Connecting To An LDAP Server Or Microsoft Active Directory And Azure AD

In production systems it is required that AtScale communicates with an external directory service to authenticate users. This topic describes the steps necessary to configure AtScale to inter-operate with an external directory service such as Microsoft Active Directory or Azure Active Directory.

Before You Begin: Importing A Certificate

If you are connecting AtScale to a secure LDAP server, you must set up a trust chain from the LDAP server to the AtScale node (if you have a single-instance installation of AtScale) or to the nodes in an AtScale cluster. For example, if you are using self-signed certificates, you must follow these steps to copy the LDAP server's self-signed certificate into the Java certificate store on the AtScale node:

For more information, see Configuring TLS.

1. Download the LDAPS Server's certificate.

   You can use this command if you have OpenSSL set up on the LDAPS server: `openssl s_client -connect ldap_server.domain:636`

2. Copy the lines starting from `-----BEGIN CERTIFICATE-----` and ending with `-----END CERTIFICATE-----` into a separate file. The name of this file must have the .cert extension.

   

   AtScale requires a full certificate chain in order to function correctly. The certificates should contain the public portion of the certificate, plus any intermediate CA certificates and root certificates needed to build the chain to the root CA. Failure to do so will result in errors during certificate renewal.

3. On each AtScale Server:

1. Update atscale.yaml file and add the <path to your .cert file> to `tls.custom_crt.path`.

   Alternatively, you can place the <filename>.cert in the `/opt/atscale/data/security/crt` directory. In this case your atscale.yaml entry should be like in the example below:

   ```
   tls:
     certificate: /opt/atscale/conf/server.cert
     enabled: false
     key: /opt/atscale/conf/server.key
     custom_crt:
       path: "/opt/atscale/data/security/crt"
   ```

2. Execute the `configurator.sh` tool with the `--apply` option to apply the new configuration as the Atscale installation user (atscale in this example).

   ```
   su - atscale
   cd /opt/atscale/current
   ./bin/configurator.sh --apply/opt/atscale/current/bin/configurator.sh --apply
   ```

3. Check if the certificate is imported and filename is the alias in the truststore:

   ```
   /opt/atscale/current/pkg/jdk/bin/keytool -list -keystore /opt/atscale/current/security/truststore.jks -alias
   <filename>.cert
   ```

4. Restart AtScale

   1. To stop all AtScale processes, run the following command on the AtScale node (if you have a single-instance installation of AtScale) or on all of the nodes in your AtScale cluster:

      ```
      /opt/atscale/bin/atscale_stop_apps
      ```

   2. To start all AtScale processes, run the following command where you ran the previous command:

      ```
      /opt/atscale/bin/atscale_start_apps
      ```

Azure Ad

If you are connecting AtScale to an Azure AD LDAPS server, you must adhere to the prerequisites found here. After uploading your certificate to the AtScale engine's truststore and enabling LDAPS for your Azure AD Domain Services (DS), the following configurations should be made on the AtScale custom directory service setup page. More information pertaining to the AtScale directory service setup can be found in the Procedure section below.

- Enable **Use SSL** from the Custom Directory Setup page in AtScale when setting up the connection between AtScale and Azure AD.
- The default port for Azure AD LDAPS is **636**. If not conforming to the default port protocols, ensure the port used in your Azure AD configuration matches the port set in AtScale.

About This Task

You must configure a connection to one external directory service for each AtScale organization. Each organization can connect to a different external directory service.

Procedure

1. In Design Center, select **SECURITY > Directory (see left nav section) > SETUP**.
2. Select **Custom Directory** as the type of directory service that you want to connect to.
3. Save a copy of the current configuration by scrolling to the bottom of the page and click the **Download Configuration** button. The browser will save the current configuration to your hard drive.
4. Configure the directory connection and authentication information:

- Name

  An arbitrary label for this connection.

- Hostname

  The external DNS name of the LDAP server.

- Port

  The port that the LDAP server is listening on for client connections. The default LDAP port is 389. The default LDAPS port is 636.

- Use SSL

  Select to encrypt connections between AtScale and the LDAP server. This option requires that AtScale is configured to use SSL. Check your browser address bar when connected to Design Center to see if HTTPS is being used. If not, you will have to configure AtScale to use SSL.

- Directory Username

  The distinguished name (DN) of the LDAP administrative user that AtScale should use to bind to the LDAP directory server. For example: uid=admin,ou=system

- Directory Password

  The password for the LDAP administrative user.

- Synchronize group assignments when users log in

  LDAP users and group assignments are automatically synchronized when they successfully log into AtScale or access a published datasource from client BI software. Additionally, the LDAP administrative user will be synchronized to AtScale after successfully authenticating to the LDAP server.

  Note that some client BI software tools send repeated requests to AtScale to authenticate users who are querying datasources. To decrease the time required to satisfy these repeated requests, AtScale caches the information in the groups-synch cache for a default duration of 30 seconds. If you believe that you need to change this interval, a user with the Organization Administrator role or a superuser may do so from the Organization Settings screen (SETTINGS > ORGANIZATION). Find the **Refresh Rate for the Groups-Synch Cache** option and click the OVERRIDE button to change the setting.

5. Configure the base LDAP schema information:

- Base DN

  Specifies the distinguished name (DN) of the location in the LDAP directory tree from which to search for user and group entries. For example: `dc=ldap,dc=atscale,dc=com`

- Additional User DN

  The additional DN to append to the Base DN for the location of user entries. For example: `cn=users`

  If users are located in multiple locations in your directory, you can separate DNs using double pipes (||). For example: `ou=us_east||ou=us_west||ou=us_central`

- Additional Group DN

  The additional DN to append to the Base DN for the location of group entries. For example: `cn=groups`

6. Configure the user schema information.

   - User Object Classes

     These are the LDAP object classes used to define a user. The default object classes for Active Directory users are `user, top, person, organizationalPerson`.

   - User Object Filter

     An LDAP filter to restrict the search scope for users in the directory tree. For example, to restrict access to users who are members of a specific LDAP group.

   - Proxy User Attribute

     The attribute of user objects that is passed in by BI clients as a proxy user. This setting identifies what user attribute is being passed in by Tableau Server as the proxy user. The PROXY USER ATTRIBUTE should match the attribute sent in by the BI Tool. For example, Tableau Server Impersonation passes in the `sAMAccountName`. Therefore, the PROXY USER ATTRIBUTE should be set to `sAMAccountName`.

   - User Kerberos Principal Attribute

     The LDAP attribute used as the Kerberos Principal. If using Kerberos authentication, users will connect to AtScale using the LDAP value of this attribute. The recommended attribute for Active Directory is `userPrincipalName`.

   - User Unique ID Attribute

The LDAP attribute that specifies the unique user ID. If your data warehouse cluster uses an authentication manager configured to work with LDAP, such as Sentry or Ranger, then set this attribute to the same value used by the cluster's authentication provider. For example, the default attribute used by Sentry is `userPrincipalName` and the default attribute used by Ranger is `sAMAccountName`. If using NTLM authentication you will likely need to set this value to `sAMAccountName`.

- User Name Attribute

  The LDAP attribute that specifies the username. The default attribute for Active Directory is `name`.

- User First Name Atribute

  The LDAP attribute that specifies the user first name (givenName).

- User Last Name Attribute

  The LDAP attribute that specifies the user surname (sn).

- User Display Name Attribute

  The LDAP attribute that specifies the user display name (displayName).

- User Email Attribute

  The LDAP attribute that specifies the user email address (mail).

7. Configure the group schema information.

   - Default Group Memberships

     The default LDAP groups for newly added users (only applies if using the local directory).

   - Group Object Class

     These are the LDAP object classes used to define a group. The default object classes for Active Directory groups are `top, group`.

   - Group Object Filter

     An LDAP filter to restrict the search scope for groups in the directory tree. For example, to restrict to specific groups only.

   - Group Name Attribute

     The LDAP attribute that specifies the group name. The default attribute for Active Directory is `name`.

   - Group Description Attribute

     The LDAP attribute that specifies the group description.

8. Configure the membership schema settings.

   - Group Members Attribute

     The LDAP group attribute that specifies the members of a group; for example, `memberUid`. Select the **Search Group Members By DN** check box if your LDAP server stores the distinguished names of users as the value for group membership. For example, rather than using the user ID `hans@your_company.com`, your server might use `uid=hans@your_company.com,cn=users,dc=ldap,dc=your_company,dc=com`.

   - Search Group Members By Dn

     Search for group members by using the user's DN instead of the User Unique ID.

   - User Membership Attribute (Use the User Membership Attribute)

     The LDAP user attribute that specifies membership in a group; for example, `memberOf`. Group membership is specified by either a group members or user membership attribute (not both). Choose the right attribute depending on your directory service.

   - Use the User Membership Attribute

     Enable if your directory server supports the group membership attribute on the user. By default this is the `memberOf` attribute.

9. Click **Save** and **Test Configuration**.

Known Issues

Directory synchronization fails if there are special characters in the user names. (ATSCALE-16664,ATSCALE-15843)