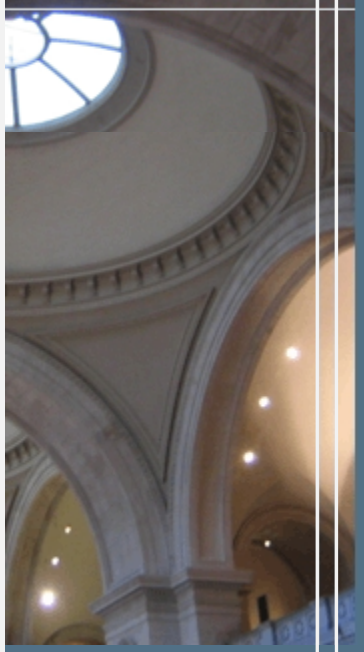
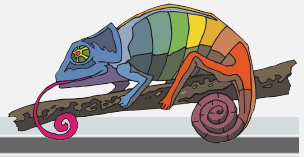


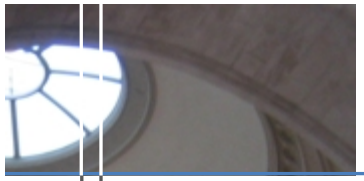


Technology Transfer Partners

# Linux authentication using the System Security Services Daemon (SSSD) explained

Lawrence Kearney
TTP Advisory Board
System Administrator Principal
The University of Georgia (USA)

e. lawrence.kearney@earthlink.net
w. www.lawrencekearney.com





Initially, the answer to all my computer managers questions was:

# “ I Dunno' ”

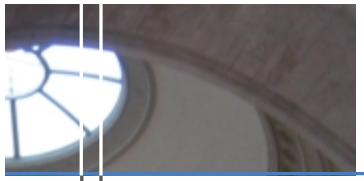
## Origins in the freeIPA project (**I**dentity, **P**olicy and **A**udit)

There is a freeIPA client

## Red Hat originates a new client project

Narrower in scope
Provided funding and (2) dedicated developers
Commercially viable software base to bubble up from the Cent OS and Fedora projects

Thank goodness!  A name change opportunity is upon us!





## Seriously ?!

“System Security Services Daemon”

## We would have very happily accepted:

“Single Sign on Service Daemon”
“Simple Sign on Solution Daemon”

## Even:

“Simplesmente Sancionar Servicos Daemon”

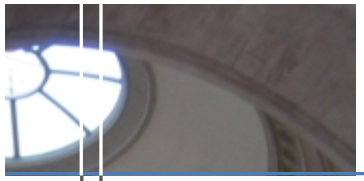
## What need is SSSD addressing?

PAM and NSS frameworks have scaling caveats, and are becoming legacy as identity management frameworks evolve

Linux servers currently aren't ideal federation platform candidates as a result

LDAP directories are becoming more specialised and are proliferating

Better Active Directory integration is more mission critical





Local files

☑ ticked, next

Network Information Service (NIS)

☑ ticked, next

pam_unix  nss_ldap

Local authentication, remote user store

Password management

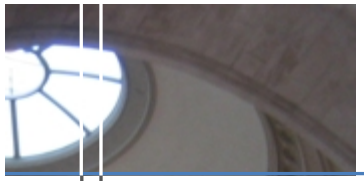
No session management

pam_ldap  nss_ldap

Secure remote user look up and authentication

Password management

No session management





pam_ldap  pam_krb5  nss_ldap

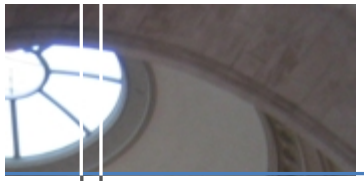
Secure remote user look up and authentication

Password management

Session management (SSO capable)

MIT kerberos capable

MS Windows® and Active Directory for Domains capable



# The usual suspects

pam_ldap pam_krb5 pam_winbind nss_ldap

Secure remote user lookup and authentication

Password management

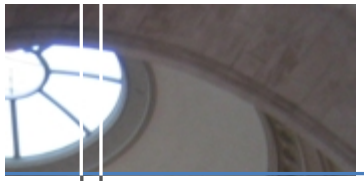
Session management (SSO capable)

MIT kerberos capable

MS Windows® RPC capable

MS Windows® and Active Directory for Domains capable

MS Windows® file share participation





## Name Service Caching daemon (nscd)

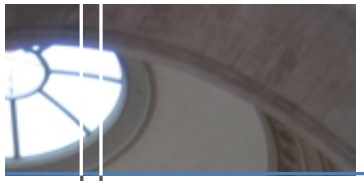
Next query caching for users, groups, hosts and services
No offline authentication but can maintain active sessions

## Windows Bind daemon (winbindd)

Does not require remote posix attributes
Requires AD Domain joining
Serves as a front end for PAM, NSS and Samba

## LDAP Name Service daemon (nslcd)

Simplified configuration file
Requires remote posix attributes
Does not require AD Domain joining





Large scale deployments become complex

/etc/nscd.conf /etc/nslcd.conf /etc/nsswitch.conf

/etc/samba/smb.conf /etc/samba/secrets.tdb

/etc/ldap.conf /etc/openldap/ldap.conf /etc/winbind.conf

/etc/krb5.conf /etc/krb5.keytab

/etc/pam.d /* /etc/autofs_auth_ldap.conf /etc/pam_ldap.conf

**SUSE Red Hat / CentOS / Fedora Ubuntu Debian**

Workforce and administrator skill set considerations ...

## Authentication service enhancements

Greater extensibility

Multiple concurrently available identity stores

Single configuration file

Reduced server loads

Security is required

SASL/GSSAPI, Kerberos and SSO features

ID collision features

Offline authentication

## Configuration consolidation

Backward compatible with legacy PAM / NSS stacks

Legacy PAM / NSS / winbindd[1] modules not required

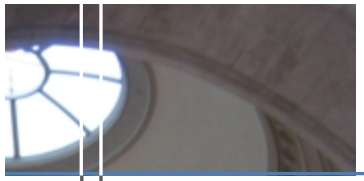
Integrates with windbindd[1] if necessary

Integrated service configurations (ssh, sudo, autofs, cifs[1] etc.)

Uniform configuration methods across platforms

Reduced complexity

[1] Current versions are supporting some of these features





## MS Windows® or Samba file shares

Still require winbindd be configured and used

## NFS file shares

May still require nscd but without user and group caching

## Interactions with some older Linux applications

Those that aren't flexible concerning case

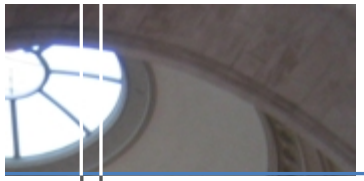
Those that will only talk to legacy PAM and NSS modules

## Migrating configurations that use id mapping can be more complex

Seriously, if I type:

# “SSSH” or “SSSL”

One more time I may scream !!





SSSD uses a parent/child process monitoring model

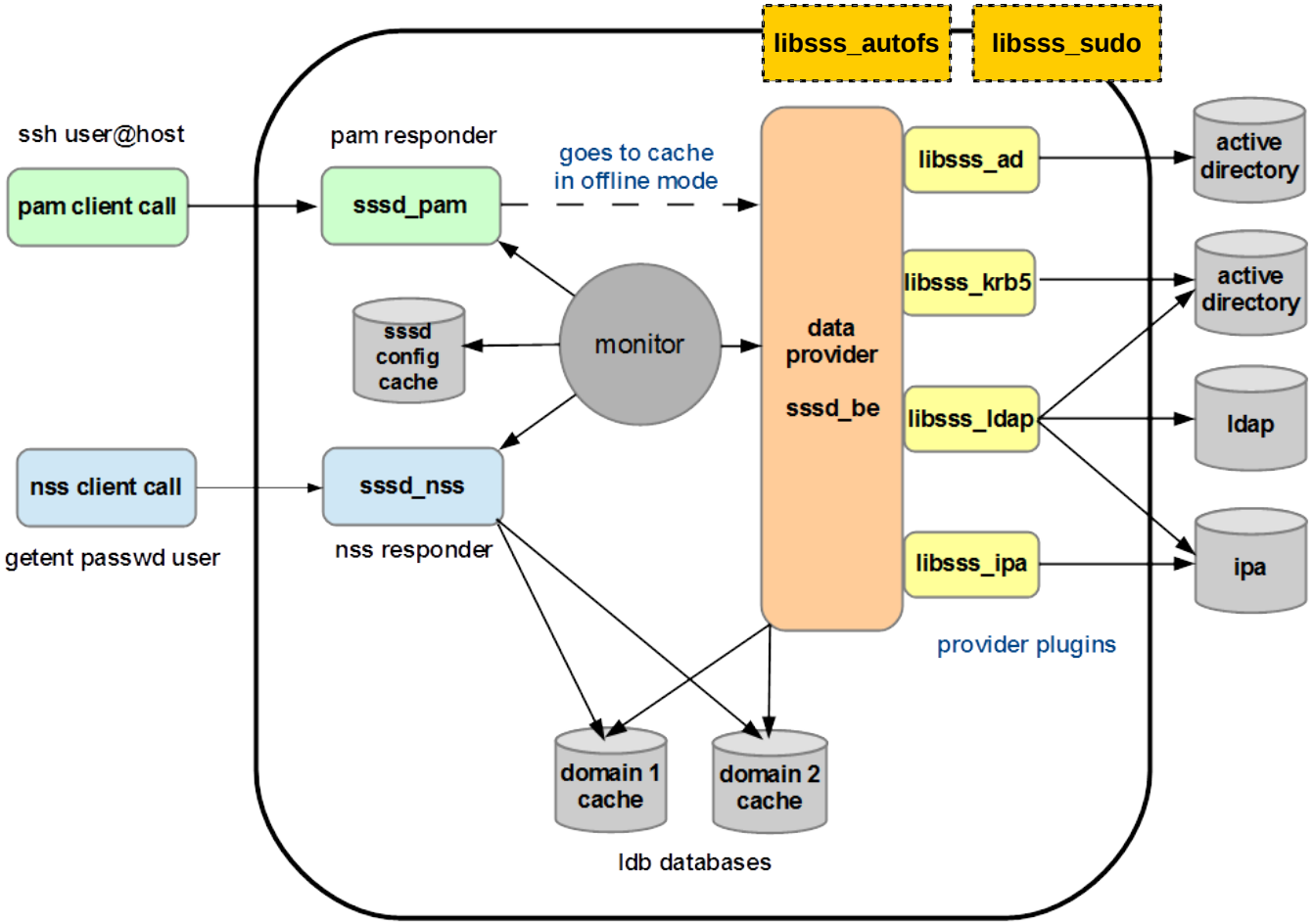
/etc/sssd/sssd.conf file

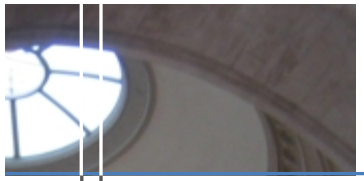
| | |
|---|---|
| [sssd] | Parent process, Monitor |
| [nss] | Child process, Responder |
| [domain/LDAP] | Child process, Provider |

## 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 overview





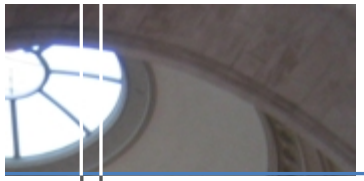


[sssd] Global parameters
services =
domains =

[nss], [pam], [sudo] Service parameters
reconnection_retries =
filter_users =

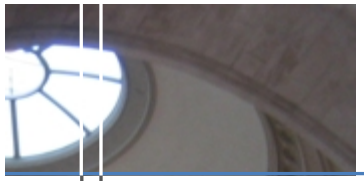
[domain/NAME] SSSD domain parameters
id_provider =
auth_provider =
chpass_provider =
access_provider =

SSSD Domain = Identity Provider + Authentication provider





| | |
|---|---|
| Local | Accounts are kept in a ldb database |
| LDAP | Relies on installed extensions of target directory |
| Kerberos | |
| AD | Supports many native Active Directory features |
| iPA | Supports trusts with Active Directory domains |
| IdM | Integrates tightly with RHEL IdM implementations |
| Proxy | Permits integration of other providers |





## Local

Enhanced local account features
Familiar local user management tools

## LDAP

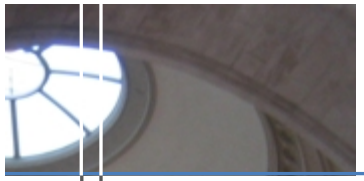
Flexible attribute mapping capabilities

## Kerberos

SASL/GSSAPI support improves application support

## AD

Login performance improvements
Trust and domain auto-discovery features
Native schema, DNS update and security support





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

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

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

Different providers can and often are be combined

## Many Linux distributions are now SSSD aware

Auto-configuration using native distribution utilities

## Enterprise Linux distributions include

| | |
|---|---|
| Red Hat Enterprise Linux 5.6: | SSSD 1.5 * |
| Red Hat Enterprise Linux 6: | SSSD 1.9 |
| Red Hat Enterprise Linux 7: | SSSD 1.11 |
| SUSE Linux Enterprise Server 11.2: | SSSD 1.9 |
| SUSE Linux Enterprise Server 12: | SSSD 1.11 |

## Identify existing services that should be modified

PAM LDAP and NSS LDAP configurations

NSCD user, group, host or service caching

## 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 setup[2]
Not all distributions package SSSD uniformly

## Configure transport security

TLS/SSL for eDirectory over LDAP
TLS/SSL for AD over LDAP
SASL/GSSAPI for AD over LDAP/Kerberos

## Configure SSSD identity providers and access control

Identity and access control providers can be mixed

[2] Initial connectivity to AD domains requires legacy Linux tools

SUSE and Red Hat are aligning with AD integration maturity

Would like to see the AD id provider included in SLES 11.4*

## SSSD 1.11

Realmd utility will auto-configure AD id provider

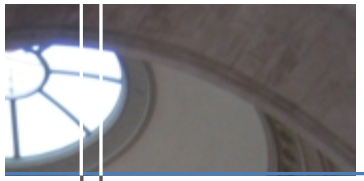
Expanded AD access control provider

NetBIOS/DNS domain name auto-discovery

## Beyond 1.11

AD access control provider will include group policy support

SSSD CIFS integration





# Thank you for attending!

Come to the workshop later in the week

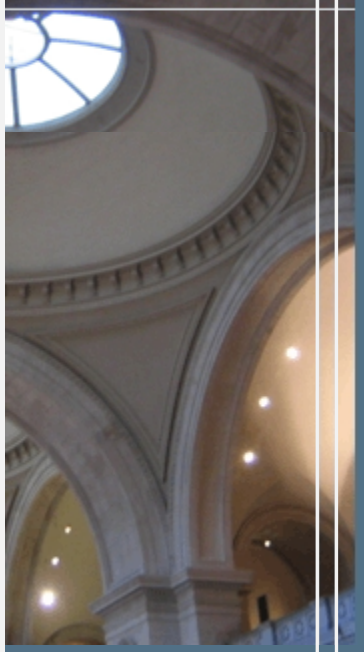
SLES 11 and 12 deployment examples and labs

Implementing SSL/TLS and SASL/GSSAPI security

Active Directory for Domains configurations

LDAP / Kerberos and AD SSSD provider configurations

Basic and advanced SSSD configurations



# Questions

Lawrence Kearney
TTP Advisory Board
System Administrator Principal
The University of Georgia (USA)

e. lawrence.kearney@earthlink.net
w. www.lawrencekearney.com