FreeIPA and cross-distribution packaging experience

Alexander Bokovoy
about:me

Red Hat
  - Sr. Principal software engineer at Red Hat
  - Identity management and security engineering

Upstream hat
  - FreeIPA core developer
  - Samba Team member
  - Fedora Project contributor
FreeIPA core

- **FreeIPA framework**
  - Web application (Python) runs under `mod_wsgi` in Apache
  - Tight integration with `mod_gssapi` and GSS-Proxy
  - Python-based installers
  - Custodia secrets proxy in Python

### Language Breakdown

<table>
<thead>
<tr>
<th>Language</th>
<th>Code Lines</th>
<th>Comment Lines</th>
<th>Comment Ratio</th>
<th>Blank Lines</th>
<th>Total Lines</th>
<th>Total Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Python</td>
<td>275,161</td>
<td>46,287</td>
<td>14.4%</td>
<td>44,050</td>
<td>365,498</td>
<td>73.1%</td>
</tr>
<tr>
<td>C</td>
<td>43,533</td>
<td>8,184</td>
<td>15.8%</td>
<td>8,134</td>
<td>59,851</td>
<td>12.0%</td>
</tr>
<tr>
<td>JavaScript</td>
<td>43,267</td>
<td>13,177</td>
<td>23.3%</td>
<td>10,415</td>
<td>66,859</td>
<td>13.4%</td>
</tr>
</tbody>
</table>

Figure 1: Code base statistics
FreeIPA at a distance

▶ Kerberos KDC
  ▶ MIT Kerberos with own database driver and additional plugins for PKINIT, certificate mapping, KDC discovery
  ▶ RADIUS proxy to handle multi-factor authentication (2FA, ipa-otpd)
▶ Kerberos proxy application (MS-KKDCP) in Python
FreeIPA at a distance

- LDAP server
  - 389-ds directory server
  - 15 additional plugins for 389-ds
- SSSD on servers and clients
- Dogtag Certificate Authority
  - Server in Java + deployment tools in Python
  - Depends on NSS crypto library (and Java bindings)
  - ... and a lot of Java ecosystem packages (Tomcat, etc.)
FreeIPA at a distance

- DNS server
  - BIND 9
  - LDAP database driver `bind-dyndb-ldap`
  - DNSSEC keys synchronization daemon (Python)
- Samba
  - PASSDB plugin (`ipasam`)
  - Extensive use of Samba Python bindings for integrating with Active Directory
(Some) real world examples

- GNOME.org, since 2014
- Fedora Project infrastructure, since 2016
- Red Hat IT, since 2016
Distribution support

- Fedora, Red Hat Enterprise Linux, CentOS, ALT Linux
  - Full server support, including replication
  - Full client support
Distribution support

- Debian GNU/Linux and derivatives
  - Client support mostly complete
  - Troubled server support
Distribution support

- ArchLinux
  - No server support
  - Troubled client support
- openSUSE / SUSE Enterprise Linux
  - No server support (anymore)
  - Troubled client support
What does ‘mostly complete’ mean?

- FreeIPA development drives changes in other projects
- SSSD adds support for new FreeIPA features
- Old SSSD version represent a barrier for adoption
- Active Directory integration since SSSD 1.10
- Smartcard support since SSSD 1.15
- FleetCommander integration for GNOME since SSSD 1.16
What does ‘mostly complete’ mean?

- Kerberos story is more complex
  - MIT Kerberos gets extended to cover new usages
    - Prompts to support multi-factor authentication
    - SPAKE exchange, 2FA support using RADIUS
    - Certificate mapping extensions for flexible PKINIT
    - Automated translation methods between POSIX identities and Kerberos principals
What does ‘mostly complete’ mean?

- FreeIPA requires coordination between multiple packages
  - Typical: SSSD, MIT Kerberos, 389-ds, Dogtag, Samba, and FreeIPA versions need to be aligned
  - Samba update needs updates to ldb, tevent, talloc
- Backports aren’t always possible
  - ABI stability promises
  - Dependency chain reaction
What does ‘troubled support’ mean?

- FreeIPA relies on MIT Kerberos
- C code level dependency on MIT Kerberos API
- Heimdal Kerberos and MIT Kerberos have incompatible ABI (and sometimes API)
  - Features are not fully matching as well
What does ‘troubled support’ mean?

- Debian and derivatives have Samba compiled against Heimdal Kebreros
- Enabled to allow Samba AD DC build
- Active Directory integration is not available in FreeIPA
  - `ipasam` PASSDB driver for Samba requires MIT Kerberos
  - `smbd` and `winbindd` load PASSDB modules -> cannot load `ipasam`
- Credential cache formats aren't fully compatible either
  - Protocol level compatibility only
What does ‘troubled support’ mean?

- Dogtag depends on a particular version of Java
  - JDK 11 is not supported yet, Debian moved to JDK 11 recently
- Dogtag depends on NSS
  - Hard dependency, a lot of code assumes operations on NSS
    - System-wide integration is hard if distribution is OpenSSL-based
    - `nss-pem` PKCS#11 module was a hope but it relies on static private libraries from NSS
    - NSS upstream (Mozilla) refused to make the code a public shared library: Mozilla#1429692
    - `nss-pem` was forked out, Debian only recently packaged it
What does ‘troubled support’ mean?

- FreeIPA operates multiple system services and touches many configuration files
- Many utilities differ across distributions
  - PAM/nsswitch.conf set up is different in Fedora/RHEL/Debian…
  - authconfig / authselect / …
- There is an abstraction layer in FreeIPA for system management
  - Support for RHEL, Debian, Fedora upstream
  - ArchLinux holds downstream patch which was never submitted upstream
Automating integration into a released distribution
FreeIPA upstream CI

- Upstream pull requests get through a CI runs
  - tests cover most common code paths:
    - Deployment of a server and a replica
    - Deployment of a client
    - Administration via command line and Web UI
    - Integration on a client side (HBAC rules, SUDO rules, etc)
    - A simple containerized deployment
  - In total, 55 test suites for each PR CI run
    - roughly 2 hours of wall clock
FreeIPA and cross-distribution packaging experience

FreeIPA upstream CI: nightly runs

- Nightly runs test upstream code against known distribution releases
  - Fedora 28, 29, Rawhide
  - Images rebased once a month
- In total, 96 test suites, more than 700 individual tests
  - Around 8 hours wall clock, more than 60 hours of testing
Figure 2: Typical nightly run on Fedora 29
FreeIPA downstream testing: Fedora

- Integration at update submission time
  - Bodhi update runs OpenQA tests
    - Any critical path update + a white list of packages cause testing FreeIPA
- Fedora OpenQA tests:
  - Install a master and a replica
  - Enroll a client via both `realmd` and `cockpit` Web UI
  - Test access of services (ssh, sudo, etc)
  - Test FreeIPA management operations
  - Test full desktop experience
    - logon with GDM
    - Single sign-on to FreeIPA web UI
  - Test upgrade of both a server and a client
    - Upgrade a server from previous Fedora release
    - Upgrade a client from previous Fedora release
Two test runs:
- Deploying domain controller: test run #348824
- Deploying a client and using it: test run #348826
Can we catch non-trivial bugs?

- Yes, we can!
- More than 30 bugs found in various components
  - RHBZ#1644919, RHBZ#1636633, RHBZ#1629935,
  - RHBZ#1622760, RHBZ#1620315, RHBZ#1615586
  - RHBZ#1615452, RHBZ#1610536, RHBZ#1609477
  - RHBZ#1607635, RHBZ#1606541, RHBZ#1588192
  - RHBZ#1574711, RHBZ#1559680, RHBZ#1559677
  - RHBZ#1558818, RHBZ#1558817, RHBZ#1557609
  - RHBZ#1551677, RHBZ#1508662, RHBZ#1503321
  - RHBZ#1496562, RHBZ#1489184, RHBZ#1488640
  - RHBZ#1483170, RHBZ#1483159, RHBZ#1469799
  - RHBZ#1465390, RHBZ#1455561, RHBZ#1430247
  - RHBZ#1403352, RHBZ#1353054, RHBZ#1348946
Case in point: RHBZ#1636633 and RHBZ#1633089

- A bug in MIT Kerberos causes crash in multiple applications
- The real cause was a bug in 389-ds where multiple threads stepped over the same Kerberos ccache
- While fixing the bug in both krb5 and 389-ds, a security fix was published for MIT Kerberos
  - The fixed MIT Kerberos package backed off a fix for RHBZ#1636633 by mistake
  - OpenQA noticed this and it took several iterations to restore the fix
- 389-ds, meanwhile, broke another part of FreeIPA when releasing own fix for RHBZ#1633089
  - Fixed now in Fedora 29 on February 1st, 2019
  - Still visible in FreeIPA Upstream Nightly CI tests (needs an image rebase)
Directory server update was tested as part of the submission to Fedora 29 updates:

Figure 4: 389-ds Bodhi update test run
What is next?
Fedora CI

- Fedora and CentOS CI integration
  - We test at Bodhi, we need to test a Fedora package pull request step
  - Fedora CI standard test environment is not multi-host compatible
  - Fedora messaging bus to help
    - Listen to the Pagure messages
    - Kick off a test run in FreeIPA CI
    - Report results back to Fedora messaging bus
    - Store results in the ResultsDB
Upstream

- Looking forward for contributions for other OS
- Test runs for upstream pull requests CI
- Nightly runs for your distro
FreeIPA and cross-distribution packaging experience