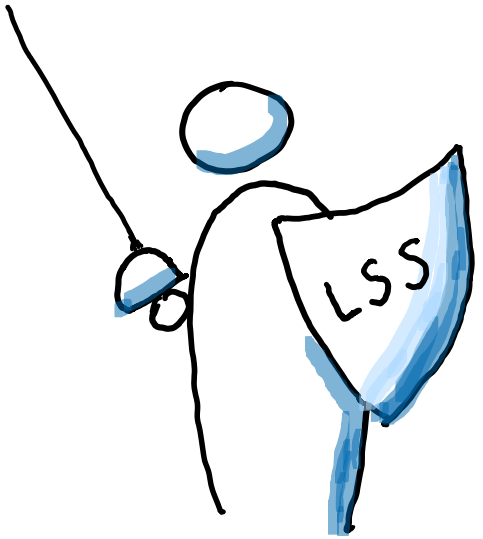
Microsoft

SAP® on

Part IV

System Refresch with Local Secure Store (LSS)



Microsoft
Ralf Klahr
Azure Compute

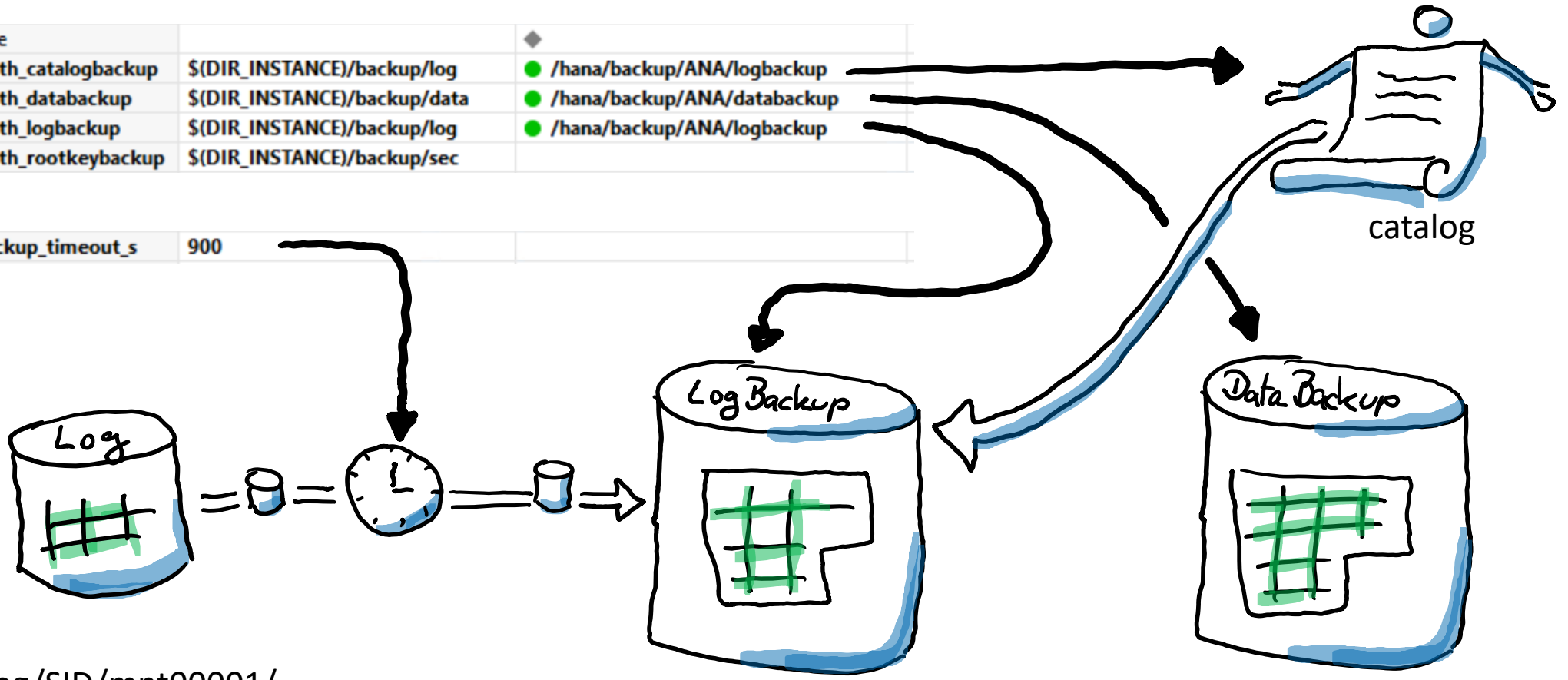
Agenda

Backup Parameter
Recovery Process SYSTEMDB
azacsnap
SSFS Encryption
LSS Encryption

Backup Parameter

$(DIR_INSTANCE) = /hana/shared/<SID>/HDB<ID>/backup/

[ ] persistence		
basepath_catalogbackup	$(DIR_INSTANCE)/backup/log	/hana/backup/ANA/logbackup
basepath_databackup	$(DIR_INSTANCE)/backup/data	/hana/backup/ANA/databackup
basepath_logbackup	$(DIR_INSTANCE)/backup/log	/hana/backup/ANA/logbackup
basepath_rootkeybackup	$(DIR_INSTANCE)/backup/sec	
log_backup_timeout_s	900	



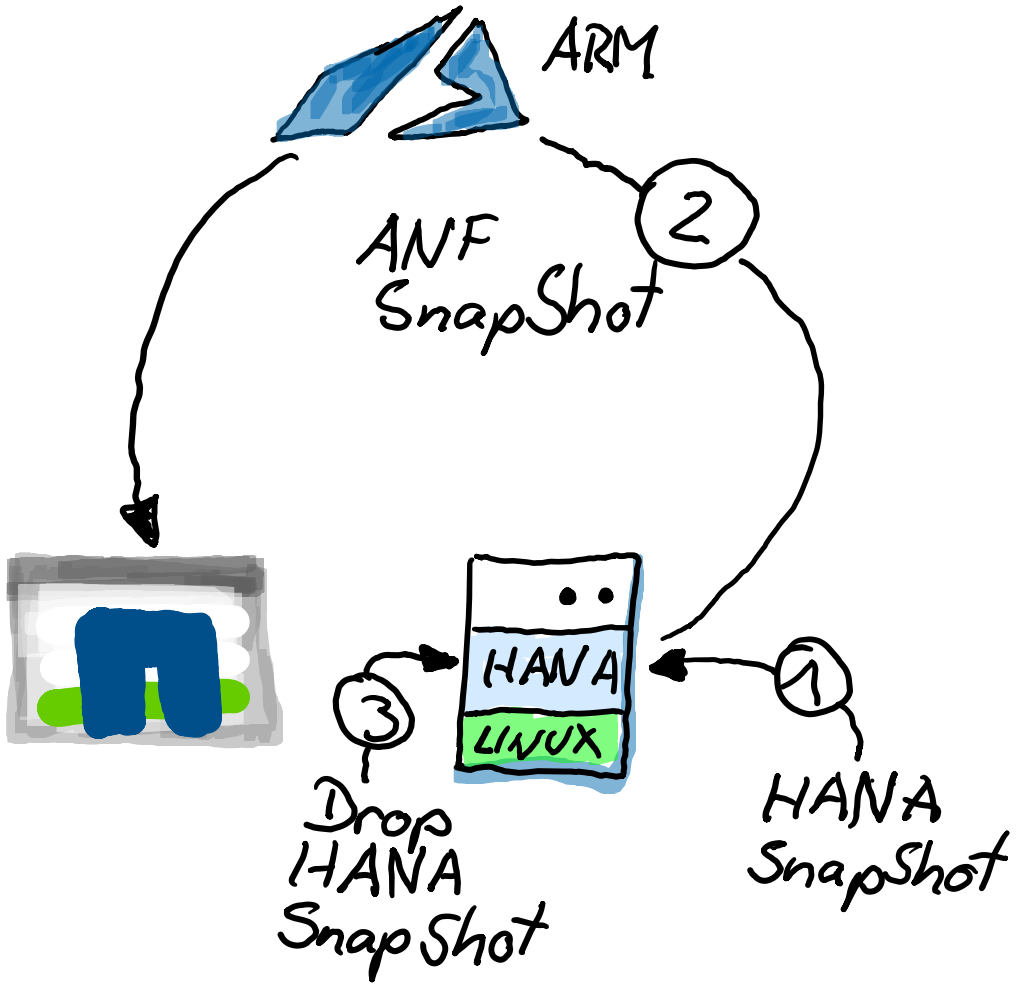
/hana/log/SID/mnt00001/
→hdb00001 → SYSTEMDB
→hdb00002 → TenantDB
→hdb00003 → XS Engine

/hana/backup/SID/logbackup
→SYSTEMDB
→DB_SID

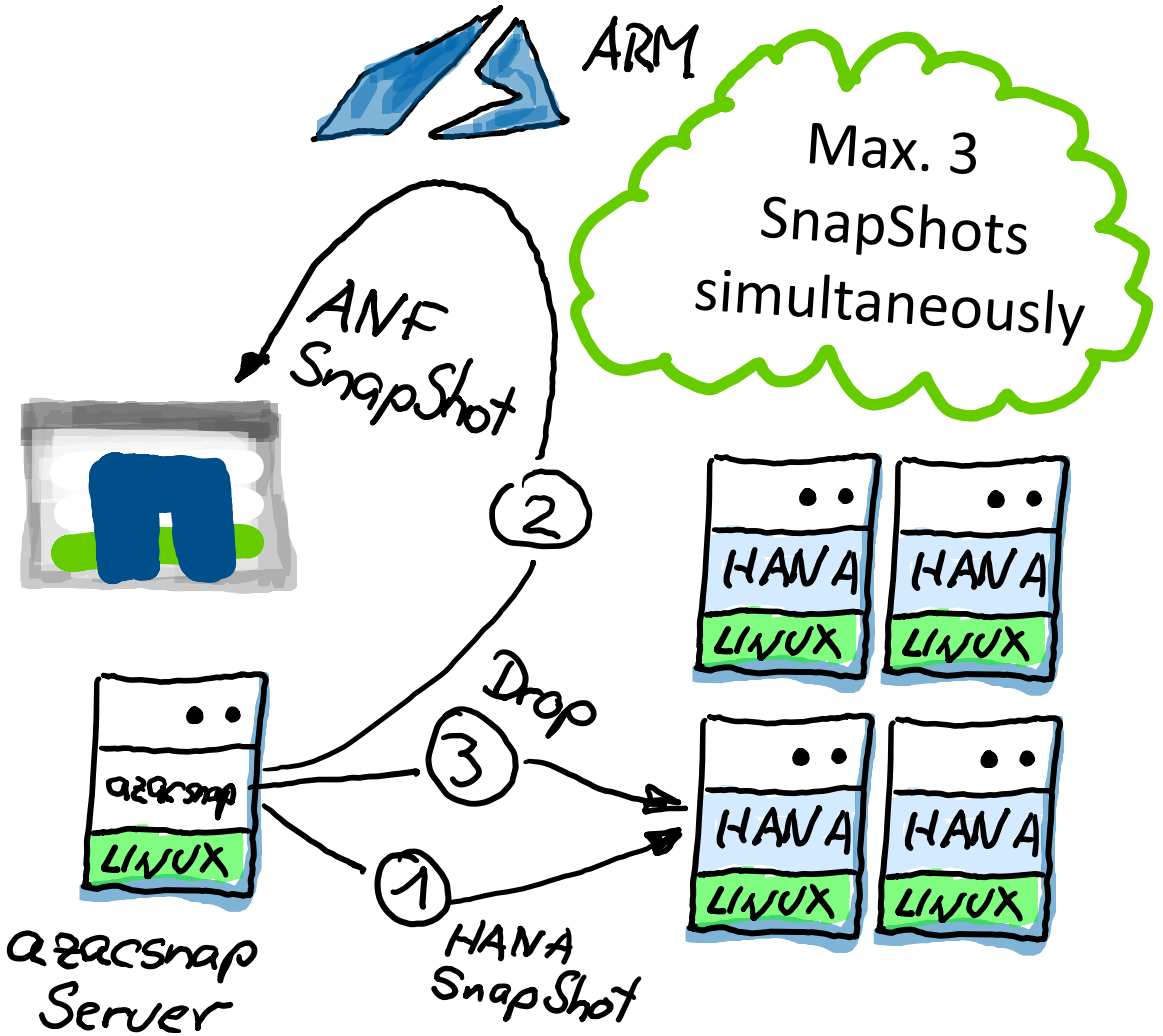
/hana/backup/SID/databackup
→SYSTEMDB
→DB_SID

azacsnap

Local Installation



Distributed Installation

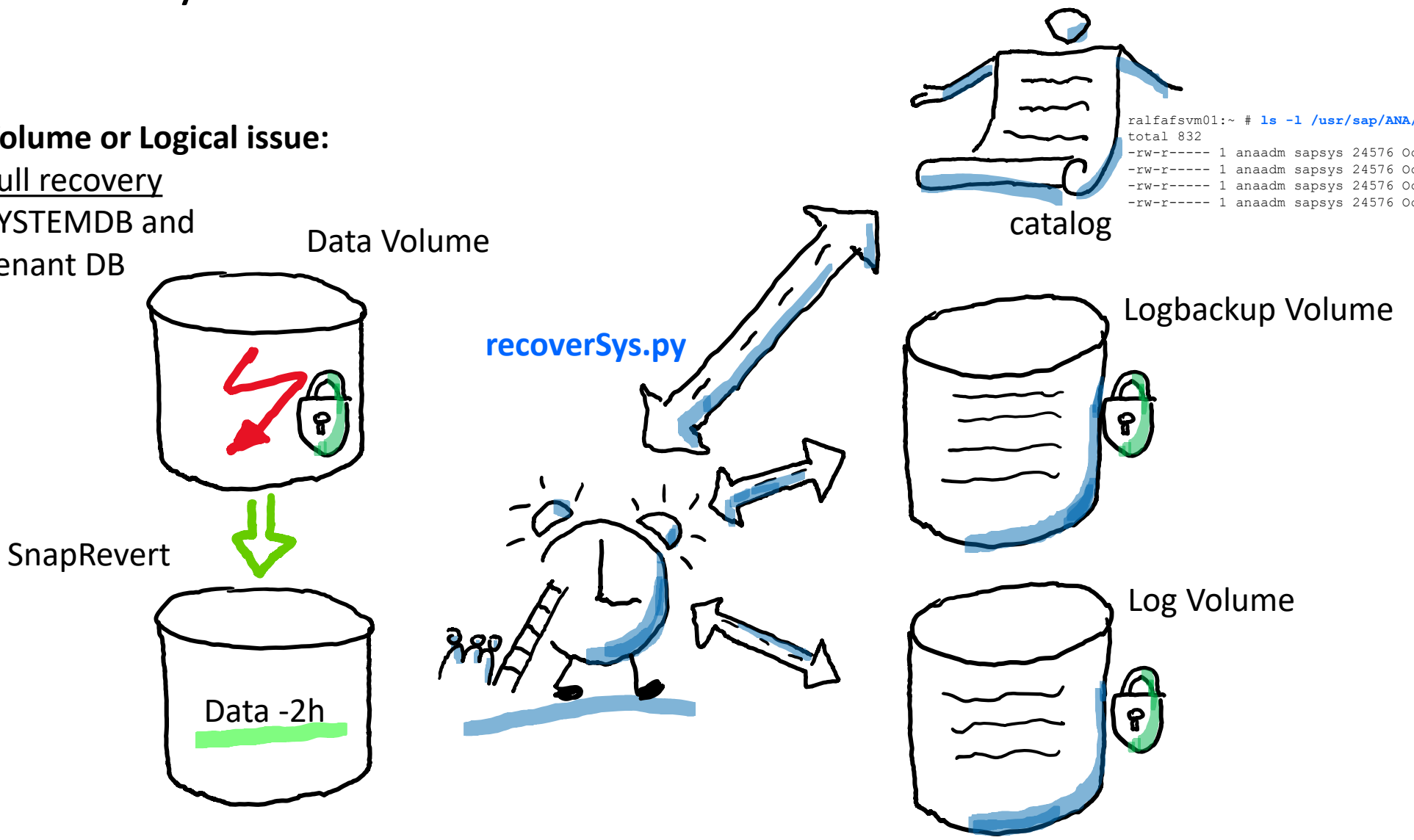


Recovery Process SYSTEMDB

Volume or Logical issue:

Full recovery

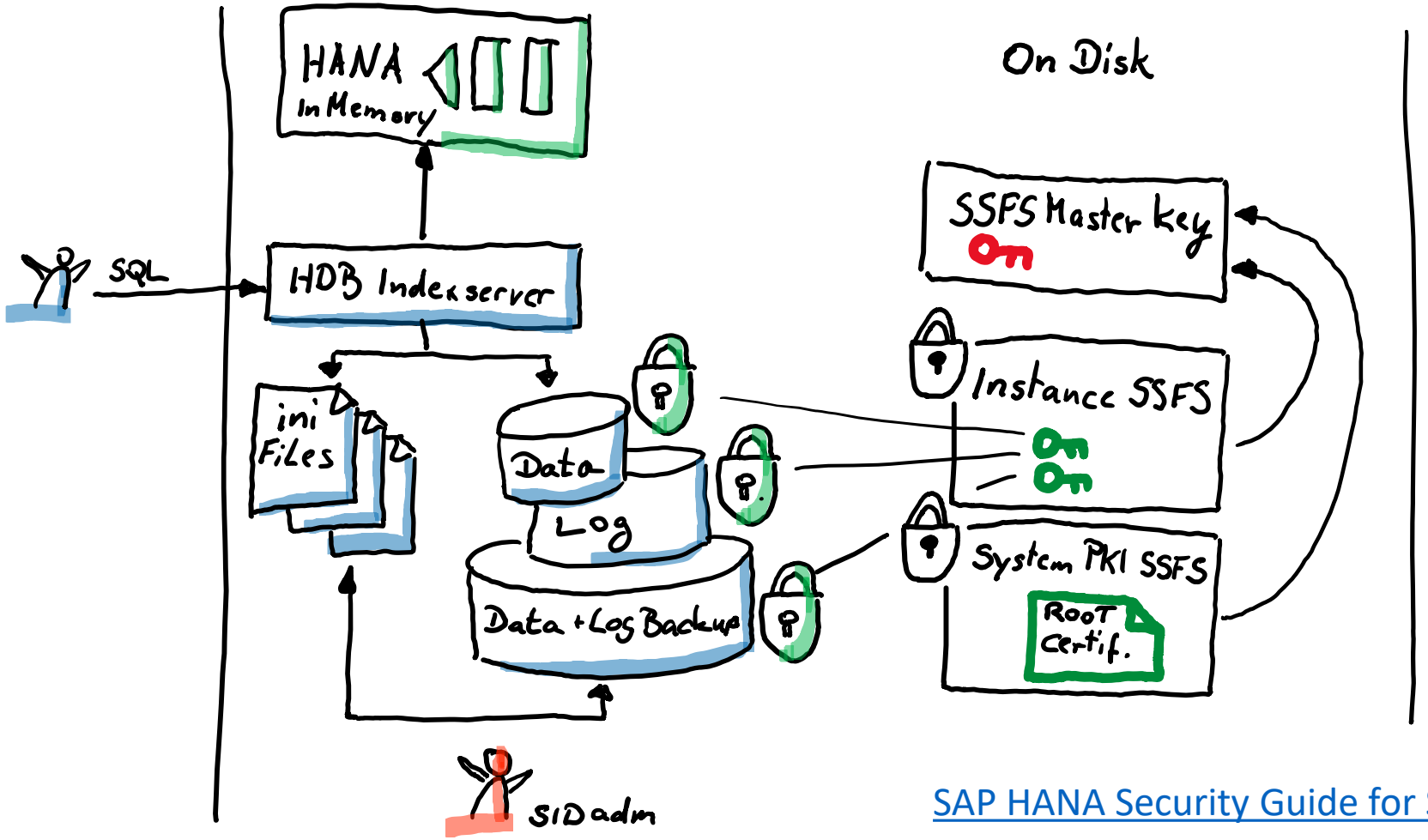
SYSTEMDB and Tenant DB




```
ralfafsvm01:~ # ls -l /usr/sap/ANA/HDB00/backup/log/SYSTEMDB
total 832
-rw-r----- 1 anaadm sapsys 24576 Oct  5 08:06 log_backup_0_0_0_0.16015608
-rw-r----- 1 anaadm sapsys 24576 Oct  5 08:06 log_backup_0_0_0_0.16011961
-rw-r----- 1 anaadm sapsys 24576 Oct  5 08:06 log_backup_0_0_0_0.16051086
-rw-r----- 1 anaadm sapsys 24576 Oct  5 08:08 log_backup_0_0_0_0.16012858
```

Secure Store in the File System (SSFS)

SAP HANA uses two secure stores in the file system: the instance SSFS and the system PKI SSFS. The instance SSFS protects the root keys used for all data-at-rest encryption services and the internal application encryption service. The system PKI SSFS protects system-internal root certificates required for secure internal communication.



[SAP HANA Security Guide for SAP HANA Platform]

Default SSFS Config

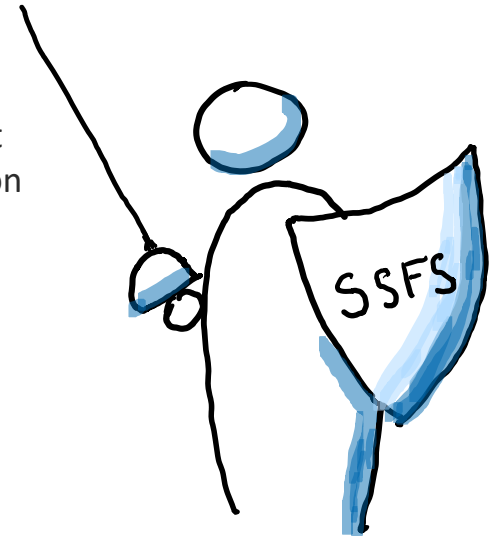
Server-Side Data Encryption
SAP HANA has a built-in encryption service to help manage the encryption of data hosted in the data and log volumes.
This service uses a *secure store in the file system* (SSFS) to protect the encryption root keys. Encryption root keys are the basis for all public or private keys used to encrypt data or communications within the SAP HANA system.

The instance SSFS key is stored on the OS in the following location by default:
`/usr/sap/<SID>/SYS/global/hdb/security/ssfs`

The system PKI SSFS key is stored on the OS in the following location by default:
`/usr/sap/<SID>/SYS/global/security/rsecssfs/data`

Configuring Authentication Between Sites (HSR)
To ensure that only configured systems in a system replication landscape can communicate with each other, SAP HANA uses certificate-based authentication based on the system PKI. To establish trust between systems, you must copy the system PKI SSFS data file and key file from the primary system to the same location on the secondary system(s). These files can be found at the following locations:

```
$DIR_INSTANCE/../SYS/global/security/rsecssfs/data/SSFS_.DAT
$DIR_INSTANCE/../SYS/global/security/rsecssfs/key/SSFS_.KEY
```



[Learn SAP HANA: Data Encryption (sap-press.com)]

Changing the Root Keys within an SSFS Config

A unique root key is generated during the standard installation or upgrade of each SAP HANA instance.
A standard installation is one in which a documented SAP HANA installation method is followed. However, because SAP HANA is often delivered as an appliance, it's possible that the appliance vendor used a copy of the same encryption root keys within each of its appliance builds.

- Generate new root keys using SQL commands.
- Backup the new keys and store them in a secure file location.
- Activate the new keys using SQL commands.

To establish this password, execute the following SQL statement:

```
ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD "<Password>";
```

To generate new root keys for the SAP HANA data volume, execute the following SQL command:

```
ALTER SYSTEM PERSISTENCE ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE;
```

To generate new root keys for the SAP HANA log volume, execute the following SQL command:

```
ALTER SYSTEM LOG ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE;
```

To generate new root keys for SAP HANA's internal application encryption, execute the following SQL command:

```
ALTER SYSTEM APPLICATION ENCRYPTION CREATE NEW ROOT KEY WITHOUT ACTIVATE;
```

Backup the Root Keys

```
./hdbnsutil -backupRootKeys <file path and name>.rkb --dbid=<dbid> --type='ALL'
```

[Learn SAP HANA: Data Encryption (sap-press.com)]

Changing the Root Keys within an SSFS Config

Before activating the new root keys, it's important to validate that you have the correct password required to restore the root keys.
To do so, execute the following command from the SAP HANA OS shell:

```
./hdbnsutil -validateRootKeysBackup <path to filename> --password="<password>"
```

When a backup is created with data and log volume encryption enabled, that backup can only be restored to a system with the same SSFS and root keys.
In the event that we need to restore a backup to a system with different root keys, we must first restore the root keys from the RKB file.
To recover root keys, execute the following command from the operating system shell;
you must be authenticated as the <sid>adm user to restore the root keys:

```
./hdbnsutil -recoverRootKeys <path to filename>.rkb --dbid=<dbid> --password="<password>" --type=ALL
```

Once the backup file is generated and validated, we can activate the new keys within the system. To activate the keys for all three areas, execute the following three statements:

```
ALTER SYSTEM PERSISTENCE ENCRYPTION ACTIVATE NEW ROOT KEY;
ALTER SYSTEM LOG ENCRYPTION ACTIVATE NEW ROOT KEY;
ALTER SYSTEM APPLICATION ENCRYPTION ACTIVATE NEW ROOT KEY;
```

To view the current and historical status of root keys generated within the system, query the ENCRYPTION_ROOT_KEYS system view. To query this view, execute the following SQL statement from the SQL console:

```
SELECT * FROM SYS.ENCRYPTION_ROOT_KEYS;
```

[Learn SAP HANA: Data Encryption (sap-press.com)]

Encrypting the Data- and Log Volume

There are two main ways to enable data volume encryption in SAP HANA: via a specialized SQL statement or via the security management options in SAP HANA Studio.

Using SQL
Note that you can't enable data volume encryption if extended storage has already been enabled within the system; you'll need to move extended storage tables back to in-memory and disable extended storage prior to executing the command successfully.
To enable data volume encryption, execute the following SQL command:

```
ALTER SYSTEM PERSISTENCE ENCRYPTION ON;
```

To monitor the status of data volume encryption, execute the following SQL statement:

```
SELECT * FROM SYS.M_ENCRYPTION_OVERVIEW
```

Encrypting the log volume is a feature that was first made available in SAP HANA 2.0 SPS 00. As of the time of writing, the log volume encryption can only be enabled using SQL commands. To enable log volume encryption, execute the following SQL command:

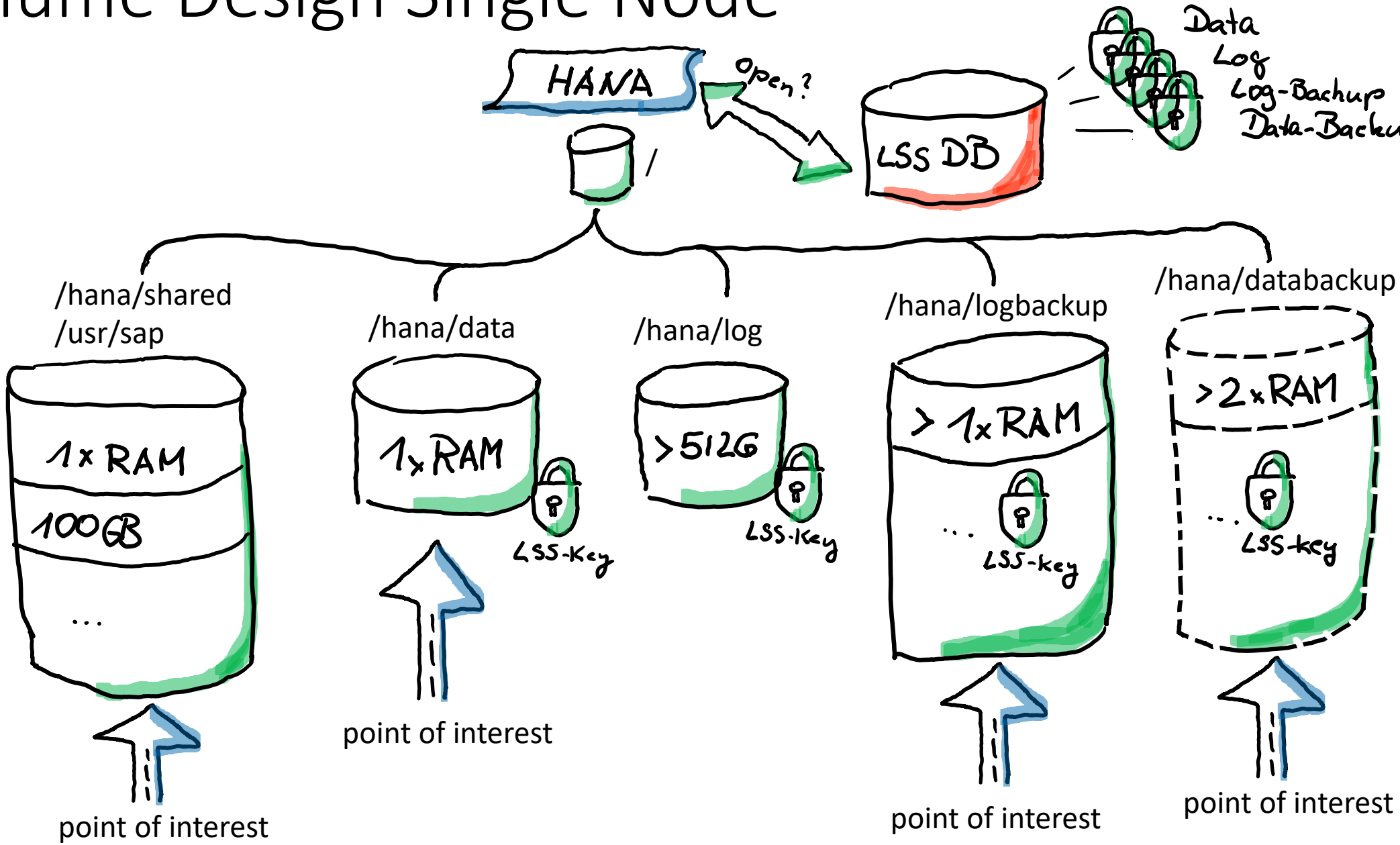
```
ALTER SYSTEM LOG ENCRYPTION ON;
```

To monitor the status of log volume encryption, execute the following SQL statement:

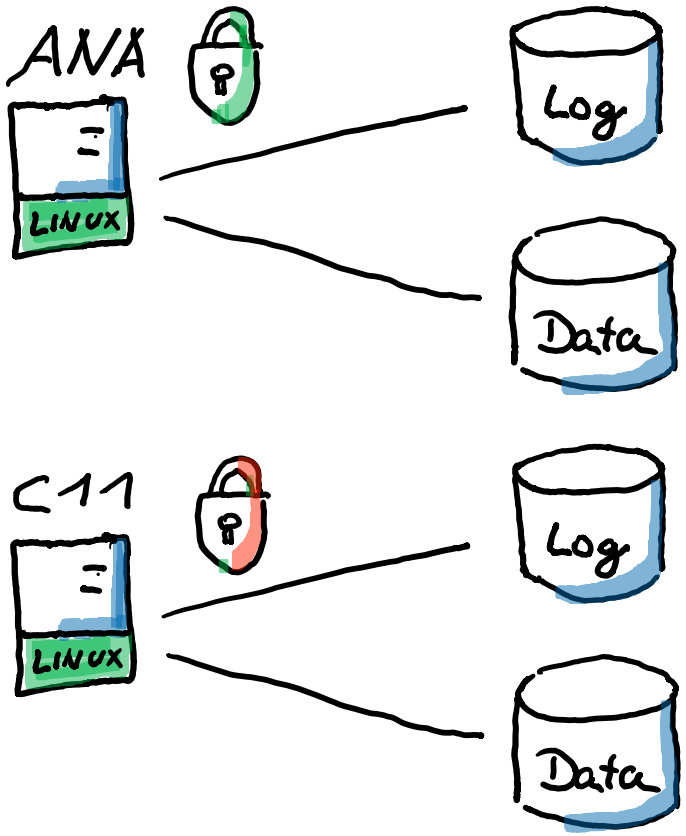
```
SELECT * FROM SYS.M_ENCRYPTION_OVERVIEW
```

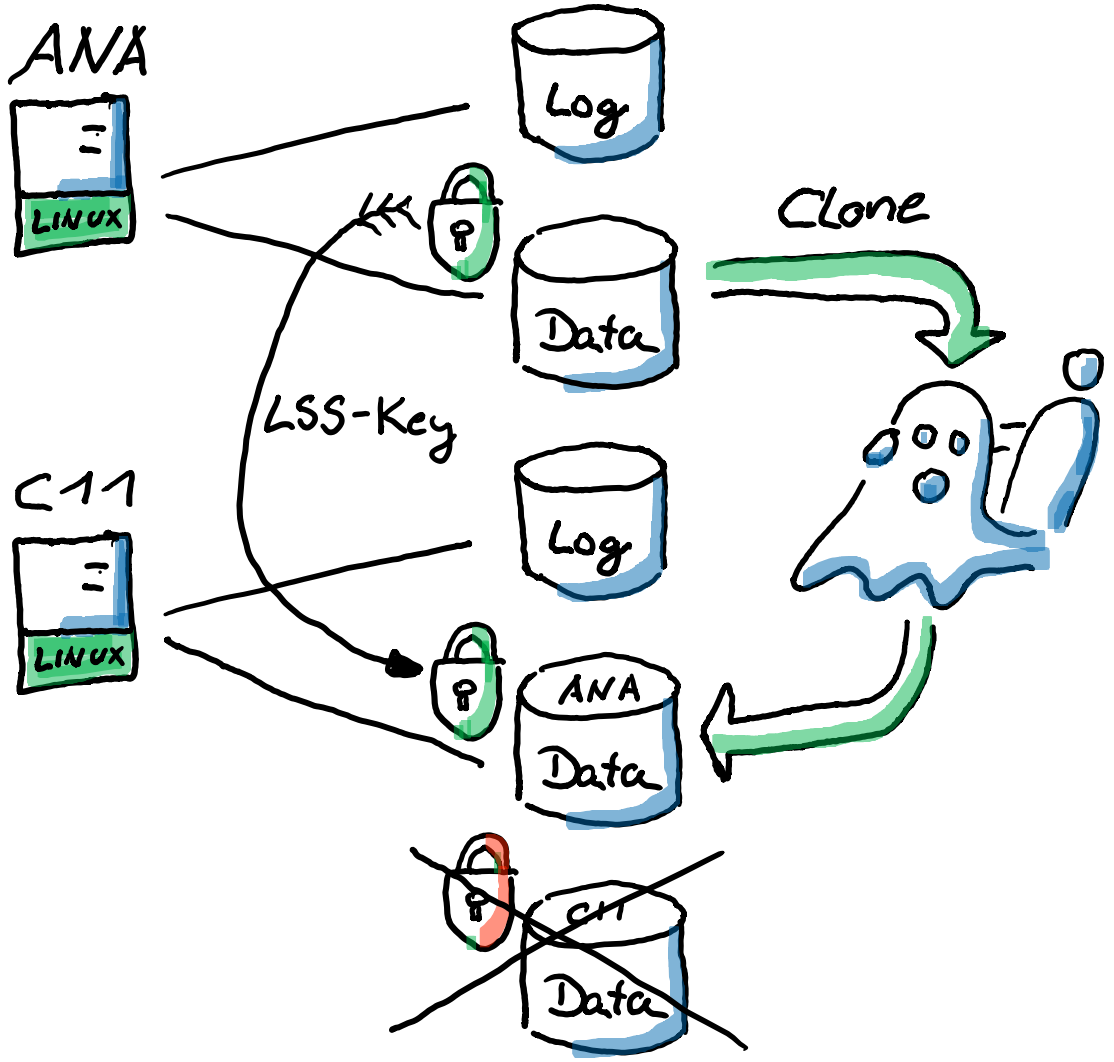
[Learn SAP HANA: Data Encryption (sap-press.com)]

Volume Design Single Node

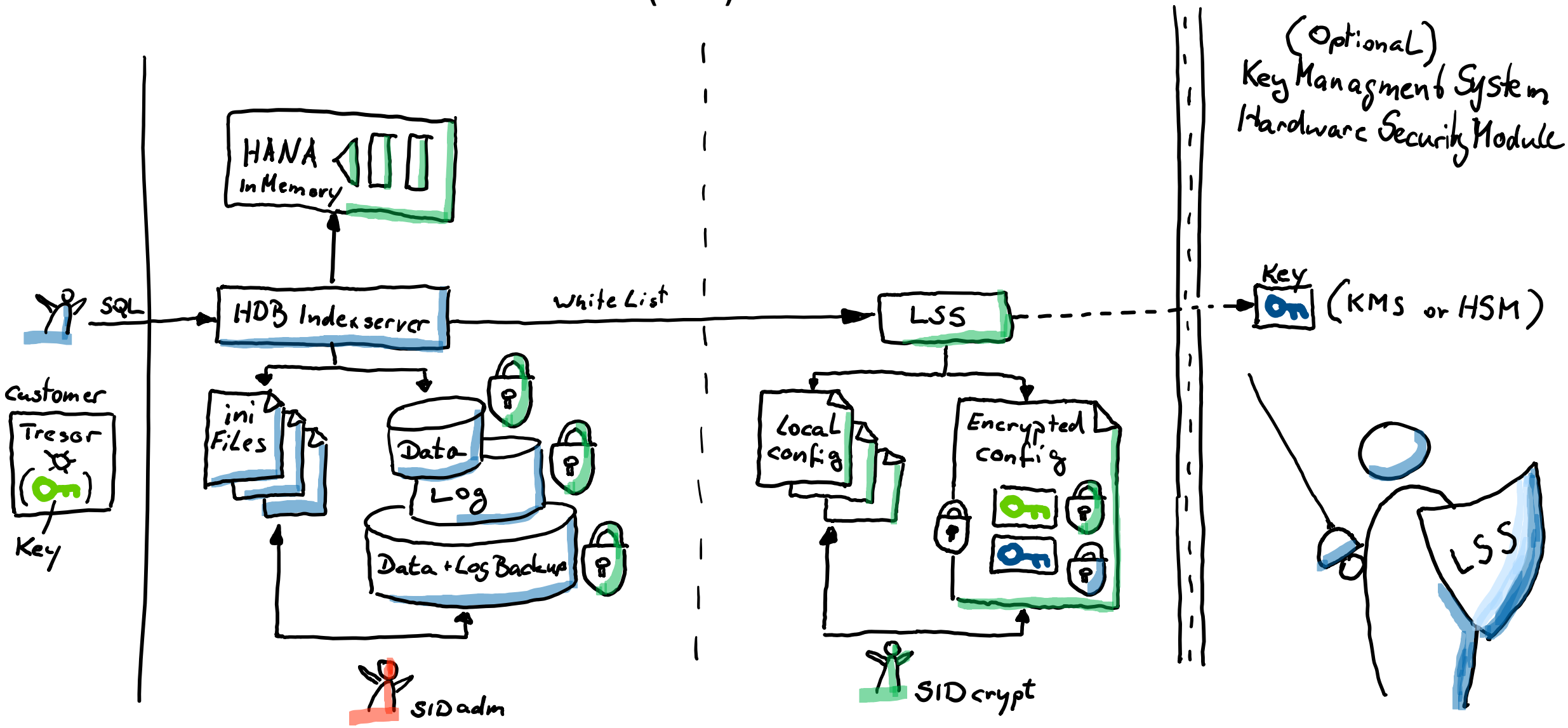


System Cloning / Snap to Volume





SAP HANA Local Secure Store (LSS)



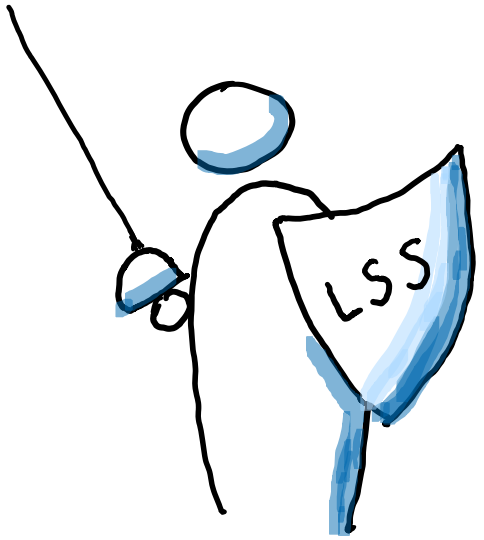
Install the LSS Componant

Download the LSS component from the SAP Marcetplace

```
SAPCAR -xf HDB_LSS_2_053_0-80004532.SAR

cd /hana/shared/ANA/hdblcm
./hdblcm --component_dirs=/Software/SAP_HANA_LSS/

SAP HANA Lifecycle Management - SAP HANA Database 2.00.052.00.1599235305
************************************************************************
Choose an action
Index | Action                       | Description
-------------------------------------------------------------------------------
...
14    | update_components            | Install or Update Additional Components

Enter selected action index [16]: 14  (Install or Update Additional Components)

Scanning software locations...
Detected components:
    SAP HANA Local Secure Store (2.4.29.0) in /Software/SAP_HANA_LSS/packages
…
```

switch the Encryption method from SSFS to LSS

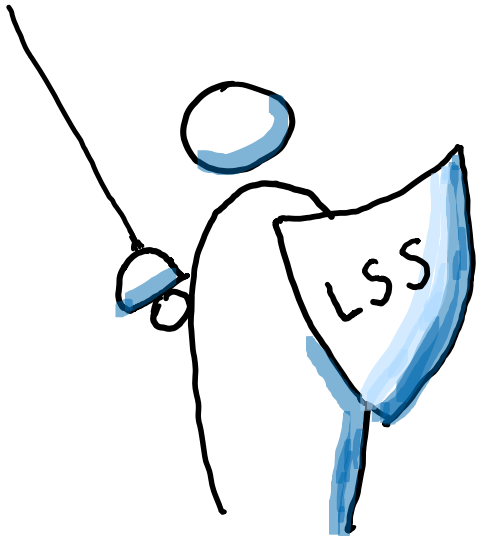
```
su - anaadm
sapcontrol -nr 00 -function StopSystem

hdbnsutil -migrateSecureStore --target=LSS
```



Install the LSS Componant on the Destination site

retrieve the DB-ID from HANA (Studio)

```
HDB info
USER          PID     PPID  %CPU        VSZ        RSS COMMAND
c11adm      22191    22190   0.0      20828       9208 -sh
c11adm       6343    22191   0.0      14124       3964  \_ /bin/sh /usr/sap/C11/HDB00/HDB info
c11adm       6374     6343   0.0      34888       3568      \_ ps fx -U c11adm -o user:8,pid:8,ppid:8,pcpu:5,vsz:10
c11adm       5002        1   0.0     715800      50976 hdbrsutil  --start --port 30003 --volume 3 --volumesuffix
c11adm       2694        1   0.0     715748      53192 hdbrsutil  --start --port 30001 --volume 1 --volumesuffix
c11adm       1572        1   0.0      23068       3092 sapstart pf=/usr/sap/C11/SYS/profile/C11_HDB00_ralfafsvm02
c11adm       1581     1572   0.1     466868      79192  \_ /usr/sap/C11/HDB00/ralfafsvm02/trace/hdb.sapC11_HDB00
c11crypt     1607     1581   0.4    1225148     101352      \_ lss {Controller}
c11crypt     1629     1607   0.4    1222588      99004      |   \_ lss [C11]
c11crypt     1631     1607   0.3    1218748      90360      |   \_ lss [SYSTEMDB]
c11adm       1611     1581  34.3    5978328    3037388      \_ hdbnameserver
c11adm       3227     1581   0.4    1486980     159180      \_ hdbcompileserver
c11adm       3230     1581   0.4    1755320     186784      \_ hdbpreprocessor
c11adm       3278     1581  46.3    6299284    3224848      \_ hdbindexserver -port 30003
c11adm       3281     1581   2.9    4633100    1314432      \_ hdbxsengine -port 30007
c11adm       5350     1581   1.4    3478612     634064      \_ hdbwebdispatcher
c11adm       1962        1   0.0     634964      37832 /usr/sap/C11/HDB00/exe/sapstartsrv
c11adm
c11adm       1873        1   0.0      72220       7928 /usr/lib/systemd/systemd --user
c11adm       1874     1873   0.0     117072       2572  \_ (sd-pam)
```

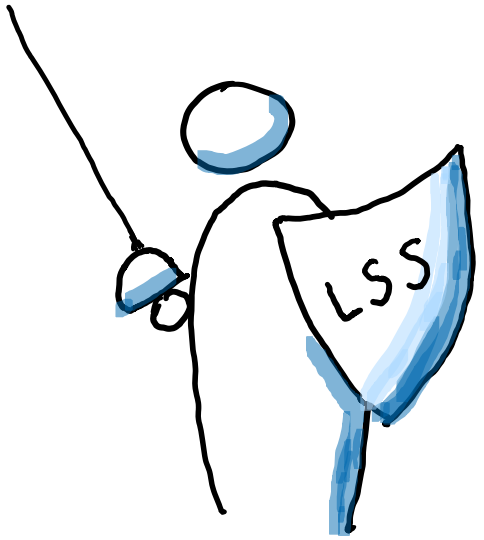


Install the LSS Componant

Download the LSS component from the SAP Marcetplace

```
sapcontrol -nr 00 -function StartSystem
```

```
anaadm@ralfafsvm01:/usr/sap/ANA/SYS/global/hdb/custom/config> HDB info
USER          PID     PPID  %CPU        VSZ        RSS COMMAND
anaadm       1452     1451   0.0      21368       9700 -sh
anaadm      10196     1452   0.0      14128       3900  \_ /bin/sh /usr/sap/ANA/HDB00/HDB info
anaadm      10227    10196   0.0      34888       3552      \_ ps fx -U anaadm -o user:8,pid:8,ppid:8,pcpu:5,vsz:10,rss:10,args
anaadm       5180        1   0.0      23068       3072 sapstart pf=/usr/sap/ANA/SYS/profile/ANA_HDB00_ralfafsvm01
anaadm       5187     5180   0.6     470592      80436  \_ /usr/sap/ANA/HDB00/ralfafsvm01/trace/hdb.sapANA_HDB00
anacrypt     5215     5187   0.6    1227708     102400      \_ lss {Controller}
anacrypt     5235     5215   0.6    1221308      94692      |   \_ lss [AN1]
anacrypt     5237     5215   0.6    1221308      99928      |   \_ lss [ANA]
anacrypt     5239     5215   0.6    1220028      92072      |   \_ lss [SYSTEMDB]
anaadm       5218     5187  50.7    6228816    3215404      \_ hdbnameserver
anaadm       7210     5187   1.0    1486984     154096      \_ hdbcompileserver
anaadm       7213     5187   1.3    1754040     178596      \_ hdbpreprocessor
anaadm       7263     5187  97.8    6672660    3453820      \_ hdbindexserver -port 30040
anaadm       7266     5187   111    7070484    4074732      \_ hdbindexserver -port 30003
anaadm       7269     5187  14.1    4891448    1273024      \_ hdbxsengine -port 30007
anaadm      10061     5187  19.0    3476048     635108      \_ hdbwebdispatcher
anaadm     102235        1   0.0     715800      53420 hdbrsutil  --start --port 30003 --volume 2
anaadm     102233        1   0.0     715804      50812 hdbrsutil  --start --port 30040 --volume 2
anaadm     101709        1   0.0     715744      53368 hdbrsutil  --start --port 30001 --volume 1
anaadm     100984        1   0.0     568324      35844 /usr/sap/ANA/HDB00/exe/sapstartsrv
anaadm     100894        1   0.0      72104       7912 /usr/lib/systemd/systemd --user
anaadm     100895   100894   0.0     227940     113092  \_ (sd-pam)
```



Install the LSS Componant

retrieve the DB-ID from HANA (Studio)

```
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);
```

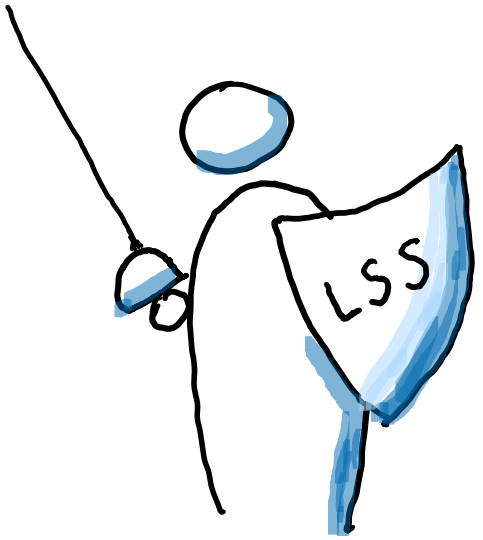
	DATABASE_NAME	DATABASE_ID
1	AN1	4
2	ANA	3
3	SYSTEMDB	1

```
ALTER SYSTEM ENCRYPTION CONFIGURATION CONTROLLED BY LOCAL DATABASES;
```
(on SYSTEMDB)

```
ALTER SYSTEM SET ENCRYPTION ROOT KEYS BACKUP PASSWORD "XXXXXXXXX"
```
(on every TenantDB)

Backup and validate the root-key

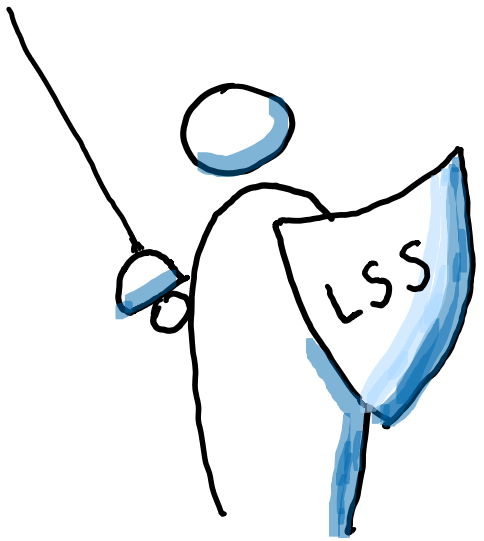
```
hdbnsutil -backupRootKeys ANA-tenant-backup-root-keys.rkb --dbid=3
done.
hdbnsutil -backupRootKeys AN1-tenant-backup-root-keys.rkb --dbid=4
done.
hdbnsutil -ValidateRootKeysBackup ANA-tenant-backup-root-keys.rkb
Please Enter the password:
hdbnsutil -ValidateRootKeysBackup AN1-tenant-backup-root-keys.rkb
Please Enter the password:
```



Install the LSS Componant on the Destination site

retrieve the DB-ID from HANA (Studio)

```
HDB info
hdbsql -u system -p <password> -n localhost:30013
hdbsql SYSTEMDB=> alter system stop database c11
hdbsql SYSTEMDB=> rename database c11 to ana
hdbsql SYSTEMDB=> alter system start database ana
hdbsql SYSTEMDB=> create database an1 system user password "<password>";

HDB info
USER          PID     PPID  %CPU        VSZ        RSS COMMAND
c11adm      22191    22190   0.0      20828       9208 -sh
c11adm      15490    22191   0.0      14124       3880  \_ /bin/sh /usr/sap/C11/HDB00/HDB info
c11adm      15521    15490   0.0      34888       3496      \_ ps fx -U c11adm -o user:8,pid:8
c11adm      13308        1   0.0     716080      53212 hdbrsutil  --start --port 30040
c11adm       5002        1   0.0     715800      50976 hdbrsutil  --start --port 30003
c11adm       2694        1   0.0     715748      53192 hdbrsutil  --start --port 30001
c11adm       1572        1   0.0      23068       3092 sapstart pf=/usr/sap/C11/SYS/profile
c11adm       1581     1572   0.0     466868      79216  \_ /usr/sap/C11/HDB00/ralfafsvm02/
c11crypt     1607     1581   0.4    1226428     117392      \_ lss {Controller}
c11crypt     1631     1607   0.3    1218748      90624      |   \_ lss [SYSTEMDB]
c11crypt     9325     1607   0.4    1221308      95748      |   \_ lss [ANA]
c11crypt    11980     1607   0.5    1220028     100820      |   \_ lss [AN1]
c11adm       1611     1581   8.3    5978328    3099680      \_ hdbnameserver
c11adm       3227     1581   0.3    1488260     165604      \_ hdbcompileserver
c11adm       3230     1581   0.4    1755320     188960      \_ hdbpreprocessor
```



Install the LSS Componant on the Destination site

Stop the DB and unmount the “old” data-volume.

```
HDB stop

umount /hana/data/C11/mnt00001
```

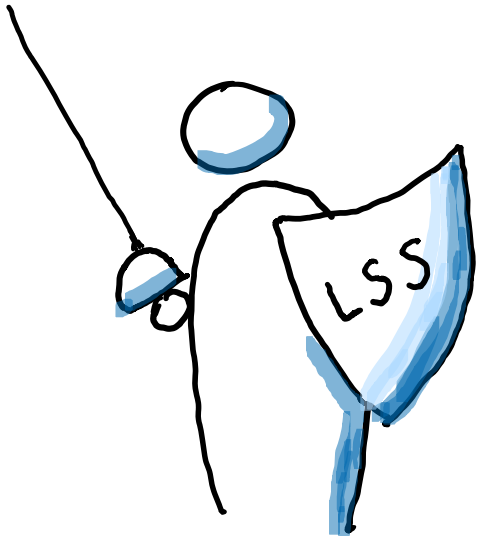
Clone the volume fron a Source DB snapshot and mount the „cloned“ volume into the data path.

```
ralfafsvm02:~ # mount -a
ralfafsvm02:~ # df -h
...
..
10.4.2.4:/ralfanfclone02       101T   11G  100T   1% /hana/data/C11/mnt00001
```

← new (cloned) Data Volume

Copy the root-keys from the source to the target side.

```
cd /usr/sap/C11/HDB00

scp root@ralfafsvm01:/usr/sap/ANA/HDB00/*.rkb .
root@ralfafsvm01's password:

AN1-tenant-backup-root-keys.rkb                100% 1440   434.2KB/s   00:00
ANA-tenant-backup-root-keys.rkb                100% 1440   610.1KB/s   00:00
```



Install the LSS Componant on the Destination site

Import the root keys from the source system to the target system

For Database ANA

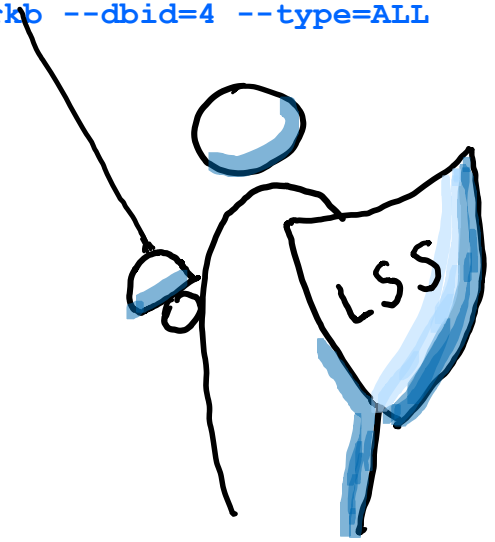
```
c11adm@ralfafsvm02:/usr/sap/C11/HDB00> hdbnsutil -recoverRootKeys ANA-tenant-backup-root-keys.rkb --dbid=3 --type=ALL
Please Enter the password:XXX
nameserver ralfafsvm02:30001 not responding.
nameserver ralfafsvm02:30001 not responding.
Importing root keys for DBID: 3 from /hana/shared/C11/HDB00/ANA-tenant-backup-root-keys.rkb
Successfully imported root keys from /hana/shared/C11/HDB00/ANA-tenant-backup-root-keys.rkb
done.
```

For database AN1

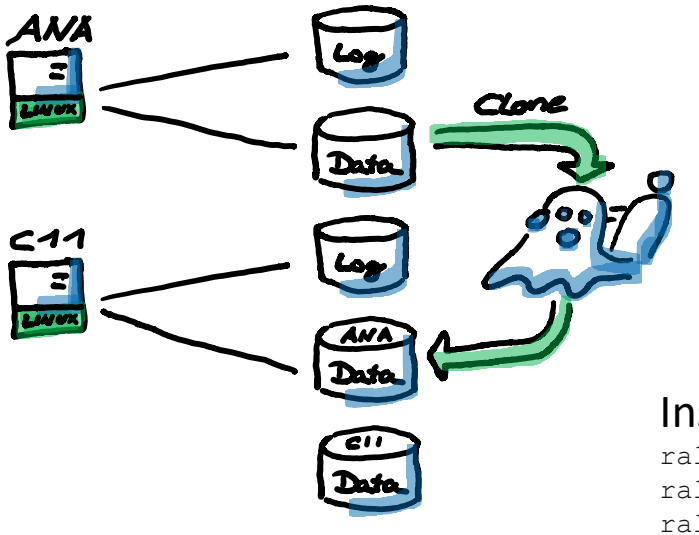
```
c11adm@ralfafsvm02:/usr/sap/C11/HDB00> hdbnsutil -recoverRootKeys AN1-tenant-backup-root-keys.rkb --dbid=4 --type=ALL
Please Enter the password:XXX
nameserver ralfafsvm02:30001 not responding.
nameserver ralfafsvm02:30001 not responding.
Importing root keys for DBID: 4 from /hana/shared/C11/HDB00/AN1-tenant-backup-root-keys.rkb
Successfully imported root keys from /hana/shared/C11/HDB00/AN1-tenant-backup-root-keys.rkb
done.
```

Change the access rights to the data volume (as root)

```
ralfafsvm02:~ # chown -R c11adm:sapsys /hana/data
```



System Cloning / Snap 2 Volume / CLI




```
az netappfiles snapshot list -g ralfAFSrg --account-name ralfanftest01 --pool-name
ralfanf01 --volume-name ralfanfdata01

az netappfiles volume create -g ralfAFSrg --account-name ralfanftest01 --pool-name ralfanf01 -
-name ralfanfclone01 --location  centraluseuap --usage-threshold 512 --service-level premium -
-vnet ralfAFSnw --subnet ralfanfsubnet --file-path "ralfanfclone01" --protocol-types NFSv4.1 -
-snapshot-id 362ce440-a082-b14d-d22a-43109d542cc9
```

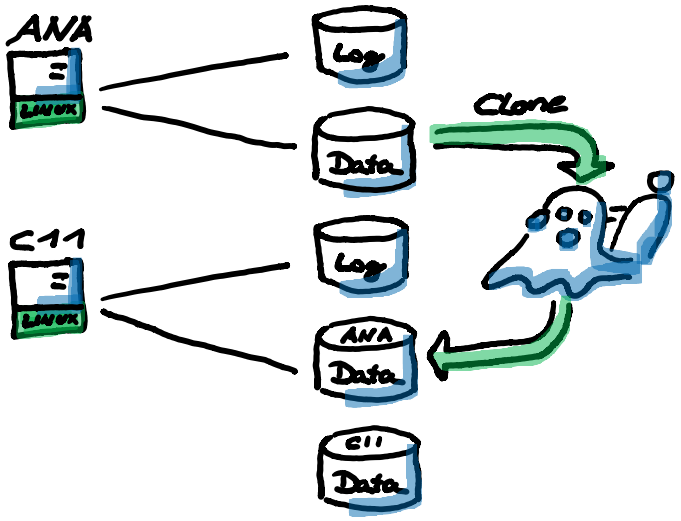
Install HANA on the second node

```
ralfafsvm02:/Software # zypper install insserv
ralfafsvm02:/Software # cd SAP_HANA_DATABASE/
ralfafsvm02:/Software/SAP_HANA_DATABASE # ./hdblcm --ignore=check_signature_file
```

Shutdown HANA and mount the Clone of the data volume from ANA

```
ralfafsvm02:/Software # su - c11adm
c11adm@ralfafsvm02:/usr/sap/C11/HDB00> sapcontrol -nr 00 -function StopSystem  , exit
ralfafsvm02:~ # umount /hana/data/C11/mnt00001
ralfafsvm02:~ # mount /hana/data/C11/mnt00001     # after changing /etc/fstab for data
ralfafsvm02:~ # df -h
Filesystem                      Size  Used Avail Use% Mounted on
10.4.2.5:/ralfanflog01/C11      1.1T  7.8G 1020G   1% /hana/log/C11/mnt00001
10.4.2.5:/ralfanfbackup01/C11   514G  3.9G  510G   1% /hana/backup/C11
10.4.2.5:/ralfanfshared01/C11   1.1T   20G 1016G   2% /hana/shared/C11
10.4.2.5:/ralfanfclone01        515G  6.6G  509G   2% /hana/data/C11/mnt00001
```

System Cloning / Snap 2 Volume / CLI



After mounting the cloned volume we need to recover HANA

SYSTEMDB first

```
ralfafsvm02:/ # chown -R c11adm:sapsys /hana/data/C11


ralfafsvm02:/Software # su - c11adm
c11adm@ralfafsvm02:/usr/sap/C11/HDB00> cd exe/python_support
c11adm@ralfafsvm02:/usr/sap/C11/HDB00/exe/python_support>
                                    python recoverSys.py --command="RECOVER DATA USING SNAPSHOT CLEAR LOG"
...
sapcontrol returned successfully:
2020-10-08T12:50:48+00:00  P0018658      1750843342f INFO    RECOVERY RECOVER DATA finished successfully
```

Then Recover the TenantDB with SID change from ANA to C11

```
c11adm@ralfafsvm02:/usr/sap/C11/HDB00/exe/python_support> hdbsql -u system -p <pwd> -n localhost:30013
hdbsql SYSTEMDB=> recover data for C11 using snapshot clear log
0 rows affected (overall time 61.742062 sec; server time 61.739634 sec)

hdbsql SYSTEMDB=> exit
```


Thank You