



Cloud Sync 文档

Cloud Sync

NetApp
April 07, 2022

目录

Cloud Sync 文档	1
发行说明	2
Cloud Sync 的新增功能	2
限制	11
入门	12
Cloud Sync 概述	12
Cloud Sync 快速入门	14
支持的同步关系	15
准备源和目标	22
Cloud Sync 网络概述	28
安装数据代理	31
使用 Cloud Sync	44
在源和目标之间同步数据	44
在免费试用结束后为同步关系付费	61
管理同步关系	63
管理数据代理组	68
创建和查看报告以调整配置	75
卸载数据代理	78
云同步 API	80
入门	80
API 参考	81
使用列表 API	81
概念	84
许可概述	84
数据隐私	85
Cloud Sync 技术常见问题解答	85
知识和支持	92
注册以获得支持	92
获取帮助	92
法律声明	93

Cloud Sync 文档

发行说明

Cloud Sync 的新增功能

了解 Cloud Sync 中的新增功能。

2022 年 4 月 3 日

数据代理组增强功能

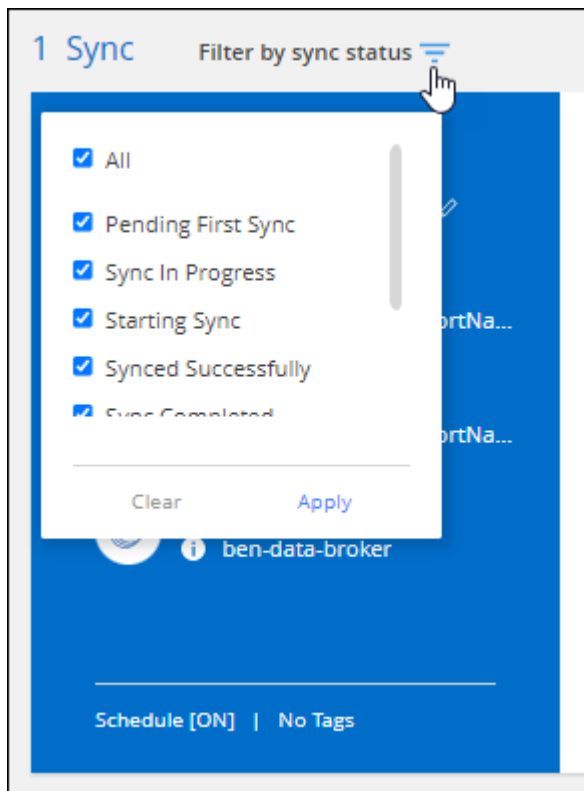
我们对数据代理组进行了多项增强：

- 现在，您可以将数据代理移动到新的或现有的组。
- 现在，您可以更新数据代理的代理配置。
- 最后，您还可以删除数据代理组。

["了解如何管理数据代理组"](#)。

信息板筛选器

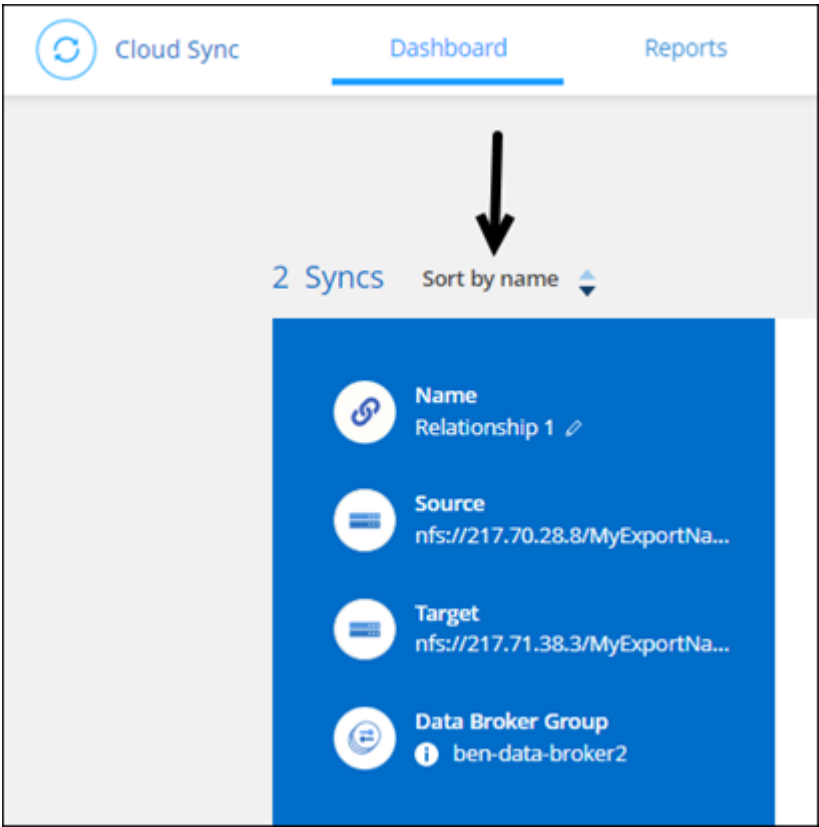
现在，您可以筛选 "同步信息板" 的内容，以便更轻松地查找与特定状态匹配的同步关系。例如，您可以筛选状态为失败的同步关系



2022 年 3 月 3 日

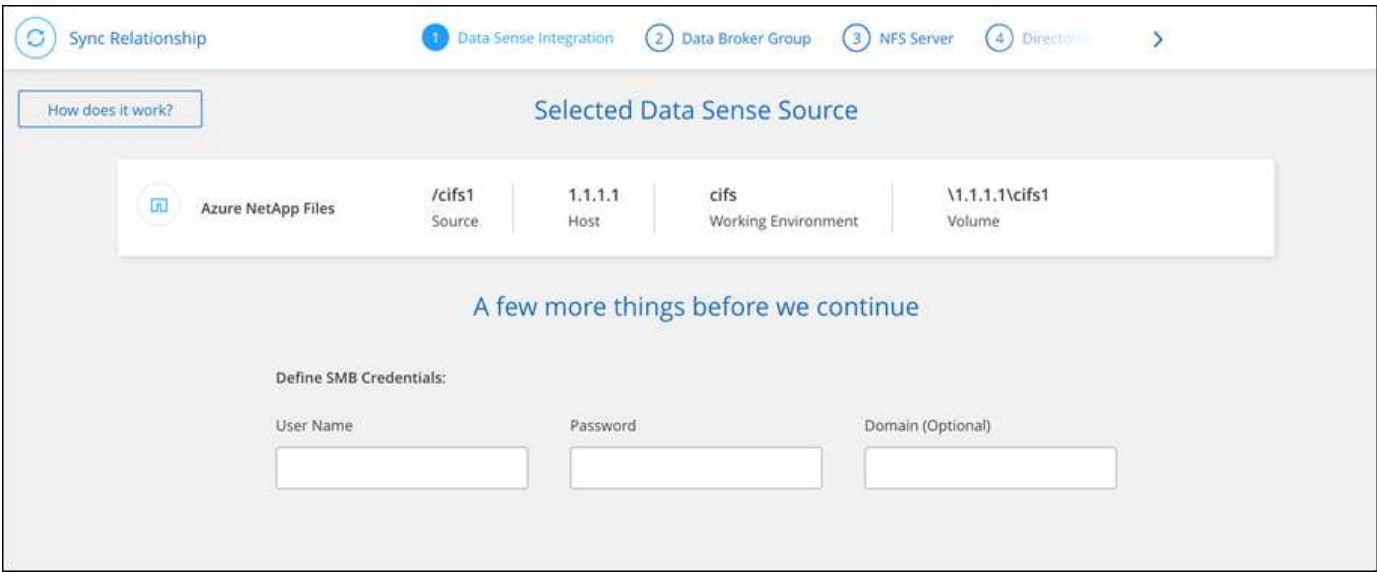
在信息板中排序

现在，您可以按同步关系名称对信息板进行排序。



增强了 Data sense 集成功能

在上一版本中，我们引入了 Cloud Sync 与 Cloud Data sense 的集成。在此更新中，我们简化了创建同步关系的过程，从而增强了集成能力。从 Cloud Data sense 启动数据同步后，所有源信息都包含在一个步骤中，只需输入几个关键详细信息即可。

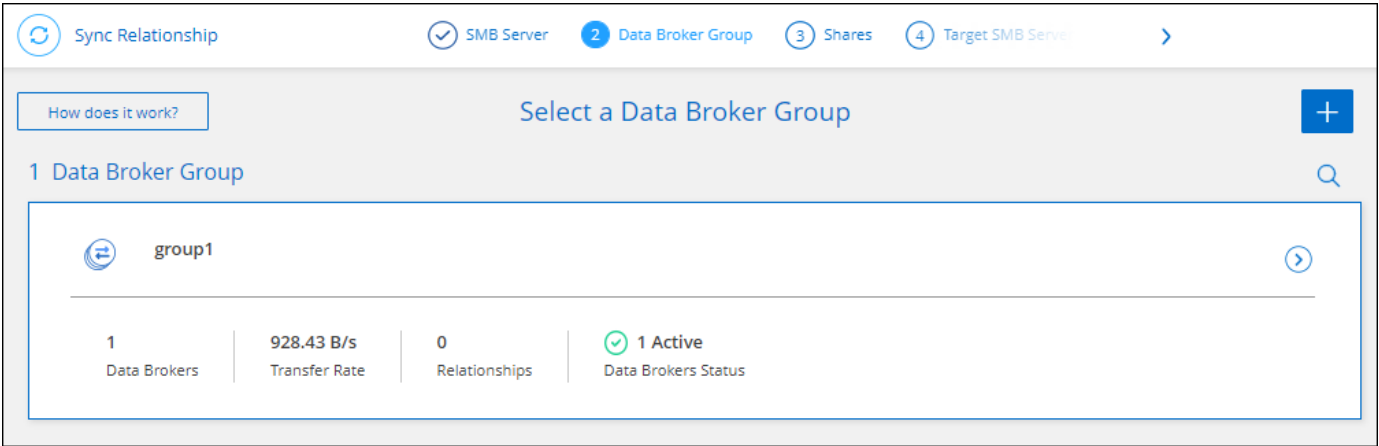


2022 年 2 月 6 日

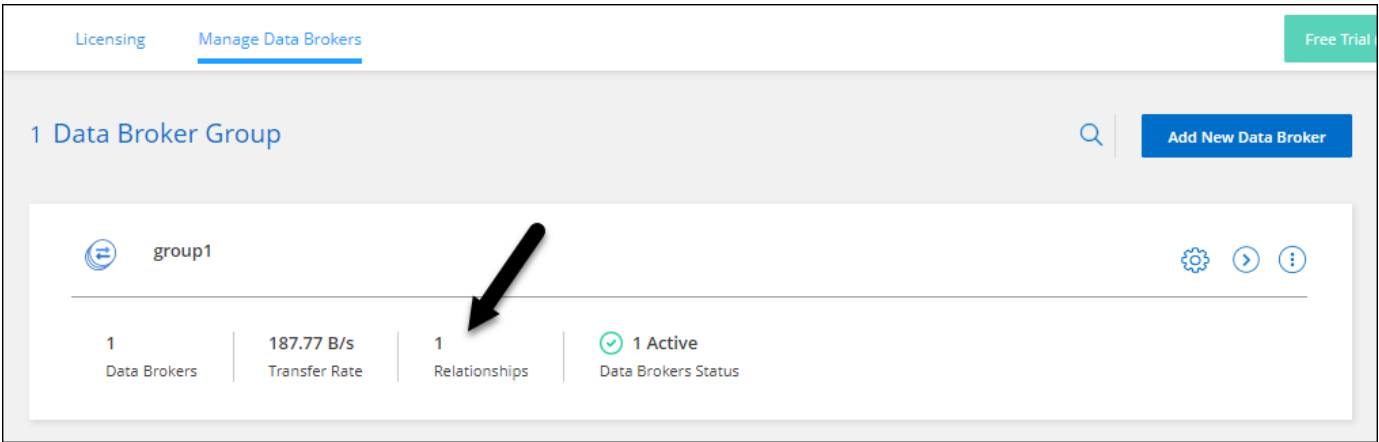
数据代理组的增强功能

我们通过强调数据代理 `_groups_` 来 改变您与数据代理的交互方式。

例如，在创建新的同步关系时，您可以选择要用于该关系的数据代理 *group* ，而不是特定的数据代理。



在 * 管理数据代理 * 选项卡中，我们还会显示数据代理组正在管理的同步关系的数量。



下载 PDF 报告

现在，您可以下载报告的 PDF 。

["了解有关报告的更多信息"](#)。

2022 年 1 月 2 日

新的框同步关系

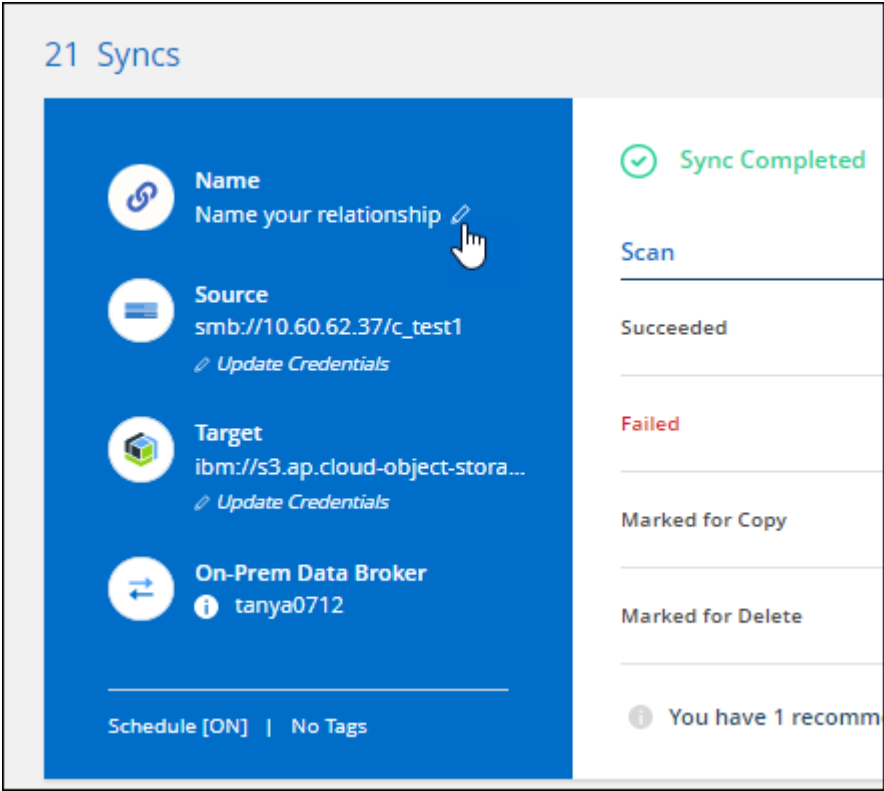
支持两种新的同步关系：

- Azure NetApp Files 对应的方框
- Amazon FSX for ONTAP 对应的框

"查看支持的同步关系列表"。

关系名称

现在，您可以为每个同步关系提供一个有意义的名称，以便更轻松确定每个关系的用途。您可以在创建关系时以及之后的任何时间添加此名称。



S3 专用链路

在与 Amazon S3 同步数据时，您可以选择是否使用 S3 专用链路。当数据代理将数据从源复制到目标时，它将通过专用链路。

请注意，与数据代理关联的 IAM 角色需要以下权限才能使用此功能：

```
"ec2:DescribeVpcEndpoints"
```

此权限会自动添加到您创建的任何新数据代理中。

Glacier 即时检索

现在，如果 Amazon S3 是同步关系中的目标，您可以选择 _Glacier 即时检索_ 存储类。

从对象存储到 SMB 共享的 ACL

现在，Cloud Sync 支持将 ACL 从对象存储复制到 SMB 共享。以前，我们仅支持将 ACL 从 SMB 共享复制到对象存储。

SFTP 到 S3

现在，可以在用户界面中创建从 SFTP 到 Amazon S3 的同步关系。此同步关系以前仅支持 API。

表视图增强功能

我们重新设计了信息板上的表视图，以便于使用。如果单击 * 更多信息 *，Cloud Sync 将筛选信息板，以显示有关该特定关系的更多信息。

4 Syncs

Name	Source	Target	Sync Status	More
hll	s3://phoebe	ibmc/r1.1.1.1:80/medium/test	Sync Completed	More info
test	s3://small	s3://phoebe	Sync Completed	More info
Name your relationship	s3://medium	s3://joey	Sync Completed	More info
Name your relationship	s3://small	s3://joey	Sync Completed	More info

支持 Jarkarta 地区

Cloud Sync 现在支持在 AWS 亚太地区（雅加达）部署数据代理。

2021 年 11 月 28 日

从 SMB 到对象存储的 ACL

现在，在设置从源 SMB 共享到对象存储的同步关系时，Cloud Sync 可以复制访问控制列表（ACL）（ONTAP S3 除外）。

Cloud Sync 不支持将 ACL 从对象存储复制到 SMB 共享。

"了解如何从 SMB 共享复制 ACL"。

更新许可证

现在，您可以更新已扩展的 Cloud Sync 许可证。

如果您延长了从 NetApp 购买的 Cloud Sync 许可证，则可以重新添加此许可证以刷新到期日期。

"了解如何更新许可证"。

更新框凭据

现在，您可以更新现有同步关系的 Box 凭据。

"了解如何更新凭据"。

2021 年 10 月 31 日

盒装支持

现在，Cloud Sync 用户界面中提供了盒式支持预览功能。

Box 可以是多种类型的同步关系中的源或目标。 ["查看支持的同步关系列表"](#)。

创建日期设置

如果 SMB 服务器是源服务器，则可以使用名为 *Date Created* 的新同步关系设置来同步在特定日期之后，特定日期之前或在特定时间范围之间创建的文件。

["了解有关 Cloud Sync 设置的更多信息"](#)。

2021 年 10 月 4 日

额外的箱体支持

Cloud Sync 现在支持的其他同步关系 ["框中"](#) 使用 Cloud Sync API 时：

- Amazon S3 收箱
- IBM Cloud Object Storage to Box
- StorageGRID 到框
- NFS 服务器的复选框
- SMB 服务器

["了解如何使用 API 设置同步关系"](#)。

报告 SFTP 路径

您现在可以：["创建报告"](#) 用于 SFTP 路径。

2021 年 9 月 2 日

支持适用于 ONTAP 的 FSX

现在，您可以将数据同步到 Amazon FSX for ONTAP 文件系统或从 Amazon FSX 文件系统同步数据。

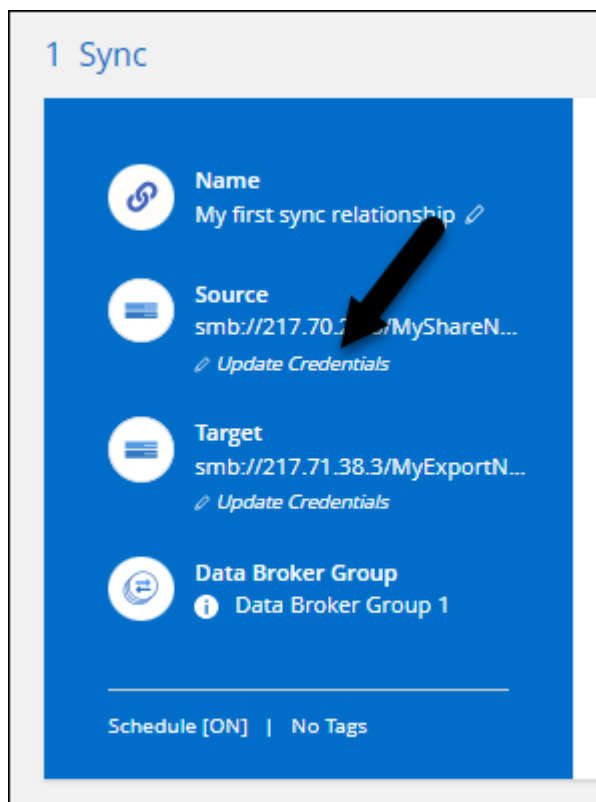
- ["了解适用于 ONTAP 的 Amazon FSX"](#)
- ["查看支持的同步关系"](#)
- ["了解如何为适用于 ONTAP 的 Amazon FSX 创建同步关系"](#)

2021 年 8 月 1 日

更新凭据

现在，您可以通过 Cloud Sync 使用现有同步关系中源或目标的最新凭据更新数据代理。

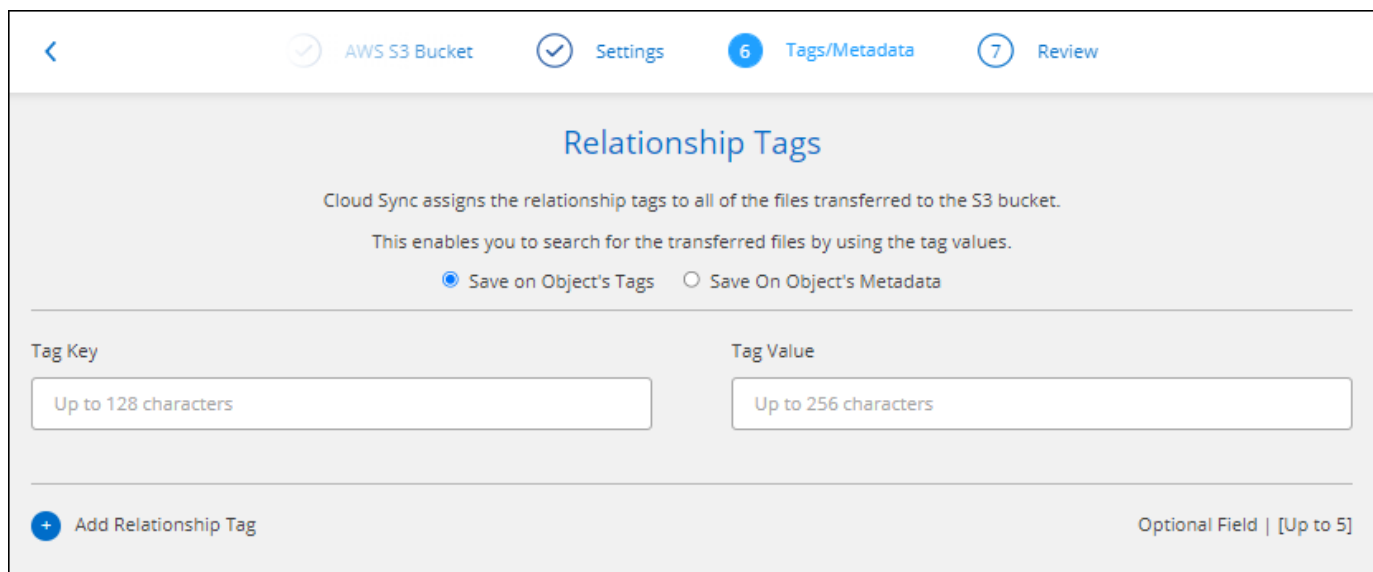
如果安全策略要求您定期更新凭据，此增强功能将很有帮助。 ["了解如何更新凭据"](#)。



对象存储目标的标记

现在，在创建同步关系时，您可以在同步关系中向对象存储目标添加标记。

Amazon S3， Azure Blob， Google Cloud Storage， IBM Cloud Object Storage 和 StorageGRID 支持添加标记。



支持 **Box**

Cloud Sync 现在支持 "框中" 在使用 Cloud Sync API 时，作为与 Amazon S3，StorageGRID 和 IBM 云对象存储的同步关系中的源。

["了解如何使用 API 设置同步关系"](#)。

用于 **Google Cloud** 中数据代理的公有 IP

在 Google Cloud 中部署数据代理时，您现在可以选择是为虚拟机实例启用还是禁用公有 IP 地址。

["了解如何在 Google Cloud 中部署数据代理"](#)。

适用于 **Azure NetApp Files** 的双协议卷

在为 Azure NetApp Files 选择源卷或目标卷时，无论您为同步关系选择哪种协议，Cloud Sync 现在都会显示双协议卷。

2021 年 7 月 7 日

ONTAP S3 存储和 Google 云存储

现在，Cloud Sync 支持通过用户界面在 ONTAP S3 存储和 Google 云存储分段之间建立同步关系。

["查看支持的同步关系列表"](#)。

对象元数据标记

现在，在创建同步关系并启用设置时，Cloud Sync 可以在基于对象的存储之间复制对象元数据和标记。

["了解有关 "复制对象" 设置的更多信息"](#)。

支持 **HashiCorp** 存储

现在，您可以通过使用 Google Cloud 服务帐户进行身份验证来设置数据代理，以便从外部 HashiCorp Vault 访问凭据。

["了解有关将 HashiCorp Vault 与数据代理结合使用的更多信息"](#)。

为 **S3** 存储分段定义标记或元数据

现在，在设置与 Amazon S3 存储分段的同步关系时，您可以通过同步关系向导定义要保存在目标 S3 存储分段中对象上的标记或元数据。

标记选项以前是同步关系设置的一部分。

2021 年 6 月 7 日

Google Cloud 中的存储类

如果 Google Cloud Storage 存储分段是同步关系中的目标，您现在可以选择要使用的存储类。Cloud Sync 支持

以下存储类：

- 标准
- 近线
- 冷线
- 归档

2021 年 5 月 2 日

报告中存在错误

现在，您可以查看在报告中发现的错误，并且可以删除上一个报告或所有报告。

["了解有关创建和查看报告以调整配置的更多信息"](#)。

比较属性

现在，每个同步关系都有一个新的 * 比较依据 * 设置。

通过此高级设置，您可以选择 Cloud Sync 在确定文件或目录是否已更改并应重新同步时是否应比较某些属性。

["了解有关更改同步关系设置的更多信息"](#)。

2021 年 4 月 11 日

独立 **Cloud Sync** 服务已停用

独立的 Cloud Sync 服务已停用。现在，您应直接从 Cloud Manager 访问 Cloud Sync，在 Cloud Manager 中，所有相同的特性和功能均可用。

登录到 Cloud Manager 后，您可以切换到顶部的 "同步" 选项卡并查看您的关系，就像以前一样。

Google Cloud 分段用于不同项目

在设置同步关系时，如果您为数据代理的服务帐户提供了所需的权限，则可以从不同项目中的 Google Cloud 存储分段中进行选择。

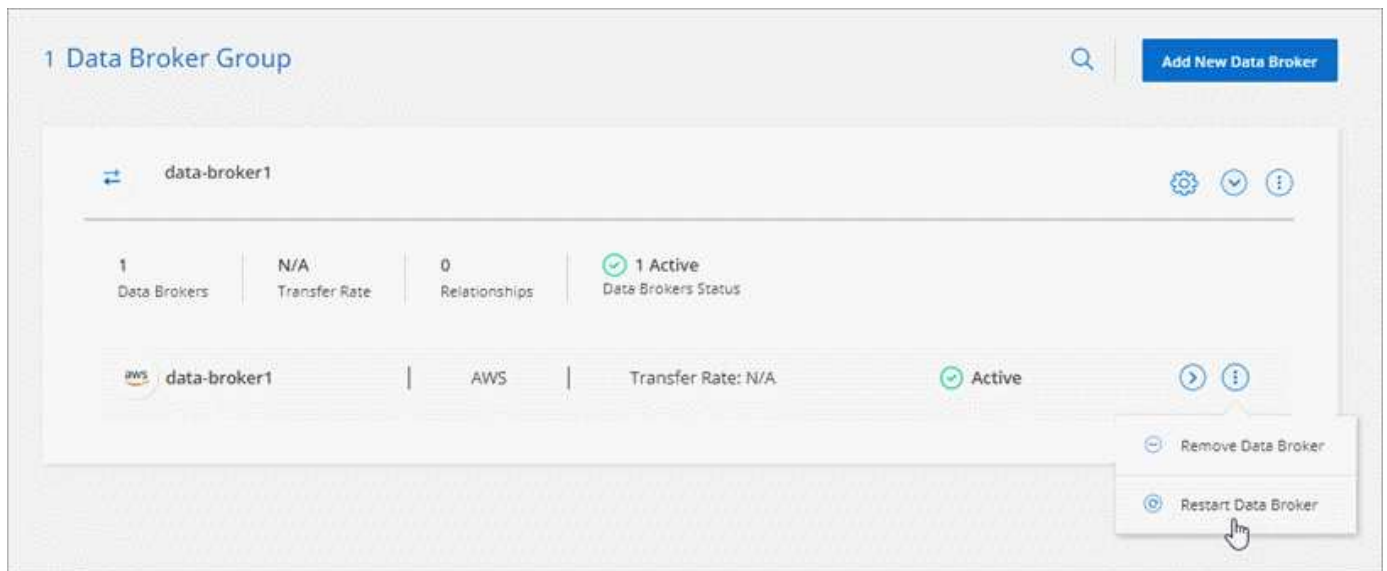
["了解如何设置服务帐户"](#)。

Google Cloud Storage 和 **S3** 之间的元数据

现在，Cloud Sync 可在 Google 云存储和 S3 提供程序（AWS S3，StorageGRID 和 IBM 云对象存储）之间复制元数据。

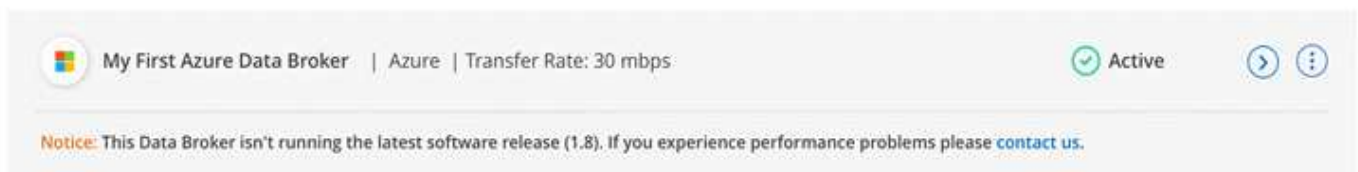
重新启动数据代理

现在，您可以从 Cloud Sync 重新启动数据代理。



未运行最新版本时的消息

现在， Cloud Sync 可以确定数据代理何时未运行最新软件版本。此消息有助于确保您获得最新的特性和功能。



限制

已知限制确定了本产品版本不支持的平台、设备或功能、或者这些平台、设备或功能无法与产品正确交互操作。仔细审查这些限制。

- 中国不支持云同步。
- 除中国外、以下地区不支持 Cloud Sync 数据代理：
 - Azure US gov 酒店
 - Azure US DoD

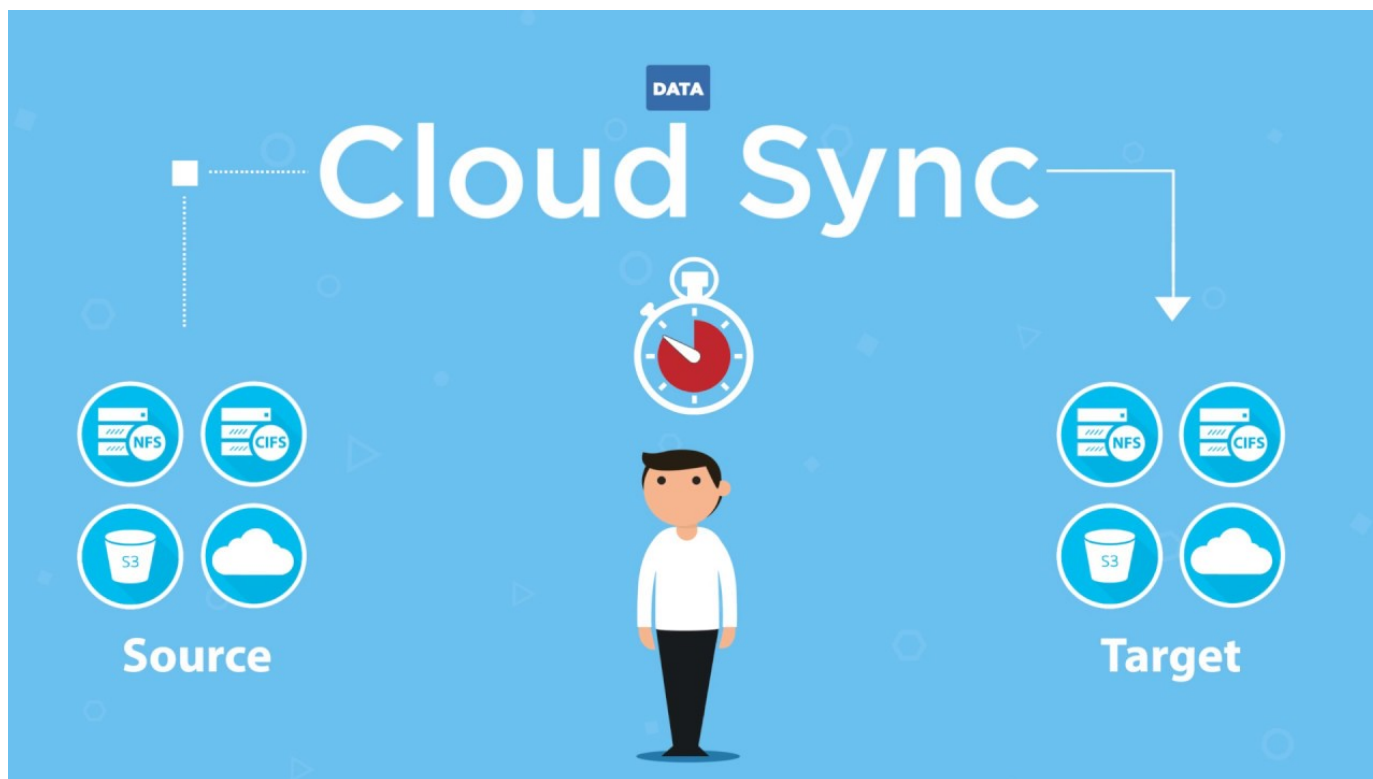
入门

Cloud Sync 概述

NetApp Cloud Sync 服务提供了一种简单、安全且自动化的方式、可以将数据迁移到云或您的企业内部的任何目标。无论是基于文件的 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、Cloud Sync 都可以为您转换和移动它。

功能

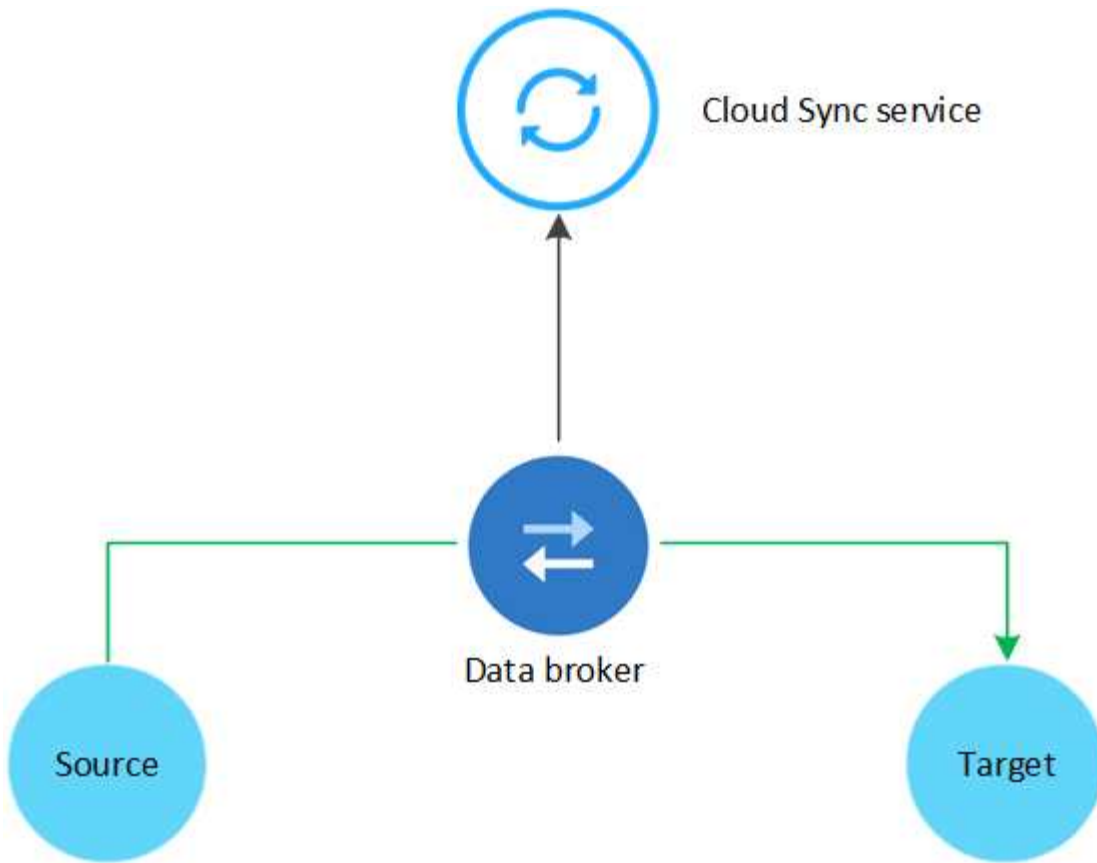
观看以下视频以了解 Cloud Sync 的概述：



Cloud Sync 的工作原理

Cloud Sync 是一个软件即服务（SaaS）平台，由一个数据代理组，一个通过 Cloud Manager 提供的基于云的界面以及一个源和目标组成。

下图显示了 Cloud Sync 组件之间的关系：



NetApp 数据代理软件会将数据从源同步到目标（称为 *sync relationship*）。您可以在 AWS、Azure、Google Cloud 平台或内部运行数据代理。一个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 Internet 连接，以便能够与 Cloud Sync 服务进行通信并联系其他一些服务和存储库。["查看端点列表。"](#)

初始副本之后、服务将根据您设置的计划同步所有更改的数据。

支持的存储类型

Cloud Sync 支持以下存储类型：

- 任何 NFS 服务器
- 任何 SMB 服务器
- Amazon EFS
- 适用于 ONTAP 的 Amazon FSX
- Amazon S3
- Azure Blob
- Azure NetApp Files
- 框（可作为预览版使用）
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud 存储
- IBM 云对象存储

- 内部 ONTAP 集群
- ONTAP S3 存储
- SFTP （仅使用 API ）
- StorageGRID

["查看支持的同步关系"](#)。

Costs

使用 Cloud Sync 会产生两种成本：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。

服务费用

在 14 天免费试用结束后、有两种方式可以支付同步关系的费用。第一种选择是从 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"](#)。

Cloud Sync 快速入门

Cloud Sync 服务入门包括几个步骤。

验证您的源和目标是否受支持和设置。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"](#)

NetApp 数据代理软件会将数据从源同步到目标（称为 *sync relationship*）。您可以在 AWS、Azure、Google Cloud 平台或内部运行数据代理。一个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 Internet 连接，以便能够与 Cloud Sync 服务进行通信并联系其他一些服务和存储库。["查看端点列表。"](#)

在创建同步关系时，Cloud 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自己的 Linux 主机下载安装脚本。

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

登录到 ["云管理器"](#)，单击 * 同步 *，然后拖放您为源和目标选择的内容。按照提示完成设置。["了解更多信息。"](#)

从 AWS 或 Azure 订阅以按需购买或每年支付。或直接从 NetApp 购买许可证。只需转到 Cloud Sync 中的“许可证设置”页面即可进行设置。["了解更多信息。"](#)

支持的同步关系

使用 Cloud Sync 可以将数据从源同步到目标。这称为同步关系。您应该先了解支持的关系，然后再开始。

源位置	支持的目标位置
Amazon EFS	<ul style="list-style-type: none">• Amazon EFS• 适用于 ONTAP 的 Amazon FSX• Amazon S3• Azure Blob• Azure NetApp Files• Cloud Volumes ONTAP• Cloud Volumes Service• Google Cloud 存储• IBM 云对象存储• NFS 服务器• 内部 ONTAP 集群• SMB 服务器• StorageGRID
适用于 ONTAP 的 Amazon FSX	<ul style="list-style-type: none">• Amazon EFS• 适用于 ONTAP 的 Amazon FSX• Amazon S3• Azure Blob• Azure NetApp Files• Cloud Volumes ONTAP• Cloud Volumes Service• Google Cloud 存储• IBM 云对象存储• NFS 服务器• 内部 ONTAP 集群• SMB 服务器• StorageGRID

源位置	支持的目标位置
Amazon S3	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • 盒装 ^2 , 3^ • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID
Azure Blob	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID

源位置	支持的目标位置
Azure NetApp Files	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID
盒 ²	<ul style="list-style-type: none"> • Amazon S3 • IBM 云对象存储 • NFS 服务器 • SMB 服务器 • StorageGRID
Cloud Volumes ONTAP	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID

源位置	支持的目标位置
Cloud Volumes Service	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID
Google Cloud 存储	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • ONTAP S3 存储 • SMB 服务器 • StorageGRID

源位置	支持的目标位置
IBM 云对象存储	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • 盒装 ^2 , 3^ • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID
NFS 服务器	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID

源位置	支持的目标位置
内部 ONTAP 集群	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • SMB 服务器 • StorageGRID
ONTAP S3 存储	<ul style="list-style-type: none"> • Google Cloud 存储 • SMB 服务器 • StorageGRID • ONTAP S3 存储
SFTP ¹	S3
SMB 服务器	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • ONTAP S3 存储 • SMB 服务器 • StorageGRID

源位置	支持的目标位置
StorageGRID	<ul style="list-style-type: none"> • Amazon EFS • 适用于 ONTAP 的 Amazon FSX • Amazon S3 • Azure Blob • Azure NetApp Files • 盒装 ^2 , 3^ • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud 存储 • IBM 云对象存储 • NFS 服务器 • 内部 ONTAP 集群 • ONTAP S3 存储 • SMB 服务器 • StorageGRID

注释：

1. 仅使用 Cloud Sync API 支持与此源 / 目标的同步关系。
2. 预览版可提供盒式支持。
3. 当 BLOB 容器是目标容器时，可以选择特定的 Azure Blob 存储层：
 - 热存储
 - 冷却存储
4. **【存储类】** 当 Amazon S3 为目标时，您可以选择特定的 S3 存储类：
 - 标准（这是默认类）
 - Intelligent-Hierarchy
 - 标准—不经常访问
 - 一个 ZONE 不常访问
 - 冰河
 - Glacier 深度存档
5. 当 Google Cloud Storage 存储分段为目标时，您可以选择特定的存储类：
 - 标准
 - 近线
 - 冷线

- 归档

准备源和目标

验证源和目标是否满足以下要求。

网络

- 源和目标必须与数据代理组建立网络连接。

例如，如果数据中心中有 NFS 服务器，而 AWS 中有数据代理，则需要从网络到 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

创建同步关系时，您可以使用 Cloud Sync 选择现有目标目录，然后选择在该目录中创建一个新文件夹。因此，请确保您的首选目标目录已存在。

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，Cloud Sync 需要对目录或文件夹具有读取权限。

NFS

必须使用文件和目录上的 uid/GID 在源 / 目标上定义权限。

对象存储

- 对于 AWS 和 Google Cloud，数据代理必须具有列表对象权限（如果您按照数据代理安装步骤进行操作，则默认情况下会提供这些权限）。
- 对于 Azure，StorageGRID 和 IBM，您在设置同步关系时输入的凭据必须具有列表对象权限。

SMB

设置同步关系时输入的 SMB 凭据必须具有列表文件夹权限。



默认情况下，数据代理会忽略以下目录：.snapshot，~snapshot，.copy-of-overt

Amazon S3 存储分段要求

确保您的 Amazon S3 存储分段满足以下要求。

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 或您的内部部署数据代理。在这两种情况下、Cloud Sync 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。

在其他 **AWS** 帐户中 **S3** 数据段所需的权限

在设置同步关系时，您可以指定一个 S3 存储分段，该存储分段驻留在与数据代理不关联的 AWS 帐户中。

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


请注意以下有关 JSON 文件中包含的权限的信息：

1. `<BucketName>` 是位于 AWS 帐户中且与数据代理无关的存储分段名称。
2. 应将 `<RoleARN>` 替换为以下项之一：
 - 如果在 Linux 主机上手动安装了数据代理，则 `RoleARN` 应是部署数据代理时为其提供 AWS 凭据的 AWS 用户的 ARN。
 - 如果使用 CloudFormation 模板在 AWS 中部署了数据代理，则 `RoleARN` 应是此模板创建的 IAM 角色的 ARN。

您可以通过转至 EC2 控制台、选择数据代理实例并从“描述”选项卡中单击 IAM 角色来查找角色 ARN。然后，应在 IAM 控制台中查看包含角色 ARN 的“摘要”页面。

Summary

Delete role

Role ARN `arn:aws:iam::142581783291:role/tanyaBroker0304-DataBrokerIamRole-1VMHWXMW3AQ05` 

Role description [Edit](#)

Azure Blob 存储要求

确保 Azure Blob 存储满足以下要求。

Azure Blob 支持的数据代理位置

如果同步关系包括 Azure Blob 存储，则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，需要使用存储帐户连接字符串提供 Cloud Sync：

a63cde60b553020 - Access keys

Storage account

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Storage Explorer (preview)

Settings

Access keys
CORS
Configuration
Encryption

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）。在 blob 容器和 NFS 或 SMB 服务器之间同步时，您还可以选择使用 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 还必须包括以下权限：

- 对于源 blob 容器：读取并列出
- 对于目标 BLOB 容器：读取、写入、列出、添加和创建

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

Azure NetApp Files 要求

在与 Azure NetApp Files 同步数据时，请使用高级或超高级服务级别。如果磁盘服务级别为标准，则可能会出现故障和性能问题。



如果您需要帮助确定合适的服务级别，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"。](#)

包装箱要求

- 要创建包含框的同步关系，您需要提供以下凭据：
 - 客户端 ID
 - 客户端密钥
 - 专用密钥。
 - 公有密钥 ID
 - 密码短语

- 企业 ID
- 如果要创建从 Amazon S3 到 Box 的同步关系，则必须使用具有统一配置且以下设置设置为 1 的数据代理组：
 - 扫描程序并发
 - 扫描程序进程限制
 - 传输并发性
 - 传输程序进程限制

["了解如何为数据代理组定义统一配置"](#)。

Google Cloud 存储桶要求

确保 Google Cloud 存储桶满足以下要求。

Google Cloud 存储支持的数据代理位置

包含 Google Cloud Storage 的同步关系要求在 Google Cloud 或内部部署一个数据代理。在创建同步关系时，Cloud Sync 将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 地区

支持所有区域。

其他 Google Cloud 项目中的存储分段的权限

在设置同步关系时，如果您为数据代理的服务帐户提供了所需的权限，则可以从不同项目中的 Google Cloud 存储分段中进行选择。 ["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 / 列表" 权限足以将数据从源同步到目标。

NFS 服务器要求

- NFS 服务器可以是 NetApp 系统或非 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 NFS 导出列表的访问（已启用 `vserver nfs modify -vserver svm_name -showmount`）。



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 或内部 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。复制 ACL 时需要执行此操作。

ONTAP S3 存储要求

设置包括的同步关系时 "[ONTAP S3 存储](#)"，您需要提供以下内容：

- 连接到 ONTAP S3 的 LIF 的 IP 地址
- ONTAP 配置为使用的访问密钥和机密密钥

SMB 服务器要求

- SMB 服务器可以是 NetApp 系统或非 NetApp 系统。
- 您需要为 Cloud Sync 提供对 SMB 服务器具有权限的凭据。
 - 对于源 SMB 服务器，需要以下权限：`list` 和 `read`。

源 SMB 服务器支持备份操作员组的成员。

 - 对于目标 SMB 服务器，需要以下权限：`list`，`read` 和 `write`。
- 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。
- 向 "管理员" 组授予对源文件夹和目标文件夹的 "完全控制" 权限。

如果不授予此权限，则数据代理可能没有足够的权限来获取文件或目录上的 ACL。如果发生这种情况，您将收到以下错误：`"getxattr error 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 限制会影响隐藏的目录和文件。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。

由于大小写不敏感限制而导致的 SMB 同步行为

SMB 协议不区分大小写，这意味着大小写字母将被视为相同。如果同步关系包含 SMB 服务器且目标上已存在数据，则此行为可能会导致文件被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 Cloud Sync 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 Cloud Sync 尝试将名为 "b" 的目录复制到目标时，Cloud Sync 会收到一条错误，指出此目录已存在。因此，Cloud Sync 始终无法复制名为 "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。

Cloud Sync 网络概述

Cloud Sync 网络包括数据代理组与源位置和目标位置之间的连接，以及数据代理通过端口 443 的出站 Internet 连接。

数据代理位置

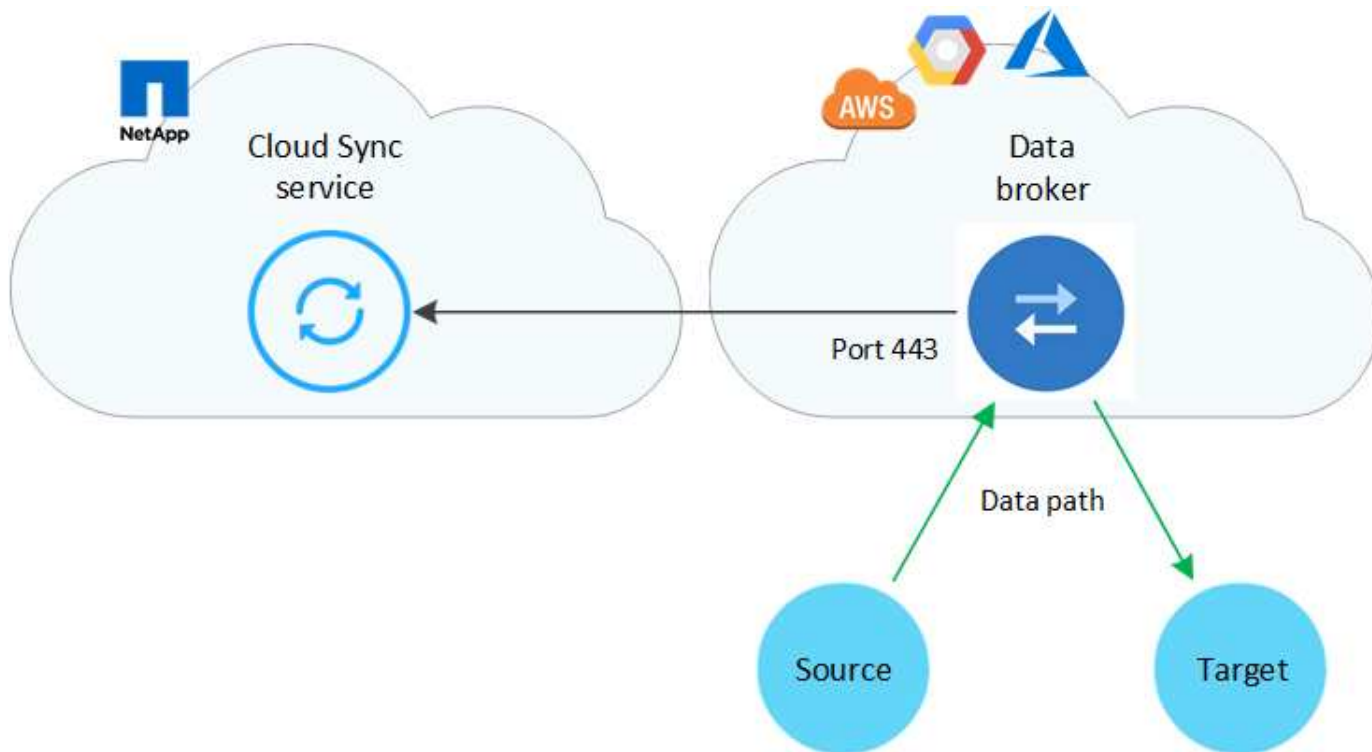
数据代理组由一个或多个安装在云或内部的数据代理组成。

云中的数据代理

下图显示了在云中运行的数据代理，该代理可以在 AWS，Google Cloud 或 Azure 中运行。只要与数据代理建立连接，源和目标就可以位于任何位置。例如，您可能会从数据中心连接到云提供商。

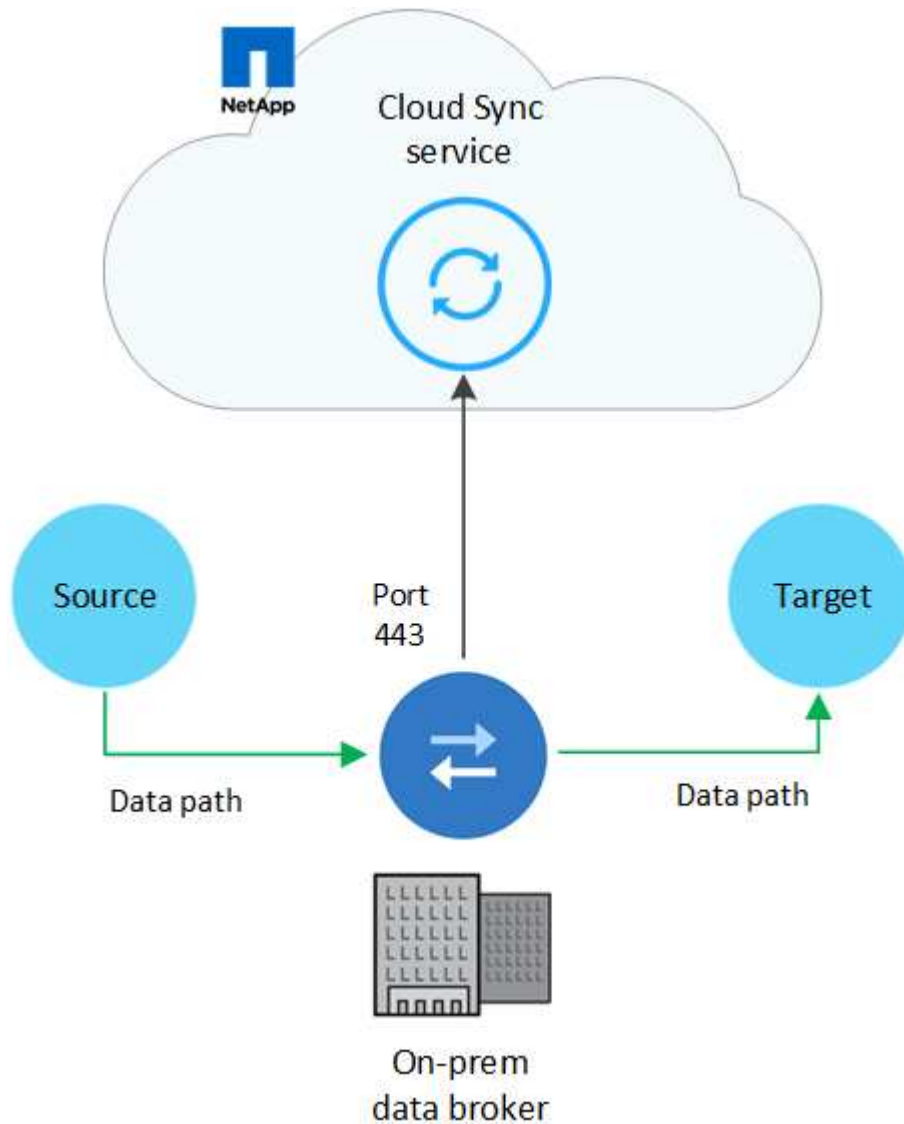


当 Cloud Sync 在 AWS，Azure 或 Google Cloud 中部署数据代理时，它会创建一个安全组来实现所需的出站通信。



数据代理

下图显示了在数据中心内运行在 Prem 上的数据代理。同样，只要与数据代理建立连接，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建立网络连接。

例如，如果数据中心中有 NFS 服务器，而 AWS 中有数据代理，则需要从网络到 VPC 的网络连接（VPN 或 Direct Connect）。

- 数据代理需要出站 Internet 连接，以便可以通过端口 443 轮询 Cloud Sync 服务以查找任务。
- 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 Internet 访问、以便与 Cloud Sync 服务进行通信、并与其他一些服务和存储库联系。您的本地 Web 浏览器还需要访问端点才能执行某些操作。如果需要限制出站连接、请在为出站通信配置防火墙时参考以下端点列表。

数据代理端点

数据代理会联系以下端点：

端点	目的
https://olcentgbl.trafficmanager.net	可与存储库联系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。
https://rpm.nodesource.com https://registry.npmjs.org https://nodejs.org :	与存储库联系以更新节点 .js 、 NPM 和开发中使用的其他第三方软件包。
https://tgz.pm2.io	访问用于更新 PM2 的存储库、该存储库是用于监控云同步的第三方软件包。
https://sqs.us-east-1.amazonaws.com https://kinesis.us-east-1.amazonaws.com	联系 Cloud Sync 用于操作的 AWS 服务（对文件进行排队、注册操作以及向数据代理提供更新）。
https://s3.region.amazonaws.com ， 例如： s3.us-east-2.amazonaws.com:443 https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region ["有关 S3 端点的列表，请参见 AWS 文档"]	在同步关系包括 S3 存储区时联系 Amazon S3 。
https://s3.us-east-1.amazonaws.com	从 Cloud Sync 下载数据代理日志时，数据代理会将其日志目录置于 Z 形结构中，并将日志上传到 us-east-1 区域的预定义 S3 存储分段。
https://cf.cloudsync.netapp.com https://repo.cloudsync.netapp.com	可与 Cloud Sync 服务联系。
https://support.netapp.com	在使用 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 才能向 NetApp 技术支持发送 AutoSupport 消息。
https://sts.amazonaws.com	在 AWS 中部署数据代理或在内部部署数据代理时验证 AWS 凭据，并提供 AWS 凭据。数据代理会在部署期间，更新时以及重新启动时联系此端点。
https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	在使用 Data sense 为新同步关系选择源文件时联系 Cloud Data sense 。

Web 浏览器端点

您的 Web 浏览器需要访问以下端点才能下载日志以进行故障排除：

logs.cloudsync.netapp.com:443

安装数据代理

在 AWS 中创建新的数据代理

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。Cloud Sync 可指导您完成安装过程、但本页中重复了这些要求和步骤以帮助您做好安装准备。

您还可以选择在云中的现有 Linux 主机或您的企业中安装数据代理。["了解更多信息。"](#)

支持的 AWS 区域

除中国地区外，所有地区均受支持。

网络要求

- 数据代理需要出站 Internet 连接、因此可以通过端口 443 轮询 Cloud Sync 服务以了解任务。

当 Cloud 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将数据代理配置为使用代理服务器。

如果需要限制出站连接，请参见 ["数据代理所联系的端点的列表"](#)。

- NetApp 建议将源、目标和数据代理配置为使用网络时间协议（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 用户帐户必须具有中包含的权限 ["此 NetApp 提供的策略"](#)。

在 AWS 数据代理中使用您自己的 IAM 角色的要求

当 Cloud Sync 部署数据代理时、它会为数据代理实例创建 IAM 角色。如果您愿意，可以使用自己的 IAM 角色部署数据代理。如果您的组织具有严格的安全策略，则可以使用此选项。

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。

在部署数据代理时，请按照以下步骤指定 IAM 角色。

创建数据代理

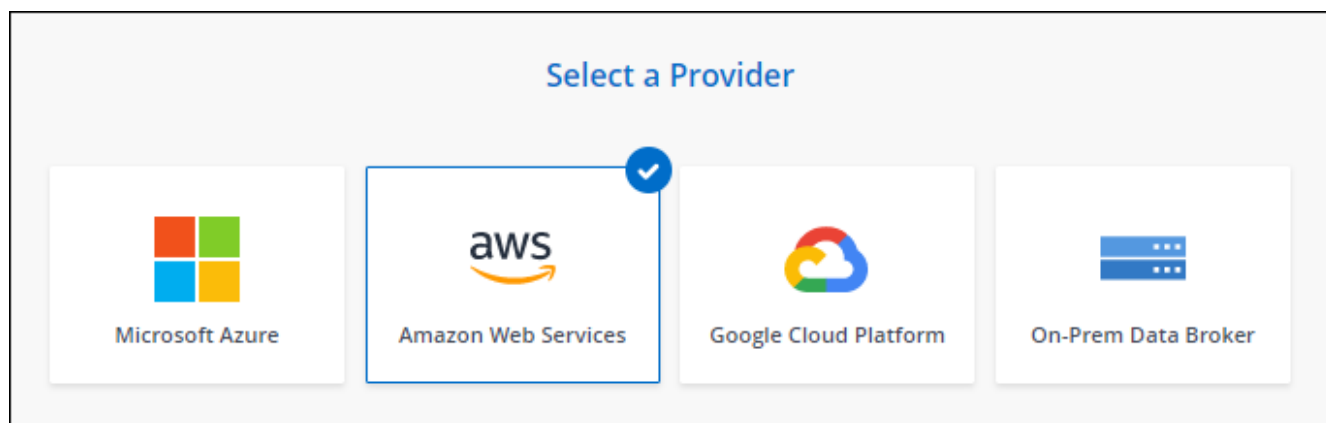
可以通过几种方法创建新的数据代理。以下步骤介绍如何在创建同步关系时在 AWS 中安装数据代理。

步骤

1. 单击 * 创建新同步 *。
2. 在 * 定义同步关系 * 页面上，选择一个源和目标，然后单击 * 继续 *。

完成这些步骤，直到显示 * 数据代理组 * 页面为止。

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



4. 输入数据代理的名称，然后单击 * 继续 *。
5. 输入 AWS 访问密钥，以便 Cloud Sync 可以代表您在 AWS 中创建数据代理。

这些密钥不会保存或用于任何其他目的。

如果您不想提供访问密钥，请单击页面底部的链接以改用 CloudFormation 模板。使用此选项时，您无需提供凭据，因为您直接登录到 AWS。

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

► https://docs.netapp.com/zh-cn/cloud-manager-sync//media/video_cloud_sync.mp4 (video)

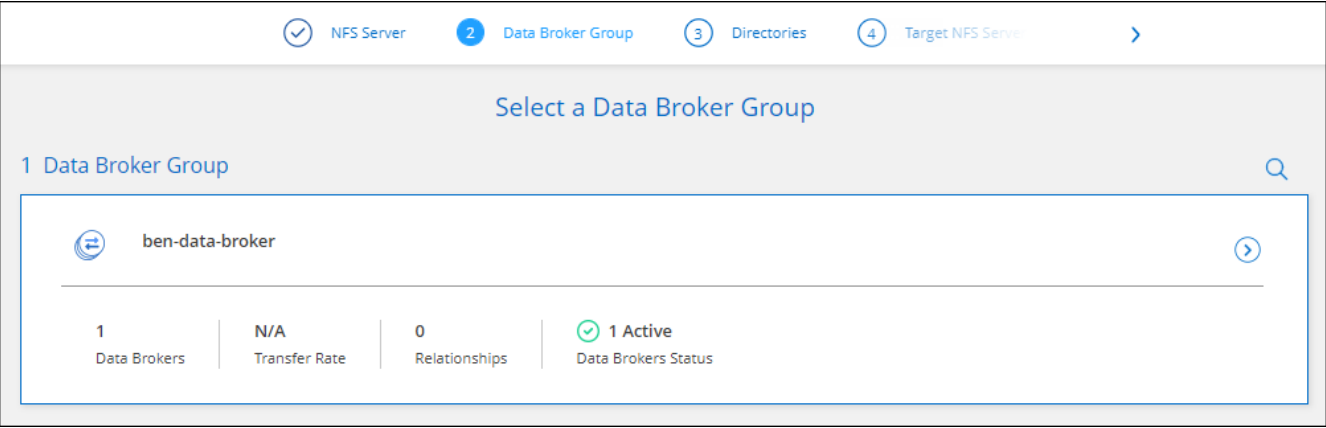
6. 如果您输入了 AWS 访问密钥，请为实例选择一个位置，选择一个密钥对，选择是否启用公有 IP 地址，然后选择现有的 IAM 角色，或者将此字段留空，以便 Cloud Sync 为您创建角色。

如果您选择自己的 IAM 角色， [您需要提供所需的权限](#)。

The image shows a 'Basic Settings' form with two main sections. The 'Location' section on the left includes dropdown menus for 'Region' (set to 'US West | Oregon'), 'VPC' (set to 'vpc-3c46c059 - 10.60.21.0/25'), and 'Subnet' (set to '10.60.21.0/25'). The 'Connectivity' section on the right includes a 'Key Pair' dropdown (set to 'newKey'), a radio button group for 'Enable Public IP?' (with 'Enable' selected), and an 'IAM Role (optional)' text input field with an information icon.

- 7. 如果 VPC 中的 Internet 访问需要代理，请指定代理配置。
- 8. 数据代理可用后，单击 Cloud Sync 中的 * 继续 * 。

下图显示了 AWS 中已成功部署的实例：



- 9. 完成向导中的页面以创建新的同步关系。

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结合使用。

有关数据代理实例的详细信息

Cloud Sync 使用以下配置在 AWS 中创建数据代理。

Instance type

m5n.xlarge （如果在区域中可用），否则为 m5.xlarge

vCPU

4.

RAM

16 GB

操作系统

Amazon Linux 2.

磁盘大小和类型

10 GB GP2 SSD

在 **Azure** 中创建新的数据代理

创建新的数据代理组时，请选择 Microsoft Azure 以在 vNet 中的新虚拟机上部署数据代理软件。Cloud Sync 可指导您完成安装过程、但本页中重复了这些要求和步骤以帮助您做好安装准备。

您还可以选择在云中的现有 Linux 主机或您的企业中安装数据代理。"了解更多信息。"。

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。

网络要求

- 数据代理需要出站 Internet 连接、因此可以通过端口 443 轮询 Cloud Sync 服务以了解任务。

当 Cloud 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，请参见 ["数据代理所联系的端点的列表"](#)。

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

身份验证方法

部署数据代理时，您需要选择一种身份验证方法：密码或 SSH 公共 - 私有密钥对。

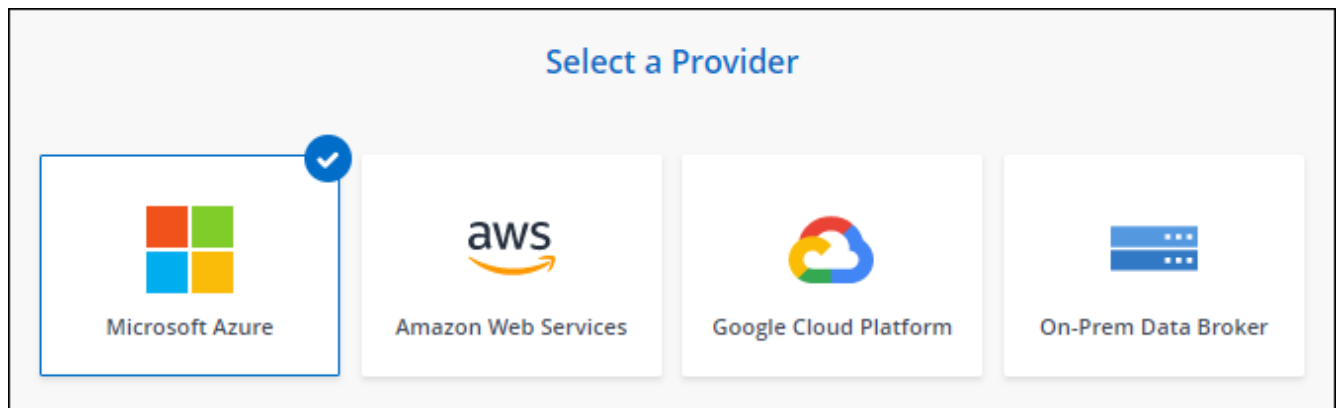
有关创建密钥对的帮助，请参见 ["Azure 文档：在 Azure 中为 Linux VM 创建和使用 SSH 公共 - 私有密钥对"](#)。

创建数据代理

可以通过几种方法创建新的数据代理。以下步骤介绍如何在创建同步关系时在 Azure 中安装数据代理。

步骤

1. 单击 * 创建新同步 *。
 2. 在 * 定义同步关系 * 页面上，选择一个源和目标，然后单击 * 继续 *。
- 完成这些步骤，直到显示 * 数据代理组 * 页面为止。
3. 在 * 数据代理组 * 页面上，单击 * 创建数据代理 *，然后选择 * Microsoft Azure*。



4. 输入数据代理的名称，然后单击 * 继续 *。
5. 如果出现提示，请登录到您的 Microsoft 帐户。如果未出现提示，请单击 * 登录到 Azure*。

此表由 Microsoft 拥有和托管。您的凭据不会提供给 NetApp。

6. 为数据代理选择一个位置，然后输入有关虚拟机的基本详细信息。

The screenshot shows the Azure portal configuration page for a Virtual Machine. The page is divided into two main sections: **Location** and **Virtual Machine**.

Location Section:

- Subscription:** OCCM Dev
- Azure Region:** West US 2
- VNet:** Vnet1
- Subnet:** Subnet1

Virtual Machine Section:

- VM Name:** netappdatabroker
- User Name:** databroker
- Authentication Method:**
 - ☒ Password
 - ☐ Public Key
- Enter Password:** (masked with dots)
- Resource Group:**
 - ☒ Generate a new group
 - ☐ Use an existing group

7. 如果在 vNet 中需要代理才能访问 Internet，请指定代理配置。

8. 单击 * 继续 * 并保持此页面打开，直到部署完成。

此过程可能需要长达 7 分钟。

9. 在 Cloud Sync 中，一旦数据代理可用，请单击 * 继续 *。

10. 完成向导中的页面以创建新的同步关系。

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。

是否收到有关需要管理员同意的消息？

如果 Microsoft 通知您需要管理员批准，因为 Cloud Sync 需要您的权限来代表您访问您组织中的资源，则您有两种选择：

1. 请您的 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其访问公司数据 *。

2. 请您的 AD 管理员使用以下 URL 代表您同意使用 * CloudSync-AzureDataBrokerCreator*（这是管理员同意的端点）：

[https://login.microsoftonline.com/{FILL 此处为您的租户 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/{FILL 此处为您的租户 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 中所示，我们的应用程序 URL 为 <https://cloudsync.netapp.com>，应用程序客户端 ID 为 8ee4ca3a-BAFA-4831-97CC-5a38923cab85。

有关数据代理 VM 的详细信息

Cloud Sync 使用以下配置在 Azure 中创建数据代理。

VM 类型

标准 DS4 v2

vCPU

8.

RAM

28 GB

操作系统

CentOS 7.7

磁盘大小和类型

64 GB 高级 SSD

在 Google Cloud 中创建新的数据代理

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。Cloud Sync 可指导您完成安装过程、但本页中重复了这些要求和步骤以帮助您做好安装准备。

您还可以选择在云中的现有 Linux 主机或您的企业中安装数据代理。 [了解更多信息。](#)

支持的 Google Cloud 地区

支持所有区域。

网络要求

- 数据代理需要出站 Internet 连接、因此可以通过端口 443 轮询 Cloud Sync 服务以了解任务。

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

如果需要限制出站连接，请参见 ["数据代理所联系的端点的列表"](#)。

- NetApp 建议将源、目标和数据代理配置为使用网络时间协议（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.*
- iam.serviceAccounts.signJwt
```



只有在计划设置数据代理以使用外部 HashiCorp 存储时，才需要 iam.serviceAccounts.signJwt" 权限。

创建数据代理

可以通过几种方法创建新的数据代理。以下步骤介绍如何在创建同步关系时在 Google Cloud 中安装数据代理。

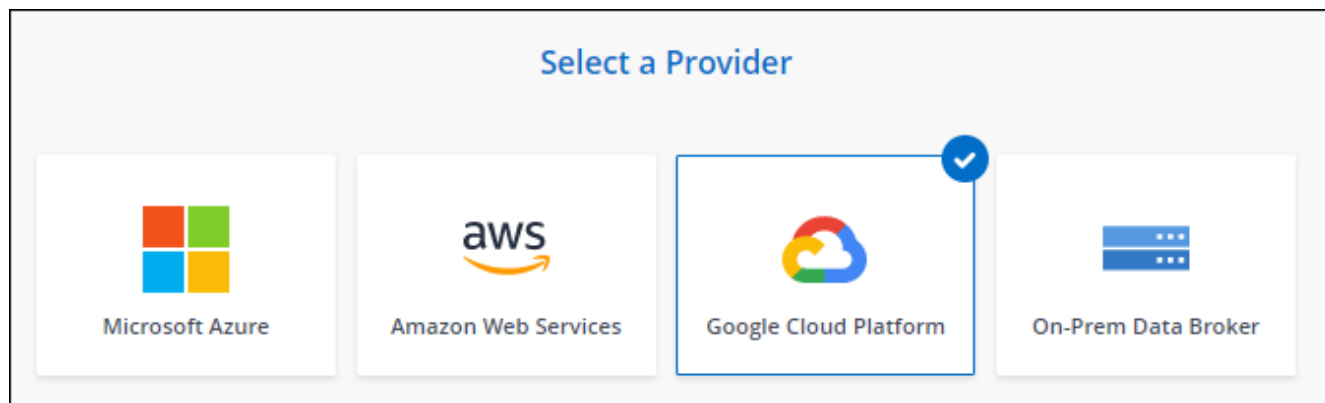
步骤

1. 单击 * 创建新同步 *。

2. 在 * 定义同步关系 * 页面上，选择一个源和目标，然后单击 * 继续 * 。

完成这些步骤，直到显示 * 数据代理组 * 页面为止。

3. 在 * 数据代理组 * 页面上，单击 * 创建数据代理 * ，然后选择 * Microsoft Azure* 。



4. 输入数据代理的名称，然后单击 * 继续 * 。

5. 如果出现提示，请使用 Google 帐户登录。

此表由 Google 拥有和托管。您的凭据不会提供给 NetApp 。

6. 选择项目和服务帐户，然后为数据代理选择一个位置，包括是否要启用或禁用公有 IP 地址。

如果不启用公有 IP 地址，则需要在下一步中定义代理服务器。

Basic Settings

Project

Project

OCCM-Dev

Location

Region

us-west1

Service Account

test

Zone

us-west1-a

Select a Service Account that includes [these permissions](#)

VPC

default

Subnet

default

Public IP

Enable

7. 如果 VPC 中的 Internet 访问需要代理，请指定代理配置。

如果需要代理才能访问 Internet ，则该代理必须位于 Google Cloud 中，并使用与数据代理相同的服务帐户。

8. 数据代理可用后，单击 Cloud Sync 中的 * 继续 * 。

部署该实例大约需要 5 到 10 分钟。您可以从 Cloud Sync 服务监控进度、该服务在实例可用时自动刷新。

9. 完成向导中的页面以创建新的同步关系。

您已在 Google Cloud 中部署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** 项目中使用存储分段的权限

在创建同步关系并选择 Google Cloud Storage 作为源或目标时，您可以通过 Cloud Sync 从数据代理的服务帐户有权使用的分段中进行选择。默认情况下，此值包括与数据代理服务帐户位于 *same* 项目中的分段。但是，如果您提供了所需的权限，则可以从 *_other* 项目中选择分段。

步骤

1. 打开 Google Cloud Platform 控制台并加载云存储服务。
2. 单击要在同步关系中用作源或目标的存储分段的名称。
3. 单击 * 权限 * 。

4. 单击 * 添加 *。
5. 输入数据代理的服务帐户的名称。
6. 选择提供的角色 [与上述权限相同](#)。
7. 单击 * 保存 *。

设置同步关系时，您现在可以选择该存储分段作为同步关系中的源或目标。

有关数据代理 **VM** 实例的详细信息

Cloud Sync 使用以下配置在 Google Cloud 中创建数据代理。

计算机类型

N1-standard-4

vCPU

4.

RAM

15 GB

操作系统

Red Hat Enterprise Linux 7.7

磁盘大小和类型

标准配置 20 GB HDD PD

在 Linux 主机上安装数据代理

创建新的数据代理组时，请选择 On-Prem Data Broker 选项，以便在内部 Linux 主机或云中的现有 Linux 主机上安装数据代理软件。Cloud Sync 可指导您完成安装过程、但本页中重复了这些要求和步骤以帮助您做好安装准备。

Linux 主机要求

- * 操作系统 * :
 - CentOS 7.0 , 7.7 和 8.0
 - 不支持 CentOS 流。
 - Red Hat Enterprise Linux 7.7 和 8.0
 - Ubuntu Server 20.04 LTS
 - SUSE Linux Enterprise Server 15 SP1

安装数据代理之前，必须在主机上运行命令 `yum update all`。

Red Hat Enterprise Linux 系统必须在 Red Hat 订购管理中注册。如果未注册、系统将无法在安装期间访问存储库以更新所需的第三方软件。

- * RAM * : 16 GB
- * CPU * : 4 个核心
- * 可用磁盘空间 * : 10 GB
- * SELinux* : 建议您禁用 "SELinux" 在主机上。

SELinux 会强制实施一种策略，该策略会阻止数据代理软件更新，并阻止数据代理与正常运行所需的端点联系。

网络要求

- Linux 主机必须与源主机和目标主机建立连接。
- 文件服务器必须允许 Linux 主机访问导出。
- 必须在 Linux 主机上打开端口 443，以便向 AWS 发送出站流量（数据代理会不断与 Amazon SQS 服务进行通信）。
- NetApp 建议将源、目标和数据代理配置为使用网络时间协议（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 存储分段的同步关系中的数据代理，则应准备 Linux 主机以进行 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 "[此 NetApp 提供的策略](#)"

["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这些密钥。

启用对 **Google Cloud** 的访问

如果您计划将数据代理与包含 Google Cloud 存储分段的同步关系结合使用，则应准备 Linux 主机以进行 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一个密钥。

步骤

1. 如果您还没有存储管理员权限，请创建一个 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"](#)

此文件应至少包含以下属性："project_id"，"private_key" 和 "client_email"



创建密钥时、文件将生成并下载到计算机中。

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，可以按关系定义对 Azure 的访问。

安装数据代理

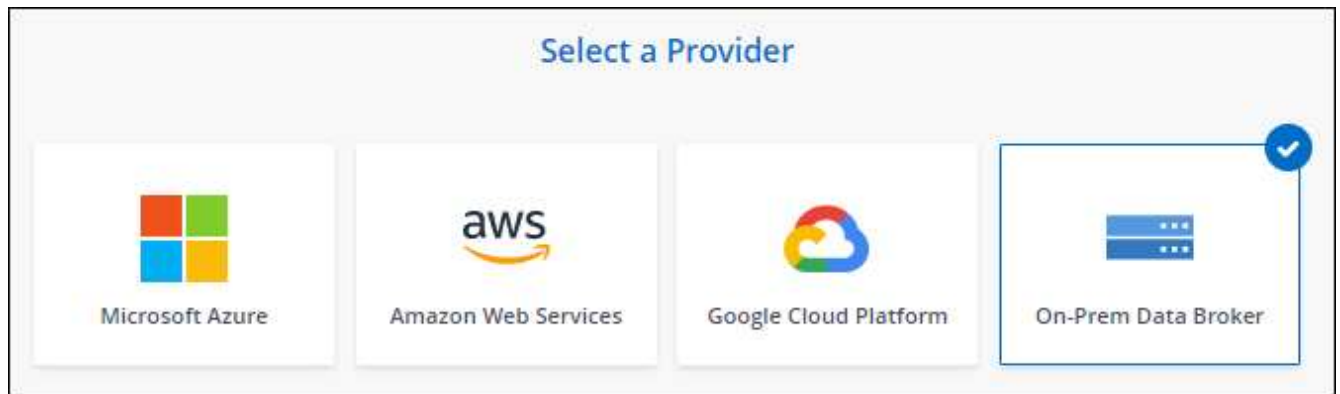
您可以在创建同步关系时在 Linux 主机上安装数据代理。

步骤

1. 单击 * 创建新同步 *。
2. 在 * 定义同步关系 * 页面上，选择一个源和目标，然后单击 * 继续 *。

完成这些步骤，直到显示 * 数据代理组 * 页面为止。

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



即使此选项标记为 * ; on-Prem_ Data Broker*，它也会对内部或云中的 Linux 主机进行适用场景。

4. 输入数据代理的名称，然后单击 * 继续 *。

此时将很快加载说明页面。您需要按照这些说明进行操作，其中包括一个用于下载安装程序的唯一链接。

5. 在说明页面上：
 - a. 选择是启用对 * AWS *，* Google Cloud* 的访问，还是同时启用这两者的访问。
 - b. 选择一个安装选项：* 无代理 *，* 使用代理服务器 * 或 * 使用代理服务器进行身份验证 *。
 - 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确切的命令。

- 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>
```

- 使用具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

Cloud Sync 会在说明页面上显示安装文件的 URI，在按照提示部署内部数据代理时会加载此 URI。此 URI 不会在此重复，因为此链接是动态生成的，只能使用一次。 [按照以下步骤从 Cloud Sync 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确切的命令。

- 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 <abasal_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 <abasal_path_to_the_json_file> -h  
<proxy_host> -p <proxy_port>
```

- 具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 <abasal_path_to_the_json_file> -h  
<proxy_host> -p <proxy_port> -u <proxy_username> -w <proxy_password>
```

AWS 密钥

这些是您应准备好的用户密钥 [请按照以下步骤操作](#)。AWS 密钥存储在数据代理上，该代理在内部或云网络中运行。NetApp 不会在数据代理之外使用密钥。

JSON 文件

此 JSON 文件包含您应已准备好的服务帐户密钥 [请按照以下步骤操作](#)。

6. 数据代理可用后，单击 Cloud Sync 中的 * 继续 *。
7. 完成向导中的页面以创建新的同步关系。

使用 Cloud Sync

在源和目标之间同步数据

创建同步关系

创建同步关系时、Cloud Sync 服务会将文件从源复制到目标。初始副本完成后、服务将每 24 小时同步所有更改的数据。

在创建某些类型的同步关系之前，您需要先在 Cloud Manager 中创建一个工作环境。

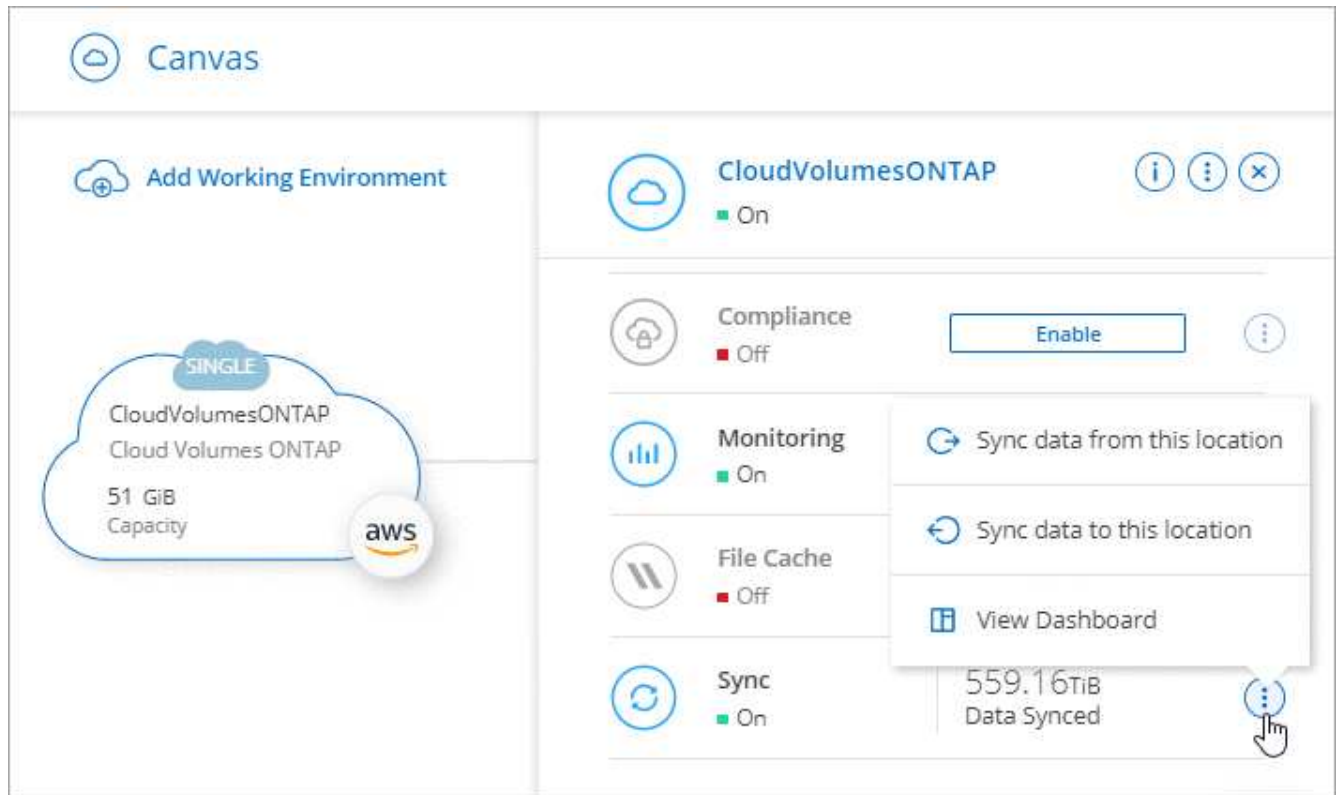
为特定类型的工作环境创建同步关系

如果要为以下任一项创建同步关系，则首先需要创建或发现工作环境：

- 适用于 ONTAP 的 Amazon FSX
- Azure NetApp Files
- Cloud Volumes ONTAP
- 内部 ONTAP 集群

步骤

1. 创建或发现工作环境。
 - ["创建适用于 ONTAP 的 Amazon FSX 工作环境"](#)
 - ["设置和发现 Azure NetApp Files"](#)
 - ["在 AWS 中启动 Cloud Volumes ONTAP"](#)
 - ["在 Azure 中启动 Cloud Volumes ONTAP"](#)
 - ["在 Google Cloud 中启动 Cloud Volumes ONTAP"](#)
 - ["添加现有 Cloud Volumes ONTAP 系统"](#)
 - ["发现 ONTAP 集群"](#)
2. 单击 * 画布 *。
3. 选择与上述任何类型匹配的工作环境。
4. 选择 Sync 旁边的操作菜单。



5. 选择 * 从此位置同步数据 * 或 * 将数据同步到此位置 *，然后按照提示设置同步关系。

创建其他类型的同步关系

使用以下步骤将数据同步到或不同步适用于 ONTAP， Azure NetApp Files， Cloud Volumes ONTAP 或内部 ONTAP 集群的 Amazon FSX 以外的受支持存储类型。以下步骤提供了一个示例，说明如何设置从 NFS 服务器到 S3 存储分段的同步关系。

1. 在 Cloud Manager 中，单击 * 同步 *。
2. 在 * 定义同步关系 * 页面上，选择源和目标。

以下步骤提供了如何创建从 NFS 服务器到 S3 存储区的同步关系的示例。

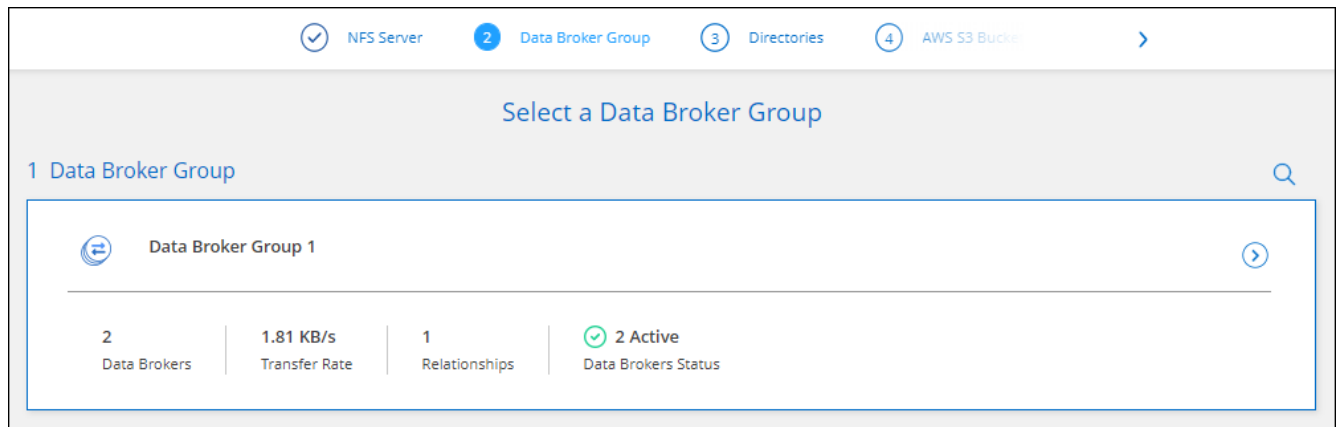


3. 在 * NFS Server* 页面上，输入要同步到 AWS 的 NFS 服务器的 IP 地址或完全限定域名。
4. 在 * 数据代理组 * 页面上，按照提示在 AWS ， Azure 或 Google Cloud Platform 中创建数据代理虚拟机，或者在现有 Linux 主机上安装数据代理软件。

有关详细信息，请参阅以下页面：

- ["在 AWS 中创建数据代理"](#)
- ["在 Azure 中创建数据代理"](#)
- ["在 Google Cloud 中创建数据代理"](#)
- ["在 Linux 主机上安装数据代理"](#)

5. 安装数据代理后，单击 * 继续 * 。



6. 在 * 目录 * 页面上，选择顶级目录或子目录。

如果 Cloud Sync 无法检索导出，请单击 * 手动添加导出 * 并输入 NFS 导出的名称。



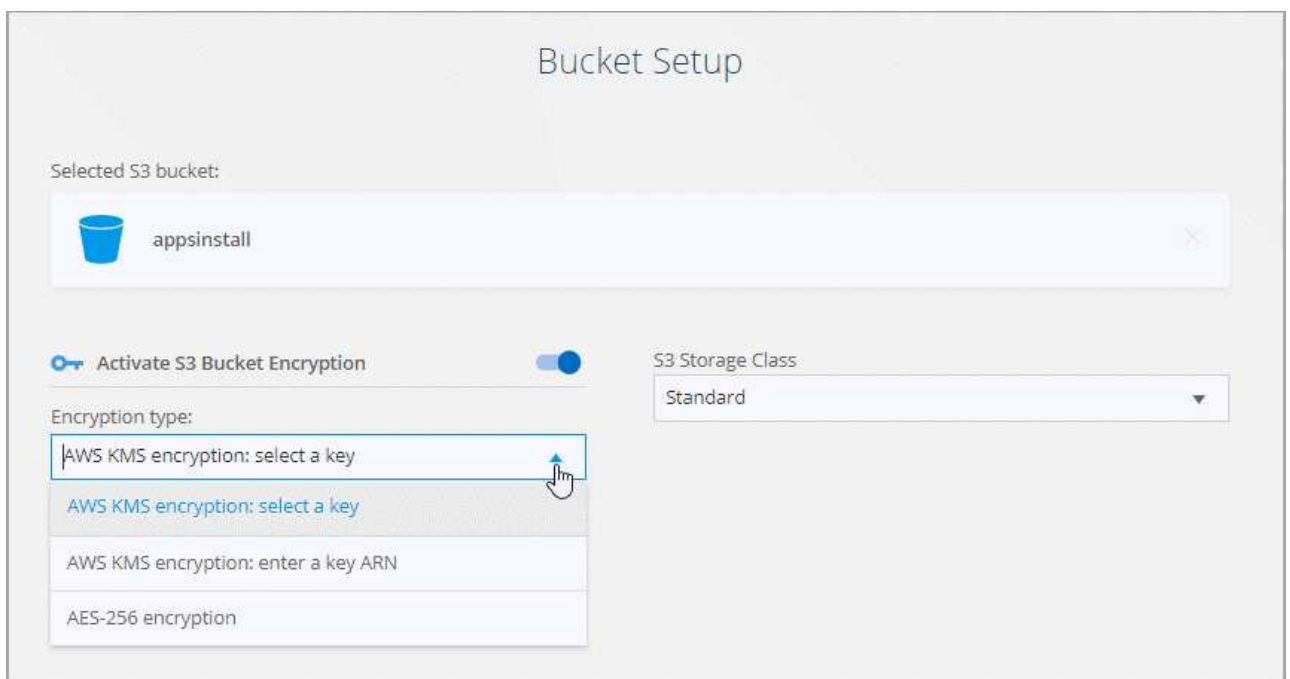
如果要同步 NFS 服务器上的多个目录、则必须在完成后创建其他同步关系。

7. 在 * AWS S3 Bucket* 页面上，选择一个存储分段：

- 向下钻取以选择存储桶中的现有文件夹或选择在存储桶内创建的新文件夹。
- 单击 * 添加到列表 * 以选择与您的 AWS 帐户无关的 S3 存储分段。"必须将特定权限应用于 S3 存储区。"。

8. 在 * 分段设置 * 页面上，设置分段：

- 选择是否启用 S3 存储分段加密，然后选择 AWS KMS 密钥，输入 KMS 密钥的 ARN 或选择 AES-256 加密。
- 选择 S3 存储类。"查看支持的存储类。"。



9. 【设置】在 * 设置 * 页面上，定义源文件和文件夹在目标位置的同步和维护方式：

计划

为将来的同步选择重复计划或关闭同步计划。您可以计划一个关系以每 1 分钟同步一次数据。

重试

定义在跳过文件之前、Cloud Sync 应重试同步文件的次数。

比较依据

选择 Cloud Sync 在确定文件或目录是否已更改并应重新同步时是否应比较某些属性。

即使取消选中这些属性，Cloud Sync 仍会通过检查路径、文件大小和文件名来将源与目标进行比较。如果有任何更改，则会同步这些文件和目录。

您可以选择启用或禁用 Cloud Sync 以比较以下属性：

- * mtime*：文件的上次修改时间。此属性对目录无效。
- * uid*，* gid* 和 * 模式 *：Linux 的权限标志。

复制对象

启用此选项可复制对象存储元数据和标记。如果用户更改了源上的元数据，则 Cloud Sync 会在下次同步时复制此对象，但如果用户更改了源上的标记（而不是数据本身），则 Cloud Sync 不会在下次同步时复制对象。

创建关系后，您无法编辑此选项。

包含 S3 兼容端点（S3，StorageGRID 或 IBM 云对象存储）的同步关系支持复制标记。

以下任一端点之间的 "云到云" 关系支持复制元数据：

- AWS S3
- Azure Blob
- Google Cloud 存储
- IBM 云对象存储
- StorageGRID

最近修改的文件

选择排除在计划同步之前最近修改的文件。

删除源上的文件

选择在 Cloud Sync 将文件复制到目标位置后从源位置删除文件。此选项包括数据丢失的风险，因为源文件会在复制后被删除。

如果启用此选项，则还需要更改数据代理上 local.json 文件中的参数。打开文件并按如下所示进行更新：

```
{
  "workers":{
    "transferrer":{
      "delete-on-source": true
    }
  }
}
```

删除目标上的文件

如果文件已从源文件中删除，请选择从目标位置删除这些文件。默认情况下，从不从目标位置删除文件。

文件类型

定义要包括在每个同步中的文件类型：文件、目录和符号链接。

排除文件扩展名

通过键入文件扩展名并按 * 输入 * 来指定要从同步中排除的文件扩展名。例如，键入 *log* 或 *.log* 排除 * .log 文件。多个扩展不需要分隔符。以下视频提供了简短演示：

► https://docs.netapp.com/zh-cn/cloud-manager-sync//media/video_file_extensions.mp4 (video)

文件大小

选择同步所有文件、无论文件大小如何、还是仅同步特定大小范围内的文件。

修改日期

选择所有文件，无论其上次修改日期、在特定日期之后修改的文件、特定日期之前或时间范围之间的文件。

创建日期

如果 SMB 服务器是源服务器，则可以通过此设置在特定日期之后，特定日期之前或特定时间范围之间同步创建的文件。

ACL — 访问控制列表

通过在创建关系时或创建关系后启用设置，从 SMB 服务器复制 ACL。

10. 在 * 标记 / 元数据 * 页面上，选择是将密钥值对另存为传输到 S3 存储分段的所有文件的标记，还是为所有文件分配元数据密钥值对。



将数据同步到 StorageGRID 和 IBM 云对象存储时，也可以使用此功能。对于 Azure 和 Google Cloud Storage，只有元数据选项可用。

11. 查看同步关系的详细信息，然后单击 * 创建关系 *。

◦ 结果 *

Cloud Sync 开始在源和目标之间同步数据。

从 **Cloud Data sense** 创建同步关系

Cloud Sync 与云数据感知相集成。在 Data sense 中，您可以使用 Cloud Sync 选择要同步到目标位置的源文件。

从 Cloud Data sense 启动数据同步后，所有源信息都包含在一个步骤中，只需输入几个关键详细信息即可。然后，选择新同步关系的目标位置。

"了解如何从 Cloud Data sense 启动同步关系"。

从 SMB 共享复制 ACL

Cloud Sync 可以在源 SMB 共享和目标 SMB 共享之间复制访问控制列表（ACL），也可以从源 SMB 共享复制到对象存储（ONTAP S3 除外）。如果需要，您还可以选择使用 Robocopy 在 SMB 共享之间手动保留 ACL。



Cloud Sync 不支持将 ACL 从对象存储复制回 SMB 共享。

选项

- [设置 Cloud Sync 以自动复制 ACL](#)
- [在 SMB 共享之间手动复制 ACL](#)


设置 Cloud Sync 以从 SMB 服务器复制 ACL

通过在创建关系时或创建关系后启用设置，从 SMB 服务器复制 ACL。

此功能适用于 *any* 类型的数据代理：AWS，Azure，Google Cloud Platform 或内部数据代理。内部数据代理可以运行 ["任何受支持的操作系统"](#)。

新关系的步骤

1. 在 Cloud Sync 中，单击 * 创建新同步 *。
2. 将 * SMB Server* 拖放到源，选择 SMB 服务器或对象存储作为目标，然后单击 * 继续 *。
3. 在 * SMB Server* 页面上：
 - a. 输入新的 SMB 服务器或选择现有服务器，然后单击 * 继续 *。
 - b. 输入 SMB 服务器的凭据。
 - c. 选择 * 将访问控制列表复制到目标 *，然后单击 * 继续 *。



Select an SMB Source

SMB Version: 2.1 ▼

Selected SMB Server: 10.20.30.152

Define SMB Credentials:

User Name: user1 Password: ***** Domain (Optional):

ACL - Access Control List

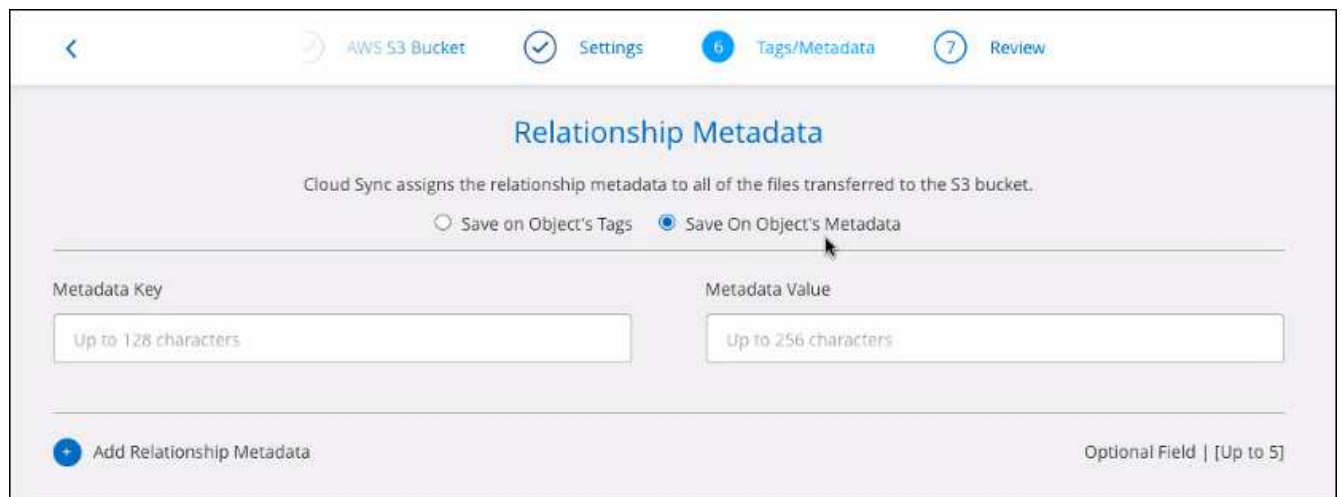
☒ Copy Access Control Lists to the target

Notice: Copying ACLs can affect sync performance.
You can change this setting after you create the relationship.

4. 按照其余提示创建同步关系。

将 ACL 从 SMB 复制到对象存储时，您可以选择将 ACL 复制到对象的标记或对象的元数据上，具体取决于目标。对于 Azure 和 Google Cloud Storage，只有元数据选项可用。

以下屏幕截图显示了一个可以选择此操作的步骤示例。



< AWS S3 Bucket Settings **6** Tags/Metadata **7** Review

Relationship Metadata

Cloud Sync assigns the relationship metadata to all of the files transferred to the S3 bucket.

☐ Save on Object's Tags ☒ Save On Object's Metadata

Metadata Key: Up to 128 characters Metadata Value: Up to 256 characters

+ Add Relationship Metadata Optional Field | [Up to 5]

现有关系的步骤

1. 将鼠标悬停在“同步关系”上，然后单击“操作”菜单。
2. 单击 * 设置 *。
3. 选择 * 将访问控制列表复制到目标 *。
4. 单击 * 保存设置 *。

同步数据时，Cloud Sync 会保留源和目标 SMB 共享之间的 ACL，或者从源 SMB 共享保留到对象存储。

在 SMB 共享之间手动复制 ACL

您可以使用 Windows robocopy 命令手动保留 SMB 共享之间的 ACL。

步骤

1. 确定具有对 SMB 共享的完全访问权限的 Windows 主机。
2. 如果任一端点需要身份验证，请使用 * 网络使用 * 命令从 Windows 主机连接到这些端点。

在使用 Robocopy 之前，必须执行此步骤。

3. 从 Cloud Sync 中，在源设备和目标 SMB 共享之间创建新关系或同步现有关系。
4. 数据同步完成后、从 Windows 主机运行以下命令以同步 ACL 和所有权：

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots  
/UNILOG:"[logfilepath]
```

源 *sourc* 和目标 *_* 均应使用 UNC 格式指定。例如：\\<server> \<share> \<path>

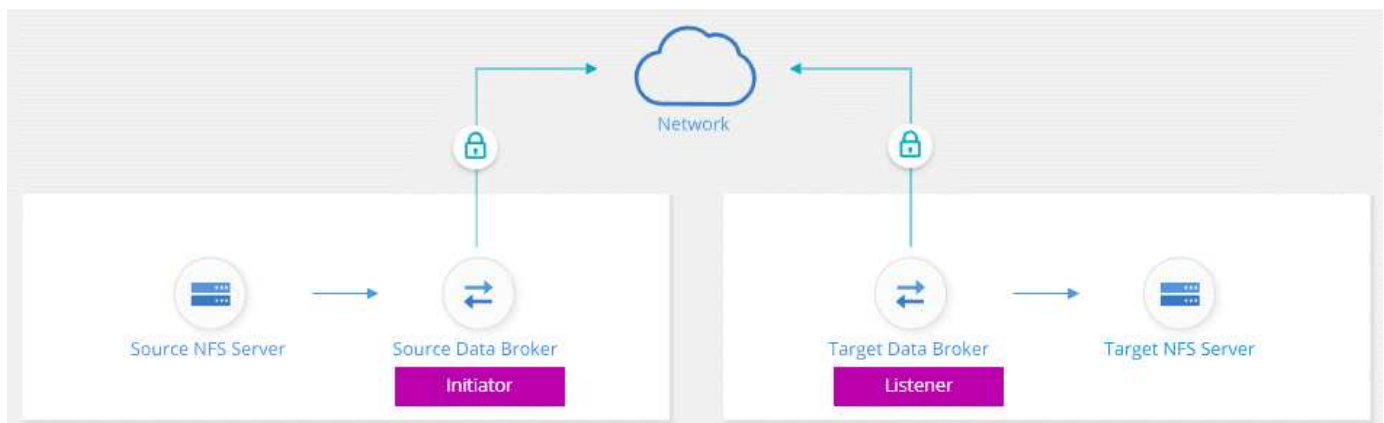
使用传输中数据加密同步 NFS 数据

如果您的企业拥有严格的安全策略，则可以使用数据传输加密来同步 NFS 数据。从 NFS 服务器到另一个 NFS 服务器以及从 Azure NetApp Files 到 Azure NetApp Files 均支持此功能。

例如，您可能希望在位于不同网络的两个 NFS 服务器之间同步数据。或者，您可能需要在子网或区域之间安全地传输 Azure NetApp Files 上的数据。

飞行中数据加密的工作原理

传输中数据加密在两个数据代理之间通过网络发送 NFS 数据时对其进行加密。下图显示了两个 NFS 服务器和两个数据代理之间的关系：



一个数据代理充当 *initiator*。同步数据时，它会向另一个数据代理（即 *listener*）发送连接请求。该数据代理会侦听端口 443 上的请求。如果需要，您可以使用其他端口，但请务必检查此端口是否未被其他服务使用。

例如，如果将数据从内部 NFS 服务器同步到基于云的 NFS 服务器，则可以选择哪个数据代理侦听连接请求并将其发送。

以下是动态加密的工作原理：

1. 创建同步关系后、启动程序将启动与其他数据代理的加密连接。
2. 源数据代理使用 TLS 1.3 对源中的数据进行加密。
3. 然后通过网络将数据发送到目标数据代理。
4. 目标数据代理会先对数据进行解密，然后再将其发送到目标。
5. 初始副本完成后、服务将每 24 小时同步所有更改的数据。如果有要同步的数据，则进程将从启动程序打开与其他数据代理的加密连接开始。

如果您希望更频繁地同步数据，"[您可以在创建关系后更改此计划](#)"。

支持的 NFS 版本

- 对于 NFS 服务器，NFS 版本 3，4.0，4.1 和 4.2 支持传输中数据加密。
- 对于 Azure NetApp Files，NFS 版本 3 和 4.1 支持传输中数据加密。

代理服务器限制

如果创建加密同步关系，加密数据将通过 HTTPS 发送，不能通过代理服务器路由。

您将需要什么才能开始

请确保具有以下内容：

- 两个 NFS 服务器相结合 "[源和目标要求](#)" 或 Azure NetApp Files。
- 服务器的 IP 地址或完全限定域名。
- 两个数据代理的网络位置。

您可以选择现有的数据代理、但它必须作为启动程序运行。侦听器数据代理必须是 *new* 数据代理。

如果要使用现有数据代理组，该组必须只有一个数据代理。加密的同步关系不支持组中的多个数据代理。

如果尚未部署数据代理、请查看数据代理要求。由于您具有严格的安全策略，请务必查看网络要求，其中包括端口 443 和的出站流量 "[Internet 端点](#)" 数据代理所联系的。

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

使用传输中数据加密同步 NFS 数据

在两个 NFS 服务器之间或 Azure NetApp Files 之间创建新的同步关系，启用正在传输的加密选项，然后按照提示进行操作。

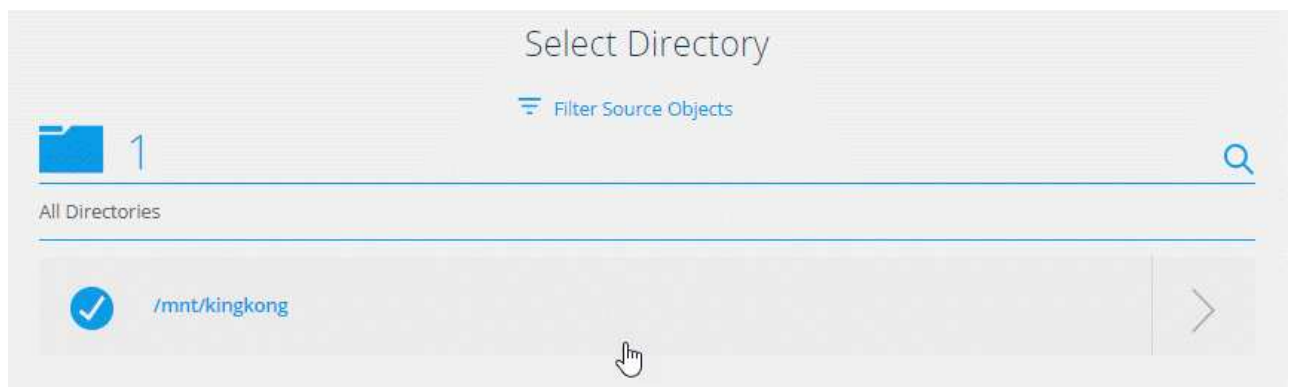
步骤

1. 单击 * 创建新同步 *。
2. 将 * NFS Server* 拖放到源位置和目标位置，或者将 * Azure NetApp Files * 拖放到源位置和目标位置，然后选择 * 是 * 以启用传输中数据加密。
3. 按照提示创建关系：
 - a. * NFS Server*/* Azure NetApp Files*：选择 NFS 版本，然后指定新的 NFS 源或选择现有服务器。
 - b. * 定义数据代理功能 *：定义哪个数据代理侦听端口上的连接请求以及哪个数据代理启动连接。根据您的网络要求做出选择。
 - c. * 数据代理 *：按照提示添加新的源数据代理或选择现有数据代理。

请注意以下事项：

- 如果要使用现有数据代理组，该组必须只有一个数据代理。加密的同步关系不支持组中的多个数据代理。
 - 如果源数据代理充当侦听程序、则它必须是新的数据代理。
 - 如果需要新的数据代理、Cloud Sync 会提示您安装说明。您可以在云中部署数据代理或为自己的 Linux 主机下载安装脚本。
- d. * 目录 *：选择要同步的目录，方法是选择所有目录，或者向下钻取并选择子目录。

单击 * 筛选源对象 * 可修改用于定义源文件和文件夹在目标位置的同步和维护方式的设置。




- e. * 目标 NFS 服务器 / 目标 NFS*：选择 Azure NetApp Files 版本，然后输入新的 目标或选择现有服务器。
- f. * 目标数据代理 *：按照提示添加新的源数据代理或选择现有数据代理。


如果目标数据代理充当侦听程序、则它必须是新的数据代理。

以下是目标数据代理充当侦听器时的提示示例。请注意指定端口的选项。


Select a Provider




Microsoft Azure



Amazon Web Services



Google Cloud Platform

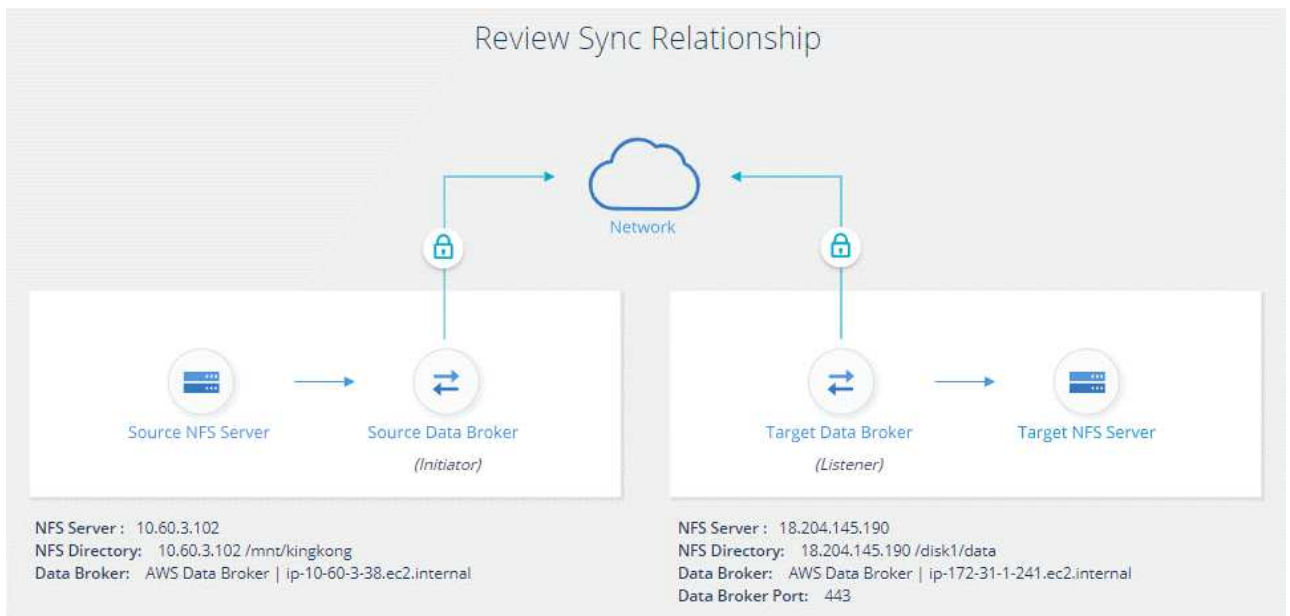


On-Prem Data Broker

Data Broker Name

Port

- a. * 目标目录 *：选择顶级目录，或者向下钻取以选择现有子目录或在导出中创建新文件夹。
- b. * 设置 *：定义如何在目标位置同步和维护源文件和文件夹。
- c. * 审阅 *：查看同步关系的详细信息，然后单击 * 创建关系 *。



Cloud Sync 开始创建新的同步关系。完成后，单击 **在信息板中查看** 以查看有关新关系的详细信息。

设置数据代理组以使用外部 HashiCorp 存储

创建需要 Amazon S3，Azure 或 Google Cloud 凭据的同步关系时，您需要通过 Cloud Sync 用户界面或 API 指定这些凭据。另一种方法是设置数据代理组，以便直接从外部 HashiCorp 存储访问凭据（或 *secrets*）。

此功能通过 Cloud Sync API 提供支持，并且同步关系需要 Amazon S3，Azure 或 Google Cloud 凭据。

通过设置 URL 来准备存储以向数据代理组提供凭据。存储中的机密 URL 必须以 `_Creds_` 结尾。

通过修改组中每个数据代理的本地配置文件，使数据代理组做好准备，以便从外部存储提取凭据。

设置完所有内容后，您可以发送 API 调用来创建同步关系，以使用存储获取密码。

准备存储

您需要为 Cloud Sync 提供存储中机密的 URL。通过设置这些 URL 来准备存储。您需要为计划创建的同步关系中的每个源和目标的凭据设置 URL。

必须按如下所示设置 URL：

` /<path>/<RequestId>/<Endpoint-protocol>Creds`

路径

密钥的前缀路径。这可以是您独有的任何值。

请求 ID

需要生成的请求 ID。创建同步关系时，您需要在 API POST 请求中的一个标题中提供 ID。

端点协议

定义的以下协议之一 ["在关系后 v2 文档中"](#)：S3，Azure 或 GCP（每个都必须大写）。

创建

URL 必须以 `_Creds_` 结尾。

示例

以下示例显示了指向机密的 URL。

源凭据的完整 URL 和路径示例

<http://example.vault.com:8200/my-path/all-secrets/hb312vdsr2/S3Creds>

如示例中所示，前缀路径为 `//my-path/all-sects/`，请求 ID 为 `hb312vdsr2`，源端点为 S3。

目标凭据的完整 URL 和路径示例

<http://example.vault.com:8200/my-path/all-secrets/n32hcbnejk2/AZURECreds>

前缀路径为 `//my-path/all-sections/_`，请求 ID 为 `n32hcbnejk2`，目标端点为 Azure。

正在准备数据代理组

通过修改组中每个数据代理的本地配置文件，使数据代理组做好准备，以便从外部存储提取凭据。

步骤

1. 通过 SSH 连接到组中的数据代理。
2. 编辑 `/opt/netapp/databroker/config` 中的 `local.json` 文件。
3. 将 `enable` 设置为 `* true *`，并按如下所示在 `external-积分 .hashashicorp` 下设置配置参数字段：

enabled

- 有效值： true/false
- 类型：布尔值
- 默认值： false
- true：数据代理从您自己的外部 HashiCorp Vault 获取机密
- false：数据代理将凭据存储在其本地存储中

url

- 键入： string
- value：外部存储的 URL

path

- 键入： string
- value：使用凭据将路径前缀为密钥

拒绝 - 未授权

- 确定是否希望数据代理拒绝未经授权的外部存储
- 类型：布尔值
- 默认值： false

auth-method

- 数据代理从外部存储访问凭据时应使用的身份验证方法
- 键入： string
- 有效值： "AWS-iam"/"role-app"/"GCP-iam"

角色名称

- 键入： string
- 您的角色名称（如果您使用 AWS-iam 或 GCP-iam）

Secretid 和 rootid

- type： string（如果使用 app-role）

命名空间

- 键入： string
- 命名空间（如果需要，则为 X-Vault-Namespace 标头）

4. 对组中的任何其他数据代理重复上述步骤。

AWS 角色身份验证示例

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "https://example.vault.com:8200",
      "path": "my-path/all-secrets",
      "reject-unauthorized": false,
      "auth-method": "aws-role",
      "aws-role": {
        "role-name": "my-role"
      }
    }
  }
}
```

GCP-iam 身份验证示例

```
{
  "external-integrations": {
    "hashicorp": {
      "enabled": true,
      "url": "http://ip-10-20-30-55.ec2.internal:8200",
      "path": "v1/secret",
      "namespace": "",
      "reject-unauthorized": true,
      "auth-method": "gcp-iam",
      "aws-iam": {
        "role-name": ""
      },
      "app-role": {
        "root_id": "",
        "secret_id": ""
      },
      "gcp-iam": {
        "role-name": "my-iam-role"
      }
    }
  }
}
```

使用 GCP-iam 身份验证时设置权限

如果您使用的是 *gcp-iam* 身份验证方法，则数据代理必须具有以下 GCP 权限：

```
- iam.serviceAccounts.signJwt
```

"详细了解数据代理的 [GCP 权限要求](#)"。

使用存储中的密钥创建新的同步关系

设置完所有内容后，您可以发送 API 调用来创建同步关系，以使用存储获取密码。

使用 Cloud Sync REST API 发布关系。

```
Headers:  
Authorization: Bearer <user-token>  
Content-Type: application/json  
x-account-id: <accountid>  
x-netapp-external-request-id-src: request ID as part of path for source  
credentials  
x-netapp-external-request-id-trg: request ID as part of path for target  
credentials  
Body: post relationship v2 body
```

- 要获取用户令牌和 Cloud Central 帐户 ID ， ["请参见文档中的此页面"](#)。
- 为您的后关系构建实体， ["请参见 relationships-v2 API 调用"](#)。

示例

POST 请求示例：

```
url: https://api.cloudsync.netapp.com/api/relationships-v2
headers:
"x-account-id": "CS-SasdW"
"x-netapp-external-request-id-src": "hb312vdasr2"
"Content-Type": "application/json"
"Authorization": "Bearer eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ik..."
Body:
{
  "dataBrokerId": "5e6e111d578dtyuu1555sa60",
  "source": {
    "protocol": "s3",
    "s3": {
      "provider": "sgws",
      "host": "1.1.1.1",
      "port": "443",
      "bucket": "my-source"
    }
  },
  "target": {
    "protocol": "s3",
    "s3": {
      "bucket": "my-target-bucket"
    }
  }
}
```

在免费试用结束后为同步关系付费

在 14 天免费试用结束后、有两种方式可以支付同步关系的费用。第一种选择是从 AWS 或 Azure 订阅“按需购买、渐进购买”或“每年支付”。第二种选择是直接从 NetApp 购买许可证。

您可以从 AWS Marketplace 或 Azure Marketplace 订阅。您不能同时从这两个订阅。

您可以选择将 NetApp 的许可证与 Marketplace 订阅结合使用。例如，如果您有 25 个同步关系、则可以使用许可证支付前 20 个同步关系的费用、然后从 AWS 或 Azure 中按原样支付剩余的 5 个同步关系的费用。

[了解有关许可证工作原理的更多信息。](#)

如果在免费试用结束后，我不能立即支付费用，该怎么办？

您将无法创建任何其他关系。现有关系不会被删除、但您必须订阅或输入许可证才能对其进行任何更改。

从 AWS 订阅

AWS 使您可以按需付费或每年支付。

按需购买的步骤

1. 单击 * 同步 > 许可 *。
2. 选择 * AWS *。
3. 单击 * 订阅 *，然后单击 * 继续 *。
4. 从 AWS Marketplace 订阅，然后重新登录到 Cloud Sync 服务以完成注册。

以下视频显示了该过程：

► https://docs.netapp.com/zh-cn/cloud-manager-sync//media/video_cloud_sync_registering.mp4 (video)

每年支付的步骤

1. "转至 [AWS Marketplace 页面](#)。"
2. 单击 * 继续订阅 *。
3. 选择您的合同选项，然后单击 * 创建合同 *。

从 Azure 订阅

Azure 使您可以按需付费或每年支付。

在相关订阅中具有“贡献者”或“所有者”权限的 Azure 用户帐户。

步骤

1. 单击 * 同步 > 许可 *。
2. 选择 * Azure *。
3. 单击 * 订阅 *，然后单击 * 继续 *。
4. 在 Azure 门户中，单击 * 创建 *，选择您的选项，然后单击 * 订阅 *。

选择 * 按月 * 按小时付费，或者选择 * 按年 * 按前一年付费。

5. 部署完成后，在通知弹出窗口中单击 SaaS 资源的名称。
6. 单击 * 配置帐户 * 以返回到 Cloud Sync。

以下视频显示了该过程：

► https://docs.netapp.com/zh-cn/cloud-manager-sync//media/video_cloud_sync_registering_azure.mp4

(video)

从 NetApp 购买许可证并将其添加到 Cloud Sync

要预先支付同步关系的费用、您必须购买一个或多个许可证并将其添加到 Cloud Sync 服务。

您需要提供许可证的序列号以及与许可证关联的 NetApp 支持站点帐户的用户名和密码。

步骤

1. 请发送邮件至：ng-cloudsync-contact@netapp.com？ Subject=Cloud%20Sync%20Service%20-%20BYOL%20License%20Purches%20Request[联系 NetApp] 购买许可证。
2. 在 Cloud Manager 中，单击 * 同步 > 许可 *。
3. 单击 * 添加许可证 * 并添加所需信息：
 - a. 输入序列号。
 - b. 选择与要添加的许可证关联的 NetApp 支持站点帐户：
 - 如果您的帐户已添加到 Cloud Manager 中，请从下拉列表中选择它。
 - 如果尚未添加您的帐户，请单击 * 添加 NSS 凭据 *，输入用户名和密码，单击 * 注册 *，然后从下拉列表中选择它。
 - c. 单击 * 添加 *。

更新许可证

如果您延长了从 NetApp 购买的 Cloud Sync 许可证，则新的到期日期不会在 Cloud Sync 中自动更新。要刷新到期日期，您需要重新添加许可证。

步骤

1. 在 Cloud Manager 中，单击 * 同步 > 许可 *。
2. 单击 * 添加许可证 * 并添加所需信息：
 - a. 输入序列号。
 - b. 选择与要添加的许可证关联的 NetApp 支持站点帐户：
 - c. 单击 * 添加 *。

Cloud Sync 会使用新的到期日期更新现有许可证。


管理同步关系

您可以通过立即同步数据、更改计划等随时管理同步关系。

执行即时数据同步

您可以按按钮立即在源和目标之间同步数据，而不是等待下一个计划同步。

步骤

1. 在 * 信息板 * 中，导航到同步关系，然后单击 
2. 单击 * 立即同步 * ，然后单击 * 同步 * 进行确认。

Cloud Sync 将启动关系的数据同步过程。

加快同步性能

通过向管理同步关系的组添加额外的数据代理来提高同步关系的性能。其他数据代理必须是 *new* 数据代理。


如果数据代理组管理其他同步关系，则添加到组中的新数据代理也会提高这些同步关系的性能。

例如，假设您有三个关系：

- 关系 1 由数据代理组 A 管理
- 关系 2 由数据代理组 B 管理
- 关系 3 由数据代理组 A 管理

您希望提高关系 1 的性能，以便向数据代理组 A 添加新的数据代理由于组 A 还管理同步关系 3 ，因此关系的同步性能也会自动提高。

步骤

1. 确保关系中至少有一个现有数据代理处于联机状态。
2. 在 * 信息板 * 中，导航到同步关系，然后单击 
3. 单击 * 加速 * 。
4. 按照提示创建新的数据代理。

Cloud Sync 会将新数据代理添加到组中。应加快下一个数据同步的性能。

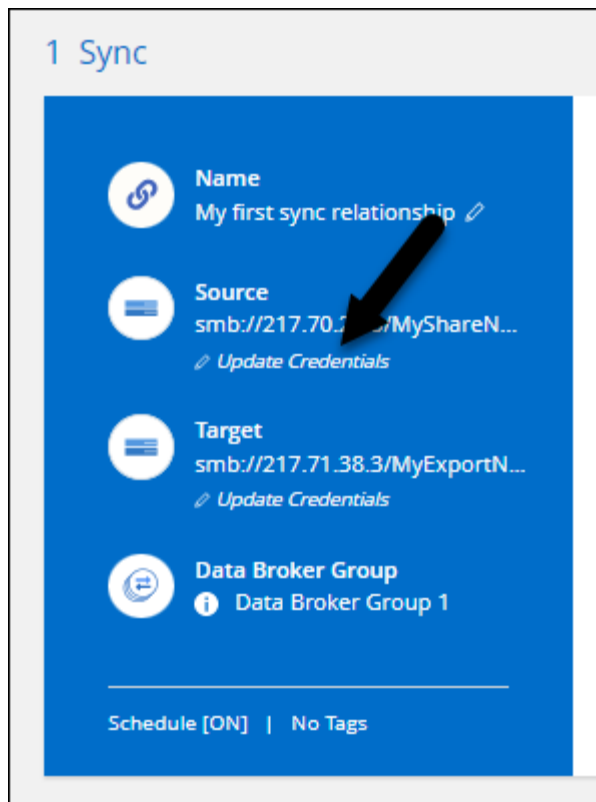
正在更新凭据

您可以使用现有同步关系中源或目标的最新凭据更新数据代理。如果安全策略要求您定期更新凭据，则更新凭据会很有帮助。

Cloud Sync 需要以下凭据的任何源或目标均支持更新凭据： Azure Blob ， Box ， IBM 云对象存储， StorageGRID ， ONTAP S3 存储， SFTP 和 SMB 服务器。

步骤

1. 从 * 同步信息板 * 中，转到需要凭据的同步关系，然后单击 * 更新凭据 * 。



2. 输入凭据并单击 * 更新 *。


有关 SMB 服务器的注意事项：如果此域是新域，则在更新凭据时需要指定它。如果域未更改，则无需重新输入。

如果您在创建同步关系时输入了域，但在更新凭据时未输入新域，则 Cloud Sync 将继续使用您提供的原始域。

Cloud Sync 将更新数据代理上的凭据。可能需要 10 分钟，直到数据代理开始使用更新后的数据同步凭据。

更改同步关系的设置

修改定义源文件和文件夹在目标位置的同步和维护方式的设置。

1. 在 * 信息板 * 中，导航到同步关系，然后单击 
2. 单击 * 设置 *。
3. 修改任何设置。

General

Schedule	ON Every 1 Day	▼
Retries	Retry 3 times before skipping file	▼

Files and Directories

Compare By	The following attributes (and size): uid, gid, mode, mtime	▼
Recently Modified Files	Exclude files that are modified up to 30 Seconds before a scheduled sync	▼
Delete Files On Source	Never delete files from the source location	▼
Delete Files On Target	Never delete files from the target location	▼
File Types	Include All: Files, Directories, Symbolic Links	▼
Exclude File Extensions	None	▼
File Size	All	▼
Date Modified	All	▼
Date Created	All	▼
ACL - Access Control List	Inactive	▼

Reset to defaults

【 { deleteonsource } 】下面是每个设置的简短问题描述：

计划

为将来的同步选择重复计划或关闭同步计划。您可以计划一个关系以每 1 分钟同步一次数据。

重试

定义在跳过文件之前、Cloud Sync 应重试同步文件的次数。

比较依据

选择 Cloud Sync 在确定文件或目录是否已更改并应重新同步时是否应比较某些属性。

即使取消选中这些属性，Cloud Sync 仍会通过检查路径，文件大小和文件名来将源与目标进行比较。如

果有任何更改，则会同步这些文件和目录。

您可以选择启用或禁用 Cloud Sync 以比较以下属性：

- `* mtime*`：文件的上次修改时间。此属性对目录无效。
- `* uid*`，`* gid*` 和 `* 模式 *`：Linux 的权限标志。

复制对象

创建关系后，您无法编辑此选项。

最近修改的文件

选择排除在计划同步之前最近修改的文件。

删除源上的文件

选择在 Cloud Sync 将文件复制到目标位置后从源位置删除文件。此选项包括数据丢失的风险，因为源文件会在复制后被删除。

如果启用此选项，则还需要更改数据代理上 `local.json` 文件中的参数。打开文件并按如下所示进行更新：

```
{
  "workers": {
    "transferrer": {
      "delete-on-source": true
    }
  }
}
```

删除目标上的文件

如果文件已从源文件中删除，请选择从目标位置删除这些文件。默认情况下，从不从目标位置删除文件。

文件类型

定义要包括在每个同步中的文件类型：文件、目录和符号链接。

排除文件扩展名

通过键入文件扩展名并按 `*` 输入 `*` 来指定要从同步中排除的文件扩展名。例如，键入 `log` 或 `.log` 排除 `*`。`log` 文件。多个扩展不需要分隔符。以下视频提供了简短演示：

► https://docs.netapp.com/zh-cn/cloud-manager-sync//media/video_file_extensions.mp4 (video)

文件大小

选择同步所有文件、无论文件大小如何、还是仅同步特定大小范围内的文件。

修改日期

选择所有文件，无论其上次修改日期、在特定日期之后修改的文件、特定日期之前或时间范围之间的文件。

创建日期

如果 SMB 服务器是源服务器，则可以通过此设置在特定日期之后，特定日期之前或特定时间范围之间同步创建的文件。

ACL — 访问控制列表

通过在创建关系时或创建关系后启用设置，从 SMB 服务器复制 ACL。


4. 单击 * 保存设置 *。

Cloud Sync 会修改与新设置的同步关系。

删除关系

如果不再需要在源和目标之间同步数据，则可以删除同步关系。此操作不会删除数据代理组（或单个数据代理实例），也不会删除目标中的数据。

步骤

1. 在 * 信息板 * 中，导航到同步关系，然后单击 
2. 单击 * 删除 *，然后再次单击 * 删除 * 进行确认。

Cloud Sync 会删除同步关系。

管理数据代理组

数据代理组将数据从源位置同步到目标位置。对于您创建的每个同步关系，组中至少需要一个数据代理。通过向组中添加新数据代理，查看组信息等来管理数据代理组。

数据代理组的工作原理

一个数据代理组可以包含一个或多个数据代理。将数据代理分组在一起有助于提高同步关系的性能。

组可以管理多个关系

数据代理组一次可以管理一个或多个同步关系。

例如，假设您有三个关系：

- 关系 1 由数据代理组 A 管理
- 关系 2 由数据代理组 B 管理
- 关系 3 由数据代理组 A 管理

您希望提高关系 1 的性能，以便向数据代理组 A 添加新的数据代理由于组 A 还管理同步关系 3，因此关系的同步性能也会自动提高。

组中数据代理的数量

在许多情况下、单个数据代理可以满足同步关系的性能要求。如果不支持，您可以通过向组添加其他数据代理来

提高同步性能。但是，您应该首先检查可能影响同步性能的其他因素。 ["详细了解如何确定何时需要多个数据代理"](#)。

安全建议

为了确保数据代理计算机的安全性， NetApp 建议执行以下操作：

- SSH 不应允许 X11 转发
- SSH 不应允许 TCP 连接转发
- SSH 不应允许使用通道
- SSH 不应接受客户端环境变量

这些安全建议有助于防止未经授权连接到数据代理计算机。

将新数据代理添加到组

可以通过多种方法创建新的数据代理：

- 创建新同步关系时

["了解如何在创建同步关系时创建新的数据代理"](#)。

- 在 * 管理数据代理 * 页面中，单击 * 添加新数据代理 *，以在新组中创建数据代理
- 通过在现有组中创建新的数据代理，从 * 管理数据代理 * 页面访问此信息

开始之前

- 您不能将数据代理添加到管理加密同步关系的组中。
- 如果要在现有组中创建数据代理，数据代理必须是内部数据代理或相同类型的数据代理。

例如，如果某个组包含 AWS 数据代理，则可以在该组中创建 AWS 数据代理或内部数据代理。您不能创建 Azure 数据代理或 Google Cloud 数据代理，因为它们不是相同的数据代理类型。

在新组中创建数据代理的步骤

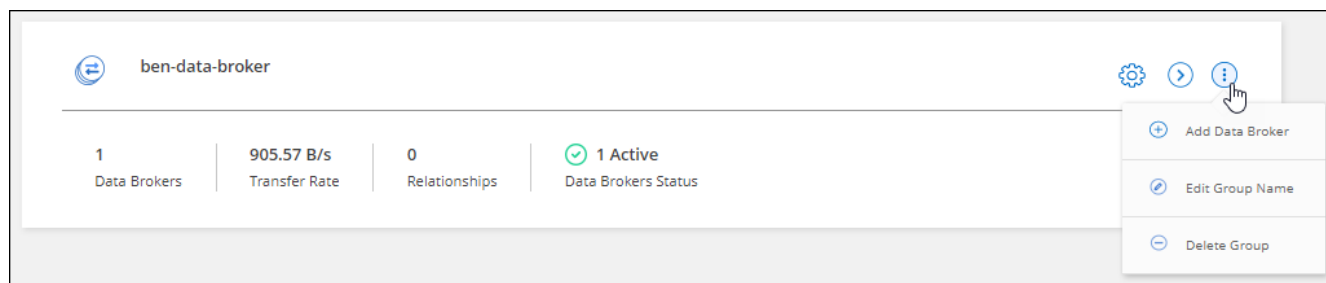
1. 单击 * 同步 > 管理数据代理 *。
2. 单击 * 添加新数据代理 *。
3. 按照提示创建数据代理。

要获得帮助，请参见以下页面：

- ["在 AWS 中创建数据代理"](#)
- ["在 Azure 中创建数据代理"](#)
- ["在 Google Cloud 中创建数据代理"](#)
- ["在 Linux 主机上安装数据代理"](#)

在现有组中创建数据代理的步骤

1. 单击 * 同步 > 管理数据代理 *。
2. 单击操作菜单并选择 * 添加数据代理 *。



3. 按照提示在组中创建数据代理。

要获得帮助，请参见以下页面：

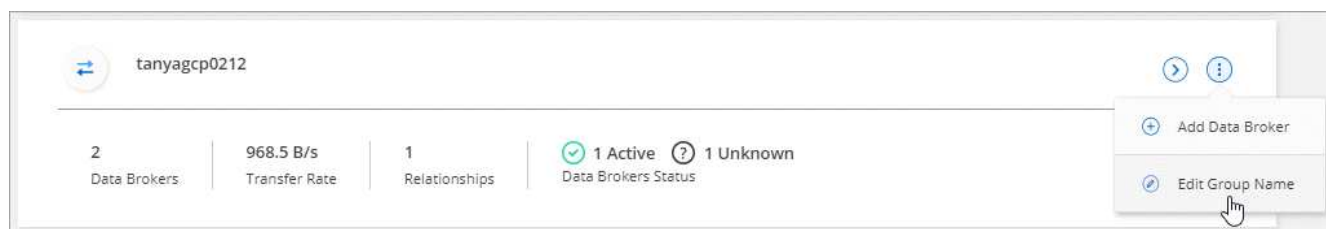
- ["在 AWS 中创建数据代理"](#)
- ["在 Azure 中创建数据代理"](#)
- ["在 Google Cloud 中创建数据代理"](#)
- ["在 Linux 主机上安装数据代理"](#)

编辑组的名称

随时更改数据代理组的名称。

步骤

1. 单击 * 同步 > 管理数据代理 *。
2. 单击操作菜单并选择 * 编辑组名称 *。



3. 输入新名称并单击 * 保存 *。

Cloud Sync 将更新数据代理组的名称。

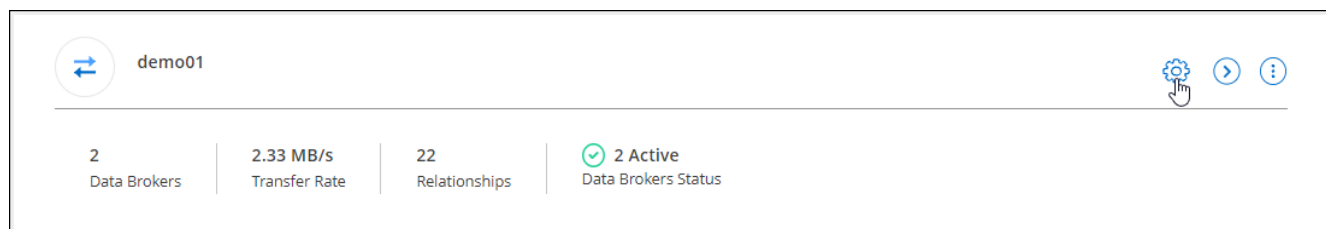
设置统一配置

如果同步关系在同步过程中遇到错误，统一数据代理组的并发性有助于减少同步错误的数量。请注意，更改组的配置可能会降低传输速度，从而影响性能。

建议不要自行更改配置。您应咨询 NetApp，了解何时更改配置以及如何更改配置。

步骤

1. 单击 * 管理数据代理 *。
2. 单击数据代理组的设置图标。



3. 根据需要更改设置，然后单击 * 统一配置 *。

请注意以下事项：

- 您可以选择要更改的设置—不需要一次性更改全部四个设置。
- 将新配置发送到数据代理后，数据代理将自动重新启动并使用新配置。
- 此更改可能需要长达一分钟的时间，此更改将在 Cloud Sync 界面中显示。
- 如果数据代理未运行，则其配置不会更改，因为 Cloud Sync 无法与其通信。数据代理重新启动后，配置将发生更改。
- 设置统一配置后，任何新的数据代理都将自动使用新配置。

在组之间移动数据代理


如果需要提高目标数据代理组的性能，请将数据代理从一个组移动到另一个组。

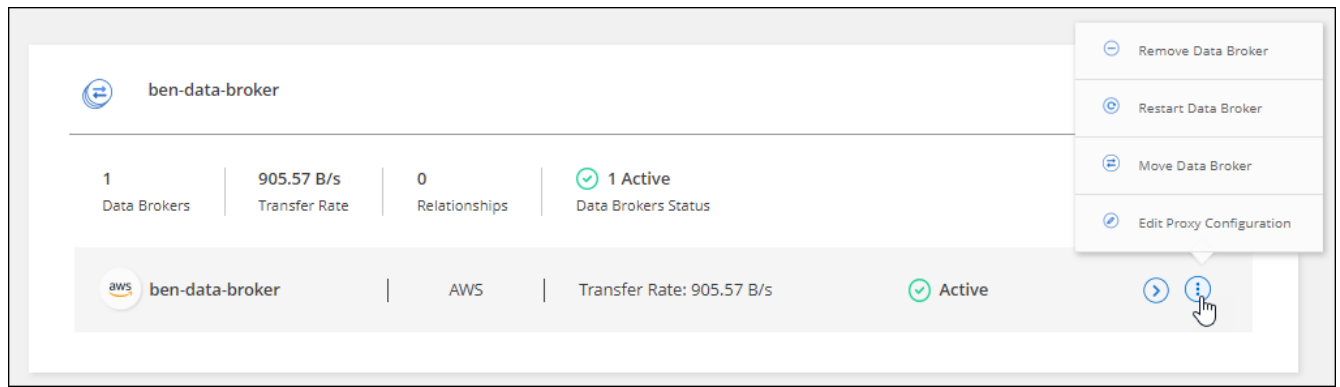
例如，如果某个数据代理不再管理同步关系，您可以轻松地将其移动到另一个管理同步关系的组。

限制

- 如果某个数据代理组正在管理同步关系，并且该组中只有一个数据代理，则无法将该数据代理移动到另一个组。
- 您不能将数据代理移入或移出管理加密同步关系的组。
- 您无法移动当前正在部署的数据代理。

步骤

1. 单击 * 同步 > 管理数据代理 *。
2. 单击  展开组中的数据代理列表。
3. 单击数据代理的操作菜单，然后选择 * 移动数据代理 *。




4. 创建新的数据代理组或选择现有数据代理组。
5. 单击 * 移动 *。

Cloud Sync 会将数据代理移动到新的或现有的数据代理组。如果上一个组中没有其他数据代理，则 Cloud Sync 会将其删除。

更新代理配置

通过添加有关新代理配置的详细信息或编辑现有代理配置来更新数据代理的代理配置。

步骤

1. 单击 * 同步 > 管理数据代理 *。
2. 单击  展开组中的数据代理列表。
3. 单击数据代理的操作菜单，然后选择 * 编辑代理配置 *。
4. 指定有关代理的详细信息：主机名，端口号，用户名和密码。
5. 单击 * 更新 *。

Cloud Sync 会更新数据代理，以使用代理配置进行 Internet 访问。

查看数据代理的配置

您可能希望查看有关数据代理的详细信息，以确定主机名，IP 地址，可用 CPU 和 RAM 等内容。



Cloud Sync 提供了有关数据代理的以下详细信息：

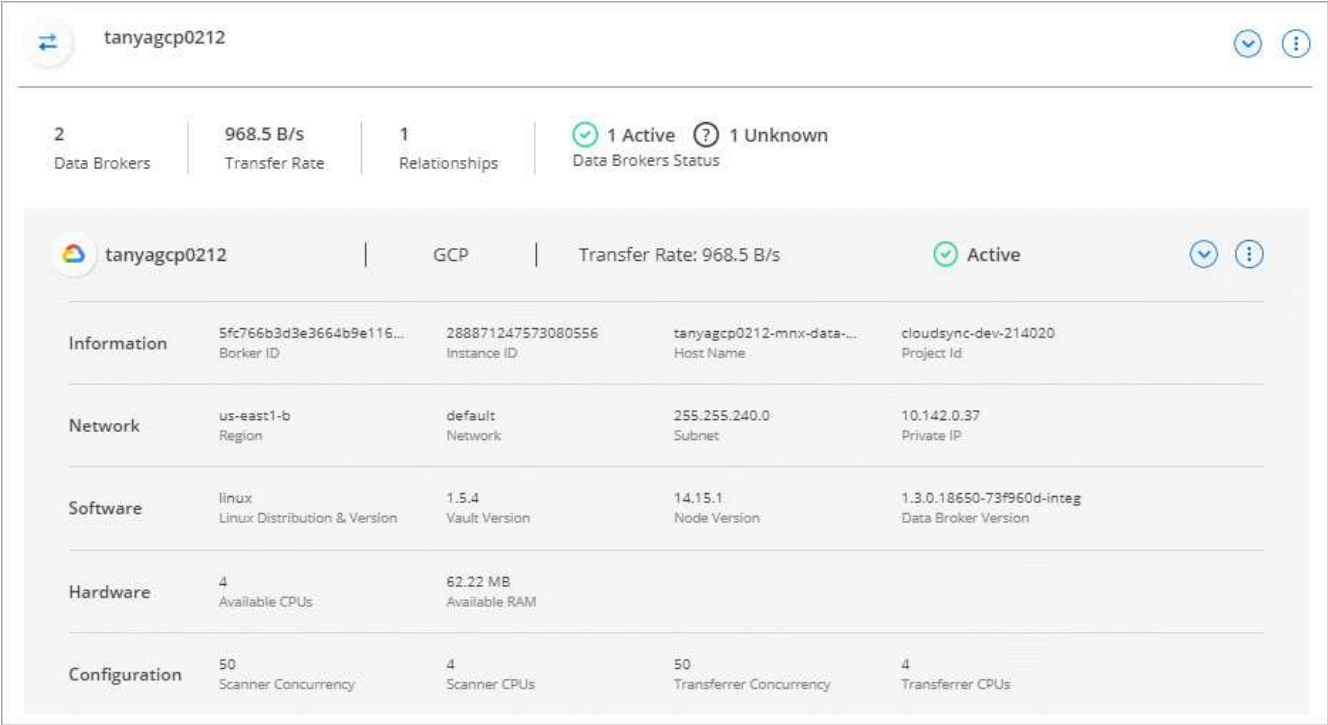
- 基本信息：实例 ID，主机名等
- 网络：区域，网络，子网，专用 IP 等
- 软件：Linux 分发版，数据代理版本等
- 硬件：CPU 和 RAM
- 配置：有关数据代理的两种主要进程的详细信息—扫描程序和传输程序



扫描程序将扫描源和目标，并确定应复制的内容。传输器将执行实际复制。NetApp 人员可能会使用这些配置详细信息来建议可优化性能的操作。

步骤

- 1. 单击 * 同步 > 管理数据代理 * 。
- 2. 单击  展开组中的数据代理列表。
- 3. 单击  查看有关数据代理的详细信息。

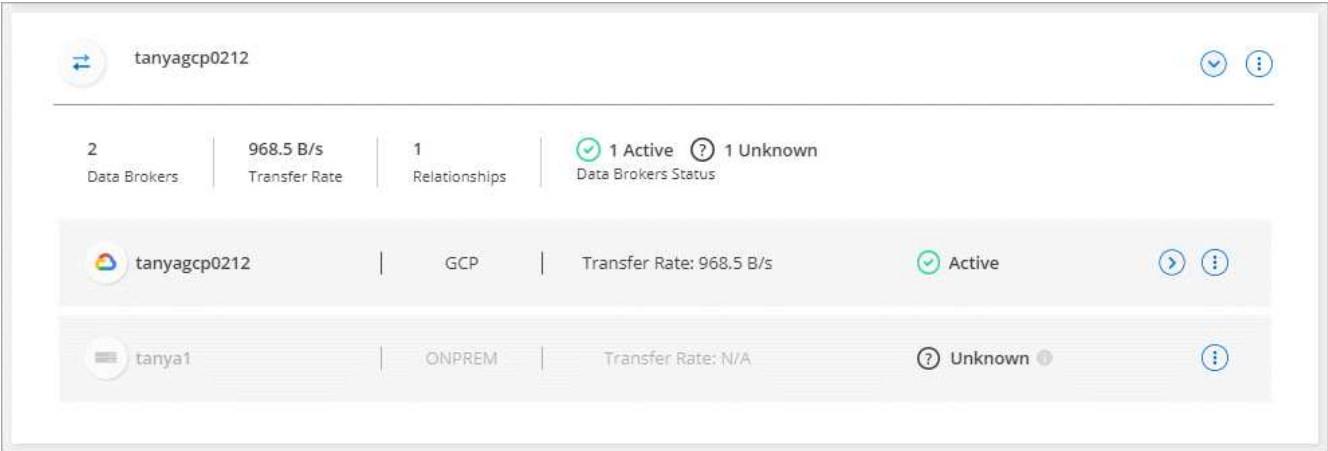


解决数据代理的问题

Cloud Sync 会显示每个数据代理的状态，以帮助您解决问题。

步骤

- 1. 确定状态为 " 未知 " 或 " 失败 " 的任何数据代理。



- 2. 将鼠标悬停在上  图标以查看失败原因。

3. 更正问题描述。

例如，如果数据代理脱机，您可能只需重新启动它，或者如果初始部署失败，您可能需要删除数据代理。


从组中删除数据代理

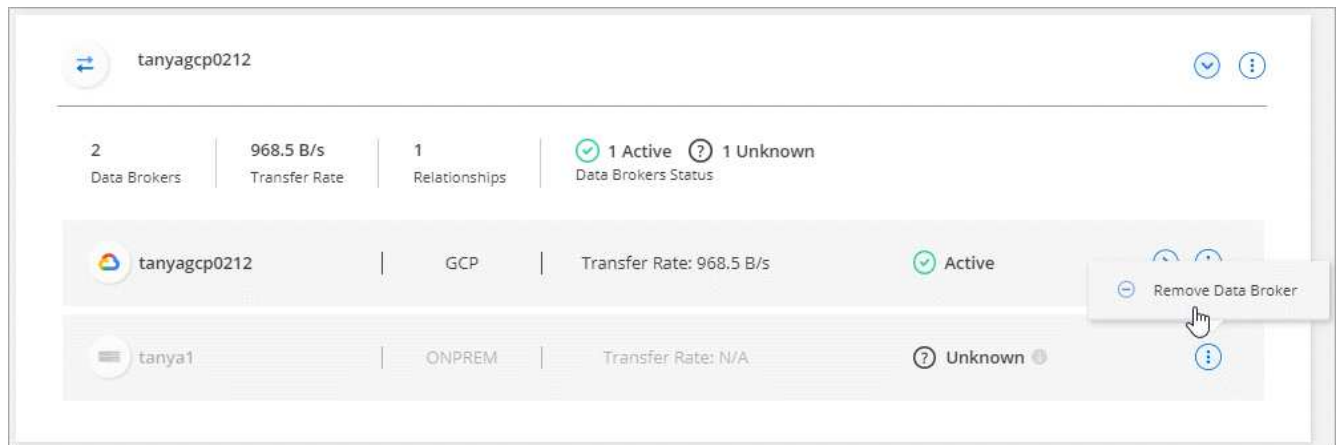
如果不再需要数据代理或初始部署失败，您可以从组中删除该数据代理。此操作仅从 Cloud Sync 的记录中删除数据代理。您需要手动删除数据代理以及任何其他云资源。

您应了解的事项

- 当您从组中删除最后一个数据代理时，Cloud Sync 将删除组。
- 如果某个关系正在使用某个组，则不能从该组中删除最后一个数据代理。

步骤

1. 单击 * 同步 > 管理数据代理 *。
2. 单击  展开组中的数据代理列表。
3. 单击数据代理的操作菜单，然后选择 * 删除数据代理 *。



4. 单击 * 删除数据代理 *。

Cloud Sync 将从组中删除数据代理。

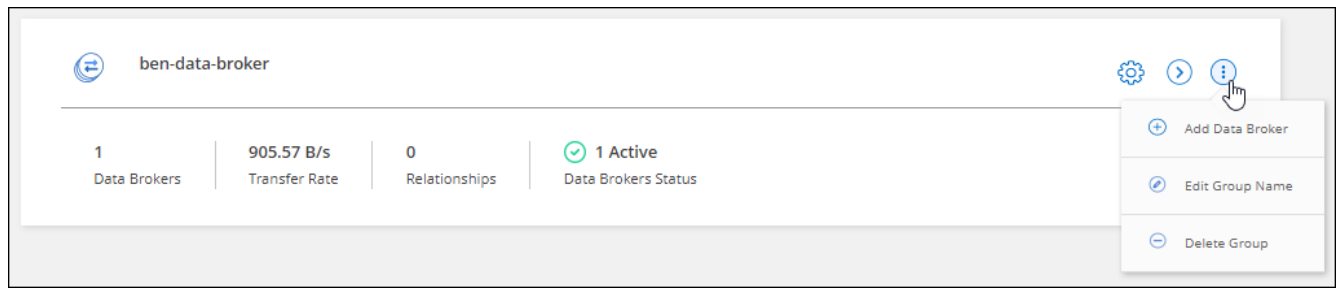
删除数据代理组

如果某个数据代理组不再管理任何同步关系，您可以删除该组，从而从 Cloud Sync 中删除所有数据代理。

Cloud Sync 删除的数据代理仅会从 Cloud Sync 的记录中删除。您需要从云提供商和任何其他云资源中手动删除数据代理实例。

步骤

1. 单击 * 同步 > 管理数据代理 *。
2. 单击操作菜单并选择 * 删除组 *。



3. 要进行确认，请输入组名称，然后单击 * 删除组 *。

Cloud Sync 将删除数据代理并删除组。

创建和查看报告以调整配置

创建和查看报告以获取信息，您可以在 NetApp 人员的帮助下使用这些信息来调整数据代理的配置并提高性能。

每个报告都提供有关同步关系中某个路径的详细信息。例如，文件系统的报告显示了目录和文件的数量，文件大小分布，目录的深度和宽度等。

创建报告

每次创建报告时，Cloud Sync 都会扫描路径，然后将详细信息编译为报告。

步骤

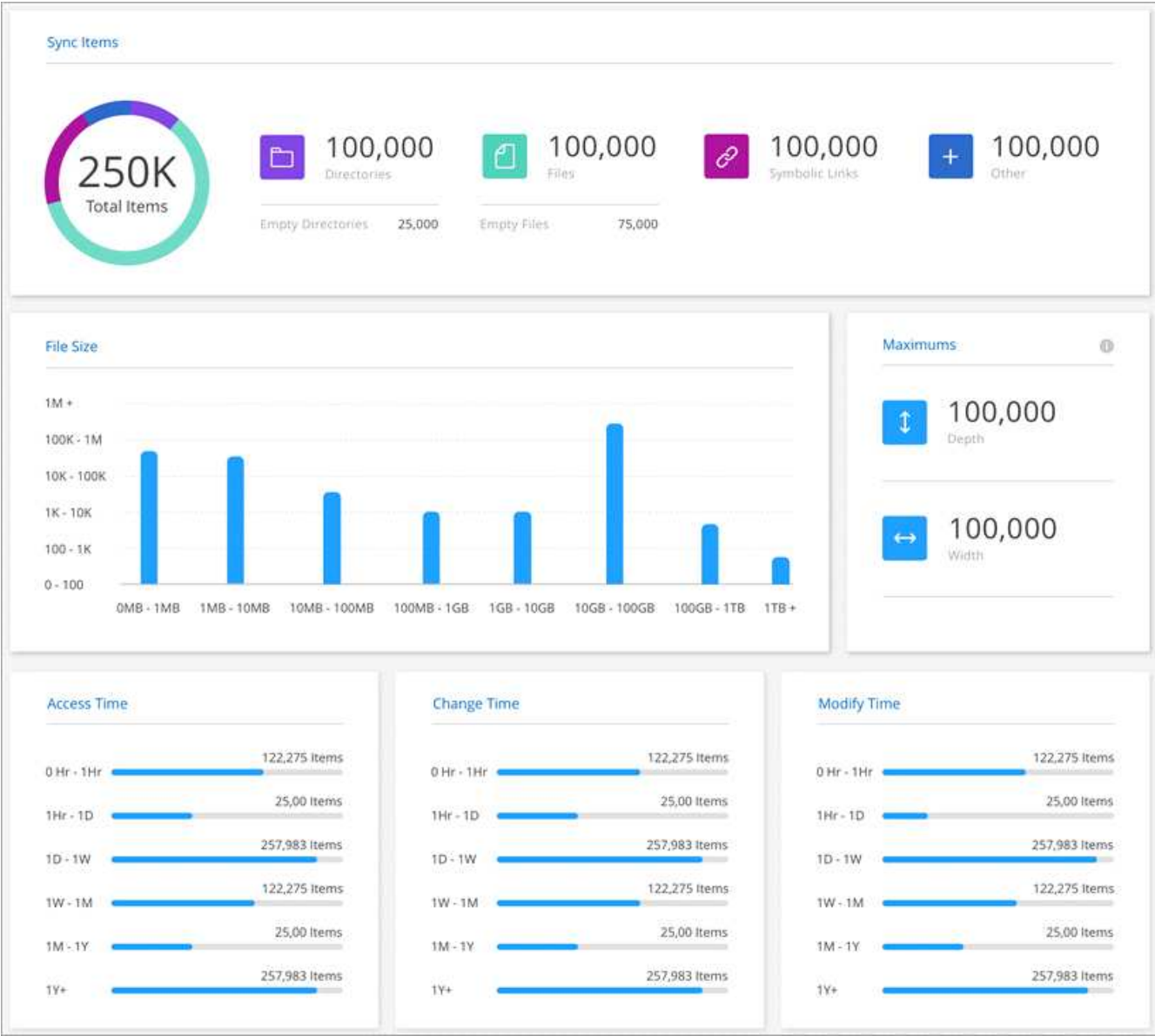
1. 单击 * 同步 > 报告 *。

每个同步关系中的路径（源或目标）显示在一个表中。

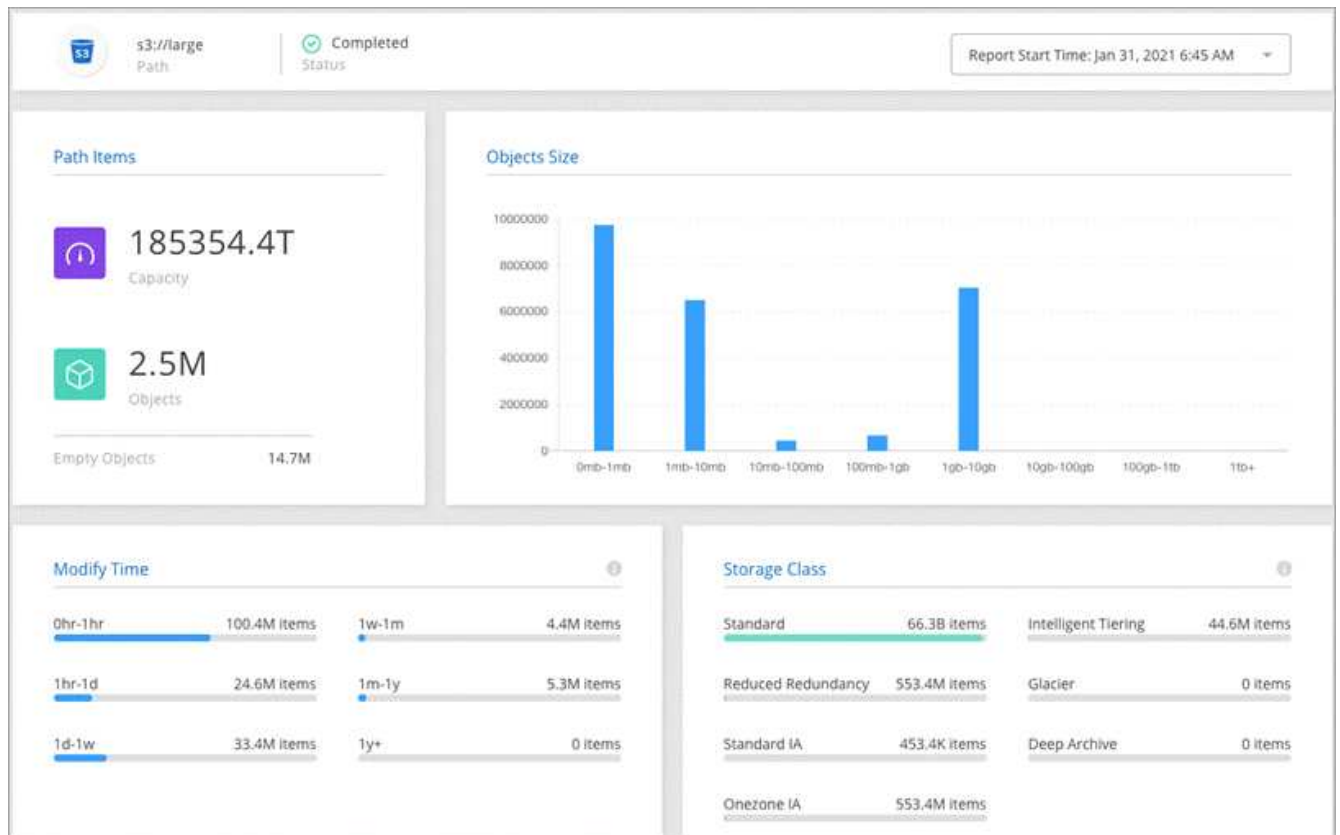
2. 在 * 报告操作 * 列中，转到特定路径并单击 * 创建 *，或者单击操作菜单并选择 * 新建 *。

3. 报告准备就绪后，单击操作菜单并选择 * 查看 *。

下面是文件系统路径的示例报告。



下面是对象存储示例报告。

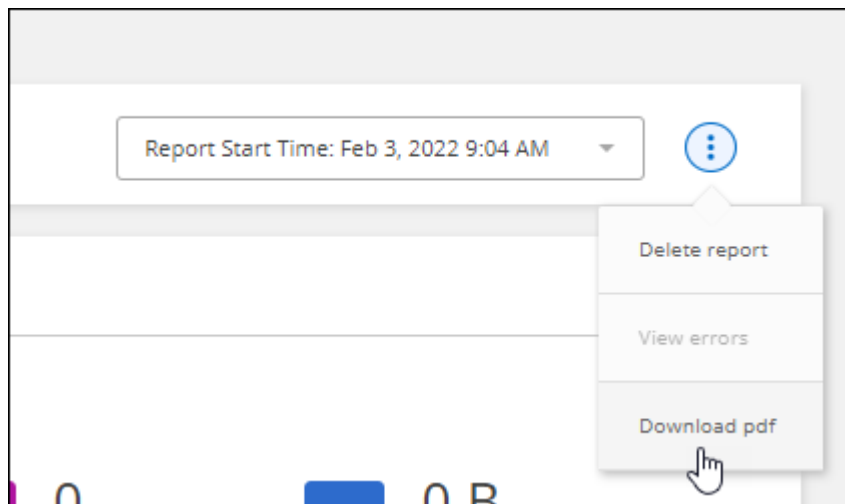


下载报告

您可以下载 PDF 格式的报告，以便脱机查看或共享它。

步骤

1. 单击 * 同步 > 报告 *。
2. 在 * 报告操作 * 列中，单击操作菜单并选择 * 查看 *。
3. 在报告右上角，单击操作菜单并选择 * 下载 pdf*。



查看报告错误

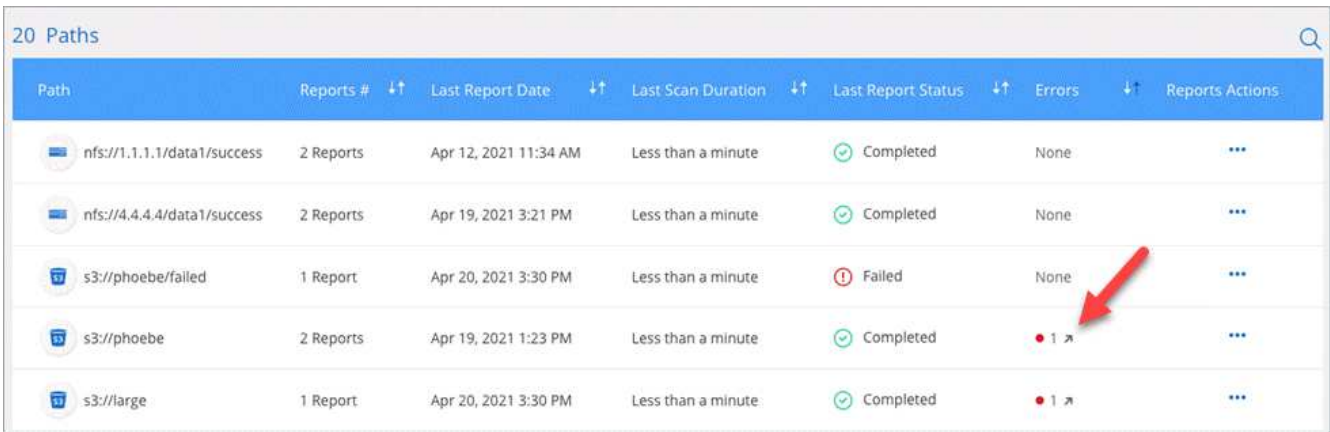
路径表可确定最新报告中是否存在任何错误。错误标识了 Cloud Sync 在扫描路径时面临的问题描述。

例如，报告可能包含权限被拒绝错误。此类错误可能会影响 Cloud Sync 扫描整个文件和目录集的能力。

查看错误列表后，您可以解决问题并再次运行报告。

步骤

1. 单击 * 同步 > 报告 *。
2. 在 * 错误 * 列中，确定报告中是否存在任何错误。
3. 如果存在错误，请单击错误数旁边的箭头。



Path	Reports #	Last Report Date	Last Scan Duration	Last Report Status	Errors	Reports Actions
nfs://1.1.1.1/data1/success	2 Reports	Apr 12, 2021 11:34 AM	Less than a minute	Completed	None	...
nfs://4.4.4.4/data1/success	2 Reports	Apr 19, 2021 3:21 PM	Less than a minute	Completed	None	...
s3://phoebe/failed	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Failed	None	...
s3://phoebe	2 Reports	Apr 19, 2021 1:23 PM	Less than a minute	Completed	1	...
s3://large	1 Report	Apr 20, 2021 3:30 PM	Less than a minute	Completed	1	...

4. 使用错误中的信息更正问题描述。

解决问题描述后，下次运行报告时不应显示此错误。

删除报告

您可以删除报告中包含您修复的错误，或者如果报告与您删除的同步关系相关。

步骤

1. 单击 * 同步 > 报告 *。
2. 在 * 报告操作 * 列中，单击某个路径的操作菜单，然后选择 * 删除最后一个报告 * 或 * 删除所有报告 *。
3. 确认要删除一个或多个报告。

卸载数据代理

如果需要，请运行卸载脚本以删除数据代理以及在安装数据代理时创建的软件包和目录。

步骤

1. 登录到数据代理主机。
2. 更改为数据代理目录：`/opt/netapp/databroker`

3. 运行以下命令：

```
chmod +x uninstaller-DataBroker.sh `./uninstaller-DataBroker.sh`
```

4. 按 'y' 确认卸载。

云同步 API

通过 Web UI 提供的 Cloud Sync 功能也可通过 RESTful API 获得。

入门

要开始使用 Cloud Sync API，您需要获取用户令牌和您的 Cloud Central 帐户 ID。在进行 API 调用时，您需要将令牌和帐户 ID 添加到授权标题中。

步骤

1. 从 NetApp Cloud Central 获取用户令牌。

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
  "username": "<user_email>",
  "scope": "profile",
  "audience": "https://api.cloud.netapp.com",
  "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
  "grant_type": "password",
  "password": "<user_password>"
}
```

2. 获取 Cloud Central 帐户 ID。

```
GET https://api.cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

此 API 将返回如下响应：

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. 在每个 API 调用的 Authorization 标头中添加用户令牌和帐户 ID。

◦ 示例 *

以下示例显示了在 Microsoft Azure 中创建数据代理的 API 调用。您只需将 <user_token> 和 <AccountID> 替换为您在上述步骤中获得的令牌和 ID 即可。

```
POST https://api.cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

令牌过期时应执行什么操作？

来自 NetApp Cloud Central 的用户令牌具有到期日期。要刷新令牌、您需要再次调用步骤 1 中的 API。

API 响应包括一个 "expires_in" 字段、该字段指出令牌何时过期。

API 参考

有关每个 Cloud Sync API 的文档，请参见 <https://api.cloudsync.netapp.com/docs>。

使用列表 API

列表 API 是异步 API，因此不会立即返回结果（例如：get /data-brokers/ { id } /list-nfs-export-folders 和 get /data-brokers/ { id } /list-s3-basses）。服务器的唯一响应是 HTTP 状态 202。要获得实际结果，您必须使用 GET /messages/client API。

步骤

1. 调用要使用的列表 API。
2. 使用 get /messages/client API 查看操作结果。
3. 使用相同的 API，方法是将其附加到刚刚收到的 ID：get
`http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

请注意，每次调用 get /messages/client API 时，ID 都会发生更改。

◦ 示例 *

调用 list-s3-bates API 时，不会立即返回结果：

```
GET http://api.cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

结果是 HTTP 状态代码 202、这意味着邮件已被接受、但尚未处理。

要获得操作的结果，您需要使用以下 API：

```
GET http://api.cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

结果是一个数组，其中一个对象包含 ID 字段。ID 字段表示服务器发送的最后一条消息。例如：

```
[
  {
    "header": {
      "requestId": "init",
      "clientId": "init",
      "agentId": "init"
    },
    "payload": {
      "init": {}
    },
    "id": "5801"
  }
]
```

现在，您可以使用刚才收到的 ID 进行以下 API 调用：

```
GET
http://api.cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

结果是一组消息。每个消息内部都是一个有效负载对象，该对象由操作的名称（作为密钥）及其结果（作为值）组成。例如：

```
[
  {
    "payload": {
      "list-s3-buckets": [
        {
          "tags": [
            {
              "Value": "100$",
              "Key": "price"
            }
          ],
          "region": {
            "displayName": "US West (Oregon)",
            "name": "us-west-2"
          },
          "name": "small"
        }
      ]
    },
    "header": {
      "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
      "clientId": "5beb032f548e6e35f4ed1ba9",
      "agentId": "5bed61f4489fb04e34a9aac6"
    },
    "id": "5802"
  }
]
```

概念

许可概述

在 14 天免费试用结束后、有两种方式可以支付同步关系的费用。第一种选择是从 AWS 或 Azure 订阅“按需购买、渐进购买”或“每年支付”。第二种选择是直接从 NetApp 购买许可证。

市场订阅

通过从 AWS 或 Azure 订阅 Cloud Sync 服务、您可以按小时付费或每年付款。"[您可以通过 AWS 或 Azure 订阅](#)"，具体取决于您要向何处付费。

每小时订阅

使用每小时按需购买订阅，您将根据创建的同步关系数量按小时付费。

- "[查看 Azure 中的定价](#)"
- "[在 AWS 中查看按需购买定价](#)"

按年订阅

年度订阅为 20 种同步关系提供许可、您可以预先支付费用。如果您的同步关系超过 20 个，并且您已通过 AWS 订阅，则可以按小时支付额外的关系费用。

["查看 AWS 中的年度定价"](#)

来自 NetApp 的许可证

另一种提前支付同步关系费用的方法是直接从 NetApp 购买许可证。每个许可证最多可创建 20 个同步关系。

您可以将这些许可证与 AWS 或 Azure 订阅一起使用。例如，如果您有 25 个同步关系、则可以使用许可证支付前 20 个同步关系的费用、然后从 AWS 或 Azure 中按原样支付剩余的 5 个同步关系的费用。

["了解如何购买许可证并将其添加到 Cloud Sync 中。"](#)

许可条款

购买“将您自己的许可证（BYOL）带到云同步服务”的客户应了解与许可证权利相关的限制。

- 客户有权在自交付之日起一年内利用 BYOL 许可证。
- 客户有权利用 BYOL 许可证在源和目标之间建立总共不超过 20 个单独的连接（每个连接均为“同步关系”）。
- 无论客户是否已达到 20 个同步关系限制、客户的权利在一年许可期限结束时到期。
- 如果客户选择续订其许可证、则与以前的许可证授权关联的未使用同步关系不会滚动到许可证续订。

数据隐私

NetApp 无法访问您在使用 Cloud Sync 服务时提供的任何凭据。凭据直接存储在驻留在网络中的数据代理计算机上。

根据您的配置、在创建新关系时，Cloud Sync 可能会提示您输入凭据。例如，在设置包含 SMB 服务器的关系时，或者在 AWS 中部署数据代理时。

这些凭据始终直接保存到数据代理本身。数据代理驻留在您网络中的计算机上，无论该计算机位于内部还是位于您的云帐户中。NetApp 从不能获得凭据。

凭据在数据代理计算机上使用 HashiCorp Vault 进行本地加密。

Cloud Sync 技术常见问题解答

如果您只是在寻找一个问题的快速答案，此常见问题解答将会有所帮助。

入门

以下问题与 Cloud Sync 入门相关。

Cloud Sync 如何工作？

Cloud Sync 使用 NetApp 数据代理软件将数据从源同步到目标（称为 *sync relationship*）。

数据代理组控制源与目标之间的同步关系。建立同步关系后，Cloud Sync 会分析您的源系统并将其分成多个复制流以推入选定的目标数据。

初始副本之后，服务将根据您设置的计划同步所有更改的数据。

14 天免费试用如何工作？

14 天免费试用将在您注册 Cloud Sync 服务时开始。对于您创建的 14 天 Cloud Sync 关系，您无需支付 NetApp 费用。但是，您部署的任何数据代理的所有资源费用仍然适用。

Cloud Sync 的成本是多少？

使用 Cloud Sync 需要两种类型的成本：服务费用和资源费用。

- 服务费用 *

对于按需购买的定价，根据您的创建的同步关系数量，Cloud Sync 服务的收费是每小时一次的。

- ["在 AWS 中查看按需购买定价"](#)
- ["查看 AWS 中的年度定价"](#)
- ["查看 Azure 中的定价"](#)

您的 NetApp 代表也可以获得 Cloud Sync 许可证。每个许可证可在 12 个月内实现 20 个同步关系。

["了解有关许可证的更多信息。"](#)



Cloud Volumes Service 和 Azure NetApp Files 均可免费使用 Cloud Sync 关系。

- 资源费用 *

资源费用与在云中运行数据代理的计算和存储成本相关。

如何对 **Cloud Sync** 进行收费？

在 14 天免费试用结束后、有两种方式可以支付同步关系的费用。第一种选择是从 AWS 或 Azure 订阅、这使您可以按需付费或每年付款。第二种选择是直接从 NetApp 购买许可证。

是否可以在云之外使用 **Cloud Sync** ？

是的、您可以在非云架构中使用 Cloud Sync 。源和目标可以驻留在内部，数据代理软件也可以驻留在内部。

请注意以下有关在云之外使用云同步的要点：

- 对于内部同步，可通过 NetApp StorageGRID 获得私有 Amazon S3 数据段。
- 数据代理组需要 Internet 连接才能与 Cloud Sync 服务进行通信。
- 如果您不直接从 NetApp 购买许可证，则需要一个 AWS 或 Azure 帐户才能为 PAYGO Cloud Sync 服务计费。

什么是数据代理组？

每个数据代理都属于一个数据代理组。将数据代理分组在一起有助于提高同步关系的性能。

如何访问 **Cloud Sync** ？

Cloud Sync 可从 Cloud Manager 的 * 同步 * 选项卡中访问。

支持的源和目标

以下问题与同步关系中支持的源和目标有关。

Cloud Sync 支持哪些源和目标？

Cloud Sync 支持多种不同类型的同步关系。 ["查看整个列表。"](#)

Cloud Sync 支持哪些版本的 **NFS** 和 **SMB** ？

Cloud Sync 支持 NFS 版本 3 和更高版本以及 SMB 版本 1 和更高版本。

["了解有关同步要求的更多信息。"](#)

当 **Amazon S3** 成为目标时、能否将数据分层到特定的 **S3** 存储类？

是的、当 AWS S3 为目标时，您可以选择特定的 S3 存储类：

- 标准（这是默认类）
- Intelligent-Hierarchy
- 标准—不经常访问
- 一个 ZONE 不常访问
- 冰河
- Glacier 深度存档

Azure Blob Storage 的存储层如何？

当 BLOB 容器是目标容器时，可以选择特定的 Azure Blob 存储层：

- 热存储
- 冷却存储

您是否支持 Google Cloud 存储层？

是的，当 Google Cloud Storage 存储分段为目标时，您可以选择特定的存储类：

- 标准
- 近线
- 冷线
- 归档

网络

以下问题与 Cloud Sync 的网络要求有关。

Cloud Sync 的网络要求是什么？

Cloud Sync 环境要求数据代理组通过选定协议或对象存储 API（Amazon S3，Azure Blob，IBM 云对象存储）与源和目标连接。

此外，数据代理组需要通过端口 443 建立出站 Internet 连接，以便可以与 Cloud Sync 服务进行通信并联系其他一些服务和存储库。

有关详细信息：["查看网络要求："](#)。

是否可以将代理服务器与数据代理结合使用？

是的。

Cloud Sync 支持具有或不具有基本身份验证的代理服务器。如果在部署数据代理时指定代理服务器，则数据代理的所有 HTTP 和 HTTPS 流量都将通过代理路由。请注意，NFS 或 SMB 等非 HTTP 流量不能通过代理服务器路由。

唯一的代理服务器限制是在 NFS 或 Azure NetApp Files 同步关系中使用传输中数据加密时。加密数据通过 HTTPS 发送，不能通过代理服务器路由。

数据同步

以下问题与数据同步的工作原理有关。

同步发生的频率是多少？

默认计划设置为每日同步。初始同步后，您可以：

- 将同步计划修改为所需的天数、小时数或分钟数
- 禁用同步计划
- 删除同步计划（不会丢失任何数据；只会删除同步关系）

最低同步计划是什么？

您可以计划一个关系以每 1 分钟同步一次数据。

文件无法同步时，数据代理组是否会重试？还是超时？

当单个文件无法传输时，数据代理组不会超时。相反，数据代理组会重试 3 次，然后跳过该文件。重试值可在同步关系的设置中进行配置。

["了解如何更改同步关系的设置。"](#)

如果我有一个非常大的数据集会怎样？

如果一个目录包含 60 万个或更多文件，请发送电子邮件至：ng-cloudsync-support@netapp.com，以便我们帮助您配置数据代理组来处理有效负载。我们可能需要向数据代理组添加更多内存。

请注意，挂载点中的文件总数没有限制。对于包含 600,000 个或更多文件的大型目录，无论其在层次结构中的级别如何（顶层目录或子目录），都需要额外的内存。

安全性

以下与安全相关的问题。

云同步是否安全？

是的。所有 Cloud Sync 服务网络连接均使用完成 ["Amazon Simple Queue Service（SQS）"](#)。

数据代理组与 Amazon S3，Azure Blob，Google Cloud Storage 和 IBM Cloud Object Storage 之间的所有通信均通过 HTTPS 协议完成。

如果您将 Cloud Sync 与内部（源或目标）系统结合使用，建议使用以下连接选项：

- AWS Direct Connect、Azure ExpressRoute 或 Google Cloud 互连连接（非 Internet 路由）（并且只能与您指定的云网络通信）
- 内部网关设备与云网络之间的 VPN 连接
- 为了通过 S3 Battle、Azure Blob Storage 或 Google Cloud Storage 实现额外的安全数据传输、可以建立 Amazon 私有 S3 端点、Azure 虚拟网络服务端点或私有 Google Access。

其中任何一种方法都可以在内部 NAS 服务器和 Cloud Sync 数据代理组之间建立安全连接。

数据是否通过 **Cloud Sync** 加密？

- Cloud Sync 支持在源 NFS 服务器和目标 NFS 服务器之间进行数据流加密。"[了解更多信息。](#)"。
- 对于 SMB，Cloud Sync 支持在服务器端加密的 SMB 3.0 和 3.11 数据。Cloud Sync 会将加密数据从源复制到数据保持加密的目标。

Cloud Sync 无法对 SMB 数据本身进行加密。

- 如果 Amazon S3 存储分段是同步关系中的目标，您可以选择是使用 AWS KMS 加密还是 AES-256 加密启用数据加密。

权限

以下问题与数据权限相关。

SMB 数据权限是否与目标位置同步？

您可以设置 Cloud Sync 以保留源 SMB 共享和目标 SMB 共享之间以及从源 SMB 共享到对象存储（ONTAP S3 除外）的访问控制列表（ACL）。



Cloud Sync 不支持将 ACL 从对象存储复制到 SMB 共享。

"[了解如何在 SMB 共享之间复制 ACL。](#)"。

NFS 数据权限是否与目标位置同步？

Cloud Sync 会自动在 NFS 服务器之间复制 NFS 权限，如下所示：

- NFS 版本 3：Cloud Sync 会复制权限和用户组所有者。
- NFS 版本 4：Cloud Sync 会复制 ACL。

对象存储元数据

对于以下类型的同步关系，Cloud Sync 会将对象存储元数据从源复制到目标：

- Amazon S3 → Amazon S3 ¹
- Amazon S3 → StorageGRID
- StorageGRID → Amazon S3
- StorageGRID → StorageGRID
- StorageGRID → Google 云存储
- Google 云存储 → StorageGRID ¹
- Google Cloud Storage → IBM Cloud Object Storage ¹
- Google Cloud Storage → Amazon S3 ¹
- Amazon S3 → Google Cloud Storage

- IBM Cloud Object Storage → Google Cloud Storage
- StorageGRID → IBM 云对象存储
- IBM 云对象存储 → StorageGRID
- IBM Cloud Object Storage → IBM Cloud Object Storage

¹ 对于这些同步关系，您需要 ["创建同步关系时启用设置"](#)。

性能

以下问题与云同步性能有关。

同步关系的进度指示符代表什么？

同步关系显示数据代理组的网络适配器的吞吐量。如果使用多个数据代理提高同步性能、则吞吐量是所有流量的总和。此吞吐量每 20 秒刷新一次。

我遇到了性能问题。我们是否可以限制并发传输的数量？

如果文件非常大（每个有多个 Tib），则可能需要很长时间才能完成传输过程，并且性能可能会受到影响。

限制并发传输的数量有助于实现这一目标。mailto：ng-cloudsync-support@netapp.com。

为什么使用 **Azure NetApp Files** 时性能较低？

在与 Azure NetApp Files 同步数据时，如果磁盘服务级别为标准，则可能会出现故障和性能问题。

将服务级别更改为高级或超高级以提高同步性能。

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

为什么我在使用适用于 **AWS** 的 **Cloud Volumes Service** 时遇到性能低下的问题？

在将数据同步到云卷或从云卷同步时，如果云卷的性能级别是标准的、则可能会遇到故障和性能问题。

将服务级别更改为“高级”或“至尊”以提高同步性能。

一个组需要多少个数据代理？

创建新关系时，您可以从组中的单个数据代理开始（除非您选择了属于加速同步关系的现有数据代理）。在许多情况下、单个数据代理可以满足同步关系的性能要求。否则，您可以通过向组中添加其他数据代理来提高同步性能。但是，您应该首先检查可能影响同步性能的其他因素。

多个因素会影响数据传输性能。由于网络带宽、延迟和网络拓扑以及数据代理 VM 规格和存储系统性能的影响、整体同步性能可能会受到影响。例如，一个组中的单个数据代理可以达到 100 MB/ 秒，而目标上的磁盘吞吐量可能仅允许 64 MB/ 秒因此，数据代理组会不断尝试复制数据，但目标无法达到数据代理组的性能。

因此，请务必检查网络的性能以及目标上的磁盘吞吐量。

然后，您可以考虑向组添加额外的数据代理来共享该关系的负载，从而加快同步性能。 ["了解如何提高同步性能"](#)。

删除内容

以下问题与从源和目标删除同步关系和数据有关。

如果删除了我的云同步关系，会发生什么情况？

删除关系将停止所有将来的数据同步并终止付款。与目标同步的任何数据均保持原样。

如果从源服务器中删除某些内容会发生什么情况？它是否也从目标中删除？

默认情况下，如果您具有活动同步关系、则在下次同步时不会从目标中删除源服务器上已删除的项目。但是，每个关系的同步设置中都有一个选项，您可以在其中定义：如果从源中删除了目标位置中的文件，则 Cloud Sync 将删除这些文件。

["了解如何更改同步关系的设置。"](#)

如果我从目标中删除某些内容会发生什么情况？它是否也从我的来源中删除？

如果从目标中删除了项目，则不会从源中删除该项目。这种关系是从源到目标的单向关系。在下一个同步周期中、Cloud Sync 会将源与目标进行比较、确定缺少该项目、然后 Cloud Sync 会将其从源再次复制到目标。

故障排除

["NetApp 知识库：Cloud Sync 常见问题解答：支持和故障排除"](#)

数据代理深入探讨

以下问题与数据代理有关。

您能否解释数据代理的架构？

当然。以下是最重要的一点：

- 数据代理是在 Linux 主机上运行的一个 node.js 应用程序。
- Cloud Sync 按以下方式部署数据代理：
 - AWS：来自 AWS Cloudformation 模板
 - Azure：来自 Azure Resource Manager
 - Google：来自 Google Cloud 部署管理器
 - 如果您使用自己的 Linux 主机、则需要手动安装软件
- 数据代理软件会自动升级到最新版本。
- 数据代理使用 AWS SQS 作为可靠、安全的通信通道以及进行控制和监控。SQS 还提供持久性层。
- 您可以向组中添加其他数据代理，以提高传输速度并增加高可用性。如果一个数据代理出现故障，则具有服务弹性。

知识和支持

注册以获得支持

!!!

获取帮助

!!!

法律声明

""

""

"云同步注意事项"

Copyright Information

Copyright © 2022 NetApp, Inc. All rights reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means-graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system-without prior written permission of the copyright owner.

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

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. 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).

Trademark Information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.