使用NetApp Backup and Recovery

NetApp Backup and Recovery

NetApp
February 11, 2026

目录

使用NetApp Backup and Recovery

在NetApp Backup and Recovery仪表板上查看保护健康状况

监控工作负载的健康状况可确保您了解工作负载保护的问题并可以采取措施解决这些问题。在NetApp Backup and Recovery仪表板上查看备份和恢复的状态。您可以查看系统摘要、保护摘要、作业摘要、恢复摘要等。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员、备份和恢复恢复管理员、备份和恢复克隆管理员或备份和恢复查看器角色。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Console菜单中，选择 保护 > 备份和恢复。
2. 选择一个工作负载图块（例如，Microsoft SQL Server）。
3. 从备份和恢复菜单中，选择*仪表板*。

   您可以查看以下类型的信息：

   - 发现的主机或虚拟机的数量
   - 发现的 Kubernetes 集群数量
   - 对象存储上的备份目标数量
   - vCenter 数量
   - ONTAP中的存储集群数量

查看保护摘要

查看保护摘要中的以下信息：

- 受保护和不受保护的数据库、虚拟机和数据存储区的总数。

  受保护的数据库是已分配备份策略的数据库。不受保护的数据库是未分配备份策略的数据库。

- 成功、出现警告或失败的备份次数。
- 备份服务发现的总容量以及受保护的容量和不受保护的容量。将鼠标悬停在“i”图标上即可查看详细信息。

查看职位摘要

在作业摘要中查看已完成、正在运行或失败的作业总数。

步骤

1. 对于每个作业分布，更改过滤器以根据天数显示失败、正在运行和完成的摘要，例如过去 30 天、过去 7 天、过去 24 小时或过去 1 年。

2. 通过选择“查看作业监控”来查看失败、正在运行和已完成作业的详细信息。

查看还原摘要

查看还原摘要中的以下信息：

- 执行的恢复作业总数
- 已恢复的总容量
- 在本地、辅助和对象存储上执行的恢复作业的数量。将鼠标悬停在图表上即可查看详细信息。

创建和管理策略来管理NetApp Backup and Recovery中的备份

在NetApp Backup and Recovery中，创建您自己的策略来控制备份频率、备份时间以及保留的备份文件数量。

其中一些选项和配置部分并不适用于所有工作负载。

如果从SnapCenter导入资源，您可能会发现SnapCenter中使用的策略与NetApp Backup and Recovery中使用的策略存在一些差异。看"SnapCenter与NetApp Backup and Recovery之间的策略差异"。

您可以实现以下与政策相关的目标：

- 创建本地快照策略
- 创建复制到辅助存储的策略
- 为对象存储设置创建策略
- 配置高级策略设置
- 编辑策略（不适用于 VMware 预览工作负载）
- 删除策略

查看政策

1. 从NetApp Backup and Recovery菜单中，选择 策略。
2. 查看这些政策详情。
    - 工作负载：示例包括 Microsoft SQL Server、卷、VMware、KVM、Hyper-V、Oracle Database 或 Kubernetes。
    - 备份类型：例如完整备份和日志备份。
    - 架构：示例包括本地快照、扇出、级联、磁盘到磁盘和磁盘到对象存储。
    - 受保护的资源：显示该工作负载的总资源中有多少资源受到保护。
    - 勒索软件保护：显示策略是否包括本地快照上的快照锁定、二级存储上的快照锁定或对象存储上的 DataLock 锁定。

创建策略

您可以创建策略来管理本地快照、复制到二级存储以及备份到对象存储。3-2-1 策略的一部分包括创建主存储系统上的实例、数据库、应用程序或虚拟机的快照。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

开始之前

如果您计划复制到二级存储并希望在本地快照或远程ONTAP二级存储上使用快照锁定，则首先需要在集群级别初始化ONTAP合规时钟。这是在策略中启用快照锁定的要求。

有关如何执行此操作的说明，请参阅 "在ONTAP中初始化合规性时钟"。

有关快照锁定的一般信息，请参阅 "ONTAP中的快照锁定"。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 策略。
2. 在“策略”页面中，选择“创建新策略”。
3. 在“策略”页面中，提供以下信息。

    - *详细信息*部分：
        - 工作负载类型：选择将使用该策略的工作负载。
        - 输入策略名称。

            要查看要避免的角色列表，请参阅悬停提示。

        - 从*代理*列表中选择一个控制台代理。
    - *备份架构*部分：选择向下箭头并选择备份的数据流，例如 3-2-1 扇出、3-2-1 级联或磁盘到磁盘。
        - **3-2-1 fanout**：主存储（磁盘）到辅助存储（磁盘）到云（对象存储）。在不同的存储系统中创建多个数据副本，例如 ONTAP 到 ONTAP 和 ONTAP 到对象存储配置。这可以是云超大规模对象存储或私有对象存储。这些配置有助于实现最佳的数据保护和灾难恢复。

            此选项不适用于Amazon FSx for NetApp ONTAP。

            对于 VMware 工作负载，这会在主数据存储或虚拟机上配置本地快照，并从主磁盘存储复制到辅助磁盘存储以及从主存储复制到云对象存储。

        - **3-2-1** 级联：（不适用于 Kubernetes 工作负载）主存储（磁盘）到辅助存储（磁盘）以及主存储（磁盘）到云存储（对象存储）。这可以是云超大规模对象存储或私有对象存储 - StorageGRID。这会在多个系统之间创建数据复制链，以确保冗余和可靠性。

            此选项不适用于Amazon FSx for NetApp ONTAP。

        对于 VMware 工作负载，这会在主存储上的数据存储区或虚拟机上配置本地快照，以及从主磁盘存储到辅助磁盘存储再到云对象存储的级联。

- 磁盘到磁盘：（不适用于 Kubernetes 工作负载）主存储（磁盘）到辅助存储（磁盘）。ONTAP到ONTAP数据保护策略在两个ONTAP系统之间复制数据，以确保高可用性和灾难恢复。这通常是使用SnapMirror实现的，它支持同步和异步复制。此方法可确保您的数据持续更新并可在多个位置使用，从而提供强大的数据丢失保护。

  对于 VMware 工作负载，这会在主存储系统上的数据存储或 VMware 上配置本地快照，然后将数据从主磁盘存储系统复制到辅助磁盘存储系统。

- 磁盘到对象存储：主存储（磁盘）到云（对象存储）。这会将数据从ONTAP系统复制到对象存储系统，例如 AWS S3、Azure Blob Storage 或StorageGRID。这通常是使用SnapMirror Cloud 实现的，它通过在初始基线传输后仅传输更改的数据块来提供永久增量备份。这可以是云超大规模对象存储或私有对象存储 - StorageGRID。该方法非常适合长期数据保留和存档，为数据保护提供了经济高效且可扩展的解决方案。

  对于 VMWare 工作负载，这会在主数据存储或虚拟机上配置本地快照，并从主磁盘存储到云对象存储进行复制。

- 磁盘到磁盘扇出：（不适用于 Kubernetes 工作负载）主存储（磁盘）到辅助存储（磁盘）以及主存储（磁盘）到辅助存储（磁盘）。

  您可以为磁盘到磁盘扇出选项配置多个辅助设置。

对于 VMware 工作负载，这会将主磁盘存储配置为辅助磁盘存储，并将主磁盘存储复制到辅助磁盘存储。

- 本地快照：所选卷上的本地快照（Microsoft SQL Server）。本地快照是数据保护策略的关键组成部分，可以捕获特定时间点的数据状态。这将创建工作负载正在运行的生产卷的只读、时间点副本。快照占用的存储空间极小，并且产生的性能开销可以忽略不计，因为它仅记录自上次快照以来文件的更改。您可以使用本地快照来恢复数据丢失或损坏，以及为灾难恢复目的创建备份。

  对于 VMware 工作负载，这会在主存储系统上的数据存储或虚拟机上配置本地快照。

创建本地快照策略

提供本地快照的信息。

- 选择“添加计划”选项来选择快照计划或计划。您最多可以有 5 个时间表。
- 快照频率：选择每小时、每天、每周、每月或每年的频率。 Kubernetes 工作负载没有年度频率。
- 快照保留：输入要保留的快照数量。
- 启用日志备份：（仅适用于 Microsoft SQL Server 工作负载和 Oracle 数据库工作负载。）启用此选项可备份日志并设置日志备份的频率和保留。为此，您必须已经配置了日志备份。看"配置日志目录"。
  - 备份后修剪存档日志：（仅限 Oracle 数据库工作负载）如果启用了日志备份，您可以选择启用此功能来限制备份和恢复保留 Oracle 存档日志的时间。您可以选择保留期限以及备份和恢复应删除存档日志的位置。
- 提供商：（仅限 Kubernetes 工作负载）选择托管 Kubernetes 应用程序资源的存储提供商。

为辅助设置创建策略（复制到辅助存储）

提供复制到辅助存储的信息。本地快照设置的计划信息会显示在辅助设置中。这些设置不适用于 Kubernetes 工作负载。

- 备份：选择每小时、每天、每周、每月或每年的频率。
- 备份目标：选择二级存储上用于备份的目标系统。
- 保留：输入要保留的快照数量。
- 启用快照锁定：选择是否要启用防篡改快照。
- 快照锁定期限：输入您想要锁定快照的天数、月数或年数。
- 转入中学：
  - 默认情况下，选择 * ONTAP传输计划 - 内联* 选项，这表示快照会立即传输到二级存储系统。您不需要安排备份。
  - 其他选项：如果您选择延期转账，则转账不是立即进行的，您可以设置时间表。
- * SnapMirror和SnapVault SMAS 二级关系*：对 SQL Server 工作负载使用SnapMirror和SnapVault SMAS 二级关系。

为对象存储设置创建策略

提供备份到对象存储的信息。这些设置被称为 Kubernetes 工作负载的“备份设置”。

出现的字段根据所选的提供商和架构而有所不同。

为 **AWS** 对象存储创建策略

在这些字段中输入信息：

- 提供商：选择*AWS*。
- **AWS** 账户：选择 AWS 账户。
- 备份目标：选择已注册的 S3 对象存储目标。确保目标在您的备份环境中可访问。
- **IPspace**：选择用于备份操作的 IP 空间。如果您有多个 IP 空间并想要控制哪一个用于备份，这将非常有用。
- 计划设置：选择为本地快照设置的计划。您可以删除计划，但不能添加计划，因为计划是根据本地快照计划设置的。
- 保留副本：输入要保留的快照数量。
- 运行于：选择ONTAP传输计划将数据备份到对象存储。
- 将备份从对象存储分层到档案存储：如果您选择将备份分层到档案存储（例如，AWS Glacier），请选择层选项和存档天数。
- 启用完整性扫描：（不适用于 Kubernetes 工作负载）选择是否要在对象存储上启用完整性扫描（快照锁定）。这可确保备份有效并可成功恢复。完整性扫描频率默认设置为 7 天。为了保护您的备份不被修改或删除，请选择*完整性扫描*选项。扫描仅发生在最新的快照上。您可以对最新快照启用或禁用完整性扫描。

为 **Microsoft Azure** 对象存储创建策略

在这些字段中输入信息：

- 提供商：选择*Azure*。
- **Azure** 订阅：从发现的 Azure 订阅中选择。

- **Azure** 资源组：从发现的资源组中选择 Azure 资源组。
- 备份目标：选择已注册的对象存储目标。确保目标在您的备份环境中可访问。
- **IPspace**：选择用于备份操作的 IP 空间。如果您有多个 IP 空间并想要控制哪一个用于备份，这将非常有用。
- 计划设置：选择为本地快照设置的计划。您可以删除计划，但不能添加计划，因为计划是根据本地快照计划设置的。
- 保留副本：输入要保留的快照数量。
- 运行于：选择ONTAP传输计划将数据备份到对象存储。
- 将备份从对象存储分层到档案存储：如果您选择将备份分层到档案存储，请选择层选项和存档天数。
- 启用完整性扫描：（不适用于 Kubernetes 工作负载）选择是否要在对象存储上启用完整性扫描（快照锁定）。这可确保备份有效并可成功恢复。完整性扫描频率默认设置为 7 天。为了保护您的备份不被修改或删除，请选择*完整性扫描*选项。扫描仅发生在最新的快照上。您可以对最新快照启用或禁用完整性扫描。

为**StorageGRID**对象存储创建策略

在这些字段中输入信息：

- 提供商：选择* StorageGRID*。
- * StorageGRID凭证*：从发现的凭证中选择StorageGRID凭证。这些凭据用于访问StorageGRID对象存储系统，并在“设置”选项中输入。
- 备份目标：选择已注册的 S3 对象存储目标。确保目标在您的备份环境中可访问。
- **IPspace**：选择用于备份操作的 IP 空间。如果您有多个 IP 空间并想要控制哪一个用于备份，这将非常有用。
- 计划设置：选择为本地快照设置的计划。您可以删除计划，但不能添加计划，因为计划是根据本地快照计划设置的。
- 保留副本：输入每个频率保留的快照数量。
- 对象存储的传输计划：（不适用于 Kubernetes 工作负载）选择ONTAP传输计划将数据备份到对象存储。
- 启用完整性扫描：（不适用于 Kubernetes 工作负载）选择是否要在对象存储上启用完整性扫描（快照锁定）。这可确保备份有效并可成功恢复。完整性扫描频率默认设置为 7 天。为了保护您的备份不被修改或删除，请选择*完整性扫描*选项。扫描仅发生在最新的快照上。您可以对最新快照启用或禁用完整性扫描。
- 将备份从对象存储分层到档案存储：（不适用于 Kubernetes 工作负载）如果您选择将备份分层到档案存储，请选择层选项和存档天数。

在策略中配置高级设置

您也可以选择在策略中配置高级设置。这些设置适用于所有备份架构，包括本地快照、复制到二级存储以及备份到对象存储。这些设置不适用于 Kubernetes 工作负载。可用的高级设置将根据您在页面顶部选择的工作负载而有所不同，因此此处描述的高级设置可能不适用于所有工作负载。为 Kubernetes 工作负载配置策略时，高级设置不可用。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 策略。
2. 在“策略”页面中，选择“创建新策略”。

3. 在“策略 > 高级”设置部分中，选择“选择高级操作”菜单，从高级设置列表中进行选择。
4. 启用您想要查看或更改的任何设置，然后选择*接受*。
5. 提供以下信息：
   - 仅复制备份：（仅适用于 Microsoft SQL Server 工作负载）如果您需要使用其他备份应用程序备份资源，请选择仅复制备份（一种 Microsoft SQL Server 备份）。
   - 可用性组设置：（仅适用于 Microsoft SQL Server 工作负载）选择首选备份副本或指定特定副本。如果您有一个 SQL Server 可用性组并且想要控制用于备份的副本，则此设置很有用。
   - 最大传输速率：若不设置带宽使用限制，请选择*无限制*。如果要限制传输速率，请选择*限制*，并选择分配给将备份上传到对象存储的 1 到 1,000 Mbps 之间的网络带宽。默认情况下， ONTAP可以使用无限量的带宽将备份数据从系统中的卷传输到对象存储。如果您注意到备份流量影响了正常的用户工作负载，请考虑减少传输过程中使用的网络带宽量。
   - 备份重试：（不适用于 VMware 工作负载）要在发生故障或中断时重试作业，请选择*启用故障期间的作业重试*。输入快照和备份作业重试的最大次数以及重试时间间隔。重新计票数必须少于 10。如果您想要确保在发生故障或中断时重试备份作业，此设置很有用。

     如果快照频率设置为 1 小时，则最大延迟以及重试次数不应超过 45 分钟。

   - 启用虚拟机一致性快照：选择是否启用虚拟机一致性快照。这样可以确保新创建的快照与创建快照时虚拟机的状态保持一致。这有助于确保备份能够成功恢复，并且数据处于一致状态。这不适用于现有快照。
   - 勒索软件扫描：选择是否要在每个存储桶上启用勒索软件扫描。这需要对对象存储进行 DataLock 锁定。输入扫描频率（以天为单位）。此选项适用于 AWS 和 Microsoft Azure 对象存储。请注意，此选项可能会产生额外费用，具体取决于云提供商。
   - 备份验证：（不适用于 VMware 工作负载）选择是否要启用备份验证以及是否立即或稍后进行。此功能可确保备份有效并可成功恢复。我们建议您启用此选项以确保备份的完整性。默认情况下，如果配置了辅助存储，则备份验证从辅助存储运行。如果未配置辅助存储，则备份验证从主存储运行。

     此外，配置以下选项：

     - 每日、每周、*每月*或*每年*验证：如果您选择*稍后*作为备份验证，请选择备份验证的频率。这可确保定期检查备份的完整性并可成功恢复。
     - 备份标签：输入备份的标签。此标签用于识别系统中的备份，并可用于跟踪和管理备份。
     - 数据库一致性检查：（不适用于 VMware 工作负载）选择是否要启用数据库一致性检查。此选项可确保数据库在备份之前处于一致状态，这对于确保数据完整性至关重要。
     - 验证日志备份：（不适用于 VMware 工作负载）选择是否要验证日志备份。选择验证服务器。如果您选择磁盘到磁盘或 3-2-1，还请选择验证存储位置。此选项可确保日志备份有效并可成功恢复，这对于维护数据库的完整性非常重要。
   - 网络：选择用于备份操作的网络接口。如果您有多个网络接口并想要控制哪一个用于备份，这将非常有用。
     - **IPspace**：选择用于备份操作的 IP 空间。如果您有多个 IP 空间并想要控制哪一个用于备份，这将非常有用。
     - 私有端点配置：如果您使用私有端点进行对象存储，请选择用于备份操作的私有端点配置。如果您想确保备份通过专用网络连接安全传输，这将非常有用。
   - 通知：选择是否要为备份操作启用电子邮件通知。如果您希望在备份操作开始、完成或失败时收到通知，这将非常有用。

- 独立磁盘：（仅适用于 VMware 工作负载）选中此项可将任何包含临时数据的独立磁盘数据存储包含在备份中。独立磁盘是未包含在 VMware 快照中的 VM 磁盘。
- * SnapMirror卷和快照格式*：（可选）在管理 Microsoft SQL Server 工作负载备份的策略中输入您自己的快照名称。输入格式和自定义文本。如果您选择备份到二级存储，您还可以添加SnapMirror卷前缀和后缀。

编辑策略

您可以编辑备份架构、备份频率、保留策略和策略的其他设置。

您可以在编辑策略时添加另一个保护级别，但不能删除保护级别。例如，如果策略仅保护本地快照，则可以将复制添加到辅助存储或将备份添加到对象存储。如果您有本地快照和复制，则可以添加对象存储。但是，如果您有本地快照、复制和对象存储，则不能删除其中一个级别。

如果您正在编辑备份到对象存储的策略，则可以启用存档。

如果您从SnapCenter导入资源，您可能会发现SnapCenter中使用的策略与NetApp Backup and Recovery中使用的策略存在一些差异。看"SnapCenter与NetApp Backup and Recovery之间的策略差异"。

所需的**NetApp Console**角色

备份和恢复超级管理员。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 在NetApp Console中，转到 保护 > 备份和恢复。
2. 选择*政策*选项。
3. 选择要编辑的策略。
4. 选择*操作*•••图标，然后选择*编辑*。

删除策略

如果您不再需要某个策略，则可以将其删除。

您不能删除与工作负载关联的策略。

步骤

1. 在控制台中，转到*保护*>*备份和恢复*。
2. 选择*政策*选项。
3. 选择要删除的策略。
4. 选择*操作*•••图标，然后选择*删除*。
5. 确认操作，然后选择*删除*。

保护ONTAP卷工作负载

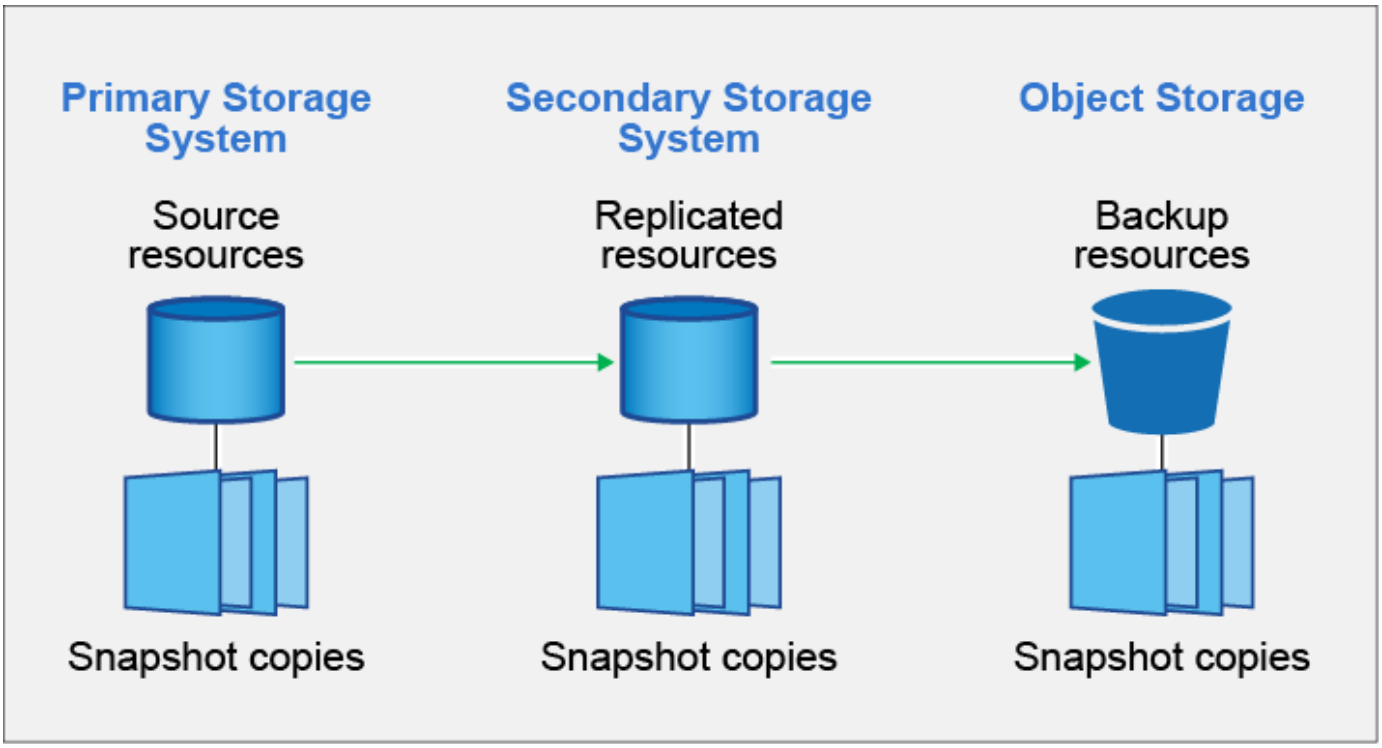
使用NetApp Backup and Recovery保护您的ONTAP卷数据

NetApp Backup and Recovery提供备份和恢复功能，用于保护和长期存档您的ONTAP卷数据。您可以实施 3-2-1 策略，即在 2 个不同的存储系统上保留 3 个源数据副本，并在云中保留 1 个副本。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

激活后，备份和恢复会创建块级、增量永久备份，这些备份存储在另一个ONTAP集群和云中的对象存储中。除了源卷之外，您还将拥有：

- 源系统上卷的快照
- 不同存储系统上的复制卷
- 对象存储中的卷备份



NetApp Backup and Recovery利用 NetApp 的SnapMirror数据复制技术，通过创建快照并将其传输到备份位置，确保所有备份完全同步。

3-2-1 方法的优点包括：

- 多个数据副本可防止内部和外部网络安全威胁。
- 如果一种媒体发生故障，使用不同类型的媒体可以帮助您恢复。
- 您可以从现场副本快速恢复，如果现场副本受到损害，则可以使用异地副本。

必要时，您可以将整个卷、文件夹或一个或多个文件从任何备份副本恢复到相同或不同的系统。

功能

复制功能：

- 在ONTAP存储系统之间复制数据以支持备份和灾难恢复。
- 通过高可用性确保您的 DR 环境的可靠性。
- 通过两个系统之间的预共享密钥 (PSK) 设置的本机ONTAP动态加密。
- 复制的数据是不可变的，直到您使其可写并可供使用为止。
- 如果传输失败，复制可以自我修复。
- 与……相比 "NetApp Replication"， NetApp Backup and Recovery中的复制包括以下功能：
  - 一次将多个FlexVol卷复制到辅助系统。
  - 使用 UI 将复制的卷还原到源系统或其他系统。

看"ONTAP卷的复制限制"了解NetApp Backup and Recovery for ONTAP卷不可用的复制功能列表。

备份到对象功能：

- 将数据卷的独立副本备份到低成本的对象存储。
- 将单个备份策略应用于群集中的所有卷，或为具有唯一恢复点目标的卷分配不同的备份策略。
- 创建一个备份策略，以应用于集群中创建的所有未来卷。
- 制作不可变的备份文件，以便在保留期内锁定和保护它们。
- 扫描备份文件以查找可能的勒索软件攻击 - 并自动删除/替换受感染的备份。
- 将较旧的备份文件分层到档案存储以节省成本。
- 删除备份关系，以便您可以存档不需要的源卷，同时保留卷备份。
- 从云备份到云，从本地系统备份到公共云或私有云。
- 备份数据在静态时通过 AES-256 位加密保护，在动态时通过 TLS 1.2 HTTPS 连接保护。
- 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。
- 支持单个卷最多 4,000 个备份。

恢复功能：

- 从对象存储中的本地快照、复制卷或备份卷恢复特定时间点的数据。
- 将卷、文件夹或单个文件还原到源系统或其他系统。
- 将数据恢复到使用不同订阅/帐户或位于不同区域的系统。
- 将卷从云存储快速恢复到Cloud Volumes ONTAP系统或本地系统；非常适合需要尽快提供对卷的访问的灾难恢复情况。
- 在块级别恢复数据，将数据直接放置在您指定的位置，同时保留原始 ACL。
- 浏览和搜索文件目录，轻松选择单个文件夹和文件进行单个文件恢复。

支持备份和恢复操作的系统

NetApp Backup and Recovery支持ONTAP系统以及公共和私有云提供商。

支持的区域

NetApp Backup and Recovery在许多 Amazon Web Services、Microsoft Azure 和 Google Cloud 区域中均支持Cloud Volumes ONTAP 。

"使用全球区域地图了解更多信息"

支持的备份目标

NetApp Backup and Recovery使您能够将ONTAP卷从以下源系统备份到以下辅助系统以及公有云和私有云提供商中的对象存储。快照保留在源系统上。

源系统	辅助系统（复制）	目标对象存储（备份）
AWS 中的Cloud Volumes ONTAP	AWS 本地ONTAP系统中的Cloud Volumes ONTAP	Amazon S3
Azure 中的Cloud Volumes ONTAP	Azure 本地ONTAP系统中的Cloud Volumes ONTAP	Azure Blob
Google 的Cloud Volumes ONTAP	Google 本地ONTAP系统中的Cloud Volumes ONTAP	Google Cloud Storage
本地ONTAP系统	Cloud Volumes ONTAP本地ONTAP系统	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID ONTAP S3

支持的还原目标

您可以将ONTAP数据从位于辅助系统（复制卷）或对象存储（备份文件）中的备份文件还原到以下系统。快照位于源系统上，并且只能还原到同一系统。

备份文件位置		目的地系统
对象存储（备份）	辅助系统（复制）	
Amazon S3	AWS 本地ONTAP系统中的Cloud Volumes ONTAP	AWS 本地ONTAP系统中的Cloud Volumes ONTAP
Azure Blob	Azure 本地ONTAP系统中的Cloud Volumes ONTAP	Azure 本地ONTAP系统中的Cloud Volumes ONTAP
Google Cloud Storage	Google 本地ONTAP系统中的Cloud Volumes ONTAP	Google 本地ONTAP系统中的Cloud Volumes ONTAP
NetAppStorageGRID	本地ONTAP系统Cloud Volumes ONTAP	本地ONTAP系统
ONTAP S3	本地ONTAP系统Cloud Volumes ONTAP	本地ONTAP系统

请注意，“本地ONTAP系统”包括FAS、 AFF和ONTAP Select系统。

支持的卷

NetApp Backup and Recovery支持以下类型的卷：

- FlexVol读写卷
- FlexGroup卷（需要ONTAP 9.12.1 或更高版本）
- SnapLock Enterprise卷（需要ONTAP 9.11.1 或更高版本）
- 适用于本地卷的SnapLock Compliance （需要ONTAP 9.14 或更高版本）
- SnapMirror数据保护 (DP) 目标卷

NetApp Backup and Recovery不支持FlexCache卷的备份。

请参阅"ONTAP卷的备份和还原限制"了解其他要求和限制。

成本

使用NetApp Backup and Recovery与ONTAP系统相关的成本有两种：资源费用和服务费用。这两项费用均针对服务的对象部分备份。

创建快照或复制卷不收取任何费用——除了存储快照和复制卷所需的磁盘空间。

资源费用

资源费用是向云提供商支付的，用于对象存储容量以及将备份文件写入和读取到云中。

- 对于备份到对象存储，您需要向云提供商支付对象存储费用。

  由于NetApp Backup and Recovery保留了源卷的存储效率，因此您需要向云提供商对象存储支付ONTAP效率之后的数据费用（针对应用重复数据删除和压缩后的较少量的数据）。

- 对于使用“搜索和还原”还原数据，您的云提供商会提供某些资源，并且您的搜索请求扫描的数据量会产生每 TiB 成本。 （浏览和恢复不需要这些资源。）
  - 在 AWS 中， "亚马逊雅典娜"和 "AWS Glue"资源部署在新的 S3 存储桶中。
  - 在 Azure 中， "Azure Synapse 工作区"和 "Azure 数据湖存储"在您的存储帐户中配置以存储和分析您的数据。
  - 在 Google 中，部署了一个新的存储桶，并且 "Google Cloud BigQuery 服务"在帐户/项目级别进行配置。
- 如果您计划从已移动到档案对象存储的备份文件中恢复卷数据，则云提供商会收取额外的每 GiB 检索费和每请求费。
- 如果您计划在恢复卷数据的过程中扫描备份文件中的勒索软件（如果您已为云备份启用了 DataLock 和勒索软件恢复功能），那么您还将产生来自云提供商的额外出口成本。

服务费

服务费用支付给NetApp ，涵盖创建对象存储备份的成本以及从这些备份中恢复卷或文件的成本。您只需为对象存储中保护的数据付费，该费用按备份到对象存储的ONTAP卷的源逻辑使用容量（ ONTAP效率之前）计算。此容量也称为前端兆字节 (FETB)。

有三种方式可以支付备份服务费用。第一个选项是从您的云提供商处订阅，这样您就可以按月付费。第二种选择是签订年度合同。第三种选择是直接从NetApp购买许可证。

许可

NetApp Backup and Recovery适用于以下消费模式：

- **BYOL**：从NetApp购买的许可证，可与任何云提供商一起使用。
- **PAYGO**：从云提供商的市场按小时订阅。
- 年度：来自云提供商市场的年度合同。

仅当从对象存储进行备份和恢复时才需要备份许可证。创建快照和复制卷不需要许可证。

自带驾照

BYOL 是基于期限（1、2 或 3 年）和容量的，以 1 TiB 为增量。您向NetApp付费以使用该服务一段时间（比如 1 年）以及最大容量（比如 10 TiB）。

您将收到一个序列号，请在NetApp Console中输入该序列号以启用该服务。当达到任一限制时，您都需要更新许可证。备份 BYOL 许可证适用于与您的NetApp Console组织或帐户关联的所有源系统。

"了解如何管理您的 BYOL 许可证"。

按需付费订阅

NetApp Backup and Recovery以按需付费模式提供基于消费的许可。通过云提供商的市场订阅后，您需要按 GiB 为备份数据付费 - 无需预付款。您的云提供商将通过每月账单向您收费。

"了解如何设置即用即付订阅"。

请注意，当您首次注册 PAYGO 订阅时，可以享受 30 天的免费试用。

年度合同

使用 AWS 时，有两种年度合同可供选择，期限分别为 1 年、2 年或 3 年：

- “云备份”计划使您能够备份Cloud Volumes ONTAP数据和本地ONTAP数据。
- “CVO Professional”计划使您能够捆绑Cloud Volumes ONTAP和NetApp Backup and Recovery。这包括根据此许可证收费的Cloud Volumes ONTAP卷的无限制备份（备份容量不计入许可证）。

使用 Azure 时，有两种年度合同可供选择，分别为 1 年、2 年或 3 年：

- “云备份”计划使您能够备份Cloud Volumes ONTAP数据和本地ONTAP数据。
- “CVO Professional”计划使您能够捆绑Cloud Volumes ONTAP和NetApp Backup and Recovery。这包括根据此许可证收费的Cloud Volumes ONTAP卷的无限制备份（备份容量不计入许可证）。

当您使用 GCP 时，您可以向NetApp请求私人优惠，然后在NetApp Backup and Recovery激活期间从 Google Cloud Marketplace 订阅时选择该计划。

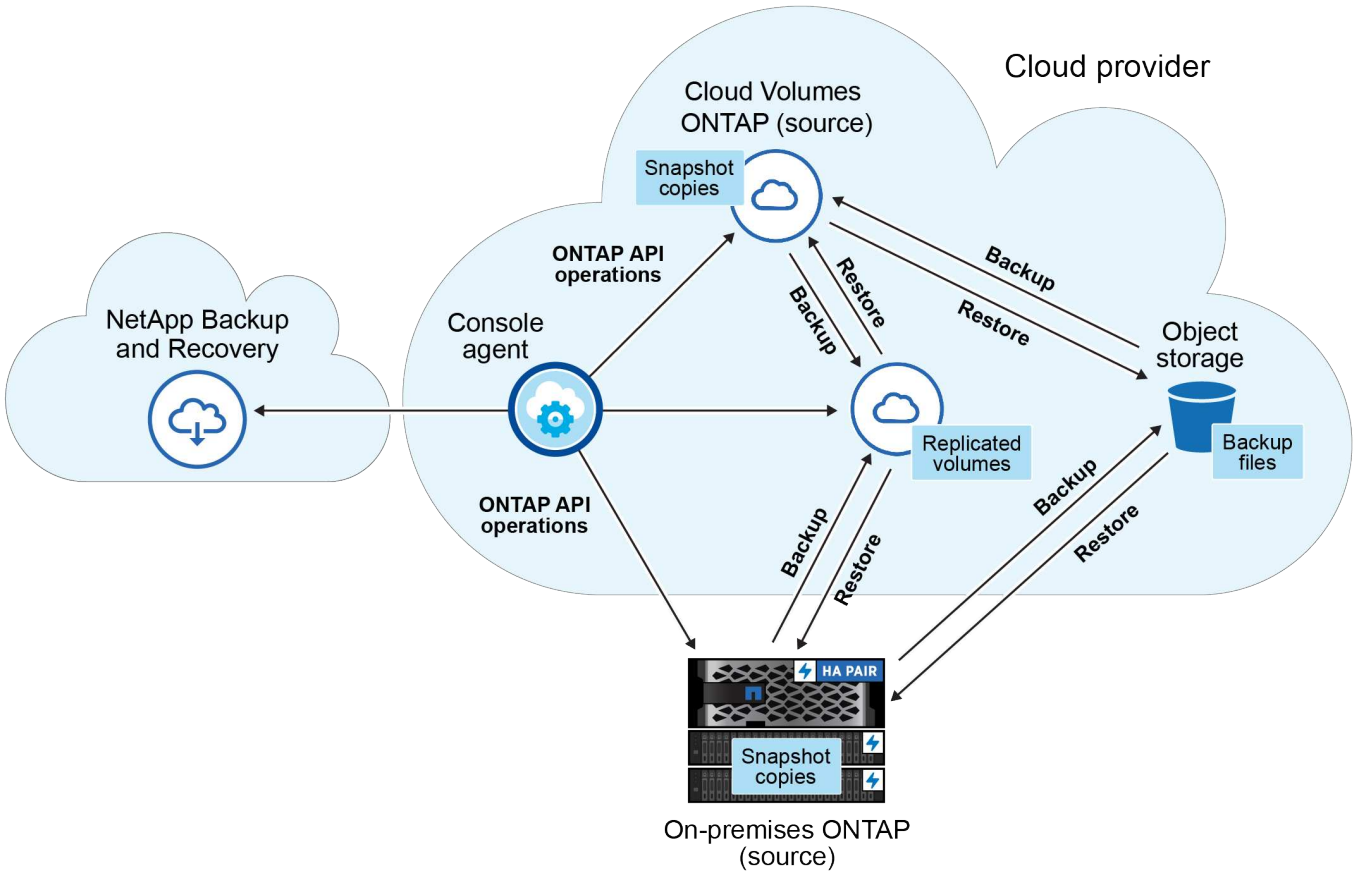
"了解如何制定年度合同"。

NetApp Backup and Recovery的工作原理

当您在Cloud Volumes ONTAP或本地ONTAP系统上启用NetApp Backup and Recovery时，该服务会对您的数据执行完整备份。初始备份之后，所有附加备份都是增量的，这意味着只备份更改的块和新块。这使得网络流量保持最低限度。对象存储备份建立在 "NetApp SnapMirror云技术"。

直接从您的云提供商环境采取的任何管理或更改云备份文件的操作都可能损坏文件并导致不受支持的配置。

下图显示了各个组件之间的关系：



该图显示卷被复制到Cloud Volumes ONTAP系统，但卷也可以复制到本地ONTAP系统。

备份所在位置

根据备份类型，备份位于不同的位置：

- 快照存储在源系统的源卷上。
- _复制卷_驻留在二级存储系统上 - Cloud Volumes ONTAP或本地ONTAP系统。
- _备份副本_存储在控制台在您的云帐户中创建的对象存储中。每个集群/系统有一个对象存储，控制台将对象存储命名为：“netapp-backup-clusteruuid”。请确保不要删除此对象存储。
  - 在 AWS 中，控制台可以实现 "Amazon S3 阻止公共访问功能" 在 S3 铲斗上。
  - 在 Azure 中，控制台使用新的或现有的资源组，并为 Blob 容器分配存储帐户。控制台 "阻止公众访问您的 Blob 数据" 默认情况下。

- 在 GCP 中，控制台使用带有 Google Cloud Storage 存储桶存储帐户的新项目或现有项目。
- 在StorageGRID中，控制台使用现有的租户帐户来管理 S3 存储桶。
- 在ONTAP S3 中，控制台使用 S3 存储桶的现有用户帐户。

如果您将来想要更改集群的目标对象存储，则需要"取消注册系统的NetApp Backup and Recovery"，然后使用新的云提供商信息启用NetApp Backup and Recovery 。

可自定义的备份计划和保留设置

当您为系统启用NetApp Backup and Recovery时，您最初选择的所有卷都将使用您选择的策略进行备份。您可以为快照、复制卷和备份文件选择不同的策略。如果您想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，则可以为该集群创建其他策略，并在激活NetApp Backup and Recovery后将这些策略分配给其他卷。

您可以选择所有卷的每小时、每天、每周、每月和每年备份的组合。对于对象备份，您还可以选择系统定义的策略之一，提供 3 个月、1 年和 7 年的备份和保留。您使用ONTAP System Manager 或ONTAP CLI 在集群上创建的备份保护策略也将作为选择出现。这包括使用自定义SnapMirror标签创建的策略。

应用于卷的快照策略必须具有您在复制策略和备份到对象策略中使用的标签之一。如果未找到匹配的标签，则不会创建备份文件。例如，如果您想要创建“每周”复制卷和备份文件，则必须使用创建“每周”快照的快照策略。

一旦达到某个类别或间隔的最大备份数量，较旧的备份就会被删除，以便您始终拥有最新的备份（因此过时的备份不会继续占用空间）。

数据保护卷备份的保留期与源SnapMirror关系中定义的保留期相同。如果您愿意，可以使用 API 来更改此设置。

备份文件保护设置

如果您的集群使用ONTAP 9.11.1 或更高版本，您可以保护对象存储中的备份免遭删除和勒索软件攻击。每个备份策略都为_DataLock 和 Ransomware Resilience_ 提供了一个部分，可以在特定时间段（即_保留期_）内应用于您的备份文件。

- *DataLock* 保护您的备份文件不被修改或删除。
- _勒索软件保护_会在创建备份文件时以及恢复备份文件中的数据时扫描您的备份文件以查找勒索软件攻击的证据。

默认情况下启用计划的勒索软件防护扫描。扫描频率的默认设置为 7 天。扫描仅发生在最新的快照上。可以禁用计划扫描以降低成本。您可以通过“高级设置”页面上的选项，启用或禁用最新快照上的计划勒索软件扫描。如果启用它，则默认每周执行一次扫描。您可以将该计划更改为几天或几周，或者禁用它，以节省成本。

备份保留期与备份计划保留期相同，再加上最多 31 天的缓冲期。例如，每周备份保留 5 份副本，每个备份文件将锁定 5 周。每月备份保留 6 份副本，每个备份文件将锁定 6 个月。

当您的备份目标是 Amazon S3、Azure Blob 或NetApp StorageGRID时，当前可获得支持。未来版本中将添加其他存储提供商目的地。

欲了解更多详细信息，请参阅以下信息：

- "DataLock 和勒索软件保护的工作原理"。
- "如何在“高级设置”页面中更新勒索软件防护选项"。

如果您将备份分层到档案存储，则无法启用 DataLock。

旧备份文件的存档存储

使用某些云存储时，您可以在一定天数后将较旧的备份文件移动到较便宜的存储类/访问层。您还可以选择立即将备份文件发送到档案存储，而无需写入标准云存储。请注意，如果您启用了 DataLock，则无法使用档案存储。

- 在 AWS 中，备份从“标准”存储类开始，并在 30 天后转换到“标准-不频繁访问”存储类。

  如果您的集群使用的是ONTAP 9.10.1 或更高版本，您可以选择在一定天数后将旧备份分层到NetApp Backup and RecoveryUI 中的“S3 Glacier”或“S3 Glacier Deep Archive”存储，以进一步优化成本。"了解有关 AWS 档案存储的更多信息"。

- 在 Azure 中，备份与 *Cool* 访问层相关联。

  如果您的集群使用的是ONTAP 9.10.1 或更高版本，您可以选择在一定天数后将旧备份分层到NetApp Backup and RecoveryUI 中的“Azure Archive”存储，以进一步优化成本。"了解有关 Azure 档案存储的更多信息"。

- 在 GCP 中，备份与 *Standard* 存储类相关联。

  如果您的集群使用的是ONTAP 9.12.1 或更高版本，您可以选择在一定天数后将旧备份分层到NetApp Backup and Recovery UI 中的“*Archive*”存储中，以进一步优化成本。"详细了解 Google 归档存储"。

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

  如果您的本地集群使用的是ONTAP 9.12.1 或更高版本，并且您的StorageGRID系统使用的是 11.4 或更高版本，则可以在一定天数后将较旧的备份文件存档到公共云存档存储。当前支持 AWS S3 Glacier/S3 Glacier Deep Archive 或 Azure Archive 存储层。"了解有关从StorageGRID归档备份文件的更多信息"。

有关存档旧备份文件的详细信息，请参阅 xref:./prev-ontap-policy-object-options.html]。

FabricPool分层策略注意事项

当您要备份的卷位于FabricPool聚合上，并且分配了分层策略时，您需要注意以下几点 `none`：

- FabricPool分层卷的第一次备份需要读取所有本地和所有分层数据（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。

  此操作可能会导致从云提供商读取数据的成本一次性增加。

  - 后续备份是增量的，不会产生这种影响。
  - 如果在最初创建卷时将分层策略分配给卷，则您将不会看到此问题。

- 在分配之前考虑备份的影响 `all`对卷进行分层策略。由于数据是立即分层的，NetApp Backup and Recovery 将从云层而不是本地层读取数据。由于并发备份操作共享与云对象存储的网络链接，因此如果网络资源饱和，可能会出现性能下降。在这种情况下，您可能需要主动配置多个网络接口 (LIF) 来减少这种类型的网络饱和。

使用NetApp Backup and Recovery规划您的保护之旅

NetApp Backup and Recovery使您能够创建最多三个源卷副本来保护您的数据。在卷上启用备份和恢复时，您可以选择许多选项，因此您应该检查您的选择以做好准备。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

我们将讨论以下选项：

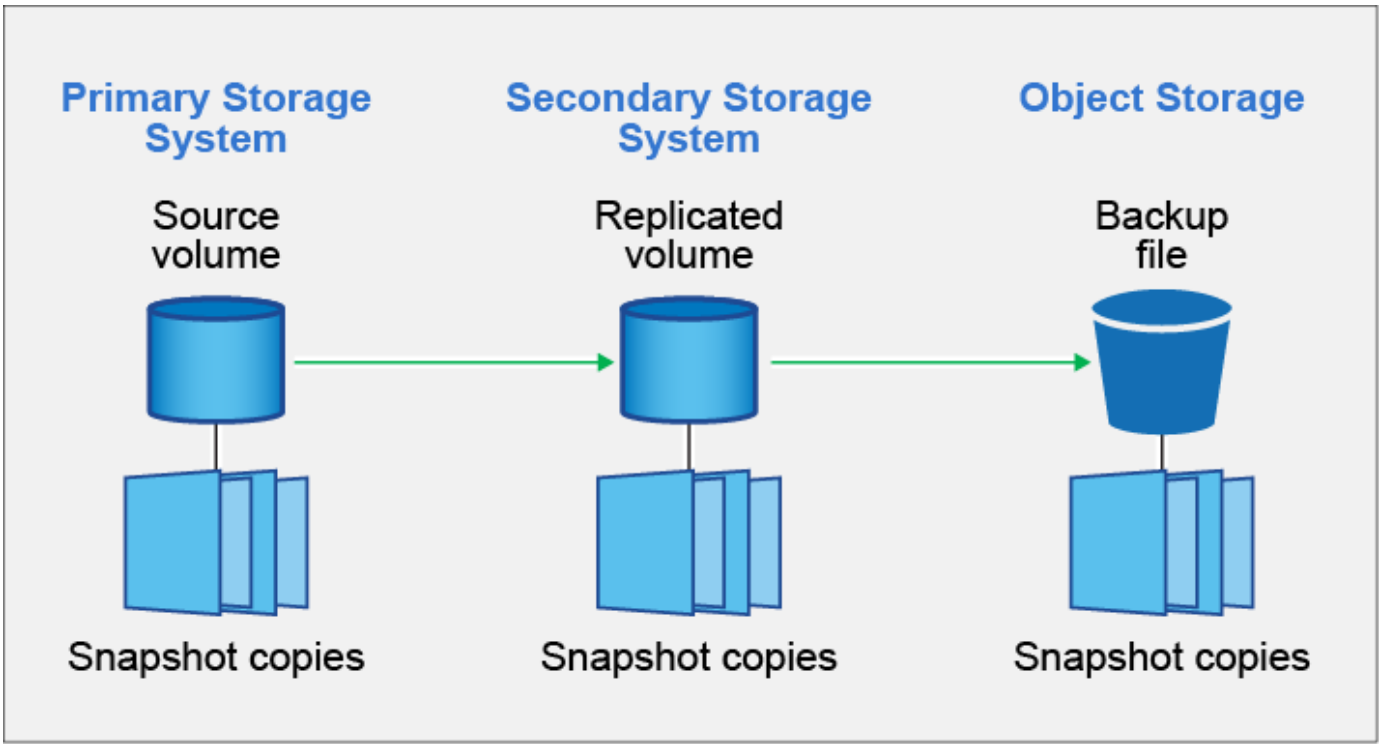
- 您将使用哪些保护功能：快照、复制卷和/或云备份
- 您将使用哪种备份架构：卷的级联备份还是扇出备份
- 您是否会使用默认备份策略，还是需要创建自定义策略
- 您希望服务为您创建云存储桶，还是希望在开始之前创建对象存储容器
- 您使用哪种控制台代理部署模式（标准、受限或私有模式）

您将使用哪些保护功能

在您选择要使用的功能之前，这里简要介绍一下每个功能的作用以及它提供的保护类型。

备份类型	描述
Snapshot	创建源卷中某个卷的只读、时间点映像作为快照。您可以使用快照来恢复单个文件，或者恢复整个卷的内容。
复制	在另一个ONTAP存储系统上创建数据的辅助副本并不断更新辅助数据。您的数据将保持最新状态，并在您需要时随时可用。
云备份	将您的数据备份到云端，以进行保护并用于长期存档。如果需要，您可以将卷、文件夹或单个文件从备份还原到相同或不同的系统。

快照是所有备份方法的基础，是使用备份和恢复服务的必需条件。快照是卷的只读、时间点图像。该图像占用极少的存储空间，并且由于它只记录自上次快照以来文件发生的更改，因此对性能的影响可以忽略不计。在卷上创建的快照用于保持复制卷和备份文件与源卷所做的更改同步——如图所示。



您可以选择在另一个ONTAP存储系统上创建复制卷，并在云中创建备份文件。或者您可以选择仅创建复制卷或备份文件 - 这是您的选择。

总而言之，这些是您可以为ONTAP系统中的卷创建的有效保护流程：

- 源卷 → 快照 → 复制卷 → 备份文件
- 源卷 → 快照 → 备份文件
- 源卷 → 快照 → 复制卷

复制卷或备份文件的初始创建包括源数据的完整副本 - 这称为_基线传输_。后续传输仅包含源数据的差异副本（快照）。

不同备份方法的比较

下表显示了三种备份方法的总体比较。虽然对象存储空间通常比本地磁盘存储便宜，但如果您认为您可能会频繁从云中恢复数据，那么云提供商的出口费用可能会减少您的一些节省。您需要确定需要多久从云中的备份文件中恢复数据。

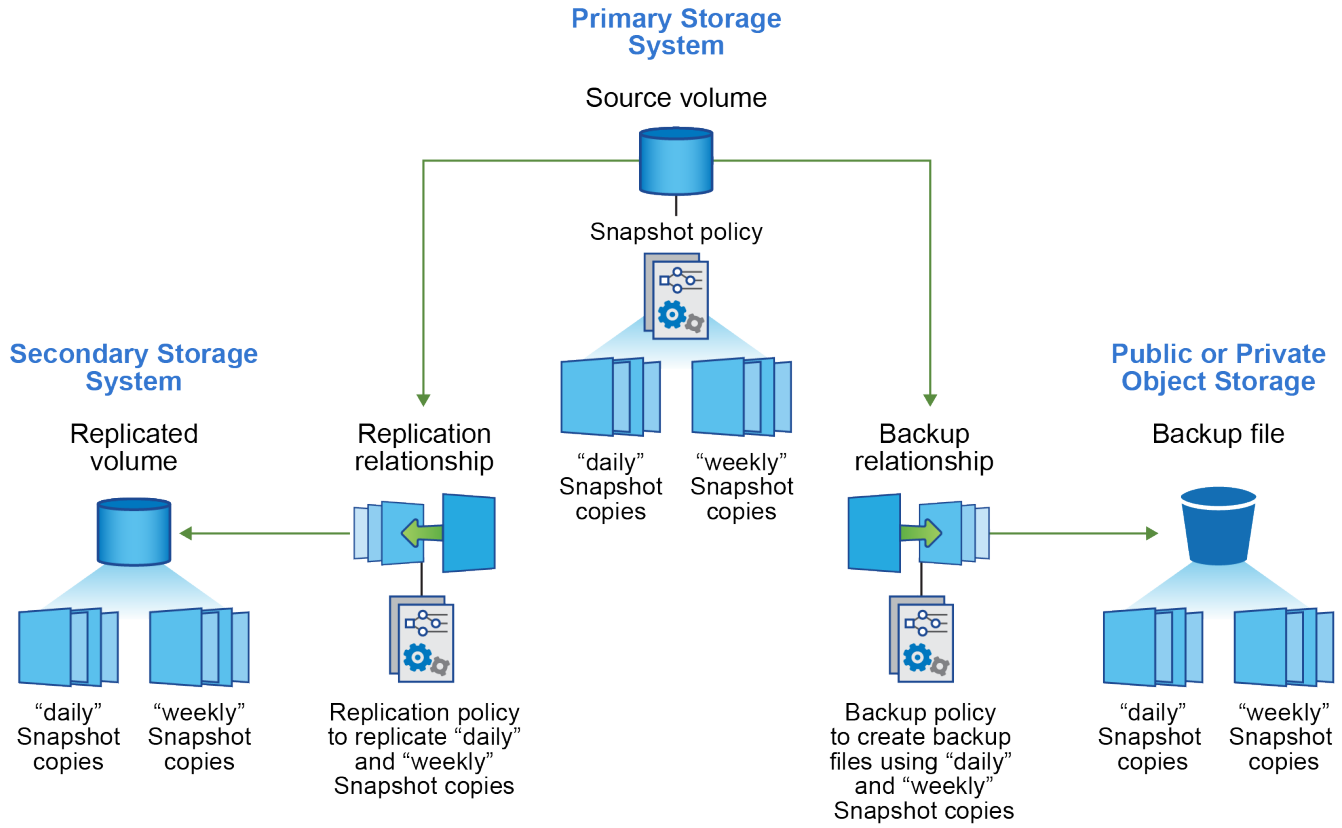
除了此标准之外，如果您使用 DataLock 和勒索软件恢复功能，云存储还可以提供额外的安全选项，并且通过为旧备份文件选择存档存储类可以节省额外的成本。"了解有关 DataLock 和勒索软件保护以及档案存储设置的更多信息"。

备份类型	备份速度	备份成本	恢复速度	恢复成本
快照	高	低（磁盘空间）	高	低
复制	中	中等（磁盘空间）	中	中（网络）
云备份	低	低（物体空间）	低	高（提供商费用）

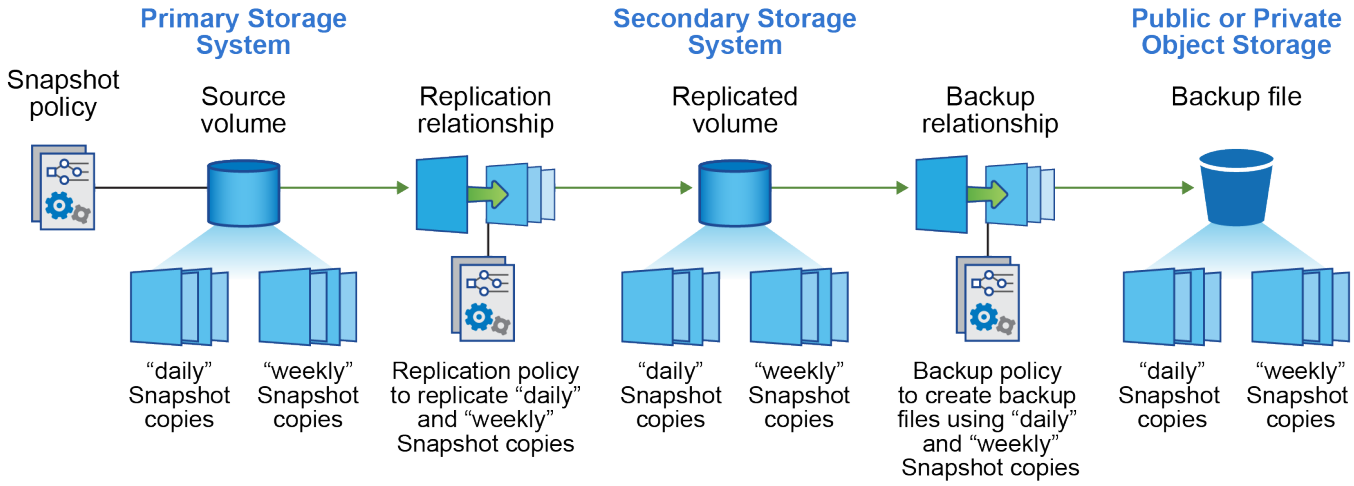
您将使用哪种备份架构

在创建复制卷和备份文件时，您可以选择扇出或级联架构来备份卷。

扇出式架构将快照独立地传输到目标存储系统和云端备份对象。



级联架构首先将快照传输到目标存储系统，然后该系统将副本传输到云端的备份对象。



不同架构选择的比较

该表提供了扇出型和级联型架构的比较。

扇出	级联
由于源系统需要向两个不同的系统发送快照，因此对源系统的性能影响很小。	对源存储系统的性能影响较小，因为它只发送一次快照。
更易于设置，因为所有策略、网络和ONTAP配置都在源系统上完成	还需要从辅助系统完成一些网络和ONTAP配置。

您是否会使用快照、复制和备份的默认策略

您可以使用NetApp提供的默认策略来创建备份，也可以创建自定义策略。当您使用激活向导为您的卷启用备份和恢复服务时，您可以从默认策略和系统中已经存在的任何其他策略（Cloud Volumes ONTAP或本地ONTAP系统）中进行选择。如果您想使用与现有策略不同的策略，您可以在开始之前或使用激活向导时创建该策略。

- 默认快照策略会创建每小时、每天和每周快照，保留 6 个每小时快照、2 个每天快照和 2 个每周快照。
- 默认复制策略复制每日和每周快照，保留 7 个每日快照和 52 个每周快照。
- 默认备份策略复制每日和每周快照，保留 7 个每日快照和 52 个每周快照。

如果您为复制或备份创建自定义策略，则策略标签（例如“每日”或“每周”）必须与快照策略中存在的标签匹配，否则将不会创建复制的卷和备份文件。

您可以在NetApp Backup and RecoveryUI 中创建快照、复制和备份到对象存储策略。请参阅"添加新的备份策略"了解详情。

除了使用NetApp Backup and Recovery创建自定义策略之外，您还可以使用 System Manager 或ONTAP命令行界面 (CLI)：

- "使用 System Manager 或ONTAP CLI 创建快照策略"
- "使用 System Manager 或ONTAP CLI 创建复制策略"

*注意：*使用系统管理器时，选择*异步*作为复制策略的策略类型，并选择*异步*和*备份到云*作为备份到对象策略。

以下是一些ONTAP CLI 命令示例，如果您要创建自定义策略，这些命令可能会有所帮助。请注意，您必须使用_admin_ vserver（存储虚拟机）作为 `<vserver_name>`在这些命令中。

政策描述	命令
简单快照策略	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
简单备份到云端	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

政策描述	命令
使用 DataLock 和勒索软件保护功能备份到云端	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
使用归档存储类备份到云	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
简单复制到另一个存储系统	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

只有保险库策略可用于备份到云关系。

我的政策在哪里?

根据您计划使用的备份架构，备份策略位于不同的位置：扇出式或级联式。复制策略和备份策略的设计方式不同，因为复制将两个ONTAP存储系统配对，而对象备份使用存储提供程序作为目标。

- 快照策略始终驻留在主存储系统上。
- 复制策略始终驻留在辅助存储系统上。
- 备份到对象策略是在源卷所在的系统上创建的 - 这是扇出配置的主集群，也是级联配置的辅助集群。

这些差异如表所示。

架构	**Snapshot** 策略	复制策略	备份策略
扇出	主云	二级	主云
级联	主云	二级	二级

因此，如果您计划在使用级联架构时创建自定义策略，则需要在将创建复制卷的辅助系统上创建复制和备份到对象策略。如果您计划在使用扇出架构时创建自定义策略，则需要在将创建复制卷的辅助系统上创建复制策略，并在主系统上备份到对象策略。

如果您使用所有ONTAP系统上存在的默认策略，那么一切就都设置好了。

你想创建自己的对象存储容器吗

当您在系统的对象存储中创建备份文件时，默认情况下，备份和恢复服务会在您配置的对象存储帐户中为备份文件创建容器（存储桶或存储帐户）。 AWS 或 GCP 存储桶默认名为“netapp-backup-<uuid>”。 Azure Blob 存储帐户名为“netappbackup<uuid>”。

如果您想使用某个前缀或分配特殊属性，您可以在对象提供者帐户中自行创建容器。如果您想创建自己的容器，则必须在启动激活向导之前创建它。 NetApp Backup and Recovery可以使用任何存储桶并共享存储桶。备份激活向导将自动发现所选帐户和凭据的配置容器，以便您选择要使用的容器。

您可以从控制台或云提供商创建存储桶。

- "从控制台创建 Amazon S3 存储桶"
- "从控制台创建 Azure Blob 存储帐户"
- "从控制台创建 Google Cloud Storage 存储桶"

如果您计划使用与“netapp-backup-xxxxxx”不同的存储桶前缀，则需要修改控制台代理 IAM 角色的 S3 权限。

高级存储桶设置

如果您计划将较旧的备份文件移动到档案存储，或者如果您计划启用 DataLock 和勒索软件保护来锁定备份文件并扫描其中是否存在可能的勒索软件，则需要使用某些配置设置创建容器：

- 目前，当您在集群上使用ONTAP 9.10.1 或更高版本软件时，AWS S3 存储支持您自己的存储桶上的存档存储。默认情况下，备份从 S3 *Standard* 存储类开始。确保使用适当的生命周期规则创建存储桶：
  - 30 天后将整个存储桶范围内的对象移动到 S3 *Standard-IA*。
  - 将带有标签“smc_push_to_archive: true”的对象移动到_Glacier Flexible Retrieval_（以前称为 S3 Glacier）
- 当集群上使用ONTAP 9.11.1 或更高版本软件时，AWS 存储支持 DataLock 和勒索软件保护；当使用ONTAP 9.12.1 或更高版本软件时，Azure 存储支持 DataLock 和勒索软件保护。
  - 对于 AWS，您必须使用 30 天的保留期在存储桶上启用对象锁定。
  - 对于 Azure，您需要创建具有版本级不变性支持的存储类。

您正在使用哪种控制台代理部署模式

如果您已经使用控制台来管理您的存储，那么控制台代理已经安装。如果您计划将相同的控制台代理与NetApp Backup and Recovery一起使用，那么一切就绪了。如果您需要使用不同的控制台代理，则需要在开始备份和恢复实施之前安装它。

NetApp Console提供多种部署模式，使您能够以满足业务和安全要求的方式使用控制台。 _标准模式_利用控制台 SaaS 层提供全部功能，而_限制模式_和_私人模式_适用于有连接限制的组织。

"了解有关NetApp Console部署模式的更多信息"。

支持具有完整互联网连接的网站

当在具有完全互联网连接（也称为_标准模式_或_SaaS 模式_）的站点中使用NetApp Backup and Recovery时，您可以在控制台管理的任何本地ONTAP或Cloud Volumes ONTAP系统上创建复制卷，并且可以在任何受支持的云提供商的对象存储上创建备份文件。"查看受支持的备份目标的完整列表"。

有关有效控制台代理位置的列表，请参阅您计划创建备份文件的云提供商的以下备份程序之一。存在一些限制，控制台代理必须手动安装在 Linux 机器上或部署在特定的云提供商中。

- "将Cloud Volumes ONTAP数据备份到 Amazon S3"
- "将Cloud Volumes ONTAP数据备份到 Azure Blob"

- "将Cloud Volumes ONTAP数据备份到 Google Cloud"
- "将本地ONTAP数据备份到 Amazon S3"
- "将本地ONTAP数据备份到 Azure Blob"
- "将本地ONTAP数据备份到 Google Cloud"
- "将本地ONTAP数据备份到StorageGRID"
- "将本地ONTAP备份到ONTAP S3"

支持互联网连接有限的网站

NetApp Backup and Recovery可用于互联网连接受限的站点（也称为“受限模式”）来备份卷数据。在这种情况下，您需要在目标云区域部署控制台代理。

- 您可以将数据从本地ONTAP系统或安装在 AWS 商业区域的Cloud Volumes ONTAP系统备份到 Amazon S3。"将Cloud Volumes ONTAP数据备份到 Amazon S3"。
- 您可以将数据从本地ONTAP系统或安装在 Azure 商业区域中的Cloud Volumes ONTAP系统备份到 Azure Blob。"将Cloud Volumes ONTAP数据备份到 Azure Blob"。

支持没有互联网连接的网站

NetApp Backup and Recovery可用于没有互联网连接的站点（也称为_私有模式_或_暗站_）来备份卷数据。在这种情况下，您需要在同一站点的 Linux 主机上部署控制台代理。

BlueXP私有模式（传统BlueXP接口）通常用于没有互联网连接的本地环境和安全云区域，其中包括 AWS Secret Cloud、AWS Top Secret Cloud 和 Azure IL6。NetApp继续通过传统的BlueXP界面支持这些环境。有关旧版BlueXP界面中的私人模式文档，请参阅 "BlueXP私人模式的 PDF 文档"。

- 您可以将数据从本地ONTAP系统备份到本地NetApp StorageGRID系统。"将本地ONTAP数据备份到StorageGRID"。
- 您可以将数据从本地ONTAP系统备份到本地ONTAP系统或为 S3 对象存储配置的Cloud Volumes ONTAP系统。"将本地ONTAP数据备份到ONTAP S3"。

使用NetApp Backup and Recovery管理ONTAP卷的备份策略

使用NetApp Backup and Recovery，使用NetApp提供的默认备份策略来创建备份，或创建自定义策略。策略控制备份频率、备份时间以及保留的备份文件数量。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

当您使用激活向导为您的卷启用备份和恢复服务时，您可以从默认策略和系统中已经存在的任何其他策略（Cloud Volumes ONTAP或本地ONTAP系统）中进行选择。如果您想使用与现有策略不同的策略，您可以在使用激活向导之前或使用激活向导时创建该策略。

要了解提供的默认备份策略，请参阅"规划您的保护之旅"。

NetApp Backup and Recovery提供三种类型的ONTAP数据备份：快照、复制和对象存储备份。根据您使用的架

构和备份类型，它们的策略位于不同的位置：

架构	快照策略存储位置	复制策略存储位置	备份到对象策略存储位置
扇出	主云	二级	主云
级联	主云	二级	二级

根据您的环境、偏好和保护类型，使用以下工具创建备份策略：

- NetApp Console界面
- 系统管理器用户界面
- ONTAP 命令行界面

使用系统管理器时，选择*异步*作为复制策略的策略类型，并选择*异步*和*备份到云*作为备份到对象策略。

查看系统的策略

1. 在控制台 UI 中，选择 卷 > 备份设置。
2. 从备份设置页面，选择系统，选择*操作*•••图标，然后选择*策略管理*。

   出现“策略管理”页面。默认显示快照策略。

3. 要查看系统中存在的其他策略，请选择“复制策略”或“备份策略”。如果现有策略可用于您的备份计划，则一切就绪。如果您需要具有不同特征的策略，您可以从此页面创建新策略。

创建策略

您可以创建策略来管理对象存储的快照、复制和备份：

- [启动快照之前创建快照策略]
- [在启动复制之前创建复制策略]
- [在启动备份之前创建备份到对象存储策略]

启动快照之前创建快照策略

3-2-1 策略的一部分包括创建主存储系统上卷的快照。

策略创建过程的一部分涉及识别表示计划和保留的快照和SnapMirror标签。您可以使用预定义标签或创建自己的标签。

步骤

1. 在控制台 UI 中，选择 卷 > 备份设置。
2. 从备份设置页面，选择系统，选择*操作*•••图标，然后选择*策略管理*。

   出现“策略管理”页面。

3. 在策略页面中，选择*创建策略* > 创建快照策略。

4. 指定策略名称。
5. 选择一个或多个快照计划。您最多可以拥有 5 个标签。或者，创建一个时间表。
6. 如果您选择创建时间表：
    a. 选择每小时、每天、每周、每月或每年的频率。
    b. 指定表示计划和保留的快照标签。
    c. 输入拍摄快照的时间和频率。
    d. 保留：输入要保留的快照数量。
7. 选择“创建”。

使用级联架构的快照策略示例

此示例创建具有两个集群的快照策略：

1. 集群 1：
    a. 在策略页面上选择集群 1。
    b. 忽略复制和备份到对象策略部分。
    c. 创建快照策略。
2. 集群 2：
    a. 在策略页面上选择集群 2。
    b. 忽略快照策略部分。
    c. 配置复制和备份到对象策略。

在启动复制之前创建复制策略

您的 3-2-1 策略可能包括在不同的存储系统上复制卷。复制策略驻留在*辅助*存储系统上。

步骤

1. 在“策略”页面中，选择“创建策略”>“创建复制策略”。
2. 在“策略详细信息”部分中，指定策略名称。
3. 指定SnapMirror标签（最多 5 个）以表示每个标签的保留。
4. 指定传输时间表。
5. 选择“创建”。

在启动备份之前创建备份到对象存储策略

您的 3-2-1 策略可能包括将卷备份到对象存储。

根据备份架构，此存储策略位于不同的存储系统位置：

- 扇出：主存储系统
- 级联：二级存储系统

步骤

1. 在策略管理页面中，选择*创建策略* > 创建备份策略。
2. 在“策略详细信息”部分中，指定策略名称。
3. 指定SnapMirror标签（最多 5 个）以表示每个标签的保留。
4. 指定设置，包括传输计划和何时存档备份。
5. （可选）要在一定天数后将较旧的备份文件移动到较便宜的存储类或访问层，请选择*存档*选项并指示存档数据之前应经过的天数。输入 **0** 作为“存档天数”以将备份文件直接发送到存档存储。

   "了解有关档案存储设置的更多信息"。

6. （可选）为保护您的备份不被修改或删除，请选择*DataLock 和勒索软件保护*选项。

   如果您的集群使用的是ONTAP 9.11.1 或更高版本，您可以选择通过配置“DataLock”和“勒索软件保护”来保护您的备份免遭删除。

   "了解有关可用 DataLock 设置的更多信息"。

7. 选择“创建”。

编辑策略

您可以编辑自定义快照、复制或备份策略。

更改备份策略会影响所有使用该策略的卷。

步骤

1. 在策略管理页面中，选择策略，选择*操作*•••图标，然后选择*编辑策略*。

   复制和备份策略的过程相同。

2. 在“编辑策略”页面中进行更改。
3. 选择*保存*。

删除策略

您可以删除与任何卷均不关联的策略。

如果某个策略与某个卷关联，并且您想要删除该策略，则必须先从该卷中删除该策略。

步骤

1. 在策略管理页面中，选择策略，选择*操作*•••图标，然后选择*删除快照策略*。
2. 选择*删除*。

查找更多信息

有关使用 System Manager 或ONTAP CLI 创建策略的说明，请参阅以下内容：

"使用 System Manager 创建 Snapshot 策略" "使用ONTAP CLI 创建 Snapshot 策略" "使用 System Manager 创

建复制策略" "使用ONTAP CLI 创建复制策略" "使用 System Manager 创建对象存储策略的备份" "使用ONTAP CLI 创建对象存储策略备份"

NetApp Backup and Recovery中的备份到对象策略选项

NetApp Backup and Recovery使您能够为本地ONTAP和Cloud Volumes ONTAP系统创建具有各种设置的备份策略。

这些策略设置仅与备份到对象存储相关。这些设置都不会影响您的快照或复制策略。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

备份计划选项

NetApp Backup and Recovery使您能够为每个系统（集群）创建具有唯一计划的多个备份策略。您可以为具有不同恢复点目标 (RPO) 的卷分配不同的备份策略。

每个备份策略都提供了一个“标签和保留”部分，您可以将其应用于备份文件。请注意，应用于卷的 Snapshot 策略必须是NetApp Backup and Recovery识别的策略之一，否则将不会创建备份文件。

该计划分为两部分：标签和保留值：

- 标签 定义了从卷创建（或更新）备份文件的频率。您可以从以下标签类型中进行选择：
  - 您可以选择*每小时*、每天、每周、*每月*和*每年*时间范围中的一个或多个组合。
  - 您可以选择系统定义的策略之一，提供 3 个月、1 年或 7 年的备份和保留。
  - 如果您已使用ONTAP System Manager 或ONTAP CLI 在集群上创建了自定义备份保护策略，则可以选择其中一个策略。
- *保留*值定义每个标签（时间范围）保留多少个备份文件。一旦达到某个类别或间隔内的最大备份数量，较旧的备份就会被删除，以便您始终拥有最新的备份。这还可以节省您的存储成本，因为过时的备份不会继续占用云中的空间。

例如，假设您创建一个备份策略，该策略创建 7 个 每周 备份和 12 个 每月 备份：

- 每周和每月都会为卷创建一个备份文件
- 在第 8 周，删除第一个每周备份，并添加第 8 周的新每周备份（最多保留 7 个每周备份）
- 在第 13 个月，删除第一个月度备份，并添加第 13 个月的新月度备份（最多保留 12 个月度备份）

年度备份在传输到对象存储后会自动从源系统中删除。可以在系统的高级设置页面中更改此默认行为。

DataLock 和勒索软件保护选项

NetApp Backup and Recovery为您的卷备份提供 DataLock 和勒索软件保护支持。这些功能使您能够锁定备份文件并对其进行扫描以检测备份文件上可能存在的勒索软件。这是一个可选设置，当您想为集群的卷备份提供额外保护时，可以在备份策略中定义它。

这两个功能都可以保护您的备份文件，以便在您的备份遭受勒索软件攻击时，您始终拥有一个有效的备份文件来恢复数据。满足某些监管要求也很有帮助，在这些要求中，备份需要被锁定并保留一段时间。启用 DataLock 和

勒索软件恢复选项后，作为NetApp Backup and Recovery激活的一部分配置的云存储桶将启用对象锁定和对象版本控制。

此功能不为您的源卷提供保护；仅为这些源卷的备份提供保护。使用一些 "ONTAP提供的反勒索软件保护"保护您的源卷。

- 如果您计划使用 DataLock 和勒索软件保护，则可以在创建第一个备份策略并为该集群激活NetApp Backup and Recovery时启用它。您可以稍后使用NetApp Backup and Recovery高级设置启用或禁用勒索软件扫描。
- 当控制台在恢复卷数据时扫描备份文件中的勒索软件时，您将产生来自云提供商的额外出口成本以访问备份文件的内容。

什么是**DataLock**

借助此功能，您可以锁定通过SnapMirror复制到云端的云快照，还可以启用该功能来检测勒索软件攻击并恢复对象存储上快照的一致副本。此功能在 AWS、Azure、Google Cloud Platform 和StorageGRID上均受支持。

DataLock 可保护您的备份文件在一定时间内不被修改或删除 - 也称为_不可变存储_。此功能使用对象存储提供商的技术进行“对象锁定”。

云提供商使用保留截止日期 (RUD)，该日期是根据快照保留期计算的。快照保留期是根据备份策略中定义的标签和保留计数计算的。

最短快照保留期为 30 天。让我们看一些例子来了解它的工作原理：

- 如果您选择保留计数为 20 的 **Daily** 标签，则快照保留期为 20 天，默认为最短 30 天。
- 如果您选择保留计数为 4 的 每周 标签，则快照保留期为 28 天，默认为最短 30 天。
- 如果您选择保留计数为 3 的“每月”标签，则快照保留期为 90 天。
- 如果您选择保留计数为 1 的 每年 标签，则快照保留期为 365 天。

什么是保留截止日期 **(RUD)**？如何计算？

保留截止日期 (RUD) 根据快照保留期确定。保留截止日期是通过将快照保留期与缓冲区相加来计算的。

- 缓冲为转移时间缓冲（3天）+成本优化缓冲（28天），总计31天。
- 最短保留截止日期为 30 天 + 31 天缓冲期 = 61 天。

以下是一些示例：

- 如果您创建具有 12 个保留的每月备份计划，则您的备份将被锁定 12 个月（加 31 天），然后才会被删除（由下一个备份文件替换）。
- 如果您创建的备份策略创建了 30 个每日备份、7 个每周备份和 12 个每月备份，则有三个锁定保留期：
  - “每日 30 次”备份将保留 61 天（30 天加上 31 天缓冲），
  - “每周 7 次”备份保留 11 周（7 周加 31 天），并且
  - “12 个月”备份将保留 12 个月（加 31 天）。
- 如果您创建具有 24 个保留的每小时备份计划，您可能会认为备份被锁定 24 小时。但是，由于该时间少于 30 天的最低限制，因此每个备份将被锁定并保留 61 天（30 天加上 31 天的缓冲时间）。

旧备份将在 DataLock 保留期到期后删除，而不是在备份策略保留期到期后删除。

DataLock 保留设置将覆盖备份策略中的策略保留设置。这可能会影响您的存储成本，因为您的备份文件将在对象存储中保存更长时间。

启用 **DataLock** 和勒索软件保护

您可以在创建策略时启用 DataLock 和勒索软件保护。创建策略后，您无法启用、修改或禁用此功能。

1. 创建策略时，展开“DataLock 和勒索软件弹性”部分。
2. 选择下列选项之一：
   - 无：DataLock 保护和勒索软件恢复功能已禁用。
   - 已解锁：DataLock 保护和勒索软件恢复功能已启用。具有特定权限的用户可以在保留期内覆盖或删除受保护的备份文件。
   - 已锁定：DataLock 保护和勒索软件恢复功能已启用。在保留期内，任何用户都不能覆盖或删除受保护的备份文件。这满足了完全的监管合规性。

参考"如何在“高级设置”页面中更新勒索软件防护选项"。

什么是勒索软件保护

勒索软件防护会扫描您的备份文件以寻找勒索软件攻击的证据。勒索软件攻击的检测是使用校验和比较来执行的。如果在新的备份文件与之前的备份文件中发现潜在的勒索软件，则该较新的备份文件将被未显示任何勒索软件攻击迹象的最新备份文件替换。（被判定为遭受勒索软件攻击的文件在被替换1天后被删除。）

扫描发生在以下情况下：

- 云备份对象传输到云对象存储后，很快就会启动对云备份对象的扫描。当备份文件首次写入云存储时，不会执行扫描，而是在写入下一个备份文件时执行扫描。
- 当选择备份进行恢复过程时，可以启动勒索软件扫描。
- 可以随时按需进行扫描。

恢复过程如何进行？

当检测到勒索软件攻击时，该服务使用 Active Data Console 代理 Integrity Checker REST API 来启动恢复过程。数据对象的最旧版本是事实来源，并作为恢复过程的一部分转化为当前版本。

让我们看看它是如何工作的：

- 如果发生勒索软件攻击，该服务会尝试覆盖或删除存储桶中的对象。
- 由于云存储支持版本控制，它会自动创建备份对象的新版本。如果在启用版本控制的情况下删除对象，则会将其标记为已删除，但仍可检索。如果对象被覆盖，则会存储并标记以前的版本。
- 当启动勒索软件扫描时，将验证两个对象版本的校验和并进行比较。如果校验和不一致，则表示检测到了潜在的勒索软件。
- 恢复过程涉及恢复到最后一个已知的良好副本。

支持的系统和对象存储提供商

在以下公共和私有云提供商中使用对象存储时，您可以从以下系统在ONTAP卷上启用 DataLock 和勒索软件保护。

源系统	备份文件目标位置
AWS 中的Cloud Volumes ONTAP	Amazon S3
Azure 中的Cloud Volumes ONTAP	Azure Blob
Google Cloud 中的Cloud Volumes ONTAP	Google Cloud
本地ONTAP系统	Amazon S3 Azure Blob Google Cloud NetApp StorageGRID

要求

- 对于 AWS：
  - 您的集群必须运行ONTAP 9.11.1 或更高版本
  - 控制台代理可以部署在云端或您的本地
  - 以下 S3 权限必须是向控制台代理提供权限的 IAM 角色的一部分。它们位于资源“arn:aws:s3:::netapp-backup-*”的“backupS3Policy”部分：

AWS S3 权限

- s3:获取对象版本标记
- s3：获取存储桶对象锁配置
- s3:获取对象版本Acl
- s3：PutObjectTagging
- s3：删除对象
- s3：删除对象标记
- s3：获取对象保留
- s3：删除对象版本标记
- s3：Put对象
- s3：获取对象
- s3:PutBucketObjectLock配置
- s3:获取生命周期配置
- s3：获取存储桶标记
- s3：删除对象版本
- s3：列出存储桶版本
- s3：列表桶
- s3：PutBucket标记
- s3:获取对象标记
- s3：PutBucket版本控制
- s3：PutObjectVersionTagging
- s3：获取存储桶版本
- s3：获取存储桶Acl
- s3：绕过治理保留
- s3：PutObjectRetention
- s3：获取存储桶位置
- s3：获取对象版本

"查看策略的完整 JSON 格式，您可以在其中复制并粘贴所需的权限"。

- 对于 Azure：
  - 您的集群必须运行ONTAP 9.12.1 或更高版本
  - 控制台代理可以部署在云端或您的本地
- 对于 Google Cloud：
  - 您的集群必须运行ONTAP 9.17.1 或更高版本

- 控制台代理可以部署在云端或您的本地

- 对于StorageGRID：
  - 您的集群必须运行ONTAP 9.11.1 或更高版本
  - 您的StorageGRID系统必须运行 11.6.0.3 或更高版本
  - 控制台代理必须部署在您的场所（可以安装在有或没有互联网访问的站点）
  - 以下 S3 权限必须是向控制台代理提供权限的 IAM 角色的一部分：

    StorageGRID S3 权限

    - s3:获取对象版本标记
    - s3：获取存储桶对象锁配置
    - s3:获取对象版本Acl
    - s3：PutObjectTagging
    - s3：删除对象
    - s3：删除对象标记
    - s3：获取对象保留
    - s3：删除对象版本标记
    - s3：Put对象
    - s3：获取对象
    - s3:PutBucketObjectLock配置
    - s3:获取生命周期配置
    - s3：获取存储桶标记
    - s3：删除对象版本
    - s3：列出存储桶版本
    - s3：列表桶
    - s3：PutBucket标记
    - s3:获取对象标记
    - s3：PutBucket版本控制
    - s3：PutObjectVersionTagging
    - s3：获取存储桶版本
    - s3：获取存储桶Acl
    - s3：PutObjectRetention
    - s3：获取存储桶位置
    - s3：获取对象版本

限制

- 如果您在备份策略中配置了档案存储，则 DataLock 和勒索软件保护功能不可用。
- 激活NetApp Backup and Recovery时选择的 DataLock 选项必须用于该集群的所有备份策略。
- 您不能在单个集群上使用多种 DataLock 模式。
- 如果启用 DataLock，所有卷备份都将被锁定。您不能为单个集群混合锁定和非锁定卷备份。
- DataLock 和勒索软件保护适用于使用启用了 DataLock 和勒索软件保护的备份策略的新卷备份。您可以稍后使用高级设置选项启用或禁用这些功能。
- 只有在使用ONTAP 9.13.1 或更高版本时， FlexGroup卷才能使用 DataLock 和勒索软件保护。

如何降低 **DataLock** 成本的技巧

您可以启用或禁用勒索软件扫描功能，同时保持 DataLock 功能处于活动状态。为了避免额外费用，您可以禁用计划的勒索软件扫描。这使您可以自定义安全设置并避免产生云提供商的费用。

即使禁用了计划的勒索软件扫描，您仍然可以在需要时执行按需扫描。

您可以选择不同级别的保护：

- 无需勒索软件扫描的 **DataLock**：为目标存储中的备份数据提供保护，可以处于治理模式或合规模式。
  - 治理模式：为管理员提供覆盖或删除受保护数据的灵活性。
  - 合规模式：在保留期到期之前提供完全不可磨灭性。这有助于满足严格监管环境中最严格的数据安全要求。数据在其生命周期内无法被覆盖或修改，为您的备份副本提供最强大的保护级别。

    Microsoft Azure 使用锁定和解锁模式。

- 带有勒索软件扫描的 **DataLock**：为您的数据提供额外的安全保护。此功能有助于检测任何更改备份副本的尝试。如果进行任何尝试，则会谨慎地创建新版本的数据。扫描频率可以更改为 1、2、3、4、5、6 或 7 天。如果将扫描设置为每 7 天一次，则成本会显著降低。

有关降低 DataLock 成本的更多提示，请参阅https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475[]

此外，您还可以访问以下网站获取与 DataLock 相关的成本估算： "NetApp Backup and Recovery总拥有成本 (TCO) 计算器" 。

档案存储选项

使用 AWS、Azure 或 Google 云存储时，您可以在一定天数后将较旧的备份文件移动到较便宜的存档存储类或访问层。您还可以选择立即将备份文件发送到档案存储，而无需写入标准云存储。只需输入 **0** 作为“几天后存档”即可将备份文件直接发送到档案存储。对于很少需要访问云备份数据的用户或正在替换磁带备份解决方案的用户来说，这尤其有用。

存档层中的数据在需要时无法立即访问，并且需要更高的检索成本，因此在决定存档备份文件之前，您需要考虑需要多久从备份文件中恢复一次数据。

- 即使您选择“0”将所有数据块发送到档案云存储，元数据块也始终写入标准云存储。
- 如果您启用了 DataLock，则无法使用档案存储。
- 选择 **0** 天（立即存档）后，您无法更改存档策略。

每个备份策略都提供了一个“存档策略”部分，您可以将其应用于备份文件。

- 在 AWS 中，备份从“标准”存储类开始，并在 30 天后转换到“标准-不频繁访问”存储类。

  如果您的集群使用的是ONTAP 9.10.1 或更高版本，您可以将较旧的备份分层到 *S3 Glacier* 或 *S3 Glacier Deep Archive* 存储。"了解有关 AWS 档案存储的更多信息"。

  - 如果您在激活NetApp Backup and Recovery时在第一个备份策略中未选择任何存档层，那么 *S3 Glacier* 将是您未来策略的唯一存档选项。
  - 如果您在第一个备份策略中选择了“S3 Glacier”，那么您可以将该集群的未来备份策略更改为“S3 Glacier Deep Archive”层。
  - 如果您在第一个备份策略中选择“S3 Glacier Deep Archive”，则该层将是该集群未来备份策略唯一可用的存档层。
- 在 Azure 中，备份与 *Cool* 访问层相关联。

  如果您的集群使用的是ONTAP 9.10.1 或更高版本，则可以将旧备份分层到_Azure Archive_存储。"了解有关 Azure 档案存储的更多信息"。
- 在 GCP 中，备份与 *Standard* 存储类相关联。

  如果您的本地集群使用的是ONTAP 9.12.1 或更高版本，您可以选择在一定天数后将旧备份分层到NetApp Backup and Recovery UI 中的“*Archive*”存储中，以进一步优化成本。"详细了解 Google 归档存储"。
- 在StorageGRID中，备份与 *Standard* 存储类相关联。

  如果您的本地集群使用ONTAP 9.12.1 或更高版本，并且您的StorageGRID系统使用 11.4 或更高版本，则可以将较旧的备份文件存档到公共云档案存储。

  - 对于 AWS，您可以将备份分层存储到 AWS *S3 Glacier* 或 *S3 Glacier Deep Archive* 存储中。"了解有关 AWS 档案存储的更多信息"。
  - 对于 Azure，您可以将较旧的备份分层存储到 *Azure Archive* 存储中。"了解有关 Azure 档案存储的更多信息"。

在**NetApp Backup and Recovery**高级设置中管理备份到对象存储选项

您可以使用“高级设置”页面更改在为每个ONTAP系统激活NetApp Backup and Recovery时设置的集群级别、备份到对象存储设置。您还可以修改一些作为“默认”备份设置的设置。这包括更改备份到对象存储的传输速率、是否将历史快照导出为备份文件，以及启用或禁用系统的勒索软件扫描。

这些设置仅适用于备份到对象存储。这些设置都不会影响您的快照或复制设置。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

您可以在高级设置页面中更改以下选项：

- 更改授予ONTAP系统访问对象存储权限的存储密钥
- 更改连接到对象存储的ONTAP IP 空间
- 使用“最大传输速率”选项更改分配给上传备份到对象存储的网络带宽
- 更改是否将历史快照导出为备份文件并将其包含在未来卷的初始基线备份文件中
- 更改是否从源系统中删除“年度”快照
- 启用或禁用系统的勒索软件扫描，包括计划扫描

查看集群级别备份设置

您可以查看每个系统的集群级系统设置和提供商设置。

步骤

1. 从控制台菜单中，选择*保护>备份和恢复*。
2. 从*Volumes*选项卡中，选择*Backup Settings*。
3. 在“备份设置”页面中，选择 ••• 选择“配置高级设置 > 系统设置”查看系统设置，选择“配置高级设置 > 提供商设置”查看提供商设置。

   生成的页面会显示该系统的当前设置。查看提供商设置时，显示的提供商设置与您在页面顶部选择的存储桶相关。

请注意，根据源集群上的ONTAP版本和备份所在的云提供商目标位置，某些选项不可用。

更改可用于将备份上传到对象存储的网络带宽

当您为系统激活NetApp Backup and Recovery时，默认情况下， ONTAP可以使用无限量的带宽将备份数据从系统中的卷传输到对象存储。如果您注意到备份流量影响了正常的用户工作负载，您可以使用“高级设置”页面中的最大传输速率选项来限制传输过程中使用的网络带宽量。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 在“备份设置”页面中，单击 ••• 在系统中，选择“配置高级设置 > 系统设置”。
3. 在高级设置页面中，展开*最大传输速率*部分。
4. 选择 1 到 1,000 Mbps 之间的值作为最大传输速率。
5. 选择*Limited*单选按钮并输入可使用的最大带宽，或选择*Unlimited*表示没有限制。
6. 选择*应用*。

此设置不会影响分配给系统中卷配置的任何其他复制关系的带宽。

更改是否将历史快照导出为备份文件

如果存在与本系统中使用的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则可以将这些历史快照导出到对象存储作为备份文件。这样，您就可以通过将较旧的快照移动到基线备份副本中来初始化云端备份。

请注意，此选项仅适用于新读/写卷的新备份文件，并且不支持数据保护 (DP) 卷。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 在“备份设置”页面中，单击 ••• 在系统中，选择“配置高级设置 > 系统设置”。
3. 在“高级设置”页面中，展开“导出现有快照副本”部分。
4. 选择是否要导出现有快照。
5. 选择*应用*。

更改是否从源系统中删除“年度”快照

当您为任何卷选择“年度”备份策略标签时，创建的快照将非常大。默认情况下，这些年度快照在传输到对象存储后会自动从源系统中删除。您可以从“年度快照删除”部分更改此默认行为。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 在“备份设置”页面中，单击 ••• 在系统中，选择“配置高级设置 > 系统设置”。
3. 在高级设置页面中，展开*年度快照删除*部分。
4. 选择“禁用”以在源系统上保留年度快照。
5. 选择*应用*。

启用或禁用勒索软件扫描

默认情况下启用勒索软件防护扫描。扫描频率的默认设置为 7 天。扫描仅发生在最新的快照上。

有关 DataLock 和勒索软件恢复选项的详细信息，请参阅"DataLock 和勒索软件恢复选项"。

您可以将该计划更改为几天或几周，或者禁用它，以节省成本。

根据云提供商的不同，启用勒索软件扫描将产生额外费用。

如果禁用计划的勒索软件扫描，您仍然可以执行按需扫描，并且恢复操作期间的扫描仍会发生。

参考"管理策略"有关管理实施勒索软件检测的政策的详细信息。

启用或禁用系统的勒索软件扫描

您可以为集群启用或禁用勒索软件扫描。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。

2. 在“备份设置”页面中，单击 ••• 在系统中，选择“配置高级设置 > 系统设置”。
3. 在出现的页面中，展开“勒索软件扫描”部分。
4. 启用或禁用*勒索软件扫描*。
5. 选择*计划勒索软件扫描*。
6. 或者，将每周默认扫描更改为几天或几周。
7. 设置扫描运行的频率（以天数或周数为单位）。
8. 选择*应用*。

启用或禁用提供商的勒索软件扫描

您可以通过提供商设置页面在提供商级别启用或禁用勒索软件扫描。页面上的设置与您在页面顶部选择的存储桶相关。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 在“备份设置”页面中，单击 ••• 在系统中，选择“配置高级设置 > 提供商设置”。
3. 在出现的页面顶部，选择需要更改设置的存储桶。
4. 展开“勒索软件扫描”部分。
5. 启用或禁用*勒索软件扫描*。
6. 选择*计划勒索软件扫描*。
7. 或者，将每周默认扫描更改为几天或几周。
8. 设置扫描运行的频率（以天数或周数为单位）。
9. 选择*应用*。

使用NetApp Backup and Recovery将Cloud Volumes ONTAP数据备份到 Amazon S3

完成NetApp Backup and Recovery中的几个步骤即可开始将卷数据从Cloud Volumes ONTAP系统备份到 Amazon S3。

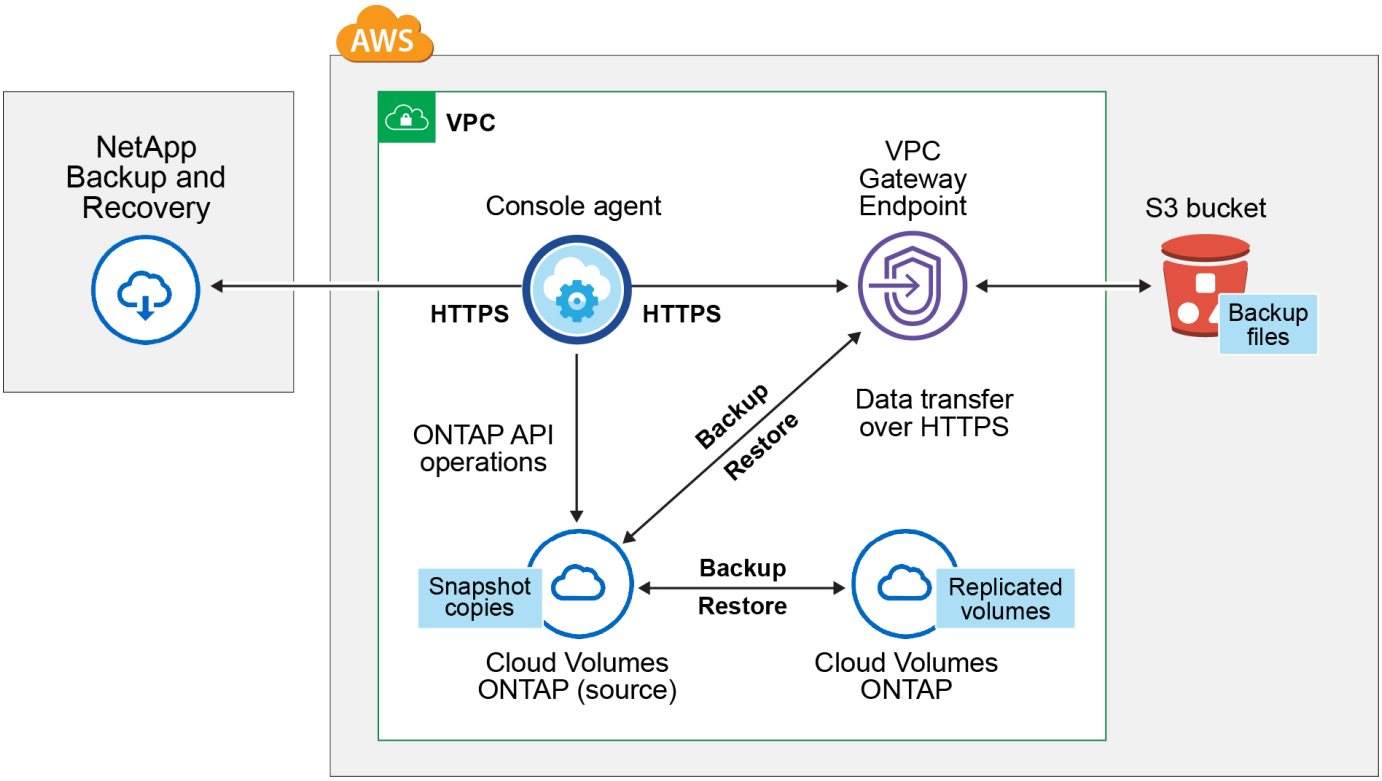
要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

验证对您的配置的支持

在开始将卷备份到 S3 之前，请阅读以下要求以确保您具有受支持的配置。

下图显示了每个组件以及您需要在它们之间准备的连接。

或者，您也可以使用公共或私有连接连接到用于复制卷的辅助ONTAP系统。



VPC 网关端点必须已经存在于您的 VPC 中。 "了解有关网关端点的更多信息" 。

支持的 **ONTAP** 版本

最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。

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密钥进行数据加密，而不是使用默认的 Amazon S3 加密密钥。在这种情况下，您需要设置加密管理密钥。 "了解如何使用您自己的密钥" 。

验证许可证要求

对于NetApp Backup and Recovery PAYGO 许可，可在 AWS Marketplace 中订阅控制台，从而支持部署Cloud Volumes ONTAP和NetApp Backup and Recovery。你需要 "订阅此NetApp Console"在启用NetApp Backup and Recovery之前。 NetApp Backup and Recovery的计费通过此订阅完成。

对于允许您备份Cloud Volumes ONTAP数据和本地ONTAP数据的年度合同，您需要从 "AWS Marketplace 页面" 进而 "将订阅与您的 AWS 凭证关联"。

对于允许您捆绑Cloud Volumes ONTAP和NetApp Backup and Recovery 的年度合同，您必须在创建Cloud Volumes ONTAP系统时设置年度合同。此选项不允许您备份本地数据。

对于NetApp Backup and RecoveryBYOL 许可，您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。"了解如何管理您的 BYOL 许可证"。当控制台代理和Cloud Volumes ONTAP系统部署在暗站中时，您必须使用 BYOL 许可证。

并且您需要有一个 AWS 帐户，用于存储备份所在的存储空间。

准备控制台代理

控制台代理必须安装在具有完全或有限互联网访问权限（“标准”或“受限”模式）的 AWS 区域。 "有关详细信息，请参阅NetApp Console部署模式" 。

- "了解控制台代理"
- "在 AWS 中以标准模式（完全互联网访问）部署控制台代理"
- "以受限模式安装控制台代理（限制出站访问）"

验证或添加控制台代理的权限

为控制台提供权限的 IAM 角色必须包含最新的 S3 权限 "控制台策略"。如果策略不包含所有这些权限，请参阅 "AWS 文档：编辑 IAM 策略"。

以下是该政策的具体权限：

```
{
  "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:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "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-*"
        ]
    }
```

在 AWS 中国区域创建备份时，您需要将 IAM 策略中所有_Resource_部分下的 AWS 资源名称“arn”从“aws”更改为“aws-cn”；例如 `arn:aws-cn:s3:::netapp-backup-*`。

所需的 **AWS Cloud Volumes ONTAP**权限

当您的Cloud Volumes ONTAP系统运行ONTAP 9.12.1 或更高版本的软件时，为该系统提供权限的 IAM 角色必须包含一组新的 S3 权限，专门用于NetApp Backup and Recovery，从最新的 "Cloud Volumes ONTAP策略"。

如果您使用控制台版本 3.9.23 或更高版本创建了Cloud Volumes ONTAP系统，则这些权限应该已经是 IAM 角色的一部分。否则您将需要添加缺少的权限。

支持的 **AWS** 区域

所有 AWS 区域（包括 AWS GovCloud 区域）均支持NetApp Backup and Recovery 。

在不同的 **AWS** 账户中创建备份所需的设置

默认情况下，使用与Cloud Volumes ONTAP系统相同的帐户创建备份。如果您想要使用不同的 AWS 账户进行备份，则必须：

- 验证权限“s3：PutBucketPolicy”和“s3：PutBucketOwnershipControls”是否属于为控制台代理提供权限的 IAM 角色的一部分。
- 在控制台中添加目标 AWS 账户凭证。 "了解如何操作" 。
- 在第二个帐户的用户凭证中添加以下权限：

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

创建您自己的存储桶

默认情况下，该服务会为您创建存储桶。如果您想使用自己的存储桶，您可以在启动备份激活向导之前创建它们，然后在向导中选择这些存储桶。

"了解有关创建您自己的存储桶的更多信息"。

验证**ONTAP**复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地**ONTAP**网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。
- 要在不同子网中的两个Cloud Volumes ONTAP系统之间复制数据，子网必须一起路由（这是默认设置）。

在**Cloud Volumes ONTAP**上启用**NetApp Backup and Recovery**

启用NetApp Backup and Recovery非常简单。根据您拥有的是现有Cloud Volumes ONTAP系统还是新系统，步骤略有不同。

在新系统上启用**NetApp Backup and Recovery**

NetApp Backup and Recovery在系统向导中默认启用。确保该选项保持启用状态。

看 "在 AWS 中启动Cloud Volumes ONTAP"了解创建Cloud Volumes ONTAP系统的要求和详细信息。

步骤

1. 从控制台*系统*页面，选择*添加系统*，选择云提供商，然后选择*添加新*。选择“创建Cloud Volumes ONTAP”。
2. 选择*Amazon Web Services*作为云提供商，然后选择单节点或 HA 系统。
3. 填写详细信息和凭证页面。
4. 在服务页面上，保持服务启用并选择*继续*。
5. 完成向导中的页面以部署系统。

结果

系统上已启用NetApp Backup and Recovery 。在这些Cloud Volumes ONTAP系统上创建卷后，启动NetApp Backup and Recovery并"在您想要保护的每个卷上激活备份"。

在现有系统上启用**NetApp Backup and Recovery**

随时直接从控制台在现有系统上启用NetApp Backup and Recovery。

步骤

1. 从控制台*系统*页面中，选择集群并选择右侧面板中备份和恢复旁边的*启用*。

   如果备份的 Amazon S3 目标在 系统 页面上以集群形式存在，则可以将该集群拖到 Amazon S3 系统上以启动设置向导。

激活**ONTAP**卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- [选择要备份的卷]
- [定义备份策略]
- [检查您的选择]

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：

   - 从控制台*系统*页面中，选择系统，然后选择右侧面板中备份和恢复旁边的*启用>备份卷*。

     如果备份的 AWS 目标作为系统存在于控制台 系统 页面上，则可以将ONTAP集群拖到 AWS 对象存储上。

   - 在备份和恢复栏中选择“卷”。在“卷”选项卡中，选择“操作”。 ••• 图标选项，选择“激活 3-2-1 保护”，适用于单个卷（尚未启用复制或备份到对象存储）。

   向导的介绍页面显示保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。

2. 继续以下选项：

   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您还没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷（FlexGroup卷一次只能选择一个）。要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及设置以下选项：

- 您是否需要一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构
- 本地快照策略
- 复制目标和策略

如果您选择的卷具有与您在此步骤中选择的策略不同的快照和复制策略，则现有策略将被覆盖。

- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：如果您正在执行复制或备份到对象存储，则必须创建本地快照。
   - 复制：在另一个ONTAP存储系统上创建复制卷。
   - 备份：将卷备份到对象存储。在选择现有存储桶或配置新存储桶时，每个集群最多可以备份 6 个存储桶中的卷。
2. 架构：如果您选择复制和备份，请选择以下信息流之一：
   - 级联：信息从主存储系统流向辅助存储系统，再从辅助存储系统流向对象存储。
   - 扇出：信息从主存储系统流向辅助存储系统，再从主存储系统流向对象存储。

   有关这些架构的详细信息，请参阅"规划您的保护之旅"。
3. 本地快照：选择现有的快照策略或创建新的快照策略。

要在激活快照之前创建自定义策略，请参阅"创建策略"。

要创建策略，请选择“创建新策略”并执行以下操作：

a. 输入策略的名称。
b. 选择最多五个时间表，通常频率不同。
c. 选择“创建”。

4. 复制：设置以下选项：
   - 复制目标：选择目标系统和存储虚拟机。（可选）选择目标聚合或多个聚合，以及要添加到复制卷名称的前缀或后缀。
   - 复制策略：选择现有的复制策略或创建一个。

     要创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：

     i. 输入策略的名称。
     ii. 选择最多五个时间表，通常频率不同。
     iii. 选择“创建”。

5. 备份：设置以下选项：
   - 提供商：选择*Amazon Web Services*。
   - 提供商设置：输入提供商详细信息和存储备份的区域。

     输入用于存储备份的 AWS 账户。这可以是与Cloud Volumes ONTAP系统所在的帐户不同的帐户。

     如果您想要使用不同的 AWS 账户进行备份，则必须在控制台中添加目标 AWS 账户凭证，并将权限“s3：PutBucketPolicy”和“s3：PutBucketOwnershipControls”添加到为控制台提供权限的 IAM 角色。

     选择存储备份的区域。这可能与Cloud Volumes ONTAP系统所在的区域不同。

     创建新存储桶或选择现有存储桶。

   - 加密：如果您创建了一个新的存储桶，请输入提供商提供给您的加密密钥信息。您可以选择使用默认的 AWS 加密密钥，或者从您的 AWS 账户中选择您自己的客户管理密钥来管理数据的加密。("了解如何使用您自己的加密密钥"）。

     如果您选择使用自己的客户管理密钥，请输入密钥保管库和密钥信息。

     如果您选择了现有的存储桶，则加密信息已经可用，因此您现在无需输入。

   - 网络：配置此提供商的网络选项。
   - 备份策略：选择现有的备份到对象存储策略或创建一个。

     要在激活备份之前创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：

i. 输入策略的名称。

ii. 选择最多五个时间表，通常频率不同。

iii. 对于备份到对象策略，设置 DataLock 和 Ransomware Resilience 设置。有关 DataLock 和勒索软件恢复的详细信息，请参阅"备份到对象策略设置"。

iv. 选择“创建”。

- 导出现有快照：如果此系统中存在与您刚刚为此系统选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框，即可将所有历史快照复制到对象存储作为备份文件，以确保您的卷得到最全面的保护。

6. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中该复选框可“自动修复本地快照、复制和备份中不匹配的标签”。这将创建与快照、复制和备份策略中的标签相匹配的标签的快照。
3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括主存储系统数据的完整副本。后续传输包含快照中包含的主存储系统数据的差异副本。

在目标集群中创建一个复制卷，该卷将与主存储卷同步。

在您输入的 S3 访问密钥和密钥指示的服务帐户中创建一个 S3 存储桶，并将备份文件存储在那里。

显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

使用NetApp Backup and Recovery将Cloud Volumes ONTAP数据备份到 Azure Blob 存储

完成NetApp Backup and Recovery中的几个步骤，开始将卷数据从Cloud Volumes ONTAP系统备份到 Azure Blob 存储。

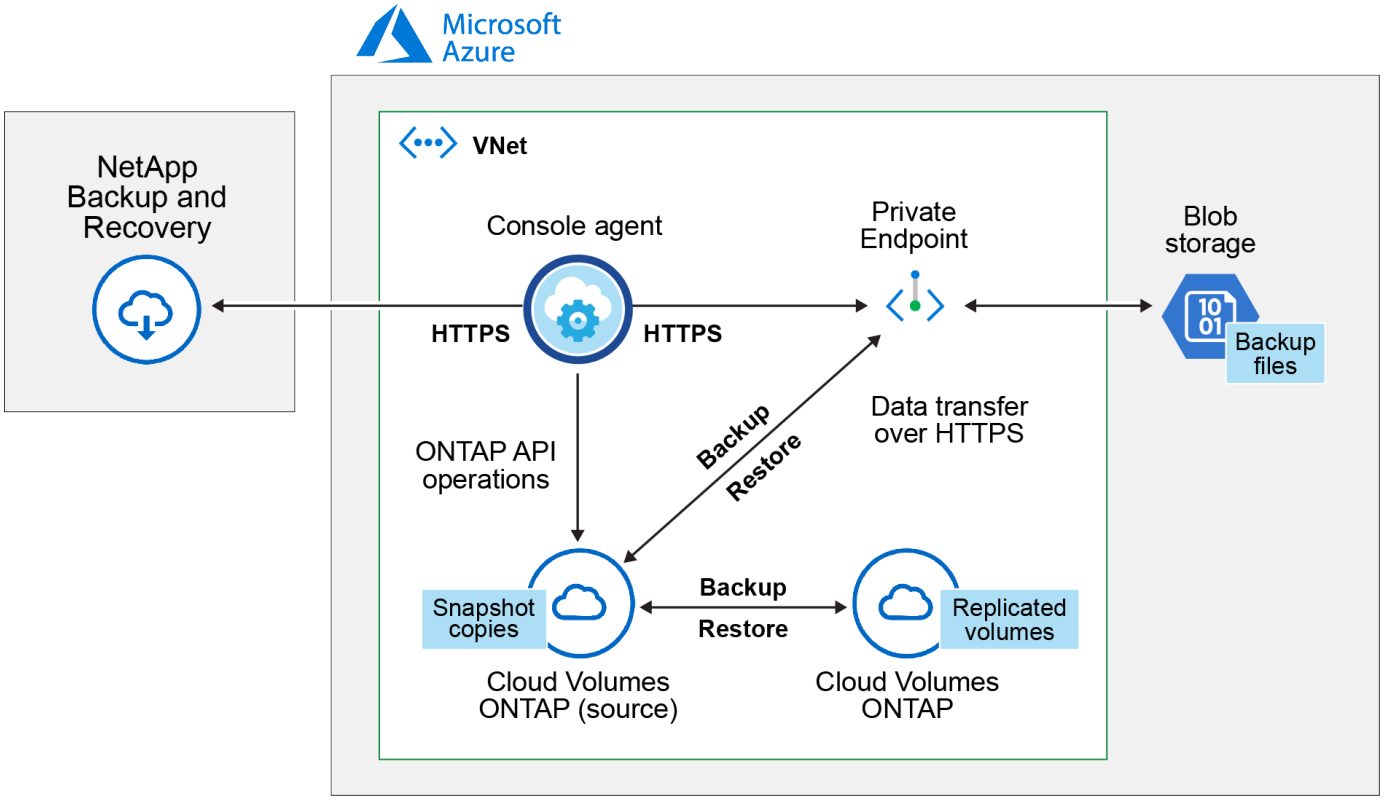
要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

验证对您的配置的支持

在开始将卷备份到 Azure Blob 存储之前，请阅读以下要求以确保具有受支持的配置。

下图显示了每个组件以及您需要在它们之间准备的连接。

或者，您也可以使用公共或私有连接连接到用于复制卷的辅助ONTAP系统。



支持的 **ONTAP** 版本

最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。

支持的 **Azure** 区域

所有 Azure 区域（包括 Azure 政府区域）都支持NetApp Backup and Recovery。

默认情况下， NetApp Backup and Recovery为 Blob 容器提供本地冗余 (LRS) 以优化成本。如果您想确保数据在不同区域之间复制，则可以在激活NetApp Backup and Recovery后将此设置更改为区域冗余 (ZRS)。请参阅 Microsoft 说明 "更改存储帐户的复制方式"。

在不同的 **Azure** 订阅中创建备份所需的设置

默认情况下，使用与Cloud Volumes ONTAP系统相同的订阅来创建备份。

验证许可证要求

对于NetApp Backup and Recovery PAYGO 许可，在启用NetApp Backup and Recovery之前，需要通过 Azure Marketplace 进行订阅。 NetApp Backup and Recovery的计费通过此订阅完成。 "您可以从系统向导的“详细信

息和凭证”页面进行订阅" 。

对于NetApp Backup and RecoveryBYOL 许可，您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。"了解如何管理您的 BYOL 许可证"。当控制台代理和Cloud Volumes ONTAP系统部署在暗站（“私有模式”）时，您必须使用 BYOL 许可证。

并且您需要订阅 Microsoft Azure 以获取备份所在的存储空间。

准备控制台代理

控制台代理可以安装在具有完全或有限互联网访问权限（“标准”或“受限”模式）的 Azure 区域中。 "有关详细信息，请参阅NetApp Console部署模式" 。

- "了解控制台代理"
- "在 Azure 中以标准模式（完全互联网访问）部署控制台代理"
- "以受限模式安装控制台代理（限制出站访问）"

验证或添加控制台代理的权限

要使用NetApp Backup and Recovery搜索和还原功能，您需要在控制台代理的角色中拥有特定权限，以便它可以访问 Azure Synapse 工作区和数据湖存储帐户。请参阅下面的权限，如果需要修改策略，请按照以下步骤操作。

开始之前

- 您必须向您的订阅注册 Azure Synapse Analytics 资源提供程序（称为“Microsoft.Synapse”）。 "了解如何为您的订阅注册此资源提供程序" 。您必须是订阅*所有者*或*贡献者*才能注册资源提供者。
- 必须打开端口 1433 才能实现控制台代理和 Azure Synapse SQL 服务之间的通信。

步骤

1. 确定分配给控制台代理虚拟机的角色：
    a. 在 Azure 门户中，打开虚拟机服务。
    b. 选择控制台代理虚拟机。
    c. 在“设置”下，选择“身份”。
    d. 选择“Azure 角色分配”。
    e. 记下分配给控制台代理虚拟机的自定义角色。
2. 更新自定义角色：
    a. 在 Azure 门户中，打开你的 Azure 订阅。
    b. 选择“访问控制 (IAM)”>“角色”。
    c. 选择自定义角色的省略号（...），然后选择*编辑*。
    d. 选择 **JSON** 并添加以下权限：

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"查看策略的完整 JSON 格式"

e. 选择*审核 + 更新*，然后选择*更新*。

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使用自己的客户管理密钥进行数据加密，而不是使用默认的 Microsoft 管理加密密钥。在这种情况下，您将需要有 Azure 订阅、Key Vault 名称和密钥。 "了解如何使用您自己的密钥" 。

NetApp Backup and Recovery支持 Azure 访问策略、Azure 基于角色的访问控制 (Azure RBAC) 权限模型和托管硬件安全模型 (HSM)（请参阅 "什么是 Azure Key Vault 托管 HSM？ "）。

创建 **Azure Blob** 存储帐户

默认情况下，该服务会为您创建存储帐户。如果您想使用自己的存储帐户，您可以在启动备份激活向导之前创建它们，然后在向导中选择这些存储帐户。

"了解有关创建自己的存储帐户的更多信息"。

验证**ONTAP**复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地**ONTAP**网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。
- 要在不同子网中的两个Cloud Volumes ONTAP系统之间复制数据，子网必须一起路由（这是默认设置）。

在**Cloud Volumes ONTAP**上启用**NetApp Backup and Recovery**

启用NetApp Backup and Recovery非常简单。根据您拥有的是现有Cloud Volumes ONTAP系统还是新系统，步骤略有不同。

在新系统上启用**NetApp Backup and Recovery**

NetApp Backup and Recovery在系统向导中默认启用。确保该选项保持启用状态。

看 "在 Azure 中启动Cloud Volumes ONTAP"了解创建Cloud Volumes ONTAP系统的要求和详细信息。

如果您想选择资源组的名称，请在部署Cloud Volumes ONTAP时*禁用* NetApp Backup and Recovery 。

步骤

1. 从控制台*系统*页面，选择*添加系统*，选择云提供商，然后选择*添加新*。选择“创建Cloud Volumes

ONTAP”。

2. 选择 **Microsoft Azure** 作为云提供商，然后选择单节点或 HA 系统。
3. 在“定义 Azure 凭据”页面中，输入凭据名称、客户端 ID、客户端密钥和目录 ID，然后选择“继续”。
4. 填写“详细信息和凭据”页面并确保已订阅 Azure 市场，然后选择“继续”。
5. 在服务页面上，保持服务启用并选择*继续*。
6. 完成向导中的页面以部署系统。

结果

系统上已启用NetApp Backup and Recovery 。在这些Cloud Volumes ONTAP系统上创建卷后，启动NetApp Backup and Recovery并"在您想要保护的每个卷上激活备份"。

在现有系统上启用**NetApp Backup and Recovery**

随时直接从系统启用NetApp Backup and Recovery。

步骤

1. 从控制台*系统*页面中，选择系统并选择右侧面板中备份和恢复旁边的*启用*。

   如果备份的 Azure Blob 目标作为系统存在于控制台*系统*页面上，则可以将集群拖到 Azure Blob 系统上以启动设置向导。

2. 完成向导中的页面以部署NetApp Backup and Recovery。
3. 当您想要启动备份时，请继续激活ONTAP卷上的备份。

激活**ONTAP**卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- [选择要备份的卷]
- [定义备份策略]
- [检查您的选择]

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：
   - 从控制台*系统*页面中，选择系统，然后选择右侧面板中备份和恢复旁边的*启用>备份卷*。

     如果备份的 Azure 目标作为系统存在于 系统 页面上，则可以将ONTAP集群拖到 Azure Blob 对象存储上。

   - 在备份和恢复栏中选择*卷*。从卷选项卡中，选择*操作*•••图标并选择单个卷（尚未启用复制或备份到对象存储）的*激活备份*。

向导的介绍页面显示保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。

2. 继续以下选项：
   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您还没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷。 （一次只能选择一个FlexGroup卷。）要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及设置以下选项：

- 您是否需要一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构
- 本地快照策略
- 复制目标和策略

如果您选择的卷具有与您在此步骤中选择的策略不同的快照和复制策略，则现有策略将被覆盖。

- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：如果您正在执行复制或备份到对象存储，则必须创建本地快照。

- 复制：在另一个ONTAP存储系统上创建复制卷。
- 备份：将卷备份到对象存储。

2. 架构：如果您选择复制和备份，请选择以下信息流之一：
   - 级联：信息从主存储系统流向辅助存储系统，再从辅助存储系统流向对象存储。
   - 扇出：信息从主存储系统流向辅助存储系统，再从主存储系统流向对象存储。

   有关这些架构的详细信息，请参阅"规划您的保护之旅"。

3. 本地快照：选择现有的快照策略或创建一个。

   要在激活快照之前创建自定义策略，请参阅"创建策略"。

   要创建策略，请选择“创建新策略”并执行以下操作：

   - 输入策略的名称。
   - 选择最多五个时间表，通常频率不同。
   - 选择“创建”。

4. 复制：设置以下选项：
   - 复制目标：选择目标系统和 SVM。或者，选择将添加到复制卷名称的目标聚合或聚合以及前缀或后缀。
   - 复制策略：选择现有的复制策略或创建一个。

     要在激活复制之前创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：

     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。

5. 备份到对象：如果您选择了*备份*，请设置以下选项：
   - 提供商：选择*Microsoft Azure*。
   - 提供商设置：输入提供商详细信息。

     输入存储备份的区域。这可能与Cloud Volumes ONTAP系统所在的区域不同。

     创建一个新的存储帐户或选择一个现有的存储帐户。

     输入用于存储备份的 Azure 订阅。这可能是与Cloud Volumes ONTAP系统所在的订阅不同的订阅。

     创建自己的管理 Blob 容器的资源组，或者选择资源组类型和组。

     如果您想保护备份文件不被修改或删除，请确保创建存储帐户时启用了 30 天保留期的不可变存储。

- 加密密钥：如果您创建了新的 Azure 存储帐户，请输入提供商提供给您的加密密钥信息。选择是否使用默认 Azure 加密密钥，或者从 Azure 帐户中选择您自己的客户管理密钥来管理数据加密。

  如果您选择使用自己的客户管理密钥，请输入密钥保管库和密钥信息。 "了解如何使用自己的密钥" 。

  如果您选择了现有的 Microsoft 存储帐户，则加密信息已经可用，因此您现在无需输入。

- 网络：选择 IP 空间，以及是否使用私有端点。默认情况下，私有端点是禁用的。
  i. 您要备份的卷所在的ONTAP集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
  ii. 或者，选择是否使用之前配置的 Azure 专用终结点。 "了解如何使用 Azure 专用终结点" 。
- 备份策略：选择现有的备份到对象存储策略。

  要在激活备份之前创建自定义策略，请参阅"创建策略"。

  要创建策略，请选择“创建新策略”并执行以下操作：

  - 输入策略的名称。
  - 对于备份到对象策略，设置 DataLock 和 Ransomware Resilience 设置。有关 DataLock 和勒索软件恢复的详细信息，请参阅"备份到对象策略设置"。
  - 选择最多五个时间表，通常频率不同。
  - 选择“创建”。
- 将现有快照导出到对象存储作为备份副本：如果此系统中存在与您刚刚为此系统选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框可将所有历史快照复制到对象存储作为备份文件，以确保对您的卷进行最全面的保护。

6. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中复选框*自动将快照策略标签与复制和备份策略标签同步*。这将创建具有与复制和备份策略中的标签匹配的标签的快照。
3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括主存储系统数据的完整副本。后续传输包含快照中包含的主存储数据的差异副本。

在目标集群中创建一个复制卷，该复制卷将与主卷同步。

在您输入的资源组中创建一个 Blob 存储容器，并将备份文件存储在那里。

默认情况下， NetApp Backup and Recovery为 Blob 容器提供本地冗余 (LRS) 以优化成本。如果您想确保数据

在不同区域之间复制，则可以将此设置更改为区域冗余（ZRS）。请参阅 Microsoft 说明 "更改存储帐户的复制方式"。

显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

下一步是什么？

- 你可以"管理您的备份文件和备份策略"。这包括启动和停止备份、删除备份、添加和更改备份计划等。
- 你可以"管理集群级备份设置"。这包括更改ONTAP用于访问云存储的存储密钥、更改可用于将备份上传到对象存储的网络带宽、更改未来卷的自动备份设置等等。
- 您还可以"从备份文件恢复卷、文件夹或单个文件"到 AWS 中的Cloud Volumes ONTAP系统，或到本地ONTAP系统。

使用NetApp Backup and Recovery将Cloud Volumes ONTAP数据备份到 Google Cloud Storage

完成NetApp Backup and Recovery中的几个步骤，开始将卷数据从Cloud Volumes ONTAP系统备份到 Google Cloud Storage。

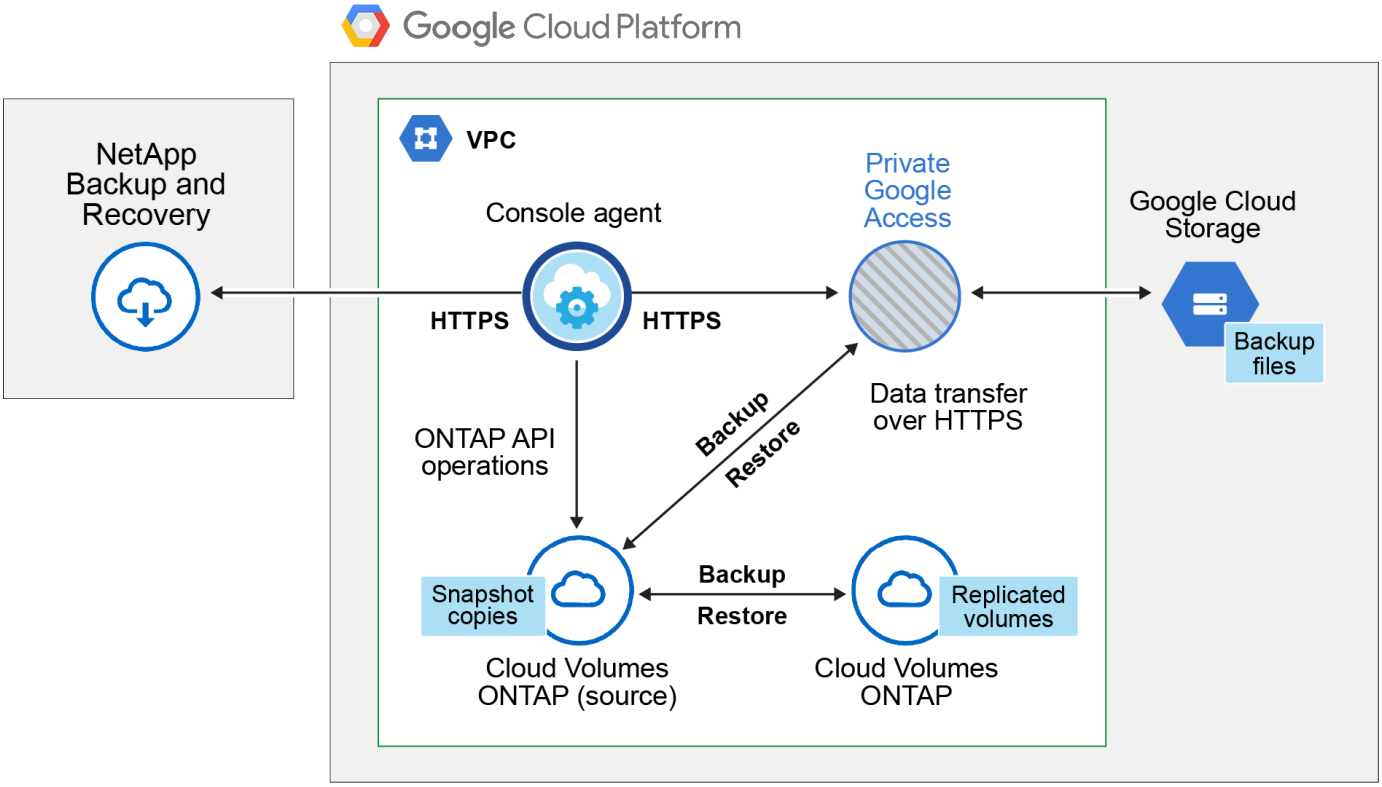
要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

验证对您的配置的支持

在开始将卷备份到 Google Cloud Storage 之前，请阅读以下要求以确保您具有受支持的配置。

下图显示了每个组件以及您需要在它们之间准备的连接。

或者，您也可以使用公共或私有连接连接到用于复制卷的辅助ONTAP系统。



支持的 **ONTAP** 版本

最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。

支持的 **GCP** 区域

所有 GCP 区域均支持NetApp Backup and Recovery。

GCP 服务帐户

您需要在 Google Cloud 项目中拥有一个具有自定义角色的服务帐户。 "了解如何创建服务帐号" 。

启用NetApp Backup and Recovery来访问 Google Cloud Storage 存储桶的服务帐户不再需要存储管理员角色。

验证许可证要求

对于NetApp Backup and Recovery PAYGO 许可，可在 Google Marketplace 中订阅控制台，从而实现Cloud Volumes ONTAP和NetApp Backup and Recovery 的部署。你需要 "订阅此控制台订阅"在启用NetApp Backup and Recovery之前。 NetApp Backup and Recovery的计费通过此订阅完成。 "您可以从系统向导的“详细信息和凭证”页面进行订阅" 。

对于NetApp Backup and RecoveryBYOL 许可，您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。"了解如何管理您的 BYOL 许可证"。

并且您需要向 Google 订阅用于存储备份的存储空间。

准备控制台代理

控制台代理必须安装在可以访问互联网的 Google 区域。

- "了解控制台代理"
- "在 Google Cloud 中部署控制台代理"

验证或添加控制台代理的权限

要使用NetApp Backup and Recovery的“搜索和恢复”功能，您需要在控制台代理的角色中拥有特定权限，以便它可以访问 Google Cloud BigQuery 服务。请参阅下面的权限，如果需要修改策略，请按照以下步骤操作。

步骤

1. 在 "Google 云端控制台"，转到*角色*页面。
2. 使用页面顶部的下拉列表，选择包含要编辑的角色的项目或组织。
3. 选择自定义角色。
4. 选择*编辑角色*来更新角色的权限。
5. 选择*添加权限*为角色添加以下新权限。

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. 选择*更新*以保存编辑的角色。

使用客户管理的加密密钥 **(CMEK)** 所需的信息

您可以使用自己的客户管理密钥进行数据加密，而不是使用默认的 Google 管理加密密钥。跨区域和跨项目密钥均受支持，因此您可以为存储桶选择与 CMEK 密钥的项目不同的项目。如果您打算使用自己的客户管理密钥：

- 您需要有密钥环和密钥名称，以便可以在激活向导中添加此信息。 "了解有关客户管理加密密钥的更多信息"。
- 您需要验证控制台代理的角色是否包含这些必需的权限：

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 您需要验证您的项目中是否启用了 Google“云密钥管理服务 (KMS)”API。查看 "Google Cloud 文档：启用 API"了解详情。

CMEK 注意事项：

- 支持 HSM（硬件支持）和软件生成的密钥。
- 支持新创建或导入的 Cloud KMS 密钥。
- 仅支持区域密钥；不支持全局密钥。
- 目前仅支持“对称加密/解密”目的。
- NetApp Backup and Recovery为与存储帐户关联的服务代理分配了“CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)”IAM 角色。

创建您自己的存储桶

默认情况下，该服务会为您创建存储桶。如果您想使用自己的存储桶，您可以在启动备份激活向导之前创建它们，然后在向导中选择这些存储桶。

"了解有关创建您自己的存储桶的更多信息"。

验证**ONTAP**复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地**ONTAP**网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。
- 要在不同子网中的两个Cloud Volumes ONTAP系统之间复制数据，子网必须一起路由（这是默认设置）。

在Cloud Volumes ONTAP上启用NetApp Backup and Recovery

启用NetApp Backup and Recovery步骤略有不同，具体取决于您拥有的是现有Cloud Volumes ONTAP系统还是新系统。

在新系统上启用NetApp Backup and Recovery

当您完成系统向导以创建新的Cloud Volumes ONTAP系统时，可以启用NetApp Backup and Recovery 。

您必须已经配置了服务帐户。如果在创建Cloud Volumes ONTAP系统时未选择服务帐户，则需要关闭系统并从 GCP 控制台将服务帐户添加到Cloud Volumes ONTAP 。

看 "在 GCP 中启动Cloud Volumes ONTAP"了解创建Cloud Volumes ONTAP系统的要求和详细信息。

步骤

1. 从控制台*系统*页面，选择*添加系统*，选择云提供商，然后选择*添加新*。选择“创建Cloud Volumes ONTAP”。
2. 选择位置：选择*Google Cloud Platform*。
3. 选择类型：选择* Cloud Volumes ONTAP*（单节点或高可用性）。
4. 详细信息和凭证：输入以下信息：
   a. 如果您要使用的项目与默认项目（控制台代理所在的项目）不同，请单击“编辑项目”并选择一个新项目。
   b. 指定集群名称。
   c. 启用*服务帐户*开关并选择具有预定义存储管理员角色的服务帐户。这是启用备份和分层所必需的。
   d. 指定凭据。

      确保已订阅 GCP Marketplace。
5. 服务：保持NetApp Backup and Recovery处于启用状态，然后单击*继续*。
6. 完成向导中的页面以部署系统，如中所述 "在 GCP 中启动Cloud Volumes ONTAP"。

结果

系统上已启用NetApp Backup and Recovery 。在这些Cloud Volumes ONTAP系统上创建卷后，启动NetApp Backup and Recovery并"在您想要保护的每个卷上激活备份"。

在现有系统上启用NetApp Backup and Recovery

您可以随时直接从系统启用NetApp Backup and Recovery 。

步骤

1. 从控制台*系统*页面中，选择系统并选择右侧面板中备份和恢复旁边的*启用*。

   如果您的备份的 Google Cloud Storage 目标作为系统存在于控制台*系统*页面上，则可以将集群拖到 Google Cloud Storage 系统上以启动设置向导。

准备 Google Cloud Storage 作为备份目标

准备 Google Cloud Storage 作为备份目标涉及以下步骤：

- 设置权限。
- （可选）创建您自己的存储桶。 （如果您愿意，该服务将为您创建存储桶。）
- （可选）设置客户管理的密钥以进行数据加密

设置权限

您需要使用自定义角色为具有特定权限的服务帐户提供存储访问密钥。服务帐户使NetApp Backup and Recovery能够验证和访问用于存储备份的 Cloud Storage 存储桶。需要密钥，以便 Google Cloud Storage 知道谁在发出请求。

步骤

1. 在 "Google 云端控制台"，转到*角色*页面。
2. "创建新角色"具有以下权限：

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. 在 Google Cloud 控制台中， "前往服务帐户页面" 。
4. 选择您的云项目。
5. 选择*创建服务帐户*并提供所需信息：
   a. 服务帐户详细信息：输入名称和描述。
   b. 授予此服务帐户访问项目的权限：选择您刚刚创建的自定义角色。
   c. 选择*完成*。
6. 前往 "GCP 存储设置"并为服务帐户创建访问密钥：
   a. 选择一个项目，然后选择*互操作性*。如果您还没有这样做，请选择*启用互操作性访问*。
   b. 在*服务帐户的访问密钥*下，选择*为服务帐户创建密钥*，选择刚刚创建的服务帐户，然后单击*创建密钥*。

      稍后配置备份服务时，您需要在NetApp Backup and Recovery中输入密钥。

创建您自己的存储桶

默认情况下，该服务会为您创建存储桶。或者，如果您想使用自己的存储桶，您可以在启动备份激活向导之前创建它们，然后在向导中选择这些存储桶。

"了解有关创建您自己的存储桶的更多信息"。

设置客户管理的加密密钥 **(CMEK)** 以进行数据加密

您可以使用自己的客户管理密钥进行数据加密，而不是使用默认的 Google 管理加密密钥。跨区域和跨项目密钥均受支持，因此您可以为存储桶选择与 CMEK 密钥的项目不同的项目。

如果您打算使用自己的客户管理密钥：

- 您需要有密钥环和密钥名称，以便可以在激活向导中添加此信息。 "了解有关客户管理加密密钥的更多信息"。
- 您需要验证控制台代理的角色是否包含这些必需的权限：

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 您需要验证您的项目中是否启用了 Google“云密钥管理服务 (KMS)”API。查看 "Google Cloud 文档：启用 API"了解详情。

CMEK 注意事项：

- 支持 HSM（硬件支持）和软件生成的密钥。
- 支持新创建或导入的 Cloud KMS 密钥。
- 仅支持区域密钥，不支持全局密钥。
- 目前仅支持“对称加密/解密”目的。
- NetApp Backup and Recovery为与存储帐户关联的服务代理分配了“CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)”IAM 角色。

激活**ONTAP**卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- [选择要备份的卷]
- [定义备份策略]

- [检查您的选择]

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：
   - 从控制台*系统*页面*中，选择系统并选择右侧面板中备份和恢复旁边的*启用>备份卷*。

     如果备份的 GCP 目标作为系统存在于控制台*系统*页面上，则可以将ONTAP集群拖到 GCP 对象存储上。
   - 在备份和恢复栏中选择*卷*。从卷选项卡中，选择*操作*•••图标并选择单个卷（尚未启用复制或备份到对象存储）的*激活备份*。

   向导的介绍页面显示保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。
2. 继续以下选项：
   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您还没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

请注意，如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷（FlexGroup卷一次只能选择一个）。要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及设置以下选项：

- 您是否需要一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构
- 本地快照策略
- 复制目标和策略

> 如果您选择的卷具有与您在此步骤中选择的策略不同的快照和复制策略，则现有策略将被覆盖。

- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：如果您正在执行复制或备份到对象存储，则必须创建本地快照。
   - 复制：在另一个ONTAP存储系统上创建复制卷。
   - 备份：将卷备份到对象存储。
2. 架构：如果您选择复制和备份，请选择以下信息流之一：
   - 级联：信息从主存储系统流向辅助存储系统，再从辅助存储系统流向对象存储。
   - 扇出：信息从主存储系统流向辅助存储系统，再从主存储系统流向对象存储。

   有关这些架构的详细信息，请参阅"规划您的保护之旅"。
3. 本地快照：选择现有的快照策略或创建一个。

   > 要在激活备份之前创建自定义策略，请参阅"创建策略"。

   要创建策略，请选择“创建新策略”并执行以下操作：
   - 输入策略的名称。
   - 选择最多五个时间表，通常频率不同。
   - 对于备份到对象策略，配置 Datalock 和 Ransomware Resilience。有关 Datalock 和勒索软件恢复的详细信息，请参阅"备份到对象策略设置"。
   - 选择“创建”。
4. 复制：设置以下选项：
   - 复制目标：选择目标系统和 SVM。或者，选择将添加到复制卷名称的目标聚合或聚合以及前缀或后缀。
   - 复制策略：选择现有的复制策略或创建一个。

     > 要在激活复制之前创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：
     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。

- 选择“创建”。

5. 备份到对象：如果您选择了*备份*，请设置以下选项：
   - 提供商：选择*Google Cloud*。
   - 提供商设置：输入提供商详细信息和存储备份的区域。

     创建新存储桶或选择现有存储桶。

   - 加密密钥：如果您创建了新的 Google 存储桶，请输入提供商提供给您的加密密钥信息。选择是否使用默认的 Google Cloud 加密密钥，或者从您的 Google 帐户中选择您自己的客户管理密钥来管理您的数据加密。

     如果您选择使用自己的客户管理密钥，请输入密钥保管库和密钥信息。

     如果您选择了现有的 Google Cloud 存储桶，则加密信息已经可用，因此您现在无需输入。

   - 备份策略：选择现有的备份到对象存储策略或创建一个。

     要在激活备份之前创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：

     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。

   - 将现有快照导出到对象存储作为备份副本：如果此系统中存在与您刚刚为此系统选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框可将所有历史快照复制到对象存储作为备份文件，以确保对您的卷进行最全面的保护。
6. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中复选框*自动将快照策略标签与复制和备份策略标签同步*。这将创建具有与复制和备份策略中的标签匹配的标签的快照。
3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括主存储系统数据的完整副本。后续传输包含快照中包含的主存储系统数据的差异副本。

在目标集群中创建一个复制卷，该卷将与主存储系统卷同步。

在您输入的 Google 访问密钥和密钥所指示的服务帐户中创建一个 Google Cloud Storage 存储桶，并将备份文件存储在那里。

默认情况下，备份与_Standard_存储类相关联。您可以使用成本较低的_Nearline_、_Coldline_或_Archive_存储类。但是，您通过 Google 配置存储类，而不是通过NetApp Backup and Recovery UI。请参阅 Google 主题 "更改存储桶的默认存储类别"了解详情。

显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

下一步是什么?

- 你可以"管理您的备份文件和备份策略"。这包括启动和停止备份、删除备份、添加和更改备份计划等。
- 你可以"管理集群级备份设置"。这包括更改ONTAP用于访问云存储的存储密钥、更改可用于将备份上传到对象存储的网络带宽、更改未来卷的自动备份设置等等。
- 您还可以"从备份文件恢复卷、文件夹或单个文件"到 AWS 中的Cloud Volumes ONTAP系统，或到本地ONTAP系统。

使用**NetApp Backup and Recovery**将本地**ONTAP**数据备份到 **Amazon S3**

完成NetApp Backup and Recovery中的几个步骤，开始将卷数据从本地ONTAP系统备份到二级存储系统和 Amazon S3 云存储。

“本地ONTAP系统”包括FAS、 AFF和ONTAP Select系统。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

识别连接方法

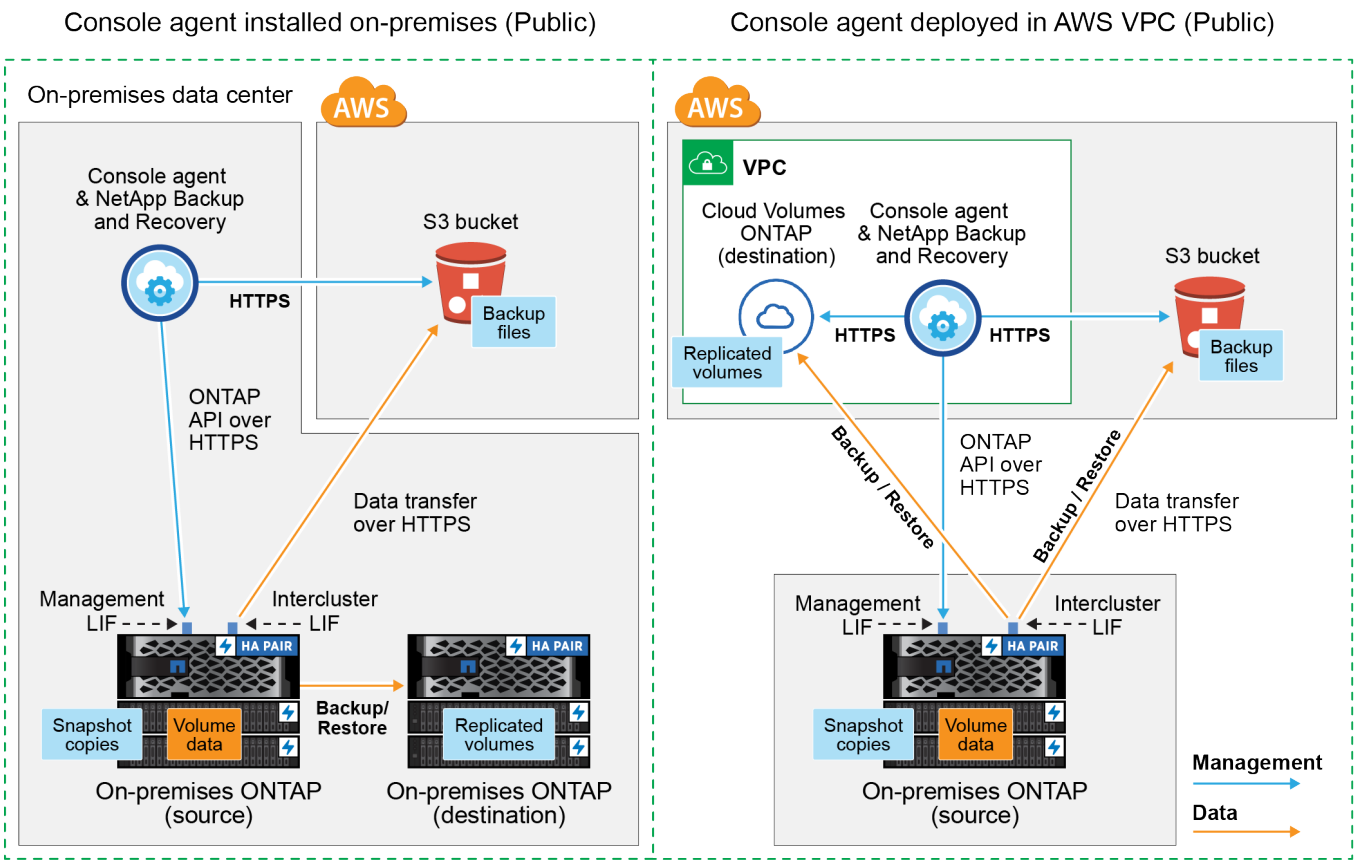
选择在配置从本地ONTAP系统到 AWS S3 的备份时要使用的两种连接方法中的哪一种。

- 公共连接 - 使用公共 S3 端点将ONTAP系统直接连接到 AWS S3。
- 私人连接 - 使用 VPN 或 AWS Direct Connect 并通过使用私人 IP 地址的 VPC Endpoint 接口路由流量。

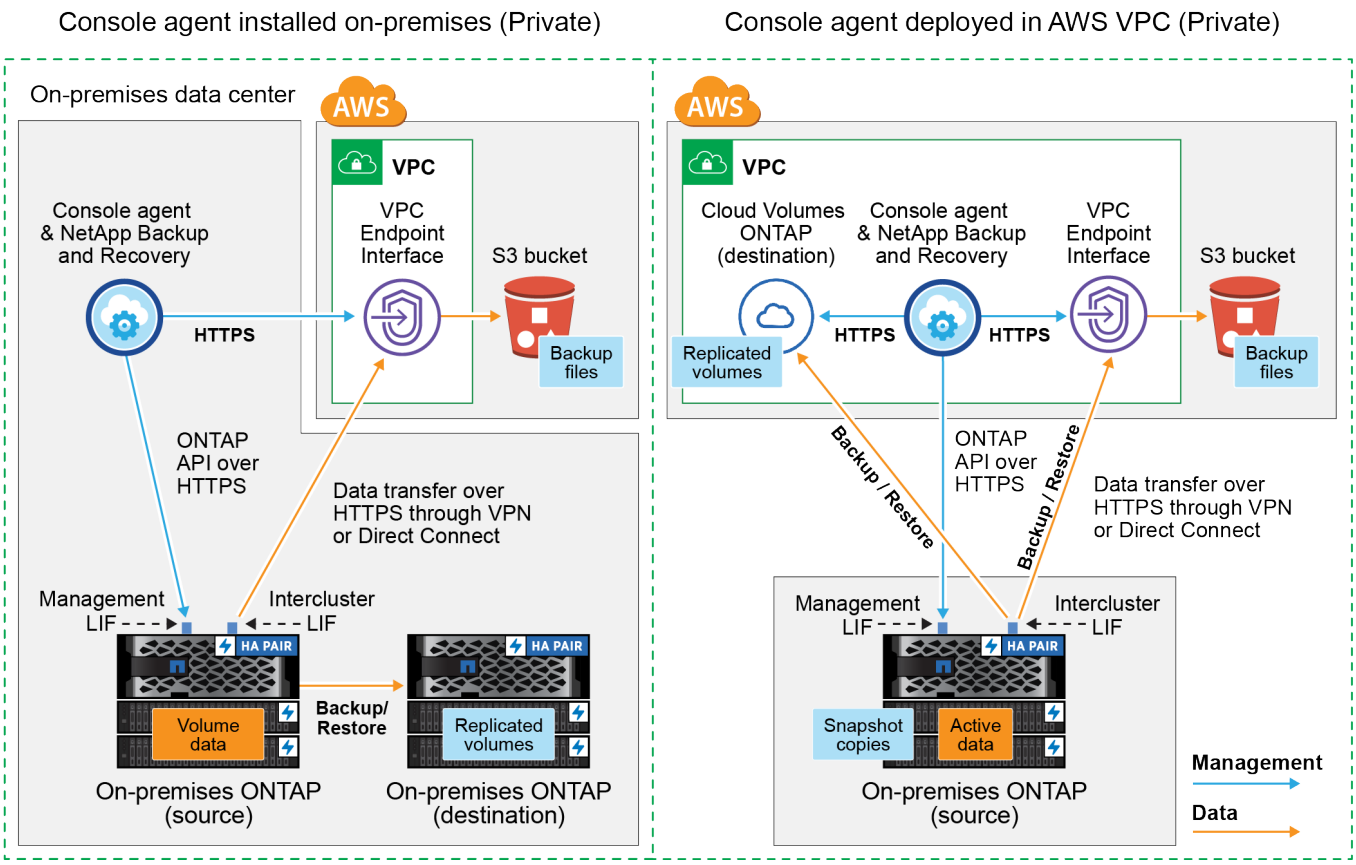
或者，您也可以使用公共或私有连接连接到用于复制卷的辅助ONTAP系统。

下图显示了*公共连接*方法以及您需要在组件之间准备的连接。您可以使用在您的场所安装的控制台代理，或者

在 AWS VPC 中部署的控制台代理。



下图显示了*私有连接*方法以及您需要在组件之间准备的连接。您可以使用在您的场所安装的控制台代理，或者在 AWS VPC 中部署的控制台代理。



准备控制台代理

控制台代理是NetApp Console功能的主要软件。需要控制台代理来备份和恢复您的ONTAP数据。

创建或切换控制台代理

如果您已经在 AWS VPC 或您的场所部署了控制台代理，那么一切就绪了。

如果没有，那么您需要在其中一个位置创建一个控制台代理，以将ONTAP数据备份到 AWS S3 存储。您不能使用部署在其他云提供商的控制台代理。

- "了解控制台代理"
- "在 AWS 中安装控制台代理"
- "在您的场所安装控制台代理"
- "在 AWS GovCloud 区域安装控制台代理"

  当控制台代理部署在云中时（而不是安装在您的场所中时）， NetApp Backup and Recovery在 GovCloud 区域受支持。此外，您必须从 AWS Marketplace 部署控制台代理。您无法从NetApp Console SaaS 网站在政府区域部署控制台代理。

准备控制台代理网络要求

确保满足以下网络要求：

- 确保安装控制台代理的网络启用以下连接：
  - 通过端口 443 建立到NetApp Backup and Recovery以及 S3 对象存储的 HTTPS 连接("查看端点列表")
  - 通过端口 443 建立到ONTAP集群管理 LIF 的 HTTPS 连接
  - AWS 和 AWS GovCloud 部署需要额外的入站和出站安全组规则。看 "AWS 中的控制台代理规则"了解详情。
- 如果您有从ONTAP集群到 VPC 的 Direct Connect 或 VPN 连接，并且您希望控制台代理和 S3 之间的通信保持在 AWS 内部网络（*私有*连接）中，则需要启用到 S3 的 VPC 端点接口。使用 VPC 终端节点接口配置系统以进行私有连接。

验证许可证要求

您需要验证 AWS 和NetApp Console的许可证要求：

- 在为集群激活NetApp Backup and Recovery之前，您需要订阅 AWS 提供的即用即付 (PAYGO) NetApp Console Marketplace，或者从NetApp购买并激活NetApp Backup and Recovery BYOL 许可证。这些许可证适用于您的帐户，可以在多个系统中使用。
  - 对于NetApp Backup and Recovery PAYGO 许可，您需要订阅 "AWS Marketplace 提供的NetApp Console"。 NetApp Backup and Recovery的计费通过此订阅完成。
  - 对于NetApp Backup and RecoveryBYOL 许可，您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。
- 您需要订阅用于存储备份的对象存储空间的 AWS。

支持地区

您可以在所有区域（包括 AWS GovCloud 区域）中从本地系统创建到 Amazon S3 的备份。您在设置服务时指定存储备份的区域。

准备**ONTAP**集群

准备源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统。

准备ONTAP集群涉及以下步骤：

- 在NetApp Console中发现您的ONTAP系统
- 验证ONTAP系统要求
- 验证ONTAP网络要求以将数据备份到对象存储
- 验证ONTAP复制卷的网络要求

在**NetApp Console**中发现您的**ONTAP**系统

您的源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统都必须在NetApp Console*系统*页面上可用。

您需要知道集群管理 IP 地址和管理员用户帐户的密码才能添加集群。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["了解如何发现集群"^]。

验证ONTAP系统要求

确保您的ONTAP系统满足以下要求：

- 最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。
- SnapMirror许可证（包含在高级捆绑包或数据保护捆绑包中）。

  *注意：*使用NetApp Backup and Recovery时不需要“混合云捆绑包”。

  了解如何 "管理您的集群许可证"。

- 时间和时区设置正确。了解如何 "配置集群时间"。
- 如果您复制数据，请检查源系统和目标系统是否运行兼容的ONTAP版本。

  "查看与SnapMirror关系兼容的ONTAP版本"。

验证ONTAP网络要求以将数据备份到对象存储

您必须在连接到对象存储的系统上配置以下要求。

- 对于扇出备份架构，请在主系统上配置以下设置。
- 对于级联备份架构，请在_辅助_系统上配置以下设置。

需要满足以下ONTAP集群网络要求：

- 集群需要从控制台代理到集群管理 LIF 的入站 HTTPS 连接。
- 每个托管要备份的卷的ONTAP节点上都需要一个集群间 LIF。这些集群间 LIF 必须能够访问对象存储。

  集群通过端口 443 启动从集群间 LIF 到 Amazon S3 存储的出站 HTTPS 连接，以执行备份和还原操作。ONTAP从对象存储读取和写入数据 - 对象存储从不启动，它只是响应。

- 集群间 LIF 必须与ONTAP用于连接对象存储的 *IPspace* 相关联。 "了解有关 IP 空间的更多信息" 。

  当您设置NetApp Backup and Recovery时，系统会提示您输入要使用的 IP 空间。您应该选择与这些 LIF 关联的 IP 空间。这可能是“默认” IP 空间或您创建的自定义 IP 空间。

  如果您使用的 IP 空间与“默认”不同，那么您可能需要创建静态路由来访问对象存储。

  IP 空间内的所有集群间 LIF 都必须具有对象存储的访问权限。如果您无法为当前 IP 空间配置此功能，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。

- 必须为卷所在的存储虚拟机配置 DNS 服务器。了解如何 "为 SVM 配置 DNS 服务"。
- 如有必要，请更新防火墙规则，以允许NetApp Backup and Recovery通过端口 443 从ONTAP连接到对象存储，并通过端口 53（TCP/UDP）从存储虚拟机到 DNS 服务器的名称解析流量。
- 如果您在 AWS 中使用私有 VPC 接口端点进行 S3 连接，那么为了使用 HTTPS/443，您需要将 S3 端点证书加载到ONTAP集群中。使用 VPC 终端节点接口配置系统以进行私有连接。
- 确保您的ONTAP集群有权访问 S3 存储桶。

验证ONTAP复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地ONTAP网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。

准备 Amazon S3 作为备份目标

准备 Amazon S3 作为备份目标涉及以下步骤：

- 设置 S3 权限。
- （可选）创建您自己的 S3 存储桶。 （如果您愿意，该服务将为您创建存储桶。）
- （可选）设置客户管理的 AWS 密钥以进行数据加密。
- （可选）使用 VPC 终端节点接口配置系统以进行私有连接。

设置 S3 权限

您需要配置两组权限：

- 控制台代理创建和管理 S3 存储桶的权限。
- 本地ONTAP集群的权限，以便它可以读取和写入 S3 存储桶的数据。

步骤

1. 确保控制台代理具有所需的权限。有关详细信息，请参阅 "NetApp Console策略权限"。

   在 AWS 中国区域创建备份时，您需要将 IAM 策略中所有_Resource_部分下的 AWS 资源名称“arn”从“aws”更改为“aws-cn”；例如 `arn:aws-cn:s3:::netapp-backup-*`。

2. 当您激活该服务时，备份向导将提示您输入访问密钥和密钥。这些凭证被传递到ONTAP集群，以便ONTAP可以将数据备份和恢复到 S3 存储桶。为此，您需要创建具有以下权限的 IAM 用户。

   请参阅 "AWS 文档：创建角色以将权限委托给 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"
    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:PutObject",
        "s3:DeleteObject",
        "s3:ListAllMyBuckets",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:RestoreObject",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetObjectRetention",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutObjectRetention"
      ],
      "Resource": "arn:aws:s3:::netapp-backup*/*",
      "Effect": "Allow"
    }
  ]
}
```

创建您自己的存储桶

默认情况下，该服务会为您创建存储桶。或者，如果您想使用自己的存储桶，您可以在启动备份激活向导之前创建它们，然后在向导中选择这些存储桶。

"了解有关创建您自己的存储桶的更多信息"。

如果您创建自己的存储桶，则应使用存储桶名称“netapp-backup”。如果需要使用自定义名称，请编辑 `ontapcloud-instance-policy-netapp-backup`为现有 CVO 添加 IAMRole，并将以下 JSON 块添加到 S3 权限中 `Statement`大批。您需要包括 `"Resource": "arn:aws:s3:::*"`并分配与存储桶关联的所有必要权限。

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

设置客户管理的 **AWS** 密钥以进行数据加密

如果您想使用默认的 Amazon S3 加密密钥来加密您的本地集群和 S3 存储桶之间传递的数据，那么您已经完成了所有设置，因为默认安装使用这种类型的加密。

如果您想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，那么您需要在启动NetApp Backup and Recovery向导之前设置加密管理密钥。

"请参阅如何在Cloud Volumes ONTAP中使用您自己的 Amazon 加密密钥"。

"请参阅如何在NetApp Backup and Recovery中使用您自己的 Amazon 加密密钥"。

使用 VPC 终端节点接口配置系统以进行私有连接

如果您想使用标准公共互联网连接，那么所有权限都由控制台代理设置，您无需执行任何其他操作。

如果您希望通过互联网从本地数据中心到 VPC 建立更安全的连接，则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 通过使用私有 IP 地址的 VPC 终端节点接口连接您的本地系统，则需要它。

步骤

1. 使用 Amazon VPC 控制台或命令行创建接口终端节点配置。 "请参阅有关使用 AWS PrivateLink for Amazon S3 的详细信息" 。
2. 修改与控制台代理关联的安全组配置。您必须将策略更改为“自定义”（从“完全访问”），并且您必须从备份策略添加 S3 权限如前所示。

   如果您使用端口 80（HTTP）与私有端点进行通信，则一切就绪。您现在可以在集群上启用NetApp Backup and Recovery。

   如果您使用端口 443（HTTPS）与私有端点通信，则必须从 VPC S3 端点复制证书并将其添加到您的ONTAP集群，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。
4. 从 VPC S3 端点获取证书。你可以通过以下方式做到这一点 "登录到托管控制台代理的虚拟机"并运行以下命令。输入端点的 DNS 名称时，在开头添加“bucket”，替换“*”：

   ```
   openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
   ```

5. 从此命令的输出中，复制 S3 证书的数据（BEGIN / END CERTIFICATE 标签之间（包括 BEGIN / END CERTIFICATE 标签）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-----
   ```

6. 登录ONTAP集群 CLI 并使用以下命令应用您复制的证书（替换您自己的存储虚拟机名称）：

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

激活**ONTAP**卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- [选择要备份的卷]
- [定义备份策略]
- [检查您的选择]

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：
   - 从控制台*系统*页面中，选择系统，然后选择右侧面板中备份和恢复旁边的*启用>备份卷*。

     如果备份的 Amazon S3 目标作为系统存在于控制台*系统*页面上，则可以将ONTAP集群拖到 Amazon S3 对象存储上。

   - 在备份和恢复栏中选择*卷*。从卷选项卡中，选择*操作*•••图标并选择单个卷（尚未启用复制或备份到对象存储）的*激活备份*。

   向导的介绍页面显示保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。
2. 继续以下选项：
   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您还没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷（FlexGroup卷一次只能选择一个）。要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及设置以下选项：

- 您是否需要一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构
- 本地快照策略
- 复制目标和策略

> 如果您选择的卷具有与您在此步骤中选择的策略不同的快照和复制策略，则现有策略将被覆盖。

- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：如果您正在执行复制或备份到对象存储，则必须创建本地快照。
   - 复制：在另一个ONTAP存储系统上创建复制卷。
   - 备份：将卷备份到对象存储。
2. 架构：如果您选择复制和备份，请选择以下信息流之一：
   - 级联：信息从主存储流向辅助存储，再流向对象存储，再从辅助存储流向对象存储。
   - 扇出：信息从主存储流向辅助存储，再从主存储流向对象存储。

   有关这些架构的详细信息，请参阅"规划您的保护之旅"。
3. 本地快照：选择现有的快照策略或创建策略。

> 要在激活快照之前创建自定义策略，请参阅"创建策略"。

4. 要创建策略，请选择“创建新策略”并执行以下操作：
   - 输入策略的名称。
   - 选择最多五个时间表，通常频率不同。

- 对于备份到对象策略，设置 DataLock 和 Ransomware Resilience 设置。有关 DataLock 和勒索软件恢复的详细信息，请参阅"备份到对象策略设置"。

- 选择“创建”。

5. 复制：设置以下选项：
   - 复制目标：选择目标系统和 SVM。或者，选择将添加到复制卷名称的目标聚合或聚合以及前缀或后缀。
   - 复制策略：选择现有的复制策略或创建策略。

     要在激活复制之前创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：
     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。
6. 备份到对象：如果您选择了*备份*，请设置以下选项：
   - 提供商：选择*Amazon Web Services*。
   - 提供商设置：输入提供商详细信息和将存储备份的 AWS 区域。

     访问密钥和密钥适用于您创建的 IAM 用户，用于授予ONTAP集群对 S3 存储桶的访问权限。
   - 存储桶：选择现有的 S3 存储桶或创建一个新的。参考 "添加 S3 存储桶"。
   - 加密密钥：如果您创建了新的 S3 存储桶，请输入提供商提供给您的加密密钥信息。选择是否使用默认的 Amazon S3 加密密钥，或者从您的 AWS 账户中选择您自己的客户管理密钥来管理数据的加密。

     如果您选择了现有的存储桶，则加密信息已经可用，因此您现在无需输入。
   - 网络：选择 IP 空间，以及是否使用私有端点。默认情况下，私有端点是禁用的。
     i. 您要备份的卷所在的ONTAP集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
     ii. 或者，选择是否使用您之前配置的 AWS PrivateLink。 "查看有关将 AWS PrivateLink 用于 Amazon S3 的详细信息" 。
   - 备份策略：选择现有的备份策略或创建策略。

     要在激活备份之前创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：
     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。
   - 将现有快照导出到对象存储作为备份副本：如果此系统中存在与您刚刚为此系统选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框可将所有历史快照复制到对象存储作为备份文件，以确保对您的卷进行最全面的保护。

7. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中复选框*自动将快照策略标签与复制和备份策略标签同步*。这将创建具有与复制和备份策略中的标签匹配的标签的快照。
3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括主存储系统数据的完整副本。后续传输包含快照中所含主数据的差异副本。

在目标集群中创建一个复制卷，该卷将与主存储卷同步。

S3 存储桶在您输入的 S3 访问密钥和密钥指示的服务帐户中创建，并且备份文件存储在那里。显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

使用**NetApp Backup and Recovery**将本地**ONTAP**数据备份到 **Azure Blob** 存储

完成NetApp Backup and Recovery中的几个步骤，开始将卷数据从本地ONTAP系统备份到二级存储系统和 Azure Blob 存储。

“本地ONTAP系统”包括FAS、 AFF和ONTAP Select系统。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

识别连接方法

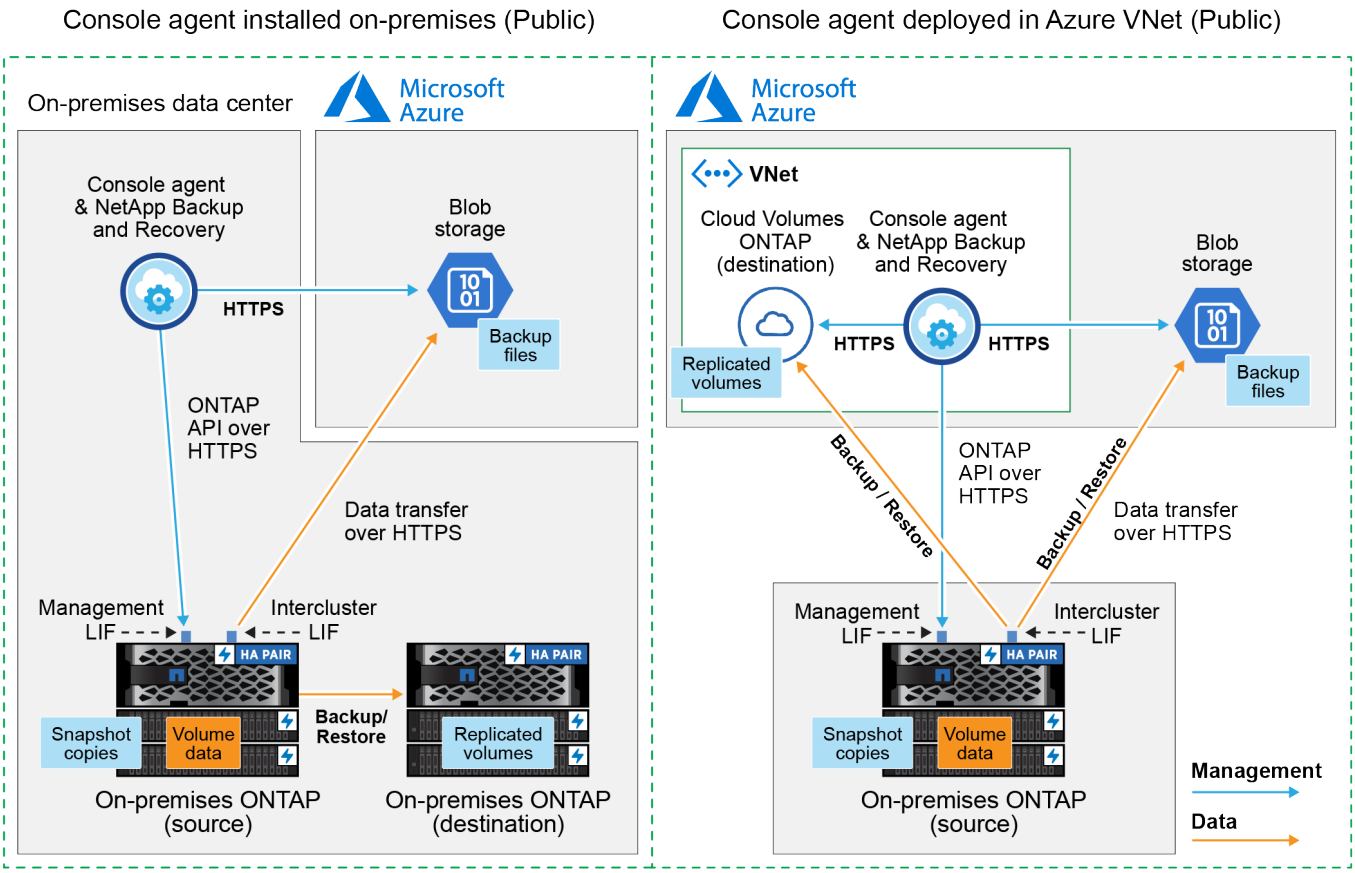
选择在配置从本地ONTAP系统到 Azure Blob 的备份时要使用的两种连接方法中的哪一种。

- 公共连接 - 使用公共 Azure 端点将ONTAP系统直接连接到 Azure Blob 存储。

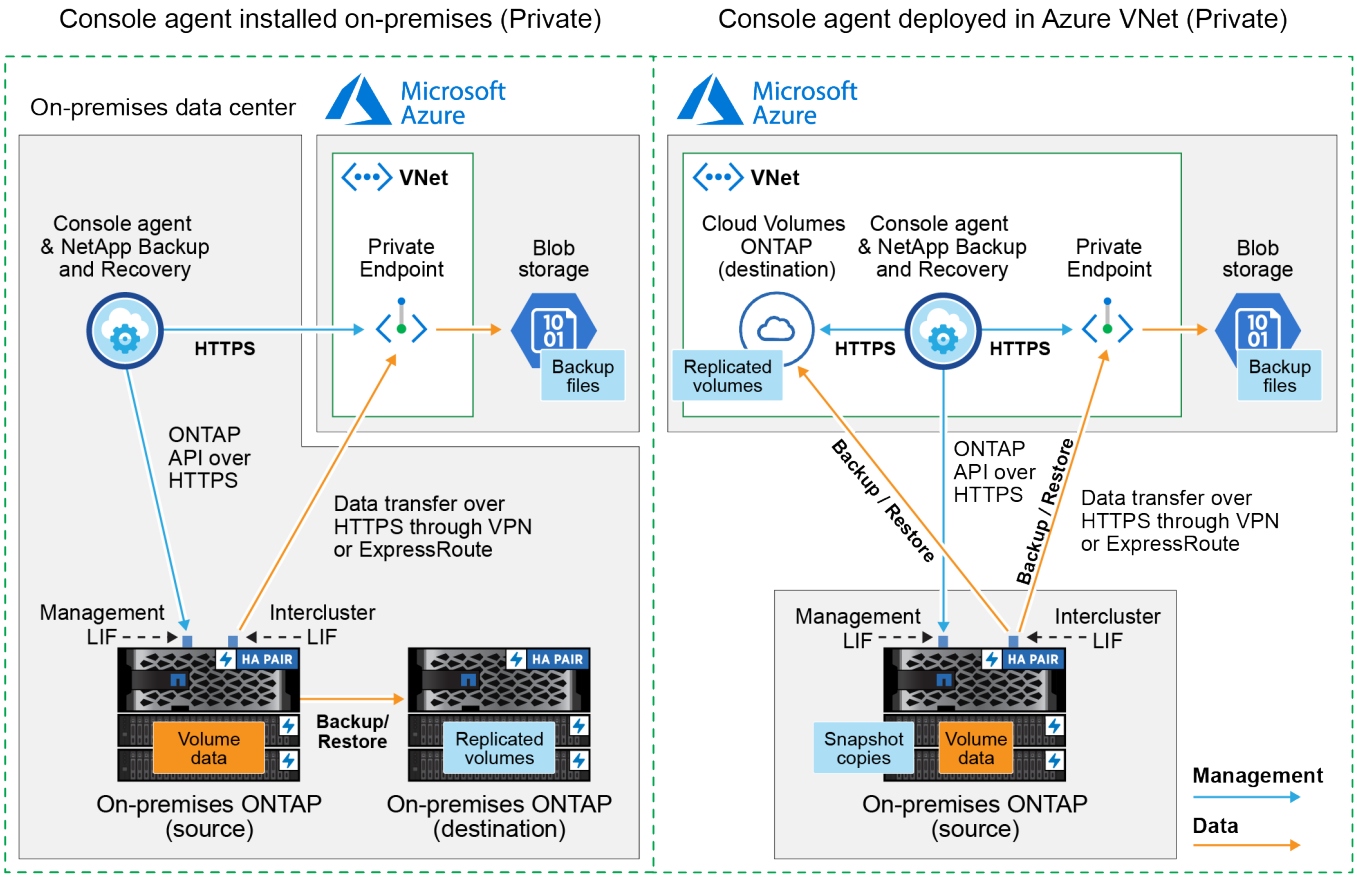
- 私人连接 - 使用 VPN 或 ExpressRoute 并通过使用私人 IP 地址的 VNet 私人端点路由流量。

或者，您也可以使用公共或私有连接连接到用于复制卷的辅助ONTAP系统。

下图显示了*公共连接*方法以及您需要在组件之间准备的连接。您可以使用已在本地安装的控制台代理，或者已在 Azure VNet 中部署的控制台代理。



下图显示了*私有连接*方法以及您需要在组件之间准备的连接。您可以使用已在本地安装的控制台代理，或者已在 Azure VNet 中部署的控制台代理。



准备控制台代理

控制台代理是NetApp Console功能的主要软件。需要控制台代理来备份和恢复您的ONTAP数据。

创建或切换控制台代理

如果您已经在 Azure VNet 或本地部署了控制台代理，那么一切就绪了。

如果没有，那么您需要在其中一个位置创建一个控制台代理，以将ONTAP数据备份到 Azure Blob 存储。您不能使用部署在其他云提供商的控制台代理。

- "了解控制台代理"
- "在 Azure 中安装控制台代理"
- "在您的场所安装控制台代理"
- "在 Azure 政府区域中安装控制台代理"

  当控制台代理部署在云中时（而不是安装在您的场所中时），Azure 政府区域支持NetApp Backup and Recovery。此外，您必须从 Azure 市场部署控制台代理。您无法从 Console SaaS 网站在政府区域部署 Console 代理。

为控制台代理准备网络

确保控制台代理具有所需的网络连接。

步骤

1. 确保安装控制台代理的网络启用以下连接：
   - 通过端口 443 建立到NetApp Backup and Recovery以及 Blob 对象存储的 HTTPS 连接("查看端点列表")
   - 通过端口 443 建立到ONTAP集群管理 LIF 的 HTTPS 连接
   - 为了使NetApp Backup and Recovery搜索与还原功能正常工作，必须打开端口 1433 以便控制台代理和 Azure Synapse SQL 服务之间进行通信。
   - Azure 和 Azure 政府部署需要额外的入站安全组规则。看 "Azure 中的控制台代理规则"了解详情。
2. 启用 VNet 专用终结点到 Azure 存储。如果您有从ONTAP集群到 VNet 的 ExpressRoute 或 VPN 连接，并且希望控制台代理和 Blob 存储之间的通信保持在虚拟专用网络（*专用*连接）中，则需要这样做。

验证或添加控制台代理的权限

要使用NetApp Backup and Recovery搜索和还原功能，您需要在控制台代理的角色中拥有特定权限，以便它可以访问 Azure Synapse 工作区和数据湖存储帐户。请参阅下面的权限，如果需要修改策略，请按照以下步骤操作。

开始之前

您必须向您的订阅注册 Azure Synapse Analytics 资源提供程序（称为“Microsoft.Synapse”）。 "了解如何为您的订阅注册此资源提供程序" 。您必须是订阅*所有者*或*贡献者*才能注册资源提供者。

步骤

1. 确定分配给控制台代理虚拟机的角色：
   a. 在 Azure 门户中，打开虚拟机服务。
   b. 选择控制台代理虚拟机。
   c. 在*设置*下，选择*身份*。
   d. 选择“Azure 角色分配”。
   e. 记下分配给控制台代理虚拟机的自定义角色。
2. 更新自定义角色：
   a. 在 Azure 门户中，打开你的 Azure 订阅。
   b. 选择“访问控制 (IAM)”>“角色”。
   c. 选择自定义角色的省略号（...），然后选择*编辑*。
   d. 选择 **JSON** 并添加以下权限：

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"查看策略的完整 JSON 格式"

e. 选择*审核 + 更新*，然后选择*更新*。

验证许可证要求

您需要验证 Azure 和控制台的许可证要求：

- 在为集群激活NetApp Backup and Recovery之前，您需要订阅 Azure 提供的即用即付 (PAYGO) 控制台市场，或者从NetApp购买并激活NetApp Backup and Recovery BYOL 许可证。这些许可证适用于您的帐户，可以在多个系统中使用。
  - 对于NetApp Backup and Recovery PAYGO 许可，您需要订阅 "Azure 市场提供的NetApp Console"。NetApp Backup and Recovery的计费通过此订阅完成。
  - 对于NetApp Backup and RecoveryBYOL 许可，您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。"了解如何管理您的 BYOL 许可证"。
- 您需要对用于存储备份的对象存储空间进行 Azure 订阅。

支持地区

您可以在所有区域（包括 Azure 政府区域）中创建从本地系统到 Azure Blob 的备份。您在设置服务时指定存储备份的区域。

准备**ONTAP**集群

准备源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统。

准备ONTAP集群涉及以下步骤：

- 在NetApp Console中发现您的ONTAP系统
- 验证ONTAP系统要求
- 验证ONTAP网络要求以将数据备份到对象存储
- 验证ONTAP复制卷的网络要求

在**NetApp Console**中发现您的**ONTAP**系统

您的源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统都必须在NetApp Console*系统*页面上可用。

您需要知道集群管理 IP 地址和管理员用户帐户的密码才能添加集群。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["了解如何发现集群"^]。

验证**ONTAP**系统要求

确保您的ONTAP系统满足以下要求：

- 最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。
- SnapMirror许可证（包含在高级捆绑包或数据保护捆绑包中）。

  *注意：*使用NetApp Backup and Recovery时不需要“混合云捆绑包”。

  了解如何 "管理您的集群许可证"。

- 时间和时区设置正确。了解如何 "配置集群时间"。

- 如果您复制数据，请检查源系统和目标系统是否运行兼容的ONTAP版本。

  "查看与SnapMirror关系兼容的ONTAP版本"。

验证**ONTAP**网络要求以将数据备份到对象存储

您必须在连接到对象存储的系统上配置以下要求。

- 对于扇出备份架构，请在主系统上配置以下设置。
- 对于级联备份架构，请在_辅助_系统上配置以下设置。

需要满足以下ONTAP集群网络要求：

- ONTAP集群通过端口 443 启动从集群间 LIF 到 Azure Blob 存储的 HTTPS 连接，以执行备份和还原操作。

  ONTAP从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。

- ONTAP需要从控制台代理到集群管理 LIF 的入站连接。控制台代理可以驻留在 Azure VNet 中。
- 每个托管要备份的卷的ONTAP节点上都需要一个集群间 LIF。 LIF 必须与ONTAP用于连接对象存储的 *IPspace* 相关联。 "了解有关 IP 空间的更多信息" 。

  当您设置NetApp Backup and Recovery时，系统会提示您输入要使用的 IP 空间。您应该选择与每个 LIF 关联的 IP 空间。这可能是“默认” IP 空间或您创建的自定义 IP 空间。

- 节点和集群间 LIF 能够访问对象存储。
- 已为卷所在的存储虚拟机配置 DNS 服务器。了解如何 "为 SVM 配置 DNS 服务"。
- 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NetApp Backup and Recovery服务通过端口 443 从ONTAP连接到对象存储，并通过端口 53（TCP/UDP）从存储虚拟机到 DNS 服务器的名称解析流量。

验证**ONTAP**复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地**ONTAP**网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。

准备 **Azure Blob** 作为备份目标

1. 您可以在激活向导中使用自己的自定义管理密钥进行数据加密，而不是使用默认的 Microsoft 管理加密密钥。在这种情况下，您将需要有 Azure 订阅、Key Vault 名称和密钥。 "了解如何使用自己的密钥" 。

   请注意，备份和恢复支持_Azure 访问策略_作为权限模型。目前不支持 Azure 基于角色的访问控制 (Azure RBAC) 权限模型。

2. 如果您希望通过公共互联网从本地数据中心到 VNet 建立更安全的连接，则可以在激活向导中配置 Azure 专用端点。在这种情况下，您需要了解此连接的 VNet 和子网。 "请参阅有关使用私有端点的详细信息" 。

创建 **Azure Blob** 存储帐户

默认情况下，该服务会为您创建存储帐户。如果您想使用自己的存储帐户，您可以在启动备份激活向导之前创建它们，然后在向导中选择这些存储帐户。

"了解有关创建自己的存储帐户的更多信息"。

激活**ONTAP**卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- [选择要备份的卷]
- [定义备份策略]
- [检查您的选择]

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：

   - 从控制台*系统*页面中，选择系统并选择右侧面板中备份和恢复服务旁边的*启用>备份卷*。

     如果控制台*系统*页面上存在备份的 Azure 目标，则可以将ONTAP集群拖到 Azure Blob 对象存储上。

   - 在备份和恢复栏中选择*卷*。从卷选项卡中，选择*操作*•••图标并选择单个卷（尚未启用复制或备份到对象存储）的*激活备份*。

   向导的介绍页面显示保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。

2. 继续以下选项：

   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您还没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

请注意，如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷（FlexGroup卷一次只能选择一个）。要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及设置以下选项：

- 您是否需要一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构
- 本地快照策略
- 复制目标和策略

  如果您选择的卷具有与您在此步骤中选择的策略不同的快照和复制策略，则现有策略将被覆盖。

- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：如果您正在执行复制或备份到对象存储，则必须创建本地快照。
   - 复制：在另一个ONTAP存储系统上创建复制卷。
   - 备份：将卷备份到对象存储。
2. 架构：如果您选择复制和备份，请选择以下信息流之一：
   - 级联：信息从主存储流向次存储，再从次存储流向对象存储。
   - 扇出：信息从主存储流向辅助存储，再从主存储流向对象存储。

有关这些架构的详细信息，请参阅"规划您的保护之旅"。

3. 本地快照：选择现有的快照策略或创建新的快照策略。

要在激活快照之前创建自定义策略，请参阅"创建策略"。

要创建策略，请选择“创建新策略”并执行以下操作：

- 输入策略的名称。
- 选择最多五个时间表，通常频率不同。
- 选择“创建”。

4. 复制：设置以下选项：
   - 复制目标：选择目标系统和 SVM。或者，选择将添加到复制卷名称的目标聚合或聚合以及前缀或后缀。
   - 复制策略：选择现有的复制策略或创建新的复制策略。

要在激活复制之前创建自定义策略，请参阅"创建策略"。

要创建策略，请选择“创建新策略”并执行以下操作：

- 输入策略的名称。
- 选择最多五个时间表，通常频率不同。
- 选择“创建”。

5. 备份到对象：如果您选择了*备份*，请设置以下选项：
   - 提供商：选择*Microsoft Azure*。
   - 提供商设置：输入提供商详细信息和存储备份的区域。

创建一个新的存储帐户或选择一个现有的存储帐户。

创建自己的管理 Blob 容器的资源组，或者选择资源组类型和组。

如果您想保护备份文件不被修改或删除，请确保创建存储帐户时启用了 30 天保留期的不可变存储。

如果要将较旧的备份文件分层到 Azure 存档存储以进一步优化成本，请确保存储帐户具有适当的生命周期规则。

- 加密密钥：如果您创建了新的 Azure 存储帐户，请输入提供商提供给您的加密密钥信息。选择是否使用默认 Azure 加密密钥，或者从 Azure 帐户中选择您自己的客户管理密钥来管理数据加密。

如果您选择使用自己的客户管理密钥，请输入密钥保管库和密钥信息。

如果您选择了现有的 Microsoft 存储帐户，则加密信息已经可用，因此您现在无需输入。

- 网络：选择 IP 空间，以及是否使用私有端点。默认情况下，私有端点是禁用的。

i. 您要备份的卷所在的ONTAP集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。

ii. 或者，选择是否使用之前配置的 Azure 专用终结点。 "了解如何使用 Azure 专用终结点" 。

- 备份策略：选择现有的备份到对象存储策略或创建一个新的策略。

  要在激活备份之前创建自定义策略，请参阅"创建策略"。

  要创建策略，请选择“创建新策略”并执行以下操作：

  - 输入策略的名称。
  - 选择最多五个时间表，通常频率不同。
  - 对于备份到对象策略，设置 DataLock 和 Ransomware Resilience 设置。有关 DataLock 和勒索软件恢复的详细信息，请参阅"备份到对象策略设置"。
  - 选择“创建”。

- 将现有快照导出到对象存储作为备份副本：如果此系统中存在与您刚刚为此系统选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框可将所有历史快照复制到对象存储作为备份文件，以确保对您的卷进行最全面的保护。

6. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中复选框*自动将快照策略标签与复制和备份策略标签同步*。这将创建具有与复制和备份策略中的标签匹配的标签的快照。
3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括主存储系统数据的完整副本。后续传输包含快照中包含的主存储系统数据的差异副本。

在目标集群中创建一个复制卷，该复制卷将与主卷同步。

在您输入的资源组中创建一个 Blob 存储帐户，并将备份文件存储在那里。显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

使用NetApp Backup and Recovery将本地ONTAP数据备份到 Google Cloud Storage

完成NetApp Backup and Recovery中的几个步骤，开始将卷数据从本地主ONTAP系统备份到二级存储系统和 Google Cloud Storage。

“本地ONTAP系统”包括FAS、 AFF和ONTAP Select系统。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

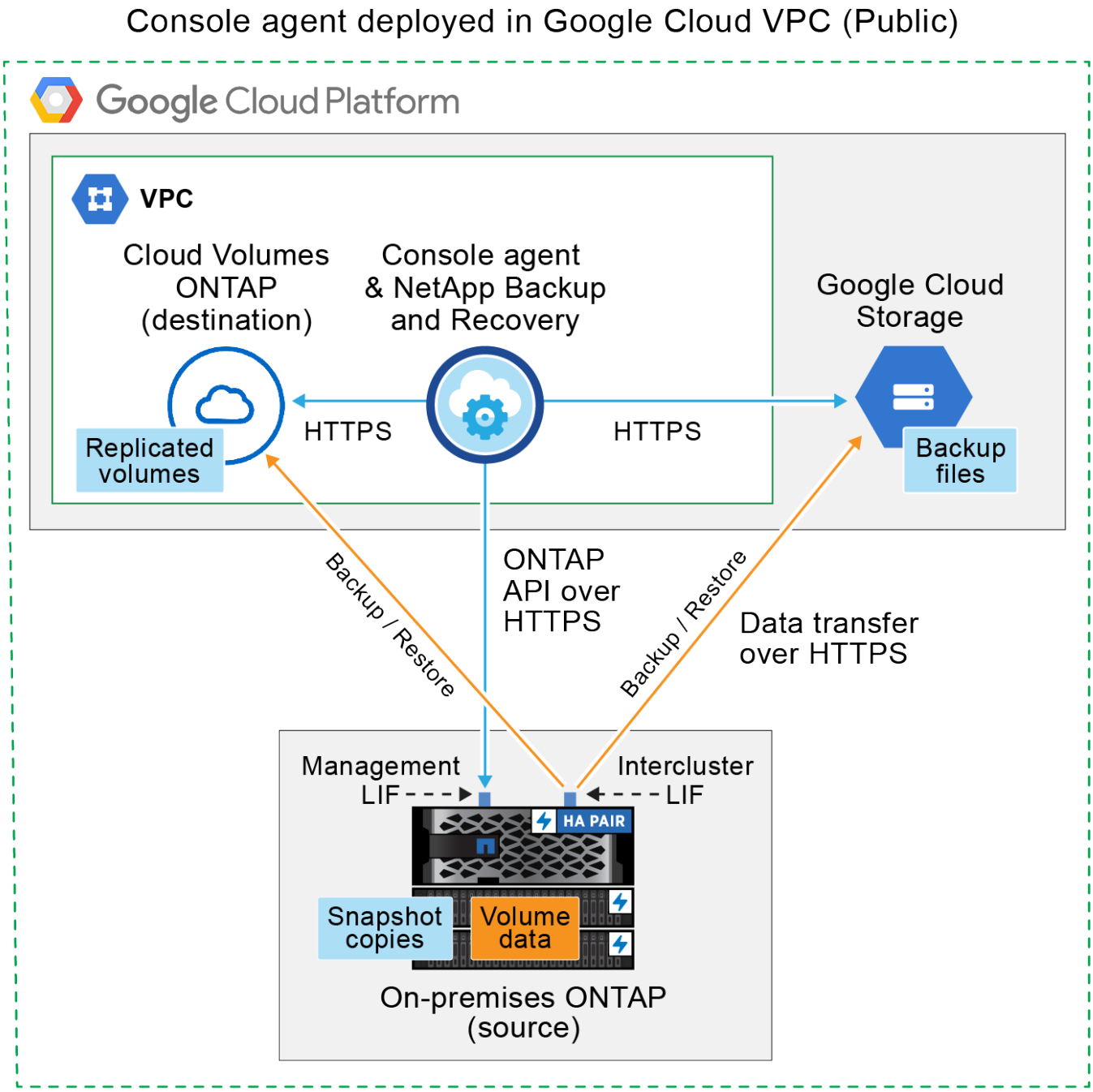
识别连接方法

选择在配置从本地ONTAP系统到 Google Cloud Storage 的备份时要使用的两种连接方法中的哪一种。

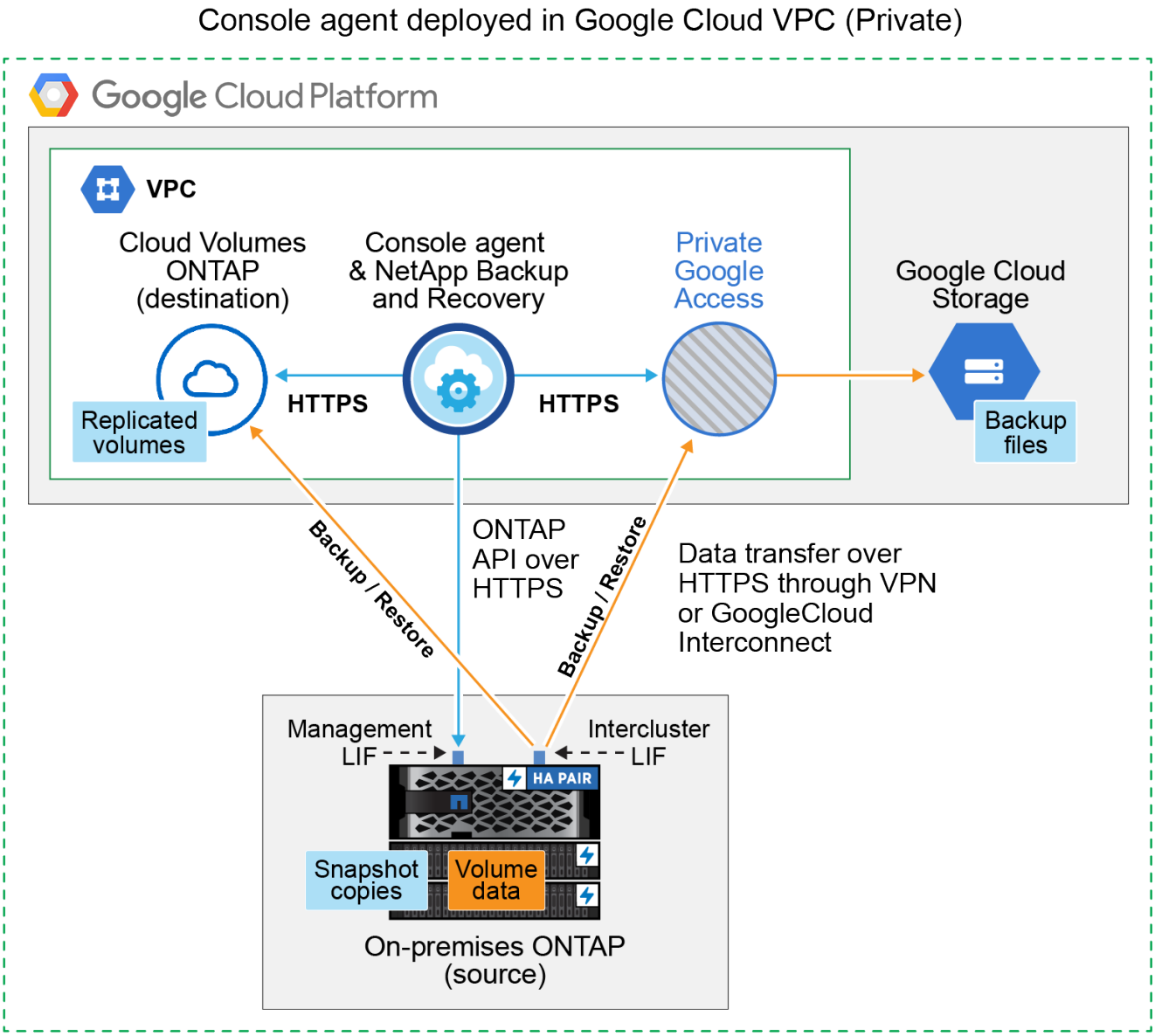
- 公共连接 - 使用公共 Google 端点将ONTAP系统直接连接到 Google Cloud Storage。
- 私人连接 - 使用 VPN 或 Google Cloud Interconnect 并通过使用私人 IP 地址的私人 Google Access 接口路由流量。

或者，您也可以使用公共或私有连接连接到用于复制卷的辅助ONTAP系统。

下图显示了*公共连接*方法以及您需要在组件之间准备的连接。控制台代理必须部署在 Google Cloud Platform VPC 中。



下图显示了*私有连接*方法以及您需要在组件之间准备的连接。控制台代理必须部署在 Google Cloud Platform VPC 中。



准备控制台代理

控制台代理是控制台功能的主要软件。需要控制台代理来备份和恢复您的ONTAP数据。

创建或切换控制台代理

如果您已经在 Google Cloud Platform VPC 中部署了控制台代理，那么一切就绪了。

如果没有，那么您需要在该位置创建一个控制台代理，以将ONTAP数据备份到 Google Cloud Storage。您不能使用部署在其他云提供商或本地的控制台代理。

- "了解控制台代理"
- "在 GCP 中安装控制台代理"

为控制台代理准备网络

确保控制台代理具有所需的网络连接。

步骤

1. 确保安装控制台代理的网络启用以下连接：
   - 通过端口 443 建立到NetApp Backup and Recovery以及您的 Google Cloud 存储的 HTTPS 连接("查看端点列表")
   - 通过端口 443 建立到ONTAP集群管理 LIF 的 HTTPS 连接
2. 在您计划部署控制台代理的子网上启用私有 Google Access（或私有服务连接）。 "私人 Google 访问权限"或者 "私人服务连接"如果您有从ONTAP集群到 VPC 的直接连接，并且希望控制台代理和 Google Cloud Storage 之间的通信保持在虚拟专用网络（*专用*连接）中，则需要。

   按照 Google 说明设置这些私人访问选项。确保您的 DNS 服务器已配置为指向 `www.googleapis.com`和 `storage.googleapis.com`到正确的内部（私有）IP 地址。

验证或添加控制台代理的权限

要使用NetApp Backup and Recovery的“搜索和恢复”功能，您需要在控制台代理的角色中拥有特定权限，以便它可以访问 Google Cloud BigQuery 服务。查看以下权限，如果需要修改策略，请按照以下步骤操作。

步骤

1. 在 "Google 云端控制台"，转到*角色*页面。
2. 使用页面顶部的下拉列表，选择包含要编辑的角色的项目或组织。
3. 选择自定义角色。
4. 选择*编辑角色*来更新角色的权限。
5. 选择*添加权限*为角色添加以下新权限。

```
bigquery.jobs.get
bigquery.jobs.list
bigquery.jobs.listAll
bigquery.datasets.create
bigquery.datasets.get
bigquery.jobs.create
bigquery.tables.get
bigquery.tables.getData
bigquery.tables.list
bigquery.tables.create
```

6. 选择*更新*以保存编辑的角色。

验证许可证要求

- 在为集群激活NetApp Backup and Recovery之前，您需要订阅 Google 提供的即用即付 (PAYGO) 控制台市场，或者从NetApp购买并激活NetApp Backup and Recovery BYOL 许可证。这些许可证适用于您的帐户，

可以在多个系统中使用。

- 对于NetApp Backup and Recovery PAYGO 许可，您需要订阅 "Google Marketplace 提供的NetApp Console"。 NetApp Backup and Recovery的计费通过此订阅完成。
- 对于NetApp Backup and RecoveryBYOL 许可，您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。"了解如何管理您的 BYOL 许可证"。

- 您需要向 Google 订阅用于存储备份的对象存储空间。

支持地区

您可以从本地系统创建备份到所有地区的 Google Cloud Storage。您在设置服务时指定存储备份的区域。

准备**ONTAP**集群

准备源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统。

准备ONTAP集群涉及以下步骤：

- 在NetApp Console中发现您的ONTAP系统
- 验证ONTAP系统要求
- 验证ONTAP网络要求以将数据备份到对象存储
- 验证ONTAP复制卷的网络要求

在**NetApp Console**中发现您的**ONTAP**系统

您的源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统都必须在NetApp Console*系统*页面上可用。

您需要知道集群管理 IP 地址和管理员用户帐户的密码才能添加集群。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["了解如何发现集群"^]。

验证**ONTAP**系统要求

确保您的ONTAP系统满足以下要求：

- 最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。
- SnapMirror许可证（包含在高级捆绑包或数据保护捆绑包中）。

  *注意：*使用NetApp Backup and Recovery时不需要“混合云捆绑包”。

  了解如何 "管理您的集群许可证"。

- 时间和时区设置正确。了解如何 "配置集群时间"。
- 如果您复制数据，请检查源系统和目标系统是否运行兼容的ONTAP版本。

  "查看与SnapMirror关系兼容的ONTAP版本"。

验证ONTAP网络要求以将数据备份到对象存储

您必须在连接到对象存储的系统上配置以下要求。

- 对于扇出备份架构，请在主系统上配置以下设置。
- 对于级联备份架构，请在_辅助_系统上配置以下设置。

需要满足以下ONTAP集群网络要求：

- ONTAP集群通过端口 443 启动从集群间 LIF 到 Google Cloud Storage 的 HTTPS 连接，以进行备份和还原操作。

  ONTAP从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。

- ONTAP需要从控制台代理到集群管理 LIF 的入站连接。控制台代理可以驻留在 Google Cloud Platform VPC 中。
- 每个托管要备份的卷的ONTAP节点上都需要一个集群间 LIF。 LIF 必须与ONTAP用于连接对象存储的 *IPspace* 相关联。 "了解有关 IP 空间的更多信息" 。

  当您设置NetApp Backup and Recovery时，系统会提示您输入要使用的 IP 空间。您应该选择与每个 LIF 关联的 IP 空间。这可能是“默认” IP 空间或您创建的自定义 IP 空间。

- 节点的集群间 LIF 能够访问对象存储。
- 已为卷所在的存储虚拟机配置 DNS 服务器。了解如何 "为 SVM 配置 DNS 服务"。

  如果您使用的是 Private Google Access 或 Private Service Connect，请确保您的 DNS 服务器已配置为指向 `storage.googleapis.com`到正确的内部（私有）IP 地址。

- 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NetApp Backup and Recovery通过端口 443 从ONTAP连接到对象存储，并通过端口 53（TCP/UDP）从存储虚拟机到 DNS 服务器的名称解析流量。

验证ONTAP复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地ONTAP网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。

准备 **Google Cloud Storage** 作为备份目标

准备 Google Cloud Storage 作为备份目标涉及以下步骤：

- 设置权限。
- （可选）创建您自己的存储桶。（如果您愿意，该服务将为您创建存储桶。）
- （可选）设置客户管理的密钥以进行数据加密

设置权限

您需要使用自定义角色为具有特定权限的服务帐户提供存储访问密钥。服务帐户使NetApp Backup and Recovery能够验证和访问用于存储备份的 Cloud Storage 存储桶。需要密钥，以便 Google Cloud Storage 知道谁在发出请求。

步骤

1. 在 "Google 云端控制台"，转到*角色*页面。
2. "创建新角色"具有以下权限：

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. 在 Google Cloud 控制台中， "前往服务帐户页面" 。
4. 选择您的云项目。
5. 选择*创建服务帐户*并提供所需信息：
   a. 服务帐户详细信息：输入名称和描述。
   b. 授予此服务帐户访问项目的权限：选择您刚刚创建的自定义角色。
   c. 选择*完成*。
6. 前往 "GCP 存储设置"并为服务帐户创建访问密钥：
   a. 选择一个项目，然后选择*互操作性*。如果您还没有这样做，请选择*启用互操作性访问*。
   b. 在*服务帐户的访问密钥*下，选择*为服务帐户创建密钥*，选择刚刚创建的服务帐户，然后单击*创建密钥*。

      稍后配置备份服务时，您需要在NetApp Backup and Recovery中输入密钥。

创建您自己的存储桶

默认情况下，该服务会为您创建存储桶。或者，如果您想使用自己的存储桶，您可以在启动备份激活向导之前创建它们，然后在向导中选择这些存储桶。

"了解有关创建您自己的存储桶的更多信息"。

设置客户管理的加密密钥 **(CMEK)** 以进行数据加密

您可以使用自己的客户管理密钥进行数据加密，而不是使用默认的 Google 管理加密密钥。跨区域和跨项目密钥均受支持，因此您可以为存储桶选择与 CMEK 密钥的项目不同的项目。

如果您打算使用自己的客户管理密钥：

- 您需要有密钥环和密钥名称，以便可以在激活向导中添加此信息。 "了解有关客户管理加密密钥的更多信息"。
- 您需要验证控制台代理的角色是否包含这些必需的权限：

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 您需要验证您的项目中是否启用了 Google“云密钥管理服务 (KMS)”API。查看 "Google Cloud 文档：启用 API"了解详情。

CMEK 注意事项：

- 支持 HSM（硬件支持）和软件生成的密钥。
- 支持新创建或导入的 Cloud KMS 密钥。
- 仅支持区域密钥，不支持全局密钥。
- 目前仅支持“对称加密/解密”目的。
- NetApp Backup and Recovery为与存储帐户关联的服务代理分配了“CryptoKey Encrypter/Decrypter (roles/cloudkms.cryptoKeyEncrypterDecrypter)”IAM 角色。

激活**ONTAP**卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- [选择要备份的卷]
- [定义备份策略]

- [检查您的选择]

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：
   - 从控制台*系统*页面中，选择系统，然后选择右侧面板中备份和恢复旁边的*启用>备份卷*。

     如果您的备份的 Google Cloud Storage 目标存在于控制台 系统 页面上，则可以将ONTAP集群拖到 Google Cloud 对象存储上。
   - 在备份和恢复栏中选择*卷*。从卷选项卡中，选择*操作*•••图标并选择单个卷（尚未启用复制或备份到对象存储）的*激活备份*。

   向导的介绍页面显示保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。
2. 继续以下选项：
   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您还没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷（FlexGroup卷一次只能选择一个）。要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及设置以下选项：

- 您是否需要一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构
- 本地快照策略
- 复制目标和策略

> 如果您选择的卷具有与您在此步骤中选择的策略不同的快照和复制策略，则现有策略将被覆盖。

- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：如果您正在执行复制或备份到对象存储，则必须创建本地快照。
   - 复制：在另一个ONTAP存储系统上创建复制卷。
   - 备份：将卷备份到对象存储。
2. 架构：如果您选择复制和备份，请选择以下信息流之一：
   - 级联：信息从主存储流向辅助存储，再从辅助存储流向对象存储。
   - 扇出：信息从主存储流向辅助存储，再从主存储流向对象存储。

   有关这些架构的详细信息，请参阅"规划您的保护之旅"。
3. 本地快照：选择现有的快照策略或创建新的快照策略。

   > 要创建自定义策略，请参阅"创建策略"。

   要创建策略，请选择“创建新策略”并执行以下操作：
   - 输入策略的名称。
   - 选择最多五个时间表，通常频率不同。
   - 选择“创建”。
4. 复制：设置以下选项：
   - 复制目标：选择目标系统和 SVM。或者，选择将添加到复制卷名称的目标聚合或聚合以及前缀或后缀。
   - 复制策略：选择现有的复制策略或创建新的复制策略。

     > 要创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：
     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。

5. 备份到对象：如果您选择了*备份*，请设置以下选项：
   - 提供商：选择*Google Cloud*。
   - 提供商设置：输入提供商详细信息和存储备份的区域。

     创建新存储桶或选择已创建的存储桶。

     如果您希望将较旧的备份文件分层到 Google Cloud Archive 存储以进一步优化成本，请确保存储桶具有适当的生命周期规则。

     输入 Google Cloud 访问密钥和密钥。
   - 加密密钥：如果您创建了新的 Google Cloud 存储帐户，请输入提供商提供给您的加密密钥信息。选择是否使用默认的 Google Cloud 加密密钥，或者从您的 Google Cloud 帐户中选择您自己的客户管理密钥来管理您的数据加密。

     如果您选择了现有的 Google Cloud 存储帐户，则加密信息已经可用，因此您现在无需输入。

     如果您选择使用自己的客户管理密钥，请输入密钥环和密钥名称。 "了解有关客户管理加密密钥的更多信息" 。
   - 网络：选择 IP 空间。

     您要备份的卷所在的ONTAP集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限。
   - 备份策略：选择现有的备份到对象存储策略或创建一个新的策略。

     要创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：
     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。
   - 将现有快照导出到对象存储作为备份副本：如果此系统中存在与您刚刚为此系统选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框可将所有历史快照复制到对象存储作为备份文件，以确保对您的卷进行最全面的保护。
6. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中复选框*自动将快照策略标签与复制和备份策略标签同步*。这将创建具有与复制和备份策略中的标签匹配的标签的快照。

3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括主存储系统数据的完整副本。后续传输包含快照中包含的主存储系统数据的差异副本。

在目标集群中创建一个复制卷，该卷将与源卷同步。

系统会在您输入的 Google 访问密钥和密钥所指示的服务帐户中自动创建一个 Google Cloud Storage 存储桶，并将备份文件存储在那里。显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

使用**NetApp Backup and Recovery**将本地**ONTAP**数据备份到**ONTAP S3**

完成NetApp Backup and Recovery中的几个步骤即可开始从主本地ONTAP系统备份卷数据。您可以将备份发送到辅助ONTAP存储系统（复制卷）或配置为 S3 服务器的ONTAP系统上的存储桶（备份文件），或同时发送到两者。

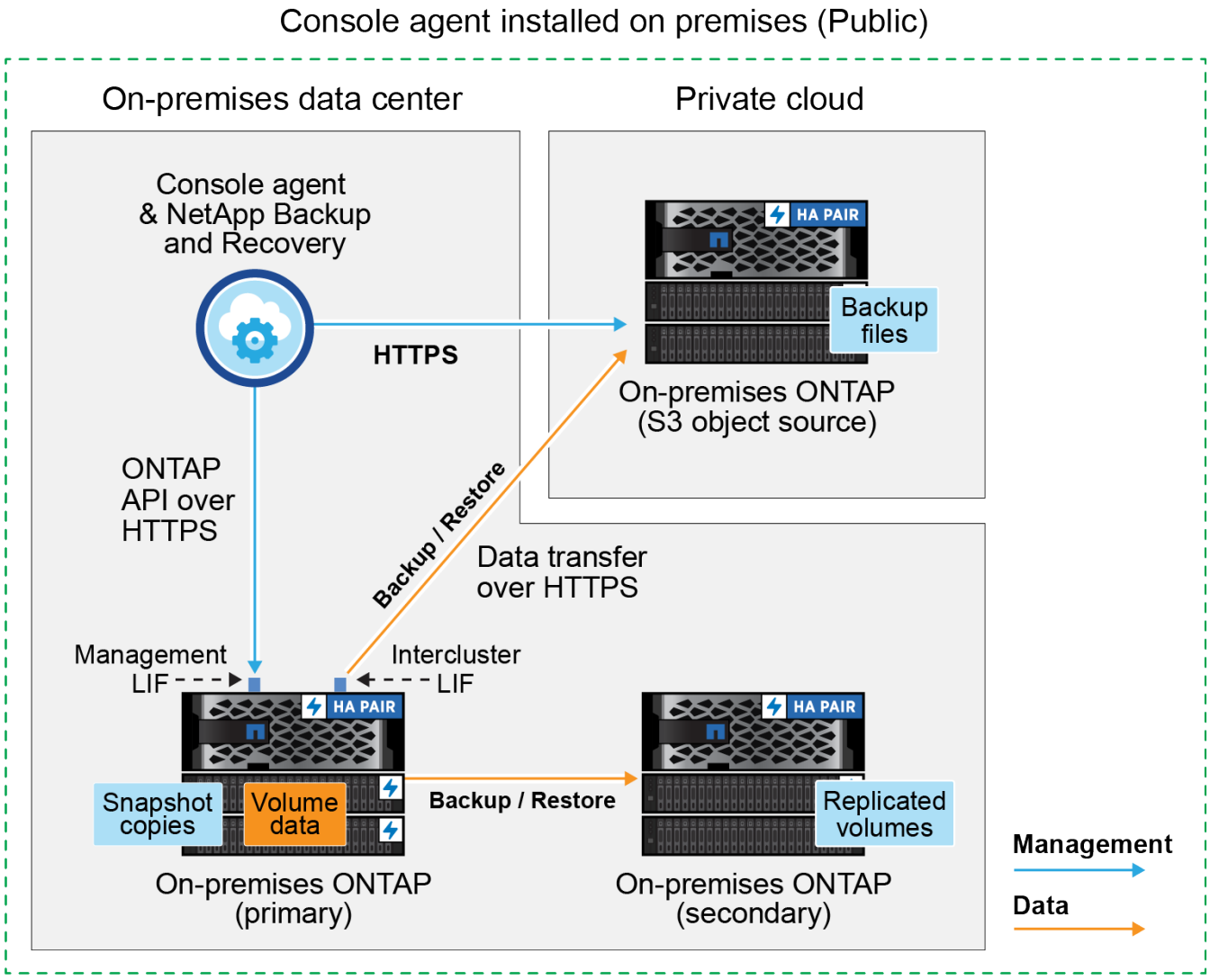
主本地ONTAP系统可以是FAS、 AFF或ONTAP Select系统。辅助ONTAP系统可以是本地ONTAP或Cloud Volumes ONTAP系统。对象存储可以位于本地ONTAP系统或已启用简单存储服务 (S3) 对象存储服务器的Cloud Volumes ONTAP系统上。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

识别连接方法

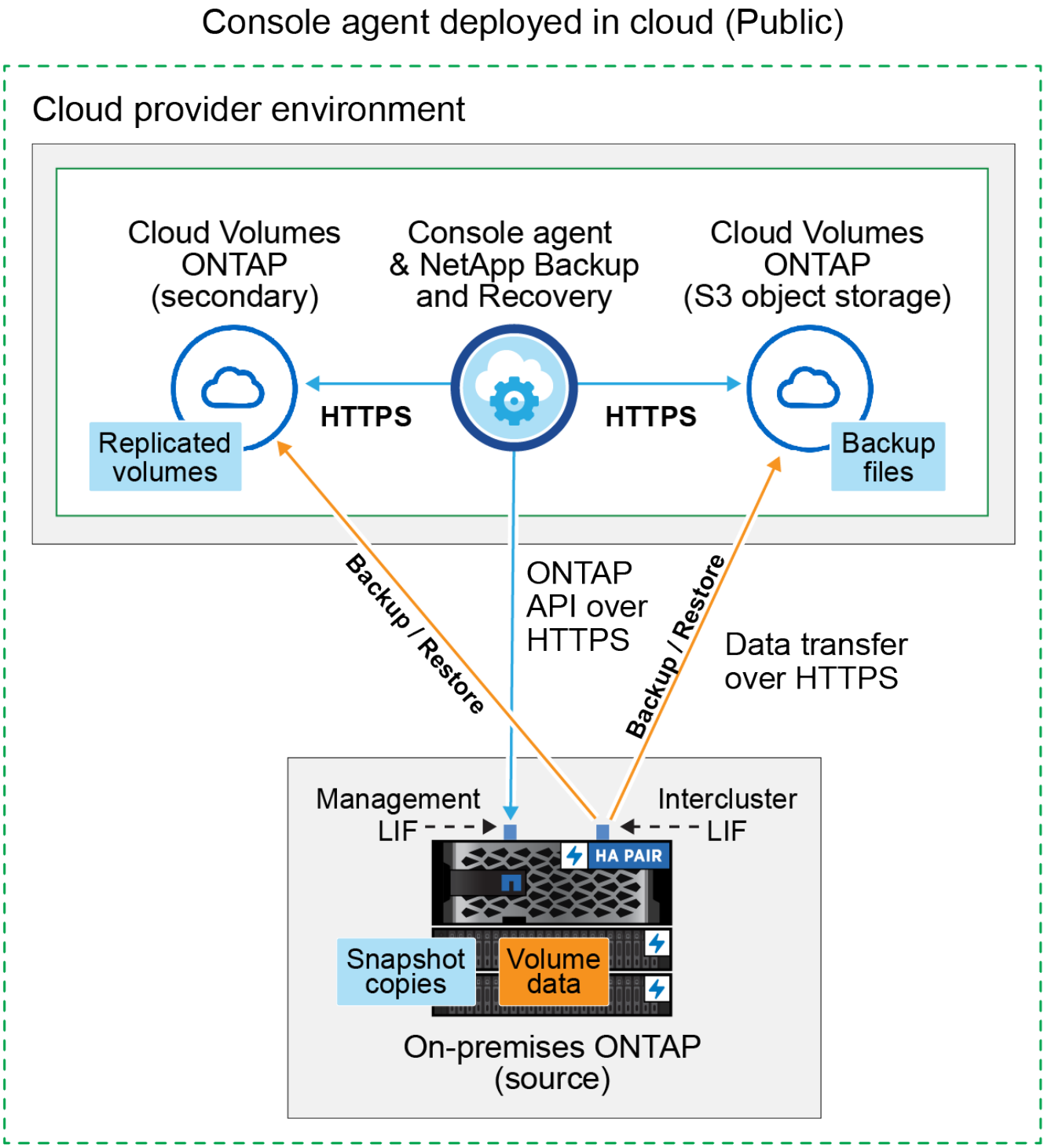
您可以使用多种配置在ONTAP系统上创建 S3 存储桶的备份。下面显示了两种情况。

下图显示了将主本地ONTAP系统备份到为 S3 配置的本地ONTAP系统时的每个组件以及您需要在它们之间准备的连接。它还显示了与同一本地位置的辅助ONTAP系统的连接以复制卷。



当控制台代理和主本地ONTAP系统安装在没有互联网访问的本地位置（“私有”模式部署）时， ONTAP S3 系统必须位于同一个本地数据中心。

下图显示了将主本地ONTAP系统备份到为 S3 配置的Cloud Volumes ONTAP系统时的每个组件以及您需要在它们之间准备的连接。它还显示了与同一云提供商环境中的辅助Cloud Volumes ONTAP系统的连接，以复制卷。



在这种情况下，控制台代理应部署在部署Cloud Volumes ONTAP系统的同一云提供商环境中。

准备控制台代理

控制台代理是控制台功能的主要软件。需要控制台代理来备份和恢复您的ONTAP数据。

创建或切换控制台代理

当您将数据备份到ONTAP S3 时，您的本地或云中必须有控制台代理。您需要安装新的控制台代理，或者确保

当前选定的控制台代理位于其中一个位置。本地控制台代理可以安装在有或没有互联网访问的站点中。

- "了解控制台代理"
- "在您的云环境中安装控制台代理"
- "在具有互联网访问权限的 Linux 主机上安装控制台代理"
- "在没有互联网访问的 Linux 主机上安装控制台代理"
- "在控制台代理之间切换"

准备控制台代理网络要求

确保安装控制台代理的网络启用以下连接：

- 通过端口 443 到ONTAP S3 服务器的 HTTPS 连接
- 通过端口 443 建立到源ONTAP集群管理 LIF 的 HTTPS 连接
- 通过端口 443 到NetApp Backup and Recovery 的出站互联网连接（当控制台代理安装在“暗站”时不需要）

私人模式（暗站）注意事项

NetApp Backup and Recovery功能内置于控制台代理中。当以私人模式安装时，您需要定期更新控制台代理软件才能访问新功能。检查"NetApp Backup and Recovery新功能"查看每个NetApp Backup and Recovery版本中的新功能。当您想要使用新功能时，请按照以下步骤操作 "升级控制台代理软件"。

当您在标准 SaaS 环境中使用NetApp Backup and Recovery时， NetApp Backup and Recovery配置数据将备份到云端。当您在没有互联网访问的站点中使用NetApp Backup and Recovery时， NetApp Backup and Recovery配置数据将备份到存储备份的ONTAP S3 存储桶中。

验证许可证要求

在为集群激活NetApp Backup and Recovery之前，您需要从NetApp购买并激活NetApp Backup and Recovery BYOL 许可证。该许可证用于备份和恢复对象存储 - 创建快照或复制卷不需要许可证。此许可证适用于该帐户，可跨多个系统使用。

您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。"了解如何管理您的 BYOL 许可证"。

将文件备份到ONTAP S3 时不支持 PAYGO 许可。

准备**ONTAP**集群

准备源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统。

准备ONTAP集群涉及以下步骤：

- 在NetApp Console中发现您的ONTAP系统
- 验证ONTAP系统要求
- 验证ONTAP网络要求以将数据备份到对象存储
- 验证ONTAP复制卷的网络要求

在NetApp Console中发现您的ONTAP系统

您的源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统都必须在NetApp Console*系统*页面上可用。

您需要知道集群管理 IP 地址和管理员用户帐户的密码才能添加集群。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["了解如何发现集群"^]。

验证ONTAP系统要求

确保您的ONTAP系统满足以下要求：

- 最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。
- SnapMirror许可证（包含在高级捆绑包或数据保护捆绑包中）。

  *注意：*使用NetApp Backup and Recovery时不需要“混合云捆绑包”。

  了解如何 "管理您的集群许可证"。

- 时间和时区设置正确。了解如何 "配置集群时间"。
- 如果您复制数据，请检查源系统和目标系统是否运行兼容的ONTAP版本。

  "查看与SnapMirror关系兼容的ONTAP版本"。

验证ONTAP网络要求以将数据备份到对象存储

您必须确保连接到对象存储的系统满足以下要求。

- 当您使用扇出备份架构时，必须在主存储系统上配置设置。
- 当您使用级联备份架构时，必须在_辅助_存储系统上配置设置。

  "了解有关备份架构类型的更多信息"。

需要满足以下ONTAP集群网络要求：

- ONTAP集群通过用户指定的端口从集群间 LIF 启动到ONTAP S3 服务器的 HTTPS 连接，以执行备份和还原操作。该端口可在备份设置期间配置。

  ONTAP从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。

- ONTAP需要从控制台代理到集群管理 LIF 的入站连接。
- 每个托管要备份的卷的ONTAP节点上都需要一个集群间 LIF。 LIF 必须与ONTAP用于连接对象存储的 *IPspace* 相关联。 "了解有关 IP 空间的更多信息" 。

  当您设置NetApp Backup and Recovery时，系统会提示您输入要使用的 IP 空间。您应该选择与每个 LIF 关联的 IP 空间。这可能是“默认” IP 空间或您创建的自定义 IP 空间。

- 节点的集群间 LIF 能够访问对象存储（当控制台代理安装在“暗”站点中时不需要）。
- 已为卷所在的存储虚拟机配置 DNS 服务器。了解如何 "为 SVM 配置 DNS 服务"。

- 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NetApp Backup and Recovery服务通过您指定的端口（通常为端口 443）从ONTAP连接到对象存储，并通过端口 53（TCP/UDP）从存储虚拟机到 DNS 服务器的名称解析流量。

验证**ONTAP**复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地**ONTAP**网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。

准备**ONTAP S3** 作为备份目标

您必须在计划用于对象存储备份的ONTAP集群中启用简单存储服务 (S3) 对象存储服务器。查看 "ONTAP S3 文档"了解详情。

*注意：*您可以将此集群添加到控制台*系统*页面，但它不会被识别为 S3 对象存储服务器，并且您无法将源系统拖放到此 S3 系统上以启动备份激活。

此ONTAP系统必须满足以下要求。

支持的 **ONTAP** 版本

本地ONTAP系统需要ONTAP 9.8 及更高版本。 Cloud Volumes ONTAP系统需要ONTAP 9.9.1 及更高版本。

S3 凭证

您必须创建 S3 用户来控制对ONTAP S3 存储的访问。 "有关详细信息，请参阅ONTAP S3 文档" 。

当您设置备份到ONTAP S3 时，备份向导会提示您输入用户帐户的 S3 访问密钥和密钥。该用户帐户使NetApp Backup and Recovery能够验证和访问用于存储备份的ONTAP S3 存储桶。需要密钥，以便ONTAP S3 知道谁在发出请求。

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",
"s3:GetBucketLocation"
```

激活**ONTAP**卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- 选择要备份的卷
- 定义备份策略和政策
- 检查您的选择

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：
   - 从控制台*系统*页面中，选择系统，然后选择右侧面板中备份和恢复旁边的*启用>备份卷*。
   - 在备份和恢复栏中选择*卷*。从“卷”选项卡中，选择“操作 (…)”选项，然后为单个卷（尚未启用复制或备份到对象存储）选择“激活备份”。

   向导的简介页面显示了保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。
2. 继续以下选项：
   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

请注意，如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷（FlexGroup卷一次只能选择一个）。要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及配置以下选项：

- 保护选项：您是否要实施一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构：您是否要使用扇出式或级联备份架构
- 本地快照策略
- 复制目标和策略
- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：创建本地快照。
   - 复制：在另一个ONTAP存储系统上创建复制卷。
   - 备份：将卷备份到为 S3 配置的ONTAP系统上的存储桶。
2. 架构：如果您同时选择了复制和备份，请选择以下信息流之一：
   - 级联：备份数据从主系统流向辅助系统，然后从辅助系统流向对象存储。
   - 扇出：备份数据从主系统流向辅助系统，并从主系统流向对象存储。

   有关这些架构的详细信息，请参阅"规划您的保护之旅"。
3. 本地快照：选择现有的快照策略或创建新的快照策略。

   如果要在激活快照之前创建自定义策略，则可以使用 System Manager 或ONTAP CLI `snapmirror policy create`命令。参考。

   要使用备份和恢复创建自定义策略，请参阅"创建策略"。

   要创建策略，请选择“创建新策略”并执行以下操作：
   - 输入策略的名称。
   - 选择最多五个时间表，通常频率不同。

- 选择“创建”。

4. 复制：如果选择了*复制*，请设置以下选项：
   - 复制目标：选择目标系统和 SVM。或者，选择目标聚合（或FlexGroup卷的聚合）以及将添加到复制卷名称的前缀或后缀。
   - 复制策略：选择现有的复制策略或创建新的复制策略。

     要创建策略，请选择“创建新策略”并执行以下操作：

     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。
5. 备份到对象：如果您选择了*备份*，请设置以下选项：
   - 提供商：选择* ONTAP S3*。
   - 提供商设置：输入 S3 服务器 FQDN 详细信息、端口以及用户的访问密钥和密钥。

     访问密钥和密钥用于您创建的用户，以授予ONTAP集群对 S3 存储桶的访问权限。
   - 网络：选择要备份的卷所在的源ONTAP集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限（当控制台代理安装在“暗站”中时不需要）。

     选择正确的 IP 空间可确保NetApp Backup and Recovery可以建立从ONTAP到ONTAP S3 对象存储的连接。
   - 备份策略：选择现有的备份策略或创建新的备份策略。

     您可以使用 System Manager 或ONTAP CLI 创建策略。使用ONTAP CLI 创建自定义策略 `snapmirror policy create`命令，请参阅。

     要使用备份和恢复创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：

     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 对于备份到对象策略，设置 DataLock 和 Ransomware Resilience 设置。有关 DataLock 和勒索软件恢复的详细信息，请参阅"备份到对象策略设置"。
     - 选择“创建”。
   - 将现有快照导出到对象存储作为备份文件：如果此系统中存在与您刚刚选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框可将所有历史快照复制到对象存储作为备份文件，以确保对您的卷进行最全面的保护。
6. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中复选框*自动将快照策略标签与复制和备份策略标签同步*。这将创建具有与复制和备份策略中的标签匹配的标签的快照。如果策略不匹配，则不会创建备份。
3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括源数据的完整副本。后续传输包含快照中包含的主存储数据的差异副本。

在目标集群中创建一个复制卷，该卷将与主存储卷同步。

在您输入的 S3 访问密钥和密钥指示的服务帐户中创建一个 S3 存储桶，并将备份文件存储在那里。

显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

使用NetApp Backup and Recovery将本地ONTAP数据备份到StorageGRID

完成NetApp Backup and Recovery中的几个步骤，开始将卷数据从本地主ONTAP系统备份到二级存储系统以及NetApp StorageGRID系统中的对象存储。

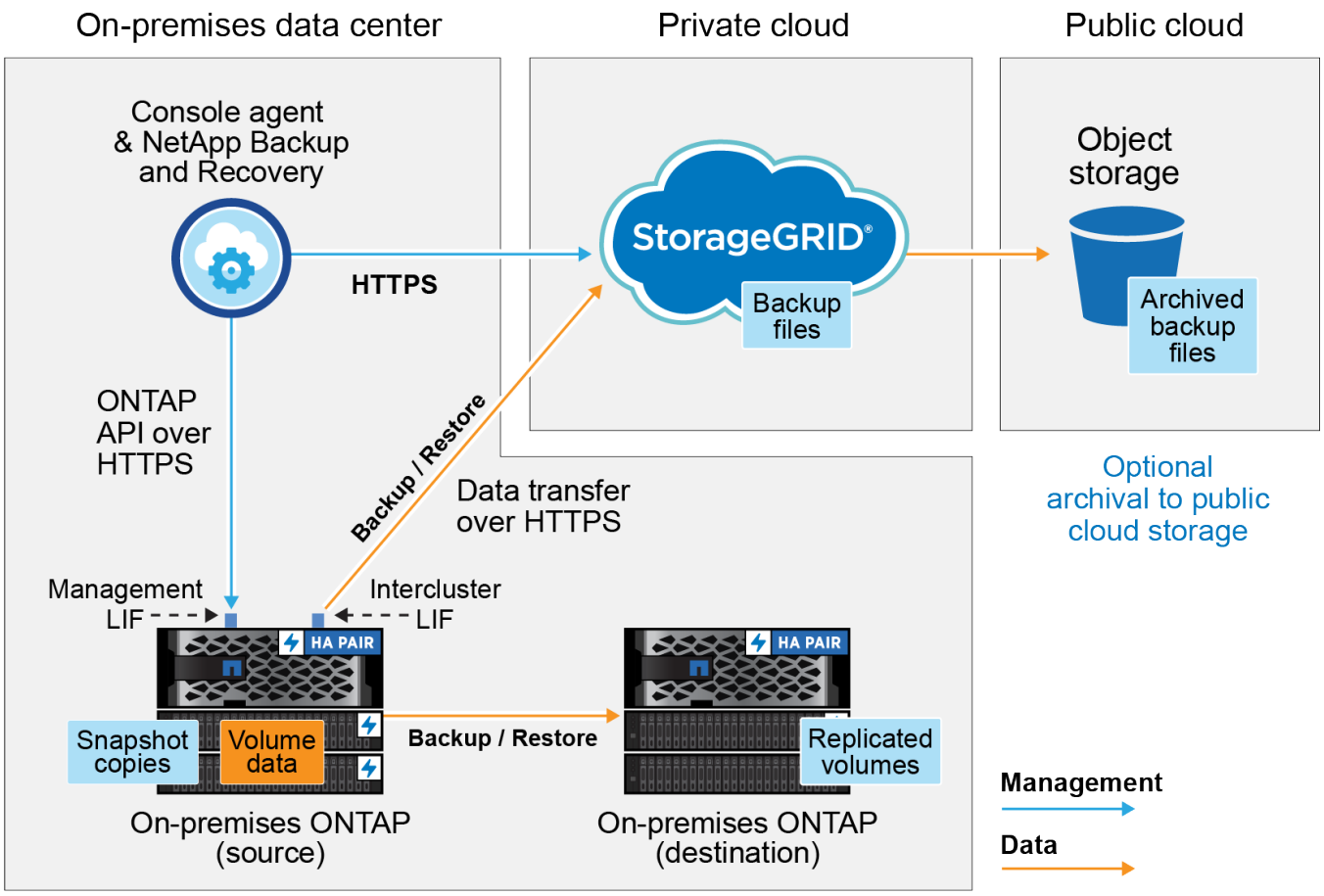
“本地ONTAP系统”包括FAS、 AFF和ONTAP Select系统。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

识别连接方法

下图显示了将本地ONTAP系统备份到StorageGRID时的每个组件以及您需要在它们之间准备的连接。

或者，您可以连接到同一本地位置的辅助ONTAP系统来复制卷。



当控制台代理和本地ONTAP系统安装在没有互联网访问的本地位置（“暗站”）时， StorageGRID系统必须位于同一个本地数据中心。暗站配置不支持将旧备份文件存档到公共云。

准备控制台代理

控制台代理是控制台功能的主要软件。需要控制台代理来备份和恢复您的ONTAP数据。

创建或切换控制台代理

当您将数据备份到StorageGRID时，您的场所必须有控制台代理。您需要安装新的控制台代理或确保当前选定的控制台代理位于本地。控制台代理可以安装在有或没有互联网访问的站点。

- "了解控制台代理"
- "在具有互联网访问权限的 Linux 主机上安装控制台代理"
- "在没有互联网访问的 Linux 主机上安装控制台代理"
- "在控制台代理之间切换"

准备控制台代理网络要求

确保安装控制台代理的网络启用以下连接：

- 通过端口 443 到StorageGRID网关节点的 HTTPS 连接
- 通过端口 443 建立到ONTAP集群管理 LIF 的 HTTPS 连接

- 通过端口 443 到NetApp Backup and Recovery 的出站互联网连接（当控制台代理安装在“暗站”时不需要）

私人模式（暗站）注意事项

- NetApp Backup and Recovery功能内置于控制台代理中。当以私人模式安装时，您需要定期更新控制台代理软件才能访问新功能。检查"NetApp Backup and Recovery新功能"查看每个NetApp Backup and Recovery版本中的新功能。当您想要使用新功能时，请按照以下步骤操作 "升级控制台代理软件"。

  新版NetApp Backup and Recovery除了可以创建对象存储备份外，还增加了计划和创建快照及复制卷的功能，但需要使用 3.9.31 或更高版本的控制台代理。因此建议您获取此最新版本来管理所有备份。

- 当您在 SaaS 环境中使用NetApp Backup and Recovery时， NetApp Backup and Recovery配置数据将备份到云端。当您在没有互联网访问的站点中使用NetApp Backup and Recovery时， NetApp Backup and Recovery配置数据将备份到存储备份的StorageGRID桶中。

验证许可证要求

在为集群激活NetApp Backup and Recovery之前，您需要从NetApp购买并激活NetApp Backup and Recovery BYOL 许可证。此许可证适用于该帐户，可跨多个系统使用。

您需要NetApp提供的序列号，以便您在许可证的有效期和容量内使用该服务。"了解如何管理您的 BYOL 许可证"。

将文件备份到StorageGRID时不支持 PAYGO 许可。

准备**ONTAP**集群

准备源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统。

准备ONTAP集群涉及以下步骤：

- 在NetApp Console中发现您的ONTAP系统
- 验证ONTAP系统要求
- 验证ONTAP网络要求以将数据备份到对象存储
- 验证ONTAP复制卷的网络要求

在**NetApp Console**中发现您的**ONTAP**系统

您的源本地ONTAP系统和任何辅助本地ONTAP或Cloud Volumes ONTAP系统都必须在NetApp Console*系统*页面上可用。

您需要知道集群管理 IP 地址和管理员用户帐户的密码才能添加集群。https://docs.netapp.com/us-en/storage-management-ontap-onprem/task-discovering-ontap.html["了解如何发现集群"^]。

验证**ONTAP**系统要求

确保您的ONTAP系统满足以下要求：

- 最低版本为ONTAP 9.8；建议使用ONTAP 9.8P13 及更高版本。
- SnapMirror许可证（包含在高级捆绑包或数据保护捆绑包中）。

*注意：*使用NetApp Backup and Recovery时不需要“混合云捆绑包”。

了解如何 "管理您的集群许可证"。

- 时间和时区设置正确。了解如何 "配置集群时间"。
- 如果您复制数据，请检查源系统和目标系统是否运行兼容的ONTAP版本。

"查看与SnapMirror关系兼容的ONTAP版本"。

验证**ONTAP**网络要求以将数据备份到对象存储

您必须在连接到对象存储的系统上配置以下要求。

- 当您使用扇出备份架构时，必须在主存储系统上配置以下设置。
- 当您使用级联备份架构时，必须在_辅助_存储系统上配置以下设置。

需要满足以下ONTAP集群网络要求：

- ONTAP集群通过用户指定的端口从集群间 LIF 启动到StorageGRID网关节点的 HTTPS 连接，以执行备份和还原操作。该端口可在备份设置期间配置。

  ONTAP从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。

- ONTAP需要从控制台代理到集群管理 LIF 的入站连接。控制台代理必须位于您的场所。
- 每个托管要备份的卷的ONTAP节点上都需要一个集群间 LIF。 LIF 必须与ONTAP用于连接对象存储的 *IPspace* 相关联。 "了解有关 IP 空间的更多信息" 。

  当您设置NetApp Backup and Recovery时，系统会提示您输入要使用的 IP 空间。您应该选择与每个 LIF 关联的 IP 空间。这可能是“默认” IP 空间或您创建的自定义 IP 空间。

- 节点的集群间 LIF 能够访问对象存储（当控制台代理安装在“暗”站点中时不需要）。
- 已为卷所在的存储虚拟机配置 DNS 服务器。了解如何 "为 SVM 配置 DNS 服务"。
- 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NetApp Backup and Recovery服务通过您指定的端口（通常为端口 443）从ONTAP连接到对象存储，并通过端口 53（TCP/UDP）从存储虚拟机到 DNS 服务器的名称解析流量。

验证**ONTAP**复制卷的网络要求

如果您计划使用NetApp Backup and Recovery在辅助ONTAP系统上创建复制卷，请确保源系统和目标系统满足以下网络要求。

本地**ONTAP**网络要求

- 如果集群位于本地，则您应该从公司网络连接到云提供商中的虚拟网络。这通常是 VPN 连接。
- ONTAP集群必须满足额外的子网、端口、防火墙和集群要求。

  由于您可以复制到Cloud Volumes ONTAP或本地系统，因此请查看本地ONTAP系统的对等要求。 "查看ONTAP文档中的集群对等前提条件" 。

Cloud Volumes ONTAP网络要求

- 实例的安全组必须包含所需的入站和出站规则：具体来说，ICMP 和端口 11104 和 11105 的规则。这些规则包含在预定义的安全组中。

准备**StorageGRID**作为备份目标

StorageGRID必须满足以下要求。查看 "StorageGRID文档"了解更多信息。

有关StorageGRID的 DataLock 和勒索软件恢复要求的详细信息，请参阅"备份到对象策略选项"。

支持的**StorageGRID**版本

支持StorageGRID 10.3 及更高版本。

要使用 DataLock 和 Ransomware Resilience 进行备份，您的StorageGRID系统必须运行 11.6.0.3 或更高版本。

要将旧备份分层到云档案存储，您的StorageGRID系统必须运行 11.3 或更高版本。此外，您的StorageGRID系统必须在控制台*系统*页面上被发现。

对于用户档案存储，需要管理节点 IP 访问。

始终需要网关 IP 访问。

S3 凭证

您必须创建 S3 租户帐户来控制对StorageGRID存储的访问。 "有关详细信息，请参阅StorageGRID文档" 。

当您设置备份到StorageGRID时，备份向导会提示您输入租户帐户的 S3 访问密钥和密钥。租户帐户使NetApp Backup and Recovery能够验证和访问用于存储备份的StorageGRID桶。需要密钥，以便StorageGRID知道谁在发出请求。

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

您不能在对象存储桶上手动启用StorageGRID对象版本控制。

准备将较旧的备份文件存档到公共云存储

将较旧的备份文件分层到档案存储中可以节省资金，因为您可以使用较便宜的存储类来存储您可能不需要的备份。 StorageGRID是一种内部部署（私有云）解决方案，不提供档案存储，但您可以将较旧的备份文件移动到公共云档案存储。以这种方式使用时，分层到云存储的数据或从云存储恢复的数据会在StorageGRID和云存储之间传输 - 控制台不参与此数据传输。

当前支持使您能够将备份存档到 AWS *S3 Glacier*/*S3 Glacier Deep Archive* 或 *Azure Archive* 存储。

- ONTAP要求*
- 您的集群必须使用ONTAP 9.12.1 或更高版本。
- StorageGRID要求*
- 您的StorageGRID必须使用 11.4 或更高版本。
- 您的StorageGRID必须 "在控制台中发现并可用"。

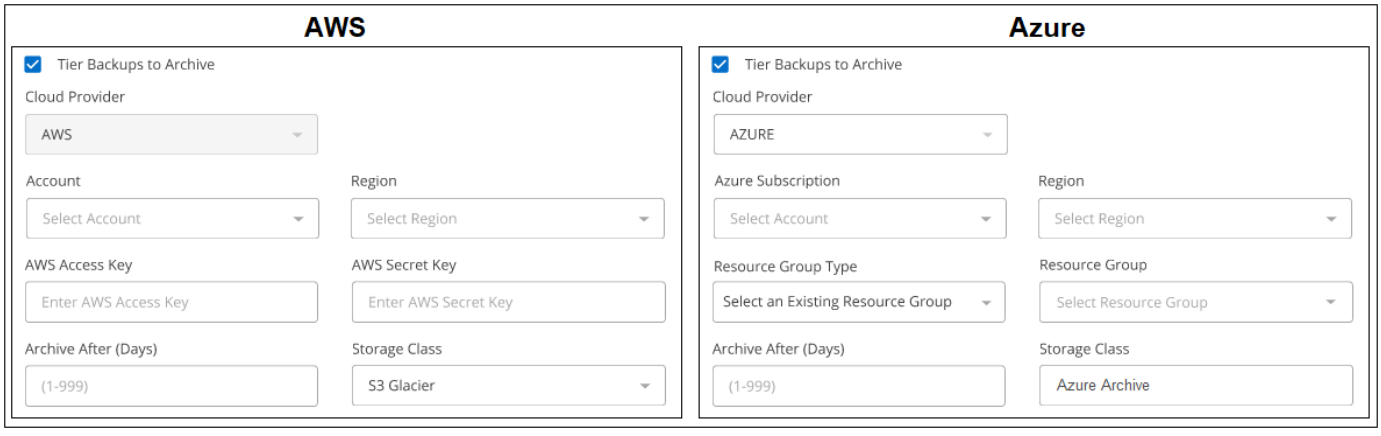
Amazon S3 要求

- 您需要注册一个 Amazon S3 帐户，用于存储存档备份所在的存储空间。
- 您可以选择将备份分层到 AWS S3 Glacier 或 S3 Glacier Deep Archive 存储。"了解有关 AWS 存档层的更多信息"。
- StorageGRID应该对存储桶具有完全控制访问权限(`s3:*`）；但是，如果这不可能，则存储桶策略必须向StorageGRID授予以下 S3 权限：
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Azure Blob 要求

- 您需要注册 Azure 订阅，以获取存档备份所在的存储空间。
- 激活向导使您能够使用现有的资源组来管理将存储备份的 Blob 容器，或者您可以创建一个新的资源组。

在为集群的备份策略定义存档设置时，您将输入云提供商凭据并选择要使用的存储类。当您激活集群备份时，NetApp Backup and Recovery会创建云存储桶。 AWS 和 Azure 档案存储所需的信息如下所示。



您选择的归档策略设置将在StorageGRID中生成信息生命周期管理 (ILM) 策略，并将设置添加为“规则”。

- 如果存在现有的活动 ILM 策略，则会将新规则添加到 ILM 策略中以将数据移动到存档层。
- 如果存在处于“建议”状态的现有 ILM 策略，则无法创建和激活新的 ILM 策略。 "了解有关StorageGRID ILM策略和规则的更多信息" 。

激活ONTAP卷上的备份

随时直接从您的本地系统激活备份。

向导将引导您完成以下主要步骤：

- [选择要备份的卷]
- [定义备份策略]
- [检查您的选择]

您还可以显示 API 命令在审查步骤中，您可以复制代码来自动为未来的系统激活备份。

启动向导

步骤

1. 使用以下方式之一访问激活备份和恢复向导：
   - 从控制台*系统*页面中，选择系统，然后选择右侧面板中备份和恢复旁边的*启用>备份卷*。

     如果备份目标在控制台*系统*页面上作为系统存在，则可以将ONTAP集群拖到对象存储上。
   - 在备份和恢复栏中选择*卷*。从“卷”选项卡中，选择“操作 (…)”选项，然后为单个卷（尚未启用复制或备份到对象存储）选择“激活备份”。

   向导的介绍页面显示保护选项，包括本地快照、复制和备份。如果您在此步骤中选择了第二个选项，则会出现“定义备份策略”页面，其中选择一个卷。
2. 继续以下选项：
   - 如果您已经有控制台代理，那么一切就绪了。只需选择*下一步*。
   - 如果您还没有控制台代理，则会出现“添加控制台代理”选项。参考[准备控制台代理]。

选择要备份的卷

选择您想要保护的卷。受保护的卷是具有以下一项或多项的卷：快照策略、复制策略、备份到对象策略。

您可以选择保护FlexVol或FlexGroup卷；但是，在激活系统备份时不能选择这些卷的混合。了解如何"激活系统中附加卷的备份"（FlexVol或FlexGroup）在为初始卷配置备份后。

- 您一次只能在单个FlexGroup卷上激活备份。
- 您选择的卷必须具有相同的SnapLock设置。所有卷都必须启用SnapLock Enterprise或禁用SnapLock 。

步骤

如果您选择的卷已经应用了快照或复制策略，那么您稍后选择的策略将覆盖这些现有策略。

1. 在“选择卷”页面中，选择要保护的一个或多个卷。
   - 或者，过滤行以仅显示具有特定卷类型、样式等的卷，以便更轻松地进行选择。
   - 选择第一个卷后，您可以选择所有FlexVol卷（FlexGroup卷一次只能选择一个）。要备份所有现有的FlexVol卷，请先选中一个卷，然后选中标题行中的框。
   - 要备份单个卷，请选中每个卷对应的复选框。
2. 选择“下一步”。

定义备份策略

定义备份策略涉及设置以下选项：

- 您是否需要一个或所有备份选项：本地快照、复制和备份到对象存储
- 架构
- 本地快照策略
- 复制目标和策略

  如果您选择的卷具有与您在此步骤中选择的策略不同的快照和复制策略，则现有策略将被覆盖。

- 备份到对象存储信息（提供商、加密、网络、备份策略和导出选项）。

步骤

1. 在“定义备份策略”页面中，选择以下一项或全部。默认情况下，所有三个都被选中：
   - 本地快照：如果您正在执行复制或备份到对象存储，则必须创建本地快照。
   - 复制：在另一个ONTAP存储系统上创建复制卷。
   - 备份：将卷备份到对象存储。
2. 架构：如果您同时选择了复制和备份，请选择以下信息流之一：
   - 级联：信息从主存储流向辅助存储，然后从辅助存储流向对象存储。
   - 扇出：信息从主存储流向辅助存储，再从主存储流向对象存储。

   有关这些架构的详细信息，请参阅"规划您的保护之旅"。
3. 本地快照：选择现有的快照策略或创建新的快照策略。

   要创建自定义策略，请参阅"创建策略"。

   要创建策略，请选择“创建新策略”并执行以下操作：
   - 输入策略的名称。
   - 选择最多五个时间表，通常频率不同。
   - 选择“创建”。

4. 复制：设置以下选项：
   - 复制目标：选择目标系统和 SVM。或者，选择将添加到复制卷名称的目标聚合或聚合以及前缀或后缀。
   - 复制策略：选择现有的复制策略或创建一个。

     要创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：

     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 选择“创建”。
5. 备份到对象：如果您选择了*备份*，请设置以下选项：
   - 提供商：选择* StorageGRID*。
   - 提供商设置：输入提供商网关节点 FQDN 详细信息、端口、访问密钥和密钥。

     访问密钥和密钥适用于您创建的 IAM 用户，用于授予ONTAP集群对存储桶的访问权限。
   - 网络：选择要备份的卷所在的ONTAP集群中的 IP 空间。此 IP 空间的集群间 LIF 必须具有出站互联网访问权限（当控制台代理安装在“暗站”中时不需要）。

     选择正确的 IP 空间可确保NetApp Backup and Recovery可以建立从ONTAP到StorageGRID对象存储的连接。
   - 备份策略：选择现有的备份到对象存储策略或创建一个。

     要创建自定义策略，请参阅"创建策略"。

     要创建策略，请选择“创建新策略”并执行以下操作：

     - 输入策略的名称。
     - 选择最多五个时间表，通常频率不同。
     - 对于备份到对象策略，设置 DataLock 和 Ransomware Resilience 设置。有关 DataLock 和勒索软件恢复的详细信息，请参阅"备份到对象策略设置"。

       如果您的集群使用的是ONTAP 9.11.1 或更高版本，您可以选择通过配置“DataLock”和“Ransomware Resilience”来保护您的备份免遭删除和勒索软件攻击。 *DataLock* 保护您的备份文件不被修改或删除，而 *Ransomware Resilience* 会扫描您的备份文件以查找备份文件中勒索软件攻击的证据。
     - 选择“创建”。

     如果您的集群使用的是ONTAP 9.12.1 或更高版本，并且您的StorageGRID系统使用的是 11.4 或更高版本，您可以选择在一定天数后将旧备份分层到公共云存档层。当前支持 AWS S3 Glacier/S3 Glacier Deep Archive 或 Azure Archive 存储层。了解如何配置您的系统以实现此功能。
   - 分层备份到公共云：选择您想要分层备份的云提供商并输入提供商详细信息。

     选择或创建一个新的StorageGRID集群。有关创建StorageGRID集群以便控制台可以发现它的详细信息

，请参阅 "StorageGRID文档"。

- 将现有快照导出到对象存储作为备份副本：如果此系统中存在与您刚刚为此系统选择的备份计划标签（例如，每日、每周等）匹配的卷的本地快照，则会显示此附加提示。选中此框可将所有历史快照复制到对象存储作为备份文件，以确保对您的卷进行最全面的保护。

6. 选择“下一步”。

检查您的选择

这是审查您的选择并在必要时进行调整的机会。

步骤

1. 在“审核”页面中，审核您的选择。
2. （可选）选中复选框*自动将快照策略标签与复制和备份策略标签同步*。这将创建具有与复制和备份策略中的标签匹配的标签的快照。
3. 选择*激活备份*。

结果

NetApp Backup and Recovery开始对您的卷进行初始备份。复制卷和备份文件的基线传输包括源数据的完整副本。后续传输包含快照中包含的主存储数据的差异副本。

在目标集群中创建一个复制卷，该卷将与主存储卷同步。

在您输入的 S3 访问密钥和密钥指示的服务帐户中创建一个 S3 存储桶，并将备份文件存储在那里。

显示卷备份仪表板，以便您可以监控备份的状态。

您还可以使用"作业监控页面"。

显示 **API** 命令

您可能想要显示并选择性地复制激活备份和恢复向导中使用的 API 命令。您可能希望这样做以便在未来的系统中自动激活备份。

步骤

1. 从激活备份和恢复向导中，选择*查看 API 请求*。
2. 要将命令复制到剪贴板，请选择*复制*图标。

在NetApp Backup and Recovery中使用SnapMirror将卷迁移到 Cloud Resync

NetApp Backup and Recovery中的SnapMirror到云重新同步功能简化了NetApp环境中卷迁移期间的数据保护和连续性。当使用SnapMirror逻辑复制 (LRSE) 将卷从一个本地NetApp部署迁移到另一个部署，或迁移到基于云的解决方案（例如Cloud Volumes ONTAP）时， SnapMirror到 Cloud Resync 可确保现有的云备份保持完整并可正常运行。

此功能无需重新建立基线，即可在迁移后继续备份。此功能在工作负载迁移场景中很有价值，支持 FlexVols 和 FlexGroups，并且从ONTAP版本 9.16.1 开始可用。

此功能从 2025 年 5 月发布的NetApp Backup and Recovery版本 4.0.3 开始提供。

SnapMirror到 Cloud Resync 可跨环境保持备份连续性，从而更容易在混合云和多云环境中管理数据。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

开始之前

确保满足以下先决条件：

- 目标ONTAP集群必须运行ONTAP版本 9.16.1 或更高版本。
- 必须使用NetApp Backup and Recovery保护旧的源ONTAP集群。
- SnapMirror到云重新同步功能从 2025 年 5 月发布的NetApp Backup and Recovery版本 4.0.3 开始提供。
- 确保对象存储中的最新备份是旧源、新源和对象存储的通用快照。不要使用比备份到对象存储的最新快照更旧的通用快照。
- 在开始重新同步操作之前，必须在新ONTAP集群上创建旧ONTAP集群上使用的快照策略和SnapMirror策略。如果在重新同步过程中使用任何策略，则还必须创建该策略。重新同步操作不会创建策略。
- 确保应用于迁移卷SnapMirror关系的SnapMirror策略包含云关系使用的相同标签。为避免出现问题，请使用管理卷和所有快照的精确镜像的策略。

目前不支持使用 SVM-Migrate、SVM-DR 或 Head Swap 方法迁移后将SnapMirror重新同步到Cloud。

NetApp Backup and Recovery SnapMirror到 Cloud Resync 的工作原理

如果您完成技术更新或将卷从一个ONTAP集群迁移到另一个 ONTAP 集群，那么确保备份继续不间断地工作非常重要。 NetApp Backup and Recovery SnapMirror到 Cloud Resync 可帮助您实现这一点，确保您的云备份即使在卷迁移后也能保持一致。

以下是一个例子：

假设您有一个名为 Vol1a 的本地卷。该卷有三个快照：S1、S2 和 S3。这些快照是还原点。 Vol1 使用SnapMirror to Cloud (SM-C) 备份到云端，但对象存储中只有 S1 和 S2。

现在，您想要将 Vol1 迁移到另一个ONTAP集群。为此，您需要创建与名为 Vol1b 的新云卷的SnapMirror逻辑复制 (LRSE) 关系。这会将所有三个快照（S1、S2 和 S3）从 Vol1a 传输到 Vol1b。

迁移完成后，您将获得以下设置：

- 删除原有的SM-C关系（Vol1a→Object store）。
- LRSE 关系 (Vol1a → Vol1b) 也被删除。
- Vol1b 现在是您的活动卷。

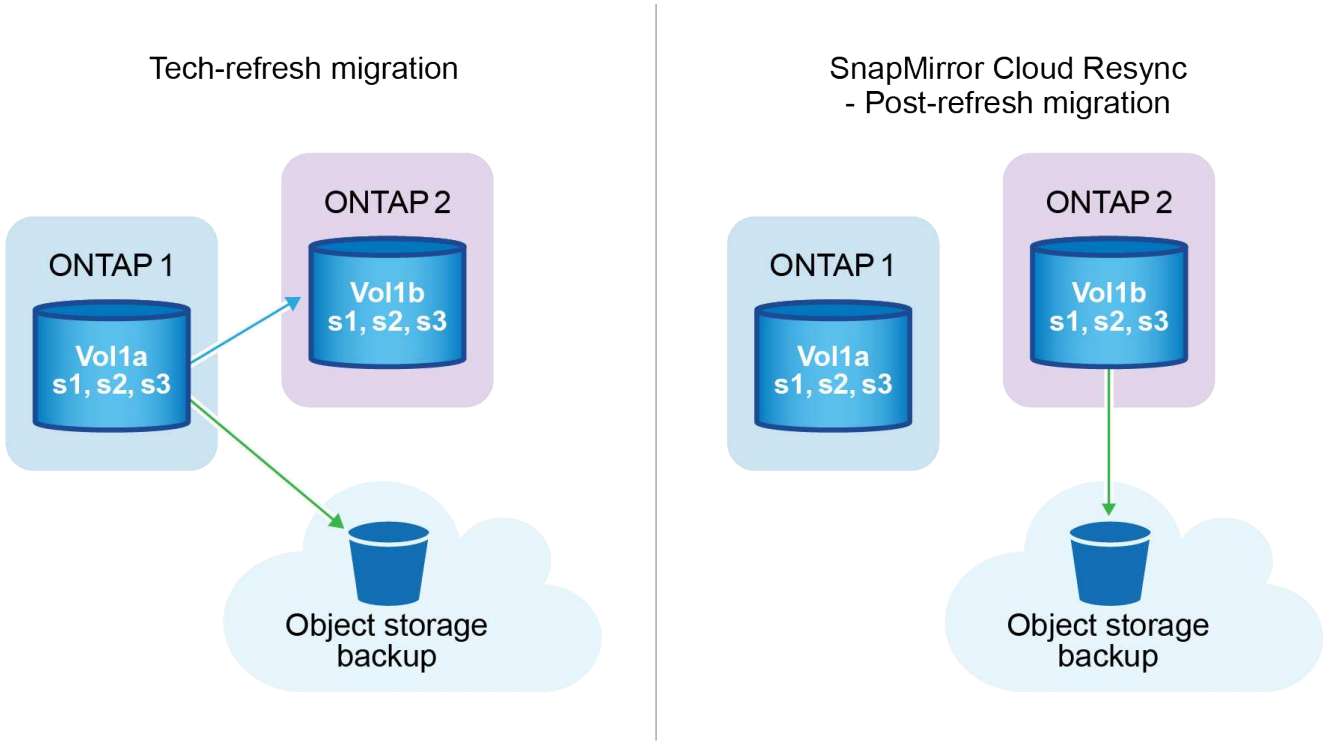
此时，您想要继续将 Vol1b 备份到同一个云端点。但是，您无需从头开始进行完整备份（这会花费时间和资源），而是使用SnapMirror进行 Cloud Resync。

重新同步的工作原理如下：

- 系统检查 Vol1a 和对象存储之间的公共快照。在这种情况下，两者都有 S2。
- 由于这个共享快照，系统只需要传输 S2 和 S3 之间的增量变化。

这意味着只有 S2 之后添加的新数据被发送到对象存储，而不是整个卷。

此过程可防止重复备份，节省带宽，并在迁移后保持备份运行。



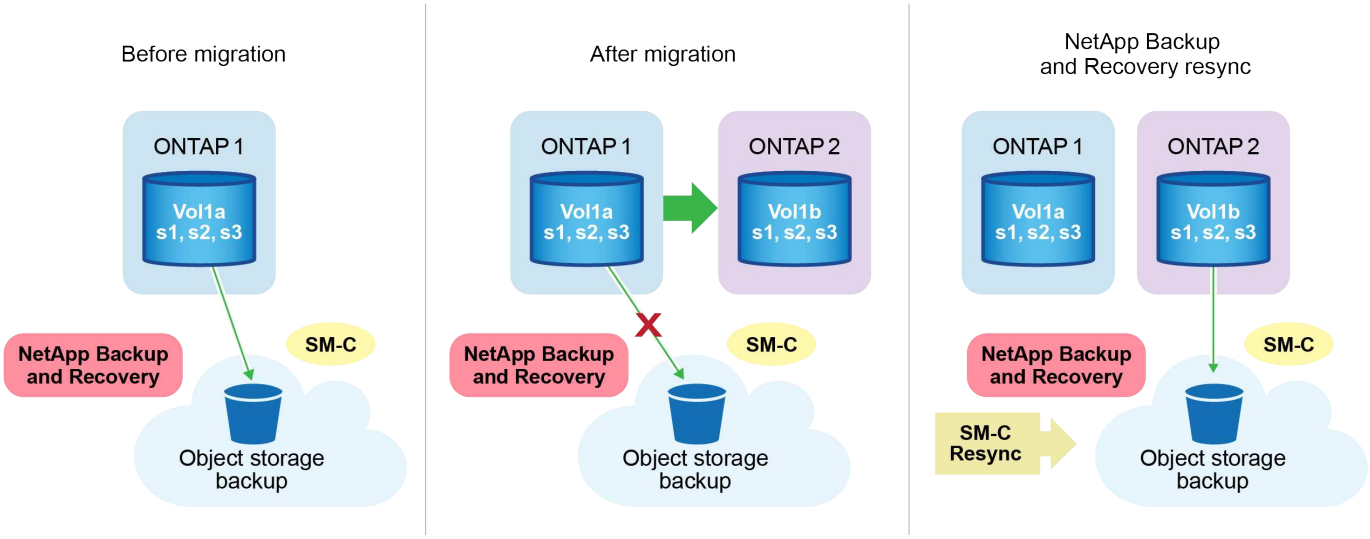
程序说明

- 不使用NetApp Backup and Recovery执行迁移和技术更新。它们应该由专业服务团队或合格的存储管理员来执行。
- NetApp迁移团队会在源 ONTAP 集群和目标ONTAP集群之间创建SnapMirror关系，以帮助迁移卷。
- 确保技术更新期间的迁移基于基于SnapMirror的迁移。

如何使用**SnapMirror**将卷迁移到 **Cloud Resync**

使用SnapMirror到 Cloud Resync 迁移卷涉及以下主要步骤，下面将更详细地描述每个步骤：

- 遵循迁移前检查清单：在开始迁移之前， NetApp Tech Refresh 团队会确保满足以下先决条件，以避免数据丢失并确保迁移过程顺利进行。
- 遵循迁移后检查清单：迁移后， NetApp Tech Refresh 团队确保完成以下步骤以建立保护并为重新同步做好准备。
- 执行**SnapMirror**到 **Cloud Resync**：迁移后， NetApp Tech Refresh 团队执行SnapMirror到 Cloud Resync 操作，以从新迁移的卷恢复云备份。



遵循迁移前检查清单

在迁移之前， NetApp技术更新团队会检查这些先决条件，以防止数据丢失并确保过程顺利进行。

1. 确保所有要迁移的卷都使用NetApp Backup and Recovery进行保护。
2. 记录卷实例 UUID。在开始迁移之前，记下所有卷的实例 UUID。这些标识符对于稍后的映射和重新同步操作至关重要。
3. 在删除任何SnapMirror关系之前，对每个卷进行最终快照以保留最新状态。
4. 记录SnapMirror策略。记录当前附加到每个卷关系的SnapMirror策略。稍后在SnapMirror到 Cloud Resync过程中将需要此功能。
5. 删除SnapMirror Cloud 与对象存储的关系。
6. 与新的ONTAP集群创建标准SnapMirror关系，以将卷迁移到新的目标ONTAP集群。

遵循迁移后检查清单

迁移后， NetApp技术更新团队将确保完成以下步骤以建立保护并为重新同步做好准备。

1. 记录目标ONTAP集群中所有迁移卷的新卷实例 UUID。
2. 确认旧ONTAP集群中可用的所有必需SnapMirror策略均已在新ONTAP集群中正确配置。
3. 在控制台*系统*页面中将新的ONTAP集群添加为系统。

> 应该使用卷实例 UUID，而不是卷 ID。卷实例 UUID 是一个唯一标识符，在迁移过程中保持一致，而卷 ID 可能会在迁移后发生变化。

执行**SnapMirror**到云重新同步

迁移后， NetApp Tech Refresh 团队执行SnapMirror到 Cloud Resync 操作，以从新迁移的卷恢复云备份。

1. 在控制台*系统*页面中将新的ONTAP集群添加为系统。
2. 查看NetApp Backup and Recovery卷页面以确保旧源系统详细信息可用。

3. 从NetApp Backup and Recovery卷页面中，选择*备份设置*。
   - 在备份设置页面中，选择*查看全部*。
   - 从新源右侧的操作…菜单中，选择*重新同步备份*。
4. 在重新同步系统页面中，执行以下操作：
   a. 新源系统：进入已迁移卷的新ONTAP集群。
   b. 现有目标对象存储：选择包含来自旧源系统的备份的目标对象存储。
5. 选择“下载 CSV 模板”以下载重新同步详细信息 Excel 表。使用此表输入要迁移的卷的详细信息。在 CSV 文件中，输入以下详细信息：
   - 源集群中的旧卷实例 UUID
   - 来自目标集群的新卷实例 UUID
   - 要应用于新关系的SnapMirror策略。
6. 选择“上传卷映射详细信息”下的“上传”，将完成的 CSV 表上传到NetApp Backup and RecoveryUI。

   应该使用卷实例 UUID，而不是卷 ID。卷实例 UUID 是一个唯一标识符，在迁移过程中保持一致，而卷 ID 可能会在迁移后发生变化。

7. 输入重新同步操作所需的提供商和网络配置信息。
8. 选择*提交*开始验证过程。

   NetApp Backup and Recovery验证选择重新同步的每个卷是否都是最新快照，并且至少有一个通用快照。这可确保卷已准备好进行SnapMirror到 Cloud Resync 操作。

9. 查看验证结果，包括新的源卷名称和每个卷的重新同步状态。
10. 检查容量是否合格。系统检查卷是否符合重新同步的条件。如果卷不符合条件，则意味着它不是最新的快照或未找到通用快照。

    为了确保卷仍然符合SnapMirror到 Cloud Resync 操作的条件，请在迁移前阶段删除任何SnapMirror关系之前，为每个卷拍摄最终快照。这保留了数据的最新状态。

11. 选择*重新同步*以开始重新同步操作。系统使用最新且通用的快照仅传输增量更改，确保备份的连续性。
12. 在作业监视器页面中监视重新同步过程。

在暗站中恢复NetApp Backup and Recovery配置数据

在没有互联网访问的站点（称为_私有模式_）中使用NetApp Backup and Recovery时，NetApp Backup and Recovery配置数据将备份到存储备份的StorageGRID或ONTAP S3 存储桶中。如果控制台代理主机系统出现问题，您可以部署新的控制台代理并恢复关键的NetApp Backup and Recovery数据。

此过程仅适用于ONTAP卷数据。

当您在 SaaS 环境中使用NetApp Backup and Recovery，并在云提供商或您自己的互联网连接主机上部署控制台代理时，系统会备份并保护云中所有重要的配置数据。如果您遇到控制台代理问题，请创建一个新的控制台代

理并添加您的系统。备份详细信息将自动恢复。

备份的数据有两种类型：

- NetApp Backup and Recovery数据库 - 包含所有卷、备份文件、备份策略和配置信息的列表。
- 索引目录文件 - 包含用于搜索和恢复功能的详细索引，使您在查找要恢复的卷数据时搜索非常快速和有效。

这些数据每天午夜备份一次，每个文件最多保留 7 份副本。如果控制台代理正在管理多个本地ONTAP系统，则NetApp Backup and Recovery文件将存储在首先激活的系统的存储桶中。

NetApp Backup and Recovery数据库或索引目录文件中从未包含任何卷数据。

将**NetApp Backup and Recovery**数据还原到新的控制台代理

如果您的内部控制台代理停止工作，您将需要安装新的控制台代理，然后将NetApp Backup and Recovery数据还原到新的控制台代理。

您需要执行以下任务才能使NetApp Backup and Recovery系统恢复工作状态：

- 安装新的控制台代理
- 还原NetApp Backup and Recovery数据库
- 恢复索引目录文件
- 将所有本地ONTAP系统和StorageGRID系统重新发现到NetApp ConsoleUI

检查系统正常运行后，创建新的备份文件。

你需要什么

您需要从存储备份文件的StorageGRID或ONTAP S3 存储桶访问最新的数据库和索引备份：

- NetApp Backup and RecoveryMySQL 数据库文件

  该文件位于存储桶中的以下位置 `netapp-backup-<GUID>/mysql_backup/`，它被命名为 `CBS_DB_Backup_<day>_<month>_<year>.sql`。

- 索引目录备份 zip 文件

  该文件位于存储桶中的以下位置 `netapp-backup-<GUID>/catalog_backup/`，它被命名为 `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip`。

在新的本地 **Linux** 主机上安装新的控制台代理

安装新的控制台代理时，请下载与原始代理相同的软件版本。 NetApp Backup and Recovery数据库的更改可能会导致较新的软件版本无法与旧的数据库备份一起使用。你可以 "恢复备份数据库后，将控制台代理软件升级到最新版本"。

1. "在新的本地 Linux 主机上安装控制台代理"
2. 使用您刚刚创建的管理员用户凭据登录控制台。

还原**NetApp Backup and Recovery**数据库

1. 将 MySQL 备份从备份位置复制到新的控制台代理主机。下面我们将使用示例文件名“CBS_DB_Backup_23_05_2023.sql”。
2. 根据您使用的是 Docker 还是 Podman 容器，使用以下命令之一将备份复制到 MySQL docker 容器中：

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. 根据您使用的是 Docker 还是 Podman 容器，使用以下命令之一进入 MySQL 容器 shell：

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. 在容器shell中，部署“env”。
5. 您将需要 MySQL DB 密码，因此请复制键“MYSQL_ROOT_PASSWORD”的值。
6. 使用以下命令还原NetApp Backup and RecoveryMySQL DB：

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. 使用以下 SQL 命令验证NetApp Backup and Recovery MySQL DB 是否已正确恢复：

```
mysql -u root -p cloud_backup
```

8. 输入密码。

```
mysql> show tables;
mysql> select * from volume;
```

9. 请确保显示的卷与原始环境中的卷相同。

恢复索引目录文件

1. 将 Indexed Catalog 备份 zip 文件（我们将使用示例文件名“Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip”）从备份位置复制到“/opt/application/netapp/cbs”文件夹中的新控制台代理主机。
2. 使用以下命令解压缩“Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip”文件：

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. 运行 **ls** 命令以确保已创建文件夹“catalogdb1”，其下有子文件夹“changes”和“snapshots”。

发现您的**ONTAP**集群和**StorageGRID**系统

1. "探索所有本地ONTAP系统"在您之前的环境中可用。这包括您用作 S3 服务器的ONTAP系统。
2. "发现您的StorageGRID系统"。

设置**StorageGRID**环境详细信息

添加与您的ONTAP系统关联的StorageGRID系统的详细信息，因为它们是在原始控制台代理设置上使用"NetApp ConsoleAPI"。

以下信息适用于从NetApp Console 3.9.xx 开始的私有模式安装。对于旧版本，请使用以下步骤： "DarkSite 云备份：MySQL 和索引目录备份和恢复" 。

您需要对将数据备份到StorageGRID 的每个系统执行这些步骤。

1. 使用以下 oauth/token API 提取授权令牌。

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

虽然 IP 地址、用户名和密码是自定义值，但帐户名不是。帐户名称始终为“account-DARKSITE1”。此外，用户名必须使用电子邮件格式的名称。

此 API 将返回如下响应。您可以如下所示检索授权令牌。

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. 使用 tenancy/external/resource API 提取系统 ID 和 X-Agent-Id。

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

此 API 将返回如下响应。“resourceIdentifier”下的值表示_WorkingEnvironment Id_，“agentId”下的值表示_x-agent-id_。

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. 使用与系统关联的StorageGRID系统的详细信息更新NetApp Backup and Recovery数据库。确保输入StorageGRID的完全限定域名以及访问密钥和存储密钥，如下所示：

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

验证NetApp Backup and Recovery设置

1. 选择每个ONTAP系统，然后单击右侧面板中备份和恢复服务旁边的“查看备份”。

   您应该会看到为您的卷创建的所有备份。

2. 在“恢复仪表板”的“搜索和恢复”部分下，单击“索引设置”。

   确保之前启用了索引编目的系统仍然保持启用状态。

3. 在“搜索和恢复”页面中，运行一些目录搜索以确认索引目录恢复已成功完成。

使用NetApp Backup and Recovery管理ONTAP系统的备份

借助NetApp Backup and Recovery，您可以通过更改备份计划、启用/禁用卷备份、暂停备份、删除备份、强制删除备份等方式管理Cloud Volumes ONTAP和本地ONTAP系统的备份。这包括所有类型的备份，包括快照、复制卷和对象存储中的备份文件。您还可以取消注册NetApp Backup and Recovery。

请勿直接在存储系统或云提供商环境中管理或更改备份文件。这可能会损坏文件并导致不受支持的配置。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

查看系统中卷的备份状态

您可以在卷备份仪表板中查看当前正在备份的所有卷的列表。这包括所有类型的备份，包括快照、复制卷和对象存储中的备份文件。您还可以查看系统中当前未备份的卷。

步骤

1. 从控制台菜单中，选择*保护>备份和恢复*。
2. 选择“**Volumes**”菜单以查看Cloud Volumes ONTAP和本地ONTAP系统的备份卷列表。
3. 如果您正在寻找特定系统中的特定卷，您可以按系统和卷优化列表。您还可以使用搜索过滤器，或者可以根据卷样式（FlexVol或FlexGroup）、卷类型等对列进行排序。

   要显示其他列（聚合、安全样式（Windows 或 UNIX）、快照策略、复制策略和备份策略），请选择加号。

4. 查看“现有保护”列中保护选项的状态。这 3 个图标分别代表“本地快照”、“复制卷”和“对象存储中的备份”。

   当该备份类型激活时，相应的图标会亮起；当该备份类型未激活时，图标会变为灰色。您可以将鼠标悬停在每个图标上，查看正在使用的备份策略以及每种备份类型的其他相关信息。

激活系统中附加卷的备份

如果您在首次启用NetApp Backup and Recovery时仅在系统中的某些卷上激活了备份，则可以稍后在其他卷上激活备份。

步骤

1. 在“卷”选项卡中，找到要激活备份的卷，然后选择“操作”菜单。 ••• 在行尾，选择“激活 3-2-1 保护”。
2. 在“定义备份策略”页面中，选择备份架构，然后定义本地快照、复制卷和备份文件的策略和其他详细信息。查看您在此系统中激活的初始卷的备份选项的详细信息。然后选择“下一步”。
3. 检查此卷的备份设置，然后选择*激活备份*。

更改分配给现有卷的备份设置

您可以更改分配给已分配策略的现有卷的备份策略。您可以更改本地快照、复制卷和备份文件的策略。您想要应用于卷的任何新快照、复制或备份策略都必须已经存在。

编辑单个卷上的备份设置

步骤

1. 从“卷”菜单中，找到要修改策略设置的卷，然后选择“操作”菜单。 ••• 在行尾，选择“编辑备份策略”。
2. 在“编辑备份策略”页面中，对本地快照、复制卷和备份文件的现有备份策略进行更改，然后选择“下一步”。

   如果在为此集群激活NetApp Backup and Recovery时，在初始备份策略中为云备份启用了 *DataLock* 和 *Ransomware Resilience*，您将只会看到已使用 DataLock 配置的其他策略。如果您在激活NetApp Backup and Recovery时未启用“DataLock 和 Ransomware Resilience”，您将只会看到未配置 DataLock 的其他云备份策略。

3. 检查此卷的备份设置，然后选择*激活备份*。

编辑多个卷上的备份设置

如果您想在多个卷上使用相同的备份设置，您可以同时在多个卷上激活或编辑备份设置。您可以选择没有备份设置、只有快照设置、只有备份到云设置等的卷，并使用不同的备份设置对所有这些卷进行批量更改。

当使用多个卷时，所有卷必须具有以下共同特征：

- 同一系统
- 相同样式（FlexVol或FlexGroup卷）
- 相同类型（读写或数据保护卷）

当启用备份的卷超过五个时， NetApp Backup and Recovery一次只会初始化五个卷。当这些完成后，它会以 5 个为一组继续进行，直到所有卷都初始化完毕。

步骤

1. 从“卷”选项卡中，按卷所在的系统进行过滤。
2. 选择您想要管理备份设置的所有卷。
3. 根据您要配置的备份操作类型，单击批量操作菜单中的按钮：

备份操作...	选择此按钮...
管理快照备份设置	管理本地快照
管理复制备份设置	管理复制
管理备份到云备份设置	管理备份
管理多种类型的备份设置。此选项还使您能够更改备份架构。	管理备份和恢复

4. 在出现的备份页面中，对本地快照、复制卷或备份文件的现有备份策略进行更改，然后选择“保存”。

   如果在为此集群激活NetApp Backup and Recovery时，在初始备份策略中为云备份启用了 *DataLock* 和 *Ransomware Resilience*，您将只会看到已使用 DataLock 配置的其他策略。如果您在激活NetApp Backup and Recovery时未启用“DataLock 和 Ransomware Resilience”，您将只会看到未配置 DataLock 的其他云备份策略。

随时创建手动卷备份

您可以随时创建按需备份来捕获卷的当前状态。如果对卷进行了非常重要的更改并且您不想等待下一次计划的备份来保护该数据，这将非常有用。您还可以使用此功能为当前未备份且想要捕获其当前状态的卷创建备份。

您可以创建卷的临时快照或备份到对象存储。您无法创建临时复制卷。

备份名称包含时间戳，以便您可以从其他计划备份中识别出您的按需备份。

如果在为此集群激活NetApp Backup and Recovery时启用了“DataLock 和 Ransomware Resilience”，则按需备份也将配置 DataLock，保留期为 30 天。临时备份不支持勒索软件扫描。"了解有关 DataLock 和勒索软件保护的更多信息"。

当您创建临时备份时，会在源卷上创建快照。由于此快照不是正常快照计划的一部分，因此它不会旋转。备份完成后，您可能希望从源卷中手动删除此快照。这将允许释放与此快照相关的块。快照名称将以 `cbs-snapshot-adhoc-`。 "了解如何使用ONTAP CLI 删除快照" 。

数据保护卷不支持按需卷备份。

步骤

1. 从“卷”选项卡中选择•••对于卷并选择*备份*>*创建临时备份*。

该卷的备份状态列显示“进行中”，直到备份创建完成。

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（例如上次备份、当前备份策略、备份文件大小等）。

步骤

1. 从“卷”选项卡中选择•••对于源卷并选择*查看卷详细信息*。

   显示卷的详细信息和快照列表。

2. 选择“快照”、“复制”或“备份”以查看每种备份类型的所有备份文件列表。

对对象存储中的卷备份运行勒索软件扫描

当创建目标文件备份时以及恢复备份文件中的数据时， NetApp Backup and Recovery会扫描您的备份文件以查找勒索软件攻击的证据。您还可以随时运行按需扫描，以验证对象存储中特定备份文件的可用性。如果您在特定卷上遇到勒索软件问题并且想要验证该卷的备份不受影响，这将很有用。

仅当卷备份是从具有ONTAP 9.11.1 或更高版本的系统创建的，并且在备份到对象策略中启用了_DataLock 和 Ransomware Resilience_ 时，此功能才可用。

步骤

1. 从“卷”选项卡中选择•••对于源卷并选择*查看卷详细信息*。

   将显示该卷的详细信息。

2. 选择*备份*以查看对象存储中的备份文件列表。
3. 选择•••对于您想要扫描勒索软件的卷备份文件，然后单击*扫描勒索软件*。

   勒索软件恢复力列显示扫描正在进行中。

管理与源卷的复制关系

在两个系统之间设置数据复制后，您可以管理数据复制关系。

步骤

1. 从“卷”选项卡中选择•••对于源卷并选择*复制*选项。您可以看到所有可用的选项。
2. 选择您想要执行的复制操作。

下表描述了可用的操作：

操作	描述
查看复制	显示有关卷关系的详细信息：传输信息、上次传输信息、有关卷的详细信息以及有关分配给该关系的保护策略的信息。
更新复制	启动增量传输来更新目标卷，使其与源卷同步。
暂停复制	暂停快照的增量传输，以更新目标卷。如果您想重新开始增量更新，可以稍后再恢复。
中断复制	打破源卷和目标卷之间的关系，并激活目标卷进行数据访问 - 使其可读写。当源卷由于数据损坏、意外删除或离线状态等事件而无法提供数据时，通常使用此选项。https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["了解如何在ONTAP文档中配置目标卷以进行数据访问并重新激活源卷"^]
中止复制	禁用将此卷备份到目标系统，并且还禁用还原卷的功能。任何现有的备份都不会被删除。这不会删除源卷和目标卷之间的数据保护关系。
反向重新同步	反转源卷和目标卷的角色。原始源卷的内容将被目标卷的内容覆盖。当您想要重新激活离线的源卷时，这很有用。上次数据复制和源卷禁用之间写入原始源卷的任何数据都不会保留。
删除关系	删除源卷和目标卷之间的数据保护关系，这意味着卷之间不再发生数据复制。此操作不会激活目标卷以进行数据访问 - 这意味着它不会使其可读写。如果系统之间没有其他数据保护关系，此操作还会删除集群对等关系和存储虚拟机 (SVM) 对等关系。

结果

选择操作后，控制台将更新关系。

编辑现有的备份到云策略

您可以更改当前应用于系统中的卷的备份策略的属性。更改备份策略会影响所有使用该策略的现有卷。

- 如果在为此集群激活NetApp Backup and Recovery时在初始策略中启用了_DataLock 和 Ransomware Resilience_，则您编辑的任何策略都必须配置相同的 DataLock 设置（治理或合规性）。如果您在激活NetApp Backup and Recovery时未启用“DataLock 和 Ransomware Resilience”，则现在无法启用 DataLock。
- 在 AWS 上创建备份时，如果您在激活NetApp Backup and Recovery时在第一个备份策略中选择了 *S3 Glacier* 或 *S3 Glacier Deep Archive*，则该层将是编辑备份策略时唯一可用的存档层。如果您在第一个备份策略中未选择存档层，那么在编辑策略时，*S3 Glacier* 将是您唯一的存档选项。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 在“备份设置”页面中，选择…对于您想要更改策略设置的系统，然后选择*管理策略*。
3. 在“管理策略”页面中，选择您想要在该系统中更改的备份策略的“编辑”。
4. 在“编辑策略”页面中，选择向下箭头展开“标签和保留”部分以更改计划和/或备份保留，然后选择“保存”。

   如果您的集群运行的是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备份分层到档案存储。

"了解有关使用 AWS 档案存储的更多信息"。"了解有关使用 Azure 档案存储的详细信息"。"详细了解如何使用 Google 归档存储"。（需要ONTAP 9.12.1。）

请注意，如果您停止将备份分层到归档存储，则任何已分层到归档存储的备份文件仍将保留在该层中 - 它们不会自动移回标准层。只有新创建的卷备份才会位于标准层。

添加新的备份到云策略

当您为系统启用NetApp Backup and Recovery时，您最初选择的所有卷都将使用您定义的默认备份策略进行备份。如果您想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。

如果要将新的备份策略应用到系统中的某些卷，首先需要将备份策略添加到系统中。然后你可以将策略应用于该系统中的卷。

- 如果在为此集群激活NetApp Backup and Recovery时在初始策略中启用了_DataLock 和 Ransomware Resilience_，则您创建的任何其他策略都必须使用相同的 DataLock 设置（治理或合规性）进行配置。如果您在激活NetApp Backup and Recovery时未启用“DataLock 和 Ransomware Resilience”，则无法创建使用 DataLock 的新策略。
- 在 AWS 上创建备份时，如果您在激活NetApp Backup and Recovery时在第一个备份策略中选择了 *S3 Glacier* 或 *S3 Glacier Deep Archive*，则该层将是该集群未来备份策略可用的唯一存档层。如果您在第一个备份策略中未选择存档层，那么_S3 Glacier_ 将是您未来策略的唯一存档选项。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 在“备份设置”页面中，选择•••对于您想要添加新策略的系统，然后选择*管理策略*。
3. 从“管理策略”页面中，选择“添加新策略”。
4. 在“添加新策略”页面中，选择向下箭头展开“标签和保留”部分以定义计划和备份保留，然后选择“保存”。

   如果您的集群运行的是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备份分层到档案存储。

   "了解有关使用 AWS 档案存储的更多信息"。"了解有关使用 Azure 档案存储的详细信息"。"详细了解如何使用 Google 归档存储"。（需要ONTAP 9.12.1。）

删除备份

NetApp Backup and Recovery使您能够删除单个备份文件、删除卷的所有备份或删除系统中所有卷的所有备份。如果您不再需要备份，或者您删除了源卷并想要删除所有备份，则可能需要删除所有备份。

您无法删除使用 DataLock 和勒索软件保护锁定的备份文件。如果您选择了一个或多个锁定的备份文件，则 UI 中的“删除”选项将不可用。

如果您计划删除具有备份的系统或集群，则必须在删除系统之前删除备份。当您删除系统时，NetApp Backup and Recovery不会自动删除备份，并且 UI 中当前不支持在删除系统后删除备份。您将继续为任何剩余的备份支付对象存储费用。

删除系统的所有备份文件

删除系统对象存储上的所有备份并不会禁用该系统中卷的未来备份。如果要停止创建系统中所有卷的备份，您可以停用备份如此处所述。

请注意，此操作不会影响快照或复制卷——这些类型的备份文件不会被删除。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 选择…对于要删除所有备份的系统，然后选择*删除所有备份*。
3. 在确认对话框中，输入系统的名称。
4. 选择“高级设置”。
5. 强制删除备份：指示是否要强制删除所有备份。

   在某些极端情况下，您可能希望NetApp Backup and Recovery不再访问备份。例如，如果服务不再有权访问备份存储桶或备份受到 DataLock 保护但您不再需要它们，则可能会发生这种情况。以前，您无法自行删除这些内容，而需要致电NetApp支持。在此版本中，您可以使用选项强制删除备份（在卷和系统级别）。

   请谨慎使用此选项，并且仅在极端清理需要时使用。即使这些备份未被从对象存储中删除，NetApp Backup and Recovery也将无法再访问它们。您需要前往云提供商并手动删除备份。

6. 选择*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。

步骤

1. 在“卷”选项卡中，单击…对于源卷并选择*详细信息和备份列表*。

   显示所有备份文件的列表。

2. 选择*操作* > 删除所有备份。
3. 输入卷名称。
4. 选择“高级设置”。
5. 强制删除备份：指示是否要强制删除所有备份。

   在某些极端情况下，您可能希望NetApp Backup and Recovery不再访问备份。例如，如果服务不再有权访问备份存储桶或备份受到 DataLock 保护但您不再需要它们，则可能会发生这种情况。以前，您无法自行删除这些内容，而需要致电NetApp支持。在此版本中，您可以使用选项强制删除备份（在卷和系统级别）。

   请谨慎使用此选项，并且仅在极端清理需要时使用。即使这些备份未被从对象存储中删除，NetApp Backup and Recovery也将无法再访问它们。您需要前往云提供商并手动删除备份。

6. 选择*删除*。

删除卷的单个备份文件

如果您不再需要单个备份文件，可以将其删除。这包括删除卷快照的单个备份或对象存储中的备份。

您不能删除复制的卷（数据保护卷）。

步骤

1. 从“卷”选项卡中选择•••对于源卷并选择*查看卷详细信息*。

   显示卷的详细信息，您可以选择*快照*、*复制*或*备份*来查看该卷的所有备份文件的列表。默认情况下，会显示可用的快照。

2. 选择“快照”或“备份”来查看要删除的备份文件类型。
3. 选择•••对于要删除的卷备份文件，然后选择*删除*。
4. 在确认对话框中，选择*删除*。

删除卷备份关系

如果您想停止创建新的备份文件并删除源卷，但保留所有现有的备份文件，则删除卷的备份关系为您提供了一种存档机制。这样，您就可以在将来需要时从备份文件中恢复卷，同时清除源存储系统中的空间。

您不一定需要删除源卷。您可以删除卷的备份关系并保留源卷。在这种情况下，您可以稍后在卷上“激活”备份。在这种情况下，将继续使用原始基线备份副本 - 不会创建新的基线备份副本并将其导出到云端。请注意，如果您重新激活备份关系，则会为该卷分配默认备份策略。

仅当您的系统运行ONTAP 9.12.1 或更高版本时，此功能才可用。

您无法从NetApp Backup and Recovery用户界面删除源卷。但是，您可以打开控制台*系统*页面上的卷详细信息页面，然后 "从那里删除卷"。

一旦关系被删除，您就无法删除单个卷备份文件。但是，您可以删除该卷的所有备份。

步骤

1. 从“卷”选项卡中选择•••对于源卷，然后选择*备份*>*删除关系*。

停用系统的**NetApp Backup and Recovery**

停用系统的NetApp Backup and Recovery会禁用系统上每个卷的备份，还会禁用还原卷的功能。任何现有的备份都不会被删除。这不会从系统中取消注册备份服务 - 它基本上允许您暂停所有备份和恢复活动一段时间。

请注意，除非您删除备份。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 从“备份设置”页面中选择•••对于您想要禁用备份的系统，然后选择*停用备份*。
3. 在确认对话框中，选择*停用*。

当备份被禁用时，该系统会出现一个“激活备份”按钮。当您想要重新启用该系统的备份功能时，可以选择此按钮。

取消注册系统的NetApp Backup and Recovery

如果您不再想使用备份功能并且不想再为该系统的备份付费，则可以取消注册NetApp Backup and Recovery 。通常，当您计划删除系统并想要取消备份服务时使用此功能。

如果您想更改存储集群备份的目标对象存储，也可以使用此功能。取消注册系统的NetApp Backup and Recovery后，您可以使用新的云提供商信息为该集群启用NetApp Backup and Recovery 。

在取消注册NetApp Backup and Recovery之前，您必须按顺序执行以下步骤：

- 停用系统的NetApp Backup and Recovery
- 删除该系统的所有备份

这两个操作完成之前，取消注册选项不可用。

步骤

1. 从*Volumes*选项卡中，选择*Backup Settings*。
2. 从“备份设置”页面中选择•••对于您想要取消注册备份服务的系统，然后选择*取消注册*。
3. 在确认对话框中，选择*取消注册*。

从ONTAP备份还原

使用NetApp Backup and Recovery从备份文件恢复ONTAP数据

ONTAP卷数据的备份以快照的形式存储在复制卷上，或存储在对象存储中。您可以从这些位置中的任何一个位置恢复特定时间点的数据。使用NetApp Backup and Recovery，您可以根据需要恢复整个卷、文件夹或单个文件。

要切换到NetApp Backup and Recovery工作负载，请参阅"切换到不同的NetApp Backup and Recovery工作负载"。

- 您可以将*卷*（作为新卷）还原到原始系统、使用相同云帐户的其他系统或本地ONTAP系统。
- 您可以将*文件夹*还原到原始系统中的卷、使用相同云帐户的不同系统中的卷或本地ONTAP系统上的卷。
- 您可以将*文件*还原到原始系统中的卷、使用相同云帐户的不同系统中的卷或本地ONTAP系统上的卷。

您需要有效的NetApp Backup and Recovery许可证才能将数据恢复到生产系统。

总而言之，这些是可用于将卷数据还原到ONTAP系统的有效流程：

- 备份文件 → 恢复卷
- 复制卷 → 恢复卷
- 快照 → 已恢复卷

如果还原操作未完成，请等到作业监视器显示“失败”后再重试还原操作。

有关还原ONTAP数据的限制，请参阅"ONTAP卷的备份和还原限制"。

恢复仪表板

您可以使用还原仪表板执行卷、文件夹和文件还原操作。要访问恢复仪表板，请从控制台菜单中选择“备份和恢复”，然后选择“恢复”选项卡。您也可以选择 从“服务”面板的“备份和恢复服务”中查看“恢复仪表板”。

NetApp Backup and Recovery必须已为至少一个系统激活，并且必须存在初始备份文件。

恢复仪表板提供了两种从备份文件恢复数据的不同方法：浏览和恢复*和*搜索和恢复。

比较“浏览和还原”与“搜索和还原”

广义上讲，当您需要恢复上周或上个月的特定卷、文件夹或文件时，_浏览和恢复_通常更好——并且您知道文件的名称和位置，以及文件最后处于良好状态的日期。当您需要恢复卷、文件夹或文件，但不记得确切的名称、它所在的卷或它最后处于良好状态的日期时，_搜索和恢复_通常会更好。

该表提供了两种方法的功能比较。

浏览和恢复	搜索和恢复
浏览文件夹样式结构以查找单个备份文件中的卷、文件夹或文件。	通过部分或完整卷名、部分或完整文件夹/文件名、大小范围和其他搜索过滤器，在*所有备份文件*中搜索卷、文件夹或文件。
如果文件已被删除或重命名，并且用户不知道原始文件名，则不处理文件恢复	处理新创建/删除/重命名的目录和新创建/删除/重命名的文件
支持快速恢复。	不支持快速恢复。

该表根据备份文件所在的位置提供了有效还原操作的列表。

备份类型	浏览和恢复			搜索和恢复		
	恢复音量	恢复文件	恢复文件夹	恢复音量	恢复文件	恢复文件夹
Snapshot	是	否	否	是	是	是
复制卷	是	否	否	是	是	是
备份文件	是	是	是	是	是	是

在使用任何一种恢复方法之前，请配置您的环境以满足资源要求。详情请见以下章节。

请参阅要使用的还原操作类型的要求和还原步骤：

- "使用“浏览和恢复”恢复卷"
- "使用“浏览和恢复”功能恢复文件夹和文件"
- "使用“搜索和还原”功能还原卷、文件夹和文件"

使用搜索和恢复功能从**ONTAP**备份恢复

您可以使用搜索和恢复功能从ONTAP备份文件中恢复卷、文件夹或文件。搜索和恢复功能允许您搜索所有备份（包括本地快照、复制卷和对象存储），而无需提供确切的系统、卷或文件名。

从本地快照或复制卷恢复通常比从对象存储恢复更快、更便宜。

恢复整个卷时， NetApp Backup and Recovery会使用备份数据创建一个新卷。您可以恢复到原始系统、同一云帐户内的另一个系统或本地ONTAP系统。文件夹和文件可以恢复到其原始位置、同一系统中的不同卷、同一云帐户中的另一个系统或本地系统。

恢复功能取决于您的ONTAP版本：

- 文件夹： 使用ONTAP 9.13.0 或更高版本，您可以恢复包含所有文件和子文件夹的文件夹；使用早期版本，您只能恢复文件夹中的文件。
- *归档存储：*从归档存储恢复（ ONTAP 9.10.1 或更高版本可用）速度较慢，并且可能会产生额外费用。
- 目标集群要求：
  - 卷恢复： ONTAP 9.10.1 或更高版本
  - 文件恢复： ONTAP 9.11.1 或更高版本
  - Google Archive 和StorageGRID： ONTAP 9.12.1 或更高版本
  - 文件夹恢复： ONTAP 9.13.1 或更高版本

"了解有关从 AWS 档案存储恢复的更多信息"。"了解有关从 Azure 档案存储还原的详细信息"。"详细了解如何从 Google 存档存储中恢复"。

- 如果对象存储中的备份文件已配置 DataLock 和勒索软件保护，则仅当ONTAP版本为 9.13.1 或更高版本时才支持文件夹级还原。如果您使用的是早期版本的ONTAP，则可以从备份文件恢复整个卷，然后访问所需的文件夹和文件。
- 如果对象存储中的备份文件驻留在档案存储中，则仅当ONTAP版本为 9.13.1 或更高版本时才支持文件夹级还原。如果您使用的是早期版本的ONTAP，则可以从尚未存档的较新备份文件中还原文件夹，也可以从存档的备份中还原整个卷，然后访问所需的文件夹和文件。
- 将数据从 Azure 档案存储还原到StorageGRID系统时，不支持“高”还原优先级。
- 目前不支持从ONTAP S3 对象存储中的卷还原文件夹。

在开始之前，您应该对要还原的卷或文件的名称或位置有所了解。

搜索和恢复支持的系统和对象存储提供商

您可以将ONTAP数据从位于二级系统（复制卷）或对象存储（备份文件）中的备份文件还原到以下系统。快照保存在源系统上，并且只能还原到同一系统。

*注意：*您可以从任何类型的备份文件恢复卷和文件，但目前只能从对象存储中的备份文件恢复文件夹。

备份文件位置		目的地系统
对象存储（备份）	辅助系统（复制）	
Amazon S3	AWS 本地ONTAP系统中的Cloud Volumes ONTAP	AWS 本地ONTAP系统中的Cloud Volumes ONTAP
Azure Blob	Azure 本地ONTAP系统中的Cloud Volumes ONTAP	Azure 本地ONTAP系统中的Cloud Volumes ONTAP

备份文件位置		目的地系统
Google Cloud Storage	Google 本地ONTAP系统中的Cloud Volumes ONTAP	Google 本地ONTAP系统中的Cloud Volumes ONTAP
NetAppStorageGRID	本地ONTAP系统Cloud Volumes ONTAP	本地ONTAP系统
ONTAP S3	本地ONTAP系统Cloud Volumes ONTAP	本地ONTAP系统

对于搜索和还原，控制台代理可以安装在以下位置：

- 对于 Amazon S3，控制台代理可以部署在 AWS 或您的场所
- 对于 Azure Blob，控制台代理可以部署在 Azure 中或您的本地
- 对于 Google Cloud Storage，控制台代理必须部署在您的 Google Cloud Platform VPC 中
- 对于StorageGRID，控制台代理必须部署在您的场所；无论是否有互联网访问
- 对于ONTAP S3，控制台代理可以部署在您的场所（有或没有互联网访问）或云提供商环境中

请注意，“本地ONTAP系统”包括FAS、 AFF和ONTAP Select系统。

搜索与恢复的先决条件

启用搜索和恢复功能前，请确保您的环境满足以下要求：

- 集群要求：
  - ONTAP版本必须为 9.8 或更高版本。
  - 卷所在的存储虚拟机 (SVM) 必须具有配置的数据 LIF。
  - 必须在卷上启用 NFS（支持 NFS 和 SMB/CIFS 卷）。
  - 必须在 SVM 上激活 SnapDiff RPC 服务器。当您在系统上启用索引时，控制台会自动执行此操作。（SnapDiff 是一种能够快速识别快照之间文件和目录差异的技术。）
- NetApp建议在控制台代理上挂载单独的卷，以提高搜索和恢复的弹性。有关说明，请参阅挂载卷以重新索引目录。

旧版搜索与恢复的先决条件（使用索引目录 **v1**）

以下是使用传统索引时搜索和恢复功能的要求：

- AWS 要求：
  - 必须将特定的 Amazon Athena、AWS Glue 和 AWS S3 权限添加到为控制台提供权限的用户角色。"确保所有权限均已正确配置"。

    请注意，如果您已经使用NetApp Backup and Recovery以及您过去配置的控制台代理，则现在需要将 Athena 和 Glue 权限添加到控制台用户角色。它们是搜索和恢复所必需的。

- Azure 要求：
  - 您必须向您的订阅注册 Azure Synapse Analytics 资源提供程序（称为“Microsoft.Synapse”）。"了解如何为您的订阅注册此资源提供程序" 。您必须是订阅*所有者*或*贡献者*才能注册资源提供者。
  - 必须将特定的 Azure Synapse Workspace 和 Data Lake Storage 帐户权限添加到为控制台提供权限的用户角色。"确保所有权限均已正确配置"。

    请注意，如果您已经使用过去配置的控制台代理来使用NetApp Backup and Recovery ，则现在需要将 Azure Synapse Workspace 和 Data Lake Storage 帐户权限添加到控制台用户角色。它们是搜索和恢复所必需的。

  - 控制台代理必须配置为*不带*代理服务器才能与互联网进行 HTTP 通信。如果您已为控制台代理配置了 HTTP 代理服务器，则无法使用搜索和还原功能。
- Google Cloud 要求：
  - 必须将特定的 Google BigQuery 权限添加到为NetApp Console提供权限的用户角色。"确保所有权限均已正确配置"。

    如果您已经使用NetApp Backup and Recovery以及您过去配置的控制台代理，则现在需要将 BigQuery 权限添加到控制台用户角色。它们是搜索和恢复所必需的。

- StorageGRID和ONTAP S3 要求：

  根据您的配置，有两种方法可以实现“搜索和还原”：

  - 如果您的帐户中没有云提供商凭据，则索引目录信息将存储在控制台代理上。

    有关索引目录 v2 的信息，请参阅下面有关如何启用索引目录的部分。

  - 如果您在私人（暗）站点中使用控制台代理，则索引目录信息将存储在控制台代理上（需要控制台代理版本 3.9.25 或更高版本）。
  - 如果你有 "AWS 凭证"或者 "Azure 凭据"在帐户中，索引目录存储在云提供商处，就像在云中部署控制台代理一样。 （如果您拥有这两个凭证，则默认选择 AWS。）

    即使您使用的是本地控制台代理，也必须满足控制台代理权限和云提供商资源的云提供商要求。使用此实现时，请参阅上面的 AWS 和 Azure 要求。

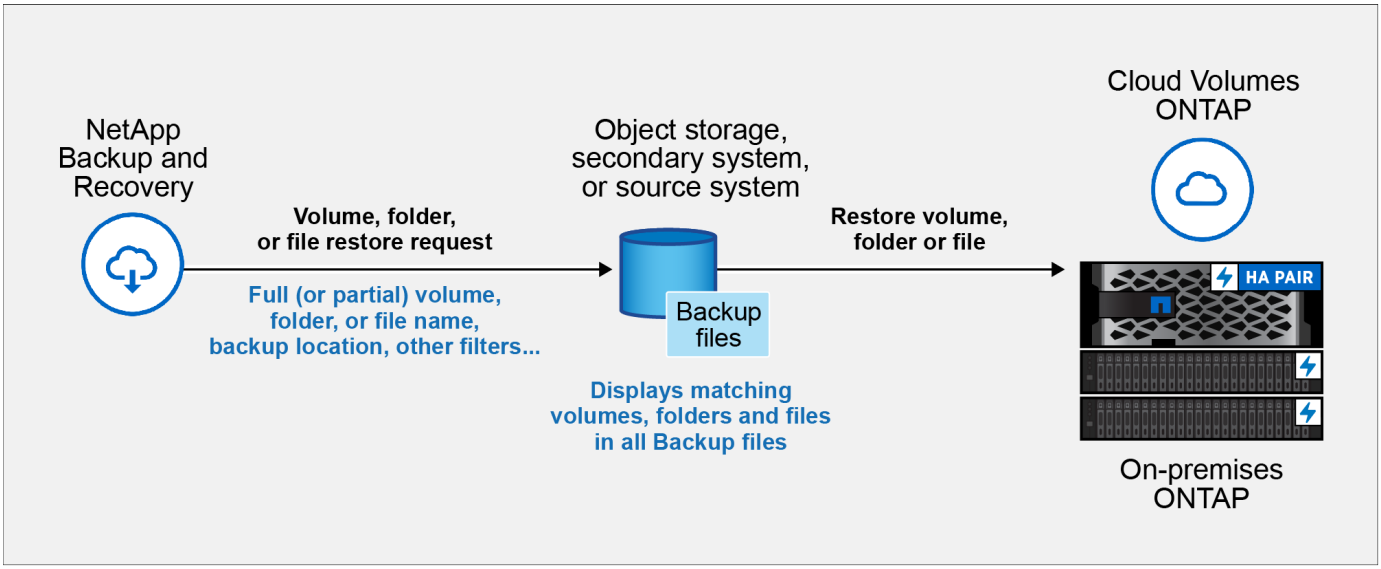
搜索和恢复过程

这个过程如下：

1. 在使用搜索和还原之前，您需要在要从中还原卷数据的每个源系统上启用“索引”。这使得索引目录可以跟踪每个卷的备份文件。

2. 当您想要从卷备份中恢复卷或文件时，在“搜索和恢复”下选择“搜索和恢复”。
3. 通过部分或完整卷名、部分或完整文件名、备份位置、大小范围、创建日期范围、其他搜索过滤器输入卷、文件夹或文件的搜索条件，然后选择*搜索*。

   搜索结果页面显示具有符合搜索条件的文件或卷的所有位置。
4. 选择要用于恢复卷或文件的位置的“查看所有备份”，然后在要使用的实际备份文件上选择“恢复”。
5. 选择您想要恢复卷、文件夹或文件的位置，然后选择*恢复*。
6. 卷、文件夹或文件已恢复。



您只需要知道部分名称， NetApp Backup and Recovery就会搜索所有与您的搜索匹配的备份文件。

为每个系统启用索引目录

在使用搜索和还原之前，您需要在计划还原卷或文件的每个源系统上启用“索引”。这使得索引目录可以跟踪每个卷和每个备份文件 - 使您的搜索非常快速和高效。

索引目录是一个数据库，用于存储系统中所有卷和备份文件的元数据。搜索和恢复功能使用它来快速找到包含要恢复的数据的备份文件。

索引目录功能

使用索引目录时， NetApp Backup and Recovery不会配置单独的存储桶。相反，对于存储在 AWS、Azure 、Google Cloud Platform、 StorageGRID或ONTAP S3 中的备份，该服务会在控制台代理或云提供商环境上提供空间。

索引目录支持以下功能：

- 3分钟内即可实现全球搜索效率
- 最多 50 亿个文件
- 每个集群最多 5000 个卷
- 每个卷最多 10 万个快照
- 基线索引的最长时间少于 7 天。实际时间将根据您的环境而有所不同。

为系统启用索引的步骤：

如果您的系统已启用索引，请转到下一部分来恢复您的数据。

您首先需要挂载一个单独的卷来存放目录文件。这样可以防止因保存快照的文件过大而导致数据丢失。并非每个集群都需要这样做；您可以从环境中的任何集群挂载任何一个卷。如果不这样做，索引可能无法正常工作。

对于装订体积，请参考以下尺寸指南：

- 使用NetApp NFS 卷
- 推荐使用磁盘吞吐量为 300 MB/s 的AFF存储。吞吐量降低会影响搜索和其他操作。
- 启用NetApp快照功能，除了保护目录备份 zip 文件外，还可以保护目录元数据。
- 每10亿个文件占用50GB空间
- 目录数据占用 20 GB 空间，另有空间用于创建 zip 文件和存放临时文件。

挂载卷以重新索引目录的步骤

1. 将卷挂载到 `/opt/application/netapp/cbs` 输入以下命令，其中：
    - `volume name` 这是集群上用于存储目录文件的卷。
    - `/opt/application/netapp/cbs` 这是它安装的路径。

    ```
    mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
    ```

    示例：

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

启用索引的步骤

1. 执行以下操作之一：
    - 如果没有系统被索引，请在“恢复仪表板”的“搜索和恢复”下，选择“启用系统索引”。
    - 如果至少有一个系统已被索引，请在“搜索和恢复”下的“恢复仪表板”上选择“索引设置”。
2. 为系统选择*启用索引*。

结果

在所有服务都配置完毕并且索引目录被激活后，系统将显示为“活动”状态。

根据系统中卷的大小以及所有 3 个备份位置的备份文件数量，初始索引过程可能需要长达一个小时。此后，它会每小时透明地更新，并进行增量更改以保持最新状态。

使用“搜索和还原”功能还原卷、文件夹和文件

之后为您的系统启用索引，您可以使用“搜索和还原”还原卷、文件夹和文件。这使您可以使用广泛的过滤器从所有备份文件中找到要恢复的确切文件或卷。

步骤

1. 从控制台菜单中，选择*保护>备份和恢复*。
2. 选择“恢复”选项卡，将显示“恢复仪表板”。
3. 从“搜索和恢复”部分，选择“搜索和恢复”。
4. 从“搜索和恢复”部分，选择“搜索和恢复”。
5. 从“搜索和还原”页面：
   a. 在“搜索栏”中，输入完整或部分卷名、文件夹名或文件名。
   b. 选择资源类型：卷、文件、文件夹*或*全部。
   c. 在“过滤依据”区域中，选择过滤条件。例如，您可以选择数据所在的系统和文件类型，例如 .JPEG 文件。或者，如果您只想在对象存储中的可用快照或备份文件中搜索结果，则可以选择备份位置类型。
6. 选择*搜索*，搜索结果区域将显示所有具有与您的搜索相匹配的文件、文件夹或卷的资源。
7. 找到包含您要恢复的数据的资源，然后选择“查看所有备份”以显示包含匹配卷、文件夹或文件的所有备份文件。
8. 找到您想要用于恢复数据的备份文件并选择*恢复*。

   请注意，搜索结果会识别包含您搜索文件的本地卷快照和远程复制卷。您可以选择从云备份文件、快照或复制卷中恢复。

9. 选择要恢复卷、文件夹或文件的目标位置，然后选择*恢复*。
   - 对于卷，您可以选择原始目标系统，也可以选择备用系统。恢复FlexGroup卷时，您需要选择多个聚合。
   - 对于文件夹，您可以恢复到原始位置，也可以选择备用位置；包括系统、卷和文件夹。
   - 对于文件，您可以恢复到原始位置，也可以选择备用位置；包括系统、卷和文件夹。选择原始位置时，您可以选择覆盖源文件或创建新文件。

     如果您选择本地ONTAP系统，并且尚未配置与对象存储的集群连接，系统将提示您输入其他信息：

     - 从 Amazon S3 还原时，选择ONTAP集群中目标卷所在的 IP 空间，输入您创建的用户的访问密钥和密钥，以授予ONTAP集群对 S3 存储桶的访问权限，并可选择选择私有 VPC 端点以进行安全数据传输。"查看有关这些要求的详细信息"。
     - 从 Azure Blob 还原时，选择目标卷所在的ONTAP集群中的 IP 空间，并通过选择 VNet 和子网来选择用于安全数据传输的私有端点。"查看有关这些要求的详细信息"。
     - 从 Google Cloud Storage 恢复时，选择目标卷所在的ONTAP集群中的 IP 空间，以及用于访问对象存储的访问密钥和密钥。"查看有关这些要求的详细信息"。
     - 从StorageGRID还原时，输入StorageGRID服务器的 FQDN 和ONTAP应用于与StorageGRID进行 HTTPS 通信的端口，输入访问对象存储所需的访问密钥和密钥，以及目标卷所在的ONTAP集群中的 IP 空间。"查看有关这些要求的详细信息"。
     - 从ONTAP S3 还原时，输入ONTAP S3 服务器的 FQDN 和ONTAP应用于与ONTAP S3 进行 HTTPS 通信的端口，选择访问对象存储所需的访问密钥和密钥，以及目标卷所在的ONTAP集群中的 IP 空间。"查看有关这些要求的详细信息"。

结果

卷、文件夹或文件已恢复，您将返回到恢复仪表板，以便您可以查看恢复操作的进度。您还可以选择“作业监控”选项卡来查看恢复进度。看"作业监控页面"。

使用“浏览和还原”功能还原**ONTAP**数据

使用NetApp Backup and Recovery，通过浏览和恢复功能恢复ONTAP数据。恢复之前，请记下源卷名称、源系统和 SVM 以及备份文件日期。您可以从快照、复制卷或存储在对象存储中的备份恢复ONTAP数据。

恢复功能取决于您的ONTAP版本：

- 文件夹： 使用ONTAP 9.13.0 或更高版本，您可以恢复包含所有文件和子文件夹的文件夹；使用早期版本，您只能恢复文件夹中的文件。
- *归档存储：*从归档存储恢复（ ONTAP 9.10.1 或更高版本可用）速度较慢，并且可能会产生额外费用。
- 目标集群要求：
  - 卷恢复： ONTAP 9.10.1 或更高版本
  - 文件恢复： ONTAP 9.11.1 或更高版本
  - Google Archive 和StorageGRID： ONTAP 9.12.1 或更高版本
  - 文件夹恢复： ONTAP 9.13.1 或更高版本

"了解有关从 AWS 档案存储恢复的更多信息"。"了解有关从 Azure 档案存储还原的详细信息"。"详细了解如何从 Google 存档存储中恢复"。

将数据从 Azure 档案存储还原到StorageGRID系统时不支持高优先级。

浏览并恢复支持的系统和对象存储提供商

您可以将ONTAP数据从位于二级系统（复制卷）或对象存储（备份文件）中的备份文件还原到以下系统。快照保存在源系统上，并且只能还原到同一系统。

*注意：*您可以从任何类型的备份文件恢复卷，但目前只能从对象存储中的备份文件恢复文件夹或单个文件。

来自对象存储（备份）	来自主（快照）	来自辅助系统（复制）	至目的地系统
Amazon S3	AWS 本地ONTAP系统中的Cloud Volumes ONTAP	AWS 本地ONTAP系统中的Cloud Volumes ONTAP	Azure Blob
Azure 本地ONTAP系统中的Cloud Volumes ONTAP	Azure 本地ONTAP系统中的Cloud Volumes ONTAP	Google Cloud Storage	Google 本地ONTAP系统中的Cloud Volumes ONTAP
Google 本地ONTAP系统中的Cloud Volumes ONTAP	NetAppStorageGRID	本地ONTAP系统	本地ONTAP系统Cloud Volumes ONTAP
到本地ONTAP系统	ONTAP S3	本地ONTAP系统	本地ONTAP系统Cloud Volumes ONTAP

对于浏览和恢复，控制台代理可以安装在以下位置：

- 对于 Amazon S3，控制台代理可以部署在 AWS 或您的场所
- 对于 Azure Blob，控制台代理可以部署在 Azure 中或您的本地

- 对于 Google Cloud Storage，控制台代理必须部署在您的 Google Cloud Platform VPC 中
- 对于StorageGRID，控制台代理必须部署在您的场所；无论是否有互联网访问
- 对于ONTAP S3，控制台代理可以部署在您的场所（有或没有互联网访问）或云提供商环境中

请注意，“本地ONTAP系统”包括FAS、 AFF和ONTAP Select系统。

如果您系统上的ONTAP版本低于 9.13.1，并且备份文件已配置 DataLock 和勒索软件，则您无法恢复文件夹或文件。在这种情况下，您可以从备份文件恢复整个卷，然后访问所需的文件。

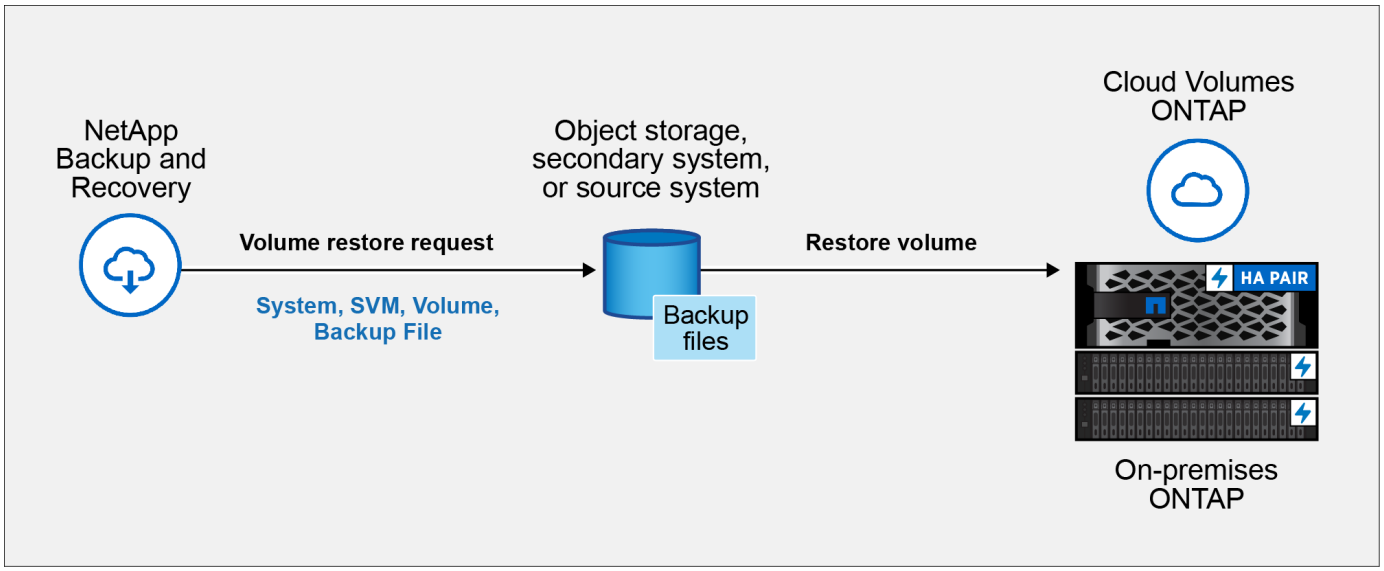
使用“浏览和还原”还原卷

当您从备份文件恢复卷时， NetApp Backup and Recovery会使用备份中的数据创建一个_新_卷。使用对象存储备份时，您可以将数据还原到原始系统中的卷、与源系统位于同一云帐户的其他系统或本地ONTAP系统。

将云备份还原到使用ONTAP 9.13.0 或更高版本的Cloud Volumes ONTAP系统或运行ONTAP 9.14.1 的本地ONTAP系统时，您可以选择执行_快速还原_操作。快速恢复非常适合需要尽快提供对卷的访问的灾难恢复情况。快速还原将备份文件中的元数据还原到卷，而不是还原整个备份文件。不建议对性能或延迟敏感的应用程序使用快速恢复，并且不支持归档存储中的备份。

仅当创建云备份的源系统运行ONTAP 9.12.1 或更高版本时， FlexGroup卷才支持快速还原。并且仅当源系统运行ONTAP 9.11.0 或更高版本时才支持SnapLock卷。

从复制卷还原时，您可以将卷还原到原始系统或Cloud Volumes ONTAP或本地ONTAP系统。



要还原卷，您需要源系统名称、存储虚拟机、卷名称和备份文件日期。

步骤

1. 从控制台菜单中，选择*保护>备份和恢复*。
2. 选择“恢复”选项卡，将显示“恢复仪表板”。
3. 从“浏览和恢复”部分，选择“恢复卷”。
4. 在“选择源”页面中，导航到要恢复的卷的备份文件。选择具有要恢复的日期/时间戳的*系统*、*卷*和*备份*文件。

位置 列显示备份文件（快照）是*本地*（源系统上的快照）、辅助（辅助ONTAP系统上的复制卷）还是*对象存储*（对象存储中的备份文件）。选择您想要恢复的文件。

5. 选择“下一步”。

   请注意，如果您选择对象存储中的备份文件，并且该备份的勒索软件恢复功能处于活动状态（如果您在备份策略中启用了 DataLock 和勒索软件恢复功能），则系统会提示您在恢复数据之前对备份文件运行额外的勒索软件扫描。我们建议您扫描备份文件以查找勒索软件。 （您将需要向云提供商支付额外的出口成本才能访问备份文件的内容。）

6. 在“选择目标”页面中，选择要恢复卷的*系统*。
7. 从对象存储还原备份文件时，如果您选择本地ONTAP系统并且尚未配置与对象存储的集群连接，系统将提示您输入其他信息：
   - 从 Amazon S3 还原时，选择ONTAP集群中目标卷所在的 IP 空间，输入您创建的用户的访问密钥和密钥，以授予ONTAP集群对 S3 存储桶的访问权限，并可选择选择私有 VPC 端点以进行安全数据传输。
   - 从 Azure Blob 还原时，选择目标卷所在的ONTAP集群中的 IP 空间，选择用于访问对象存储的 Azure 订阅，并通过选择 VNet 和子网来选择用于安全数据传输的私有端点。
   - 从 Google Cloud Storage 还原时，选择 Google Cloud 项目以及访问密钥和密钥来访问对象存储、存储备份的区域以及目标卷所在的ONTAP集群中的 IP 空间。
   - 从StorageGRID还原时，输入StorageGRID服务器的 FQDN 和ONTAP应用于与StorageGRID进行 HTTPS 通信的端口，选择访问对象存储所需的访问密钥和密钥，以及目标卷所在的ONTAP集群中的 IP 空间。
   - 从ONTAP S3 还原时，输入ONTAP S3 服务器的 FQDN 和ONTAP应用于与ONTAP S3 进行 HTTPS 通信的端口，选择访问对象存储所需的访问密钥和密钥，以及目标卷所在的ONTAP集群中的 IP 空间。
8. 输入要用于恢复的卷的名称，然后选择卷所在的存储虚拟机和聚合。恢复FlexGroup卷时，您需要选择多个聚合。默认情况下，**<source_volume_name>_restore** 用作卷名。

   当将备份从对象存储还原到使用ONTAP 9.13.0 或更高版本的Cloud Volumes ONTAP系统或运行ONTAP 9.14.1 的本地ONTAP系统时，您可以选择执行_快速还原_操作。

   如果您要从位于归档存储层（从ONTAP 9.10.1 开始可用）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 档案存储恢复的更多信息"。"了解有关从 Azure 档案存储还原的详细信息"。"详细了解如何从 Google 存档存储中恢复"。Google Archive 存储层中的备份文件几乎可以立即恢复，并且不需要恢复优先级。

9. 选择“下一步”来选择是否执行正常还原或快速还原过程：
   - 正常还原：在需要高性能的卷上使用正常还原。还原过程完成之前，卷将不可用。
   - 快速恢复：恢复的卷和数据将立即可用。请勿在需要高性能的卷上使用此功能，因为在快速恢复过程中，访问数据的速度可能比平时慢。
10. 选择“恢复”，您将返回到恢复仪表板，以便查看恢复操作的进度。

结果

NetApp Backup and Recovery根据您选择的备份创建一个新卷。

请注意，从驻留在档案存储中的备份文件恢复卷可能需要几分钟或几小时，具体取决于档案层和恢复优先级。您可以选择“作业监控”选项卡来查看恢复进度。

如果您只需要从ONTAP卷备份中恢复几个文件，则可以选择恢复文件夹或单个文件，而不是恢复整个卷。您可以将文件夹和文件还原到原始系统中的现有卷，或还原到使用相同云帐户的其他系统。您还可以将文件夹和文件还原到本地ONTAP系统上的卷。

目前，您只能从对象存储中的备份文件恢复文件夹或单个文件。目前不支持从本地快照或位于辅助系统（复制卷）中的备份文件恢复文件和文件夹。

如果选择多个文件，它们将被还原到同一目标卷。要将文件还原到不同的卷，请多次运行该过程。

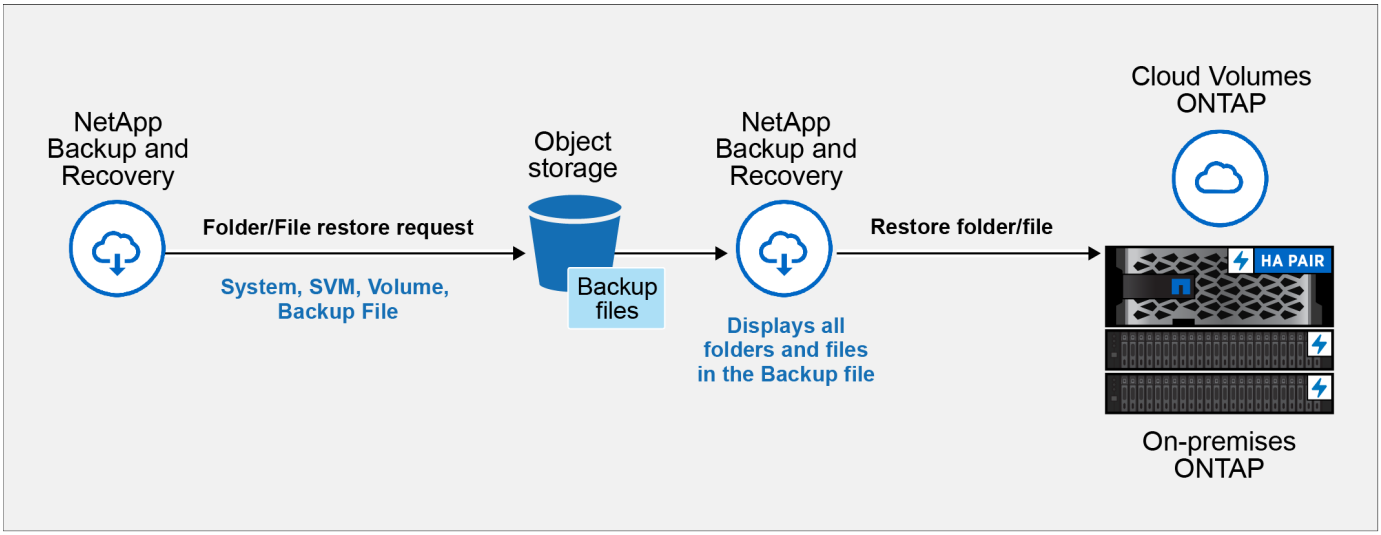
使用ONTAP 9.13.0 或更高版本时，您可以还原文件夹以及其中的所有文件和子文件夹。使用 9.13.0 之前的ONTAP版本时，仅恢复该文件夹中的文件 - 不会恢复子文件夹或子文件夹中的文件。

- 如果备份文件已配置 DataLock 和勒索软件保护，则仅当ONTAP版本为 9.13.1 或更高版本时才支持文件夹级还原。如果您使用的是早期版本的ONTAP，则可以从备份文件恢复整个卷，然后访问所需的文件夹和文件。
- 如果备份文件驻留在档案存储中，则仅当ONTAP版本为 9.13.1 或更高版本时才支持文件夹级还原。如果您使用的是早期版本的ONTAP，则可以从尚未存档的较新备份文件中还原文件夹，也可以从存档的备份中还原整个卷，然后访问所需的文件夹和文件。
- 使用ONTAP 9.15.1，您可以使用“浏览和恢复”选项恢复FlexGroup文件夹。此功能处于技术预览模式。

  您可以使用 "NetApp Backup and Recovery2024 年 7 月版本博客"。

还原文件夹和文件

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



开始之前

- ONTAP版本必须为 9.6 或更高版本才能执行_文件_恢复操作。
- ONTAP版本必须为 9.11.1 或更高版本才能执行_文件夹_还原操作。如果数据位于档案存储中，或者备份文件使用 DataLock 和勒索软件保护，则需要ONTAP版本 9.13.1。

- ONTAP版本必须为 9.15.1 p2 或更高版本才能使用浏览和还原选项还原FlexGroup目录。

步骤

1. 从控制台菜单中，选择*保护>备份和恢复*。
2. 选择“恢复”选项卡，将显示“恢复仪表板”。
3. 从“浏览和恢复”部分，选择“恢复文件或文件夹”。
4. 在“选择源”页面中，导航到包含要还原的文件夹或文件的卷的备份文件。选择具有要从中恢复文件的日期/时间戳的*系统*、卷*和*备份。
5. 选择“下一步”，将显示卷备份中的文件夹和文件列表。

   如果您要从位于档案存储层的备份文件还原文件夹或文件，则可以选择还原优先级。

   "了解有关从 AWS 档案存储恢复的更多信息"。"了解有关从 Azure 档案存储还原的详细信息"。"详细了解如何从 Google 存档存储中恢复"。Google Archive 存储层中的备份文件几乎可以立即恢复，并且不需要恢复优先级。

   如果备份文件的勒索软件恢复功能处于活动状态（如果您在备份策略中启用了 DataLock 和勒索软件恢复功能），则会提示您在恢复数据之前对备份文件运行额外的勒索软件扫描。我们建议您扫描备份文件以查找勒索软件。 （您将需要向云提供商支付额外的出口成本才能访问备份文件的内容。）

6. 在“选择项目”页面中，选择要恢复的文件夹或文件，然后选择“继续”。为了帮助您找到该物品：
   - 如果看到文件夹或文件名，您可以选择它。
   - 您可以选择搜索图标并输入文件夹或文件的名称以直接导航到该项目。
   - 您可以使用行尾的向下箭头向下导航文件夹级别来查找特定文件。

     当您选择文件时，它们会被添加到页面的左侧，以便您可以看到已经选择的文件。如果需要，您可以通过选择文件名旁边的 **x** 从此列表中删除文件。

7. 在“选择目标”页面中，选择要恢复项目的*系统*。

   如果您选择本地集群，并且尚未配置与对象存储的集群连接，系统将提示您输入其他信息：

   - 从 Amazon S3 还原时，输入目标卷所在的ONTAP集群中的 IP 空间，以及访问对象存储所需的 AWS 访问密钥和密钥。您还可以选择专用链接配置来连接到集群。
   - 从 Azure Blob 还原时，输入目标卷所在的ONTAP集群中的 IP 空间。您还可以为与集群的连接选择私有端点配置。
   - 从 Google Cloud Storage 恢复时，输入目标卷所在的ONTAP集群中的 IP 空间，以及访问对象存储所需的访问密钥和密钥。
   - 从StorageGRID还原时，输入StorageGRID服务器的 FQDN 和ONTAP应用于与StorageGRID进行 HTTPS 通信的端口，输入访问对象存储所需的访问密钥和密钥，以及目标卷所在的ONTAP集群中的 IP 空间。

8. 然后选择要恢复文件夹或文件的*卷*和*文件夹*。

   恢复文件夹和文件时，您有几个位置选项可供选择。

   - 当您选择“选择目标文件夹”时，如上所示：

        - 您可以选择任意文件夹。
        - 您可以将鼠标悬停在文件夹上，然后单击行尾以深入查看子文件夹，然后选择一个文件夹。
    - 如果您选择了与源文件夹/文件相同的目标系统和卷，则可以选择*维护源文件夹路径*将文件夹或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必须已经存在；不会创建文件夹。将文件还原到原始位置时，您可以选择覆盖源文件或创建新文件。
9. 选择“恢复”返回恢复仪表板并查看恢复操作的进度。

保护 Microsoft SQL Server 工作负载

使用NetApp Backup and Recovery保护 Microsoft SQL 工作负载概述

使用NetApp Backup and Recovery将 Microsoft SQL Server 应用程序数据从本地ONTAP系统备份到 AWS、Azure 或StorageGRID 。系统会根据您的政策自动在您的云帐户中创建并存储备份。使用 3-2-1 策略：在两个存储系统上保留数据的三个副本，在云中保留一个副本。

3-2-1 方法的优点包括：

- 多个数据副本可防止内部和外部网络安全威胁。
- 如果一种媒体发生故障，使用不同类型的媒体可以帮助您恢复。
- 您可以从现场副本快速恢复，如果现场副本受到损害，则可以使用异地副本。

NetApp Backup and Recovery使用NetApp SnapMirror通过创建快照并将其传输到备份位置来同步备份。

您可以执行以下操作来保护您的数据：

- "如果从SnapCenter导入，则配置其他项目"
- "发现 Microsoft SQL Server 工作负载并选择性地导入SnapCenter资源"
- "使用本地ONTAP主存储上的本地快照备份工作负载"
- "将工作负载复制到ONTAP二级存储"
- "将工作负载备份到对象存储位置"
- "立即备份工作负载"
- "恢复工作负载"
- "克隆工作负载"
- "管理工作负载清单"
- "管理快照"

要备份工作负载，您需要创建管理备份和恢复操作的策略。看"创建策略"了解更多信息。

支持的备份目标

NetApp Backup and Recovery使您能够将以下源系统中的 Microsoft SQL Server 实例和数据库备份到以下辅助系统以及公有云和私有云提供商中的对象存储。快照保留在源系统上。

源系统	辅助系统（复制）	目标对象存储（备份）
AWS 中的Cloud Volumes ONTAP	AWS 本地ONTAP系统中的Cloud Volumes ONTAP	亚马逊 S3 ONTAP S3
Azure 中的Cloud Volumes ONTAP	Azure 本地ONTAP系统中的Cloud Volumes ONTAP	Azure Blob ONTAP S3
本地ONTAP系统	Cloud Volumes ONTAP本地ONTAP系统	Amazon S3 Azure Blob NetApp StorageGRID ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	不适用

支持的还原目标

您可以将 Microsoft SQL Server 实例和数据库从驻留在主存储或辅助系统（复制卷）或对象存储（备份文件）中的备份还原到以下系统。快照保存在源系统上，并且只能还原到同一系统。

从备份文件位置		至目的地系统
对象存储（备份）	辅助系统（复制）	
Amazon S3	AWS 本地ONTAP系统中的Cloud Volumes ONTAP	AWS 本地ONTAP系统ONTAP S3 中的云卷
Azure Blob	Azure 本地ONTAP系统中的Cloud Volumes ONTAP	Azure 中的Cloud Volumes ONTAP 本地ONTAP系统ONTAP S3
StorageGRID	Cloud Volumes ONTAP本地ONTAP系统	本地ONTAP系统ONTAP S3
Amazon FSx for NetApp ONTAP	Amazon FSx for NetApp ONTAP	不适用

“本地ONTAP系统”包括FAS和AFF系统。

从插件服务导入**NetApp Backup and Recovery** 的先决条件

如果您要将资源从 Microsoft SQL Server 的SnapCenter插件服务导入NetApp Backup and Recovery，则需要配置更多项目。

首先在**NetApp Console**中创建系统

如果要从SnapCenter导入资源，则应先将所有本地SnapCenter群集存储添加到控制台 系统 页面，然后再从SnapCenter导入。这确保主机资源能够被正确发现和导入。

确保安装**SnapCenter**插件的主机要求

要从适用于 Microsoft SQL Server 的SnapCenter插件导入资源，请确保满足安装适用于 Microsoft SQL Server 的SnapCenter插件的主机要求。

专门检查SnapCenter要求"NetApp Backup and Recovery前提条件"。

禁用用户帐户控制远程限制

从SnapCenter导入资源之前，请禁用SnapCenter Windows 主机上的用户帐户控制 (UAC) 远程限制。如果您使用本地管理帐户远程连接到SnapCenter服务器主机或 SQL 主机，请禁用 UAC。

安全考虑

在禁用 UAC 远程限制之前，请考虑以下问题：

- 安全风险：禁用令牌过滤可能会使您的系统面临安全漏洞，尤其是在本地管理帐户受到恶意行为者的攻击时。
- 谨慎使用：
  - 仅当该设置对于您的管理任务至关重要时才修改它。
  - 确保采用强密码和其他安全措施来保护管理帐户。

替代解决方案

- 如果需要远程管理访问，请考虑使用具有适当权限的域帐户。
- 使用符合最佳安全实践的安全远程管理工具来最大限度地降低风险。

禁用用户帐户控制远程限制的步骤

1. 修改 `LocalAccountTokenFilterPolicy`SnapCenter Windows 主机上的注册表项。

   使用以下方法之一执行此操作，并按照下面的说明进行操作：

   - 方法 1：注册表编辑器
   - 方法 2：PowerShell 脚本

方法 **1**：使用注册表编辑器禁用用户帐户控制

这是您可以用来禁用用户帐户控制的方法之一。

步骤

1. 通过执行以下操作，在SnapCenter Windows 主机上打开注册表编辑器：
   a. 按 `Windows+R`打开运行对话框。
   b. 类型 `regedit`并按 `Enter`。
2. 导航至策略密钥：

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
   ```

3. 创建或修改 `DWORD`价值：
   a. 定位： `LocalAccountTokenFilterPolicy`
   b. 如果不存在，则创建一个新的 `DWORD`（32 位）值命名 `LocalAccountTokenFilterPolicy`。
4. 支持以下值。对于此场景，将值设置为 `1`：
   - `0`（默认）：启用 UAC 远程限制。本地帐户在远程访问时已过滤令牌。

- 1：UAC 远程限制已禁用。本地帐户绕过令牌过滤并在远程访问时拥有完全的管理权限。

5. 单击“确定”。
6. 关闭注册表编辑器。
7. 重新启动SnapCenter Windows 主机。

注册表修改示例

此示例将 LocalAccountTokenFilterPolicy 设置为“1”，禁用 UAC 远程限制。

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]

"LocalAccountTokenFilterPolicy"=dword:00000001
```

方法 2：使用 **PowerShell** 脚本禁用用户帐户控制

这是您可以用来禁用用户帐户控制的另一种方法。

以提升的权限运行 PowerShell 命令可能会影响系统设置。在运行命令之前，请确保您理解这些命令及其含义。

步骤

1. 在SnapCenter Windows 主机上打开具有管理权限的 PowerShell 窗口：
   a. 单击“开始”菜单。
   b. 搜索 **PowerShell 7** 或 **Windows Powershell**。
   c. 右键单击该选项并选择*以管理员身份运行*。
2. 确保您的系统上安装了 PowerShell。安装后，它应该出现在*开始*菜单中。

   Windows 7 及更高版本默认包含 PowerShell。

3. 要禁用 UAC 远程限制，请通过运行以下命令将 LocalAccountTokenFilterPolicy 设置为“1”：

   ```
   Set-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
   "LocalAccountTokenFilterPolicy" -Value 1 -Type DWord
   ```

4. 验证当前值是否设置为“1” `LocalAccountTokenFilterPolicy``通过运行：

   ```
   Get-ItemProperty -Path
   "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
   "LocalAccountTokenFilterPolicy"
   ```

- 如果值为 1，则禁用 UAC 远程限制。
- 如果值为 0，则启用 UAC 远程限制。

5. 要应用更改，请重新启动计算机。

禁用 **UAC** 远程限制的 **PowerShell 7** 命令示例：

此示例中的值设置为“1”，表示 UAC 远程限制被禁用。

```
# Disable UAC remote restrictions

Set-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy" -Value 1 -Type DWord

# Verify the change

Get-ItemProperty -Path
"HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System" -Name
"LocalAccountTokenFilterPolicy"

# Output

LocalAccountTokenFilterPolicy : 1
```

发现 **Microsoft SQL Server** 工作负载并可选择从**NetApp Backup and Recovery**中的**SnapCenter**导入

NetApp Backup and Recovery需要首先发现 Microsoft SQL Server 工作负载，您才能使用该服务。如果您已经安装了SnapCenter ，则可以选择从SnapCenter导入备份数据和策略。

所需的**NetApp Console**角色 备份和恢复超级管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

发现 **Microsoft SQL Server** 工作负载并选择性地导入**SnapCenter**资源

在发现过程中， NetApp Backup and Recovery会分析组织内系统中的 Microsoft SQL Server 实例和数据库。

NetApp Backup and Recovery评估 Microsoft SQL Server 应用程序。该服务评估现有保护级别，包括当前的备份保护策略、快照以及备份和恢复选项。

发现以下列方式发生：

- 如果您已有SnapCenter ，请使用NetApp Backup and Recovery and Recovery UI 将SnapCenter资源导入NetApp Backup and Recovery and Recovery。

如果您已经拥有SnapCenter，请先检查以确保在从SnapCenter导入之前已满足先决条件。例如，您应该先将本地SnapCenter集群存储系统添加到NetApp Console，然后再从SnapCenter导入。看"从SnapCenter导入资源的先决条件"。

- 如果您还没有SnapCenter，您仍然可以通过手动添加 vCenter 并执行发现来发现工作负载。

如果已安装**SnapCenter** ，请将**SnapCenter**资源导入**NetApp Backup and Recovery**

如果您已安装SnapCenter ，请按照以下步骤将SnapCenter资源导入NetApp Backup and Recovery 。 NetApp Console从SnapCenter发现资源、主机、凭据和计划；您不必重新创建所有这些信息。

您可以通过以下方式执行此操作：

- 在发现期间，选择一个选项从SnapCenter导入资源。
- 发现后，从“清单”页面选择一个选项来导入SnapCenter资源。
- 发现后，从“设置”菜单中选择一个选项来导入SnapCenter资源。有关详细信息，请参阅"配置NetApp Backup and Recovery"。

这是一个由两部分组成的过程：

- 导入SnapCenter Server 应用程序和主机资源
- 管理选定的SnapCenter主机资源

导入**SnapCenter Server** 应用程序和主机资源

第一步从SnapCenter导入主机资源，并在NetApp Backup and Recovery清单页面中显示这些资源。此时，资源尚未由NetApp Backup and Recovery管理。

导入SnapCenter主机资源后， NetApp Backup and Recovery不会自动接管保护管理。为此，您必须明确选择在NetApp Backup and Recovery中管理导入的资源。这可确保您已准备好通过NetApp Backup and Recovery备份这些资源。

步骤

1. 从NetApp Console左侧导航中，选择 保护 > 备份和恢复。
2. 选择*库存*。
3. 选择*发现资源*。
4. 从NetApp Backup and Recovery Discover 工作负载资源页面中，选择 从**SnapCenter**导入。
5. 输入* SnapCenter应用程序凭据*：
   a. * SnapCenter FQDN 或 IP 地址*：输入SnapCenter应用程序本身的 FQDN 或 IP 地址。
   b. 端口：输入SnapCenter服务器的端口号。
   c. 用户名*和*密码：输入SnapCenter服务器的用户名和密码。
   d. 控制台代理：选择SnapCenter的控制台代理。
6. 输入* SnapCenter服务器主机凭据*：
   a. 现有凭证：如果选择此选项，则可以使用已添加的现有凭证。选择凭证名称。

b. 添加新凭据：如果您没有现有的SnapCenter主机凭据，则可以添加新凭据。输入凭证名称、身份验证模式、用户名和密码。

7. 选择“导入”来验证您的条目并注册SnapCenter服务器。

如果SnapCenter服务器已注册，您可以更新现有的注册详细信息。

结果

清单页面显示导入的SnapCenter资源，包括 MS SQL 主机、实例和数据库。

要查看导入的SnapCenter资源的详细信息，请从“操作”菜单中选择“查看详细信息”选项。

管理**SnapCenter**主机资源

导入SnapCenter资源后，在NetApp Backup and Recovery中管理这些主机资源。选择管理这些资源后，NetApp Backup and Recovery能够备份和恢复您从SnapCenter导入的资源。您不再在SnapCenter Server 中管理这些资源。

步骤

1. 导入SnapCenter资源后，从备份和恢复菜单中选择*Inventory*。
2. 从“清单”页面中，选择您希望从现在开始使用NetApp Backup and Recovery进行管理的导入的SnapCenter主机。
3. 选择“操作”图标 > *查看详情*显示工作量详情。
4. 在清单 > 工作负载页面中，选择操作图标 > 管理 显示管理主机页面。
5. 选择*管理*。
6. 在管理主机页面中，选择使用现有 vCenter 或添加新的 vCenter。
7. 选择*管理*。

   库存页面显示新管理的SnapCenter资源。

您可以选择从“操作”菜单中选择“生成报告”选项来创建管理资源的报告。

从清单页面发现后导入**SnapCenter**资源

如果您已经发现资源，则可以从清单页面导入SnapCenter资源。

步骤

1. 从控制台左侧导航中，选择*保护*>*备份和恢复*。
2. 选择*库存*。
3. 从库存页面中，选择*导入SnapCenter资源*。
4. 按照上面“导入SnapCenter资源”部分中的步骤导入SnapCenter资源。

如果您尚未安装**SnapCenter** ，请添加 **vCenter** 并发现资源

如果您尚未安装SnapCenter ，您可以添加 vCenter 信息并让NetApp备份和恢复发现工作负载。在每个控制台代理中，选择您想要发现工作负载的系统。

如果您有 VMware 环境，这是可选的。

步骤

1. 从控制台左侧导航中，选择*保护*>*备份和恢复*。

   如果您是第一次登录备份和恢复，并且在控制台中有一个系统但没有发现任何资源，则会显示“欢迎使用新的NetApp备份和恢复”页面，其中包含“发现资源”选项。

2. 选择*发现资源*。
3. 输入以下信息：
   a. 工作负载类型：对于此版本，仅 Microsoft SQL Server 可用。
   b. **vCenter** 设置：选择现有的 vCenter 或添加新的 vCenter。要添加新的 vCenter，请输入 vCenter FQDN 或 IP 地址、用户名、密码、端口和协议。

      如果要输入 vCenter 信息，请输入 vCenter 设置和主机注册的信息。如果您在这里添加或输入了 vCenter 信息，接下来您还需要在高级设置中添加插件信息。

   c. 主机注册：选择*添加凭据*并输入包含您想要发现的工作负载的主机的信息。

      如果要添加独立服务器而不是 vCenter 服务器，则仅输入主机信息。

4. 选择*发现*。

   此过程可能需要几分钟。

5. 继续高级设置。

在发现期间设置高级设置选项并安装插件

使用高级设置，您可以在所有注册的服务器上手动安装插件代理。这使您能够将所有SnapCenter工作负载导入NetApp Backup and Recovery，以便您可以在那里管理备份和恢复。 NetApp Backup and Recovery显示了安装插件所需的步骤。

步骤

1. 在“发现资源”页面中，单击右侧的向下箭头继续进行“高级设置”。
2. 在发现工作负载资源页面中，输入以下信息。
   - 输入插件端口号：输入插件使用的端口号。
   - 安装路径：输入插件的安装路径。
3. 如果要手动安装SnapCenter代理，请选中以下选项的复选框：
   - 使用手动安装：选中此框可手动安装插件。
   - 添加集群中的所有主机：选中此框可在发现期间将集群中的所有主机添加到NetApp Backup and Recovery 。
   - 跳过可选的预安装检查：选中此框可跳过可选的预安装检查。例如，如果您知道内存或空间考虑因素将在不久的将来发生变化，并且您想立即安装插件，那么您可能想要这样做。

4. 选择*发现*。

继续访问**NetApp Backup and Recovery**仪表板

1. 从NetApp Console菜单中，选择 保护 > 备份和恢复。
2. 选择一个工作负载图块（例如，Microsoft SQL Server）。
3. 从备份和恢复菜单中，选择*仪表板*。
4. 审查数据保护的健康状况。处于危险中或受保护的工作负载的数量会根据新发现、受保护和备份的工作负载而增加。

   "了解仪表板显示的内容"。

使用**NetApp Backup and Recovery**Microsoft SQL Server 工作负载

将 Microsoft SQL Server 应用程序数据从本地ONTAP系统备份到 Amazon Web Services、Microsoft Azure 或StorageGRID。系统会自动创建备份并将其存储在您的云帐户的对象存储中以保护数据。

- 要按计划备份工作负载，请创建管理备份和恢复操作的策略。看"创建策略"以获取说明。
- 在开始备份之前配置已发现主机的日志目录。
- 立即备份工作负载（立即创建按需备份）。

查看工作负载保护状态

在开始备份之前，请查看工作负载的保护状态。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员、备份和恢复恢复管理员、备份和恢复克隆管理员或备份和恢复查看器角色。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 查看主机、保护组、可用性组、实例和数据库选项卡上的详细信息。

配置发现主机的日志目录

设置已发现主机的活动日志路径，以便在备份工作负载之前跟踪操作状态。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员或备份和恢复恢复管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。

2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择主机。
5. 选择“操作”图标 ••• > 配置日志目录。
6. 输入主机路径或浏览主机或节点列表以找到要存储主机日志的位置。
7. 选择您想要存储日志的那些。

   显示的字段根据所选的部署模型而有所不同，例如故障转移群集实例或独立实例。

8. 选择*保存*。

创建保护组

创建保护组来管理多个工作负载的备份和还原操作。保护组是工作负载的逻辑分组。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择*创建保护组*。
6. 为保护组提供一个名称。
7. 选择要包含在保护组中的实例或数据库。
8. 选择“下一步”。
9. 选择要应用于保护组的*备份策略*。

   如果要创建策略，请选择*创建新策略*并按照提示创建策略。看"创建策略"了解更多信息。

10. 选择“下一步”。
11. 检查配置。
12. 选择“创建”来创建保护组。

立即使用按需备份来备份工作负载

在对系统进行更改之前运行按需备份，以确保您的数据受到保护。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从菜单中选择*库存*。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择“保护组”、“实例”或“数据库”选项卡。
5. 选择要备份的实例或数据库。
6. 选择“操作”图标 ••• > 立即备份。
7. 选择要应用于备份的策略。
8. 选择计划层级。
9. 选择*立即备份*。

暂停备份计划

暂停计划以在维护或故障排除期间暂时停止备份。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择“保护组”、“实例”或“数据库”选项卡。
5. 选择要暂停的保护组、实例或数据库。
6. 选择“操作”图标 ••• > 暂停。

删除保护组

删除保护组会删除该保护组以及所有相关的备份计划。如果不再需要某个保护组，您可能需要将其删除。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择“操作”图标 ••• > 删除保护组。

删除工作负载的保护

如果您不再想要备份某个工作负载，或者想要停止在NetApp Backup and Recovery中管理该工作负载，则可以

从该工作负载中删除保护。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择“保护组”、“实例”或“数据库”选项卡。
5. 选择保护组、实例或数据库。
6. 选择“操作”图标 ••• > 移除保护。
7. 在“删除保护”对话框中，选择是否要保留备份和元数据或删除它们。
8. 选择*删除*以确认操作。

使用**NetApp Backup and Recovery**恢复 **Microsoft SQL Server** 工作负载

使用NetApp Backup and Recovery恢复 Microsoft SQL Server 工作负载。使用快照、复制到辅助存储的备份或对象存储中的备份。将工作负载恢复到原始系统、具有相同云帐户的不同系统或本地ONTAP系统。

从这些位置恢复

您可以从不同的起始位置恢复工作负载：

- 从主要位置还原
- 从复制的资源还原
- 从对象存储备份恢复

恢复到这些点

您可以将数据还原到最新快照或以下点：

- 从快照还原
- 如果您知道文件名、位置和最后有效日期，则还原到特定时间点
- 恢复到最新备份

从对象存储中恢复的注意事项

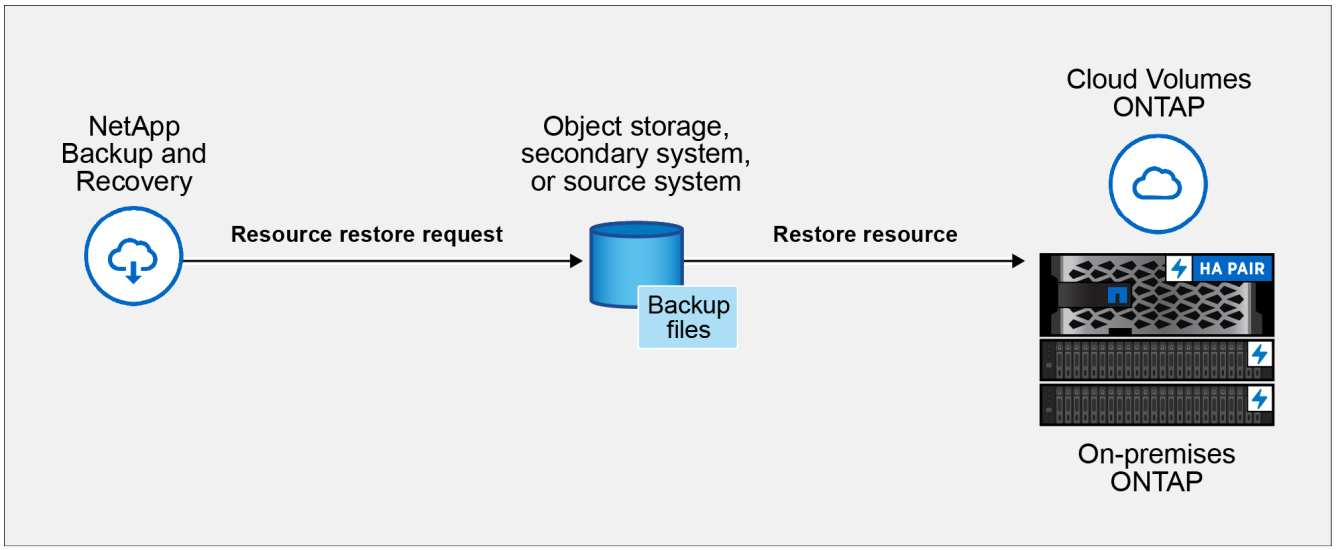
如果您选择对象存储中的备份文件，并且该备份的勒索软件恢复功能处于活动状态（如果您在备份策略中启用了 DataLock 和勒索软件恢复功能），则系统会提示您在恢复数据之前对备份文件运行额外的完整性检查。我们建议您执行扫描。

您需要向云提供商支付额外费用才能访问备份文件。

恢复工作负载的工作原理

恢复工作负载时，会发生以下情况：

- 当您从备份文件恢复工作负载时， NetApp Backup and Recovery会使用备份中的数据创建一个_新_资源。
- 从复制的工作负载恢复时，您可以将工作负载恢复到原始系统或本地ONTAP系统。



- 从对象存储还原备份时，您可以将数据还原到原始系统或本地ONTAP系统。

恢复方法

使用以下方法之一恢复工作负载：

- 从恢复页面：当您不知道资源的名称、位置或最后有效日期时，使用此选项可恢复资源。使用过滤器搜索快照。
- 从库存页面：当您知道特定资源的名称、位置和最后有效日期时，使用此选项可恢复该资源。浏览列表以查找资源。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

从“恢复”选项恢复工作负载数据

使用恢复选项恢复数据库工作负载。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 恢复。
2. 选择要还原的数据库。使用过滤器进行搜索。
3. 选择恢复选项：
    - 从快照还原
    - 如果您知道文件名、位置和最后有效日期，则还原到特定时间点
    - 恢复到最新备份

从快照恢复工作负载

1. 继续从恢复选项页面，选择*从快照恢复*。

   出现快照列表。

2. 选择要恢复的快照。
3. 选择“下一步”。

   接下来您将看到目的地选项。

4. 在目的地详情页面中，输入以下信息：
   - 目标设置：选择是否将数据恢复到原始位置还是其他位置。对于备用位置，选择主机名和实例，输入数据库名称，然后输入要还原快照的目标路径。
   - 预恢复选项：
     - 恢复时覆盖同名数据库：恢复时，保留原始数据库名称。
     - 保留 **SQL** 数据库复制设置：恢复操作后保留 SQL 数据库的复制设置。
     - 恢复前创建事务日志备份：在恢复操作之前创建事务日志备份。* 如果还原前的事务日志备份失败，则退出还原：如果事务日志备份失败，则停止还原操作。
     - **Prescript**：输入应在恢复操作之前运行的脚本的完整路径、脚本所需的任何参数以及等待脚本完成的时间。
   - 恢复后选项：
     - 可操作，但无法恢复其他事务日志。应用事务日志备份后，数据库将恢复在线状态。
     - 不可操作，但可用于恢复额外的事务日志。在还原事务日志备份的同时，在还原操作后将数据库维持在非操作状态。此选项对于恢复额外的事务日志很有用。
     - 只读模式，可用于恢复额外的事务日志。以只读模式恢复数据库并应用事务日志备份。
     - 后记：输入恢复操作后应运行的脚本的完整路径以及脚本所采用的任何参数。
5. 选择*恢复*。

恢复到特定时间点

NetApp Backup and Recovery使用日志和最新的快照来创建数据的时间点恢复。

1. 继续从“恢复选项”页面，选择“恢复到特定时间点”。
2. 选择“下一步”。
3. 在“还原到特定时间点”页面中，输入以下信息：
   - 数据恢复的日期和时间：输入您要恢复的数据的确切日期和时间。此日期和时间来自 Microsoft SQL Server 数据库主机。
4. 选择*搜索*。
5. 选择要恢复的快照。
6. 选择“下一步”。
7. 在目的地详情页面中，输入以下信息：

- 目标设置：选择是否将数据恢复到原始位置还是其他位置。对于备用位置，请选择主机名和实例，输入数据库名称，然后输入目标路径。
- 预恢复选项：
  - 保留原始数据库名称：在恢复过程中，保留原始数据库名称。
  - 保留 **SQL** 数据库复制设置：恢复操作后保留 SQL 数据库的复制设置。
  - **Prescript**：输入应在恢复操作之前运行的脚本的完整路径、脚本所需的任何参数以及等待脚本完成的时间。
- 恢复后选项：
  - 可操作，但无法恢复其他事务日志。应用事务日志备份后，数据库将恢复在线状态。
  - 不可操作，但可用于恢复额外的事务日志。在还原事务日志备份的同时，在还原操作后将数据库维持在非操作状态。此选项对于恢复额外的事务日志很有用。
  - 只读模式，可用于恢复额外的事务日志。以只读模式恢复数据库并应用事务日志备份。
  - 后记：输入恢复操作后应运行的脚本的完整路径以及脚本所采用的任何参数。

8. 选择*恢复*。

恢复到最新备份

此选项使用最新的完整备份和日志备份将数据恢复到最后的良好状态。系统扫描从上次快照到现在的日志。该过程跟踪变化和活动以恢复数据的最新和最准确的版本。

1. 继续从恢复选项页面，选择*恢复到最新备份*。

   NetApp Backup and Recovery向您显示可用于恢复操作的快照。

2. 在恢复到最新状态页面中，选择本地、二级存储或对象存储的快照位置。
3. 选择“下一步”。
4. 在目的地详情页面中，输入以下信息：
   - 目标设置：选择是否将数据恢复到原始位置还是其他位置。对于备用位置，请选择主机名和实例，输入数据库名称，然后输入目标路径。
   - 预恢复选项：
     - 恢复时覆盖同名数据库：恢复时，保留原始数据库名称。
     - 保留 **SQL** 数据库复制设置：恢复操作后保留 SQL 数据库的复制设置。
     - 恢复前创建事务日志备份：在恢复操作之前创建事务日志备份。
     - 如果还原前的事务日志备份失败，则退出还原：如果事务日志备份失败，则停止还原操作。
     - **Prescript**：输入应在恢复操作之前运行的脚本的完整路径、脚本所需的任何参数以及等待脚本完成的时间。
   - 恢复后选项：
     - 可操作，但无法恢复其他事务日志。应用事务日志备份后，数据库将恢复在线状态。
     - 不可操作，但可用于恢复额外的事务日志。在还原事务日志备份的同时，在还原操作后将数据库维持在非操作状态。此选项对于恢复额外的事务日志很有用。

- 只读模式，可用于恢复额外的事务日志。以只读模式恢复数据库并应用事务日志备份。
- 后记：输入恢复操作后应运行的脚本的完整路径以及脚本所采用的任何参数。

5. 选择*恢复*。

从 **Inventory** 选项恢复工作负载数据

从库存页面恢复数据库工作负载。使用 Inventory 选项，您只能恢复数据库，而不能恢复实例。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择要恢复的资源所在的主机。
3. 选择*操作*•••图标，然后选择*查看详细信息*。
4. 在 Microsoft SQL Server 页面上，选择“数据库”选项卡。
5. 在数据库菜单中，选择具有“受保护”状态的数据库。
6. 选择*操作*•••图标，然后选择*恢复*。

   与从“恢复”页面恢复时出现的三个选项相同：

   - 从快照还原
   - 恢复到特定时间点
   - 恢复到最新备份
7. 继续执行与“恢复”页面中的恢复选项相同的步骤

使用**NetApp Backup and Recovery**克隆 **Microsoft SQL Server** 工作负载

使用NetApp Backup and Recovery将 Microsoft SQL Server 应用程序数据克隆到 VM 以进行开发、测试或保护。从 SQL Server 工作负载的即时或现有快照创建克隆。

从以下克隆类型中进行选择：

- 即时快照和克隆：您可以从即时快照创建 Microsoft SQL Server 工作负载的克隆，即时快照是从备份创建的源数据的时间点副本。克隆存储在您的公共或私有云帐户的对象存储中。如果数据丢失或损坏，您可以使用克隆来恢复您的工作负载。
- 从现有快照克隆：您可以从可用于工作负载的快照列表中选择一个现有快照。如果您想从特定时间点创建克隆，此选项很有用。克隆到主存储或辅助存储。

您可以实现以下保护目标：

- 创建克隆
- 刷新克隆
- 分裂克隆
- 删除克隆

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服

务的NetApp Console访问角色" 。

创建克隆

您可以创建 Microsoft SQL Server 工作负载的克隆。克隆是从备份创建的源数据的副本。克隆存储在您的公共或私有云帐户的对象存储中。如果数据丢失或损坏，您可以使用克隆来恢复您的工作负载。

您可以从现有快照或即时快照创建克隆。即时快照是根据备份创建的源数据的时间点副本。如果数据丢失或损坏，您可以使用克隆来恢复您的工作负载。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 克隆。
2. 选择*创建新克隆*。
3. 选择克隆类型：
   - 从现有快照克隆和刷新数据库：选择快照并配置克隆选项。
   - 即时快照和克隆：立即对源数据进行快照并从该快照创建克隆。如果您想从源工作负载中的最新数据创建克隆，此选项很有用。
4. 完成*数据库源*部分：
   - 单个克隆或批量克隆：选择创建单个克隆还是多个克隆。如果您选择*批量克隆*，则可以使用已创建的保护组一次创建多个克隆。如果您想为不同的工作负载创建多个克隆，此选项很有用。
   - 源数据库主机、实例和名称：选择克隆的源数据库主机、实例和名称。源数据库是将创建克隆的数据库。
5. 完成*数据库目标*部分：
   - 目标数据库主机、实例和名称：选择克隆的目标数据库主机、实例和名称。目标数据库是将创建克隆的位置。

     或者，从目标名称下拉列表中选择 **Suffix**，并为克隆的数据库名称添加后缀。如果不添加后缀，克隆的数据库名称与源数据库名称相同。

   - **QoS**（最大吞吐量）：为克隆选择服务质量（QoS）最大吞吐量（MBps）。 QoS 定义了克隆的性能特征，例如最大吞吐量和 IOPS。
6. 完成*Mount*部分：
   - 自动分配挂载点：自动为对象存储中的克隆分配挂载点。
   - 定义挂载点路径：输入克隆的挂载点。挂载点是克隆将在对象存储中挂载的位置。选择驱动器号，输入数据文件路径，输入日志文件路径。
7. 选择“下一步”。
8. 选择还原点：
   - 现有快照：从可用于工作负载的快照列表中选择一个现有快照。如果您想从特定时间点创建克隆，此选项很有用。
   - 即时快照和克隆：从可用于工作负载的快照列表中选择最新快照。如果您想从源工作负载中的最新数据创建克隆，此选项很有用。
9. 如果您选择创建*即时快照和克隆*，请选择克隆存储位置：
   - 本地存储：选择此选项可在ONTAP系统的本地存储中创建克隆。本地存储是直接连接到ONTAP系统的

存储。

- 二级存储：选择此选项可在ONTAP系统的二级存储中创建克隆。辅助存储是用于备份和恢复工作负载的存储。

10. 选择数据和日志的目标位置。
11. 选择“下一步”。
12. 完成*高级选项*部分。
13. 如果您选择*即时快照和克隆*，请完成以下选项：
    - 克隆刷新计划和到期时间：如果您选择*即时克隆*，请输入开始刷新克隆的日期。克隆计划定义了何时创建克隆。
      - 如果计划到期则删除克隆：如果您想在克隆到期日时删除克隆。
      - 刷新克隆频率：选择克隆的刷新频率。您可以选择每小时、每天、每周、每月或每季度刷新克隆。如果您希望克隆与源工作负载保持同步，则此选项很有用。
    - 前言和后记：可选地，添加在克隆创建之前和之后运行的脚本。这些脚本可以执行额外的任务，例如设置克隆或发送通知。
    - 通知：可选地，指定电子邮件地址以接收有关克隆创建状态以及作业报告的通知。您还可以指定一个 webhook URL 来接收有关克隆创建状态的通知。您可以指定是否需要成功和失败通知，或者仅需要其中一个。
    - 标签：选择标签以帮助您稍后搜索资源组，然后选择*应用*。例如，如果您将“HR”作为标签添加到多个资源组，则以后可以找到与“HR”标签关联的所有资源组。
14. 选择“创建”。
15. 当克隆创建完成后，您可以在*库存*页面中查看它。

刷新克隆

您可以刷新 Microsoft SQL Server 工作负载的克隆。刷新克隆会使用源工作负载中的最新数据来更新克隆。如果您希望使克隆与源工作负载保持同步，这将非常有用。

您可以选择更改数据库名称、使用最新的即时快照或从现有生产快照刷新。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 克隆。
2. 选择要刷新的克隆。
3. 选择“操作”图标 ••• > 刷新克隆。
4. 完成“高级设置”部分：
    - 恢复范围：选择是否恢复所有日志备份或直到特定时间点的日志备份。如果您想将克隆恢复到特定时间点，此选项很有用。
    - 克隆刷新计划和到期时间：如果您选择*即时克隆*，请输入开始刷新克隆的日期。克隆计划定义了何时创建克隆。
      - 如果计划到期则删除克隆：如果您想在克隆到期日时删除克隆。
      - 刷新克隆频率：选择克隆的刷新频率。您可以选择每小时、每天、每周、每月或每季度刷新克隆。如果您希望克隆与源工作负载保持同步，则此选项很有用。

- **iGroup** 设置：选择克隆的 iGroup。iGroup 是用于访问克隆的启动器的逻辑分组。您可以选择现有的 iGroup 或创建一个新的 iGroup。从主或辅助ONTAP存储系统中选择 iGroup。
- 前言和后记：可选地，添加在克隆创建之前和之后运行的脚本。这些脚本可以执行额外的任务，例如设置克隆或发送通知。
- 通知：可选地，指定电子邮件地址以接收有关克隆创建状态以及作业报告的通知。您还可以指定一个 webhook URL 来接收有关克隆创建状态的通知。您可以指定是否需要成功和失败通知，或者仅需要其中一个。
- 标签：输入一个或多个标签，以帮助您稍后搜索资源组。例如，如果您将“HR”作为标签添加到多个资源组，则以后可以找到与 HR 标签关联的所有资源组。

5. 在刷新确认对话框中，要继续，请选择*刷新*。

跳过克隆刷新

跳过克隆刷新以保持克隆不变。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 克隆。
2. 选择您想要跳过刷新的克隆。
3. 选择“操作”图标 ••• > 跳过刷新。
4. 在“跳过刷新确认”对话框中，执行以下操作：
   a. 要仅跳过下一个刷新计划，请选择*仅跳过下一个刷新计划*。
   b. 要继续，请选择*跳过*。

分裂克隆

您可以拆分 Microsoft SQL Server 工作负载的克隆。拆分克隆将从克隆中创建一个新的备份。新的备份可用于恢复工作负载。

您可以选择将克隆拆分为独立克隆或长期克隆。向导会显示 SVM 的聚合列表、其大小以及克隆卷所在的位置。NetApp Backup and Recovery还会指示是否有足够的空间来拆分克隆。克隆分裂后，克隆成为一个独立的数据库进行保护。

克隆作业不会被删除，并且可以再次用于其他克隆。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 克隆。
2. 选择一个克隆。
3. 选择“操作”图标 ••• > 分裂克隆。
4. 查看拆分克隆详细信息并选择*拆分*。
5. 当分裂克隆创建完成后，您可以在*库存*页面中查看它。

删除克隆

您可以删除 Microsoft SQL Server 工作负载的克隆。删除克隆会从对象存储中移除该克隆并释放存储空间。

如果策略保护克隆，则克隆及其作业都会被删除。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 克隆。
2. 选择一个克隆。
3. 选择“操作”图标 ••• > 删除克隆。
4. 在克隆删除确认对话框中，查看删除详细信息。
   a. 要从SnapCenter中删除克隆的资源，即使克隆或其存储不可访问，也请选择“强制删除”。
   b. 选择*删除*。
5. 当克隆被删除时，它将从*库存*页面中删除。

使用NetApp Backup and Recovery管理 Microsoft SQL Server 库存

NetApp Backup and Recovery可帮助您管理 Microsoft SQL Server 主机、数据库和实例。您可以查看、更改或删除库存的保护设置。

您可以完成以下与管理库存相关的任务：

- 管理主机信息
  - 暂停时间表
  - 编辑或删除主机
- 管理实例信息
  - 将凭证与资源关联
  - 立即启动按需备份
  - 编辑保护设置
- 管理数据库信息
  - 保护数据库
  - 还原数据库
  - 编辑保护设置
  - 立即启动按需备份
- 配置日志目录（从 清单 > 主机）。如果要在快照中备份数据库主机的日志，请首先在NetApp Backup and Recovery中配置日志。有关详细信息，请参阅"配置NetApp Backup and Recovery设置"。

管理主机信息

您可以管理主机信息以确保正确的主机受到保护。您可以查看、编辑和删除主机信息。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员、备份和恢复恢复管理员或备份和恢复克隆管理员角色。 "了解所有服务的NetApp Console访问角色" 。

- 配置日志目录。有关详细信息，请参阅"配置NetApp Backup and Recovery设置"。

- 暂停时间表
- 编辑主机
- 删除主机

管理主机

您可以管理系统中发现的主机。您可以单独或作为一个组来管理它们。

您可以在“主机”列中管理状态为“未管理”的主机。 NetApp Backup and Recovery已经管理具有“托管”状态的主机。

在NetApp Backup and Recovery中管理主机后， SnapCenter不再管理这些主机上的资源。

所需的**NetApp Console**角色 存储查看器，或备份和恢复超级管理员。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从菜单中选择*库存*。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择“主机”选项卡。
5. 选择一个或多个主机。如果您选择多个主机，则会出现批量操作选项，您可以在其中选择*管理（最多 5 个主机）*。
6. 选择“操作”图标 ••• > 管理。
7. 查看主机依赖关系：
   - 如果未显示 vCenter，请选择铅笔图标来添加或编辑 vCenter 详细信息。
   - 如果您添加了 vCenter，您还必须通过选择“注册 vCenter”来注册 vCenter。
8. 选择*验证设置*来测试您的设置。
9. 选择*管理*来管理主机。

暂停时间表

暂停计划以在主机维护期间停止备份和恢复操作。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择要暂停计划的主机。
3. 选择*操作* ••• 图标，然后选择*暂停计划*。
4. 在确认对话框中，选择*暂停*。

编辑主机

您可以更改 vCenter 服务器信息、主机注册凭据和高级设置选项。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择要编辑的主机。
3. 选择*操作*•••图标，然后选择*编辑主机*。
4. 编辑主机信息。
5. 选择*完成*。

删除主机

您可以删除主机信息以停止服务收费。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择要删除的主机。
3. 选择*操作*•••图标，然后选择*删除主机*。
4. 查看确认信息并选择*删除*。

管理实例信息

您可以通过以下方式管理实例信息，分配适当的凭证来保护资源并备份资源：

- 保护实例
- 关联凭证
- 取消关联凭证
- 编辑保护
- 立即备份

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

保护数据库实例

您可以使用管理资源保护计划和保留的策略将策略分配给数据库实例。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择您想要查看的工作负载并选择*查看*。
3. 选择“实例”选项卡。
4. 选择实例。
5. 选择*操作*•••图标，然后选择*保护*。
6. 选择一个策略或创建一个新策略。

   有关创建策略的详细信息，请参阅"创建策略"。

7. 提供有关您想要在备份之前和之后运行的脚本的信息。
    - 预脚本：输入您的脚本文件名和位置，以便在触发保护操作之前自动运行它。这有助于执行保护工作流程之前需要执行的额外任务或配置。
    - 后脚本：输入您的脚本文件名和位置，以便在保护操作完成后自动运行它。这有助于执行保护工作流程之后需要执行的附加任务或配置。
8. 提供有关如何验证快照的信息：
    - 存储位置：选择验证快照的存储位置。
    - 验证资源：选择要验证的资源是在本地快照上还是在ONTAP二级存储上。
    - 验证计划：选择每小时、每天、每周、每月或每年的频率。

将凭证与资源关联

您可以将凭证与资源关联起来，以便进行保护。

有关详细信息，请参阅"配置NetApp Backup and Recovery设置，包括凭据"。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择您想要查看的工作负载并选择*查看*。
3. 选择“实例”选项卡。
4. 选择实例。
5. 选择*操作*•••图标，然后选择*关联凭证*。
6. 使用现有凭证或创建新凭证。

编辑保护设置

您可以更改策略、创建新策略、设置时间表和设置保留设置。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择您想要查看的工作负载并选择*查看*。
3. 选择“实例”选项卡。
4. 选择实例。
5. 选择*操作*•••图标，然后选择*编辑保护*。

   有关创建策略的详细信息，请参阅"创建策略"。

立即备份

立即备份您的数据以立即保护它。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。

2. 选择您想要查看的工作负载并选择*查看*。
3. 选择“实例”选项卡。
4. 选择实例。
5. 选择*操作*•••图标，然后选择*立即备份*。
6. 选择备份类型并设置计划。

   有关创建临时备份的详细信息，请参阅"创建策略"。

管理数据库信息

您可以通过以下方式管理数据库信息：

- 保护数据库
- 还原数据库
- 查看保护详细信息
- 编辑保护设置
- 立即备份

保护数据库

您可以更改策略、创建新策略、设置时间表和设置保留设置。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择您想要查看的工作负载并选择*查看*。
3. 选择“数据库”选项卡。
4. 选择数据库。
5. 选择*操作*•••图标，然后选择*保护*。

   有关创建策略的详细信息，请参阅"创建策略"。

还原数据库

恢复数据库以保护您的数据。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

1. 选择“数据库”选项卡。
2. 选择数据库。
3. 选择*操作*•••图标，然后选择*恢复*。

有关恢复工作负载的信息，请参阅"恢复工作负载"。

编辑保护设置

您可以更改策略、创建新策略、设置时间表和设置保留设置。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择您想要查看的工作负载并选择*查看*。
3. 选择“数据库”选项卡。
4. 选择数据库。
5. 选择*操作*•••图标，然后选择*编辑保护*。

   有关创建策略的详细信息，请参阅"创建策略"。

立即备份

您现在可以备份您的 Microsoft SQL Server 实例和数据库，以立即保护您的数据。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择您想要查看的工作负载并选择*查看*。
3. 选择“实例”或“数据库”选项卡。
4. 选择实例或数据库。
5. 选择*操作*•••图标，然后选择*立即备份*。

使用**NetApp Backup and Recovery**管理 **Microsoft SQL Server** 快照

您可以通过从NetApp Backup and Recovery中删除 Microsoft SQL Server 快照来管理它们。

删除快照

您只能删除本地快照。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 在NetApp Backup and Recovery中，选择 **Inventory**。

2. 选择工作负载并选择*查看*。
3. 选择“数据库”选项卡。
4. 选择要删除快照的数据库。
5. 从操作菜单中，选择*查看保护详情*。
6. 选择要删除的本地快照。

   验证该行*位置*列中的本地快照图标是否显示为蓝色。

7. 选择*操作*•••图标，然后选择*删除本地快照*。
8. 在确认对话框中，选择*删除*。

在NetApp Backup and Recovery中为 Microsoft SQL Server 工作负载创建报告

在NetApp Backup and Recovery中，创建 Microsoft SQL Server 工作负载的报告，以查看备份状态和详细信息，包括成功和失败的备份计数、备份类型、存储系统和时间戳。

创建报告

所需的NetApp Console角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员、备份和恢复恢复管理员、备份和恢复克隆管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色"。

1. 从NetApp Backup and Recovery菜单中，选择 报告 选项。
2. 选择*创建报告*。
3. 输入报告范围详细信息：
   - 报告名称：输入报告的唯一名称。
   - 报告类型：选择您想要按帐户还是按工作量（Microsoft SQL Server）报告。
   - 选择主机：如果您按工作负载选择，请选择要为其生成报告的主机。
   - 选择内容：选择报告是否包含所有备份的摘要或每个备份的详细信息。 （如果您选择“按帐户”）
4. 输入报告范围：选择您是否希望报告包含过去一天、过去 7 天、过去 30 天、上个季度或去年的数据。
5. 输入报告发送详情：如果您希望通过电子邮件发送报告，请选中*通过电子邮件发送报告*。输入您想要接收报告的电子邮件地址。

   在设置页面配置电子邮件通知。有关配置电子邮件通知的详细信息，请参阅"配置设置"。

保护 VMware 工作负载（不含适用于 VMware 的 SnapCenter 插件）

使用NetApp Backup and Recovery保护 VMware 工作负载概述

使用NetApp Backup and Recovery保护您的 VMware VM 和数据存储。 NetApp Backup and Recovery提供快速、节省空间、崩溃一致和 VM 一致的备份和恢复操作。您可以将

VMware 工作负载备份到 Amazon Web Services S3 或StorageGRID ，并将 VMware 工作负载恢复到本地 VMware 主机。

此版本的NetApp Backup and Recovery仅支持 VMware vCenter，并且无法发现vVols或vVols上的 VM。

使用NetApp Backup and Recovery实施 3-2-1 策略，即在 2 个不同的存储系统上保留 3 个源数据副本，并在云中保留 1 个副本。3-2-1 方法的优点包括：

- 多个数据副本可防止内部和外部网络安全威胁。
- 如果一种媒体发生故障，使用不同类型的媒体可以帮助您恢复。
- 您可以从现场副本快速恢复，如果现场副本受到损害，则可以使用异地副本。

要切换到NetApp Backup and Recovery UI 版本或从 NetApp Backup and Recovery UI 版本切换，请参阅"切换到以前的NetApp Backup and RecoveryUI"。

您可以使用NetApp Backup and Recovery执行与 VMware 工作负载相关的以下任务：

- "发现 VMware 工作负载"
- "为 VMware 工作负载创建和管理保护组"
- "备份 VMware 工作负载"
- "恢复 VMware 工作负载"

使用**NetApp Backup and Recovery**发现 **VMware** 工作负载

NetApp Backup and Recovery服务需要首先发现在ONTAP系统上运行的 VMware 数据存储和虚拟机，以便您使用该服务。如果您已安装SnapCenter Plug-in for VMware vSphere导入备份数据和策略。

所需的控制台角色 备份和恢复超级管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

发现 **VMware** 工作负载并选择性地导入**SnapCenter**资源

在发现过程中， NetApp Backup and Recovery会分析您组织内的 VMware 工作负载，并评估和导入现有的保护策略、快照以及备份和恢复选项。

您可以将 VMware NFS 和 VMFS 数据存储库和虚拟机从其内部部署的SnapCenter Plug-in for VMware vSphere到NetApp Backup and Recovery库存中。

此版本的NetApp Backup and Recovery仅支持 VMware vCenter，并且无法发现vVols或vVols上的 VM。

在导入过程中， NetApp Backup and Recovery执行以下任务：

- 启用对 vCenter 服务器的安全 SSH 访问。

- 在 vCenter 服务器中的所有资源组上激活维护模式。
- 准备 vCenter 的元数据并在NetApp Console中将其标记为不受管理。
- 配置数据库访问。
- 发现 VMware vCenter、数据存储区和虚拟机。
- 从SnapCenter Plug-in for VMware vSphere导入现有的保护策略、快照以及备份和恢复选项。
- 显示在NetApp Backup and Recovery清单页面中发现的资源。

发现以下列方式发生：

- 如果您已经拥有SnapCenter Plug-in for VMware vSphere，请使用NetApp Backup and Recovery UI将SnapCenter资源导入NetApp Backup and Recovery 。

  如果您已有SnapCenter插件，请确保在从SnapCenter导入之前已满足先决条件。例如，您应该先在NetApp Console中为所有本地SnapCenter集群存储创建系统，然后再从SnapCenter导入。看"从SnapCenter导入资源的先决条件"。

- 如果您还没有SnapCenter插件，您仍然可以通过手动添加 vCenter 并执行发现来发现系统中的工作负载。

如果尚未安装**SnapCenter**插件，请添加 **vCenter** 并发现资源

如果您尚未安装适用于 VMware 的SnapCenter插件，请添加 vCenter 信息并让NetApp Backup and Recovery发现工作负载。在每个控制台代理中，选择您想要发现工作负载的系统。

步骤

1. 从NetApp Console左侧导航中，选择 保护 > 备份和恢复。

   如果您是第一次登录备份和恢复，并且在控制台中有一个系统但没有发现任何资源，则会显示“欢迎使用新的NetApp备份和恢复”页面，其中包含“发现资源”选项。

2. 选择*发现资源*。
3. 输入以下信息：
   a. 工作负载类型：选择*VMware*。
   b. **vCenter** 设置：添加新的 vCenter。要添加新的 vCenter，请输入 vCenter FQDN 或 IP 地址、用户名、密码、端口和协议。

      如果要输入 vCenter 信息，请输入 vCenter 设置和主机注册的信息。如果您在这里添加或输入了 vCenter 信息，接下来您还需要在高级设置中添加插件信息。

   c. 主机注册：VMware 不需要。
4. 选择*发现*。

   此过程可能需要几分钟。

5. 继续高级设置。

如果已安装**SnapCenter**插件，请将适用于 **VMware** 资源的**SnapCenter**插件导入**NetApp Backup and Recovery**

如果您已安装适用于 VMware 的SnapCenter插件，请按照以下步骤将SnapCenter插件资源导入NetApp Backup and Recovery 。控制台发现 vCenter 中的 ESXi 主机、数据存储区和虚拟机，并从插件中安排时间表；您不必重新创建所有这些信息。

您可以通过以下方式执行此操作：

- 在发现期间，选择一个选项从SnapCenter插件导入资源。
- 发现后，从“清单”页面中选择一个选项来导入SnapCenter插件资源。
- 发现后，从“设置”菜单中选择一个选项来导入SnapCenter插件资源。有关详细信息，请参阅"配置NetApp Backup and Recovery"。VMware 不支持此功能。

本节描述了一个由两部分组成的过程：

1. 从SnapCenter插件导入 vCenter 元数据。导入的 vCenter 资源尚未由NetApp Backup and Recovery管理。
2. 在NetApp Backup and Recovery中启动选定 vCenter、VM 和数据存储库的管理。启动管理后， NetApp Backup and Recovery会在 Inventory 页面上将 vCenter 标记为“Managed”，并且能够备份和恢复您导入的资源。在NetApp Backup and Recovery中启动管理后，您将不再在SnapCenter插件中管理这些资源。

从**SnapCenter**插件导入 **vCenter** 元数据

第一步是从SnapCenter插件导入 vCenter 元数据。此时，资源尚未由NetApp Backup and Recovery管理。

从SnapCenter插件导入 vCenter 元数据后， NetApp Backup and Recovery不会自动接管保护管理。为此，您必须明确选择在NetApp Backup and Recovery中管理导入的资源。这可确保您已准备好通过NetApp Backup and Recovery备份这些资源。

步骤

1. 从控制台左侧导航中，选择*保护*>*备份和恢复*。
2. 选择*库存*。
3. 从NetApp Backup and Recovery Discover 工作负载资源页面中，选择 从**SnapCenter**导入。
4. 在“导入自”字段中，选择“* SnapCenter Plug-in for VMware*”。
5. 输入*VMware vCenter 凭据*：
   a. **vCenter IP/**主机名：输入要导入NetApp Backup and Recovery 的vCenter 的 FQDN 或 IP 地址。
   b. **vCenter** 端口号：输入 vCenter 的端口号。
   c. **vCenter** 用户名 和 密码：输入 vCenter 的用户名和密码。
   d. 连接器：选择 vCenter 的控制台代理。
6. 输入* SnapCenter插件主机凭据*：
   a. 现有凭证：如果选择此选项，则可以使用已添加的现有凭证。选择凭证名称。
   b. 添加新凭据：如果您没有现有的SnapCenter插件主机凭据，则可以添加新凭据。输入凭证名称、身份验证模式、用户名和密码。
7. 选择“导入”来验证您的条目并注册SnapCenter插件。

如果SnapCenter插件已注册，您可以更新现有的注册详细信息。

结果

库存页面显示 vCenter 在NetApp Backup and Recovery中处于未管理状态，直到您明确选择管理它。

管理从**SnapCenter**插件导入的资源

从适用于 VMware 的SnapCenter插件导入 vCenter 元数据后，管理NetApp Backup and Recovery中的资源。在您选择管理这些资源后， NetApp Backup and Recovery能够备份和恢复您导入的资源。在NetApp Backup and Recovery中启动管理后，您将不再在SnapCenter插件中管理这些资源。

选择管理资源后，资源、虚拟机和策略将从 VMware 的SnapCenter插件导入。资源组、策略和快照从插件迁移并在NetApp Backup and Recovery中进行管理。

步骤

1. 从SnapCenter插件导入 VMware 资源后，从“备份和恢复”菜单中选择“**Inventory**”。
2. 从“库存”页面中，选择您希望从现在开始由NetApp Backup and Recovery管理的导入 vCenter。
3. 选择“操作”图标 ••• > *查看详情*显示工作量详情。
4. 从清单 > 工作负载页面中，选择操作图标 ••• > 管理 显示管理 vCenter 页面。
5. 选中“您想继续迁移吗？”复选框并选择*迁移*。

结果

清单页面显示新管理的 vCenter 资源。

继续访问**NetApp Backup and Recovery**仪表板

1. 要显示仪表板，请从“备份和恢复”菜单中选择“仪表板”。
2. 审查数据保护的健康状况。处于危险中或受保护的工作负载的数量会根据新发现、受保护和备份的工作负载而增加。

   "了解仪表板显示的内容"。

使用**NetApp Backup and Recovery**为 **VMware** 工作负载创建和管理保护组

创建保护组来管理一组工作负载的备份和还原操作。保护组是您想要一起保护的资源（例如虚拟机和数据存储区）的逻辑分组。

您可以执行与保护组相关的以下任务：

- 创建保护组。
- 查看保护详情。
- 立即备份保护组。看"立即备份 VMware 工作负载"。
- 暂停和恢复保护组的备份计划。
- 删除保护组。

创建保护组

将您想要保护的工作负载分组到保护组中，以便一起备份和还原它们。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择*创建保护组*。
6. 为保护组提供一个名称。
7. 选择要包含在保护组中的虚拟机或数据库。
8. 选择“下一步”。
9. 选择要应用于保护组的*备份策略*。

   如果要创建策略，请选择*创建新策略*并按照提示创建策略。看"创建策略"了解更多信息。
10. 选择“下一步”。
11. 检查配置。
12. 选择“创建”来创建保护组。

暂停保护组的备份计划

暂停保护组以暂停其计划的备份。

当您暂停保护组时，保护状态将更改为“维护中”。您可以随时恢复备份计划。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择“操作”图标 ••• > 暂停保护组。
6. 查看确认消息并选择*暂停*。

恢复保护组的备份计划

恢复已暂停的保护组将重新启动该保护组的计划备份。

当您暂停保护组时，保护状态将从“维护中”更改为当您恢复保护组时“受保护”。您可以随时恢复备份计划。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择“操作”图标 ••• > 恢复保护组。
6. 查看确认消息并选择*恢复*。

结果

如果计划有效，系统将验证计划，并将保护状态更改为“已保护”。如果计划无效，系统将显示错误消息并且不会恢复保护组。

删除保护组

删除保护组时，也会删除该组以及该组的所有备份计划。如果不再需要某个保护组，请将其删除。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择要删除的保护组。
6. 选择“操作”图标 ••• > 删除。
7. 查看有关删除相关备份的确认消息并确认删除。

使用**NetApp Backup and Recovery**VMware 工作负载

将 VMware VM 和数据存储区从本地ONTAP系统备份到 Amazon Web Services、 Azure NetApp Files或StorageGRID，以确保您的数据受到保护。备份会自动生成并存储在您的公共或私有云帐户的对象存储中。

- 要按计划备份工作负载，请创建管理备份和还原操作的策略。看"创建策略"以获取说明。
- 创建保护组来管理一组资源的备份和还原操作。看"使用NetApp Backup and Recovery为 VMware 工作负载创建和管理保护组"了解更多信息。
- 立即备份工作负载（立即创建按需备份）。

立即使用按需备份来备份工作负载

立即创建按需备份。如果您要对系统进行更改并希望确保在开始之前有备份，则可能需要运行按需备份。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从备份和恢复菜单中，选择*库存*。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择“保护组”、“数据存储”或“虚拟机”选项卡。
5. 选择要备份的保护组、数据存储区或虚拟机。
6. 选择“操作”图标 ••• > 立即备份。

   应用于备份的策略与分配给保护组、数据存储区或虚拟机的策略相同。

7. 选择计划层级。
8. 选择*立即备份*。

恢复 VMware 工作负载

使用NetApp Backup and Recovery恢复 VMware 工作负载

使用NetApp Backup and Recovery从快照、复制到辅助存储的工作负载备份或存储在对象存储中的备份恢复 VMware 工作负载。

从这些位置恢复

您可以从不同的起始位置恢复工作负载：

- 从主位置恢复（本地快照）
- 从二级存储上的复制资源恢复
- 从对象存储备份恢复

恢复到这些点

您可以将数据恢复到以下点：

- 恢复到原始位置：虚拟机将恢复到原始位置，即相同的 vCenter 部署、ESXi 主机和数据存储。虚拟机及其所有数据均被覆盖。
- 恢复到备用位置：您可以选择不同的 vCenter、ESXi 主机或数据存储作为虚拟机的恢复目标。这对于管理位于不同位置和状态的同一虚拟机的不同副本非常有用。

从对象存储中恢复的注意事项

如果为对象存储中的备份文件启用了勒索软件恢复功能，则要求您在恢复之前运行额外的检查。我们建议进行扫描。

您可能需要向云提供商支付额外费用才能访问备份文件。

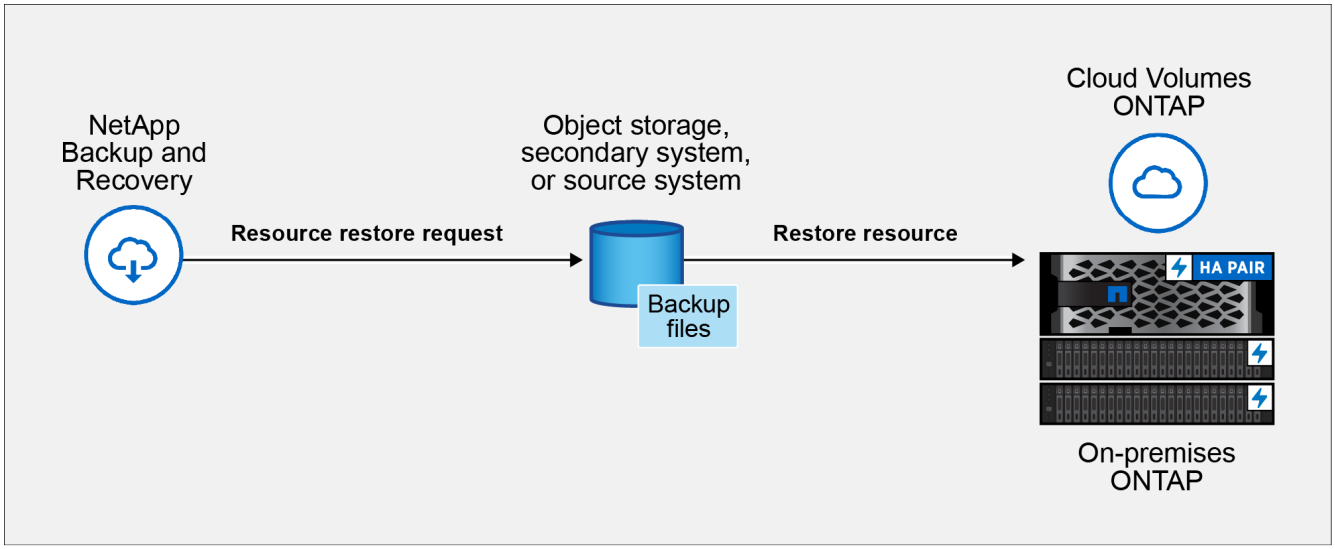
恢复工作负载的工作原理

恢复工作负载时，会发生以下情况：

- 当您从本地快照或远程备份还原工作负载时，如果您还原到原始位置， NetApp Backup and Recovery会覆

盖原始虚拟机；如果您还原到备用位置，则会创建一个新的资源。

- 从复制的工作负载恢复时，您可以将工作负载恢复到原始的本地ONTAP系统，也可以恢复到不同的本地ONTAP系统。



- 从对象存储还原备份时，您可以将数据还原到原始系统或本地ONTAP系统。

在“恢复”页面（搜索和恢复）中，您可以通过使用过滤器搜索快照来恢复资源，即使您不记得它的确切名称、位置或最后已知日期。

从恢复选项恢复工作负载数据（搜索和恢复）

使用恢复选项恢复 VMware 工作负载。您可以按名称或使用过滤器来搜索快照。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复恢复管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 恢复。
2. 从名称搜索字段右侧的下拉列表中，选择 **VMware**。
3. 输入要恢复的资源的名称，或者筛选要恢复的资源所在的 vCenter、数据中心或数据存储。

   将显示符合您搜索条件的虚拟机列表。
4. 在列表中找到要从中恢复的虚拟机，然后选择该虚拟机的选项菜单按钮。
5. 在出现的菜单中，选择“恢复虚拟机”。

   显示在该虚拟机上创建的快照（还原点）列表。默认情况下，会显示您在“时间范围”下拉菜单中选择的时间范围内的最新快照。

   对于每个快照，*位置*列中任何亮起的图标都表示快照可用的存储位置（主存储、辅助存储或对象存储）。
6. 启用要恢复的快照对应的单选按钮。
7. 选择“下一步”。

显示快照位置选项。

8. 选择快照的还原目标位置：
   - 本地：从本地位置恢复快照。
   - 辅助：从远程存储位置恢复快照。
   - 对象存储：从对象存储恢复快照。

     如果选择辅助存储，请从下拉列表中选择目标位置。
9. 选择“下一步”继续。
10. 选择恢复目标位置和设置：

目的地选择

恢复到原始位置

恢复到原始位置时，您无法更改目标 vCenter、ESXi 主机、数据存储或虚拟机的名称。恢复操作会覆盖原始虚拟机。

1. 选择“原始位置”窗格。
2. 从下列选项中进行选择：
   - *恢复前选项*部分：
     - 预设脚本：启用此选项可在恢复操作开始前运行自定义脚本，以自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
   - *恢复后选项*部分：
     - 重启虚拟机：启用此选项可在恢复操作完成后以及应用恢复后脚本后重启虚拟机。
     - 附言：启用此选项可在恢复完成后运行自定义脚本，从而自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
3. 选择*恢复*。

恢复至备用位置

恢复到备用位置时，您可以更改目标 vCenter、ESXi 主机、数据存储和虚拟机名称，以便在不同的位置或使用不同的名称创建虚拟机的新副本。

1. 选择“备用位置”窗格。
2. 输入以下信息：
   - *目的地设置*部分：
     - **vCenter FQDN** 或 **IP** 地址：选择要还原快照的 vCenter 服务器。
     - **ESXi** 主机：选择要将快照还原到的主机。
     - 网络：选择要将快照还原到的网络。
     - 数据存储：从下拉列表中，选择要将快照还原到的数据存储的名称。
     - 虚拟机名称：输入要将快照还原到的虚拟机的名称。如果名称与数据存储中已存在的虚拟机匹配，备份和恢复功能会通过附加当前时间戳来使名称唯一。
   - *恢复前选项*部分：
     - 预设脚本：启用此选项可在恢复操作开始前运行自定义脚本，以自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
   - *恢复后选项*部分：
     - 重启虚拟机：启用此选项可在恢复操作完成后以及应用恢复后脚本后重启虚拟机。
     - 附言：启用此选项可在恢复完成后运行自定义脚本，从而自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
3. 选择*恢复*。

从备份中恢复特定虚拟磁盘

您可以从传统虚拟机的主备份或辅助备份中恢复现有的虚拟磁盘 (VMDK)，或者已删除或已分离的虚拟磁盘。这样，您就可以只恢复特定的虚拟机数据或应用程序，而无需在仅影响特定数据的情况下恢复整个虚拟机及其所有关联的虚拟磁盘。虚拟磁盘恢复后，会附加到其原始虚拟机，即可使用。

您可以将虚拟机上的一个或多个虚拟机磁盘 (VMDK) 还原到同一数据存储或不同的数据存储。

为了提高 NFS 环境中恢复操作的性能，请启用 VMware 应用程序 vStorage API for Array Integration (VAAI)。

开始之前

- 必须存在备份。
- VM 不得处于传输状态。

  您要恢复的虚拟机不能处于 vMotion 或 Storage vMotion 状态。

关于此任务

- 如果 VMDK 被删除或从 VM 中分离，则还原操作会将 VMDK 附加到 VM。
- 如果虚拟机所在的FabricPool的存储层不可用，则恢复操作可能会失败。
- 连接和恢复操作使用默认的 SCSi 控制器连接 VMDK。但是，当备份连接到具有 NVMe 磁盘的 VM 的 VMDK 时，连接和恢复操作将使用 NVMe 控制器（如果可用）。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 恢复。
2. 从名称搜索字段右侧的下拉列表中，选择 **VMware**。
3. 输入要恢复的资源的名称，或者筛选要恢复的资源所在的 vCenter、数据中心或数据存储。

   将显示符合您搜索条件的虚拟机列表。

4. 在列表中找到要从中恢复的虚拟机，然后选择该虚拟机的选项菜单按钮。
5. 在出现的菜单中，选择“恢复虚拟磁盘”。

   显示在该虚拟机上创建的快照（还原点）列表。默认情况下，会显示您在“时间范围”下拉菜单中选择的时间范围内的最新快照。

   对于每个快照，*位置*列中任何亮起的图标都表示快照可用的存储位置（主存储、辅助存储或对象存储）。

6. 启用要恢复的快照对应的单选按钮。
7. 选择“下一步”。

   显示快照位置选项。

8. 选择快照的还原目标位置：
   - 本地：从本地位置恢复快照。

- 辅助：从远程存储位置恢复快照。
- 对象存储：从对象存储恢复快照。

  如果选择辅助存储，请从下拉列表中选择目标位置。

9. 选择“下一步”继续。
10. 选择恢复目标位置和设置：

目的地选择

恢复到原始位置

恢复到原始位置时，您无法更改目标 vCenter、ESXi 主机、数据存储或虚拟磁盘的名称。原虚拟磁盘被覆盖。

1. 选择“原始位置”窗格。
2. 在“目标设置”部分，选中要恢复的任何虚拟磁盘的复选框。
3. 从下列选项中进行选择：
   - *恢复前选项*部分：
     - 预设脚本：启用此选项可在恢复操作开始前运行自定义脚本，以自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
   - *恢复后选项*部分：
     - 附言：启用此选项可在恢复完成后运行自定义脚本，从而自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
4. 选择*恢复*。

恢复至备用位置

恢复到备用位置时，您可以更改目标数据存储。无论您选择哪个数据存储，恢复操作后虚拟磁盘都会附加到原始虚拟机。

1. 选择“备用位置”窗格。
2. 在“目标设置”部分，选中要恢复的任何虚拟磁盘的复选框。
3. 对于您选择的任何虚拟磁盘：
   a. 选择“选择数据存储”可为虚拟磁盘选择不同的数据存储还原目标。
   b. 选择“选择”以确认您的选择并关闭选择窗口。
4. 从下列选项中进行选择：
   - *恢复前选项*部分：
     - 预设脚本：启用此选项可在恢复操作开始前运行自定义脚本，以自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
   - *恢复后选项*部分：
     - 附言：启用此选项可在恢复完成后运行自定义脚本，从而自动执行其他任务。请输入要运行的脚本的完整路径以及脚本接受的所有参数。
5. 选择*恢复*。

恢复访客文件和文件夹

恢复访客文件和文件夹的要求和限制

您可以从 Windows 客户操作系统上的虚拟机磁盘 (VMDK) 还原文件或文件夹。

来宾还原工作流

客户操作系统还原操作包括以下步骤：

1. 附

   将虚拟磁盘附加到客户虚拟机并启动客户文件恢复会话。

2. 等待

   请等待附加操作完成，然后才能浏览和恢复。附加操作完成后，会自动创建一个访客文件恢复会话。

3. 选择文件或文件夹

   浏览 VMDK 文件，选择一个或多个文件或文件夹进行还原。

4. 还原

   将选定的文件或文件夹还原到指定位置。

恢复访客文件和文件夹的先决条件

在 Windows 客户操作系统上从 VMDK 还原文件或文件夹之前，请检查所有要求。

- 必须安装并运行 VMware 工具。

  NetApp Backup and Recovery使用来自 VMware 工具的信息来建立与 VMware 客户操作系统的连接。

- Windows 客户操作系统必须运行 Windows Server 2008 R2 或更高版本。

  有关受支持版本的最新信息，请参阅 "NetApp互操作性矩阵工具 (IMT)"。

- 目标虚拟机的凭据使用用户名为“Administrator”的内置域或本地管理员帐户。在开始恢复操作之前，请配置要附加虚拟磁盘的虚拟机的凭据。附加和恢复操作都需要凭据。工作组用户可以使用内置的本地管理员帐户。

  如果您必须使用非内置管理员帐户但在 VM 内具有管理权限的帐户，则必须在来宾 VM 上禁用 UAC。

- 您必须知道要从中恢复的备份快照和 VMDK。

  NetApp Backup and Recovery不支持搜索文件或文件夹进行还原。开始之前，您必须知道快照中的文件或文件夹以及相应的 VMDK 的位置。

- 要附加的虚拟磁盘必须位于NetApp Backup and Recovery备份中。

  包含要还原的文件或文件夹的虚拟磁盘必须位于使用NetApp Backup and Recovery执行的 VM 备份中。

- 对于名称非英文字母的文件，您必须将它们恢复到目录中，而不是作为单个文件。

  您可以通过恢复文件所在的目录来恢复具有非字母名称的文件，例如日语汉字。

来宾文件还原限制

在从客户操作系统恢复文件或文件夹之前，您应该了解其功能限制。

- 您无法在来宾操作系统内恢复动态磁盘类型。
- 如果恢复加密的文件或文件夹，则不会保留加密属性。
- 您无法将文件或文件夹还原到加密文件夹。
- 隐藏的文件和文件夹会显示在文件浏览页面中，但您无法对其进行筛选。
- 您无法从 Linux 客户操作系统恢复。

  您无法从运行 Linux 客户操作系统的 VM 还原文件和文件夹。但是，您可以附加 VMDK，然后手动恢复文件和文件夹。有关受支持的客户操作系统的最新信息，请参阅 "NetApp互操作性矩阵工具 (IMT)"。

- 您无法从 NTFS 文件系统还原到 FAT 文件系统。

  当您尝试从 NTFS 格式还原为 FAT 格式时，不会复制 NTFS 安全描述符，因为 FAT 文件系统不支持 Windows 安全属性。

- 您无法从克隆的 VMDK 或未初始化的 VMDK 恢复客户文件。
- 您无法恢复文件的目录结构。

  从嵌套目录恢复文件时，系统只会恢复文件本身，而不会恢复其目录结构。要恢复整个目录树，请复制顶层目录。

- 您无法将客户文件从 vVol VM 还原到备用主机。
- 您无法恢复加密的访客文件。

从 **VMDK** 还原客户机文件和文件夹

您可以从 Windows 客户操作系统上的 VMDK 还原一个或多个文件或文件夹。

开始之前

在从NetApp Backup and Recovery中还原文件和文件夹之前，您需要为来宾虚拟机创建凭据。NetApp Backup and Recovery使用这些凭据在附加虚拟磁盘时对来宾虚拟机进行身份验证。

关于此任务

来宾文件或文件夹恢复性能取决于两个因素：正在恢复的文件或文件夹的大小；以及正在恢复的文件或文件夹的数量。如果要恢复的数据集大小相同，则恢复大量小文件可能比恢复少量大文件花费的时间比预期的要长。

一台虚拟机上同时只能运行一个连接或还原操作。您不能在同一台虚拟机上运行并行连接或恢复操作。

借助访客恢复功能，您可以查看和恢复系统文件和隐藏文件，以及查看加密文件。请勿覆盖现有系统文件或将加密文件恢复到加密文件夹。在恢复操作期间，访客文件的隐藏属性、系统属性和加密属性不会保留在恢复的文件中。查看或浏览保留分区可能会导致错误。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择“虚拟机”菜单。
3. 从列表中选择包含要恢复的文件的虚拟机。
4. 选择“操作”图标 ••• 针对该虚拟机。
5. 选择“恢复文件和文件夹”。
6. 选择要从中恢复的快照，然后选择“下一步”。
7. 选择要从中恢复的快照位置。如果选择辅助位置，请从列表中选择辅助快照。
8. 选择“下一步”。
9. 从列表中选择要附加到虚拟机的虚拟磁盘，然后选择“下一步”。
10. 在“选择虚拟机凭据”页面上，如果您尚未存储客户虚拟机的凭据，请选择“添加凭据”并执行以下操作：
    a. 凭证名称：输入凭证的名称。
    b. 身份验证模式：选择 **Windows**。
    c. 代理：从列表中选择一个控制台代理，该代理将处理NetApp Backup and Recovery与此主机之间的通信。
    d. 域和用户名：输入凭据的 NetBIOS 或域 FQDN 和用户名。
    e. 密码：请输入凭据的密码。
    f. 选择“添加”。
11. 选择用于向客户虚拟机进行身份验证的虚拟机凭据。

    NetApp Backup and Recovery将虚拟磁盘附加到虚拟机，并显示所有文件和文件夹，包括隐藏的文件和文件夹。它会为每个分区（包括系统保留分区）分配一个驱动器号。

    您选择的文件和文件夹会列在屏幕右侧窗格中。
12. 选择“下一步”。
13. 输入将恢复所选文件的来宾的 UNC 共享路径。
    - IPv4 地址示例： `\\10.60.136.65\c$`
    - IPv6地址示例： `\\fd20-8b1e-b255-832e—61.ipv6-literal.net\C\restore`

    如果存在同名文件，您可以选择覆盖或跳过它们。
14. 选择*恢复*。

    您可以在“作业监控”页面上查看恢复进度。

访客文件恢复故障排除

尝试恢复访客文件时，您可能会遇到以下任一情况。

来宾文件恢复会话为空白

如果在创建客户机文件恢复会话期间客户机操作系统重启，则会出现此问题。客户操作系统中的 VMDK 可能处于离线状态，因此客户文件恢复会话列表为空。

要解决此问题，请在客户操作系统中手动将 VMDK 重新置于联机状态。当 VMDK 在线时，来宾文件恢复会话将显示正确的内容。

来宾文件恢复附加磁盘操作失败

当您启动客户机文件还原操作时会出现此问题，但即使 VMware 工具正在运行且客户机操作系统凭据正确，连接磁盘操作也会失败。如果发生这种情况，将返回以下错误：

```
Error while validating guest credentials, failed to access guest system using specified credentials: Verify VMWare tools is running properly on system and account used is Administrator account, Error is SystemError vix error codes = (3016, 0).
```

要解决此问题，请在客户机操作系统上重新启动 VMware Tools Windows 服务，然后重试客户机文件还原操作。

来宾文件恢复会话停止后，备份不会分离

当您从 VM 一致的备份执行来宾文件还原操作时会出现此问题。当来宾文件恢复会话处于活动状态时，将对同一 VM 执行另一个 VM 一致性备份。当客户文件恢复会话断开时（手动或 24 小时后自动断开），该会话的备份不会被分离。

要解决此问题，请手动分离从活动来宾文件还原会话附加的 VMDK。

保护 KVM 工作负载（预览版）

保护 KVM 工作负载概述

使用NetApp Backup and Recovery保护您的托管 KVM 虚拟机和存储池。NetApp Backup and Recovery提供快速、节省空间、崩溃一致性和 VM 一致性的备份和恢复操作。在使用备份和恢复功能保护 KVM 主机和虚拟机之前，必须先使用 Apache CloudStack 等管理平台来管理它们。

您可以将 KVM 工作负载备份到 Amazon Web Services S3、 Azure NetApp Files或StorageGRID ，并将 KVM 工作负载还原到本地 KVM 主机。

使用NetApp Backup and Recovery实施 3-2-1 保护策略，其中您在 2 个不同的存储系统上拥有 3 个源数据副本，并在云中拥有 1 个副本。3-2-1 方法的优点包括：

- 多个数据副本可防止内部和外部网络安全威胁。
- 如果一种媒体发生故障，使用不同类型的媒体可以帮助您恢复。
- 您可以从现场副本快速恢复，如果现场副本受到损害，则可以使用异地副本。

要切换到NetApp Backup and Recovery UI 版本或从 NetApp Backup and Recovery UI 版本切换，请参阅"切换到以前的NetApp Backup and RecoveryUI"。

您可以使用NetApp Backup and Recovery执行与 KVM 工作负载相关的以下任务：

- "发现 KVM 工作负载"
- "为 KVM 工作负载创建和管理保护组"
- "备份 KVM 工作负载"
- "恢复 KVM 工作负载"

发现NetApp Backup and Recovery中的 KVM 工作负载

NetApp Backup and Recovery需要先发现 KVM 主机和虚拟机，然后才能对其进行保护。必须先使用 Apache CloudStack 等管理平台管理您的 KVM 主机和虚拟机，然后才能将其添加到备份和恢复中。

所需的控制台角色 备份和恢复超级管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

添加管理平台、KVM 主机并发现资源

添加管理平台和 KVM 主机信息，让NetApp Backup and Recovery发现工作负载。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 在“工作负载”下，选择“KVM”磁贴。

   如果您是第一次登录备份和恢复，并且在控制台中有一个系统但没有发现任何资源，则会显示“欢迎使用新的NetApp备份和恢复”页面，其中包含“发现资源”选项。

3. 选择*发现资源*。
4. 输入以下信息：
   a. 工作负载类型：选择*KVM*。
   b. 如果您尚未将管理平台与备份和恢复功能集成，请选择“添加管理平台”。
      i. 输入以下信息：
         - 管理平台 **IP** 地址或 **FQDN**：输入管理平台的 IP 地址或完全限定域名。
         - **API**密钥：输入用于验证API请求的API密钥。
         - 密钥：输入用于验证 API 请求的密钥。
         - 端口：输入备份和恢复与管理平台之间通信所用的端口。
         - 代理：选择一个控制台代理，用于促进备份和恢复与管理平台之间的通信。
      ii. 完成后，选择“添加”。
   c. **KVM** 设置：通过输入以下信息添加新的 KVM 主机：

- **KVM FQDN** 或 **IP** 地址：输入主机的 FQDN 或 IP 地址。
- 凭据：输入 KVM 主机的用户名和密码。
- 控制台代理：选择用于备份和恢复与 KVM 主机之间通信的控制台代理。
- 端口号：输入备份和恢复与 KVM 主机之间通信所用的端口。
- 管理平台：如果 KVM 主机是受管理的，并且您已将管理平台添加到备份和恢复中，请从列表中选择管理平台。

5. 选择*发现*。

此过程可能需要几分钟。

结果

KVM 工作负载显示在“库存”页面的工作负载列表中。

继续访问**NetApp Backup and Recovery**仪表板

步骤

1. 从NetApp Console菜单中，选择 保护 > 备份和恢复。
2. 选择一个工作负载图块（例如，Microsoft SQL Server）。
3. 从备份和恢复菜单中，选择*仪表板*。
4. 审查数据保护的健康状况。处于危险中或受保护的工作负载的数量会根据新发现、受保护和备份的工作负载而增加。

使用**NetApp Backup and Recovery**为 **KVM** 工作负载创建和管理保护组

创建保护组来管理一组 KVM 资源的备份操作。保护组是您想要一起保护的资源（例如虚拟机和存储池）的逻辑分组。您需要创建一个保护组来备份KVM虚拟机或存储池。

您可以执行与保护组相关的以下任务：

- 创建保护组。
- 查看保护详情。
- 立即备份保护组。看"立即备份 KVM 工作负载"。
- 删除保护组。

创建保护组

将您想要保护的虚拟机和存储池分组到保护组中。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。

2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择*创建保护组*。
6. 为保护组提供一个名称。
7. 选择要包含在保护组中的虚拟机或存储池。
8. 选择“下一步”。
9. 选择要应用于保护组的*备份策略*。

   有关创建备份策略的更多信息，请参阅"创建和管理策略"。

10. 选择“下一步”。
11. 检查配置。
12. 选择“创建”来创建保护组。

删除保护组

删除保护组会删除该保护组以及所有相关的备份计划。如果不再需要某个保护组，您可能需要将其删除。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择要删除的保护组。
6. 选择“操作”图标 ••• > 删除。
7. 查看有关删除相关备份的确认消息并确认删除。

使用NetApp Backup and RecoveryKVM 工作负载

将 KVM 保护组从本地ONTAP系统备份到 Amazon Web Services、 Azure NetApp Files 或StorageGRID，以确保您的数据受到保护。备份保护组时， NetApp Console会备份该保护组中包含的虚拟机和存储池。备份会自动生成并存储在您的公共或私有云帐户的对象存储中。

要按计划备份保护组，请创建管理备份和还原操作的策略。看"创建策略"以获取说明。

- 创建保护组来管理一组资源的备份和还原操作。看"使用NetApp Backup and Recovery为 KVM 工作负载创建和管理保护组"了解更多信息。

立即使用按需备份来备份保护组

您可以立即运行按需备份。如果您要对系统进行更改并希望确保在开始之前进行备份，这将很有帮助。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 在 KVM 图块中，选择 发现和管理。
3. 选择*库存*。
4. 选择一个工作负载来查看保护详细信息。
5. 选择“操作”图标 ••• > 查看详情。
6. 选择“保护组”、“数据存储”或“虚拟机”选项卡。
7. 选择要备份的保护组。
8. 选择“操作”图标 ••• > 立即备份。

   应用于备份的策略与分配给保护组的策略相同。

9. 选择计划层级。
10. 选择*备份*。

使用NetApp Backup and Recovery还原 KVM 虚拟机

使用NetApp Backup and Recovery从快照、复制到辅助存储的保护组备份或存储在对象存储中的备份恢复 KVM 虚拟机。

从这些位置恢复

您可以从不同的起始位置还原虚拟机：

- 从主位置恢复（本地快照）
- 从二级存储上的复制资源恢复
- 从对象存储备份恢复

恢复到这些点

您可以将数据恢复到以下点：

- 恢复到原始位置

从对象存储中恢复的注意事项

如果您选择对象存储中的备份文件，并且该备份的勒索软件保护处于活动状态（如果您在备份策略中启用了 DataLock 和勒索软件恢复），则系统会提示您在恢复数据之前对备份文件运行额外的完整性检查。我们建议您执行扫描。

您将需要向云提供商支付额外的出口费用才能访问备份文件的内容。

虚拟机恢复的工作原理

还原虚拟机时，会发生以下情况：

- 当您从本地备份文件恢复工作负载时， NetApp Backup and Recovery会使用备份中的数据创建一个_新_资源。
- 从复制的虚拟机还原时，您可以将其还原到原始系统或本地ONTAP系统。
- 从对象存储还原备份时，您可以将数据还原到原始系统或本地ONTAP系统。

从“还原”页面（也称为“搜索和还原”），您可以还原虚拟机，即使您不记得确切的名称、虚拟机所在的位置或虚拟机上次处于良好状态的日期。您可以使用过滤器搜索快照。

从恢复选项恢复虚拟机（搜索和恢复）

使用恢复选项恢复 KVM 虚拟机。您可以按名称或使用过滤器来搜索快照。

所需的控制台角色 备份和恢复超级管理员或备份和恢复恢复管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 从NetApp Backup and Recovery菜单中，选择 恢复。
3. 从名称搜索字段右侧的下拉列表中，选择 **KVM**。
4. 输入要还原的 VM 的名称或筛选要还原的资源所在的 VM 主机或存储池。

   出现符合您的搜索条件的快照列表。

5. 选择要恢复的快照的“恢复”按钮。

   出现可能的还原点列表。

6. 选择您想要使用的还原点。
7. 选择快照源位置。
8. 选择“下一步”继续。
9. 选择恢复目标位置和设置：

目的地选择

恢复到原始位置

1. 启用快速恢复：选择此选项可执行快速恢复操作。恢复的卷和数据将立即可用。请勿在需要高性能的卷上使用此功能，因为在快速恢复过程中，访问数据的速度可能比平时慢。
2. 预恢复选项：输入应在恢复操作之前运行的脚本的完整路径以及该脚本所采用的任何参数。
3. 恢复后选项：
   - 重新启动 **VM**：选择此选项可在还原操作完成后以及应用还原后脚本后重新启动 VM。
   - 后记：输入恢复操作后应运行的脚本的完整路径以及脚本所采用的任何参数。
4. *通知*部分：
   - 启用电子邮件通知：选择此选项可接收有关恢复操作的电子邮件通知，并指示您想要接收的通知类型。
5. 选择*恢复*。

恢复至备用位置

不适用于 KVM 工作负载预览。

保护 **Hyper-V** 工作负载

保护 **Hyper-V** 工作负载概述

使用NetApp Backup and Recovery保护您的 Hyper-V 虚拟机。NetApp Backup and Recovery为独立实例和 FCI 集群实例提供快速、节省空间、崩溃一致性和 VM 一致性的备份和恢复操作。您还可以保护由 System Center Virtual Machine Manager (SCVMM) 配置并托管在 CIFS 共享上的 Hyper-V 虚拟机。

您可以将 Hyper-V 工作负载备份到 Amazon Web Services S3 或StorageGRID ，并将 Hyper-V 工作负载恢复到本地 Hyper-V 主机。

使用NetApp Backup and Recovery实施 3-2-1 保护策略，其中您在 2 个不同的存储系统上拥有 3 个源数据副本，并在云中拥有 1 个副本。3-2-1 方法的优点包括：

- 多个数据副本可防止内部和外部网络安全威胁。
- 多种媒体类型可确保在一种媒体类型发生物理或逻辑故障时能够进行故障转移。
- 现场副本可帮助您快速恢复数据，并且如果现场副本受到损害，您可以使用异地副本。

当您添加 Hyper-V 主机并发现资源时， NetApp Backup and Recovery会在 Hyper-V 主机上安装NetApp Hyper-V 插件和NetApp SnapCenter Windows FileSystem 插件，以帮助管理和保护虚拟机。

要切换到NetApp Backup and Recovery UI 版本或从 NetApp Backup and Recovery UI 版本切换，请参阅"切换到以前的NetApp Backup and RecoveryUI"。

您可以使用NetApp Backup and Recovery执行与 Hyper-V 工作负载相关的以下任务：

- "发现 Hyper-V 工作负载"

- "为 Hyper-V 工作负载创建和管理保护组"
- "备份 Hyper-V 工作负载"
- "恢复 Hyper-V 工作负载"

在NetApp Backup and Recovery中发现 Hyper-V 工作负载

NetApp Backup and Recovery必须先发现 Hyper-V 虚拟机，然后您才能保护它们。

所需的控制台角色 备份和恢复超级管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

添加 **Hyper-V** 主机并发现资源

添加 Hyper-V 主机信息并让NetApp Backup and Recovery发现虚拟机。在每个控制台代理中，选择您想要发现资源的系统。

当您添加 Hyper-V 主机并发现资源时， NetApp Backup and Recovery会在 Hyper-V 主机上安装NetApp Hyper-V 插件和NetApp SnapCenter Windows FileSystem 插件，以帮助管理和保护虚拟机。

步骤

1. 从NetApp Console菜单中，选择 保护 > 备份和恢复。

   如果这是您第一次登录NetApp Backup and Recovery，并且控制台中已经有系统，但尚未发现任何资源，则会出现“欢迎使用新的NetApp Backup and Recovery”登录页面并显示“发现资源”选项。

2. 选择*发现资源*。
3. 输入以下信息：
   a. 工作负载类型：选择*Hyper-V*。
   b. 如果您尚未存储此 Hyper-V 主机的凭据，请选择“添加凭据”。
      i. 选择与该主机一起使用的控制台代理。
      ii. 输入此凭证的名称。
      iii. 输入该帐户的用户名和密码。
      iv. 选择*完成*。
   c. 主机注册：通过输入主机的 FQDN 或 IP 地址、凭据、控制台代理和端口号来添加新的 Hyper-V 主机。如果控制台代理无法解析 FQDN，则改用 IP 地址。对于 FCI 集群，请输入 FCI 集群管理 IP 地址。
4. 选择*发现*。

   此过程可能需要几分钟。

结果

NetApp Backup and Recovery发现资源后，“清单”页面会在工作负载列表中显示 Hyper-V 工作负载。

继续访问**NetApp Backup and Recovery**仪表板

步骤

1. 从NetApp Console菜单中，选择 保护 > 备份和恢复。
2. 选择一个工作负载图块（例如，Microsoft SQL Server）。
3. 从备份和恢复菜单中，选择*仪表板*。
4. 审查数据保护的健康状况。处于危险中或受保护的工作负载的数量会根据新发现、受保护和备份的工作负载而增加。

使用**NetApp Backup and Recovery**为 **Hyper-V** 工作负载创建和管理保护组

创建保护组来管理一组虚拟机的备份操作。保护组是您想要一起保护的资源（例如虚拟机）的逻辑分组。

您可以执行与保护组相关的以下任务：

- 创建保护组。
- 查看保护详情。
- 立即备份保护组。看"立即备份 Hyper-V 工作负载"。
- 删除保护组。

创建保护组

将您想要保护的工作负载分组到一个保护组中。创建保护组来一起备份和恢复工作负载。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择“保护组”菜单。
5. 选择*创建保护组*。
6. 为保护组提供一个名称。
7. 选择要包含在保护组中的虚拟机。
8. 选择“下一步”。
9. 选择要应用于保护组的*备份策略*。
10. 选择“下一步”。
11. 检查配置。
12. 选择“创建”来创建保护组。

编辑保护组

编辑保护组以更改其名称或设置。如果保护组中的资源发生了变化，您可能需要编辑该保护组。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 > 查看详情。
4. 选择*保护组*选项卡。
5. 选择要编辑的保护组。
6. 选择“操作”图标 > 编辑。
7. 更改保护组的任何设置，例如名称或组中的虚拟机。
8. 选择“下一步”。
9. 必要时更改保护策略。完成后，选择“下一步”。
10. 检查配置并选择“提交”。

删除保护组

删除保护组会删除该保护组以及所有相关的备份计划。如果不再需要某个保护组，您可能需要将其删除。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 > 查看详情。
4. 选择*保护组*选项卡。
5. 选择要删除的保护组。
6. 选择“操作”图标 > 删除。
7. 查看有关删除相关备份的确认消息并确认删除。

使用**NetApp Backup and Recovery**Hyper-V 工作负载

将 Hyper-V VM 从本地ONTAP系统备份到 Amazon Web Services、 Azure NetApp Files或StorageGRID，以确保您的数据受到保护。备份会自动生成并存储在您的公共或私有云帐户的对象存储中。

- 要按计划备份工作负载，请创建管理备份和还原操作的策略。看"创建策略"以获取说明。
- 创建保护组来管理一组资源的备份和还原操作。看"使用NetApp Backup and Recovery为 Hyper-V 工作负载创建和管理保护组"了解更多信息。
- 立即备份工作负载（立即创建按需备份）。

立即使用按需备份来备份工作负载

使用按需备份，以便在进行系统更改之前保护您的数据。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从菜单中选择*库存*。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 > 查看详情。
4. 选择“保护组”、“数据存储”或“虚拟机”选项卡。
5. 选择要备份的保护组或虚拟机。
6. 选择“操作”图标 > 立即备份。

   备份使用分配给保护组或虚拟机的相同策略。

7. 选择计划层级。
8. 选择*备份*。

使用NetApp Backup and Recovery恢复 Hyper-V 工作负载

使用NetApp Backup and Recovery从快照、复制到辅助存储的工作负载备份或存储在对象存储中的备份恢复 Hyper-V 工作负载。

从这些位置恢复

您可以从不同的起始位置恢复工作负载：

- 从主位置恢复（本地快照）
- 从二级存储上的复制资源恢复
- 从对象存储备份恢复

恢复到这些点

您可以将数据恢复到以下点：

- 恢复到原始位置
- 恢复到备用位置

从对象存储中恢复的注意事项

如果您选择对象存储中的备份文件，并且该备份的勒索软件保护处于活动状态（如果您在备份策略中启用了 DataLock 和勒索软件恢复），则系统会提示您在恢复数据之前对备份文件运行额外的完整性检查。我们建议您执行扫描。

您将需要向云提供商支付额外的出口费用才能访问备份文件的内容。

恢复工作负载的工作原理

恢复工作负载时，会发生以下情况：

- 当您从本地备份文件恢复工作负载时， NetApp Backup and Recovery会使用备份中的数据创建一个_新_资源。
- 从复制的工作负载恢复时，您可以将工作负载恢复到原始系统或本地ONTAP系统。

从“恢复”页面（也称为“搜索和恢复”），您可以恢复资源，即使您不记得确切的名称、它所在的位置或它最后处于良好状态的日期。您可以使用过滤器搜索快照。

从恢复选项恢复工作负载数据（搜索和恢复）

使用恢复选项恢复 Hyper-V 工作负载。您可以按名称或使用过滤器来搜索快照。

所需的控制台角色 备份和恢复超级管理员或备份和恢复恢复管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 恢复。
2. 从名称搜索字段右侧的下拉列表中，选择 **Hyper-V**。
3. 输入要还原的资源的名称，或者筛选要还原的资源所在的 VM 名称、VM 主机或存储池。

   出现符合您的搜索条件的快照列表。

4. 选择要恢复的快照的“恢复”按钮。

   出现可能的还原点列表。

5. 选择您想要使用的还原点。
6. 选择快照源位置。
7. 选择“下一步”继续。
8. 选择恢复目标位置和设置：

目的地选择

恢复到原始位置

恢复到原始位置后，您可以通过展开“目标设置”部分来查看目标设置，但您无法更改它们。

1. 在“恢复后选项”部分，请考虑以下选项：
   - 启动虚拟机：启用此选项可在恢复后启动新的虚拟机。
2. 选择*恢复*。

恢复至备用位置

1. 在“目标设置”部分，输入以下信息：
   - **Hyper-V FQDN** 或 **IP** 地址：输入目标 Hyper-V 主机的完全限定域名或 IP 地址。
   - 网络：选择要将快照还原到的目标网络。
   - 虚拟机名称：输入要还原的虚拟机的名称。
   - 目标位置：输入应包含已恢复数据的目标文件夹或 CIFS 共享。
2. 在“恢复前选项”部分，请考虑以下选项：
   - 快速恢复：启用此选项可使恢复的虚拟机立即可用。仅从对象存储中恢复运行虚拟机所需的文件，而不是整个卷。
3. 在“恢复后选项”部分，请考虑以下选项：
   - 启动虚拟机：启用此选项可在恢复后启动新的虚拟机。
4. 选择*恢复*。

保护 **Oracle Database** 工作负载（预览）

保护 **Oracle** 数据库工作负载概述

使用 NetApp Backup and Recovery 保护 Oracle 数据库和日志。获取快速、节省空间、故障一致和数据库一致的备份和恢复。将 Oracle Database 工作负载备份到 AWS S3、NetApp StorageGRID、Azure Blob Storage 或 ONTAP S3。将备份还原到本地 Oracle 主机。

使用NetApp Backup and Recovery实施 3-2-1 保护策略，其中您在 2 个不同的存储系统上拥有 3 个源数据副本，并在云中拥有 1 个副本。3-2-1 方法的优点包括：

- 多个数据副本可防止内部和外部网络安全威胁。
- 如果一种媒体发生故障，使用不同类型的媒体可以帮助您恢复。
- 您可以从现场副本快速恢复，如果现场副本受到损害，则可以使用异地副本。

要切换到NetApp Backup and Recovery UI 版本或从 NetApp Backup and Recovery UI 版本切换，请参阅"切换到以前的NetApp Backup and RecoveryUI"。

您可以使用 NetApp Backup and Recovery 执行以下与 Oracle 数据库工作负载相关的任务：

- "发现 Oracle Database 工作负载"
- "为 Oracle Database 工作负载创建和管理保护组"
- "备份 Oracle Database 工作负载"
- "还原 Oracle Database 工作负载"

在 NetApp Backup and Recovery 中发现 Oracle 数据库工作负载

NetApp Backup and Recovery需要首先发现您的 Oracle 数据库，以便您可以保护它们。

所需的控制台角色 备份和恢复超级管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

添加 Oracle 主机并发现资源

添加 Oracle 主机信息并让NetApp Backup and Recovery发现工作负载。在每个控制台代理中，选择您想要发现工作负载的系统。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 在“工作负载”下，选择“Oracle”磁贴。

   如果您是第一次登录备份和恢复，并且在控制台中有一个系统但没有发现任何资源，则会显示“欢迎使用新的NetApp备份和恢复”页面，其中包含“发现资源”选项。

3. 选择*发现资源*。
4. 输入以下信息：
   a. 工作负载类型：选择*Oracle*。
   b. 如果您尚未存储此 Oracle 主机的凭据，请选择“添加凭据”。
      i. 选择与该主机一起使用的控制台代理。
      ii. 输入此凭证的名称。
      iii. 输入该帐户的用户名和密码。
      iv. 选择*完成*。
   c. 主机注册：添加新的 Oracle 主机。输入主机的 FQDN 或 IP 地址、凭据、控制台代理和端口号。
5. 选择*发现*。

   此过程可能需要几分钟。

结果

Oracle 工作负载显示在清单页面的工作负载列表中。

继续访问NetApp Backup and Recovery仪表板

1. 从NetApp Console菜单中，选择 保护 > 备份和恢复。

2. 选择一个工作负载图块（例如，Microsoft SQL Server）。
3. 从备份和恢复菜单中，选择*仪表板*。
4. 审查数据保护的健康状况。处于危险中或受保护的工作负载的数量会根据新发现、受保护和备份的工作负载而增加。

使用 NetApp Backup and Recovery 为 Oracle Database 工作负载创建和管理保护组

创建保护组来管理一组 Oracle 数据库资源的备份操作。保护组是您想要一起保护的资源（例如数据库）的逻辑分组。您需要创建一个保护组来备份 Oracle 数据库。

您可以执行与保护组相关的以下任务：

- 创建保护组。
- 查看保护详情。
- 立即备份保护组。请参阅 "立即备份 Oracle Database 工作负载"。
- 删除保护组。

创建保护组

将您想要保护的虚拟机和存储池分组到保护组中。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择*创建保护组*。
6. 为保护组提供一个名称。
7. 选择要包含在保护组中的虚拟机或存储池。
8. 选择“下一步”。
9. 选择要应用于保护组的*备份策略*。

   如果要创建策略，请选择*创建新策略*并按照提示创建策略。看"创建策略"了解更多信息。
10. 选择“下一步”。
11. 检查配置。
12. 选择“创建”来创建保护组。

删除保护组

删除保护组会删除该保护组以及所有相关的备份计划。如果不再需要某个保护组，您可能需要将其删除。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择一个工作负载来查看保护详细信息。
3. 选择“操作”图标 ••• > 查看详情。
4. 选择*保护组*选项卡。
5. 选择要删除的保护组。
6. 选择“操作”图标 ••• > 移除保护。
7. 查看有关删除相关备份的确认消息并确认删除。

使用 **NetApp Backup and Recovery** 备份 **Oracle Database** 工作负载

使用NetApp Backup and Recovery将 Oracle 数据库保护组或数据库从本地ONTAP系统备份到云存储，包括 Amazon S3、 NetApp StorageGRID、Microsoft Azure Blob Storage或ONTAP S3。 NetApp Backup and Recovery每个保护组中的数据库和日志数据。

要按计划备份保护组或单个数据库，请创建管理备份和还原操作的策略。看"创建策略"以获取说明。

- 创建保护组以管理一组资源的备份和还原操作。有关详细信息，请参见 "使用 NetApp Backup and Recovery 为 Oracle Database 工作负载创建和管理保护组"。
- 立即备份保护组（立即创建按需备份）。
- 立即备份数据库。

立即使用按需备份来备份保护组

在进行系统更改之前运行按需备份以确保您的数据受到保护。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 在“工作负载”下，选择“Oracle”磁贴。
3. 选择*库存*。
4. 选择一个工作负载来查看保护详细信息。
5. 选择“操作”图标 ••• > 查看详情。
6. 选择“保护组”、“数据存储”或“虚拟机”选项卡。
7. 选择要备份的保护组。

8. 选择“操作”图标 ••• > 立即备份。

   NetApp Backup and Recovery对备份和保护组使用相同的策略。

9. 选择计划层级。
10. 选择*备份*。

立即使用按需备份来备份数据库

您可以运行单个数据库的按需备份。

所需的控制台角色 备份和恢复超级管理员或备份和恢复备份管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 在“工作负载”下，选择“Oracle”磁贴。
3. 选择*库存*。
4. 选择一个工作负载来查看保护详细信息。
5. 选择“操作”图标 ••• > 查看详情。
6. 选择“数据库”选项卡。
7. 选择要备份的数据库。
8. 选择“操作”图标 ••• > 立即备份。
9. 选择计划层级。
10. 选择*备份*。

使用NetApp Backup and Recovery恢复 Oracle 数据库

使用NetApp Backup and Recovery从快照、复制到辅助存储的备份或存储在对象存储中的备份恢复 Oracle 数据库。

从这些位置恢复

您可以从不同的起始位置恢复数据库：

- 从主位置恢复（本地快照）
- 从二级存储上的复制资源恢复
- 从对象存储备份恢复

恢复到这些点

您可以将数据恢复到原始位置；在此私人预览版中不提供恢复到备用位置的功能。

- 恢复到原始位置

Oracle 数据库恢复的工作原理

还原 Oracle 数据库时，会发生以下情况：

- 当您从本地快照恢复数据库时， NetApp Backup and Recovery会使用备份中的数据创建一个_新_资源。
- 从复制的存储恢复时，您可以将其恢复到原始位置。
- 从对象存储还原备份时，您可以将数据还原到源存储或本地ONTAP系统，然后从那里恢复数据库。

从“恢复”页面（也称为“搜索和恢复”），您可以恢复数据库，即使您不记得确切的名称、它所在的位置或它最后处于良好状态的日期。您可以使用过滤器搜索数据库。

还原 Oracle 数据库

根据您的需要，将 Oracle 数据库还原到特定时间点、特定系统更改号 (SCN) 或最后的良好状态。您还可以简单地从快照恢复数据库并跳过自动恢复过程。如果您想手动执行恢复，您可能希望跳过自动恢复过程。您可以使用数据库名称或特定过滤器来搜索数据库。

所需的控制台角色 备份和恢复超级管理员或备份和恢复恢复管理员角色。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 从NetApp Backup and Recovery菜单中，选择 恢复。
3. 从名称搜索字段右侧的下拉列表中，选择 **Oracle**。
4. 输入要还原的数据库的名称或筛选要还原的数据库所在的数据库主机。

   出现符合您的搜索条件的快照列表。
5. 选择要恢复的数据库的“恢复”按钮。
6. 选择恢复选项：

恢复到特定时间点

a. 选择*恢复到特定时间点*。
b. 选择“下一步”。
c. 从下拉菜单中选择一个日期，然后选择*搜索*。

   显示指定日期的匹配快照列表。

恢复到特定的系统变更号 **(SCN)**

a. 选择*恢复到特定的系统变更号 (SCN)*。
b. 选择“下一步”。
c. 输入要用作还原点的 SCN，然后选择*搜索*。

   显示指定 SCN 的匹配快照列表。

恢复到最新备份（上次良好状态）

a. 选择*恢复到最新备份*。
b. 选择“下一步”。

   显示最新的完整备份和日志备份。

从快照还原，无需恢复

a. 选择*从没有恢复的快照中恢复*。
b. 选择“下一步”。

   显示匹配的快照。

7. 选择快照源位置。
8. 选择“下一步”继续。
9. 选择恢复目标位置和设置：

目的地选择

恢复到原始位置

1. 目的地设置：
   - 选择恢复整个数据库或仅恢复数据库的表空间。
   - 控制文件：可选地，启用此选项也可以恢复数据库控制文件。
2. 预恢复选项：
   - 或者，启用此选项并输入应在还原操作之前运行的脚本的完整路径以及该脚本所采用的任何参数。
   - 为脚本选择一个超时值。如果脚本未能在此时间段内执行，则恢复仍将继续。
3. 恢复后选项：
   - 后记：可选地，启用此选项并输入应在恢复操作后运行的脚本的完整路径以及该脚本所采用的任何参数。
   - 恢复后以 **READ-WRITE** 模式打开数据库或容器数据库：恢复操作完成后，备份和恢复将为数据库启用 READ-WRITE 模式。
4. *通知*部分：
   - 启用电子邮件通知：选择此选项可接收有关恢复操作的电子邮件通知，并指示您想要接收的通知类型。
5. 选择*恢复*。

恢复至备用位置

不适用于 Oracle Database 工作负载预览。

使用NetApp Backup and Recovery挂载和卸载 Oracle 数据库恢复点

如果您需要以受控状态访问数据库来执行恢复操作，则可能需要安装 Oracle 数据库恢复点。

安装 Oracle 数据库还原点

如果您将数据库的保护策略配置为保留存档日志，则可以挂载恢复点来查看数据库更改历史记录。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 选择 Oracle 图块。
3. 在备份和恢复菜单中，选择*Inventory*。
4. 对于列表中的 Oracle 数据库工作负载，选择“查看”。
5. 选择*数据库*菜单。
6. 从列表中选择一个数据库并选择“操作”图标 ••• > 查看保护详情。

   出现该数据库的恢复点列表。
7. 从列表中选择一个恢复点，然后选择“操作”图标 ••• > 安装。

8. 在出现的对话框中，执行以下操作：
   a. 从列表中选择应安装恢复点的主机。
   b. 选择“备份和恢复”应使用哪个位置来安装恢复点。对于预览版本，不支持从对象存储挂载。

      显示备份和恢复应使用的安装路径。
9. 选择*安装*。

   恢复点安装在 Oracle 主机上。

卸载 **Oracle** 数据库还原点

当您不再需要查看对该数据库所做的更改时，请卸载恢复点。

步骤

1. 从NetApp Console菜单中，选择“保护”>“备份和恢复”。
2. 选择 Oracle 图块。
3. 在备份和恢复菜单中，选择*Inventory*。
4. 对于列表中的 Oracle 工作负载，选择“查看”。
5. 选择*数据库*菜单。
6. 从列表中选择一个数据库并选择“操作”图标 ••• > 查看保护详情。

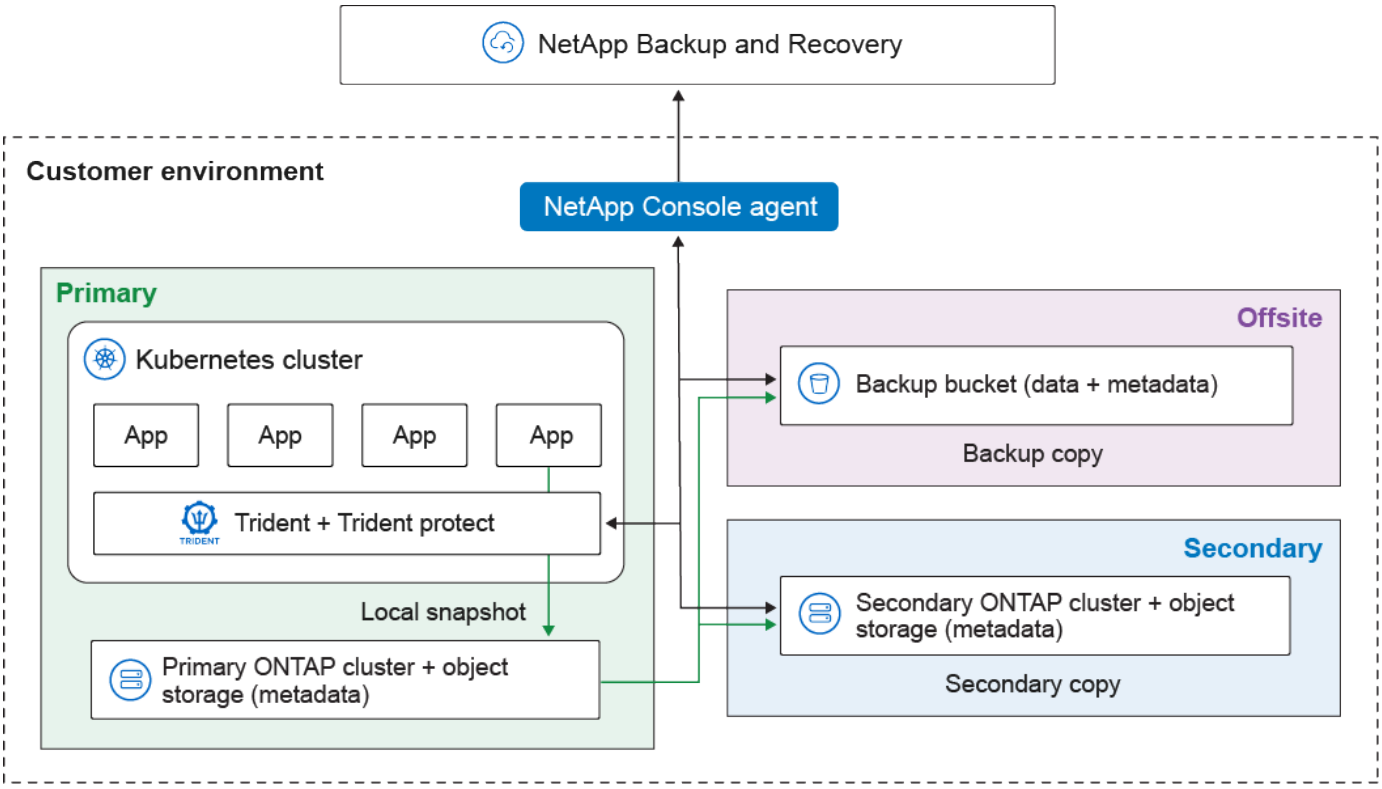
   出现该数据库的恢复点列表。
7. 从列表中选择一个恢复点，然后选择“操作”图标 ••• > 卸载。
8. 选择“卸载”确认操作。

保护 **Kubernetes** 工作负载（预览版）

管理 **Kubernetes** 工作负载概览

通过在NetApp Backup and Recovery中管理 Kubernetes 工作负载，您可以在一个地方发现、管理和保护您的 Kubernetes 集群和应用程序。您可以管理托管在 Kubernetes 集群上的资源和应用程序。您还可以创建保护策略并将其与 Kubernetes 工作负载关联，所有这些都使用单一界面完成。

下图展示了 Kubernetes 工作负载的备份和恢复的组件和基本架构，以及如何将数据的不同副本存储在不同位置：



NetApp Backup and Recovery为管理 Kubernetes 工作负载提供了以下优势：

- 单一控制平面，用于保护跨多个 Kubernetes 集群运行的应用程序。这些应用程序可以包括在 Kubernetes 集群上运行的容器或虚拟机。
- 与NetApp SnapMirror本机集成，为所有备份和恢复工作流程提供存储卸载功能。
- Kubernetes 应用程序的永久增量备份，转化为更低的恢复点目标 (RPO) 和恢复时间目标 (RTO)。

本文档作为技术预览提供。在预览期间，不建议将 Kubernetes 功能用于生产工作负载。对于此预览版产品， NetApp保留在正式发布之前修改产品详细信息、内容和时间表的权利。

您可以完成与管理 Kubernetes 工作负载相关的以下任务：

- "发现 Kubernetes 工作负载"。
- "管理 Kubernetes 集群"。
- "添加和保护 Kubernetes 应用程序"。
- "管理 Kubernetes 应用程序"。
- "恢复 Kubernetes 应用程序"。

探索NetApp Backup and Recovery中的 Kubernetes 工作负载

NetApp Backup and Recovery需要在保护 Kubernetes 工作负载之前发现它们。

所需的**NetApp Console**角色 备份和恢复超级管理员。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

发现 **Kubernetes** 工作负载

在备份和恢复清单中，发现您环境中的 Kubernetes 工作负载。添加工作负载会将 Kubernetes 集群添加到NetApp Backup and Recovery。然后，您可以添加应用程序并保护集群资源。

> 当您发现当前受 Trident Protect 保护的群集时，在发现过程中将禁用与 Trident Protect 一起使用的任何备份计划（Trident Protect 备份计划与 Backup and Recovery 不兼容）。要保护群集的应用程序，"创建新的保护策略"或将应用程序与现有策略关联。然后，如果需要，您可以删除 Trident Protect 备份计划。

步骤

1. 执行以下操作之一：
   - 如果您是第一次发现 Kubernetes 工作负载，请在NetApp Backup and Recovery中，在“工作负载”下，选择“Kubernetes”磁贴。
   - 如果您已经发现 Kubernetes 工作负载，请在NetApp Backup and Recovery中选择 **Inventory** > **Workloads**，然后选择 **Discover resources**。
2. 选择 **Kubernetes** 工作负载类型。
3. 输入集群名称并选择与集群一起使用的连接器。
4. 按照出现的命令行说明进行操作：
   - 创建 Trident Protect 命名空间
   - 创建 Kubernetes 机密
   - 添加 Helm 存储库
   - 安装或升级 Trident Protect 和 Trident Protect 连接器

     这些步骤确保NetApp Backup and Recovery可以与集群交互。
5. 完成这些步骤后，选择*发现*。

   该集群已添加到清单中。
6. 在关联的 Kubernetes 工作负载中选择“查看”以查看该工作负载的应用程序、集群和命名空间列表。

继续访问**NetApp Backup and Recovery**仪表板

按照以下步骤查看NetApp Backup and Recovery仪表板。

1. 从NetApp Console菜单中，选择 保护 > 备份和恢复。
2. 选择一个工作负载图块（例如，Microsoft SQL Server）。
3. 从备份和恢复菜单中，选择*仪表板*。
4. 审查数据保护的健康状况。处于危险中或受保护的工作负载的数量会根据新发现、受保护和备份的工作负载而增加。

   "了解仪表板显示的内容"。

添加和保护 **Kubernetes** 应用程序

添加和保护 **Kubernetes** 应用程序

NetApp Backup and Recovery使您能够轻松发现 Kubernetes 集群，而无需生成和上传 kubeconfig 文件。您可以使用从NetApp Console用户界面复制的简单命令连接 Kubernetes 集群并安装所需的软件。

所需的**NetApp Console**角色

组织管理员或SnapCenter管理员。"了解NetApp Backup and Recovery访问角色" 。 "了解所有服务的NetApp Console访问角色" 。

添加并保护新的 **Kubernetes** 应用程序

保护 Kubernetes 应用程序的第一步是在NetApp Backup and Recovery中创建应用程序。创建应用程序时，您会让控制台了解 Kubernetes 集群上正在运行的应用程序。

开始之前

在添加和保护 Kubernetes 应用程序之前，您需要"发现 Kubernetes 工作负载"。

使用 **Web UI** 添加应用程序

步骤

1. 在NetApp Backup and Recovery中，选择 **Inventory**。
2. 选择一个 Kubernetes 实例，然后选择“查看”以查看与该实例关联的资源。
3. 选择“应用程序”选项卡。
4. 选择*创建应用程序*。
5. 输入应用程序的名称。
6. 或者，选择以下任意字段来搜索您想要保护的资源：
   - 关联集群
   - 关联的命名空间
   - 资源类型
   - 标签选择器
7. （可选）选择“集群范围资源”以选择任何在集群级别范围限定的资源。如果包含这些资源，它们会在创建应用程序时添加到应用程序中。
8. 或者，选择“搜索”以根据您的搜索条件查找资源。

   控制台不存储搜索参数或结果；这些参数用于在选定的 Kubernetes 集群中搜索可包含在应用程序中的资源。

9. 控制台显示符合您的搜索条件的资源列表。
10. 如果列表包含您想要保护的资源，请选择“下一步”。
11. （可选）在“策略”区域中，选择现有保护策略来保护应用程序，或者创建新策略。如果不选择策略，则创建的应用程序将不带保护策略。你可以"添加保护策略"之后。
12. 在*Prescripts and postscripts*区域中，启用并配置您想要在备份操作之前或之后运行的任何prescript或postscript执行挂钩。要启用处方或附言，您必须至少已创建了一个"执行钩子模板"。
13. 选择“创建”。

结果

应用程序已创建并出现在 Kubernetes 清单的 应用程序 选项卡中的应用程序列表中。 NetApp Console根据您的设置启用对应用程序的保护，并且您可以在备份和恢复的*监控*区域中监控进度。

使用 **CR** 添加应用程序

步骤

1. 创建目标应用程序 CR 文件：
   a. 创建自定义资源 (CR) 文件并将其命名（例如， `my-app-name.yaml`）。
   b. 配置以下属性：
      - **metadata.name**：（必需）应用程序自定义资源的名称。请注意您选择的名称，因为保护操作所需的其他 CR 文件会引用此值。
      - **spec.includedNamespaces**: (*Required*) 使用命名空间和标签选择器指定应用程序使用的命名

空间和资源。应用程序命名空间必须是此列表的一部分。标签选择器是可选的，可用于筛选每个指定命名空间内的资源。

- **spec.includedClusterScopedResources**: (*Optional*) 使用此属性指定要包含在应用程序定义中的群集范围的资源。此属性允许您根据其组、版本、种类和标签选择这些资源。
  - **groupVersionKind**：（必需）指定集群范围内资源的 API 组、版本和种类。
  - **labelSelector**：（可选）根据集群范围资源的标签对其进行筛选。

c. 如果需要，请配置以下注释：

- **metadata.annotations.protect.trident.netapp.io/skip-vm-freeze**：（*Optional*）此批注仅适用于从虚拟机定义的应用程序，例如在 KubeVirt 环境中，快照之前会发生文件系统冻结。指定此应用程序是否可以在快照期间写入文件系统。如果设置为 true，应用程序将忽略全局设置，并且可以在快照期间写入文件系统。如果设置为 false，应用程序将忽略全局设置，并在快照期间冻结文件系统。如果指定，但应用程序在应用程序定义中没有虚拟机，则忽略批注。如果未指定，则应用程序遵循 "全局文件系统冻结设置"。
- **protect.trident.netapp.io/protection-command**：（可选）使用此注释指示 Backup and Recovery 保护或停止保护应用程序。可能的值为 `protect`或 `unprotect`。
- **protect.trident.netapp.io/protection-policy-name**: (可选) 使用此注释指定要用于保护此应用程序的 Backup and Recovery 保护策略的名称。此保护策略必须已存在于 Backup and Recovery 中。

如果需要在已创建应用程序后应用此批注，可以使用以下命令：

```
kubectl annotate application -n <application CR namespace> <application CR name> protect.trident.netapp.io/skip-vm-freeze="true"
```

+
示例 YAML：

+

```
apiVersion: protect.trident.netapp.io/v1
kind: Application
metadata:
  annotations:
    protect.trident.netapp.io/skip-vm-freeze: "false"
    protect.trident.netapp.io/protection-command: "protect"
    protect.trident.netapp.io/protection-policy-name: "policy-name"
  name: my-app-name
  namespace: my-app-namespace
spec:
  includedNamespaces:
    - namespace: namespace-1
      labelSelector:
        matchLabels:
          app: example-app
    - namespace: namespace-2
      labelSelector:
        matchLabels:
          app: another-example-app
  includedClusterScopedResources:
    - groupVersionKind:
        group: rbac.authorization.k8s.io
        kind: ClusterRole
        version: v1
      labelSelector:
        matchLabels:
          mylabel: test
```

1. （*Optional*）添加包含或排除标有特定标签的资源的筛选：

   - **resourceFilter.resourceSelectionCriteria**：（筛选时需要）使用 `Include`或 `Exclude`来包含或排除在 resourceMatchers 中定义的资源。添加以下 resourceMatchers 参数以定义要包括或排除的资源：

     - **resourceFilter.resourceMatchers**：resourceMatcher 对象数组。如果在此数组中定义多个元素，则它们将作为 OR 操作进行匹配，并且每个元素（组、种类、版本）内的字段将作为 AND 操作进行匹配。

       - **resourceMatchers[].group**：（*Optional*）要筛选的资源的组。
       - **resourceMatchers[].kind**：（*Optional*）要筛选的资源的类型。
       - **resourceMatchers[].version**：（*Optional*）要筛选的资源的版本。

- **resourceMatchers[].names**：（可选）要过滤的资源的 Kubernetes metadata.name 字段中的名称。
- **resourceMatchers[].namespaces**: (*Optional*) 要过滤的资源的 Kubernetes metadata.name 字段中的命名空间。
- **resourceMatchers[].labelSelectors**: (*Optional*) 资源的 Kubernetes metadata.name 字段中的标签选择器字符串，如 "Kubernetes 文档" 中所定义。例如："trident.netapp.io/os=linux"。

> 当同时使用 `resourceFilter`和 `labelSelector`时， `resourceFilter`首先运行，然后将 `labelSelector`应用于生成的资源。

例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

2. 创建与环境匹配的应用程序 CR 后，应用 CR。例如：

```
kubectl apply -f my-app-name.yaml
```

立即使用 **Backup and Recovery Web UI** 备份 **Kubernetes** 应用程序

NetApp Backup and Recovery 使您能够使用 Web 界面手动备份 Kubernetes 应用程序。

所需的**NetApp Console**角色

组织管理员或SnapCenter管理员。"了解NetApp Backup and Recovery访问角色" 。 "了解所有服务的NetApp Console访问角色" 。

立即使用 **Web UI** 备份 **Kubernetes** 应用程序

手动创建 Kubernetes 应用程序的备份，为未来的备份和快照建立基线，或确保最新数据受到保护。

步骤

1. 在NetApp Backup and Recovery中，选择 **Inventory**。
2. 选择一个 Kubernetes 实例，然后选择“查看”以查看与该实例关联的资源。
3. 选择“应用程序”选项卡。
4. 在应用程序列表中，选择要备份的应用程序并选择相关的操作菜单。
5. 选择*立即备份*。
6. 确保选择了正确的应用程序名称。
7. 选择*备份*。

结果

控制台创建应用程序的备份并在备份和恢复的*监控*区域中显示进度。该备份是根据与应用程序关联的保护策略创建的。

现在使用 **Backup and Recovery** 中的自定义资源备份 **Kubernetes** 应用程序

NetApp Backup and Recovery 使您能够使用自定义资源 (CR) 手动备份 Kubernetes 应用程序。

现在使用自定义资源备份 **Kubernetes** 应用程序

手动创建 Kubernetes 应用程序的备份，为未来的备份和快照建立基线，或确保最新数据受到保护。

如果集群范围的资源在应用程序定义中显式引用，或者它们引用了任何应用程序命名空间，则会包含在备份、快照或克隆中。

开始之前

确保 AWS 会话令牌过期时间足以支持任何长时间运行的 s3 备份操作。如果令牌在备份操作期间过期，操作可能会失败。

- 有关检查当前会话令牌过期的详细信息，请参见 "AWS API 文档"。
- 有关 AWS 资源凭据的详细信息，请参见 "AWS IAM 文档"。

使用自定义资源创建本地快照

要创建 Kubernetes 应用程序的快照并将其存储在本地，请使用具有特定属性的 Snapshot 自定义资源。

步骤

1. 创建自定义资源 (CR) 文件并将其命名为 `local-snapshot-cr.yaml`。
2. 在创建的文件中，配置以下属性：
   - **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
   - **spec.applicationRef**：要快照的应用程序的 Kubernetes 名称。

- **spec.appVaultRef**：（必需）应存储快照内容（元数据）的 AppVault 的名称。
- **spec.reclaimPolicy**：（可选）定义删除快照 CR 时快照的 AppArchive 会发生什么情况。这意味着即使设置为 `Retain`，快照也将被删除。有效选项：
  - `Retain` (默认)
  - `Delete`

```
apiVersion: protect.trident.netapp.io/v1
kind: Snapshot
metadata:
  namespace: my-app-namespace
  name: local-snapshot-cr
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  reclaimPolicy: Retain
```

3. 使用正确的值填充 `local-snapshot-cr.yaml`文件后，应用 CR：

```
kubectl apply -f local-snapshot-cr.yaml
```

使用自定义资源将应用程序备份到对象存储

创建具有特定属性的 Backup CR，以将应用程序备份到对象存储。

步骤

1. 创建自定义资源 (CR) 文件并将其命名为 `object-store-backup-cr.yaml`。
2. 在创建的文件中，配置以下属性：
   - **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
   - **spec.applicationRef**：（必需）要备份的应用程序的 Kubernetes 名称。
   - **spec.appVaultRef**：（必需，与 *spec.appVaultTargetsRef* 互斥）如果使用相同的存储桶存储快照和备份，则这是应存储备份内容的 AppVault 的名称。
   - **spec.appVaultTargetsRef**：（必需，与 *spec.appVaultRef* 互斥）如果您使用不同的存储桶来存储快照和备份，这是应存储备份内容的 AppVault 的名称。
   - **spec.dataMover**：（*Optional*）一个字符串，指示要用于备份操作的备份工具。该值区分大小写，必须为 `CBS`。
   - **spec.reclaimPolicy**：（可选）定义删除 Backup CR 时备份内容（元数据/卷数据）会发生什么。可能的值：
     - `Delete`
     - `Retain` (默认)

- **spec.cleanupSnapshot**：（必需）确保备份 CR 创建的临时快照在备份操作完成后不被删除。建议值：`false`。

使用同一存储桶存储快照和备份时的示例 YAML：

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: my-cr-name
spec:
  applicationRef: my-application
  appVaultRef: appvault-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

使用不同存储桶存储快照和备份时的示例 YAML：

```
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: object-store-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
```

3. 使用正确的值填充 `object-store-backup-cr.yaml`文件后，应用 CR：

```
kubectl apply -f object-store-backup-cr.yaml
```

使用自定义资源创建 3-2-1 扇出备份

使用 3-2-1 扇出架构进行备份会将备份复制到辅助存储和对象存储。要创建 3-2-1 扇出备份，请创建具有特定属性的 Backup CR。

步骤

1. 创建自定义资源 (CR) 文件并将其命名为 `3-2-1-fanout-backup-cr.yaml`。
2. 在创建的文件中，配置以下属性：

- **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
- **spec.applicationRef**：（必需）要备份的应用程序的 Kubernetes 名称。
- **spec.appVaultTargetsRef**: (*Required*) 备份内容应存储的 AppVault 的名称。
- **spec.dataMover**：（*Optional*）一个字符串，指示要用于备份操作的备份工具。该值区分大小写，必须为 `CBS`。
- **spec.reclaimPolicy**：（可选）定义删除 Backup CR 时备份内容（元数据/卷数据）会发生什么。可能的值：
  - `Delete`
  - `Retain` (默认)
- **spec.cleanupSnapshot**：（必需）确保备份 CR 创建的临时快照在备份操作完成后不被删除。建议值：`false`。
- **spec.replicateSnapshot**：（*Required*）指示 Backup and Recovery 将快照复制到二级存储。必需值：`true`。
- **spec.replicateSnapshotReclaimPolicy**: (*Optional*) 定义已复制快照在删除时会发生什么。可能的值：
  - `Delete`
  - `Retain` (默认)

  示例 YAML：

```yaml
apiVersion: protect.trident.netapp.io/v1
kind: Backup
metadata:
  namespace: my-app-namespace
  name: 3-2-1-fanout-backup-cr
spec:
  applicationRef: my-application
  appVaultTargetsRef: appvault-targets-name
  dataMover: CBS
  reclaimPolicy: Retain
  cleanupSnapshot: false
  replicateSnapshot: true
  replicateSnapshotReclaimPolicy: Retain
```

3. 使用正确的值填充 `3-2-1-fanout-backup-cr.yaml`文件后，应用 CR：

```
kubectl apply -f 3-2-1-fanout-backup-cr.yaml
```

支持的备份注释

下表介绍了创建备份 CR 时可以使用的批注。

标注	类型	描述	默认值
protect.trident.netapp.io/full-backup	string	指定备份是否应为非增量备份。设置为 `true` 以创建非增量备份。最佳做法是定期执行完整备份，然后在完整备份之间执行增量备份，以最大限度地降低与恢复相关的风险。	"false"
protect.trident.netapp.io/snapshot-completion-timeout	string	整个快照操作完成所允许的最长时间。	“60 分钟”
protect.trident.netapp.io/volume-snapshots-ready-to-use-timeout	string	允许卷快照达到准备就绪状态的最长时间。	"30 分钟"
protect.trident.netapp.io/volume-snapshots-created-timeout	string	允许创建卷快照的最长时间。	"5 分钟"
protect.trident.netapp.io/pvc-bind-timeout-sec	string	在操作失败之前，等待任何新创建的 PersistentVolumeClaims (PVC) 到达 `Bound` 阶段的最长时间（秒）。	"1200"（20 分钟）

恢复 **Kubernetes** 应用程序

使用 **Web UI** 还原 **Kubernetes** 应用程序

NetApp Backup and Recovery使您能够恢复已通过保护策略保护的应用程序。要恢复应用程序，应用程序需要至少有一个可用的恢复点。恢复点由本地快照或对象存储备份（或两者）组成。您可以使用本地、辅助或对象存储存档来恢复应用程序。

开始之前

如果要还原使用 Trident Protect 备份的应用程序，请确保 Trident Protect 同时安装在源和目标集群上。

所需的**NetApp Console**角色

组织管理员或SnapCenter管理员。"了解NetApp Backup and Recovery访问角色" 。 "了解所有服务的NetApp Console访问角色" 。

步骤

1. 在 NetApp Backup and Recovery 菜单中，选择*恢复*。
2. 从列表中选择一个 Kubernetes 应用程序，并为该应用程序选择*查看和恢复*。

   出现还原点列表。

3. 选择要使用的还原点的 **Restore** 按钮。

常规设置

1. 选择要从中还原的源位置。
2. 从*Cluster*列表中选择目标集群。

   目前不支持将 Trident Protect 创建的本地快照还原到其他集群。

3. 选择还原到原始命名空间或新命名空间。
4. 如果选择还原到新命名空间，请输入要使用的目标命名空间。
5. 选择“下一步”。

资源选择

1. 选择是否要恢复与应用程序相关的所有资源，或者使用过滤器选择要恢复的特定资源：

恢复所有资源

1. 选择*恢复所有资源*。
2. 选择“下一步”。

恢复特定资源

1. 选择*选择性资源*。
2. 选择资源过滤器的行为。如果您选择“包括”，则会恢复您选择的资源。如果您选择“排除”，则您选择的资源将不会被恢复。
3. 选择*添加规则*来添加定义选择资源的过滤器的规则。您至少需要一条规则来过滤资源。

   每个规则都可以根据资源命名空间、标签、组、版本和种类等标准进行过滤。
4. 选择*保存*来保存每条规则。
5. 添加完所有需要的规则后，选择*搜索*即可查看备份档案中符合过滤条件的可用资源。

   显示的资源是集群上当前存在的资源。
6. 对结果满意后，选择*下一步*。

目的地设置

1. 展开 **Destination settings** 部分，然后选择恢复到默认存储类、其他存储类，或者如果要恢复到其他集群，则将存储类映射到目标集群。
2. 如果选择还原到其他存储类，请选择与每个源存储类匹配的目标存储类。
3. 或者，如果您要还原使用 Trident Protect 创建的备份或快照，请查看 AppVault 用作还原操作存储桶的详细信息。如果您的环境或 AppVault 状态发生变化，请选择 **Sync App Vault** 以刷新详细信息。

   如果需要在 Kubernetes 集群上创建 AppVault 以便还原使用 Trident Protect 创建的备份或快照，请参阅 "使用 Trident Protect AppVault 对象管理存储桶"。
4. （可选）展开 **Restore scripts** 部分，并启用 **Postscript** 选项以选择将在还原操作完成后运行的执行钩子模板。如果需要，请输入脚本需要的任何参数，并添加标签选择器以根据资源标签筛选资源。
5. 选择*恢复*。

使用自定义资源还原 **Kubernetes** 应用程序

您可以使用自定义资源从快照或备份还原应用程序。将应用程序还原到同一集群时，从现有快照还原将更快。

- 还原应用程序时，为应用程序配置的所有执行挂钩都会随应用程序一起还原。如果存在还原后执行挂钩，它将作为还原操作的一部分自动运行。
- qtree 卷支持从备份还原到其他命名空间或原始命名空间。但是，qtree 卷不支持从快照还原到其他命名空间或原始命名空间。
- 您可以使用高级设置自定义还原操作。要了解更多信息，请参阅 "使用高级自定义资源还原设置"。

将备份还原到其他命名空间

使用 BackupRestore CR 将备份还原到其他命名空间时，Backup and Recovery 会在新命名空间中还原应用程序，并为还原的应用程序创建应用程序 CR。要保护还原的应用程序，请创建按需备份或快照，或建立保护计划。

- 使用现有资源将备份还原到其他命名空间不会更改与备份中的名称共享的任何资源。要还原备份中的所有资源，请删除并重新创建目标命名空间，或将备份还原到新命名空间。
- 使用 CR 还原到新命名空间时，您必须在应用 CR 之前手动创建目标命名空间。Backup and Recovery 仅在使用 CLI 时自动创建命名空间。

开始之前

确保 AWS 会话令牌过期时间足以进行任何长期运行的 s3 还原操作。如果令牌在还原操作期间过期，则操作可能会失败。

- 有关检查当前会话令牌过期的详细信息，请参见 "AWS API 文档"。
- 有关 AWS 资源凭据的详细信息，请参见 "AWS IAM 文档"。

使用 Kopia 作为数据移动器还原备份时，可以选择在 CR 中指定注释，以控制 Kopia 使用的临时存储的行为。有关可以配置的选项的详细信息，请参见 "Kopia 文档"。

步骤

1. 创建自定义资源 (CR) 文件并将其命名为 `trident-protect-backup-restore-cr.yaml`。
2. 在创建的文件中，配置以下属性：
   - **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
   - **spec.appArchivePath**：AppVault 中存储备份内容的路径。您可以使用以下命令查找此路径：

     ```
     kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
     ='{.status.appArchivePath}'
     ```

   - **spec.appVaultRef**：（必需）存储备份内容的 AppVault 的名称。
   - **spec.namespaceMapping**：还原操作的源命名空间到目标命名空间的映射。使用环境中的信息替换

`my-source-namespace`和 `my-destination-namespace`。

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. （可选）如果需要仅选择要还原的应用程序的某些资源，请添加包含或排除标有特定标签的资源的筛选：

> Trident Protect 会自动选择一些资源，因为它们与您选择的资源之间存在关系。例如，如果您选择了永久卷声明资源，并且它具有关联的 pod，则 Trident Protect 也将还原关联的 pod。

- **resourceFilter.resourceSelectionCriteria**：（筛选时需要）使用 `Include`或 `Exclude`来包含或排除在 resourceMatchers 中定义的资源。添加以下 resourceMatchers 参数以定义要包括或排除的资源：
  - **resourceFilter.resourceMatchers**：resourceMatcher 对象数组。如果在此数组中定义多个元素，则它们将作为 OR 操作进行匹配，并且每个元素（组、种类、版本）内的字段将作为 AND 操作进行匹配。
    - **resourceMatchers[].group**：（*Optional*）要筛选的资源的组。
    - **resourceMatchers[].kind**：（*Optional*）要筛选的资源的类型。
    - **resourceMatchers[].version**：（*Optional*）要筛选的资源的版本。
    - **resourceMatchers[].names**：（可选）要过滤的资源的 Kubernetes metadata.name 字段中的名称。
    - **resourceMatchers[].namespaces**: (*Optional*) 要过滤的资源的 Kubernetes metadata.name 字段中的命名空间。
    - **resourceMatchers[].labelSelectors**: (*Optional*) 资源的 Kubernetes metadata.name 字段中的标签选择器字符串，如 "Kubernetes 文档" 中所定义。例如：`"trident.netapp.io/os=linux"`。

      例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 使用正确的值填充 `trident-protect-backup-restore-cr.yaml`文件后，应用 CR：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

将备份还原到原始命名空间

您可以随时将备份还原到原始命名空间。

开始之前

确保 AWS 会话令牌过期时间足以进行任何长期运行的 s3 还原操作。如果令牌在还原操作期间过期，则操作可能会失败。

- 有关检查当前会话令牌过期的详细信息，请参见 "AWS API 文档"。
- 有关 AWS 资源凭据的详细信息，请参见 "AWS IAM 文档"。

> 使用 Kopia 作为数据移动器还原备份时，可以选择在 CR 中指定注释，以控制 Kopia 使用的临时存储的行为。有关可以配置的选项的详细信息，请参见 "Kopia 文档"。

步骤

1. 创建自定义资源 (CR) 文件并将其命名为 `trident-protect-backup-ipr-cr.yaml`。
2. 在创建的文件中，配置以下属性：
   - **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
   - **spec.appArchivePath**：AppVault 中存储备份内容的路径。您可以使用以下命令查找此路径：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.appVaultRef**：（必需）存储备份内容的 AppVault 的名称。

  例如：

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appArchivePath: my-backup-path
  appVaultRef: appvault-name
```

3. （可选）如果需要仅选择要还原的应用程序的某些资源，请添加包含或排除标有特定标签的资源的筛选：

   Trident Protect 会自动选择一些资源，因为它们与您选择的资源之间存在关系。例如，如果您选择了永久卷声明资源，并且它具有关联的 pod，则 Trident Protect 也将还原关联的 pod。

   - **resourceFilter.resourceSelectionCriteria**：（筛选时需要）使用 `Include`或 `Exclude`来包含或排除在 resourceMatchers 中定义的资源。添加以下 resourceMatchers 参数以定义要包括或排除的资源：
     - **resourceFilter.resourceMatchers**：resourceMatcher 对象数组。如果在此数组中定义多个元素，则它们将作为 OR 操作进行匹配，并且每个元素（组、种类、版本）内的字段将作为 AND 操作进行匹配。
       - **resourceMatchers[].group**：（*Optional*）要筛选的资源的组。
       - **resourceMatchers[].kind**：（*Optional*）要筛选的资源的类型。
       - **resourceMatchers[].version**：（*Optional*）要筛选的资源的版本。
       - **resourceMatchers[].names**：（可选）要过滤的资源的 Kubernetes metadata.name 字段中的名称。
       - **resourceMatchers[].namespaces**: (*Optional*) 要过滤的资源的 Kubernetes metadata.name 字段中的命名空间。
       - **resourceMatchers[].labelSelectors**: (*Optional*) 资源的 Kubernetes metadata.name 字段中的标签选择器字符串，如 "Kubernetes 文档" 中所定义。例如：`"trident.netapp.io/os=linux"`。

         例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 使用正确的值填充 `trident-protect-backup-ipr-cr.yaml`文件后，应用 CR：

```
kubectl apply -f trident-protect-backup-ipr-cr.yaml
```

将备份还原到其他集群

如果原始群集出现问题，可以将备份还原到其他群集。

- 使用 Kopia 作为数据移动器还原备份时，可以选择在 CR 中指定注释，以控制 Kopia 使用的临时存储的行为。有关可以配置的选项的详细信息，请参见 "Kopia 文档"。
- 当使用 CR 还原到新的命名空间时，您必须在应用 CR 之前手动创建目标命名空间。

开始之前

确保满足以下先决条件：

- 目标集群已安装 Trident Protect。
- 目标集群可以访问与源集群相同的 AppVault 存储桶路径，备份存储在该路径中。
- 确保 AWS 会话令牌过期时间足以进行任何长期运行的还原操作。如果令牌在还原操作期间过期，则操作可能会失败。
  - 有关检查当前会话令牌过期的详细信息，请参见 "AWS API 文档"。
  - 有关 AWS 资源凭据的详细信息，请参见 "AWS 文档"。

步骤

1. 使用 Trident Protect CLI 插件检查目标集群上 AppVault CR 的可用性：

```
tridentctl-protect get appvault --context <destination_cluster_name>
```

确保目标集群上存在用于应用程序还原的命名空间。

2. 从目标集群查看可用的 AppVault 的备份内容：

```
tridentctl-protect get appvaultcontent <appvault_name> \
--show-resources backup \
--show-paths \
--context <destination_cluster_name>
```

运行此命令会显示 AppVault 中的可用备份，包括其原始群集、相应的应用程序名称、时间戳和存档路径。

输出示例：

```
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
|   CLUSTER   |    APP    |  TYPE  |      NAME       |         TIMESTAMP
|    PATH     |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
| production1 | wordpress | backup | wordpress-bkup-1| 2024-10-30
08:37:40 (UTC)| backuppath1 |
| production1 | wordpress | backup | wordpress-bkup-2| 2024-10-30
08:37:40 (UTC)| backuppath2 |
+-------------+-----------+--------+-----------------
+--------------------------+-------------+
```

3. 使用 AppVault 名称和存档路径将应用程序还原到目标集群：
4. 创建自定义资源 (CR) 文件并将其命名为 `trident-protect-backup-restore-cr.yaml`。
5. 在创建的文件中，配置以下属性：
   - **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
   - **spec.appVaultRef**：（必需）存储备份内容的 AppVault 的名称。
   - **spec.appArchivePath**：AppVault 中存储备份内容的路径。您可以使用以下命令查找此路径：

```
kubectl get backups <BACKUP_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

如果 BackupRestore CR 不可用，您可以使用步骤 2 中提到的命令查看备份内容。

- **spec.namespaceMapping**：还原操作的源命名空间到目标命名空间的映射。使用环境中的信息替换 `my-source-namespace`和 `my-destination-namespace`。

  例如：

```
apiVersion: protect.trident.netapp.io/v1
kind: BackupRestore
metadata:
  name: my-cr-name
  namespace: my-destination-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-backup-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

6. 使用正确的值填充 `trident-protect-backup-restore-cr.yaml`文件后，应用 CR：

```
kubectl apply -f trident-protect-backup-restore-cr.yaml
```

将快照还原到其他命名空间

您可以使用自定义资源 (CR) 文件将数据从快照还原到不同的命名空间或原始源命名空间。使用 SnapshotRestore CR 将快照还原到其他命名空间时，Backup and Recovery 会在新的命名空间中还原应用程序，并为还原的应用程序创建应用程序 CR。要保护还原的应用程序，请创建按需备份或快照，或建立保护计划。

- SnapshotRestore 支持 `spec.storageClassMapping`属性，但仅当源和目标存储类使用相同的存储后端时。如果尝试还原到使用不同存储后端的 `StorageClass`，还原操作将失败。
- 当使用 CR 还原到新的命名空间时，您必须在应用 CR 之前手动创建目标命名空间。

开始之前

确保 AWS 会话令牌过期时间足以进行任何长期运行的 s3 还原操作。如果令牌在还原操作期间过期，则操作可能会失败。

- 有关检查当前会话令牌过期的详细信息，请参见 "AWS API 文档"。
- 有关 AWS 资源凭据的详细信息，请参见 "AWS IAM 文档"。

步骤

1. 创建自定义资源 (CR) 文件并将其命名为 `trident-protect-snapshot-restore-cr.yaml`。
2. 在创建的文件中，配置以下属性：
   - **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
   - **spec.appVaultRef**：（必需）存储快照内容的 AppVault 的名称。

- **spec.appArchivePath**：AppVault 中存储快照内容的路径。您可以使用以下命令查找此路径：

```
kubectl get snapshots <SNAPHOT_NAME> -n my-app-namespace -o jsonpath
='{.status.appArchivePath}'
```

- **spec.namespaceMapping**：还原操作的源命名空间到目标命名空间的映射。使用环境中的信息替换 `my-source-namespace`和 `my-destination-namespace`。

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
  namespaceMapping: [{"source": "my-source-namespace", "destination":
"my-destination-namespace"}]
```

3. （可选）如果需要仅选择要还原的应用程序的某些资源，请添加包含或排除标有特定标签的资源的筛选：

> Trident Protect 会自动选择一些资源，因为它们与您选择的资源之间存在关系。例如，如果您选择了永久卷声明资源，并且它具有关联的 pod，则 Trident Protect 也将还原关联的 pod。

- **resourceFilter.resourceSelectionCriteria**：（筛选时需要）使用 `Include`或 `Exclude`来包含或排除在 resourceMatchers 中定义的资源。添加以下 resourceMatchers 参数以定义要包括或排除的资源：
  - **resourceFilter.resourceMatchers**：resourceMatcher 对象数组。如果在此数组中定义多个元素，则它们将作为 OR 操作进行匹配，并且每个元素（组、种类、版本）内的字段将作为 AND 操作进行匹配。
    - **resourceMatchers[].group**：（*Optional*）要筛选的资源的组。
    - **resourceMatchers[].kind**：（*Optional*）要筛选的资源的类型。
    - **resourceMatchers[].version**：（*Optional*）要筛选的资源的版本。
    - **resourceMatchers[].names**：（可选）要过滤的资源的 Kubernetes metadata.name 字段中的名称。
    - **resourceMatchers[].namespaces**: (*Optional*) 要过滤的资源的 Kubernetes metadata.name 字段中的命名空间。
    - **resourceMatchers[].labelSelectors**: (*Optional*) 资源的 Kubernetes metadata.name 字段中的标签选择器字符串，如 "Kubernetes 文档" 中所定义。例如：`"trident.netapp.io/os=linux"`。

      例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 使用正确的值填充 `trident-protect-snapshot-restore-cr.yaml`文件后，应用 CR：

```
kubectl apply -f trident-protect-snapshot-restore-cr.yaml
```

将快照还原到原始命名空间

您可以随时将快照还原到原始命名空间。

开始之前

确保 AWS 会话令牌过期时间足以进行任何长期运行的 s3 还原操作。如果令牌在还原操作期间过期，则操作可能会失败。

- 有关检查当前会话令牌过期的详细信息，请参见 "AWS API 文档"。
- 有关 AWS 资源凭据的详细信息，请参见 "AWS IAM 文档"。

步骤

1. 创建自定义资源 (CR) 文件并将其命名为 `trident-protect-snapshot-ipr-cr.yaml`。
2. 在创建的文件中，配置以下属性：
   - **metadata.name**：（*Required*）此自定义资源的名称；为您的环境选择一个唯一且合理的名称。
   - **spec.appVaultRef**：（必需）存储快照内容的 AppVault 的名称。
   - **spec.appArchivePath**：AppVault 中存储快照内容的路径。您可以使用以下命令查找此路径：

```
kubectl get snapshots <SNAPSHOT_NAME> -n my-app-namespace -o
jsonpath='{.status.appArchivePath}'
```

```
apiVersion: protect.trident.netapp.io/v1
kind: SnapshotInplaceRestore
metadata:
  name: my-cr-name
  namespace: my-app-namespace
spec:
  appVaultRef: appvault-name
  appArchivePath: my-snapshot-path
```

3. （可选）如果需要仅选择要还原的应用程序的某些资源，请添加包含或排除标有特定标签的资源的筛选：

   Trident Protect 会自动选择一些资源，因为它们与您选择的资源之间存在关系。例如，如果您选择了永久卷声明资源，并且它具有关联的 pod，则 Trident Protect 也将还原关联的 pod。

   - **resourceFilter.resourceSelectionCriteria**：（筛选时需要）使用 `Include`或 `Exclude`来包含或排除在 resourceMatchers 中定义的资源。添加以下 resourceMatchers 参数以定义要包括或排除的资源：
     - **resourceFilter.resourceMatchers**：resourceMatcher 对象数组。如果在此数组中定义多个元素，则它们将作为 OR 操作进行匹配，并且每个元素（组、种类、版本）内的字段将作为 AND 操作进行匹配。
       - **resourceMatchers[].group**：（*Optional*）要筛选的资源的组。
       - **resourceMatchers[].kind**：（*Optional*）要筛选的资源的类型。
       - **resourceMatchers[].version**：（*Optional*）要筛选的资源的版本。
       - **resourceMatchers[].names**：（可选）要过滤的资源的 Kubernetes metadata.name 字段中的名称。
       - **resourceMatchers[].namespaces**: (*Optional*) 要过滤的资源的 Kubernetes metadata.name 字段中的命名空间。
       - **resourceMatchers[].labelSelectors**: (*Optional*) 资源的 Kubernetes metadata.name 字段中的标签选择器字符串，如 "Kubernetes 文档" 中所定义。例如：`"trident.netapp.io/os=linux"`。

         例如：

```
spec:
  resourceFilter:
    resourceSelectionCriteria: "Include"
    resourceMatchers:
      - group: my-resource-group-1
        kind: my-resource-kind-1
        version: my-resource-version-1
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
      - group: my-resource-group-2
        kind: my-resource-kind-2
        version: my-resource-version-2
        names: ["my-resource-names"]
        namespaces: ["my-resource-namespaces"]
        labelSelectors: ["trident.netapp.io/os=linux"]
```

4. 使用正确的值填充 `trident-protect-snapshot-ipr-cr.yaml`文件后，应用 CR：

```
kubectl apply -f trident-protect-snapshot-ipr-cr.yaml
```

使用高级自定义资源还原设置

您可以使用高级设置（如注释、命名空间设置和存储选项）自定义还原操作，以满足您的特定要求。

还原和故障转移操作期间的命名空间注释和标签

在恢复和故障转移操作期间，目标命名空间中的标签和注释将与源命名空间中的标签和注释匹配。将添加目标命名空间中不存在的源命名空间中的标签或注释，并覆盖已存在的任何标签或注释，以匹配源命名空间中的值。仅存在于目标命名空间上的标签或注释保持不变。

> 如果使用 Red Hat OpenShift，请务必注意命名空间注释在 OpenShift 环境中的关键作用。命名空间注释可确保还原的 Pod 遵守 OpenShift 安全上下文约束 (SCC) 定义的适当权限和安全配置，并且可以访问卷而不会出现权限问题。有关详细信息，请参见 "OpenShift 安全上下文约束文档"。

在执行还原或故障转移操作之前，可以通过设置 Kubernetes 环境变量 `RESTORE_SKIP_NAMESPACE_ANNOTATIONS`来防止目标命名空间中的特定注释被覆盖。例如：

```
helm upgrade trident-protect -n trident-protect netapp-trident-
protect/trident-protect \
  --set-string
restoreSkipNamespaceAnnotations="{<annotation_key_to_skip_1>,<annotation_k
ey_to_skip_2>}" \
  --reuse-values
```

执行还原或故障切换操作时，在 `restoreSkipNamespaceAnnotations`和 `restoreSkipNamespaceLabels`中指定的任何命名空间批注和标签都将从还原或故障切换操作中排除。确保在初始 Helm 安装过程中配置了这些设置。要了解更多信息，请参阅"配置其他 Trident Protect helm 图表设置"。

如果使用带有 `--create-namespace` 标志的 Helm 安装源应用程序，则会对 `name` 标签键进行特殊处理。在还原或故障转移过程中，Trident Protect 会将此标签复制到目标命名空间，但如果来自源的值与源命名空间匹配，则将值更新为目标命名空间值。如果此值与源命名空间不匹配，则将其复制到目标命名空间，不进行任何更改。

示例

以下示例显示了源和目标命名空间，每个命名空间都有不同的注释和标签。您可以查看操作之前和之后的目标命名空间的状态，以及如何在目标命名空间中组合或覆盖注释和标签。

还原或故障转移操作之前

下表显示了还原或故障转移操作之前的示例源和目标命名空间的状态：

命名空间	标注	标签
命名空间 ns-1（源）	• annotation.one/key: "updatedvalue" • annotation.two/key: "true"	• environment=production • 合规性=hipaa • name=ns-1
命名空间 ns-2（目标）	• annotation.one/key: "true" • annotation.three/key: "false"	• 角色=数据库

还原操作后

下表显示了还原或故障转移操作后示例目标命名空间的状态。已添加一些键，一些键已被覆盖，并且已更新 `name` 标签以匹配目标命名空间：

命名空间	标注	标签
命名空间 ns-2（目标）	• annotation.one/key: "updatedvalue" • annotation.two/key: "true" • annotation.three/key: "false"	• name=ns-2 • 合规性=hipaa • environment=production • 角色=数据库

支持的字段

本节描述可用于还原操作的其他字段。

存储类映射

该 `spec.storageClassMapping` 属性定义从源应用程序中存在的存储类到目标集群上的新存储类的映射。您可以在具有不同存储类的集群之间迁移应用程序或更改 BackupRestore 操作的存储后端时使用此功能。

示例：

```
storageClassMapping:
  - destination: "destinationStorageClass1"
    source: "sourceStorageClass1"
  - destination: "destinationStorageClass2"
    source: "sourceStorageClass2"
```

支持的注释

本节列出了用于在系统中配置各种行为的支持注释。如果用户未明确设置注释，系统将使用默认值。

标注	类型	描述	默认值
protect.trident.netapp.io/data-mover-timeout-sec	string	允许数据移动器操作停止的最长时间（以秒为单位）。	"300"
protect.trident.netapp.io/kopia-content-cache-size-limit-mb	string	Kopia 内容缓存的最大大小限制（以兆字节为单位）。	"1000"
protect.trident.netapp.io/pvc-bind-timeout-sec	string	在操作失败之前，等待任何新创建的 PersistentVolumeClaims (PVC) 到达 `Bound`阶段的最长时间（以秒为单位）。适用于所有还原 CR 类型（BackupRestore、BackupInplaceRestore、SnapshotRestore、SnapshotInplaceRestore）。如果您的存储后端或集群通常需要更多时间，请使用更高的值。	"1200"（20 分钟）

管理 **Kubernetes** 集群

NetApp Backup and Recovery使您能够发现和管理 Kubernetes 集群，以便您可以保护集群托管的资源。

所需的**NetApp Console**角色

组织管理员或SnapCenter管理员。"了解NetApp Backup and Recovery访问角色" 。 "了解所有服务的NetApp Console访问角色" 。

要发现 Kubernetes 集群，请参阅"发现 Kubernetes 工作负载"。

编辑 **Kubernetes** 集群信息

如果需要更改集群名称，您可以编辑集群。

步骤

1. 在NetApp Backup and Recovery中，选择 **Inventory** > **Clusters**。
2. 在集群列表中，选择要编辑的集群并选择相关的操作菜单。
3. 选择*编辑集群*。
4. 对集群名称进行任何必要的更改。集群名称需要与您在发现过程中使用 Helm 命令的名称相匹配。
5. 选择*完成*。

删除 **Kubernetes** 集群

要停止保护 Kubernetes 集群，请禁用保护并删除相关应用程序，然后从NetApp Backup and Recovery中删除该集群。 NetApp Backup and Recovery不会删除集群或其资源；它只会从NetApp Console清单中删除集群。

步骤

1. 在NetApp Backup and Recovery中，选择 **Inventory** > **Clusters**。
2. 在集群列表中，选择要编辑的集群并选择相关的操作菜单。
3. 选择*删除集群*。
4. 查看确认对话框中的信息，然后选择*删除*。

管理 **Kubernetes** 应用程序

NetApp Backup and Recovery使您能够取消保护并删除 Kubernetes 应用程序及相关资源。

所需的**NetApp Console**角色

组织管理员或SnapCenter管理员。"了解NetApp Backup and Recovery访问角色" 。 "了解所有服务的NetApp Console访问角色" 。

取消保护 **Kubernetes** 应用程序

如果您不再需要保护某个应用程序，可以取消保护。当您取消保护应用程序时， NetApp Backup and Recovery会停止保护该应用程序，但保留所有相关的备份和快照。

当保护操作仍在运行时，您无法取消对应用程序的保护。要么等待操作完成，要么作为解决方法，删除还原点正在运行的保护操作正在使用的。然后，您可以取消对应用程序的保护。

步骤

1. 在NetApp Backup and Recovery中，选择 **Inventory**。
2. 选择一个 Kubernetes 实例，然后选择“查看”以查看与该实例关联的资源。
3. 选择“应用程序”选项卡。
4. 在应用程序列表中，选择要取消保护的应用程序并选择相关的操作菜单。
5. 选择*取消保护*。
6. 阅读通知，准备好后，选择*取消保护*。

删除 **Kubernetes** 应用程序

删除不再需要的应用程序。 NetApp Backup and Recovery停止保护并删除已删除应用程序的所有备份和快照。

步骤

1. 在NetApp Backup and Recovery中，选择 **Inventory**。
2. 选择一个 Kubernetes 实例，然后选择“查看”以查看与该实例关联的资源。
3. 选择“应用程序”选项卡。
4. 在应用程序列表中，选择要删除的应用程序并选择相关的操作菜单。
5. 选择*删除*。
6. 启用*删除快照和备份*以删除应用程序的所有快照和备份。

   您将无法再使用这些快照和备份恢复应用程序。

7. 确认操作并选择*删除*。

删除 **Kubernetes** 应用程序的还原点

如果需要取消对应用程序的保护，并且保护操作当前正在运行，则可能需要删除该应用程序的还原点。

步骤

1. 在 NetApp Backup and Recovery 菜单中，选择*恢复*。
2. 从列表中选择一个 Kubernetes 应用程序，并为该应用程序选择*查看和恢复*。

   出现还原点列表。

3. 选择需要删除的恢复点，然后选择操作图标 ••• > 删除恢复点 将其删除。

管理适用于 **Kubernetes** 工作负载的**NetApp Backup and Recovery**执行挂钩模板

执行钩子是一种自定义操作，它与托管 Kubernetes 应用程序中的数据保护操作一起运行。例如，通过使用执行挂钩在快照之前暂停数据库事务并在之后恢复它们来创建应用程

序一致的快照。创建执行钩子模板时，指定钩子类型、要运行的脚本以及目标容器的过滤器。使用模板将执行挂钩链接到您的应用程序。

NetApp Backup and Recovery 会在数据保护期间冻结和解冻应用程序的文件系统，例如 KubeVirt。您可以全局禁用此行为，也可以使用 Trident Protect 文档对特定应用程序禁用此行为：

- 要为所有应用程序禁用此行为，请参阅 "使用 KubeVirt 虚拟机保护数据"。
- 要针对特定应用程序禁用此行为，请参阅 "定义应用程序"。

所需的**NetApp Console**角色

组织管理员或SnapCenter管理员。"了解NetApp Backup and Recovery访问角色" 。 "了解所有服务的NetApp Console访问角色" 。

执行钩子的类型

NetApp Backup and Recovery根据运行时间支持以下类型的执行挂钩：

- 预快照
- 快照后
- 预备份
- 备份后
- 恢复后

执行顺序

当运行数据保护操作时，执行挂钩事件按以下顺序发生：

1. 任何适用的自定义预操作执行挂钩都在适当的容器上运行。您可以创建多个自定义预操作挂钩，但它们的执行顺序无法保证或配置。
2. 如果适用，则会发生文件系统冻结。
3. 执行数据保护操作。
4. 如果适用，冻结的文件系统将被解冻。
5. NetApp Backup and Recovery在适当的容器上运行任何适用的自定义操作前执行挂钩。您可以创建多个自定义后操作挂钩，但它们的执行顺序无法保证或配置。

如果创建多个相同类型的钩子，则无法保证它们的执行顺序。不同类型的钩子总是按照指定的顺序运行。例如，以下是具有所有不同类型钩子的配置的执行顺序：

1. 快照前钩子执行
2. 快照后钩子执行
3. 执行备份前挂钩
4. 执行备份后钩子

在生产中启用执行挂钩脚本之前对其进行测试。使用“kubectl exec”测试脚本，然后通过将应用程序克隆到临时命名空间并恢复来验证快照和备份。

如果快照前执行钩子添加、更改或删除 Kubernetes 资源，则这些更改将包含在快照或备份以及任何后续恢复操作中。

关于自定义执行钩子的重要说明

在为您的应用程序规划执行挂钩时，请考虑以下事项。

- 执行钩子必须使用脚本来执行操作。许多执行钩子可以引用同一个脚本。
- 执行钩子需要以可执行shell脚本的格式编写。
- 脚本大小限制为 96KB。
- 执行挂钩设置和任何匹配标准用于确定哪些挂钩适用于快照、备份或恢复操作。

执行挂钩可以减少或禁用应用程序功能。让您的自定义钩子尽快运行。如果您启动带有相关执行挂钩的备份或快照操作，但随后取消它，则如果备份或快照操作已经开始，则仍允许挂钩运行。这意味着备份后执行挂钩中使用的逻辑不能假定备份已完成。

执行钩子过滤器

当您为应用程序添加或编辑执行挂钩时，您可以向执行挂钩添加过滤器来管理该挂钩将匹配哪些容器。过滤器对于在所有容器上使用相同容器镜像但可能将每个镜像用于不同目的的应用程序（例如 Elasticsearch）很有用。过滤器允许您创建执行挂钩在某些（但不一定是所有）相同的容器上运行的场景。如果为单个执行挂钩创建多个过滤器，它们将通过逻辑 AND 运算符组合在一起。每个执行挂钩最多可以有 10 个活动过滤器。

添加到执行挂钩的每个过滤器都使用正则表达式来匹配集群中的容器。当钩子与容器匹配时，钩子将在该容器上运行其关联的脚本。过滤器的正则表达式使用正则表达式 2 (RE2) 语法，该语法不支持创建从匹配列表中排除容器的过滤器。有关NetApp Backup and Recovery在执行钩子过滤器中支持的正则表达式的语法的信息，请参见 "正则表达式 2 (RE2) 语法支持"。

如果将命名空间过滤器添加到在恢复或克隆操作后运行的执行挂钩，并且恢复或克隆源和目标位于不同的命名空间中，则命名空间过滤器仅适用于目标命名空间。

执行钩子示例

访问 "NetApp Verda GitHub 项目"下载流行应用程序（如 Apache Cassandra 和 Elasticsearch）的真实执行挂钩。您还可以查看示例并获得构建您自己的自定义执行挂钩的想法。

创建执行钩子模板

您可以创建自定义执行挂钩模板，用于在应用程序上执行数据保护操作之前或之后执行操作。

此处创建的模板仅在保护 Kubernetes 工作负载时可用。

步骤

1. 在控制台中，转到*保护*>*备份和恢复*。

2. 选择“设置”选项卡。
3. 展开*执行钩子模板*部分。
4. 选择*创建执行钩子模板*。
5. 输入执行挂钩的名称。
6. （可选）选择一种钩子类型。例如，还原后钩子会在还原操作完成后运行。
7. 在 **Script** 文本框中，输入要作为执行挂钩模板的一部分运行的可执行 shell 脚本。或者，您可以选择*上传脚本*来上传脚本文件。
8. 选择“创建”。

   创建模板后，它将出现在*执行挂钩模板*部分的模板列表中。

监控NetApp Backup and Recovery中的作业

使用NetApp Backup and Recovery，监控您启动的本地快照、复制和备份作业。跟踪您启动的恢复作业。查看已完成、正在进行或失败的作业以帮助诊断问题。在NetApp Console通知中心启用电子邮件通知，以便在未登录时随时了解系统活动。使用控制台时间线查看从 UI 或 API 启动的所有操作的详细信息。

NetApp Backup and Recovery会将作业信息保留 15 天，然后删除作业信息并将其从作业监视器中移除。

所需的**NetApp Console**角色 存储查看器、备份和恢复超级管理员、备份和恢复备份管理员、备份和恢复恢复管理员、备份和恢复克隆管理员或备份和恢复查看器角色。了解详情"备份和恢复角色和权限"。 "了解所有服务的NetApp Console访问角色" 。

在作业监视器上查看作业状态

您可以在“作业监控”选项卡中查看所有快照、复制、备份到对象存储和恢复操作的列表及其当前状态。这包括来自您的Cloud Volumes ONTAP、本地ONTAP、应用程序和虚拟机的操作。每个操作或作业都有唯一的 ID 和状态。

状态可以是：

- 成功
- 进行中
- 已排队
- 警告
- 失败

您从NetApp Backup and RecoveryUI 和 API 启动的快照、复制、对象存储备份和还原操作均可在“作业监控”选项卡中找到。

如果您已将ONTAP系统升级到 9.13.x，但在作业监视器中没有看到正在进行的计划备份操作，请重新启动NetApp Backup and Recovery。"了解如何重新启动NetApp Backup and Recovery"。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 监控。
2. 要显示其他列（系统、SVM、用户名、工作负载、策略名称、快照标签），请选择加号。

搜索并过滤职位列表

您可以使用多个筛选器在“作业监控”页面上筛选操作，例如策略、快照标签、操作类型（保护、恢复、保留或其他）和保护类型（本地快照、复制或备份到云）。

默认情况下，“作业监控”页面显示过去 24 小时的保护和恢复作业。您可以使用时间范围过滤器更改时间范围。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 监控。
2. 要对结果进行不同的排序，请选择每个列标题以按状态、开始时间、资源名称等进行排序。
3. 如果您正在寻找特定的工作，请选择“高级搜索和过滤”区域以打开“搜索”面板。

   使用此面板可以输入任何资源的自由文本搜索；例如“卷 1”或“应用程序 3”。您还可以根据下拉菜单中的项目过滤作业列表。

   大多数过滤器都是不言自明的。通过“工作量”过滤器，您可以查看以下类别的作业：

   - ONTAP卷（Cloud Volumes ONTAP和本地ONTAP卷）
   - Microsoft SQL Server
   - 虚拟机
   - Kubernetes

   - 仅当您首先选择了一个系统后，您才可以在特定的“SVM”中搜索数据。
   - 只有当您选择了“保护”的“类型”时，您才可以使用“保护类型”过滤器进行搜索。

4. 要立即更新页面，请选择  按钮。否则，此页面每 15 分钟刷新一次，以便您始终看到最新的工作状态结果。

查看职位详情

您可以查看与特定已完成作业相对应的详细信息。您可以以 JSON 格式导出特定作业的详细信息。

您可以查看作业类型（计划或按需）、 SnapMirror备份类型（初始或定期）、开始和结束时间、持续时间、从系统到对象存储的传输数据量、平均传输速率、策略名称、启用的保留锁、执行的勒索软件扫描、保护源详细信息和保护目标详细信息等详细信息。

恢复作业显示详细信息，例如备份目标提供商（Amazon Web Services、Microsoft Azure、Google Cloud、本地）、S3 存储桶名称、SVM 名称、源卷名称、目标卷、快照标签、恢复的对象数、文件名、文件大小、上次修改日期和完整文件路径。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 监控。
2. 选择作业的名称。

3. 选择“操作”菜单 ••• 并选择“查看详细信息”。
4. 展开每个部分以查看详细信息。

下载作业监控结果报告

您可以在过滤或排序结果后将主作业监控页面的内容下载为报告。NetApp Backup and Recovery会生成并下载一个 .CSV 文件，您可以根据需要查看该文件并发送给其他组。.CSV 文件包含最多 10,000 行数据。

从作业监控详细信息中，您可以下载包含单个作业详细信息的 JSON 文件。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 监控。
2. 要下载所有作业的 CSV 文件，请选择“下载”按钮并在下载目录中找到该文件。
3. 要下载单个作业的 JSON 文件，请选择“操作”菜单 ••• 对于该作业，选择*下载 JSON 文件*，然后在下载目录中找到该文件。

审查保留（备份生命周期）作业

监控保留（备份生命周期）流程以检查备份、确保其安全并支持审计。确定备份副本何时过期以跟踪生命周期。

备份生命周期作业跟踪所有已删除或正在排队等待删除的快照。从ONTAP 9.13 开始，您可以在“作业监控”页面上查看所有名为“保留”的作业类型。

“保留”作业类型捕获在受NetApp Backup and Recovery保护的卷上启动的所有快照删除作业。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 监控。
2. 选择“高级搜索和过滤”区域以打开搜索面板。
3. 选择“保留”作为工作类型。

在NetApp Console通知中心查看备份和恢复警报

NetApp Console通知中心跟踪您启动的备份和恢复作业的进度，以便您可以验证操作是否成功。

您可以在通知中心查看警报，并配置控制台以发送重要系统活动的电子邮件警报，即使您未登录。 "了解有关通知中心以及如何发送备份和恢复作业警报电子邮件的更多信息" 。

通知中心会显示大量的快照、复制、云备份和恢复事件，但只有某些事件会触发电子邮件警报：

操作类型	事件	已生成警报	电子邮件已发送
激活	系统备份和恢复激活失败	是	是
激活	系统备份和恢复编辑失败	是	是
激活	卷现在与快照策略关联	是	是
激活	卷备份或状态已修改	是	是
激活	系统备份和恢复激活成功	是	是

操作类型	事件	已生成警报	电子邮件已发送
激活	临时卷备份失败	是	是
激活	临时卷备份成功	是	否
激活	多卷备份失败	是	是
定时任务	检查是否缺少快照标签	是	是
定时任务	未能向ONTAP发送此系统的安全令牌	是	是
酒吧/订阅活动	连接失败	是	否
酒吧/订阅活动	删除计划快照失败	是	否
酒吧/订阅活动	卷的计划备份失败	是	否
酒吧/订阅活动	卷恢复成功	是	否
酒吧/订阅活动	卷恢复失败	是	否
勒索软件	在备份副本上发现潜在的勒索软件攻击	是	是
勒索软件	该系统的备份副本上检测到潜在的勒索软件攻击	是	是
本地快照	NetApp Backup and Recovery临时快照创建作业失败	是	是
复制	修改复制关系以克服容量故障	是	是
复制	NetApp Backup and Recovery临时复制作业失败	是	是
复制	NetApp Backup and Recovery复制暂停作业失败	是	否
复制	NetApp Backup and Recovery复制中断作业失败	是	否
复制	NetApp Backup and Recovery复制重新同步作业失败	是	否
复制	NetApp Backup and Recovery复制停止作业失败	是	否
复制	NetApp Backup and Recovery复制反向重新同步作业失败	是	是
复制	NetApp Backup and Recovery复制删除作业失败	是	是
目标行动	恢复到本地或云端目标故障	是	是
目标行动	按需恢复失败	是	是
系统操作	临时卷快照创建失败	是	是

从ONTAP 9.13.0 开始，所有警报都会出现在Cloud Volumes ONTAP和本地ONTAP系统中。对于具有Cloud Volumes ONTAP 9.13.0 和本地ONTAP 的系统，仅出现与“恢复作业已完成，但有警告”相关的警报。

默认情况下， NetApp Console组织和帐户管理员会收到所有“严重”和“建议”警报的电子邮件。默认情况下，系统不设置其他用户和收件人接收通知邮件。为NetApp云帐户中的任何控制台用户或需要了解备份和恢复活动的其他收件人配置电子邮件警报。

要接收NetApp Backup and Recovery电子邮件警报，您需要在通知设置页面中选择通知严重性类型“严重”、“警告”和“错误”。

"了解如何发送备份和恢复作业的警报电子邮件"。

步骤

1. 从控制台菜单中，选择（  ）。
2. 查看通知。

在控制台时间线中查看操作活动

您可以在控制台时间线中查看备份和恢复操作的详细信息以供进一步调查。控制台时间线提供每个事件的详细信息，无论是用户发起的还是系统发起的，并显示在 UI 中或通过 API 发起的操作。

"了解时间轴和通知中心之间的区别"。

重新启动NetApp Backup and Recovery

在某些情况下，您可能需要重新启动NetApp Backup and Recovery。

控制台代理包括NetApp Backup and Recovery功能。

步骤

1. 连接到控制台代理正在运行的 Linux 系统。

控制台代理位置	操作步骤
云部署	按照说明进行操作 "连接到控制台代理 Linux 虚拟机"取决于您使用的云提供商。
手动安装	登录Linux系统。

2. 输入命令重启服务。

控制台代理位置	**Docker** 命令	**Podman** 命令
云部署	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
手动安装（需联网）	`docker restart cloudmanager_cbs`	`podman restart cloudmanager_cbs`
无需互联网访问即可手动安装	`docker restart ds_cloudmanager_cbs_1`	`podman restart ds_cloudmanager_cbs_1`