RED HAT ENTERPRISE LINUX: ACTIVE DIRECTORY - CLIENT INTEGRATION OPTIONS

TECHNOLOGY BRIEF

INTRODUCTION

For many organizations, Microsoft Active Directory is the hub for user identity management. Typically, all system user accounts, including those from Linux systems are stored in Active Directory. In these environments, Linux systems require access to Active Directory to perform authentication and identity lookups. This Technology Brief provides an overview on the options available for integrating Red Hat Enterprise Linux clients with Active Directory.

APPROACHES

At the broadest level, there are two approaches to Active Directory integration:

1. **Direct Integration** - Red Hat Enterprise Linux systems are joined directly into an Active Directory domain as shown in *Figure 1* below.

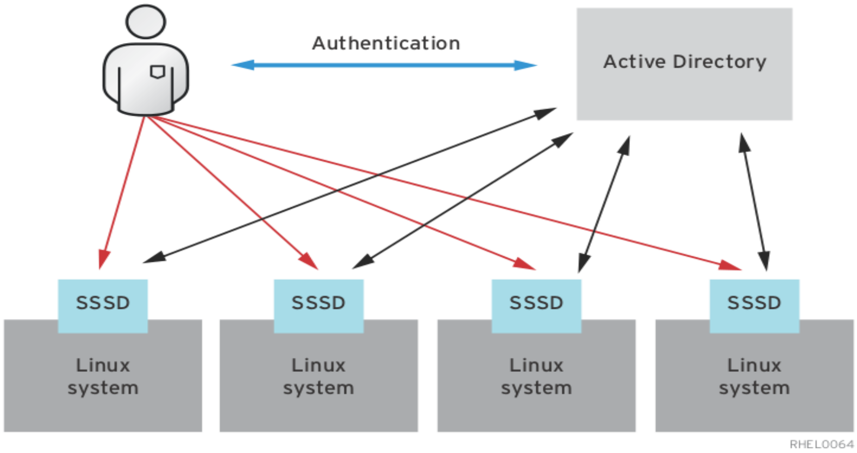

Figure 1: Linux system integration with Active Directory.

Direct integration is limited in that it only provides the authentication and identity information related to users. Host systems do not get policies and data, thereby limiting their identity and access control potential.

2. Indirect Integration - Red Hat Enterprise Linux systems are joined indirectly into an Active Directory domain through the use of an interim server that has a trusted relationship to an Active Directory server.

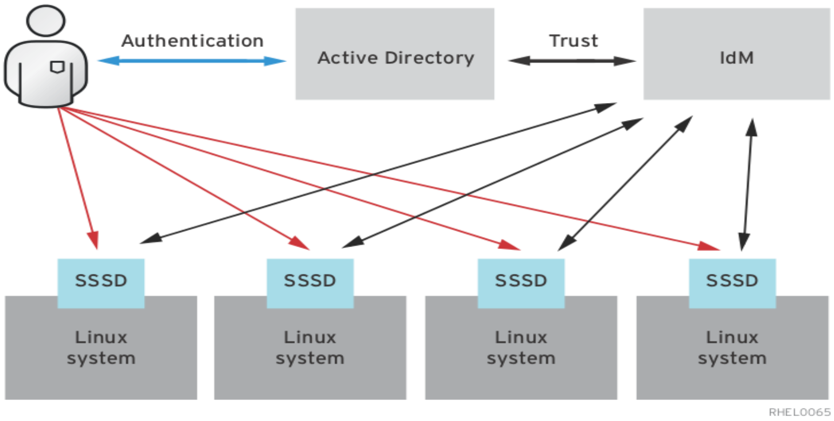

Figure 2: Cross-realm trust between Active Directory and Red Hat Enterprise Linux identity management

Figure 2 above shows how Identity Management (IdM) in Red Hat Enterprise Linux provides this access to IdM clients through the use of cross-realm Kerberos trusts. Red Hat Enterprise Linux systems that are members of an IdM domain, can access policies like SUDO rules, Host-based access control (HBAC), automount, netgroups, SELinux user mappings, and other capabilities from a central identity management server. The identity management server provides centralized management of Linux systems giving them identity and credential services.

Indirect integration is constrained only by the limitations of the client software and is discussed further in subsequent sections.

INTEGRATION COMPONENTS AND TOOLS

Client Utilities

ipa-client-install

The ***ipa-client-install*** utility provides a clean, simple command line interface that streamlines the configuration of Red Hat Enterprise Linux hosts as members of an IdM domain.

- *ipa-client-install* is supported on all versions of Red Hat Enterprise Linux starting with version 5.7
- *ipa-client-install* facilitates indirect integration of IdM clients to Active Directory domains when used in a cross-realm Kerberos trust configuration.

realmd

Red Hat Enterprise Linux 7.0 introduced a new tool called ***realmd*** that simplifies the configuration of clients. ***realmd*** is a front-end configurator for SSSD that uses DNS to detect central identity servers such as Active Directory, IdM or MIT Kerberos.

- *realmd* is supported on all versions of Red Hat Enterprise Linux starting with version 7.0
- *realmd* can be used for both direct and indirect Active Directory integration

- When an IdM server is detected, *realmd* calls *ipa-client-install*
- *realmd* is the *preferred* tool to use for clients running Red Hat Enterprise Linux 7 or higher

While it is possible to manually edit client systems, it is not recommended as extensive knowledge is required of the underlying configuration files, communication protocols and services on the IdM server and client.

Server Utilities

Compatibility Mode

In order to support earlier Red Hat Enterprise Linux clients, Identity Management in Red Hat Enterprise Linux 7 introduced a server-side feature called *compatibility mode*. Compatibility mode permits IdM clients running earlier versions of Red Hat Enterprise Linux (*i.e. - v6.4 or earlier*) to leverage a cross-realm Kerberos trust to Active Directory.

- Compatibility mode can be enabled at any time on a Red Hat Enterprise Linux 7 Identity Management server by running ***ipa-adtrust --enable-compat***

ipa-advise

Introduced in Red Hat Enterprise Linux 7, ***ipa-advise*** is a server tool that simplifies the configuration of earlier clients. When run on a Red Hat Enterprise Linux 7 Identity Management server, ***ipa-advise*** produces output that is then copied into a terminal session or file, and run on the IdM client.

- The *ipa-advise* utility is supported on Identity Management in Red Hat Enterprise Linux servers starting with version 7.0. The generated output supports all client versions, but is primarily designed to be run on clients running Red Hat Enterprise Linux versions 4, 5 and 6.0-6.4.
- For earlier Red Hat Enterprise Linux clients (*i.e.- v6.4 or earlier*) using Active Directory accounts across a cross-realm Kerberos trust, *compatibility mode* must also be enabled on the Identity Management server.

DIRECT INTEGRATION

Client Options

When *direct integration* is used to integrate Red Hat Enterprise Linux clients to Active Directory, the following options are available:

Legacy

The ***Legacy*** option connects client systems to Active Directory using NSS, PAM, LDAP or Kerberos modules. This option provides basic user authentication and identity lookup, but is limited in terms of the user features, performance and security capabilities available in other client options.

- The *Legacy* option is supported on all versions of Red Hat Enterprise Linux

Traditional

The ***Traditiona***l option is based on Samba/Winbind. Samba supports CIFS file sharing capabilities, and Winbind provides user lookup and identity mapping. This option takes advantage of native Windows and LDAP protocols, and also works with Active Directory trusts between domains and forests.

The primary limitation of the traditional option is the lack of centralized policy management. In addition, the only identity provider currently supported by Samba/Winbind is Active Directory.

- The *Traditional* option is supported on all versions of Red Hat Enterprise Linux

Third-party

A number of ***Third-party*** solutions based on commercial software are available. Most are well-established, mature products that provide the same capabilities as the traditional option but with additional features such as centralized management of policies, user privileges and host-based access control (HBAC) through a modern management console.

Third-party solutions are attractive to organizations interested in non-native Linux and/or cross-platform solutions. However, for cost-conscious organizations, the ***Modern*** integration option (*below*) presents a viable alternative that is native to the underlying Linux operating system.

- The *Third-party* option is vendor dependent and support may vary across versions of Red Hat Enterprise Linux

Modern

The ***Modern*** integration option is based on the **System Security Services Daemon (SSSD)**. SSSD is included on all Red Hat Enterprise Linux hosts starting with version 5.6. SSSD consists of a set of services that provide user authentication, identity lookup and access control capabilities. SSSD supports off-line caching of user credentials and reduces loading on identity servers.

- The *Modern* option is supported on all versions of Red Hat Enterprise Linux starting with version 5.7
- Starting with Red Hat Enterprise Linux v7.1, SSSD also supports CIFS file sharing, allowing Red Hat Enterprise Linux systems to be both a CIFS client and a CIFS file server.

Regardless of which option is selected, the ***Modern*** option is *preferred* for directly integrating Red Hat Enterprise Linux clients running v7.0 or higher with Active Directory.

Client Configuration

Table 1 - Direct Integration - Client Configuration provides a summary of the steps required when configuring Red Hat Enterprise Linux hosts as Active Directory clients using *direct* integration.

	Red Hat Enterprise Linux Client Version	**Client Configuration**
Legacy	All versions	http://www.redhat.com/en/resources/integrating-red-hat-enterprise-linux-6-active-directory (Configuration 4)
Traditional	All versions	http://www.redhat.com/en/resources/integrating-red-hat-enterprise-linux-6-active-directory (Configurations 1, 2)
Third-party	Vendor dependent	See vendor documentation
Modern	v7.0 or higher	run ***realm discover*** then ***realm join***
	v5.7 - v6.x	http://www.redhat.com/en/resources/integrating-red-hat-enterprise-linux-6-active-directory (Configuration 3)

Table 1: Direct Integration - Client Configuration

INDIRECT INTEGRATION

Client Options

When *indirect integration* is used to integrate Red Hat Enterprise Linux clients into Active Directory, the following options are available:

NSS-PAM-LDAP

The ***NSS-PAM-LDAP*** option connects clients to the Identity Management server using a combination of NSS and/or PAM and LDAP.

- The *NSS-PAM-LDAP* option is *recommended* for Red Hat Enterprise Linux clients running v5.5 or earlier
- This option requires the *compatibility tree* to be enabled on the Red Hat Enterprise Linux 7 Identity Management server

SSSD/LDAP

The ***SSSD/LDAP*** option connects clients to the Identity Management server using a combination of SSSD and LDAP.

- The *SSSD/LDAP* option is *recommended* for Red Hat Enterprise Linux clients running v5.6 through v6.4
- This option requires the *compatibility tree* to be enabled on the Red Hat Enterprise Linux 7 Identity Management server

SSSD/Kerberos

The ***SSSD/Kerberos*** option combines the benefits and features of SSSD with the proven security of Kerberos single sign-on (SSO).

- The *SSSD/Kerberos* option is *preferred* for Red Hat Enterprise Linux clients running v6.5 or higher
- This option is configured by default when either ***realmd*** or ***ipa-client-install*** are run

Client Configuration

Table 2 - Indirect Integration - Client Configuration provides a summary of the steps required when configuring Red Hat Enterprise Linux hosts as Active Directory clients using *indirect* integration.

	Red Hat Enterprise Linux Client Version	**Client Configuration**
NSS-PAM-LDAP	v5.5 or earlier	run ***ipa-advise config-redhat-nss-pam-ldap*** on IdM server; copy output then paste/run on IdM client
SSSD/LDAP	v5.6-6.4	run ***ipa-advise config-redhat-sssd-before-1-9*** on IdM server; copy output then paste/run on IdM client
SSSD/Kerberos	v7.0 or higher	run ***realm discover*** then ***realm join*** (preferred) or run ***ipa-client-install***
	v6.5 or higher	run ***ipa-client-install***

Table 2: Indirect Integration - Client Configuration

Client Trust Capabilities

Table 3: Indirect Integration - Client Trust Features provides a summary of the features available to IdM clients for versions of Red Hat Enterprise Linux.

	Red Hat Enterprise Linux Client Version	**Client Configuration**
NSS-PAM-LDAP	v5.5 or earlier	**Limited Capabilities** - ID lookup - Password authentication
SSSD/LDAP	v5.6-6.4	**Limited Capabilities** - ID lookup - Password authentication
SSSD/Kerberos	v7.0 or higher	**Full Capabilities** - ID lookup - Password authentication - Kerberos single sign-on (SSO) - Host-based access control (HBAC) - SELinux user maps - SUDO rules
	v6.5 or higher	

Table 3: Indirect Integration - Client Trust Features

ADDITIONAL NOTES

Fedora Clients

Fedora clients follow the same configuration guidelines as Red Hat Enterprise Linux hosts. Consult the Fedora (*fedoraproject.org*), SSSD (fedorahosted.*org/sssd*) and FreeIPA (*freeipa.org*) websites for further details.

Non-Red Hat Enterprise Linux clients

Non-Red Hat Enterprise Linux clients (*Solaris*, *AIX*, *HP-UX*, *OS X* and *MS Windows*) are restricted to the native protocols and services provided by the vendor to connect to a central LDAP server such as Identity Management in Red Hat Enterprise Linux (IdM) or Active Directory. These clients are normally configured using a combination of NSS, PAM, LDAP or Kerberos. Consult the vendor documentation for further details.

CONCLUSION

Numerous options exist for integrating Red Hat Enterprise Linux clients with Microsoft Active Directory. Understanding the approaches, components, tools and capabilities of each option is fundamental to successfully integrating clients. The concepts, guidelines presented here, provide an overview to simplify and assist in the decision making process.

REFERENCES

Red Hat Enterprise Linux

www.redhat.com

Identity Management (IdM) in Red Hat Enterprise Linux

https://access.redhat.com/documentation/en-US/
Red_Hat_Enterprise_Linux/7/html/
Linux_Domain_Identity_Authentication_and_Policy_Guide/index.html

Windows Integration Guide

https://access.redhat.com/site/documentation/en-US/
Red_Hat_Enterprise_Linux/7/html/
Windows_Integration_Guide/index.html

FreeIPA

https://www.freeipa.org

SSSD

https://fedorahosted.org/sssd/

Red Hat Reference Architectures

http://www.redhat.com/en/resources
https://access.redhat.com/search/#/knowledgebase

ABOUT RED HAT

Red Hat is the world's leading provider of open source solutions, using a community-powered approach to provide reliable and high-performing cloud, virtualization, storage, Linux, and middleware technologies. Red Hat also offers award-winning support, training, and consulting services. Red Hat is an S&P company with more than 80 offices spanning the globe, empowering its customers' businesses.

NORTH AMERICA
1–888–REDHAT1
www.redhat.com

EUROPE,
MIDDLE EAST,
AND AFRICA
00800 7334 2835
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
info-latam@redhat.com