VNET - SQL DB System Tables with VNET metadata

Last updated by | Vitor Tomaz | Aug 5, 2020 at 12:40 PM PDT

SQL VNET Firewall Table

sys.vnet_firewall_rules_table

This sys table will contain the list of server-level rules and will be created on Logical Master. This data will not be available for customers to see on their databases.

Note: For current iteration (Argon/Potassium), the Subnet ID/Name is required to be present although it is planned in the future to be optional. To avoid changing the schema of this table in the future, subnet_id column will be left Nullable while the enforcement of subnet_id existence will be applied on the creation API.

name	Data type	Description
id	**INT**	**The identifier of the server-level firewall setting.**
name	**NVARCHAR(128)**	**The name you chose to describe and distinguish the server-level firewall setting.**
gre_key	**INT**	**(Internal) 32 bit VNET Traffic tag used to identify allowed vnet and compare against incoming connections.**
subnet_id	**INT NULLABLE**	**(Internal) 16 bit Subnet traffic tag used to identify allowed specific subnet id and compare against incoming connections.**
create_date	**DATETIME**	**UTC date and time when the server-level firewall setting was created.**
modify_date	**DATETIME**	**UTC date and time when the server-level firewall setting was last modified.**

SQL new special stored procedures

1. sp_set_vnet_firewall_rule

This spec proc will be used to add entries into the server-level table.

Note: this spec proc execution permissions should only be granted to system to preserve Separation of Roles [Use case 2].

Currently, IPv4 Firewall rules are limited to a non-configurable 128 rules per Logical Server. VNET Firewall Rules will start with the same **configurable** limit controlled by a SQL Server config value (controlled by us, not

exposed to customer).

Due to the Login Cache, increasing the maximum number of firewall rules has memory usage side-effects on SQL user databases, if this limit increases we should be mindful of different SLO limitations.

Parameters:

Name	Datatype	Description
[@name =] *'name'*	NVARCHAR(128)	The name used to describe and distinguish the server-level firewall setting.
[@gre_key =] *'gre_key'*	INT	32 bit VNET Traffic tag used to identify allowed vnet and compare against incoming connections.
[@subnet_id =] *'subnet_id'*	INT	**(Optional)** 16 bit Subnet traffic tag used to identify allowed specific subnet id and compare against incoming connections.

1. sp_delete_vnet_firewall_rule [DM3] [JP4]

This spec proc will be used to remove entries from the Server-level VNET Firewall Rules list. Also requires sysadmin permissions.

The argument of this spec proc is the name of the rule to be deleted: [@name =] '*name*'.

How good have you found this content?