需求
Kubernetes clusters

NetApp
July 19, 2022

目錄

需求

AWS中Kubernetes叢集的需求

您可以將AWS上的託管Amazon Elastic Kubernetes Service（EKS）叢集或自我管理Kubernetes叢集新增至Cloud Manager。在將叢集新增至Cloud Manager之前、您必須確保符合下列需求。

本主題使用_Kubernetes叢集_、其中EKS和自我管理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

AWS的for AWS必須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

連接器必須以所需權限在AWS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 Connector角色必須在每個Kubernetes叢集上獲得授權。 深入瞭解。

準備連接器

AWS需要Cloud Manager Connector來探索及管理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。

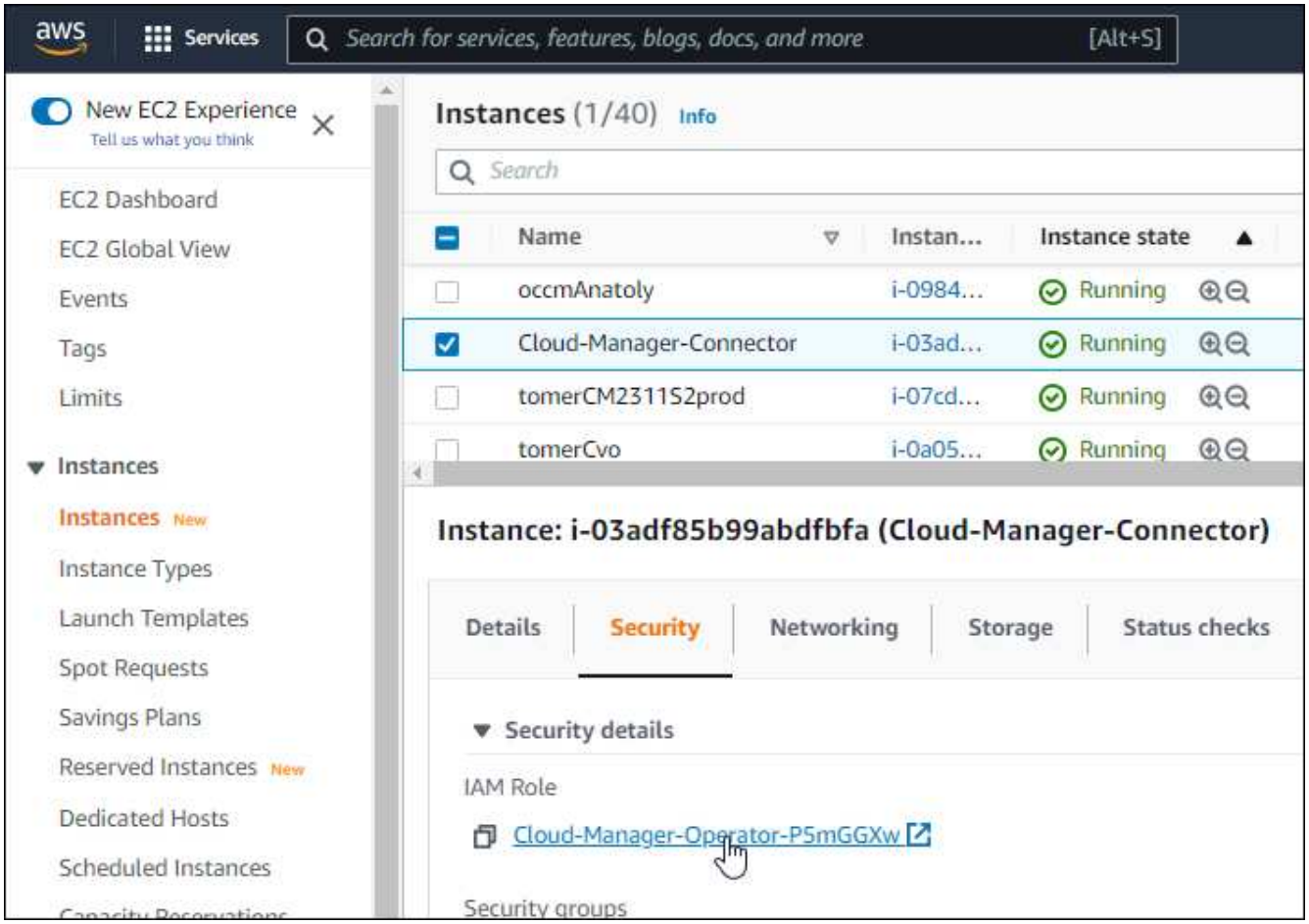
- "從Cloud Manager建立Connector" （建議）
- "從AWS Marketplace建立連接器"
- "在AWS中現有的Linux主機上安裝Connector"

將必要的權限新增至現有的**Connector**

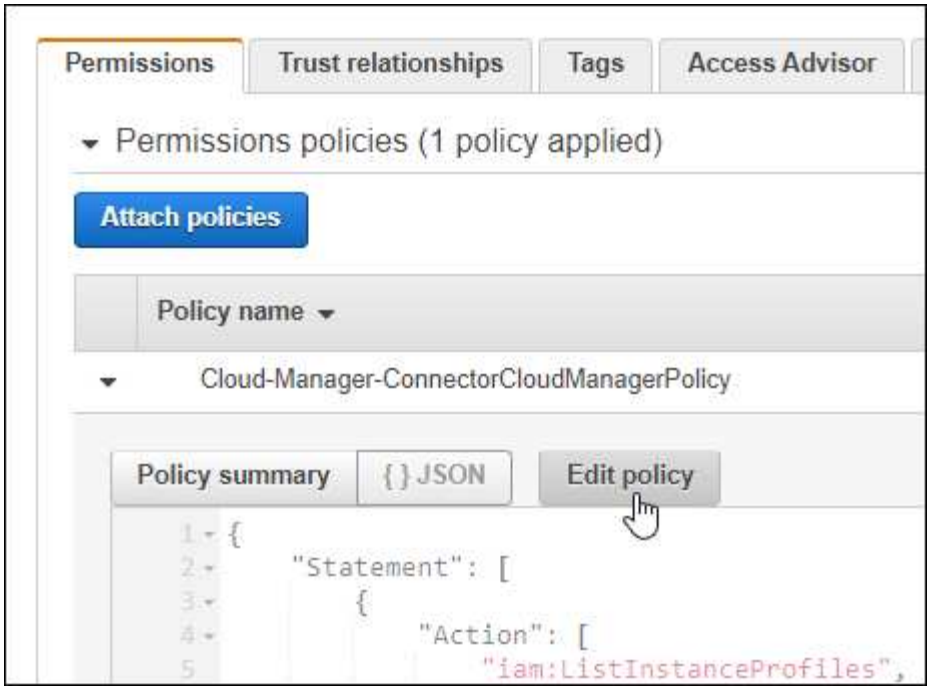
從3.9.13版開始、任何_new建立的連接器都包含三個新的AWS權限、可用來探索及管理Kubernetes叢集。如果您在此版本之前建立了Connector、則需要修改Connector IAM角色的現有原則、以提供權限。

步驟

1. 移至AWS主控台並開啟EC2服務。
2. 選取連接器執行個體、按一下*安全性*、然後按一下IAM角色名稱、即可檢視IAM服務中的角色。



3. 在「權限」索引標籤中、展開原則、然後按一下「編輯原則」。



4. 按一下「* JSON*」、然後在第一組動作下新增下列權限：

   - EC2：取消註冊
   - EKS：清單叢集
   - EKS：取消叢集
   - IAM：GetInstanceProfile

   "檢視原則的完整Json格式"

5. 按一下「檢閱原則」、然後按一下「儲存變更」。

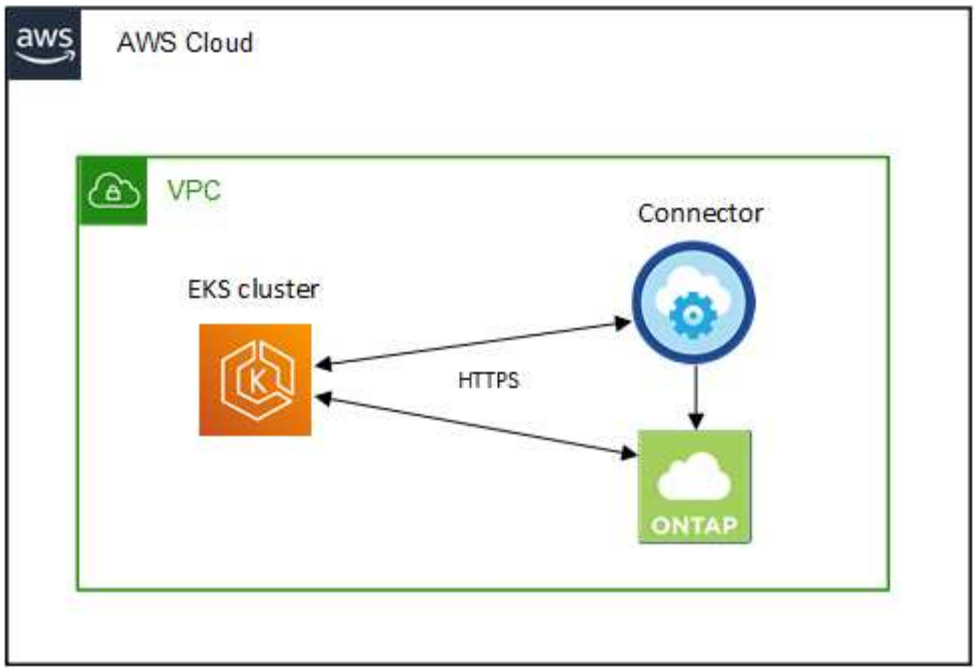
檢閱網路需求

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。

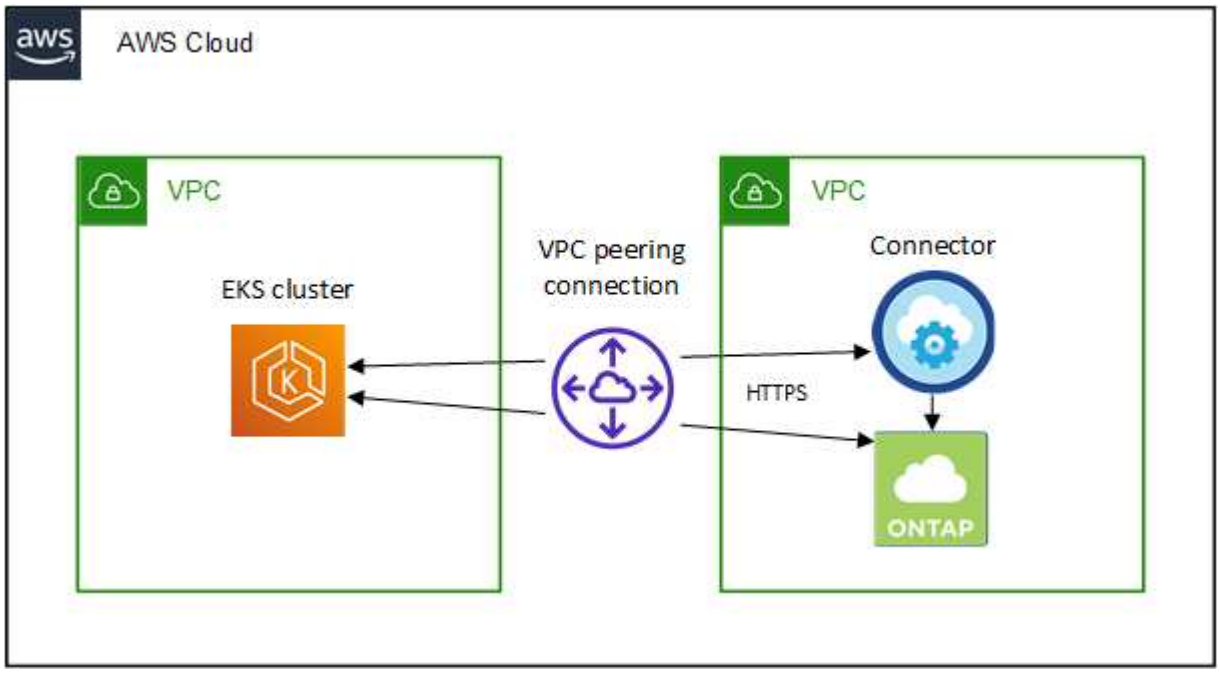
- 每個Kubernetes叢集都必須有來自Connector的傳入連線
- 連接器必須透過連接埠443連線至每個Kubernetes叢集

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

以下範例顯示同一VPC中的每個元件。



以下是另一個範例、顯示在不同VPC上執行的EKS叢集。在此範例中、VPC對等功能可在EKS叢集的VPC與連接器和Cloud Volumes ONTAP 物件的VPC之間建立連線。



設定RBAC授權

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

需要不同的授權才能啟用不同的功能。

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。

步驟

1. 建立叢集角色和角色繫結。
   a. 根據您的授權要求、建立包含下列文字的Y反 洗錢檔案。

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: Group
      name: cloudmanager-access-group
      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: Group
      name: cloudmanager-access-group
      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。

```
eksctl create iamidentitymapping --cluster < > --region < > --arn
< > --group "system:masters" --username
system:node:{{EC2PrivateDNSName}}
```

b. 將組態套用至叢集。

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

2. 建立權限群組的身分識別對應。

使用**eksctl**

使用eksctl在叢集與Cloud Manager Connector的IAM角色之間建立IAM身分識別對應。

"如需完整說明、請參閱eksctl文件"。

以下為範例。

```
eksctl create iamidentitymapping --cluster <eksCluster> --region
<us-east-2> --arn <ARN of the Connector IAM role> --group
cloudmanager-access-group --username
system:node:{{EC2PrivateDNSName}}
```

編輯**AWS/AUTH**

直接編輯AWS/AUTH ConfigMap、將RBAC存取權限新增至Cloud Manager Connector的IAM角色。

"如需完整指示、請參閱AWS EKS文件"。

以下為範例。

```
apiVersion: v1
data:
  mapRoles: |
    - groups:
      - cloudmanager-access-group
      rolearn: <ARN of the Connector IAM role>
     username: system:node:{{EC2PrivateDNSName}}
kind: ConfigMap
metadata:
  creationTimestamp: "2021-09-30T21:09:18Z"
  name: aws-auth
  namespace: kube-system
  resourceVersion: "1021"
  selfLink: /api/v1/namespaces/kube-system/configmaps/aws-auth
  uid: dcc31de5-3838-11e8-af26-02e00430057c
```

版權資訊

商標資訊