# Los geht's

## Setup and administration

NetApp
February 02, 2026

# Inhalt

# Los geht’s

## Lernen Sie die Grundlagen kennen

### Erfahren Sie mehr über NetApp Workload Factory

NetApp Workload Factory ist eine leistungsstarke Lebenszyklus-Management-Plattform, die Ihnen dabei hilft, Ihre Workloads mithilfe von Amazon FSx for NetApp ONTAP -Dateisysteme zu optimieren. Zu den Workloads, die mit Workload Factory und FSx für ONTAP optimiert werden können, gehören Datenbanken, VMware-Migrationen zu VMware Cloud auf AWS, KI-Chatbots und mehr.

Eine *Arbeitslast* umfasst eine Kombination aus Ressourcen, Code und Diensten oder Anwendungen, die darauf ausgelegt sind, ein Geschäftsziel zu erreichen. Dies kann alles Mögliche sein, von einer kundenorientierten Anwendung bis hin zu einem Backend-Prozess. Workloads können sich auf eine Teilmenge der Ressourcen innerhalb eines einzelnen AWS-Kontos beziehen oder sich über mehrere Konten erstrecken.

Amazon FSx for NetApp ONTAP bietet vollständig verwaltete, AWS-native NFS-, SMB/CIFS- und iSCSI-Speichervolumes für unternehmenskritische Anwendungen, Datenbanken, Container, VMware Cloud-Datenspeicher und Benutzerdateien. Sie können FSx für ONTAP über Workload Factory und mithilfe nativer AWS-Verwaltungstools verwalten.

#### Funktionen

Die Workload Factory-Plattform bietet die folgenden Hauptfunktionen.

**Flexibler und kostengünstiger Storage**

Erkennung, Implementierung und Management von Amazon FSX für NetApp ONTAP-Filesystemen in der Cloud FSX for ONTAP bringt alle Funktionen von ONTAP in einen nativen AWS Managed Service ein und bietet so eine konsistente Nutzung der Hybrid Cloud.

**Migrieren Sie lokale vSphere Umgebungen zu VMware Cloud on AWS**

Mit dem Migrationsberater von VMware Cloud on AWS können Sie Ihre aktuellen Konfigurationen von Virtual Machines in lokalen vSphere-Umgebungen analysieren, einen Plan zur Implementierung empfohlener VM-Layouts in VMware Cloud on AWS erstellen und die benutzerdefinierten Amazon FSX for NetApp ONTAP-Filesysteme als externe Datastores verwenden.

**Lifecycle Management der Datenbank**

Entdecken Sie Datenbank-Workloads und analysieren Sie Kosteneinsparungen mit Amazon FSX for NetApp ONTAP, nutzen Sie Storage- und Applikationsvorteile bei der Migration von SQL Server-Datenbanken auf FSX für ONTAP Storage, implementieren Sie SQL Server, Datenbanken und Datenbankklone, die Best Practices von Anbietern implementieren, nutzen Sie eine Infrastruktur als Code-Pilotprojekt zur Automatisierung von Abläufen und überwachen und optimieren Sie SQL Server-Bestände kontinuierlich, um Performance, Verfügbarkeit, Schutz und Kosteneffizienz zu verbessern.

**KI-Chatbot-Entwicklung**

Nutzen Sie Ihre FSX für ONTAP-Dateisysteme zum Speichern Ihrer Unternehmen Chatbot-Quellen und die KI-Engine-Datenbanken. Auf diese Weise können Sie die unstrukturierten Daten Ihres Unternehmens in eine Chatbot-Anwendung des Unternehmens einbetten.

### Einsparungsrechner, um Kosten zu sparen

Analysieren Sie Ihre aktuellen Implementierungen, die Amazon Elastic Block Store (EBS) oder Elastic File System (EFS) Storage oder Amazon FSX für Windows File Server verwenden, um zu erfahren, wie viel Geld Sie durch einen Wechsel zu Amazon FSX für NetApp ONTAP sparen können. Mit dem Rechner können Sie auch ein Was-wäre-wenn-Szenario für eine zukünftige Bereitstellung, die Sie planen, ausführen.

### Service-Konten zur Förderung der Automatisierung

Verwenden Sie Servicekonten, um NetApp Workload Factory-Vorgänge sicher und zuverlässig zu automatisieren. Servicekonten bieten eine zuverlässige, dauerhafte Automatisierung ohne Einschränkungen bei der Benutzerverwaltung und sind sicherer, da sie nur API-Zugriff bieten.

### Ask Me KI-Assistent

Stellen Sie dem KI-Assistenten Fragen zur Verwaltung und zum Betrieb von FSx für ONTAP Dateisystemen. Mithilfe des Model Context Protocol (MCP) stellt Ask Me eine sichere Schnittstelle zu externen Umgebungen her und fragt API-Tools ab, um Antworten zu liefern, die auf Ihre spezifische Speicherumgebung zugeschnitten sind.

## Unterstützte Cloud-Provider

Mit Workload Factory können Sie Cloud-Speicher verwalten und Workload-Funktionen in Amazon Web Services nutzen.

## Sicherheit

Sicherheit hat für NetApp NetApp Workload Factory höchste Priorität. Alle Workloads in Workload Factory laufen auf Amazon FSx for NetApp ONTAP. Zusätzlich zu allen "AWS-Sicherheitsfunktionen"NetApp Workload Factory hat erhalten "SOC2 Typ 1-Konformität, SOC2 Typ 2-Konformität und HIPAA-Konformität"Die

Amazon FSx for NetApp ONTAP für NetApp Workload Factory ist ein"AWS-Lösung zum Bereitstellen von Unternehmens-Apps" das unter Berücksichtigung bewährter Vorgehensweisen erstellt wurde.

## Kosten

Die Nutzung von Workload Factory ist kostenlos. Die Kosten, die Sie an Amazon Web Services (AWS) zahlen, hängen von den Speicher- und Workload-Diensten ab, die Sie bereitstellen möchten. Dies beinhaltet die Kosten für Amazon FSx for NetApp ONTAP Dateisysteme, VMware Cloud auf AWS-Infrastruktur, AWS-Dienste und mehr.

## Funktionsweise von Workload Factory

Workload Factory umfasst eine webbasierte Konsole, die über die SaaS-Schicht bereitgestellt wird, ein Konto, Betriebsmodi, die den Zugriff auf Ihre Cloud-Umgebung steuern, Links, die eine getrennte Konnektivität zwischen Workload Factory und einem AWS-Konto bereitstellen, und mehr.

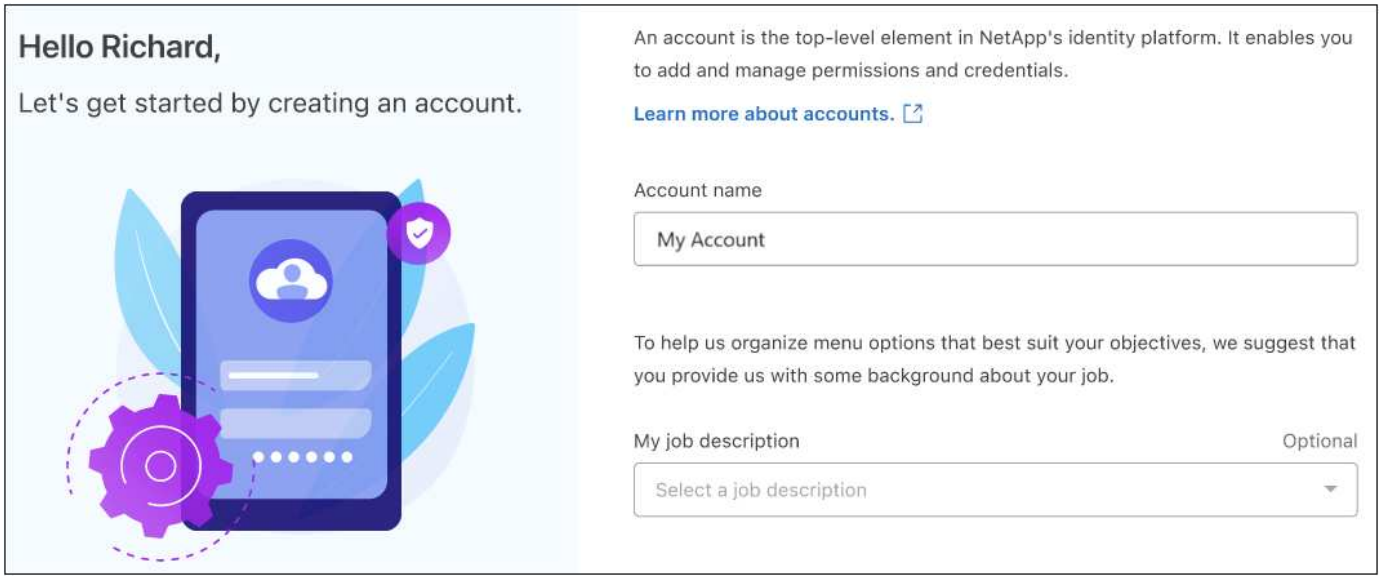
#### Software-as-a-Service

Der Zugriff auf Workload Factory erfolgt über die"NetApp Workload Factory-Konsole" und die"NetApp Konsole" . Diese SaaS-Erfahrungen ermöglichen Ihnen den automatischen Zugriff auf die neuesten Funktionen, sobald diese veröffentlicht werden, und das einfache Wechseln zwischen Ihren Workload Factory-Konten und -Links.

"Erfahren Sie mehr über die verschiedenen Konsolenerlebnisse."

#### Konten

Wenn Sie sich zum ersten Mal bei Workload Factory anmelden, werden Sie aufgefordert, ein Konto zu erstellen. Mit diesem Konto können Sie Ihre Ressourcen, Workloads und den Workload-Zugriff für Ihre Organisation mithilfe von Anmeldeinformationen organisieren.




Wenn Sie ein Konto erstellen, sind Sie der einzige *Account admin* Benutzer für dieses Konto.

Wenn Ihr Unternehmen zusätzliche Konto- oder Benutzerverwaltung benötigt, wenden Sie sich über den Produktchat an uns.

Wenn Sie die NetApp Konsole verwenden, gehören Sie bereits einem Konto an, da Workload Factory NetApp -Konten nutzt.

### Servicekonten

Ein Servicekonto fungiert als „Benutzer“, der zu Automatisierungszwecken autorisierte API-Aufrufe an NetApp Workload Factory tätigen kann. Dies erleichtert die Verwaltung der Automatisierung, da Sie keine Automatisierungsskripte basierend auf dem Benutzerkonto einer realen Person erstellen müssen, die das Unternehmen jederzeit verlassen kann. Alle Kontoinhaber in Workload Factory gelten als Kontoadministratoren. Kontoadministratoren können mehrere Dienstkonten erstellen und löschen.

"Erfahren Sie, wie Sie Servicekonten verwalten"

#### Berechtigungen

Workload Factory bietet flexible Berechtigungsrichtlinien, mit denen Sie den Zugriff auf Ihre Cloud-Umgebung präzise steuern und Workload Factory basierend auf Ihren IT-Richtlinien schrittweise Vertrauen zuweisen können.

"Erfahren Sie mehr über die Berechtigungsrichtlinien von Workload Factory."

#### Verbindungsverbindungen

Ein Workload Factory-Link erstellt eine Vertrauensbeziehung und Konnektivität zwischen Workload Factory und einem oder mehreren FSx for ONTAP Dateisystemen. Auf diese Weise können Sie bestimmte Dateisystemfunktionen direkt über die ONTAP REST-API-Aufrufe überwachen und verwalten, die über die

Amazon FSx for ONTAP -API nicht verfügbar sind.

Sie benötigen keinen Link, um mit Workload Factory zu beginnen, aber in einigen Fällen müssen Sie einen Link erstellen, um alle Funktionen und Workload-Funktionen von Workload Factory freizuschalten.

Links nutzen derzeit AWS Lambda.

"Weitere Informationen zu Links"

#### Codebox-Automatisierung

Codebox ist ein Co-Pilot für Infrastructure as Code (IaC), der Entwicklern und DevOps-Ingenieuren dabei hilft, den Code zu generieren, der zum Ausführen aller von Workload Factory unterstützten Vorgänge erforderlich ist. Zu den Codeformaten gehören Workload Factory REST API, AWS CLI und AWS CloudFormation.

Codebox ist auf die Betriebsmodi der Workload Factory (*basic*, *read-only* und *read/write*) abgestimmt und legt einen klaren Pfad für die Ausführungsbereitschaft sowie einen Automatisierungskatalog für die schnelle zukünftige Wiederverwendung fest.

Im Codebox-Fenster wird die IAC angezeigt, die von einem bestimmten Job-Flow-Vorgang generiert wird und von einem grafischen Assistenten oder einer Konversations-Chat-Schnittstelle abgeglichen wird. Codebox unterstützt Farbcodierung und Suche für eine einfache Navigation und Analyse, aber es ist nicht erlaubt zu bearbeiten. Sie können nur im Automatisierungskatalog kopieren oder speichern.

"Erfahren Sie mehr über Codebox"

#### Einsparungsrechner

Workload Factory bietet Kostenrechner, mit denen Sie die Kosten Ihrer Speicherumgebungen, Datenbanken oder VMware-Workloads auf FSx for ONTAP -Dateisystemen mit anderen Amazon-Diensten vergleichen können. Je nach Ihren Speicheranforderungen könnten Sie feststellen, dass FSx für ONTAP -Dateisysteme die kostengünstigste Option für Sie darstellen.

- "Erfahren Sie, wie Sie die Einsparungen in Ihren Storage-Umgebungen untersuchen können"
- "Erfahren Sie, welche Einsparungen Sie für Ihre Datenbank-Workloads erzielen können"
- "Erfahren Sie, wie Sie bei Ihren VMware-Workloads Einsparungen erzielen können."

#### Gut strukturierte Arbeitslasten

Workload Factory unterstützt Sie bei der Wartung und dem Betrieb zuverlässiger, sicherer, effizienter und kostengünstiger Speicher- und Datenbankkonfigurationen, die mit dem AWS Well-Architected Framework übereinstimmen. Workload Factory scannt FSx täglich nach ONTAP -Dateisystemen, SQL Server- und Oracle-Datenbankbereitstellungen, um Einblicke in potenzielle Fehlkonfigurationen zu gewinnen und entweder manuelle oder automatisierte Maßnahmen zur Behebung von Problemen zu empfehlen.

"Erfahren Sie mehr über gut strukturierte Workloads."

### Tools zur Verwendung von NetApp Workload Factory

Sie können NetApp Workload Factory mit den folgenden Tools verwenden:

- **Workload Factory-Konsole**: Die Workload Factory-Konsole bietet eine visuelle, ganzheitliche Ansicht Ihrer Anwendungen und Projekte.
- * NetApp Konsole*: Die NetApp Konsole bietet eine hybride Benutzeroberfläche, sodass Sie Workload

Factory zusammen mit anderen NetApp -Datendiensten verwenden können.

- **Fragen Sie mich**: Verwenden Sie den KI-Assistenten „Fragen Sie mich“, um Fragen zu stellen und mehr über Workload Factory zu erfahren, ohne die Workload Factory-Konsole zu verlassen. Greifen Sie über das Hilfemenü von Workload Factory auf „Fragen Sie mich“ zu.
- **CloudShell CLI**: Workload Factory enthält eine CloudShell CLI zum Verwalten und Betreiben von AWS- und NetApp -Umgebungen über Konten hinweg von einer einzigen, browserbasierten CLI aus. Greifen Sie über die obere Leiste der Workload Factory-Konsole auf CloudShell zu.
- **REST-API**: Verwenden Sie die Workload Factory REST-APIs, um Ihre FSx für ONTAP Dateisysteme und andere AWS-Ressourcen bereitzustellen und zu verwalten.
- **CloudFormation**: Verwenden Sie AWS CloudFormation-Code, um die Aktionen auszuführen, die Sie in der Workload Factory-Konsole definiert haben, um AWS- und Drittanbieterressourcen aus dem CloudFormation-Stack in Ihrem AWS-Konto zu modellieren, bereitzustellen und zu verwalten.
- **Terraform NetApp Workload Factory-Anbieter**: Verwenden Sie Terraform, um in der Workload Factory-Konsole generierte Infrastruktur-Workflows zu erstellen und zu verwalten.

#### Rest-APIs

Mit Workload Factory können Sie Ihre FSx for ONTAP -Dateisysteme für bestimmte Workloads optimieren, automatisieren und betreiben. Jede Arbeitslast stellt eine zugehörige REST-API bereit. Zusammen bilden diese Workloads und APIs eine flexible und erweiterbare Entwicklungsplattform, die Sie zur Verwaltung Ihrer FSx for ONTAP Dateisysteme verwenden können.

Die Verwendung der Workload Factory REST-APIs bietet mehrere Vorteile:

- Die APIs wurden auf der Grundlage von REST-Technologie und aktuellen Best Practices entwickelt. Zu den Kerntechnologien gehören HTTP und JSON.
- Die Workload Factory-Authentifizierung basiert auf dem OAuth2-Standard. NetApp verlässt sich auf die Implementierung des Auth0-Dienstes.
- Die webbasierte Konsole von Workload Factory verwendet dieselben zentralen REST-APIs, sodass zwischen den beiden Zugriffspfaden Konsistenz besteht.

"Dokumentation zur Workload Factory REST-API anzeigen"

## Konsolenerfahrungen

Auf NetApp Workload Factory kann über zwei webbasierte Konsolen zugegriffen werden. Erfahren Sie, wie Sie über die Workload Factory-Konsole und die NetApp -Konsole auf Workload Factory zugreifen.

- * NetApp Konsole*: Bietet eine Hybriderfahrung, bei der Sie Ihre FSx für ONTAP -Dateisysteme und Workloads, die auf Amazon FSx for NetApp ONTAP ausgeführt werden, am selben Ort verwalten können.
- **Workload Factory-Konsole**: Bietet eine dedizierte Workload Factory-Erfahrung mit Schwerpunkt auf Workloads, die auf Amazon FSx for NetApp ONTAP ausgeführt werden.

#### Zugriff auf Workload Factory in der NetApp -Konsole

Sie können über die NetApp Console auf Workload Factory zugreifen. Zusätzlich zur Nutzung von Workload Factory für AWS-Speicher- und Workload-Funktionen können Sie auch auf andere Datendienste wie NetApp Copy and Sync und mehr zugreifen.

**Schritte**

1. Melden Sie sich an bei"NetApp Konsole" .
2. Wählen Sie im NetApp -Konsolenmenü **Workloads** und dann **Übersicht** aus.

#### Greifen Sie in der Workload Factory-Konsole auf Workload Factory zu

Sie können über die Workload Factory-Konsole auf Workload Factory zugreifen.

**Schritt**

1. Melden Sie sich an bei"Workload Factory-Konsole" .

## Berechtigungen für NetApp Workload Factory

Um die Funktionen und Dienste von NetApp Workload Factory nutzen zu können, müssen Sie Berechtigungen erteilen, damit Workload Factory Vorgänge in Ihrer Cloud-Umgebung ausführen kann.

#### Warum Berechtigungen verwenden

Wenn Sie Berechtigungen erteilen, ordnet Workload Factory der Instanz eine Richtlinie mit Berechtigungen zur Verwaltung von Ressourcen und Prozessen innerhalb dieses AWS-Kontos zu. Dies ermöglicht es Workload Factory, verschiedene Operationen auszuführen, von der Erkennung Ihrer Speicherumgebungen bis hin zur Bereitstellung von AWS-Ressourcen wie Dateisystemen im Speichermanagement oder Wissensdatenbanken für GenAI-Workloads.

Wenn Workload Factory beispielsweise bei Datenbank-Workloads über die erforderlichen Berechtigungen verfügt, scannt es alle EC2-Instanzen in einem bestimmten Konto und einer bestimmten Region und filtert alle Windows-basierten Maschinen. Wenn der AWS Systems Manager (SSM)-Agent installiert ist und auf dem Host ausgeführt wird und das System Manager-Netzwerk ordnungsgemäß konfiguriert ist, kann Workload Factory auf die Windows-Maschine zugreifen und überprüfen, ob die SQL Server-Software installiert ist oder nicht.

#### Berechtigungen nach Workload

Jede Arbeitslast verwendet Berechtigungen, um bestimmte Aufgaben in Workload Factory auszuführen. Berechtigungen werden in festgelegten Berechtigungsrichtlinien gebündelt. Scrollen Sie zu der von Ihnen verwendeten Arbeitslast, um mehr über die Berechtigungsrichtlinien, kopierbares JSON für die Berechtigungsrichtlinien und eine Tabelle zu erfahren, die alle Berechtigungen, ihren Zweck, ihre Verwendung und die sie unterstützenden Berechtigungsrichtlinien auflistet.

##### Berechtigungen für Speicher

Die für Storage verfügbaren IAM-Richtlinien bieten die Berechtigungen, die Workload Factory benötigt, um Ressourcen und Prozesse in Ihrer öffentlichen Cloud-Umgebung zu verwalten.

Für den Speicher stehen folgende Berechtigungsrichtlinien zur Auswahl:

- **Ansicht, Planung und Analyse**: Sehen Sie sich FSx for ONTAP -Dateisysteme an, erfahren Sie mehr über den Systemzustand, erhalten Sie eine fundierte Analyse Ihrer Systeme und entdecken Sie Einsparmöglichkeiten.
- **Betrieb und Fehlerbehebung**: Führen Sie operative Aufgaben durch, wie z. B. die Anpassung der Dateisystemkapazität und die Behebung von Problemen in Ihren Dateisystemkonfigurationen.
- **Dateisystemerstellung und -löschung**: Erstellen und Löschen von FSx-Dateisystemen und Speicher-

VMs für ONTAP .

Die erforderlichen IAM-Richtlinien anzeigen:

## IAM-Richtlinien für Storage

**Ansicht, Planung und Analyse**

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

**Betriebs- und Sanierungsmaßnahmen**

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

**Dateisystemerstellung und -löschung**

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

In der folgenden Tabelle werden die Berechtigungen für Speicher angezeigt.

**Berechtigungstabelle für Speicher**

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Erstellen Sie ein FSX für ONTAP-Dateisystem | fsx:CreateFileSystem | Einsatz | Dateisystemerstellung und -löschung |
| Erstellen Sie eine Sicherheitsgruppe für ein FSX für ONTAP-Dateisystem | ec2:CreateSecurityGroup | Einsatz | Dateisystemerstellung und -löschung |
| Fügen Sie Tags zu einer Sicherheitsgruppe für ein FSX für ONTAP-Dateisystem hinzu | ec2:CreateTags | Einsatz | Dateisystemerstellung und -löschung |
| Ausgang und Zugang der Sicherheitsgruppe für ein FSX für ONTAP Filesystem autorisieren | ec2:AuthoriseSecurityGroupEgress | Einsatz | Dateisystemerstellung und -löschung |
| | ec2:AuthoriseSecurityGroupIngress | Einsatz | Dateisystemerstellung und -löschung |
| Die gewährte Rolle bietet die Kommunikation zwischen FSX für ONTAP und anderen AWS-Services | iam:CreateServiceLinkedRole | Einsatz | Dateisystemerstellung und -löschung |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Hier erhalten Sie Informationen zum Ausfüllen des Formulars FSX für die Bereitstellung des Dateisystems für ONTAP | ec2:DescribeVpcs | • Einsatz<br>• Einsparungen entdecken | Dateisystemerstellung und -löschung |
| | ec2:DescribeSubnets | • Einsatz<br>• Einsparungen entdecken | Dateisystemerstellung und -löschung |
| | ec2:DescribeSecurityGroups | • Einsatz<br>• Einsparungen entdecken | Dateisystemerstellung und -löschung |
| | ec2:DescribeRouteTables | • Einsatz<br>• Einsparungen entdecken | Dateisystemerstellung und -löschung |
| | ec2:DescribeNetworkInterfaces | • Einsatz<br>• Einsparungen entdecken | Dateisystemerstellung und -löschung |
| | ec2:DescribeVolumeStatus | • Einsatz<br>• Einsparungen entdecken | Dateisystemerstellung und -löschung |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| KMS-Schlüsseldetails erhalten und FSX für ONTAP-Verschlüsselung verwenden | Km:CreateGrant | Einsatz | Dateisystemerstellung und -löschung |
| | Kms:DescribeKey | Einsatz | Dateisystemerstellung und -löschung |
| | Kms:Listenschlüssel | Einsatz | Dateisystemerstellung und -löschung |
| | Km:ListAliase | Einsatz | Dateisystemerstellung und -löschung |
| Abrufen von Volume-Details für EC2-Instanzen | ec2:DescribeVolumes | • Inventar<br>• Einsparungen entdecken | Ansicht, Planung und Analyse |
| Informieren Sie sich über Details für EC2 Instanzen | ec2:DescribeInstances | Einsparungen entdecken | Ansicht, Planung und Analyse |
| Elastic File System im Einsparungsrechner beschreiben | Elasticfilesystem:DescribeFileSystems | Einsparungen entdecken | Ansicht, Planung und Analyse |
| Listen Sie Tags für FSX for ONTAP-Ressourcen auf | fsx:ListTagsForRessource | Inventar | Ansicht, Planung und Analyse |
| Ausgang und Ingress der Sicherheitsgruppe für ein FSX für ONTAP Filesystem managen | ec2:RevokeSecurityGroupIngress | Managementvorgänge | Dateisystemerstellung und -löschung |
| | ec2: RevokeSecurityGroupEgress | Managementvorgänge | Dateisystemerstellung und -löschung |
| | ec2:DeleteSecurityGroup | Managementvorgänge | Dateisystemerstellung und -löschung |

| Zweck | Aktion | Wo verwendet | Berechtigungs richtlinie |
| --- | --- | --- | --- |
| Erstellen, Anzeigen und Verwalten von FSX for ONTAP-Dateisystemressourcen | | | |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
| --- | --- | --- | --- |
| | fsx:UntagResource | Managementvorgänge | Betriebs- und Sanierungsmaßnahmen |
| | fsx:DescribeBackups | Managementvorgänge | Ansicht, Planung und Analyse |
| | fsx:CreateBackup | Managementvorgänge | Betriebs- und Sanierungsmaßnahmen |
| | fsx:CreateVolumeFromBackup | Managementvorgänge | Betriebs- und Sanierungsmaßnahmen |
| | fsx:Backup löschen | Managementvorgänge | Betriebs- und Sanierungsmaßnahmen |
| Abrufen von Kennzahlen zu Dateisystem und Volume | cloudwatch:GetMetricData | Managementvorgänge | Ansicht, Planung und Analyse |
| | cloudwatch:GetMetricStatistics | Managementvorgänge | Ansicht, Planung und Analyse |
| Simulieren Sie Workload-Vorgänge, um verfügbare Berechtigungen zu validieren und sie mit den erforderlichen AWS Kontoberechtigungen zu vergleichen | iam:SimulatePrincipalPolicy | Einsatz | Alle |
| Bereitstellung KI-basierter Erkenntnisse für FSx für ONTAP EMS-Ereignisse | Bedrock:ListInferenceProfiles | FSx für ONTAP EMS-Analyse | Betriebs- und Sanierungsmaßnahmen |
| | bedrock:GetInferenceProfile | FSx für ONTAP EMS-Analyse | Betriebs- und Sanierungsmaßnahmen |
| | bedrock:InvokeModelWihResponseStream | FSx für ONTAP EMS-Analyse | Betriebs- und Sanierungsmaßnahmen |
| | Bedrock:InvokeModel | FSx für ONTAP EMS-Analyse | Betriebs- und Sanierungsmaßnahmen |
| Rufen Sie Kosten- und Nutzungsdaten für FSx for ONTAP -Dateisysteme über den AWS Cost Explorer ab. | ce:GetCostAndUsage | Kosten- und Nutzungsanalyse | Ansicht, Planung und Analyse |
| | ce:GetTags | Kosten- und Nutzungsanalyse | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Erstellen Sie einen S3-Zugriffspunkt und verbinden Sie ihn mit einem FSx for ONTAP Dateisystem | fsx:CreateAndAttachS3AccessPoint | S3-Zugangspunktverwaltung | Betriebs- und Sanierungsmaßnahmen |
| Einen S3-Zugriffspunkt von einem FSx for ONTAP Dateisystem trennen und löschen | fsx:DetachAndDeleteS3AccessPoint | S3-Zugangspunktverwaltung | Betriebs- und Sanierungsmaßnahmen |
| Erstellen Sie einen S3-Zugriffspunkt für eine vereinfachte Bucket-Zugriffsverwaltung | s3:CreateAccessPoint | S3-Zugangspunktverwaltung | Betriebs- und Sanierungsmaßnahmen |
| Löschen eines S3 Access Point | s3:DeleteAccessPoint | S3-Zugangspunktverwaltung | Betriebs- und Sanierungsmaßnahmen |
| Fügen Sie einem S3-Zugriffspunkt Tags hinzu | s3:TagResource | S3-Zugangspunktverwaltung | Betriebs- und Sanierungsmaßnahmen |
| Tags auf einem S3-Zugriffspunkt auflisten und anzeigen | s3:ListTagsForResource | S3-Zugangspunktverwaltung | Betriebs- und Sanierungsmaßnahmen |
| Tags von einem S3-Zugriffspunkt entfernen | s3:UntagResource | S3-Zugangspunktverwaltung | Betriebs- und Sanierungsmaßnahmen |
| Objekte in einem S3 access point Bucket ermitteln | s3:ListBucket | S3-Bucket-Operationen | Betriebs- und Sanierungsmaßnahmen |
| S3-Tabellen-Buckets auflisten, erstellen und beschreiben | s3tables:ListTableBuckets<br>s3tables:CreateTableBucket<br>s3tables:GetTableBucket | S3-Tabellen-Bucket-Verwaltung | Betriebs- und Sanierungsmaßnahmen |
| S3-Tabellen auflisten, erstellen und abrufen | s3tables:ListTables<br>s3tables:CreateTable<br>s3tables:GetTable | S3-Tabellenoperationen | Betriebs- und Sanierungsmaßnahmen |
| Speicherort der Tabellenmetadaten lesen | s3tables:GetTableMetadataLocation | S3-Tabellenmetadatenoperationen | Betriebs- und Sanierungsmaßnahmen |
| Speicherort der Tabellenmetadaten aktualisieren | s3tables:UpdateTableMetadataLocation | S3-Tabellenmetadatenoperationen | Betriebs- und Sanierungsmaßnahmen |
| Tabellen-Namespaces auflisten, erstellen und abrufen | s3tables:ListNamespaces<br>s3tables:CreateNamespace<br>s3tables:GetNamespace | S3-Namensraumoperationen | Betriebs- und Sanierungsmaßnahmen |
| Tabellendaten lesen (select, scan) | s3tables:GetTableData | S3-Tabellendatenoperationen | Betriebs- und Sanierungsmaßnahmen |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Tabellendaten schreiben (insert) | s3tables:PutTableData | S3-Tabellendatenoperationen | Betriebs- und Sanierungsmaßnahmen |
| Tags in einer Inventartabelle auflisten (FSx for ONTAP, Storage-VM, Volume-IDs abrufen) | s3tables:ListTagsForResource | S3-Tabellen-Tag-Operationen | Betriebs- und Sanierungsmaßnahmen |
| Kennzeichnen Sie eine Inventartabelle für die Workload Factory-Suche | s3tables:TagResource | S3-Tabellen-Tag-Operationen | Betriebs- und Sanierungsmaßnahmen |
| Objekt-Tags über Zugriffspunkt abrufen | s3:GetObjectTagging | S3-Objektoperationen | Betriebs- und Sanierungsmaßnahmen |

#### Berechtigungen für Datenbank-Workloads

Die für Datenbank-Workloads verfügbaren IAM-Richtlinien bieten die Berechtigungen, die Workload Factory benötigt, um Ressourcen und Prozesse in Ihrer öffentlichen Cloud-Umgebung zu verwalten.

Für Datenbanken stehen folgende Berechtigungsrichtlinien zur Auswahl:

- **Ansicht, Planung und Analyse**: Sehen Sie sich das Inventar der Datenbankressourcen an, erfahren Sie mehr über den Zustand Ihrer Ressourcen, überprüfen Sie die gut strukturierte Analyse Ihrer Datenbankkonfigurationen und entdecken Sie Einsparmöglichkeiten, erhalten Sie eine Fehlerprotokollanalyse und entdecken Sie Einsparmöglichkeiten.
- **Betrieb und Fehlerbehebung**: Führen Sie operative Aufgaben für Ihre Datenbankressourcen durch und beheben Sie Probleme mit Datenbankkonfigurationen und dem zugrunde liegenden FSx for ONTAP Dateisystemspeicher.
- **Erstellung von Datenbank-Hosts**: Bereitstellung von Datenbank-Hosts und des zugrunde liegenden FSx for ONTAP Dateisystemspeichers gemäß bewährten Verfahren.

Wählen Sie Ihren Betriebsmodus aus, um die erforderlichen IAM-Richtlinien anzuzeigen:

**Ansicht, Planung und Analyse**

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

**Betriebs- und Sanierungsmaßnahmen**

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

**Erstellung eines Datenbankhosts**

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

In der folgenden Tabelle werden die Berechtigungen für Datenbank-Workloads angezeigt.

**Berechtigungstabelle für Datenbank-Workloads**

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Erhalten Sie Metrikstatistiken für FSx für ONTAP, EBS und FSx für Windows File Server sowie Empfehlungen zur Rechenoptimierung. | cloudwatch:GetMetricStatistics | • Inventar<br>• Einsparungen entdecken | Ansicht, Planung und Analyse |
| Sammeln Sie in Amazon CloudWatch gespeicherte Leistungsmetriken von registrierten SQL-Knoten. Die Daten werden in Leistungstrenddiagrammen auf dem Bildschirm „Instanzverwaltung“ für registrierte SQL-Instanzen generiert. | cloudwatch:GetMetricData | Inventar | Ansicht, Planung und Analyse |
| Informieren Sie sich über Details für EC2 Instanzen | ec2:DescribeInstances | • Inventar<br>• Einsparungen entdecken | Ansicht, Planung und Analyse |
| | ec2:DescribeKeypairs | Einsatz | Ansicht, Planung und Analyse |
| | ec2:DescribeNetworkInterfaces | Einsatz | Ansicht, Planung und Analyse |
| | ec2:DescribeInstanceTypes | • Einsatz<br>• Einsparungen entdecken | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungs richtlinie |
|---|---|---|---|
| Informieren Sie sich, wie Sie das FSX for ONTAP-Implementierungsformular ausfüllen | ec2:DescribeVpcs | • Einsatz<br>• Inventar | Ansicht, Planung und Analyse |
| | ec2:DescribeSubnets | • Einsatz<br>• Inventar | Ansicht, Planung und Analyse |
| | ec2:DescribeSecurityGroups | Einsatz | Ansicht, Planung und Analyse |
| | ec2:DescribeBilder | Einsatz | Ansicht, Planung und Analyse |
| | ec2:DescribeRegionen | Einsatz | Ansicht, Planung und Analyse |
| | ec2:DescribeRouteTables | • Einsatz<br>• Inventar | Ansicht, Planung und Analyse |
| Holen Sie sich alle vorhandenen VPC-Endpunkte, um zu ermitteln, ob neue Endpunkte vor der Implementierung erstellt werden müssen | ec2:DescribeVpcEndpunkte | • Einsatz<br>• Inventar | Ansicht, Planung und Analyse |
| Erstellen Sie VPC-Endpunkte, wenn sie für erforderliche Services unabhängig von der öffentlichen Netzwerkkonnektivität auf EC2-Instanzen nicht vorhanden sind | ec2:CreateVpcEndpoint | Einsatz | Erstellung eines Datenbankhosts |
| Abrufen von Instanztypen in der Region für Validierungsknoten (t2.micro/t3.micro) | ec2:DescribeInstanceTypeOfferings | Einsatz | Ansicht, Planung und Analyse |
| Erhalten Sie Snapshot-Details zu jedem angebundenen EBS Volumes zur Preisgestaltung und Schätzung der Einsparungen | ec2:DescribeSnapshots | Einsparungen entdecken | Ansicht, Planung und Analyse |
| Informieren Sie sich über die einzelnen angebundenen EBS Volumes und erhalten Sie Informationen zu Preisen und einer Schätzung, die Einsparungen schätzt | ec2:DescribeVolumes | • Inventar<br>• Einsparungen entdecken | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungs richtlinie |
|---|---|---|---|
| Erhalten Sie KMS-Schlüsseldetails für FSX für ONTAP-Dateisystemverschlüsselung | Km:ListAliase | Einsatz | Ansicht, Planung und Analyse |
| | Kms:Listenschlüssel | Einsatz | Ansicht, Planung und Analyse |
| | Kms:DescribeKey | Einsatz | Ansicht, Planung und Analyse |
| Holen Sie sich eine Liste der CloudFormation Stacks in der Umgebung, um Quota Limit zu überprüfen | CloudFormation:ListenStacks | Einsatz | Ansicht, Planung und Analyse |
| Überprüfen Sie die Kontenlimits für Ressourcen, bevor Sie die Bereitstellung auslösen | Cloudformation:DescribeAccount Limits | Einsatz | Ansicht, Planung und Analyse |
| Holen Sie sich eine Liste der von AWS gemanagten Active Directories in der Region | ds:DescribeDirectories | Einsatz | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Hier erhalten Sie Listen und Details zu Volumes, Backups, SVMs, Filesystemen in AZS und Tags für das Filesystem FSX for ONTAP | fsx:DescribeVolumes | • Inventar<br>• Einsparungen Entdecken | Ansicht, Planung und Analyse |
| | fsx:DescribeBackups | • Inventar<br>• Einsparungen Entdecken | Ansicht, Planung und Analyse |
| | fsx:DescribeStorageVirtualMachines | • Einsatz<br>• Managementvorgänge<br>• Inventar | Ansicht, Planung und Analyse |
| | fsx:DescribeFileSystems | • Einsatz<br>• Managementvorgänge<br>• Inventar<br>• Einsparungen entdecken | Ansicht, Planung und Analyse |
| | fsx:ListTagsForRessource | Managementvorgänge | Ansicht, Planung und Analyse |
| Servicekontingente für CloudFormation und VPC abrufen / Geheimnisse in einem Benutzerkonto für die für SQL, Domäne und FSx für ONTAP bereitgestellten Anmeldeinformationen erstellen | Service-Equotas:ListServiceQuotas | Einsatz | Ansicht, Planung und Analyse |
| Verwenden Sie SSM-basierte Abfrage, um die aktualisierte Liste von FSX für ONTAP unterstützte Regionen zu erhalten | ssm:GetParametersByPath | Einsatz | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Abfrage der SSM-Antwort nach dem Senden des Befehls für Verwaltungsoperationen nach der Bereitstellung | ssm:GetCommandInvocation | • Managementvorgänge<br>• Inventar<br>• Einsparungen entdecken<br>• Optimierung | Ansicht, Planung und Analyse |
| Senden Sie Befehle über SSM an EC2-Instanzen zur Erkennung und Verwaltung. | ssm:SendCommand | • Managementvorgänge<br>• Inventar<br>• Einsparungen entdecken<br>• Optimierung | Ansicht, Planung und Analyse |
| Ermitteln Sie den SSM-Konnektivitätsstatus der Instanzen nach der Bereitstellung | ssm:GetConnectionStatus | • Managementvorgänge<br>• Inventar<br>• Optimierung | Ansicht, Planung und Analyse |
| Abrufen des SSM-Zuordnungsstatus für eine Gruppe von gemanagten EC2-Instanzen (SQL-Nodes) | ssm:DescribeInstanceInformation | Inventar | Ansicht, Planung und Analyse |
| Liste der verfügbaren Patch-Basispläne für die Bewertung von Patches des Betriebssystems abrufen | ssm:DescribePatchBaselines | Optimierung | Ansicht, Planung und Analyse |
| Ermitteln Sie den Patchstatus auf Windows EC2-Instanzen für die Bewertung von Betriebssystem-Patches | ssm:DescribeInstancePatchStates | Optimierung | Ansicht, Planung und Analyse |
| Führen Sie Befehle auf, die von AWS Patch Manager auf EC2-Instanzen für das Patch-Management des Betriebssystems ausgeführt werden | ssm:ListCommands | Optimierung | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
| --- | --- | --- | --- |
| Prüfen Sie, ob das Konto bei AWS Compute Optimizer registriert ist | compute-Optimizer:GetEnrollmentStatus | • Einsparungen entdecken<br>• Optimierung | Erstellung eines Datenbankhosts |
| Aktualisieren Sie in AWS Compute Optimizer eine vorhandene Empfehlung, um die auf SQL Server-Workloads abgestimmten Empfehlungen zu erhalten | compute-Optimizer:PutRecommendationPreferences | • Einsparungen entdecken<br>• Optimierung | Erstellung eines Datenbankhosts |
| Holen Sie sich die empfohlenen Einstellungen für eine bestimmte Ressource von AWS Compute Optimizer | compute-Optimizer:GetEffectiveEmpfehlungPreferences | • Einsparungen entdecken<br>• Optimierung | Erstellung eines Datenbankhosts |
| Holen Sie sich Empfehlungen ab, die AWS Compute Optimizer für Amazon Elastic Compute Cloud (Amazon EC2) Instanzen generiert | compute-Optimizer:GetEC2InstanceRecommendations | • Einsparungen entdecken<br>• Optimierung | Erstellung eines Datenbankhosts |
| Überprüfen Sie die Zuordnung von Instanzen zu Gruppen mit automatischer Skalierung | Automatische Skalierung:DescribeAutoScalingGroups | • Einsparungen entdecken<br>• Optimierung | Erstellung eines Datenbankhosts |
| | Automatische Skalierung:DescribeAutoScalingInstances | • Einsparungen entdecken<br>• Optimierung | Erstellung eines Datenbankhosts |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Abrufen, Auflisten, Erstellen und Löschen von SSM-Parametern für AD, FSX für ONTAP und SQL-Benutzeranmeldeinformationen, die während der Bereitstellung verwendet oder in Ihrem AWS-Konto verwaltet werden | ssm:GetParameter [1] | • Einsatz<br>• Managementvorgänge<br>• Inventar | Ansicht, Planung und Analyse |
| | ssm:GetParameters [1] | • Einsatz<br>• Managementvorgänge<br>• Inventar | Ansicht, Planung und Analyse |
| | ssm:PutParameter [1] | • Einsatz<br>• Managementvorgänge | Ansicht, Planung und Analyse |
| | ssm:DeleteParameters [1] | • Einsatz<br>• Managementvorgänge | Ansicht, Planung und Analyse |
| Zuordnen von Netzwerkressourcen zu SQL-Knoten und Validierungsknoten und Hinzufügen weiterer sekundärer IPs zu SQL-Knoten | ec2:AllocateAddress [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AllocateHosts [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AssignPrivateIpAddresses [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AssociateAddress [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AssociateRouteTable [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AssociateSubnetCidrBlock [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AssociateVpcCidrBlock [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AttachInternetGateway [1] | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AttachNetworkInterface [1] | Einsatz | Erstellung eines Datenbankhosts |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Verbinden Sie die für die Implementierung erforderlichen EBS Volumes mit den SQL Nodes | ec2:AttachVolume | Einsatz | Erstellung eines Datenbankhosts |
| Weisen Sie bereitgestellten EC2-Instanzen Sicherheitsgruppen zu und ändern Sie Regeln. | ec2:AuthoriseSecurityGroupEgress | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:AuthoriseSecurityGroupIngress | Einsatz | Erstellung eines Datenbankhosts |
| Erstellen Sie EBS Volumes, die den SQL Nodes für die Implementierung benötigt werden | ec2:CreateVolume | Einsatz | Erstellung eines Datenbankhosts |
| Entfernen Sie die temporären Validierungs-Nodes, die vom Typ t2.micro erstellt wurden, und für Rollback oder erneute Versuche ausgefallener EC2 SQL-Nodes | ec2:DeleteNetworkInterface | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DeleteSecurityGroup | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DeleteTags | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DeleteVolume | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DetachNetworkInterface | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DetachVolume | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DisassociateAddress | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DisassociateIamInstanceProfil | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DisassociateRouteTable | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DisassociateSubnetCidrBlock | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:DisassociateVpcCidrBlock | Einsatz | Erstellung eines Datenbankhosts |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Attribute für erstellte SQL-Instanzen ändern. Gilt nur für Namen, die mit WLMDB beginnen. | ec2:ModifyInstanceAttribut | Einsatz | Betriebs- und Sanierungsmaßnahmen |
| | ec2: ModifyInstancePlacement | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:ModifyNetworkInterface Attribute | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:ModifySubnetAttribute | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:ModifyVolume | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:ModifyVolumeAttribute | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:ModifyVpcAttribute | Einsatz | Erstellung eines Datenbankhosts |
| Aufheben und Löschen von Validierungsinstanzen | ec2: ReleaseAddress | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:ReplaceRoute | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:ReplaceRouteTableAssociation | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:RevokeSecurityGroupEgress | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:RevokeSecurityGroupIngress | Einsatz | Erstellung eines Datenbankhosts |
| Starten Sie die bereitgestellten Instanzen | ec2:StartInstances | Einsatz | Betriebs- und Sanierungsmaßnahmen |
| Stoppen Sie die bereitgestellten Instanzen | ec2:StopInstances | Einsatz | Betriebs- und Sanierungsmaßnahmen |
| Markieren Sie benutzerdefinierte Werte für von WLMDB erstellte Amazon FSX for NetApp ONTAP-Ressourcen, um Rechnungsdetails während der Ressourcenverwaltung zu erhalten | fsx:TagResource [1] | • Einsatz<br>• Managementvorgänge | Erstellung eines Datenbankhosts |

| Zweck | Aktion | Wo verwendet | Berechtigungs richtlinie |
|---|---|---|---|
| CloudFormation-Vorlage für die Bereitstellung erstellen und validieren | CloudFormation:CreateStack | Einsatz | Erstellung eines Datenbankhosts |
| | Molkenbildung:DescribeStackEvents | Einsatz | Erstellung eines Datenbankhosts |
| | Wolkenbildung:DescribeStacks | Einsatz | Erstellung eines Datenbankhosts |
| | CloudFormation:ListenStacks | Einsatz | Ansicht, Planung und Analyse |
| | Cloudformation:ValidierteVorlage | Einsatz | Erstellung eines Datenbankhosts |
| Erstellen Sie verschachtelte Stapelvorlagen für den erneuten Versuch und Rollback | ec2:CreateLaunchTemplate | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:CreateLaunchTemplateVersion | Einsatz | Erstellung eines Datenbankhosts |
| Verwalten von Tags und Netzwerksicherheit auf erstellten Instanzen | ec2:CreateNetworkInterface | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:CreateSecurityGroup | Einsatz | Erstellung eines Datenbankhosts |
| | ec2:CreateTags | Einsatz | Erstellung eines Datenbankhosts |
| Abrufen von Instanzdetails für die Bereitstellung | ec2:DescribeAddresses | Einsatz | Ansicht, Planung und Analyse |
| | ec2:DescribeLaunchTemplates | Einsatz | Ansicht, Planung und Analyse |
| Starten Sie die erstellten Instanzen | ec2:RunInstances | Einsatz | Erstellung eines Datenbankhosts |
| Erstellen Sie FSX for ONTAP-Ressourcen, die für die Bereitstellung erforderlich sind. Für bestehende FSX for ONTAP Systeme wird eine neue SVM erstellt, die SQL Volumes hostet. | fsx:CreateFileSystem | Einsatz | Erstellung eines Datenbankhosts |
| | fsx:CreateStorageVirtualMachine | Einsatz | Erstellung eines Datenbankhosts |
| | fsx: CreateVolume erstellen | • Einsatz<br>• Managementvorgänge | Erstellung eines Datenbankhosts |
| FSX for ONTAP – Details | fsx:DescribeFileSystemAliases | Einsatz | Erstellung eines Datenbankhosts |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Ändern der Größe von FSX für ONTAP-Dateisystem, um Reserve des Dateisystems zu beheben | fsx:UpdateFilesystem | Optimierung | Betriebs- und Sanierungsmaßnahmen |
| Ändern Sie die Größe von Volumes zur Korrektur von Protokoll- und tempdb-Laufwerkgrößen | fsx:UpdateVolumen | Optimierung | Betriebs- und Sanierungsmaßnahmen |
| KMS-Schlüsseldetails erhalten und FSX für ONTAP-Verschlüsselung verwenden | Km:CreateGrant | Einsatz | Erstellung eines Datenbankhosts |
| | kms:DescribeCustomKeyStores | Einsatz | Erstellung eines Datenbankhosts |
| | Kms:GenerateDataKey | Einsatz | Erstellung eines Datenbankhosts |
| Erstellen Sie CloudWatch-Protokolle für Validierungs- und Bereitstellungsskripte, die auf EC2-Instanzen ausgeführt werden | Protokolle:CreateLogGroup | Einsatz | Erstellung eines Datenbankhosts |
| | Protokolle:CreateLogStream | Einsatz | Erstellung eines Datenbankhosts |
| | Protokolle:GetLogGroupFields | Einsatz | Erstellung eines Datenbankhosts |
| | Protokolle:GetLogRecord | Einsatz | Erstellung eines Datenbankhosts |
| | Protokolle:ListLogDeliveries | Einsatz | Erstellung eines Datenbankhosts |
| | Protokolle:PutLogEvents | • Einsatz<br>• Managementvorgänge | Erstellung eines Datenbankhosts |
| | Protokolle:TagResource | Einsatz | Erstellung eines Datenbankhosts |
| Workload Factory wechselt zu Amazon CloudWatch-Protokollen für die SQL-Instanz, wenn eine Kürzung der SSM-Ausgabe auftritt | Protokolle:GetLogEvents | • Storage-Bewertung (Optimierung)<br>• Inventar | Ansicht, Planung und Analyse |
| Erlauben Sie Workload Factory, aktuelle Protokollgruppen abzurufen und zu überprüfen, ob die Aufbewahrung für von Workload Factory erstellte Protokollgruppen festgelegt ist | Protokolle:DescribeLogGroups | • Storage-Bewertung (Optimierung)<br>• Inventar | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Erlauben Sie Workload Factory, eine eintägige Aufbewahrungsrichtlinie für von Workload Factory erstellte Protokollgruppen festzulegen, um eine unnötige Ansammlung von Protokollströmen für SSM-Befehlsausgaben zu vermeiden. | Protokolle:PutRetentionPolicy | • Storage-Bewertung (Optimierung)<br>• Inventar | Ansicht, Planung und Analyse |
| Führen Sie die SNS-Themen des Kunden auf und veröffentlichen Sie sie in WLMDB-Backend-SNS sowie in Kunden-SNS, falls ausgewählt | sns:listTopics | Einsatz | Ansicht, Planung und Analyse |
| | sns:Veröffentlichen | Einsatz | Erstellung eines Datenbankhosts |
| Erforderliche SSM-Berechtigungen, um das Erkennungsskript auf bereitgestellten SQL-Instanzen auszuführen und die aktuelle Liste von FSX für von ONTAP unterstützte AWS-Regionen abzurufen. | ssm:PutComplianceItems | Einsatz | Erstellung eines Datenbankhosts |
| | ssm:PutConfigurePackageResult | Einsatz | Erstellung eines Datenbankhosts |
| | ssm:PutInventory | Einsatz | Erstellung eines Datenbankhosts |
| | ssm:UpdateAssociationStatus | Einsatz | Erstellung eines Datenbankhosts |
| | ssm:UpdateInstanceAssociationStatus | Einsatz | Erstellung eines Datenbankhosts |
| | ssm:UpdateInstanceInformation | Einsatz | Erstellung eines Datenbankhosts |
| | ssmmesages:CreateControlChannel | Einsatz | Erstellung eines Datenbankhosts |
| | ssmmesages:CreateDataChannel | Einsatz | Erstellung eines Datenbankhosts |
| | ssmmesages:OpenControlChannel | Einsatz | Erstellung eines Datenbankhosts |
| | ssmmesages:OpenDataChannel | Einsatz | Erstellung eines Datenbankhosts |
| Signal CloudFormation Stack auf Erfolg oder Misserfolg. | Cloudformation:SignalRessource [1] | Einsatz | Erstellung eines Datenbankhosts |
| Fügen Sie die von Vorlage erstellte EC2-Rolle zum Instanzprofil von EC2 hinzu, um Skripts auf EC2 Zugriff auf die für die Implementierung erforderlichen Ressourcen zu ermöglichen. | iam:AddRoleToInstanceProfile | Einsatz | Erstellung eines Datenbankhosts |

| Zweck | Aktion | Wo verwendet | Berechtigungs richtlinie |
|---|---|---|---|
| Instanzprofil für EC2 erstellen und erstellte EC2-Rolle zuweisen. | iam:CreateInstanceProfil | Einsatz | Erstellung eines Datenbankhosts |
| EC2-Rolle über Vorlage mit den unten aufgeführten Berechtigungen erstellen | iam:CreateRollenole | Einsatz | Erstellung eines Datenbankhosts |
| Mit EC2-Service verknüpfte Rolle erstellen | iam:CreateServiceLinkedRole [2] | Einsatz | Erstellung eines Datenbankhosts |
| Löschen Sie das während der Bereitstellung speziell für die Validierungsknoten erstellte Instanzprofil | iam:DeleteInstanceProfil | Einsatz | Erstellung eines Datenbankhosts |
| Rufen Sie die Rollen- und Richtliniendetails ab, um Lücken in der Berechtigung zu ermitteln und die Bereitstellung zu validieren | iam:GetPolicy | Einsatz | Erstellung eines Datenbankhosts |
| | iam:GetPolicyVersion | Einsatz | Erstellung eines Datenbankhosts |
| | iam:GetRole | Einsatz | Erstellung eines Datenbankhosts |
| | iam:GetRolePolicy | Einsatz | Erstellung eines Datenbankhosts |
| | iam:GetUser | Einsatz | Erstellung eines Datenbankhosts |
| Übergeben Sie die erstellte Rolle an EC2-Instanz | iam:PassRole [3] | Einsatz | Erstellung eines Datenbankhosts |
| Fügen Sie der erstellten EC2-Rolle eine Richtlinie mit den erforderlichen Berechtigungen hinzu | iam:PuttePolicy | Einsatz | Erstellung eines Datenbankhosts |
| Trennen der Rolle vom bereitgestellten EC2-Instanzprofil | iam:RemoveRoleFromInstanceProfile | Einsatz | Erstellung eines Datenbankhosts |
| Simulieren Sie Workload-Vorgänge, um verfügbare Berechtigungen zu validieren und sie mit den erforderlichen AWS Kontoberechtigungen zu vergleichen | iam:SimulatePrincipalPolicy | Einsatz | Alle |
| Nutzen Sie die verfügbaren Basismodelle für die Fehlerprotokollanalyse. | Bedrock:GetFoundationModelVerfügbarkeit | Fehlerprotokollanalyse | Ansicht, Planung und Analyse |
| Liste der in Amazon Bedrock verfügbaren Schnittstellenprofile für die Fehlerprotokollanalyse | Bedrock:ListInferenceProfiles | Fehlerprotokollanalyse | Ansicht, Planung und Analyse |

1. Die Berechtigung ist auf Ressourcen beschränkt, die mit WLMDB beginnen.

2. „iam:CreateServiceLinkedRole“ begrenzt durch „iam:AWSServiceName“: „ec2.amazonaws.com"*
3. "iam:PassRole" begrenzt durch "iam:PassedToService": "ec2.amazonaws.com"*

#### Berechtigungen für GenAI-Workloads

Die IAM-Richtlinien für VMware-Workloads bieten die Berechtigungen, die Workload Factory für VMware benötigt, um Ressourcen und Prozesse in Ihrer öffentlichen Cloud-Umgebung basierend auf dem Betriebsmodus zu verwalten, in dem Sie arbeiten.

GenAI IAM-Richtlinien sind nur mit Lese-/Schreibberechtigungen verfügbar:

- **Lesen/Schreiben**: Führt in Ihrem Namen Operationen in AWS aus und automatisiert diese, wobei die zugewiesenen Anmeldeinformationen über die erforderlichen und validierten Berechtigungen für die Ausführung verfügen.

**IAM-Richtlinien für GenAI-Workloads**

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

Die folgende Tabelle enthält Einzelheiten zu den Berechtigungen für GenAI-Workloads.

**Berechtigungstabelle für GenAI-Workloads**

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Ein Cloud-Formation-Stack für KI-Engine entsteht während Implementierung und Wiederherstellung | CloudFormation:CreateStack | Einsatz | Lese-/Schreibzugriff |
| Der Cloud-Formation-Stack für KI-Engine | Wolkenbildung:DescribeStacks | Einsatz | Lese-/Schreibzugriff |
| Listen Sie Regionen für den Implementierungsassistenten für KI-Engines auf | ec2:DescribeRegionen | Einsatz | Lese-/Schreibzugriff |
| Anzeigen von KI-Engine-Tags | ec2:DescribeTags | Einsatz | Lese-/Schreibzugriff |
| S3-Buckets auflisten | s3:ListAllMyBuchs | Einsatz | Lese-/Schreibzugriff |
| VPC-Endpunkte vor der Erstellung des AI-Engine-Stacks auflisten | ec2:CreateVpcEndpoint | Einsatz | Lese-/Schreibzugriff |
| Erstellen einer Sicherheitsgruppe für KI-Engines während der Erstellung des AI-Engine-Stacks bei Implementierungen und Neuerstellungen | ec2:CreateSecurityGroup | Einsatz | Lese-/Schreibzugriff |
| Markieren Sie Ressourcen, die durch die Stack-Erstellung von KI-Engines erstellt wurden, während der Implementierung oder Wiederherstellung | ec2:CreateTags | Einsatz | Lese-/Schreibzugriff |
| Veröffentlichen Sie verschlüsselte Ereignisse im WLMAI-Backend aus dem AI-Engine-Stack | Kms:GenerateDataKey | Einsatz | Lese-/Schreibzugriff |
| | KMS:Entschlüsseln | Einsatz | Lese-/Schreibzugriff |
| Veröffentlichen Sie Ereignisse und benutzerdefinierte Ressourcen im WLMAI-Backend aus dem Stack der ai-Engine | sns:Veröffentlichen | Einsatz | Lese-/Schreibzugriff |
| VPCs während des Assistenten für die Implementierung einer KI-Engine auflisten | ec2:DescribeVpcs | Einsatz | Lese-/Schreibzugriff |
| Subnetze im Assistenten für die Bereitstellung der ai-Engine auflisten | ec2:DescribeSubnets | Einsatz | Lese-/Schreibzugriff |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Routingtabellen werden bei der Implementierung und beim Rebuild der KI-Engine abgerufen | ec2:DescribeRouteTables | Einsatz | Lese-/Schreibzugriff |
| Auflistung von Schlüsselpaaren während des Implementierungsassistenten für KI-Engines | ec2:DescribeKeypairs | Einsatz | Lese-/Schreibzugriff |
| Auflistung der Sicherheitsgruppen bei der Erstellung von KI-Engines (so werden Sicherheitsgruppen an privaten Endpunkten gefunden) | ec2:DescribeSecurityGroups | Einsatz | Lese-/Schreibzugriff |
| VPC-Endpunkte abrufen, um zu ermitteln, ob bei der Implementierung der KI-Engine irgendwelche erstellt werden sollten | ec2:DescribeVpcEndpunkte | Einsatz | Lese-/Schreibzugriff |
| Listen Sie die Anwendungen von Amazon Q Business auf | QBusiness:ListenApplications | Einsatz | Lese-/Schreibzugriff |
| Führen Sie Instanzen auf, um den Status der AI-Engine herauszufinden | ec2:DescribeInstances | Fehlerbehebung | Lese-/Schreibzugriff |
| Listet Images während der Erstellung des AI-Engine-Stacks bei Implementierungen und Neuerstellungen auf | ec2:DescribeBilder | Einsatz | Lese-/Schreibzugriff |
| Erstellung und Aktualisierung von Sicherheitsgruppen für AI-Instanzen und private Endpunkte während der Erstellung des KI-Instanz-Stacks bei Implementierungen und Neuerstellungen | ec2:RevokeSecurityGroupEgress | Einsatz | Lese-/Schreibzugriff |
| | ec2:RevokeSecurityGroupIngress | Einsatz | Lese-/Schreibzugriff |
| Während der Erstellung eines Cloud-Formation-Stacks führen Sie die KI-Engine während der Implementierung und Neuerstellung aus | ec2:RunInstances | Einsatz | Lese-/Schreibzugriff |
| Während der Stack-Erstellung während der Implementierung und der Wiederherstellung können Sie dann Sicherheitsgruppen hinzufügen und Regeln für die KI-Engine ändern | ec2:AuthoriseSecurityGroupEgress | Einsatz | Lese-/Schreibzugriff |
| | ec2:AuthoriseSecurityGroupIngress | Einsatz | Lese-/Schreibzugriff |

| Zweck | Aktion | Wo verwendet | Berechtigungs richtlinie |
|---|---|---|---|
| Initiieren Sie eine Chat-Anfrage an eines der Basismodelle | Bedrock:InvokeModelWithin ResponseStream | Einsatz | Lese-/Schreibzugriff |
| Chat-/Einbettungsanfrage für Grundmodelle starten | Bedrock:InvokeModel | Einsatz | Lese-/Schreibzugriff |
| Zeigen Sie die verfügbaren Fundamentmodelle in einer Region an | Bedrock:ListFoundationModels | Einsatz | Lese-/Schreibzugriff |
| Informationen zu einem Basismodell abrufen | Bedrock:GetFoundationModel | Einsatz | Lese-/Schreibzugriff |
| Überprüfen Sie den Zugriff auf das Basismodell | Bedrock:GetFoundationModelVerf ügbarkeit | Einsatz | Lese-/Schreibzugriff |
| Überprüfen Sie, ob die Amazon CloudWatch-Protokollgruppe während der Bereitstellung und Neuerstellung erstellt werden muss | Protokolle:DescribeLogGroups | Einsatz | Lese-/Schreibzugriff |
| Holen Sie sich Regionen, die FSX und Amazon Bedrock unterstützen, während der KI-Engine-Assistent | ssm:GetParametersByPath | Einsatz | Lese-/Schreibzugriff |
| Nutzen Sie das aktuelle Amazon Linux Image für die Implementierung der KI-Engine während des Implementierungs- und Neuerstellungsvorgangs | ssm:GetParameters | Einsatz | Lese-/Schreibzugriff |
| Erhalten Sie die SSM-Antwort vom Befehl, der an die AI-Engine gesendet wird | ssm:GetCommandInvocation | Einsatz | Lese-/Schreibzugriff |
| Überprüfen Sie die SSM-Verbindung zur AI-Engine | ssm:SendCommand | Einsatz | Lese-/Schreibzugriff |
| | ssm:GetConnectionStatus | Einsatz | Lese-/Schreibzugriff |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Erstellung eines Instanzprofils für die KI-Engine bei der Stack-Erstellung während der Implementierung oder Neuerstellung | iam:CreateRollenole | Einsatz | Lese-/Schreibzugriff |
| | iam:CreateInstanceProfil | Einsatz | Lese-/Schreibzugriff |
| | iam:AddRoleToInstanceProfile | Einsatz | Lese-/Schreibzugriff |
| | iam:PuttePolicy | Einsatz | Lese-/Schreibzugriff |
| | iam:GetRolePolicy | Einsatz | Lese-/Schreibzugriff |
| | iam:GetRole | Einsatz | Lese-/Schreibzugriff |
| | iam:TagRole | Einsatz | Lese-/Schreibzugriff |
| | iam:PassRole | Einsatz | Lese-/Schreibzugriff |
| Simulieren Sie Workload-Vorgänge, um verfügbare Berechtigungen zu validieren und sie mit den erforderlichen AWS Kontoberechtigungen zu vergleichen | iam:SimulatePrincipalPolicy | Einsatz | Lese-/Schreibzugriff |
| Listen Sie FSX für ONTAP-Dateisysteme während des Assistenten „Create Knowledge Base“ auf | fsx:DescribeVolumes | Erstellung einer Wissensdatenbank | Lese-/Schreibzugriff |
| Listen Sie FSX für ONTAP-Dateisystem-Volumes während des Assistenten „Create Knowledge Base“ auf | fsx:DescribeFileSystems | Erstellung einer Wissensdatenbank | Lese-/Schreibzugriff |
| Management von Wissensdatenbanken auf Basis der KI-Engine bei Neuerstellungen | fsx:ListTagsForRessource | Fehlerbehebung | Lese-/Schreibzugriff |
| Listen Sie FSX für ONTAP Dateisystem Speicher virtuelle Maschinen während des „Create Knowledge“-Knowledgebase-Assistenten auf | fsx:DescribeStorageVirtualMachines | Einsatz | Lese-/Schreibzugriff |
| Verschieben Sie die Wissensdatenbank in eine neue Instanz | fsx:UntagResource | Fehlerbehebung | Lese-/Schreibzugriff |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Verwalten Sie die Wissensdatenbank auf der KI-Engine während des Rebuilds | fsx:TagResource | Fehlerbehebung | Lese-/Schreibzugriff |
| Speichern Sie SSM Secrets (ECR-Token, CIFS-Anmeldedaten, Mandanten-Service-Kontoschlüssel) auf sichere Weise | ssm:GetParameter | Einsatz | Lese-/Schreibzugriff |
| | ssm:PutParameter | Einsatz | Lese-/Schreibzugriff |
| Bei der Implementierung und Wiederherstellung werden die AI-Engine-Protokolle an die Amazon CloudWatch Protokollgruppe gesendet | Protokolle:CreateLogGroup | Einsatz | Lese-/Schreibzugriff |
| | Protokolle:PutRetentionPolicy | Einsatz | Lese-/Schreibzugriff |
| Senden Sie die AI-Engine-Protokolle an die Amazon CloudWatch-Protokollgruppe | Protokolle:TagResource | Fehlerbehebung | Lese-/Schreibzugriff |
| SSM-Antwort von Amazon CloudWatch abrufen (wenn die Antwort zu lang ist) | Protokolle:DescribeLogStreams | Fehlerbehebung | Lese-/Schreibzugriff |
| Erhalten Sie die SSM-Antwort von Amazon CloudWatch | Protokolle:GetLogEvents | Fehlerbehebung | Lese-/Schreibzugriff |
| Erstellen einer Amazon CloudWatch-Protokollgruppe für Amazon Bedrock-Protokolle während der Stack-Erstellung bei Bereitstellungs- und Neuerstellungsvorgängen | Protokolle:CreateLogGroup | Einsatz | Lese-/Schreibzugriff |
| | Protokolle:PutRetentionPolicy | Einsatz | Lese-/Schreibzugriff |
| | Protokolle:TagResource | Einsatz | Lese-/Schreibzugriff |
| Inferenzprofile für das Modell auflisten | Bedrock:ListInferenceProfiles | Fehlerbehebung | Lese-/Schreibzugriff |

#### Berechtigungen für VMware-Workloads

Für VMware-Workloads stehen folgende Berechtigungsrichtlinien zur Auswahl:

- **Ansicht, Planung und Analyse**: Sehen Sie sich das Inventar der EVS-Virtualisierungsumgebungen an, erhalten Sie eine fundierte Analyse Ihrer Systeme und entdecken Sie Einsparmöglichkeiten.
- **Bereitstellung und Anbindung von Datenspeichern**: Stellen Sie empfohlene VM-Layouts auf Amazon EVS-, Amazon EC2- oder VMware Cloud on AWS vSphere-Clustern bereit und verwenden Sie angepasste Amazon FSx for NetApp ONTAP Dateisysteme als externe Datenspeicher.

Wählen Sie die Berechtigungsrichtlinie aus, um die erforderlichen IAM-Richtlinien anzuzeigen:

### IAM-Richtlinien für VMware-Workloads

**Ansicht, Planung und Analyse**

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

**Datenspeicherbereitstellung und -konnektivität**

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

Die folgende Tabelle enthält Einzelheiten zu den Berechtigungen für VMware-Workloads.

**Berechtigungstabelle für VMware-Workloads**

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Fügen Sie Sicherheitsgruppen hinzu, und ändern Sie Regeln für die bereitgestellten Knoten | ec2:AuthoriseSecurityGroupIngress | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| Erstellen von EBS Volumes | fsx: CreateVolume erstellen | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| Markieren Sie benutzerdefinierte Werte für FSX for NetApp ONTAP-Ressourcen, die von VMware-Workloads erstellt wurden | fsx:TagResource | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| Erstellen und Validieren der CloudFormation-Vorlage | CloudFormation:CreateStack | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| Verwalten von Tags und Netzwerksicherheit auf erstellten Instanzen | ec2:CreateSecurityGroup | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| Starten Sie die erstellten Instanzen | ec2:RunInstances | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| Hier finden Sie Details zur EC2-Instanz | ec2:DescribeInstances | Inventar | Datenspeicherbereitstellung und -konnektivität |
| Führen Sie während der Stapelerstellung während der Bereitstellung und Neuerstellung Images auf | ec2:DescribeBilder | Inventar | Datenspeicherbereitstellung und -konnektivität |
| Konfigurationsdetails der DHCP-Optionssätze anzeigen, die mit VPCs verknüpft sind | ec2:DescribeDhcpOptions | Inventar | Ansicht, Planung und Analyse |
| Rufen Sie die VPCs in der ausgewählten Umgebung auf, um das Bereitstellungsformular auszufüllen | ec2:DescribeVpcs | • Einsatz<br>• Inventar | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungs richtlinie |
|---|---|---|---|
| Rufen Sie die Subnetze in der ausgewählten Umgebung ab, um das Bereitstellungsformular auszufüllen | ec2:DescribeSubnets | • Einsatz<br>• Inventar | Ansicht, Planung und Analyse |
| Rufen Sie die Sicherheitsgruppen in der ausgewählten Umgebung auf, um das Bereitstellungsformular auszufüllen | ec2:DescribeSecurityGroups | Einsatz | Ansicht, Planung und Analyse |
| Abrufen der Verfügbarkeitszonen in der ausgewählten Umgebung | ec2:DescribeAvailability Zones | • Einsatz<br>• Inventar | Ansicht, Planung und Analyse |
| Informieren Sie sich über die Regionen mit Amazon FSX for NetApp ONTAP Support | ec2:DescribeRegionen | Einsatz | Ansicht, Planung und Analyse |
| Holen Sie sich die Aliase von KMS-Schlüsseln, die für die Verschlüsselung mit Amazon FSX for NetApp ONTAP verwendet werden | Km:ListAliase | Einsatz | Ansicht, Planung und Analyse |
| Nutzen Sie KMS-Schlüssel für die Verschlüsselung mit Amazon FSX for NetApp ONTAP | Kms:Listenschlüssel | Einsatz | Ansicht, Planung und Analyse |
| Erhalten Sie KMS-Schlüssel Ablaufdetails für Amazon FSX für NetApp ONTAP-Verschlüsselung verwendet werden | Kms:DescribeKey | Einsatz | Ansicht, Planung und Analyse |
| Geheimnisse im AWS Secrets Manager auflisten | secretsmanager:ListSecrets | Inventar | Ansicht, Planung und Analyse |
| Rufen Sie eine Liste der Umgebungen von Amazon EVS ab. | evs:ListEnvironments | Inventar | Ansicht, Planung und Analyse |
| Erhalten Sie detaillierte Informationen über eine bestimmte Amazon EVS-Umgebung | evs:GetEnvironment | Inventar | Ansicht, Planung und Analyse |
| Liste der VLANs, die einer Amazon EVS-Umgebung zugeordnet sind | evs:ListEnvironmentVlans | Inventar | Ansicht, Planung und Analyse |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Erstellen Sie die für die Bereitstellung erforderlichen Ressourcen für Amazon FSX for NetApp ONTAP | fsx:CreateFileSystem | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| | fsx:CreateStorageVirtualMachine | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| | fsx: CreateVolume erstellen | • Einsatz<br>• Managementvorgänge | Datenspeicherbereitstellung und -konnektivität |
| Amazon FSX for NetApp ONTAP – Details | fsx:Beschreiben* | • Einsatz<br>• Inventar<br>• Managementvorgänge<br>• Einsparungen entdecken | Datenspeicherbereitstellung und -konnektivität |
| KMS-Kerndetails und Verwendung für Amazon FSX for NetApp ONTAP Verschlüsselung | Km:CreateGrant | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| | Km:Beschreiben* | Einsatz | Ansicht, Planung und Analyse |
| | Km:Liste* | Einsatz | Ansicht, Planung und Analyse |
| | KMS:Entschlüsseln | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| | Kms:GenerateDataKey | Einsatz | Datenspeicherbereitstellung und -konnektivität |

| Zweck | Aktion | Wo verwendet | Berechtigungsrichtlinie |
|---|---|---|---|
| Listen Sie die SNS-Themen des Kunden auf und veröffentlichen Sie sie in WLMVMC-Backend-SNS sowie in Kunden-SNS, falls ausgewählt | sns:Veröffentlichen | Einsatz | Datenspeicherbereitstellung und -konnektivität |
| Simulieren Sie Workload-Vorgänge, um verfügbare Berechtigungen zu validieren und sie mit den erforderlichen AWS Kontoberechtigungen zu vergleichen | iam:SimulatePrincipalPolicy | Einsatz | • Datenspeicherbereitstellung und -konnektivität<br>• Ansicht, Planung und Analyse |

### Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

#### 1. Februar 2025

Dem Speicherworkload wurden folgende Berechtigungen hinzugefügt:

- `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. Dezember 2025

Dem Speicherworkload wurden folgende Berechtigungen hinzugefügt:

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

#### 27. November 2025

Dem Speicherworkload wurden folgende Berechtigungen hinzugefügt:

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

#### 2. November 2025

Die Berechtigungsrichtlinien „Nur lesen“ und „Lesen/Schreiben“ wurden in den Workloads Storage, Database und VMware ersetzt, um eine feinere Granularität und Flexibilität bei der Zuweisung von Berechtigungen zu ermöglichen.

#### 5. Oktober 2025

Die folgenden Berechtigungen wurden aus GenAI entfernt und werden jetzt von der GenAI-Engine verwaltet:

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

#### 29 Juni 2025

Die folgende Berechtigung ist jetzt im *schreibgeschützten* Modus für Datenbanken verfügbar: `cloudwatch:GetMetricData` .

#### 3 Juni 2025

Die folgende Berechtigung ist jetzt im Lese-/Schreibmodus für GenAI verfügbar: `s3:ListAllMyBuckets`.

#### 4 Mai 2025

Die folgende Berechtigung ist jetzt im Lese-/Schreibmodus für GenAI verfügbar: `qbusiness:ListApplications`.

Die folgenden Berechtigungen sind jetzt im *schreibgeschützten* Modus für Datenbanken verfügbar:

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

Die folgende Berechtigung ist jetzt im Lese-/Schreibmodus für Datenbanken verfügbar: `logs:PutRetentionPolicy`.

#### Bis 2. April 2025

Die folgende Berechtigung ist jetzt im *schreibgeschützten* Modus für Datenbanken verfügbar: `ssm:DescribeInstanceInformation`.

#### 30 März 2025

### Aktualisierung der GenAI-Workload-Berechtigungen

Die folgenden Berechtigungen sind jetzt im Lese-/Schreibmodus für GenAI verfügbar:

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

Die folgende Berechtigung wurde aus dem Lese-/Schreibmodus für GenAI entfernt: `Bedrock:GetFoundationModel`.

### iam:SimulatePrincipalPolicy-Berechtigungsaktualisierung

Der `iam:SimulatePrincipalPolicy` Die Berechtigung ist Teil aller Workload-Berechtigungsrichtlinien, wenn Sie die automatische Berechtigungsprüfung beim Hinzufügen zusätzlicher AWS-Kontoanmeldeinformationen oder beim Hinzufügen einer neuen Workload-Funktion über die Workload Factory-Konsole aktivieren. Die Berechtigung simuliert Workload-Vorgänge und prüft, ob Sie über die erforderlichen AWS-Kontoberechtigungen verfügen, bevor Sie Ressourcen aus Workload Factory bereitstellen. Durch die Aktivierung dieser Prüfung verringern Sie den Zeit- und Arbeitsaufwand, der möglicherweise zum Bereinigen von Ressourcen aus fehlgeschlagenen Vorgängen und zum Hinzufügen fehlender Berechtigungen erforderlich ist.

#### 2 März 2025

Die folgende Berechtigung ist jetzt im Lese-/Schreibmodus für GenAI verfügbar:

`bedrock:GetFoundationModel` .

**3 Februar 2025**

Die folgende Berechtigung ist jetzt im *schreibgeschützten* Modus für Datenbanken verfügbar: `iam:SimulatePrincipalPolicy` .

# Schnellstart für NetApp Workload Factory

Beginnen Sie mit NetApp Workload Factory, indem Sie sich anmelden und ein Konto erstellen, Anmeldeinformationen hinzufügen, damit Workload Factory AWS-Ressourcen direkt verwalten kann, und dann Ihre Workloads mithilfe von Amazon FSx for NetApp ONTAP optimieren.

NetApp Workload Factory ist für Benutzer als Cloud-Service über die webbasierte Konsole zugänglich. Bevor Sie beginnen, sollten Sie Folgendes verstehen:"Workload Factory" Die

**Registrieren Sie sich und erstellen Sie ein Konto**

Gehen Sie zum "Workload Factory-Konsole" , melden Sie sich an und erstellen Sie ein Konto.

"Erfahren Sie, wie Sie sich anmelden und ein Konto erstellen".

**AWS-Anmeldeinformationen zu Workload Factory hinzufügen**

Dieser Schritt ist optional. Sie können Workload Factory nutzen, ohne Anmeldeinformationen für den Zugriff auf Ihr AWS-Konto hinzufügen zu müssen. Durch das Hinzufügen von AWS-Anmeldeinformationen zu Workload Factory erhält Ihr Workload Factory-Konto die erforderlichen Berechtigungen zum Erstellen und Verwalten von FSx for ONTAP -Dateisystemen sowie zum Bereitstellen und Verwalten bestimmter Workloads, wie z. B. Datenbanken und GenAI.

"Hier erfahren Sie, wie Sie Ihrem Konto Anmeldeinformationen hinzufügen".

**Mit FSX for ONTAP können Sie Ihre Workloads optimieren**

Nachdem Sie sich angemeldet, ein Konto erstellt und optional AWS-Anmeldeinformationen hinzugefügt haben, können Sie mit der Verwendung von Workload Factory beginnen, um Ihre Workloads mit FSx for ONTAP zu optimieren.

"Optimieren Sie Ihre Workloads mit FSx für ONTAP" .

# Registrieren Sie sich bei NetApp Workload Factory

Auf NetApp Workload Factory kann über eine webbasierte Konsole zugegriffen werden. Wenn Sie mit Workload Factory beginnen, müssen Sie sich zunächst mit Ihren vorhandenen Anmeldeinformationen für die NetApp Support-Site anmelden oder ein NetApp Cloud-Login erstellen.

Sie können auch andere Personen einladen, Ihrem Workload Factory-Konto beizutreten, damit auch diese auf

Workload Factory zugreifen und es nutzen können.

## Registrieren Sie sich bei Workload Factory

Sie können sich mit einer der folgenden Optionen bei Workload Factory anmelden:

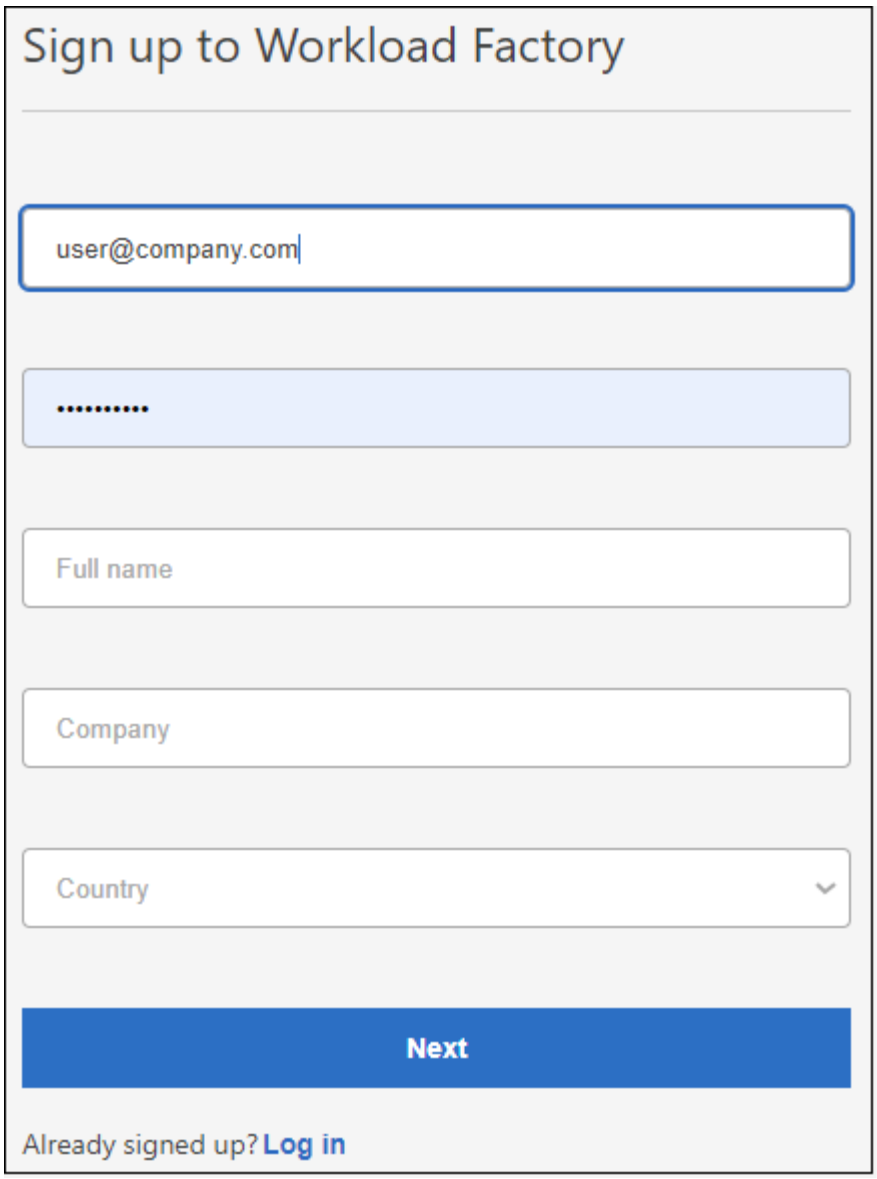
- Ihre vorhandenen Zugangsdaten für die NetApp Support Site (NSS
- Geben Sie Ihre E-Mail-Adresse und ein Passwort an, um sich bei einem NetApp Cloud-Login anzumelden

**Schritte**

1. Öffnen Sie einen Webbrowser und gehen Sie zu "Workload Factory-Konsole"
2. Wenn Sie über ein NetApp Support Site Konto verfügen, geben Sie die mit Ihrem NSS Konto verknüpfte E-Mail-Adresse direkt auf der **Anmelden** Seite ein.

   Sie können die Anmeldeseite überspringen, wenn Sie ein NSS-Konto haben. Workload Factory wird Sie im Rahmen dieser ersten Anmeldung anmelden.

3. Wenn Sie noch keinen NSS-Account haben und sich mit einem NetApp Cloud Login registrieren möchten, wählen Sie **Registrieren**.




4. Geben Sie auf der Seite **Anmelden** die erforderlichen Informationen ein, um einen NetApp-Cloud-Login zu erstellen, und wählen Sie **Weiter**.

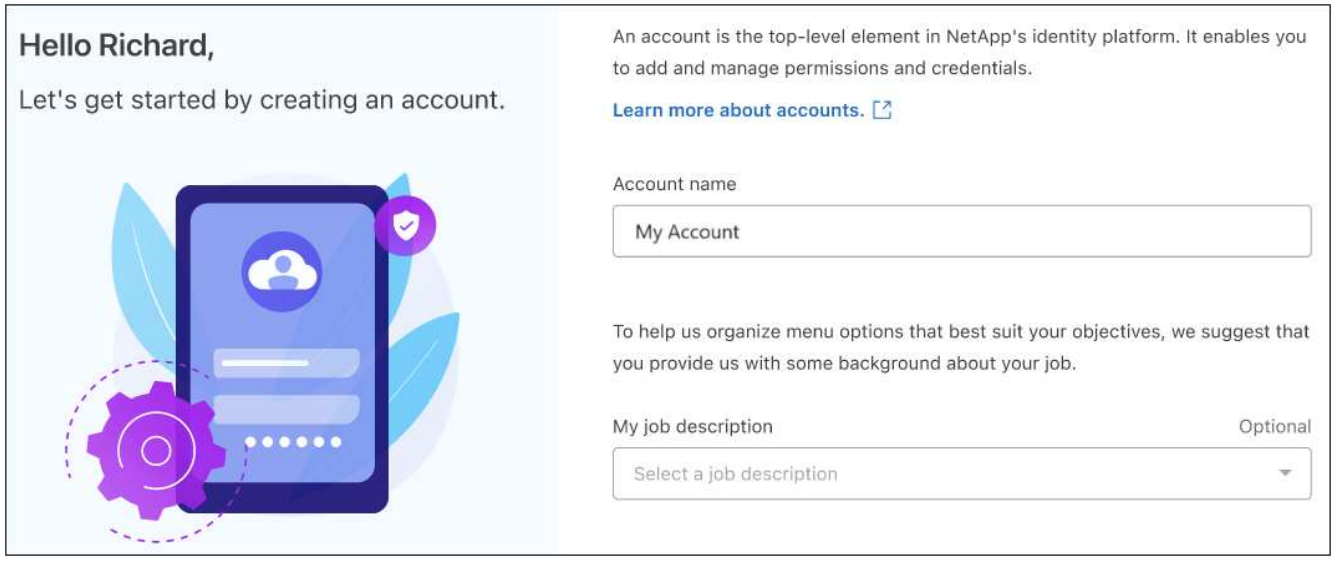
   Beachten Sie, dass nur englische Zeichen im Anmeldeformular zulässig sind.

5. Geben Sie die detaillierten Informationen für Ihr Unternehmen ein und wählen Sie **Anmelden**.
6. In Ihrem Posteingang finden Sie eine E-Mail von NetApp, die Anweisungen zur Überprüfung Ihrer E-Mail-Adresse enthält.

   Dieser Schritt ist erforderlich, bevor Sie sich anmelden können.

7. Wenn Sie dazu aufgefordert werden, lesen Sie die Endbenutzer-Lizenzvereinbarung, akzeptieren Sie die Bedingungen und wählen Sie **Weiter** aus.
8. Geben Sie auf der Seite **Account** einen Namen für Ihr Konto ein und wählen Sie optional Ihre Stellenbeschreibung aus.

   Ein Account ist das wichtigste Element der Identitätsplattform von NetApp, über das Sie Berechtigungen und Anmeldeinformationen hinzufügen und managen können.




9. Wählen Sie **Erstellen** und die Startseite von Workload Factory wird angezeigt.

**Ergebnis**

Sie verfügen jetzt über einen Workload Factory-Login und ein Konto. Sie gelten als Kontoadministrator und haben Zugriff auf alle Funktionen von Workload Factory.

## Laden Sie andere ein, einem Konto in Workload Factory beizutreten.

Als Kontoadministrator können Sie andere Personen einladen, Ihrem Workload Factory-Konto beizutreten, damit diese auf Workload Factory zugreifen und es nutzen können. Die Kontoverwaltung ist nur über die NetApp Console möglich.

Siehe die Dokumentation der NetApp Console . "Erfahren Sie, wie Sie Mitglieder (Benutzerkonten) hinzufügen."zu Ihrem Workload Factory-Konto.

**Ergebnis**

Der eingeladene Benutzer erhält eine E-Mail mit Anweisungen zum Beitritt zu Ihrem Workload Factory-Konto.

# AWS-Anmeldeinformationen zu Workload Factory hinzufügen

Fügen Sie AWS-Anmeldeinformationen hinzu und verwalten Sie diese, damit NetApp Workload Factory über die erforderlichen Berechtigungen zum Bereitstellen und Verwalten von Cloud-Ressourcen in Ihren AWS-Konten verfügt.

## Überblick

Sie können einem vorhandenen Workload Factory-Konto AWS-Anmeldeinformationen von der Seite „Anmeldeinformationen“ aus hinzufügen. Dadurch erhält Workload Factory die erforderlichen Berechtigungen zum Verwalten von Ressourcen und Prozessen in Ihrer AWS-Cloud-Umgebung.

Sie können Anmeldeinformationen mit zwei Methoden hinzufügen:

- **Manuell**: Sie erstellen die IAM-Richtlinie und die IAM-Rolle in Ihrem AWS-Konto, während Sie Anmeldeinformationen in Workload Factory hinzufügen.

- **Automatisch**: Sie erfassen eine minimale Menge an Informationen über Berechtigungen und verwenden dann einen CloudFormation-Stack, um die IAM-Richtlinien und Rolle für Ihre Anmeldeinformationen zu erstellen.

## AWS Referenzen

Wir haben einen Registrierungsfluss von AWS Angenommen Role Credentials entworfen, der Folgendes ermöglicht:

- Unterstützt stärker ausgerichtete AWS-Kontoberechtigungen, indem Sie die Workload-Funktionen angeben können, die Sie verwenden möchten, und die IAM-Richtlinienanforderungen entsprechend dieser Auswahl bereitstellen.
- Hier können Sie die gewährten AWS-Kontonberechtigungen anpassen, wenn Sie bestimmte Workload-Funktionen aktivieren oder deaktivieren.
- Vereinfacht die manuelle Erstellung von IAM-Richtlinien durch maßgeschneiderte JSON-Richtliniendateien, die Sie in der AWS Konsole anwenden können.
- Weitere Vereinfachung des Registrierungsprozesses von Anmeldeinformationen, indem Benutzern eine automatisierte Option für die erforderliche IAM-Richtlinie und die Rollenerstellung mithilfe von AWS CloudFormation-Stacks zur Verfügung gestellt wird.
- Bessere Ausrichtung an FSX für ONTAP-Benutzer, die ihre Anmeldedaten lieber innerhalb der Grenzen des AWS-Cloud-Ecosystems speichern möchten, indem sie die Zugangsdaten für FSX für ONTAP-Services in einem AWS-basierten Geheimmanagement-Back-End speichern lassen.

#### Eine oder mehrere AWS Zugangsdaten

Wenn Sie Ihre erste Workload Factory-Funktion (oder -Funktionen) verwenden, müssen Sie die Anmeldeinformationen mit den für diese Workload-Funktionen erforderlichen Berechtigungen erstellen. Sie fügen die Anmeldeinformationen zu Workload Factory hinzu, müssen jedoch auf die AWS-Managementkonsole zugreifen, um die IAM-Rolle und -Richtlinie zu erstellen. Diese Anmeldeinformationen sind in Ihrem Konto verfügbar, wenn Sie eine beliebige Funktion in Workload Factory verwenden.

Ihre anfänglichen AWS-Anmeldeinformationen können eine IAM-Berechtigungsrichtlinie für eine oder mehrere Funktionen enthalten. Das hängt ganz von Ihren geschäftlichen Anforderungen ab.

Durch das Hinzufügen mehrerer AWS-Anmeldeinformationen zu Workload Factory erhalten Sie zusätzliche Berechtigungen, die für die Verwendung zusätzlicher Funktionen erforderlich sind, z. B. FSx für ONTAP -Dateisysteme, das Bereitstellen von Datenbanken auf FSx für ONTAP, das Migrieren von VMware-Workloads und mehr.

## Fügen Sie einem Konto manuell Anmeldeinformationen hinzu

Sie können AWS-Anmeldeinformationen manuell zu Workload Factory hinzufügen, um Ihrem Workload Factory-Konto die erforderlichen Berechtigungen zum Verwalten der AWS-Ressourcen zu erteilen, die Sie zum Ausführen Ihrer individuellen Workloads verwenden. Jeder Satz von Anmeldeinformationen, den Sie hinzufügen, enthält eine oder mehrere IAM-Richtlinien basierend auf den Workload-Funktionen, die Sie verwenden möchten, und eine IAM-Rolle, die Ihrem Konto zugewiesen ist.

Sie können einem Konto entweder über die Workload Factory-Konsole oder über die NetApp Konsole AWS-Anmeldeinformationen hinzufügen.

Die Erstellung der Anmeldedaten besteht aus drei Teilen:

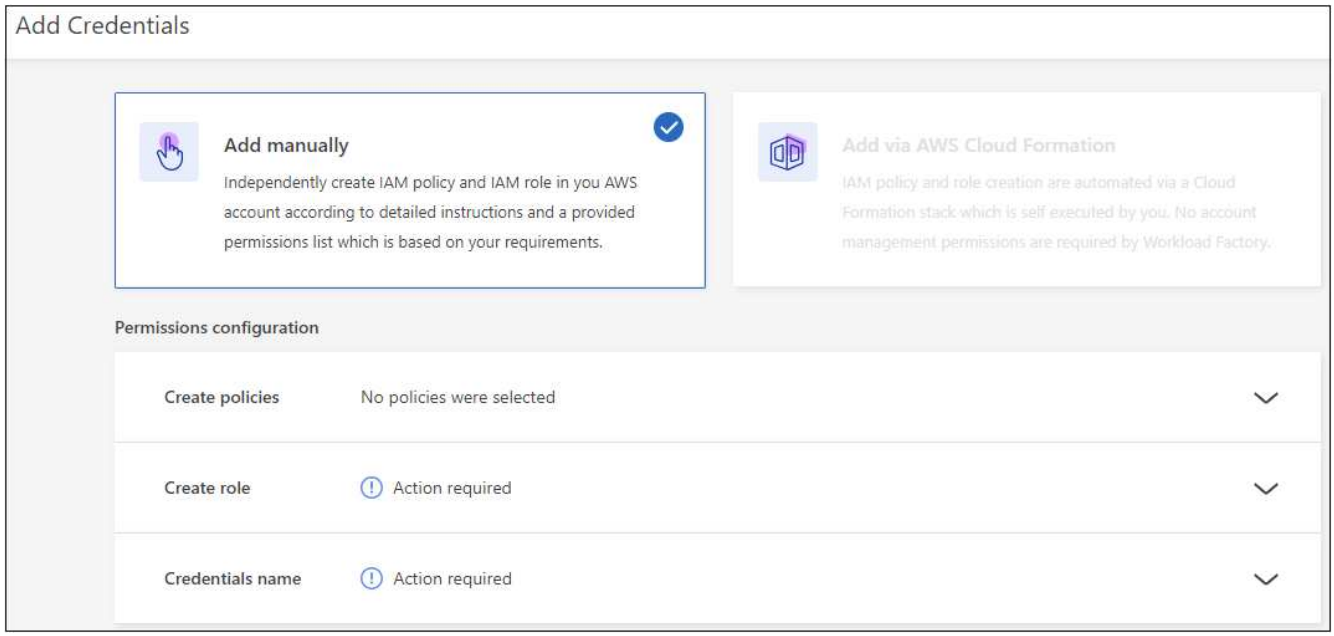
- Wählen Sie die gewünschte Service- und Berechtigungsebene aus und erstellen Sie anschließend IAM-Richtlinien über die AWS Management Console.
- Erstellen Sie eine IAM-Rolle über die AWS Management Console.
- Geben Sie in Workload Factory einen Namen ein und fügen Sie die Anmeldeinformationen hinzu.

**Bevor Sie beginnen**

Um sich bei Ihrem AWS-Konto anzumelden, müssen Sie über Anmeldedaten verfügen.

**Schritte**

1. Melden Sie sich an bei "Workload Factory-Konsole" .
2. Wählen Sie im Menü **Administration** und dann **Anmeldeinformationen**.
3. Wählen Sie auf der Seite Anmeldeinformationen die Option **Anmeldeinformationen hinzufügen**.
4. Wählen Sie auf der Seite Anmeldeinformationen hinzufügen die Option **manuell hinzufügen** aus, und führen Sie dann die folgenden Schritte aus, um jeden Abschnitt unter *Berechtigungskonfiguration* abzuschließen.




### Schritt 1: Wählen Sie die Workload-Funktionen aus und erstellen Sie die IAM-Richtlinien

In diesem Abschnitt legen Sie fest, welche Arten von Workload-Funktionen im Rahmen dieser Anmeldedaten gemanagt werden können und welche Berechtigungen für jeden Workload aktiviert werden. Sie müssen die Richtlinienberechtigungen für jeden ausgewählten Workload aus der Codebox kopieren und zur Erstellung der Richtlinien in die AWS Management Console innerhalb Ihres AWS-Kontos hinzufügen.

**Schritte**

1. Aktivieren Sie im Abschnitt **Richtlinien erstellen** die Workload-Funktionen, die Sie in diese Anmeldedaten aufnehmen möchten.

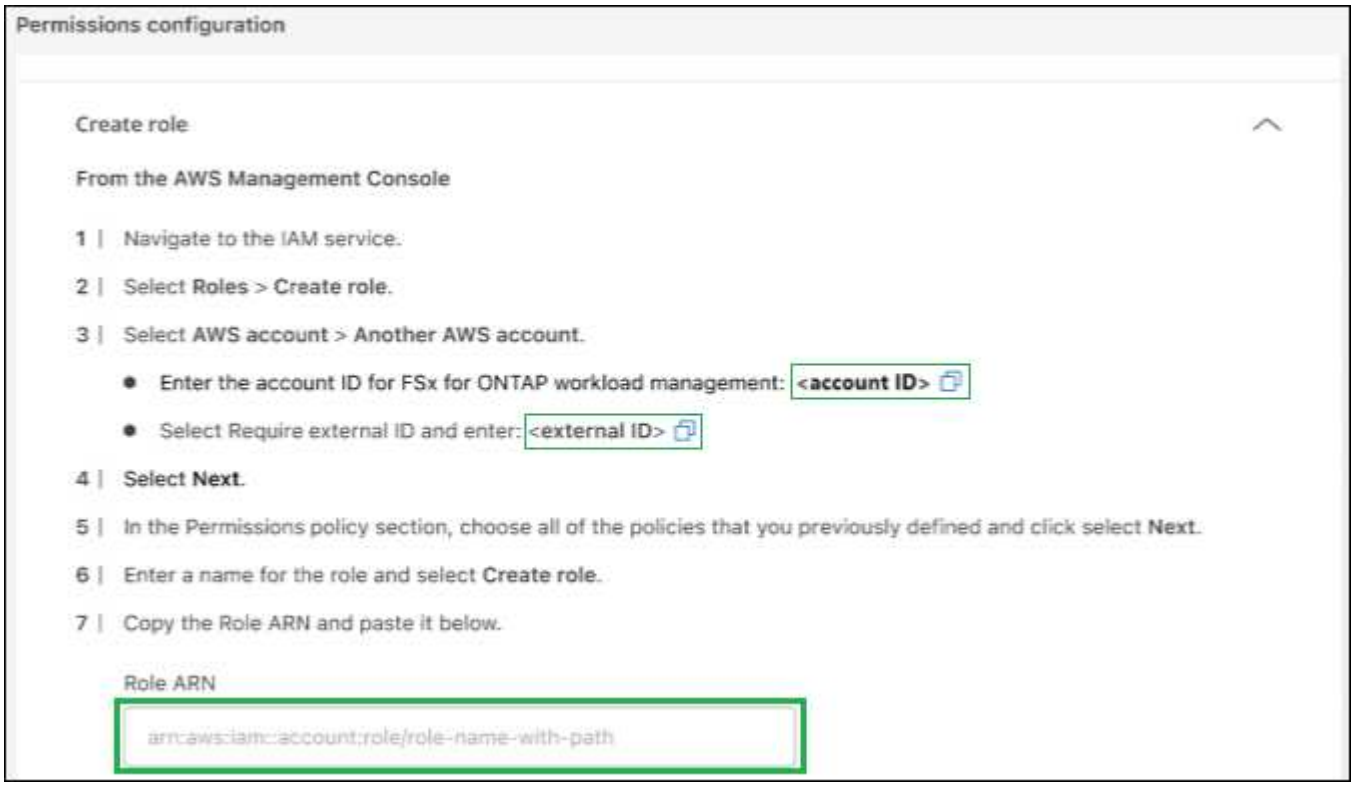
   Sie können später weitere Funktionen hinzufügen. Wählen Sie also einfach die Workloads aus, die Sie aktuell implementieren und managen möchten.

2. Wählen Sie für diejenigen Workload-Funktionen, die eine Auswahl an Berechtigungsrichtlinien bieten, die Art der Berechtigungen aus, die mit diesen Anmeldeinformationen verfügbar sein sollen.

3. Optional: Wählen Sie **Enable automatic permissions Check** aus, um zu überprüfen, ob Sie die erforderlichen AWS-Kontoberechtigungen für die Ausführung von Workload-Vorgängen besitzen. Durch Aktivieren der Prüfung wird die zu Ihren Berechtigungsrichtlinien hinzugefügt `iam:SimulatePrincipalPolicy permission`. Mit dieser Berechtigung werden nur Berechtigungen bestätigt. Sie können die Berechtigung nach dem Hinzufügen von Anmeldeinformationen entfernen. Wir empfehlen jedoch, sie beizubehalten, um die Ressourcenerstellung für teilweise erfolgreiche Vorgänge zu verhindern und Sie vor der erforderlichen manuellen Ressourcenbereinigung zu schützen.
4. Kopieren Sie im Codebox-Fenster die Berechtigungen für die erste IAM-Richtlinie.
5. Öffnen Sie ein anderes Browserfenster, und melden Sie sich bei Ihrem AWS-Konto in der AWS Management Console an.
6. Öffnen Sie den IAM-Dienst, und wählen Sie dann **Richtlinien** > **Richtlinie erstellen** aus.
7. Wählen Sie JSON als Dateityp aus, fügen Sie die Berechtigungen ein, die Sie in Schritt 3 kopiert haben, und wählen Sie **Weiter** aus.
8. Geben Sie den Namen für die Richtlinie ein und wählen Sie **Richtlinie erstellen**.
9. Wenn Sie in Schritt 1 mehrere Workload-Funktionen ausgewählt haben, wiederholen Sie diese Schritte, um eine Richtlinie für jeden Satz von Workload-Berechtigungen zu erstellen.

### Schritt 2: Erstellen Sie die IAM-Rolle, die die Richtlinien verwendet

In diesem Abschnitt richten Sie eine IAM-Rolle ein, die von Workload Factory übernommen wird und die die gerade erstellten Berechtigungen und Richtlinien umfasst.




**Schritte**

1. Wählen Sie in der AWS Management Console **Roles > Create Role** aus.
2. Wählen Sie unter **Vertrauenswürdiger Entitätstyp AWS-Konto** aus.
   a. Wählen Sie **Ein anderes AWS-Konto** aus und kopieren Sie die Konto-ID für das FSx for ONTAP -Workload-Management aus der Workload Factory-Benutzeroberfläche und fügen Sie sie ein.

b. Wählen Sie **Erforderliche externe ID** aus und kopieren Sie die externe ID aus der Workload Factory-Benutzeroberfläche und fügen Sie sie ein.

3. Wählen Sie **Weiter**.
4. Wählen Sie im Abschnitt „Berechtigungsrichtlinie“ alle zuvor definierten Richtlinien aus und wählen Sie **Weiter** aus.
5. Geben Sie einen Namen für die Rolle ein und wählen Sie **Rolle erstellen**.
6. Kopieren Sie die Rolle ARN.
7. Kehren Sie zur Seite „Anmeldeinformationen hinzufügen“ in Workload Factory zurück, erweitern Sie den Abschnitt **Rolle erstellen** unter **Berechtigungskonfiguration** und fügen Sie die ARN in das Feld *Rollen-ARN* ein.

#### Schritt 3: Geben Sie einen Namen ein und fügen Sie die Anmeldeinformationen hinzu

Der letzte Schritt besteht darin, einen Namen für die Anmeldeinformationen in Workload Factory einzugeben.

**Schritte**

1. Erweitern Sie auf der Seite „Anmeldeinformationen hinzufügen“ in Workload Factory unter „Berechtigungskonfiguration“ den Eintrag „**Name der Anmeldeinformationen**“.
2. Geben Sie den Namen ein, den Sie für diese Anmeldedaten verwenden möchten.
3. Wählen Sie **Hinzufügen**, um die Anmeldeinformationen zu erstellen.

**Ergebnis**

Die Anmeldeinformationen werden erstellt, und Sie werden zur Seite Anmeldedaten zurückgeführt.

## Fügen Sie Anmeldeinformationen zu einem Konto über CloudFormation hinzu

Sie können mithilfe eines AWS CloudFormation-Stacks AWS-Anmeldeinformationen zu Workload Factory hinzufügen, indem Sie die gewünschten Workload Factory-Funktionen auswählen und dann den AWS CloudFormation-Stack in Ihrem AWS-Konto starten. CloudFormation erstellt die IAM-Richtlinien und die IAM-Rolle basierend auf den von Ihnen ausgewählten Workload-Funktionen.

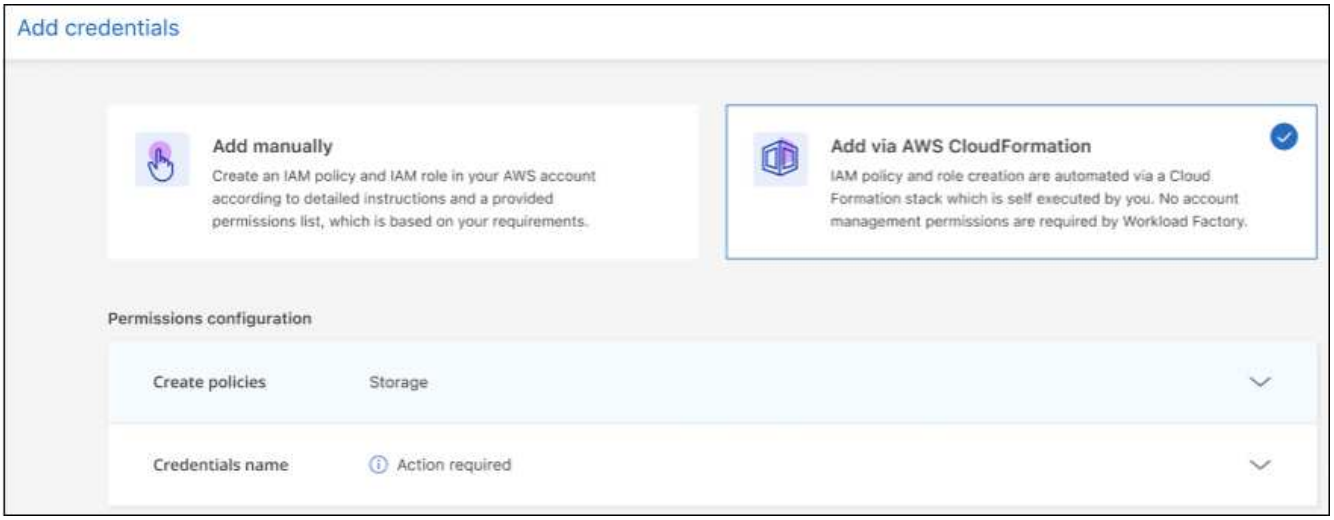
**Bevor Sie beginnen**

- Um sich bei Ihrem AWS-Konto anzumelden, müssen Sie über Anmeldedaten verfügen.
- Sie müssen über die folgenden Berechtigungen in Ihrem AWS-Konto verfügen, wenn Sie Anmeldeinformationen mit einem CloudFormation-Stack hinzufügen:

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

**Schritte**

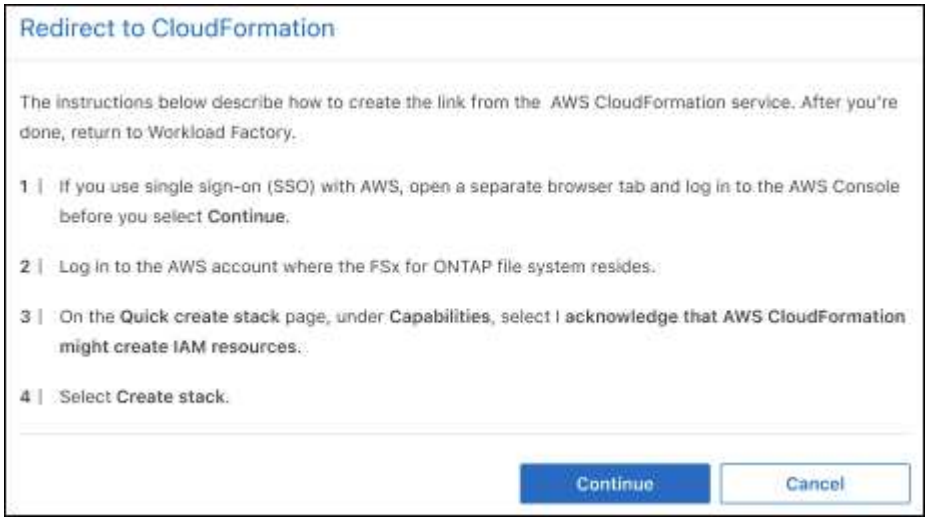
1. Melden Sie sich an bei "Workload Factory-Konsole" .
2. Wählen Sie im Menü **Administration** und dann **Anmeldeinformationen**.
3. Wählen Sie auf der Seite Anmeldeinformationen die Option **Anmeldeinformationen hinzufügen**.
4. Wählen Sie **Add via AWS CloudFormation** aus.




5. Aktivieren Sie unter **Create Policies** die Workload-Funktionen, die Sie in diese Anmeldedaten aufnehmen möchten, und wählen Sie eine Berechtigungsstufe für jeden Workload aus.

   Sie können später weitere Funktionen hinzufügen. Wählen Sie also einfach die Workloads aus, die Sie aktuell implementieren und managen möchten.

6. Optional: Wählen Sie **Enable automatic permissions Check** aus, um zu überprüfen, ob Sie die erforderlichen AWS-Kontoberechtigungen für die Ausführung von Workload-Vorgängen besitzen. Durch Aktivieren der Prüfung wird die Berechtigung zu Ihren Berechtigungsrichtlinien hinzugefügt `iam:SimulatePrincipalPolicy`. Mit dieser Berechtigung werden nur Berechtigungen bestätigt. Sie können die Berechtigung nach dem Hinzufügen von Anmeldeinformationen entfernen. Wir empfehlen jedoch, sie beizubehalten, um die Ressourcenerstellung für teilweise erfolgreiche Vorgänge zu verhindern und Sie vor der erforderlichen manuellen Ressourcenbereinigung zu schützen.
7. Geben Sie unter **Name der Anmeldeinformationen** den Namen ein, den Sie für diese Anmeldeinformationen verwenden möchten.
8. Fügen Sie die Zugangsdaten von AWS CloudFormation hinzu:
   a. Wählen Sie **Add** (oder wählen Sie **Redirect to CloudFormation**) und die Seite Redirect to CloudFormation wird angezeigt.




   b. Wenn Sie Single Sign-On (SSO) mit AWS verwenden, öffnen Sie eine separate Browser-Registerkarte und melden Sie sich bei der AWS-Konsole an, bevor Sie **Weiter** auswählen.

Sie sollten sich beim AWS-Konto anmelden, wo sich das FSX für ONTAP-Dateisystem befindet.

c. Wählen Sie auf der Seite „Umleiten zur CloudFormation“ die Option **Weiter**.

d. Wählen Sie auf der Seite „schneller Stapel erstellen“ unter „Funktionen“ **Ich bestätige, dass AWS CloudFormation IAM-Ressourcen erstellen könnte**.

e. Wählen Sie **Stapel erstellen**.

f. Kehren Sie zu Workload Factory zurück und überwachen Sie die Seite „Anmeldeinformationen“, um zu überprüfen, ob die neuen Anmeldeinformationen in Bearbeitung sind oder hinzugefügt wurden.

# Optimieren Sie Workloads mit NetApp Workload Factory

Nachdem Sie sich angemeldet und NetApp Workload Factory eingerichtet haben, können Sie verschiedene Funktionen von Workload Factory nutzen, z. B. Amazon FSx für ONTAP Dateisysteme erstellen, Datenbanken auf FSx für ONTAP Dateisystemen bereitstellen und Konfigurationen virtueller Maschinen zu VMware Cloud auf AWS migrieren, wobei FSx für ONTAP -Dateisysteme als externe Datenspeicher verwendet werden.

- "Amazon FSX für NetApp ONTAP"

  Bewerten und analysieren Sie aktuelle Datenbestände auf mögliche Kosteneinsparungen durch Einsatz von FSX for ONTAP als Storage-Infrastruktur, Bereitstellung und Vorlagenatisierung von FSX für ONTAP Implementierungen basierend auf Best Practices und Zugriff auf erweiterte Managementfunktionen.

- "Datenbank-Workloads"

  Erkennen Sie Ihren vorhandenen Datenbankbestand auf AWS, ermitteln Sie potenzielle Kosteneinsparungen durch einen Wechsel zu FSX für ONTAP, implementieren Sie Datenbanken durchgängig mit integrierten Best Practices zur Optimierung und automatisieren Sie Thin Cloning für CI/CD-Pipelines.

- "GenAI"

  Durch die Implementierung und das Management einer RAG-Infrastruktur (Retrieval-Augmented Generation) werden die Genauigkeit und Einzigartigkeit Ihrer KI-Applikationen verbessert. Erstellen Sie eine RAG Knowledge Base auf FSX for ONTAP mit integrierter Datensicherheit und Compliance.

- "VMware-Workloads"

  Optimieren Sie Migrationen und Betriebsabläufe mithilfe intelligenter Empfehlungen und automatischer Problembehebung. Implementieren Sie effiziente Backups und zuverlässige Disaster Recovery. Überwachen Sie Ihre VMs und beheben Sie Fehler.

- "EDA-Workloads"

  FSx für ONTAP über mehrere Dateisysteme hinweg optimieren, um die Leistung zu steigern und die Betriebskosten durch automatisiertes Speicherparametermanagement zu senken.