CHAPTER 18

Using LDAP

This chapter provides information about using Lightweight Directory Access Protocol (LDAP) with Cisco Access Registrar to access information directories. You can use Cisco AR to authenticate and authorize access requests by querying user information through LDAP.

Note Cisco AR 4.1 requires an LDAP Version 2 directory server for any remote server used for LDAP.

Revised: April 6, 2008, OL-8558-04

Configuring LDAP

To use LDAP in Cisco AR, use **aregcmd** to do the following:

1. Configure an LDAP Service.
2. Configure an LDAP RemoteServer object.
3. Set LDAP service as the default AA service.
4. Save your configuration.

After you issue the **save** command, Cisco AR attempts to validate the configuration, checks for all required properties, and ensures there is no logic error. If the validation is successful, Cisco AR saves the configuration to the MCD database. When Cisco AR is reloaded, it shuts down any current LDAP connections and builds new connections for the configured LDAP remote servers.

Configuring the LDAP Service

You configure an LDAP service under **/Radius/Services**. When you define an LDAP service under **/Radius/Services**, you must set its type to LDAP.

```
[ //localhost/Radius/Services/AR-LDAP ]
    Name = AR-LDAP
    Description =
    Type = ldap
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    MultipleServersPolicy = Failover
    RemoteServers/
```

Table 18-1 describes the LDAP service properties.

Table 18-1 LDAP Service Properties

Parameter	Description
Name	Required; inherited from the upper directory
Description	An optional description of the service
Type	Must be set to LDAP for LDAP service
IncomingScript	Optional
OutgoingScript	Optional
OutagePolicy	Required; must be set to AcceptAll or Drop Packet, or defaults to RejectAll
OutageScript	Optional
MultipleServersPolicy	Required; must be set to RoundRobin or defaults to Failover.
RemoteServers	Required; list of one or more remote servers defined under **/Radius/Services/LDAP/RemoteServers**. These servers must be listed in order under **/Radius/RemoteServers.**

MultipleServersPolicy

Use the MultipleServersPolicy property to configure the LDAP remote servers in RoundRobin mode, or the default Failover mode applies. When set to Failover, Cisco AR directs requests to the first server in the **/Radius/Services/LDAP/RemoteServers** list. If that server should fail or go offline, Cisco AR redirects all requests to the next server in the list. The process continues until Cisco AR locates an on-line server.

When set to RoundRobin, Cisco AR directs each request to the next server in the RemoteServers list to share the resource load across all listed servers.

RemoteServers

Use the RemoteServers directory to list one or more remote servers to process access requests. The servers must also be listed in order under **/Radius/RemoteServers.**

The order of the RemoteServers list determines the sequence for directing access requests when MultipleServersPolicy is set to RoundRobin mode. The first server in the list receives all access requests when MultipleServersPolicy is set to Failover mode.

Configuring an LDAP RemoteServer

Use the **aregcmd** command **add** to add LDAP servers under **/Radius/RemoteServers**. You must configure an LDAP RemoteServer object for each RemoteServer object you list under **/Radius/Services/LDAP/RemoteServers**.

The following properties must be configured to use an LDAP remote server:

- Name
- Protocol
- Port

- HostName
- BindName
- BindPassword
- SearchPath

Table 18-2 describes the LDAP Remote Server properties.

Table 18-2 LDAP Remote Server Properties

Parameter	Description
Name	Required name you assign
Description	Optional description of the server
Protocol	Required and must be set to LDAP; no default value
Port	Required; port on which LDAP server listens, default is port 389. **Note** If port is not set or set to zero, LDAP remote server will automatically be set to port 389.
ReactivateTimerInterval	Required; default is 300000 (ms)
Timeout	Required; specifies length of time Cisco AR waits for a response from the LDAP server before noting the server as down; default is 15 (seconds)
HostName	Required; specifies the hostname, FQDN, or IP address of the LDAP server
BindName	Specifies the distinguished name (DN) in the LDAP server for Cisco AR to bind with the LDAP server
BindPassword	Specifies the password for the distinguished name
UseSSL	FALSE by default
SearchPath~	Specifies search base to the organization and domain; for example: o=cisco.com
Filter~	(uid=%s) by default
UserPasswordAttribute	Should be set to the attribute in the directory server which stores users' passwords; default is *userpassword*
LimitOutstandingRequests	FALSE by default
MaxOutstandingRequests	Limits the number of requests to the LDAP server; used to throttle the request load when the LDAP server does not function well under high TPS rates (default is 0)
MaxReferrals	Limits the number of referrals Cisco AR allows when working with LDAPv2 (default is 0)
ReferralAttribute	LDAP attribute that contains a referral for LDAPv2
ReferralFilter	Filter used when following a referral for LDAPv2

Table 18-2 LDAP Remote Server Properties (continued)

Parameter	Description
PasswordEncryptionStyle	Dynamic by default; must be set to one of the following depending on the algorithm used by the LDAP server to encrypt passwords: Dynamic Crypt None SHA-1 SSHA-1 When set to *Dynamic*, Cisco AR analyzes the password and detects the encryption algorithm used. *None* indicates that the LDAP server stores clear text passwords. **Note** If CHAP authentication is used with LDAP backing store, passwords in LDAP must be stored as clear text.
EscapeSpecialCharInUserName	FALSE by default
DNSLookupAndLDAPRebindInterval	Specifies the timeout period after which the Cisco AR server will attempt to resolve the LDAP hostname to IP address (DNS resolution); 0 by default
DataSourceConnections	Specifies the number of concurrent connections to the LDAP server. The default value is 8.
SearchScope	Specifies how deep to search within a search path; default is *SubTree* which indicates a search of the base object and the entire subtree of which the base object distinguished name is the highest object. *Base* indicates a search of the base object only. *OneLevel* indicates a search of objects immediately subordinate to the base object, but does not include the base object.
LDAPToRadiusMappings	Optional; a list of name/value pairs in which the name is the name of the **ldap** attribute to retrieve from the user record, and the value is the name of the RADIUS attribute to set to the value of the **ldap** attribute retrieved. For example, when the **LDAPToRadiusMappings** has the entry: **FramedIPAddress = Framed-IP-Address**, the RemoteServer retrieves the **FramedIPAddress** attribute from the **ldap** user entry for the specified user, uses the value returned, and sets the Response variable **Framed-IP-Address** to that value.

Table 18-2 LDAP Remote Server Properties (continued)

Parameter	Description
LDAPToEnvironmentMappings	Optional; a list of name/value pairs in which the name is the name of the **ldap** attribute to retrieve from the user record, and the value is the name of the Environment variable to set to the value of the **ldap** attribute retrieved. For example, when the **LDAPToEnvironmentMappings** has the entry: **group = User-Group**, the RemoteServer retrieves the **group** attribute from the **ldap** user entry for the specified user, uses the value returned, and sets the Environment variable **User-Group** to that value.
LDAPToCheckItemMappings	Optional; list of LDAP *attribute/value* pairs which must be present in the RADIUS access request and must match, both name and value, for the check to pass.

DNS Look Up and LDAP Rebind Interval

Cisco AR provides a DNS Look-up and LDAP Rebind feature that enables you to use a smart DNS server for LDAP hostname resolution, allows you to query a DNS server at set intervals to resolve the LDAP hostname, and optionally rebind to the LDAP server, if necessary.

When you configure Cisco AR to use an LDAP directory server, you can specify the hostname of the LDAP directory server. The hostname can be a qualified or an unqualified name. You can also specify a timeout period after which Cisco AR will again resolve the hostname. If the IP address returned is different from the previous, Cisco AR establishes a new LDAP bind connection.

The DNSLookupAndLDAPRebindInterval property specifies the timeout period after which the Cisco AR server will attempt to resolve the LDAP hostname to IP address (DNS resolution). When you do not modify DNSLookupAndLDAPRebindInterval, the default value zero indicates the server will perform normal connection and binding only at start-up time or during a reload. Unless you change the default to a value greater than zero, the server will not perform periodic DNS lookups.

Cisco AR maintains and uses the existing bind connection until a new one is established to minimize any performance impact during the transfer. Cisco AR ensures that no requests are dropped or lost during the transfer to a new LDAP binding.

Set the DNSLookupAndLDAPRebindInterval using a numerical value and the letter H for hours or M for minutes, such as in the following examples:

set DNSLookupAndLDAPRebindInterval 15M—performs DNS resolution every 15 minutes

Note We recommend that you do not set DNSLookupAndLDAPRebindInterval to a value less than 15 minutes to minimize its effect on server performance.

set DNSLookupAndLDAPRebindInterval 1h—performs DNS resolution every hour

The following shows an example configuration for the DNS Look-up and LDAP Rebind feature.

Step 1 Login to the Cisco AR server, and use **aregcmd** to navigate to **//localhost/Radius/Remoteservers**. If necessary, add the LDAP server, or change directory to it.

cd /Radius/RemoteServers/ldap-serv1/

Step 2 Set the DNSLookupAndLDAPRebindInterval property to the interval time desired.

set DNSLookupAndLDAPRebindInterval 30 M

LDAP Rebind Failures

Cisco AR records any name resolution failures, bind successes and failures, and the destination hostname and IP address in the log file. At trace level 3, Cisco AR also logs the time of any new bind connections and the closing of any old bind connections.

If either the name resolution or bind attempt fail, Cisco AR continues using the existing bind connection until the timeout has expired again. If there is no existing bind connection, Cisco AR marks the remote server object as *down*.

LDAPToRadiusMappings

Configure LDAPToRadiusMappings with a list of *name/value* pairs where name is the name of the data store attribute to retrieve from the user record and the value is the name of the RADIUS attribute to set to the value of the data store attribute retrieved.

Values stored in a multi-valued field in the LDAP directory are mapped to multiple RADIUS attributes, For example, if the LDAPToRadiusMappings has the following entry:

```
tunnel-info = Cisco-AVPair
```

The following LDAP fields in the user's record will create four Cisco-AVPair attributes in the user's Access-Accept RADIUS packet:

```
tunnel-info: vpdn:tunnel-id=ssg001
tunnel-info: vpdn:tunnel-type=12tp
tunnel-info: vpdn:ip-addresses=10.2.2.2
tunnel-info: vpdn:12tp-tunnel-password=secret
```

LDAPToEnvironmentMappings

LDAPToEnvironmentMappings comprises a list of attribute name/value pairs or AV pairs where the name is the name of the data store attribute to retrieve from the user record, and the value is the name of the Environment variable to set to the value of the LDAP attribute retrieved.

For example, when the LDAPToEnvironmentMappings has the entry: group =User-Group, the RemoteServer retrieves the attribute from the LDAP user entry for the specified user, uses the value returned, and sets the Environment variable User-Group to that value.

LDAPToCheckItemMappings

LDAPToCheckItemMappings comprises a list of LDAP AV pairs which must be present in the RADIUS access request and must match, both name and value, for the check to pass. Cisco AR will first authenticate the user's password in the Access-Request before validating the check item attributes.

Setting LDAP As Authentication and Authorization Service

Use **aregcmd** to configure the LDAP Service as the default authentication and authorization service under **/Radius** as in the following:

set DefaultAuthenticationService ***AR-LDAP***

set DefaultAuthorizationService ***AR-LDAP***

Saving Your Configuration

When you use **aregcmd** to **save** your configuration, Cisco AR does the following:

- Attempts to validate the configuration
- Checks for all required parameters
- Ensures there are no logic errors

If the validation is successful, Cisco AR saves the configuration to the MCD database. When you **reload**, Cisco AR shuts down any current LDAP connections and builds new connections for the configured LDAP servers.

CHAP Interoperability with LDAP

If the you plan to use CHAP authentication with an LDAP backing store, the password in LDAP must be stored as clear text. This is due to the one-way hash used by the CHAP, crypt, SHA-1, and SSHA encryption algorithms.

Allowing Special Characters in LDAP Usernames

This feature allows you to use special characters in LDAP usernames. The allowable special characters are *, (,), and \. These special characters can be included in the string passed to LDAP as the LDAP username value (usually the RADIUS username attribute).

The default of EscapeSpecialCharInUserName is FALSE. To enable this feature, use **aregcmd** to set the EscapeSpecialCharInUserName attribute in **/Radius/RemoteServers/ldap-server** to TRUE, as shown in the following example.

cd /Radius/RemoteServers/ldap-server

set EscapeSpecialCharInUserName TRUE

```
/Radius/RemoteServers/Ldap-Server
EscapeSpecialCharinUserName = TRUE
```

Note This feature supports the LDAP V3 library.

Dynamic LDAP Search Base

A new environment variable, Dynamic-Search-Path (see **rex.h**), can be used to set the dynamic LDAP search base. If this environment variable is defined for an LDAP service, it will override the default LDAP search base defined in the LDAP Remote Server configuration. This allows the LDAP search base to be configured on a per-user basis.

For example, you could match the search base to the organization and domain (in a Tcl script called from **/Radius/IncomingScript**):

```
set user [ $request get User-Name ]
if { [ regexp {^[^@]+@([^\.]+)\.(.+)$} $user m org domain ] } {
$environ put Dynamic-Search-Path "ou=$org,ou=people,o=$domain"
```

Analyzing LDAP Trace Logs

Cisco AR records in the log files any name resolution failures, bind successes and failures, and the destination hostname and IP address. At trace level 3, Cisco AR logs the time of any new bind connections and the closure of any old bind connections and also information about user login requests and reply messages.

Successful Bind Message

The following message is logged in the **name_radius_1_trace** file, when the Cisco AR server successfully binds to the LDAP server. In this case, spatula-u5 is the LDAP server listening on port number 389.

```
04/23/2003 11:02:57: Log: Successfully bind to LDAP Server ldapserver (spatula-u5:389)
```

Bind Failure Messages

The following messages are logged in the **name_radius_1_trace** file, when AR server fails to bind to the LDAP server.

```
04/23/2003 11:10:50: Log: Write in LDAPClient returned an error (32)

04/23/2003 11:10:50: Log: Remote LDAP Server ldapserver (spatula-u5:387): Unable to
bind to LDAP Server: Can't contact LDAP server

04/23/2003 11:10:50: Log: Remote LDAP Server ldapserver (spatula-u5:387): Failed to
open the connection to the LDAP server
```

Messages like those above could indicate that the hostname specified does not resolve to the correct IP address of the LDAP server or the configured port number might not be the port on which the LDAP server listens.

The following messages are logged in the **name_radius_1_trace** file, when AR server fails to bind to the LDAP server.

```
04/23/2003 11:45:14: Log: Remote LDAP Server ldapserver (spatula-u5:389): Unable to
bind to LDAP Server: No such object ()
```

```
04/23/2003 11:45:14: Log: Remote LDAP Server ldapserver (spatula-u5:389): Failed to
open the connection to the LDAP server
```

The Distinguished Name (DN) provided in the BindName property was invalid. The DN provided in the BindName property should contain the exact string used in the directory server to define the object.

The following messages are logged in the **name_radius_1_trace** file, when AR server fails to bind to the LDAP server.

```
04/23/2003 11:51:55: Log: Remote LDAP Server ldapserver (spatula-u5:389): Unable to
bind to LDAP Server: Invalid credentials
04/23/2003 11:51:55: Log: Remote LDAP Server ldapserver (spatula-u5:389): Failed to
open the connection to the LDAP server
```

The messages above indicate that the password provided in the BindPassword property was incorrect.

Login Failure Messages

The following messages are logged in the **name_radius_1_trace** file, when user ***jane*** tries to login. These messages indicate that user *jane* does not have a record in the directory server or the SearchPath property has an incorrect value. The SearchPath property should have the directory where the user record is stored in the directory server.

Notice how the messages specify the service, remote LDAP server, user name, and contents of the Access-Reject packet.

```
04/23/2003 11:24:17: P8457: Authenticating and Authorizing with Service AR-LDAP
04/23/2003 11:24:17: id = 5
04/23/2003 11:24:17: P8457: Remote LDAP Server ldapserver (spatula-u5: 389): Querying
LDAP server, id = 5.
04/23/2003 11:24:17: P8457: Remote LDAP Server ldapserver (spatula-u5: 389): GotLDAP
response, id = 5.
04/23/2003 11:24:17: P8457: Remote LDAP Server ldapserver (spatula-u5: 389): No
matching entries returned from LDAP query.
04/23/2003 11:24:17: P8457: User jane was not found in the LDAP store
04/23/2003 11:24:17: P8457: Rejecting request
04/23/2003 11:24:17: P8457: Rejecting request
04/23/2003 11:24:17: P8457: Trace of Access-Reject packet
04/23/2003 11:24:17: P8457: identifier = 4
04/23/2003 11:24:17: P8457: length = 35
04/23/2003 11:24:17: P8457: reqauth = 01:ad:cf:c7:4f:8e:a4:38:b0:d8:0a:e5:3d:9f:64:16
04/23/2003 11:24:17: P8457: Reply-Message = Access Denied
```

The following messages are logged in the **name_radius_1_trace** file, when user ***bob*** tries to login. These messages indicate that user *bob* tried to login with an incorrect password.

```
04/23/2003 11:36:59: P8461: Authenticating and Authorizing with Service AR-LDAP
04/23/2003 11:36:59: id = 7
04/23/2003 11:36:59: P8461: Remote LDAP Server ldapserver (spatula-u5: 389): Querying
LDAP server, id = 7.
04/23/2003 11:36:59: P8461: Remote LDAP Server ldapserver (spatula-u5: 389): Got LDAP
response, id = 7.
04/23/2003 11:36:59: P8461: Remote Server ldapserver (spatula-u5:389): User bob's
password does not match
04/23/2003 11:36:59: P8461: User bob's password does not match
04/23/2003 11:36:59: P8461: Rejecting request
04/23/2003 11:36:59: P8461: Rejecting request
04/23/2003 11:36:59: P8461: Trace of Access-Reject packet
04/23/2003 11:36:59: P8461: identifier = 6
04/23/2003 11:36:59: P8461: length = 35
04/23/2003 11:36:59: P8461: reqauth = de:8d:4b:c4:f9:c0:06:a6:98:2d:8c:e9:f3:a9:a3:c2
```

```
04/23/2003 11:36:59: P8461: Reply-Message = Access Denied
```

The following messages are logged in the **name_radius_1_trace** file, when user ***bob*** tries to login. These messages indicate the user record for user *bob* does not contain an attribute called pass. The UserPasswordAttribute property has an incorrect value called *pass*. The UserPasswordAttribute property should have the attribute name in the directory records where the user password is stored.

```
04/23/2003 12:02:09: P9865: Authenticating and Authorizing with Service AR-LDAP
04/23/2003 12:02:09: id = 2
04/23/2003 12:02:09: P9865: Remote LDAP Server ldapserver (spatula-u5: 389): Querying
LDAP server, id = 2.
04/23/2003 12:02:09: P9865: Remote LDAP Server ldapserver (spatula-u5: 389): Got LDAP
response, id = 2.
04/23/2003 12:02:09: P9865: Remote LDAP Server ldapserver (spatula-u5: 389): LDAP
entry for user bob did not have a password (" pass") attribute
04/23/2003 12:02:09: P9865: User bob's password does not match
04/23/2003 12:02:09: P9865: Rejecting request
04/23/2003 12:02:09: P9865: Rejecting request
04/23/2003 12:02:09: P9865: Trace of Access-Reject packet
04/23/2003 12:02:09: P9865: identifier = 10
04/23/2003 12:02:09: P9865: length = 35
04/23/2003 12:02:09: P9865: reqauth = 0d:b6:83:f9:e8:3d:a4:ad:f1:c9:33:72:91:0b:29:1c
04/23/2003 12:02:09: P9865: Reply-Message = Access Denied
```

Note Remember to **reload** the Cisco AR server after any changes to the LDAP server configuration.