The System Security Services Daemon (SSSD), SLES12 and Active Directory

Lawrence Kearney
System Administrator Principal
The University of Georgia
lkearney@uga.edu

Mark Robinson
Trainer and Consultant
Mrlinux training and consultancy (U.K.)
mark@mrlinux.co.uk

SSSD 101

First, Seek to Understand

Features and Architecture of the SSSD:

- The needs the SSSD is addressing
- The advantages of the SSSD
- Speaking SSSD

The Needs Addressed by the SSSD

Legacy PAM and NSS Framework Caveats

Complex configurations that do not scale easily

Linux servers dedicated authentication to one remote back end

Relatively poor Active Directory integration

No real offline authentication capability

The Needs Addressed by the SSSD

Modern Linux Infrastructure Needs

Specialised directory stores are proliferating

Linux platforms limited as viable federation candidates

Better Active Directory integration is more mission critical

Reduced configuration and operational complexity

The Advantages of using the SSSD

Authentication service enhancements

Greater extensibility

Multiple concurrently available identity stores

Active Directory integration approaching domain member servers

ID collision management features

SSL/TLS or SASL/GSSAPI is required

Single configuration file

Reduced server loads

Offline authentication

Speaking SSSD

Daemon concepts and components

SSSD concepts				
The Monitor	Parent process for all SSSD processes			
Providers	Modules with specific auth back end awareness			
Responders	Interact with Linux and implement features			
SSSD components				
SSSD Provider	--->	SSSD Responder	--->	SSSD Monitor
libsss_ldap.so	--->	sssd_nss	--->	sssd
/etc/sssd/sssd.conf	Monitor, provider and responder configuration			

Speaking SSSD

The 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 Active Directory domains
Proxy	Permits integration of other provider modules
autofs	Supports integration using LDAP
sudo	Supports integration using LDAP

Speaking SSSD

What are IPA and IdM Back Ends?

Free IPA is an integrated Identity and Authentication solution for Linux/UNIX networked environments.

Version 3 began focus is on Active Directory® integration

IdM is a way to create identity stores, centralized authentication, domain control for Kerberos and DNS services, and authorization policies on Linux systems, using native Linux tools.

Integration focus heavily favours Active Directory.

Speaking SSSD

The SSSD Responders

[nss]	User and group name resolution	(**configurable**)
[pam]	User and group authentication control	(**configurable**)
[autofs]	Automounter control	(**configurable**)
[sudo]	Sudo rule control	(**configurable**)
[ssh]	openSSH public key control	(**configurable**)
[sssd_be]	SSSD back end control	(**non-configurable**)

The SSSD Configuration File

SSSD Authentication Domain = Identity Provider + Authentication provider

[sssd]	Global/Monitor configuration directives
services =	Responders to start and monitor
domains =	(authentication domains and search order)
[nss], [pam], [sudo]	Responder configuration directives
reconnection_retries =	
filter_users =	
[domain/NAME]	SSSD authentication domain configuration directives
id_provider =	
auth_provider =	

The SSSD Processes

SSSD uses a parent/child process monitoring model

[sssd]	Parent process, Monitor
[nss]	Child process, Responder
[domain/ad.domain]	Child process, Provider(s)

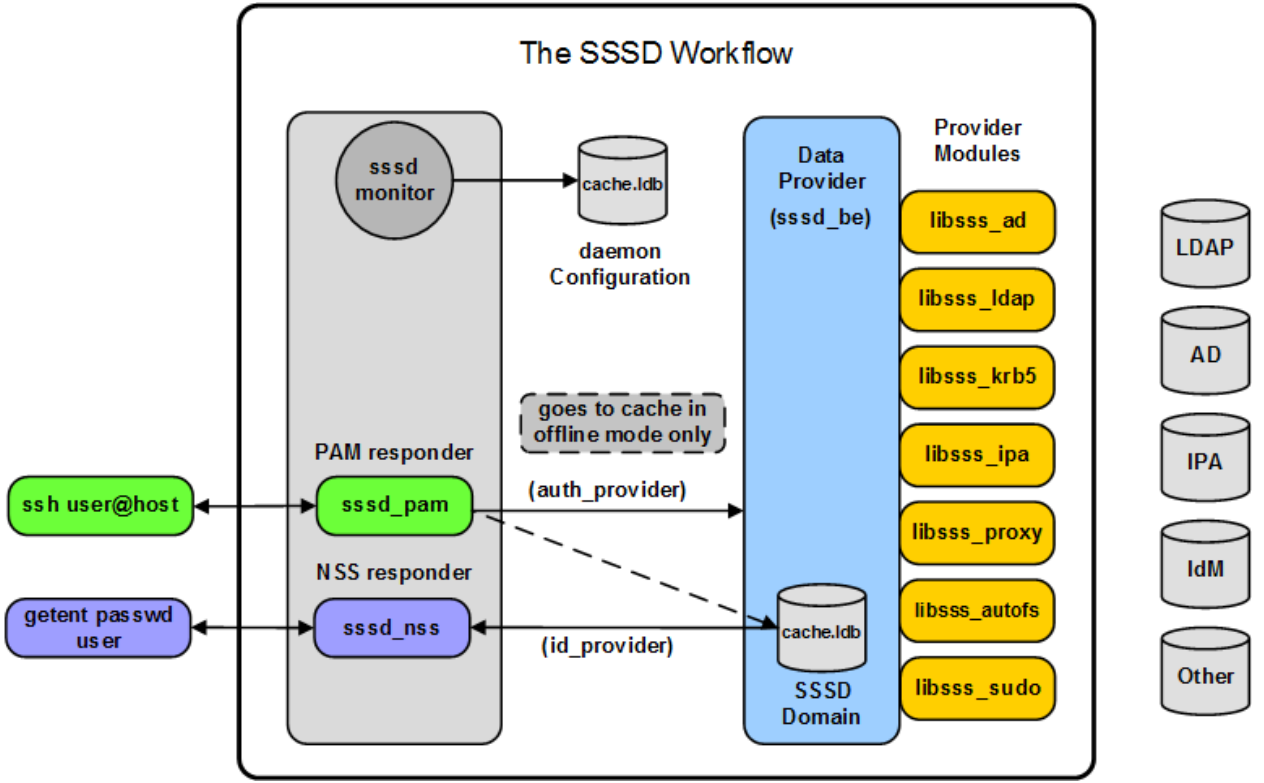
The SSSD Processes

~# 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
ad.dom.com
```

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

The Complete Picture



Before You Deploy

First, Seek to Understand

Decisions, requirements and advice:

- POSIX attributes
- LDAP Providers
- LDAP and Kerberos Providers
- Active Directory Providers
- Other back end clients

POSIX Attribute Standards

Active Directory schema vs. LDAP schemas

Active Directory	LDAP RFC
MsSFU30UidNumber	uidNumber
msSFU30GidNumber	gidNumber
MsSFU30Gecos	gecos
MsSFU30HomeDirectory	unixHomeDirectory
MsSFU30LoginShell	loginShell

POSIX Attribute Planning

Planning and design requirements before deploying

POSIX attributes

Where they come from is important

Changes can impact access

POSIX Attribute Planning

Two methods can provide Linux POSIX attributes:

- Dynamically mapping user and group attributes using the SSSD
- Storing user and group attributes in the directory

Only one method can be implemented per SSSD domain

Migrating systems using PAM_LDAP is not complex

Migrating using existing LDAP back ends is not complex

Migrating domains between methods can be complex

POSIX Attribute Planning

Storing and managing POSIX attributes in the directory:

- Identity Management for UNIX role can still be used
- Other identity management tools or systems can be used
- Provisioning, planning and design tasks
- Greater control over user primary group assignments
- Greater control over other user and group Linux attributes
- Less possibility of UID and GID collisions

POSIX Attribute Planning

Dynamically mapping user/group attributes using the SSSD:

- Simple to deploy using the SSSD software stack
- Fewer Linux specific provisioning tasks
- Uniquely generated user and group UIDs and GIDs
- Less possibility of UID and GID collisions

- Less control for user primary group assignment
- Less control over other user and group Linux attributes
- Some Active Directory® attributes applied by local system defaults

User Home Directory Planning

Home directories are POSIX attributes with file system bits

Use cases to consider:

- Do users have home directories on remote servers that will be mounted?
- Should home directories be created on user login?
- Should user home directories for be redirected, or reference another path for SSSD authentication domains?

The SSSD LDAP Providers

Use cases:

- Maximum compatability with multiple back ends
- Can utilise SSL and TLS security
- Does not require Domain membership

The SSSD LDAP and Kerberos Providers

Use cases:

- Reasonable compatability with Active Directory, IPA and IdM back ends
- Can utilise SSL, TLS and SASL\GSSAPI security
- Requires Domain membership

The SSSD Active Directory Providers

Use cases:

- Member server compatability with Active Directory, IPA and IdM back ends
- Requires SASL\GSSAPI security
- Requires Domain membership

The openLDAP, Kerberos and Samba Clients

Why install and configure these clients:

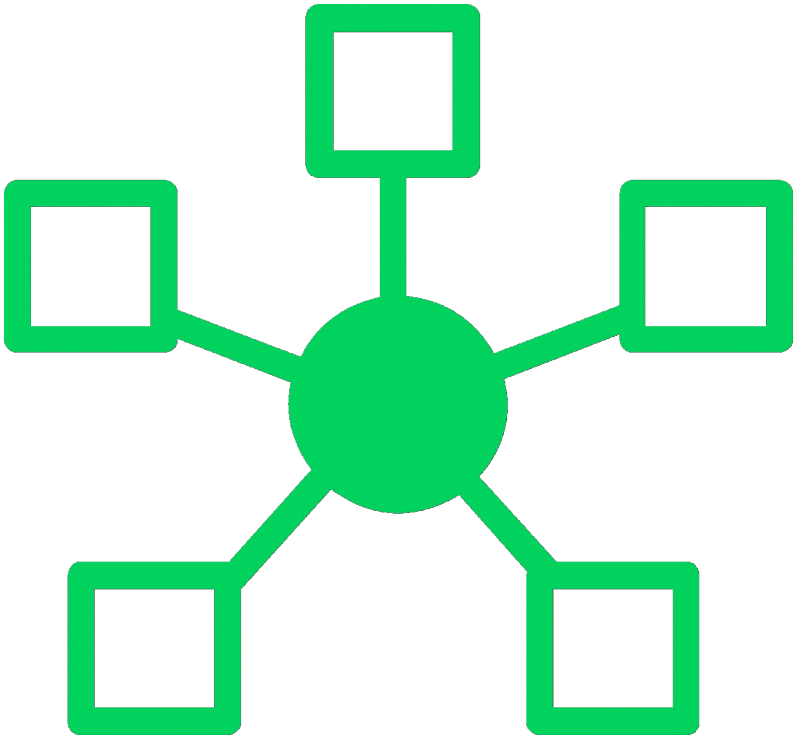
- Perform initial Active Directory domain integration tasks the SSSD Kerberos provider cannot
- Provide “out of band” tools for troubleshooting Active Directory connectivity and protocols (SSL, TLS and SASLGSSAPI)
- Provide CLI tools for manual and scripted server deployments for joined servers
- Provide CLI tools for Kerberos keytab file updates
- Require minimal configuration to obtain maximum benefits

Deployment

Deployment

Decisions made:

- Direct or indirect integration with Active Directory
- Mapped vs. non-mapped ID models
- Home directory model to use
- SSSD providers to use



Deployment

Procedures:

- Install SSSD software
- De-configure PAM LDAP and Kerberos configurations (**migration**)
- Disable name service caching daemon (**migration**)
- Configure SSSD software

Deployment Examples (LDAP Providers)

[domain/**LDAP1**]
id_provider = **ldap**
auth_provider = **ldap**

enumerate = false
cache_credentials = true

ldap_schema = ad

Most of the file is omitted for brevity, remainder of file shown in session

Deployment Examples (LDAP-Kerberos Providers)

[domain/**dvc.darkvixen.com**]
id_provider = **ldap**
auth_provider = **krb5**

enumerate = false
cache_credentials = true

ldap_schema = ad

Most of the file is omitted for brevity, remainder of file shown in session

Deployment Examples (Active Directory Providers)

[domain/**dvc.darkvixen.com**]
id_provider = **ad**
auth_provider = **ad**

enumerate = false
cache_credentials = true

ad_server = _srv_,darkvixen160win.dvc.darkvixen.com

Some of the file is omitted for brevity, remainder of file shown in session

Questions

Contact, info and additional training

Lawrence Kearney:
email: lawrence.kearney@earthlink.net
Presentations and articles: www.lawrencekearney.com
Tutorial videos: Doing stuff with the SSSD

SUSECON:

Implementing the SSSD using SLES12 and Active Directory - **HO85752**

SUSE Training:

Administering SSSD on SUSE Linux Enterprise Server 12 - **SLE342**


SUSE®
We adapt. You succeed.