Requirements

Kubernetes clusters

NetApp
July 18, 2022

Table of Contents

Requirements 1
Requirements for Kubernetes clusters in Azure 1

Requirements

Requirements for Kubernetes clusters in Azure

You can add and manage managed Azure Kubernetes clusters (AKS) and self-managed Kubernetes clusters in Azure using Cloud Manager. Before you can add the clusters to Cloud Manager, ensure the following requirements are met.

This topic uses *Kubernetes cluster* where configuration is the same for AKS and self-managed Kubernetes clusters. The cluster type is specified where configuration differs.

Requirements

Astra Trident

One of the four most recent versions of Astra Trident is required. You can install Astra Trident directly from Cloud Manager. You should review the prerequisites prior to installing Astra Trident.

To upgrade Astra Trident, upgrade with the operator.

Cloud Volumes ONTAP

Cloud Volumes ONTAP must be set up as backend storage for the cluster. Go to the Astra Trident docs for configuration steps.

Cloud Manager Connector

A Connector must be running in Azure with the required permissions. Learn more below.

Network connectivity

Network connectivity is required between the Kubernetes cluster and the Connector and between the Kubernetes cluster and Cloud Volumes ONTAP. Learn more below.

RBAC authorization

Cloud Manager supports RBAC-enabled clusters with and without Active Directory. The Cloud Manager Connector role must be authorized on each Azure cluster. Learn more below.

Prepare a Connector

A Cloud Manager Connector in Azure is required to discover and manage Kubernetes clusters. You'll need to create a new Connector or use an existing Connector that has the required permissions.

Create a new Connector

Follow the steps in one of the links below.

- Create a Connector from Cloud Manager (recommended)
- Create a Connector from the Azure Marketplace
- Install the Connector on an existing Linux host

Add the required permissions to an existing Connector (to discover a managed AKS cluster)

If you want to discover a managed AKS cluster, you might need to modify the custom role for the Connector to provide the permissions.

Steps

1. Identify the role assigned to the Connector virtual machine:
   a. In the Azure portal, open the Virtual machines service.
   b. Select the Connector virtual machine.
   c. Under Settings, select **Identity**.
   d. Click **Azure role assignments**.
   e. Make note of the custom role assigned to the Connector virtual machine.
2. Update the custom role:
   a. In the Azure portal, open your Azure subscription.
   b. Click **Access control (IAM) > Roles**.
   c. Click the ellipsis (…) for the custom role and then click **Edit**.
   d. Click JSON and add the following permissions:

```
"Microsoft.ContainerService/managedClusters/listClusterUserCredential
/action"
"Microsoft.ContainerService/managedClusters/read"
```

   e. Click **Review + update** and then click **Update**.

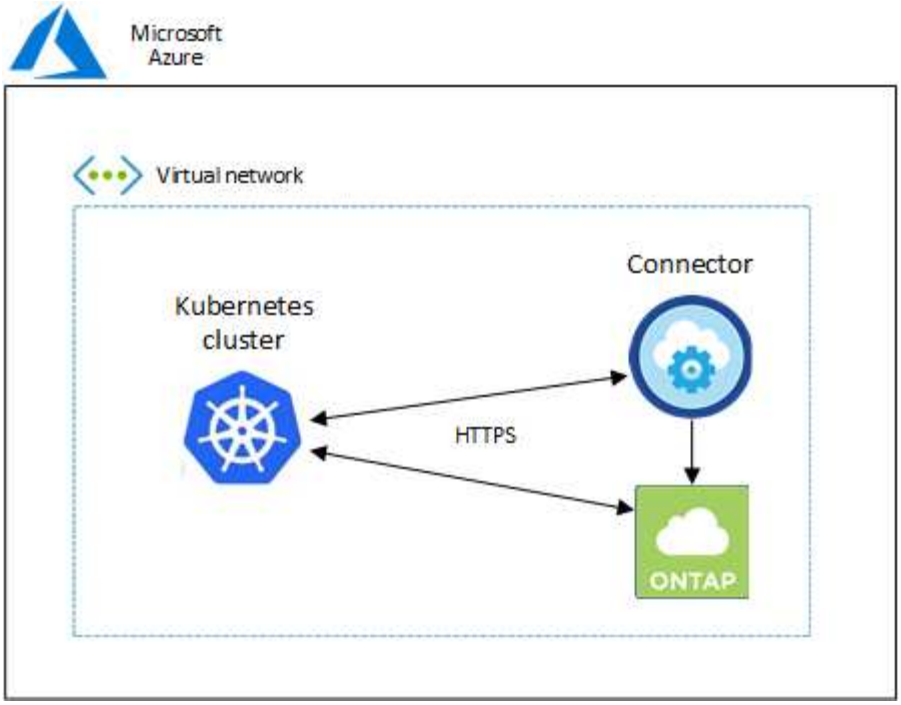
Review networking requirements

You need to provide network connectivity between the Kubernetes cluster and the Connector and between the Kubernetes cluster and the Cloud Volumes ONTAP system that provides backend storage to the cluster.

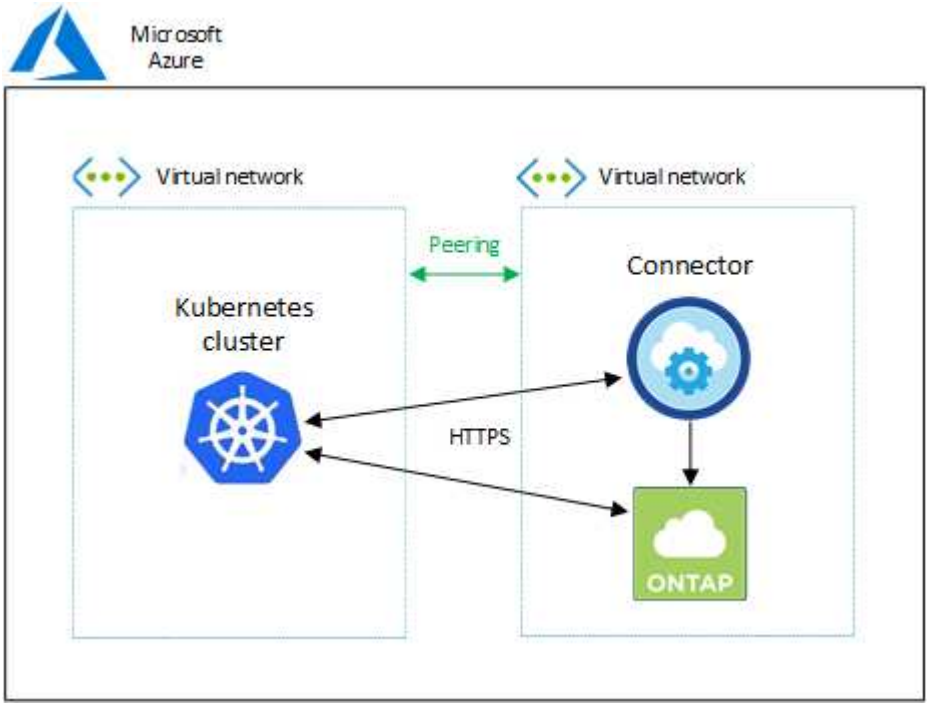
- Each Kubernetes cluster must have an inbound connection from the Connector
- The Connector must have an outbound connection to each Kubernetes cluster over port 443

The simplest way to provide this connectivity is to deploy the Connector and Cloud Volumes ONTAP in the same VNet as the Kubernetes cluster. Otherwise, you need to set up a peering connection between the different VNets.

Here's an example that shows each component in the same VNet.



And here's another example that shows a Kubernetes cluster running in a different VNet. In this example, peering provides a connection between the VNet for the Kubernetes cluster and the VNet for the Connector and Cloud Volumes ONTAP.



Set up RBAC authorization

RBAC validation occurs only on Kubernetes clusters with Active Directory (AD) enabled. Kubernetes clusters without AD will pass validation automatically.

You need authorize the Connector role on each Kubernetes cluster so the Connector can discover and manage a cluster.

Backup and restore

Backup and restore requires only basic authorization.

Add storage classes

Expanded authorization is required to add storage classes using Cloud Manager.

Install Astra trident

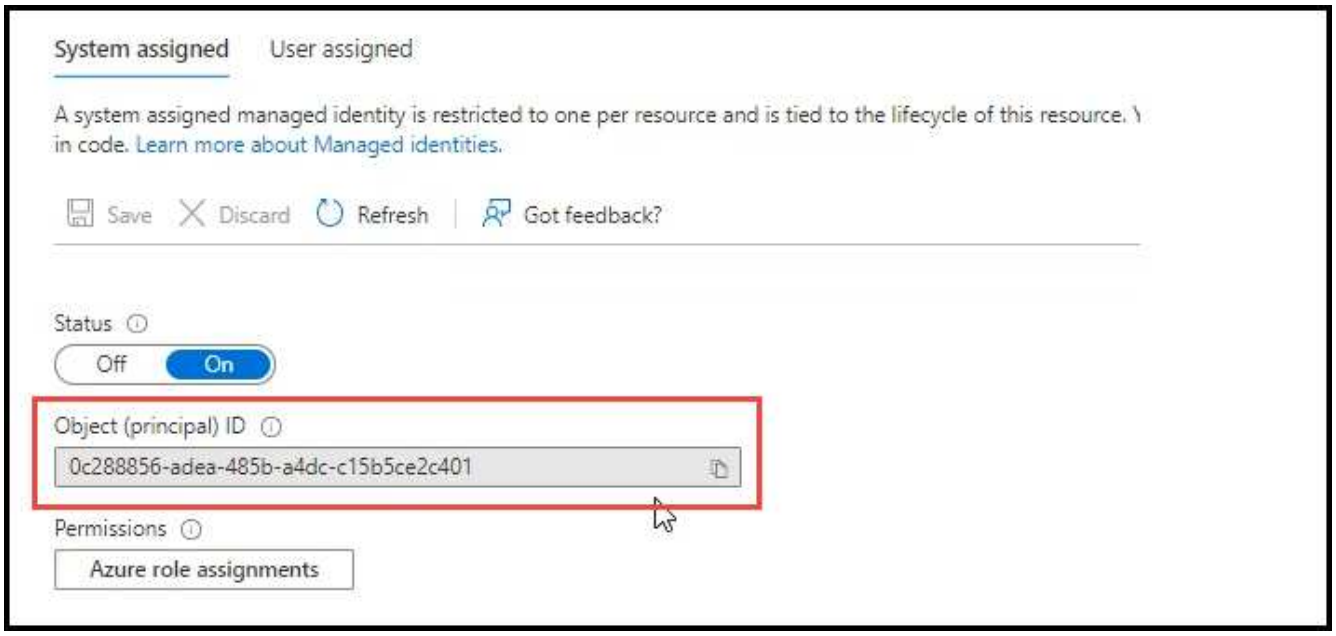
You need to provide full authorization for Cloud Manager to install Astra Trident.

When installing Astra Trident, Cloud Manager installs the Astra Trident backend and Kubernetes secret that contains the credentials Astra Trident needs to communicate with the storage cluster.

Before you begin

Your RBAC `subjects: name:` configuration varies slightly based on your Kubernetes cluster type.

- If you are deploying a **managed AKS cluster**, you need the Object ID for the system-assigned managed identity for the Connector. This ID is available in Azure management portal.



- If you are deploying a **self-managed Kubernetes cluster**, you need the username of any authorized user.

Steps

Create a cluster role and role binding.

1. Create a YAML file that includes the following text based on your authorization requirements. Replace the `subjects: kind:` variable with your username and `subjects: user:` with either the Object ID for the system-assigned managed identity or username of any authorized user as described above.

Backup/restore

Add basic authorization to enable backup and restore for Kubernetes clusters.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
        - ''
      resources:
        - namespaces
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumes
      verbs:
        - list
    - apiGroups:
        - ''
      resources:
        - pods
        - pods/exec
      verbs:
        - get
        - list
    - apiGroups:
        - ''
      resources:
        - persistentvolumeclaims
      verbs:
        - list
        - create
    - apiGroups:
        - storage.k8s.io
      resources:
        - storageclasses
      verbs:
        - list
    - apiGroups:
        - trident.netapp.io
      resources:
        - tridentbackends
```

```
      verbs:
          - list
    - apiGroups:
          - trident.netapp.io
      resources:
          - tridentorchestrators
      verbs:
          - get
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Storage classes

Add expanded authorization to add storage classes using Cloud Manager.

```
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
    name: cloudmanager-access-clusterrole
rules:
    - apiGroups:
          - ''
      resources:
          - secrets
          - namespaces
          - persistentvolumeclaims
          - persistentvolumes
          - pods
          - pods/exec
      verbs:
          - get
          - list
          - create
          - delete
    - apiGroups:
```

```
            - storage.k8s.io
        resources:
            - storageclasses
        verbs:
            - get
            - create
            - list
            - delete
            - patch
    - apiGroups:
            - trident.netapp.io
        resources:
            - tridentbackends
            - tridentorchestrators
            - tridentbackendconfigs
        verbs:
            - get
            - list
            - create
            - delete
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
    name: k8s-access-binding
subjects:
    - kind: User
      name:
      apiGroup: rbac.authorization.k8s.io
roleRef:
    kind: ClusterRole
    name: cloudmanager-access-clusterrole
    apiGroup: rbac.authorization.k8s.io
```

Install Trident

Use the command line to provide full authorization and enable Cloud Manager to install Astra Trident.

```
kubectl create clusterrolebinding test --clusterrole cluster-admin
--user <Object (principal) ID>
```

2. Apply the configuration to a cluster.

```
kubectl apply -f <file-name>
```