How to AAD Security Groups

Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:41 AM PST

Contents

How to configure AAD Security Groups

Follow these steps to use:

1. Customer must sync this security group to AAD.
2. Find the mapping group in AAD,
   a. and use DisplayName field of the group in CREATE USER statement.

- This can be done through Azure portal "Azure Active Directory -> Groups blade" or Azure AD PowerShell command "Get-AzureADGroup".

Customers needs to connect with an Active directory user to be able to create a user for the security group

Then:

To add member to a database role, you can either alter the role or use sp_addrolemember, more information here: https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-addrolemember-transact-sql?view=sql-server-2017

For the full list of Database level Roles: https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles?view=sql-server-2017

Here are some pointers if you come across such cases

- Ask the customer to follow the steps in https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure#_provision-an-azure-active-directory-administrator-for-your-managed-instance

- There are some differences between Managed Instance and SQL DB in AAD space and the major one is - MI requires that user explicitly you have grants read permissions on active directory to the managed instance. Granting this permission can only be done by "Global Admin" type of AAD user

- If they have not granted this, they will see an error like below:
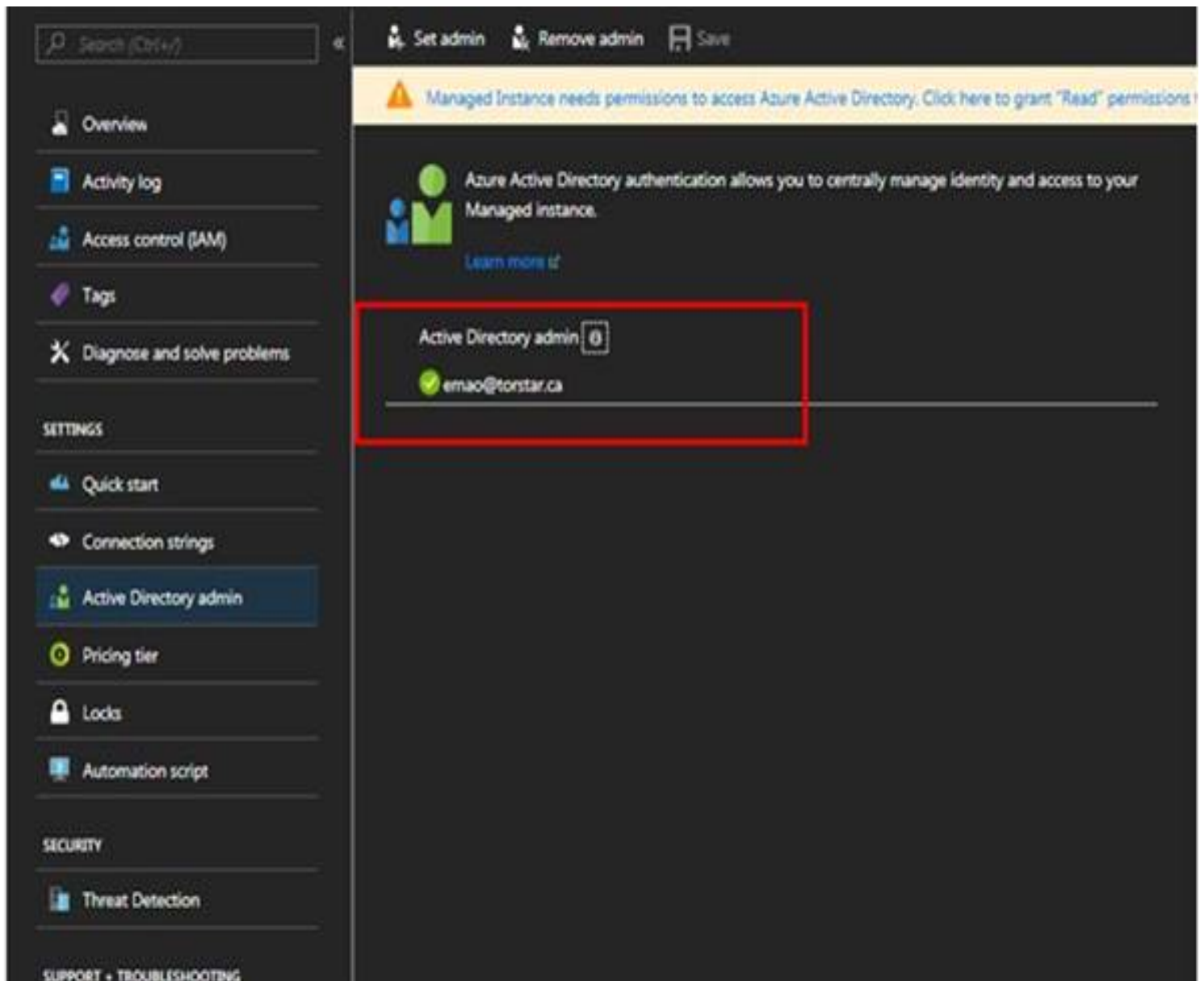
This is documented in our onenote here -
[How to configure AAD Auth to connect Managed Instance](#)   ([Web view](#))

We still have known issue using AD group in master 4/10

How good have you found this content?