AD integration OS-layer with SAP/HA solutions
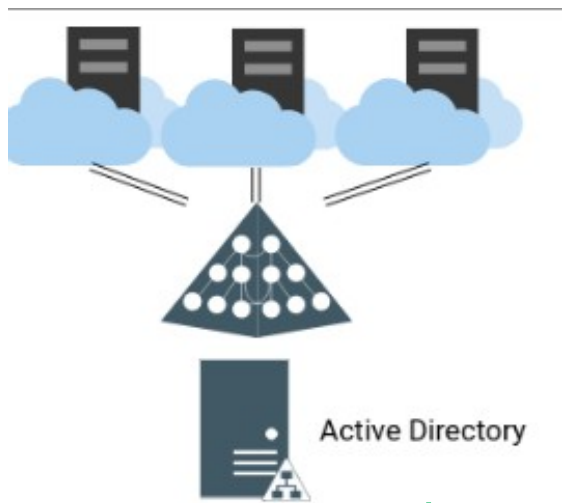
<Dario Maiocchi dmaiocchi@suse.com>

SUSE

RATIONALE:

Install, manage SAP/HA cluster components with AD users

SUSE

Active Directory

The AD administrator create user and groups into AD.

hacluster , <sid>adm user and others groups.

The groups/user must have POSIX attributes with right number of SID and GID
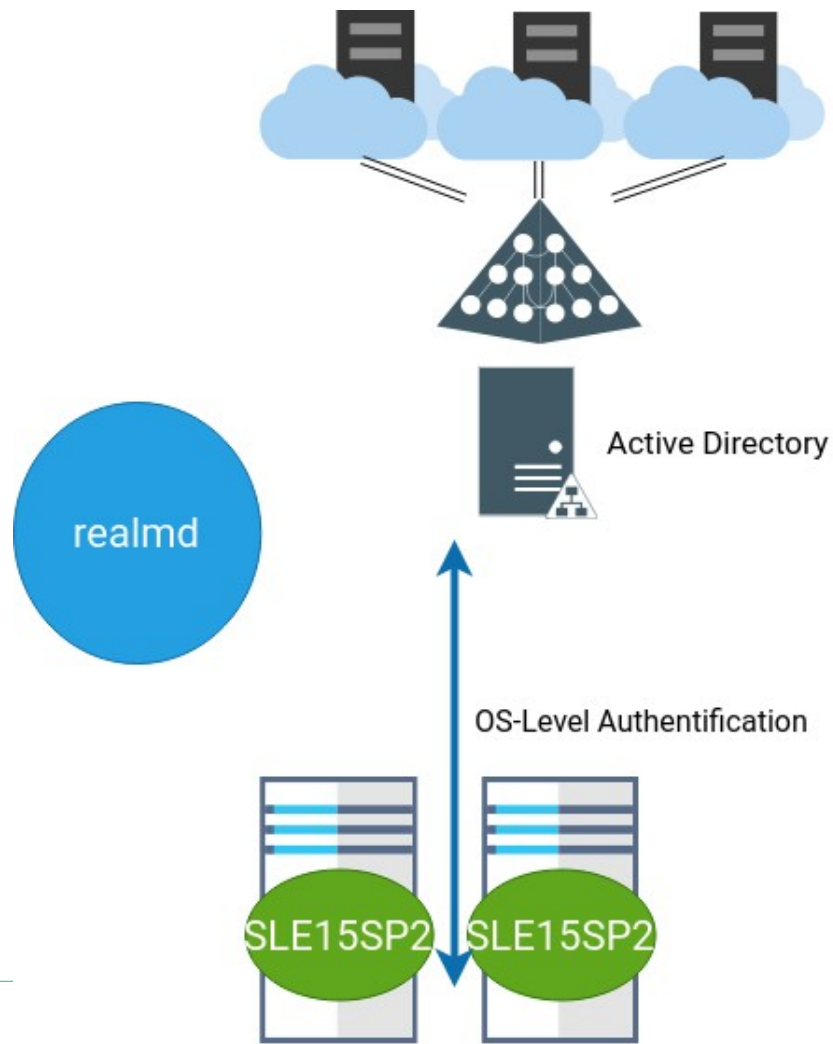
SUSE

Which Users needs to be managed from AD:

- 1) HA cluster user/hawk: hacluster, <<SID>>adm for RA
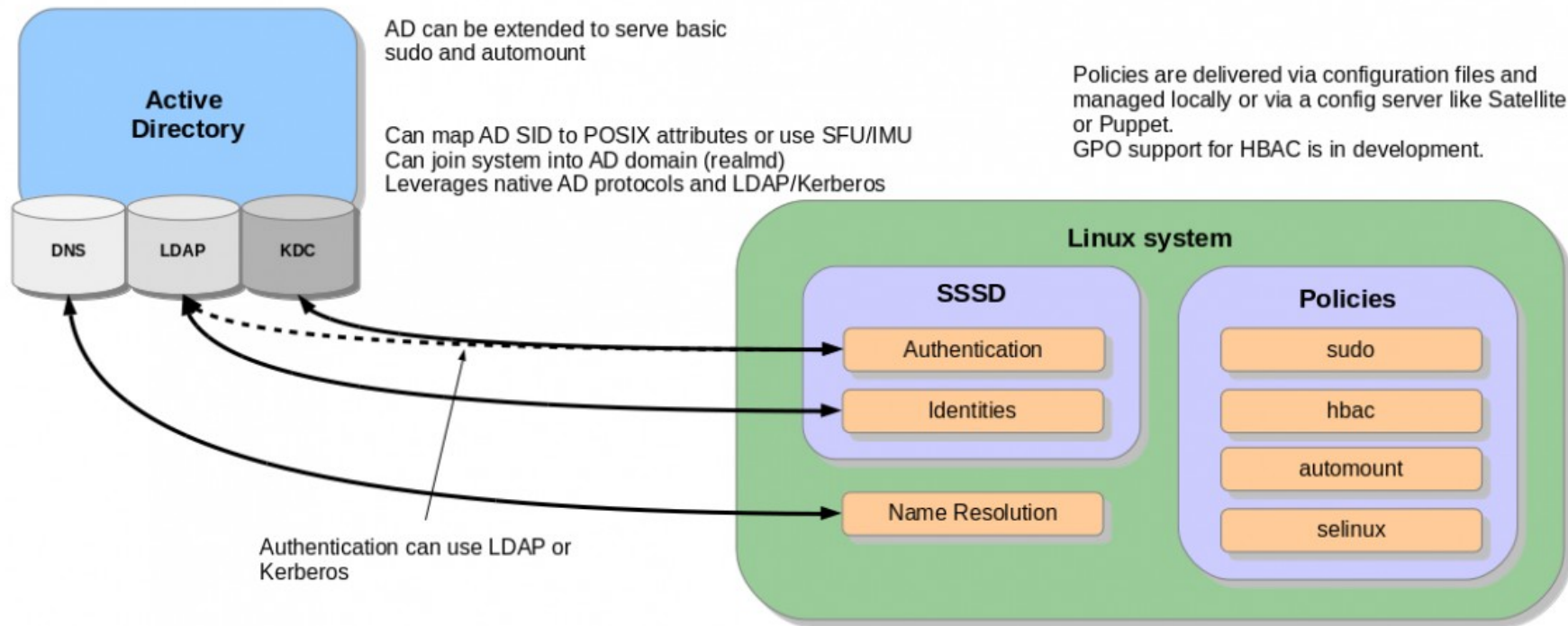
- 2) SAP HANA: <<SID>>adm

- 3) Netweaver: <<SID>>adm

SUSE

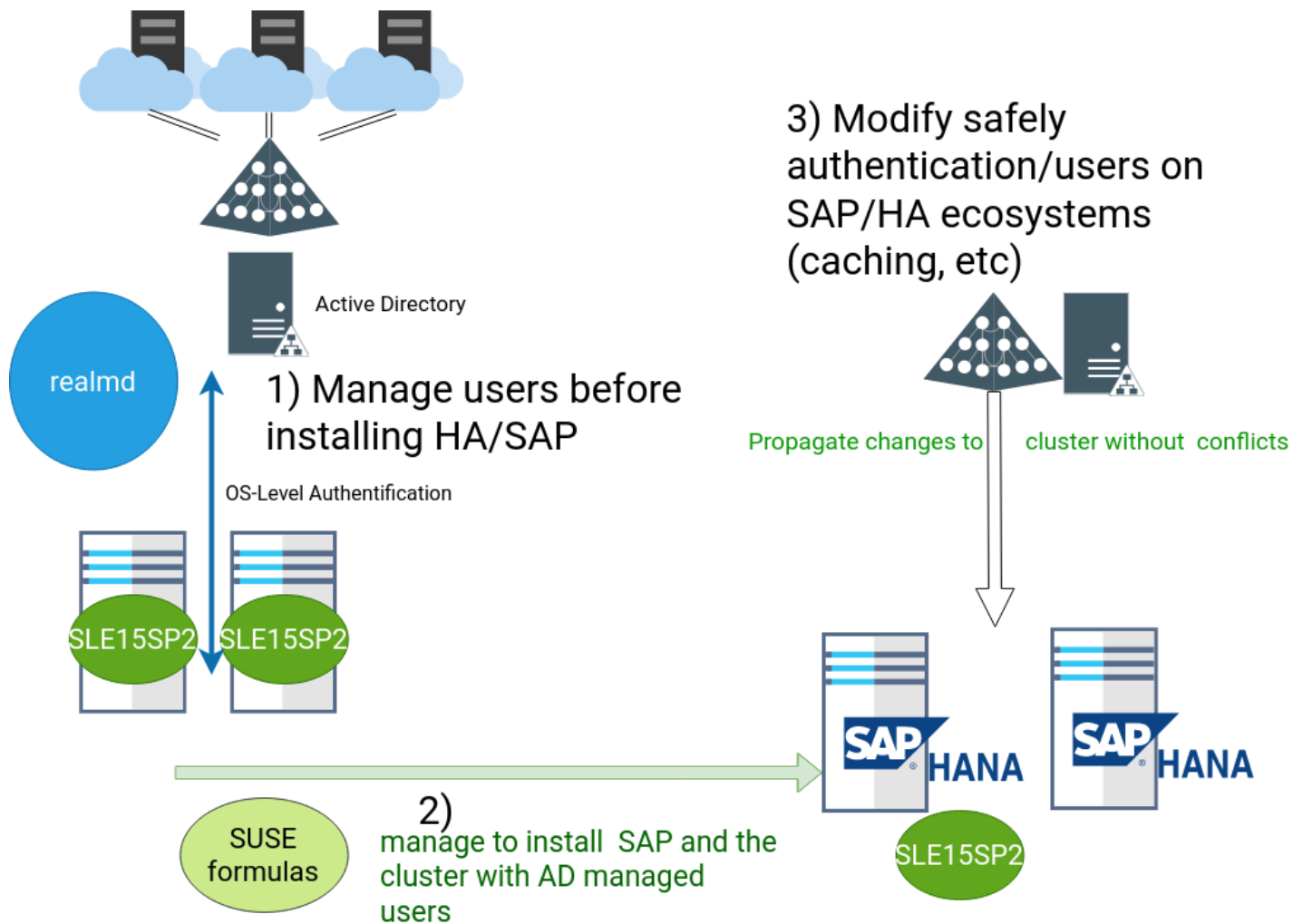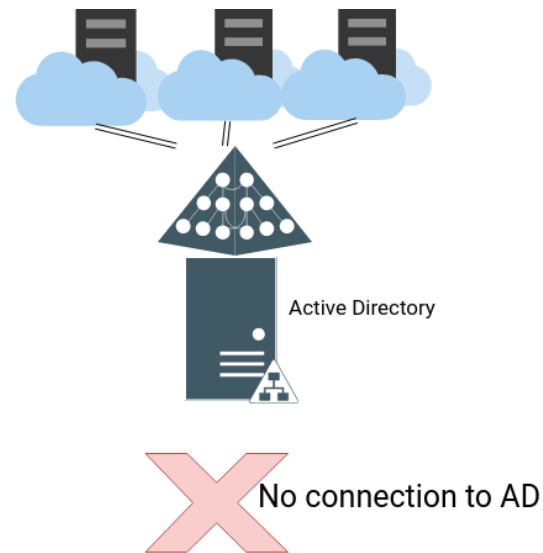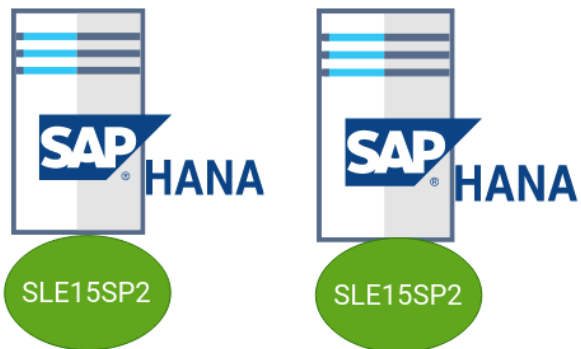# Ad configuration must occur before the installation

REALM configure Linux machines for AD

(sssd, pam etc)

SUSE

Active Directory

DNS   LDAP   KDC

AD can be extended to serve basic
sudo and automount

Can map AD SID to POSIX attributes or use SFU/IMU
Can join system into AD domain (realmd)
Leverages native AD protocols and LDAP/Kerberos

Policies are delivered via configuration files and
managed locally or via a config server like Satellite
or Puppet.
GPO support for HBAC is in development.

Linux system

SSSD

Authentication

Identities

Name Resolution

Policies

sudo

hbac

automount

selinux

Authentication can use LDAP or
Kerberos

SUSE

realmd

Active Directory

1) Manage users before installing HA/SAP

OS-Level Authentification

SLE15SP2   SLE15SP2

SUSE formulas

2) manage to install SAP and the cluster with AD managed users

3) Modify safely authentication/users on SAP/HA ecosystems (caching, etc)

Propagate changes to   cluster without conflicts

SAP HANA   SAP HANA

SLE15SP2

SUSE

Active Directory

Authenticate <sid>ADM and other users

SLE15SP2

SLE15SP2

Active Directory

No connection to AD

SLE15SP2

SLE15SP2

9

SUSE

Active Directory

No connection to AD

NO cache properly configured with SSD

SLE15SP2

SLE15SP2

10

SUSE
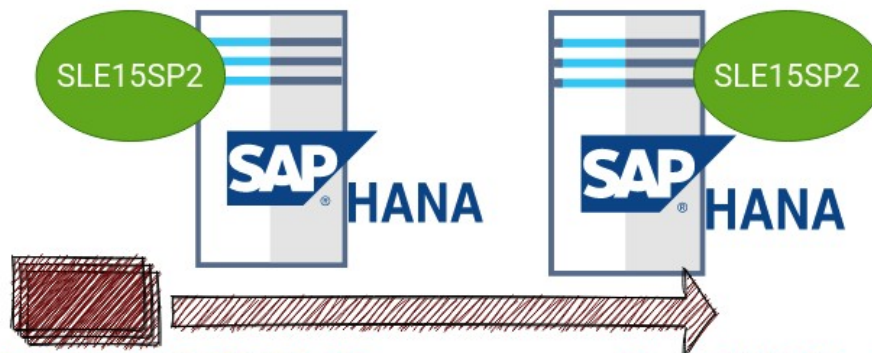
RESOURCE AGENT FOR HANA START FAILING

Migrate HANADB to other node

Active Directory

No connection to AD

SLE15SP2

SLE15SP2

SSSD CACHE

SSSD CACHE

SUSE
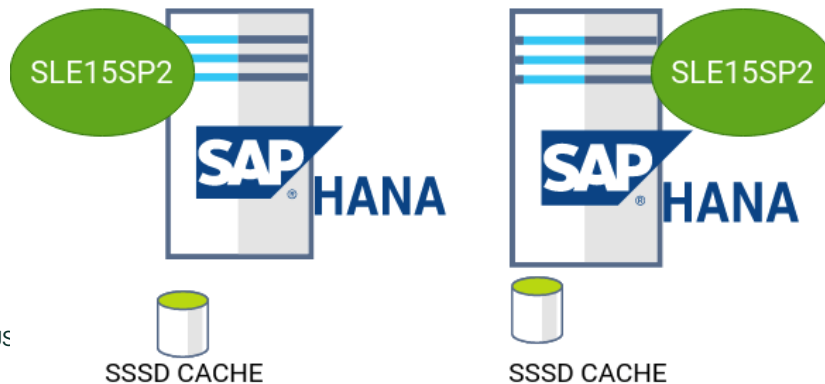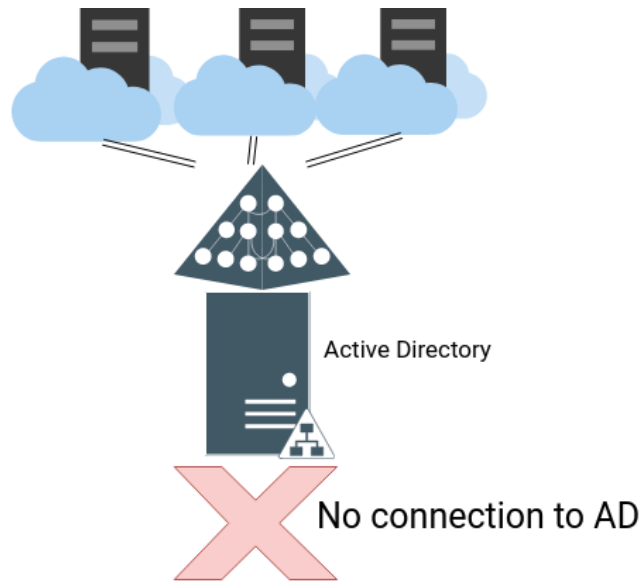
SSSD.conf file * solving the sudo problem for RA

```
[sssd]
services = nss,pam

...

[pam]
offline_credentials_expiration = 3

...

[domain/EXAMPLE]
cache_credentials = true

...
```

`offline_credentials_expiration` sets the number of days after a successful login that a single credentials entry for a user is preserved in cache. Setting this to zero (0) means that entries are kept forever.

SUSE

SUSE