



ONTAP 操作和 Lambda 链接（客户 VPC 组件）

Information Security for Workload Factory

NetApp
September 16, 2026

目录

- ONTAP 操作和 Lambda 链接（客户 VPC 组件） 1
 - 了解 NetApp Workload Factory 的 Lambda 链接 1
 - 链路安全架构 1
 - Lambda 链接与 NetApp Console 代理 2
 - 相关信息 2
 - Lambda 链接端口和 NetApp Workload Factory 调用 2
 - 请求类型 3
 - 出站网络边界 3
 - Workload Factory 调用 Lambda 链接 3
 - 相关信息 3
 - NetApp Workload Factory 的 Lambda 链接 IAM 权限 3
 - Lambda 执行角色权限 3
 - Workload Factory 调用权限 4
 - NetApp Workload Factory 的 Lambda 链接生命周期 4
 - 生命周期控制点 4

ONTAP 操作和 Lambda 链接（客户 VPC 组件）

了解 NetApp Workload Factory 的 Lambda 链接

NetApp Workload Factory 使用 *link*（部署在 VPC 中的 AWS Lambda 函数），在 Amazon FSx for NetApp ONTAP API 未公开这些操作时，将 ONTAP 原生操作保留在 AWS 账户边界内。链接在您的子网和安全组中运行，因此执行组件保留在您的 AWS 环境中。Workload Factory 仅针对需要直接访问 ONTAP 的操作调用链接，而非可用的 AWS 服务 API。它将链接的架构与 NetApp Console 代理的安全和操作配置文件进行比较。

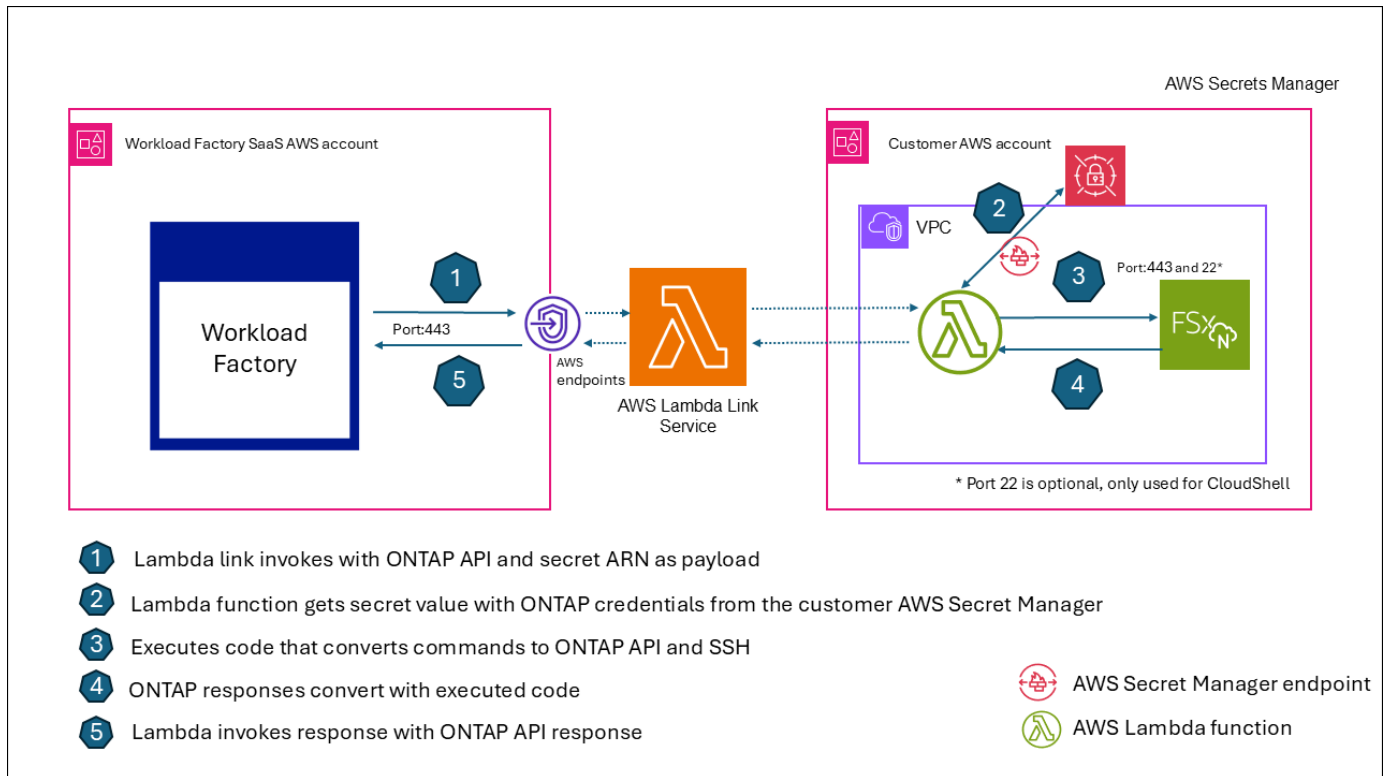
链路安全架构

Workload Factory 链接在 Workload Factory 帐户与一个或多个 FSx for ONTAP 文件系统之间创建信任关系和间接连接。

下表概述了 Lambda 链接安全架构。使用此信息了解如何在 AWS 账户中部署和执行 Lambda 函数，包括其网络配置、运行时环境和操作限制。

属性	详细信息
计算	AWS Lambda（容器映像）
运行时	Node.js 22
部署	CloudFormation 堆栈到您的 AWS 账户中
VPC 放置	您的子网、安全组
超时	每次调用 10 秒
调用	同步 (RequestResponse)
软件包类型	容器镜像（来自 NetApp ECR）

下图显示了 Lambda 链接的安全架构。



Lambda 链接与 NetApp Console 代理

Lambda 链接和 NetApp Console 代理用途不同，具有不同的安全性和操作性影响。

维度	链接（基于 Lambda）	NetApp Console 代理（基于 VM/Pod）
运行时模型	无服务器（AWS Lambda），客户部署	客户部署的VM/容器；运行NetApp控制台服务Pod
主要范围	控制平面 ONTAP REST 操作（仅当 AWS API 不支持此操作时）	业务流程加上对数据服务的支持
数据服务支持	不托管数据服务	可以托管数据服务（运行 NetApp 控制台服务 Pod）
运营开销	无始终在线的虚拟机	虚拟机生命周期管理和升级

相关信息

要查看完整的跨系统连接图，请参阅 ["NetApp Workload Factory 的连接和信任路径"](#)。

Lambda 链接端口和 NetApp Workload Factory 调用

NetApp Workload Factory 使用 Lambda 链接请求和端口边界来定义所需的出站连接和 IAM 授权调用。该链接支持到 ONTAP 管理端点的 HTTPS 请求、用于诊断的只读 SSH 命令和运行状况检查。所有连接都是从 VPC 内的链接出站，因此不需要入站连接或公开的端点。Workload Factory 使用基于 IAM 的授权通过 AWS Lambda API 调用链接。

请求类型

- HTTPS (ONTAP REST API) : 将 HTTPS 调用代理到 ONTAP 管理端点 (端口 443) , 用于卷、存储 VM 和集群操作。
- SSH (ONTAP CLI) : 在端口 22 上执行用于诊断和性能数据的只读 ONTAP CLI 命令。
- 运行状况检查: 返回状态和支持的功能。

出站网络边界

方向	端口	目标	目的
出站	443	ONTAP 管理 IP (在您的 VPC 内)	REST API 操作
出站	22	ONTAP 管理 IP (在您的 VPC 内)	SSH 命令行界面命令
出站	443	AWS Secrets Manager 端点 (可选)	使用 Secrets Manager 时的凭据检索

无需入站连接。该链接不会公开任何端点。Workload Factory 使用 `AWS lambda:InvokeFunction` API 调用它。

Workload Factory 调用 Lambda 链接

Workload Factory 通过 AWS Lambda API(`lambda:InvokeFunction`) 使用基于 IAM 的授权调用 Lambda 链接。

调用负载包含:

- 目标 ONTAP 管理端点 (IP/主机名)
- 要执行的操作 (REST API 路径或 SSH 命令)
- 身份验证信息 (内联凭据或 Secrets Manager ARN 参考)

相关信息

要查看完整的跨系统连接图, 请参阅 ["NetApp Workload Factory 的连接和信任路径"](#)。

NetApp Workload Factory 的 Lambda 链接 IAM 权限

NetApp Workload Factory 使用 Lambda 链接权限边界来定义 Lambda 执行和 Workload Factory 调用所需的 IAM 访问。这些权限是可选的, 但 ONTAP 原生操作需要这些权限。当您配置 Secrets Manager 支持时, 链接在运行时直接从 AWS Secrets Manager 检索 ONTAP 凭据, 密码仅在 VPC 内从 Secrets Manager 传输到 Lambda 函数, 然后传输到 ONTAP 端点。

要了解请求路径和端口要求, 请参阅 ["Lambda 链路端口和调用"](#)。

Lambda 执行角色权限

在 VPC 中部署链接时, Lambda 执行角色需要以下权限:

权限	目的
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	标准 VPC 连接的 Lambda 网络
ec2:AssignPrivateIpAddresses / ec2:UnassignPrivateIpAddresses	VPC ENI IP 管理
secretsmanager:GetSecretValue（作用域为 FSxSecret*）	检索 ONTAP 凭据（仅在启用 Secrets Manager 时）
CloudWatch 日志（托管策略）	Lambda 执行日志记录

Workload Factory 调用权限

Lambda 链接基于资源的策略授予 NetApp Workload Factory 服务主体以下权限：

权限	目的
lambda:InvokeFunction	执行 Lambda
lambda:GetFunction	运行状况和状态检查
lambda:UpdateFunctionCode	版本升级（映像更新）
lambda:GetFunctionConfiguration	配置验证

NetApp Workload Factory 的 Lambda 链接生命周期

NetApp Workload Factory 使用 Lambda 链接生命周期控制来管理部署、运行状况监控和受控映像更新，同时将操作风险降至最低。您可以使用 `lambda:UpdateFunctionCode` 权限更新 Lambda 链接容器映像以部署改进或安全修补程序，而无需重新部署 Amazon CloudFormation 堆栈。生命周期控件还定义了如何监控链接运行状况，以及在不再需要 Lambda 链接及其相关资源时如何将其删除。

生命周期控制点

- 部署：通过 Amazon CloudFormation 或 Terraform 堆栈部署实现自动化
- 监控：运行状况检查检测连接问题；故障计数器跟踪可靠性
- 删除：删除 CloudFormation 堆栈会从 AWS 帐户中删除 Lambda 和相关资源

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。