA

To check encryption status ***select * from SYS.M_ENCRYPTION_OVERVIEW***

```
select * from SYS.M_ENCRYPTION_OVERVIEW
```

	SCOPE	IS_ENCRYPTION_ACTIVE	LAST_CHANGE_TIME	CONFIGURATION_CONTROL	ENCRYPTION_CONTROL_LAST_CHANGE_TIME	
1	PERSISTENCE	FALSE	Jun 17, 2021 1:43:14.0 PM	LOCAL DATABASE	Jun 17, 2021 1:43:36.0 PM	
2	LOG	FALSE	Jun 17, 2021 1:43:21.0 PM	LOCAL DATABASE	Jun 17, 2021 1:43:36.0 PM	
3	BACKUP	FALSE	Jun 17, 2021 1:43:28.0 PM	LOCAL DATABASE	Jun 17, 2021 1:43:36.0 PM	

How to enable Encryption on SYSTEM DB

Set the Root Key Backup Password

This root key backup password is required to decrypt the root key backup file while any restore or recovery is being performed. This can be done via HANA Studio or Cockpit.

ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD
<PASSPHRASE>

```
B11@B11 (SYSTEM) 11/23/24
```

```
SQL
```

```
ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD "Welcome.1"
```

Once the password is created, this will be stored in SSFS along with other keys.

To validate the password run below SQL statement.

ALTER SYSTEM VALIDATE ENCRYPTION ROOT KEYS BACKUP PASSWORD
"Welcome.1"

If password is wrong output will be as below.

```
SQL
ALTER SYSTEM VALIDATE ENCRYPTION ROOT KEYS BACKUP PASSWORD "Welcome1"
```

Could not execute 'ALTER SYSTEM VALIDATE ENCRYPTION ROOT KEYS BACKUP PASSWORD "Welcome1"' in 7 ms 575 μ s .
SAP DBTech JDBC: [703]: incorrect root keys backup password: Validation of the Root Keys Backup Password failed.

Could not execute 'ALTER SYSTEM VALIDATE ENCRYPTION ROOT KEYS BACKUP PASSWORD "Welcome1"' in 7 ms 575 μ s .

SAP DBTech JDBC: [703]: incorrect root keys backup password: Validation of the Root Keys Backup Password failed.

Generate New Root Keys

Below are the unique keys which are created during installation.

*select * from ENCRYPTION_ROOT_KEYS;*

select * from ENCRYPTION_ROOT_KEYS									
	ROOT_KEY_TYPE	ROOT_KEY_VERSION	CREATE_TIMESTAMP	IS_CONSISTENT	RESET_COUNT	IS_USED	ROOT_KEY_STATUS	ROOT_KEY_HASH	IN_B
1	PERSISTENCE	0	Jun 17, 2021 5:42:33.0 PM	TRUE	0	FALSE	ACTIVE	ccc1a2c280d7e3b560c214f3722f04cacda0d1615f0df14c6bfb53f233073d...	FALS
2	DPAPI	0	Jun 17, 2021 5:42:43.0 PM	TRUE	0	TRUE	ACTIVE	951c5e941d916e91b35473ac51ca1f4d9f065028be44099146e2a824e86...	FALS
3	LOG	0	Jun 17, 2021 5:43:02.0 PM	TRUE	0	FALSE	ACTIVE	b1913d0d8376b4f13b73fd9a7d9280d0378a8dee7b6d4187793ec862e3...	FALS
4	BACKUP	0	Jun 17, 2021 5:42:52.0 PM	TRUE	0	?	ACTIVE	80e87e5f8969556adf5dd91d4122048c4c80d79fbf992653c8e277aa0d7c...	FALS

In order to change the root key, the below commands need to be executed based on the encryption.

- Data Volume encryption --> *ALTER SYSTEM PERSISTENCE ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE*

```
Statement 'ALTER SYSTEM PERSISTENCE ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE'
successfully executed in 2.414 seconds (server processing time: 2.414 seconds) - Rows Affected: 0
```

- Redo log encryption --> *ALTER SYSTEM LOG ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE*
- Data & Redo log --> *ALTER SYSTEM BACKUP ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE*

Statement 'ALTER SYSTEM BACKUP ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE'

successfully executed in 2.415 seconds (server processing time: 2.414 seconds) - Rows Affected: 0

To verify the above step

*select * from ENCRYPTION_ROOT_KEYS. Keys generated above will be in PREACTIVE status.*

select * from ENCRYPTION_ROOT_KEYS								
	ROOT_KEY_TYPE	ROOT_KEY_VERSION	CREATE_TIMESTAMP	IS_CONSISTENT	RESET_COUNT	IS_USED	ROOT_KEY_STATUS	ROOT_KEY_HASH
1	PERSISTENCE	0	Jun 17, 2021 5:42:33.0 PM	TRUE	0	FALSE	ACTIVE	ccc1a2c280d7e3b560c214f3722f04caeda0d1615f0d1f4c6bfb531233073d...
2	PERSISTENCE	1	Jun 18, 2021 6:14:14.0 PM	TRUE	0	FALSE	PREACTIVE	70e9391966a5a9f1803f18524c4d77e242c5de207050f5e197ac6ecf6adb0...
3	DPAPI	0	Jun 17, 2021 5:42:43.0 PM	TRUE	0	TRUE	ACTIVE	951c5e941d916e91b35473ac51ca114d69f065028be44099146e2a824e86...
4	LOG	0	Jun 17, 2021 5:43:02.0 PM	TRUE	0	FALSE	ACTIVE	b1913d0d8376b4113b73fd9a7d9280d0378a8dee7b6d4187f793ec862e3...
5	LOG	1	Jun 18, 2021 6:14:40.0 PM	TRUE	0	FALSE	PREACTIVE	16e0804327f3d61b697fbb78395881fad52201486ec7d93ed4085b91034...
6	BACKUP	0	Jun 17, 2021 5:42:52.0 PM	TRUE	0	?	ACTIVE	80e87e5f8969556ad5dd91d4122048c4c80d79fbf992653c8e277aa0d7c...
7	BACKUP	1	Jun 18, 2021 6:15:03.0 PM	TRUE	0	?	PREACTIVE	f9394a298275154172488cc65adeca962ebc9c9b53d69da010f39a1ccf30a...

Back Up Root Keys

Once the new keys are created, backup them from OS level. Before taking the backup of keys, find the dbid using below SQL statement.

SELECT DATABASE_NAME, CASE WHEN (DBID = '' AND DATABASE_NAME = 'SYSTEMDB') THEN 1 WHEN (DBID = '' AND DATABASE_NAME <> 'SYSTEMDB') THEN 3 ELSE TO_INT(DBID) END DATABASE_ID FROM (SELECT DISTINCT DATABASE_NAME, SUBSTR_AFTER (SUBPATH,':') AS DBID FROM SYS_DATABASES.M_VOLUMES)

SQL Result		
SELECT DATABASE_NAME, CASE WHEN (DBID = '' AND DATABASE_NAME = 'SYSTEMDB') THEN 1 WHEN (DBID = '' AND DATABASE_NAME <> 'SYSTEMDB') THEN 3 ELSE TO_INT(DBID) END DATABASE_ID FROM (SELECT DISTINCT DATABASE_NAME, SUBSTR_AFTER (SUBPATH,':') AS DBID FROM SYS_DATABASES. M_VOLUMES)		
	DATABASE_NAME	DATABASE_ID
1	B11	3
2	SYSTEMDB	1

Now with hanasidadm go to /usr/sap/<SID>/HDB00/exe and then run below command

./hdbnsutil -backupRootKeys <filename>.rkb --dbid=dbid --type='ALL'

Dbid --> Database ID

Type=ALL --> One of these values can be given- ALL, DATA, LOG, BACKUP. If we don't give pass this then it will take backup of all keys related to Data/Log/Backup volumes.

```

$lladm@B11:~/usr/app/B11/HDB04/exe> ./hdbsnutil -backupRootKeys B11 Tenant.rkb -dbid=3 --type="ALL"
Exporting root keys for DBID: 3 to /hana/shared/B11/exe/linuxx86_64/HDB_2.00.055.00.1615413201_05fd01c3749db22de9f4eea75e45ed541c4b9a22/B11_Tenant.rkb
Successfully exported root keys.
Done.

```

To validate the root key backup run below command and enter the password which has been generated in Root Key Backup step.

Go to /usr/sap/SAR/HDB00/exe and then run below command

```
./hdbnsutil -validateRootKeysBackup <location>/<filename.rkb>
```

Then enter the password that has been given in Root Key Backup step.

```
billadm@b11-tenant:~$ cd /usr/sap/B11/HDB04/exe> ./hdbsut1l -validateRootKeysBackup B11_Tenant.rkb
Please Enter the password:
Successfully validated the backup file /hana/shared/B11/exe/linuxx86_64/HDB_2.00.055.00.1615413201_05fd01c3749db22de9f4eea75e45ed541c4b9a22/B11_Tenant.rkb
done.
billadm@b11-tenant:~$ cd /usr/sap/B11/HDB04/exe>
```

Backup of the keys can be taken from HANA Studio as well.

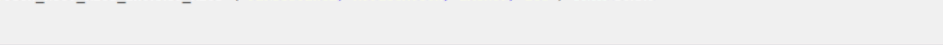
```
SELECT ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS ('PERSISTENCE,  
APPLICATION, BACKUP, LOG') FROM DUMMY
```

```
SELECT ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS ('PERSISTENCE, APPLICATION, BACKUP, LOG') FROM DUMMY
```



```
ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS(PERSISTENCE, APPLICATION, BACKUP, LOG)
```


1	tsMAAigAAAAIoAAAAAogWyyPAuud220XRZGAgGxGjRWedlNmJwT4AC0P7adwLe5/5HzcRr+TNGws88EO3N4wqAAAAAAAAAAAAAAAAAAAAAAAEQ9TRVWRVhVMS9QRVITSYNUROSQRVIAAAAA
---	---



The screenshot shows a SQL query in a database client's query editor:

```
SELECT ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS ('PERSISTENCE, APPLICATION, BACKUP, LOG') FROM DUMMY
```

The query is executed, and the results are displayed in a table with one row:

	ENCRYPTION_ROOT_KEYS_EXTRACT_KEYS(PERSISTENCE, APPLICATION, BACKUP, LOG)
1	tMsAAVgAAAUolAAAAAXogWyyPAAvd220YXRZjGjKk4ojRWedLnmUjwTAACOP7xrdLpS(5HczjR+TNGuacB8tF03jAdwrsAAAAAAAAAAAAAAAAAAAAAAAAAAAAAehEQj9TRVjWRVivMS9QRVjTSVNURUSDQAAAAAAAAA

A context menu is open over the first cell of the result, showing options:

- Export Cell To
- Export Result...
- Refresh (F5)
- Close (Ctrl+F4)
- Close All Results (Ctrl+Shift+A)
- Copy Cells (Ctrl+C)
- Copy Rows
- Details...
- Columns...

Export the result with extension as .rkb and save them at secure external location

Now we can see all the keys backup is TRUE.

select * from ENCRYPTION_ROOT_KEYS									
	ROOT_KEY_TYPE	ROOT_KEY_VERSION	CREATE_TIMESTAMP	IS_CONSISTENT	RESET_COUNT	IS_USED	ROOT_KEY_STATUS	ROOT_KEY_HASH	IN_BACKUP
1	PERSISTENCE	0	Jun 17, 2021 5:42:33.0 PM	TRUE	0	FALSE	ACTIVE	ccc1a2c280d7e3b560c214f372204caccda0d1615d0df4c6efb531233073d...	TRUE
2	PERSISTENCE	1	Jun 18, 2021 6:14:14.0 PM	TRUE	0	FALSE	PRI-ACTIVE	70e9391966a5a9f803f18524c4d77e242c5de207050f5e197ac6ec1eadb0...	TRUE
3	DPAPI	0	Jun 17, 2021 5:42:43.0 PM	TRUE	0	TRUE	ACTIVE	951c5e941d916e91b35473ac51ca194669f065028be44099146e2a824e86...	TRUE
4	LOG	0	Jun 17, 2021 5:43:02.0 PM	TRUE	0	FALSE	ACTIVE	b1913d0d8376b4f13b739d9a7d9280d0378a8dee7b6d4187f793ec862e3...	TRUE
5	LOG	1	Jun 18, 2021 6:14:40.0 PM	TRUE	0	FALSE	PRI-ACTIVE	16e0804327f3d61b697fb78395881fad52201486ec7d93ed4085e91034...	TRUE
6	BACKUP	0	Jun 17, 2021 5:42:52.0 PM	TRUE	0	?	ACTIVE	80e87e5f8969556adff5dd91d4122048c4c80d79fb992653c8e277aa0d7c...	TRUE
7	BACKUP	1	Jun 18, 2021 6:15:03.0 PM	TRUE	0	?	PRI-ACTIVE	f9394a298275154172488cc65adeca962ebc9c9b53d69da010f39a1ccf30a...	TRUE

Activate New Root Keys

Once the backup of new encryption root keys is taken, the keys need to be activated.

Activate new root keys by following commands

- Data volume encryption à *ALTER SYSTEM PERSISTENCE ENCRYPTION ACTIVATE NEW ROOT KEY*

Statement 'ALTER SYSTEM PERSISTENCE ENCRYPTION ACTIVATE NEW ROOT KEY'

successfully executed in 2.419 seconds (server processing time: 2.418 seconds) -
Rows Affected: 0

- Redo log encryption à *ALTER SYSTEM LOG ENCRYPTION ACTIVATE NEW ROOT KEY*

Statement 'ALTER SYSTEM LOG ENCRYPTION ACTIVATE NEW ROOT KEY'

successfully executed in 2.419 seconds (server processing time: 2.418 seconds) -
Rows Affected: 0

- Data and log backup encryption à *ALTER SYSTEM BACKUP ENCRYPTION ACTIVATE NEW ROOT KEY*

Statement 'ALTER SYSTEM BACKUP ENCRYPTION ACTIVATE NEW ROOT KEY'

successfully executed in 2.419 seconds (server processing time: 2.418 seconds) -
Rows Affected: 0

*****After activating the root keys ,take a backup of keys and validate the new key file.**

We can validate whether keys are activated, and a backup of keys is done.

```
select * from ENCRYPTION_ROOT_KEYS
```

	ROOT_KEY_TYPE	ROOT_KEY_VERSION	CREATE_TIMESTAMP	IS_CONSISTENT	RESET_COUNT	IS_USED	ROOT_KEY_STATUS	ROOT_KEY_HASH	IN_BACKUP
1	PERSISTENCE	0	Jun 17, 2021 5:42:33.0 PM	TRUE	0	FALSE	ACTIVE	ccc1a2c280d7e3b590c214f3722f04cadda0d1615f0d14c6fb531233073d...	TRUE
2	PERSISTENCE	1	Jun 18, 2021 6:14:14.0 PM	TRUE	0	FALSE	PREACTIVE	70e9391966a5a9f803f18524e4d77e242c5de207050f5e197ac6ec1fad0...	TRUE
3	DPAPI	0	Jun 17, 2021 5:42:43.0 PM	TRUE	0	TRUE	ACTIVE	951c5e941d916e91b35473ac51ca154669f065028be44099146e2a824e96...	TRUE
4	LOG	0	Jun 17, 2021 5:43:02.0 PM	TRUE	0	FALSE	ACTIVE	b1913d0d8376b4f13b73f95a7d9280d0378a8dee7b6d4187f793ec862e3...	TRUE
5	LOG	1	Jun 18, 2021 6:14:40.0 PM	TRUE	0	FALSE	PREACTIVE	16e0804327f1d61b697fb78395881fad352201486ec7d93ed4085e91034...	TRUE
6	BACKUP	0	Jun 17, 2021 5:42:52.0 PM	TRUE	0	?	ACTIVE	80e87e5f8969556ad15dd91d4122048c4c80d79fbf992653cbe277aa0d7c...	TRUE
7	BACKUP	1	Jun 18, 2021 6:15:03.0 PM	TRUE	0	?	PREACTIVE	f9394a298275154172488cc65adeca962ebc9c9b53d69da010f39a1ccf30a...	TRUE

If required, take backup of keys as shown above.

Enabling Encryption on Data and Log Volumes

Enabling ENCRYPTION on:

- Data Volume --> **ALTER SYSTEM PERSISTENCE ENCRYPTION ON**

If you enable encryption in an operational database, only the pages in use in the data volumes are encrypted. Pages in data volumes that are not in use may still contain old content, and are only overwritten and encrypted over time. This means that your data in data volumes will only be fully encrypted after some delay. If your DB is huge then it is recommended to take a backup (after encryption) and then restore it.

Statement 'ALTER SYSTEM PERSISTENCE ENCRYPTION ON'

successfully executed in 2.408 seconds (server processing time: 2.408 seconds) - Rows Affected: 0

- Log Volume --> **ALTER SYSTEM LOG ENCRYPTION ON**

Redo log entries that are created after encryption are encrypted. Redo log files that were created before encryption was enabled are not encrypted and they will be encrypted when they are overwritten.

Statement 'ALTER SYSTEM LOG ENCRYPTION ON'

successfully executed in 2.408 seconds (server processing time: 2.408 seconds) -
Rows Affected: 0

- Backup Volume --> *ALTER SYSTEM BACKUP ENCRYPTION ON*

We cannot enable or disable encryption for a single Full/Incremental/log backup.
Backups which were taken before encryption will still be in unencrypted format only.

Statement 'ALTER SYSTEM BACKUP ENCRYPTION ON'

successfully executed in 2.408 seconds (server processing time: 2.408 seconds) -
Rows Affected: 0

Now validate the encryption status of database.

<i>select * from SYS.M_ENCRYPTION_OVERVIEW</i>					
	SCOPE	IS_ENCRYPTION_ACTIVE	LAST_CHANGE_TIME	CONFIGURATION_CONTROL	ENCRYPTION_CONTROL_LAST_CHANGE_TIME
1	PERSISTENCE	TRUE	Jun 18, 2021 2:30:20.0 PM	LOCAL DATABASE	Jun 17, 2021 1:43:36.0 PM
2	LOG	TRUE	Jun 18, 2021 2:30:32.0 PM	LOCAL DATABASE	Jun 17, 2021 1:43:36.0 PM
3	BACKUP	TRUE	Jun 18, 2021 2:30:39.0 PM	LOCAL DATABASE	Jun 17, 2021 1:43:36.0 PM

- **Enabling Encryption on Initial Tenant DB (created with installation) or existing Tenant:**

Perform same steps as SYSTEM DB on the initial tenant DB or running tenants

- Set the backup password for root key backup.
- Change the root keys for all encryption services (DATA/Log/Backup). As part of this step ,Generate new keys without Activate, Backup the root keys, Activate the Root keys and backup the root keys.
- Enable the Encryption for Data/Log/Backup.

Enabling Encryption on subsequent Tenant DB:

Below are the steps to be performed to enable encryption on newly created tenant DB.

- Set password for root key backup.
- Backup the root keys
- Enable the encryption for Data/Log/Backup.

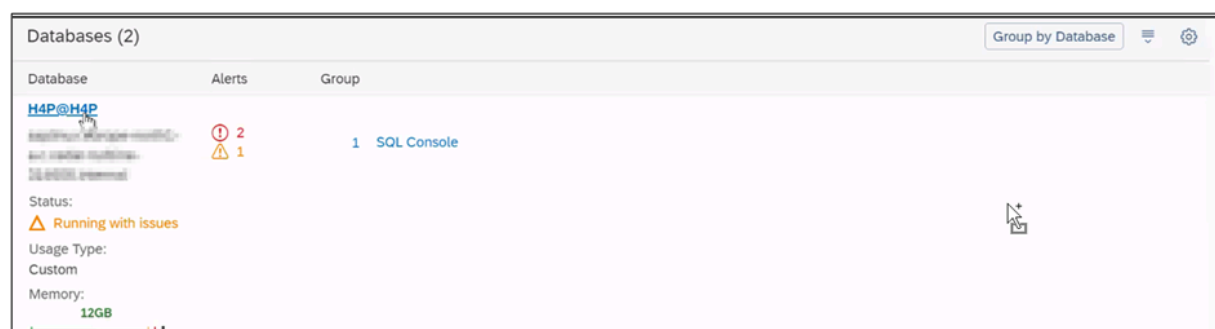
How to change Keys:

It is always highly recommended to change the keys regularly as per customer security policy. Below is the procedure to change the keys

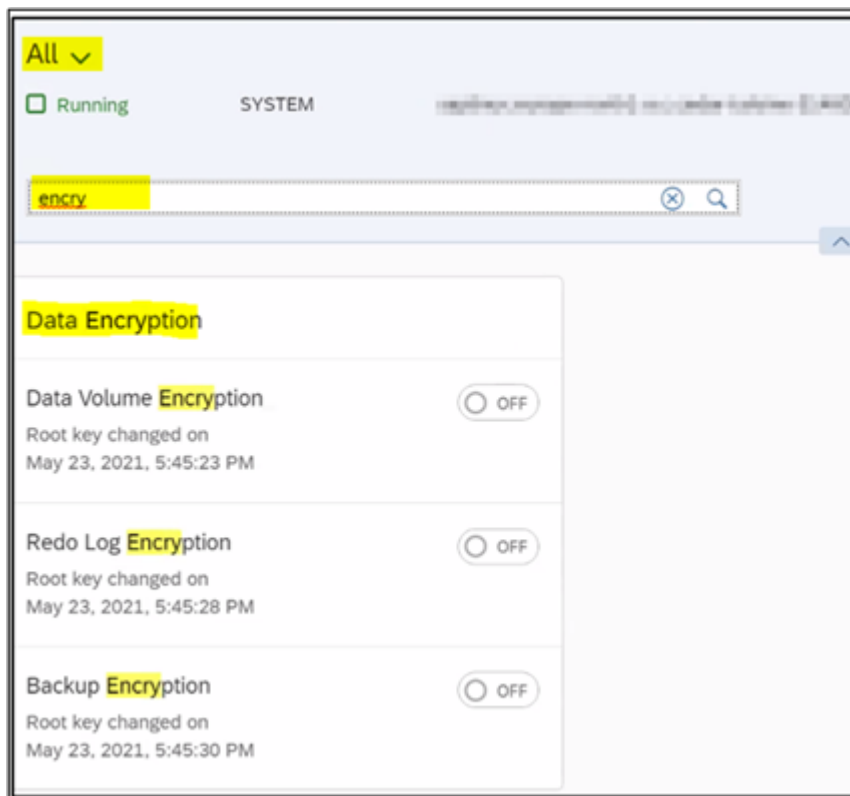
1. a) Generate new keys without Activate.
2. b) Back up new keys.
3. c) Activate new keys.
4. d) Back up activated keys

Enable and Disable Encryption from HANA Cockpit

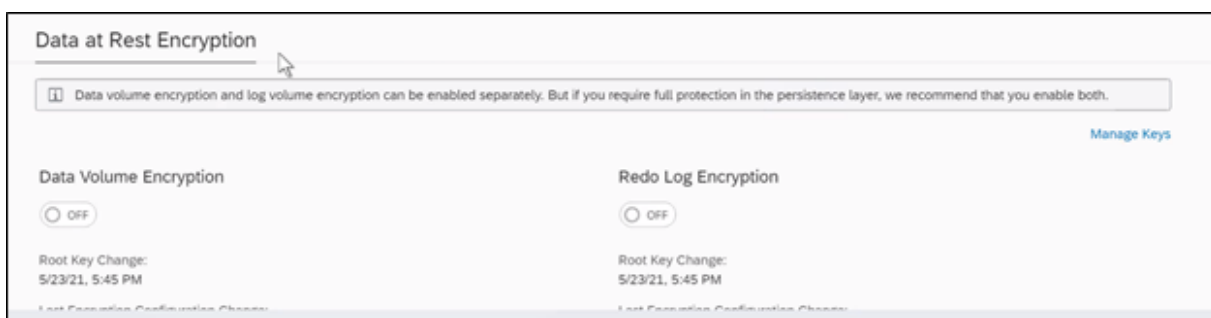
Login to HANA Cockpit and ensure the DB's are added and correct credentials are maintained



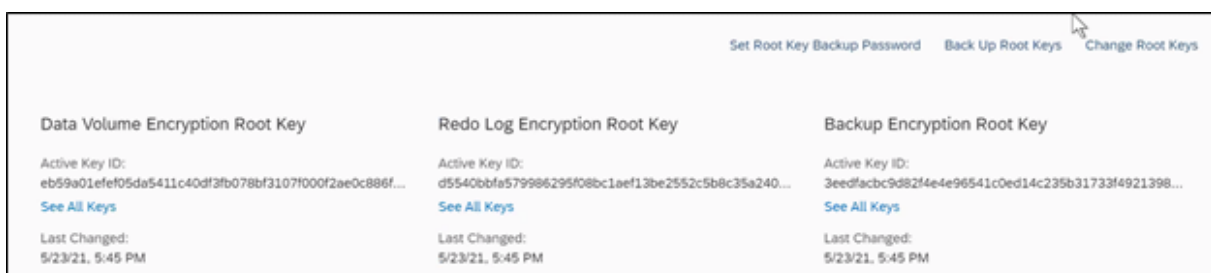
Click on Data Encryption Tile



Click on Manage Keys



Below keys are generated during installation. Click Change Root Keys



Enter the password and ensure that this password is remembered as this will be needed when the DB needs to be restored/recovered.

1. Root Key Backup Password

 This password protects your root key backup files so keep it safe. Losing it may result in the database being unrecoverable.

*Password:

*Password Confirmation:

Select which service root keys that needs to be changed. In this step it will generate new keys but will not activate them yet.

2. Keys to Be Changed

Select the root keys that you want to change.

- ☒ Data volume encryption root key
- ☒ Redo log encryption root key
- ☒ Backup encryption root key
- ☐ Application encryption service root key

Step 3

Download the keys and keep it in a safe location.

3. Root Key Backup

 You must now back up all your root keys to an external location. This ensures that if you ever have to recover your database, you have all the root keys required to restore encrypted data from a data backup.

Download Root Keys

Once keys are downloaded in previous step, select yes and click Activate Root Keys. This step will now activate the new keys that have been generated in the previous step.

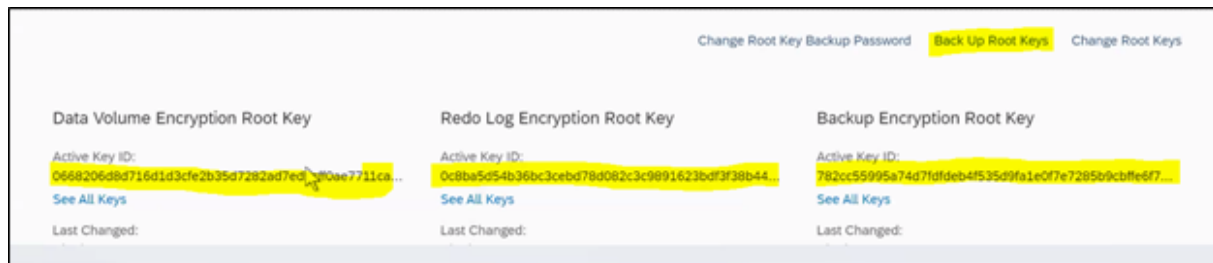
4. Root Key Activation

Have you backed up the root keys?

- ☒ Yes
- ☐ No

Activate Root Keys

Now new keys are generated for Data/Log/Backup volumes. Click on Backup root Keys, this will download the root keys backup of activated keys and ensure that these keys are kept very safe as these keys need to be imported on target DB during restore.



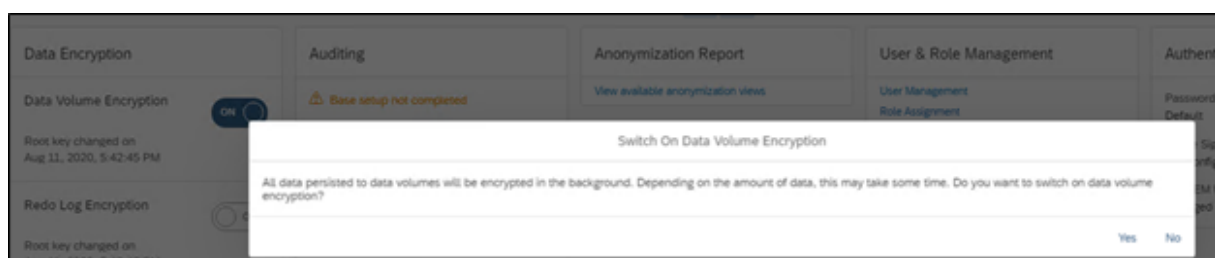
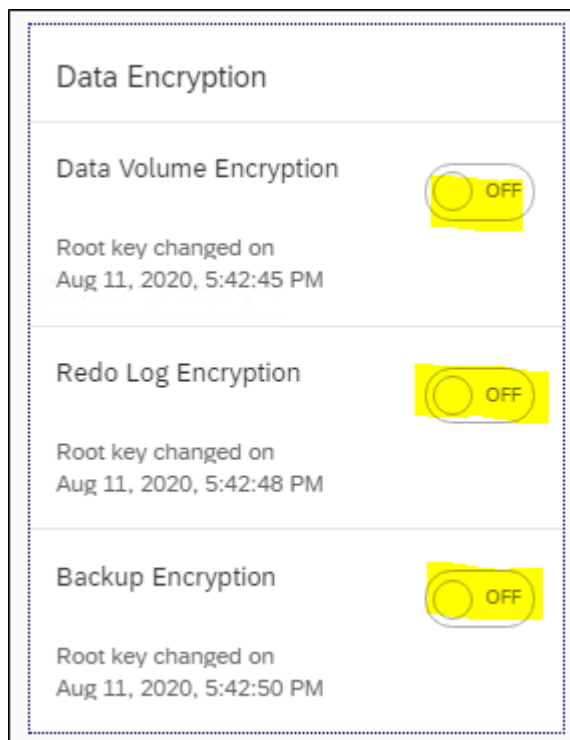
Once downloaded, if you want to validate the keys then copy the .rbd files to OS level and run below commands.

```
cd /usr/sap/<sid>/<HDBinstance_no>/exe
```

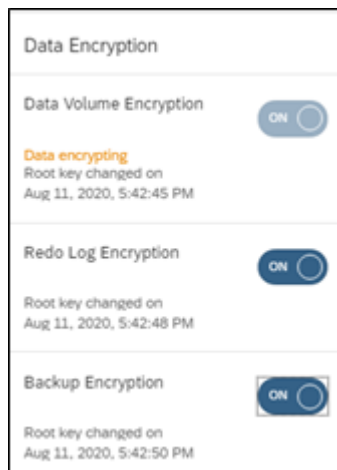
```
./hdbnsutil -validateRootKeysBackup <filename>
```

This will ask for password, give the password that has been set in Step 1

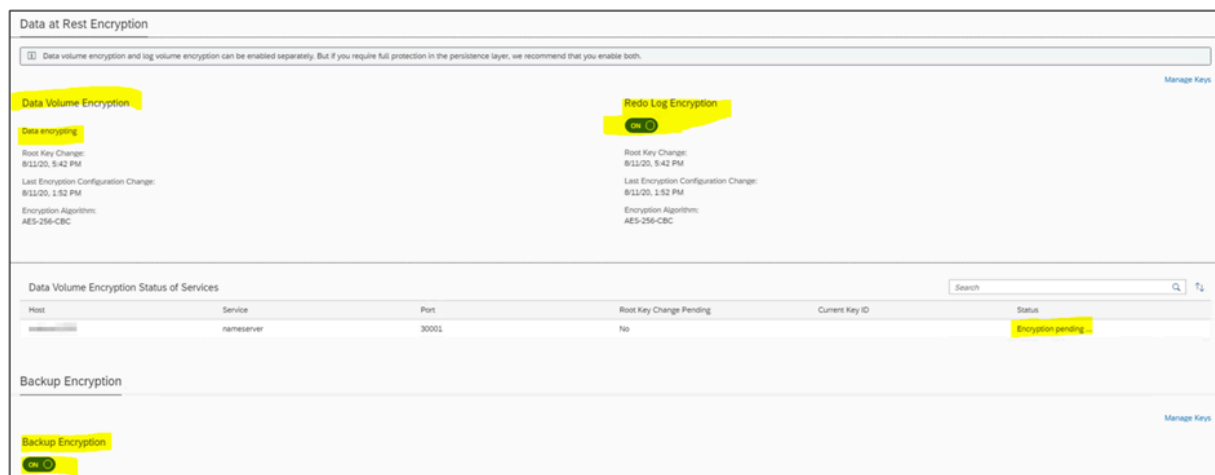
Now enable the Encryption. To do this go to home page where Data Encryption tile can be seen and click on buttons highlighted below.



Similarly do it for log and backup volume as per your scenario.



Now click on Data Encryption tile to see the status.



Enabling Encryption on Initial Tenant DB(created with installation) or existing Tenant

If you have a Tenant DB which is installed during installation or in all existing tenants, follow the same steps as performed for SYSTEM DB to enable encryption.

The screenshot shows the 'Data Encryption' configuration page for the 'SYSTEM' database. It includes sections for 'Data at Rest Encryption', 'Data Volume Encryption', 'Redo Log Encryption', and 'Backup Encryption'. The 'Data Volume Encryption' and 'Redo Log Encryption' sections show 'On' status with 'Encryption pending...' messages. Below these is a table titled 'Data Volume Encryption Status of Services'.

Host	Service	Port	Root Key Change Pending	Current Key ID	Status
indserver	indexserver	30003	No		Encryption pending...
	xsengine	30007	Yes		Encryption pending...

The 'Backup Encryption' section at the bottom shows a status of 'On'.

For further additional tenants which are created post encryption was enabled in SYSTEM DB, follow the below steps. In my case D12 is the new tenant I have created after enabling encryption on System DB D11 and Tenant DB D11.

The screenshot shows the 'Databases (3)' overview table in the SAP HANA Cockpit. It lists three databases: SYSTEMDB@D11, D11@D11, and D12@D11. Each row includes status, usage type, database name, alerts, memory, CPU, disk, expensive statements, group, type/version, credentials, and SAP control credentials.

Status	Usage Type	Database	Alerts	Memory	CPU	Disk	Expensive Statements	Group	Type/Version	Credentials	SAP Control Credentials
Running with issues	Test	SYSTEMDB@D11	1	150B	19%	21%	0	SAP HANA System Database	2.00.048.00.1581325702 (SAP HANA a2up04)	User: SYSTEM Manage Credentials	User: sLLadm Manage Credentials Database Management ...
Running with issues	Test	D11@D11	1	150B	12%	21%	0	SAP HANA Tenant Database	2.00.048.00.1581325702 (SAP HANA a2up04)	User: SYSTEM Manage Credentials	SQL Console
Running	Test	D12@D11						SAP HANA Tenant Database	2.00.048.00.1581325702 (SAP HANA a2up04)	Enter Credentials	SQL Console

Connect to Tenant DB from cockpit and click on Data Encryption tile and click on Manage Keys.

Click on Data Encryption tile

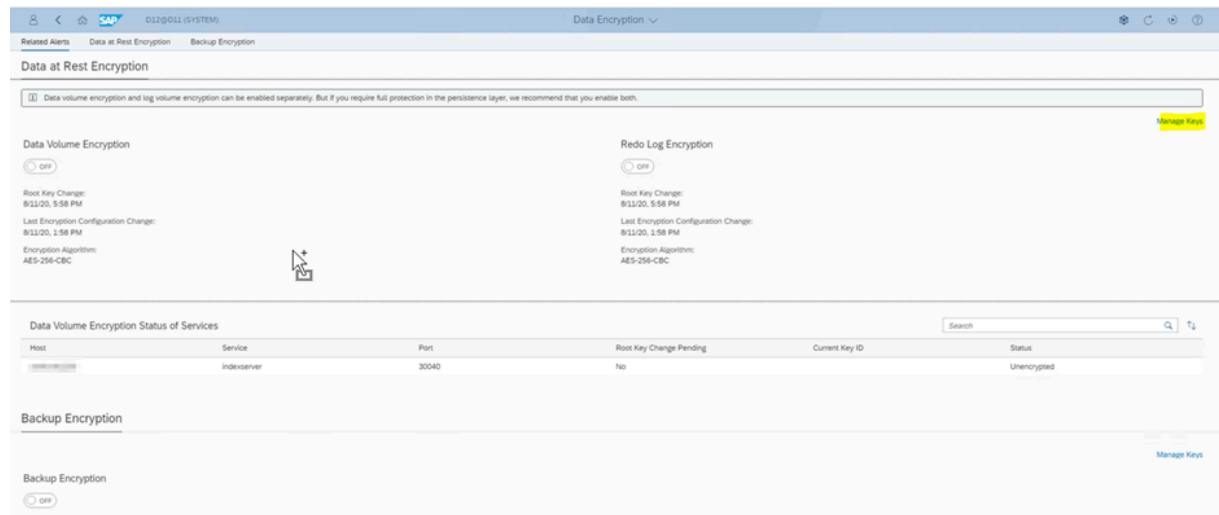
The screenshot shows the 'Data Encryption' configuration page for the 'D12@D11 (SYSTEM)' tenant database. It includes sections for 'Data Volume Encryption', 'Redo Log Encryption', and 'Backup Encryption'. All three sections show 'Off' status.

Data Volume Encryption
Root key changed on Aug 11, 2020, 5:58:02 PM

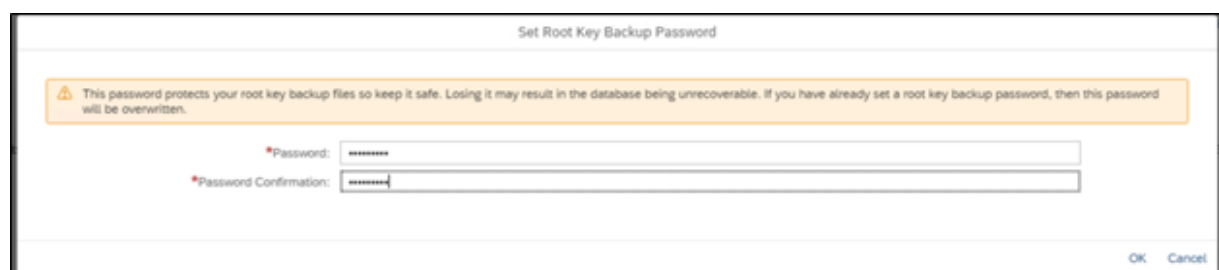
Redo Log Encryption
Root key changed on Aug 11, 2020, 5:58:07 PM

Backup Encryption
Root key changed on Aug 11, 2020, 5:58:09 PM

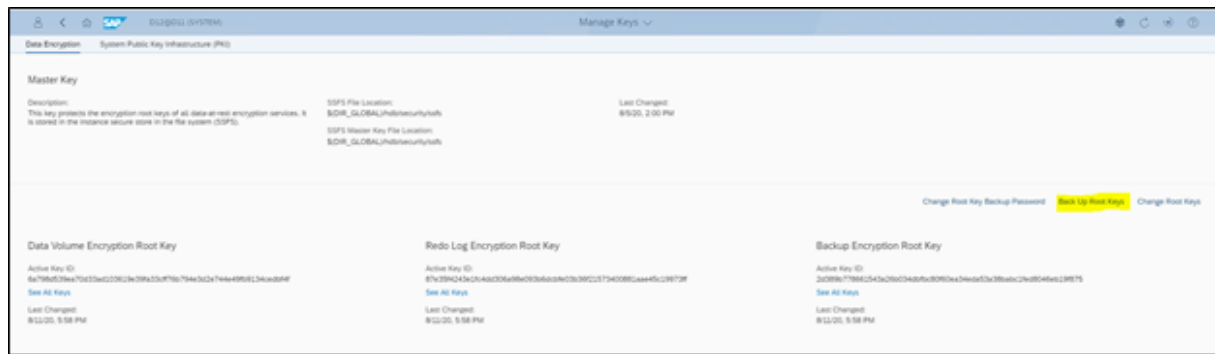
Click on Manage Keys



1. Click on Set Root Key Backup Password



1. Click on Backup Root Keys, this will download the backup file.



1. Now go to Data Encryption tile on tenant homepage and enable the tabs as per your scenario.

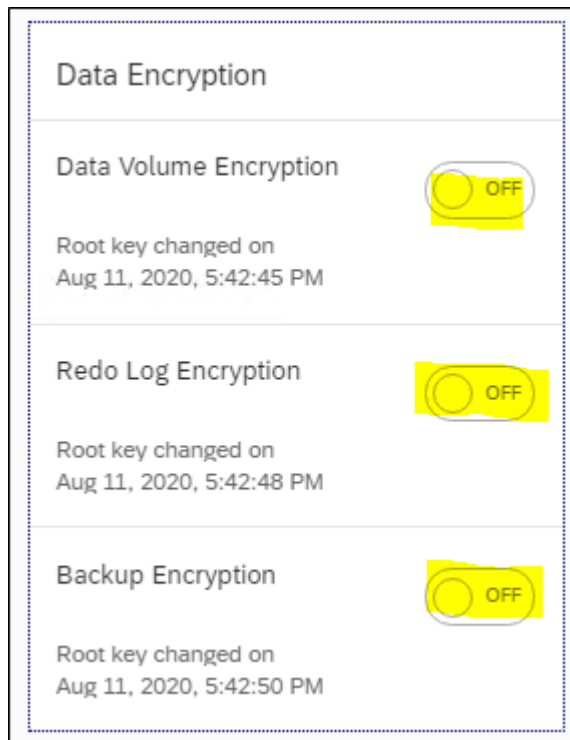
Enabling Encryption Scenario from Single Container to Multi-Container Conversion

If Encryption is already enabled on Single Container, the Tenant DB Inherits the Encrypted.

Encryption on System DB needs to be configured manually if required.

- **Disable Encryption**

Set the buttons to OFF to Disable Encryption



- **Disable encryption**

Encryption can be disabled as required by running following statements.

- Data volume: *ALTER SYSTEM PERSISTENCE ENCRYPTION OFF*
- Redo log volume: *ALTER SYSTEM LOG ENCRYPTION OFF*
- Backup Volume: *ALTER SYSTEM BACKUP ENCRYPTION OFF*

By default, enable and disable of Encryption can be done from respective DB itself. We can enable or disable encryption of a tenant DB from System Database by passing control to SYSTEM DB. Tenant DB can take back the control whenever it wants. As highlighted, respective tenant DB can only enable or disable encryption of that tenant DB.

SQL Result					
select * from SYS.M_ENCRYPTION_OVERVIEW					
	SCOPE	IS_ENCRYPTION_ACTIVE	LAST_CHANGE_TIME	CONFIGURATION_CONTROL	ENCRYPTION_CONTROL_LAST_CHANGE_TIME
1	PERSISTENCE	FALSE	Aug 5, 2020 1:38:31.0 PM	LOCAL DATABASE	Aug 5, 2020 1:38:39.0 PM
2	LOG	FALSE	Aug 5, 2020 1:38:34.0 PM	LOCAL DATABASE	Aug 5, 2020 1:38:39.0 PM
3	BACKUP	FALSE	Aug 5, 2020 1:38:36.0 PM	LOCAL DATABASE	Aug 5, 2020 1:38:39.0 PM

- To pass the control to SYSTEM DB, from where encryption of tenant can be enabled or disabled, run below SQL statement.

ALTER SYSTEM ENCRYPTION CONFIGURATION CONTROLLED BY SYSTEM DATABASE

- To take back control from SYSTEM DB then run the below SQL statement from system DB.

ALTER DATABASE <database_name> ENCRYPTION CONFIGURATION CONTROLLED BY LOCAL DATABASE

- To enable and disable by parameter database_initial_encryption section of global.ini configuration file.

persistence_encryption (default: off)

log_encryption (default: off)

backup_encryption (default: off)

encryption_config_control (default: local_database)

- To enable or disable encryption for a tenant DB from system DB then below are the SQL statements

ALTER DATABASE <database_name> PERSISTENCE ENCRYPTION ON

ALTER DATABASE <database_name> LOG ENCRYPTION ON

ALTER DATABASE <database_name> BACKUP ENCRYPTION ON

For More information please refer to below blogs:

<https://blog.sap-press.com/learn-sap-hana-data-encryption>

https://help.sap.com/docs/SAP_HANA_PLATFORM/6b94445c94ae495c83a19646e7c3fd56/355291043bee4053af4b848...

Tags:

database encryption

11 Comments



PriyankaPuvvada

Discoverer



2022 Nov 18 8:44 PM



0 Kudos

Very informative blog!



MustafaBensan

Active Contributor

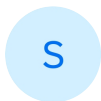


2022 Nov 19 11:39 AM



0 Kudos

Since SAP HANA Studio is being deprecated, I imagine the future-proof approach for configuring encryption would be to use the SAP HANA Cockpit.



saroopreddy88

Explorer



2022 Nov 21 10:32 PM



0 Kudos

Step by step process to enable Encryption from HANA Cockpit are also mentioned in the blog.



antonio_vacas

Explorer



2023 Mar 01 9:30 AM



0 Kudos

Hi

Anyone knows how to force data volumen encryption to all pages? Apparently pages

while are not persisted to disk are unencrypted according to this info.

https://help.sap.com/docs/SAP_HANA_PLATFORM/b3ee5778bc2e4a089d3299b82ec762a7/dc01f36fbb5710148b66820...

Is there anyway to be sure of having 100% of data volume encrypted? I have checked that restore of DB is the only way.

Kind regards



former_member847476

Explorer



2023 Mar 22 6:38 PM



0 Kudos

Can you please explain the purpose of changing root key, why not to use existing key, and just set root key backup password, and encrypt?



former_member847476

Explorer



2023 Mar 22 6:44 PM



0 Kudos

I tried in HANA cockpit, and it shows all data will be encrypted, it took a while to complete the task, so I think all pages were encrypted.



darrylmg

Explorer



2023 May 18 3:40 PM



0 Kudos

There is no way other than backup & restore.

**vamsialluri**

Explorer



2023 Aug 01 11:11 PM



0 Kudos

Very useful information Thanks Saroop.

**rodrigo_monroy**

Discoverer



2023 Sep 05 11:26 PM



0 Kudos

Hello Saroop

We are considering to do the Encryption in our hana databases but we have any doubt about the possible impacts can be exist after to do the Encryption like performances issues, increase the infraestructure (CPU, RAM) or any issue into SAP systems.

In your experience, do you identify any impact or any consideration that we must take before or after to do the Encryption ?

Regards

**saroopreddy88**

Explorer



2024 Apr 30 5:28 PM



0 Kudos

@rodrigo_monroy you may see very minimal impact in terms of CPU when an encrypted backup triggers. We have seen 5% higher CPU consumption than what regular backups. This is not overall CPU consumption but just considering the CPU consumed by backups only.

**divikaus**

Explorer



2024 May 08 3:11 PM



0 Kudos

Hello,

Very useful blog, but one correction:

```
./hdbnsutil -backupRootKeys <filename>.rkb --dbid=dbid --type='ALL'
```

Type=ALL --> One of these values can be given- ALL, DATA, LOG, BACKUP. If we don't give pass this then it will take backup of all keys related to Data/Log/Backup volumes.

the command will be:

```
./hdbnsutil -backupRootKeys <filename>.rkb --dbid=dbid --type='PERSISTENCE'
```

i You must be a registered user to add a comment. If you've already registered, sign in. Otherwise, register and sign in.

Comment

Labels In This Area

"Aging List of Receivables" 1 "as_written_by_Marian_Zeis" 1

"automatische backups" 1 "regelmäßige sicherung" 1 "SAP BW" 3

"SAP VARIANT CONFIGURATION" 2 "SAPDatasphere" 1

"TypeScript" "Development" "FeedBack" 1 *SAP" 1

-147 Get CurrentUserInfo failed 1 2YM 1 3-TIER Extensibility 1

505 Technology Updates 53 1 @RetroDate_HireDateCorrection 1

@sapilm @archiving @sapiq 1 @SCPI 2

A Comprehensive Guide to Using OLE Objects in SAP ABAP 1 aATP 1 ABAP 36

ABAP 7.4 2 ABAP API 1 ABAP BTP 1 ABAP CDS VIEW 2

ABAP CDS Views 11 ABAP CDS Views - BW Extraction 3

ABAP CDS Views - CDC (Change Data Capture) 3 ABAP Class 3 ABAP Cloud 7

ABAP Cloud Developer Trial 1 ABAP DDIC CDS view 1 ABAP Development 9

ABAP Environment & RAP 2 ABAP Extensibility 2 ABAP for EWM 1

ABAP in Eclipse 3 ABAP Interface 1 ABAP New Syntax 1 ABAP ODATA 1

ABAP on HANA 1 ABAP OOABAP 1 ABAP PLATFORM 1 ABAP Platform Trial 2

ABAP Programming 6 ABAP Push Channels 1 ABAP Query 1 ABAP RAP 4

ABAP RAP custom action 1 ABAP RAP(RESTful Application Programming) 4

ABAP RESTful API 1 ABAP RESTful Application Programming Model 2

ABAP String functions 1 abap technical 1 ABAP test cockpit 1 abap to xml 1

abapGit 1 absl 2 Access data from datasphere to ADF Azure Data Factory 2

access data from SAP Datasphere directly from Snowflake 1

Access data from SAP datasphere to QlikSense 2 Accessibility 1

Accessibility in SAPUI5 1 Accrual 1 Acquire SAC Knowledge 2 action 1

actions 1 Activity 1 adapter 2 adapter modules 1

[ADDING LEAN SERVICES 2](#)[Addon 2](#)[Adobe Document Services 1](#)[Adobe forms 1](#)[ADS 1](#)[ADS Config 1](#)[ADS with ABAP 1](#)[ADS with Java 1](#)[ADT 3](#)[Advance Shipping and Receiving 1](#)[Advanced Event Mesh 4](#)[Advanced formula 1](#)[Advanced Metric 1](#)[Advanced SAP Techniques 1](#)[Advanced Scripting in SAC 1](#)[Advanced Workflow 1](#)[AEM 1](#)[AEM Event Portal 1](#)[agile 2](#)[agile development 1](#)[agile teams 1](#)[ai 15](#)[AI Agents 1](#)[AI Essentials 1](#)[ai generated content 1](#)[ai in transportation 1](#)[AI Integration 2](#)[AI Launchpad 3](#)[AI Optimizer 1](#)[AI Projects 2](#)[AI TOOLS 1](#)[aichallenges 1](#)

Related Content

File Upload in cloud using RAP.

in Technology Blogs by Members an hour ago



New Machine Learning features in SAP HANA 2.0 SPS 08

in Technology Blogs by SAP Friday



Internal error: Error opening the cursor for the remote database [Microsoft] [ODBC Driver 17 for SQL

in Technology Q&A Friday



Understanding SAP Fiori Architecture: A Guide to its Three Key Layers

in Technology Blogs by Members Friday



Issue while uploading S4 HANA Database to Maintenance planner

in Technology Q&A Friday



Popular Blog Posts



SAP PI for Beginners



former_member200339
Participant

👁 720767 💬 154 👍 387



ABAP 7.40 Quick Reference



jeffrey_towell2
Participant

👁 1191130 💬 75 👍 341



Difference between SAP S/4HANA :Public Vs Private edition : RISE with SAP



rajarajeswari_kaliyaperum

Active Participant

👁 176570 💬 47 👍 302

Top Kudoed Authors



EmersonATosin

👍 12



Marian_Zeis

👍 12



ivo_skolek

👍 11



A_ER

👍 11



AndySilvey

👍 7



Sandra_Rossi

👍 6

**venkateshgolla**

6

**hazem2020**

5

**Robert_Eijpe**

4

**jeffrey_towell2**

4

View all[Privacy](#)[Terms of Use](#)[Copyright](#)[Legal Disclosure](#)[Trademark](#)[Support](#)[Cookie Preferences](#)[Follow](#)