NetApp Workload Factory 设置和管理文档

Setup and administration

NetApp
February 02, 2026

目录

NetApp Workload Factory 设置和管理文档 1
发行说明 2
NetApp Workload Factory 管理功能的新增功能 2
2026 年 2 月 1 日 2
2026年1月4日 2
2025年11月27日 3
2025年10月6日 3
2025年10月5日 3
2025年9月9日 3
2025年6月29日 4
2025年5月4日 4
2025年3月30日 4
2025年2月2日 4
2025年1月22日 5
2025年1月5日 5
2024年11月11日 5
2024年9月1日 5
2024 年 8 月 4 日 7
2024年7月7日 7
开始使用 8
了解基础知识 8
了解NetApp Workload Factory 8
控制台体验 12
NetApp Workload Factory 的权限 12
NetApp Workload Factory 快速入门 57
注册NetApp Workload Factory 58
注册 Workload Factory 58
邀请其他人加入 Workload Factory 帐户 60
将 AWS 凭证添加到 Workload Factory 60
概述 60
AWS凭据 61
手动向帐户添加凭据 61
使用CloudFormation向帐户添加凭据 64
使用NetApp Workload Factory 优化工作负载 66
管理工作负载工厂 67
登录NetApp Workload Factory 67
管理服务帐户 67
创建服务帐户 68
删除服务帐户 68

构建和运行架构良好的工作负载 69
工作原理 69
为什么这很重要 69
开始使用 Workload Factory 来检测和纠正错误配置 69
存储工作负载的最佳实践和建议 70
数据库工作负载的最佳实践和建议 72
EVS 工作负载的最佳实践和建议 75
相关信息 76
配置NetApp Workload Factory 通知 76
通知类型和消息 76
配置工作负载工厂通知 78
订阅 Amazon SNS 主题 79
筛选通知 79
使用CodeBox自动执行任务 81
了解CODEBox自动化 81
使用 Codebox 实现NetApp Workload Factory 中的自动化 82
在NetApp Workload Factory 中使用 CloudShell 85
关于此任务 85
CloudShell命令 86
开始之前 87
部署CloudShell 87
重命名CloudShell会话选项卡 89
重复的CloudShell会话选项卡 89
关闭CloudShell会话选项卡 90
拆分CloudShell会话选项卡 90
更新CloudShell会话的设置 90
从NetApp Workload Factory 中删除凭据 91
知识和支持 92
注册以获得支持 92
支持注册概述 92
注册您的帐户以获得NetApp支持 92
获取帮助 94
获取FSx for ONTAP支持 94
使用自助支持选项 94
向NetApp支持部门创建案例 94
管理支持案例(预览) 96
NetApp Workload Factory 的法律声明 99
版权 99
商标 99
专利 99
隐私政策 99

开放源代码 99

NetApp Workload Factory 设置和管理文档

发行说明

NetApp Workload Factory 管理功能的新增功能

了解 Workload Factory 管理功能的新功能：云提供商凭证、Codebox 增强功能等。

2026 年 2 月 1 日

精心设计的更新

NetApp Workload Factory 包括针对 Elastic VMware Service (EVS) 工作负载的精心设计的评估，并添加了针对存储和数据库工作负载的新配置。

- **VMware** 工作负载 NetApp Workload Factory 为运行架构良好的 Amazon Elastic VMware Service (EVS) 工作负载提供了最佳实践和建议。

  "实施精心设计的 EVS 配置"

- **Storage workloads** 在 Storage workload 中的精心架构功能中添加了几种新配置，以便您更深入地了解存储性能和成本。
  - Storage VM 逻辑报告
  - 优化缓存卷大小
  - 孤立的块设备

    "为存储工作负载实施精心设计的文件系统配置"

- 数据库工作负载 Workload Factory for Databases 包括新的 Oracle 存储配置，用于启用和设置 Direct NFS (dNFS)，以提高 I/O 性能并降低主机和存储系统的负载。
  - dNFS 启用
  - dNFS 一致的 IP 解析
  - dNFS 配置文件
  - dNFS `nosharecache`

    "实现架构良好的数据库工作负载"

Storage 的新权限

已将新权限添加到 Storage 工作负载，以增强对 S3 访问点的管理。

"权限引用更改日志"

2026年1月4日

问我关于人工智能助手首页集成的问题

Workload Factory 控制台主页嵌入了 Ask me AI 助手，使您可以询问有关您自己的存储环境的问题，直接从您的环境中获取个性化见解，并参考以前的对话。您可以与“问我”进行交互，以了解您的工作负载、解决问题并了解更多关于工作负载工厂的信息——所有这些都无需离开控制台。

2025年11月27日

存储权限更新

FSx for ONTAP EMS 事件分析器使用 *operations and remediation* 权限策略中的以下 Amazon Bedrock 权限来获取存储工作负载的事件数据。

- `bedrock:ListInferenceProfiles`
- `bedrock:GetInferenceProfile`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:InvokeModel`

"权限引用更改日志"

2025年10月6日

BlueXP workload factory现为**NetApp**工作负载工厂

BlueXP已重命名并重新设计，以更好地反映其在管理数据基础设施中的作用。因此， BlueXP workload factory已重命名为NetApp工作负载工厂。

Ask Me 与 **MCP** 集成

Workload Factory 的 AI 助手 Ask Me 与模型上下文协议 (MCP) 集成。使用 MCP，Ask Me 可以安全地与外部环境交互并查询 API 工具，以提供适合您特定存储环境的响应。

2025年10月5日

存储的新通知

NetApp Workload Factory 通知服务包括针对存储架构问题的通知。

"NetApp Workload Factory 通知"

2025年9月9日

存储的新通知

BlueXP workload factory通知服务包括存储自动容量管理通知。

"BlueXP workload factory的通知"

2025年6月29日

更新数据库的权限

现在，数据库在只读模式下具有以下权限： `cloudwatch:GetMetricData` 。

"权限引用更改日志"

BlueXP 工作负载工厂通知服务支持

BlueXP 工作负载工厂通知服务支持工作负载工厂向 BlueXP 警报服务或 Amazon SNS 主题发送通知。发送到 BlueXP 警报的通知会显示在 BlueXP 警报面板中。当工作负载工厂向 Amazon SNS 主题发布通知时，该主题的订阅者（例如人员或其他应用程序）会在为该主题配置的终端节点上收到通知（例如电子邮件或短信）。

"配置 BlueXP 工作负载工厂通知"

2025年5月4日

CloudShell自动完成支持

使用BlueXP Workload Factory CloudShell时、您可以开始键入命令、然后按Tab键查看可用选项。如果存在多种可能、命令行界面将显示建议列表。此功能可最大限度地减少错误并加快命令执行速度、从而提高工作效率。

更新了权限术语

工作负载工厂用户界面和文档现在使用“只读”来指代读取权限，使用“读/写”来指代自动化权限。

2025年3月30日

CloudShell会报告**ONTAP**命令行界面命令的**AI**生成的错误响应

使用CloudShell时、每次发出ONTAP命令行界面命令并出现错误时、您都可以获得AI生成的错误响应、其中包括故障说明、故障原因和详细解决方案。

"使用CloudShell"

IAM：**SimulatePermission Policy**权限更新

现在、当您添加其他AWS帐户凭据或添加新工作负载功能(例如GenAI工作负载)时、您可以从工作负载出厂控制台管理此 `iam:SimulatePrincipalPolicy`权限。

"权限引用更改日志"

2025年2月2日

BlueXP 工作负载出厂控制台中提供了**CloudShell**

您可以从BlueXP 工作负载出厂控制台中的任何位置访问CloudShell。通过CloudShell、您可以使用在BlueXP帐户中提供的AWS和ONTAP凭据、并在类似于Shell的环境中执行AWS命令行界面命令或ONTAP命令行界面命令。

"使用CloudShell"

更新数据库的权限

现在，以下权限在_read_模式下可用于数据库： `iam:SimulatePrincipalPolicy`。

"权限引用更改日志"

2025年1月22日

BlueXP 工作负载出厂权限

现在、您可以查看BlueXP 工作负载工厂执行各种操作所使用的权限、这些操作从发现存储环境到为GenAI工作负载部署AWS资源(例如存储中的文件系统或知识库)不等。您可以查看存储、数据库、VMware和GenAI工作负载的IAM策略和权限。

"BlueXP 工作负载出厂权限"

2025年1月5日

支持**BlueXP** 工作负载工厂中的服务帐户

现在、BlueXP 工作负载工厂支持服务帐户。您可以创建服务帐户、以充当自动化基础架构操作的计算机用户。

"创建和管理服务帐户"

2024年11月11日

工作负载在出厂时集成在**BlueXP** 控制台中

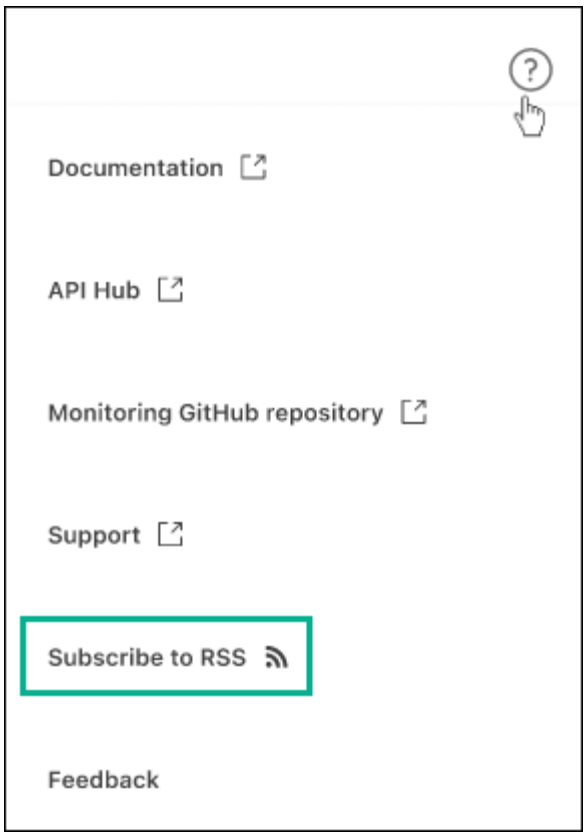
现在，您可以从使用工作负载工厂"BlueXP控制台"。BlueXP 控制台体验可提供与工作负载出厂控制台相同的功能。

"了解如何从BlueXP 控制台访问工作负载工厂"

2024年9月1日

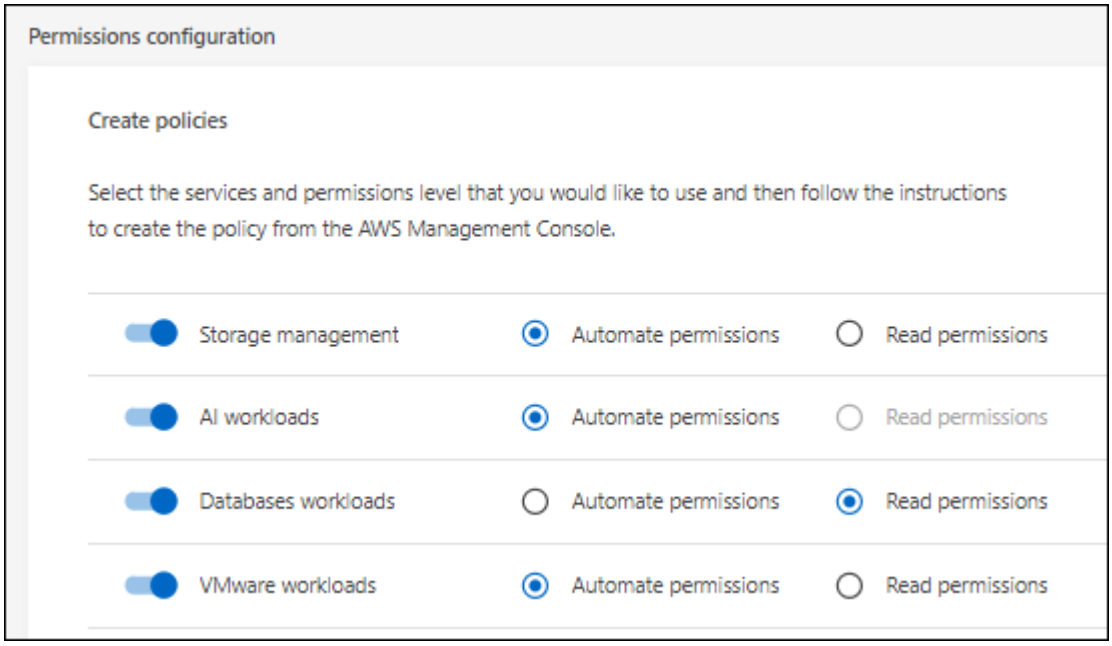
RSS订阅

可从获取RSS订阅"工作负载出厂控制台"。使用RSS源是一种简单的使用方法、可以了解BlueXP 工作负载工厂中的变化。



支持每个工作负载使用一个权限策略

现在、在工作负载工厂添加AWS凭据时、您可以为每个工作负载和存储管理选择一个读取或自动模式权限策略。



"将AWS凭据添加到工作负载工厂"

2024 年 8 月 4 日

Terraform支持

Amazon FSx支持Terraform来部署NetApp ONTAP文件系统和创建Storage VM。现在、设置和管理指南提供了有关如何使用CodeBox中的Terraform的说明。

"使用CodeBox中的Terraform"

2024年7月7日

BlueXP 工作负载出厂初始版本

BlueXP 工作负载工厂是一个功能强大的生命周期管理平台、旨在帮助您使用适用于NetApp ONTAP文件系统的Amazon FSx优化工作负载。可以使用工作负载工厂和FSx for ONTAP简化的工作负载包括数据库、VMware迁移到VMware Cloud on AWS、AI聊天机器人等。

开始使用

了解基础知识

了解**NetApp Workload Factory**

NetApp Workload Factory 是一个强大的生命周期管理平台，旨在帮助您使用Amazon FSx for NetApp ONTAP文件系统优化工作负载。可以使用 Workload Factory 和 FSx for ONTAP简化的工作负载包括数据库、VMware 迁移到 VMware Cloud on AWS、AI 聊天机器人等。

工作负载是指资源、代码、服务或应用程序的组合，旨在服务于业务目标。这可以是任何内容，从面向客户的应用程序到后端流程。工作负载可能涉及单个 AWS 账户中的部分资源，也可能跨越多个账户。

Amazon FSx for NetApp ONTAP为关键任务应用程序、数据库、容器、VMware Cloud 数据存储和用户文件提供完全托管的 AWS 原生 NFS、SMB/CIFS 和 iSCSI 存储卷。您可以通过 Workload Factory 和使用原生 AWS 管理工具来管理 FSx for ONTAP 。

功能

Workload Factory平台提供以下主要功能。

灵活、低成本的存储

在云中发现、部署和管理Amazon FSx for NetApp ONTAP文件系统。FSx for ONTAP将ONTAP的全部功能引入原生AWS托管服务、提供一致的混合云体验。

将内部**vSphere**环境迁移到基于**AWS**的**VMware Cloud**

通过VMware Cloud on AWS迁移顾问、您可以分析内部vSphere环境中的当前虚拟机配置、生成将建议的虚拟机布局部署到VMware Cloud on AWS的计划、并将适用于NetApp ONTAP文件系统的自定义Amazon FSx用作外部数据存储库。

数据库生命周期管理

利用Amazon FSx for NetApp ONTAP发现数据库工作负载并分析节省的成本；在将SQL Server数据库迁移到FSx for ONTAP存储时利用存储和应用程序的优势；部署SQL Server、数据库和数据库克隆以实施供应商最佳实践；使用基础架构即代码联合试点来自动执行操作；持续监控和优化SQL Server资产以提高性能、可用性、保护能力和成本效益。

AI聊天机器人开发

利用FSx for ONTAP文件系统存储组织的聊天机器人源和AI引擎数据库。这样、您就可以将组织的非结构化数据嵌入到企业聊天机器人应用程序中。

节省成本的计算器

分析您当前使用Amazon Elecic Block Store (EBS)或Elecic File System (EFS)存储或Amazon FSx for Windows File Server的部署、了解通过迁移到Amazon FSx for NetApp ONTAP可以节省多少资金。您还可以使用计算器为您计划的未来部署执行"假设"方案。

服务帐户以促进自动化

使用服务帐户安全可靠地自动化NetApp Workload Factory 操作。服务帐户提供可靠、持久的自动化，不受

任何用户管理限制，并且由于它们仅提供 API 访问，因此更加安全。

问我人工智能助手

向 AI 助手询问有关管理和操作 FSx for ONTAP文件系统的问题。使用模型上下文协议 (MCP)，Ask Me 可以安全地与外部环境交互并查询 API 工具，以提供适合您特定存储环境的响应。

支持的云提供商

Workload Factory 使您能够管理云存储并使用 Amazon Web Services 中的工作负载功能。

安全性

NetApp Workload Factory的安全性是NetApp的首要任务。Workload Factory 中的所有工作负载均运行在Amazon FSx for NetApp ONTAP之上。除此之外，还有所有 "AWS 安全功能"NetApp Workload Factory已收到 "SOC2 Type 1 合规性、SOC2 Type 2 合规性和 HIPAA 合规性"。

Amazon FSx for NetApp ONTAP for NetApp Workload Factory 是一款"用于部署企业应用程序的 AWS 解决方案"它是在充分考虑了架构良好的最佳实践的基础上创建的。

成本

Workload Factory 可以免费使用。您向 Amazon Web Services (AWS) 支付的费用取决于您计划部署的存储和工作负载服务。这包括Amazon FSx for NetApp ONTAP 、AWS 基础设施上的 VMware Cloud、AWS 服务等的成本。

工作负载工厂的工作原理

Workload Factory 包括通过 SaaS 层提供的基于 Web 的控制台、帐户、控制对云资产的访问的操作模式、提供 Workload Factory 和 AWS 帐户之间隔离连接的链接等。

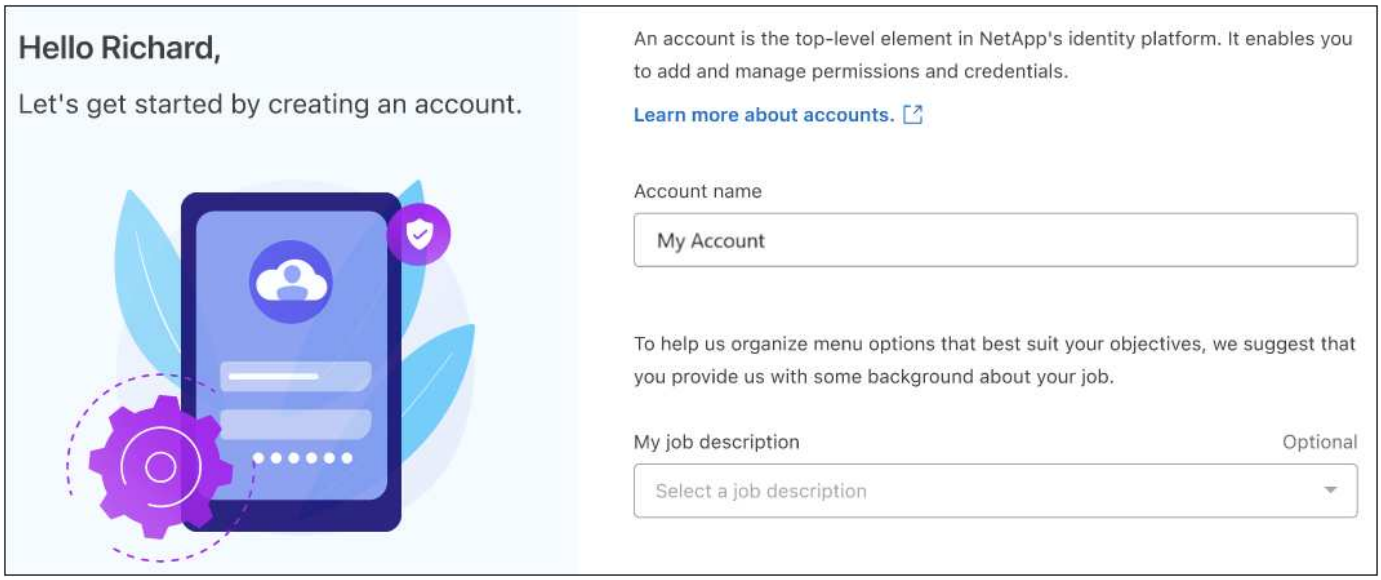
软件即服务

可通过以下方式访问 Workload Factory"NetApp Workload Factory 控制台"以及"NetApp控制台"。这些 SaaS 体验使您能够在最新功能发布时自动访问它们，并轻松地在 Workload Factory 帐户和链接之间切换。

"了解更多关于不同游戏主机体验的信息"

帐户

当您第一次登录 Workload Factory 时，系统会提示您创建一个帐户。此帐户使您能够使用凭据为您的组织组织资源、工作负载和工作负载访问权限。



创建帐户时、您是该帐户的单个_account admin_用户。

如果您的组织需要额外的帐户或用户管理、请通过产品内聊天联系我们。

如果您使用NetApp控制台，那么您已经属于一个帐户，因为 Workload Factory 利用NetApp帐户。

服务帐户

服务帐户充当“用户”，可以对NetApp Workload Factory 进行授权 API 调用以实现自动化目的。这使得管理自动化变得更加容易，因为您不需要基于可以随时离开公司的真实人员的用户帐户来构建自动化脚本。 Workload Factory 中的所有帐户持有者都被视为帐户管理员。帐户管理员可以创建和删除多个服务帐户。

"了解如何管理服务帐户"

权限

Workload Factory 提供灵活的权限策略，使您能够仔细控制对云环境的访问，并根据您的 IT 策略为 Workload Factory 分配递增的信任。

"了解更多关于工作负载工厂权限策略的信息"

连接链路

Workload Factory 链接在 Workload Factory 与一个或多个 FSx for ONTAP文件系统之间建立信任关系和连接。这使您能够直接从ONTAP REST API 调用监控和管理某些文件系统功能，而这些功能无法通过Amazon FSx for ONTAP API 获得。

您不需要链接即可开始使用 Workload Factory，但在某些情况下，您需要创建链接来解锁所有 Workload Factory 功能和工作负载能力。

当前、链路会利用AWS Lamb流程。

"了解有关链接的更多信息"

CodeBox自动化

Codebox 是一个基础设施即代码 (IaC) 副驾驶，可帮助开发人员和 DevOps 工程师生成执行 Workload Factory 支持的任何操作所需的代码。代码格式包括 Workload Factory REST API、AWS CLI 和 AWS CloudFormation。

Codebox 与 Workload Factory 操作模式（*basic*、*read-only* 和 *read/write*）保持一致，并为执行准备设置了清晰的路径以及自动化目录，以便将来快速重用。

CodeBox窗格显示由特定作业流操作生成的IAC、并通过图形向导或对话聊天界面进行匹配。虽然CodeBox支持颜色编码和搜索、以便于导航和分析、但它不允许编辑。您只能复制或保存到自动化目录。

"了解有关CodeBox的更多信息"

节省计算器

Workload Factory 提供节省计算器，以便您可以将存储环境、数据库或 VMware 工作负载在 FSx for ONTAP文件系统上的成本与其他 Amazon 服务进行比较。根据您的存储需求，您可能会发现 FSx for ONTAP文件系统是最具成本效益的选择。

- "了解如何探索存储环境的节省"
- "了解如何探索为数据库工作负载节省的空间"
- "了解如何为您的 VMware 工作负载节省成本"

架构良好的工作负载

Workload Factory 可帮助您维护和运行符合 AWS 良好架构框架的可靠、安全、高效且经济的存储和数据库配置。Workload Factory 每天扫描 FSx 中的ONTAP文件系统、SQL Server 和 Oracle 数据库部署情况，以提供有关潜在错误配置的见解，并建议手动或自动操作来修复问题。

"了解更多关于架构良好的工作负载的信息"

使用**NetApp Workload Factory** 的工具

您可以将NetApp Workload Factory 与以下工具一起使用：

- **Workload Factory** 控制台：Workload Factory 控制台提供您的应用程序和项目的可视化、整体视图。
- * NetApp控制台*： NetApp控制台提供混合界面体验，以便您可以将 Workload Factory 与其他NetApp数据服务一起使用。
- 问我：使用问我 AI 助手来提问并了解有关 Workload Factory 的更多信息，而无需离开 Workload Factory 控制台。从 Workload Factory 帮助菜单访问“问我”。
- **CloudShell CLI**：Workload Factory 包含一个 CloudShell CLI，可通过基于浏览器的单个 CLI 跨账户管理和操作 AWS 和NetApp环境。从 Workload Factory 控制台顶部栏访问 CloudShell。
- **REST API**：使用 Workload Factory REST API 部署和管理您的 FSx for ONTAP文件系统和其他 AWS 资源。
- **CloudFormation**：使用 AWS CloudFormation 代码执行您在 Workload Factory 控制台中定义的操作，以从您的 AWS 账户中的 CloudFormation 堆栈对 AWS 和第三方资源进行建模、配置和管理。
- **Terraform NetApp Workload Factory** 提供商：使用 Terraform 构建和管理在 Workload Factory 控制台中生成的基础架构工作流。

REST API

Workload Factory 使您能够针对特定工作负载优化、自动化和操作 FSx for ONTAP文件系统。每个工作负载都公开一个相关的 REST API。总的来说，这些工作负载和 API 构成了一个灵活且可扩展的开发平台，您可以使用它来管理 FSx for ONTAP文件系统。

使用 Workload Factory REST API 有几个好处：

- 这些API是根据REST技术和当前最佳实践设计的。核心技术包括HTTP和JSON。
- Workload Factory 身份验证基于 OAuth2 标准。 NetApp依赖于 Auth0 服务实现。
- Workload Factory 基于 Web 的控制台使用相同的核心 REST API，因此两个访问路径之间具有一致性。

"查看 Workload Factory REST API 文档"

控制台体验

NetApp Workload Factory 可通过两个基于 Web 的控制台访问。了解如何使用 Workload Factory 控制台和NetApp控制台访问 Workload Factory。

- * NetApp控制台*：提供混合体验，您可以在同一位置管理 FSx for ONTAP文件系统和在Amazon FSx for NetApp ONTAP上运行的工作负载。
- **Workload Factory** 控制台：提供专用的 Workload Factory 体验，专注于在Amazon FSx for NetApp ONTAP上运行的工作负载。

在**NetApp**控制台中访问工作负载工厂

您可以从NetApp Console访问 Workload Factory。除了使用 Workload Factory 来获取 AWS 存储和工作负载功能外，您还可以访问其他数据服务，例如NetApp Copy and Sync等。

步骤

1. 登录"NetApp控制台"。
2. 从NetApp控制台菜单中，选择 **Workloads**，然后选择 **Overview**。

在 **Workload Factory** 控制台中访问 **Workload Factory**

您可以从 Workload Factory 控制台访问 Workload Factory。

步骤

1. 登录"工作负载工厂控制台"。

NetApp Workload Factory 的权限

要使用NetApp Workload Factory 功能和服务，您需要提供权限，以便 Workload Factory 可以在您的云环境中执行操作。

为什么要使用权限

当您提供权限时，Workload Factory 会将策略附加到实例，该策略具有管理该 AWS 账户中资源和进程的权限。

这使得 Workload Factory 能够执行各种操作，从发现您的存储环境到部署 AWS 资源，例如存储管理中的文件系统或 GenAI 工作负载的知识库。

例如，对于数据库工作负载，当 Workload Factory 被授予所需的权限时，它会扫描给定帐户和区域中的所有 EC2 实例，并过滤所有基于 Windows 的机器。如果主机上安装并运行了 AWS Systems Manager (SSM) Agent ，并且 System Manager 网络配置正确，则 Workload Factory 可以访问 Windows 机器并验证是否安装了 SQL Server 软件。

按工作负载划分的权限

每个工作负载都使用权限在工作负载工厂中执行特定任务。权限被打包成一系列权限策略。滚动到您使用的工作负载，了解权限策略、权限策略的可复制 JSON 以及列出所有权限、其用途、使用位置以及支持它们的权限策略的表格。

存储的权限

存储可用的 IAM 策略为 Workload Factory 提供了管理公有云环境中的资源和进程所需的权限。

存储功能提供以下权限策略供您选择：

- 查看、规划和分析：查看 FSx for ONTAP文件系统，了解系统运行状况，获取系统架构完善的分析，并探索节省成本的方法。
- 操作和修复：执行操作任务，例如调整文件系统容量和修复文件系统配置问题。
- 文件系统创建和删除：创建和删除ONTAP文件系统和存储虚拟机的 FSx。

查看所需的身份和访问管理 (IAM) 策略：

存储的**IAM**策略

视图、规划和分析

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:DescribeVolumes",
        "fsx:ListTagsForResource",
        "fsx:DescribeBackups",
        "fsx:DescribeSharedVpcConfiguration",
        "cloudwatch:GetMetricData",
        "cloudwatch:GetMetricStatistics",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "elasticfilesystem:DescribeFileSystems",
        "ce:GetCostAndUsage",
        "ce:GetTags",
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

运营和补救

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateVolume",
        "fsx:DeleteVolume",
        "fsx:UpdateFileSystem",
```

```
        "fsx:UpdateStorageVirtualMachine",
        "fsx:UpdateVolume",
        "fsx:CreateBackup",
        "fsx:CreateVolumeFromBackup",
        "fsx:DeleteBackup",
        "fsx:TagResource",
        "fsx:UntagResource",
        "fsx:CreateAndAttachS3AccessPoint",
        "fsx:DetachAndDeleteS3AccessPoint",
        "s3:CreateAccessPoint",
        "s3:DeleteAccessPoint",
        "s3:GetObjectTagging",
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListInferenceProfiles",
        "bedrock:GetInferenceProfile",
        "s3tables:CreateTableBucket",
        "s3tables:ListTables",
        "s3tables:GetTable",
        "s3tables:GetTableMetadataLocation",
        "s3tables:CreateTable",
        "s3tables:GetNamespace",
        "s3tables:PutTableData",
        "s3tables:CreateNamespace",
        "s3tables:GetTableData",
        "s3tables:ListNamespaces",
        "s3tables:ListTableBuckets",
        "s3tables:GetTableBucket",
        "s3tables:UpdateTableMetadataLocation",
        "s3tables:ListTagsForResource",
        "s3tables:TagResource",
        "s3:GetObjectTagging",
        "s3:ListBucket"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

文件系统的创建和删除

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DeleteFileSystem",
        "fsx:DeleteStorageVirtualMachine",
        "fsx:TagResource",
        "fsx:UntagResource",
        "kms:CreateGrant",
        "iam:CreateServiceLinkedRole",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeRouteTables",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVolumeStatus",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:DeleteSecurityGroup"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/AppCreator": "NetappFSxWF"
        }
      }
    },
```

```
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

下表显示了存储的权限。

存储权限表

目的	操作	使用位置	权限政策
创建FSx for ONTAP文件系统	FSx：CreateFileSystem	部署	文件系统的创建和删除
为FSx for ONTAP文件系统创建安全组	EC2：CreateSecurityGroup	部署	文件系统的创建和删除
为FSx for ONTAP文件系统的安全组添加标记	EC2：CreateTags	部署	文件系统的创建和删除
授权FSx for ONTAP文件系统的安全组传出和传入	EC2：AuthorizeSecurityGroupEgress	部署	文件系统的创建和删除
	EC2：AuthorizeSecurityGroupIngress	部署	文件系统的创建和删除
已授予角色可在FSx for ONTAP与其他AWS服务之间进行通信	IAM：CreateServiceLinkedIn	部署	文件系统的创建和删除
获取详细信息以填写FSx for ONTAP文件系统部署表	EC2：Describe	• 部署 • 了解节省量	文件系统的创建和删除
	EC2：Describe子网	• 部署 • 了解节省量	文件系统的创建和删除
	EC2：Describe安全性组	• 部署 • 了解节省量	文件系统的创建和删除
	EC2：Describe RouteTables	• 部署 • 了解节省量	文件系统的创建和删除
	EC2：Describe网络接口	• 部署 • 了解节省量	文件系统的创建和删除
	EC2：描述卷状态	• 部署 • 了解节省量	文件系统的创建和删除
获取KMS密钥详细信息并用于FSx以进行ONTAP加密	公里：CreateGrant	部署	文件系统的创建和删除
	Kms：可通过键进行操作	部署	文件系统的创建和删除
	Kms：ListKey	部署	文件系统的创建和删除
	Kms：ListAliases	部署	文件系统的创建和删除

目的	操作	使用位置	权限政策
获取EC2实例的卷详细信息	EC2：Describe卷	• 清单 • 了解节省量	视图、规划和分析
获取EC2实例的详细信息	EC2：Describe实例	了解节省量	视图、规划和分析
在节省量计算器中描述Elelic File System	Elasticfilesystem：描述文件系统	了解节省量	视图、规划和分析
列出FSx for ONTAP资源的标记	FSx：ListTagsForResource	清单	视图、规划和分析
管理FSx for ONTAP文件系统的安全组传出和传入	EC2 ：RevokeSecurityGroupIngress	管理操作	文件系统的创建和删除
	ec2：撤销安全组出口	管理操作	文件系统的创建和删除
	EC2：DeleteSecurityGroup	管理操作	文件系统的创建和删除

目的	操作	使用位置	权限政策
创建、查看和管理FSx for ONTAP文件系统资源	FSx：CreateVolume	管理操作	运营和补救
	FSx：TagResource	管理操作	运营和补救
	FSx ：CreateStorageVirtualMachine	管理操作	文件系统的创建和删除
	fsx：删除文件系统	管理操作	文件系统的创建和删除
	fsx：删除存储虚拟机	管理操作	视图、规划和分析
	FSx：可对FileSystems进行情况分类	清单	视图、规划和分析
	FSx：讲解StorageVirtualMachine	清单	视图、规划和分析
	fsx：描述共享虚拟PC配置	清单	视图、规划和分析
	fsx：更新文件系统	管理操作	运营和补救
	fsx：更新存储虚拟机	管理操作	运营和补救
	FSx：可对卷进行分过程	清单	视图、规划和分析
	FSx：UpdateVolume	管理操作	运营和补救
	fsx：删除卷	管理操作	运营和补救
	FSx：UnTagResource	管理操作	运营和补救
	FSx：对备份进行了分过程	管理操作	视图、规划和分析
	fsx:创建备份	管理操作	运营和补救
	fsx：从备份创建卷	管理操作	运营和补救
	fsx：删除备份	管理操作	运营和补救
获取文件系统和卷指标	CloudWatch：GetMetricData	管理操作	视图、规划和分析
	CloudWatch：GetMetricStatistics	管理操作	视图、规划和分析
模拟工作负载操作以验证可用权限并与所需的AWS帐户权限进行比较	IAM：SimulatePrincipalPolicy	部署	全部

目的	操作	使用位置	权限政策
为ONTAP EMS 事件的 FSx 提供基于人工智能的洞察	Bedrock：ListInferenceProfile	FSx 用于ONTAP EMS 分析	运营和补救
	基岩：获取推理配置文件	FSx 用于ONTAP EMS 分析	运营和补救
	基岩：调用模型及其响应流	FSx 用于ONTAP EMS 分析	运营和补救
	基岩：InvokeModel	FSx 用于ONTAP EMS 分析	运营和补救
从 AWS Cost Explorer 获取 FSx for ONTAP文件系统的成本和使用情况数据。	ce:获取成本和使用情况	成本和使用情况分析	视图、规划和分析
	ce:GetTags	成本和使用情况分析	视图、规划和分析
创建 S3 接入点并将其附加到 FSx for ONTAP 文件系统	fsx:CreateAndAttachS3AccessPoint	S3 接入点管理	运营和补救
从 FSx for ONTAP 文件系统中分离 S3 接入点并将其删除	fsx:DetachAndDeleteS3AccessPoint	S3 接入点管理	运营和补救
创建 S3 访问点以简化存储桶访问管理	s3：CreateAccessPoint	S3 接入点管理	运营和补救
删除 S3 接入点	s3：DeleteAccessPoint	S3 接入点管理	运营和补救
向 S3 接入点添加标记	s3:TagResource	S3 接入点管理	运营和补救
列出和查看 S3 接入点上的标签	s3：ListTagsForResource	S3 接入点管理	运营和补救
从 S3 接入点删除标记	s3：UntagResource	S3 接入点管理	运营和补救
发现 S3 接入点存储桶中的对象	s3:ListBucket	S3 存储桶操作	运营和补救
列出、创建和描述 S3 表存储桶	s3tables:ListTableBuckets s3tables:CreateTableBucket s3tables:GetTableBucket	S3 表存储桶管理	运营和补救
列出、创建和检索 S3 表	s3tables:ListTables s3tables:CreateTable s3tables:GetTable	S3 表操作	运营和补救
读取表元数据位置	s3tables ：GetTableMetadataLocation	S3 表元数据操作	运营和补救
更新表元数据位置	s3tables ：UpdateTableMetadataLocation	S3 表元数据操作	运营和补救
列出、创建和检索表命名空间	s3tables:ListNamespaces s3tables:CreateNamespace s3tables:GetNamespace	S3 命名空间操作	运营和补救
读取表数据（select、scan）	s3tables：GetTableData	S3 表数据操作	运营和补救

目的	操作	使用位置	权限政策
写入表数据（插入）	s3tables：PutTableData	S3 表数据操作	运营和补救
在库存表上列出标签（获取 FSx for ONTAP、存储 VM、卷 ID）	s3tables：ListTagsForResource	S3 表标签操作	运营和补救
标记 Workload Factory 查找的清单表	s3tables：TagResource	S3 表标签操作	运营和补救
通过接入点检索对象标记	s3:GetObjectTagging	S3 对象操作	运营和补救

数据库工作负载的权限

数据库工作负载可用的 IAM 策略提供了 Workload Factory 管理公有云环境中的资源和进程所需的权限。

数据库提供以下权限策略供您选择：

- 查看、规划和分析：查看数据库资源清单，了解资源的运行状况，审查数据库配置的良好架构分析，探索节省成本的方法，获取错误日志分析，并探索节省成本的方法。
- 操作和修复：对数据库资源执行操作任务，并修复数据库配置和底层 FSx for ONTAP文件系统存储的问题。
- 数据库主机创建：根据最佳实践部署数据库主机和底层 FSx for ONTAP文件系统存储。

选择操作模式以查看所需的IAM策略：

视图、规划和分析

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CommonGroup",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:GetMetricStatistics",
                "cloudwatch:GetMetricData",
                "sns:ListTopics",
                "ec2:DescribeInstances",
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeImages",
                "ec2:DescribeRegions",
                "ec2:DescribeRouteTables",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeInstanceTypes",
                "ec2:DescribeVpcEndpoints",
                "ec2:DescribeInstanceTypeOfferings",
                "ec2:DescribeSnapshots",
                "ec2:DescribeVolumes",
                "ec2:DescribeAddresses",
                "kms:ListAliases",
                "kms:ListKeys",
                "kms:DescribeKey",
                "cloudformation:ListStacks",
                "cloudformation:DescribeAccountLimits",
                "ds:DescribeDirectories",
                "fsx:DescribeVolumes",
                "fsx:DescribeBackups",
                "fsx:DescribeStorageVirtualMachines",
                "fsx:DescribeFileSystems",
                "servicequotas:ListServiceQuotas",
                "ssm:GetParametersByPath",
                "ssm:GetCommandInvocation",
                "ssm:SendCommand",
                "ssm:GetConnectionStatus",
                "ssm:DescribePatchBaselines",
                "ssm:DescribeInstancePatchStates",
                "ssm:ListCommands",
```

```
                "ssm:DescribeInstanceInformation",
                "fsx:ListTagsForResource",
                "logs:DescribeLogGroups",
                "bedrock:GetFoundationModelAvailability",
                "bedrock:ListInferenceProfiles"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "SSMParameterStore",
            "Effect": "Allow",
            "Action": [
                "ssm:GetParameter",
                "ssm:GetParameters",
                "ssm:PutParameter",
                "ssm:DeleteParameters"
            ],
            "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmdb/*"
        },
        {
            "Sid": "SSMResponseCloudWatch",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents",
                "logs:PutRetentionPolicy"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:netapp/wlmdb/*"
        }
    ]
}
```

运营和补救

```
[
    {
        "Sid": "FSxRemediation",
        "Effect": "Allow",
        "Action": [
            "fsx:UpdateFileSystem",
            "fsx:UpdateVolume"
        ],
        "Resource": "*"
    },
    {
        "Sid": "EC2Remediation",
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:ModifyInstanceAttribute",
            "ec2:StopInstances"
        ],
        "Resource": "*",
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/aws:cloudformation:stack-name":
"WLMDB*"
            }
        }
    }
]
```

创建数据库主机

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "EC2TagGroup",
            "Effect": "Allow",
            "Action": [
                "ec2:AllocateAddress",
                "ec2:AllocateHosts",
                "ec2:AssignPrivateIpAddresses",
                "ec2:AssociateAddress",
                "ec2:AssociateRouteTable",
                "ec2:AssociateSubnetCidrBlock",
                "ec2:AssociateVpcCidrBlock",
                "ec2:AttachInternetGateway",
```

```
                "ec2:AttachNetworkInterface",
                "ec2:AttachVolume",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateVolume",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteTags",
                "ec2:DeleteVolume",
                "ec2:DetachNetworkInterface",
                "ec2:DetachVolume",
                "ec2:DisassociateAddress",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DisassociateRouteTable",
                "ec2:DisassociateSubnetCidrBlock",
                "ec2:DisassociateVpcCidrBlock",
                "ec2:ModifyInstancePlacement",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:ModifySubnetAttribute",
                "ec2:ModifyVolume",
                "ec2:ModifyVolumeAttribute",
                "ec2:ReleaseAddress",
                "ec2:ReplaceRoute",
                "ec2:ReplaceRouteTableAssociation",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
                }
            }
        },
        {
            "Sid": "FSxNGroup",
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "aws:ResourceTag/aws:cloudformation:stack-
name": "WLMDB*"
```

```
                }
            }
        },
        {
            "Sid": "CreationGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStacks",
                "cloudformation:ValidateTemplate",
                "ec2:CreateLaunchTemplate",
                "ec2:CreateLaunchTemplateVersion",
                "ec2:CreateNetworkInterface",
                "ec2:CreateSecurityGroup",
                "ec2:CreateTags",
                "ec2:CreateVpcEndpoint",
                "ec2:RunInstances",
                "ec2:DescribeTags",
                "ec2:DescribeLaunchTemplates",
                "ec2:ModifyVpcAttribute",
                "fsx:CreateFileSystem",
                "fsx:CreateStorageVirtualMachine",
                "fsx:CreateVolume",
                "fsx:DescribeFileSystemAliases",
                "kms:CreateGrant",
                "kms:DescribeCustomKeyStores",
                "kms:GenerateDataKey",
                "kms:Decrypt",
                "logs:CreateLogGroup",
                "logs:CreateLogStream",
                "logs:GetLogGroupFields",
                "logs:GetLogRecord",
                "logs:ListLogDeliveries",
                "logs:PutLogEvents",
                "logs:TagResource",
                "sns:Publish",
                "ssm:PutComplianceItems",
                "ssm:PutConfigurePackageResult",
                "ssm:PutInventory",
                "ssm:UpdateAssociationStatus",
                "ssm:UpdateInstanceAssociationStatus",
                "ssm:UpdateInstanceInformation",
                "ssmmessages:CreateControlChannel",
                "ssmmessages:CreateDataChannel",
                "ssmmessages:OpenControlChannel",
```

```
                "ssmmessages:OpenDataChannel",
                "compute-optimizer:GetEnrollmentStatus",
                "compute-optimizer:PutRecommendationPreferences",
                "compute-
optimizer:GetEffectiveRecommendationPreferences",
                "compute-optimizer:GetEC2InstanceRecommendations",
                "autoscaling:DescribeAutoScalingGroups",
                "autoscaling:DescribeAutoScalingInstances",
                "iam:GetPolicy",
                "iam:GetPolicyVersion",
                "iam:GetRole",
                "iam:GetRolePolicy",
                "iam:GetUser"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ArnGroup",
            "Effect": "Allow",
            "Action": [
                "cloudformation:SignalResource"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:*:stack/WLMDB*",
                "arn:aws:logs:*:*:log-group:WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup1",
            "Effect": "Allow",
            "Action": [
                "iam:AddRoleToInstanceProfile",
                "iam:CreateInstanceProfile",
                "iam:DeleteInstanceProfile",
                "iam:PutRolePolicy",
                "iam:RemoveRoleFromInstanceProfile"
            ],
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ]
        },
        {
            "Sid": "IAMGroup2",
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup3",
            "Effect": "Allow",
            "Action": "iam:PassRole",
            "Resource": [
                "arn:aws:iam::*:instance-profile/*",
                "arn:aws:iam::*:role/WLMDB*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PassedToService": "ec2.amazonaws.com"
                }
            }
        },
        {
            "Sid": "IAMGroup4",
            "Effect": "Allow",
            "Action": "iam:CreateRole",
            "Resource": "arn:aws:iam::*:role/WLMDB*"
        }
    ]
}
```

下表显示了数据库工作负载的权限。

数据库工作负载的权限表

目的	操作	使用位置	权限政策
获取 FSx for ONTAP、EBS 和 FSx for Windows File Server 的指标统计数据以及计算优化建议	CloudWatch：GetMetricStatistics	• 清单 • 了解节省量	视图、规划和分析
从已注册的 SQL 节点收集已保存到 Amazon CloudWatch 的性能指标。数据将在已注册 SQL 实例的管理实例屏幕上生成性能趋势图。	CloudWatch：GetMetricData	清单	视图、规划和分析
获取EC2实例的详细信息	EC2：Describe实例	• 清单 • 了解节省量	视图、规划和分析
	EC2：Describe KeyPairs	部署	视图、规划和分析
	EC2：Describe网络接口	部署	视图、规划和分析
	EC2：可说明实例型	• 部署 • 了解节省量	视图、规划和分析
获取详细信息以填写FSx for ONTAP部署表	EC2：Describe	• 部署 • 清单	视图、规划和分析
	EC2：Describe子网	• 部署 • 清单	视图、规划和分析
	EC2：Describe安全性组	部署	视图、规划和分析
	EC2：Describe	部署	视图、规划和分析
	EC2：Describe注册	部署	视图、规划和分析
	EC2：Describe RouteTables	• 部署 • 清单	视图、规划和分析
获取任何现有VPC端点、以确定是否需要在部署之前创建新端点	EC2：Describe VpcEndpoints	• 部署 • 清单	视图、规划和分析
如果所需服务不存在VPC端点、则无论EC2实例上的公共网络连接如何、均可创建VPC端点	EC2：CreateVpcEndpoint	部署	创建数据库主机

目的	操作	使用位置	权限政策
获取验证节点所在地区可用的实例类型(t2.micro/t3.micro)	EC2：说明InstanceTypeOfferings	部署	视图、规划和分析
获取所连接的每个EBS卷的快照详细信息、以了解定价和预计节省量	EC2：Describe Snapshot	了解节省量	视图、规划和分析
获取所连接的每个EBS卷的详细信息、以了解定价和预计节省量	EC2：Describe卷	• 清单 • 了解节省量	视图、规划和分析
获取FSx for ONTAP文件系统加密的KMS密钥详细信息	Kms：ListAliases	部署	视图、规划和分析
	Kms：ListKey	部署	视图、规划和分析
	Kms：可通过键进行操作	部署	视图、规划和分析
获取环境中运行的CloudFormation堆栈列表以检查配额限制	CloudFormation：ListStack	部署	视图、规划和分析
在触发部署之前、请检查资源的帐户限制	CloudFormation：可进行详细信息帐户限制	部署	视图、规划和分析
获取区域中AWS管理的Active Directory列表	DS：可通过子目录进行操作	部署	视图、规划和分析
获取适用于ONTAP文件系统的FSx的卷、备份、SVM、文件系统(以英文)和标记的列表和详细信息	FSx：可对卷进行分过程	• 清单 • 了解节省量	视图、规划和分析
	FSx：对备份进行了分过程	• 清单 • 了解节省量	视图、规划和分析
	FSx：讲解StorageVirtualMachine	• 部署 • 管理操作 • 清单	视图、规划和分析
	FSx：可对FileSystems进行情况分类	• 部署 • 管理操作 • 清单 • 了解节省量	视图、规划和分析
	FSx：ListTagsForResource	管理操作	视图、规划和分析
获取 CloudFormation 和 VPC 的服务配额限制 / 为用户帐户中提供的 SQL、域和 FSx for ONTAP凭据创建密钥	serviceequotas：ListServiceQuotas	部署	视图、规划和分析

目的	操作	使用位置	权限政策
使用基于SSM的查询获取FSx for ONTAP支持的区域的更新列表	SSM：GetPathetersByPath	部署	视图、规划和分析
在发送部署后用于管理操作的命令后轮询 SSM 响应	SSM：GetCommandInvation	• 管理操作 • 清单 • 了解节省量 • 优化	视图、规划和分析
通过 SSM 向 EC2 实例发送命令以进行发现和管理	SSM：SendCommand	• 管理操作 • 清单 • 了解节省量 • 优化	视图、规划和分析
获取部署后实例的SSM连接状态	SSM：GetConnectionStatus	• 管理操作 • 清单 • 优化	视图、规划和分析
提取一组受管EC2实例(SQL节点)的SSM关联状态	SSM：说明实例信息	清单	视图、规划和分析
获取可用于操作系统修补程序评估的修补程序基线列表	SSM：对修补程序基准线进行了详述	优化	视图、规划和分析
获取Windows EC2实例上的修补状态、以进行操作系统修补程序评估	SSM：说明InstancePatchStates	优化	视图、规划和分析
列出AWS Patch Manager在EC2实例上执行的命令、用于管理操作系统修补程序	SSM：ListCommands	优化	视图、规划和分析
检查帐户是否已在AWS计算控制器中注册	计算优化器：GetEnrollmentStatus	• 了解节省量 • 优化	创建数据库主机
更新AWS计算改进器中的现有建议首选项、以便为SQL Server工作负载量身定制建议	计算优化器:PutRecommentationPreferences	• 了解节省量 • 优化	创建数据库主机
从AWS计算最佳器中获取对给定资源有效的建议首选项	计算优化器：GetEffectiveRecommentationPreferences	• 了解节省量 • 优化	创建数据库主机
提取AWS计算最佳器为Amazon Elecic计算云(Amazon EC2)实例生成的建议	计算优化器：GetEC2InstanceRecommandations	• 了解节省量 • 优化	创建数据库主机

目的	操作	使用位置	权限政策
检查实例是否与自动缩放组关联	自动缩放：自适应缩放组的情况	• 了解节省量 • 优化	创建数据库主机
	自动缩放：可通过它来进行自适应缩放	• 了解节省量 • 优化	创建数据库主机
获取、列出、创建和删除在部署期间使用或在AWS帐户中管理的AD、FSx for ONTAP和SQL用户凭据的SSM参数	SSM：Get参 比器[1]	• 部署 • 管理操作 • 清单	视图、规划和分析
	SSM：GetParameters [1]	• 部署 • 管理操作 • 清单	视图、规划和分析
	SSM：Put参 比器[1]	• 部署 • 管理操作	视图、规划和分析
	SSM：删除参数[1]	• 部署 • 管理操作	视图、规划和分析
将网络资源与SQL节点和验证节点相关联、并向SQL节点添加其他辅助IP	EC2：AllocateAddress [1]	部署	创建数据库主机
	EC2：AllocateHsts [1]	部署	创建数据库主机
	EC2：AssignPrivateIpAddresses [1]	部署	创建数据库主机
	EC2：AssociateAddress [1]	部署	创建数据库主机
	EC2：AssociateRouteTable [1]	部署	创建数据库主机
	EC2 ：AssociateSubnetCindrBlock [1]	部署	创建数据库主机
	EC2：AssociateVpcCindrBlock [1]	部署	创建数据库主机
	EC2：AttachInternetGateway [1]	部署	创建数据库主机
	EC2：AttachNetworkInterface [1]	部署	创建数据库主机
将所需的EBS卷连接到SQL节点以进行部署	EC2：Attach卷	部署	创建数据库主机
将安全组附加到已配置的 EC2 实例并修改规则	EC2 ：AuthorizeSecurityGroupEgress	部署	创建数据库主机
	EC2 ：AuthorizeSecurityGroupIngress	部署	创建数据库主机
创建部署SQL节点所需的EBS卷	EC2：CreateVolume	部署	创建数据库主机

目的	操作	使用位置	权限政策
删除为类型T2.micro创建的临时验证节点、以便回滚或重试失败的EC2 SQL节点	EC2：DeleteNetworkInterface	部署	创建数据库主机
	EC2：DeleteSecurityGroup	部署	创建数据库主机
	EC2：DeleteTags	部署	创建数据库主机
	EC2：DeleteVolume	部署	创建数据库主机
	EC2：DetachNetworkInterface	部署	创建数据库主机
	EC2：分离卷	部署	创建数据库主机
	EC2：与地址断开关联	部署	创建数据库主机
	EC2：DisassociateIamInstanceProfile	部署	创建数据库主机
	EC2：与RouteTable断开关联	部署	创建数据库主机
	EC2：DisAssociateSubnetCindrBlock	部署	创建数据库主机
	EC2：与VpcCindrBlock断开关联	部署	创建数据库主机
修改已创建SQL实例的属性。仅适用于以“以期名”开头的名称。	EC2：ModifyInstance属性	部署	运营和补救
	EC2：可通过实例布局进行设置	部署	创建数据库主机
	EC2：ModifyNetworkInterfaceAttribute	部署	创建数据库主机
	EC2：可使用的子网属性	部署	创建数据库主机
	EC2：ModifyVolume	部署	创建数据库主机
	EC2：ModifyVolumeAttribute	部署	创建数据库主机
	EC2：modfyVpcAttribute.	部署	创建数据库主机
取消关联并销毁验证实例	EC2：ReleraAddress	部署	创建数据库主机
	EC2：ReteraRoute	部署	创建数据库主机
	EC2：ReporteRouteTableAssociation	部署	创建数据库主机
	EC2：RevokeSecurityGroupEgress	部署	创建数据库主机
	EC2：RevokeSecurityGroupIngress	部署	创建数据库主机
启动已部署的实例	EC2：StartInstances	部署	运营和补救
停止已部署的实例	EC2：StopInstances	部署	运营和补救
标记由Windows资源管理组织创建的Amazon FSx for NetApp ONTAP资源的自定义值、以便在资源管理期间获取帐单详细信息	FSx：TagResource [1]	• 部署 • 管理操作	创建数据库主机

目的	操作	使用位置	权限政策
创建并验证用于部署的CloudFormation模板	CloudFormation：CreateStack	部署	创建数据库主机
	CloudFormation：Describe StackEvents	部署	创建数据库主机
	CloudFormation：Describe堆栈	部署	创建数据库主机
	CloudFormation：ListStack	部署	视图、规划和分析
	CloudFormation：验证模板	部署	创建数据库主机
创建嵌套堆栈模板以重试和回滚	EC2：CreateLaunch模板	部署	创建数据库主机
	EC2：CreateLaunch模板版本	部署	创建数据库主机
管理已创建实例上的标记和网络安全性	EC2：CreateNetworkInterface	部署	创建数据库主机
	EC2：CreateSecurityGroup	部署	创建数据库主机
	EC2：CreateTags	部署	创建数据库主机
获取用于配置的实例详细信息	ec2:描述地址	部署	视图、规划和分析
	ec2：描述启动模板	部署	视图、规划和分析
启动已创建的实例	EC2：RunInstances	部署	创建数据库主机
创建配置所需的FSx for ONTAP资源。对于现有FSx for ONTAP系统、将创建一个新的SVM来托管SQL卷。	FSx：CreateFileSystem	部署	创建数据库主机
	FSx：CreateStorageVirtualMachine	部署	创建数据库主机
	FSx：CreateVolume	• 部署 • 管理操作	创建数据库主机
获取FSx for ONTAP详细信息	fsx:描述文件系统别名	部署	创建数据库主机
调整FSx for ONTAP文件系统的大小以修复文件系统余量	FSx：UpdateFilesystem	优化	运营和补救
调整卷大小以修复日志和TempDB驱动器大小	FSx：UpdateVolume	优化	运营和补救
获取KMS密钥详细信息并用于FSx以进行ONTAP加密	公里：CreateGrant	部署	创建数据库主机
	kms:描述自定义密钥存储	部署	创建数据库主机
	Kms：GenerateDataKey	部署	创建数据库主机

目的	操作	使用位置	权限政策
为在EC2实例上运行的验证和配置脚本创建CloudWatch日志	日志：CreateLogGroup	部署	创建数据库主机
	日志：CreateLogStream	部署	创建数据库主机
	日志：获取日志组字段	部署	创建数据库主机
	日志：获取日志记录	部署	创建数据库主机
	日志：ListLogDelivery	部署	创建数据库主机
	日志：PutLogEvents	• 部署 • 管理操作	创建数据库主机
	日志:TagResource	部署	创建数据库主机
遇到 SSM 输出截断时，Workload Factory 会切换到 SQL 实例的 Amazon CloudWatch 日志	日志：GetLogEvents	• 存储评估(优化) • 清单	视图、规划和分析
允许 Workload Factory 获取当前日志组并检查 Workload Factory 创建的日志组是否设置了保留	日志：可通过"LogBeLogGroup"进行操作	• 存储评估(优化) • 清单	视图、规划和分析
允许 Workload Factory 为其创建的日志组设置一天的保留策略，以避免 SSM 命令输出的日志流不必要地积累	日志：PutRettionPolicy	• 存储评估(优化) • 清单	视图、规划和分析
列出客户SNS主题、并发布到符合以下条件的系统日志和客户SNS (如果已选择)	SnS：ListTopics	部署	视图、规划和分析
	SNS：发布	部署	创建数据库主机
在已配置的SQL实例上运行发现脚本以及提取FSx for ONTAP支持的AWS区域的最新列表所需的SSM权限。	SSM：PutCompletianceItems	部署	创建数据库主机
	SSM：PutConfigurePackageResult	部署	创建数据库主机
	SSM：PutInventory	部署	创建数据库主机
	SSM：UpdateAssociationStatus	部署	创建数据库主机
	SSM：UpdateInstanceAssociationStatus	部署	创建数据库主机
	SSM：UpdateInstanceInformation	部署	创建数据库主机
	ssmmessages：创建控制通道	部署	创建数据库主机
	ssmmessages：创建数据通道	部署	创建数据库主机
	ssmmessages：打开控制通道	部署	创建数据库主机
	ssmmessages：开放数据通道	部署	创建数据库主机

目的	操作	使用位置	权限政策
成功或失败时向CloudFormation堆栈发送信号。	CloudFormation：SignalResource [1]	部署	创建数据库主机
将模板创建的EC2角色添加到EC2的实例配置文件中、以允许EC2上的脚本访问部署所需的资源。	IAM：AddRoleToInstanceProfile	部署	创建数据库主机
为EC2创建实例配置文件并附加已创建的EC2角色。	IAM：CreateInstanceProfile	部署	创建数据库主机
使用下面列出的权限通过模板创建EC2角色	IAM：CreateRole	部署	创建数据库主机
创建链接到EC2服务的角色	IAM：CreateServiceLinkedIn Role [2]	部署	创建数据库主机
删除在部署期间专为验证节点创建的实例配置文件	IAM：DeleteInstanceProfile	部署	创建数据库主机
获取角色和策略详细信息、以确定权限方面的任何差距并进行部署验证	IAM：GetPolicy	部署	创建数据库主机
	IAM：GetPolicyVersion	部署	创建数据库主机
	IAM：GetRole	部署	创建数据库主机
	IAM：GetRolePolicy	部署	创建数据库主机
	IAM：GetUser	部署	创建数据库主机
将创建的角色传递到EC2实例	IAM：PassRole [3]	部署	创建数据库主机
将具有所需权限的策略添加到已创建的EC2角色	IAM：PutRolePolicy	部署	创建数据库主机
从配置的EC2实例配置文件中断开角色	IAM：RemoveRoleFromInstanceProfile	部署	创建数据库主机
模拟工作负载操作以验证可用权限并与所需的AWS帐户权限进行比较	IAM：SimulatePrincipalPolicy	部署	全部
获取可用于错误日志分析的基础模型	Bound：GetFoundation论 可用性	错误日志分析	视图、规划和分析
列出 Amazon Bedrock 中可用于错误日志分析的接口配置文件	Bedrock：ListInferenceProfile	错误日志分析	视图、规划和分析

1. 权限仅限于从“资源管理模块”开始的资源。
2. "IAM：CreateServiceLinkedIn Role"受"iam：AVsServiceName"限制：ec2.amazonaws.com"*
3. "IAM：PassRole"受"iam：PassedToService"限制：ec2.amazonaws.com"*

GenAI工作负载的权限

VMware 工作负载的 IAM 策略根据您所处的运行模式，提供 Workload Factory for VMware 管理公共云环境中的资源和流程所需的权限。

GenAI IAM 策略仅支持读/写权限：

- 读/写：使用分配的凭证代表您在 AWS 中执行和自动执行操作，这些凭证具有执行所需的已验证权限。

适用于GenAI工作负载的IAM策略

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CloudformationGroup",
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks"
      ],
      "Resource": "arn:aws:cloudformation:*:*:stack/wlmai*/*"
    },
    {
      "Sid": "EC2Group",
      "Effect": "Allow",
      "Action": [
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/aws:cloudformation:stack-name": "wlmai*"
        }
      }
    },
    {
      "Sid": "EC2DescribeGroup",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:CreateVpcEndpoint",
        "ec2:CreateSecurityGroup",
        "ec2:CreateTags",
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeRouteTables",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeVpcEndpoints",
        "ec2:DescribeInstances",
        "ec2:DescribeImages",
```

```
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:RunInstances"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup",
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:PutRolePolicy",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMGroup2",
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:PassedToService": "ec2.amazonaws.com"
        }
      }
    },
    {
      "Sid": "FSXNGroup",
      "Effect": "Allow",
      "Action": [
        "fsx:DescribeVolumes",
        "fsx:DescribeFileSystems",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:ListTagsForResource"
      ],
      "Resource": "*"
    },
    {
      "Sid": "FSXNGroup2",
      "Effect": "Allow",
      "Action": [
```

```
        "fsx:UntagResource",
        "fsx:TagResource"
      ],
      "Resource": [
        "arn:aws:fsx:*:*:volume/*/*",
        "arn:aws:fsx:*:*:storage-virtual-machine/*/*"
      ]
    },
    {
      "Sid": "SSMParameterStore",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameter",
        "ssm:PutParameter"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/netapp/wlmai/*"
    },
    {
      "Sid": "SSM",
      "Effect": "Allow",
      "Action": [
        "ssm:GetParameters",
        "ssm:GetParametersByPath"
      ],
      "Resource": "arn:aws:ssm:*:*:parameter/aws/service/*"
    },
    {
      "Sid": "SSMMessages",
      "Effect": "Allow",
      "Action": [
        "ssm:GetCommandInvocation"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMCommandDocument",
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand"
      ],
      "Resource": [
        "arn:aws:ssm:*:*:document/AWS-RunShellScript"
      ]
    },
    {
      "Sid": "SSMCommandInstance",
```

```
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:GetConnectionStatus"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ],
      "Condition": {
        "StringLike": {
          "ssm:resourceTag/aws:cloudformation:stack-name": "wlmai-*"
        }
      }
    },
    {
      "Sid": "KMS",
      "Effect": "Allow",
      "Action": [
        "kms:GenerateDataKey",
        "kms:Decrypt"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SNS",
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatch",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogGroups"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchAiEngine",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
```

```
        "logs:DescribeLogStreams"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*"
    },
    {
      "Sid": "CloudWatchAiEngineLogStream",
      "Effect": "Allow",
      "Action": [
        "logs:GetLogEvents"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/netapp/wlmai*:*"
    },
    {
      "Sid": "BedrockGroup",
      "Effect": "Allow",
      "Action": [
        "bedrock:InvokeModelWithResponseStream",
        "bedrock:InvokeModel",
        "bedrock:ListFoundationModels",
        "bedrock:GetFoundationModelAvailability",
        "bedrock:GetModelInvocationLoggingConfiguration",
        "bedrock:PutModelInvocationLoggingConfiguration",
        "bedrock:ListInferenceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudWatchBedrock",
      "Effect": "Allow",
      "Action": [
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource"
      ],
      "Resource": "arn:aws:logs:*:*:log-group:/aws/bedrock*"
    },
    {
      "Sid": "BedrockLoggingAttachRole",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::*:role/NetApp_AI_Bedrock*"
    },
    {
```

```
      "Sid": "BedrockLoggingIamOperations",
      "Effect": "Allow",
      "Action": [
        "iam:CreatePolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "QBusiness",
      "Effect": "Allow",
      "Action": [
        "qbusiness:ListApplications"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

下表提供了有关GenAI工作负载的权限的详细信息。

GenAI工作负载的权限表

目的	操作	使用位置	权限政策
在部署和重建操作期间创建AI引擎CloudFormation堆栈	CloudFormation：CreateStack	部署	读/写
创建AI引擎CloudFormation堆栈	CloudFormation：Describe堆栈	部署	读/写
列出AI引擎部署向导的区域	EC2：Describe注册	部署	读/写
显示AI引擎标签	EC2：Describe标记	部署	读/写
列出 S3 存储桶	S3： ListAllMy桶	部署	读/写
在创建AI引擎堆栈之前列出VPC端点	EC2：CreateVpcEndpoint	部署	读/写
在部署和重建操作期间创建AI引擎堆栈期间创建AI引擎安全组	EC2：CreateSecurityGroup	部署	读/写
标记在部署和重建操作期间创建AI引擎堆栈所创建的资源	EC2：CreateTags	部署	读/写
从AI引擎堆栈将加密事件发布到WLAMAI后端	Kms：GenerateDataKey	部署	读/写
	Kms：解密	部署	读/写
将事件和自定义资源从AI引擎堆栈发布到WLAMAI后端	SNS：发布	部署	读/写
在AI引擎部署向导期间列出vPC	EC2：Describe	部署	读/写
在AI引擎部署向导上列出子网	EC2：Describe子网	部署	读/写
在AI引擎部署和重建期间获取路由表	EC2：Describe RouteTables	部署	读/写
在AI引擎部署向导期间列出密钥对	EC2：Describe KeyPairs	部署	读/写
在创建AI引擎堆栈期间列出安全组(以在专用端点上查找安全组)	EC2：Describe安全性组	部署	读/写
获取VPC端点以确定是否应在AI引擎部署期间创建任何端点	EC2：Describe VpcEndpoints	部署	读/写
列出Amazon Q Business应用程序	qBusiness：ListApplications	部署	读/写
列出实例以了解AI引擎状态	EC2：Describe实例	故障排除	读/写
在部署和重建操作期间创建AI引擎堆栈期间列出映像	EC2：Describe	部署	读/写
在部署和重建操作期间创建AI实例堆栈期间、创建并更新AI实例和专用端点安全组	EC2 ：RevokeSecurityGroupEgress	部署	读/写
	EC2 ：RevokeSecurityGroupIngress	部署	读/写
在部署和重建操作期间创建CloudFormation堆栈期间运行AI引擎	EC2：RunInstances	部署	读/写

目的	操作	使用位置	权限政策
在部署和重建操作期间创建堆栈期间、附加安全组并修改AI引擎的规则	EC2：AuthorizeSecurityGroupEgress	部署	读/写
	EC2：AuthorizeSecurityGroupIngress	部署	读/写
向其中一个基础模型发起聊天请求	Bedrock：Invoke的 使用ResponseStream的数据	部署	读/写
开始聊天/嵌入基础模型请求	基岩：InvokeModel	部署	读/写
显示一个区域中可用的基础模型	Bound：ListFoundation们	部署	读/写
获取有关基础模型的信息	基岩：GetFoundationModel	部署	读/写
验证对基础模型的访问权限	Bound：GetFoundation论 可用性	部署	读/写
验证是否需要在部署和重建操作期间创建Amazon CloudWatch日志组	日志：可通过"LogBeLogGroup"进行操作	部署	读/写
在AI引擎向导期间获取支持FSx和Amazon Brock的区域	SSM：GetPathetersByPath	部署	读/写
获取用于在部署和重建操作期间部署AI引擎的最新Amazon Linux映像	SSM：GetParameters	部署	读/写
从发送到AI引擎的命令中获取SSM响应	SSM：GetCommandInvation	部署	读/写
检查与AI发动机的SSM连接	SSM：SendCommand	部署	读/写
	SSM：GetConnectionStatus	部署	读/写
在部署和重建操作期间创建堆栈期间创建AI引擎实例配置文件	IAM：CreateRole	部署	读/写
	IAM：CreateInstanceProfile	部署	读/写
	IAM：AddRoleToInstanceProfile	部署	读/写
	IAM：PutRolePolicy	部署	读/写
	IAM：GetRolePolicy	部署	读/写
	IAM：GetRole	部署	读/写
	IAM：TagRole	部署	读/写
	IAM：PassRole	部署	读/写
模拟工作负载操作以验证可用权限并与所需的AWS帐户权限进行比较	IAM：SimulatePrincipalPolicy	部署	读/写
在"创建数据库"向导期间列出FSx for ONTAP文件系统	FSx：可对卷进行分过程	创建知识库	读/写
在"创建集群"向导期间列出适用于ONTAP文件系统卷的FSx	FSx：可对FileSystems进行情况分类	创建知识库	读/写
在重建操作期间管理有关AI引擎的知识库	FSx：ListTagsForResource	故障排除	读/写

目的	操作	使用位置	权限政策
在"创建信息库"向导期间列出FSx for ONTAP文件系统Storage Virtual Machine	FSx：讲解StorageVirtualMachine	部署	读/写
将此信息文档移至新实例	FSx：UnTagResource	故障排除	读/写
在重建期间管理AI引擎上的信息存储	FSx：TagResource	故障排除	读/写
以安全的方式保存SSM密钥(ECR令牌、CIFS凭据、租户服务帐户密钥)	SSM：Get参 比器	部署	读/写
	SSM：Put\n参比器	部署	读/写
在部署和重建操作期间、将AI引擎日志发送到Amazon CloudWatch日志组	日志：CreateLogGroup	部署	读/写
	日志：PutRettionPolicy	部署	读/写
将AI引擎日志发送到Amazon CloudWatch日志组	日志:TagResource	故障排除	读/写
从Amazon CloudWatch获取SSM响应(响应时间过长)	日志：特性日志流	故障排除	读/写
从Amazon CloudWatch获取SSM响应	日志：GetLogEvents	故障排除	读/写
在部署和重建操作期间创建堆栈期间、为Amazon基岩日志创建Amazon CloudWatch日志组	日志：CreateLogGroup	部署	读/写
	日志：PutRettionPolicy	部署	读/写
	日志:TagResource	部署	读/写
列出模型的参考轮廓	Bedrock：ListInferenceProfile	故障排除	读/写

VMware工作负载的权限

VMware 工作负载有以下权限策略可供选择：

- 查看、规划和分析：查看 EVS 虚拟化环境的清单，获取系统架构完善的分析，并探索节省成本的方法。
- 数据存储部署和连接：将推荐的 VM 布局部署到 Amazon EVS、Amazon EC2 或 VMware Cloud on AWS vSphere 集群，并使用定制的Amazon FSx for NetApp ONTAP文件系统作为外部数据存储。

选择权限策略以查看所需的 IAM 策略：

视图、规划和分析

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeVpcs",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeDhcpOptions",
        "kms:DescribeKey",
        "kms:ListKeys",
        "kms:ListAliases",
        "secretsmanager:ListSecrets",
        "evs:ListEnvironments",
        "evs:GetEnvironment",
        "evs:ListEnvironmentVlans"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

数据存储部署和连接

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*"
```

```
    },
    {
      "Effect": "Allow",
      "Action": [
        "fsx:CreateFileSystem",
        "fsx:DescribeFileSystems",
        "fsx:CreateStorageVirtualMachine",
        "fsx:DescribeStorageVirtualMachines",
        "fsx:CreateVolume",
        "fsx:DescribeVolumes",
        "fsx:TagResource",
        "sns:Publish",
        "kms:GenerateDataKey",
        "kms:Decrypt",
        "kms:CreateGrant"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:DescribeInstances",
        "ec2:CreateSecurityGroup",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:SimulatePrincipalPolicy"
      ],
      "Resource": "*"
    }
  ]
}
```

下表提供了有关VMware工作负载权限的详细信息。

VMware工作负载的权限表

目的	操作	使用位置	权限政策
附加安全组并修改已配置节点的规则	EC2：AuthorizeSecurityGroupIngress	部署	数据存储部署和连接
创建EBS卷	FSx：CreateVolume	部署	数据存储部署和连接
为VMware工作负载创建的FSx for NetApp ONTAP资源标记自定义值	FSx：TagResource	部署	数据存储部署和连接
创建并验证CloudFormation模板	CloudFormation：CreateStack	部署	数据存储部署和连接
管理已创建实例上的标记和网络安全性	EC2：CreateSecurityGroup	部署	数据存储部署和连接
启动已创建的实例	EC2：RunInstances	部署	数据存储部署和连接
获取EC2实例详细信息	EC2：Describe实例	清单	数据存储部署和连接
在部署和重建操作期间创建堆栈期间列出映像	EC2：Describe	清单	数据存储部署和连接
查看与 VPC 关联的 DHCP 选项集的配置详情	ec2:描述DHCP选项	清单	视图、规划和分析
获取选定环境中的vPC以完成部署表单	EC2：Describe	• 部署 • 清单	视图、规划和分析
获取选定环境中的子网以完成部署表单	EC2：Describe子网	• 部署 • 清单	视图、规划和分析
获取选定环境中的安全组以完成部署表单	EC2：Describe安全性组	部署	视图、规划和分析
获取选定环境中的可用性分区	EC2：特性可用性区域	• 部署 • 清单	视图、规划和分析
通过Amazon FSx for NetApp ONTAP支持获取各个地区的信息	EC2：Describe注册	部署	视图、规划和分析
获取用于Amazon FSx for NetApp ONTAP加密的KMS密钥别名	Kms：ListAliases	部署	视图、规划和分析
获取用于Amazon FSx for NetApp ONTAP加密的KMS密钥	Kms：ListKey	部署	视图、规划和分析
获取用于Amazon FSx for NetApp ONTAP加密的KMS密钥到期详细信息	Kms：可通过键进行操作	部署	视图、规划和分析

目的	操作	使用位置	权限政策
列出 AWS Secrets Manager 中的密钥	secretsmanager:列出秘密	清单	视图、规划和分析
从 Amazon EVS 获取环境列表	evs:列出环境	清单	视图、规划和分析
获取有关特定 Amazon EVS 环境的详细信息	evs:GetEnvironment	清单	视图、规划和分析
列出与 Amazon EVS 环境关联的 VLAN	evs:列出环境VLAN	清单	视图、规划和分析
创建配置所需的Amazon FSx for NetApp ONTAP资源	FSx：CreateFileSystem	部署	数据存储部署和连接
	FSx ：CreateStorageVirtualMachine	部署	数据存储部署和连接
	FSx：CreateVolume	• 部署 • 管理操作	数据存储部署和连接
获取Amazon FSx for NetApp ONTAP详细信息	FSX：描述*	• 部署 • 清单 • 管理操作 • 了解节省量	数据存储部署和连接
获取KMS密钥详细信息并用于Amazon FSx以进行NetApp ONTAP加密	公里：CreateGrant	部署	数据存储部署和连接
	公里：描述*	部署	视图、规划和分析
	公里：列表*	部署	视图、规划和分析
	Kms：解密	部署	数据存储部署和连接
	Kms：GenerateDataKey	部署	数据存储部署和连接
列出客户SNS主题并发布到WLMVMC后端SNS以及客户SNS (如果选择)	SNS：发布	部署	数据存储部署和连接
模拟工作负载操作以验证可用权限并与所需的AWS帐户权限进行比较	IAM：SimulatePrincipalPolicy	部署	• 数据存储部署和连接 • 视图、规划和分析

更改日志

添加和删除权限后、我们将在以下各节中记录这些权限。

2025 年 2 月 1 日

以下权限已添加到存储工作负载：

- `s3:TagResource`
- `s3:ListTagsForResource`
- `s3:UntagResource`
- `s3tables:CreateTableBucket`
- `s3tables:ListTables`
- `s3tables:GetTable`
- `s3tables:GetTableMetadataLocation`
- `s3tables:CreateTable`
- `s3tables:GetNamespace`
- `s3tables:PutTableData`
- `s3tables:CreateNamespace`
- `s3tables:GetTableData`
- `s3tables:ListNamespaces`
- `s3tables:ListTableBuckets`
- `s3tables:GetTableBucket`
- `s3tables:UpdateTableMetadataLocation`
- `s3tables:ListTagsForResource`
- `s3tables:TagResource`
- `s3:GetObjectTagging`
- `s3:ListBucket`

2025 年 12 月 4 日

以下权限已添加到存储工作负载：

- `fsx:CreateAndAttachS3AccessPoint`
- `fsx:DetachAndDeleteS3AccessPoint`
- `s3:CreateAccessPoint`
- `s3:DeleteAccessPoint`

2025年11月27日

以下权限已添加到存储工作负载：

- `bedrock:ListInferenceProfiles`
- `bedrock:GetInferenceProfile`
- `bedrock:InvokeModelWithResponseStream`
- `bedrock:InvokeModel`

2025年11月2日

存储、数据库工作负载和 VMware 工作负载中的“只读”和“读/写”权限策略已被替换，以便在分配权限时提供更精细的粒度和更大的灵活性。

2025年10月5日

以下权限已从 GenAI 中删除，现在由 GenAI 引擎处理：

- `bedrock:GetModelInvocationLoggingConfiguration`
- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:CreatePolicy`

2025年6月29日

现在，数据库在只读模式下具有以下权限： `cloudwatch:GetMetricData` 。

2025年6月3日

现在，GenAI 在读/写模式下具有以下权限： `s3:ListAllMyBuckets` 。

2025年5月4日

现在，GenAI 在读/写模式下具有以下权限： `qbusiness:ListApplications` 。

现在，数据库在只读模式下具有以下权限：

- `logs:GetLogEvents`
- `logs:DescribeLogGroups`

现在，数据库在读/写模式下具有以下权限：
`logs:PutRetentionPolicy` 。

2025年4月2日

现在，数据库在只读模式下具有以下权限： `ssm:DescribeInstanceInformation` 。

2025年3月30日

GenAI工作负载权限更新

GenAI 的“读/写模式”下现在提供以下权限：

- `bedrock:PutModelInvocationLoggingConfiguration`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `iam:createPolicy`
- `bedrock:ListInferenceProfiles`

已从 GenAI 的“读/写模式”中删除以下权限： `Bedrock:GetFoundationModel` 。

IAM：SimulatePrincipalPolicy权限更新

这 `iam:SimulatePrincipalPolicy`如果您在添加其他 AWS 账户凭证或从 Workload Factory 控制台添加新的工作负载功能时启用自动权限检查，则权限是所有工作负载权限策略的一部分。该权限模拟工作负载操作，并在从工作负载工厂部署资源之前检查您是否具有所需的 AWS 账户权限。启用此检查可减少清理失败操作的资源和添加缺少的权限所需的时间和精力。

2025年3月2日

现在，GenAI 在读/写模式下具有以下权限： `bedrock:GetFoundationModel` 。

2025年2月3日

现在，数据库在只读模式下具有以下权限： `iam:SimulatePrincipalPolicy` 。

NetApp Workload Factory 快速入门

通过注册并创建账户开始使用NetApp Workload Factory，添加凭证以便 Workload Factory 可以直接管理 AWS 资源，然后使用Amazon FSx for NetApp ONTAP优化您的工作负载。

NetApp Workload Factory可通过基于 Web 的控制台以云服务的形式供用户访问。在开始之前，你应该了解 ……"工作负载工厂" 。

1 注册并创建帐户

前往 "工作负载工厂控制台"，注册并创建帐户。

"了解如何注册和创建帐户"(英文)

2 将 **AWS** 凭证添加到 **Workload Factory**

此步骤为可选步骤。您无需添加凭证即可使用 Workload Factory 访问您的 AWS 账户。将 AWS 凭证添加到 Workload Factory，即可使您的 Workload Factory 帐户拥有创建和管理 FSx for ONTAP文件系统以及部署和管

理特定工作负载（例如数据库和 GenAI）所需的权限。

"了解如何向帐户添加凭据"(英文)

3 使用**FSx for ONTAP**优化工作负载

注册、创建帐户并选择性添加 AWS 凭证后，您可以开始使用 Workload Factory 通过 FSx for ONTAP优化您的工作负载。

"使用 FSx for ONTAP优化您的工作负载" 。

注册NetApp Workload Factory

NetApp Workload Factory 可通过基于 Web 的控制台访问。当您开始使用 Workload Factory 时，您的第一步是使用现有的NetApp支持站点凭据进行注册或创建NetApp云登录。

您还可以邀请其他人加入您的 Workload Factory 帐户，以便他们可以访问和使用 Workload Factory。

注册 Workload Factory

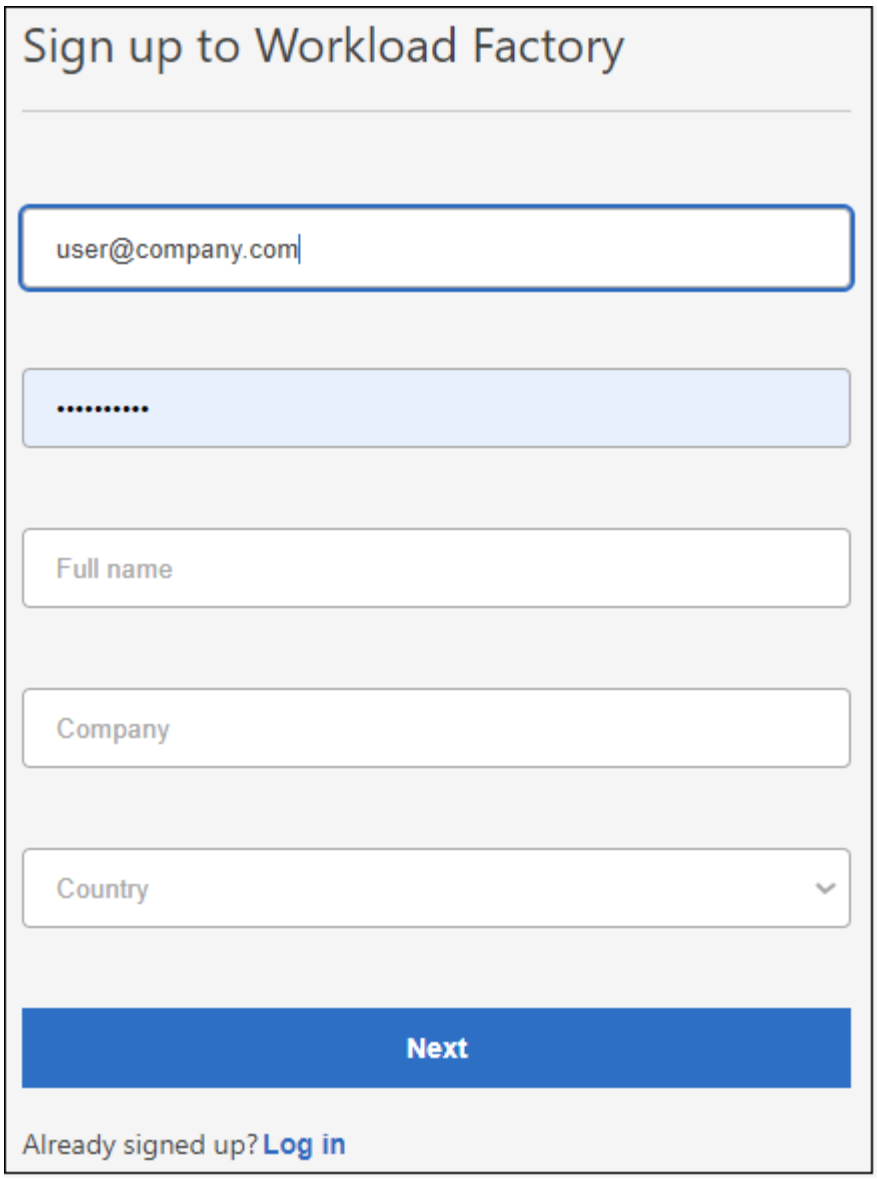
您可以使用以下选项之一注册 Workload Factory：

- 您的现有NetApp 支持站点 (NSS)凭据
- 通过指定您的电子邮件地址和密码来登录NetApp云

步骤

1. 打开 Web 浏览器并转到 "工作负载工厂控制台"
2. 如果您有NetApp 支持站点 帐户，请直接在*Log In*页面上输入与您的NSS帐户关联的电子邮件地址。

   如果您有 NSS 帐户，则可以跳过注册页面。 Workload Factory 将在您首次登录时为您注册。
3. 如果您没有NSS帐户、但要通过创建NetApp云登录来注册、请选择*注册*。



4. 在*注册*页面上、输入创建NetApp云登录所需的信息、然后选择*下一步*。

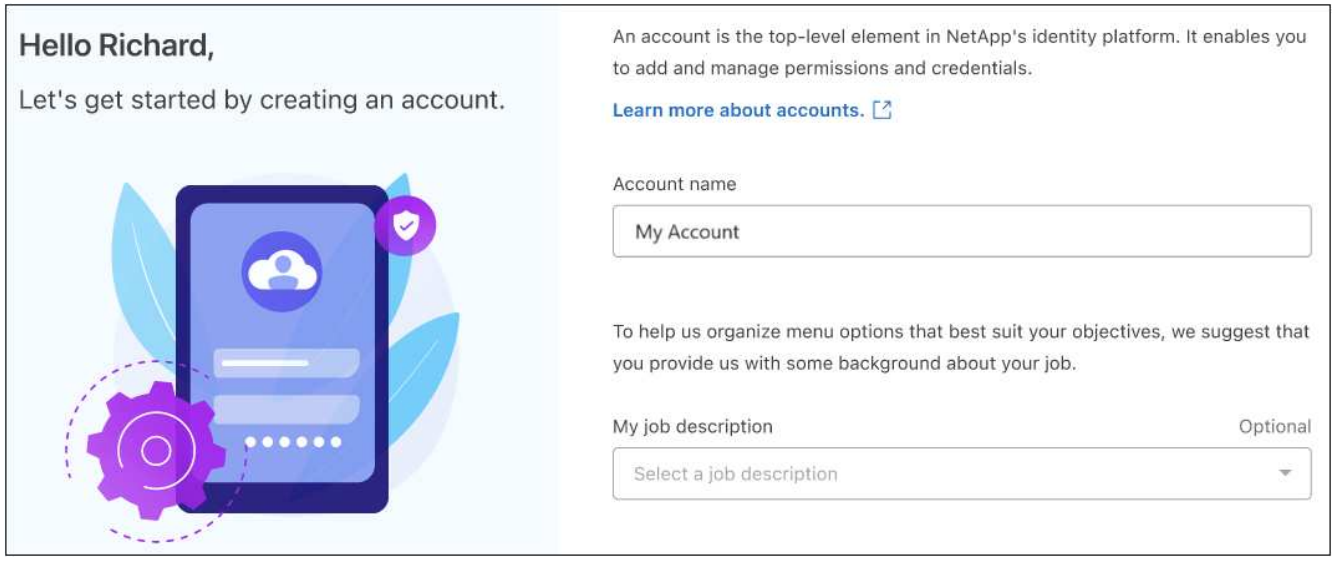
   请注意、注册表单中仅允许使用英文字符。

5. 输入您公司的详细信息，然后选择*Sign Up。
6. 检查您的收件箱中是否有来自NetApp的电子邮件、其中包含验证您的电子邮件地址的说明。

   必须先执行此步骤、然后才能登录。

7. 出现提示时，查看最终用户许可协议并接受条款，然后选择*CONTINUE*。
8. 在*Account*页面上，输入帐户名称，并选择您的工作描述。

   帐户是NetApp身份平台中的顶级元素、可用于添加和管理权限和凭据。



9. 选择*创建*，将显示 Workload Factory 主页。

结果

您现在拥有 Workload Factory 登录名和帐户。您被视为帐户管理员，可以访问所有 Workload Factory 功能。

邀请其他人加入 **Workload Factory** 帐户

作为帐户管理员，您可以邀请其他人加入您的 Workload Factory 帐户，以便他们可以访问和使用 Workload Factory。账户管理只能通过NetApp Console进行。

请参阅NetApp Console文档。 "了解如何添加成员（用户帐户）"到您的 Workload Factory 帐户。

结果

受邀用户将收到一封电子邮件，其中包含加入您的 Workload Factory 帐户的说明。

将 **AWS** 凭证添加到 **Workload Factory**

添加和管理 AWS 凭证，以便NetApp Workload Factory 拥有在您的 AWS 账户中部署和管理云资源所需的权限。

概述

您可以从“凭证”页面将 AWS 凭证添加到现有的 Workload Factory 帐户。这为 Workload Factory 提供了管理 AWS 云环境中的资源和流程所需的权限。

您可以使用两种方法添加凭据：

- 手动：您在 Workload Factory 中添加凭证时在您的 AWS 账户中创建 IAM 策略和 IAM 角色。
- 自动：您捕获有关权限的最少信息、然后使用CloudFormation堆栈为凭据创建IAM策略和角色。

AWS凭据

我们设计了一个AWS假定角色凭据注册流、该流可：

- 通过允许您指定要使用的工作负载功能并根据这些选择提供IAM策略要求、支持更一致的AWS帐户权限。
- 允许您在选择加入或退出特定工作负载功能时调整已授予的AWS帐户权限。
- 通过提供可在AWS控制台中应用的定制JSON策略文件、简化手动IAM策略创建。
- 通过使用AWS CloudFormation堆栈为用户提供所需IAM策略和角色创建的自动化选项、进一步简化了凭据注册流程。
- 通过允许将FSx for ONTAP服务凭据存储在基于AWS的机密管理后端、更好地与FSx for ONTAP用户保持一致、他们强烈希望将其凭据存储在AWS云生态系统的边界内。

一个或多个**AWS**凭据

当您使用第一个工作负载工厂功能（或多个功能）时，您需要使用这些工作负载功能所需的权限来创建凭据。您将把凭证添加到 Workload Factory，但您需要访问 AWS 管理控制台来创建 IAM 角色和策略。当使用 Workload Factory 中的任何功能时，这些凭证将在您的帐户中可用。

您的初始 AWS 凭证集可以包含针对一项功能或多项功能的 IAM 权限策略。这完全取决于您的业务需求。

向 Workload Factory 添加多组 AWS 凭证可提供使用其他功能所需的额外权限，例如 FSx for ONTAP文件系统、在 FSx for ONTAP上部署数据库、迁移 VMware 工作负载等。

手动向帐户添加凭据

您可以手动将 AWS 凭证添加到 Workload Factory，以授予您的 Workload Factory 帐户管理用于运行独特工作负载的 AWS 资源所需的权限。您添加的每组凭证都将包含一个或多个基于您要使用的工作负载功能的 IAM 策略，以及分配给您账户的 IAM 角色。

您可以从 Workload Factory 控制台或NetApp控制台将 AWS 凭证添加到帐户。

创建凭据分为三部分：

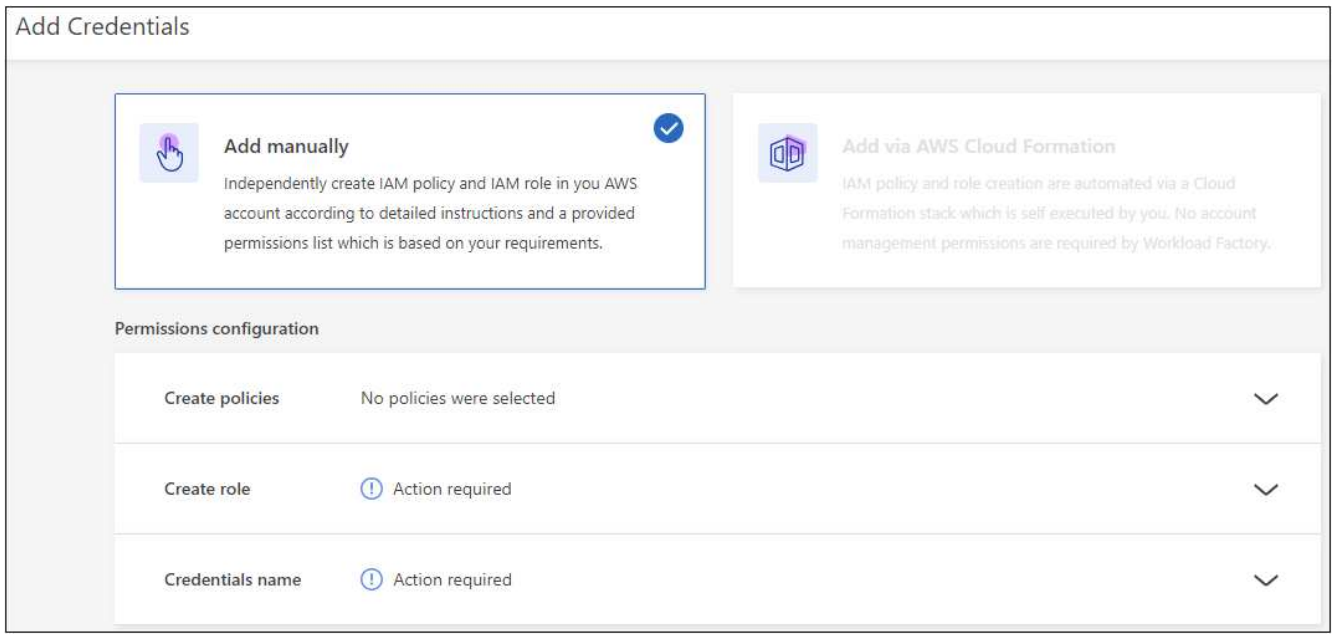
- 选择要使用的服务和权限级别、然后从AWS管理控制台创建IAM策略。
- 从AWS管理控制台创建IAM角色。
- 从 Workload Factory 中输入名称并添加凭据。

开始之前

您需要具有凭据才能登录到AWS帐户。

步骤

1. 登录 "工作负载工厂控制台"。
2. 从菜单中选择“管理”，然后选择“凭据”。
3. 在“凭据”页面上，选择*添加凭据*。
4. 在添加凭据页面上、选择*手动添加*、然后使用以下步骤完成_Permissions configuration_下的每个部分。



第**1**步：选择工作负载功能并创建**IAM**策略

在本节中、您将选择哪些类型的工作负载功能可作为这些凭据的一部分进行管理、以及为每个工作负载启用的权限。您需要从CodeBox中复制每个选定工作负载的策略权限、并将其添加到AWS帐户中的AWS管理控制台中以创建策略。

步骤

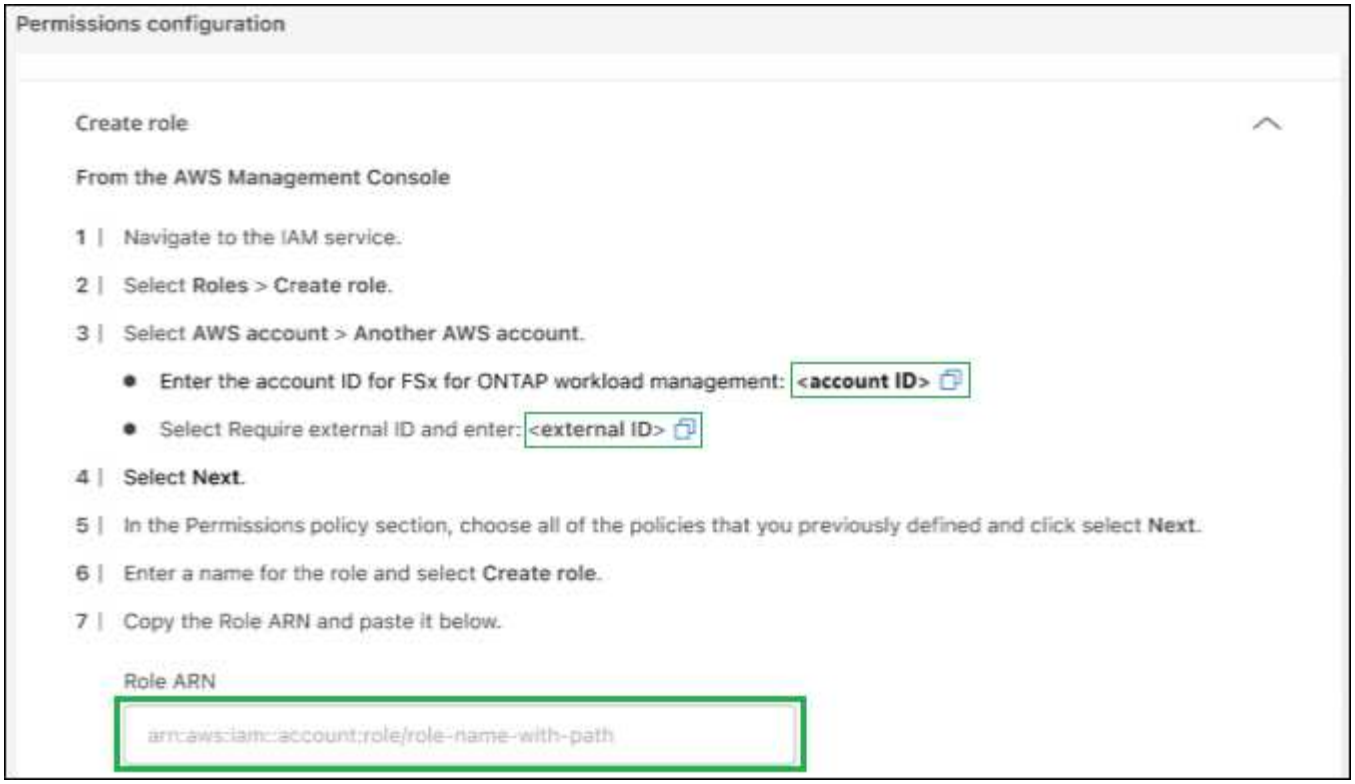
1. 在*Create Policies*部分中，启用要包含在这些凭据中的每个工作负载功能。

   您可以稍后添加其他功能、因此只需选择当前要部署和管理的工作负载即可。

2. 对于那些提供权限策略选择的工作负载功能，请选择使用这些凭据可获得的权限类型。
3. 可选：选择*启用自动权限检查*以检查您是否具有完成工作负载操作所需的AWS帐户权限。启用此复选框会将添加 `iam:SimulatePrincipalPolicy permission`到权限策略中。此权限的目的仅是确认权限。您可以在添加凭据后删除此权限、但我们建议保留此权限、以防止为部分成功的操作创建资源、并避免手动清理任何所需的资源。
4. 在CodeBox窗口中、复制第一个IAM策略的权限。
5. 打开另一个浏览器窗口、并在AWS管理控制台中登录到您的AWS帐户。
6. 打开IAM服务，然后选择*Policies*>*Create Policy*。
7. 选择JSON作为文件类型，粘贴您在第3步中复制的权限，然后选择*Next*。
8. 输入策略的名称，然后选择*Create Policy*。
9. 如果您在步骤1中选择了多个工作负载功能、请重复这些步骤为每组工作负载权限创建一个策略。

第**2**步：创建使用策略的**IAM**角色

在本节中，您将设置 Workload Factory 将承担的 IAM 角色，其中包括您刚刚创建的权限和策略。



步骤

1. 在AWS管理控制台中、选择*角色>创建角色*。
2. 在 * 可信实体类型 * 下，选择 * AWS 帐户 * 。
   a. 选择 另一个 **AWS** 账户，然后从 Workload Factory UI 复制并粘贴 FSx for ONTAP工作负载管理的账户 ID。
   b. 选择*所需的外部 ID*并从 Workload Factory UI 复制并粘贴外部 ID。
3. 选择 * 下一步 * 。
4. 在权限策略部分中，选择先前定义的所有策略，然后选择*Next*。
5. 输入角色的名称，然后选择*Create Role*。
6. 复制角色ARN。
7. 返回 Workload Factory 中的“添加凭证”页面，展开“权限配置”下的“创建角色”部分，然后将 ARN 粘贴到“角色 ARN”字段中。

第**3**步：输入名称并添加凭据

最后一步是在 Workload Factory 中输入凭证的名称。

步骤

1. 在 Workload Factory 中的“添加凭据”页面中，展开“权限配置”下的“凭据名称”。
2. 输入要用于这些凭据的名称。
3. 选择*Add*以创建凭据。

结果

此时将创建凭据、您将返回到"凭据"页面。

使用CloudFormation向帐户添加凭据

您可以使用 AWS CloudFormation 堆栈将 AWS 凭证添加到 Workload Factory，方法是选择要使用的 Workload Factory 功能，然后在您的 AWS 账户中启动 AWS CloudFormation 堆栈。 CloudFormation 将根据您选择的工作负载功能创建 IAM 策略和 IAM 角色。

开始之前

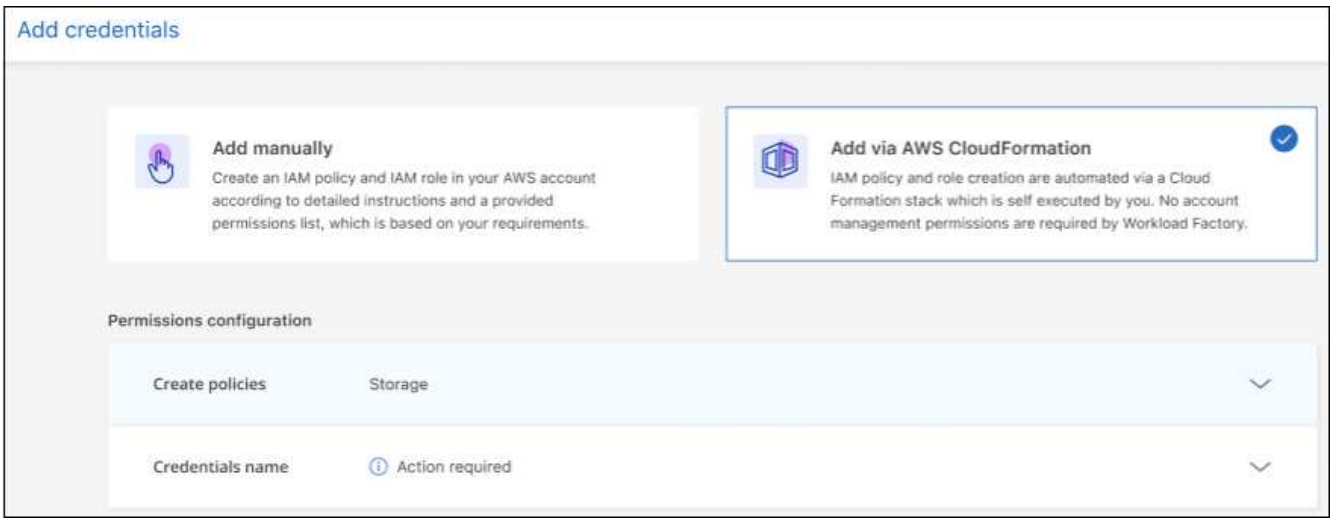
- 您需要具有凭据才能登录到AWS帐户。
- 使用CloudFormation堆栈添加凭据时、您需要在AWS帐户中具有以下权限：

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:UpdateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeChangeSet",
        "cloudformation:ExecuteChangeSet",
        "cloudformation:ListStacks",
        "cloudformation:ListStackResources",
        "cloudformation:GetTemplate",
        "cloudformation:ValidateTemplate",
        "lambda:InvokeFunction",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:UpdateAssumeRolePolicy",
        "iam:AttachRolePolicy",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

步骤

1. 登录 "工作负载工厂控制台"。
2. 从菜单中选择“管理”，然后选择“凭据”。

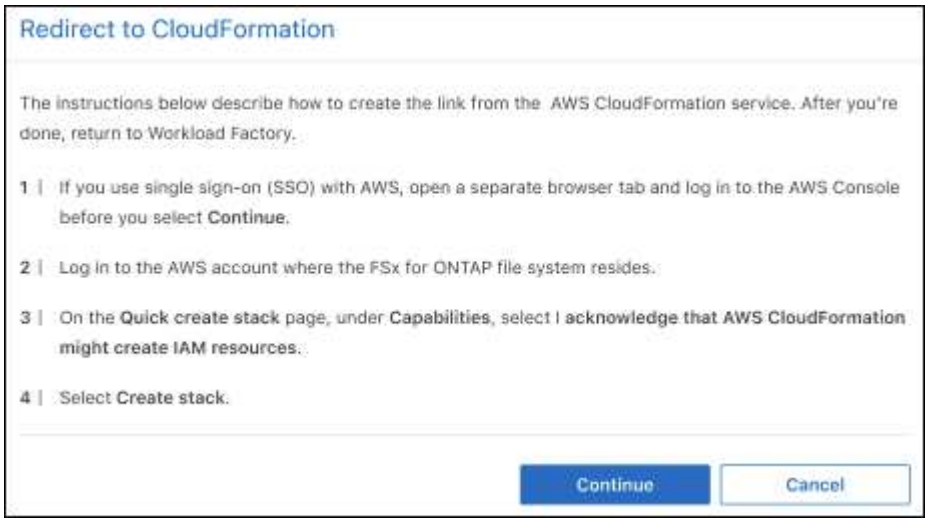
3. 在“凭据”页面上，选择*添加凭据*。
4. 选择*通过AWS CloudFormation*添加。



5. 在*创建策略*下，启用要包含在这些凭据中的每个工作负载功能，然后为每个工作负载选择一个权限级别。

   您可以稍后添加其他功能、因此只需选择当前要部署和管理的工作负载即可。

6. 可选：选择*启用自动权限检查*以检查您是否具有完成工作负载操作所需的AWS帐户权限。启用此复选框会将权限添加 `iam:SimulatePrincipalPolicy`到权限策略中。此权限的目的仅是确认权限。您可以在添加凭据后删除此权限、但我们建议保留此权限、以防止为部分成功的操作创建资源、并避免手动清理任何所需的资源。
7. 在*凭据名称*下，输入要用于这些凭据的名称。
8. 从AWS CloudFormation添加凭据：
   a. 选择*添加*(或选择*重定向到CloudFormation*)、此时将显示重定向到CloudFormation页面。



   b. 如果在AWS中使用单点登录(SSO)、请先打开单独的浏览器选项卡并登录AWS控制台、然后再选择*继续*。

      您应登录到FSx for ONTAP文件系统所在的AWS帐户。

c. 从重定向到CloudFormation页面中选择*继续*。

d. 在Quick create堆栈页面的"Capabilities"下、选择*我确认AWS CloudFormation可能会创建IAM资源*。

e. 选择*创建堆栈*。

f. 返回 Workload Factory 并监视 Credentials 页面以验证新凭证是否正在进行中，或者是否已添加。

使用NetApp Workload Factory 优化工作负载

登录并设置NetApp Workload Factory 后，您可以开始使用多种 Workload Factory 功能，例如创建Amazon FSx for ONTAP文件系统、在 FSx for ONTAP文件系统上部署数据库以及使用 FSx for ONTAP文件系统作为外部数据存储将虚拟机配置迁移到 VMware Cloud on AWS。

- "适用于 NetApp ONTAP 的 Amazon FSX"

  通过使用FSx for ONTAP作为存储基础架构、根据最佳实践配置FSx for ONTAP部署并对其进行模板化、以及访问高级管理功能、评估和分析当前数据资产、以节省潜在成本。

- "数据库工作负载"

  在AWS上检测现有数据库资产、通过迁移到FSx for ONTAP评估潜在的成本节省、利用内置的最佳优化实践端到端部署数据库、以及自动执行CI/CD管道精简克隆。

- "GenAI"

  部署和管理"再构建一代"(RAG)基础架构、以提高AI应用程序的准确性和独特性。创建有关FSx for ONTAP的RAG知识库、其中包含内置的数据安全性和合规性。

- "VMware工作负载"

  利用智能建议和自动修复简化迁移和操作。部署高效备份和强大的灾难恢复。监控VM并对其进行故障排除。

- "EDA工作负载"

  通过自动化存储参数管理，优化跨多个文件系统的 FSx for ONTAP ，以提高性能并降低运营成本。

管理工作负载工厂

登录NetApp Workload Factory

注册NetApp Workload Factory 后，您可以随时从基于 Web 的控制台登录，开始管理您的工作负载和 FSx for ONTAP文件系统。

关于此任务

您可以使用以下选项之一登录 Workload Factory 基于 Web 的控制台：

- 您的现有NetApp 支持站点 (NSS)凭据
- 使用您的电子邮件地址和密码登录NetApp云

步骤

1. 打开 Web 浏览器并转到 "工作负载工厂控制台"。
2. 在*登录*页面上、输入与您的登录关联的电子邮件地址。
3. 根据与您的登录关联的身份验证方法、系统将提示您输入凭据：
   - NetApp云凭据：输入密码
   - 联合用户：输入您的联合身份凭据
   - NetApp 支持站点 帐户：输入您的NetApp 支持站点 凭据
4. 选择*登录*。

   如果您以前成功登录，您将看到 Workload Factory 主页，并且您将使用默认帐户。

   如果这是您首次登录，您将被引导至*Account*页面。

   - 如果您是单个帐户的成员，请选择*继续*。
   - 如果您是多个帐户的成员，请选择该帐户并选择*CONTINUE*。

结果

您现在已登录并可以开始使用 Workload Factory 来管理 FSx for ONTAP文件系统和您的工作负载。

管理服务帐户

创建服务帐户、充当自动化基础架构操作的计算机用户。您可以随时撤消或更改对服务帐户的访问权限。

关于此任务

服务帐户是NetApp提供的多租户功能。帐户管理员创建服务帐户、控制访问和删除服务帐户。您可以在NetApp控制台或NetApp Workload Factory 控制台中管理服务帐户。

与在NetApp控制台中管理服务帐户（您可以在其中重新创建客户端密钥）不同，Workload Factory 仅支持创建和删除服务帐户。如果您想在NetApp Workload Factory 控制台中为特定服务帐户重新创建客户端密钥，则需要删除服务帐户， 进而创建一个新的。

服务帐户使用客户端ID和密钥进行身份验证、而不是使用密码。客户端ID和密钥将一直固定、直到帐户管理员决定更改它们为止。要使用服务帐户、您将需要客户端ID和密钥来生成访问令牌、否则您将无法获得访问权限。请注意、访问令牌寿命很短、只能使用几个小时。

开始之前

决定是否要在NetApp控制台或 Workload Factory 控制台中创建服务帐户。存在一些细微的差别。以下说明描述了如何在 Workload Factory 控制台中管理服务帐户。

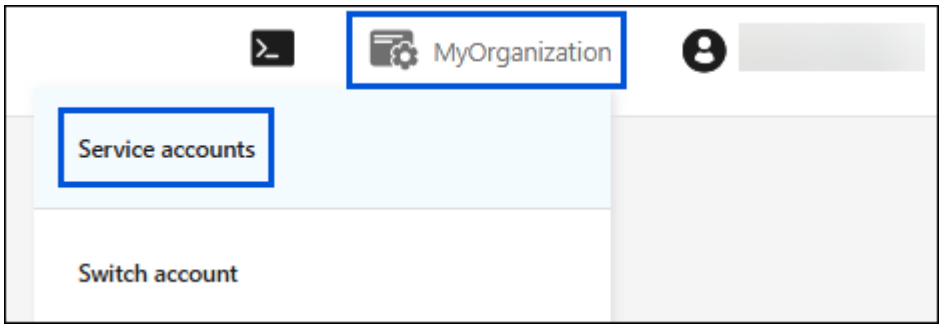
要在NetApp控制台中管理服务帐户，"了解身份和访问管理的工作原理"和"了解如何添加 IAM 成员并管理他们的权限"。

创建服务帐户

当您创建服务帐户时，Workload Factory 允许您复制或下载该服务帐户的客户端 ID 和客户端密钥。该密钥对用于与 Workload Factory 进行身份验证。

步骤

1. 在Workload Factory控制台中，选择*Account*图标，然后选择*Service accounts*。



2. 在*服务帐户*页面上，选择*创建服务帐户*。
3. 在“创建服务帐户”对话框中，在*Service account name*字段中输入服务帐户的名称。

   此时将预选*角色*作为*帐户管理员*。

4. 选择 * 继续 * 。
5. 复制或下载客户端 ID 和客户端密钥。

   客户端密钥仅可见一次，并且不会被 Workload Factory 存储在任何地方。复制或下载秘密并安全存储。

6. 或者，您可以通过执行客户端凭证交换来获取 Auth0 管理 API 的访问令牌。 curl 示例展示了如何获取客户端 ID 和密钥并使用 API 生成有时间限制的访问令牌。该令牌可提供数小时的NetApp Workload Factory API访问权限。
7. 选择 * 关闭 * 。

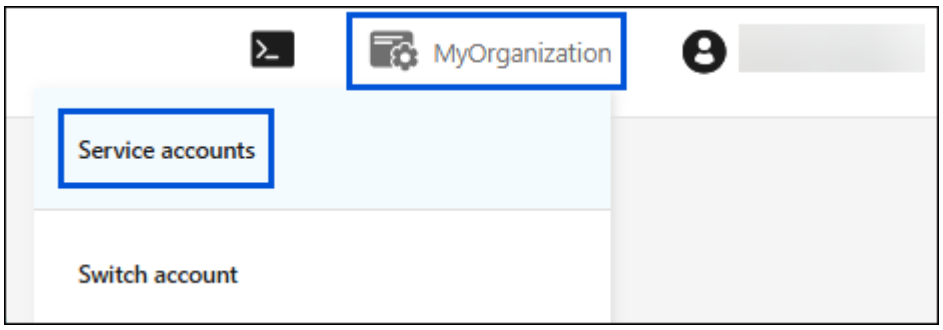
此时将创建新的服务帐户、并将其列在服务帐户页面上。

删除服务帐户

如果不再需要使用某个服务帐户，请将其删除。

步骤

1. 在Workload Factory控制台中，选择*Account*图标，然后选择*Service accounts*。



2. 在*服务帐户*页面上，选择操作菜单，然后选择*删除*。
3. 在“删除服务帐户”对话框中，在文本框中输入*DELETE*。
4. 选择*Delete*确认删除。

构建和运行架构良好的工作负载

Workload Factory 是NetApp为Amazon FSx for NetApp ONTAP开发的管理套件，可帮助您维护和运行符合 AWS 良好架构框架的可靠、安全、高效且经济的存储和数据库配置。Workload Factory 提供每日存储和数据库工作负载分析、建议和自动修复，以促进健康的工作负载运行。通过自动化这一过程，工作负载工厂最大限度地减少了人为错误，并确保了工作负载管理的一致性。

工作原理

Workload Factory 每天分析 Amazon FSx for NetApp ONTAP 文件系统、Microsoft SQL Server 和 Oracle 数据库部署。该分析提供了精心设计的状态、见解和建议。您可以自动修复配置问题，以满足最佳实践并高效运行。

每日分析完成后，部署的配置会在“架构完善”仪表板中显示为“已优化”或“未优化”。您将看到总优化得分、按类别划分的配置问题以及配置问题和建议列表。您可以查看针对配置问题的建议。有些问题可以由工作负载工厂自动修复，而另一些问题则需要人工干预。在这种情况下，工作负载工厂会提供详细的说明来帮助您实施建议的更改。

您可以忽略不适用于您环境的配置分析。这样可以避免不必要的警报和不准确的优化结果。当您忽略特定配置分析时，Workload Factory 不将配置包含在总优化分数中。

为什么这很重要

Workload Factory 通过将持续评估与建议见解和补救措施相结合，将最佳实践应用于大型存储或数据库环境。自动化修复可减少人为错误，确保统一管理，并保持性能和可靠性。在 Workload Factory 控制台中应用的修复减少了人为错误，并确保了统一的管理。自动化可确保正确应用和维护配置，从而保持整个工作负载基础架构的性能和可靠性。

开始使用 **Workload Factory** 来检测和纠正错误配置

要开始使用 Workload Factory，请注册、添加凭据并建立连接，以便使用 Amazon FSx for NetApp ONTAP 管理 AWS 资源并优化工作负载。

"快速入门"

存储工作负载的最佳实践和建议

Workload Factory 评估存储配置，以提供 ONTAP 配置最佳实践的深入视图，并符合 AWS Well-Architected Framework。评估还提出了改进和修复建议。

精心设计的分析将配置按以下框架支柱进行分类：可靠性、安全性、卓越运营、成本优化_和_性能效率。

可靠性

可靠性确保工作负载即使在出现中断的情况下也能正确、持续地执行其预期功能。

- 安排 **FSx** 用于**ONTAP**备份

  FSx for ONTAP：备份卷有助于支持数据保留和合规性需求。使用 FSx for ONTAP 备份为您的数据设置自动备份和保留。

- 安排本地快照

  安排本地快照以实现高效备份和快速恢复。快照是卷的即时、特定时间点的图像。

- 跨区域复制

  跨区域复制可确保将您的数据复制到另一个 AWS 区域，从而提高数据的持久性和可用性。Workload Factory 建议设置跨区域复制，以帮助灾难恢复和合规性。

- 设置数据复制

  为了提高数据可靠性，可以将数据复制到同一区域或其他区域的 FSx for ONTAP文件系统。设置数据复制以支持跨文件系统的迁移、灾难恢复和长期保留。

- 提高固态硬盘容量阈值

  SSD存储层的容量利用率不应持续超过80%。这可能会影响对容量池存储层的数据读取和写入，并影响文件系统的吞吐量。容量不足可能导致数据卷变为只读，尝试写入新数据的服务可能会失败。

- 核对标签以确保数据可靠性

  源卷的快照策略标签和复制策略标签必须匹配，以确保数据可靠性。

- 提高文件容量阈值

  应提高文件容量阈值，以避免达到卷容量限制。文件容量（inodes）不足，无法向卷中写入更多数据。Workload Factory 建议持续将可用文件容量的利用率保持在 80% 以下。需要有足够的可用文件容量才能在该卷中创建新文件。

安全性

安全重点在于通过风险评估和缓解策略来保护数据、系统和资产。

- 启用**ARP/AI**

NetApp Autonomous Ransomware Protection with AI (ARP/AI) 有助于保护您的卷免受勒索软件威胁。Workload Factory 建议为所有卷启用 ARP/AI。

- 未经授权访问卷

  使用 iSCSI 提供应用程序数据的卷不应允许并行访问 NAS。Workload Factory 建议，通过 iSCSI 协议访问的卷应限制为仅支持其他协议。

卓越运营

卓越运营的重点在于提供最优的架构和业务价值。

- 启用自动容量管理

  应启用自动容量管理，定期确保 SSD 层不超过阈值。

- 产能利用率阈值

  Workload Factory 建议容量利用率不要持续超过 80%。这可能会影响应用程序的数据读取和写入。容量增加可以手动进行，也可以使用容量自动增长功能自动进行。

- 产能利用率接近饱和

  当卷接近满负荷时，Workload Factory 建议采取措施增加卷容量，以避免潜在的应用程序中断。

- 缓存关系写入模式

  为了获得最佳性能，Workload Factory 会推荐最适合您工作负载的缓存关系写入模式。对于读取密集型工作负载和小文件，写回模式可提供更好的性能；而对于写入密集型工作负载和大文件，写回模式可提供更好的性能。

- 优化缓存卷大小

  Workload Factory 建议在缓存卷上启用卷自动调整大小和清理，以保持最佳大小，并将缓存集中在热数据上，以实现最高效率。

- **Storage VM** 逻辑报告

  Workload Factory 建议将存储虚拟机的默认报告设置设置为逻辑，以便更好地了解卷级别的存储使用情况。

成本优化

成本优化可帮助您在保持低成本的同时为业务创造最大价值。

- 通过对冷数据进行分层来优化总体拥有成本

  应启用冷数据分层，以降低 SSD 存储层的使用率。建议对每个卷应用分层策略。FSx for ONTAP会持续扫描数据，检测冷数据并将其移动到容量存储池层，而不会造成任何中断。

- 提高存储效率

  应启用存储效率提升功能（压缩、整理和去重），以优化存储利用率并降低 SSD 层成本。

- 不必要的快照和备份删除

  为降低成本，应删除不再需要的快照和备份。

- 孤立的块设备

  在块设备未使用七天后，Workload Factory 建议归档块设备数据或删除未使用的块设备以降低成本。

数据库工作负载的最佳实践和建议

Workload Factory 提供了一套运行架构良好的数据库工作负载的最佳实践和建议。精心设计的分析评估了 Microsoft SQL Server 和 Oracle 数据库的配置和设置，包括存储大小、存储布局、存储配置、计算、应用程序（SQL Server）和弹性。

存储尺寸

- 存储层

  为获得最佳存储性能，请在主 SSD 层上创建 FSx for ONTAP 卷。使用容量池层可能会降低性能并增加延迟。

- 文件系统余量

  要优化存储性能，请将文件系统容量设置为卷总大小的 1.35 倍。

  文件系统剩余空间百分比如下：

  - 准备不足：< 35%
  - 优化范围：35-100%
  - 资源过度配置：> 100%

- 日志驱动器大小

  确保 SQL Server 日志驱动器的大小准确，并定期进行监控，以防止因日志驱动器已满而导致的事务回滚、数据库不可用、数据损坏和性能下降等问题。

  日志驱动器容量百分比如下：

  - 准备不足：< 20%
  - 优化后：20-30%
  - 超额配置：> 30%

- **TempDB** 驱动器大小

  确保 SQL Server TempDB 的大小准确，并定期进行监控，以优化性能并保持整体稳定性。正确配置 TempDB 可以防止性能问题和系统不稳定。空间不足或竞争激烈会导致查询速度变慢、应用程序超时和系统崩溃。

  TempDB 驱动器大小百分比如下：

  - 准备不足：< 10%

- 优化后：10-20%
- 超额配置：> 20%

存储布局

- 数据文件（**.mdf**）放置位置

  将数据和日志文件分离到不同的驱动器上，以提高性能、启用独立备份计划并改进还原功能。对于较小的数据库，请将数据和日志 LUN 路径分隔到不同的卷中。对于多个大型数据库（> 500 GiB），需要进行此分离。

- 日志文件（**.ldf**）放置位置

  将数据和日志文件分离到不同的驱动器上，以提高性能、启用独立备份计划并改进还原功能。对于较小的数据库，请将数据和日志 LUN 路径分隔到不同的卷中。对于多个大型数据库（> 500 GiB），需要进行此分离。

- **TempDB** 放置

  通过将 TempDB 放置在其自身的专用驱动器上，隔离 TempDB 的 I/O，避免与其他数据库发生 I/O 争用。此优化可提高 SQL Server 的整体性能和稳定性。否则可能会导致严重的 I/O 瓶颈、查询性能下降以及潜在的系统不稳定。

存储配置

- ONTAP配置*

实体	设置	建议
卷	• 精简配置（-space -guarantee = none） • 自动调整大小 • 自动调整大小模式 = 增长 • 部分准备金率 = 0% • 快照副本预留量 = 0% • 快照自动删除（按卷/最早的快照优先） • 空间管理优先尝试 = volume_grow	为了优化存储效率和成本效益，请为 FSx for ONTAP卷配置精简配置、自动调整大小和空间管理选项。如果没有精简配置，存储空间会被预先分配，导致过度配置，从而造成使用效率低下和成本增加；静态分配会导致为未使用的容量付费，增加支出；缺乏动态分配会阻碍可扩展性和灵活性，影响性能；如果没有空间回收，删除的数据会占用空间，降低效率。
卷	• 分层策略 = 仅快照 • 分级最低制冷天数 = 7	为了获得最佳的数据库性能和成本效益，Workload Factory 建议仅将快照移动到容量层。该策略可在保证高性能的同时降低成本。尤其建议对超过 7 天的快照进行分层。

实体	设置	建议
LUN	操作系统类型 = windows_2008	ONTAP LUN OS 类型值应与操作系统分区方案相匹配，以实现 I/O 对齐。配置不正确可能会导致性能不佳。
LUN	已启用空间预订	启用空间预留后， ONTAP会在卷中预留足够的空间，以避免因磁盘空间不足而导致对这些 LUN 的写入失败。
LUN	空间分配已启用	此选项可确保 FSx for ONTAP在卷已满且无法接受写入时通知 EC2 主机。此设置还允许 FSx for ONTAP在 EC2 主机上的 SQL Server 删除数据时自动回收空间。如果禁用此功能，可能会出现写入失败，并且空间利用率可能不高。

- Windows存储配置

实体	设置	建议
Microsoft 多路径 I/O (MPIO)	• 状态 = 已启用 • 策略 = 轮询 • 疗程次数 = 5	为了确保在 EC2 上使用 FSx for ONTAP中配置的底层 LUN 的 Microsoft SQL Server 数据库的最佳正常运行时间和数据访问一致性，Workload Factory 建议启用和配置多路径 I/O (MPIO)。MPIO 为ONTAP提供多条 FSx 访问路径，从而增强了系统的弹性和性能。这种最佳实践通过即使某个组件发生故障也能保持数据访问，从而防止潜在的数据丢失或停机。
分配单位大小	NTFS 分配单元大小 = 64K	将 NTFS 分配单元大小设置为 64K，以更好地利用磁盘空间，减少碎片，并提高文件读/写性能。如果未能正确配置，可能会导致磁盘使用效率低下和性能下降。

计算

- 计算资源调整

  为确保您的 SQL Server EC2 实例达到最佳性能和成本效益，我们建议您根据工作负载需求调整实例大小。如果您的当前实例配置不足，升级将提升 CPU、内存和 I/O 容量。如果资源配置过高，降级配置既能保持性能，又能降低成本。

- 操作系统补丁

  Workload Factory 建议应用最新修补程序以确保安全性、保护 SQL Server 数据库免受漏洞影响以及提高系统可靠性。

- 网络适配器设置

  准确配置接收端缩放 (RSS) 对于 Microsoft SQL Server 实例的最佳网络性能至关重要。RSS 将网络处理分布到多个处理器上，防止出现瓶颈，提高系统性能。Workload Factory 建议采用以下 RSS 设置：

- 禁用 TCP 卸载功能：确保所有 TCP 卸载功能均已禁用。
- 接收队列数量：如果 vCPU 数量大于 8，则设置为 8。如果 vCPU 数量 ≤ 8，则设置为 vCPU 的数量。
- RSS配置文件：设置为NUMAStatic。
- 基本处理器编号：设置为 2。

  按照这些设置操作，将提高 Microsoft SQL Server 实例的性能和可靠性。我们建议您在对生产环境进行更改之前，先测试推荐的设置，以确定性能改进情况。

应用程序（**SQL Server**）

- 执照

  SQL Server 许可证评估和建议是在主机级别提供的。

  未优化：当 Workload Factory 检测到您的数据库基础架构未使用您付费购买的任何商业软件许可功能时，该许可证将被视为“未优化”。未优化的许可证可能会导致不必要的成本。

  优化：当数据库的商业软件许可证满足您的性能要求时，该许可证就被认为是“优化”的。

- 微软 **SQL Server** 补丁

  Workload Factory 建议应用最新修补程序以确保安全性、保护 SQL Server 数据库免受漏洞影响以及提高系统可靠性。

- **MAXDOP**

  设置最大并行度 (MAXDOP) 以平衡并行处理，从而优化查询性能。精确的 MAXDOP 配置可提高性能和效率。在大多数使用场景下，将 MAXDOP 设置为 4、8 或 16 通常可以获得最佳效果。我们建议您测试您的工作负载，并监控任何与并行性相关的等待类型，例如 CXPACKET。

可靠性

- 安排 **FSx** 用于**ONTAP**备份

  备份 Microsoft SQL Server 卷对于支持数据保留和合规性要求至关重要。使用 FSx for ONTAP 备份来设置 SQL Server 数据的自动备份和保留。

- 安排本地快照

  安排本地快照以实现高效备份和快速恢复。快照是卷的即时、特定时间点的图像。

- 跨区域复制

  跨区域复制可确保将您的数据复制到另一个 AWS 区域，从而提高数据的持久性和可用性。Workload Factory 建议设置跨区域复制，以帮助灾难恢复和合规性。

EVS 工作负载的最佳实践和建议

Workload Factory 为运行架构良好的 Amazon Elastic VMware Service (EVS) 工作负载提供了最佳实践和建议。

精心设计的分析评估 EVS 配置，以帮助确保您的 VMware 环境在可靠性、安全性、卓越运营、成本优化和性能效率方面得到优化。在 VMware 中精心设计的状态选项卡中，您可以找到见解和建议，以帮助为您的 EVS 环境实施精心设计的最佳实践。

精心设计的分析将配置分类到框架的以下支柱中：可靠性 和 安全性。

可靠性

可靠性确保工作负载即使在出现中断的情况下也能正确、持续地执行其预期功能。

- **EVS** 环境弹性

  确保您的 EVS 群集节点正确分布在分区放置组中。所有节点都应是配置有四个或更多分区的单个分区放置组的成员。正确的分区放置可确保您的 EVS 群集节点分布在 AWS 可用区内的多个故障隔离硬件分区中。如果分区发生故障，错位可能会导致处理能力的严重损失或停机。

安全性

安全重点在于通过风险评估和缓解策略来保护数据、系统和资产。

- 集群节点管理

  确保您的 EVS 集群节点配置了适当的 EC2 停止和终止保护。EVS ESXi 节点应仅使用 vCenter 或其他 VMware 级管理工具进行管理。如果没有适当的 EC2 级保护，节点可能会意外停止或从 EC2 控制台终止，从而可能导致虚拟机数据不可用或数据丢失。

相关信息

- "为ONTAP文件系统实现架构良好的 FSx"
- "实现架构良好的数据库工作负载"
- "实施精心设计的 EVS 配置"

配置NetApp Workload Factory 通知

您可以配置NetApp Workload Factory 通知服务，以将通知作为NetApp控制台中的警报或 Amazon SNS 主题发送。当您部署控制台代理或链接时，以警报形式发送的通知会出现在NetApp控制台中。当 Workload Factory 向 Amazon SNS 主题发布通知时，该主题的订阅者（例如人员或其他应用程序）会在为该主题配置的端点接收通知（例如电子邮件或短信）。

通知类型和消息

Workload Factory 针对以下事件发送通知：

事件	说明	通知类型	严重性	工作负载	资源类型
您帐户中的某些数据库实例架构不佳	您的帐户中的所有 Microsoft SQL Server 实例均已针对架构问题进行分析。此事件的描述给出了架构良好的实例和未优化的实例的数量。从工作负载工厂控制台查看数据库清单中精心设计的状态结果和建议。	架构完善	建议	数据库	Microsoft SQL Server 实例
Microsoft SQL Server/PostgreSQL 服务器部署成功	Microsoft SQL Server 或 PostgreSQL 主机部署成功。更多信息，请参考作业监控。	部署	成功	数据库	FSx for ONTAP，数据库主机
Microsoft SQL Server/PostgreSQL 服务器部署失败	Microsoft SQL Server 或 PostgreSQL 主机部署失败。更多信息，请参考作业监控。	部署	错误	数据库	FSx for ONTAP，数据库主机
复制关系创建失败	SnapMirror复制关系创建失败。欲了解更多信息，请访问 Tracker。	复制	批判的	常规存储	适用于ONTAP的FSx
FSx for ONTAP 创建失败	FSx for ONTAP 文件系统创建过程失败。欲了解更多信息，请访问 Tracker。	FSx for ONTAP 文件系统操作	批判的	常规存储	适用于ONTAP的FSx
自动增加 SSD 容量或 inode 成功	在最近的自动容量管理更新期间，FSx for ONTAP文件系统成功增加了 SSD 容量或卷 inode。欲了解更多信息，请访问 Tracker。	容量管理	成功	常规存储	FSx for ONTAP 文件

事件	说明	通知类型	严重性	工作负载	资源类型
自动增加 SSD 容量或 inode 失败	在最近的自动容量管理更新期间，FSx for ONTAP文件系统未能增加 SSD 容量或卷 inode。欲了解更多信息，请访问 Tracker。	容量管理	批判的	常规存储	FSx for ONTAP 文件系统
检测到 FSx for ONTAP问题	所有 FSx for ONTAP文件系统均已针对架构问题进行了分析。扫描检测到一个或多个问题。有关更多信息，请查看 Workload Factory 控制台中存储仪表板的精心设计的分析。	精心设计的分析	建议	常规存储	FSx for ONTAP 文件系统
FSx for ONTAP 的自动容量管理事件	FSx for ONTAP 文件系统的 SSD 性能层级已达到警告阈值容量/百分比总和。	容量管理	警告	常规存储	FSx for ONTAP 文件系统
FSx for ONTAP 的自动 inode 管理事件	ONTAP卷的 FSx inode 计数达到警告阈值计数/百分比总数。	容量管理	警告	常规存储	FSx for ONTAP 文件系统

配置工作负载工厂通知

使用NetApp控制台或 Workload Factory 控制台配置 Workload Factory 通知。如果您使用NetApp控制台，则可以配置 Workload Factory 以将通知作为NetApp控制台中的警报或 Amazon SNS 主题发送。您可以从NetApp控制台中的 通知设置 配置通知。

开始之前

- 您需要使用 Amazon SNS 控制台或 AWS CLI 配置 Amazon SNS 并创建 Amazon SNS 主题。
- 请注意，Workload Factory 支持 标准 主题类型。这种类型的主题不能确保通知按照收到的顺序发送给订阅者，因此如果您有关键或紧急通知，请考虑这一点。

从**NetApp**控制台配置通知

步骤

1. 登录"NetApp控制台"。
2. 从NetApp控制台菜单中，选择 **Workloads**、**Administration**，然后选择 **Notifications setup**。
3. 在通知设置页面上，执行以下操作：
   a. 可选：选择“启用NetApp控制台通知”以配置 Workload Factory 在NetApp控制台中发送通知。
   b. 选择*启用 SNS 通知*。
   c. 按照说明从 Amazon SNS 控制台配置 Amazon SNS。

      创建主题后，复制主题 ARN 并将其输入到 通知设置 页面上的 **SNS** 主题 **ARN** 字段中。
4. 通过发送测试通知验证配置后，选择*应用*。

结果

Workload Factory 已配置为向您指定的 Amazon SNS 主题发送通知。

从 **Workload Factory** 控制台配置通知

步骤

1. 登录"工作负载工厂控制台"。
2. 从 Workload Factory 控制台菜单中，选择 **Workloads**、**Administration**，然后选择 **Notifications setup**。
3. 选择*启用 SNS 通知*。
4. 按照说明从 Amazon SNS 控制台配置 Amazon SNS。
5. 通过发送测试通知验证配置后，选择*应用*。

结果

Workload Factory 已配置为向您指定的 Amazon SNS 主题发送通知。

订阅 **Amazon SNS** 主题

配置 Workload Factory 向主题发送通知后，请按照 "说明"在 Amazon SNS 文档中订阅该主题，以便您可以接收来自 Workload Factory 的通知。

筛选通知

您可以通过对通知应用过滤器来减少不必要的通知流量，并为特定用户提供特定的通知类型。您可以使用 Amazon SNS 策略来发送 SNS 通知，并使用NetApp控制台中的通知设置来执行此操作。

筛选 **Amazon SNS** 通知

当您订阅 Amazon SNS 主题时，默认情况下您会收到发布到该主题的所有通知。如果您只想接收来自主题的特定通知，则可以使用过滤策略来控制接收哪些通知。过滤策略使 Amazon SNS 仅向订阅者发送符合过滤策略的通知。

您可以按照以下条件筛选 Amazon SNS 通知：

说明	过滤策略字段名称	可能值
资源类型	`resourceType`	• `DB` • `Microsoft SQL Server host` • `PostgreSQL Server host`
工作负载	`workload`	`WLMDB`
优先级	`priority`	• `Success` • `Info` • `Recommendation` • `Warning` • `Error` • `Critical`
通知类型	`notificationType`	• `Deployment` • `Well-architected`

步骤

1. 在 Amazon SNS 控制台中，编辑 SNS 主题的订阅详细信息。
2. 在*订阅过滤策略*区域，选择按*消息属性*进行过滤。
3. 启用*订阅过滤策略*选项。
4. 在 **JSON** 编辑器 框中输入 JSON 过滤策略。

   例如，以下 JSON 过滤策略接受来自 Microsoft SQL Server 资源的与 WLMDB 工作负载相关的通知，优先级为成功或错误，并提供有关 Well-architected 状态的详细信息：

```
{
  "accountId": [
    "account-a"
  ],
  "resourceType": [
    "Microsoft SQL Server host"
  ],
  "workload": [
    "WLMDB"
  ],
  "priority": [
    "Success",
    "Error"
  ],
  "notificationType": [
    "Well-architected"
  ]
}
```

5. 选择“保存更改”。

有关过滤策略的其他示例，请参阅 "Amazon SNS 示例筛选策略"。

有关创建过滤策略的更多信息，请参阅 "Amazon SNS文档"。

NetApp控制台中的过滤通知

您可以使用NetApp控制台通知设置按严重性级别（例如“严重”、“信息”或“警告”）过滤控制台中收到的通知。

有关在控制台中过滤通知的更多信息，请参阅 "NetApp控制台文档"。

使用CodeBox自动执行任务

了解CODEBox自动化

Codebox 是一个基础设施即代码 (IaC) 辅助工具，可帮助开发人员和 DevOps 生成执行NetApp Workload Factory支持的任何操作所需的代码。 Codebox 与 Workload Factory 的权限策略保持一致，并为执行准备工作设定了清晰的路径，同时还提供了一个自动化目录，以便将来快速重用。

CodeBox功能

CodeBox提供了两项关键IAC功能：

- _CodeBox Viewer_显示了由特定作业流操作生成的IAC，它通过匹配图形向导或对话聊天界面中的条目和选择来生成。尽管CodeBox查看器支持颜色编码以方便导航和分析，但它不允许编辑，仅允许将代码复制或保

存到自动化目录中。

- _CodeBox自动化目录_显示所有已保存的IAC作业、便于您轻松参考这些作业以供将来使用。自动化目录作业会另存为模板、并显示在应用于这些作业的资源的上下文中。

此外，在设置 Workload Factory 凭证时，Codebox 会动态显示创建 IAM 策略所需的 AWS 权限。每个 Workload Factory 功能（数据库、AI、FSx for ONTAP等）都提供了相应的权限，并且这些权限是可以自定义的。您只需从 Codebox 复制权限，然后将其粘贴到 AWS 管理控制台中，以便 Workload Factory 拥有管理您的工作负载的正确权限。

支持的代码格式

支持的代码格式包括：

- 工作负载工厂 REST API
- AWS命令行界面
- AWS CloudFormation
- 地形

相关信息

"了解如何使用CodeBox"(英文)

"工作负载工厂 REST API 文档" 。

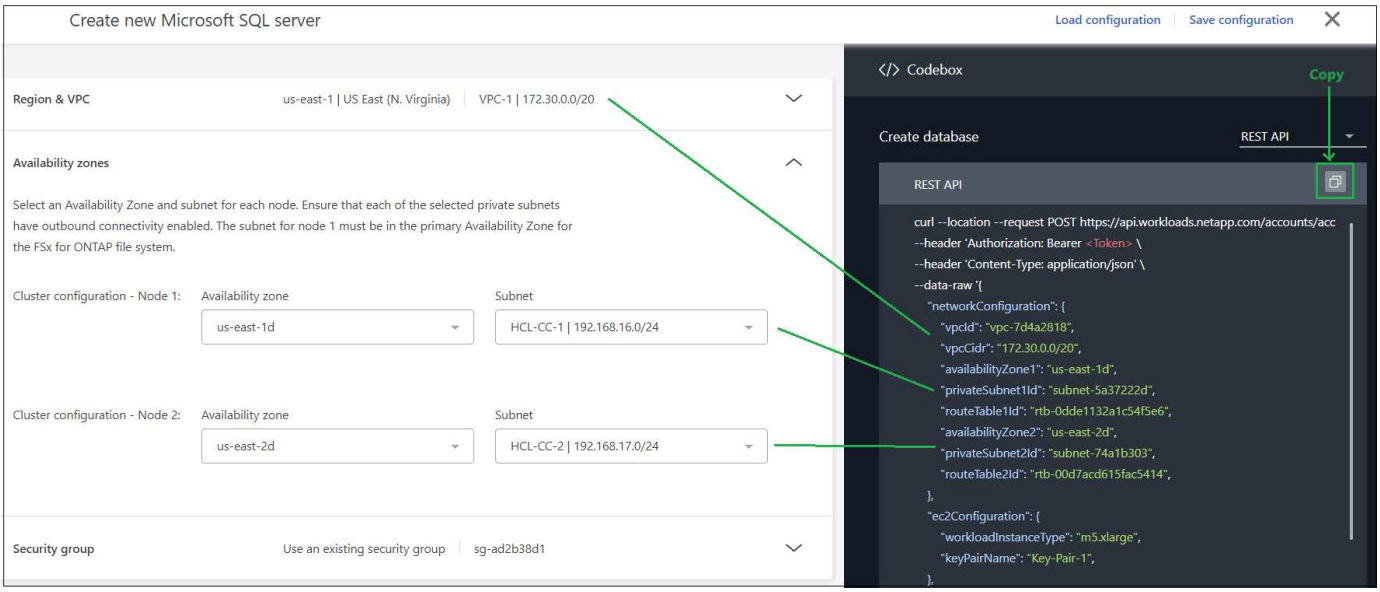
使用 **Codebox** 实现**NetApp Workload Factory** 中的自动化

您可以使用 Codebox 生成执行NetApp Workload Factory 支持的任何操作所需的代码。您可以生成可使用 Workload Factory REST API、AWS CLI 和 AWS CloudFormation 使用和运行的代码。

Codebox 与 Workload Factory 权限策略保持一致，根据 Workload Factory 账户中为每个用户提供的 AWS 权限，在代码中填充相应的数据。该代码可以像模板一样使用，您可以在运行代码之前填写缺失的信息（例如，凭据）或自定义某些数据。

如何使用**CodeBox**

当您在 Workload Factory UI 向导中输入值时，您可以在完成每个字段时看到 Codebox 中的数据更新。完成向导后，在选择页面底部的“创建”按钮之前，选择在 Codebox 中复制以捕获构建配置所需的代码。例如，此创建新 Microsoft SQL Server 的屏幕截图显示了 VPC 和可用区域的向导条目以及 Codebox 中用于 REST API 实现的等效条目。



对于某些代码格式，您还可以选择下载按钮将代码保存在可以带到另一个系统的文件中。如果需要，您可以在下载代码后编辑它，以便使其适应其他 AWS 账户。

使用**CodeBox**中的**CloudFormation**代码

您可以复制从 Codebox 生成的 CloudFormation 代码，然后在您的 AWS 账户中启动 Amazon Web Services CloudFormation 堆栈。 CloudFormation 将执行您在 Workload Factory UI 中定义的操作。

使用 CloudFormation 代码的步骤可能会有所不同，具体取决于您是部署 FSx for ONTAP文件系统、创建帐户凭据还是执行其他 Workload Factory 操作。

请注意、出于安全原因、CloudFormation生成的YAML文件中的代码将在7天后过期。

开始之前

- 您需要具有凭据才能登录到AWS帐户。
- 要使用CloudFormation堆栈、您需要具有以下用户权限：

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:UpdateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeChangeSet",
                "cloudformation:ExecuteChangeSet",
                "cloudformation:ListStacks",
                "cloudformation:ListStackResources",
                "cloudformation:GetTemplate",
                "cloudformation:ValidateTemplate",
                "lambda:InvokeFunction",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:UpdateAssumeRolePolicy",
                "iam:AttachRolePolicy",
                "iam:CreateServiceLinkedRole"
            ],
            "Resource": "*"
        }
    ]
}
```

步骤

1. 使用 Workload Factory 控制台定义要执行的操作后，复制 Codebox 中的代码。
2. 选择*重定向到CloudFormation*、此时将显示重定向到CloudFormation页面。
3. 打开另一个浏览器窗口并登录到AWS管理控制台。
4. 从重定向到CloudFormation页面中选择*继续*。
5. 登录到应运行此代码的AWS帐户。
6. 在快速创建堆栈页面上的"功能"下、选择*我确认AWS CloudFormation可能…*。
7. 选择*创建堆栈*。
8. 从 AWS 或 Workload Factory 监控进度。

使用来自**CodeBox**的**REST API**代码

您可以使用 Codebox 生成的 Workload Factory REST API 来部署和管理 FSx for ONTAP文件系统和其他 AWS 资源。

您可以从任何支持CURL且具有Internet连接的主机运行API。

请注意、身份验证令牌在CodeBox中处于隐藏状态、但在复制和粘贴API调用时会填充这些令牌。

步骤

1. 使用 Workload Factory 控制台定义要执行的操作后，复制 Codebox 中的 API 代码。
2. 粘贴代码并在主机系统上运行。

使用**CodeBox**中的**AWS**命令行界面代码

您可以使用从CodeBox生成的Amazon Web Services命令行界面来部署和管理适用于ONTAP文件系统和其他AWS资源的FSx。

步骤

1. 使用 Workload Factory 控制台定义要执行的操作后，将 AWS CLI 复制到 Codebox 中。
2. 打开另一个浏览器窗口并登录到AWS管理控制台。
3. 粘贴代码并运行。

使用**CodeBox**中的**Terraform**

您可以使用Terraform部署和管理适用于ONTAP文件系统和其他AWS资源的FSx。

开始之前

- 您需要安装Terraform的系统(Windows/Mac/Linux)。
- 您需要具有凭据才能登录到AWS帐户。

步骤

1. 使用 Workload Factory 控制台定义要执行的操作后，从 Codebox 下载 Terraform 代码。
2. 将下载的脚本归档文件复制到安装了Terraform的系统。
3. 解压缩zip文件、然后按照README.MD文件中的步骤进行操作。

在NetApp Workload Factory 中使用 CloudShell

打开 CloudShell 以从NetApp Workload Factory 控制台中的任何位置执行 AWS 或ONTAP CLI 命令。

关于此任务

CloudShell 允许您在 Workload Factory 控制台内类似 shell 的环境中执行 AWS CLI 命令或ONTAP CLI 命令。它在浏览器中模拟终端会话，通过 Workload Factory 的后端提供终端功能和代理消息。它允许您使用您在NetApp帐户中提供的 AWS 凭证和ONTAP凭证。

CloudShell功能包括：

- 多个CloudShell会话：一次部署多个CloudShell会话以并行发出多个命令序列、
- 多个视图：拆分CloudShell选项卡会话、以便您可以同时水平或垂直查看两个或多个选项卡
- 会话重命名：根据需要重命名会话
- 上次会话内容持久性：如果您错误地关闭了上次会话、请重新打开它
- 设置首选项：更改字体大小和输出类型
- AI生成的ONTAP命令行界面命令错误响应
- 自动完成支持：开始键入命令，然后使用*Tab*键查看可用选项

CloudShell命令

在CloudShell图形用户界面中、您可以输入 `help`以查看可用的`CloudShell`命令。发出命令后 `help`、将显示以下参考信息。

说明

NetApp CloudShell 是NetApp Workload Factory 内置的 GUI 界面，可让您在类似 shell 的环境中执行 AWS CLI 命令或ONTAP CLI 命令。它在浏览器中模拟终端会话，通过 Workload Factory 中的后端提供终端功能和代理消息。它使您能够使用您在NetApp帐户中提供的 AWS 凭证和ONTAP凭证。

可用命令

- `clear`
- `help`
- `[--fsx <fsxId>] <ontap-command> [parameters]`
- `aws <aws-command> <aws-sub-command> [parameters]`

环境

每个终端会话都在特定环境下运行：凭据、区域以及可选的FSx for ONTAP文件系统。

+ 所有 AWS 命令都在提供的上下文中执行。仅当提供的凭证在指定区域具有权限时，AWS 命令才会成功。

+ 您可以使用可选的ONTAP命令指定 `fsxId`。如果您提供 `fsxId`使用单独的ONTAP命令，则此 ID 将覆盖上下文中的 ID。如果终端会话没有 FSx for ONTAP文件系统 ID 上下文，则必须提供 `fsxId`每个ONTAP命令。

+ 要更新不同的上下文细节，请执行以下操作：* 要更改凭据：“使用凭据 <credentialId>”* 要更改区域：“使用区域 <regionCode>”* 要更改 FSx for ONTAP文件系统：“使用 fsx <fileSystemId>”

显示项目

- 要显示可用凭据、请执行以下操作："显示凭据"
- 要显示可用区域："显示区域"
- 要显示命令历史记录："show histy"

变量

以下是设置和使用变量的示例。如果变量值包含空格、则应将其设置在引号内。

+ * 设置变量：$<variable> = <value> * 使用变量：$<variable> * 设置变量的示例：$svm1 = svm123 * 使用变量的示例：--fsx FileSystem-1 volumes show --vserver $svm1 * 设置具有字符串值的变量的示例 $comment1 = "带有空格的注释"

运算符

不支持管道、后台执行 `&`和重定向 `>`等`Shell`运算符 `|`。如果包含这些运算符、则命令执行将失败。

开始之前

CloudShell可在您的AWS凭据环境中运行。要使用CloudShell、您必须至少提供一个AWS凭据。

您可以使用CloudShell执行任何AWS或ONTAP命令行界面命令。但是，如果要在FSx for ONTAP文件系统的环境中工作，请确保发出以下命令： `using fsx <file-system-name>`。

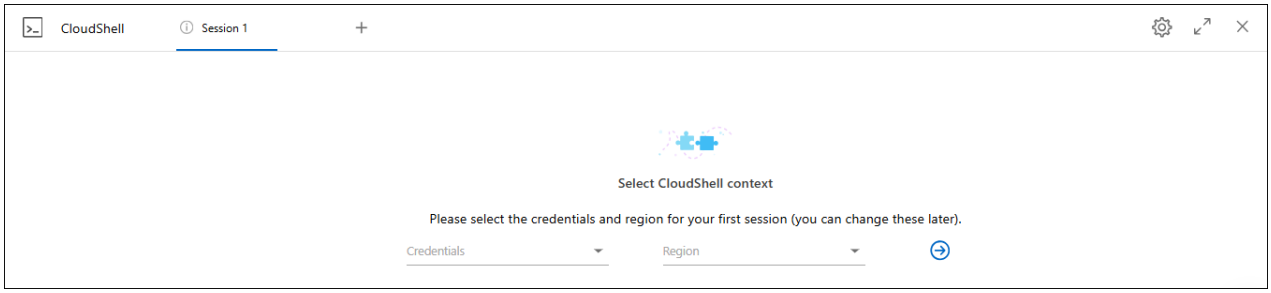
部署CloudShell

您可以从NetApp Workload Factory 控制台中的任何位置部署 CloudShell。您还可以从NetApp控制台部署CloudShell。

从 **Workload Factory** 控制台部署

步骤

1. 登录 "工作负载工厂控制台"。
2. 从菜单中选择“管理”，然后选择“**CloudShell**”。
3. 在CloudShell窗口中、为CloudShell会话选择凭据和区域、然后选择箭头以继续。



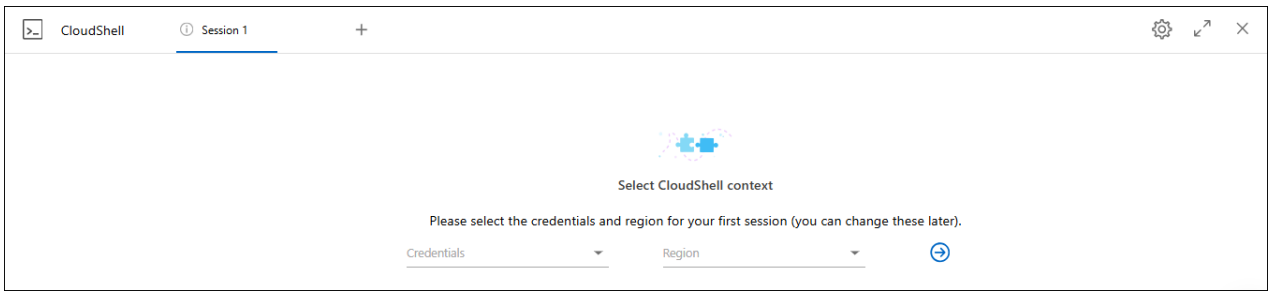
4. 输入 `help`以查看可用CloudShell命令命令和说明、或者参阅以下命令行界面参考文档以了解可用命令：
   - "AWS CLI参考"：对于与FSx for ONTAP相关的命令，请选择*FSX*。
   - "ONTAP命令行界面参考"
5. 在CloudShell会话中发出命令。

   如果在发出ONTAP命令行界面命令后发生错误、请选择灯泡图标以获取由AI生成的简短错误响应、并提供故障说明、故障原因和详细解决方案。有关详细信息，请选择*阅读更多*。

从**NetApp**控制台部署

步骤

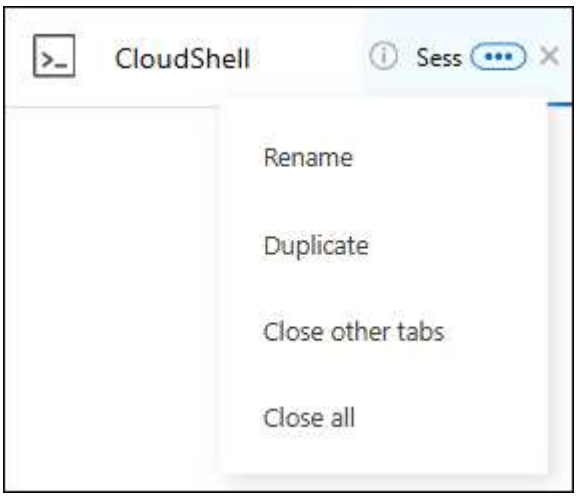
1. 登录"NetApp控制台"。
2. 从菜单中选择“工作负载”，然后选择“管理”。
3. 从管理菜单中，选择 **CloudShell**。
4. 在CloudShell窗口中、为CloudShell会话选择凭据和区域、然后选择箭头以继续。



5. 输入 `help`以查看可用的CloudShell命令和说明、或者参阅以下命令行界面参考文档以了解可用命令：
   - "AWS CLI参考"：对于与FSx for ONTAP相关的命令，请选择*FSX*。
   - "ONTAP命令行界面参考"
6. 在CloudShell会话中发出命令。

如果在发出ONTAP命令行界面命令后发生错误、请选择灯泡图标以获取由AI生成的简短错误响应、并提供故障说明、故障原因和详细解决方案。有关详细信息，请选择*阅读更多*。

通过选择打开的 CloudShell 会话选项卡的操作菜单，可以完成此屏幕截图中显示的 CloudShell 任务。以下是每个任务的说明。



重命名CloudShell会话选项卡

您可以重命名CloudShell会话选项卡以帮助您识别会话。

步骤

1. 选择 CloudShell 会话选项卡的操作菜单。
2. 选择 * 重命名 * 。
3. 为会话选项卡输入新名称、然后单击选项卡名称外部以设置新名称。

结果

新名称将显示在CloudShell会话选项卡中。

重复的CloudShell会话选项卡

您可以复制CloudShell会话选项卡、以创建具有相同名称、凭据和区域的新会话。原始选项卡中的代码不会在复制选项卡中复制。

步骤

1. 选择 CloudShell 会话选项卡的操作菜单。
2. 选择*复制*。

结果

此时将显示与原始选项卡同名的新选项卡。

关闭CloudShell会话选项卡

您可以一次关闭一个CloudShell选项卡、关闭其他未处理的选项卡或一次性关闭所有选项卡。

步骤

1. 选择 CloudShell 会话选项卡的操作菜单。
2. 选择以下选项之一：
   - 在CloudShell选项卡窗口中选择"X"、一次关闭一个选项卡。
   - 选择*关闭其他选项卡*以关闭除您正在处理的选项卡之外所有其他已打开的选项卡。
   - 选择*关闭所有选项卡*关闭所有选项卡。

结果

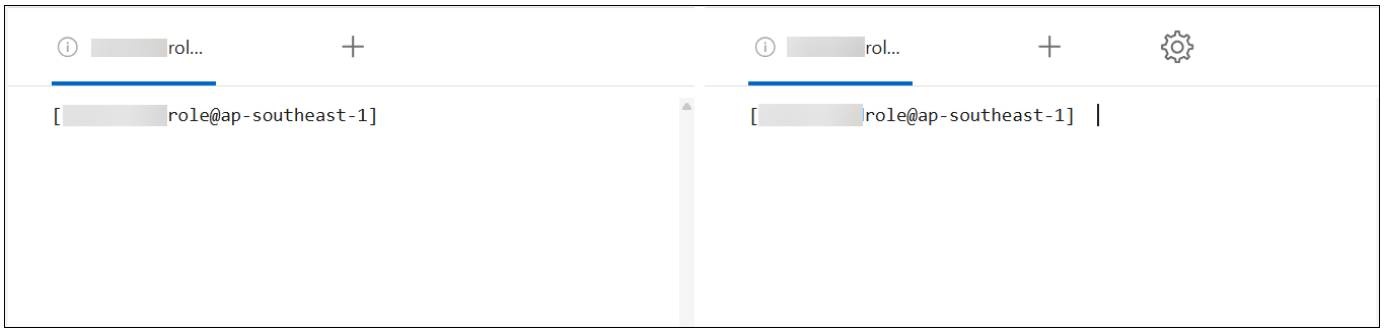
此时将关闭选定的CloudShell会话选项卡。

拆分CloudShell会话选项卡

您可以拆分CloudShell会话选项卡以同时查看两个或更多选项卡。

步骤

将CloudShell会话选项卡拖放到CloudShell窗口的顶部、底部、左侧或右侧以拆分视图。



更新CloudShell会话的设置

您可以更新CloudShell会话的字体和输出类型设置。

步骤

1. 部署CloudShell会话。
2. 在CloudShell选项卡中、选择设置图标。

   此时将显示设置对话框。

3. 根据需要更新字体大小和输出类型。

   丰富的输出适用于JSON对象和表格格式。所有其他输出均显示为纯文本。

4. 选择 * 应用 * 。

结果

此时将更新CloudShell设置。

从NetApp Workload Factory 中删除凭据

如果您不再需要一组凭证，您可以从 Workload Factory 中删除它们。您只能删除与 FSx for ONTAP文件系统无关的凭据。

步骤

1. 使用其中一个登录"控制台体验"。
2. 从菜单中选择“管理”，然后选择“凭据”。
3. 在 **Credentials** 页面上，执行以下操作：
   - 在 Workload Factory 控制台中，选择一组凭据的操作菜单，然后选择*删除*。选择*删除*进行确认。
   - 在NetApp控制台中，选择一组凭据的操作菜单，然后选择*删除*。选择*删除*进行确认。

知识和支持

注册以获得支持

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

注册支持并不能使NetApp获得云提供商文件服务的支持。有关云提供商文件服务、其基础设施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”。

"适用于 ONTAP 的 Amazon FSX"

支持注册概述

注册您的帐户 ID 支持订阅（位于NetApp控制台中的“支持资源”页面上的 20 位 960xxxxxxxxx 序列号）作为您的单一支持订阅 ID。每个NetApp帐户级支持订阅都必须注册。

注册后即可实现开立支持票和自动生成案例等功能。通过将NetApp支持站点 (NSS) 帐户添加到NetApp控制台即可完成注册，如下所述。

注册您的帐户以获得**NetApp**支持

要注册支持并激活支持权利，您帐户中的一名用户必须将NetApp支持站点帐户与其NetApp控制台登录名关联。如何注册NetApp支持取决于您是否已经拥有NetApp支持站点 (NSS) 帐户。

具有**NSS**帐户的现有客户

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

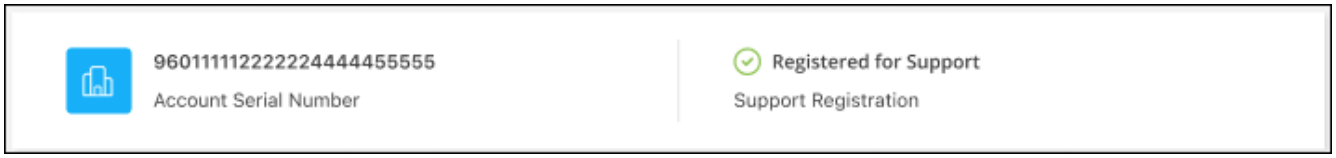
步骤

1. 在 Workload Factory 控制台的右上角，选择 帮助 > 支持。

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

2. 从NetApp控制台菜单中，选择 管理，然后选择 凭据。
3. 选择*用户凭据*。
4. 选择*添加NSS凭证*，然后按照NetApp 支持站点(NSS)鉴定提示进行操作。
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控制台用户尚未将NetApp支持站点帐户与其NetApp控制台登录名关联，则他们将看不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。只要账户中有一位用户遵循了这些步骤，那么您的账户就注册成功了。

现有客户、但无**NSS**帐户

如果您是现有NetApp客户，拥有现有许可证和序列号但没有 NSS 帐户，则需要创建一个 NSS 帐户并将其与您的NetApp控制台登录关联。

步骤

1. 完成以创建NetApp支持站点帐户 "NetApp 支持站点 用户注册表"
   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)。这将加快账户处理速度。
2. 完成以下步骤，将您的新 NSS 帐户与您的NetApp控制台登录关联具有NSS帐户的现有客户。

NetApp的新品牌

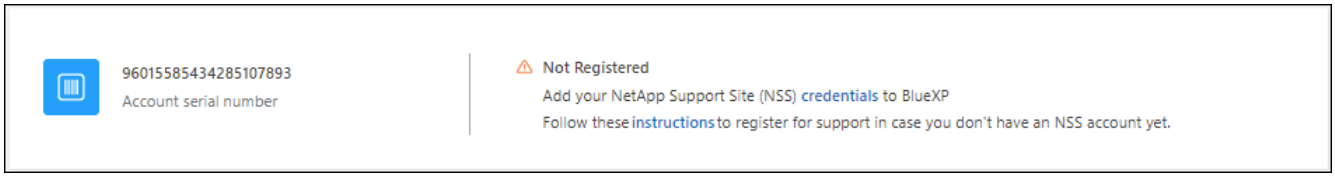
如果您是NetApp的新客户、并且没有NSS帐户、请按照以下每个步骤进行操作。

步骤

1. 在 Workload Factory 控制台的右上角，选择 帮助 > 支持。

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

2. 从支持资源页面中找到您的帐户ID序列号。



3. 导航到 "NetApp的支持注册站点" 并选择*我不是NetApp的注册客户*。
4. 填写必填字段(带有红色星号的字段)。
5. 在*产品线*字段中、选择*云管理器*、然后选择适用的计费提供商。
6. 复制上述第2步中的帐户序列号、完成安全检查、然后确认您已阅读NetApp的全球数据隐私政策。

   系统会立即向提供的邮箱发送一封电子邮件、以完成此安全事务。如果验证电子邮件未在几分钟内收到、请务必检查您的垃圾邮件文件夹。

7. 在电子邮件中确认操作。

   确认将向NetApp提交您的请求、并建议您创建NetApp 支持站点 帐户。

8. 完成以创建NetApp支持站点帐户 "NetApp 支持站点 用户注册表"
   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)。这样可以加快帐户处理速度。

完成后

在此过程中、NetApp应与您联系。这是针对新用户的一次性入职练习。

拥有NetApp支持站点帐户后，请按照以下步骤将该帐户与您的NetApp控制台登录关联具有NSS帐户的现有客户。

获取帮助

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。您的支持注册包含通过网络工单获取的远程技术支持。

获取**FSx for ONTAP**支持

有关 FSx for ONTAP、其基础架构或任何使用该服务的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”。

"适用于 ONTAP 的 Amazon FSX"

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

使用自助支持选项

这些选项每周 7 天，每天 24 小时免费提供：

- 文档

  您当前正在查看的 Workload Factory 文档。

- "知识库"

  搜索 Workload Factory 知识库以查找有助于解决问题的文章。

- "社区"

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

向**NetApp**支持部门创建案例

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

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支持站点凭据与您的 Workload Factory 登录名关联。"了解如何注册获取支持" 。

步骤

1. 在 Workload Factory 控制台的右上角，选择 帮助 > 支持。

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

2. 在*资源*页面上、在技术支持下选择一个可用选项：

   a. 如果您想通过电话与某人通话，请选择*呼叫我们*。系统会将您定向到netapp.com上的一个页面、其中列出了您可以拨打的电话号码。

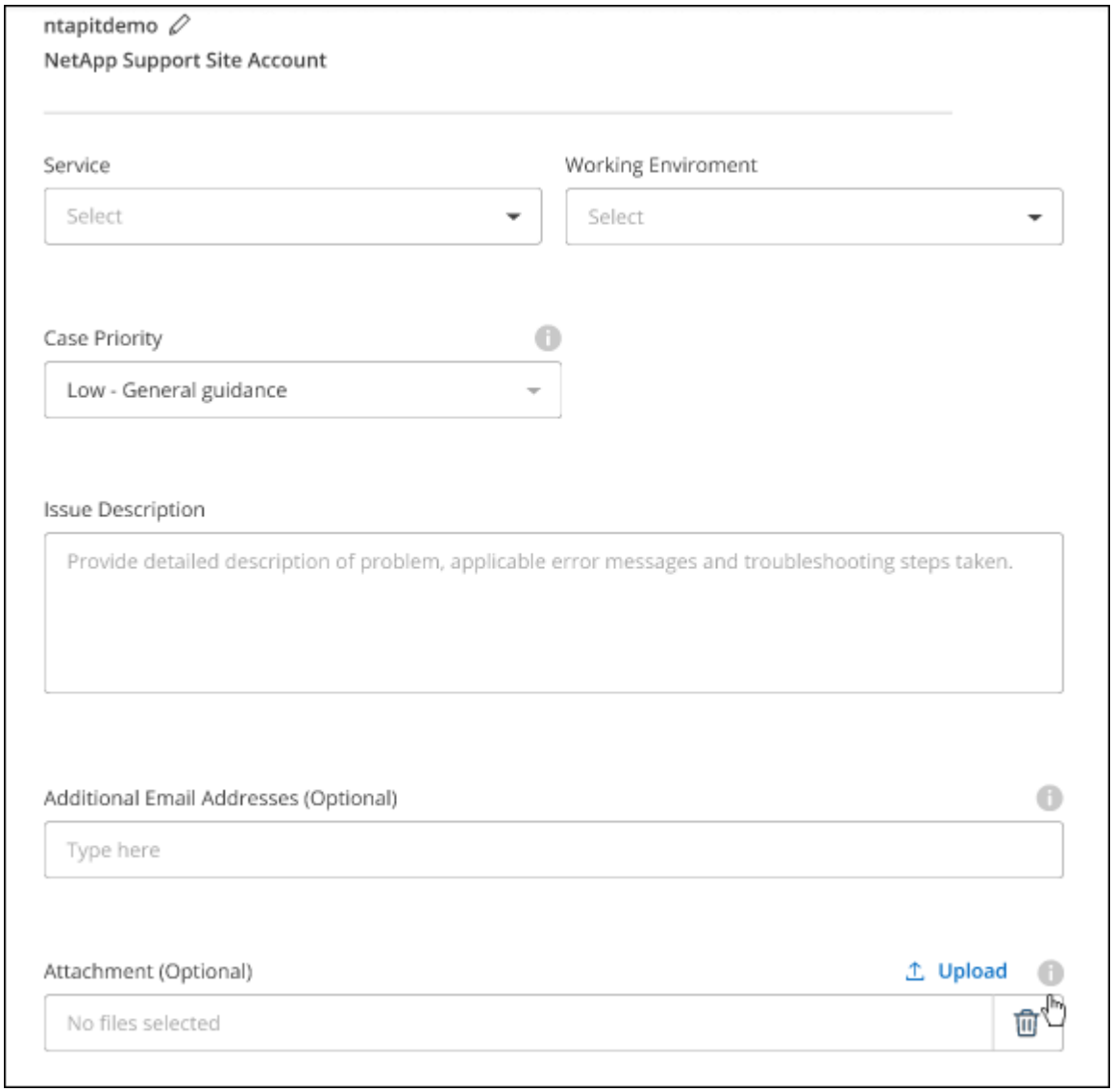
   b. 选择*创建案例*向NetApp支持专家开立TT：

      - 服务：选择*工作负载工厂*。
      - 案例优先级：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 *：提供问题的详细问题描述 、包括任何适用的错误消息或您执行的故障排除步骤。
      - 其他电子邮件地址：如果您希望其他人了解此问题描述 、请输入其他电子邮件地址。
      - 附件(可选)：一次最多上传五个附件。

        每个文件的附件数限制为25 MB。支持以下文件扩展名：txt、log、pdf、jp6/jpeu、rtf、 doc/docx 、xls/xlsx和csv。



完成后

此时将显示一个弹出窗口、其中包含您的支持案例编号。NetApp支持专家将审核您的案例、并尽快与您联系。

要查看支持案例的历史记录，您可以选择*设置>时间线*并查找名为“创建支持案例”的操作。最右侧的按钮可用于展开操作以查看详细信息。

尝试创建案例时、您可能会遇到以下错误消息：

"您无权针对选定服务创建案例"

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

- 使用产品内聊天功能
- 请通过提交非技术案例 https://mysupport.netapp.com/site/help

管理支持案例(预览)

您可以直接从NetApp控制台查看和管理活动和已解决的支持案例。您可以管理与您的 NSS 帐户和公司相关的案例。

案例管理以预览形式提供。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。请通过产品内聊天向我们发送反馈。

请注意以下事项：

- 页面顶部的案例管理信息板提供了两个视图：
  - 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。
  - 右侧视图显示了过去3个月内根据用户NSS帐户在公司级别开立的案例总数。

  此表中的结果反映了与选定视图相关的案例。
- 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。

  有关更多详细信息、请查看以下步骤。
- 在每个案例级别、我们可以更新案例备注或关闭尚未处于"已关闭"或"待关闭"状态的案例。

步骤

1. 在 Workload Factory 控制台的右上角，选择 帮助 > 支持。

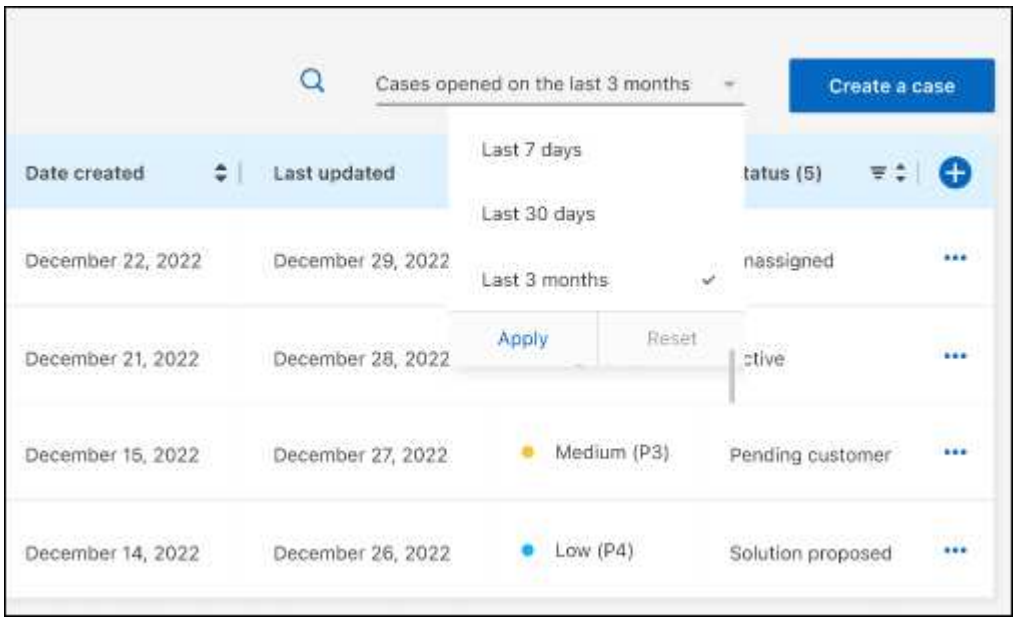
   选择此选项将打开NetApp控制台的新浏览器选项卡并加载支持仪表板。

2. 选择*案例管理*，如果出现提示，请将您的 NSS 帐户添加到NetApp控制台。

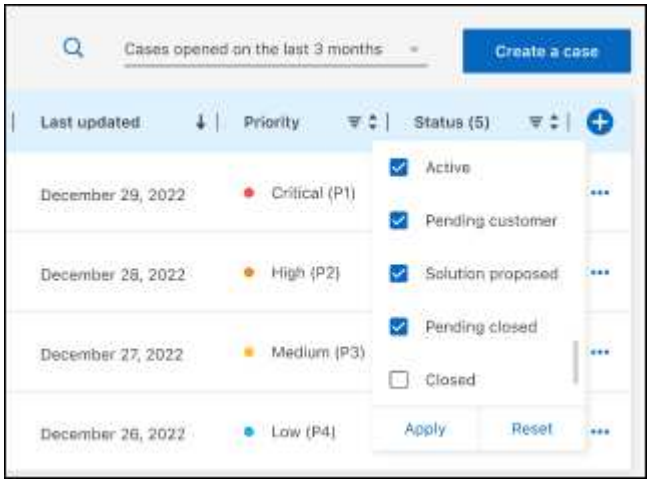
   案例管理*页面显示与您的**NetApp**控制台用户帐户关联的 **NSS** 帐户相关的未结案例。这与出现在 ***NSS** 管理 页面顶部的 NSS 帐户相同。

3. 也可以修改表中显示的信息：
   - 在“组织案例”下，选择“查看”以查看与贵公司关联的所有案例。

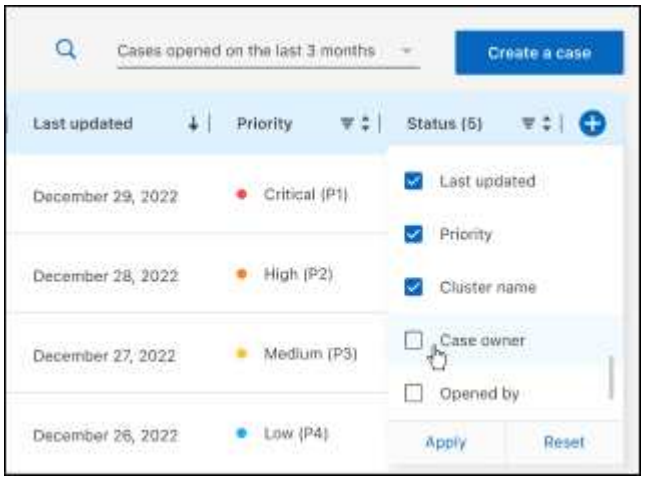
- 通过选择确切的日期范围或选择其他时间范围来修改日期范围。



- 筛选列的内容。



- 通过选择并选择要显示的列来更改表中 显示的列。

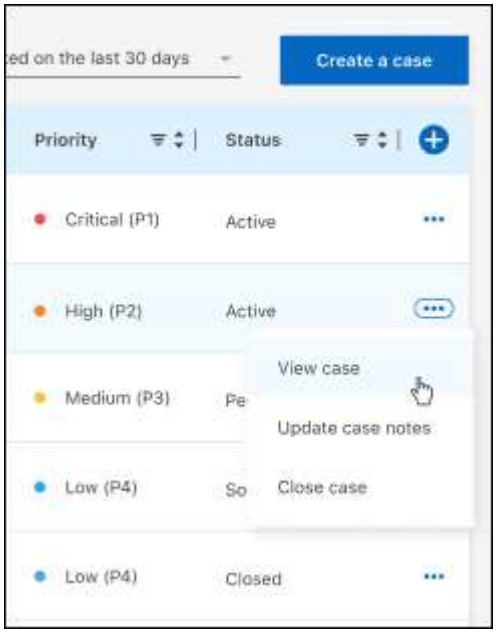


4. 通过选择并选择一个可用选项来管理现有案例 ••• ：

   - 查看案例：查看有关特定案例的完整详细信息。
   - 更新案例注释：提供有关您的问题的更多详细信息、或者选择*上传文件*最多附加五个文件。

     每个文件的附件数限制为25 MB。支持以下文件扩展名：txt、log、pdf、jp6/jpeu、rtf、 doc/docx、xls/xlsx和csv。

   - 关闭案例：提供关闭案例的详细原因，然后选择*关闭案例*。



NetApp Workload Factory 的法律声明

法律声明提供对版权声明、商标、专利等的访问。

版权

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

商标

NetApp 、 NetApp 徽标和 NetApp 商标页面上列出的标记是 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

有关 NetApp 拥有的专利的最新列表，请访问：

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

隐私政策

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

开放源代码

通知文件提供有关 NetApp 软件中使用的第三方版权和许可证的信息。

"NetApp工作负载工厂"