

# Implementing Linux Authentication and Authorisation Using SSSD

## **Lawrence Kearney**

Enterprise Service and Integration Specialist  
Technology Transfer Partnership (TTP)  
[lawrence.kearney@earthlink.net](mailto:lawrence.kearney@earthlink.net)

## **Mark Robinson**

Trainer and Consultant  
mrlinux training & consultancy  
[mark@mrlinux.co.uk](mailto: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]                      Global parameters  
services =  
domains =

[nss], [pam], [sudo]      Service parameters  
reconnection\_retries =  
filter\_users =

[domain/NAME]              SSSD domain parameters  
id\_provider =  
auth\_provider =  
chpass\_provider =  
access\_provider =



# 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**

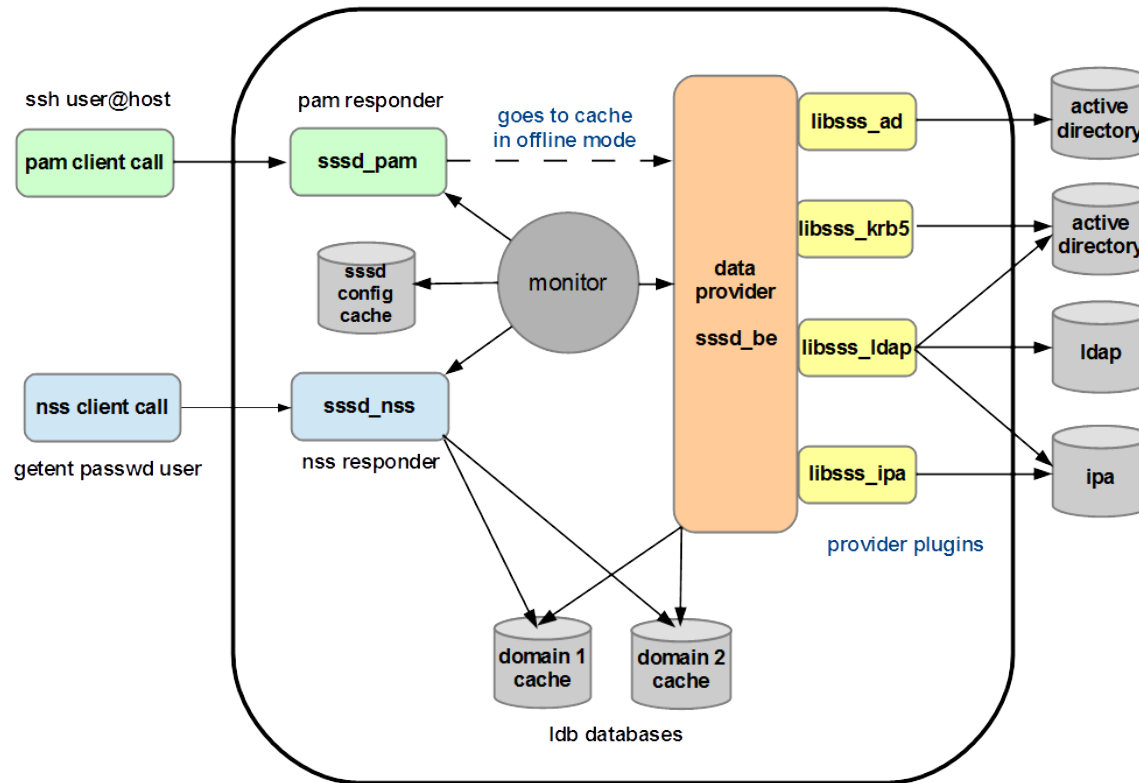
```
root 1476      1          0   /usr/sbin/sss  
root 1478      1476       0   /usr/libexec/sss/sss_nss  
root 41279     1476       0   /usr/libexec/sss/sss_be --domain LDAP
```

**pstree -A -p 1476**

```
sss (1476)  - + - sss_be (41279)  
            | - sss_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

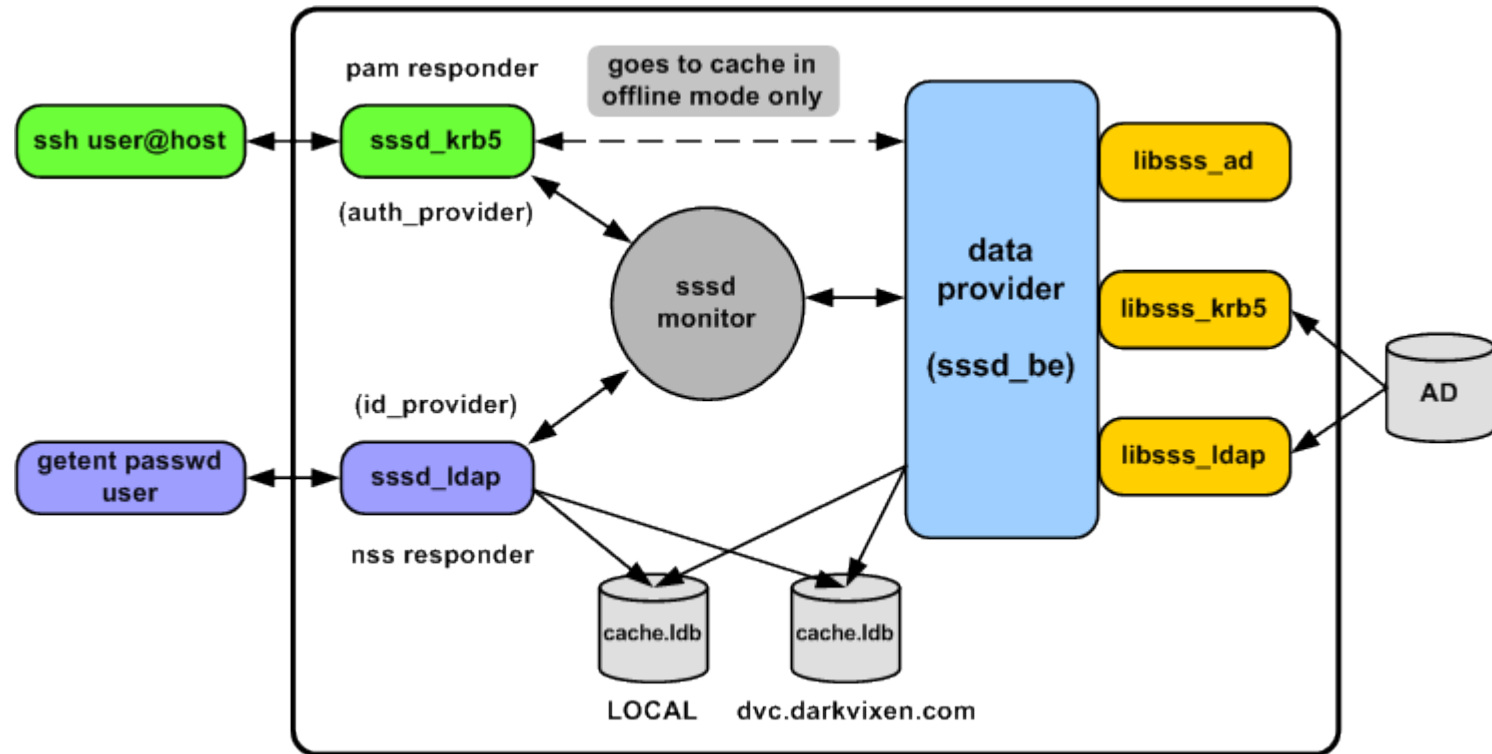
TLS/SSL for eDirectory® and Active Directory® over LDAP

SASL/GSSAPI for Active Directory® over LDAP/kerberos

Configure SSSD identity providers (and access providers?)



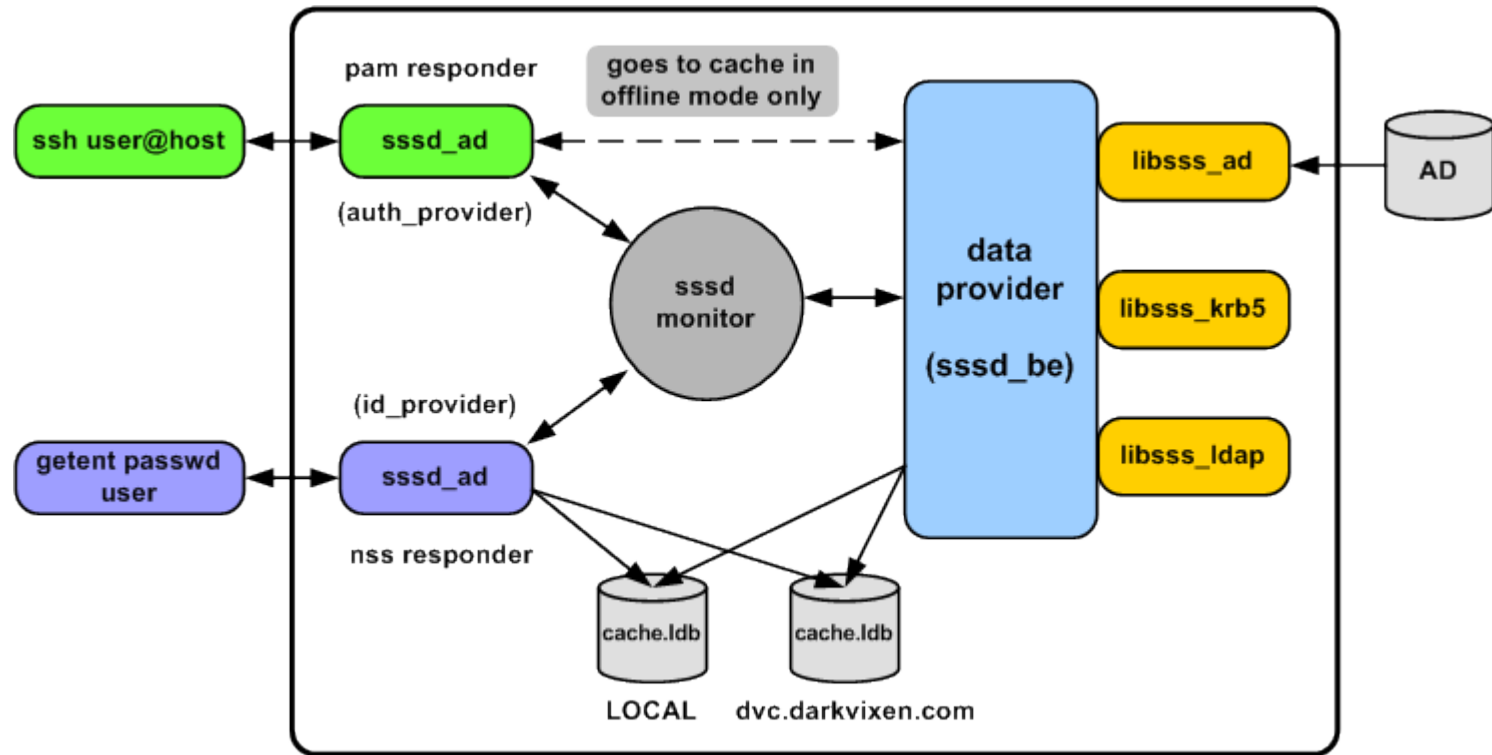
# LDAP ID and Kerberos Auth Providers



# 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](http://www.suse.com)

Join us on:  
[www.opensuse.org](http://www.opensuse.org)

## **Unpublished Work of SUSE LLC. All Rights Reserved.**

This work is an unpublished work and contains confidential, proprietary and trade secret information of SUSE LLC. Access to this work is restricted to SUSE employees who have a need to know to perform tasks within the scope of their assignments. No part of this work may be practiced, performed, copied, distributed, revised, modified, translated, abridged, condensed, expanded, collected, or adapted without the prior written consent of SUSE. Any use or exploitation of this work without authorization could subject the perpetrator to criminal and civil liability.

## **General Disclaimer**

This document is not to be construed as a promise by any participating company to develop, deliver, or market a product. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. SUSE makes no representations or warranties with respect to the contents of this document, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. The development, release, and timing of features or functionality described for SUSE products remains at the sole discretion of SUSE. Further, SUSE reserves the right to revise this document and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes. All SUSE marks referenced in this presentation are trademarks or registered trademarks of Novell, Inc. in the United States and other countries. All third-party trademarks are the property of their respective owners.

