요구 사항

Kubernetes clusters

NetApp
July 18, 2022

목차

요구 사항

Azure의 Kubernetes 클러스터 요구사항

Cloud Manager를 사용하여 Azure에서 관리되는 Azure Kubernetes 클러스터(AKS) 및 자체 관리 Kubernetes 클러스터를 추가하고 관리할 수 있습니다. 클러스터를 Cloud Manager에 추가하려면 먼저 다음 요구사항을 충족해야 합니다.

이 항목에서는 AKS 및 자체 관리 Kubernetes 클러스터의 구성이 동일한 _Kubernetes 클러스터를 사용합니다. 클러스터 유형은 구성이 다른 곳에서 지정됩니다.

요구 사항

아스트라 트리덴트

Astra Trident의 최신 버전 4개 중 하나가 필요합니다. Cloud Manager에서 Astra Trident를 직접 설치할 수 있습니다. 당신은 해야 한다 "사전 요구 사항을 검토합니다" Astra Trident를 설치하기 전

Astra Trident를 업그레이드하려면 "운영자와 함께 업그레이드하십시오".

Cloud Volumes ONTAP

Cloud Volumes ONTAP를 클러스터에 대한 백엔드 스토리지로 설정해야 합니다. "구성 단계를 보려면 Astra Trident 문서로 이동합니다".

Cloud Manager 커넥터

Connector는 필요한 권한을 사용하여 Azure에서 실행 중이어야 합니다. 아래에서 자세히 알아보십시오.

네트워크 연결

Kubernetes 클러스터와 Connector 간, Kubernetes 클러스터와 Cloud Volumes ONTAP 사이에 네트워크 연결이 필요합니다. 아래에서 자세히 알아보십시오.

RBAC 인증

Cloud Manager는 Active Directory를 사용 또는 사용하지 않는 RBAC 지원 클러스터를 지원합니다. Cloud Manager Connector 역할은 각 Azure 클러스터에서 인증되어야 합니다. 아래에서 자세히 알아보십시오.

커넥터를 준비합니다

Kubernetes 클러스터를 검색하고 관리하려면 Azure의 Cloud Manager Connector가 필요합니다. 새 Connector를 만들거나 필요한 권한이 있는 기존 Connector를 사용해야 합니다.

새 커넥터를 작성합니다

아래 링크 중 하나에 있는 단계를 따르십시오.

- "Cloud Manager에서 커넥터를 생성합니다" (권장)
- "Azure Marketplace에서 Connector를 생성합니다"
- "기존 Linux 호스트에 커넥터를 설치합니다"

기존 **Connector**에 필요한 사용 권한 추가(관리되는 **AKS** 클러스터 검색)

관리되는 AKS 클러스터를 검색하려면 Connector의 사용자 지정 역할을 수정하여 사용 권한을 제공해야 할 수 있습니다.

단계

1. Connector 가상 머신에 할당된 역할을 확인합니다.
   a. Azure 포털에서 가상 머신 서비스를 엽니다.
   b. Connector 가상 머신을 선택합니다.
   c. 설정에서 * ID * 를 선택합니다.
   d. Azure 역할 할당 * 을 클릭합니다.
   e. Connector 가상 머신에 할당된 사용자 지정 역할을 기록해 둡니다.
2. 사용자 지정 역할 업데이트:
   a. Azure 포털에서 Azure 구독을 엽니다.
   b. IAM(액세스 제어) > 역할 * 을 클릭합니다.
   c. 사용자 지정 역할에 대한 줄임표(…)를 클릭한 다음 * 편집 * 을 클릭합니다.
   d. JSON을 클릭하고 다음 권한을 추가합니다.

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

   e. 검토 + 업데이트 * 를 클릭한 다음 * 업데이트 * 를 클릭합니다.

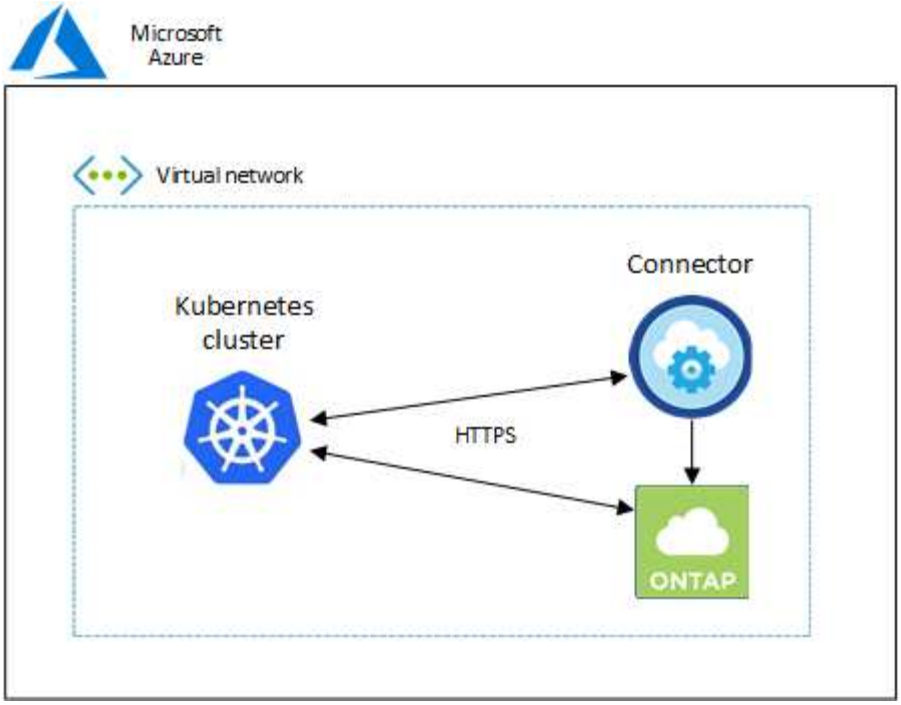
네트워킹 요구 사항을 검토합니다

Kubernetes 클러스터와 Connector 간, Kubernetes 클러스터와 클러스터에 백엔드 스토리지를 제공하는 Cloud Volumes ONTAP 시스템 간에 네트워크 연결을 제공해야 합니다.

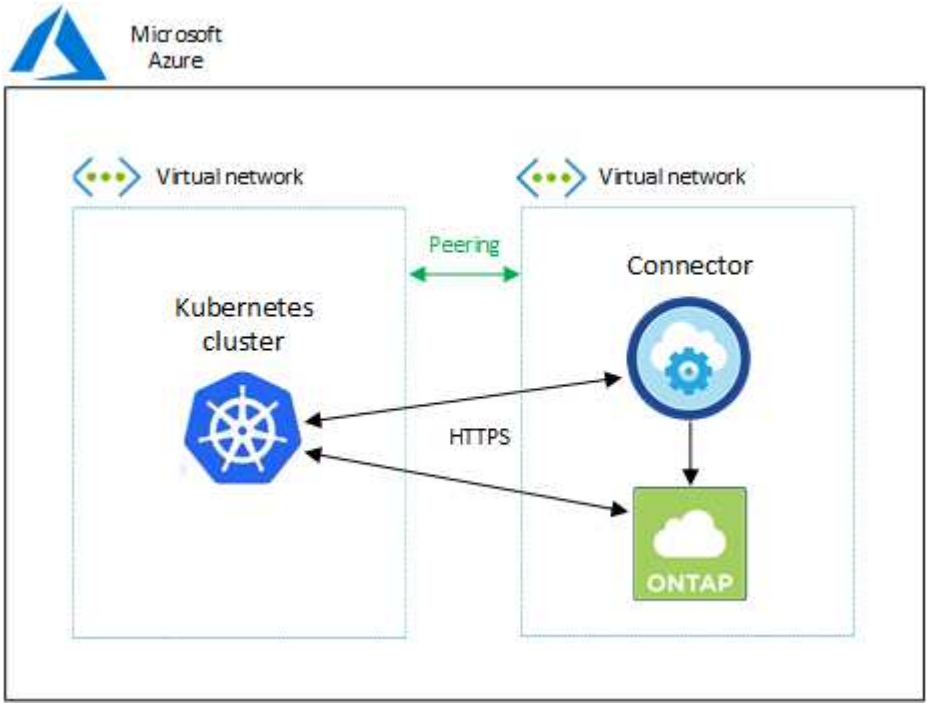
- 각 Kubernetes 클러스터에는 Connector로부터 인바운드 연결이 있어야 합니다
- Connector는 포트 443을 통해 각 Kubernetes 클러스터에 대한 아웃바운드 연결을 가지고 있어야 합니다

이 연결을 제공하는 가장 간단한 방법은 Kubernetes 클러스터와 같은 VNET에 Connector와 Cloud Volumes ONTAP를 구축하는 것입니다. 그렇지 않으면 다른 VNets 간의 피어링 연결을 설정해야 합니다.

다음은 동일한 VNET의 각 구성 요소를 보여 주는 예입니다.



그리고 다른 VNET에서 실행되는 Kubernetes 클러스터를 보여 주는 또 다른 예가 있습니다. 이 예에서 피어링은 Kubernetes 클러스터의 VNET와 커넥터 및 Cloud Volumes ONTAP용 VNET 간의 연결을 제공합니다.



RBAC 승인을 설정합니다

RBAC 검증은 AD(Active Directory)가 활성화된 Kubernetes 클러스터에서만 실행됩니다. AD를 사용하지 않는 Kubernetes 클러스터는 검증을 자동으로 통과합니다.

Connector가 클러스터를 검색 및 관리할 수 있도록 각 Kubernetes 클러스터에서 커넥터 역할을 승인해야 합니다.

백업 및 복원

백업 및 복원에는 기본 인증만 필요합니다.

스토리지 클래스를 추가합니다

Cloud Manager를 사용하여 스토리지 클래스를 추가하려면 확장된 인증이 필요합니다.

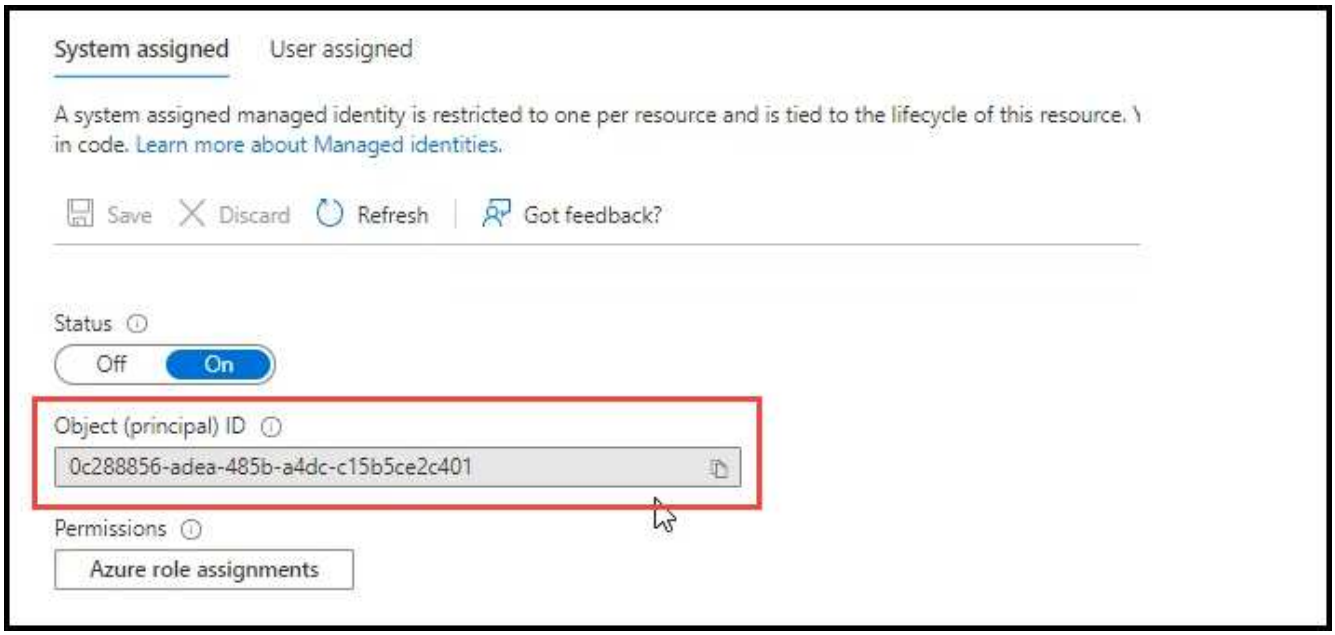
Astra 트리덴트 설치

Astra Trident를 설치하려면 Cloud Manager에 대한 전체 인증을 제공해야 합니다.

Astra Trident를 설치할 때 Cloud Manager는 Astra Trident와 스토리지 클러스터와 통신하는 데 필요한 자격 증명이 포함된 Astra Trident 백엔드 및 Kubernetes 암호를 설치합니다.

RBAC "프로젝트:이름:" 구성은 Kubernetes 클러스터 유형에 따라 약간 다릅니다.

- 관리되는 AKS 클러스터 * 를 배포하는 경우, Connector에 대해 시스템에서 할당한 관리 ID의 객체 ID가 필요합니다. 이 ID는 Azure 관리 포털에서 사용할 수 있습니다.



- 자체 관리되는 Kubernetes 클러스터 * 를 구축하는 경우 권한이 있는 사용자의 사용자 이름이 필요합니다.

클러스터 역할 및 역할 바인딩을 생성합니다.

1. 귀하의 승인 요구 사항에 따라 다음 텍스트가 포함된 YAML 파일을 생성합니다. 'Subjects:kind:' 변수를 사용자 이름으로 바꾸고 'Subjects:user:'를 위에서 설명한 대로 시스템에서 할당한 관리 ID의 개체 ID 또는 권한이 있는 사용자의 사용자 이름으로 바꿉니다.

백업/복원

Kubernetes 클러스터의 백업 및 복원을 위한 기본 인증을 추가하십시오.

```
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
```

스토리지 클래스

Cloud Manager를 사용하여 스토리지 클래스를 추가하려면 확장 인증을 추가합니다.

```
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
```

Trident를 설치합니다

명령줄을 사용하여 전체 인증을 제공하고 Cloud Manager에서 Astra Trident를 설치할 수 있도록 합니다.

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

2. 클러스터에 구성을 적용합니다.

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