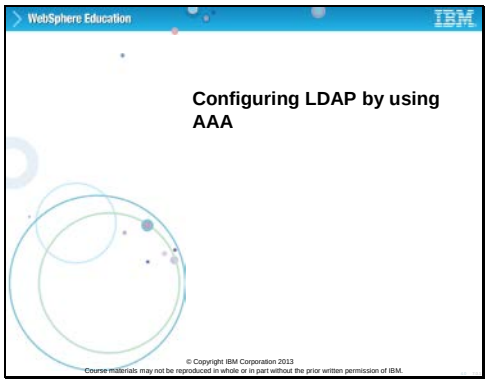
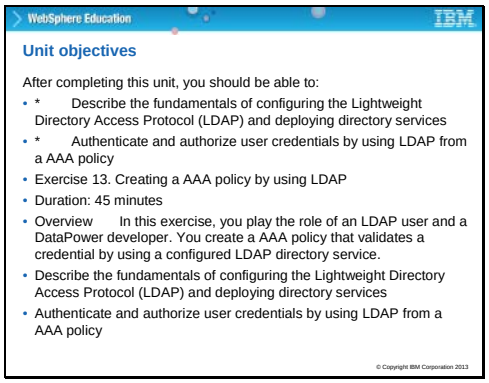
Slide 1

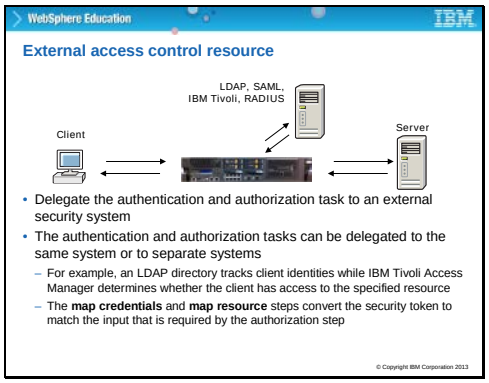

WebSphere Education
IBM
Configuring LDAP by using AAA
© Copyright IBM Corporation 2013
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Slide 2



This presentation briefly covers some LDAP concepts before examining the details of configuring a AAA policy that connects to LDAP. Students learn how to authenticate and authorize clients by using LDAP.

Slide 3



External access control resource

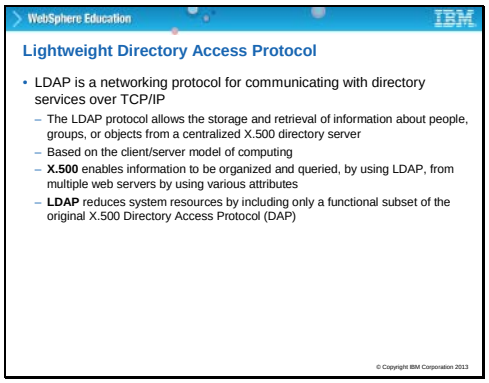
DataPowers external access control allows for the delegation of the authentication and authorization task to an external security system.

The authentication and authorization tasks can be delegated to the same system or to separate systems.

For example, an LDAP directory tracks client identities while IBM Tivoli Access Manager determines whether the client has access to the specified resource.

The map credentials and map resource steps can convert the security token to match the input that is required by the authorization step.

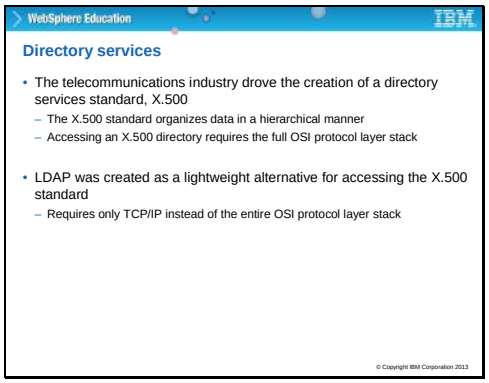
Slide 4



Lightweight Directory Access Protocol

Lightweight Directory Access Protocol, or LDAP as it is commonly known, is a networking protocol for communicating with directory services over TCP/IP. The LDAP protocol allows the storage and retrieval of data on people, groups, or objects from a centralized X.500 directory server. It is based on the client/server model of computing. X.500 enables information to be organized and queried, by using LDAP, from multiple web servers by using various attributes. LDAP reduces system resources by including only a functional subset of the original X.500 Directory Access Protocol (DAP).

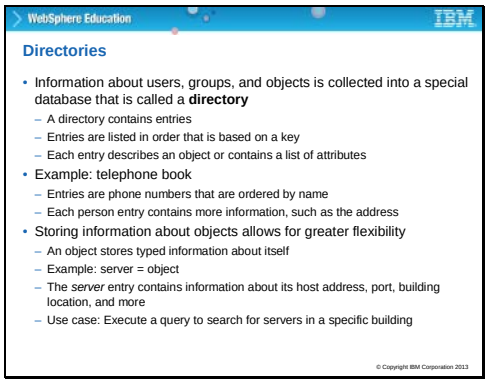
Slide 5



Directory services

The telecommunications industry in the early 1980s drove the creation of a directory services standard, X.500. The X.500 standard organized data in a hierarchical manner, but accessing an X.500 directory required the full OSI protocol layer stack, and was unwieldy. After OSI fell out of favor, LDAP was created as a lightweight alternative for accessing the X.500 standard, but it was designed to use TCP/IP instead of the entire OSI protocol layer stack.

Slide 6



Directories

Information about users, groups, and objects is collected into a special database that is called a directory that contains entries that are listed in order that is based on a key. Each entry describes an object or contains a list of attributes. An example of a typical directory might be a telephone book, in which entries are peoples phone numbers that are ordered by name. Each person contains more information; such as the address, occupation, alternative number, and spouse name. Storing extra information about objects allows for greater flexibility.

An object can store typed information about itself, such as a directory of computer hardware assets might include lists of servers that are owned by a company. In this context, a server is an object and might also contain information about its host address, port, building location, and more. So a typical use case of the directory might be to run a query to search for servers in a specific building.

Slide 7

WebSphere Education

Common LDAP attributes

Attribute, alias	Attribute syntax	Description	Example
commonName, cn	cis	Common name of an entry	John
surname, sn	cis	Surname (family name) of a person	Smith
TelephoneNumber	tel	Telephone number	555-555-1111
organizationalUnitName, ou	cis	Name of organizational unit	WebSphere
owner	dn	DN of person who owns the entry	cn=John Smith, o=IBM,c=ca
organization, o	cis	Name of organization	IBM
jpegPhoto	bin	Photographic image in JPEG format	Photograph of John Smith

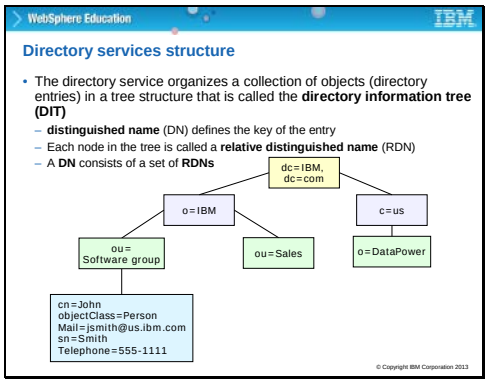
Common LDAP attributes

LDAP classifies data by “attributes” which are standard types of data that is typically stored in an LDAP directory. Attributes have a long name and an abbreviation, typically 1 or 2 characters. For example, the attribute called “organization” can be abbreviated as “o”.

Attributes also have a “syntax” which defines how the data is stored. “cis” stands for “case ignored string” meaning that capitalization is ignored. So in the first example, the name “John” would match regardless of whether it is all uppercase, all lowercase, or mixed case.

Other syntax types include “tel” for a telephone number, and “bin” for binary data, such as a JPEG image or MP3 file. A special syntax of “dn” denotes a “distinguished name”, which is a unique key. A “dn” might be a single attribute, or a collection of attributes.

Slide 8



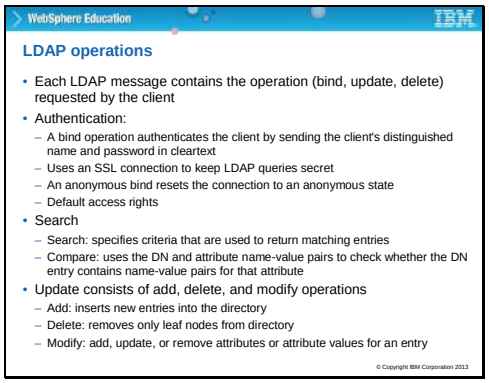
Directory services structure

The directory service organizes a collection of objects (directory entries) in a tree structure that is called the directory information tree (DIT) in which entries keyed by their distinguished name (DN).

Each node in the tree is called a relative distinguished name (RDN), and a DN consists of a set of RDNs.

LDAP follows a hierarchical structure in the way data is inter-related. By following down the directory information tree, you can arrive at a unique data item, which is identified by its distinguished name.

Slide 9



LDAP operations

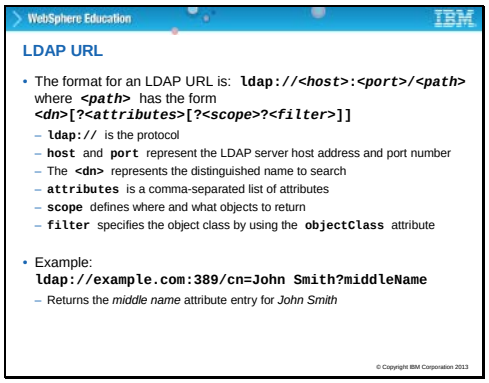
Each LDAP message contains the operation code (either bind or update) as requested by the client. [note typographical error in line 1 – “delete” should not be there]

Each operation is authenticated. A bind operation authenticates the client by sending the clients distinguished name and password in cleartext, which is why LDAP normally uses an SSL connection to keep LDAP queries secret. You can also request an anonymous bind that allows for default access rights, usually a limited subset of the data.

Search parameters specify criteria that are used to return matching entries, and Compare parameters use the DN and attribute name-value pairs to check whether the DN entry contains that attributes name-value pairs.

An update operation allows you to add, delete, and modify entries in the directory. The delete operation removes only leaf nodes from directory – you cannot delete a whole branch at once. The modify operation allows you to add, update, or remove attributes or attribute values for an entry.

Slide 10



LDAP URL

The format for an LDAP URL is: `ldap://<host>:<port>/<path>`, where `<path>` has the form `<dn>[?<attributes>[?<scope>?<filter>]]`

`ldap://` is the protocol.

Host and port represent the LDAP server host address and port number

The `<dn>` represents the distinguished name to search

Attributes is a comma-separated list of attributes

Scope defines where and what objects to return

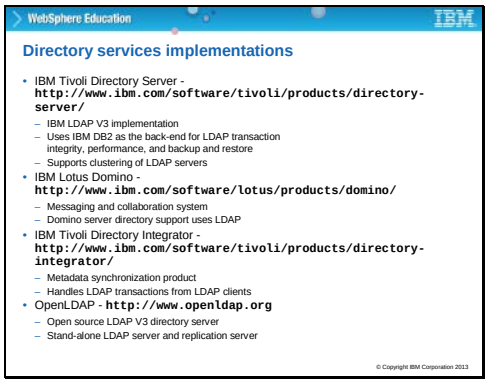
Filter specifies the object class by using the objectClass attribute

Example: `ldap://example.com:389/cn=John Smith?middleName`

Returns the middle name attribute entry for John Smith

(This example is incorrect: you might not actually have a space between the given name and the surname as in this example.)

Slide 11



Directory services implementations

There are many implementations of LDAP, for example:

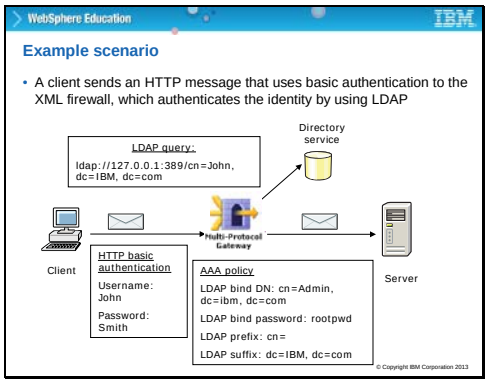
IBM Tivoli Directory Service is an LDAP V3 implementation that uses IBM DB2 as the back-end for LDAP transactions, providing integrity, performance, and backup and restore. It also supports the clustering of LDAP servers.

IBM Lotus Domino is a messaging and collaboration system provides directory support by using LDAP.

IBM Tivoli Directory Integrator is a metadata synchronization product that handles LDAP transactions from LDAP clients and mediates multiple LDAP servers.

If you want to experiment with LDAP yourself, there is always the free OpenLDAP product, which is an open source LDAP V3 directory server that includes a stand-alone LDAP server and replication server. LDAP does not define how the data is stored and retrieved – just the interface and structure.

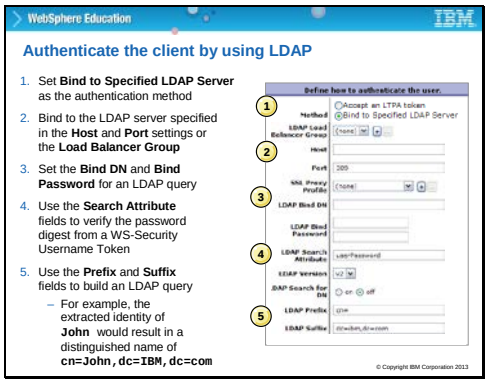
Slide 12



Example scenario

Here, is shown how an incoming message has a plain-text name and password must be authenticated. The connection to the LDAP server includes some credentials that allow access LDAP, shown here as “cn=admin” with a password of “rootpwd”. When gained access to LDAP is earned, then send the user name and password that are being sought to authenticate, along with the appropriate prefix and suffix. The term “dc” in this context means “domain component”.

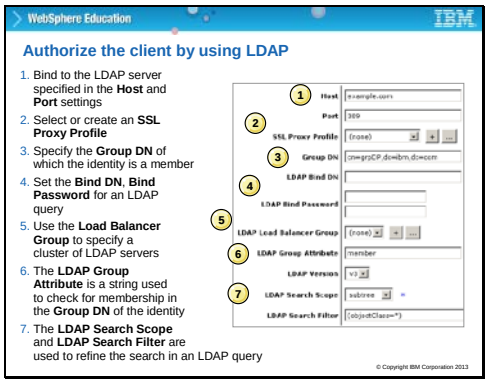
Slide 13



Authenticate the client by using LDAP

Here is how to configure the AAA action to authenticate by using LDAP.
Set “Bind to Specified LDAP Server” as the authentication method. The remainder of the screen changes to show LDAP parameters, including the LDAP server Host and Port settings. LDAP servers can also be configured as a Load Balancer Group.
Set the Bind DN and Bind Password for an LDAP query, and use the Search Attribute fields to verify the password digest from a WS-Security Username Token. Then, supply the Prefix and Suffix fields that DataPower uses to build an LDAP query. For example, the extracted identity of John would result in a distinguished name of `cn=John,dc=IBM,dc=com` in this example.

Slide 14



Authorize the client by using LDAP

In this example, the screen capture is showing how to check the user's authority by looking at group membership.

Bind to the LDAP server specified in the Host and Port settings, including selecting or creating an SSL proxy profile.

Specify the Group DN of which the identity is a member, and set the Bind DN, Bind Password for an LDAP query.

Use the Load Balancer Group to specify a cluster of LDAP servers.

The LDAP Group Attribute is a string that is used to check for membership in the Group DN of the identity.

The LDAP Search Scope and LDAP Search Filter are used to refine the search in an LDAP query.

Slide 15

WebSphere Education

Unit summary

Having completed this unit, you should be able to:

- * Describe the fundamentals of configuring the Lightweight Directory Access Protocol (LDAP) and deploying directory services
- * Authenticate and authorize user credentials by using LDAP from a AAA policy
- Exercise 13. Creating a AAA policy by using LDAP
- Duration: 45 minutes
- Overview In this exercise, you play the role of an LDAP user and a DataPower developer. You create a AAA policy that validates a credential by using a configured LDAP directory service.
- Describe the fundamentals of configuring the Lightweight Directory Access Protocol (LDAP) and deploying directory services
- Authenticate and authorize user credentials by using LDAP from a AAA policy

Slide 16

Checkpoint questions

1. True or False: In LDAP, a collection of objects is organized in a directory structure.
2. True or False: In the AAA policy, the LDAP bind DN and LDAP bind password are configured.
3. True or False: LDAP is a choice for only the authentication step in a AAA policy.

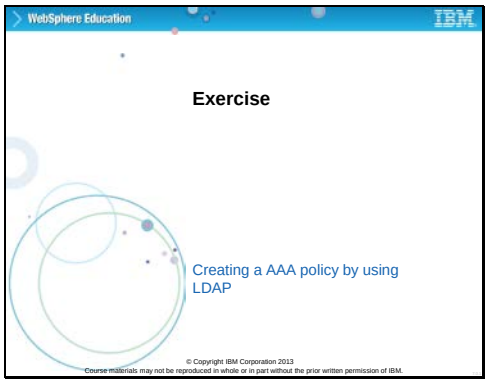
Slide 17

WebSphere Education

Checkpoint answers

1. True. With LDAP, a collection of objects is organized in a directory structure.
2. True. In the AAA policy, the LDAP bind DN and LDAP bind password are configured.
3. False. LDAP is a choice for both the authentication step and the authorization step in a AAA policy.

Slide 18


WebSphere Education
IBM
Exercise
Creating a AAA policy by using LDAP
© Copyright IBM Corporation 2013
Course materials may not be reproduced in whole or in part without the prior written permission of IBM.

Slide 19

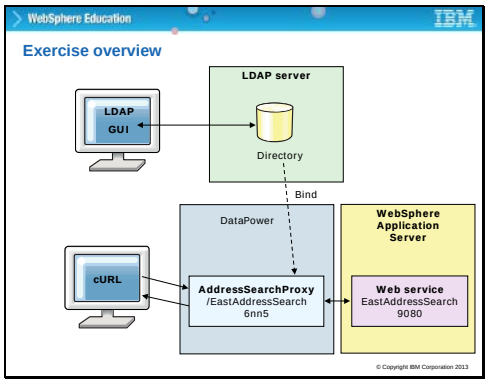
WebSphere Education

Exercise objectives

After completing this exercise, you should be able to:

- Add entries to the IBM Tivoli Directory Server LDAP server
- Authenticate and authorize users on an LDAP server by configuring a AAA policy

Slide 20


WebSphere Education
IBM
Exercise overview
LDAP server
LDAP GUI
Directory
Bind
DataPower
WebSphere Application Server
cURL
AddressSearchProxy
/EastAddressSearch
6nn5
Web service
EastAddressSearch
9080
© Copyright IBM Corporation 2013