Common files

Contents

Glossary

access control list (ACL)
In computer security, a list that is associated with an object that identifies all the subjects that can access the object and their access rights.

access control groups
Groups to be used for access control. Each group contains a multivalued attribute that consists of member DNs. Access control groups have an object class of 'AccessGroup'.

access permissions
There are two sets of access permissions:

- Permissions that apply to an entire object
- Permissions that apply to attribute access classes or individual attributes.

aclEntry
A multivalue attribute that contains information that pertains to the access allowed to the entry and its attributes. An aclEntry lists the following types of information: who has rights to the entry (scope of the protection), what attributes or classes of attributes the user has access to (attribute access classes), and what rights the user or group has (permission).

aclPropagate
The attribute that controls ACL propagation. If the value is set to true, ACLs are propagated down the hierarchy tree. If the value is set to false, the ACL becomes an override, pertaining only to this particular object.

aclSource
A read only operational attribute that is associated with each object. This attribute contains the distinguished name (DN) of the entry in which the access control list (ACL) is defined.

Advanced Encryption Standard (AES)
A data encryption technique that improved upon and officially replaced the Data Encryption Standard (DES).

alias
A pointer to another directory object. Aliases can be used within LDAP to reference entries anywhere within the directory tree.

attribute access class
Class that consists of attributes that require similar permission for access. Attributes are assigned to an access class within the schema files. The user-modifiable access classes are normal, sensitive, critical, and restricted. An additional class of system is not user-modifiable.

bulkload
A command-line utility that is used for bulk-loading large amounts of data in LDIF format.

cascading replication
A replication topology in which there are multiple tiers of servers. A peer/master server replicates to a small set of read-only servers, which in turn replicate to other servers. Such a topology off-loads replication work from the master servers.

cipher
A cryptographic algorithm that is used to encrypt data that is unreadable until converted into plain data with a predefined key.

CipherSpec
The combination of encryption algorithm and hash function that is applied to an SSL message after authentication completes.

cipher specifications
Specifications that indicate the data encryption algorithm and key size to use for secure connections.

cipher suite
The combination of authentication, key exchange algorithm, and the Secure Sockets Layer (SSL) cipher specification used for the secure exchange of data.

consumer server
A server that receives changes through replication from a supplier server.

digital signature
Information that is encrypted with a private key and is appended to a message or object to assure the recipient of the authenticity and integrity of the message or object. The digital signature proves that the message or object was signed by the entity that owns, or has access to, the private key or shared-secret symmetric key. Digital signatures are used for authentication and integrity assurance of digital data.

directory schema
The valid attribute types, object classes, matching rules and syntaxes that can appear in a directory. The attribute types and object classes define the syntax of the attribute values, which attributes must be present, and which attributes might be present for specific object classes.

Directory Server instance
A Directory Server instance is comprised of all of the nonexecutable files that are required for a Directory Server and its corresponding administration daemon to run on a machine. These files include the ibmslapd.conf file, the schema files, the stash files, and the log files of the Directory Server instance. Each server instance and its corresponding administration daemon listens on a unique port with the same IP address.

distinguished name (DN)
The name that uniquely identifies an entry in a directory. A distinguished name is made up of attribute=value pairs, which are separated by commas.

dynamic group
A group that is defined by using a search expression. A directory entry that matches the search expression is automatically a member of the group.

DMS (Database Managed Space)
A table space where the database manager controls the storage space.

entryOwner
An attribute whose value can refer to a user or a group. Each entry has an associated entryOwner attribute. However, the entryOwner subject has all authority to the entry.

Federated Directory Server
Federated Directory Server enables a collection of directories and other sources of data to be combined and treated as a single hierarchical directory.

Forwarding server
A read-only server that replicates all changes sent to it. This server contrasts to a peer/master server in that it is read only and it can have no peers.

Gateway server
A server that forwards all replication traffic from the local replication site where it resides to other Gateway servers in the replicating network. Also receives replication traffic from other Gateway servers within the replication network, which it forwards to all servers on its local replication site.

Gateway servers must be masters (writable).

group
A logical organization of users based on some common criteria. Groups can be used in specifying a common set of directory access permissions.

hashing algorithm
The algorithm that is used by the anonymizer to anonymize a hash value into a cryptographic irreversible data value.

iKeyman

A tool supplied with the Gateway for maintaining digital certificates for SSLight and JSSE.

The ikeyman tool is a user-friendly GUI tool for managing key files. This tool allows creating of public-private key pairs and certificate requests, receiving certificate requests into a key database, and managing keys in a key database.

virtual appliance
A virtual appliance is a pre-configured virtual desktop environment.

Virtual Directory
Virtual Directory is an advance proxy server that works with LDAP directories from different vendors in the back-end. It aggregates identity data across multiple sources to create a single point of access. All identity remains in the original source and is fetched or updated at real-time.

indexing rules
Index rules that are attached to attributes make it possible to retrieve information faster. The IBM® Security Directory Suite provides the following indexing rules:

- Equality
- Approximate
- Substring
- Reverse

ldapadd
The LDAP modify-entry and LDAP add-entry tool ldapmodify is a shell-accessible interface to the ldap_modify and ldap_add library calls. **ldapadd** is implemented as a renamed version of **ldapmodify**. When invoked as ldapadd the **-a** (add new entry) flag is turned on automatically.

ldapdelete
The LDAP delete-entry tool ldapdelete is a shell-accessible interface to the ldap_delete library call. ldapdelete opens a connection to an LDAP server and binds and deletes one or more entries. If one or more dn arguments are provided, entries with those Distinguished Names (DN) are deleted. Each DN must be a string-represented DN.

ldapmodify
The LDAP modify-entry and LDAP add-entry tools ldapmodify is a shell-accessible interface to the ldap_modify and ldap_add library calls. **ldapadd** is implemented as a renamed version of **ldapmodify**. When invoked as ldapadd, the **-a** (add new entry) flag is turned on automatically.

ldapmodrdn
LDAP modify-entry RDN tool ldapmodrdn is a shell-accessible interface to the ldap_modrdn library call. **ldapmodrdn** opens a connection to an LDAP server and binds and modifies the RDN of entries. The entry information is read from standard input, from a file, by using the **-f** option, or from the command-line pair DN and RDN.

ldapsearch
The LDAP search tool ldapsearch is a shell-accessible interface to the ldap_search library call. **ldapsearch** opens a connection to an LDAP server and binds and does a search by using the filter . The filter must conform to the string representation for LDAP filters.

LDAP Data Interchange Format (LDIF)
A format that is used by the LDAP import-export tools and ldapmodify, ldapadd, and ldapsearch command-line utilities to represent LDAP entries or changes to entries in a standard portable text form. See RFC 2849.

ldif2db
This program is used to load entries that are specified in text LDAP Directory Interchange Format (LDIF) into a directory stored in a relational database. The database must already exist. **ldif2db** can be used to add entries to an empty directory database or to a database that already contains entries.

LMI
The local management interface (LMI) is the graphical user interface for virtual appliance.

matching rule
A rule that describes how to do a comparison.

multiple values
Multiple values are used to assign more than one value to an attribute. The attribute can have multiple values, for example, to accommodate a maiden and married surname. To add multiple values to an attribute, click **Multiple values**, then add one value per line. If an attribute contains multiple values, the field is displayed as a drop-down list.

nested group
A child group entry whose distinguished name (DN) is referenced by an attribute contained within a parent group entry. The ibm-membergroup attribute is defined to explicitly distinguish nested groups from ordinary members.

nested subtree
A subtree within another subtree of the directory.

object class definition
Statement that specifies which attributes must be present in an object of that class, and also attributes that might be present. Every entry contains an objectClass attribute that identifies what type of information the entry contains.

object class types
Object classes can be structural, for example, person; abstract, for example top; or auxiliary, for example ePerson.

ownerPropagate
The attribute that controls directory object ownership propagation. If the value is set to true, directory object ownership is propagated down the hierarchy tree. If that attribute is set to false, the entry owner that is specified is an override, pertaining only to this particular entry.

ownerSource
A read only operational attribute that contains the distinguished name (DN) of the entry in which the owner values are defined. Each entry has an associated ownerSource attribute. This attribute is maintained by the server but can be retrieved for administrative purposes.

Peer server
The term that is used for a master server when there are multiple masters for a specified subtree. A peer server does not replicate changes that are sent to it from another peer server; it replicates only the changes that are originally made on it.

Proxy Server
A server that receives requests that are intended for another server and that acts on the client's behalf (as the client's proxy) to obtain the requested service. A Proxy Server is often used when the client and the server are incompatible for direct connection. For example, the client is unable to meet the security authentication requirements of the server but must be permitted some services.

public key

The non-secret half of a cryptographic key pair that is used with a public key algorithm. The public key is made available to everyone. Public keys are typically used to verify digital signatures or decrypt data that was encrypted with the corresponding private key.

In secure communication, an algorithmic pattern that is used to decrypt messages that were encrypted by the corresponding private key. A public key is also used to encrypt messages that can be decrypted only by the corresponding private key. Users broadcast their public keys to everyone with whom they must exchange encrypted messages.

quiesce
To put the server into a state in which it does not accept client updates, except for the updates that are done by the administrator and accompanied by replication management control.

referral
A way for servers to refer clients to additional Directory Servers. Referrals can distribute namespace information among multiple servers, provide knowledge of where data resides within a set of interrelated servers, and route client requests to the appropriate server. The general format for a referral is: ldap[s]://hostname:port. Typically the format for a referral to a nonsecure server is: `ldap://hostname:389` and to a secure SSL server is: `ldaps://hostname:636`.

relative distinguished name (RDN)
The first component of the distinguished name (DN). For example, if the entry's DN is cn=John Doe,ou=Test,o=sample, the RDN is cn=John Doe.

replica
A server that contains a copy of the directory or a copy of part of the directory of another server. Replicas back up servers to enhance performance or response times and to ensure data integrity.

replicated subtree
A portion of the directory information tree (DIT) that is replicated from one server to another. Under this design, a specified subtree can be replicated to some servers and not to others. A subtree can be writable on a specified server, while other subtrees might be read-only.

Replicating network
A network that contains connected replication sites.

replication agreement
Information that is contained in the directory that defines the connection or replication path between two servers. One server is called the supplier (the one that sends the changes) and the other is the consumer (the one that receives the changes). The agreement contains all the information needed for making a connection from the supplier to the consumer and scheduling replication.

replication context
The replication context identifies the root of a replicated subtree. The configuration information that is related to replication is maintained in a set of entries created below a replication context.

replication site
A Gateway server and any master, peer, or replica servers that are configured to replicate together.

role
A job function that identifies the tasks that a user can do and the resources to which a user has access. A user can be assigned one or more roles.

```
or
```

Defines what access levels a specified user has and the specific resources they can modify at those levels. The user might be limited in how they can access information if they do not have the proper role. Multiple roles are permissible.

RSA encryption
A system for public-key cryptography used for encryption and authentication. It was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. The security of the system depends on the difficulty of factoring the product of two large prime numbers.

SCIM
The System for Cross-Domain Identity Management (SCIM) is a standard that defines schema and protocol for identity management.

Secure Sockets Layer (SSL)
A security protocol that provides communication privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering, and message forgery. SSL was developed by Netscape Communications Corp. and RSA Data Security, Inc.

SMS (System Managed Space)
A table space where the operating system’s file System Manager allocates and manages the space where the table is stored.

sorted search
Search that allows a client to receive search results sorted based on a list of criteria, where each criteria represents a sort key. This moves the responsibility of sorting from the client application to the server, where it might be done more efficiently.

subtree
A section of a directory hierarchy, which is also called a directory tree. The subtree typically starts at a particular directory and includes all subdirectories and objects below that directory in the directory hierarchy; that is, any subdirectories or objects connected to the directory or to any lower level of its subdirectories.

suffix
A distinguished name (DN) that identifies the top entry in a locally held directory hierarchy. Because of the relative naming scheme that is used in Lightweight Directory Access Protocol (LDAP), this suffix applies to every other entry within that directory hierarchy. A Directory Server can have multiple suffixes, each identifying a locally held directory hierarchy. A suffix is also known as a naming context.

supplier server
A server that sends changes to a consumer server.

syntax
Syntax refers to the required format for the values of an attribute. Supported syntaxes are:

```
IBM Attribute Type Description
     Matching Rule Description
     Name Form Description
     Attribute Type Description
     Object Class Description
     DIT Structure Rule Description
     DIT Content Rule Description
     LDAP Syntax Description
     OID
     Matching Rule Use Description
     Boolean - TRUE/FALSE
     Binary - octet string
     INTEGER - integral number
     Generalized Time
     IA5 String - case-sensitive string
     Directory String - case-insensitive
                        string
     UTC time
     Telephone Number
     DN - distinguished name
```

Transport Layer Security (TLS)
An Internet Engineering Task Force (IETF)-defined security protocol that is based on Secure Sockets Layer (SSL) and is specified in RFC 2246.

VLV (Virtual List View)
A GUI technique that can be employed where ordered lists that contain many entries need to be displayed. VLV provides a scrollable view of large sorted data set through a window that contains few visible entries.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection, and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated, or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Accessibility

Accessibility features help users with a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

For more information, see "Accessibility features for IBM Security Directory Suite" in the IBM Knowledge Center.

Copyright statement

Note: This edition applies to version 8.0.1.x of *IBM Security Directory Suite* (product number 5725-Y17) and to all subsequent releases and modifications until otherwise indicated in new editions.

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBMproducts. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Each copy or any portion of these sample programs or any derivative work must include a copyright notice as follows:
© (your company name) (year).
Portions of this code are derived from IBM Corp. Sample Programs.
© Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

Index