



数据治理、隐私和生命周期 Information Security for Workload Factory

NetApp
September 16, 2026

目录

- 数据治理、隐私和生命周期 1
 - NetApp Workload Factory 的数据处理和驻留 1
 - Workload Factory 处理的数据类 1
 - Workload Factory 保留的数据类 1
 - 信息的保存位置 1
 - 信息保存多长时间 2
 - 哪些信息会离开 VPC 2
 - 配置和元数据收集范围 3
 - NetApp Workload Factory 的加密和密钥管理 6
 - FSx 的 KMS 静态加密范围 6
 - 凭据保护（服务端信封加密） 7
 - NetApp Workload Factory 帐户删除 7

数据治理、隐私和生命周期

NetApp Workload Factory 的数据处理和驻留

NetApp Workload Factory 将数据处理组织成多个类别，用于描述服务所处理的运营数据、每个数据类在安全模型中的位置、数据的存储位置、保留时长以及数据是否离开客户环境。主要数据类包括配置和元数据、操作日志和事件以及遥测数据。保留的数据可以包括 FSx for ONTAP 配置快照、凭据引用、AI 使用和成本数据、审计记录以及短期响应缓存。存储和处理位置因数据类型而异：某些信息保留在客户 AWS 账户中，而其他操作数据则存储在 NetApp 账户中。

Workload Factory 处理的数据类

Workload Factory 处理以下数据类：

- 配置和元数据
- 操作日志和事件
- 遥测

Workload Factory 保留的数据类

Workload Factory 保留以下数据：

- FSx 配置快照（每次扫描时刷新）
- ONTAP 凭据引用或使用 KMS 信封加密方式加密的凭据材料（取决于所选凭据模式）
- EDA 指标
- CloudFormation 模板（7 天 `Expires` 标题）
- AI 使用和成本数据
- 审核记录
- Redis 缓存（FSx 响应），TTL 为 20 分钟

信息的保存位置

AWS 帐户

- ONTAP 管理员密码存储在 AWS Secrets Manager 中。
- Amazon Bedrock 通过您的 AWS 账户中的 STS 假定角色，使用您的推理配置文件 ARN 处理 AI 推理（EMS 分析）。

NetApp 帐户

- FSx 配置、平衡计划、ARP 配置和 AI 使用限制
- 临时 AWS STS 凭据（缓存在 Redis 中）、响应缓存、锁定和部署状态

- CloudFormation/Terraform 模板、WAD 配置描述符和压缩报告
- AI 使用计量和收集器性能指标
- EDA 汇总指标
- 操作审核跟踪
- OpenTelemetry 追踪

地区注意事项

- 存储在提供 Amazon Bedrock 服务的地区。
- NetApp internal 在 `us-east-1` 和 `us-west-2` 中运行。

信息保存多长时间

本节总结了保留类别。有关详细的值和策略行为，请参见链接页面。

- 凭据和临时 AWS STS 凭据保留：["NetApp Workload Factory 的凭据保留"](#)
- 运营指标和遥测保留：["NetApp Workload Factory 的指标和遥测参考"](#)
- 审核记录保留：受 NetApp Console 保留策略管理（不受 Workload Factory 控制）

哪些信息会离开 VPC

本节总结出站数据类别。有关协议级别和功能级别的详细信息，请参阅链接页面。

到 **Workload Factory** 服务的管理平面流量

对于管理操作，FSx 配置、卷元数据、资源标识符和操作命令通过 HTTPS 流向 NetApp Workload Factory 服务层。

审核记录到 **NetApp Console** 审核服务

每个跟踪的操作都会发送以下信息：

- accountId
- actionName
- status
- resourceId
- userId
- requestData
- responseData
- timestamps
- IP address
- workspaceId

AI 分析流量

FSx for ONTAP 紧急管理系统 (EMS) 事件、为 AI 诊断提交的延迟数据和错误日志通过您的 AWS 账户使用您配置的推理配置文件传输到 Amazon Bedrock，因此这些流量保留在您的环境中，而不是到达 NetApp 系统。

有关 AI 分析流量的更多信息，请参阅：

- ["NetApp Workload Factory 的 AI 控制概述"](#)
- ["Bedrock 选择加入 NetApp Workload Factory AI 诊断"](#)
- ["NetApp Workload Factory 的 AI 工具边界"](#)

AWS 服务 API 流量

请参阅 ["NetApp Workload Factory 的连接和信任路径"](#)。

遥测和指标收集

请参见 ["指标和遥测参考"](#)。

配置和元数据收集范围

文件系统级别

- 文件系统配置（部署类型 Gen1/Gen2、吞吐量容量、存储容量、存储类型）
- 首选子网、安全组、VPC 配置
- KMS加密密钥元数据
- 文件系统标记
- 文件系统生命周期状态
- 维护窗口设置

卷级别（综合）

- 身份和状态：卷名、UUID、类型（rw/dp/ls）、样式（FlexVol/FlexGroup）、状态（在线/离线/受限）、创建时间
- 容量：总大小、已用、可用、物理已用、已用百分比、SSD占用空间、容量池占用空间、非活动数据字节/百分比
- 分级：策略（all/auto/none/snapshot_only），最短冷却天数
- QoS：分配的 QoS 策略名称
- NAS 配置：连接路径、导出策略分配、UNIX 权限、安全样式（unix/ntfs/mixed）
- 快照：快照保留大小/百分比/已使用，自动删除设置
- 数据效率：压缩类型/状态、重复数据删除、压缩、节省空间
- 自动调整大小：模式（grow/grow_shrink/off），最小/最大大小，增长/收缩阈值
- SnapLock：类型（合规性/企业/非 SnapLock）、保留期（最小/最大/默认）、自动提交期

- 克隆：父卷/快照/存储虚拟机，是FlexClone，拆分状态
- Inodes/files：最大可能数、最大配置数、已用计数
- 加密：已启用/已禁用状态
- 访问时间：atime 更新已启用/禁用及更新周期
- SnapMirror：保护状态、目标类型（云/ONTAP）
- FlexGroup 重新平衡：不平衡百分比，最大阈值
- 卷移动：目标聚合、移动状态
- FlexCache 端点类型：none/cache/origin
- 标签：ONTAP 级别卷标签

Snapshot数据

- 快照名称、UUID、创建时间、到期时间
- 大小（字节）
- SnapMirror 标签
- SnapLock 到期和锁定状态
- 状态（有效/无效/部分）
- 用户评论
- 快照策略：名称、启用状态、计划副本（计数、保留期、计划名称、前缀、SnapMirror 标签）

导出策略

- 策略名称、ID、关联的Storage VM
- 规则：协议列表（NFS/CIFS/FlexCache），客户端匹配模式，只读规则，读/写规则，超级用户规则，规则索引/优先级
- SUID、设备创建、chown 模式、匿名用户映射、NTFS UNIX 安全设置

S3 接入点

- 生命周期状态（可用/创建/删除/失败/配置错误）
- 创建时间、ARN、别名、名称
- 文件所有者用户和类型（UNIX/WINDOWS）
- 网络配置（互联网与 VPC 访问、VPC ID）
- AWS 标记
- 元数据扫描启用、日志记录启用、CloudTrail ARN

反勒索软件防护(ARP)

Workload Factory 收集配置状态和事件详细信息：

- 每个卷的状态（启用/禁用/dry_run/暂停）

- 攻击概率（无/低/中/高）
- 带时间戳的攻击报告
- 检测参数：文件扩展名阈值、重命名率波动%、熵率波动%、文件创建/删除率波动%
- 可疑文件：文件路径、文件名、文件格式、可疑时间、相关卷

复制 / SnapMirror

- 关系 UUID、状态、健康状态
- 源和目标（Storage VM、路径、集群）
- 传输统计信息（传输的字节数、持续时间、结束时间、状态）
- 策略（名称、类型：async/sync/continuous）
- 限速设置
- 滞后时间
- 不健康的原因（消息和代码）
- 当前传输错误

iGroups

- 名称、UUID、协议（FCP/iSCSI/混合）、操作系统类型
- 启动器（IQN/WWPN）、连接状态、上次访问时间
- LUN映射（逻辑单元号、LUN详细信息）

LUN 数

- 名称、UUID、序列号、操作系统类型、启用状态
- 大小、已用空间、精简配置设置
- 位置（卷、节点、逻辑单元路径）
- 自动删除设置
- 容器状态、映射状态、只读状态
- QoS策略
- 性能指标（IOPS、延迟、每次读/写/总吞吐量）
- 一致性组成员身份

FlexCache

- 原始卷/存储 VM/集群，缓存大小，路径
- 已启用写回，DR 缓存状态
- 相对大小配置
- 预填充目录路径
- 缓存和源之间的连接状态

Storage VM级别

- 名称、UUID、状态（运行/停止）、子类型
- 启用/允许的协议（NFS、CIFS、iSCSI、FCP、NVMe、S3）
- DNS 服务器和域
- 名称服务开关配置（passwd、group、hosts 等）
- IP接口（名称、IP地址、服务）
- 分配的聚合
- 反勒索软件默认卷状态
- 空间强制设置
- 对等关系（应用程序、状态、远程集群/存储 VM）

聚合/存储级别

- 聚合名称、UUID、状态、RAID 状态
- 块存储：磁盘计数、RAID 大小、可用/已用/总空间、物理已用
- 已使用云存储
- 效率：比率、逻辑使用、节省
- 加密、镜像、SnapLock 设置
- 性能指标（IOPS、延迟、吞吐量）

利用率指标（EDA）

- 采集节奏：容量/吞吐量每 12 小时一次；延迟每 20 分钟一次
- 粒度：归一化为每个时间范围约 60 个数据点
- 保留和存储详细信息：["指标和遥测参考"](#)

NetApp Workload Factory 的加密和密钥管理

NetApp Workload Factory 使用静态加密，并在 Workload Factory 和 AWS 服务中定义明确的密钥管理责任。对于 Amazon FSx for NetApp ONTAP 文件系统，您可以选择自己的 AWS KMS 密钥或使用 AWS 托管的默认密钥，FSx for ONTAP 将使用该密钥执行加密操作。Workload Factory 还使用信封加密来保护存储的 ONTAP 凭据。

FSx 的 KMS 静态加密范围

通过 Workload Factory 为 ONTAP 文件系统创建 FSx 时，您可以选择指定自己的 AWS KMS 密钥进行静态数据加密。如果您未指定密钥，Workload Factory 将使用 AWS 管理的默认 FSx 密钥。

什么是加密的

存储在支持 FSx for ONTAP 文件系统的底层 EBS 卷上的所有数据（AWS FSx 静态加密）。

密钥所有权

KMS 密钥位于您的 AWS 账户中。

密钥选择和使用所需的权限

Workload Factory 需要：

- kms:DescribeKey
- kms:ListKeys
- kms:ListAliases
- kms:CreateGrant （允许 FSx for ONTAP 服务使用密钥）

密钥访问模式

Workload Factory 绝不会使用您的 KMS 密钥直接加密或解密数据。它在文件系统创建期间将密钥 ID 传递给 Amazon FSx for NetApp ONTAP API；Amazon FSx for NetApp ONTAP 负责执行加密操作。

凭据保护（服务端信封加密）

当您通过 Workload Factory 存储 ONTAP 凭据（管理员密码）时，系统会在保存凭据之前使用信封加密对其进行保护。

加密方法

每个凭据记录具有唯一数据加密密钥（DEK）的 AES-256-CBC。

信封加密流程

1. 每个凭据生成唯一的 256 位 DEK。
2. DEK 对凭据（密码）进行加密。
3. DEK 本身使用根密钥加密，并与加密凭据一起存储。
4. 明文 DEK 从不存储。

加密上下文

每个数据密钥都以加密方式绑定到其特定凭据记录，防止跨记录重复使用密钥。

替代方案：AWS Secrets Manager

您可以在自己的账户中将 ONTAP 凭据存储在 AWS Secrets Manager 中，而不是在服务中存储加密密码。Workload Factory 不会查看或存储密码；它将 Secrets Manager ARN 传递给 Lambda link，后者在您的 VPC 中的运行时检索密码。



GovCloud 账户需要 AWS Secrets Manager。

NetApp Workload Factory 帐户删除

帐户删除不是自助服务操作；它是一个离线工作流程，涉及 Workload Factory 服务和 AWS 帐户中的资源。清理包括安全删除与 Workload Factory 帐户、FSx for ONTAP 文件系统、凭据、链接、通知通道以及相关 IAM、AWS Lambda 和 Amazon CloudWatch 资源关联的任何数据。该操作是不可逆的。

当您需要删除 Workload Factory 帐户时，您必须 ["请联系 NetApp 支持人员。"](#)

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。