Implementing the SSSD using SUSE® Linux Enterprise Server 12 and Active Directory

Lawrence Kearney
System Administrator Principal
The University of Georgia
TTP Advisory Board member
lkearney@uga.edu

Mark Robinson
Trainer and Consultant
mrlinux training and consultancy (U.K.)
TTP Advisory Board member
mark@mrlinux.co.uk

What is the 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 back end system to connect to multiple different account sources.

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

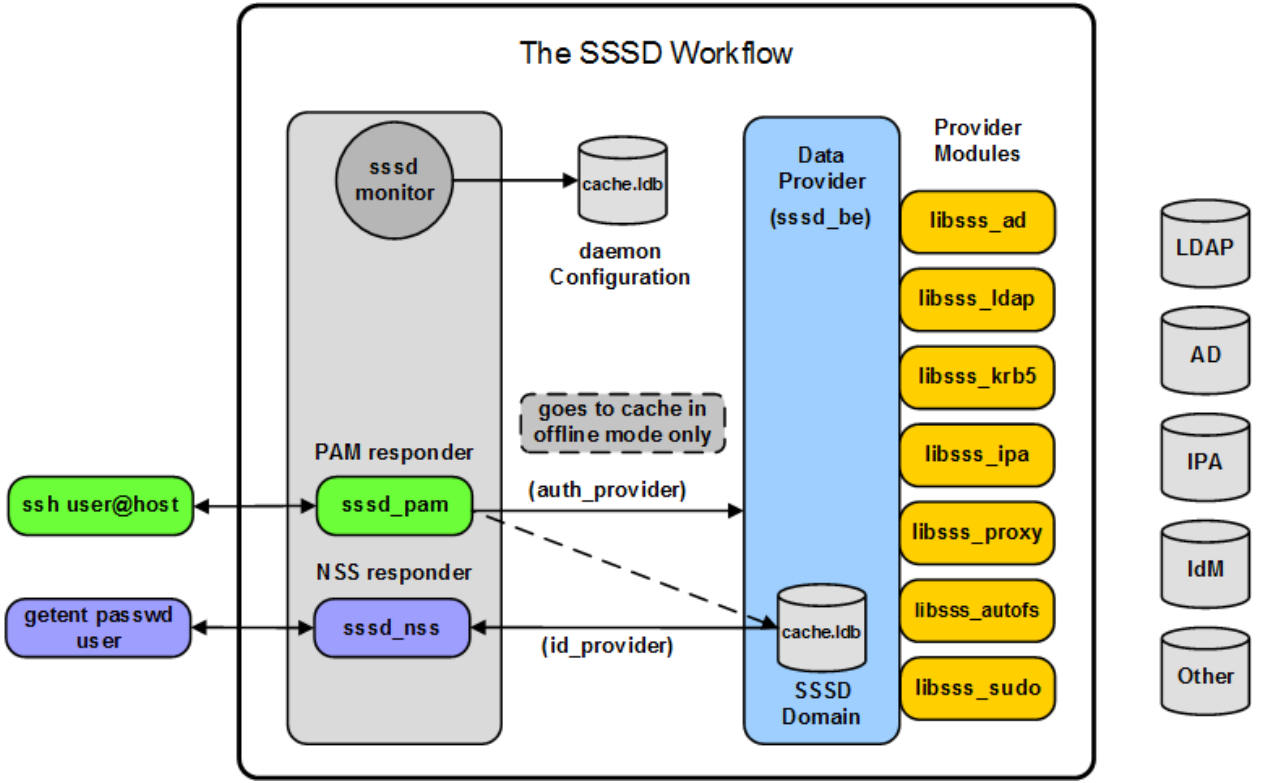
[sssd]	Global/Monitor configuration directives
services =	Responders to start and monitor
domains =	(authentication domains and search order)
[nss], [pam], [sudo]	Responder configuration directives
reconnection_retries =	
filter_users =	
[domain/NAME]	SSSD authentication domain configuration directives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

The SSSD Processes

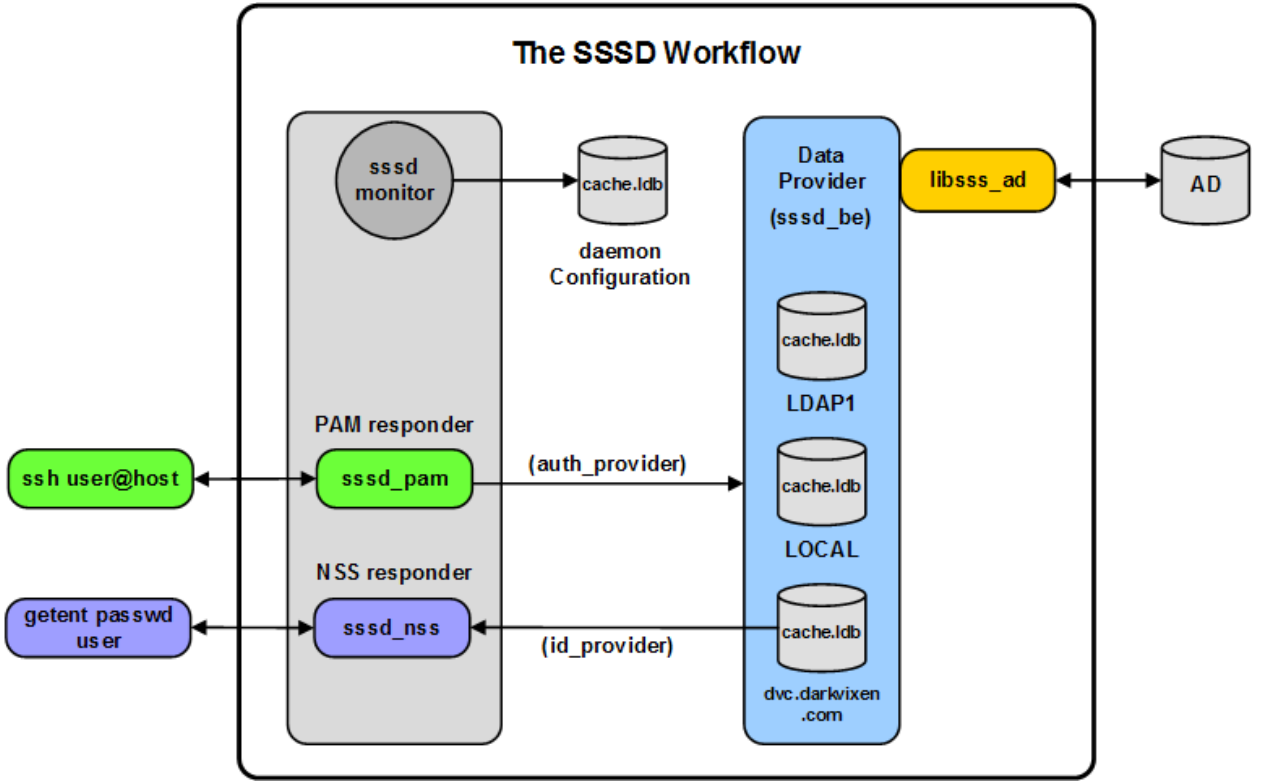
SSSD uses a parent/child process monitoring model

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

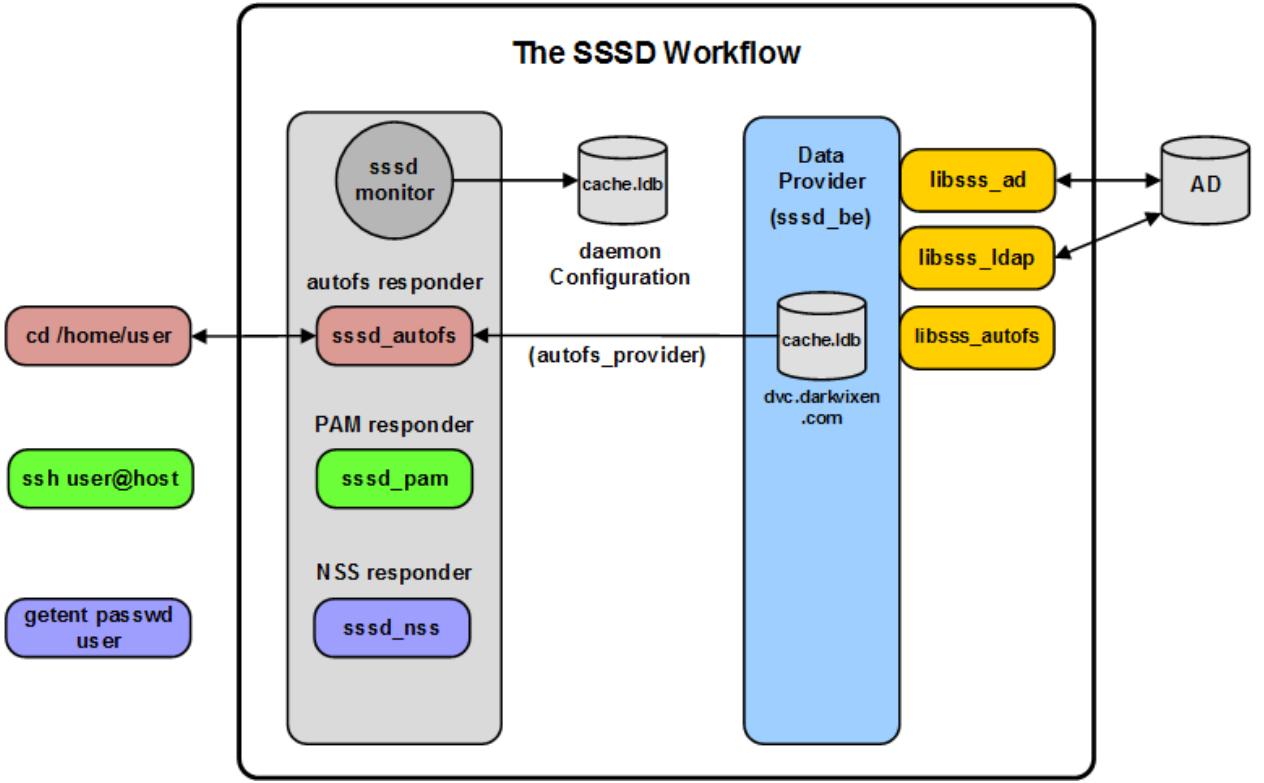
The Complete Picture



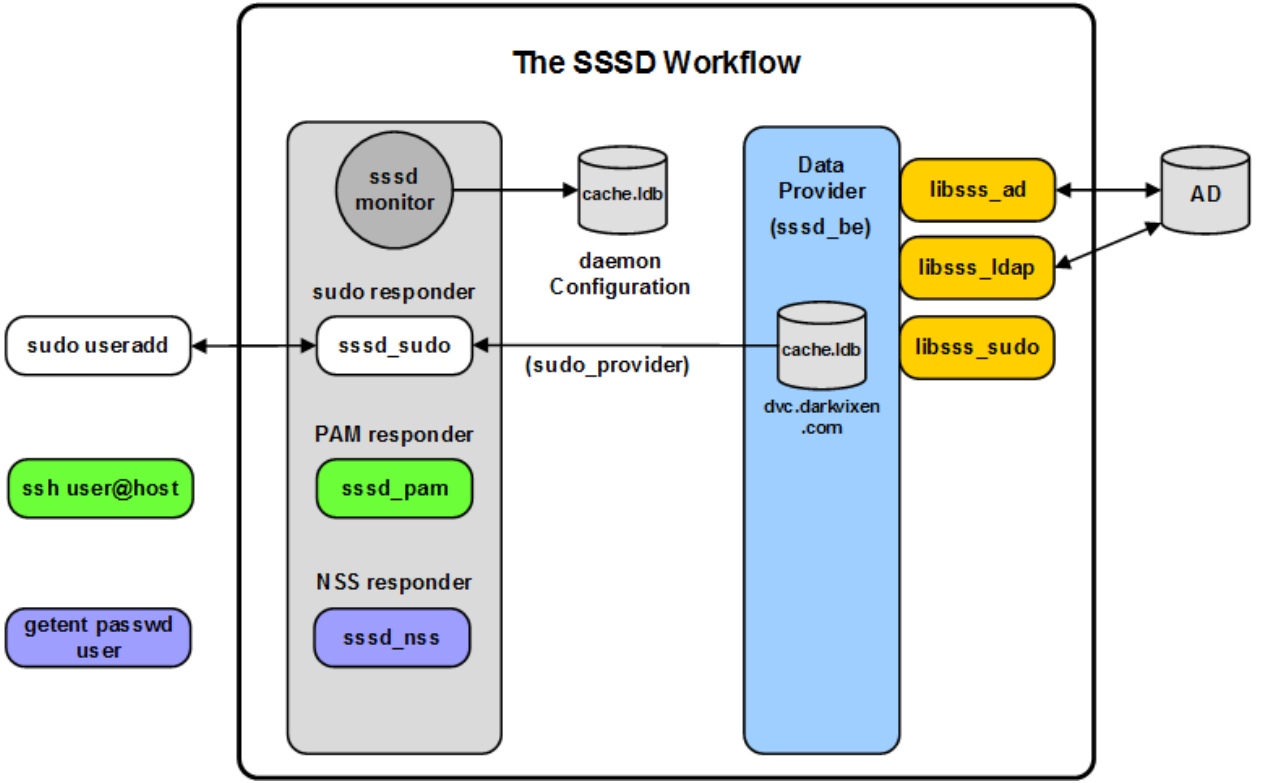
The Active Directory Providers



The AutoFS Provider



The Sudo Provider



SUSE Linux Enterprise 12 lab
SSSD Active Directory, autofs and sudo providers

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

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


SUSE®
We adapt. You succeed.