## Lab 8-01: Azure Key Vault

### Service Introduction

Azure Key Vault is a secure and centralized cloud service provided by Microsoft Azure for managing and safeguarding cryptographic keys, secrets, and certificates used by cloud applications and services. It acts as a key management solution that helps organizations protect sensitive information, such as API keys, connection strings, and encryption keys, by storing them in a highly secure and compliant manner. Azure Key Vault provides features like access policies, access logging, and hardware security modules (HSMs) to ensure robust security and compliance with regulatory requirements. Developers can seamlessly integrate Azure Key Vault into their applications, and it plays a crucial role in enhancing overall security posture by allowing for the separation of application secrets from the application code, enabling secure and dynamic management of cryptographic keys and other sensitive information.

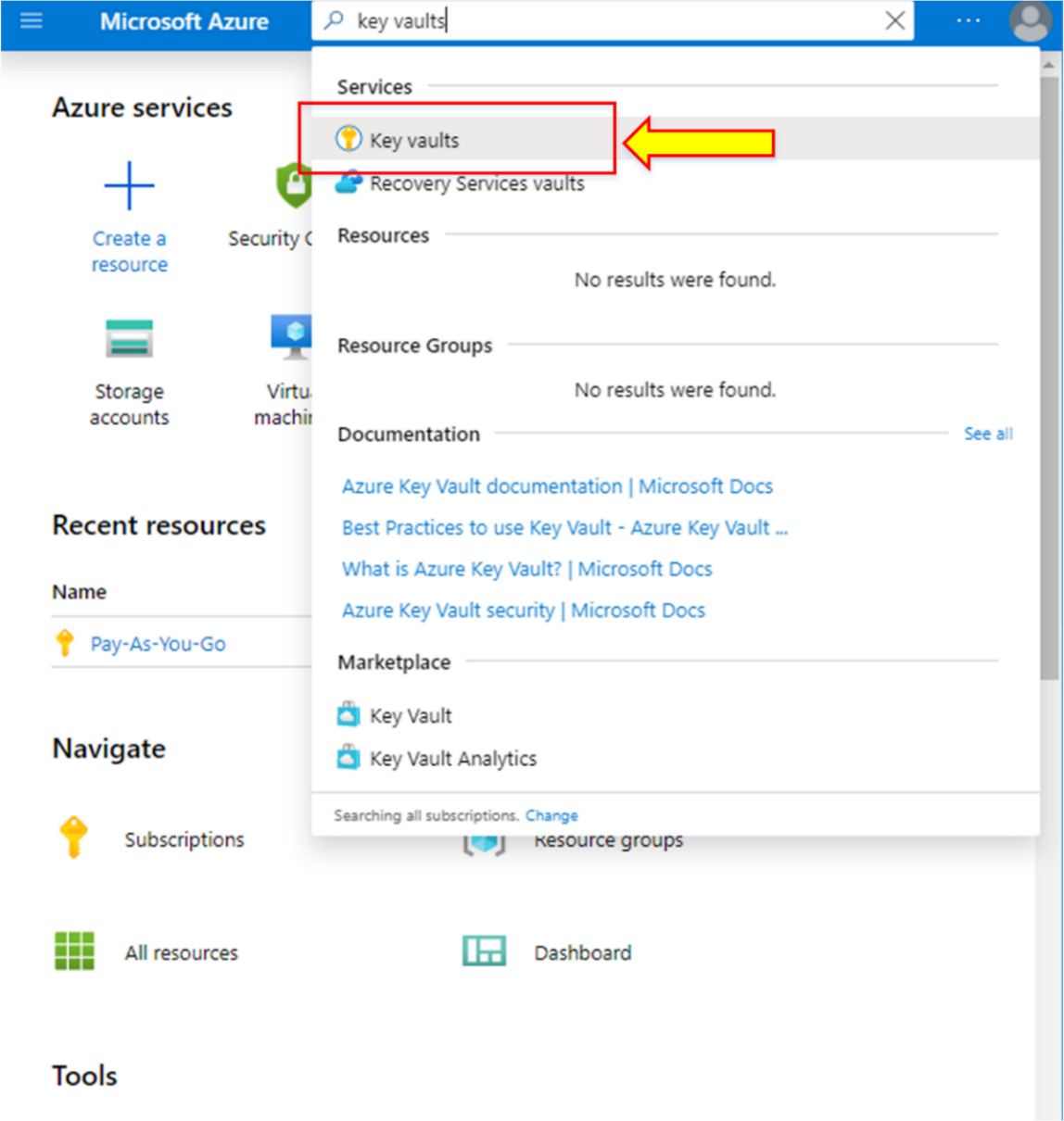
### Problem

An organization must share a secret with a third party for business enhancement. How can the organization build an access policy for others to share its secret without revealing the encryption and security rules, ensuring secure internet traffic?

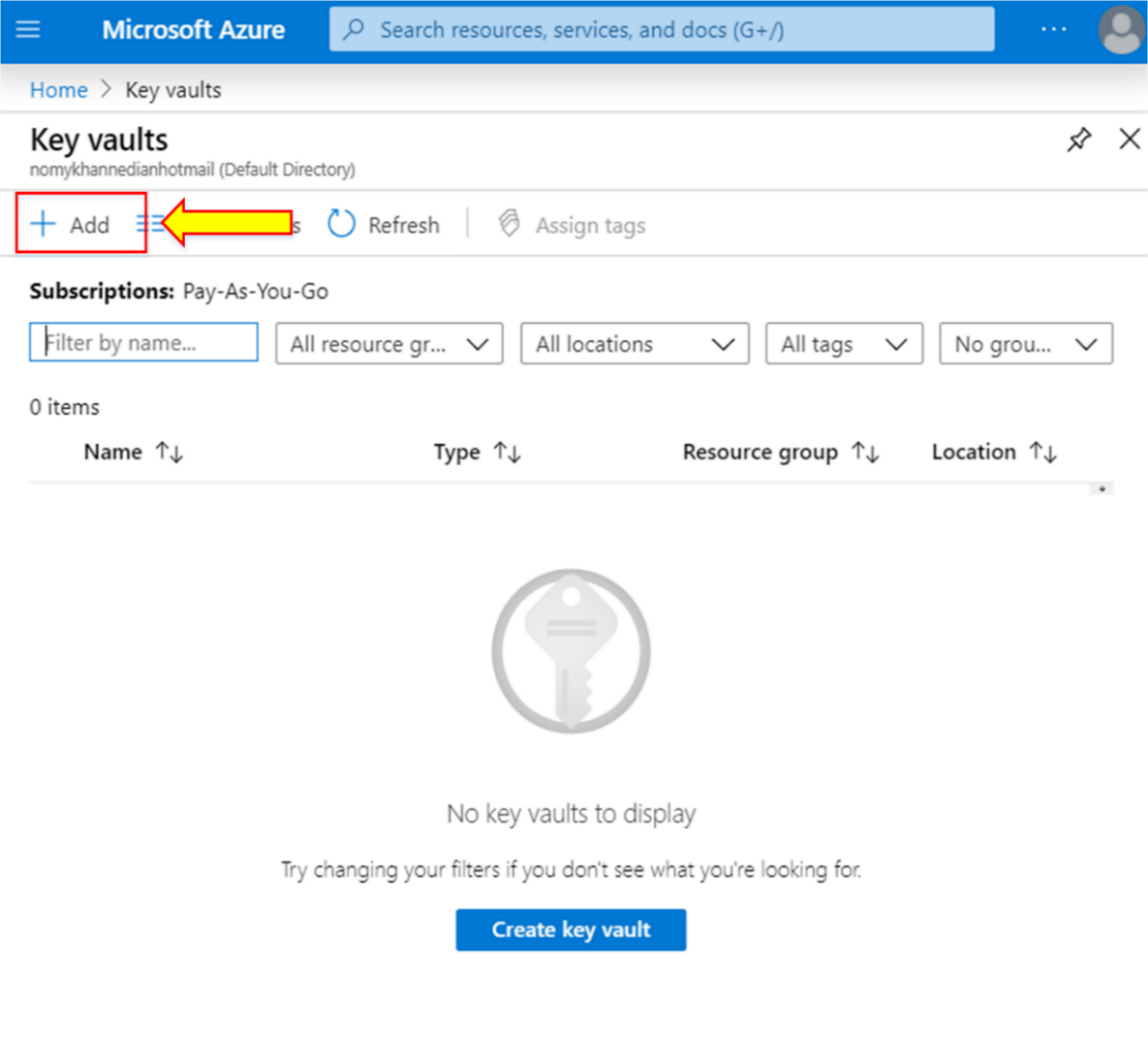
### Solution

Azure Key Vault is a useful tool for managing and sharing secrets. First, Azure Key Vault is created, then a secret is built in the given Key Vault that can be accessible to others. In the given situation, the organization can allow others to access the secret without revealing the secret by using Azure Key Vault.

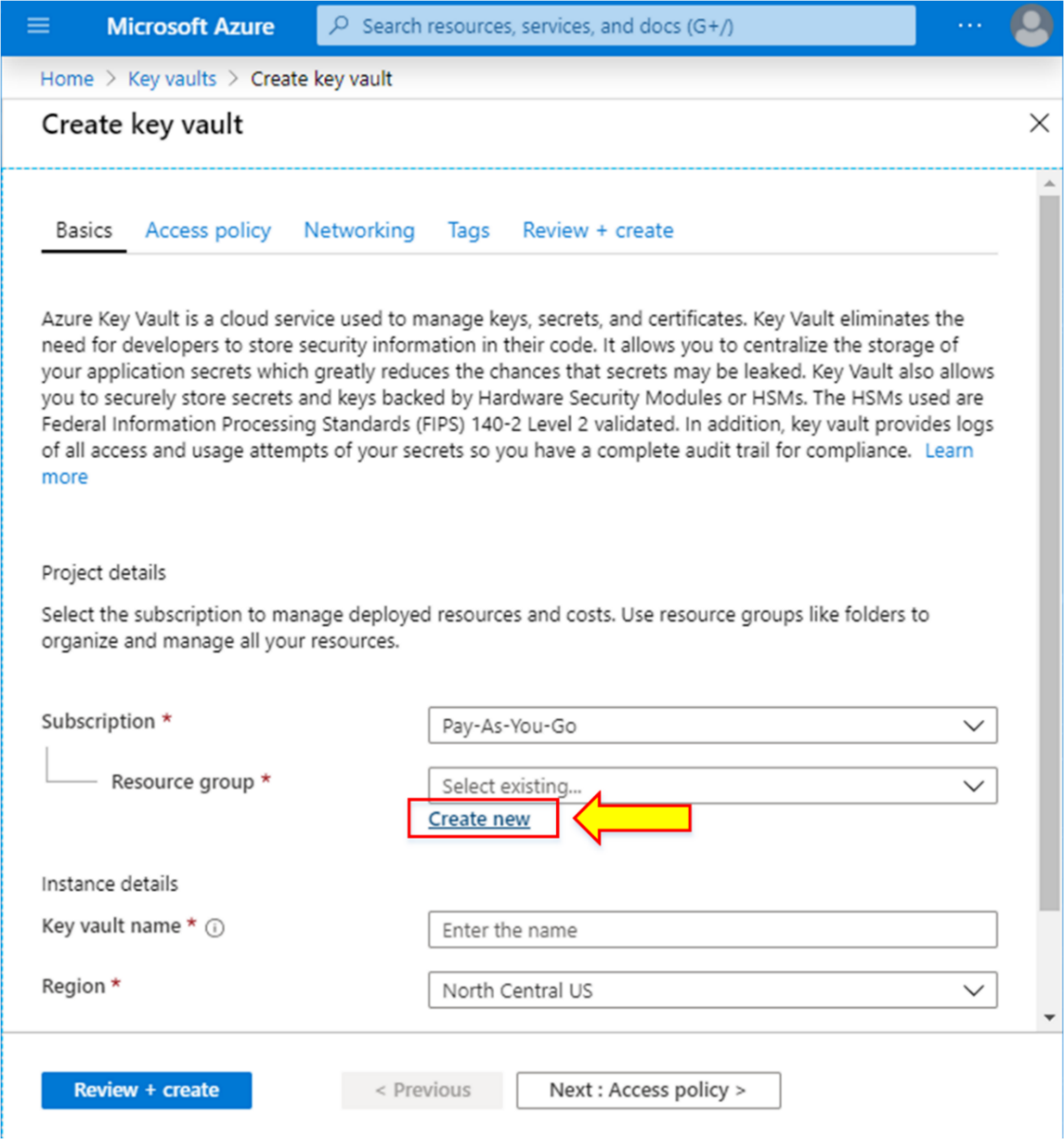
1. Log in to the Microsoft Azure portal, go to the search bar, and type **“Key Vaults”** in the given space.



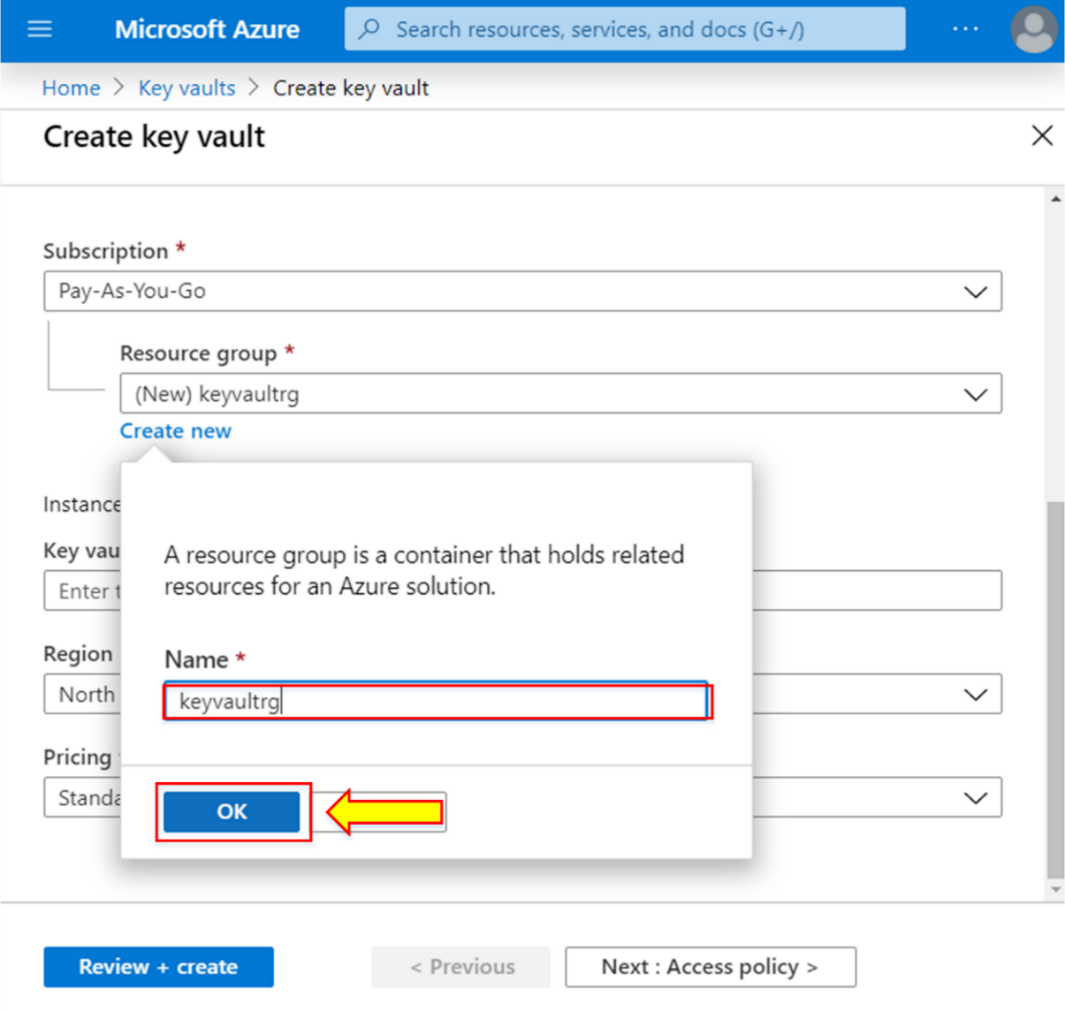
1. The “**Key Vaults**” tab will appear. Click on **“+ Add”** to create a Key Vault.



1. Click on “**Create new**” to enter the Resource group.



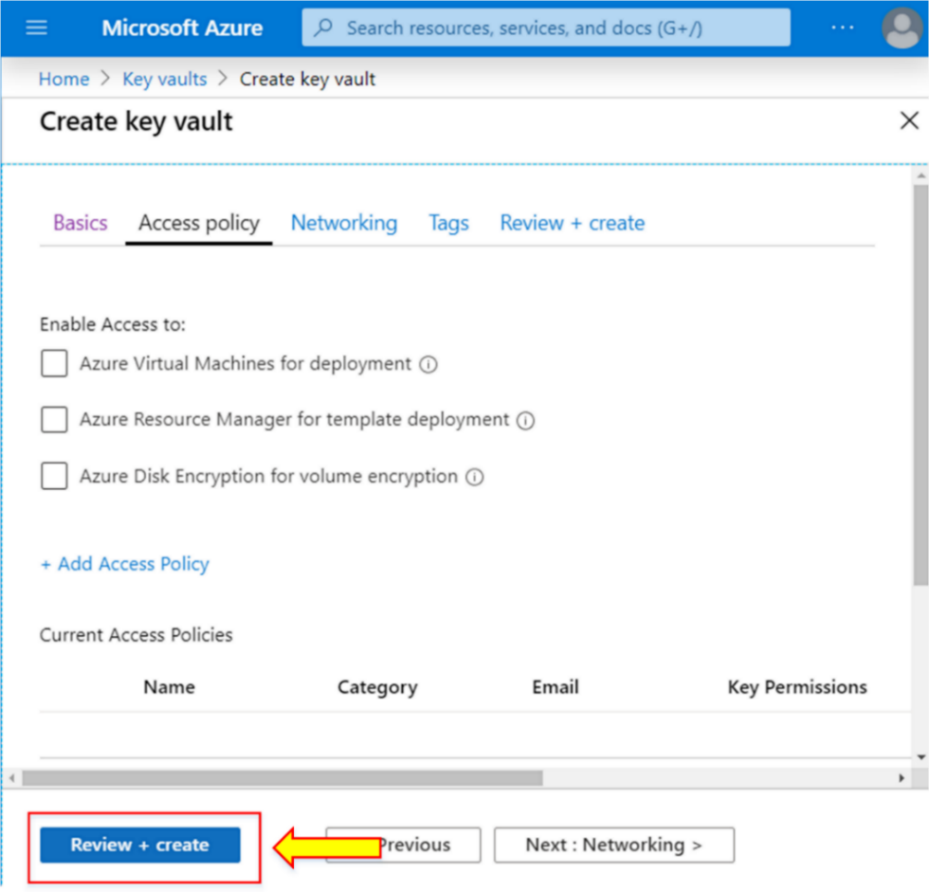
1. Write the name of the Resource group as “**keyvaultrg.”**
2. Then click on “**OK.”**



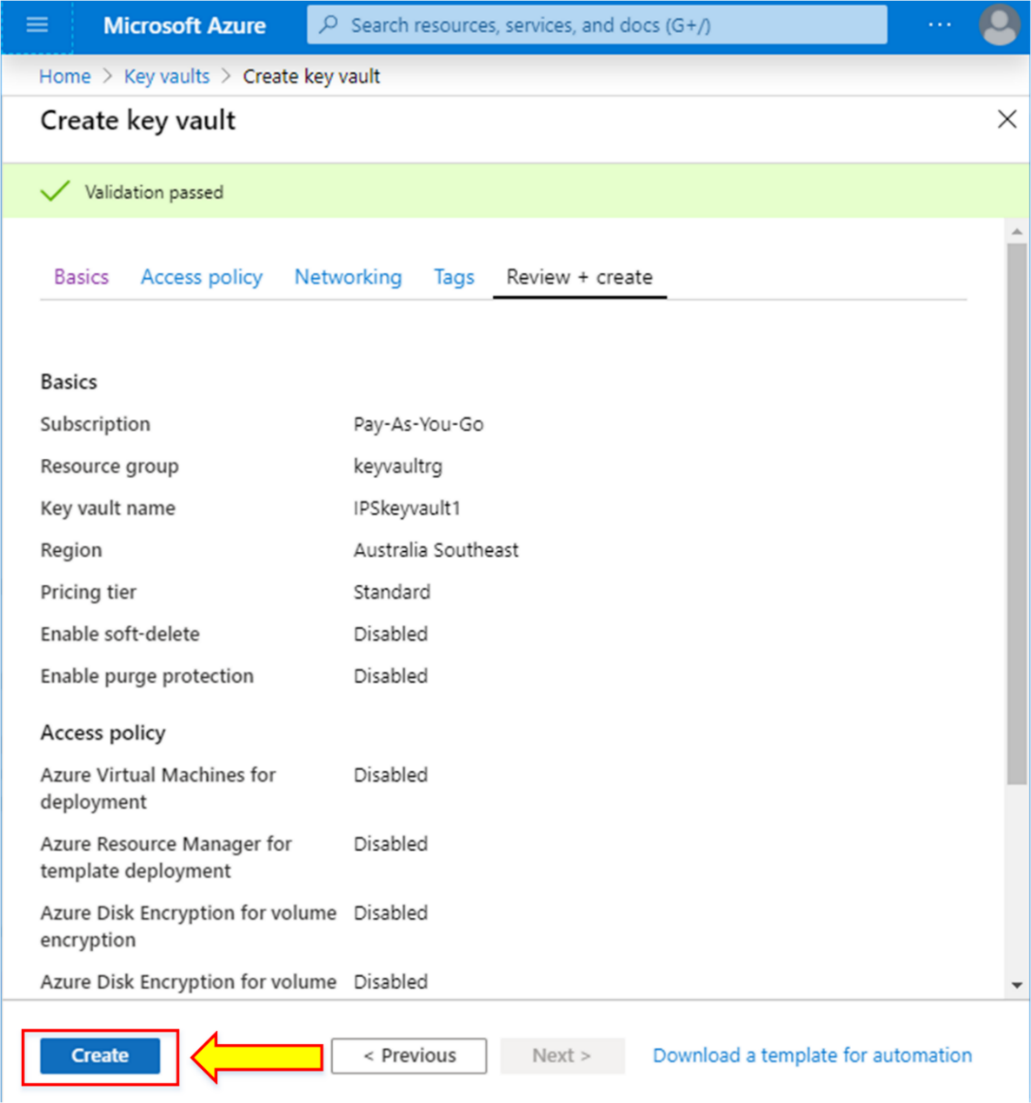
1. Write “**Key Vault name\*,”** “**Region\*,”** and “**Pricing tier\*”** in the **“Instance details.”**
2. Now, click on “**Next: Access policy >.”**



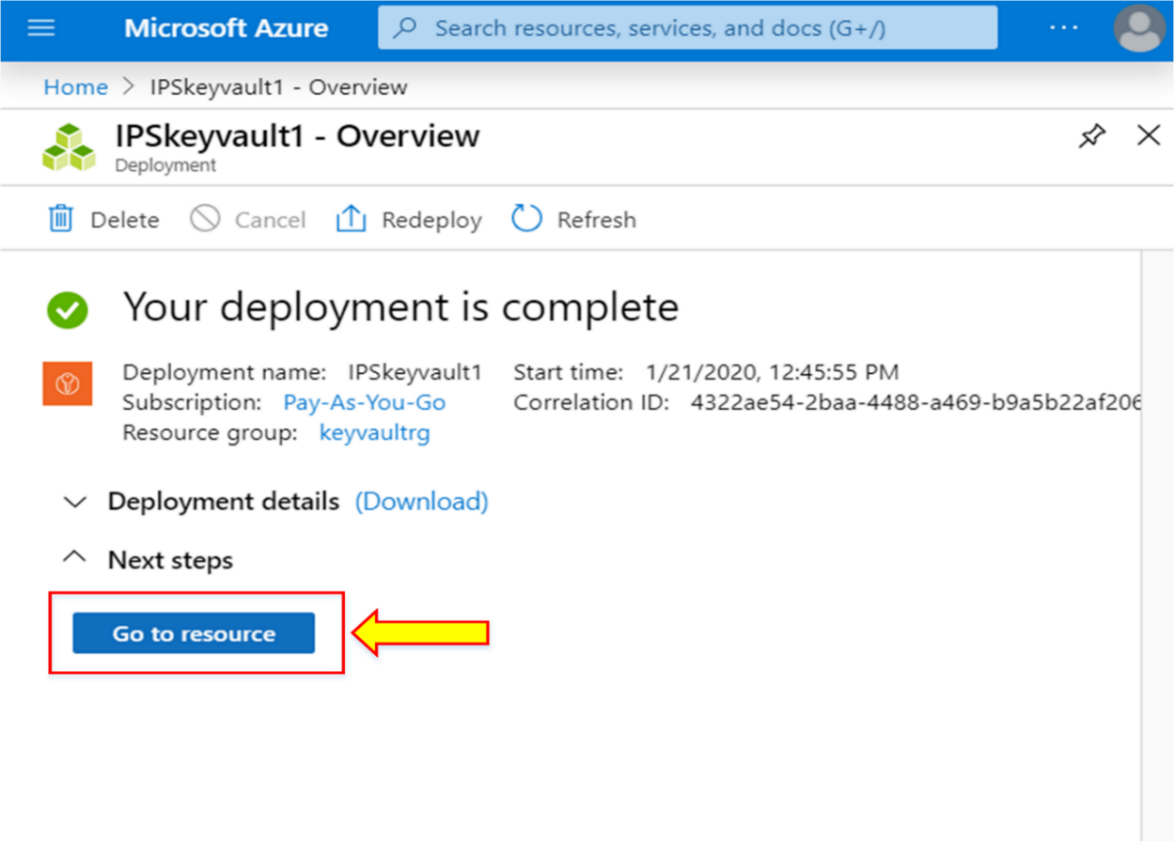
1. The access policy tab will appear. Now, click on “**Review + create.”**



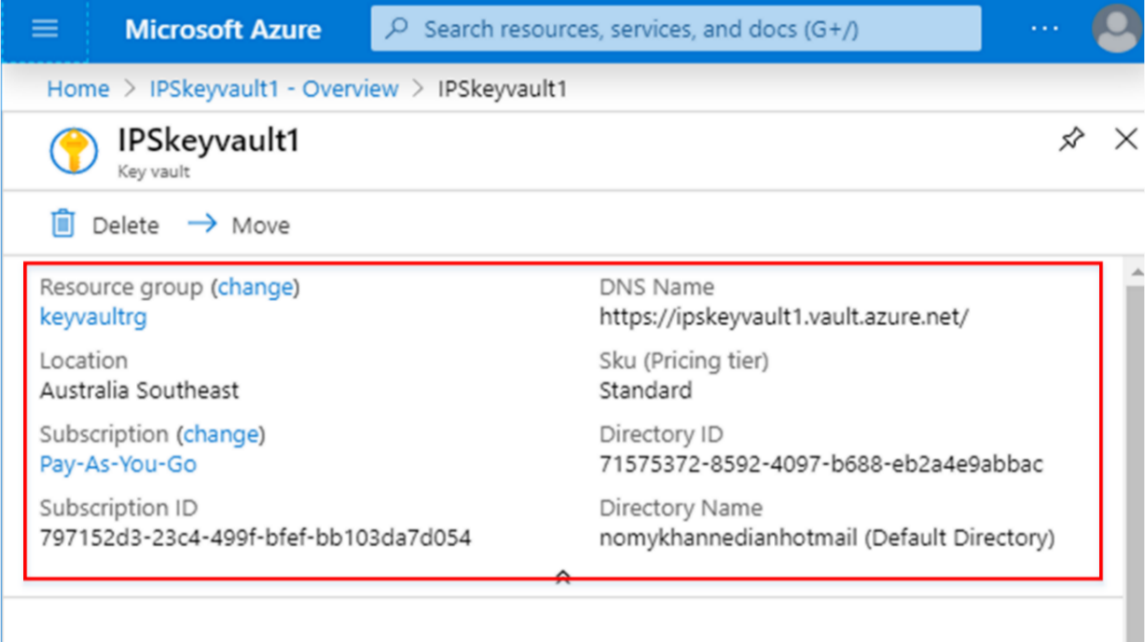
1. Once the validation is passed, click on “**Create.”**



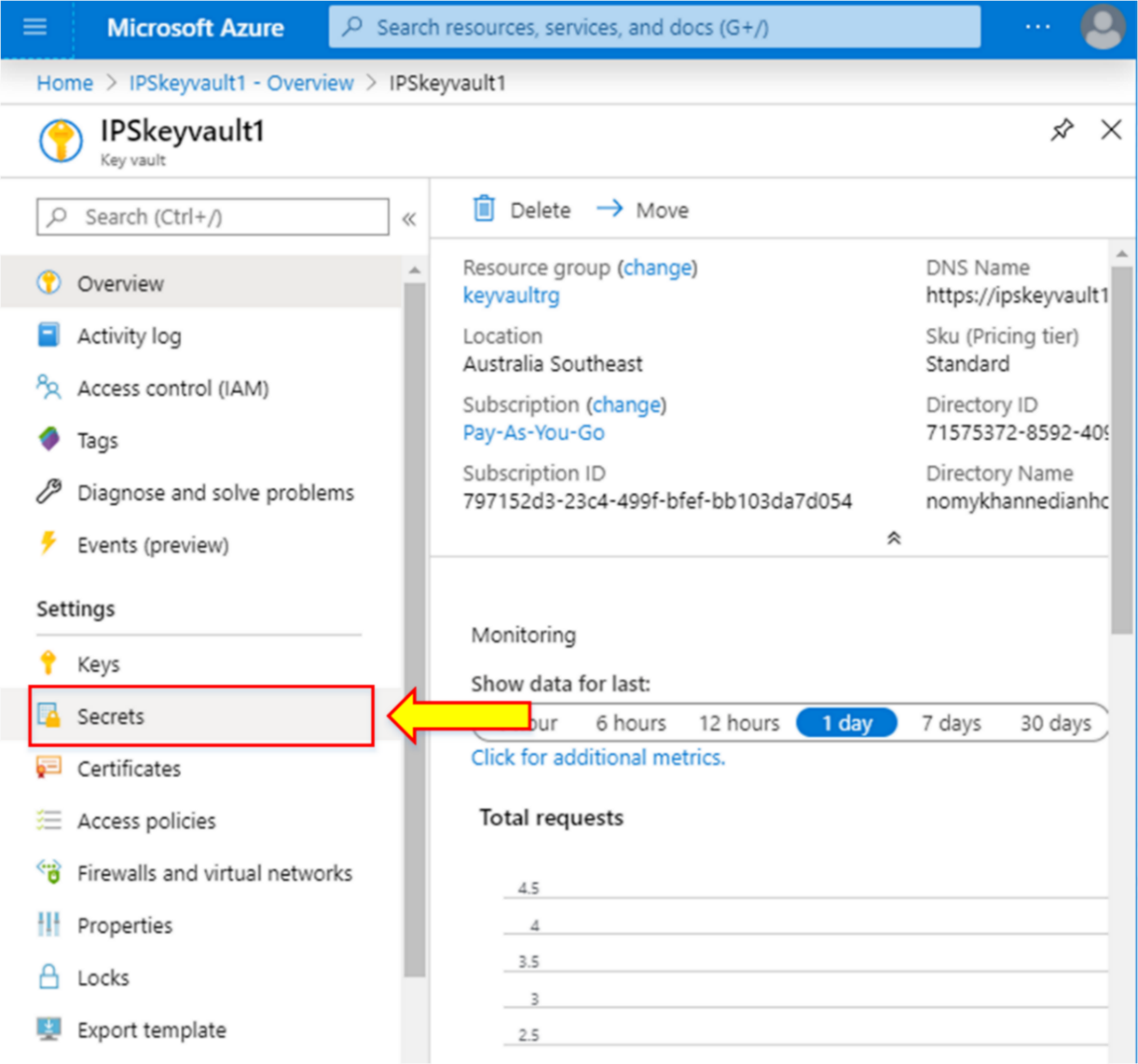
1. “**IPSKeyvault1”** has been created.
2. Click on “**Go to resource.”**



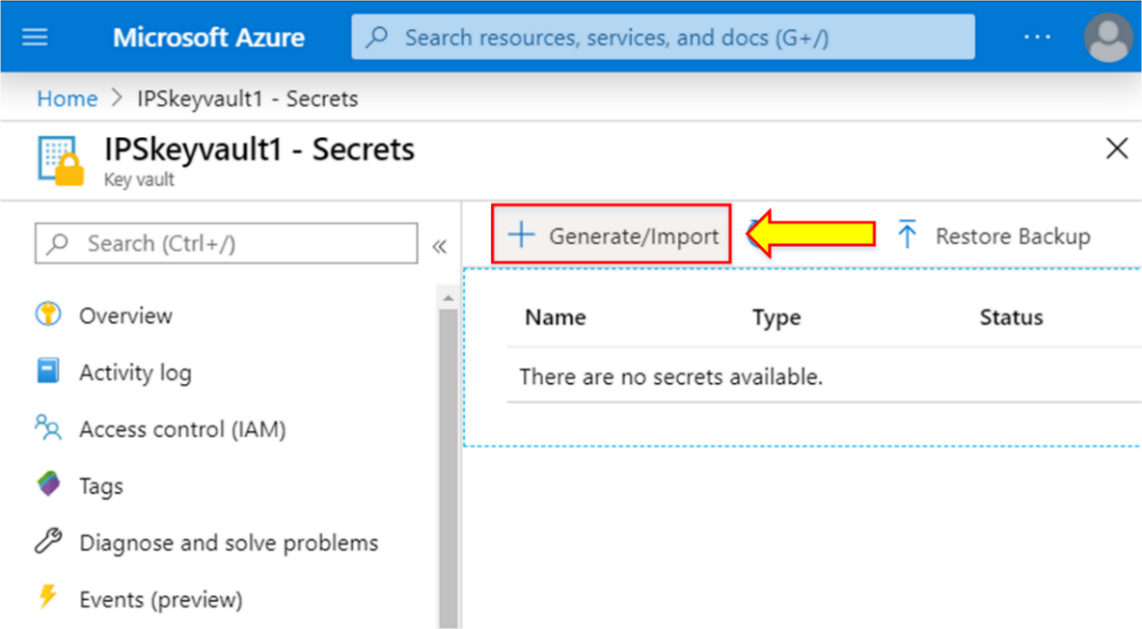
1. The details of the created Key Vault will have appeared.



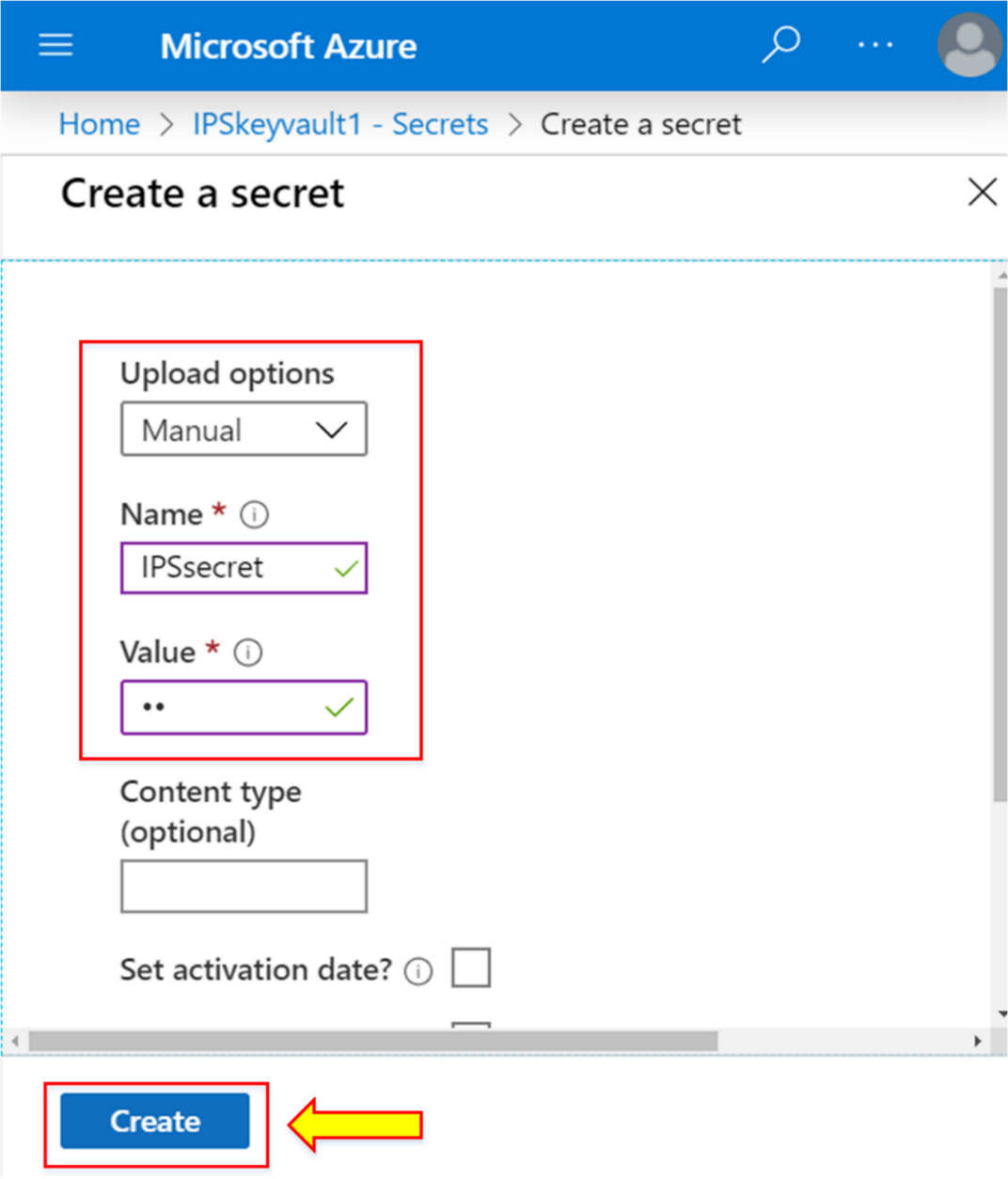
1. To add a secret, click on “**Secret”** from the left side of the **IPSkeyvault1** tab.



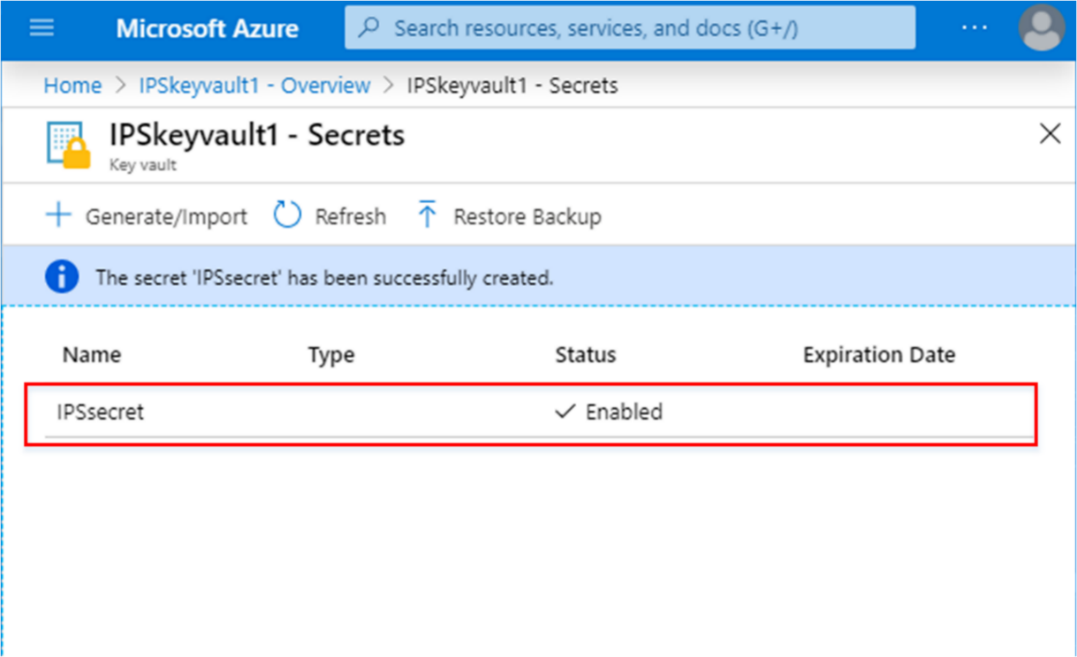
1. Click on **“+ Generate/Import”** to add a secret.



1. Select “**Manual”** from the Upload options.
2. Write “**Name\*”** and **“Value\*”** of the secret.
3. Click on “**Create.”**



1. The secret “**IPSsecret”** has been successfully created.



## Lab 8-02: Network Access to VM using NSG

### Service Introduction

Network Security Groups (NSGs) in Microsoft Azure play a pivotal role in controlling network access to virtual machines (VMs). NSGs act as virtual firewalls, allowing or denying inbound and outbound traffic to VMs based on defined rules. By associating NSGs with VMs, administrators can regulate access by specifying allowed protocols, source IP addresses, and destination ports. This fine-grained control enhances security by restricting unnecessary traffic and mitigating potential vulnerabilities. Whether applied at the subnet or individual VM level, NSGs provide a crucial layer of network defense, helping organizations maintain a secure and compliant network environment within the Azure cloud infrastructure. Through thoughtful configuration of NSG rules, administrators can enforce network access policies tailored to their specific security requirements, ensuring a robust defense against unauthorized access to virtual machines.

Top of Form

### Problem

A company has recently shifted all its on-prem resources to the Azure cloud and now wants to explore the services offered by Azure. The security and management team is currently assigned to create a secure way to access the web server through a virtual machine. How can they do that?

### Solution

By using the Network Security Group feature of Azure, the organization can easily make secure network access to Azure virtual machines.

|  |
| --- |
| 1. Log in to the **Microsoft Azure** portal.   C:\Users\ad\Desktop\Azure_Pic\cr_1.png   1. Go to the options present at the top of the portal page. 2. Click on **Azure Cloud Shell**.   C:\Users\ad\Desktop\Azure_Pic\az_1.png   1. Click on **“Create storage.”**   C:\Users\ad\Desktop\Azure_Pic\az_2.png  **Note:** Azure Cloud Shell requires an Azure files share to persist files. This will create a new storage account with some monthly costs.   1. The Azure Cloud Shell session will be connected in a moment.   C:\Users\ad\Desktop\Azure_Pic\sc_15.png   1. Run “**az”** to connect to the Azure CLI session.   C:\Users\ad\Desktop\Azure_Pic\az_3.png  **Note:** Azure CLI enables you to set the default values. Azure CLI allows you to create and place your desired virtual machine in several default locations and regions.   1. The Azure CLI session will be connected in a moment. 2. After that, run the following set of commands to create a virtual machine.   az vm create \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --name ipsvm01 \  --image UbuntuLTS \  --admin-username azureuser \  --generate-ssh-keys     1. The command will take some time to deploy the VM and display the following updates:      1. After the deployment, the following output will appear, showing all the configuration details.     **Note:** You can verify the deployment of the VM from Azure Portal.   1. After deployment, run the following command to configure the Nginx on the recently deployed virtual machine.   az vm extension set \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --vm-name ipsvm01 \  --name customScript \  --publisher Microsoft.Azure.Extensions \  --version 2.1 \  --settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \  --protected-settings '{"commandToExecute": "./configure-nginx.sh"}'     1. The following output will appear.      1. To see the list of Azure VM IP addresses, run the following command:   IPADDRESS="$(az vm list-ip-addresses \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --name ipsvm01 \  --query "[].virtualMachine.network.publicIpAddresses[\*].ipAddress" \  --output tsv)"    **Note:** The above set of commands will store the IP address of the virtual machine in the bash variable.   1. After that, run the following command to download the homepage of the webserver.   curl --connect-timeout 5 http://$IPADDRESS     1. Run the following command to get the VM IP address.   echo $IPADDRESS     1. Copy this IP address and open it in a new browser.      1. You will find that access is currently blocked to access this VM.      1. To verify the access, run the following command to view the network security group list.   az network nsg list \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --query '[].name' \  --output tsv     1. You will get the NSG name in the output.      1. After that, run the set of commands and see the output.   az network nsg rule list \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --nsg-name ipsvm01NSG     1. Run the following set of commands to view the NSG rule list.   az network nsg rule list \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --nsg-name ipsvm01NSG \  --query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \  --output table     1. To create an NSG rule, run the following set of commands:   az network nsg rule create \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --nsg-name ipsvm01NSG \  --name allow-http \  --protocol tcp \  --priority 100 \  --destination-port-ranges 80 \  --access Allow     1. The following output will appear.      1. Now, run the following commands to check the NSG rule list.   az network nsg rule list \  --resource-group learn-3894d88b-13a0-4bf7-ad8b-13861b5a2e4f \  --nsg-name ipsvm01NSG \  --query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \  --output table  28. You will see the new NSG rule in the list.     1. Now, run the following command to access the webserver again.   curl --connect-timeout 5 <http://$IPADDRESS>     1. Verify the above output by navigating to the same VM IP address. |