Connecting To Active Directory That Uses LDAP Channel Binding

In production systems AtScale can communicate with Active Directory to authenticate users. For security reasons, sometimes Active Directory is configured to use channel binding via the LdapEnforceChannelBinding registry setting. Here you can find information how to configure the communication between AtScale and Active Directory in such situations.

There are two main steps, described in the sections below:

1. Create a computer account for AtScale
2. Enable NTLM pass-through authentication

Before You Begin

- Active Directory is already configured to use channel binding. For details, see 2020 LDAP channel binding and LDAP signing requirements for Windows.
- You are familiar with the procedure for creating a computer account in Active Directory. For details, see Create a New Computer Account.
- AtScale is already configured to inter-operate with Microsoft Active Directory. For details, see Connecting to an LDAP Server or Microsoft Active Directory and Azure AD.
- You are familiar with the procedure for modifying the settings of the AtScale engine. For details, see Changing Engine Settings.

Creating A Computer Account For AtScale

Perform the following steps on the Active Directory system:

1. Log in to the system using an account that has the required privileges.
2. Go to Control Panel and choose System and Security > Administrative Tools > Active Directory Users and Computers.
3. In the console tree, right-click Computers and choose New > Computer in the context menu.
4. Enter the computer name for the AtScale system and save your changes.

   You can use any name that is less than 15 characters and meets the naming conventions for Active Directory. For the examples shown in this document, it is assumed that the name is `atscale-node`.

5. Create a password for the computer account:

1. Start PowerShell and execute the following command: `Set-ADAccountPassword -Reset -Identity atscale-node$`

   Note that the computer account name is like the computer name, with '$' character added at the end. In the example here, it is `atscale-node$`.

2. Enter the password.

   For the examples shown in this document, it is assumed that the password is `@scaledummy`.

Remember the computer account name and password you set, you would need them when configuring AtScale.

Enabling NTLM Pass-Through Authentication Via Netlogon

Log in AtScale as administrator, go to Settings > Engine, and configure the following parameters:

- Enable `AUTH.NETLOGON.ENABLED`.

  This is the main parameter for enabling NTLM pass-through via the Netlogon protocol. When enabled, it takes precedence over the `AUTH.NTLM.ENABLED` parameter used for configuring Windows Authentication.

- Set `AUTH.NETLOGON.COMPUTER.NAME` to the computer account created in Active Directory.
- Set `AUTH.NETLOGON.DOMAIN` to the domain name of the Active Directory server.
- Set `AUTH.NETLOGON.DOMAINCONTROLLER` to the hostname (FQDN) of the Active Directory server.
- Set `AUTH.NETLOGON.COMPUTER.PASSWORD` to the password created for the computer account.
- Set `AUTH.NETLOGON.NETBIOS.DOMAIN` to the first part of the domain of the Active Directory server.

Based on sample name and password used when creating the computer account, here is an example for setting the parameters in AtScale:

```
AUTH.NETLOGON.ENABLED = true
AUTH.NETLOGON.COMPUTER.NAME = atscale-node
AUTH.NETLOGON.DOMAIN = mycorptest.infra.atscale.com
AUTH.NETLOGON.DOMAINCONTROLLER = atscalead.mycorptest.infra.atscale.com
AUTH.NETLOGON.COMPUTER.PASSWORD = @scaledummy
AUTH.NETLOGON.NETBIOS.DOMAIN = mycorptest
```

Finally, you need to restart the AtScale engine to apply the parameters. For more information on how to do this on single instance or cluster, see Changing Advanced Engine Settings.

More Information

- Create a New Connection in Excel
- Using AtScale with Microsoft Power BI Desktop

▲ Connecting to AtScale Using Windows Authentication