**Azure Network Watcher**

Network Watcher is designed to monitor and repair the network health of IaaS (Infrastructure-as-a-Service) products which includes Virtual Machines, Virtual Networks, Application Gateways, Load balancers, etc

Tools:

1) **connection monitor**

* it provides unified end-to-end connection monitoring in azure network watcher
* it supports both azure and hybrid setup
* it can be used to get better visibility into network performance.
* it support connectivity checks based on http, tcp, icmp

**2) IP flow verify - detect traffic filtering problem**

* this tool cab be used to check if packet is allowed or denied access to or from a virtual machine
* it can be used to check the packet flow based on protocol (tcp, udp), local / remote ip address and port number
* this tool basically looks at the rules in network security group assigned to the subnet or the virtual machine nic.
* this tool checks and confirms whether a rule in nsg is blocking ingress or egress traffic to or from a virtual machine

**3) next hop - detect virtual machine routing problem**

* this tool is used to check the traffic is being sent to the destination based on routes associated with the nic
* you will get the next hop type, ip address and route table is used to route traffic
* it can be used to check whether traffic is being routed to the intended destination

**4) connection troubleshoot - diagnose connectivity**

* this tool can be used to check the connectivity between virtual machine or from a virtual machine to fqdn, url.
* this tool can be used to give insight into connectivity issue based on nsg and firewall on the virtual machine

**5) vpn troubleshoot**

* this tool can be used to check the connectivity between on-premise and other virtual network in azure

**6) packet capture**

* this can be used to capture the traffic to and from a virtual machine

**7) network security group logging**

* this tool provides more information on the ingress and egress ip traffic flow via nsg
* all the logs are written in json format

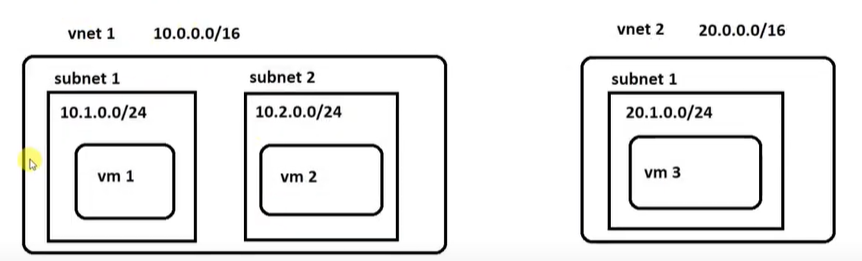
**8) traffic analysis**

* this provides visibility into the user and application activity
* this tool analyzes the nsg flow logs

**IP Flow Verify:**

It checks packet which come to VM and go outside from VM check it is allow or deny through NSG

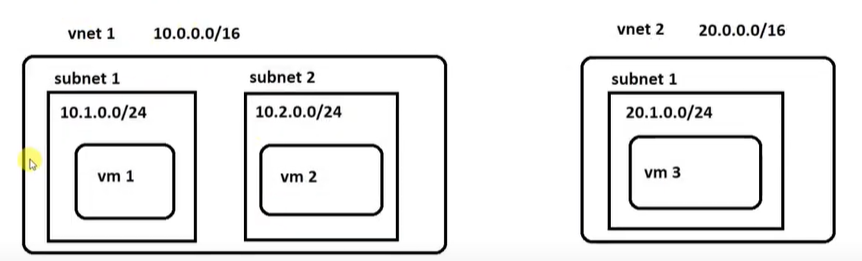
Setup this scenario



* search for network watcher
* go to ip flow verify
* choose subscription
* choose RG
* select VM
* choose protocol and direction
* add local ip address and port
* add remote ip and port

it will check this port is allow ot not

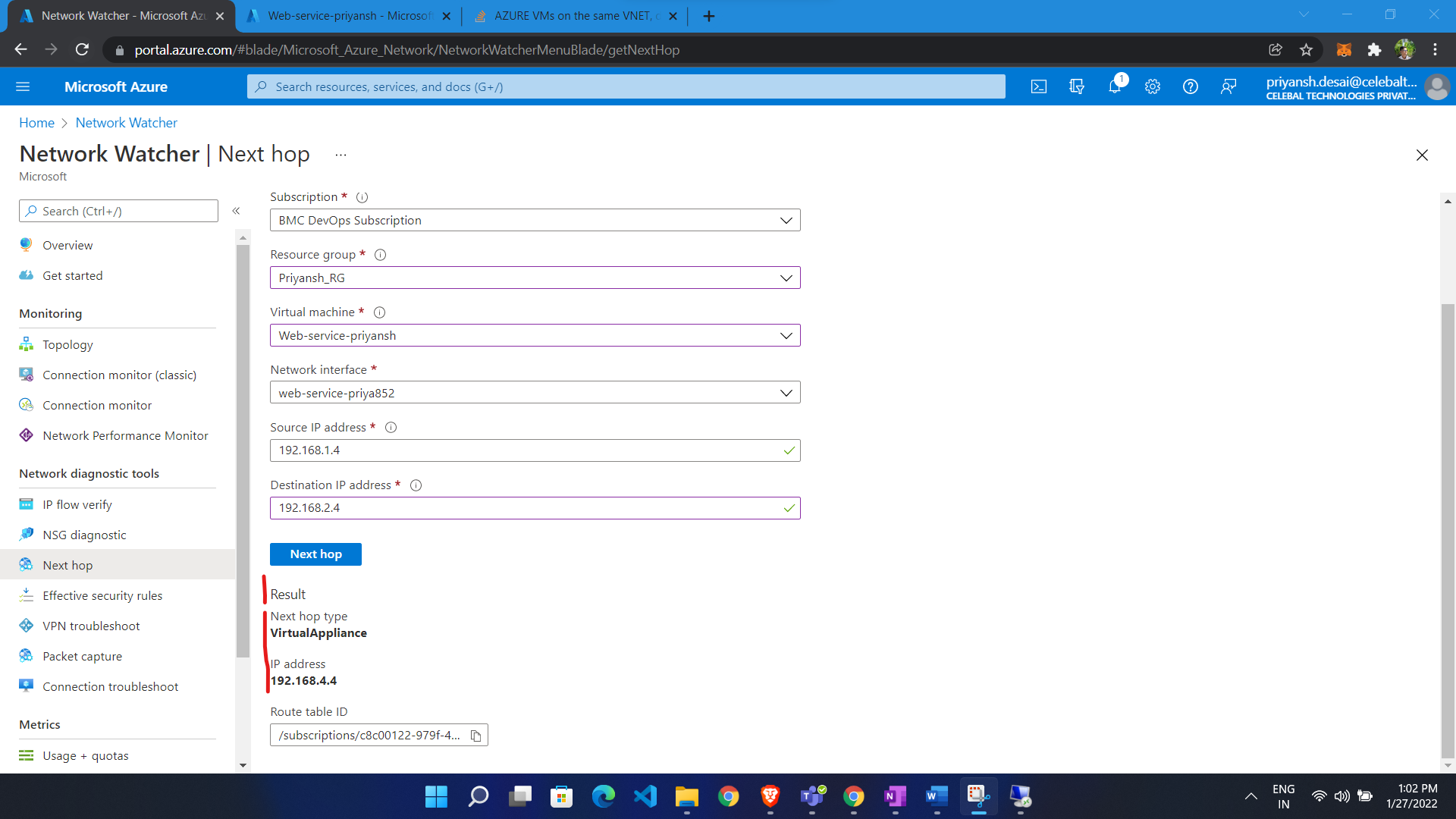
**Next hope:**



If we add firewall rule between VM1 and VM2 then traffic go from VM1 to VM2 is via firewall rule

So fo VM1 next hope is firewall

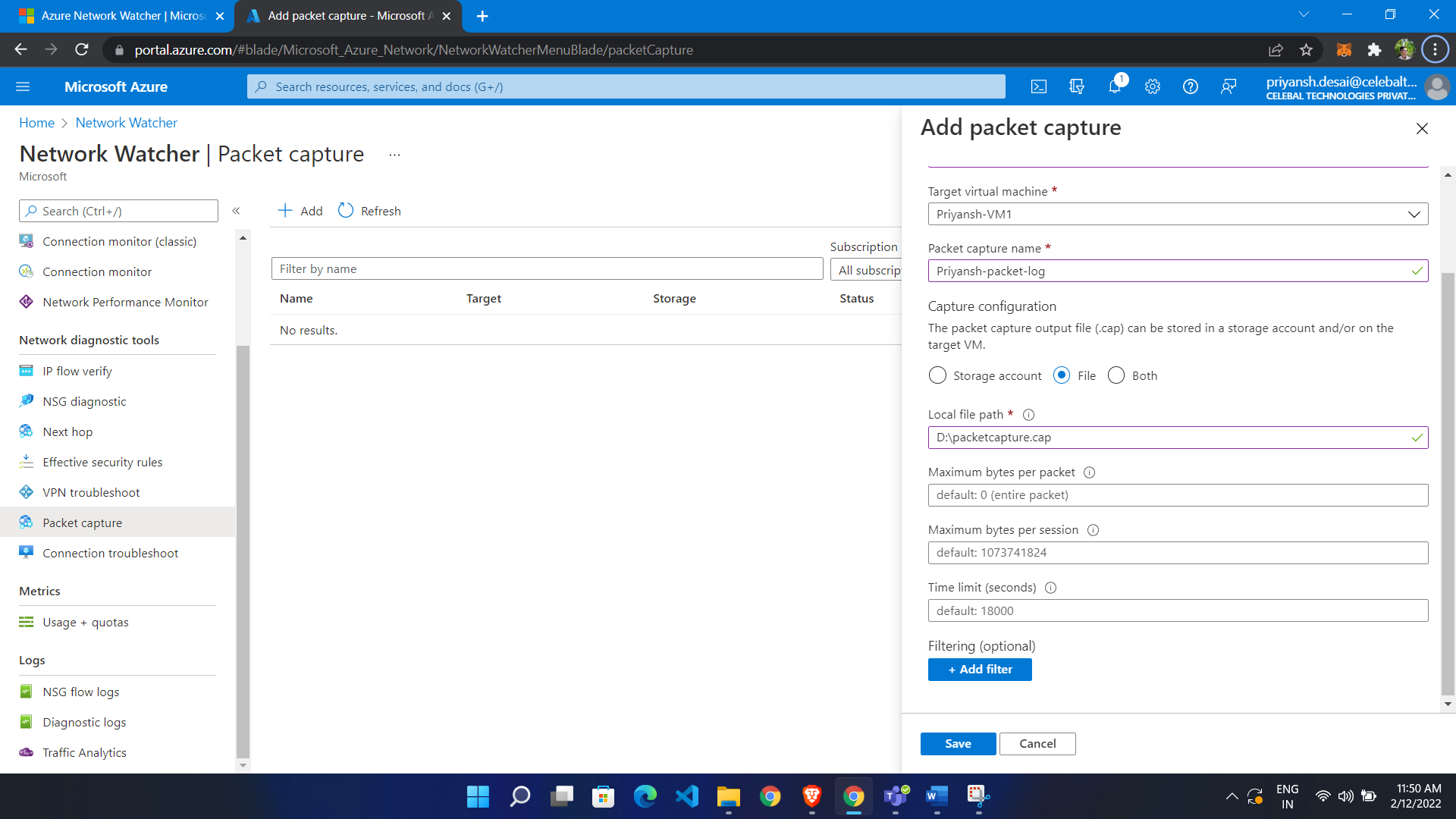
* Select resource group
* Virtual machine
* Network interface
* Source ip
* Destination ip

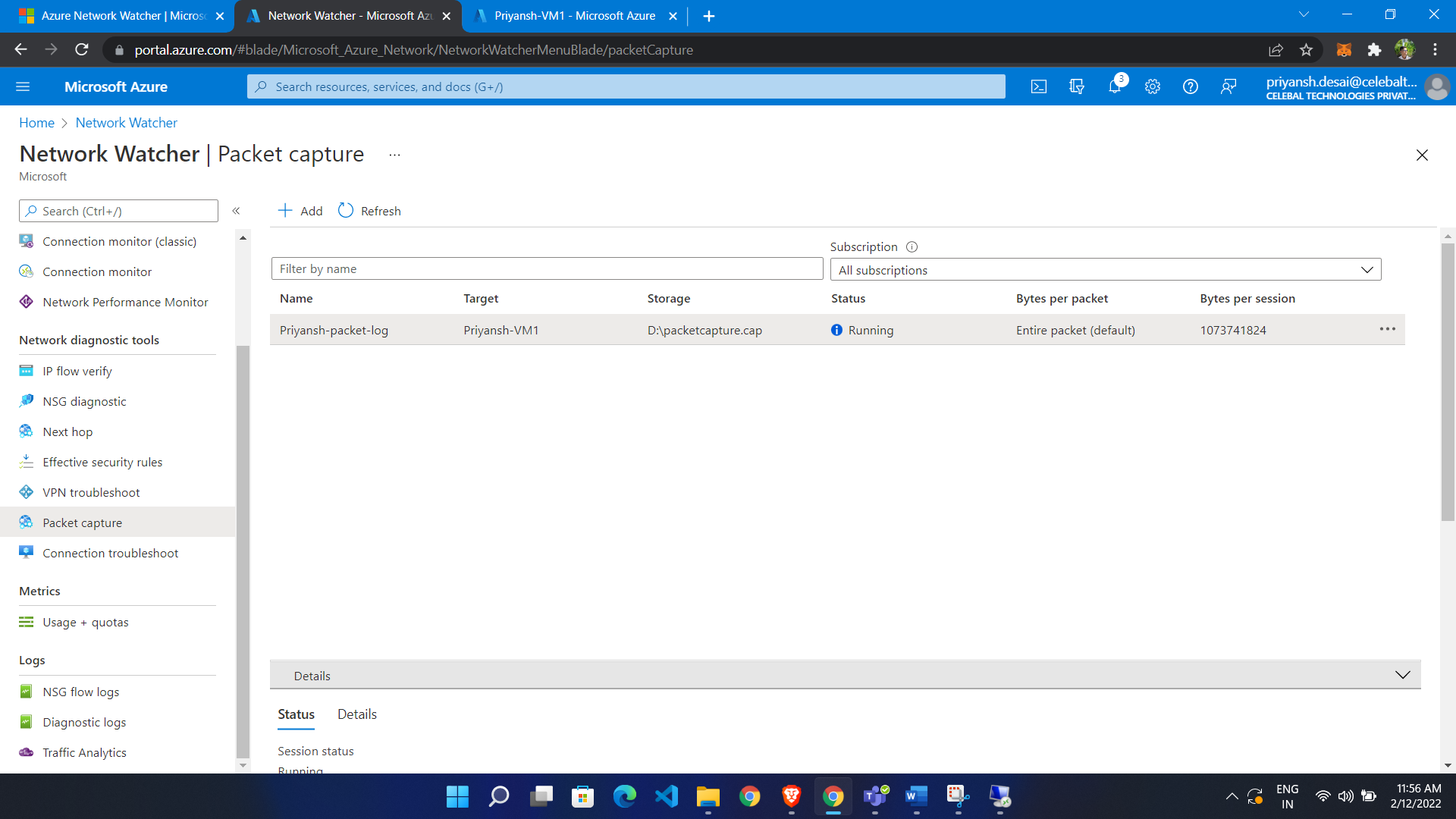


**Packet Capture:**

It will capture session which go from VM or come to VM

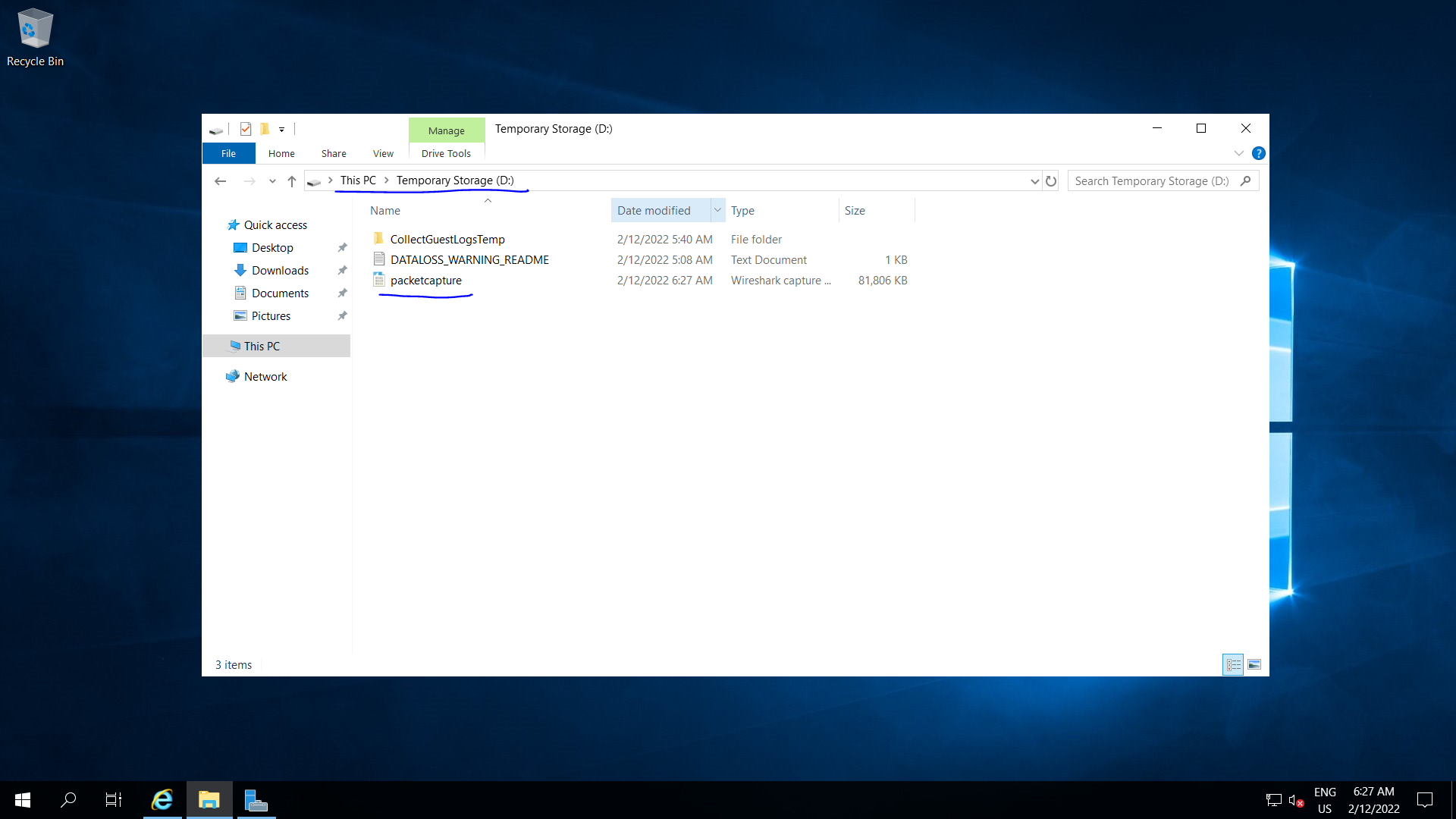
* Go to network watcher
* Go to packet capture
* Click ADD
* Choose RG
* Choose VM
* Give name
* Choose storage (storage account or vm local)

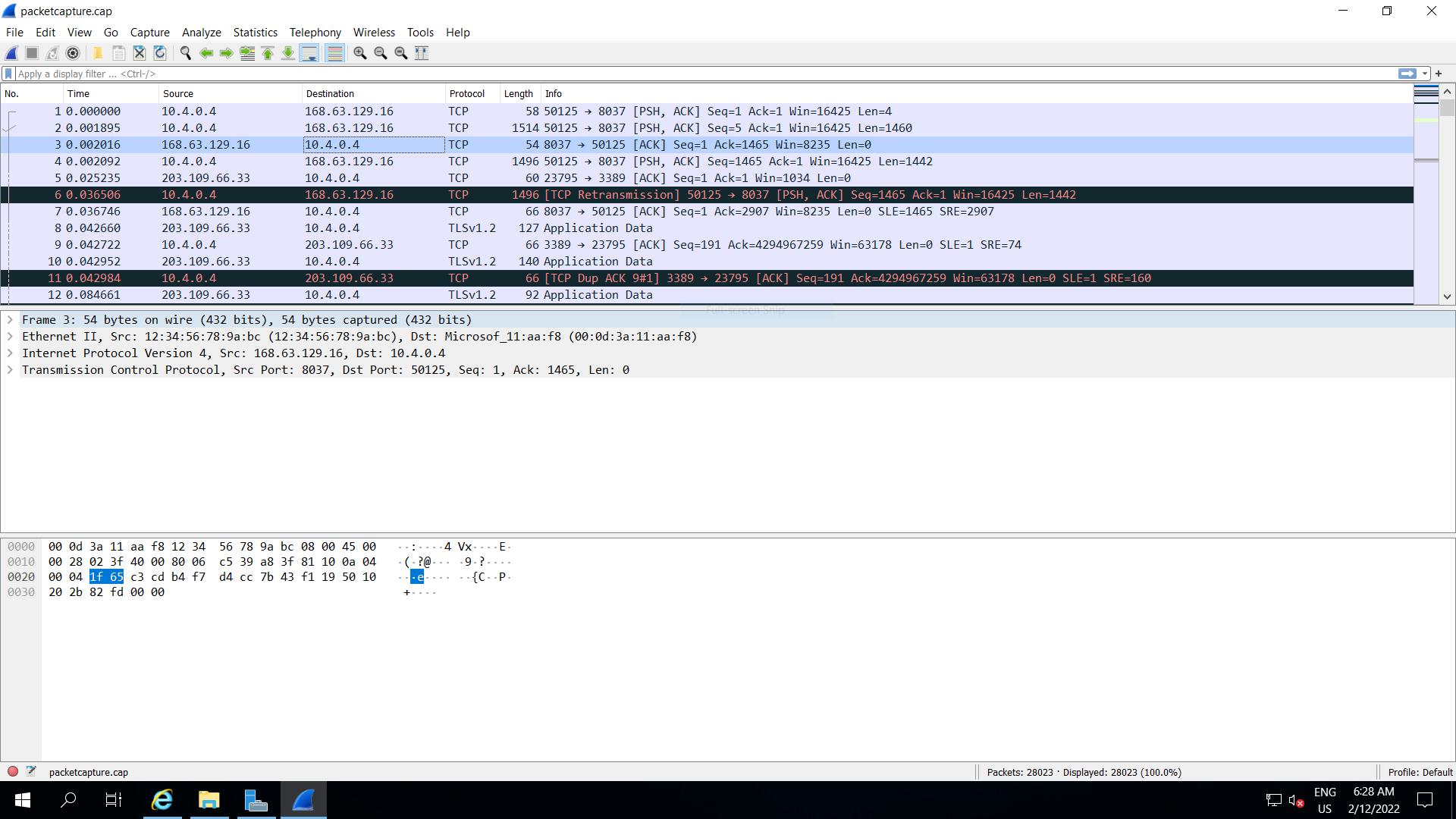




Now download packet analyze tool: (Wireshark)

Packet stored there

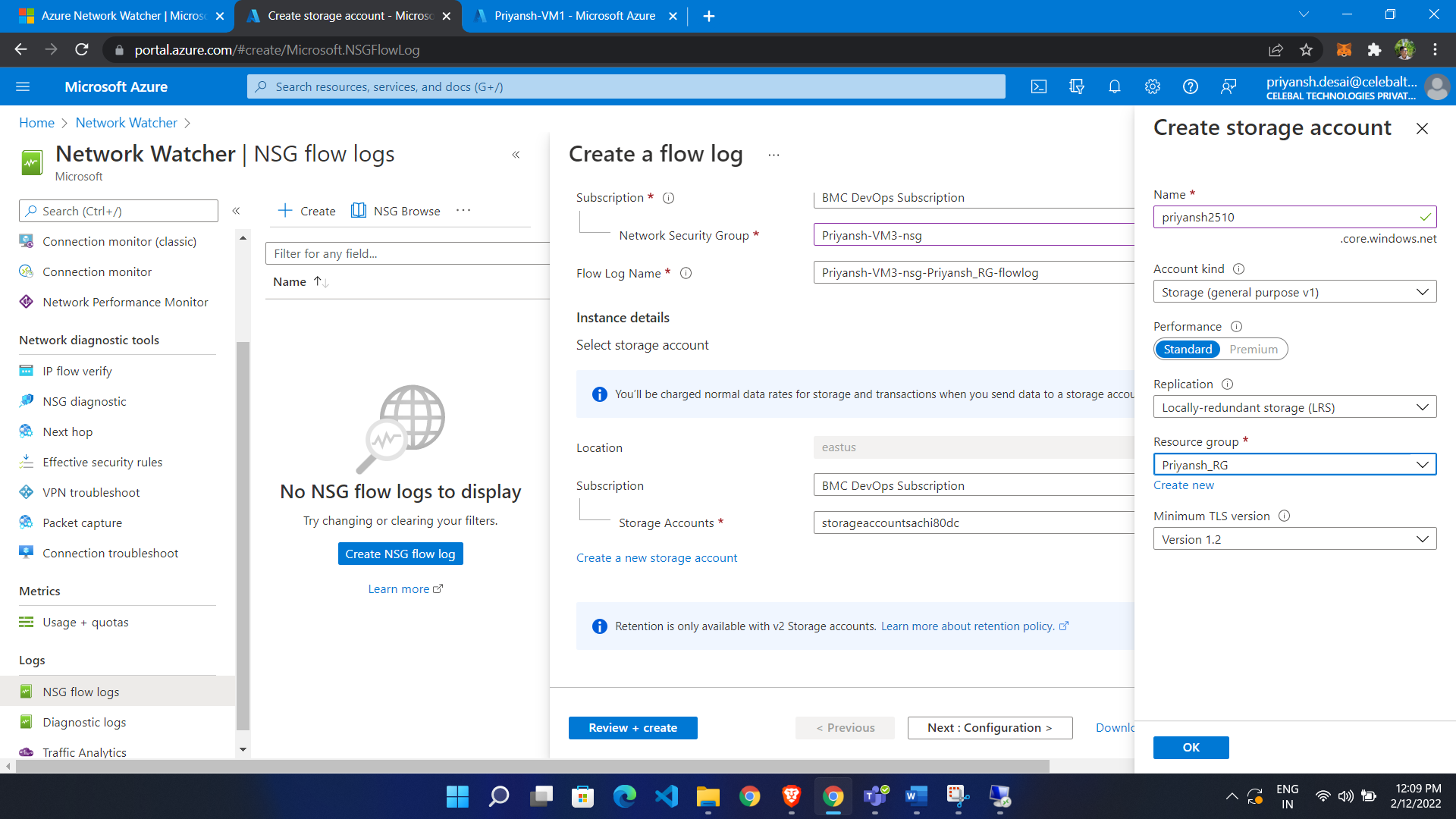




NSG FLOW Log:

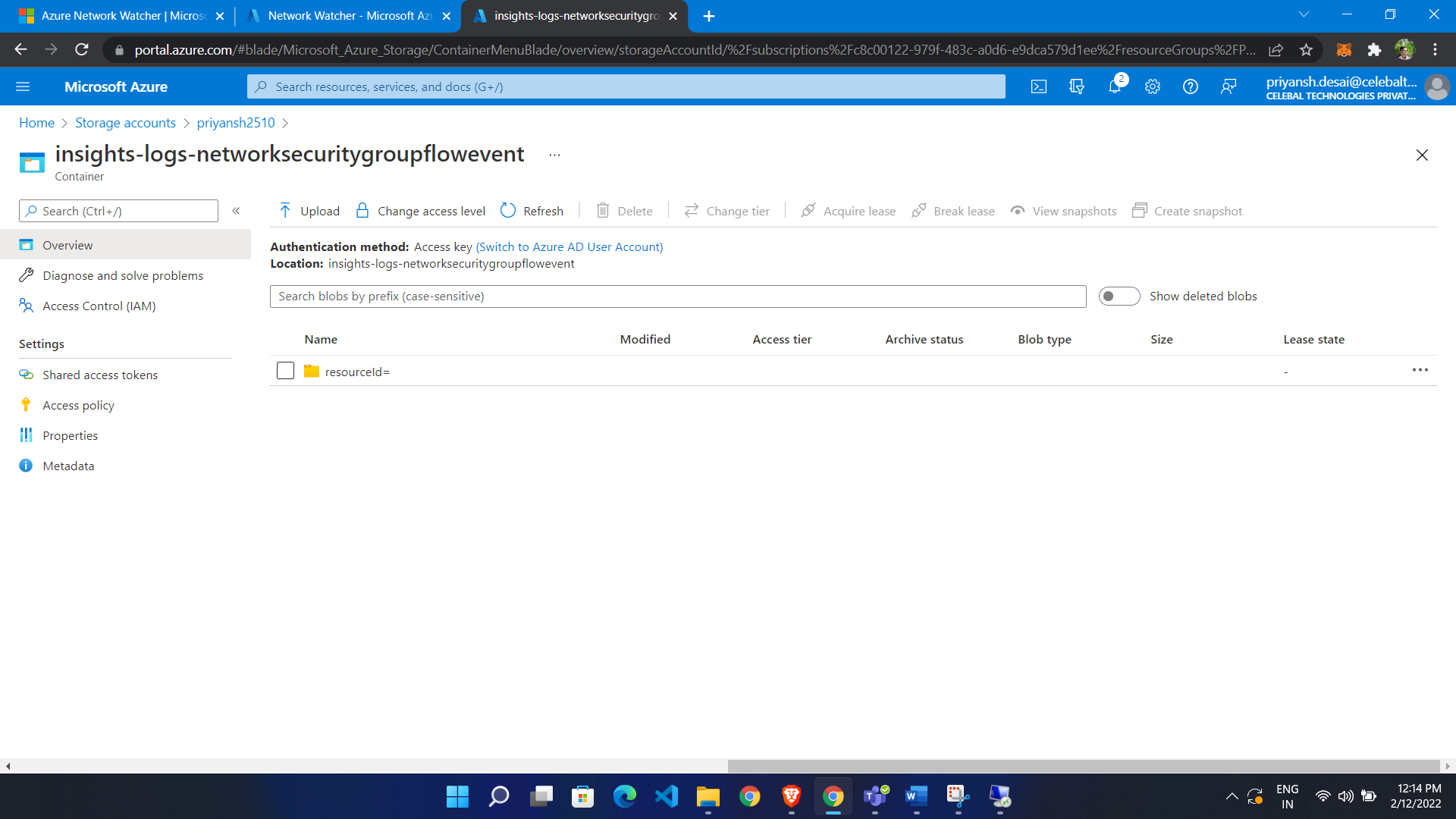
Network security group (NSG) flow logs is a feature of Azure Network Watcher that allows you to log information about IP traffic flowing through an NSG

* Go to network watcher
* Click nsg flow log
* Click create
* Choose nsg
* Give name
* Store it in storage account

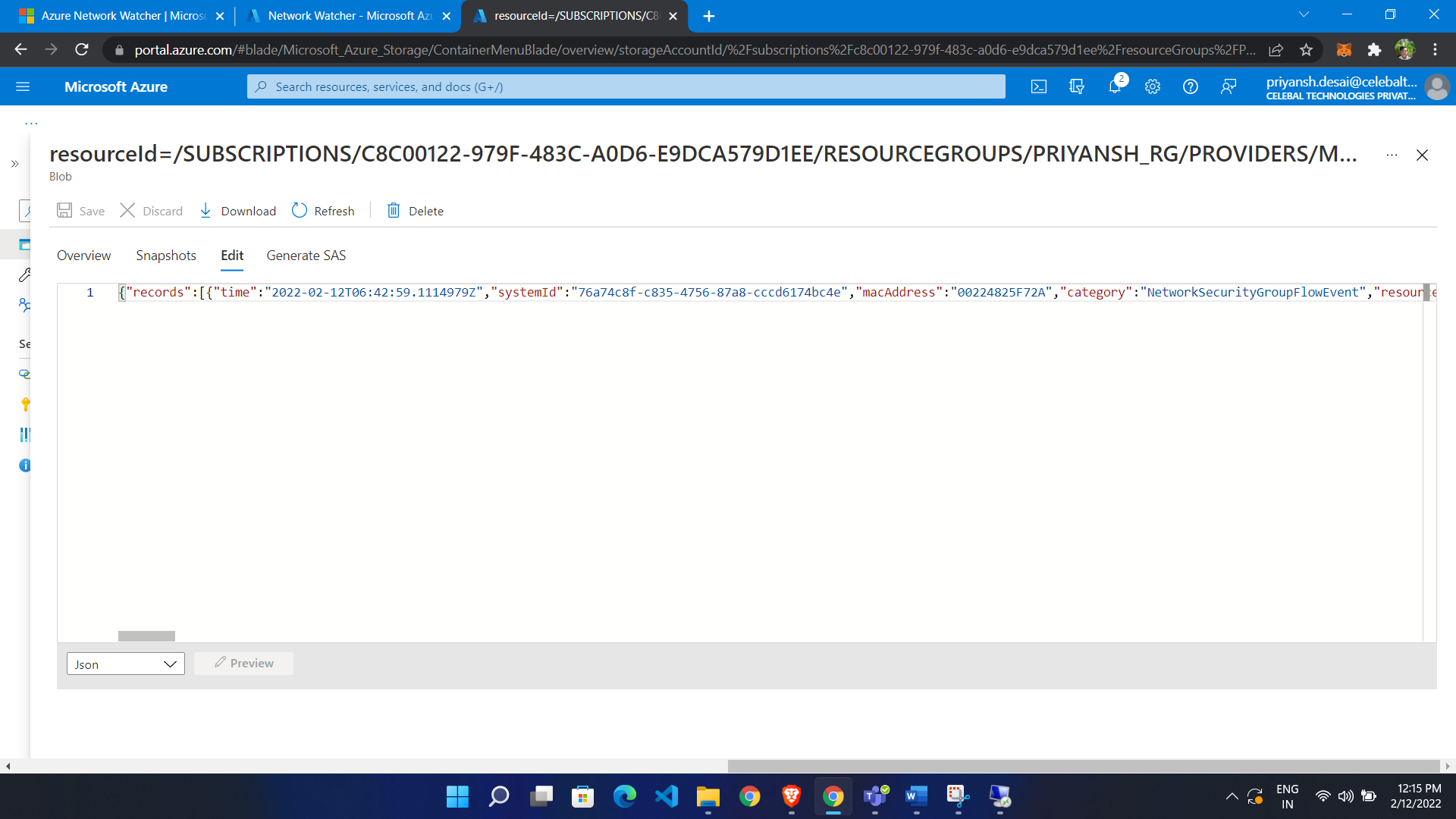


Now take rdp of that vm and do some activity

In storage account we see it



We are able to see logs

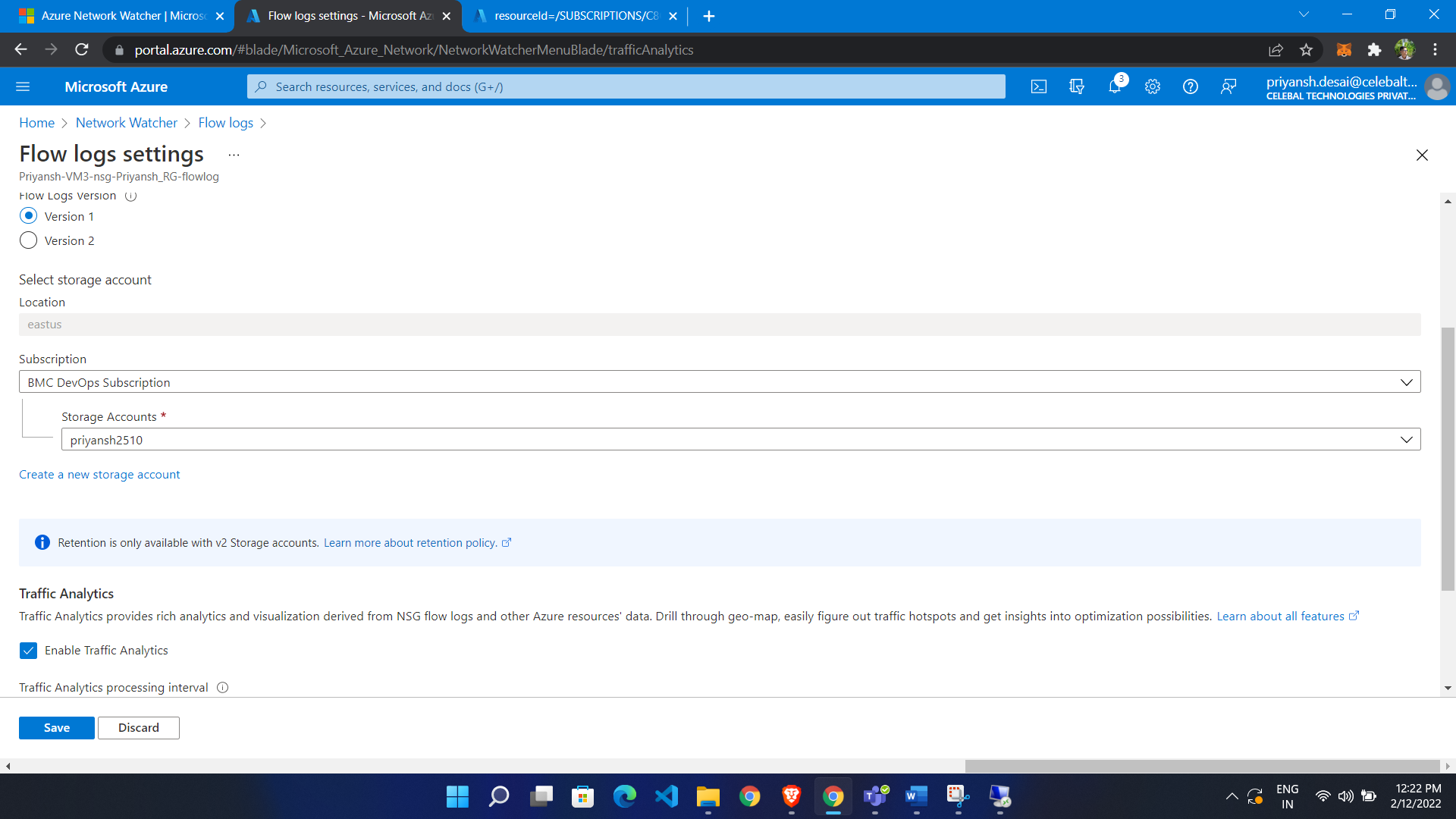


**Traffic Analyst:**

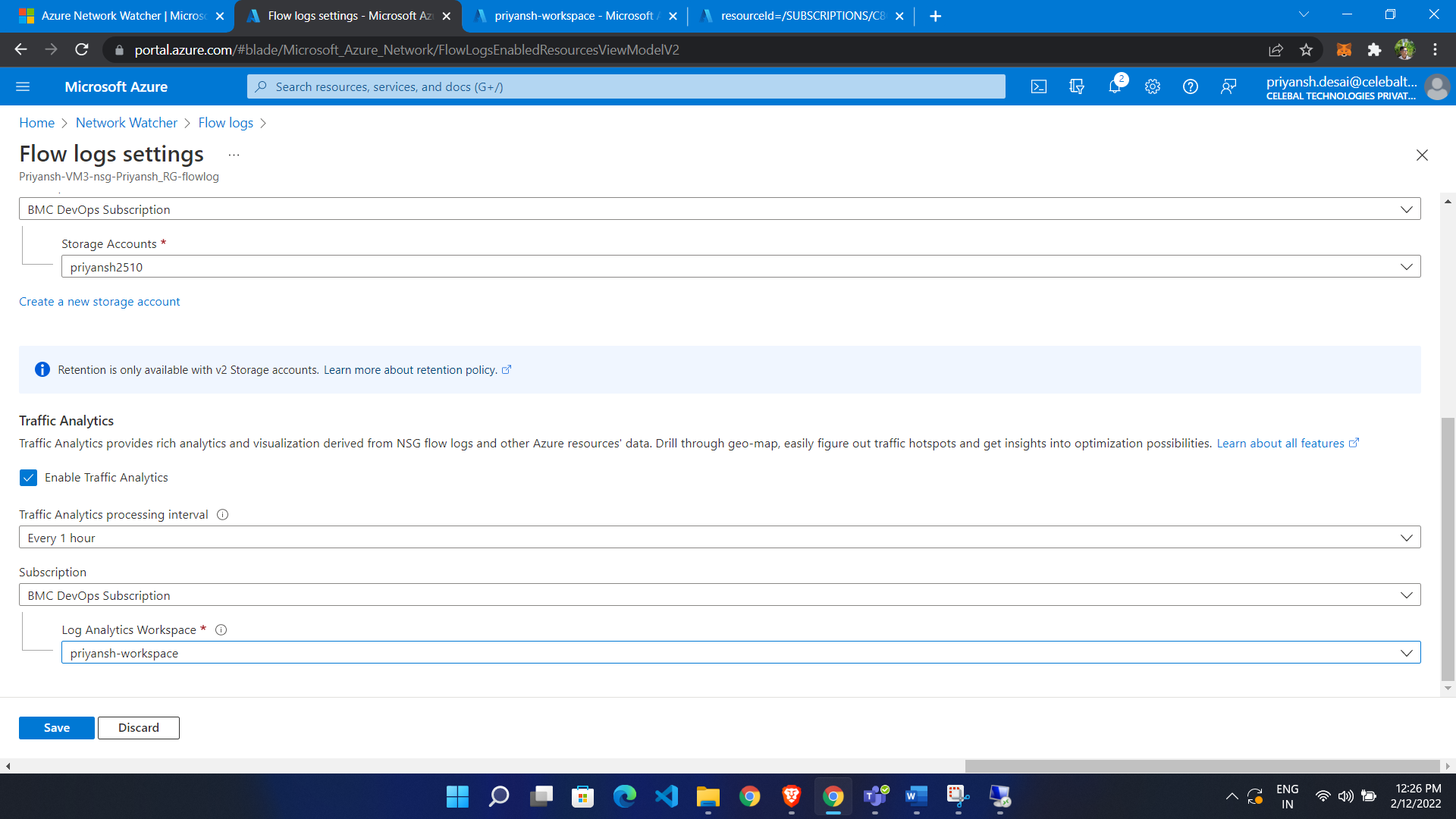
We are able to do analyze or visualize which activity done in cloud.

If we enable NSG flow log than we analyze traffic

* Go to network watcher
* Click on traffic analytics
* Click configure
* Chose NSG on which we enable NSG flow log
* Enable traffic analytics



Choose log analytics workspace



It will take 4-5 hour