Integrating Linux systems with Active Directory

Dmitri Pal
Engineering Director, Red Hat, Inc.

Security Camp at BU
Agenda

- Problem statement
- Aspects of integration
- Integration options
- Recommendations
Problem Statement

- 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 is he 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?
Integration Options

Direct Integration

- Active Directory
  - Linux system
  - Linux system
  - Linux system

Indirect Integration

- Active Directory
  - Central Identity Server
  - Linux system
  - Linux system
  - Linux system
Direct Integration Options

- 3rd party
- Legacy (pam_krb5, pam_ldap, nss_ldap, ns1cd)
- Traditional – winbind
- Contemporary – SSSD (with realmd)
Third Party Direct Integration

Authentication can be LDAP or Kerberos

Client may use native AD protocols

ID mapping is implementation specific or uses SFU/IMU extensions in AD

Security Camp at Boston University: August 20th, 2015
Pros and Cons of the 3rd Party Option

• Pros
  – Everything is managed in one place including policies

• Cons
  – Requires third party vendor
  – Extra cost per system (adds up)
  – Limits UNIX/Linux environment independence
  – Requires software on AD side
Legacy Integration Option

ID mapping uses SFU/IMU extensions in AD

AD can be extended to serve basic sudo and automount

Policies are delivered via configuration files and managed locally or via a config server like Satellite or Puppet.

Authentication can be LDAP or Kerberos

Security Camp at Boston University: August 20th, 2015
Pros and Cons of the Legacy Option

• Pros:
  − Free
  − No third party vendor is needed
  − Intuitive

• Cons:
  − Requires SFU/IMU AD extension
  − Policies are not centrally managed
  − Hard to configure securely
Traditional Integration Option

Active Directory

- DNS
- LDAP
- KDC

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 (net join or realm)
Leverages native AD protocols and LDAP/Kerberos

Policies are delivered via configuration files and managed locally or via a config server like Satellite or Puppet.

Authentication can use LDAP, Kerberos or NTLM

Linux system

Samba Winbind
- Authentication
- Identities
- Name Resolution

Policies
- sudo
- hbac
- automount
- selinux
Pros and Cons of the Traditional Option

• Pros:
  – Well known
  – Does not require third party
  – Does not require SFU/IMU
  – Supports trusted domains

• Cons:
  – Can connect only to AD and very MSFT focused
  – Has some perceived stability issues
  – Policies are not centrally managed
Introducing SSSD

- 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

- Top technology in the evolution chain of the client side IdM components
SSSD Features

- Multiple parallel sources of identity and authentication – domains
- All information is cached locally for offline use
  - Remote data center use case
  - Laptop or branch office system use case
- Advanced features for
  - FreeIPA integration
  - AD integration
Identity Source Integration with SSSD

- Client
- NSS Responder
- Identity Provider
- Auth Provider
- Domain Provider
- Cache
- SSSD
- Identity Server
- Authentication Server
Why SSSD is our choice?

- Supports everything that previous UNIX solutions support and more
- Brings architecture to the next level
- Supports multiple sources – domains
- Supports IdM specific features
- Supports trusts between AD and IdM
- Has a feature parity with windbind in core areas
Contemporary Integration Option

Active Directory

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 (realm)
Leverages native AD protocols and LDAP/Kerberos

Authentication can use LDAP or Kerberos

Linux system

SSSD

Authentication
Identities
Name Resolution

Policies

sudo
hbac
automount
selinux

GPO support for HBAC is available.
Other policies are delivered via configuration files and managed locally or via a config server like Puppet.
Pros and Cons of the Contemporary Option

• Pros:
  – Does not require SFU/IMU but can use them
  – Can be used with different identity sources
  – Support transitive trusts in AD domains and 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)
<table>
<thead>
<tr>
<th>Feature</th>
<th>LDAP/KRB</th>
<th>Winbind</th>
<th>SSSD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate using Kerberos or LDAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Identities are looked up in AD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Requires SFU/IMU</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>ID mapping</td>
<td>None</td>
<td>Multiple ways</td>
<td>Most popular way</td>
</tr>
<tr>
<td>System is joined into AD</td>
<td>Manual</td>
<td>Has join utility</td>
<td>Realmd</td>
</tr>
<tr>
<td>Supports trusts for AD domains</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Supports heterogeneous domains and advanced features</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Support file sharing</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>HBAC GPO</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>NTLM support</td>
<td>No</td>
<td>Yes</td>
<td>1.14 (spring 2016)</td>
</tr>
</tbody>
</table>
Bottom Line of the Direct Integration

- SSSD is the way to go
- Winbind is the fallback option:
  - if you rely on NTLM (please do not, it is very insecure)
  - If you have multiple forests and need users from different forests to access the Linux system
Limitations of the Direct Integration Options

- Policy management is mostly left out
- Per system CALs add to cost
- Linux/UNIX administrators do not have control over the environment

*All these limitations prevent growth of the Linux environment inside your organization!*
Domain trust is established on the Kerberos level. DNS zone can be delegated to FreeIPA, can be a subdomain. Client software connects to the right server depending on the information it needs. Policies are managed centrally.
Pros and Cons of the FreeIPA Trust

- **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
Terminology

• FreeIPA – open source project and technology
• IdM – Identity Management in Red Hat Enterprise Linux or CentOS
• IdM is a stable version of the FreeIPA project
## Direct vs. Indirect

<table>
<thead>
<tr>
<th>Use Case</th>
<th>Direct Integration</th>
<th>Trust-based Integration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Linux Clients</td>
<td>• Small, less than 30</td>
<td>• Large, 30 or more</td>
</tr>
<tr>
<td>Policy Management</td>
<td>• Requires separate solution</td>
<td>• Included with FreeIPA</td>
</tr>
<tr>
<td>Cost</td>
<td>• Grows with # of clients(CALs)</td>
<td>• Fixed at one connection</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Free in Fedora/RHEL/CentOS</td>
</tr>
<tr>
<td>Best Investment Profile</td>
<td>• Short-term</td>
<td>• Long-term</td>
</tr>
</tbody>
</table>

If you think environment is big enough for a content management system it is big enough for FreeIPA!
Summary

- Consider direct integration for a small deployment
- Consider SSSD as a main solution for direct integration
- Use winbind as a fallback alternative
- Consider IdM/FreeIPA trust based solution for a bigger or growing environment
- Use Fedora to discover, CentOS to prepare and RHEL to deploy your central identity management solution
Resources

- **FreeIPA**
  - Project wiki: [www.freeipa.org](http://www.freeipa.org)
  - Project trac: [https://fedorahosted.org/freeipa/](https://fedorahosted.org/freeipa/)
  - Code: [http://git.fedorahosted.org/git/?p=freeipa.git](http://git.fedorahosted.org/git/?p=freeipa.git)
  - Mailing lists:
    - freeipa-users@redhat.com
    - freeipa-devel@redhat.com
    - freeipa-interest@redhat.com

- **SSSD**: [https://fedorahosted.org/sssd/](https://fedorahosted.org/sssd/)
  - Mailing lists:
    - sssd-devel@lists.fedorahosted.org
    - sssd-users@lists.fedorahosted.org

- **Certmonger**: [https://fedorahosted.org/certmonger/](https://fedorahosted.org/certmonger/)
Questions?
THANK YOU!