



# 开始使用

## NetApp Backup and Recovery

NetApp  
February 13, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/data-services-backup-recovery/concept-backup-to-cloud.html> on February 13, 2026. Always check docs.netapp.com for the latest.

# 目录

|                                                      |    |
|------------------------------------------------------|----|
| 开始使用                                                 | 1  |
| 了解NetApp Backup and Recovery                         | 1  |
| NetApp Backup and Recovery                           | 1  |
| 使用NetApp Backup and Recovery的优势                      | 2  |
| 成本                                                   | 3  |
| 许可                                                   | 4  |
| 支持的工作负载、系统和备份目标                                      | 4  |
| NetApp Backup and Recovery的工作原理                      | 5  |
| 可能对您使用NetApp Backup and Recovery有帮助的术语               | 6  |
| NetApp Backup and Recovery前提条件                       | 7  |
| ONTAP 9.8 及更高版本的先决条件                                 | 7  |
| 备份到对象存储的先决条件                                         | 7  |
| 保护 Microsoft SQL Server 工作负载的要求                      | 7  |
| 保护 VMware 工作负载的要求                                    | 8  |
| 保护 KVM 工作负载的要求                                       | 8  |
| 保护 Oracle Database 工作负载的要求                           | 9  |
| 保护 Kubernetes 应用程序的要求                                | 9  |
| 保护 Hyper-V 工作负载的要求                                   | 10 |
| 在NetApp Console中                                     | 11 |
| 设置NetApp Backup and Recovery 的许可                     | 11 |
| 30天免费试用                                              | 12 |
| 使用NetApp Backup and Recovery PAYGO 订阅                | 12 |
| 使用年度合同                                               | 13 |
| 使用NetApp Backup and RecoveryBYOL 许可证                 | 14 |
| 超出许可证容量                                              | 14 |
| 在NetApp Backup and Recovery中为StorageGRID和ONTAP设置安全证书 | 14 |
| 为StorageGRID创建安全证书                                   | 14 |
| 为ONTAP创建安全证书                                         | 18 |
| 为ONTAP和StorageGRID创建证书                               | 21 |
| 在使用NetApp Backup and Recovery之前设置备份目标                | 22 |
| 准备备份目标                                               | 22 |
| 设置 S3 权限                                             | 23 |
| 登录NetApp Backup and Recovery                         | 25 |
| 在NetApp Backup and Recovery中发现异地备份目标                 | 25 |
| 发现备份目标                                               | 25 |
| 为备份目标添加存储桶                                           | 27 |
| 更改备份目标的凭据                                            | 28 |
| 切换到不同的NetApp Backup and Recovery工作负载                 | 28 |
| 切换到不同的工作负载                                           | 28 |

|                                                 |    |
|-------------------------------------------------|----|
| 配置NetApp Backup and Recovery设置 .....            | 29 |
| 为主机资源添加凭据 .....                                 | 29 |
| 维护 VMware vCenter 设置 .....                      | 31 |
| 导入和管理SnapCenter主机资源 .....                       | 31 |
| 添加 KVM 管理平台 .....                               | 33 |
| 在 Windows 主机的快照中配置日志目录 .....                    | 33 |
| 创建执行钩子模板 .....                                  | 33 |
| 在 NetApp Backup and Recovery 中设置基于角色的访问控制 ..... | 34 |
| 相关信息 .....                                      | 35 |

# 开始使用

## 了解NetApp Backup and Recovery

NetApp Backup and Recovery是一种数据服务，可为您的所有ONTAP工作负载（包括卷、数据库、虚拟机和 Kubernetes 工作负载）提供高效、安全且经济高效的数据保护。

所有ONTAP系统都已内置对备份和恢复的支持，因此无需额外的硬件、软件许可证或媒体网关。这使得备份操作变得简单且经济高效。NetApp Console简化了任何备份策略的实施，包括所有 3-2-1 备份变体，而无需多个资源管理器或专业人员。



有关保护 VMware、KVM、Hyper-V 和 Kubernetes 工作负载的文档以技术预览的形式提供。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。

## NetApp Backup and Recovery

使用NetApp Backup and Recovery实现以下目标：

- \* ONTAP卷工作负载\*：
  - 创建本地快照，复制到二级存储，并将ONTAP卷从本地ONTAP或Cloud Volumes ONTAP系统备份到公共或私有云帐户中的对象存储。
  - 创建块级、增量永久备份，并将其存储在另一个ONTAP集群和云中的对象存储中。
  - 将NetApp Backup and Recovery与SnapCenter一起使用。
  - 参考["保护ONTAP卷"](#)。
- **Microsoft SQL Server** 工作负载：
  - 从本地ONTAP、Cloud Volumes ONTAP或Amazon FSx for NetApp ONTAP备份 Microsoft SQL Server 实例和数据库。
  - 还原 Microsoft SQL Server 数据库。
  - 克隆 Microsoft SQL Server 数据库。
  - 不使用SnapCenter即可使用NetApp Backup and Recovery。
  - 参考["保护 Microsoft SQL Server 工作负载"](#)。
- VMware 工作负载（使用新 UI 预览，无需SnapCenter Plug-in for VMware vSphere）\*：
  - 使用NetApp Backup and Recovery保护您的 VMware VM 和数据存储。
  - 将 VMware 工作负载备份到 Amazon Web Services S3 或StorageGRID（预览版）。
  - 将 VMware 数据从云端恢复到本地 vCenter。
  - 您可以将虚拟机恢复到与备份完全相同的位置或其他位置。
  - 使用NetApp Backup and Recovery，无需SnapCenter Plug-in for VMware vSphere。
  - 参考["保护 VMware 工作负载"](#)。
- VMware 工作负载（使用SnapCenter Plug-in for VMware vSphere）

- 将虚拟机和数据存储备份到 Amazon Web Services S3、Microsoft Azure Blob、Google Cloud Platform 和 StorageGRID，并将虚拟机还原回 SnapCenter Plug-in for VMware vSphere。
- 使用 NetApp Backup and Recovery 将虚拟机数据从云恢复到本地 vCenter。您可以将虚拟机恢复到与备份完全相同的位置或其他位置。
- 将 NetApp Backup and Recovery 与适用于 SnapCenter Plug-in for VMware vSphere 一起使用。
- 参考["保护 VMware 工作负载"](#)。
- KVM 工作负载（预览版）
  - 备份和还原虚拟机
  - 备份 KVM 存储池
  - 使用保护组管理备份任务
  - 参考["保护 KVM 工作负载"](#)。
- Hyper-V 工作负载（预览版）
  - 备份和还原虚拟机
  - 使用保护组管理备份任务
  - 参考["保护 Hyper-V 工作负载"](#)。
- **Oracle Database** 工作负载（预览）：
  - 备份和恢复数据库和日志
  - 使用保护组管理备份任务
  - 创建策略来管理数据库和日志备份
  - 使用 3-2-1 备份架构保护数据库
  - 配置备份保留
  - 挂载和卸载 ARCHIVELOG 备份
  - 请参见 ["保护 Oracle Database 工作负载"](#)。
- Kubernetes 工作负载（预览版）
  - 在一个地方管理和保护您的 Kubernetes 应用程序和资源。
  - 使用保护策略来构建增量备份。
  - 将应用程序和资源恢复到相同或不同的集群和命名空间。
  - 不使用 SnapCenter 即可使用 NetApp Backup and Recovery。
  - 参考["保护 Kubernetes 工作负载"](#)。

## 使用 NetApp Backup and Recovery 的优势

NetApp Backup and Recovery 具有以下优势：

- **高效：** NetApp Backup and Recovery 执行块级、永久增量复制，从而显著减少复制和存储的数据量。这有助于最大限度地减少网络流量和存储成本。
- **安全：** NetApp Backup and Recovery 对传输中和静止的数据进行加密，并使用安全通信协议来保护您的数据。

- 经济高效： NetApp Backup and Recovery使用您的云帐户中可用的成本最低的存储层，有助于降低成本。
- 自动化： NetApp Backup and Recovery根据预定义的计划自动生成备份，这有助于确保您的数据受到保护。
- 灵活： NetApp Backup and Recovery使您能够将数据恢复到相同或不同的系统，从而为数据恢复提供了灵活性。

## 成本

NetApp不会向您收取试用版的使用费用。但是，您需要承担与您使用的云资源相关的费用，例如存储和数据传输费用。

使用NetApp Backup and Recovery与ONTAP系统的备份到对象功能会产生两种类型的成本：

- 资源费用
- 服务费

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

对于ONTAP卷工作负载，您只需为受对象存储保护的卷付费。费用是根据源ONTAP卷在应用效率之前所使用的逻辑容量计算的，也称为前端 TB（FETB）。

对于 Kubernetes 工作负载，将根据所有永久卷的总大小向您收费。

对于所有其他工作负载，您需要为至少保护到一个辅助存储目标或对象存储目标的资源付费。费用是根据源工作负载的逻辑大小计算的。对于数据库而言，这意味着数据库的大小；对于虚拟机而言，这意味着虚拟机的大小。

备份和恢复服务有三种付费方式：

- 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。
- 第二种选择是购买年度合同。
- 第三种选择是直接从NetApp购买许可证。请参阅 [许可](#) 详情请见相关章节。

## 许可

NetApp Backup and Recovery提供免费试用，允许您在限定时间内无需许可证密钥即可使用。

只有涉及对象存储的备份和恢复操作才需要备份许可证。创建快照和复制卷不需要许可证。

您可以从三种授权选项中进行选择：

- 自带许可证 (**BYOL**)：从NetApp购买基于期限（1 年、2 年或 3 年）和容量（以 1-TiB 为增量）的许可证。在NetApp Console中输入提供的序列号进行激活。该许可证涵盖您组织中的所有源系统。当期限或容量达到限制时，需要续约。
- 按需付费 (**PAYGO**)：通过云服务提供商的市场订阅，并按备份数据的 GiB 数量付费，按月计费。无需预付任何费用。首次注册即可享受 30 天免费试用。更多信息，请参阅 ["使用NetApp Backup and Recovery按需付费订阅"](#)。
- 年度合同：可通过 AWS 和 Azure Marketplace 购买，期限为 1 年、2 年或 3 年。现有两份年度合同可供选择：
  - 云备份：备份Cloud Volumes ONTAP和本地ONTAP数据。
  - **CVO** 专业版：捆绑了Cloud Volumes ONTAP和NetApp Backup and Recovery，Cloud Volumes ONTAP卷可进行无限备份（备份容量不计入许可证）。
    - CVO 专业版计划包含两种收费方式：
      - 资源费用：根据存储使用情况而定。更多信息，请参阅 ["Cloud Volumes ONTAP的许可"](#)。
      - 服务费用：NetApp Backup and Recovery费用。但是，如果源卷位于使用 CVO 专业计划的存储系统中，则NetApp Backup and Recovery是免费提供的。

当您使用 Google Cloud Platform 时，请向NetApp申请私有报价，并在 Google Cloud Marketplace 激活时选择您的套餐。

["了解如何设置许可证"](#)。

## 支持的工作负载、系统和备份目标

支持的工作负载

NetApp Backup and Recovery可保护以下类型的工作负载：

- ONTAP卷
- 存储在物理磁盘和 VMware 虚拟机磁盘 (VMDK) 上的 Microsoft SQL Server 实例和数据库，通过 VMFS 或 NFS 文件系统进行存储。
- VMware 虚拟机和数据存储区
- KVM 工作负载（预览）

- Hyper-V 工作负载（预览版）
- Oracle 数据库工作负载（预览版）
- Kubernetes 工作负载（预览版）

#### 支持的系统

- 本地部署的ONTAP SAN（iSCSI 协议）和 NAS（使用 NFS 和 CIFS 协议），ONTAP版本需为 9.8 或更高版本。
- 适用于 AWS 的Cloud Volumes ONTAP 9.8 或更高版本（使用 SAN 和 NAS）
- 适用于 Google Cloud Platform 的Cloud Volumes ONTAP 9.8 或更高版本（使用 NFS 和 CIFS 协议）
- 适用于 Microsoft Azure 的Cloud Volumes ONTAP 9.8 或更高版本（使用 SAN 和 NAS）
- Amazon FSx for NetApp ONTAP（仅限 Microsoft SQL Server 工作负载）

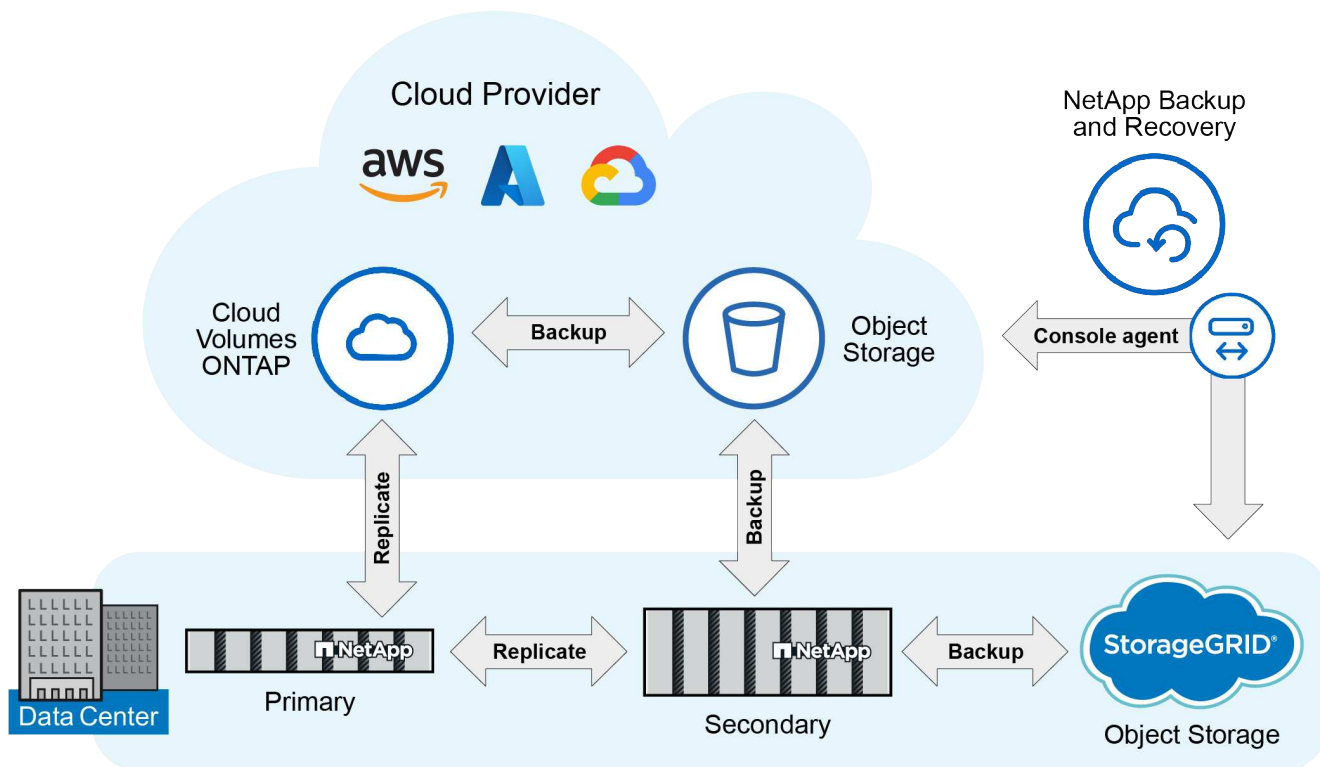
#### 支持的备份目标

- 亚马逊网络服务（AWS）S3
- Google Cloud Storage
- Microsoft Azure Blob（预览版不适用于 VMware 工作负载）
- StorageGRID
- ONTAP S3（预览版不适用于 VMware 工作负载）

## NetApp Backup and Recovery的工作原理

当您启用NetApp Backup and Recovery，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备份。这使得网络流量保持最低限度。

下图显示了组件之间的关系。



还支持从主存储到对象存储，而不仅仅是从二级存储到对象存储。

## 备份在对象存储位置的位置

备份副本存储在NetApp Console在您的云帐户中创建的对象存储中。每个集群或系统都有一个对象存储，控制台按如下方式命名该对象存储：netapp-backup-clusteruuid。请确保不要删除此对象存储。

- 在 AWS 中，NetApp Console可以实现以下功能：["Amazon S3 阻止公共访问功能"](#)在 S3 铲斗上。
- 在 Azure 中，NetApp Console使用包含 Blob 容器存储帐户的新建或现有资源组。["阻止公众访问您的 Blob 数据"](#)默认情况下。
- 在StorageGRID中，控制台使用现有的存储帐户作为对象存储桶。
- 在ONTAP S3 中，控制台使用 S3 存储桶的现有用户帐户。

## 备份副本与您的NetApp Console组织相关联

备份副本与控制台代理所在的NetApp Console组织相关联。["了解NetApp Console身份和访问"](#)。

如果同一个NetApp Console组织中有多个控制台代理，则每个控制台代理都会显示相同的备份列表。

## 可能对您使用NetApp Backup and Recovery有帮助的术语

了解一些与保护相关的术语可能会对您有所帮助。

- **保护**：NetApp Backup and Recovery中的保护意味着确保使用保护策略定期将快照和不可变备份发送到不同的安全域。

- 工作负载： NetApp Backup and Recovery中的工作负载可以包括ONTAP卷、Microsoft SQL Server 实例和数据库；VMware VM 和数据存储区；或 Kubernetes 集群和应用程序。

## NetApp Backup and Recovery前提条件

通过验证操作环境、 NetApp Console代理和NetApp Console帐户的准备情况，开始使用NetApp Backup and Recovery 。要使用NetApp Backup and Recovery，您需要满足这些先决条件。

### ONTAP 9.8 及更高版本的先决条件

必须在本地ONTAP实例上启用ONTAP One 许可证。

### 备份到对象存储的先决条件

要使用对象存储作为备份目标，您需要一个具有 AWS S3、Microsoft Azure Blob、 StorageGRID或ONTAP 的帐户并配置适当的访问权限。

- ["保护您的ONTAP卷数据"](#)

### 保护 Microsoft SQL Server 工作负载的要求

要将NetApp Backup and Recovery用于 Microsoft SQL Server 工作负载，您需要满足以下主机系统、空间和大  
小调整前提条件。

| 物品                         | 要求                                                                                                                                                                                                                                                                                         |
|----------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 操作系统                       | Microsoft Windows 有关受支持版本的最新信息，请参阅 <a href="#">"NetApp 互操作性表工具"</a> 。                                                                                                                                                                                                                      |
| Microsoft SQL Server 版本    | VMware 虚拟机文件系统 (VMFS) 和 VMware 虚拟机磁盘 (VMDK) NFS 支持 2012 及更高版本。                                                                                                                                                                                                                             |
| SnapCenter服务器版本            | <p>如果要将现有数据从SnapCenter导入NetApp Backup and Recovery ， 则需要SnapCenter Server 5.0 或更高版本。</p> <div>  <p>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。看"<a href="#">从SnapCenter导入资源的先决条件</a>"。</p> </div> |
| SQL Server 主机上插件的最小 RAM    | 1 GB                                                                                                                                                                                                                                                                                       |
| SQL Server 主机上插件的最小安装和日志空间 | <p>5 GB</p> <p>分配足够的磁盘空间并监控日志文件夹的存储消耗。所需的日志空间取决于执行的备份次数和数据保护操作的频率。如果没有足够的空间，则不会为操作创建日志。</p>                                                                                                                                                                                                |

| 物品     | 要求                                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 所需的软件包 | <ul style="list-style-type: none"> <li>• ASP.NET Core Runtime 8.0.12 托管包（以及所有后续 8.0.x 补丁）</li> <li>• PowerShell 7.4.2</li> </ul> <p>有关受支持版本的最新信息，请参阅 <a href="#">"NetApp 互操作性表工具"</a>。</p> |

## 保护 VMware 工作负载的要求

您需要特定的要求来发现和保护您的 VMware 工作负载。

### 软件支持

- 支持 NFS 和 VMFS 数据存储区。
- 支持的 NFS 版本：NFS 3 和 NFS 4.1
- 支持的 VMware ESXi Server 版本：7.0U1 及以上
- 支持的 VMware vCenter vSphere 版本：7.0U1 及以上
- IP 地址：IPv4 和 IPv6
- VMware TLS：1.2、1.3
- 支持的连接存储：ONTAP 9.13 或更高版本

### 保护 VMware 工作负载的连接和端口要求

| 端口类型              | 预配置端口                                                        |
|-------------------|--------------------------------------------------------------|
| VMware ESXi 服务器端口 | 443 (HTTPS)，双向。来宾文件恢复功能使用此端口。                                |
| 存储集群或存储虚拟机端口      | 443 (HTTPS)，双向。80 (HTTP)，双向。此端口用于虚拟设备与存储虚拟机或包含存储虚拟机的集群之间的通信。 |

### 保护 VMware 工作负载的基于角色的访问控制 (RBAC) 要求

vCenter 管理员帐户必须具有所需的 vCenter 权限。

有关所需 vCenter 权限的列表，请参阅 ["SnapCenter Plug-in for VMware vSphere vCenter 权限"](#)。

## 保护 KVM 工作负载的要求

您需要特定的要求来发现和保护 KVM 虚拟机。

- 运行内核版本 5.14.0-503.22.1.el9\_5.x86\_64（长期）或更高版本的现代 Linux 发行版
- 您的 KVM 主机和虚拟机必须由管理平台进行管理。NetApp Backup and Recovery 支持以下管理平台：
  - Apache CloudStack 4.22.0.0
- 确保允许从控制台代理到 KVM 主机的入站网络流量到达端口 22。

- QEMU Guest Agent 版本 9.0.0 或更高版本
- libvirt 版本 10.5.0 或更高版本



为确保 KVM 工作负载恢复成功完成，请确保在用于 KVM 备份的保护策略中启用“启用 VM 一致性快照”设置。

要启用对非 root 用户管理的 KVM 虚拟机的保护，请按以下步骤操作：

1. 将卷挂载为 NFS3 类型，以避免使用 nobody 用户和组。
2. 使用以下命令将非root用户添加到 qemu 在保留现有群体的同时，组建新的群体：

```
usermod -aG qemu <non-root-user>
```



3. 使用以下命令将挂载路径的所有权授予..... qemu 用户和组，并更改挂载路径的权限：

```
chown -R qemu:qemu <kvm_vm_mount_path> & chmod 771  
<kvm_vm_mount_path>
```

4. 如果存在 NetApp\_SnapCenter\_Backups 目录，请将其删除。

## 保护 Oracle Database 工作负载的要求

确保您的环境满足发现和保护 Oracle 资源的特定要求。

- Oracle 数据库：
  - Oracle 19C 和 21C 在独立部署中受支持。
  - Oracle 数据库必须部署在主或辅助NetApp ONTAP存储中。
  - 主机操作系统支持：Red Hat Enterprise Linux 8 和 9
- 对象存储支持：
  - Azure 对象存储
  - 亚马逊 AWS
  - NetAppStorageGRID
  - ONTAP S3

## 保护 Kubernetes 应用程序的要求

您需要特定的要求来发现 Kubernetes 资源并保护您的 Kubernetes 应用程序。

有关NetApp Console要求，请参阅[在NetApp Console中](#)。

- 主ONTAP系统（ONTAP 9.16.1 或更高版本）

- Kubernetes 集群 - 支持的 Kubernetes 发行版和版本包括：
  - Anthos On-Prem (VMware) 和 Anthos on Bare Metal 1.16
  - Kubernetes 1.27 - 1.33
  - OpenShift 4.10 - 4.18
  - Rancher Kubernetes Engine 2 (RKE2) v1.26.7+rke2r1、v1.28.5+rke2r1
  - Suse Rancher
- NetApp Trident 24.10 或更高版本
- NetApp Trident Protect 25.07 或更高版本（在 Kubernetes 工作负载发现期间安装）
- NetApp Trident Protect Connector 25.07 或更高版本（在 Kubernetes 工作负载发现期间安装）
  - 确保 TCP 端口 443 在 Kubernetes 集群、Trident Protect Connector 和 Trident Protect 代理之间的出站方向上未过滤。

## 保护 Hyper-V 工作负载的要求

确保您的 Hyper-V 实例满足发现和保护虚拟机的特定要求。

- Hyper-V Windows Server 主机的软件要求：
  - Microsoft Hyper-V 2019、2022 和 2025 版本
  - ASP.NET Core Runtime 8.0.12 托管包（以及所有后续 8.0.x 补丁）
  - PowerShell 7.4.2 或更高版本
  - 如果非管理员域用户要保护 Hyper-V 虚拟机，请确保该用户拥有以下权限：
    - 请确保该用户是本地管理员组成员。
    - 确保用户已加入“以服务身份登录”本地安全策略。
  - 确保 Windows 防火墙设置中允许以下端口进行双向 HTTPS 通信：
    - 8144（适用于 Hyper-V 的 NetApp 插件）
    - 8145（适用于 Windows 的 NetApp 插件）
- Hyper-V 主机的硬件要求：
  - 支持独立主机和 FCI 集群主机
  - Hyper-V 主机上的 NetApp Hyper-V 插件至少需要 1GB RAM
  - Hyper-V 主机上插件的最低安装和日志空间为 5GB



确保在 Hyper-V 主机上为日志文件夹分配足够的磁盘空间并定期监控其使用情况。所需空间取决于备份和数据保护操作发生的频率。如果空间不足，则不会生成日志。

- NetApp ONTAP 配置要求：
  - 主 ONTAP 系统（ONTAP 9.14.1 或更高版本）
  - 对于使用 CIFS 共享存储虚拟机数据的 Hyper-V 部署，请确保在 ONTAP 系统上启用了连续可用性共享属性。请参阅 ["ONTAP 文档"](#) 以获取说明。

## 在NetApp Console中

确保NetApp Console满足以下要求。

- 控制台用户应具有对 Microsoft SQL Server 和 Kubernetes 工作负载执行操作所需的角色和权限。要发现资源，您必须具有NetApp Backup and Recovery超级管理员角色。看["NetApp Backup and Recovery基于角色的功能访问"](#)有关在NetApp Backup and Recovery中执行操作所需的角色和权限的详细信息。
- 具有至少一个活动控制台代理的控制台组织，该代理连接到本地ONTAP集群或Cloud Volumes ONTAP。
- 至少一个具有NetApp本地ONTAP或Cloud Volumes ONTAP集群的控制台系统。
- 控制台代理

参考 ["了解如何配置控制台代理"](#)和 ["标准NetApp Console要求"](#)。

- 预览版需要 Ubuntu 22.04 LTS 操作系统作为控制台代理。

## 设置NetApp Console

下一步是设置控制台和NetApp Backup and Recovery。

审查 ["标准NetApp Console要求"](#)。

### 创建控制台代理

您应该联系您的NetApp产品团队来尝试备份和恢复。然后，当您使用控制台代理时，它将包含适合该服务的功能。

要在使用服务之前在NetApp Console中创建控制台代理，请参阅描述 ["如何创建控制台代理"](#)。

### 控制台代理的安装位置

要完成还原操作，可以在以下位置安装控制台代理：

- 对于 Amazon S3，控制台代理可以部署在您的场所。
- 对于 Azure Blob，可以在您的场所部署控制台代理。
- 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



“本地ONTAP系统”包括FAS和AFF系统。

## 设置NetApp Backup and Recovery 的许可

您可以通过从云提供商处购买按使用量付费 (PAYGO) 或年度市场订阅 \* NetApp Intelligent Services\* 来获得NetApp Backup and Recovery许可，或者通过从NetApp购买自带许可 (BYOL)。需要有效的许可证才能在系统上激活NetApp Backup and Recovery、创建生产数据的备份以及将备份数据还原到生产系统。

在您继续阅读之前，请注意以下几点：

- 如果您已经在云提供商的市场中订阅了Cloud Volumes ONTAP系统的即用即付 (PAYGO) 订阅，那么您也会自动订阅NetApp Backup and Recovery。您无需再次订阅。
- NetApp Backup and Recovery自带许可证 (BYOL) 是一种浮动许可证，您可以在与NetApp Console组织或帐户关联的所有系统中使用它。因此，如果您现有的 BYOL 许可证具有足够的备份容量，则无需购买另一个 BYOL 许可证。
- 如果您使用 BYOL 许可证，建议您也订阅 PAYGO 订阅。如果您备份的数据超出了 BYOL 许可证允许的范围，或者许可证期限已过期，则备份将通过您的即用即付订阅继续进行 - 不会中断服务。
- 将本地ONTAP数据备份到StorageGRID时，您需要 BYOL 许可证，但云提供商存储空间无需付费。

["了解有关使用NetApp Backup and Recovery 的成本的更多信息。"](#)

## 30天免费试用

如果您在云提供商的市场中注册按使用量付费订阅 \* NetApp Intelligent Services\*，则可以获得NetApp Backup and Recovery 30 天免费试用。免费试用从您订阅市场列表时开始。请注意，如果您在部署Cloud Volumes ONTAP系统时支付市场订阅费用，然后在 10 天后开始NetApp Backup and Recovery免费试用，那么您将有 20 天的剩余时间来使用免费试用版。

免费试用结束后，您将自动切换到 PAYGO 订阅，不会中断。如果您决定不再继续使用NetApp Backup and Recovery，只需["从系统中取消注册NetApp Backup and Recovery"](#)在试用期结束前，您将不会被收费。

### 结束免费试用

如果您想在免费试用结束后继续使用NetApp Backup and Recovery，则必须设置付费订阅。您可以从NetApp Console界面导航到计费部分并选择适合您需求的订阅计划来执行此操作。如果您不想继续使用NetApp Backup and Recovery，您可以结束免费试用。

当您结束免费试用而未订阅付费计划时，您的数据将在免费试用结束后 60 天自动删除。您可以选择让系统立即删除您的数据。

### 步骤

1. 从NetApp Backup and Recovery登录页面，选择 查看免费试用版。
2. 选择\*结束免费试用\*。
3. 选择“免费试用结束后立即删除数据”以立即删除您的数据。
4. 在框中输入\*结束试用\*。
5. 选择\*结束\*进行确认。

## 使用NetApp Backup and Recovery PAYGO 订阅

对于即用即付，您将在单个订阅中按小时向云提供商支付对象存储成本和NetApp备份许可成本。即使您有免费试用版或自带许可证 (BYOL)，也应该在 Marketplace 中订阅 \* NetApp Intelligent Services\*：

- 订阅可确保免费试用结束后服务不会中断。试用期结束后，我们将根据您备份的数据量按小时向您收费。
- 如果您备份的数据超出了 BYOL 许可证允许的范围，则数据备份和恢复操作将通过即用即付订阅继续进行。例如，如果您拥有 10 TiB BYOL 许可证，则超过 10 TiB 的所有容量都将通过 PAYGO 订阅收费。

在免费试用期间或未超出 BYOL 许可证的情况下，您无需支付即用即付订阅费用。

NetApp Backup and Recovery有几种 PAYGO 计划：

- “云备份”包使您能够备份Cloud Volumes ONTAP数据和本地ONTAP数据。
- “CVO Professional” 软件包使您能够捆绑Cloud Volumes ONTAP和NetApp Backup and Recovery。这包括使用许可证对Cloud Volumes ONTAP系统进行无限制备份（备份容量不计入许可容量）。此选项不允许您备份本地ONTAP数据。

请注意，此选项还需要备份和恢复 PAYGO 订阅，但符合条件的Cloud Volumes ONTAP系统不会产生任何费用。

["了解有关这些基于容量的许可证包的更多信息"](#)。

使用这些链接从您的云提供商市场订阅NetApp Backup and Recovery：

- AWS：["前往NetApp Intelligent Services市场了解定价详情"](#)。
- Azure：["前往NetApp Intelligent Services市场了解定价详情"](#)。
- Google Cloud：["前往NetApp Intelligent Services市场了解定价详情"](#)。

## 使用年度合同

通过购买年度合同每年支付NetApp Backup and Recovery的费用。期限分为 1 年、2 年或 3 年。

如果您与市场签订了年度合同，则所有NetApp Backup and Recovery消费均根据该合同收费。您不能将年度市场合同与 BYOL 混合搭配。

当您使用 AWS 时，有两种年度合同可供选择 ["AWS Marketplace 页面"](#)对于Cloud Volumes ONTAP和本地ONTAP系统：

- “云备份”计划使您能够备份Cloud Volumes ONTAP数据和本地ONTAP数据。

如果您想使用此选项，请从 Marketplace 页面设置您的订阅，然后 ["将订阅与您的 AWS 凭证关联"](#)。请注意，您还需要使用此年度合同订阅来支付您的Cloud Volumes ONTAP系统的费用，因为您只能在控制台中为您的 AWS 凭证分配一个有效订阅。

- “CVO Professional”计划使您能够捆绑Cloud Volumes ONTAP和NetApp Backup and Recovery。这包括使用许可证对Cloud Volumes ONTAP系统进行无限制备份（备份容量不计入许可容量）。此选项不允许您备份本地ONTAP数据。

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

如果您想使用此选项，可以在创建Cloud Volumes ONTAP系统时设置年度合同，控制台会提示您订阅 AWS Marketplace。

使用 Azure 时，有两份年度合同可供选择 ["Azure 市场页面"](#)对于Cloud Volumes ONTAP和本地ONTAP系统：

- “云备份”计划使您能够备份Cloud Volumes ONTAP数据和本地ONTAP数据。

如果您想使用此选项，请从 Marketplace 页面设置您的订阅，然后 ["将订阅与您的 Azure 凭据关联"](#)。请注意，您还需要使用此年度合同订阅来支付您的Cloud Volumes ONTAP系统的费用，因为您只能在控制台中为您的 Azure 凭据分配一个有效订阅。

- “CVO Professional”计划使您能够捆绑Cloud Volumes ONTAP和NetApp Backup and Recovery。这包括使用许可证对Cloud Volumes ONTAP系统进行无限制备份（备份容量不计入许可容量）。此选项不允许您备份本地ONTAP数据。

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

如果您想使用此选项，可以在创建Cloud Volumes ONTAP系统时设置年度合同，控制台会提示您订阅 Azure Marketplace。

当您使用 GCP 时，请联系您的NetApp销售代表购买年度合同。该合同在 Google Cloud Marketplace 中以私人优惠形式提供。

NetApp向您提供专属优惠后，您可以在激活NetApp Backup and Recovery时通过 Google Cloud Marketplace 订阅并选择年度计划。

## 使用NetApp Backup and RecoveryBYOL 许可证

NetApp提供的自带许可证的有效期为 1 年、2 年或 3 年。您只需为您保护的数据付费，该费用根据正在备份的源ONTAP卷的逻辑使用容量（任何效率之前）计算。此容量也称为前端兆字节 (FETB)。

BYOL NetApp Backup and Recovery许可证是一种浮动许可证，其总容量在与您的NetApp Console组织或帐户关联的所有系统之间共享。对于ONTAP系统，您可以通过运行 CLI 命令粗略估计所需的容量 ``volume show -fields logical-used-by-afs`` 对于您计划备份的卷。

如果您没有NetApp Backup and Recovery BYOL 许可证，请单击控制台右下角的聊天图标购买。

或者，如果您拥有未分配的基于节点的Cloud Volumes ONTAP许可证但不会使用，则可以将其转换为具有相同美元等值和相同到期日期的NetApp Backup and Recovery许可证。 ["点击此处了解详情"](#)。

您可以使用NetApp Console来管理 BYOL 许可证。您可以从控制台添加新许可证、更新现有许可证以及查看许可证状态。

["了解如何添加许可证"](#)。

## 超出许可证容量

超过许可容量会触发 PAYGO 费率；如果没有 PAYGO 订阅，您将无法创建新的备份，尽管现有备份在没有服务保障的情况下仍可恢复。请务必在许可证过期之前续订许可证；过期的许可证会阻止新的备份并中断服务。

## 在NetApp Backup and Recovery中为StorageGRID和ONTAP设置安全证书

创建安全证书以启用NetApp Backup and Recovery与StorageGRID或ONTAP之间的通信。

### 为StorageGRID创建安全证书

如果NetApp Backup and Recovery容器与StorageGRID之间的通信应该验证StorageGRID证书，则完成以下步骤。

生成的证书应具有 CN 和主题备用名称，作为激活备份时NetApp Backup and Recovery中提供的名称。

#### 步骤

1. 按照StorageGRID文档中的步骤创建StorageGRID证书。

["有关配置证书的StorageGRID信息"](#)

2. 如果您尚未更新StorageGRID，请使用证书进行更新。
3. 以 root 用户身份登录控制台代理。运行：

```
sudo su
```

4. 获取NetApp Backup and Recovery (Cloud Backup Service) Docker 卷。运行：

```
docker volume ls | grep cbs
```

输出示例：

```
local service-manager-2_cloudmanager_cbs_volume"
```



标准、私有和受限部署模式的卷名称不同。本示例使用标准模式。参考 ["NetApp Console部署模式"](#)。

5. 找到NetApp Backup and Recovery卷的挂载点。运行：

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep Mountpoint
```

输出示例：

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data"
```



标准、私有和受限部署模式的挂载点有所不同。此示例展示了标准云部署。参考 ["NetApp Console部署模式"](#)。

6. 更改为 MountPoint 目录。运行：

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

7. 如果 StorageGRID 的证书由根 CA 和中间 CA 签名，则附加 `pem` 将两个文件合并到一个名为 `sgws.crt` 在当前位置。不要将叶证书添加到此文件。

## cloudmanager\_cbs 容器的步骤

您需要在 NetApp Backup and Recovery (Cloud Backup Service) 中启用 StorageGRID 服务器证书验证。

1. 将目录更改为前面步骤中获得的 Docker 卷。

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

2. 将目录更改为配置目录。

```
cd cbs_config
```

3. 根据您的部署环境，创建并保存如下所示的配置文件，并使用以下名称之一：

- `production-customer.json` 用于标准模式和限制模式部署。
- `darksite-customer.json` 用于私人模式部署。

参考 ["NetApp Console 部署模式"](#)。

配置文件

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  }
}
```

4. 退出容器。运行：

```
exit
```

5. 重启 cloudmanager\_cbs。运行：

```
docker restart cloudmanager_cbs
```

### cloudmanager\_cbs\_catalog 容器的步骤

接下来，您需要为编目服务启用StorageGRID服务器证书验证。

1. 将目录更改为 Docker 卷：

```
cd /var/lib/docker/volumes/service-manager-  
2_cloudmanager_cbs_volume/_data
```

2. 配置目录。运行：

```
cd cbs_catalog_config
```

3. 根据您的部署环境，使用以下名称之一创建如下所示的配置文件：

- `production-customer.json` 用于标准模式和限制模式部署。
- `darksite-customer.json` 用于私人模式部署。

参考 ["NetApp Console部署模式"](#)。

目录配置文件

```
{  
  "protocols": {  
    "sgws": {  
      "certificates": {  
        "reject-unauthorized": true,  
        "ca-bundle": "/config/sgws.crt"  
      }  
    }  
  }  
}
```

4. 重新启动目录。运行：

```
docker restart cloudmanager_cbs_catalog
```

根据代理操作系统使用**StorageGRID**证书更新控制台代理证书

## Ubuntu

1. 将 SGWS 证书复制到 /usr/local/share/ca-certificates。以下是一个例子：

```
cp /config/sgws.crt /usr/local/share/ca-certificates/
```

在哪里 `sgws.crt` 是根 CA 证书。

2. 使用StorageGRID证书更新主机证书。运行

```
sudo update-ca-certificates
```

## Red Hat Enterprise Linux

1. 将 SGWS 证书复制到 /etc/pki/ca-trust/source/anchors/。

```
cp /config/sgws.crt /etc/pki/ca-trust/source/anchors/
```

在哪里 `sgws.crt` 是根 CA 证书。

2. 使用StorageGRID证书更新主机证书。

```
update-ca-trust extract
```

3. 更新 ca-bundle.crt

```
cd /etc/pki/tls/certs/  
openssl x509 -in ca-bundle.crt -text -noout
```

4. 要检查证书是否存在，请运行以下命令：

```
openssl crl2pkcs7 -nocrl -certfile /etc/pki/tls/certs/ca-bundle.crt |  
openssl pkcs7 -print_certs | grep subject | head
```

## 为ONTAP创建安全证书

如果NetApp Backup and Recovery容器与ONTAP之间的通信应验证ONTAP证书，则完成以下步骤。

NetApp Backup and Recovery使用 Cluster Management IP 连接到ONTAP。在证书的主题备用名称中输入集群

的 IP 地址。使用系统管理器 UI 生成 CSR 时指定此步骤。

使用系统管理器文档为ONTAP创建新的 CA 证书。

- ["使用系统管理器管理证书"](#)
- ["如何使用 System Manager 管理ONTAP SSL 证书"](#)

步骤

1. 以 root 身份登录控制台代理。运行：

```
sudo su
```

2. 获取NetApp Backup and RecoveryDocker 卷。运行：

```
docker volume ls | grep cbs
```

输出示例：

```
local service-manager-2_cloudmanager_cbs_volume
```



标准、私有和受限部署模式的卷名称不同。此示例展示了标准云部署。参考 ["NetApp Console部署模式"](#)。

3. 获取卷的挂载。运行：

```
docker volume inspect service-manager-2_cloudmanager_cbs_volume | grep Mountpoint
```

输出示例：

```
"Mountpoint": "/var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```



标准、私有和受限部署模式的挂载点有所不同。此示例展示了标准云部署。参考 ["NetApp Console部署模式"](#)。

4. 更改为挂载点目录。运行：

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

## 5. 完成以下步骤之一：

- 如果ONTAP证书由根 CA 和中间 CA 签名，则附加 `pem` 将两个文件合并到一个名为 `ontap.crt` 在当前位置。
- 如果ONTAP证书由单个 CA 签名，则重命名 `pem` 文件为 `ontap.crt` 并将其复制到当前位置。不要将叶证书添加到此文件。

## cloudmanager\_cbs 容器的步骤

接下来，在NetApp Backup and Recovery（Cloud Backup Service）中启用ONTAP服务器证书验证。

### 1. 将目录更改为前面步骤中获得的 Docker 卷。

```
cd /var/lib/docker/volumes/service-manager-2_cloudmanager_cbs_volume/_data
```

### 2. 切换到配置目录。运行：

```
cd cbs_config
```

### 3. 根据您的部署环境，创建一个如下所示的配置文件，并使用以下名称之一：

- `production-customer.json` 用于标准模式和限制模式部署。
- `darksite-customer.json` 用于私人模式部署。

参考 ["NetApp Console部署模式"](#)。

配置文件

```
{
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

### 4. 退出容器。运行：

```
exit
```

### 5. 重新启动NetApp Backup and Recovery。运行：

```
docker restart cloudmanager_cbs
```

## cloudmanager\_cbs\_catalog 容器的步骤

为编目服务启用ONTAP服务器证书验证。

1. 将目录更改为 Docker 卷。运行：

```
cd /var/lib/docker/volumes/service-manager-  
2_cloudmanager_cbs_volume/_data
```

2. 运行：

```
cd cbs_catalog_config
```

3. 根据您的部署环境，创建一个如下所示的配置文件，并使用以下名称之一：

- `production-customer.json` 用于标准模式和限制模式部署。
- `darksite-customer.json` 用于私人模式部署。

参考 ["NetApp Console部署模式"](#)。

配置文件

```
{  
  "ontap": {  
    "certificates": {  
      "reject-unauthorized": true,  
      "ca-bundle": "/config/ontap.crt"  
    }  
  }  
}
```

4. 重新启动NetApp Backup and Recovery。运行：

```
docker restart cloudmanager_cbs_catalog
```

## 为ONTAP和StorageGRID创建证书

如果您需要为ONTAP和StorageGRID启用证书，则配置文件如下所示：

```
{
  "protocols": {
    "sgws": {
      "certificates": {
        "reject-unauthorized": true,
        "ca-bundle": "/config/sgws.crt"
      }
    }
  },
  "ontap": {
    "certificates": {
      "reject-unauthorized": true,
      "ca-bundle": "/config/ontap.crt"
    }
  }
}
```

## 在使用NetApp Backup and Recovery之前设置备份目标

在使用NetApp Backup and Recovery之前，请执行几个步骤来设置备份目标。

在开始之前，请查看["前提条件"](#)以确保您的环境已准备就绪。

### 准备备份目标

准备以下一个或多个备份目标：

- NetAppStorageGRID。

参考 ["了解StorageGRID"](#)。

参考 ["StorageGRID文档"](#)有关StorageGRID的详细信息。

- 亚马逊网络服务。参考 ["Amazon S3 文档"](#)。

执行以下操作以准备将 AWS 作为备份目标：

- 在 AWS 中设置一个帐户。
- 在 AWS 中配置 S3 权限，列于下一部分。
- 有关在控制台中管理 AWS 存储的详细信息，请参阅 ["管理您的 Amazon S3 存储桶"](#)。

- 微软 Azure。
  - 参考 ["Azure NetApp Files文档"](#)。
  - 在 Azure 中设置一个帐户。

- 配置 ["Azure 权限"](#)在 Azure 中。
- 有关在控制台中管理 Azure 存储的详细信息，请参阅 ["管理 Azure 存储帐户"](#)。

在备份目标本身中配置选项后，您稍后会将其配置为NetApp Backup and Recovery中的备份目标。有关如何在NetApp Backup and Recovery中配置备份目标的详细信息，请参阅["发现备份目标"](#)。

## 设置 S3 权限

您需要配置两组 AWS S3 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"
    }
  ]
}

```

# 登录NetApp Backup and Recovery

您可以使用NetApp Console登录到NetApp Backup and Recovery。

NetApp Backup and Recovery使用身份和访问管理来控制每个用户可以做什么。

有关每个角色可以执行的操作的详细信息，请参阅["NetApp Backup and Recovery用户角色"](#)。

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

所需的**NetApp Console**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"](#)。

要添加控制台代理，您必须具有备份和恢复超级管理员角色。

## 步骤

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

出现NetApp Console登录页面。

2. 登录控制台。

3. 从控制台左侧导航中，选择\*保护\*>\*备份和恢复\*。

- 如果您是第一次登录备份和恢复，并且还没有将系统添加到“系统”页面，则备份和恢复将显示“欢迎使用新的NetApp Backup and Recovery”登录页面，并提供添加系统的选项。有关向“系统”页面添加系统的详细信息，请参阅 ["NetApp Console标准模式入门"](#)。
- 如果您是第一次登录备份和恢复，并且在控制台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。

4. 如果您还没有这样做，请选择\*发现和管理\*选项。

- 对于 Microsoft SQL Server 工作负载，请参阅["发现 Microsoft SQL Server 工作负载"](#)。
- 对于 VMware 工作负载，请参阅["发现 VMware 工作负载"](#)。
- 对于 KVM 工作负载，请参阅["发现 KVM 工作负载"](#)。
- 对于 Oracle Database 工作负载，请参阅 ["发现 Oracle Database 工作负载"](#)。
- 对于 Hyper-V 工作负载，请参阅["发现 Hyper-V 工作负载"](#)。
- 对于 Kubernetes 工作负载，请参阅["发现 Kubernetes 工作负载"](#)。

## 在NetApp Backup and Recovery中发现异地备份目标

完成几个步骤即可在NetApp Backup and Recovery中发现或手动添加异地备份目标。

### 发现备份目标

在使用NetApp Backup and Recovery之前，请配置您的备份目标（Amazon Web Services (AWS) S3、Microsoft Azure Blob Storage、Google Cloud Storage 或StorageGRID）。

您可以自动发现这些目标或手动添加它们。

提供访问存储帐户的凭据。 NetApp Backup and Recovery使用这些凭据来发现您想要备份的工作负载。

开始之前

您需要先发现至少一个工作负载，然后才能添加异地备份目标。

步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择\*异地备份目标\*选项卡。
3. 选择\*发现备份目标\*。
4. 选择以下备份目标类型之一：**Amazon Web Services (AWS) S3**、**Microsoft Azure Blob Storage**、\***StorageGRID**\* 或 \***ONTAP S3**\*。
5. 在“选择凭证位置”部分中，选择凭证所在的位置，然后选择如何关联凭证。
6. 选择“下一步”。
7. 输入凭据信息。根据您选择的备份目标类型和凭据位置，信息会有所不同。
  - 对于 AWS：
    - 凭证名称：输入 AWS 凭证名称。
    - 访问密钥：输入 AWS 密钥。
    - 密钥：输入 AWS 密钥。
  - 对于 Azure：
    - 凭据名称：输入 Azure Blob 存储凭据名称。
    - 客户端密钥：输入 Azure Blob 存储客户端密钥。
    - 应用程序（客户端）ID：选择 Azure Blob 存储应用程序 ID。
    - 目录租户 ID：输入 Azure Blob 存储租户 ID。
  - 对于StorageGRID：
    - 凭证名称：输入StorageGRID凭证名称。
    - 网关节点 **FQDN**：输入StorageGRID的 FQDN 名称。
    - 端口：输入StorageGRID的端口号。
    - 访问密钥：输入StorageGRID S3 访问密钥。
    - 密钥：输入StorageGRID S3 密钥。
  - 对于ONTAP S3：
    - 凭证名称：输入ONTAP S3 凭证名称。
    - 网关节点 **FQDN**：输入ONTAP S3 的 FQDN 名称。
    - 端口：输入ONTAP S3 的端口号。
    - 访问密钥：输入ONTAP S3 访问密钥。
    - 密钥：输入ONTAP S3 密钥。

## 8. 选择\*发现\*。

### 为备份目标添加存储桶

您可以手动将存储桶添加到异地备份目标，而不是让NetApp Backup and Recovery自动发现存储桶。

#### 步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择\*异地备份目标\*。
3. 选择目标，然后在右侧选择“操作”  图标并选择\*添加存储桶\*。
4. 输入存储桶信息。根据您选择的备份目标类型，信息会有所不同。
  - 对于 AWS：
    - 存储桶名称：输入 S3 存储桶的名称。“netapp-backup”前缀是必需的前缀，会自动添加到您提供的名称中。
    - **AWS** 账户：输入 AWS 账户名称。
    - 存储桶区域：输入存储桶的 AWS 区域。
    - 启用 **S3** 对象锁：选择此选项可为存储桶启用 S3 对象锁。S3 对象锁可防止在指定的保留期内删除或覆盖对象，从而提供额外的数据保护层。您只能在创建存储桶时启用此功能，并且以后无法将其关闭。
      - 治理模式：选择此选项可为 S3 对象锁定存储桶启用治理模式。治理模式使您能够保护对象不被大多数用户删除或覆盖，但允许某些用户更改保留设置。
      - 合规模式：选择此选项可为 S3 对象锁定存储桶启用合规模式。合规模式可防止任何用户（包括根用户）在保留期到期之前更改保留设置或删除对象。
    - 版本控制：选择此选项可为 S3 存储桶启用版本控制。版本控制使您能够在存储桶中保留对象的多个版本，这对于备份和恢复目的很有用。
    - 标签：选择 S3 存储桶的标签。标签是可用于组织和管理 S3 资源的键值对。
    - 加密：选择 S3 存储桶的加密类型。选项是 AWS S3 管理密钥或 AWS 密钥管理服务密钥。如果您选择 AWS Key Management Service 密钥，则必须提供密钥 ID。
  - 对于 Azure：
    - 订阅：选择 Azure Blob 存储容器的名称。
    - 资源组：选择 Azure 资源组的名称。
    - 实例详情：
      - 存储帐户名称：输入 Azure Blob 存储容器的名称。
      - **Azure** 区域：输入容器的 Azure 区域。
      - 性能类型：为 Azure Blob 存储容器选择标准或高级性能类型，以指示所需的性能级别。
      - 加密：选择 Azure Blob 存储容器的加密类型。选项包括 Microsoft 管理的密钥或客户管理的密钥。如果选择客户管理的密钥，则必须提供密钥保管库名称和密钥名称。
  - 对于StorageGRID：
    - 备份目标名称：选择StorageGRID桶的名称。

- 存储桶名称：输入StorageGRID桶的名称。
  - 区域：输入存储桶的StorageGRID区域。
  - 启用版本控制：选择此选项可为StorageGRID桶启用版本控制。版本控制使您能够在存储桶中保留对象的多个版本，这对于备份和恢复目的很有用。
  - 对象锁定：选择此选项可为StorageGRID桶启用对象锁定。对象锁定可防止对象在指定的保留期内被删除或覆盖，从而提供额外的数据保护层。您只能在创建存储桶时启用此功能，并且以后无法将其关闭。
  - 容量：输入StorageGRID桶的容量。这是存储桶中可以存储的最大数据量。
- 对于ONTAP S3：
- 备份目标名称：选择ONTAP S3 存储桶的名称。
  - 存储桶目标名称：输入ONTAP S3 存储桶的名称。
  - 容量：输入ONTAP S3 存储桶的容量。这是存储桶中可以存储的最大数据量。
  - 启用版本控制：选择此选项可为ONTAP S3 存储桶启用版本控制。版本控制使您能够在存储桶中保留对象的多个版本，这对于备份和恢复目的很有用。
  - 对象锁定：选择此选项可为ONTAP S3 存储桶启用对象锁定。对象锁定可防止对象在指定的保留期内被删除或覆盖，从而提供额外的数据保护层。您只能在创建存储桶时启用此功能，并且以后无法将其关闭。

5. 选择“添加”。

## 更改备份目标的凭据

输入访问备份目标所需的凭据。

### 步骤

1. 从NetApp Backup and Recovery菜单中，选择 **Inventory**。
2. 选择\*异地备份目标\*。
3. 选择目标，然后在右侧选择“操作”  图标并选择\*更改凭据\*。
4. 输入备份目标的新凭据。根据您选择的备份目标类型，信息会有所不同。
5. 选择\*完成\*。

## 切换到不同的NetApp Backup and Recovery工作负载

您可以在不同的NetApp Backup and Recovery工作负载之间切换。

### 切换到不同的工作负载

您可以在NetApp Backup and RecoveryUI 中切换到不同的工作负载。

### 步骤

1. 从控制台左侧导航中，选择\*保护\*>\*备份和恢复\*。
2. 从页面右上角，选择\*切换工作负载\*下拉列表。

3. 选择您想要切换到工作负载。

页面刷新并显示所选的工作负载。

## 配置NetApp Backup and Recovery设置

设置NetApp Console后，配置备份和恢复设置。添加主机资源的凭据、导入SnapCenter资源、配置日志目录以及设置 VMware vCenter 设置。在备份或恢复数据之前完成这些步骤。

- [\[为主机资源添加凭据\]](#) 适用于NetApp Backup and Recovery需要进行身份验证的任何 Windows、Microsoft SQL Server、Oracle Database 或 Linux 主机。这包括恢复访客文件或文件夹时使用的 Windows 访客操作系统凭据。
- [维护 VMware vCenter 设置。](#)
- [导入和管理SnapCenter主机资源。](#)（仅限 Microsoft SQL Server 工作负载）
- [添加 KVM 管理平台。](#)（仅限 KVM 工作负载）
- [在 Windows 主机的快照中配置日志目录。](#)
- [\[创建执行钩子模板\]](#) 在备份作业之前和之后运行脚本。（仅限 Kubernetes 工作负载）

所需的**NetApp Console**角色 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。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"](#)。

### 为主机资源添加凭据

添加主机资源凭据。NetApp Backup and Recovery使用这些凭据来发现工作负载并应用备份策略。

如果您没有凭据，请创建具有访问和管理主机工作负载的权限的凭据。

您需要配置以下类型的凭据：

- Microsoft SQL Server 凭据
- SnapCenter Windows 主机凭据
- 恢复客户机文件或文件夹时使用的 Windows 客户机操作系统凭据
- Oracle 数据库凭据
- Linux 主机凭据

#### 步骤

1. 从NetApp Backup and Recovery菜单中，选择 设置。
2. 选择“凭证”的向下箭头。
3. 选择\*添加新凭证\*。
4. 请输入登录凭证信息。根据您选择的身份验证模式，会显示不同的字段。将鼠标悬停在信息 i 图标上，可查看有关字段的更多信息。
  - 凭证名称：输入凭证的名称。

- 身份验证模式：选择 **Windows**、**Microsoft SQL**、**Oracle Database** 或 **Linux**。



对于 Microsoft SQL Server 工作负载，您需要输入 Windows 和 Microsoft SQL Server 的凭据，因此您需要添加两组凭据。

#### **Windows**

i. 如果您选择了 **Windows**：

- 代理：从列表选择一个控制台代理。
- 域和用户名：输入凭据的 NetBIOS 或域 FQDN 和用户名。
- 密码：输入凭证的密码。

#### **Microsoft SQL Server**

i. 如果您选择了 **Microsoft SQL Server**：

- 域和用户名：输入凭据的 NetBIOS 或域 FQDN 和用户名。
- 密码：输入凭证的密码。
- 主机：选择已发现的 SQL Server 主机地址。
- **SQL Server 实例**：选择已发现的 SQL Server 实例。

#### **Oracle 数据库**

i. 如果您选择了\*Oracle数据库\*：

- 代理：从列表选择一个控制台代理。
- 用户名：请输入用于登录凭据的用户名。
- 密码：输入凭证的密码。

#### **Linux**

i. 如果您选择了 **Linux**：

- 代理：从列表选择一个控制台代理。
- 用户名：请输入用于登录凭据的用户名。
- 密码：输入凭证的密码。

#### 5. 选择“添加”。

#### 编辑主机资源的凭据

您之后可以编辑您创建的任何凭据的密码。

#### 步骤

1. 从NetApp Backup and Recovery菜单中，选择 设置。
2. 选择向下箭头以展开“**Credentials**”部分。
3. 选择“操作”图标 ...> 编辑凭证。

- 密码：输入凭证的密码。

#### 4. 选择\*保存\*。

## 维护 VMware vCenter 设置

提供 VMware vCenter 凭据来发现要备份的工作负载。如果您没有凭据，请创建具有访问和管理 VMware vCenter Server 工作负载的权限的凭据。

### 步骤

1. 从NetApp Backup and Recovery菜单中，选择 设置。
2. 选择向下箭头以展开 **VMware vCenter** 部分。
3. 选择“添加 vCenter”。
4. 输入 VMware vCenter Server 信息。
  - **vCenter FQDN 或 IP 地址**：输入 VMware vCenter Server 的 FQDN 名称或 IP 地址。
  - **用户名\*和密码**：输入 VMware vCenter Server 的用户名和密码。
  - **端口**：输入 VMware vCenter Server 的端口号。
  - **协议**：选择\*HTTP\*或\*HTTPS\*。
5. 选择“添加”。

## 导入和管理SnapCenter主机资源

如果您之前使用SnapCenter备份资源，则可以在NetApp Backup and Recovery中导入和管理这些资源。此选项使您能够导入SnapCenter服务器信息以注册多个SnapCenter服务器并发现数据库工作负载。

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不会接管保护管理。为此，您必须明确选择在NetApp Backup and Recovery中管理这些资源。

### 步骤

1. 从NetApp Backup and Recovery菜单中，选择 设置。
2. 选择向下箭头以展开“从SnapCenter导入”部分。
3. 选择\*从SnapCenter导入\*以导入SnapCenter资源。
4. 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。
5. 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。输入凭证名称。
  - 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。
6. 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。

## 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。在您选择管理这些导入的资源后，NetApp Backup and Recovery可以备份和恢复您从SnapCenter导入的资源。您不再需要在SnapCenter Server 中管理这些资源。

## 步骤

1. 导入SnapCenter资源后，在出现的“清单”页面上，选择您导入的、希望从现在开始由NetApp Backup and Recovery管理的SnapCenter资源。
2. 选择“操作”图标 > 管理 管理资源。
3. 选择“在NetApp Console中管理”\*。

清单页面在主机名下显示 **Managed**，表示所选主机资源现在由NetApp Backup and Recovery管理。

## 编辑导入的SnapCenter资源

您稍后可以重新导入SnapCenter资源或编辑导入的SnapCenter资源以更新注册详细信息。

您只能更改SnapCenter服务器的端口和密码详细信息。

## 步骤

1. 从NetApp Backup and Recovery菜单中，选择 设置。
2. 选择“从SnapCenter导入”的向下箭头。

从SnapCenter导入页面显示所有以前的导入。

3. 选择“操作”图标 > \*编辑\*以更新资源。
4. 根据需要更新SnapCenter密码和端口详细信息。
5. 选择\*导入\*。

## 添加 KVM 管理平台

如果您使用 Apache CloudStack 管理平台来管理 KVM 资源，则需要将其与 NetApp Backup and Recovery 集成，以便 Backup and Recovery 可以发现和保护受管 KVM 主机和虚拟机。

### 步骤

1. 从 NetApp Backup and Recovery 菜单中，选择 **设置**。
2. 选择向下箭头展开“管理平台”部分。
3. 选择“添加管理平台凭证”。
4. 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。
5. 完成后，选择“添加”。

## 在 Windows 主机的快照中配置日志目录

在为 Windows 主机创建策略之前，您应该为 Windows 主机配置快照中的日志目录。日志目录用于存储备份过程中生成的日志。

### 步骤

1. 从 NetApp Backup and Recovery 菜单中，选择 **Inventory**。
2. 在清单页面中，选择一個工作负载，然后选择操作图标  > \*查看详情\* 显示工作量详情。
3. 从显示 Microsoft SQL Server 的库存详细信息页面中，选择“主机”选项卡。
4. 在清单详细信息页面中，选择一个主机并选择操作图标  > 配置日志目录。
5. 浏览或输入日志目录的路径。
6. 选择\*保存\*。

## 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。

## 在 NetApp Backup and Recovery 中设置基于角色的访问控制

若要提高安全性并控制资源访问，请为 NetApp Backup and Recovery 配置基于角色的访问。NetApp Console 支持某些 Backup and Recovery 工作负载的基于角色的访问控制 (RBAC)。您可以为这些工作负载指定特定的管理员或查看者角色。在支持项目级关联之前，具有 Backup and Recovery 角色的所有用户仍可访问尚未支持基于角色的访问控制的其他工作负载。

按照下面的步骤控制对组织中资源的访问。在 NetApp Console 菜单的\*管理 > 身份和访问\*页面中进行更改。



这些步骤假设您在 Console 中被分配了组织管理员角色。

### 步骤

1. 创建身份和访问项目结构。

作为组织管理员，设置工作负载所在的 Identity and access 文件夹和项目结构。

2. 分配用户角色。

- a. 主要选项：

将用户添加到指定用于工作负载的每个项目，并授予他们适当的角色。例如：

- 组织管理员\*和 \***Backup and Recovery** 超级管理员：具有这些角色的用户可以查看所有组织中的所有资源，并发现 Backup and Recovery 工作负载并将其分配给项目（例如，US East 或 US West）。
- 文件夹或项目管理员\*和 \***Backup and Recovery** 超级管理员：具有这些角色的用户只能查看其具有权限的文件夹或项目中的资源，但可以发现 Backup and Recovery 工作负载并将其分配给该项目。

- b. 备选方案：

您可以为自己分配 Backup and Recovery 超级管理员角色并直接发现工作负载，而不是授予用户完整的 Backup and Recovery 管理员访问权限。

3. 在 Backup and Recovery 中发现工作负载。

组织管理员或文件夹或项目管理员发现可用的工作负载，并选择适当的项目（如 US East 或 US West）。每个工作负载都会自动与选定项目关联。

4. 将用户添加到项目。

组织管理员或文件夹/项目管理员将 Console 用户添加到具有工作负载的项目。根据用户的访问需求，为其分配组织查看者角色和 Backup and Recovery 角色。具有正确 Backup and Recovery 角色的用户将自动获得对这些项目中新工作负载的访问权限。

## 相关信息

- ["了解 NetApp Console 身份和访问管理"](#)。
- ["NetApp Console 中的 NetApp Backup and Recovery 角色"](#)。

## 版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

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

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

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

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

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

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。