



参考

NetApp Backup and Recovery

NetApp

February 10, 2026

This PDF was generated from <https://docs.netapp.com/zh-cn/data-services-backup-recovery/reference-policy-differences-snapcenter.html> on February 10, 2026. Always check docs.netapp.com for the latest.

目录

- 参考 1
 - SnapCenter中的策略与NetApp Backup and Recovery中的策略比较 1
 - 计划层级 1
 - SnapCenter中具有相同计划层的多个策略 1
 - 导入的SnapCenter每日计划 1
 - 导入的SnapCenter每小时计划 2
 - SnapCenter策略的日志保留 2
 - 日志备份保留 2
 - SnapCenter策略的保留计数 2
 - SnapCenter策略中的SnapMirror标签 2
 - NetApp Backup and Recovery身份和访问管理 (IAM) 角色 3
 - 在暗站中恢复NetApp Backup and Recovery配置数据 3
 - 将NetApp Backup and Recovery数据还原到新的控制台代理 3
 - NetApp Backup and Recovery支持的 AWS 存档存储层 8
 - NetApp Backup and Recovery支持的 S3 归档存储类 8
 - 从档案存储中恢复数据 8
 - NetApp Backup and Recovery支持的 Azure 存档访问层 9
 - NetApp Backup and Recovery支持的 Azure Blob 访问层 9
 - 从档案存储中恢复数据 10
 - NetApp Backup and Recovery支持 Google 归档存储层 10
 - NetApp Backup and Recovery支持的 Google 归档存储类 10
 - 从档案存储中恢复数据 11

参考

SnapCenter中的策略与NetApp Backup and Recovery中的策略比较

SnapCenter中使用的策略与NetApp Backup and Recovery中使用的策略之间存在一些差异，这可能会影响您从SnapCenter导入资源和策略后看到的内容。

计划层级

SnapCenter使用以下计划层：

- 每小时：多个小时和分钟，任意小时（0-23）和任意分钟（0-60）。
- 每日：选择每隔一定天数重复一次，例如每 3 天。
- 每周：周日至周一，可选择在一周的第一天或一周中的多天执行快照。
- 每月：一月至十二月，可选择每月特定日期或多日演出，例如 7 号。

NetApp Backup and Recovery使用以下计划层，它们略有不同：

- 每小时：仅以 15 分钟为间隔执行快照，例如 1 小时或 15 分钟间隔小于 60。
- 每日：一天中的小时数（0-23），开始时间例如为上午 10:00，并可选择每隔几小时执行一次。
- 每周：一周中的某天（周日至周一），可选择在 1 天或多天内执行。这与SnapCenter相同。
- 每月：每月的日期（0-30），开始时间为每月的多个日期。
- 每年：每月。这与 SnapCenter 的月度相匹配。

SnapCenter中具有相同计划层的多个策略

您可以将具有相同计划层的多个策略分配给SnapCenter中的资源。但是，NetApp Backup and Recovery不支持在使用相同计划层的资源上应用多个策略。

示例：如果您在SnapCenter中使用三个策略（用于数据、日志和快照日志），则从SnapCenter迁移后，NetApp Backup and Recovery将使用单个策略而不是全部三个策略。

导入的SnapCenter每日计划

NetApp Backup and Recovery按如下方式调整SnapCenter计划：

- 如果SnapCenter计划设置为小于或等于 7 天，NetApp Backup and Recovery会将计划设置为每周。本周内有些快照被跳过。

示例：如果您有一个SnapCenter每日策略，从星期一开始每 3 天重复一次，NetApp Backup and Recovery会将计划设置为每周一、周四和周日。由于并非每 3 天一次，因此有些日子会被跳过。

- 如果SnapCenter计划设置为超过 7 天，NetApp Backup and Recovery会将计划设置为每月。该月将跳过一些快照。

示例：如果您有一个SnapCenter每日策略，其重复间隔为从每月 2 号开始每 10 天一次，则NetApp Backup and Recovery在迁移后会将计划设置为每月 2 日、12 日和 22 日执行。NetApp Backup and Recovery会在下个月跳过某些天。

导入的**SnapCenter**每小时计划

重复间隔大于一小时的SnapCenter每小时策略将转换为NetApp Backup and Recovery中的每日策略。

任何重复间隔不是 24 倍（例如 5、7 等）的每小时策略都会跳过一天中的某些快照。

示例：如果您有一个SnapCenter每小时策略，从凌晨 1:00 开始每 5 小时重复一次，NetApp Backup and Recovery（迁移后）将把计划设置为每天，间隔 5 小时，时间为凌晨 1:00、上午 6:00、上午 11:00、下午 4:00 和晚上 9:00。有些时间会被跳过，晚上 9:00 之后应该是凌晨 2:00，每 5 小时重复一次，但始终是凌晨 1:00。

SnapCenter策略的日志保留

如果SnapCenter中的资源具有多个策略，NetApp Backup and Recovery将使用以下优先级顺序来分配日志保留值：

- 对于SnapCenter中的“使用日志备份策略的完整备份”加上“仅日志”策略，NetApp Backup and Recovery使用仅日志策略保留值。
- 对于SnapCenter中的“仅带日志的完整备份”和“完整和日志”策略，NetApp Backup and Recovery使用仅日志保留值。
- 对于SnapCenter中的“完整备份和日志”加上“完整备份”，NetApp Backup and Recovery使用“完整备份和日志”保留值。
- 如果您在SnapCenter中只有完整备份，NetApp Backup and Recovery不会启用日志备份。

日志备份保留

SnapCenter支持资源策略的多个保留值。NetApp Backup and Recovery仅支持每个资源一个保留值。

SnapCenter策略的保留计数

如果您在SnapCenter中启用了二级保护的资源具有多个源卷、多个目标卷和多个SnapMirror关系，NetApp Backup and Recovery仅使用第一个策略的保留计数。

示例：如果您有一个保留计数为 5 的SnapCenter策略和另一个保留计数为 10 的策略，NetApp Backup and Recovery将使用保留计数 5。

SnapCenter策略中的**SnapMirror**标签

即使层级发生变化，SnapCenter也会在迁移后保留每个策略的SnapMirror标签。

示例：SnapCenter的每小时策略可能会在NetApp Backup and Recovery中更改为每日。但是，迁移后SnapMirror标签保持不变。

NetApp Backup and Recovery身份和访问管理 (IAM) 角色

NetApp Backup and Recovery采用身份和访问管理 (IAM) 来管理每个用户对特定功能和操作的访问权限。

要了解特定于NetApp Backup and Recovery 的IAM 角色，请参阅 ["NetApp Console中的NetApp Backup and Recovery角色"](#)。

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。您可以 ["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": "password" }'
> '
```

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": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiaXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoieWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWVpY2NtYXV0aDo4NDIwLyJ9CjRlY2Z3PokyLg1f67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-114v_pNDsPyNDyWqHaKizThdjJHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5ykODNDmrv5At_f9HHp0-xVMYHqywZ4nNFalMvAh4xESc5jfoKOZc-IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrzB81-o-ipvrOqSoliwIeHXZJJV-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 eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiaXVkiJpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoieWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWVpY2NtYXV0aDo4NDIwLyJ9CjRlY2Z3PokyLg1f67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-114v_pNDsPyNDyWqHaKizThdjJHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5ykODNDmrv5At_f9HHp0-xVMYHqywZ4nNFalMvAh4xESc5jfoKOZc-IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrzB81-o-ipvrOqSoliwIeHXZJJV-Uswun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA" }
```


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
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjZlIn0eyJzdWIiOiJvY
2NtYXV0aHwIiwiaXVkaIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbnVsbF9uYW1lIjoieYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFPbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWx1IiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOiE2NzI3NDQzMtMTsImIzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdsWjWcNvw2rRkFzjHpWrETgfgAMkZcAukV4DHuxogHWh6-
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。

NetApp Backup and Recovery支持的 AWS 存档存储层

NetApp Backup and Recovery支持两种 S3 存档存储类和大多数区域。



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"](#)。

NetApp Backup and Recovery支持的 S3 归档存储类

最初创建备份文件时，它们存储在 S3 *Standard* 存储中。此层针对存储不经常访问的数据进行了优化；但也允许您立即访问它。30 天后，备份将转换为 S3_标准-不频繁访问_存储类以节省成本。

如果您的源集群运行的是ONTAP 9.10.1 或更高版本，您可以选择在一定天数（通常超过 30 天）后将备份分层到 S3 *Glacier* 或 S3 *Glacier Deep Archive* 存储，以进一步优化成本。您可以将其设置为“0”或 1-999 天。如果将其设置为“0”天，则以后不能将其更改为1-999天。

这些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，因此您需要考虑可能需要多久从这些存档的备份文件中恢复数据。请参阅此页面上有关从档案存储恢复数据的部分。

- 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。

请注意，当您使用此类生命周期规则配置NetApp Backup and Recovery时，在 AWS 帐户中设置存储桶时不得配置任何生命周期规则。

["了解 S3 存储类别"](#)。

从档案存储中恢复数据

虽然将较旧的备份文件存储在档案存储中比标准或标准 IA 存储便宜得多，但从档案存储中的备份文件中访问数据进行恢复操作将花费更长的时间并且花费更多。

从 **Amazon S3 Glacier** 和 **Amazon S3 Glacier Deep Archive** 恢复数据需要多少费用？

从 Amazon S3 Glacier 检索数据时，您可以选择 3 个还原优先级；从 Amazon S3 Glacier Deep Archive 检索数据时，您可以选择 2 个还原优先级。S3 Glacier Deep Archive 的成本低于 S3 Glacier：

存档层	恢复优先级和成本		
	高的	标准	低的
S3 冰川	检索速度最快，成本最高	检索速度较慢，成本较低	检索速度最慢，成本最低

存档层	恢复优先级和成本		
S3 Glacier 深度存档		检索速度更快，成本更高	检索速度较慢，成本最低

每种方法都有不同的每 GB 检索费用和每请求费用。有关 AWS 区域 S3 Glacier 的详细定价，请访问 ["Amazon S3 定价页面"](#)。

恢复存档在 **Amazon S3 Glacier** 中的对象需要多长时间？

总还原时间由两部分组成：

- 检索时间：从存档中检索备份文件并将其放置在标准存储中的时间。这有时被称为“补水”时间。检索时间根据您选择的恢复优先级而不同。

存档层	恢复优先级和检索时间		
	高的	标准	低的
S3 冰川	3-5分钟	3-5小时	5-12小时
S3 Glacier 深度存档		12 小时	48 小时

- 恢复时间：从标准存储中的备份文件恢复数据的时间。这次与不使用存档层时直接从标准存储进行的典型恢复操作没有什么不同。

有关 Amazon S3 Glacier 和 S3 Glacier Deep Archive 检索选项的更多信息，请参阅 ["关于这些存储类别的 Amazon 常见问题解答"](#)。

NetApp Backup and Recovery支持的 Azure 存档访问层

NetApp Backup and Recovery支持一个 Azure 存档访问层和大多数区域。



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"](#)。

NetApp Backup and Recovery支持的 Azure Blob 访问层

最初创建备份文件时，它们存储在_Cool_访问层中。此层针对存储不经常访问的数据进行了优化；但在需要时可以立即访问。

如果您的源集群运行的是ONTAP 9.10.1 或更高版本，您可以选择在一定天数（通常超过 30 天）后将备份从“Cool_”存储分层到“Azure Archive_”存储，以进一步优化成本。此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，因此您需要考虑可能需要多久从这些存档的备份文件中恢复数据。请参阅此页面上有关从档案存储恢复数据的部分。

请注意，当您使用此类生命周期规则配置NetApp Backup and Recovery时，在 Azure 帐户中设置容器时不得配置任何生命周期规则。

["了解 Azure Blob 访问层"](#)。

从档案存储中恢复数据

虽然将较旧的备份文件存储在档案存储中比冷存储便宜得多，但从 Azure 存档中的备份文件访问数据进行还原操作将花费更长的时间并且花费更多。

从 **Azure** 存档恢复数据需要多少费用？

从 Azure 存档检索数据时，可以选择两个还原优先级：

- 高：检索速度最快，成本较高
- 标准：检索速度较慢，成本较低

每种方法都有不同的每 GB 检索费用和每请求费用。有关 Azure 区域 Azure 存档定价的详细信息，请访问 ["Azure 定价页面"](#)。



将数据从 Azure 还原到 StorageGRID 系统时不支持高优先级。

恢复 **Azure** 存档中存档的数据需要多长时间？

恢复时间由两部分组成：

- 检索时间：从 Azure 存档中检索存档的备份文件并将其放置在冷存储中的时间。这有时被称为“补水”时间。检索时间根据您选择的恢复优先级而不同：
 - 高：< 1 小时
 - 标准：< 15 小时
- 恢复时间：从冷存储中的备份文件恢复数据的时间。这次与不使用存档层时直接从冷存储进行的典型恢复操作没有什么不同。

有关 Azure 存档检索选项的更多信息，请参阅 ["此 Azure 常见问题解答"](#)。

NetApp Backup and Recovery 支持 Google 归档存储层

NetApp Backup and Recovery 支持一个 Google 归档存储类和大多数区域。



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 Recovery UI"](#)。

NetApp Backup and Recovery 支持的 Google 归档存储类

最初创建备份文件时，它们存储在 _标准_ 存储中。此层针对存储不经常访问的数据进行了优化；但也允许您立即访问它。

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（通常超过 30 天）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。此层中的数据将需要更高的检索成本，因此您需要考虑可能需要多久从这些存档的备份文件中恢复数据。请参阅此页面上有关从档案存储恢复数据的部分。

请注意，当您使用此类生命周期规则配置 NetApp Backup and Recovery 时，在 Google 帐户中设置存储桶时不

得配置任何生命周期规则。

["了解 Google 存储类别"](#)。

从档案存储中恢复数据

虽然将较旧的备份文件存储在存档存储中比标准存储便宜得多，但从存档存储中的备份文件中访问数据进行恢复操作将花费更长的时间并且花费更多。

从 **Google Archive** 恢复数据需要多少钱？

要了解按地区划分的 Google Cloud Storage 详细定价，请访问 ["Google Cloud Storage 定价页面"](#)。

恢复我在 **Google Archive** 中存档的对象需要多长时间？

总还原时间由两部分组成：

- 检索时间：从存档中检索备份文件并将其放置在标准存储中的时间。这有时被称为“补水”时间。与其他云提供商提供的“最冷”存储解决方案不同，您的数据可以在几毫秒内访问。
- 恢复时间：从标准存储中的备份文件恢复数据的时间。这次与不使用存档层时直接从标准存储进行的典型恢复操作没有什么不同。

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。