SUSE Manager 3 Authentication

Be smart. Think open source.

SUSE Manager 3 - Authentication

Agenda

- SSSD
- PAM
- User Import

SSSD

Provider

- LDAP
- Active Directory
- Identity Management
- Kerberos (auth only)

SSSD - AD Provider

Example configuration `/etc/sssd/sssd.conf`

```
[nss]
filter_users = root
filter_groups = root

[pam]

[sssd]
config_file_version = 2
services = nss, pam
domains = sub.mydomain.com

[domain/sub.mydomain.com]
ad_server =  dc1.sub.mydomain.com, dc2.sub.mydomain.com
id_provider = ad
default_shell = /bin/bash
ad_access_filter = (memberOf=cn=admins,ou=groups,dc=mydomain,dc=com)
```

SSSD - nsswitch

Example `/etc/nsswitch.conf`

```
passwd: file sss
group:  file sss
shadow: file sss
```

SSSD - nscd

Must to be stoped and disbaled as sssd now caches:

```
# systemctl stop nscd.service

# systemctl disable nscd.service
```

PAM

/etc/pam.d/common-auth

```
auth    required        pam_env.so
auth    sufficient      pam_unix.so     try_first_pass
auth    sufficient      pam_krb5.so     use_first_pass
auth    required        pam_sss.so      use_first_pass
```

/etc/pam.d/susemanager

```
auth     include        common-auth
account  include        common-account
password include        common-password
```

/etc/rhn/rhn.conf

```
pam_auth_service = susemanager
```

User import

```
## Configuration ##
#AD Group
ADGROUP=APP_RH_SUSEManager
# SUMA Local Admin
SPACEUSR=Admin
# SUMA Local Password
SPACEPW=...
# Domain Part of EMAIL address
DOMAIN_EMAIL=sub.mydomain.com
# Roles that need to be assigned to the user
ROLES="satellite_admin activation_key_admin system_group_admin org_admin config_admin channel_admin"

## Automatic Lists ##
SCMD="/usr/bin/spacecmd -y -q -u $SPACEUSR -p $SPACEPW"
GRPUSRS=$(getent group "${ADGROUP}" | cut -f4 -d: | sed 's/,/ /g' | sed "s/\'//g")
SUMAUSRS=$($SCMD user_list | grep -v -x $SPACEUSR)

## Magic ##
for each in ${GRPUSRS}
      do
      PAM_USER="${each}"
      USREXIST=$(echo "$SUMAUSRS" | grep -x "$PAM_USER")
      if [ -z "${USREXIST}" ]; then
        ${SCMD} "user_create -u ${PAM_USER} -f ${PAM_USER} -l ${PAM_USER} -e ${PAM_USER}@${DOMAIN_EMAIL} --pam
        for each in ${ROLES}
         do
         ${SCMD} user_addrole ${PAM_USER} "${each}"
        done
        logger $0 : added ${each} as SUMA Admin
      fi
done

for each in ${SUMAUSRS}
      do
            if [ "${each}" == "${SPACEUSR}" ]; then
                  break
```

User Import

`/etc/rhn/sw-ldap-user-sync.conf`

```
directory:
  user: uid=xyz,dc=example,dc=com
  password: xxx
  url: ldaps://ldap.example.com:636
  group: cn=admin,ou=groups,dc=example,dc=com
  users: ou=people,dc=example,dc=com
spacewalk:
  url: http://localhost/rpc/api
  user: spacewalk
  password: xxx
```

`/usr/bin/sw-ldap-user-sync`

Feel Free to Contact Us

www.adfinis-sygroup.ch

Tech Blog

GitHub

info@adfinis-sygroup.ch

Twitter