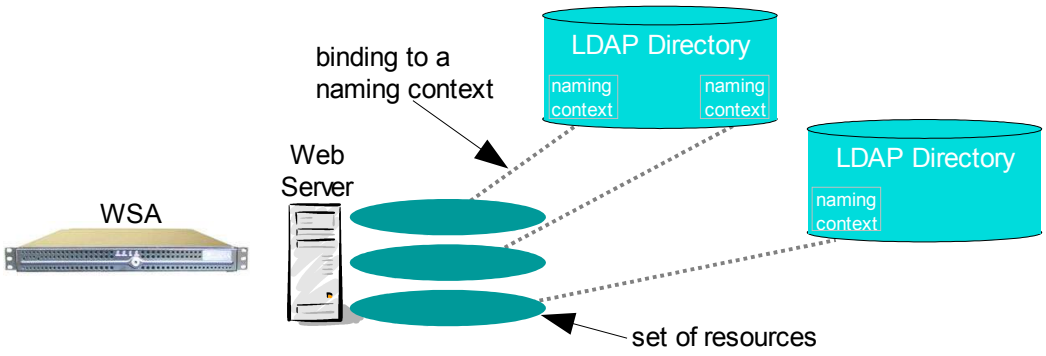
The Sevan WSA in Directory-Driven Enterprises

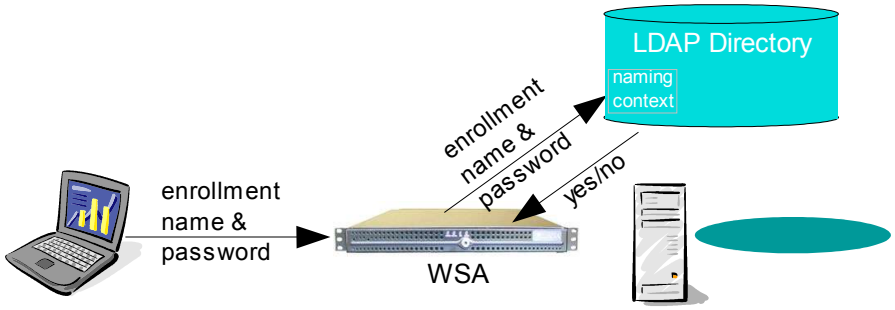
A Sevan White Paper

Businesses are increasingly looking to directories for managing employees, partners, and customers. Although the directories hold the identities and user rights, the enforcement of those rights is performed by external devices. This paper shows how the Sevan WSA is used as an enforcement point for web content and applications.

Once an administrator uses the WSA to partition the web site into sets of independent resources, the WSA restricts access to each set of resources to only authorized users. Administrators can manage users through the WSA (as a standalone device) or by binding the WSA to one or more naming contexts within external LDAP directories. As suggested in the figure below, each set of resources can be bound to different naming context.



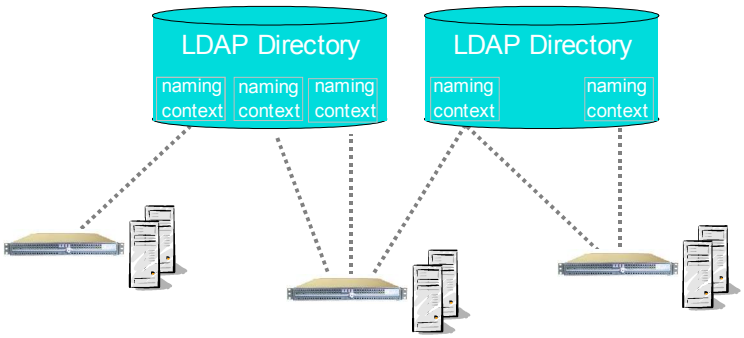
When a set of resources is bound to a LDAP directory, only users with valid accounts (names and passwords) within the naming context can access the resources. Specifically, the WSA uses the LDAP accounts to control user enrollments: the WSA allows an enrollment only after the directory validates the user's enrollment name and password within the naming context. When a directory administrator adds a new account, the WSA immediately honors the account. When an administrator removes an account or changes a password, the WSA revokes access or forces the user to reenroll after a configurable refresh time.



When the set of resources is configured for certificate-based authentication, the WSA manages the certificates, so the directory need not be burdened with certificates. As a matter of fact, the WSA's do not post information to the directory nor do they require schema changes. The WSAs simply request that the directory validates enrollment names and passwords through an LDAP logon. This provides a very loose coupling between the WSA and the

directories, which makes this arrangement very easy to setup and maintain.

Multiple WSAs can be deployed in a directory-driven enterprise as shown below. In this simple example, three WSAs are bound to two directories. The middle WSA has three sets of resources, which are bound to three different naming contexts within two directories. The right most WSA has two sets of resources and one set shares the naming context with the middle WSA.



In this arrangement, resource administration is performed on the WSA. That is, the WSA administrators define the scope of the managed resources. User administration is performed through the directories. Typically a directory administrator creates a naming context for each set of resources requiring its own group of users.

In summary, combining the WSA with enterprise directories:

- supports enterprise-wide, centralized user management
- leverages investments in user provisioning and management systems
- provides the highest level of security through the WSA appliance
- separates security from the business logic on the web servers

sevan networks

Sevan Networks, Inc
1310 Hollenbeck Ave, Ste F
Sunnyvale, CA 94087
Tel: 408.830.1000
Fax: 408.830.1001
www.sevannetworks.com

