Authenticating Admins Using LDAP

LDAP (Lightweight Directory Access Protocol) is an internet protocol for accessing distributed directory services. The NIOS appliance can authenticate admin accounts by verifying user names and passwords against LDAP. The NIOS appliance queries the LDAP server for the group membership information of the admin. The appliance matches the group names from the LDAP server with the admin groups in its local database. It then authorizes services and grants the admin privileges, based upon the matching admin group on the appliance. Figure 4.8 illustrates the LDAP authentication process.

![Figure 4.8 Authenticating using an LDAP server](image)

**Figure 4.8 Authenticating using an LDAP server**

**Authentication Protocols**

When you configure the NIOS appliance to authenticate admins against an LDAP server group, you must specify the authentication protocol of each LDAP server, which can be either anonymous or authenticated. The NIOS appliance connects anonymously to the LDAP server when the authentication type is anonymous. With authenticated type, the NIOS appliance connects using the bind DN and bind password defined for that server.

You can configure one of the following modes to send the authentication request to the LDAP server:

- **Ordered**: In this mode, the authentication request is sent to the first server in the list. The authentication request is sent to the next server only when the first server is out of service or unavailable.
- **Round Robin**: In this mode, the first authentication request is sent to a server chosen randomly in a group. If there is no response from the server, continued attempts are performed sequentially until it selects the last server in the list. Then it starts with the first server in the list and continues the selection process until all the servers have been attempted.

You can also specify the authentication type, for admins who belong to specific groups. The NIOS appliance uses the selected group authentication type to query the LDAP server and retrieve the group names to which the admin belongs. In LDAP, you can group users by any custom object classes. Example: objectclass groupofNames, objectclass posixGroup, etc. In NIOS, when you select Member Group Attribute as the group authentication type, the appliance uses custom LDAP group attributes to query the LDAP server and retrieve the group names for authentication. Example: memberOf, isMemberOf, etc. When you select Posix Group as the authentication type, the appliance uses "memberuid" and "objectClass" to query the server and retrieve the group names for authentication.

**Configuring LDAP**

Do the following to configure NIOS to use one or more LDAP server groups to authenticate administrators:

- Configure at least one LDAP authentication server group. For more information, see Configuring an LDAP Server Group.
• Define admin groups for the admins that are authenticated by the LDAP servers and specify their privileges and settings. The group names in NIOS must match the admin group names on the LDAP server. For more information about defining admin groups, see About Admin Groups.

• In the authentication policy, add the LDAP server groups and the admin groups that match those on the LDAP server. You can also designate an admin group as the default group for remote admins. NIOS assigns admins to this group when it does not find a matching group for a remote admin. For more information about configuring the policy, see Defining the Authentication Policy.

Configuring an LDAP Server Group

You can add one or more LDAP servers to an LDAP group for redundancy. The NIOS appliance tries to connect with the LDAP server based on the method you configure for the authentication request. If it does not receive a response within the configured timeout period and has tried to connect the specified retry value, then it tries the next LDAP server on the list. The appliance makes a syslog entry when it fails to connect to any of the servers in the group and sends an SNMP trap and an email notification if configured.

To configure an LDAP server group on the NIOS appliance:

1. From the Administration tab, click the Authentication Server Groups tab.
2. Click the Add icon in the LDAP Services subtab.
3. In the Add LDAP Authentication Service wizard, complete the following:

• Name: Enter the name of the server group.

• LDAP Servers: Click the Add icon and enter the following:
  • Server Name or IP Address: Enter the FQDN (fully-qualified domain name) of the server or enter the IPv4/IPv6 address.
  • LDAP Version: Select the LDAP version. The NIOS appliance supports both LDAPv2 and LDAPv3. The default LDAP version is v3.
  • Base DN: Enter the base DN (Distinguished Name) value. All entries stored in an LDAP directory have a unique DN.
  • Authentication Type: Select the authentication type from the drop-down list. The supported authenticated types are as follows:
    • Anonymous: Select this to connect to the LDAP server anonymously. This is selected by default.
    • Authenticated: Select this to connect using the bind DN and bind password defined for that server.
      • Bind User DN: Enter the bind user DN.
      • Bind Password: Enter the bind password.
  • Encryption: Select the encryption type from the drop-down list.
    • SSL: This is selected by default. All the network traffic is encrypted through an SSL (Secure Sockets Layer) protocol. The appliance automatically updates the authentication port to 636 for SSL. You must upload a CA certificate that verifies the LDAP server certificate. Click CA Certificates to upload the certificate. In the CA Certificates dialog box, click the Add icon, and then navigate to the certificate to upload it.
    • NONE: Select this to unencrypt the connection. Note that Infoblox strongly recommends that you select the SSL option to ensure the security of all communications between the server and the member.
  • Network Port: Enter the authentication port number on the LDAP server to which the appliance sends authentication requests. The default value is 389. When you select NONE from the Encryption drop-down list, the appliance automatically updates the authentication port to 389.
  • Comment: Enter useful information about the LDAP server.
  • Connect through Management Interface: Select this so that the NIOS appliance uses the MGMT port for administrator authentication communications with just this LDAP server.

• Disable Server: Select this to disable the LDAP server if, for example, the connection to the server is down and you want to stop the NIOS appliance from trying to connect to this server. You cannot disable the only server in a group if it is already being used by the remote authentication policy.

• Click Test to test the configuration. If the NIOS appliance connects to the LDAP server using the configuration you entered, it displays a message confirming the configuration is valid. If it is unable to connect to the server, the appliance displays a message indicating an error in the configuration.

• Click Add to add the LDAP server to the group.

When you add multiple LDAP servers, the appliance lists the servers in the order you added them. This list also determines the order in which the NIOS appliance attempts to contact an LDAP server. You can move a server up or down the list by selecting it and clicking the up or down arrow. You can also delete a server by selecting it and clicking the Delete icon.

• Server Timeout(s): Specify the number of seconds that the appliance waits for a response from the LDAP server. The default value is 5 seconds.

• Retries: Specify how many times the appliance attempts to contact an authentication LDAP server. The default value is 5.

If you have configured multiple LDAP servers for authentication and the NIOS appliance fails to contact the first server after the last attempt when the appliance could not connect to the LDAP server or when the LDAP server did not send a reply within the configured response timeouts and retry attempts.

• Mode: Specifies the order in which a Grid member connects to an LDAP server.
  • Ordered List: The Grid member always selects the first LDAP server in the list when it sends an authentication request. It queries the next server only when the first server is considered down. This is the default.
  • Round Robin: The Grid member sends the first authentication request to a server chosen randomly in a group. If there is no response from the server, the Grid member selects the next server in the group. Continued attempts are performed sequentially until it selects the last server in the group. Then it starts with the first server in the group and continues the selection process until all the servers have been attempted.

• Recovery Interval: Specify the number of seconds that the appliance waits to recover from the last failed attempt in connecting to an LDAP server. Select the time unit from the drop-down list. The default is 30 seconds. This is the time interval that NIOS waits before it tries to contact the server again since the last attempt when the appliance could not connect to the LDAP server or when the LDAP server did not send a reply within the configured response timeouts and retry attempts.

• Group Authentication Type: Select the group authentication type for LDAP authentication service from the drop-down list. By default, Group Membership Attribute authentication type is selected. When you select Member Group Attribute, you can specify custom LDAP group attribute in the Group Membership Attribute field. For example, memberOf, isMemberOf, etc. The appliance uses this attribute to retrieve the group names to which the admin belongs. When you select Posix Group, the appliance uses "memberuid" and "objectClass" to retrieve the group names to which the admin belongs.

• Group Membership Attribute: Specify the LDAP group attribute (such as "memberOf" and "isMemberOf"). This is used to query the server and retrieve the group names to which the admin belongs. This field is enabled only when you select Member Group Attribute in the Group Authentication Type drop-down list. The default value is memberOf.

• LDAP Search Scope: To search for an admin user name in the LDAP directory, select one of the following LDAP search scope:
  • Base: Specify Base to perform search only on base in the LDAP directory. This is the top level of the LDAP directory.
- **One Level**: Specify One Level to perform search on base DN and one level below the base in the LDAP directory.
- **Subtree**: Specify Sub tree to perform search on base and all the entries below the base DN in the LDAP directory.
  
  The default value is One Level.

- **User ID**: Specify the attribute associated with the user object in the LDAP server, such as "uid" and "cn". This attribute is used to match the NIOS user name.

- **Map LDAP Field to Extensible Attribute (for Captive Portal Users only)**: If you configure the LDAP authentication server group to authenticate the captive portal users, you can map an LDAP attribute value to an existing extensible attribute. This mapping is optional. By doing so, the LDAP attribute value will be queried from the LDAP server once the captive portal user authentication is successful. The attribute value received from the LDAP server is mapped to the corresponding extensible attribute. NIOS updates or creates a MAC address filter depending on the captive portal user or the client's hardware and name.

  Click the Add icon and enter the following:
  
  - **LDAP Field**: Enter the LDAP attribute. This attribute is queried in the LDAP directory server.
  - **Extensible Attributes**: Select an attribute from the drop-down list. The drop-down list displays only the extensible attributes configured with attribute type as string. Infoblox recommends that you avoid confidential data while mapping extensible attribute to an LDAP attribute because this data is visible in the extensible attribute field of the corresponding MAC address filter.

**Note**: Mapping an extensible attribute to an LDAP attribute must be unique for a given LDAP server. Attribute not defined in the LDAP directory for a given user is considered as null and is mapped to the corresponding extensible attribute with a default value. The default value of extensible attribute is Not Found. This default value is not configurable and they do not cause the authentication to fail.

- **Comment**: Enter useful information about the LDAP server group.

- **Disable**: Select this to disable the LDAP authentication server group. Note that you cannot disable an LDAP group if it is already being used to authenticate one or more administrators and/or captive portal users.

4. Save the configuration and click **Restart** if it appears at the top of the screen.