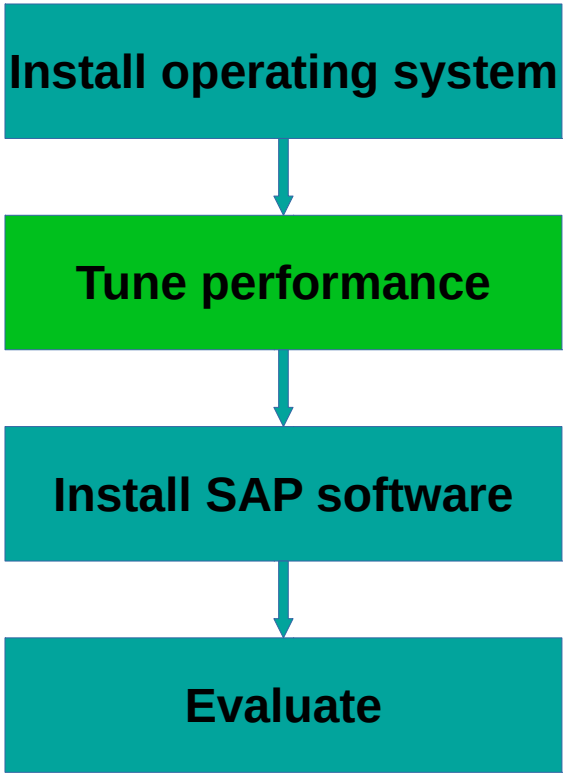
Unleash hardware's full potential with smart system tuning for SAP workloads

Howard Guo
Senior Software Developer
hguo@suse.com

Getting ready for SAP



Challenges

- SAP tuning guides only written for individual software solutions.
- Lengthy tuning guides take considerable effort to implement.
- Combining tuning guides from various solutions is error prone.
- Lacking manageability in ongoing system maintenance.

Legacy method - “sapconf”

- Available in all editions of SUSE Linux Enterprise 11 and 12.
- Using a checklist approach, profiles are provided for popular solutions:
  - SAP Netweaver
  - SAP HANA
  - SAP ASE and BusinessObjects
- Only one profile may be activated at a time.
- No way to verify system state in ongoing maintenance.

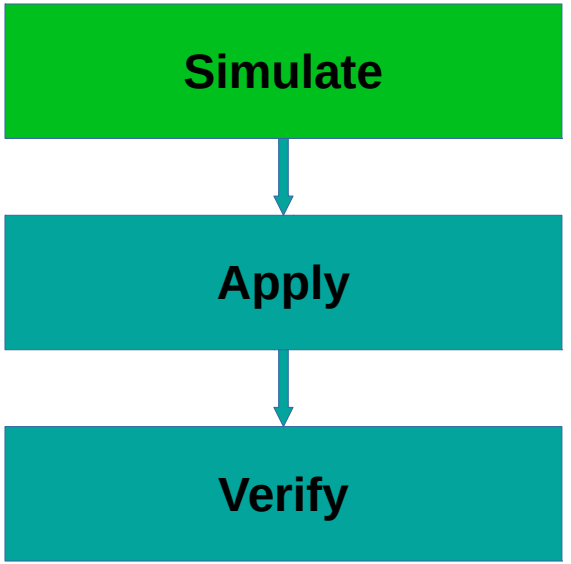
Introducing saptune - comprehensive tuning management

New utility - saptune

- Available in SUSE Linux Enterprise For SAP since 12 SP2.
- Tune for individual and combination of SAP solutions.
- Conduct simulation run to determine how system will be changed.
- Verify system state for ongoing maintenance.
- Reverse tuning actions on-demand.
- Capable of operating in virtualised environments such as public and private cloud.

Link: project source code https://github.com/HouzuoGuo/saptune

Workflow

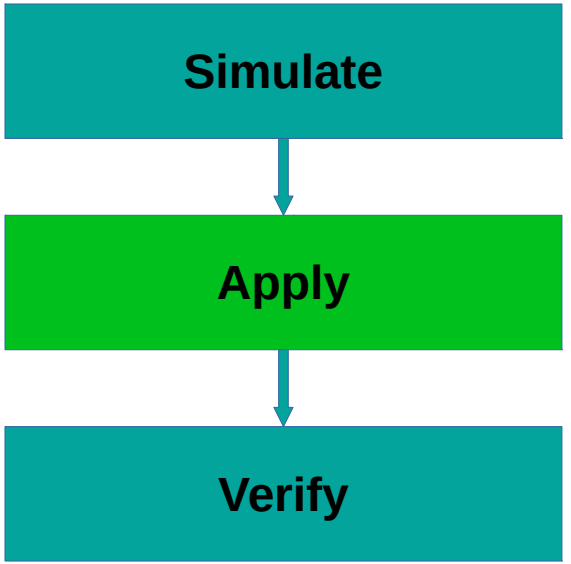


Step 1 – simulate

- Choose solutions (e.g. Netweaver/HANA) to tune for.
- Run “saptune simulate solution”.
- Evaluate before/after values:

```
root@d147 ~ # saptune solution simulate HANA
If you run `saptune solution apply HANA`, the following changes will be applied to your system:
1984787 - SUSE LINUX Enterprise Server 12: Installation notes -
        (no change)
1557506 - Linux paging improvements -
        (no change)
2205917 - SAP HANA DB: Recommended OS settings for SLES 12 / SLES for SAP Applications 12 -
        KernelMMTransparentHugepage : never
1275776 - Linux: Preparing SLES for SAP environments -
        VMMaxMapCount : 2000000
        ShmFileSystemSizeMB : 7527
root@d147 ~ #
```

Workflow

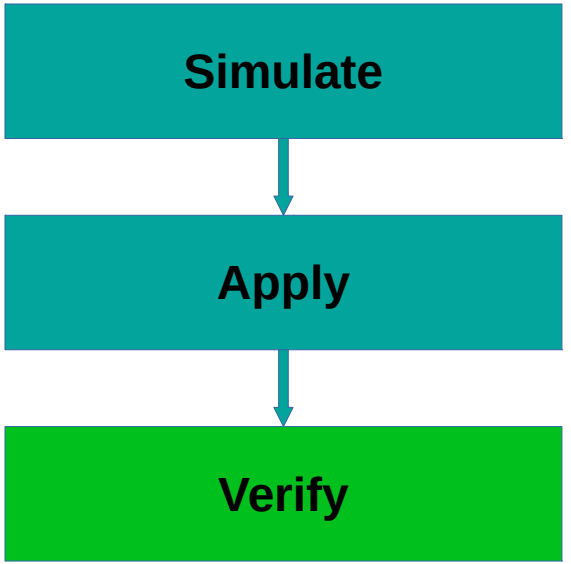


Step 2 – apply

- Conduct system tuning prior to installing SAP software.
- Apply tuning options for all applicable SAP solutions:

```
root@d147 ~ # saptune solution apply HANA
All tuning options for the SAP solution have been applied successfully.
root@d147 ~ # saptune solution apply NETWEAVER
All tuning options for the SAP solution have been applied successfully.
root@d147 ~ #
```

Workflow



Step 3 – verify

- Ensure current configuration does not deviated from optimal setting.
- Conduct verification periodically in ongoing maintenance.

```
root@d147 ~ # saptune solution verify NETWEAVER
1275776 - Linux: Preparing SLES for SAP environments -
        ShmFileSystemSizeMB Expected: 7527
        ShmFileSystemSizeMB Actual  : 3991
        VMMaxMapCount Expected: 2000000
        VMMaxMapCount Actual  : 65530
The parameters listed above have deviated from the specified SAP solution recommendations.
```

Rationale in tuning for SAP softwares

Common technique in tuning kernel resources

- As much as possible, loosen restrictions on:
  - Shared memory capacity
  - Semaphore capacity
  - Number of memory map areas
- Disable computation-intensive memory management features:
  - Automated NUMA-balancing
  - Same page merging
  - Transparent huge pages

Common technique in tuning page cache

- Tell kernel to avoid moving application memory into swap.
- Ensure consistent application response time.
- Calculate “vm.pagecache_limit_mb”:
  - Different SAP solutions suggest
  - Automatically tuned by both sapconf and saptune.

Situational techniques

- Decrease swap usage.
- Allow over committing memory usage.
- Experiment with alternative IO schedulers.
- Tweak file system parameters according to storage capability.
- Adjust VFS cache behaviour in preparation for memory pressure.
- Make IO read-ahead more aggressive.

More situational techniques

- Increase buffer and backlog capacity in network stack.
- Disable advanced computation-intensive TCP features.
- Bind processes to specific number of CPUs.

Link: OS tuning and optimisation guide
https://www.suse.com/communities/blog/sles-1112-os-tuning-optimisation-guide-part-1/

Bonus topic – data-at-rest encryption

Challenges

- Each encrypted disk should use a unique key instead of a common password.
- Central management of encryption keys is a difficult administrative challenge.
- Encryption mechanism should be transparent to applications.

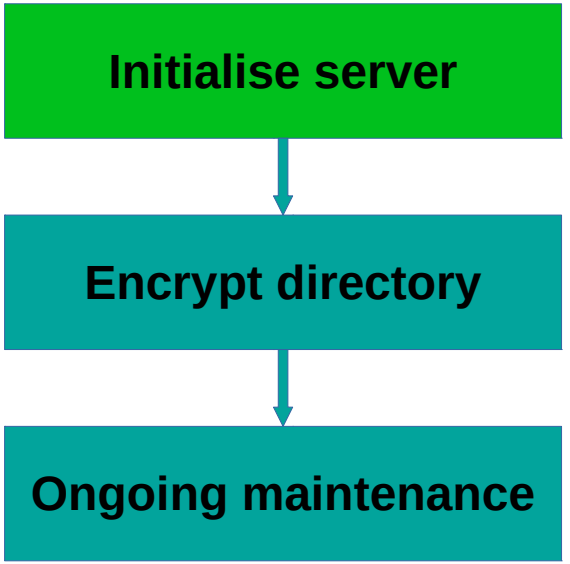
Introducing cryptctl - KMIP-capable disk encryption management

Introducing cryptctl

- Available in SUSE Linux Enterprise For SAP since 12 SP2.
- Install unique key to encrypted partitions.
- Track and monitor key usage.
- Transparent to applications, tailored for SAP workload.
- Integrates with key management appliances via KMIP – Key Management Interoperability Protocol.
- Use a KMIP-compatible appliance to centrally manage all types of keys and secrets, including disk encryption keys.

Link: project source code https://github.com/HouzuoGuo/cryptctl

Workflow

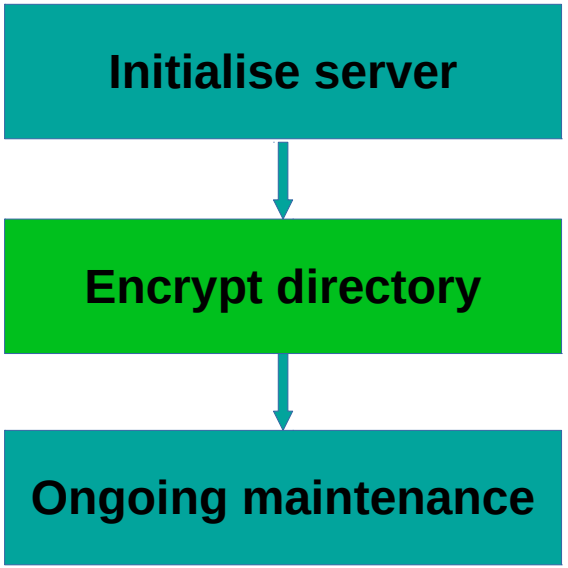

Initialise server
Encrypt directory
Ongoing maintenance

Initialise server

- Specify master password and set up TLS certificate.
- Optionally:
  - Enable client certificate verification.
  - Connect to a KMIP appliance.
  - Set up Email notification.

```
root@d42 ~ # 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 [d42.suse.de]:
Generating certificate...
```

Workflow


Initialise server
Encrypt directory
Ongoing maintenance

Encrypt directory

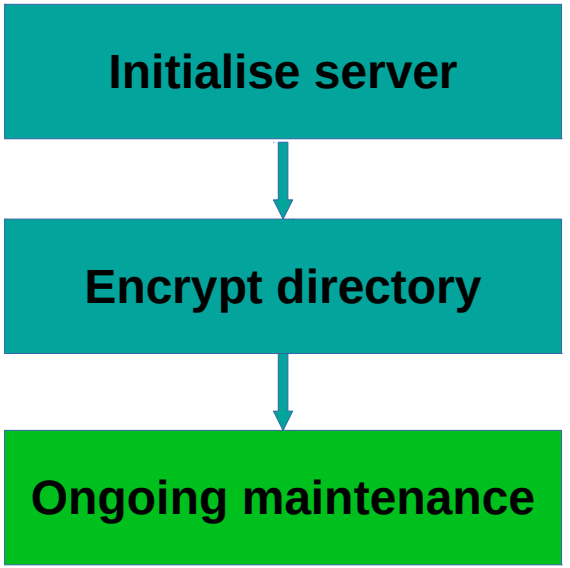
- Set up transparent encryption using Linux Unified Key Setup.
- Use randomly generated key and safe keep it in database.
- Encrypted directories are automatically opened upon reboot.

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

Please double check the details and type Yes to proceed [no]: yes
```

… and success!

```
3. Announce the encrypted disk to key server "d42.suse.de".

Congratulations! Data in "/topsecret" is now safely encrypted in "/dev/vdb".
Remember to manually delete the original un-encrypted copy in "/cryptctl-moved-t
opsecret".
```

Workflow


Initialise server
Encrypt directory
Ongoing maintenance

Ongoing maintenance

- Alter mount point directory and mount options.
- Issue commands from key server to open and close encrypted directories on specific client computer.
- Revoke encryption key – effectively erasing encrypted data.

```
root@d42 ~ # cryptctl list-keys
2017/08/18 12:10:15 DB.ReloadDB: successfully loaded database of 1 records
Total: 1 records (date and time are in zone CEST)
Used By         When                ID          UUID                                 Max.Users Num.Users Mount Point
10.160.64.42    2017-08-18 12:06:26 1           91c1f7c5-d96e-48a1-86ee-7e09febc40d5 1         1         /topsecret
```

Ongoing maintenance

Audit key usage - timestamp, computer IP, and many other details are recorded along with disk unlocking attempts.

```
root@d42 ~ # cryptctl show-key 91c1f7c5-d96e-48a1-86ee-7e09febc40d5
UUID                                91c1f7c5-d96e-48a1-86ee-7e09febc40d5
Mount Point                         /topsecret
Mount Options                       rw,relatime,data=ordered
Maximum Computers                   1
Computer Keep-Alive Timeout (sec)   30
Last Retrieved By                   10.160.64.42 (d42.suse.de)
Last Retrieved On                   2017-08-18 12:06:26
Current Active Computers            1
                                    2017-08-18 12:11:21 10.160.64.42 (d42.suse.de)
                                    2017-08-18 12:11:31 10.160.64.42 (d42.suse.de)
                                    2017-08-18 12:11:41 10.160.64.42 (d42.suse.de)
```

Open Discussion