Interoperability Update:
Red Hat Enterprise Linux 7 beta
and Microsoft Windows

Mark Heslin
Principal Systems Engineer
Red Hat Systems Engineering

Dmitri Pal
Senior Engineering Manager
Red Hat Software Engineering
Agenda

• Integration Overview
• Building Blocks
• Integration Options - Red Hat Enterprise Linux 6
• Integration Options - Red Hat Enterprise Linux 7
• Future Features
• Q&A
• Summary
Why Integrate?

• Simplify, consolidate user account administration
• Cost savings
• Flexibility
• Customization
...etc...
Where to start?

• Much material available (*blogs, docs, web articles*)
• Initially appears simple
• Upon closer examination...
  • Overwhelming number of integration options
  • Most material covers one configuration
  • None present full range

*The devil is in the details...*
What is Needed?

• Thorough understanding of components, interactions
• Awareness of technical, non-technical considerations
• Comparison of configurations, options
• Best practices, guidelines
• Assistance in making a selection
How to Integrate?

• Two options:
  1. Direct Integration
     • Connect systems directly to Active Directory using native Linux or 3rd party solutions
  2. Indirect Integration
     • Connect systems to centralized identity server which integrates to Active Directory
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 Solutions

• Native Linux:
  • Samba/Winbind
  • SSSD
  • Legacy (nss_ldap/pam_ldap/pam_krb5)

• 3rd Party:
  • Centrify
  • Quest (Dell)
  • Likewise (EMC)
Indirect Integration Solutions

- LDAP (account sync)
- Kerberos (cross-realm trust)
- Identity Management in Red Hat Enterprise Linux (IdM)
  - Account sync
  - Cross-realm Trust
Agenda

• Integration Overview

• Building Blocks

• Integration Options - Red Hat Enterprise Linux 6

• Integration Options - Red Hat Enterprise Linux 7

• Future Features

• Q&A

• Summary
Building Blocks - Overview

• Integration utilizes both applications and services
• Applications (e.g. Samba/Winbind, SSSD, etc.) depend on services
• Services common to both platforms:
  • DNS, Kerberos, LDAP, NTP
  • Differences in options, implementation details
• Service location can vary – i.e. different server, DNS domain, etc.

* Services are often the root-cause of integration issues *
Integration Building Blocks

Red Hat Enterprise Linux
- Samba
- IdM
- NTP
- Kerberos
- LDAP
- Winbind
- SSSD
- Legacy
- Third Party

Microsoft Windows Server
- Active Directory
- NTP
- Kerberos
- DNS
- LDAP
- IMU/SFU

Your goal: "Seamless Integration"

* Many options, considerations within each component *
Active Directory Domain Services (AD DS)

• Suite of directory services
• Customized versions:
  • Kerberos
  • Domain Name System (DNS)
  • Lightweight Directory Access Protocol (LDAP)
  • Network Time Protocol (NTP)
• Object hierarchy – nodes, trees, forests, domains
• Renamed in Windows Server 2008 R2

* Included in Windows Server (Server Role) *
Identity Management for UNIX (IMU)

• Extends Active Directory LDAP schema (UNIX Attributes)
• Defined by RFC 2307/bis (aka – POSIX attributes)
• Provides more granularity, central control over UNIX accounts:
  • Login Shell
  • Home Directory
• Activation:
  • Windows Server 2012, 2008 R2: enable IMU role service
  • Windows Server 2008, 2003 R2: enable IMU service
  • Windows Server 2003: enable SFU (services for UNIX)
Kerberos

• Provides single-sign on (SSO) capabilities
• Clients request ticket from trusted third party (KDC)
• Behavior configured by /etc/krb5.conf
• Applications (services) authenticate via PAM libraries:
  • pam_winbind (Samba), pam_sss (SSSD), pam_krb5 (Kerberos)
• Users authenticate via 'kinit'

* Install krb5-workstation for testing/troubleshooting *
LDAP (Lightweight Directory Access Protocol)

• Hierarchical directory service based on X.500
• Provides information storage/lookup (users, hosts, groups, etc.)
• Data transmitted securely via SSL, TLS
• Server implementations:
  • Red Hat Directory Server - enterprise level features and capabilities
  • OpenLDAP – may be used for development and small deployments

* Install openldap-clients for troubleshooting purposes *
Identity Management in RHEL (IdM)

- Centralized authentication, identity, policy management
- Based on FreeIPA (Identity, Policy and Audit)
- Contains native Linux domain services:
  - Kerberos
  - Domain Name System (DNS)
  - Lightweight Directory Access Protocol (LDAP)
  - Network Time Protocol (NTP)
  - Certificate Authority (CA)

*Similar to Active Directory but for Linux/UNIX clients*
Samba

• Open source suite of programs
• Provides file and print services
• Includes two daemons:
  • smbd (file and print services)
  • nmbd (NetBIOS name server)
• Samba v3.6 is current version (RHEL 6.5)
• Samba can be configured as client, server or both

* Behavior configured by /etc/samba/smb.conf *
Winbind

• Daemon included with Samba suite
• Unified logon to Active Directory accounts
• Minimizes need for separate accounts
• Primary functions:
  • Authentication of user credentials ("Who")
  • ID Tracking/Name Resolution via nsswitch ("Where")
  • ID Mapping of UID/GID <-> SID ("What")
• ID Mapping implemented through “backends”
SSSD (System Security Services Daemon)

• Access to different identity, authentication providers  
  (e.g. - Active Directory, IdM, LDAP native, LDAP w/Kerberos)
• Extensible (new identity, authentication sources)
• Supports off-line caching of user credentials (clients)
• Reduces load on identity servers
• Does not provide file sharing capabilities (yet)

* Extensible, enhanced alternative to Winbind *

Kerberos/LDAP client side (Legacy)

• NSS and PAM modules
  • nss_ldap
  • pam_ldap/pam_krb5
• Limited capabilities
• Load into the application memory bringing a lot of dependencies

* Consider using more advanced solutions *
Agenda

• Integration Overview
• Building Blocks
• Integration Options - Red Hat Enterprise Linux 6
• Integration Options - Red Hat Enterprise Linux 7
• Future Features
• Q&A
• Summary
Direct Integration Options in RHEL 6

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 – Red Hat Enterprise Linux 6

* Reference Architecture configurations – all components available today in Red Hat Enterprise Linux *
Which to choose?

• Recommended configurations selected based on:
  • Customer, field, partner interest
  • Engineering, Support, Services review
  • Feasibility, practicality for production environments
• SSSD is the **preferred** configuration
• If SSSD does not fit your needs then consider a Samba/Winbind configuration
• Legacy Kerberos/LDAP configuration is **least preferred**
## Configuration Comparison

<table>
<thead>
<tr>
<th>Configuration</th>
<th>Services Provided</th>
<th>Features</th>
<th>Use Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Samba/Winbind (idmap_rid)</td>
<td>• File sharing</td>
<td>• Templated shell, home dirs</td>
<td>&quot;Template-driven&quot;</td>
</tr>
<tr>
<td></td>
<td>• Login access</td>
<td>• Least intrusive to AD (No user/group ID attribute changes)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Algorithmic ID mappings</td>
<td></td>
</tr>
<tr>
<td>2. Samba/Winbind (idmap_ad)</td>
<td>• File sharing</td>
<td>• Customizable shell, home dirs</td>
<td>&quot;Customizable&quot;</td>
</tr>
<tr>
<td></td>
<td>• Login access</td>
<td>• Centralized user mgmt</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Assigned ID mappings</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User/group ID attributes set in AD (requires IMU)</td>
<td></td>
</tr>
<tr>
<td>3. SSSD w/AD provider</td>
<td>• Login access</td>
<td>• Advanced authentication</td>
<td>&quot;Enhanced&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User credential caching</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reduces client loading on server</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User/group ID attributes set in AD - optional (IMU - optional; RHEL 6.4+ not required)</td>
<td></td>
</tr>
<tr>
<td>4. Kerberos/LDAP</td>
<td>• Login access</td>
<td>• No off-line caching user credentials</td>
<td>&quot;Legacy&quot;</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• User/group ID attributes set in AD (requires IMU)</td>
<td></td>
</tr>
</tbody>
</table>
Decision Tree

Start

File sharing required?

User attributes modifiable in AD?

Deploy Recommended Configuration 1
Samba/Winbind (idmap_rid) "Template Driven"

Deploy Recommended Configuration 2
Samba/Winbind (idmap_ad) "Customizable"

Deploy Recommended Configuration 3
SSSD/Kerberos/LDAP "Enhanced"

Deploy Recommended Configuration 4
LDAP/Kerberos "Legacy"

Use enhanced capabilities?

Y
N

Y

N

N

Y
Reference Architecture

- Simplifies selection, deployment, integration
- Details components, considerations
- Compares “landscape” of configurations, options
- Provides best practices, guidelines, decision tree

Indirect Integration Options in RHEL 6

Direct Integration

Indirect Integration

Central Identity Server

Active Directory

Linux system

Linux system

Linux system
Indirect Integration – Red Hat Enterprise Linux 6

* All components available today in Red Hat Enterprise Linux *
IdM Benefits

• Linux infrastructure is managed via native concepts and protocols
• Centralized:
  • Host Based Access Control, SUDO, SSH keys, automount maps, SELinux user mappings, host groups, netgroups and more
• Separation of duties between different IT departments
• Reduced cost
Agenda

• Integration Overview
• Building Blocks
• Integration Options - Red Hat Enterprise Linux 6
  • Integration Options - Red Hat Enterprise Linux 7
• Future Features
• Q&A
• Summary
Direct Integration Improvements in RHEL 7

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 Improvements

• The majority of new features involved the AD provider
  • SSSD is now able to retrieve users and groups from trusted domains in the same forest
  • NetBIOS domain name can be used to qualify names
  • DNS updates and scavenging
  • DNS site discovery
  • Improved access control using AD access control provider
• The recommended way of setting up the AD provider is using `realmd`
Joining the AD domain with realmd

- `realmd` is a package that manages discovery and enrollment to several centralized directories including AD or IPA
- Easy to use
- By default, realmd sets up SSSD's AD provider
- Advanced features available – one-time password for join, custom OUs, etc
realmd Examples

• To discover all domains (requires NetworkManager)
  • realm discover

• To discover a particular domain
  • realm discover ad.example.com

• To join a domain
  • realm join ad.example.com
<table>
<thead>
<tr>
<th>Feature</th>
<th>SSSD with AD Provider</th>
<th>Winbind</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requires POSIX attributes</td>
<td>No (default)</td>
<td>No</td>
</tr>
<tr>
<td>Supports ID mapping</td>
<td>One method</td>
<td>Multiple methods</td>
</tr>
<tr>
<td>AD specific optimizations</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CIFS integration</td>
<td>Not yet (available upstream)</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS site support</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>DNS dynamic updates</td>
<td>Yes</td>
<td>Yes (requires manual configuration)</td>
</tr>
<tr>
<td>Enrollment with realmd</td>
<td>Yes (default)</td>
<td>Yes (must be explicitly selected)</td>
</tr>
</tbody>
</table>
Indirect Integration Improvements in RHEL 7

Direct Integration

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

Indirect Integration

- Active Directory
  - Central Identity Server
  - Linux system
  - Linux system
  - Linux system
IdM AD Integration Improvements

• IdM now supports cross realm Kerberos trusts with AD
  • Users from AD realm can access hosts and services on Linux side
  • IdM can trust different forests
  • IdM recognizes domain structure inside AD forest

• ID mapping:
  • Dynamic SID <-> POSIX mapping similar to how Samba did it
  • If you had POSIX attributes in AD they are respected

• Legacy clients can be exposed to AD users (Tech Preview)
  • Configure clients to use LDAP compatibility tree in IdM
Cross-realm Deployment

Identity Store

Active Directory

Trust

Active Directory

Central Identity Server

IdM in RHEL 7

Components

SSSD

SSSD

SSSD

Platform

RHEL 6.6+/7.0+ (Full trust capabilities)

RHEL 6.4/6.5 (Limited trust capabilities)

RHEL 5/6.3 + earlier (No trust capabilities)

Non-RHEL (No trust capabilities)
# Client Support with Cross-realm Trusts

<table>
<thead>
<tr>
<th>Feature/Client</th>
<th>Information look-up</th>
<th>Password auth</th>
<th>Kerberos auth</th>
<th>HBAC</th>
<th>SELinux user mapping</th>
<th>SUDO rules</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL 7 (main tree)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>RHEL 6.5 (main tree)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+/-</td>
<td>+</td>
</tr>
<tr>
<td>RHEL 6.4 (main tree)</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>RHEL 6.3 (compat tree)</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>RHEL 5.10 (compat tree)</td>
<td>+</td>
<td>+</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
</tbody>
</table>
## Direct vs. Indirect Integration

<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 IdM in RHEL</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>• Feature set free in RHEL</td>
</tr>
<tr>
<td>Best Investment Profile</td>
<td>• Short-term</td>
<td>• Long-term</td>
</tr>
</tbody>
</table>
Agenda

• Integration Overview
• Building Blocks
• Integration Options - Red Hat Enterprise Linux 6
• Integration Options - Red Hat Enterprise Linux 7
• Future Features
• Q&A
• Summary
Features Targeted for Follow up Releases

• Direct Integration:
  • GPO access control provider
  • SSSD CIFS integration

• Indirect Integration:
  • Qualification of the legacy client support
  • IdM users accessing AD resources – Global Catalog
  • Samba FS as a member server in the trust based deployment
  • Samba DC and IdM in cross forest trust relationships
Questions?
Summary (1)

- Viable AD integration options exist in the shipping software
- Decide which approach best fits your needs
  - Direct vs. Indirect
- Red Hat Enterprise Linux 6
  - Reference Architecture is available – covers direct integration options
Summary (2)

• Red Hat Enterprise Linux 7
  • RHEL 7 introduces new options and opportunities
  • IdM with trusts:
    • Brings integration to the next level
    • Simplifies heterogeneous architectures
  • New Reference Architecture is forthcoming
• Improving interoperability is an ongoing effort spanning multiple releases
  • Follow our efforts in the Open Source communities - SSSD, FreeIPA, Kerberos, 389, Dogtag and others
Thank you!

*Please complete an evaluation form!*
Supporting Slides
Detailed configuration examples
# cat /etc/samba/smb.conf

```
[global]
  workgroup = REFARCH-AD
  password server = WIN-SRV1.REFARCH-AD.REDHAT.COM
  realm = REFARCH-AD.REDHAT.COM
  security = ads
  idmap uid = 10000-19999
  idmap gid = 10000-19999
  idmap config REFARCH-AD:backend = rid
  idmap config REFARCH-AD:range = 10000000-19999999
  winbind enum users = no
  winbind enum groups = no
  winbind separator = +
  winbind use default domain = yes
  template homedir = /home/%D/%U
  template shell = /bin/bash
```
Configuration 1 - alternative (winbind – idmap_authorid)

• New backend introduced in Samba 3.6/RHEL 6.4
• Automatically allocates ID ranges when no domain is specified

```
# cat /etc/samba/smb.conf

[global]
    workgroup = EXAMPLE-AD
    password server = WIN-SRV1.EXAMPLE-AD.REDHAT.COM
    realm = EXAMPLE-AD.REDHAT.COM
    security = ads

    idmap config * : backend = autorid
    idmap config * : range = 1000000-19999999
    idmap config * : rangesize = 1000000

    idmap config REFARCH-AD:backend = ad
    idmap config REFARCH-AD:range = 20000000-29999999
```
Configuration 2 (winbind – idmap_ad)

```
# cat /etc/samba/smb.conf

[global]
  workgroup = REFARCH-AD
  password server = WIN-SRV1.REFARCH-AD.REDHAT.COM
  realm = REFARCH-AD.REDHAT.COM
  security = ads
  idmap uid = 20000-29999
  idmap gid = 20000-29999
  idmap config REFARCH-AD:backend = ad
  idmap config REFARCH-AD:range = 20000000-29999999
  idmap config REFARCH-AD:default = yes
  idmap config REFARCH-AD:schema_mode = rfc2307
  winbind nss info = rfc2307
  winbind enum users = no
  winbind enum groups = no
  winbind separator = +
  winbind use default domain = yes
  winbind nested groups = yes

<--- Integration Best Practice: *
  * Set uid/gid defaults for troubleshooting purposes *
```
Configuration 3 (SSSD/Kerberos/LDAP – w/AD provider)

```
# cat /etc/sssd/sssd.conf

[sssd]
config_file_version = 2
debug_level = 0
domains = refarch-ad.cloud.lab.eng.bos.redhat.com
services = nss, pam

# Uncomment/adjust as needed if IMU is not used:
# override_homedir = /home/%d/%u
# default_shell = /bin/bash

[domain/refarch-ad.cloud.lab.eng.bos.redhat.com]
id_provider = ad
access_provider = ad

# Permits offline logins:
# cache_credentials = true

# Use when service discovery not working:
# ad_server = win-srv1.refarch-ad.cloud.lab.eng.bos.redhat.com

# Enables use of POSIX UIDs and GIDs:
ldap_id_mapping = false
```
Configuration 4 (Kerberos/LDAP)

```
# cat /etc/nslcd.conf

binddn cn=AD LDAP-Bind,cn=users,dc=refarch-ad,dc=redhat,dc=com
bindpw LDAPBind!!
pagesize 1000
referrals off

filter passwd (&(objectClass=user)(!(objectClass=computer)) \ 
  (uidNumber=*))(unixHomeDirectory=*)
map passwd uid sAMAccountName
map passwd homeDirectory unixHomeDirectory
map passwd gecos displayName

filter shadow (&(objectClass=user)(!(objectClass=computer)) \ 
  (uidNumber=*))(unixHomeDirectory=*)
map shadow uid sAMAccountName
map shadow shadowLastChange pwdLastSet

filter group (objectClass=group)
map group uniqueMember member

uid nslcd
gid ldap
uri ldap://win-srv1.refarch-ad.redhat.com
base dc=refarch-ad,dc=redhat,dc=com
```
# Configuration 4 (Kerberos/LDAP) – continued

- PAM library configuration files (/etc/pam.d/password-auth, /etc/pam.d/system-auth)

## Before

<table>
<thead>
<tr>
<th>Type</th>
<th>Option</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>sufficient</td>
<td>pam_sss.so use_first_pass</td>
</tr>
<tr>
<td>account</td>
<td>[default=bad success=ok user_unknown=ignore]</td>
<td>pam_sss.so</td>
</tr>
<tr>
<td>password</td>
<td>sufficient</td>
<td>pam_sss.so use_authtok</td>
</tr>
<tr>
<td>session</td>
<td>optional</td>
<td>pam_sss.so</td>
</tr>
</tbody>
</table>

## After

<table>
<thead>
<tr>
<th>Type</th>
<th>Option</th>
<th>Module</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>sufficient</td>
<td>pam_krb5.so use_first_pass</td>
</tr>
<tr>
<td>account</td>
<td>[default=bad success=ok user_unknown=ignore]</td>
<td>pam_krb5.so</td>
</tr>
<tr>
<td>password</td>
<td>sufficient</td>
<td>pam_krb5.so use_authtok</td>
</tr>
<tr>
<td>session</td>
<td>optional</td>
<td>pam_krb5.so</td>
</tr>
</tbody>
</table>