身份、凭据和最低权限

Information Security for Workload Factory

NetApp

September 16, 2026

目录

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