Security in Azure SQL database

Azure SQL database provides the proactive security using

1. Dynamic data masking
2. Automated auditing
3. Threat detection

Access control:

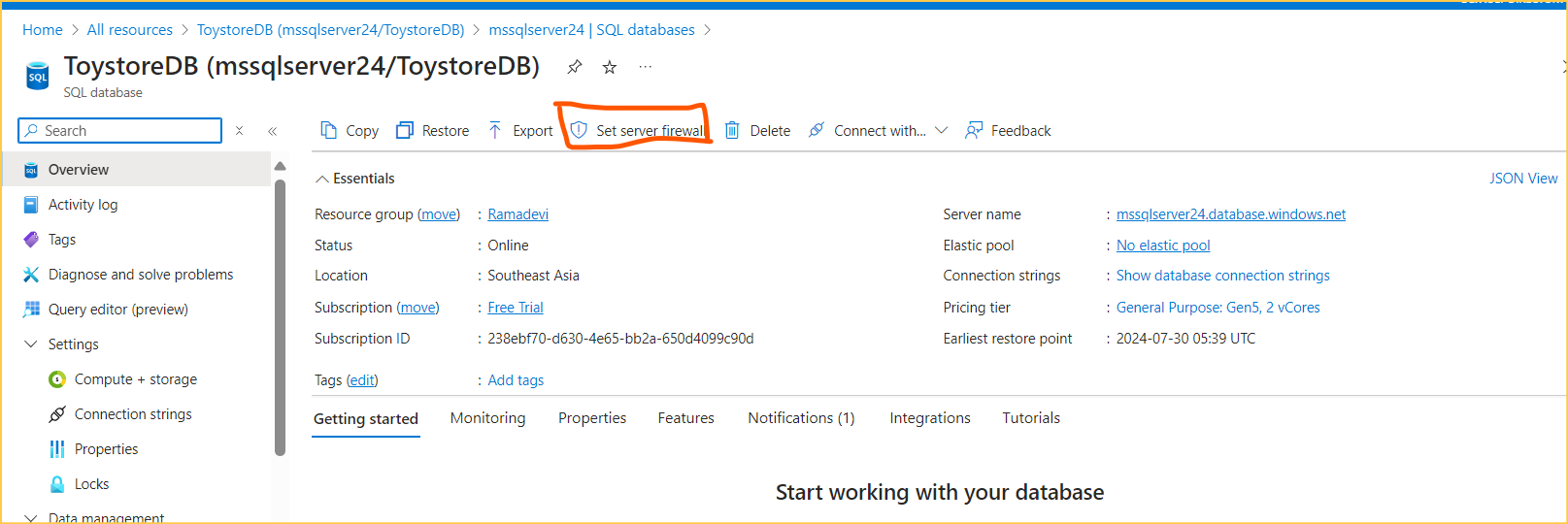
Access control methods

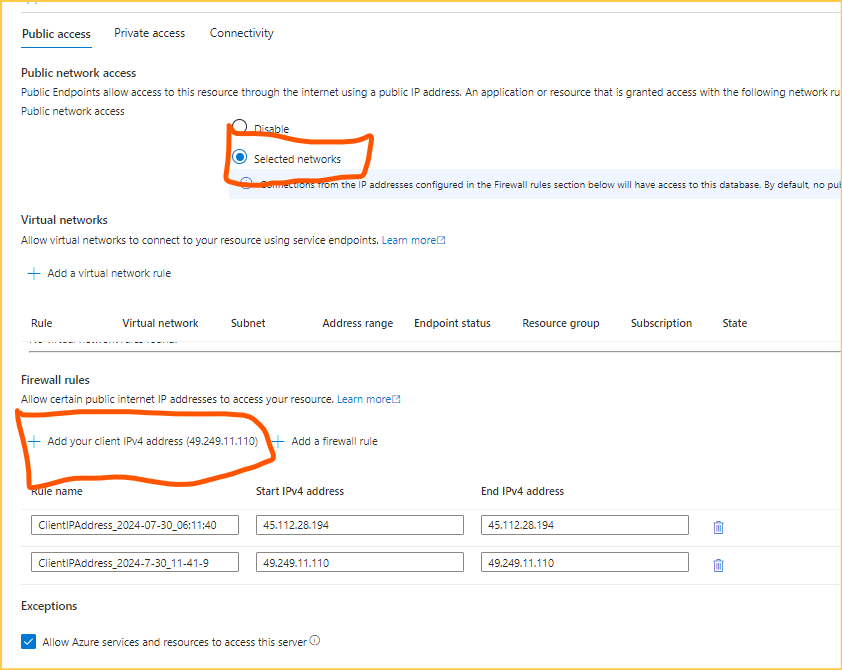
Firewall rules:

* It limits the access to IP address or range of IP address
* Firewall connection will be at database level and server level
* When we want to connect to the server or database, we need access to the database and server

Database level firewall connection:

* Select the database to set the firewall from the Azure portal
* Select set server firewall

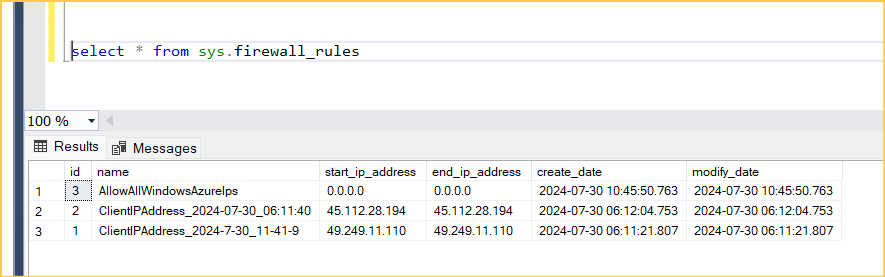




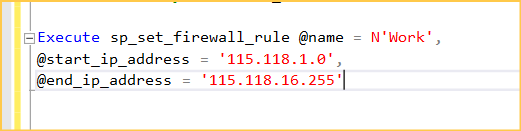
* Click save

**Server level firewall using T SQL**

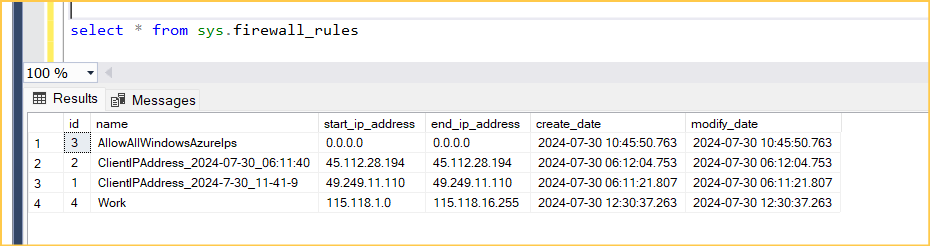
**Run the query to list all the firewall rules**



We can set new firewall rule using fallowing Query

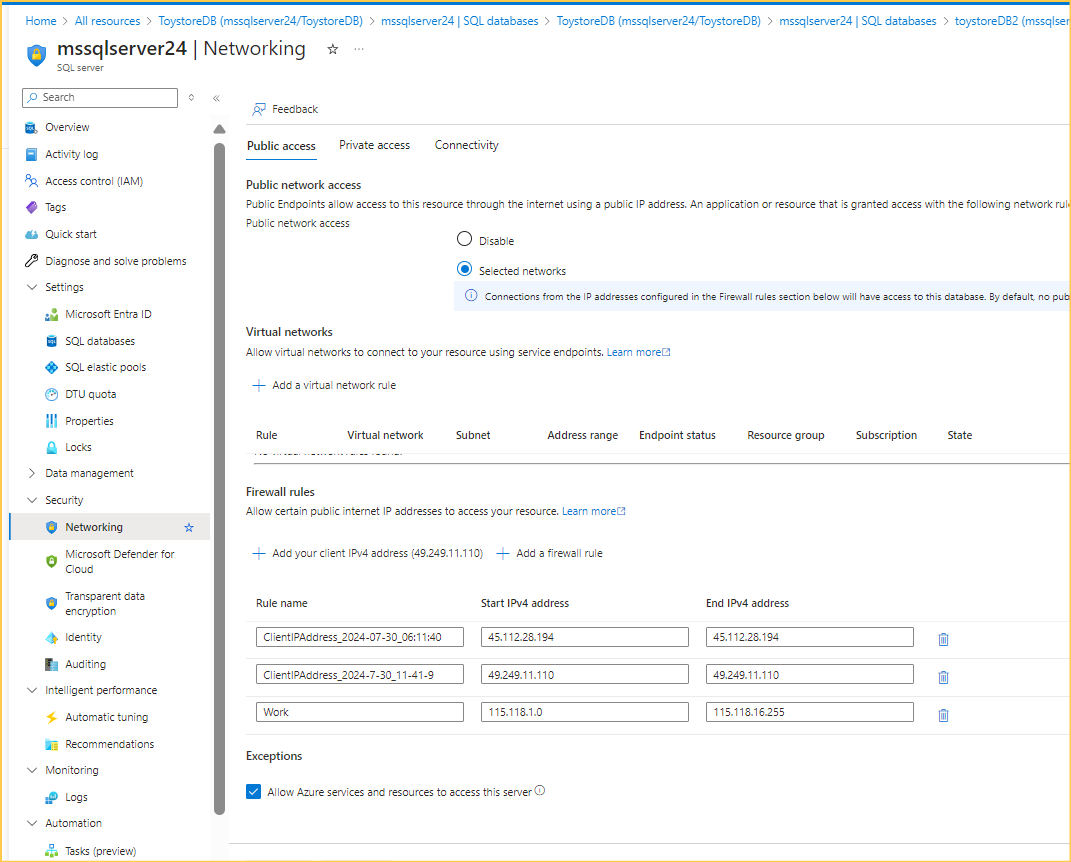


Verify the rule is added or not

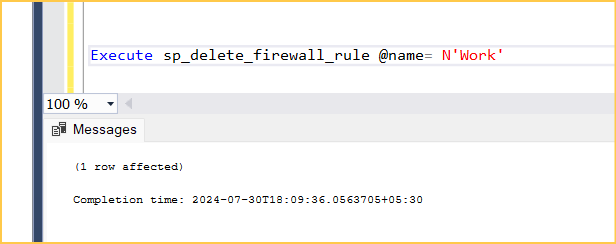
New firewall rule is added

Verify in Azure portal

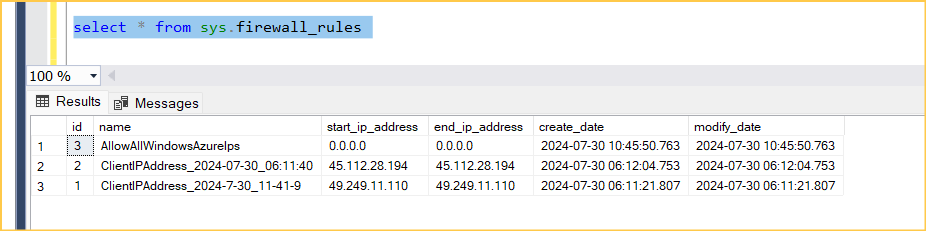
* Select the server----> select networking under the security---> New firewall rule is added



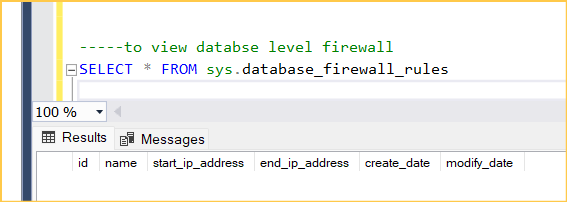
* We can delete the firewall rule using the below query

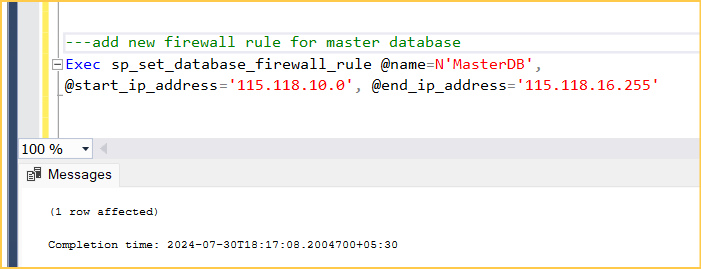


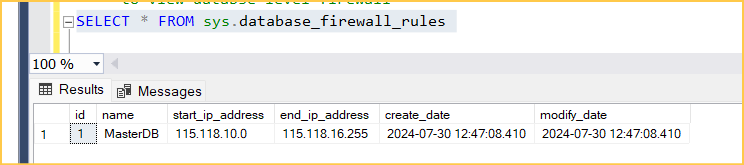
* Verify

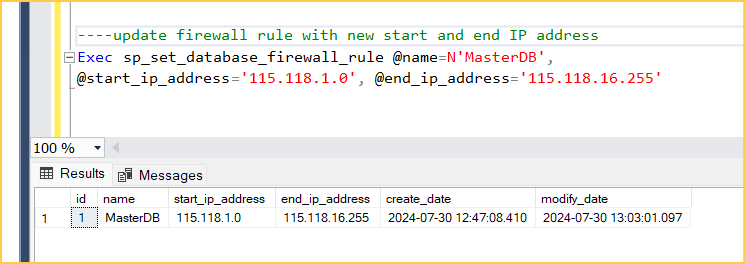


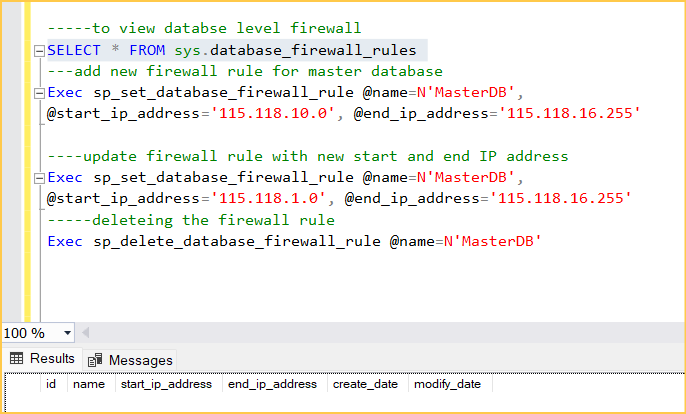
**Database level firewall using T-SQL**



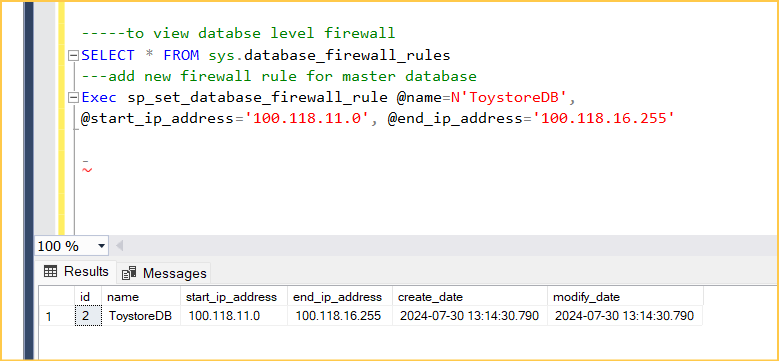








* Adding the firewall to user defined databases



Authentication:

Two types of authentication mechanism

* SQL server authentication
* Microsoft Entra ID

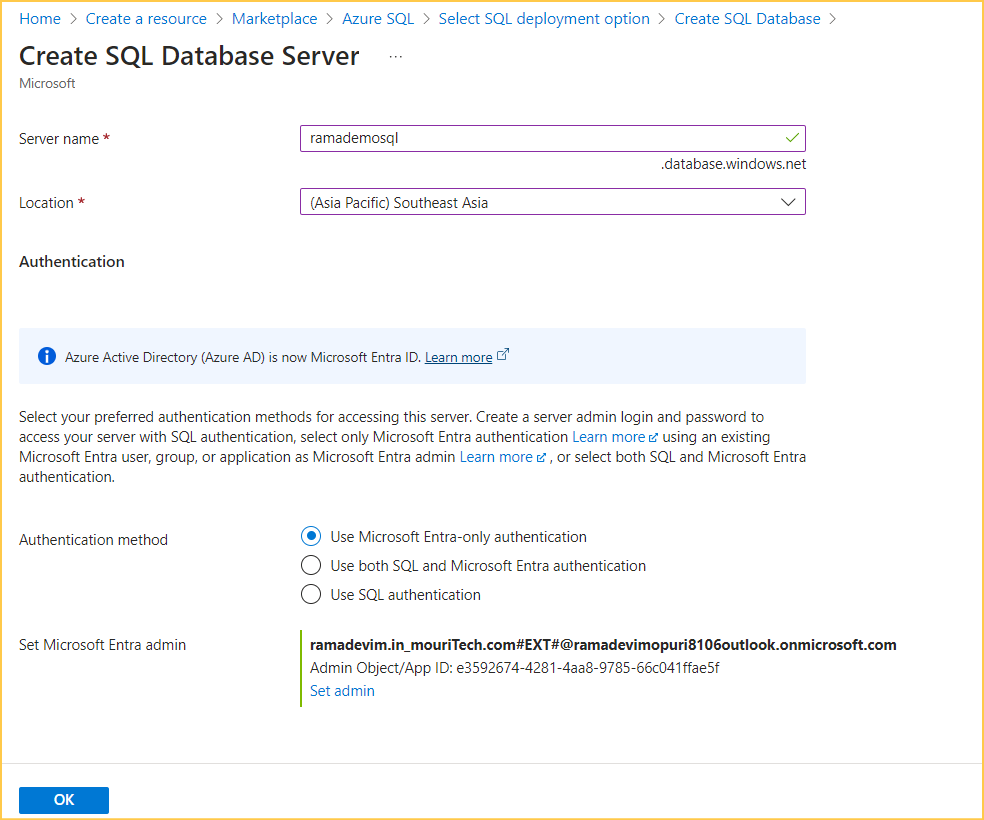
SQL server authentication (more friendly)

* It is like on premise SQL server connection
* Username and password

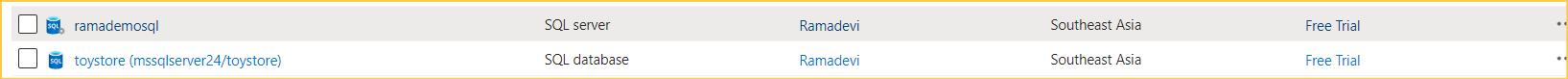
Microsoft Entra ID:(more secure)

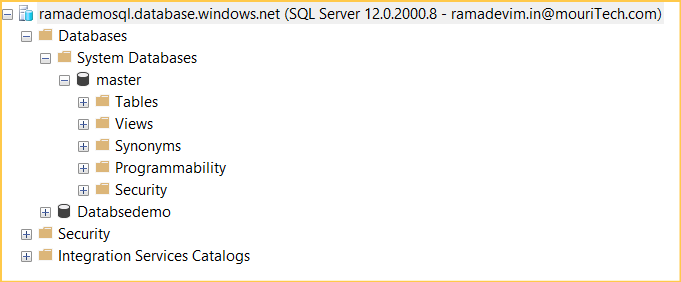
* Microsoft Entra ID was previously known as Azure Active Directory (Azure AD).
* It has the different ways to authenticate
* Microsoft Entra MFA
* Microsoft Entra password
* Microsoft Entra integrated
* Microsoft Entra default
* Microsoft Entra managed identity
* Microsoft Entra server principals

Create a SQL server with Microsoft Entra id authentication



Server is created with the Microsoft Entra id authentication

Now we can connect with to SSMS



**Microsoft Entra password**

**Creating the user in the Microsoft Entra id**

Authorization

* Authorization refers to the object-level permission a user has within a SQL database.

Server lever administrative roles

There are two roles

* Database creator
* Login manager

Database creator

In security we have

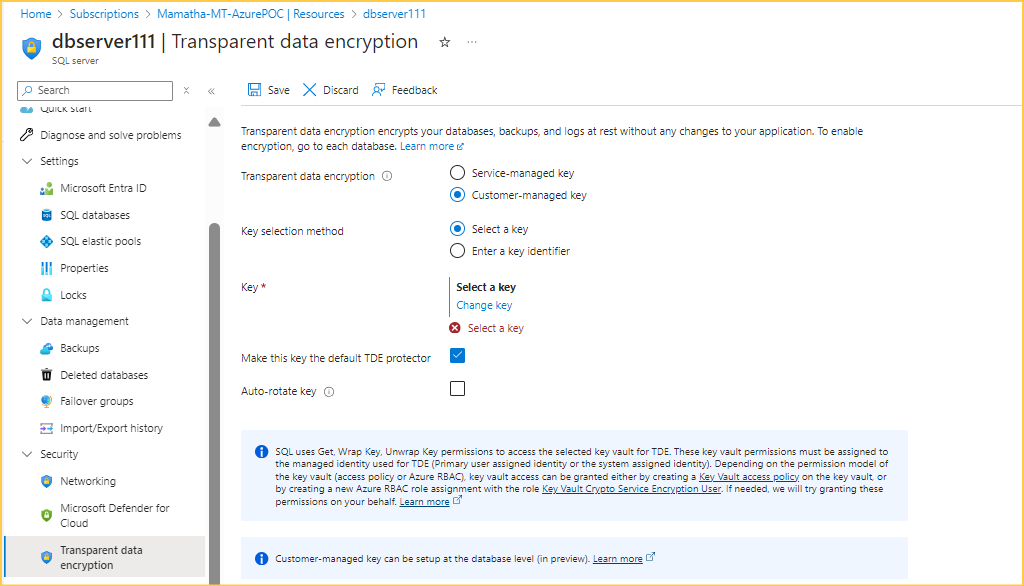
1. Network security
2. Identity and access management
3. Data protection
4. Security management

Data encryption

Dynamic data masking  
set up and configure data protection

Configure TDE:

Azure portal---->security---->TDE--->



Transparent data encryption at server level we have

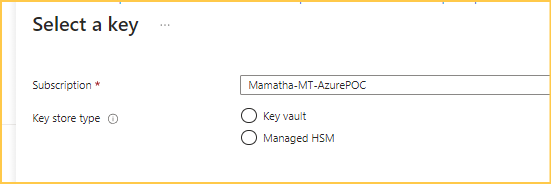
* Service managed key
* Customer managed key

### **Key Differences**

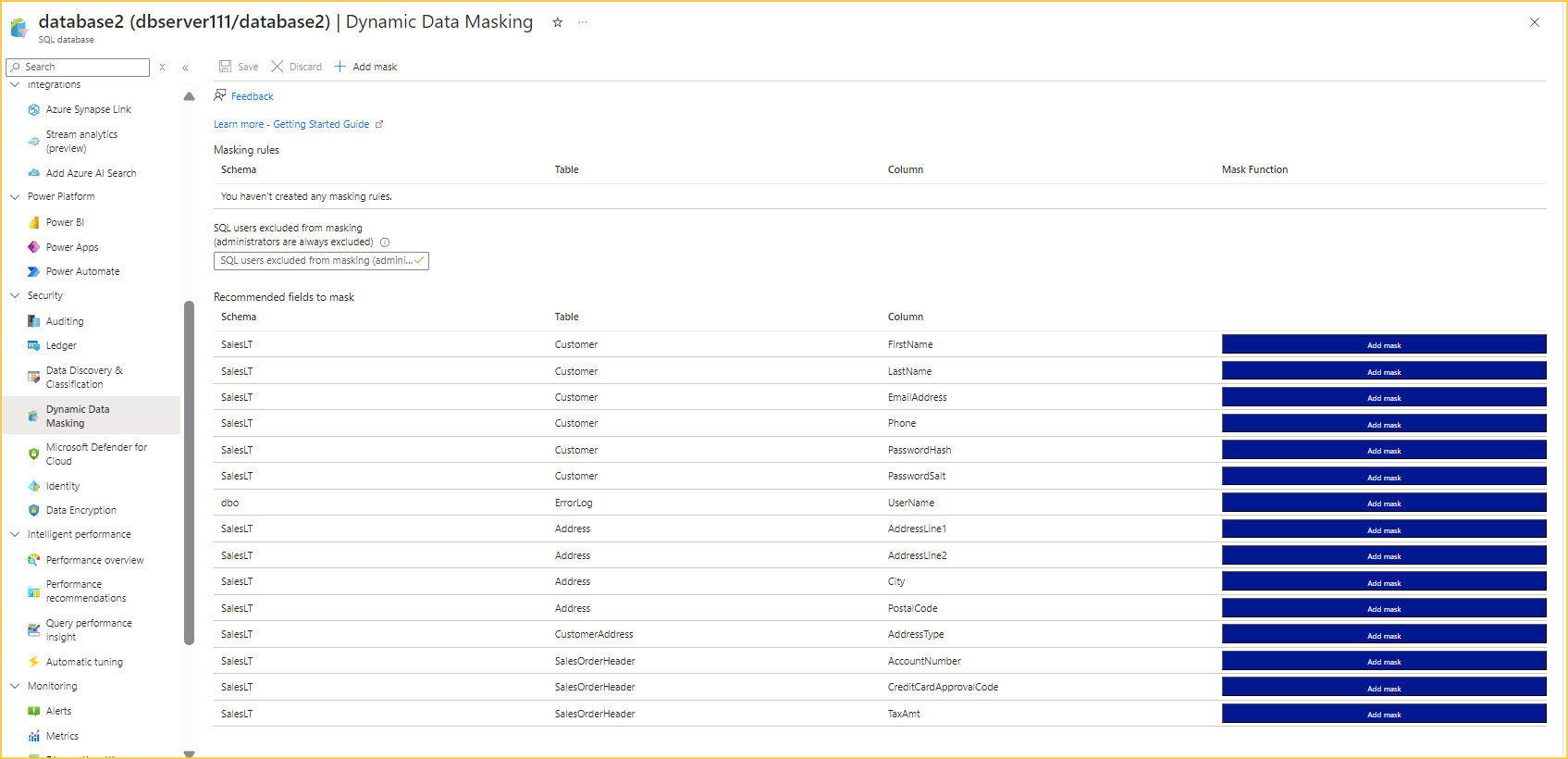
|  |  |  |
| --- | --- | --- |
| **Feature** | **Service Managed Key (SMK)** | **Customer Managed Key (CMK)** |
| **Control** | Managed by the service provider | Managed by the customer |
| **Setup Complexity** | Low | Higher, with more configuration needed |
| **Compliance** | May not meet strict compliance needs | Can meet stringent compliance standards |
| **Key Rotation** | Handled automatically by provider | Customer-defined policies and schedules |
| **Use Cases** | General purpose, low to moderate security | High security, compliance-driven |
| **Access Revocation** | Limited to service provider policies | Full control over revocation |

Customer managed key

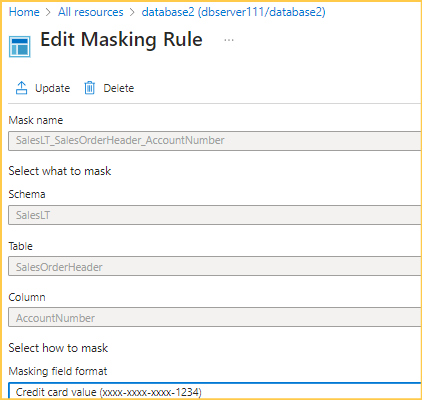
We must create a key



Dynamic data masking



Add mask to the column



Microsoft Entra id

* Create a user in Microsoft Entra ID
* Only create a user and assign any authorization he can't be able to access the anything inside the account
* We need to assign roles to user

Resources trying to ech other