Configuring Kerberos

You can configure the AtScale Identity Broker to use Kerberos authentication with your LDAP server.

Note: AtScale only supports Kerberos authentication with Microsoft Active Directory.

Before You Begin

Before configuring Kerberos authentication for AtScale, consider the following:

- AtScale supports Kerberos login on HTTP endpoint with SPNEGO token.
- Only client and server tickets issued by Microsoft KDC are supported.
- Tickets issued by MIT KDC are not supported. This means you cannot use a multi-forest setup with a trust enabled between Microsoft AD and MIT KDC.
- Configuring AtScale to use Kerberos for inbound authentication has only been verified to work when using Windows Authentication with Microsoft Excel, Power BI Service, and Power BI Desktop.

Prepare Active Directory And The KDC

First, you need to set up and configure several components in Active Directory (AD) and your key distribution center (KDC).

1. Add a DNS Entry for AtScale:

   In DNS Manager, add a record for the new AtScale instance. There must be an A record, followed by the Reverse Lookup Zone and Entry. For example: `FQDN: kerberos-sso-node-01.pbi.example.com. -> 10.108.4.41`

   You should create the Reverse Lookup Zone before creating the A record so that the record is automatically created for the server.

2. In Active Directory, add a Service User. This will serve and act as an SPN (Service Principal Name).

   - On the **Account** tab, check the **Password never expires** checkbox.
   - AtScale also recommends checking the **This account supports Kerberos AES 256 bit encryption** checkbox in order to use stronger encryption keys for increased security.

3. Create an SPN:

   In the domain controller/KDC, start PowerShell with elevated rights and run the following command:

   `setspn -s <spn>`

   Where `<spn>` is your SPN. For example, `HTTP/kerberos-sso-node-01.pbi.example.com PBI\kerberossso01`.

4. Create a Keytab file:

   In the domain controller/KDC, start PowerShell with elevated rights and run the following command:

   `ktpass -princ '<principal>' -crypto <encryption_mechanisms> -mapuser '<user>' -pass * -out <filename> -ptype KRB5_NT_PRINCIPAL`

   Where:

   - `<principal>` is the FQDN of your Kerbeors principal. For example, `HTTP/kerberos-sso-node-01.pbi.example.com@PBI.EXAMPLE.COM`. Note that the domain name must be in capital letters.
   - `<encryption_mechanisms>` are the encryption mechanisms you want to use. The following are supported: DES-CBC-CRC, DES-CBC-MD5, RC4-HMAC-NT, AES256-SHA1, AES128-SHA1, All. AtScale recommends using strong encryption (AES-128 & AES-256), which is enabled explicitly for the account.
   - `<user>` is the user account to map the principal to.
   - `<filename>` is the name of the keytab file that will be generated.

   For more information, see ktpass documentation.

5. Enter the password when prompted.

Add Active Directory As The User Federation Provider In The Identity Broker

Next, you must add Active Directory as your user federation provider in the AtScale Identity Broker. Complete the steps in Connecting to an LDAP Server, then move on to the next section.

Enable The AtScale Engine To Use Kerberos

Finally, you need to enable the AtScale engine to use Kerberos.

Do the following on the engine container in your cluster:

1. Set the following environment variables:

   - `ATSCALE_ENGINE_AUTH_XMLA_KERBEROS_ENABLED`: Set to `true`.
   - `ATSCALE_ENGINE_AUTH_XMLA_KERBEROS_KEYTAB`: Set to the path to your keytab file.
   - `ATSCALE_ENGINE_AUTH_XMLA_KERBEROS_SPN`: Set to the SPN you created above.

2. Update the `krb5.conf` file to match the Kerberos configuration for your LDAP server.
3. Mount the following files:

- `/app/conf/<keytab_file>` (where `<keytab_file>` is your keytab file)
- `/etc/krb5.conf`