安全模式和责任

Information Security for Workload Factory

NetApp
September 16, 2026

目录

安全模式和责任

了解 NetApp Workload Factory 的安全模型

NetApp Workload Factory 是一个 SaaS 控制平面，可帮助您管理和优化 AWS 环境中在 Amazon FSx for NetApp ONTAP 上运行的工作负载。安全成果取决于 NetApp、AWS 和您的组织之间的共同责任。

高级安全模型

- Workload Factory 使用 IAM assume-role 模型获取临时 AWS STS 凭据，以便在您的账户中调用 AWS API。
- 某些工作流程需要未通过 AWS API 公开的 ONTAP 原生操作；您可以使用客户部署的执行组件（例如 Lambda link）在 VPC 内执行这些操作。
- 可观测性信号（指标、遥测和运营记录）支持运营监控和调查。

关键审核问题

- Workload Factory 需要对您的 AWS 账户进行何种访问（角色信任 + 权限）？
- 哪些执行路径适用于您预期的工作流（仅 AWS API 或通过 VPC 组件的 ONTAP 原生操作）？
- 处理哪些数据类别（配置/元数据、操作日志/事件、遥测）以及它们存储在哪里？
- 存在哪些监控信号，它们的保留特性是什么？

下一步

- "NetApp Workload Factory 的责任共担边界"
- "NetApp Workload Factory 的连接和信任路径"
- "适用于 NetApp Workload Factory 的最小特权权限层级"

NetApp Workload Factory 的责任共担边界

NetApp Workload Factory 的安全责任在 NetApp（SaaS 运营）、AWS（云基础设施和托管服务）和您（客户配置）之间共同承担。了解各方责任的起点和终点，有助于您正确配置 AWS 环境并避免安全漏洞。这些界限明确了 NetApp 负责运营的内容、AWS 负责保护的内容，以及您必须自行配置和维护的内容。

NetApp 职责（服务方）

NetApp 负责运营和保护 Workload Factory SaaS 平台。这包括对存储的配置引用和操作数据的服务端处理。

AWS 职责（云平台）

AWS 负责您的部署和工作流使用的云基础架构和托管服务的安全性（例如，IAM/STS、FSx for ONTAP

、CloudWatch、KMS、Secrets Manager、CloudFormation、Lambda 和网络基元）。

客户责任（您的配置）

您有责任：

- AWS IAM 角色、信任策略和最低权限
- VPC 控制（子网、安全组、路由、端点和出口）
- 凭据治理（如果工作流需要，包括 ONTAP 凭据）
- 加密和密钥管理决策（例如，适用于 FSx for ONTAP 的可选客户管理 KMS 密钥）
- 监控、警报、保留策略和事件响应流程

要捕获的证据

- IAM 角色信任关系（包括外部 ID 条件）
- IAM 权限层选择和策略构件
- 网络边界决策（仅 AWS API 与 VPC 执行组件（如 Lambda 链接））
- 可观察性决策和保留预期
- AI 启用决策（除非明确禁用，否则默认情况下启用 AI 诊断）

NetApp Workload Factory 入职安全工作流程

加入 NetApp Workload Factory 可在您开始使用产品之前建立对 AWS 环境的安全访问。该流程结合了 AWS 信任配置、权限范围界定、连接设置、可观察性验证以及可选的 AI 诊断启用。

步骤 1：确定您的引导方式

- 识别 AWS 账户和环境边界（例如，生产环境与非生产环境的分离）。
- 确定所需的工作流（只读发现与预置与 ONTAP 原生操作）。
- 根据工作流需求决定是否部署 VPC 执行组件（例如 Lambda link）。
- 决定是否启用 AI 诊断（默认情况下启用）。

相关信息

- "凭据类型"
- "Lambda 链接概述"
- "AI 控制概述"

步骤 2：建立 AWS 信任和访问

1. 在您的 AWS 账户中部署 IAM 角色。
2. 使用信任策略中的外部 ID 限制角色代入。

3. 在 Workload Factory 中注册角色 ARN 和外部 ID。

相关信息

"AWS 帐户集成"

步骤 3：应用最小特权权限

1. 选择支持预期工作流程的最低权限层。
2. 验证每个请求会话策略是否将操作限制为正在执行的操作。

相关信息

"适用于 NetApp Workload Factory 的最小特权权限层级"。

步骤 4：配置连接和 VPC 边界（根据需要）

1. 验证 AWS 端点所需的网络路径。
2. 如果需要 ONTAP 原生操作，请在 VPC 中部署并验证相应的执行选项。

相关信息

- "NetApp Workload Factory 的连接和信任路径"
- "适用于 NetApp Workload Factory 的 ONTAP 执行选项"

第 5 步：验证可观察性

1. 确认指标和遥测数据按预期收集和保留。
2. 确认您可以访问所需的操作记录以进行故障排除和调查。

相关信息

- "NetApp Workload Factory 的可观察性概述"
- "NetApp Workload Factory 的指标和遥测"

步骤 6：启用 AI 诊断（可选）

默认情况下，AI 诊断处于启用状态。如果启用此功能，请验证您是否满足前提条件并将范围权限限制为所需的最低权限。

相关信息

- "Bedrock 选择加入 NetApp Workload Factory AI 诊断"
- "NetApp Workload Factory 的 AI 工具边界"

NetApp Workload Factory 的合规性和安全态势

NetApp Workload Factory 以合规性和安全性为核心优先事项。Workload Factory 中的所有工作负载均在 Amazon FSx for NetApp ONTAP 上运行。除 "AWS 安全功能" 之外，NetApp Workload Factory 还具有 "SOC2 Type 1、SOC2 Type 2 和 HIPAA 合规性"。

Amazon FSx for NetApp ONTAP for NetApp Workload Factory 是"用于部署企业应用的 AWS 解决方案"，它遵循 AWS Well-Architected 最佳实践。