Red Hat Identity Management
Overview

Thorsten Scherf
Senior Consultant
Red Hat Global Professional Services
Agenda

• What is Red Hat Identity Management?
• Main values
• Architecture
• Features
• Active Directory Integration
• Resources
What is Red Hat Identity Management?

• Red Hat Identity Management is a solution based on FreeIPA (or just IPA) open source technology
• IPA stands for Identity, Policy, Audit
  • FreeIPA open source project was started in 2007
  • FreeIPA v1 was released in 2008
  • FreeIPA v3 RC is available
Main values

- IPA is a domain controller for Linux/UNIX environment
  - Think Active Directory but for Linux
  - Central server that stores identity information, policies related to identities and performs authentication
High Level Architecture

- PKI
- KDC
- LDAP
- CLI/GUI

Unix/Linux

Admin
Why IPA?

• Identity and authentication is a complex problem – many disjoint technologies exist
• We want to make it more simple to deploy and use
• With the growth of the Linux share of servers in the enterprises there should be a server that has needs of Linux clients in its heart
Features

• Centralized authentication via Kerberos or LDAP
• Identity management:
  • users, groups, hosts, host groups, netgroups, services
• Manageability:
  • Simple installation scripts for server and client
  • Rich CLI and web-based user interface
  • Pluggable and extensible framework for UI/CLI
  • Flexible delegation and administrative model
Features (Continued)

- Certificate provisioning for hosts and services
- Serving sets of automount maps to different clients
- Advanced features:
  - Host-based access control
  - Centrally-managed SUDO
  - Group-based password policies
  - Automatic management of private groups
  - Can act as NIS server for legacy systems
  - Painless password migration
  - Managed hosts
Features (Continued)

- SELinux policy management
- SSH key management
- Cross Kerberos-Trust for mixed IdM <-> AD setups
- Optional integrated DNS server managed by IPA
- Replication:
  - Supports multi-server deployment based on the multi-master replication
  - User replication with MS Active Directory
  - Separate topology for CAs
- Compatibility with broad set of clients
Under the Hood

IPA Core
- NTP
- CA
- Directory Server
- DNS
- Management framework

Authentication
- Kerberos KDC

Users, Groups, Netgroups, HBAC
- SSSD
- Certmonger

Name lookups and service discovery
- nss_ldap

Cert tracking & provisioning
- ipa-client

Other maps
- Other maps

Enrollment & un-enrollment

Management Station
- CLI
- WEBUI
- Browser

Managed host (client)

Management
Under the Hood

**IPA Core**
- NTP
- CA
- Directory Server
- DNS
- Management framework

**Kerberos KDC**

**Directory Server**

**Certmonger**
- Configures nss_ldap
  - Cert tracking & provisionning
  - Other maps
  - Enrollment & un-enrollment

**SSSD**
- Configures ipa-client

**Managed host (client)**

**Management Station**
- CLI
- WEBUI
- Browser

**Authentication**

**Users, Groups, Netgroups, HBAC**

**Name lookups and service discovery**

**Enrollment & un-enrollment**
Client Configurations

- **SSSD**
  - With IPA back end
  - LDAP or Proxy for identity
  - Kerberos or LDAP for authentication
  - nss_ldap for other maps

- **Non-SSSD**
  - LDAP (nss_ldap) or NIS (nss_nis) for identity
  - LDAP (pam_ldap) or Kerberos (pam_krb5) for auth
AD – IdM Integration

• For most companies AD is the central hub of the user identity management inside the enterprise

• All systems that AD users can access (including Linux) need (in some way, i.e. directly or indirectly) to have access to AD to perform authentication and identity lookups

• In some cases the AD is the only allowed central authentication server due to compliance requirements

• In some cases DNS is tightly controlled by the Windows side of the enterprise and non Windows systems need to adapt to this
Aspects of integration

- Authentication
  - User logs into a Linux system, how he is authenticated?
- Identity lookup
  - How system knows about the right accounts?
  - How AD accounts are mapped to POSIX?
- Name resolution and service discovery
  - How system knows where is its authentication and identity server?
- Policy management
  - How other identity related policies are managed on the system?
**IdM Based Integration Option**

**AD**
- DNS
- LDAP
- KDC

**IdM**
- DNS
- LDAP
- KDC

Users are synchronized from AD to IdM

A DNS zone is delegated by AD to IdM to manage Linux environment

**Linux System**

**SSSD**
- Authentication
- Identities
- Name resolution

**Policies**
- sudo
- hbac
- automount
- selinux

Policies are centrally managed over LDAP

Name resolution and service discovery queries are resolved against IdM
IdM – AD Trust

Domains trust each other. Users stay where they are, no synchronization needed.

A DNS zone is delegated by AD to IdM to manage Linux systems or IdM has an independent namespace.

Policies are centrally managed over LDAP.

Client software connects to the right server depending on the information it needs.

Linux System

SSSD
- Authentication
- Identities
- Name resolution

Policies
- sudo
- hbac
- automount
- selinux
IdM 3.0

- Targeted for RHEL6.4
- Cross Kerberos-Trust for mixed IdM <-> AD setups
- Multiple IdM domains
- SELinux policy management
- Additional standard maps
- UI enhancements
Future features

- Disk encryption key management
- External authentication integration (OTP)
- User certificate management
- RADIUS
Resources

- Project wiki: www.freeipa.org
- Project trac: https://fedorahosted.org/freeipa/
- Code: http://git.fedorahosted.org/git/?p=freeipa.git
- SSSD: https://fedorahosted.org/sssd/
- Certmonger: https://fedorahosted.org/certmonger/
- Mailing lists:
  - freeipa-users@redhat.com
  - freeipa-devel@redhat.com
  - freeipa-interest@redhat.com
Resources

• Project wiki: www.freeipa.org
• Project trac: https://fedorahosted.org/freeipa/
• Code: http://git.fedorahosted.org/git/?p=freeipa.git
• SSSD: https://fedorahosted.org/sssd/
• Certmonger: https://fedorahosted.org/certmonger/
• Mailing lists:
  • freeipa-users@redhat.com
  • freeipa-devel@redhat.com
  • freeipa-interest@redhat.com
Questions?