SAP HANA Replication and SUSE HA Security
Best Practice
2 April 2019

Tinus Brink
Consulting Director
SAB&T TEC / tbrink@sabttec.com
How Much Is Your Data Worth?
The Cost of Non-Secure Data Could be High

- Your data is your most valuable asset – it is what your business depends on
- We understand the impact of data loss due to natural or man-made disasters
- What is your data worth to 3rd parties?
  - Personal Data
  - Financial Information
  - Health Information
  - Intellectual Property
  - Legal Information
  - Login Data

- What would be the impact on your business if your hardware was stolen or compromised?
  - Reputational risk, notify everyone whose data has been compromised
  - Contractual agreements and obligations
  - Penalties for business depending on Jurisdiction
  - Compensation for damages with possible lawsuits
  - Shares of a company or planned sale could be jeopardized
The Cost of Non-Secure Data Could be High

• Your data is the most valuable asset you have – it is what your business depends on
• We understand the impact of data loss due to natural or man-made disasters
The Cost of Non-Secure Data Could be High

• Your data is the most valuable asset you have – it is what your business depends on
• We understand the impact of data loss due to natural or man-made disasters
• What is your data worth to 3rd parties
  • Personal Data
  • Financial Information
  • Health Information
  • Intellectual Property
  • Legal Information
  • Login Data
The Cost of Non-Secure Data Could be High

- Your data is the most valuable asset you have – it is what your business depends on
- We understand the impact of data loss due to natural or man-made disasters
- What is your data worth to 3rd parties
  - Personal Data
  - Financial Information
  - Health Information
  - Intellectual Property
  - Legal Information
  - Login Data
- What would the impact on your business be should your hardware get stolen or compromised?
  - Reputational Risk, Notify everyone whose data has been compromised
  - Contractual Agreements and obligations
  - Penalties for Business depending on Jurisdiction
  - Compensation for Damages with possible lawsuits
  - Shares of a company or planned sale could be jeopardized
SAP HANA – Stolen Data Scenario

• Datacentre breach

• Possible stolen backups
• Possible stolen server (whole blade or rack)
• Possible stolen hard drives (decommissioned, replaced or new)

Any of the above mentioned scenarios could leave your data compromised

• SAP HANA SYSTEM user can be used as a super user to get all data back
• Performing the RESET SYSTEM User procedure could enable anyone to get hold of your data

What is the answer to the problem?

• Protect your data using security implemented from SUSE and SAP
SAP HANA – Stolen Data Scenario

- Datacentre breach
  - Possible stolen backups
  - Possible stolen server (whole blade or rack)
  - Possible stolen hard drives (decommissioned, replaced or new)
SAP HANA – Stolen Data Scenario

• Datacentre breach
  • Possible stolen backups
  • Possible stolen server (whole blade or rack)
  • Possible stolen hard drives (decommissioned, replaced or new)

• Any of these scenarios could leave your data compromised

• SAP HANA SYSTEM user can be used as a super user to get all data back
  • Performing the RESET SYSTEM User procedure could enable anyone to get hold of your data

• What is the answer to the problem?

• Protect your data using security implemented from SUSE and SAP
SAP HANA – Stolen Data Scenario

• Datacentre breach
  • Possible stolen backups
  • Possible stolen server (whole blade or rack)
  • Possible stolen hard drives (decommissioned, replaced or new)

• Any of these scenarios could leave your data compromised
• SAP HANA SYSTEM user can be used as a super user to get all data back
SAP HANA – Stolen Data Scenario

- Datacentre breach
  - Possible stolen backups
  - Possible stolen server (whole blade or rack)
  - Possible stolen hard drives (decommissioned, replaced or new)

- Any of these scenarios could leave your data compromised
- SAP HANA SYSTEM user can be used as a super user to get all data back
- Performing the RESET SYSTEM User procedure could enable anyone to get hold of your data

- Protect your data using security implemented from SUSE and SAP
SAP HANA – Stolen Data Scenario

• Datacentre breach
  • Possible stolen backups
  • Possible stolen server (whole blade or rack)
  • Possible stolen hard drives (decommissioned, replaced or new)

• Any of these scenarios could leave your data compromised
• SAP HANA SYSTEM user can be used as a super user to get all data back
• Performing the RESET SYSTEM User procedure could enable anyone to get hold of your data

• What is the answer to the problem?
SAP HANA – Stolen Data Scenario

- Datacentre breach
  - Possible stolen backups
  - Possible stolen server (whole blade or rack)
  - Possible stolen hard drives (decommissioned, replaced or new)

- Any of these scenarios could leave your data compromised

- SAP HANA SYSTEM user can be used as a super user to get all data back

- Performing the RESET SYSTEM User procedure could enable anyone to get hold of your data

- What is the answer to the problem?

- Protect your data using security implemented from SUSE and SAP
SUSE Linux Enterprise Server Security – cryptctl
Secure SAP HANA with cryptctl

- **cryptctl Client**
  - Waits for kernel notification that a disk was attached
  - Sends RPC request to retrieve encryption key
  - Uses key to mount partition

- **cryptctl Server**
  - Listens for RPC requests over TCP
  - Records request in system journal
  - Responds to RPC request with partition key
Cryptctl Server in Demo, hostname = centralhost

**cryptctl Client**
- Waits for kernel notification that a disk was attached
- Sends RPC request to retrieve encryption key
- Uses key to mount partition

**cryptctl Server**
- Listens for RPC requests over TCP
- Records request in system journal
- Responds to RPC request with partition key

**centralhost**
Host: hanahost1 Is the Primary SAP HANA Server

**cryptctl Client**
- Waits for kernel notification that a disk was attached
- Sends RPC request to retrieve encryption key
- Uses key to mount partition

**cryptctl Server**
- Listens for RPC requests over TCP
- Records request in system journal
- Responds to RPC request with partition key

Hanahost1

Centralhost
Host: hanahost2 Is the Replicated SAP HANA Server

cryptctl Client

hanahost1

hanahost2

Waits for kernel notification that a disk was attached

Sends RPC request to retrieve encryption key

Uses key to mount partition

cryptctl Server

centralhost

Listens for RPC requests over TCP

Records request in system journal

Responds to RPC request with partition key
SLES Firewall, Permanent Rule for cryptctl on Keyserver
SLES Firewall, Port and Protocol configure port 3737

- Make sure the rule is also set up as runtime on firewall
Configure cryptctl (Keyserver) 1/3

centralhost:~ # zypper install -y cryptctl
configure cryptctl (keyserver) 1/3

centralhost:~ # zypper install -y cryptctl
Refreshing service 'basesystem_module_15_x86_64'.
Refreshing service 'desktop_applications_module_15_x86_64'.
Refreshing service 'sap_applications_module_15_x86_64'.
Refreshing service 'suse_linux_enterprise_high_availability_extension_15_x86_64'.
Refreshing service 'suse_linux_enterprise_server_for_sap_applications_15_x86_64'.
Refreshing service 'server_applications_module_15_x86_64'.
Retrieving repository 'sle-module-basesystem15-updates' metadata ........................................... [done]
Building repository 'sle-module-basesystem15-updates' cache ............................................................ [done]
Retrieving repository 'sle-module-desktop-applications15-updates' metadata ........................................... [done]
Building repository 'sle-module-desktop-applications15-updates' cache ................................................... [done]
Retrieving repository 'sle-module-server-applications15-updates' metadata ........................................... [done]
Building repository 'sle-module-server-applications15-updates' cache ................................................... [done]
Loading repository data...
Reading installed packages...
Resolving package dependencies...

the following new package is going to be installed:
   cryptctl

1 new package to install.
Overall download size: 1.8 MiB. Already cached: 0 B. After the operation, additional 6.3 MiB will be used.
Continue? [y/n/...? shows all options] (y): y
Retrieving package cryptctl-2.3-2.40.x86_64 (1/1), 1.8 MiB ( 6.3 MiB unpacked)
Retrieving: cryptctl-2.3-2.40.x86_64.rpm .......................................................... [done (288.0 KiB/s)]
Checking for file conflicts: ...............................................................[done]
(1/1) Installing: cryptctl-2.3-2.40.x86_64 ..........................................................[done]
Additional rpm output:
Updating /etc/sysconfig/cryptctl-server ...
Updating /etc/sysconfig/cryptctl-client ...
Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):
Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):
Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value. Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(leave blank to auto-generate self-signed certificate):
centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:

Configure cryptctl (Keyserver) 2/3

```
centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:
Generating certificate...

Self-signed certificate has been generated for host name "centralhost.sabttec.com":
/etc/cryptctl/servertls/centralhost.sabttec.com.crt
/etc/cryptctl/servertls/centralhost.sabttec.com.key
```

Important notes for client computers:
- They must have a copy of certificate file "centralhost.sabttec.com.crt" to communicate securely with this server.
- In cryptctl commands, the key server's host name must use "centralhost.sabttec.com".
- When cryptctl commands ask for key server's CA, they must be given "/path/to/centralhost.sabttec.com.crt".
- Consult manual page cryptctl(8) section Communication Security for more information.

IP address for the server to listen on (0.0.0.0 to listen on all network interfaces) [0.0.0.0]:
configure cryptctl (keyservers) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:
Generating certificate...

Self-signed certificate has been generated for host name "centralhost.sabttec.com":
/etc/cryptctl/servertls/centralhost.sabttec.com.crt
/etc/cryptctl/servertls/centralhost.sabttec.com.key

Important notes for client computers:
- They must have a copy of certificate file "centralhost.sabttec.com.crt" to communicate securely with this server.
- In cryptctl commands, the key server's host name must use "centralhost.sabttec.com".
- When cryptctl commands ask for key server's CA, they must be given "/path/to/centralhost.sabttec.com.crt".
- Consult manual page cryptctl(8) section Communication Security for more information.

IP address for the server to listen on (0.0.0.0 to listen on all network interfaces) [0.0.0.0]:
TCP port number to listen on [3737]:
Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value. Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file 
(leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:
Generating certificate...

Self-signed certificate has been generated for host name "centralhost.sabttec.com":
/etc/cryptctl/servertls/centralhost.sabttec.com.crt
/etc/cryptctl/servertls/centralhost.sabttec.com.key

Important notes for client computers:
- They must have a copy of certificate file "centralhost.sabttec.com.crt" to communicate securely with this server.
- In cryptctl commands, the key server's host name must use "centralhost.sabttec.com".
- When cryptctl commands ask for key server's CA, they must be given "/path/to/centralhost.sabttec.com.crt".
- Consult manual page cryptctl(8) section Communication Security for more information.

IP address for the server to listen on (0.0.0.0 to listen on all network interfaces) [0.0.0.0]:
TCP port number to listen on [3737]:
Key database directory [/var/lib/cryptctl/keydb]:
Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(Leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:
Generating certificate...

Self-signed certificate has been generated for host name "centralhost.sabttec.com":
/etc/cryptctl/servertls/centralhost.sabttec.com.crt
/etc/cryptctl/servertls/centralhost.sabttec.com.key

Important notes for client computers:
- They must have a copy of certificate file "centralhost.sabttec.com.crt" to communicate securely with this server.
- In cryptctl commands, the key server's host name must use "centralhost.sabttec.com".
- When cryptctl commands ask for key server's CA, they must be given "/path/to/centralhost.sabttec.com.crt".
- Consult manual page cryptctl(8) section Communication Security for more information.

IP address for the server to listen on (0.0.0.0 to listen on all network interfaces) [0.0.0.0]:
TCP port number to listen on [3737]:
Key database directory [/var/lib/cryptctl/keydb]:
Should clients present their certificate in order to access this server? [no]:

Configure cryptctl (Keys server) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(Leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:
Generating certificate...

Self-signed certificate has been generated for host name "centralhost.sabttec.com":
/etc/cryptctl/server_tls/centralhost.sabttec.com.crt
/etc/cryptctl/server_tls/centralhost.sabttec.com.key

Important notes for client computers:
- They must have a copy of certificate file "centralhost.sabttec.com.crt" to communicate securely with this server.
- In cryptctl commands, the key server's host name must use "centralhost.sabttec.com".
- When cryptctl commands ask for key server's CA, they must be given "/path/to/centralhost.sabttec.com.crt".
- Consult manual page cryptctl(8) section Communication Security for more information.

IP address for the server to listen on (0.0.0.0 to listen on all network interfaces) [0.0.0.0]:
TCP port number to listen on [3737]:
Key database directory [/var/lib/cryptctl/keydb]:
Should clients present their certificate in order to access this server? [no]:
Should encryption keys be kept on a KMIP-compatible key management appliance? [no]:
Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(Leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:
Generating certificate...

Self-signed certificate has been generated for host name "centralhost.sabttec.com":
/etc/cryptctl/servertls/centralhost.sabttec.com.crt
/etc/cryptctl/servertls/centralhost.sabttec.com.key

Important notes for client computers:
- They must have a copy of certificate file "centralhost.sabttec.com.crt" to communicate securely with this server.
- In cryptctl commands, the key server's host name must use "centralhost.sabttec.com".
- When cryptctl commands ask for key server's CA, they must be given "/path/to/centralhost.sabttec.com.crt".
- Consult manual page cryptctl(8) section Communication Security for more information.

IP address for the server to listen on (0.0.0.0 to listen on all network interfaces) [0.0.0.0]:
TCP port number to listen on [3737]:
Key database directory [/var/lib/cryptctl/keydb]:
Should clients present their certificate in order to access this server? [no]:
Should encryption keys be kept on a KMIP-compatible key management appliance? [no]:

To enable Email notifications, enter the following parameters:
SMTP server name (not IP address) and port such as "example.com:25":

Configure cryptctl (Keyserver) 2/3

centralhost:~ # cryptctl init-server
Please enter value for the following parameters, or leave blank to accept the default value.
Access password (min. 10 chars, no echo):

Confirm access password (no echo):

PEM-encoded TLS certificate or a certificate chain file
(Leave blank to auto-generate self-signed certificate):
Host name for the generated certificate [centralhost.sabttec.com]:
Generating certificate...

Self-signed certificate has been generated for host name "centralhost.sabttec.com":
/etc/cryptctl/servertls/centralhost.sabttec.com.crt
/etc/cryptctl/servertls/centralhost.sabttec.com.key

Important notes for client computers:
- They must have a copy of certificate file "centralhost.sabttec.com.crt" to communicate securely with this server.
- In cryptctl commands, the key server's host name must use "centralhost.sabttec.com".
- When cryptctl commands ask for key server's CA, they must be given "/path/to/centralhost.sabttec.com.crt".
- Consult manual page cryptctl(8) section Communication Security for more information.

IP address for the server to listen on (0.0.0.0 to listen on all network interfaces) [0.0.0.0]:
TCP port number to listen on [3737]:
Key database directory [/var/lib/cryptctl/keydb]:
Should clients present their certificate in order to access this server? [no]:
Should encryption keys be kept on a KTMIP-compatible key management appliance? [no]:

To enable Email notifications, enter the following parameters:
SMTP server name (not IP address) and port such as "example.com:25":

Settings have been saved successfully!
Would you like to start key server (cryptctl-server) now? [yes]: yes
Configure cryptctl (Keyserver) 3/3

centralhost:~ # systemctl status cryptctl-server.service
Configure cryptctl (Keyserver) 3/3

centralhost:~ # systemctl status cryptctl-server.service
• cryptctl-server.service - Disk encryption utility (cryptctl) - key server
  Loaded: loaded (/usr/lib/systemd/system/cryptctl-server.service; enabled; vendor preset: disabled)
  Active: active (running) since Mon 2019-02-18 19:57:25 SAST; 395 ago
  Main PID: 23869 (cryptctl)
    Tasks: 7 (limit: 4915)
    CGroup: /system.slice/cryptctl-server.service
  23869 /usr/sbin/cryptctl daemon

Feb 18 19:57:25 centralhost systemd[1]: Started Disk encryption utility (cryptctl) - key server.
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 Email notifications are not enabled: [Recipient address]
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 GOMAXPROCS is currently: 4
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 CryptServer.ListenTCP: listening on 0.0.0.0:3737 using
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 CryptServer.ListenUnix: listening on /var/run/cryptctl-
Configure cryptctl (Keyserver) 3/3

```
centralhost:~ # systemctl status cryptctl-server.service
• cryptctl-server.service - Disk encryption utility (cryptctl) - key server
   Loaded: loaded (/usr/lib/systemd/system/cryptctl-server.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-02-18 19:57:25 SAST; 39s ago
Main PID: 23869 (cryptctl)
   Tasks: 7 (limit: 4915)
   CGroup: /system.slice/cryptctl-server.service
       23869 /usr/sbin/cryptctl daemon

Feb 18 19:57:25 centralhost systemd[1]: Started Disk encryption utility (cryptctl) - key server.
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 Email notifications are not enabled: [Recipient address]
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 GOMAXPROCS is currently: 4
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 CryptServer.ListenTCP: listening on 0.0.0.0:3737 using
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 CryptServer.ListenUnix: listening on /var/run/cryptctl-

centralhost:~ # cp /etc/cryptctl/servertls/centralhost.sabttec.com.crt /root/
```
Configure cryptctl (Keyserver) 3/3

```
centralhost:~ # systemctl status cryptctl-server.service
● cryptctl-server.service - Disk encryption utility (cryptctl) - key server
   Loaded: loaded (/usr/lib/systemd/system/cryptctl-server.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2019-02-18 19:57:25 SAST; 39s ago
   Main PID: 23869 (cryptctl)
   Tasks: 7 (limit: 4915)
   CGroup: /system.slice/cryptctl-server.service
          └── 23869 /usr/sbin/cryptctl daemon

Feb 18 19:57:25 centralhost systemd[1]: Started Disk encryption utility (cryptctl) - key server.
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 Email notifications are not enabled: [Recipient addresses]
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 GOMAXPROCS is currently: 4
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 CryptServer.ListenTCP: listening on 0.0.0.0:3737 using

centralhost:~ # cp /etc/cryptctl/servertls/centralhost.sabttec.com.crt /root/
centralhost:~ # scp /root/centralhost.sabttec.com.crt hanahost1:/root/
Password:

centralhost.sabttec.com.crt 100% 1273 1.3MB/s 00:00
```
Configure cryptctl (Keyserver) 3/3

```
centralhost:~ # systemctl status cryptctl-server.service
  ● cryptctl-server.service - Disk encryption utility (cryptctl) - key server
    Loaded: loaded (/usr/lib/systemd/system/cryptctl-server.service; enabled; vendor preset: disabled)
    Active: active (running) since Mon 2019-02-18 19:57:25 SAST; 395 ago
  Main PID: 23869 (cryptctl)
    Tasks: 7 (limit: 4915)
    CGroup: /system.slice/cryptctl-server.service
    └─23869 /usr/sbin/cryptctl daemon

Feb 18 19:57:25 centralhost systemd[1]: Started Disk encryption utility (cryptctl) - key server.
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 Email notifications are not enabled: [Recipient address]
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 GOMAXPROCS is currently: 4
Feb 18 19:57:25 centralhost cryptctl[23869]: 2019/02/18 19:57:25 CryptServer.ListenTCP: listening on 0.0.0.0:3737 using

centralhost:~ # cp /etc/cryptctl/servertls/centralhost.sabttec.com.crt /root/
centralhost:~ # scp /root/centralhost.sabttec.com.crt hanahost1:/root/
Password: centralhost.sabttec.com.crt
100% 1273  1.3MB/s  00:00
centralhost:~ # scp /root/centralhost.sabttec.com.crt hanahost2:/root/
Password: centralhost.sabttec.com.crt
100% 1273  1.3MB/s  00:00
```
Configure cryptctl (Client) 1/4

hanahost1:~ # lsblk -f
Configure cryptctl (Client) 1/4

```
hanahost1:~ # lsblk -f
NAME   FSTYPE LABEL  UUID                      MOUNTPOINT
sda     86fdee28-d919-43c2-b077-b3456efe170d [SWAP]       
sda2 swap 4d4b1c9f-16c6-4038-8922-b82556885df5  /          
sr0 iso9660 SLE-15-Installer-DVD-x86_64-001 /run/media/root/SLE-15-Installer-DVD
vda     0c2937bf-1be7-4751-8bbd-3038dbfa93ac /hana
vda1 xfs
vdb
vdb1
```
Configure cryptctl (Client) 1/4

```
hanahost1:~ $ lsblk -f
NAME  FSTYPE  LABEL  UUID                      MOUNTPOINT
sda
 ├── sda1
 │   └── sda2  swap  86fdee28-d919-43c2-b077-b3456efe170d [SWAP] /swap
 │   └── sda3  btrfs  4d4b1c9f-16c6-4038-8922-b82556885df5 /run/media/root/SLE-15-Installer-DVD
├── vda
 │   └── vdal  xfs  0c2937bf-1be7-4751-8bbd-3038dbfa93ac /hana
├── vdb
└── vdb1
hanahost1:~ $ lsblk
```
```bash
hanahost1:~ # lsblk -f

<table>
<thead>
<tr>
<th>NAME</th>
<th>FSTYPE</th>
<th>LABEL</th>
<th>UUID</th>
<th>MOUNTPOINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>sda1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>sda2</td>
<td>swap</td>
<td></td>
<td>86fdee28-d919-43c2-b077-b3456efe170d [SWAP]</td>
<td></td>
</tr>
<tr>
<td>sda3</td>
<td>btrfs</td>
<td></td>
<td>4d4b1c9f-16c6-4038-8922-b82a56845f5</td>
<td>/</td>
</tr>
<tr>
<td>vda1</td>
<td>xfs</td>
<td></td>
<td>0c2937bf-1be7-4751-8bbd-3038dbfa93ac</td>
<td>/hana</td>
</tr>
</tbody>
</table>

hanahost1:~ # lsblk

<table>
<thead>
<tr>
<th>NAME</th>
<th>MAJ:MIN</th>
<th>RM</th>
<th>SIZE</th>
<th>RO</th>
<th>TYPE</th>
<th>MOUNTPOINT</th>
</tr>
</thead>
<tbody>
<tr>
<td>sda1</td>
<td>8:0</td>
<td>0</td>
<td>50G</td>
<td>0</td>
<td>disk</td>
<td></td>
</tr>
<tr>
<td>sda1</td>
<td>8:1</td>
<td>0</td>
<td>4M</td>
<td>0</td>
<td>part</td>
<td></td>
</tr>
<tr>
<td>sda2</td>
<td>8:2</td>
<td>0</td>
<td>2G</td>
<td>0</td>
<td>part</td>
<td></td>
</tr>
<tr>
<td>sda3</td>
<td>8:3</td>
<td>0</td>
<td>48G</td>
<td>0</td>
<td>part</td>
<td></td>
</tr>
<tr>
<td>sr0</td>
<td>11:0</td>
<td>1</td>
<td>635M</td>
<td>0</td>
<td>rom</td>
<td></td>
</tr>
<tr>
<td>vda</td>
<td>253:0</td>
<td>0</td>
<td>102.4M</td>
<td>0</td>
<td>disk</td>
<td></td>
</tr>
<tr>
<td>vda1</td>
<td>253:1</td>
<td>0</td>
<td>101.4M</td>
<td>0</td>
<td>part</td>
<td>/hana</td>
</tr>
<tr>
<td>vdb</td>
<td>253:16</td>
<td>0</td>
<td>50G</td>
<td>0</td>
<td>disk</td>
<td></td>
</tr>
<tr>
<td>vdb1</td>
<td>253:17</td>
<td>0</td>
<td>50G</td>
<td>0</td>
<td>part</td>
<td></td>
</tr>
</tbody>
</table>
```
Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Configure cryptctl (Client) 2/4

hanahost1:~ $ cryptctl encrypt
Key server’s host name [centralhost.sabttec.com]:

Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
(Optional) PEM-encoded CA certificate of key server [/root/centralhost.sabttec.com.crt]:
Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
(Optional) PEM-encoded CA certificate of key server [/root/centralhost.sabttec.com.crt]:
If key server will validate client identity, enter path to PEM-encoded client certificate:
Enter key server's password (no echo):
Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
(Optional) PEM-encoded CA certificate of key server [/root/centralhost.sabttec.com.crt]:
If key server will validate client identity, enter path to PEM-encoded client certificate:
Enter key server's password (no echo):
Establishing connection to centralhost.sabttec.com on port 3737...
Path of directory to be encrypted: /hana
Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
(Optional) PEM-encoded CA certificate of key server [/root/centralhost.sabttec.com.crt]:
If key server will validate client identity, enter path to PEM-encoded client certificate:
Enter key server's password (no echo):
establishing connection to centralhost.sabttec.com on port 3737...
Path of directory to be encrypted: /hana
Path of disk partition (/dev/sdXXX) that will hold the directory after encryption: /dev/vdbl
Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
(Optional) PEM-encoded CA certificate of key server [/root/centralhost.sabttec.com.crt]:
If key server will validate client identity, enter path to PEM-encoded client certificate:
Enter key server's password (no echo):
Establishing connection to centralhost.sabttec.com on port 3737...
Path of directory to be encrypted: /hana
Path of disk partition (/dev/sdXXX) that will hold the directory after encryption: /dev/vdb1
How many computers can use the encrypted disk simultaneously [1]:

Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
(Optional) PEM-encoded CA certificate of key server [/root/centralhost.sabttec.com.crt]:
If key server will validate client identity, enter path to PEM-encoded client certificate:
Enter key server's password (no echo):
Establishing connection to centralhost.sabttec.com on port 3737...
Path of directory to be encrypted: /hana
Path of disk partition (/dev/sdXXX) that will hold the directory after encryption: /dev/vdb1
How many computers can use the encrypted disk simultaneously [1]:
If the key server does not hear from this computer for so many seconds, other computers will be allowed to use the key [30]:
Configure cryptctl (Client) 2/4

hanahost1:~ # cryptctl encrypt
Key server's host name [centralhost.sabttec.com]:
Key server's port number [3737]:
(Optional) PEM-encoded CA certificate of key server [/root/centralhost.sabttec.com.crt]:
If key server will validate client identity, enter path to PEM-encoded client certificate:
Enter key server's password (no echo):
Establishing connection to centralhost.sabttec.com on port 3737...
Path of directory to be encrypted: /hana
Path of disk partition (/dev/sdXXX) that will hold the directory after encryption: /dev/vdbl
How many disk partitions can use the encrypted disk simultaneously [1]:
If the key server does not hear from this computer for so many seconds, other computers will be allowed to use the key [30]:

Please take note to:
- Avoid touching the encrypted disk/directory until the operation completes.
- Ignore desktop prompts for entering disk password.

The encryption sequence will carry out the following tasks:
1. Completely erase disk "/dev/vdbl" and install encryption key on it.
2. Copy data from "/hana" into the disk.
3. Announce the encrypted disk to key server.

Please double check the details and type Yes to proceed [no]: yes
1. Completely erase disk "/dev/vdb1" and install encryption key on it.

2. Copy data from "/hana" into the disk.
   sending incremental file list

```
,/
```

   sent 49 bytes  received 19 bytes  136.00 bytes/sec
   total size is 0  speedup is 0.00

3. Announce the encrypted disk to key server "centralhost.sabttec.com:3737".

Congratulations! Data in "/hana" is now safely encrypted in "/dev/vdb1".
Remember to manually delete the original un-encrypted copy in "/cryptctl-moved-hana".
Configure cryptctl (Client) 3/4

1. Completely erase disk "/dev/vdb1" and install encryption key on it.

2. Copy data from "/hana" into the disk.
   sending incremental file list
   ./

   sent 49 bytes received 19 bytes 136.00 bytes/sec
total size is 0 speedup is 0.00

3. Announce the encrypted disk to key server "centralhost.sabttec.com:3737".

Congratulations! Data in "/hana" is now safely encrypted in "/dev/vdb1".
Remember to manually delete the original un-encrypted copy in "/cryptctl-moved-hana".

```bash
hanahost1:~ # lsblk -f
NAME      FSTYPE LABEL UUID                      MOUNTPOINT
sda
  -sda1
  -sda2 swap
  -sda3 btrfs
vda
  -vda1 xfs
vdb
  -vdb1 crypto_LUKS
     -cryptctl-unlocked-vdb1 xfs
  -vdb2 xfs
c02937bf-1be7-4751-8bba-3038dbfa93ac /cryptctl-moved-hana
ca56d0e3-980e-463f-9dec-a96e7f0af478
6e86f846f-df0a-4f6d-bbd8-7e18b9bd0493 /hana
```
Configure cryptctl (Client) 4/4

UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /var btrfs defaults 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /usr/local btrfs subvol=/@/var 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /tmp btrfs subvol=/@/usr/local 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /srv btrfs subvol=/@/tmp 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /root btrfs subvol=/@/srv 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /opt btrfs subvol=/@/root 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /home btrfs subvol=/@/opt 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /boot/grub2/x86_64-efi btrfs subvol=/@/home 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /boot/grub2/i386-pc btrfs subvol=/@/boot/grub2/x86_64-efi 0 0
UUID=86fde28-d919-43c2-b077-b3456e6fe170d swap swap defaults 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5  /.snapshots btrfs subvol=/@/swap 0 0
UUID=66ee846f-df0a-4f6d-bbd8-7e18b9bd0493 hana xfs defaults, netdev 0 0
10.0.0.7:/databig/soft/sapsoft software nfs defaults 0 0
Configure cryptctl (Client) 4/4

```
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /                     btrfs defaults 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /var                   btrfs subvol=/var 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /usr/local            btrfs subvol=/usr/local 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /tmp                  btrfs subvol=/tmp 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /srv                  btrfs subvol=/srv 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /root                btrfs subvol=/root 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /opt                 btrfs subvol=/opt 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /home            btrfs subvol=/home 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /boot/grub2/x86_64-efi btrfs subvol=/boot/grub2/x86_64-efi 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /boot/grub2/i386-pc btrfs subvol=/boot/grub2/i386-pc 0 0
UUID=86fde28d-919-43c2-b077-b3456e6fe170d swap               swap defaults 0 0
UUID=4d4b1c9f-16c6-4038-8922-b82556885df5 /.snapshots         btrfs subvol=./.snapshots 0 0
UUID=66ee846f-df0a-4f6d-bbd8-7e18b9bd0493 hana            xfs defaults, netdev 0 0
10.0.0.7:/databig/soft/sapsoft /software            nfs defaults 0 0
```

hanahost1:~ # umount /hana
hanahost1:~ # mount /hana
hanahost1:~ # lsblk

```
NAME       MAJ:MIN  RM  SIZE RO TYPE MOUNTPOINT
sda         8:0      0  50G  0 disk
├─sda1       8:1      0  4M   0 part
├─sda2       8:2      0  2G   0 part  [SWAP]
├─sda3       8:3      0  48G  0 part  /
sr0         11:0      1  635M 0 part /run/media/root/SLE-15-Installer-DVD-x86_646.001
vda         253:0     0 102.4M 0 disk
└─vda1       253:1     0 101.4M 0 part /cryptctl-moved-hana
vdb         253:16    0  50G  0 disk
└─vdb1       253:17    0  50G  0 part
  └─cryptctl-unlocked-vdb1 254:0    0  50G  0 crypt /hana
```
SAP HANA Security
SAP HANA Security – Important Critical Config

Critical Changes that need to be applied to any SAP HANA system

• The master keys of the following stores have to be changed:
  • The secure store in the file system (SSFS) of the instance
  • The SSFS used by the system public key infrastructure (PKI)
  • The SAP HANA secure user store (hdbuserstore) of the SAP HANA client
• Critical privileges are only assigned to trusted users
• Critical privilege combinations are avoided if possible
• The network configuration of your SAP HANA system is set up to protect internal SAP HANA communications channels
• Latest security patches are applied for the SAP HANA system, as well as the underlying operating system.

REF: SAP HANA Security Guide
SAP HANA Communication Channels

- SAP HANA cockpit (offline)
- SAP HANA studio
- BW/BI tools
- Suite / CRM etc.
- Excel
- Browser or mobile app
- UAA
- SAP HANA XS Client
- Other data sources
- SAP Landscape Transformation
- SAP Data Services
- SAP Replication Server
- SAP Event Stream Processor
- Streaming Client
- SAP Host Agent
- SAP HANA Database Lifecycle Manager
- Smart data streaming
- XS app
- DP server
- Instance agent
- R client
- SMD Agent
- Hdbiess
- smartdata access
- other web servers
- e-mail servers
- DP agent
- other data sources
- Rserve
SAP HANA Encryption Options

• Secure Communication
  • Encryption of data communication in the network is supported
  • Network traffic can be encrypted using Transport Layer Security (TLS)
  • TLS can be used to secure communications between clients and the database, as well as distributed hosts
SAP HANA Encryption Options

• Secure Communication
  • Encryption of data communication in the network is supported
  • Network traffic can be encrypted using Transport Layer Security (TLS)
  • TLS can be used to secure communications between clients and the database, as well as distributed hosts

• Encryption of the data persistence layer
  • The SAP HANA database can encrypt data at rest
  • Encryption works at the page level and uses the AES256 encryption algorithm
  • Redo log encryption of log volumes on disk
  • Data and Log backup encryption for full data backups, delta data backups and log backups
  • Encryption does not include database traces that might contain security-relevant data
SAP HANA Encryption Options

• Secure Communication
  • Encryption of data communication in the network is supported
  • Network traffic can be encrypted using Transport Layer Security (TLS)
  • TLS can be used to secure communications between clients and the database, as well as distributed hosts

• Encryption of the data persistence layer
  • The SAP HANA database can encrypt data at rest
  • Encryption works at the page level and uses the AES256 encryption algorithm
  • Redo log encryption of log volumes on disk
  • Data and Log backup encryption for full data backups, delta data backups and log backups
  • Encryption does not include database traces that might contain security-relevant data

• SAP HANA supports the following cryptographic libraries
  • CommonCryptoLib, installed by default as part of SAP HANA
  • OpenSSL, installed by default as part of SUSE
SAP HANA Data Volume Encryption

• Enable Data Encryption using SQL:
  • Data Volume encryption: ALTER SYSTEM PERSISTENCE ENCRYPTION ON
  • Redo Log encryption: ALTER SYSTEM LOG ENCRYPTION ON
  • Backup encryption: ALTER SYSTEM PERSISTENCE BACKUP ON

• Disable Data Encryption using SQL:
  • Data Volume encryption: ALTER SYSTEM PERSISTENCE ENCRYPTION OFF
  • Redo Log encryption: ALTER SYSTEM LOG ENCRYPTION OFF
  • Backup encryption: ALTER SYSTEM PERSISTENCE BACKUP OFF
SAP HANA Data Volume Encryption

• Enable Data Encryption using SQL:
  • Data Volume encryption: ALTER SYSTEM PERSISTENCE ENCRYPTION ON
  • Redo Log encryption: ALTER SYSTEM LOG ENCRYPTION ON
  • Backup encryption: ALTER SYSTEM PERSISTENCE BACKUP ON

• Disable Data Encryption using SQL:
  • Data Volume encryption: ALTER SYSTEM PERSISTENCE ENCRYPTION OFF
  • Redo Log encryption: ALTER SYSTEM LOG ENCRYPTION OFF
  • Backup encryption: ALTER SYSTEM PERSISTENCE BACKUP OFF

Instance SSFS (Secure Store in the File System) protects root keys used for all data-at-rest encryption
• Data Volume encryption, redo log encryption, internal application encryption service of the database, password of the root key backup, encryption configuration information
• $(DIR_GLOBAL)/hdb/security/ssfs
SAP HANA Data Volume Encryption

• Enable Data Encryption using SQL:
  • Data Volume encryption: ALTER SYSTEM PERSISTENCE ENCRYPTION ON
  • Redo Log encryption: ALTER SYSTEM LOG ENCRYPTION ON
  • Backup encryption: ALTER SYSTEM PERSISTENCE BAKUP ON

• Disable Data Encryption using SQL:
  • Data Volume encryption: ALTER SYSTEM PERSISTENCE ENCRYPTION OFF
  • Redo Log encryption: ALTER SYSTEM LOG ENCRYPTION OFF
  • Backup encryption: ALTER SYSTEM PERSISTENCE BAKUP OFF

• Instance SSFS (Secure Store in the File System) protects root keys used for all data-at-rest encryption
  • Data Volume encryption, redo log encryption, internal application encryption service of the database, password of the root key backup, encryption configuration information
  • $(DIR_GLOBAL)/hdb/security/ssfs
SAP HANA Replication
SAP HANA Recovery, Disaster Recovery and Replication

• SAP HANA has fault recovery support, for example:
  • Service Auto-Restart with a short Recovery Time Objective (RTO) and no costs involved
  • SAP HANA Auto-Restart has a long RTO but also no costs involved
  • Host Auto-Failover has a medium RTO and also medium costs
SAP HANA Recovery, Disaster Recovery and Replication

• SAP HANA has fault recovery support, for example:
  • Service Auto-Restart with a short Recovery Time Objective (RTO) and no costs involved
  • SAP HANA Auto-Restart has a long RTO but also no costs involved
  • Host Auto-Failover has a medium RTO and also medium costs

• When we look at Disaster recovery support, these options include:
  • Backups with Long RTO and low costs to the business
  • Storage Replication with medium RTO and medium costs
  • System Replication with short RTO and high costs
  • System Replication also supports Active/Active and Replication without Data Preload
SAP HANA Recovery, Disaster Recovery and Replication

• SAP HANA has fault recovery support, for example:
  • Service Auto-Restart with a short Recovery Time Objective (RTO) and no costs involved
  • SAP HANA Auto-Restart has a long RTO but also no costs involved
  • Host Auto-Failover has a medium RTO and also medium costs

• When we look at Disaster recovery support, these options include:
  • Backups with Long RTO and low costs to the business
  • Storage Replication with medium RTO and medium costs
  • System Replication with short RTO and high costs
  • System Replication also supports Active/Active and Replication without Data Preload

• SAP HANA System Replication modes
  • Asynchronous, primary system does not wait for confirmed redo logs sent
  • Synchronous in memory, primary system waits until secondary system has received the log
  • Synchronous, primary system waits until secondary system persistently received log to disk
  • Full Synchronous
SAP HANA Recovery, Disaster Recovery and Replication

Performance Optimized

Cost Optimized

Chain

Scale-Out *

Multi Tenancy (MCD)

Public Cloud (AWS)

* currently Tech-Preview
SAP HANA Replication Configuration – Performance Optimized
Replication Modes Available to SAP HANA

- Asynchronous

- Parameter: replicationMode=async
  - Primary node sends redo log

- Synchronous in Memory
- Parameter: replicationMode=syncmem
  - Synchronous

- Full Synchronous
- Parameter: replicationMode=Full Sync
Replication Modes Available to SAP HANA

• Asynchronous

• Synchronous in Memory
Replication Modes Available to SAP HANA

- Asynchronous
- Synchronous in Memory
- Synchronous
Replication Modes Available to SAP HANA

• Asynchronous

• Synchronous in Memory

• Synchronous

• Full Synchronous
Replication Modes Available to SAP HANA

- Asynchronous
  - Parameter: replicationMode=async
  - Primary node sends redo log
- Synchronous in Memory
- Synchronous
- Full Synchronous
Replication Modes Available to SAP HANA

- Asynchronous
  - Parameter: replicationMode=async
  - Primary node sends redo log
- Synchronous in Memory
  - Parameter: replicationMode=syncmem
- Synchronous
- Full Synchronous
Replication Modes Available to SAP HANA

- Asynchronous
  - Parameter: replicationMode=async
  - Primary node sends redo log
- Synchronous in Memory
  - Parameter: replicationMode=syncmem
- Synchronous
  - Parameter: replicationMode=sync
- Full Synchronous
Replication Modes Available to SAP HANA

- Asynchronous
  - Parameter: replicationMode=async
  - Primary node sends redo log
- Synchronous in Memory
  - Parameter: replicationMode=syncmem
- Synchronous
  - Parameter: replicationMode=sync
- Full Synchronous
  - Parameter: replicationMode=Full Sync
Operation Modes for System Replication

• Delta Data Shipping
  
  • Parameter: operation_mode=delta_datashipping
  
  This mode establishes a system replication and by default, every 10 seconds, a delta data shipping takes place.
  
  Continuous log shipping will still apply, this is however not replayed on the secondary node.

• Continuous Log Replay
  
  • Parameter: operation_mode=logreplay
  
  This mode does not require delta data shipping.
  
  The shipped redo log is continuously replayed on the secondary node.

• Continuous Log Replay with Active/Active
  
  • Parameter: operation_mode=logreplay_readaccess
  
  This mode continuously replays the redo log to the secondary node.
  
  It also allows for read-only access to the secondary node.
Operation Modes for System Replication

• Delta Data Shipping

• Continuous Log Replay
Operation Modes for System Replication

• Delta Data Shipping

• Continuous Log Replay

• Continuous Log Replay with Active/Active
Operation Modes for System Replication

- Delta Data Shipping
  - Parameter: operation_mode=delta_datashipping
  - This mode establishes a system replication and by default, a delta data shipping takes place every 10 seconds.
  - Continuous log shipping will still apply; however, this is not replayed on the secondary node.

- Continuous Log Replay

- Continuous Log Replay with Active/Active
Operation Modes for System Replication

• Delta Data Shipping
  • Parameter: operation_mode=delta_datashipping
  • This mode establishes a system replication and by default, a delta data shipping takes place every 10 seconds.
  • Continuous log shipping will still apply; however, this is not replayed on the secondary node.

• Continuous Log Replay
  • Parameter: operation_mode=logreplay
  • This mode does not require delta data shipping.
  • The shipped redo log is continuously replayed on the secondary node.

• Continuous Log Replay with Active/Active
Operation Modes for System Replication

• Delta Data Shipping
  • Parameter: operation_mode=delta_datashipping
  • This mode establishes a system replication and by default, a delta data shipping takes place every 10 seconds.
  • Continuous log shipping will still apply; however, this is not replayed on the secondary node.

• Continuous Log Replay
  • Parameter: operation_mode=logreplay
  • This mode does not require delta data shipping.
  • The shipped redo log is continuously replayed on the secondary node.

• Continuous Log Replay with Active/Active
  • Parameter: operation_mode=logreplay_readaccess
  • This mode continuously replays the redo log to the secondary node.
  • It also allows for read-only access to the secondary node.
HANA Cockpit Manager Setup

- HANA Cockpit Manager needs to be set up for SAP HANA 2.0
  - URL Used in DEMO: https://centralhost.sabttec.com:51031
  - Login User: COCKPIT_ADMIN (Should be changed to named user)
- Resources setup:

![HANA Cockpit Manager Setup](image)
• Replication of the two nodes can be set up within HANA Cockpit

SAP HANA SYSTEM
Database   User: SYSTEM   User: tecadm
2.00.033.00.1535711040 (a/hana2sp03)
Manage Credentials   Manage Credentials

• After the credentials per host is maintained, replication setup can begin
  • Before replication can be configured, a backup of each node is required
  • SSFS_<SID>.DAT and SSFS_<SID>.KEY from Primary should be copied to Secondary

• We then simply click on “Configure System Replication” to start the configuration
## HANA Cockpit Configuration, Replication Setup 2/3

### Tier 1 System Details

- **Site Name:** Datacenter1
- **Host:** hanahost1
- **Instance Number:** 00
- **Last Data Backup Performed On:** Feb 19, 2019, 11:06:34 AM

### Tier 2 System Details

- **Site Name:** Datacenter2
- **Secondary System Host:** 10.0.0.54
- **Replication Mode:** Synchronous in Memory
- **Operation Mode:** Log Replay
- **Host of Source System:** hanahost1
- **Instance Number:** 00
- **Initiate Data Shipping:** No

- **Start the secondary system after registration.**
HANA Cockpit Configuration, Replication Setup 3/3

- HANA System Replication is now configured
- This example is a 2-Tier configuration with simple failover available

**System Replication Overview**

- **System Site:** Tier 1 - Datacenter1
- **Site Role:** PRIMARY
- **Operation Mode:** LOGREPLAY
- **Estimated Log Full Time:** 9,354 Days
- **Network Security Settings:** DEFAULT

- **SYNCMEM - Network**
  - Datacenter1
    - hanahost1
  - Datacenter2
    - hanahost2

- At this stage, we don’t have automated failover; only replication has been set up. We still require SUSE HA to be configured.

<table>
<thead>
<tr>
<th>Site ID</th>
<th>Site Name</th>
<th>Secondary Site Name</th>
<th>Service</th>
<th>Port</th>
<th>Database Name</th>
<th>Replication Mode</th>
<th>Full Sync</th>
<th>Replication Status</th>
<th>Replication Details</th>
<th>Secondary Fully Recoverable</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Datacenter1 hanahost1</td>
<td>Datacenter2 hanahost2</td>
<td>xengine</td>
<td>30007</td>
<td>TEC</td>
<td>SYNCMEM</td>
<td>disabled</td>
<td>active</td>
<td>true</td>
<td>&gt;</td>
</tr>
<tr>
<td></td>
<td>indexserver</td>
<td></td>
<td></td>
<td>30003</td>
<td>TEC</td>
<td>SYNCMEM</td>
<td>disabled</td>
<td>active</td>
<td>true</td>
<td>&gt;</td>
</tr>
<tr>
<td></td>
<td>nameserver</td>
<td></td>
<td></td>
<td>30001</td>
<td>SYSTEMDB</td>
<td>SYNCMEM</td>
<td>disabled</td>
<td>active</td>
<td>true</td>
<td>&gt;</td>
</tr>
</tbody>
</table>
SUSE High Availability
SLES for SAP Key Features

- HANA Firewall
- Remote Storage
- Encryption Management
- HA Resource Agents
- 24/7 Live cycle Priority Support
SUSE High Availability Features

- Service Availability 24/7
- Data Replication
- Node Recovery
- Cluster File System
- Unlimited Geo Clustering
- Virtualization Ready
- Network Load-Balancer
- Free Resource Agents
- Clustered Samba
- Broad Platform Support
SUSE High Availability – Live Demo
SUSE High Availability (DEMO)

Live DEMO of High Availability
Best Practice
SLES Best Practice

• Recommended use of SUSE Manager for any SAP and SAP HANA environment running SLES:
  • System Deployment
  • Patch Management
  • Service Pack Application
  • Subscription Management
  • Configuration Maintenance
  • Compliance Management
SUSE Manager Benefits

• Manage Systems across physical, virtual and cloud environments
  • Reduced costs
  • Reduced complexity
  • Change control
  • Optimization
  • Negate risk
  • Compliance tracking
• Open source, one-to-many system management
• Reduce errors by proactive and automated patching
• Complete lifecycle management, compliance and security framework
SAP HANA Best Practice 1/2

- Overview of SAP HANA Python Scripts
  - HDB Admin – Graphical SAP HANA administration tool on Linux (SAP Note: 2520774)
  - SAP HANASitter – Automated capturing of SAP HANA trace dump information (SAP Note: 2399979)
  - SAP HANACleaner – Automated clean-up of HANA trace, log and backup catalog files (SAP Note: 2399996)
  - SAP HANADumpViewer – Simplifies the analysis of important SAP HANA dump files (SAP Note: 2491748)
  - SAP HANA Timer – Schedule database requests and measure runtime information (SAP Note: 2634449)
  - landscapeHostConfiguration.py – Check overall status of primary system using <sid>adm (SAP Note: 2518979)
  - systemReplicationStatus.py – Check overall status of system replication using <sid>adm (SAP Note: 2518979)
Use Solution Manager for Monitoring and Analysis of HANA environment
SAP HANA Best Practice 2/2

Use Solution Manager for Monitoring and Analysis of HANA environment

• System & Application Monitoring
  • One infrastructure for monitoring and alerting, covering SAP and non-SAP applications
  • System monitoring, User Experience monitoring, Integration monitoring, Job monitoring
  • HANA and Business Intelligence monitoring
SAP HANA Best Practice 2/2

Use Solution Manager for Monitoring and Analysis of HANA environment

• System & Application Monitoring
  • One infrastructure for monitoring and alerting covering SAP and non-SAP applications
  • System monitoring, User Experience monitoring, Integration monitoring, Job monitoring
  • HANA and Business Intelligence monitoring

• Root Cause Analysis and Exception Management
  • Analyse issues in heterogeneous landscapes
  • Ensure compliant configuration and reliable handling of technical and business exceptions
SAP HANA Best Practice 2/2

Use Solution Manager for Monitoring and Analysis of HANA environment

• System & Application Monitoring
  • One infrastructure for monitoring and alerting covering SAP and non-SAP applications
  • System monitoring, User Experience monitoring, Integration monitoring, Job monitoring
  • HANA and Business Intelligence monitoring

• Root Cause Analysis and Exception Management
  • Analyse issues in heterogeneous landscapes
  • Ensure compliant configuration and reliable handling of technical and business exceptions

• Technical Analytics and Dashboards
  • Metric value analytics for different target groups
  • Embedded into monitoring applications
  • Cross applications via Dashboard Builder and Customer specific via Dashboard Factory
SAP HANA Best Practice 2/2

Use Solution Manager for Monitoring and Analysis of HANA environment

• System & Application Monitoring
  • One infrastructure for monitoring and alerting covering SAP and non-SAP applications
  • System monitoring, User Experience monitoring, Integration monitoring, Job monitoring
  • HANA and Business Intelligence monitoring

• Root Cause Analysis and Exception Management
  • Analyse issues in heterogeneous landscapes
  • Ensure compliant configuration and reliable handling of technical and business exceptions

• Technical Analytics and Dashboards
  • Metric value analytics for different target groups
  • Embedded into monitoring applications
  • Cross applications via Dashboard Builder and Customer specific via Dashboard Factory

• Technical Administration and Guided Procedures
  • Central management of customer landscapes
  • Automated and guided handling of IT related activities, including IT Task Management
Recommendations
Recommendations to Keep Your Data Secure

• Perform Installations with recommendations from Vendor Installation guides
• Implement SLES and SAP HANA Security Guide recommendations
• Secure your SAP HANA Environment
• Use Encryption where possible
• Back up data securely and encrypt backups
• Patch SLES and SAP HANA regularly, especially security patches
• Train your company’s technical resources
• Ensure Certified SAP HANATEC resources maintain SAP HANA Environment
• Ensure Certified SUSE Linux Administrators maintain SLES for SAP
• Keep track of changes performed on environment, such as upgrade, patch and maintenance
Required Courses for Administrators

• SUSE Training for Administrators
  • SLE201 – SUSE Linux Enterprise Server 12 Administration
  • SLE221 – SUSE Linux Enterprise Server 12 for SAP Applications
  • SLE301 – SUSE Linux Enterprise Server 12 Advanced Administration
  • SLE321 – High Availability Clustering with SUSE Linux Enterprise

• SAP Training for Administrators
  • HA100 – SAP HANA Introduction
  • HA200 – SAP HANA 2.0 – Installation and Administration
  • HA201 – SAP HANA 2.0 – High Availability and Disaster Tolerance Administration
  • HA215 – SAP HANA 2.0 – Using Monitoring and Performance Tools
Required Courses for Administrators

- SUSE Training for Administrators
  - SLE201 – SUSE Linux Enterprise Server 12 Administration
  - SLE221 – SUSE Linux Enterprise Server 12 for SAP Applications
  - SLE301 – SUSE Linux Enterprise Server 12 Advanced Administration
  - SLE321 – High Availability Clustering with SUSE Linux Enterprise

- SAP Training for Administrators
  - HA100 – SAP HANA Introduction
  - HA200 – SAP HANA 2.0 – Installation and Administration
  - HA201 – SAP HANA 2.0 – High Availability and Disaster Tolerance Administration
  - HA215 – SAP HANA 2.0 – Using Monitoring and Performance Tools
Questions and Answers
Appendix
Appendix: HANA Host Install 1/3

hanahost1:/software/HDB_LCM_LINUX_X86_64 # ./hdblcm

Choose an action

<table>
<thead>
<tr>
<th>Index</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>install</td>
<td>Install new system</td>
</tr>
<tr>
<td>2</td>
<td>extract_components</td>
<td>Extract components</td>
</tr>
<tr>
<td>3</td>
<td>Exit (do nothing)</td>
<td></td>
</tr>
</tbody>
</table>

Enter selected action index [3]: 1

SAP HANA Database version '2.00.033.00.1535711040' will be installed.

Select additional components for installation:

<table>
<thead>
<tr>
<th>Index</th>
<th>Components</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>all</td>
<td>All components</td>
</tr>
<tr>
<td>2</td>
<td>server</td>
<td>No additional components</td>
</tr>
<tr>
<td>3</td>
<td>client</td>
<td>Install SAP HANA Database Client version 2.3.119.1535661774</td>
</tr>
<tr>
<td>4</td>
<td>studio</td>
<td>Install SAP HANA Studio version 2.3.41.000000</td>
</tr>
<tr>
<td>5</td>
<td>smartda</td>
<td>Install SAP HANA Smart Data Access version 2.00.3.000.0</td>
</tr>
<tr>
<td>6</td>
<td>xs</td>
<td>Install SAP HANA XS Advanced Runtime version 1.0.88.12598</td>
</tr>
<tr>
<td>7</td>
<td>afl</td>
<td>Install SAP HANA AFL (incl.PAL,BFL,OFL) version 2.00.033.0000.1535724035</td>
</tr>
<tr>
<td>8</td>
<td>eml</td>
<td>Install SAP HANA EML AFL version 2.00.033.0000.1535724035</td>
</tr>
<tr>
<td>9</td>
<td>epmmds</td>
<td>Install SAP HANA EPM-MDS version 2.00.033.0000.1535724035</td>
</tr>
</tbody>
</table>

Enter comma-separated list of the selected indices [3]: 1
Appendix: HANA Host Install 2/3

Enter Installation Path [/hana/shared]:
Enter Local Host Name [hanahost1]:
Do you want to add hosts to the system? (y/n) [n]:
Enter SAP HANA System ID: TEC
Enter Instance Number [00]:
Enter Local Host Worker Group [default]:

<table>
<thead>
<tr>
<th>Index</th>
<th>System Usage</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>production</td>
<td>System is used in a production environment</td>
</tr>
<tr>
<td>2</td>
<td>test</td>
<td>System is used for testing, not production</td>
</tr>
<tr>
<td>3</td>
<td>development</td>
<td>System is used for development, not production</td>
</tr>
<tr>
<td>4</td>
<td>custom</td>
<td>System usage is neither production, test nor development</td>
</tr>
</tbody>
</table>

Select System Usage / Enter Index [4]:
Enter Location of Data Volumes [/hana/data/TEC]:
Enter Location of Log Volumes [/hana/log/TEC]:
Restrict maximum memory allocation? [n]:
Enter Certificate Host Name For Host 'hanahost1' [hanahost1]:
Enter SAP Host Agent User (sapadm) Password:
Confirm SAP Host Agent User (sapadm) Password:
Enter System Administrator (tecadm) Password:
Confirm System Administrator (tecadm) Password:
Enter System Administrator Home Directory [/usr/sap/TEC/home]:
Enter System Administrator Login Shell [/bin/sh]:
Enter System Administrator User ID [1001]:
Enter ID of User Group (sapsys) [79]: 101
Enter System Database User (SYSTEM) Password:
Confirm System Database User (SYSTEM) Password:
Restart system after machine reboot? [n]: [ ]
Appendix: HANA Host Install 3/3

Summary before execution:
=================================

SAP HANA Database System Installation
Installation Parameters
  Remote Execution: ssh
  Database Isolation: low
  Installation Path: /hana/shared
  Local Host Name: hanahost1
  SAP HANA System ID: TEC
  Instance Number: 00
  Local Host Worker Group: default
  System Usage: custom
  Location of Data Volumes: /hana/data/TEC
  Location of Log Volumes: /hana/log/TEC
  Certificate Host Names: hanahost1 -> hanahost1
  System Administrator Home Directory: /usr/sap/TEC/home
  System Administrator Login Shell: /bin/sh
  System Administrator User ID: 1001
  ID of User Group (sapsys): 101
  SAP HANA Database Client Installation Path: /hana/shared/TEC/hdbclient
Software Components
  SAP HANA Database
    Install version 2.00.033.00.1535711040
    Location: /software/SAP_SOFTWARE/HANA2.0_SPS3_Rev33_Linux_x86_64/DATA_UNITS/HDB_SERVER_LINUX_X86_64/server
  SAP HANA AFL (incl.PAL,BFL,OFL)
    Do not install
  SAP HANA EML AFL
    Do not install
  SAP HANA EPM-MDS
    Do not install
  SAP HANA Database Client
    Install version 2.3.119.1535661774
    Location: /software/SAP_SOFTWARE/HANA2.0_SPS3_Rev33_Linux_x86_64/DATA_UNITS/HDB_CLIENT_LINUX_X86_64/client
  SAP HANA Studio
    Do not install
  SAP HANA Smart Data Access
    Do not install
  SAP HANA XS Advanced Runtime
    Do not install

Do you want to continue? (y/n): y
centralhost:/software/SAP_SOFT/HANA2.0Cockpit9_5 # ./hdblcm.sh

SAP HANA Lifecycle Management - SAP HANA Cockpit 2.0.9.5.0
*****************************************************************************

Choose an action

<table>
<thead>
<tr>
<th>Index</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>install</td>
<td>Install new SAP HANA Cockpit system</td>
</tr>
<tr>
<td>2</td>
<td>Exit (do nothing)</td>
<td></td>
</tr>
</tbody>
</table>

Enter selected action index [2]: 1

Enter Installation Path [/hana/shared]:
Enter Local Host Name [centralhost]:
Enter SAP HANA System ID [H4C]:
Enter Instance Number [96]:
Enter Master Password:
Confirm Master Password:
Enter XS Advanced Admin User [COCKPIT_ADMIN]:
Appendix: HANA Replication Keys Copy

```bash
hanahost1:/hana/shared/TEC/global/security/rsecssfs/data # scp -pr SSFS_TEC.DAT hanahost2:/hana/shared/TEC/global/security/rsecssfs/data/
The authenticity of host 'hanahost2 (10.0.0.54)' can't be established. 
ECDSA key fingerprint is SHA256:ESYqEXMtqt0+W2GiNj1jxQSSfP03D0SEMBm1L36Ei5Pw. 
Are you sure you want to continue connecting (yes/no)? yes 
Warning: Permanently added 'hanahost2,10.0.0.54' (ECDSA) to the list of known hosts.
Password: 
SSFS_TEC.DAT
hanahost1:/hana/shared/TEC/global/security/rsecssfs/key # scp -pr SSFS_TEC.KEY hanahost2:/hana/shared/TEC/global/security/rsecssfs/key/
Password: 
SSFS_TEC.KEY
```

---

100% 2960  2.0MB/s  00:00

100% 187  252.1KB/s  00:00