需求
Kubernetes clusters

NetApp
June 02, 2022

目錄

需求

Azure中Kubernetes叢集的需求

您可以使用Cloud Manager、在Azure中新增及管理託管Azure Kubernetes叢集（KS）和自我管理的Kubernetes叢集。在將叢集新增至Cloud Manager之前、請先確保符合下列需求。

本主題使用_Kubernetes叢集_、其中的設定與自我管理Kubernetes叢集的組態相同。叢集類型是在組態不同的地方指定。

需求

Astra Trident

需要最新版Astra Trident的四種版本之一。您可以直接從Cloud Manager安裝Astra Trident。您應該 "檢閱先決條件" 安裝Astra Trident之前。

若要升級Astra Trident、 "與營運者一起升級"。

Cloud Volumes ONTAP

必須將其設定為叢集的後端儲存設備。Cloud Volumes ONTAP "如需組態步驟、請前往Astra Trident文件"。

Cloud Manager Connector

連接器必須在具備必要權限的Azure中執行。 深入瞭解。

網路連線能力

Kubernetes叢集和Connector之間、以及Kubernetes叢集和Cloud Volumes ONTAP 整個過程之間、都需要網路連線。 深入瞭解。

RBAC授權

Cloud Manager支援啟用RBAC的叢集、可搭配或不使用Active Directory。Cloud Manager Connector角色必須在每個Azure叢集上獲得授權。 深入瞭解。

準備連接器

Azure中的Cloud Manager Connector需要探索及管理Kubernetes叢集。您需要建立新的Connector、或是使用具有所需權限的現有Connector。

建立新的**Connector**

請遵循下列其中一個連結中的步驟。

- "從Cloud Manager建立Connector" （建議）
- "從Azure Marketplace建立連接器"
- "在現有的Linux主機上安裝Connector"

將必要的權限新增至現有的**Connector**（以探索託管的高層叢集）

如果您想要探索託管的高效能叢集、可能需要修改Connector的自訂角色、以提供權限。

步驟

1. 識別指派給Connector虛擬機器的角色：
   a. 在Azure入口網站中、開啟虛擬機器服務。
   b. 選取 Connector 虛擬機器。
   c. 在「設定」下、選取「身分識別」。
   d. 按一下* Azure角色指派*。
   e. 記下指派給Connector虛擬機器的自訂角色。
2. 更新自訂角色：
   a. 在Azure入口網站中、開啟您的Azure訂閱。
   b. 按一下*存取控制（IAM）>角色*。
   c. 按一下自訂角色的省略符號（...）、然後按一下*編輯*。
   d. 按一下Json並新增下列權限：

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

   e. 按一下「檢閱+更新」、然後按一下「更新」。

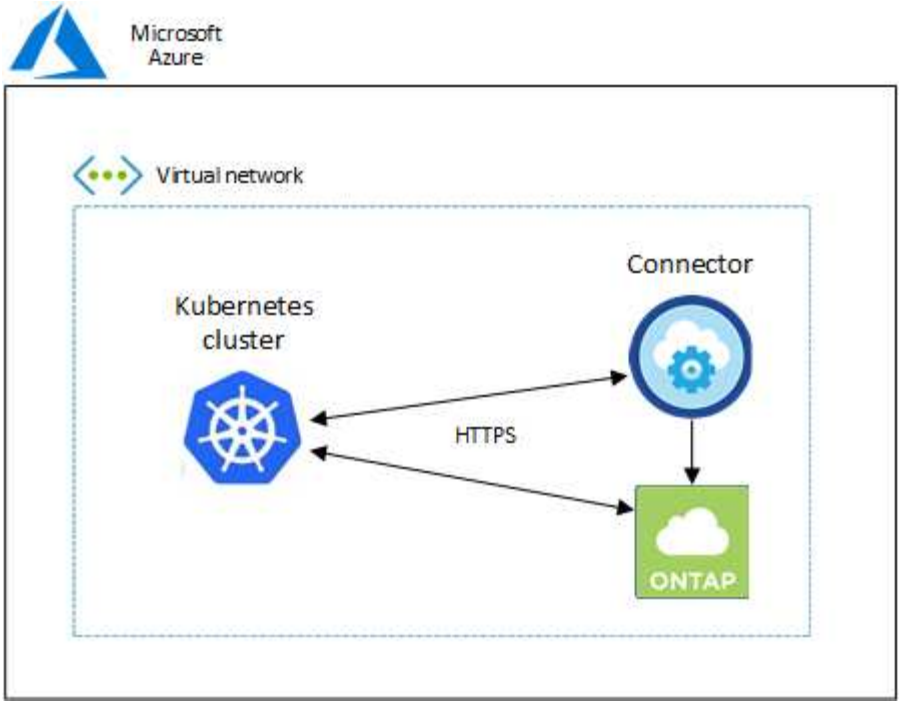
檢閱網路需求

您需要在Kubernetes叢集與Connector之間、以及Kubernetes叢集與Cloud Volumes ONTAP 為叢集提供後端儲存功能的支援系統之間、提供網路連線。

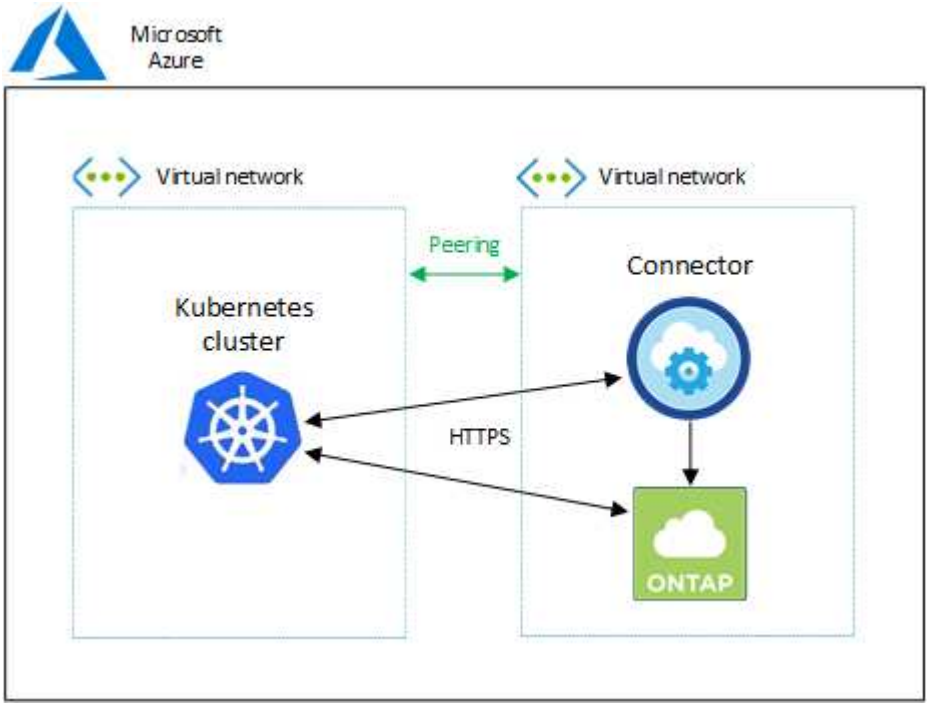
- 每個Kubernetes叢集都必須有來自Connector的傳入連線
- 連接器必須透過連接埠443連線至每個Kubernetes叢集

提供這種連線能力的最簡單方法、就是將Connector和Cloud Volumes ONTAP DB2部署在Kubernetes叢集所在的相同vnet中。否則、您需要在不同的VNets之間設定對等連線。

以下範例顯示同一個vnet中的每個元件。



以下是另一個範例、顯示Kubernetes叢集在不同的vnet上執行。在此範例中、對等功能可在Kubernetes叢集的vnet與Connector和Cloud Volumes ONTAP 物件的vnet之間建立連線。



設定RBAC授權

RBAC驗證只會在啟用Active Directory（AD）的Kubernetes叢集上執行。未使用AD的Kubernetes叢集將自動通過驗證。

您需要在每個Kubernetes叢集上授權Connector角色、以便Connector探索及管理叢集。

備份與還原

備份與還原僅需基本授權。

新增儲存類別

若要使用Cloud Manager新增儲存類別、則需要擴大授權。

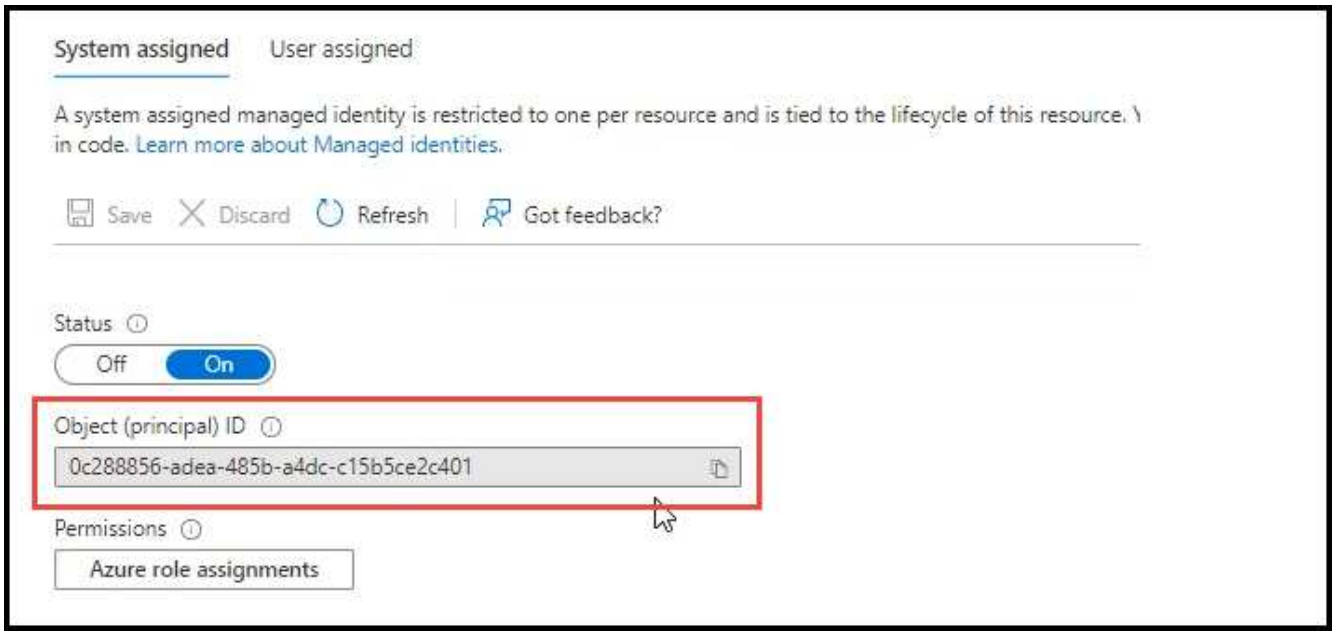
安裝**Astra Trident**

您必須提供Cloud Manager完整授權、才能安裝Astra Trident。

安裝Astra Trident時、Cloud Manager會安裝Astra Trident後端和Kubernetes機密、其中包含Astra Trident與儲存叢集通訊所需的認證資料。

您的RBAC「子項目：名稱：」組態會因Kubernetes叢集類型而稍有不同。

- 如果要部署*託管的高層叢集*、則需要連接器系統指派的託管身分識別物件ID。此ID可在Azure管理入口網站取得。



- 如果您要部署*自我管理的Kubernetes叢集*、則需要任何授權使用者的使用者名稱。

建立叢集角色和角色繫結。

1. 根據您的授權要求、建立包含下列文字的Y反 洗錢檔案。使用您的使用者名稱取代「子物件：種類：」變數、並將「子物件：使用者：」取代為系統指派的託管身分識別的物件ID、或是如上所述的任何授權使用者的使用者名稱。

備份/還原

新增基本授權以啟用Kubernetes叢集的備份與還原。

```
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
```

儲存類別

新增擴充授權、以使用Cloud Manager新增儲存類別。

```
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
```

安裝Trident

使用命令列提供完整授權、並讓Cloud Manager安裝Astra Trident。

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

2. 將組態套用至叢集。

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