Unable to create Vnet firewall rule

Last updated by | Ahmed Mahmoud | Nov 2, 2022 at 4:29 AM PDT

Unable to create Vnet firewall rule

Issue 1

When adding a virtual network rule to allow '**enxtwe-bnet216**/ 10.130.5.96/28',got an error: {'error':{'code':'OperationCancelled','message':'The operation has been cancelled by user.'}}

Kusto showed the cancelation right after the submission and Network resource provider returned following error:

'Subnets **enxtwe-bnet109** of virtual network /subscriptions/*SubscriptionId*/resourceGroups/enxt-rg001/providers/Microsoft.Network/virtualNetworks/enxtwe-vnet001 do not have ServiceEndpoints for Microsoft.Sql resources configured. Add Microsoft.Sql to subnet's ServiceEndpoints collection before trying to ACL Microsoft.Sql resources to these subnets.'

Cause

To successfully add Vnet firewall rule, you need to have service endpoints enabled on all subnets that have VNET firewall rules added to them and IgnoreMissingServiceEndpoint is not true. You do not need service endpoints enabled on all subnets. You will only have to enable SE on those subnets that had the VNET firewall rules on them.
Revision from case #118101225002342

Internal Reference

https://portal.microsofticm.com/imp/v3/v3/incidents/details/79528783/home ⧉

Issue 2

When trying to configure a new Vnet endpoint on the Azure SQL Server customer got this error:
Failed to update vnet rules for server: <servername>. ErrorCode: 502 ErrorMessage: Azure SQL Server Virtual

Network Rule encountered permission error: The client 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx' with object id 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx' **does not have authorization to perform action** 'Microsoft.Network/virtualNetworks/taggedTrafficConsumers/validate/action' over scope '/subscriptions/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/<RGname>/providers/Microsoft.Network/virtualNetworks/<VNetname>/taggedTrafficConsumers/Microsoft.SQL'.

or

Failed to update vnet rules for server: <servername>. **ErrorCode: 500 ErrorMessage: Gateway authentication failed for 'Microsoft.Sql'**. Diagnostic information: timestamp '20220526T100442Z', tracking id 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx', request correlation id 'xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxx'.

The error message is about not having authorization.
The Azure SQL Server was located on one subscription and the Vnet was located on another subscription
The customer was the owner of both subscriptions
Both Azure SQL Server and Vnet were on the same region
All the requirements documented were met.

Cause

The root cause was that the subscription where the Vnet was located didn't had the provider Microsoft.Sql registered.
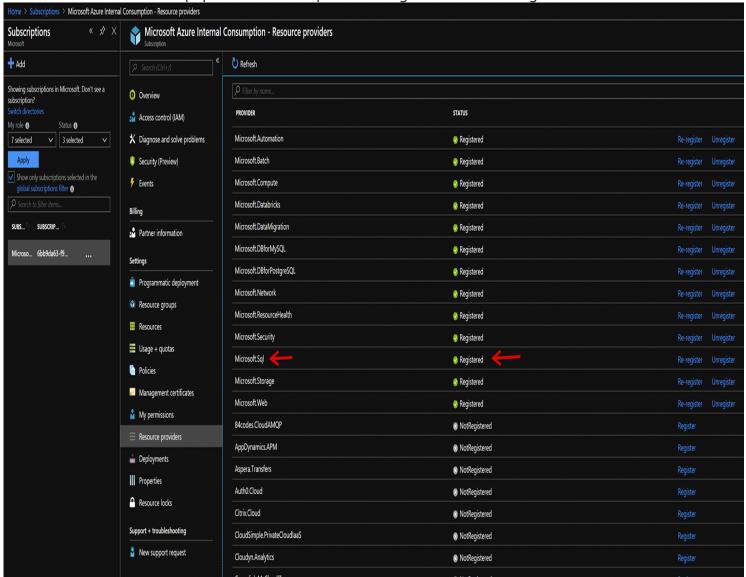
Mitigation

Register the Microsoft.Sql provider on the subscription where the Vnet was located.
We can register the provider using the Azure portal or using powershell.

Using the Azure portal
Go to "Subscriptions" and then on the "Resource providers" we will see the list of providers.

Search for the "Microsoft.Sql" provider and the press the "register" link on the right.

Using powershell
Read in more detail on this article: https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-supported-services ⧉ Read more at https://docs.microsoft.com/en-us/azure/azure-sql/database/vnet-service-endpoint-rule-overview?view=azuresql#azure-rbac-alternative ⧉

Classification

Root Cause: Azure SQL DB v2\Connectivity\Login Errors\Firewall errors and misconfigurations

How good have you found this content?

🙂 🙁