Setup blob storage account

Loginto <https://portal.azure.com>

Search storage in the search bar and click on storage accounts

Graphical user interface, text, application, email

Description automatically generated

Next click create

Graphical user interface, text, application, email

Description automatically generated

Select the appropriate Azure Subscription(were you want the money to be billed to for charges), Click create New for the resource group and name it Azure\_PCAPStorage(this is to make sure it is not accidentally deleted if a customer deletes one of there resource groups), set storageaccount name to pcapstoreXXXXXX (xxx is contracted without -), Select the regon best located for the customer meaning were most of the resources are located.

Graphical user interface, text, application

Description automatically generated

Click Next: Advanced button and uncheck the Enable blob public access checkbox

Graphical user interface, text, application, email

Description automatically generated

Then click review +Create once button un grays click Create

This will take a few min to deploy/setup. Once done the page will have a button to go to the resource . Click it

Graphical user interface, text, application, email

Description automatically generated

Next click access keys   
Then select show keys and copy and document the key for future useGraphical user interface, text, application

Description automatically generated

Next lets SSH TO our processing box and mount the storage Blob

Install Blobfuse on box to read captures:

wget https://packages.microsoft.com/config/ubuntu/20.04/packages-microsoft-prod.deb

sudo dpkg -i packages-microsoft-prod.deb

sudo apt-get update

sudo apt-get install blobfuse

sudo mkdir /blob

touch /opt/fuse\_connection.cfg

edit with preferred editor

paste following and replace with documented info(I have filled in the account name as an example

accountName pcapstore2021223s

accountKey YOURKEY

containerName network-watcher-logs

Then mount your storage blob(Does not persist a reboot can add to startup script or whatever you would like)

sudo blobfuse /blob --tmp-path=/mnt/resource/blobfusetmp --config-file=/opt/fuse\_connection.cfg -o attr\_timeout=240 -o entry\_timeout=240 -o negative\_timeout=120

Then install azurecli

Sudo apt-get install azure-cli

Get all VMS and resourcegroups:

for i in `az account list -o tsv | awk '{print $3}'`; do az account set --subscription $i; az vm list --query [].[name,resourceGroup] --output tsv; done

next we will need to pipe each of those results into this command(I am not great at formatting and such so defer to Bill) I was running manually but example below

az network watcher packet-capture create --resource-group {resourceGroupName} --vm {vmName} --name VMNameDATETIME --storage-account STORAGEACCOUNTNAME

this then writes them to a long path so not sure how to handle that for merge cap/zeek ingest.

For this example it dumps to

/blob/subscriptions/fcd5d2db-c4d9-4358-86c1-23e5d96280c1/resourceGroups/GROUPNAME/providers/Microsoft.Compute/virtualMachines/VMNAME/YEAR/MONTH/DAY/