Connect via Linked Server with AAD Auth

Last updated by | Vitor Tomaz | Sep 1, 2022 at 10:20 AM PDT

Contents

Self-help content presented in Azure Portal

(This content was shown to the customer during case submission. It's also visible on 'Diagnose and solve problems' blade.)

Learn how to create a linked server in Managed Instance which connects to Synapse with managed identity Azure AD authentication.

Pre-requisites.

- Verified NSG group of MI's subnet to make sure outbound port 1433 is whitelisted.

- Ensure Synapse networking end allows Azure services.

Below are the steps to create SQL Managed Instance linked server with managed identity Azure AD authentication .

To create a linked server with managed identity authentication, execute the following T-SQL. The authentication method uses ActiveDirectoryMSI in the @provstr parameter. Consider optionally using @locallogin = NULL to allow all local logins.

```
EXEC master.dbo.sp_addlinkedserver
@server     = N'MyLinkedServer',
@srvproduct = N'',
@provider   = N'MSOLEDBSQL',
@provstr    = N'Server=es-t-adp-01-sql.azuresynapse.net,1433; Authentication=ActiveDirectoryMSI;';

EXEC master.dbo.sp_addlinkedsrvlogin
@rmtsrvname = N'MyLinkedServer',
@useself    = N'False',
@locallogin = N'user1@domain1.com';
```

If Azure SQL Managed Instance managed identity (formerly called managed service identity) is added as login to a remote managed instance, then Managed Identity authentication is possible with linked server. Both system assigned and user assigned managed identities are supported.

If primary identity is set, it will be used, otherwise system assigned managed identity will be used. If managed identity is recreated with the same name, login on the remote instance also needs to be recreated, because new managed identity Application ID and Managed Instance service principal SID no longer match. To verify these two values match, convert SID to application ID with following query.
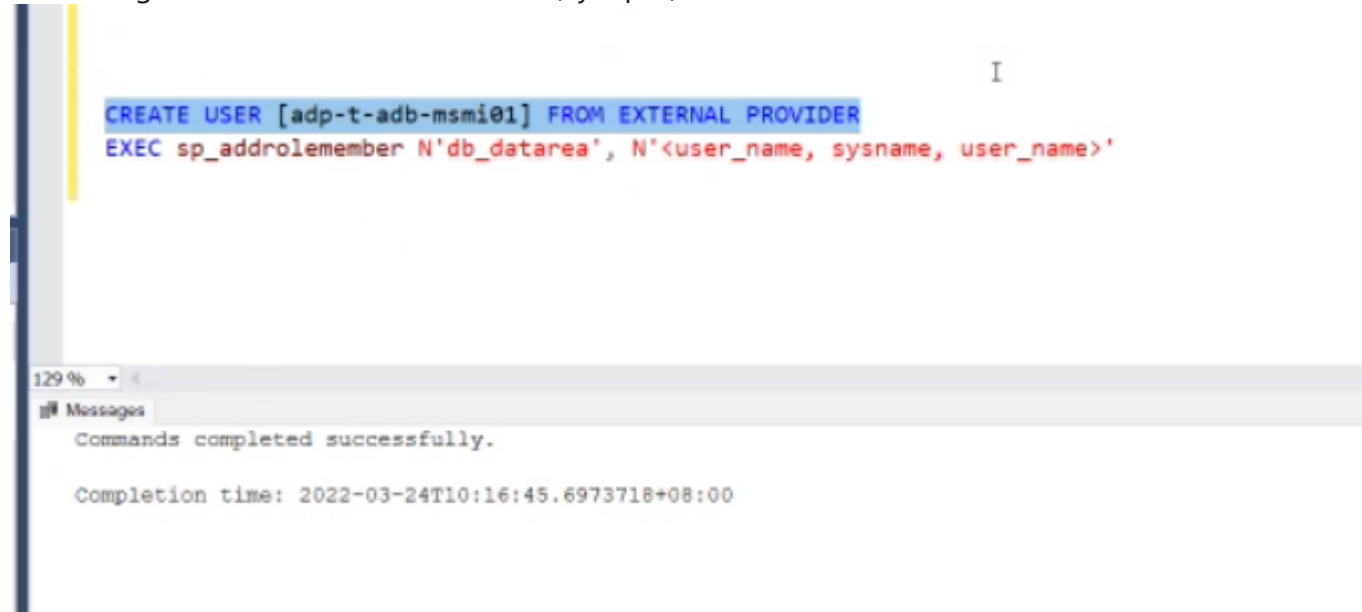
```
SELECT convert(uniqueidentifier, sid) as AADApplicationID
FROM sys.server_principals
WHERE name = '<managed_instance_name>';
```

Test the linked server:

Considering either of the following two approaches to test a linked server's authentication in your current security context.

- To test the ability to connect to a linked server in SSMS, browse to the linked server in Object Explorer, right-click the linked server and then select Test Connection.
- To test the ability to connect to a linked server in T-SQL , execute a simple statement, for example, create the contained user for the Managed Instance MSI on Synapse. This example creates the contained user for

the Managed Instance MSI on the linked (Synapse) server.

Note : Azure SQL Managed Instance lets you directly execute the queries on other Managed Instances, Azure SQL Database, and SQL Servers using linked server technology ⬈.

Resources

- Create linked servers - SQL Server | Microsoft Docs ⬈
- Create SQL Managed Instance linked server with managed identity Azure AD authentication ⬈
- Create SQL Managed Instance linked server with pass-through Azure AD authentication ⬈

How good have you found this content?