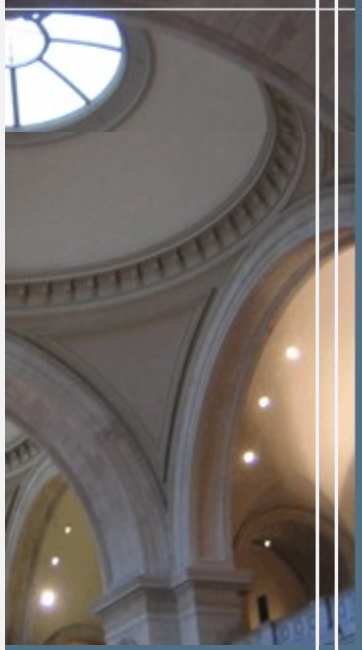


Stuff everyone should know about the SSSD

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

e. lkearney@uga.edu
w. www.lawrencekearney.com

John Webb
System Administrator Specialist
The University of Georgia

e. jwebb@uga.edu

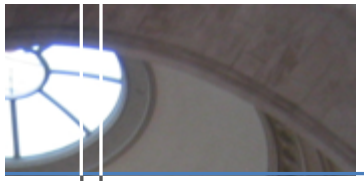
Origins in the freeIPA project (**I**dentity, **P**olicy and **A**udit)

There is a freeIPA client

Red Hat originates a new client project

Narrower in scope
Provided funding and two dedicated developers
Enterprise software bubbles up from the Fedora project and eventually finds its way to CentOS releases

Thank goodness! A name change opportunity is upon us!



Seriously ?!

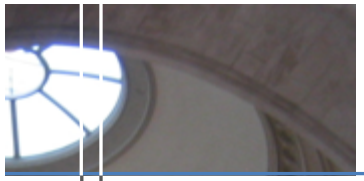
“System Security Services Daemon”

We would have very happily accepted:

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

Even:

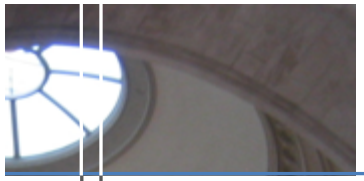
“Simplesmente Sancionar Serviços Daemon”



The 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.



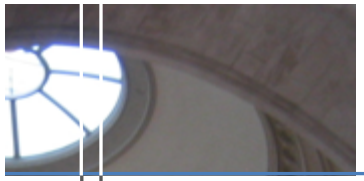
What need is the SSSD addressing?

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

Tighter Active Directory integration is more mission critical



pam_ldap pam_krb5 pam_winbind nss_ldap

Secure remote user lookup and authentication

Password management

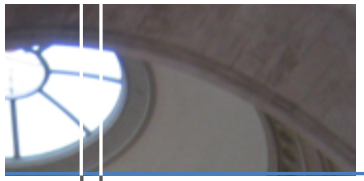
Session management (SSO capable)

MIT kerberos capable

MS Windows® RPC capable

MS Windows® and Active Directory for Domains capable

MS Windows® file share participation



The usual daemons

Name Service Caching daemon (nscd)

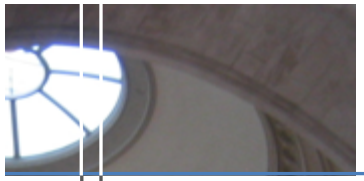
Next query caching for users, groups, hosts and services
No offline authentication but can maintain active sessions

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



Enough rabbit holes

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

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

More features, less configuration

/etc/sssd/sssd.conf
/etc/nsswitch.conf

Optionally:

/etc/autofs_auth_ldap.conf

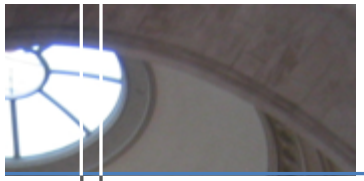
But mostly, reduced complexity and much better Active Directory integration!

Continued AD integration is the development focus:

[ad_master_domain_netlogon] **Found flat name [MYID].**
[ad_master_domain_netlogon] **Found site [UGA-Athens-GA-US].**
[ad_master_domain_netlogon] **Found forest [domain.uga.edu].**
[ad_srv_plugin_dcs_done] About to locate suitable site
[ad_get_client_site_done] Found site: UGA-Athens-GA-US
[ad_srv_plugin_send] About to find domain controllers
[ad_get_dc_servers] Looking up domain controllers in uga.edu
[ad_get_dc_servers] **Found 6 DCs in domain uga.edu**
[ad_srv_plugin_servers_done] Got 2 primary and 4 backup servers
[fo_add_server] **primary server** 'dc01.uga.edu:389' to service 'AD'
[fo_add_server] primary server 'dc02.uga.edu:389' to service 'AD'
[fo_add_server] **backup server** 'dc03.uga.edu:389' to service 'AD'
[fo_add_server] backup server 'dc04.uga.edu:389' to service 'AD'

Continued AD integration is the development focus:

[sssd[be]] : Option **ad_gpo**_access_control has value permissive
[sssd[be]] : Option **ad_gpo**_cache_timeout has value 5
[sssd[be]] : Option **ad_gpo**_map_interactive has no value
[sssd[be]] : Option **ad_gpo**_map_remote_interactive has no value
[sssd[be]] : Option **ad_gpo**_map_network has no value
[sssd[be]] : Option **ad_gpo**_map_batch has no value
[sssd[be]] : Option **ad_gpo**_map_service has no value
[sssd[be]] : Option **ad_gpo**_map_permit has no value
[sssd[be]] : Option **ad_gpo**_map_deny has no value
[sssd[be]] : Option **ad_gpo**_default_right has no value



SSSD disadvantages

MS Windows® or Samba file shares

Still requires winbindd be configured and used

NFS file shares

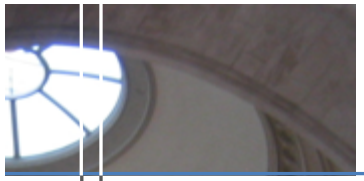
May still require nscd with user and group caching disabled

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

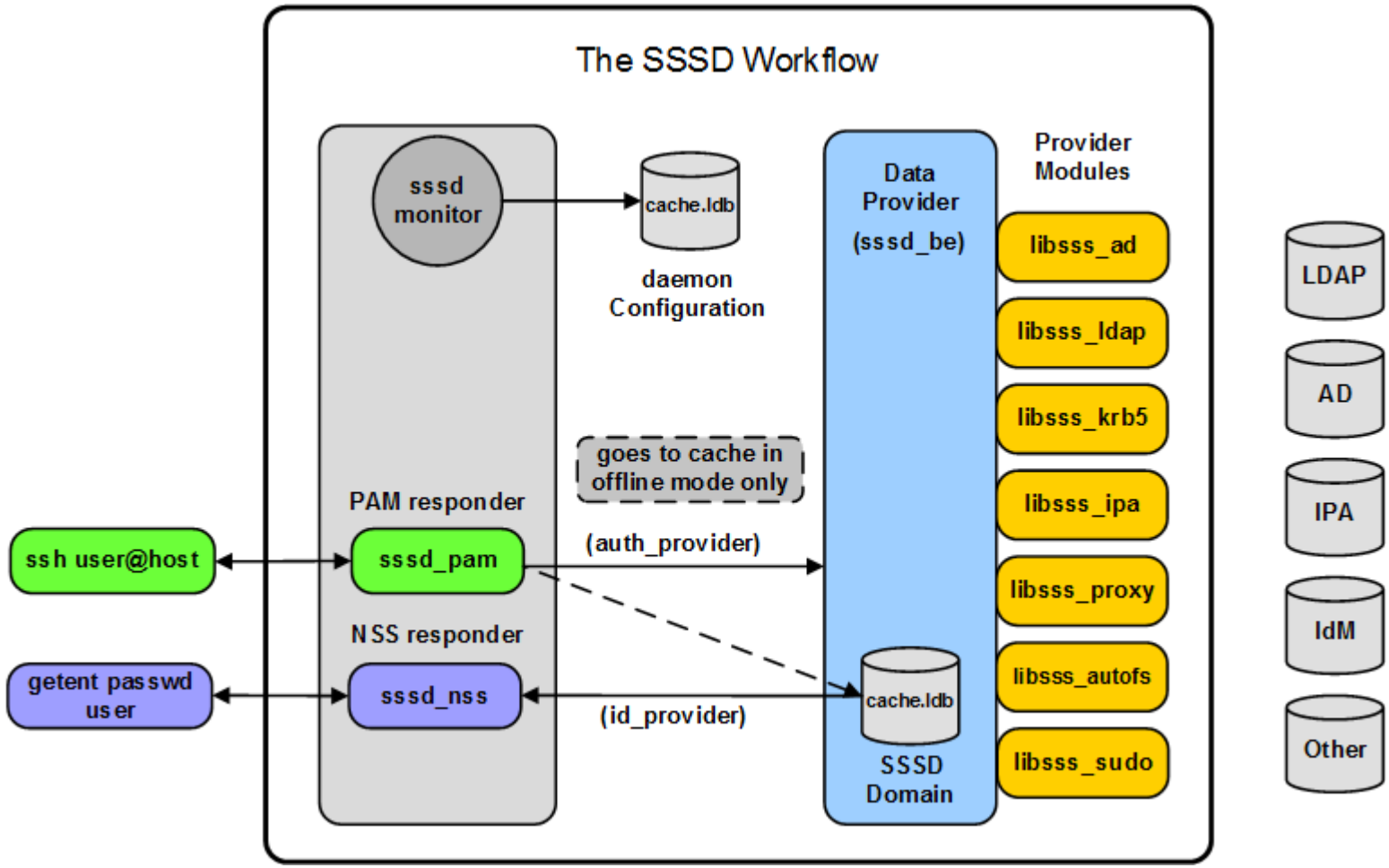


Seriously, if I type:

“SSSH” or “SSSL”

One more time I may scream !!

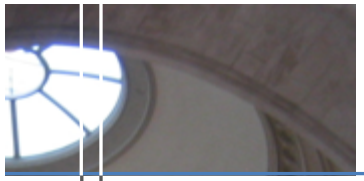
“SSSD” architecture overview



Learning to “speak” SSSD

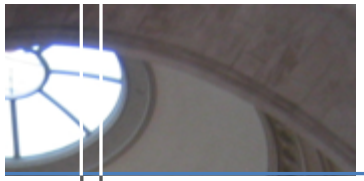
The Monitor
Providers (identity, authentication, service)
Responders
Authentication Domains

SSSD provider --> SSSD responder --> SSSD monitor
libsss_ldap.so --> ssss_nss --> sssd



SSSD Identity Providers

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



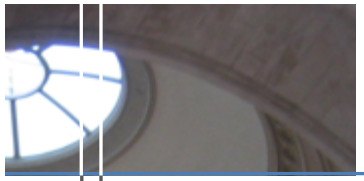
What are IPA and IdM backends?

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

Version 3 began focus is on Active Directory® integration

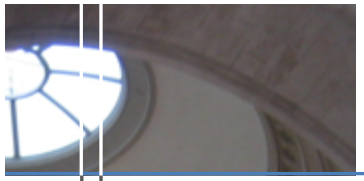
IdM is a way to create identity stores, centralized authentication, domain control for Kerberos and DNS services, and authorization policies on Linux systems, using native Linux tools.

Integration focus heavily favours Active Directory®.



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)



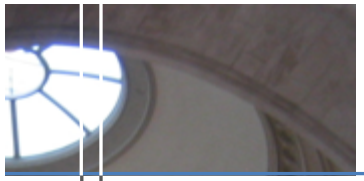
The SSSD configuration file

[sssd] — Global parameters
services =
domains =

[nss], [pam], [sudo] — Responder parameters
reconnection_retries =
filter_users =

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

SSSD Domain = Identity Provider + Authentication provider



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)
```

Has standardized on using the SSSD on all systems.

The majority of those Linux systems are joined to the domain, and are using the same daemon and configuration across several distributions and versions, reliably.

Have benefited from case indifference with back ends and file systems.

Have benefited from offline authentication services.

The necessary sssd.conf in our AD/POSIX world:

[domain/**gacrc.uga.edu**]
id_provider = ad
auth_provider = ad

enumerate = false
cache_credentials = true

ad_enable_gc = false
dns_discovery_domain = domain.uga.edu
dyndns_update = false

ldap_schema = ad
ldap_id_mapping = False
ldap_referrals = False

ldap_user_uid_number = extensionAttribute11
ldap_user_gid_number = extensionAttribute12
ldap_user_home_directory = extensionAttribute13
ldap_user_shell = extensionAttribute14
ldap_user_gecos = displayNamePrintable

ldap_group_name = msExchExtensionAttribute16
ldap_group_gid_number = extensionAttribute12

The likely sssd.conf in a standard AD/POSIX world:

[domain/**gacrc.uga.edu**]

id_provider = ad
auth_provider = ad

enumerate = false
cache_credentials = true

ad_enable_gc = false
dns_discovery_domain = domain.uga.edu
dyndns_update = false

Has implemented the SSSD against **Active Directory LDS** facing systems.

Select Red Hat systems were migrated from native PAM LDAP configurations to SSSD LDAP provider configuratiuons.

System migrations were completed in minutes.

The attribute mapping capabilities of the SSSD were key to the success of the migrations.

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

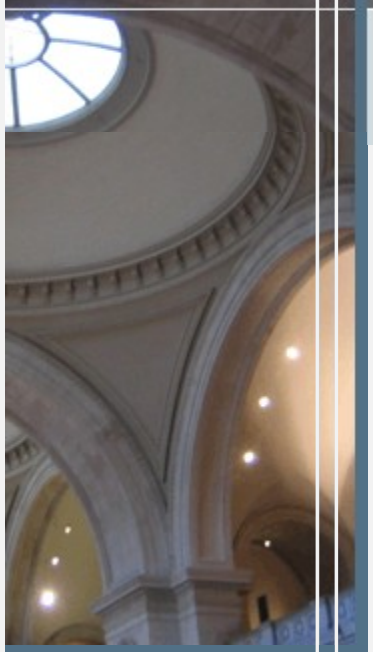
Configure transport security

TLS/SSL for eDirectory over LDAP
TLS/SSL for AD over LDAP
SASL/GSSAPI for AD over LDAP/Kerberos [2]

Configure SSSD identity providers and access control

Identity and access control providers can be mixed

[2] Initial connectivity to AD domains may require legacy tools



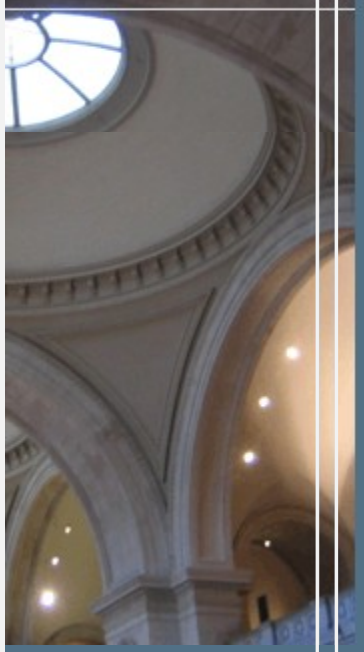
Questions

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

e. lkearney@uga.edu
w. www.lawrencekearney.com

John Webb
System Administrator Specialist
The University of Georgia

e. jwebb@uga.edu



Additional information:

Administering SSSD on SUSE Linux Enterprise Server 12 — Course SLE342

Available to USG sites at no cost if delivered by me!

Hardware, lab environment and printed student materials furnished by the site,