Aprenda o básico

Setup and administration

NetApp
February 02, 2026

Índice

Aprenda o básico

Saiba mais sobre o NetApp Workload Factory

O NetApp Workload Factory é uma poderosa plataforma de gerenciamento de ciclo de vida projetada para ajudar você a otimizar suas cargas de trabalho usando o Amazon FSx for NetApp ONTAP . As cargas de trabalho que podem ser simplificadas usando o Workload Factory e o FSx para ONTAP incluem bancos de dados, migrações do VMware para o VMware Cloud na AWS, chatbots de IA e muito mais.

Uma *carga de trabalho* engloba uma combinação de recursos, código e serviços ou aplicações, concebida para atingir um objetivo de negócio. Isso pode ser qualquer coisa, desde um aplicativo voltado para o cliente até um processo de back-end. As cargas de trabalho podem envolver um subconjunto de recursos dentro de uma única conta da AWS ou abranger várias contas.

O Amazon FSx for NetApp ONTAP fornece volumes de armazenamento NFS, SMB/CIFS e iSCSI nativos da AWS totalmente gerenciados para aplicativos de missão crítica, bancos de dados, contêineres, datastores do VMware Cloud e arquivos de usuários. Você pode gerenciar o FSx para ONTAP por meio do Workload Factory e usando ferramentas de gerenciamento nativas da AWS.

Caraterísticas

A plataforma Workload Factory oferece os seguintes recursos principais.

Armazenamento flexível e de baixo custo

Descubra, implante e gerencie os sistemas de arquivos do Amazon FSX for NetApp ONTAP na nuvem. O FSX para ONTAP oferece todos os recursos do ONTAP para um serviço gerenciado nativo da AWS que oferece uma experiência consistente de nuvem híbrida.

Migre ambientes vSphere locais para o VMware Cloud na AWS

O consultor de migração do VMware Cloud on AWS permite analisar as configurações atuais da máquina virtual em ambientes vSphere locais, gerar um plano para implantar layouts de VM recomendados no VMware Cloud on AWS e usar sistemas de arquivos personalizados do Amazon FSX for NetApp ONTAP como datastores externos.

Gerenciamento do ciclo de vida do banco de dados

Descubra cargas de trabalho de banco de dados e analise a economia de custos com o Amazon FSX for NetApp ONTAP; aproveite os benefícios de armazenamento e aplicação ao migrar bancos de dados do servidor SQL para o FSX for ONTAP; implante servidores SQL, bancos de dados e clones de bancos de dados que implementam as melhores práticas do fornecedor; use um copiloto de infraestrutura como código para automatizar operações; e monitore e otimize continuamente as propriedades do servidor SQL para melhorar o desempenho, disponibilidade, proteção e economia.

Desenvolvimento de chatbot de IA

Aproveite seus sistemas de arquivos FSX for ONTAP para armazenar suas organizações fontes de chatbot e os bancos de dados do AI Engine. Isso permite que você incorpore os dados não estruturados da sua organização em um aplicativo de chatbot corporativo.

Calculadoras de poupança para poupar custos

Analise suas implantações atuais que usam o armazenamento Amazon Elastic Block Store (EBS) ou Elastic File System (EFS), ou o Amazon FSX for Windows File Server, para ver quanto dinheiro você pode

economizar ao migrar para o Amazon FSX for NetApp ONTAP. Você também pode usar a calculadora para executar um cenário "e se" para uma implantação futura que você está planejando.

Contas de serviço para promover a automação

Use contas de serviço para automatizar as operações do NetApp Workload Factory de forma segura e confiável. As contas de serviço fornecem automação confiável e duradoura, sem quaisquer restrições de gerenciamento de usuários e são mais seguras porque fornecem apenas acesso à API.

Assistente de IA Ask Me

Faça perguntas ao assistente de IA sobre como gerenciar e operar o FSx para sistemas de arquivos ONTAP . Usando o Model Context Protocol (MCP), o Ask Me interage com segurança com ambientes externos e consulta ferramentas de API para fornecer respostas personalizadas para seu ambiente de armazenamento específico.

Fornecedores de nuvem compatíveis

O Workload Factory permite que você gerencie o armazenamento em nuvem e use recursos de carga de trabalho no Amazon Web Services.

Segurança

A segurança do NetApp Workload Factory é uma prioridade máxima para a NetApp. Todas as cargas de trabalho no Workload Factory são executadas sobre o Amazon FSx for NetApp ONTAP. Além de tudo "Recursos de segurança da AWS"O NetApp Workload Factory recebeu "Conformidade com SOC2 Tipo 1, conformidade com SOC2 Tipo 2 e conformidade com HIPAA.".

O Amazon FSx for NetApp ONTAP para NetApp Workload Factory é um"Solução AWS para implantação de aplicativos corporativos" que foi criado com as melhores práticas bem arquitetadas em mente.

Custo

O Workload Factory é gratuito. O custo que você paga à Amazon Web Services (AWS) depende dos serviços de armazenamento e carga de trabalho que você planeja implantar. Isso inclui o custo do Amazon FSx for NetApp ONTAP , infraestrutura do VMware Cloud na AWS, serviços da AWS e muito mais.

Como funciona o Workload Factory

O Workload Factory inclui um console baseado na web fornecido por meio da camada SaaS, uma conta, modos operacionais que controlam o acesso ao seu ambiente de nuvem, links que fornecem conectividade segregada entre o Workload Factory e uma conta da AWS e muito mais.

Software como serviço

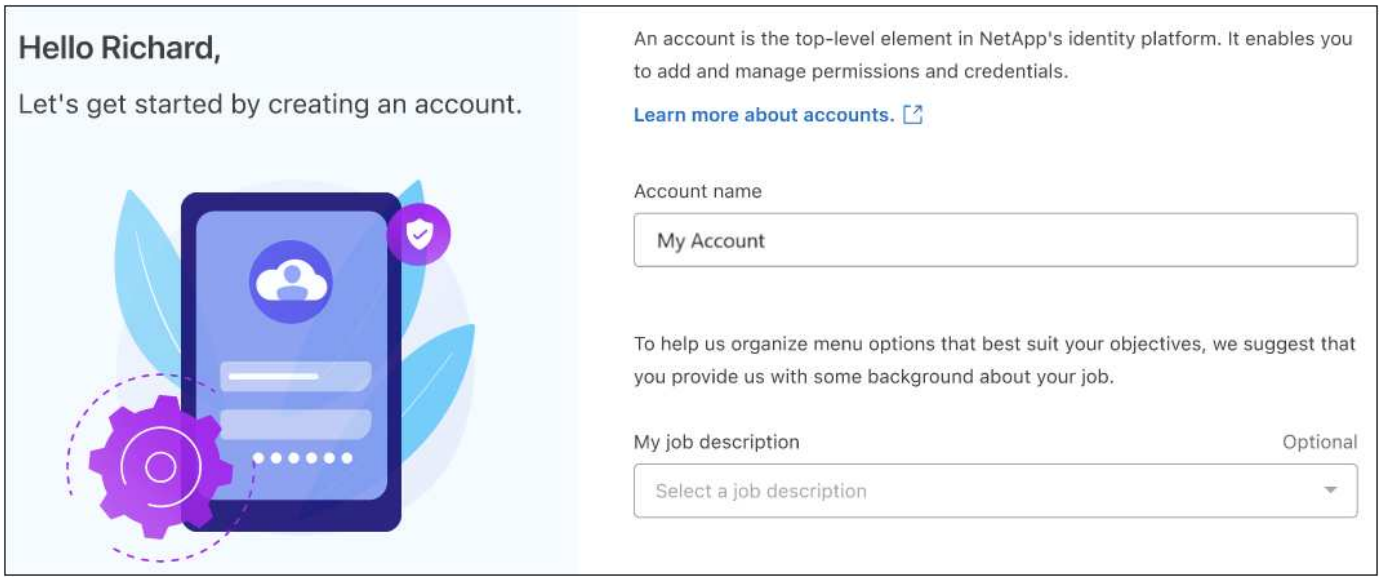
O Workload Factory pode ser acessado através do"Console do NetApp Workload Factory" e o"Console NetApp" . Essas experiências SaaS permitem que você acesse automaticamente os recursos mais recentes assim que são lançados e alterne facilmente entre suas contas e links do Workload Factory.

"Saiba mais sobre as diferentes experiências de console."

Contas

Ao efetuar login no Workload Factory pela primeira vez, você será solicitado a criar uma conta. Esta conta permite que você organize seus recursos, cargas de trabalho e acesso a cargas de trabalho para sua

organização usando credenciais.



Quando você cria uma conta, você é o único usuário *Account admin* dessa conta.

Se a sua organização necessitar de uma conta adicional ou gestão de utilizadores, contacte-nos através do chat no produto.

Se você usar o NetApp Console, já pertencerá a uma conta porque o Workload Factory utiliza contas NetApp .

Contas de serviço

Uma conta de serviço atua como um "usuário" que pode fazer chamadas de API autorizadas ao NetApp Workload Factory para fins de automação. Isso facilita o gerenciamento da automação porque você não precisa criar scripts de automação com base na conta de usuário de uma pessoa real que pode sair da empresa a qualquer momento. Todos os titulares de contas no Workload Factory são considerados administradores de contas. Os administradores de contas podem criar e excluir várias contas de serviço.

"Saiba como gerenciar contas de serviço"

Permissões

O Workload Factory oferece políticas de permissão flexíveis que permitem controlar cuidadosamente o acesso ao seu ambiente de nuvem e atribuir níveis incrementais de confiança ao Workload Factory com base em suas políticas de TI.

"Saiba mais sobre as políticas de permissão do Workload Factory."

Ligações de conetividade

Um link do Workload Factory cria uma relação de confiança e conectividade entre o Workload Factory e um ou mais sistemas de arquivos FSx para ONTAP . Isso permite que você monitore e gerencie determinados recursos do sistema de arquivos diretamente das chamadas da API REST do ONTAP que não estão disponíveis por meio da API do Amazon FSx para ONTAP .

Você não precisa de um link para começar a usar o Workload Factory, mas em alguns casos você precisará criar um link para desbloquear todos os recursos e funcionalidades de carga de trabalho do Workload Factory.

Atualmente, os links utilizam o AWS Lambda.

"Saiba mais sobre links"

Automação Codebox

O Codebox é um copiloto de Infraestrutura como Código (IaC) que ajuda desenvolvedores e engenheiros de DevOps a gerar o código necessário para executar qualquer operação suportada pelo Workload Factory. Os formatos de código incluem API REST do Workload Factory, AWS CLI e AWS CloudFormation.

O Codebox está alinhado com os modos de operação do Workload Factory (*básico*, *somente leitura* e *leitura/gravação*) e define um caminho claro para prontidão de execução, bem como um catálogo de automação para rápida reutilização futura.

O painel Codebox mostra o IAC que é gerado por uma operação de fluxo de trabalho específica e é correspondido por um assistente gráfico ou interface de chat conversacional. Embora o Codebox suporte codificação de cores e pesquisa para facilitar a navegação e análise, ele não permite edição. Você só pode copiar ou salvar no Catálogo de Automação.

"Saiba mais sobre o Codebox"

Calculadoras de poupança

O Workload Factory oferece calculadoras de economia para que você possa comparar os custos de seus ambientes de armazenamento, bancos de dados ou cargas de trabalho VMware em sistemas de arquivos FSx para ONTAP com outros serviços da Amazon. Dependendo das suas necessidades de armazenamento, você pode descobrir que os sistemas de arquivos FSx para ONTAP são a opção mais econômica para você.

- "Saiba como explorar a economia para seus ambientes de armazenamento"
- "Saiba como explorar a economia para suas cargas de trabalho de banco de dados"
- "Aprenda como explorar oportunidades de economia para suas cargas de trabalho VMware."

Cargas de trabalho bem arquitetadas

O Workload Factory ajuda você a manter e operar configurações de armazenamento e banco de dados confiáveis, seguras, eficientes e econômicas, alinhadas ao AWS Well-Architected Framework. O Workload Factory analisa diariamente as instalações do FSx em busca de sistemas de arquivos ONTAP , SQL Server e bancos de dados Oracle para fornecer informações sobre possíveis erros de configuração e recomendar ações manuais ou automatizadas para corrigir os problemas.

"Saiba mais sobre cargas de trabalho bem arquitetadas."

Ferramentas para usar o NetApp Workload Factory

Você pode usar o NetApp Workload Factory com as seguintes ferramentas:

- **Console do Workload Factory**: O console do Workload Factory fornece uma visão visual e holística de seus aplicativos e projetos.
- * NetApp Console*: O NetApp Console oferece uma experiência de interface híbrida para que você possa usar o Workload Factory junto com outros serviços de dados do NetApp .
- **Pergunte-me**: use o assistente de IA Ask me para fazer perguntas e saber mais sobre o Workload Factory sem sair do console do Workload Factory. Acesse Pergunte-me no menu de ajuda do Workload Factory.

- **CloudShell CLI**: O Workload Factory inclui um CloudShell CLI para gerenciar e operar ambientes AWS e NetApp em todas as contas a partir de um único CLI baseado em navegador. Acesse o CloudShell na barra superior do console do Workload Factory.
- **API REST**: Use as APIs REST do Workload Factory para implantar e gerenciar seu FSx para sistemas de arquivos ONTAP e outros recursos da AWS.
- **CloudFormation**: use o código do AWS CloudFormation para executar as ações definidas no console do Workload Factory para modelar, provisionar e gerenciar recursos da AWS e de terceiros da pilha do CloudFormation na sua conta da AWS.
- **Provedor do Terraform NetApp Workload Factory**: use o Terraform para criar e gerenciar fluxos de trabalho de infraestrutura gerados no console do Workload Factory.

APIS REST

O Workload Factory permite que você otimize, automatize e opere seus sistemas de arquivos FSx for ONTAP para cargas de trabalho específicas. Cada carga de trabalho expõe uma API REST associada. Coletivamente, essas cargas de trabalho e APIs formam uma plataforma de desenvolvimento flexível e extensível que você pode usar para administrar seus sistemas de arquivos FSx para ONTAP .

Há vários benefícios ao usar as APIs REST do Workload Factory:

- As APIs foram projetadas com base na TECNOLOGIA REST e nas práticas recomendadas atuais. As tecnologias principais incluem HTTP e JSON.
- A autenticação do Workload Factory é baseada no padrão OAuth2. O NetApp depende da implementação do serviço Auth0.
- O console baseado na Web do Workload Factory usa as mesmas APIs REST principais para que haja consistência entre os dois caminhos de acesso.

"Veja a documentação da API REST do Workload Factory"

Experiências de console

O NetApp Workload Factory pode ser acessado por meio de dois consoles baseados na Web. Saiba como acessar o Workload Factory usando o console do Workload Factory e o NetApp Console.

- * NetApp Console*: Oferece uma experiência híbrida onde você pode gerenciar seus sistemas de arquivos FSx para ONTAP e cargas de trabalho em execução no Amazon FSx for NetApp ONTAP no mesmo lugar.
- **Console do Workload Factory**: Oferece uma experiência dedicada do Workload Factory focada em cargas de trabalho em execução no Amazon FSx for NetApp ONTAP.

Acesse o Workload Factory no console do NetApp

Você pode acessar o Workload Factory a partir do NetApp Console. Além de usar o Workload Factory para armazenamento e recursos de carga de trabalho da AWS, você também pode acessar outros serviços de dados, como o NetApp Copy and Sync, entre outros.

Passos

1. Faça login no"Console NetApp" .
2. No menu do NetApp Console, selecione **Cargas de trabalho** e depois **Visão geral**.

Acesse o Workload Factory no console do Workload Factory

Você pode acessar o Workload Factory no console do Workload Factory.

Passo

1. Faça login no"Console da Workload Factory" .

Permissões para o NetApp Workload Factory

Para usar os recursos e serviços do NetApp Workload Factory, você precisará fornecer permissões para que o Workload Factory possa executar operações no seu ambiente de nuvem.

Por que usar permissões

Ao conceder permissões, o Workload Factory associa uma política à instância com permissões para gerenciar recursos e processos dentro dessa conta da AWS. Isso permite que o Workload Factory execute diversas operações, desde a descoberta de seus ambientes de armazenamento até a implantação de recursos da AWS, como sistemas de arquivos no gerenciamento de armazenamento ou bases de conhecimento para cargas de trabalho do GenAI.

Para cargas de trabalho de banco de dados, por exemplo, quando o Workload Factory recebe as permissões necessárias, ele verifica todas as instâncias do EC2 em uma determinada conta e região e filtra todas as máquinas baseadas no Windows. Se o agente do AWS Systems Manager (SSM) estiver instalado e em execução no host e a rede do System Manager estiver configurada corretamente, o Workload Factory poderá acessar a máquina Windows e verificar se o software SQL Server está instalado ou não.

Permissões por carga de trabalho

Cada carga de trabalho utiliza permissões para executar determinadas tarefas no Workload Factory. As permissões são agrupadas em políticas de permissão definidas. Role a página até a carga de trabalho que você utiliza para saber mais sobre as políticas de permissão, o JSON copiável dessas políticas e uma tabela que lista todas as permissões, sua finalidade, onde são usadas e quais políticas de permissão as suportam.

Permissões para armazenamento

As políticas do IAM disponíveis para o Storage fornecem as permissões necessárias para que o Workload Factory gerencie recursos e processos em seu ambiente de nuvem pública.

O armazenamento oferece as seguintes políticas de permissão para escolha:

- **Visualização, planejamento e análise**: Visualize os sistemas de arquivos FSx para ONTAP , aprenda sobre a integridade do sistema, obtenha uma análise bem arquitetada para seus sistemas e explore oportunidades de economia.
- **Operações e correções**: Execute tarefas operacionais como ajustar a capacidade do sistema de arquivos e corrigir problemas nas configurações do seu sistema de arquivos.
- **Criação e exclusão de sistemas de arquivos**: Crie e exclua sistemas de arquivos FSx para ONTAP e máquinas virtuais de armazenamento.

Veja as políticas IAM necessárias:

Políticas do IAM para armazenamento

Visualização, planejamento e análise

```
{
  "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": "*"
    }
  ]
}
```

Operações e remediação

```
{
  "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": "*"
    }
  ]
}
```

Criação e exclusão de sistemas de arquivos

```
{
  "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": "*"
    }
  ]
}
```

A tabela a seguir exibe as permissões para armazenamento.

Tabela de permissões para armazenamento

Finalidade	Ação	Onde usado	Política de permissão
Crie um sistema de arquivos FSX for ONTAP	fsx:CreateFileSystem	Implantação	Criação e exclusão de sistemas de arquivos
Crie um grupo de segurança para um sistema de arquivos FSX for ONTAP	EC2:CreateSecurityGroup	Implantação	Criação e exclusão de sistemas de arquivos
Adicione tags a um grupo de segurança para um sistema de arquivos FSX for ONTAP	EC2:CreateTags	Implantação	Criação e exclusão de sistemas de arquivos
Autorize a saída do grupo de segurança e a entrada para um sistema de arquivos FSX for ONTAP	EC2:AutorizeSecurityGroupEgress	Implantação	Criação e exclusão de sistemas de arquivos
	EC2:AutorizeSecurityGroupIngress	Implantação	Criação e exclusão de sistemas de arquivos
A função concedida fornece comunicação entre o FSX for ONTAP e outros serviços da AWS	IAM:CreateServiceLinkRole	Implantação	Criação e exclusão de sistemas de arquivos

Finalidade	Ação	Onde usado	Política de permissão
Obtenha detalhes para preencher o formulário de implantação do sistema de arquivos FSX for ONTAP	EC2: DescribeVPCs	• Implantação • Explore as poupanças	Criação e exclusão de sistemas de arquivos
	EC2: DescribeSubnets	• Implantação • Explore as poupanças	Criação e exclusão de sistemas de arquivos
	EC2:DescribeSecurityGroups	• Implantação • Explore as poupanças	Criação e exclusão de sistemas de arquivos
	EC2:DescribeRouteTables	• Implantação • Explore as poupanças	Criação e exclusão de sistemas de arquivos
	EC2:DescribeNetworkInterfaces	• Implantação • Explore as poupanças	Criação e exclusão de sistemas de arquivos
	EC2:DescribeVolumeStatus	• Implantação • Explore as poupanças	Criação e exclusão de sistemas de arquivos
Obtenha os detalhes das chaves do KMS e use a criptografia FSX for ONTAP	Kms:CreateGrant	Implantação	Criação e exclusão de sistemas de arquivos
	Kms:DescribeKey	Implantação	Criação e exclusão de sistemas de arquivos
	Kms: ListKeys	Implantação	Criação e exclusão de sistemas de arquivos
	Kms:ListAliases	Implantação	Criação e exclusão de sistemas de arquivos

Finalidade	Ação	Onde usado	Política de permissão
Obtenha detalhes do volume para instâncias EC2	EC2:DescribeVolumes	• Inventário • Explore as poupanças	Visualização, planejamento e análise
Obtenha detalhes para instâncias EC2	EC2: DescribeInstances	Explore as poupanças	Visualização, planejamento e análise
Descrever o Elastic File System na calculadora de economia	Elasticfilesystem:DescreverSistemasDeArquivos	Explore as poupanças	Visualização, planejamento e análise
Listar tags para recursos do FSX for ONTAP	fsx:ListTagsForResource	Inventário	Visualização, planejamento e análise
Gerencie a saída do grupo de segurança e o ingresso para um sistema de arquivos FSX for ONTAP	EC2:RevokeSecurityGroupIngress	Operações de gerenciamento	Criação e exclusão de sistemas de arquivos
	ec2: RevokeSecurityGroupEgress	Operações de gerenciamento	Criação e exclusão de sistemas de arquivos
	EC2:DeleteSecurityGroup	Operações de gerenciamento	Criação e exclusão de sistemas de arquivos

Finalidade	Ação	Onde usado	Política de permissão
Crie, visualize e gerencie recursos do sistema de arquivos FSX for ONTAP			

	fsx:DescribeBackups	Operações de gerenciamento	Visualização, planejamento e análise
Finalidade	**Ação**	**Onde usado**	**Política de permissão**
	fsx:CriarBackup	Operações de gerenciamento	Operações e remediação
	fsx:CriarVolumeA partirDoBackup	Operações de gerenciamento	Operações e remediação
	fsx:ExcluirBackup	Operações de gerenciamento	Operações e remediação
Obtenha métricas de volume e sistema de arquivos	cloudwatch: GetMetricData	Operações de gerenciamento	Visualização, planejamento e análise
	cloudwatch:GetMetricStatistics	Operações de gerenciamento	Visualização, planejamento e análise
Simule operações de carga de trabalho para validar permissões disponíveis e compare com as permissões de conta da AWS necessárias	IAM:SimulatePrincipalPolicy	Implantação	Todos
Fornecer insights baseados em IA para eventos FSx para ONTAP EMS	Bedrock:ListInferenceProfiles	FSx para análise ONTAP EMS	Operações e remediação
	bedrock:GetInferenceProfile	FSx para análise ONTAP EMS	Operações e remediação
	bedrock:InvokeModelWithResponseStream	FSx para análise ONTAP EMS	Operações e remediação
	Bedrock:modelo InvokeModel	FSx para análise ONTAP EMS	Operações e remediação
Obtenha dados de custo e uso para sistemas de arquivos FSx para ONTAP no AWS Cost Explorer.	ce:ObterCustoEUso	Análise de custos e utilização	Visualização, planejamento e análise
	ce:ObterTags	Análise de custos e utilização	Visualização, planejamento e análise
Crie um ponto de acesso S3 e conecte-o a um sistema de arquivos Amazon FSx for NetApp ONTAP	fsx:CreateAndAttachS3AccessPoint	Gerenciamento de pontos de acesso S3	Operações e remediação
Desconecte um ponto de acesso S3 de um sistema de arquivos FSx for ONTAP e exclua-o	fsx:DetachAndDeleteS3AccessPoint	Gerenciamento de pontos de acesso S3	Operações e remediação
Crie um ponto de acesso S3 para simplificar o gerenciamento de acesso ao bucket	s3:CreateAccessPoint	Gerenciamento de pontos de acesso S3	Operações e remediação

Finalidade	Ação	Onde usado	Política de permissão
Excluir um ponto de acesso S3	s3:DeleteAccessPoint	Gerenciamento de pontos de acesso S3	Operações e remediação
Adicionar tags a um ponto de acesso S3	s3:TagResource	Gerenciamento de pontos de acesso S3	Operações e remediação
Listar e visualizar tags em um ponto de acesso S3	s3:ListTagsForResource	Gerenciamento de pontos de acesso S3	Operações e remediação
Remova tags de um ponto de acesso S3	s3:UntagResource	Gerenciamento de pontos de acesso S3	Operações e remediação
Descobrir objetos em um bucket de ponto de acesso S3	s3:ListBucket	Operações de bucket S3	Operações e remediação
Listar, criar e descrever buckets de tabela S3	s3tables:ListTableBuckets s3tables:CreateTableBucket s3tables:GetTableBucket	Gerenciamento de bucket de tabela S3	Operações e remediação
Liste, crie e recupere tabelas S3	s3tables:ListTables s3tables:CreateTable s3tables:GetTable	Operações de tabela S3	Operações e remediação
Ler localização dos metadados da tabela	s3tables:GetTableMetadataLocation	Operações de metadados da tabela S3	Operações e remediação
Atualizar localização dos metadados da tabela	s3tables:UpdateTableMetadataLocation	Operações de metadados da tabela S3	Operações e remediação
Listar, criar e recuperar namespaces de tabelas	s3tables:ListNamespaces s3tables:CreateNamespace s3tables:GetNamespace	Operações de namespace S3	Operações e remediação
Ler dados da tabela (select, scan)	s3tables:GetTableData	Operações de dados da tabela S3	Operações e remediação
Escrever dados da tabela (insert)	s3tables:PutTableData	Operações de dados da tabela S3	Operações e remediação
Listar tags em uma tabela de inventário (obter FSx for ONTAP, storage VM, IDs de volume)	s3tables:ListTagsForResource	Operações de tags de tabela S3	Operações e remediação
Marque uma tabela de inventário para pesquisa na NetApp Workload Factory	s3tables:TagResource	Operações de tags de tabela S3	Operações e remediação
Recuperar marcação de objetos via ponto de acesso	s3:GetObjectTagging	Operações de objetos S3	Operações e remediação

Permissões para cargas de trabalho de banco de dados

As políticas do IAM disponíveis para cargas de trabalho de banco de dados fornecem as permissões necessárias para que o Workload Factory gerencie recursos e processos em seu ambiente de nuvem pública.

O banco de dados oferece as seguintes políticas de permissão para escolha:

- **Visualização, planejamento e análise**: Visualize o inventário de recursos do banco de dados, aprenda sobre a integridade de seus recursos, revise a análise de arquitetura adequada para suas configurações de banco de dados e explore oportunidades de economia, obtenha análises de logs de erros e explore possíveis economias.
- **Operações e correção**: Execute tarefas operacionais para seus recursos de banco de dados e corrija problemas de configuração do banco de dados e do sistema de arquivos FSx para ONTAP subjacente.
- **Criação de hosts de banco de dados**: Implante os hosts de banco de dados e o armazenamento do sistema de arquivos FSx para ONTAP subjacente de acordo com as melhores práticas.

Selecione o modo operacional para visualizar as políticas do IAM necessárias:

Políticas de IAM para cargas de trabalho de banco de dados

Visualização, planejamento e análise

```
{
    "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/*"
        }
    ]
}
```

Operações e remediação

```
[
    {
        "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*"
            }
        }
    }
]
```

Criação de host de banco de dados

```
{
    "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*"
        }
    ]
}
```

A tabela a seguir exibe as permissões para cargas de trabalho de banco de dados.

Tabela de permissões para workloads de banco de dados

Finalidade	Ação	Onde usado	Política de permissão
Obtenha estatísticas métricas para FSx para ONTAP, EBS e FSx para Windows File Server e para recomendação de otimização de computação	cloudwatch:GetMetricStatistics	• Inventário • Explore as poupanças	Visualização, planejamento e análise
Reúna métricas de desempenho salvas no Amazon CloudWatch a partir de nós SQL registrados. Os dados são gerados em gráficos de tendências de desempenho na tela de gerenciamento de instâncias SQL registradas.	cloudwatch: GetMetricData	Inventário	Visualização, planejamento e análise
Obtenha detalhes para instâncias EC2	EC2: DescribeInstances	• Inventário • Explore as poupanças	Visualização, planejamento e análise
	EC2: DescribeKeyPairs	Implantação	Visualização, planejamento e análise
	EC2:DescribeNetworkInterfaces	Implantação	Visualização, planejamento e análise
	EC2:DescribeInstanceTypes	• Implantação • Explore as poupanças	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Obtenha detalhes para preencher o formulário de implantação do FSX for ONTAP	EC2: DescribeVPCs	• Implantação • Inventário	Visualização, planejamento e análise
	EC2: DescribeSubnets	• Implantação • Inventário	Visualização, planejamento e análise
	EC2:DescribeSecurityGroups	Implantação	Visualização, planejamento e análise
	EC2: DescribeImages	Implantação	Visualização, planejamento e análise
	EC2:DescribeRegiões	Implantação	Visualização, planejamento e análise
	EC2:DescribeRouteTables	• Implantação • Inventário	Visualização, planejamento e análise
Obtenha quaisquer endpoints VPC existentes para determinar se novos endpoints precisam ser criados antes das implantações	EC2:DescribeVpcEndpoints	• Implantação • Inventário	Visualização, planejamento e análise
Crie endpoints VPC se eles não existirem para serviços necessários, independentemente da conetividade de rede pública em instâncias EC2	EC2:CreateVpcEndpoint	Implantação	Criação de host de banco de dados
Obter tipos de instância disponíveis na região para nós de validação (T2.micro/T3.micro)	EC2:DescribeInstanceTypeOfferings	Implantação	Visualização, planejamento e análise
Obtenha detalhes de snapshot de cada volume EBS anexado para estimativa de preços e economia	EC2:DescribeSnapshots	Explore as poupanças	Visualização, planejamento e análise
Obtenha detalhes de cada volume EBS anexado para estimativa de preços e economia	EC2:DescribeVolumes	• Inventário • Explore as poupanças	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Obtenha detalhes da chave do KMS para criptografia do sistema de arquivos FSX for ONTAP	Kms:ListAliases	Implantação	Visualização, planejamento e análise
	Kms: ListKeys	Implantação	Visualização, planejamento e análise
	Kms:DescribeKey	Implantação	Visualização, planejamento e análise
Obtenha uma lista de pilhas do CloudFormation em execução no ambiente para verificar o limite de cota	Cloudformation:ListStacks	Implantação	Visualização, planejamento e análise
Verifique os limites de conta para recursos antes de acionar a implantação	Cloudformation:DescribeAccount Limits	Implantação	Visualização, planejamento e análise
Obtenha a lista de diretórios ativos gerenciados pela AWS na região	ds:DescribeDirectories	Implantação	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Obtenha listas e detalhes de volumes, backups, SVMs, sistemas de arquivos no AZs e tags para o sistema de arquivos FSX for ONTAP	fsx:DescribeVolumes	• Inventário • Explore a economia	Visualização, planejamento e análise
	fsx:DescribeBackups	• Inventário • Explore a economia	Visualização, planejamento e análise
	fsx:DescribeStorageVirtualMachines	• Implantação • Operações de gerenciamento • Inventário	Visualização, planejamento e análise
	fsx:DescribeFileSystems	• Implantação • Operações de gerenciamento • Inventário • Explore as poupanças	Visualização, planejamento e análise
	fsx:ListTagsForResource	Operações de gerenciamento	Visualização, planejamento e análise
Obtenha os limites de cota de serviço para CloudFormation e VPC / Crie segredos em uma conta de usuário para as credenciais fornecidas para SQL, domínio e FSx para ONTAP	Servicequotas:ListServiceQuotes	Implantação	Visualização, planejamento e análise
Use a consulta com base no SSM para obter a lista atualizada de regiões compatíveis com o FSX para ONTAP	ssm:GetParametersByPath	Implantação	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Aguardar resposta do SSM após o envio do comando para operações de gerenciamento pós-implantação	ssm:GetCommandInvocation	• Operações de gerenciamento • Inventário • Explore as poupanças • Otimização	Visualização, planejamento e análise
Enviar comandos via SSM para instâncias EC2 para descoberta e gerenciamento.	ssm:SendCommand	• Operações de gerenciamento • Inventário • Explore as poupanças • Otimização	Visualização, planejamento e análise
Obtenha o status de conetividade SSM em instâncias após a implantação	ssm:GetConnectionStatus	• Operações de gerenciamento • Inventário • Otimização	Visualização, planejamento e análise
Buscar status de associação SSM para um grupo de instâncias EC2 gerenciadas (nós SQL)	ssm:DescribeInstanceInformation	Inventário	Visualização, planejamento e análise
Obtenha a lista de linhas de base de patch disponíveis para avaliação de patches do sistema operacional	ssm:DescribePatchBaselines	Otimização	Visualização, planejamento e análise
Obtenha o estado de correção em instâncias do Windows EC2 para avaliação de patches do sistema operacional	ssm:DescribeInstancePatchStates	Otimização	Visualização, planejamento e análise
Listar comandos executados pelo AWS Patch Manager em instâncias do EC2 para gerenciamento de patches do sistema operacional	ssm:ListCommands	Otimização	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Verifique se a conta está inscrita no AWS Compute Optimizer	Otimizador de computação:GetEnrollmentStatus	• Explore as poupanças • Otimização	Criação de host de banco de dados
Atualize uma preferência de recomendação existente no AWS Compute Optimizer para personalizar sugestões para cargas de trabalho do servidor SQL	Otimizador de computação:PutRecommendationPreferences	• Explore as poupanças • Otimização	Criação de host de banco de dados
Obtenha preferências de recomendação que estão em vigor para um determinado recurso do AWS Compute Optimizer	Compute-Optimizer:GetEffectiveRecommendationPreferences	• Explore as poupanças • Otimização	Criação de host de banco de dados
Obtenha recomendações que o AWS Compute Optimizer gera para instâncias do Amazon Elastic Compute Cloud (Amazon EC2)	Otimizador de computação:GetEC2InstanceRecommendations	• Explore as poupanças • Otimização	Criação de host de banco de dados
Verifique a associação de instância aos grupos de dimensionamento automático	Dimensionamento automático:DescribeAutoScalingGroups	• Explore as poupanças • Otimização	Criação de host de banco de dados
	Dimensionamento automático:DescribeAutoScalingInstances	• Explore as poupanças • Otimização	Criação de host de banco de dados

Finalidade	Ação	Onde usado	Política de permissão
Obtenha, liste, crie e exclua parâmetros SSM para credenciais de usuário do AD, FSX for ONTAP e SQL usadas durante a implantação ou gerenciadas em sua conta da AWS	ssm: GetParameter 1	• Implantação • Operações de gerenciamento • Inventário	Visualização, planejamento e análise
	ssm: GetParameters 1	• Implantação • Operações de gerenciamento • Inventário	Visualização, planejamento e análise
	ssm: PutParameter 1	• Implantação • Operações de gerenciamento	Visualização, planejamento e análise
	ssm:DeleteParameters 1	• Implantação • Operações de gerenciamento	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Associe recursos de rede a nós SQL e nós de validação e adicione IPs secundários adicionais a nós SQL	EC2:AllocateAddress 1	Implantação	Criação de host de banco de dados
	EC2:AllocateHosts 1	Implantação	Criação de host de banco de dados
	EC2:AssignPrivateIpAddresses 1	Implantação	Criação de host de banco de dados
	EC2:AssociateAddress 1	Implantação	Criação de host de banco de dados
	EC2:AssociateRouteTable 1	Implantação	Criação de host de banco de dados
	EC2:AssociateSubnetCidrBlock 1	Implantação	Criação de host de banco de dados
	EC2:AssociateVpcCidrBlock 1	Implantação	Criação de host de banco de dados
	EC2:AttachInternetGateway 1	Implantação	Criação de host de banco de dados
	EC2:AttacNetworkInterface 1	Implantação	Criação de host de banco de dados
Anexe volumes EBS necessários aos nós SQL para implantação	EC2: Attachvolume	Implantação	Criação de host de banco de dados
Associe grupos de segurança e modifique regras às instâncias EC2 provisionadas.	EC2:AutorizeSecurityGroupEgress	Implantação	Criação de host de banco de dados
	EC2:AutorizeSecurityGroupIngress	Implantação	Criação de host de banco de dados
Crie volumes EBS necessários para os nós SQL para implantação	EC2:Createvolume	Implantação	Criação de host de banco de dados

Finalidade	Ação	Onde usado	Política de permissão
Remova os nós de validação temporária criados do tipo T2.micro e para reversão ou tentativa de reversão de nós SQL EC2 com falha	EC2:DeleteNetworkInterface	Implantação	Criação de host de banco de dados
	EC2:DeleteSecurityGroup	Implantação	Criação de host de banco de dados
	EC2:DeleteTags	Implantação	Criação de host de banco de dados
	EC2:Deletevolume	Implantação	Criação de host de banco de dados
	EC2: DetachNetworkInterface	Implantação	Criação de host de banco de dados
	EC2: Detachvolume	Implantação	Criação de host de banco de dados
	EC2:Endereço Desassociativo	Implantação	Criação de host de banco de dados
	EC2:DesassociateIamInstanceProfile	Implantação	Criação de host de banco de dados
	EC2:DesassociateRouteTable	Implantação	Criação de host de banco de dados
	EC2:DesassociateSubnetCidrBlock	Implantação	Criação de host de banco de dados
	EC2:DesassociateVpcCidrBlock	Implantação	Criação de host de banco de dados

Finalidade	Ação	Onde usado	Política de permissão
Modifique atributos para instâncias SQL criadas. Apenas aplicável a nomes que começam com WLMDB.	EC2:ModifyInstanceAttribute	Implantação	Operações e remediação
	EC2:ModifyInstancePlacement	Implantação	Criação de host de banco de dados
	EC2:ModifyNetworkInterfaceAttribute	Implantação	Criação de host de banco de dados
	EC2:ModifySubnetAttribute	Implantação	Criação de host de banco de dados
	EC2:Modifyvolume	Implantação	Criação de host de banco de dados
	EC2:ModifyVolumeAtributo	Implantação	Criação de host de banco de dados
	EC2:ModifyVpcAttribute	Implantação	Criação de host de banco de dados
Desassocie e destrua instâncias de validação	EC2: Endereço de entrega	Implantação	Criação de host de banco de dados
	EC2:ReplaceRoute	Implantação	Criação de host de banco de dados
	EC2:ReplaceRouteAssociation	Implantação	Criação de host de banco de dados
	EC2:RevokeSecurityGroupEgress	Implantação	Criação de host de banco de dados
	EC2:RevokeSecurityGroupIngress	Implantação	Criação de host de banco de dados
Inicie as instâncias implantadas	EC2: StartInstances	Implantação	Operações e remediação
Pare as instâncias implantadas	EC2:StopInstances	Implantação	Operações e remediação

Finalidade	Ação	Onde usado	Política de permissão
Marque valores personalizados para os recursos do Amazon FSX for NetApp ONTAP criados pelo WLMDB para obter detalhes de cobrança durante o gerenciamento de recursos	Bem-vindo ao site 1	• Implantação • Operações de gerenciamento	Criação de host de banco de dados
Crie e valide o modelo do CloudFormation para implantação	Formação de nuvens: CreateStack	Implantação	Criação de host de banco de dados
	Cloudformation:DescribeStackEvents	Implantação	Criação de host de banco de dados
	Cloudformation:DescribeStacks	Implantação	Criação de host de banco de dados
	Cloudformation:ListStacks	Implantação	Visualização, planejamento e análise
	Cloudformation:ValidateTemplate	Implantação	Criação de host de banco de dados
Crie modelos de pilha aninhados para tentar novamente e reverter	EC2:CreateLaunchTemplate	Implantação	Criação de host de banco de dados
	EC2:CreateLaunchTemplateVersion	Implantação	Criação de host de banco de dados
Gerencie tags e segurança de rede em instâncias criadas	EC2: CreateNetworkInterface	Implantação	Criação de host de banco de dados
	EC2:CreateSecurityGroup	Implantação	Criação de host de banco de dados
	EC2:CreateTags	Implantação	Criação de host de banco de dados
Obter detalhes da instância para provisionamento	ec2:DescreverEndereços	Implantação	Visualização, planejamento e análise
	ec2:DescreverModelos de Lançamento	Implantação	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Inicie as instâncias criadas	EC2:RunInstances	Implantação	Criação de host de banco de dados
Crie recursos do FSX for ONTAP necessários para o provisionamento. Para sistemas FSX para ONTAP existentes, um novo SVM foi criado para hospedar volumes SQL.	fsx:CreateFileSystem	Implantação	Criação de host de banco de dados
	fsx:CreateStorageVirtualMachine	Implantação	Criação de host de banco de dados
	fsx:Createvolume	• Implantação • Operações de gerenciamento	Criação de host de banco de dados
Obtenha os detalhes do FSX for ONTAP	fsx:DescribeFileSystemAliases	Implantação	Criação de host de banco de dados
Redimensione o sistema de arquivos FSX for ONTAP para corrigir o espaço livre do sistema de arquivos	fsx:UpdateFilesystem	Otimização	Operações e remediação
Redimensione volumes para corrigir os tamanhos de unidades de log e TempDB	fsx:Updatevolume	Otimização	Operações e remediação
Obtenha os detalhes das chaves do KMS e use a criptografia FSX for ONTAP	Kms:CreateGrant	Implantação	Criação de host de banco de dados
	kms:DescreverCustomKeyStores	Implantação	Criação de host de banco de dados
	Kms:GenerateDataKey	Implantação	Criação de host de banco de dados

Finalidade	Ação	Onde usado	Política de permissão
Crie logs do CloudWatch para scripts de validação e provisionamento executados em instâncias do EC2	Logs:CreateLogGroup	Implantação	Criação de host de banco de dados
	Logs:CreateLogStream	Implantação	Criação de host de banco de dados
	registros:GetLogGroupFields	Implantação	Criação de host de banco de dados
	registros: Obter Registro de Log	Implantação	Criação de host de banco de dados
	Registos:ListLogDeliveries	Implantação	Criação de host de banco de dados
	Logs:PutLogEvents	• Implantação • Operações de gerenciamento	Criação de host de banco de dados
	Logs:TagResource	Implantação	Criação de host de banco de dados
O Workload Factory alterna para logs do Amazon CloudWatch para a instância SQL ao encontrar truncamento de saída do SSM	Logs:GetLogEvents	• Avaliação de armazenamento (otimização) • Inventário	Visualização, planejamento e análise
Permitir que o Workload Factory obtenha grupos de log atuais e verificar se a retenção está definida para grupos de log criados pelo Workload Factory	Logs:DescribeLogGroups	• Avaliação de armazenamento (otimização) • Inventário	Visualização, planejamento e análise
Permitir que o Workload Factory defina uma política de retenção de um dia para grupos de log criados pelo Workload Factory para evitar acúmulo desnecessário de fluxos de log para saídas de comando do SSM	Logs:PutRetentationPolicy	• Avaliação de armazenamento (otimização) • Inventário	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Liste os tópicos do SNS do cliente e publique no SNS de back-end do WLMDB, bem como no SNS do cliente, se selecionado	sns:ListTopics	Implantação	Visualização, planejamento e análise
	sns:publicar	Implantação	Criação de host de banco de dados
Permissões de SSM necessárias para executar o script de descoberta em instâncias SQL provisionadas e buscar a lista mais recente de regiões AWS compatíveis com o FSX para ONTAP.	ssm: Aplicação de segurança	Implantação	Criação de host de banco de dados
	ssm:PutConfigurePackageResult	Implantação	Criação de host de banco de dados
	ssm:Stock	Implantação	Criação de host de banco de dados
	ssm:UpdateAssociationStatus	Implantação	Criação de host de banco de dados
	ssm:UpdateInstanceAssociationStatus	Implantação	Criação de host de banco de dados
	ssm:UpdateInstanceInformation	Implantação	Criação de host de banco de dados
	ssmmessages:CriarCanalDeControle	Implantação	Criação de host de banco de dados
	ssmmessages:CriarCanalDeDados	Implantação	Criação de host de banco de dados
	ssmmessages:OpenControlChannel	Implantação	Criação de host de banco de dados
	ssmmessages:OpenDataChannel	Implantação	Criação de host de banco de dados
Sinalize a pilha do CloudFormation com sucesso ou falha.	Cloudformation: SignalResource 1	Implantação	Criação de host de banco de dados
Adicione a função EC2 criada por modelo ao perfil de instância do EC2 para permitir que scripts no EC2 acessem os recursos necessários para implantação.	IAM:AddRoleToInstanceProfile	Implantação	Criação de host de banco de dados

Finalidade	Ação	Onde usado	Política de permissão
Crie o perfil de instância para EC2 e anexe a função EC2 criada.	IAM:CreateInstanceProfile	Implantação	Criação de host de banco de dados
Crie uma função EC2D através de modelo com as permissões listadas abaixo	IAM:CreateRole	Implantação	Criação de host de banco de dados
Criar função vinculada ao serviço EC2	ISO:CreateServiceLinkRole 2	Implantação	Criação de host de banco de dados
Excluir perfil de instância criado durante a implantação especificamente para os nós de validação	IAM:DeleteInstanceProfile	Implantação	Criação de host de banco de dados
Obtenha os detalhes da função e da política para determinar quaisquer lacunas na permissão e validar para a implantação	IAM:GetPolicy	Implantação	Criação de host de banco de dados
	IAM:GetPolicyVersion	Implantação	Criação de host de banco de dados
	IAM: GetRole	Implantação	Criação de host de banco de dados
	IAM:GetRolePolicy	Implantação	Criação de host de banco de dados
	IAM:GetUser	Implantação	Criação de host de banco de dados
Passe a função criada para a instância EC2	3	Implantação	Criação de host de banco de dados
Adicione a política com as permissões necessárias à função EC2 criada	IAM:PutRolePolicy	Implantação	Criação de host de banco de dados
Separe a função do perfil de instância do EC2 provisionado	IAM:RemoveRoleFromInstanceProfile	Implantação	Criação de host de banco de dados
Simule operações de carga de trabalho para validar permissões disponíveis e compare com as permissões de conta da AWS necessárias	IAM:SimulatePrincipalPolicy	Implantação	Todos

Finalidade	Ação	Onde usado	Política de permissão
Obtenha os modelos básicos disponíveis para análise de logs de erros.	Bedrock:GetFoundationModelAvailability	Análise do registro de erros	Visualização, planejamento e análise
Liste os perfis de interface disponíveis no Amazon Bedrock para análise de logs de erros.	Bedrock:ListInferenceProfiles	Análise do registro de erros	Visualização, planejamento e análise

1. A permissão é restrita a recursos que começam com WLMDB.
2. "IAM:CreateServiceLinkRole" limitado por "iam:AWSServiceName": "ec2.amazonaws.com"*
3. "IAM:PassRole" limitado por "iam:PassedToService": "ec2.amazonaws.com"*

Permissões para cargas de trabalho do GenAI

As políticas do IAM para cargas de trabalho do VMware fornecem as permissões que o Workload Factory for VMware precisa para gerenciar recursos e processos dentro do seu ambiente de nuvem pública com base no modo operacional em que você opera.

As políticas GenAI IAM estão disponíveis apenas com permissões de *leitura/gravação*:

- **Leitura/Gravação**: executa e automatiza operações na AWS em seu nome, utilizando as credenciais atribuídas que possuem as permissões necessárias e validadas para a execução.

Políticas do IAM para workloads do GenAI

```
{
  "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": "*"
    }
  ]
}
```

A tabela a seguir fornece detalhes sobre as permissões para cargas de trabalho do GenAI.

Tabela de permissões para workloads do GenAI

Finalidade	Ação	Onde usado	Política de permissão
Crie uma pilha de formação de nuvem do mecanismo de AI durante as operações de implantação e recriação	Formação de nuvens: CreateStack	Implantação	Leitura/escrita
Crie a pilha de formação de nuvem do mecanismo de AI	Cloudformation:DescribeStacks	Implantação	Leitura/escrita
Listar regiões para o assistente de implantação do mecanismo de IA	EC2:DescribeRegiões	Implantação	Leitura/escrita
Exibir tags de mecanismo AI	EC2: DescribeTags	Implantação	Leitura/escrita
Listar buckets S3	S3:ListAllMyBuckets	Implantação	Leitura/escrita
Listar os endpoints da VPC antes da criação da pilha do mecanismo de IA	EC2:CreateVpcEndpoint	Implantação	Leitura/escrita
Crie um grupo de segurança do mecanismo de AI durante a criação da stack de mecanismos de AI durante as operações de implantação e reconstrução	EC2:CreateSecurityGroup	Implantação	Leitura/escrita
Identifique os recursos criados pela criação da pilha do mecanismo de AI durante as operações de implantação e reconstrução	EC2:CreateTags	Implantação	Leitura/escrita
Publique eventos criptografados no backend WLMAI da pilha de mecanismos de IA	Kms:GenerateDataKey	Implantação	Leitura/escrita
	Kms:desencriptar	Implantação	Leitura/escrita
Publique eventos e recursos personalizados no backend WLMAI a partir da pilha de ai-Engine	sns:publicar	Implantação	Leitura/escrita
Listar VPCs durante o assistente de implantação do mecanismo de IA	EC2: DescribeVPCs	Implantação	Leitura/escrita
Liste sub-redes no assistente de implantação do AI-Engine	EC2: DescribeSubnets	Implantação	Leitura/escrita
Obtenha tabelas de rota durante a implantação e reconstrução do mecanismo de IA	EC2:DescribeRouteTables	Implantação	Leitura/escrita

Finalidade	Ação	Onde usado	Política de permissão
Listar pares de chaves durante o assistente de implantação do mecanismo de IA	EC2: DescribeKeyPairs	Implantação	Leitura/escrita
Listar grupos de segurança durante a criação da pilha do mecanismo de IA (para localizar grupos de segurança nos endpoints privados)	EC2:DescribeSecurityGroups	Implantação	Leitura/escrita
Obtenha endpoints de VPC para determinar se algum deve ser criado durante a implantação do mecanismo de AI	EC2:DescribeVpcEndpoints	Implantação	Leitura/escrita
Liste os aplicativos do Amazon Q Business	Qbusiness:ListAplicações	Implantação	Leitura/escrita
Liste instâncias para descobrir o estado do mecanismo de IA	EC2: DescribeInstances	Solução de problemas	Leitura/escrita
Listar imagens durante a criação da pilha do mecanismo de AI durante as operações de implantação e reconstrução	EC2: DescribeImages	Implantação	Leitura/escrita
Crie e atualize instância de IA e grupo de segurança de endpoint privado durante a criação da pilha de instâncias de IA durante as operações de implantação e reconstrução	EC2:RevokeSecurityGroupEgress	Implantação	Leitura/escrita
	EC2:RevokeSecurityGroupIngress	Implantação	Leitura/escrita
Execute o mecanismo de AI durante a criação da stack de cloudformation durante as operações de implantação e recriação	EC2:RunInstances	Implantação	Leitura/escrita
Anexe o grupo de segurança e modifique as regras do mecanismo de AI durante a criação da stack durante as operações de implantação e recriação	EC2:AutorizeSecurityGroupEgress	Implantação	Leitura/escrita
	EC2:AutorizeSecurityGroupIngress	Implantação	Leitura/escrita
Inicie a solicitação de bate-papo para um dos modelos básicos	Bedrock:InvokeModelWithResponseStream	Implantação	Leitura/escrita
Inicie a solicitação de bate-papo/incorporação para modelos de base	Bedrock:modelo InvokeModel	Implantação	Leitura/escrita
Mostre os modelos de fundação disponíveis em uma região	Bedrock:ListFoundationModels	Implantação	Leitura/escrita

Finalidade	Ação	Onde usado	Política de permissão
Obtenha informações sobre um modelo de fundação	Bedrock:GetFoundationModel	Implantação	Leitura/escrita
Verifique o acesso ao modelo da base	Bedrock:GetFoundationModelAvailability	Implantação	Leitura/escrita
Verifique a necessidade de criar o grupo de log do Amazon CloudWatch durante as operações de implantação e reconstrução	Logs:DescribeLogGroups	Implantação	Leitura/escrita
Obtenha regiões compatíveis com FSX e Amazon bedrock durante o assistente do mecanismo de AI	ssm:GetParametersByPath	Implantação	Leitura/escrita
Obtenha a imagem mais recente do Amazon Linux para a implantação do mecanismo de IA durante as operações de implantação e reconstrução	ssm:GetParameters	Implantação	Leitura/escrita
Obtenha a resposta SSM do comando enviado ao mecanismo de IA	ssm:GetCommandInvocation	Implantação	Leitura/escrita
Verifique a ligação SSM ao motor AI	ssm:SendCommand	Implantação	Leitura/escrita
	ssm:GetConnectionStatus	Implantação	Leitura/escrita
Crie um perfil de instância do mecanismo de AI durante a criação de stack durante as operações de implantação e reconstrução	IAM:CreateRole	Implantação	Leitura/escrita
	IAM:CreateInstanceProfile	Implantação	Leitura/escrita
	IAM:AddRoleToInstanceProfile	Implantação	Leitura/escrita
	IAM:PutRolePolicy	Implantação	Leitura/escrita
	IAM:GetRolePolicy	Implantação	Leitura/escrita
	IAM: GetRole	Implantação	Leitura/escrita
	IAM:TagRole	Implantação	Leitura/escrita
	IAM:PassRole	Implantação	Leitura/escrita
Simule operações de carga de trabalho para validar permissões disponíveis e compare com as permissões de conta da AWS necessárias	IAM:SimulatePrincipalPolicy	Implantação	Leitura/escrita
Liste o FSX para sistemas de arquivos ONTAP durante o assistente "criar base de conhecimento"	fsx:DescribeVolumes	Criação da base de conhecimento	Leitura/escrita

Finalidade	Ação	Onde usado	Política de permissão
Liste os volumes do sistema de arquivos do FSX for ONTAP durante o assistente "criar base de conhecimento"	fsx:DescribeFileSystems	Criação da base de conhecimento	Leitura/escrita
Gerencie bases de conhecimento no mecanismo de AI durante as operações de reconstrução	fsx:ListTagsForResource	Solução de problemas	Leitura/escrita
Liste as máquinas virtuais de armazenamento do sistema de arquivos do FSX for ONTAP durante o assistente "criar base de conhecimento"	fsx:DescribeStorageVirtualMachines	Implantação	Leitura/escrita
Mova a base de conhecimento para uma nova instância	fsx:UntagResource	Solução de problemas	Leitura/escrita
Gerencie a base de conhecimento no mecanismo de IA durante a reconstrução	fsx:TagResource	Solução de problemas	Leitura/escrita
Salve segredos SSM (token ECR, credenciais CIFS, chaves de contas de serviço de locação) de forma segura	ssm: GetParameter	Implantação	Leitura/escrita
	ssm: PutParameter	Implantação	Leitura/escrita
Envie os logs do mecanismo de IA para o grupo de logs do Amazon CloudWatch durante as operações de implantação e reconstrução	Logs:CreateLogGroup	Implantação	Leitura/escrita
	Logs:PutRetentationPolicy	Implantação	Leitura/escrita
Envie os logs do mecanismo de IA para o grupo de logs do Amazon CloudWatch	Logs:TagResource	Solução de problemas	Leitura/escrita
Obtenha resposta SSM do Amazon CloudWatch (quando a resposta for muito longa)	Logs:DescribeLogStreams	Solução de problemas	Leitura/escrita
Obtenha a resposta SSM do Amazon CloudWatch	Logs:GetLogEvents	Solução de problemas	Leitura/escrita
Crie um grupo de log do Amazon CloudWatch para logs do Amazon bedrock durante a criação da pilha durante as operações de implantação e reconstrução	Logs:CreateLogGroup	Implantação	Leitura/escrita
	Logs:PutRetentationPolicy	Implantação	Leitura/escrita
	Logs:TagResource	Implantação	Leitura/escrita
Listar perfis de inferência para o modelo	Bedrock:ListInferenceProfiles	Solução de problemas	Leitura/escrita

Permissões para cargas de trabalho VMware

As cargas de trabalho do VMware oferecem as seguintes políticas de permissão para escolha:

- **Visualização, planejamento e análise**: Visualize o inventário de ambientes de virtualização da EVS, obtenha uma análise bem arquitetada para seus sistemas e explore oportunidades de economia.
- **Implantação e conectividade do armazenamento de dados**: Implante os layouts de VM recomendados em clusters Amazon EVS, Amazon EC2 ou VMware Cloud on AWS vSphere e use sistemas de arquivos Amazon FSx for NetApp ONTAP como armazenamentos de dados externos.

Selecione a política de permissões para visualizar as políticas IAM necessárias:

Políticas do IAM para workloads da VMware

Visualização, planejamento e análise

```
{
  "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": "*"
    }
  ]
}
```

Implantação e conectividade do armazenamento de dados

```
{
  "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": "*"
    }
  ]
}
```

A tabela a seguir fornece detalhes sobre as permissões para cargas de trabalho VMware.

Tabela de permissões para workloads da VMware

Finalidade	Ação	Onde usado	Política de permissão
Anexe grupos de segurança e modifique regras para os nós provisionados	EC2:AutorizeSecurityGroupIngress	Implantação	Implantação e conectividade do armazenamento de dados
Criar volumes EBS	fsx:Createvolume	Implantação	Implantação e conectividade do armazenamento de dados
Marque valores personalizados para os recursos do FSX for NetApp ONTAP criados pelas cargas de trabalho da VMware	fsx:TagResource	Implantação	Implantação e conectividade do armazenamento de dados
Crie e valide o modelo do CloudFormation	Formação de nuvens: CreateStack	Implantação	Implantação e conectividade do armazenamento de dados
Gerencie tags e segurança de rede em instâncias criadas	EC2:CreateSecurityGroup	Implantação	Implantação e conectividade do armazenamento de dados
Inicie as instâncias criadas	EC2:RunInstances	Implantação	Implantação e conectividade do armazenamento de dados
Obtenha detalhes da instância do EC2	EC2: DescribeInstances	Inventário	Implantação e conectividade do armazenamento de dados
Listar imagens durante a criação da pilha durante as operações de implantação e reconstrução	EC2: DescribeImages	Inventário	Implantação e conectividade do armazenamento de dados
Visualizar detalhes de configuração dos conjuntos de opções DHCP associados às VPCs	ec2:DescribeDhcpOptions	Inventário	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Obtenha os VPCs no ambiente selecionado para preencher o formulário de implantação	EC2: DescribeVPCs	• Implantação • Inventário	Visualização, planejamento e análise
Obtenha as sub-redes no ambiente selecionado para preencher o formulário de implantação	EC2: DescribeSubnets	• Implantação • Inventário	Visualização, planejamento e análise
Obtenha os grupos de segurança no ambiente selecionado para preencher o formulário de implantação	EC2:DescribeSecurityGroups	Implantação	Visualização, planejamento e análise
Obtenha as zonas de disponibilidade no ambiente selecionado	EC2:DescribeDisabilityZones	• Implantação • Inventário	Visualização, planejamento e análise
Obtenha as regiões com o suporte do Amazon FSX para NetApp ONTAP	EC2:DescribeRegiões	Implantação	Visualização, planejamento e análise
Obtenha aliases de chaves KMS para serem usadas para criptografia do Amazon FSX para NetApp ONTAP	Kms:ListAliases	Implantação	Visualização, planejamento e análise
Obtenha chaves KMS para serem usadas para criptografia do Amazon FSX for NetApp ONTAP	Kms: ListKeys	Implantação	Visualização, planejamento e análise
Obtenha os detalhes de expiração das chaves KMS a serem usados para a criptografia do Amazon FSX for NetApp ONTAP	Kms:DescribeKey	Implantação	Visualização, planejamento e análise
Listar segredos no AWS Secrets Manager	gerenciador de segredos:ListarSegredos	Inventário	Visualização, planejamento e análise
Obtenha uma lista de ambientes do Amazon EVS.	evs:ListarAmbientes	Inventário	Visualização, planejamento e análise
Obtenha informações detalhadas sobre um ambiente específico do Amazon EVS.	evs:ObterAmbiente	Inventário	Visualização, planejamento e análise
Liste as VLANs associadas a um ambiente Amazon EVS.	evs:ListarVlansDeAmbiente	Inventário	Visualização, planejamento e análise

Finalidade	Ação	Onde usado	Política de permissão
Crie os recursos do Amazon FSX for NetApp ONTAP necessários para o provisionamento	fsx:CreateFileSystem	Implantação	Implantação e conectividade do armazenamento de dados
	fsx:CreateStorageVirtualMachine	Implantação	Implantação e conectividade do armazenamento de dados
	fsx:Createvolume	• Implantação • Operações de gerenciamento	Implantação e conectividade do armazenamento de dados
Obtenha detalhes do Amazon FSX para NetApp ONTAP	fsx:descrever*	• Implantação • Inventário • Operações de gerenciamento • Explore as poupanças	Implantação e conectividade do armazenamento de dados

Finalidade	Ação	Onde usado	Política de permissão
Obtenha detalhes das chaves do KMS e use a criptografia do Amazon FSX for NetApp ONTAP	Kms:CreateGrant	Implantação	Implantação e conectividade do armazenamento de dados
	Kms: Descrever*	Implantação	Visualização, planejamento e análise
	Kms:Lista*	Implantação	Visualização, planejamento e análise
	Kms:desencriptar	Implantação	Implantação e conectividade do armazenamento de dados
	Kms:GenerateDataKey	Implantação	Implantação e conectividade do armazenamento de dados
Liste os tópicos do SNS do cliente e publique no SNS de back-end do WLMVMC, bem como no SNS do cliente, se selecionado	sns:publicar	Implantação	Implantação e conectividade do armazenamento de dados
Simule operações de carga de trabalho para validar permissões disponíveis e compare com as permissões de conta da AWS necessárias	IAM:SimulatePrincipalPolicy	Implantação	• Implantação e conectividade do armazenamento de dados • Visualização, planejamento e análise

Alterar registo

À medida que as permissões são adicionadas e removidas, vamos anotá-las nas seções abaixo.

1 de fevereiro de 2025

As seguintes permissões foram adicionadas à carga de trabalho de armazenamento:

- `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`

04 de dezembro de 2025

As seguintes permissões foram adicionadas à carga de trabalho de armazenamento:

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

27 de novembro de 2025

As seguintes permissões foram adicionadas à carga de trabalho de armazenamento:

- `bedrock:ListInferenceProfiles`
- `bedrock:GetInferenceProfile`

- `bedrock:InvokeModelWithResponseStream`
- `bedrock:InvokeModel`

2 de novembro de 2025

As políticas de permissão "somente leitura" e "leitura/gravação" foram substituídas em cargas de trabalho de armazenamento, banco de dados e VMware para fornecer mais granularidade e flexibilidade na atribuição de permissões.

5 de outubro de 2025

As seguintes permissões foram removidas do GenAI e agora são gerenciadas pelo mecanismo GenAI:

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

29 de junho de 2025

A seguinte permissão agora está disponível no modo *somente leitura* para bancos de dados: `cloudwatch:GetMetricData` .

3 de junho de 2025

A seguinte permissão agora está disponível no modo *leitura/gravação* para GenAI: `s3:ListAllMyBuckets` .

4 de maio de 2025

A seguinte permissão agora está disponível no modo *leitura/gravação* para GenAI: `qbusiness:ListApplications` .

As seguintes permissões agora estão disponíveis no modo *somente leitura* para bancos de dados:

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

A seguinte permissão agora está disponível no modo *leitura/gravação* para bancos de dados: `logs:PutRetentionPolicy` .

2 de abril de 2025

A seguinte permissão agora está disponível no modo *somente leitura* para bancos de dados: `ssm:DescribeInstanceInformation` .

30 de março de 2025

Atualização das permissões de workload do GenAI

As seguintes permissões agora estão disponíveis no *modo de leitura/gravação* para GenAI:

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

A seguinte permissão foi removida do *modo de leitura/gravação* para GenAI: `Bedrock:GetFoundationModel`.

IAM:SimulatePrincipalPolicy permission update

O `iam:SimulatePrincipalPolicy` a permissão faz parte de todas as políticas de permissão de carga de trabalho se você habilitar a verificação automática de permissões ao adicionar credenciais de conta adicionais da AWS ou adicionar um novo recurso de carga de trabalho no console do Workload Factory. A permissão simula operações de carga de trabalho e verifica se você tem as permissões de conta da AWS necessárias antes de implantar recursos do Workload Factory. Habilitar essa verificação reduz o tempo e o esforço que você pode precisar para limpar recursos de operações com falha e adicionar permissões ausentes.

2 de março de 2025

A seguinte permissão agora está disponível no modo *leitura/gravação* para GenAI: `bedrock:GetFoundationModel`.

3 de fevereiro de 2025

A seguinte permissão agora está disponível no modo *somente leitura* para bancos de dados: `iam:SimulatePrincipalPolicy`.

Informações sobre direitos autorais

Informações sobre marcas comerciais