State of authentication and identity management in Red Hat Enterprise Linux 8 and Fedora 30/31

Red Hat Enterprise Linux 8

Alexander Bokovoy
Sr. Principal Software Engineer

Security / Identity Management Engineering
Red Hat Limited, Finland

40 years of POSIX API service

Identities in POSIX API

- getpw*() and getgr*() came in Version 7 AT&T UNIX, 1979
- Name Service Switch, ~1993

Authentication APIs

- Pluggable Authentication Modules API: 1995, OpenGroup X/Open Single Sign-on spec: 1997

Name Service Switch *‘/etc/nsswitch.conf’*

Pluggable Authentication Modules *‘/etc/pam.d/*’*

THE LAST ABIS MADE IN THE 90s
JÄTETÄÄN TÄÄ PASKA SEURAAVILLE SUKUPOLVILLE

Slow evolution

- SMB: 1984
- Kerberos v4: 1988, v5: 1993
- NIS+: 1992
- LDAP: 1993
- PKCS#11: ~1994
- Active Directory: 1998
  - Kerberos + LDAP + SMB

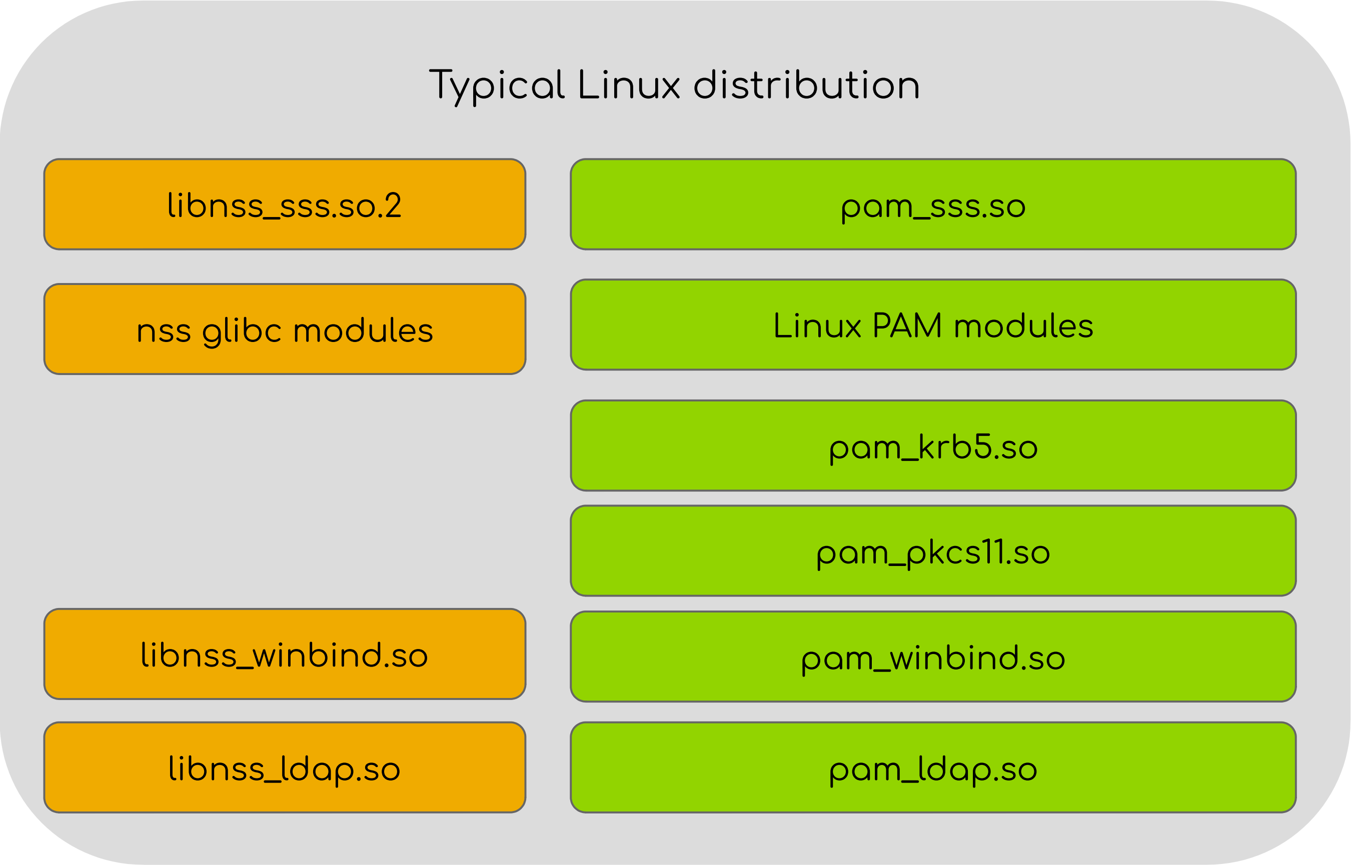
Standard API

Variety of implementations

- nss-pam-ldapd
- SSSD
- nss_ldap / pam_ldap
- pam_krb5 (x2)
- pam_pkcs11
- nss_winbind / pam_winbind
- Vendor-specific PAM modules (RSA, ...)

Production use experience

NSS and PAM



Typical Linux distribution

libnss_sss.so.2

pam_sss.so

nss glibc modules

Linux PAM modules

pam_krb5.so

pam_pkcs11.so

libnss_winbind.so

pam_winbind.so

libnss_ldap.so

pam_ldap.so

Configuration complexity

- Modular stack
- Authconfig macaroni

Deployment complexity

- Local access control settings
- Configuration responsibility diffuse

New requirements

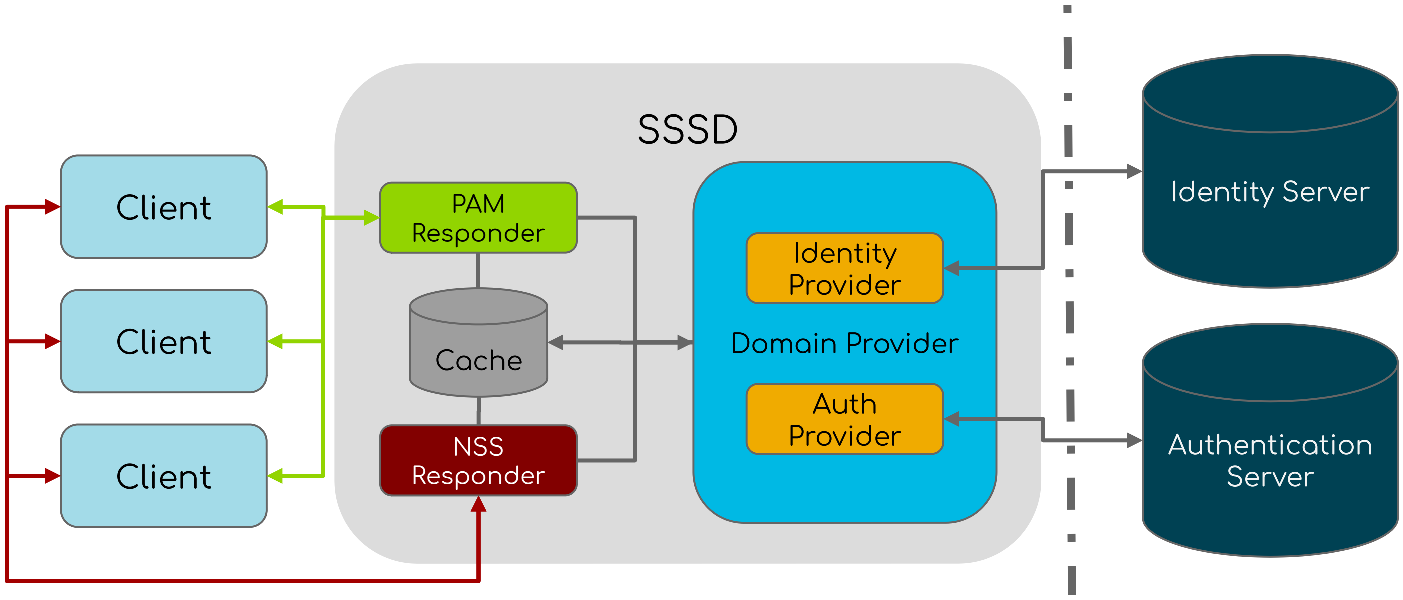
- Universal access to identity information in applications beyond POSIX-specific attributes

Standard API Variety of issues

Long-term issues

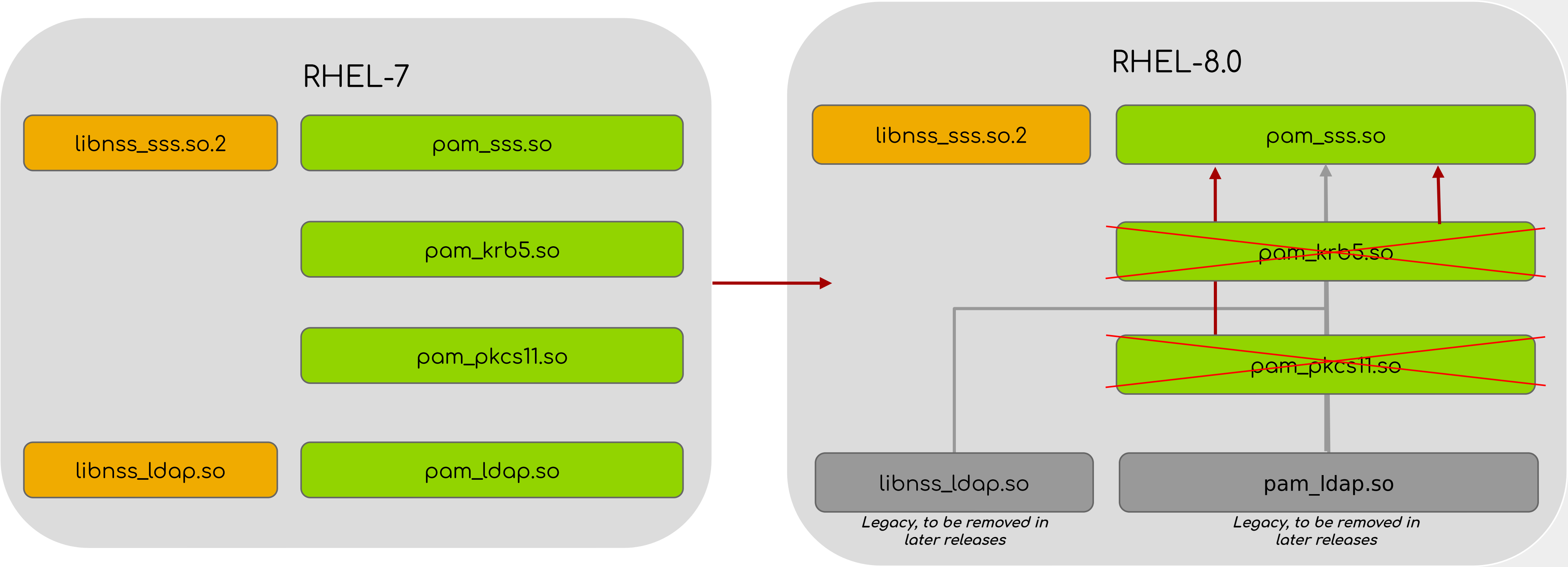
- Modular tumbleweed
  - (lack of) execution context isolation
  - (lack of) configuration scaling
  - (lack of support)
- Lack of “fanciness“ for new generations of developers
  - Life is easy with REST?

SSSD: a decade of Fedora service



- First Fedora release: Fedora Core 11
- Binds a client machine to centralized identity management systems (FreeIPA, Samba AD, LDAP, …)
- Identity details are cached for offline use
- SUDO and SELinux policies when using FreeIPA and AD environments
- Multi-factor authentication support
  - OTP tokens
  - Smart-cards

Modular evolution: Fedora isn’t the most extreme one!



RHEL-7

libnss_sss.so.2

pam_sss.so

pam_krb5.so

pam_pkcs11.so

libnss_ldap.so

pam_ldap.so

RHEL-8.0

libnss_sss.so.2

pam_sss.so

~~pam_krb5.so~~

~~pam_pkcs11.so~~

libnss_ldap.so

Legacy, to be removed in later releases

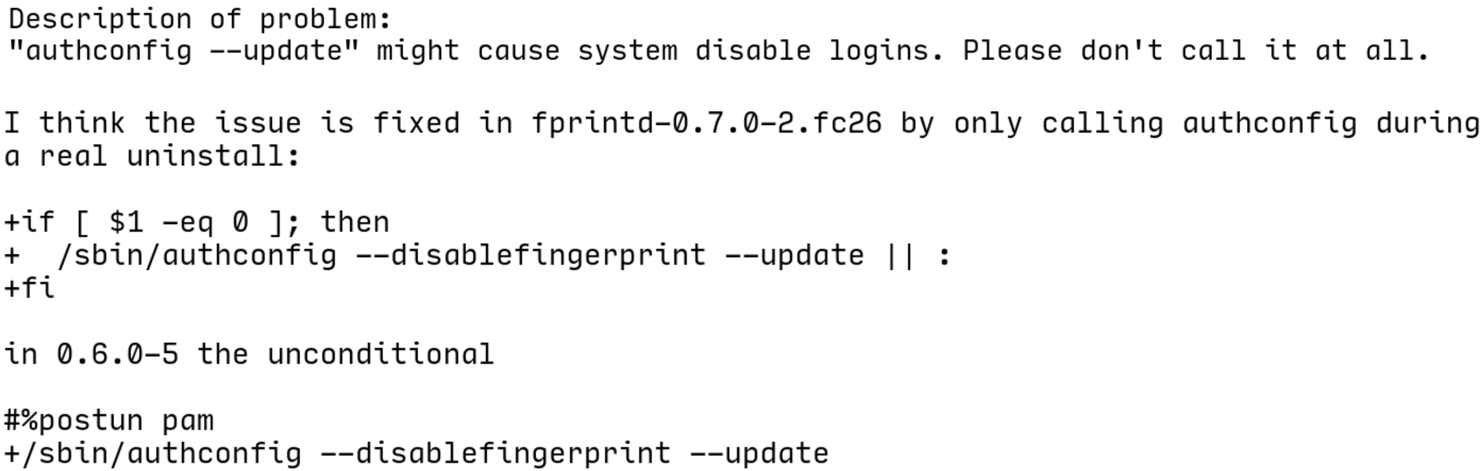
pam_ldap.so

Legacy, to be removed in later releases

Single host configuration management: authselect

- NSS / PAM configuration
  - Using pre-defined configuration profiles
  - Predictable and tested behavior
  - Customization is possible with /etc/authselect/custom

authconfig –update (rhbz#1423480) horror stories:



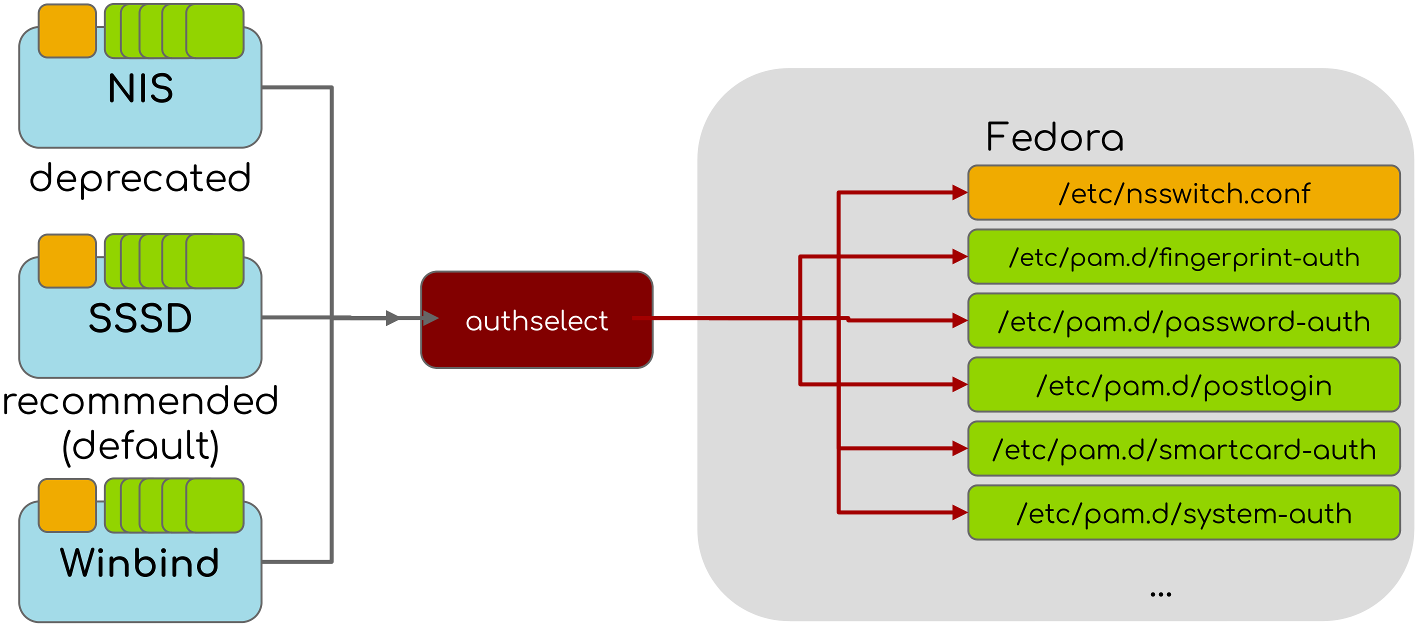
```
Description of problem:
"authconfig --update" might cause system disable logins. Please don't call it at all.

I think the issue is fixed in fprintd-0.7.0-2.fc26 by only calling authconfig during
a real uninstall:

+if [ $1 -eq 0 ]; then
+  /sbin/authconfig --disablefingerprint --update || :
+fi

in 0.6.0-5 the unconditional

#%postun pam
+/sbin/authconfig --disablefingerprint --update
```

- authconfig replacement
  - Python 2 – no Python 3 plans
  - 20 years of authconfig evolution (since 1999) created unmaintainable code base

  - Hard to guarantee working configuration in general

  - Contradicting user experience
    - --update does “update” configuration but forces you to specify all original options if you want them to persist

Single host configuration management: authselect



Authselect requirements

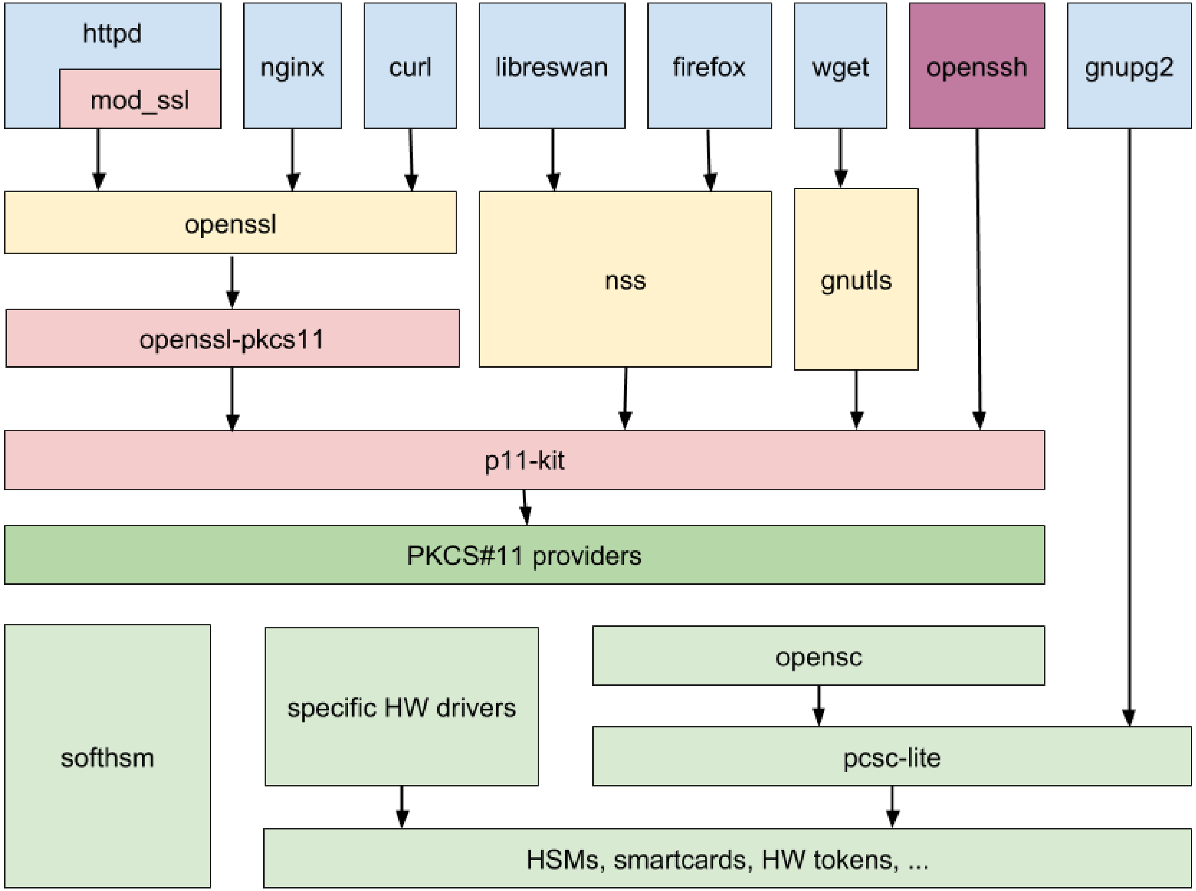
- Identity and authentication configuration
  - Pre-defined templates for /etc/nsswitch.conf and PAM configuration
- authselect does not configure PAM modules itself
  - ipa-client-install
  - realm join
  - Ansible roles
- authconfig became a wrapper over authselect
  - supports only most used options, without full flexibility

NIS: time has (almost) come

- NIS components marked for deprecation in RHEL 7.6
  - **ypserv, ypbind, yptools**
- glibc removed SUN RPC and NIS API upstream
  - SUN RPC / NIS API are part of libtirpc now

- NIS client is available for high performance computing nodes
  - Primarily for static user allocation deployments
- NIS server support will be removed in RHEL 9

Authentication: unified PKCS#11 stack



PKCS#11 URI standardization

- RFC 7512 (~2015)

p11-kit

- Automatically exposes smartcards, hardware and software tokens, and HSMs to applications
- No additional configuration is needed for single device use thanks to p11-kit-proxy

```
$ ssh -i pkcs11: example.com
$ ssh -i “pkcs11:id=%01” example.com
```

mod_ssl configuration:

```
SSLCertificateKeyFile pkcs11:id=
%01;type=private?pin-value=111111
```

Firefox

- Automatically loads p11-kit-proxy and makes tokens available without manual configuration

Authentication: Kerberos

Client side

- Kerberos Credential Manager (KCM)
- Hybrid DNS resolution support

Crypto changes

- DES/3DES removed
- Kerberos IV removed
- SPAKE support by default

Kerberos Credential Manager

- Protocol supported by MIT Kerberos 1.13+
- SSSD implements KCM server side
- Kerberos client can use FILE:, DIR:, KEYRING:, KCM: credential caches and cache collections

- SSSD KCM:
  - Persistent storage (across reboots)
  - Larger collection sizes
    - Helps sysadmins who need to administer 1000s hosts over SSH with GSSAPI
  - Can be used in containers (UID namespacing), as it is UNIX domain socket-accessible
    - Fedora Toolbox automatically imports KCM: credentials into its containers

Hybrid DNS resolution

- MIT Kerberos supports DNS URI discovery (RFC 7553)
  - Used by Fedora Project to expose FreeIPA KDC for contributors via fedora-packager package

- DNS canonicalization is a tristate now
  - True, false, fallback
  - Fallback to DNS canonicalization if KDC responds that a requested server principal is unknown
  - Fixes use of OpenShift-based applications (and some legacy mixed deployments)

- Future work:
  - Support for KDC proxies in KDC locator plugin interface to help SSSD and Samba to discover proxies
    - Fedora Project exposes KDC proxy for Fedora contributors

Crypto modernization

- RFC 6649 and RFC 8429
  - RFC 6649: deprecate DES and RC4-HMAC-EXP
  - RFC 8429: deprecate 3DES and RC4-HMAC

- Support for DES/3DES encryption is removed completely

- RC4-HMAC is marked deprecated
  - System-wide crypto policy makes it not visible in the set of default encryption types
  - Applications can still request and use it explicitly
    - Needed for SMB implementation in Samba and FreeIPA

Crypto modernization II

- SPAKE pre-authentication is enabled by default
  - Improved password protection
    - Public key cryptography protection against password dictionary attacks on Kerberos
  - Downgrade attacks are still possible if encrypted timestamp pre-authentication is still enabled
- Authentication Indicators support is available in FreeIPA
  - Can be used to force access to high security resources with the smartcards or 2FA
- Ongoing work
  - Still work in progress to enable flexible KDC policies
  - FIDO U2F in Kerberos
  - 2FA in SPAKE exchanges
  - Mapping authentication indicators and Active Directory asserted SIDs to enable FreeIPA and Samba AD high security support in SMB

Authentication and authorization in Apache

Authentication method	Authentication	Authorization	User identity lookup
Kerberos	mod_auth_gssapi ~~(mod_auth_kerb)~~	mod_authnz_pam	mod_lookup_idenity
Certificates	mod_ssl ~~(mod_nss, mod_revokator)~~		
Form processing	mod_intercept_form_submit		
SAML	mod_auth_mellon		
OpenID Connect	mod_auth_openidc		

Apache authentication modules removal in Red Hat Enterprise Linux 8

- **mod_auth_kerb removed**
  - Replaced by mod_auth_gssapi (RHEL 7+)
- **mod_nss removed**
  - RHEL IdM moved on to mod_ssl
  - mod_ssl cannot be used together with mod_ssl in a single deployment
  - World moved on to OpenSSL
- **mod_revocator**
  - Requires mod_nss → removed
  - Can be replaced with a systemd timer and mod_ssl

Identity servers in Fedora and Red Hat Enterprise Linux 8

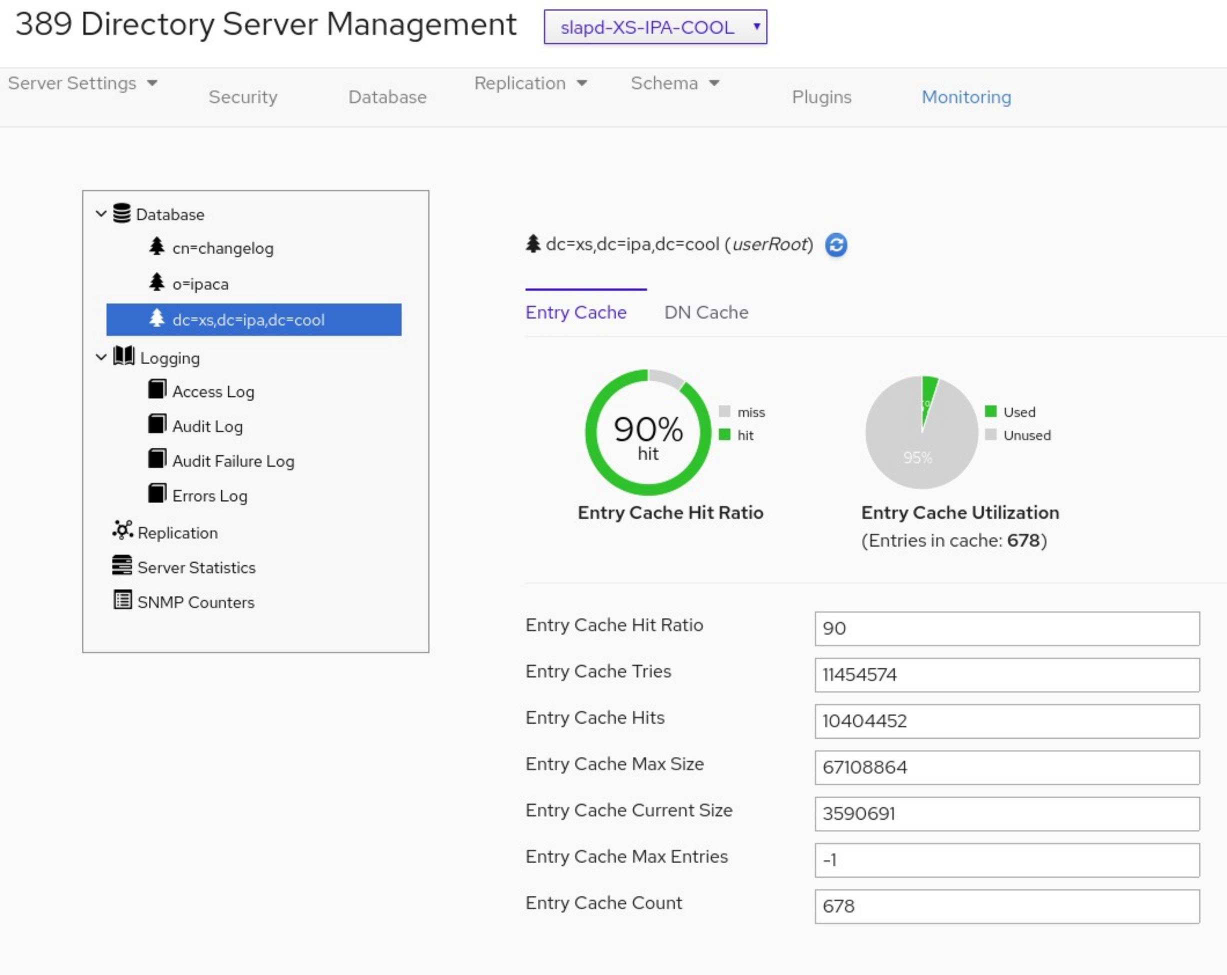
Fedora alternatives:

- 389-ds directory server
- FreeIPA on top of it
- Samba AD
- OpenLDAP

Red Hat Enterprise Linux 8:

- RHEL IdM
- RHDS
- Partner offerings

389-ds directory server



Entry Cache Hit Ratio

Entry Cache Utilization
(Entries in cache: **678**)

Entry Cache Hit Ratio	90
Entry Cache Tries	11454574
Entry Cache Hits	10404452
Entry Cache Max Size	67108864
Entry Cache Current Size	3590691
Entry Cache Max Entries	-1
Entry Cache Count	678

- New Cockpit UI plugin
  - Full management and monitoring
- A lot of improvements in auto-tuning in a joint work with SUSE
- Performance improvements for virtual attributes and parallel searches

FreeIPA

- FreeIPA 4.8.0
  - Removal of deprecated crypto
  - Integration with system-wide crypto policy
  - Samba file server on FreeIPA clients
  - Hidden / unadvertised replicas
  - Certificate management improvements
    - Default CA key size is now 3072
    - Dogtag configuration extensions to tune CA at deployment time
    - Support for IP addresses in certificates
- Health check utility to diagnose typical deployment issues
  - ipa-healthcheck
- Ansible integration
  - GSSAPI authentication support in Ansible
  - ansible-freeipa: client, master, replica deployments, resource management

Modular RHEL IdM

- RHEL 8 adds modular repositories
  - Parallel package versions availability (streams)
  - Single version installability
  - Package dependency isolation
  - Installation groups (profiles) per stream in addition to global distro package groups
- Stream **idm:client**
  - Enabled by default (kickstart use)
  - Contains only packages needed for IdM client deployment
- Stream **idm:DL1** (domain level 1)
  - Server components
  - Depends on 389-ds and pki-core (pki-deps) modules
  - Allows quick profile-based installation

Stream idm:DL1 profiles:

- idm:DL1/server
- idm:DL1/client
- idm:DL1/dns
- idm:DL1/adtrust

IdM module update policy:

- Deployment-incompatible changes will be done in a separate stream (DL2, ..)
- Existing streams are provided for the lifetime of the distribution

Samba

- Samba 4.11
  - SMB1 is disabled by default (Fedora 31)
  - LanMan and plaintext auth deprecated
  - Full Python 3 support, Python 2 support removed
  - Extensive JSON-based logging
  - GPO support improvements
  - Offline domain backups
  - LDAP server improvements
  - AD DC improvements

- Work in progress:
  - Crypto unification with GnuTLS
    - Performance improvements 2x-10x with SMB3
  - POSIX extensions for SMB3 protocol
    - Hopefully, will be in use by Fedora 32
  - MIT Kerberos integration for Samba AD
    - S4U* extensions and constrained S4U support

Thank you