BEA AquaLogic Enterprise Security™

Glossary

Verson: 2.6
Revised: April 2007

Contents

Glossary

Glossary

This glossary defines terms used in the BEA AquaLogic Enterprise Security product documentation. Please contact us at docsupport@bea.com if you know of a relevant term that is not defined in this glossary or if you believe there is an error or misconception given for any of our terms.

A

AAA

A computer security term referring to a server or system software that provides the *three A's:* Authentication, Authorization, and Accounting (sometimes referred to as Auditing).

access control

Protection of system resources against unauthorized access; a process by which use of system resources is regulated according to an authorization policy and is permitted by only authorized entities.

access decision

Determines whether a user, group or role has permission to perform a given operation on a resource. The outcome of an access decision is either to permit or deny access, or abstain from making a decision. An access decision is determined through by the authorization provider and the established security policy.

accountability

The property of a system that ensures that the actions of a system entity may be traced uniquely to that entity, which can be held responsible for its actions.

adjudication provider

A security provider that resolves conflicts between multiple access decisions and determines the final permit, deny, or abstain decision.

administration console

The browser-based application for administering the configuration and deployment of security provider configuration and authorization policy. The administration console allows authorized users to create, manage, and analyze both security provider configuration and authorization policy.

administration server

In BEA AquaLogic Enterprise Security, an Administration Console, Policy Distributor (PD), Authorization and Role Mapping Engine (ARME), Policy Loader, and Service Control Manager (SCM) are all components of the Administration Application.

all

A keyword that signifies a privilege group containing all privileges (`//privgrp/all`). `all` is mainly for delegation. `all` cannot be used in access policies.

allusers

A keyword that represents an implied group and is used in policies to mean *all users in a group* (`//sgrp/wles/allusers`). Note that anonymous users are included in allusers.

anonymous

Type of principal that accesses a resource without being authenticated.

any

A keyword that signifies either “any privilege” or “any group” The former use is much more common. Only the privilege form can appear in access policies.

applet

Client-side Java program, usually embedded in an HTML page and viewed with a Java-enabled web browser.

application component

Server-side component, such as an EJB, JSP, servlet, or connector that is deployed, managed, and executed on an application server.

Component made available to a web client by an application server and then executed on the web client tier, such as a Java applet and a DHTML page. See application server.

application node

A resource that logically represents an application in the resource hierarchy. In AquaLogic Enterprise Security, application nodes are bound to a Security Service Module.

application programming interface (API)

1) Application-level environment, including functions, for supporting a particular system software product.
2) Set of code that enables a developer to initiate and complete client/server requests within an application.
3) Set of calling conventions that define how to invoke a service. A set of well-defined programming interfaces (entry points, calling parameters, and return values) through which one software program utilizes the services of another.

application security

The ability to lockdown an application and all of its components through a managed authorization policy; this may include application components distributed across multiple systems.

application server

A server designed to make it easier for developers to isolate the business logic in their projects (usually through components) and develop three-tier applications. Resources include databases, ERP applications, and traditional mainframe applications. Application servers also provide tools for developing user interfaces and for deploying an application to the web. Many application servers offer additional features such as transaction management, clustering, failover, and load balancing. BEA WebLogic Server is a Java Application Server, which complies with the Java 2 Enterprise Edition (J2EE) platform.

AquaLogic Enterprise Security component

AquaLogic Enterprise Security implements J2EE component technologies, which include servlets, JSP Pages, and Enterprise JavaBeans. To build a WebLogic Server application, you must create and assemble components, using the service APIs when necessary. Components are executed in the WebLogic Server web container or EJB container. Web components provide the presentation logic for browser-based J2EE applications. EJB components encapsulate business objects and processes.

AquaLogic Enterprise Security Framework

Interfaces in the `weblogic.security.service` package that unify security enforcement and present security as a service to other components. Security providers call into the Security Framework on behalf of applications requiring security services.

asymmetric key cryptography

A key-based cryptography that uses an encryption algorithm in which different keys, private and public, are used to encrypt and decrypt the data. Data that is encrypted with the public key can be decrypted only with the private key. Conversely, data encrypted with the private key can be decrypted only with the public key. This asymmetry is the property that makes public key cryptography so useful. Asymmetric key cryptography is also called public key cryptography. See private key, public key, and symmetric key cryptography.

attribute

Characteristic that further defines a user, group, resource or other policy element. Attributes may be associated with users or groups (subject attributes), resources (resource attributes) or policy requests (dynamic attributes). Attributes can describe the entity, configure policy engine behavior, manage delegated administration, or be used to form policy as part of a constraint. Attributes must have a defined type that denotes the range of legal values that it may have. A number of predefined types exist, such as string, date, time, or IP address. You can also supply a custom attribute type. The value of the attribute can be assigned to only one instance of an attribute.

attribute converter

A plugin to convert context data to a consistent internal attribute format. These plug-in functions extend the capabilities of the existing security providers. You can use these to manipulate existing policy data in a way that is not already provided or to retrieve data from external sources to add to an authorization or role mapping decision or a deployment audit.

auditing

Process whereby information about operating requests and the outcome of those requests is collected, stored, and distributed for the purposes of non-repudiation. Auditing provides an electronic trail of transaction activity, and may include changes to system configuration parameters, policy changes, transactions, and security breach attempts of any type. BEA AquaLogic Enterprise Security supports Log4j auditing features.

auditing provider

A security provider that provides auditing services. See auditing and security provider.

authentication

Process whereby the identity of users or system processes are proven or verified. Authentication also involves remembering, transporting, and making identity information available to various components of a system when that information is needed. Authentication typically involves username/password combinations, but can also be done using tokens. See

authentication provider, identity assertion, LoginModule, perimeter authentication, and token.

authentication provider

A security provider that enables the server to establish trust by validating the credentials of a user. Various authentication providers are available to perform username/password and certificate based authentication. See authentication, digital certificate, security provider, and user.

authentication service

A security service that verifies an identity claimed by or for an entity.

authorization

Process whereby the ability of a user or group to access a resource is determined through the role assigned to the user or group and the authorization policy assigned to the requested resource. Access control is frequently viewed as synonymous with authorization, however, AquaLogic Enterprise Security extends to contextual business-policy-driven solutions. See authorization provider, accountability, user, access control, and resource.

authorization policy

See policy, access. Also referred to as access policy.

authorization provider

A security provider that controls access to resources based on both the role of the user or group and the authorization policy assigned to the requested resource. See security provider, user, and resource.

B

bind

Associates a security configuration with an authorization policy for the purpose of deployment. See binding node.

binding node

Represents a Security Service Module configuration that is bound to a Service Control Manager for the purpose of policy and configuration distribution.

Boolean operators

Logical operators used to combine constraints, including: *AND*, *OR*, and *NOT*. See constraint.

built-in type

A type declaration that is predefined in BEA AquaLogic Enterprise Security.

C

callback

1) A method defined on the client that your web service can call. Callbacks make it possible to have an asynchronous two-way exchange between a client and a service. For example, if the service performs an operation that takes awhile, the service can immediately acknowledge the client's request with a simple return value, then use the callback later to return the full result of the operation. A callback must participate in a conversation. See callback handler.
2) Method defined on the client that can be called by your service. Callbacks make it possible to support an asynchronous two-way exchange between a client and a service. For example, if a service performs a time-consuming operation, the service can immediately acknowledge the client's request with a simple return value, then use the callback later to return the full result of the operation. A callback must participate in a conversation.

callback handler

1) A web service method that runs as soon as your service receives the corresponding callback. The callback handler is defined by the control that includes the callback. For example, the timer control has an onTimeout callback that fires when a timeout occurs. You can implement the onTimeout callback handler in your service to run code when the timer fires.
2) Method run by your service when it receives a corresponding callback. It is defined by the control that includes the callback. For example, the timer control provides the onTimeout method as a callback handler. You have the option of adding code that runs when the timer fires. See callback.

certificate

A digital statement that associates a particular public key with a name or other attributes. It is digitally signed by a certificate authority. By trusting that authority to sign only true statements, you can trust that the public key belongs to the person named in the certificate. See digital certificate.

certificate authentication

Method of providing a confident identification of a client by a server through the use of digital certificates. Certificate authentication is generally preferred over password

authentication because it is based on what the user has (a private key), as well as what the user knows (a password that protects the private key).

See authentication, certificate authority, and digital certificate.

certificate authority

A trusted entity that issues public key certificates. A certificate authority attests to a user's real-world identity, much as a notary public does. See certificate chain, digital certificate, private key, public key, and trusted (root) certificate authority.

certificate chain

An array that contains a private key, the matching public key, and a chain of digital certificates for trusted certificate authorities, each of which is the issuer of the previous digital certificate. The certificate for the server, authority, authority2, and authority3, constitute a chain, where the server certificate is signed by the authority, the authority's certificate is signed by authority2, and authority2's certificate is signed by authority3. If the certificate authority for any of these authorities is recognized by the client, the client authenticates the server. See certificate authority.

cipher

In cryptography, a coding system used to create encrypted messages. See cipher suite, cipher text, cipher suiteand Secure Sockets Layer (SSL).

cipher suite

Secure sockets layer (SSL) encryption method. Includes three types of algorithms that can be used to protect the integrity of a communication: the key exchange algorithm, the symmetric encryption algorithm, and the secure hash algorithm. See cipher and Secure Sockets Layer (SSL).

cipher text

In cryptography, text that is encrypted.

class

Category of objects used in object-oriented programming. A class defines the implementation of a particular kind of object. A class definition defines instances and class variables and methods, and specifies the interfaces and class implementations and the immediate superclass of the class. If the superclass is not explicitly specified, it is implicitly assumed to be an Object. See object-oriented programming (OOP) and class library.

class library

A set of client programming tools called classes. You can use these tools in a Java or C++ program or in a Java applet that can be embedded in a web page. See class and CLASSPATH.

CLASSPATH

List of paths for the file system directories or Java archive files that the Java Virtual Machine (JVM) searches at run time to locate the executable class files required. The list may be supplied through an operating system environment variable (CLASSPATH) or a command-line switch (-classpath) sent to the virtual machine. Application server containers, such as servlet engines and EJB containers, can contain additional levels of classpath information. See class and class library.

cloning

Creating a new user with the characteristics of an existing user; privileges and privilege groups can also be cloned (similar to a copy).

closed-world assumption

A state indicating that unless an explicit authorization policy exists that specifically grants access, then access is denied. By default, this assumption is enforced by the ASI Authorization Provider.

comparison operator

A symbol that represents the relationship between two values in a constraint.

constant

One of the four types of declarations that you an apply to a constraint. A constant has a name and a static value or set of values, that does not change at runtime. See constant list and constraint.

constant list

A set of named, predefined, static values you can apply to a constraint to define a role or authorization policy. See constant and constraint.

constraint

A condition attached to a role definition or authorization policy that must be true for it to apply or a group of constraints connected with Boolean operators. constraint set.

constraint set

A set of items that is tested in a constraint by using the keywords `IN` and `NOTIN`. See constraint.

context handler

A ContextHandler is a high-performing class that obtains additional context and container-specific information from the resource container, and provides that information to security providers (authorization and authentication) making access or role mapping decisions. The `ContextHandler` interface provides a way for an internal resource container to pass additional information to a call, so that a security provider can obtain contextual information beyond what is provided by the arguments to a particular method. A ContextHandler is essentially a name/value list and requires that a security provider know what names to look for. In other words, use of a ContextHandler requires close cooperation between the resource container and the security provider.

control flag

If there are multiple authentication providers configured, the control flag determines whether or not the authentication continues down the chain of authentication providers if authentication fails.

credential

Security-related attribute of a subject that may contain information used to authenticate the subject to new services. Types of credentials include username/password combinations, Kerberos tickets, and public key certificates. See credential mapping, credential mapping provider, digital certificate, Kerberos ticket, public key, and subject.

credential mapping

The process whereby a legacy system database (or any remote system) is used to obtain an appropriate set of credentials to authenticate a user to a target resource. AquaLogic Enterprise Security uses credential mapping to map credentials. The credential maps are then used to log in to a remote system on behalf of an authenticated subject. See credential, credential mapping provider, and resource.

credential mapping provider

A security provider that provides credential mapping services and bring new types of credentials into the environment. See credential mapping, credential, and resource.

CSIv2 protocol

A protocol that is based on IIOP (GIOP 1.2) and the CORBA Common Secure Interoperability version 2 (CSIv2) CORBA specification. The secure interoperability

requirements for EJB2.0 and other J2EE1.4.1 containers correspond to Conformance Level 0 of the CSIv2 specification. The CORBA Security Attribute Service (SAS) is the protocol that is used in CSIv2. For more information, see:

http://www.omg.org/technology/documents/formal/omg_security.htm

custom security provider

Security provider written by a third-party security vendor or security developer that can be integrated into BEA AquaLogic Enterprise Security. Custom security providers are implementations of the Security Service Provider Interfaces (SSPIs) and are *not* supplied with the product.

D

data source

A database that provides a schema to store user, group, and password information; also referred to as a user store. See identity and directory, metadirectory and virtual directory.

declaration

A readable name that represents a value that is either predefined or defined by a function at runtime. There are four types of declarations: types, constants, evaluation functions and attributes. See type declaration, constant, evaluation function and attribute.

delegatee

The identity receiving the delegated rights.

delegation

Delegation is the transfer of a portion of one user's privileges to a resource to another user for a finite time under certain conditions. Delegation is often used by administrative users to control policy for other administrative users or for application users to allow someone else to perform an action for them or in their absence.

delegator

The identity providing the delegated rights to the delegatee. See delegation.

deny policy

An authorization policy that prevents a user, group or role from accessing a resource or performing certain actions on a resource.

deployment

Process used to distribute authorization policies, role data definitions and security configurations to a Security Service Module.

digital certificate

Digital equivalent of an ID card used with a public key encryption system to authenticate. A digital certificate is a digital statement that associates a particular public key with a name or other attributes used to identify the owner of the certificate. The statement is digitally signed by a certificate authority. By trusting that certificate authority to sign only true statements, you can trust that the public key belongs to the entity (typically, a person, a corporation, or an agency) named in the certificate.

digital signature

String of bits used to protect the security of data being exchanged between two entities by verifying the identities of those entities. Specifically, this string is used to verify that the data came from the sending entity of record and was not modified in transit. A digital signature is computed from an entity's signed data and private key. It can be trusted only to the extent that the public key used to verify it can be trusted.

directory, metadirectory and virtual directory

In AquaLogic Enterprise Security, the term *directory* applies to all types of information storage dealing with identity, including application databases, LDAP directory servers, e-mail address books, network databases, and others. These directories are at the core of any identity management solution because every information store has its own approach to the storage of identity information.

The Internet has played an important part in the adoption of directories. The cornerstone of most successful Internet-based commercial applications is the ability of an enterprise to effectively select and manage information from each identity store used to communicate with employees, customers and trading partners. Managing the information is a key to providing an effective extranet solution.

Identity directory refers to any user store configured for use with BEA AquaLogic Enterprise Security including application databases, LDAP directory servers, e-mail address books, network databases, and others. In the Administration Console, the identity directory defines a logical collection of users, groups and their attributes, that you can use to design your authorization and role mapping policy and store information about who is authorized through your policies. An identity directory typically represents groups of users of a particular resource, users in a specific location, or users imported from an external repositories (see Metadirectory).

Metadirectory refers to the concept of using a replication-based model to copy attributes from each of the proprietary directories to build an entry in a central directory that contains all attributes. After the central directory is created, updates to it are replicated to the appropriate proprietary directory. Metadirectories are useful when multiple internal proprietary directories exist (including LDAP, databases, and applications) and there is a need to share common data about individuals across them. The maintenance cost of sharing information is reduced and improves the accuracy and the overall security of an application. In AquaLogic Enterprise Security, this is a uni-directional process and changes and additions to identity data are not propagated back to the original source.

Virtual Directory refers to the concept of eliminating the central repository and building directory clients capable of accessing information from many different proprietary and standard directory sources. Virtual directories use the mapping abilities of a metadirectory, without actually combining directory information that is required for a central store of information. Virtual directories merge whole directory trees, where metadirectories join partial data from multiple trees into a single entry. Because there is only one source of information for any particular data record or directory tree, virtual directories bypass the complexity of dealing with the flow of data between directories. As such, a virtual directory is ideal when bringing together information from disparate sources.

distribution point

A node in the resource hierarchy from which authorization policy is distributed. When selected, all policy that is applicable to resources including and beneath that node are deployed and distributed to the appropriate Security Service Modules for enforcement.

domain

A collection of resources and services administered in a coordinated fashion for a single Security Service Module. An environment or context defined by a authorization policy, security model, or security architecture to include a set of system resources and the set of identities that have the right to access the resources.

dynamic attribute

An attribute where the value is either provided by an external source (such as the context handler) or calculated dynamically at runtime by the authorization policy.

dynamic credential

A credential function that returns a value.

E

encryption

Process of algorithmically scrambling data to prevent (or hinder) unauthorized disclosure, while still preserving access to the original data by authorized users. To read an encrypted file, a recipient must have access to a secret key or password that enables the recipient to decrypt it. Unencrypted data is called plaintext; encrypted data is referred to as ciphertext.

encryption key pair

Encryption key pair consists of the public key used to encrypt information and a private key used to decipher the information.

enrollment

Process by which a Security Service Module or Service Control Manager registers with an Administration Server.

Enterprise JavaBeans (EJB)

Java API that defines a component architecture for multitier client/server systems. Specifically, the EJB specifies an architecture for the development and deployment of object-oriented, distributed, enterprise-level applications. Applications written using the EJB architecture are scalable, transactional, and secure. See Java 2 Standard Edition (J2SE).

enumerated type

A type that consists of a predefined list of ordered values.

evaluation function

One of the four declaration types. This type returns one of two values, either *true* or *false.*

eXtensible Markup Language (XML)

Metalanguage (a language for describing languages) that you can use to define customized markup languages. It is composed of a subset of standardized general markup language (SGML).

XML facilitates the development of user-defined document types and the creation of programs that can use data from documents of such types. It is rapidly becoming a universal standard for defining, validating, and sharing data formats and documents.

Because XML is text-based (that is, it is not written in binary format), and it uses syntax rather than binary markers to organize data, it can be deployed across heterogeneous and potentially incompatible systems and platforms.

extranet

An intranet that is partially accessible to authorized outsiders.

F

failover

Capability of the system to recover a database, application server, or other with either little or no user intervention. In other words, the ability of a system to transfer control to a backup component when a failure occurs in any one of these areas.

firewall

Software that monitors traffic between an internal network and the Internet, and that regulates the type of network traffic that can enter and leave the internal network. A firewall can be connected to the Internet or set up within a company's network to prevent unauthorized access to the network. Firewalls protect information on computers and information carried over the network. Firewalls use various types of filters to prevent access, including limiting the types of protocols allowed and restricting access from network nodes by IP addresses and DNS node names.

fully-qualified name

A path name for a policy element, consisting of a series of simple names separated by slash marks.

G

grant policy

An authorization policy that permits a privilege of a resource to a user, group or role.

group

Collection of users that share some characteristic, such as a department, a job function, or a job title. A group has a static identity that a server administrator assigns and is associated with one or more roles. Giving permission to a group is the same as giving the permission to each user who is a member of the group. See group membership.

group membership

The quality of a user or group belonging to a given role. See group.

H

host

A computer that is attached to a communication network and can use services provided by the network to exchange data with other attached systems.

host name verification

The process of verifying that the name of the host to which an SSL connection is made is the intended or authorized party.

host name verifier

Code that validates that the host to which an SSL connection is made is the intended or authorized party. A Host Name Verifier is useful when a client or a server instance acts as an SSL client to another application server. It helps prevent man-in-the-middle attacks. By default, as a function of the SSL handshake, BEA AquaLogic Enterprise Security compares the common name in the subject distinguished name (DN) of the SSL server's digital certificate with the host name of the SSL server used to initiate the SSL connection. If the subject DN and the host name do not match, the SSL connection is dropped.

I

identity

Set of unique user attributes assigned to a principal. No two identities of principals can be identical. Principals can have several different kinds of identities, each of which must be unique. See authentication, digital certificate, identity assertion provider, single sign-on, SSL tunneling, identity attribute and token.

identity attribute

Static data associated with a user or group that contains small strings of characters containing information about the user or group to which the attribute belongs. These attributes are inherited by the member users of a group.

identity assertion

Special type of authentication whereby a client identity is established through the use of client-supplied tokens generated from an outside source. Identity is asserted when these tokens are mapped to usernames. For example, the client identity can be established by using a digital certificate, and that certificate can be passed around the system so that users are not asked to sign on more than once. Thus, identity assertion can be used to enable single sign-on. See authentication, digital certificate, identity assertion provider, single sign-on, SSL tunneling, and token.

identity assertion provider

A security provider that performs perimeter authentication—a special type of authentication using tokens. Identity assertion providers also allow the security system to establish trust by validating a user. Thus, the function of an Identity Assertion provider is to validate and map a token to a username. See authentication, digital certificate, identity assertion, single sign-on, SSL tunneling, and token.

import

The process of adding existing policy or configuration data stored in an external file to the policy database (also referred to as loading).

IN

A keyword used to test constraint sets for a specific member.

J

JAAS control flag

If a security configuration has multiple authentication providers, then the JAAS control flag determines how the login sequence uses the authentication providers.

JAAS Login Module

Responsible for authenticating users within the policy domain and for populating a subject with the necessary principals (users/groups). A LoginModule is a required component of an authentication provider, and can be a component of an identity assertion provider if you want to develop a separate LoginModule for perimeter authentication. LoginModules that are not used for perimeter authentication also verify the proof material submitted (for example, a user's password).

Java 2 Standard Edition (J2SE)

Standard Java Development Kit (JDK) and runtime environment (JRE) as provided by Sun Microsystems.

Java Authentication and Authorization Service (JAAS)

Set of Java packages that enable services to authenticate and enforce access controls upon users. JAAS implements a Java version of the standard pluggable Authentication Module framework, and supports user-based authorization. AquaLogic Enterprise Security implements only the authentication portion of JAAS.

Java Cryptography Architecture

A framework for accessing and developing cryptographic functionality for the Java platform. For a description of the Java Cryptography Architecture provided by Sun Microsystems, Inc., see http://java.sun.com/j2se/1.4/docs/guide/security/CryptoSpec.html#Introduction.

Java Cryptography Extensions (JCE)

Set of Java packages that extends the Java Cryptography Architecture API to include APIs for encryption, key exchange, and Message Authentication Code (MAC) algorithms. See http://java.sun.com/j2se/1.4/docs/guide/security/jce/JCERefGuide.html for a description of JCE provided by Sun Microsystems, Inc.

Java Management Extensions (JMX)

A standard architecture, design patterns, API, and services for application and network management and monitoring in the Java programming language.

Java Naming and Directory Interface (JNDI)

The Java Naming and Directory Interface (JNDI) is an application programming interface (API) that provides naming services to Java applications. JNDI is an integral component of the Sun Microsystems J2EE technology and is defined to be independent of any specific naming or directory service implementation. It supports the use of a single method for accessing various new and existing services. This support allows any service-provider implementation to be plugged into the JNDI framework using the standard service provider interface (SPI) conventions. In addition, JNDI allows Java applications in to access external directory services such as LDAP in a standardized fashion, by plugging in the appropriate service provider.

K

Kerberos ticket

A sequence of a few hundred bytes in length that is used to control access to physically insecure networks. Kerberos tickets are based on the Kerberos protocol. Kerberos is a network authentication protocol that allows entities (users and services) communicating over networks to prove their identity to each other, while preventing eavesdropping or replay attacks. The protocol was designed to provide strong authentication for client/server applications by using secret-key cryptography. For more information, see http://web.mit.edu/kerberos/www/.

keystore

An in-memory collection of private key and trusted certificate pairs. The information is protected by a passphrase, such as a password, a credit card number, Personal Identification Number, or some other form of personal identification information. In the Administration Console, the keystore is referred to as the Trusted Keystore. For more information, see SDK 1.4.2 Javadoc produced by Sun Microsystems, Inc., which is available at http://java.sun.com/j2se/1.4.2/docs/api/index.html.

L

LDAP authentication provider

Authentication provider that uses a Lightweight Data Access Protocol (LDAP) server to access user and group information, for example, the iPlanet Active Directory (now known as Sun ONE) and Novell OpenLDAP.

Lightweight Directory Access Protocol (LDAP)

An Internet protocol used by E-mail programs to obtain user information from some form of directory containing contact information.

LIKE

A keyword for using wildcard characters to test for the presence of a text string within another text string.

logical name

A shorthand name for the fully-qualified name of a resource.

login

The act of providing credentials as part of the authentication process.

LoginModule

Responsible for authenticating users and for populating users and groups. A LoginModule is a required component of an authentication provider and can be a component of an identity assertion provider if you want to develop a separate LoginModule for perimeter authentication. LoginModules that are not used for perimeter authentication also verify the proof material submitted (for example, a user password).

M

message digest algorithm

A computational procedure that is used to produce a message digest from a block of plain text. Once a message digest is produced, other security mechanisms are used to encrypt and convey the digest.

Metadirectory

See directory, metadirectory and virtual directory.

mutual authentication

Authentication that requires both client and server to present proof of identity. Two-way SSL authentication is a form of mutual authentication in that both client and server present digital certificates to prove their identity. However, with two-way SSL, the authentication happens at the SSL level, whereas other forms of mutual authentication are executed at higher levels in the protocol stack.

mutually exclusive roles

A relationship between two roles where a member of one role is not allowed to be a member of another role and vice versa.

N

node

An object on the application tree, including the application nodes, organization nodes, resource nodes.

non-repudiation

Irrefutable evidence that a security event occurred.

O

object-oriented programming (OOP)

Type of programming that merges data, information about its structure, and the functions to process the data into a single object. Relationships can be created between one object and another.

one-way SSL authentication

Type of SSL authentication that requires the server to present a certificate to the client, but the client is not required to present a certificate to the server. The client must authenticate the

server, but the server accepts any client into the connection. One-way SSL authentication is enabled by default in BEA AquaLogic Enterprise Security.

organization node

A group of resource nodes in the hierarchy (with their child nodes). As its name implies, its purpose is to organize your nodes into sets for ease of maintenance. Organization nodes are available for use in access policies.

P

pass phrase

A pass phrase is one or more sequences of bytes, typically characters, including punctuation, and non-printable characters, that is typically separated by a space. The use of pass phrases strengthens the passwords, which are considered a weak form of security.

password

A secret data value, usually a character string, used as authentication information.

perimeter authentication

Authentication that occurs outside the application server domain. Perimeter authentication is typically accomplished when a remote user specifies an asserted identity and some form of corresponding proof material, normally in the form of a passphrase (such as a password, a credit card number, Personal Identification Number, or some other form of personal identification information.), to an authentication server (typically a Web server) that performs the verification and then passes an artifact, or token, to the application server domain. The application server can then pass the token around to systems in the domain so that users are not asked to sign on more than once.

The authentication agent that actually vouches for the identity, can take many forms, such as a Virtual Private Network (VPN), a firewall, an enterprise authentication service (web server), or some other form of global identity service.

The AquaLogic Enterprise Security architecture supports identity assertion providers that perform perimeter authentication (web server, firewall, VPN) and handle multiple security token types and protocols (SOAP, IIOP-CSIv2).

plug-in API

A Java API that allows you to create security service modules to extend the capabilities of BEA AquaLogic Enterprise Security services.

policy, access

A statement are composed of privileges, resources, policy subjects (users, groups, or roles) and constraints that apply to that policy.

policy analysis

A collective term for tools in the administration console that answer questions about how the policy is evaluated at runtime, including policy inquiry and policy verification.

policy distributor

A component of the administration server that pushes the access policies and security configuration data to the policy database and supplies provider configuration.

policy inquiry

A type of policy analysis that allows console users to ask questions about how an authorization policy responds to specific access requests.

policy verification

A type of policy analysis that allows console users to ask about contradictions in the authorization policy for a user, group or role.

principal

The identity assigned to a user, group or system process as a result of authentication. A principal can consist of any number of users and groups. Principals are typically stored within subjects.

principal validation

The act of signing and later verifying that a principal was not altered since it was signed. Principal validation establishes trust of principals.

privacy

The right an entity, acting in its own behalf, to determine the degree to which it interacts with its environment, including the degree to which the entity shares information about itself with others.

private key

An encryption/decryption key known only to the party or parties that exchange secret messages. It is called private because it must be kept secret from everyone but the owner. Private keys use an algorithm or computational procedure to encode or encrypt ciphertext. Data encrypted with the private key can only be decrypted by the public key.

private key algorithm

The computational procedure used to encode or encrypt ciphertext. Data encrypted with the private key can only be decrypted by the public key.

privilege

An action permitted or denied in the context of the authorization policy.

privilege group

A collection of related privileges for organizational purposes.

programmatic security

Application security checks that are performed in the application by calling explicit methods rather than by being handled by the container.

provisioning, user

The creation, modification, deletion, suspension or restoration of identity, profile, policy and configuration attributes, within the scope of a defined business process or interaction.

An identity management technique focused on the automatic management of resources, such as accounts, passwords, business partners, and authorization policy in heterogeneous applications and application infrastructure. The automation, driven off of business and corporate policies governing when resources are allocated and revoked, allows employees and business partners to become productive quickly without waiting for costly, slow and error-prone manual processes.

public key

Value provided by a certificate authority as an encryption/decryption key that, combined with a private key, can be used to effectively encrypt and decrypt messages and digital signatures. The key is called public because it can be made available to anyone. Public key cryptography is also called asymmetric cryptography because different keys are used to encrypt and decrypt the data. See asymmetric key cryptography.

public key algorithm

The computational procedure used to encode or encrypt plain text. Data encrypted with the public key can only be decrypted by the private key.

Q

R

relative name

A shorthand name that you may use in situations where the product can infer the fully-qualified name.

resource

A hierarchal collection of unique identifiers typically representing an application or application component that you protect through your authorization policy; however, a resource can be any entity to which you can control access.

resource attribute

An attribute associated with a resource.

resource converter

A plugin to convert context data to a consistent internal resource format. These plug-in functions extend the capabilities of the existing providers. You can use these to manipulate existing policy data in a way that is not already provided or to retrieve data from external sources to add to an authorization or role mapping decision or a deployment audit.

resource node

A named entity in the hierarchy that represents a component of an application over which you want to control access.

resource, virtual

Virtual resources are not defined as part of the resource hierarchy. When you designate a resource as "supporting virtual," any resource below it is protected by the same policy as its parent. An example of this would be a URL such as http://www.myname.com/private/dir1/dir2/. You could create the resources up to http://www.myname.com/private, and then make private a supporting virtual resource so that dir1/dir2 are automatically protected without needing to create additional explicit resources.

response attributes

A list of the attributes you want to extract from a directory entry, when a request is made. Return attributes provide a mechanism for allowing the authorization provider to pass arbitrary information back through the framework to the caller. The use of this information is typically application specific. One common use case is for personalization.

role inheritance

A quality where a user or group inherits all the roles based on its group membership, either directly or indirectly through its parent.

role mapping

Process by which the users or groups are compared against a condition to determine whether or not they should be dynamically granted a role. Role mapping occurs at runtime, just prior to when an access decision is rendered for a protected resource.

role mapping provider

A security provider that determines what roles apply to the principals stored in a subject when the subject is attempting to perform an operation on a resource. Because this operation usually involves gaining access to the resource, role mapping providers are typically used with authorization providers.

runtime class

Java class that implements a Security Service Provider Interface (SSPI) and contains the actual security-related behavior for a security provider.

S

Secure Sockets Layer (SSL)

An Internet transport-level technology developed by Netscape to provide data privacy between applications. Generally, Secure Sockets Layer (SSL) provides (1) a mechanism that the applications can use to authenticate each other's identity and (2) encryption of the data exchanged by the applications. SSL supports the use of public key cryptography for authentication, and secret key cryptography and digital signatures to provide privacy and data integrity.

Security Assertion Markup Language (SAML)

An XML-based framework for exchanging security information. This security information is expressed in the form of assertions about subjects, where a subject is an entity (human, business, application, or computer) with an identity in some security domain (for more information, see http://xml.coverpages.org/saml.html). You can develop custom Identity Assertion providers that support different token types, including SAML.

security configuration

A set of security providers configured to use with a specific Security Service Module bound to a specific Service Control Manager.

Security Framework

See AquaLogic Enterprise Security Framework.

security provider

Any of the providers supplied with a Security Service Module or one custom designed and configured by a development organization or third party. A security provider consists of runtime classes created from SSPIs, respectively. Such providers are developed using the Security Service Provider Interfaces (SSPIs) and the Java API. They are used to provide services to applications; these services include authentication, authorization, auditing, role mapping and credential mapping. See Security Service Provider Interfaces (SSPIs).

security service

A processing or communication service that is provided by a system to give a specific kind of protection to system resources. Security services implement security policies and are implemented by security mechanisms.

Security Service Provider Interfaces (SSPIs)

Set of packages that allow developers and third-parties to create custom security providers to be integrated with the product. These interfaces are implemented by both the AquaLogic Enterprise Security providers and custom security providers. The security framework calls methods in these interfaces to perform security operations.

single sign-on

Ability to require a user to sign on to an application only once and gain access to many different application components in a DNS domain, even though these components have their own authentication schemes. Single sign-on is achieved using identity assertion, LoginModules, and tokens.

SSL tunneling

Tunneling Secure Socket Layer (SSL) over an IP-based protocol. Tunneling means that each SSL record is encapsulated and packaged with the headers needed to send the record over another protocol.

static credential

An instance of a given type, either a built-in type or a user-defined type, that has its value set in a policy. Static credentials are user, group, and resource attributes.

structural change

A change to a resource and identity directory that you must deploy before it takes affect. That is, certain changes that you make to a resource and identity directory are not implemented until they are distributed.

subject

A grouping of related information for a single entity, such as a person, as specified by the Java Authentication and Authorization Service (JAAS). The related information includes the Subject's identities, or Principals, as well as its security-related attributes (for example, passwords and cryptographic keys). A subject can contain any number of Principals. Both users and groups can be used as Principals by application servers such as WebLogic Server. In security providers supplied, the Subject contains a Principal for the user (`WLSUser Principal`) and a Principal for each group of which the user is a member (`WLSGroups Principals`). Custom security providers can store identities differently.

symmetric key cryptography

A key-based cryptography that uses an encryption algorithm in which the same key is used both to encrypt and decrypt the data. Symmetric key cryptography is also called secret key cryptography.

T

token

Artifact generated as part of the authentication process of users or system processes. When using Identity Assertion, a token is presented to show that the user was authenticated. Tokens come in many different types, including Kerberos and Security Assertion Markup Language (SAML).

Trust Manager

An interface that enables you to override validation errors in a peer's digital certificate and continue the SSL handshake. You can also use the interface to discontinue an SSL handshake by performing additional validation on a server's digital certificate chain.

trusted (root) certificate authority

A trusted third-party organization or company that issues digital certificates used to create digital signatures and public-private key pairs. The function of the trusted certificate authority is similar to that of a notary public: to guarantee the identity of the individual or organization presenting the certificate. Trusted certificate authorities issue certificates used to sign other certificates. Certificate authorities are referred to as root certificate authorities because their authority is recognized and thus they do not need anyone to validate their

identity. Trusted (root) certificate authority (CA) certificates are installed in applications that authenticate certificates. For example, web browsers are usually distributed with several trusted (root) CA certificates pre-installed. If the server certificate is not signed by a certificate authority and you want to ensure that the server's certificate is authenticated by the client, it is good practice for the server to issue a certificate chain that terminates with a certificate that is signed by a certificate authority.

two-way SSL authentication

Authentication that requires both the client and server to present a certificate before the connection thread is enabled between the two. With two-way SSL authentication, BEA AquaLogic Enterprise Security not only authenticates itself to the client (which is the minimum requirement for certificate authentication), but also requires authentication from the requesting client. Clients are required to submit digital certificates issued by a trusted certificate authority. This type of authentication is useful when you must restrict access to trusted clients only. Two-way SSL authentication is a form of mutual authentication.

type declaration

One of the four declaration types. A type is a class or group of values from which you can create credential declarations, represented as variables.

U

user

A subject that represents a person who is granted or denied privileges to resources through your authorization policy and who can be authenticated through an authentication service. A user can be a person or a software entity, such as a Java client. Each user is given a unique identity within an identity directory. For more efficient security management, BEA recommends adding users to groups, and then associating groups with roles. A group is a collection of users who have something in common, such as working in the same department in a company or performing the same tasks. Users can be placed into groups that are associated with roles or they can be directly associated with roles.

user attribute

See identity attribute.

V

Virtual Resources

In addition to the resources that you define in the resource tree, you have the option of defining virtual resources, which do not appear in the resource tree. This feature offers some

flexibility as to the levels of resource hierarchy that must be included in the resource tree so that protections can be assigned.

To define a virtual resource, select a resource on the resource tree and configure it as “supporting virtual.” Once you configure a resource as "supporting virtual," any resources below it, that is, its child resources, are, in effect, virtual resources and are protected by the same policies as their parent, even though they do not appear in the resource tree. For example, given a resource hierarchy URL such as `http://www.myname.com/private/dir1/dir2/`, if you create the resource tree up to `http://www.myname.com/private` and then configure `private` as “supporting virtual,” `dir1` and `dir2` are automatically protected by the protections you assign to `private`, without having to add them as explicit resources on the resource tree or assigning them explicit protection.

W

WebLogic Portal

An enterprise portal platform that simplifies the development of custom-fit portals. A unified portal framework is provided to enable the creation of managed network portals.

Tools for the developer and administrator help in the management of the portal lifecycle. Applications are enhanced with the portal business services, including content management, personalization, commerce, and collaboration.

wildcard characters

Special text characters that represent an unknown character or characters in some text. The most common wildcard characters are `*` and `?`. Wildcard characters are used to search for specific strings of text and setting console properties.

WS-Security (WSS)

A specification that describes enhancements to SOAP messaging to provide the quality of protection through message integrity, message confidentiality, and single message authentication, along with a general-purpose mechanism for associating security tokens with messages. The mechanisms defined in the specification can be used to accommodate a wide variety of security models and encryption technologies, as well as support for multiple security token formats. The OASIS Technical Committee has defined a set of profiles that describe bindings for encoding popular security tokens, including Kerberos, SAML, and X.509 digital certificates. These profiles describe how the particular security token is formatted and transferred to provide interoperable identity propagation.

X

XML Digital Signatures (XMLDSIG)

A specification that defines an XML schema for cryptographically authenticating data through the use of digital signatures. The authenticated data may consist of a complete XML document, individual elements in an XML document, or an external data object referenced by an XML document. The XML Digital Signatures specification is in W3C recommendation status, is the basis for a number of XML security standards, and plays a prominent role in providing security to web services.

XML Encryption (XMLENC)

A specification that defines an XML schema for encrypting data. The encrypted data may consist of a complete XML document, individual elements in an XML document or an external data object referenced by an XML document.

XML Key Management (XKMS)

Provides trusted web-based services for managing cryptographic keys. The current W3C [XKMS] specification separates the XML Key Management Services into three separate services:

XML Key Information Service (X-KISS) provides services used by a party relying on a cryptographic key. Services are divided into three tiers: retrieval (tier 0), location (tier 1), and validation (tier 2).

XML Key Registration Service (X-KRSS) provides services used by the holder of a cryptographic key. These services include registration, revocation, reissue, and key recovery.

Bulk Key Registration (X-Bulk) is an extension of X-KRSS that allows bulk registration of cryptographic keys for hardware manufacturing applications.

The XKMS X-KISS tier 1 service can be used to retrieve the digital certificate for an identity that could then be carried in an XML Digital Signature. This signature could be part of the security header defined for use by the Web Services Specification. The X-KISS tier 2 service could be used to validate a digital certificate carried in a Web Services Security header or XML Digital Signature. The validation of the digital certificate would include checking whether the digital certificate has been revoked.