RED HAT DIRECTORY SERVER

CENTRALIZE IDENTITY INFORMATION IN A NETWORK-BASED REGISTRY

WHAT IS IT?

Red Hat Directory Server is an LDAP-compliant server that centralizes application settings, user profiles, group data, policies, and access control information in a network-based registry.

WHAT DOES IT DO?

Directory Server simplifies user management by eliminating data redundancy and automating data maintenance. Red Hat Directory Server also improves security, enabling administrators to store policies and access control information in the directory for a single authentication source across enterprise or extranet applications.

WHY SHOULD I CARE?

Directory Server reduces administration costs and increases availability, providing the scalability and information control to manage access across partner, supplier, and customer relationships.

FEATURES OVERVIEW

- Centralizes management of people and their profiles, thus reducing administrative costs
- Acts as a central repository for user profiles and preferences, enabling personalization of applications and systems
- Allows four-way, multi-master replication of data across the enterprise, providing a centralized, consistent data source available to enterprise applications
- Enables single sign-on access
- Provides scalability for massive numbers of users by containing the information control required for developing extranet applications

REDUCES ADMINISTRATION COSTS

Red Hat Directory Server lets administrators establish a network-based registry that applications can use to store shared data, such as user information, groups, and preferences. With Directory Server, applications can achieve location independence by storing and retrieving preferences in the directory instead of reading separate files on a user's desktop. This allows users to work at virtually any computer as if they were at their own desktops. It also enables IT administrators to manage user credentials and profiles in one place, regardless of the size or number of applications that leverage the information.

To enable customer self-administration, Red Hat Directory Server distributes administrative control over one or more levels of enterprise management.

DIRECTORY FEATURES INCREASE AVAILABILITY

One way Red Hat Directory Server ensures high availability is with four-way, multi-master replication. Deploying multiple master servers eliminates write availability as a single point of failure. Simple Network Management Protocol (SNMP) provides flexible network monitoring. Red Hat Directory Server also minimizes downtime for administration and maintenance by allowing backups, configuration changes, schema updates, indexing, and restoration of data to occur while the directory is online.

MANAGES ACCESS ACROSS PARTNER, SUPPLIER, AND CUSTOMER RELATIONSHIPS

As an enterprise extends partner, supplier, and customer relationships online, managing access becomes increasingly difficult and expensive. Red Hat Directory Server provides the scalability and information control required for developing extranet applications for massive numbers of users. By centralizing users, groups, and access controls across multiple applications, Red Hat Directory Server dramatically simplifies administration. It also provides the foundation for strong certificate-based authentication when used in conjunction

with an X.509v3 public key certificate solution such as Red Hat Certificate System.

FLEXIBLE DATA STORAGE AND VIRTUAL VIEWS

Red Hat Directory Server can store user profile and preferences to authenticate, authorize access, and personalize information delivery. This allows LDAP-enabled applications to read user data and dynamically generate a personalized web environment. The data can be configured and extended on the fly via schema updates without downtime.

Virtual directory information tree views enable creation of custom DITs for specific applications and purposes without having to change the physical location of directory entries.

Virtual Attribute Search allows the use of virtual attributes in ACLs and in regular search filters.

MULTI-MASTER REPLICATION

Four-way multi-master replication brings directory availability and failover to unprecedented levels of performance. It increases flexibility in architecture and design of the directory deployment. Scripts for monitoring and troubleshooting replication simplify the process for administrators. Updates can be simultaneously applied to one or more directories and changes automatically propagate to other participating servers.

FEATURES

LDAP version 2 and 3 implementation

- Implements relevant LDAPv2 and v3 RFCs including RFC 2251–2256, 2829, 2830 and 4514
- Supports LDAPv2 and v3 operations
- Supports LDAP search filters including presence, equality, sub-string, approximate (“sounds like”), and the Boolean operators and (&), or (|) and not (!)
- Supports LDAPv3 intelligent referrals which let a directory refer a query to another directory
- Integrates presence and status from instant messaging deployments using standard LDAP commands

High-performance server

- Manages millions of entries and handles thousands of queries per second, per server
- Directory data can be logically partitioned across many servers
- Scales linearly with multiple CPUs
- Includes flexible attribute-level indexes that allow performance to be optimized based on the usage profile
- Supports 64-bit Red Hat Enterprise Linux, providing high levels of performance and scalability for large databases (>1 GB)

Flexible replication models

- Supports four-way multi-master replication across a LAN or WAN
- Helps lower network costs, improve response time, and eliminate single points of failure with directory replication
- Implements replication over LDAPv3
- Supports cascaded replication (when server A replicates to server B, which then replicates to server C)
- Supports replication of a subset of attributes (fractional replication)

Advanced security features

- Restricts access to directory data with control down to the attribute value level
- Controls user’s ability to perform read, write, search, or compare operations
- Server-enforced minimum security strength configuration option
- Provides access control based on user identity, group membership, role identity, IP address, domain name, or pattern-based rules
- Allows access anonymously or via authentication methods such as user ID/password or X.509v3 public key certificates

- Stores access control list (ACL) information with each entry so that security policy is replicated with the data
- Supports LDAP over Secure Sockets Layer (SSL) and Transport Layer Security (TLS), providing privacy (encryption), integrity, and authentication services
- Supports PKCS #11 for hardware accelerated SSL/TLS
- Supports fine-grained password policy management (from subtree down to user), providing hack protection (retry attempts, lockout) and crack protection (min/max length, triviality checking, password history)
- Supports configurable encryption for all attributes
- Supports SASL encryption and GSS-SASL authentication, typically used for Kerberos encryption and authentication

High availability

- Provides 24x7 read and write availability
- Allows multiple databases to be defined for storing data across multiple disk partitions or multiple machines
- Supports replication for data redundancy
- Implements a transactional data store, allowing seamless recovery from catastrophic failure
- Allows most administrative operations such as backups, schema updates, and configuration changes to be performed online

Powerful administration tools

- Allows delegation of administrative authority to the host, server, and task level
- Allows administrators to monitor and tune server performance
- Provides an easy-to-use, GUI-based Java console for system administrators to manage the servers
- Allows the use of custom attributes to extend the definition of users and managers to fit enterprise or application-specific needs
- Includes certificate and replication setup wizards that make configuration easy
- Offers context sensitive help
- Supports SNMP with the IETF-defined standard Mail and Directory Management (MADMAN MIB)
- Supports LDAPI interface for fast, secure local connections

Extensible architecture

- Class of Service allows population of attribute values based on user roles and services
- Allows developers to write business rules that are triggered by directory operations
- Allows developers to authenticate users against an existing authentication or authorization service, such as Kerberos
- Enables pluggable components for customized sorting and collation of international character set
- Supports a dynamically extensible schema
- Supports bi-directional password synchronization with Windows Active Directory

Developer tools and utilities

- Supports popular LDAP extensions, such as persistent search, server-side sorting, and virtual list view
- Includes Red Hat Directory Software Development Kit (SDK) that lets developers create LDAP-enabled applications using JavaScript, XML, C, Java, Perl, and other programming languages

SUPPORTED PLATFORM AND SYSTEMS REQUIREMENTS

HARDWARE	ARCHITECTURE	OPERATING SYSTEM	MEMORY	DISK SPACE
Intel / AMD	i386 and x86_64	Red Hat Enterprise Linux 6, 32- and 64-bit versions	256 MB (required)	200 MB (minimum)

RED HAT SALES AND INQUIRIES

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

Copyright © 2012 Red Hat, Inc. “Red Hat,” Red Hat Linux, the Red Hat “Shadowman” logo, and the products listed are trademarks of Red Hat, Inc., registered in the U.S. and other countries. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.