

WHITEPAPER

IDENTITY MANAGEMENT IN LINUX AND UNIX ENVIRONMENTS

EXECUTIVE SUMMARY

In today's IT environments everything is growing, especially the number of users, systems, services, applications, and virtual machines. Manually managing user accounts, passwords, and access permissions on a machine per-machine basis is no longer feasible in the era of virtualization and increased regulation. Most companies are still dealing with siloed identity stores that force users to remember multiple passwords and administrators to duplicate user provisioning across numerous systems and applications, all of which is time consuming, prone to error, and can lead to breaches in security and loss of productivity. IT organizations supporting Linux and UNIX environments are struggling to find a simple, secure, scalable, and affordable solution to centrally manage and authenticate identities and control and ensure authorized access to resources, applications, and data.

Unfortunately, most identity and access management solutions are complex, expensive to implement, and designed for homogenous environments. None of these solutions is designed to use native Linux tools to support mixed Linux and UNIX environments. In addition, the expertise necessary to successfully implement and maintain even the simplest solution is generally lacking.

Identity Management in Red Hat Enterprise Linux provides a centralized and efficient way to manage identities for users, machines, and services within Linux and UNIX enterprise environments – and provides a way to define system and Linux service access control policies to govern those identities.

Because Identity Management is integrated with Red Hat Enterprise Linux, it is easy and cost-effective to introduce identity and policy management into a Linux and UNIX environment wherever you need it.

EXISTING SOLUTIONS AND THEIR DRAWBACKS

IT organizations previously had three options to manage identities and access: build a solution in-house, deploy a proprietary third-party solution, or attempt to integrate with an existing Microsoft Active Directory solution. All of these options have drawbacks that make them less than ideal.

Build In-House

In-house identity management projects are expensive, long term projects that require a large amount of integration between protocols and applications to securely manage user authentication and authorization to applications and data. These environments frequently consist of an NIS domain to track machines, an LDAP directory for storing user identities, Kerberos for authentication, and sudo to manage access. Some organizations have deployed Kerberos to provide enterprise single sign-on capabilities. Sometimes this is combined with a central LDAP-based identity store, but the resulting solution is highly complex and requires a constant effort to maintain consistency between the separate identity sources.

While these solutions can be powerful, they are complex to implement and maintain, not tightly integrated, and lack comprehensive tools or a Web GUI. As a result, this option requires a very high degree of expertise in LDAP and significant configuration and customization, which makes the solution costly and inflexible. In addition, while this option is adequate for managing identities, it is difficult to enact and manage policies for fine-grained access control.

Proprietary Solutions

A variety of software companies offer solutions to manage and enforce identity and access policies. These applications have been available for many years but also introduce a number of issues. First, while full-featured and powerful, these solutions are also complex and expensive. Smaller, proprietary point solutions do not fill every need and can be difficult to integrate with other point products and enterprise applications. As a result, many organizations limit deployment to specific high-risk machines, or only deploy pieces of the overall solution. Second, these solutions are large, proprietary applications that are difficult to enhance, customize, and integrate, which limits flexibility. Finally, identity data is often stored in a proprietary format that makes it difficult for other applications to reuse or analyze policy and audit data.

Integrating with Microsoft Active Directory

Many organizations already maintain a Microsoft Active Directory infrastructure to support the Windows environment and attempt to extend it to Linux or UNIX systems by making them members of the Active Directory domain. There are a number of open source and third-party solutions to accomplish this, but these are either limited or require additional investment.

This approach is generally adequate for user authentication but not sufficient for policy, as it forces Windows policy concepts on to Linux and UNIX systems. In addition, the Linux and UNIX environment becomes completely dependent on the Active Directory administrators for updates and changes, which introduces delay, limits flexibility, and increases security risk.

IDENTITY MANAGEMENT IN RED HAT ENTERPRISE LINUX

Identity Management in Red Hat Enterprise Linux provides the tools to quickly install, configure, and centrally manage identity management servers in large and small Linux and UNIX enterprise environments, using Linux tools on Linux systems. It also providing the option to interoperate with Microsoft Active Directory. Integrated into Red Hat Enterprise Linux, Identity Management allows you to expand your use of Linux, at the same time reducing costs, administrative load, and rising compliance levels by implementing central authentication, identity lookup service, and fine-grained access control.

Identity Management integrates capabilities from Kerberos, LDAP, DNS, and x.509 certificates to provide a reliable, scalable, simple-to-use, and secure identity management solution. While centralized identity/policy/authorization software is hardly new, Identity Management is one of the only options that supports Linux and UNIX domains using Linux tools.

Enhanced Security

Identity Management enhances security by helping to ensure that people have access only to the systems, services, and data that they need to perform their jobs. It provides the policies and mechanism to authenticate users and machines and to authorize users to access corporate systems and data, thus preventing accidental or fraudulent use that could negatively impact the business. For example, a backup administrator can be given root access to a small set of commands on a limited number of systems.

Because all data is centralized, a number of activities can be automated to increase security. For example:

- **User provisioning/deprovisioning:** User accounts can be quickly provisioned, modified, or deactivated across all systems and services when users join, move within, or leave the organization. If integrated with Active Directory, user accounts that are disabled in one domain are disabled in the other.
- **Password policies:** Password policies minimize risk by enforcing adequate complexity standards to thwart brute force attacks and to ensure passwords are changed frequently enough to mitigate the risk of someone revealing or discovering a password. In addition, if also using Active Directory, passwords can be synchronized both ways.
- **Compliance:** Identity Management helps organizations comply with corporate and governmental regulations by limiting access to applications and data and providing one traceable identity for all users.
- **Recertification:** Sarbanes-Oxley (SOX) requires financial services firms, as well as other publicly-traded companies, to review every employee at least once a year to re-certify that they still need access to systems. Identity Management can provide a Web-based view of individuals and their access to make it easier for managers to verify employment status against HR records.

Enterprise Single Sign-On

Identity Management provides the centralized user authentication required to implement enterprise single sign-on (eSSO). eSSO enables users to access many different enterprise resources after their initial log-in without having to log in to each resource. This streamlined access increases productivity and reduces password fatigue and help desk calls for forgotten passwords. If interoperability with Active Directory is enabled, users are authenticated when they log in to their desktop.

Identity Management adds Kerberos eSSO and LDAP to Linux, UNIX, and Mac systems in the way these systems expect. It also provides Kerberos-based out-of-the-box eSSO for any enterprise application that supports Kerberos or LDAP, including Samba, Apache, SSH, NFS, WebSphere, JBoss, Tomcat, SAP, Oracle, and MySQL.

Centralized Administration and Control

A major goal of Identity Management is to greatly reduce administrative overhead. This is accomplished by integrating all of the different applications together seamlessly, using a single and simplified tool set. Users, machines, services, and policies are all configured and managed in one place. A Web user interface and CLI provide a layer that unifies all of the services and simplifies administration tasks for managing users, systems, and security.

These interfaces allow management tasks to be automated and performed repeatedly in a consistent manner for greater efficiency and security. For example, identities are maintained on a central identity service represented by a group of replicating servers and users and policies are uniformly applied to enrolled machines. And, because Identity Management creates a domain, multiple machines can all use the same configuration and the same resources simply by joining the domain. As a result, administrators are less dependent on complex scripts and senior administrators to manage user identities and access.

The centralized identity store of Identity Management also enables better control over who has access to which systems and resources. User accounts are consolidated, which makes it easier to enforce security policies. Integrated authorization enables you to control how and when users can access Linux and UNIX systems, and exactly which commands they can execute on those systems. This allows you to apply granular protection to enterprise resources. For example, you can configure end-user self service to allow end users to update their own personal profile information and change passwords. You can set different access levels for laptops and remote users, or you can restrict the hours of access for certain groups of users.

Finally, the Web user interface shows instant, visual relationships between entities. For example, all of the groups, access rules, and policies associated with a user. With this information, managers can see a list of staff and the access rights assigned to them so they can better understand if there is a compromise, or determine if people have access to the tools and processes they need to perform their jobs.

Standards-Based Integrated Components

Identity Management provides an integrated, unified interface for the standards-based capabilities of Kerberos, LDAP, DNS and x.509 certificates to deliver a reliable, scalable, simple-to-use identity management solution. Although all of these components can be used individually to implement a solution, Identity Management in Red Hat Enterprise Linux is more flexible and easier to administer because it is designed and optimized for a single purpose: to manage identities.

Identity Management focuses on centrally managing identities (user and machine) and the policies that relate to those identities and their interactions. While it uses LDAP to store its data, Identity Management provides a purpose-built structure that defines a particular set of identity-related entry types and their relationships in detail.

The Identity Management server is deployed solely to manage identities, which produces a great deal of administrative simplicity. It provides a simple, one-command installation – that also installs a Web server and Web application to manage the solution – an easy configuration process, and a unified set of commands. It also has a clearly defined role in the overall IT infrastructure. An Identity Management domain is easy to configure, join, and manage, and the functions that it serves – particularly identity and authentication tasks like enterprise SSO – are also easier to perform with Identity Management than with a more general-purpose directory server. In addition, the Identity Management server can easily be replicated to provide load balancing and high availability.

Identity Management creates an alternative to Active Directory for Linux and UNIX systems and provides administrators more control over identities in their Linux and UNIX environment. Identity Management takes over the role of Active Directory and provides authentication, authorization, and administration infrastructure to the rest of the enterprise, including Linux, UNIX, and Mac systems. Identity Management brings native control to Linux and UNIX servers, using native tools and applications – something that is not possible in Active Directory. Additionally, because Identity Management is Windows-aware, critical user data, including passwords, can be synchronized between Active Directory and Identity Management, preserving a centralized user store.

Reduce Costs

Identity Management is integrated into Red Hat Enterprise Linux and does not require an additional subscription. When you use Identity Management, you eliminate the need to purchase a third-party solution to integrate Linux and UNIX users into Active Directory.

Other savings include:

- **Eliminates the cost of integration:** protocols, data, and access applications are already integrated and managed with a single tool.
- **Reduces help desk calls:** A simple password reset tool helps reduce costs as a large percentage of help desk calls are related to password resets. Self-service helps alleviate the strain on the help desk and the investment in human capital required to provide this kind of basic support.
- **Allows for faster deployment:** New applications can be deployed faster and users can be provisioned faster. New employees need access to applications and resources as quickly as possible. Identity Management can be used to automate user provisioning and deprovisioning that can help ensure that all tasks are completed as quickly as possible. Hosts and virtual machines can be provisioned faster by automatically enrolling and connecting them to the Identity Management server.
- **Reduces administrator costs:** Frees IT administrators from manually managing security processes. Also increases productivity by enabling enterprise single sign-on.
- **Reduces training costs:** Enables you to harness the power of LDAP, Kerberos, and Certificate Authority without extensive training and expertise.

FOR MORE INFORMATION

To learn more about Red Hat Enterprise Linux, contact your local sales person or visit redhat.com.

ABOUT RED HAT

Red Hat was founded in 1993 and is headquartered in Raleigh, NC. Today, with more than 60 offices around the world, Red Hat is the largest publicly traded technology company fully committed to open source. That commitment has paid off over time, for us and our customers, proving the value of open source software and establishing a viable business model built around the open source way.

SALES AND INQUIRIES

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

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

ASIA PACIFIC
+65 6490 4200
www.apac.redhat.com
apac@redhat.com

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