Kerberos Connections To XMLA Endpoints

Here you can find information on how to configure AtScale to use Kerberos for inbound authentication connecting to XMLA endpoints.

Introduction

Consider the following before you start:

- 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 yet supported, thus multi-forest setup with a trust enabled between Microsoft AD and MIT KDC will not work.
- For a clustered setup, the SPN needs to match on the load balancer address.
- 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 Windows AD And KDC

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

1. Add a DNS Entry

   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`

   Note that a Reverse Lookup zone should be created before the creation of the A record. This way, it will automatically create the record for the server.

2. Add Service User in Active Directory:

   - You need to create a service user to serve and act as an SPN (Service Principal Name).
   - In the Account tab, check the Password Never expires checkbox.
   - Checking the This account supports Kerberos AES 256 bit encryption checkbox is strongly recommended in order to use stronger encryption keys for increased security.

3. Create SPN:

   In the Domain controller/KDC, start PowerShell with elevated rights and use this command (replace the SPN with yours):

   ```
   setspn -s HTTP/kerberos-sso-node-01.pbi.example.com PBI\kerberossso01
   ```

4. Create Keytab

   In the Domain controller/KDC, start PowerShell with elevated rights and use this command (replace the Principal, mapuser, and Output parameters with yours):

   ```
   ktpass -princ 'HTTP/kerberos-sso-node-01.pbi.example.com@PBI.EXAMPLE.COM' -crypto {ENCRYPTION_MECHANISM(S)} -mapuser 'PBI\kerberossso01' -pass * -out C:\kerberossso01.keytab -ptype KRB5_NT_PRINCIPAL
   ```

   Note the following:

   - There will be a prompt for the password.
   - AtScale supports and recommends the use of strong (AES-128 & AES-256) encryption, which is enabled explicitly for the account.
   - Supported {ENCRYPTION_MECHANISM(S)} are {DES-CBC-CRC|DES-CBC-MD5|RC4-HMAC-NT|AES256-SHA1|AES128-SHA1|All}
   - When generating the keytab, the domain name must be in capital letters!
   - For more information, see ktpass documentation.

Configuring AtScale

After completing the steps above for AD and KDC, you should perform the following steps in AtScale:

1. Copy the keytab file to the AtScale host.

   It is recommended - but not required - to put the keytab file in /opt/atscale/conf.

2. Go to Settings > Organization Settings > Engine, locate the following settings, and configure them in the following:

   - `auth.xmla.kerberos.enabled` - enable this setting
   - `auth.xmla.kerberos.keytab` - specify the location to the keytab file
   - `auth.xmla.kerberos.spn` - specify the service principal name

3. Save your changes.

More Information

In case you use Power Bi Service, after completing the steps above you can set up Power BI as described in Power BI Service SSO via Inbound Kerberos.