Lightweight Directory Access Protocol

User's Guide for IBM @server BladeCenter Management Module and IBM Remote Supervisor Adapters

Lightweight Directory Access Protocol

User's Guide for IBM @server BladeCenter Management Module and IBM Remote Supervisor Adapters

Note: Before using this information and the product it supports, read the general information in Appendix B, “Notices,” on page 31.

First Edition (April 2004)

Contents

Configuring an LDAP client and LDAP server

This document provides information about how to configure the Lightweight Directory Authentication Protocol (LDAP) client and an LDAP server to support remote authentication for the IBM® Remote Supervisor Adapter, IBM Remote Supervisor Adapter II, and the IBM @server BladeCenter™ Management Module.

Information about configuring the following two LDAP servers is provided:

- Novell eDirectory version 8.7.1
- Microsoft® Windows® Server 2003 Active Directory

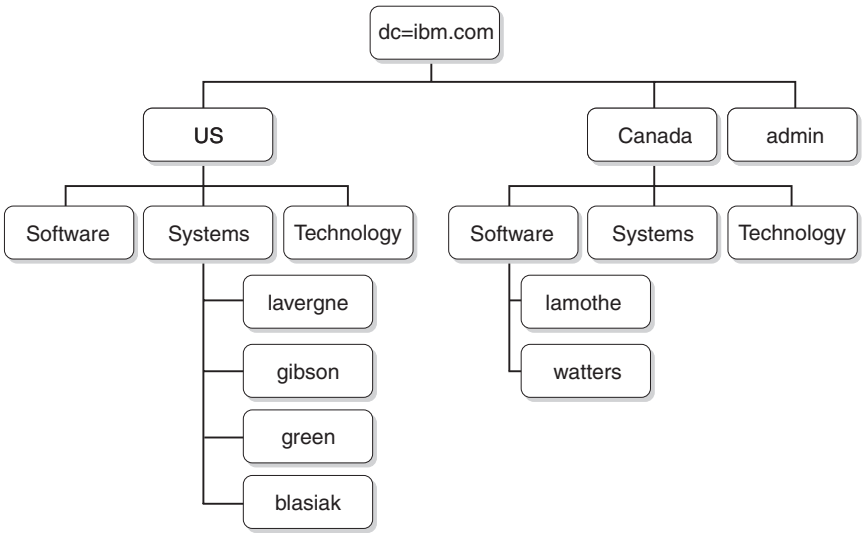
Note: Throughout this document, the term Remote Supervisor Adapter II is used interchangeably with Remote Supervisor Adapter and BladeCenter management module, unless otherwise noted.

User schema example

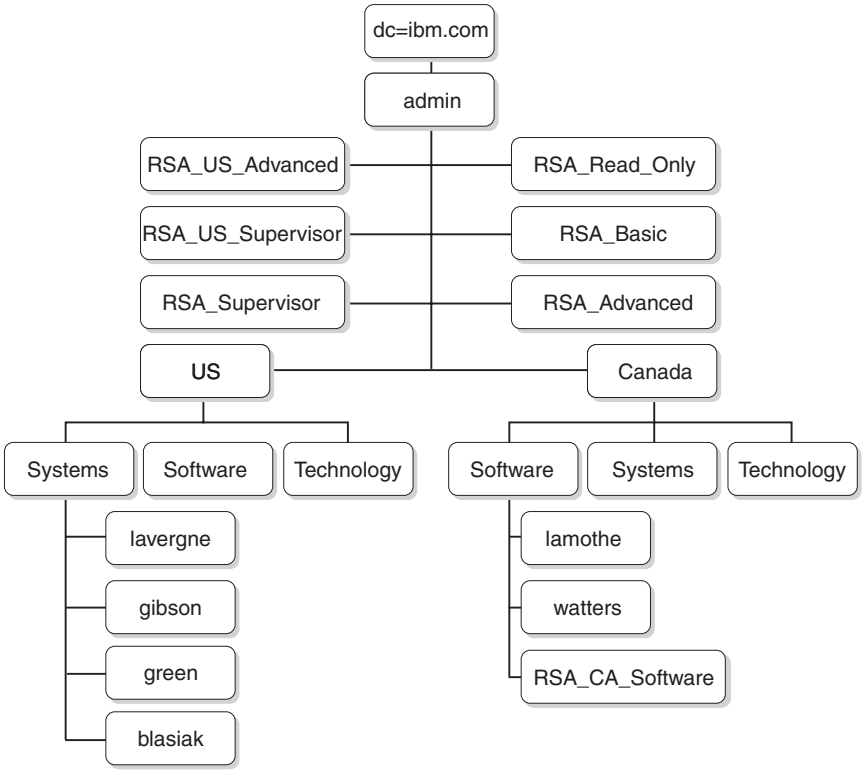
A simple user schema example is described in this section. This schema example is used throughout the document to illustrate the configuration on both the LDAP client and the LDAP server.

The user schema example is rooted at a domain component called ibm.com. That is, every object in this tree has a root distinguished name equal to dc=ibm,dc=com. Now assume that this tree represents a company that wants to classify users and user groups based on their country and organization. The hierarchy is root → country → organization → people.

The following illustration shows a simplified view of the schema used in this document. Note the use of a user account (userid=admin) directly below the root. This is the administrator.



The following illustration shows the addition of user groups. Six user groups are defined and added to the first level, and another user group is added to the Software organization in the country Canada.



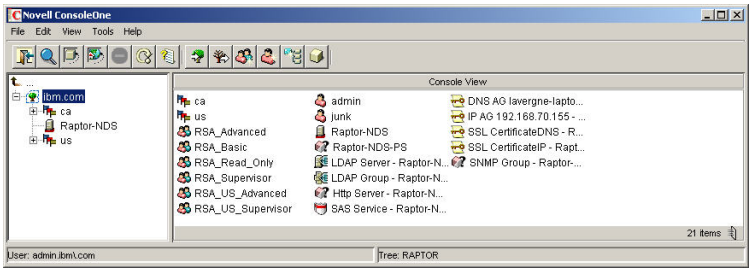
The users and associated user groups in Table 1 are used to complete the schema.

Table 1. User to Group mapping

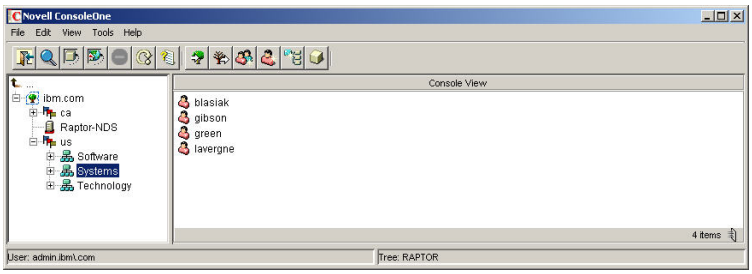
User distinguished name	Group membership
cn=lavergne, o=Systems, c=us, dc=ibm.com	cn=RSA_Supervisor, dc=ibm.com cn=RSA_US_Supervisor, dc=ibm.com
cn=blasiak, o=Systems, c=us, dc=ibm.com	cn=RSA_US_Advanced, dc=ibm.com
cn=gibson, o=Systems, c=us, dc=ibm.com	cn=RSA_Basic, dc=ibm.com
cn=green, o=Systems, c=us, dc=ibm.com	cn=RSA_Read_Only, dc=ibm.com
cn=watters, o=Systems, c=ca, dc=ibm.com	cn=RSA_CA_Software, o=Software, c=ca, dc=ibm.com
cn=lamothe, o=Systems, c=ca, dc=ibm.com	cn=RSA_CA_Software, o=Software, c=ca, dc=ibm.com

Novell eDirectory schema view

Using the Novell ConsoleOne tool, the schema described in “User schema example” on page 1 was pulled into a Novell eDirectory. The following illustration shows the top level view of the schema, as seen through the ConsoleOne tool.



The following illustration captures the users under o=Systems, c=us, dc=ibm.com.



Group membership

Novell eDirectory uses an attribute called GroupMembership to identify the groups to which a user is a member. The User object class specifically uses this attribute. The LDAP client uses a default value of memberOf in its search request to the LDAP server when querying the groups to which a user is a member.

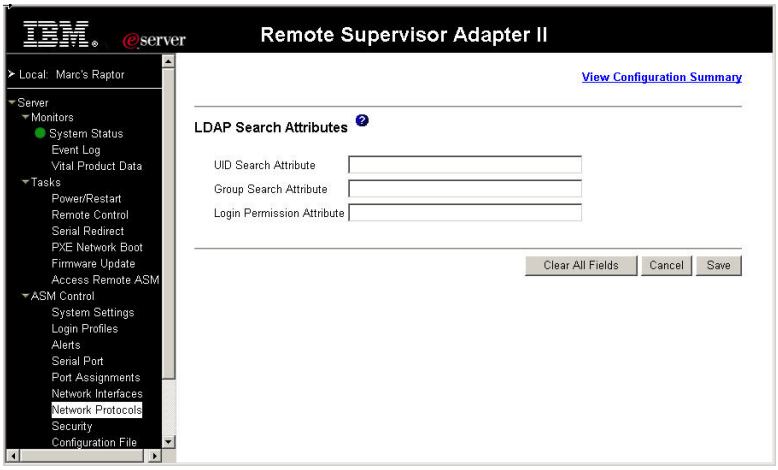
You can configure the LDAP client for membership queries using one of the following methods:

- Configure the value GroupMembership in the **Group Search Attribute** field on the LDAP client.

- Create an attribute mapping between GroupMembership and memberOf on the Novell eDirectory LDAP server.

Complete the following steps to configure the default attribute on the LDAP client:

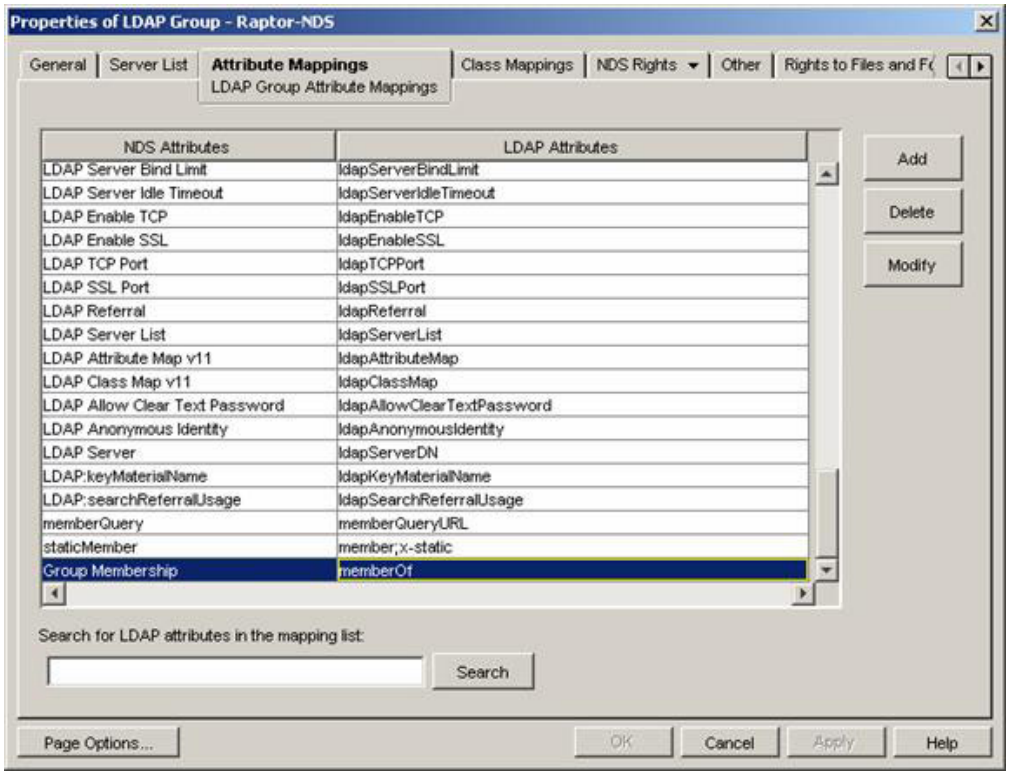
1. In the Remote Supervisor Adapter II Web interface, in the left navigation pane, click **Network Protocols**.
2. Scroll to the LDAP Search Attributes page. A page similar to the one in the following illustration is displayed.



3. In the **Group Search Attribute** field, type the default attribute that you want.

If the **Group Search Attribute** field is blank, it will default to memberOf and you will have to configure the Novell eDirectory server to map the attribute GroupMembership to memberOf. Complete the following steps to configure the Novell eDirectory server to map the attribute GroupMembership to memberOf.

1. Using ConsoleOne tool, right-click the **LDAP Group** icon and click **Properties**. The Properties of LDAP Group window opens.
2. Click the **Attribute Mappings** tab.
3. Click **Add** and then create a mapping between Group Membership and memberOf.
4. Click **OK**. A page similar to the one in the following illustration opens.

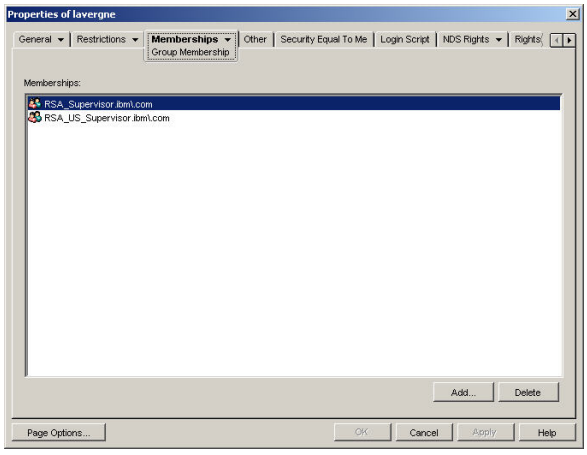


Adding users to user groups

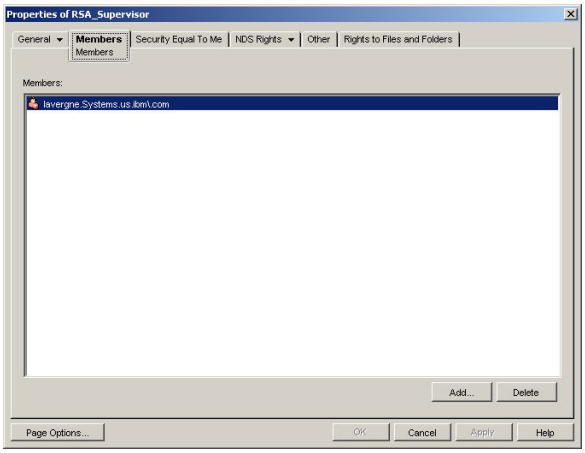
You can add users to the appropriate user groups either by adding the groups to the profile of a user, or adding users to the profile of a group. The end result is identical.

For example, in the user schema example on page 1, user lavergne is a member of both RSA_US_Supervisor and RSA_Supervisor. Using a browser tool such as Novell Console One, you can verify the schema (double-click **user lavergne** and select the **Memberships** tab.

A page similar to the one in the following illustration opens.



Similarly, if the properties of the RSA_Supervisor group are displayed, and you select the **Members** tab, a page similar to the one in the following illustration opens.

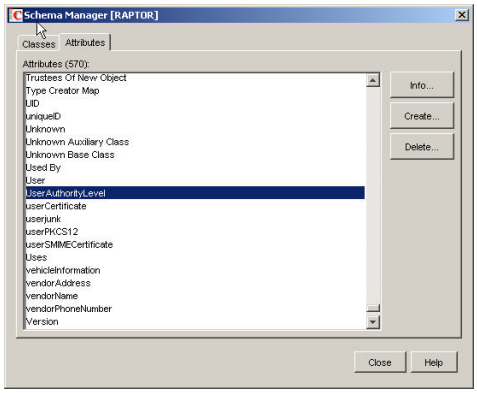


Authority levels

To use the authority levels feature, use ConsoleOne to create a new attribute labeled UserAuthorityLevel on the Novell eDirectory. This new attribute will be used to support authority levels. For more information about authority levels, see “Authority level (or login permissions) concepts” on page 26.

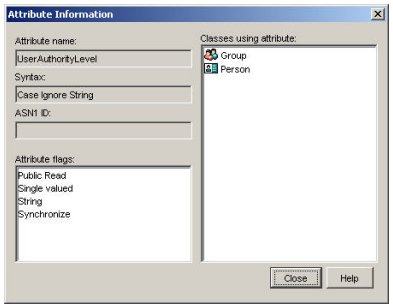
Complete the following steps to create a new attribute on the Novell eDirectory:

1. In the Novell ConsolOne tool, click **Tools → Schema Manager**.
2. Click the **Attributes** tab, and click **Create**.
3. Label the attribute UserAuthorityLevel. Leave ASN1 ID blank or see your LDAP administrator to determine the value to use. Click **Next**.
4. Set the syntax to Case Ignore String. Click **Next**.
5. Set the flags as applicable. See your LDAP administrator to make sure these are set correctly. Click the **Public Read** check box; then, click **Next**.
6. Click **Finish**. A page similar to the one in the following illustration opens.



7. Return to the Schema Manager window and click the **Classes** tab.
8. Click the **Person** class and click **Add**. Note that you can use the User object class instead.
9. Scroll down to the UserAuthorityLevel attribute, select it, and add it to the attributes for this class. Click **OK**.

10. Click the **Group** class and click **Add**.
11. Scroll down to the UserAuthorityLevel attribute, select it, and add it to the attributes for this class. Click **OK**.
12. To verify that the attribute was successfully added to the class, in the Schema Manager window, select the **Attributes** class.
13. Scroll to the UserAuthorityLevel attribute; then, click **Info**. A page similar to the one in the following illustration opens.



Setting authority levels

This section explains how to interpret and use the UserAuthorityLevel attribute. The value assigned to the UserAuthorityLevel attribute determines the permissions (or authority levels) assigned to a user after a successful authentication. The algorithm used to assign this authority level is described in “Configuring the search algorithm” on page 27.

The UserAuthorityLevel attribute is read as a bit-string or 0s and 1s. The bits are numbered from left to right. The first bit is bit position 0. The second bit is bit position 1, and so on.

- Bit position 0 - **Deny Always**. If set, a user will always fail authentication. Use this function to block a particular user or users associated with a particular group.
- Bit position 1 - **Supervisor Access**. If set, a user is given administrator privileges. The user has read and write access to every function. If you set this bit, you do not have to be individually set the other bits.
- Bit position 2 - **Read Only Access**. If set, a user has read-only access and cannot perform any maintenance procedures (for example, restart, remote actions, and firmware updates), and nothing can be modified (using the save, clear, or restore functions). Note that read-only and all other bits are mutually exclusive, with read-only having the lowest precedence. That is, if any other bit is set, this bit will be ignored.
- Bit position 3 - **Networking & Security**. If set, a user can modify the configuration in the Security, Network Protocols, Network Interface, Port Assignments, and Serial Port pages in the Web interface.
- Bit position 4 - **User Account Management**. If set, a user can add, modify, and delete users and change the Global Login Settings in the Login Profiles page in the Web interface.
- Bit position 5 - **Remote Console Access**. If set, a user can access the remote server console.

  For the BladeCenter management module only: Bit position 5 - **Blade Server Remote Console Access**. If set, a user can access a remote blade server video console with keyboard and mouse control.

- Bit position 6 - **Remote Console and Virtual Media Access**. If set, a user can access the remote server console and the virtual media functions for the remote server.

  For the BladeCenter management module only: Bit position 6 - **Blade Server Remote Console and Virtual Media Access**. If set, a user can access a remote blade server video console with keyboard and mouse control and can also access the virtual media features for that remote blade server.
- Bit position 7 - **Remote Server Power/Restart Access**. If set, a user can access the power on and restart functions for the remote server. These functions are available in the Power/Restart page in the Web interface.

  For the BladeCenter management module only: Bit position 7 - **Blade Server and I/O Module Power/Restart Access**. If set, a user can access the power on and restart functions for the blade servers and I/O modules. These functions are available on the Blade Tasks Power/Restart page and the I/O Module Tasks Power/Restart page in the Web interface.
- Bit position 8 - **Basic Adapter Configuration**. If set, a user can modify basic configuration parameters in the System Settings and Alerts pages in the Web interface.
- Bit position 9 - **Ability to Clear Event Logs**. If set, a user can clear the event logs. Everyone can look at the event logs, but this particular permission is required to clear the logs.
- Bit position 10 - **Advanced Adapter Configuration**. If set, a user has no restrictions when configuring the adapter. In addition, the user is said to have administrative access to the Remote Supervisor Adapter II, meaning that the user can also perform the following advanced functions: firmware updates, PXE network boot, restore adapter factory defaults, modify and restore adapter configuration from a configuration file, and restart and reset the adapter.
- Bit position 11 - **Reserved**. Reserved for future use.

The following list contains examples and their descriptions:

010000000000 Supervisor Access (bit position 1 is set)

001000000000 Read-Only Access (bit position 2 is set)

100000000000 No Access (bit position 0 is set)

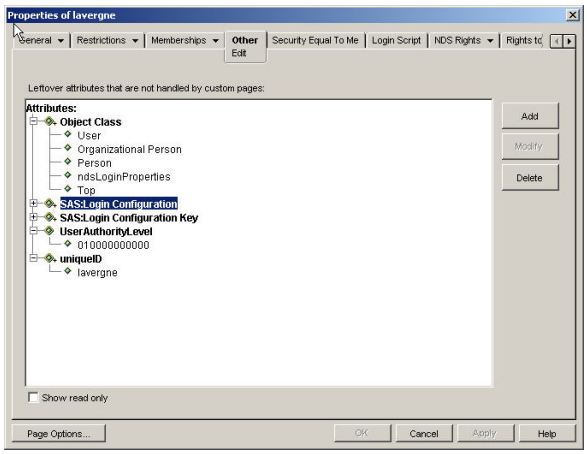
000011111100 All authorities except Advanced Adapter Configuration

000011011110 All authorities except access to virtual media

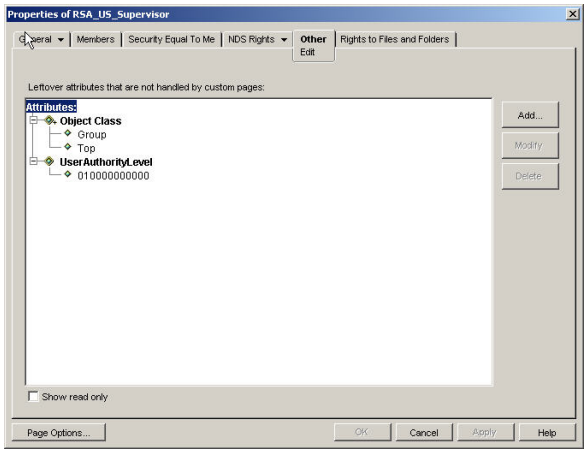
Complete the following steps to add the UserAuthorityLevel attribute to user lavergne, and to each of the user groups:

1. Right-click user **lavergne** and click **Properties**.
2. Click the **Other** tab. Click **Add**.
3. Scroll down to the UserAuthorityAttribute and click **OK**.
4. Fill in the value that you want for the attribute. For example, if you want to assign Supervisor access, set the attribute to 010000000000. Click **OK**.
5. Repeat steps 1 through 4 for each user group and set the UserAuthorityLevel as appropriate.

The following illustration shows the properties of user lavergne.



The following illustration shows the properties of RSA_US_Supervisor.



The following table shows the UserAuthorityLevel assigned to each of the user groups in the user schema example on page 1.

Table 2. UserAuthorityLevel assignments to user groups

User group	UserAuthorityLevel	Translation
RSA_Basic	000100000000	Networking and security
RSA_CA_Software	000101111010	Networking and security Remote console and virtual media access Remote server power and restart access Basic adapter configuration Advanced adapter configuration
RSA_Advanced	000110111100	Networking and security Remote console and virtual media access Remote server power and restart access Basic adapter configuration Advanced adapter configuration Ability to clear event logs
RSA_Supervisor	010000000000	Supervisor access
RSA_Read_Only	001000000000	Read-only access

Table 2. UserAuthorityLevel assignments to user groups (continued)

User group	UserAuthorityLevel	Translation
RSA_US_Advanced	000110111100	Networking and security User account management Remote console and virtual media access Remote server power and restart access Basic adapter configuration Ability to clear event logs
RSA_US_Supervisor	010000000000	Supervisor access

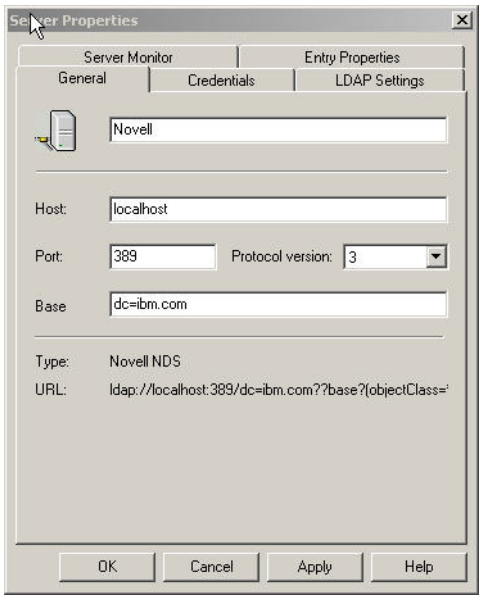
Browsing the LDAP server

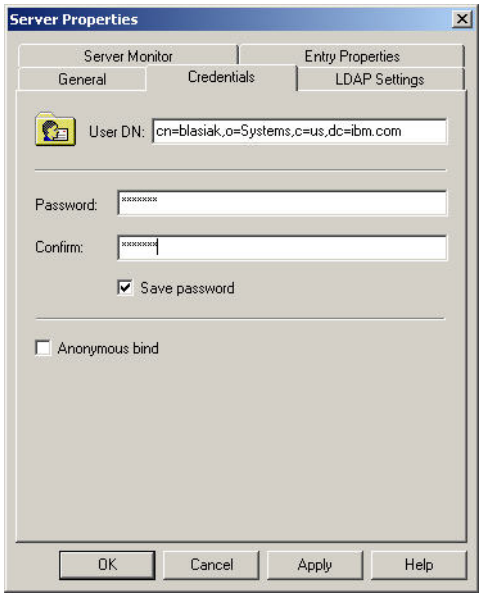
Before you attempt to connect from the LDAP client on the Remote Supervisor Adapter II to your LDAP server, connect to your LDAP server using a third-party LDAP browser of your choice. For example, there is a directory browsing tool available from http://www.ldapbrowser.com.

Using the LDAP browser before attempting to use the Remote Supervisor Adapter II LDAP client has the following advantages:

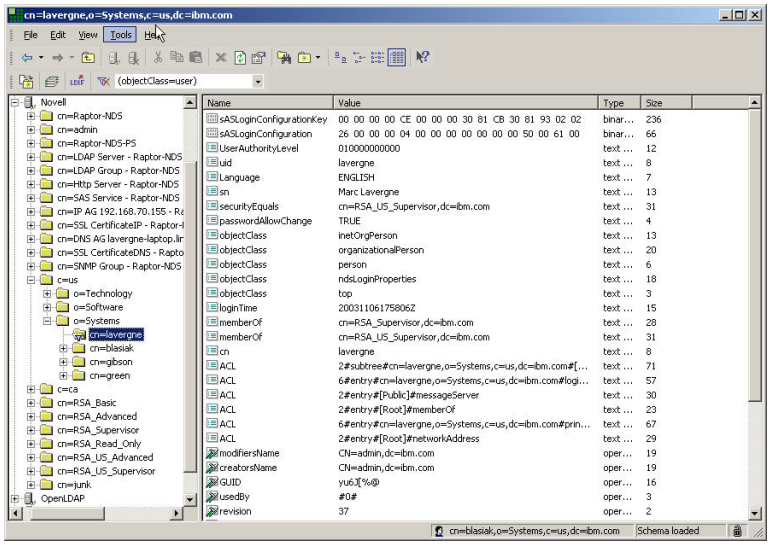
- The ability to bind to a server using various credentials. This will show whether the user accounts on the LDAP server are set up correctly. If you can bind to the server using the browser, but cannot bind to the server using the Remote Supervisor Adapter II LDAP client, the LDAP client is configured incorrectly. If you cannot bind using the browser, you will not be able to bind with the LDAP client on the Remote Supervisor Adapter II.
- After you successfully bind to the server, you can navigate through the LDAP server database and quickly issue search queries. This will confirm whether the LDAP server is configured the way you want it, with respect to access to the various objects. For example, you might find that you cannot view a particular attribute or you might not see all of the objects you were expecting to see under a specific search request. This indicates that the permissions assigned to the objects (for example, what is publicly visible or what is hidden) are not configured correctly. Contact the LDAP server administrator to correct the problem. It is important to note that the credentials you use to bind determine what privileges you will have on the server.
- Verify the group membership for all users. Verify the UserAuthorityLevel attribute assigned to users and user groups.

The following illustrations show various queries and search results made to a Novell eDirectory server configured with the user schema example from page 1. In this case, the Softerra LDAP browser tool was used. The initial bind to the server was made with the properties and credentials that are shown in the illustration.

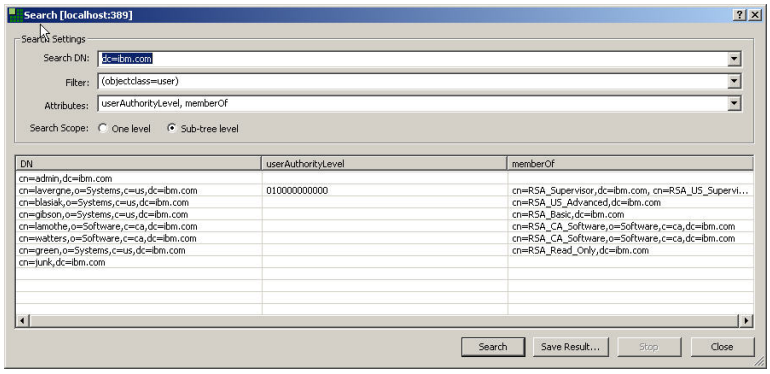

Server Properties
Server Monitor
Entry Properties
General
Credentials
LDAP Settings
Novell
Host:
localhost
Port:
389
Protocol version:
3
Base
dc=ibm.com
Type:
Novell NDS
URL:
ldap://localhost:389/dc=ibm.com??base?(objectClass=
OK
Cancel
Apply
Help


Server Properties
Server Monitor
Entry Properties
General
Credentials
LDAP Settings
User DN:
cn=blasiak,o=Systems,c=us,dc=ibm.com
Password:
Confirm:
Save password
Anonymous bind
OK
Cancel
Apply
Help

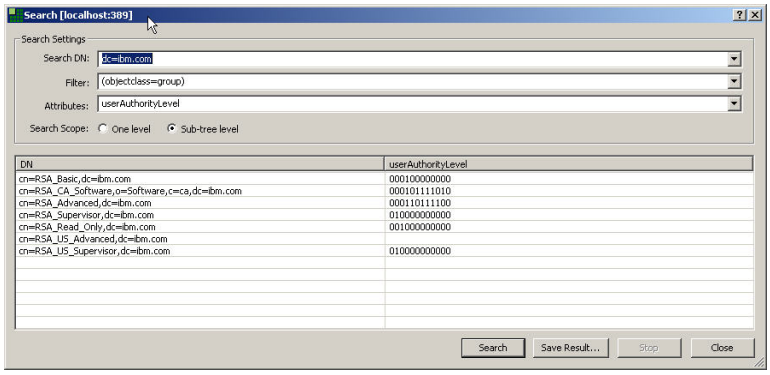
After the initial bind succeeds, the following view of the schema on the Novell eDirectory is displayed.



The following illustration shows a query of all users, with a request to retrieve the userAuthorityLevel and memberOf attributes.



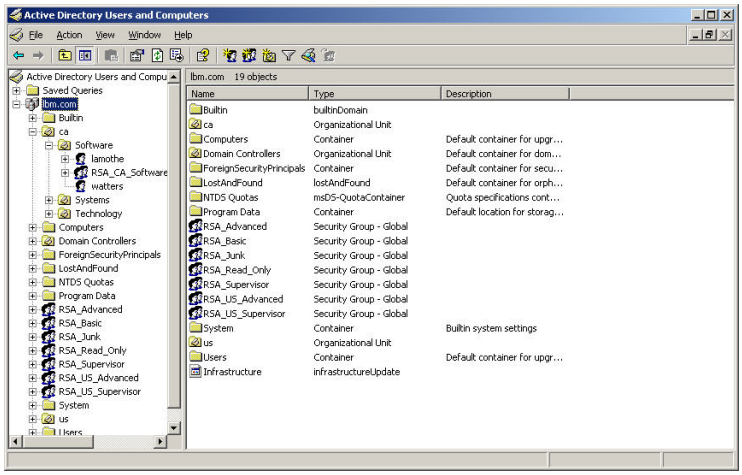
The following illustration shows a query of all user groups, with a request to retrieve the userAuthorityLevel attribute.



Microsoft Windows Server 2003 Active Directory schema view

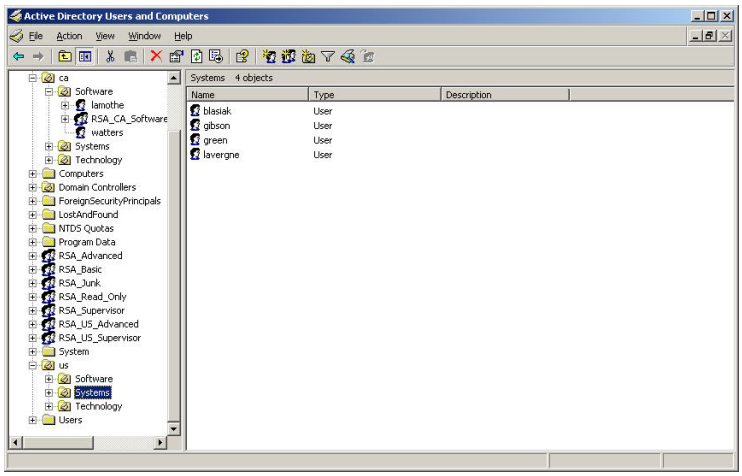
This section describes some of the configuration aspects relating to capturing the user schema example from page 1 on Microsoft Windows Server 2003 Active Directory.

The following illustration shows the top level view of the schema, as seen through the Active Directory Users and Computers management tool.



Note: The organizational unit object class was used to model the country. As such, the distinguished name for the Systems organizational unit in the US is ou=Systems, ou=us, dc=ibm, dc=com. Note that in the Novell eDirectory schema, the distinguished name would be o=Systems, c=us, dc=ibm.com.

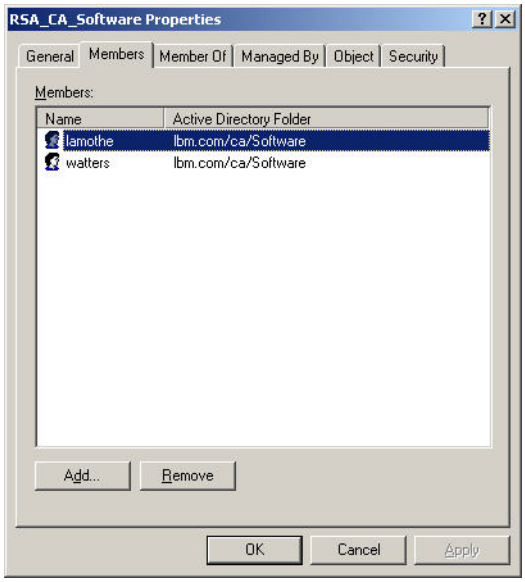
The following illustration shows the users under ou=Systems, ou=us, dc=ibm, dc=com.



Adding users to user groups

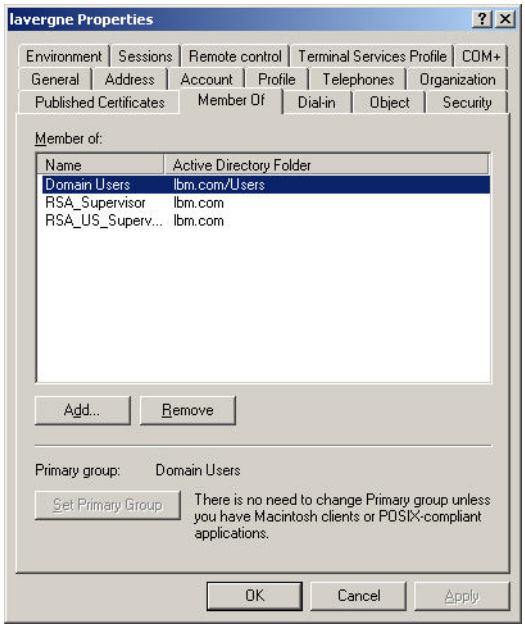
In Active Directory, you can either add groups to a specific user, or add users to a specific group. Right-click the user or user group object; then, click **Properties**.

If you select a user group and then click the **Members** tab, a page similar to the one in the following illustration opens.



To add or delete users from the user group, click **Add** or **Remove**.

If you select a user, and then click the **MembersOf** tab, a page similar to the one in the following illustration opens.



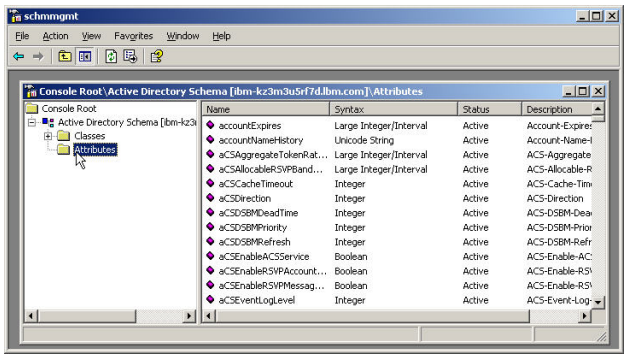
To add or delete users from the user group, click **Add** or **Remove**.

Authority levels

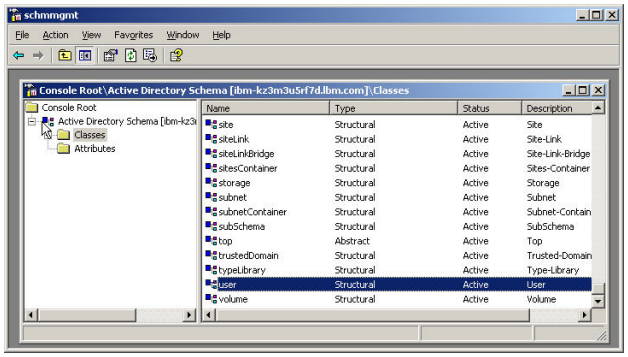
The section “Authority levels” on page 6 describes how to create a new attribute with the Novell eDirectory server in order to support the concept of authority levels, and how they are assigned to users who authenticate to an LDAP server from a Remote Supervisor Adapter II. The attribute created was called UserAuthorityLevel. In this section, you will create this attribute on Active Directory.

1. Install the Active Directory Schema Snap-In. For more information, see the documentation that comes with Active Directory.

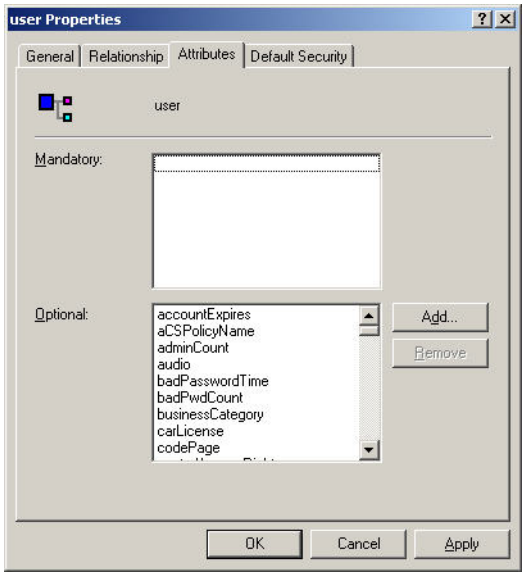
2. Start the Active Directory Schema.
3. Click **Action → Create Attribute**. Fill in the following fields:
   - Set Common Name to UserAuthorityLevel.
   - Set Syntax to Case Insensitive String
   - Set Minimum and Maximum to 12
4. Contact your system administrator to assign a new X.500 OID. If you do not want to define a new X.500 OID, use an existing attribute instead of creating a new attribute for the authority level.



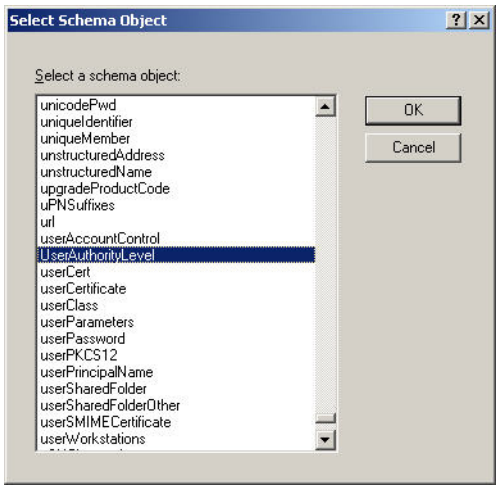
5. After the attribute is saved, select the **Classes** folder.



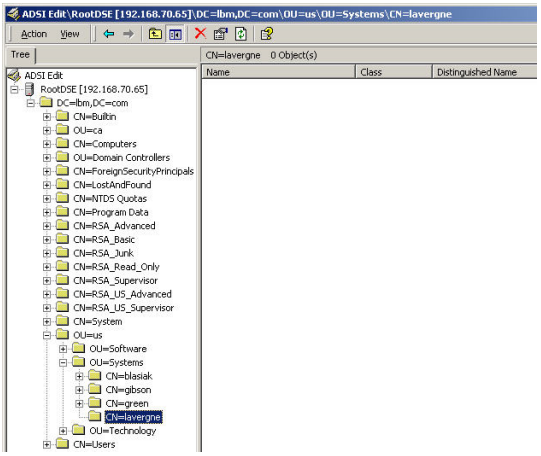
6. Double-click the class **user**. The user Properties window opens.



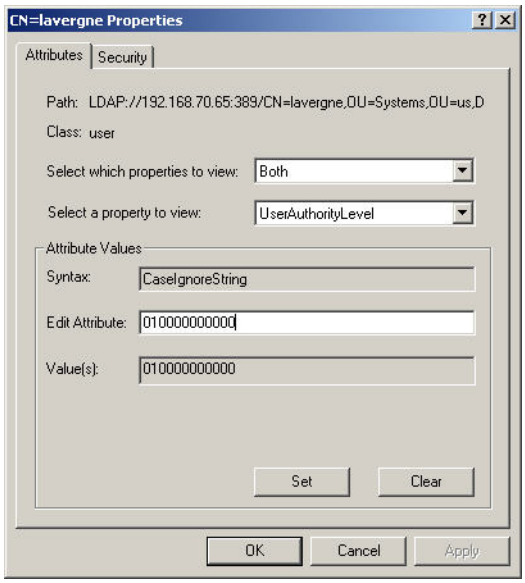
7. Select the **Attributes** tab and then click **Add**. The Select Schema Object window opens.



8. Scroll down to UserAuthorityLevel and click **OK**. This attribute will now appear in the list of optional attributes for the user object class.
9. Repeat step 6 on page 15 through step 8 for the class **groups**. This enables the UserAuthorityLevel attribute to be assigned to a user or a user group. These are the only two object classes that need to use this new attribute.
10. Assign the UserAuthorityLevel attribute to the appropriate users and user groups. To match the schema defined under the Novell eDirectory server, use the same values as in “Setting authority levels” on page 7. You can use the ADSI Edit tool to do this. The Microsoft ADSI Edit support tool is a Microsoft Management Console (MMC) snap-in used to view all objects in the directory (including schema and configuration information), modify objects, and set access control lists on objects.
11. For this example, assume that you want to add the UserAuthorityLevel attribute to user lavergne. Use ADSI Edit to do this. Note that you must supply the appropriate credentials to connect to Active Directory. Otherwise, you might not have the proper user privileges to modify objects on the server. The following illustration shows the schema, as seen by ADSI, after connecting to the server.



12. Right-click **lavergne** and click **Properties**. A window similar to the one in the following illustration opens.



13. In the **Select which properties to view** field, select **UserAuthorityLevel**.
14. In the **Edit Attribute** field, type `010000000000`, which translates to Supervisor Access. Click **Set**.
15. Click **OK**.
16. You can add this attribute to user groups by following the same steps for the user group object that you want to modify.

Checking Active Directory configuration

Before attempting to connect the Remote Supervisor Adapter II LDAP client to the Active Directory (to authenticate users), browse the Active Directory schema with an LDAP browser. Issue at least the queries listed in the following table to check authority levels and group membership.

Table 3. Checking authority levels and group membership

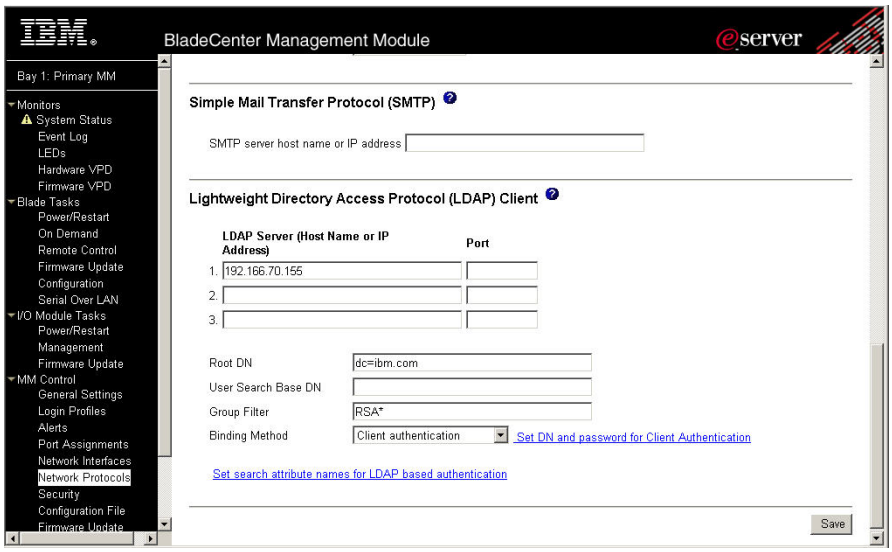
Search distinguished name	Filter	Attributes
DC=ibm, DC=com	(objectclass=user)	memberOf, userAuthorityLevel
DC=ibm, DC=com	(objectclass=group)	member, userAuthorityLevel

Configuring the LDAP client

After the LDAP server is properly configured using either the Novell eDirectory server or Microsoft Active Directory, you must then configure the Remote Supervisor Adapter II LDAP client to access the LDAP server.

Main LDAP configuration page for Novell eDirectory

The main LDAP configuration page for Novell eDirectory is shown in the following illustration.

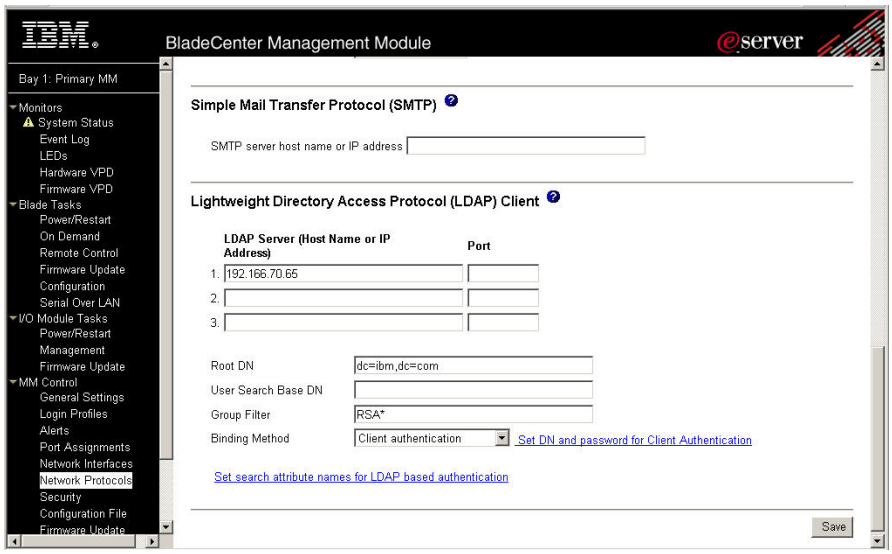


The **Binding Method** field for Novell eDirectory must be set to Client Authentication, as shown in the previous illustration.

Note: Novell eDirectory does not support the User Principal Name and Strict User Principal Name options.

Main LDAP configuration page for Active Directory

The main LDAP configuration page for Active Directory is shown in the following illustration.

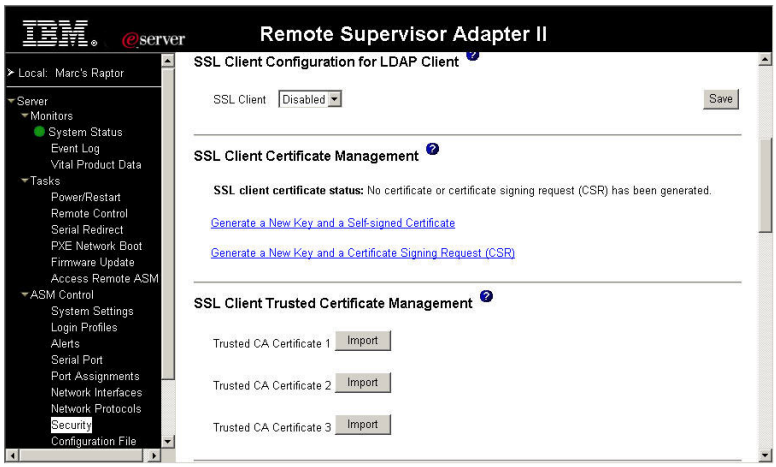


Note the difference in the notation for the Distinguished Name (DN). With Active Directory, the Root DN must be set to dc=ibm,dc=com. Using dc=ibm.com does not work.

Usage notes about the main LDAP configuration page

Read the following general information:

- In the user schema example that is used in this document, only one LDAP server is configured. You can configure up to three servers. If the **Port** field for a server is blank, the LDAP client will bind using the default port 389 for non-secured connections, and 636 for secured connections. The LDAP client will only attempt to use a secured connection if the SSL client for LDAP is enabled. The Security page is used to configure the SSL Client for LDAP. The following illustration shows that the SSL client is disabled.



- If more than one LDAP server is configured, it is assumed that the databases are replicated across the servers. That is, only use multiple LDAP servers for redundancy purposes. If invalid credentials (for example, a wrong password or invalid user ID) are supplied during the authentication process, the LDAP client will fail authentication immediately, without trying the next server in the list. However, if the first server is not available, an attempt is made to authenticate with the next server in the list.
- In the user schema example, the root of the tree is at dc=ibm.com. This is the value that must be configured in the **Root DN** field for Novell eDirectory. With Active Directory, the notation is slightly different. The root of the tree is denoted by dc=ibm,dc=com.
- The **User Search Base DN** field indicates where all the searches for users and groups begin. Leave this field blank, which means that it will default to the same value as the Root DN. The only time it should be configured with a more specific search distinguished name is when all users and groups in your schema can be found below that sub-tree, making the search more efficient.
- The **Group Filter** field determines how group authentication is performed. If this field is blank, group authentication is disabled. This means that a user does not have to be a member of a specific group to pass the authentication process. When it is configured with a value, group authentication is enabled. When group authentication is enabled, any user who attempts to authenticate via the LDAP server must be a member of at least one user group whose name matches the **Group Filter** field. In the user schema example, the configured value is RSA*. This means that a user will only pass group authentication if he is a member of at least one group whose name starts with the prefix RSA.

  Using the user schema example on page 1, Table 4 on page 20 illustrates who could successfully pass group authentication, if you configure the Group Filter with the different values listed.

Note: Use Table 1 on page 3 as a cross-reference. It shows the user groups of which each user is a member.

Table 4. Group filter scenarios

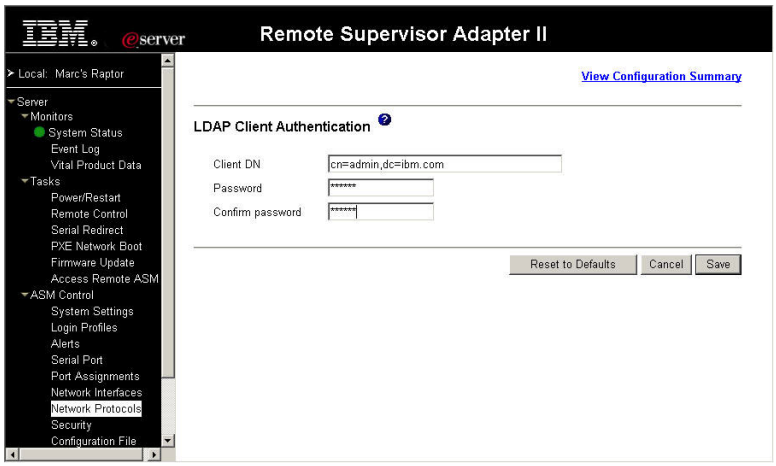
Group filter	Group authentication	Matches	Valid users
*	Enabled	All groups	All users
RSA*	Enabled	RSA_Basic RSA_CA_Software RSA_Advanced RSA_Supervisor RSA_Read_Only RSA_US_Advanced RSA_US_Supervisor	All users except admin
RSA_CA*	Enabled	RSA_CA_Software	lamothe walters
RSA_US*	Enabled	RSA_US_Advanced RSA_US_Supervisor	blasiak lavergne
RSA_Supervisor	Enabled	RSA_Supervisor	lavergne
RSA	Enabled	No match	None
	Disabled		All users

- The **Binding Method** field must be set to Client Authentication for access to a Novell eDirectory server. For access to a Microsoft Active Directory server, it can be set to Client Authentication, User Principal Name, or Strict User Principle Name.

  The concept of the User Principle Name (UPN) attribute is proprietary to the Microsoft Active Directory server.

  Do not set the Binding Method to Anonymous Authentication. Although you will succeed in binding to the LDAP server using this method, it is unlikely that any search requests (which are part of the authentication process) will succeed. In most cases, the LDAP server administrator will provide very limited read access to an anonymous user. Therefore, if the LDAP client does not have read access to users, authentication will always fail.

  When the Binding Method is set to Client Authentication, you must configure credentials in the LDAP Client Authentication page. These credentials are used when the LDAP client on the Remote Supervisor Adapter II first binds to the LDAP server. The following illustration shows the credentials used in the user schema example environment (for Novell eDirectory). The notation for Client DN will change to dc=ibm,dc=com for Active Directory.



Note that these credentials are used only on the initial bind to the server. The subsequent search request for the record of the user (the one attempting to log in to the Remote Supervisor Adapter II) will only succeed if the LDAP server administrator has provided sufficient user privileges to this particular client distinguished name. If the search is successful, a second bind attempt will be made to the server, this time with the distinguished name of the user (retrieved from the search response) and password (from the logon attempt).

When the Binding Method is set to UPN or Strict UPN (which are only used with Active Directory), there is no need to configure the above LDAP Client Authentication page (any values configured in this page are ignored).

Using UPN or Strict UPN as the binding method means that the credentials (user ID and password) provided by the user (when logging into the Remote Supervisor Adapter II) will be used directly as is for the credentials on the first bind to the LDAP server. If the credentials are valid, the bind will succeed and the user will have passed the user authentication process (group authentication would then take place, if enabled). The only difference between UPN and Strict UPN is that a fully qualified user name[1] must be provided if Strict UPN is used (for example, lavergne@ibm.com). The user name will be parsed for the @ symbol, and it must contain it for the authentication process to proceed.

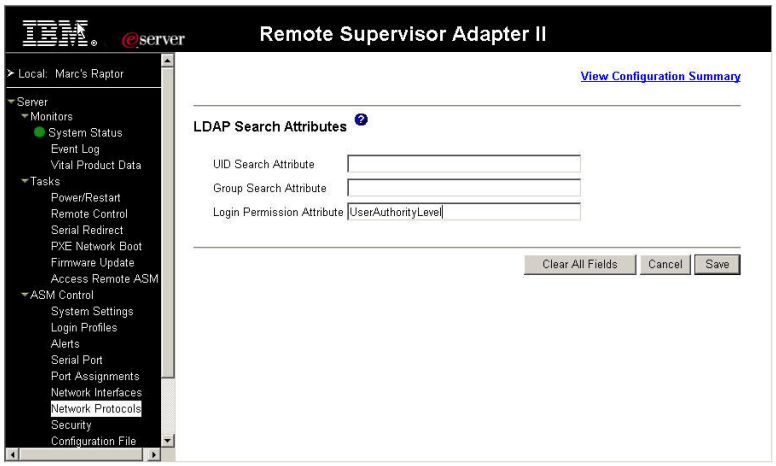
Configuring the LDAP search attribute page

To complete the configuration of the LDAP client, you must configure the LDAP Search Attributes page.

1. With Microsoft Active Directory server, the attribute used in a search request for a specific user is changed to userPrincipalName when a fully qualified user name is used during the login process (and binding method is UPN or Strict UPN). For example, if a user name is lavergne@ibm.com and Strict UPN is configured, the first search request sent to the LDAP server after the initial bind will have the form (&(objectclass=user)(userPrincipalName=lavergne@ibm.com)).

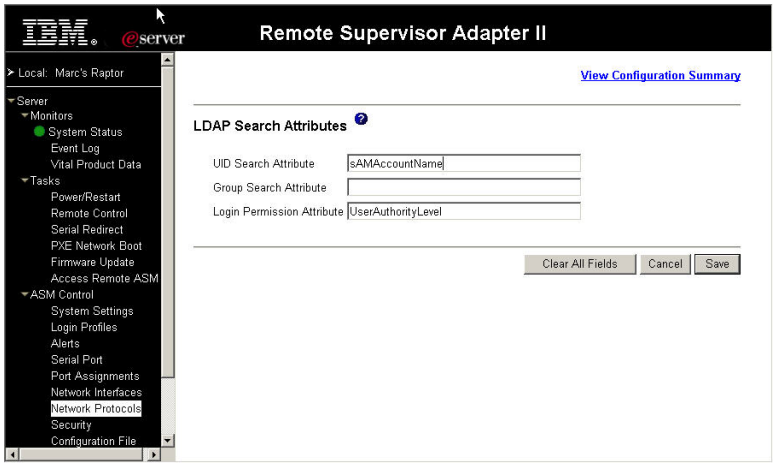
LDAP search attribute page for Novell eDirectory

The following illustration shows the LDAP search attribute page for Novell eDirectory.



LDAP search attribute page for Active Directory

The following illustration shows the LDAP search attribute page for Active Directory.



Usage notes about the LDAP search attribute page

Read the following important information.

UID Search Attribute field

The UID Search Attribute is used by the LDAP client on the Remote Supervisor Adapter II to search the user record associated with a particular user ID (the logon name for the user attempting to gain access to the Remote Supervisor Adapter II). When this field is blank, the default value *uid* is used.

For Novell eDirectory: The **UID Search Attribute** field should be blank. Novell eDirectory supports the standard UID attribute.

For Active Directory: The **UID Search Attribute** field should be set to sAMAccountName. Active Directory does not support the standard UID attribute. Instead, the sAMAccountName is usually used for the logon name.

As previously described, after the first successful bind to the LDAP server, the LDAP client will issue its first search request (to find the distinguished name of the user, the groups to which a user is a member, and what, if any, authority levels are associated with this user). The search request contains a search filter, which will have the following form (assuming that the user ID entered during the login process was lavergne)[2]:

```
(&(objectclass=user)(uid=lavergne))
```

If the **UID Search Attribute** field is not blank, the value configured will replace the word *uid* in the previous search filter. If you choose to configure a different UID Search Attribute, you must first use your LDAP browsing tool and issue search requests with the appropriate filter. If the search requests are successful, you will know that the LDAP server was properly configured to recognize this attribute.

In addition to including the search filter, the search request also contains the names of attributes that the LDAP client needs to retrieve to complete the authentication process. In particular, it needs to retrieve the distinguished name of the user[3], the names of the user groups to which the user is a member, and the optional authority level.

Group Search Attribute field

To retrieve the user groups, the attribute memberOf is usually used. Active Directory supports it, and as shown earlier in the Novell eDirectory section, the attribute memberOf was mapped to what Novell eDirectory uses for that purpose (attribute Group Membership).

The **Group Search Attribute** field should be blank if you want to use the default of memberOf to search for group membership. If another attribute should be used instead, you must configured it in the **Group Search Attribute** field.

Login Permission Attribute field

The **Login Permission Attribute** field is used for authority levels. There is no default for this field. To correctly assign user authority levels to a user being authenticated via an LDAP server, you must indicate what attribute to use.

For Novell eDirectory, you created an attribute called UserAuthorityLevel for this purpose (see “Setting authority levels” on page 7). For the example user schema, this is the value that must be configured in the **Login Permission Attribute** field, as shown in the illustration in “LDAP search attribute page for Novell eDirectory” on page 22.

If the **Login Permission Attribute** field is blank, the user will always be assigned Read-Only permissions (assuming that the user first passes the user authentication process). You must configure this field to avoid this situation. The LDAP server must be configured to recognize this attribute. You can either create a new attribute on

---

2. The exception, as noted on the previous page, is with Microsoft Active Directory, when the user name contains the @ symbol, and UPN or Strict UPN is used as the binding method. In this case, the search filter is (&(objectclass=user)(userPrincipalName=<fully_qualified_name>)), regardless of what is configured as the UID Search Attribute.
3. The distinguished name of the user is only required when the Binding Method selected is Client Authentication. This is because after the first search request, the LDAP client must attempt to rebind to the LDAP server using the actual password provided during the login process. This bind request will contain the distinguished name of the user and the password. This is the only scenario in which a second bind attempt is required. With UPN and Strict UPN, the first bind attempt uses the credentials provided by the user immediately.

the LDAP server (as you did with the UserAuthorityLevel on both the Novell eDirectory server and the Active Directory server), or use an attribute which already exists in your schema.

Understanding authority levels

The authority level assigned to a user depends on several factors. For the example user schema, assume that the attribute UserAuthorityLevel is used to identify the authority level. There are two possibilities to consider:

- If you want to assign an authority level directly to a user, the UserAuthorityLevel attribute should be part of the record of the user. In this case, the value of this attribute will be assigned directly to the user, before group authentication (if required), is even attempted. See "Adding users to user groups" on page 5.
- If you do not want to assign an authority level directly to a user, the only alternative is to assign an authority level based on the groups to which a user is a member. In this case, you must add the UserAuthorityLevel attribute to the appropriate user groups. See "Adding users to user groups" on page 5.

  If the LDAP client cannot find the UserAuthorityLevel attribute directly in the record of the user, it will assign an authority level during the group authentication phase. The algorithm used is described in the following sections.

  If group authentication is disabled or if the ASM Group Filter is a wildcard (*):

  1. Find the groups to which the user is a member. Name this set of groups Set A.
  2. For each group in Set A, read the UserAuthorityLevel.
  3. The authority level assigned to the user is the strongest inclusive OR of all the UserAuthorityLevel attributes from Set A. Strongest means that the Read-only bit and Deny Always bit have the lowest priority, and the supervisor bit has the highest priority.
  4. If none of the groups in Set A have a UserAuthorityLevel attribute associated with them, or if Set A is empty, the user is assigned a default authority level of Read-Only.

  Otherwise, if group authentication is enabled and the ASM Group Filter is not a wildcard:

  1. Find the groups to which the user is a member. Name this set of groups Set A.
  2. If Set A is empty, fail the authentication (because the user has failed the group authentication).
  3. Otherwise, from Set A, find the subset of groups that match the ASM Group Filter that you defined (see "Usage notes about the main LDAP configuration page" on page 19) for the Remote Supervisor Adapter II. Name this subset Set B.
  4. If Set B is empty, fail the authentication (because the user has failed the group authentication).
  5. Otherwise, read the UserAuthorityLevel for each group in Set B.
  6. The authority level assigned to the user is the strongest inclusive OR of all the UserAuthorityLevel attributes from Set B.
  7. If none of the groups in Set B have a UserAuthorityLevel attribute associated with them, the user is assigned a default authority level of Read-Only.

Appendix A. Using the LDAP search algorithm

This appendix describes the LDAP search algorithm and how the configuration parameters for LDAP are used in the search.

Using multiple LDAP servers

You can configure up to three LDAP servers. The IP address is usually used to identify a particular LDAP server. The port number that is used to connect to the LDAP server can be optionally configured. If the field is blank, the default value is 389 for non-secured LDAP connections, and 636 for secured LDAP connections. In this context, *secured* means that the SSL client is enabled. When the SSL client is disabled, communication with the LDAP server is not encrypted.

For more information about setting up a client to use an LDAP server, see the *IBM Remote Supervisor Adapter II User's Guide* or the *IBM @server BladeCenter Management Module User's Guide*.

The LDAP client always attempts to connect with the first LDAP server that is configured. The next server configured in the list is used only if the previous server is unavailable.

Note: If a user attempts to authenticate by using invalid user credentials (for example, an invalid password or non-existent account) on the first server, no attempt will be made to authenticate on the next server in the list. Multiple LDAP servers are used to support redundancy only. Therefore, if a user account exists on one LDAP server, it must also exist on every other configured LDAP server.

Defining the user authentication method

You can authenticate users locally or using LDAP. You can configure the authentication method using the Global Login Settings page in the Web interface. You can choose one of the following authentication methods:

- Local only
- LDAP only
- Local first, then LDAP
- LDAP first, then Local

Note: Use "LDAP only" authentication cautiously. If the LDAP servers are unavailable, or if the user credentials are invalid, access to the Remote Supervisor Adapter II will fail.

For more information about user authentication methods, see the *IBM Remote Supervisor Adapter II User's Guide* or the *IBM @server BladeCenter Management Module User's Guide*.

Group authentication concepts

There are two parts to user authentication:

- Validating the user ID and password (mandatory)
- Validating group membership (optional)

To validate a user ID and password, there must be an exact match. After validation is completed, group membership is verified, if required.

The Group Filter parameter defines whether or not group membership verification is required. If it is blank, group membership is not verified. When configured, group membership must be verified. This step must succeed for the user to complete user authentication. The Group Filter parameter identifies the group (or set of groups) to which this particular Remote Supervisor II is a member. The filter can be one of the following:

- A specific group name which matches only one group (for example, RSAWest)
- The wildcard character *, which matches all groups
- The wildcard character * with a prefix (for example, RSA*), which matches all groups with that specific prefix in their name

For more information about the Group Filter parameter, see the *IBM Remote Supervisor Adapter II User's Guide* or the *IBM @server BladeCenter Management Module User's Guide*.

After the user ID and password for a user are verified, the LDAP server is queried for the group (or groups) of which this user is a member. Group membership succeeds if at least one of the groups of which the user is a member matches the Group Filter. If there is no match, group membership fails, which means that user authentication also fails.

For example, assume the Group Filter name configured is IT*. If the user is a member of groups Admin, ITNorth, and ITWest, there is a match. If the user is a member of only groups Admin and Accounting, there is no match. If the Group Filter name is *, everything matches.

Authority level (or login permissions) concepts

After a user is successfully authenticated, you must assign an authority level (or login permissions) to the user. These login permissions identify what the user can and cannot do while logged in. For example, some users should only have read-only permissions, while others should have full administrative privileges (can perform all tasks). Also, some users will have a variety of permissions, meaning that they have write access to some tasks, and read-only access to everything else.

The login permissions are retrieved from the LDAP server. They are assigned as follows:

- If login permissions are found in the profile for the user being authenticated, it is these permissions that are assigned to the user.
- If login permissions are not found in the profile of the user, they must be retrieved from the groups of which the user is a member. The login permissions assigned are an aggregate of the login permissions of the groups that match the ASM Group Filter.
- If login permissions are not found in the profile of the user, and are not found in any of the groups of which the user is a member (or if group membership verification is skipped), the user is assigned default read-only permissions.

Configuring the search algorithm

This section describes the procedure that is used during user authentication through an LDAP server. It is assumed that you are familiar with LDAP terminology and the configuration parameters.

For more information about LDAP and the configuration parameters, see the *IBM Remote Supervisor Adapter II User's Guide* or the *IBM @server BladeCenter Management Module User's Guide*.

Note: SSL messages are not covered in this document. If the SSL client for LDAP is enabled, it is assumed that all of the messages between the LDAP client and the LDAP server are secure.

Complete the following steps to configure the LDAP search algorithm:

1. Retrieve the address of the next LDAP server (and port number). A bind request is sent to the server on that port (if no port is configured, port 389 will be used as the default if the SSL client for LDAP is disabled; port 636 will be used as the default if the SSL client for LDAP is enabled). The contents of the bind request depend on the Binding Method configured.
   - If **Client Authentication** is selected in the **Binding Method** field, the bind request contains the user distinguished name and password that area configured in the LDAP Client Authentication page.
   - If **UPN** is selected in the **Binding Method** field, the bind request contains the user ID and password that are entered by the user in the login screen. That is, whatever is entered as the user ID is passed directly to the LDAP server as is.
   - If **Strict UPN** is selected in the **Binding Method** field, the bind request contains the user ID and password that are entered by the user in the login screen. The user ID must be in UPN format, meaning it must have the form userid@somedomain.xyz. The user ID will be parsed for the @ symbol, and user authentication will terminate immediately if it does not contain it.
2. Choose one of the following actions, depending on the results of the bind request:
   - If the bind request fails because the user supplied invalid credentials, the user authentication process is terminated immediately and has failed.
   - If the bind request fails for any other reason, and there is at least one more server to try, repeat step 1. Otherwise, user authentication terminates and has failed.
   - If the bind request succeeds, go to step 3.

   Note: The use of "Anonymous Authentication" as the Binding Method is discouraged because subsequent search requests will fail (when a null user ID and null password are used as the parameters to the initial bind request).
3. If the initial bind request has succeeded, you can build a search request message in order to retrieve specific user-related attributes from the LDAP server. The search request message contains the following parameters:
   - **Distinguished name to be used as the search base**. This parameter is set to the configured "User Search Base DN" value. If this value is not configured (for example, it is blank), the "Root DN" value is used instead.
   - **Search filter.** The search filter is set to "(&(objectClass=user)(param1=param2))", where

param1 = “userPrincipalName”, if the Binding Method = UPN or Strict UPN

param1 = Configured UID Search Attribute value

param1 = “uid”, if the configured UID Search Attribute value is blank

param2 = user ID entered by user during login process

- **Attributes to retrieve.** This parameter tells the LDAP server which user attribute to retrieved from the profile of the user. The following attributes are requested:
  - **distinguishedName:** The distinguished name associated with the user identified in the previous Search Filter.
  - **Configured Group Search Attribute value:** This string represents the name of the attribute in the profile of the user, which identifies the groups of which the user is a member. If the configured value is blank, the default “memberOf” is used.
  - **Configured Login Permission Attribute value:** This string represents the name of the attribute in the profile of the user, which identifies the login permissions associated with this user. This parameter has no default, which means it must be configured by the user. If it is blank, the login permissions can never be retrieved from the LDAP server, meaning that the user will always be assigned default read-only permissions.

The search request message is sent to the LDAP server. If a successful response is received, go to step 4; otherwise, user authentication terminates and has failed.

4. If a response to the initial search request is received, choose one of the following actions:
   - If the initial Binding Method used in step 1 was **UPN** or **Strict UPN**, the password entered by the user is verified. Go to step 6.
   - If the initial Binding Method used in step 1 is **Client Authentication**, the password entered by the user during the login process is not verified yet. Go to step 5.
5. Retrieve the distinguished name of the user from the search response message. A new bind request message is constructed with this distinguished name and the password entered by the user during the login process. The bind request is sent to the LDAP server to validate this password. Choose one of the following actions:
   - If the bind request succeeds, the user password is validated. Go to step 6.
   - If the bind request fails because the credentials of the user were invalid, user authentication terminates immediately and has failed.
   - If the bind request fails for any other reason and if there is at least one more LDAP server to try, repeat step 1 on page 27. Otherwise, user authentication terminates immediately and has failed.
6. Determine if the search response (from step 3 on page 27) contains the login permissions associated with the user. Remember that the search request contained the attribute asking for these login permissions.

   If the response does not contain the login permissions (for example, the record of the user on the LDAP server does not contain the login permissions attribute), go to step 7 on page 29.

   If the response does contain the login permissions, proceed as follows:
   - Assign the login permissions to the user for the duration of the user session.

- If the configured ASM Group Filter value is blank, there is no need to perform group membership verification. If this is the case, user authentication terminates and has succeeded.
- If the configured ASM Group Filter value is not blank, group membership verification must occur. Proceed as follows:
  - Retrieve the group (or groups) of which the user is a member from the search response. Remember that the search request contained the attribute asking for these groups.
  - Find at least one group that matches the configured ASM Group Filter value.
  - If there is a match, group membership authentication succeeds. As a result, user authentication terminates immediately, and has succeeded.
  - If there is no match, group membership authentication has failed. As a result, user authentication terminates immediately and has failed.

7. If the search response does not contain login permissions for the user, choose one of the following actions:
   - If the configured ASM Group Filter value is blank, there is no need to perform group membership verification. Assign read-only permission to the user. User authentication terminates immediately and has succeeded.
   - If the configured ASM Group Filter value is not blank, complete the following steps to perform group membership verification:
     a. Retrieve the group (or groups) of which the user is a member from the search response (from step 3 on page 27).
     b. For each group name retrieved, check to see if it matches the configured ASM Group Filter.
     c. If no group name matches, group membership verification has failed. User authentication terminates immediately and has failed.
     d. If there is at least one match, group membership verification has succeeded. Assign the login permissions to the user from these groups.
8. For each group name that matches, send a new search request message to the LDAP server containing the following parameters:
   - **DN to be used as the search base**. Use this parameter to set the configured “User Search Base DN” value. If this value is not configured, the “Root DN” value is used instead.
   - **Search filter**. The search filter is set to “(&(objectClass=group)(cn=param1))”, where param1 = the first cn parameter in the distinguished name of the group name (for example, if the distinguished name of the group is “cn=RSA, cn=users, dn=abc, dn=com”, param1 equals “RSA”).
   - **Attributes to retrieve**. Use this parameter to tell the LDAP server which attributes to retrieve. The following attributes are requested:
     - **distinguishedName:** The distinguished name of the entry.
     - **Configured Login Permission Attribute**
   - Retrieve the login permissions from the search response, and perform a bit-wise (for example, logical) OR operation with the current login permissions of the user.
   - If none of the search responses contain the login permissions attribute, assign the user a default of read-only permission.

Appendix B. Notices

This information was developed for products and services offered in the U.S.A.

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 give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

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 states 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 Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product, and use of those Web sites is at your own risk.

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

Edition notice

Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

Active Memory
Active PCI
Active PCI-X
Alert on LAN
BladeCenter
C2T Interconnect
Chipkill
EtherJet
e-business logo
@server
FlashCopy
IBM
IBM (logo)
IntelliStation
NetBAY
Netfinity
NetView
OS/2 WARP
Predictive Failure Analysis
PS/2
ServeRAID
ServerGuide
ServerProven
TechConnect
ThinkPad
Tivoli
Tivoli Enterprise
Update Connector
Wake on LAN
XA-32
XA-64
X-Architecture
XceL4
XpandOnDemand
xSeries

Lotus, Lotus Notes, SmartSuite, and Domino are trademarks of Lotus Development Corporation and/or IBM Corporation in the United States, other countries, or both.

Intel, MMX, and Pentium are trademarks of Intel Corporation in the United States, other countries, or both.

Microsoft, Windows, and Windows NT are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Index

T

Part Number: 25K8154

Printed in USA

(1P) P/N: 25K8154