

Jespa

Java Active Directory Integration

Jespa is a Java software library that provides advanced integration between Microsoft Active Directory and Java applications. Jespa is a comprehensive language-level security solution for Java applications. Rather than wrapping or inserting security into applications such as websites, Jespa provides highly intuitive, concrete "security provider" classes for performing a wide variety of security related functions including but not limited to authentication, manipulating accounts and groups, setting and changing passwords and much more. Jespa includes several ready-to-use components that use these security providers to implement various features such as the highly desired NTLMv2 enterprise Single Sign-On (SSO) authentication for HTTP applications. *Virtually all new Windows deployments require NTLMv2 authentication* and specifically exclude the older DES based NTLMv1.

Some things you can do with Jespa are:

- Authenticate HTTP clients using the NTLMv2 Single Sign-On (SSO) capability built into Internet Explorer and other browsers. This feature allows clients that are already logged into the domain to transparently authenticate using their existing credentials. Once a client is authenticated, the "security provider" may be retrieved to perform various security related operations in the context of the user.
- Use the simple LDAP API to easily create, update and delete accounts, groups and other LDAP entries, set and change passwords, search, check group membership and validate credentials using the conventional "simple" LDAP bind technique. Using the Jespa LDAP API, these operations are trivial when compared to the equivalent JNDI code that would be required. The LDAP API works with both Active Directory and RFC based LDAP servers.
- Enable NTLMv2 authentication and transport encryption in existing JNDI LDAP code. This eliminates the need for SSL certificates and slow SSL communication.
- Chain multiple authentication mechanisms together to implement redundancy and failover capabilities. For example, a chain might be used to authenticate an HTTP client using NTLM, then LDAP and finally a custom security provider that uses SQL to query a local database of accounts.
- Use the advanced Jespa HTTP client (which of course supports proper NTLMv2 authentication) to securely access IWA or Jespa protected websites.

Other noteworthy features of the Jespa library include:

- Transparent domain controller and DNS nameserver failover
- Efficient implementation that minimizes network communication and memory usage
- Detailed documentation
- Fast Windows group based access control
- HTTP URL "handler" for enabling NTLM in existing Java applications
- Enable NTLM in SASL servers and clients with full transport encryption
- Use the NTLM security provider directly to create custom NTLM solutions
- Use the Jespa LDAP API with non-Active Directory LDAP servers such as OpenLDAP
- Cost effective licensing with steep discounts for multiple installations in the same Active Directory forest or when shipped with your product

Some of these features are described further below.

The NTLM Security Provider

The centerpiece of the Jespa library is its high quality implementation of the NTLM challenge response authentication protocol which can properly validate credentials with the NETLOGON service of Active Directory domain controllers. The Jespa NTLM implementation matches the functionality of the Windows NTLMSSP and supports all security policies exhibited by Windows clients and servers¹. Jespa fully implements NTLMv2 and uses it by default when acting as an initiator or acceptor. Jespa supports all LmCompatibilityLevel, NtlmMinServerSec and NtlmMinClientSec values used by Windows Server 2008.

NTLM HTTP Single Sign-On (SSO) Authentication

Many web browsers support a type of Single Sign-On (SSO) authentication that uses NTLM. This is a highly desirable feature because clients will not need to enter their password (unlike some "SSO" solutions where the user is redirected between secondary websites which usually still require entering credentials anyway). A Jespa enabled website can automatically authenticate the client and acquire detailed information about the user like their fully expanded group membership which it can then use to perform very fast Windows group based access control. Jespa includes a standard Java Servlet Filter for protecting sites with NTLM as well as an HttpSecurityService component for creating customized HTTP authentication solutions.

Windows Group Based Access Control

The Jespa NTLM security provider can check a user's group membership using standard windows group names like:

```
if (request.isUserInRole("BUSICORP\\ERP Admins")) {  
    // Only users in the Engineers group will be able to reach this
```

These checks are extremely fast. The user's fully expanded list of group SIDs is acquired during NETLOGON authentication. Once the group names within your code or configs have been translated into Windows SIDs, they are cached for subsequent access checks. This means that group based access checks almost never require communication with the domain controller until the application is restarted.

The Jespa LDAP API

Jespa 1.1 now includes an excellent LDAP API that makes performing common LDAP operations "as simple as possible, but not simpler". The developer can create user accounts, set passwords, add group members, perform advanced searches and much more with only a few lines of code. The Jespa LDAP API is much easier to use than the JNDI LDAP API but the two can still be used together (see the PagedResultsControl example). The API documentation includes many code examples and the examples directory includes many fully function example programs. Admins who use Linux or other non-Windows systems will greatly appreciate the LdapSearch command line utility which can easily and securely search Active Directory and other LDAP servers using RFC2255 style LDAP URLs.

Advanced Service Location and Failover

Jespa uses DNS SRV lookups to locate AD services just like an Active Directory Sites & Services client should. If Jespa cannot contact a domain controller, it will transparently try the next domain controller. If Jespa cannot contact a DNS server, it will transparently try another. Jespa supports a DNS "records file" for bypassing DNS SRV lookups entirely. These features mean that Jespa requires very little configuration and is robust when a required service becomes suddenly unavailable.

--

This document lists only a small subset of the features of Jespa. Please look at the Jespa Operator's Manual and API documentation for details. The API documentation contains many small example code fragments and the examples directory includes many complete example programs. If you have any questions please contact support@ioplex.com or sales@ioplex.com.

¹ Only versions of Windows supported by Microsoft are tested regularly and supported by IOPLEX (although older versions such as Windows 2000 have been tested successfully in the past)