RED HAT® ENTERPRISE LINUX®

redhat.

RED HAT ENTERPRISE LINUX: IDENTITY MANAGEMENT

TECHNOLOGY BRIEF

INTRODUCTION

Today's application environments are large, dynamic, and often virtualized. Systems can be spun up and shut down in a matter of seconds, so centralized identity management becomes essential to securing the environment. Local user accounts and per-machine policies do not scale to meet today's needs.

Red Hat® Enterprise Linux® gives customers a centralized way to manage identities and define access-control policies for users, machines, and services within large Linux and UNIX enterprise environments. In addition, identity management features simplify maintenance of multiple domains by supporting interoperability with Microsoft Active Directory.

Identity management (IdM) in Red Hat Enterprise Linux presents a unifying umbrella for standards-defined, common network services, including LDAP, Kerberos, DNS, NTP, and certificate services. This allows any Red Hat Enterprise Linux system to serve as a domain controller in a Linux environment. Domain controllers can deliver enterprise-level single-sign-on, certificate management, DNS integration, and command-line and web user interfaces (UI) for managing enterprise identities, certificates, and keys.

CENTRALIZED IDENTITY MANAGEMENT

To address the challenges of managing identities in Linux or in a mixed Linux and Windows environment, Red Hat Enterprise Linux:

- Supports increasing numbers of systems in the datacenter.
- Delivers native Linux interfaces and objects expected by Linux systems.
- Provides more advanced capabilities than LDAP, including host-based access control, control over privilege elevation, and certificate management.
- Enables Windows and Linux infrastructures to coexist for identity management.
- Allows Linux and Windows administrators a clear separation of duties within the IT organization.
- Integrates easily with an organization's life cycle management, provisioning tools, and workflow choices.
- Reduces the need for costly third-party integration software.

ACTIVE DIRECTORY INTEROPERABILITY

For many organizations, Microsoft Active Directory is the hub for user identity management. It is often the case that all system user accounts, including those from Linux systems, are stored in Active Directory. Therefore, Linux systems need access to Active Directory to perform authentication and identity lookups. Red Hat Enterprise Linux 7 beta offers two paths to Active Directory access:

1. Direct integration when Red Hat Enterprise Linux systems are joined directly into an Active Directory domain.
2. Indirect access through cross-realm Kerberos trusts between IdM in Red Hat Enterprise Linux and an Active Directory forest.

FEATURES AND CAPABILITIES

DIRECT INTEGRATION

If the number of Linux clients in the environment is small, and the cost and time consumed managing these clients individually is not an issue, using direct integration of the clients is an option. Linux systems can be connected to Active Directory directly by configuring a system security services daemon (SSSD), as shown in Figure 1. SSSD acts as an identity and authentication gateway into a central identity store. SSSD can be easily configured using a component called realmd. Realmd detects an available domain based on the DNS records and configures SSSD to interact with the right identity source. Realmd can connect Linux systems to either IdM or Active Directory as shown below. Once the system is joined into the domain, users managed by this domain can access the joined systems. They are authenticated, and their POSIX attributes, as well as group membership, is recognized by the Linux system.

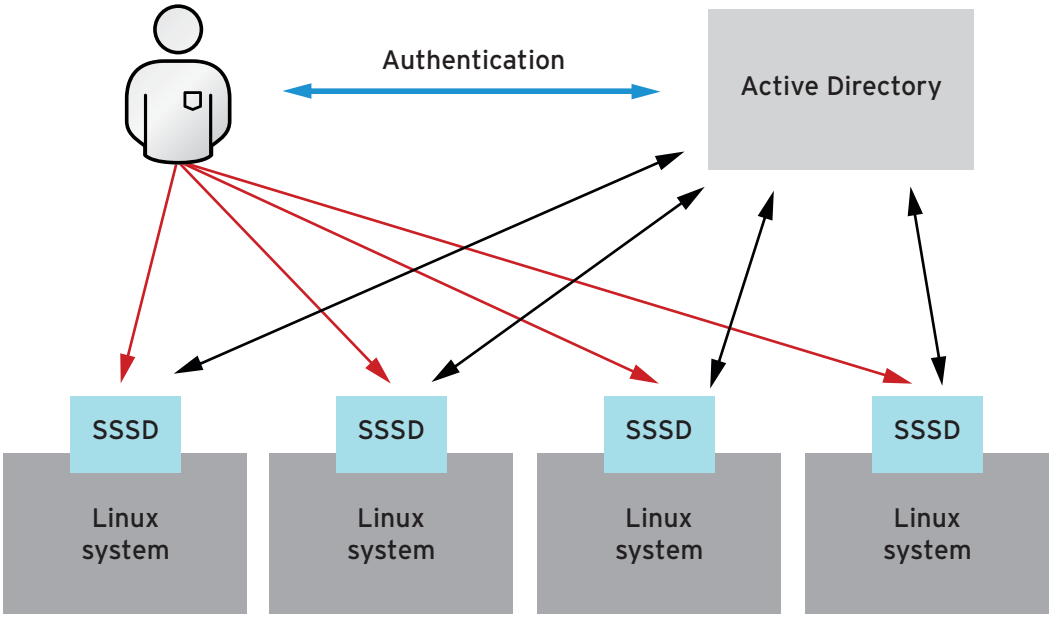


Figure 1: Linux system integration with Active Directory.

CROSS-REALM TRUST-BASED INTEGRATION

Direct integration is limited, only using the authentication and identity information related to users. Systems do not get policies and data, which limits their identity and access control potential. Linux systems can get policies like SUDO, host-based access control rules, 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 credentials services In most environments, identities that are stored and authenticated by Active Directory also need to have access to Linux resources. That can be accomplished by establishing a trust relationship between the identity management server and Active Directory. Figure 2 shows how users from an Active Directory forest gain access to the Linux systems joined into the identity management domain.

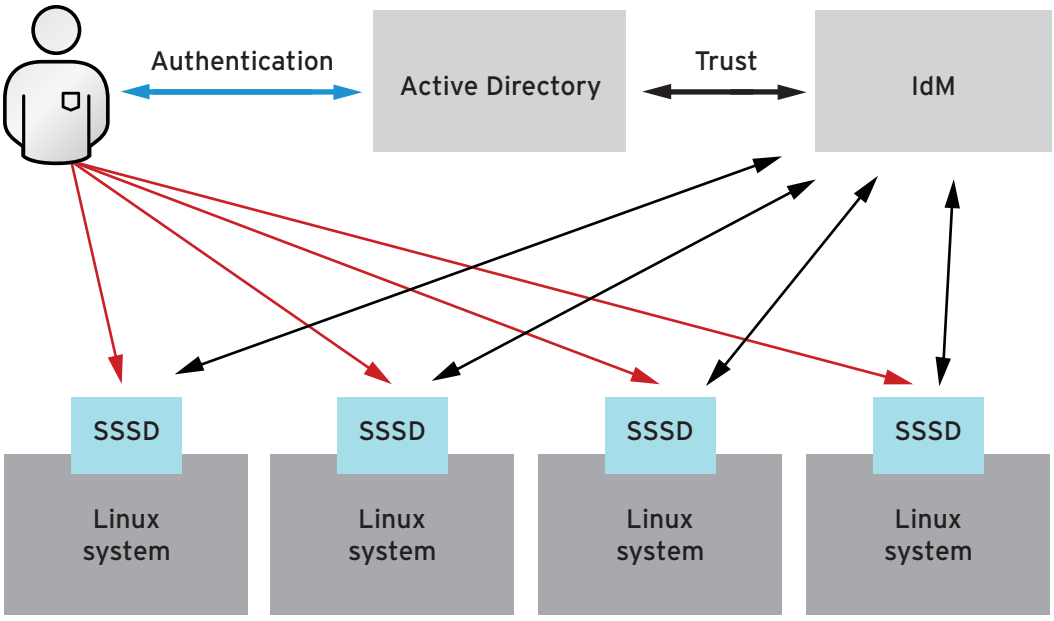


Figure 2: Cross-realm trust between Active Directory and Red Hat Enterprise Linux identity management

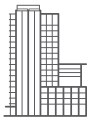
TABLE 1:
CHOOSING BETWEEN DIRECT OR TRUST-BASED INTEGRATION

USE CASE	DIRECT INTEGRATION	TRUST-BASED INTEGRATION
Number of Linux clients	Small, less than 30	Large, 30 or more
Policy management	No Red Hat solution out-of-the-box	Included in identity management features
Cost	Grows as number of clients grows	Fixed at one connection, Features free in Red Hat Enterprise Linux
Best investment profile	Short term	Long term
Integrated with Red Hat product portfolio	No	Yes

TABLE 2:
BENEFITS OF IDENTITY MANAGEMENT IN RED HAT ENTERPRISE LINUX

	WITHOUT IDENTITY MANAGEMENT	WITH IDENTITY MANAGEMENT
Growth	Limited number of Linux systems can be handled per administrator.	Thousands of Linux systems can be centrally managed with limited resources.
Control	All control is in the hands of Active Directory administrators. Responsibilities regarding management of Linux systems are not well defined.	Linux administrators are in charge of the Linux infrastructure, which is brought into the global company infrastructure using trusts with Active Directory.
Cost	Per-system client access licenses (CALs) and the extra cost of third-party software	No additional cost--included with subscription.
Vendor simplicity	Mixture of vendors	One open source integrated solution: LDAP, Kerberos, DNS, CA
Ease of management	Linux systems are managed with Windows-based tools. Labor intensive, requires extra installation and configuration efforts per system.	Linux systems are managed with Linux tools, including easy-to-use web and command-line interfaces as well as a simple utility to enroll the system.
Ease of deployment	Usually requires installation of non-native components (clients, agents).	All components are provided.
Value	Varies by solution	Linux systems are controlled over native protocols using concepts natural for Linux.

Taking advantage of the identity management included in Red Hat Enterprise Linux creates a balanced solution that supports the Linux infrastructure as it grows to meet business needs and the Microsoft Windows segments of the datacenter. This approach facilitates a better separation of duties in the IT organization and allows teams to focus on their core areas of expertise. By eliminating third-party vendors and the overhead of managing systems individually, it streamlines Linux system life cycle management and day-to-day operations to reduce costs.



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 70 offices spanning the globe, empowering its customers' businesses.

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

NORTH AMERICA
1 888 REDHAT1

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

redhat.com
#12069297_0414