要求
Kubernetes clusters

NetApp
June 02, 2022

目录

要求

Azure 中 Kubernetes 集群的要求

您可以使用 Cloud Manager 在 Azure 中添加和管理受管 Azure Kubernetes 集群（ AKS ）和自管 Kubernetes 集群。在将集群添加到 Cloud Manager 之前，请确保满足以下要求。

本主题使用 *Kubernetes cluster* ，其中对于 AKS 和自管理 Kubernetes 集群的配置相同。在配置不同的位置指定集群类型。

要求

Astra Trident

需要使用四个最新版本的 Astra Trident 之一。您可以直接从 Cloud Manager 安装 Astra Trident 。您应该 "查看前提条件" 安装 Astra Trident 之前。

要升级 Astra Trident ， "使用操作员升级"。

Cloud Volumes ONTAP

必须将 Cloud Volumes ONTAP 设置为集群的后端存储。 "有关配置步骤，请转至 Astra Trident 文档"。

Cloud Manager Connector

Connector 必须使用所需权限在 Azure 中运行。 在下方了解更多信息。

网络连接

Kubernetes 集群和 Connector 之间以及 Kubernetes 集群和 Cloud Volumes ONTAP 之间需要网络连接。 在下方了解更多信息。

RBAC 授权

Cloud Manager 支持使用和不使用 Active Directory 的已启用 RBAC 的集群。必须在每个 Azure 集群上授权 Cloud Manager Connector 角色。 在下方了解更多信息。

准备连接器

要发现和管理 Kubernetes 集群，需要使用 Azure 中的 Cloud Manager Connector 。您需要创建新的 Connector 或使用具有所需权限的现有 Connector 。

创建新的 **Connector**

按照以下链接之一中的步骤进行操作。

- "从 Cloud Manager 创建 Connector" 建议
- "从 Azure Marketplace 创建 Connector"
- "在现有 Linux 主机上安装 Connector"

向现有 **Connector** 添加所需权限（以发现受管 **AKS** 集群）

如果要发现受管 AKS 集群，您可能需要修改 Connector 的自定义角色以提供权限。

步骤

1. 确定分配给 Connector 虚拟机的角色：
   a. 在 Azure 门户中，打开虚拟机服务。
   b. 选择 Connector 虚拟机。
   c. 在设置下，选择 * 身份 * 。
   d. 单击 * Azure 角色分配 * 。
   e. 记下分配给 Connector 虚拟机的自定义角色。
2. 更新自定义角色：
   a. 在 Azure 门户中，打开 Azure 订阅。
   b. 单击 * 访问控制（ IAM ） > 角色 * 。
   c. 单击自定义角色的省略号（ ... ），然后单击 * 编辑 * 。
   d. 单击 JSON 并添加以下权限：

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

   e. 单击 * 查看 + 更新 * ，然后单击 * 更新 * 。

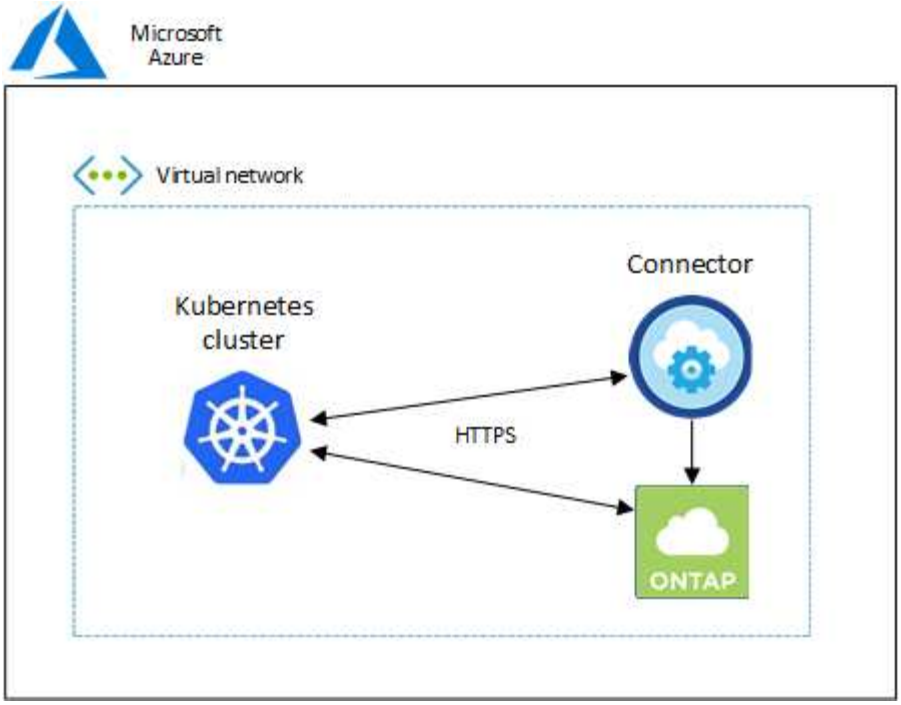
查看网络连接要求

您需要在 Kubernetes 集群和 Connector 之间以及 Kubernetes 集群与为集群提供后端存储的 Cloud Volumes ONTAP 系统之间提供网络连接。

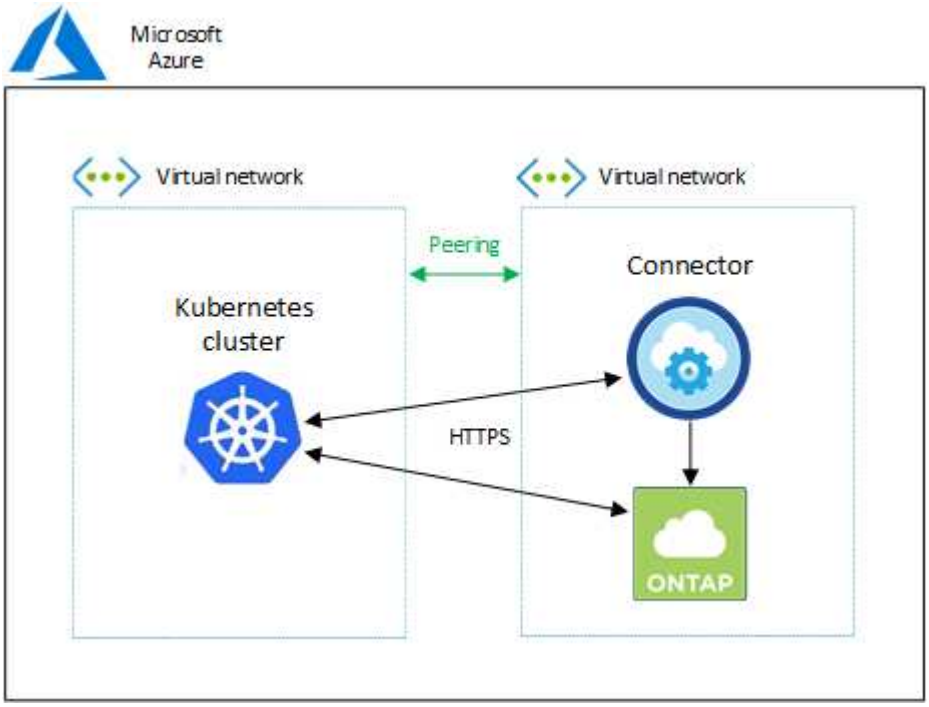
- 每个 Kubernetes 集群都必须与 Connector 建立入站连接
- 此连接器必须通过端口 443 与每个 Kubernetes 集群建立出站连接

提供此连接的最简单方法是，将 Connector 和 Cloud Volumes ONTAP 部署在与 Kubernetes 集群相同的 VNet 中。否则，您需要在不同的 VN 集之间设置对等连接。

以下示例显示了同一 vNet 中的每个组件。



下面是另一个示例，其中显示了一个 Kubernetes 集群运行在另一个 vNet 中。在此示例中，对等关系可在 Kubernetes 集群的 vNet 与 Connector 和 Cloud Volumes ONTAP 的 vNet 之间建立连接。



设置 RBAC 授权

RBAC 验证仅在启用了 Active Directory （AD ）的 Kubernetes 集群上进行。不带 AD 的 Kubernetes 集群将自动通过验证。

您需要在每个 Kubernetes 集群上授权 Connector 角色，以便 Connector 可以发现和管理集群。

备份和还原

备份和还原只需要基本授权。

添加存储类

要使用 Cloud Manager 添加存储类，需要扩展授权。

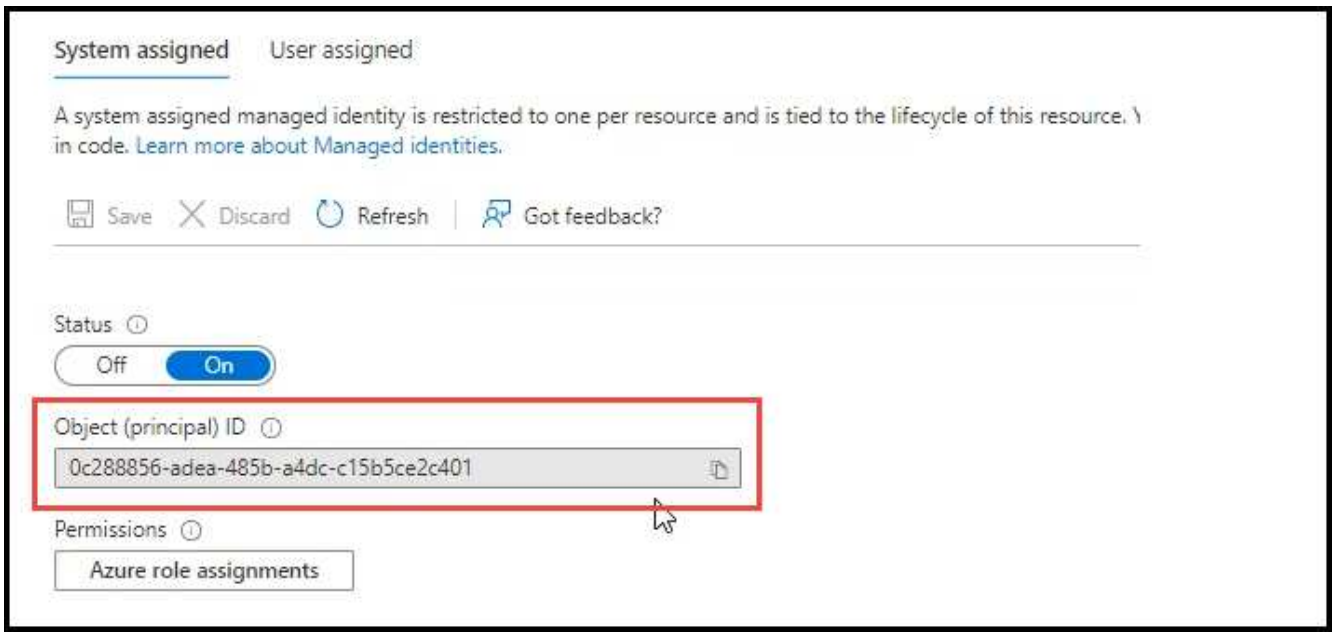
安装 **Astra Trident**

要安装 Astra Trident ，您需要为 Cloud Manager 提供完全授权。

安装 Astra Trident 时， Cloud Manager 会安装 Astra Trident 后端和 Kubernetes 密钥，其中包含 Astra Trident 与存储集群通信所需的凭据。

您的 RBAC s对象： `name` ： 配置会根据您的 Kubernetes 集群类型稍有不同。

- 如果要部署 * 受管 AKS 集群 * ，则需要为 Connector 的系统分配的受管身份提供对象 ID 。此 ID 可在 Azure 管理门户中使用。



- 如果要部署 * 自管理 Kubernetes 集群 * ，则需要任何授权用户的用户名。

创建集群角色和角色绑定。

1. 根据您的授权要求创建包含以下文本的 YAML 文件。将 `ssubjects ： kind ：` 变量替换为您的用户名，将 `ssubjects ： user ：` 替换为系统分配的受管身份的对象 ID 或上述任何授权用户的用户名。

备份 / 还原

添加基本授权，以便为 Kubernetes 集群启用备份和还原。

```
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
```

存储类

添加扩展授权以使用 Cloud Manager 添加存储类。

```
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
```

安装 Trident

使用命令行提供完全授权并启用 Cloud Manager 以安装 Astra Trident 。

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

2. 将配置应用于集群。

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