



架构和连接性

Information Security for Workload Factory

NetApp
September 16, 2026

目录

- 架构和连接性 1
 - NetApp Workload Factory 的连接和信任路径 1
 - 连接路径 1
 - 连接组（协议、端口和身份验证） 3
 - 摘要：VPC 的网络要求 4
 - 适用于 NetApp Workload Factory 的 ONTAP 执行选项 5
 - 执行选项 5
 - 安全注意事项 5
 - 相关信息 5

架构和连接性

NetApp Workload Factory 的连接和信任路径

NetApp Workload Factory 与 AWS API、客户 AWS 帐户资源、AWS Lambda 链接和 Amazon Bedrock 进行通信，每个都有自己的协议、端口和身份验证方法。这些连接被组织成分组，将 AWS 管理平面、ONTAP 数据平面和 Lambda 链接流量分开，以便您可以独立评估信任边界。

连接路径

Workload Factory 建立了几条不同的连接路径，每条路径都用于发现、配置和管理 AWS 和 ONTAP 资源的特定目的。有些路径源自 Workload Factory 本身，使用假定的 AWS 凭据，而其他路径则通过 Lambda link 运行，该链接在您的 VPC 内部运行，以访问 ONTAP 管理端点，而无需将其公开暴露。通往 Amazon Bedrock 的可选路径支持 AI 辅助诊断，仅在您的组织启用该功能时才处于活动状态。

以下各节将介绍每条路径，包括所涉及的 AWS 或 ONTAP API、使用的凭据或身份验证以及确定路径是否处于活动状态的任何条件。了解这些路径有助于您评估 Workload Factory 所需的网络访问和权限，以及数据跨越帐户或 VPC 边界的位置。

Workload Factory 到 AWS API

Workload Factory 使用 `DescribeFileSystems`、`DescribeVolumes`、`CreateVolume`、`UpdateVolume`、`DeleteVolume`、`CreateFileSystem`、`CreateBackup`、`DescribeBackups` 和 EC2/VPC API 进行子网和安全组发现。

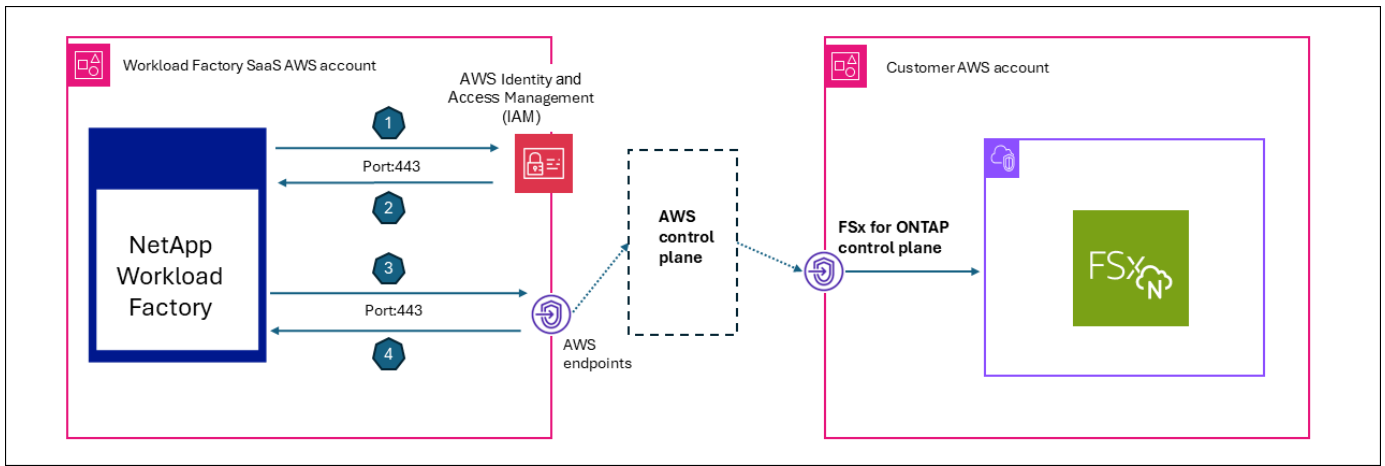
- 收集器服务大约每五小时扫描一次。
- CRUD 操作按需运行。
- 所有调用均使用带有外部 ID 的 STS 假定临时凭据。

Workload Factory 到客户 AWS 帐户资源（编排和自动化）

Workload Factory 与 AWS 交互以进行通信和创建资源。编排和自动化有几种方式。

- AWS CloudFormation 模板：Workload Factory 使用 AWS CloudFormation 模板来创建角色和文件系统等资源。例如，当您在用户界面中创建文件系统时，Workload Factory 会直接调用 CloudFormation 并将您重定向到您的 AWS 帐户。
- AWS API 调用：Workload Factory 使用 AWS API 调用 (`STS AssumeRole`) 为 FSx for ONTAP 相关活动发送 API 命令。
- AWS Lambda：NetApp Workload Factory 使用 CloudFormation 为与 ONTAP 通信的链接部署 AWS Lambda 函数。

下图显示了 Workload Factory 如何利用 NetApp AWS 帐户与具有 FSx for ONTAP 文件系统的客户 AWS 帐户之间的信任关系。



1. Workload Factory 使用来自 AWS IAM 服务的特定客户外部 ID 请求 AWS STS AssumeRole。
2. AWS IAM 服务检索角色并创建会话。
3. Workload Factory 发出具有会话权限的 AWS API 请求。
4. Workload Factory 接收来自 FSx for ONTAP 控制平面的 AWS API 响应。

Lambda 到 ONTAP 管理端点的连接

Lambda 链接在客户 VPC 内部运行，用于私有子网访问，而不会公开暴露 ONTAP。从链接到 ONTAP 管理端点的所有连接均仅为出站连接，因此不需要进站连接或暴露端点。此链接仅用于 Amazon FSx for NetApp ONTAP API 不会公开的 ONTAP 原生操作。

Workload Factory 对卷、存储 VM 和集群操作以及只读诊断和性能数据使用以下协议：

- HTTPS/443 (REST)
- SSH/22 (CLI)

Lambda 链接到 AWS Secrets Manager (ONTAP 凭据检索)

仅当 ONTAP 管理员凭据存储在 AWS Secrets Manager 中时使用（替代方案：使用信封加密在 Workload Factory 中加密的凭据）。

- 代理转发器在标头中传递 `x-aws-secret-arn` (Base64 编码)。
- Lambda 链接在执行时调用 `GetSecretValue` 以检索密码。

这将密码保留在您的账户边界内，并防止从 Workload Factory 传输。

Workload Factory 和客户组件到 Amazon Bedrock (AI 诊断)

仅当启用了 AI 诊断时，才会使用此路径。

- 事件分析器使用此路径进行 EMS 分析和延迟诊断。
- Bedrock 使用您假定的凭据和推理配置文件 ARN 运行，因此数据不会流向 NetApp 的帐户。

发送到 Bedrock 的数据可以包括 EMS 事件 JSON、QoS 统计、卷配置、聚合数据和节点信息。仅当为每个组织配置了推理配置文件时，路径才处于活动状态 (`ai_analyzer_config` 表)。

连接组（协议、端口和身份验证）

A 组 — AWS 管理平面信任路径（假定凭据）

连接	协议	端口	方向	身份验证	理由
STS AssumeRole	HTTPS	443	WF → AWS STS (客户帐户)	IAM 凭据 + ExternalId	获取临时跨账户凭据
FSx API (描述/创建/更新/删除)	HTTPS	443	WF → AWS FSx 端点 (客户区域)	STS 临时凭据	文件系统和卷生命周期管理
EC2/VPC API	HTTPS	443	WF → AWS EC2 端点	STS 临时凭据	安全组、子网和 VPC 发现
CloudFormation API	HTTPS	443	WF → AWS CFN 端点	STS 临时凭据	IAM 角色和 FSx 配置的堆栈部署
Secrets Manager GetSecretValue	HTTPS	443	WF → AWS Secrets Manager 端点 (客户帐户)	STS 临时凭据	检索 ONTAP 管理员密码 (当 Secrets Manager 存储时)
KMS加密/解密	HTTPS	443	WF → AWS KMS 端点	STS 临时凭据	卷加密密钥操作

所有 AWS API 调用都使用客户的区域端点，如果已配置，可以通过 VPC 端点进行路由。

B 组 — ONTAP 数据平面

ONTAP 数据平面始终通过 Lambda 链接进行代理；Workload Factory 服务从不直接连接到 ONTAP。

连接	协议	端口	方向	身份验证	理由
ONTAP REST API	HTTPS	443	链接 (客户 VPC) → ONTAP 管理 LIF	基本身份验证 (用户名/密码) 或 Secrets Manager ARN	集群、卷和存储 VM 配置 ; QoS; EMS 事件; ARP 状态
ONTAP SSH CLI	SSH	22	链接 (客户 VPC) → ONTAP 管理 LIF	密码认证	诊断命令 (QoS 统计、df、 事件日志、效率)

代理转发器的路由策略（优先级顺序）：

1. 显式 `x-link-id` 标头：从数据库中查找 Lambda ARN
2. 目标 ID (FSx 文件系统 ID)：查找关联的链接
3. 控制台代理 ID：通过消息代理路由到控制台代理

组 C — AWS Lambda 链接（部署在您的 VPC 中）

连接	协议	端口	方向	身份验证	理由
Lambda 调用	HTTPS (AWS SDK)	443	WF → AWS Lambda API (客户帐户)	IAM (lambda:InvokeFunction)	从客户 VPC 中执行 ONTAP REST/SSH 命令
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda (客户 VPC) → ONTAP 管理 LIF	基本身份验证/密码	通过私有子网访问 ONTAP，无需公开暴露

D 组 — NetApp Console Agent (VPC 中的 EC2，仅出站)

连接	协议	端口	方向	身份验证	理由
代理轮询	HTTPS	443	控制台代理 (客户 VPC) → WF 消息代理	不记名令牌 (occm-access-scope)	长时间轮询挂起的 ONTAP 命令 (7 秒超时；重新连接)
代理响应	HTTPS	443	控制台代理 (客户 VPC) → WF 消息代理	Bearer 令牌	返回 ONTAP 命令结果 (可选 zlib 压缩)
控制台代理 → ONTAP	HTTPS + SSH	443, 22	控制台代理 (客户 VPC) → ONTAP 管理 LIF	基本身份验证/密码	执行代理的 ONTAP 操作

关键设计：Workload Factory 从不向 Console 代理发起入站连接。工作在 Redis 流中排队；Console 代理轮询 GET /messagebroker/v1/requests 并响应 POST /messagebroker/v1/responses。

组 E — CloudFormation 自定义资源回调

连接	协议	端口	方向	身份验证	理由
CloudFormation → WF Lambda	HTTPS	443	CloudFormation (客户) → WF Lambda (NetApp)	JWT 令牌 + 引用令牌	报告 IAM 角色创建状态并传回角色 ARN
ONTAP CloudFormation 资源提供程序 → 链接	HTTPS	443	CloudFormation 资源 Lambda (客户) → 链接 Lambda (客户)	身份与访问管理	在堆栈操作期间创建/更新/删除 ONTAP 资源

摘要：VPC 的网络要求

组件	入站	出站
FSx for ONTAP	来自 Link Lambda 或控制台代理安全组的端口 443 和 22	不适用
链接 Lambda	无	端口 443 (ONTAP、AWS APIs) 和端口 22 (ONTAP SSH)

组件	入站	出站
控制台代理 EC2	无	端口 443（WF 端点、ONTAP、AWS APIs）和端口 22（ONTAP SSH）
VPC端点（可选）	不适用	STS、FSx、S3、Secrets Manager、Lambda、CloudFormation

客户 VPC 中的任何组件都不需要入站互联网访问。所有连接都是出站发起的（控制台代理轮询）或通过 AWS 服务 API 调用（Lambda Invoke）。

适用于 NetApp Workload Factory 的 ONTAP 执行选项

某些 NetApp Workload Factory 工作流需要 ONTAP 原生操作，这些操作未通过 AWS API 公开。Workload Factory 提供两种执行选项，可将这些操作保持在 AWS 账户边界内：从 VPC 内运行 ONTAP 操作的 Lambda 链接，以及使用来自 EC2 实例的仅出站连接的 NetApp Console Agent。这两个选项都允许您在安全模型范围内执行所需的 ONTAP 操作，同时将网络、凭据和生命周期决策保留其中。

执行选项

Lambda 链接（VPC 中的 AWS Lambda）

在 VPC 内执行 ONTAP REST 和只读 ONTAP CLI 诊断，而不公开 ONTAP。

NetApp Console Agent（VPC 中的 EC2，仅出站）

执行代理的 ONTAP 操作，其中代理启动出站连接，而 Workload Factory 从不向代理发起入站连接。

安全注意事项

- 网络边界：确认所需的出站端口（443/22）和目的地。
- 凭据边界：决定 ONTAP 凭据是存储在 Workload Factory（信封加密）还是从 AWS Secrets Manager 引用。
- 可审核性：确认组件活动和故障的操作记录。
- 生命周期管理：确认更新和删除的发生方式。

相关信息

- ["NetApp Workload Factory 的 Lambda 链接概述"](#)
- ["NetApp Workload Factory 的连接和信任路径"](#)
- ["NetApp Workload Factory 的加密和密钥管理"](#)

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。