SQL Access with Managed VNET and Private Endpoint

Last updated by | Veena Pachauri | Mar 8, 2023 at 10:57 PM PST

Issue Description

This specific troubleshoot is based on the tutorial presented in:

https://docs.microsoft.com/en-us/azure/data-factory/tutorial-managed-virtual-network-sql-managed-instance ⊡

On the particular scenario that generated this TSG, the customer was able to reach SQL private endpoint. However, 2 weeks ago, for costs reason, customer shutdown the VMs behind the load balancer and, when he restarted the service, the TCP flow to the SQL server was not possible anymore.

Note on this TSG that a collab for Linux can be required to help with this configuration update.

Resolution

We have investigated the issue and we concluded that the root cause was related with the script below:

```
sudo ./ip_fwd.sh -i eth0 -f 1433 -a <FQDN/IP> -b 1433
```

The script works fine: it builds the IP tables and activates the IP forwarding in the Kernel. However, it is not solid enough because if the VMs behind the load balancer are stopped, the configuration is lost and the customer **needs to rerun the script again**. We managed to solve this problem by making the iptables persistent in linux Debian and Red Hat distributions. Actually the customer had two VMs, each one with its own distribution type. Besides none of the distribution brings the iptables-persistent module. We will need to install it on the server with customer approval.

Two steps are required, one regarding the Iptables, and another regarding the ip forwarding, as you can see next:

Regarding Iptables:

a) For Debian Linux Distributions (Ubuntu), type deb, we followed the procedure below:

1. lsb_release -a – get the ubuntu version
2. wget http://archive.ubuntu.com/ubuntu/pool/universe/i/iptables-persistent/iptables-persistent_1.0.4+nmu2_all.deb ⊡ – get the deb SW for iptables persistency
3. sudo apt-get update – update the repository
4. sudo apt-get install iptables-persistent – install the iptables-persistent SW
5. backup copy iptables-save > /etc/iptables/rules.v4 ip6tables-save > /etc/iptables/rules.v6
6. service iptables-persistent start

b) For Fedora Linux Distributions (Redhat 7.x), type deb, we followed the procedure below:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-setting_and_controlling_ip_sets_using_iptables ⊡

In this case, the service firewall must be disabled.

Regarding ip forwarding:

The ip_fwd.sh contains the following bash function:

```
#2. Make sure IP Forwarding is enabled in the kernel
echo -e "\e[32mEnabling IP forwarding...\e[0m"
echo "1" > /proc/sys/net/ipv4/ip_forward
```

Again, this means that the ip forwarding is enabled until the next reboot.

a) For Debian Linux Distributions (Ubuntu), type deb, we followed the procedure below:

1. Edit the following file: vi /etc/sysctl.conf
2. Add the following line : net.ipv4.ip_forward = 1
3. Save and close the file. Apply the changes: sysctl -p

b) For Fedora Linux Distributions (Redhat 7.x), type deb, we followed the procedure below: Please see link: https://rhel7tutorial.wordpress.com/how-to-enable-ip-forwarding/ ⊡

Acknowledgements: A special thank you to Joao Camilo joao.camilo for his work on this TSG.