Administering Security

Configuring and administering
Configuring and administering the Apache Geronimo Server

This topic covers some common security related tasks such as adding and removing users and groups, dealing with digital certificates and increasing the security level by using different realms and authentication methods.

- Administering certificates — This section is about how to administer certificates from console.
- Administering security realms — To administer security realms via the Geronimo Administration Console the Security Realms portlet is available on the Console Navigation menu on the left hand side.
  - Certificate Properties File Realm
  - Configuring Kerberos Realm
  - Database (SQL) Realm
  - LDAP Realm
  - Properties File Realm
- Administering users and groups
  - Obscuring Passwords
- Basic Hints on Security Configuration
- Certification Authority
- Configuring HTTP header-based authentication — This chapter introduces the process of achieving Single Sign-on by using CA severs,such as Siteminder http://www.ca.com/us/internet-access-control.aspx, to validate authentication information passed by the the HTTP headers http://www.w3.org/Protocols/HTTP/1.0/spec.html#Message-Headers.
- Configuring JavaEE App Client Security — Application client security starts with specifying the CallbackHandler you want to use in the app client deployment descriptor (in Geronimo) or in a similar element in the Geronimo deployment plan.
- Configuring login modules — Geronimo replaces login.conf entirely with one that is configured via GenericSecurityRealm GBeans.
- Configuring run-as and Default Subjects, and principal-role mapping — Starting in Geronimo 2.0.1 we have adopted the basic principle that all security flows from Subjects that result from logging in to a security realm.
- Configuring secure JMX server — Geronimo has a secure JMX server embedded. However, the JMX server is not started by default.
- OpenID — OpenID http://openid.net is an open specification for distributed authentication for web apps popularly used for social networking applications.
- Replacing default Realm in Geronimo — This article is about how to replace default .properties realm geronimo-admin with SQL or LDAP realms.
- Using SPNEGO in Geronimo — Using the Simple and Protected GSS-API Negotiation Mechanism(SPNEGO) ftp://ftp.isi.edu/in-notes/rfc2478.txt in Geronimo allows HTTP users to log in and authenticate only once in their desktop, then they can receive automatic authentication from the Geronimo server.