Handling POSIX attributes for trusted Active Directory users and groups in FreeIPA

Alexander Bokovoy <ab@samba.org>
May 21th, 2015

Samba Team / Red Hat
FreeIPA

What is FreeIPA?

Cross Forest Trusts

Original FreeIPA assumptions

Identity Views

Demo
FreeIPA
FreeIPA

What is FreeIPA?

Cross Forest Trusts

Original FreeIPA assumptions

Identity Views

Demo
FreeIPA: [http://www.freeipa.org](http://www.freeipa.org)

**I: Identity**
- LDAP-based store for common objects (users, groups, hosts, services, ...)
- 389-ds as an LDAP server with FreeIPA server-side plugins
- MIT Kerberos KDC with FreeIPA driver
- Integrated certificate management with Dogtag Certificate Authority
- Python-based command line and Web management tools

**P: Policy**
- Delegation and separation of access
  - Flexible delegation of editing controls
- Host-based access controls to services:
  - Everything is denied by default, define rules to allow
  - `<user or group[, source host]> → <host, service>`
- Rules enforced at client side with SSSD project

**A: Audit Coming ...**
FreeIPA: http://www.freeipa.org
POSIX attributes for Active Directory users and groups in FreeIPA

FreeIPA

What is FreeIPA?

Cross Forest Trusts

Original FreeIPA assumptions

Identity Views

Demo
FreeIPA supports Active Directory native cross-forest trusts

- FreeIPA acts as ‘Active Directory forest root domain’ that can only establish trust but can’t join Windows machines
- technically: KDC + CLDAP + LSA RPCs
- FreeIPA provides KDC and LDAP, Samba provides LSA RPC
- no Global Catalog yet

- Works well for Active Directory users accessing FreeIPA resources
Full overview is available at http://freeipa.org/page/IPAv3_Architecture
Identities of Active Directory users and groups resolved with the help of SSSD

- SSSD on IPA master talks to AD DCs and Global Catalog
- Kerberos credentials of host/ipa.master@IPA.REALM are used to authenticate against AD DCs
- Two-way trust is needed to allow issuing cross-realm TGTs
- Other IPA clients’ SSSDs talk to IPA master to resolve AD users and groups
FreeIPA

What is FreeIPA?
Cross Forest Trusts
Original FreeIPA assumptions
Identity Views

Demo
Original FreeIPA assumptions

- Linux users are in FreeIPA, single LDAP entry defines POSIX attributes
- SUDO rules are in FreeIPA as LDAP objects
- HBAC rules are in FreeIPA as LDAP objects
- Public SSH keys for users and hosts are in FreeIPA as well
- Two-factor authentication tokens are in FreeIPA as LDAP objects
- ... or referenced to external RADIUS servers defined as LDAP objects in FreeIPA
Consequences

- Linux machines have uniform view of the information above
- No per-machine shell or home directory for a user
- No per-machine public SSH keys for users
- No Active Directory users or groups in LDAP
FreeIPA is a progress ...

... in ID management on Linux but there are anomalies too:

- Migration from other solutions often imposes requirements:
  - File servers might need to keep old user and group IDs for some time locally
  - Users might want to use different shells or home directories per machine
  - Public SSH keys access into a common account (think Gitlab or Github-like deployments) might differ per server
  - Old application might rely on specific values of GECOS field for users
FreeIPA is a progress ...

... in ID management on Linux but there are anomalies too:

✖ When Active Directory forest is trusted by FreeIPA:
  ✖ AD users and groups have templated POSIX attributes, no way to individualize them
  ✖ AD users cannot have associated public SSH keys

✖ When existing environment with AD synchronization is being migrated to AD Trusts
  ✖ AD users synchronized to IPA use UID/GID from IPA range
  ✖ AD users used via AD Trusts will use UID/GID generated from their SID or specific POSIX UID/GID
We don’t like to see another Progress spin, don’t we?
FreeIPA

What is FreeIPA?

Cross Forest Trusts

Original FreeIPA assumptions

Identity Views

Demo
FreeIPA 4.1 introduced a way to redefine POSIX attributes for a group of machines

**ID View**
- A container of ’corrected’ POSIX attributes for users or groups
- Can be applied to a host or a group of hosts, or to all hosts
- Each entry in the view is an override of the original attributes

**Defaults**
- For FreeIPA users and groups the default values are in their primary entry
- For Active Directory users and groups there is a ’Default Trust View’
  - Overrides from the default trust view apply to all FreeIPA clients
# ID View overrides

- Each override applies to a single user or group

<table>
<thead>
<tr>
<th>User</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Description</td>
</tr>
<tr>
<td>User login</td>
<td>Group name</td>
</tr>
<tr>
<td>User ID (uid)</td>
<td>Group ID (gid)</td>
</tr>
<tr>
<td>User GECOS field</td>
<td>User home directory</td>
</tr>
<tr>
<td>User group ID (gid)</td>
<td>User shell</td>
</tr>
<tr>
<td>User home directory</td>
<td>User public SSH key</td>
</tr>
</tbody>
</table>
How ID override looks like in LDAP?
ID Views are applied on the IPA master and IPA client sides by SSSD

Host-specific views applied on the IPA client directly

Default trusted view applied by the IPA master

It is not possible to use host-specific view on IPA master

Key logic is performed by SSSD 1.12.2 or later

Available in Fedora 21+, RHEL 6.7 beta, RHEL 7.1, CentOS 7.1

Legacy clients supported through the compat tree
Default Trust View overrides are always applied to Active Directory users and groups
IPA clients always use IPA masters to resolve AD users and groups
POSIX attributes from Default Trust View will be returned to all SSSD clients (Fedora, RHEL 6.x, RHEL 7.0, RHEL 7.1)
Public SSH keys from Default Trust View will be returned to new SSSD clients (Fedora 21+, RHEL 7.1, RHEL 6.7)
IPA client’s SSSD applies host-specific ID view
All attributes from the assigned ID View are applied
ID overrides are applied per attribute per user
Host-specific view is always applied last
If no ID override exist for the attribute of the user in all views, original value is used
Legacy clients are those without SSSD supporting AD trusts

- RHEL 5.x, RHEL 6.x, AIX, Solaris, FreeBSD, other Linux machines without SSSD 1.12+

Legacy clients use compat tree for all requests

- Base DN: cn=compat,$SUFFIX
- RFC2307 schema, no public SSH keys

Default Trust View is applied by IPA server automatically, no need to change anything on the legacy client

To use host-specific view on top of that, change base DN on the client to cn=viewname,cn=views,cn=compat,$SUFFIX
Caveats

- OTP tokens cannot be attached to Active Directory users in FreeIPA 4.1 yet
- RADIUS server authentication cannot be used for Active Directory users in FreeIPA 4.1 yet
- With SSSD before 1.12.2 ID overrides only be actual for groups at the user’s login time, not before
- Removing host-specific ID view from the host requires clean up of the SSSD cache and restart of SSSD on that host
Upstream design page
   http://www.freeipa.org/page/V4/Migrating_existing_environments_to_Trust

Red Hat Enterprise Linux Windows Integration Guide
Demo
Demo videos will be published on Youtube after Red Hat Summit in June 2015
Questions & Answers

Slides http://www.samba.org/~ab/sambaxp/2015/