FreeIPA
Open Source Identity Management

Florence Blanc-Renaud & Fraser Tweedale
2018-07-04
Workshop goals

● Understand high-level architecture of FreeIPA
● Get experience, become comfortable with...
  ○ deploying FreeIPA
  ○ enrolling clients
  ○ managing users, services, access policies
  ○ using IPA for web authnz
Workshop outline

- Brief overview of FreeIPA architecture
- Set up Vagrant environment
- Workshop curriculum
  - Install server
  - Enrol client machine
  - User management
  - Host-based Access Control (HBAC)
  - Web app authnz using FreeIPA
  - ... and more!
Identity Management & FreeIPA
What is Identity Management?

- Define users, hosts, services, access policies
- Authentication and authorisation mechanisms
- Increase security and productivity
- Reduce cost and risk
Included technologies

- **LDAP** (directory services)
- **Kerberos** (authentication)
- **X.509** (digital certificates)
- **DNS** (service discovery, host identity)
- Open Source identity management solution
- Integrate with Windows environments via **trusts**
- Fedora, RHEL, CentOS, Ubuntu
Components

- MIT Kerberos
- 389 DS
- BIND DNS
- Dogtag PKI
- SSSD (client)
FreeIPA Server

**Components:**
- CA (Dogtag)
- KRA (Certmonger)
- DNS (BIND)
- NTP (time sync)
- KDC (MIT Kerberos)
- LDAP 389 DS
- Server API (Apache)

**FreeIPA Client**
- SSSD
- Certmonger

**Mandatory Components:**
- Host
- User
- Group
- Service
- RBAC
- DNS
- Topo
- Cert
- HBAC

**Optional Components:**
- NTP
- LDAP
- KDC
- Server API

**Legend:**
- Mandatory
- Optional
1. Authentication

2. Ticket Granting Ticket (TGT)

3. TGT

4. Service Ticket

5. Request + Service Ticket

6. Response + Authenticator
Workshop time!
Resources

- freeipa-users@lists.fedorahosted.org
- #freeipa  #sssd
- Blogs: http://planet.freeipa.org/
- https://github.com/freeipa
THANK YOU