Autres façons de créer des connecteurs

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

Autres façons de créer des connecteurs

Exigences relatives à l'hôte de connecteur

Le logiciel du connecteur doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des ports, etc.

Un hôte dédié est requis

Le connecteur n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié.

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons une instance t3.XLarge d'utiliser ce type d'instance lorsque vous déployez le connecteur directement depuis Cloud Manager.

Taille des machines virtuelles Azure

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons la version DS3 v2 et d'utiliser cette taille de machine virtuelle lorsque vous déployez le connecteur directement depuis Cloud Manager.

Type de machine GCP

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons n1-standard-4 et d'utiliser ce type de machine lorsque vous déployez le connecteur directement depuis Cloud Manager.

Systèmes d'exploitation pris en charge

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation du connecteur.

  Le connecteur est pris en charge sur les versions en anglais de ces systèmes d'exploitation.

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter CentOS ou Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"^]

Espace disque dans /opt

100 Go d'espace doivent être disponibles

Accès Internet sortant

Un accès Internet sortant est nécessaire pour installer le connecteur et pour que le connecteur gère les ressources et les processus au sein de votre environnement de cloud public. Pour obtenir la liste des noeuds finaux, reportez-vous à la section "Exigences de mise en réseau pour le connecteur".

Création d'un connecteur à partir d'AWS Marketplace

Il est préférable de créer un connecteur directement depuis Cloud Manager, mais vous pouvez lancer un connecteur depuis AWS Marketplace, si vous ne souhaitez pas spécifier de clés d'accès AWS. Une fois que vous avez créé et configuré ce connecteur, Cloud Manager l'utilise automatiquement lors de la création de nouveaux environnements de travail.

Étapes

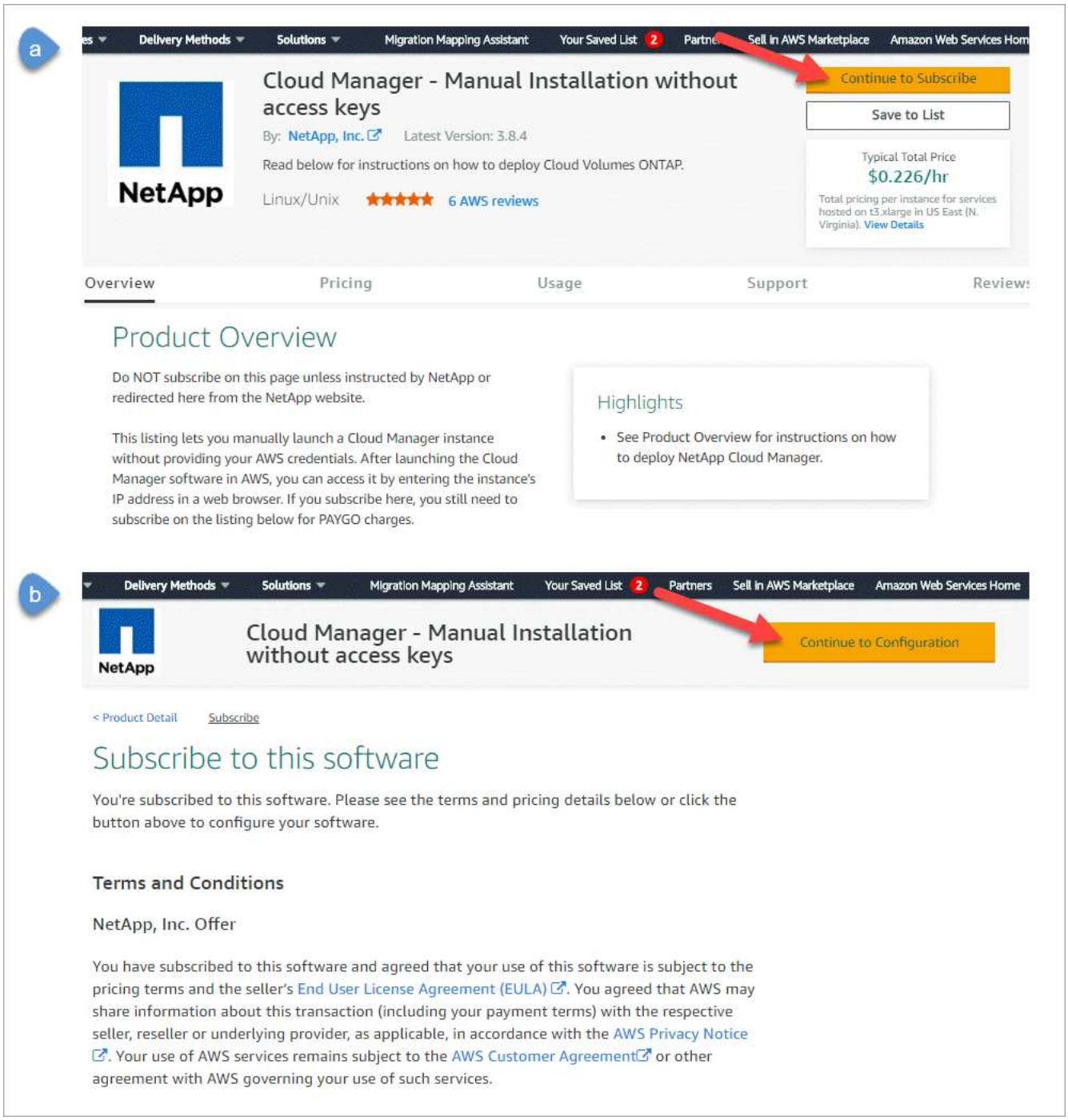
1. Créer une règle IAM et un rôle pour l'instance EC2 :
   a. Téléchargez la politique IAM de Cloud Manager à partir de l'emplacement suivant :

      "NetApp Cloud Manager : règles AWS, Azure et GCP"

   b. À partir de la console IAM, créez votre propre stratégie en copiant et en collant le texte de la stratégie IAM de Cloud Manager.
   c. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez la stratégie que vous avez créée à l'étape précédente au rôle.
2. Maintenant, allez au "Page Cloud Manager sur AWS Marketplace" Pour déployer Cloud Manager à partir d'une ami.

   L'utilisateur IAM doit disposer d'autorisations AWS Marketplace pour vous abonner et se désabonner.

3. Sur la page Marketplace, cliquez sur **Continuer pour s'abonner**, puis cliquez sur **Continuer la configuration**.



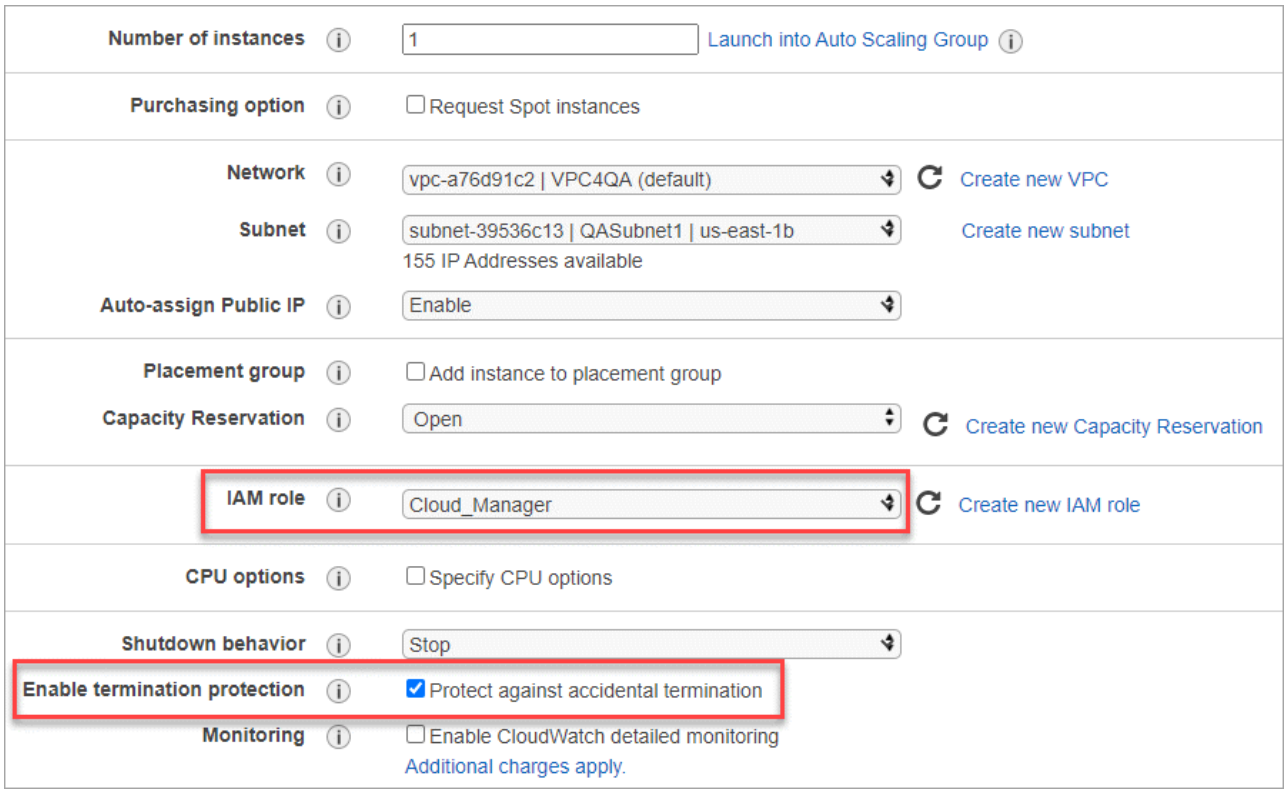
4. Modifiez l'une des options par défaut et cliquez sur **Continuer pour lancer**.
5. Sous **choisir action**, sélectionnez **lancer via EC2**, puis cliquez sur **lancer**.

   Ces étapes expliquent comment lancer l'instance à partir de la console EC2, car la console vous permet d'associer un rôle IAM à l'instance Cloud Manager. Cela n'est pas possible en utilisant l'action **lancer à partir du site Web**.

6. Suivez les invites pour configurer et déployer l'instance :
   - **Choisissez le type d'instance** : selon la disponibilité de la région, choisissez l'un des types d'instance pris en charge (t3.XLarge est recommandé).

     "Vérifiez les conditions requises pour l'instance".

- **Configurer l'instance** : sélectionnez un VPC et un sous-réseau, choisissez le rôle IAM que vous avez créé à l'étape 1, activez la protection de terminaison (recommandée) et choisissez toutes les autres options de configuration qui répondent à vos exigences.



- **Ajouter stockage** : conservez les options de stockage par défaut.
- **Ajouter des balises** : saisissez des balises pour l'instance, si vous le souhaitez.
- **Configurer le groupe de sécurité** : spécifiez les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.
- **Revue**: Passez en revue vos sélections et cliquez sur **lancer**.

  AWS lance le logiciel avec les paramètres spécifiés. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

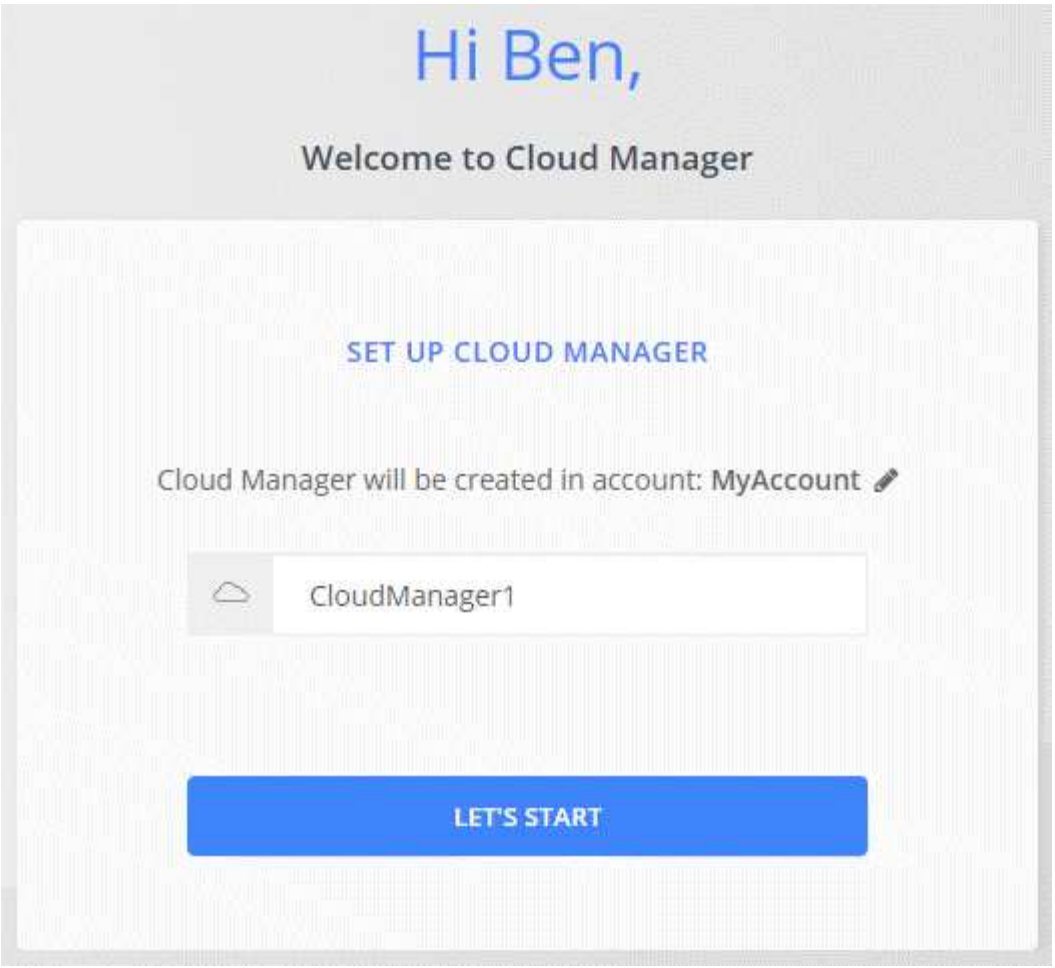
7. Ouvrez un navigateur Web à partir d'un hôte connecté à l'instance Connector et saisissez l'URL suivante :

   http://ipaddress:80

8. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré avec votre compte Cloud Central. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire "basculer entre eux".

Création d'un connecteur à partir d'Azure Marketplace

Il est préférable de créer un connecteur directement depuis Cloud Manager, mais vous pouvez également lancer un connecteur depuis Azure Marketplace, si vous préférez. Une fois que vous avez créé et configuré ce connecteur, Cloud Manager l'utilise automatiquement lors de la création de nouveaux environnements de travail.

Création d'un connecteur dans Azure

Déployez le connecteur dans Azure en utilisant l'image dans Azure Marketplace, puis connectez-vous au connecteur pour spécifier votre compte Cloud Central.

Étapes

1. "Accédez à la page Azure Marketplace pour Cloud Manager".
2. Cliquez sur **l'obtenir maintenant**, puis sur **Continuer**.
3. Sur le portail Azure, cliquez sur **Créer** et suivez les étapes de configuration de la machine virtuelle.

Noter les éléments suivants lors de la configuration de la machine virtuelle :

- Cloud Manager peut fonctionner de manière optimale avec des disques durs ou SSD.
- Choisissez une taille de machine virtuelle qui répond aux exigences en matière de CPU et de RAM. Nous recommandons DS3 v2.

  "Vérifier les exigences relatives aux machines virtuelles".

- Pour le groupe de sécurité réseau, le connecteur nécessite des connexions entrantes via SSH, HTTP et HTTPS.

  "En savoir plus sur les règles de groupe de sécurité pour le connecteur".

- Sous **Management**, activez **l'identité gérée attribuée par le système** pour le connecteur en sélectionnant **On**.

  Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s'identifier à Azure Active Directory sans fournir d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure".

4. Dans la page **Revue + créer**, vérifiez vos sélections et cliquez sur **Créer** pour démarrer le déploiement.

   Azure déploie la machine virtuelle avec les paramètres spécifiés. Le logiciel de la machine virtuelle et du connecteur doit s'exécuter en cinq minutes environ.

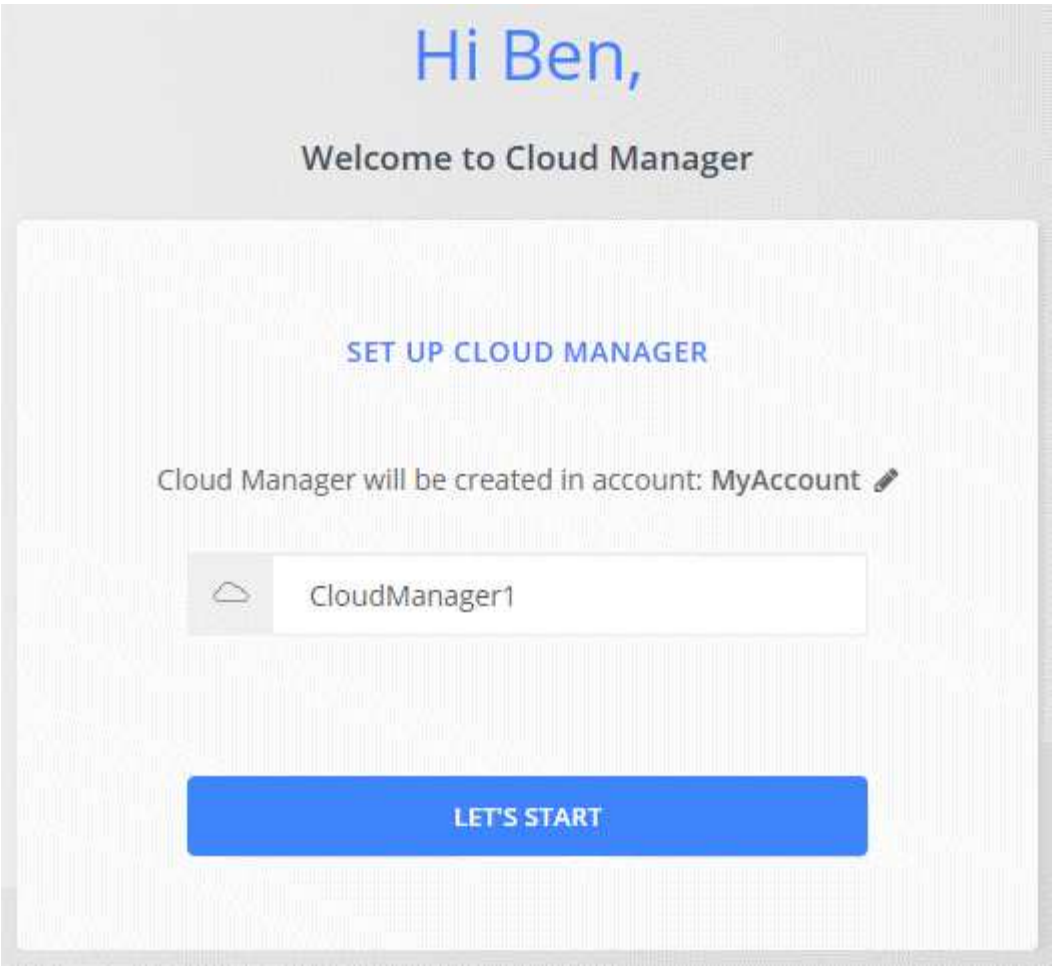
5. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

   http://ipaddress:80

6. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré. Vous devez accorder des autorisations Azure avant que les utilisateurs puissent déployer Cloud Volumes ONTAP dans Azure.

Octroi d'autorisations Azure

Lorsque vous avez déployé le connecteur dans Azure, vous devez avoir activé un "identité gérée attribuée par le système". Vous devez maintenant accorder les autorisations Azure requises en créant un rôle personnalisé, puis en attribuant le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Créez un rôle personnalisé à l'aide de la stratégie Cloud Manager :

   a. Téléchargez le "Politique de Cloud Manager Azure".

   b. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

      Vous devez ajouter l'ID de chaque abonnement Azure à partir duquel les utilisateurs créeront des systèmes Cloud Volumes ONTAP.

      Exemple

      « Assigner les Scopes » : [»/abonnements/d333af45-0d07-4154-943d-c25fbzzzzzzzzzz », «/abonnements/54b91999-b3e6-4599-908e-416e0zzzzzz », «/abonnements/8e474b-94b-4b-4b-4b-4b-4439-4b-4b-4b-4b-4b-4b-4b-4b-4b-4b-

c. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure.

   L'exemple suivant montre comment créer un rôle personnalisé à l'aide de l'interface de ligne de commande Azure CLI 2.0 :

   ```
   az role definition create --role-definition
   C:\Policy_for_cloud_Manager_Azure_3.8.7.json
   ```

Vous devez maintenant avoir un rôle personnalisé appelé opérateur Cloud Manager que vous pouvez attribuer à la machine virtuelle Connector.

2. Attribuez le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements :
   a. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
   b. Cliquez sur **contrôle d'accès (IAM)**.
   c. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **opérateur** de Cloud Manager.

        L'opérateur de Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
      - Sélectionnez la machine virtuelle Connector.
      - Cliquez sur **Enregistrer**.
   d. Si vous souhaitez déployer Cloud Volumes ONTAP à partir d'abonnements supplémentaires, passez à cet abonnement, puis répétez ces étapes.

Résultat

Le connecteur dispose désormais des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire "basculer entre eux".

Installation du logiciel de connecteur sur un hôte Linux existant

La méthode la plus courante pour créer un connecteur consiste à partir de Cloud Manager ou du Marketplace d'un fournisseur cloud. Mais vous avez la possibilité de télécharger et d'installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud.

Pour créer un système Cloud Volumes ONTAP dans Google Cloud, vous devez également disposer d'un connecteur exécuté dans Google Cloud. Vous ne pouvez pas utiliser un connecteur qui fonctionne à un autre emplacement.

De formation

- L'hôte doit se réunir "Configuration requise pour le connecteur".
- Un système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation.
- Le programme d'installation du connecteur accède à plusieurs URL pendant le processus d'installation. Vous devez vous assurer que l'accès Internet sortant est autorisé à ces noeuds finaux :
  - http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
  - https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  - https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

    L'hôte peut essayer de mettre à jour les packages du système d'exploitation lors de l'installation. L'hôte peut contacter différents sites de mise en miroir pour ces packages OS.

Description de la tâche

- Les privilèges root ne sont pas nécessaires pour installer le connecteur.
- L'installation installe les outils de ligne de commande AWS (awscli), afin d'activer les procédures de reprise à partir du support NetApp.

  Si vous recevez un message indiquant que l'installation de awscli a échoué, vous pouvez ignorer le message en toute sécurité. Le connecteur peut fonctionner sans outils.

- Le programme d'installation disponible sur le site du support NetApp peut être une version antérieure. Après l'installation, le connecteur se met automatiquement à jour si une nouvelle version est disponible.

Étapes

1. Téléchargez le logiciel Cloud Manager sur le "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Pour obtenir de l'aide sur la connexion et la copie du fichier vers une instance EC2 dans AWS, reportez-vous à la section "Documentation AWS : connexion à votre instance Linux à l'aide de SSH".

2. Attribuez des autorisations pour exécuter le script.

   Exemple

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Exécutez le script d'installation :
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent exécute l'installation sans vous demander des informations.

   proxy est requis si l'hôte est derrière un serveur proxy.

   proxyport est le port du serveur proxy.

   proxyuser est le nom d'utilisateur du serveur proxy, si une authentification de base est requise.

proxypwd est le mot de passe du nom d'utilisateur que vous avez spécifié.

3. Sauf si vous avez spécifié le paramètre silencieux, tapez **y** pour continuer le script, puis entrez les ports HTTP et HTTPS lorsque vous y êtes invité.

   Cloud Manager est maintenant installé. À la fin de l'installation, le service Cloud Manager (occm) redémarre deux fois si vous avez spécifié un serveur proxy.

4. Ouvrez un navigateur Web et entrez l'URL suivante :

   https://ipaddress:port

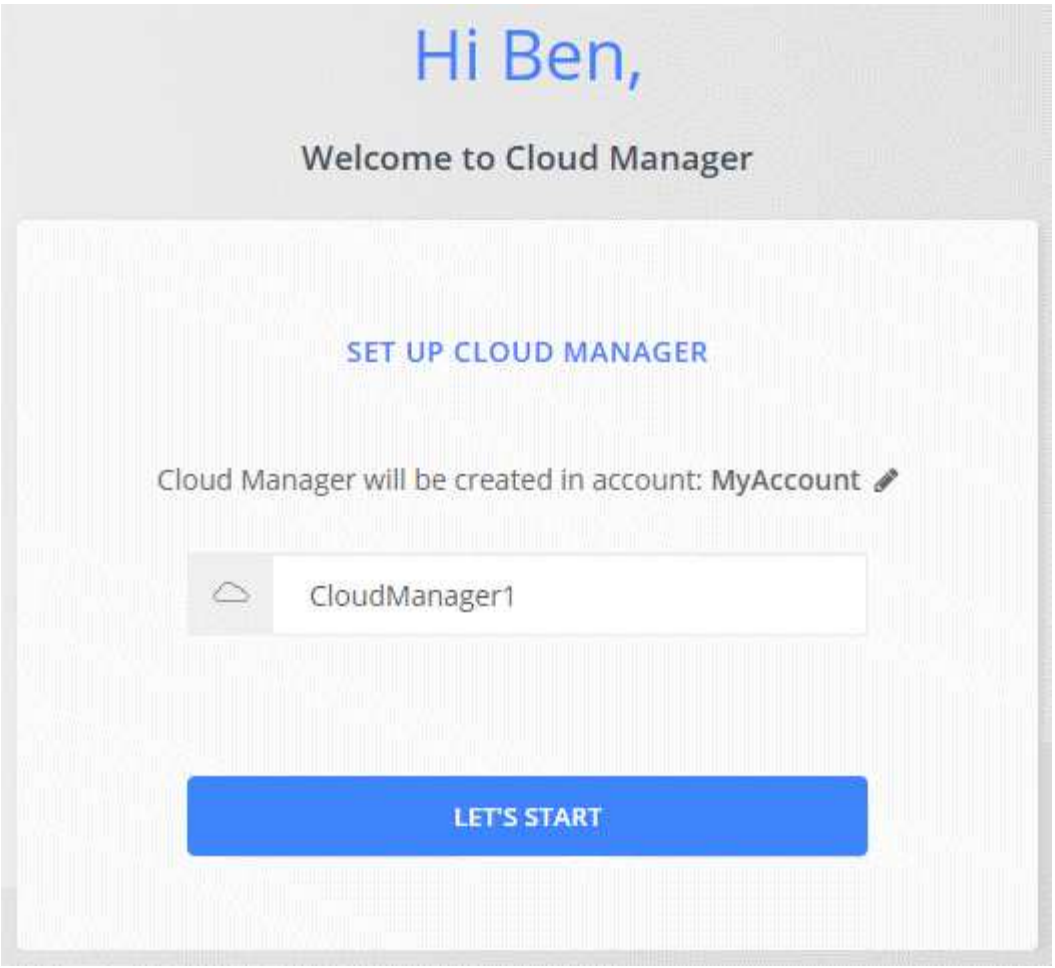
   Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte. Par exemple, si le connecteur est dans le Cloud public sans adresse IP publique, vous devez entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

   Port est nécessaire si vous avez modifié les ports HTTP (80) ou HTTPS (443) par défaut. Par exemple, si le port HTTPS a été modifié en 8443, vous pouvez entrer https://ipaddress:8443

5. Inscrivez-vous sur NetApp Cloud Central ou connectez-vous.
6. Une fois connecté, configurez Cloud Manager :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré avec votre compte Cloud Central. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail.

Une fois que vous avez terminé

Configurez des autorisations pour que Cloud Manager puisse gérer les ressources et les processus dans votre environnement de cloud public :

- AWS : "Configurez un compte AWS, puis ajoutez-le à Cloud Manager".
- Azure : "Configurez un compte Azure, puis ajoutez-le à Cloud Manager".
- GCP : configurez un compte de service disposant des autorisations nécessaires à Cloud Manager pour créer et gérer des systèmes Cloud Volumes ONTAP dans des projets.
  a. "Créer un rôle dans GCP" qui inclut les autorisations définies dans le "Règle Cloud Manager pour GCP".
  b. "Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer".
  c. "Associer ce compte de service à la VM Connector".
  d. Si vous souhaitez déployer Cloud Volumes ONTAP dans d'autres projets, "Accordez l'accès en ajoutant le compte de service avec le rôle Cloud Manager à ce projet". Vous devrez répéter cette étape pour chaque projet.

Informations sur le copyright

Informations sur les marques commerciales