Implementing Linux Authentication and Authorisation Using SSSD

Lawrence Kearney
Enterprise Service and Integration Specialist
Technology Transfer Partnership (TTP)
lawrence.kearney@earthlink.net

Mark Robinson
Trainer and Consultant
mrlinux training & consultancy
mark@mrlinux.co.uk

What is SSSD?

SSSD package description:

Provides a set of daemons to manage access to remote directories and authentication mechanisms.

Provides an NSS and PAM interface toward the system and a pluggable backend system to connect to multiple different account sources.

What's In a Name?

Seriously ?!

“System Security Services Daemon”

We would have very happily accepted:

“Single Sign on Service Daemon”

“Simple Sign on Solution Daemon”

Even:

“Simplesmente Autenticação Serviços Daemon”

Moving On
(There is Lab Work To Do...)

What need is SSSD addressing?

- PAM and NSS frameworks have scaling caveats
- Specialised directories stores are proliferating
- Linux platforms as viable federation candidates
- Better Active Directory® integration is more mission critical

SSSD Advantages

Authentication service enhancements

- Greater extensibility
- Multiple concurrently available identity stores
- ID collision management features
- SSL/TLS or SASL/GSSAPI is required
- Single configuration file
- Reduced server loads
- Offline authentication

SSSD Disadvantages

Microsoft Windows® or Samba file shares

Still require winbindd be configured and used (for now)

NFS file shares

May still require nscd but without user and group caching

Migrating from configurations using id mapping can be more complex

The SSSD Configuration File

SSSD Domain = Identity Provider + Authentication provider

[sssd] services = domains =	Global parameters
[nss], [pam], [sudo] reconnection_retries = filter_users =	Service parameters
[domain/NAME] id_provider = auth_provider = chpass_provider = access_provider =	SSSD domain parameters

SSSD Providers

Local	Accounts are kept in a local database
LDAP	Relies on installed extensions of target directory
Kerberos	Relies on installed extensions of target directory
AD	Supports many native Active Directory® features
iPA	Supports trusts with Active Directory® domains
IdM	Integrates tightly with IdM® implementations
Proxy	Permits integration of other provider modules

SSSD Provider Roles

Id, Authentication, Access Control and Changing Passwords

id_provider = ldap, ipa, krb5, ad, proxy

auth_provider = ldap, ipa, krb5, ad, proxy

access_provider = permit, deny, ldap, ipa, ad, simple

chpass_provider = ldap, ipa, krb5, ad, proxy, none

- Most providers fulfill multiple roles
- Different providers can, and often are combined

SSSD Processes

SSSD uses a parent/child process monitoring model

[sssd]	Parent process, Monitor
[nss]	Child process, Responder
[domain/LDAP]	Child process, Provider

SSSD Processes

SSSD process example:

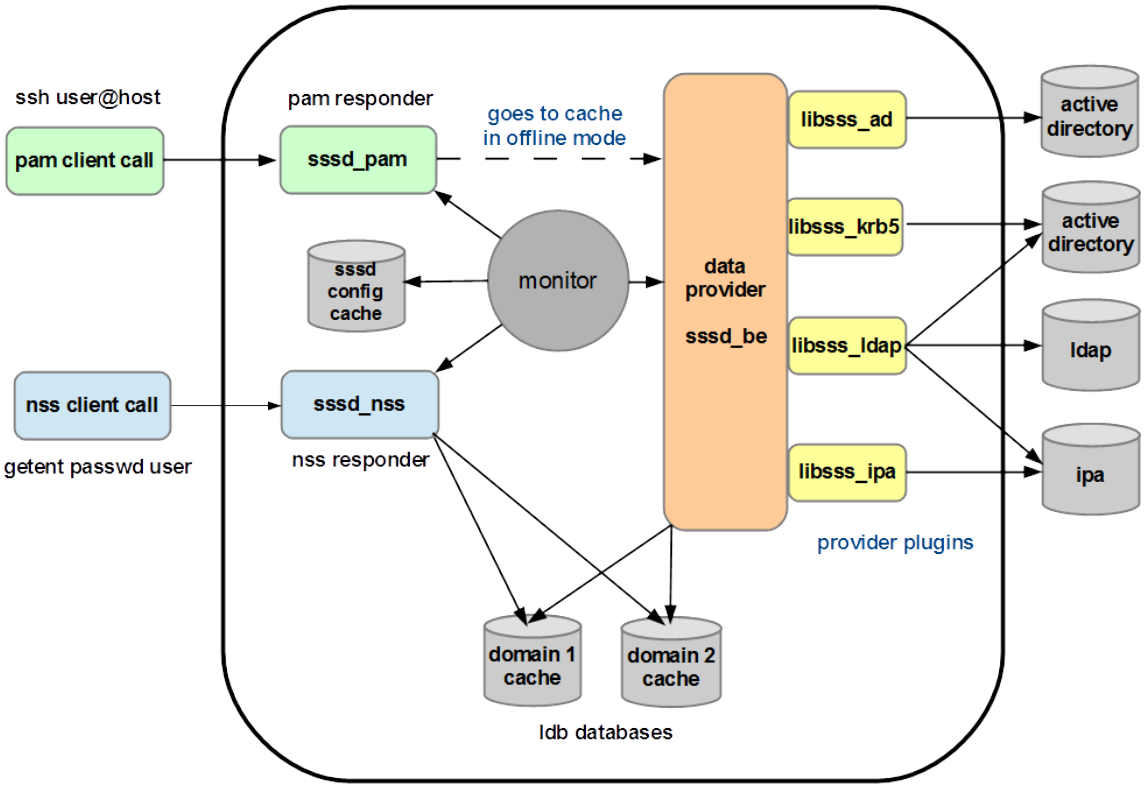
ps -eaf | grep sssd

```
root  1476     1      0    /usr/sbin/sssd
root  1478     1476   0    /usr/libexec/sssd/sssd_nss
root  41279    1476   0    /usr/libexec/sssd/sssd_be --domain LDAP
```

pstree -A -p 1476

```
sssd (1476)    -  +  - sssd_be (41279)
                     |  - sssd_nss (1478)
```

SSSD Architecture



Deploying SSSD

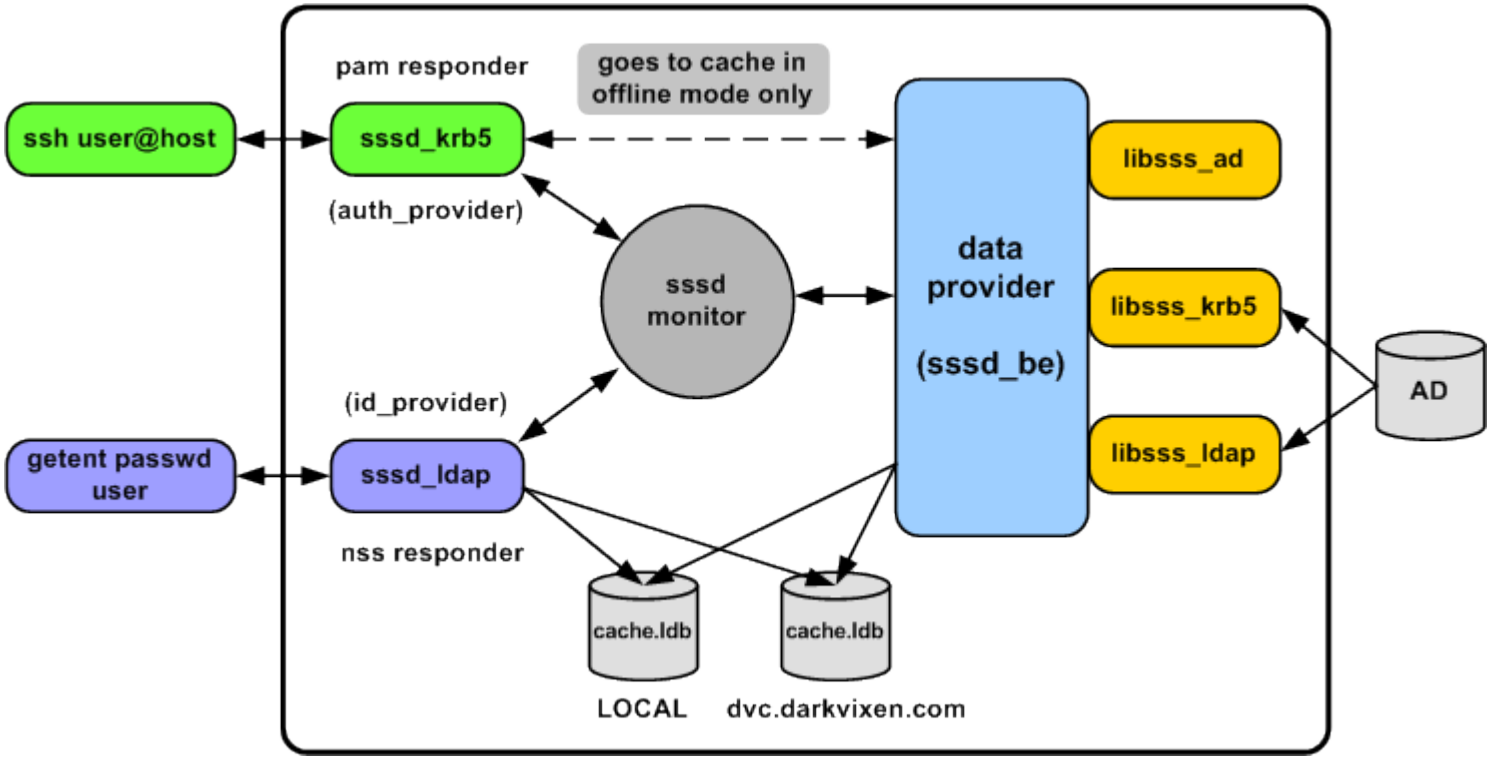
Determine how posix attributes will be provided
Provided by directory service or Linux ID mapping

Install software on your platform
Typically samba and kerberos are required for initial setups
Not all distributions package SSSD similarly

Configure transport security
TLS/SSL for eDirctory® and Active Directory® over LDAP
SASL/GSSAPI for Active Directory® over LDAP/kerberos

Configure SSSD identity providers (and access providers?)

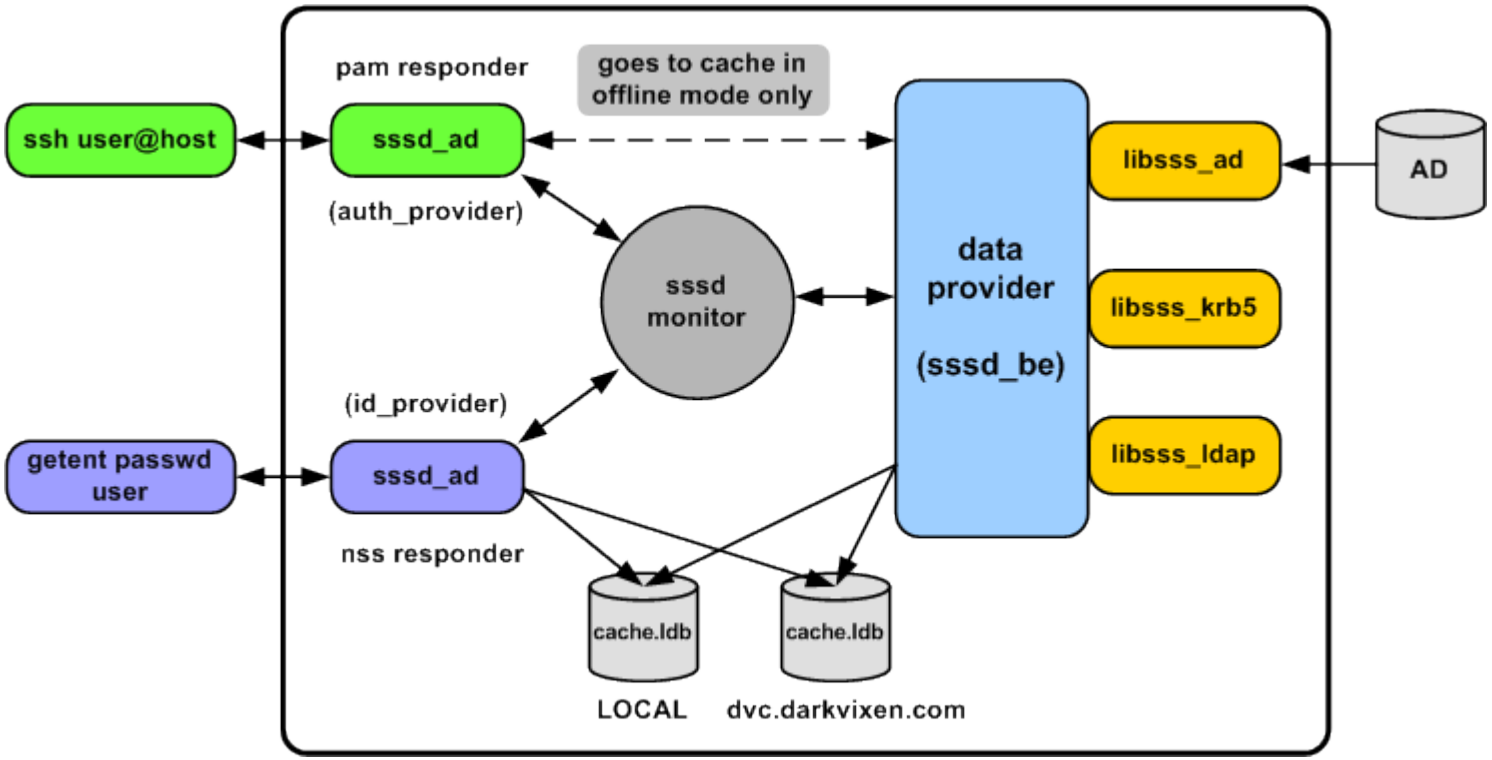
LDAP ID and Kerberos Auth Providers



SUSE Linux Enterprise 11 SSSD

LDAP and Kerberos Providers

Active Directory ID and Auth Providers



SUSE Linux Enterprise 12 SSSD

Active Directory Provider

Corporate Headquarters
Maxfeldstrasse 5
90409 Nuremberg
Germany

+49 911 740 53 0 (Worldwide)
www.suse.com

Join us on:
www.opensuse.org