Azure credentials

Set up and administration

NetApp
July 18, 2022

目录

Azure credentials

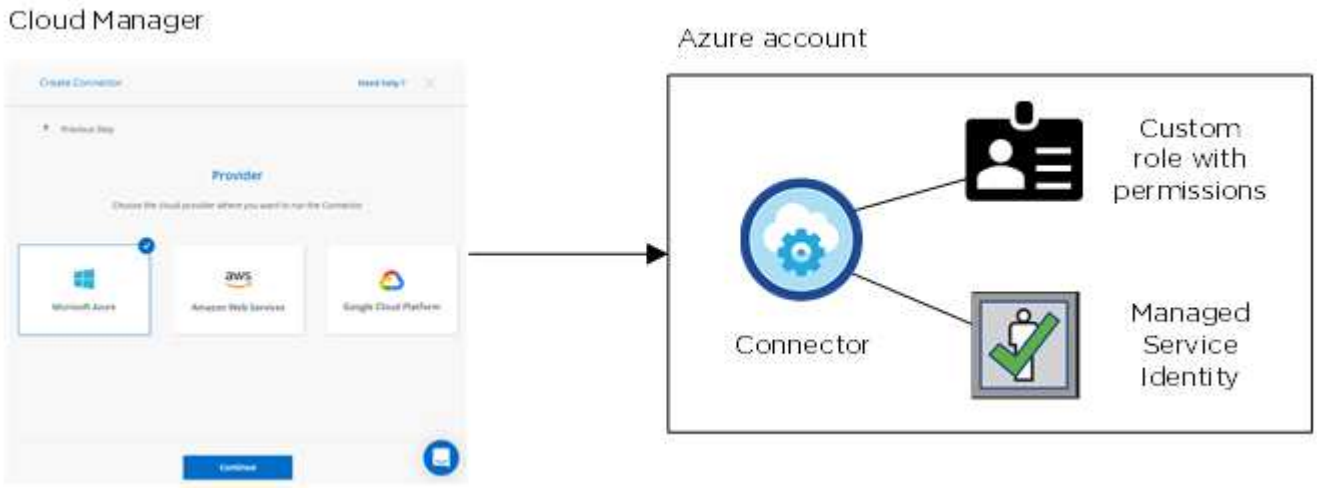
Azure 凭据和权限

通过 Cloud Manager ，您可以选择部署 Cloud Volumes ONTAP 时要使用的 Azure 凭据。您可以使用初始 Azure 凭据部署所有 Cloud Volumes ONTAP 系统，也可以添加其他凭据。

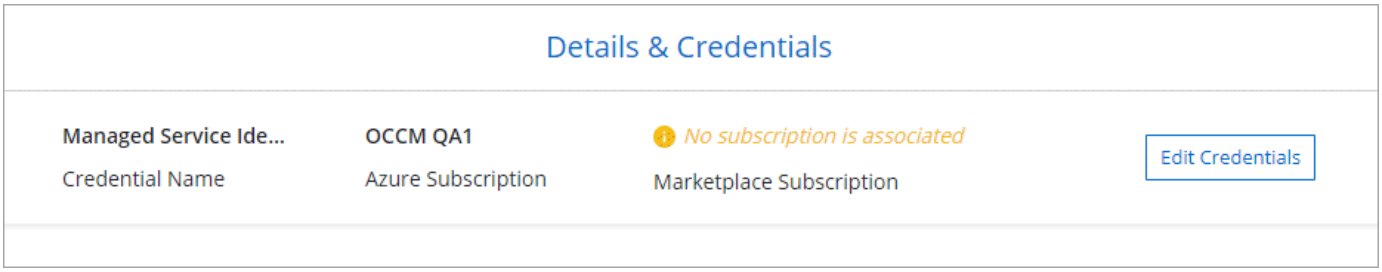
初始 **Azure** 凭据

从 Cloud Manager 部署 Connector 时，您需要使用有权部署 Connector 虚拟机的 Azure 帐户或服务主体。中列出了所需的权限 "适用于 Azure 的连接器部署策略"。

当 Cloud Manager 在 Azure 中部署 Connector 虚拟机时，它会启用 "系统分配的受管身份" 在虚拟机上，创建自定义角色并将其分配给虚拟机。此角色为 Cloud Manager 提供了管理该 Azure 订阅中的资源和流程的权限。 "查看 Cloud Manager 如何使用权限"。



在为 Cloud Volumes ONTAP 创建新工作环境时， Cloud Manager 会默认选择以下 Azure 凭据：

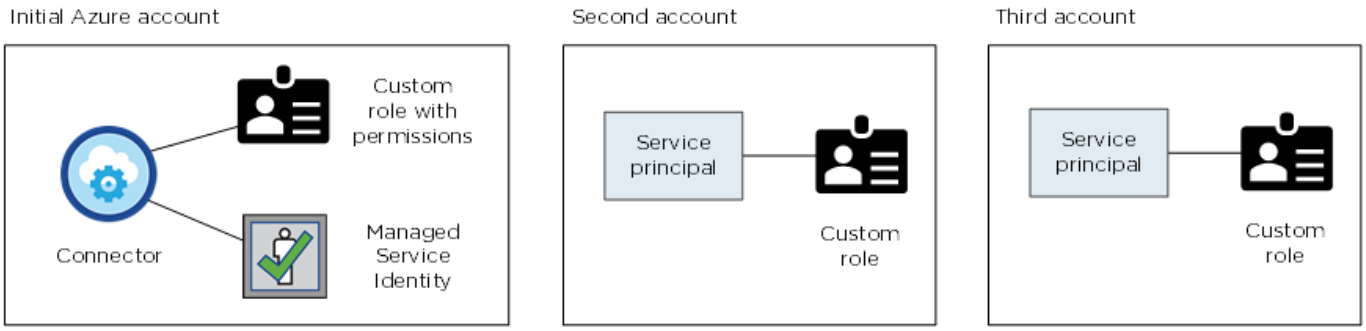


为受管身份订阅其他 **Azure**

托管身份与启动 Connector 的订阅相关联。如果要选择其他 Azure 订阅，则需要 "将托管身份与这些订阅相关联"。

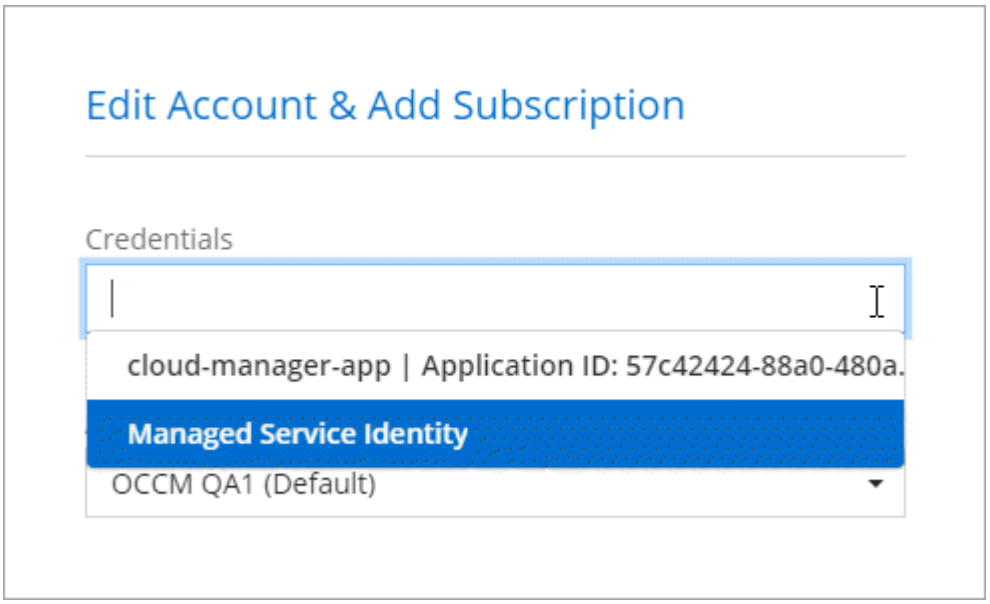
其他 Azure 凭据

如果要使用不同的 Azure 凭据部署 Cloud Volumes ONTAP ，则必须通过授予所需权限 "在 Azure Active Directory 中创建和设置服务主体" 对于每个 Azure 帐户。下图显示了另外两个帐户，每个帐户都设置有一个服务主体和一个提供权限的自定义角色：



您可以这样做 "将帐户凭据添加到 Cloud Manager" 提供有关 AD 服务主体的详细信息。

添加另一组凭据后，您可以在创建新的工作环境时切换到这些凭据：



市场部署和内部部署如何?

以上各节介绍了从 NetApp Cloud Central 为 Connector 推荐的部署方法。您也可以从在 Azure 中部署 Connector "Azure Marketplace"，您可以 "在内部安装 Connector"。

如果您使用 Marketplace ，则会以相同方式提供权限。您只需手动创建并设置 Connector 的托管身份，然后为任何其他帐户提供权限即可。

对于内部部署，您不能为 Connector 设置托管身份，但可以像使用服务主体为其他帐户提供权限一样提供权限。

管理 Cloud Manager 的 Azure 凭据和订阅

创建 Cloud Volumes ONTAP 系统时，您需要选择要用于该系统的 Azure 凭据。如果您使用的是按需购买许可，则还需要选择 Marketplace 订阅。如果您需要使用多个 Azure 凭据或多个适用于 Cloud Volumes ONTAP 的 Azure Marketplace 订阅，请按照此页面上的步骤进行操作。

可以通过两种方式在 Cloud Manager 中添加其他 Azure 订阅和凭据。

1. 将其他 Azure 订阅与 Azure 托管身份关联。
2. 如果要使用不同的 Azure 凭据部署 Cloud Volumes ONTAP ，请使用服务主体授予 Azure 权限，并将其凭据添加到 Cloud Manager 。

将其他 Azure 订阅与受管身份关联

通过 Cloud Manager ，您可以选择要在其中部署 Cloud Volumes ONTAP 的 Azure 凭据和 Azure 订阅。除非关联，否则您无法为托管身份配置文件选择其他 Azure 订阅 "托管身份" 这些订阅。

托管身份为 "初始 Azure 帐户" 从 Cloud Manager 部署 Connector 时。部署 Connector 时， Cloud Manager 会创建 Cloud Manager 操作员角色并将其分配给 Connector 虚拟机。

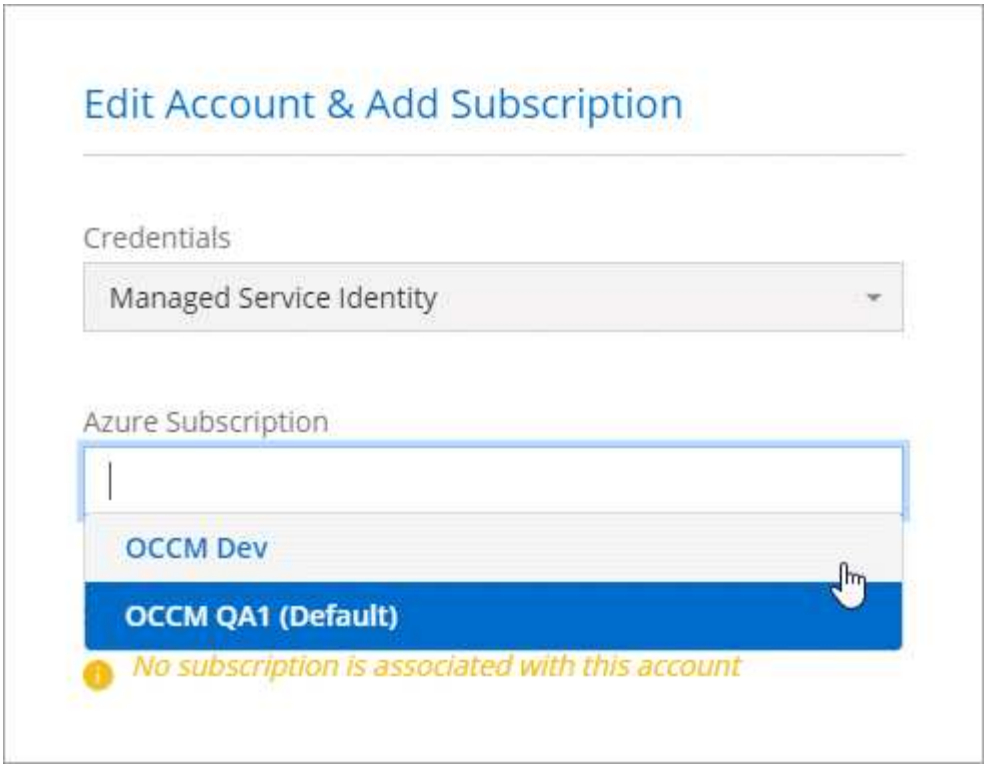
步骤

1. 登录 Azure 门户。
2. 打开 * 订阅 * 服务，然后选择要部署 Cloud Volumes ONTAP 的订阅。
3. 单击 * 访问控制（ IAM ） * 。
    a. 单击 * 添加 * > * 添加角色分配 * ，然后添加权限：
        - 选择 * Cloud Manager Operator* 角色。

        > Cloud Manager Operator是Connector策略中提供的默认名称。如果您为角色选择了其他名称，请选择该名称。

        - 分配对 * 虚拟机 * 的访问权限。
        - 选择创建 Connector 虚拟机的订阅。
        - 选择 Connector 虚拟机。
        - 单击 * 保存 * 。
4. 对其他订阅重复这些步骤。

创建新的工作环境时，您现在应该能够为托管身份配置文件从多个 Azure 订阅中进行选择。



向 **Cloud Manager** 添加其他 **Azure** 凭据

从 Cloud Manager 部署 Connector 时， Cloud Manager 会在具有所需权限的虚拟机上启用系统分配的托管身份。在为 Cloud Volumes ONTAP 创建新工作环境时， Cloud Manager 会默认选择以下 Azure 凭据：

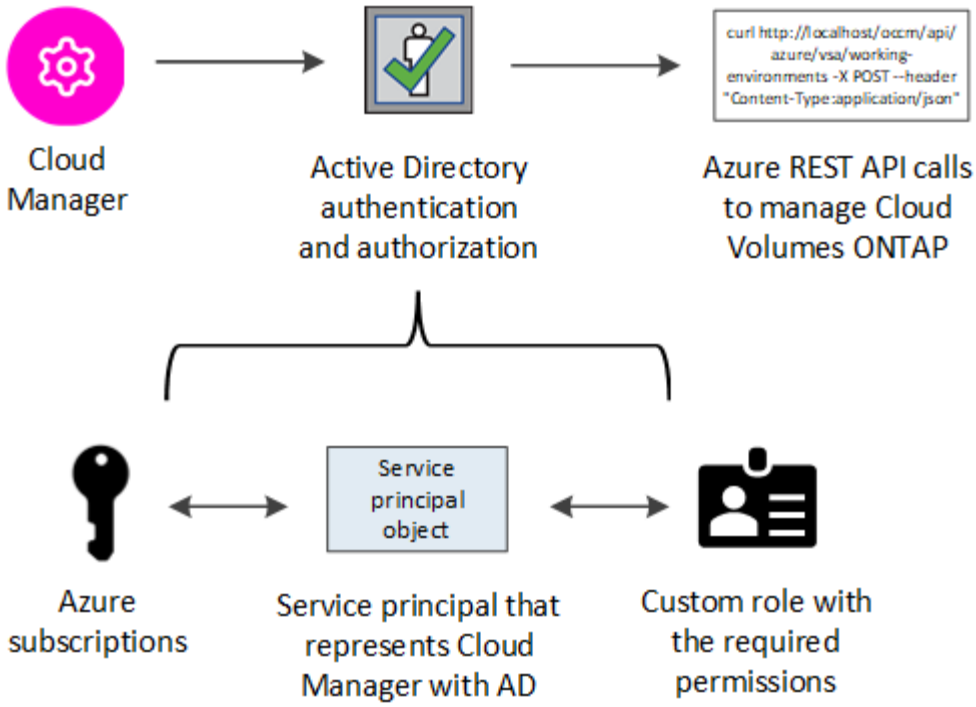
如果在现有系统上手动安装 Connector 软件，则不会添加一组初始凭据。 "了解 Azure 凭据和权限"。

如果您要使用 *Different* Azure 凭据部署 Cloud Volumes ONTAP ，则必须通过在 Azure Active Directory 中为每个 Azure 帐户创建和设置服务主体来授予所需权限。然后，您可以将新凭据添加到 Cloud Manager 。

使用服务主体授予 **Azure** 权限

Cloud Manager 需要权限才能在 Azure 中执行操作。您可以通过在 Azure Active Directory 中创建和设置服务主体以及获取 Cloud Manager 所需的 Azure 凭据来为 Azure 帐户授予所需权限。

下图描述了 Cloud Manager 如何获得在 Azure 中执行操作的权限。与一个或多个 Azure 订阅绑定的服务主体对象表示 Azure Active Directory 中的 Cloud Manager 并分配给允许所需权限的自定义角色。



步骤

1. 创建 Azure Active Directory 应用程序。
2. 将应用程序分配给角色。
3. 添加 Windows Azure 服务管理 API 权限。
4. 获取应用程序 ID 和目录 ID。
5. 创建客户端密钥。

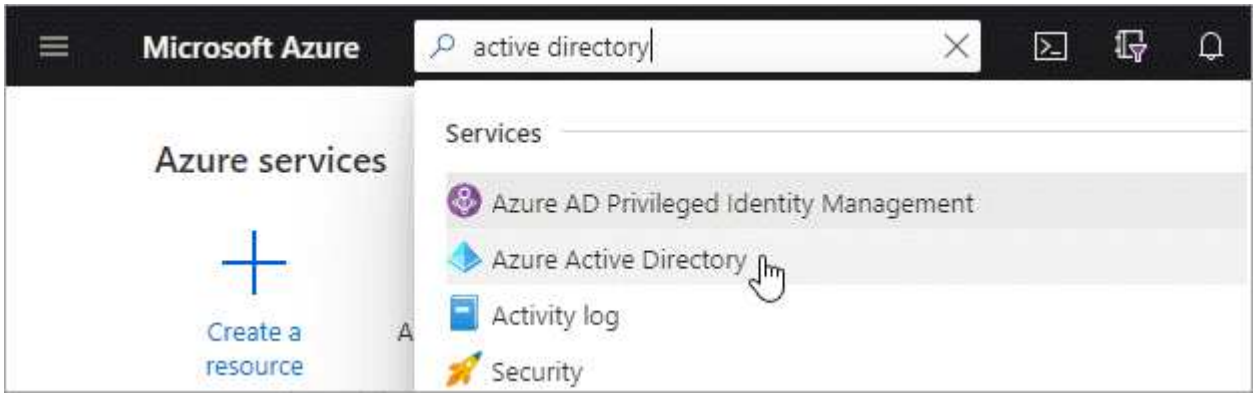
创建 **Azure Active Directory** 应用程序

创建一个 Azure Active Directory （ AD ）应用程序和服务主体， Cloud Manager 可使用该应用程序和服务主体进行基于角色的访问控制。

要创建 Active Directory 应用程序并将此应用程序分配给角色，您必须在 Azure 中拥有适当的权限。有关详细信息，请参见 "Microsoft Azure 文档：所需权限"。

步骤

1. 从 Azure 门户中，打开 * Azure Active Directory* 服务。



2. 在菜单中，单击 * 应用程序注册 * 。
3. 单击 * 新建注册 * 。
4. 指定有关应用程序的详细信息：
   - * 名称 * ： 输入应用程序的名称。
   - * 帐户类型 * ： 选择帐户类型（任何将适用于 Cloud Manager ）。
   - * 重定向 URI* ： 可以将此字段留空。
5. 单击 * 注册 * 。

您已创建 AD 应用程序和服务主体。

将应用程序分配给角色

您必须将服务主体绑定到一个或多个 OnCommand 订阅，并为其分配自定义 "Cloud Manager 操作员 " 角色，以便 管理器在 Azure 中具有权限。

步骤

1. 创建自定义角色：
   a. 复制的内容 "Connector的自定义角色权限" 并将其保存在JSON文件中。
   b. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

      您应该为每个 Azure 订阅添加 ID 、用户将从中创建 Cloud Volumes ONTAP 系统。

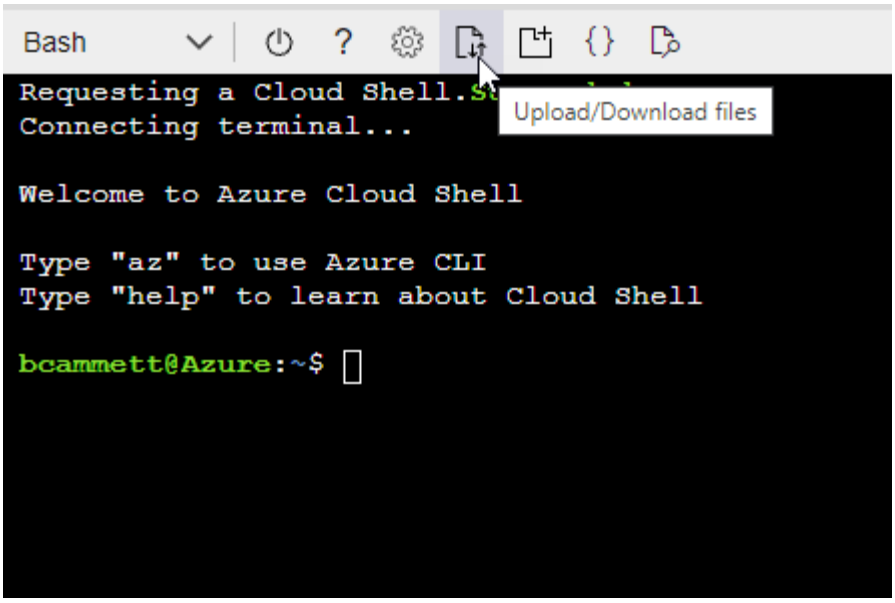
      - 示例 *

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. 使用 JSON 文件在 Azure 中创建自定义角色。

      以下步骤介绍如何在 Azure Cloud Shell 中使用 Bash 创建角色。

      - start "Azure Cloud Shell" 并选择 Bash 环境。
      - 上传 JSON 文件。



- 输入以下 Azure 命令行界面命令：

```
az role definition create --role-definition
Policy_for_Setup_As_Service_Azure.json
```

现在，您应该拥有一个名为 Cloud Manager Operator 的自定义角色，可以将该角色分配给 Connector 虚拟机。

2. 将应用程序分配给角色：

a. 从 Azure 门户中，打开 * 订阅 * 服务。

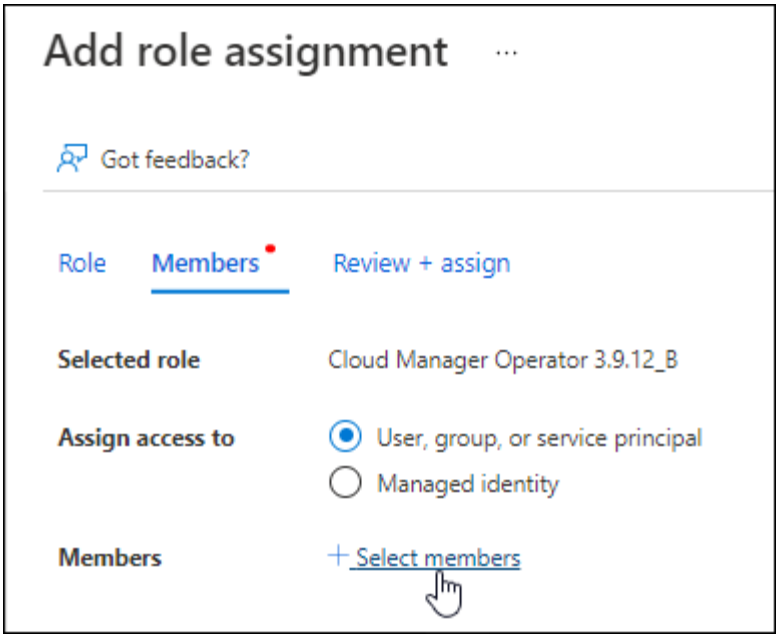
b. 选择订阅。

c. 单击 * 访问控制（ IAM ） > 添加 > 添加角色分配 * 。

d. 在 * 角色 * 选项卡中，选择 * Cloud Manager 操作员 * 角色，然后单击 * 下一步 * 。

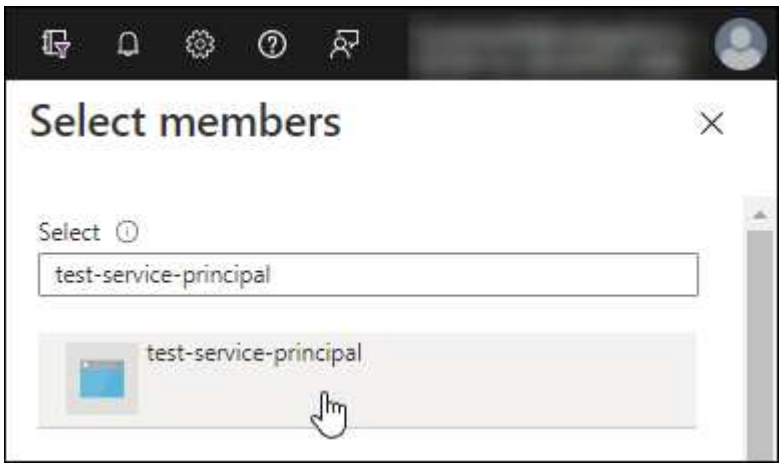
e. 在 * 成员 * 选项卡中，完成以下步骤：

- 保持选中 * 用户，组或服务主体 * 。
- 单击 * 选择成员 * 。



- 搜索应用程序的名称。

  以下是一个示例：



- 选择应用程序并单击 * 选择 * 。
- 单击 * 下一步 * 。

f. 单击 * 审核 + 分配 * 。

现在，服务主体具有部署 Connector 所需的 Azure 权限。

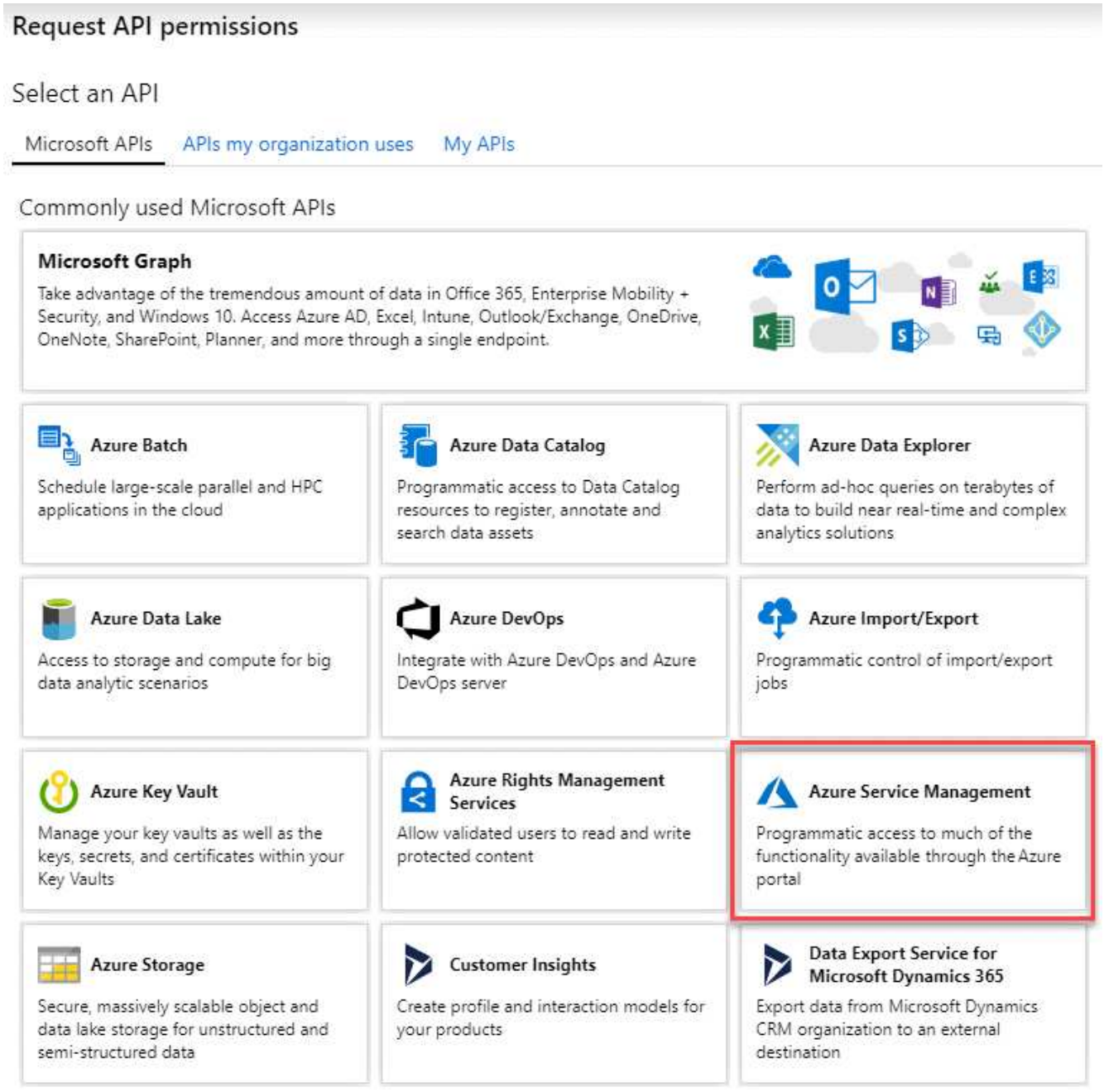
如果要从多个 Azure 订阅部署 Cloud Volumes ONTAP ，则必须将服务主体绑定到每个订阅。使用 Cloud Manager ，您可以选择部署 Cloud Volumes ONTAP 时要使用的订阅。

添加 **Windows Azure** 服务管理 **API** 权限

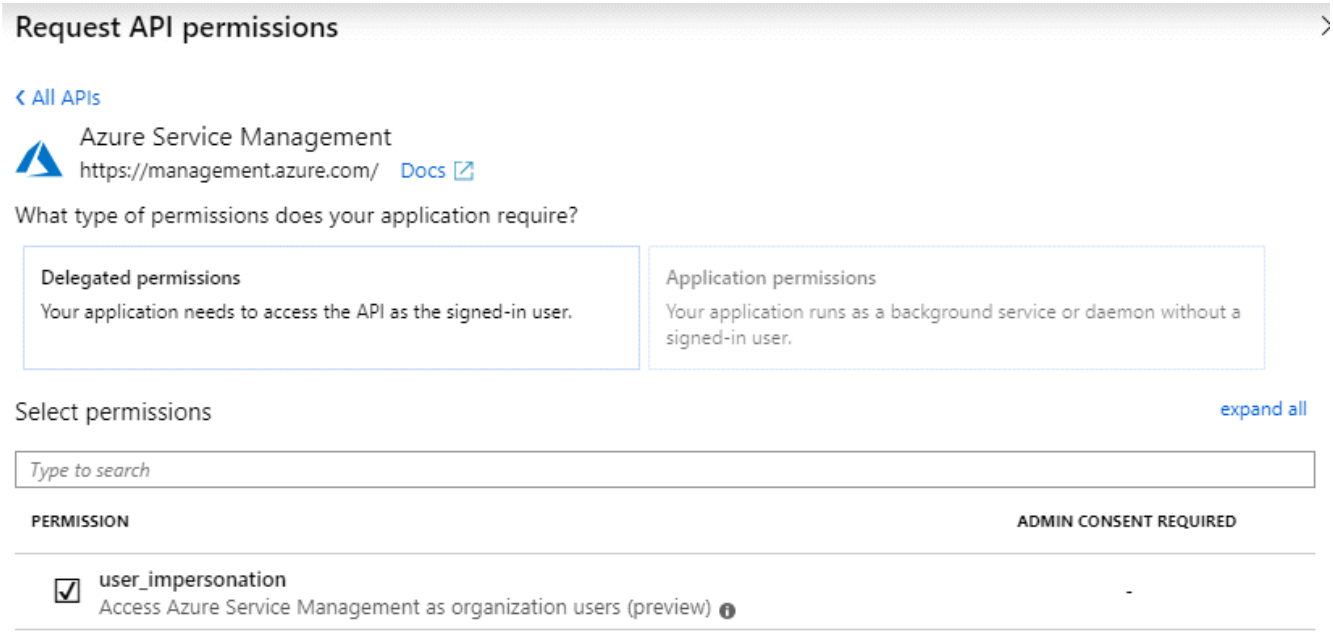
服务主体必须具有 "Windows Azure 服务管理 API" 权限。

步骤

1. 在 * Azure Active Directory* 服务中，单击 * 应用程序注册 * 并选择应用程序。
2. 单击 * API 权限 > 添加权限 * 。
3. 在 * Microsoft APIs* 下，选择 * Azure Service Management* 。



4. 单击 * 以组织用户身份访问 Azure 服务管理 * ，然后单击 * 添加权限 * 。

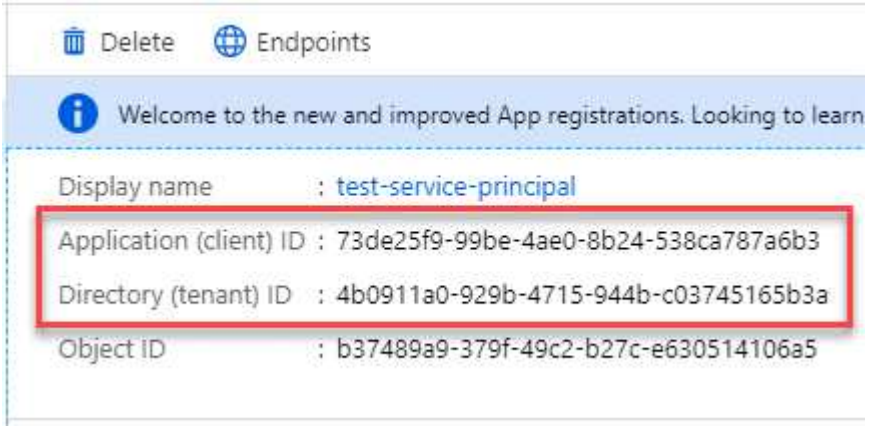


获取应用程序 **ID** 和目录 **ID**

将 Azure 帐户添加到 Cloud Manager 时，您需要提供应用程序（客户端） ID 和目录（租户） ID 。Cloud Manager 使用 ID 以编程方式登录。

步骤

1. 在 * Azure Active Directory* 服务中，单击 * 应用程序注册 * 并选择应用程序。
2. 复制 * 应用程序（客户端） ID* 和 * 目录（租户） ID* 。



创建客户端密钥

您需要创建客户端密钥，然后向 Cloud Manager 提供该密钥的值，以便 Cloud Manager 可以使用它向 Azure AD 进行身份验证。

步骤

1. 打开 * Azure Active Directory* 服务。
2. 单击 * 应用程序注册 * 并选择您的应用程序。

3. 单击 * 证书和密码 > 新客户端密钥 * 。
4. 提供密钥和持续时间的问题描述。
5. 单击 * 添加 * 。
6. 复制客户端密钥的值。

此时，您的服务主体已设置完毕，您应已复制应用程序（客户端） ID ，目录（租户） ID 和客户端密钥值。添加 Azure 帐户时，您需要在 Cloud Manager 中输入此信息。

将凭据添加到 **Cloud Manager**

在为 Azure 帐户提供所需权限后，您可以将该帐户的凭据添加到 Cloud Manager 中。完成此步骤后，您可以使用不同的 Azure 凭据启动 Cloud Volumes ONTAP 。

如果您刚刚在云提供商中创建了这些凭据，则可能需要几分钟的时间才能使用这些凭据。请等待几分钟，然后再将凭据添加到 Cloud Manager 。

您需要先创建 Connector ，然后才能更改 Cloud Manager 设置。 "了解如何操作"。

步骤

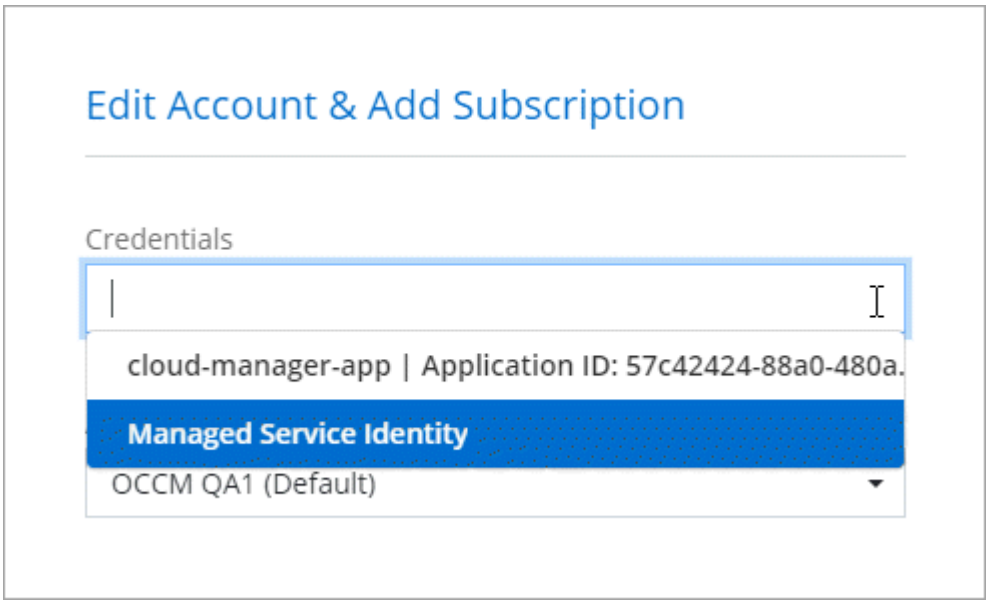
1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。

2. 单击 * 添加凭据 * ，然后按照向导中的步骤进行操作。
   a. * 凭据位置 * ： 选择 * Microsoft Azure > Connector* 。
   b. * 定义凭据 * ： 输入有关授予所需权限的 Azure Active Directory 服务主体的信息：
      - 应用程序（客户端） ID ： 请参见 [Getting the application ID and directory ID]。
      - 目录（租户） ID ： 请参见 [Getting the application ID and directory ID]。
      - 客户端密钥：请参见 [Creating a client secret]。
   c. * 市场订阅 * ： 通过立即订阅或选择现有订阅，将市场订阅与这些凭据相关联。

      要按每小时费率（ PAYGO ）购买 Cloud Volumes ONTAP ，这些 Azure 凭据必须与 Azure Marketplace 中的订阅相关联。

d. * 查看 * ： 确认有关新凭据的详细信息，然后单击 * 添加 * 。

现在，您可以从 " 详细信息和凭据 " 页面切换到不同的凭据集 "创建新的工作环境时"



管理现有凭据

通过关联 Marketplace 订阅，编辑凭据并将其删除，管理已添加到 Cloud Manager 的 Azure 凭据。

将 **Azure Marketplace** 订阅与凭据关联

将 Azure 凭据添加到 Cloud Manager 后，您可以将 Azure Marketplace 订阅与这些凭据相关联。通过订阅，您可以创建按需购买的 Cloud Volumes ONTAP 系统并使用其他 NetApp 云服务。

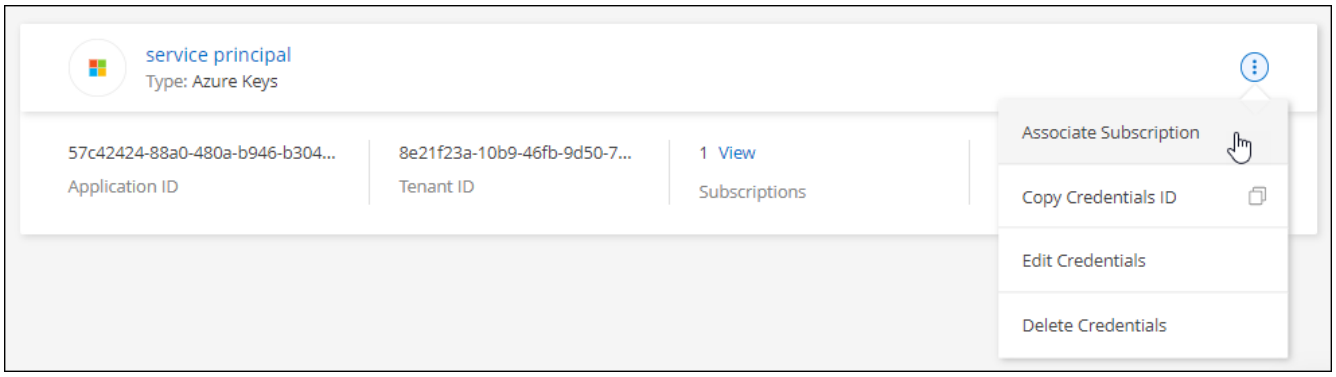
在以下两种情况下，您可能会在将凭据添加到 Cloud Manager 后关联 Azure Marketplace 订阅：

- 最初将凭据添加到 Cloud Manager 时，您未关联订阅。
- 您希望将现有 Azure Marketplace 订阅替换为新订阅。

您需要先创建 Connector ，然后才能更改 Cloud Manager 设置。 "了解如何操作"。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。
2. 单击一组凭据的操作菜单，然后选择 * 关联订阅 * 。



3. 从下拉列表中选择订阅或单击 * 添加订阅 * ，然后按照步骤创建新订阅。

   以下视频从工作环境向导的上下文中启动，但在您单击 * 添加订阅 * 后显示相同的工作流：

   ► https://docs.netapp.com/zh-cn/cloud-manager-setup-admin//media/video_subscribing_azure.mp4

(video)

编辑凭据

通过修改 Azure 服务凭据的详细信息，在 Cloud Manager 中编辑 Azure 凭据。例如，如果为服务主体应用程序创建了新密钥，则可能需要更新客户端密钥。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。
2. 单击一组凭据的操作菜单，然后选择 * 编辑凭据 * 。
3. 进行所需的更改，然后单击 * 应用 * 。

正在删除凭据

如果您不再需要一组凭据，可以从 Cloud Manager 中删除这些凭据。您只能删除与工作环境无关的凭据。

步骤

1. 在 Cloud Manager 控制台的右上角，单击设置图标，然后选择 * 凭据 * 。
2. 单击一组凭据的操作菜单，然后选择 * 删除凭据 * 。
3. 单击 * 删除 * 进行确认。