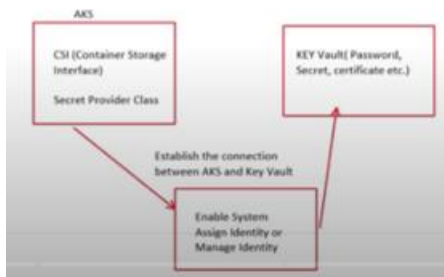


Key Vault Integration In AKS

Method One: Securing Secrets with Azure Key Vault Using Managed Identity

- Enable the CSI Driver In AKS
- Create Key Vault
- Enable Key Vault Add-on In AKS
- Enable System Assign Identity or Managed Identity in AKS
- Create Secret provide Class and Pod deployment in AKS
- Verify status in AKS



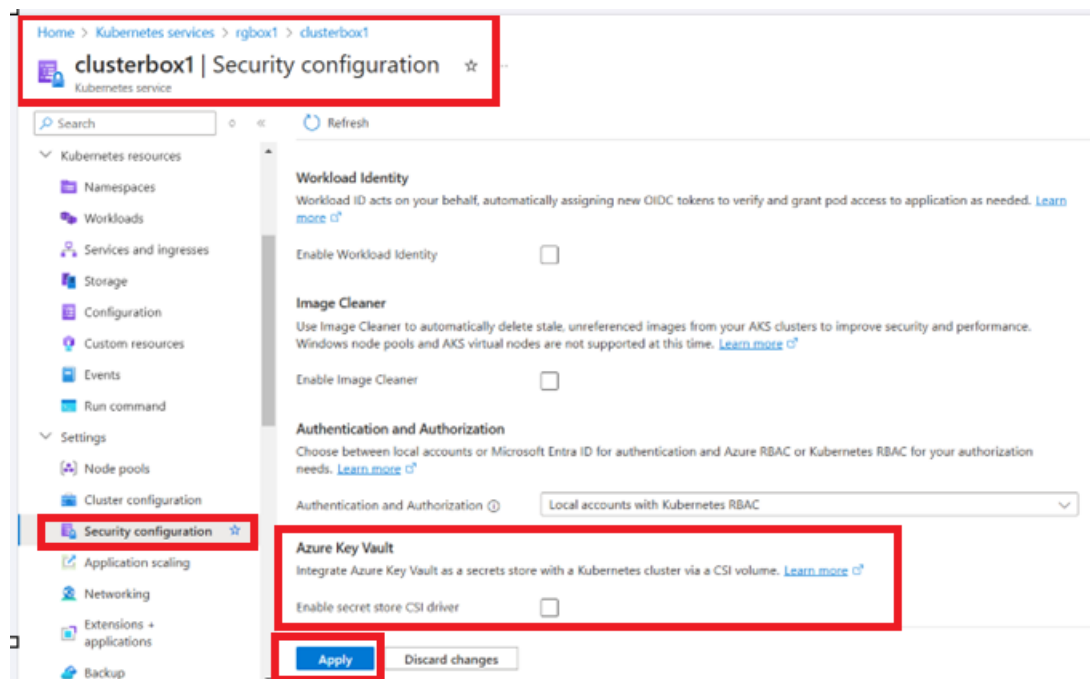
Step1: Enabling the Secret Store CSI Driver in AKS

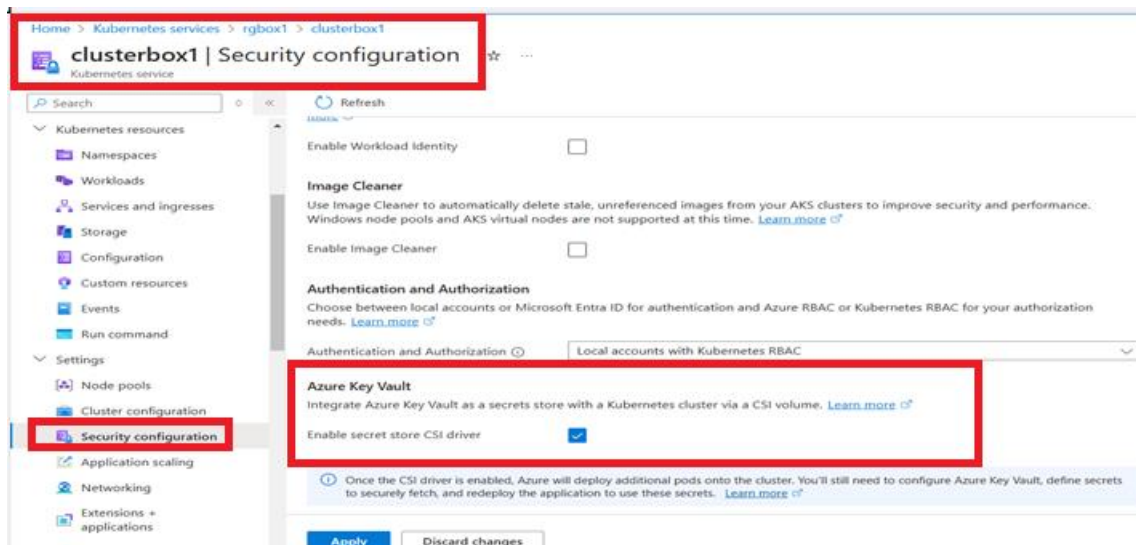
CLI Method to Enable the CSI Driver in AKS

```
az aks update --name clusterbox1 --resource-group rgbox1 --enable-disk-driver --enable-file-driver --enable-blob-driver --enable-snapshot-controller
```

```
az aks update --name clusterbox1 --resource-group rgbox1 --enable-secret-store-csi-driver
```

GUI Method to Enable the CSI Driver in AKS





Step2: Verify Installation in AKS

kubect get pods -n kube-system

```
PS F:\> kubectl get csidrivers
NAME          ATTACHREQUIRED  PODINFOONMOUNT  STORAGECAPACITY  TOKENREQUESTS  REQUIRESREPUBLISH  MODES                      AGE
blob.csi.azure.com  false           true             false             api://AzureADTokenExchange  false              Persistent,Ephemeral      100m
disk.csi.azure.com  true            false            false             <unset>         false              Persistent                 4h47m
file.csi.azure.com  false           true             false             api://AzureADTokenExchange  false              Persistent,Ephemeral      4h47m
PS F:\>
```

Step3: Set Up Azure Key Vault

i. Create an Azure Key Vault

CLI Method to Create Azure Key Vault in AKS

az keyvault create --name satkeyvault --resource-group rgbox1 --location eastus

Create a key vault

Create new

Instance details

Key vault name *

arkeyvault0

Region *

East US

Pricing tier *

Standard

Recovery options

Soft delete protection will automatically be enabled on this key vault. This feature allows you to recover or permanently delete a key vault and secrets for the duration of the retention period. This protection applies to the key vault and the secrets stored within the key vault.

To enforce a mandatory retention period and prevent the permanent deletion of key vaults or secrets prior to the retention period elapsing, you can turn on purge protection. When purge protection is enabled, secrets cannot be purged by users or by Microsoft.

Soft-delete

Enabled

Days to retain deleted vaults *

90

Purge protection

- ☒ Disable purge protection (allow key vault and objects to be purged during retention period)
- ☐ Enable purge protection (enforce a mandatory retention period for deleted

Previous

Next

Review + create

Create a key vault

Grant data plane access by using a Azure RBAC or Key Vault access policy

- ☐ Azure role-based access control (recommended)
- ☒ Vault access policy

Resource access

- ☐ Azure Virtual Machines for deployment
- ☐ Azure Resource Manager for template deployment
- ☐ Azure Disk Encryption for volume encryption

Access policies

Access policies enable you to have fine grained control over access to vault items. [Learn more](#)

+ Create Edit Delete

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
------	-------	-----------------	--------------------	-------------------------

Satish Ranjan	SatishRanjan@drgaauravraj1993@gmail.onmicros...	Get, List, Update, Create, Import, Delete, Recov...	Get, List, Set, Delete, Recover, Backup, Restore	Get, List, Update, Create, Import, Delete, Recov...
---------------	---	---	--	---

Previous

Next

Review + create

Give feedback

Home > Key vaults >

Create a key vault

Basics Access configuration Networking Tags **Review + create**

Review + create

Basics

Subscription	Free Trial
Resource group	e2e-rg
Key vault name	rankeyvault
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access configuration

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled

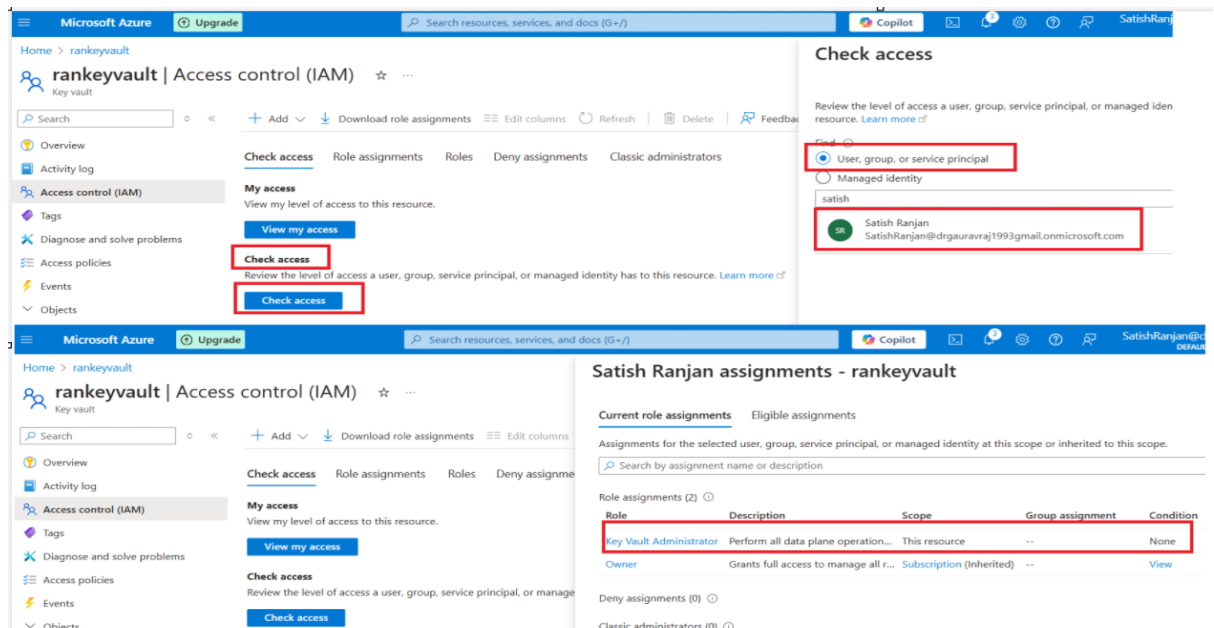
Previous Next **Create**

ii. Key Vault Administrator role in Azure Key Vault's IAM (Identity and Access Management)

GUI

The sequence of screenshots illustrates the process of assigning the Key Vault Administrator role:

- Screenshot 1:** Shows the Azure portal navigation pane. The 'Access control (IAM)' option is highlighted in the left sidebar. A red box highlights the 'rankeyvault' key vault in the top navigation bar.
- Screenshot 2:** Shows the 'Access control (IAM)' page for the 'rankeyvault' key vault. The 'Access control (IAM)' tab is selected. A red box highlights the 'Add role assignment' button.
- Screenshot 3:** Shows the 'Add role assignment' page. The 'Key Vault Administrator' role is selected from the 'Selected role' dropdown. A red box highlights the 'Key Vault Administrator' role. The 'Members' section shows 'Sateish Rangan' as the selected member.
- Screenshot 4:** Shows the 'Review + assign' page. The 'Review + assign' button is highlighted in red.

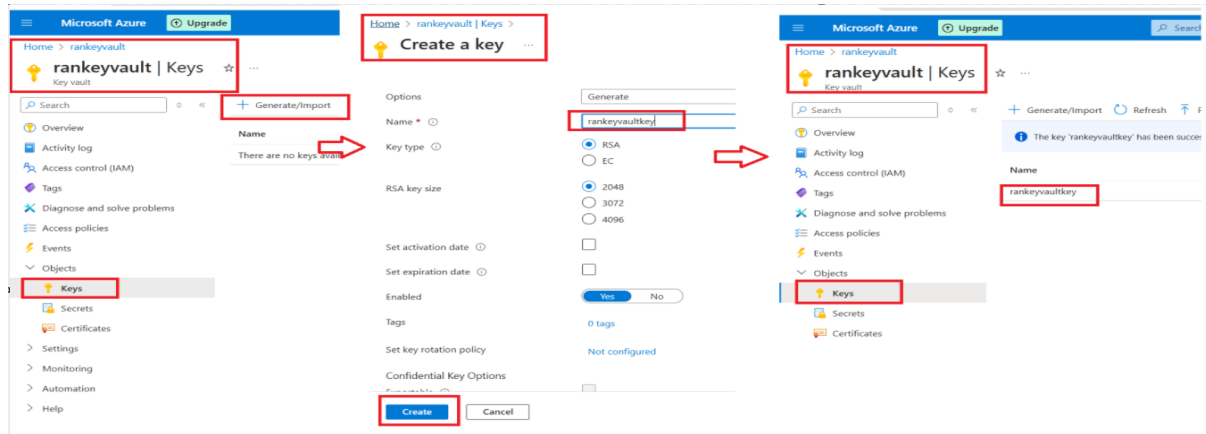


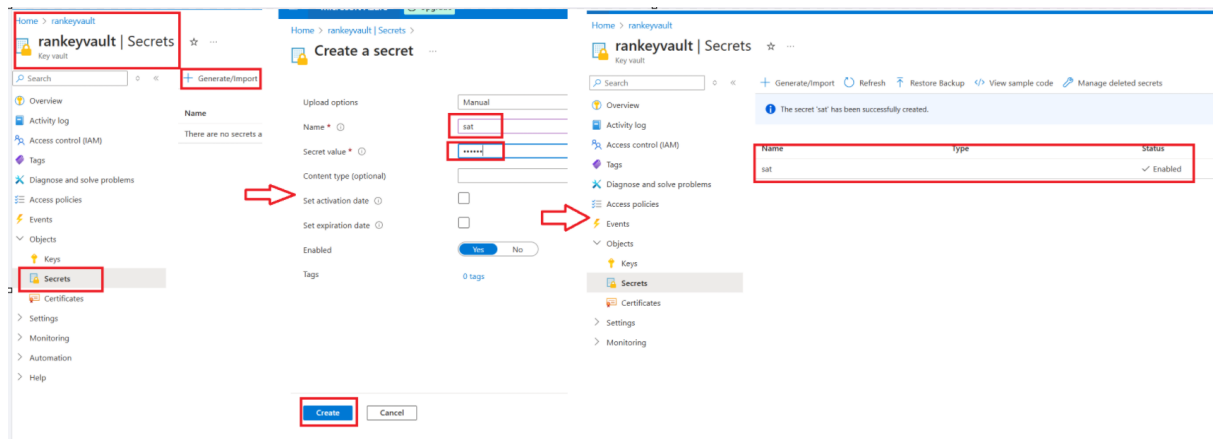
iii. Add Secrets to the Vault

CLI

az keyvault secret set --vault-name satkeyvault --name MySecret --value "SuperSecretValue"

GUI





iv. Enable KeyVault Add-on in AKS Or Enable CSI / Enable CSI Driver

CLI

az aks enable-addons --addons azure-keyvault-secrets-provider --name clusterbox1 --resource-group rgbox1

To Verify

kubectl get pod -n kube-system

```
PS F:\> kubectl get pod -n kube-system
```

NAME	READY	STATUS	RESTARTS	AGE
aks-secrets-store-csi-driver-mr5vr	3/3	Running	0	7m8s
aks-secrets-store-csi-driver-v98kz	3/3	Running	0	7m8s
aks-secrets-store-provider-azure-cmng4	1/1	Running	0	7m8s
aks-secrets-store-provider-azure-zcj68	1/1	Running	0	7m8s
azure-cns-2nldz	1/1	Running	0	6h20m
azure-cns-bj74t	1/1	Running	0	6h20m

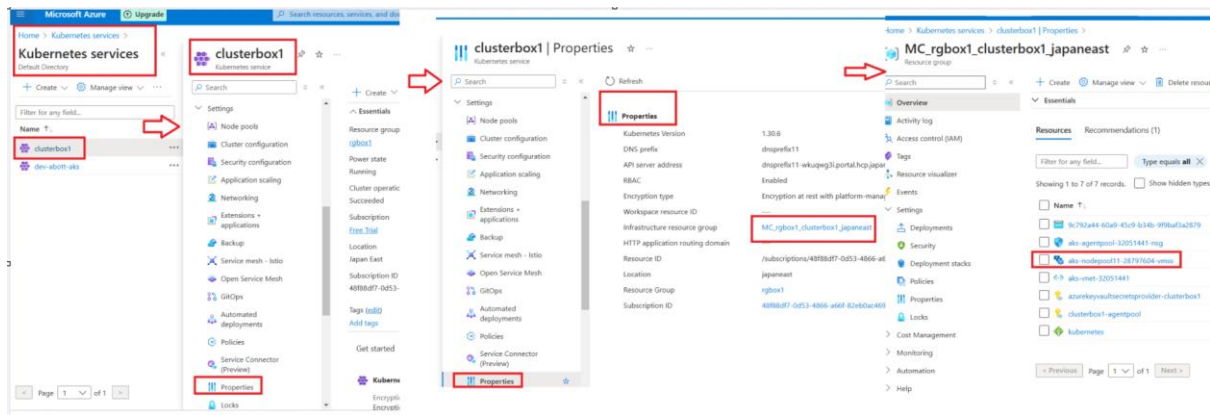
Step4: Enable System Assign Identity or Managed Identity in AKS and Key Vault

Permission of Managed Identity at AKS Side

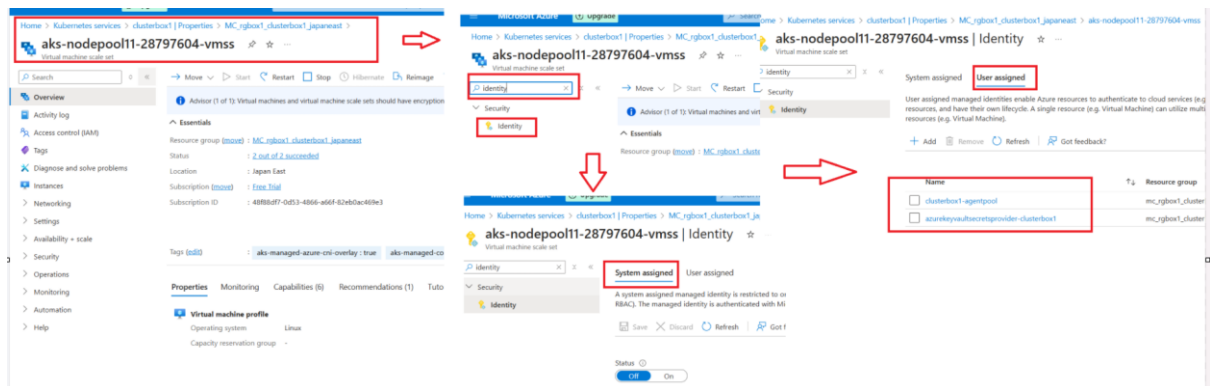
CLI

az aks update -g MyResourceGroup -n MyAKSCluster --assign-identity

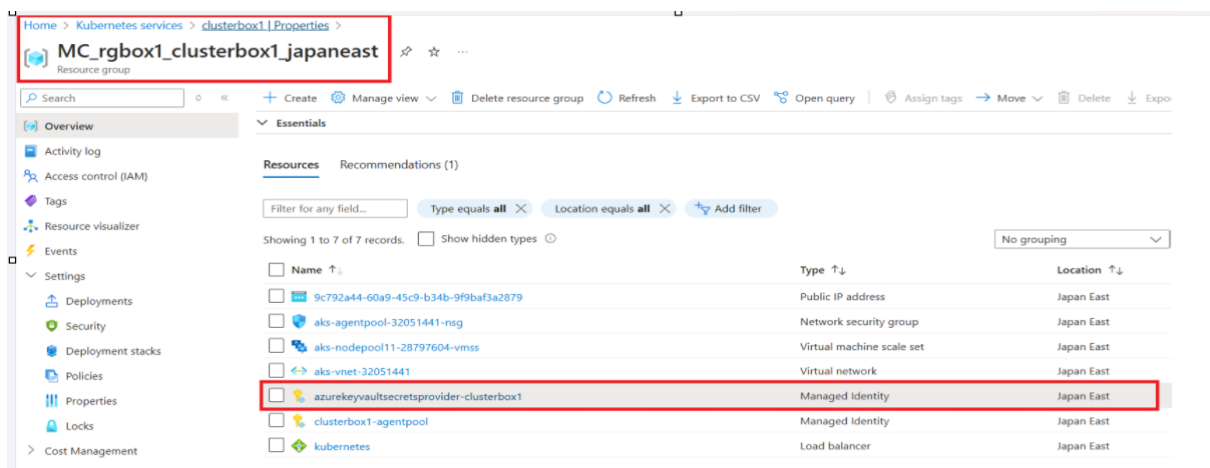
GUI



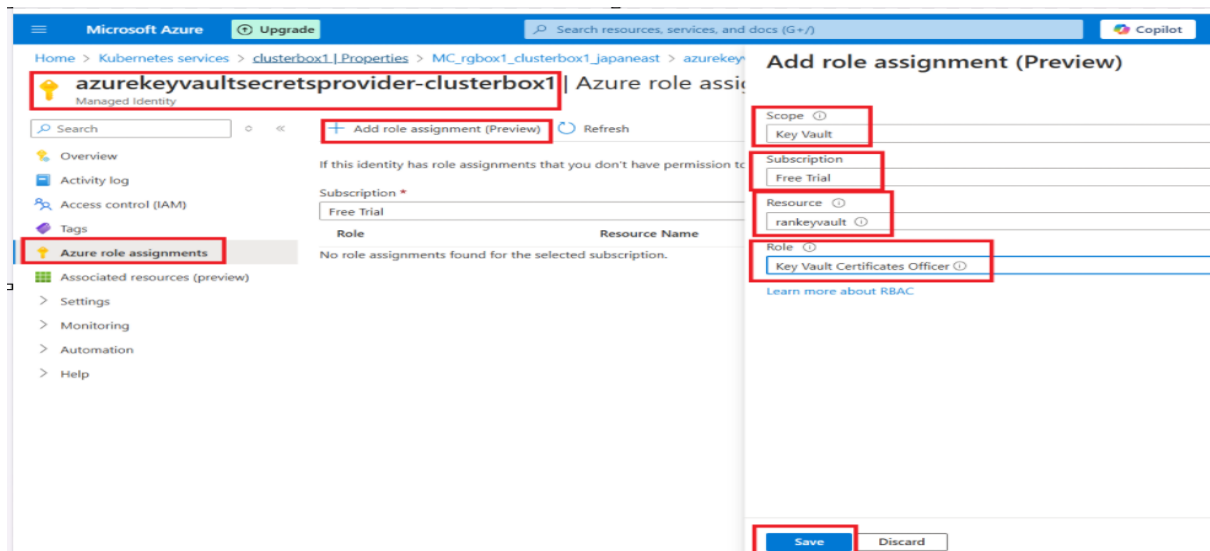
Here in VMSS given system and user identity, but we need to use managed identity,



But we will go with the Managed Identity, by default when enable the azure key vault provider in AKS , by default it created the managed identity.



Now Need to Assign Key vault certificate officer role for this managed identity.



Home > Kubernetes services > clusterbox1 | Properties > MC_rgbox1_clusterbox1_japaneast > azurekeyvaultsecretsprovider-clusterbox1

azurekeyvaultsecretsprovider-clusterbox1 | Azure role assignments ☆ ...

Managed Identity

Search Add role assignment (Preview) Refresh

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *
Free Trial

Role	Resource Name	Resource Type	Assigned To	Condition
Key Vault Certificates Officer	rankeyvault	Key vault	azurekeyvaultsecretsprovider-cluster...	None

Overview
Activity log
Access control (IAM)
Tags
Azure role assignments
Associated resources (preview)
Settings
Monitoring
Automation
Help

To Verify

Microsoft Azure Upgrade Search resources, services, and docs (G+)

Home > Kubernetes services > clusterbox1 | Properties > MC_rgbox1_clusterbox1_japaneast > aks-nodepool11-28797604-vmss

aks-nodepool11-28797604-vmss | Identity ☆ ...

Virtual machine scale set

Search ide

Diagnose and solve problems
Security
Identity
Help

Support + Troubleshooting

System assigned User assigned

User assigned managed identities enable Azure resources to authenticate to cloud services (e.g. Azure Key Vault) without storing credentials in code. This type of managed identities are created resources, and have their own lifecycle. A single resource (e.g. Virtual Machine) can utilize multiple user assigned managed identities. Similarly, a single user assigned managed identity can be st resources (e.g. Virtual Machine).

+ Add Remove Refresh Got feedback?

Name	Resource group	Subscription
<input type="checkbox"/> clusterbox1-agentpool	mc_rgbox1_clusterbox1_japaneast	48f88df7-0d53-4866-a66f-82eb0ac469e3
<input type="checkbox"/> azurekeyvaultsecretsprovider-clusterbox1	mc_rgbox1_clusterbox1_japaneast	48f88df7-0d53-4866-a66f-82eb0ac469e3

Give Required Permission to Managed Identity at Key Vault Side

CLI

az keyvault set-policy -n MyKeyVault --secret-permissions get --spn <aks-identity-client-id>

GUI

Microsoft Azure Upgrade Search resources, services, and docs (G+/J) Copilot

Home > **Key vaults** Default Directory

+ Create Manage deleted vaults Manage view Refresh Export to CSV Open query Assign tags

Filter for any field... Subscription equals all Resource group equals all Location equals all Add filter

Showing 1 to 3 of 3 records.

Name	Type	Resource group	Location	Subscription
arkeyvault1	Key vault	rgbox1	East US	Free Trial

Microsoft Azure Upgrade Search resources, services, and docs (G+/J)

Home > Key vaults > arkeyvault1

Key vaults Default Directory

+ Create

Filter for any field...

Name arkeyvault1 rankeyvault satkeyvault

arkeyvault1 | Access policies

+ Create Refresh Delete Edit

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Access policies Events

Access policies enable you to have fine grained control over access

Search Permissions: All Type

Showing 1 to 1 of 1 records.

Name	Email
USER	
Satish Ranjan	SatishRanjan@drgauravraj...

Home > Key vaults > arkeyvault1 | Access policies > Create an access policy

Permissions Principal Application (optional) Review + create

Configure from a template Select a template

Key permissions

Key Management Operations

Select all

Get List Update Create Import Delete Recover Backup Restore

Secret permissions

Secret Management Operations

Select all

Get List Set Delete Recover Backup Restore

Privileged Secret Operations

Select all

Certificate permissions

Certificate Management Operations

Select all

Get List Update Create Import Delete Recover Backup Restore

Create an access policy

Permissions Principal Application (optional) Review + create

Only 1 principal can be assigned per access policy. Use the new embedded experience to select a principal. The previous experience is deprecated.

Search azureke azurekeyvaultsecretsprovider-clusterbox1 5027e56a-585e-4fc9-98cd-e67ef07de448 azurekeyvaultsecretsprovider-dev-abott-aks 1243d6e3-feab-47eb-989-897b5efcc5a8

Selected item

azurekeyvaultsecretsprovider-clusterbox1 5027e56a-585e-4fc9-98cd-e67ef07de448

Managed identity

Previous Next

Key Permissions

Key Management Operations None selected

Cryptographic Operations None selected

Privileged Key Operations None selected

Rotation Policy Operations None selected

Secret Permissions

Secret Management Operations All selected

Privileged Secret Operations None selected

Certificate Permissions

Certificate Management Operations None selected

Privileged Certificate Operations None selected

Principal

Principal name azurekeyvaultsecretsprovider-clusterbox1

Object ID 44c3b0ef-36a1-4283-9988-5d807977e45e

Previous Create

Home > Key vaults > arkeyvault1

Key vaults Default Directory

+ Create

Filter for any field...

Name arkeyvault1 rankeyvault satkeyvault

arkeyvault1 | Access policies

+ Create Refresh Delete Edit

Overview Activity log Access control (IAM) Tags Diagnose and solve problems Access policies Events Objects

Access policies enable you to have fine grained control over access to vault items. Learn more

Search Permissions: All Type: All

Showing 1 to 2 of 2 records.

Name	Email	Key Permissions	Secret Permissions	Certificate Permissions
APPLICATION				
azurekeyvaultsecretsprovid...		Get, List, Set, Delete, Recov...		
USER				
Satish Ranjan	SatishRanjan@drgauravraj...	Get, List, Update, Create, I...	Get, List, Set, Delete, Recov...	Get, List, Update, Create, I...

Step5: Configure and Deploy to Kubernetes

1. Create a SecretProviderClass for VM Managed Identity:

Yaml File for SecretProviderClass

```
apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: azure-kvname-system-mi
  namespace: default
spec:
  parameters:
    cloudName: AzurePublicCloud
    keyvaultName: aksdemopg
    objects: |
      array:
      - |
        objectName: pgpassword
        objectType: secret          # object types: secret, key, or cert
        objectVersion: ""          # [OPTIONAL] object versions, default to
    tenantId: 4cd93cbc-b026-4c7d-86f1-76fcb7292573 # The Directory ID of the
    usePodIdentity: "false"
    useVMManagedIdentity: "true"
    userAssignedIdentityID: 3457145b-5926-4a60-8d5f-7bb929192891 #Manage iden
  provider: azure
```

2. Deploy Your Application:

```
apiVersion: v1
kind: Pod
metadata:
  name: busybox-secrets-store-inline-system-mi
  namespace: default
spec:
  containers:
  - name: busybox
    image: k8s.gcr.io/e2e-test-images/busybox:1.29-4
    command:
    - /bin/sleep
    - '10000'
    resources: {}
    volumeMounts:
    - name: secrets-store01-inline
      readOnly: true
      mountPath: /mnt/secrets-store
  volumes:
  - name: secrets-store01-inline
    csi:
      driver: secrets-store.csi.k8s.io
      readOnly: true
      volumeAttributes:
        secretProviderClass: azure-kvname-system-mi
```

Step 5: Access Your Secrets

```
PS C:\Users\NIRAV> kubectl exec busybox-secrets-store-inline-system-mi -- ls /mnt/secrets-store/
postgrespw
PS C:\Users\NIRAV> kubectl exec busybox-secrets-store-inline-system-mi -- cat /mnt/secrets-store/postgrespw
password
PS C:\Users\NIRAV>
```

cat /mnt/secrets-store/MySecret

Method 2: Securing Secrets with Azure Key Vault Using User Assigned Identity

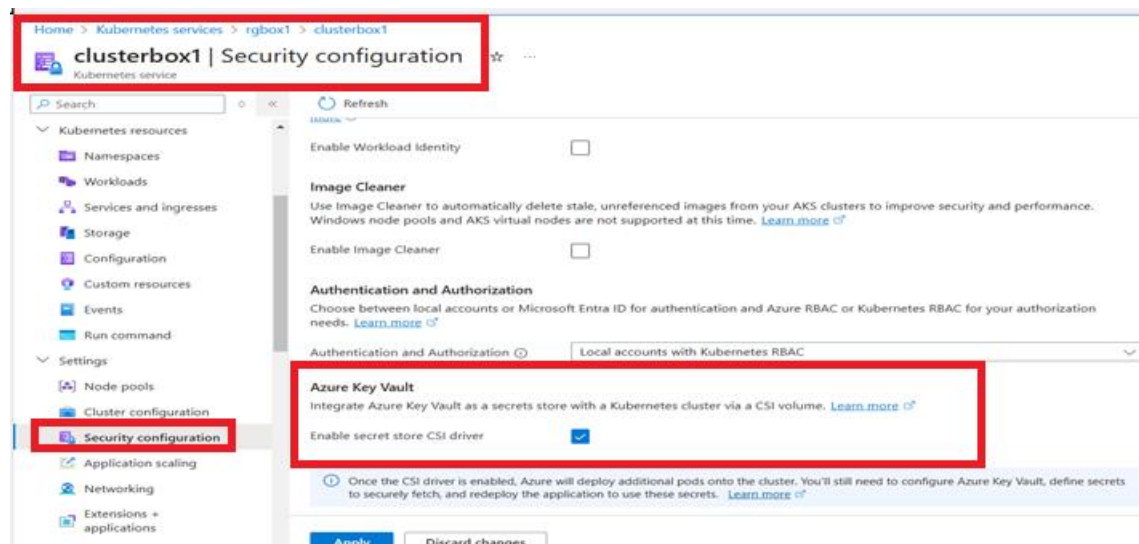
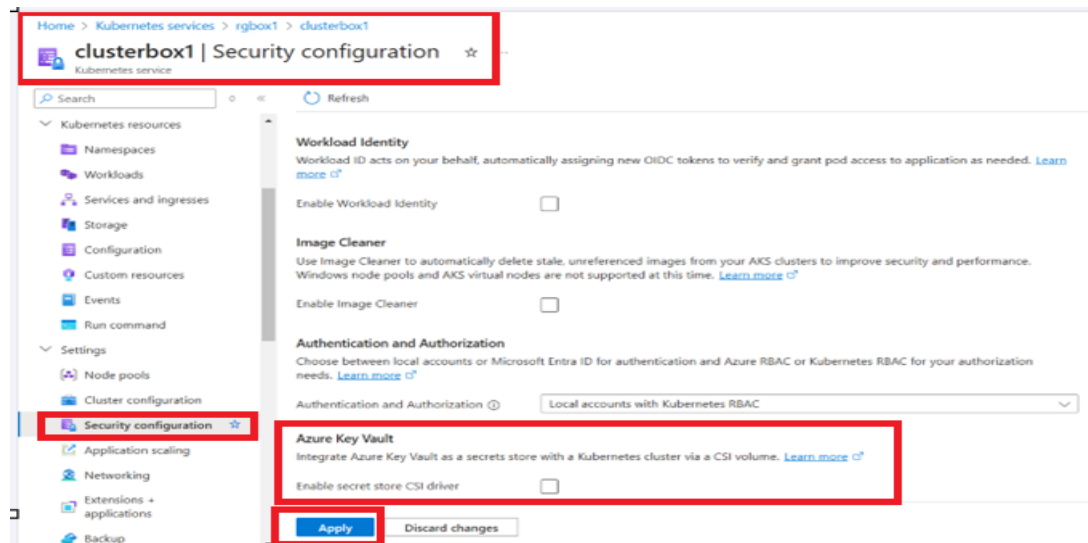
Step1: Enabling the Secret Store CSI Driver in AKS

CLI Method to Enable the CSI Driver in AKS

```
az aks update --name clusterbox1 --resource-group rgbox1 --enable-disk-driver --enable-file-driver --enable-blob-driver --enable-snapshot-controller
```

```
az aks update --name clusterbox1 --resource-group rgbox1 --enable-secret-store-csi-driver
```

GUI Method to Enable the CSI Driver in AKS



Step2: Verify Installation in AKS

```
kubectl get pods -n kube-system
```

```
PS F:\> kubectl get csidrivers
NAME                                ATTACHREQUIRED  PODINFOONMOUNT  STORAGECAPACITY  TOKENREQUESTS  REQUIRESREUBLISH  MODES                                AGE
blob.csi.azure.com                 false           true             false             api://AzureADTokenExchange  false             Persistent,Ephemeral  100m
disk.csi.azure.com                  true            false            false             <unset>         false             Persistent             4h47m
file.csi.azure.com                  false           true             false             api://AzureADTokenExchange  false             Persistent,Ephemeral  4h47m
PS F:\>
```

Step3: Set Up Azure Key Vault

i. Create an Azure Key Vault

CLI Method to Create Azure Key Vault in AKS

```
az keyvault create --name satkeyvault --resource-group rgbox1 --location eastus
```

Home > Key vaults >

Create a key vault

Create new

Instance details

Key vault name * ⓘ

Region *

Pricing tier * ⓘ

Recovery options

Soft delete ⓘ Enabled

Days to retain deleted vaults * ⓘ

Purge protection ⓘ

☒ Disable purge protection (allow key vault and objects to be purged during retention period)

☐ Enable purge protection (enforce a mandatory retention period for deleted

Previous **Next** Review + create

Home > Key vaults >

Create a key vault

Grant data plane access by using a Azure RBAC or Key Vault access policy

☐ Azure role-based access control (recommended) ⓘ

☒ Vault access policy ⓘ

Resource access

☐ Azure Virtual Machines for deployment ⓘ

☐ Azure Resource Manager for template deployment ⓘ

☐ Azure Disk Encryption for volume encryption ⓘ

Access policies

Access policies enable you to have fine grained control over access to vault items. [Learn more](#)

+ Create Edit Delete

Name ↑	Email ↑	Key Permissions	Secret Permissions	Certificate Permissions
+ Add user				
<input type="checkbox"/> Satish Ranjan	SatishRanjan@dgauravraj1993@gmail.onmicros...	Get, List, Update, Create, Import, Delete, Recov...	Get, List, Set, Delete, Recover, Backup, Restore	Get, List, Update, Create, Import, Delete, Recov...

Previous Next **Review + create**

[Give feedback](#)

Home > Key vaults >

Create a key vault

Basics Access configuration Networking Tags **Review + create**

Review + create

Basics

Subscription	Free Trial
Resource group	e2e-rg
Key vault name	rankeyvault
Region	East US
Pricing tier	Standard
Soft-delete	Enabled
Purge protection during retention period	Disabled
Days to retain deleted vaults	90 days

Access configuration

Azure Virtual Machines for deployment	Disabled
Azure Resource Manager for template deployment	Disabled
Azure Disk Encryption for volume encryption	Disabled

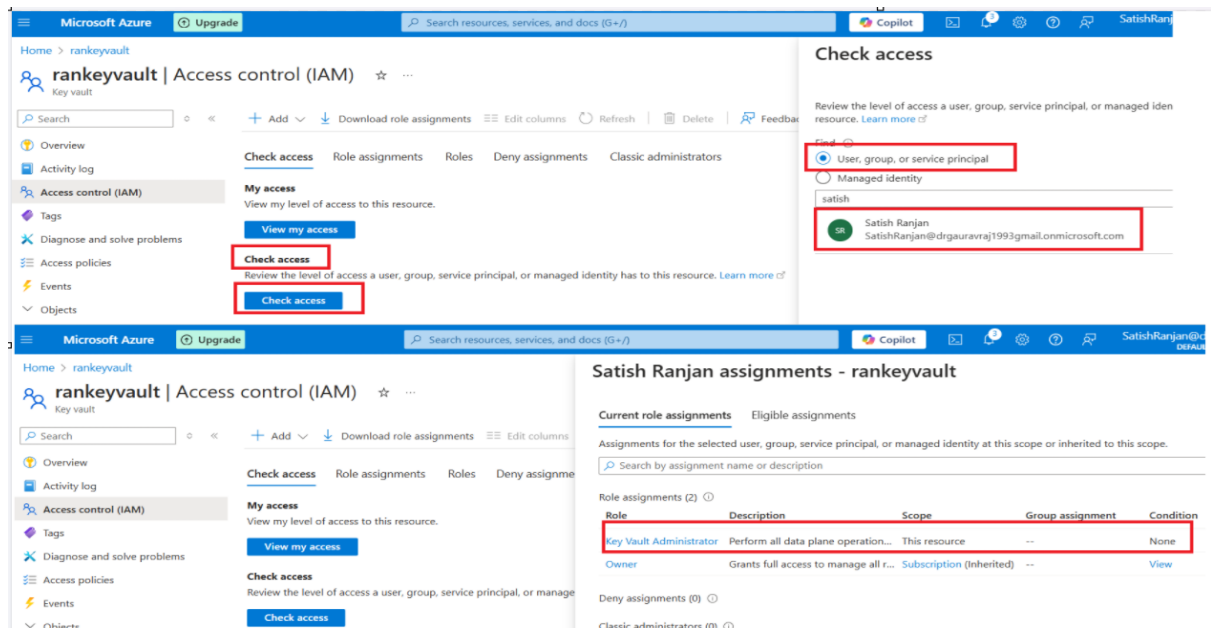
Previous Next **Create**

ii. Key Vault Administrator role in Azure Key Vault's IAM (Identity and Access Management)

GUI

The sequence of screenshots illustrates the process of assigning the Key Vault Administrator role:

- Screenshot 1:** Shows the Azure portal navigation pane. The 'Access control (IAM)' option is highlighted in the left sidebar. A red box highlights the 'rankeyvault' key vault in the top navigation bar.
- Screenshot 2:** Shows the 'Access control (IAM)' page for the 'rankeyvault' key vault. The 'Access control (IAM)' option is highlighted in the left sidebar. A red box highlights the 'Add role assignment' button.
- Screenshot 3:** Shows the 'Add role assignment' page. The 'Key Vault Administrator' role is selected from the 'Role' dropdown. A red box highlights the 'Key Vault Administrator' role. A red box highlights the 'Members' section, where the user 'Sathish Rangan' is selected.
- Screenshot 4:** Shows the 'Add role assignment' page with the 'Key Vault Administrator' role assigned to the user 'Sathish Rangan'. The 'Review + assign' button is highlighted in a red box.

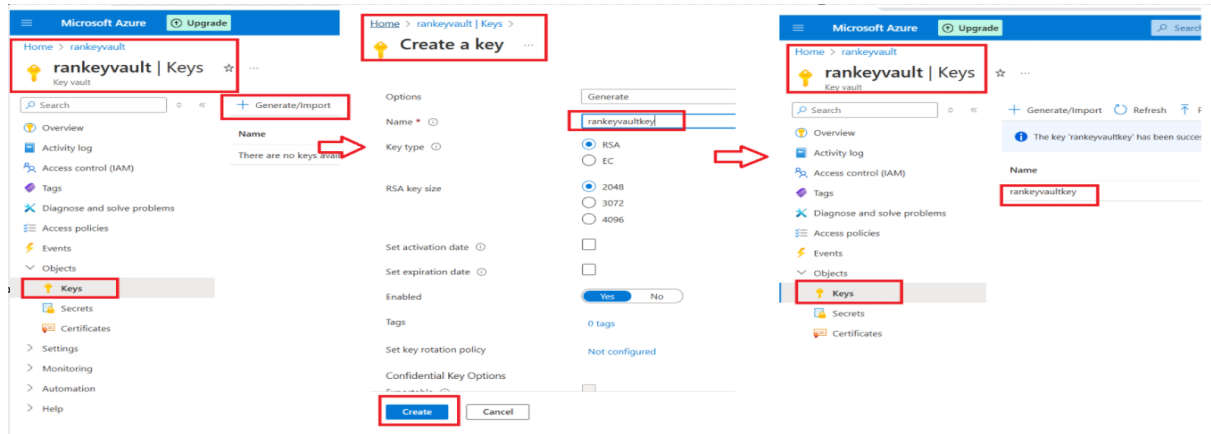


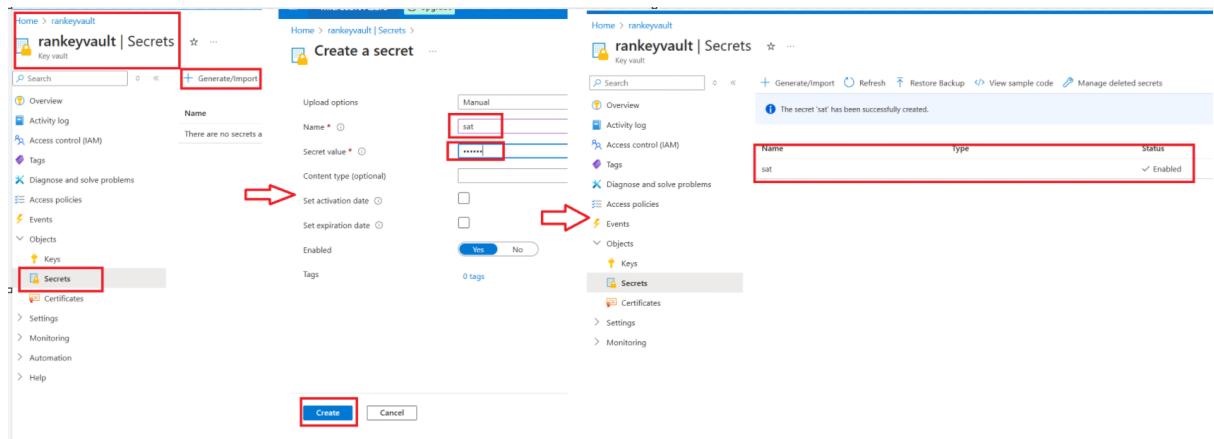
iii. Add Secrets to the Vault

CLI

az keyvault secret set --vault-name satkeyvault --name MySecret --value "SuperSecretValue"

GUI





iv. Enable KeyVault Add-on in AKS Or Enable CSI / Enable CSI Driver

CLI

az aks enable-addons --addons azure-keyvault-secrets-provider --name clusterbox1 --resource-group rgbox1

To Verify

kubectl get pod -n kube-system

```
PS F:\> kubectl get pod -n kube-system
```

NAME	READY	STATUS	RESTARTS	AGE
aks-secrets-store-csi-driver-mr5vr	3/3	Running	0	7m8s
aks-secrets-store-csi-driver-v98kz	3/3	Running	0	7m8s
aks-secrets-store-provider-azure-cmng4	1/1	Running	0	7m8s
aks-secrets-store-provider-azure-zcj68	1/1	Running	0	7m8s
azure-cns-2nldz	1/1	Running	0	6h20m
azure-cns-bj74t	1/1	Running	0	6h20m

Step4: Set up a User Managed Identity in AKS and Key Vault

CLI

GUI

Create one User Managed Identity in AKS

Microsoft Azure

Upgrade

Home > Managed Identities >

Managed Identities

Default Directory (drgauravraj1993@gmail.onmicrosoft.com)

Create

Manage view

Refresh

Filter for any field...

Subscription equals all

Showing 1 to 4 of 4 records.

Name

↑

Create User Assigned Managed Identity

Basics

Tags

Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource manage all your resources.

Subscription *

Free Trial

rgbox1

Create new

Instance details

Region *

East US

Name *

arman123456

Basics

Tags

Review + create

View automation template

Basics

Subscription

Free Trial

Resource group

rgbox1

Region

East US

Name

arman123456

Previous

Next

Create

Permission of User Managed Identity at AKS Side

Home > Kubernetes services > dev-abott-aks

Kubernetes services

Default Directory (drgauravraj1993@gmail.onmicros...

Create

Manage view

Filter for any field...

Name

↑

dev-abott-aks

dev-abott-aks | Properties

Kubernetes service

Search

Refresh

Security configuration

Application scaling

Networking

Extensions + applications

Backup

Service mesh - Istio

Open Service Mesh

GitOps

Automated deployments

Policies

Service Connector (Preview)

Properties

Locks

Properties

Kubernetes Version

1.30.6

DNS prefix

devabottaks

API server address

devabottaks-lakzlau0.portal.hcp.canadacentral.azmk8s.io

RBAC

Enabled

Encryption type

Encryption at rest with platform-managed key

Workspace resource ID

Infrastructure resource group

MC_dev-abott-rg_dev-abott-aks_canadacentral

HTTP application routing domain

Resource ID

/subscriptions/48f88df7-0d53-4866-a66f-82eb0ac469e3/resou

Location

canadacentral

Resource Group

dev-abott-rg

Subscription ID

48f88df7-0d53-4866-a66f-82eb0ac469e3

Permission of User Managed Identity at Keyvault side

Home > Kubernetes services > dev-abott-aks | Properties

MC_dev-abott-rg_dev-abott-aks_canadacentral

Resource group

Search

Refresh

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Cost Management

Monitoring

Automation

Help

Resources

Recommendations (4)

Filter for any field...

Type equals all

Location equals all

Add filter

Showing 1 to 10 of 10 records

Show hidden types

Name

↑

aks-agentpool-27919674-rg

aks-default-61929445-vmss

aks-vnet-27919674

azurkeyvaultcertprovider-dev-abott-aks

dev-abott-aks-agentpool

vh4326b4-91aa-4895-9ed7-69a40115efc

ingress-appgateway

ingress-appgateway-appgw

Type

↑

Network security group

Virtual machine scale set

Virtual network

Managed identity

Managed identity

Public IP address

Application gateway

Public IP address

aks-default-61929445-vmss | Identity

Virtual machine scale set

Search

Refresh

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Instances

Security

Identity

Operations

System assigned

User assigned

+

+

+

+

Name

dev-abott-aks-agentpool

ingressapplicationgateway-dev-abott-aks

azurkeyvaultcertprovider-dev-abott-aks

Add user assigned managed identity

Select a subscription

Free Trial

User assigned managed identities

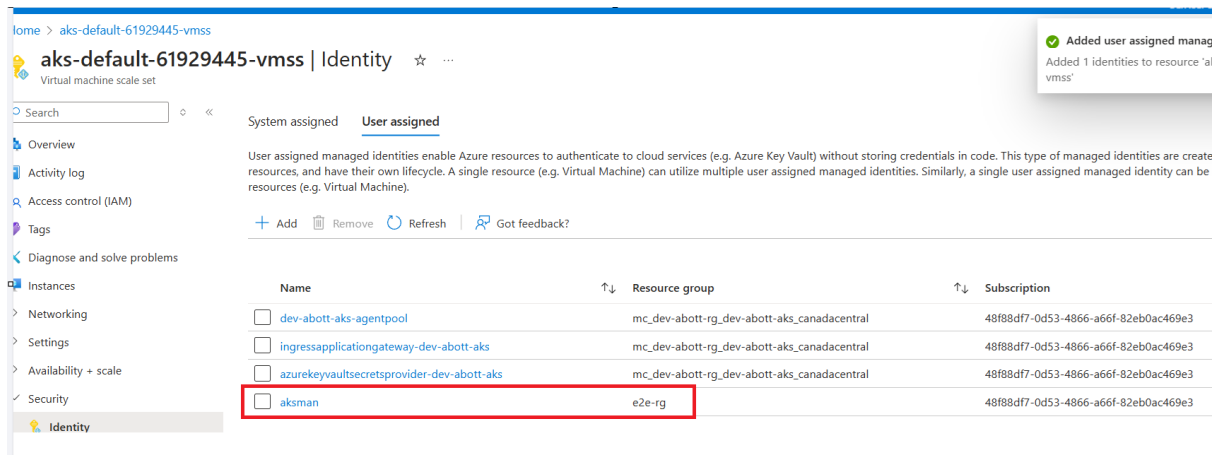
Filter by identity name and/or resource group name

aksman

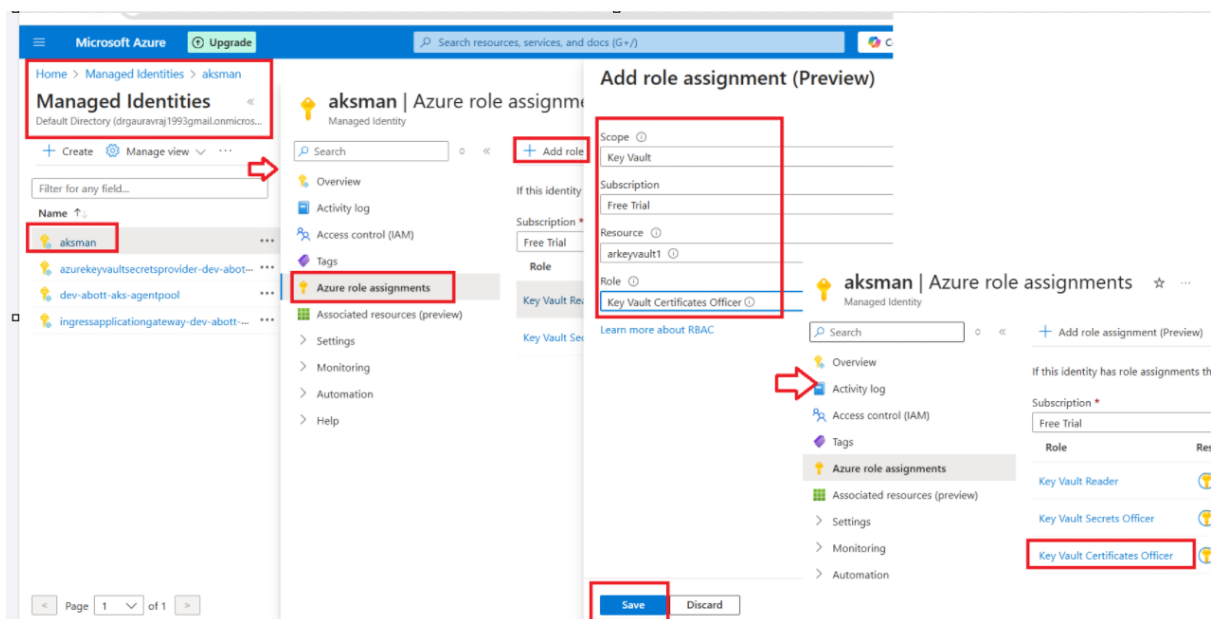
Resource Group: aks-rg

Selected identities

No user assigned managed identities selected. Select one or more user assign identities you want to assign to this resource.



Now Need to Assign Key vault certificate officer role for this user managed identity.

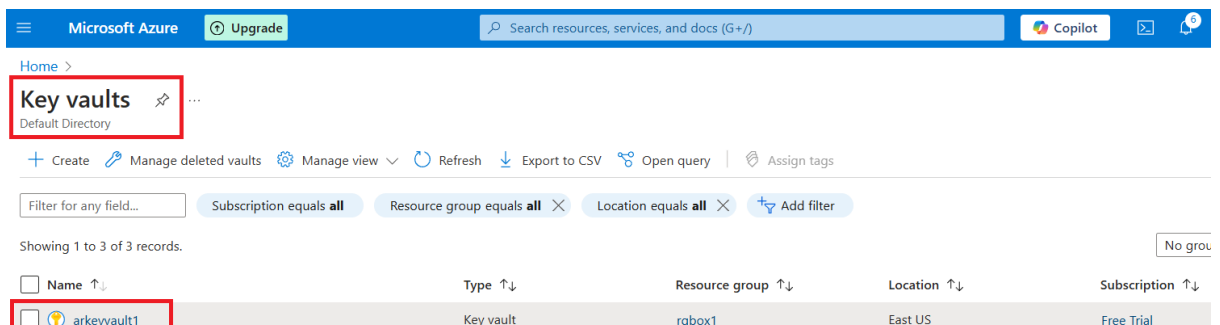


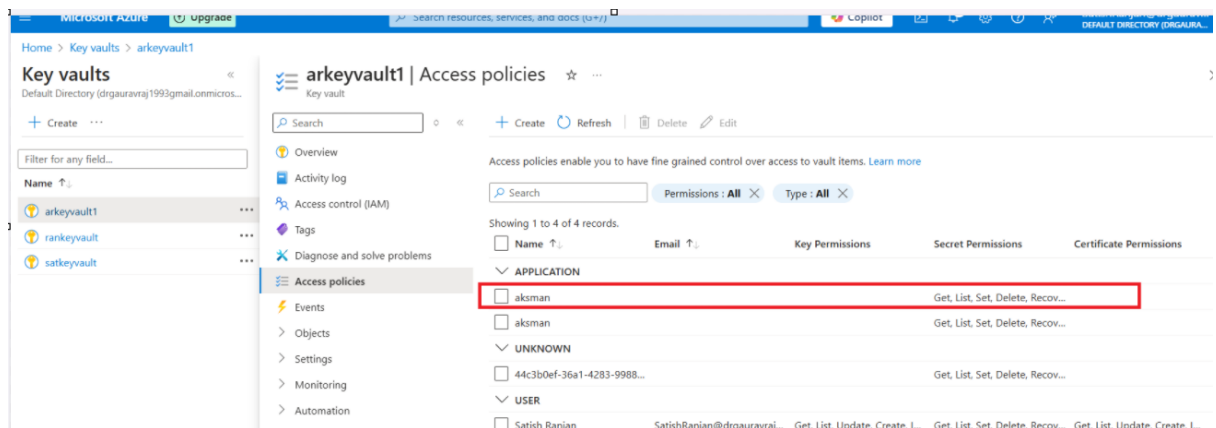
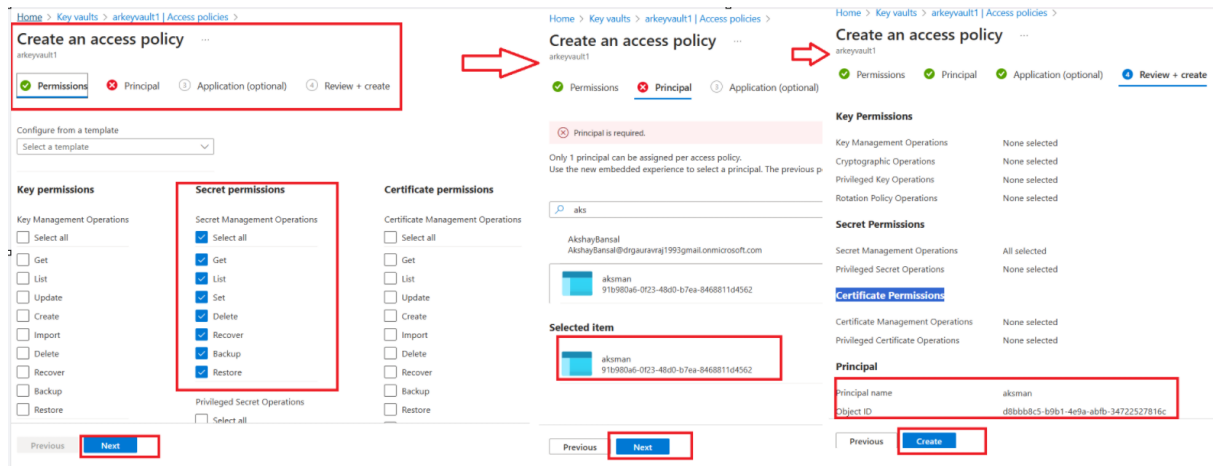
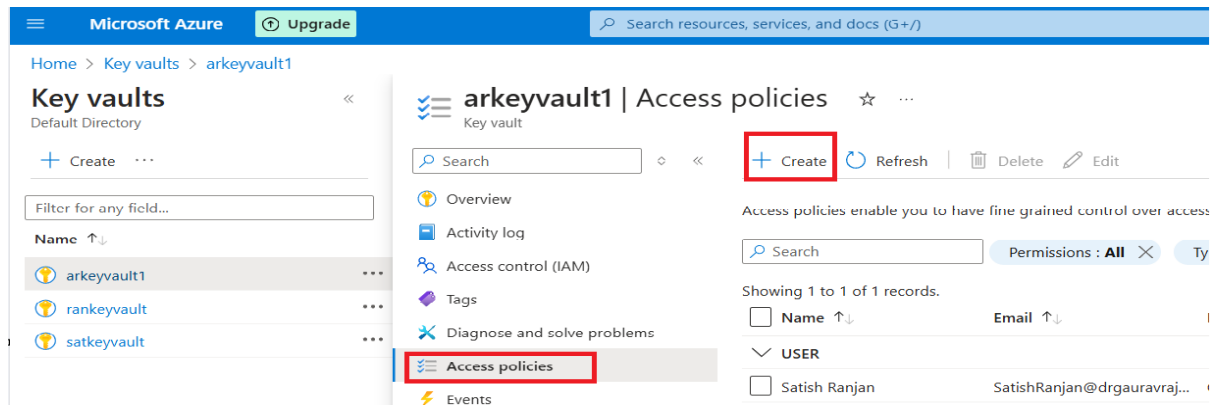
Give Required Permission to Managed Identity at Key Vault Side

CLI

```
az keyvault set-policy -n MyKeyVault --secret-permissions get --spn <aks-identity-client-id>
```

GUI





Step5: Configure and Deploy to Kubernetes

1. Create a SecretProviderClass for VM Managed Identity:

Yaml File for SecretProviderClass

```

apiVersion: secrets-store.csi.x-k8s.io/v1
kind: SecretProviderClass
metadata:
  name: azure-kvname-system-mi
  namespace: default
spec:
  parameters:
    cloudName: AzurePublicCloud
    keyvaultName: aksdemopg
    objects: |
      array:
        - |
          objectName: pgpassword
          objectType: secret          # object types: secret, key, or cert
          objectVersion: ""          # [OPTIONAL] object versions, default to
    tenantId: 4cd93cbc-b026-4c7d-86f1-76fcb7292573 # The Directory ID of the
    usePodIdentity: "false"
    useVMManagedIdentity: "true"
    userAssignedIdentityID: 3457145b-5926-4a60-8d5f-7bb929192891 #Manage iden
    provider: azure

```

2. Deploy Your Application:

```

apiVersion: v1
kind: Pod
metadata:
  name: busybox-secrets-store-inline-system-mi
  namespace: default
spec:
  containers:
    - name: busybox
      image: k8s.gcr.io/e2e-test-images/busybox:1.29-4
      command:
        - /bin/sleep
        - '10000'
      resources: {}
      volumeMounts:
        - name: secrets-store01-inline
          readOnly: true
          mountPath: /mnt/secrets-store
  volumes:
    - name: secrets-store01-inline
      csi:
        driver: secrets-store.csi.k8s.io
        readOnly: true
        volumeAttributes:
          secretProviderClass: azure-kvname-system-mi

```

Step 5: Access Your Secrets

```

PS C:\Users\NIRAV> kubectl exec busybox-secrets-store-inline-system-mi -- ls /mnt/secrets-store/
postgrespw
PS C:\Users\NIRAV> kubectl exec busybox-secrets-store-inline-system-mi -- cat /mnt/secrets-store/postgrespw
password
PS C:\Users\NIRAV>

```

cat /mnt/secrets-store/MySecret