Open Source Identity Management

From Password to Policy

David Sirrine
Senior Technical Account Manager - Red Hat
03 June, 2016
What to expect:

- Introductions
- What’s in an identity and why is it important?
- What are my options?
- Why is this all important?
- Put the sexy back in Identity Management
Introductions
Who am I?

- Senior Technical Account Manager at Red Hat
- Community member for FreeIPA, Dogtag, SSSD, opensc, and 389-ds
- Husband
- Father
- Baker
- Dog owner
- Man of many interests
Also... Happy National Donut Day!

I LOVE DONUTS

DONUTS ARE MY FAVORITE
What is an identity?
So... Who do you think you are?
Or “what” for that matter...

- #define identity
- Everything has an identity!
- To secure your environment, you must first identify your environment
  - People (users)
  - Places (locations, hosts, etc.)
  - Things (hosts, services, devices, etc.)
- You ARE a unique snowflake.
- You ARE your job. You ARE the clothes you wear!
  - Sorry Tyler... You’re wrong.
So why is this important?

- Well, knowing is half the battle!
  - <pause for unanimous G. I. Joe!>
- When you know WHO you have, and WHAT you have, you can apply policy!
  - Policy provides the when, where, and why
OK... What are my options?
So many tools, not enough time.

- So many different tools out there
  - OpenLDAP
  - MIT Kerberos
  - Etc.
- We’re going to focus on a couple today.
  - Enter FreeIPA!
FreeIPA Architecture

- KDC
- PKI
- LDAP
- DNS
- CLI/UI
- Linux
- UNIX
- Admin
FreeIPA Architecture Is...

- Each component provided by individual projects:
  - MIT Kerberos
  - bind, bind-dyndb, bind-ldap
  - 389-ds
  - Dogtag
- client/server based
  - Ipa-server
  - Ipa-client
- SSSD as authentication ‘gateway’
FreeIPA Features

- Centralized authentication via Kerberos or LDAP
- Identity management:
  - users, groups, hosts, host groups, netgroups, services
  - user lifecycle management
    - Stage, Active, Preserved
- 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
    - Self, delegated, role based; read permissions
Features (cont.)

- Replication:
  - Supports multi-server deployment based on the multi-master replication (up to 20 replicas)
  - Recommended deployment 2K-3K clients per replica
  - Details depend on the number of data centers and their geo location

- Backup and Restore

- Compatibility with broad set of clients (LINUX/UNIX)
Policy Features

- Host-based access control
- Centrally-managed SUDO
- SSH key management
- Group-based password policies
- Automatic management of private groups
- Can act as NIS server for legacy systems
- SELinux user mapping
- Auto-membership for hosts and users
- Serving sets of automount maps to different clients
- Different POSIX data and SSH keys for different sets of hosts
Two factor authentication

- **2FA**
  - Native HOTP/TOTP support with FreeOTP and Yubikey
  - Proxied 2FA authentication over RADIUS for other solutions
  - 2FA for AD users (in works)
- **Smart Card**
  - Associate X.509 certificate with user record
  - Leverage SSSD or pam_pkcs11 to leverage for authentication
DNS

- DNS is optional but convenient
- Advantages (automation and security):
  - The SRV records get created automatically
  - Host records get created automatically when hosts are added
  - The clients can update their DNS records in a secure way (GSS-TSIG)
  - The admin can delegate management of the zones to whomever he likes
  - Built in DNSSEC support (Tech Preview in RHEL 7.2)
- Disadvantages:
  - You need to delegate a zone
PKI

- CA related capabilities
  - Certificate provisioning for users (new in RHEL-7.2), hosts and services
  - Multiple certificate profiles (new in RHEL-7.2)
  - Sub CAs (in works)

- CA deployment types
  - CA-less
  - Chained to other CA
  - Self-signed root

- Tool to change deployment type and rotate CA keys
  - Flexibility in deploying CAs on different replicas

- Key store (Vault) - new in RHEL-7.2
Requisite Meme

YOUR PKI IS BAD
AND YOU SHOULD FEEL BAD

memegenerator.net
Managing Identities (GUI)
Managing Policy (GUI)
Managing Authentication (GUI)
Managing Network Services (GUI)

<table>
<thead>
<tr>
<th>Identity</th>
<th>Policy</th>
<th>Authentication</th>
<th>Network Services</th>
<th>IPA Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automount</td>
<td>DNS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Automount Locations**

- Location
- default

Showing 1 to 1 of 1 entries.
Managing the IPA server (GUI)
So what about the CLI?

- Everything done through the GUI has an associated CLI command
- Leverages API backend.
- `ipa <operation> <options>`
- Examples:
  - `ipa user-add dsirrine --first David --last Sirrine`
  - `ipa group-add foo --users=dsirrine`
  - `ipa sudocmd-add --setattr=<attribute>`
SSSD

- SSSD = System Security Services Daemon
- SSSD is a service used to retrieve information from a central identity management system.
- SSSD connects a Linux system to a central identity store:
  - Active Directory
  - FreeIPA
  - Any other directory server
- Provides authentication and access control
- Credential caching
SSSD/FreeIPA Integration

Authentication can be LDAP or Kerberos

And more: netgroups, automembership, OTP...

Linux System

SSSD
- Authentication
- Identities
- Name Resolution
- Certificates/Keys

Policies
- sudo
- HBAC
- automount
- selinux
- ssh public keys
Realmd

- Component of Linux
- Main goal is to detect domain environment using DNS (detection)
  - AD
  - FreeIPA
  - Kerberos
- Join system to the domain (using SSSD or Winbind)
- Do it in one command or click
- Availability: command line, D-BUS interface, system installer, desktop
  - realm {join, leave, list, trust}
Active Directory Integration
SSSD Based Direct Integration

AD can be extended to serve basic sudo and automount
Can map AD SID to POSIX attributes or use SFU/IMU
Can join system into AD domain (realmd)
Leverages native AD protocols and LDAP/Kerberos

Authentication can be LDAP or Kerberos
GPO support for HBAC is available
Other policies are delivered via configuration files and managed locally or via a config server like Satellite or Puppet.

Active Directory
- DNS
- LDAP
- KDC

Linux System
- SSSD
  - Authentication
  - Identities
  - Name Resolution
- Policies
  - sudo
  - HBAC
  - automount
  - selinux
  - ssh keys
SSSD Based Direct Integration
Pros and Cons

- **Pros:**
  - Does not require SFU/IMU but can use them
  - Can be used with different identity sources
  - Support transitive trusts in AD domains and forest trusts with FreeIPA
  - Supports CIFS client and Samba FS integration
  - GPO for Windows based HBAC

- **Cons:**
  - No NTLM support, no support for AD forest trusts (yet)
  - No SSO with OTP
  - Not all policies are centrally managed
FreeIPA/IdM AD Integration with Trust

FreeIPA/IdM
- PKI
- DNS
- LDAP
- KDC

Active Directory
- KDC
- LDAP
- DNS
- PKI

Linux System
SSSD
- Authentication
- Identities
- Name Resolution
- Certificates/Keys

Policies
- sudo
- HBAC
- automount
- selinux
- ssh keys

PKI
DNS
LDAP
KDC
FreeIPA/IdM AD Integration with Trust

Chain

Linux System

FreeIPA/IdM

PKI, DNS, LDAP, KDC

Active Directory

KDC, LDAP, DNS, PKI

SSSD

Authentication, Identities, Name Resolution, Certificates/Keys

Policies

sudo, HBAC, automount, selinux, ssh keys
FreeIPA/IdM AD Integration with Trust

FreIIPA/IdM

PKI
DNS
LDAP
KDC

Delegate Zone

Active Directory

KDC
LDAP
DNS
PKI

Linux System

SSSD
Authentication
Identities
Name Resolution
Certificates/Keys

Policies
sudo
HBAC
automount
selinux
ssh keys
FreeIPA/IdM AD Integration with Trust

FreeIPA/IdM

PKI
DNS
LDAP
KDC

Active Directory

KDC
LDAP
DNS
PKI

Cross Forest Trust

Linux System

SSSD
Authentication
Identities
Name Resolution
Certificates/Keys

Policies
sudo
HBAC
automount
selinux
ssh keys

PKI
DNS
LDAP
KDC

David Sirrine - Red Hat
FreeIPA/IdM AD Integration with Trust

FreeIPA/IdM
- PKI
- DNS
- LDAP
- KDC

Active Directory
- KDC
- LDAP
- DNS
- PKI

Linux System
- SSSD
  - Authentication
  - Identities
  - Name Resolution
  - Certificates/Keys
- Policies
  - sudo
  - HBAC
  - automount
  - selinux
  - ssh keys
Trust Based Solution
Pros and Cons

● Pros:
  ○ Reduces cost – no CALs or 3rd party
  ○ Policies are centrally managed
  ○ Gives control to Linux admins
  ○ Enabled independent growth of the Linux environment
  ○ No synchronization required
  ○ Authentication happens in AD

● Requirement:
  ○ Proper DNS setup
User Mapping

Details

- Can leverage SFU/IMU for POSIX (brown field)
- Can do dynamic mapping of the SIDs to UIDs & GIDs (green field)
- Static override with ID views
Trust

Details

- Two-way and one-way trust (FreeIPA trusts AD)
  - AD/Samba DC trusting FreeIPA is on the roadmap
- Trust agents (different behavior of different replicas)
- Migration from the sync to trust
Federated Identity with Ipsilon or Keycloak

- Bring your own Identity Provider (IDP)
- SAML, OpenID, OAUTH
- Allows for authentication with trusted credentials from outside source
  - You’ve seen it. “Log in with your Facebook now!”
- Think of connecting all your services with a single trusted identity
Interesting and upcoming

- **Clevis and Tang**
  - Asymmetric secret sharing based on environmental data

- **pam_hbac**
  - Module that provides hbac support for Unix

- **pam_sudo**
  - Module that provides sudo support for Unix
Why is this all important?
Limit your known unknowns

- Solid Identity Management concepts and practices can limit your known unknowns
- Users, groups, hosts, services, policies... They’re all tied together.
Putting the sexy back in Identity Management
Resources, blogs, etc.

- Where can you find me?
  - Twitter: @dsirrine
  - https://dsirlab.wordpress.com
  - #freeipa
  - #dogtag-pki
Training

- Training
  - http://www.freeipa.org/page/Documentation#FreeIPA_Training_Series
- Blog aggregation
  - http://planet.freeipa.org/
- FreeIPA demo instance in the cloud
  - http://www.freeipa.org/page/Demo
More resources!

- **Community Sites:**
  - FreeIPA - [www.freeipa.org](http://www.freeipa.org)
    - freeipa-users@redhat.com & freeipa-devel@redhat.com
  - SSSD - [https://fedorahosted.org/sssd/](https://fedorahosted.org/sssd/)
    - sssd-users@redhat.com & sssd-devel@redhat.com
  - Dogtag - [https://pki.fedoraproject.org](https://pki.fedoraproject.org)
    - pki-users@redhat.com & pki-devel@redhat.com
    - 389-users@redhat.com & 389-devel@redhat.com
Blogs

- Pam_hbac
  - [https://jhrozek.wordpress.com/2016/05/26/pam_hbac-a-pam-module-to-enforce-ipa-access-control-rules/](https://jhrozek.wordpress.com/2016/05/26/pam_hbac-a-pam-module-to-enforce-ipa-access-control-rules/)

- Clevis and Tang
  - [https://blog-ftweedal.rhcloud.com/2016/02/introduction-to-tang-and-clevis/](https://blog-ftweedal.rhcloud.com/2016/02/introduction-to-tang-and-clevis/)

- PKI Goodness
  - [https://blog-nkinder.rhcloud.com/](https://blog-nkinder.rhcloud.com/)
  - [https://blog-ftweedal.rhcloud.com/](https://blog-ftweedal.rhcloud.com/)

- Security
  - [http://sobersecurity.blogspot.com/](http://sobersecurity.blogspot.com/)
THANK YOU