SSSD – Zentrale User- und Gruppeninformationen

OpenRheinRuhr 2018

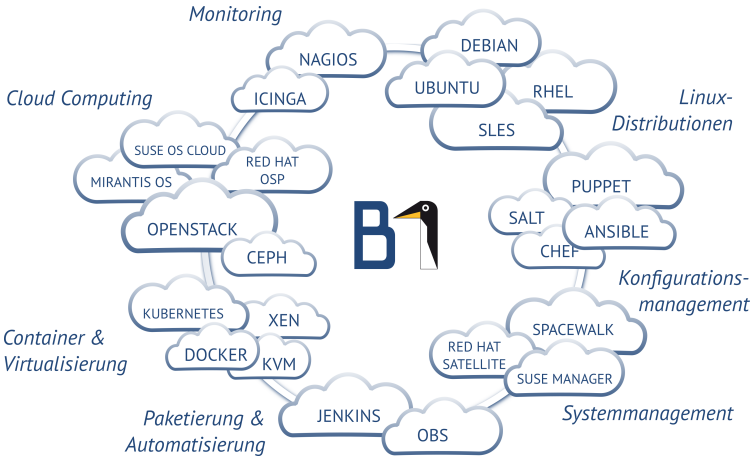
3. November 2018

Michael Wandel
Linux Consultant & Trainer
B1 Systems GmbH
wandel@b1-systems.de

Vorstellung B1 Systems

- gegründet 2004
- primär Linux/Open Source-Themen
- national & international tätig
- über 100 Mitarbeiter
- unabhängig von Soft- und Hardware-Herstellern
- Leistungsangebot:
  - Beratung & Consulting
  - Support
  - Entwicklung
  - Training
  - Betrieb
  - Lösungen
- Standorte in Rockolding, Köln, Berlin & Dresden

Schwerpunkte



System Security Services Daemon

SSSD – Funktion und Einsatzgebiet

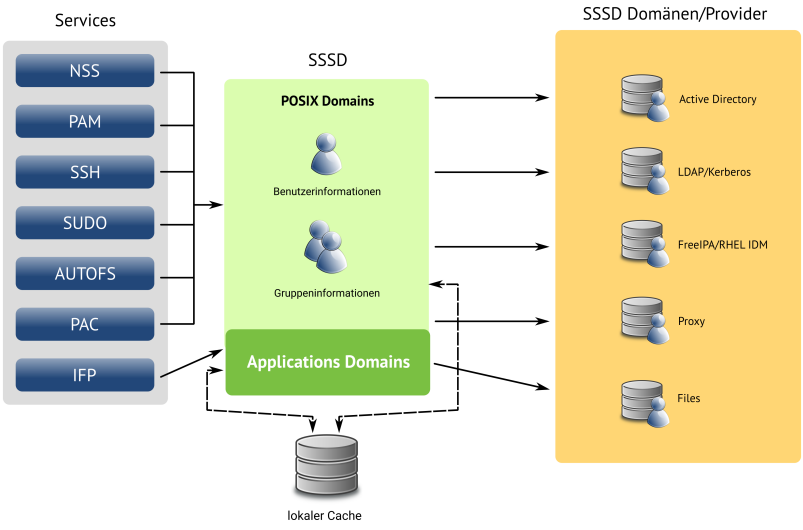
- Teil des FreeIPA-Projekts
- multiple Datenquellen für User-/Gruppendaten
- traditionelle Werkzeuge:
  - `nss-ldap`, `nslcd`, `pam-ldap`, `pam-krb5`, `winbindd`
- ein Service Daemon, vielseitig konfigurierbar
- Integration verschiedener Services

Vorteile von SSSD

- unterschiedlichste Datenquellen
- lokaler Cache, kein `nscd` notwendig
- detaillierte Logdateien/Loglevel
- verschiedene Zugriffsbeschränkungen
- Integration Session-Recording
- Systemtap-Schnittstelle
- aktive Entwicklung

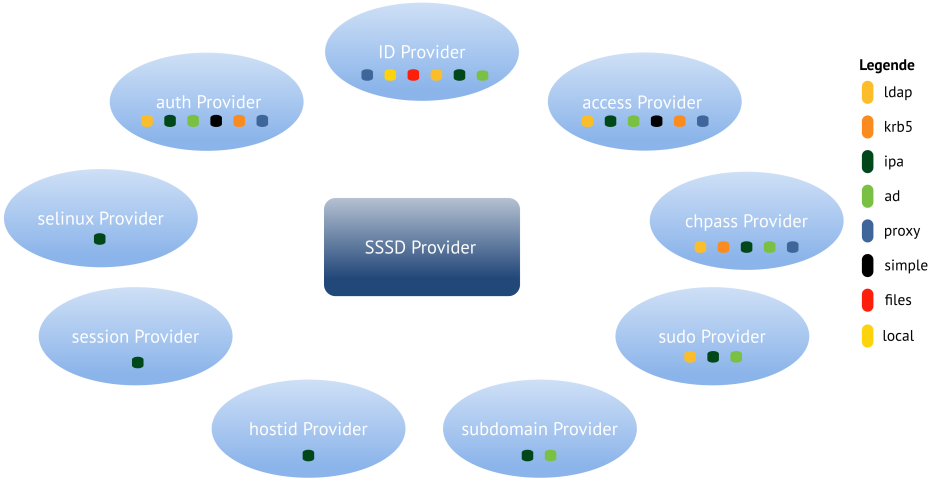
Datenquelle für Posix-Informationen

- LDAP
- Kerberos
- FreeIPA
- Active Directory (AD)
- Files
- Proxy


Services
NSS
PAM
SSH
SUDO
AUTOFS
PAC
IFP
SSSD
POSIX Domains
Benutzerinformationen
Gruppeninformationen
Applications Domains
lokaler Cache
SSSD Domänen/Provider
Active Directory
LDAP/Kerberos
FreeIPA/RHEL IDM
Proxy
Files

Provider, Provider, Provider, ...

- `id_provider`
- `auth_provider`
- `chpass_provider`
- `access_provider`
- `sudo_provider`
- `ssh_provider`
- `autofs_provider`
- `ifp_provider`, `selinux_provider`, `hostid_provider`, `session_provider`, ...


ID Provider
auth Provider
access Provider
selinux Provider
SSSD Provider
chpass Provider
session Provider
sudo Provider
hostid Provider
subdomain Provider
Legende
ldap
krb5
ipa
ad
proxy
simple
files
local

AD Provider im Detail

- ID Mapping
  - ID Mapping automatisch
  - ID Mapping basieren auf Posix-Attributen
- SRV Discovery
- Site Discovery
- Global Catalog
- Failover-Strategie
- Password Policy
- Access Provider AD
- GPO für Login-Restriktionen
- Update Computer Password periodisch
- Nutzung Kerberos PAC (Privilege Account Certificate)

AD Pflegetools

`winbind`	Teil des Samba-Projekts
`msktutil`	Kerberos Principal Utility
`realmd`	Discover und Join Utility
`adcli`	User/Gruppen/Computer CLI Tool

AD Join Vorbereitung

Vorbereitung DNS, /etc/resolv.conf

```
search example-ad.test
nameserver 192.168.122.61
```

Optional: /etc/krb5.conf

```
[libdefaults]
 dns_lookup_kdc = true
 forwardable = true
 default_realm = EXAMPEL-AD.TEST
```

AD discover

```
realm discover EXAMPLE-AD.TEST
```

```
example-ad.test
  type: kerberos
  realm-name: EXAMPLE-AD.TEST
  domain-name: example-ad.test
  configured: no
  server-software: active-directory
  client-software: sssd
  required-package: oddjob
  required-package: oddjob-mkhomedir
  required-package: sssd
  required-package: adcli
  required-package: samba-common-tools
```

AD Join mit `realmd`

Eventuell fehlende Pakete installieren, die beim Discover als *required-package* angezeigt werden.

AD Domain Join

```
# realm  join EXAMPLE-AD.TEST --computer-ou=OU=server,OU=firma
Password for Administrator:
```

Domain Infos abfragen

```
# adcli info EXAMPLE-AD.TEST
[domain]
domain-name = example-ad.test
domain-short = EXAMPLE-AD
domain-forest = example-ad.test
domain-controller = ad1-dc1.example-ad.test
domain-controller-site = Default-First-Site-Name
domain-controller-flags = pdc gc ldap ds kdc timeserv closest writable \
good-timeserv full-secret ads-web
domain-controller-usable = yes
domain-controllers = ad1-dc1.example-ad.test
[computer]
computer-site = Default-First-Site-Name
```

AD User/Gruppen Infos

AD Userinfo abfragen

```
# id user1@example-ad.test
uid=270401108(user1) gid=270400513(domain_users) Gruppen=270400513(domain_users),270401106(linux-user)
```

AD Userinfo abfragen

```
# getent group linux-admins@example-ad
linux-admins@example-ad.test:*:270401105:luser1@example-ad.test
```

DNS abfragen

```
dig +short client1.example-ad.test
192.168.122.101
```

Krb5 Keytab prüfen

```
# klist -ke /etc/krb5.keytab
Keytab name: FILE:/etc/krb5.keytab
KVNO Principal
---- --------------------------------------------------------------------------
   6 host/client1.example-ad.test@EXAMPLE-AD.TEST (des-cbc-crc)
   6 host/CLIENT1@EXAMPLE-AD.TEST (des-cbc-crc)
   ....
   6 CLIENT1$@EXAMPLE-AD.TEST (aes256-cts-hmac-sha1-96)
```

Computer TGT testen

```
# kinit -k 'CLIENT1$'
# klist
Ticket cache: FILE:/tmp/krb5cc_0
Default principal: CLIENT1$@EXAMPLE-AD.TEST

Valid starting       Expires              Service principal
....
```

GPO Access

Allow/Deny

log on locally login, su, xdm, kdm, gdm-* , ...

log on through Remote Desktop Services sshd, cockpit

this Computer from the network ftp, samba

log on as batch job crond

log on as service kein Default

Alternative Simple-Provider

- einfache user-/gruppenbasierte Zugriffskontrolle
- geringere Anfälligkeit als in komplexen AD-/LDAP-Filtern
- Unterstützung geschachtelter Gruppen

Zeit für ein wenig Praxis

Vielen Dank für Ihre Aufmerksamkeit!

Bei weiteren Fragen wenden Sie sich bitte an info@b1-systems.de oder +49 (0)8457 - 931096