FreeIPA Cross Forest Trusts

Alexander Bokovoy <ab@samba.org>
Andreas Schneider <asn@samba.org>

Red Hat

May 10th, 2012

FreeIPA Cross Forest Trusts

1 FreeIPA
- What is FreeIPA?
- Cross Forest Trusts

2 Samba
- Work on Samba for FreeIPA

3 Demo

Talloc Tutorial

Pavel Brezina wrote Talloc tutorial!

http://talloc.samba.org/

FreeIPA Cross Forest Trusts

1 FreeIPA
- What is FreeIPA?
- Cross Forest Trusts

2 Samba
- Work on Samba for FreeIPA

3 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 v2.2

FreeIPA v2.2 is the current stable version:

- SE Linux user maps deployment, SSH known hosts management with SSSD 1.8.0
- Available in Fedora 17 beta 1
- Will be available in Red Hat Enterprise Linux 6.3

Allows to deploy full GNU/Linux-based solution with centrally manageable servers and clients:

- Multi-master replication
- Client systems support with SSSD and LDAP/Kerberos-compatible solutions like nss_ldap,pam_ldap
- Active Directory two-way synchronization for side-by-side deployments

Active Directory integration

Winsync plugin for Active Directory triggers synchronization of users and groups:

- Configured as a IPA replica of special type
- Two-way, change in AD brings in change to IPA and backward
- Only allows sync back users, not groups
- Incomplete management of password change enforcement

A better integration solution is required!

FreeIPA Cross Forest Trusts

1 FreeIPA
- What is FreeIPA?
- Cross Forest Trusts

2 Samba
- Work on Samba for FreeIPA

3 Demo

Kerberos cross-forest trusts

FreeIPA deployment is a fully managed Kerberos realm

- Can be integrated with Windows as RFC4120-compliant Kerberos realm
- Traditional Kerberos trust management applies:
  - on GNU/Linux side `~/.k5login` should be defined to impersonate users with identities
  - on Active Directory side manual mapping is performed with special tools in a similar way
- Does not scale well for thousands of users and hosts:
  - a foreign realm principal impersonates our realm's user
  - requires additional management of special users to impersonate doubling the management effort
  - mapping has to happen on every single machine. Manually?

Kerberos cross-forest trusts

Active Directory native cross forest trusts

- Require two Active Directory domains
- AD domain establishes trust with another AD domain via LSA RPC
- AD uses LSA RPC to map incoming principals to SIDs
  - technically: KDC + CLDAP + LSA RPC
  - FreeIPA provides KDC and LDAP, Samba 3 provides LSA RPC
- Stage 1: we are interested in allowing AD users to connect to FreeIPA services
  - e.g. PuTTY from Windows machine connecting to FreeIPA ssh service

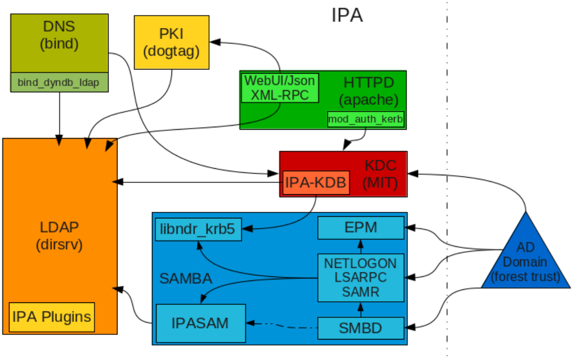
Kerberos cross-forest trusts

What was missing?

- Samba passdb backend to FreeIPA supporting trust storage and retrieval
- CLDAP plugin to FreeIPA to respond on AD discovery queries
- FreeIPA KDC backend to generate MS PAC
- Configuration tools to setup trusts

FreeIPA v3 architecture

Full overview is available at
`http://freeipa.org/page/IPAv3_Architecture`



Kerberos cross-forest trusts

FreeIPA passdb backend:

- Expansion of traditional LDAP passdb backend
- New schema objects and attributes to support trusted domain information
- Support for uid/gid ranges for multi-master replicas
- Kerberos principal creation for foreign domain account

FreeIPA KDC backend:

- Generates MS PAC information out of LDAP info and add to the ticket
- Allows to accept principals and tickets from a trusted cross forest realm
- Verifies and sign MS PAC coming from a trusted cross forest realm

Kerberos cross-forest trusts

FreeIPA configuration tools:

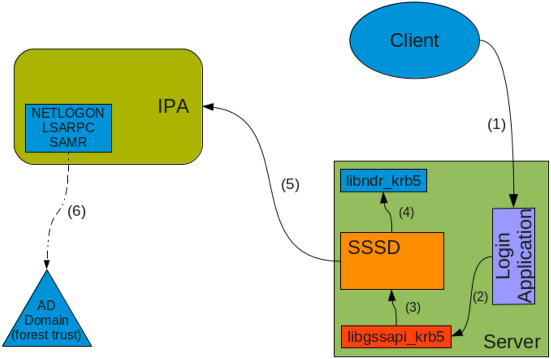
- FreeIPA has command line (CLI) and Web user interfaces
- `ipa trust-ad-add` creates new cross-forest trust
  - CLI operates with Kerberos authentication
  - Request is sent to FreeIPA server via XML-RPC over HTTPS with Kerberos auth
  - FreeIPA uses S4U2Proxy Kerberos feature to allow constrained delegation
  - Samba 4 Python bindings are used to establish trust
    - Code runs under non-privileged account (apache)
    - Uses Kerberos ticket obtained via XML-RPC with the help of mod_kerb_auth
    - Issues Kerberos-authenticated LSA RPC requests to a local smbd
    - Uses AD credentials or shared secret passed via XML-RPC request to talk to AD DC

Using FreeIPA services with AD credentials

Use of FreeIPA client system with AD cross forest credentials:

- Client system is provisioned with `ipa-client-install`
- SSSD is configured during provisioning to talk to FreeIPA LDAP
- krb5.conf is configured to perform mapping of cross forest trusted realm principal to user name 1:1 without removing the realm, e.g. Administrator@ad.local becomes user 'Administrator@ad.local'

Using FreeIPA services with AD credentials



Using FreeIPA services with AD credentials

On client SSH log-in following happens:

- SSH checks if user exists on the system
- SSSD NSS plugin handles the request and sees the user is not local. It requests additonal FreeIPA extended operation plugin for 389-ds that performs external domain user/group mapping using Winbind
- UID/GID are returned to SSH, GSSAPI is used to log-in that 'local' user now
- Now SSSD NSS plugin uses MS PAC from the Kerberos ticket to fill up groups information using FreeIPA LDAP

FreeIPA Cross Forest Trusts

1 FreeIPA
- What is FreeIPA?
- Cross Forest Trusts

2 Samba
- Work on Samba for FreeIPA

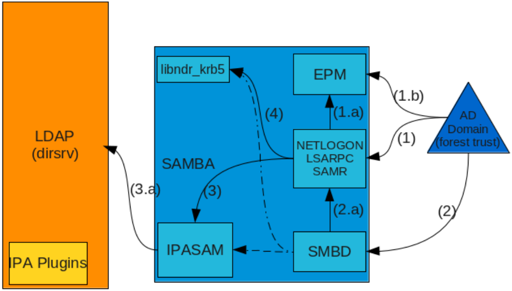
3 Demo

What did we do?

What a wurst!

- Spoolss Rewrite
- Spoolss Daemon
- Endpoint Mapper Daemon
- Pimped RPC Server
- Prefork Library
- LSA Service Daemon

This is the wurst!



Spoolss Rewrite

- Use winreg to store spoolss values instead of several tdb's
- Improve internal/(external) rpc connection handling

Spoolss Daemon

- Named pipe proxy over unix socket
- Doesn’t scale but works for testing

Named Pipe Proxy

- A special unix socket
- smbd just accepts the named pipe connection and forwards it to the unix socket
- Authentication is done by the service handling the named pipe proxy.

Endpoint Mapper Daemon

- It is a simple port mapper needed for tcp/ip communication
- First implementation only supported named pipes
- If you want to know more look at my SambaXP talk from 2011

Pimped RPC Server

- Added tcp/ip support
- Added ncalrpc support over unix sockets
- ncalrpc special root mode for privileged operations

Preforked Library

- Research: We want a preforked library with a mutex around accept(2)
- The mutex didn't work that well, so we do a race on accept(2) now
- Small daemon with pretty small memory footprint
- We prefork 5 children by default
- Values are tunable via config options for each daemon

Preforked Spoolss Daemon

- Research: We want a preforked library with a mutex around accept()

LSA Service Daemon

- Preforked daemon
- Handles TCP/IP, Named Pipe and NCALRPC connections
- Provides LSA/SAMR/Netlogon Services

FreeIPA Cross Forest Trusts

- EPMD and LSASD is all we need from Samba

DEMO

Questions & Answers

- Slides `http://www.samba.org/~asn/`