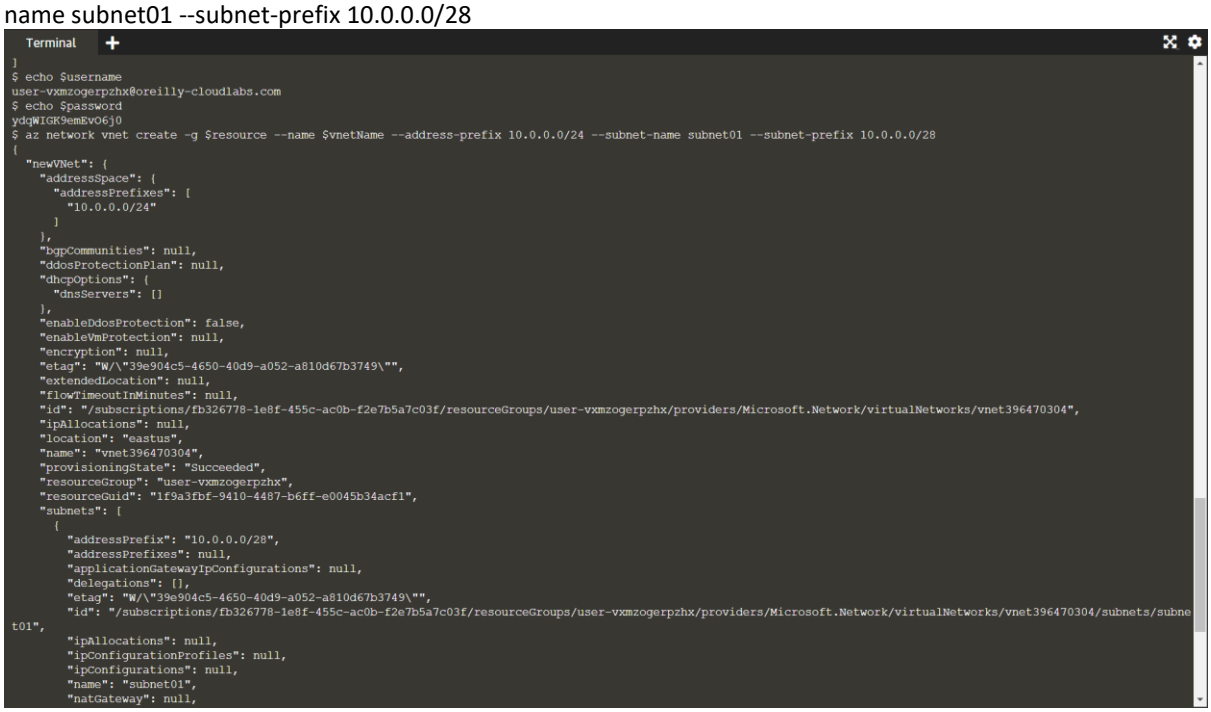
Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in Azure VNets.
In this lab, you will learn how to do the following:

Log into the Azure CLI
Understand Azure Network Watcher
Use the Azure Network Watcher Connection Monitor

Login to azure cli :
Az login -u $username -p $password

To create a new Azure Virtual Network and a subnet:
az network vnet create --resource-group $resource --name $vnetName --address-prefix 10.0.0.0/24 --subnet-name subnet01 --subnet-prefix 10.0.0.0/28



To create a new Azure Virtual Machine in the preceding subnet:
az vm create --resource-group $resource --name $vmName --image win2016datacenter --vnet-name vnetName --subnet subnet01 --public-ip-sku Standard --admin-username katavmuser --admin-password $password

--public-ip-sku: This specifies the SKU of the public IP address to use for the virtual machine. In this case, it's the Standard SKU.

In this lab, we will work with the Azure Network Watcher.
Understand Azure Network Watcher
Azure directs Azure VNet subnet traffic to destinations (next hop) using route tables. Azure automatically creates a default route table for each VNet subnet and adds system default routes to the table. These default routes specify where the subnet network traffic should be routed to.

Azure Network Watcher provides tools to monitor, diagnose, view metrics, and enable or disable logs for resources in Azure VNets.

We already created a new Azure Virtual Machine for you.
az vm list --resource-group $resource --query "[].{Name:name}"

```
$ az vm list --resource-group $resource --query "[].{Name:name}"
[
  {
    "Name": "vm396470304"
  }
]
$
```

In this lab, we will use the Azure Network Watcher to confirm (diagnose) the connectivity between this machine and the internet.

Work with Azure Network Watcher Connection Monitor using Azure CLI
In order to use Azure Network Watcher to diagnose VM network connectivity, you need to install an extension agent in the machine using this command:

az vm extension set --name NetworkWatcherAgentWindows --version 1.4.2331.0 --resource-group $resource --vm-name $vmName --publisher Microsoft.Azure.NetworkWatcher

Note: The NetworkWatcher agent has both Linux and Windows versions. Choose the right version based on your VM OS.

This appears to be a command for setting the Network Watcher Agent extension on a Windows virtual machine in an Azure environment. Let me break it down for you:

az: This is the Azure CLI command prefix.
vm extension set: This is the command to set a virtual machine extension.
--name NetworkWatcherAgentWindows: This specifies the name of the extension to set, which is the Network Watcher Agent for Windows.
--version 1.4.2331.0: This specifies the version of the extension to set.
--resource-group $resource: This specifies the name of the Azure resource group that contains the virtual machine. The $resource variable likely contains the name of the resource group.
--vm-name $vmName: This specifies the name of the virtual machine to which the extension should be added. The $vmName variable likely contains the name of the virtual machine.
--publisher Microsoft.Azure.NetworkWatcher: This specifies the name of the publisher of the extension, which is Microsoft.Azure.NetworkWatcher.

Now, you can use the az network watcher test-connectivity command to check connectivity between your VM and a public IP address (randomly chosen):

az network watcher test-connectivity --resource-group $resource --source-resource $vmName --dest-address 141.193.213.20 --dest-port 443 --query "connectionStatus"

Here are the command parameters:

--source-resource: The VM name for which you are checking connectivity
--dest-address: The IP address the VM needs to reach
--dest-port: The port number for which you are diagnosing connectivity
--query: The port number for which you are diagnosing connectivity

The preceding command is useful when you need to make sure that applications running on your VM can access a specific destination—for example, a Docker container registry or any other public service.

In the next step, we will clean the VM we created in this lab.