RED HAT SUMMIT
10 YEARS and counting
SAN FRANCISCO | APRIL 14-17, 2014

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

redhat.

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...

redhat.

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...

redhat.

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

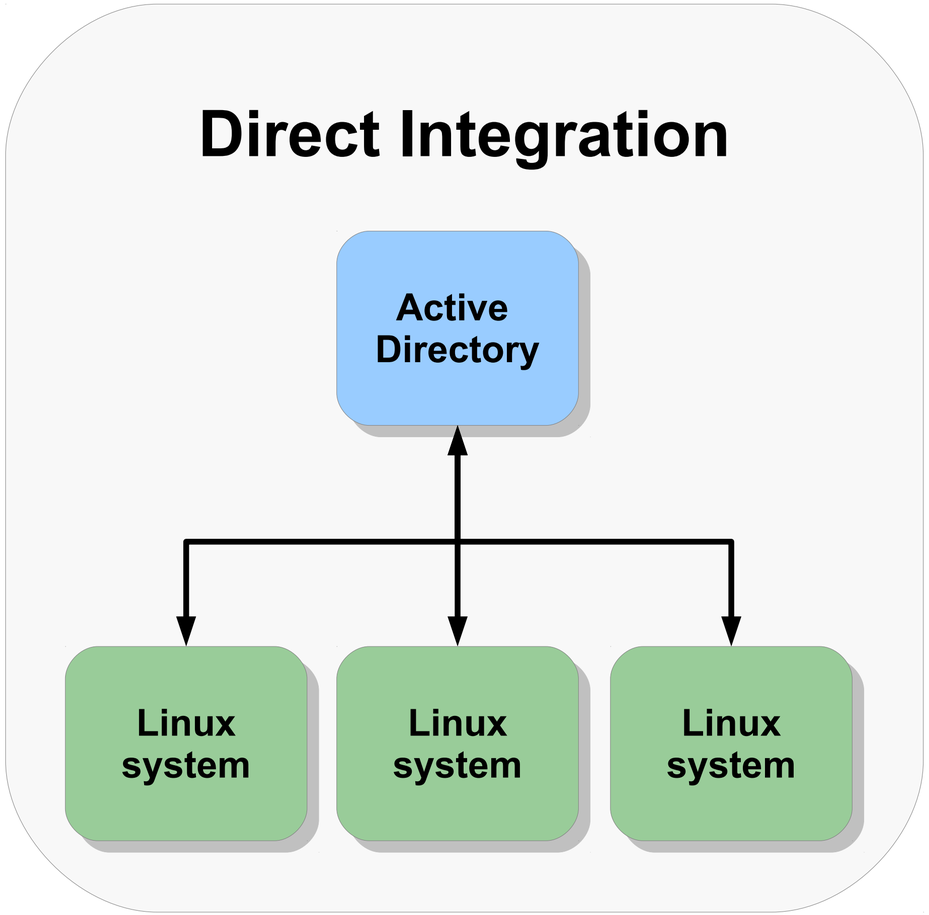
redhat.

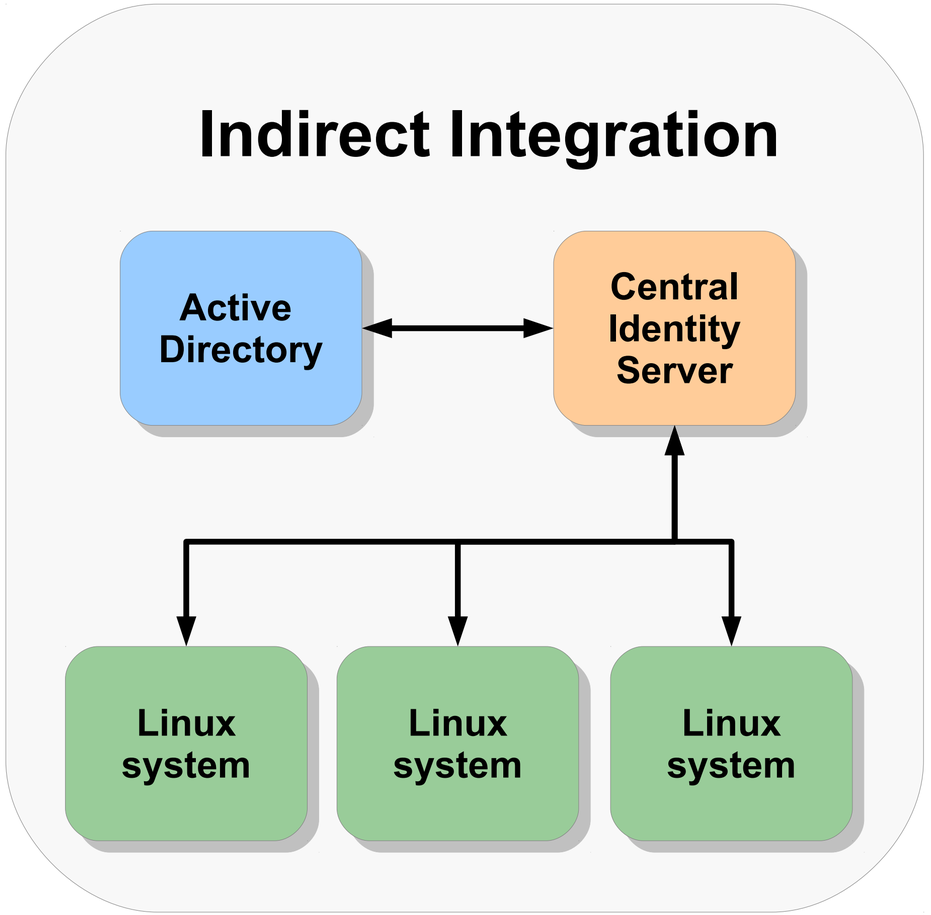
How to Integrate?

- 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

redhat.

Integration Options





redhat.

Direct Integration Solutions

- Native Linux:
  - Samba/Winbind
  - SSSD
  - Legacy (nss_ldap/pam_ldap/pam_krb5)
- 3rd Party:
  - Centrify
  - Quest (Dell)
  - Likewise (EMC)

redhat.

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

redhat.

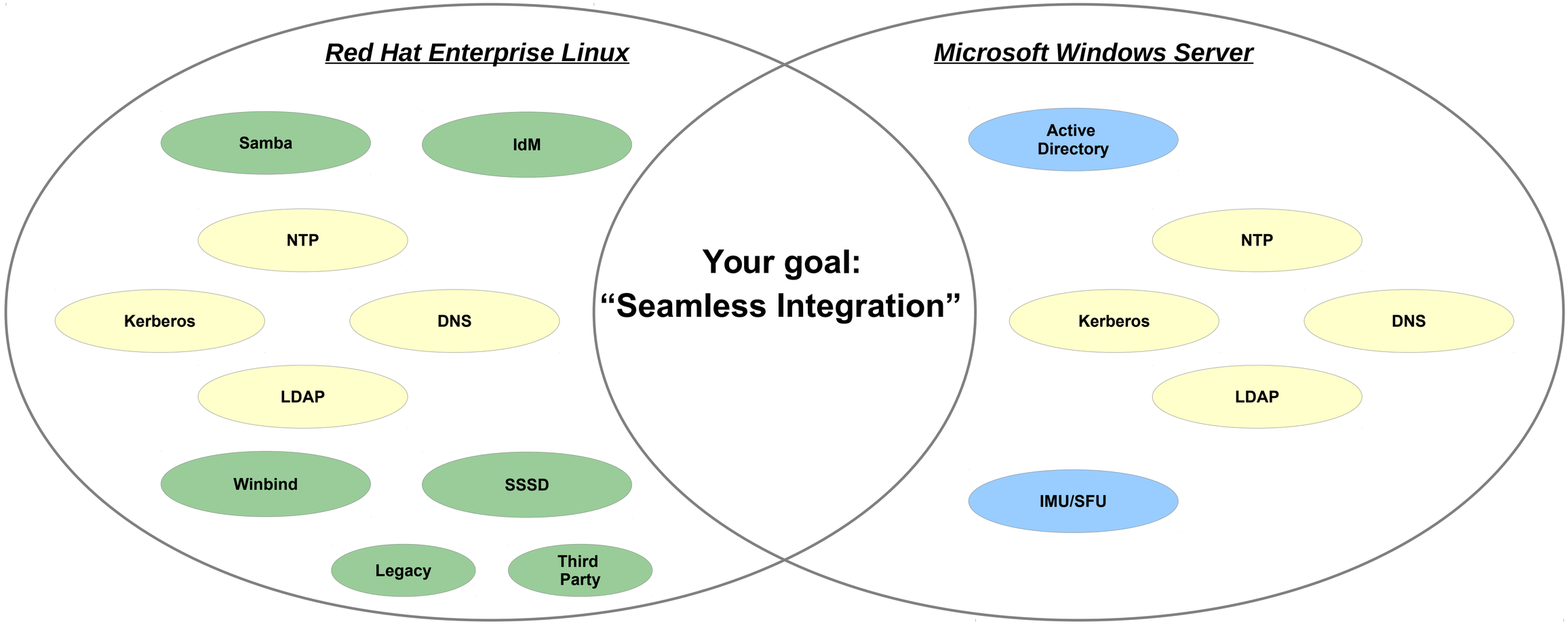
Building Blocks - Overview

- 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 **

redhat.

Integration Building Blocks



** Many options, considerations within each component **

redhat.

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) **

redhat.

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)

redhat.

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 **

redhat.

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 **

redhat.

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 **

redhat.

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 **

redhat.

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”

redhat.

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 **

redhat.

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

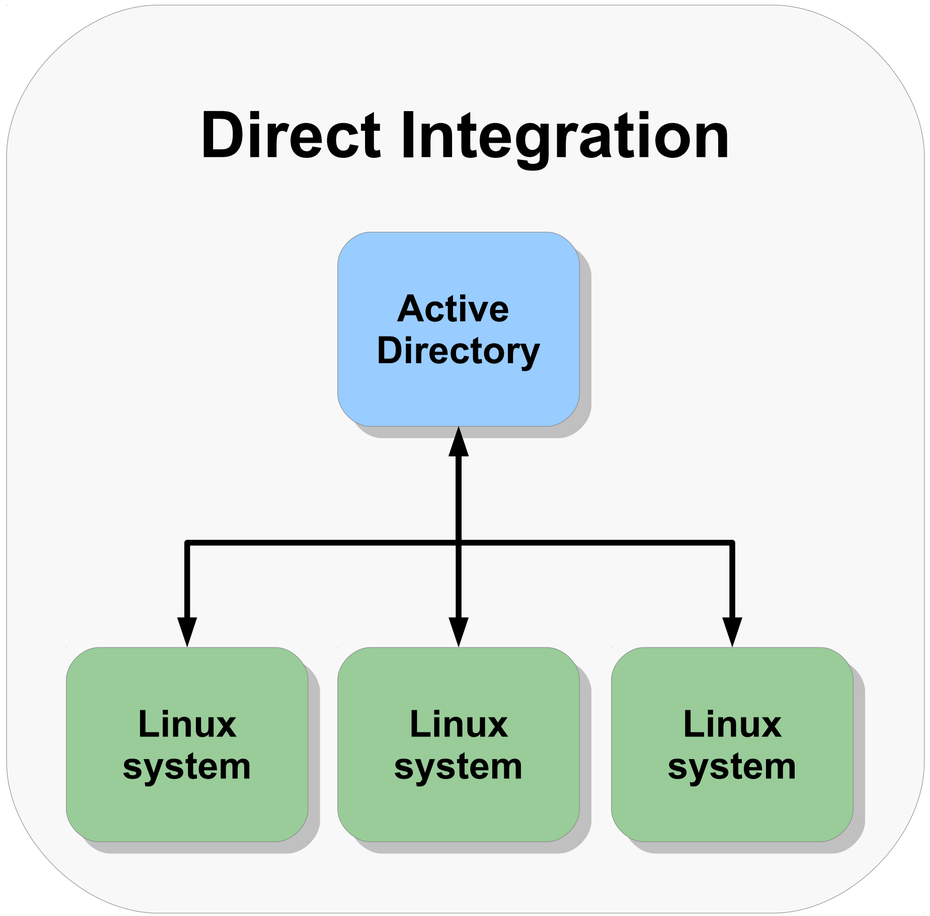
** Consider using more advanced solutions **

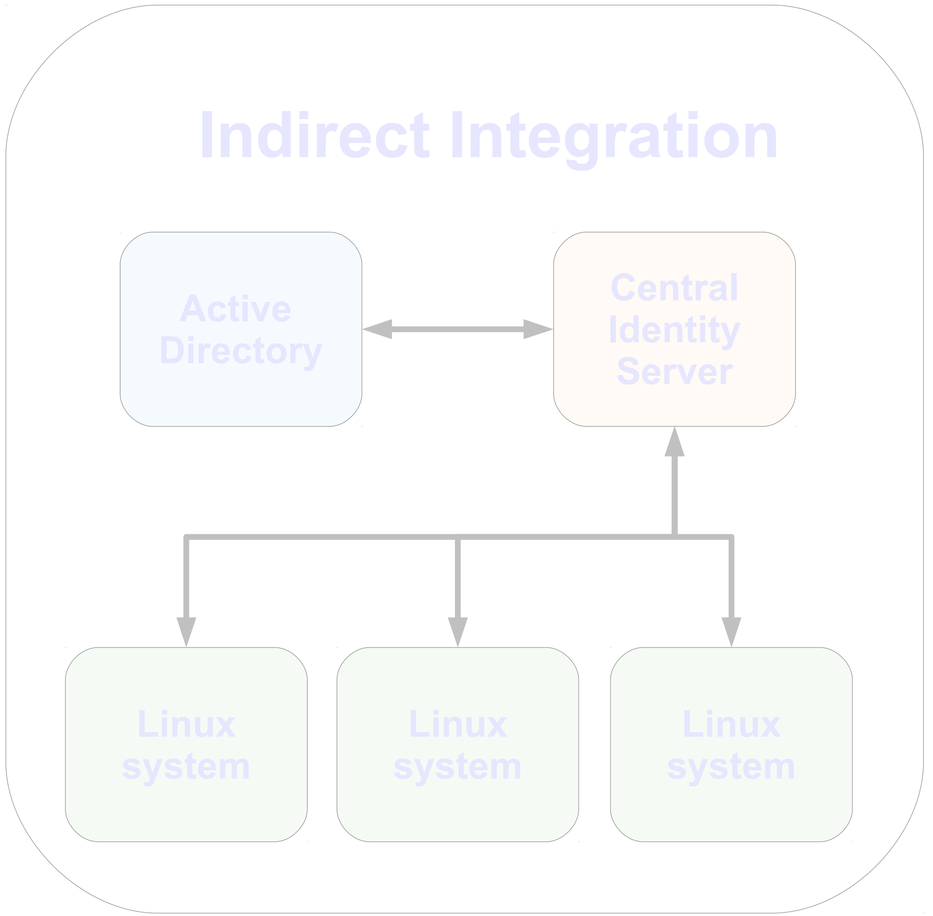
redhat.

Agenda

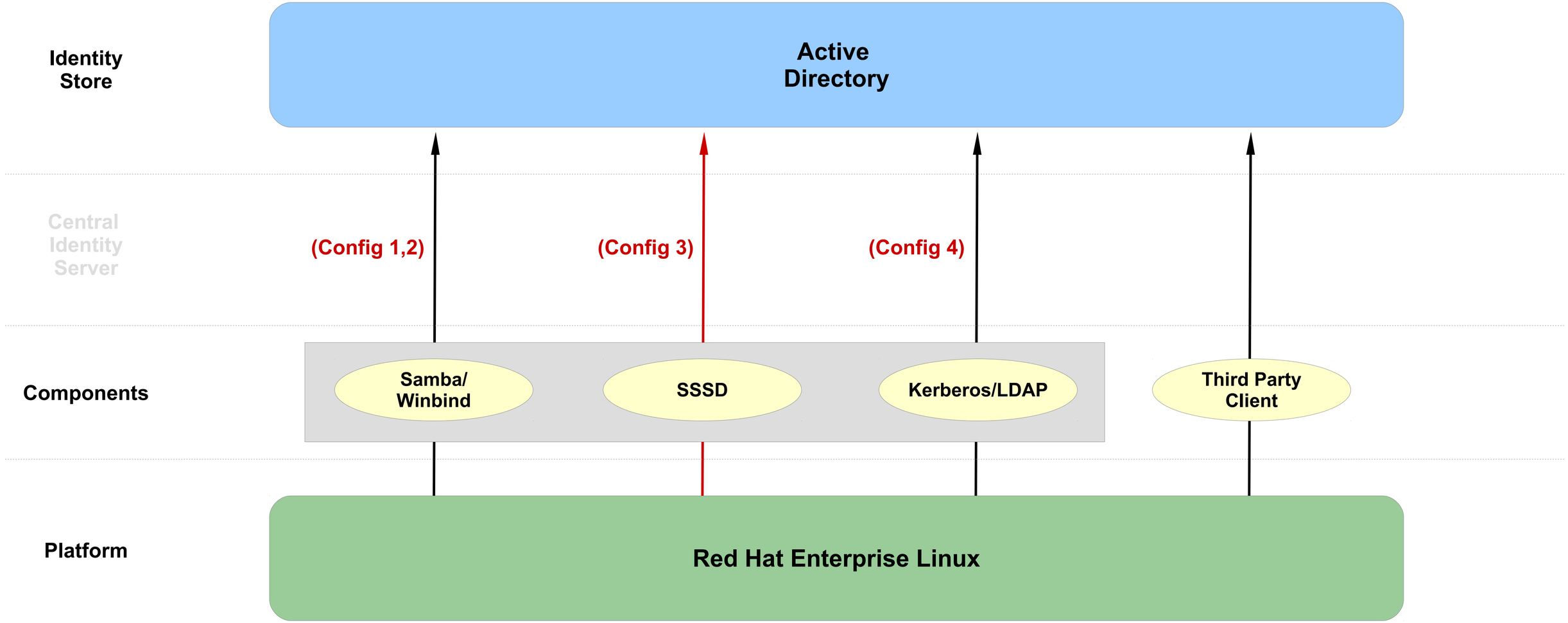
- Integration Overview
- Building Blocks
- *Integration Options - Red Hat Enterprise Linux 6*
- Integration Options - Red Hat Enterprise Linux 7
- Future Features
- Q&A
- Summary

Direct Integration Options in RHEL 6





Direct Integration – Red Hat Enterprise Linux 6



** Reference Architecture configurations – all components available today in Red Hat Enterprise Linux **

redhat.

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***

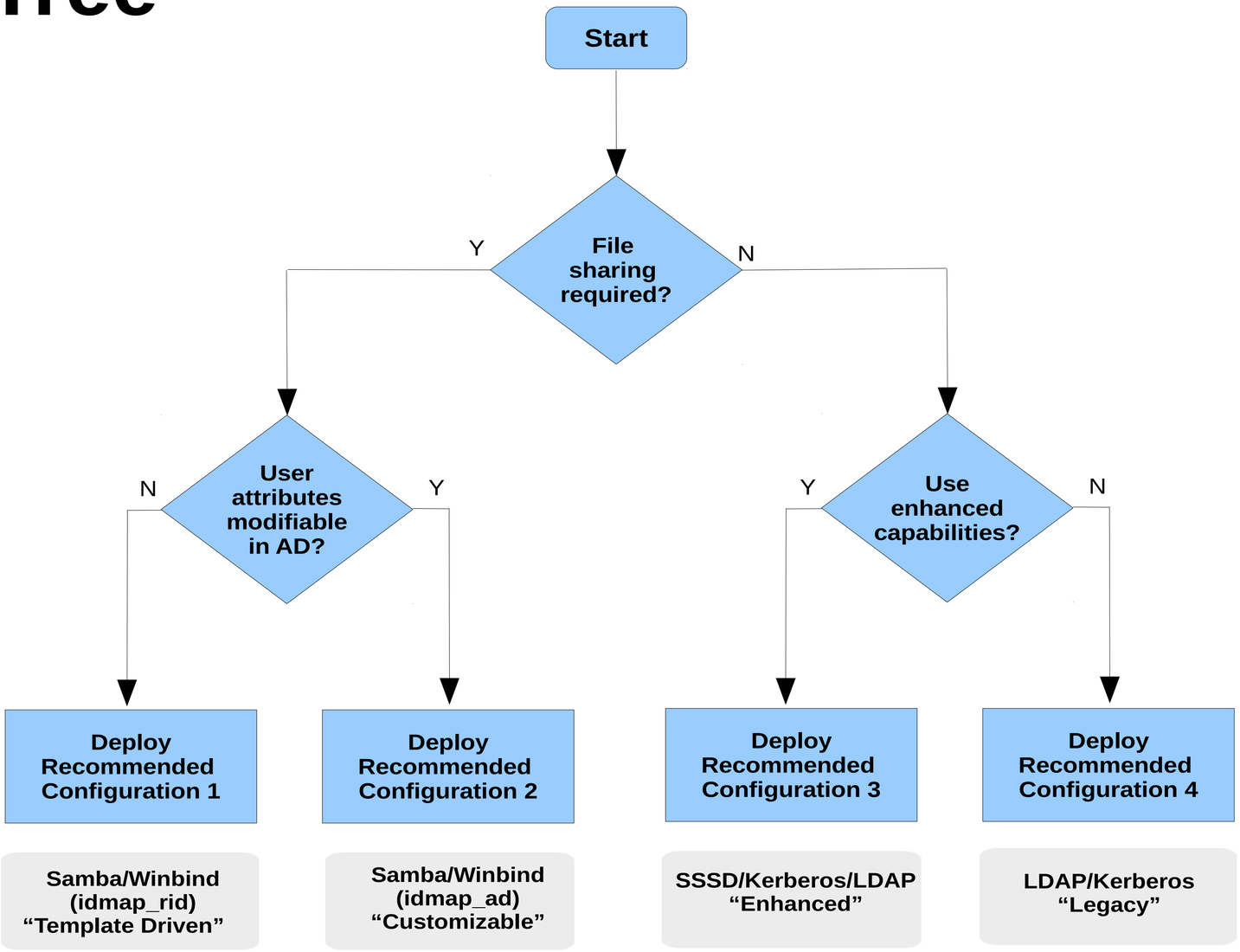
redhat.

Configuration Comparison

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

redhat.

Decision Tree



redhat.

Reference Architecture

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

https://www.redhat.com/resourcelibrary/reference-architectures/integrating-red-hat-enterprise-linux-6-with-active-directory

Red Hat Reference Architecture Series

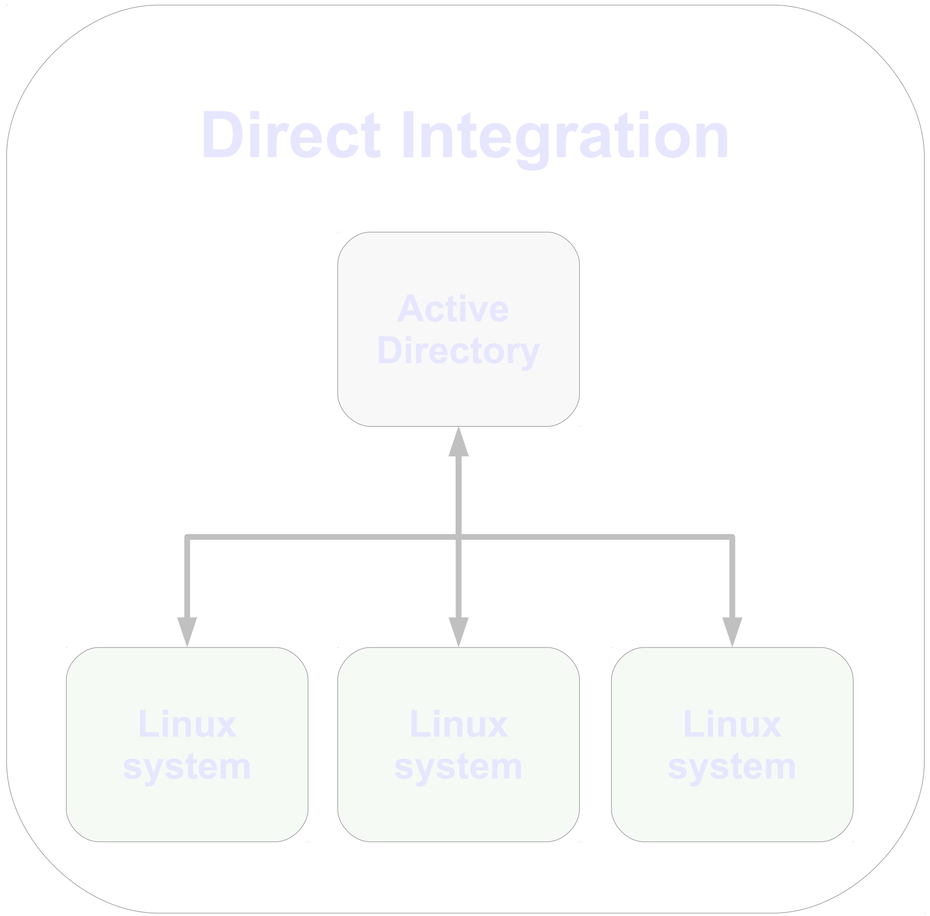
Integrating Red Hat Enterprise Linux 6 with Active Directory

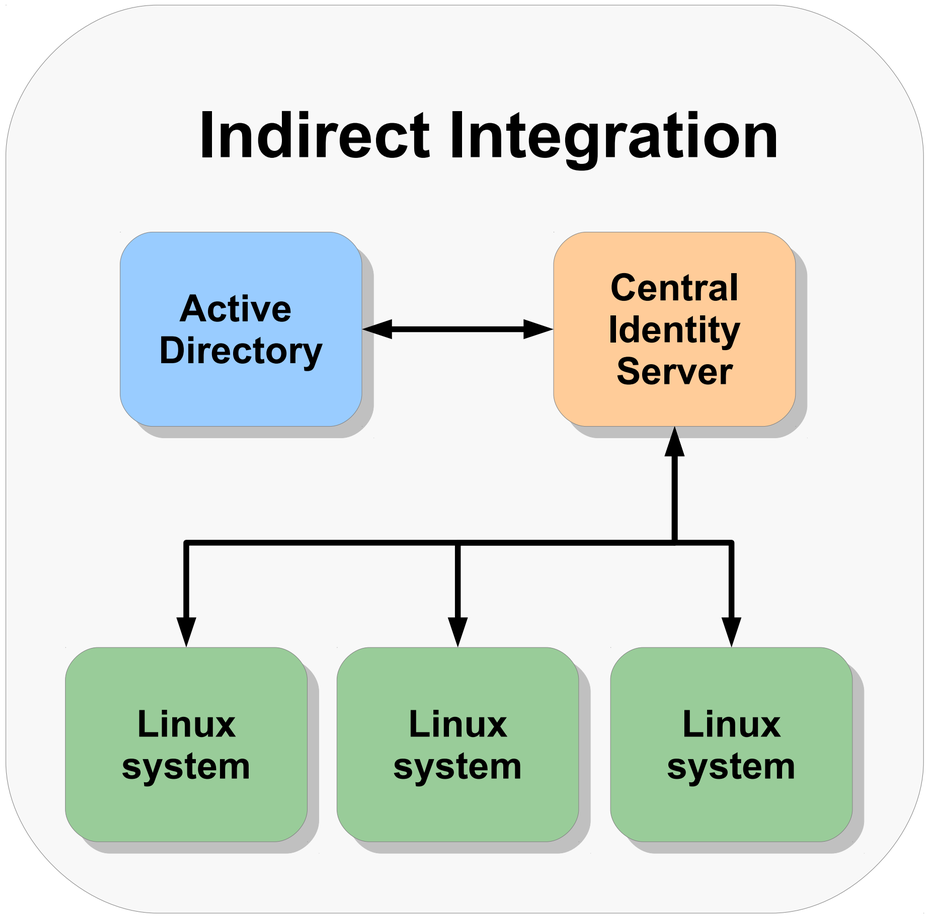
Mark Heslin
Principal Software Engineer

Version 1.5
March 2014

redhat.

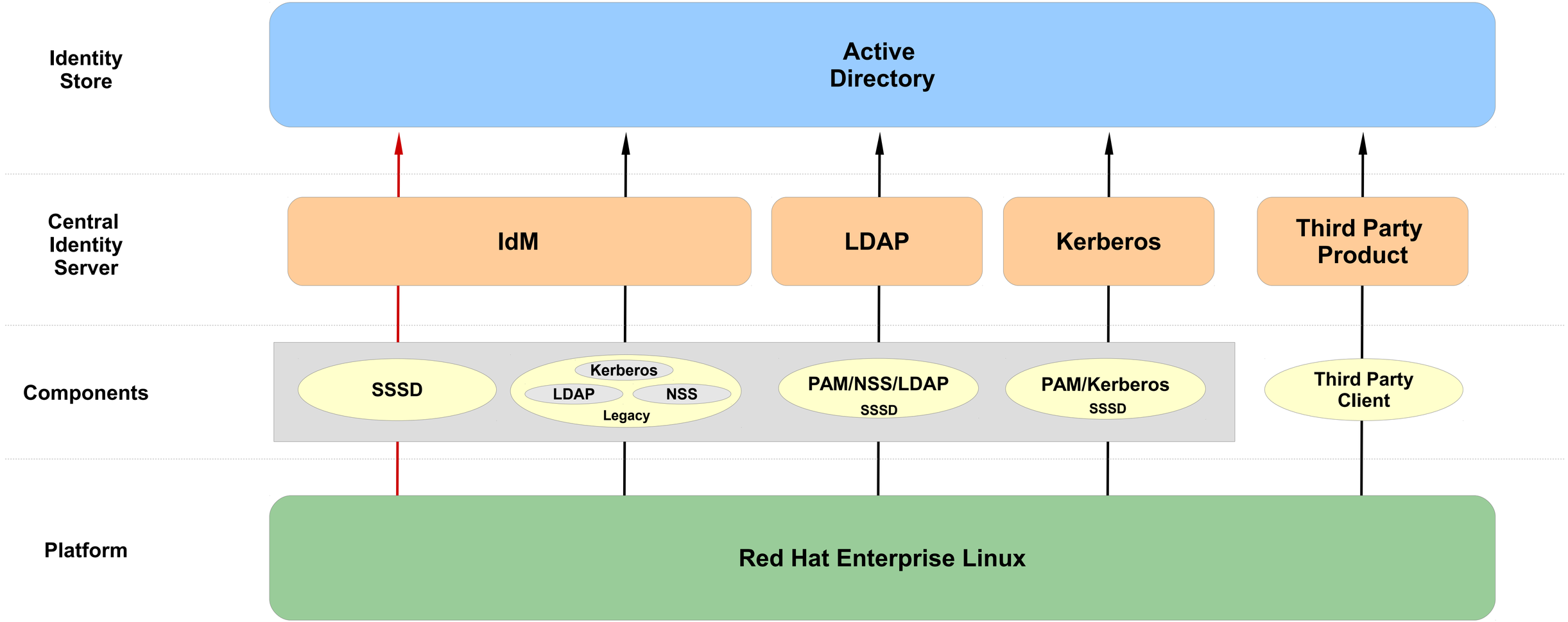
Indirect Integration Options in RHEL 6





redhat.

Indirect Integration – Red Hat Enterprise Linux 6



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

redhat.

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

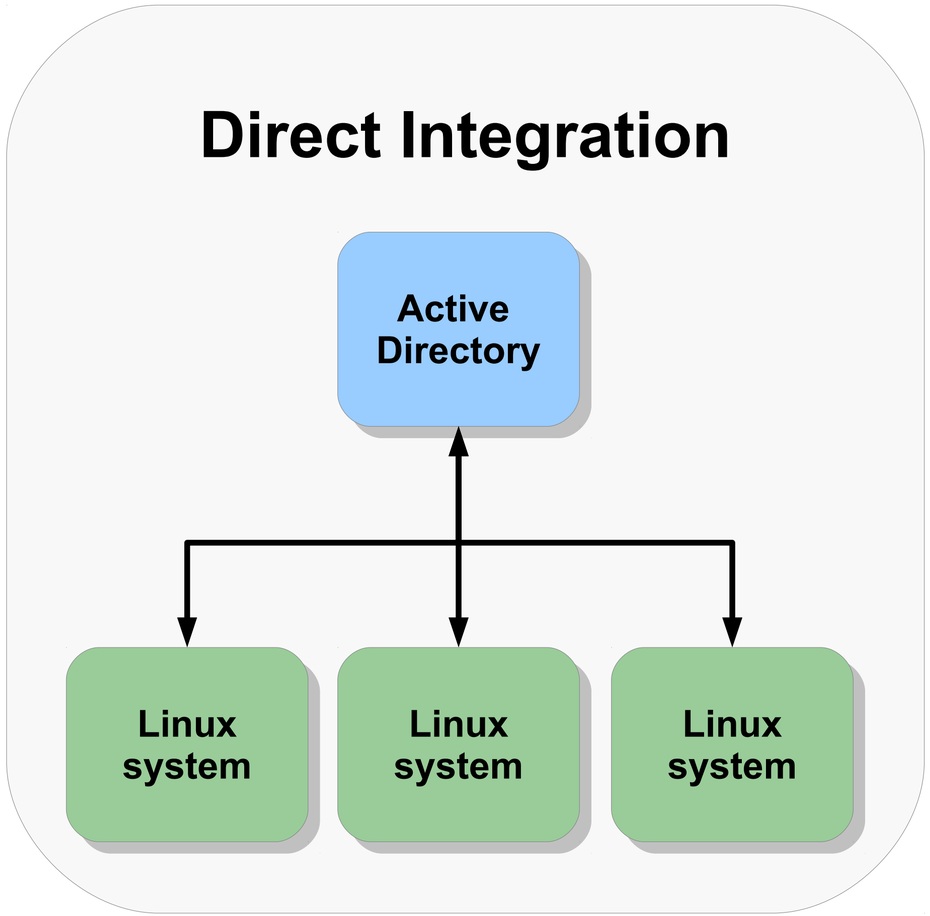
redhat.

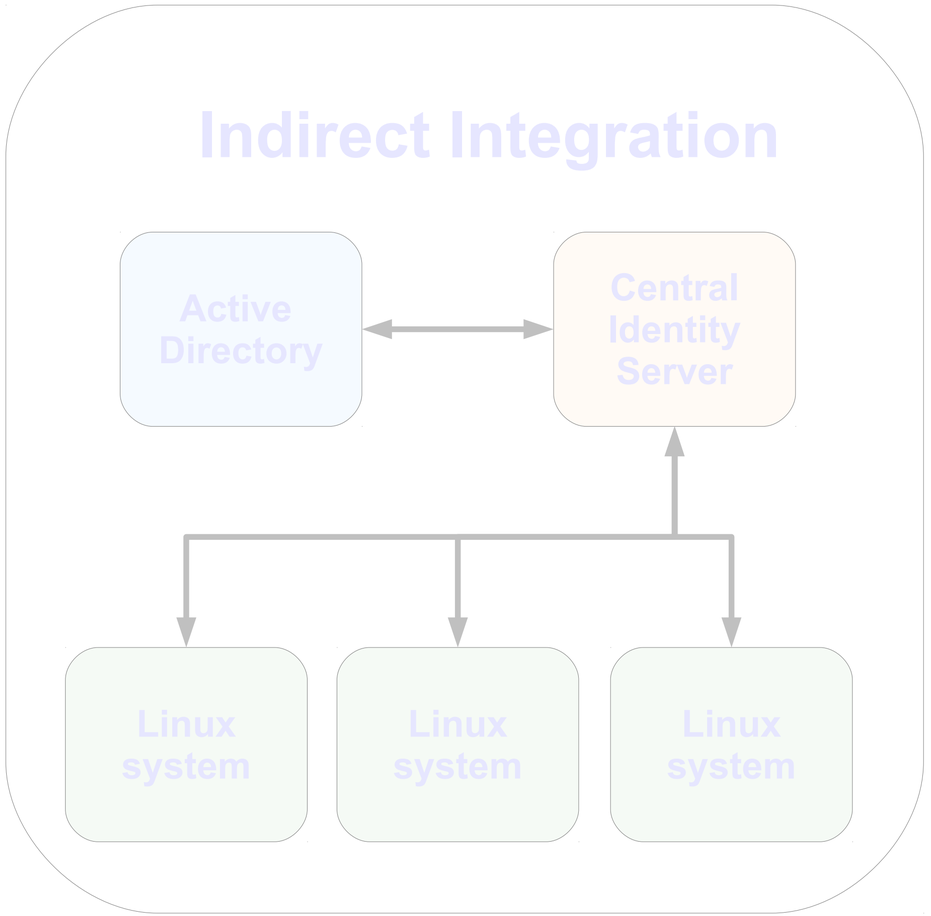
Agenda

- Integration Overview
- Building Blocks
- Integration Options - Red Hat Enterprise Linux 6
- *Integration Options - Red Hat Enterprise Linux 7*
- Future Features
- Q&A
- Summary

redhat.

Direct Integration Improvements in RHEL 7





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*

redhat.

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

redhat.

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`

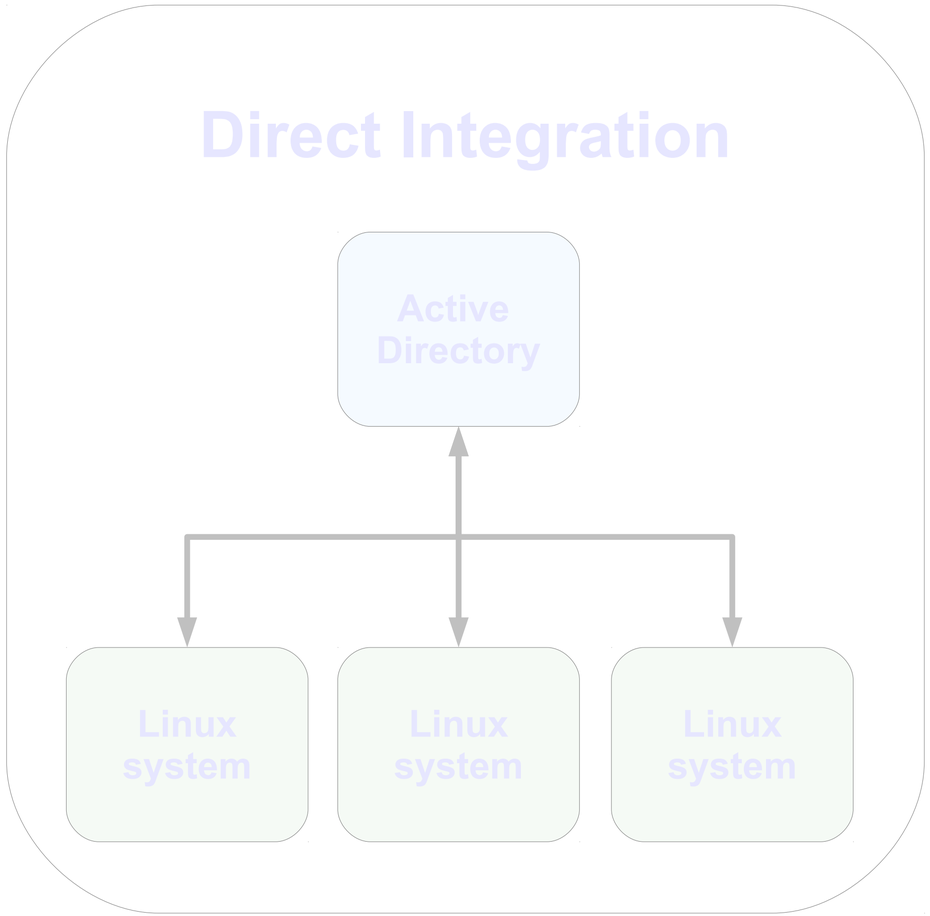
redhat.

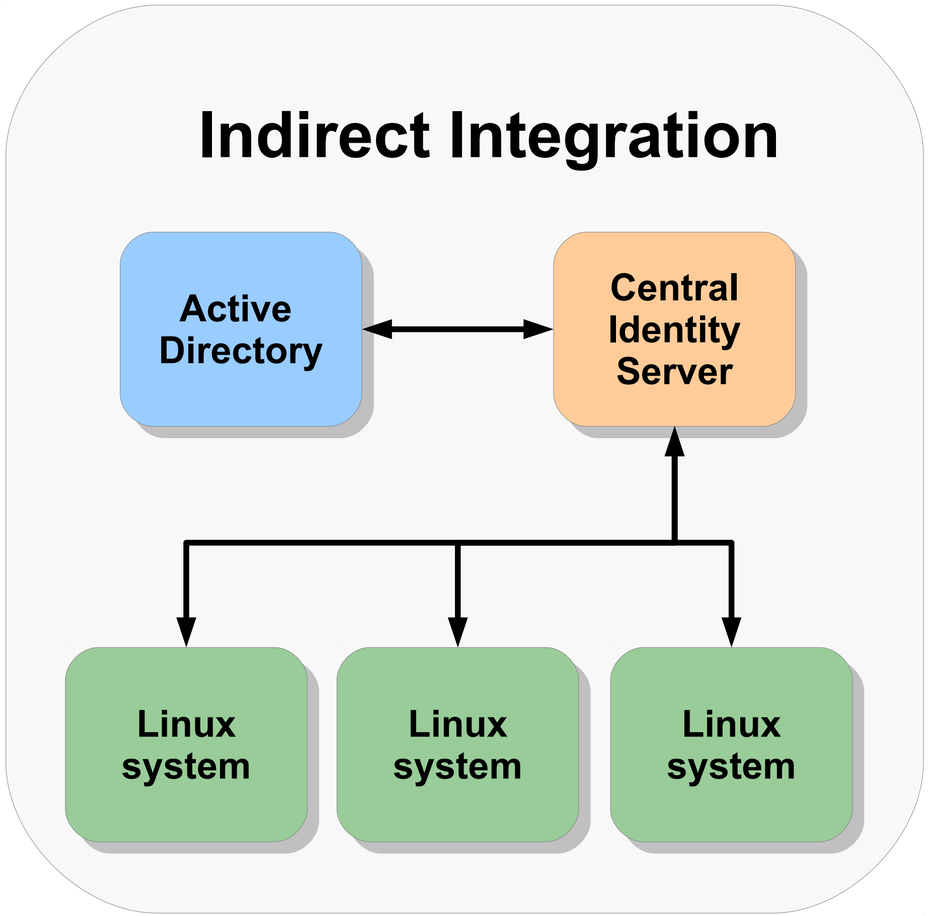
SSSD vs. Winbind in RHEL 7

Feature	SSSD with AD Provider	Winbind
Requires POSIX attributes	No (default)	No
Supports ID mapping	One method	Multiple methods
AD specific optimizations	Yes	Yes
CIFS integration	Not yet (available upstream)	Yes
DNS site support	Yes	Yes
DNS dynamic updates	Yes	Yes (requires manual configuration)
Enrollment with realmd	Yes (default)	Yes (must be explicitly selected)

redhat.

Indirect Integration Improvements in RHEL 7





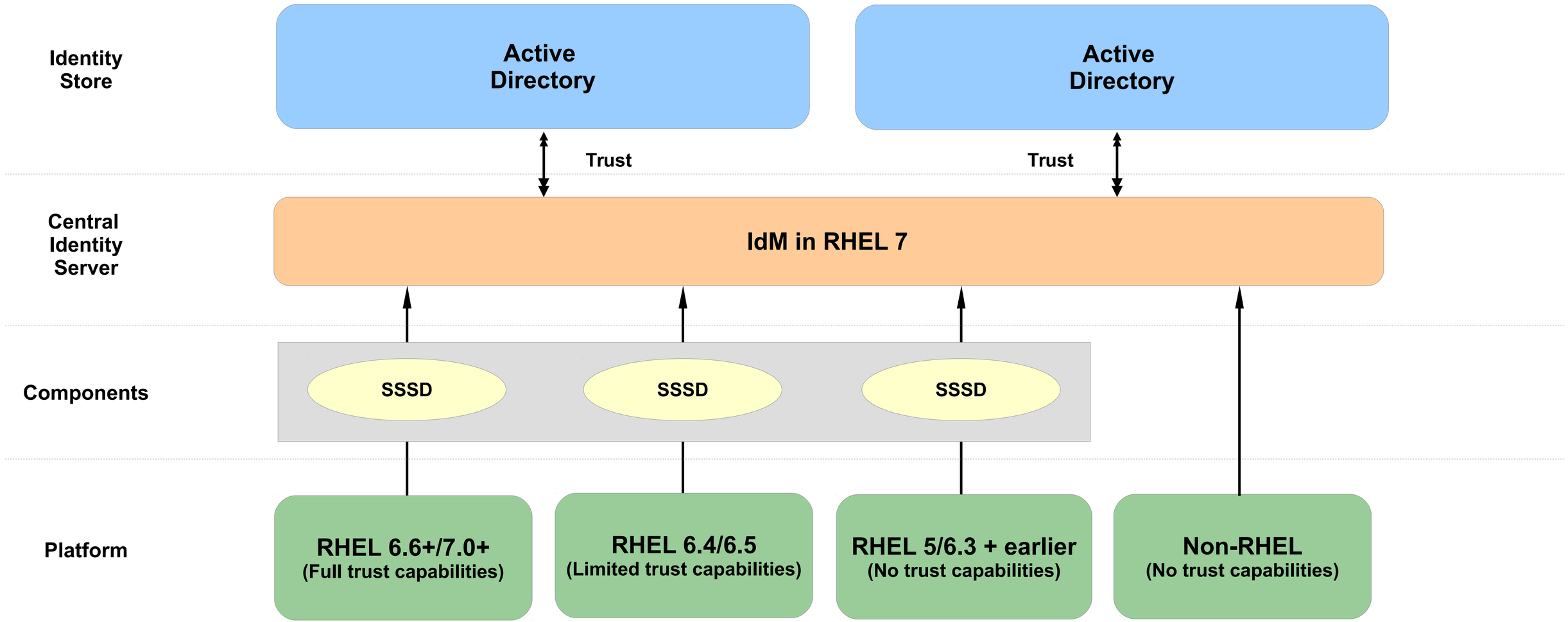
redhat.

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

redhat.

Cross-realm Deployment



redhat.

Client Support with Cross-realm Trusts

Feature/Client	Information look-up	Password auth	Kerberos auth	HBAC	SELinux user mapping	SUDO rules
RHEL 7 (main tree)	+	+	+	+	+	+
RHEL 6.5 (main tree)	+	+	+	+	+/-	+
RHEL 6.4 (main tree)	+	+	+	+	-	-
RHEL 6.3 (compat tree)	+	+	-	-	-	-
RHEL 5.10 (compat tree)	+	+	-	-	-	-

redhat.

Direct vs. Indirect Integration

Use Case	Direct Integration	Trust-based Integration
Number of Linux Clients	• Small, less than 30	• Large, 30 or more
Policy Management	• Requires separate solution	• Included with IdM in RHEL
Cost	• Grows with # of clients(CALs)	• Fixed at one connection • Feature set free in RHEL
Best Investment Profile	• Short-term	• Long-term

redhat.

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

redhat.

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

redhat.

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

redhat.

Thank you!

Please complete an evaluation form!

Supporting Slides

Detailed configuration examples

Configuration 1 (winbind – idmap_rid)

```
# 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
```

<--- Integration Best Practice:

** Set uid/gid defaults for troubleshooting purposes **

redhat.

Configuration 1 - alternative (winbind – idmap_autorid)

- 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
```


redhat.

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                    <--- Integration Best Practice:
     idmap gid = 20000-29999                      * Set uid/gid defaults for troubleshooting purposes *
     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
```


redhat.

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
```


redhat.

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
```


redhat.

Configuration 4 (Kerberos/LDAP) – continued

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

Before

```
auth      sufficient    pam_sss.so use_first_pass
account   [default=bad success=ok user_unknown=ignore] pam_sss.so
password  sufficient    pam_sss.so use_authtok
session   optional      pam_sss.so
```

After

```
auth       sufficient    pam_krb5.so use_first_pass
account    [default=bad success=ok user_unknown=ignore] pam_krb5.so
password   sufficient    pam_krb5.so use_authtok
session    optional      pam_krb5.so
```


redhat.