开始使用
Setup and administration

NetApp
February 02, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/workload-setup-admin/workload-factory-overview.html on February 02, 2026. Always check docs.netapp.com for the latest.

目录

开始使用 . . . 1
了解基础知识 . . . 1
了解NetApp Workload Factory . . . 1
控制台体验 . . . 5
NetApp Workload Factory 的权限 . . . 5
NetApp Workload Factory 快速入门 . . . 50
注册NetApp Workload Factory . . . 51
注册 Workload Factory . . . 51
邀请其他人加入 Workload Factory 帐户 . . . 53
将 AWS 凭证添加到 Workload Factory . . . 53
概述 . . . 53
AWS凭据 . . . 54
手动向帐户添加凭据 . . . 54
使用CloudFormation向帐户添加凭据 . . . 57
使用NetApp Workload Factory 优化工作负载 . . . 59

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。

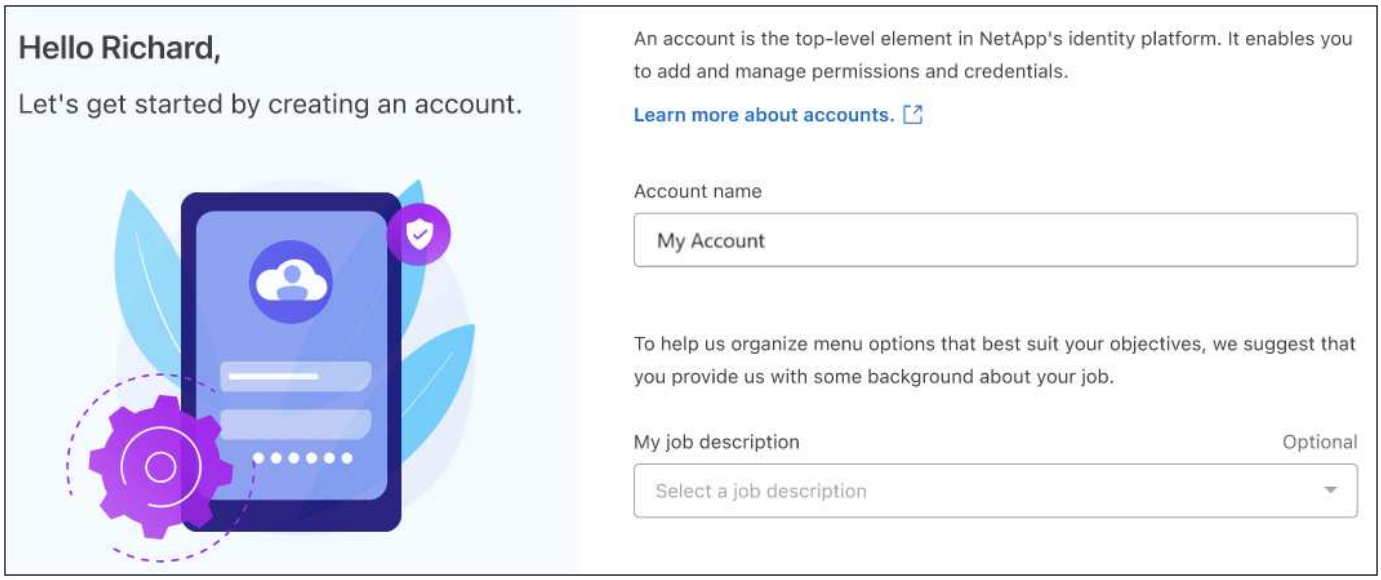
软件即服务

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：

数据库工作负载的 **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：

VMware工作负载的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：

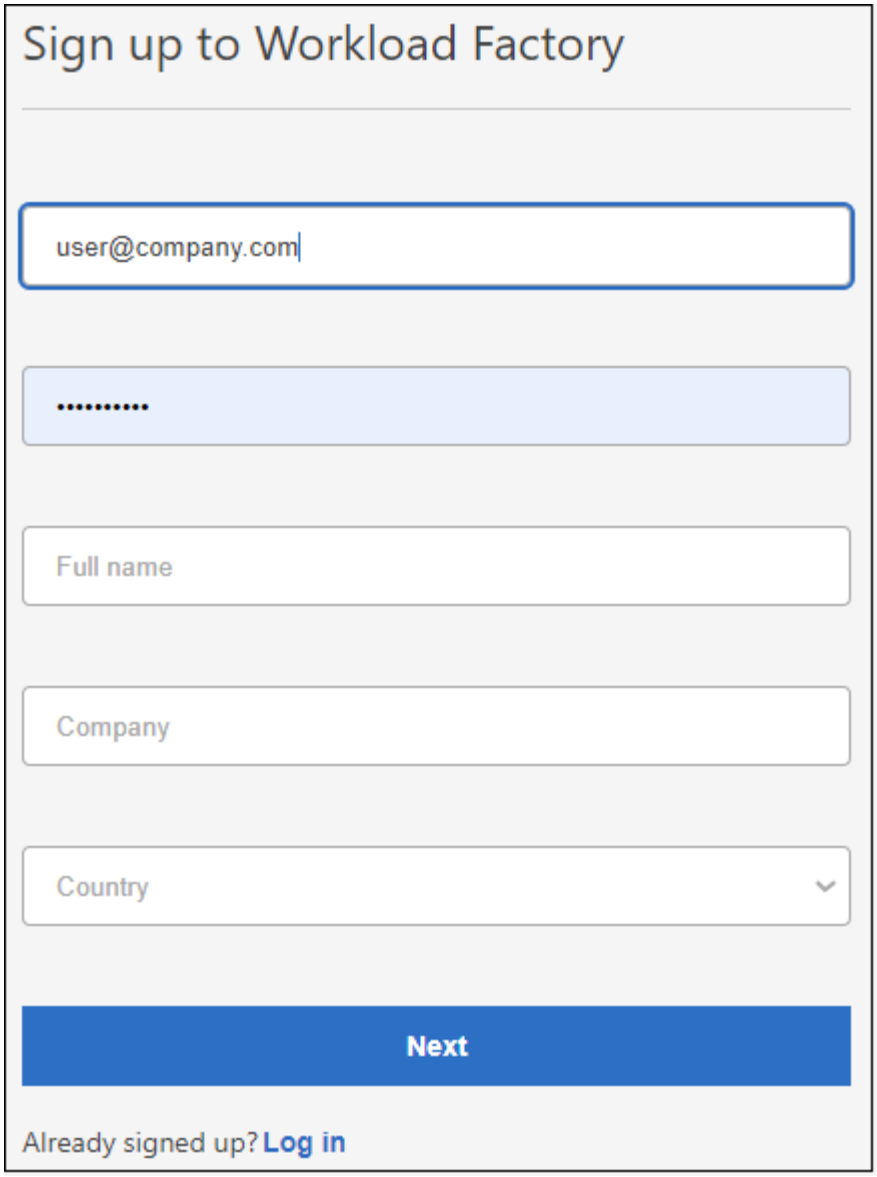
- 您的现有NetApp 支持站点 (NSS)凭据
- 通过指定您的电子邮件地址和密码来登录NetApp云

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*。

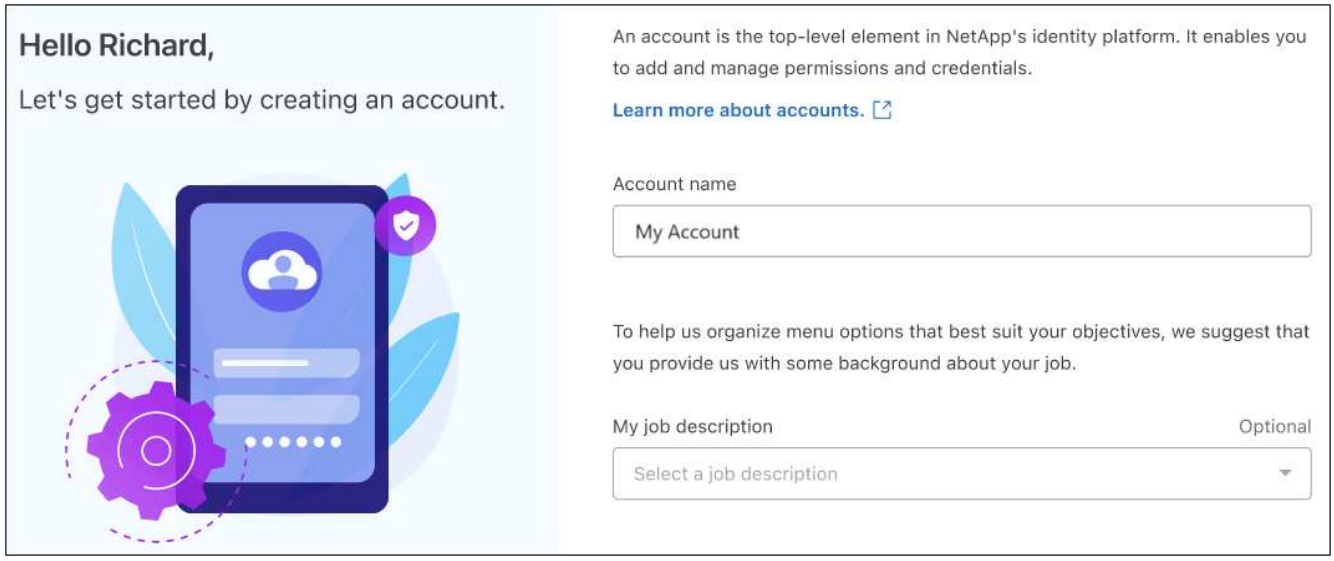
   请注意、注册表单中仅允许使用英文字符。

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：

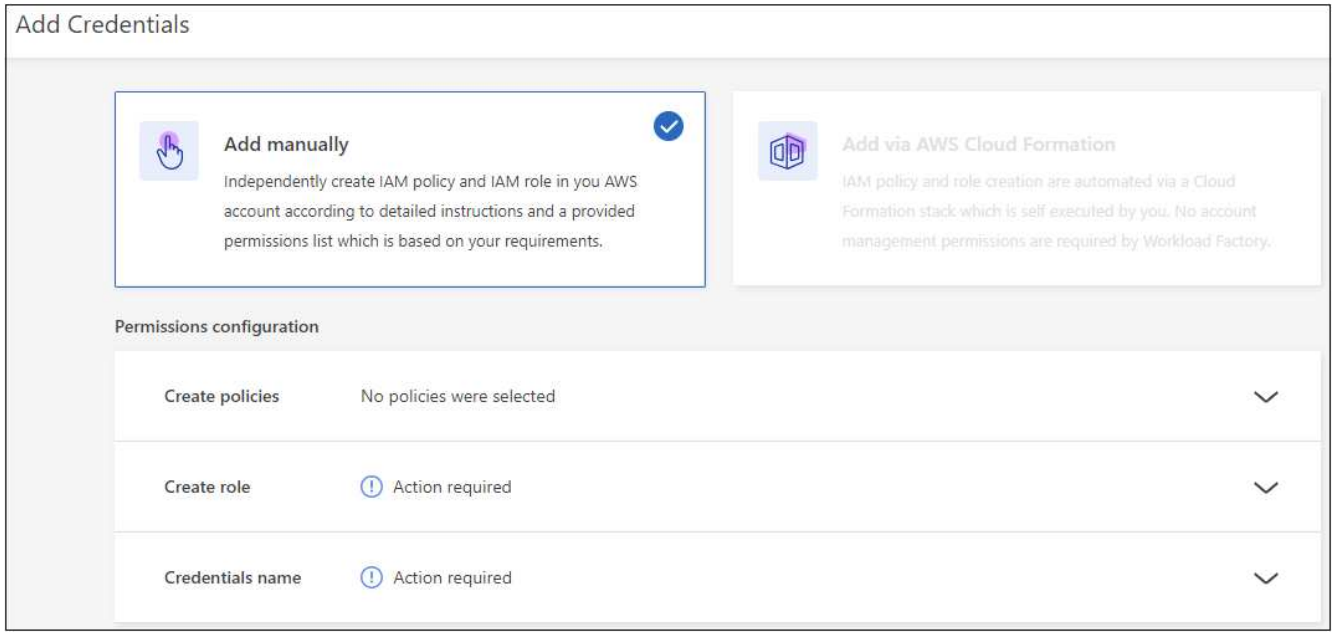
- 选择要使用的服务和权限级别、然后从AWS管理控制台创建IAM策略。
- 从AWS管理控制台创建IAM角色。
- 从 Workload Factory 中输入名称并添加凭据。

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

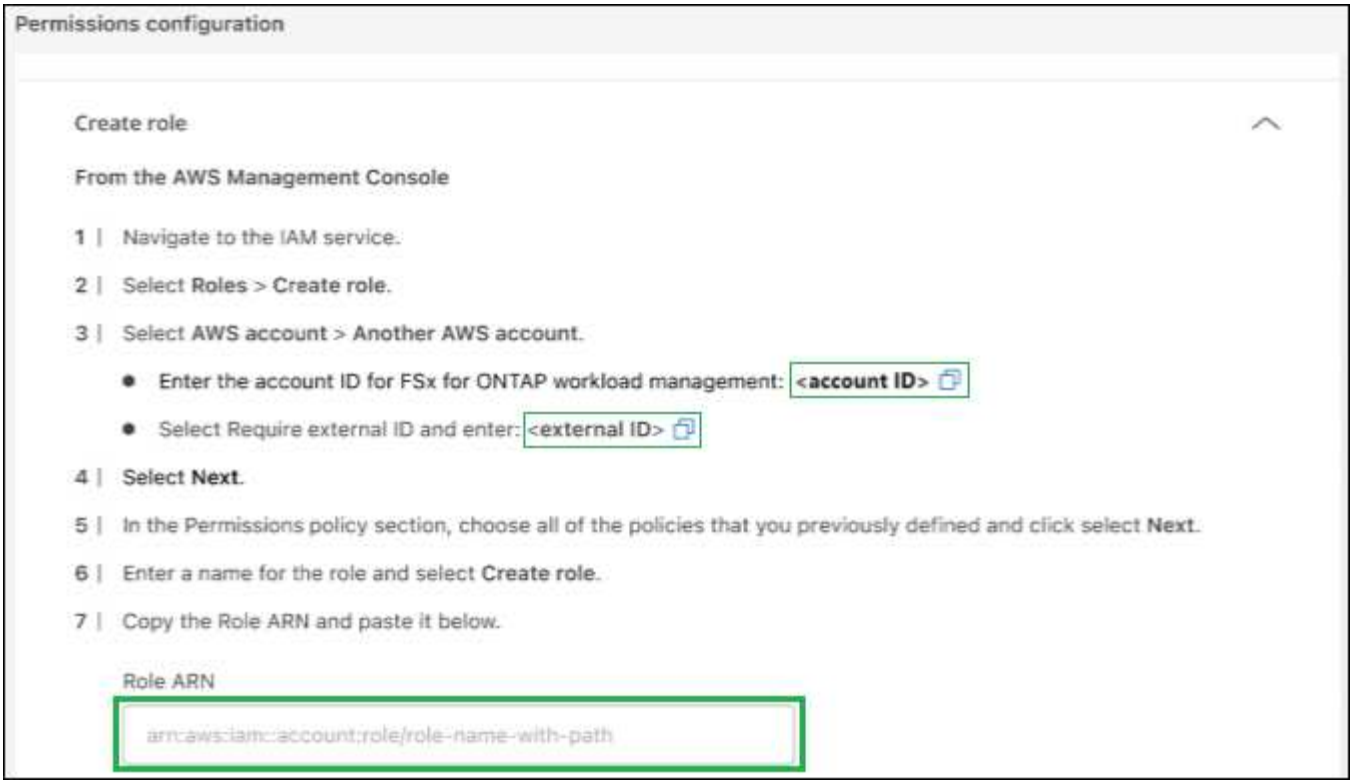
1. 在*Create Policies*部分中，启用要包含在这些凭据中的每个工作负载功能。

   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

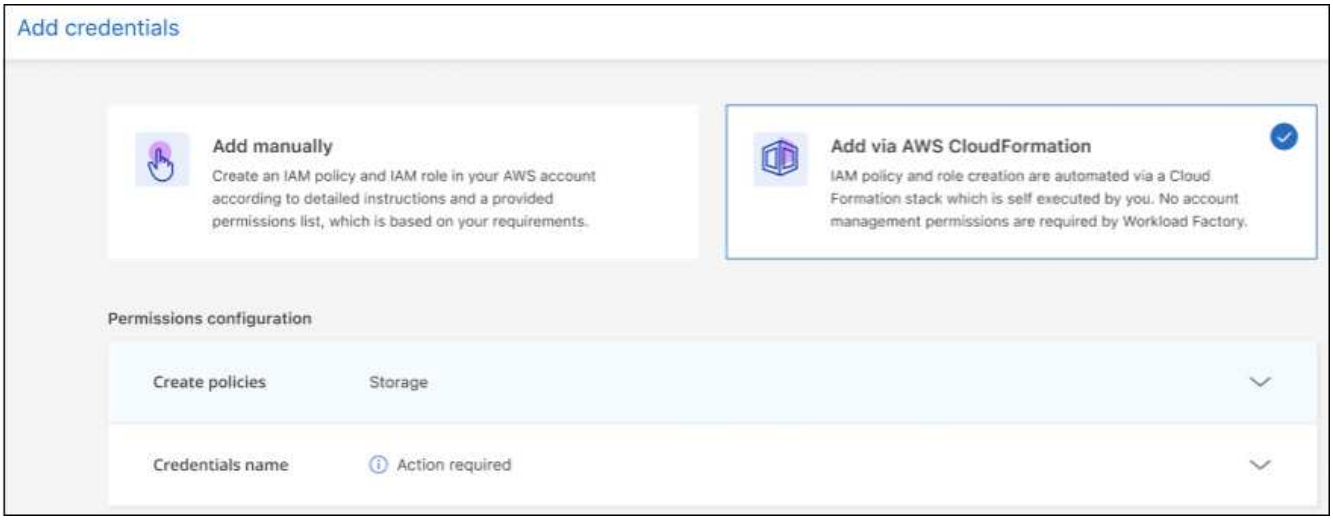
- 您需要具有凭据才能登录到AWS帐户。
- 使用CloudFormation堆栈添加凭据时、您需要在AWS帐户中具有以下权限：

```
{
  "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”。

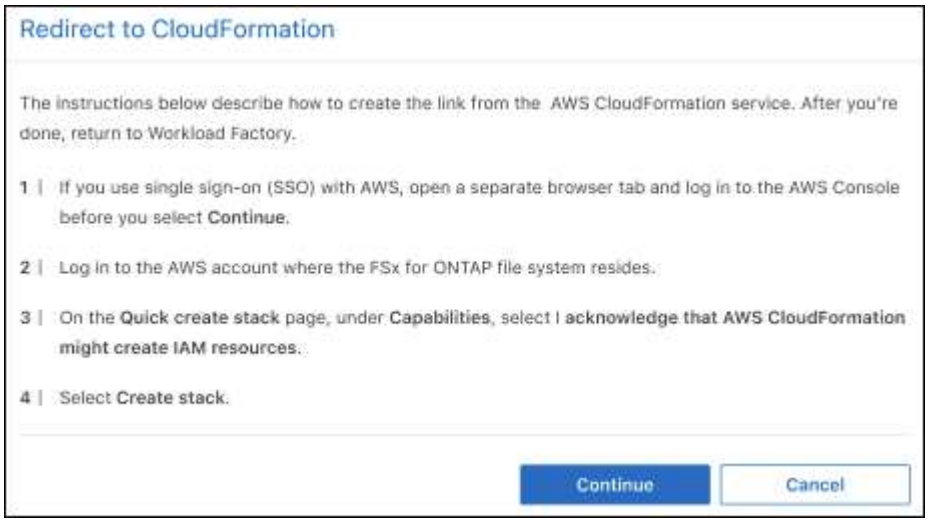
3. 在“凭据”页面上，选择*添加凭据*。
4. 选择*通过AWS CloudFormation*添加。



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。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。