SSSD Active Directory Improvements

New features in SSSD AD back end for 7.0

Jakub Hrozek

2014-03-31

SSSD 1.11 in a nutshell

- RHEL 7.0 ships with SSSD 1.11

- The majority of new features involved the AD provider

  - SSSD is now able to retrieve users and groups from trusted domains in the same forest

  - NetBIOS domain name can be used to qualify names

  - DNS updates and scavenging (separate presentation)

  - DNS site discovery (separate presentation)

  - Improved access control (separate presentation)

- The recommended way of setting up the AD provider is using *realmd*

RED HAT CONFIDENTIAL

The AD provider overview

- When enrolling an AD client, always use the AD provider, not the LDAP provider

- The AD provider gives you:

  - Simple configuration – the defaults correspond to Active Directory environments

  - Faster logins – all group memberships are retrieved in a single call.

  - Secure by default – uses GSSAPI to encrypt lookups

  - ID mapping by default – no need to define the POSIX IDs on the server side

  - ...and all the new features described in this presentation

redhat.

New features in more detail

NetBIOS domain names

- SSSD 1.11 allows using NetBIOS domain names for both input and output

- The NetBIOS domain name is autodiscovered

- Can be used anywhere just like a name qualified with full domain name

  - `getent passwd AD\\Administrator`

  - Including logins or the simple access provider

- The NetBIOS name can be set in output format as well

  - See description of `full_name_format` in man `sssd.conf(5)`

Users and groups from trusted domains

- SSSD 1.11 allows retrieving info about and authenticating as users from trusted domains in the same forest

- Trusted domains are autodiscovered on startup and at runtime

- Since user names in different domains often overlap, it is necessary to fully qualify user names
  - `getent passwd user@ad.example.com`
  - `getent passwd user@subdom.ad.example.com`

Enumerating users and groups from trusted domains

- AD provider supports user and group enumeration from trusted domains

- Even if master domain is set to enumerate, trusted domains must be allowed explicitly

- See `subdomain_enumerate` in man `sssd.conf`

- Enumeration is *strongly* discouraged for performance reasons!

Using POSIX attributes with trusted domains

- The AD provider defaults to ID mapping
  - Set `ldap_id_mapping=False` to use POSIX attributes
- The user and group information is first downloaded from Global Catalog with an optional fallback to LDAP
  - Only a subset of attributes is present in the Global Catalog
  - For better performance, it is recommended to replicate POSIX attributes to Global Catalog on the AD side

Joining the AD domain

Joining the AD domain with realmd

- *realmd* is a package that manages discovery and enrollment to several centralized directories including AD or IPA

- Easy to use and secure by default

- By default, realmd sets up SSSD's AD provider

- Advanced features available – one-time password for join, custom OUs, etc

- See the documentation for more details!
  - `http://freedesktop.org/software/realmd/`

redhat.

Realmd examples

- To discover all domains (requires NetworkManager)
  - `realm discover`
- To discover a particular domain
  - `realm discover ad.example.com`
- To join a domain
  - `realm join ad.example.com`

Comparing Winbind and SSSD's AD and LDAP

Feature	SSSD with AD provider (recommended)	SSSD with LDAP/KRB5 providers	Winbind
Requires POSIX attributes	No (default)	No (requires manual configuration)	No
Supports ID mapping	One method	Yes, requires manual configuration	Multiple methods
AD specific optimizations	Yes	No	Yes
Provides plugin for cifs-utils	No (available upstream)	No	Yes
DNS site support	Yes	No	Yes
DNS dynamic updates	Yes	No	Yes, requires manual configuration
Enrollment with realmd	Yes (default)	No	Yes (must be selected explicitly)

redhat.

Thank you