Samba 4.0 in Fedora

Alexander Bokovoy,
Simo Sorce

Samba Team / Red Hat

May 16th, 2013

Samba 4.0 in Fedora

Samba in Fedora

- File and print server
- Classic domain controller
- Identity client (winbindd and SSSD)
- FreeIPA integration
- OpenChange client
- Desktop integration (libsmbclient, net utility)
- Samba Python bindings

Samba structure

- Samba 4.0 is the first Samba release that combines
  - traditional SMB file server: `smbd`
  - domain controller and member for classic 'NT networks': `smbd`, `nmbd`
  - identity mapping and domain topology discovery: `winbindd`
  - Active Directory-compatible domain controller: `samba`
- and there are two client side components
  - `libsmbclient`, stable C API to talk SMB protocol
  - C libraries and Python bindings to a large set of DCE RPC calls and AD DC functionality

Samba structure in Fedora

- Samba 4.0 is the first Samba release that combines
  - traditional SMB file server: `smbd`
  - domain controller and member for classic 'NT networks': `smbd`, `nmbd`
  - identity mapping and domain topology discovery: `winbindd`
  - Active Directory-compatible domain controller: `samba`
- and there are two client side components
  - `libsmbclient`, stable C API to talk SMB protocol
  - C libraries and Python bindings to a large set of DCE RPC calls and AD DC functionality

Samba in Fedora

- There is a lot of confusion over naming and functionality
  - Both file serving and AD DC modes require `smbd` and `winbindd` (a different winbindd for each mode)
  - It is easy to create a bad configuration and shoot oneself into the foot, like `https://bugzilla.redhat.com/show_bug.cgi?id=956582`
- The AD domain controller code is not compiled in
  - Uses embedded Heimdal Kerberos KDC
  - Utilizes some Heimdal-specific code as well
  - (it would cause Samba client libraries to be compiled against Heimdal)

Kerberos in Fedora

- Kerberos: Fedora builds against MIT Kerberos
- Active expansion of features through MIT Kerberos Consortium work
  - DIR:: credential caches
  - clock anti-skewing
  - OTP support in Fedora 19
  - interposer plugins (GSS-Proxy)
  - Credential Store Extensions
  - Keytab Initiation
  - etc...
- Kerberos implementations are compatible through the protocol, not at the API or file data level
- Kerberos libraries are a fundamental system component, cannot be easily swapped out

Using Samba bits for identity management

- Active Directory is one of the most popular IdM systems
  - Windows AD or Samba AD should be used for Windows Clients
- Red Hat sponsors the development of FreeIPA
  - FreeIPA's main purpose is to handle Linux machines
  - FreeIPA looks like an Active Directory forest to an AD domain controller
  - We integrated the Samba classic domain controller code and MIT Kerberos KDC
  - Samba is used to support cross-forest trusts functionality

FreeIPA integration

- FreeIPA implements management of POSIX clients:
  - automated configuration of LDAP, Kerberos, DNS, and Certificate Authority
  - SSSD complements client-side for both POSIX and users/groups from a trusted domain
- `winbindd` runs only on FreeIPA servers, no need to run it on clients
- `ipasam` PASSDB module retrieves trusted domains and user/groups from FreeIPA LDAP server

Why Samba classic domain controller?

- Samba classic domain controller
  - `smbd` abstracts UID, GID, name, and SID management via IDMAP API
  - For the local domain IDMAP is re-routed to the PASSDB API
  - PASSDB modules are responsible for presenting users, groups, domains, and their properties
  - the default passdb module is tdbsam, but a very commonly ldapsam is used instead
  - Both IDMAP and PASSDB API allow to plug different backends and ID allocation algorithms
- Samba AD domain controller
  - Stores all information in LDB database with LDAP schema compatible to Active Directory schema
  - There is no pluggable API for IDMAP and PASSDB-like functionality (yet)

Lessons learned from FreeIPA AD trusts work

- no need to run KDC embedded into the `samba` process address space
  - close cooperation between the LDAP server and the KDC database driver is still required
  - The CLDAP responder is implemented as a LDAP server plugin
  - The KDC database driver knows about trusted domains topology and SIDs of objects
  - *A KDC database driver to use Samba database interfaces was prototyped a few years ago*
- Common algorithms and libraries to perform ID mapping and trust topology handling are required
- LSA external pipe support allows for inter-daemon communication
- Code running on the client side should be more granular than current `winbindd`

What is planned?

- Update MIT KDC database driver, using `source4/kdc/mit_samba.c` as a glue
- Make sure Heimdal-specific calls in Samba abstracted to allow interchange (it is not just Kerberos...)
- Add cross-forest trust support to Samba AD DC
- Ensure common ID mapping solutions for all types of domain controllers

Python bindings to Samba

The following bindings are available in Fedora:

- All DCE RPC calls have auto-generated Python bindings
- Key Samba supporting libraries (ldb, talloc, tdb, tevent)

A few notes:

- These bindings are actively used by external projects
- The whole Samba code base depends on WAF build system, written in Python
- The Fedora Project has started to plan the move to Python 3. Samba needs to get ready

Example from FreeIPA

FreeIPA uses Samba Python bindings to implement trust management with Active Directory

```
from samba import param, credentials
from samba.dcerpc import security, lsa
 ...
pipe = lsa.lsarpc(binding, parm, creds)
 ...
objectAttribute = lsa.ObjectAttribute()
objectAttribute.sec_qos = lsa.QosInfo()
policy_handle = pipe.OpenPolicy2(u"", objectAttribute,
                                 security.SEC_FLAG_MAXIMUM_ALLOWED)
result = pipe.QueryInfoPolicy2(policy_handle, lsa.LSA_POLICY_INFO_DNS)
 ...
info = lsa.TrustDomainInfoInfoEx()
info.domain_name.string = domain['dns_domain']
info.netbios_name.string = domain['name']
info.sid = security.dom_sid(domain['sid'])
info.trust_direction = \
     lsa.LSA_TRUST_DIRECTION_INBOUND | lsa.LSA_TRUST_DIRECTION_OUTBOUND
info.trust_type = lsa.LSA_TRUST_TYPE_UPLEVEL
info.trust_attributes = lsa.LSA_TRUST_ATTRIBUTE_FOREST_TRANSITIVE

trustdom_handle = pipe.CreateTrustedDomainEx2(policy_handle, info,
                                              auth_info, security.SEC_STD_DELETE)
```

Samba security in Fedora

- Samba runs fine with SELinux enabled
  - Look at `samba_selinux(8)`, `samba_net_selinux(8)`, `samba_unconfined_script_selinux(8)` manual pages for details of configuring your own paths
- FreeIPA `ipasam` module uses a non-privileged Kerberos principal to authenticate against the LDAP server, no admin-level rights exposure
- *ldapsam needs to be expanded to support Kerberos auth method instead of using admin DN, borrowing code from ipasam*
- GSSProxy integration is coming past Fedora 19, will allow to reduce Kerberos keys exposure in Samba keytabs
- Samba code is compiled with PIC (but PIE is not supported by WAF yet!!)

Performance considerations

- Change of the build system in Samba 4.0 brought more granular library split
- We provide more than 150 shared objects (libraries and modules) in non-AD DC mode
- It is far from monolythic Samba 3.x releases
- Memory consumption is higher per process:
  - `smbd` 3.6.9 (RHEL6) takes 1860 kB resident and 1088 kB dirty RAM on x86_64
  - `smbd` 4.0.5 (Fedora 19) takes 4460 kB resident and 1560 kB dirty RAM on x86_64
- With position independent executable (PIE) support, `smbd` performance characteristics need to be re-evaluated
- PIE brings 3-4% slowdown on application start up on x86_64, reports of testing on a higher-end hardware are welcome!

Packaging issues

- We used to have parallel packages (samba4 and samba) for 4.0 and 3.x releases. Fedora 18 has a single samba package set.
- Common libraries (tdb, ldb, tevent, talloc, ...) are provided independently of Samba packages
- Sometimes tdb, ldb, tevent, etc releases don't get properly tagged upstream when Samba is released
- Untagged changes in those libraries in Samba tree are referenced by Samba configure scripts as new versions
- As result, new Samba release packaging is prevented until tdb, ldb, tevent, etc will be released

Questions & Answers

- Alexander Bokovoy, mailto:ab@samba.org
- Simo Sorce, mailto:simo@samba.org
- Slides http://www.samba.org/~ab/sambaxp/2013/