



管理 **S3** 接入点

Workload Factory for NetApp Console

NetApp
October 07, 2026

目录

- 管理 S3 接入点 1
 - 在 NetApp Workload Factory 中为卷创建 S3 访问点 1
 - 在 NetApp Workload Factory 中管理卷的 S3 访问点 2
 - 编辑卷的 S3 访问点 2
 - 查看卷的 S3 访问点详细信息 2
 - 删除 NetApp Workload Factory 中卷的 S3 访问点 3
- 设置 NetApp Workload Factory 的日志表基础结构 3
 - 关于此任务 3
 - 开始之前 4
 - 设置日志表基础架构 6
 - 对日志表的基础设施设置进行故障诊断 7
 - 日记表设置的权限引用 10

管理 S3 接入点

在 NetApp Workload Factory 中为卷创建 S3 访问点

在 NetApp Workload Factory 中为卷创建和附加 S3 访问点。

关于此任务

Amazon FSx for NetApp ONTAP 允许 NFS 和 SMB 文件系统访问 S3 数据并连接到 Amazon Bedrock、SageMaker、Athena、AWS Glue 等 AWS 服务。您可以将 AWS 服务连接到所有对象存储数据。

将 S3 接入点连接到 FSx for ONTAP 文件系统上的 NFS 和 SMB 卷，以便 AWS 服务像在 S3 存储桶中一样访问文件。连接接入点时，请定义唯一 ID，选择文件访问类型（UNIX 或 Windows），并添加用于访问授权的用户名。

连接 S3 访问点后，它会以唯一的别名显示在 AWS Management Console 中。使用此别名作为 AWS 服务（例如 Amazon Bedrock）的 S3 存储桶名称，以访问 FSx for ONTAP 卷中的文件。

您可以将多个 S3 接入点连接到单个 FSx for ONTAP 卷，每个接入点都具有唯一的访问级别，以连接到多个 AWS 服务。

开始之前

开始之前，请完成以下要求。

- 您必须具有带有 S3 访问点的现有卷。["使用 S3 访问点创建卷"](#)
- 必须["使用 *operations and remediation* 权限策略授予凭据"](#)在 Workload Factory 中才能完成此任务。

步骤

1. 登录到 ["NetApp Console"](#)。
2. 选择菜单 ，**Workloads > Volumes explorer**。
3. 选择要使用的卷的操作菜单，然后选择 **Advanced actions**，然后选择 **Manage S3 access points**。
4. 在"管理 S3 接入点"页面上，选择*创建并连接 S3 接入点*。
5. 在 创建并附加 **S3** 接入点 页面上，提供以下信息：
 - **S3 接入点名称**：输入 S3 接入点的名称。
 - **User**：选择有权访问卷的现有用户或创建新用户。
 - 用户类型：选择 **UNIX** 或 **Windows** 作为用户类型。
 - 网络配置：选择*互联网*或*虚拟私有云 (VPC)*。您选择的网络类型决定了接入点是可从互联网访问还是仅限于特定的 VPC。要使用 Journal 表功能，您必须选择*互联网*作为网络配置。
 - 库存表：可选。需要 `getObject` 权限。启用卷上的库存表以生成 S3 访问点可访问的所有对象的元数据，并产生 AWS S3 请求成本。有关详细信息，请参见["Amazon S3 定价文档"](#)。表格每 24 小时更新一次。
 - **S3 接入点标签**：您最多可以添加 50 个标签或删除标签。
6. 选择 **Create**。

相关信息

您可以选择将日志表功能与 Workload Factory 中的 S3 访问点一起使用。日志表基础架构可捕获并存储跨 Amazon FSx for ONTAP 卷访问点的用户访问事件和对象操作的审核日志。要启用日志表功能，您必须设置必要的 AWS 基础架构，包括 AWS CloudTrail、AWS CloudWatch、AWS S3 存储桶、AWS CloudWatch 日志组以及 AWS Identity and Access Management (IAM) 角色和策略。["设置 NetApp Workload Factory 的日记表基础结构"](#)。

其他相关主题：

["编辑或删除 NetApp Workload Factory 中卷的 S3 访问点"](#)

在 NetApp Workload Factory 中管理卷的 S3 访问点

更新 NetApp Workload Factory 中卷的 S3 访问点详细信息或删除 S3 访问点。

您还可以启用或禁用接入点的*库存表*。库存表会为 S3 接入点可访问的所有对象生成元数据，并产生 AWS S3 请求成本。有关详细信息，请参见["Amazon S3 定价文档"](#)。

编辑卷的 S3 访问点

在 NetApp Workload Factory 中编辑卷的 S3 访问点。

步骤

1. 登录到 ["NetApp Console"](#)。
2. 选择菜单 ，**Workloads > Storage > Volumes explorer**。
3. 选择要编辑其 S3 接入点的卷的操作菜单，然后选择 **Advanced actions**，然后选择 **Manage S3 access points**。
4. 在*管理 S3 接入点*屏幕中，选择操作菜单，然后选择*编辑接入点*。
5. 进行更新，然后选择 **Apply**。

要为日志表功能设置基础架构，您必须选择 **Internet** 作为 S3 访问端点的网络配置。["了解如何为 NetApp Workload Factory 设置日志表基础结构"](#)。

查看卷的 S3 访问点详细信息

查看 S3 接入点详细信息，如别名、ARN 和 S3 URI。启用库存和日记表后，您可以查看跨 S3 访问点的用户访问事件和对象操作的元数据和审计日志。

关于此任务

当在卷上启用清单表时，您可以查看连接到卷的现有 S3 访问点的访问点、清单表和表存储桶详细信息。系统还提供到 AWS Management Console 中清单表的链接。

启用日志表后，Workload Factory 将在表中的访问点上生成日志供您参考。该表包括 CloudTrail 事件、跟踪（AWS 活动的记录）、CloudTrail 过滤器、CloudWatch 日志组等。

您可以复制访问点详细信息以用于其他应用程序。

步骤

1. 登录到 ["NetApp Console"](#)。
2. 选择菜单 ，**Workloads > Storage > Volumes explorer**。
3. 选择要查看其详细信息的卷的操作菜单，然后选择*高级操作*，然后选择*查看详细信息*。

详细信息显示在四个选项卡下：**Access point**、**Inventory table**、**Journal table** 和 **Table bucket**。

4. 如果已启用库存或日记帐表的状态，但缺少 ``get:Object`` 权限，请按照对话框中的说明添加所需的权限。
5. 当日记账表状态为挂起时，您必须提供 CloudTrail ARN 才能将日记帐表连接到创建的基础设施。按照说明使用 AWS CLI 或 AWS 管理控制台部署 CloudFormation 堆栈，然后返回 Workload Factory 控制台输入 CloudTrail ARN。

删除 NetApp Workload Factory 中卷的 S3 访问点

从 NetApp Workload Factory 中的卷删除现有 S3 访问点。

步骤

1. 登录到 ["NetApp Console"](#)。
2. 选择菜单 ，**Workloads > Storage > Volumes explorer**。
3. 选择要为其管理 S3 接入点的卷的操作菜单，然后选择 **Advanced actions**，然后选择 **Manage S3 access points**。
4. 选择要删除的 S3 接入点的操作菜单，然后选择 **Delete**。
5. 在*删除 S3 接入点*对话框中，选择*删除*以从卷中删除 S3 接入点。

Workload Factory 不会删除库存或日记表，但您可以从 AWS 管理控制台手动删除它们。

相关信息

- ["设置日志表基础架构"](#)

设置 NetApp Workload Factory 的日志表基础结构

设置日志表基础架构，以捕获和存储跨 Amazon FSx for ONTAP 卷访问点的用户访问事件和对象操作的审计日志。需要执行几个步骤来为 AWS 服务设置基础架构，如 AWS CloudTrail、AWS CloudWatch、AWS S3 存储桶、AWS CloudWatch 日志组、AWS Identity and Access Management (IAM) 和 AWS S3 Tables，以便日志事件正确通过管道传输并由 Workload Factory 读取。

关于此任务

日志表功能捕获受监控 FSx for ONTAP S3 访问点的 S3 数据平面事件（PutObject、GetObject、DeleteObject 等）。它使用部署到您的 AWS 账户中的 AWS 服务链。正确设置基础架构后，它将连接到 FSx for ONTAP 卷访问点，并建立在日志表中捕获用户访问和对象操作审核事件的管道。

下表列出了作为基础架构一部分的 AWS 服务、它们各自的资源名称模式以及服务在管道中的用途。

AWS 服务	资源名称模式	目的
AWS CloudFormation	netapp-metadata-*	将所有基础架构部署为堆栈
AWS S3 存储桶	netapp-metadata-cloudtrail-events-logs-{uuid}	存储原始 CloudTrail 日志文件
AWS CloudTrail	netapp-metadata-journal-data-events-trail-{uuid}	捕获特定接入点的 S3 数据事件
AWS CloudWatch 日志组	netapp-metadata-journal-data-events-{uuid}	以结构化日志条目的形式接收 CloudTrail 事件
IAM 角色	- netapp-metadata-cloudtrail-cw-role-{uuid} - netapp-metadata-s3table-integration-role-{uuid}	主动集成
ObservabilityAdmin	S3TableIntegration	将 CloudWatch 日志桥接到 S3 Tables 表中
S3 表	aws-cloudwatch bucket → logs.aws_cloudtrail__data	以 Iceberg 格式存储结构化、可查询的 CloudTrail 事件

{uuid} 是创建模板时生成的随机 8 个字符的标识符。

开始之前

要启用日志表功能，请执行以下步骤：

- 具有 S3 访问点的现有卷。["使用 S3 访问点创建卷"](#)
- 将 S3 访问端点的网络配置设置为 **Internet**。["编辑 S3 接入点的网络配置"](#)。
- ["授予 *operations and remediation* 权限"](#) 到您的 Workload Factory 凭据。
- 将以下 IAM 策略权限添加到用于运行 CloudFormation 部署的 AWS 账户，以设置 Journal 表。

▼ 日志表设置的 IAM 策略权限

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CFNStack",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/netapp-
metadata-*/*"
    },
  ],
}
```

```

{
  "Sid": "StarResources",
  "Effect": "Allow",
  "Action": [
    "cloudformation:GetTemplateSummary",
    "cloudtrail:DescribeTrails",
    "logs:DescribeLogGroups",
    "logs:ListSourcesForS3TableIntegration",
    "observabilityadmin:CreateS3TableIntegration",
    "observabilityadmin:GetS3TableIntegration",
    "observabilityadmin:TagResource",
    "observabilityadmin:ListTagsForResource"
  ],
  "Resource": "*"
},
{
  "Sid": "S3Bucket",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:PutBucketPolicy",
    "s3:PutBucketTagging"
  ],
  "Resource": "arn:aws:s3:::netapp-metadata-*"
},
{
  "Sid": "IAMRoles",
  "Effect": "Allow",
  "Action": [
    "iam:CreateRole",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:GetRole"
  ],
  "Resource": "arn:aws:iam::*:role/netapp-metadata-*"
},
{
  "Sid": "PassRole",
  "Effect": "Allow",
  "Action": "iam:PassRole",
  "Resource": "arn:aws:iam::*:role/netapp-metadata-*",
  "Condition": {
    "StringEquals": {
      "iam:PassedToService": [
        "cloudtrail.amazonaws.com",
        "logs.amazonaws.com"
      ]
    }
  }
}

```

```

    ]
  }
},
{
  "Sid": "CloudTrail",
  "Effect": "Allow",
  "Action": [
    "cloudtrail:CreateTrail",
    "cloudtrail:StartLogging",
    "cloudtrail:AddTags",
    "cloudtrail:PutEventSelectors"
  ],
  "Resource": "arn:aws:cloudtrail:*:*:trail/netapp-metadata-
* "
},
{
  "Sid": "CWLogGroup",
  "Effect": "Allow",
  "Action": [
    "logs:CreateLogGroup",
    "logs>DeleteLogGroup",
    "logs:PutRetentionPolicy",
    "logs:TagResource",
    "logs:AssociateSourceToS3TableIntegration"
  ],
  "Resource": "arn:aws:logs:*:*:log-group/netapp-metadata-*"
},
{
  "Sid": "S3Table",
  "Effect": "Allow",
  "Action": [
    "s3tables>CreateTableBucket",
    "s3tables:PutTableBucketEncryption",
    "s3tables:PutTableBucketPolicy"
  ],
  "Resource": "arn:aws:s3tables:*:*:bucket/aws-cloudwatch"
}
]
}

```

设置日志表基础架构

设置基础设施以从日志表中的 S3 访问点捕获 AWS 服务事件。

步骤

1. 登录到 ["NetApp Console"](#)。
2. 选择菜单 ，**Workloads > Storage > FSx for ONTAP**。
3. 从 **FSx for ONTAP** 中，选择包含要更新的卷的文件系统的操作菜单，然后选择*管理*。
4. 从文件系统概述中，选择*卷*选项卡。
5. 从"卷"选项卡中，选择要为其管理 S3 接入点的卷的操作菜单，然后选择 高级操作，然后选择 管理 **S3** 接入点。
6. 在*管理 S3 接入点*屏幕中，选择操作菜单，然后选择*编辑接入点*。
7. 在 编辑 **S3** 接入点 对话框中，确保网络配置设置为 **Internet**。
8. 按照对话框中的说明设置日记表功能的基础架构。
9. 下载 CloudFormation 模板。
10. 在 AWS 帐户中部署 CloudFormation 堆栈。
 - a. 将模板 JSON 保存到文件。
 - b. 使用 AWS CLI 或 AWS 管理控制台部署模板。
 - c. 等待堆栈达到 `CREATE_COMPLETE` 状态。
 - d. 从堆栈输出中获取 CloudTrail ARN。
11. 返回到 Workload Factory 控制台并返回到卷以管理 S3 访问点。
12. 从卷操作菜单中选择 查看详细信息。
13. 在 **Journal table** 选项卡中，输入 CloudTrail ARN。
14. 选择*应用*。

如果任何步骤失败，[对日志表的基础设施设置进行故障排除](#) 或联系 NetApp 支持人员以获得帮助。

对日志表的基础设施设置进行故障诊断

您可以使用 AWS 管理控制台或 AWS CLI 对 CloudFormation 堆栈部署期间的故障及其创建的资源进行故障排除。

解决此问题后，请再次提交 CloudTrail ARN 以重新启动日记表设置。

常见 CloudFormation 部署失败

IAM 权限不足

部署角色/用户需要一组特定的权限。有关完整策略，请参阅 [开始之前](#)。

如果堆栈因 `AccessDenied` 或 `InsufficientPermission` 错误而失败，请检查堆栈事件，并在 `ResourceStatusReason` 字段中查找缺少的权限。

CloudTrail 限制

AWS 强制执行每个区域 5 条跟踪路径的默认限制。如果帐户已有 5 个轨迹，则 `the FsxDatEventTrail` 资源将失败：超出最大轨迹数 (5)。您可以使用以下命令检查区域级别的轨迹数量：

```
aws cloudtrail describe-trails \
  --no-include-shadow-trails \
  --region <region> \
  --query "length(trailList)"
```

解决方案选项

- 选项 1：删除该区域中未使用的跟踪以腾出空间。
- 选项 2：使用现有路径。在再次部署 CloudFormation 堆栈之前，请从模板中删除 `FsxDataEventTrail`、`CloudTrailBucket`、`CloudTrailBucketPolicy` 和 `CloudTrailToCloudWatchRole` 资源。然后在启动步骤中传递现有跟踪的 ARN。现有跟踪必须配置 CloudWatch 日志组，与日志组关联的 `S3TableIntegration`，并记录数据事件。

S3 表集成已存在

如果帐户已具有 `aws_cloudtrail` 数据源的 `S3TableIntegration`，则 `LogsToS3TableIntegration` 资源将失败。

解决方法

在再次部署 CloudFormation 堆栈之前，请从模板中删除 `LogsToS3TableIntegration` 和 `S3TableIntegrationRole` 资源。只要您为 `aws_cloudtrail` 数据事件配置现有集成，系统就会自动使用该集成。

要检查现有集成：

```
aws observabilityadmin list-s3-table-integrations --region <your-region>
```

S3 存储桶名称已存在

存储桶名称 `netapp-metadata-cloudtrail-events-logs-{uuid}` 是全局唯一的。如果发生冲突，请重新请求模板以获取新的 UUID。

IAM 角色已存在

如果之前的部分部署留下了具有 `netapp-metadata-*` 名称模式的 IAM 角色，则堆栈将在角色创建时失败。首先删除孤立角色：

```
aws iam delete-role-policy \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid> \
  --policy-name <policy-name>
aws iam delete-role \
  --role-name netapp-metadata-cloudtrail-cw-role-<uuid>
```

启用日记表后失败

提交 CloudTrail ARN 后，Workload Factory 通过自动发送 *seed* 或测试事件来验证整个资源管道。如果成功，种子事件将到达 S3 Tables 表中。测试大约需要 10 分钟。

如果测试验证失败，您可能会收到以下错误消息之一：

错误消息	含义
未在 {bucket} 中创建表 aws_cloudtrail__data。验证 s3table 权限。	S3TableIntegration 未创建 CloudWatch-managed 表。CloudWatch 日志和 S3 表之间的管道已中断。
表存在，但日记账种子事件未出现。验证 CloudTrail 和 CloudWatch 权限。	该表存在，但特定的种子事件从未到达。CloudTrail 和 S3 Tables 表之间的管道已断开。
无法启动日志设置。.....	后台种子/轮询流程期间出错。有关详细信息，请查看尾部消息。

解决步骤

当日志到达 FAILED 时，通过管道阶段跟踪种子事件，以准确识别其停止的位置。每个步骤都映射到由模板创建的特定 AWS 资源。

1. 检查 CloudTrail S3 Bucket。

该跟踪将原始事件日志写入 S3 存储桶 netapp-metadata-cloudtrail-events-logs。查找最近的日志文件。

如果不存在日志文件，则 CloudTrail 不会捕获事件。请检查以下内容：

- 跟踪正在记录 (IsLogging: true)
- 高级事件选择器包括正确的接入点 ARN
- 高级事件选择器包括 eventCategory = Data 和 resources.type = AWS::S3::AccessPoint 的筛选器

2. 检查 CloudWatch 日志组。

该跟踪还向 CloudWatch 日志组提供事件。日志组名称以 netapp-metadata-journal-data-events-`<uuid>` 开头。

- 如果日志组为空，则 CloudTrail 不会将事件传递到 CloudWatch。检查 CloudTrailToCloudWatchRole IAM 角色是否存在，是否具有 logs:CreateLogStream 和 logs:PutLogEvents 权限，以及跟踪是否配置了正确的 CloudWatchLogsLogGroupArn 和 CloudWatchLogsRoleArn。
- 如果种子事件出现在日志组中，则问题在下游 — 继续执行步骤 3。

3. 检查 S3 Tables 表 (aws-cloudwatch) 。

S3TableIntegration 会自动创建一个名为 aws-cloudwatch 的表存储桶，并填充 logs.aws_cloudtrail__data 处的表。此表仅在第一个事件流过后才会创建。

- 如果 aws-cloudwatch 表存储桶不存在，则 S3TableIntegrationRole 缺少权限。它需要 `s3tables:CreateTableBucket`、`s3tables:PutTableBucketEncryption` 和 `s3tables:PutTableBucketPolicy`——所有范围均为 `arn:aws:s3tables:*:*:bucket/aws-cloudwatch`。
- 如果表存储桶存在但 `logs.aws_cloudtrail__data` 不存在，则集成不会路由事件。集成必须显示 `Status: ACTIVE` 并包含 `aws_cloudtrail` 作为日志源。

- 如果该表存在但种子事件不在其中，则该事件可能仍在传输中。S3 Tables 摄取有一些延迟。再等几分钟。如果 15-20 分钟后仍未显示，则集成可能会中断。

4. 直接查询种子事件。

- 在 AWS 管理控制台中打开 S3 Tables。
- 导航到 aws-cloudwatch 表存储桶 → aws_cloudtrail__data 表，然后使用 **Preview** 按钮直接在浏览器中运行快速查询。
- 如果事件存在于表中，但日志仍显示 FAILED，则可能在事件到达之前轮询窗口已过期。

解决问题后，返回 Workload Factory 控制台。通过再次提交 Trail ARN 来重试 [启动日志表设置](#)。

- 如果设置继续失败，请联系 NetApp 支持以获得帮助。

日记表设置的权限引用

部署 CloudFormation 堆栈以启用 Journal 表功能的 IAM 角色需要以下权限。请参阅 [开始之前](#) 以获取具有所需权限的可复制 JSON 策略。

堆栈操作

权限	资源	为什么
cloudformation: CreateStack	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	创建堆栈
cloudformation: DescribeStacks	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	监控堆栈状态
cloudformation: DescribeStackEvents	arn:aws:cloudformation:*:*:stack/netapp-metadata-/	诊断资源级故障 cloudformation:GetTemplateSummary * 预检模板验证

CloudTrail

权限	资源	为什么
cloudtrail: CreateTrail	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	创建路径
cloudtrail: StartLogging	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	启用日志记录
cloudtrail: AddTags	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	应用识别标签
cloudtrail: PutEventSelectors	arn:aws:cloudtrail:*:*:trail/netapp-metadata-*	配置数据事件捕获
cloudtrail: DescribeTrails	*	解析堆栈输出的跟踪 ARN

S3

权限	资源	为什么
s3: CreateBucket	arn:aws:s3:::netapp-metadata-*	创建 CloudTrail 日志桶
s3: PutBucketPolicy	arn:aws:s3:::netapp-metadata-*	允许 CloudTrail 写入日志
s3: PutBucketTagging	arn:aws:s3:::netapp-metadata-*	应用识别标签

身份与访问管理

权限	资源	为什么
iam: CreateRole	arn:aws:iam::*:role/netapp-metadata-*	创建两个 IAM 角色
iam: PutRolePolicy	arn:aws:iam::*:role/netapp-metadata-*	附加内联策略
iam: TagRole	arn:aws:iam::*:role/netapp-metadata-*	应用识别标签
iam: GetRole	arn:aws:iam::*:role/netapp-metadata-*	确认角色处于活动状态
iam: PassRole	arn:aws:iam::*:role/netapp-metadata-* (条件 : PassedToService = cloudtrail.amazonaws.com, logs.amazonaws.com)	将角色传递给 CloudTrail 和 CloudWatch Logs

CloudWatch 日志

权限	资源	为什么
logs: CreateLogGroup	arn:aws:logs::*:log-group:netapp-metadata-*	创建日志组
日志: DeleteLogGroup	arn:aws:logs::*:log-group:netapp-metadata-*	创建失败时清理日志组
日志: PutRetentionPolicy	arn:aws:logs::*:log-group:netapp-metadata-*	设置 30 天保留期
日志: TagResource	arn:aws:logs::*:log-group:netapp-metadata-*	应用识别标签
logs: 将源关联到 S3 表集成	arn:aws:logs::*:log-group:netapp-metadata-*	将 CloudTrail 源链接到 S3 Tables
日志: DescribeLogGroups	*	检查日志组是否存在
logs: 列出 S3 表集成的来源	*	确认集成关联

ObservabilityAdmin

权限	资源	为什么
observabilityadmin: CreateS3TableIntegration	*	创建 CloudWatch → S3 Tables 桥

权限	资源	为什么
observabilityadmin:GetS3TableIntegration	*	确认集成处于活动状态
observabilityadmin: TagResource	*	应用识别标签
observabilityadmin : ListTagsForResource	*	漂移检测

S3 表

权限	资源	为什么
s3tables: CreateTableBucket	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	创建 S3 Tables 存储桶（通过集成角色）
s3tables : PutTableBucketEncryption	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	设置 AES256 加密
s3tables: PutTableBucketPolicy	arn:aws:s3tables:*:*:bucket/aws-cloudwatch	允许 CloudWatch Logs 访问

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。