



开始使用

NetApp Copy and Sync

NetApp
December 16, 2025

This PDF was generated from <https://docs.netapp.com/zh-cn/data-services-copy-sync/concept-cloud-sync.html> on December 16, 2025. Always check docs.netapp.com for the latest.

目录

开始使用	1
了解NetApp Copy and Sync	1
NetApp Console	1
NetApp Copy and Sync的工作原理	1
支持的存储类型	2
成本	2
NetApp Copy and Sync快速入门	3
NetApp Copy and Sync中支持的同步关系	4
在NetApp Copy and Sync中准备源和目标	11
网络连接	11
目标目录	11
读取目录的权限	11
Amazon S3 存储桶要求	12
Azure Blob 存储要求	13
Azure 数据湖存储 Gen2	14
Azure NetApp Files要求	14
盒子要求	15
Google Cloud Storage 存储桶要求	15
Google 云端硬盘	16
NFS 服务器要求	16
ONTAP 要求	17
ONTAP S3 存储要求	17
SMB 服务器要求	17
NetApp Copy and Sync的网络概述	18
数据代理位置	18
网络要求	19
网络端点	19
登录NetApp Copy and Sync	21
安装数据代理	21
在 AWS 中为NetApp Copy and Sync创建新的数据代理	21
在 Azure 中为NetApp Copy and Sync创建新的数据代理	25
在 Google Cloud 中为NetApp Copy and Sync创建新的数据代理	30
在 Linux 主机上安装用于NetApp Copy and Sync的数据代理	35

开始使用

了解NetApp Copy and Sync

NetApp Copy and Sync提供了一种简单、安全且自动化的方式，可将您的数据迁移到云端或本地的任何目标。无论它是基于文件的 NAS 数据集（NFS 或 SMB）、Amazon Simple Storage Service (S3) 对象格式、NetApp StorageGRID设备还是任何其他云提供商对象存储，Copy and Sync 都可以为您转换和移动它。

NetApp Console

可以通过NetApp Console访问NetApp Copy and Sync。

NetApp Console提供企业级跨本地和云环境的NetApp存储和数据服务的集中管理。需要控制台才能访问和使用NetApp数据服务。作为管理界面，它使您能够从一个界面管理许多存储资源。控制台管理员可以控制企业内所有系统的存储和服务的访问。

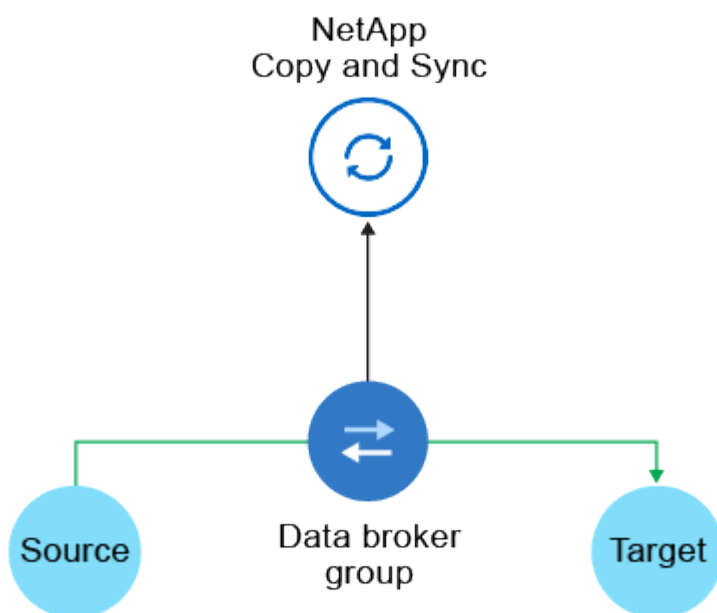
您不需要许可证或订阅即可开始使用NetApp Console，并且只有当您需要在云中部署控制台代理以确保与存储系统或NetApp数据服务的连接时才需要付费。但是，一些可从控制台访问的NetApp数据服务是需要许可或基于订阅的。

详细了解 "[NetApp Console](#)"。

NetApp Copy and Sync的工作原理

NetApp Copy and Sync是一个软件即服务 (SaaS) 平台，由数据代理组、可通过NetApp Console访问的基于云的界面以及源和目标组成。

下图显示了 Copy 和 Sync 组件之间的关系：



NetApp数据代理软件将数据从源同步到目标（这称为_同步关系_）。您可以在 AWS、Azure、Google Cloud

Platform 或您的本地运行数据代理。由一个或多个数据代理组成的数据代理组需要通过端口 443 建立出站互联网连接，以便它可以与复制和同步进行通信并联系其他一些服务和存储库。["查看端点列表"](#)。

初始复制后，“复制和同步”会根据您设置的计划同步任何更改的数据。

支持的存储类型

复制和同步支持以下存储类型：

- 任何 NFS 服务器
- 任何 SMB 服务器
- 亚马逊 EFS
- 适用于ONTAP 的Amazon FSx
- Amazon S3
- Azure Blob
- Azure 数据湖存储 Gen2
- Azure NetApp Files
- Box（可预览）
- Cloud Volumes ONTAP
- Google Cloud Storage
- Google 云端硬盘
- IBM Cloud Object Storage
- 本地ONTAP集群
- ONTAP S3 存储
- SFTP（仅使用 API）
- StorageGRID

["查看支持的同步关系"](#)。

成本

使用复制和同步涉及两种类型的成本：资源费用和服务费用。

资源费用

资源费用与在云中运行一个或多个数据代理的计算和存储成本有关。

服务费

14 天免费试用期结束后，有两种方式可以支付同步关系的费用。第一个选项是从 AWS 或 Azure 订阅，这样您就可以按小时或按年付费。第二种选择是直接从NetApp购买许可证。

["了解许可的工作原理"](#)。

NetApp Copy and Sync快速入门

开始使用NetApp Copy and Sync包括几个步骤。

1

登录并设置NetApp Console

您应该已经开始使用NetApp Console，其中包括登录、设置帐户以及可能部署控制台代理和创建系统。

如果您想要为以下任何一项创建同步关系，那么您首先需要创建或发现一个系统：

- 适用于ONTAP 的Amazon FSx
- Azure NetApp Files
- Cloud Volumes ONTAP
- 本地ONTAP集群

Cloud Volumes ONTAP、本地ONTAP集群和Amazon FSx for ONTAP都需要控制台代理。

- ["了解如何开始使用NetApp Console"](#)
- ["了解有关控制台代理的更多信息"](#)

2

准备源和目标

验证您的源和目标是否受支持并已设置。最重要的要求是验证数据代理组与源位置和目标位置之间的连接。

- ["查看支持的关系"](#)
- ["准备源和目标"](#)

3

为NetApp数据代理准备位置

NetApp数据代理软件将数据从源同步到目标（这称为_同步关系_）。您可以在 AWS、Azure、Google Cloud Platform 或您的本地运行数据代理。由一个或多个数据代理组成的数据代理组需要通过端口 443 建立出站互联网连接，以便与NetApp Copy and Sync并联系其他一些服务和存储库。["查看端点列表"](#)。

当您创建同步关系时， NetApp Copy and Sync会指导您完成安装过程，此时您可以在云中部署数据代理或为您自己的 Linux 主机下载安装脚本。

- ["检查 AWS 安装"](#)
- ["查看 Azure 安装Review Azure installation"](#)
- ["检查 Google Cloud 安装"](#)
- ["检查 Linux 主机安装"](#)

4

创建您的第一个同步关系

登录 ["NetApp Console"](#)，选择*同步*，然后拖放源和目标的选择。按照提示完成设置。["了解更多"](#)。

从 AWS 或 Azure 订阅，按使用量付费或按年付费。或者直接从NetApp购买许可证。只需转到NetApp Copy and Sync中的“许可证设置”页面进行设置。[了解更多](#)。

NetApp Copy and Sync中支持的同步关系

NetApp Copy and Sync使您能够将数据从源同步到目标。这被称为同步关系。在开始之前您应该了解所支持的关系。

源位置	支持的目标位置
亚马逊 EFS	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • SMB 服务器 • StorageGRID
适用于ONTAP 的Amazon FSx	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • SMB 服务器 • StorageGRID

源位置	支持的目标位置
Amazon S3	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • 盒子¹ • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存储 • SMB 服务器 • StorageGRID
Azure Blob	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • SMB 服务器 • StorageGRID

源位置	支持的目标位置
Azure 数据湖存储 Gen2	• Azure NetApp Files • Cloud Volumes ONTAP • 适用于ONTAP的 FSx • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP • ONTAP S3 存储 • SMB 服务器 • StorageGRID
Azure NetApp Files	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • SMB 服务器 • StorageGRID
盒子 ¹	• 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure NetApp Files • Cloud Volumes ONTAP • IBM Cloud Object Storage • NFS 服务器 • SMB 服务器 • StorageGRID

源位置	支持的目标位置
Cloud Volumes ONTAP	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • SMB 服务器 • StorageGRID
Google Cloud Storage	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存储 • SMB 服务器 • StorageGRID
Google 云端硬盘	• NFS 服务器 • SMB 服务器

源位置	支持的目标位置
IBM Cloud Object Storage	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • 盒子¹ • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • SMB 服务器 • StorageGRID
NFS 服务器	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Google 云端硬盘 • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存储 • SMB 服务器 • StorageGRID

源位置	支持的目标位置
本地ONTAP集群（NFS 或 SMB）	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • SMB 服务器 • StorageGRID
ONTAP S3 存储	• Amazon S3 • Azure 数据湖存储 Gen2 • Google Cloud Storage • NFS 服务器 • SMB 服务器 • StorageGRID • ONTAP S3 存储
SFTP ²	S3

源位置	支持的目标位置
SMB 服务器	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • Cloud Volumes ONTAP • Google Cloud Storage • Google 云端硬盘 • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存储 • SMB 服务器 • StorageGRID
StorageGRID	• 亚马逊 EFS • 适用于ONTAP 的Amazon FSx • Amazon S3 • Azure Blob • Azure 数据湖存储 Gen2 • Azure NetApp Files • 盒子¹ • Cloud Volumes ONTAP • Google Cloud Storage • IBM Cloud Object Storage • NFS 服务器 • 本地ONTAP集群（NFS 或 SMB） • ONTAP S3 存储 • SMB 服务器 • StorageGRID

注：

1. Box 支持目前可作为预览使用。

2. 仅通过使用复制和同步 API 支持与此源/目标的同步关系。
3. 当 Blob 容器是目标时，您可以选择特定的 Azure Blob 存储层：
 - 热存储
 - 冷藏
4. 当 Amazon S3 是目标时，您可以选择特定的 S3 存储类：
 - 标准（这是默认类）
 - 智能分层
 - 标准-不频繁访问
 - 单区-不频繁访问
 - 冰川深度档案
 - 冰川灵活检索
 - 冰川即时检索
5. 当 Google Cloud Storage 存储桶是目标时，您可以选择特定的存储类别：
 - 标准
 - 近线
 - 冷线
 - 归档

在NetApp Copy and Sync中准备源和目标

验证您的源和目标是否满足NetApp Copy and Sync中的以下要求。

网络连接

- 源和目标必须与数据代理组有网络连接。

例如，如果 NFS 服务器位于您的数据中心，而数据代理位于 AWS 中，那么您需要从您的网络到 VPC 的网络连接（VPN 或 Direct Connect）。

- NetApp建议配置源、目标和数据代理以使用网络时间协议 (NTP) 服务。三个组件之间的时间差不应超过5分钟。

目标目录

当您创建同步关系时，“复制和同步”使您能够选择现有的目标目录，然后可以选择在该目录内创建一个新文件夹。因此请确保您的首选目标目录已经存在。

读取目录的权限

为了显示源或目标中的每个目录或文件夹，“复制和同步”需要对该目录或文件夹的读取权限。

NFS

必须在源/目标上使用文件和目录的 uid/gid 定义权限。

对象存储

- 对于 AWS 和 Google Cloud，数据代理必须具有列表对象权限（如果您遵循数据代理安装步骤，则默认提供这些权限）。
- 对于 Azure、StorageGRID 和 IBM，设置同步关系时输入的凭据必须具有列出对象权限。

SMB

设置同步关系时输入的 SMB 凭据必须具有列出文件夹权限。



数据代理默认忽略以下目录：.snapshot、~snapshot、.copy-offload



使用复制和同步将 SMB 数据复制到 Cloud Volumes ONTAP 时，源系统中的文件和文件夹所有权不会被保留。出现这种行为的原因是 Copy and Sync 使用了 Linux SMB 客户端，该客户端会将所有权分配给用于验证传输的用户或服务帐户。虽然可以保留访问控制列表，但所有权和审计信息可能与源系统不同。此行为是预期的。

Amazon S3 存储桶要求

确保您的 Amazon S3 存储桶满足以下要求。

Amazon S3 支持的数据代理位置

包含 S3 存储的同步关系需要在 AWS 或您的场所部署数据代理。无论哪种情况，复制和同步都会提示您在安装期间将数据代理与 AWS 帐户关联。

- ["了解如何部署 AWS 数据代理"](#)
- ["了解如何在 Linux 主机上安装数据代理"](#)

支持的 AWS 区域

除中国地区外，所有地区均受支持。

其他 AWS 帐户中的 S3 存储桶所需的权限

设置同步关系时，您可以指定位于与数据代理无关的 AWS 帐户中的 S3 存储桶。

["此 JSON 文件中包含的权限"](#)必须应用于该 S3 存储桶，以便数据代理可以访问它。这些权限使数据代理能够将数据复制到存储桶或从存储桶中复制数据，并列出存储桶中的对象。

请注意 JSON 文件中包含的权限的以下几点：

1. `<BucketName>` 是位于与数据代理无关的 AWS 帐户中的存储桶的名称。
2. `<RoleARN>` 应替换为以下之一：
 - 如果在 Linux 主机上手动安装了数据代理，则 `RoleARN` 应该是您在部署数据代理时为其提供 AWS 凭证的 AWS 用户的 ARN。

- 。如果使用 CloudFormation 模板在 AWS 中部署了数据代理，则 *RoleARN* 应该是该模板创建的 IAM 角色的 ARN。

您可以通过转到 EC2 控制台、选择数据代理实例，然后从描述选项卡中选择 IAM 角色来找到角色 ARN。然后，您应该会在 IAM 控制台中看到包含角色 ARN 的“摘要”页面。

Summary

Delete role

Role ARN `arn:aws:iam::142981742600:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 
Role description [Edit](#)

Azure Blob 存储要求

确保您的 Azure Blob 存储满足以下要求。

Azure Blob 支持的数据代理位置

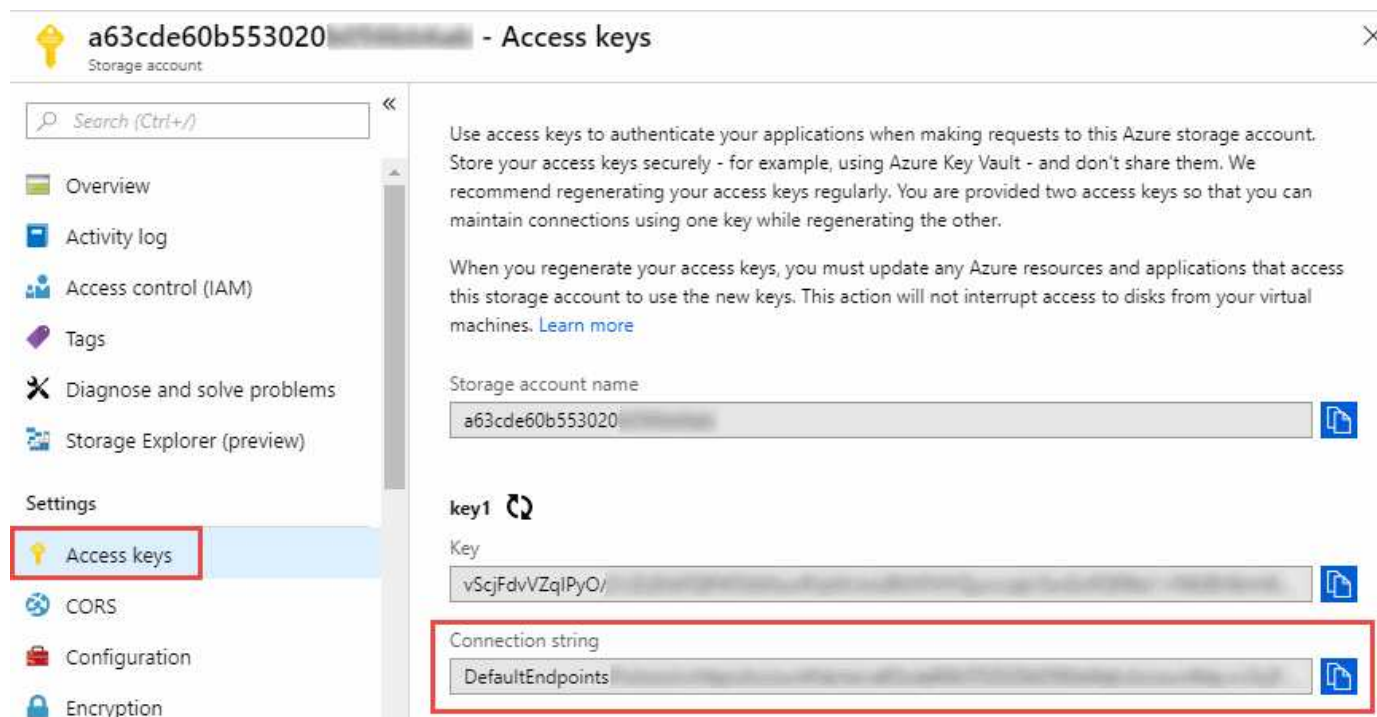
当同步关系包括 Azure Blob 存储时，数据代理可以驻留在任何位置。

支持的 Azure 区域

除中国、美国政府和美国国防部地区外，所有地区均受支持。

包含 Azure Blob 和 NFS/SMB 的关系的连接字符串

在 Azure Blob 容器和 NFS 或 SMB 服务器之间创建同步关系时，需要为复制和同步提供存储帐户连接字符串：



a63cde60b553020 - Access keys

Use access keys to authenticate your applications when making requests to this Azure storage account. Store your access keys securely - for example, using Azure Key Vault - and don't share them. We recommend regenerating your access keys regularly. You are provided two access keys so that you can maintain connections using one key while regenerating the other.

When you regenerate your access keys, you must update any Azure resources and applications that access this storage account to use the new keys. This action will not interrupt access to disks from your virtual machines. [Learn more](#)

Storage account name: `a63cde60b553020`

key1

Key: `vScjFdvVZqIPyO/`

Connection string: `DefaultEndpoints`

如果要在两个 Azure Blob 容器之间同步数据，则连接字符串必须包含“共享访问签名”（SAS）。您还可以选择在 Blob 容器和 NFS 或 SMB 服务器之间同步时使用 SAS。

SAS 必须允许访问 Blob 服务和所有资源类型（服务、容器和对象）。SAS 还必须包含以下权限：

- 对于源 Blob 容器：读取和列出
- 对于目标 Blob 容器：读取、写入、列出、添加和创建

Storage account: a63cde60b553020 - Shared access signature

Search (Ctrl+/)

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Storage Explorer (preview)

Settings

Access keys

CORS

Configuration

Encryption

Shared access signature

Firewalls and virtual networks

Advanced Threat Protection (pr...

Properties

Locks

Allowed services ⓘ

☒ Blob ☐ File ☐ Queue ☐ Table

Allowed resource types ⓘ

☒ Service ☒ Container ☒ Object

Allowed permissions ⓘ

☒ Read ☒ Write ☒ Delete ☒ List ☒ Add ☒ Create ☐ Update ☐ Process

Start and expiry date/time ⓘ

Start

2018-10-23 10:07:32 AM

End

2019-10-23 6:07:32 PM

(UTC-04:00) --- Current Time Zone ---

Allowed IP addresses ⓘ

for example, 168.1.5.65 or 168.1.5.65-168.1.5.70

Allowed protocols ⓘ

☒ HTTPS only ☐ HTTPS and HTTP

Signing key ⓘ

key1

Generate SAS and connection string



如果您选择实现包含 Azure Blob 容器的连续同步关系，则可以使用常规连接字符串或 SAS 连接字符串。如果使用 SAS 连接字符串，则不得将其设置为在不久的将来过期。

Azure 数据湖存储 Gen2

创建包含 Azure Data Lake 的同步关系时，需要为复制和同步提供存储帐户连接字符串。它必须是常规连接字符串，而不是共享访问签名（SAS）。

Azure NetApp Files 要求

在与 Azure NetApp Files 同步数据时，请使用 Premium 或 Ultra 服务级别。如果磁盘服务级别为标准，您可能会遇到故障和性能问题。



如果您需要帮助确定正确的服务级别，请咨询解决方案架构师。卷大小和卷层决定了您可以获得的吞吐量。

["详细了解Azure NetApp Files服务级别和吞吐量"](#)。

盒子要求

- 要创建包含 Box 的同步关系，您需要提供以下凭据：
 - 客户端 ID
 - 客户端机密
 - 私钥
 - 公钥ID
 - 密码短语
 - 企业 ID
- 如果您创建从 Amazon S3 到 Box 的同步关系，则必须使用具有统一配置的数据代理组，其中以下设置设置为 1：
 - 扫描仪并发
 - 扫描仪进程限制
 - 转账并发
 - 转移者进程限制

["了解如何为数据代理组定义统一配置"](#)。

Google Cloud Storage 存储桶要求

确保您的 Google Cloud Storage 存储桶满足以下要求。

Google Cloud Storage 支持的数据代理位置

包含 Google Cloud Storage 的同步关系需要在 Google Cloud 或您的场所部署数据代理。当您创建同步关系时，复制和同步会指导您完成数据代理安装过程。

- ["了解如何部署 Google Cloud 数据代理"](#)
- ["了解如何在 Linux 主机上安装数据代理"](#)

支持的 Google Cloud 区域

支持所有地区。

其他 Google Cloud 项目中存储桶的权限

设置同步关系时，如果您向数据代理的服务帐户提供所需的权限，则可以从不同项目中的 Google Cloud 存储桶中进行选择。["了解如何设置服务帐户"](#)。

SnapMirror目标的权限

如果同步关系的源是SnapMirror目标（只读），则“读取/列出”权限足以将数据从源同步到目标。

加密 Google Cloud 存储桶

您可以使用客户管理的 KMS 密钥或默认的 Google 管理密钥加密目标 Google Cloud 存储桶。如果存储桶已添加了 KMS 加密，它将覆盖默认的 Google 管理加密。

要添加客户管理的 KMS 密钥，您需要使用具有 **"正确的权限"**，并且 key 必须与 bucket 位于同一区域。

Google 云端硬盘

当您设置包含 Google Drive 的同步关系时，您需要提供以下信息：

- 有权访问您要同步数据的 Google Drive 位置的用户的电子邮件地址
- 有权访问 Google Drive 的 Google Cloud 服务帐户的电子邮件地址
- 服务帐户的私钥

要设置服务帐户，请按照 Google 文档中的说明进行操作：

- ["创建服务帐户和凭据"](#)
- ["将域范围的权限委托给您的服务帐户"](#)

编辑 OAuth 范围字段时，输入以下范围：

- <https://www.googleapis.com/auth/drive>
- <https://www.googleapis.com/auth/drive.file>

NFS 服务器要求

- NFS 服务器可以是NetApp系统，也可以是非NetApp系统。
- 文件服务器必须允许数据代理主机通过所需端口访问导出。
 - 111 TCP/UDP
 - 2049 TCP/UDP
 - 5555 TCP/UDP
- 支持 NFS 版本 3、4.0、4.1 和 4.2。

必须在服务器上启用所需的版本。

- 如果要从ONTAP系统同步 NFS 数据，请确保已启用对 SVM 的 NFS 导出列表的访问（`vserver nfs modify -vserver svm_name -showmount enabled`）。



从ONTAP 9.2 开始，showmount 的默认设置为 *enabled*。

ONTAP 要求

如果同步关系包括Cloud Volumes ONTAP或本地ONTAP集群，并且您选择了 NFSv4 或更高版本，则需要 在ONTAP系统上启用 NFSv4 ACL。这是复制 ACL 所必需的。

ONTAP S3 存储要求

当您设置包含以下内容的同步关系时 **"ONTAP S3 存储"**，您需要提供以下信息：

- 连接到ONTAP S3 的 LIF 的 IP 地址
- ONTAP配置使用的访问密钥和密钥

SMB 服务器要求

- SMB 服务器可以是NetApp系统，也可以是非NetApp系统。
- 您需要向复制和同步提供在 SMB 服务器上具有权限的凭据。
 - 对于源 SMB 服务器，需要以下权限：列出和读取。

备份操作员组的成员受到源 SMB 服务器的支持。

- 对于目标 SMB 服务器，需要以下权限：列出、读取和写入。
- 文件服务器必须允许数据代理主机通过所需端口访问导出。
 - 139 TCP
 - 445 TCP
 - 137-138 UDP
- 支持 SMB 版本 1.0、2.0、2.1、3.0 和 3.11。
- 授予“管理员”组对源文件夹和目标文件夹的“完全控制”权限。

如果您不授予此权限，则数据代理可能没有足够的权限来获取文件或目录的 ACL。如果发生这种情况，您将收到以下错误：“getxattr 错误 95”

隐藏目录和文件的 **SMB** 限制

在 SMB 服务器之间同步数据时，SMB 限制会影响隐藏目录和文件。如果源 SMB 服务器上的任何目录或文件通过 Windows 隐藏，则隐藏属性不会复制到目标 SMB 服务器。

由于不区分大小写限制导致的 **SMB** 同步行为

SMB 协议不区分大小写，这意味着大写字母和小写字母被视为相同。如果同步关系包括 SMB 服务器并且目标上已存在数据，则此行为可能导致文件覆盖和目录复制错误。

例如，假设源上有一个名为“a”的文件，目标上有一个名为“A”的文件。当复制和同步将名为“a”的文件复制到目标时，文件“A”将被源中的文件“a”覆盖。

对于目录，假设源上有一个名为“b”的目录，目标上有一个名为“B”的目录。当“复制和同步”尝试将名为“b”的目录复制到目标时，“复制和同步”会收到一条错误消息，提示该目录已存在。因此，复制和同步总是无法复制名为“b”的目录。

避免此限制的最佳方法是确保将数据同步到空目录。

NetApp Copy and Sync的网络概述

NetApp Copy and Sync的网络包括数据代理组与源位置和目标位置之间的连接，以及通过端口 443 来自数据代理的出站互联网连接。

数据代理位置

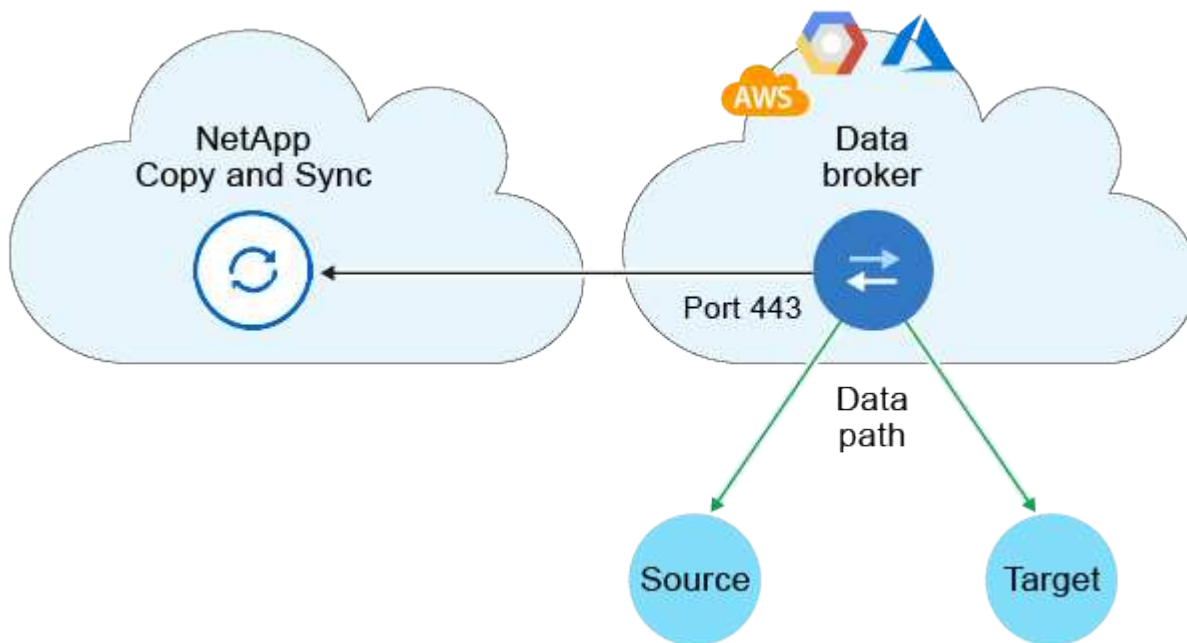
数据代理组由安装在云端或您的场所的一个或多个数据代理组成。

云端数据代理

下图显示了在 AWS、Google Cloud 或 Azure 云中运行的数据代理。只要与数据代理有连接，源和目标就可以位于任何位置。例如，您可能有一个从数据中心到云提供商的 VPN 连接。

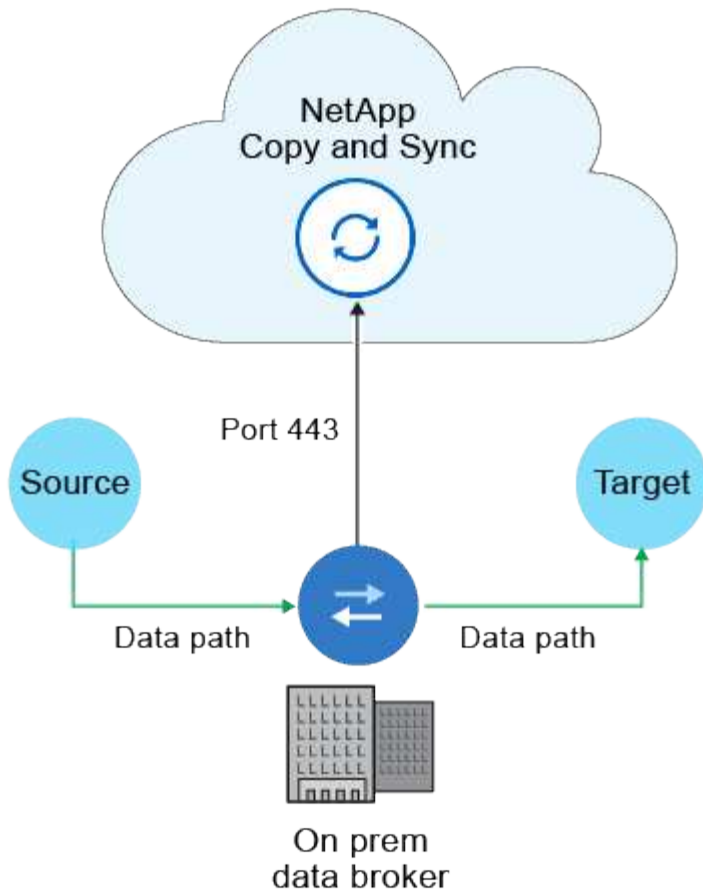


当 Copy and Sync 在 AWS、Azure 或 Google Cloud 中部署数据代理时，它会创建一个安全组来启用所需的出站通信。



您所在地的数据代理

下图显示了在数据中心内部运行的数据代理。同样，只要与数据代理有连接，源和目标就可以位于任何位置。



网络要求

- 源和目标必须与数据代理组有网络连接。
- 例如，如果 NFS 服务器位于您的数据中心，而数据代理位于 AWS 中，那么您需要从您的网络到 VPC 的网络连接（VPN 或 Direct Connect）。
- 数据代理需要出站互联网连接，以便它可以通过端口 443 轮询复制和同步任务。
- NetApp建议配置源、目标和数据代理以使用网络时间协议 (NTP) 服务。三个组件之间的时间差不应超过5分钟。

网络端点

NetApp数据代理需要通过端口 443 进行出站互联网访问，以便与 Copy 和 Sync 进行通信并联系其他一些服务和存储库。您的本地网络浏览器也需要访问端点才能执行某些操作。如果您需要限制出站连接，请在为出站流量配置防火墙时参考以下端点列表。

数据代理端点

数据代理联系以下端点：

端点	目的
https://olcentgbl.trafficmanager.net	联系存储库以更新数据代理主机的 CentOS 软件包。仅当您在 CentOS 主机上手动安装数据代理时才会联系此端点。

端点	目的
\ https://rpm.nodesource.com \ https://registry.npmjs.org \ https://nodejs.org :	联系存储库以更新 Node.js、npm 和开发中使用的其他第三方包。
\ https://tgz.pm2.io	访问用于更新 PM2 的存储库，PM2 是用于监控复制和同步的第三方包。
\ https://sqs.us-east-1.amazonaws.com \ https://kinesis.us-east-1.amazonaws.com	联系复制和同步用于操作（排队文件、注册操作以及向数据代理传递更新）的 AWS 服务。
\ "请参阅 AWS 文档 以获取 S3 端点列表"	当同步关系包含 S3 存储桶时联系 Amazon S3。
\ https://s3.amazonaws.com/	当您从复制和同步下载数据代理日志时，数据代理会压缩其日志目录并将日志上传到 us-east-1 区域中预定义的 S3 存储桶。
\ https://storage.googleapis.com/	当同步关系使用 GCP 存储桶时联系 Google Cloud。
https://storage-account.blob.core.windows.net如果使用 Azure Data Lake Gen2 : https://storage-account.dfs.core.windows.net[]其中 storage-account 是用户的源存储帐户。	打开到用户 Azure 存储帐户地址的代理。
\ https://cf.cloudsync.netapp.com \ https://repo.cloudsync.netapp.com	联系复制和同步。
\ https://support.netapp.com	使用 BYOL 许可证进行同步关系时联系 NetApp 支持。
https://fedoraproject.org	在安装和更新期间在数据代理虚拟机上安装 7z。需要 7z 才能将 AutoSupport 消息发送给 NetApp 技术支持。
\ https://sts.amazonaws.com \ https://sts.us-east-1.amazonaws.com	当数据代理部署在 AWS 中或部署在您的场所并提供 AWS 凭证时，验证 AWS 凭证。数据代理在部署、更新和重新启动时联系此端点。
\ https://api.blueexp.netapp.com \ https://netapp-cloud-account.auth0.com	当您使用分类来选择新同步关系的源文件时，请联系 NetApp Data Classification。
\ https://pubsub.googleapis.com	如果从 Google 存储帐户创建连续同步关系。

端点	目的
<pre>https://storage-account.queue.core.windows.net\ https://management.azure.com/subscriptions/ \${subscriptionId} /resourceGroups/\${resourceGroup}/providers/Microsoft.EventGrid/*</pre> 其中 storage-account 是用户的源存储帐户 ， subscriptionid 是源订阅 ID ， resourceGroup 是源资源组。	如果从 Azure 存储帐户创建连续同步关系。

Web 浏览器端点

您的 Web 浏览器需要访问以下端点来下载日志以进行故障排除：

logs.cloudsync.netapp.com:443

登录NetApp Copy and Sync

使用NetApp Console登录到NetApp Copy and Sync。

要登录控制台，您可以使用您的NetApp支持站点凭据，也可以使用您的电子邮件和密码注册NetApp云登录。 "[了解有关登录的更多信息](#)"。

NetApp Copy and Sync使用身份访问管理来控制每个用户对特定操作的访问权限。

必需的**NetApp Console**角色 组织管理员角色。 "[了解NetApp Console访问角色](#)"。

步骤

1. 打开 Web 浏览器并转到 "[NetApp Console](#)"。

出现NetApp Console登录页面。

2. 登录控制台。
3. 从控制台左侧导航中，选择*移动性*>*复制和同步*。

安装数据代理

在 **AWS** 中为**NetApp Copy and Sync**创建新的数据代理

为NetApp Copy and Sync创建新的数据代理组时，请选择 Amazon Web Services 在 VPC

中的新 EC2 实例上部署数据代理软件。NetApp Copy and Sync将指导您完成安装过程，但此页面上重复了要求和步骤，以帮助您做好安装准备。

您还可以选择在云端或本地的现有 Linux 主机上安装数据代理。[了解更多](#)。

支持的 AWS 区域

除中国地区外，所有地区均受支持。

Root权限

数据代理软件在 Linux 主机上自动以 root 身份运行。以 root 身份运行是数据代理操作的必要条件。例如，挂载共享。

网络要求

- 数据代理需要出站互联网连接，以便它可以通过端口 443 轮询复制和同步任务。

当 Copy and Sync 在 AWS 中部署数据代理时，它会创建一个安全组来启用所需的出站通信。请注意，您可以在安装过程中配置数据代理以使用代理服务器。

如果需要限制出站连接，请参阅["数据代理联系的端点列表"](#)。

- NetApp建议配置源、目标和数据代理以使用网络时间协议 (NTP) 服务。三个组件之间的时间差不应超过5分钟。

在 AWS 中部署数据代理所需的权限

用于部署数据代理的 AWS 用户帐户必须具有以下权限：["NetApp提供的政策"](#)。

将您自己的 IAM 角色与 AWS 数据代理结合使用的要求

当 Copy and Sync 部署数据代理时，它会为数据代理实例创建一个 IAM 角色。如果您愿意，您可以使用自己的 IAM 角色部署数据代理。如果您的组织有严格的安全策略，您可以使用此选项。

IAM 角色必须满足以下要求：

- 必须允许 EC2 服务作为受信任实体承担 IAM 角色。
- ["此 JSON 文件中定义的权限"](#)必须附加到 IAM 角色，以便数据代理可以正常运行。

按照以下步骤在部署数据代理时指定 IAM 角色。

创建数据代理

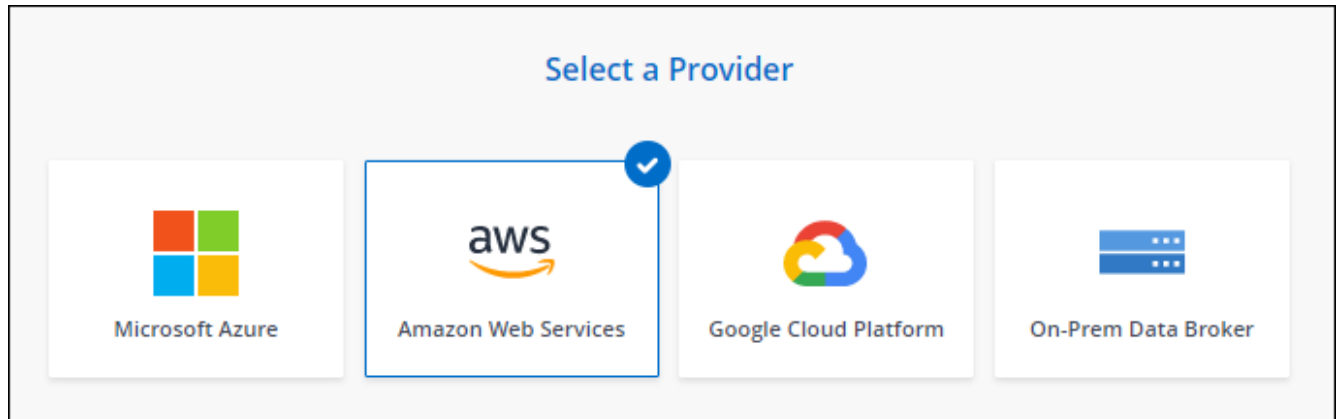
有几种方法可以创建新的数据代理。这些步骤描述了如何在创建同步关系时在 AWS 中安装数据代理。

步骤

1. ["登录以复制和同步"](#)。
2. 选择*创建新同步*。
3. 在*定义同步关系*页面上，选择源和目标，然后选择*继续*。

完成这些步骤，直到到达*数据经纪人组*页面。

4. 在*数据代理组*页面上，选择*创建数据代理*，然后选择*Amazon Web Services*。



5. 输入数据代理的名称并选择*继续*。
6. 输入 AWS 访问密钥，以便 Copy and Sync 可以代表您在 AWS 中创建数据代理。

密钥不会被保存或用于任何其他目的。

如果您不想提供访问密钥，请选择页面底部的链接以使用 CloudFormation 模板。当您使用此选项时，您不需要提供凭证，因为您直接登录到 AWS。

以下视频展示了如何使用 CloudFormation 模板启动数据代理实例：

[从 AWS CloudFormation 模板启动数据代理](#)

7. 如果您输入了 AWS 访问密钥，请选择实例的位置、选择密钥对、选择是否启用公共 IP 地址并选择现有的 IAM 角色，或者将字段留空，以便复制和同步为您创建角色。您还可以选择使用 KMS 密钥加密您的数据代理。

如果您选择自己的 IAM 角色，[您需要提供所需的权限](#)。

Basic Settings

Location

VPC

Select VPC ▼

Subnet

Select Subnet ▼

Connectivity

Key Pair

Select Key Pair ▼

Enable Public IP?

☒ Enable ☐ Disable

IAM Role (optional)

IAM Role (optional) ⓘ

KMS Key for EBS volume (optional)

Select KMS Key for EBS Encryption ▼

8. 如果 VPC 中的互联网访问需要代理，请指定代理配置。
9. 数据代理可用后，在复制和同步中选择*继续*。

下图显示了 AWS 中成功部署的实例：

✓ NFS Server
2 Data Broker Group
 3 Directories
 4 Target NFS Server
 >

Select a Data Broker Group

1 Data Broker Group 🔍

🔍
ben-data-broker
➔

1	N/A	0	✓ 1 Active
Data Brokers	Transfer Rate	Relationships	Data Brokers Status

10. 完成向导中的页面以创建新的同步关系。

结果

您已在 AWS 中部署了数据代理并创建了新的同步关系。您可以将此数据代理组与其他同步关系一起使用。

有关数据代理实例的详细信息

复制和同步使用以下配置在 AWS 中创建数据代理。

Node.js 兼容性

v21.2.0

实例类型

如果该地区可用，则使用 m5n.xlarge，否则使用 m5.xlarge

虚拟 CPU

4

RAM

16 GB

操作系统

亚马逊Linux 2023

磁盘大小和类型

10 GB GP2 固态硬盘

在 Azure 中为 NetApp Copy and Sync 创建新的数据代理

为 NetApp Copy and Sync 创建新的数据代理组时，请选择 Microsoft Azure 在 VNet 中的新虚拟机上部署数据代理软件。NetApp Copy and Sync 将指导您完成安装过程，但此页面上重复了要求和步骤，以帮助您做好安装准备。

您还可以选择在云端或本地的现有 Linux 主机上安装数据代理。["了解更多"](#)。

支持的 Azure 区域

除中国、美国政府和美国国防部地区外，所有地区均受支持。

Root 权限

数据代理软件在 Linux 主机上自动以 root 身份运行。以 root 身份运行是数据代理操作的必要条件。例如，挂载共享。

网络要求

- 数据代理需要出站互联网连接，以便它可以通过端口 443 轮询复制和同步服务的任务。

当 Copy and Sync 在 Azure 中部署数据代理时，它会创建一个安全组来启用所需的出站通信。

如果需要限制出站连接，请参阅["数据代理联系的端点列表"](#)。

- NetApp 建议配置源、目标和数据代理以使用网络时间协议 (NTP) 服务。三个组件之间的时间差不应超过 5 分钟。

在 Azure 中部署数据代理所需的权限

确保用于部署数据代理的 Azure 用户帐户具有以下权限：

```
{
  "Name": "Azure Data Broker",
  "Actions": [
    "Microsoft.Resources/subscriptions/read",

    "Microsoft.Resources/deployments/operationstatuses/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Resources/subscriptions/resourceGroups/write",

    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/validate/action",

    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/disks/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/publicIPAddresses/delete",

    "Microsoft.Network/networkSecurityGroups/securityRules/delete",

    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Compute/disks/write",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/publicIPAddresses/read",

    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/publicIPAddresses/join/action",
```

```

        "Microsoft.Network/networkInterfaces/join/action",
        "Microsoft.Storage/storageAccounts/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/write",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/read",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/delete",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action",

"Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes
/action",
        "Microsoft.EventGrid/systemTopics/read",
        "Microsoft.EventGrid/systemTopics/write",
        "Microsoft.EventGrid/systemTopics/delete",
        "Microsoft.EventGrid/eventSubscriptions/write",
        "Microsoft.Storage/storageAccounts/write"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read"

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write"

"Microsoft.Network/networkSecurityGroups/securityRules/read",
        "Microsoft.Network/networkSecurityGroups/read",

```

```

    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure Data Broker",
    "IsCustom": "true"
}

```

注:

1. 仅当您计划启用 ["连续同步设置"](#) 从 Azure 到另一个云存储位置的同步关系:
 - "Microsoft.Storage/storageAccounts/read",
 - "Microsoft.EventGrid/systemTopics/eventSubscriptions/write",
 - "Microsoft.EventGrid/systemTopics/eventSubscriptions/read",
 - 'Microsoft.EventGrid/systemTopics/eventSubscriptions/delete',

- 'Microsoft.EventGrid/systemTopics/eventSubscriptions/getFullUrl/action',
- “Microsoft.EventGrid/systemTopics/eventSubscriptions/getDeliveryAttributes/action”,
- “Microsoft.EventGrid/systemTopics/读取”,
- “Microsoft.EventGrid/systemTopics/write”,
- “Microsoft.EventGrid/systemTopics/删除”,
- “Microsoft.EventGrid/eventSubscriptions/write”,
- “Microsoft.Storage/storageAccounts/write”

此外，如果您计划在 Azure 中实现连续同步，则必须将可分配范围设置为订阅范围而不是资源组范围。

2. 仅当您计划为数据代理创建选择自己的安全性时才需要以下权限：

- “Microsoft.Network/networkSecurityGroups/securityRules/读取”
- “Microsoft.Network/networkSecurityGroups/读取”

身份验证方法

部署数据代理时，您需要为虚拟机选择一种身份验证方法：密码或 SSH 公钥-私钥对。

有关创建密钥对的帮助，请参阅 ["Azure 文档：在 Azure 中为 Linux VM 创建并使用 SSH 公钥-私钥对"](#)。

创建数据代理

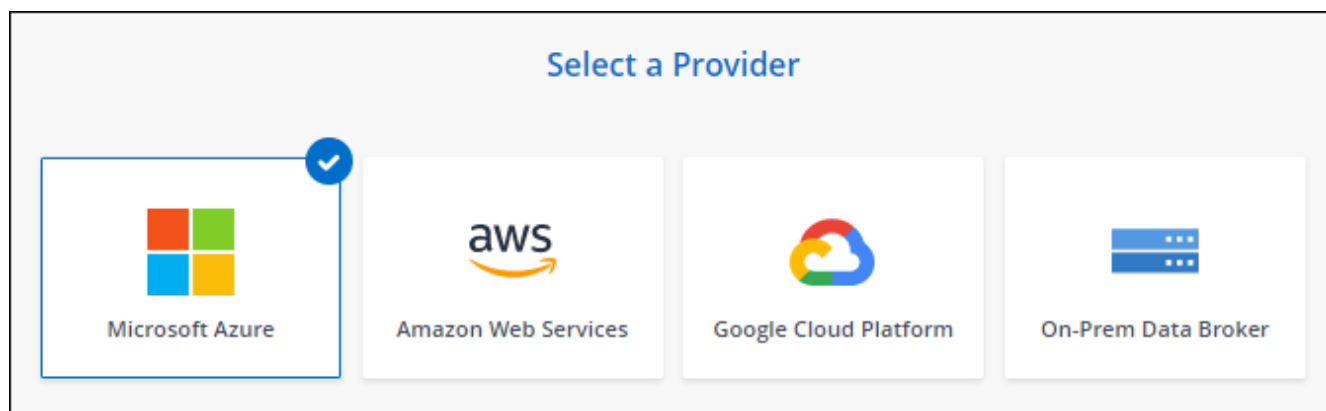
有几种方法可以创建新的数据代理。这些步骤描述了在创建同步关系时如何在 Azure 中安装数据代理。

步骤

1. ["登录以复制和同步"](#)。
2. 选择*创建新同步*。
3. 在*定义同步关系*页面上，选择源和目标，然后选择*继续*。

完成这些步骤，直到到达*数据经纪人组*页面。

4. 在“数据代理组”页面上，选择“创建数据代理”，然后选择“Microsoft Azure”。



5. 输入数据代理的名称并选择*继续*。

6. 如果出现提示，请登录您的 Microsoft 帐户。如果没有提示，请选择“登录 Azure”。

该表单由 Microsoft 拥有并托管。您的凭据未提供给 NetApp。

7. 选择数据代理的位置并输入有关虚拟机的基本详细信息。



如果您计划实现持续同步关系，则必须为数据代理分配自定义角色。这也可以在创建代理后手动完成。

8. 如果 VNet 中的 Internet 访问需要代理，请指定代理配置。

9. 选择*继续*。如果您想向数据代理添加 S3 权限，请输入您的 AWS 访问和密钥。

10. 选择*继续*并保持页面打开，直到部署完成。

该过程最多可能需要 7 分钟。

11. 在复制和同步中，一旦数据代理可用，请选择*继续*。

12. 完成向导中的页面以创建新的同步关系。

结果

您已在 Azure 中部署了数据代理并创建了新的同步关系。您可以将此数据代理与其他同步关系一起使用。

收到需要管理员同意的消息吗？

如果 Microsoft 通知您需要管理员批准，因为复制和同步需要代表您访问组织中的资源的权限，那么您有两个选择：

1. 要求您的 AD 管理员为您提供以下权限：

在 Azure 中，转到 管理中心 > **Azure AD** > 用户和组 > 用户设置 并启用 用户可以同意应用程序代表他们访问公司数据。

2. 请求您的 AD 管理员代表您同意使用以下 URL（这是管理员同意端点） **CloudSync-AzureDataBrokerCreator**：

\ [https://login.microsoftonline.com/ {在此处填写您的租户 ID}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri= https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read](https://login.microsoftonline.com/{在此处填写您的租户 ID}/v2.0/adminconsent?client_id=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read)

如URL所示，我们的应用程序URL是\ <https://cloudsync.netapp.com> ，应用程序客户端ID是8ee4ca3a-bafa-4831-97cc-5a38923cab85。

有关数据代理虚拟机的详细信息

复制和同步使用以下配置在 Azure 中创建数据代理。

Node.js 兼容性

v21.2.0

VM 类型

标准 DS4 v2

虚拟 CPU

8

RAM

28 GB

操作系统

Rocky Linux 9.0

磁盘大小和类型

64 GB 高级固态硬盘

在 Google Cloud 中为NetApp Copy and Sync创建新的数据代理

为NetApp Copy and Sync创建新的数据代理组时，请选择 Google Cloud Platform 在 Google Cloud VPC 中的新虚拟机实例上部署数据代理软件。 NetApp Copy and Sync将指导您完成安装过程，但此页面上重复了要求和步骤，以帮助您做好安装准备。

您还可以选择在云端或本地的现有 Linux 主机上安装数据代理。["了解更多"](#)。

支持的 Google Cloud 区域

支持所有地区。

Root 权限

数据代理软件在 Linux 主机上自动以 root 身份运行。以 root 身份运行是数据代理操作的必要条件。例如，挂载共享。

网络要求

- 数据代理需要出站互联网连接，以便它可以通过端口 443 轮询复制和同步任务。

当 Copy and Sync 在 Google Cloud 中部署数据代理时，它会创建一个安全组来启用所需的出站通信。

如果需要限制出站连接，请参阅["数据代理联系的端点列表"](#)。

- NetApp 建议配置源、目标和数据代理以使用网络时间协议 (NTP) 服务。三个组件之间的时间差不应超过 5 分钟。

在 Google Cloud 中部署数据代理所需的权限

确保部署数据代理的 Google Cloud 用户具有以下权限：

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

服务帐户所需的权限

部署数据代理时，您需要选择具有以下权限的服务帐户：

```
- logging.logEntries.create
- resourceManager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.getIamPolicy
- storage.objects.list
- storage.objects.setIamPolicy
- storage.objects.update
- iam.serviceAccounts.signJwt
- pubsub.subscriptions.consume
- pubsub.subscriptions.create
- pubsub.subscriptions.delete
- pubsub.subscriptions.list
- pubsub.topics.attachSubscription
- pubsub.topics.create
- pubsub.topics.delete
- pubsub.topics.list
- pubsub.topics.setIamPolicy
- storage.buckets.update
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

注：

1. 仅当您计划设置数据代理以使用外部 HashiCorp 保险库时才需要“iam.serviceAccounts.signJwt”权限。
2. 仅当您计划在从 Google Cloud Storage 到另一个云存储位置的同步关系上启用连续同步设置时，才需要“pubsub.*”和“storage.buckets.update”权限。[了解有关持续同步选项的更多信息](#)。
3. 仅当您计划在目标 Google Cloud Storage 存储桶上使用客户管理的 KMS 密钥时，才需要“cloudkms.cryptoKeys.list”和“cloudkms.keyRings.list”权限。

创建数据代理

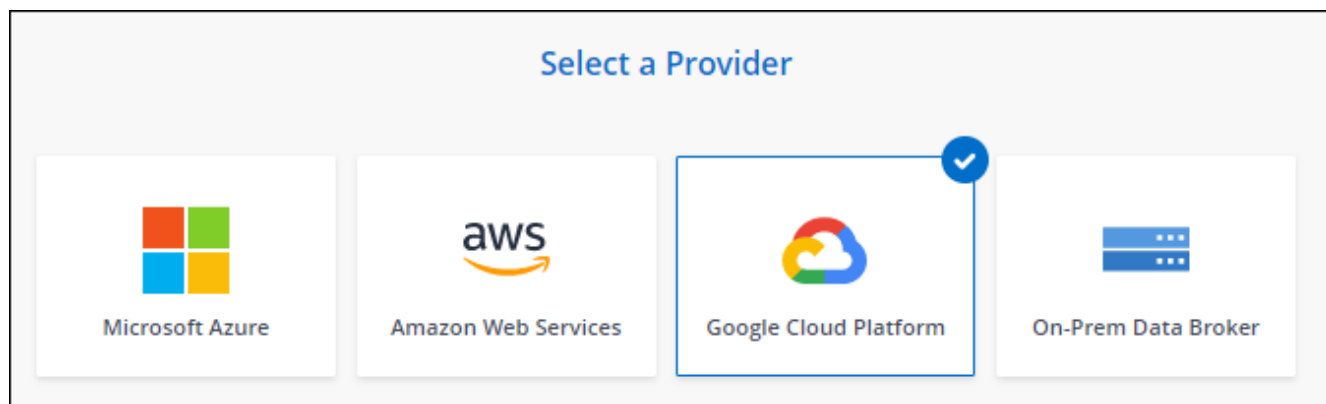
有几种方法可以创建新的数据代理。以下步骤描述了在创建同步关系时如何在 Google Cloud 中安装数据代理。

步骤

1. ["登录以复制和同步"](#)。
2. 选择*创建新同步*。
3. 在*定义同步关系*页面上，选择源和目标，然后选择*继续*。

完成这些步骤，直到到达*数据经纪人组*页面。

4. 在*数据经纪人组*页面上，选择*创建数据经纪人*，然后选择*Google Cloud Platform*。



5. 输入数据代理的名称并选择*继续*。

6. 如果出现提示，请使用您的 Google 帐户登录。

该表单由 Google 拥有并托管。您的凭据未提供给NetApp。

7. 选择一个项目和服务帐户，然后选择数据代理的位置，包括是否要启用或禁用公共 IP 地址。

如果您没有启用公共 IP 地址，那么您需要在下一步中定义代理服务器。

The screenshot shows a 'Basic Settings' form with two columns. The left column contains 'Project' (dropdown with 'OCCM-Dev') and 'Service Account' (dropdown with 'test'). Below these is a link: 'Select a Service Account that includes [these permissions](#)'. The right column contains 'Location' with 'Region' (dropdown with 'us-west1') and 'Zone' (dropdown with 'us-west1-a'). Below these are 'VPC' (dropdown with 'default') and 'Subnet' (dropdown with 'default'). At the bottom is 'Public IP' (dropdown with 'Enable').

8. 如果 VPC 中的互联网访问需要代理，请指定代理配置。

如果需要代理才能访问互联网，则代理必须位于 Google Cloud 中并使用与数据代理相同的服务帐户。

9. 一旦数据代理可用，请在复制和同步中选择*继续*。

该实例大约需要 5 到 10 分钟才能部署。您可以从复制和同步中监控进度，当实例可用时会自动刷新。

10. 完成向导中的页面以创建新的同步关系。

结果

您已在 Google Cloud 中部署了数据代理并创建了新的同步关系。您可以将此数据代理与其他同步关系一起使用。

提供在其他 Google Cloud 项目中使用存储桶的权限

当您创建同步关系并选择 Google Cloud Storage 作为源或目标时，复制和同步可让您从数据代理的服务帐户有权使用的存储桶中进行选择。默认情况下，这包括与数据代理服务帐户位于同一项目中的存储桶。但是如果您提供所需的权限，您可以从其他项目中选择存储桶。

步骤

1. 打开 Google Cloud Platform 控制台并加载 Cloud Storage 服务。
2. 选择您想要用作同步关系中的源或目标的存储桶的名称。
3. 选择*权限*。
4. 选择“添加”。
5. 输入数据代理的服务帐户的名称。
6. 选择提供以下功能的角色[与上面显示的权限相同](#)。
7. 选择*保存*。

结果

当您设置同步关系时，您现在可以选择该存储桶作为同步关系中的源或目标。

有关数据代理虚拟机实例的详细信息

复制和同步使用以下配置在 Google Cloud 中创建数据代理。

Node.js 兼容性

v21.2.0

机器类型

n2-标准-4

虚拟 CPU

4

RAM

15 GB

操作系统

Rocky Linux 9.0

磁盘大小和类型

20 GB 硬盘 pd-标准

在 Linux 主机上安装用于NetApp Copy and Sync的数据代理

为NetApp Copy and Sync创建新的数据代理组时，请选择 On-Prem Data Broker 选项在本地 Linux 主机或云中的现有 Linux 主机上安装数据代理软件。NetApp Copy and Sync将指导您完成安装过程，但此页面上重复了要求和步骤，以帮助您做好安装准备。

Linux 主机要求

- Node.js 兼容性：v21.2.0
- 操作系统：
 - CentOS 8.0 和 8.5
 - CentOS Stream 不受支持。
 - Red Hat Enterprise Linux 8.5、8.8、8.9 和 9.4
 - Rocky Linux 9
 - Ubuntu Server 20.04 LTS、23.04 LTS 和 24.04 LTS
 - SUSE Linux Enterprise Server 15 SP1

命令 `yum update` 在安装数据代理之前必须在主机上运行。

Red Hat Enterprise Linux 系统必须在 Red Hat 订阅管理中注册。如果未注册，系统将无法访问存储库来在安装期间更新所需的第三方软件。

- 内存：16 GB
- **CPU**：4核
- 可用磁盘空间：10 GB
- **SELinux**：我们建议您在主机上禁用 SELinux。

SELinux 强制执行阻止数据代理软件更新的策略，并可以阻止数据代理联系正常运行所需的端点。

Root权限

数据代理软件在 Linux 主机上自动以 root 身份运行。以 root 身份运行是数据代理操作的必要条件。例如，挂载共享。

网络要求

- Linux 主机必须与源和目标建立连接。

- 文件服务器必须允许 Linux 主机访问导出。
- Linux 主机上必须打开端口 443 才能向 AWS 发送出站流量（数据代理不断与 Amazon SQS 服务通信）。
- NetApp 建议配置源、目标和数据代理以使用网络时间协议 (NTP) 服务。三个组件之间的时间差不应超过 5 分钟。

启用对 **AWS** 的访问

如果您计划使用包含 S3 存储桶的同步关系的数据代理，那么您应该准备好 Linux 主机以供 AWS 访问。安装数据代理时，您需要为具有编程访问权限和特定权限的 AWS 用户提供 AWS 密钥。

步骤

1. 使用创建 IAM 策略 ["NetApp 提供的政策"](#)

["查看 AWS 说明"](#)

2. 创建具有编程访问权限的 IAM 用户。

["查看 AWS 说明"](#)

请务必复制 AWS 密钥，因为您需要在安装数据代理软件时指定它们。

启用对 **Google Cloud** 的访问

如果您计划使用包含 Google Cloud Storage 存储桶的同步关系的数据代理，那么您应该准备 Linux 主机以供 Google Cloud 访问。安装数据代理时，您需要为具有特定权限的服务帐户提供密钥。

步骤

1. 如果您还没有 Google Cloud 服务帐户，请创建一个具有存储管理员权限的 Google Cloud 服务帐户。
2. 创建以 JSON 格式保存的服务帐户密钥。

["查看 Google Cloud 说明"](#)

该文件至少应包含以下属性：“project_id”、“private_key”和“client_email”



当您创建密钥时，文件就会生成并下载到您的机器上。

3. 将 JSON 文件保存到 Linux 主机。

启用对 **Microsoft Azure** 的访问

通过在同步关系向导中提供存储帐户和连接字符串来定义每个关系对 Azure 的访问。

安装数据代理

创建同步关系时，您可以在 Linux 主机上安装数据代理。

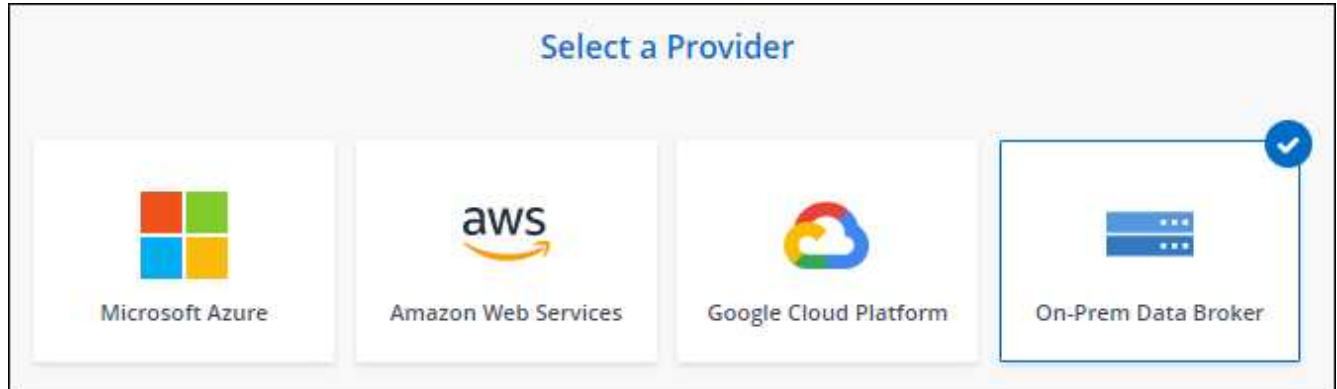
步骤

1. ["登录以复制和同步"](#)。

2. 选择*创建新同步*。
3. 在*定义同步关系*页面上，选择源和目标，然后选择*继续*。

完成这些步骤，直到到达*数据经纪人组*页面。

4. 在*数据代理组*页面上，选择*创建数据代理*，然后选择*本地数据代理*。



尽管该选项标记为 **On-Prem Data Broker**，但它适用于您所在地或云中的 Linux 主机。

5. 输入数据代理的名称并选择*继续*。

说明页面很快就会加载。您需要遵循这些说明 - 它们包含下载安装程序的唯一链接。

6. 在说明页面上：
 - a. 选择是否启用对 **AWS**、**Google Cloud** 或两者的访问。
 - b. 选择安装选项：无代理、使用代理服务器*或*使用带有身份验证的代理服务器。



该用户必须是本地用户。不支持域用户。

- c. 使用命令下载并安装数据代理。

以下步骤提供了有关每个可能的安装选项的详细信息。按照说明页面根据您的安装选项获取准确的命令。

- d. 下载安装程序：

- 无代理：

```
curl <URI> -o data_broker_installer.sh
```

- 使用代理服务器：

```
curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
```

- 使用带有身份验证的代理服务器：

```
curl <URI> -o data_broker_installer.sh -x  
<proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
```

URI

复制和同步会在说明页面上显示安装文件的 URI，当您按照提示部署 On-Prem 数据代理时，该页面会加载。该 URI 不会在此重复，因为链接是动态生成的并且只能使用一次。[按照以下步骤从复制和同步中获取 URI](#)。

e. 切换到超级用户，使安装程序可执行并安装软件：



下面列出的每个命令都包含 AWS 访问和 Google Cloud 访问的参数。按照说明页面根据您的安装选项获取准确的命令。

▪ 无代理配置：

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file>
```

▪ 代理配置：

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

▪ 带有身份验证的代理配置：

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

AWS 密钥

这些是您应该为用户准备的密钥[按照以下步骤](#)。AWS 密钥存储在数据代理上，该代理在您的本地或云网络中运行。NetApp 不使用数据代理之外的密钥。

JSON 文件

这是包含您应该准备好的服务帐户密钥的 JSON 文件[按照以下步骤](#)。

7. 一旦数据代理可用，请在复制和同步中选择*继续*。
8. 完成向导中的页面以创建新的同步关系。

版权信息

版权所有 © 2025 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 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。