NetApp Workload Factory 的信息安全

Information Security for Workload Factory

NetApp
September 16, 2026

目录

了解 NetApp Workload Factory 的信息安全

信息安全是 NetApp Workload Factory 设计和运营的核心部分。信息安全、云平台和存储团队可以使用这些详细信息来评估和引入 Workload Factory，以支持企业安全要求。

什么是 NetApp Workload Factory

Workload Factory 是一个 SaaS 生命周期管理平台，旨在帮助您使用 Amazon FSx for NetApp ONTAP 优化和管理工作负载（例如存储、VMware 迁移、EDA 项目和数据库环境）。您的工作负载在 AWS 中运行。

Workload Factory 将 AWS API 用于通过 AWS 原生提供的所有 FSx for ONTAP 操作，并将 ONTAP REST API 用于平台支持但无法通过 AWS API 原生提供的 Workload Factory 操作。

本指南中使用的核心安全原则

保密
: 通过身份控制、最小权限、加密和网络边界保护数据免受未经授权的访问。

完整性
: 使用权限范围、更改控制和可审核性来保护系统和配置免受未经授权或意外的更改。

可用性
: 通过弹性 AWS 设计和运营监控，确保授权用户可以访问服务和工作负载。

本指南涵盖的信息类型

以下各节提供相关信息，帮助您以符合企业安全要求的方式评估和加入 Workload Factory。

1. 安全模式和责任
   - "安全模型概览"
   - "共同责任界限"
2. 架构和连接性
   - "连接和信任路径"
   - "ONTAP 执行选项"
3. 身份、凭据和最低权限
   - "AWS 帐户集成"
   - "最小权限层级"
4. 数据治理、隐私和生命周期
   - "数据处理和驻留"
   - "帐户删除核对清单"
5. 可观察性和监测

    - "指标和遥测"
6. AI 控件和 VPC 组件
    - "AI 控制概述"
    - "Lambda 链接概述"

快速入门

- 请从_view、planning 和 analysis_（只读）权限开始，并仅根据需要扩展。
- 使用 AWS CloudTrail 验证集成角色 `sts:AssumeRole`的活动。
- 提前决定是否需要部署 Lambda 链接或 NetApp Console 代理的 ONTAP 原生操作。
- 预先决定是否允许生成式 AI，以及驻留限制是否需要单区域推理配置文件。

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。

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。

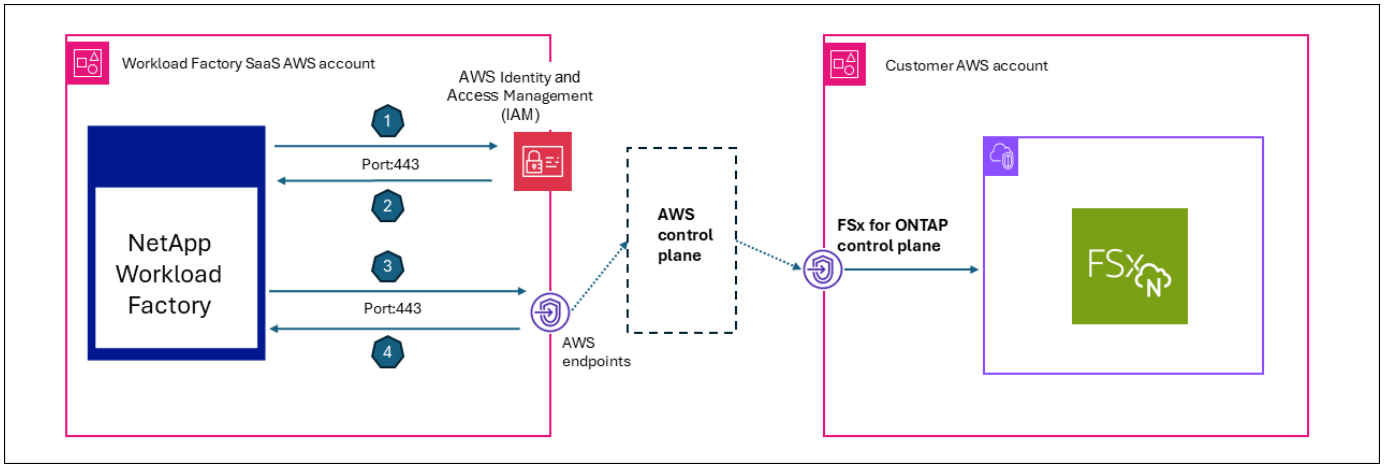
- 收集器服务大约每五小时扫描一次。
- CRUD 操作按需运行。
- 所有调用均使用带有外部 ID 的 STS 假定临时凭据。

Workload Factory 到客户 **AWS** 账户资源（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 账户。
- 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 账户与具有 FSx for ONTAP 文件系统的客户 AWS 账户之间的信任关系。



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，因此不需要入站连接或暴露端点。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"

身份、凭据和最低权限

适用于 NetApp Workload Factory 的 AWS 账户集成

Workload Factory 使用 AWS `sts:AssumeRole`为您的 AWS 账户获取临时凭据，因此服务不会存储长期 AWS 访问密钥。在入门过程中，您可以配置 IAM 角色，Workload Factory 可以使用该角色执行已批准的 AWS API 操作，并使用外部 ID 帮助防止未经授权的跨账户访问。然后，Workload Factory 在运行时使用生成的短期凭据，AWS 会在每次会话结束后自动使其过期。

AWS 帐户配置

要允许 Workload Factory 访问您的 AWS 账户：

1. 在您的 AWS 账户中部署 IAM 角色（使用 CloudFormation 或手动）。
2. 确保角色信任策略允许 Workload Factory 的服务主体代入该角色，并通过外部 ID 进行限制。
3. 使用外部 ID 作为客户和 Workload Factory 之间独占共享的唯一密钥标识符（UUID v4）。

   将其作为条件嵌入到您的 IAM 角色信任策略中 (`sts:ExternalId`）。

   外部 ID 可防止混淆代理攻击。在跨账户访问模型中，发现客户角色 ARN 的攻击者如果没有相应的外部 ID ，则无法代入该角色。AWS 建议将此模式用于第三方跨账户访问。有关详细信息，请参阅 AWS IAM 文档页面 "访问第三方拥有的 AWS 帐户"。

   外部 ID 在凭据载入期间生成一次，并与角色 ARN 一起加密存储在 Workload Factory 数据库中。
4. 在 Workload Factory 中注册角色 ARN 和外部 ID。

运行时

在运行时，Workload Factory 将承担您的 IAM 角色，以获取每个 AWS API 操作的短期凭据：

1. Workload Factory 调用 `sts:AssumeRole`时使用您的角色 ARN 和外部 ID。
2. AWS 返回临时凭据（访问密钥、私有密钥和会话令牌）。
3. Workload Factory 将临时凭据用于您账户中的 AWS API 操作。
4. 凭据会自动过期（默认情况下，一小时）。

AWS 凭据如何通过 NetApp Workload Factory 传输

AWS 凭据流描述了 NetApp Workload Factory 在入门和运行时操作期间如何处理角色标识符、外部 ID 和短期 AWS STS 凭据。在一次性设置期间，您需要在 AWS 账户中创建 IAM 角色，并配置需要 Workload Factory 服务主体和正确外部 ID 的信任策略。在运行时 ，Workload Factory 使用存储的角色 ARN 和外部 ID 来请求由每请求会话策略限定范围的临时凭据，并重用缓存的凭据，直到其过期。

一次性设置

对于一次性设置，流程如下所示：

步骤

1. 您可以在 AWS 帐户中启动 CloudFormation 堆栈或手动创建 IAM 角色。
2. IAM 角色信任策略指定了两个条件：
   a. 只有 Workload Factory 的服务主体才能担任该角色。
   b. 调用方必须提供正确的外部 ID。
3. Workload Factory 在其数据库中存储角色 ARN 和外部 ID（已加密）。

运行时（每个 **API** 操作）

在运行时，Workload Factory 使用存储的角色 ARN 和外部 ID 为每个 API 操作获取临时 AWS STS 凭据。此流程如下：

步骤

1. Workload Factory 从 MySQL 检索存储的角色 ARN 和外部 ID。
2. 它检查 Redis 中是否存在此角色的缓存临时 AWS STS 凭据集。
3. 在缓存未命中时，Workload Factory 调用 `sts:AssumeRole`角色 ARN 和外部 ID。该调用包括每个请求的内联会话策略，该策略将权限限制为仅限该操作所需的特定 AWS 操作。
4. AWS STS 返回带有过期时间戳的临时凭据（访问密钥 ID、秘密访问密钥、会话令牌）。
5. Workload Factory将这些凭据缓存在Redis中，并使用它们来调用目标AWS API。
6. 在缓存命中时，Workload Factory 会跳过 STS 调用并直接使用缓存的凭据。

会话策略

每个 STS 调用都包含一个内联会话策略，其范围限定为所需的最低 AWS 操作。

相关信息

- "最小权限层级"

AWS 凭据保留（适用于 NetApp Workload Factory）

Workload Factory 通过短期 AWS STS 凭据、加密角色元数据和有限保留行为来保护凭据处理。凭据模型将保留的角色元数据与用于 API 操作的临时 AWS 凭据分开。临时凭据仅在有限的时间内缓存，并在 AWS 强制执行下自动过期。删除凭据会阻止 Workload Factory 获取帐户的新凭据，而任何缓存的凭据很快就会过期。

关键行为

- Workload Factory 不存储长期 AWS 访问密钥。

Workload Factory 仅存储指针（角色 ARN）和共享密钥（外部 ID）。两者都不会自行授予 AWS 访问权限。

- 临时 AWS STS 凭据的最长硬性生存期为 1 小时（AWS 强制）。

  Workload Factory 在强制进行新的 STS 调用之前，最多将其缓存在 Redis 中 30 分钟。

- 如果缓存凭据集的剩余时间少于 15 分钟，Workload Factory 将丢弃该凭据集并获取新凭据集。
- 客户删除凭据会立即撤销 Workload Factory 访问该帐户的能力。

  下一次 AssumeRole 调用失败，缓存的凭据将在几分钟内过期。

保留和存储摘要

数据	存储位置	保留持续时间	自动过期？	删除方法
IAM 角色 ARN + 外部 ID	MySQL（静态加密）	无限期（存储，直到客户明确移除）	否	客户在 UI 中单击"删除凭据"
临时 AWS STS 凭据（访问密钥 + 密钥 + 会话令牌）	Redis（内存缓存）	最长 30 分钟（缓存 TTL）。基础 STS 凭据的有效期最长为一小时（AWS 默认值）。作为安全边际，缓存会在到期前五分钟逐出。	是（Redis TTL 自动删除；AWS 凭据过期由 AWS 强制执行）	自动
ONTAP 管理员密码	MySQL（使用 KMS 的 AES-256-CBC 信封加密）	无限期（存储，直到客户删除凭据或删除文件系统）	否	客户删除凭据，或文件系统删除触发清理
解密的 ONTAP 密码（明文）	仅在内存中（从不写入磁盘或缓存）	单个请求的持续时间（毫秒）	是（请求完成后进行垃圾回收）	自动

安全控制

- 外部ID可防止混淆副手攻击。
- 会话策略对每个请求强制执行最小权限原则。
- Workload Factory 在风险到期窗口之前刷新短期临时 AWS STS 凭据。
- 地区和账户类型的处理方式因标准、GovCloud 和中国环境而异。
- Workload Factory 从不存储长期 AWS 访问密钥。
- Workload Factory 绝不会修改您的 IAM 角色的权限。
- Workload Factory 永远不会超出您的角色策略所授予的权限范围。
- 会话策略只能减少权限；NetApp Workload Factory 永远不会扩展它们。

NetApp Workload Factory 的凭据类型

NetAppWorkload Factory 使用分离凭据模型来将 AWS 控制平面权限与直接 ONTAP 管理访问权限隔离开来。AWS IAM 角色向 AWS API 验证 Workload Factory 的身份，以进行文件系统管理、备份管理和资源发现等操作。ONTAP 凭据通过 Lambda 链接验证对 ONTAP 管理端点的直接访问，以进行需要管理配置或诊断的操作。当某些工作流结合了 AWS API 操作与直接 ONTAP 管理任务时，它们需要这两种凭据类型。

凭据类型

下表总结了 Workload Factory 中使用的两种凭据类型及其各自的身份验证目标。

凭据类型	验证到	用于
AWS 凭据（AssumeRole）	AWS APIs	通过 AWS FSx 服务 API 进行的所有操作
ONTAP 凭据（管理员密码）	ONTAP 管理端点	需要直接访问 ONTAP REST API 或 CLI 的操作

AWS 仅凭据操作

这些操作仅与 AWS API 交互，并且只需要 IAM 角色：

- 文件系统创建和删除
- 文件系统容量和吞吐量变化
- 备份创建和管理
- VPC、子网和安全组发现
- KMS密钥枚举
- CloudWatch 指标检索
- Cost Explorer 查询
- 使用 FSx API 进行标签管理

ONTAP 纯凭据操作

这些操作通过 Lambda 链接直接与 ONTAP 管理端点通信，并需要 ONTAP 管理员凭据：

- 卷级 QoS 策略配置
- 导出策略和规则管理
- 存储 VM 协议配置（NFS、CIFS、iSCSI）
- igroup 和 LUN 管理
- SnapMirror（复制）配置
- Snapshot 策略管理（ONTAP 级别）
- 性能诊断（QoS 统计、延迟细分）

- EMS 事件检索和分析
- 反勒索软件保护状态监控
- FlexCache 管理
- 网络接口(LIF)查询

同时需要 **AWS** 和 **ONTAP** 凭据的操作

工作流	**AWS** 凭据用于	**ONTAP** 凭据用于
基于 AI 的事件分析	调用 Bedrock，描述文件系统	检索 EMS 事件，使用 SSH 运行诊断
使用 Storage VM 设置创建文件系统	创建文件系统（AWS API）	配置 Storage VM 协议（ONTAP REST）
使用导出策略创建卷	创建卷（AWS API）	设置导出策略规则（ONTAP REST）
存储容量管理	更新文件系统容量 (AWS API)	检查聚合利用率（ONTAP SSH）

相关信息

- "ONTAP 执行选项"
- "Lambda 链接概述"

NetApp Workload Factory 的凭据存储选项

NetApp Workload Factory 支持保留最小权限并减少 ONTAP 管理机密泄露的凭据处理模式。AI 驱动的诊断功能在可用时使用只读 ONTAP 凭据，因此诊断代理可以在不修改存储环境的情况下进行观察和诊断。您可以使用 Workload Factory 管理的加密存储，或将 ONTAP 密码存储在 AWS Secrets Manager 中，并为 Workload Factory 提供参考。所做的选择会影响密码的存储位置、加密方式以及管理GovCloud支持和凭据轮换等要求的方式。

只读 **ONTAP** 访问模型

对于事件分析和延迟诊断等 AI 功能，Workload Factory 在可用时使用只读 ONTAP 凭据。只读凭据模型确保 AI 诊断代理无法对您的存储环境进行修改——它只能观察和诊断。

凭据存储选项比较

AWS 凭据

AWS 凭据始终通过 IAM 角色来获取。Workload Factory 可以在内部管理角色信息，也可以从 AWS Secrets Manager 引用角色信息。

选项	**AWS** 凭据	存储的内容	加密
Workload Factory 管理	IAM 角色 ARN + 外部 ID	IAM 角色 ARN + 外部 ID	角色 ARN 不是秘密（按原样存储）

ONTAP 凭据

Workload Factory 可以使用加密存储在内部管理 ONTAP 凭据，也可以从 AWS Secrets Manager 引用它们。该选择会影响密码的存储、加密和轮换方式。

Workload Factory 需要 ONTAP 凭据才能通过 "Lambda 链接" 与 ONTAP 文件系统 API 进行交互。

选项	**ONTAP** 凭据	存储的内容	加密
Workload Factory 管理	密码（加密）	ONTAP 管理员密码（加密）	ONTAP 密码使用 AES-256 信封加密
AWS Secrets Manager	Secrets Manager ARN 参考	Secrets Manager ARN	Secrets ARN 不是加密内容（按原样存储）；AWS Secrets Manager 会加密您账户中的密钥

其他注意事项

GovCloud 要求

使用标准 IAM 角色；ONTAP 凭据必须使用 Secrets Manager（不允许密码存储）。

旋转

角色策略已在您的账户中更新。在 Workload Factory 中更新 ONTAP 密码（托管选项），或在 AWS Secrets Manager 中轮换密码。

适用于 NetApp Workload Factory 的最小特权权限层级

您可以随时限制 Workload Factory IAM 权限，以符合最低权限要求，例如限制对特定资源 (ARN) 的访问以及应用 IAM 条件，例如标记和 CIDR 范围。

分层权限模型

Workload Factory 使用与最小权限原则对应的分层权限模型。您可以选择在添加 AWS 凭据时要启用的功能层。您可以从只读发现开始，并根据需要进行扩展。

Workload Factory 通过您 AWS 账户中的 IAM 角色授予所有权限，该角色通过带有外部 ID 的 STS 进行代入。

Workload Factory 使用内联会话策略进一步限定每个 API 调用的范围。

在 Workload Factory 控制台中，AI 聊天功能 *Ask Me* 可以通过建议限制选项并生成要在 AWS 中应用更新后的策略，帮助您安全地细化权限。

授予权限

将 AWS 凭据添加到 NetApp Workload Factory 时，您可以选择要启用的权限层。您可以随时启用或禁用层级。

层级是累积的：启用较高的层级会自动启用所有较低的层级。

安全控制

- 外部 ID（混淆代理人保护）
- 按操作会话策略（每个请求的最低权限）
- 基于标记的条件（安全组修改仅限于 Workload Factory 创建的资源）
- Secret ARN 范围（Secrets Manager 访问仅限于 `FSxSecret*`）
- 运行时权限验证（针对目标修正报告缺少操作/资源）

权限文档

Workload Factory 权限的主要参考是 Workload Factory 设置和管理文档中的 "权限参考"。您可以在此参考中找到有关从存储 IAM 策略中删除权限的影响的信息。

Amazon CloudWatch 监控 NetApp Workload Factory 的权限

Amazon CloudWatch 监控权限在 NetApp Workload Factory 中是可选的，仅在部署单独的监控堆栈时适用。监控堆栈通过收集文件系统指标、发布事件日志、管理 CloudWatch 仪表板和警报以及通过 Amazon SNS 发送警报通知来提供操作可见性。该堆栈还需要访问权限，以便在监控需要时检索 ONTAP 凭据。

所需 CloudWatch 监控权限

可选监控堆栈需要以下权限：

权限	目的
fsx:Describe* / fsx:ListTagsForResource	收集文件系统指标
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	管理仪表板和报警
logs:CreateLogGroup / logs:CreateLogStream / logs:PutLogEvents	发布事件日志
sns:Publish	发送警报通知
secretsmanager:GetSecretValue	检索 ONTAP 凭据以进行监控

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。"

可观测性（日志、指标、遥测）

了解 NetApp Workload Factory 中的可观察性

可观察性信号有助于支持运营监控、故障排除和调查。在 NetApp Workload Factory 中，可观察性包括指标、遥测和操作记录，这些记录提供了对服务行为、AI 使用情况以及通过 Workload Factory 执行的操作的可见性。遥测和操作记录支持内部监控和面向客户的审计可见性，Tracker 可帮助您查看受支持操作的进度、状态和详细信息。

遥测和运营记录

Workload Factory 使用以下遥测和操作记录类型：

- OpenTelemetry 追踪通过 OTLP HTTP 导出至 SigNoz（内部可观测性）
- AI 使用计量（令牌计数、模型成本）存储在 AWS Timestream 中
- NetApp Console 审核记录（操作名称、状态、请求/响应元数据、时间戳）

Workload Factory 中的审核日志记录

Workload Factory 提供了 Tracker，这是一项监控功能，可用于监控哪些操作正在运行以及何时运行。使用 Tracker，您可以跟踪 FSx for ONTAP、凭据和链接操作的进度和状态，查看操作任务和子任务的详细信息，并诊断任何问题或故障。

Tracker 中提供了几种操作。您可以按时间范围（过去 24 小时、7 天、14 天或 30 天）、工作负载、状态和用户筛选作业；使用搜索功能查找作业；并将作业表下载为 CSV 文件。

- "在 Workload Factory 中使用 Tracker 监控操作"

相关信息

- "NetApp Workload Factory 的指标和遥测"

NetApp Workload Factory 的指标和遥测

NetApp Workload Factory 在 AWS CloudWatch 中收集和存储卷级和文件系统级指标，为您提供存储性能和容量的操作可见性。计算指标（例如吞吐量）来自这些收集的值。了解指标定义、收集节奏、刷新行为和保留详细信息。

包含的指标

NetApp Workload Factory 将以下指标用于操作日志和事件：

- 卷级 CloudWatch 指标（按卷收集）
- 文件系统级 CloudWatch 指标（按文件系统收集）
- 计算指标

- 收集计划和保留

关于运营指标

计算指标使用以下公式：

- 吞吐量（字节/秒） = （NetworkSentBytes + NetworkReceivedBytes）/周期

刷新行为：

- 卷和集群指标每 12 小时刷新一次。
- 延迟指标每 20 分钟刷新一次。
- DynamoDB 项目在 14 天后自动过期。

关于遥测数据收集

- OpenTelemetry 追踪通过 OTLP HTTP 导出至 SigNoz（内部可观测性）
- AI 使用计量（令牌计数、模型成本）存储在 AWS Timestream 中
- NetApp Console 审核记录（操作名称、状态、请求/响应元数据、时间戳）

卷级 **CloudWatch** 指标（按卷收集）

指标	**AWS CloudWatch** 名称	单位	它所衡量的内容
卷存储容量	StorageCapacity	字节	已调配总容量
已使用的存储空间	StorageUsed	字节	实际存储的数据
数据读取字节	DataReadBytes	字节	读取吞吐量
数据写入字节	DataWriteBytes	字节	写入吞吐量
数据读取操作	DataReadOperations	计数	读取 IOPS
数据写入操作	DataWriteOperations	计数	写入 IOPS
元数据操作	MetadataOperations	计数	元数据 IOPS
数据读取操作时间	DataReadOperationTime	秒	读取延迟
数据写入操作时间	DataWriteOperationTime	秒	写入延迟
元数据操作时间	MetadataOperationTime	秒	元数据延迟

文件系统级 **CloudWatch** 指标

指标	**AWS CloudWatch** 名称	单位	它所衡量的内容
SSD存储容量	StorageCapacity	字节	SSD 层总容量
已使用 SSD 存储	StorageUsed (SSD 层)	字节	SSD 层消耗
已用容量池	StorageUsed（容量池）	字节	容量池消耗
CPU 利用率	CPU 利用率	百分比	文件服务器CPU

指标	**AWS CloudWatch** 名称	单位	它所衡量的内容
SSD容量利用率	StorageCapacityUtilization	百分比	已使用的 SSD 层百分比
网络吞吐量利用率	NetworkThroughputUtilization	百分比	已利用网络百分比
磁盘 IOPS 利用率	DiskIopsUtilization	百分比	已利用磁盘 IOPS 百分比
磁盘吞吐量利用率	FileServerDiskThroughputUtilization	百分比	已利用磁盘吞吐量百分比
磁盘 IOPS 利用率（服务器）	FileServerDiskIopsUtilization	百分比	服务器磁盘 IOPS 使用百分比
存储效率节省量	StorageEfficiencySavings	字节	效率节省的空间
已接收网络	NetworkReceivedBytes	字节	入站网络
网络已发送	NetworkSentBytes	字节	出站网络

收集计划和保留

时间范围	收集期间	数据点	存储	保留
1 天	24分钟	~60	DynamoDB	14 天（TTL）
1 周	~2.8小时	~60	DynamoDB	14 天（TTL）
1 个月	12 小时	~60	DynamoDB	14 天（TTL）
3 个月	~1.5 天	~60	DynamoDB	14 天（TTL）
1 年	~6 天	~60	DynamoDB	14 天（TTL）

生成式 AI 安全控制

了解 NetApp Workload Factory 中的 AI 控件

NetApp Workload Factory 包括生成式 AI 功能，可加速诊断，同时对模型访问、数据范围和运行时行为实施安全控制。

默认情况下，Workload Factory 启用 AI 诊断。您可以随时通过 Workload Factory **Administration** 设置禁用生成式 AI 功能。 "详细了解如何管理 GenAI 功能。"

安全范围的 AI 功能概述

Workload Factory 目前将生成式 AI 应用于以下功能：

- Ask Me 助手（RAG，包含精选 NetApp 文档，响应有来源支持）
- 延迟分析
- EMS 事件分析
- 错误日志分析

AWS Bedrock 概述（用于 AI 诊断）

Workload Factory 使用 Amazon Bedrock 进行 AI 推理。推理在您的 AWS 账户中运行，使用您配置的凭据和推理配置文件。

相关信息

- "Amazon Bedrock 选择加入 NetApp Workload Factory AI 诊断"
- "NetApp Workload Factory 的 AI 工具边界"
- "NetApp Workload Factory 的 AI 模型参数和计费"

Amazon Bedrock 选择加入 NetApp Workload Factory AI 诊断

NetApp Workload Factory AI 诊断使用 Amazon Bedrock 来分析事件，默认情况下该功能处于启用状态。在 Workload Factory 可以调用选定的 Bedrock 模型并收集诊断数据之前，您必须配置 IAM 权限、推理配置文件和具有 SSH 功能的已连接 Lambda 链接。如果这些组件中的任何一个缺失或 Bedrock 配置被删除，则 AI 诊断将不可用。

默认情况下，AI 诊断处于启用状态。

开始之前

- 确保您的帐户包含 AWS Bedrock 推理配置文件。
- 具有用于诊断数据收集的 SSH 功能的已连接 Lambda 链路。

步骤

1. 在您的 IAM 角色中授予 Bedrock 权限：
   - `bedrock:InvokeModel`
   - `bedrock:InvokeModelWithResponseStream`
   - `bedrock:ListInferenceProfiles`
   - `bedrock:GetInferenceProfile`
2. 在 Workload Factory 设置中配置推断配置文件 ARN。

如果缺少任何先决条件，系统将报告缺少的特定组件，AI 功能将保持非活动状态。

禁用 AI 诊断

要禁用 AI 诊断：

- 从您的 IAM 角色中删除 Bedrock 权限，或
- 在 Workload Factory 设置中删除 Bedrock 配置。

AI 诊断立即变为不可用，且不会发生任何残留数据处理。

区域和跨区域推理配置文件

Bedrock 推理在您的推理配置文件指定的 AWS 区域中执行。如果使用跨区域推理配置文件，AWS 可能会根据标准 AWS Bedrock 行为将请求路由到配置文件配置中的任何区域。数据不会离开 AWS 基础架构。

NetApp Workload Factory 的 AI 工具边界

NetApp Workload Factory 严格限制其 AI 功能与 AWS 和 ONTAP 环境的交互方式，因此您可以信任 AI 辅助诊断，而无需担心发生意外更改。Amazon Bedrock 使用只读的 AWS CLI 和 ONTAP CLI 诊断工具，这些工具会阻止变更命令并按大小和执行时间限制输出，所用的任何数据均为临时性数据，不会由 NetApp Workload Factory 或 AWS 保留。

工具安全控制

工具	功能	安全控制
AWS CLI（只读）	执行只读 AWS CLI 命令（ describe、list、get）	阻止所有变异动词（create、delete、modify 、update、put、remove）。每步最多 10 个命令。输出截断为 20 KB。
ONTAP CLI（只读）	使用 SSH 执行只读 ONTAP CLI 命令	阻止所有变异动词（DELETE、DESTROY 、CREATE、MODIFY、MOVE）。输出被截断。

代理无法修改、创建或删除资源。它只能观察和诊断。

数据保留和模型训练边界

根据 AWS 政策，Amazon Bedrock 不会存储或使用您的输入和输出来训练或改进基础模型。对于按需推理（由 Workload Factory 使用），AWS 会暂时处理您的数据，并在返回响应后不会保留数据。

NetApp Workload Factory 的 AI 模型参数和计费

NetApp Workload Factory 定义了与 AI 治理相关的模型配置、使用和计费边界。配置的模型使用确定性参数并返回结构化 JSON，以支持一致的分析结果。AWS 向您的账户收取 Amazon Bedrock 推理费用，而 Workload Factory 则跟踪 AI 使用情况并提供每个账户的每月成本可见性。这些部分描述了模型参数以及适用于 AI 消耗的限制。

型号和参数

参数	值
型号	Anthropic Claude（使用跨区域推理配置文件）
温度	0（确定性，无随机性）
最大输出令牌数	2,048
最大推理步骤	每次分析 15 次
输出格式	结构化 JSON（摘要、严重程度、根本原因、纠正措施）

账单和使用限制

- AWS 会将 Bedrock 推理费用计入您的账户（您的推理配置文件、您的凭据）。
- Workload Factory 在内部跟踪 AI 使用情况。
- Workload Factory 提供每个帐户的每月成本可见性。

  "在 NetApp Workload Factory 中跟踪存储成本"

Ask Me AI助手

适用于 NetApp Workload Factory 的 Ask Me 安全架构

Ask Me 是一款嵌入在 NetApp Workload Factory 中的生成式人工智能助手。它为 Amazon FSx for NetApp ONTAP 和 Workload Factory 主题提供实时对话支持。回复基于经过验证的 NetApp 文档，Ask Me 无法访问公共互联网或使用客户数据来训练模型。多个安全层有助于阻止恶意查询、限制对受支持域的响应，并防止用户输入覆盖系统指令。当 Ask Me 使用工具时，授权边界、只读查询强制执行、临时沙箱和审核日志记录有助于约束和监控执行。

您可以随时通过 Workload Factory 的 **Administration**（管理）设置退出 Ask Me，这将禁用针对您用户帐户的助手。"详细了解如何管理 GenAI 功能。"

Ask Me 中的 **RAG** 架构

Ask Me 使用检索增强生成（RAG）。

- 精心策划的知识库：回复基于经过验证的已发布 NetApp 文档的托管语料库。
- 检索评分和过滤：模型上下文中仅包含足够相关的内容。
- 无法访问互联网：模型无法获取、浏览或抓取外部内容。
- 源归因：回复包括对所用源文档的引用。

多层提示安全

- 第1层：安全分类器（LLM-as-a-judge）拦截恶意查询（提示注入、权限升级、数据泄露、社交工程、策略违规）。

  系统会记录被阻止的查询，生成模型永远不会看到这些查询。

- 第2层：系统提示强化可防止用户输入覆盖系统指令。
- 第 3 层：域范围限制将响应限定在 FSx ONTAP 和 Workload Factory 主题范围内。
- 第4层：工具使用治理在强化沙箱中验证参数并运行查询；模型无法执行任意操作。

模型数据隔离和隐私

- 不对客户数据进行模型训练
- 请求级隔离（无跨租户数据泄露）
- 具有有界历史记录的会话范围对话上下文
- 无持久模型内存
- 受管推理基础设施

工具使用和代理安全

- 授权范围的工具（强制执行用户权限边界）
- 严格的工具执行超时
- 用于检索数据的临时会话范围沙箱
- 使用允许列表实施只读查询
- 具有敏感参数清理功能的工具调用可审计性

适用于 **NetApp Workload Factory** 的 **Ask Me** 访问控制

在 NetApp Workload Factory 中，Ask Me 的访问安全核心在于运行时操作期间的身份验证会话、用户级问责制和受保护的密钥处理。身份验证控件会验证每个会话，并将交互与特定用户关联。敏感凭据在运行时从托管密钥保管库中检索，并从日志中清除。该服务还应用基础架构控制，包括非 root 容器执行和受限的 CORS 允许列表。

身份验证

- 带有加密验证的签名 JWT 身份验证（包括受众、颁发者和算法检查，如 RS256）
- 服务边界处中间件强制身份验证
- 用户身份范围界定，以便交互可归因于特定用户

凭据保护和密钥处理

- 安全保管库存储：服务使用的敏感凭据存储在托管密钥保管库中，并在运行时检索。应用程序代码、配置文件或容器映像中不存储任何机密。
- 日志清理：敏感值（凭据、令牌、密码、访问密钥、证书）在写入日志之前会从日志中隐去。

基础设施安全

- 非 root 容器执行
- CORS 限制为受信任的 NetApp 域的显式允许列表

适用于 **NetApp Workload Factory** 的 **Ask Me** 执行模式

NetApp Workload Factory 为 Ask Me 提供多种执行模式，每种执行模式具有不同的安全和隐私特性。当 Ask Me 使用工具集成时，例如查询客户自己的 Workload Factory 资源，工具执行通过分层保护进行控制。启用工具的执行在经过身份验证的用户权限内运行，并对每个操作的持续时间和范围施加限制。检索到的数据保留在阻止外部访问的临时会话沙箱中，并在会话结束时销毁。独立的提示和代码控制强制执行只读查询，而审核记录捕获工具活动并清除敏感值。

工具执行保障措施

- 授权范围的工具在经过身份验证的用户权限内运行。
- 工具执行超时限制长时间运行的操作。
- 临时数据沙箱在会话范围内存储工具检索的数据，在引擎级别阻止外部访问、文件 I/O、网络调用和扩展加载，并在会话结束时销毁。
- 只读查询强制执行通过严格的允许列表验证生成的查询。
- 提示执行和代码执行的安全性是独立应用的。
- 工具调用可审计性日志记录工具名称、参数、时间戳和结果状态，并对敏感值进行脱敏处理。

输出控制

- 令牌限制强制执行
- 分类/安全关键操作的确定性输出（温度 0）
- 提前终止和清理的流式传输

向我询问 **NetApp Workload Factory** 的隐私和可用性

在 NetApp Workload Factory 中，Ask Me 隐私控制可限制数据泄露、保持会话处理隔离，并维护用户交互的隐私边界。您的输入由托管 AI 服务处理，该服务不会使用这些输入来训练或改进基础模型。检索到的操作数据在会话期间保留在临时内存存储中，不会被持久化或共享。跨多个云区域的多模型回退链可在主模型受到限制或不可用时支持可用性，同时相同的安全控制也适用于回退模型。

数据处理和隐私

- 提示中的用户数据：由托管 AI 服务处理，不使用您的输入来训练或改进基础模型。
- 知识库内容：仅限精选、已发布的 NetApp 文档；您的数据不包括在内。
- 操作数据：仅在用户查询自己的资源时检索；在会话期间保存在临时内存存储中，不持久化或共享。
- 审核日志：记录查询元数据（匿名用户 ID、时间戳、持续时间），并清除敏感字段。
- 反馈数据：单独存储并链接到查询 ID，而非匿名用户 ID 以外的个人身份信息。

可用性和隔离控制

Ask Me 在多个云区域采用多模型后备链。

如果主模型受到限制或不可用，系统可以故障转移到其他模型。

所有模型均受相同的安全控制、系统提示加固和隔离保证。

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。

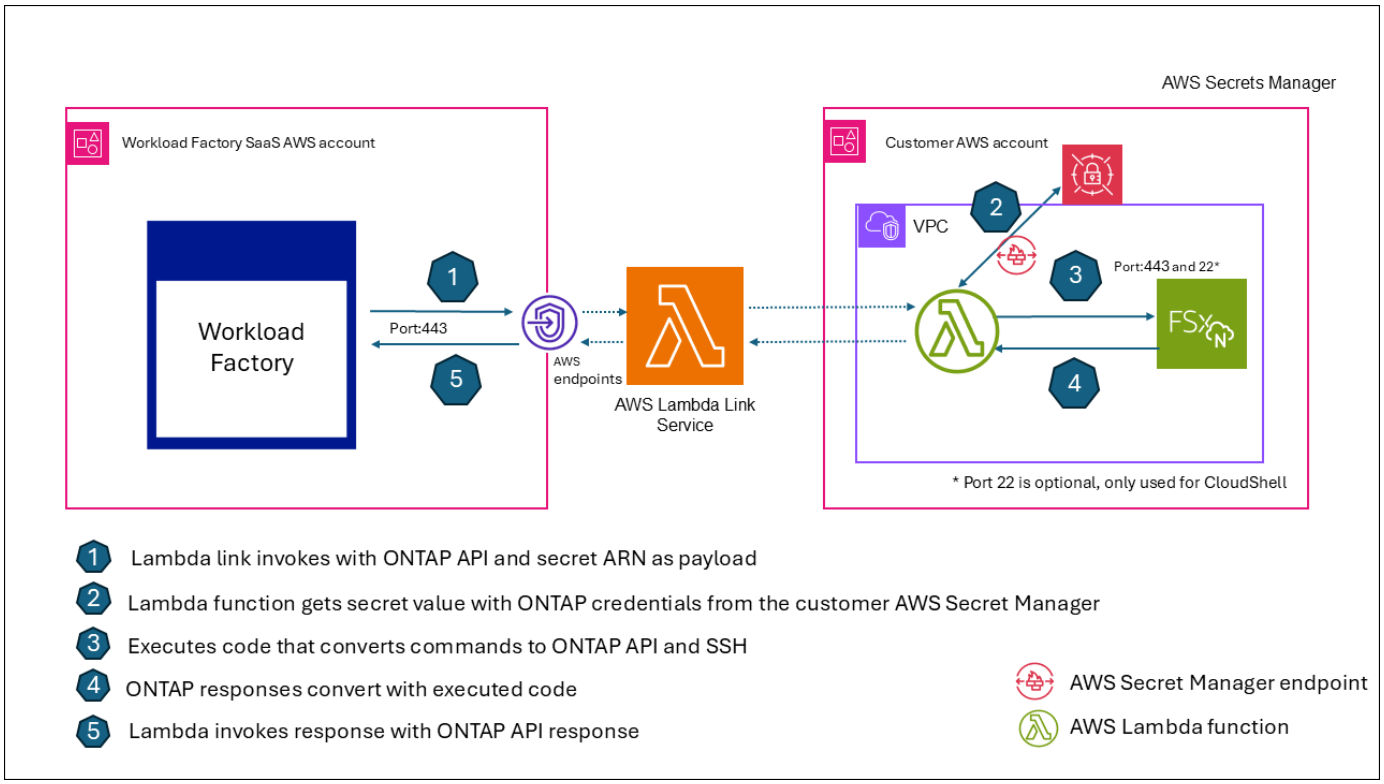
链路安全架构

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

知识和支持

向 NetApp 支持部门注册

在通过 NetApp 技术支持创建支持案例之前，您需要将 NetApp 支持站点帐户添加到 Workload Factory，然后注册以获取支持。

需要注册支持才能获得特定于 NetApp Workload Factory 及其存储解决方案和服务的技术支持。您必须从 NetApp Console 注册支持，NetApp Console 是独立于 Workload Factory 的基于 Web 的控制台。

注册支持不会为云提供商文件服务启用 NetApp 支持。有关与云提供商文件服务、其基础架构或使用该服务的任何解决方案相关的技术支持，请参阅该产品的 Workload Factory 文档中的"获取帮助"。

"Amazon FSx for ONTAP"

支持注册概述

注册您的帐户 ID 支持订阅（您的 20 位 960xxxxxxxxx 序列号位于 NetApp Console 的"支持资源"页面上）即作为您的单个支持订阅 ID。每个 NetApp 帐户级别的支持订阅都必须注册。

注册可启用打开支持工单和自动生成案例等功能。通过将 NetApp Support Site (NSS) 帐户添加到 NetApp Console 来完成注册，如下所述。

注册账号以获取 **NetApp** 支持

要注册支持并激活支持授权，您帐户中的一个用户必须将 NetApp Support Site 帐户与其 NetApp Console 登录相关联。如何注册 NetApp 支持取决于您是否已经拥有 NetApp Support Site (NSS) 帐户。

拥有 **NSS** 账号的现有客户

如果您是拥有 NSS 帐户的 NetApp 客户，只需通过 NetApp Console 注册即可获得支持。

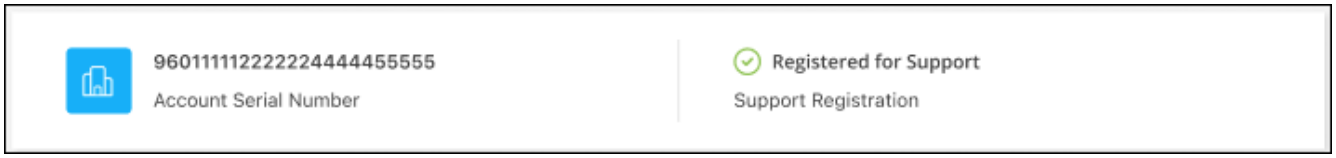
步骤

1. 在 Workload Factory 控制台的右上角，选择 **Help > Support**。

   选择此选项将在新浏览器选项卡中打开 NetApp Console，并加载支持仪表板。

2. 从 NetApp Console 菜单中，选择*管理*，然后选择*凭据*。
3. 选择*用户凭据*。
4. 选择*添加 NSS 凭据*，然后按照 NetApp 支持站点 (NSS) 身份验证提示操作。
5. 要确认注册过程是否成功，请选择"帮助"图标，然后选择 **Support**。

   *资源*页面应显示您的帐户已注册支持。



请注意，如果其他 NetApp Console 用户未将 NetApp 支持站点帐户与其 NetApp Console 登录相关联，则不会看到相同的支持注册状态。但是，这并不意味着您的 NetApp 帐户未注册支持。只要帐户中有一位用户执行了这些步骤，您的帐户即已注册。

现有客户，但没有 **NSS** 帐户

如果您是具有现有许可证和序列号但_无_ NSS 帐户的现有 NetApp 客户，则需要创建 NSS 帐户并将其与 NetApp Console 登录相关联。

步骤

1. 通过完成以下步骤创建 NetApp 支持站点帐户： "NetApp 支持站点用户注册表单"
   a. 请务必选择适当的用户级别，通常为 **NetApp** 客户/最终用户。
   b. 请务必复制上面用于序列号字段的 NetApp 帐户序列号（960xxxx）。这将加快账号处理速度。
2. 完成 拥有 NSS 账号的现有客户 下的步骤，将您的新 NSS 帐户与您的 NetApp Console 登录相关联。

全新接触 **NetApp**

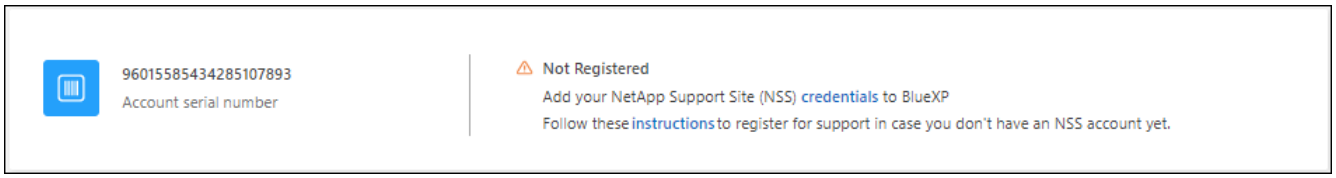
如果您是首次接触 NetApp 且没有 NSS 帐户，请按照以下步骤操作。

步骤

1. 在 Workload Factory 控制台的右上角，选择 **Help > Support**。

   选择此选项将在新浏览器选项卡中打开 NetApp Console，并加载支持仪表板。

2. 从"支持资源"页面找到您的账号 ID 序列号。



3. 导航到 "NetApp 的支持注册站点"并选择 我不是注册 **NetApp** 客户。
4. 填写必填字段（带红色星号的字段）。
5. 在*产品线*字段中，选择 **Cloud Manager**，然后选择适用的计费提供商。
6. 复制上述第 2 步中的账号序列号，完成安全检查，然后确认您已阅读 NetApp 的《全球数据隐私政策》。

   电子邮件将立即发送到所提供的邮箱，以完成此安全交易。如果验证电子邮件未在几分钟内到达，请务必检查垃圾邮件文件夹。

7. 从电子邮件中确认操作。

   确认将您的请求提交到 NetApp，并建议您创建 NetApp 支持站点帐户。

8. 通过完成以下步骤创建 NetApp 支持站点帐户： "NetApp 支持站点用户注册表单"
   a. 请务必选择适当的用户级别，通常为 **NetApp** 客户/最终用户。
   b. 请务必复制上面用于序列号字段的帐户序列号（960xxxx）。这将加快账号处理速度。

完成后

NetApp 应在此过程中与您联系。这是针对新用户的一次性引导练习。

拥有 NetApp 支持站点帐户后，请完成 拥有 NSS 账号的现有客户 下的步骤，将该帐户与您的 NetApp Console 登录相关联。

获取有关 FSx for ONTAP for NetApp Workload Factory 的帮助

NetApp 通过多种方式为 Workload Factory 及其云服务提供支持。全天候提供广泛的免费自助支持选项，例如知识库 (KB) 文章和社区论坛。您的支持注册包括通过 Web 票务系统获得远程技术支持。

获取 FSx for ONTAP 的支持

有关 FSx for ONTAP、其基础架构或使用该服务的任何解决方案的技术支持，请参阅该产品的 Workload Factory 文档中的"获取帮助"。

"Amazon FSx for ONTAP"

要获得特定于 Workload Factory 及其存储解决方案和服务的技术支持，请使用下面描述的支持选项。

使用自助服务选项

这些选项每周7天、每天24小时免费提供：

- 文档

  当前正在查看的 Workload Factory 文档。

- "知识库"

  搜索 Workload Factory 知识库以查找用于解决问题的有用文章。

- "社区"

  加入 Workload Factory 社区，关注正在进行的讨论或创建新的讨论。

创建 NetApp 支持案例

除了上述自助服务选项之外，您还可以在激活支持后与 NetApp 支持专家合作解决任何问题。

在开始之前

要使用*创建案例*功能，您必须首先注册支持。将您的 NetApp Support Site 凭据与您的 Workload Factory 登录名相关联。"了解如何注册以获取支持"。

步骤

1. 在 Workload Factory 控制台的右上角，选择 **Help > Support**。

选择此选项将在新浏览器选项卡中打开 NetApp Console，并加载支持仪表板。

2. 在*资源*页面上，在"技术支持"下选择一个可用选项：

   a. 如果您想与他人通话，请选择*致电我们*。您将被引导到 netapp.com/cn 上的一个页面，其中列出了您可以拨打的电话号码。

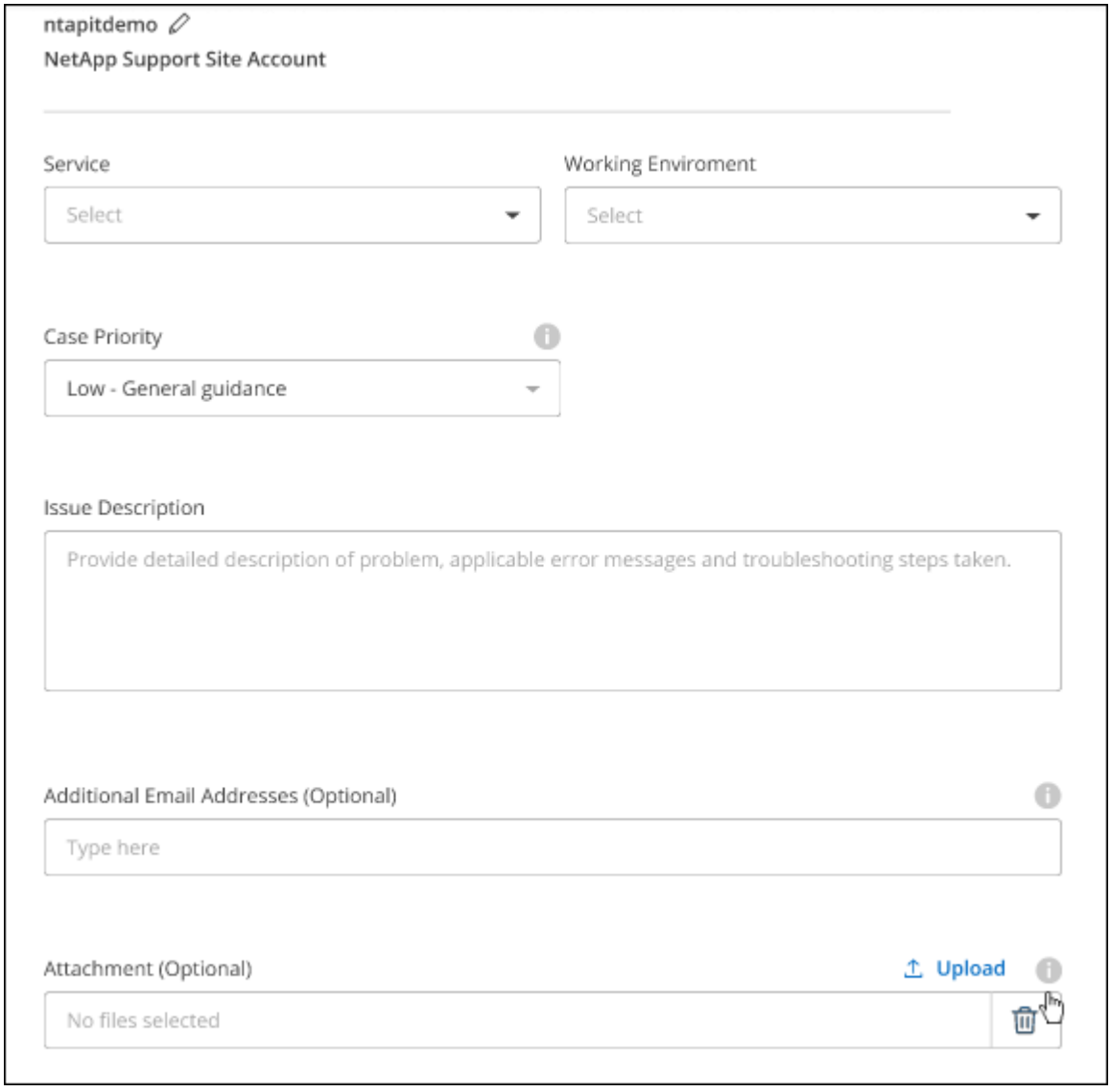
   b. 选择 创建个案 以向 NetApp 支持专员提交工单：

      - 服务：选择 **Workload Factory**。
      - **Case Priority**：选择案例的优先级，可以是低、中、高或严重。

        要了解有关这些优先级的更多详细信息，请将鼠标悬停在字段名称旁边的信息图标上。

      - 问题描述：请详细说明您的问题，包括任何适用的错误消息或您执行的故障排除步骤。
      - **Additional Email Addresses**：如果您想告知其他人此问题，请输入其他电子邮件地址。
      - 附件（可选）：上传最多五个附件，一次一个。

        每个文件的附件限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。



完成后

此时会弹出一个窗口，其中包含您的支持案例编号。NetApp 支持专家将审查您的案例并尽快与您联系。

有关支持案例的历史记录，您可以选择*设置 > 时间轴*并查找名为"创建支持案例"的操作。通过最右侧的按钮，您可以展开操作以查看详细信息。

尝试创建个案时，您可能会遇到以下错误消息：

"您无权针对所选服务创建案例"

此错误可能意味着 NSS 帐户及其关联的记录公司与 NetApp Console 帐户序列号（即960xxxx）或系统序列号的记录公司不同。您可以使用以下选项之一寻求帮助：

- 使用产品内聊天
- 在 https://mysupport.netapp.com/site/help提交非技术案例

管理您的支持案例（预览）

您可以直接从 NetApp Console 查看和管理进行中和已解决的支持个案。您可以管理与您的 NSS 帐户和公司相关的个案。

个案管理可作为预览提供。我们计划改进此体验，并在即将发布的版本中添加增强功能。请使用产品内聊天向我们发送反馈。

请注意以下事项：

- 页面顶端的个案管理控制面板提供两种视图：
  - 左侧视图显示了您提供的用户 NSS 帐户在过去 3 个月内打开的案例总数。
  - 右侧视图根据您的用户 NSS 帐户显示了贵公司在过去 3 个月内打开的案例总数。

  表格中的结果反映了与所选视图相关的案例。
- 您可以添加或删除感兴趣的列，也可以筛选优先级和状态等列的内容。其他列仅提供排序功能。

  有关更多信息，请查看以下步骤。
- 在个案级别，我们提供更新个案备注或关闭尚未处于"已关闭"或"待关闭"状态的个案的功能。

步骤

1. 在 Workload Factory 控制台的右上角，选择 **Help > Support**。

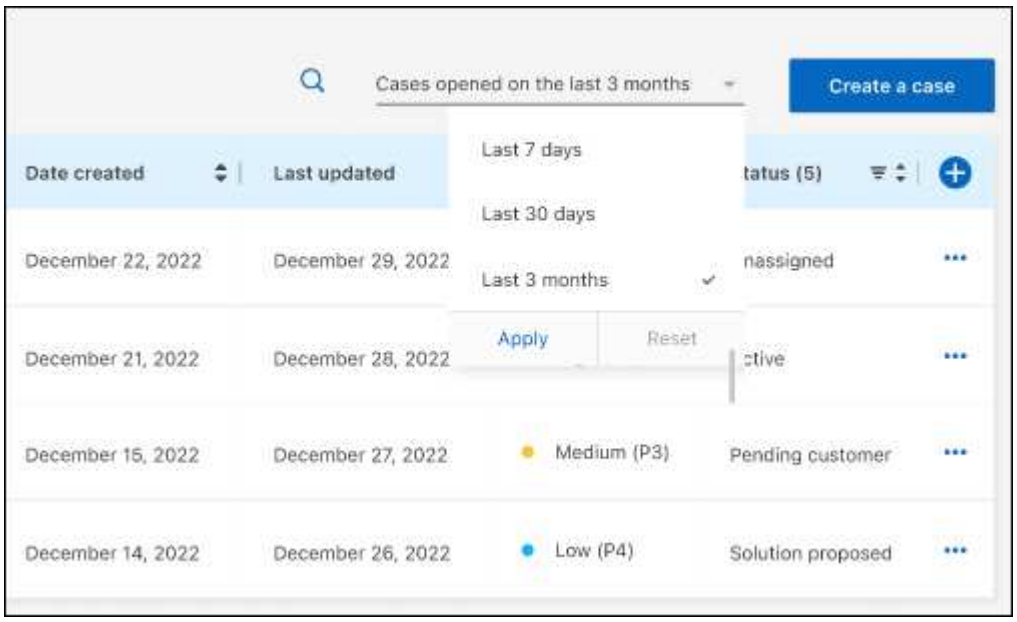
   选择此选项将在新浏览器选项卡中打开 NetApp Console 并加载支持仪表板。

2. 选择*个案管理*，如果系统提示，请将您的 NSS 帐户添加到 NetApp Console。

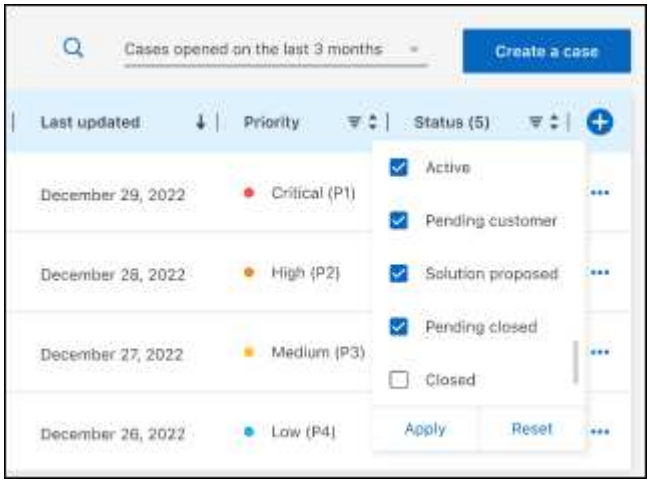
   *案例管理*页面显示与您的 NetApp Console 用户账号关联的 NSS 账号相关的未结案例。这与 *NSS 管理*页面顶部显示的 NSS 账号相同。

3. （可选）修改此表中显示的信息：
   - 在*组织的案例*下，选择*查看*以查看与贵公司相关的所有案例。

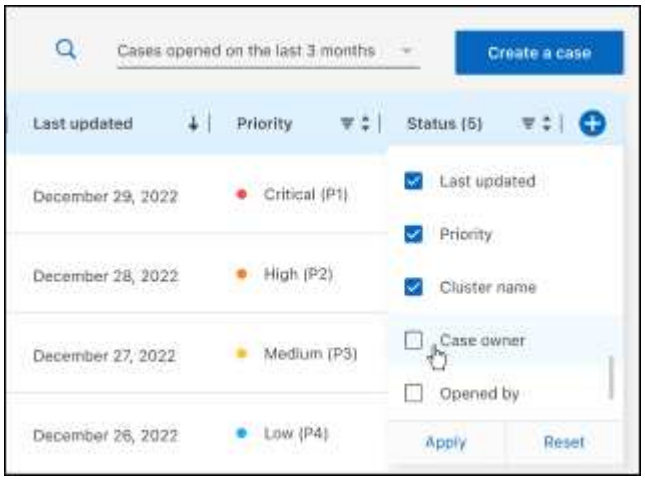
- 通过选择确切的日期范围或选择其他时间范围来修改日期范围。



- 筛选列的内容。



- 通过选择  然后选择要显示的列来更改表格中显示的列。

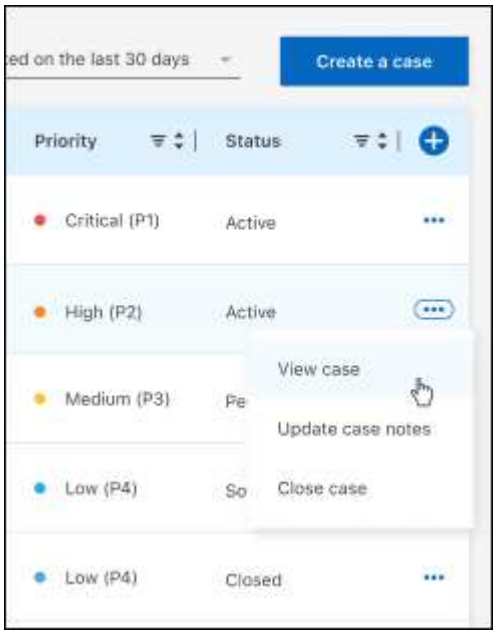


4. 通过选择 ••• 并选择一个可用选项来管理现有个案：

   - 查看个案：查看有关特定个案的完整详细信息。
   - 更新案例备注：提供有关您问题的其他详细信息，或选择*上传文件*以附加最多五个文件。

     每个文件的附件限制为 25 MB。支持以下文件扩展名：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx 和 csv。

   - 关闭个案：请详细说明您关闭个案的原因，然后选择*关闭个案*。



NetApp Workload Factory 的法律声明

法律声明提供对版权声明、商标、专利等信息的访问。

版权

"https://www.netapp.com/company/legal/copyright/"

商标

NETAPP、NETAPP 标识和 NetApp 商标页面上所列的商标是 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。

"https://www.netapp.com/company/legal/trademarks/"

专利

当前 NetApp 拥有的专利列表可以在以下网址找到：

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

隐私政策

"https://www.netapp.com/company/legal/privacy-policy/"

开源

通知文件提供有关 NetApp 软件中使用的第三方版权和许可的信息。

"NetApp Workload Factory"