SSSD Active Directory

Improvements

New features in SSSD 1.11 AD backend

Jakub Hrozek

2014-03-31
SSSD 1.11 in a nutshell

- SSSD 1.11 was first shipped in Fedora 19
- 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`
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
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 ssssd.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_enumebrate 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/software/realmd/](http://freedesktop.org/software/software/realmd/)
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

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