



## 设置连接器 Set up and administration

NetApp  
July 17, 2022

# 目录

- 设置连接器 ..... 1
  - 了解连接器 ..... 1
  - 为连接器设置网络连接 ..... 5
  - 从 Cloud Manager 在 AWS 中创建连接器 ..... 9
  - 从 Cloud Manager 在 Azure 中创建 Connector ..... 14
  - 从 Cloud Manager 在 Google Cloud 中创建 Connector ..... 28

# 设置连接器

## 了解连接器

大多数情况下，客户管理员需要在云或内部网络中部署 *Connector*。连接器是 Cloud Manager 日常使用的关键组件。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。

### 需要连接器时

要使用 Cloud Manager 中的许多功能和服务，需要使用 Connector。

#### 服务

- 适用于 ONTAP 的 Amazon FSX 管理功能
- Amazon S3发现
- Azure Blob发现
- 云备份
- 云数据感知
- 云分层
- Cloud Volumes ONTAP
- 全局文件缓存
- Google Cloud Storage发现
- Kubernetes 集群
- 监控
- 内部 ONTAP 集群

以下服务需要使用连接器 \*。not\_\*：

- Active IQ 数字顾问
- 创建适用于 ONTAP 的 Amazon FSx 工作环境虽然创建工作环境不需要使用 Connector，但需要使用它来创建和管理卷，复制数据以及将适用于 ONTAP 的 FSx 与 Data sense 和 Cloud Sync 等 NetApp 云服务集成。
- Azure NetApp Files

虽然设置和管理 Azure NetApp Files 不需要连接器，但如果要使用云数据感知扫描 Azure NetApp Files 数据，则需要连接器。

- 适用于 Google Cloud 的 Cloud Volumes Service
- Cloud Sync

## 数字电子钱包

在几乎所有情况下，您都可以在没有连接器的情况下向数字电子钱包添加许可证。

只有在使用 Cloud Volumes ONTAP \_node-based\_ 许可证时，才需要使用 Connector 向数字电子钱包添加许可证。在这种情况下，需要使用连接器，因为数据是从 Cloud Volumes ONTAP 系统上安装的许可证中获取的。

## 支持的位置

以下位置支持连接器：

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- 在您的内部环境中
- 在您的内部环境中，无法访问 Internet

请注意 **Azure** 部署

如果在 Azure 中部署连接器，则应将其部署在与所管理的 Cloud Volumes ONTAP 系统相同的 Azure 区域中，或者部署在中 ["Azure 区域对"](#) 对于 Cloud Volumes ONTAP 系统。此要求可确保在 Cloud Volumes ONTAP 与其关联存储帐户之间使用 Azure 专用链路连接。 ["了解 Cloud Volumes ONTAP 如何使用 Azure 专用链路"](#)。

有关 **Google Cloud** 部署的注意事项

如果要在 Google Cloud 中创建 Cloud Volumes ONTAP 系统，则必须同时在 Google Cloud 中运行 Connector。您不能使用在 AWS，Azure 或内部运行的 Connector。

## 连接器应保持运行状态

连接器应始终保持运行状态。对于您启用的服务的持续运行状况和运行来说，这一点非常重要。

例如，连接器是 Cloud Volumes ONTAP 运行状况和运行的关键组件。如果某个连接器已关闭，则使用基于节点的许可的 Cloud Volumes ONTAP PAYGO 系统将在与某个连接器失去通信超过 14 天之后关闭。

## 如何创建 **Connector**

在工作空间管理员创建 Cloud Volumes ONTAP 工作环境并使用上述任何其他服务之前，客户管理员需要先创建连接器。管理员可以通过多种方式创建 Connector：

- 直接从 Cloud Manager（建议）
  - ["在 AWS 中创建"](#)
  - ["在 Azure 中创建"](#)
  - ["在 GCP 中创建"](#)
- 在您自己的 Linux 主机上手动安装软件
  - ["在可访问 Internet 的主机上"](#)

- ["在无法访问 Internet 的内部主机上"](#)
- 来自云提供商的市场
  - ["AWS Marketplace"](#)
  - ["Azure Marketplace"](#)

如果需要创建一个 Connector 来完成操作，Cloud Manager 将提示您创建一个连接器。

## 权限

创建 Connector 需要特定权限，而 Connector 实例本身也需要另一组权限。

### 创建 **Connector** 的权限

从 Cloud Manager 创建 Connector 的用户需要特定权限才能在您选择的云提供商中部署此实例。Cloud Manager 将在您创建 Connector 时提醒您权限要求。

- ["查看所需的AWS权限"](#)
- ["查看所需的Azure权限"](#)
- ["查看所需的Google Cloud权限"](#)

### **Connector** 实例的权限

Connector 需要特定的云提供商权限才能代表您执行操作。例如，部署和管理 Cloud Volumes ONTAP。

直接从 Cloud Manager 创建 Connector 时，Cloud Manager 会使用所需权限创建 Connector。您无需执行任何操作。

如果您自己从 AWS Marketplace，Azure Marketplace 或通过手动安装软件来创建 Connector，则需要确保已设置正确的权限。

- ["了解Connector如何使用AWS权限"](#)
- ["了解Connector如何使用Azure权限"](#)
- ["了解Connector如何使用Google Cloud权限"](#)

## 连接器升级

我们通常每月更新一次 Connector 软件，以引入新功能并提高稳定性。虽然 Cloud Manager 平台中的大多数服务和功能均通过基于 SaaS 的软件提供，但有几项特性和功能取决于 Connector 的版本。其中包括 Cloud Volumes ONTAP 管理，内部 ONTAP 集群管理，设置和帮助。

只要有最新版本，Connector 就会自动将其软件更新到最新版本 ["出站 Internet 访问"](#) 以获取软件更新。

## 每个连接器的工作环境数量

Connector 可以在 Cloud Manager 中管理多个工作环境。一个 Connector 应管理的最大工作环境数因情况而异。具体取决于工作环境的类型，卷数量，要管理的容量以及用户数量。

如果您要进行大规模部署，请与 NetApp 代表合作来估算您的环境规模。如果您在此过程中遇到任何问题，请通

过产品内聊天联系我们。

## 何时使用多个连接器

在某些情况下，您可能只需要一个连接器，但可能需要两个或更多连接器。

以下是几个示例：

- 您正在使用多云环境（AWS 和 Azure），因此在 AWS 中有一个连接器，在 Azure 中有另一个连接器。每个都管理在这些环境中运行的 Cloud Volumes ONTAP 系统。
- 服务提供商可能会使用一个 NetApp 帐户为其客户提供服务，而使用另一个帐户为其某个业务部门提供灾难恢复。每个帐户都有单独的 Connectors。

## 在相同的工作环境中使用多个连接器

您可以同时管理具有多个连接器的工作环境，以实现灾难恢复。如果一个连接器发生故障，您可以切换到另一个连接器以立即管理工作环境。

要设置此配置，请执行以下操作：

1. ["切换到另一个连接器"](#)
2. 发现现有工作环境。
  - ["将现有 Cloud Volumes ONTAP 系统添加到 Cloud Manager"](#)
  - ["发现 ONTAP 集群"](#)
3. 设置 ["容量管理模式"](#)

只能将主连接器设置为 \* 自动模式 \*。如果出于灾难恢复目的而切换到另一个连接器，则可以根据需要更改容量管理模式。

## 何时在连接器之间切换

创建首个 Connector 时，Cloud Manager 会自动对您创建的每个附加工作环境使用此 Connector。创建额外的 Connector 后，您需要在它们之间切换，以查看每个 Connector 特有的工作环境。

["了解如何在连接器之间切换"](#)。

## 本地用户界面

而您应从执行几乎所有任务 ["SaaS 用户界面"](#)，连接器上仍提供本地用户界面。如果您在无法访问 Internet 的环境中安装 Connector，并且需要从 Connector 本身执行一些任务，而不是从 SaaS 界面执行这些任务，则需要使用此接口：

- ["设置代理服务器"](#)
- 安装修补程序（您通常与 NetApp 人员一起安装修补程序）
- 下载 AutoSupport 消息（通常在遇到问题时由 NetApp 人员指导）

["了解如何访问本地 UI"](#)。

# 为连接器设置网络连接

设置您的网络，以便 Connector 可以管理公有云环境中的资源和流程。最重要的步骤是确保对各种端点的出站 Internet 访问。

此页面上的信息适用于 Connector 具有出站 Internet 访问权限的典型部署。



如果您的网络使用代理服务器与 Internet 进行所有通信，则可以从设置页面指定代理服务器。请参见 ["将 Connector 配置为使用代理服务器"](#)。

## 连接到目标网络

连接器要求与您要创建的工作环境类型以及计划启用的服务建立网络连接。

例如，如果您在公司网络中安装了连接器，则必须设置与启动 Cloud Volumes ONTAP 的 VPC 或 vNet 的 VPN 连接。

## 可能与 172 范围内的 IP 地址冲突

Cloud Manager 使用 IP 地址位于 172.17.0.0/16 和 172.18.0.0/16 范围的两个接口部署 Connector 。

如果您的网络配置了其中任一范围的子网，则可能会在 Cloud Manager 中遇到连接失败。例如，在 Cloud Manager 中发现内部 ONTAP 集群可能会失败。

请参见知识库文章 ["Cloud Manager Connector IP与现有网络冲突"](#) 有关如何更改连接器接口的IP地址的说明。

## 出站 Internet 访问

需要从 Connector 进行出站 Internet 访问。

用于管理公有云环境中资源的端点

连接器需要通过出站 Internet 访问来管理公有云环境中的资源和流程。

端点	目的
<a href="https://support.netapp.com">https://support.netapp.com</a>	获取许可信息并向 NetApp 支持部门发送 AutoSupport 消息。
<a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a>	在 Cloud Manager 中提供 SaaS 功能和服务。
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	升级 Connector 及其 Docker 组件。

用于在 Linux 主机上安装 Connector 的端点

您可以选择在自己的 Linux 主机上手动安装 Connector 软件。否则，Connector 的安装程序必须在安装过程中访问以下 URL：

- <https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm>

- <https://s3.amazonaws.com/aws-cli/awscri-bundle.zip>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) 或 <https://hub.docker.com>

主机可能会在安装期间尝试更新操作系统软件包。主机可以联系这些操作系统软件包的不同镜像站点。

## 端口和安全组

除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 "本地 UI"，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

### AWS 中连接器的规则

Connector 的安全组需要入站和出站规则。

#### 入站规则

协议	Port	目的
SSH	22.	提供对 Connector 主机的 SSH 访问
HTTP	80	提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问，以及从 Cloud Data sense 实例建立的连接
TCP	3128	如果您的 AWS 网络不使用 NAT 或代理，则可为云数据感知实例提供 Internet 访问
TCP	9060	支持启用和使用 Cloud Data sense（仅适用于 GovCloud 部署）

#### 出站规则

连接器的预定义安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

#### 基本外向规则

Connector 的预定义安全组包括以下出站规则。

协议	Port	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

#### 高级出站规则

如果您需要对出站流量设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。



源 IP 地址是 Connector 主机。



服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 AWS 和 ONTAP，云数据感知，勒索软件服务以及向 NetApp 发送 AutoSupport 消息
API 调用	TCP	3000	ONTAP HA 调解器	与 ONTAP HA 调解器通信
	TCP	8088	备份到 S3	对备份到 S3 进行 API 调用
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

## Azure 中连接器的规则

Connector 的安全组需要入站和出站规则。

### 入站规则

协议	Port	目的
SSH	22.	提供对 Connector 主机的 SSH 访问
HTTP	80	提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问，以及从 Cloud Data sense 实例建立的连接
TCP	9060	支持启用和使用 Cloud Data Asense（仅适用于政府云部署）

### 出站规则

连接器的预定义安全组将打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

### 基本外向规则

Connector 的预定义安全组包括以下出站规则。

协议	Port	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

### 高级出站规则

如果您需要对出站流量设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。



源 IP 地址是 Connector 主机。

服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 AWS 和 ONTAP ，云数据感知，勒索软件服务以及向 NetApp 发送 AutoSupport 消息
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

## GCP 中连接器的规则

Connector 的防火墙规则需要入站和出站规则。

### 入站规则

协议	Port	目的
SSH	22.	提供对 Connector 主机的 SSH 访问
HTTP	80	提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问

### 出站规则

连接器的预定义防火墙规则会打开所有出站流量。如果可以接受，请遵循基本出站规则。如果您需要更严格的规则、请使用高级出站规则。

### 基本外向规则

Connector 的预定义防火墙规则包括以下出站规则。

协议	Port	目的
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

### 高级出站规则

如果您需要对出站流量设置严格的规则，则可以使用以下信息仅打开 Connector 进行出站通信所需的端口。



源 IP 地址是 Connector 主机。

服务	协议	Port	目标	目的
API 调用和 AutoSupport	HTTPS	443.	出站 Internet 和 ONTAP 集群管理 LIF	API 调用 GCP 和 ONTAP，云数据感知，勒索软件服务以及向 NetApp 发送 AutoSupport 消息
DNS	UDP	53.	DNS	用于云管理器进行 DNS 解析

## 内部连接器的端口

在内部 Linux 主机上手动安装时，Connector 会使用以下 *inbound* 端口。

这些入站规则适用于以下两种部署模式：通过 Internet 访问或不通过 Internet 访问安装的内部连接器。

协议	Port	目的
HTTP	80	提供从客户端 Web 浏览器到本地用户界面的 HTTP 访问
HTTPS	443.	提供从客户端 Web 浏览器到本地用户界面的 HTTPS 访问

## 从 Cloud Manager 在 AWS 中创建连接器

客户管理员需要先部署 *Connector*，然后才能使用大多数 Cloud Manager 功能。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。["了解何时需要连接器"](#)。

此页面介绍如何直接从 Cloud Manager 在 AWS 中创建 Connector。["了解部署 Connector 的其他方法"](#)。

这些步骤必须由具有帐户管理员角色的用户完成。Workspace 管理员无法创建 Connector。

## 设置 AWS 身份验证

Cloud Manager 需要先向 AWS 进行身份验证，然后才能在 VPC 中部署 Connector 实例。您可以选择以下身份验证方法之一：

- 让 Cloud Manager 承担具有所需权限的 IAM 角色
- 为具有所需权限的 IAM 用户提供 AWS 访问密钥和机密密钥

无论选择哪一种方式、您都需要首先创建一个包含所需权限的 IAM 策略。

### 创建 IAM 策略

此策略仅包含从 Cloud Manager 在 AWS 中启动 Connector 实例所需的权限。请勿在其他情况下使用此策略。

在 Cloud Manager 创建 Connector 时、它会将一组新的权限应用于 Connector 实例、从而使 Connector 能够管理公有云环境中的资源。

### 步骤

1. 转到 AWS IAM 控制台。

2. 单击\*策略>创建策略\*。
3. 单击\*。JSON\*。
4. 复制并粘贴以下策略：

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam:DeleteRole",
      "iam:PutRolePolicy",
      "iam:CreateInstanceProfile",
      "iam:DeleteRolePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam:DeleteInstanceProfile",
      "iam:PassRole",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:CreateSecurityGroup",
      "ec2:DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2:DescribeInstances",
      "ec2:CreateTags",
      "ec2:DescribeImages",
      "cloudformation:CreateStack",
      "cloudformation:DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
```

```

        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. 单击\*下一步\*并根据需要添加标记。
6. 单击\*下一步\*并输入名称和问题描述。
7. 单击\*创建策略\*。

将此策略附加到Cloud Manager可以承担的IAM角色或IAM用户。

## 设置 IAM 角色

设置一个 IAM 角色，Cloud Manager 可以承担此角色，以便在 AWS 中部署 Connector。

### 步骤

1. 转到目标帐户中的 AWS IAM 控制台。
2. 在访问管理下，单击 \* 角色 > 创建角色 \*，然后按照步骤创建角色。

请务必执行以下操作：

- 在 \* 可信实体类型 \* 下，选择 \* AWS 帐户 \*。
- 选择 \* 其他 AWS 帐户 \*，然后输入 Cloud Manager SaaS 帐户的 ID：952013314444

。选择在上一节中创建的策略。

3. 创建角色后、复制角色ARN、以便您可以在创建Connector时将其粘贴到Cloud Manager中。

IAM 角色现在具有所需的权限。

为 **IAM** 用户设置权限

创建 Connector 时，您可以为拥有部署 Connector 实例所需权限的 IAM 用户提供 AWS 访问密钥和机密密钥。

步骤

1. 在AWS IAM控制台中、单击\*用户\*、然后选择用户名。
2. 单击\*添加权限>直接附加现有策略\*。
3. 选择创建的策略。
4. 单击\*下一步\*、然后单击\*添加权限\*。
5. 确保您有权访问 IAM 用户的访问密钥和机密密钥。

AWS 用户现在具有从 Cloud Manager 创建 Connector 所需的权限。在 Cloud Manager 提示时，您需要为此用户指定 AWS 访问密钥。

## 创建连接器

您可以通过 Cloud Manager 直接从其用户界面在 AWS 中创建 Connector 。

您需要什么？ **#8217** ；将需要什么

- AWS 身份验证方法： Cloud Manager 可承担的 IAM 角色的 ARN ， 或者 IAM 用户的 AWS 访问密钥和机密密钥。
- 您选择的 AWS 区域中的 VPC ， 子网和密钥对。
- 如果您不希望 Cloud Manager 自动为 Connector 创建 IAM 角色，则需要创建您自己的角色 "[使用此页面上的策略](#)"。

这些权限是 Connector 在公有 云环境中管理资源所需的权限。它与您为创建 Connector 实例提供的权限集不同。

步骤

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \* 。



2. 选择 \* Amazon Web Services\* 作为您的云提供商，然后单击 \* 继续 \*。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：查看您需要的内容。
- \* AWS Credentials\*：指定您的 AWS 区域，然后选择身份验证方法，即 Cloud Manager 可以承担的 IAM 角色或 AWS 访问密钥和机密密钥。



如果选择 \* 承担角色 \*，则可以从 Connector 部署向导创建第一组凭据。必须从 "凭据" 页面创建任何其他凭据集。然后，这些文件将从向导的下拉列表中显示。 ["了解如何添加其他凭据"](#)。

- \* 详细信息 \*：提供有关连接器的详细信息。
  - 输入实例的名称。
  - 向实例添加自定义标记（元数据）。
  - 选择是希望 Cloud Manager 创建具有所需权限的新角色，还是要选择使用设置的现有角色 ["所需权限"](#)。
  - 选择是否要对 Connector 的 EBS 磁盘进行加密。您可以选择使用默认加密密钥或自定义密钥。
- \* 网络 \*：指定实例的 VPC，子网和密钥对，选择是否启用公有 IP 地址，并可选择指定代理配置。
- \* 安全组 \*：选择是创建新的安全组，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有安全组。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

4. 单击 \* 添加 \*。

此实例应在大约 7 分钟后准备就绪。您应停留在页面上，直到此过程完成。

您需要将连接器与工作空间关联，以便 Workspace 管理员可以使用这些连接器创建 Cloud Volumes ONTAP 系统。如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。"[了解更多信息](#)"。

如果您在创建 Connector 的同一 AWS 帐户中有 Amazon S3 存储分段，则会在 Canvas 上自动显示 Amazon S3 工作环境。"[详细了解如何使用此工作环境](#)"。

## 从 Cloud Manager 在 Azure 中创建 Connector

客户管理员需要先部署 *Connector*，然后才能使用大多数 Cloud Manager 功能。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。"[了解何时需要连接器](#)"。

此页面介绍如何直接从 Cloud Manager 在 Azure 中创建 Connector。"[了解部署 Connector 的其他方法](#)"。

这些步骤必须由具有帐户管理员角色的用户完成。Workspace 管理员无法创建 Connector。

### 概述

要部署 Connector，您需要为 Cloud Manager 提供一个登录名，该登录名必须具有在 Azure 中创建 Connector VM 所需的权限。

您有两种选择：

1. 出现提示时，使用 Microsoft 帐户登录。此帐户必须具有特定的 Azure 权限。这是默认选项。

[请按照以下步骤开始操作。](#)

2. 提供有关 Azure AD 服务主体的详细信息。此服务主体还需要特定权限。

[请按照以下步骤开始操作。](#)

### 有关 Azure 地区的说明

此连接器应部署在与其管理的 Cloud Volumes ONTAP 系统所在的同一 Azure 区域或中 "[Azure 区域对](#)" 对于 Cloud Volumes ONTAP 系统。此要求可确保在 Cloud Volumes ONTAP 与其关联存储帐户之间使用 Azure 专用链路连接。"[了解 Cloud Volumes ONTAP 如何使用 Azure 专用链路](#)"。

### 使用 Azure 帐户创建 Connector

在 Azure 中创建 Connector 的默认方法是，在出现提示时使用 Azure 帐户登录。此登录表由 Microsoft 拥有和托管。您的凭据不会提供给 NetApp。

为 **Azure** 帐户设置权限

在从 Cloud Manager 部署 Connector 之前，您需要确保 Azure 帐户具有正确的权限。

#### 步骤

1. 在 Azure 中复制新自定义角色所需的权限、并将其保存在 JSON 文件中。





此策略仅包含从Cloud Manager在Azure中启动Connector VM所需的权限。请勿在其他情况下使用此策略。在Cloud Manager创建Connector时、它会将一组新的权限应用于Connector VM、从而使Connector能够管理公有云环境中的资源。

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

    "Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
```

```

d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}

```

## 2. 通过将Azure订阅ID添加到可分配范围来修改JSON。

◦ 示例 \*

```

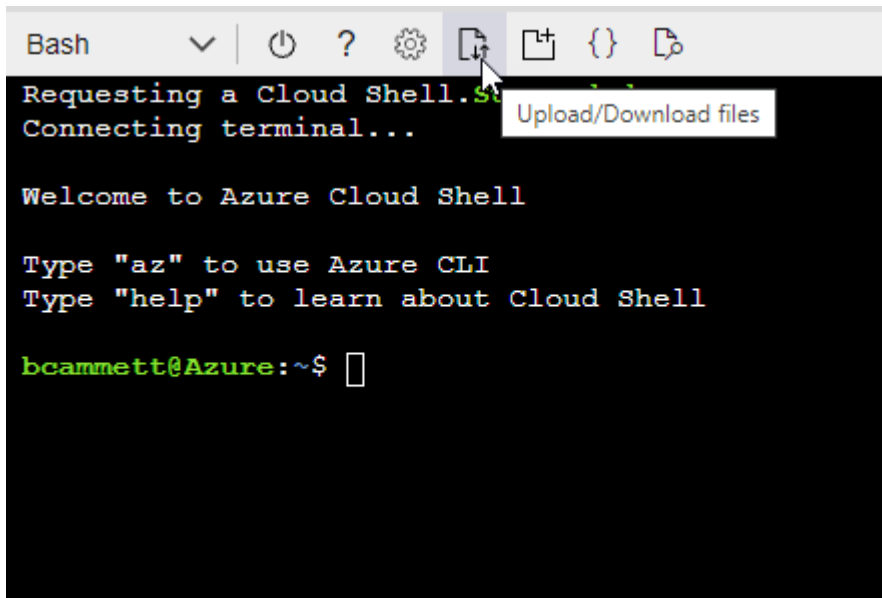
"AssignableScopes": [
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

## 3. 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。

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



- c. 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，您应具有一个名为 *Azure SetupAsService* 的自定义角色。

4. 将角色分配给要从 Cloud Manager 部署 Connector 的用户：

- a. 打开 \* 订阅 \* 服务并选择用户的订阅。
- b. 单击 \* 访问控制（IAM） \*。
- c. 单击 \* 添加 \* > \* 添加角色分配 \*，然后添加权限：
  - 选择 \* Azure SetupAsService \* 角色，然后单击 \* 下一步 \*。



Azure SetupAsService 是 Azure 的 Connector 部署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。

- 保持选中 \* 用户，组或服务主体 \*。
- 单击 \* 选择成员 \*，选择您的用户帐户，然后单击 \* 选择 \*。
- 单击 \* 下一步 \*。
- 单击 \* 审核 + 分配 \*。

Azure 用户现在具有从 Cloud Manager 部署 Connector 所需的权限。

## 使用 Azure 帐户登录以创建 Connector

您可以通过 Cloud Manager 直接从其用户界面在 Azure 中创建 Connector。

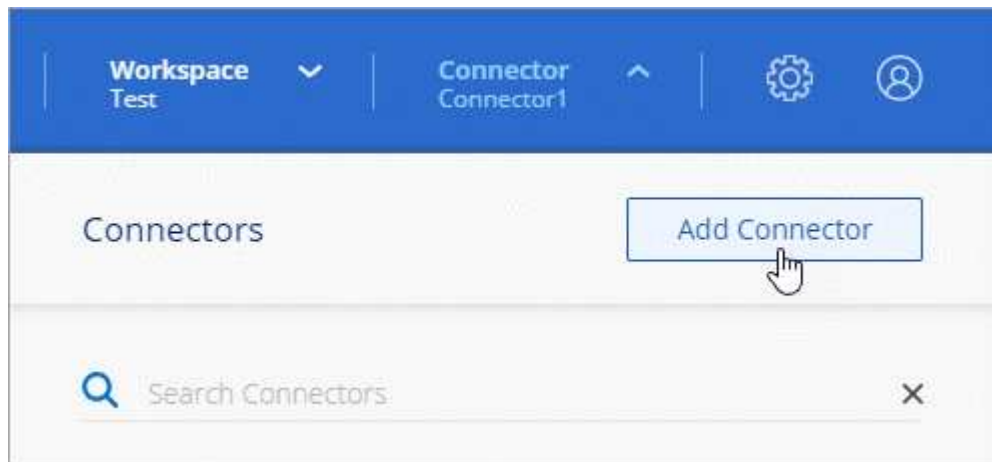
您需要什么？ #8217 ；将需要什么

- Azure 订阅。
- 您选择的 Azure 区域中的 vNet 和子网。
- 如果您不希望 Cloud Manager 自动为 Connector 创建 Azure 角色，则需要创建您自己的角色 ["使用此页面上的策略"](#)。

这些权限适用于 Connector 实例本身。它是一组与您先前设置的权限不同的权限，只需部署 Connector 即可。

### 步骤

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \*。



2. 选择 \* Microsoft Azure\* 作为云提供商。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：查看您需要的内容，然后单击 \* 下一步 \*。
- 如果出现提示，请登录到您的 Microsoft 帐户，该帐户应具有创建虚拟机所需的权限。

此表由 Microsoft 拥有和托管。您的凭据不会提供给 NetApp。



如果您已登录到 Azure 帐户，则 Cloud Manager 将自动使用该帐户。如果您有多个帐户，则可能需要先注销，以确保您使用的是正确的帐户。

- \* 虚拟机身份验证 \*：选择 Azure 订阅，位置，新资源组或现有资源组，然后选择身份验证方法。
- \* 详细信息 \*：输入实例的名称，指定标记，然后选择是希望 Cloud Manager 创建具有所需权限的新角

色，还是要选择使用设置的现有角色 ["所需权限"](#)。

请注意，您可以选择与此角色关联的订阅。您选择的每个订阅都为 Connector 提供了在这些订阅中部署 Cloud Volumes ONTAP 的权限。

- \* 网络 \*：选择 vNet 和子网，是否启用公有 IP 地址，并可选择指定代理配置。
- \* 安全组 \*：选择是创建新的安全组，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有安全组。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

#### 4. 单击 \* 添加 \*。

虚拟机应在大约 7 分钟内准备就绪。您应停留在页面上，直到此过程完成。

您需要将连接器与工作空间关联，以便 Workspace 管理员可以使用这些连接器创建 Cloud Volumes ONTAP 系统。如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。 ["了解更多信息。"](#)

如果您在创建 Connector 的同一 Azure 帐户中使用 Azure Blob 存储，则会在 Canvas 上自动显示 Azure Blob 工作环境。 ["详细了解如何使用此工作环境"](#)。

## 使用服务主体创建连接器

您还可以选择为 Cloud Manager 提供具有所需权限的 Azure 服务主体的凭据，而不是使用 Azure 帐户登录。

### 使用服务主体授予 **Azure** 权限

通过在 Azure Active Directory 中创建和设置服务主体并获取 Cloud Manager 所需的 Azure 凭据，授予在 Azure 中部署 Connector 所需的权限。

#### 步骤

1. [\[Create an Azure Active Directory application\]](#)。
2. [\[Assign the application to a role\]](#)。
3. [\[Add Windows Azure Service Management API permissions\]](#)。
4. [\[Get the application ID and directory ID\]](#)。
5. [\[Create a client secret\]](#)。

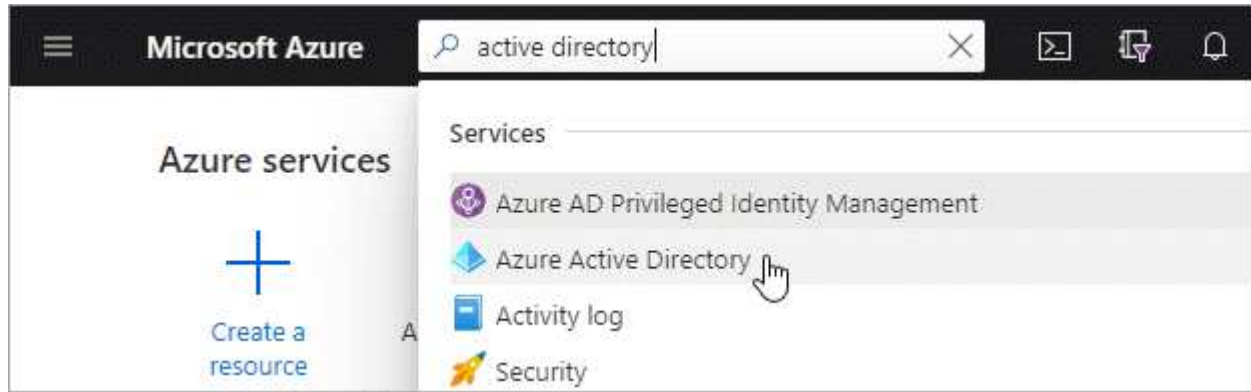
#### 创建 **Azure Active Directory** 应用程序

创建一个 Azure Active Directory（AD）应用程序和服务主体，Cloud Manager 可使用此主体部署 Connector。

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计划部署 Connector 的 Azure 订阅，并为其分配自定义 "Azure SetupAsService" 角色。

步骤

1. 在 Azure 中复制新自定义角色所需的权限、并将其保存在 JSON 文件中。



此策略仅包含从 Cloud Manager 在 Azure 中启动 Connector VM 所需的权限。请勿在其他情况下使用此策略。在 Cloud Manager 创建 Connector 时、它会将一组新的权限应用于 Connector VM、从而使 Connector 能够管理公有云环境中的资源。

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
```

```
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
"Microsoft.Resources/subscriptions/resourceGroups/delete",
"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/roleDefinitions/write",
```

```

        "Microsoft.Authorization/roleAssignments/write",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}

```

## 2. 通过将 Azure 订阅 ID 添加到可分配范围来修改 JSON 文件。

◦ 示例 \*

```

"AssignableScopes": [
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]

```

## 3. 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。

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





c. 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，您应具有一个名为 *Azure SetupAsService* 的自定义角色。

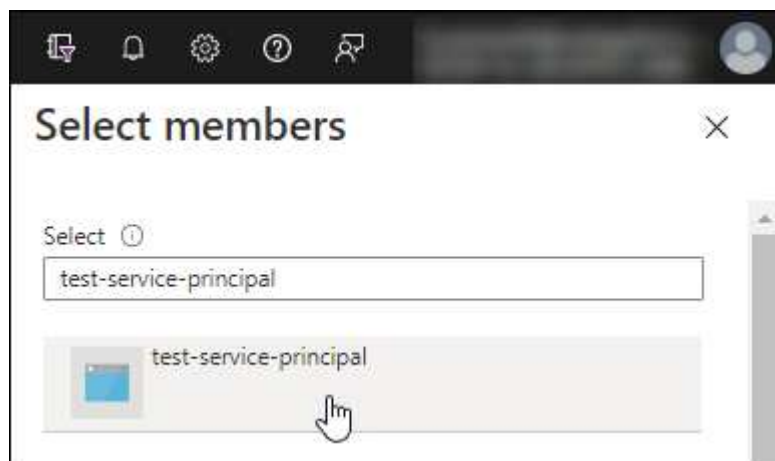
4. 将应用程序分配给角色：

- 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 \* Azure SetupAsService\* 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 \*。
- a. 单击 \* 审核 + 分配 \*。

现在，服务主体具有部署 Connector 所需的 Azure 权限。

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\* 。













## Request API permissions

### Select an API

Microsoft APIs   APIs my organization uses   My APIs

#### Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

 <b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	 <b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	 <b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 <b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios	 <b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server	 <b>Azure Import/Export</b> Programmatic control of import/export jobs
 <b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
 <b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 <b>Customer Insights</b> Create profile and interaction models for your products	 <b>Data Export Service for Microsoft Dynamics 365</b> Export data from Microsoft Dynamics CRM organization to an external destination

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 \* 。

## Request API permissions

< All APIs



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

获取应用程序 ID 和目录 ID

从 Cloud Manager 创建 Connector 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。

### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA

Copy to clipboard

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。创建 Connector 时，您需要在 Cloud Manager 中输入此信息。

### 使用服务主体登录以创建 Connector

您可以通过 Cloud Manager 直接从其用户界面在 Azure 中创建 Connector。

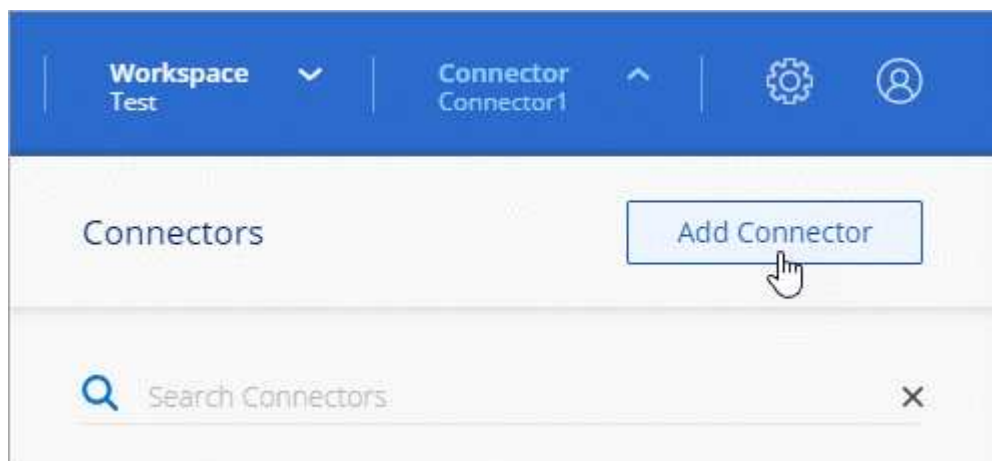
您需要什么？ #8217 ； 将需要什么

- Azure 订阅。
- 您选择的 Azure 区域中的 vNet 和子网。
- 如果您不希望 Cloud Manager 自动为 Connector 创建 Azure 角色，则需要创建您自己的角色 ["使用此页面上的策略"](#)。

这些权限适用于 Connector 实例本身。它是一组与您先前设置的权限不同的权限，只需部署 Connector 即可。

### 步骤

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \*。



## 2. 选择 \* Microsoft Azure\* 作为云提供商。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

## 3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：单击 \* Azure AD 服务主体 \* 并输入有关 Azure Active Directory 服务主体的信息，该服务主体授予所需权限：
  - 应用程序（客户端）ID：请参见 [\[Get the application ID and directory ID\]](#)。
  - 目录（租户）ID：请参见 [\[Get the application ID and directory ID\]](#)。
  - 客户端密钥：请参见 [\[Create a client secret\]](#)。
- \* 虚拟机身份验证 \*：选择 Azure 订阅，位置，新资源组或现有资源组，然后选择身份验证方法。
- \* 详细信息 \*：输入实例的名称，指定标记，然后选择是希望 Cloud Manager 创建具有所需权限的新角色，还是要选择使用设置的现有角色 ["所需权限"](#)。

请注意，您可以选择与此角色关联的订阅。您选择的每个订阅都为 Connector 提供了在这些订阅中部署 Cloud Volumes ONTAP 的权限。

- \* 网络 \*：选择 vNet 和子网，是否启用公有 IP 地址，并可选择指定代理配置。
- \* 安全组 \*：选择是创建新的安全组，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有安全组。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

## 4. 单击 \* 添加 \*。

虚拟机应在大约 7 分钟内准备就绪。您应停留在页面上，直到此过程完成。

您需要将连接器与工作空间关联，以便 Workspace 管理员可以使用这些连接器创建 Cloud Volumes ONTAP 系统。如果您只有帐户管理员，则不需要将 Connector 与工作空间相关联。默认情况下，帐户管理员可以访问 Cloud Manager 中的所有工作空间。 ["了解更多信息"](#)。

如果您在创建 Connector 的同一 Azure 帐户中使用 Azure Blob 存储，则会在 Canvas 上自动显示 Azure Blob 工作环境。 ["详细了解如何使用此工作环境"](#)。

# 从 Cloud Manager 在 Google Cloud 中创建 Connector

客户管理员需要先部署 *Connector*，然后才能使用大多数 Cloud Manager 功能。 ["了解何时需要连接器"](#)。借助此连接器，Cloud Manager 可以管理公有云环境中的资源和流程。

此页面介绍如何直接从 Cloud Manager 在 Google Cloud 中创建 Connector。 ["了解部署 Connector 的其他方法"](#)。

这些步骤必须由具有帐户管理员角色的用户完成。Workspace 管理员无法创建 Connector。



在创建首个 Cloud Volumes ONTAP 工作环境时，如果您还没有连接器，Cloud Manager 将提示您创建一个连接器。

## 设置部署Connector的权限

在部署Connector之前、您需要确保Google Cloud帐户具有正确的权限。

### 步骤

1. "创建自定义角色" 其中包括以下权限：

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
Cloud Manager
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
```

```
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list
```

2. 将自定义角色附加到要从Cloud Manager部署Connector的用户。

Google Cloud用户现在具有创建Connector所需的权限。

## 为Connector设置服务帐户

需要使用服务帐户为Connector提供在Google Cloud中管理资源所需的权限。创建此服务帐户时，您需要将其与Connector VM 关联。

此服务帐户的权限与您在上一节中设置的权限不同。

### 步骤

1. "创建自定义角色" 其中包括以下权限：

```
title: NetApp Cloud Manager
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
```



- `compute.regionBackendServices.create`
- `compute.regionBackendServices.get`
- `compute.regionBackendServices.list`
- `compute.networks.updatePolicy`
- `compute.backendServices.create`
- `compute.addresses.list`
- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `compute.disks.get`
- `compute.disks.list`
- `compute.disks.setLabels`
- `compute.disks.use`
- `compute.firewalls.create`
- `compute.firewalls.delete`
- `compute.firewalls.get`
- `compute.firewalls.list`
- `compute.globalOperations.get`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`

- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `logging.logEntries.list`
- `logging.privateLogEntries.list`
- `resourcemanager.projects.get`
- `storage.buckets.create`
- `storage.buckets.delete`
- `storage.buckets.get`
- `storage.buckets.list`
- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`
- `storage.buckets.update`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.list`
- `storage.objects.get`
- `storage.objects.list`
- `monitoring.timeSeries.list`
- `storage.buckets.getIamPolicy`

2. "创建Google Cloud服务帐户并应用您刚刚创建的自定义角色"。
3. 如果要在其他项目中部署 Cloud Volumes ONTAP ， "通过向该项目添加具有 Cloud Manager 角色的服务帐户来授予访问权限"。您需要对每个项目重复此步骤。

已设置Connector VM的服务帐户。

## 共享 VPC 权限

如果您使用共享 VPC 将资源部署到服务项目中，则需要以下权限。此表仅供参考，您的环境应在 IAM 配置完成后反映权限表。

身份	创建者	托管在中	服务项目权限	托管项目权限	目的
用于部署Connector的Google帐户	自定义	服务项目	• "以上部分中的权限"	• compute.networkUser	在服务项目中部署Connector
连接器服务帐户	自定义	服务项目	• "以上部分中的权限"	• compute.networkUser • deploymentmanager.editor	在服务项目中部署和维护 Cloud Volumes ONTAP 和服务
Cloud Volumes ONTAP 服务帐户	自定义	服务项目	• storage.admin • 成员： Cloud Manager 服务帐户为 serviceAccount.user	不适用	(可选) 适用于数据分层和 Cloud Backup
Google API 服务代理	Google Cloud	服务项目	• (默认) 编辑器	• compute.networkUser	代表部署与Google Cloud API进行交互。允许 Cloud Manager 使用共享网络。
Google Compute Engine 默认服务帐户	Google Cloud	服务项目	• (默认) 编辑器	• compute.networkUser	代表部署部署部署部署Google Cloud实例和计算基础架构。允许 Cloud Manager 使用共享网络。

注释：

1. 只有在未向部署传递防火墙规则并选择让 Cloud Manager 为您创建这些规则的情况下，主机项目才需要使用 deploymentManager.editor.如果未指定任何规则， Cloud Manager 将在包含 VPC0 防火墙规则的主机项目中创建部署。
2. 只有当您不向部署传递防火墙规则并选择让 Cloud Manager 为您创建这些规则时，才需要 firewall.create 和 firewall.delete 。这些权限位于 Cloud Manager 服务帐户 .yaml 文件中。如果要使用共享 VPC 部署 HA 对，则会使用这些权限为 VC1 ， 2 和 3 创建防火墙规则。对于所有其他部署，这些权限还将用于为 VPC0 创建

规则。

3. 对于数据分层，分层服务帐户必须在服务帐户上具有 `serviceAccount.user` 角色，而不仅仅是在项目级别。目前，如果您在项目级别分配 `serviceAccount.user`，则在使用 `getIAMPolicy` 查询服务帐户时不会显示权限。

## 启用 Google Cloud API

部署连接器和 Cloud Volumes ONTAP 需要多个 API。

### 步骤

1. "在项目中启用以下 Google Cloud API"。
  - Cloud Deployment Manager V2 API
  - 云日志记录 API
  - Cloud Resource Manager API
  - 计算引擎 API
  - 身份和访问管理（IAM）API

## 在Google Cloud中创建连接器

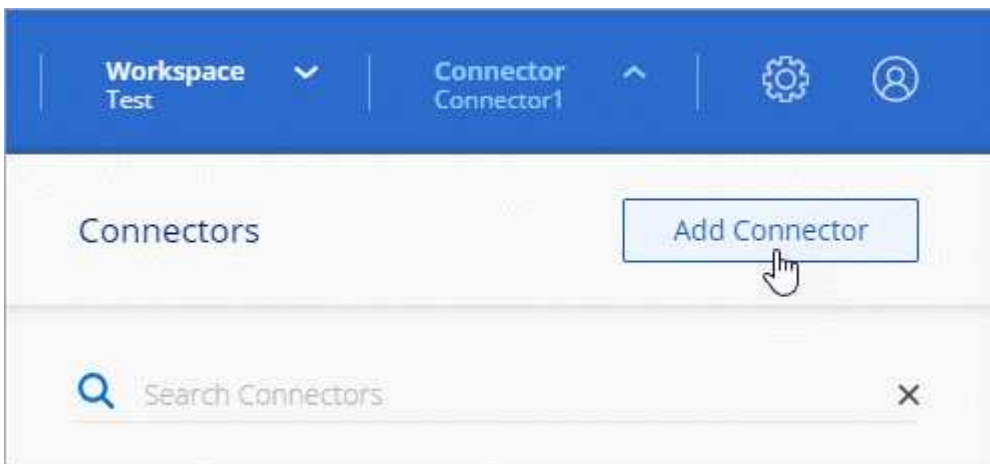
直接从 Cloud Manager 用户界面或使用 `gcloud` 在 Google Cloud 中创建 Connector。

您需要什么？ **#8217**；将需要什么

- 您的Google Cloud帐户所需的权限、如本页面第一部分所述。
- Google Cloud 项目。
- 一种具有创建和管理 Cloud Volumes ONTAP 所需权限的服务帐户，如本页面第一部分所述。
- 您选择的 Google Cloud 区域中的 VPC 和子网。

## 云管理器

1. 如果要创建首个工作环境，请单击 \* 添加工作环境 \* 并按照提示进行操作。否则，请单击 \* 连接器 \* 下拉列表并选择 \* 添加连接器 \*。



2. 选择 \* Google Cloud Platform\* 作为云提供商。

请记住，Connector 必须与您要创建的工作环境类型以及您计划启用的服务建立网络连接。

["详细了解 Connector 的网络要求"](#)。

3. 按照向导中的步骤创建 Connector：

- \* 准备就绪 \*：查看您需要的内容。
- 如果出现提示，请登录到您的 Google 帐户，该帐户应具有创建虚拟机实例所需的权限。

此表由 Google 拥有和托管。您的凭据不会提供给 NetApp。

- \* 基本设置 \*：输入虚拟机实例的名称，指定标记，选择项目，然后选择具有所需权限的服务帐户（有关详细信息，请参见上述部分）。
- \* 位置 \*：指定实例的区域，分区，VPC 和子网。
- \* 网络 \*：选择是否启用公有 IP 地址，并可选择指定代理配置。
- \* 防火墙策略 \*：选择是创建新的防火墙策略，还是选择允许入站 HTTP，HTTPS 和 SSH 访问的现有防火墙策略。



除非您启动 Connector，否则不会向其传入流量。HTTP 和 HTTPS 可用于访问 ["本地 UI"](#)，在极少数情况下使用。只有在需要连接到主机进行故障排除时，才需要使用 SSH。

- \* 审核 \*：查看您选择的内容，确认您的设置正确无误。

4. 单击 \* 添加 \*。

此实例应在大约 7 分钟后准备就绪。您应停留在页面上，直到此过程完成。

## 云

### 1. 使用您首选的方法登录到 gcloud SDK。

在我们的示例中、我们将使用安装了gcloud SDK的本地Shell、但您可以在Google云控制台中使用原生Google Cloud Shell。

有关 Google Cloud SDK 的详细信息，请访问 ["Google Cloud SDK 文档页面"](#)。

### 2. 验证您是否以具有上一节中定义的所需权限的用户身份登录：

```
gcloud auth list
```

输出应显示以下内容，其中 \* 用户帐户是要以身份登录的所需用户帐户：

```
Credentialed Accounts
ACTIVE  ACCOUNT
      some_user_account@domain.com
*      desired_user_account@domain.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

### 3. 运行 gcloud compute instances create 命令：

```
gcloud compute instances create <instance-name>
  --machine-type=n1-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<<service-account>>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

实例名称

VM 实例所需的实例名称。

## 项目

(可选) 要部署 VM 的项目。

## 服务帐户

步骤 2 输出中指定的服务帐户。

## 分区

要部署 VM 的区域

## 无地址

(可选) 不使用外部 IP 地址 (您需要云 NAT 或代理将流量路由到公有 Internet)

## 网络标记

(可选) 添加网络标记以使用标记将防火墙规则链接到 Connector 实例

## 网络路径

(可选) 添加要将 Connector 部署到的网络的名称 (对于共享 VPC, 您需要完整路径)

## 子网路径

(可选) 添加要将 Connector 部署到的子网的名称 (对于共享 VPC, 您需要完整路径)

## kms-key-path

(可选) 添加 KMS 密钥以加密连接器的磁盘 (还需要应用 IAM 权限)

有关这些标志的详细信息, 请访问 ["Google Cloud 计算 SDK 文档"](#)。

+

运行命令可使用 NetApp 黄金映像部署 Connector。Connector 实例和软件应在大约五分钟内运行。

1. 从已连接到 Connector 实例的主机打开 Web 浏览器, 然后输入以下 URL:

`http://ipaddress:80[]`

2. 登录后, 设置 Connector:

- a. 指定要与 Connector 关联的 NetApp 帐户。

["了解 NetApp 客户"](#)。

- b. 输入系统名称。



现在，您可以使用 NetApp 帐户安装并设置 Connector。Cloud Manager 将在您创建新的工作环境时自动使用此 Connector。但是，如果您有多个 Connector，则需要 ["在它们之间切换"](#)。

如果您在创建Connector的同一Google Cloud帐户中有Google Cloud Storage存储分段、则会在Canvas上自动显示Google Cloud Storage工作环境。 ["详细了解如何使用此工作环境"](#)。



## 版权信息

版权所有©2022 NetApp、Inc.。保留所有权利。Printed in the U.S.版权所涵盖的本文档的任何部分不得以任何形式或任何手段复制、包括影印、录制、磁带或存储在电子检索系统中—未经版权所有者事先书面许可。

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

本软件由NetApp按"原样"提供、不含任何明示或默示担保、包括但不限于适销性和特定用途适用性的默示担保、特此声明不承担任何任何责任。IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

RESTRICTED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.277-7103 (October 1988) and FAR 52-227-19 (June 1987).

## 商标信息

NetApp、NetApp标识和中列出的标记 <http://www.netapp.com/TM> 是NetApp、Inc.的商标。其他公司和产品名称可能是其各自所有者的商标。