FreelIPA
Community Portal

Christian Heimes
cheimes@redhat.com
2015-08-27
Topics

1. Introduction
2. Features and open issues
3. Installation (demo)
4. Community Portal workflow (demo)
5. FreeIPA Web UI (demo)
6. Open Discussion
Please mute your client.
Topics

1. Introduction
2. Features and open issues
3. Installation (demo)
4. Community Portal workflow (demo)
5. FreeIPA Web UI (demo)
6. Open Discussion
Hi, my name is Christian.

- Red Hatter since May 2015
- developer with FreeIPA & Certificate System
- remotee from Hamburg / Germany
- German (sorry for my accent)
- I’m rather new to FreeIPA stack.
  (I may not be able to answer all questions.)
About FreeIPA

- Integrated security information management solution
- combines
  - Linux
  - 389 Directory Server (LDAP)
  - MIT Kerberos
  - Bind DNS
  - Dogtag PKI certificate system
  - more (SSSD, NTP, Radius, …)
About FreeIPA (2)

- Identity management (users, groups, hosts, services)
- Permissions (roles, privileges, delegations)
- Policies (sudo, SELinux, passwords)
- Authentication (Kerberos, SSSD, OTP, ssh keys, X.509 certs, smart cards)
- Public Key Infrastructure to issue and track X.509 certs
- ...

About community portal

- written by our intern Drew Erny during the summer
- show case for self-service features
  - self registration of new users
  - password reset
- written in Python as standalone WSGI service
- uses FreeIPA’s Python API for RPC
Topics

1. Introduction
2. Features and open issues
3. Installation (demo)
4. Community Portal workflow (demo)
5. FreeIPA Web UI (demo)
6. Open Discussion
Scope and features

Community Portal
- self-registration
- password reset

FreeIPA web UI / CLI
- SSH keys
- certificates
- user data
- vault
- administration
Technologies

- WSGI application
- Python 2.7 (FreeIPA 4.2 restriction)
- CherryPy
- SQLAlchemy + sqlite
- captcha
- Jinja2 as templating language
- smtplib for notifications (to be replaced)
- ipalib for RPC
- Kerberos client tab for authentication
Self registration

- A user can apply for an account.
  - Registration is protected by a captcha.
- New accounts are in a staging area.
- An admin has to approve new accounts first.
- Self registered users are tracked in a user group.
Self registration (2)

Missing features:

- No email validation.
- Unique email addresses are not enforced.
- User is not informed when an account has been approved or rejected.
- User can’t set a password. She has to go through password rest after her account has been activated.
Password reset

- A user can request a password reset by login.
- Reset is protected by a captcha.
- The portal sends a reset token to the user’s email address.
- The reset token allows the user to set a new password.
Password reset (2)

Missing features:

- Password change isn’t supported yet. Instead the portal assigns a temporary password. The user has to set a new password in the FreeIPA Web UI or Kerberos.
- Account lookup by email address is not supported.
- Logins or external password changes don’t invalidate a reset token.
Security

- Portal has limited permissions.
  - It can only create stage users.
  - Can only modify password of self-registered users.
- Restrictions are enforced on server side and LDAP.
  For example LDAP ACIs forbid password changes except for members of the self-service group.
- Password reset doesn’t reveal existence of a user.
- All forms are protected by captchas.
Future improvements

- customization support for templates
- i18n
- email notification
- audit logs
Topics

1. Introduction
2. Features and open issues
3. Installation (demo)
4. Community Portal workflow (demo)
5. FreeIPA Web UI (demo)
6. Open Discussion
Installation on Fedora 22

- install dependencies
- install portal
- configure server as FreeIPA client
- create portal user, authentication and permissions
- configure portal

For now the portal is designed to run on its own machine.
Topics

1. Introduction
2. Features and open issues
3. Installation (demo)
4. Community Portal workflow (demo)
5. FreeIPA Web UI (demo)
6. Open Discussion
Self registration of a new user

Demo
Password reset

Demo
Topics

1. Introduction
2. Features and open issues
3. Installation (demo)
4. Community Portal workflow (demo)
5. FreeIPA Web UI (demo)
6. Open Discussion
Topics

1. Introduction
2. Features and open issues
3. Installation (demo)
4. Community Portal workflow (demo)
5. FreeIPA Web UI (demo)
6. Open Discussion
Resources

Source code and issuer tracker

https://github.com/freeipa/freeipa-community-portal

Documentation:

http://freeipa-community-portal.readthedocs.org/

Design specs:

https://www.freeipa.org/page/Category:FreeIPA_Community_Portal

Contact:

cheimes@redhat.com

Freenode #freeipa
Resources (2)

Talking to FreeIPA API With Sessions and JSON-RPC