



Cloud Backup 文档

Cloud Backup

NetApp
June 20, 2022

目录

Cloud Backup 文档	1
Cloud Backup 的新增功能	2
2022年6月14日	2
2022年6月8日	2
2022年5月2日	3
2022 年 4 月 4 日	3
2022 年 3 月 3 日	4
2022 年 2 月 14 日	4
2022 年 1 月 2 日	4
2021 年 11 月 28 日	5
2021 年 11 月 5 日	5
2021 年 10 月 4 日	5
2021 年 9 月 2 日	6
2021 年 8 月 1 日	6
2021 年 7 月 7 日	6
2021 年 6 月 7 日	7
2021 年 5 月 5 日	7
入门	8
了解 Cloud Backup	8
为 Cloud Backup 设置许可	10
备份和还原 ONTAP 数据	15
使用云备份保护 ONTAP 集群数据	15
将 Cloud Volumes ONTAP 数据备份到 Amazon S3	21
将内部 ONTAP 数据备份到 Amazon S3	27
将内部 ONTAP 数据备份到 StorageGRID	39
管理 ONTAP 系统的备份	45
从备份文件还原 ONTAP 数据	60
备份和还原 Kubernetes 数据	76
使用 Cloud Backup 保护 Kubernetes 集群数据	76
将 Kubernetes 永久性卷数据备份到 Amazon S3	79
管理 Kubernetes 系统的备份	85
从备份文件还原 Kubernetes 数据	94
备份和还原内部应用程序数据	97
保护内部应用程序数据	97
将内部应用程序数据备份到云	98
管理应用程序的保护	101
还原应用程序数据	103
备份和还原虚拟机数据	106
保护虚拟机数据	106

将数据存储库备份到云	108
管理虚拟机的保护	109
从云还原虚拟机	111
Cloud Backup API	112
入门	112
使用API的示例	114
API 参考	116
参考	117
AWS S3 归档存储类和还原检索时间	117
Azure 归档层和还原检索时间	118
知识和支持	120
注册以获得支持	120
获取帮助	121
法律声明	123
版权	123
商标	123
专利	123
隐私政策	123
开放源代码	123

Cloud Backup 文档

Cloud Backup 的新增功能

了解 Cloud Backup 中的新增功能。

2022年6月14日

增加了对在无法访问Internet的站点中备份内部ONTAP 集群数据的支持

如果您的内部ONTAP 集群位于无法访问Internet的站点中、也称为非公开站点或脱机站点、则现在您可以使用Cloud Backup将卷数据备份到同一站点中的NetApp StorageGRID 系统。此功能还要求在脱机站点中部署Cloud Manager Connector (版本3.9.19或更高版本)。

"请参见如何在脱机站点中安装Connector"。 <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html>["了解如何将ONTAP 数据备份到脱机站点中的StorageGRID"]。

2022年6月8日

适用于虚拟机的Cloud Backup 1.1.0现已正式上市

您可以通过将适用于VMware vSphere的SnapCenter 插件与Cloud Manager集成来保护虚拟机上的数据。您可以将数据存储库备份到云、并将虚拟机轻松还原回适用于VMware vSphere的内部部署SnapCenter 插件。

"了解有关保护虚拟机到云的更多信息"。

ONTAP 浏览和还原功能不需要云还原实例

以前从S3和Blob存储执行文件级浏览和还原操作需要一个单独的Cloud Restore实例/虚拟机。此实例在不使用时关闭、但在还原文件时仍会增加一些时间和成本。此功能已被一个免费容器所取代、此容器可在需要时部署在Connector上。它具有以下优势：

- 文件级还原操作不会增加成本
- 文件级还原操作速度更快
- 支持在内部安装Connector时从云中对文件执行浏览和还原操作

请注意、如果您先前使用了Cloud Restore实例/VM、则该实例/VM将自动删除。Cloud Backup进程将每天运行一次、以删除所有旧的Cloud Restore实例。此更改是完全透明的—不会对数据产生任何影响、您也不会注意到备份或还原作业发生了任何更改。

浏览并还原对Google Cloud和StorageGRID 存储中文件的支持

现在、通过添加用于浏览和还原操作的容器(如上所述)、可以从存储在Google Cloud和StorageGRID 系统中的备份文件执行文件还原操作。现在、浏览和还原可用于在所有公有云提供商之间以及从StorageGRID 还原文件。"请参见如何使用浏览和放大功能；还原ONTAP 备份中的卷和文件"。

拖放以启用Cloud Backup到S3存储

如果用于备份的Amazon S3目标作为工作环境存在于Canvas上、则可以将本地ONTAP 集群或Cloud Volumes

ONTAP 系统(安装在AWS中)拖动到Amazon S3工作环境中以启动设置向导。

自动将备份策略应用于Kubernetes集群中新创建的卷

如果您在激活Cloud Backup后向Kubernetes集群添加了新的永久性卷、则在过去、您需要记住为这些卷配置备份。现在、您可以选择将自动应用于新创建的卷的策略 "[从_Backup Settings_页面](#)" 适用于已激活Cloud Backup的集群。

Cloud Backup API现在可用于管理备份和还原操作

这些API可从[获取 https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html](https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html)。请参见 "[此页面](#)" 有关API的概述。

2022年5月2日

现在、Google Cloud Storage中的备份文件支持搜索和还原

4月份、在AWS中存储备份文件的用户开始使用"搜索和还原"方法来还原卷和文件。现在、将备份文件存储在Google Cloud Storage中的用户可以使用此功能。 "[请参见如何使用搜索和放大器还原卷和文件](#)"。

配置要自动应用于Kubernetes集群中新创建的卷的备份策略

如果您在激活Cloud Backup后向Kubernetes集群添加了新的永久性卷、则在过去、您需要记住为这些卷配置备份。现在、您可以选择将自动应用于新创建的卷的策略。在为新Kubernetes集群激活Cloud Backup时、此选项可在设置向导中使用。

Cloud Backup现在需要获得许可证、才能在工作环境中激活

在Cloud Backup中实施许可的方式方面、有一些变化：

- 您必须先从云提供商处注册PAYGO Marketplace订阅、或者从NetApp购买BYOL许可证、然后才能激活Cloud Backup。
- 30天免费试用版仅在使用云提供商提供的PAYGO订阅时可用、而在使用BYOL许可证时不可用。
- 免费试用从Marketplace订阅开始的那一天开始。例如、如果在对Cloud Volumes ONTAP 系统使用Marketplace订阅30天之后激活免费试用、则Cloud Backup试用将不可用。

["详细了解可用的许可模式"](#)。

2022 年 4 月 4 日

适用于应用程序的 Cloud Backup 1.1.0 （由 SnapCenter 提供支持）现已正式上市

通过全新的Cloud Backup for Applications功能、您可以将适用于Oracle和Microsoft SQL的现有应用程序一致性快照(备份)从内部主存储卸载到Amazon S3或Azure Blob中的云对象存储。

如果需要、您可以将此数据从云还原到内部环境。

["了解有关保护内部应用程序数据到云的更多信息"](#)。

新的搜索和还原功能可在所有 **ONTAP** 备份文件中搜索卷或文件

现在，您可以按部分或完整卷名称，部分或完整文件名称，大小范围以及其他搜索筛选器在 * 所有 ONTAP 备份文件 * 中搜索卷或文件。如果您不确定哪个集群或卷是数据源，这是一种很好的新方法来查找要还原的数据。 "[了解如何使用搜索和放大；还原](#)"。

2022 年 3 月 3 日

能够将永久性卷从 **GKEKubernetes** 集群备份到 **Google Cloud** 存储

如果您的 GKE 集群安装了 NetApp Astra Trident，并且使用适用于 GCP 的 Cloud Volumes ONTAP 作为集群的后端存储，则可以将永久性卷备份到 Google Cloud 存储或从 Google Cloud 存储还原。 "[有关详细信息，请访问此处](#)"。

此版本已停止使用 **Cloud Data sense** 扫描 **Cloud Backup** 文件的测试版功能

2022 年 2 月 14 日

现在，您可以将备份策略分配给单个集群中的各个卷

过去，您只能为集群中的所有卷分配一个备份策略。现在，您可以为一个集群创建多个备份策略，并将不同的策略应用于不同的卷。 "[请参见如何为集群创建新的备份策略并将其分配给选定卷](#)"。

通过一个新选项，您可以自动将默认备份策略应用于新创建的卷

过去，激活 Cloud Backup 后在工作环境中创建的新卷要求您手动应用备份策略。现在，无论卷是在 Cloud Manager，System Manager，CLI 中创建的，还是使用 API 创建的，Cloud Backup 都将发现卷并应用您选择作为默认策略的备份策略。

如果新的工作环境中启用备份，或者从 *Manage Volumes* 页面为现有工作环境启用备份，则可以使用此选项。

新的作业监控器可用于查看所有备份和还原作业的正在处理状态

如果您对多个卷启动了操作，例如更改备份策略或删除备份，则作业监控器会非常有用，这样您可以查看操作何时在所有卷上完成。 "[请参见如何使用作业监控器](#)"。

2022 年 1 月 2 日

能够将永久性卷从 **AKS Kubernetes** 集群备份到 **Azure Blob** 存储

如果您的 AKS 集群安装了 NetApp Astra Trident，并且使用适用于 Azure 的 Cloud Volumes ONTAP 作为集群的后端存储，则可以将卷备份到 Azure Blob 存储以及从 Azure Blob 存储还原卷。 "[有关详细信息，请访问此处](#)"。

此版本中更改了 **Cloud Backup Service** 费用，以便与行业标准更加一致

现在，您无需根据备份文件的大小为 NetApp 支付容量费用，而是仅为所保护的数据付费，该数据是通过要备份

的源 ONTAP 卷的逻辑已用容量（在 ONTAP 效率之前）计算得出的。此容量也称为前端 TB（前端 TB）。

2021 年 11 月 28 日

能够将 EKS Kubernetes 集群中的永久性卷备份到 Amazon S3

如果您的 EKS 集群安装了 NetApp Astra Trident，并且使用 Cloud Volumes ONTAP for AWS 作为集群的后端存储，则可以将卷备份到 Amazon S3 或从 Amazon S3 还原卷。["有关详细信息，请访问此处"](#)。

用于备份 DP 卷的增强功能

现在，Cloud Backup 支持为 SVM-DR 关系中目标 ONTAP 系统上的 DP 卷创建备份。存在一些限制，请参见 ["限制"](#) 了解详细信息。

2021 年 11 月 5 日

可以在将卷还原到内部 ONTAP 系统时选择专用端点

从 Amazon S3 或 Azure Blob 上的备份文件将卷还原到内部 ONTAP 系统时，现在您可以选择一个私有端点，用于以私密方式安全地连接到内部系统。

现在，您可以在数天后将旧备份文件分层到归档存储，以节省成本

如果集群运行的是 ONTAP 9.10.1 或更高版本，而您使用的是 AWS 或 Azure 云存储，则可以将备份分层到归档存储。请参见有关的详细信息 ["AWS S3 归档存储类"](#) 和 ["Azure Blob 归档访问层"](#)。

Cloud Backup BYOL 许可证已移至 "数字电子钱包" 中的 "数据服务许可证" 选项卡

Cloud Backup 的 BYOL 许可已从 Cloud Backup Licenses 选项卡移至 Cloud Manager Digital Wallet 中的 Data Services Licenses 选项卡。

2021 年 10 月 4 日

现在，在执行卷或文件还原时，备份文件大小将显示在备份页面中

如果您要删除不必要的大型备份文件，或者您可以比较备份文件大小，以确定可能因恶意软件攻击而导致的任何异常备份文件，则此功能非常有用。

TCO 计算器可用于比较 Cloud Backup 成本

总拥有成本计算器可帮助您了解 Cloud Backup 的总拥有成本，并将这些成本与传统备份解决方案进行比较，并估算潜在节省量。请查看<https://cloud.netapp.com/cloud-backup-service-tco-calculator>[\["此处"\]](#)。

能够为工作环境取消注册 Cloud Backup

现在，您可以轻松地完成这项工作 ["为工作环境取消注册 Cloud Backup"](#) 如果您不想再对该工作环境使用备份功能（或需要付费），

2021 年 9 月 2 日

能够为卷创建按需备份

现在，您可以随时创建按需备份来捕获卷的当前状态。如果对卷进行了重要更改，而您不想等待下一次计划的备份来保护该数据，则此功能非常有用。

["了解如何创建按需备份"](#)。

可以定义专用接口连接，以便安全地备份到 **Amazon S3**

在配置从内部 ONTAP 系统到 Amazon S3 的备份时，现在您可以在激活向导中定义与专用接口端点的连接。这样，您就可以使用一个网络接口，将内部系统以私密和安全的方式连接到由 AWS PrivateLink 提供支持的服务。["查看有关此选项的详细信息"](#)。

现在，您可以在将数据备份到 **Amazon S3** 时选择自己由客户管理的数据加密密钥

为了提高安全性和控制力，您可以在激活向导中选择自己的客户管理的数据加密密钥，而不是使用默认的 Amazon S3 加密密钥。在从内部 ONTAP 系统或 AWS 中的 Cloud Volumes ONTAP 系统配置备份时，可以使用此选项。

现在，您可以从文件数超过 **30 , 000** 的目录还原文件

2021 年 8 月 1 日

可以定义专用端点连接，以便安全地备份到 **Azure Blob**

在配置从内部 ONTAP 系统到 Azure Blob 的备份时，您可以在激活向导中定义与 Azure 私有端点的连接。这样，您就可以使用一个网络接口，将您以私密方式安全地连接到由 Azure Private Link 提供支持的服务。

现在支持每小时备份策略

此新策略是对现有每日，每周和每月策略的补充。每小时备份策略可提供最小恢复点目标（RPO）。

2021 年 7 月 7 日

现在，您可以使用不同的帐户在不同的区域创建备份

现在，您可以使用与 Cloud Volumes ONTAP 系统不同的帐户 / 订阅创建备份。您还可以在部署 Cloud Volumes ONTAP 系统的区域以外的其他区域创建备份文件。

在使用 AWS 或 Azure 时可以使用此功能，并且只有在现有工作环境中启用备份时才可使用此功能——在创建新的 Cloud Volumes ONTAP 工作环境时，此功能不可用。

现在，您可以在将数据备份到 **Azure Blob** 时选择自己由客户管理的数据加密密钥

为了提高安全性和控制力，您可以在激活向导中选择自己的客户管理的数据加密密钥，而不是使用默认的 Microsoft 管理的加密密钥。在从内部 ONTAP 系统或从 Azure 中的 Cloud Volumes ONTAP 系统配置备份时，

可以使用此选项。

现在，在使用单文件还原时，一次最多可以还原 **100** 个文件

2021 年 6 月 7 日

使用 **ONTAP 9.8** 或更高版本时对 **DP** 卷取消了限制

已解决备份数据保护（DP）卷的两个已知限制：

- 以前，只有当 SnapMirror 关系类型为镜像存储或存储时，级联备份才起作用。现在，如果关系类型为 MirrorAllSnapshots，则可以进行备份。
- 现在，只要在 SnapMirror 策略中配置了 Cloud Backup，它就可以使用任何备份标签。不再要求标签每天，每周或每月都包含名称。

2021 年 5 月 5 日

将内部集群数据备份到 **Google Cloud Storage** 或 **NetApp StorageGRID** 系统

现在，您可以创建从内部 ONTAP 系统到 Google 云存储或 NetApp StorageGRID 系统的备份。请参见 ["备份到 Google Cloud Storage"](#) 和 ["备份到 StorageGRID"](#) 了解详细信息。

现在，您可以使用 **System Manager** 执行 **Cloud Backup** 操作

通过 ONTAP 9.9.1 中的一项新功能，您可以使用 System Manager 将内部 ONTAP 卷的备份发送到您通过云备份设置的对象存储。"[了解如何使用 System Manager 使用 Cloud Backup 将卷备份到云。](#)"

备份策略已通过一些增强功能进行了改进

- 现在，您可以创建一个自定义策略，其中包括每日，每周和每月备份。
- 更改备份策略时，会使用原始备份策略将适用场景 all new backups * 和 * 更改为所有卷。过去，此更改仅应用于新的卷备份。

其他备份和还原改进功能

- 现在，在为备份文件配置云目标时，您可以选择与 Cloud Volumes ONTAP 系统所在区域不同的区域。
- 可以为单个卷创建的备份文件数量已从 1，019 个增加到 4，000 个。
- 除了先前删除单个卷的所有备份文件的功能之外，现在您只能删除一个卷的单个备份文件，也可以根据需要删除整个工作环境的所有备份文件。

入门

了解 Cloud Backup

Cloud Backup 是一项适用于 Cloud Manager 工作环境的服务，可提供备份和还原功能来保护和长期归档数据。备份会自动生成并存储在公有 或私有云帐户的对象存储中。

如有必要，您可以将整个 *volume* 从备份还原到相同或不同的工作环境。备份 *ONTAP* 数据时，您还可以选择将备份中的一个或多个 *_files* 还原到相同或不同的工作环境。

["了解有关 Cloud Backup 的更多信息"](#)。

备份和还原可用于：

- 从 Cloud Volumes ONTAP 和内部 ONTAP 系统备份和还原 ONTAP 卷。 ["请参见此处的详细功能"](#)。
- 备份和还原 Kubernetes 永久性卷。 ["请参见此处的详细功能"](#)。
- 使用适用于应用程序的 Cloud Backup 将应用程序一致的快照从内部 ONTAP 备份到云。 ["请参见此处的详细功能"](#)。
- 使用适用于VMware的Cloud Backup将数据存储库备份到云、并将虚拟机还原回内部vCenter。 ["请参见此处的详细功能"](#)。



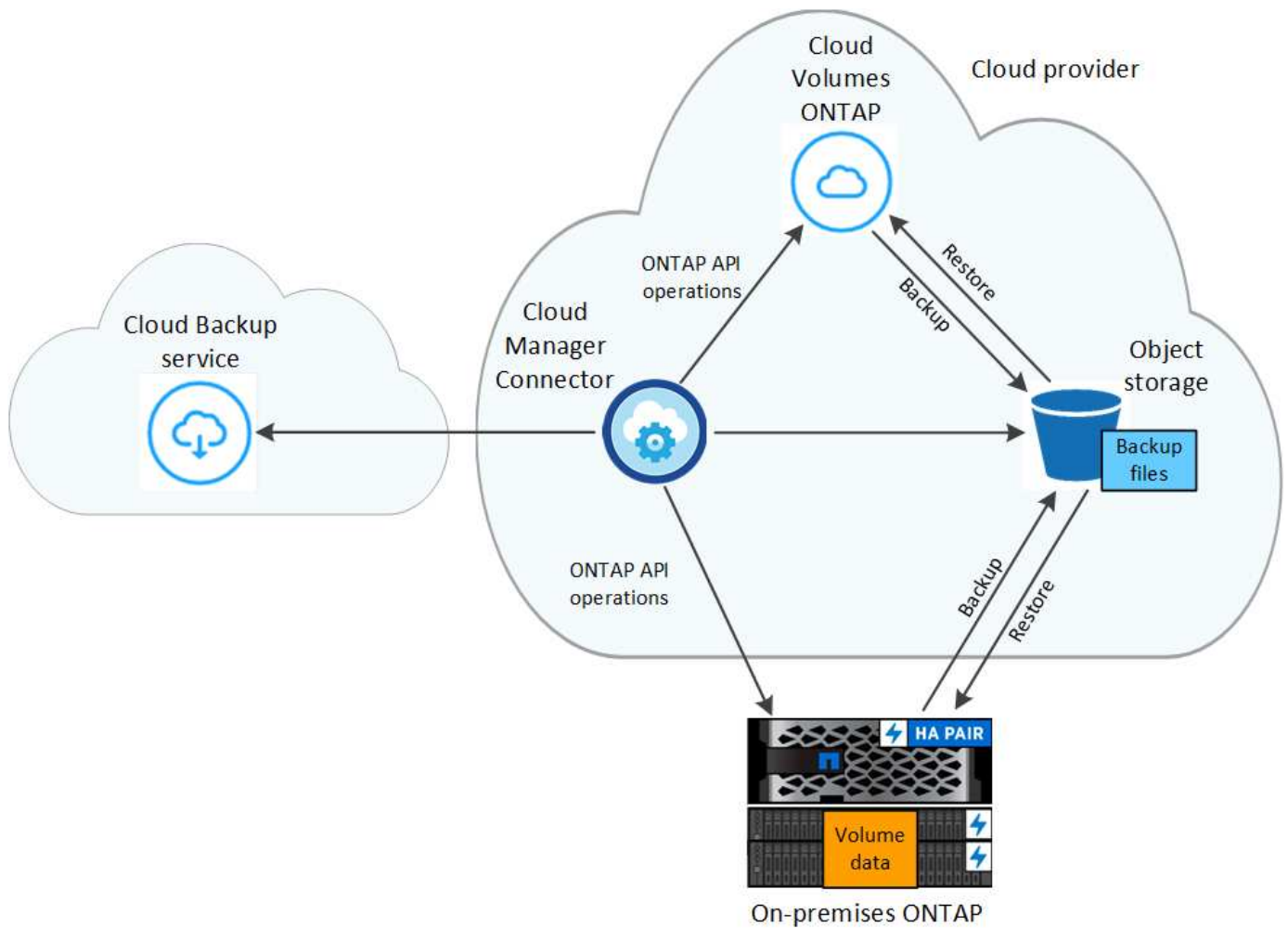
如果Cloud Manager Connector部署在云中的政府区域或无法访问Internet的站点(非公开站点)中、则Cloud Backup仅支持从ONTAP 系统执行备份和还原操作。使用这些备用部署方法时、Cloud Backup不支持从Kubernetes集群、应用程序或虚拟机执行备份和还原操作。

Cloud Backup 的工作原理

在 Cloud Volumes ONTAP 或内部 ONTAP 系统上启用 Cloud Backup 时，此服务会对您的数据执行完整备份。备份映像中不包含卷快照。初始备份之后，所有额外备份都是增量备份，这意味着只会备份更改的块和新块。这样可以将网络流量降至最低。

在大多数情况下，您将使用 Cloud Manager UI 执行所有备份操作。但是，从 ONTAP 9.9.1 开始，您可以使用 ONTAP System Manager 对内部 ONTAP 集群启动卷备份操作。 ["了解如何使用 System Manager 使用 Cloud Backup 将卷备份到云。"](#)

下图显示了每个组件之间的关系：



备份所在位置

备份副本存储在 Cloud Manager 在云帐户中创建的对象存储中。每个集群 / 工作环境有一个对象存储，Cloud Manager 将该对象存储命名为："netapp-backup-clusteruuid"。请确保不要删除此对象存储。

- 在 AWS 中，Cloud Manager 可启用 "[Amazon S3 块公有访问功能](#)" 在 S3 存储分段上。
- 在 StorageGRID 中，Cloud Manager 会将现有存储帐户用于对象存储分段。

备份在午夜进行

- 每小时备份从每小时 5 分钟开始。
- 每天的备份在每天午夜后开始。
- 每周备份将在星期日早晨午夜后开始。
- 每月备份从每个月第一天午夜后开始。

开始时间取决于每个源 ONTAP 系统上设置的时区。您不能从用户界面计划在用户指定的时间执行备份操作。有关详细信息，请联系您的系统工程师。

备份副本与您的 **NetApp** 帐户关联

备份副本与关联 **"NetApp 帐户"** 连接器所在位置。

如果在同一个 NetApp 帐户中有多个连接器，则每个连接器将显示相同的备份列表。其中包括与其他连接器中的 Cloud Volumes ONTAP 和内部 ONTAP 实例关联的备份。

为 Cloud Backup 设置许可

您可以通过从云提供商购买按需购买(PAYGO)市场订阅或从NetApp购买自带许可证(BYOL)来获得Cloud Backup的许可。要在工作环境中激活Cloud Backup、为生产数据创建备份以及将备份数据还原到生产系统、需要有效的许可证。

在阅读其他内容之前，请先阅读一些注释：

- 如果您已在云提供商的市场上为 Cloud Volumes ONTAP 系统订阅了 Cloud Manager 按需购买（PAYGO）订阅，则也会自动订阅 Cloud Backup。您无需重新订阅。
- Cloud Backup 自带许可证（BYOL）是一种浮动许可证，您可以在与 Cloud Manager 帐户关联的所有系统上使用。因此、如果现有BYOL许可证提供了足够的备份容量、则无需再购买一个BYOL许可证。
- 将内部 ONTAP 数据备份到 StorageGRID 时，您需要 BYOL 许可证，但云提供商存储空间不需要任何成本。

["详细了解与使用Cloud Backup相关的成本。"](#)

30 天免费试用

Cloud Backup 30天免费试用可从云提供商市场的按需购买订阅中获得。免费试用将在您订阅市场列表时开始。请注意、如果您在部署Cloud Volumes ONTAP 系统时为Marketplace订阅付费、然后在10天后开始免费试用Cloud Backup、您将有20天的时间使用免费试用版。

免费试用结束后、您将自动切换到PAYGO订阅、而不会中断。如果您决定不继续使用Cloud Backup、只需 ["从工作环境中取消注册Cloud Backup"](#) 在试用结束之前、您不会收到任何费用。

使用 Cloud Backup PAYGO 订阅

对于按需购买、您需要通过一个订阅按小时为云提供商支付对象存储成本和NetApp备份许可成本。即使您拥有免费试用版或自带许可证（BYOL），也应订阅：

- 订阅可确保在免费试用结束后不会中断服务。试用结束后，系统会根据您备份的数据量按小时收取费用。
- 如果备份的数据超过 BYOL 许可证允许的数量，则数据备份将通过按需购买订阅继续进行。例如，如果您拥有 10 TiB BYOL 许可证，则 10 TiB 以上的所有容量均通过 PAYGO 订阅付费。

在免费试用期间，或者如果您未超过 BYOL 许可证，则不会从按需购买订阅中收取费用。

有几个适用于Cloud Backup的PAYGO计划：

- 一个"云备份"软件包、可用于备份Cloud Volumes ONTAP 数据和内部ONTAP 数据。
- 一个"CVO专业版"软件包、可用于捆绑Cloud Volumes ONTAP 和云备份。这包括对此许可证付费的 Cloud Volumes ONTAP 卷的无限备份（备份容量不计入此许可证）。此选项不允许您备份内部 ONTAP 数

据。ifdef: : azure[]

使用以下链接从云提供商市场订阅 Cloud Backup：

- AWS ["有关定价详细信息，请访问 Cloud Manager Marketplace"](#)。

通过 AWS 订阅年度合同

可从获取两份年度合同 ["AWS Marketplace 页面"](#) 适用于 Cloud Volumes ONTAP 和内部 ONTAP 系统。这些计划的有效期为1年、2年或3年：

- 一种 "云备份" 计划，可用于备份 Cloud Volumes ONTAP 数据和内部 ONTAP 数据。

如果要使用此选项，请从 Marketplace 页面设置您的订阅，然后再执行 ["将订阅与您的 AWS 凭据关联"](#)。请注意，您还需要使用此年度合同订阅为 Cloud Volumes ONTAP 系统付费，因为您只能在 Cloud Manager 中为 AWS 凭据分配一个有效订阅。

- 一种 "CVO 专业人员" 计划，可用于捆绑 Cloud Volumes ONTAP 和云备份。这包括对此许可证付费的 Cloud Volumes ONTAP 卷的无限备份（备份容量不计入此许可证）。此选项不允许您备份内部 ONTAP 数据。

请参见 ["Cloud Volumes ONTAP 许可主题"](#) 了解有关此许可选项的更多信息。

如果要使用此选项，您可以在创建 Cloud Volumes ONTAP 工作环境时设置年度合同，而 Cloud Manager 会提示您订阅 AWS Marketplace。

使用 Cloud Backup BYOL 许可证

NetApp 自带许可证的期限为 1 年，2 年或 3 年。您只需为所保护的数据付费，此费用由要备份的源 ONTAP 卷的逻辑已用容量（_before_any 的效率）计算得出。此容量也称为前端 TB（前端 TB）。

BYOL Cloud Backup 许可证是一种浮动许可证，总容量在与您的 Cloud Manager 帐户关联的所有系统之间共享。对于 ONTAP 系统、您可以对计划备份的卷运行 CLI 命令 `volume show-space -logical-used` 来大致估算所需容量。

如果您没有 Cloud Backup BYOL 许可证，请单击 Cloud Manager 右下角的聊天图标购买一个。

或者，如果您已为 Cloud Volumes ONTAP 取消分配了基于节点的许可证，而您不会使用该许可证，则可以将其转换为具有相同美元等价性和相同到期日期的 Cloud Backup 许可证。 ["有关详细信息，请访问此处"](#)。

您可以使用 Cloud Manager 中的数字电子钱包页面管理 BYOL 许可证。您可以从 Digital Wallet 添加新许可证、更新现有许可证以及查看许可证状态。

获取 Cloud Backup 许可证文件

购买 Cloud Backup 许可证后、您可以通过输入 Cloud Backup 序列号和 NSS 帐户或上传 NLF 许可证文件在 Cloud Manager 中激活此许可证。以下步骤显示了如果您计划使用此方法，如何获取 NLF 许可证文件。

如果您在无法访问 Internet 的内部站点上运行 Cloud Backup，这意味着您已在脱机内部站点的主机上部署 Cloud Manager Connector，则需要从已连接 Internet 的系统获取许可证文件。使用序列号和 NSS 帐户激活许可证不可用于脱机（非公开站点）安装。

步骤

1. 登录到 "NetApp 支持站点" 然后单击 * 系统 > 软件许可证 *。
2. 输入 Cloud Backup 许可证序列号。

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		CLOUD_BKP_SERVICE	Get NetApp License File		100	12/31/9998

3. 在 * 许可证密钥 * 列中，单击 * 获取 NetApp 许可证文件 *。
4. 输入您的 Cloud Manager 帐户 ID （在支持站点上称为租户 ID ），然后单击 * 提交 * 下载许可证文件。

Get License

SERIAL NUMBER: 4810

LICENSE: CLOUD_BKP_SERVICE

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

[Cancel](#) [Submit](#)

您可以通过从 Cloud Manager 顶部选择 * 帐户 * 下拉列表，然后单击您帐户旁边的 * 管理帐户 * 来查找 Cloud Manager 帐户 ID 。您的帐户 ID 位于概述选项卡中。

将 **Cloud Backup BYOL** 许可证添加到您的帐户

为 NetApp 帐户购买 Cloud Backup 许可证后，您需要将此许可证添加到 Cloud Manager 中。

步骤

1. 单击 * 所有服务 > 数字电子钱包 > 数据服务许可证 *。
2. 单击 * 添加许可证 *。
3. 在 *Add License* 对话框中，输入许可证信息并单击 * 添加许可证 *：
 - 如果您有备份许可证序列号并且知道您的 NSS 帐户，请选择 * 输入序列号 * 选项并输入该信息。
 - 如果下拉列表中没有您的 NetApp 支持站点帐户， "[将 NSS 帐户添加到 Cloud Manager](#)"。
 - 如果您有备份许可证文件（安装在非公开站点时需要），请选择 * 上传许可证文件 * 选项，然后按照提示附加该文件。

Add Cloud Backup License

A Backup License must be installed with an active subscription. A Backup license enables you to use Cloud Backup for a certain period of time and for a maximum amount of backup space.

☒ Enter Serial Number
 ☐ Upload License File

Serial Number

NetApp Support Site Account

☐ Enter Serial Number
 ☒ Upload License File

To install a license, follow these instructions:

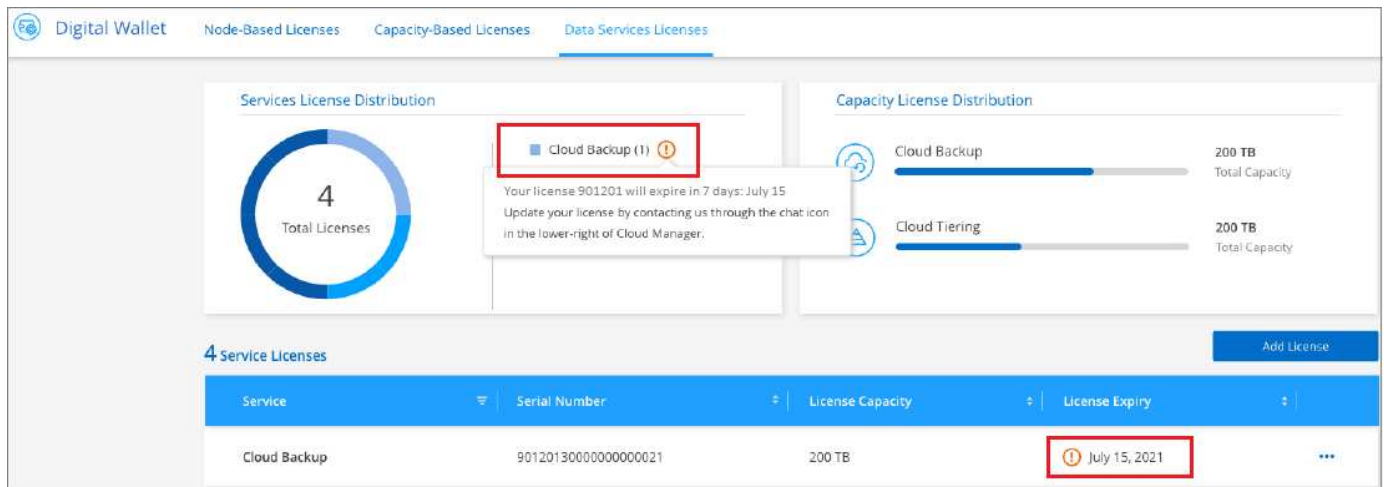
- Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- Click Upload File and then select the file.

Upload License File

Cloud Manager 会添加许可证，以便 Cloud Backup 处于活动状态。

更新 Cloud Backup BYOL 许可证

如果您的许可期限即将到期，或者您的许可容量即将达到限制，您将在备份 UI 中收到通知。此状态也会显示在 "数字电子钱包" 页面和中 "通知"。



您可以在 Cloud Backup 许可证到期之前对其进行更新，以便备份和还原数据的能力不会中断。

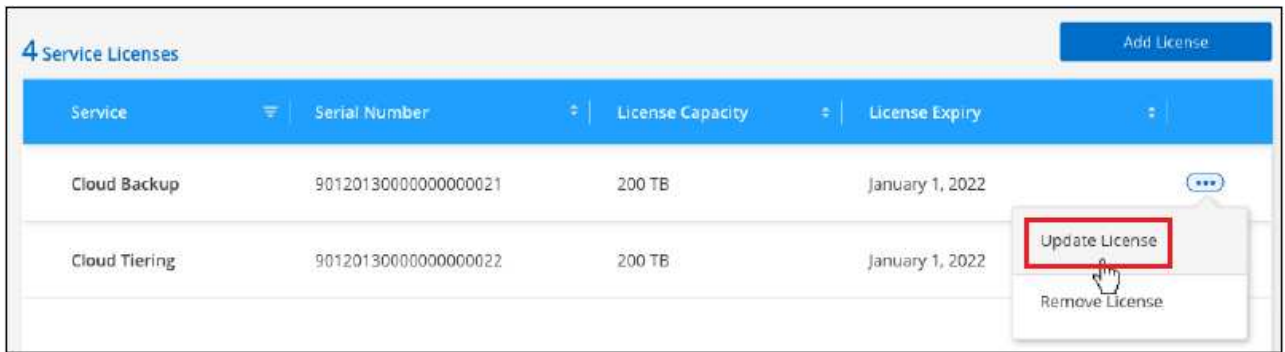
步骤

- 单击 Cloud Manager 右下角的聊天图标或联系支持部门，请求延长您的期限或为特定序列号申请 Cloud Backup 许可证的额外容量。

在您为许可证付费并将其注册到 NetApp 支持站点后，Cloud Manager 会自动在数字电子邮件中更新许可证，并且数据服务许可证页面将在 5 到 10 分钟内反映此更改。

- 如果 Cloud Manager 无法自动更新许可证（例如，安装在非公开站点时），则需要手动上传许可证文件。
 - 您可以 [从 NetApp 支持站点获取许可证文件](#)。
 - 在数字电子邮件页面 *Data Services Licenses* 选项卡上，单击 ... 对于要更新的服务序列号，请单击 * 更

新许可证*。



c. 在 *Update License* 页面中，上传许可证文件并单击 * 更新许可证*。

Cloud Manager 会更新许可证，以便 Cloud Backup 继续处于活动状态。

BYOL 许可证注意事项

使用 Cloud Backup BYOL 许可证时，如果要备份的所有数据的大小接近容量限制或接近许可证到期日期，Cloud Manager 将在用户界面中显示警告。您将收到以下警告：

- 备份达到许可容量的 80% 时，再次达到限制时
- 许可证到期前 30 天，许可证到期后再次

如果您看到这些警告，请使用 Cloud Manager 界面右下角的聊天图标续订许可证。

BYOL许可证到期后、可能会发生以下两种情况：

- 如果您使用的帐户具有 Marketplace 帐户，则备份服务将继续运行，但您将转移到 PAYGO 许可模式。您需要为备份所使用的容量付费。
- 如果您正在使用的帐户没有Marketplace帐户、备份服务将继续运行、但您仍会看到警告。

续订 BYOL 订阅后，Cloud Manager 会自动更新许可证。如果 Cloud Manager 无法通过安全 Internet 连接访问此许可证文件（例如，安装在非公开站点时），您可以自行获取此文件并手动将其上传到 Cloud Manager。有关说明，请参见 ["如何更新 Cloud Backup 许可证"](#)。

已转移到 PAYGO 许可证的系统将自动返回到 BYOL 许可证。如果系统运行时没有许可证、则会停止显示警告。

备份和还原 ONTAP 数据

使用云备份保护 ONTAP 集群数据

Cloud Backup 提供备份和还原功能，用于保护和长期归档 ONTAP 集群数据。备份会自动生成并存储在公有或私有云帐户的对象存储中，而与用于近期恢复或克隆的卷 Snapshot 副本无关。

如有必要，您可以将整个 *volume* 或一个或多个 *_files* 从备份还原到相同或不同的工作环境。

功能

备份功能：

- 将数据卷的独立副本备份到低成本对象存储。
- 将单个备份策略应用于集群中的所有卷，或者将不同的备份策略分配给具有唯一恢复点目标的卷。
- 将旧备份文件分层到归档存储以节省成本(使用ONTAP 9.10.1+时支持)
- 从云备份到云，从内部系统备份到公有或私有云。
- 对于 Cloud Volumes ONTAP 系统，备份可以位于不同的订阅 / 帐户或不同的区域。
- 使用 AES-256 位空闲加密和正在传输的 TLS 1.2 HTTPS 连接保护备份数据。
- 使用您自己的客户管理密钥进行数据加密，而不是使用云提供商提供的默认加密密钥。
- 一个卷最多支持 4 , 000 个备份。

还原功能：

- 从特定时间点还原数据。
- 将卷或单个文件还原到源系统或其他系统。
- 使用不同的订阅 / 帐户或位于不同区域的工作环境还原数据。
- 还原块级别的数据，将数据直接放置在您指定的位置，同时保留原始 ACL 。
- 可浏览且可搜索的文件目录、用于选择单个文件进行单个文件还原。

支持的 ONTAP 工作环境和对象存储提供程序

通过 Cloud Backup ，您可以将 ONTAP 卷从以下工作环境备份到以下公有 和私有云提供商中的对象存储：

源工作环境	备份文件目标
AWS 中的 Cloud Volumes ONTAP	Amazon S3 <code>endif: : AWS]] ifdef: : azure[]</code>
Azure 中的 Cloud Volumes ONTAP	Azure Blob <code>endif: : azure[] ifdef: : GCP[]</code>
Google 中的 Cloud Volumes ONTAP	Google Cloud Storage <code>endif: gcp[]</code>

源工作环境	备份文件目标 ifdef: : AWS]]
内部部署 ONTAP 系统	ifdef: : : AWS]] Amazon S3 endf: : AWS]] ifdef: : azure[] Azure Blob endf: : azure[] ifdef: : GCP ; Google Cloud Storage endf: : GCP; NetApp StorageGRID

您可以将卷或单个文件从 ONTAP 备份文件还原到以下工作环境：

备份文件	目标工作环境	
* 位置 *	* 卷还原 *	文件还原 ifdef: : AWS
Amazon S3	AWS 内部 ONTAP 系统中的 Cloud Volumes ONTAP	AWS内部部署ONTAP 系统中的Cloud Volumes ONTAP endf: AWS [] ifdef: : azure[]
Azure Blob	Azure 内部 ONTAP 系统中的 Cloud Volumes ONTAP	Azure内部ONTAP 系统中的Cloud Volumes ONTAP endf: azure[] ifdef: : gcp[]
Google Cloud 存储	Google 内部 ONTAP 系统中的 Cloud Volumes ONTAP	Google内部部署ONTAP 系统中的Cloud Volumes ONTAP endf: gcp[]
NetApp StorageGRID	内部部署 ONTAP 系统	内部部署 ONTAP 系统

请注意，" 内部 ONTAP 系统 " 的引用包括 FAS ， AFF 和 ONTAP Select 系统。

支持无 **Internet** 连接的站点

Cloud Backup 可在没有 Internet 连接的站点（也称为 " 脱机 " 或 " 暗 " 站点）中使用，以便将卷数据从本地内部 ONTAP 系统备份到本地 NetApp StorageGRID 系统。在这种情况下、您需要在非公开站点中部署Cloud Manager Connector (最低版本为3.9.19)。请参见 ["将内部 ONTAP 数据备份到 StorageGRID"](#) 了解详细信息。

成本

将 Cloud Backup 与 ONTAP 系统结合使用会产生两种成本：资源费用和服务费用。

- 资源费用 *

向云提供商支付对象存储容量和在云中运行虚拟机 / 实例的资源费用。

- 对于备份，您需要为云提供商支付对象存储成本。

由于云备份会保留源卷的存储效率，因此您需要为云提供商的对象存储成本支付 **data_after_ ONTAP** 效率（适用于应用重复数据删除和数据压缩后少量的数据）。

- 对于使用搜索和还原的卷或文件还原、某些资源由云提供商配置、搜索请求扫描的数据量会产生每TiB成本。
 - 在AWS中、["Amazon Athena"](#) 和 ["AWS 胶水"](#) 资源部署在新的S3存储分段中。
- 如果您需要从已移至归档存储的备份文件还原卷数据、则云提供商会额外收取每GiB检索费用和每请求费用。
- 服务费用 *

服务费用支付给 NetApp，用于支付这些备份的 *creation_backup* 和 *restor* 卷或文件的费用。您只需为所保护的数据付费，该数据是通过备份到对象存储的 ONTAP 卷的源逻辑已用容量（*_before_ONTAP* 效率）计算得出的。此容量也称为前端 TB（前端 TB）。

有三种方式可以为备份服务付费。第一种选择是从云提供商订阅，这样您可以按月付费。第二种选择是获得年度合同。第三种选择是直接 NetApp 购买许可证。阅读 [许可](#) 部分以了解详细信息。

许可

Cloud Backup 提供了几种许可选项：

- 按需购买(PAYGO)订阅
- AWS Marketplace 的年度合同
- 自带许可证(BYOL)

首次注册 PAYGO 订阅时，您可以获得 30 天免费试用。

按需购买订阅

Cloud Backup 以按需购买模式提供基于消费的许可。在通过云提供商的市场订阅后，您可以按 GiB 为备份的数据付费— 无需预先付费。您的云提供商会通过每月账单向您开具账单。

["了解如何设置按需购买订阅"](#)。

年度合同（仅限 AWS）

AWS Marketplace 提供两份年期合同，合同期限分别为 12，24 或 36 个月：

- 一种 "云备份" 计划，可用于备份 Cloud Volumes ONTAP 数据和内部 ONTAP 数据。
- 一种 "CVO 专业人员" 计划，可用于捆绑 Cloud Volumes ONTAP 和云备份。这包括对此许可证付费的 Cloud Volumes ONTAP 卷的无限备份（备份容量不计入此许可证）。

["了解如何设置年度 AWS 合同"](#)。

自带许可证

BYOL 基于期限（12，24 或 36 个月）和容量，以 1 TiB 为增量。您需要向 NetApp 支付一段时间（如 1 年）使用此服务的费用，最大容量（如 10 TiB）。

您将收到一个序列号，您可以在 Cloud Manager 数字电子邮件页面中输入此序列号来启用此服务。达到任一限制后，您需要续订许可证。备份 BYOL 许可证适用场景 与关联的所有源系统 ["Cloud Manager 帐户"](#)。

["了解如何管理 BYOL 许可证"](#)。

Cloud Backup 的工作原理

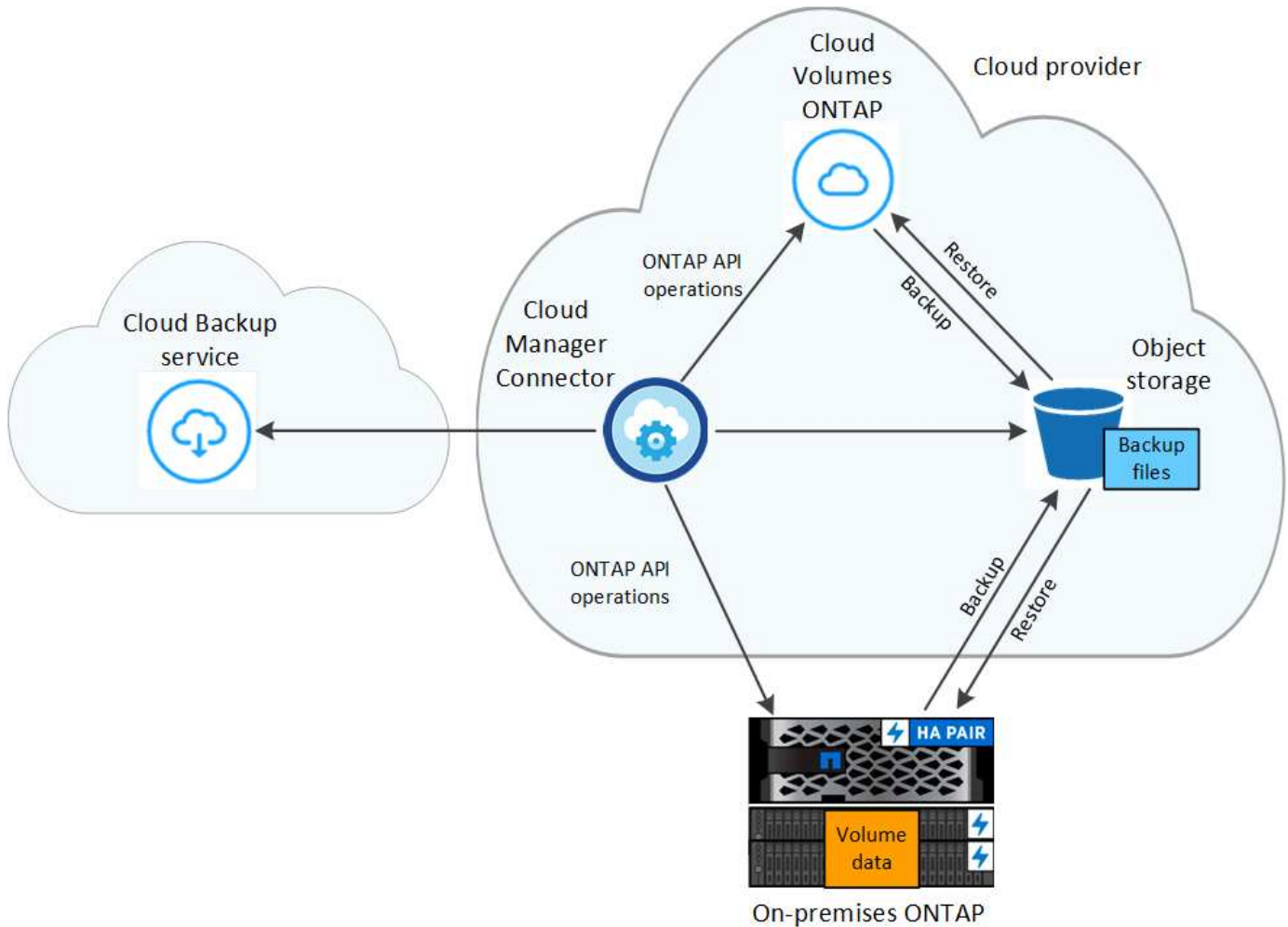
在 Cloud Volumes ONTAP 或内部 ONTAP 系统上启用 Cloud Backup 时，此服务会对您的数据执行完整备份。备份映像中不包含卷快照。初始备份之后，所有额外备份都是增量备份，这意味着只会备份更改的块和新块。这样可以网络流量降至最低。

在大多数情况下，您将使用 Cloud Manager UI 执行所有备份操作。但是，从 ONTAP 9.9.1 开始，您可以使用 ONTAP System Manager 对内部 ONTAP 集群启动卷备份操作。"[了解如何使用 System Manager 使用 Cloud Backup 将卷备份到云。](#)"



直接从云提供商环境中执行的任何备份文件管理或更改操作可能会损坏这些文件，并导致配置不受支持。

下图显示了每个组件之间的关系：



备份所在位置

备份副本存储在 Cloud Manager 在云帐户中创建的对象存储中。每个集群 / 工作环境有一个对象存储，Cloud Manager 将该对象存储命名为："netapp-backup-clusteruuid"。请确保不要删除此对象存储。

- 在 AWS 中，Cloud Manager 可启用 "[Amazon S3 块公有访问功能](#)" 在 S3 存储分段上。
- 在 StorageGRID 中，Cloud Manager 会将现有存储帐户用于对象存储分段。

如果您希望将来更改集群的目标对象存储，则需要 "[取消注册适用于工作环境的 Cloud Backup](#)"，然后使用新的云提供商信息启用 Cloud Backup。

支持的存储类或访问层

- 在 AWS 中，备份从 *Standard* 存储类开始，并在 30 天后过渡到 *Standard-Infrequent Access* 存储类。

如果集群使用的是 ONTAP 9.10.1 或更高版本，则可以选择在一定天数后将旧备份分层到 *S3 Glacier* 或 *S3 Glacier Deep Archive* 存储，以进一步优化成本。[了解有关 AWS 归档存储的更多信息](#)。

- 在 StorageGRID 中，备份与 *Standard* 存储类关联。

每个集群可自定义的备份计划和保留设置

在为工作环境启用 Cloud Backup 时，您最初选择的所有卷都会使用您定义的默认备份策略进行备份。如果要为具有不同恢复点目标（RPO）的某些卷分配不同的备份策略，您可以为该集群创建其他策略并将这些策略分配给其他卷。

您可以选择对所有卷进行每小时，每天，每周和每月备份的组合。您还可以选择系统定义的策略之一，这些策略可提供 3 个月，1 年和 7 年的备份和保留期限。这些策略包括：

备份策略名称	每间隔备份数 ...			最大备份
	* 每日 *	* 每周 *	* 每月 *	
NetApp 3 个月保留	30 个	13	3.	46
NetApp 保留 1 年	30 个	13	12	55
NetApp 7 年保留	30 个	53.	84.	167.

使用 ONTAP 系统管理器或 ONTAP 命令行界面在集群上创建的备份保护策略也会显示为选项。

达到某个类别或间隔的最大备份数后，较早的备份将被删除，以便始终拥有最新的备份。

请注意，您可以 [创建卷的按需备份](#) 除了从计划的备份创建的备份文件之外，还可以随时从备份信息板访问这些备份文件。



数据保护卷备份的保留期限与源 SnapMirror 关系中定义的保留期限相同。您可以根据需要使用 API 更改此设置。

FabricPool 分层策略注意事项

当您备份的卷位于 FabricPool 聚合上且其分配的策略不是 `none` 时，您需要注意以下几点：

- FabricPool 分层卷的首次备份要求读取所有本地数据和所有分层数据（从对象存储）。备份操作不会“重新加热”对象存储中分层的冷数据。

此操作可能发生原因会一次性增加从云提供商读取数据的成本。

- 后续备份是增量备份，不会产生这种影响。
- 如果在最初创建卷时为其分配了分层策略，则不会显示此问题描述。
- 在将 All 分层策略分配给卷之前，请考虑备份的影响。由于数据会立即分层，因此 Cloud Backup 将从云层读取数据，而不是从本地层读取数据。由于并发备份操作会共享指向云对象存储的网络链路，因此，如果网络资源饱和，性能可能会下降。在这种情况下，您可能需要主动配置多个网络接口（LIF）以降低此类网络

饱和。

支持的卷

Cloud Backup 支持 FlexVol 读写卷和 SnapMirror 数据保护（DP）目标卷。

目前不支持 FlexGroup 卷和 SnapLock 卷。

限制

- 要将旧备份文件分层到归档存储、集群必须运行ONTAP 9.10.1或更高版本。从归档存储中的备份文件还原卷还要求目标集群运行 ONTAP 9.10.1+。
- 在创建或编辑备份策略时，如果没有为该策略分配任何卷，则保留的备份数最多可以为 1018。作为临时决策，您可以减少备份数量以创建策略。然后，在为策略分配卷后，您可以编辑此策略以创建多达 4000 个备份。
- 备份数据保护（DP）卷时，不会将具有以下 SnapMirror 标签的关系备份到云：
 - 应用程序一致
 - all_source_snapshot
- 支持 SVM-DR 卷备份，但有以下限制：
 - 仅支持从 ONTAP 二级系统进行备份。
 - 应用于卷的 Snapshot 策略必须是 Cloud Backup 可识别的策略之一，包括每日，每周，每月等。默认的 "sm_created" 策略（用于 * 镜像所有快照 *）无法识别，并且 DP 卷不会显示在可备份的卷列表中。
- 数据保护卷不支持使用 * 立即备份 * 按钮进行临时卷备份。
- 不支持 SM-BC 配置。
- 仅 ONTAP 二级系统支持 MetroCluster（MCC）备份：MCC > SnapMirror > ONTAP > 云备份 > 对象存储。
- ONTAP 不支持扇出从一个卷到多个对象存储的 SnapMirror 关系；因此，Cloud Backup 不支持此配置。
- 不支持对象存储上的 WORM/Compliance 模式。

单个文件还原限制

这些限制适用于恢复文件的搜索和还原以及浏览和还原方法；除非特别说明。

- 浏览和还原一次最多可还原100个单个文件。
- 搜索和还原一次可以还原1个文件。
- 目前不支持还原文件夹 / 目录。
- 要还原的文件必须使用与目标卷上的语言相同的语言。如果语言不同，您将收到一条错误消息。
- 如果在不同子网中将同一帐户与不同的 Cloud Manager 结合使用，则不支持文件级还原。
- 如果备份文件驻留在归档存储中，则无法还原单个文件。
- 如果Connector安装在无法访问Internet的站点(非公开站点)上、则不支持使用搜索和还原进行文件级还原。

将 Cloud Volumes ONTAP 数据备份到 Amazon S3

完成几个步骤，开始将数据从 Cloud Volumes ONTAP 备份到 Amazon S3。

快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。

跨度 class="image">https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png" Alt-one"> 验证是否支持您的配置

- 您正在 AWS 中运行 Cloud Volumes ONTAP 9.6 或更高版本。
- 您已为备份所在的存储空间订阅了有效的云提供商。
- 您已订阅 "Cloud Manager Marketplace Backup 产品"，和 "AWS 年度合同"或您已购买 "并激活" NetApp 提供的 Cloud Backup BYOL 许可证。
- 为 Cloud Manager Connector 提供权限的 IAM 角色包括最新版本的 S3 权限 "Cloud Manager 策略"。

跨度 class="image">https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png" Alt-twe"> 在新系统或现有系统上启用 Cloud Backup

- 新系统：在工作环境向导中，Cloud Backup 默认处于启用状态。请务必保持此选项处于启用状态。
- 现有系统：选择工作环境，然后单击右侧面板中备份和还原服务旁边的 * 启用 *，然后按照设置向导进行操作。



选择 AWS 帐户以及要创建备份的区域。您还可以选择自己的客户管理密钥进行数据加密，而不是使用默认的 Amazon S3 加密密钥。

Provider Settings

Provider Information

AWS Account

AWS_Account_1

AWS Access Key

Enter AWS Access Key

AWS Secret Key

Enter AWS Secret Key

Location & Connectivity

Region

us-east-2

Encryption

Encryption Key Type: AWS SSE-S3

Change Key

默认策略每天备份卷，并保留每个卷的最新 30 个备份副本。更改为每小时，每天，每周或每月备份，或者选择

一个提供更多选项的系统定义策略。您还可以更改要保留的备份副本数。

默认情况下，备份存储在 S3 标准存储中。如果集群使用的是 ONTAP 9.10.1 或更高版本，则可以选择在一定天数后将备份分层到 S3 Glacier 或 S3 Glacier 深度归档存储，以进一步优化成本。

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy - Retention & Schedule

☒ Create a New Policy

☐ Select an Existing Policy

☐ Hourly

Number of backups to retain

24

☒ Daily

Number of backups to retain

30

☐ Weekly

Number of backups to retain

52

☐ Monthly

Number of backups to retain

12

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

30

Storage Class

S3 Glacier

S3 Glacier

S3 Glacier Deep Archive

S3 Bucket

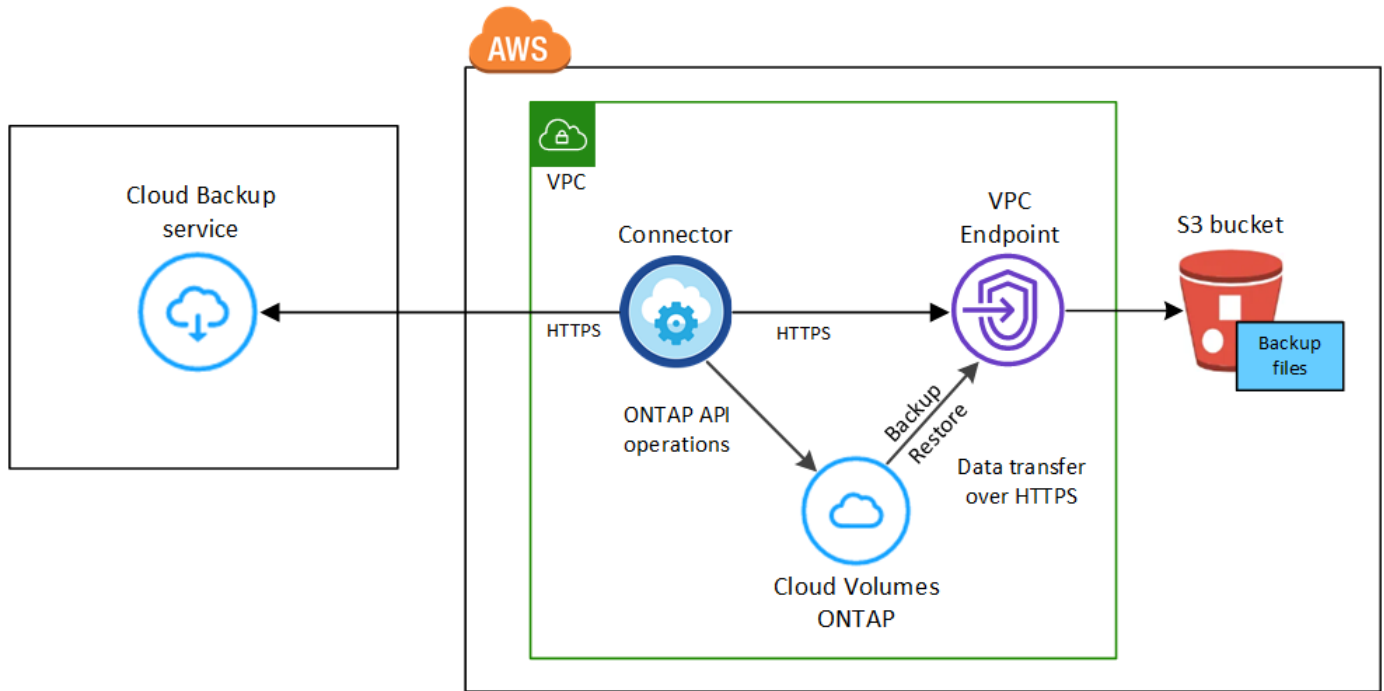
Cloud Manager will create the S3 bucket for you.

在选择卷页面中，使用默认备份策略确定要备份的卷。如果要为某些卷分配不同的备份策略，可以创建其他策略并稍后将其应用于卷。

要求

开始将卷备份到 S3 之前，请阅读以下要求，以确保您的配置受支持。

下图显示了每个组件以及需要在它们之间准备的连接：



支持的 **ONTAP** 版本

建议至少使用ONTAP 9.6；ONTAP 9.8P11及更高版本。

许可证要求

对于 Cloud Backup PAYGO 许可，AWS Marketplace 中提供了 Cloud Manager 订阅，用于部署 Cloud Volumes ONTAP 和 Cloud Backup。您需要 ["订阅此 Cloud Manager 订阅"](#) 启用 Cloud Backup 之前。Cloud Backup 的计费通过此订阅完成。

对于能够同时备份 Cloud Volumes ONTAP 数据和内部 ONTAP 数据的年度合同，您需要从订阅 ["AWS Marketplace 页面"](#) 然后 ["将订阅与您的 AWS 凭据关联"](#)。

对于能够捆绑 Cloud Volumes ONTAP 和云备份的年度合同，您必须在创建 Cloud Volumes ONTAP 工作环境时设置年度合同。此选项不允许您备份内部数据。

对于 Cloud Backup BYOL 许可，您需要 NetApp 提供的序列号，以便在许可证有效期和容量内使用此服务。["了解如何管理 BYOL 许可证"](#)。

您需要为备份所在的存储空间创建一个 AWS 帐户。

支持的 **AWS** 区域

所有 AWS 地区均支持 Cloud Backup ["支持 Cloud Volumes ONTAP 的位置"](#)；包括 AWS GovCloud 地区。

使用客户管理的密钥进行数据加密所需的信息

您可以在激活向导中选择自己的客户管理的数据加密密钥，而不是使用默认的 Amazon S3 加密密钥。在这种情况下，您需要已设置加密受管密钥。["了解如何使用您自己的密钥"](#)。

需要 **AWS** 权限

为 Cloud Manager 提供权限的 IAM 角色必须包含最新版本的 S3 权限 ["Cloud Manager 策略"](#)。

以下是策略中的特定权限：

```

{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
}

```

如果您使用 3.9.15 或更高版本部署了 Connector，则这些权限应已属于 IAM 角色。否则，您需要添加缺少权限。具体来说就是 "Athena" 和 "glue" 权限，因为它们是搜索和还原所必需的。

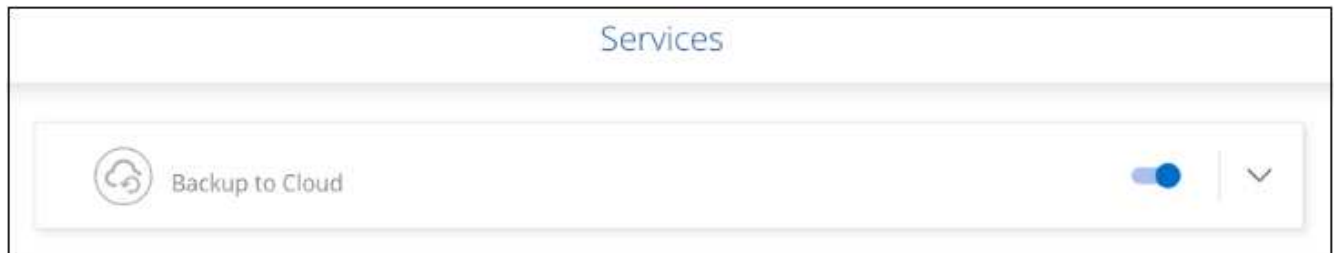
在新系统上启用 **Cloud Backup**

Cloud Backup 在工作环境向导中默认处于启用状态。请务必保持此选项处于启用状态。

请参见 ["在 AWS 中启动 Cloud Volumes ONTAP"](#) 有关创建 Cloud Volumes ONTAP 系统的要求和详细信息，请参见。

步骤

1. 单击 * 创建 Cloud Volumes ONTAP *。
2. 选择 Amazon Web Services 作为云提供商，然后选择单个节点或 HA 系统。
3. 填写详细信息和凭据页面。
4. 在服务页面上，保持服务处于启用状态，然后单击 * 继续 *。



5. 完成向导中的页面以部署系统。

Cloud Backup 在系统上启用，每天备份卷，并保留最近 30 个备份副本。

您可以 ["启动和停止卷备份或更改备份计划"](#)。您也可以 ["从备份文件还原整个卷或单个文件"](#) 连接到 AWS 中的 Cloud Volumes ONTAP 系统或内部 ONTAP 系统。

在现有系统上启用 Cloud Backup

可随时直接从工作环境启用 Cloud Backup。

步骤

1. 选择工作环境，然后单击右面板中备份和还原服务旁边的 * 启用 *。

如果您的备份的 Amazon S3 目标作为工作环境存在于 Canvas 上、您可以将集群拖动到 Amazon S3 工作环境中以启动设置向导。



2. 选择提供程序详细信息并单击 * 下一步 *：
 - a. 用于存储备份的 AWS 帐户。此帐户可以与 Cloud Volumes ONTAP 系统所驻留的帐户不同。
 - b. 要存储备份的区域。此区域可以与 Cloud Volumes ONTAP 系统所在的区域不同。
 - c. 是使用默认 Amazon S3 加密密钥，还是从 AWS 帐户中选择您自己的客户管理密钥来管理数据加密。（[了解如何使用您自己的加密密钥](#)）。

Provider Settings

Provider Information

AWS Account

AWS Access Key

AWS Secret Key

Location & Connectivity

Region

Encryption ⓘ

Encryption Key Type: AWS SSE-S3 [Change Key](#)

3. 输入默认备份策略详细信息，然后单击 * 下一步 *。
 - a. 定义备份计划并选择要保留的备份数。"请参见您可以选择的现有策略列表"。
 - b. 使用 ONTAP 9.10.1 及更高版本时，您可以选择在一定天数后将备份分层到 S3 Glacier 或 S3 Glacier 深度归档存储，以进一步优化成本。"了解有关使用归档层的更多信息"。

Define Policy

This policy is applied to the volumes you select in the next step. You can apply different policies to volumes after activating backup.

Policy - Retention & Schedule

☒ Create a New Policy
 ☐ Select an Existing Policy

<input type="checkbox"/> Hourly	Number of backups to retain	<input type="text" value="24"/>
<input checked="" type="checkbox"/> Daily	Number of backups to retain	<input type="text" value="30"/>
<input type="checkbox"/> Weekly	Number of backups to retain	<input type="text" value="52"/>
<input type="checkbox"/> Monthly	Number of backups to retain	<input type="text" value="12"/>

Archival Policy

Backups reside in S3 Standard storage for frequently accessed data. Optionally, you can tier backups to either S3 Glacier or S3 Glacier Deep Archive storage for further cost optimization.

☒ Tier Backups to Archival

Archive after (Days)

Storage Class

S3 Glacier

S3 Glacier Deep Archive

S3 Bucket

Cloud Manager will create the S3 bucket for you.

4. 在选择卷页面中，使用默认备份策略选择要备份的卷。如果要为某些卷分配不同的备份策略，可以创建其他策略并稍后将其应用于这些卷。

Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy						

。要备份所有卷，请选中标题行 (☒ Volume Name)。

。要备份单个卷，请选中每个卷对应的框 (☒ Volume_1)。

5. 如果希望将来添加的所有卷都启用备份，只需选中 "自动备份未来卷 ..." 复选框即可。如果禁用此设置，则需要手动为未来的卷启用备份。

6. 单击 * 激活备份 *，Cloud Backup 将开始对每个选定卷进行初始备份。

Cloud Backup 将开始对每个选定卷进行初始备份，此时将显示卷备份信息板，以便您可以监控备份的状态。

您可以 "启动和停止卷备份或更改备份计划"。您也可以 "从备份文件还原整个卷或单个文件" 连接到 AWS 中的 Cloud Volumes ONTAP 系统或内部 ONTAP 系统。

将内部 ONTAP 数据备份到 Amazon S3

完成几个步骤，开始将数据从内部 ONTAP 系统备份到 Amazon S3 存储。

请注意，"内部 ONTAP 系统" 包括 FAS，AFF 和 ONTAP Select 系统。

快速入门

按照以下步骤快速入门。本主题的以下各节提供了每个步骤的详细信息。

选择是通过公有 Internet 将内部 ONTAP 集群直接连接到 AWS S3、还是使用 VPN 或 AWS Direct Connect 并通过专用 VPC 端点接口将流量路由到 AWS S3。

[请参见可用的连接方法。](#)

如果您已在 AWS VPC 中部署了 Connector，则可以随时完成所有操作。如果没有，则需要先在 AWS 中创建连接器，以便将 ONTAP 数据备份到 AWS S3 存储。您还需要自定义 Connector 的网络设置，以便它可以连接到 AWS S3。

[请参见如何创建 Connector 以及如何定义所需的网络设置。](#)

在 Cloud Manager 中发现您的 ONTAP 集群，验证集群是否满足最低要求，并自定义网络设置，以便集群可以连接到 AWS S3。

[了解如何使内部 ONTAP 集群做好准备。](#)

为Connector设置创建和管理S3存储分段的权限。您还需要为内部ONTAP 集群设置权限、以便其可以向S3存储分段读取和写入数据。

或者，您也可以为数据加密设置自己的自定义管理密钥，而不是使用默认的 Amazon S3 加密密钥。 [了解如何让 AWS S3 环境做好接收 ONTAP 备份的准备。](#)

选择工作环境，然后单击右侧面板中备份和还原服务旁边的 * 启用 > 备份卷 *。然后，按照设置向导定义默认备份策略和要保留的备份数，并选择要备份的卷。

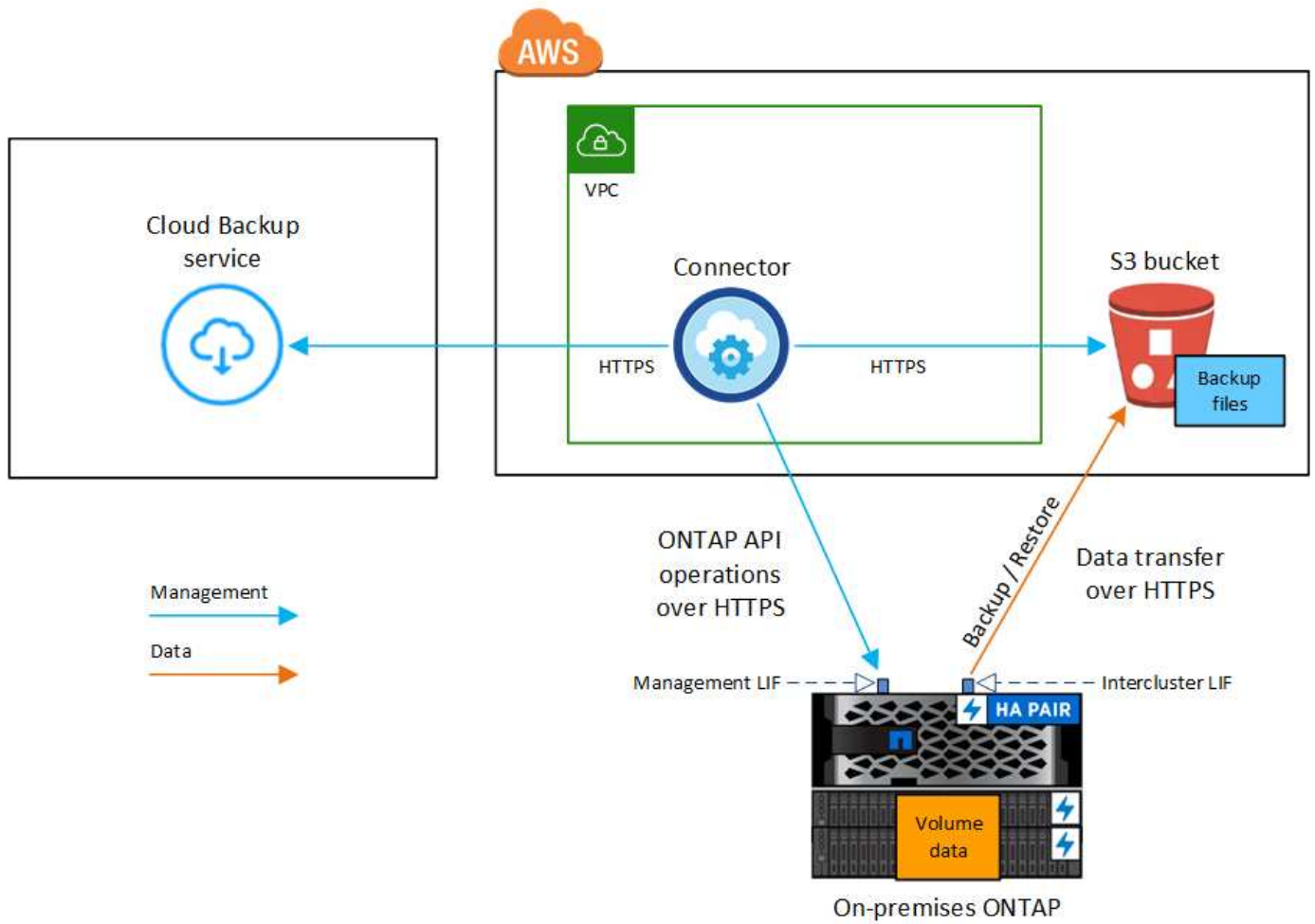
[了解如何在卷上激活 Cloud Backup。](#)

连接选项的网络图

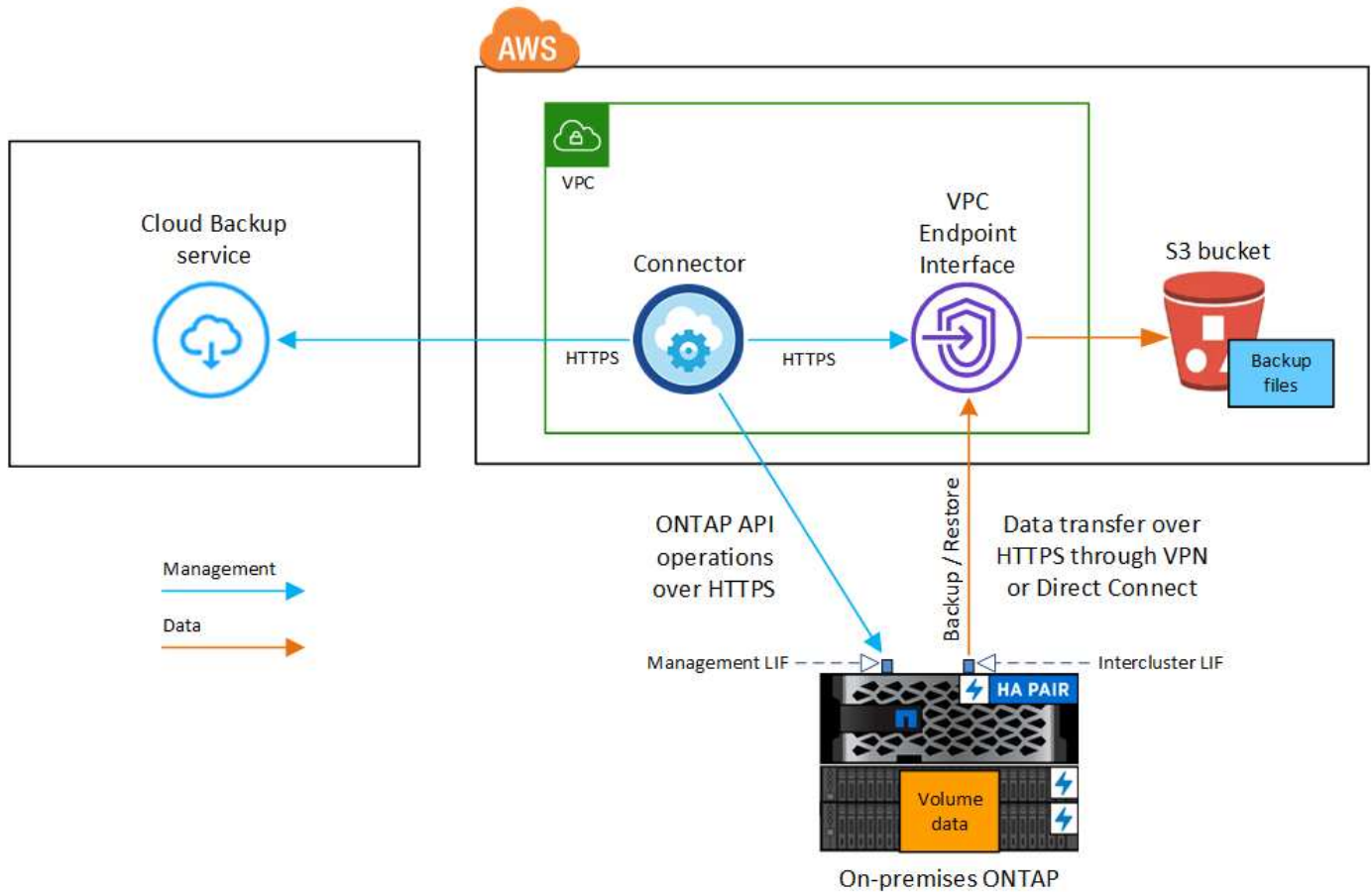
在配置从内部 ONTAP 系统到 AWS S3 的备份时，您可以使用两种连接方法。

- 公有 连接—使用公有 S3 端点将 ONTAP 系统直接连接到 AWS S3。
- 专用连接—使用 VPN 或 AWS Direct Connect，并通过使用专用 IP 地址的 VPC 端点接口路由流量。

下图显示了*公有 connection*方法以及组件之间需要准备的连接：



下图显示了*专用连接*方法以及组件之间需要准备的连接：



准备您的连接器

Cloud Manager Connector 是 Cloud Manager 功能的主要软件。需要使用连接器来备份和还原 ONTAP 数据。

创建或切换连接器

如果您已在 AWS VPC 中部署了 Connector，则可以随时完成所有操作。如果没有，则需要在 AWS 中创建新的连接器，以便将 ONTAP 数据备份到 AWS S3 存储。您不能使用部署在内部或部署在其他云提供商中的 Connector。

- ["了解连接器"](#)
- ["连接器入门"](#)
- ["在 AWS 中创建连接器"](#)

连接器网络连接要求

- 确保安装 Connector 的网络启用以下连接：
 - 通过端口443与Cloud Backup Service 和S3对象存储建立HTTPS连接(请参见端点列表 ["此处"](#))
 - 通过端口 443 与 ONTAP 集群管理 LIF 建立 HTTPS 连接
- ["确保Connector具有管理S3存储分段的权限"](#)。
- 如果从ONTAP 集群到VPC具有直接连接或VPN连接、并且您希望连接器和S3之间的通信保持在AWS内部网络中、则需要启用连接到S3的VPC端点接口。 [请参见如何设置 VPC 端点接口](#)。

准备 ONTAP 集群

在 Cloud Manager 中发现您的 ONTAP 集群

您需要先在 Cloud Manager 中发现内部 ONTAP 集群，然后才能开始备份卷数据。要添加集群，您需要知道集群管理 IP 地址和管理员用户帐户的密码。

["了解如何发现集群"](#)。

ONTAP 要求

- 建议至少使用 ONTAP 9.7P5；ONTAP 9.8P11 及更高版本。
- SnapMirror 许可证（作为超值包或数据保护包的一部分提供）。
- 注意：* 使用 Cloud Backup 时不需要 "混合云捆绑包"。

请参见操作说明 ["管理集群许可证"](#)。

- 已正确设置时间和时区。

请参见操作说明 ["配置集群时间"](#)。

集群网络连接要求

- 集群需要从 Connector 到集群管理 LIF 的入站 HTTPS 连接。
- 托管要备份的卷的每个 ONTAP 节点都需要一个集群间 LIF。这些集群间 LIF 必须能够访问对象存储。

集群通过端口 443 从集群间 LIF 启动出站 HTTPS 连接到 Amazon S3 存储，以执行备份和还原操作。ONTAP 在对象存储中读取和写入数据—对象存储从不启动，它只是响应。

- 集群间 LIF 必须与 `_IP 空间 _` 关联，ONTAP 应使用此 `_IP 空间 _` 连接到对象存储。 ["了解有关 IP 空间的更多信息"](#)。

设置 Cloud Backup 时，系统会提示您使用 IP 空间。您应选择与这些 LIF 关联的 IP 空间。这可能是您创建的 "默认" IP 空间或自定义 IP 空间。

如果您使用的 IP 空间与 "默认" 不同，则可能需要创建静态路由才能访问对象存储。

IP 空间中的所有集群间 LIF 都必须能够访问对象存储。如果无法为当前 IP 空间配置此空间、则需要创建一个专用 IP 空间、其中所有集群间 LIF 都可以访问对象存储。

- 必须已为卷所在的 Storage VM 配置 DNS 服务器。请参见操作说明 ["为 SVM 配置 DNS 服务"](#)。
- 如有必要，请更新防火墙规则，以允许通过端口 443 从 ONTAP 到对象存储的 Cloud Backup 连接以及通过端口 53（TCP/UDP）从 Storage VM 到 DNS 服务器的名称解析流量。
- 如果在 AWS 中使用专用 VPC 接口端点进行 S3 连接、则使用 HTTPS/443、您需要将 S3 端点证书加载到 ONTAP 集群中。 [请参见如何设置 VPC 端点接口并加载 S3 证书](#)。
- ["确保 ONTAP 集群具有访问 S3 存储分段的权限"](#)。

验证许可证要求

- 在为集群激活Cloud Backup之前、您需要从AWS订阅按需购买(PAYGO) Cloud Manager Marketplace产品、或者从NetApp购买并激活Cloud Backup BYOL许可证。这些许可证适用于您的帐户，可在多个系统中使用。
 - 对于 Cloud Backup PAYGO 许可，您需要订阅 ["AWS Cloud Manager Marketplace 产品"](#) 使用Cloud Backup。Cloud Backup 的计费通过此订阅完成。
 - 对于 Cloud Backup BYOL 许可，您需要 NetApp 提供的序列号，以便在许可证有效期和容量内使用此服务。 ["了解如何管理 BYOL 许可证"](#)。
- 您需要为备份所在的对象存储空间订阅 AWS 。

您可以在所有地区创建从内部系统到 Amazon S3 的备份 ["支持 Cloud Volumes ONTAP 的位置"](#)；包括 AWS GovCloud 地区。您可以在设置服务时指定要存储备份的区域。

准备 AWS 环境

设置 S3 权限

您需要配置两组权限：

- Connector创建和管理S3存储分段的权限。
- 内部 ONTAP 集群的权限，以便可以将数据读写到 S3 存储分段。

步骤

1. 确认以下 S3 权限（从最新版本开始） ["Cloud Manager 策略"](#)）是为 Connector 提供权限的 IAM 角色的一部分。

```

{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:DeleteObject",
        "s3:PutObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutEncryptionConfiguration",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ]
}

```

如果您使用 3.9.15 或更高版本部署了 Connector，则这些权限应已属于 IAM 角色。否则，您需要添加缺少的权限。具体来说就是 "Athena" 和 "glue" 权限，因为它们是搜索和还原所必需的。请参见 ["AWS 文档：编辑 IAM 策略"](#)。

2. 激活此服务时，备份向导将提示您输入访问密钥和机密密钥。这些凭据将传递到 ONTAP 集群，以便 ONTAP 可以将数据备份和还原到 S3 存储分段。为此，您需要创建具有以下权限的 IAM 用户：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketLocation",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "arn:aws:s3:::netapp-backup-*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    }
  ]
}
```

请参见 ["AWS 文档：创建角色以向 IAM 用户委派权限"](#) 了解详细信息。

设置客户管理的AWS密钥以进行数据加密

如果您要使用默认Amazon S3加密密钥对内部集群和S3存储分段之间传递的数据进行加密、则会进行全部设置、因为默认安装会使用此类型的加密。

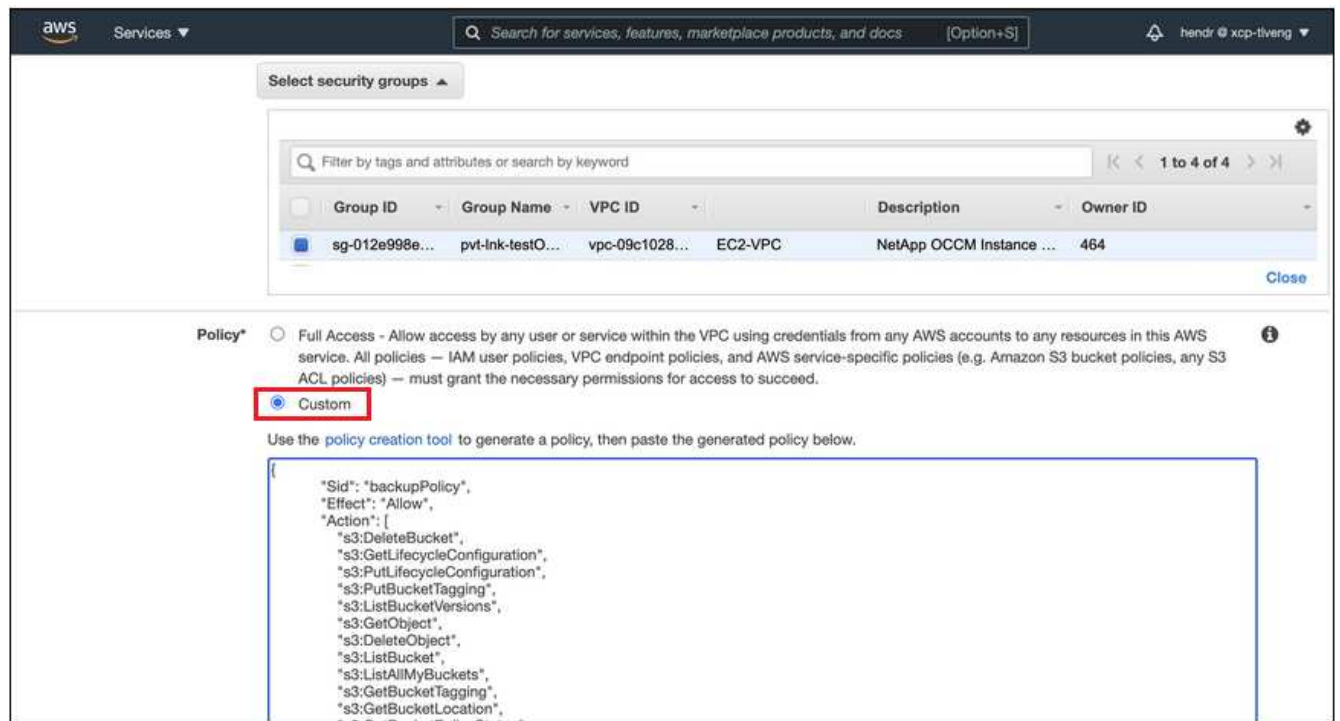
如果您要使用自己的客户管理密钥进行数据加密、而不是使用默认密钥、则在启动Cloud Backup向导之前、您需要先设置加密管理密钥。 ["了解如何使用您自己的密钥"](#)。

使用VPC端点接口为系统配置专用连接

如果您要使用标准公有 Internet连接、则所有权限均由Connector设置、无需执行任何其他操作。此类型的连接如中所示 ["第一个图"](#)。

如果您希望通过Internet从内部数据中心到VPC建立更安全的连接、可以在备份激活向导中选择AWS PrivateLink连接。如果您计划使用VPN或AWS Direct Connect通过使用专用IP地址的VPC端点接口连接内部系统、则必须使用此功能。此类型的连接如中所示 ["第二个图"](#)。

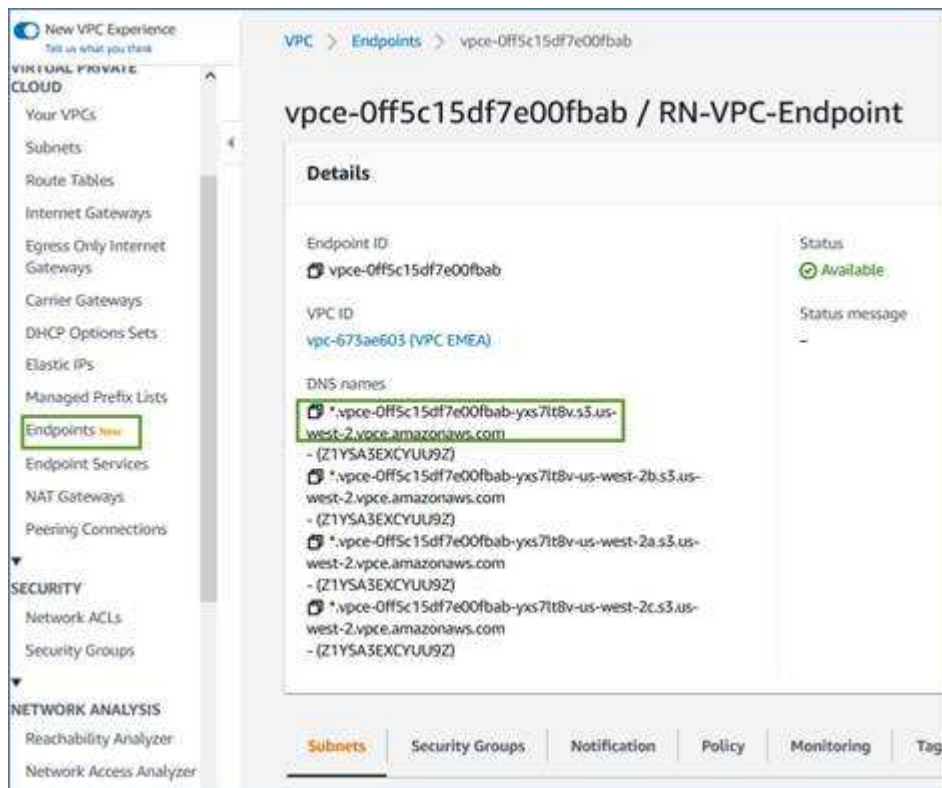
1. 使用 Amazon VPC 控制台或命令行创建接口端点配置。 ["请参见有关使用适用于 Amazon S3 的 AWS PrivateLink 的详细信息"](#)。
2. 修改与 Cloud Manager Connector 关联的安全组配置。您必须将此策略更改为 "Custom"（自定义）（从 "Full Access"），并且必须将其更改为 "Custom"（自定义） [从备份策略添加 S3 权限](#) 如前面所示。



如果您使用端口80 (HTTP)与专用端点进行通信、则表示您已设置完毕。您现在可以在集群上启用 Cloud Backup 。

如果您使用端口443 (HTTPS)与专用端点进行通信、则必须从VPC S3端点复制证书并将其添加到ONTAP 集群中、如接下来的4个步骤所示。

3. 从 AWS 控制台获取端点的 DNS 名称。



- 从 VPC S3 端点获取证书。您可以通过执行此操作 ["登录到托管 Cloud Manager Connector 的 VM"](#) 并运行以下命令。输入端点的 DNS 名称时，在开头添加 "分段"，替换 "*"：

```
[ec2-user@ip-10-160-4-68 ~]$ openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
```

- 从此命令的输出中，复制 S3 证书的数据（包括开始 / 结束证书标记之间的所有数据）：

```
Certificate chain
0 s:/CN=s3.us-west-2.amazonaws.com`
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
-----BEGIN CERTIFICATE-----
MIIM6zCCC9OgAwIBAgIQA7MGJ4FaDBR8uL0KR3oltTANBgkqhkiG9w0BAQsFADBG
...
...
GqvbOz/oO2NWLLFCqI+xmkLcMiPrZy+/6Af+HH2mLCM4EsI2b+IpBmPkriWnnxo=
-----END CERTIFICATE-----
```

- 登录到 ONTAP 集群命令行界面并使用以下命令应用您复制的证书（替换您自己的 Storage VM 名称）：

```
cluster1::> security certificate install -vserver cluster1 -type server-ca
Please enter Certificate: Press <Enter> when done
```

启用 Cloud Backup

可随时直接从内部工作环境启用 Cloud Backup。

步骤

- 在 Canvas 中，选择工作环境，然后单击右侧面板中备份和还原服务旁边的 * 启用 > 备份卷 *。

如果您的备份的 Amazon S3 目标作为工作环境存在于 Canvas 上、您可以将集群拖动到 Amazon S3 工作环境中以启动设置向导。



- 选择 Amazon Web Services 作为您的提供商，然后单击 * 下一步 *。
- 输入提供程序详细信息并单击 * 下一步 *。

- a. 用于存储备份的 AWS 帐户，AWS 访问密钥和机密密钥。

访问密钥和机密密钥适用于您创建的 IAM 用户，用于为 ONTAP 集群授予对 S3 存储分段的访问权限。

- b. 要存储备份的 AWS 区域。

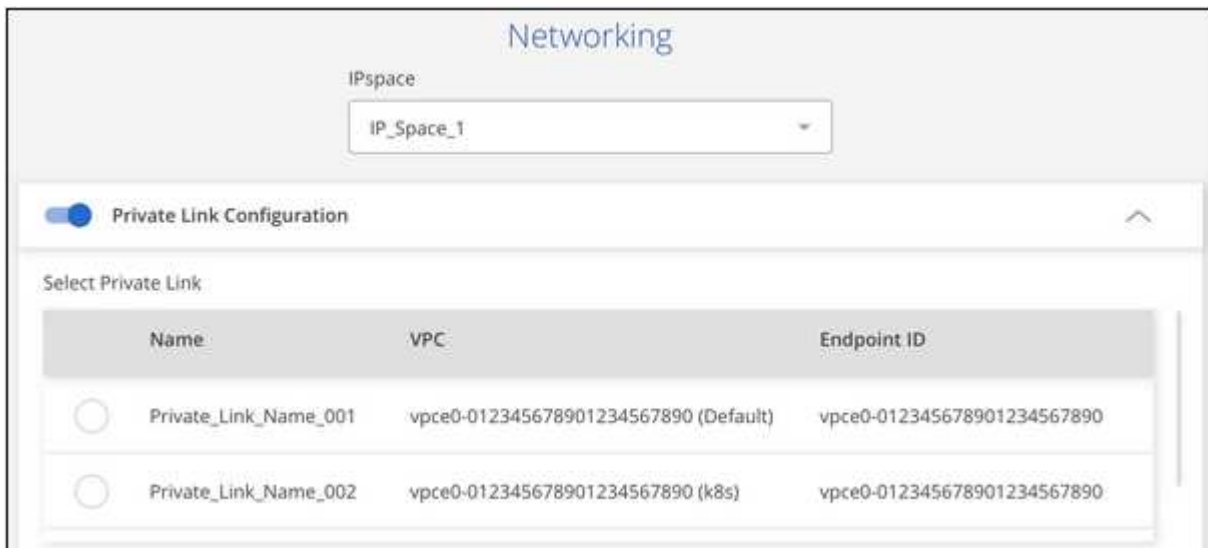
- c. 您是使用默认 Amazon S3 加密密钥，还是从 AWS 帐户中选择您自己的客户管理密钥来管理数据加密。
("了解如何使用您自己的密钥")。



4. 如果您的帐户没有 Cloud Backup 许可证、此时将提示您选择要使用的充电方法类型。您可以订阅 AWS 提供的按需购买(PAYGO) Cloud Manager Marketplace 产品(如果您有多个订阅、则需要选择一个)、或者从 NetApp 购买并激活 Cloud Backup BYOL 许可证。"了解如何设置 Cloud Backup 许可。"

5. 输入网络连接详细信息并单击 * 下一步 *。

- a. 要备份的卷所在的 ONTAP 集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站 Internet 访问权限。
- b. 或者，选择是否使用先前配置的 AWS PrivateLink。"请参见有关使用适用于 Amazon S3 的 AWS PrivateLink 的详细信息"。



Name	VPC	Endpoint ID
<input type="radio"/> Private_Link_Name_001	vpce0-012345678901234567890 (Default)	vpce0-012345678901234567890
<input type="radio"/> Private_Link_Name_002	vpce0-012345678901234567890 (k8s)	vpce0-012345678901234567890

6. 输入默认备份策略详细信息，然后单击 * 下一步 *。

- a. 定义备份计划并选择要保留的备份数。"请参见您可以选择的现有策略列表"。

- b. 使用 ONTAP 9.10.1 及更高版本时，您可以选择在一定天数后将备份分层到 S3 Glacier 或 S3 Glacier 深度归档存储，以进一步优化成本。"[了解有关使用归档层的更多信息](#)"。

7. 在选择卷页面中，使用默认备份策略选择要备份的卷。如果要为某些卷分配不同的备份策略，可以创建其他策略并稍后将其应用于这些卷。

- 要备份所有卷，请选中标题行 (☒ Volume Name)。
- 要备份单个卷，请选中每个卷对应的框 (☒ Volume_1)。

<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active

☒ Automatically back up future volumes on all storage VMs with the selected backup policy

如果希望将来添加的所有卷都启用备份，只需选中 "自动备份未来卷 ..." 复选框即可。如果禁用此设置，则需要手动为未来的卷启用备份。

8. 单击 * 激活备份 * ， Cloud Backup 将开始对卷进行初始备份。

Cloud Backup 将开始对每个选定卷进行初始备份，此时将显示卷备份信息板，以便您可以监控备份的状态。

您可以 ["启动和停止卷备份或更改备份计划"](#)。您也可以 ["从备份文件还原整个卷或单个文件"](#) 连接到 AWS 中的 Cloud Volumes ONTAP 系统或内部 ONTAP 系统。

将内部 ONTAP 数据备份到 StorageGRID

完成几个步骤，开始将数据从内部 ONTAP 系统备份到 NetApp StorageGRID 系统中的对象存储。

请注意，"内部 ONTAP 系统" 包括 FAS ， AFF 和 ONTAP Select 系统。

快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。

跨度 class="image">https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png" Alt-one"> 验证是否支持您的配置

- 您已发现内部集群并将其添加到 Cloud Manager 中的工作环境中。请参见 ["发现 ONTAP 集群"](#) 了解详细信息。
 - 此集群运行的是 ONTAP 9.7P5 或更高版本。
 - 集群具有 SnapMirror 许可证—它作为超值包或数据保护包的一部分提供。
 - 集群必须与 StorageGRID 和 Connector 建立所需的网络连接。
- 您的内部安装了一个 Connector 。
 - 无论是否可访问 Internet ， 均可将 Connector 安装在站点中。
 - 通过为连接器建立网络，可以与 ONTAP 集群和 StorageGRID 建立出站 HTTPS 连接。
- 您已购买 ["并激活"](#) NetApp 提供的 Cloud Backup BYOL 许可证。
- 您的 StorageGRID 安装了 10.3 或更高版本，并且访问密钥具有 S3 权限。

选择工作环境，然后单击右侧面板中备份和还原服务旁边的 * 启用 > 备份卷 * ， 然后按照设置向导进行操作。



选择 StorageGRID 作为提供程序，然后输入 StorageGRID 服务器和服务帐户详细信息。您还需要在卷所在的 ONTAP 集群中指定 IP 空间。

默认策略每天备份卷，并保留每个卷的最新 30 个备份副本。更改为每小时，每天，每周或每月备份，或者选择一个提供更多选项的系统定义策略。您还可以更改要保留的备份副本数。

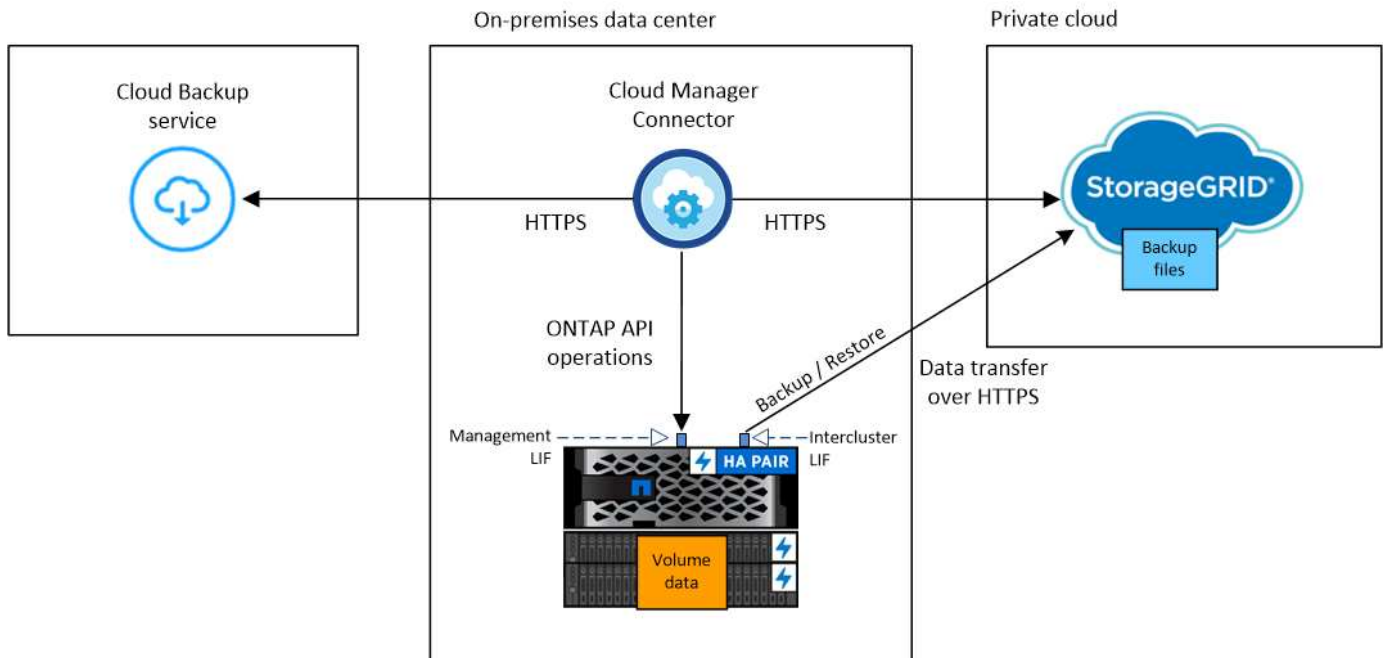
在选择卷页面中，使用默认备份策略确定要备份的卷。如果要为某些卷分配不同的备份策略，可以创建其他策略并稍后将其应用于卷。

系统会在您输入的 S3 访问密钥和机密密钥所指示的服务帐户中自动创建 S3 存储分段，备份文件存储在该处。

要求

在开始将内部卷备份到 StorageGRID 之前，请阅读以下要求，以确保您的配置受支持。

下图显示了将内部 ONTAP 系统备份到 StorageGRID 时的每个组件以及需要在它们之间准备的连接：



如果 Connector 和内部 ONTAP 系统安装在无法访问 Internet 的内部位置，则 StorageGRID 系统必须位于同一内部数据中心。

准备 ONTAP 集群

您需要先在 Cloud Manager 中发现内部 ONTAP 集群，然后才能开始备份卷数据。

["了解如何发现集群"](#)。

ONTAP 要求

- 建议至少使用 ONTAP 9.7P5；ONTAP 9.8P11 及更高版本。
- SnapMirror 许可证（作为超值包或数据保护包的一部分提供）。
- 注意：* 使用 Cloud Backup 时不需要 "混合云捆绑包"。

请参见操作说明 ["管理集群许可证"](#)。

- 已正确设置时间和时区。

请参见操作说明 ["配置集群时间"](#)。

集群网络连接要求

- ONTAP 集群通过用户指定的端口从集群间 LIF 启动 HTTPS 连接到 StorageGRID，以执行备份和还原操作。此端口可在备份设置期间进行配置。

ONTAP 可在对象存储之间读取和写入数据。对象存储永远不会启动，而只是响应。

- ONTAP 需要从连接器到集群管理 LIF 的入站连接。连接器必须位于您的内部。
- 托管要备份的卷的每个 ONTAP 节点都需要一个集群间 LIF。LIF 必须与 `_IP 空间_` 关联，ONTAP 应使用此 `_IP 空间_` 连接到对象存储。 ["了解有关 IP 空间的更多信息"](#)。

设置 Cloud Backup 时，系统会提示您使用 IP 空间。您应选择与每个 LIF 关联的 IP 空间。这可能是您创建的 "默认" IP 空间或自定义 IP 空间。

- 节点的集群间 LIF 可以访问对象存储（如果在 "非公开" 站点中安装了 Connector，则不需要）。
- 已为卷所在的 Storage VM 配置 DNS 服务器。请参见操作说明 ["为 SVM 配置 DNS 服务"](#)。
- 请注意，如果您使用的 IP 空间与默认 IP 空间不同，则可能需要创建静态路由才能访问对象存储。
- 如有必要，请更新防火墙规则，以允许通过您指定的端口（通常为端口 443）从 ONTAP 到对象存储的 Cloud Backup Service 连接，并允许通过端口 53（TCP/UDP）从 Storage VM 到 DNS 服务器的名称解析流量。

正在准备 StorageGRID

StorageGRID 必须满足以下要求。请参见 ["StorageGRID 文档"](#) 有关详细信息 ...

支持的 StorageGRID 版本

支持 StorageGRID 10.3 及更高版本。

S3 凭据

在设置到 StorageGRID 的备份时，备份向导会提示您为服务帐户输入 S3 访问密钥和机密密钥。通过服务帐户，Cloud Backup 可以对用于存储备份的 StorageGRID 存储分段进行身份验证和访问。这些密钥是必需的，以便 StorageGRID 知道是谁发出请求。

这些访问密钥必须与具有以下权限的用户相关联：

```
"s3:ListAllMyBuckets",  
"s3:ListBucket",  
"s3:GetObject",  
"s3:PutObject",  
"s3:DeleteObject",  
"s3:CreateBucket"
```

对象版本控制

不能在对象存储分段上启用 StorageGRID 对象版本控制。

创建或切换连接器

将数据备份到 StorageGRID 时，您的内部必须具有一个连接器。您需要安装新的 Connector 或确保当前选定的 Connector 位于内部。无论是否可访问 Internet，均可将 Connector 安装在站点中。

- ["了解连接器"](#)
- ["在可访问 Internet 的 Linux 主机上安装 Connector"](#)
- ["在无法访问 Internet 的 Linux 主机上安装 Connector"](#)
- ["在连接器之间切换"](#)



Cloud Manager Connector 内置了 Cloud Backup 功能。如果安装在无法连接 Internet 的站点上，则需要定期更新 Connector 软件才能访问新功能。检查 ["Cloud Backup 新增功能"](#) 要查看每个 Cloud Backup 版本中的新功能，然后您可以按照步骤执行操作 ["升级 Connector 软件"](#) 希望使用新功能时。

为连接器准备网络连接

确保此连接器具有所需的网络连接。

步骤

1. 确保安装 Connector 的网络启用以下连接：
 - 通过端口 443 与 StorageGRID 建立 HTTPS 连接
 - 通过端口 443 与 ONTAP 集群管理 LIF 建立 HTTPS 连接
 - 通过端口 443 与 Cloud Backup 建立出站 Internet 连接（在 "非公开" 站点中安装 Connector 时不需要）

许可证要求

在为集群激活 Cloud Backup 之前、您需要从 NetApp 购买并激活 Cloud Backup BYOL 许可证。此许可证适用于帐户，可在多个系统中使用。

您需要 NetApp 提供的序列号，以便在许可证有效期和容量内使用此服务。 ["了解如何管理 BYOL 许可证"](#)。



将文件备份到 StorageGRID 时不支持 PAYGO 许可。

启用云备份到 **StorageGRID**

可随时直接从内部工作环境启用 Cloud Backup 。

步骤

1. 在 Canvas 中，选择内部工作环境，然后单击右侧面板中备份和还原服务旁边的 * 启用 > 备份卷 *



2. 选择 * StorageGRID 提供程序 *，单击 * 下一步 *，然后输入提供程序详细信息：
 - a. StorageGRID 服务器的 FQDN 以及 ONTAP 与 StorageGRID 进行 HTTPS 通信时应使用的端口；例如：
s3.eng.company.com:8082
 - b. 用于访问存储备份的存储分段的访问密钥和机密密钥。
 - c. 要备份的卷所在的 ONTAP 集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站 Internet 访问权限（在 "非公开" 站点中安装 Connector 时不需要）。

选择正确的 IP 空间可确保 Cloud Backup 可以设置从 ONTAP 到 StorageGRID 对象存储的连接。

请注意，服务启动后，您无法更改此信息。

3. 在 *Define Policy* 页面中，选择默认备份计划和保留值，然后单击 * 下一步 *。

请参见 ["现有策略的列表"](#)。

4. 在选择卷页面中，使用默认备份策略选择要备份的卷。如果要为某些卷分配不同的备份策略，可以创建其他策略并稍后将其应用于这些卷。
 - 要备份所有卷，请选中标题行 (☒ Volume Name)。
 - 要备份单个卷，请选中每个卷对应的框 (☒ Volume_1)。

Select Volumes						
57 Volumes						
<input checked="" type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Volume_Name_1 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 On	DP	SVM_Name_2	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 On	RW	SVM_Name_1	0.25 TB	10 TB	Not Active
<input checked="" type="checkbox"/> Automatically back up future volumes on all storage VMs with the selected backup policy						

如果您希望将来添加到此集群的所有卷都启用备份，只需选中 "自动备份未来卷 ..." 复选框即可。如果禁用此设置，则需要手动为未来的卷启用备份。

5. 单击 * 激活备份 *，Cloud Backup 将开始对每个选定卷进行初始备份。

系统会在您输入的 S3 访问密钥和机密密钥所指示的服务帐户中自动创建 S3 存储分段，备份文件存储在该处。此时将显示卷备份信息板，以便您可以监控备份的状态。

您可以 ["启动和停止卷备份或更改备份计划"](#)。您也可以 ["从备份文件还原整个卷或单个文件"](#) 内部部署的ONTAP系统。

管理 ONTAP 系统的备份

您可以通过更改备份计划，启用 / 禁用卷备份，删除备份等来管理 Cloud Volumes ONTAP 和内部 ONTAP 系统的备份。



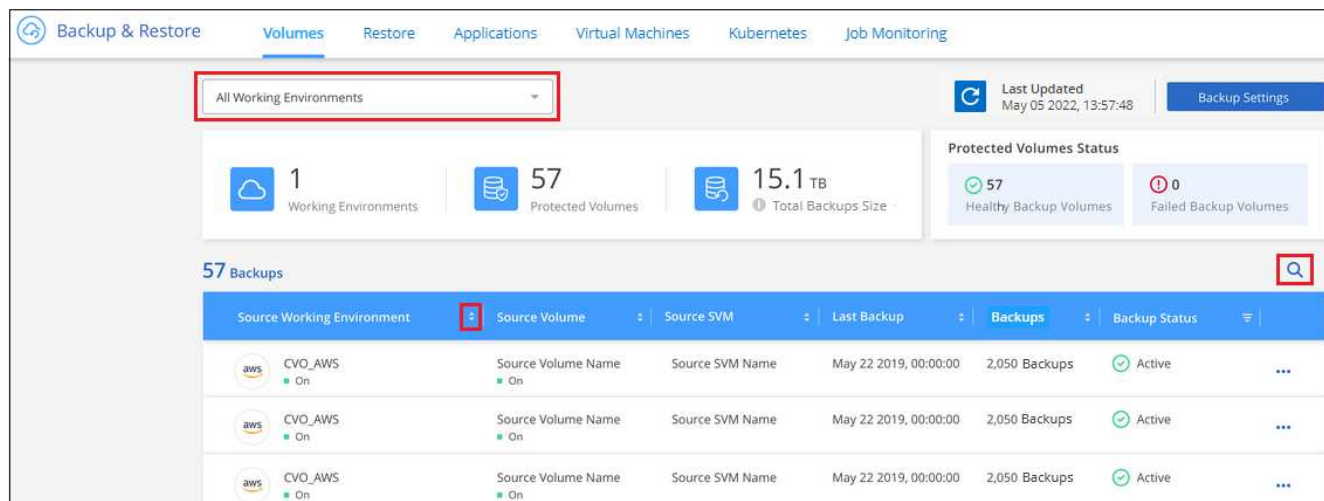
请勿直接从云提供商环境管理或更改备份文件。这可能会损坏文件并导致配置不受支持。

查看要备份的卷

您可以在备份信息板中查看当前正在备份的所有卷的列表。

步骤

1. 单击 * 备份和还原 * 选项卡。
2. 单击 * 卷 * 选项卡可查看 Cloud Volumes ONTAP 和内部 ONTAP 系统的卷列表。



如果要在某些工作环境中查找特定卷，您可以按工作环境和卷细化列表，也可以使用搜索筛选器。

启用和禁用卷备份

如果您不需要卷的备份副本，并且不想为存储备份付费，则可以停止备份卷。如果当前未备份新卷，您也可以将其添加到备份列表中。

步骤

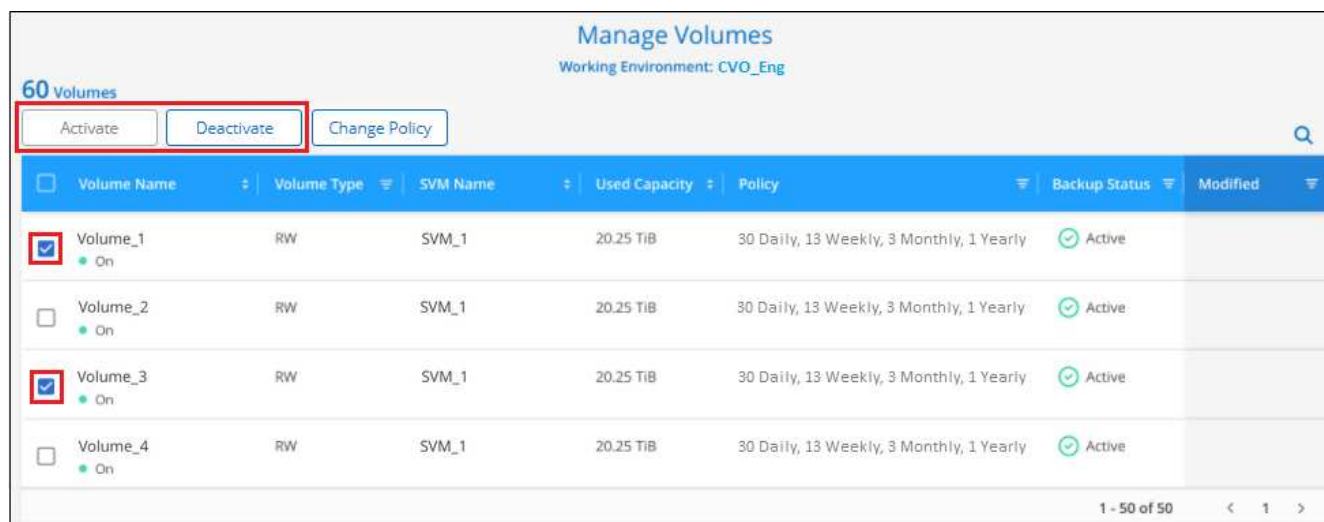
1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



2. 在 *Backup Settings* page 中，单击 ... 对于工作环境，请选择 * 管理卷 *。



3. 选中要更改的一个或多个卷对应的复选框，然后根据要启动还是停止卷的备份，单击 * 激活 * 或 * 停用 *。



4. 单击 * 保存 * 以提交更改。

- 注意：* 停止备份卷时，云提供商会继续为备份所用容量收取对象存储成本，除非您这样做 [删除备份](#)。

编辑现有备份策略

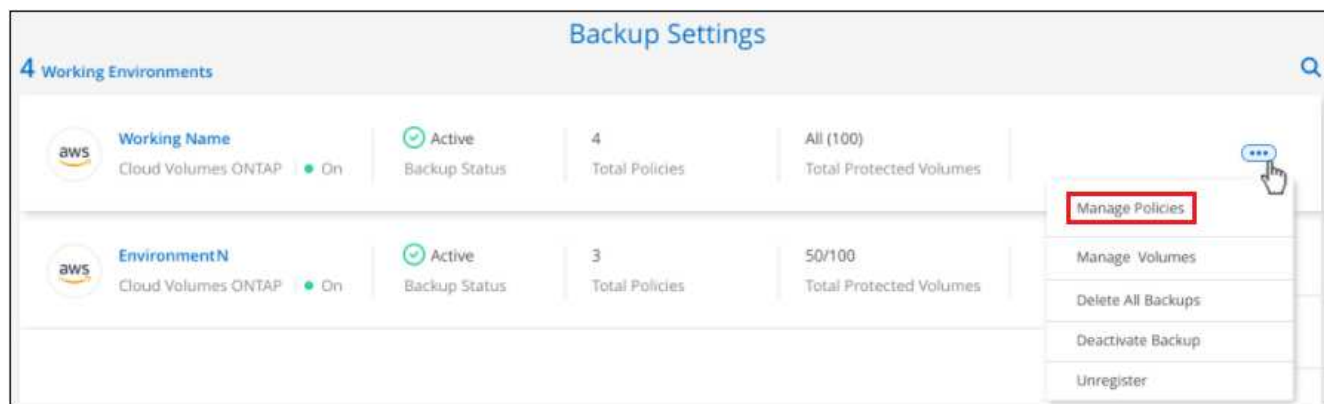
您可以更改当前应用于工作环境中卷的备份策略的属性。更改备份策略会影响正在使用此策略的所有现有卷。

步骤

1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



2. 从 *Backup Settings* 页面中，单击 ... 对于要更改设置的工作环境，请选择 * 管理策略 *。



3. 在 *Manage Policies* 页面中，为要在该工作环境中更改的备份策略单击 * 编辑策略 *。

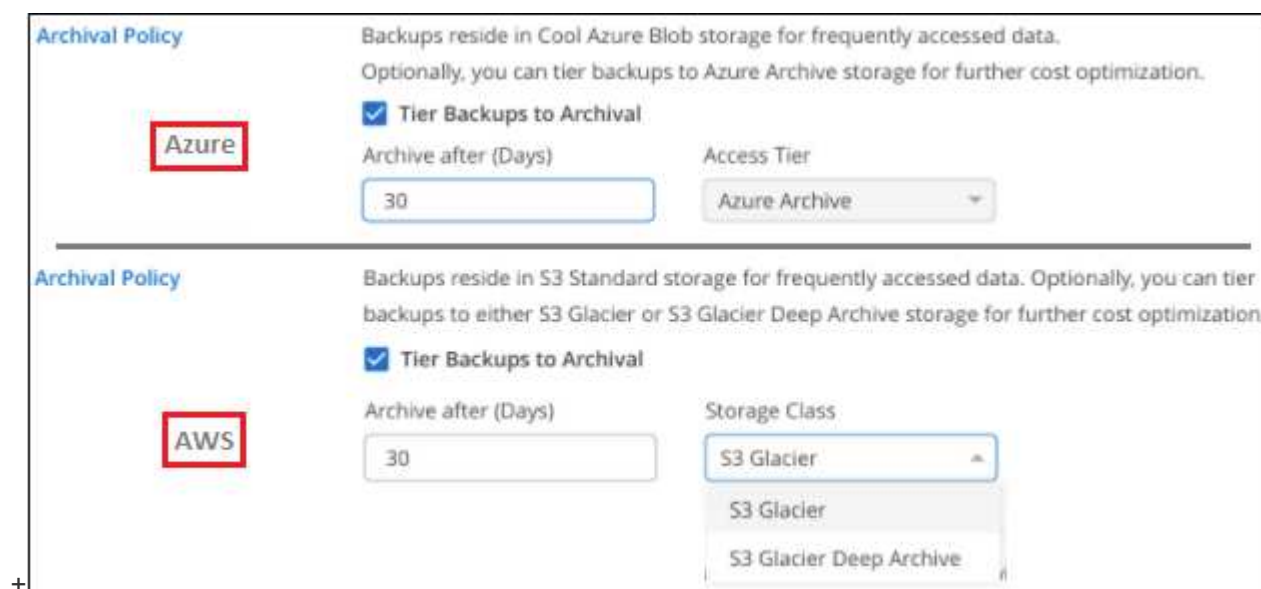


4. 在 *Edit Policy* 页面中，更改计划和备份保留，然后单击 * 保存 *。



如果集群运行的是ONTAP 9.10.1或更高版本、您还可以选择在一定天数后启用或禁用对归档存储的备份进行分层。

"了解有关使用 AWS 归档存储的更多信息"。



+ 请注意、如果您停止将备份分层到归档存储、则已分层到归档存储的所有备份文件都会保留在该层中、而不会自动将这些备份移回标准层。

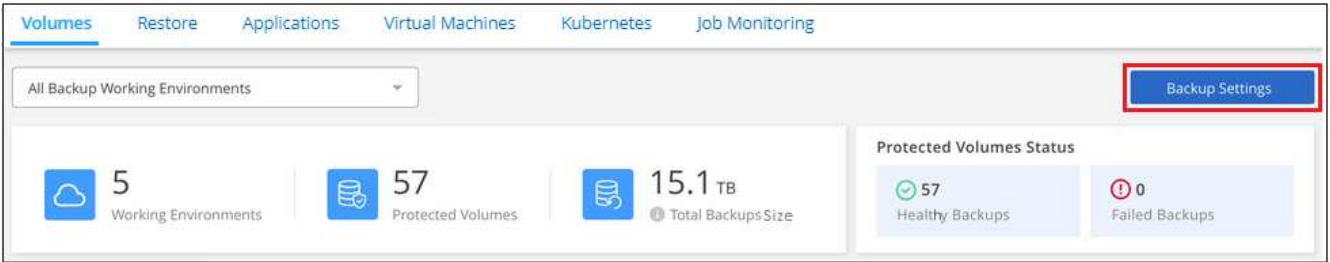
正在添加新备份策略

在为工作环境启用 Cloud Backup 时，您最初选择的所有卷都会使用您定义的默认备份策略进行备份。如果要为具有不同恢复点目标（RPO）的某些卷分配不同的备份策略，您可以为该集群创建其他策略并将这些策略分配给其他卷。

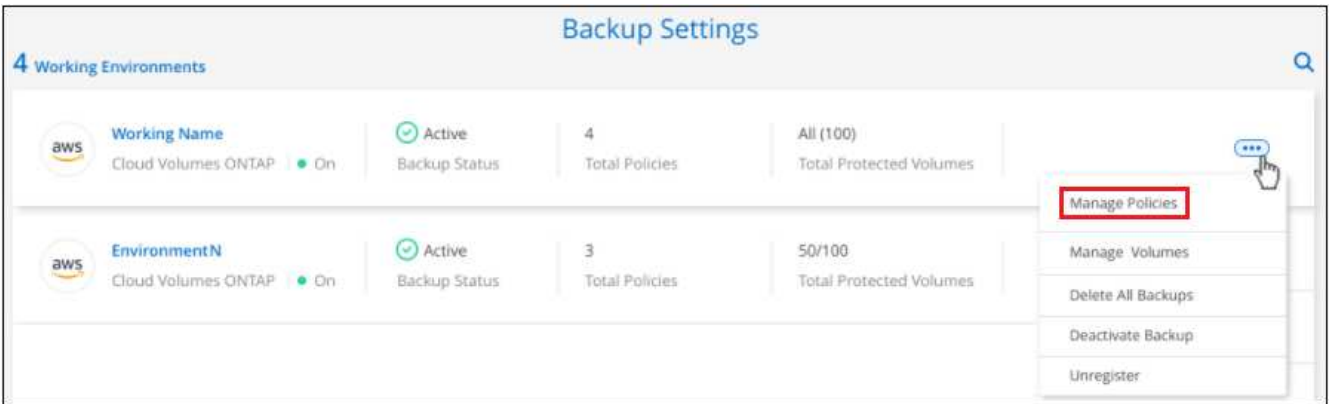
如果要对工作环境中的某些卷应用新的备份策略，则首先需要将备份策略添加到工作环境中。然后，您可以 [将此策略应用于该工作环境中的卷](#)。

步骤

1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



2. 从 *Backup Settings* 页面中，单击 ... 对于要添加新策略的工作环境，请选择 * 管理策略 *。



3. 在 *Manage Policies* 页面中，单击 * 添加新策略 *。



4. 在 *Add New Policy* 页面中，定义计划和备份保留，然后单击 * 保存 *。

如果集群运行的是ONTAP 9.10.1或更高版本、您还可以选择在一定天数后启用或禁用对归档存储的备份进行分层。

"了解有关使用 AWS 归档存储的更多信息"。

更改分配给现有卷的策略

如果要更改备份频率或更改保留值，则可以更改分配给现有卷的备份策略。

请注意，要应用于卷的策略必须已存在。 [请参见如何为工作环境添加新的备份策略。](#)

步骤

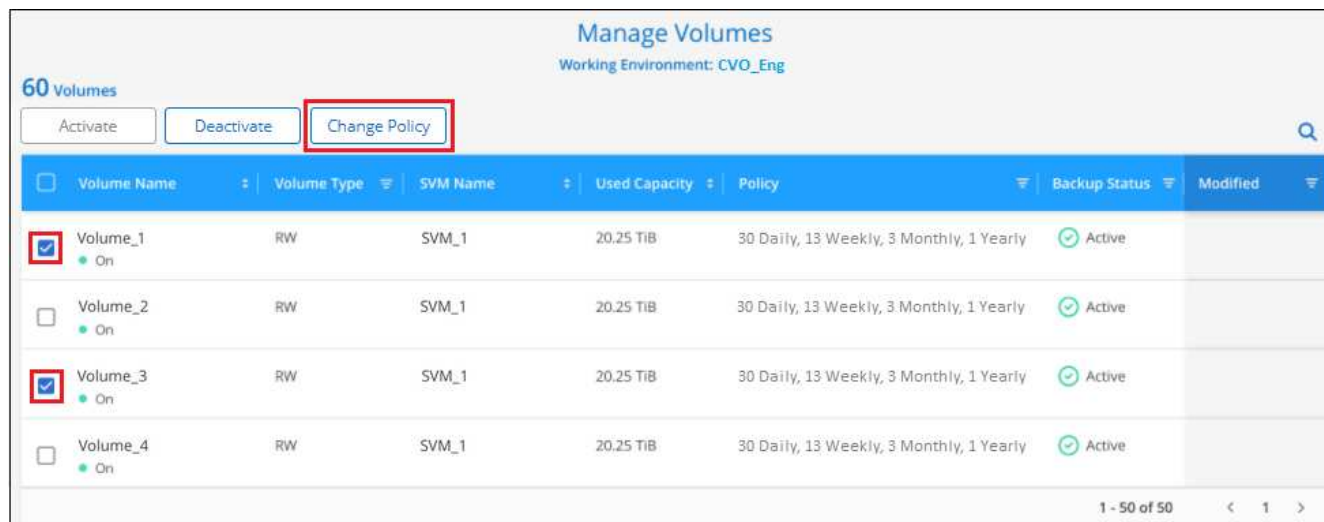
1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



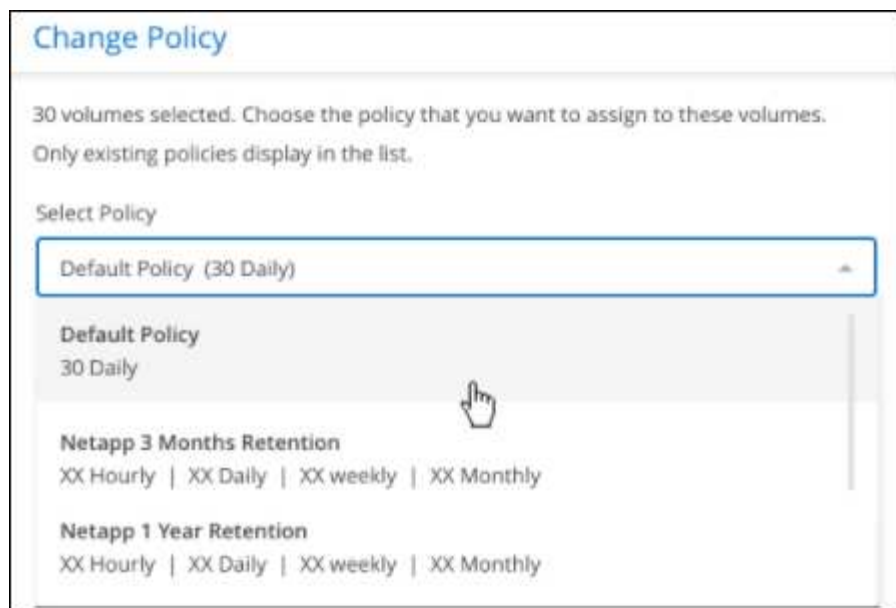
2. 在 *Backup Settings* page 中，单击 ... 对于存在卷的工作环境，请选择 * 管理卷 *。



3. 选中要更改策略的一个或多个卷对应的复选框，然后单击 * 更改策略 *。



4. 在 *Change Policy* 页面中，选择要应用于卷的策略，然后单击 * 更改策略 *。



5. 单击 * 保存 * 以提交更改。

设置要分配给新卷的备份策略

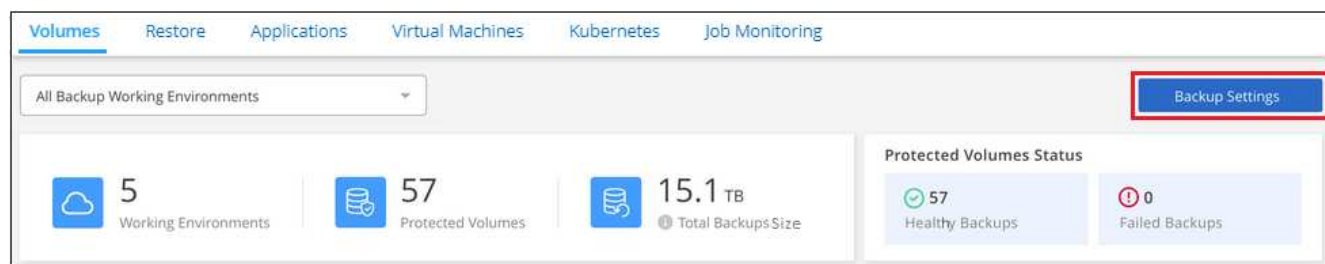
如果在ONTAP 集群上首次激活云备份时未选择将备份策略自动分配给新创建的卷的选项、则可以稍后在_Backup Settings_页面中选择此选项。为新创建的卷分配备份策略可确保所有数据都受到保护。

请注意，要应用于卷的策略必须已存在。 [请参见如何为工作环境添加新的备份策略。](#)

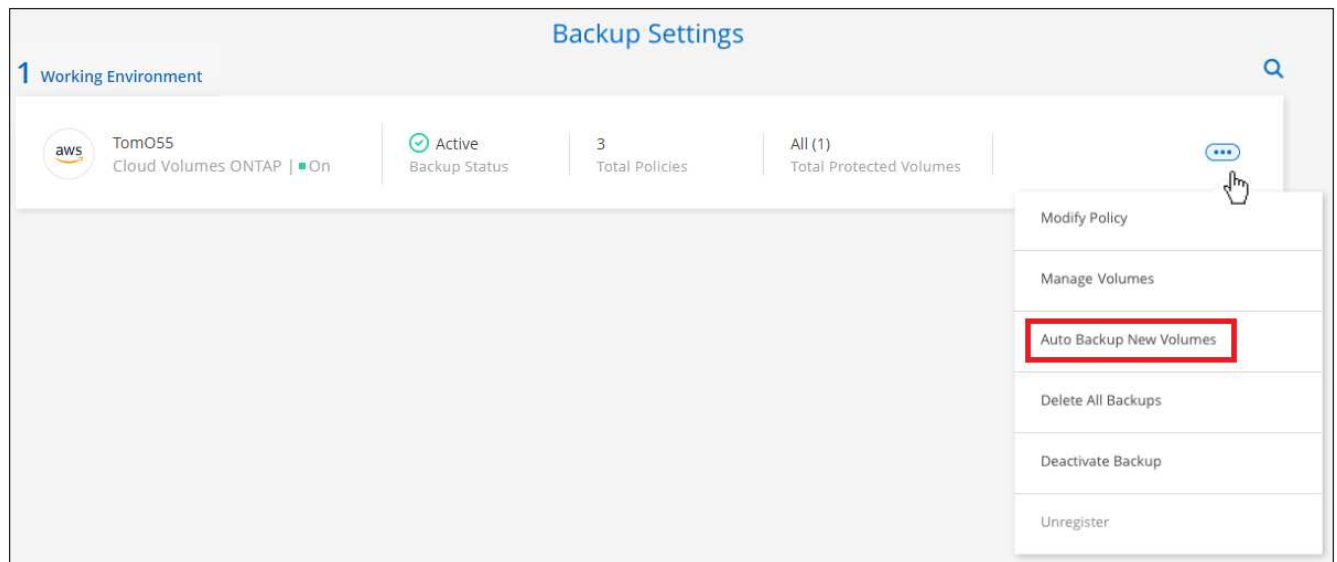
您也可以禁用此设置、以使新创建的卷不会自动备份。在这种情况下、您需要手动为将来要备份的任何特定卷启用备份。

步骤

1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



2. 在 *Backup Settings page* 中，单击 ... 对于存在卷的工作环境、请选择*自动备份新卷*。



3. 选中"自动备份新卷..."复选框、选择要应用于新卷的备份策略、然后单击*保存*。

Auto Backup New Volumes

☒ Automatically back up new volumes on all SVMs for Working Environment TomO55

Choose the policy that will be assigned to new volumes. Only existing policies are shown in the list.

Select Backup Policy

CloudBackupService-1611307085985_V2 (30 Daily)

Save

Cancel

现在、此备份策略将应用于使用Cloud Manager、System Manager或ONTAP 命令行界面在此工作环境中创建的任何新卷。

随时创建手动卷备份

您可以随时创建按需备份，以捕获卷的当前状态。如果对卷进行了非常重要的更改，而您不希望等待下一次计划备份来保护该数据，或者如果卷当前未进行备份，而您希望捕获其当前状态，则此功能将非常有用。

备份名称包含时间戳，以便您可以从其他计划的备份中确定按需备份。

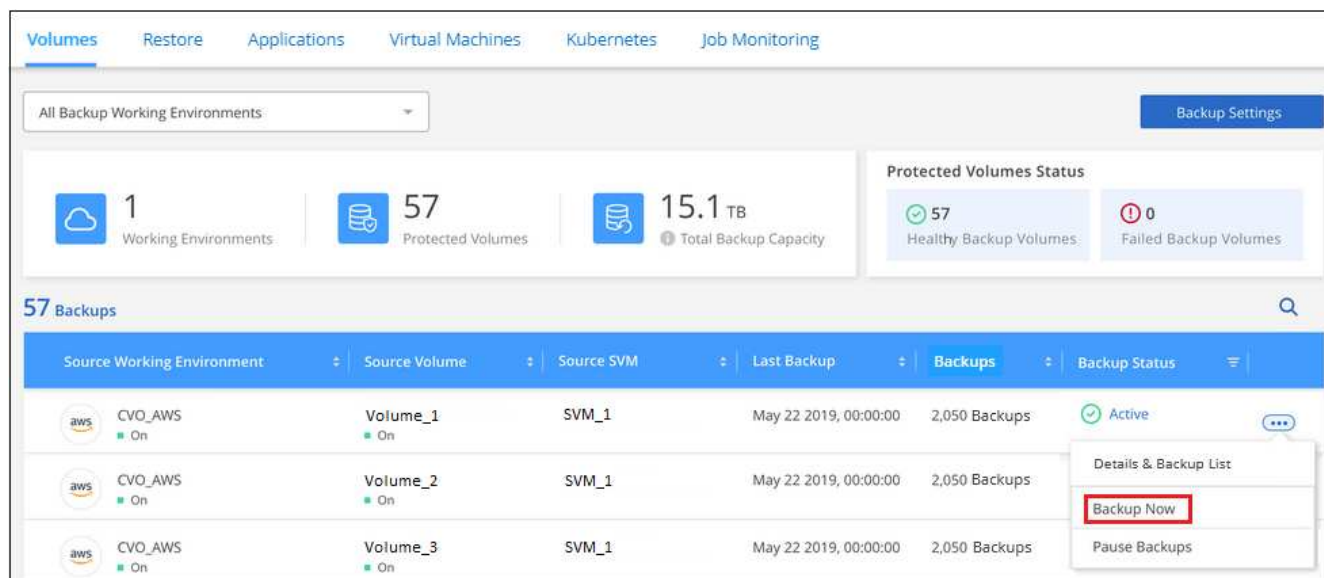
请注意、在创建临时备份时、系统会在源卷上创建Snapshot。由于此Snapshot不属于正常的Snapshot计划、因此不会关闭它。备份完成后、您可能需要从源卷中手动删除此Snapshot。这样可以释放与此Snapshot相关的块。Snapshot的名称将以`CBS-snapshot-adoc-`开头。 ["请参见如何使用ONTAP 命令行界面删除快照"](#)。



数据保护卷不支持按需卷备份。

步骤

1. 从 * 卷 * 选项卡中，单击 ... 并选择 * 立即备份 * 。



在创建备份之前，该卷的备份状态列会显示 " 正在进行 " 。

查看每个卷的备份列表

您可以查看每个卷的所有备份文件的列表。此页面显示有关源卷，目标位置和备份详细信息，例如上次执行的备份，当前备份策略，备份文件大小等。

您还可以通过此页面执行以下任务：

- 删除卷的所有备份文件
- 删除卷的单个备份文件
- 下载卷的备份报告

步骤

1. 从 * 卷 * 选项卡中，单击 ... 对于源卷，然后选择 * 详细信息和备份列表 * 。

The screenshot shows the 'Volumes' tab in the Cloud Backup console. At the top, there are navigation links: Volumes, Restore, Applications, Virtual Machines, Kubernetes, and Job Monitoring. A dropdown menu shows 'All Backup Working Environments'. A summary bar indicates 1 Working Environment, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. A 'Protected Volumes Status' box shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a table lists 57 Backups. The table has columns: Source Working Environment, Source Volume, Source SVM, Last Backup, Backups, and Backup Status. A context menu is open for the first backup, showing options: 'Details & Backup List' (highlighted), 'Backup Now', and 'Pause Backups'.

此时将显示所有备份文件的列表以及有关源卷，目标位置和备份详细信息。

The screenshot shows the 'Details & Backup List' view in the Cloud Backup console. It is divided into three main sections: Source, Destination, and Backup Information. The Source section shows 'Working Environment N...' and 'Cloud Volumes ONTAP (HA)'. The Destination section shows 'AWS' and 'us-east-1'. The Backup Information section shows 'Active' status, 'Last Backup' on Oct 05 2021, and 'Backups' count of 2,050. Below these sections, a table lists 2,050 Backups. The table has columns: Backup Name, Date, Size, and Actions. The first three rows of the table are visible, showing backup names like 'Backup_2020_Jan', 'Backup_2020_Mar', and 'Backup_2020_Apr'.

删除备份

您可以通过 Cloud Backup 删除单个备份文件，删除卷的所有备份或删除工作环境中所有卷的所有备份。如果您不再需要备份，或者删除了源卷并希望删除所有备份，则可能需要删除所有备份。



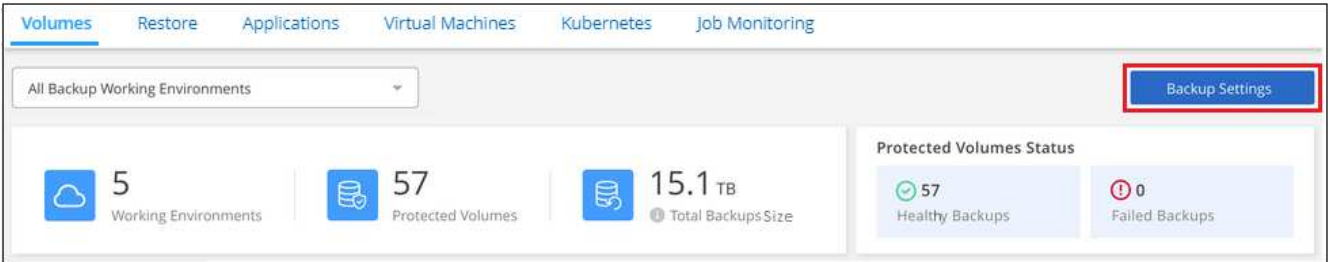
如果您计划删除具有备份的工作环境或集群，则必须删除备份 * 在删除系统之前 *。删除系统时，Cloud Backup 不会自动删除备份，并且用户界面当前不支持在删除系统后删除这些备份。对于任何剩余备份，您仍需支付对象存储成本费用。

删除工作环境中的所有备份文件

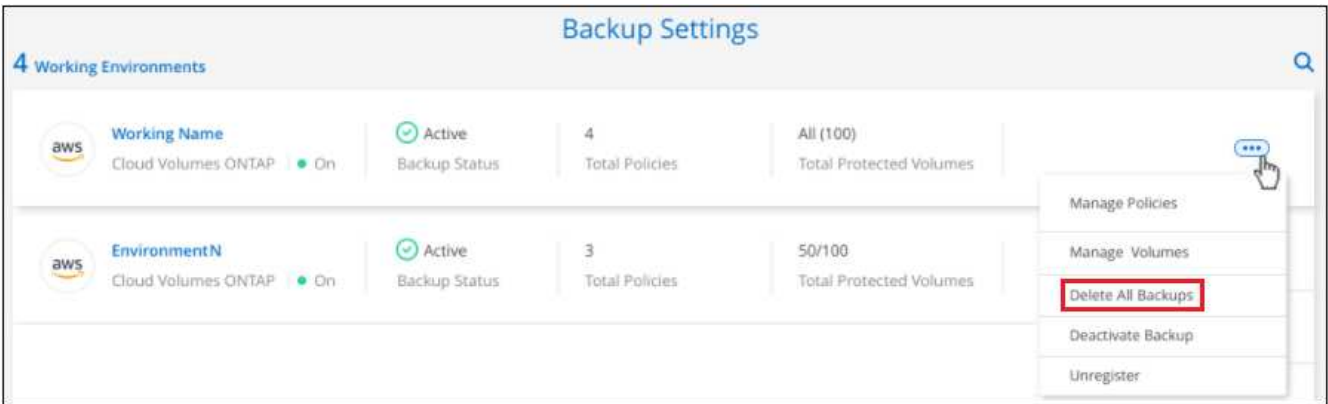
删除工作环境中的所有备份不会禁用此工作环境中的卷将来备份。如果要停止在工作环境中创建所有卷的备份，可以停用备份 [如此处所述](#)。

步骤

- 1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



- 2. 单击 ... 对于要删除所有备份并选择 * 删除所有备份 * 的工作环境。



- 3. 在确认对话框中，输入工作环境的名称，然后单击 * 删除 *。

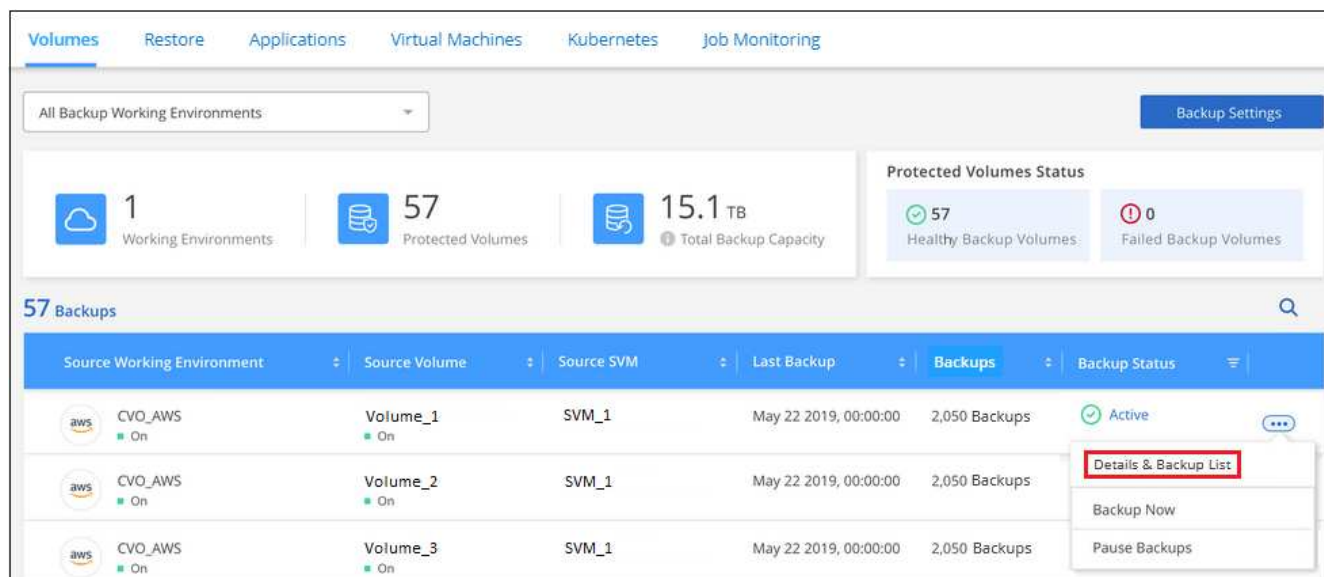
删除卷的所有备份文件

删除卷的所有备份也会禁用该卷的未来备份。

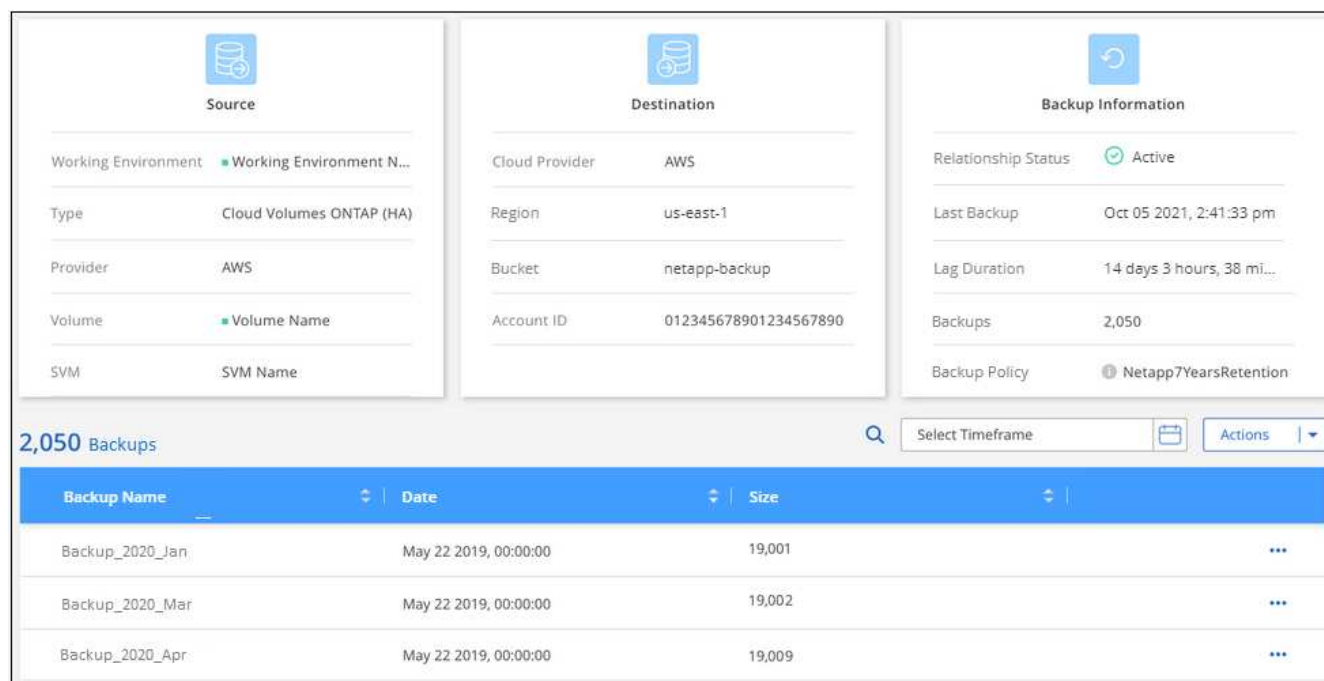
您可以 [重新开始为卷创建备份](#) 可随时从管理备份页面访问。

步骤

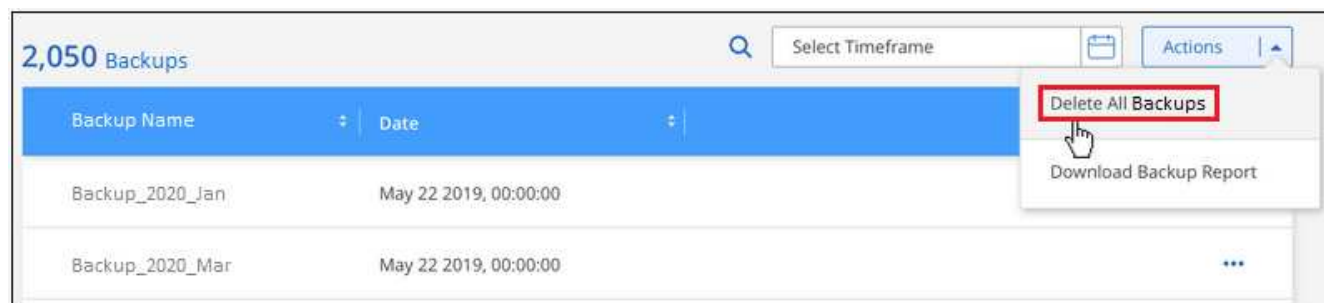
- 1. 从 * 卷 * 选项卡中，单击 ... 对于源卷，然后选择 * 详细信息和备份列表 *。



此时将显示所有备份文件的列表。



2. 单击 * 操作 * > * 删除所有备份 *。



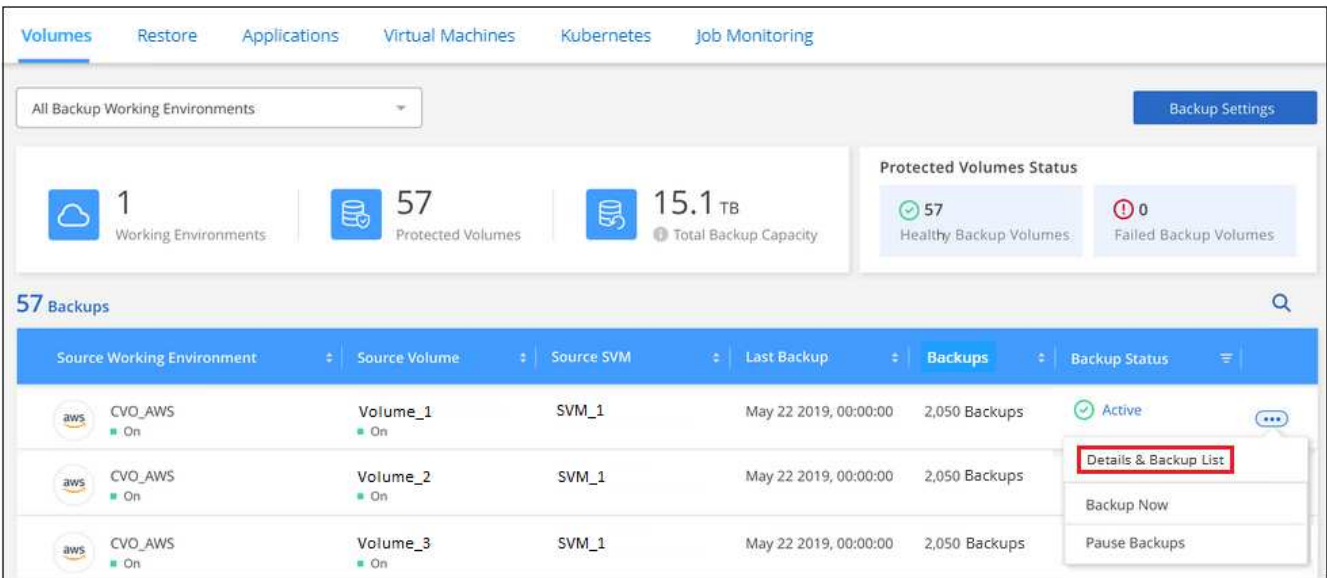
3. 在确认对话框中，输入卷名称并单击 * 删除 *。

删除卷的单个备份文件

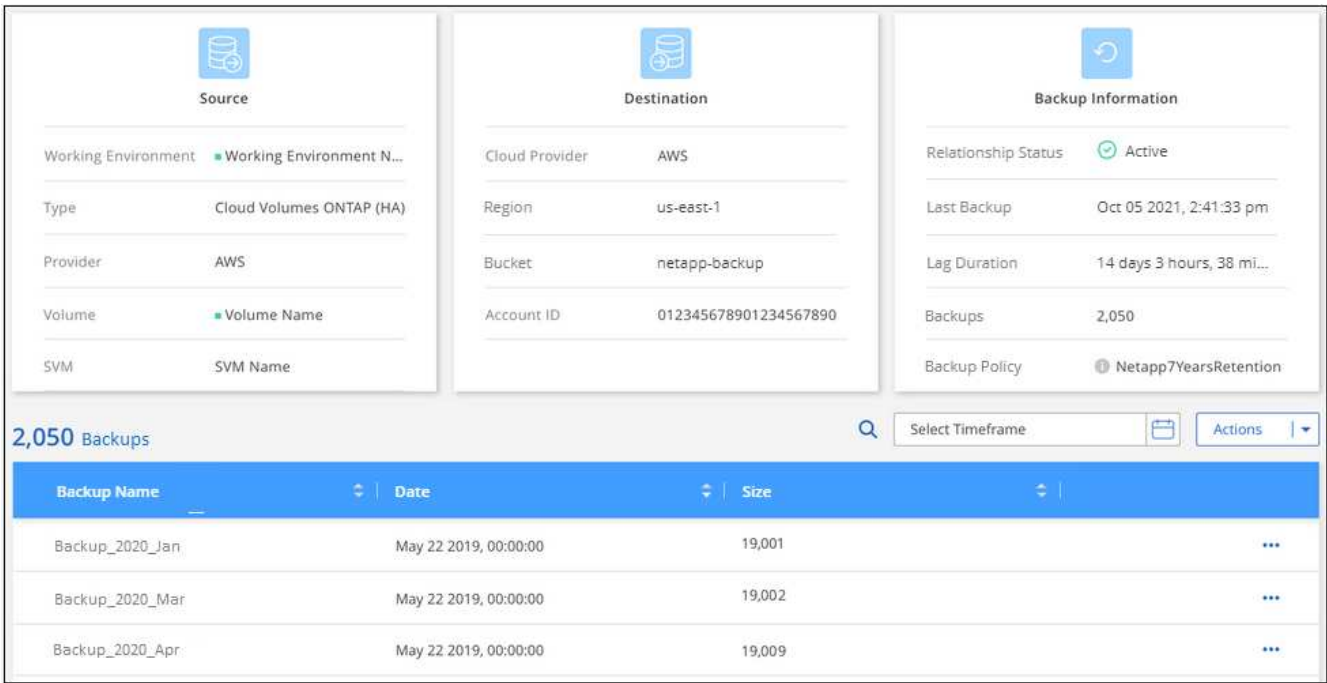
您可以删除单个备份文件。只有在使用 ONTAP 9.8 或更高版本的系统创建卷备份时，此功能才可用。

步骤

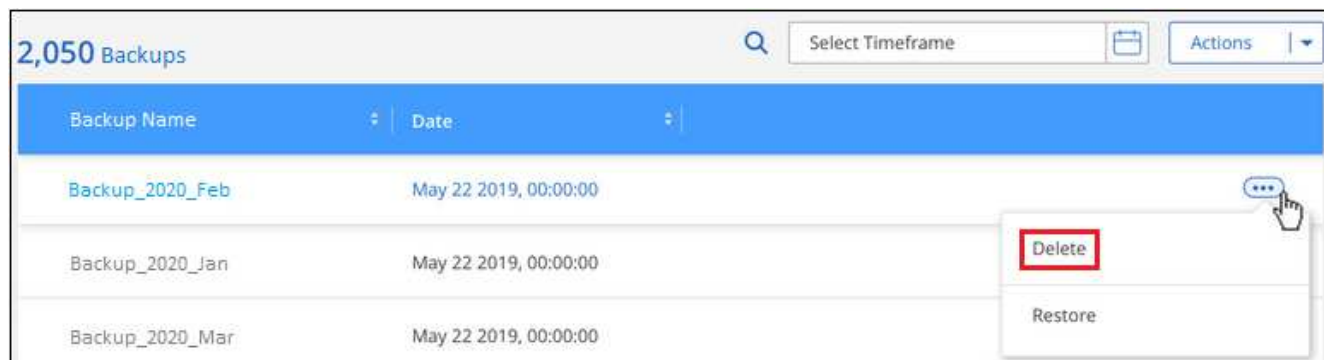
1. 从 * 卷 * 选项卡中，单击 ... 对于源卷，然后选择 * 详细信息和备份列表 * 。



此时将显示所有备份文件的列表。



2. 单击 ... 对于要删除的卷备份文件，然后单击 * 删除 * 。



3. 在确认对话框中，单击 * 删除 *。

为工作环境禁用 Cloud Backup

禁用工作环境的 Cloud Backup 会禁用系统上每个卷的备份，同时也会禁用还原卷的功能。不会删除任何现有备份。这样不会从此工作环境中取消注册备份服务—它基本上允许您将所有备份和还原活动暂停一段时间。

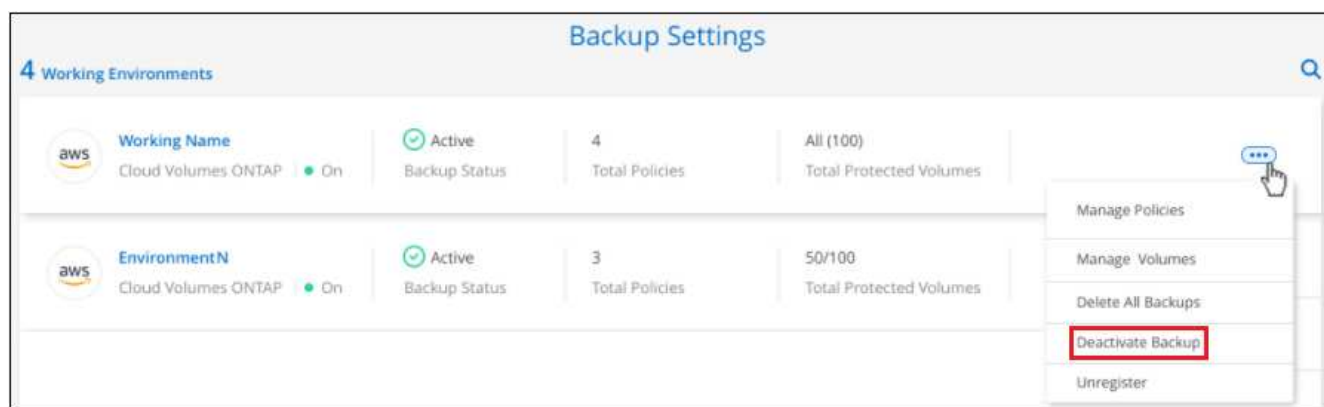
请注意，除非您的备份使用的容量，否则云提供商会继续向您收取对象存储成本 [删除备份](#)。

步骤

1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



2. 在 *Backup Settings page* 中，单击 ... 对于要禁用备份的工作环境，请选择 * 停用备份 *。



3. 在确认对话框中，单击 * 停用 *。



在禁用备份的情况下，系统将为此工作环境显示一个 * 激活备份 * 按钮。如果要为该工作环境重新启用备份功能，可以单击此按钮。

为工作环境取消注册 Cloud Backup

如果您不想再使用备份功能，而希望在工作环境中不再需要为备份付费，则可以取消注册适用于此工作环境的 Cloud Backup。通常，如果您计划删除工作环境并要取消备份服务，则会使用此功能。

如果要更改存储集群备份的目标对象存储，也可以使用此功能。在为工作环境取消注册 Cloud Backup 后，您可以使用新的云提供商信息为此集群启用 Cloud Backup。

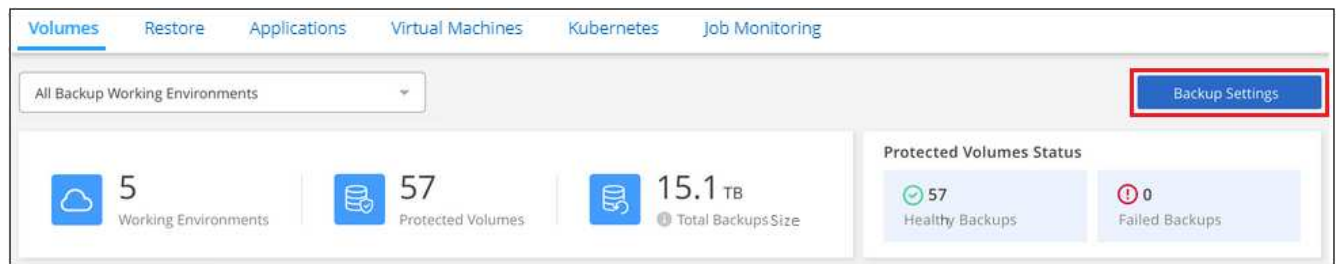
在注销 Cloud Backup 之前，必须按以下顺序执行以下步骤：

- 为工作环境停用 Cloud Backup
- 删除该工作环境的所有备份

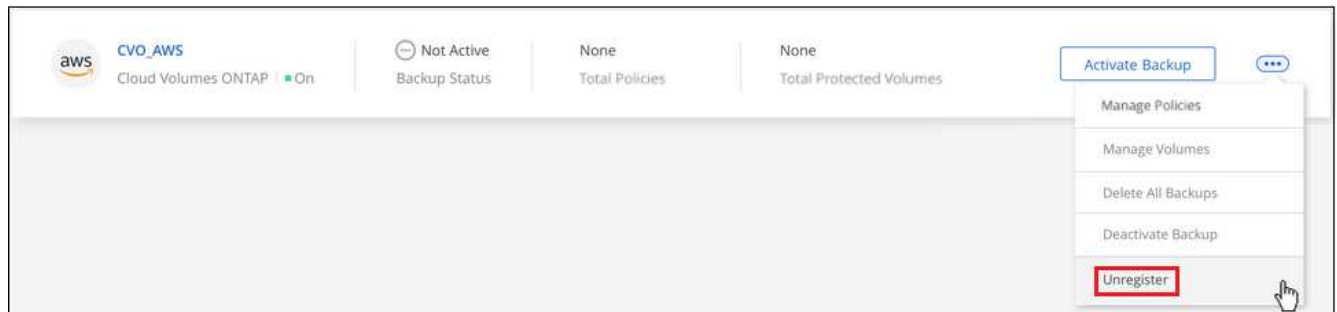
只有在这两个操作完成后，取消注册选项才可用。

步骤

1. 从 * 卷 * 选项卡中，选择 * 备份设置 *。



2. 在 *Backup Settings page* 中，单击 ... 对于要取消注册备份服务的工作环境，请选择 * 取消注册 *。



3. 在确认对话框中，单击 * 取消注册 *。

从备份文件还原 ONTAP 数据


备份存储在云帐户的对象存储中，以便您可以从特定时间点还原数据。您可以从备份文件还原整个 ONTAP 卷，也可以从备份文件还原单个文件。

您可以将 * 卷 *（作为新卷）还原到原始工作环境，使用相同云帐户的其他工作环境或内部 ONTAP 系统。

您可以将 * 文件 * 还原到原始工作环境中的卷，使用相同云帐户的其他工作环境中的卷或内部 ONTAP 系统上的卷。

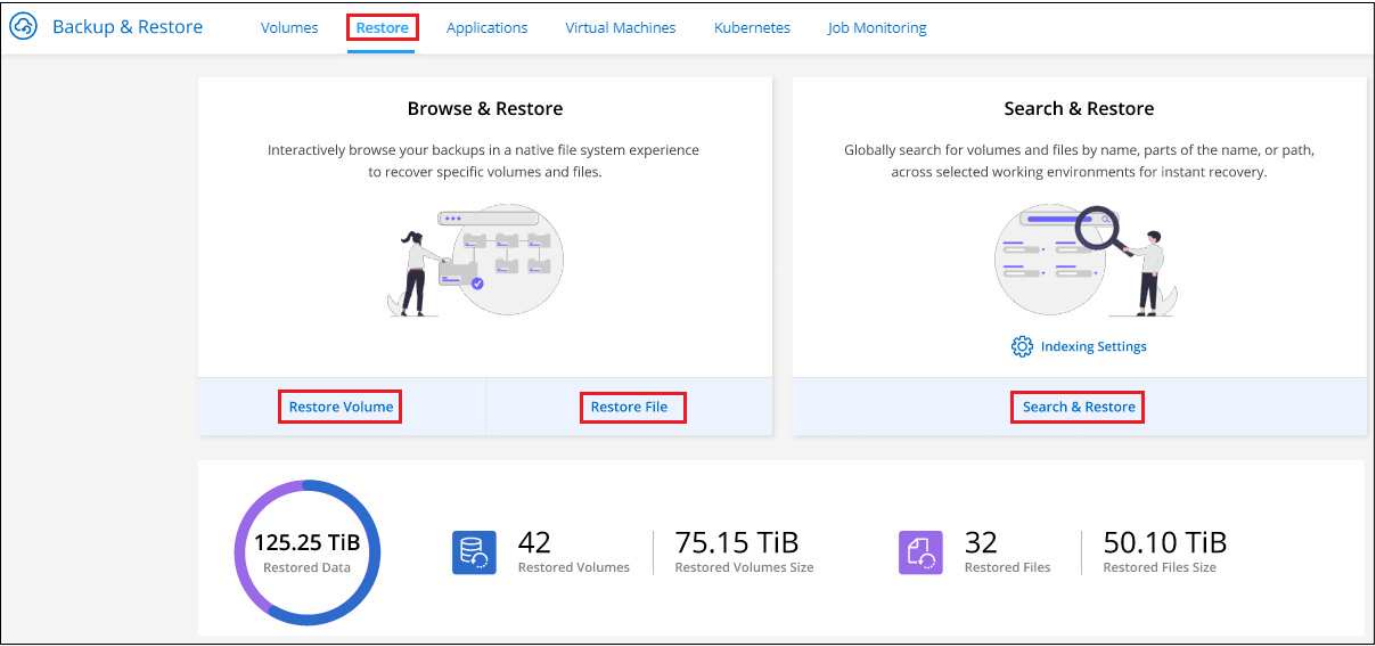
要将数据从备份文件还原到生产系统、需要有效的Cloud Backup许可证。

还原信息板

您可以使用还原信息板执行卷和文件还原操作。要访问还原信息板，请单击 Cloud Manager 顶部的 * 备份和还原 *，然后单击 * 还原 * 选项卡。您也可以单击  > "服务" 面板中的备份和还原服务中的 * 查看还原信息板 *。



必须已为至少一个工作环境激活 Cloud Backup，并且必须存在初始备份文件。



如您所见，还原信息板提供了两种不同的方法来从备份文件还原数据：* 浏览和还原 * 和 * 搜索和还原 *。

比较浏览和还原以及搜索和还原

概括地说，当您需要从过去一周或一个月还原特定卷或文件时，_Browse & Restore" 通常会更好—您知道文件的名称和位置，以及文件的最后一个状态良好的日期。通常，当您需要还原卷或文件时，_Search & Restore" 会更好，但您不记得确切的名称，卷所在的卷或最后一个卷状态良好的日期。

下表对这两种方法进行了比较。

浏览和还原	搜索和还原
浏览文件夹样式的结构以查找单个备份文件中的卷或文件	在 * 所有备份文件 * 中按部分或完整卷名称，部分或完整文件名，大小范围以及其他搜索筛选器搜索卷或文件
卷和文件还原适用于存储在Amazon S3、Azure Blob、Google Cloud和NetApp StorageGRID 中的备份文件。	卷和文件还原适用于存储在Amazon S3和Google Cloud中的备份文件
在无法访问Internet的站点中从StorageGRID 还原卷和文件	在非公开站点中不支持

浏览和还原	搜索和还原
不处理已重命名或删除的文件	处理新建 / 删除 / 重命名的目录以及新建 / 删除 / 重命名的文件
浏览公有 和私有云中的结果	浏览公有 云和本地 Snapshot 副本的结果
无需额外的云提供商资源	每个帐户需要额外的存储分段和AWS或Google资源
无需额外的云提供商成本	扫描备份和卷以查找搜索结果时与AWS或Google资源相关的成本

在使用任一还原方法之前，请确保已为环境配置了唯一的资源要求。以下各节将介绍这些要求。

请参见要使用的还原操作类型的要求和还原步骤：

- [使用浏览和放大功能还原卷；还原](#)
- [使用浏览和放大功能还原文件；还原](#)
- [使用搜索和放大器还原卷和文件；还原](#)

使用浏览和还原还原 **ONTAP** 数据

在开始还原卷或文件之前，您应知道要还原的卷或文件的名称，卷所在工作环境的名称以及要从中还原的备份文件的大致日期。

*注意：*如果要还原的卷的备份文件位于归档存储中(从ONTAP 9.10.1开始)、则还原操作将需要较长时间并产生成本。此外，目标集群还必须运行 ONTAP 9.10.1 或更高版本。

["了解有关从 AWS 归档存储还原的更多信息"](#)。

浏览并还原支持的工作环境和对象存储提供程序

您可以将卷或单个文件从 ONTAP 备份文件还原到以下工作环境：

备份文件位置	目标工作环境	
	* 卷还原 *	文件还原 ifdef: : AWS
Amazon S3	AWS 内部 ONTAP 系统中的 Cloud Volumes ONTAP	AWS内部部署ONTAP 系统中的Cloud Volumes ONTAP endf: AWS [] ifdef : : azure[]
Azure Blob	Azure 内部 ONTAP 系统中的 Cloud Volumes ONTAP	Azure内部ONTAP 系统中的Cloud Volumes ONTAP endf: azure[] ifdef : : gcp[]
Google Cloud 存储	Google 内部 ONTAP 系统中的 Cloud Volumes ONTAP	Google内部部署ONTAP 系统中的Cloud Volumes ONTAP endf : gcp[]
NetApp StorageGRID	内部部署 ONTAP 系统	内部部署 ONTAP 系统

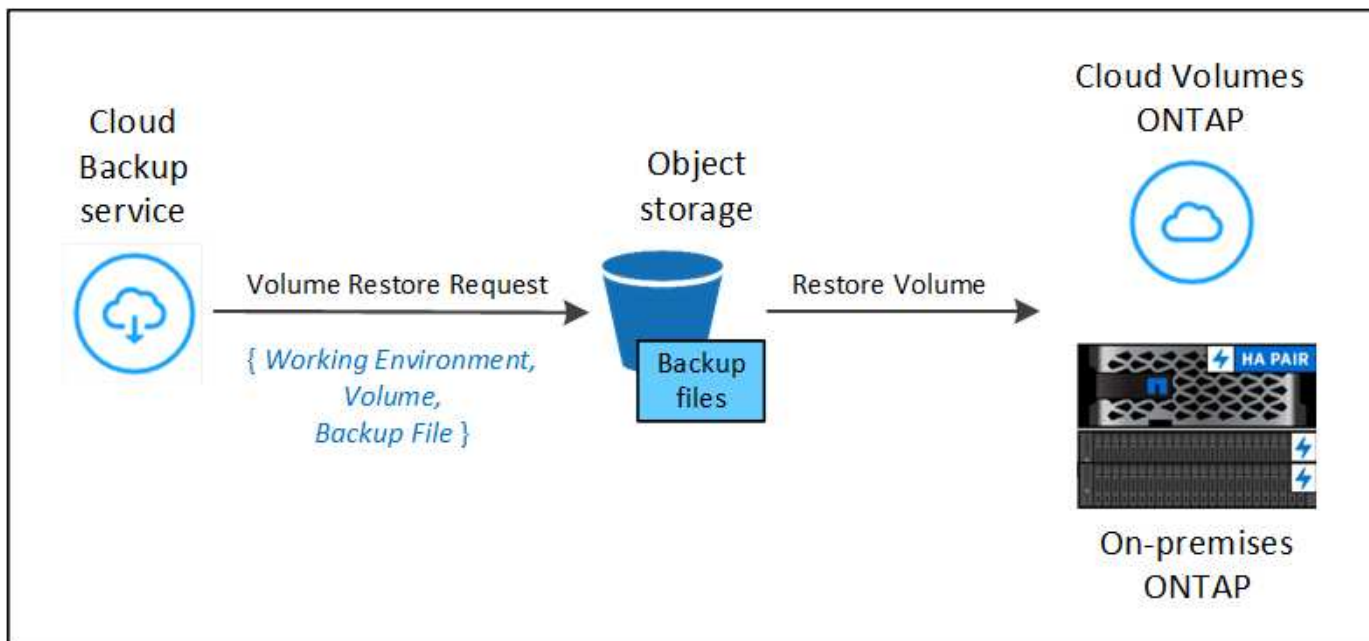
请注意， " 内部 ONTAP 系统 " 的引用包括 FAS ， AFF 和 ONTAP Select 系统。



如果备份文件驻留在归档存储中，则仅支持卷还原。使用浏览和还原时，当前不支持从归档存储还原文件。

使用浏览和还原还原卷

从备份文件还原卷时，Cloud Backup 会使用备份中的数据创建一个 *new* 卷。您可以将数据还原到原始工作环境中的卷，也可以还原到与源工作环境位于同一云帐户中的其他工作环境。您还可以将卷还原到内部 ONTAP 系统。



如您所见，要执行卷还原，您需要知道工作环境名称，卷名称和备份文件日期。

以下视频显示了还原卷的快速演练：

Cloud Backup Service: Restore Demo

Powered by Cloud Manager

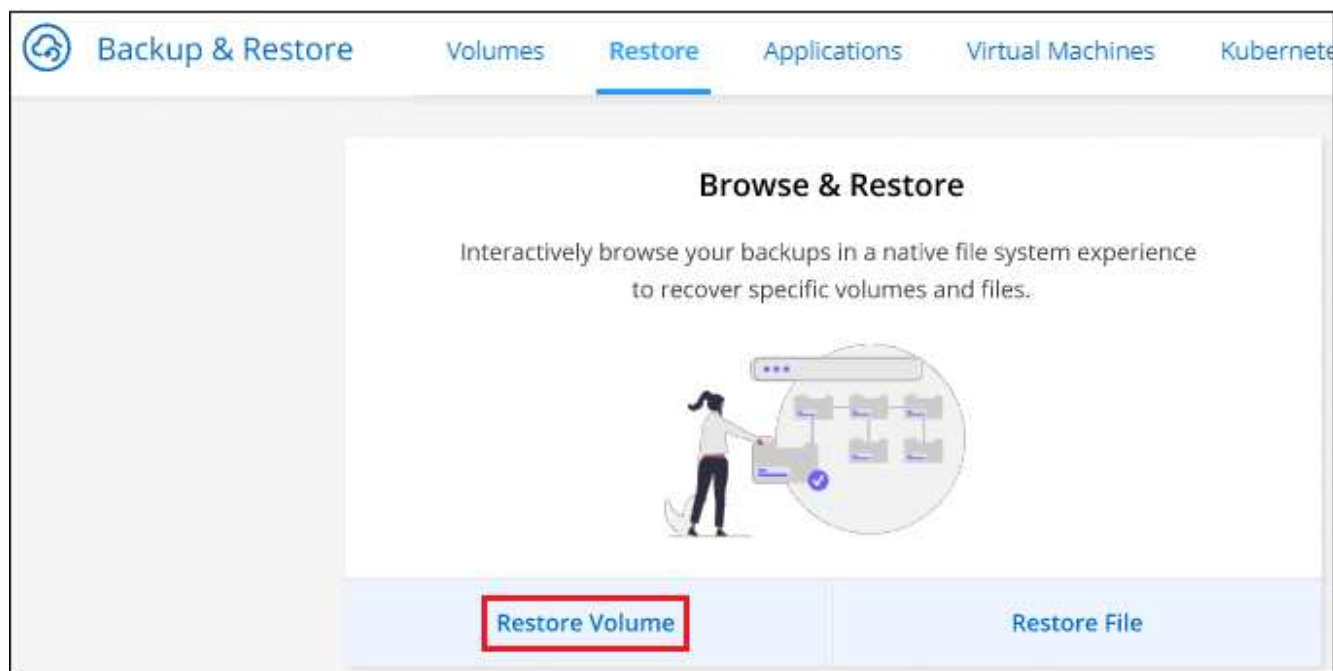
January 2022

 NetApp

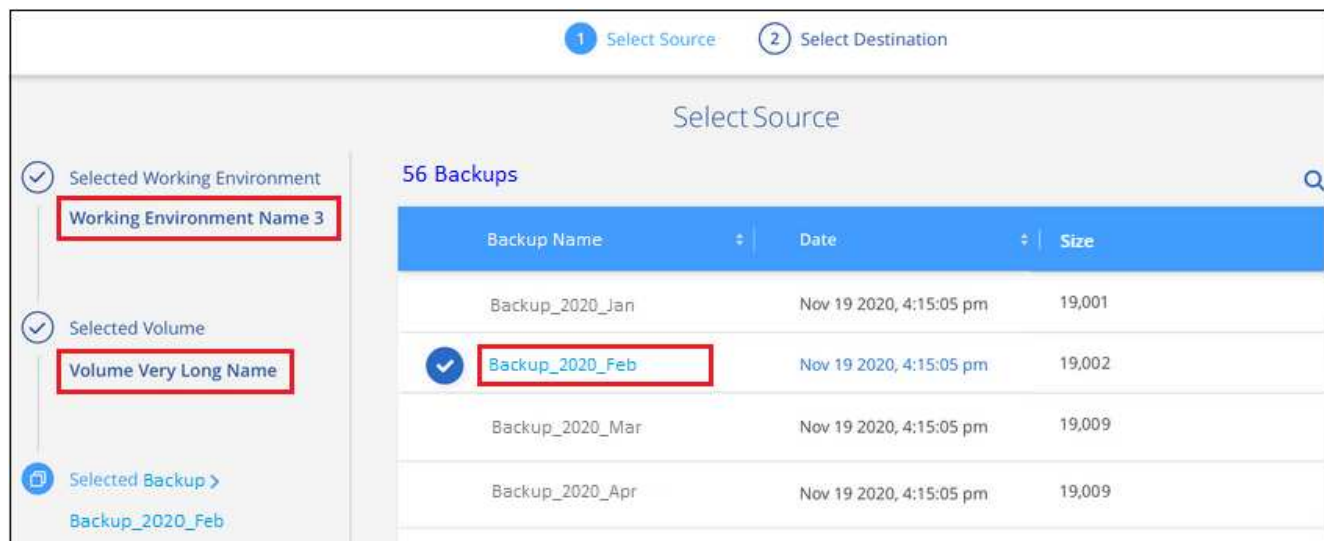


步骤

1. 选择 * 备份和还原 * 服务。
2. 单击 * 还原 * 选项卡，此时将显示还原信息板。
3. 在 *Browse & Restore* 部分中，单击 * 还原卷 *。

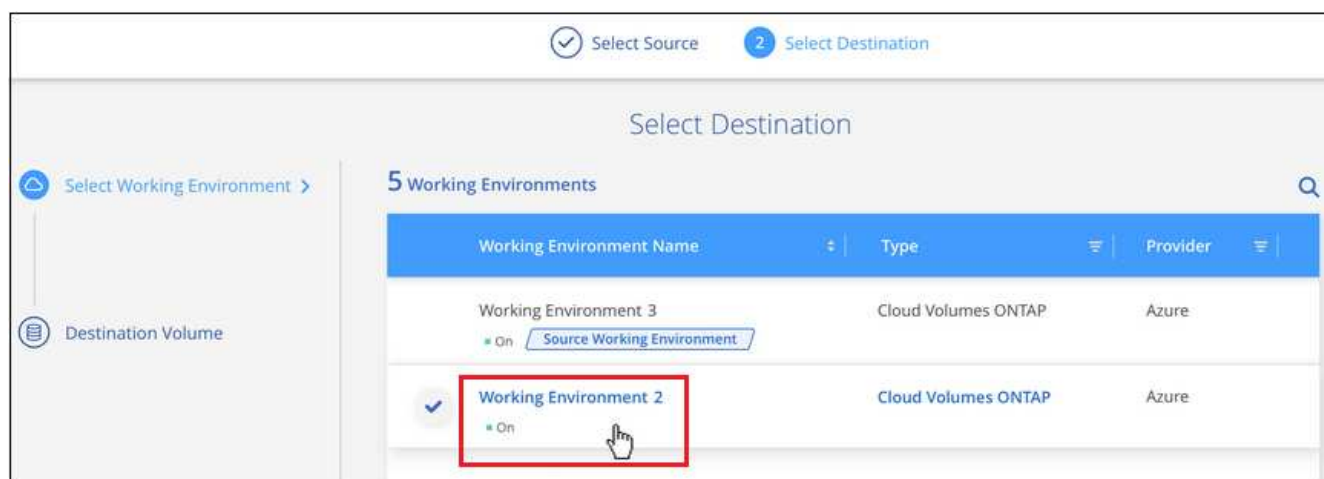


4. 在 "Select Source" 页面中，导航到要还原的卷的备份文件。选择 * 工作环境 *，* 卷 * 以及具有要还原的日期 / 时间戳的 * 备份 * 文件。



5. 单击 * 继续 *。

6. 在 *Select Destination* 页面中，选择要还原卷的 * 工作环境 *。



7. 如果您选择内部 ONTAP 系统，但尚未配置与对象存储的集群连接，则系统会提示您输入追加信息：

- 从 Amazon S3 还原时，请选择目标卷所在 ONTAP 集群中的 IP 空间，输入您创建的用户访问密钥和机密密钥，以便为 ONTAP 集群授予对 S3 存储分段的访问权限。此外，还可以选择一个专用 VPC 端点来实现安全数据传输。
- 从 StorageGRID 还原时，输入 StorageGRID 服务器的 FQDN 以及 ONTAP 与 StorageGRID 进行 HTTPS 通信时应使用的端口、选择访问对象存储所需的访问密钥和机密密钥、以及目标卷所在的 ONTAP 集群中的 IP 空间。
- a. 输入要用于还原的卷的名称，然后选择此卷要驻留的 Storage VM。默认情况下，使用 * <source_volume_name>_Restore* 作为卷名称。

只有在将卷还原到内部 ONTAP 系统时，您才能选择卷将用于其容量的聚合。

如果您要从位于归档存储层（从 ONTAP 9.10.1 开始提供）中的备份文件还原卷，则可以选择还原优先级。

["了解有关从 AWS 归档存储还原的更多信息"](#)。

1. 单击 * 还原 *，您将返回到还原信息板，以便查看还原操作的进度。

Cloud Backup 会根据您选择的备份创建一个新卷。您可以 ["管理此新卷的备份设置"](#) 根据需要。

请注意，从归档存储中的备份文件还原卷可能需要数分钟或数小时，具体取决于归档层和还原优先级。您可以单击 * 作业监控 * 选项卡查看还原进度。

使用浏览和还原还原 **ONTAP** 文件

如果您只需要从 ONTAP 卷备份还原几个文件，则可以选择还原单个文件，而不是还原整个卷。您可以将文件还原到原始工作环境中的现有卷，也可以还原到使用同一云帐户的其他工作环境。您还可以将文件还原到内部 ONTAP 系统上的卷。

如果选择多个文件，则所有文件都将还原到您选择的同一目标卷。因此，如果要将文件还原到不同的卷，则需要多次运行还原过程。



如果备份文件驻留在归档存储中，则无法还原单个文件。在这种情况下，您可以从尚未归档的较新备份文件还原文件，也可以从归档的备份还原整个卷，然后访问所需的文件，或者使用搜索和还原还原还原文件。

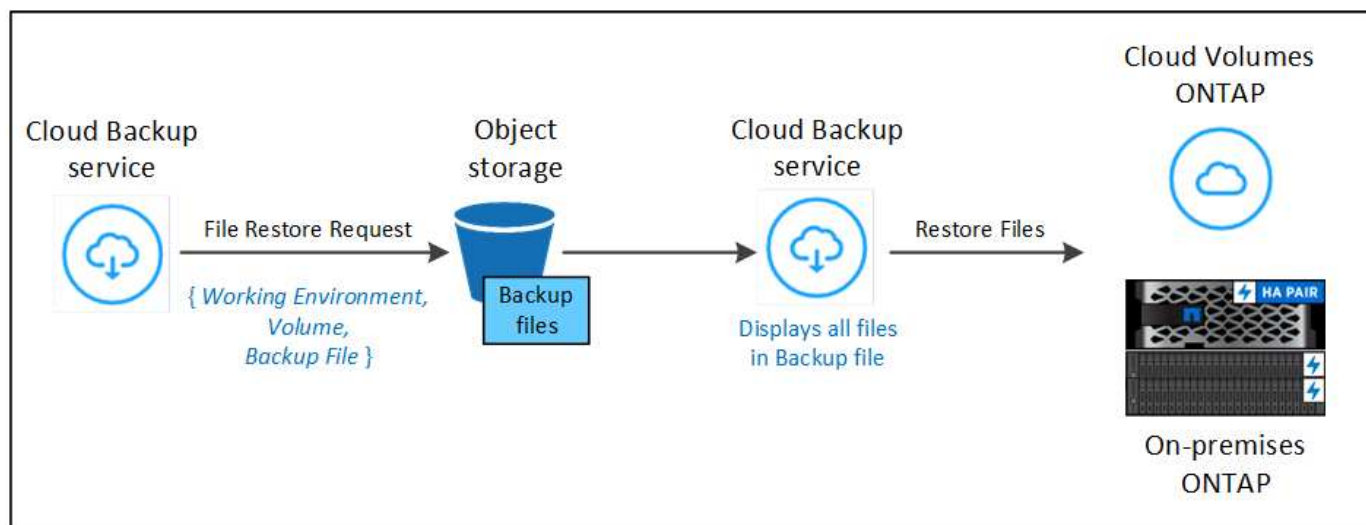
前提条件

- 要执行文件还原操作，Cloud Volumes ONTAP 或内部 ONTAP 系统中的 ONTAP 版本必须为 9.6 或更高版本。
- AWS 跨帐户还原需要在 AWS 控制台中手动执行操作。请参见 AWS 主题 ["授予跨帐户存储分段权限"](#) 了解详细信息。

文件还原过程

此过程如下所示：

1. 如果要从卷备份中还原一个或多个文件，请单击 * 还原 * 选项卡，单击 *Browse & Restore* 下的 * 还原文件 *，然后选择文件所在的备份文件。
2. Cloud Backup会显示选定备份文件中的文件夹和文件。
3. 选择要从该备份还原的一个或多个文件。
4. 选择要还原文件的位置（工作环境，卷和文件夹），然后单击 * 还原 *。
5. 文件已还原。



如您所见，要执行文件还原，您需要知道工作环境名称，卷名称，备份文件日期和文件名。

使用浏览和还原还原文件

按照以下步骤将文件从 ONTAP 卷备份还原到卷。您应知道要用于还原文件的卷名称和备份文件的日期。此功能使用实时浏览功能，以便您可以查看每个备份文件中的目录和文件列表。

以下视频显示了还原单个文件的快速演练：

Cloud Backup Service: Restore Demo

Powered by Cloud Manager

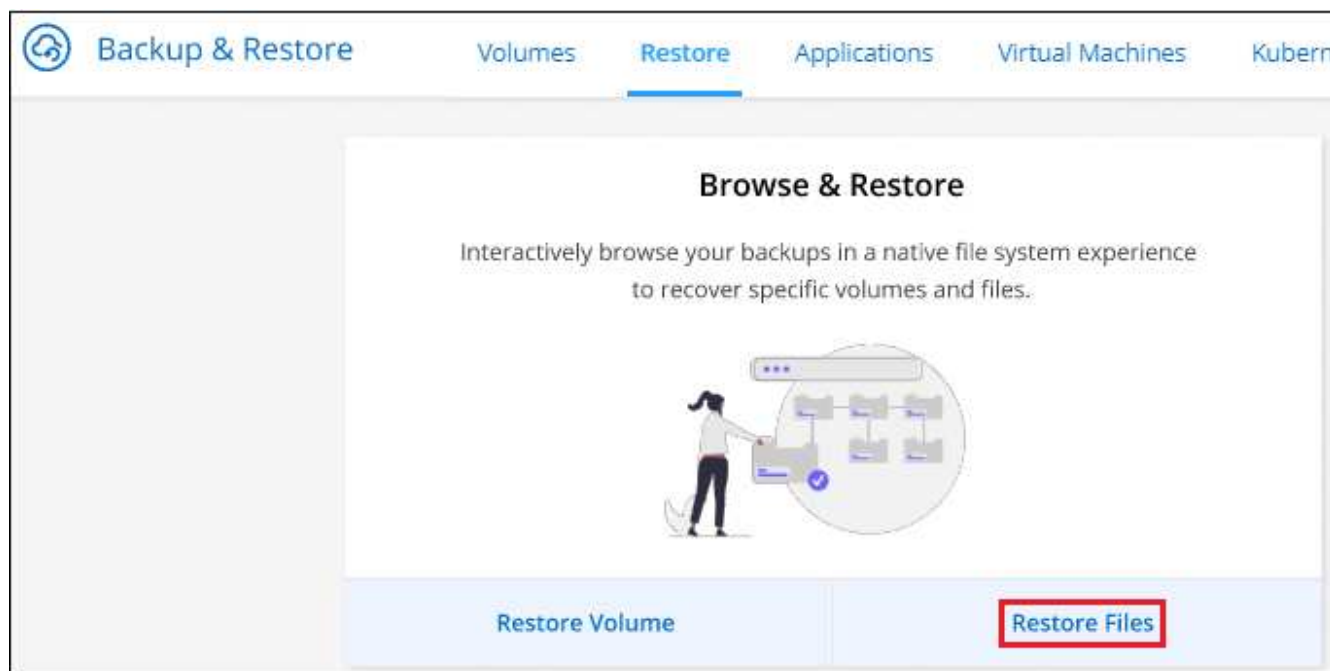
January 2022

 NetApp

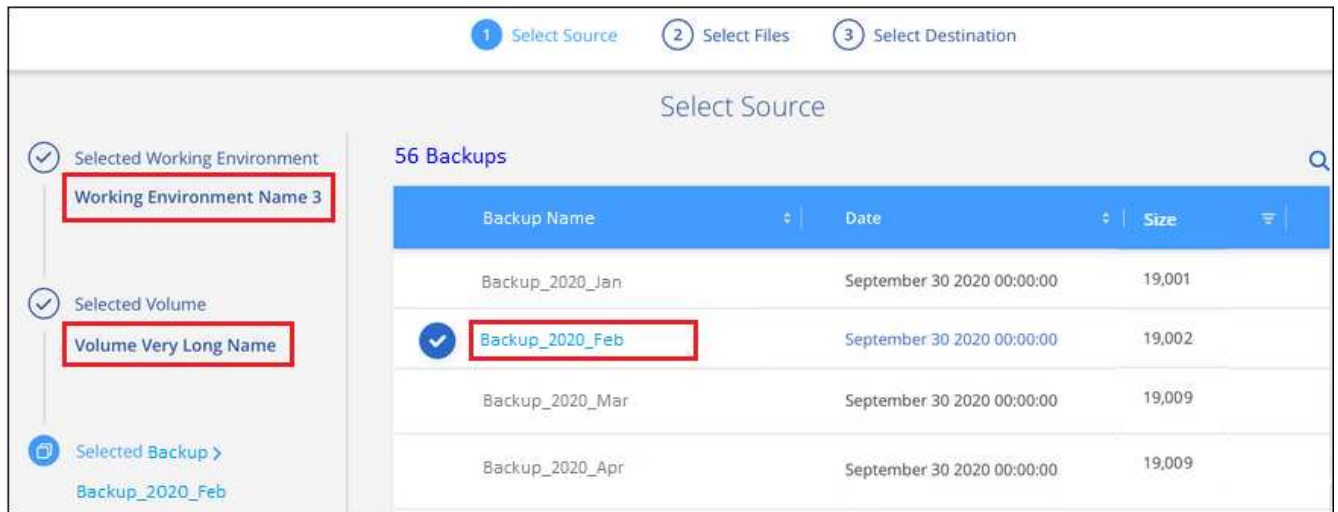


步骤

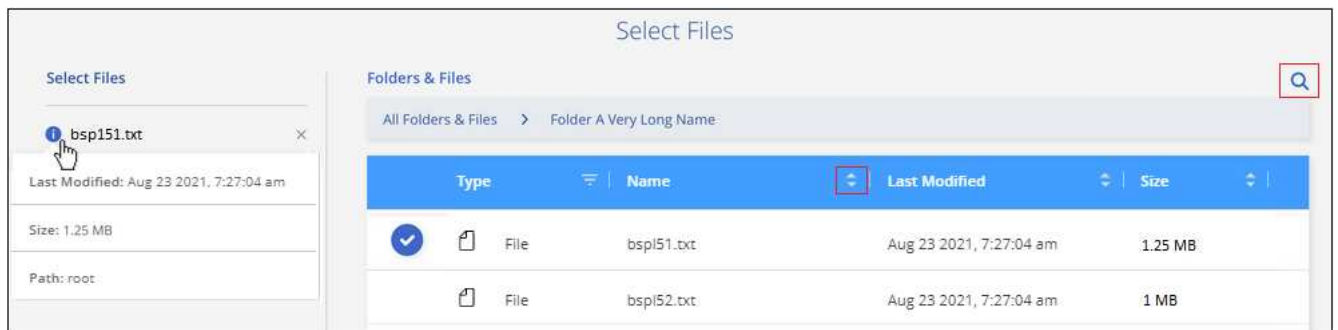
1. 选择 * 备份和还原 * 服务。
2. 单击 * 还原 * 选项卡，此时将显示还原信息板。
3. 在 *Browse & Restore* 部分中，单击 * 还原文件 * 。




4. 在 "Select Source" 页面中，导航到包含要还原的文件的卷的备份文件。选择具有要从中还原文件的日期 / 时间戳的 * 工作环境 *，* 卷 * 和 * 备份 *。



5. 单击*继续*、此时将显示卷备份中的文件夹和文件列表。

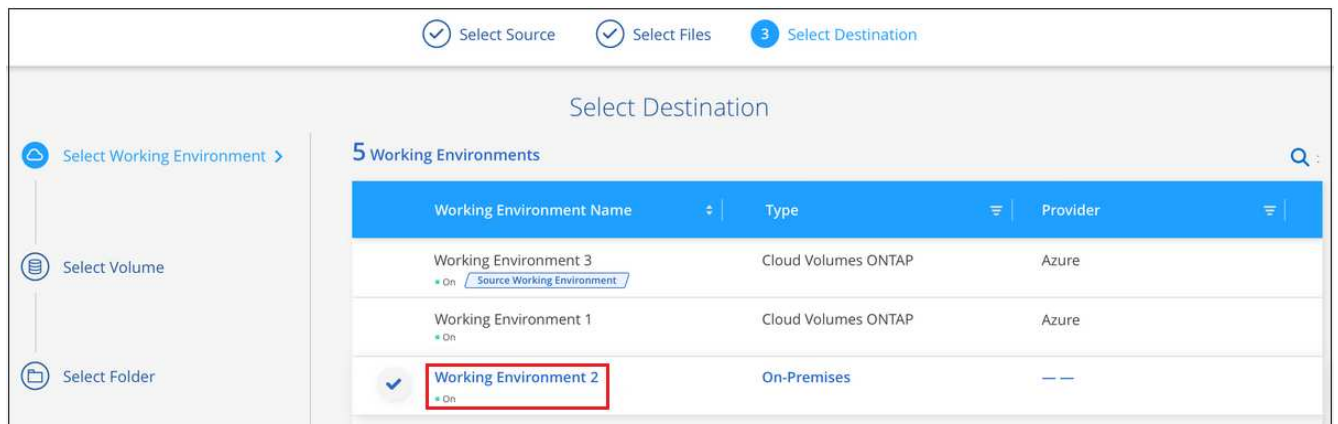


6. 在 *Select Files* 页面中，选择要还原的一个或多个文件，然后单击 * 继续 *。要帮助您查找文件，请执行以下操作：

- 如果看到文件名，可以单击它。
- 您可以单击搜索图标并输入文件的名称以直接导航到该文件。
- 您可以使用在文件夹中向下导航级别  按钮以查找文件。

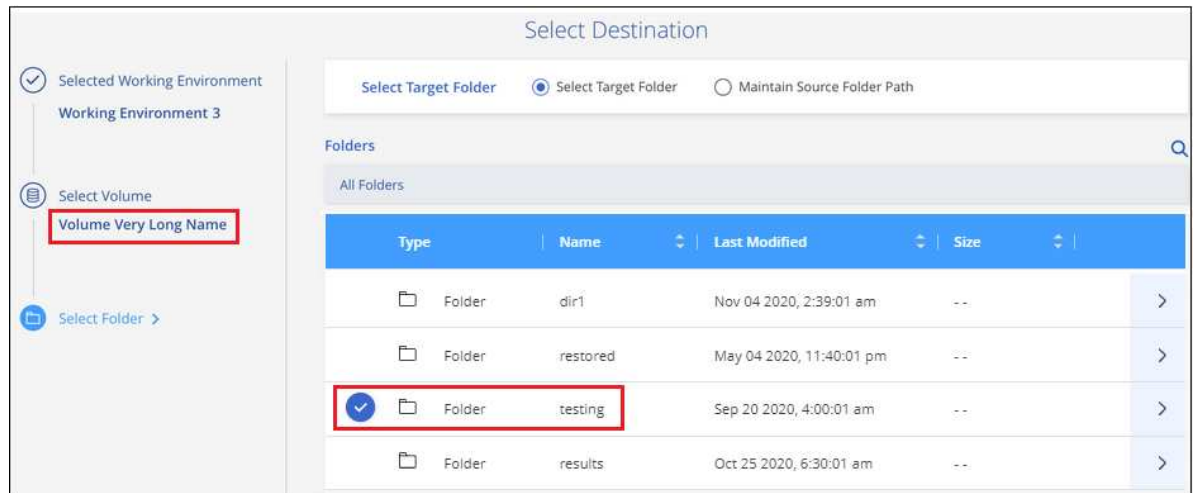
选择文件时，这些文件将添加到页面左侧，以便您可以查看已选择的文件。如果需要，您可以单击文件名旁边的 * x * 来从此列表中删除文件。

7. 在 *Select Destination* 页面中，选择要还原文件的 * 工作环境 *。



如果选择内部集群，但尚未配置与对象存储的集群连接，则系统会提示您输入追加信息：

- 从 Amazon S3 还原时，输入目标卷所在 ONTAP 集群中的 IP 空间以及访问对象存储所需的 AWS 访问密钥和机密密钥。
 - 从 StorageGRID 还原时，输入 StorageGRID 服务器的 FQDN 以及 ONTAP 与 StorageGRID 进行 HTTPS 通信时应使用的端口、输入访问对象存储所需的访问密钥和机密密钥、以及目标卷所在 ONTAP 集群中的 IP 空间。
 - a. 然后选择 * 卷 * 和 * 文件夹 * 以还原文件。



还原文件时，您可以选择一些位置选项。

- 选择 * 选择目标文件夹 * 后，如上所示：
 - 您可以选择任何文件夹。
 - 您可以将鼠标悬停在某个文件夹上并单击 ➤ 在行末尾展开以深入到子文件夹，然后选择一个文件夹。
- 如果选择的目标工作环境和卷与源文件所在的位置相同，则可以选择 * 维护源文件夹路径 * 将文件或所有文件还原到源结构中存在的同一文件夹。所有相同的文件夹和子文件夹都必须已存在；不会创建文件夹。
 - a. 单击 * 还原 *，您将返回到还原信息板，以便查看还原操作的进度。您也可以单击 * 作业监控 * 选项卡查看还原进度。

使用搜索和还原还原 ONTAP 数据

您可以使用搜索和还原从 ONTAP 备份文件还原卷或单个文件。通过搜索和还原，您可以从存储在云存储上的特定提供商的所有备份中搜索特定卷或文件，然后执行还原。您无需知道确切的工作环境名称或卷名称 - 搜索将查看所有卷备份文件。

搜索操作还会查找 ONTAP 卷中存在的所有本地 Snapshot 副本。与从备份文件还原数据相比，从本地 Snapshot 副本还原数据的速度更快，成本更低，因此您可能需要从 Snapshot 还原数据。您可以从 "画布" 上的 "卷详细信息" 页面将快照还原为新卷。

从备份文件还原卷时，Cloud Backup 会使用备份中的数据创建一个 *new* 卷。您可以将数据还原为原始工作环境中的卷，也可以还原到与源工作环境位于同一云帐户中的其他工作环境。您还可以将卷还原到内部 ONTAP 系统。

您可以将文件还原到原始卷位置，同一工作环境中的其他卷或使用同一云帐户的其他工作环境。您还可以将文件还原到内部 ONTAP 系统上的卷。

如果要还原的卷的备份文件驻留在归档存储中(从ONTAP 9.10.1开始可用)、则还原操作将需要较长时间并产生额外成本。请注意，目标集群也必须运行 ONTAP 9.10.1 或更高版本，并且当前不支持从归档存储还原文件。

["了解有关从 AWS 归档存储还原的更多信息"](#)。

开始之前，您应了解要还原的卷或文件的名称或位置。

以下视频显示了还原单个文件的快速演练：



搜索和还原支持的工作环境和对象存储提供程序

您可以将卷或单个文件从 ONTAP 备份文件还原到以下工作环境：

备份文件位置	目标工作环境	
	* 卷还原 *	文件还原 ifdef: : AWS
Amazon S3	AWS 内部 ONTAP 系统中的 Cloud Volumes ONTAP	AWS内部部署ONTAP 系统中的Cloud Volumes ONTAP endif: AWS [] ifdef: : azure[]
Azure Blob	当前不支持	endif: : azure[] ifdef: : gcp[]
Google Cloud 存储	Google 内部 ONTAP 系统中的 Cloud Volumes ONTAP	Google内部部署ONTAP 系统中的Cloud Volumes ONTAP endif: gcp[]
NetApp StorageGRID	当前不支持	

请注意， " 内部 ONTAP 系统 " 的引用包括 FAS ， AFF 和 ONTAP Select 系统。

前提条件

- 集群要求：
 - ONTAP 版本必须为 9.8 或更高版本。
 - 卷所在的 Storage VM （ SVM ） 必须已配置数据 LIF 。
 - 必须在卷上启用 NFS 。
 - 必须在 SVM 上激活 SnapDiff RPC 服务器。在工作环境中启用索引时， Cloud Manager 会自动执行此操作。
- AWS 要求：
 - 必须将特定的 Amazon Athena ， AWS glue 和 AWS S3 权限添加到为 Cloud Manager 提供权限的用户角色中。 "确保已正确配置所有权限"。

请注意，如果您已经在使用 Cloud Backup 时使用了过去配置的连接，则现在需要将 Athena 和粘附权限添加到 Cloud Manager 用户角色中。这些是新的，搜索和还原需要它们。

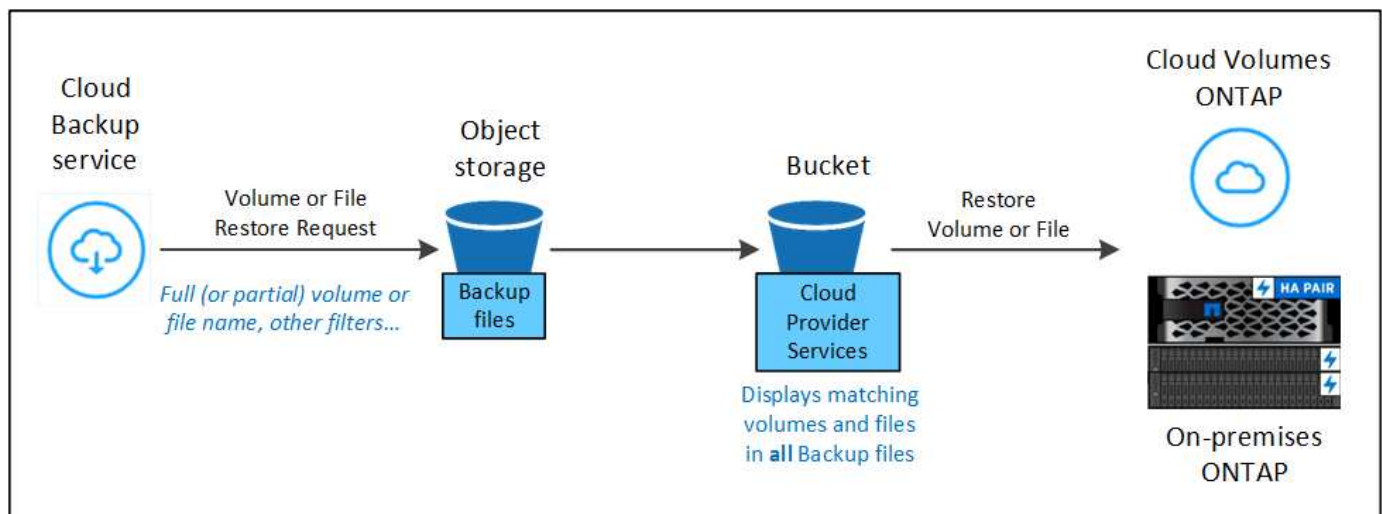
搜索和还原过程

此过程如下所示：

1. 在使用搜索和还原之前，您需要在要从中还原卷或文件的每个源工作环境中启用 " 索引编制 "。这样，索引目录就可以跟踪每个卷的备份文件。
2. 如果要从卷备份还原卷或文件，请在 *Search & Restore* 下单击 * 搜索和还原 *。
3. 按部分或完整卷名称，部分或完整文件名，大小范围，创建日期范围和其他搜索筛选器输入卷或文件的搜索条件，然后单击 * 搜索 *。

" 搜索结果 " 页面将显示文件或卷与您的搜索条件匹配的所有位置。

4. 单击 * 查看所有备份 * 以查看要用于还原卷或文件的位置，然后在要使用的实际备份文件上单击 * 还原 *。
5. 选择要还原卷或文件的位置，然后单击 * 还原 *。
6. 卷或文件已还原。



如您所见，您实际上只需要知道部分卷或文件名， Cloud Backup 会搜索与您的搜索匹配的所有备份文件。

为每个工作环境启用索引目录

在使用搜索和还原之前，您需要在计划从中还原卷或文件的每个源工作环境中启用 "索引编制"。这样，索引目录就可以跟踪每个卷和每个备份文件，从而使搜索非常快速高效。

启用此功能后、Cloud Backup会在SVM上为卷启用SnapDiff v3、并执行以下操作：

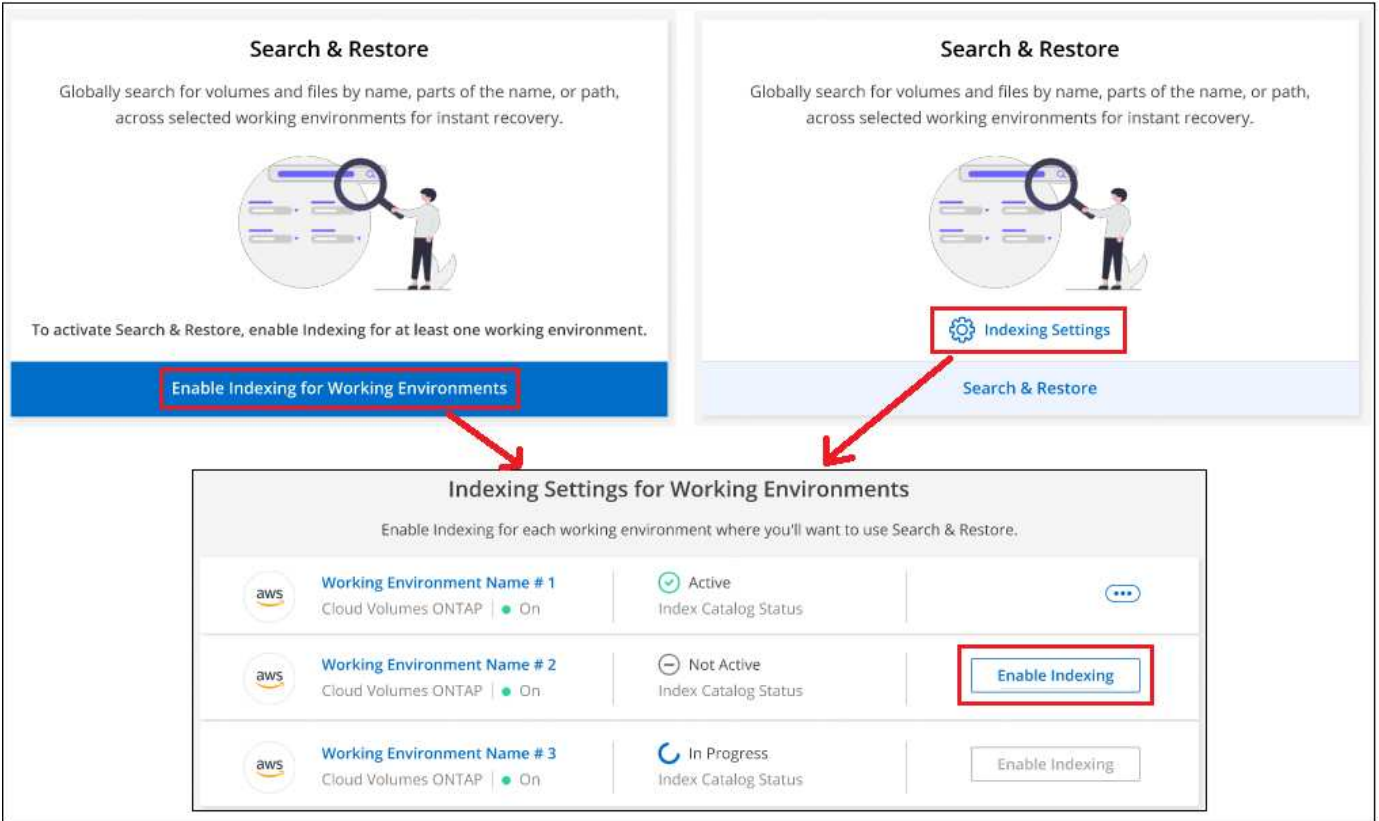
- 对于存储在AWS中的备份、它会配置一个新的S3存储分段和 "Amazon Athena 交互式查询服务" 和 "AWS 无服务器数据集成服务"。

如果您的工作环境已启用索引，请转到下一节以还原数据。

要为工作环境启用索引编制，请执行以下操作：

- 如果尚未为工作环境编制索引，请在 "Restore Dashboard" 中的 *Search & Restore* 下，单击 * 为工作环境启用索引 *，然后单击 * 为工作环境启用索引 *。
- 如果至少有一个工作环境已编制索引，请在 "Restore Dashboard" 中的 "*_Search & Restore*" 下，单击 * 索引设置 *，然后单击 * 为工作环境启用索引 *。

配置完所有服务并激活索引目录后，工作环境将显示为 "Active"。



根据工作环境中卷的大小以及云中备份文件的数量，初始索引编制过程可能需要长达一小时的时间。之后，它会每小时透明地更新一次，并进行增量更改，以保持最新状态。

使用搜索和还原还原卷和文件

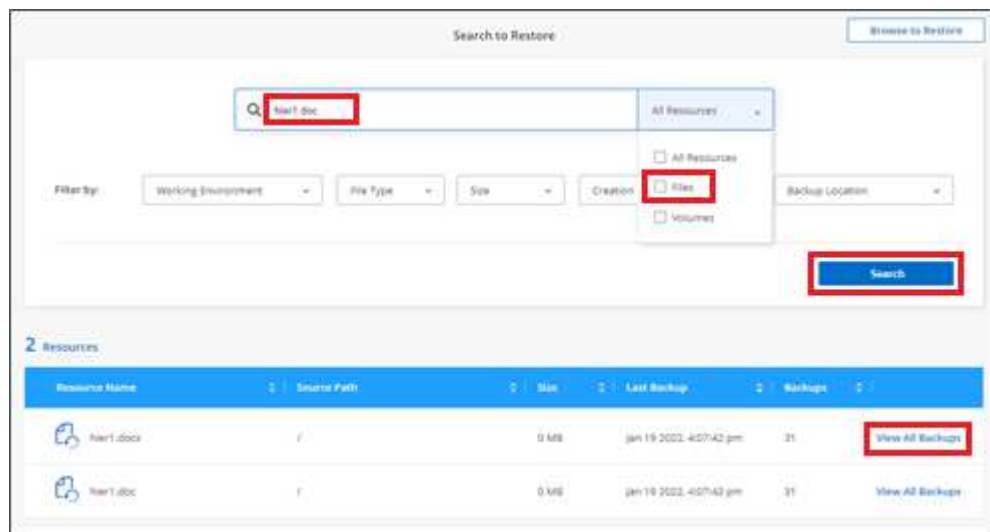
你先请 [已为您的工作环境启用索引编制](#)，您可以使用搜索和还原来还原卷或文件。这样，您就可以使用多种筛选器来查找要从所有备份文件还原的确切文件或卷。

步骤

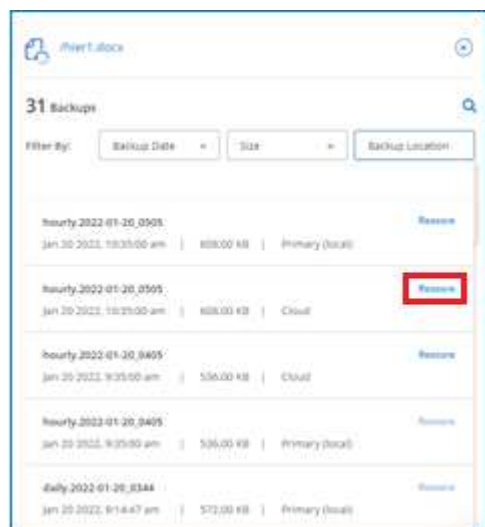
1. 选择 * 备份和还原 * 服务。
2. 单击 * 还原 * 选项卡，此时将显示还原信息板。
3. 在 *Search & Restore* 部分中，单击 * 搜索和还原 *。



4. 在 Search & Restore 页面中：
 - a. 在搜索栏中，输入完整或部分卷名称或文件名。
 - b. 在筛选器区域中，选择筛选条件。例如，您可以选择数据所在的工作环境和文件类型，例如 .doc 文件。
5. 单击 * 搜索 *，搜索结果区域将显示具有与您的搜索匹配的文件或卷的所有位置。



6. 单击 * 查看所有备份 * 以查看包含要还原的数据的位置，以显示包含卷或文件的所有备份文件。



7. 对于要用于从云还原卷或文件的备份文件，请单击 * 还原 *。

请注意，结果还会标识搜索中包含该文件的本地卷 Snapshot 副本。此时，* 还原 * 按钮对快照不起作用，但如果要从 Snapshot 副本而非备份文件还原数据，请记下卷的名称和位置，然后打开 "画布" 上的 "卷详细信息" 页面。并使用 * 从 Snapshot 副本还原 * 选项。

8. 选择要还原卷或文件的位置，然后单击 * 还原 *。

- 对于文件，您可以还原到原始位置，也可以选择其他位置
- 对于卷，您可以选择位置。

卷或文件将还原，您将返回到还原信息板，以便查看还原操作的进度。您也可以单击 * 作业监控 * 选项卡查看还原进度。

对于已还原的卷，您可以 ["管理此新卷的备份设置"](#) 根据需要。

备份和还原 Kubernetes 数据

使用 Cloud Backup 保护 Kubernetes 集群数据

Cloud Backup 提供备份和还原功能，用于保护和长期归档 Kubernetes 集群数据。备份会自动生成并存储在公有或私有云帐户的对象存储中。

如有必要，您可以将整个 _volume" 从备份还原到相同或不同的工作环境。

功能

备份功能：

- 将永久性卷的独立副本备份到低成本对象存储。
- 将单个备份策略应用于集群中的所有卷，或者将不同的备份策略分配给具有唯一恢复点目标的卷。
- 使用 AES-256 位空闲加密和正在传输的 TLS 1.2 HTTPS 连接保护备份数据。
- 一个卷最多支持 4,000 个备份。

还原功能：

- 从特定时间点还原数据。
- 将卷还原到源系统或其他系统。
- 还原块级别的数据，将数据直接放置在您指定的位置，同时保留原始 ACL。

支持的 Kubernetes 工作环境和对象存储提供程序

通过 Cloud Backup，您可以将 Kubernetes 卷从以下工作环境备份到以下公有和私有云提供商中的对象存储：

源工作环境	备份文件目标 <code>ifndef: : AWS]</code>
AWS 中的 Kubernetes 集群	Amazon S3 <code>endif: : AWS]</code> <code>ifndef: : azure[]</code>
Azure 中的 Kubernetes 集群	Azure Blob <code>endif: : azure[]</code> <code>ifndef: : GCP[]</code>
Google 中的 Kubernetes 集群	Google Cloud Storage <code>endif: gcp[]</code>

您可以将卷从 Kubernetes 备份文件还原到以下工作环境：

备份文件位置	目标工作环境 <code>ifndef: : AWS]</code>
Amazon S3	AWS 内的 Kubernetes 集群 <code>endif: : AWS]]</code> <code>ifndef: : azure[]</code>
Azure Blob	Azure 内的 Kubernetes 集群: <code>azure[]</code> <code>ifndef: : : gcp[]</code>
Google Cloud 存储	Google <code>endif</code> 中的 Kubernetes 集群: <code>GCP[]</code>

成本

使用 Cloud Backup 会产生两种成本：资源费用和服务费用。

- 资源费用 *

资源费用将支付给云提供商，用于支付云中的对象存储容量。由于云备份会保留源卷的存储效率，因此您需要为云提供商的对象存储成本支付 `data_after_ONTAP` 效率（适用于应用重复数据删除和数据压缩后少量的数据）。

- 服务费用 *

服务费用将支付给 NetApp，用于支付这些备份的 `creation_backup` 和 `restor` 卷的费用。您只需为所保护的数据付费，该数据是通过备份到对象存储的卷的源逻辑已用容量（ONTAP 效率）计算得出的。此容量也称为前端 TB（前端 TB）。

有两种方式可以为备份服务付费。第一种选择是从云提供商订阅，这样您可以按月付费。第二种选择是直接 NetApp 购买许可证。阅读 [许可](#) 部分以了解详细信息。

许可

Cloud Backup 有两种许可选项：按需购买（PAYGO）和自带许可证（BYOL）。如果您没有许可证，可以免费试用 30 天。

免费试用

使用 30 天免费试用版时，系统会通知您剩余的免费试用天数。在免费试用版结束时，备份将停止创建。您必须订阅此服务或购买许可证才能继续使用此服务。

禁用此服务后，不会删除备份文件。除非删除备份，否则云提供商会继续为您的备份所使用的容量收取对象存储成本。

按需购买订阅

Cloud Backup 以按需购买模式提供基于消费的许可。通过云提供商的市场订阅后，您需要为备份的数据按 GB 付费—there 无需预先付费。您的云提供商会通过每月账单向您开具账单。

即使您拥有免费试用版或自带许可证（BYOL），也应订阅：

- 订阅可确保在免费试用结束后不会中断服务。

试用结束后，系统会根据您备份的数据量按小时收取费用。

- 如果备份的数据超过 BYOL 许可证允许的数量，则数据备份将通过按需购买订阅继续进行。

例如，如果您拥有 10 TB BYOL 许可证，则超过 10 TB 的所有容量均通过 PAYGO 订阅付费。

在免费试用期间，或者如果您未超过 BYOL 许可证，则不会从按需购买订阅中收取费用。

["了解如何设置按需购买订阅"](#)。

自带许可证

BYOL 基于期限（12，24 或 36 个月）和容量，以 1 TB 为增量递增。您需要向 NetApp 支付一段时间（如 1 年）使用此服务的费用，并支付最大容量（如 10 TB）的费用。

您将收到一个序列号，您可以在 Cloud Manager 数字电子邮件页面中输入此序列号来启用此服务。达到任一限制后，您需要续订许可证。备份 BYOL 许可证适用场景 与关联的所有源系统 ["Cloud Manager 帐户"](#)。

["了解如何管理 BYOL 许可证"](#)。

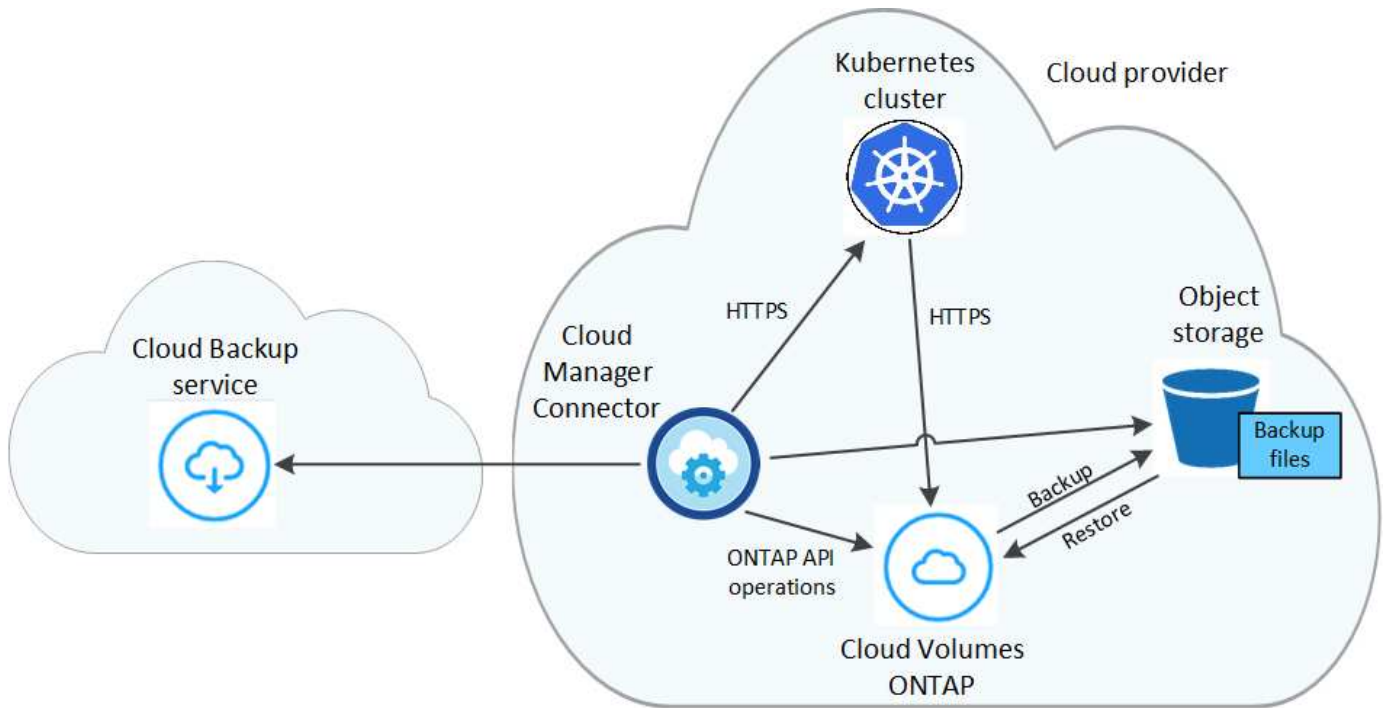
Cloud Backup 的工作原理

在 Kubernetes 系统上启用 Cloud Backup 后，此服务将对您的数据执行完整备份。初始备份之后，所有额外备份都是增量备份，这意味着只会备份更改的块和新块。这样可以将网络流量降至最低。



直接从云提供商环境中执行的任何备份文件管理或更改操作可能会损坏这些文件，并导致配置不受支持。

下图显示了每个组件之间的关系：



支持的存储类或访问层

- 在 AWS 中，备份从 *Standard* 存储类开始，并在 30 天后过渡到 *Standard-Infrequent Access* 存储类。

每个集群可自定义的备份计划和保留设置

在为工作环境启用 Cloud Backup 时，您最初选择的所有卷都会使用您定义的默认备份策略进行备份。如果要为具有不同恢复点目标（RPO）的某些卷分配不同的备份策略，您可以为该集群创建其他策略并将这些策略分配给其他卷。

您可以选择对所有卷进行每小时，每天，每周和每月备份的组合。

达到某个类别或间隔的最大备份数后，较早的备份将被删除，以便始终拥有最新的备份。

支持的卷

Cloud Backup 支持永久性卷（PV）。

限制

- 在创建或编辑备份策略时，如果没有为该策略分配任何卷，则保留的备份数最多可以为 1018。作为临时决策，您可以减少备份数量以创建策略。然后，在为策略分配卷后，您可以编辑此策略以创建多达 4000 个备份。
- Kubernetes 卷不支持使用 * 立即备份 * 按钮进行临时卷备份。

将 Kubernetes 永久性卷数据备份到 Amazon S3

完成以下几个步骤，开始将 EKS Kubernetes 集群上的永久性卷中的数据备份到 Amazon S3 存储。

快速入门

按照以下步骤快速入门，或者向下滚动到其余部分以了解完整详细信息。

跨度 `class="image"><img src="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png" Alt-one">查看前提条件`

- 您已将 Kubernetes 集群发现为 Cloud Manager 工作环境。
 - 集群上必须安装 Trident，并且 Trident 版本必须为 21.1 或更高版本。
 - 要用于创建要备份的永久性卷的所有 PVC 都必须将 "snapshotPolicy" 设置为 "default"。
 - 集群必须使用 AWS 上的 Cloud Volumes ONTAP 作为其后端存储。
 - Cloud Volumes ONTAP 系统必须运行 ONTAP 9.7P5 或更高版本。
- 您已为备份所在的存储空间订阅了有效的云提供商。
- 您已订阅 "Cloud Manager Marketplace Backup 产品"，和 "AWS 年度合同"或您已购买 "并激活" NetApp 提供的 Cloud Backup BYOL 许可证。
- 为 Cloud Manager Connector 提供权限的 IAM 角色包括最新版本的 S3 权限 "Cloud Manager 策略"。

选择工作环境，然后单击右侧面板中备份和还原服务旁边的 * 启用 *，然后按照设置向导进行操作。



默认策略每天备份卷，并保留每个卷的最新 30 个备份副本。更改为每小时，每天，每周或每月备份，或者选择一个提供更多选项的系统定义策略。您还可以更改要保留的备份副本数。

Define Policy

Policy - Retention & Schedule

<input type="checkbox"/> Hourly	Number of backups to retain	24
<input checked="" type="checkbox"/> Daily	Number of backups to retain	30
<input type="checkbox"/> Weekly	Number of backups to retain	52
<input type="checkbox"/> Monthly	Number of backups to retain	12

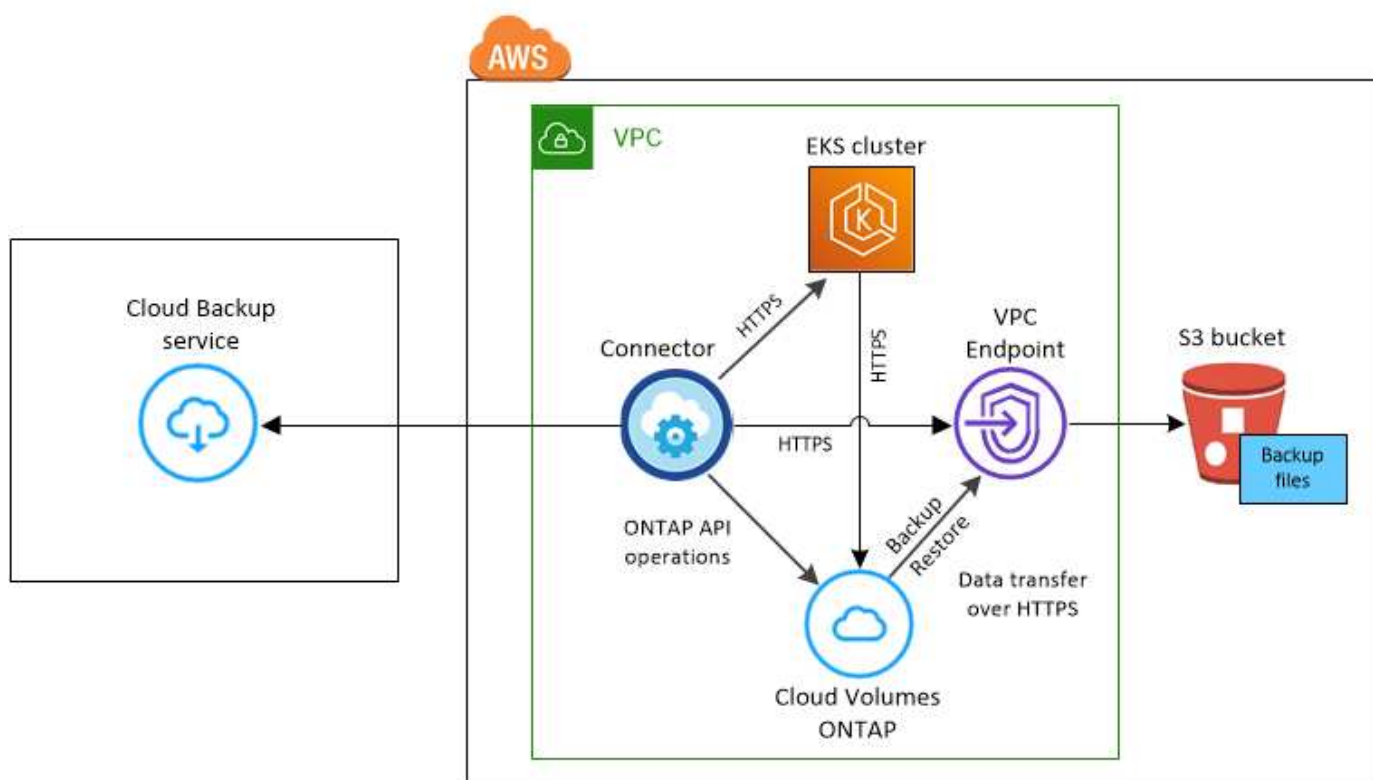
S3 Bucket Cloud Manager will create the S3 bucket after you complete the wizard

在选择卷页面中确定要备份的卷。系统会在与 Cloud Volumes ONTAP 系统相同的 AWS 帐户和区域中自动创建 S3 存储分段，并且备份文件会存储在该处。

要求

开始将 Kubernetes 永久性卷备份到 S3 之前，请阅读以下要求，以确保您的配置受支持。

下图显示了每个组件以及需要在它们之间准备的连接：



请注意，VPC 端点是可选的。

Kubernetes 集群要求

- 您已将 Kubernetes 集群发现为 Cloud Manager 工作环境。 [了解如何发现 Kubernetes 集群](#)。

- 集群上必须安装 Trident ，并且 Trident 版本必须至少为 21.1 。请参见 ["如何安装 Trident"](#) 或 ["如何升级 Trident 版本"](#)。
- 集群必须使用 AWS 上的 Cloud Volumes ONTAP 作为其后端存储。
- Cloud Volumes ONTAP 系统必须与 Kubernetes 集群位于同一 AWS 区域、并且必须运行 ONTAP 9.7P5 或更高版本(建议使用 ONTAP 9.8P11 及更高版本)。

请注意，不支持内部位置中的 Kubernetes 集群。仅支持使用 Cloud Volumes ONTAP 系统的云部署中的 Kubernetes 集群。

- 要用于创建要备份的永久性卷的所有永久性卷声明对象都必须将 "snapshotPolicy" 设置为 "default" 。

您可以通过在标注下添加 snapshotPolicy 来为单个 PVC 执行此操作：

```
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver
```

您可以通过在 backend.json 文件的 defaults 下添加 snapshotPolicy 字段来为与特定后端存储关联的所有 PVC 执行此操作：

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

许可证要求

对于 Cloud Backup PAYGO 许可，AWS Marketplace 中提供了 Cloud Manager 订阅，用于部署 Cloud Volumes ONTAP 和 Cloud Backup。您需要 ["订阅此 Cloud Manager 订阅"](#) 启用 Cloud Backup 之前。Cloud Backup 的计费通过此订阅完成。

对于能够同时备份 Cloud Volumes ONTAP 数据和内部 ONTAP 数据的年度合同，您需要从订阅 ["AWS Marketplace 页面"](#) 然后 ["将订阅与您的 AWS 凭据关联"](#)。

对于能够捆绑 Cloud Volumes ONTAP 和云备份的年度合同，您必须在创建 Cloud Volumes ONTAP 工作环境时设置年度合同。此选项不允许您备份内部数据。

对于 Cloud Backup BYOL 许可，您需要 NetApp 提供的序列号，以便在许可证有效期和容量内使用此服务。["了解如何管理 BYOL 许可证"](#)。

您需要为备份所在的存储空间创建一个 AWS 帐户。

支持的 AWS 区域

所有 AWS 地区均支持 Cloud Backup ["支持 Cloud Volumes ONTAP 的位置"](#)。

需要 AWS 备份权限

为 Cloud Manager 提供权限的 IAM 角色必须包含最新版本的 S3 权限 ["Cloud Manager 策略"](#)。

以下是策略中的特定 S3 权限：

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource": [
    "arn:aws:s3:::netapp-backup-*"
  ]
}
```

启用 Cloud Backup

可以随时直接从Kubernetes工作环境启用Cloud Backup。

步骤

1. 选择工作环境，然后单击右面板中备份和还原服务旁边的 * 启用 *。

如果您的备份的Amazon S3目标作为工作环境存在于Canvas上、您可以将Kubernetes集群拖动到Amazon S3工作环境中以启动设置向导。



2. 输入备份策略详细信息并单击 * 下一步 *。

您可以定义备份计划并选择要保留的备份数。

Define Policy

Policy - Retention & Schedule

☐ Hourly
☒ Daily
☐ Weekly
☐ Monthly

Number of backups to retain

S3 Bucket Cloud Manager will create the S3 bucket after you complete the wizard

3. 选择要备份的永久性卷。

- 要备份所有卷，请选中标题行 (☒ Volume Name)。
- 要备份单个卷，请选中每个卷对应的框 (☒ Volume_1)。

Select Volumes

57 Volumes

<input checked="" type="checkbox"/>	Persistent Volume Name	Namespace	Allocated Capacity	Backup Status
<input checked="" type="checkbox"/>	Persistent Volume 1 ● On	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Persistent Volume 2 ● On	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	Persistent Volume 3 ● On	Namespace 1	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	PV 1 ● On	Namespace 2	10 TB	⊖ Not Active
<input checked="" type="checkbox"/>	PV 2 ● On	Namespace 2	10 TB	⊖ Not Active

☒ Automatically back up all existing and future persistent volumes with the selected backup policy ⓘ

- 如果您希望所有当前卷和未来卷都启用备份、只需选中"自动备份未来卷..."复选框即可。如果禁用此设置、则需要手动为未来的卷启用备份。
- 单击 * 激活备份 *，Cloud Backup 将开始对每个选定卷进行初始备份。

系统会在与 Cloud Volumes ONTAP 系统相同的 AWS 帐户和区域中自动创建 S3 存储分段，并且备份文件会存储在该处。

此时将显示 Kubernetes 信息板，以便您可以监控备份的状态。

您可以 ["启动和停止卷备份或更改备份计划"](#)。您也可以 ["从备份文件还原整个卷"](#) 作为 AWS 中相同或不同 Kubernetes 集群上的新卷（位于同一区域）。

管理 Kubernetes 系统的备份

您可以通过更改备份计划，启用 / 禁用卷备份，删除备份等来管理 Kubernetes 系统的备份。



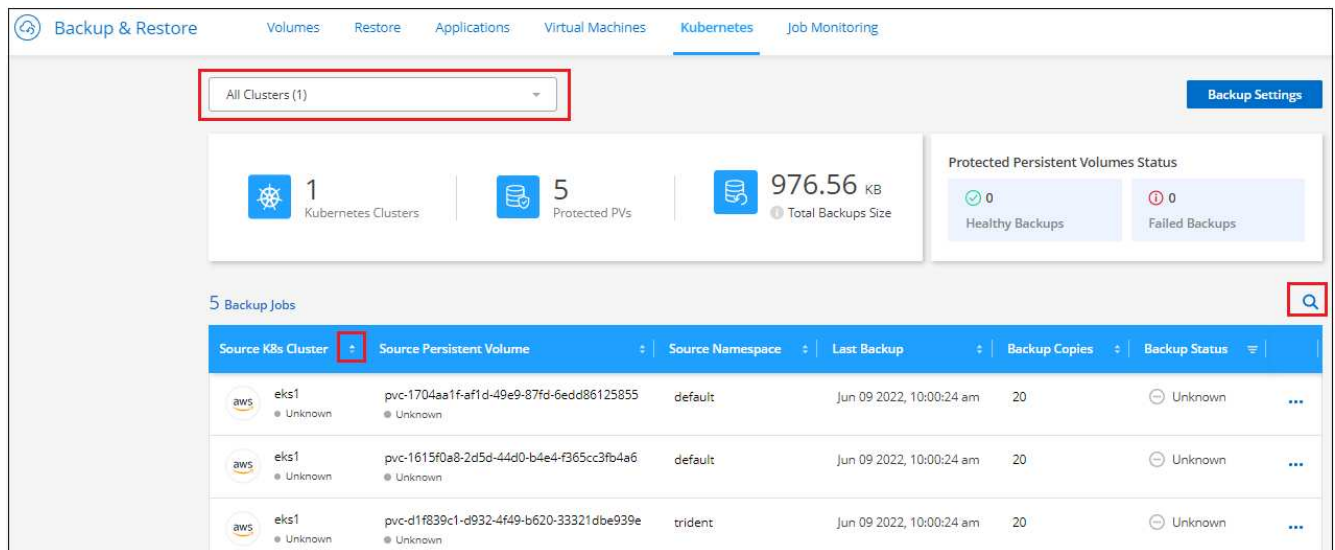
请勿直接从云提供商环境管理或更改备份文件。这可能会损坏文件并导致配置不受支持。

查看要备份的卷

您可以查看 Cloud Backup 当前正在备份的所有卷的列表。

步骤

1. 单击 * 备份和还原 * 服务。
2. 单击 * Kubernetes * 选项卡可查看 Kubernetes 系统的永久性卷列表。



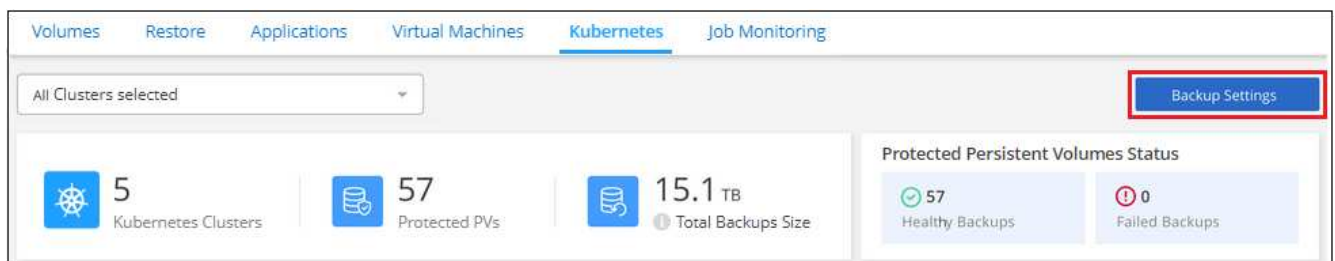
如果要在某些集群中查找特定卷、您可以按集群和卷细化此列表、也可以使用搜索筛选器。

启用和禁用卷备份

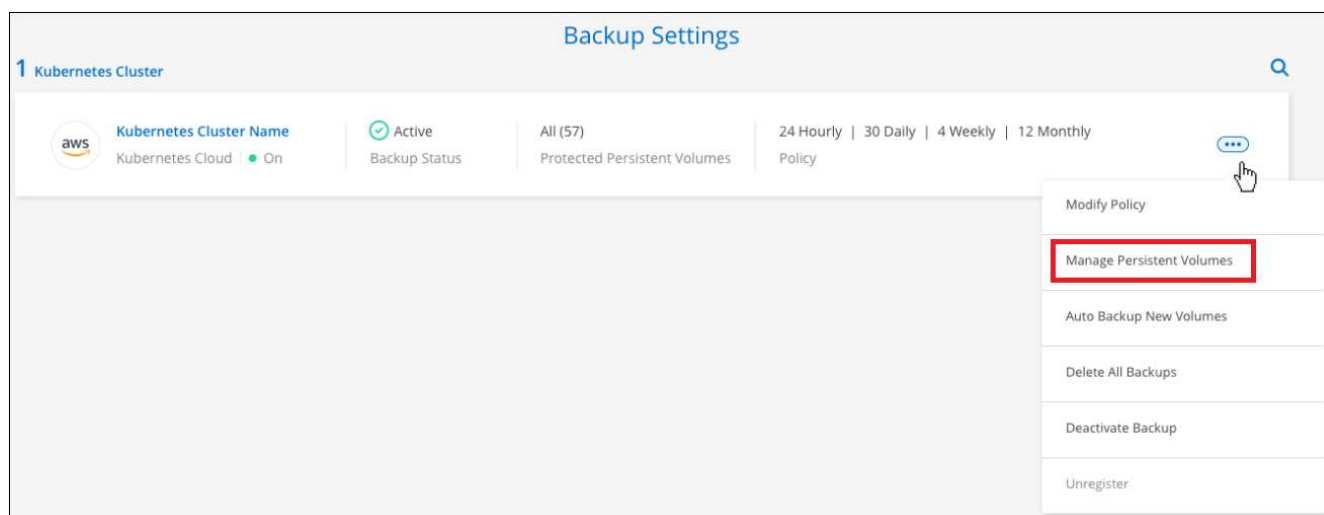
如果您不需要卷的备份副本，并且不想为存储备份付费，则可以停止备份卷。如果当前未备份新卷，您也可以将其添加到备份列表中。

步骤

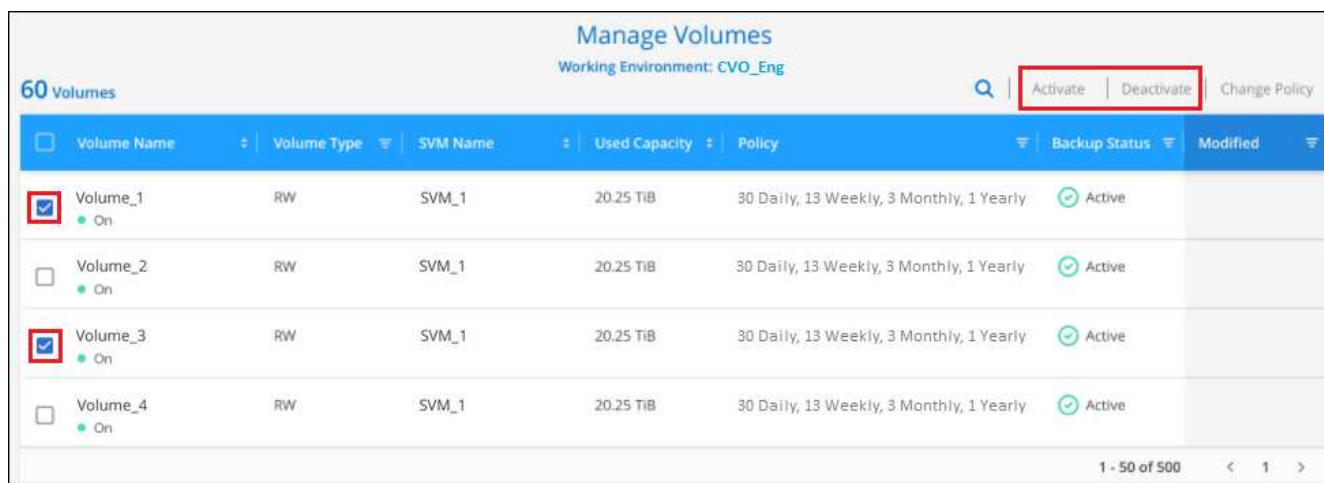
1. 从 * Kubernetes * 选项卡中，选择 * 备份设置 *。



2. 在 *Backup Settings* page 中, 单击 ... 对于Kubernetes集群、选择*管理永久性卷*。



3. 选中要更改的一个或多个卷对应的复选框, 然后根据要启动还是停止卷的备份, 单击 * 激活 * 或 * 停用 *。



4. 单击 * 保存 * 以提交更改。

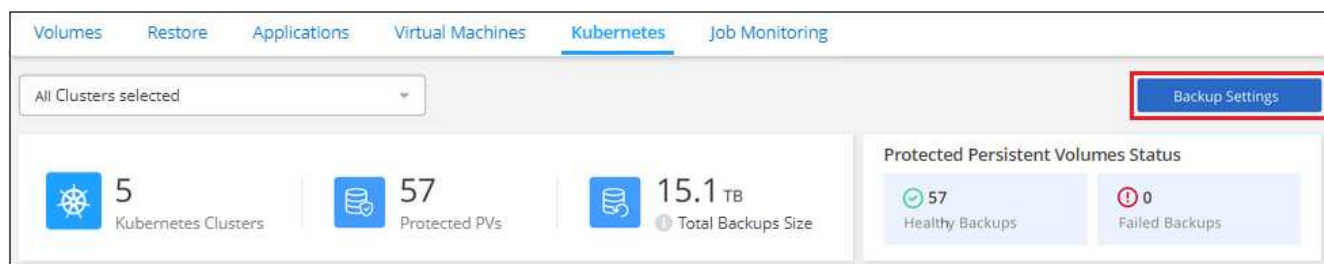
◦ 注意: * 停止备份卷时, 云提供商会继续为备份所用容量收取对象存储成本, 除非您这样做 [删除备份](#)。

编辑现有备份策略

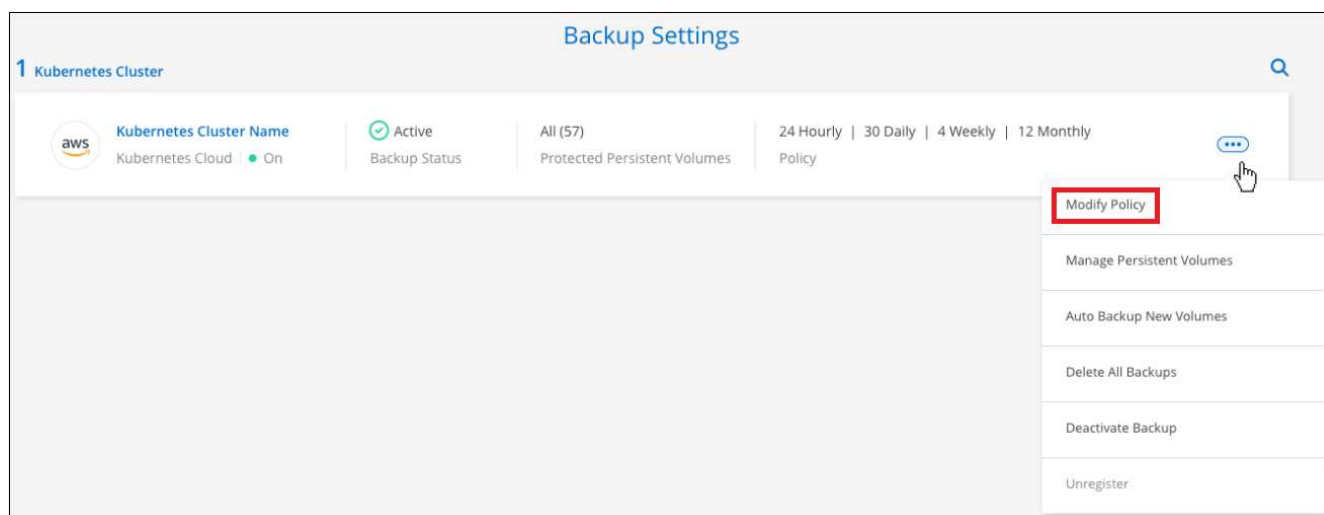
您可以更改当前应用于工作环境中卷的备份策略的属性。更改备份策略会影响正在使用此策略的所有现有卷。

步骤

1. 从 * Kubernetes * 选项卡中, 选择 * 备份设置 *。



2. 从 *Backup Settings* 页面中，单击 ... 对于要更改设置的工作环境，请选择 * 管理策略 *。



3. 在 *Manage Policies* 页面中，为要在该工作环境中更改的备份策略单击 * 编辑策略 *。



4. 在 *Edit Policy* 页面中，更改计划和备份保留，然后单击 * 保存 *。



设置要分配给新卷的备份策略

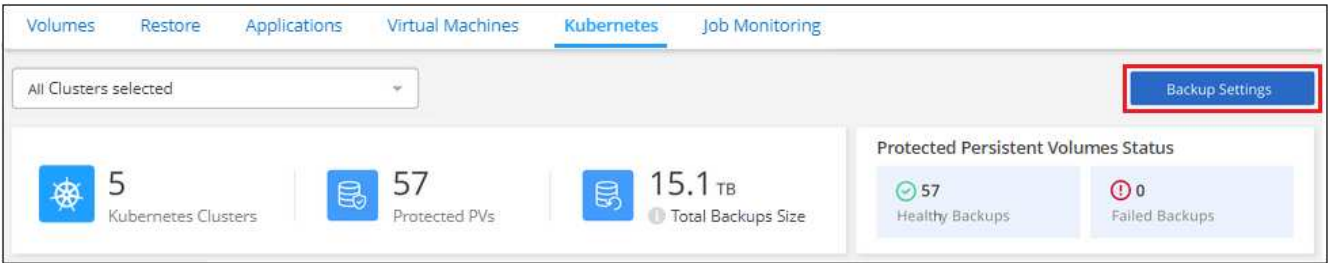
如果您未选择在首次在Kubernetes集群上激活Cloud Backup时自动为新创建的卷分配备份策略的选项，则可以稍后在_Backup Settings_页面中选择此选项。为新创建的卷分配备份策略可确保所有数据都受到保护。

请注意，要应用于卷的策略必须已存在。 [请参见如何为工作环境添加新的备份策略。](#)

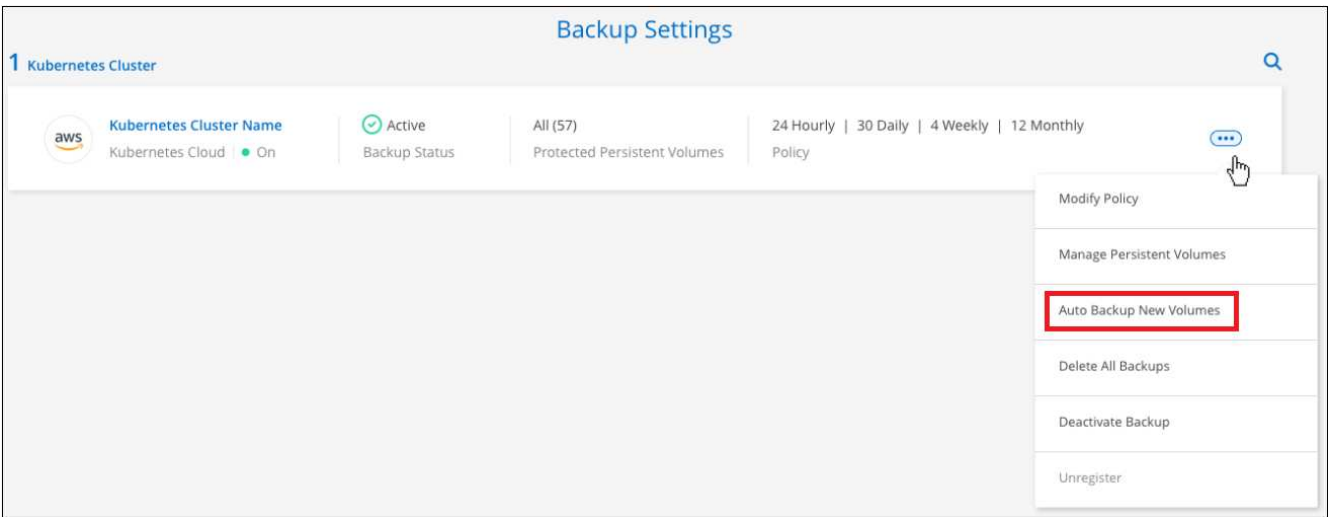
您也可以禁用此设置、以使新创建的卷不会自动备份。在这种情况下、您需要手动为将来要备份的任何特定卷启用备份。

步骤

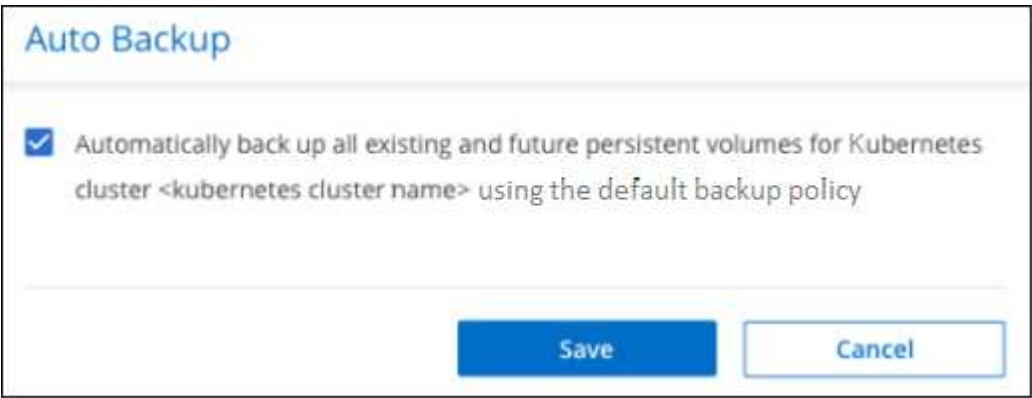
- 1. 从 * Kubernetes * 选项卡中，选择 * 备份设置 *。



- 2. 在 Backup Settings page 中，单击 ... 对于存在卷的Kubernetes集群、选择*自动备份新卷*。



- 3. 选中"自动备份未来的永久性卷..."复选框、选择要应用于新卷的备份策略、然后单击*保存*。



现在、此备份策略将应用于在此Kubernetes集群中创建的任何新卷。

查看每个卷的备份列表

您可以查看每个卷的所有备份文件的列表。此页面显示有关源卷，目标位置和备份详细信息，例如上次执行的备

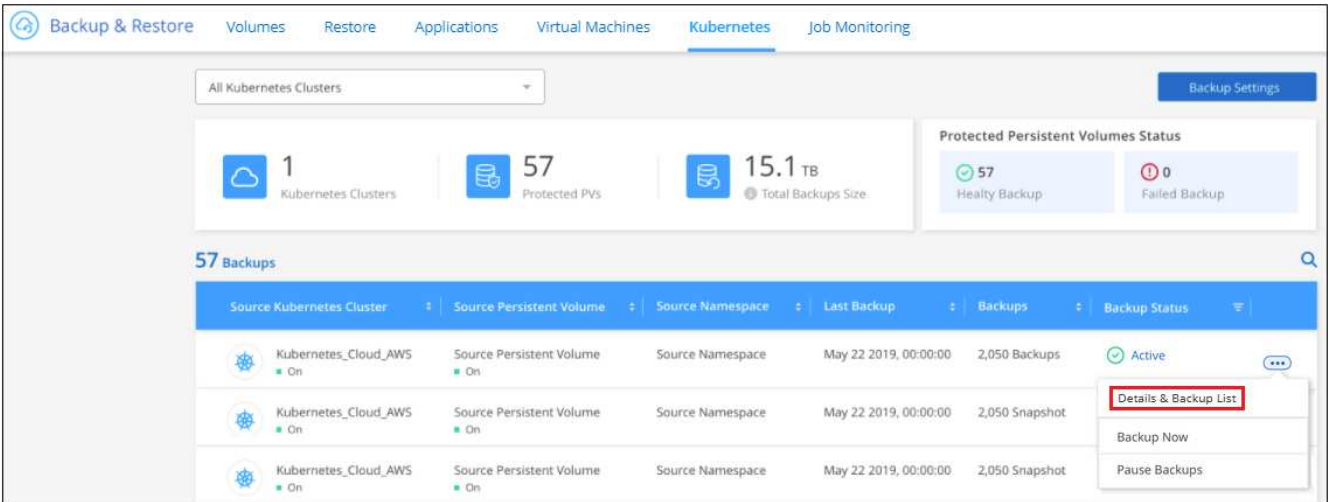
份，当前备份策略，备份文件大小等。

您还可以通过此页面执行以下任务：

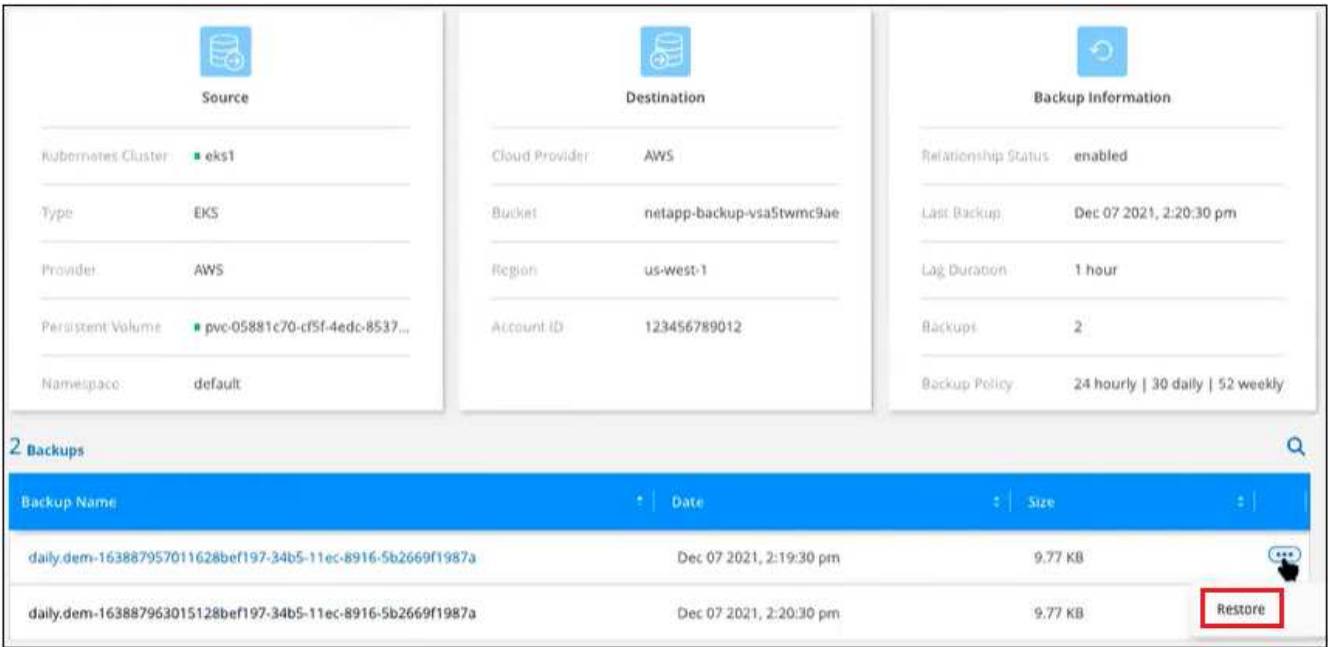
- 删除卷的所有备份文件
- 删除卷的单个备份文件
- 下载卷的备份报告

步骤

1. 从 * Kubernetes * 选项卡中，单击 ... 对于源卷，然后选择 * 详细信息和备份列表 *。



此时将显示所有备份文件的列表以及有关源卷，目标位置和备份详细信息。



删除备份

通过 Cloud Backup ，您可以删除单个备份文件，删除卷的所有备份或删除 Kubernetes 集群中所有卷的所有备

份。如果您不再需要备份，或者删除了源卷并希望删除所有备份，则可能需要删除所有备份。



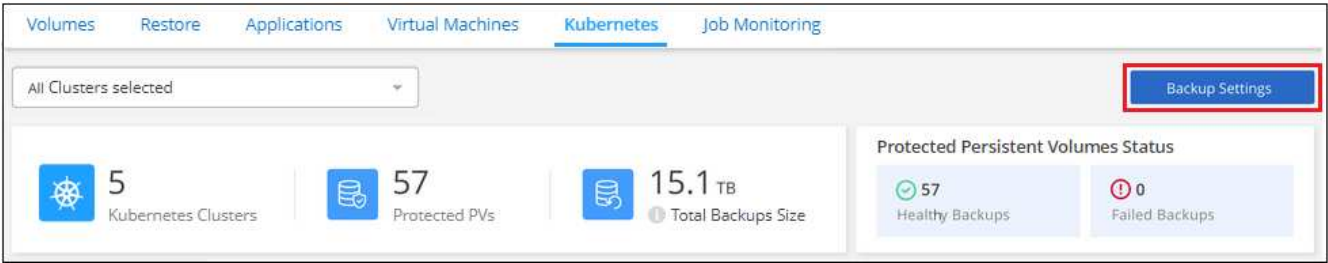
如果您计划删除具有备份的工作环境或集群，则必须删除备份 * 在删除系统之前 *。删除系统时，Cloud Backup 不会自动删除备份，并且用户界面当前不支持在删除系统后删除这些备份。对于任何剩余备份，您仍需支付对象存储成本费用。

删除工作环境中的所有备份文件

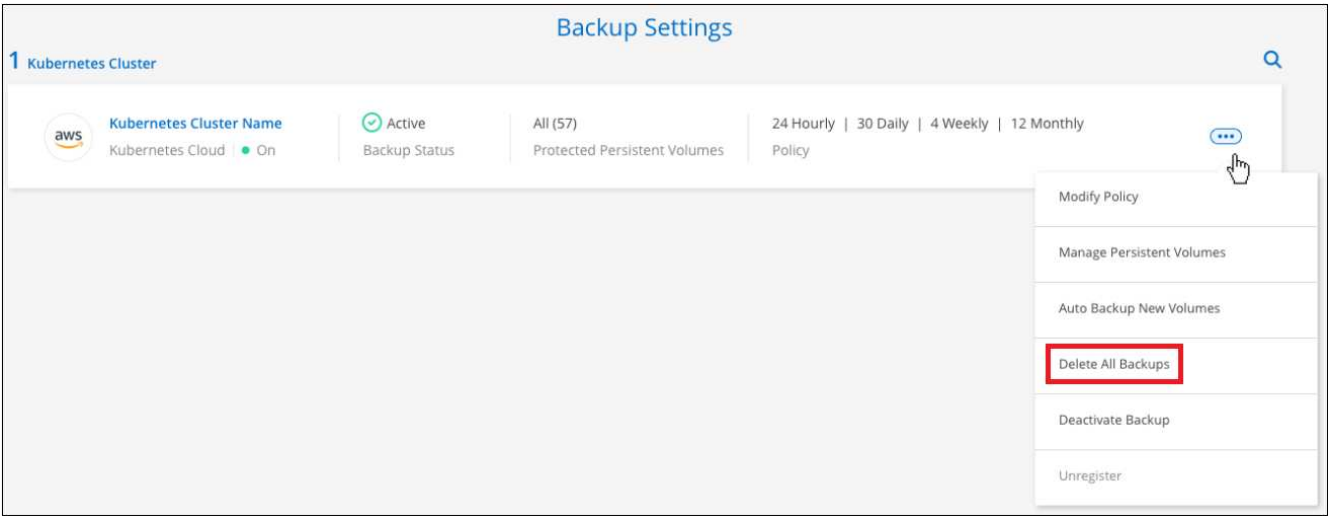
删除工作环境中的所有备份不会禁用此工作环境中的卷将来备份。如果要停止在环境中创建所有卷的备份，可以停用备份 [如此处所述](#)。

步骤

- 1. 从 * Kubernetes * 选项卡中，选择 * 备份设置 *。



- 2. 单击 ... 对于要删除所有备份的 Kubernetes 集群，请选择 * 删除所有备份 *。



- 3. 在确认对话框中，输入工作环境的名称，然后单击 * 删除 *。

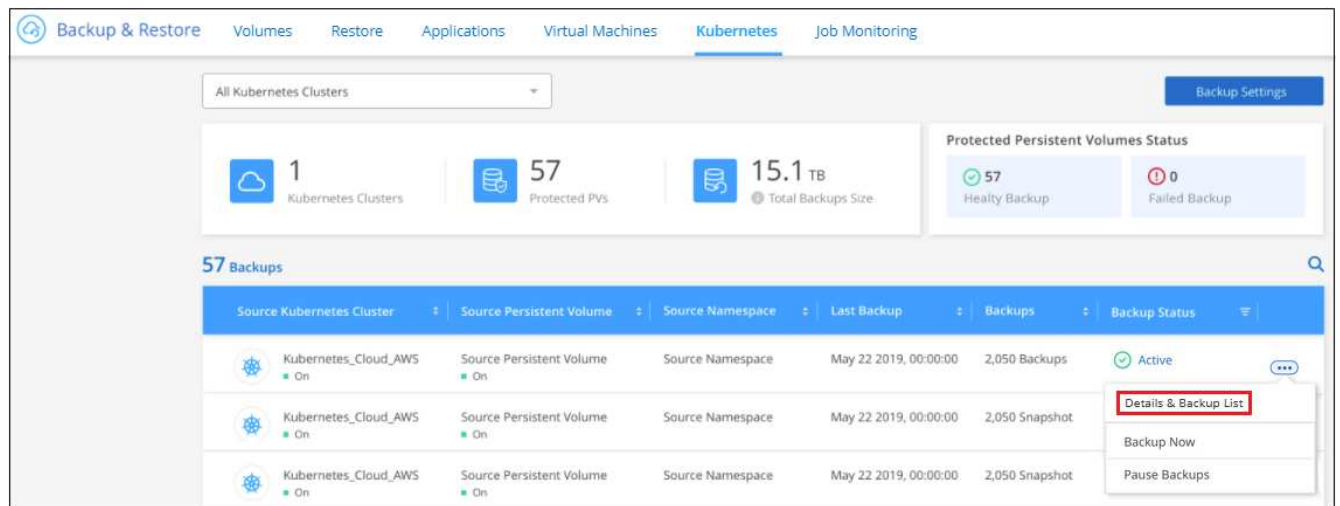
删除卷的所有备份文件

删除卷的所有备份也会禁用该卷的未来备份。

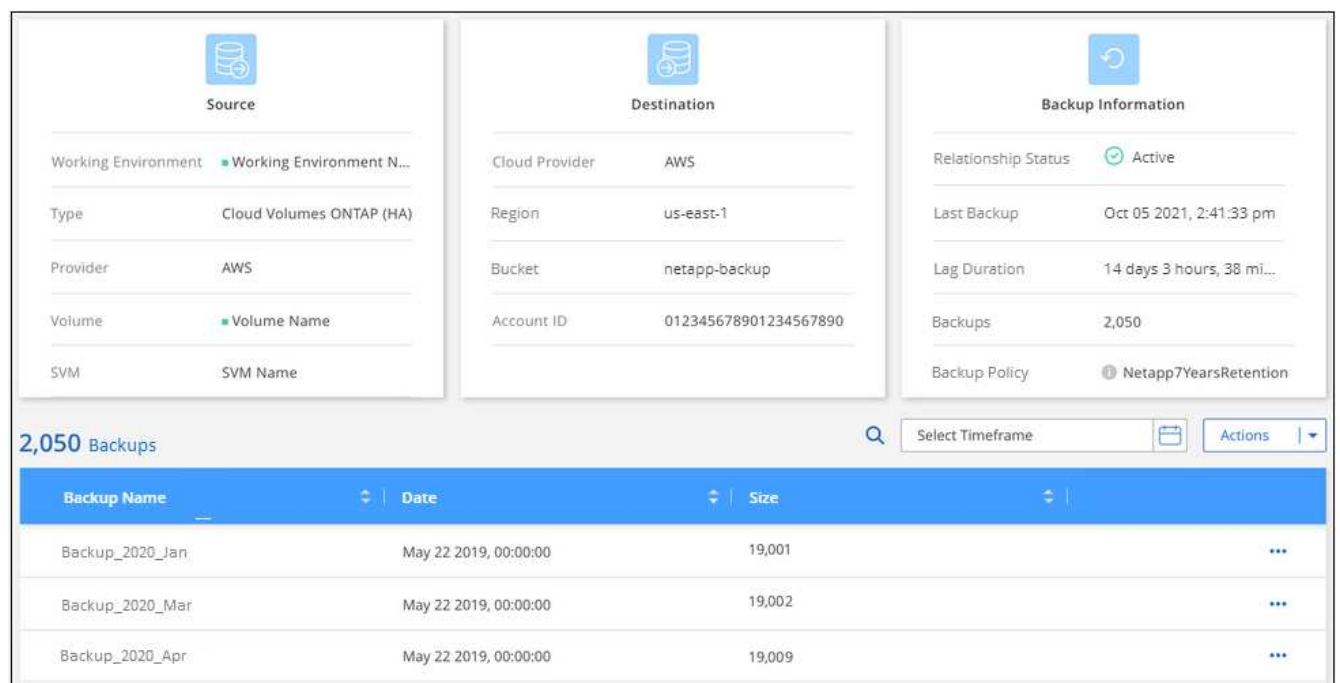
您可以 [重新开始为卷创建备份](#) 可随时从管理备份页面访问。

步骤

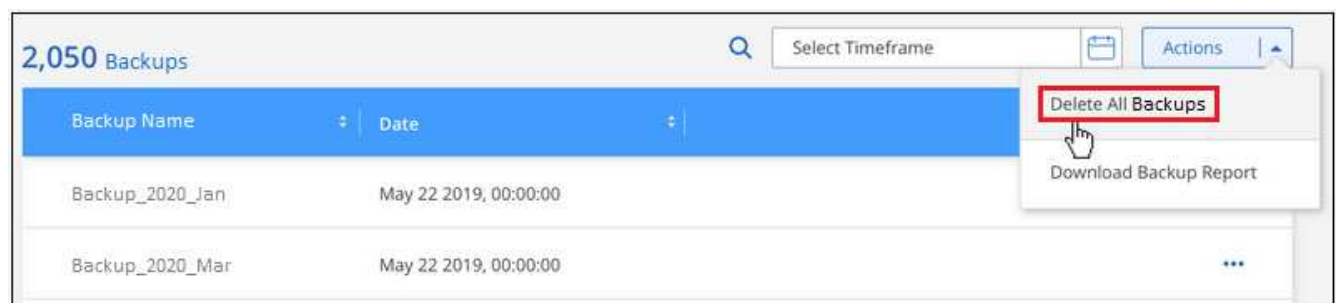
- 1. 从 * Kubernetes * 选项卡中，单击 ... 对于源卷，然后选择 * 详细信息和备份列表 *。



此时将显示所有备份文件的列表。



2. 单击 * 操作 * > * 删除所有备份 *。



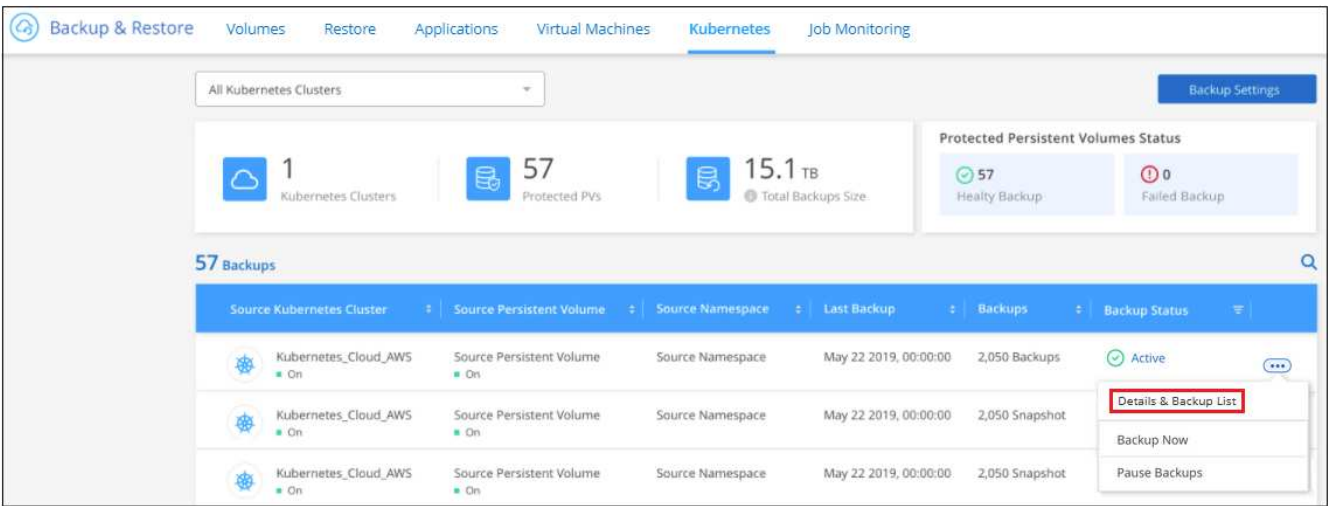
3. 在确认对话框中，输入卷名称并单击 * 删除 *。

删除卷的单个备份文件

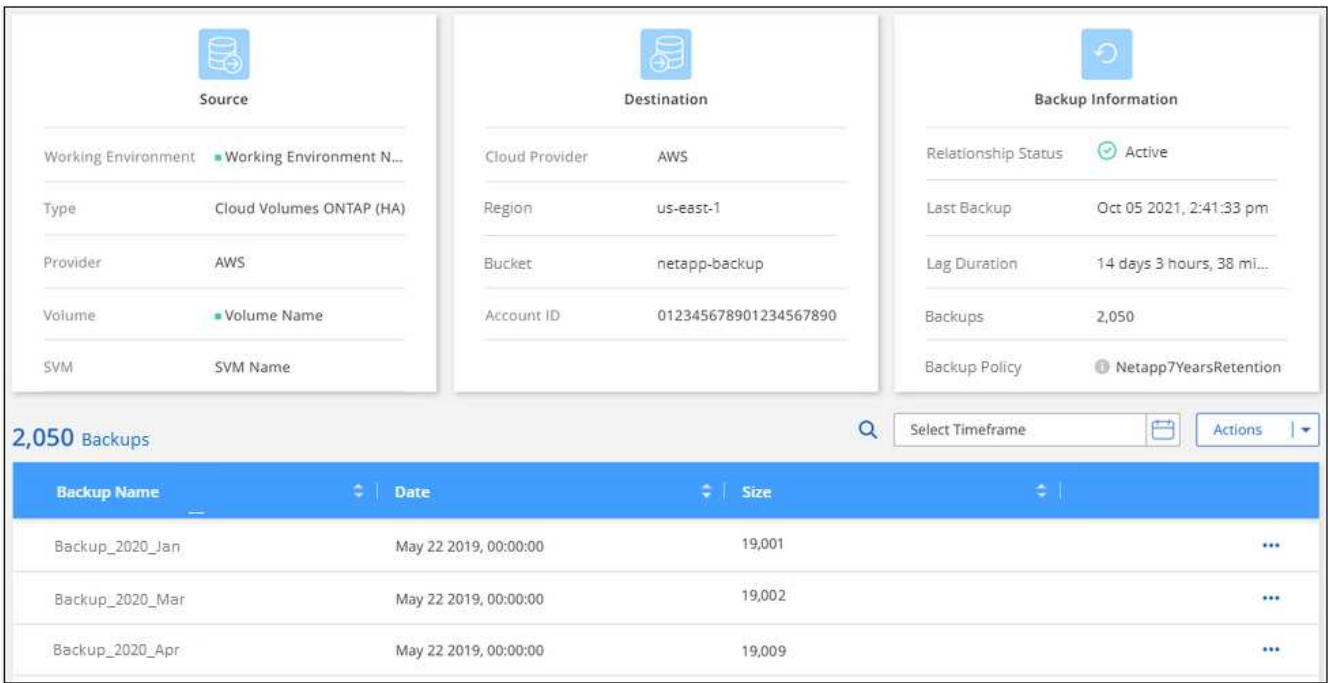
您可以删除单个备份文件。只有在使用 ONTAP 9.8 或更高版本的系统创建卷备份时，此功能才可用。

步骤

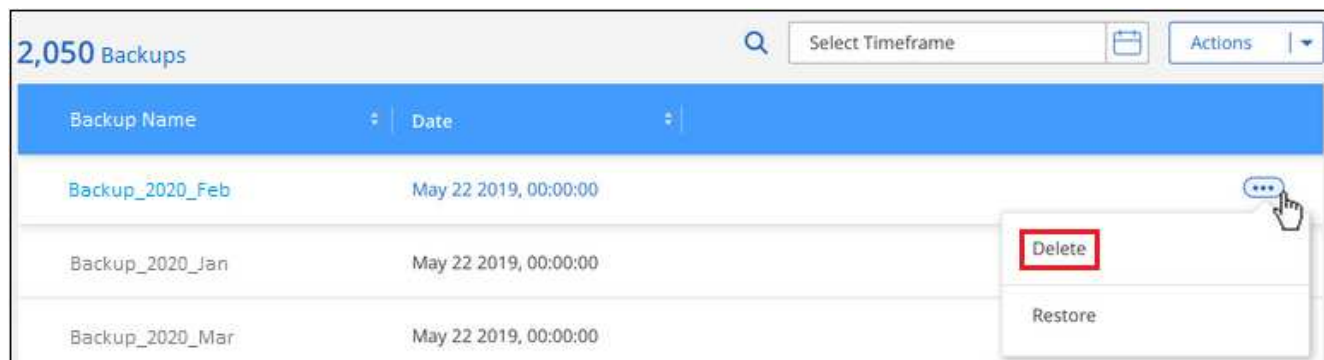
1. 从 * Kubernetes * 选项卡中，单击 ... 对于源卷，然后选择 * 详细信息和备份列表 *。



此时将显示所有备份文件的列表。



2. 单击 ... 对于要删除的卷备份文件，然后单击 * 删除 *。



3. 在确认对话框中，单击 * 删除 *。

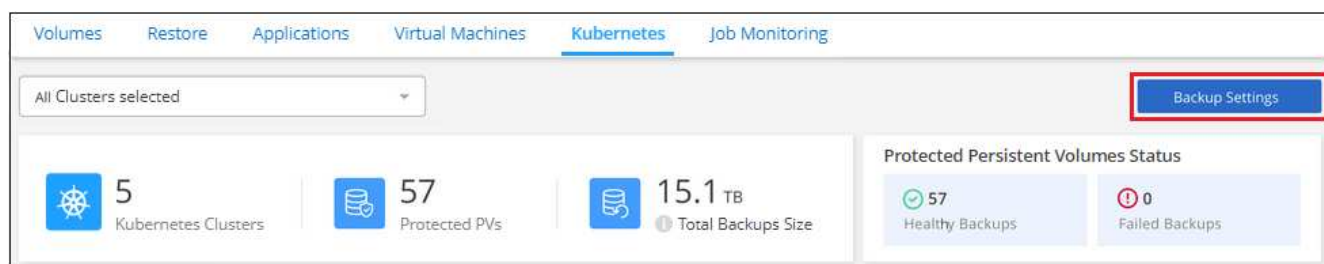
为工作环境禁用 Cloud Backup

禁用工作环境的 Cloud Backup 会禁用系统上每个卷的备份，同时也会禁用还原卷的功能。不会删除任何现有备份。这样不会从此工作环境中取消注册备份服务—它基本上允许您将所有备份和还原活动暂停一段时间。

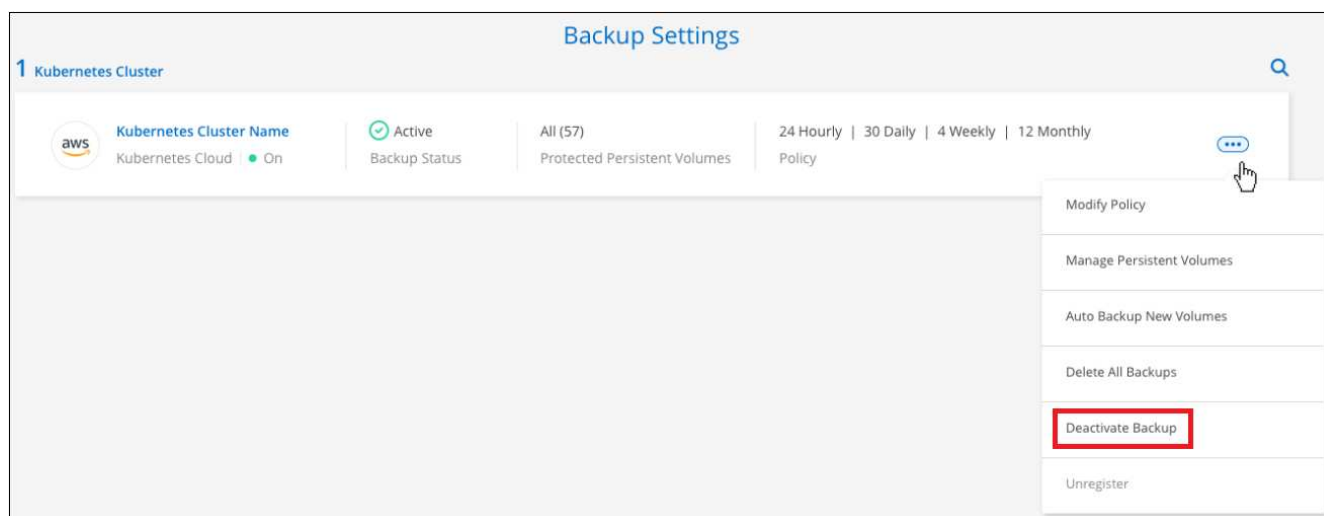
请注意，除非您的备份使用的容量，否则云提供商会继续向您收取对象存储成本 [删除备份](#)。

步骤

1. 从 * Kubernetes * 选项卡中，选择 * 备份设置 *。



2. 在 *Backup Settings page* 中，单击 ... 对于要禁用备份的工作环境或 Kubernetes 集群，请选择 * 停用备份 *。



3. 在确认对话框中，单击 * 停用 *。



在禁用备份的情况下，系统将为此工作环境显示一个 * 激活备份 * 按钮。如果要为该工作环境重新启用备份功能，可以单击此按钮。

为工作环境取消注册 Cloud Backup

如果您不想再使用备份功能，而希望在工作环境中不再需要为备份付费，则可以取消注册适用于此工作环境的 Cloud Backup。通常，当您计划删除 Kubernetes 集群并要取消备份服务时，会使用此功能。

如果要更改存储集群备份的目标对象存储，也可以使用此功能。在为工作环境取消注册 Cloud Backup 后，您可以使用新的云提供商信息为此集群启用 Cloud Backup。

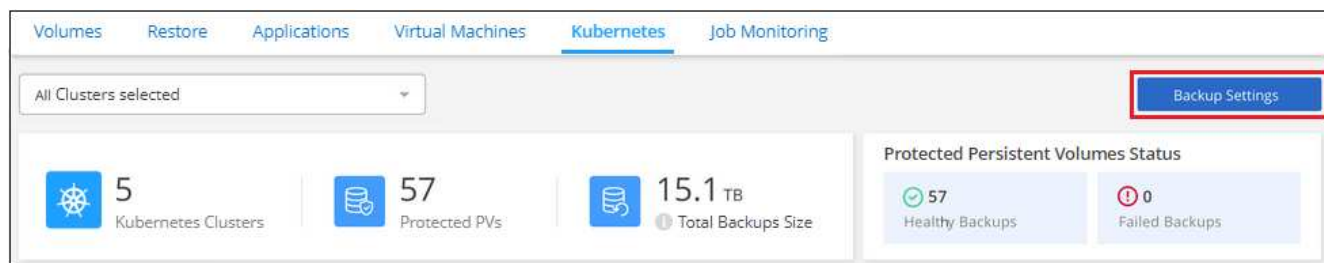
在注销 Cloud Backup 之前，必须按以下顺序执行以下步骤：

- 为工作环境停用 Cloud Backup
- 删除该工作环境的所有备份

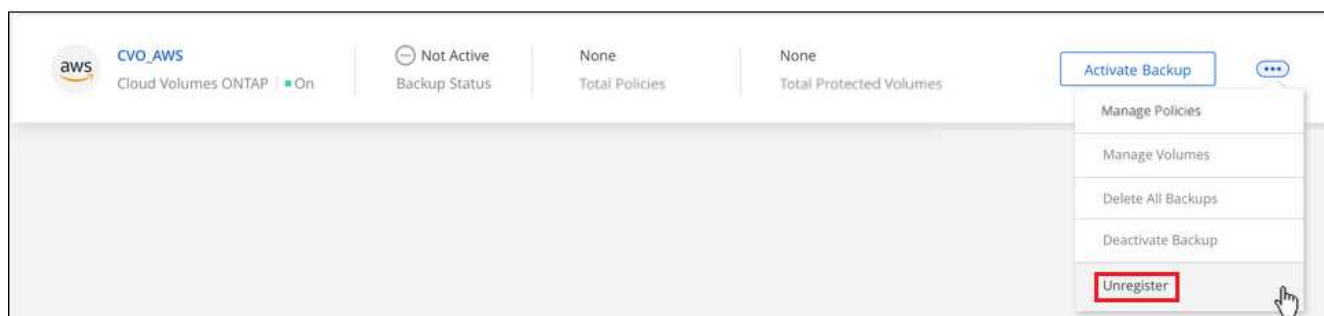
只有在这两个操作完成后，取消注册选项才可用。

步骤

1. 从 * Kubernetes * 选项卡中，选择 * 备份设置 *。



2. 在 *Backup Settings page* 中，单击 ... 对于要取消注册备份服务的 Kubernetes 集群，请选择 * 取消注册 *。



3. 在确认对话框中，单击 * 取消注册 *。

从备份文件还原 Kubernetes 数据

备份存储在云帐户的对象存储中，以便您可以从特定时间点还原数据。您可以从已保存的备份文件还原整个 Kubernetes 永久性卷。

您可以将永久性卷（作为新卷）还原到同一工作环境或使用同一云帐户的不同工作环境。

支持的工作环境和对象存储提供程序

您可以将卷从 Kubernetes 备份文件还原到以下工作环境：

备份文件位置	目标工作环境
Amazon S3	AWS内的Kubernetes集群
Azure Blob	Azure内的Kubernetes集群
Google Cloud 存储	Google 中的Kubernetes集群

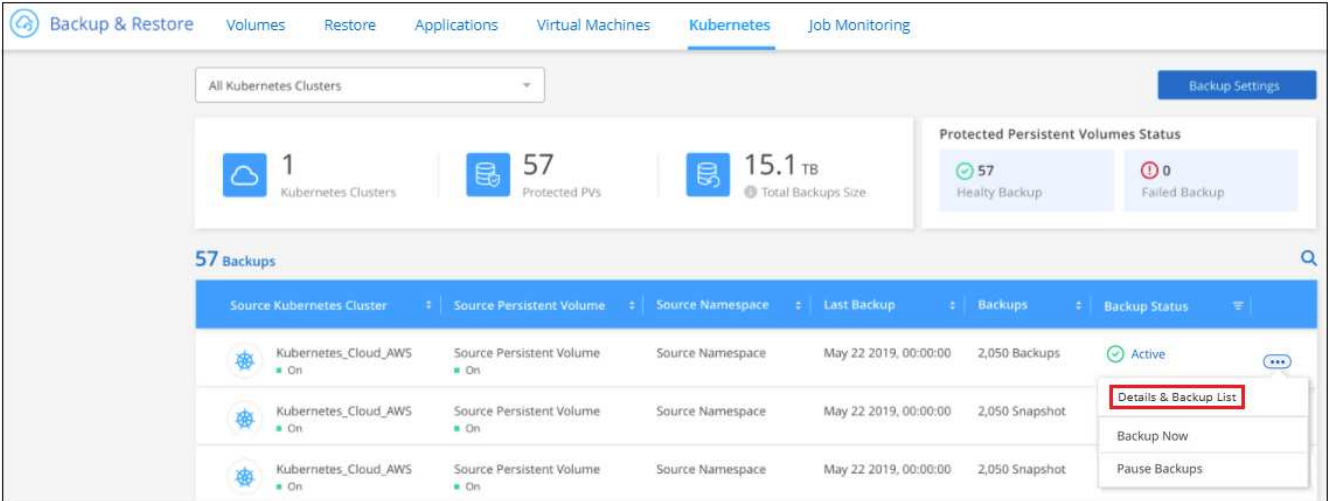
从 Kubernetes 备份文件还原卷

从备份文件还原永久性卷时，Cloud Manager 会使用备份中的数据创建 *new* 卷。您可以将数据还原到同一 Kubernetes 集群中的卷或与源 Kubernetes 集群位于同一云帐户中的其他 Kubernetes 集群。

开始之前，您应知道要还原的卷的名称以及要用于创建新还原的卷的备份文件的日期。

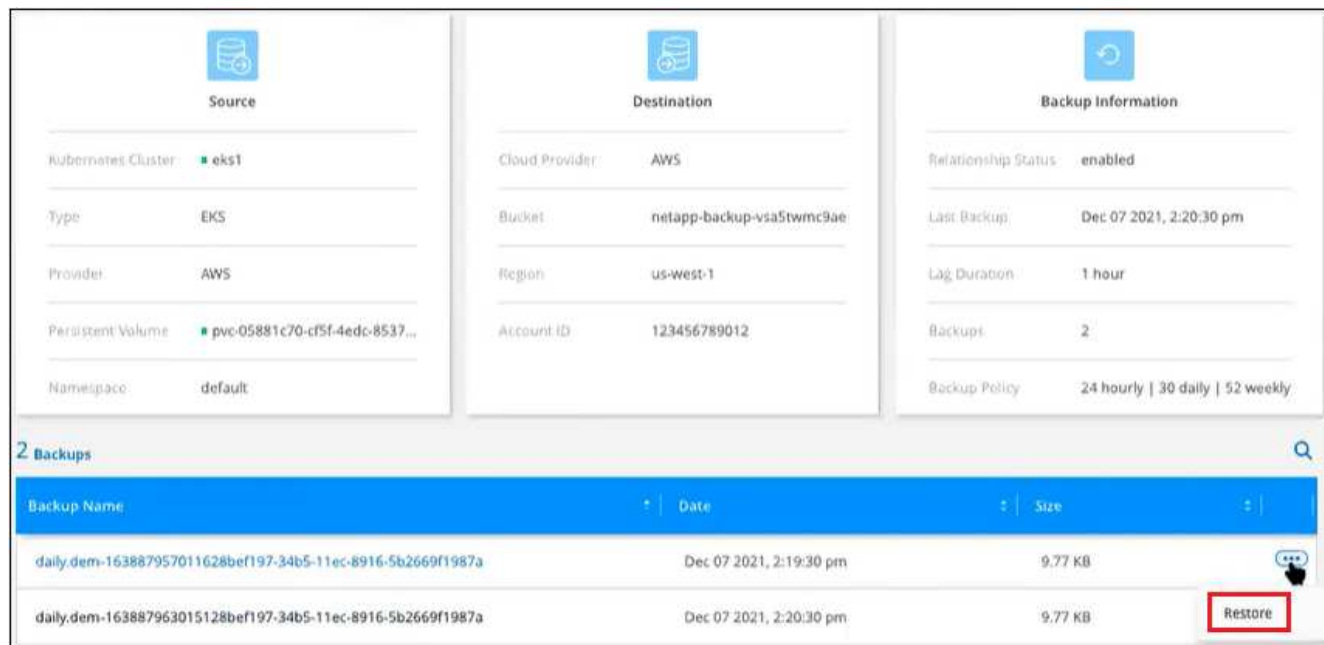
步骤

1. 选择 * 备份和还原 * 服务。
2. 单击 * Kubernetes * 选项卡，此时将显示 Kubernetes 信息板。



3. 找到要还原的卷，然后单击 ...、然后单击*详细信息和备份列表*。

此时将显示该卷的所有备份文件列表以及有关源卷，目标位置和备份详细信息。



4. 根据日期 / 时间戳找到要还原的特定备份文件，然后单击 **...**，然后是 *** 还原 ***。
5. 在 *Select Destination* 页面中，选择要还原卷的 *Kubernetes cluster*，*Namespaces*，*Storage Class* 以及新的 *_Persistent* 卷名称 *_*。

Select Destination

Select Kubernetes Cluster

eks1

Namespace

default

Storage Class

basic

PVC Name

pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1-restore

Cancel

Restore

6. 单击 *** 还原 ***，您将返回到 Kubernetes 信息板，以便查看还原操作的进度。

Cloud Manager 会根据您选择的备份在 Kubernetes 集群中创建一个新卷。您可以 ["管理此新卷的备份设置"](#) 根据需要。

备份和还原内部应用程序数据

保护内部应用程序数据

您可以将适用于应用程序的 Cloud Backup 与 Cloud Manager 和内部 SnapCenter 集成，以便将应用程序一致的 Snapshot 从内部 ONTAP 备份到云。如果需要，您可以从云还原到内部 SnapCenter 服务器。

您可以将内部 ONTAP 系统中的 Oracle 和 Microsoft SQL 应用程序数据备份到以下云提供商：

- Amazon Web Services
- Microsoft Azure



您应使用 SnapCenter 软件 4.6 。

有关适用于应用程序的 Cloud Backup 的详细信息，请参见：

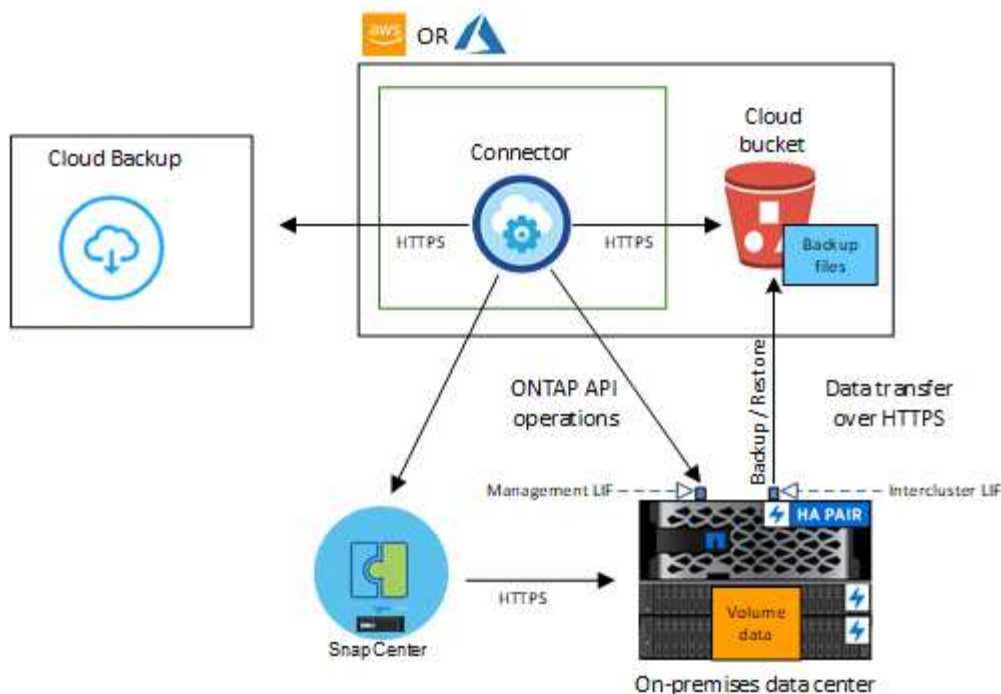
- ["借助 Cloud Backup 和 SnapCenter 实现应用程序感知备份"](#)
- ["适用于应用程序的云备份"](#)

要求

在开始将应用程序数据备份到云服务之前，请阅读以下要求，以确保您的配置受支持。

- ONTAP 9.8 或更高版本
- Cloud Manager 3.9
- SnapCenter 服务器 4.6.
- SnapCenter 服务器中应为每个应用程序至少提供一个备份
- SnapCenter 中至少有一个每日，每周或每月策略，没有与 Cloud Manager 中的 Cloud Backup for Applications 策略相同的标签。

下图显示了每个组件以及需要在它们之间准备的连接：



保护策略

您应使用 Cloud Backup for Applications 中定义的策略之一将应用程序数据备份到云。



不支持自定义策略。

Policy name	Label	保留值
1 年每日 LTR	每天	366.
5 年每日 LTR	每天	1830 年
7 年每周 LTR	每周	370
10 年每月 LTR	每月	120

可以使用 REST API 修改这些策略的标签和保留值，直到该策略与应用程序关联为止。一个应用程序只能关联一个策略，一旦关联，您就无法解除关联。

除了适用于应用程序的云备份策略之外，您还需要至少一个 SnapCenter 策略来将应用程序数据备份到云。

将内部应用程序数据备份到云

您可以通过将适用于应用程序的云备份与 Cloud Manager 和内部 SnapCenter 集成来将应用程序数据从 ONTAP 备份到云。

注册 SnapCenter 服务器

只有具有 SnapCenterAdmin 角色的用户才能注册运行 SnapCenter Server 4.6 的主机。您可以注册多个 SnapCenter 服务器主机，但一旦注册，便无法删除 SnapCenter 服务器主机。

- 步骤 *

1. 在 Cloud Manager UI 中，单击 * 备份和还原 * > * 应用程序 *。
2. 从 * 设置 * 下拉列表中，单击 * SnapCenter Servers*。
3. 单击 * 注册 SnapCenter Server*。
4. 指定以下详细信息：
 - a. 在 SnapCenter 服务器字段中，指定 SnapCenter 服务器主机的 FQDN 或 IP 地址。
 - b. 在端口字段中，指定运行 SnapCenter 服务器的端口号。

您应确保此端口已打开，以便在 SnapCenter 服务器与适用于应用程序的云备份之间进行通信。

- c. 在标记字段中，指定要标记 SnapCenter 服务器的站点名称，城市名称或任何自定义名称。

这些标记以逗号分隔。

- d. 在用户名和密码字段中，指定具有 SnapCenterAdmin 角色的用户的凭据。

5. 单击 * 注册 *。

- 完成后 *

单击 * 备份和还原 * > * 应用程序 * 可查看使用注册的 SnapCenter 服务器主机保护的所有应用程序。



对于 SQL Server 数据库，应用程序名称列会以 _application_name (主机名) _ 格式显示名称。如果您通过提供 _application_name (主机名) _ 格式的名称进行搜索，则不会显示 SQL Server 数据库详细信息。

支持的应用程序及其配置包括：

- Oracle 数据库：使用至少一个每日，每周或每月计划创建完整备份（数据 + 日志）。
- Microsoft SQL Server 数据库：
 - 独立，故障转移集群实例和可用性组
 - 已创建完整备份，其中至少包含一个每日，每周或每月计划

不会显示以下 Oracle 和 SQL Server 数据库：

- 没有备份的数据库
- 仅具有按需或每小时策略的数据库
- 位于 RDM 或 VMDK 上的数据库

备份应用程序数据

您可以使用一个策略同时将一个或多个应用程序保护到云中。只能分配默认的预制策略来保护应用程序。



如果使用的是 Cloud Manager GUI，则一次只能保护一个应用程序。但是，如果您使用的是 REST API，则可以同时保护多个应用程序。

如果要保护 SQL Server 实例，则会为该实例中符合条件的数据库的所有卷配置云保护。如果要保护 SQL Server 可用性组，则会为该可用性组中数据库的所有卷配置云保护。但是，根据备份首选项，Snapshot 将从相应的卷中复制。

• 步骤 *

1. 在 Cloud Manager UI 中，单击 * 备份和还原 * > * 应用程序 *。
2. 单击 ... 对应于应用程序，然后单击 * 激活备份 *。
3. 添加工作环境。

配置托管运行应用程序的 SVM 的 ONTAP 集群。为其中一个应用程序添加工作环境后，可以对驻留在同一 ONTAP 集群上的所有其他应用程序重复使用该环境。

- a. 选择 SVM，然后单击添加工作环境。
- b. 在添加工作环境向导中：
 - i. 指定 ONTAP 集群的 IP 地址。
 - ii. 指定管理员凭据。

Cloud Backup for Applications 仅支持集群管理。

- c. 单击 * 添加工作环境 *。



在更新工作环境详细信息之前，您不应继续操作。更新工作环境详细信息可能需要长达 30 分钟的时间。30 分钟后，您应关闭向导并从步骤 1 重试以查看工作环境详细信息。如果未更新工作环境详细信息，则重试后，请确保添加了正确的工作环境。

4. 选择并配置云提供商。

配置 Amazon Web Services

- a. 指定 AWS 帐户。
- b. 在 AWS 访问密钥字段中，指定密钥。
- c. 在 AWS 机密密钥字段中，指定密码。
- d. 选择要创建备份的区域。
- e. 指定已添加为工作环境 ONTAP 集群的 IP 地址。

5. 在分配策略页面中，选择策略并单击 * 下一步 *。
6. 查看详细信息并单击 * 激活备份 *。

以下视频显示了有关保护数据库的快速演练：

Microsoft SQL Server backup to AWS S3 or Azure blob

Manohar V Kulkarni
Technical Marketing Engineer

© 2022 NetApp, Inc. All rights reserved.



 NetApp



管理应用程序的保护

您可以查看策略和备份。根据数据库，策略或资源组的更改，您可以从 Cloud Manager UI 刷新更新。

查看策略

您可以查看所有默认预制策略。在查看每个策略的详细信息时，系统都会列出所有关联的 Cloud Backup for Applications 策略以及所有关联的应用程序。

1. 单击 * 备份和还原 * > * 应用程序 *。
2. 从 * 设置 * 下拉列表中，单击 * 策略 *。
3. 单击与要查看其详细信息的策略对应的 * 查看详细信息 *。

此时将列出关联的 Cloud Backup for Applications 策略和所有应用程序。



您不应删除适用于应用程序的 Cloud Backup 策略。

您也可以运行 `Get-SmResources SnapCenter cmdlet` 来查看云扩展 SnapCenter 策略。有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 `get-help command_name` 来获取。或者，您也可以参考 "《[SnapCenter 软件 cmdlet 参考指南](#)》"。

查看云上的备份

您可以在 Cloud Manager UI 中查看云上的备份。

1. 单击 * 备份和还原 * > * 应用程序 *。
2. 单击 ... 对应于应用程序，然后单击 * 查看详细信息 *。



列出备份所需的时间取决于 ONTAP 的默认复制计划（最长 1 小时）和 Cloud Manager（最长 6 小时）。

- 对于 Oracle 数据库，系统会列出数据备份和日志备份，每个备份的 SCN 编号，每个备份的结束日期。您只能选择数据备份并将数据库还原到内部 SnapCenter 服务器。
- 对于 Microsoft SQL Server 数据库，仅会列出完整备份和每个备份的结束日期。您可以选择备份并将数据库还原到内部 SnapCenter 服务器。
- 对于 Microsoft SQL Server 实例，不会列出备份，而是仅列出该实例下的数据库。



在启用云保护之前创建的备份不会列出进行还原。

您也可以通过运行 `Get-SmBackup SnapCenter cmdlet` 来查看这些备份。有关可与 cmdlet 结合使用的参数及其说明的信息，可通过运行 `get-help command_name` 来获取。或者，您也可以参考 "《[SnapCenter 软件 cmdlet 参考指南](#)》"。

数据库布局更改

将卷添加到数据库后，SnapCenter 服务器将根据策略和计划自动为新卷上的快照添加标签。这些新卷不会具有对象存储端点，您应执行以下步骤进行刷新：

1. 单击 * 备份和还原 * > * 应用程序 *。
2. 从 * 设置 * 下拉列表中，单击 * SnapCenter Servers*。
3. 单击 ... 对应于托管应用程序的 SnapCenter 服务器，然后单击 * 刷新 *。

此时将发现新卷。

4. 单击 ... 对应于应用程序，然后单击 * 刷新保护 * 为新卷启用云保护。

如果在配置云服务后从应用程序中删除存储卷，则对于新备份，SnapCenter 服务器将仅标记应用程序所在的快照。如果删除的卷未被任何其他应用程序使用，则应手动删除对象存储关系。如果您更新应用程序清单，它将包含应用程序的当前存储布局。

策略或资源组更改

如果 SnapCenter 策略或资源组发生更改，则应刷新保护。

1. 单击 * 备份和还原 * > * 应用程序 *。
2. 单击 ... 对应于应用程序，然后单击 * 刷新保护 *。

监控作业

系统会为所有 Cloud Backup 操作创建作业。您可以监控在每个任务中执行的所有作业和所有子任务。

1. 单击 * 备份和还原 * > * 作业监控 *。

启动操作时，将显示一个窗口，指出作业已启动。您可以单击此链接来监控作业。

2. 单击主任务可查看每个子任务的子任务和状态。

配置 CA 证书

如果您拥有 CA 证书，则应手动将根 CA 证书复制到连接器计算机。

但是，如果您没有 CA 证书，则无需配置 CA 证书即可继续操作。

• 步骤 *

1. 将证书复制到可从 Docker 代理访问的卷。

```
▪ cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir
  sc_certs
▪ chmod 777 SC_certs
```

2. 将 RootCA 证书文件复制到连接器计算机上的上述文件夹。

```
cp <path on connector>/<filename>
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs
```

3. 将此 CRL 文件复制到可从 Docker 代理访问的卷。

```
▪ cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir
  SC_CRL
▪ chmod 777 SC_CRL
```

4. 将此 CRL 文件复制到连接器计算机上的上述文件夹。

```
cp <path on connector>/<filename>
/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_ll
```

5. 复制证书和 CRL 文件后，重新启动 Cloud Backup for Apps 服务。

```
▪ sUdo Docker exec cloudmanager_snapcenter sed -I s/skipSCCertValidation :
  true/skipSCCertValidation : false/g' /opt/netapp/cloudmanager-
  snapcenter-agent/config/config.yml
▪ s使用 Docker 重新启动 cloudmanager_snapcenter
```

还原应用程序数据

还原 Oracle 数据库

您只能将 Oracle 数据库还原到同一 SnapCenter 服务器主机，同一 SVM 或同一数据库主机。对于 RAC 数据库，数据将还原到创建备份的内部节点。

仅支持具有控制文件还原的完整数据库。如果归档日志不在 AFS 中，则应指定包含恢复所需归档日志的位置。

• 步骤 *

1. 在 Cloud Manager UI 中，单击 * 备份和还原 * > * 应用程序 *。
2. 在 * 筛选依据 * 字段中，选择筛选器 * 类型 *，然后从下拉列表中选择 * Oracle *。
3. 单击与要还原的数据库对应的 * 查看详细信息 *，然后单击 * 还原 *。
4. 在还原类型页面上，执行以下操作：
 - a. 如果要还原控制文件以及完整数据库，请选择 * 控制文件 *。
 - b. 选择 * 如果需要还原和恢复更改数据库状态 *，将数据库的状态更改为执行还原和恢复操作所需的状态。

数据库从高到低的各种状态包括打开，挂载，启动和关闭。如果数据库处于较高状态，但要执行还原操作，必须将此状态更改为较低状态，则必须选中此复选框。如果数据库处于较低的状态，但要执行还原操作，必须将其更改为较高的状态，则即使未选中此复选框，数据库状态也会自动更改。

如果数据库处于打开状态，并且要还原，数据库需要处于挂载状态，则只有选中此复选框后，数据库状态才会更改。

1. 在恢复范围页面上，执行以下操作：
 - a. 指定恢复范围。

如果您 ...	执行此操作 ...
希望恢复到上一个事务	选择 * 所有日志 *。
希望恢复到特定的系统更改编号（SCN）	选择 * 直到 SCN（系统更改编号） *。
希望恢复到特定数据和时间	选择 * 日期和时间 *。 必须指定数据库主机时区的日期和时间。
不希望恢复	选择 * 无恢复 *。
希望指定任何外部归档日志位置	如果归档日志不在 AFS 中，则应指定包含恢复所需归档日志的位置。

- b. 如果要在恢复后打开数据库，请选中此复选框。

在 RAC 设置中，恢复后仅打开用于恢复的 RAC 实例。

2. 查看详细信息并单击 * 还原 *。

还原 SQL Server 数据库

您可以将 SQL Server 数据库还原到同一主机或备用主机。不支持恢复日志备份和重新选择可用性组。

- 步骤 *

1. 在 Cloud Manager UI 中，单击 * 备份和还原 * > * 应用程序 *。
2. 在 * 筛选依据 * 字段中，选择筛选器 * 类型 *，然后从下拉列表中选择 * SQL *。
3. 单击 * 查看详细信息 * 以查看所有可用备份。
4. 选择备份并单击 * 还原 *。
5. 选择要还原数据库文件的位置。

选项	Description
将数据库还原到创建备份的同一主机	如果要将数据库还原到执行备份的同一 SQL 服务器，请选择此选项。
将数据库还原到备用主机	<p>如果要将数据库还原到执行备份的同一主机或不同主机中的其他 SQL 服务器，请选择此选项。</p> <p>选择主机名，提供数据库名称（可选），选择实例并指定还原路径。</p> <div>  <p>备用路径中提供的文件扩展名必须与原始数据库文件的文件扩展名相同。</p> </div> <p>如果 " 还原范围 " 页面中未显示 * 将数据库还原到备用主机 * 选项，请清除浏览器缓存。</p>

6. 在 * 还原前选项 * 页面上，选择以下选项之一：
 - 选择 * 在还原期间覆盖同名数据库 * 以还原同名数据库。
 - 选择 * 保留 SQL 数据库复制设置 * 以还原数据库并保留现有复制设置。
7. 在 * 还原后选项 * 页面上，要指定用于还原其他事务日志的数据库状态，请选择以下选项之一：
 - 如果要立即还原所有必要的备份，请选择 * 可操作，但不可用 *。

这是默认行为，通过回滚未提交的事务使数据库做好使用准备。在创建备份之前，您无法还原其他事务日志。

- 选择 * 不可操作，但可用 * 可使数据库不可操作，而不回滚未提交的事务。

可以还原其他事务日志。在恢复数据库之前，您无法使用它。

- 选择 * 只读模式和可用 * 可使数据库保持只读模式。

此选项将撤消未提交的事务，但会将撤消的操作保存在备用文件中，以便可以还原恢复效果。

如果启用了撤消目录选项，则会还原更多事务日志。如果事务日志的还原操作失败，则可以回滚所做的更改。SQL Server 文档包含详细信息。

1. 查看详细信息并单击 * 还原 *。

备份和还原虚拟机数据

保护虚拟机数据

您可以通过将适用于VMware vSphere的SnapCenter 插件与Cloud Manager集成来保护虚拟机上的数据。您可以将数据存储库备份到云、并将虚拟机轻松还原回适用于VMware vSphere的内部部署SnapCenter 插件。

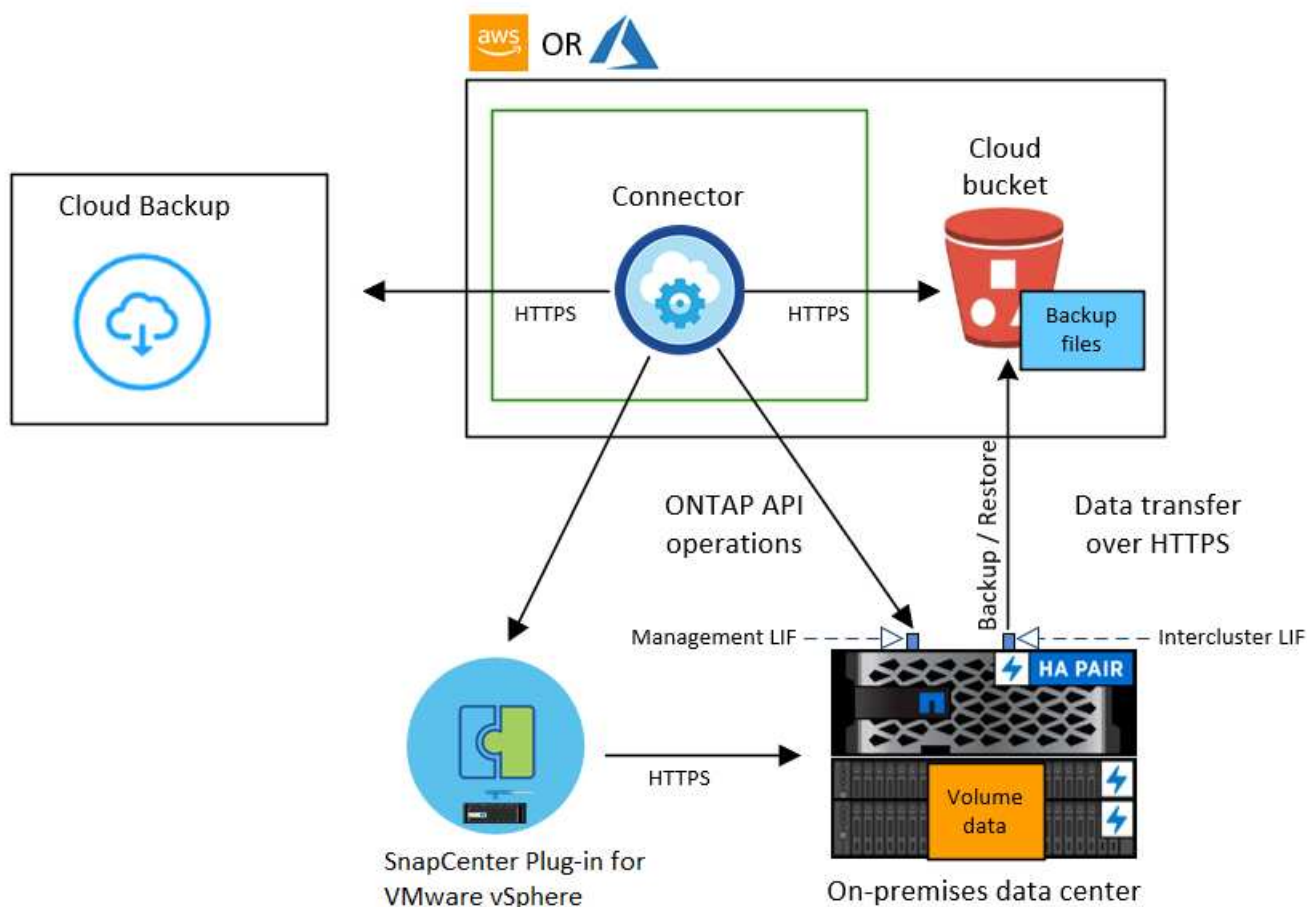
您可以将数据存储库备份到Amazon Web Services S3或Microsoft Azure Blob。

要求

在开始将数据存储库和虚拟机备份到云服务之前、请阅读以下要求、以确保您的配置受支持。

- 适用于VMware vSphere 4.6P1或更高版本的SnapCenter 插件
- ONTAP 9.8 或更高版本
- Cloud Manager 3.9或更高版本
- 适用于VMware vSphere 4.6P1的SnapCenter 插件应至少已创建一个备份。
- 适用于VMware vSphere的SnapCenter 插件中至少有一个每日、每周或每月策略、没有与Cloud Manager中适用于虚拟机的Cloud Backup策略的标签或标签。
- 对于预制策略、适用于VMware vSphere的SnapCenter 插件和云中的数据存储库的计划层应相同。
- 确保数据存储库中没有FlexGroup 卷、因为不支持备份和还原FlexGroup 卷。
- 请确保所有卷均未加密、因为不支持还原加密卷。
- 在所需资源组上禁用"近期"。如果为资源组启用了"近期"、则这些资源组的备份不能用于云数据保护、因此无法用于还原操作。
- 确保要还原虚拟机的目标数据存储库具有足够的空间来容纳所有虚拟机文件的副本、例如VMDK、VMx、VMSD等。
- 确保目标数据存储库不包含先前还原操作失败时格式为restore_xxx.xxxxxx_filename的陈旧虚拟机文件。在触发还原操作之前、您应删除陈旧的文件。

下图显示了每个组件以及需要在它们之间准备的连接：



保护策略

您应使用适用于虚拟机的Cloud Backup中定义的策略之一将数据存储库备份到云。



不支持自定义策略。

您可以通过单击Cloud Manager中的*备份和还原*>*虚拟机*>*策略*来查看默认策略。

Policy name	Label	保留值
1 年每日 LTR	每天	366.
5 年每日 LTR	每天	1830 年
7 年每周 LTR	每周	370
10 年每月 LTR	每月	120

将数据存储库备份到云

您可以通过将适用于VMware vSphere的SnapCenter 插件与Cloud Manager集成来将数据存储库备份到云。这将有助于VM管理员轻松快速地备份和归档数据以提高存储效率、并加快云过渡速度。



确保您已满足所有要求 ["要求"](#) 将数据存储库备份到云之前。

注册适用于VMware vSphere的SnapCenter 插件

您应在Cloud Manager中注册适用于VMware vSphere的SnapCenter 插件、以便在Cloud Manager中显示数据存储库和虚拟机。只有具有管理访问权限的用户才能注册适用于VMware vSphere的SnapCenter 插件。



您可以注册多个适用于VMware vSphere的SnapCenter 插件。但是、注册后、您将无法删除适用于VMware vSphere的SnapCenter 插件。

步骤

1. 在Cloud Manager UI中、单击*备份和还原*>*虚拟机*。
2. 从*设置*下拉列表中、单击*适用于VMware vSphere的SnapCenter 插件*。
3. 单击*注册适用于VMware vSphere的SnapCenter 插件*。
4. 指定以下详细信息：
 - a. 在适用于VMware vSphere的SnapCenter 插件字段中、指定适用于VMware vSphere的SnapCenter 插件的FQDN或IP地址。
 - b. 在端口字段中、指定运行适用于VMware vSphere的SnapCenter 插件的端口号。


您应确保此端口已打开、以便适用于VMware vSphere的SnapCenter 插件与适用于应用程序的云备份之间进行通信。
 - c. 在用户名和密码字段中、指定具有管理员角色的用户的凭据。
5. 单击 * 注册 *。
 - 完成后 *

单击*备份和还原>虚拟机*以查看使用适用于VMware vSphere的注册SnapCenter 插件符合保护条件的所有数据存储库和虚拟机。

备份数据存储库

您可以使用一个策略将一个或多个数据存储库同时备份到云中。只能为数据存储库分配默认策略。

步骤

1. 在Cloud Manager UI中、单击*备份和还原*>*虚拟机*。
2. 单击  对应于要备份的数据存储库、然后单击*激活备份*。
3. 添加工作环境。

配置您希望Cloud Manager发现的ONTAP 集群以备份数据存储库。为其中一个数据存储库添加工作环境后、可以对同一ONTAP 集群上的所有其他数据存储库重复使用该环境。

- a. 单击与SVM对应的*添加工作环境*。
 - b. 在添加工作环境向导中：
 - i. 指定 ONTAP 集群的 IP 地址。
 - ii. 指定ONTAP 集群用户的凭据。
 - c. 单击 * 添加工作环境 *。
4. 选择并配置云提供商。

配置 **Amazon Web Services**

- a. 指定 AWS 帐户。
- b. 在AWS访问密钥字段中、指定数据加密密钥。
- c. 在AWS机密密钥字段中、指定数据加密的密码。
- d. 选择要创建备份的区域。
- e. 指定已添加为工作环境的 ONTAP 集群的 IP 地址。

配置 **Microsoft Azure**

- a. 指定 Azure 订阅 ID 。
- b. 选择要创建备份的区域。
- c. 创建新资源组或使用现有资源组。
- d. 指定已添加为工作环境的 ONTAP 集群的 IP 地址。

5. 在分配策略页面中，选择策略并单击 * 下一步 *。
6. 查看详细信息并单击 * 激活备份 *。

管理虚拟机的保护

您可以在备份和还原数据之前查看策略、数据存储库和虚拟机。根据数据库，策略或资源组的更改，您可以从 Cloud Manager UI 刷新更新。

查看策略

您可以查看所有默认预制策略。对于其中每个策略、在查看详细信息时、将列出所有关联的Cloud Backup for Virtual Machine策略以及所有关联的虚拟机。

1. 单击*备份和还原>虚拟机*。
2. 从 * 设置 * 下拉列表中，单击 * 策略 *。
3. 单击与要查看其详细信息的策略对应的 * 查看详细信息 *。

此时将列出关联的Cloud Backup for Virtual Machine策略以及所有虚拟机。

查看数据存储库和虚拟机

此时将显示使用适用于VMware vSphere的注册SnapCenter 插件进行保护的数据存储库和虚拟机。

- 关于此任务 *
- 仅显示NFS数据存储库。
- 仅会显示已在适用于VMware vSphere的SnapCenter 插件中成功创建备份至少一个的数据存储库。

步骤

1. 在Cloud Manager UI中、单击*备份和还原*>*虚拟机*>*设置*>*适用于VMware vSphere的SnapCenter 插件*。
2. 单击要查看其数据存储库和虚拟机的适用于VMware vSphere的SnapCenter 插件。

编辑适用于VMware vSphere的SnapCenter 插件实例

您可以在Cloud Manager中编辑适用于VMware vSphere的SnapCenter 插件的详细信息

步骤

1. 在Cloud Manager UI中、单击*备份和还原*>*虚拟机*>*设置*>*适用于VMware vSphere的SnapCenter 插件*。
2. 单击并选择*编辑*
3. 根据需要修改详细信息
4. 单击 * 保存 *。

刷新保护状态

向数据库添加新卷时、或者如果策略或资源组发生更改、则应刷新保护。

1. 单击*备份和还原>虚拟机*。
2. 从*设置*下拉列表中、单击*适用于VMware vSphere的SnapCenter 插件*。
3. 单击 ... 对应于托管虚拟机的适用于VMware vSphere的SnapCenter 插件、然后单击*刷新*。

此时将发现新的更改。

4. 单击 ... 对应于数据存储库、然后单击*刷新保护*为所做的更改启用云保护。

监控作业

系统会为所有 Cloud Backup 操作创建作业。您可以监控在每个任务中执行的所有作业和所有子任务。

1. 单击*备份和还原>作业监控*。

启动操作时，将显示一个窗口，指出作业已启动。您可以单击此链接来监控作业。

2. 单击主任务可查看每个子任务的子任务和状态。

从云还原虚拟机

您可以将虚拟机从云还原到内部vCenter。备份将还原到创建备份的完全相同的位置。您不能将备份还原到任何其他备用位置。您可以从数据存储库或VM视图还原虚拟机。



您不能还原跨数据存储库的虚拟机。

确保您已满足所有要求 ["要求"](#) 从云还原虚拟机之前。

步骤

1. 在Cloud Manager中、单击*备份和还原*>*虚拟机*>*适用于VMware vSphere的SnapCenter 插件*、然后选择要还原其虚拟机的适用于VMware vSphere的SnapCenter 插件。



如果将源虚拟机移动到另一位置(vMotion)、并且用户从Cloud Manager触发该虚拟机的还原、则该虚拟机将还原到创建备份的原始源位置。

1. 从数据存储库还原：
 - a. 单击 ... 对应于要还原的数据存储库、然后单击*查看详细信息*。
 - b. 单击要还原的备份对应的*还原*。
 - c. 选择要从备份中还原的虚拟机、然后单击*下一步*。
 - d. 查看详细信息并单击 * 还原 *。
2. 要从虚拟机还原、请执行以下操作：
 - a. 单击 ... 对应于要还原的虚拟机、然后单击*还原*。
 - b. 选择要用于还原虚拟机的备份、然后单击*下一步*。
 - c. 查看详细信息并单击 * 还原 *。

虚拟机将还原到创建备份的同一位置。

Cloud Backup API

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

Cloud Backup Service 中定义了八类端点：

- backup
- 目录
- 云
- 作业
- license
- 还原
- 单个文件级还原(SFR)
- 工作环境

入门

要开始使用Cloud Backup API、您需要获取用户令牌、Cloud Central帐户ID和Cloud Connector ID。

在进行API调用时、您将在Authorization标头中添加用户令牌、并在x-agent-id标头中添加Cloud Connector ID。您应在API中使用Cloud Central帐户ID。

步骤

1. 从 NetApp Cloud Central 获取用户令牌。

请确保从以下链接生成刷新令牌：<https://services.cloud.netapp.com/refresh-token/>。刷新令牌是一个字母数字字符串、用于生成用户令牌。

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
  "grant_type": "refresh_token",
  "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
  "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

2. 获取您的NetApp Cloud Central帐户ID。

```
GET 'https://cloudmanager.cloud.netapp.com/tenancy/account' -H
'authority: cloudmanager.cloud.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.....
```

此API将返回如下响应。您可以通过解析来自*。的输出来检索帐户ID。。 * accountPublicId]*。

```
[{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}].....
```

3. 获取包含Cloud Manager Connector ID的x-agent-id。

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
-H 'authority: api.services.cloud.netapp.com' \
-H 'accept: application/json' \
-H 'accept-language: en-GB,en;q=0.9' \
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5.....
```

此API将返回如下响应。您可以通过解析*例.[0].[代理].[agentId]*中的输出来检索代理ID。

```
{ "occms": [{"account": "account-
OOnAR4ZS", "accountName": "cbs", "occm": "imEdsEW4HyYTFbt8ZcNKTkDF05jMIe6Z",
"agentId": "imEdsEW4HyYTFbt8ZcNKTkDF05jMIe6Z", "status": "ready", "occmName"
: "cbsgcpdevcntsg-
asia", "primaryCallbackUri": "http://34.93.197.21", "manualOverrideUri": [],
"automaticCallbackUri": ["http://34.93.197.21", "http://34.93.197.21/occmui", "https://34.93.197.21", "https://34.93.197.21/occmui", "http://10.138
.0.16", "http://10.138.0.16/occmui", "https://10.138.0.16", "https://10.138
.0.16/occmui", "http://localhost", "http://localhost/occmui", "http://local
host:1337", "http://localhost:1337/occmui", "https://localhost", "https://l
ocalhost/occmui", "https://localhost:1337", "https://localhost:1337/occmui
"], "createDate": "1652120369286", "agent": {"useDockerInfra": true, "network"
: "default", "name": "cbsgcpdevcntsg-
asia", "agentId": "imEdsEW4HyYTFbt8ZcNKTkDF05jMIe6Zclients", "provider": "gc
p", "systemId": "a3aa3578-bfee-4d16-9e10-
```

使用API的示例

以下示例显示了一个API调用、用于在Azure云中的East-US-2区域使用一个新策略激活工作环境备份、该策略将每天、每小时和每周标签设置为180天后进行归档。请注意、此操作仅在工作环境中启用备份、但不会备份任何卷。如果选择"auto-backup-enabled": true、则系统中已存在的任何卷都会进行备份、并添加未来的卷。

您会看到、我们使用的是Cloud Central帐户ID "account-DpTfcxN3"、Cloud Manager Connector ID "iZwFfeVCzjWnzGlw8RgD0QQNANZvpP7Icliers"和用户令牌"Bearer

JhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ikp5cXlPVFUzUWpZek1E...y6nyhBjwk

```
curl --location --request POST
'https://cloudmanager.cloud.netapp.com/account/account-
DpTfcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFfeVCzjWnzGlw8RgD0QQNANZvpP7Icliers' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ikp5cXlPVFUzUWpZek1E...y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
  "provider": "AZURE",
  "backup-policy": {
    "archive-after-days": 180,
    "rule": [
      {
        "label": "hourly",
        "retention": "2"
      },
      {
        "label": "daily",
        "retention": "30"
      },
      {
        "label": "weekly",
        "retention": "52"
      }
    ]
  },
  "ip-space": "Default",
  "region": "eastus2",
  "azure": {
    "resource-group": "rn-test-backup-rg",
    "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
  }
}'
```


response是一个作业ID、您可以监控该ID。

```
{
  "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}
```

监控响应。

```
curl --location --request GET
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSx1PVFUzUWpZek1E...hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

响应。

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

监控、直到"状态"为"已完成"为止。

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

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 Backup API 的文档、请参见 <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>。

参考

AWS S3 归档存储类和还原检索时间

Cloud Backup 支持两个 S3 归档存储类以及大多数地区。

支持 Cloud Backup 的 S3 归档存储类

首次创建备份文件时，这些备份文件会存储在 S3 *Standard* 存储中。此层已针对存储不常访问的数据进行了优化，但也允许您立即访问。30 天后，备份将过渡到 S3 *Standard-Infrequent Access* 存储类以节省成本。

如果源集群运行的是 ONTAP 9.10.1 或更高版本，您可以选择在一定天数（通常超过 30 天）后将备份分层到 S3 *Glacier* 或 S3 *Glacier Deep Archive* 存储，以便进一步优化成本。这些层中的数据无法在需要时立即访问，并且需要较高的检索成本，因此您需要考虑从这些归档备份文件还原数据的频率。请参见关于一节 [从归档存储还原数据](#)。

请注意，使用此类生命周期规则配置 Cloud Backup 时，在 AWS 帐户中设置存储分段时，不能配置任何生命周期规则。

["了解 S3 存储课程"](#)。

从归档存储还原数据

虽然将旧备份文件存储在归档存储中的成本要比标准存储或标准 IA 存储低得多，但从归档存储中的备份文件访问数据以执行还原操作将需要较长的时间，并需要较多的成本。

从 Amazon S3 Glacier 和 Amazon S3 Glacier Deep Archive 还原数据的成本是多少？

在从 Amazon S3 Glacier 检索数据时，您可以选择 3 个恢复优先级，在从 Amazon S3 Glacier 深度归档检索数据时，可以选择 2 个恢复优先级。S3 Glacier 深度归档成本低于 S3 Glacier：

归档层	还原优先级和成本		
	* 高 *	* 标准 *	* 低 *
* S3 Glacier*	检索速度最快，成本最高	检索速度较慢，成本较低	检索速度最慢，成本最低
* S3 Glacier 深度归档 *		检索速度更快，成本更高	检索速度较慢，成本最低

每种方法的每 GB 检索费用和每次请求费用不同。有关按 AWS 地区列出的 S3 Glacier 详细定价，请访问 ["Amazon S3 定价页面"](#)。

还原在 Amazon S3 Glacier 中归档的对象需要多长时间？

总还原时间由两部分组成：

- * 检索时间 *：从归档中检索备份文件并将其置于标准存储中的时间。这有时称为 "再融合 "时间。检索时间因您选择的还原优先级而异。

归档层	还原优先级和检索时间		
	* 高 *	* 标准 *	* 低 *

归档层	还原优先级和检索时间		
* S3 Glacier*	3-5 分钟	3-5 小时	5-12 小时
* S3 Glacier 深度归档 *		12 小时	48 小时

- * 还原时间 *：从标准存储中的备份文件还原数据的时间。此时间与直接从标准存储执行的典型还原操作并无不同，因为此时不使用归档层。

有关 Amazon S3 Glacier 和 S3 Glacier 深度归档检索选项的详细信息，请参见 ["有关这些存储类的 Amazon 常见问题解答"](#)。

Azure 归档层和还原检索时间

Cloud Backup 支持一个 Azure 归档访问层以及大多数地区。

支持 Cloud Backup 的 Azure Blob 访问层

首次创建备份文件时，这些备份文件将存储在 *cool* 访问层中。此层经过优化，可用于存储不常访问的数据；但在需要时，可以立即访问。

如果源集群运行的是 ONTAP 9.10.1 或更高版本，您可以选择在一定天数（通常超过 30 天）后将备份从 *cool* 分层到 *Azure Archive* 存储，以便进一步优化成本。此层中的数据无法在需要时立即访问，因此需要较高的检索成本，因此您需要考虑从这些归档备份文件还原数据的频率。请参见下一节 [从归档存储还原数据](#)。

请注意，使用此类型的生命周期规则配置 Cloud Backup 时，在 Azure 帐户中设置容器时，不能配置任何生命周期规则。

["了解 Azure Blob 访问层"](#)。

从归档存储还原数据

虽然将旧备份文件存储在归档存储中的成本要比冷存储低得多，但从 Azure 归档中的备份文件访问数据以执行还原操作将需要较长的时间，并且成本也会更高。

从 **Azure Archive** 还原数据的成本是多少？

从 Azure Archive 检索数据时，您可以选择两个还原优先级：

- * 高 *：检索速度最快，成本更高
- * 标准 *：检索速度较慢，成本较低

每种方法的每 GB 检索费用和每次请求费用不同。有关按 Azure 地区列出的 Azure Archive 详细定价，请访问 ["Azure 定价页面"](#)。

还原在 **Azure Archive** 中归档的数据需要多长时间？

还原时间由两部分组成：

- * 检索时间 *：从 Azure Archive 检索已归档备份文件并将其置于冷存储中的时间。这有时称为 "再融合" 时间。根据您选择的还原优先级，检索时间会有所不同：
 - * 高 *：< 1 小时

- * 标准 * : < 15 小时

- * 还原时间 * : 从冷存储中的备份文件还原数据的时间。这一时间与直接从冷存储执行的典型还原操作并无不同, 因为此时不使用归档层。

有关 Azure 归档检索选项的详细信息, 请参见 ["此 Azure 常见问题解答"](#)。

知识和支持

注册以获得支持

在向 NetApp 技术支持创建支持案例之前，您需要先将 NetApp 支持站点帐户添加到 Cloud Manager 中，然后注册获取支持。

添加 NSS 帐户

通过支持信息板，您可以从一个位置添加和管理所有 NetApp 支持站点帐户。

步骤

1. 如果您还没有 NetApp 支持站点帐户，["注册一个"](#)。
2. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 * 支持 *。



3. 单击 * NSS 管理 > 添加 NSS 帐户 *。
4. 出现提示时，单击 * 继续 * 以重定向到 Microsoft 登录页面。

NetApp 使用 Microsoft Azure Active Directory 作为身份提供程序来提供特定于支持和许可的身份验证服务。

5. 在登录页面上，提供 NetApp 支持站点注册的电子邮件地址和密码以执行身份验证过程。

此操作可使 Cloud Manager 使用您的 NSS 帐户。

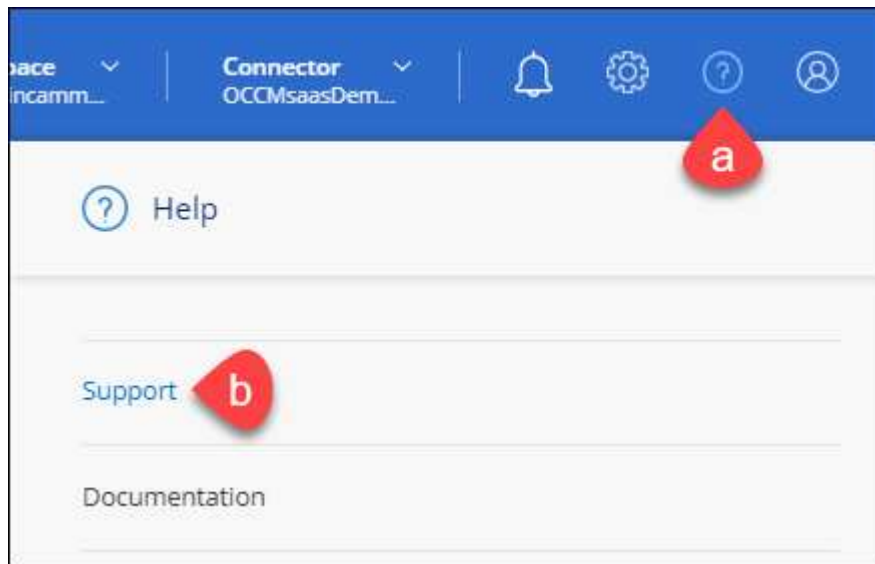
请注意，此帐户必须是客户级别的帐户（而不是来宾或临时帐户）。

注册您的帐户以获得支持

支持注册可从 Cloud Manager 的支持信息板中获取。

步骤

1. 在 Cloud Manager 控制台右上角，单击帮助图标，然后选择 * 支持 *。



2. 在 * 资源 * 选项卡中，单击 * 注册支持 *。
3. 选择要注册的 NSS 凭据，然后单击 * 注册 *。

获取帮助

NetApp 通过多种方式为 Cloud Manager 及其云服务提供支持。全天候提供丰富的免费自助支持选项，例如知识库（KB）文章和社区论坛。您的支持注册包括通过 Web 服务单提供的远程技术支持。

自助支持

这些选项每周 7 天，每天 24 小时免费提供：

- ["知识库"](#)

通过 Cloud Manager 知识库搜索，查找有助于解决问题的文章。

- ["社区"](#)

加入 Cloud Manager 社区，关注正在进行的讨论或创建新的讨论。

- 文档。

您当前正在查看的 Cloud Manager 文档。

- [mailto: ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)（反馈电子邮件）

我们非常重视您的反馈意见。提交反馈以帮助我们改进 Cloud Manager。

NetApp 支持

除了上述自助支持选项之外，您还可以在激活支持后与 NetApp 支持工程师合作解决任何问题。

步骤

1. 在 Cloud Manager 中，单击 * 帮助 > 支持 *。
2. 在 "Technical Support" 下选择一个可用选项：
 - a. 单击 * 致电我们 * 可查找 NetApp 技术支持的电话号码。
 - b. 单击 * 打开问题描述 *，选择一个选项，然后单击 * 发送 *。

NetApp 代表将审核您的案例，并尽快与您联系。

法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

<http://www.netapp.com/us/legal/copyright.aspx>

商标

NetApp、NetApp 徽标和 NetApp 商标页面上列出的标记是 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。

<http://www.netapp.com/us/legal/netapptmlist.aspx>

专利

有关 NetApp 拥有的专利的最新列表，请访问：

<https://www.netapp.com/us/media/patents-page.pdf>

隐私政策

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

- "有关 Cloud Manager 3.9 的注意事项"
- "Cloud Backup 注意事项"
- "单文件还原注意事项"

版权信息

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

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

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

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

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

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

商标信息

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