Introduction

Sun™ ONE Identity Server

Version 5.1

816-5306-10
May 2002

Contents

Introduction to Sun ONE Identity Server

This booklet introduces Sun™ ONE Identity Server version 5.1. This overview contains the following sections:

- An Overview of Sun ONE Identity Server
- Sun ONE Identity Server Benefits
- Installation and Deployment
- Documentation Resources

NOTE Sun ONE Identity Server was previously known as iPlanet™ Directory Server Access Management Edition (DSAME). The product was renamed shortly before the launch of the product.

The late renaming of this product has resulted in a situation where the new product name is not fully integrated into the shipping product. In particular, you will see the product referenced as DSAME within the product GUI and within the product documentation. For this release, please consider Sun ONE Identity Server and iPlanet Directory Server Access Management Edition as interchangeable names for the same product.

An Overview of Sun ONE Identity Server

Sun ONE Identity Server, version 5.1 provides a comprehensive solution for managing identities and for enforcing authorized access to network services and resources. It integrates the Sun ONE Directory Server with a policy service and identity management service. Combined, these services simplify and streamline the administration of identities. These services also provide for a single user-identity (single sign-on) across a range of both web-based and application-based services.

By simplifying the overhead required for identity administration, a comprehensive identity management infrastructure provides the following benefits:

- Facilitates rapid development of new applications and services within your enterprise.

  The proper deployment of an identity management infrastructure leverages existing user information and infrastructure, easing the deployment of additional applications and services. The identity management infrastructure allows deployed services to be quickly modified, without requiring new and resource-expensive programming to generate code to keep track of user data.

- Provides rapid access to appropriate web applications and content.

  Once set up, an identity management infrastructure allows authorized managers to decide which web resources will be available for a particular group of users, based on user business roles. The system is flexible, managers can specify durations for which access is granted. This allows different sites to be available to different groups of users for specified periods of time.

Sun ONE Identity Server is composed of the following components:

- Directory Server
- Identity Management Service
- Policy Service

By defining roles for users, the *Policy Service* makes it easy to grant and revoke privileges to small and large sets of identities, such as users. The *Identity Management Service* provides the flexibility to quickly and easily add, modify, delete users via centralized or delegated administration.

Directory Server

The Sun ONE Directory Server is the industry leader for e-business and extranet directory deployments. Sun ONE Directory Server delivers a high performance, highly scalable LDAP version 3-compliant data store that supports multi-master replication, chaining, roles, and class of service. Its highly advanced, carrier-grade architecture supports extremely large deployments with millions of users.

Used as the fundamental building block in a Sun ONE Identity Server deployment, Directory Server provides the “identity store” that Sun ONE Identity Server uses for its profile and policy information.

Identity Management Service

The Identity Management Service provides both centralized and delegated identity management, including self-management for system users. Administrative rights can be granted to groups, giving specified users the ability to modify profile information. Access rights can be delegated to many types of users, including employees, customers, partners, and suppliers. These administrative and access rights can be configured with unlimited levels of delegation.

By delegating the management of identities, organizations can increase the speed of updates. This increases efficiency, since the administrative tasks are transferred to the authoritative sources that are responsible for the updates. With an identity management infrastructure, you reduce user and group maintenance costs and cut down on recurring administrative overhead.

Policy Service

The Policy Service provides authentication and access enforcement to web-based and application server-based services. Future versions of Sun ONE Identity Server will provide the functionality to protect other types of resources. The Policy Service also provides single sign-on (SSO) for web-based applications. Access enforcement to protected resources is based on Roles, which can be assigned to individual users or groups of users. These Roles grant access across multiple web and application servers.

Sun ONE Identity Server Benefits

The Sun ONE Identity Server provides the following benefits:

- Lower administrative costs
- Strong, consistent security
- Rapid time-to-market
- Increased user satisfaction

Lower administrative costs — Policy-driven administration provides a way to manage privileges at the enterprise level. Using the Policy Service, you gain the ability to administer user privileges across multiple applications. The ease of identity management increases as you define discrete groups into which you can assign users. With clearly defined groups, the administrator can assign and modify policies on a group level, instead of administering privileges on a user-by-user or application-by-application basis. Using policies, administrators can centrally manage privileges, reducing the required amount of user-level administration.

Strong, consistent security — Sun ONE Identity Server replaces the ad-hoc and one-off security point solutions that tend to appear in custom web services. By making use of use of shared credential management and single sign-on, it's easy to ensure that there is a consistent security model applied across all web services. In the case where a user needs to be deactivated or deleted, the task happens simultaneously across all services.

Rapid time-to-market — Providing a common security infrastructure for identity management, user authentication, user authorization, and single sign-on, companies that deploy Sun ONE Identity Server can focus on building their application's core functionality instead of getting sidetracked on redesigning these essential identity management tools.

Increased user satisfaction — Single sign-on increases the usability of a site by enhancing user interaction. Once authenticated, users can access protected web applications without being prompted for additional user names or passwords. This amounts to a reduced load on Help Desk services; there will be fewer calls to reset passwords or grant access to varying network resources. Users will have fewer passwords to remember and access to network resources can be granted to existing users on a group-by-group basis.

Key Features of Identity Server

Sun ONE Identity Server provides the following key features, based on its servers and services.

Policy Service

The Policy Service provides the following main features:

- **Web-based single sign-on** — Allows users to sign on once for access to multiple applications and services.
- **Extensible authentication methods** — Allows users to authenticate via the following methods:
  - User ID/Password
  - Digital certificates
  - RADIUS
  - SafeWord
  - Unix
  - Anonymous

  These methods can be chained together for increased security.
- **Access enforcement of URL-based resources** — Protects access to web-based resources. Access can be granted or restricted, based on the following:
  - Full or partial URLs.
  - Prefix or suffix based wild-card matching on URLs.
  - A post authentication API is available to set the behavior after authentication has either succeeded or failed.
- **Role Based Access Control**— Users are authorized or denied access to use services (or specific features of services) based on the role or roles assigned to them.

Identity Management Service

The Identity Management Service provides the following main features:

- **Centralized Management** — Centralized administration provides a single location to view, manage, and audit a user's of any user's identity profile and access rights via an HTML based interface for anywhere, anytime management.
- **Delegated management** — Delegated management provides the ability to assign administration privileges to employees, business partners, and customers based on roles. This feature gives you unlimited levels of delegation. Custom administrators can be created who have management rights based on both the set of users who can be

managed and what for a given user can be managed. For example, you can create an “Email Administrator” who can administer only the email attributes of all users. Or perhaps you need a “Partner Administrator” to manage everything specific to a single partner company.

- **User self-registration** — Configurable to automatically grant users access to services after registering. You can also require that an administrator approve each user before granting access.
- **Customizable JSP-based GUI** — The user interface is based on Java Server Pages (JSPs) so that it is customizable to match the branding of existing web sites.

Installation and Deployment

The Sun ONE Identity Server ships as two major components, each of which needs to be installed and configured separately. While both components can theoretically be installed on a single system (or server), this deployment topology is strongly discouraged. Instead, it is recommended that you use a minimum of two servers: one for the instance of Sun ONE Directory Server and another for the Policy and Identity Management Services.

Please review the installation and deployment information in each component’s documentation before designing your Sun ONE Identity Server deployment. The recommended procedure is to consult with Sun ONE Professional Services or another Sun ONE-certified system integrator before you begin to design and deployment your Sun ONE Identity Server.

Supported Platforms and Operating Systems

Sun ONE Identity Server, version 5.1 runs on the following hardware and software systems:

- Sun Solaris® 8 Operating Environment (32-bit or 64-bit UltraSPARC)
- Microsoft® Windows® 2000 Server, Service Pack 2

Support for Industry Standards

The Sun ONE Identity Server, via the Sun ONE Directory Server, supports LDAP version 2 (LDAPv2) and LDAP version 3 (LDAPv3) operations:

- Supports X.509 digital certificates.

- Implements LDAPv2 and LDAPv3 RFCs, including RFC 1274, 1558, 1777, 1778, 1959, 2195, 2222, 2247, 2251, 2252, 2253, 2254, 2255, 2256, 2279, 2307, 2377.
- Supports LDAP search filters, including presence, equality, inequality, substring, approximate (“sounds like”), and the Boolean operators or (|), and (&), and not (!).
- Supports LDAPv3 intelligent referral, which lets a directory refer a query to another directory and LDAPv3 chaining, which allows one directory server to respond on behalf of another.

Documentation Resources

Each Sun ONE Identity Server component has its own comprehensive documentation set. The Sun ONE Identity Server documentation is supplied in the following electronic formats: HTML and Adobe® Acrobat® PDF files.

The documentation is available in the following two places:

- On the Sun ONE Identity Server documentation web site:

  `http://docs.iplanet.com/docs/manuals/dsame.html`

- On the product CD

It is recommended that you check the documentation on the web site regularly as Sun periodically updates and refreshes the documentation posted there.