LEARN. NETWORK. EXPERIENCE OPEN SOURCE.

June 11-14, 2013
Boston, MA
Red Hat Enterprise Linux 6 and Microsoft Windows Interoperability Update

Mark Heslin
Principal Systems Engineer, Red Hat
2013-06-14
Help you select the best configuration for your needs
Agenda

- **Overview**
- Components
- Configurations/Use Cases
- New Features
- Futures
- Summary/Q&A
Why Integrate?

- Simplify, consolidate user account administration
- Greater reliability, stability
- Cost savings
- Flexibility
- Customization
- Source code access
- Greater security
How to Integrate?

Options

- Third party products - Centrify, Likewise (EMC), Quest (Dell)
- VAR, systems integrator, consulting service
- In-house (“DIY”) solution

Approaches

- Direct (e.g. RHEL->AD)
- Indirect (e.g. RHEL->IdM->AD)
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
Reference Architecture

Integrating Red Hat Enterprise Linux 6 with Active Directory

Mark Heslin
Principal Software Engineer

Version 1.4
February 2013
Reference Architecture

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

Agenda

- Overview
- Components
- Configurations/Use Cases
- New Features
- Futures
- Summary/Q&A
Components - Overview

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

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

* Included in Windows Server 2008 R2 (Server Role) *
Identity Management for UNIX (IMU)

- Extends Active Directory LDAP schema (UNIX Attributes)
- Defined by RFC 2307/bis
- Provides more granularity, central control over UNIX accounts:
  - Login Shell
  - Home Directory
- Activation:
  - Windows 2008 R2: enable IMU server role
  - Windows 2008: enable IMU service
  - Windows 2003 R2: enable IMU service
  - Windows 2003: enable SFU (services for UNIX)
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 6.4)
- Samba can be configured as client, server or both

* Behavior configured by /etc/samba/smb.conf *
SMB/CIFS

- Client-server communications protocols
- Server Message Block (SMB) - IBM developed
- Common Internet File System (CIFS) – MS extended
- Both protocols used interchangeably
- SMB older, legacy servers (Windows 2000)

*Samba supports both protocols*
Winbind (1)

- 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")
Winbind (2)

- ID Mapping implemented through “backends”
- ~8 backends available
- ID Mappings classified as:
  - Allocating (r/w, local)
  - Algorithmic (r/o, calculated, consistent)
  - Assigned (r/o, assigned in AD, consistent)
- Each has advantages, disadvantages

* See Reference Architecture for further details *
Identity Management for 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 Server
- Supports AD cross domain trusts

* Similar to Active Directory but for Linux/UNIX clients *
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 (today)

* Extensible, enhanced alternative to Winbind *
Kerberos

- Provides single-sign on (SSO) capabilities
- Current version = V5
- Clients request ticket from trusted third party (KDC)
  - Key distribution center (KDC) = AD, IdM, etc.
- Behavior configured by /etc/krb5.conf
- Applications (services) authenticate via PAM libraries:
  - pam_winbind (Samba), pam_sss (SSSD), pam_krb5
- Users authenticate via 'kinit'

Integration best practice:

* Install krb5-workstation for testing/troubleshooting *
Agenda

- Overview
- Components
- Configurations/Use Cases
- New Features
- Futures
- Summary/Q&A
Configurations/Use Cases - Overview

- Many configurations and options to choose from
- Recommended configurations selected based on:
  - Customer, field, partner interest
  - Engineering, GSS 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
## Recommended Configurations - 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 • Login access</td>
<td>• Templated shell, home dirs • Least intrusive to AD (No user/group ID attribute changes) • Algorithmic ID mappings</td>
<td>“Template-driven”</td>
</tr>
<tr>
<td>2. Samba/Winbind (idmap_ad)</td>
<td>• File sharing • Login access</td>
<td>• Customizable shell, home dirs • Centralized user mgmt • Assigned ID mappings • User/group ID attributes set in AD (requires IMU)</td>
<td>“Customizable”</td>
</tr>
<tr>
<td>3. SSSD/Kerberos/LDAP</td>
<td>• Login access</td>
<td>• Advanced authentication, caching • Reduces client loading on server • SASL/GSSAPI binds (via Kerberos service principal keytab) • User/group ID attributes set in AD (requires IMU; RHEL 6.4 not required)</td>
<td>“Enhanced”</td>
</tr>
<tr>
<td>4. Kerberos/LDAP</td>
<td>• Login access</td>
<td>• No off-line caching user credentials • User/group ID attributes set in AD (requires IMU)</td>
<td>“Legacy”</td>
</tr>
</tbody>
</table>
Configuration 1 (winbind – idmap_rid)

```bash
# 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 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
```
Configuration 3 (SSSD/Kerberos/LDAP)

# cat /etc/sssd/sssd.conf

[sssd]
  config_file_version = 2
  domains = default
  services = nss, pam
  debug level = 0

[nss]

[pam]

[domain/default]
  cache_credentials = true
  enumerate = false
  id_provider = ldap
  auth_provider = krb5
  chpass_provider = krb5
  access_provider = ldap
  ldap_sasl_mech = GSSAPI
  ldap_sasl_authid = host/rhel-srv31.refarch-ad.redhat.com \ @REFARCH-AD.REDHAT.COM
Configuration 3 (SSSD/Kerberos/LDAP) - continued

```ini
ldap_schema = rfc2307bis
ldap_user_object_class = user
ldap_user_home_directory = unixHomeDirectory
ldap_user_principal = userPrincipalName
ldap_user_name = sAMAccountName
ldap_group_object_class = group
ldap_access_order = expire
ldap_account_expire_policy = ad
ldap_force_upper_caseRealm = true
ldap_disable_referrals = true

krb5_realm = REFARCH-AD.REDHAT.COM
```
# 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 changes (/etc/pam.d/password-auth, /etc/pam.d/system-auth)

**Before**

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

**After**

<table>
<thead>
<tr>
<th>Type</th>
<th>Option</th>
<th>Module</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>auth</td>
<td>sufficient</td>
<td>pam_krb5.so</td>
<td>use_first_pass</td>
</tr>
<tr>
<td>account</td>
<td>[default=bad success=ok user_unknown=ignore]</td>
<td>pam_krb5.so</td>
<td></td>
</tr>
<tr>
<td>password</td>
<td>sufficient</td>
<td>pam_krb5.so</td>
<td>use_authtok</td>
</tr>
<tr>
<td>session</td>
<td>optional</td>
<td>pam_krb5.so</td>
<td></td>
</tr>
</tbody>
</table>
Decision Tree (Which do I choose?)

1. **Start**
   - **File sharing required?**
     - **Y**
       - **User attributes modifiable in AD?**
         - **N**
           - Deploy Recommended Configuration 1
             - Samba/Winbind (idmap_rid) “Template Driven”
         - **Y**
           - Deploy Recommended Configuration 2
             - Samba/Winbind (idmap_ad) “Customizable”
     - **N**
       - **Use enhanced capabilities?**
         - **Y**
           - Deploy Recommended Configuration 3
             - SSSD/Kerberos/LDAP “Enhanced”
         - **N**
           - Deploy Recommended Configuration 4
             - LDAP/Kerberos “Legacy”
Customer, Partner, Field Requests – AD Integration
(2012-06 - 2013-06)

- Config 1 (idmap_rid)
- Config 2 (idmap_ad)
- Config 3 (sssd)
- Config 4 (Legacy)
- Misc. (Generic)
- RHS (Storage)
Agenda

- Overview
- Components
- Configurations/Use Cases
  - New Features
- Futures
- Summary/Q&A
New Features (Winbind idmap_autorid)

- New backend for 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

    ...etc...
```
New Features (Samba ID Map Changes)

- New default ID mapping for Samba 3.6/RHEL 6.4
- Default idmap uid/gid ranges deprecated

```bash
# 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 uid = 10000-19999
  idmap gid = 10000-19999
  idmap config EXAMPLE-AD : backend = rid
  idmap config EXAMPLE-AD : range = 10000000-19999999

* Deprecated ranges can remain in place - testparm *
generates warnings but ranges interpreted as:

  idmap config * : backend = tdb
  idmap config * : range = 10000-19999
```
New Features (SSSD/AD Provider)

- New provider for SSSD in RHEL 6.4
- Greatly simplifies SSSD configuration
- Identity Management for UNIX (IMU) not required
- Uses GSSAPI for encrypted identity lookups

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

[domain/example-ad.redhat.com]
enumerate = false
id_provider = ad

[sssd]
config_file_version = 2
domains = example-ad.redhat.com
services = nss, pam
```
New Features (SSSD/AD Provider – Configuration Steps)

1) Install packages
   (sssd, krb5-workstation, samba-common, authconfig)

2) Configure /etc/krb5.conf

3) Configure /etc/samba/smb.conf

4) Obtain Kerberos ticket: 'kinit Administrator'

5) Join Active Directory and obtain keytab: 'net ads join -k'

6) Verify keytab: 'klist -k'

7) Obtain Kerberos ticket using keytab: 'kinit -k'

8) Configure SSSD authentication:
   'authconfig --enablesssdauth --enablesssd --update'

9) Modify /etc/sssd/sssd.conf (as per previous page)

10) Restart SSSD: 'service sssd restart'
Agenda

- Overview
- Components
- Configurations/Use Cases
- New Features
- Futures
- Summary/Q&A
Futures

- Red Hat Enterprise Linux 7
  - Windows interoperability remains high focus
- realmd
  - New daemon simplifies AD domain join
  - Configures SSSD by default
  - CLI and GUI available
- SSSD
  - Full featured alternative to Winbind
  - File sharing capabilities (RHEL 7.1)
  - Preferred client for Red Hat Enterprise Linux
Identity Management – Red Hat Enterprise Linux 6

- **Identity Store**: Active Directory
- **IdM**: LDAP/LDAP/Kerberos
- **Framework**
  - (Config 1,2)
  - (Config 3)
  - (Config 4)
- **Components**
  - Samba/Winbind
  - SSSD
  - Legacy
- **Platform**: Red Hat Enterprise Linux

#redhat #rhsummit
Identity Management – Red Hat Product Portfolio

Identity Store
- Active Directory
- IdM
- LDAP
- LDAP/Kerberos

Identity Gateway
- Keystone
- PicketLink

Framework
- RHOS (OpenStack)
- JBoss

Components
- Samba/Winbind
- SSSD (Preferred)
- Legacy
- mod_auth_kerb
- mod_authnz_ldap

Platform
- RHEL
- RHEV
- RHS
- OSE (OpenShift)
- RHOS (OpenStack)
- JBoss

#redhat #rhsummit
Questions?
Summary (1)

- First glance deceptively simple
- Second glance appears overwhelming
- Many variables, components, interactions
- Reference Architecture simplifies selection, deployment and integration:

- See Customer Portal for additional materials:
  https://access.redhat.com/knowledge/
Summary (2)

- Hybrid configurations ok to consider
- Third-party products viable alternatives
- Prototype, test in advance
- Most issues have simple causes
- Role of SSSD, importance of IdM increasing

*Select the best configuration for your needs*
Thank you

Please complete an evaluation form!
Supplemental Slides
Bugzilla/KBase Solutions

- RHBA-2013:0486 (authconfig bugfix updates)
  (BZ #862195, BZ #874527)
- KBase #163693 (RHEL 6.3 SSSD breaks GSSAPI binds)
  https://access.redhat.com/site/solutions/163693
- KBase #296773 (Samba 3.6 ID Map Changes)
  https://access.redhat.com/site/solutions/296773
Configuration 1 (winbind – idmap_rid)

“Template-driven”
Configuration 1 (Authentication and ID Components)

- **Authentication**
  - pam_winbind
  - Kerberos

- **ID Tracking/Name Resolution**
  - nss_winbind
  - idmap_rid

---

Active Directory
Configuration 2 (winbind - idmap_ad)

Centralized Services

NTP
DNS

NTP
DNS
Samba
Winbind
rhel-srv21

NTP
DNS
Samba
Winbind
rhel-srv22

Active Directory

“Customizable”
Configuration 2 (Authentication and ID Components)

- **Winbind**
  - Authentication: pam_winbind
  - ID Tracking/Name Resolution: nss_winbind
  - ID Mapping: idmap_ad
  - Kerberos

- **Active Directory**
Configuration 3 (SSSD/Kerberos/LDAP)

Centralized Services

NTP
DNS

Active Directory

SSSD
Kerberos
LDAP

rhel-srv31

"Enhanced"

SSSD
Kerberos
LDAP

rhel-srv32
Configuration 3 (Authentication and ID Components)

- Authentication: pam_sss → Kerberos
- ID Tracking/Name Resolution: nss_sss → LDAP

SSSD

Active Directory
Configuration 4 (Kerberos/LDAP)

Centralized Services
- NTP
- DNS

Active Directory
- NTP
- DNS
- Kerberos
- LDAP

“Legacy”
- rhel-srv41
- rhel-srv42
Configuration 4 (Authentication and ID Components)

- **Authentication**
  - pam_krb5
  - Kerberos
- **ID Tracking/Name Resolution**
  - nss_ldap
  - LDAP

The diagram shows the flow of components from authentication to active directory.