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

Alexander Bokovoy <ab@samba.org>

May 21th, 2015

Samba Team / Red Hat

A crisis of identity (solved?)

FreeIPA

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

Demo

FreeIPA

POSIX attributes for Active Directory users and groups in FreeIPA

FreeIPA

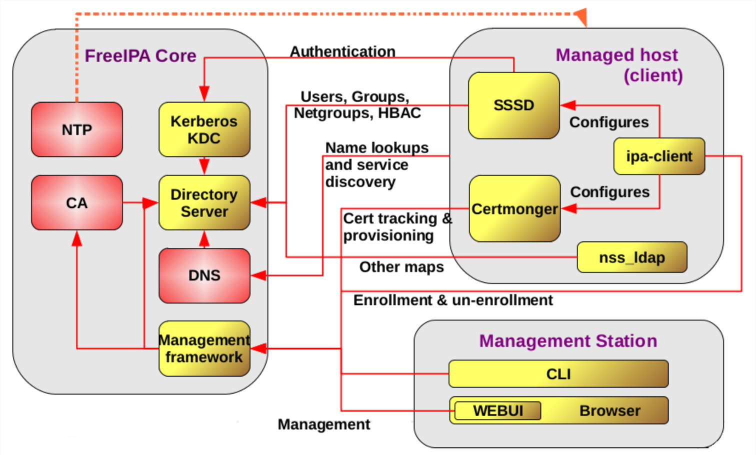
- What is FreeIPA?
- Cross Forest Trusts
- Original FreeIPA assumptions
- Identity Views

Demo

FreeIPA: 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`



FreeIPA

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

Demo

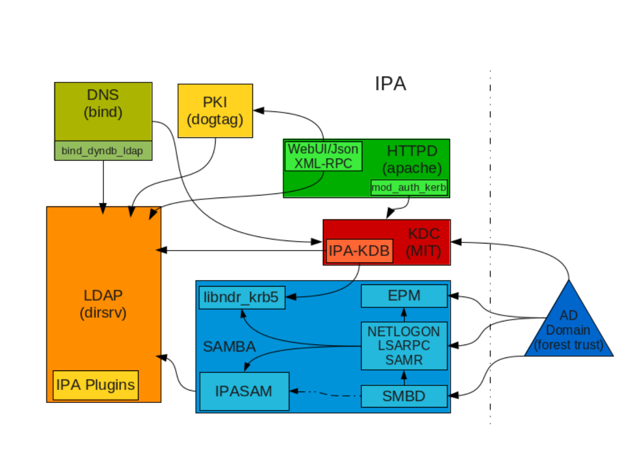
FreeIPA supports Active Directory native cross-forest trusts

- 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

FreeIPA v3 architecture

Full overview is available at

`http://freeipa.org/page/IPAv3_Architecture`



Identity management with cross-forest trust

- 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

POSIX attributes for Active Directory users and groups in FreeIPA

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?

POSIX attributes for Active Directory users and groups in FreeIPA

FreeIPA

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

Demo

Identity Views

- 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

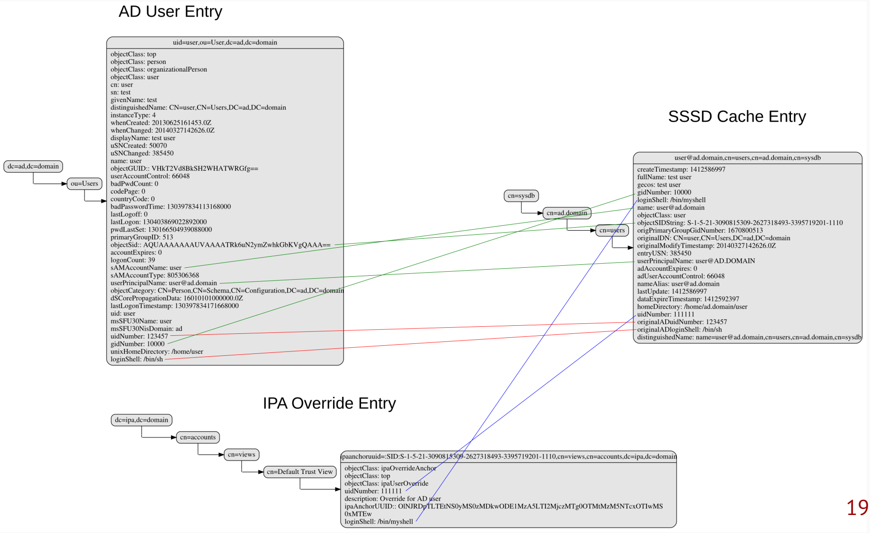
User

- Description
- User login
- User ID (uid)
- User GECOS field
- User group ID (gid)
- User home directory
- User shell
- User public SSH key

Group

- Description
- Group name
- Group ID (gid)

How ID override looks like in LDAP?



AD User Entry

dc=ad,dc=domain → ou=Users → uid=user,ou=User,dc=ad,dc=domain

```
uid=user,ou=User,dc=ad,dc=domain
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: user
sn: test
givenName: test
distinguishedName: CN=user,CN=Users,DC=ad,DC=domain
instanceType: 4
whenCreated: 20130625161453.0Z
whenChanged: 20140327142626.0Z
displayName: test user
uSNCreated: 50070
uSNChanged: 385450
name: user
objectGUID:: VHkT2Vd8BkSH2WHATWRGfg==
userAccountControl: 66048
badPwdCount: 0
codePage: 0
countryCode: 0
badPasswordTime: 130397834113168000
lastLogoff: 0
lastLogon: 130403869022892000
pwdLastSet: 130166504939088000
primaryGroupID: 513
objectSid:: AQUAAAAAAAUVAAAATRk6uN2ymZwhkGbKVgQAAA==
accountExpires: 0
logonCount: 39
sAMAccountName: user
sAMAccountType: 805306368
userPrincipalName: user@ad.domain
objectCategory: CN=Person,CN=Schema,CN=Configuration,DC=ad,DC=domain
dSCorePropagationData: 16010101000000.0Z
lastLogonTimestamp: 130397834171668000
uid: user
msSFU30Name: user
msSFU30NisDomain: ad
uidNumber: 123457
gidNumber: 10000
unixHomeDirectory: /home/user
loginShell: /bin/sh
```

SSSD Cache Entry

cn=sysdb → cn=ad.domain → cn=users → user@ad.domain,cn=users,cn=ad.domain,cn=sysdb

```
user@ad.domain,cn=users,cn=ad.domain,cn=sysdb
createTimestamp: 1412586997
fullName: test user
gecos: test user
gidNumber: 10000
loginShell: /bin/myshell
name: user@ad.domain
objectClass: user
objectSIDString: S-1-5-21-3090815309-2627318493-3395719201-1110
origPrimaryGroupGidNumber: 1670800513
originalDN: CN=user,CN=Users,DC=ad,DC=domain
originalModifyTimestamp: 20140327142626.0Z
entryUSN: 385450
userPrincipalName: user@AD.DOMAIN
adAccountExpires: 0
adUserAccountControl: 66048
nameAlias: user@ad.domain
lastUpdate: 1412586997
dataExpireTimestamp: 1412592397
homeDirectory: /home/ad.domain/user
uidNumber: 111111
originalADuidNumber: 123457
originalADloginShell: /bin/sh
distinguishedName: name=user@ad.domain,cn=users,cn=ad.domain,cn=sysdb
```

IPA Override Entry

dc=ipa,dc=domain → cn=accounts → cn=views → cn=Default Trust View → ipaanchoruuid=:SID:S-1-5-21-3090815309-2627318493-3395719201-1110,cn=views,cn=accounts,dc=ipa,dc=domain

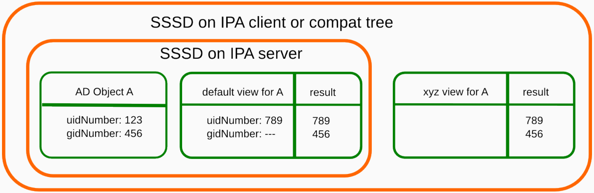
```
ipaanchoruuid=:SID:S-1-5-21-3090815309-2627318493-3395719201-1110,cn=views,cn=accounts,dc=ipa,dc=domain
objectClass: ipaOverrideAnchor
objectClass: top
objectClass: ipaUserOverride
uidNumber: 111111
description: Override for AD user
ipaAnchorUUID:: OlNJRDpTLTEtNS0yMS0zMDkwODE1MzA5LTI2MjczMTg0OTMtMzM5NTcxOTIwMS
0xMTEw
loginShell: /bin/myshell
```

Application of ID views

- 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

Application of ID views: IPA master

- 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)



SSSD on IPA client or compat tree

SSSD on IPA server

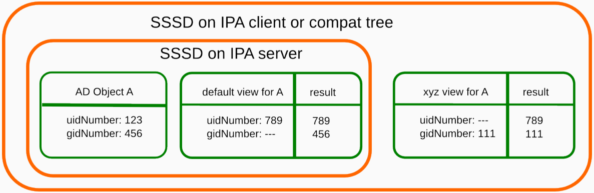
AD Object A
uidNumber: 123 gidNumber: 456

default view for A	result
uidNumber: 789 gidNumber: ---	789 456

xyz view for A	result
	789 456

Application of ID views: IPA client

- 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



SSSD on IPA client or compat tree

SSSD on IPA server

AD Object A
uidNumber: 123 gidNumber: 456

default view for A	result
uidNumber: 789 gidNumber: ---	789 456

xyz view for A	result
uidNumber: --- gidNumber: 111	789 111

Application of ID views: Legacy clients

- 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

Resources

- Upstream design page
  - `http://www.freeipa.org/page/V4/Migrating_existing_environments_to_Trust`
- Red Hat Enterprise Linux Windows Integration Guide
  - `https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/7/html/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/`