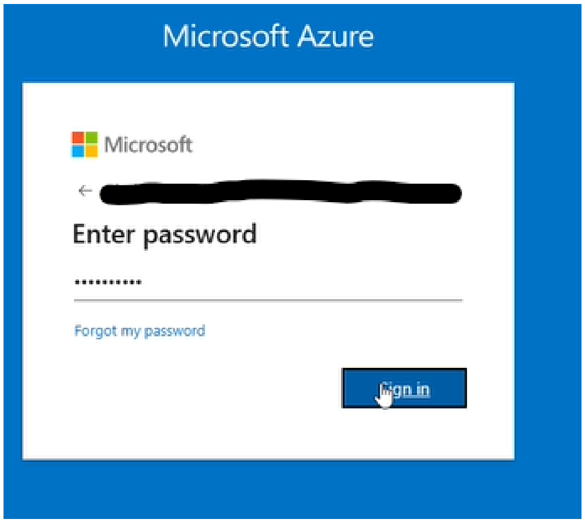
Configure Azure Role Based Access Control

Assigning an Azure Built-In Role to a User

1. Sign into the Admin Account



Microsoft Azure

Microsoft

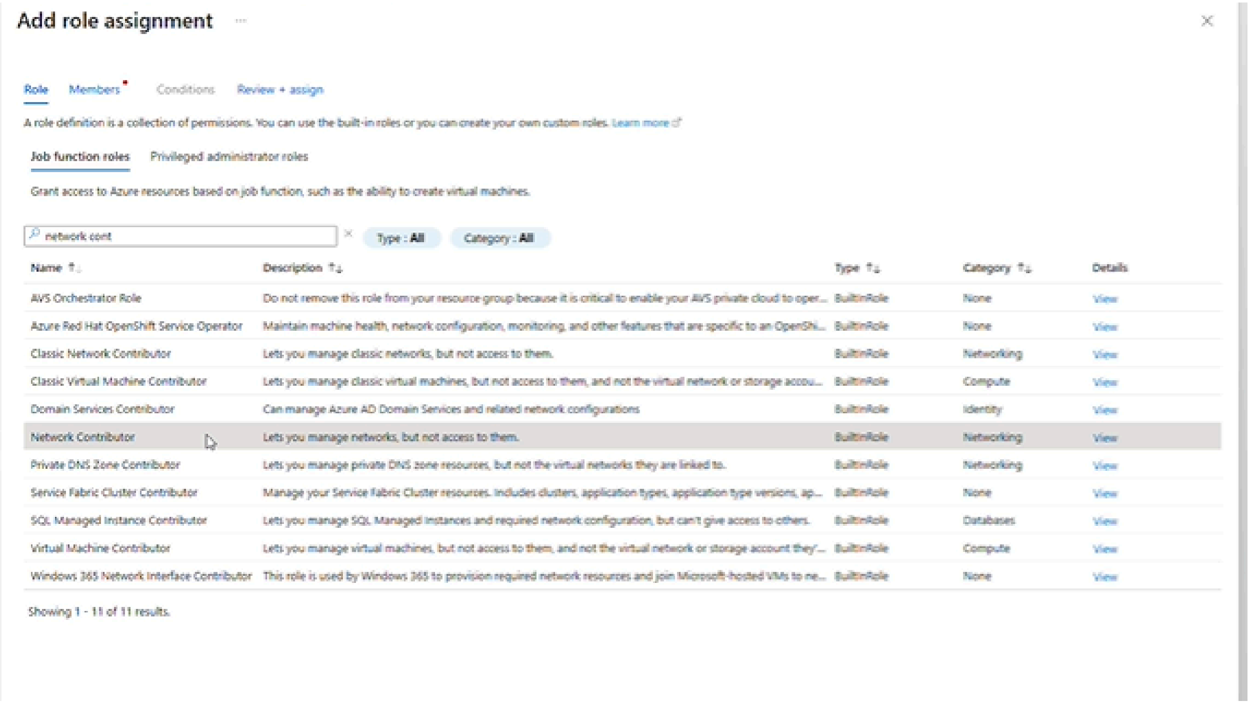
← [redacted]

Enter password

••••••••••

2. Assign the Network Contributor role to the user

- Network Contributor - lets you manage the networks, but not access them



Add role assignment

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

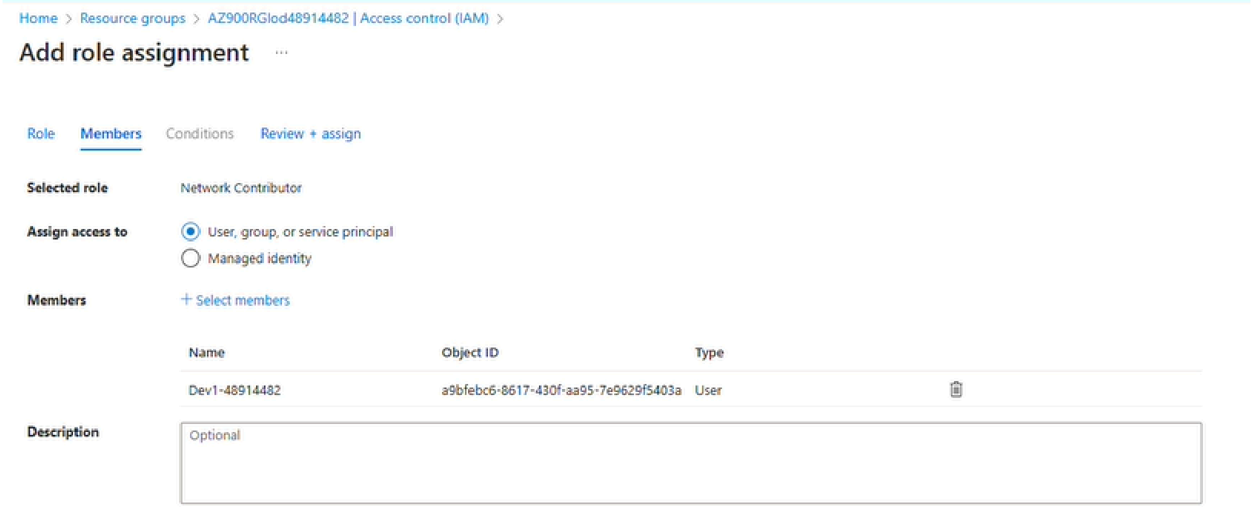
Grant access to Azure resources based on job function, such as the ability to create virtual machines.

network cont

Type : All | Category : All

Name	Description	Type	Category	Details
AVS Orchestrator Role	Do not remove this role from your resource group because it is critical to enable your AVS private cloud to oper...	BuiltInRole	None	View
Azure Red Hat OpenShift Service Operator	Maintain machine health, network configuration, monitoring, and other features that are specific to an OpenShi...	BuiltInRole	None	View
Classic Network Contributor	Lets you manage classic networks, but not access to them.	BuiltInRole	Networking	View
Classic Virtual Machine Contributor	Lets you manage classic virtual machines, but not access to them, and not the virtual network or storage accou...	BuiltInRole	Compute	View
Domain Services Contributor	Can manage Azure AD Domain Services and related network configurations	BuiltInRole	Identity	View
Network Contributor	Lets you manage networks, but not access to them.	BuiltInRole	Networking	View
Private DNS Zone Contributor	Lets you manage private DNS zone resources, but not the virtual networks they are linked to.	BuiltInRole	Networking	View
Service Fabric Cluster Contributor	Manage your Service Fabric Cluster resources. Includes clusters, application types, application type versions, ap...	BuiltInRole	None	View
SQL Managed Instance Contributor	Lets you manage SQL Managed Instances and required network configuration, but can't give access to others.	BuiltInRole	Databases	View
Virtual Machine Contributor	Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they'...	BuiltInRole	Compute	View
Windows 365 Network Interface Contributor	This role is used by Windows 365 to provision required network resources and join Microsoft-hosted VMs to ne...	BuiltInRole	None	View

Showing 1 - 11 of 11 results.



Home > Resource groups > AZ900RGlod48914482 | Access control (IAM) >

Add role assignment

Selected role: Network Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

Name	Object ID	Type
Dev1-48914482	a9bfebc6-8617-430f-aa95-7e9629f5403a	User

Description: Optional

Test an Azure built-in role assignment

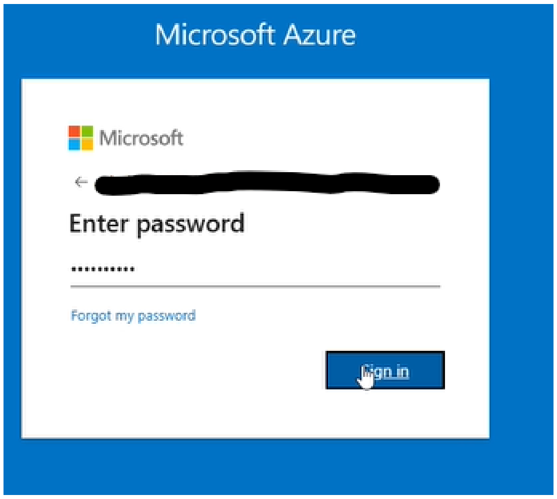
Now that the role has been assigned, create an **Azure Virtual Network (VNet)** with the following properties:

- Virtual Network (VNet): A container that holds other networking components and configurations.

- Requirements:
  - At least one subnet
  - At least one virtual address space
- Virtual Address Space: A block of IP addresses that can be divided into subnets.

Next Step:

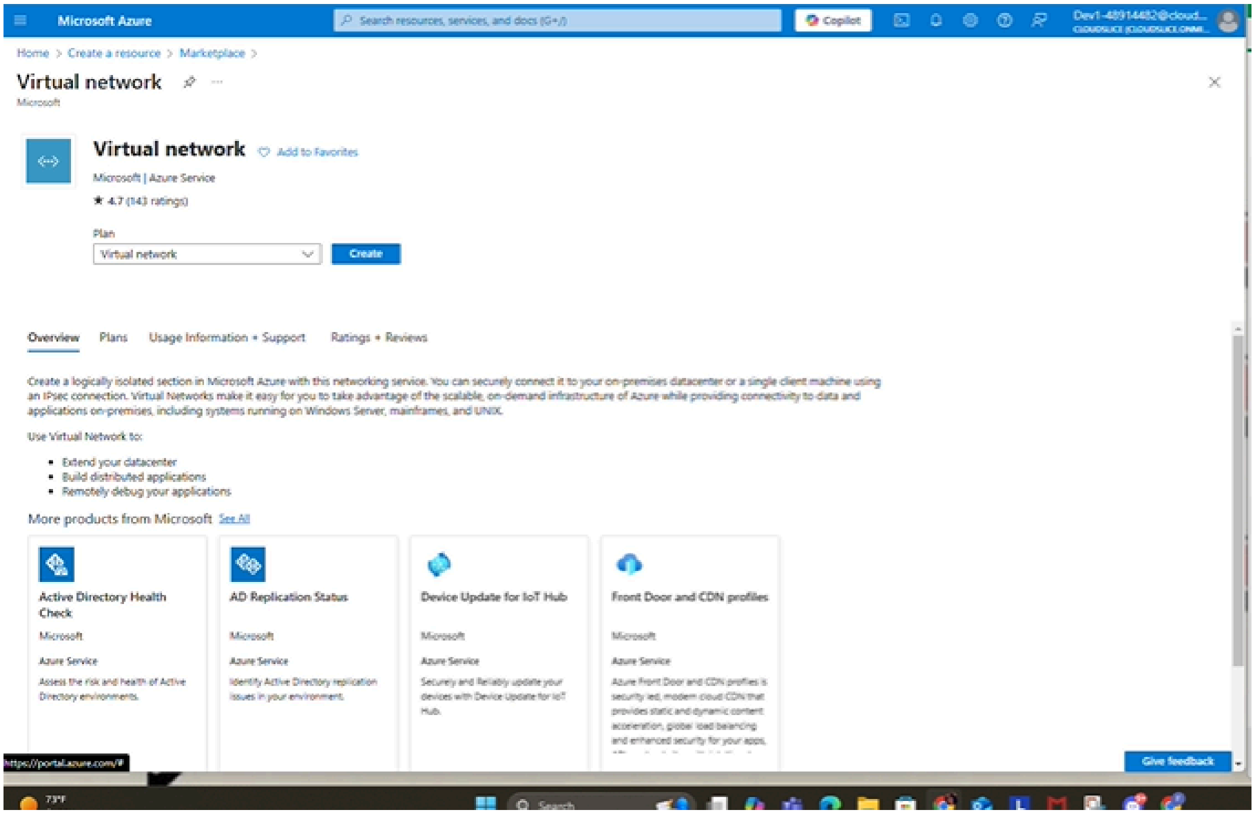
- Sign into the user that was given Network Contributor role



← [redacted]

Enter password

••••••••••



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Dev1-48914482@cloud...
CLOUDSLICE (CLOUDSLICE.ONMI...

Home > Create a resource > Marketplace >

Virtual network

Microsoft

Virtual network ♡ Add to Favorites

Microsoft | Azure Service

★ 4.7 (143 ratings)

Plan

Virtual network

Create

Overview Plans Usage Information + Support Ratings + Reviews

Create a logically isolated section in Microsoft Azure with this networking service. You can securely connect it to your on-premises datacenter or a single client machine using an IPsec connection. Virtual Networks make it easy for you to take advantage of the scalable, on-demand infrastructure of Azure while providing connectivity to data and applications on-premises, including systems running on Windows Server, mainframes, and UNIX.

Use Virtual Network to:

- Extend your datacenter
- Build distributed applications
- Remotely debug your applications

More products from Microsoft See All

Active Directory Health Check
Microsoft
Azure Service
Assess the risk and health of Active Directory environments.

AD Replication Status
Microsoft
Azure Service
Identify Active Directory replication issues in your environment.

Device Update for IoT Hub
Microsoft
Azure Service
Securely and Reliably update your devices with Device Update for IoT Hub.

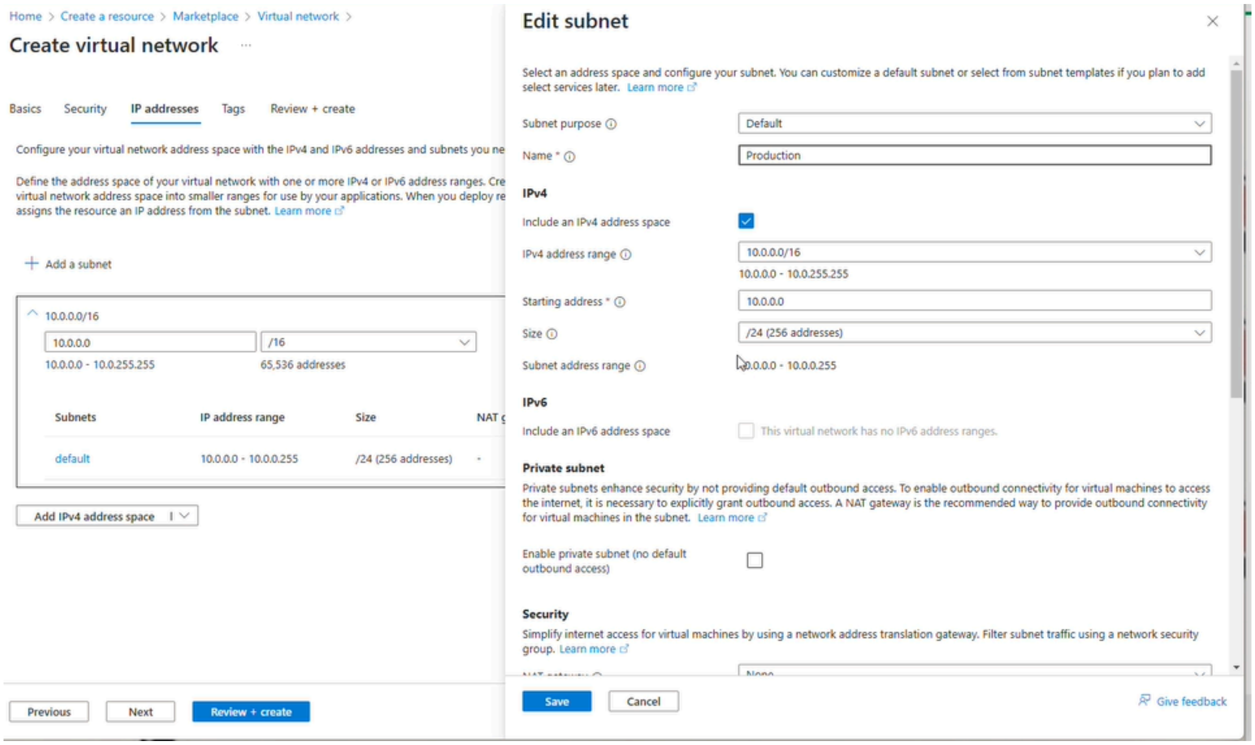
Front Door and CDN profiles
Microsoft
Azure Service
Azure Front Door and CDN profiles is security led, modern cloud CDN that provides static and dynamic content acceleration, global load balancing and enhanced security for your apps.

Give feedback

https://portal.azure.com/#

73°F

Search



Home > Create a resource > Marketplace > Virtual network >

Create virtual network ...

Basics Security IP addresses Tags Review + create

Configure your virtual network address space with the IPv4 and IPv6 addresses and subnets you ne

Define the address space of your virtual network with one or more IPv4 or IPv6 address ranges. Cre virtual network address space into smaller ranges for use by your applications. When you deploy re assigns the resource an IP address from the subnet. Learn more

+ Add a subnet

10.0.0.0/16

10.0.0.0 /16

10.0.0.0 - 10.0.255.255 65,536 addresses

Subnets	IP address range	Size	NAT g
default	10.0.0.0 - 10.0.0.255	/24 (256 addresses)	-

Add IPv4 address space

Previous Next Review + create

Edit subnet

Select an address space and configure your subnet. You can customize a default subnet or select from subnet templates if you plan to add select services later. Learn more

Subnet purpose ⓘ: Default

Name * ⓘ: Production

IPv4

Include an IPv4 address space: ☑

IPv4 address range ⓘ: 10.0.0.0/16
10.0.0.0 - 10.0.255.255

Starting address * ⓘ: 10.0.0.0

Size ⓘ: /24 (256 addresses)

Subnet address range ⓘ: 10.0.0.0 - 10.0.0.255

IPv6

Include an IPv6 address space: □ This virtual network has no IPv6 address ranges.

Private subnet

Private subnets enhance security by not providing default outbound access. To enable outbound connectivity for virtual machines to access the internet, it is necessary to explicitly grant outbound access. A NAT gateway is the recommended way to provide outbound connectivity for virtual machines in the subnet. Learn more

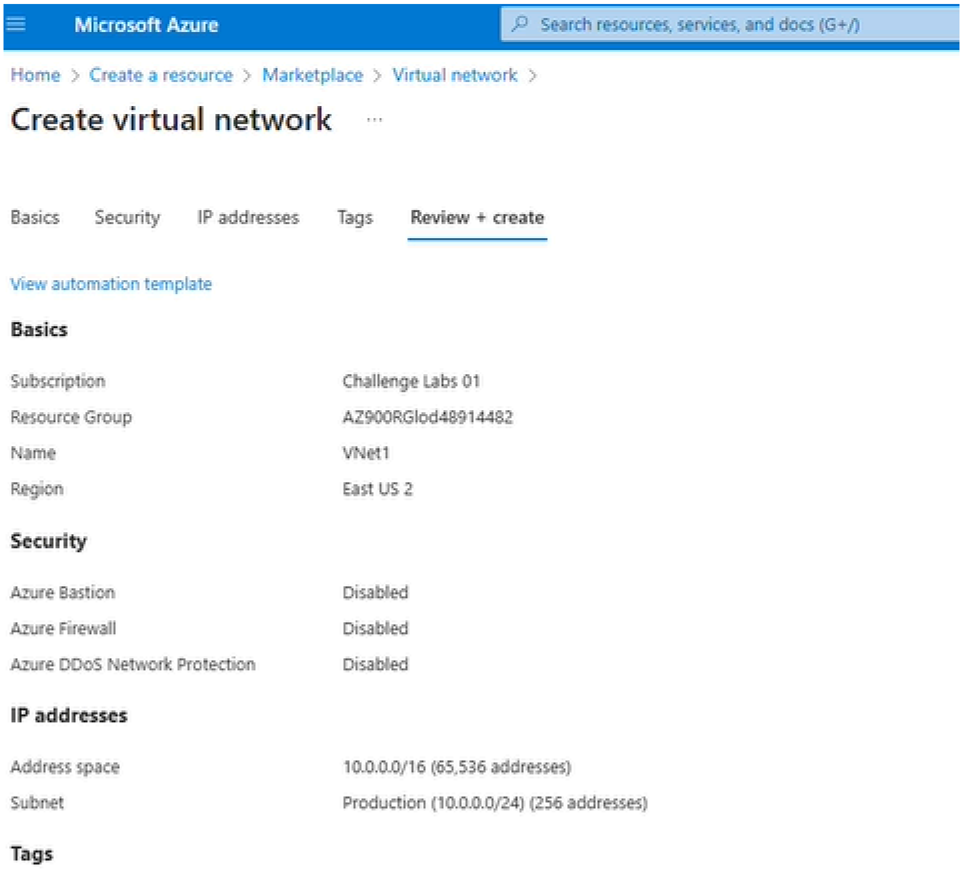
Enable private subnet (no default outbound access): □

Security

Simplify internet access for virtual machines by using a network address translation gateway. Filter subnet traffic using a network security group. Learn more

NAT gateway ⓘ: None

Save Cancel Give feedback


Microsoft Azure
Search resources, services, and docs (G+/)
Home > Create a resource > Marketplace > Virtual network >
Basics
Security
IP addresses
Tags
Review + create
View automation template

Create virtual network ...

Basics

Subscription	Challenge Labs 01
Resource Group	AZ900RGlod48914482
Name	VNet1
Region	East US 2

Security

Azure Bastion	Disabled
Azure Firewall	Disabled
Azure DDoS Network Protection	Disabled

IP addresses

Address space	10.0.0.0/16 (65,536 addresses)
Subnet	Production (10.0.0.0/24) (256 addresses)

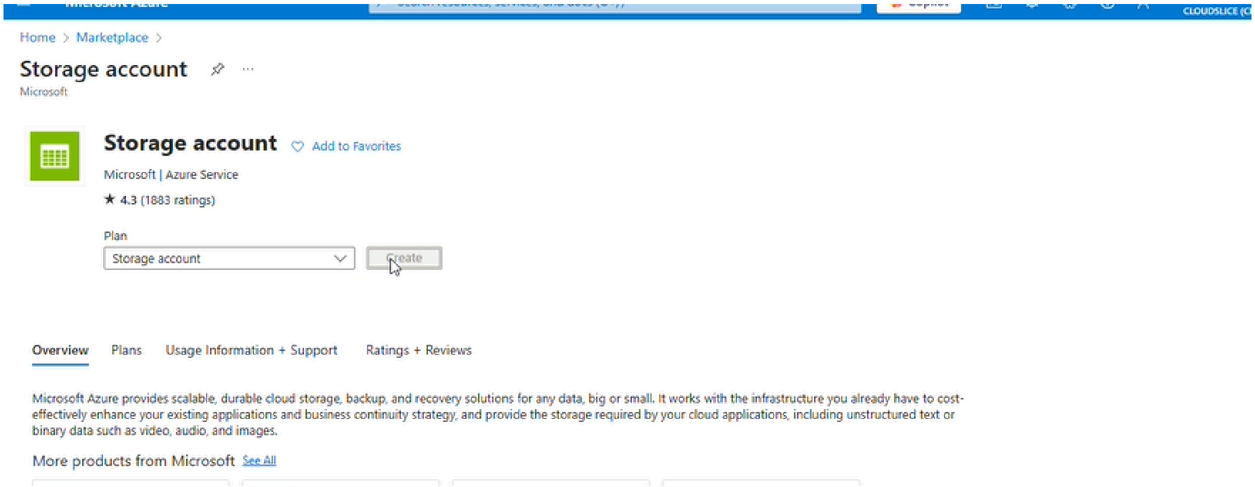
Tags

- Attempt to create a **storage account** in your resource group using default values.

Features of Azure Storage

Azure Storage includes the following services:

- **Blobs:** Unstructured data storage.
- **Files:** Fully managed, cloud-based file shares.
- **Queues:** Messaging service for asynchronous communication.
- **Tables:** NoSQL data storage for structured data.



Storage account

Microsoft

Storage account

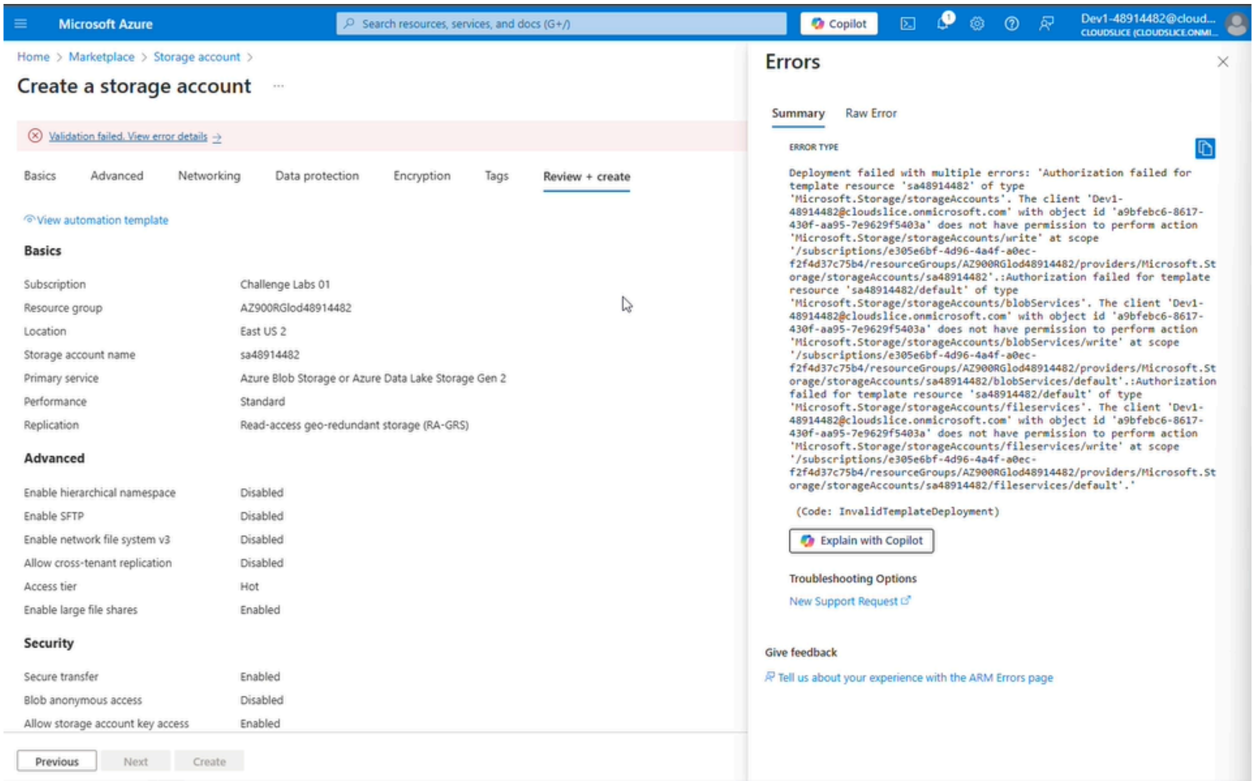
Microsoft | Azure Service

★ 4.3 (1883 ratings)

Plan: Storage account

Microsoft Azure provides scalable, durable cloud storage, backup, and recovery solutions for any data, big or small. It works with the infrastructure you already have to cost-effectively enhance your existing applications and business continuity strategy, and provide the storage required by your cloud applications, including unstructured text or binary data such as video, audio, and images.

More products from Microsoft See All



Create a storage account

Validation failed. View error details →

Basics

Subscription	Challenge Labs 01
Resource group	AZ900RGlod48914482
Location	East US 2
Storage account name	sa48914482
Primary service	Azure Blob Storage or Azure Data Lake Storage Gen 2
Performance	Standard
Replication	Read-access geo-redundant storage (RA-GRS)

Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable large file shares	Enabled

Security

Secure transfer	Enabled
Blob anonymous access	Disabled
Allow storage account key access	Enabled

Errors

ERROR TYPE

```
Deployment failed with multiple errors: 'Authorization failed for
template resource 'sa48914482' of type
'Microsoft.Storage/storageAccounts'. The client 'Dev1-
48914482@cloudslice.onmicrosoft.com' with object id 'a9bfebc6-8617-
430f-aa95-7e9629f5403a' does not have permission to perform action
'Microsoft.Storage/storageAccounts/write' at scope
'/subscriptions/e305e6bf-4d96-4a4f-a0ec-
f2f4d37c75b4/resourceGroups/AZ900RGlod48914482/providers/Microsoft.St
orage/storageAccounts/sa48914482'.:Authorization failed for template
resource 'sa48914482/default' of type
'Microsoft.Storage/storageAccounts/blobServices'. The client 'Dev1-
48914482@cloudslice.onmicrosoft.com' with object id 'a9bfebc6-8617-
430f-aa95-7e9629f5403a' does not have permission to perform action
'Microsoft.Storage/storageAccounts/blobServices/write' at scope
'/subscriptions/e305e6bf-4d96-4a4f-a0ec-
f2f4d37c75b4/resourceGroups/AZ900RGlod48914482/providers/Microsoft.St
orage/storageAccounts/sa48914482/blobServices/default'.:Authorization
failed for template resource 'sa48914482/default' of type
'Microsoft.Storage/storageAccounts/fileservices'. The client 'Dev1-
48914482@cloudslice.onmicrosoft.com' with object id 'a9bfebc6-8617-
430f-aa95-7e9629f5403a' does not have permission to perform action
'Microsoft.Storage/storageAccounts/fileservices/write' at scope
'/subscriptions/e305e6bf-4d96-4a4f-a0ec-
f2f4d37c75b4/resourceGroups/AZ900RGlod48914482/providers/Microsoft.St
orage/storageAccounts/sa48914482/fileservices/default'.'

 (Code: InvalidTemplateDeployment)
```

Troubleshooting Options

Give feedback

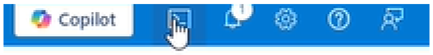
Tell us about your experience with the ARM Errors page

Why did the storage account creation fail?

- The failure occurs because the user **was not granted permissions** to create a storage account.
- To resolve this, assign the **Storage Account Contributor** role to the user, similar to how the **Network Contributor** role was assigned.

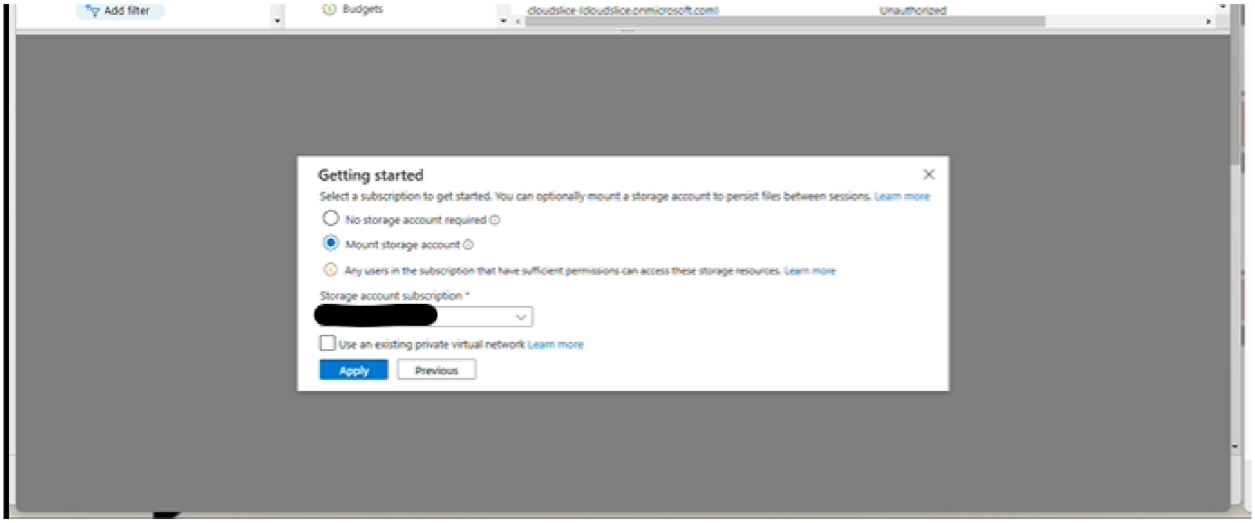
Creating a Custom Role Using Azure PowerShell

1. Switch Back to the Admin Account
2. Launch an Azure Cloud Shell PowerShell Session



Steps in PowerShell:

- Select **"Mount Storage Account"**
- Choose the relevant **storage account subscription**, then apply.
- In the **Mount Storage Account** window, select **"I want to create a storage account"**
- Enter the required information and proceed with creation and deployment.



Getting started

Select a subscription to get started. You can optionally mount a storage account to persist files between sessions. Learn more

○ No storage account required

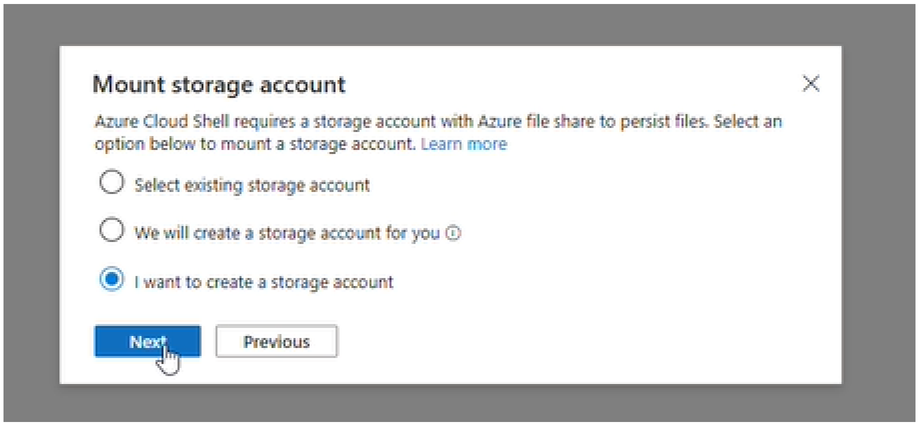
● Mount storage account

Any users in the subscription that have sufficient permissions can access these storage resources. Learn more

Storage account subscription *

[redacted]

□ Use an existing private virtual network Learn more



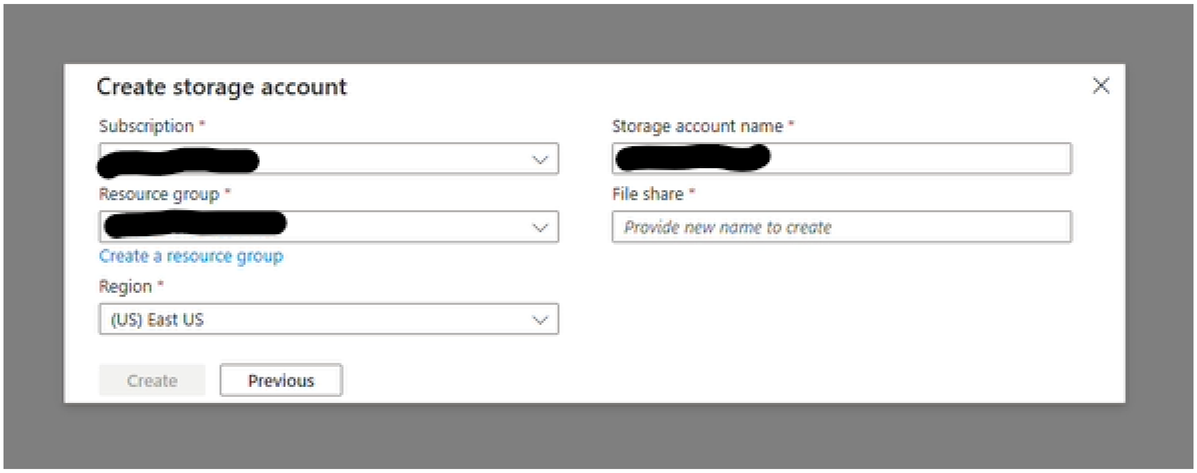
Mount storage account

Azure Cloud Shell requires a storage account with Azure file share to persist files. Select an option below to mount a storage account. Learn more

○ Select existing storage account

○ We will create a storage account for you ⓘ

● I want to create a storage account



Create storage account

Subscription *: [redacted]

Resource group *: [redacted]

Create a resource group

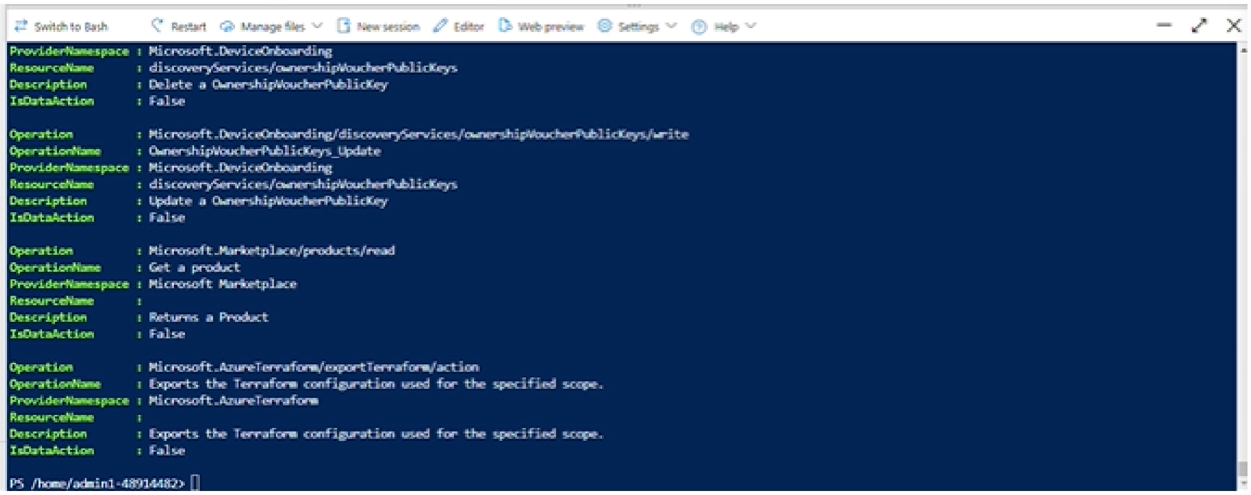
Region *: (US) East US

Storage account name *: [redacted]

File share *: Provide new name to create

Azure Cloud Shell Overview:

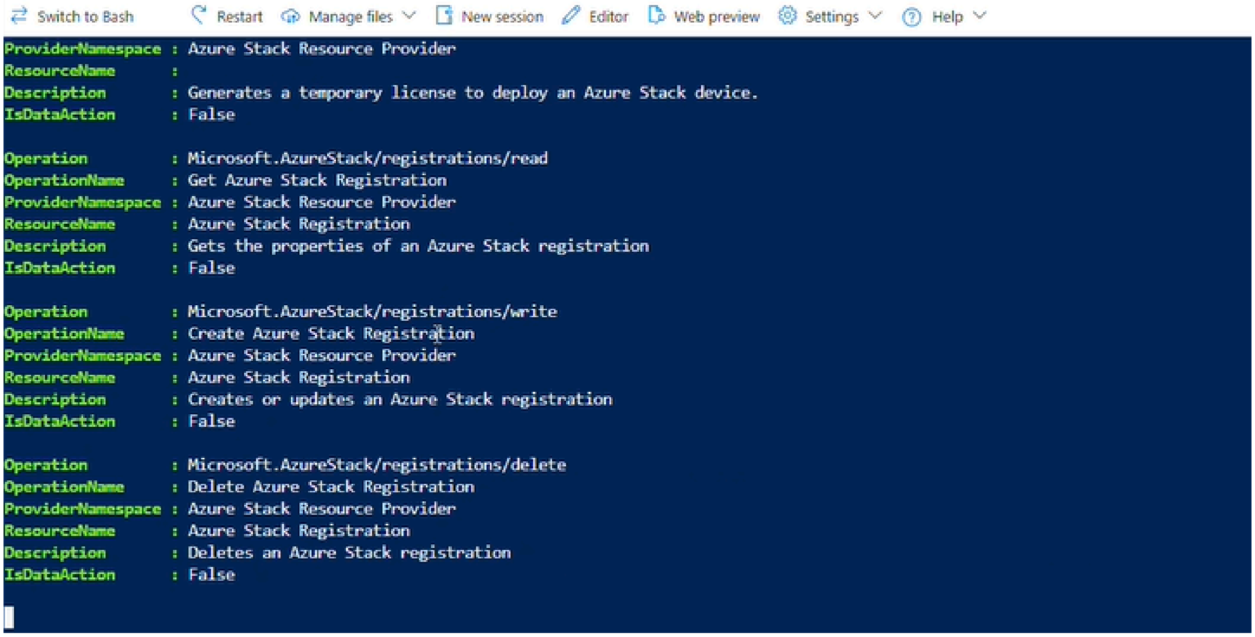
- Used to manage **Azure resources**.
- Requires a **storage account** and **file share** to store commands and scripts.



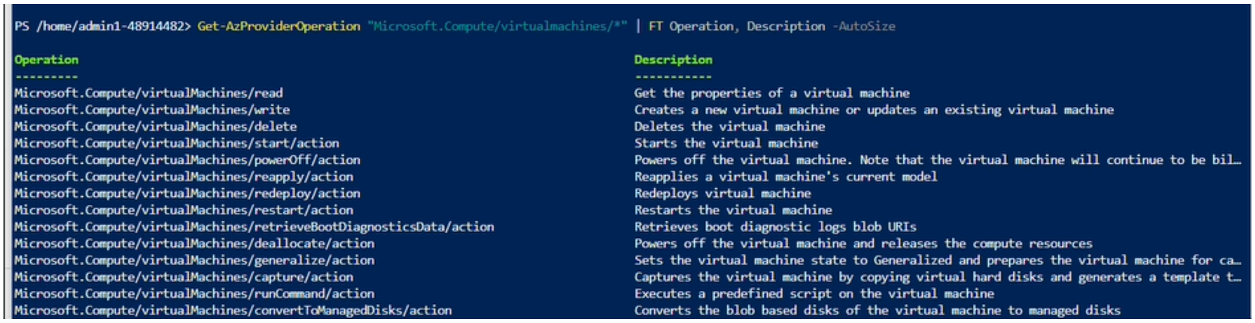
```
ProviderNamespace : Microsoft.DeviceOnboarding
ResourceName      : discoveryServices/ownershipVoucherPublicKeys
Description       : Delete a OwnershipVoucherPublicKey
IsDataAction      : False

Operation         : Microsoft.DeviceOnboarding/discoveryServices/ownershipVoucherPublicKeys/write
OperationName     : OwnershipVoucherPublicKeys_Update
ProviderNamespace : Microsoft.DeviceOnboarding
ResourceName      : discoveryServices/ownershipVoucherPublicKeys
Description       : Update a OwnershipVoucherPublicKey
IsDataAction      : False

Operation         : Microsoft.Marketplace/products/read
OperationName     : Get a product
ProviderNamespace : Microsoft Marketplace
ResourceName      :
Description       : Returns a Product
IsDataAction      : False

Operation         : Microsoft.AzureTerraform/exportTerraform/action
OperationName     : Exports the Terraform configuration used for the specified scope.
ProviderNamespace : Microsoft.AzureTerraform
ResourceName      :
Description       : Exports the Terraform configuration used for the specified scope.
IsDataAction      : False

PS /home/admin1-48914482> 
```

Using PowerShell Commands for Role Management

- **Identifying Operations Associated with Virtual Machines**
    - *Get-AzProviderOperation “Microsoft.Compute/virtualmachines/*” | FT Operation, Description -AutoSize*
- *Get-AzProviderOperation* - identify the operations associated with virtual machines



```
ProviderNamespace : Azure Stack Resource Provider
ResourceName      :
Description       : Generates a temporary license to deploy an Azure Stack device.
IsDataAction      : False

Operation         : Microsoft.AzureStack/registrations/read
OperationName     : Get Azure Stack Registration
ProviderNamespace : Azure Stack Resource Provider
ResourceName      : Azure Stack Registration
Description       : Gets the properties of an Azure Stack registration
IsDataAction      : False

Operation         : Microsoft.AzureStack/registrations/write
OperationName     : Create Azure Stack Registration
ProviderNamespace : Azure Stack Resource Provider
ResourceName      : Azure Stack Registration
Description       : Creates or updates an Azure Stack registration
IsDataAction      : False

Operation         : Microsoft.AzureStack/registrations/delete
OperationName     : Delete Azure Stack Registration
ProviderNamespace : Azure Stack Resource Provider
ResourceName      : Azure Stack Registration
Description       : Deletes an Azure Stack registration
IsDataAction      : False
```



```
PS /home/admin1-48914482> Get-AzProviderOperation "Microsoft.Compute/virtualmachines/*" | FT Operation, Description -AutoSize

Operation                                                                               Description
---------                                                                               -----------
Microsoft.Compute/virtualMachines/read                                                  Get the properties of a virtual machine
Microsoft.Compute/virtualMachines/write                                                 Creates a new virtual machine or updates an existing virtual machine
Microsoft.Compute/virtualMachines/delete                                                Deletes the virtual machine
Microsoft.Compute/virtualMachines/start/action                                          Starts the virtual machine
Microsoft.Compute/virtualMachines/powerOff/action                                       Powers off the virtual machine. Note that the virtual machine will continue to be bil…
Microsoft.Compute/virtualMachines/reapply/action                                        Reapplies a virtual machine's current model
Microsoft.Compute/virtualMachines/redeploy/action                                       Redeploys virtual machine
Microsoft.Compute/virtualMachines/restart/action                                        Restarts the virtual machine
Microsoft.Compute/virtualMachines/retrieveBootDiagnosticsData/action                    Retrieves boot diagnostic logs blob URIs
Microsoft.Compute/virtualMachines/deallocate/action                                     Powers off the virtual machine and releases the compute resources
Microsoft.Compute/virtualMachines/generalize/action                                     Sets the virtual machine state to Generalized and prepares the virtual machine for ca…
Microsoft.Compute/virtualMachines/capture/action                                        Captures the virtual machine by copying virtual hard disks and generates a template t…
Microsoft.Compute/virtualMachines/runCommand/action                                     Executes a predefined script on the virtual machine
Microsoft.Compute/virtualMachines/convertToManagedDisks/action                          Converts the blob based disks of the virtual machine to managed disks
```

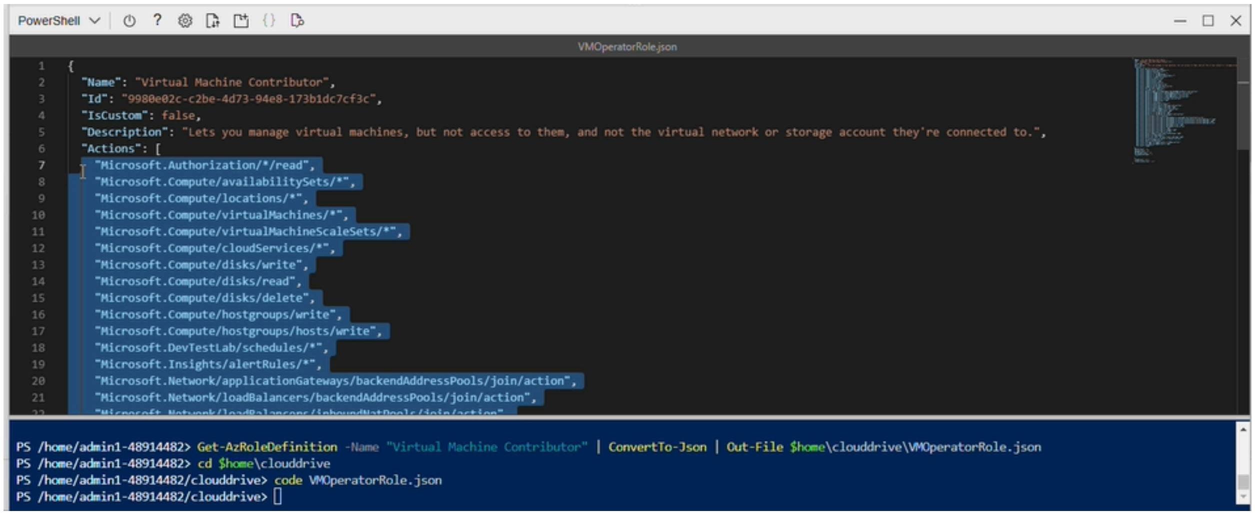
- To retrieve the role definition for the built-in the VMC role and output to *$home\clouddrive\VMOperatorRole.json* by using *Get-AzRoleDefinition*
- ***Retrieving the Built-In Virtual Machine Contributor Role Definition***

- ○ Get-AzRoleDefinition -Name “Virtual Machine Contributor” | ConvertTo-Json | Out-File $home\clouddrive\VMOperatorRole.json

Editing the Role Definition File in Cloud Shell

1. Navigate to the directory:
   - ○ cd $home\clouddrive
2. Open the JSON file for editing:
   - ○ code VMOperatorRole.json

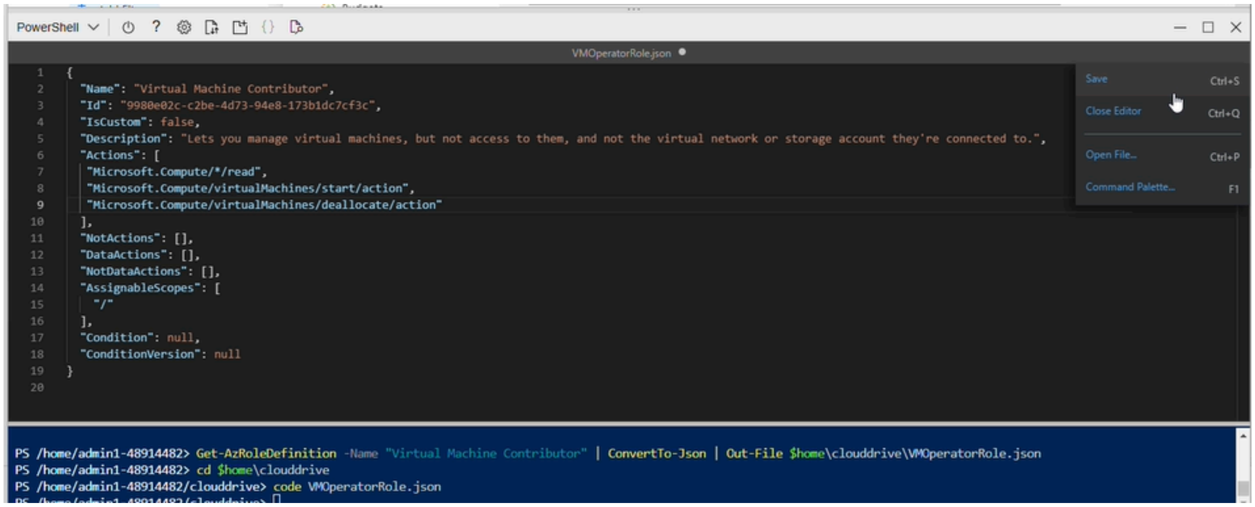
Change the code from this:



```
{
  "Name": "Virtual Machine Contributor",
  "Id": "9980e02c-c2be-4d73-94e8-173b1dc7cf3c",
  "IsCustom": false,
  "Description": "Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.",
  "Actions": [
    "Microsoft.Authorization/*/read",
    "Microsoft.Compute/availabilitySets/*",
    "Microsoft.Compute/locations/*",
    "Microsoft.Compute/virtualMachines/*",
    "Microsoft.Compute/virtualMachineScaleSets/*",
    "Microsoft.Compute/cloudServices/*",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/hostgroups/write",
    "Microsoft.Compute/hostgroups/hosts/write",
    "Microsoft.DevTestLab/schedules/*",
    "Microsoft.Insights/alertRules/*",
    "Microsoft.Network/applicationGateways/backendAddressPools/join/action",
    "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
    "Microsoft.Network/loadBalancers/inboundNatPools/join/action"
```

```
PS /home/admin1-48914482> Get-AzRoleDefinition -Name "Virtual Machine Contributor" | ConvertTo-Json | Out-File $home\clouddrive\VMOperatorRole.json
PS /home/admin1-48914482> cd $home\clouddrive
PS /home/admin1-48914482/clouddrive> code VMOperatorRole.json
PS /home/admin1-48914482/clouddrive> 
```

To this:



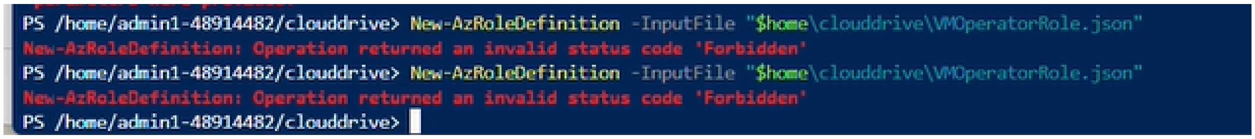
```
{
  "Name": "Virtual Machine Contributor",
  "Id": "9980e02c-c2be-4d73-94e8-173b1dc7cf3c",
  "IsCustom": false,
  "Description": "Lets you manage virtual machines, but not access to them, and not the virtual network or storage account they're connected to.",
  "Actions": [
   "Microsoft.Compute/*/read",
   "Microsoft.Compute/virtualMachines/start/action",
   "Microsoft.Compute/virtualMachines/deallocate/action"
  ],
  "NotActions": [],
  "DataActions": [],
  "NotDataActions": [],
  "AssignableScopes": [
    "/"
  ],
  "Condition": null,
  "ConditionVersion": null
}
```

```
PS /home/admin1-48914482> Get-AzRoleDefinition -Name "Virtual Machine Contributor" | ConvertTo-Json | Out-File $home\clouddrive\VMOperatorRole.json
PS /home/admin1-48914482> cd $home\clouddrive
PS /home/admin1-48914482/clouddrive> code VMOperatorRole.json
```

Then save, and close the editor

Creating a New Custom Role Using the Modified Role Definition

- *New-AzRoleDefinition -InputFile “$home\clouddrive\VMOperatorRole.json”*



```
PS /home/admin1-48914482/clouddrive> New-AzRoleDefinition -InputFile "$home\clouddrive\VMOperatorRole.json"
New-AzRoleDefinition: Operation returned an invalid status code 'Forbidden'
PS /home/admin1-48914482/clouddrive> New-AzRoleDefinition -InputFile "$home\clouddrive\VMOperatorRole.json"
New-AzRoleDefinition: Operation returned an invalid status code 'Forbidden'
PS /home/admin1-48914482/clouddrive>
```

Why Are We Getting a "Forbidden" Error?

The **forbidden error** occurs due to **restricted permissions** that prevent the current admin user from performing certain actions. To resolve this:

1. Verify that the user has the necessary **permissions**.
2. Ensure the user is assigned the appropriate **built-in or custom role** for the required operations.
3. Review **Azure role assignments** and modify them if necessary.