Sun Java™ System

Sun Java Enterprise System Glossary

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 816-6873-13

Sun Java Enterprise System Glossary

This glossary identifies terms and definitions for Java Enterprise System. Parts of speech are abbreviated “adj.” for adjectives, “n.” for nouns, and “v.” for verbs.

access control (n.) The means of securing a server by controlling access to the server.

access control entry See *ACE*.

access control instruction See *ACI*.

access control list See *ACL*.

access control rules (n.) Rules specifying user permissions for a given set of directory entries or attributes.

access domain (n.) A domain that limits access to certain Messaging Server operations from within a specified domain. For example, an access domain can be used to limit where mail for an account can be collected.

access rights (n.) Access rights specify the level of access control granted or denied. Access rights are related to the type of operation that can be performed on the directory. The following rights can be granted or denied: read, write, add, delete, search, compare, selfwrite, proxy, and all.

account (n.) Information that defines a specific user or user group. This information includes the user name or group name, valid email address or addresses, and how and where email is delivered.

account inactivation (n.) The disabling of a single user account, or set of accounts, so that all authentication attempts are automatically rejected.

ACE (access control entry) (1) (n.) A single item of information from an access control list. Also called access control information.

(2) (n.) A hierarchy of rules that the web server uses to evaluate incoming access requests.

(3) (n.) A string that provides access control for calendars, calendar properties, and calendar components such as events and tasks.

ACI (access control instruction) (n.) An instruction that grants or denies permissions to entries in the directory.

ACL (access control list) (1) (n.) The mechanism for controlling access to your directory. In Directory Server, an ACL is an ACI attribute in a directory entry.

(2) (n.) A collection of ACEs. An ACL is a mechanism for defining which users have access to your server. You can define ACL rules that are specific to a particular file or directory, granting or denying access to one or more users and groups.

(3) (n.) A set of ACE strings that collectively provide access control for calendars, calendar properties, and calendar components such as events and tasks.

(4) (n.) A set of data associated with a directory that defines the permissions that users, groups or users and groups have for accessing the directory. An ACL is composed of one or more ACE strings.

account federation (n.) A process that occurs when a user chooses to unite distinct service provider accounts with identity provider accounts. Users retain their individual account information with each provider while simultaneously establishing a link that allows the exchange of authentication information between provider accounts. Also called identity federation.

accumulated patch (n.) A patch which combines the fixes from a previous patch (or patches), any previous versions of the same patch and the current set of fixes being released.

activation (n.) The process of transferring an enterprise bean's state from secondary storage to memory.

active boot environment (n.) The environment that is currently up and running.

active node (n.) An HADB node that contains session data. If an active node fails, a spare node copies data from the mirror node and becomes active. See also *HADB node*, *spare node*, *mirror node*, and *data redundancy unit*.

address (1) (n.) Information in an email message that determines where and how the message must be sent. Addresses are found both in message headers and in message envelopes. Envelope addresses determine how the message gets routed and delivered. Header addresses are present merely for display purposes.

(2) (n.) In networking, unique code that identifies a node to the network. Names like `example.corp.com` are translated to "dotted quad" addresses (168.124.0.0) by the DNS.

address handling (n.) The actions performed by the MTA to detect errors in addressing, to rewrite addresses if necessary, and to match addresses to recipients.

addressing protocol (n.) The addressing rules that make email possible. RFC 822 is the most widely used protocol on the Internet and the protocol supported by Messaging Server. Other protocols include X.400 and UUCP.

address token (n.) The address element of a rewrite rule pattern.

admin console (n.) The administrator's Directory Server Access Management Edition GUI interface to Portal Server 6.0.

administered objects (n.) A pre-configured Java Enterprise System object (a connection factory or a destination) created by an administrator for use by one or more JMS clients.

The use of administered objects isolates Java™ Message Service (JMS) clients from the proprietary aspects of a provider. These objects are placed in a Java Naming and Directory Interface™ (JNDI) namespace by an administrator and are accessed by JMS clients using JNDI lookups.

administration console See *console*.

administration domain (n.) A region of administrative control. See also *document type definition*.

administration interface (n.) The set of browser-based forms used to configure and administer a Java™ Enterprise System server. See also *CLI*.

administration privileges (n.) A set of privileges that define a user's administrative role.

administration server (n.) An application server instance dedicated to providing the administrative functions of the Java Enterprise System Directory Server.

administration server administrator (n.) A user who has administrative privileges to start or stop a server even when there is no Java Enterprise System Directory Server connection. The administration server administrator has restricted server tasks (typically only Restart Server and Stop Server) for all servers in a local server group. When an administration server is installed, this administrator's entry is automatically created locally. This administrator is not a user in the user directory.

administrative console (n.) A workstation that is used to run cluster administrative software.

administrative domain (n.) A feature within the Java Enterprise System Application Server that allows different administrative users to create and manage their own domains. A domain is a set of instances created using a common set of installed binaries in a single system. See also *domain*.

administrator (n.) A user with a defined set of administrative privileges. See also *configuration administrator*, *Directory Manager*, *administration server*, *server administrator*, *top-level administrator*, *domain administrator*, *organization administrator*, *family group administrator*, *mail list owner*.

admpw (n.) The user name and password file for the Sun Enterprise™ Administrator Server superuser.

adoption scenario An overall reason for deploying Java Enterprise System software, characterizing the software system you start with and the goal you are trying to achieve. There are four basic Java Enterprise System adoption scenarios: new system, replacement, extension, and upgrade.

affiliation (n.) An affiliation is a group of providers formed without regard to their particular authentication domain. It is formed and maintained by an affiliation owner. An affiliation document describes a group of providers collectively identified by their providerID. Members of an affiliation may invoke services either as a member of the affiliation (by virtue of their Affiliation ID) or individually (by virtue of their Provider ID).

agent (n.) Software that runs the network-management software in a network device, such as a router, host, or X terminal. See also *intelligent agent*.

alarm event (n.) An event generated and sent by the Calendar Server ENS. When an alarm event occurs, a message reminder is sent to specific recipients.

alert (n.) Time-critical messages that users instantly receive in a pop-up window. The sender knows who has received the message and is notified that the message is read when the alert is either closed or clicked, as long as the "Show message status" option was used. If the alert message requires a response, right clicking on the alert brings up a contextual menu with an option to Chat with Sender.

alias (n.) An alternate name of an email address.

alias file (n.) A file used to set aliases not set in a directory, such as the postmaster alias.

aliasing (n.) Substituting one item for another in the Java Enterprise System Portal Server Search Engine which uses aliasing when importing resource descriptions from another Search Engine that has a different schema.

All IDs threshold (n.) A size limit that is globally applied to every index managed by the Java Enterprise System Directory Server. When the size of an entry ID list reaches this limit, the server replaces that entry ID list with an All IDs token.

All IDs token (n.) A mechanism that causes the server to assume that all directory entries match the index key. In effect, the All IDs token causes the Java Enterprise System Directory Server to perform an unindexed search to match the index key.

allowed attributes (n.) Optional attributes that can be present in entries using a particular object class. See also *attribute*, *required attributes*.

Allow filter (n.) A Java Enterprise System Messaging Server access-control rule that identifies clients that are to be allowed access to one or more POP, IMAP, or HTTP services. See also *deny filter*.

alternate address (n.) A secondary address for an account, generally a variation on the primary address. In some cases, it is convenient to have more than one address for a single account.

alternate root (n.) The location of the `root` file system on a client on which a package is installed. The alternate root is normally supplied by using `pkgadd -R`.

AML (abstract markup language) (n.) A mobile device markup language that is independent of specific vendors or models.

amnesia (n.) A condition in which a cluster restarts after a shutdown with stale *category*. For example, on a two-node cluster with only node 1 operational, if a cluster configuration change occurs on node 1, node 2's CCR becomes stale. If the cluster is shut down and then restarted on node 2, an amnesia condition results because of node 2's stale CCR.

anonymous access (n.) Access, when granted, that allows anyone to access directory information without providing credentials and regardless of the conditions of the bind.

API (application programming interface) (1) (n.) A set of instructions that a computer program can use to communicate with other software or hardware that is designed to interpret that API.

(2) (n.) A set of calling conventions or instructions defining how programs invoke services in existing software packages.

APOP (authenticated post office protocol) (n.) Similar to POP, but instead of using a plaintext password for authentication, APOP uses an encoding of the password together with a challenge string.

applet (n.) A small application written in the Java™ programming language that runs in a web browser. Typically, applets are called by or embedded in web pages to provide special functionality. A Java applet is a small application program written in the Java™ programming language that can be sent along with a web page to a user's browser. Java applets can perform tasks without having to send a user request back to the server. Instant Messaging client is a Java applet. See also *servlet*.

application client container See *container*.

application component A custom-developed software *component* that performs some specific computing function, providing *business services* to *end users* or to other application components. An application component usually conforms to a distributed component model (such as CORBA and the J2EE™ platform). These components, singly or combined, can be encapsulated as *web services*.

application server (n.) A software platform upon which business applications are run. Application servers typically provide high-level services to applications, such as component life cycle, location, and distribution and transactional resource access.

application service (n.) A component or component assembly that performs business logic on behalf of multiple clients and must therefore be a multithreaded process. An application service can also be a component or component assembly encapsulated as a web service or a stand-alone content server.

application tier (n.) A conceptual division of a J2EE application:

client tier: The user interface. End users interact with client software (such as a web browser) to use the application.

server tier: The business logic and presentation logic that make up your application, defined in the application's components.

data tier: The data access logic that enables your application to interact with a data source.

approximate index (n.) An index that allows for efficient approximate or "sounds-like" searches across the directory information tree.

architecture A design that shows the logical and physical building blocks of a distributed application (or some other software system) and their relationships to one another. In the case of a *distributed enterprise application*, the architectural design generally includes both the application's *logical architecture* and *deployment architecture*.

A record (n.) A type of DNS record containing a host name and its associated IP address. An A record is used by messaging servers on the Internet to route email. See also *domain name system*, *MX record*.

assembly (n.) The process of combining discrete components of an application into a single unit that can be deployed. See also *deployment*.

asynchronous communication (n.) A mode of communication in which the sender of a message need not wait for the sending method to return before the sender continues with other work.

attribute (1) (n.) A name-value pair in a request object that can be set by a servlet. Also a name-value pair that modifies an element in an XML file. See also *parameter*. More generally, an attribute is a unit of metadata.

(2) (n.) A name-value pair that holds descriptive information about an entry. Attributes have a type (name) and a set of values. An attribute type also specifies the syntax for the kind of information that can be stored as values of attributes of that type.

(3) (n.) Defines the parameters that a Java Enterprise System Directory Server Access Management Edition service provides to an organization. The attributes that make up a Java Enterprise System Directory Server Access Management Edition service are classified as one of the following: Dynamic, Policy, User, Organization, or Global. Using these types to subdivide the attributes in each service allows for a more consistent arrangement of the service schema and easier management of the service parameters.

attribute provider (n.) An attribute provider is a web service that hosts attribute data.

attribute list See *optional attribute list* and *request object*.

auditing (n.) The method or methods by which significant events are recorded for subsequent examination, typically in error or security breach situations.

AUTH (n.) An SMTP command enabling an SMTP client to specify an authentication method to the server, perform an authentication protocol exchange, and, if necessary, negotiate a security layer for subsequent protocol interactions.

authenticating Directory Server (n.) In PTA, the authenticating Java Enterprise System Directory Server contains the authentication credentials of the requesting client. A PTA-enabled user directory passes through bind requests to the authenticating directory, which verifies the bind credentials of the requesting client.

authentication (1) (n.) The process of determining whether someone or something is who or what it is declared to be. In private and public computer networks, including the Internet, authentication is commonly done through the use of login passwords. Knowledge of the password is assumed to guarantee that the user is authentic.

(2) (n.) The process of proving the identity of the client user to the Java Enterprise System Directory Server. Users must provide a bind DN and either the corresponding password or certificate in order to be granted access to the directory. Java Enterprise System Directory Server allows the user to perform functions or access files and directories based on the permissions granted to that user by the directory administrator. See also *server authentication*.

authentication certificate (n.) A digital file sent from server to client or client to server to verify and authenticate the other party. The certificate ensures the authenticity of its holder, the client or server. Certificates are not transferable.

authentication domain (n.) A group of service providers with at least one identity provider that agrees to exchange user authentication information using the Liberty Alliance Project (LAP). Once a *circle of trust* is established, single sign-on authentication is enabled between all the providers. Also called a circle of trust.

authorization (n.) The process of granting specific access privileges to a user. Authorization is based on authentication and enforced by access control.

automatic failback (n.) A process of returning a resource group or device group to its primary node after the primary node has failed and later is restarted as a cluster member. See also *switchback*.

autoreply option file (n.) A file used for setting options for email autoreply, such as vacation notices.

AutoReply utility (n.) A utility that automatically responds to messages sent to accounts with the AutoReply feature activated. Every account in Java Enterprise System Messaging Server can be configured to automatically reply to incoming messages.

availability service (n.) The Sun Java System Application Server feature for enabling high availability on the server instance, web container, EJB container, and also for RMI/IIOP requests.

backbone (n.) The primary connectivity mechanism of a distributed system. All systems that have connectivity to an intermediate system on the backbone are connected to each other. A backbone does not prevent you from setting up systems to bypass the backbone for reasons of cost, performance, or security.

back-end server (n.) In the context of Java Enterprise System Messaging Server, an email server whose only function is to store and retrieve email messages. Also called a message store server.

backout (n.) The removal of a software change (a patch, for example), which results in returning the system to its previous state.

back up (v.) To copy the contents of folders from the message store to a backup device. See also *restore*.

backup group See *network adapter failover group*.

backup store (n.) A repository for data, typically a file system or database. A backup store can be monitored by a background thread (sweeper thread) to remove unwanted entries.

banner (n.) A text string displayed by a service such as IMAP when a client first connects to it.

base DN (base distinguished name) (n.) An entry in the DIT. A search operation can be performed on the entry identified by the base DN, the entries that are immediately subordinate to the base DN, or to the entry and all entries below the base DN in the *DIT*.

bean-managed persistence (n.) Data transfer between an entity bean's variables and a data store. The data access logic is typically provided by a developer using Java™ Database Connectivity (JDBC™) software or other data access technologies. See also *container-managed persistence*.

bean-managed transaction (n.) Where transaction demarcation for an enterprise bean is controlled programmatically by the developer. See also *container-managed transaction*.

Berkeley DB (Berkeley database) (n.) A transactional database store intended for high-concurrency read-write workloads and for applications that require transactions and recoverability. Java Enterprise System Messaging Server uses Berkeley databases for numerous purposes.

bind DN (bind distinguished name) (n.) Distinguished name used to authenticate to a Java Enterprise System Directory Server in the bind request.

bind rule (n.) In the context of access control, the bind rule specifies the credentials and conditions that a particular user or client must satisfy in order to get access to directory information.

BLOB (binary large object) (n.) A data type used to store and retrieve complex object fields. BLOBs are binary or serializable objects, such as pictures, that translate into large byte arrays, which are then serialized into container-managed persistence fields.

BMP See *bean-managed persistence*.

BMT See *bean-managed transaction*.

body (n.) One part of an email message. Although headers and envelopes must follow a standard format, the body of the message has a content determined by the sender. The body can contain text, graphics, or multimedia. Structured bodies follow the MIME standard.

boot environment (n.) A bootable Solaris environment which consists of a set of disk slices, associated mount points and file systems. The disk slices might be on t he same disk or be distributed across multiple disks.

broker (n.) The Message Queue entity that manages Java™ Message Service (JMS) API message routing, delivery, persistence, security, and logging. Provides an interface that allows an administrator to monitor and tune performance and resource use.

browsing (n.) Within Java Enterprise System Portal Server, refers to looking through the categorical divisions of the resources in a Search database.

browsing index See *virtual list view index*.

building module (n.) A hardware or software construct with limited or no dependencies on shared services. A specific configuration that provides optimum performance and horizontal scalability.

business logic (n.) The code that implements the essential business rules of an application rather than data integration or presentation logic.

business service An *application component* or component assembly that performs business logic on behalf of multiple clients (and is therefore a multi-threaded process). A business service can also be an assembly of distributed components encapsulated as a *web service*, or it can be a standalone *server*.

CA (certificate authority) (1) (n.) An internal or third-party organization that issues digital files used for encrypted transactions.

(2) (n.) An authority in a network that issues and manages security credentials and public keys for message encryption and decryption. As part of a PKI, a CA checks with a registration authority to verify information provided by the requestor of a digital certificate. If the registration authority verifies the requestor's information, the CA can then issue a certificate. See also *PKI*.

cache (n.) A copy of original data that is stored locally. Cached data does not have to be retrieved from a remote server again when requested.

Cache Control Directive (n.) A way for Java Enterprise System Application Server to control what information is cached by a proxy server. Using cache control directives, you override the default caching of the proxy to protect sensitive information from being cached and perhaps retrieved later. For these directives to work, the proxy server must comply with HTTP 1.1.

cached rowset (n.) An object that permits you to retrieve data from a data source and then detach from the data source while you examine and modify the data. A cached row set keeps track both of the original data retrieved and any changes made to the data by your application. If the application attempts to update the original data source, the row set is reconnected to the data source, and only those rows that have changed are merged back into the database.

calendar access protocol See *CAP*.

Calendar Express (n.) A web-based calendar client program that provides access to the Calendar Server for end users.

calendar group (n.) A collection of several calendars to help a user manage more than one calendar.

calendar ID (n.) A unique identifier associated with a calendar in the Java Enterprise System Calendar Server database. Also known as `calid`.

calendar lookup database See *CLD*.

Calendar Server application programming interface See *CSAPI*.

calendar user agent See *CUA*.

callable statement (n.) A class that encapsulates a database procedure or function call for databases that support returning result sets from stored procedures.

CAP (calendar access protocol) (n.) A standard Internet protocol for calendaring based on requirements identified by the Internet Engineering Task Force (IETF).

capability (n.) A string provided to clients that defines the functionality available in a given IMAP service.

cascading replication (n.) In a cascading replication scenario, one server, often called the hub supplier, acts both as a consumer and a supplier for a particular replica. The server holds a read-only replica and maintains a change log. The server receives updates from the supplier server that holds the master copy of the data and, in turn, supplies those updates to the consumer.

catalog See *index*.

cataloging See *indexing*.

category (n.) A logical grouping of resources in the Search database. Collectively, a set of categories is sometimes called a taxonomy.

CCPP (composite capability and preference profiles) (n.) For Portal Server Mobile Access software, a specification that is used for the User Agent Profile and preconfigured data for client detection. The CCPP specification describes the capabilities of devices and user preferences.

CCR (cluster configuration repository) (n.) A highly available, replicated data store that is used by Sun™ Cluster software to persistently store cluster configuration information.

cHTML (n.) A simplified version of HTML suitable for mobile devices.

certificate (1) (n.) An electronic document used to identify an Instant Messaging Server and associated with a public key. Java Enterprise System Instant Messaging Server supports the exchange of certificates between Instant Messaging servers. The certificate exchange is transparent to individual users.

(2) (n.) Digital data that specifies the name of an individual, company, or other entity and certifies that the public key included in the certificate belongs to that entity. Both clients and servers can have certificates.

(3) (n.) A certificate strongly associates the public key of a user or CA with the identity, typically a distinguished name, of that user or CA. The certificate is digitally signed by a CA, and can be validated during an SSL connection setup to obtain the public key of the other end of the connection. X.509 certificates are stored within the directory in the `caCertificate;binary` or `userCertificate;binary` attributes.

certificate authority See *CA*.

certificate-based authentication (n.) Identification of a user from a digital certificate submitted by the client. See also *password authentication*.

certificate database (n.) A file that contains a server's digital certificate or certificates. Also called a certificate file.

certificate name (n.) The name that identifies a certificate and its owner.

certificate revocation list See *CRL*.

CGI (common gateway interface) (n.) An interface by which external programs communicate with the HTTP server. Programs that are written to use CGI are called CGI programs or CGI scripts. CGI programs handle forms or parse output the server does not normally handle or parse.

chained suffix (n.) An implementation of chaining. A chained suffix behaves like a normal suffix but has no persistent storage. Instead, a chain suffix points to data stored remotely. See also *chaining*.

chaining (n.) A method for relaying requests to another server. Results for the request are collected, compiled, and then returned to the client. In the context of replication, chaining occurs when a consumer replica receives an update request and forwards the request to the server that holds the corresponding master replica. Note that this process is not the same as a referral. See also *chained suffix*.

change log (n.) A change log is a record of the modifications that have occurred on a replica. The supplier server then replays these modifications on the replicas stored on consumer servers or on other masters, in the case of multimaster replication. Note that this is not the same as the retro changelog, which is not used for replication.

channel (1) (n.) The fundamental MTA component that processes a message. A channel represents a connection with another computer system or group of systems. Each channel consists of one or more channel programs and an outgoing message queue for storing messages that are destined to be sent to one or more of the systems associated with the channel. See also *channel block*, *channel host table*, *channel program*.

(2) (n.) In the Java Enterprise System Portal Server Desktop, a channel consists of a provider and configuration. Channels generate content that can consist of markup fragments, a frameset, an HTML page, and so on. Channel content is often aggregated with other channel content to form a Portal Desktop.

channel block (n.) A single channel definition. See also *channel host table*.

channel host table (n.) The collective set of channel definitions. See also *channel block*.

channel program (n.) Part of a channel that transmits messages to remote systems and deletes messages from the queue after they are sent and accepts messages from remote systems placing them in the appropriate channel queues. See also *master channel program*, *slave channel program*.

character type (n.) An attribute that distinguishes alphabetic characters from numeric or other characters and the mapping of uppercase to lowercase letters.

chat (n.) Instant Messaging's version of instant messaging. Chat is a real-time conversation capability. Chat sessions are held either in chat rooms created on an as-needed basis or in pre-established conference rooms.

checkpoint (n.) The notification sent by a primary node to a secondary node to keep the software state synchronized between them. See also *primary* and *secondary*.

child (n.) A category that is a subcategory of another category. See also *category*.

chroot (n.) An additional root directory you can create to limit the server to specific directories. You would use this feature to safeguard an unprotected server.

cipher (n.) A cipher is a cryptographic algorithm (a mathematical function) used for encryption or decryption.

ciphertext (n.) Encrypted information that cannot be read by anyone without the proper key to decrypt the information.

circle of trust (n.) See *authentication domain*.

CKL (compromised key list) (n.) A list of key information about users who have compromised keys. The CA also provides this list. [additional definition from "compromised key list" term. See also *CRL*.

class definition (n.) A definition specifies the information needed to create an instance of a particular object.

classic CoS (n.) Identifies the template entry by its DN and the value of one of the target entry's attributes.

classification rules (n.) A set of rules used to assign resources to a category or to several categories.

classloader (n.) A Java™ technology-based component responsible for loading Java classes according to specific rules. See also *classpath*.

class of service See *CoS*.

classpath (n.) A path that identifies directories and Java™ Archive (JAR) files where Java classes are stored. See also *classloader*.

CLD (Calendar Lookup Database) (n.) A plug-in that determines the physical location of a calendar when the calendar database is distributed over two or more back-end servers. Calendar Server provides the LDAP CLD plug-in and the algorithmic CLD plug-in.

cleartext (n.) Unencrypted text.

CLI (command-line interface) (n.) An interface that enables you to type executable instructions at a user prompt. See also *administration interface*.

client Software that requests software *services*. (Note: this is not a person—see *end user*.) A client can be a service that requests another service, or a GUI component accessed by an end user.

client authentication (n.) The process of authenticating client certificates by cryptographically verifying the certificate signature and the certificate chain leading to the CA on the trust CA list. See also *authentication*, *certificate authority*.

client contract (n.) A contract that determines the communication rules between a client and the EJB™ container, establishes a uniform development model for applications that use enterprise beans, and guarantees greater reuse of beans by standardizing the relationship with the client.

client conditional properties (n.) Properties of Portal Server Mobile Access client types that enable administrators to specify properties for a channel or container channel for a given client.

client database (n.) For Portal Server Mobile Access, a database that consists of an internal and an external library. The internal library contains all default mobile device data definitions. The external library contains customized client data definitions that override definitions in the internal library.

client detection (n.) An Access Manager process which determines the capabilities and characteristics of each mobile device that accesses the portal.

Client Editor (n.) An Access Manager interface that enables you to create a client type and to manage client properties. The Client Editor interface is accessible from the Access Manager console.

client identifier (n.) An identifier that associates a connection and its objects with a state maintained by the Java Enterprise System message server on behalf of the client.

Client Manager (n.) An Access Manager interface accessible from the console that enables you to manage client types and properties.

client profile (n.) An Access Manager profile that identifies each client.

***client runtime** See Java Enterprise System client runtime.

client-server model (n.) A computing model in which networked computers provide specific services to other client computers. Examples include the name-server and name-resolver paradigm of the DNS and file-server/file-client relationships such as NFS and diskless hosts.

***client type** (n.) An entry in the Access Manager client database.

clientType (n.) A property which refers to a name that provides a unique index for Access Manager client data.

cluster (1) (n.) A group of computers connected by a high-speed network that work together as if they were one machine with multiple CPUs. If one of the servers in the cluster fails, its services can failover to an operational server. See also *failover*.

(2) (n.) A group of remote slave administration servers added to and controlled by a master administration server. All servers in a cluster must be of the same platform and have the same userid and password.

(3) (n.) Two or more interconnected nodes or domains that share a cluster file system and are configured together to run failover, parallel, or scalable resources.

(4) (n.) Two or more interconnected brokers that work in tandem to provide messaging services.

cluster configuration repository See *category*.

cluster file system (n.) A cluster service that provides cluster-wide, highly available access to existing local file systems.

cluster interconnect (n.) The hardware networking infrastructure that includes cables, cluster transport junctions, and cluster transport adapters. The Messaging Server and data service software use this infrastructure for intra-cluster communication.

cluster member (n.) An active member of the current cluster incarnation. This member is capable of sharing resources with other cluster members and providing services both to other cluster members and to clients of the cluster. See also *cluster node*.

cluster membership monitor See *CMM*.

cluster node (n.) A node that is configured to be a cluster member. A cluster node might or might not be a current member. See also *cluster member*.

cluster transport adapter (n.) The network adapter that resides on a node and connects the node to the cluster interconnect. See also *cluster interconnect*.

cluster transport cables (n.) The network connection that connects to the endpoints. A connection between cluster transport adapters and cluster transport junctions or between two cluster transport adapters. See also *cluster interconnect*.

cluster transport junction (n.) A hardware switch that is used as part of the cluster interconnect. See also *cluster interconnect*.

CMM (cluster membership monitor) (n.) The software that maintains a consistent cluster membership roster. This membership information is used by the rest of the clustering software to decide where to locate highly available services. The CMM ensures that non-cluster members cannot corrupt data and transmit corrupt or inconsistent data to clients.

CMP See *container-managed persistence*.

CMR See *container-managed relationship*.

CMT See *container-managed transaction*.

cn See *common name attribute*.

CNAME record (n.) A type of DNS record that maps a domain name alias to a domain name.

collation order (n.) Language and cultural-specific information about how the characters of a given language are to be sorted. This information might include the sequence of letters in the alphabet or how to compare letters with accents to letters without accents.

collection (n.) A database that contains information about documents, such as a word list and file properties. Collections are used by the search function to retrieve documents matching specified search criteria.

collocation (n.) The property of being on the same node. This concept is used during cluster configuration to improve performance.

colocate (v.) To position a component in the same memory space as a related component in order to avoid remote procedure calls and improve performance.

column (n.) A field in a database table.

command line interface See *CLI*.

`comm_dssetup.pl` (n.) A Directory Server preparation tool that makes an existing Directory Server ready for use by a Messaging Server.

comment character (n.) A character at the beginning of a line that turns the line into a nonexecutable comment.

commit (v.) To complete a transaction by sending the required commands to the database. See also *rollback*, *transaction*.

common domain (n.) In a *circle of trust* having more than one identity provider, service providers need a way to determine which identity provider a principal uses. Because this function must work across any number of domain name system (DNS) domains, the Liberty approach is to create a domain common to all identity and service providers in the circle. This predetermined domain is known as the common domain. Within the common domain, when a principal has been authenticated to a service provider, the identity provider writes a common domain cookie that stores the principal's identity provider. Now, when the principal attempts to access another service provider within the circle, the service provider reads the common domain cookie and the request can be forwarded to the correct identity provider.

common log file format (n.) The format used by the server for entering information into the access logs. The format is the same among all major servers, including the Web Server.

common name attribute (n.) The `cn` attribute that identifies the person or object defined by the entry in an LDAP directory.

Communication Services (n.) A comprehensive messaging solution that enables the delivery of the integrated email, calendar, instant messaging, and presence information to enterprise customers. The Communication Services core solution consists of Messaging Server, Calendar Server and Instant Messaging Server.

Compass (n.) A search engine service that provided the search capability for Portal Server 3.0. The search engine has been incorporated into the core of Portal Server 6.0. See *Search Engine*.

component (1) (n.) A unit of software logic from which distributed applications are built. A component can be one of the *system components* included in Java Enterprise System or an *application component* that is custom developed. An application component usually conforms to a distributed component model (such as CORBA and the J2EE™ platform) and performs some specific computing function. These components, singly or combined, provide *business services* and can be encapsulated as *web services*.

(2) (n.) A web application, enterprise bean, message-driven bean, application client, or connector. See also *module*.

component contract (n.) A contract that establishes the relationship between an enterprise bean and its container.

component product descriptor file (n.) A file containing metadata for a given component product (usually in XML format).

component state (n.) A set of attributes that describe a calendar event such as a meeting. In WCAP, the `compstate` parameter allows fetch commands to return events by component state. For example, `compstate` might be `REPLY-DECLINED` (attendee has declined a meeting) or `REQUEST_NEEDS-ACTION` (attendee has not taken action on a meeting yet).

compromised key list See *CKL*.

computed attribute (n.) An attribute that are not stored with the entry itself but are returned to the client application along with normal attributes in operation results.

conference room (n.) A pre-established chat room configured by an administrator or other user with `sysRoomsAdd` privilege. The administrator or other user with `sysRoomsAdd` privilege can determine which users can view and access conference rooms.

configuration (n.) The process of tuning the server or providing metadata for a component. Normally, the configuration for a specific component is kept in the component's deployment descriptor file. See also *administrative console*, *deployment descriptor*.

configuration administrator (n.) The person who has administrative privileges to manage servers and configuration directory data in the entire server software topology. The configuration administrator has unrestricted access to all resources in the entire server software topology. This is the only administrator who can assign server access to other administrators. The configuration administrator initially manages administrative configuration until the administrator's group and its members are in place.

Configuration Directory Server (n.) A Java Enterprise System Directory Server that maintains configuration information for a server or set of servers.

configuration file (n.) A file that contains the configuration parameters for a specific component of the Messaging system.

conflict (n.) A situation that arises when changes are made to the same directory data on different directory servers before replication can synchronize the data between the servers. When the servers do synchronize, they detect that their copies are inconsistent and might resolve the conflict or log an error.

conflict resolution (n.) Deterministic procedures used to resolve change information. For more information, see the Java Enterprise System Directory Server Administration Guide.

congestion thresholds (n.) A disk space limit set by the system administrator that prevents the database from becoming overloaded by restricting new operations when system resources are insufficient.

connection (1) (n.)An active connection to a Java Enterprise System message server. The connection can be a queue connection or a topic connection.

connection factory (n.) An object that produces connection objects that enable a J2EE™ component to access a resource. Used to create Java™ Message Service (JMS) connections (TopicConnection or QueueConnection) which allow application code to make use of the provided JMS implementation. Application code uses the Java Naming and Directory Interface™ (JNDI) service to locate connection factory objects using a JNDI name.

connection pool (n.)A group of connections. Allows highly efficient access to a database by caching and reusing physical connections, thus avoiding connection overhead and allowing a small number of connections to be shared between a large number of threads. See also *JDBC™ connection pool*.

connector (n.) A standard extension mechanism for containers to provide connectivity to an EIS. A connector is specific to an EIS and consists of a resource adapter and application development tools for EIS connectivity. The resource adapter is plugged in to a container through its support for system-level contracts defined in the connector architecture.

connector architecture (n.) An architecture for the integration of J2EE™ applications with an EIS. There are two parts to this architecture: an EIS vendor-provided resource adapter and a J2EE server that allows this resource adapter to plug in. This architecture defines a set of contracts that a resource adapter has to support to plug in to a J2EE server, for example, transactions, security and resource management.

console (n.) A GUI that enables you to configure, monitor, maintain, and troubleshoot many server software components.

consume (v.) To receive a message taken from a destination by a message consumer.

consumer (1) (n.) A server containing replicated directory trees or subtrees from a supplier server.

(2) (n.) An object (MessageConsumer) created by a session that is used for receiving messages from a destination. In the point-to-point delivery model, the consumer is a receiver or browser (QueueReceiver or QueueBrowser). In the publish/subscribe delivery model, the consumer is a subscriber (TopicSubscriber).

consumer replica (n.) A replica that refers all add, modify, and delete operations to master replicas. A server can hold any number of consumer replicas of different naming contexts.

contact (n.) The userID (name) of a user or LDAP group with whom you send and receive instant messages. You add contacts to your personalized contact groups so that you can monitor their online status. Also known as buddy in other instant messaging environments.

contact group (n.) A list of contacts that a user maintains. The actual list is stored on the Instant Messaging Server. You can create contact groups to keep track of people in a logical way.

contact list (n.) In Java Enterprise System Instant Messaging, the list of all of your contact groups.

container (1) (n.) An entity that provides life-cycle management, security, deployment, and runtime services to a specific type of J2EE™ component. Java Enterprise System Application Server provides web and EJB™ containers and supports application client containers. See also *component*.

(2) (n.) In Java Enterprise System Portal Server 6.0, a container is a channel that primarily generates its content by aggregating the content of its child channels. In Java Enterprise System Directory Server Access Management Edition, a container defines a type of organizational object that can contain other Directory Server Access Management Edition objects.

container entry (n.) An entry that represents the top of a subtree in the directory.

container-managed persistence (n.) Where the EJB™ container is responsible for entity bean persistence. Data transfer between an entity bean's variables and a data store, where the data access logic is provided by the Java Enterprise System Application Server. See also *bean-managed persistence*.

container-managed relationship (n.) A relationship between fields in a pair of classes where operations on one side of the relationship affect the other side.

container-managed transaction (n.) Where transaction demarcation for an enterprise bean is specified declaratively and automatically controlled by the EJB™ container. See also *bean-managed persistence*.

control descriptor (n.) A set of enterprise bean configuration entries that enable you to specify optional individual property overrides for bean methods, plus enterprise bean transaction and security properties.

conversational state (n.) Where the state of an object changes as the result of repeated interactions with the same client. See also *persistent state*.

cookie (n.) A small collection of information that can be transmitted to a calling web browser, then retrieved on each subsequent call from that browser so the server can recognize calls from the same client. Cookies are domain-specific and can take advantage of the same web server security features as other data interchange between your application and the server. Accepting the cookies allows the web page to load more quickly and is not a threat to the security of your machine.

cooperating server (n.) A server that wants to communicate with your server and a server with which your server wants to communicate. Also known as a coserver. Each cooperating server is given a symbolic name, which is a string consisting of letters and digits, for example, `coserver`*n*, where *n* is a number.

CORBA (common object request broker architecture) (n.) A standard architecture definition for object-oriented distributed computing.

core service (n.) One or more key services that define the basic functionality provided by a Java™ Enterprise System server, as opposed to support services or adjunct services.

CoS (class of service) (n.) A method for sharing attributes between entries.

CoS definition entry (n.) An entry identifies the type of CoS you are using. The entry is stored as an LDAP subentry below the branch it affects.

coserver See *cooperating server*.

CoSNaming provider (n.) To support a global JNDI name space (accessible to IIOP application clients), Java Enterprise System Application Server includes J2EE based CosNaming provider which supports binding of CORBA references (remote EJB™ references).

CoSNaming Service (n.) An an IIOP-based naming service.

CoS template entry (n.) An entry which contains a list of the shared attribute values.

CRAM-MD5 (n.) A lightweight standards track authentication mechanism documented in RFC 2195. It provides a fast (albeit somewhat weaker) alternative to TLS (SSL) when only the user's login password needs to be protected from network eavesdroppers.

crawler See *robot*.

create method (n.) A method for customizing an enterprise bean at creation.

CRL (certificate revocation list) (n.) A list published by a certificate authority that indicates any certificates that either client users or server users should no longer trust. In this case, the certificate has been revoked. See also *CKL*.

cronjob (n.) (UNIX only) A task that is executed automatically by the cron daemon at a configured time. See also *crontab file*.

crontab file (n.) (UNIX only) A list of commands, one per line, that executes automatically at a given time.

CSAPI (Calendar Server application programming interface) (n.) A programmatic interface that provides the capability to modify or enhance the feature set of the Calendar Server. CSAPI modules are plug-ins that are loaded from the `cal/bin/plugins` directory when the Calendar Server is started.

CUA (Calendar user agent) (n.) An application that a calendar client uses to access the Calendar Server.

daemon (n.) (UNIX only) A program that runs in the background, independent of a terminal, and performs a function whenever necessary. Common examples of daemon programs are mail handlers, license servers, and print daemons.

DAP (directory access protocol) (n.) The ISO/ITU-T X.500 protocol that was the basis for LDAP.

data access logic (n.) Business logic that involves interacting with a data source.

database (n.) A generic term for relational database management system (RDBMS). A software package that enables the creation and manipulation of large amounts of related, organized data.

database connection (n.) A communication link with a database or other data source. Components can create and manipulate several database connections simultaneously to access data.

database wire protocol See *DWP*.

data redundancy unit (DRU) (n.) A set of HADB nodes containing half of the active and spare nodes and one complete copy of the data. The HADB is organized into two DRUs, which mirror each other. To ensure fault tolerance, the computers that support one DRU must be completely self-supported with respect to power, processing units, and storage. See also *HADB node*, *active node*, *spare node*, and *mirror node*.

data service (n.) An application that has been instrumented to run as a highly available resource under control of the RGM.

data source (n.) A handle to a source of data, such as a database. Data sources are registered with the Application Server and then retrieved programmatically in order to establish connections and interact with the data source. A data-source definition specifies how to connect to the source of data.

data source object (n.) A data source object has a set of properties that identify and describe the real world data source that it represents.

data store (1) (n.) A store that contains directory information, typically for an entire *DIT*.

(2) (n.) A database where information (durable subscriptions, data about destinations, persistent messages, auditing data) needed by the Message Queue broker is permanently stored.

DC tree (domain component tree) (n.) A *DIT* that mirrors the DNS network syntax. An example of a distinguished name in a DC Tree would be `cn=billbob,dc=bridge,dc=net,o=internet`.

declarative security (n.) Declaring security properties in the component's configuration file and allowing the component's container (for example, a bean's container or a servlet engine) to manage security implicitly. This type of security requires no programmatic control. Opposite of *programmatic security*. See also *container-managed persistence*.

declarative transaction See *container-managed transaction*.

decryption (n.) The process of making encrypted information intelligible. See also *encryption*.

default calendar (n.) The calendar a user first sees after logging into Calendar Express. The calendar ID of a default calendar is the usually same as the user's user ID. For example, `jdoe@example.com` would have a default calendar named `jdoe`.

default index (n.) A set of indexes that is created for each database instance when Directory Server is installed. When Java Enterprise System Directory Server is installed, a set of default indexes is created for each database instance. For more information, see the Java Enterprise System Directory Server Administration Guide.

default master (n.) The default cluster member on which a failover resource type is brought online.

defederation (n.) See *federation termination*.

definition entry See *CoS definition entry*.

defragmentation (n.) The MIME feature that enables a large message that has been broken into small messages or fragments to be reassembled. A Message Partial Content-Type header field that appears in each of the fragments contains information that helps reassemble the fragments into one message. See also *fragmentation*.

delegated administrator console (n.) A web browser-based software console that allows domain administrators to add and modify users and groups to a hosted domain. Also allows end users to change their password, set message forwarding rules, set vacation rules, and list mail list subscriptions.

delegated administrator for messaging and collaboration (n.) A set of interfaces (GUI and utilities) that allow domain administrators to add and modify users and groups on a hosted domain.

delegated administrator server (n.) A daemon program that handles access control to the directory by hosted domains.

delegation (n.) An object-oriented technique for using the composition of objects as an implementation strategy. One object, which is responsible for the result of an operation, delegates the implementation to another object. For example, a classloader often delegates the loading of some classes to its parent.

delete a message (v.) To mark a message for deletion. The deleted message is not removed from the message store until it is expunged or purged in a separate action by the user. See also *purge a message*, *expunge a message*.

delivery See *message delivery*.

delivery mode (n.) A mode that indicates the reliability of messaging: messages that are guaranteed to be delivered and successfully consumed once and only once (persistent delivery mode) or are guaranteed to be delivered at most once (non-persistent delivery mode).

delivery model (n.) A model by which messages are delivered. The model can be either point-to-point or publish/subscribe. In Java™ Message Service (JMS), separate programming domains exist for each, using specific client runtime objects and specific destination types (queue or topic), as well as a unified programming domain.

delivery policy (n.) A specification that details how a queue is to route messages when more than one message consumer is registered. The policies are single, failover, and round-robin.

delivery status notification (n.) A message giving status information about a message that is en route to a recipient, for example, a message indicating that delivery has been delayed because of network outages.

denial of service attack (n.) A situation where an individual intentionally or inadvertently overwhelms a mail server by flooding it with messages. A server's throughput could be significantly impacted or the server itself could become overloaded and nonfunctional.

deny filter (n.) A Java Enterprise System Messaging Server access-control rule that identifies clients that are to be denied access to one or more of the following services: POP, IMAP, or HTTP. See also *allowed attributes*.

deployment (n.) A stage of the Java Enterprise System solution life-cycle process in which a deployment scenario is translated into a deployment design, implemented, prototyped, and rolled out in a production environment. The end product of this process is also referred to as a deployment (or deployed solution).

deployment architecture (n.) A high-level design that depicts the mapping of a *logical architecture* to a physical computing environment. The physical environment includes the computers in an intranet or Internet environment, the network links between them, and any other physical devices needed to support the software.

deployment descriptor (n.) An XML file provided with each module and application that describes how the applications should be deployed. The deployment descriptor directs a deployment tool to deploy a module or application with specific container options and describes specific configuration requirements that a deployer must resolve.

deployment scenario (n.) A *logical architecture* for a Java Enterprise System solution and the quality-of-service requirements that the solution must satisfy to meet business needs. The quality-of-service requirements include requirement regarding: performance, availability, security, serviceability, and scalability/latent capacity. A deployment scenario is the starting point for deployment design.

depth (n.) The number of links followed from a site's starting point in the Search Engine. When you define a site, you define the number of links the robot can follow away from that point, thereby limiting the depth of the search.

dereference an alias (v.) To specify in a bind or search operation, that a directory service translate an alias distinguished name to the actual distinguished name of an entry.

Desktop See *Java™ System Portal Server Desktop*.

destination (n.) The physical location in a Java Enterprise System message server to which produced messages are delivered for routing and subsequent delivery to consumers. This physical destination is identified and encapsulated by an administered object. A client uses the administered object to specify the destination for which the client is producing messages and/or from which the client is consuming messages.

destination resource (n.) An object that represents Topic or Queue destinations. Used by applications to read and write to Queues or publish and subscribe to Topics. Application code uses the Java Naming and Directory Interface™ (JNDI) Service to locate Java™ Message Service (JMS) resource objects using a JNDI Name.

development (n.) A task in the Java Enterprise System solution deployment process, by which the custom components of a *deployment architecture* are programmed and tested.

device detection See *client detection*.

device group (n.) A user-defined group of device resources, such as disks, that can be mastered from different nodes in a cluster HA configuration. This group can include device resources of disks, Solstice DiskSuite™ software disksets, and VERITAS Volume Manager disk groups.

device ID (1) (n.) A mechanism of identifying devices that are made available by way of the Solaris™ Operating System. Device IDs are described in the `devid_get(3DEVID)` man page.

(2) (n.) The Messaging Server DID driver uses device IDs to determine correlation between the Solaris logical names on different cluster nodes. The DID driver probes each device for its device ID. If that device ID matches another device somewhere else in the cluster, both devices are given the same DID name. If the device ID has not been seen in the cluster before, a new DID name is assigned. See also *Solaris™ logical name* and *DID*.

device information (n.) Device-specific client data for Portal Server Mobile Access.

DHCP (dynamic host configuration protocol) (n.) An Internet proposed standard protocol that allows a system to dynamically assign an IP address to individual computers on a network. See also *IP address*.

DID See *device ID*.

DID driver (n.) A device ID driver implemented by Java Enterprise System Messaging Server software used to provide a consistent device namespace across the cluster. See also *DID name*.

DID name (n.) A device ID name that identifies global devices in a SunPlex™ system. A DID name is a clustering identifier with a one-to-one or a one-to-many relationship with Solaris™ Operating System logical names that takes the form `dXsY`, where *X* is an integer and *Y* is the slice name. See also *Solaris™ logical name*.

digest authentication (n.) A type of authentication which allows the user to authenticate without sending the username and password as cleartext. The browser uses the MD5 algorithm to create a digest value. The server uses the Digest Authentication plug-in to compare the digest value provided by the client.

DIGEST-MD5 (n.) A lightweight standards track authentication mechanism that is more secure then CRAM-MD5. Documented in RFC 2831 which also provides an option to protect the entire connection without the setup overhead of TLS (SSL).

digital signature (n.) An electronic security mechanism used to authenticate both a message and the signer.

directive (n.) A Search Engine statement that uses a particular format to invoke a function (such as a robot application function) and passes parameters to the function in a parameter block. For example, the following directive invokes the `enumerate-urls` function and passes parameters for `max` and `type`:

```
Enumerate fn=enumerate-urls max=1024 type=text/html
```

directory (n.) A special kind of database optimized for reading data rather than writing data. Most directories are based on LDAP (Lightweight Directory Access Protocol), an industry-standard protocol.

directory access protocol See *CUA*.

directory context (n.) The point in the directory tree information at which a search begins for entries used to authenticate a user and password for message store access. See also *base DN*.

directory entry (n.) A set of directory attributes and their values identified by a distinguished name. Each entry contains an object class attribute that specifies the kind of object the entry describes and defines the set of attributes it contains.

directory information tree See *DIT*.

directory lookup (n.) The process of searching the directory for information on a given user or resource based on that user or resource's name or other characteristic.

Directory Manager (1) (n.) A user who has administrative privileges to the directory server database. Access control does not apply to this user (think of the directory manager as the directory's superuser).

(2) (n.) The privileged database administrator who is comparable to the root user on UNIX systems. Access control does not apply to the directory manager.

directory schema (n.) The set of rules that defines the data that can be stored in the directory.

directory server (1) (n.) A server that serves information about people and resources within an organization from a logically centralized repository. See also *LDAP*, *Java™ System Directory Server*, and *Java™ System Directory Server Access Management Edition*.

(2) (n.) The Java Enterprise System directory service based on LDAP.

Directory Server Console (n.) An LDAP client application that provides a graphical user interface to browse, configure, and manage the contents of a directory. The Directory Server Console is a component of the Java Enterprise System Directory Server product.

directory service (n.) A database application designed to manage descriptive, attribute-based information about people and resources within an organization.

directory synchronization (n.) The process of synchronizing the MTA directory cache with the current directory information stored in the directory service. See also *MTA directory cache*.

disconnected state (n.) The state in which a mail client connects to the server, makes a cache copy of selected messages, then disconnects from the server.

disk device group See *device group*.

disk group See *device group*.

diskset See *device group*.

Dispatcher (n.) The MTA component that handles connection requests for defined TCP ports. The Dispatcher is a multithreaded connection dispatching agent that permits multiple multithreaded servers to share responsibility for a given service. When using the Dispatcher, you can have several multithreaded SMTP server processes running concurrently.

display profile (n.) A set of XML documents used to define and configure providers and channels in Java Enterprise System Portal Server.

distinguished name See *DN*.

distributable session (n.) A user session that is distributable among all servers in a cluster.

distributed enterprise application (n.) An application whose logic spans a network or Internet environment (the distributed aspect) and whose scope and scale meet the needs of a production environment or service provider (the enterprise aspect).

distributed indexing (n.) The process of assigning different robots in the Search Engine to index different parts of the network. Distributed indexing reduces the load on each robot. A single Search Engine can then gather all the resource descriptions from all the different robots by importing resource descriptions from each.

Distributed Lock Manager (n.) The locking software used in a shared disk Oracle Parallel Server environment. The Distributed Lock Manager enables Oracle processes running on different nodes to synchronize database access. The Distributed Lock Manager is designed for high availability. If a process or node crashes, the remaining nodes do not need to be shut down and restarted. A quick reconfiguration of the Distributed Lock Manager is performed to recover from such a failure.

distributed transaction (n.) A single transaction that can apply to multiple heterogeneous databases that might reside on separate servers.

distribution (n.) A collection of bits which manifests itself in various forms of media and packaging technologies.

distribution list See *mailing list*.

distribution list owner See *mail list owner*.

DIT (directory information tree) (n.) The logical representation of the information stored in the directory. The DIT mirrors the tree model used by most file systems, with the tree's root point appearing at the top of the hierarchy.

DN (distinguished name) (n.) String representation of an entry's name and location in the directory.

DN attribute (n.) A text string that contains identifying information for an associated user, group, or object.

DNS (domain name system) (n.) The system used by machines on a network to associate IP addresses (such as 00.120.000.168) with host names (such as `www.example.com`). Clients usually use DNS to find the IP addresses of servers they wish to contact. The data in DNS is often augmented in local tables, such as from NIS or the `/etc/hosts` file on UNIX systems. See also *IP address*.

DNS alias (n.) A host name that the DNS server knows points to a different host. The DNS alias is implemented as a DNS CNAME record. Machines always have one real name, but they can have one or more aliases. For example, an alias such as `www.example.com` might point to a real machine called `realthing.example.com` where the server currently exists.

DNS database (n.) A database of domain names (host names) and their corresponding IP addresses.

DNS domain (n.) A group of computers whose host names share a common suffix, the domain name. Syntactically, an Internet domain name consists of a sequence of names (labels) separated by periods (dots), for example, `corp.mktng.example.com`. See also *document type definition*.

DNS spoofing (n.) A form of network attack in which a DNS server has been subverted to provide false information.

document (n.) A file on the network, most often a web page or word processing document, but also possibly text files, spreadsheets, and so on. A generic term for a resource indexed by the Search Engine.

document root (1) (n.) A directory on the server machine that contains files, images, and data that will be displayed to users accessing Java Enterprise System Web Server.

(2) (n.) A directory on the server machine that contains the files, images, and data you want to present to users accessing the server.

(3) (n.) The document root (sometimes called the primary document directory) is the central directory that contains all the virtual server's files you want to make available to remote clients.

document type definition See *DTD*.

domain (1) (n.) The last part of a fully qualified domain name that identifies the company or organization that owns the domain name (for example, `example.com`, `host.example.com`).

(2) (n.) Resources under control of a single computer system. See also *administration domain*, *DNS domain*, *hosted domain*, *virtual domain*.

(3) (n.) A set of objects used by Java™ Message Service (JMS) clients to program JMS messaging operations. Two programming domains exist: one for the point-to-point delivery model and one for the publish/subscribe delivery model.

Domain Administration Server (n.) The Domain Administration Server is a specially designated Application Server instance that handles all administrative tasks for the Sun Java System Application Server. It maintains and updates the central repository for Application Server configuration information. If the Domain Application Server isn't running, administrative tasks are unavailable.

domain administrator (n.) A user who has administrative privileges to create, modify, and delete mail users, mail lists, and family accounts in a hosted domain by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs. By default, this user can act as a message store administrator for all messaging servers in the topology.

domain alias (n.) A domain entry that points to another domain. By using aliases, hosted domains can have several domain names.

domain hosting (n.) The process of hosting a domain. The ability to host one or more domains on a shared messaging server. For example, the domains `example.com` and `example.org` might both be hosted on the `example.com` mail server. Users send mail to and receive mail from the hosted domain. The name of the mail server does not appear in the email address.

domain name (1) (n.) A host name used in an email address.

(2) (n.) A unique name that defines an administrative organization. Domains can contain other domains. Domain names are interpreted from right to left. For example, `example.com` is both the domain name of the Example Company and a subdomain of the top-level `com` domain. The `example.com` domain can be further divided into subdomains such as `corp.example.com`, and so on. See also *host name*, *fully qualified domain name*.

domain name system See *DNS*.

domain organization (n.) A subdomain below a hosted domain in the organization tree. Domain organizations are useful for companies that wish to organize their user and group entries along departmental lines.

domain part (n.) The part of an email address to the right of the "at" sign (`@`). For example, `example.com` is the domain part of the email address `jdoe@example.com`.

domain quota (n.) The amount of space allocated to a domain for email messages. The amount of space is configured by the system administrator.

domain registry (n.) A single data structure that contains domain-specific information for all the domains created and configured on an installation of a server, such as domain name, domain location, domain port, domain host.

domain rewrite rules See *rewrite rule*.

domain template (n.) The part of a rewrite rule that defines how the host and domain portion of an address is rewritten. The template can include a full static host and domain address or a single field substitution string, or both.

double failure (n.) Simultaneous failure of one or more mirror node pairs in the HADB. See *HADB*, *HADB node*, *active node*, *spare node*, *mirror node*, and *data redundancy unit*.

drop word See *stop word*.

DRU See *data redundancy unit*.

DSA (directory system agent) (n.) An X.500 term for a Directory Server.

DSE (directory server entry) (n.) An entry, or DSA-specific entry, that has additional server-specific information associated with it. A DSE such as the Root DSE or schema DSE has different attributes on each server.

DSP (digital signal processing) (n.) The conversion of signals from analog to digital. A DSP cvard is required to access Portal Server software using a phone for voice access.

DSML (directory services markup language) (n.) A family of document formats for representing XML markup language that enable you to represent directory services in XML. Java Enterprise System Directory Server 5.2 conforms to version 2 of the DSML standard (DSMLv2).

DSN (n.) See *delivery status notification*.

dsservd (n.) A daemon that accesses the database files that hold the directory information and communicates with directory clients using the LDAP protocol.

dssetup (n.) A Java Enterprise System Directory Server preparation tool that makes an existing Directory Server ready for use by a Java Enterprise System Messaging Server.

DTD (document type definition) (n.) A description of the structure and properties of a class of XML files.

DWP (database wire protocol) (n.) A Calendar Server proprietary protocol that allows multiple servers to be linked together within the same Calendar Server system to form a distributed calendar store. The Calendar Servers uses DWP to retrieve remote data stored in the calendar database.

dynamic group (n.) A mail group defined by an LDAP search URL. Users usually join the group by setting an LDAP attribute in their directory entry.

dynamic redeployment See *dynamic reloading*.

dynamic reloading (n.) The process of updating and reloading a component without restarting the server. By default, servlets, pages created with JavaServer Pages™ technology (*JSP™ technology*), and enterprise bean components can be dynamically reloaded. Also known as dynamic redeployment and versioning.

dynamic web application (n.) Refers to servlets, JSP™ pages, content providers, or anything else that needs to be processed by the Java™ web container that is accessed by the user's browser. For Java Enterprise System Portal Server, the application gets installed in the web server.

EAR file (enterprise archive file) (n.) An archive file that contains a J2EE™ application. EAR files have the `.ear` extension. See also *JAR file*.

e-commerce (electronic commerce) (n.) A term for business conducted over the Internet.

EHLO command (n.) An SMTP command that queries a server to find out if the server supports extended SMTP commands. Defined in RFC 1869.

EIS (enterprise information system) (n.) Interpreted as a packaged enterprise application, a transaction system, or a user application. Examples of an EIS include R/3, PeopleSoft, Tuxedo, and CICS.

EJB container See *container*.

`ejbc` utility (n.) The compiler for enterprise beans. This utility checks all EJB classes and interfaces for compliance with the EJB™ specification and generates stubs and skeletons.

EJB™ QL (EJB™ Query Language) (n.) A query language that provides for navigation across a network of entity beans defined by container-managed relationships.

EJB™ technology (Enterprise JavaBeans™ technology) (n.) An enterprise bean is a server-side component that encapsulates the business logic of an application. The business logic is the code that fulfills the purpose of the application. For example, in an inventory control application, the enterprise beans might implement the

business logic in methods called `checkInventoryLevel` and `orderProduct`. By invoking these methods, remote clients can access the inventory services provided by the application. See also *container*, *entity bean*, *message-driven bean*, and *session bean*.

element (n.) A member of a larger set, for example, a data unit within an array or a logic element. In an XML file, an element is the basic structural unit. An XML element contains sub-elements or data and might contain attributes.

encapsulate (v.) To localize knowledge within a module. Because objects encapsulate data and implementation, the user of an object can view the object as a black box that provides services. Instance variables and methods can be added, deleted, or changed, but if the services provided by the object remain the same, code that uses the object can continue to use the object without being rewritten.

encryption (n.) Process of protecting information from unauthorized use by making the information unintelligible. Some encryption methods employ codes, called keys, which are used to encrypt the information. See also *decryption*.

endpoint (n.) A physical port on a cluster transport adapter or cluster transport junction.

end user (n.) A person who uses a distributed application, often through a graphical user interface, such as an Internet browser or mobile device GUI. the number of concurrent end users supported by an application is an important determinant of the *deployment architecture* of the application.

ENS See *event notification service*.

enterprise network (n.) A network that consists of collections of networks connected to each other over a geographically dispersed area. The enterprise network serves the needs of a widely distributed company and is used by the company's mission-critical applications.

entity bean (n.) An enterprise bean that relates to physical data, such as a row in a database. Entity beans are long lived because they are tied to persistent data. Entity beans are always transactional and multiuser aware. See *message-driven bean*, *read-only bean*, *session bean*.

entropy (n.) A measure of the randomness in a closed system. Specifically in the context of SSL, multiple seeds are used in order to introduce entropy (ensure randomness) in random number generation.

entry (n.) A group of attributes and a unique distinguished name.

entry distribution (n.) Method of distributing directory entries across more than one server in order to scale to support large numbers of entries.

entry ID list (n.) A list of entry IDs. Each index that the directory uses is composed of a table of index keys and matching entry ID lists. The entry ID list is used by the directory to build a list of candidate entries that might match the client application's search request.

enumeration (n.) The phase of a robot's operation in which the robot seeks resources, including extracting and following hypertext links.

envelope (n.) A container for transport information about the sender and the recipient of an email message. This information is not part of the message header. Envelopes are used by various email programs as messages are moved from place to place. Users see only the header and body of a message.

envelope field (n.) A named item of information, such as `RCPT TO`, in a message envelope.

equality index (n.) An index which allows you to search efficiently for entries containing a specific attribute value.

ERP (enterprise resource planning) (n.) A multi-module software system that typically includes a relationship database and applications for managing purchasing, inventory, personnel, customer service, shipping, financial planning, and other important aspects of the business.

error handler (n.) A program that handles errors. In Messaging Server, the error handler issues error messages and processes error-handler action forms after the postmaster fills them out.

error handler action form (n.) A form sent to the postmaster account that accompanies a received message that Messaging Server cannot handle. The postmaster fills out the form to instruct the server how to process the message.

error message (n.) A message reporting an error or other situation. Java Enterprise System Messaging Server generates messages in a number of situations, notably when it gets an email message that it cannot handle. Other messages, called notification errors, are for informational purposes only.

ESMTP See *extended simple mail transfer protocol*.

ESP (n.) enterprise service provider.

ETRN command (n.) An SMTP command enabling a client to request that the server start the processing of its mail queues for messages that are waiting at the server for the client machine. Defined in RFC 1985.

event (1) (n.) An entry with an associated date and time in a calendar. For example, an event might be a new meeting or appointment on a calendar.

(2) (n.) A named action that triggers a response from a module or external Java Naming and Directory Interface™ (JNDI) resource.

(3) (n.) A change in the state, mastery, severity, or description of a managed object.

event notification service (n.) A generic service that accepts reports of server-level events that can be categorized and then notifies other servers that have registered interest in certain categories of events. Allows the Java Naming and Directory Interface™ (JNDI) Service to act as a bridge to a remote JNDI server.

expander (n.) Part of an electronic mail delivery system that allows a message to be delivered to a list of addressees. Mail expanders are used to implement mail lists. Users send messages to a single address (for example, `users@example.com`) and the mail expander takes care of delivery to the mailboxes in the list. Also called mail exploders. See also *EXPN command*.

expansion (n.) The act of converting a message addressed to a mail list into enough copies for each mail list member. Applies to the MTA processing of mail lists.

expires header (n.) The expiration time of the returned document specified by the remote server.

EXPN command (n.) An SMTP command for expanding a mail list. Defined in RFC 821.

expunge a message (v.) To permanently remove a message that has been deleted from the INBOX. See also *delete a message*, *purge a message*.

extended simple mail transfer protocol (n.) An Internet message transport protocol. ESMTP adds optional commands to the SMTP command set for enhanced functionality, including the ability for ESMTP servers to discover which commands are implemented by the remote site.

extensible markup language See *XML*.

extensible style language See *XSL*.

extensible style language transformation See *XSLT*.

extracting (n.) The process of locating hypertext links in a document. Each extracted link is added to the URL pool for further processing.

extranet (n.) An extension of a company's intranet onto the Internet to allow customers, suppliers, and remote workers access to the data.

facade (n.) Where an application-specific stateful session bean is used to manage various Enterprise JavaBeans™ components.

facility (n.) In a Messaging Server log-file entry, a designation of the software subsystem (such as Network or Account) that generated the log entry.

factory class (n.) A class that creates persistence managers. See also *congestion thresholds*.

failback See *authorization*.

failfast (n.) The orderly shutdown and removal from the cluster of a faulty node before its potentially incorrect operation can prove damaging.

failover (1) (n.) A recovery process where a bean can transparently survive a server crash.

(2) (n.) The automatic transfer of a computer service from one system to another to provide redundant backup.

(3) (n.) The automatic relocation of a resource group or a device group from a current primary node to a new primary node after a failure has occurred.

failover resource (n.) A resource whose resources can correctly be mastered by only one node at a time. See also *single-instance resource* and *scalable resource*.

family group administrator (n.) A user who has administrative privileges to add and remove family members in a family group. This user can grant family group administrative access to other members of the group.

fancy indexing (n.) A method of indexing that provides more information than simple indexing. Fancy indexing displays a list of contents by name with file size, last modification date, and an icon reflecting file type. Because of this, fancy indexes might take longer than simple indexes for the client to load.

fault monitor (n.) A fault daemon and the programs used to probe various parts of data services and take action. See also *resource monitor*.

federated identity (n.) The amalgamation of the account information in all service providers that are accessed by one user (for example, personal data, authentication information, buying habits and history, shopping preferences, and so on). The information is administered by the user and, with the user's consent, securely shared with the user's providers of choice.

federation cookie (n.) A federation cookie is a cookie implemented by Access Manager with the name fedCookie. It can have a value of either yes or no based on the principal's federation status. It is not a defined part of the LAP specifications.

federation termination (n.) The process by which users cancel affiliations established between the user's identity provider and federated service provider accounts. Also called defederation.

file cache (n.) The file cache contains information about files and static file content. The file cache is turned on by default.

file extension (n.) The last part of a file name that typically defines the type of file. For example, in the file name `index.html`, the file extension is `html`.

file transfer protocol See *FTP*.

file type (n.) The format of a given file. For example, a graphics file does not have the same file type as a text file. File types are usually identified by their file extension. See also *fault monitor*.

filter (1) (n.) In a search request, a pattern which an entry in the scope of the search must match for that entry to be returned in the search response. Filters are also used in constructing role and access control definitions.

(2) (n.) A set of rules that define particular types of resources. These filters are used by site definitions to define types of resources the robot should accept or ignore.

filtered role (n.) A method by which roles are assigned to entries. Allows you to assign entries to the role depending upon the attribute contained by each entry. You do this by specifying an LDAP filter. Entries that match the filter are said to possess the role.

filtering (n.) The process of determining whether a document is part of a site that should be included in the index.

finder method (n.) A method that enables clients to look up a bean or a collection of beans in a globally available directory.

firewall (n.) A network configuration, usually both hardware and software, that protects networked computers within an organization from outside access. Firewalls are commonly used to protect information such as a network's email and data files within a physical building or organization site.

flexible log format (n.) A format used by the server for entering information into the access logs.

folder (n.) A named collection of messages. Folders can contain other folders. Also known as a mailbox. See also *personal folder*, *public folder*, *shared folder*, *INBOX*.

form action handler (n.) A specially defined method in servlet or application logic that performs an action based on a named button on a form.

FORTEZZA (n.) An encryption system used by U.S. government agencies to manage sensitive but unclassified information.

forwarding See *message forwarding*.

foundation profile (n.) A set of APIs together with the CDC that provide a J2ME™ application runtime environment targeted at next generation applications, consumer electronic, and embedded devices.

fractional replication (n.) Reproduction of a filtered subset of attributes.

fragmentation (n.) The MIME feature that allows the breaking of a large message into smaller messages. See also *default calendar*.

fresh start (n.) Starting the robot from its starting points. A fresh start deletes the robot's state information, causing the robot to begin its next run from its initial state. Opposite of a restart.

FTP (file transfer protocol) (n.) An Internet protocol that allows files to be transferred from one computer to another over a network.

fully qualified domain name (n.) The full name of a system, containing its host name and its domain name. For example: `example.sun.com`, where `example` is the host name (of a server) `sun.com` in the domain name.

gateway (n.) A system that translates from one native format to another. Examples include X.400 to and from RFC 822 electronic mail gateways. A machine that connects two or more electronic mail systems (especially dissimilar mail systems on two different networks) and transfers messages between them. Sometimes the mapping and translation can be complex. Generally requires a store-and-forward scheme whereby the message is received from one system completely before it is transmitted to the next system after suitable translations.

general access (n.) A level of user access. When granted, indicates that all authenticated users can access directory information.

general ACL (n.) A named access control list in the Java Enterprise System Directory Server that relates a user or group with one or more permissions. This list can be defined and accessed arbitrarily to record any set of permissions.

generation (n.) The phase of a robot's operation in which the robot produces a resource description for each resource discovered in the enumeration phase.

generic resource (n.) An application daemon and its child processes put under the control of the Resource Group Manager as part of a generic resource type.

generic resource type (n.) A template for a data service. A generic resource type can be used to make a simple application into a failover data service (stop on one node, start on another node). This type does not require programming by the SunPlex™ API.

generic servlet (n.) A servlet that extends `javax.servlet.GenericServlet`. Generic servlets are protocol-independent: They contain no inherent support for HTTP or any other transport protocol. See also *HTTP servlet*.

GIF (graphics interchange format) (n.) A cross-platform image format originally created by CompuServe. GIF files are usually much smaller in size than other graphic file types, for example, TIFF. GIF is one of the most common interchange formats. GIF images are readily viewable on UNIX, Microsoft Windows, and Apple Macintosh systems.

global database connection (n.) A database connection available to multiple components. Requires a resource manager.

global device (n.) A device that is accessible from all cluster members, such as disk, CD-ROM, and tape.

global device namespace (n.) A namespace that contains the logical, cluster-wide names for global devices. Local devices in the Solaris™ Operating System are defined in the `/dev/dsk`, `/dev/rdsk`, and `/dev/rmt` directories. The global device namespace defines global devices in the `/dev/global/dsk`, `/dev/global/rdsk`, and `/dev/global/rmt` directories.

global interface (n.) A network interface that physically hosts shared addresses.

global interface node (n.) A machine or domain which hosts a global interface.

global resource (n.) A highly available resource provided at the kernel level of the Java Enterprise System Messaging Server software. Global resources can include disks (HA device groups), the cluster file system, and global networking.

global transaction (n.) A transaction that is managed and coordinated by a transaction manager and can span multiple databases and processes. The transaction manager typically uses the XA protocol to interact with the database backends. See also *local transaction*.

GMT (Greenwich Mean Time) (n.) The mean solar time of the meridian of Greenwich, England, and the time standard against which all other time zones in the world are referred. GMT is not affected by Daylight Savings Time or Summer Time.

granularity level (n.) The approach to dividing an application into pieces. A high level of granularity means that the application is divided into many smaller, more narrowly defined Enterprise JavaBeans™ components. A low level of granularity means the application is divided into fewer pieces, producing a larger program.

greeting form (n.) A message usually sent to users when an account is created for them. This form acts as confirmation of the new account and verification of its contents.

group (1) (n.) Several users that are related in some way. Group membership is usually maintained by a local system administrator. See also *user*, *role*.

(2) (n.) Several LDAP mail entries that are organized under a *distinguished name*. Usually used as a mail list, but might also be used to grant certain administrative privileges to members of the group. See also *dynamic group*, *static group*.

group folders (n.) These folders that contain shared and group folders. See also *public folder*, *shared folder*.

group ID (n.) The group for Calendar Server files such as counters and logs. The group ID is stored in the `ics.conf` file in the `local.servergid` parameter. Also known as GID.

group scheduling engine (n.) The Calendar Server process that handles group scheduling. This engine enables a user to schedule events with other calendar users on the same server or on a different server. The other users can then modify, cancel, or reply to the event.

GUI (n.) graphical user interface.

HA See *high availability*.

HA data service See *data service*.

HADB See *high availability database*.

HADB node (n.) A set of HADB processes, a dedicated area of shared memory, and one or more secondary storage devices used for storing and updating session data. Each active (data storage) node must have a mirror node; therefore nodes occur in pairs. In addition, two or more spare nodes can be included to maximize availability. If an active node fails and cannot recover within a timeout period, the spare node copies the data from the mirror node and becomes active. See also *high availability database*, *active node*, *spare node*, *mirror node*, and *data redundancy unit*.handle

(n.) An object that identifies an enterprise bean. A client can serialize the handle and then later deserialize it to obtain a reference to the bean.

hard restart (n.) The termination of a process or service and its subsequent restart. See also *SOAP*.

hashdir (n.) A command-line utility for determining which directory contains the message store for a particular user.

HDML (Handheld Device Markup Language) (n.) Openwave's proprietary language to program mobile devices that use Openwave browsers.

header (n.) The portion of an email message that precedes the body of the message. The header is composed of field names followed by a colon and then values. Headers contain information useful to email programs and to users trying to make sense of the message. For example, headers include delivery information, summaries of contents, tracing, and MIME information. Headers tell whom the message is for, who sent it, when it was sent, and what it is about. Headers must be written according to RFC 822 so that email programs can read them.

header field (n.) A named item of information, such as “From:” or “To:”, in a message header. Also known as a header line.

heartbeat (n.) A periodic message sent across all available cluster interconnnect transport paths. Lack of a heartbeat after a specified interval and number of retries might trigger an internal *failover* of transport communication to another path. Failure of all paths to a cluster member results in the *CMM* reevaluating the cluster quorum.

heuristic decision (n.) The transactional mode used by a particular transaction. A transaction has to either Commit or Rollback.

high availability (n.) Enables the detection of a service interruption and provides recovery mechanisms in the event of a system failure or process fault. In addition, high availability allows a backup system to take over the services in the event of a primary system failure. Also known as HA.

high availability database (HADB) (n.) A highly scalable, highly available session state persistence infrastructure. Application Server uses the HADB to store HTTP session states and stateful session bean states. See also *HADB node*, *active node*, *spare node*, *mirror node*, and *data redundancy unit*.

home interface (n.) A mechanism that defines the methods that enable a client to create and remove an enterprise bean.

home page (n.) A document that exists on the server and acts as a catalog or entry point for the server’s contents. The location of this document is defined within the server’s configuration files.

hop (n.) A transmission between two computers.

horizontal scalability (n.) The Calendar Server’s capability to run on a single server or as a group of processes that are spread across multiple servers with a wide variety of possible configuration options.

host (n.) The machine on which one or more servers reside.

hosted domain (n.) An email domain that is outsourced to an ISP. That is, the ISP provides email domain hosting for an organization by operating and maintaining the email services for that organization. A hosted domain shares the same Java Enterprise System Messaging Server host with other hosted domains. In earlier LDAP-based email systems, a domain was supported by one or more email server hosts. With Messaging Server, many domains can be hosted on a single server. For each hosted domain, there is an LDAP entry that points to the user and group container for the domain. Also known as a virtual hosted domain or a *virtual domain*. See also *document type definition*.

host-IP authentication (n.) A security mechanism used for limiting access to the Java Enterprise System Administration Server or the files and directories on a web site by making them available only to clients using specific computers.

host name (n.) The name of a particular machine within a domain. The host name is the IP host name, which might be either a "short-form" host name (for example, `mail`) or a fully qualified host name. The fully qualified host name consists of the host name and the *domain name*. For example, `mail.example.com` is the host name `mail` in the domain `example.com`. Host names must be unique within their domains. Your organization can have multiple machines named `mail`, as long as the machines reside in different subdomains, for example, `mail.corp.example.com` and `mail.field.example.com`. Host names always map to a specific IP address. See also *fully qualified domain name*, *IP address*.

host-name hiding (n.) The practice of using domain-based email addresses that do not contain the name of a particular internal host.

HTML (hypertext markup language) (n.) A coding markup language used to create documents that can be displayed by web browsers. Each block of text is surrounded by codes that indicate the nature of the text.

HTML page (n.) A page coded in HTML and intended for display in a web browser.

HTTP (hypertext transfer protocol) (n.) The Internet protocol based on *TCP/IP* that fetches hypertext objects from remote hosts.

HTTPD (hyptertext transfer protocol daemon) (n.) An abbreviation for the HTTP daemon or service, which is a program that serves information using the HTTP protocol.

HTTP-NG (hypertext transfer protocol-next generation) (n.) The next generation of hypertext transfer protocol.

HTTPS (hypertext transfer protocol secure) (n.) A secure version of HTTP implemented using *SQL*.

HTTP servlet (n.) A servlet that extends `javax.servlet.HttpServlet`. These servlets have built-in support for the HTTP protocol. See also *generic servlet*.

hub (n.) A host that acts as the single point of contact for the system. When two networks are separated by a firewall, for example, the firewall computer often acts as a mail hub.

hub supplier (n.) In the context of *replication*, a server that holds a *replica* that is copied from a different server and in turn replicates it to a third server. See also *cascading replication*.

hypertext transfer protocol secure See *HTTP-NG*.

iCalendar Message-Based Interoperability Protocol (n.) This protocol specifies a binding from the *iCalendar Transport-Independent Interoperability Protocol* to Internet email-based transports. This protocol is also known as iMIP. iMIP is defined in RFC 2447.

iCalendar Transport-Independent Interoperability Protocol (n.) An Internet protocol based on the iCalendar object specification that provides scheduling interoperability between different calendar systems. This protocol is also known as iTIP. iTIP is defined in RFC 2446.

IDE (integrated development environment) (n.) Software that allows you to create, assemble, deploy, and debug code from a single graphical user interface.

IDENT See *Identification Protocol*.

Identification Protocol (n.) A protocol that provides a means to determine the identity of a remote process responsible for the remote end of a particular TCP connection. This protocol is also known as IDENT. Defined in RFC 1413.

identity federation (n.) See *account federation*.

identity provider (n.) A service provider that specializes in providing authentication services. As the administrating service for authentication, the identity provider maintains and manages identity information. Authentication provided by an identity provider is honored by all service providers with whom the identity provider is affiliated.

identity service (n.) An identity service is a Web service that acts upon a resource to retrieve, update, or perform some action on data attributes related to a Principal (an identity). An example of an identity service might be a corporate phone book or calendar service.

IDL (interface definition language) (n.) A language used to define interfaces to remote *CORBA* objects. The interfaces are independent of operating systems and programming languages. Describes functional interfaces for remote procedure calls (*RPC*), so that a compiler can generate proxy and stub code that marshals parameters between machines.

idle state (n.) A type of state in which the robot is still running but has processed all the URLs in its URL pool. In this state, the robot can still respond to status requests.

iHTML (i-mode hypertext markup language) (n.) The language used with NTT DoCoMo's Japanese i-mode service.

IIOP (Internet Inter-ORB Protocol) (n.) A transport-level protocol used by both Remote Method Invocation (*RMI*) over IIOP and Common Object Request Broker Architecture (*CORBA*).

IIOP cluster (n.) An IIOP cluster that has been configured for high availability of RMI/IIOP requests.

IIOP endpoint (n.) An IIOP listener that has been configured for an IIOP cluster to enable high availability of RMI/IIOP requests.

IIOP listener (n.) A listen socket that listens on a specified port and accepts incoming connections from CORBA-based client applications.

imagemap (1) (n.) A process that makes areas of an image active, letting users navigate and obtain information by clicking the different regions of the image with a mouse.

(2) (n.) A *CGI* program that is used to handle imagemap functionality in other *HTTPD* implementations.

IMAP4 (Internet Message Access Protocol Version 4) (n.) A standard protocol that allows users to be disconnected from the main messaging system and still be able to process their mail. The IMAP specification allows for administrative control for these disconnected users and for the synchronization of the users' message store once they reconnect to the messaging system.

iMIP See *iCalendar Message-Based Interoperability Protocol*.

immediate subordinate (n.) In the *DIT*, an entry is an immediate subordinate of another entry if its *distinguished name* is formed by appending its *RDM* to the distinguished name of the parent entry.

immediate superior (n.) In the *DIT*, an entry is the immediate superior of another entry if its *distinguished name*, followed by the *RDM* of the other entry, forms the distinguished name of the child entry.

import agent (n.) The process used during *importing*.

importing (n.) The process of bringing new or updated resource descriptions from another database into the Search Engine.

`imsadmin` commands (n.) A set of command-line utilities for managing domain administrators, users, and groups.

`imsimta` commands (n.) A set of command-line utilities for performing various maintenance, testing, and management tasks for the *MTA*.

inactive boot environment (n.) An environment which is not currently booted or designated for activation upon the next reboot. See also *active boot environment*.

INBOX (n.) The name reserved for a user's default mailbox. Used for mail delivery. INBOX is the only folder name that is case-insensitive, which means that INBOX, Inbox, and inbox are all valid names for a user's default mailbox.

index (n.) A centralized, searchable database of resources or documents. Also known as a catalog.

indexing (n.) The process of providing a centralized, searchable database of resources. Also known as cataloging.

index key (n.) Each index that the directory uses is composed of a table of index keys and matching entry ID lists.

indirect CoS (n.) Identifies the template entry using the value of one of the target entry's attributes.

`inittab` file (n.) (UNIX only) A file listing programs that need to be restarted if they stop for any reason. The file ensures that a program runs continuously. Because of its location, the file is also called `/etc/inittab`. This file is not available on all UNIX systems.

installation directory (n.) The directory into which the binary (executable) files of a server are installed. For the Messaging Server, the installation directory is a subdirectory of the *server root*: *server-root*`/bin/msg/`. See also *instance directory*.

instance directory (n.) The directory that contains the files that define a specific instance of a server. For the Messaging Server, the instance directory is a subdirectory of the *server root*: *server-root*`/msg-`*instance*`/`, where *instance* is the name of the server as specified at installation. See also *installation directory*.

Instant Messaging multiplexor (n.) A manager of client connections. Improves Instant Messaging Server scalability by allowing a large number of concurrent client connections to require only a few connections to the backend Instant Messaging server. Instant Messaging clients connect to the multiplexor rather than to the Instant Messaging server itself. When installed on the public side of a firewall, the multiplexor protects the user database from intruders, leaving the Instant Messaging Server behind the firewall.

Instant Messaging Server (1) (n.) Refers to the Java Enterprise System Messaging Server product itself, including all components (server, multiplexor, and Java Enterprise System Instant Messaging Server).

(2) (n.) The backend server process within the product that handles incoming commands from Instant Messaging (through the Instant Messaging Server multiplexor). The Instant Messaging Server also communicates with the LDAP server in the authentication of Instant Messaging users. See also *Instant Messaging multiplexor*.

intelligent agent (n.) An object within a server that performs various requests (such as HTTP, NNTP, SMTP, and FTP requests) on behalf of the user. In a sense, the intelligent agent acts as a client to the server, making requests that the server fulfills.

international index (n.) A type of search index. Speeds up searches for information in a *DIT* in which the attributes have language tags.

Internet Message Access Protocol Version 4 See *IMAP4*.

Internet Protocol See *IP*.

intranet (n.) A network of *TCP/IP* networks within a company or organization. Intranets enable companies to employ the same types of servers and client software used for the World Wide Web for internal applications distributed over the corporate LAN. Sensitive information on an intranet that communicates with the Internet is usually protected by a firewall. See also *firewall*, *extranet*.

invalid user (n.) An error condition that occurs during message handling. When this error condition occurs, the message store sends a communication to the MTA and then deletes its copy of the message. The MTA bounces the message back to the sender and deletes its copy of the message.

IP (Internet Protocol) (n.) Protocol within the *TCP/IP* suite used to link networks worldwide. Developed by the United States Department of Defense and used on the Internet. The prominent feature of this suite is the IP protocol.

IP address (n.) A set of numbers separated by dots, such as `192.168.255.255`, that specifies the actual location of a machine on an intranet or the Internet. A 32-bit address assigned to hosts using *TCP/IP*.

ISDN (n.) Integrated Services Digital Network.

ISINDEX (n.) An HTML tag that turns on searching in the client. Documents can use a network navigator's capabilities to accept a search string and send it to the server to access a searchable index without using forms. In order to use the `ISINDEX` HTML tag, you must create a query handler.

ISMAP (n.) An extension to the `IMG SRC` tag used in an HTML document to tell the server that the named image is an *imagemap*.

ISO 8601 (n.) An International Organization for Standardization standard that specifies the numeric representation of date and time. The Calendar Server uses ISO 8601 standard notations to represent date, time, and duration strings.

isolation level See *transaction isolation level*.

issued certificate (n.) A certificate that is issued by a *certificate authority*. See also *self-generated certificate*.

iTIP See *iCalendar Transport-Independent Interoperability Protocol*.

J2EE™ platform (Java™ 2 Platform, Enterprise Edition) (n.) An environment for developing and deploying multi-tiered, web-based enterprise applications. The J2EE platform consists of a set of services, *API*s, and protocols that provide the functionality for developing these applications.

J2ME™ platform (Java™ 2 Platform, Micro Edition) (n.) A small application environment suitable for mobile devices.

JAF (JavaBeans™ Activation Framework) (n.) Integrates support for MIME data types into the Java platform. See also *MIME data type*.

JAR file (Java™ Archive file) (n.) A file used for aggregating many files into one file. JAR files have the `.jar` extension.

JAR file contract (n.) A Java™ Archive file contract that specifies what information must be in the enterprise bean package.

JAR file format (n.) A platform-independent Java™ Archive file format that aggregates many files into one file. Multiple applets and their requisite components (class files, images, sounds, and other resource files) can be bundled in a JAR file and subsequently downloaded to a browser in a single HTTP transaction. The JAR file format also supports file compression and digital signatures.

JATO (n.) A library for converting between code written in the Java programming language and *XML*. Also known as Sun Java System Web Application Framework and Application Framework. JATO is geared toward enterprise web application development. JATO combines concepts such as display fields, application events, component hierarchies, and a page-centric development approach.

Java™ (n.) A object-oriented and platform-independent programming language developed by Sun Microsystems, Inc. in order to solve a number of problems in modern programming practice.

Java™ 2 Platform, Enterprise Edition See *J2EE™ platform*.

Java™ 2 Platform, Micro Edition See *J2ME™ platform*.

JavaBean™ namespace (n.) A standard that allows you to specify a unique label to the set of element names defined by a package. A document using that package can be included in any other document without having a conflict between element names. The elements defined in the package are uniquely identified so that, for example, the parser can determine when an element should be interpreted according to your package and not according to that of another package.

JavaBeans™ Activation Framework See *JAF*.

JavaBeans™ component architecture (n.) A portable, platform-independent reusable component model.

Java™ Development Kit See *JDK™ software*.

Java™ Enterprise System (n.) An integration of individual Sun software products into a software system that supports distributed enterprise applications.

Java™ IDL (API, extension) (Java Interface Definition Language) (n.) *API*s written in the Java programming language that provide a standards-based compatibility and connectivity with *CORBA*.

JavaMail™ (API, extension) (n.) An object used by an application to interact with a mail store. Application code uses the Java Naming and Directory Interface™ (JNDI) service to locate JavaMail session resource objects using a JNDI name.

JavaScript™ programming language (n.) A compact, object-based scripting language for developing client and server Internet applications.

JavaServer Pages™ technology See *JSP™ technology*.

Java™ System Compass Server (n.) Server technology used to facilitate user access to network resources typically used with Portal Server 3.0. Portal Server 6.0 contains a tightly integrated search engine which provides the functionality that Compass Server provided with Portal Server 3.0.

Java™ System Delegated Administrator (n.) A set of GUI and CLI interfaces that enable administrators to add users to and modify users and groups of a directory in a hosted domain.

Java™ System Directory Server (n.) The Java Enterprise System version of *LDAP*. Every instance of Application Server uses Directory Server to store shared server information, including information about users and groups.

Java™ System Directory Server Access Management Edition (n.) A set of interfaces that provide user and service management, authentication and single sign-on services, policy management, logging services, debug utility, and client support for Portal Server.

Java™ System Instant Messaging Client (n.) The client that enables users to send and receive instant messages and alerts.

Java™ System Message Queue (n.) The messaging system that implements the Java™ Message Service (JMS) open standard. Message Queue is a JMS provider.

Java™ System Portal Server (n.) A software product that enables remote users to securely access their organization's network and the network's services over the Internet. Creates a secure Internet portal, providing access to content, applications, and data to any targeted audience, including employees, business partners, or the general public. Referred to as the core part of the complete Portal Server product solution that is shared among all Portal Server packs.

Java™ System Portal Server Desktop (n.) Provides the primary end-user interface and a mechanism for extensible content aggregation through the content provider interface (PAPI). Often referred to as "Desktop." The Desktop includes a variety of providers that provide a container hierarchy and the basic building blocks for building some types of channels. The Desktop implements a display profile data storage mechanism on top of a Directory Server Access Management Edition service for storing content provider and channel data. The Desktop also includes an admin console module for editing the display profile and other Desktop service data.

Java™ System Portal Server Instant Collaboration Pack (n.) A server instant messaging product that includes the server, *multiplexor*, and Instant Messaging components. Also known as Java System Instant Messaging Server.

Java™ System Portal Server Pack (n.) A generic term that refers to an add-on product for Portal Server.

Java™ System Web Server (n.) A web server in Portal Server that is used as the web container for Portal Server and Portal Server pack web applications. Web Server is included with the Directory Server Access Management Edition product.

Java™ Web Start software (n.) A web application launcher. With Java Web Start software, applications are launched by clicking on the web link. If the application is not present on the computer, Java Web Start automatically downloads the application and caches it on the computer. Once an application is downloaded to its cache, it can be launched from a desktop icon or from a browser link. No matter which method is used to launch the application, the most current version of the application is always presented.

JAXM (Java™ API for XML Messaging) (n.) A Java API that uses the SOAP standard to enable applications to send and receive document-oriented XML messages. These messages can be with or without attachments.

JAXP (Java™ API for XML Processing) (n.) A Java API that uses DOM, SAX, and XSLT to support the processing of XML documents. Enables applications to parse and transform XML documents independent of a particular XML processing implementation.

JAXR (Java™ API for XML Registries) (n.) A uniform and standard Java API for accessing different kinds of XML registries. Enables users to build, deploy, and discover web services.

JAX-RPC (Java™ API for XML-based RPC) (n.) A Java API that enables developers to build interoperable web applications and web services based on XML-based *RPC* protocols.

JDBC™ connection pool (n.) A pool that combines the JDBC data source properties used to specify a connection to a database with the connection pool properties.

JDBC™ resource (n.) A resource used to connect an application running within the application server to a database by way of an existing JDBC connection pool. Consists of a Java Naming and Directory Interface™ (JNDI) name (which is used by the application) and the name of an existing JDBC connection pool.

JDBC™ technology (Java™ DataBase Connectivity software) (n.) A standards-based set of classes and interfaces that enable developers to create data-aware components. The JDBC API implements methods for connecting to and interacting with data sources in a platform-independent and vendor-independent way.

JDK™ software (Java™ Development Kit) (n.) Software tools used to write Java applets or application programs.

JHTML (J-Sky hypertext markup language) Vodafone's proprietary language used to program Japanese J-Sky devices.

JMS (Java™ Message Service) (n.) A standard set of interfaces and semantics that define how a Java client accesses the facilities of a message service. These interfaces provide a standard way for programs written in the Java programming language to create, send, receive, and read messages.

JMS-administered object (Java™ Message Service administered object) (n.) A pre-configured Java™ Message Service object (*JMS connection factory* or *JMS destination*) created by an administrator for use by one or more JMS clients. The use of administered objects allows JMS clients to be isolated from the proprietary aspects of a provider, thereby making the clients provider-independent. These objects are placed in a Java Naming and Directory Interface™ (JNDI) name space by an administrator and are accessed by JMS clients using JNDI lookups.

JMS API (Java™ Message Service API) (n.) A standard set of interfaces and semantics that define how a JMS client accesses the facilities of a JMS message service. These interfaces provide a standard way for programs written in the Java programming language to create, send, receive, and read messages.

JMS client (Java™ Message Service client) (n.) An application or software component that interacts with other JMS clients using a JMS message service to exchange messages.

JMS connection factory (Java™ Message Service connection factory) (n.) The object administered by the Java™ Message Service that a JMS client uses to create a connection to a JMS message service.

JMS destination (Java™ Message Service destination) (n.) The physical destination in a JMS message service to which produced messages are delivered for routing and for subsequent delivery to consumers. This physical destination is identified and encapsulated by an JMS-administered object that a JMS client uses to specify the destination of incoming and outgoing messages.

JMS messages (Java™ Message Service messages) (n.) Asynchronous requests, reports, or events that are consumed by Java™ Message Service clients. A message has a header (to which additional fields can be added) and a body. The message header specifies standard fields and optional properties. The message body contains the data that is being transmitted.

JMS provider (Java™ Message Service provider) (n.) A product that implements the JMS interfaces for a messaging system and adds the administrative and control functions needed for a complete product.

JMS service (Java™ Message Service service) (n.) Software that provides delivery services for a Java™ Message Service messaging system, including connections to JMS clients, message routing and delivery, persistence, security, and logging. The message service maintains physical destinations to which JMS clients send messages and from which the messages are delivered to consuming clients.

JNDI extension (Java Naming and Directory Interface™ extension) (n.) A standard extension to the Java platform that provides Java technology-enabled applications with a unified interface to multiple naming and directory services in the enterprise. As part of the Java™ Enterprise API set, JNDI enables connectivity to heterogeneous enterprise naming and directory services.

JNDI name (Java Naming and Directory Interface™ name) (n.) A name used to access a resource that has been registered in the JNDI naming service.

job controller (n.) The *MTA* component responsible for scheduling and executing tasks upon request by various other MTA components.

JRE (Java™ runtime environment) (n.) A subset of *JDK™ software* consisting of the Java™ Virtual Machine, the Java core classes, and supporting files. Provides runtime support for applications written in the Java programming language.

`jspc` utility (n.) The compiler for pages created with *JSP™ technology*. The utility checks all JSP pages for compliance with the JSP specification.

JSP™ technology (1) (n.) A text page written using a combination of HTML or XML tags, JSP tags, and code written in the Java™ programming language. Pages created with JSP technology combine the layout capabilities of a standard browser page with the power of a programming language.

(2) (n.) Extensions that enable all JavaServer pages [technology or software?] metafunctions, including instantiation, initialization, destruction, access from other components, and configuration management. Reusable Java applications that run on a web server rather than in a web browser.

JSS See *Network Security Services for Java (JSS)*.

JTA (Java transaction API) (n.) An API that allows applications and J2EE™ servers to access transactions.

JTS (Java transaction service) (n.) The Java service for processing transactions.

key database (n.) A file that contains the key pair or pairs for a server's certificate or certificates. Also called a key file.

key-pair file See *trust database*.

knowledge information (n.) Part of the directory service infrastructure information. The directory server uses knowledge information to pass requests for information to other servers.

knowledge reference (n.) Pointers to directory information stored in different databases.

last-modified header (n.) The last modification time of the document file that is returned in the HTTP response from the server.

LDAP (Lightweight Directory Access Protocol) (n.) Directory service protocol designed to run over TCP/IP and across multiple platforms. A simplification of the X.500 Directory Access Protocol (DAP) that allows a single point of management for storage, retrieval, and distribution of information, including user profiles, distribution lists, and configuration data across Java System servers. Directory Server uses the LDAP protocol.

LDAP database (n.) A database where lists of users and groups is stored for use in authentication.

LDAP data interchange format See *LDIF*.

LDAP filter (n.) A method of specifying a set of entries that is based on the presence of a particular attribute or attribute value.

LDAP referrals (n.) An LDAP entry that consists of a symbolic link (referral) to another LDAP entry. An LDAP referral consists of an LDAP host and a distinguished name. LDAP referrals are often used to reference existing LDAP data so that this data does not have to be replicated. The LDAP referrals are also used to maintain compatibility for programs that depend on a particular entry that might have been moved.

LDAP search string (n.) A string with replaceable parameters that defines the attributes used for directory searches. For example, an LDAP search string of "uid=%s" means that searches are based on the user ID attribute.

LDAP server (n.) A software server that maintains an LDAP directory and services queries to the directory. The Sun Directory Services and the Netscape Directory Services are implementations of an LDAP Server.

LDAP server failover (n.) A backup feature for LDAP servers. If one LDAP server fails, the system can switch over to another LDAP server.

LDAP URL (n.) A *URL* that provides the means of locating directory servers using *DNS* and then completing the query through LDAP. A sample LDAP URL is `ldap://ldap.example.com`.

LDAPv3 (n.) Version 3 of the *LDAP* protocol.

LDBM (n.) LDAP database manager.

LDBM database (n.) A high-performance, disk-based database consisting of a set of large files that contain all of the data in Directory Server.

LDIF (LDAP Data Interchange Format) (n.) The format used to represent Directory Server entries in text form using *type*:*value* pairs.

leaf entry (n.) An entry under which there are no other entries. A leaf entry cannot be a branch point in a directory tree.

Legato NetWorker® software (n.) A third-party backup utility distributed by Legato Systems, Inc.

level (n.) A designation of logging verbosity, meaning the relative number of types of events that are recorded in log files. For example, at a level of Emergency, very few events are logged. At a level of Informational, many events are logged.

Liberty-enabled client (n.) A Liberty-enabled client is a client that has, or knows how to obtain, information about the identity provider that a principal will use to authenticate to a service provider.

Liberty-enabled proxy (n.) A Liberty-enabled proxy is an HTTP proxy that emulates a Liberty-enabled client.

life-cycle event (n.) A stage in the server life cycle such as startup or shutdown.

life-cycle module (n.) A module that listens for and performs its tasks in response to events in the server life cycle.

Lightweight Directory Access Protocol See *LDAP*.

listener (n.) A class, registered with a posting object, that says what to do when an event occurs.

listen port (n.) The port that a server uses to communicate with clients and other servers.

listen socket (n.) The combination of *port* number and *IP address*. Connections between the server and clients happen on a listen socket.

LMTP (Local Mail Transfer Protocol) (n.) Similar to *SMB protocol* but does not require management of a mail delivery queue. In addition, LMTP provides a status code for each recipient of a message where SMTP provides only one status code for the message. Defined in RFC 2033.

load balancer (n.) Software that controls connections to multiple gateway machines to allow approximately equivalent loads on each of the available systems.

load balancing (n.) The process of distributing the application load across nodes in the cluster so that the client requests are serviced in a timely manner. Applies only to scalable services.

load-balancing policy (n.) The preferred way in which application request load is distributed across nodes. Applies only to scalable services.

local database connection (n.) The transaction context in a local connection is local to the current process and to the current data source, not distributed across processes or across data sources.

local disk (n.) A disk that is physically private to a given cluster node.

locale (n.) A setting that identifies the collation order, character type, monetary format, and date and time format used to present data for users of a specific region, culture, or custom. The locale includes information on how data of a given language is interpreted, stored, or collated. The locale also indicates which code page should be used to represent a given language.

local interface (n.) An interface that provides a mechanism for a client that is located in the same Java™ Virtual Machine (JVM™ machine) with a session or entity bean to access that bean.

Local Mail Transfer Protocol See *LMTP*.

local part (n.) The part of an email address that identifies the recipient. See also *domain part*.

local session (n.) A user session that is only visible to one server.

local transaction (n.) A transaction that is native to one database and is restricted within a single process. Local transactions work only against a single backend. Local transactions are typically demarcated using a JDBC™ API. See also *global transaction*, *JDBC™ technology*.

log directory (n.) The directory in which all of a service's log files are kept.

log expiration (n.) The deletion of a log file from the log directory after it has reached its maximum permitted age.

logical architecture (n.) A design that depicts the logical building blocks of a distributed application and the relationships (or interfaces) between these building blocks. The logical architecture includes both the distributed *application components* and the infrastructure services components needed to support them.

logical host (n.) A Messaging Server 2.0 (minimum) concept that includes an application, the disksets or disk groups on which the application data resides, and the network addresses used to access the cluster. This concept no longer exists in the SunPlex™ system.

logical host name (n.) A resource that contains a collection of logical host names representing network addresses. Logical host name resources can only be mastered by one node at a time. See also *logical host*.

logical network interface (n.) In the Internet architecture, a host can have one or more IP addresses. Messaging Server configures additional logical network interfaces to establish a mapping between several logical network interfaces and a single physical network interface. Each logical network interface has a single IP address. This mapping enables a single physical network interface to respond to multiple IP addresses. This mapping also enables the IP address to move from one cluster member to the other in the event of a takeover or switchover without requiring additional hardware interfaces.

log rotation (n.) The creation of a new log file to be the current log file. All subsequent logged events are written to the new current file. The log file that was the previous log file is no longer written to, but remains in the log directory.

lookup (n.) Same as a search, using the specified parameters for sorting data.

mailbox (n.) A place where messages are stored and viewed. See also *folder*.

mail client (n.) The programs that help users send and receive email. The mail client is the part of the various networks and mail programs with which users have the most contact. Mail clients create and submit messages for delivery, check for new incoming mail, and accept and organize incoming mail.

mail exchange record See *MX record*.

mailing list See *mailing list*.

mailing list owner See *mail list owner*.

mail list (n.) A list of email addresses to which a message can be sent by way of a mail list address. Sometimes called a group.

mail list owner (n.) A user who has administrative privileges to add members to and delete members from the mail list.

mail relay (n.) A mail server that accepts mail from a *user agent* or an *MTA* and relays it to the mail recipient's message store or another router.

mail router See *mail relay*.

managed object (n.) An *SNMP* data element that forms part of an *MIB*. In Directory Server, the managed objects are held in `cn=monitor`, and the SNMP agent provides the objects to the network management station. As with LDAP attributes, each managed object has a name and object identifier expressed in dot notation.

managed role (n.) Allows you to create an explicit enumerated list of members.

management information base See *MIB*.

mapping (1) (n.) The ability to tie an object-oriented model to a relational model of data, usually the schema of a relational database. The process of converting a schema to a different structure.

(2) (n.) The mapping use users to security roles.

mapping tree (n.) A data structure that associates the names of suffixes (subtrees) with databases.

master See *primary*.

master agent See *SNMP master agent*.

master channel program (n.) A channel program that typically initiates a transfer to a remote system. See also *slave channel program*.

master directory server (n.) The directory server that contains the data that will be replicated.

matching category (n.) A category that matches a search query which is returned as a result of a search submission.

matching document (n.) A document that matches a search query, which is returned as the result of a search submission.

matching rule (n.) A guideline for how the server compares strings during a search operation. In an international search, the matching rule tells the server what collation order and operator to use.

MD5 (n.) A message digest algorithm by RSA Data Security. MD5 can be used to produce a short digest of data that is unique with high probability.

MD5 signature (n.) A message digest produced by the *MD5* algorithm.

MDB (message-driven bean) (n.) An enterprise bean that is an asynchronous message consumer. A message-driven bean has no state for a specific client, but its instance variables might contain state across the handling of client messages, including an open database connection and an object reference to an object based on the EJB™ architecture. A client accesses a message-driven bean by sending messages to the destination for which the message-driven bean is a message listener.

member (n.) A user or group who receives a copy of an email addressed to a mail list. See also *mailing list*, *expansion*, *moderator*.

message (n.) The fundamental unit of email that consists of a *header* and a *body* and is often contained in an *envelope* while it is in transit from the sender to the recipient.

message access services (n.) The protocol servers, software drivers, and libraries that support client access to the Messaging Server message store.

message delivery (n.) The act that occurs when an *MTA* delivers a message to a local recipient (a mail folder or a program).

message-driven bean See *MDB*.

message forwarding (n.) The act that occurs when an *MTA* sends a message delivered to a particular account to one or more new destinations as specified by the account's attributes. Forwarding might be configurable by the user. See also *message delivery*, *message routing*.

message handling system See *MHS*.

message queue (n.) The directory where messages accepted from clients and other mail servers are queued for immediate or deferred delivery.

Message Queue client runtime (n.) Software that provides JMS clients with an interface to the Java Enterprise System message server. The client runtime supports all operations needed for clients to send messages to destinations and to receive messages from such destinations.

Message Queue message server (n.) Software that provides delivery services for a Message Queue messaging system, including connections to JMS clients, message routing and delivery, persistence, security, and logging. The message server maintains physical destinations to which JMS clients send messages, and from which the messages are delivered to consuming clients.

message quota (n.) A limit defining how much disk space a particular folder can consume.

message routing (n.) The act of transferring a message from one *MTA* to another when the first MTA determines that the recipient is not a local account, but might exist elsewhere. Routing is normally configurable only by a network administrator. See also *message forwarding*.

messages (n.) Asynchronous requests, reports, or events that are consumed by JMS clients. A message has a header (to which additional fields can be added) and a body. The message header specifies standard fields and optional properties. The message body contains the data that is being transmitted.

message selector (n.) A way for a consumer to select messages based on property values (selectors) in JMS message headers. A message service performs message filtering and routing based on criteria placed in message selectors.

message service See *Message Queue message server*.

message store (n.) The database of all locally delivered messages for a Messaging Server instance. Messages can be stored on a single physical disk or stored across multiple physical disks.

message store administrator (n.) A user who has administrative privileges to manage the message store for a Messaging Server installation. This user can view and monitor mailboxes and specify access control to the store. Using proxy authorization rights, this user can run certain utilities for managing the store.

message store partition (n.) A message store or subset of a message store residing on a single physical file system partition.

message submission (n.) The client *user agent* transfers a message to the mail server and requests delivery.

message transfer agent See *MTA*.

messaging (n.) A system of asynchronous requests, reports, or events used by enterprise applications that allows loosely coupled applications to transfer information reliably and securely.

Messaging Multiplexor See *MMP*.

Messaging Server administrator (n.) The administrator whose privileges include installation and administration of a Messaging Server instance.

messaging server base directory (n.) The directory into which all servers associated with a given Administration Server on a given host are installed. Typically designated *msg_svr_base*. See also *installation directory*.

Messenger Express (n.) A mail client that enables users to access their mailboxes through a browser-based (HTTP) interface. Messages, folders, and other mailbox information are displayed in HTML in a browser window. See also *webmail*.

Messenger Express Multiplexor (n.) A proxy messaging server that acts as a Multiplexor. The server allows you to connect to the HTTP service of Messaging Server (Messenger Express). The Messenger Express Multiplexor facilitates distributing mail users across multiple server machines.

metadata (n.) Information about a component, such as the component's name and specifications for component behavior.

metadevice state database replica (n.) A database, stored on disk, that records configuration and the state of all metadevices and error conditions. This information is important to the correct operation of Solstice DiskSuite™ software disksets.

metainformation (n.) Information about a resource, such as the name of the author, the title of a document, the date of creation, and so on. The Search Engine robot uses metainformation as well as document contents when creating resource descriptions.

MHS (message handling system) (n.) A group of connected *MTA*s, their user agents, and message stores.

MIB (management information base) (n.) A tree-like structure that defines the variables that the *SNMP master agent* can access. The MIB provides access to the HTTP server's network configuration, status, and statistics. Using SNMP, you can view this information from the *NMS*. See also *AUTH*.

migration (n.) The process of transporting data files, such as data configuration or customization, from one version of a product to another.

MIME (multipurpose internet mail extensions) (n.) An emerging standard for multimedia email and messaging. A protocol you can use to include multimedia in email messages by appending the multimedia file in the message.

MIME data type (n.) MIME types control what types of multimedia files the system supports.

`mime.types` file (n.) The MIME type configuration file. This file maps file extensions to MIME types to enable the server to determine the type of content being requested. For example, requests for resources with `.html` extensions indicate that the client is requesting an HTML file, while requests for resources with `.gif` extensions indicate that the client is requesting an image file in GIF format.

mirror node (n.) An active HADB node that contains the same data as another active node, but resides in the other data redundancy unit. Each active node must have a mirror node; therefore nodes occur in pairs. When a node detects that its mirror node has failed, it takes over the failed node's role and continues service. See also *HADB node*, *active node*, *spare node*, and *data redundancy unit* (DRU).

MMP (Messaging Multiplexor) (n.) A specialized Messaging Server that acts as a single point of connection to multiple mail servers, facilitating the distribution of a large user base across multiple mailbox hosts.

mobile application configuration (n.) An Access Manager service that allows the setup of address book, calendar, and mail applications for delivery to a mobile device.

mobile client type See **client type*.

mobile device (n.) A transportable wireless device such as a mobile phone or a personal digital assistant.

mobile devices link (n.) A hypertext link appearing on the Portal Desktop.

mobile devices page (n.) A web page which allows users to manage mobile device options.

Mobile Portal Desktop (n.) A Portal Desktop displayed on a mobile device.

moderator (n.) A person who first receives all email addressed to a mailing list in order to decide if the message should be forwarded to the mailing list. The moderator can edit the message before forwarding the message to the mailing list. See also *mailing list*, *expansion*, *member*.

module (1) (n.) A web application, enterprise bean, message-driven bean, application client, or connector that has been deployed individually and outside an application. See also *component* and *life-cycle module*.

(2) (n.) A group of Java Enterprise System servers dependent on one another or closely enough related to be deployed as a unit to provide a specific service or set of services. Service modules are multi-server assemblies that have been pre-tested for use in deployment architectures.

modutil (n.) Software utility required for installing the PKCS#11 module for external encryption or hardware accelerator devices.

MTA (message transfer agent) (n.) A specialized program for routing and delivering messages. MTAs work together to transfer messages and deliver them to the intended recipient. The MTA determines whether a message is delivered to the local message store or routed to another MTA for remote delivery.

MTA configuration file (n.) The `imta.cnf` file that contains all *channel* definitions for the Messaging Server as well as the *rewrite rule* that determine how addresses are rewritten for routing.

MTA directory cache (n.) A snapshot of the directory service information about users and groups required by the MTA to process messages. See also *directory synchronization*.

MTA hop (n.) The act of routing a message from one *MTA* to another.

MUA See *user agent*.

multihomed host (n.) A host that is on more than one public network.

multihost disk (n.) A disk that is physically connected to multiple nodes.

multimaster replication (n.) A replication model in which entries can be written and updated on any of several master replica copies without requiring communication with other master replicas before the write or update is performed. Each server maintains a change log for the replica. Modifications made on one server are automatically replicated to the other servers. In case of conflict, a time stamp is used to determine which server holds the most recent version.

multiplexor (n.) The server containing the database link that communicates with the remote server.

multipurpose internet mail extensions See *MIME*.

MX record (mail exchange record) (n.) A type of *DNS* record that maps one host name to another.

n + 1 directory problem (n.) The problem of managing multiple instances of the same information in directories and databases of different types, resulting in increased hardware and personnel costs.

NAFO See *network adapter failover group*.

name collision (n.) A conflict that occurs during replication if multiple entries have been added or renamed and there is an attempt to use the same *DN*. The conflicting entries are renamed automatically by the directory servers to ensure DN uniqueness.

name identifier (n.) The pseudonym used to map a user's account information across a number of service and identity provider organizations in order to preserve anonymity. Through the use of this identifier, neither the identity provider nor the service provider know the user's actual identity.

name resolution (n.) The process of mapping an *IP address* to the corresponding name. See also *DNS*.

namespace (n.) The tree structure of an LDAP directory. See also *DIT*.

naming attribute (n.) The final attribute in a *DIT* distinguished name. See also *relative distinguished name*.

naming context (n.) A specific suffix of a *DIT* that is identified by its *DN*. In Directory Server, specific types of directory information are stored in naming contexts. For example, a naming context that stores all entries for marketing employees who work at the Example Corporation's Boston office might be called `ou=mktg, ou=Boston, o=example, c=US`.

native channel (n.) A Portal Server channel which displays native content.

native content (n.) Content written in a native markup language such as HTML that can be sent to a client without conversion.

native desktop (n.) A Portal Server Desktop that displays native content.

NDN (nondelivery notification) (n.) A nondelivery report that the *MTA* sends back to the sender (with the original message) if the MTA does not find a match during message transmission between the *address* and a *rewrite rule*.

nested role (n.) A *role* that names other role definitions. The set of members of a nested role is the union of all members of the roles it contains. Nested roles may also define extended scope to include the members of roles in other subtrees.

NetFile (n.) A Java™ technology-based file server application that enables users to have remote access to file systems, thereby enabling remote operations on files and directories.

Netlet (n.) A Java *applet* used in Java Enterprise System Portal Server to allow any applications based on *TCP/IP* to securely connect to servers through an authenticated Portal Server connection.

NetMail (n.) The NetMail component implements the NetMail (Java technology-based client) and NetMail Lite email clients. These clients work with standard IMAP and SMTP servers.

Netscape™ Console (n.) An application written in the Java™ programming language that provides server administrators with a graphical interface for managing all Netscape™ servers from one central location anywhere within the enterprise network. From any installed instance of Netscape Console, you can see and access all the Netscape servers on the enterprise's network to which you have been granted access rights.

network adapter failover group (n.) A set of one or more network adapters on the same node and on the same subnet configured to back up each other in the event of an adapter failure. Also known as NAFO group.

network address resource See *network resource*.

network management station See *NMS*.

network manager (n.) A program that reads, formats, and displays *SNMP* data. Also known as an SNMP client.

network resource (n.) A resource that contains one (or more) *logical host name* or *shared address*.

Network Security Services for Java (JSS) (n.) A class library that provides Java bindings to the Network Security Services SSL library. Portal Server uses this class library to initiate *SQL* connections from servlets and to accept SSL connections in the Portal Server Secure Remote Access Pack gateway.

news channel (n.) Forums for posting and sharing information. Users subscribe to news channels in order to see updates. The information in a news channel is usually published automatically by way of a URL or published by a user with the proper privilege. Administrators can control news channel access by assigning users to the channels they need and deciding who can see or publish information to news channels.

news channel list (n.) A window that shows all the news channels to which you are currently subscribed. Each news channel is indicated by a separate tab.

next-hop list (n.) A list of adjacent systems that a mail route uses to determine where to transfer a message. The order of the systems in the next-hop list determines the order in which the mail route transfers messages to those systems.

NIS (network information service) (n.) (UNIX only) A system of programs and data files that UNIX systems use to collect, collate, and share specific information about machines, users, file systems, and network parameters throughout a network of computers.

NMS (network management station) (n.) A powerful workstation with one or more network management applications installed. The NMS is a machine used to remotely manage your network.

NNTP (Network News Transfer Protocol) (n.) A protocol for newsgroups. You must define your news server host to use agent services on your server.

node (1) (n.) An entry in the *DIT*.

(2) (n.) A physical machine or domain (in the Sun™ Enterprise E10000 server) that can be part of a SunPlex™ system. Also known as a *host*.

(3) (n.) A computing node. One of a number of computers in a network or Internet environment. Distributed applications are deployed across this environment, with different distributed components, business services, and servers running on the various computing nodes.

node agent (n.) A node agent is a lightweight agent that is required on every machine that hosts Application Server instances, including the machine that hosts the Domain Administration Server. The node agent performs tasks including starting, stopping, creating and deleting Application Server instances as instructed by the Domain Administration Server.

non-cluster mode (n.) The resulting state achieved by booting a cluster member with the `-x` boot option. In this state, the node is no longer a cluster member, but is still a cluster node. See also *cluster member* and *cluster node*.

nondelivery notification See *NDN*.

NoPassword authentication (n.) A type of authentication that allows users to log in to the Access Manager without being prompted for a password.

NOTARY messages (n.) Nondelivery notifications (NDNs) and delivery status notifications that conform to the NOTARY specifications RFC 1892.

notification message (n.) A type of message sent by the Messaging Server providing the status of message delivery processing and the reasons for any delivery problems or outright failures. The messages are for information al purposes and require no action from the postmaster. See also *delivery status notification*.

notification service (n.) A service that receives subscriptions and notifications from other servers and then relays notifications to specific subscribers. The Calendar Server `csnotifyd` service sends notifications of events and to-do tasks using Event Notification Service (ENS) as the broker for the events.

NSAPI See *server plug-in API*.

`ns-slapd` (n.) (UNIX only) A process or service responsible for all actions of the Directory Server. On Windows systems, the equivalent is *`slapd.exe`*.

`ns-slapd.exe` (n.) (Windows only) The process monitor on Windows systems.

`obj.conf` file (n.) The server's object configuration file. This file contains additional initialization information, settings for server customizing, and instructions that the server uses to process requests from clients (such as browsers). Web Server reads this file every time it processes a client request.

object class (n.) A template specifying the kind of object that the entry describes and the set of attributes that entry contains. For example, Directory Server specifies an `emailPerson` object class which has attributes such as `commonname`, `mail` (email address), `mailHost`, and `mailQuota`.

object identifier See *OID*.

object persistence See *persistence*.

obsolete patch (n.) A patch no longer considered valid or up-to-date. A patch is considered obsolete when a subsequent version of the patch fixes the same issue, when a different patch includes the fix from the original, or when the patch is no longer considered relevant.

offline state (n.) A state in which the mail client downloads messages from a server system to a client system where they can be viewed and answered. The messages might or might not be deleted from the server.

OID (object identifier) (n.) A string representation of an object identifier which consists of a list of decimal numbers separated by periods (for example, 1.3.6.1.4.1). In *LDAP*, object identifiers are used to uniquely identify schema elements, including object classes and attribute types. The top levels of an object identifier hierarchy are managed by standards bodies and are delegated to organizations who wish to construct their own schema definitions.

online state (n.) A state in which messages remain on the server and are remotely responded to by the mail client.

operational attribute (n.) An operational attribute contains information used internally by the directory to keep track of modifications and subtree properties. Operational attributes are not returned in response to a search unless explicitly requested.

optional attribute list (n.) A list of optional attributes for a specified object class. Optional attributes are preceded by the keyword MAY.

organization (n.) In Directory Server Access Management Edition, an object that represents the top level of a hierarchical structure used by an enterprise to manage its departments and resources. Upon installation, Directory Server Access Management Edition dynamically creates a top-level organization (`default o=isp`) to manage the Directory Server Access Management Edition enterprise configurations. Additional organizations can be created after installation to manage separate enterprises. All created organizations fall beneath the top-level organization. See also *subordinate reference*.

organization administrator (n.) A user who has administrative privileges to create, modify, and delete mail users and mail lists in an organization or suborganization by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs.

O/R mapping tool (object-to-relational database tool) (n.) A mapping tool within the Application Server Administrative interface that creates XML deployment descriptors for entity beans.

OSI tree (Open Systems Interconnect tree) (n.) A *DIT* that mirrors the Open Systems Interconnect network syntax. An example of a distinguished name (*DN*) in an OSI tree would be `cn=billt,o=bridge,c=us`.

package (n.) A collection of files and directories. Packaging is a method distributing software for installation. See also *A record*, *deployment*.

parallel resource type (n.) A resource type, such as a parallel database, that has been instrumented to run in a cluster environment so that the environment can be mastered by two or more nodes simultaneously.

parallel service instance (n.) An instance of a parallel resource type running on an individual node.

parameter (1) (n.) A name-value pair sent from the Java Enterprise System Application Server client, including form field data, HTTP header information, and so on, and encapsulated in a request object. See also *attribute*.

(2) (n.) An argument to a Java method or database-prepared command.

parent access (n.) When granted, indicates that users have access to entries below their own position in the directory tree if the *bind DN* is the parent of the targeted entry.

partition See *message store partition*.

passivation (n.) A method of releasing a bean's resources from memory without destroying the bean. In this way, a bean is made to be persistent and can be recalled without the overhead of instantiation.

pass-through authentication See *PTA*.

pass-through subtree (n.) In pass-through authentication, the PTA Directory Server passes through bind requests to the authenticating Directory Server from all clients whose *DN* is contained in this subtree.

password authentication (n.) Identification of a user through user name and password. See also *certificate-based authentication*.

password file (n.) (UNIX only) A file that stores UNIX user login names, passwords, and user ID numbers. The password file is also known as `/etc/passwd` because of where the file is located.

password policy (n.) A set of rules that govern how passwords are used in a given directory.

patch (n.) A quick modification to a routine or an object program. See also *accumulated patch*, *obsolete patch*, *patch version number*.

patch version number (n.) The last two digits of the patch identifier, for example, “nnnnnn-03”. The number is increased by one each tome a new version of the patch is released.

pattern (n.) A string expression used for matching purposes, such as in Allow and Deny filters.

PDC (personal digital certificate) (n.) An electronic certificate attached to a message that authenticates a user. A personal digital certificate can be created by correctly entering a user ID and password or by using an *SSL certificate* request that in turn uses the security certificate of the server through which the user is connected.

peer (n.) A subcategory that has the same parent category as another.

permanent failure (n.) An error condition that occurs during message handling. When a permanent failure occurs, the message store deletes its copy of an email message. The *MTA* bounces the message back to the sender and deletes its copy of the message.

permissions (1) (n.) A set of privileges granted or denied to a user or group. This information includes the user or group name, valid email address or addresses, and how and where email is delivered.

(2) (n.) In the context of access control, the permission states whether access to the directory information is granted or denied and the level of access that is granted or denied. See also *access rights*.

(3) (n.) The settings that control the access to a calendar. For example, in Calendar Express, permissions include Availability, Invite, Read, Delete, and Modify. Calendar Server administrators set permissions as *ACE* strings using command-line utilities. See also *ACL*.

persistence (1) (n.) For enterprise beans, the protocol for transferring the state of an entity bean between its instance variables and an underlying database. See also *transience*.

(2) (n.) For sessions, the session storage mechanism.

persistence manager (n.) The entity responsible for the *persistence* of the *entity bean* or beans installed in the container.

persistent state (n.) Where the state of an object is kept in persistent storage, usually a database.

personal digital certificate See *PDC*.

personal folder (n.) A folder that can be read only by the owner. See also *shared folder*.

pk12util (n.) The software utility required to export the certificate and key databases from your internal machine and import them into an external PKCS#11 module.

PKI (public key infrastructure) (n.) Enables the identity of a user to be linked to a browser or mobile device. Wireless PKI refers to *certificate-based authentication* that occurs on the handset.

plaintext (n.) A method for transmitting data. The definition depends on the context. With *SQL*, plaintext passwords are encrypted and are therefore not sent as cleartext. With *SASL*, plaintext passwords are hashed, and only a hash of the password is sent as text.

plaintext authentication See *password authentication*.

pluggable authentication (n.) A mechanism that allows J2EE™ applications to use the Java™ Authentication and Authorization Service (JAAS) software from the J2SE™ platform. Developers can plug in their own authentication mechanisms.

plug-in (1) (n.) A code extension to the browser that displays or executes content inside a web page. Plug-ins enable the browser to display page content elements that the browser would otherwise not be able to display.

(2) (n.) An accessory program that can be loaded and then used as part of the overall system. For example, the Calendar Server can use a plug-in to access a non-LDAP directory service.

pointer CoS (n.) A pointer class of service which identifies the template entry using the template DN only.

point-to-point delivery model (n.) A model where producers address messages to specific queues and consumers extract messages from queues established to hold their messages. A message is delivered to one message consumer only.

policy (1.) (n.) A rule that describes who is authorized to access a specific resource under specific conditions. The rule can be based on groups of users or roles in an organization.

(2) (n.)In Directory Server Access Management Edition, defines rules to help protect an organization's web resources. Policies are assigned to organizations and roles only.

poll (n.) The function in Instant Messaging Server that enables you to ask users for their response to a question. You can send a question and possible answers to selected users, and they respond with their selected answer.

pooling (n.) The process of providing a number of pre-configured resources to improve performance. If a resource is pooled, a component can use an existing instance from the pool rather than instantiating a new one. In the Java Enterprise System Application Server, database connections, servlet instances, and enterprise bean instances can all be pooled.

POP3 (Post Office Protocol Version 3) (n.) A protocol that provides a standard delivery method and that does not require the *MTA* to have access to a user's mail folders. Not requiring access is an advantage in a networked environment where often the mail client and the message transfer agent are on different computers.

port (n.) The location (socket) to which *TCP/IP* connections are made. Web servers traditionally use port 80, FTP uses port 21, and telnet uses port 23. Java Enterprise System Portal Server uses special ports, particularly on client systems, to securely communicate through the Portal Server session to servers.

portal (n.) An entry point to a set of resources that an enterprise wants to make available to the portal's users. For some consumer portals, the set of resources includes the entire World Wide Web, but for most enterprises, the set of resources includes information, applications, and other resources that are specific to the relationship between the user and the enterprise. The Portal Server Desktop is the application used to generate the portal in Portal Server.

Portal Desktop (n.) Any one of the desktops generated by Portal Server.

portal node (n.) A physical machine that is running Portal Server software or Portal Server Pack software. Also called a *host*.

port number (n.) A number that specifies an individual *TCP/IP* application on a host machine. Provides a destination for transmitted data.

postdeployment (n.) A stage of the Java Enterprise System solution life-cycle process in which distributed applications are started up, monitored, tuned to optimize performance, and dynamically upgraded to include new functionality.

postmaster account (n.) An alias for the email group and email addresses that receive system-generated messages from the Messaging Server. The postmaster account must point to a valid mailbox or mailboxes.

Post Office Protocol Version 3 See *POP3*.

potential master See *potential primary*.

potential primary (n.) A cluster member that is able to master a *failover resource* type if the *primary* node fails. See also *default master*.

predeployment (n.) A stage of the Java Enterprise System solution life-cycle process in which business needs are translated into a *deployment scenario*: a *logical architecture* and a set of quality-of-service requirements that a solution must meet.

prepared command (n.) A database command in *spider* that is precompiled to make repeated execution more efficient. Prepared commands can contain parameters. See also *prepared statement*.

prepared statement (n.) A class that encapsulates a `QUERY`, `UPDATE`, or `INSERT` statement that is used repeatedly to fetch data. A prepared statement contains at least one *prepared command*.

presence index (n.) A filtering method which enables efficient searching for entries that contain an attribute of a specified type, regardless of the value of the attribute in the entry.

presentation layout (n.) The format of web page content.

presentation logic (n.) Activities that create a page in an application, including processing a request, generating content in response, and formatting the page for the client. Usually handled by a web application.

preset message (n.) Short messages that can be written and saved as Portal Server Mobile Access mobile preferences for later use with a mobile mail application.

primary (n.) A *node* on which a resource group or device group is currently online. A primary is a node that is currently hosting or implementing the service associated with the resource. See also *secondary*.

primary document directory See *document root*.

primary host name (n.) The name of a node on the primary public network. The primary host name is always the node name specified in `/etc/nodename`. See also *secondary host name*.

primary key (n.) The unique identifier that enables the client to locate a particular entity bean.

primary key class name (n.) A variable that specifies the fully qualified class name of a bean's primary key. Used for Java Naming and Directory Interface™ (JNDI) lookups.

principal (n.) A principal is an entity that can acquire a federated identity, that is capable of making decisions, and to which authenticated actions are done on its behalf. Examples of principals include an individual user, a group of individuals, a corporation, other legal entities, or a component of the Liberty architecture.

private host name (n.) The *host name* alias used to communicate with a *node* over the *cluster interconnect*.

private key See *public-key cryptography*.

privilege (n.) A type of access right that is granted to a user, a set of users, or a resource.

process (1) (n.) A self-contained, fully functional execution environment set up by an operating system. Each instance of an application typically runs in a separate process. See also *thread*.

(2) (n.) Execution sequence of an active program. A process is made up of one or more threads.

produce (v.) To pass a message to the client runtime for delivery to a destination.

producer (n.) An object (MessageProducer) created by a session that is used for sending messages to a destination. In the point-to-point delivery model, a producer is a sender (QueueSender). In the publish/subscribe delivery model, a producer is a publisher (TopicPublisher).

production environment (n.) A stage of the application life-cycle process, in which distributed applications are started up, monitored, tuned to optimize performance, and dynamically upgraded to include new functionality.

programmatic security (n.) The process of controlling security explicitly in code rather than allowing the component's container, a bean's container, or a servlet engine, for instance, to handle it. Opposite of *declarative security*.

programmer-demarcated transaction See *bean-managed transaction*.

propagation behavior (n.) The synchronization process between a consumer and a supplier.

property (n.) A single attribute that defines the behavior of an application component. In the `server.xml` file, a property is an element that contains a name-value pair.

protocol (1) (n.) A set of rules that describes how devices on a network exchange information.

(2) (n.) A formal description of messages to be exchanged and rules to be followed for two or more systems to exchange information.

provider (n.) The programmatic aspect of a channel. Adding configuration data to a provider differentiates it into an instance of a channel. A provider is a Java™ class and is responsible for converting the content in a file or the output of an application or service into the proper format for a channel. A number of providers are shipped with the Portal Server including a bookmark provider, an application provider, and a notes provider. As the desktop is imaged, each provider is queried in turn for the content of its associated channel. Some providers are capable of generating multiple channels based upon their configuration.

Examples of content providers include the `UserInfoProvider` and `BookmarkProvider`. Examples of *container* providers include the `TabContainerProvider` and `SingleContainerProvider`. Examples of leaf providers include the `JSPProvider`, `XMLProvider`, `URLScraperProvider` and `SimpleWebServicesProvider`.

provisioning (n.) The process of adding, modifying or deleting entries in the Java Enterprise System Directory Server. These entries include users and groups and domain information.

proxy (1) (n.) The mechanism whereby one system acts on behalf of another system in responding to protocol requests. Proxy systems are used in network management to avoid having to implement full protocol stacks in simple devices, such as modems.

(2) (n.) An intermediary program that makes and services requests on behalf of clients. Proxies act as servers and clients in turn and are used to control the content of various network services. See also *reverse proxy*.

proxy authorization (n.) A special form of authentication where a client binds to the directory with its own identity but is granted the access rights of another user on a per operation basis. This other user is referred to as the proxy user, and its *DN* is the proxy DN.

proxy DN (n.) The *DN* of an entry that has access permissions to the target on which the client application is attempting to perform an operation. Used with *proxy authorization*.

Proxylet (n.) A dynamic proxy server than runs on a client machine to redirect a URL to the SRA Gateway. See also *Sun Java™ System Portal Secure Remote Access (SRA)*.

PTA (pass-through authentication) (n.) Mechanism by which one Java Enterprise System Directory Server consults another Directory Server to check bind rules.

PTA Directory Server (n.) In *PTA*, the PTA Directory Server sends (passes through) bind requests it receives to the authenticating Directory Server.

PTA LDAP URL (n.) In *PTA*, the URL that defines the authenticating Directory Server, pass-through subtree or subtrees, and optional parameters.

public folder (n.) A folder with multiple owners that is shared by multiple people who can access it. Depending on the *ACL*s set for the folder, more than one person can update or administer the folder.

public information directories (n.) (UNIX only) Directories not inside the document root that are in a UNIX user's home directory or under the user's control, or directories that are under the user's control.

public key (n.) The encryption key used in public-key encryption.

public-key certificate (n.) A data structure containing a user's public key, as well as information about the time and date during which the certificate is valid.

public-key cryptography An method of encryption. In public-key cryptosystems, everyone has two related complementary keys: a publicly revealed key and a secret key (also known as a private key). Each key unlocks the code that the other key makes. Knowing the public key does not help you deduce the

corresponding secret key. The public key can be published and widely disseminated across a communications network. This protocol provides privacy without the need for the secure channels that a conventional cryptosystem requires. Also known as asymmetric key cryptography.

public-key encryption (n.) A cryptographic method that uses a two-part key (code) that consists of public and private components. To encrypt messages, the published public keys of the recipients are used. To decrypt the messages, the recipients use their unpublished private keys known only to them.

public key infrastructure See *PKI*.

Public Network Management (n.) Software that uses fault monitoring and failover to prevent loss of node availability because of single network adapter or cable failure. Public Network Management failover uses sets of network adapters called a *network adapter failover group* to provide redundant connections between a cluster node and the public network. The fault monitoring and failover capabilities work together to ensure availability of resources.

publish and subscribe delivery model (n.) A model which publishers and subscribers are generally anonymous and can dynamically publish or subscribe to a topic. The system distributes messages arriving from a topic's multiple publishers to its multiple subscribers.

purge a message (v.) To permanently remove a message that has been deleted and is no longer referenced in user and group folders. The space is then returned to the message store file system. See also *delete a message* and *expunge a message*.

QOS (quality of service) (n.) The performance limits you set for a server instance or virtual server. For example, if you are an ISP, you might want to charge different fees for virtual servers depending on how much bandwidth is provided. You can limit the amount of bandwidth and the number of connections.

queue (n.) An object created by an administrator to implement the point-to-point delivery model. A queue is always available to hold messages even when the client that consumes its messages is inactive. A queue is used as an intermediary holding place between producers and consumers.

quorum device (n.) A disk shared by two or more nodes that contributes votes used to establish a quorum for the cluster to run. The cluster can operate only when a quorum of votes is available. The quorum device is used when a cluster becomes partitioned into separate sets of nodes to establish which set of nodes constitutes the new cluster.

RAF (robot application function) (n.) A function that can be used in robot filter configuration files. User-defined robot application functions are also called plug-in functions. These functions are invoked by directives.

RAM (random access memory) (n.) The physical semiconductor-based memory in a computer.

RAR file (resource archive file) (n.) A Java™ archive (JAR) file that contains a resource adapter.

RC2 (n.) A variable key-size block cipher by RSA Data Security.

`rc.2.d` file (n.) (UNIX only) A file on UNIX machines that describes programs that are run when the machine starts. This file is also called `/etc/rc.2.d` because of its location.

RC4 (n.) A stream cipher by RSA Data Security. Faster than RC2.

RD See *resource description*.

RDB (n.) Relational database.

RDBMS (n.) Relational database management system.

RDM See *resource description message*.

RDN (relative distinguished name) (n.) The name of the actual entry itself, before the entry's ancestors have been appended to the string to form the full *DN*. Most RDNs consist of a single attribute type and value from the entry.

read-only bean (n.) An entity bean that is never modified by an EJB™ client. See also *entity bean*.

realm (n.) A scope over which a common security policy is defined and enforced by the security administrator of the security service. Also known as a security policy domain or security domain in the J2EE™ specification.

redirection (n.) A mechanism by which clients accessing a particular URL are sent to a different location, either on the same server or on a different server. Redirection is useful if a resource has moved and you want the clients to use the new location transparently. Redirection is also used to maintain the integrity of relative links when directories are accessed without a trailing slash.

reference deployment architecture (n.) A *deployment architecture* that has been designed, implemented, and tested for performance. Reference deployment architectures are used as starting points for designing deployment architectures for custom solutions.

referential integrity (n.) The mechanism that ensures that relationships between entries expressed by *DN*-valued attributes are maintained within the directory.

referral (n.) When a server receives a search or update request from a client that it cannot process, the server sends back to the client a pointer to the Java Enterprise System Directory Server that can process the request.

referral hop limit (n.) The maximum number of referrals that a client should follow in a row.

regular expression (n.) A text string that uses special characters to represent ranges or classes of characters for the purpose of pattern matching.

relative distinguished name See *RDM*.

relaying (n.) The process of passing a message from one messaging server to another messaging server.

remote interface (n.) One of two interfaces for Enterprise JavaBeans™ components. The remote interface defines the business methods callable by a client.

rendering (n.) The process of converting content written in Abstract Markup Language (AML) to the appropriate device-specific markup language for a specific mobile device.

rendering channel (n.) A Portal Server Mobile Access channel that displays rendering content.

rendering engine (n.) In Portal Server, converts AML to the language appropriate for a given mobile client.

rendering filter (n.) The filter that passes content for conversion between the rendering engine and client.

replica (n.) An instance of an area of *replication* on a server. See also *consumer replica* and *supplier replica*.

replica cycle See *replication cycle*.

replica directory server (n.) The directory that receives a copy of all or part of the data.

replica group (n.) The servers that hold instances of a particular area of replication. A server can be part of several replica groups.

replication (n.) The process of synchronizing data distributed across Directory Servers and rectifying update conflicts.

replication agreement (n.) A set of configuration parameters that are stored on the supplier server and that identify the suffixes to replicate, the consumer servers to which the data is pushed, the times during which *replication* can occur, the *DN* and credentials used by the supplier to bind to the consumer, and how the connection is secured.

replication base entry (n.) The *DN* of the root of a replicated area.

replication cycle (n.) The interval during which update information is exchanged between two or more replicas. The replication cycle begins during an attempt to push data to or pull data from another replica or set of replicas and ends when the data has successfully been exchanged or when an error is encountered.

replication session (n.) A session set up between two servers in a *replica group* to pass update information as part of a *replication cycle*.

request object (n.) An object that contains page and session data produced by a client, passed as an input parameter to a servlet or a page created with the *JSP™ technology*.

required attribute list (n.) A list of required attributes for a specified object class. Required attributes are preceded by the keyword MUST.

required attributes (n.) Attributes that must be present in entries using a particular object class. See also *allowed attributes*, *attribute*.

resource (1) (n.) An instance of a resource type. Many resources of the same type might exist with each resource having its own name and set of property values so that many instances of the underlying application might run on the cluster.

(2) (n.) Any item on a network that can be identified by a *URL*, such as a web page, a document, or an FTP directory. A resource is often referred to informally as a document.

(3) (n.) Any *URL*, directory, or program that the server can access and send to a client that requests it.

resource calendar (n.) A calendar associated with a resource such as a meeting room or equipment such as a notebook computer or overhead projector.

resource description (n.) A list of attribute-value pairs associated with a resource through a *URL*. Agents can generate resource descriptions automatically or people can write resource descriptions manually. Once a repository of resource descriptions is assembled, the server can export the repository through resource description messages as a programmatic way for web agents to discover and retrieve the resource descriptions. Resource descriptions are stored in *SOIF* format.

resource description message (n.) A mechanism to discover and retrieve metadata about network-accessible resources, known as resource descriptions.

resource group (n.) A collection of resources that are managed by the *RGM* as a unit. Each resource that is managed by the RGM must be configured in a resource group. Related and interdependent resources are typically grouped.

resource group manager See *RGM*.

resource group state (n.) The state of the resource group on any given node.

resource invocation (n.) An instance of a resource type running on a node. An abstract concept representing a resource that was started on the node.

Resource Management API (n.) The application programming interface within a SunPlex™ system that makes an application highly available in a cluster environment. Also known as RMAPI.

resource manager (n.) An object that acts as a facilitator between a resource such as a database or message broker and client or clients of the resource such as Java Enterprise System Application Server processes. Controls globally available data sources.

resource monitor (n.) An optional part of a resource type implementation that runs periodic fault probes on resources to determine if the resources are running correctly and how they are performing.

resource offering (n.) In a Discovery Service, a resource offering defines associations between a piece of identity data and the service instance that provides access to it.

resource reference (n.) An element in a deployment descriptor that identifies the component's coded name for the resource.

resource state (n.) The state of an RGM resource on a given node.

resource status (n.) The condition of the resources as reported by the fault monitor.

resource type (n.) The unique name given to a *data service*, `LogicalHostname`, or `SharedAddress` cluster object. Data service resource types can either be failover types or scalable types. See also *failover resource*, *scalable resource*.

resource type property (n.) A key-value pair that is used to describe and manage resources of the given type and is stored by the RGM as part of the resource type.

response buffer (n.) The Portal Server Mobile Access server response buffer stores large responses as separate smaller responses so that they fit limited device buffers.

response object (n.) An object that references the calling client and provides methods for generating output for the client.

restart (v.) To start the *robot* without deleting its state information, which causes the robot to start running in the same state in which it previously stopped. Opposite of a *fresh start*.

restore (v.) To copy the contents of folders from a backup device to the message store. See also *back up*.

`ResultSet` object (n.) An object that implements the `java.sql.ResultSet` interface. `ResultSet` objects are used to encapsulate a set of rows retrieved from a database or other source of tabular data.

retro changelog (n.) Stores changes in the order of arrival on the local server and not in the order in which these changes were applied to the system. The retro changelog was not designed to function in a multimaster replication environment. Not the same as *change log*, as the retro changelog is not used in replication. Provides backward compatibility with Directory Server 4.

reusable component (n.) A component created so that it can be used in more than one capacity, for example, by more than one resource or application.

reverse DNS lookup (n.) The process of querying the *DNS* to resolve a numeric *IP address* into the equivalent *fully qualified domain name*.

reverse proxy (n.) A proxy that performs bidirectional URL rewriting and translation between clients and servers. Unlike a proxy, which exists at the client side, a reverse proxy exists at the server side of the network. In Java Enterprise System Portal Server, the reverse proxy exists in Java Enterprise System Portal Server Secure Remote Access Pack.

Rewriter (n.) The Rewriter provides a Java™ class library for rewriting URL references in various web languages, such as HTML, Javascript, and XML, and in HTTP location headers (redirections). The Rewriter defines a Java Enterprise System Directory Server Access Management Edition service for storing rules that define how rewriting is to be done and the data to be rewritten. The Rewriter also includes an admin console module for editing these rules.

rewrite rule (n.) A tool that the *MTA* uses to route messages to the correct host for delivery. Rewrite rules perform the following functions: (1) extract the host and domain specification from an address of an incoming message, (2) match the host and domain specification with a rewrite rule pattern, (3) rewrite the host and domain specification based on the domain template, and (4) decide which channel queue the message should be placed in. Also known as a domain rewrite rule.

RFC (request for comments) (n.) A document series maintained by the Internet Engineering Task Force that describes the Internet suite of protocols and related experiments. Very few RFCs describe Internet standards, but all Internet standards are published as RFCs. See `http://www.imc.org/rfcs.html`.

RGM (resource group manager) (n.) A software facility used to make cluster resources highly available and scalable by automatically starting and stopping these resources on selected cluster nodes. The RGM acts according to pre-configured policies in the event of hardware or software failures or reboots.

RMI (remote method invocation) (n.) A standard set of Java APIs that enable developers to write remote interfaces that can pass objects to remote processes.

RMIC (n.) remote method invocation compiler.

robot (n.) A program that finds all the resources located in a specific portion of a network.

robot application function See *RAF*.

role (1) (n.) A functional grouping of subjects in an application represented by one or more groups in a deployed environment. See also *user*, *group*.

(2) (n.) In Java Enterprise System Directory Server Access Management Edition, a grouping that represents a selection of privileged operations. By applying the role to a user or a service, the principal can perform the operations. For example, by confining certain privileges to an Employee role or a Manager role and applying the role to a user, the user's accessibility is confined to the privileges granted to it by the role. Roles are defined using access control instructions (*ACI*s).

(3) (n.) An entry grouping mechanism. Each role has members, which are the entries that possess the role.

role-based attributes (n.) Attributes that appear on an entry because the entry possesses a particular role within an associated *CoS* template.

rollback (n.) Cancellation of a *transaction*.

root (n.) (UNIX only) The most privileged user on UNIX machines. The root user has complete access privileges to all files on the machine.

root DN (n.) The *DN* of the *Directory Manager*.

Root DSE (n.) An entry that is automatically generated by the Directory Server and is returned from a `baseObject` search with a *DN* that is empty (zero bytes long). The Root DSE provides information to clients about the server's configuration, such as a pointer to the *subschema entry*, a list of the DNs of the naming contexts held by the server, and a list of the *LDAPv3* controls and extensions that the server supports. See also *DSE*.

root entry (n.) The top-level entry of the *DIT* hierarchy.

root suffix (n.) The parent of one or more *sub suffix*. A directory tree can contain more than one root suffix.

router (n.) A system responsible for determining on which path network traffic will flow. A router uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as a "routing matrix." In Open Systems Interconnect terminology, a router is a Network Layer intermediate system. See also *fully qualified domain name*.

routing See *message routing*.

routing tables (n.) The internal databases that hold the information about message originators and recipients.

row (n.) A single data record that contains values for each column in a table.

`RowSet` object (n.) An object that encapsulates a set of rows retrieved from a database or other source of tabular data. The `RowSet` object extends the `java.sql.ResultSet` interface, enabling the *`ResultSet` object* to act as a component based on the JavaBeans™ component architecture.

RPC (remote procedure call) (n.) A mechanism for accessing a remote object or service.

RTT (\round trip time) (n.) The elapsed time for transit of a signal over a closed circuit (from the server to the client and back). This delay is important in systems that require two-way interactive communication where the RTT directly affects the throughput rate. In the context of Java Enterprise System Directory Server, the RTT and the TCP window can have a significant impact on replication performance over a wide-area network. Also known as round-trip delay time.

rules (n.) Logical tests applied to determine whether a condition is met. The robot uses rules as part of filters for determining types of content to index and in classification rules to determine what category to assign to a resource.

runtime system (n.) The software environment in which programs run. The runtime system includes all the code necessary to load programs written in the Java™ programming language, to link native methods dynamically, to manage memory, and to handle exceptions. An implementation of the Java virtual machine is included, which might be a Java interpreter.

SAF (server application function) (n.) A function that participates in request processing and other server activities.

safe file system (n.) A file system that performs logging so that if a system crashes the system can roll back the data to a pre-crash state and restore all data. An example of a safe file system is Veritas File System, VxFS.

SASL (simple authentication and security layer) (n.) A means for controlling the mechanisms by which POP, IMAP or *SMB protocol* clients identify themselves to the server. Java Enterprise System Messaging Server support for SMTP SASL use complies with RFC 2554 (ESMTP AUTH). SASL is defined in RFC 2222. See also *POP3* and *IMAP4*.

scalable coherent interface (n.) High-speed interconnect hardware used as the *cluster interconnect*.

scalable resource (n.) A resource that runs on multiple nodes (an instance on each node) using *cluster interconnect* to give the appearance of a single service to remote clients of the service.

scalable service (n.) A data service implemented that runs on multiple nodes simultaneously.

schema (n.) Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory might be unable to display the proper results.

schema checking (n.) A verification process which ensures that entries added or modified in the directory conform to the defined schema. Schema checking is on by default and users receive an error if they try to save an entry that does not conform to the schema.

schema name (n.) The schema or type of a *SOIF*. For example, a SOIF for a document has the schema name `@DOCUMENT`, while a SOIF for a *resource description message* header has the schema name `@RDMHeader`.

SCM See *service control manager*.

scoping (n.) Restrictions placed on the resource descriptions imported by an import agent. The syntax used is the same as that for user searches.

search base See *base DN*.

Search database (n.) A searchable database of resource descriptions usually generated by a robot. See also *robot*.

Search Engine (n.) A search feature incorporated into Portal Server 6.0. Previously called Compass Server (Portal Server 3.0). The Search Server holds a database of resource descriptions gathered by robots, usually categorized. Users can search the resource descriptions or browse through the categories to locate particular resources.

secondary (n.) A cluster member that is available to master disk device groups and resource groups in the event that the primary fails. See also *primary*.

secondary host name (n.) The name used to access a node on a secondary public network. See also *primary host name*.

secure socket layer See *SSL*.

security (n.) A screening mechanism that ensures that application resources are only accessed by authorized clients.

security-module database (n.) A file that contains information describing hardware accelerators for *SQL* ciphers. Also called `secmod`.

self access (n.) When granted, indicates that users have access to their own entries if the *bind DN* matches the targeted entry.

self-generated certificate (n.) Public key value only used when entities are named using the message digest of their public value and when these names are securely communicated. See also *issued certificate*.

sendmail (n.) (UNIX only) A common *MTA*. In most applications, Java Enterprise System Messaging Server can be used as a drop-in replacement for sendmail.

serializable object (n.) An object that can be deconstructed and reconstructed, which enables it to be stored or distributed among multiple servers.

server (n.) A multi-threaded software process (as distinguished from a hardware server) that provides a distributed or cohesive set of services for *clients* that access the service by way of an external interface.

server administrator (n.) The person who performs server management tasks. The server administrator provides restricted access to tasks for a particular server, depending upon task *ACI*s. The configuration administrator must assign user access to a server. Once a user has server access permissions, that user is a server administrator who can provide server access permissions to users.

server assembly (n.) A group of Java Enterprise System servers dependent on one another or closely enough related to be installed or deployed as a unit.

server authentication (n.) A method of authentication which allows a client to make sure that it is connected to a secure server, preventing another computer from impersonating the server or attempting to appear secure when the server is not secure.

server daemon (n.) A process when running that listens for and accepts requests from clients.

server instance (n.) A server can contain multiple instances in the same installation on the same machine. Each instance has its own directory structure, configuration, and deployed applications. Each instance can also contain multiple virtual servers. See also *virtual server*.

Server Message Block protocol (n.) A protocol that provides a method for client applications in a computer to read and write to files on and to request services from server programs in a computer network. The SMB protocol can be used over the Internet on top of its *TCP/IP* protocol or on top of other network protocols such as Internetwork Packet Exchange and NetBEUI. Java Enterprise System Portal Server uses SMB for NetFile.

server plug-in API (n.) An extension that allows you to extend and customize the core functionality of Java Enterprise System servers and provide a scalable, efficient mechanism for building interfaces between the HTTP server and back-end applications. Also known as NSAPI.

server process (n.) A self-contained, fully functional execution environment set up by an operating system. Each instance of an application typically runs in a separate process.

server root (1) (n.) A directory on the server machine dedicated to holding the server program and configuration files, maintenance files, and information files. Also known as ServerRoot.

(2) (n.) A directory location relative to other files on a server. For example, the default Calendar Server installation for Solaris systems uses the path `/opt/SUNWics5/` as the server root.

(3) (n.) The directory into which all Java Enterprise System servers associated with a given Java Enterprise System Administration Server on a given host are installed. See also *installation directory* and *instance directory*.

server-side rules (n.) A set of rules for enabling server-side filtering of mail. Based on the Sieve mail filtering language.

service (1) (n.) A function provided by a server. For example, Java Enterprise System Messaging Server provides SMTP, POP, IMAP, and HTTP services.

(2) (n.) A software function performed for one or more *clients*. This function might be at a very low level, such as a memory management, or at a high level, such as a credit check *business service*. A high-level service can consist of a family of individual services. Services can be local (available to local clients) or distributed (available to remote clients).

service control manager (n.) (Windows NT only) An administrative program for managing services.

service quality component (n.) One of a number of kinds of *system components* included in Java Enterprise System. Support components, which include access components and administrative components, provide support for *system service components*.

service provider (n.) Commercial or not-for-profit organizations that offer web-based services. Can include internet portals, retailers, transportation providers, financial institutions, entertainment companies, libraries, universities, and governmental agencies.

service stack (n.) A layering of distributed services that are needed to support distributed enterprise applications. The layering reflects the dependency of higher-level services on the services below them in the stack.

servlet (1) (n.) Server-side programs written in the Java™ programming language that web servers run to generate content in response to a client request. Servlets are similar to applets in that they run on the server-side but servlets do not use a user interface.

(2) (n.) An instance of the `Servlet` class. A servlet is a reusable application that runs on a server. In the Java Enterprise System Application Server, a servlet acts as the central dispatcher for each interaction in an application by performing presentation logic, invoking business logic, and invoking or performing presentation layout.

servlet engine (n.) An internal object that handles all servlet metafunctions. Collectively, a set of processes that provide services for a servlet, including instantiation and execution.

servlet runner (n.) The part of the servlet engine that invokes a servlet with a request object and a response object. See *servlet engine*.

session (1) (n.) An object used by a servlet to track a user's interaction with a web application across multiple *HTTP* requests.

(2) (n.) An instance of a client-server connection. See also *client-server model*

(3) (n.) For Java Enterprise System Portal Server, a sequence of interactions between a user and one or more applications, starting with login and ending with logout or timeout.

(4) (n.) For Message Queue, a single threaded context for sending and receiving messages. This can be a queue session or a topic session.

session bean (n.) An enterprise bean that is created by a client and usually exists for the duration of a single client-server session only. A session bean performs operations for the client, such as calculations or accessing other enterprise beans. While a session bean can be transactional, a session bean is not recoverable if a system crash occurs. Session bean objects can be either stateless (not associated with a particular client) or stateful (associated with a particular client), so they can maintain conversational state across methods and transactions. See also *stateful session bean* and *stateless session bean*.

session cookie (n.) A cookie that is returned to the client containing a user session identifier. See also *sticky cookie*.

session key (n.) A common cryptographic technique to encrypt each individual conversation between two people with a separate key.

session timeout (n.) A specified duration after which a sever can invalidate a user session.

shared address (n.) A network address that can be bound by all scalable services running on nodes within the cluster to make them scale on those nodes. A cluster can have multiple shared addresses, and a service can be bound to multiple shared addresses.

shared component (n.) One of a number of kinds of *system components* included in Java Enterprise System. Shared components, usually libraries, provide local services to other system components. By contrast, a *system service component* provides distributed infrastructure services to other system components (or to *application components*).

shaded component descriptor file (n.) A file containing metadata for a given shared component (usually in XML format).

shared folder (n.) A folder that can be read by more than one person. Shared folders have an owner who can specify read access to the folder and who can delete messages from the shared folder. The shared folder can also have a moderator who can edit, block, or forward incoming messages. Only IMAP folders can be shared. See also *personal folder*, *public folder*.

shared-key cryptography (n.) A type of cryptography where each party must have the same key to encrypt or decrypt ciphertext. Also known as symmetric key cryptography.

SHTML (server-side include Hypertext markup language) (n.) An HTML file that includes embedded server-side includes (SSIs).

Sieve (n.) A proposed language for filtering mail.

simple authentication and security layer See *SASL*.

simple index (n.) A type of directory listing that displays only the names of the files without any graphical elements. The opposite of fancy indexing.

Simple Mail Transfer Protocol See *SMB protocol*.

Simple Network Management Protocol See *SNMP*.

Simple Object Access Protocol See *SOAP*.

SIMS (n.) Solstice Internet Mail Server™ and Sun Internet Mail Server™.

single field substitution string (n.) In a rewrite rule, part of the domain template that dynamically rewrites the specified address token of the host and domain address. See also *domain template*.

single identity (n.) An identity that a user has by virtue of a single user entry in a Java Enterprise System directory. Based on this single user entry a user can be allowed access to various Java Enterprise System resources, such as a portal, web pages, and services such as messaging, calendar, and instant messaging.

single-instance resource (n.) A resource for which at most one resource can be active across the cluster.

single logout (n.) The ability of a user to log out from an identity provider or a service provider, and to be logged out from all service providers or identity providers in that authentication domain.

single-master replication (n.) A replication model in which only one server, the master, allows *LDAP* write access to the replicated data. In a single-master replication model, the supplier or master server maintains a change log.

single sign-on (SSO) (1) (n.) A feature that allows a user's authentication to one service in a distributed system to be automatically applied to other services in the system.

(2) (n.) A situation where a user's authentication state can be shared across multiple J2EE™ applications in a single virtual server instance. See *SSO*.

(3) (n.) The authentication process established when a user with a federated identity authenticates to an identity provider. Because the user has a federated identity, the user can access affiliated service providers without having to reauthenticate.

site (n.) A location on the network where the *robot* goes to look for resources. You determine the address of the site and the kinds of documents you want to index there in a *site definition*.

site definition (n.) Constraints placed on where a robot can go to locate resources. Using site definitions, you can limit a robot to a particular server, a specified group of servers, or a domain. A site definition includes filters that describe what types of documents the robot should index from the site.

SIZE (n.) An *SMTP* extension enabling a client to declare the size of a particular message to a server. The server might indicate to the client that it is or is not willing to accept the message based on the declared message size. The server can declare the maximum message size it is willing to accept to a client. Defined in RFC 1870.

`slapd.exe` (n.) (Windows only) The process or service responsible for all actions of the Directory Server. On UNIX systems, the equivalent is *`ns-slapd`*.

slave channel program (n.) A channel program that accepts transfers initiated by a remote system. See also *master channel program*.

smart host (n.) The mail server in a domain to which other mail servers forward messages if they do not recognize the recipients.

SMB protocol See *Server Message Block protocol*.

SMTP (Simple Mail Transfer Protocol) (n.) The email protocol most commonly used by the Internet and the protocol supported by the Java Enterprise System Messaging Server. Defined in RFC 821, with associated message format descriptions in RFC 822.

SMTP AUTH See *AUTH*.

SMTP proxy (n.) A variant of SMTP that sends messages from one computer to another on a network and is used on the Internet to route email.

sn attribute (n.) LDAP alias for surname.

SNMP (Simple Network Management Protocol) (n.) A protocol used to exchange data about network activity. With SNMP, data travels between a managed device (anything that runs SNMP such as hosts, routers, your web server, and other servers on your network) and an *NMS*.

SNMP master agent (n.) Software that exchanges information between the various subagents and the *NMS*.

SNMP SOCKS (n.) Firewall software that establishes a connection from inside a firewall to the outside when direct connection would otherwise be prevented by the firewall software or hardware, for example, the router configuration.

SNMP subagent (n.) Software that gathers information about the managed device and passes the information to the master agent.

SOAP (Simple Object Access Protocol) (n.) A protocol that defines a standardized way of invoking methods in objects distributed in diverse operating environments across the Internet. Uses a combination of XML-based data structuring and Hypertext Transfer Protocol (HTTP).

soft restart (n.) A way to restart the server that causes the server to internally restart by rereading its configuration files. A soft restart sends the process the `HUP` signal (signal number one). The process itself does not die, as it does in a hard restart.

SOIF (summary object interchange format) (n.) A syntax for transmitting resource descriptions and other kinds of structured objects. Each resource description is represented as a list of attribute-value pairs. SOIF handles both textual and binary data as values and with some minor extensions multi-valued attributes. SOIF is a streaming format that allows bulk transfer of many resource descriptions in a single, efficient stream.

SOIF attribute (n.) A type of data base attribute. Each resource description in the search database has multiple attributes or fields. These attributes are known as SOIF attributes.

Solaris™ logical name (n.) The name typically used to manage Solaris™ Operating System devices. For disks, these usually look something like `/dev/rdsk/c0t2d0s2`. For each Solaris logical device name, there is an underlying Solaris physical device name. See also *DID name* and *Solaris™ physical name*.

Solaris™ physical name (n.) The name that is given to a device by its device driver in the Solaris™ Operating System. The name shows up on a Solaris machine as a path under the `/devices` tree. For example, a typical SI disk has a Solaris physical name similar to `devices/sbus@1f,0/SUNW,fas@e,8800000/sd@6,0:c,raw`. See also *Solaris™ logical name*.

Solstice DiskSuite™ software (n.) A volume manager used by the SunPlex™ system. See also *virtual server class*.

spare node (n.) An HADB node that can replace a failed active node. If an active node fails, a spare node copies data from the mirror node and becomes active. See also *HADB node*,*active node*, *mirror node*, and *data redundancy unit*.

spider See *robot*.

split brain (n.) A condition in which a cluster breaks up into multiple partitions, with each partition forming without the knowledge of the existence of any other partition.

spoofing (n.) A form of network attack in which a client attempting to access or send a message to a server misrepresents its host name.

SQL (structured query language) (n.) A language commonly used in relational database applications. SQL2 and SQL3 designate versions of the language.

SSL (secure socket layer) (n.) A form of secure, low-level encryption that is used by other protocols like HTTP and FTP. The SSL protocol includes provisions for server authentication, encryption of data in transit, and optional client authentication.

SSL authentication (n.) A method of authentication which confirms users' identities with security certificates by using the information in the client certificate as proof of identity, or verifying a client certificate published in an LDAP directory.

SSL certificate (n.) An electronic token that means you or a vendor have given approval to encrypt and decrypt your secure transactions using *PKI*. You create a self-signed SSL Certificate when you install Java Enterprise System Portal Server software. However, you can also obtain an SSL Certificate from a certificate vendor who authorizes secure communications services over the Internet.

SSO See *single sign-on (SSO)*.

SSR See *server-side rules*.

standard index (n.) Indexes that are maintained by default.

starting points (n.) The list of sites that a Search Engine robot visits to begin enumeration of resources.

state (1) (n.) The circumstances or condition of an entity at any given time.

(2) (n.) A distributed data storage mechanism that you can use to store the state of an application using the Java Enterprise System Application Server feature interface `IState2`. See also *conversational state*, *persistent state*.

stateful session bean (n.) A session bean that represents a session with a particular client and which automatically maintains state across multiple client-invoked methods.

stateless session bean (n.) A session bean that represents a stateless service. A stateless session bean is completely transient and encapsulates a temporary piece of business logic needed by a specific client for a limited time span.

static group (n.) A mail group defined statically by enumerating each group member. See also *dynamic group*.

static web content (n.) Static HTML files, images, applet Java™ archive (JAR) files, and anything else that can be served up directly by the web server without using the Java web container. For Java Enterprise System Portal Server, the web files are installed in the web server (same place as dynamic web application).

status event (n.) Status of a user including whether online.

sticky cookie (n.) A *cookie* that is returned to the client to force the client to always connect to the same server process. See also *session cookie*.

sticky load balancing (n.) A method of *load balancing* where an initial client request is load balanced, but subsequent requests are directed to the same process as the initial request.

stop word (n.) A word identified to the search function as a word on which the search function should not search, for example, words such as "the," "a," "an," and "and." Also known as a drop word.

stored procedure (n.) A block of statements written in *spider* and stored in a database. You can use stored procedures to perform any type of database operation, such as modifying records, inserting records, or deleting records. The use of stored procedures improves database performance by reducing the amount of information that is sent over a network.

streaming (n.) A technique for managing how data is communicated through *HTTP*. When results are streamed, the first portion of the data is available for use immediately. When results are not streamed, the whole result must be received before any part of it can be used. Streaming provides a way to allow large amounts of data to be returned in a more efficient way, improving the perceived performance of the application.

`strftime` function (n.) A function that converts a date and a time to a string. This function is used by the server when appending trailers. The `strftime` function has a special format language for the date and time that the server can use in a trailer to illustrate a file's last-modified date.

subagent See *SNMP subagent*.

subdomain (n.) The next-to-last part of a *fully qualified domain name* that identifies the division or department within a company or organization that owns the domain name (for example, `support.example.com` and `sales.example.com`). A subdomain is not always specified.

subnet (n.) The portion of an *IP address* that identifies a block of host IDs.

subordinate reference (n.) The naming context that is a child of the naming context held by your directory server. See also *knowledge information*.

suborganization (n.) In Java Enterprise System Directory Server Access Management Edition, an object created under an organization and used by an enterprise for more granular control of its departments and resources. For example, when setting up your Java Enterprise System Portal Server, you might create a suborganization called `mycompany` under the top-level object `isp`.

subschema entry (n.) An entry containing all the schema definitions (definitions of object classes, attributes, matching rules, and so on) used by entries in part of a directory tree.

substring index (n.) A search filer which allows for efficient searching against substrings within entries. Substring indexes are limited to a maximum of three characters per index key.

sub suffix (n.) A branch underneath a root suffix.

suffix (n.) The name of the entry in the directory tree below which data is stored. Multiple suffixes are possible within the same directory. Each database only has one suffix.

summary object interchange format See *SOIF*.

Sun™ Cluster software (n.) The software portion of the SunPlex™ system. See also *SunPlex™ system*.

Sun Java™ System Communications Express (n.) Software that provides an integrated web-based communication and collaboration client that caters to the needs of enterprise users for accessing email, calendar, and address book information.

Sun Java™ System Connector for Microsoft Outlook (n.) A plug-in that enables Microsoft Outlook to be used as a desktop client with Sun Java Enterprise System.

Sun Java™ System Portal Secure Remote Access (SRA) (n.) SRA allows most client devices access to personalized portal applications, content, files and services through a secure connection.

Sun Java™ System Synchronization (n.) Software that runs on a Microsoft Windows personal computer and enables users to synchronize calendar events and tasks with mobile devices and personal information managers (PIMs) such as Microsoft Outlook.

SunPlex™ system (n.) The integrated hardware and Sun™ Cluster software system that is used to create highly available and scalable services.

superuser (n.) (UNIX only) The most privileged user available on UNIX machines. Also known as root. The superuser has complete access privileges to all files on the machine.

supplier (n.) A server containing the master copy of directory trees or subtrees that are replicated to consumer servers.

supplier replica (n.) A replica that contains a master copy of directory information and can be updated. A server can hold any number of master replicas.

supplier server (n.) In the context of replication, a server that holds a replica that is copied to a different server is called a supplier server for that replica.

switchback See *failback*.

switchover (n.) (UNIX only) The orderly transfer of a resource group or device group from one master (node) in a cluster to another master (or multiple masters, if resource groups are configured for multiple primaries). A switchover is initiated by an administrator by using the `scswitch` command.

symlinks (n.) (UNIX only) A special file or directory that points to another file or directory so that both files or directories have the same contents.

symmetric encryption (n.) Encryption that uses the same key for both encrypting and decrypting. The Data Encryption Standard (DES) is an example of a symmetric encryption algorithm.

symmetric key cryptography See *shared-key cryptography*.

synchronization (1) (n.) The update of data by a master directory server to a replica directory server.

(2) (n.) The update of the *MTA* directory cache.

system administrator (n.) The person who administers Java Enterprise System software and deploys Java Enterprise System applications.

system component (n.) Any software package or set of packages included in the Java Enterprise System and installed by the Java Enterprise System installer. There are several kinds of system components: *system service components* that provide distributed infrastructure *services*, *service quality component*s which support the system services components by providing access and administrative services, and *shared components* that provide local services to other system components.

system index (n.) An index that cannot be deleted or modified as it is essential to Directory Server operations.

system service (n.) One or more distributed *services* that define the unique functionality provided by Java Enterprise System. System services normally require the support of a number of *service quality components* and/or a number of *shared components*.

system service component (n.) One of a number of kinds of *system components* included in Java Enterprise System. System services components provide the main Java Enterprise System infrastructure services: portal services, communication and collaboration services, identity and security services, web and application services, and availability services.

System Service Processor (n.) In Sun Enterprise™ 10000 server configurations, a device external to the cluster used specifically to communicate with cluster members.

table (n.) A named group of related data in rows and columns in a database.

takeover See *failover*.

target (n.) In the context of access control, the target identifies the directory information to which a particular *ACI* applies.

target entries (n.) The entries within the scope of a *CoS*.

task (n.) In Calendar Express on the client side, a component of a calendar that specifies something to be done. On the server side, a task is also called a *todo*.

taxonomy (n.) A system of categories for the resources in the Java Enterprise System Portal Server Search Engine.

TCP/IP (Transmission Control Protocol/Internet Protocol) (n.) The main network protocols for the Internet and for enterprise networks.

telnet (n.) Virtual terminal protocol in the Internet suite of protocols. Enables users of one host to log in to a remote host and interact as normal terminal users of that host.

telnet proxy (n.) An application that sits between the telnet client and telnet server and acts as an intelligent relay.

template entry See *coserver*.

terminal concentrator (n.) In configurations that are not Sun Enterprise™ 10000 configurations, a device that is external to the cluster and is used specifically to communicate with cluster members.

thread (n.) An execution sequence inside a process. A process might allow many simultaneous threads, in which case the process is multithreaded. If a process executes each thread sequentially, the process is single threaded.

timeout (n.) A specified time after which the server should give up trying to finish a service routine that appears to be hung.

time zone (n.) A geographical region that uses the same time. There are 25 hourly time zones from -12 through +12 (*GMT* is 0). Each time zone is measured relative to GMT. Most time zones have localized designations in three-letter abbreviations. The Calendar Server also identifies time zones using a time zone ID (TZID) such as America/Los_Angeles or Asia/Calcutta.

TLS (Transport Layer Security) (n.) A protocol that provides encryption and certification at the transport layer so that data can flow through a secure channel without requiring significant changes to the client and server applications. The standard for *SQL*, a public key-based protocol.

todo (n.) On the server side, a component of a calendar that specifies something to be done. In Calendar Express on the client side, a todo is called a *task*.

top (n.) (UNIX only) A program on some UNIX systems that shows the current state of system resource usage.

topic (n.) An object created by an administrator to implement the publish and subscribe delivery model. A topic can be viewed as a node in a content hierarchy that is responsible for gathering and distributing messages addressed to it. By using a topic as an intermediary, message publishers are kept separate from message subscribers.

top-level administrator (n.) A user who has administrative privileges to create, modify, and delete mail users, mail lists, family accounts, and domains in an entire Messaging Server namespace by using the Delegated Administrator for Messaging and Collaboration GUI or CLIs. By default, this user can act as a message store administrator for all messaging servers in the topology.

top-level domain authority (n.) The highest category of host name classification, usually signifying either the type of organization the domain is (for example, `.com` is a company and `.edu` is an educational institution) or the country of its origin (for example, `.us` is the United States, `.jp` is Japan, `.au` is Australia, and `.fi` is Finland).

topology (n.) The way a directory tree is divided among physical servers and how these servers link with one another.

transaction (1) (n.) A set of database commands that succeed or fail as a group. All the commands involved must succeed for the entire transaction to succeed.

(2) (n.) An atomic unit of work which must either be completed or entirely rolled back.

transaction attribute (n.) An attribute that controls the scope of a transaction.

transaction context (n.) A transaction's scope, either local or global. See *local transaction*, *global transaction*.

transaction isolation level (n.) Determines the extent to which concurrent transactions on a database are visible to one another.

transaction manager (n.) An object that controls a global transaction, normally using the *XA protocol*. See also *global transaction*.

transaction recovery (n.) Automatic or manual recovery of distributed transactions.

transience (n.) A protocol that releases a resource when it is not being used. Opposite of *persistence*.

transient failure (n.) An error condition that occurs during message handling. The remote *MTA* is unable to handle the message when the message is delivered but might be able to handle the message later. The local MTA returns the message to the queue and schedules the message for retransmission at a later time.

Transmission Control Protocol (TCP) (n.) The basic transport protocol in the Internet protocol suite that provides reliable, connection-oriented stream service between two hosts.

Transmission Control Protocol/Internet Protocol (TCP/IP) (n.) The name given to the collection of network protocols used by the Internet protocol suite. The name refers to the two primary network protocols of the suite: TCP (Transmission Control Protocol), the transport layer protocol, and IP (Internet Protocol), the network layer protocol.

Transport Layer Security (TLS) (n.) The standardized form of SSL. See also *secure socket layer*.

transport protocols (n.) Protocols which provide the means to transfer messages between *MTA*s, for example SMTP and X.400.

trust database (n.) A security file that contains the public and private keys. Also referred to as the *key-pair file*.

trusted provider (n.) One of a group of service providers and identity providers in a *circle of trust*. Users can transact and communicate with trusted providers in a secure environment.

UA See *user agent*.

UAProf (n.) A specification defined by the Open Mobile Alliance that allows a mobile device to communicate its capabilities to a network server.

UBE See *unsolicited bulk email*.

UDDI (Universal Description, Discovery, and Integration) (n.) Provides worldwide registry of web services for discovery and integration.

uid (n.) (UNIX only) A unique number associated with each user on a UNIX system.

unified messaging (n.) The concept of using a single message store for email, voicemail, fax, and other forms of communication. Java Enterprise System Messaging Server provides the basis for a complete unified messaging solution.

uniform resource indicator See *URI*.

uniform resource locator See *URL*.

uninstallation (n.) The process of removing a software component in its entirety.

universal principal name (n.) The value for a logged-in user that includes the login name combined with the domain to which the user belongs. For example, a user `bill` in domain `example.com` has the Universal Principal Name of `bill@example.com`. Also known as UPN.

unsolicited bulk email (n.) Unrequested and unwanted email sent from bulk distributors usually for commercial purposes. Also known as spam.

upgrade (n.) The process of installing updated product bits over existing product bits.

upper reference (n.) Indicates the directory server that holds the naming context above your directory server's naming context in the *DIT*.

URI (universal resource identifier) (n.) Describes a specific resource at a domain. Locally described as a subset of a base directory so that `/ham/burger` is the base directory and a URI specifies `toppings/cheese.html`. A corresponding URL would be `http://domain.port/toppings/cheese.html`.

URL (uniform resource locator) (n.) The addressing system used by the server and the client to request documents. A URL is often called a location. The format of a URL is *protocol*`://`*machine*`.`*port*`/`*document*. A sample URL is `http://www.example.com/index.html`.

URL database repair (n.) A process that repairs and updates a URL database that has been damaged by a software failure, a system crash, a disk breakdown, or a full file system.

URL mapping (n.) The process of mapping a document directory's physical path name to a user-defined alias so that files within the directory need only refer to the directory's alias instead of the file's full physical path name. Instead of identifying a file as `usr/JES/servers/docs/index.html`, you could identify the file as `/myDocs/index.html`. This mapping provides additional security for a server by eliminating the need for users to know the physical location of server files.

URL pool (n.) The list of URLs for the robot to process. When the robot starts, the URL pool consists of the starting points, but the pool is quickly augmented with any resources found during enumeration.

use case (n.) A specific end-user task or set of tasks performed by a *distributed enterprise application*, and used as a basis for designing, testing, and measuring the performance of the application.

user (n.) A person or service which uses an application. Programmatically, a user consists of a user name, password, and set of attributes that enables an application to recognize a user. See also *group* and *role*.

user account (n.) An account for accessing a server maintained as an entry on a directory server.

userAgent (n.) For Portal Server Mobile Access, a property that refers to the HTPP user-agent header. The user-agent header is often unique to a particular mobile device and can be used to detect and retrieve data for a client type.

user agent (n.) The client component, such as Netscape™ Communicator, that allows users to create, send, and receive mail messages. Also known as UA.

user entry (n.) Fields that describe information about each user, required and optional. Examples are distinguished name, full name, title, telephone number, pager number, login name, password, home directory, and so on. Also known as user profile.

user folders (n.) A user's email mailboxes.

user group (n.) The group to which the user of a Message Queue client belongs for purposes of authorizing access to Message Queue message server resources, such as connections and destinations.

User/Groups Directory Server (n.) A Directory Server that maintains information about users and groups in an organization.

user ID (1) (n.) User identification. A unique string identifying a user to a system. Also referred to as a userid.

user quota (n.) The amount of space configured by the system administrator that is allocated to a user for email messages.

user provisioning (n.) The process by which services are made available to end users or by which end users are provided with access to services. Provisioning involves identity, policy, and user account management activities, such as creating an account in a directory for each end user and populating the account with the user-specific information needed by various services.

user session (n.) A series of user application interactions that are tracked by the server. Sessions maintain user state, persistent objects, and identity authentication.

UUCP (UNIX to UNIX Copy Protocol) (n.) (UNIX only) A protocol used for communication between consenting UNIX systems.

vanity domain (n.) A domain name associated with an individual user and not with a specific server or hosted domain. A vanity domain is specified by using the `MailAlternateAddress` attribute. The vanity domain does not have an *LDAP* entry for the domain name. Vanity domains are useful for individuals or small organizations that desire a customized domain name without the administration overhead of supporting their own hosted domain. Also called custom domain.

`/var/mail` (n.) A name often used to refer to Berkeley-style inboxes in which new mail messages are stored sequentially in a single, flat text file.

Veritas Cluster Server (n.) High availability clustering software from Veritas Software with which Java Enterprise System Messaging Server can integrate.

VERITAS Volume Manager (n.) A volume manager used by the SunPlex™ system. See also *virtual server class*.

versioning See *dynamic reloading*.

virtual domain (1) (n.) An ISP-hosted domain.

(2) (n.) A domain name added by the Messaging Multiplexor to a client's user ID for LDAP searching and for logging into a mailbox server. See also *document type definition*, *hosted domain*.

virtual list view index (n.) A filtering method which speeds up the display of entries in the Directory Server Console (or other graphical user interface) if the client with the user interface uses the virtual list view extension. Virtual list view indexes can be created on any branch in the directory tree to improve display performance for specific searches. Also known as the browsing index.

virtual private network (n.) A network with the appearance and functionality of a regular network but which is similar to a private network within a public one. The use of encryption in the lower protocol layers provides a secure connection through an otherwise insecure network, typically the Internet. VPNs are generally cheaper than true private networks using private lines. VPNs rely on having the same encryption system at both ends. The encryption might be performed by firewall software or possibly by routers.

virtual server (1) (n.) A virtual web server that serves content targeted for a specific URL. Multiple virtual servers can serve content using the same or different host names, port numbers, or IP addresses. The HTTP service can direct incoming web requests to different virtual servers based on the URL. Also known as a virtual host.

(2) (n.) Virtual servers are a way of setting up multiple domain names, IP addresses, and server monitoring capabilities with a single installed server.

virtual server class (n.) A collection of virtual servers that share the same basic configuration information in a `obj.conf` file.

voice Portal Desktop (n.) The audio presentation of a Portal Server site as presented by a telephone or similar device.

voiceXML (n.) A markup language for creating audio dialogues for interactive voice response applications.

VoIP (voice over IP) (n.) Technology that provides voice telephony over IP networks.

volume manager (n.) A software product that provides data reliability through disk striping, concatenation, mirroring, and dynamic growth of metadevices or volumes.

VPN See *virtual private network*.

VPN gateway (n.) The entry point to a VPN. Typically protected by a firewall.

VRFY (n.) An SMTP command for verifying a user name. Defined in RFC 821.

WAP (Wireless Application Protocol) (n.) An open standard that runs applications through wireless communications.

WAR file See *web application archive*.

WCAP (Web Calendar Access Protocol) (n.) A high-level, command-based protocol used by clients to communicate with the Calendar Server.

web application (n.) A collection of servlets, pages created with *JSP™ technology*, HTML documents, and other web resources, which might include image files, compressed archives, and other data. A web application can be packaged into a web archive (a WAR file) or exist in an open directory structure. Java Enterprise System Application Server also supports some non Java web application technologies, such as *SHTML* and *CGI*.

web application archive (n.) An archive file that contains a complete web application in compressed form. Java Enterprise System Web Server cannot access an application in a WAR file. You must decompress a web application (deploy it using the `wdeploy` utility) before Java Enterprise System Web Server can serve it.

web cache (n.) A Java Enterprise System Application Server feature that enables a servlet or a page created with *JSP™ technology* to cache its results for a specific duration in order to improve performance. Subsequent calls to that servlet or JSP page within the duration are given the cached results so that the servlet or JSP page does not have to execute again.

web connector plug-in (n.) An extension to a web server that enables the web server to communicate with the Java Enterprise System Application Server.

web container See *container*.

webmail (n.) A generic term for browser-based email services. A browser-based client, known as a "thin" client because more processing is done on the server, accesses mail that is always stored on a server. See also *Messenger Express*.

web module (n.) An individually deployed web application. See *web application*.

web server (1) (n) A host that stores and manages HTML pages and web applications, but not full J2EE applications. The web server responds to user requests from web browsers.

(2) (n.) An application that responds to web requests such as HTTP, FTP, and so on.

(3) (n.) A software program or server computer equipped to offer World Wide Web access. A web server accommodates requests from users, retrieves requested files or applications, and issues error messages.

web server plug-in (n.) An HTTP reverse proxy plug-in that allows you to instruct a Java Enterprise System Web Server or Java Enterprise System Application Server to forward certain HTTP requests to another server.

web service (n.) A service that conforms to standardized Internet protocols for accessibility, service encapsulation, and discovery. The standards include the SOAP (Simple Object Access Protocol) messaging protocol, the WSDL (Web Service definition Language) interface definition, and the UDDI (Universal Discovery, Description, and Integration) registry standard.

(2) (n.) A service offered through the web. A self-contained, self-describing, modular application that can accept a request from a system across the Internet or an intranet, process it, and return a response.

web service consumer (n.) A web service consumer invokes the operations a Web service provides by making a request to a Web service provider.

web service provider (n.) A web service provider implements a Web service based on a request from a Web service consumer. It may run on the same Java™ virtual machine as the Web service consumer using it.

wildcard (n.) A special character in a search string that can represent one or more other characters or ranges of characters.

Windows CGI (n.) (Windows NT only) *CGI* programs written in a Windows-based programming language such as Visual Basic.

wireless desktop dispatcher (n.) A component that determines to which Portal Desktop, mobile Portal Desktop, or voice Portal Desktop user requests are routed.

withdrawn patch (n.) A patch which has been removed from distribution systems.

WML (wireless markup language) (n.) A markup language based on XML which is part of the WAP.

workgroup (n.) Local workgroup environment, where the server performs its own routing and delivery within a local office or workgroup. Interdepartmental mail is routed to a backbone server. See also *backbone*.

WSDL (web services description language) (n.) An XML-based language used to define web services in a standardized way. Describes three fundamental properties of a web service: definition of the web service, how to access that web service, and the location of that web service.

X.400 (n.) A message handling system standard.

X.500 standard (n.) The set of ISO/ITU-T documents outlining the recommended information model, object classes, and attributes used by Directory Server implementation. *LDAP* is a lightweight version of the Directory Access Protocol (DAP) used by the X.500 standard.

XA protocol (n.) A database industry standard protocol for distributed transactions.

XHTML (extensible hypertext markup language) (n.) A reformulation of HTML 4.0 which can be extended by adding new elements and attributes.

XML (extensible markup language) (n.) A flexible programming language developed by the World Wide Web Consortium (W3C) to create common information formats and to share both the format and the data on the web, intranets, and elsewhere. XML is extensible because, unlike HTML, the markup symbols are unlimited and self-defining. The Calendar Server uses XML and XSL to generate the Calendar Express user interface.

XML namespace (n.) A standard that allows you to specify a unique label to the set of element names defined by a DTD (document type definition). A document using that DTD can be included in any other document without having a conflict between element names. The elements defined in the DTD are then uniquely identified so that, for example, the parser can determine when an element should be interpreted according to your DTD and not according to that of another document type definition.

XSL (extensible style language) (n.) A language used to create style sheets for XML, similar to cascading style sheets (CSS) that are used for HTML. In XML, content and presentation are separate. XML tags do not indicate how they should be displayed. An XML document has to be formatted before it can be read, and the formatting is usually accomplished with style sheets. Style sheets consist of formatting rules for how particular XML tags affect the display of a document on a computer screen or printed page.

XSLT (extensible style language transformation) (n.) The language used by XML style sheets to transfer one form of an XML document to another XML form. This transition is extremely useful in e-commerce and e-business, as the transition serves as a common denominator across many different platforms and varying XML document coding.

Zulu time (n.) A military designation for *GMT* and UTC (coordinated universal time).