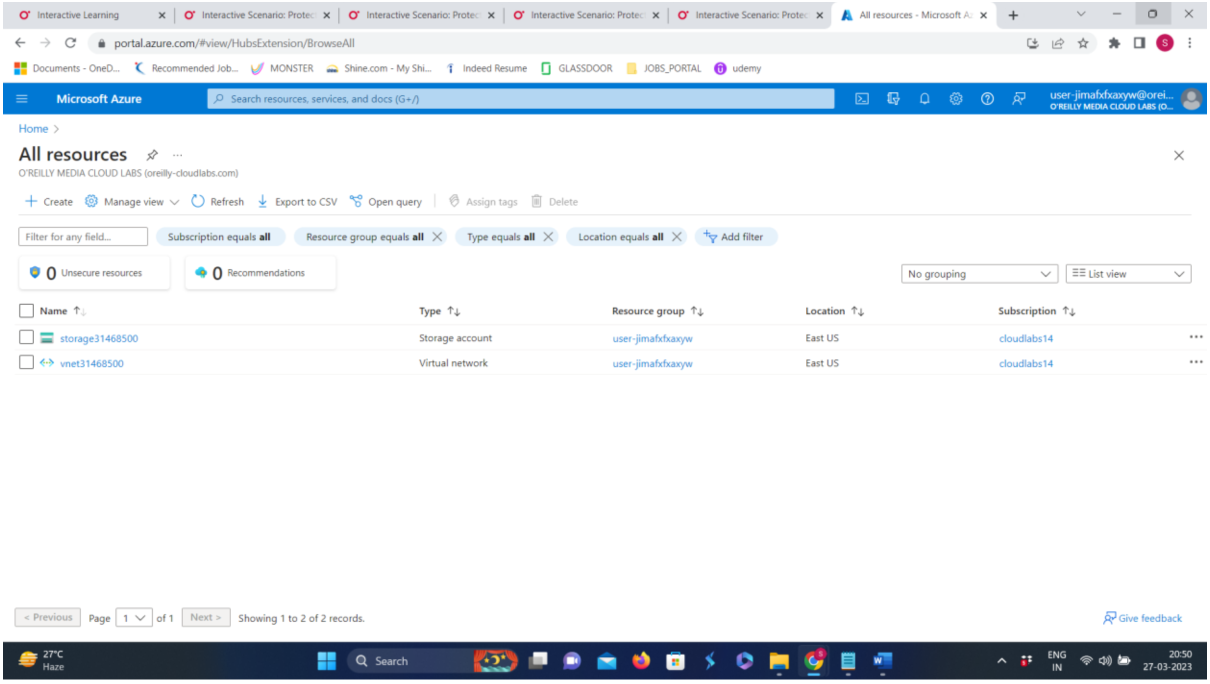
In this lab, you will learn how to do the following:

Log into the Azure CLI
Understand Azure Storage firewalls
Configure Azure Storage firewalls using Azure CLI
Confirm firewall settings using Azure CLI
Check Azure Storage firewall settings in the portal
Remove Azure Storage firewall rules

**To create a new Azure storage account:**
az storage account create -n $storageAccountName --resource-group $resource --sku Standard_LRS --default-action Deny

--default-action: specifies the default action for network access to the storage account. In the command you provided, Deny is used, which means that all network access to the storage account is denied by default.

**To create a new Azure VNet with 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


Interactive Learning
Interactive Scenario: Protec
All resources - Microsoft A
portal.azure.com/#view/HubsExtension/BrowseAll
Microsoft Azure
Search resources, services, and docs (G+/)
user-jimafxfxaxyw@orei...
O'REILLY MEDIA CLOUD LABS (O...
Home
+ Create
Manage view
Refresh
Export to CSV
Open query
Assign tags
Delete
Add filter
No grouping
List view
Give feedback

All resources

O'REILLY MEDIA CLOUD LABS (oreilly-cloudlabs.com)

Filter for any field... | Subscription equals **all** | Resource group equals **all** | Type equals **all** | Location equals **all**

0 Unsecure resources | 0 Recommendations

| Name | Type | Resource group | Location | Subscription |
|---|---|---|---|---|
| storage31468500 | Storage account | user-jimafxfxaxyw | East US | cloudlabs14 |
| vnet31468500 | Virtual network | user-jimafxfxaxyw | East US | cloudlabs14 |

< Previous Page 1 of 1 Next > Showing 1 to 2 of 2 records.

Storage account and vnet created .

Important: By passing the --default-action Deny parameter, we configured the above storage account to deny all traffic if no firewall rule matches the incoming request. Make sure you use the az storage account update command to set this flag for existing storage accounts.

Understand Azure Storage Firewall
In this lab you will learn about Azure Storage firewalls. Similar to most Azure data services, Azure Storage offers a service-level firewall enabling you to control and limit network access to your Azure storage account. This acts as a second layer of defense, preventing unauthorized users and processes to access you valuable data.

Azure Storage allows you to configure network access for the following:

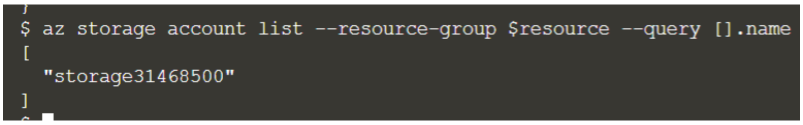
Azure Virtual Networks
Public IP addresses or IP address ranges

Azure private links/private endpoints
Individual resources
Trusted Azure services

In this lab you will explore the first two options, by configuring access for an Azure VNet and the randomly selected public IP address 20.84.181.62.

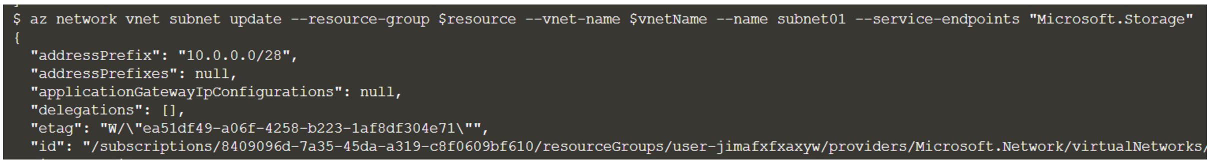
Note: The firewall rules are created at the Cosmos DB account level and will protect all the child databases and containers under said account.

We preconfigured this lab so that a new Azure storage account is created for you. Use the following command to confirm the account is present:



```
$ az storage account list --resource-group $resource --query [].name
[
  "storage31468500"
]
```

**Configure Azure Storage Firewall using Azure CLI**
First, let's create a new firewall rule allowing traffic from our subnet. Before creating the rules, use the following command to make sure the Microsoft.Storage service endpoint is added to your subnet:



```
$ az network vnet subnet update --resource-group $resource --vnet-name $vnetName --name subnet01 --service-endpoints "Microsoft.Storage"
{
  "addressPrefix": "10.0.0.0/28",
  "addressPrefixes": null,
  "applicationGatewayIpConfigurations": null,
  "delegations": [],
  "etag": "W/\"ea51df49-a06f-4258-b223-1af8df304e71\"",
  "id": "/subscriptions/8409096d-7a35-45da-a319-c8f0609bf610/resourceGroups/user-jimafxfxaxyw/providers/Microsoft.Network/virtualNetworks/
```

--service-endpoints: specifies the service endpoints to be enabled for the subnet. In the command you provided, "Microsoft.Storage" is used as an example to enable service endpoints for Azure Storage.
By enabling service endpoints for Azure Storage on a subnet, you allow traffic to Azure Storage services to flow directly over the Azure backbone network, providing faster and more secure access to storage resources.

**This command will allow resources in your subnet to talk to Azure storage accounts in general. Now you can create a firewall network rule to allow subnet traffic:**

az storage account network-rule add --resource-group $resource --account-name $storageAccountName --vnet-name $vnetName --subnet subnet01 --action Allow

Here are the command parameters:

--resource-group: Storage account parent resource group name
--account-name: Storage account name to add the network rule to
--vnet-name: Azure VNet name to allow
--subnet: Azure subnet within the above VNet to allow
--action: The rule effect; allowed values are Allow and Deny

az storage account network-rule add is a command that can be used with the Azure CLI (Command Line Interface) to add a network rule to a storage account in Azure.

By adding a network rule to a storage account, you can restrict network access to the storage account to specific virtual networks and subnets. This helps to secure your storage account and prevent unauthorized access.

There are many other options that can be used with this command to customize the network rule, such as specifying an IP address range or enabling virtual network service endpoints.

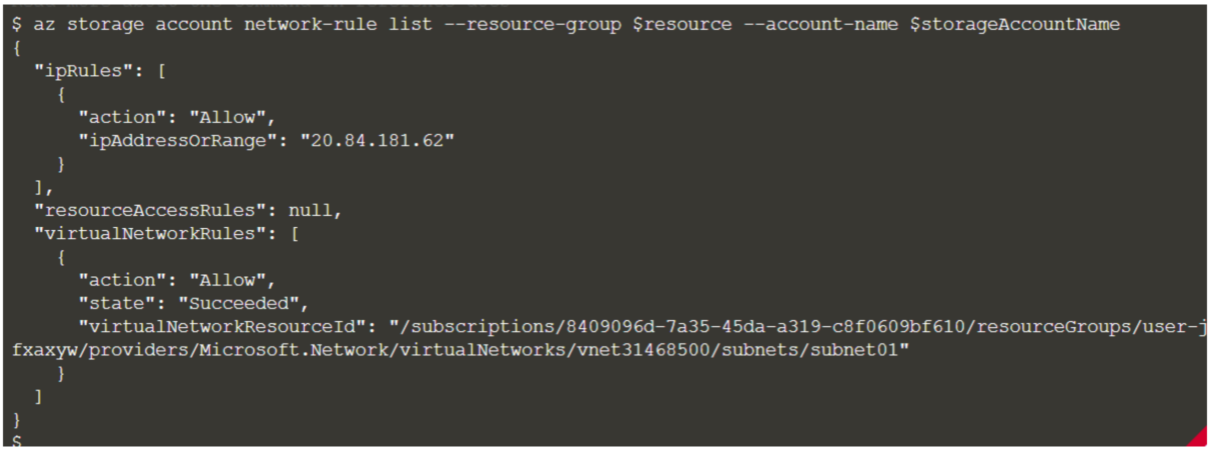
You can also allow or deny IP addresses (individual or range) as follows:
az storage account network-rule add --resource-group $resource --account-name $storageAccountName --ip-address "20.84.181.62" --action Allow

--ip-address: specifies the IP address or IP address range to allow access to the storage account.

**Confirm Firewall Settings using Azure CLI**
Use the following command to list all network IP rules for your storage account:

az storage account network-rule list --resource-group $resource --account-name $storageAccountName --query ipRules

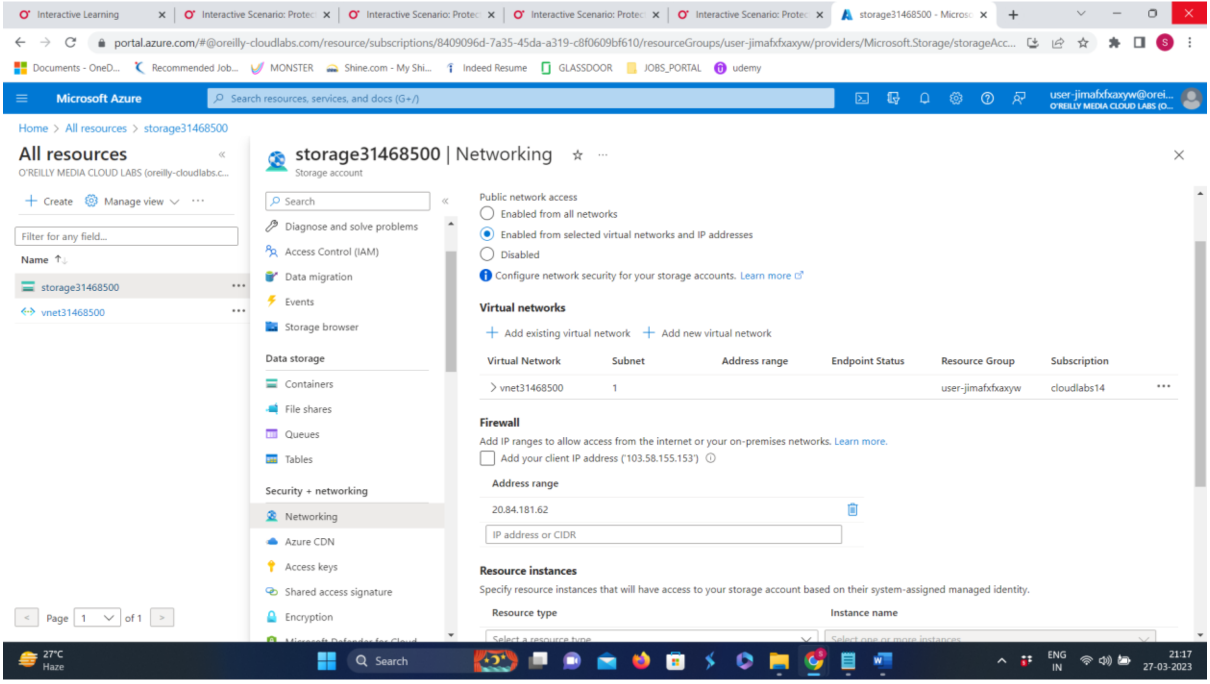
Also, the following command will list all virtual network subnet rules for your storage account:



```
$ az storage account network-rule list --resource-group $resource --account-name $storageAccountName
{
  "ipRules": [
    {
      "action": "Allow",
      "ipAddressOrRange": "20.84.181.62"
    }
  ],
  "resourceAccessRules": null,
  "virtualNetworkRules": [
    {
      "action": "Allow",
      "state": "Succeeded",
      "virtualNetworkResourceId": "/subscriptions/8409096d-7a35-45da-a319-c8f0609bf610/resourceGroups/user-j
fxaxyw/providers/Microsoft.Network/virtualNetworks/vnet31468500/subnets/subnet01"
    }
  ]
}
$
```

az storage account network-rule list --resource-group $resource --account-name $storageAccountName --query virtualNetworkRules

Check Firewall Settings in the Azure Portal
Under Security + networking, click on Networking.
We can see firewall rule and vnet is applied .



storage31468500 | Networking
Storage account

Public network access
○ Enabled from all networks
● Enabled from selected virtual networks and IP addresses
○ Disabled
Configure network security for your storage accounts. Learn more

Virtual networks
+ Add existing virtual network + Add new virtual network

| Virtual Network | Subnet | Address range | Endpoint Status | Resource Group | Subscription |
|---|---|---|---|---|---|
| vnet31468500 | 1 | | | user-jimafxfxaxyw | cloudlabs14 |

Firewall
Add IP ranges to allow access from the internet or your on-premises networks. Learn more.
□ Add your client IP address ('103.58.155.153')

Address range
20.84.181.62
IP address or CIDR

Resource instances
Specify resource instances that will have access to your storage account based on their system-assigned managed identity.
Resource type: Select a resource type
Instance name: Select one or more instances

portal.azure.com/#@oreilly-cloudlabs.com/resource/subscriptions/8409096d-7a35-45da-a319-c8f0609bf610/resourceGroups/user-jimafxfxaxyw/providers/Microsoft.Storage/storageAcc...
Microsoft Azure
Search resources, services, and docs (G+/)
Home > All resources > storage31468500
All resources
O'REILLY MEDIA CLOUD LABS (oreilly-cloudlabs.c...
storage31468500
vnet31468500
Diagnose and solve problems
Access Control (IAM)
Data migration
Events
Storage browser
Data storage
Containers
File shares
Queues
Tables
Security + networking
Networking
Azure CDN
Access keys
Shared access signature
Encryption
21:17
27-03-2023

## Remove Azure Storage Firewall Settings

Use the following command to remove the VNet rule from your storage account firewall:

```
az storage account network-rule remove --resource-group $resource --account-name $storageAccountName --vnet-name $vnetName --subnet subnet01
```

Use the following command to remove the IP rule(s) from your storage account firewall:

```
az storage account network-rule remove --resource-group $resource --account-name $storageAccountName --ip-address "20.84.181.62"
```

Finally, use this command to confirm that all the firewall rules are removed:

```
az storage account network-rule list --resource-group $resource --account-name $storageAccountName --query ipRules
```