基本事項をご確認ください

Setup and administration

NetApp
February 02, 2026

目次

基本事項をご確認ください . . . 1
NetAppワークロードファクトリーについて学ぶ . . . 1
特徴 . . . 1
サポートされているクラウドプロバイダ . . . 2
セキュリティ . . . 2
コスト . . . 2
ワークロードファクトリーの仕組み . . . 2
NetApp Workload Factory を使用するためのツール . . . 4
コンソールエクスペリエンス . . . 5
NetAppコンソールでワークロードファクトリーにアクセスする . . . 5
Workload FactoryコンソールでWorkload Factoryにアクセスします . . . 6
NetApp Workload Factory の権限 . . . 6
権限を使用する理由 . . . 6
ワークロード別の権限 . . . 6
変更ログ . . . 53

基本事項をご確認ください

NetAppワークロードファクトリーについて学ぶ

NetApp Workload Factory は、Amazon FSx for NetApp ONTAPファイルシステムを使用してワークロードを最適化できるように設計された強力なライフサイクル管理プラットフォームです。 Workload Factory と FSx for ONTAPを使用して合理化できるワークロードには、データベース、VMware Cloud on AWS への VMware の移行、AI チャットボットなどがあります。

ワークロード には、ビジネス目標を達成するために設計されたリソース、コード、サービス、またはアプリケーションの組み合わせが含まれます。これは、顧客向けのアプリケーションからバックエンドのプロセスまで、あらゆるものが対象となります。ワークロードには、単一の AWS アカウント内のリソースのサブセットが含まれる場合もあれば、複数のアカウントにまたがる場合もあります。

Amazon FSx for NetApp ONTAP は、ミッションクリティカルなアプリケーション、データベース、コンテナ、VMware Cloud データストア、およびユーザーファイル向けに、完全に管理された AWS ネイティブの NFS、SMB/CIFS、および iSCSI ストレージボリュームを提供します。 FSx for ONTAPは、Workload Factory およびネイティブ AWS 管理ツールを使用して管理できます。

特徴

Workload Factory プラットフォームは、次の主要な機能を提供します。

柔軟性に優れた低コストのストレージ

クラウドでAmazon FSx for NetApp ONTAPファイルシステムを検出、導入、管理できます。FSx for ONTAPは、ONTAPのすべての機能をAWSネイティブのマネージドサービスで利用し、一貫したハイブリッドクラウドエクスペリエンスを提供します。

オンプレミスの**vSphere**環境を**VMware Cloud on AWS**に移行

VMware Cloud on AWS Migration Advisorを使用すると、オンプレミスのvSphere環境で現在の仮想マシンの構成を分析し、推奨されるVMレイアウトをVMware Cloud on AWSに導入する計画を生成し、カスタマイズしたAmazon FSx for NetApp ONTAPファイルシステムを外部データストアとして使用できます。

データベースのライフサイクル管理

Amazon FSx for NetApp ONTAPによるデータベースワークロードの調査とコスト削減の分析、SQLサーバデータベースをFSx for ONTAPストレージに移行する際のストレージとアプリケーションのメリットの活用、ベンダーのベストプラクティスを実装したSQLサーバ、データベース、データベースクローンの導入、コードとしてのインフラの共同パイロットによる運用の自動化、SQLサーバ環境の継続的な監視と最適化によるパフォーマンス、可用性、保護、コスト効率の向上

AIチャットボットの開発

FSx for ONTAPファイルシステムを活用して、組織のチャットボットソースやAIエンジンデータベースを保存できます。これにより、組織の非構造化データをエンタープライズチャットボットアプリケーションに埋め込むことができます。

コストを削減するためのコスト削減計算ツール

Amazon Elastic Block Store（EBS）ストレージやElastic File System（EFS）ストレージ、Amazon FSx

for Windowsファイルサーバを使用している現在の環境を分析し、Amazon FSx for NetApp ONTAPに移行することでどれだけのコストを削減できるかを確認できます。また、将来の導入を計画している場合に備えて、計算ツールを使用して「what if」シナリオを実行することもできます。

自動化を促進するサービスアカウント

サービス アカウントを使用して、 NetApp Workload Factory の操作を安全かつ確実に自動化します。サービス アカウントは、ユーザー管理の制限なしに信頼性が高く長期的な自動化を提供し、API アクセスのみを提供するためより安全です。

質問するAIアシスタント

FSx for ONTAPファイルシステムの管理と操作について AI アシスタントに質問します。 Ask Me は、モデル コンテキスト プロトコル (MCP) を使用して、外部環境と安全にインターフェイスし、API ツールにクエリを実行して、特定のストレージ環境に合わせた応答を提供します。

サポートされているクラウドプロバイダ

Workload Factory を使用すると、クラウド ストレージを管理し、Amazon Web Services のワークロード機能を使用できます。

セキュリティ

NetApp Workload Factoryのセキュリティは、 NetAppにとって最優先事項です。Workload Factory のすべてのワークロードは、Amazon FSx for NetApp ONTAP上で実行されます。すべてに加えて "AWS セキュリティ機能"NetApp Workload Factoryは "SOC2 タイプ 1 コンプライアンス、SOC2 タイプ 2 コンプライアンス、および HIPAA コンプライアンス"。

Amazon FSx for NetApp ONTAP for NetApp Workload Factoryは"エンタープライズアプリを展開するためのAWSソリューション"適切に設計されたベストプラクティスを念頭に置いて作成されました。

コスト

Workload Factory は無料でご利用いただけます。 Amazon Web Services (AWS) に支払うコストは、展開する予定のストレージおよびワークロード サービスによって異なります。これには、Amazon FSx for NetApp ONTAPファイルシステム、VMware Cloud on AWS インフラストラクチャ、AWS サービスなどのコストが含まれます。

ワークロードファクトリーの仕組み

Workload Factory には、SaaS レイヤーを通じて提供される Web ベースのコンソール、アカウント、クラウド資産へのアクセスを制御する操作モード、Workload Factory と AWS アカウント間の分離された接続を提供するリンクなどが含まれます。

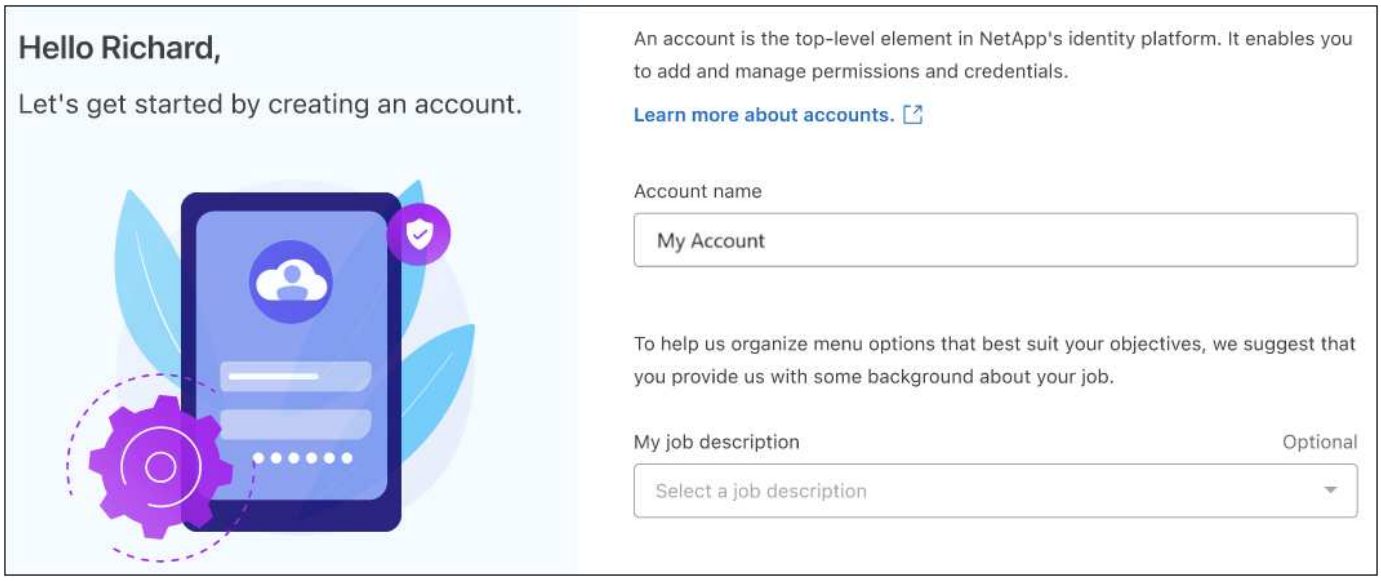
ソフトウェアサービス

ワークロードファクトリーは、"NetAppワークロード ファクトリー コンソール"そして"NetAppコンソール"。これらの SaaS エクスペリエンスにより、最新機能がリリースされると自動的にアクセスでき、Workload Factory アカウントとリンクを簡単に切り替えることができます。

"さまざまなコンソールのエクスペリエンスについて詳しく知る"

アカウント

Workload Factory に初めてログインすると、アカウントを作成するように求められます。このアカウントを使用すると、資格情報を使用して組織のリソース、ワークロード、ワークロード アクセスを整理できます。



アカウントを作成すると、そのアカウントのsingle_account admin_userになります。

組織で追加のアカウントまたはユーザー管理が必要な場合は、製品内のチャットを使用して当社に連絡してください。

NetAppコンソールを使用する場合、Workload Factory はNetAppアカウントを活用するため、すでにアカウントに属していることになります。

サービスアカウント

サービス アカウントは、自動化の目的でNetApp Workload Factory への承認済み API 呼び出しを行うことができる「ユーザー」として機能します。これにより、いつでも退職する可能性のある実際の人物のユーザー アカウントに基づいて自動化スクリプトを作成する必要がなくなるため、自動化の管理が容易になります。Workload Factory のすべてのアカウント所有者は、アカウント管理者とみなされます。アカウント管理者は複数のサービス アカウントを作成および削除できます。

"サービスアカウントの管理方法"

権限

Workload Factory は柔軟な権限ポリシーを提供し、クラウド資産へのアクセスを慎重に制御し、IT ポリシーに基づいて Workload Factory に段階的な信頼を割り当てることを可能にします。

"Workload Factory の権限ポリシーの詳細"

接続リンク

Workload Factory リンクは、Workload Factory と 1 つ以上の FSx for ONTAPファイル システム間の信頼関係と接続を作成します。これにより、Amazon FSx for ONTAP API では利用できない特定のファイルシステム機能を、 ONTAP REST API 呼び出しから直接監視および管理できるようになります。

Workload Factory の使用を開始するためにリンクは必要ありませんが、場合によっては、Workload Factory のすべての機能とワークロード機能のロックを解除するためにリンクを作成する必要があります。

現在、リンクはAWS Lambdaを利用しています。

"リンクの詳細"

コードボックス自動化

Codebox は、開発者や DevOps エンジニアが Workload Factory でサポートされているあらゆる操作を実行するために必要なコードを生成するのに役立つ Infrastructure as Code (IaC) の副操縦士です。コード形式には、Workload Factory REST API、AWS CLI、AWS CloudFormation が含まれます。

Codebox は、Workload Factory の動作モード (基本、読み取り専用、読み取り/書き込み) と連携しており、実行準備のための明確なパスと、将来の迅速な再利用のための自動化カタログを設定します。

[コードボックス]ペインには、特定のジョブフロー操作によって生成されたIACが表示され、グラフィカルウィザードまたは会話型チャットインターフェイスによって照合されます。Codeboxは、簡単なナビゲーションと分析のためにカラーコーディングと検索をサポートしていますが、編集はできません。自動化カタログにのみコピーまたは保存できます。

"Codeboxの詳細"

削減額計算ツール

Workload Factory では、FSx for ONTAPファイルシステム上のストレージ環境、データベース、またはVMware ワークロードのコストを他の Amazon サービスと比較できるコスト削減計算ツールを提供しています。ストレージ要件によっては、FSx for ONTAPファイル システムが最もコスト効率の高いオプションとなる場合があります。

- "ストレージ環境のコスト削減効果を試算する方法をご紹介します"
- "データベースワークロードの削減効果を試算する方法をご紹介します"
- "VMware ワークロードのコスト削減方法を学ぶ"

適切に設計されたワークロード

Workload Factory は、AWS Well-Architected フレームワークに準拠した、信頼性が高く、安全で、効率的で、対費用効果の高いストレージとデータベース構成の維持と運用に役立ちます。Workload Factory は、FSxのONTAPファイル システム、SQL Server、および Oracle データベースのデプロイメントを毎日スキャンして、潜在的な構成ミスに関する分析情報を提供し、問題を修正するための手動または自動のアクションを推奨します。

"Well-Architected ワークロードの詳細"

NetApp Workload Factory を使用するためのツール

NetApp Workload Factory は次のツールで使用できます。

- **Workload Factory** コンソール: Workload Factory コンソールは、アプリケーションとプロジェクトの視覚的かつ全体的なビューを提供します。
- * NetAppコンソール*: NetAppコンソールはハイブリッド インターフェイス エクスペリエンスを提供する

ため、Workload Factory を他のNetAppデータ サービスと一緒に使用できます。

- 質問する: Ask me AI アシスタントを使用すると、Workload Factory コンソールを離れることなく、質問したり、Workload Factory について詳しく知ることができます。Workload Factory のヘルプ メニューから「Ask me」にアクセスします。
- **CloudShell CLI**: Workload Factory には、単一のブラウザベースの CLI からアカウント全体の AWS およびNetApp環境を管理および操作するための CloudShell CLI が含まれています。Workload Factory コンソールの上部バーから CloudShell にアクセスします。
- **REST API**: Workload Factory REST API を使用して、FSx for ONTAPファイルシステムやその他の AWS リソースをデプロイおよび管理します。
- **CloudFormation**: AWS CloudFormation コードを使用して、Workload Factory コンソールで定義したアクションを実行し、AWS アカウントの CloudFormation スタックから AWS およびサードパーティのリソースをモデル化、プロビジョニング、管理します。
- **Terraform NetApp Workload Factory** プロバイダー: Terraform を使用して、Workload Factory コンソールで生成されたインフラストラクチャ ワークフローを構築および管理します。

REST API

Workload Factory を使用すると、特定のワークロードに合わせて FSx for ONTAPファイル システムを最適化、自動化、および操作できます。各ワークロードは関連する REST API を公開します。これらのワークロードと API を組み合わせることで、FSx for ONTAPファイルシステムの管理に使用できる柔軟で拡張可能な開発プラットフォームが構成されます。

Workload Factory REST API を使用すると、いくつかの利点があります。

- APIは、RESTテクノロジと最新のベストプラクティスに基づいて設計されています。コアテクノロジにはHTTPとJSONがあります。
- Workload Factory の認証は OAuth2 標準に基づいています。 NetApp はAuth0 サービスの実装に依存しています。
- Workload Factory の Web ベース コンソールは同じコア REST API を使用するため、2 つのアクセス パス間に一貫性が保たれます。

"Workload Factory REST API ドキュメントを見る"

コンソールエクスペリエンス

NetApp Workload Factory には、2 つの Web ベースのコンソールからアクセスできます。 Workload Factory コンソールとNetAppコンソールを使用して Workload Factory にアクセスする方法を学習します。

- * NetAppコンソール*: FSx for ONTAPファイルシステムとAmazon FSx for NetApp ONTAPで実行されているワークロードを同じ場所で管理できるハイブリッドエクスペリエンスを提供します。
- **Workload Factory** コンソール: Amazon FSx for NetApp ONTAPで実行されるワークロードに重点を置いた専用の Workload Factory エクスペリエンスを提供します。

NetAppコンソールでワークロードファクトリーにアクセスする

NetApp Consoleから Workload Factory にアクセスできます。Workload Factory を AWS ストレージおよびワ

ークロード機能に使用することに加えて、 NetApp Copy and Syncなどの他のデータ サービスにもアクセスすることができます。

手順

1. ログイン"NetAppコンソール"。
2. NetAppコンソール メニューから、ワークロード を選択し、次に 概要 を選択します。

Workload FactoryコンソールでWorkload Factoryにアクセスします

Workload Factory コンソールから Workload Factory にアクセスできます。

ステップ

1. ログイン"ワークロードファクトリーコンソール"。

NetApp Workload Factory の権限

NetApp Workload Factory の機能とサービスを使用するには、Workload Factory がクラウド環境で操作を実行できるように権限を付与する必要があります。

権限を使用する理由

権限を付与すると、Workload Factory は、その AWS アカウント内のリソースとプロセスを管理するための権限を持つポリシーをインスタンスにアタッチします。これにより、Workload Factory は、ストレージ環境の検出から、ストレージ管理のファイルシステムや GenAI ワークロードのナレッジベースなどの AWS リソースのデプロイまで、さまざまな操作を実行できるようになります。

たとえば、データベース ワークロードの場合、Workload Factory に必要な権限が付与されると、指定されたアカウントとリージョン内のすべての EC2 インスタンスがスキャンされ、すべての Windows ベースのマシンがフィルタリングされます。 AWS Systems Manager (SSM) エージェントがホストにインストールされ実行されており、System Manager ネットワークが適切に設定されている場合、Workload Factory は Windows マシンにアクセスし、SQL Server ソフトウェアがインストールされているかどうかを確認できます。

ワークロード別の権限

各ワークロードは、権限を使用して、Workload Factory で特定のタスクを実行します。権限は、設定された権限ポリシーにまとめられます。使用するワークロードまでスクロールして、アクセス許可ポリシー、アクセス許可ポリシーのコピー可能な JSON、およびすべてのアクセス許可、その目的、使用場所、およびそれらをサポートするアクセス許可ポリシーをリストした表について学習します。

ストレージの権限

ストレージに使用できる IAM ポリシーは、パブリック クラウド環境内のリソースとプロセスを管理するために Workload Factory に必要な権限を提供します。

ストレージには、次の権限ポリシーから選択できます。

- 表示、計画、分析: FSx for ONTAPファイル システムを表示し、システムの健全性を把握し、システムの Well-Architected 分析を取得して、コスト削減を検討します。
- 操作と修復: ファイル システム容量の調整やファイル システム構成の問題の修正などの運用タスクを実行

します。

- ファイルシステムの作成と削除: FSx for ONTAPファイルシステムとストレージ VM を作成および削除します。

必要な IAM ポリシーを表示します。

ストレージの**IAM**ポリシー

表示、計画、分析

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

運用と修復

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

ファイルシステムの作成と削除

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

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

次の表に、ストレージの権限を示します。

ストレージの権限の一覧

目的	アクション	使用先	許可ポリシー
FSx for ONTAPファイルシステムの作成	FSx：CreateFileSystem	導入	ファイルシステムの作成と削除
FSx for ONTAPファイルシステムのセキュリティグループを作成する	EC2：CreateSecurityGroup	導入	ファイルシステムの作成と削除
FSx for ONTAPファイルシステムのセキュリティグループにタグを追加する	ec2：CreateTags	導入	ファイルシステムの作成と削除
FSx for ONTAPファイルシステムのセキュリティグループの出力と入力を許可する	ec2：AuthorizeSecurityGroupEgress	導入	ファイルシステムの作成と削除
	ec2：AuthorizeSecurityGroupIngress	導入	ファイルシステムの作成と削除
Grantedロールは、FSx for ONTAPとその他のAWSサービス間の通信を提供します。	IAM：CreateServiceLinkedRole	導入	ファイルシステムの作成と削除
FSx for ONTAPファイルシステム導入フォームに必要事項をご記入ください	EC2: DescribeVpcs	• 導入 • コスト削減の詳細	ファイルシステムの作成と削除
	EC2: DescribeSubnets	• 導入 • コスト削減の詳細	ファイルシステムの作成と削除
	EC2: DescribeSecurityGroups	• 導入 • コスト削減の詳細	ファイルシステムの作成と削除
	EC2: DescribeRouteTables	• 導入 • コスト削減の詳細	ファイルシステムの作成と削除
	EC2: DescribeNetworkInterfaces	• 導入 • コスト削減の詳細	ファイルシステムの作成と削除
	EC2：DescripteVolumeStatus	• 導入 • コスト削減の詳細	ファイルシステムの作成と削除

目的	アクション	使用先	許可ポリシー
KMSの主要な詳細情報を入手し、FSx for ONTAPの暗号化に使用	KMS：CreateGrant	導入	ファイルシステムの作成と削除
	KMS:説明キー	導入	ファイルシステムの作成と削除
	KMS：ListKeys	導入	ファイルシステムの作成と削除
	KMS：エイリアスを確認する	導入	ファイルシステムの作成と削除
EC2インスタンスのボリュームの詳細を取得	EC2: DescribeVolumesの場合	• インベントリ • コスト削減の詳細	表示、計画、分析
EC2インスタンスの詳細を取得	EC2: DescribeInstances	コスト削減の詳細	表示、計画、分析
コスト削減試算ツールでElastic File Systemについて説明する	Elasticfilesystem:ファイルシステムの説明	コスト削減の詳細	表示、計画、分析
FSx for ONTAPリソース用のタグを挙げる	FSx：ListTagsForResource	インベントリ	表示、計画、分析
FSx for ONTAPファイルシステムのセキュリティグループの出力と入力を管理	EC2: RevokeSecurityGroupIngress	カンリシヨリ	ファイルシステムの作成と削除
	ec2: セキュリティグループの出力を取り消す	カンリシヨリ	ファイルシステムの作成と削除
	EC2: DeleteSecurityGroup	カンリシヨリ	ファイルシステムの作成と削除

目的	アクション	使用先	許可ポリシー
FSx for ONTAPファイルシステムリソースの作成、表示、管理	FSx：ボリュームの作成	カンリシヨリ	運用と修復
	FSx：TagResource	カンリシヨリ	運用と修復
	FSx：CreateStorageVirtualMachine	カンリシヨリ	ファイルシステムの作成と削除
	fsx:ファイルシステムの削除	カンリシヨリ	ファイルシステムの作成と削除
	fsx:ストレージ仮想マシンの削除	カンリシヨリ	表示、計画、分析
	FSx：DescriptionFileSystems	インベントリ	表示、計画、分析
	FSx：DescriptionStorageVirtualMachines	インベントリ	表示、計画、分析
	fsx:共有Vpc構成の説明	インベントリ	表示、計画、分析
	fsx:ファイルシステムの更新	カンリシヨリ	運用と修復
	fsx:ストレージ仮想マシンの更新	カンリシヨリ	運用と修復
	FSx：Description	インベントリ	表示、計画、分析
	FSx：UPDATEVOLUME	カンリシヨリ	運用と修復
	fsx:ボリュームの削除	カンリシヨリ	運用と修復
	FSx：UntagResource	カンリシヨリ	運用と修復
	FSx：バックアップの説明	カンリシヨリ	表示、計画、分析
	fsx:バックアップの作成	カンリシヨリ	運用と修復
	fsx:バックアップからボリュームを作成	カンリシヨリ	運用と修復
	fsx:バックアップの削除	カンリシヨリ	運用と修復
ファイルシステムとボリュームの指標を取得	CloudWatch：GetMetricData	カンリシヨリ	表示、計画、分析
	CloudWatch：GetMetricStatistics	カンリシヨリ	表示、計画、分析
ワークロードの処理をシミュレートして使用可能な権限を検証し、必要なAWSアカウントの権限と比較	IAM：SimulatePrincipalPolicy	導入	全て

目的	アクション	使用先	許可ポリシー
FSx for ONTAP EMS イベントに AI ベースの洞察を提供する	Bedrock: ListInferenceProfiles	FSx for ONTAP EMS分析	運用と修復
	bedrock:GetInferenceProfile	FSx for ONTAP EMS分析	運用と修復
	bedrock:InvokeModelWihResponseStream	FSx for ONTAP EMS分析	運用と修復
	Bedrock：InvokeModel	FSx for ONTAP EMS分析	運用と修復
AWS Cost Explorer から FSx for ONTAPファイルシステムのコストと使用状況データを取得する	ce:コストと使用量の取得	コストと使用状況の分析	表示、計画、分析
	ce:タグを取得	コストと使用状況の分析	表示、計画、分析
S3アクセスポイントを作成し、FSx for ONTAPファイルシステムに接続します	fsx:CreateAndAttachS3AccessPoint	S3 アクセスポイント管理	運用と修復
S3アクセスポイントをFSx for ONTAPファイルシステムから切り離して削除する	fsx：DetachAndDeleteS3AccessPoint	S3 アクセスポイント管理	運用と修復
簡素化されたバケットアクセス管理用の S3 アクセスポイントを作成する	s3：CreateAccessPoint	S3 アクセスポイント管理	運用と修復
S3 アクセスポイントを削除する	s3：DeleteAccessPoint	S3 アクセスポイント管理	運用と修復
S3 アクセスポイントにタグを追加する	s3：TagResource	S3 アクセスポイント管理	運用と修復
S3 アクセスポイントのタグを一覧表示および表示する	s3：ListTagsForResource	S3 アクセスポイント管理	運用と修復
S3 アクセスポイントからタグを削除する	s3：UntagResource	S3 アクセスポイント管理	運用と修復
S3 アクセスポイントバケット内のオブジェクトを検出する	s3：ListBucket	S3 バケット操作	運用と修復
S3 テーブルバケットの一覧表示、作成、説明	s3tables：ListTableBuckets s3tables：CreateTableBucket s3tables：GetTableBucket	S3 table bucket 管理	運用と修復
S3 テーブルの一覧表示、作成、取得	s3tables：ListTables s3tables：CreateTable s3tables：GetTable	S3 テーブル操作	運用と修復
テーブルメタデータの場所を読み取る	s3tables：GetTableMetadataLocation	S3 テーブルメタデータ操作	運用と修復
テーブルメタデータの場所を更新する	s3tables：UpdateTableMetadataLocation	S3 テーブルメタデータ操作	運用と修復

目的	アクション	使用先	許可ポリシー
テーブルの名前空間の一覧表示、作成、取得	s3tables：ListNamespaces s3tables：CreateNamespace s3tables：GetNamespace	S3 namespace操作	運用と修復
テーブルデータの読み取り（select、scan）	s3tables：GetTableData	S3 テーブルデータ操作	運用と修復
テーブルデータの書き込み（挿入）	s3tables：PutTableData	S3 テーブルデータ操作	運用と修復
在庫テーブル上のタグを一覧表示する（FSx for ONTAP、ストレージVM、ボリュームIDを取得）	s3tables：ListTagsForResource	S3 テーブルタグ操作	運用と修復
Workload Factory検索用のインベントリテーブルにタグを付ける	s3tables：TagResource	S3 テーブルタグ操作	運用と修復
アクセスポイント経由でオブジェクトのタグ付けを取得	s3：GetObjectTagging	S3 オブジェクト操作	運用と修復

データベースワークロードの権限

データベース ワークロードに使用できる IAM ポリシーは、パブリック クラウド環境内のリソースとプロセスを管理するために Workload Factory に必要な権限を提供します。

データベースでは、次の権限ポリシーから選択できます。

- 表示、計画、および分析: データベース リソースのインベントリを表示し、リソースの健全性を把握し、データベース構成の Well-Architected 分析を確認し、節約を検討し、エラー ログ分析を取得し、節約を検討します。
- 操作と修復: データベース リソースの運用タスクを実行し、データベース構成と基盤となる FSx for ONTAPファイル システム ストレージの問題を修正します。
- データベース ホストの作成: ベスト プラクティスに従って、データベース ホストと、その基盤となる FSx for ONTAPファイル システム ストレージをデプロイします。

運用モードを選択して、必要なIAMポリシーを表示します。

表示、計画、分析

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

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

運用と修復

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

データベースホストの作成

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

次の表に、データベースワークロードの権限を示します。

データベースワークロードの権限の一覧

目的	アクション	使用先	許可ポリシー
FSx for ONTAP、EBS、FSx for Windows File Server のメトリック統計とコンピューティング最適化の推奨事項を取得します。	CloudWatch：GetMetricStatistics	• インベントリ • コスト削減の詳細	表示、計画、分析
登録済みのSQLノードからAmazon CloudWatchに保存されたパフォーマンスメトリクスを収集します。登録済みのSQLインスタンスのインスタンス管理画面に、パフォーマンストレンドチャートにデータが生成されます。	CloudWatch：GetMetricData	インベントリ	表示、計画、分析
EC2インスタンスの詳細を取得	EC2: DescribeInstances	• インベントリ • コスト削減の詳細	表示、計画、分析
	EC2：DescribeKeyPairs	導入	表示、計画、分析
	EC2: DescribeNetworkInterfaces	導入	表示、計画、分析
	EC2:説明InstanceTypes	• 導入 • コスト削減の詳細	表示、計画、分析

目的	アクション	使用先	許可ポリシー
FSx for ONTAPの導入フォームに必要事項をご記入ください	EC2: DescribeVpcs	• 導入 • インベントリ	表示、計画、分析
	EC2: DescribeSubnets	• 導入 • インベントリ	表示、計画、分析
	EC2: DescribeSecurityGroups	導入	表示、計画、分析
	EC2: DescribeImages	導入	表示、計画、分析
	EC2: DescribeRegions (説明領域	導入	表示、計画、分析
	EC2: DescribeRouteTables	• 導入 • インベントリ	表示、計画、分析
既存のVPCエンドポイントを取得して、導入前に新しいエンドポイントを作成する必要があるかどうかを判断	EC2: DescribeVpcEndpoints	• 導入 • インベントリ	表示、計画、分析
EC2インスタンスのパブリックネットワーク接続に関係なく、必要なサービス用にVPCエンドポイントが存在しない場合はVPCエンドポイントを作成する	EC2：CreateVpcEndpoint	導入	データベースホストの作成
検証ノード（t2.micro/t3.micro）のリージョンで使用可能なインスタンスタイプを取得します。	EC2:説明InstanceTypeOfferings	導入	表示、計画、分析
接続されている各EBSボリュームのSnapshot詳細を取得して、価格設定と削減効果を見積もる	ec2: DescribeSnapshots	コスト削減の詳細	表示、計画、分析
添付されている各EBSボリュームの詳細を確認して、価格設定と削減効果を見積もる	EC2: DescribeVolumesの場合	• インベントリ • コスト削減の詳細	表示、計画、分析
FSx for ONTAPのファイルシステム暗号化に関するKMSの主な詳細情報を入手	KMS：エイリアスを確認する	導入	表示、計画、分析
	KMS：ListKeys	導入	表示、計画、分析
	KMS:説明キー	導入	表示、計画、分析

目的	アクション	使用先	許可ポリシー
環境で実行されているCloudFormationスタックのリストを取得してクォータ制限を確認	CloudFormation：リストスタック	導入	表示、計画、分析
展開を開始する前に、リソースのアカウント制限を確認する	CloudFormation：DescriptionAccountLimits	導入	表示、計画、分析
AWSが管理するリージョン内のActive Directoryのリストを取得する	ds:説明ディレクトリ	導入	表示、計画、分析
ボリューム、バックアップ、SVM、AZ内のファイルシステム、FSx for ONTAPファイルシステムのタグの一覧と詳細を取得できます	FSx：Description	• インベントリ • コスト削減額をチェック	表示、計画、分析
	FSx：バックアップの説明	• インベントリ • コスト削減額をチェック	表示、計画、分析
	FSx：DescriptionStorageVirtualMachines	• 導入 • カンリシヨリ • インベントリ	表示、計画、分析
	FSx：DescriptionFileSystems	• 導入 • カンリシヨリ • インベントリ • コスト削減の詳細	表示、計画、分析
	FSx：ListTagsForResource	カンリシヨリ	表示、計画、分析
CloudFormation と VPC のサービスクォータ制限を取得する / SQL、ドメイン、FSx for ONTAP に提供された認証情報のユーザーアカウントにシークレットを作成する	サービスクォータ：ListServiceQuotas	導入	表示、計画、分析

目的	アクション	使用先	許可ポリシー
SSMベースのクエリを使用して、FSx for ONTAPでサポートされるリージョンの最新リストを取得	SSM：GetParametersByPath	導入	表示、計画、分析
導入後の管理操作のコマンドを送信した後、SSM 応答をポーリングします	SSM：GetCommandInvocation	• カンリシヨリ • インベントリ • コスト削減の詳細 • 最適化	表示、計画、分析
検出と管理のために SSM 経由で EC2 インスタンスにコマンドを送信します	SSM:sendCommand	• カンリシヨリ • インベントリ • コスト削減の詳細 • 最適化	表示、計画、分析
導入後にインスタンスのSSM接続ステータスを取得	SSM：GetConnectionStatus	• カンリシヨリ • インベントリ • 最適化	表示、計画、分析
管理対象EC2インスタンスのグループのSSMアソシエーションステータスの取得（SQLノード）	SSM：InstanceInformationの説明	インベントリ	表示、計画、分析
オペレーティングシステムのパッチ評価に使用できるパッチベースラインのリストを入手する	SSM：DescribePatchBaselines	最適化	表示、計画、分析
オペレーティングシステムのパッチ評価のためのWindows EC2インスタンスのパッチ状態の取得	SSM:DescribeInstancePatchStates	最適化	表示、計画、分析
オペレーティングシステムのパッチ管理用にAWS Patch ManagerによってEC2インスタンスで実行されるコマンドの一覧表示	SSM：ListCommands	最適化	表示、計画、分析
アカウントがAWS Compute Optimizerに登録されているかどうかを確認	compute-optimizer：GetEnrollmentStatus	• コスト削減の詳細 • 最適化	データベースホストの作成

目的	アクション	使用先	許可ポリシー
AWS Compute Optimizerで既存の推奨構成を更新して、SQL Serverワークロードの推奨構成を調整	計算オプティマイザ:PutRecommendationPreferences	• コスト削減の詳細 • 最適化	データベースホストの作成
AWS Compute Optimizerから、特定のリソースに対して有効な推奨設定を取得する	compute-optimizer:GetEffectiveRecommendationPreferences	• コスト削減の詳細 • 最適化	データベースホストの作成
Amazon Elastic Compute Cloud（Amazon EC2）インスタンス用にAWS Compute Optimizerが生成する推奨事項を取得	コンピューティングオプティマイザ：GetEC2InstanceRecommendations	• コスト削減の詳細 • 最適化	データベースホストの作成
自動スケーリンググループへのインスタンスの関連付けのチェック	オートスケーリング:説明AutoScalingGroups	• コスト削減の詳細 • 最適化	データベースホストの作成
	オートスケーリング:説明AutoScalingInstances	• コスト削減の詳細 • 最適化	データベースホストの作成
導入時またはAWSアカウントで管理されるAD、FSx for ONTAP、SQLユーザクレデンシャルのSSMパラメータの取得、一覧表示、作成、削除	SSM：getParameter [1]	• 導入 • カンリシヨリ • インベントリ	表示、計画、分析
	SSM：GetParameters [1]	• 導入 • カンリシヨリ • インベントリ	表示、計画、分析
	SSM：PutParameter [1]	• 導入 • カンリシヨリ	表示、計画、分析
	SSM：削除パラメータ[1]	• 導入 • カンリシヨリ	表示、計画、分析

目的	アクション	使用先	許可ポリシー
ネットワークリソースをSQLノードと検証ノードに関連付け、SQLノードにセカンダリIPを追加する	EC2：AllocateAddress [1]	導入	データベースホストの作成
	EC2：AllocateHosts [1]	導入	データベースホストの作成
	EC2：AssignPrivateIpAddresses [1]	導入	データベースホストの作成
	EC2：AssociateAddress [1]	導入	データベースホストの作成
	EC2：AssociateRouteTable [1]	導入	データベースホストの作成
	EC2：AssociateSubnetCidrBlock[1]	導入	データベースホストの作成
	EC2：AssociateVpcCidrBlock[1]	導入	データベースホストの作成
	EC2：AttachInternetGateway [1]	導入	データベースホストの作成
	EC2：AttachNetworkInterface [1]	導入	データベースホストの作成
導入に必要なEBSボリュームをSQLノードに接続する	EC2：AttachVolume	導入	データベースホストの作成
プロビジョニングされた EC2 インスタンスにセキュリティ グループをアタッチし、ルールを変更する	ec2：AuthorizeSecurityGroupEgress	導入	データベースホストの作成
	ec2：AuthorizeSecurityGroupIngress	導入	データベースホストの作成
導入用にSQLノードに必要なEBSボリュームを作成する	EC2：CreateVolume	導入	データベースホストの作成

目的	アクション	使用先	許可ポリシー
タイプT2.microで作成された一時検証ノードを削除し、失敗したEC2 SQLノードのロールバックまたは再試行のために削除します。	EC2：DeleteNetworkInterface	導入	データベースホストの作成
	EC2: DeleteSecurityGroup	導入	データベースホストの作成
	EC2:タグを削除します	導入	データベースホストの作成
	EC2：DeleteVolume	導入	データベースホストの作成
	EC2：DetachNetworkInterface	導入	データベースホストの作成
	EC2：DetachVolumeの場合	導入	データベースホストの作成
	EC2：アソシエーション解除アドレス	導入	データベースホストの作成
	EC2: DisassociateIamInstanceProfile	導入	データベースホストの作成
	EC2：関連付け解除ルートテーブル	導入	データベースホストの作成
	EC2：SubnetCidrBlockの関連付けを解除	導入	データベースホストの作成
	EC2：VpcCidrBlockの関連付けを解除	導入	データベースホストの作成
作成されたSQLインスタンスの属性を変更します。WLMDBで始まる名前にのみ適用されます。	EC2：ModifyInstanceAttribute	導入	運用と修復
	EC2：ModifyInstancePlacement	導入	データベースホストの作成
	EC2:ModifyNetworkInterfaceAttributeのいずれかです	導入	データベースホストの作成
	EC2：ModifySubnetAttribute	導入	データベースホストの作成
	EC2：ModifyVolume	導入	データベースホストの作成
	EC2：ModifyVolumeAttributeのことです	導入	データベースホストの作成
	EC2：ModifyVpcAttribute	導入	データベースホストの作成

目的	アクション	使用先	許可ポリシー
検証インスタンスの関連付けを解除して破棄する	EC2：リリースアドレス	導入	データベースホストの作成
	EC2：ReplaceRoute	導入	データベースホストの作成
	EC2：ReplaceRouteTableAssociation	導入	データベースホストの作成
	EC2: RevokeSecurityGroupEgress	導入	データベースホストの作成
	EC2: RevokeSecurityGroupIngress	導入	データベースホストの作成
導入されたインスタンスの開始	EC2：StartInstances（EC2：開始インスタンス	導入	運用と修復
導入されたインスタンスの停止	EC2：StopInstances	導入	運用と修復
WLMDBによって作成されたAmazon FSx for NetApp ONTAPリソースのカスタム値にタグを付けて、リソース管理時に課金の詳細を取得	FSx：TagResource [1]	• 導入 • カンリシヨリ	データベースホストの作成
導入用のCloudFormationテンプレートを作成して検証	CloudFormation：CreateStack	導入	データベースホストの作成
	CloudFormation：DescribeStackEvents	導入	データベースホストの作成
	CloudFormation：DescribeStack	導入	データベースホストの作成
	CloudFormation：リストスタック	導入	表示、計画、分析
	CloudFormation：ValidateTemplate	導入	データベースホストの作成
再試行およびロールバック用にネストされたスタックテンプレートを作成する	EC2：CreateLaunchTemplate	導入	データベースホストの作成
	EC2：CreateLaunchTemplateVersion	導入	データベースホストの作成
作成したインスタンスのタグとネットワークセキュリティを管理します。	EC2：CreateNetworkInterface	導入	データベースホストの作成
	EC2：CreateSecurityGroup	導入	データベースホストの作成
	ec2：CreateTags	導入	データベースホストの作成
プロビジョニング用のインスタンスの詳細を取得する	ec2:アドレスの説明	導入	表示、計画、分析
	ec2:起動テンプレートの説明	導入	表示、計画、分析

目的	アクション	使用先	許可ポリシー
作成したインスタンスの開始	EC2：RunInstances	導入	データベースホストの作成
プロビジョニングに必要なFSx for ONTAPリソースを作成します。既存のFSx for ONTAPシステムでは、SQLボリュームをホストするための新しいSVMが作成されます。	FSx：CreateFileSystem	導入	データベースホストの作成
	FSx：CreateStorageVirtualMachine	導入	データベースホストの作成
	FSx：ボリュームの作成	• 導入 • カンリシヨリ	データベースホストの作成
FSx for ONTAPの詳細	fsx:ファイルシステムエイリアスの説明	導入	データベースホストの作成
FSx for ONTAPファイルシステムのサイズを変更してファイルシステムのヘッドルームを修正	FSx：ファイルシステムの更新	最適化	運用と修復
ボリュームのサイズを変更してログとtempdbのドライブサイズを修正	FSx：UPDATEVOLUME	最適化	運用と修復
KMSの主要な詳細情報を入手し、FSx for ONTAPの暗号化に使用	KMS：CreateGrant	導入	データベースホストの作成
	kms:カスタムキーストアの説明	導入	データベースホストの作成
	KMS：GenerateDataKey	導入	データベースホストの作成
EC2インスタンスで実行される検証スクリプトとプロビジョニングスクリプト用にCloudWatchログを作成する	ログ:CreateLogGroup	導入	データベースホストの作成
	ログ:CreateLogStream	導入	データベースホストの作成
	ログ:GetLogGroupFields	導入	データベースホストの作成
	ログ:GetLogRecord	導入	データベースホストの作成
	ログ:ListLogDeliveries	導入	データベースホストの作成
	ログ:PutLogEvents	• 導入 • カンリシヨリ	データベースホストの作成
	ログ:TagResource	導入	データベースホストの作成

目的	アクション	使用先	許可ポリシー
Workload Factory は、SSM 出力の切り捨てが発生すると、SQL インスタンスの Amazon CloudWatch ログに切り替えます。	ログ:GetLogEvents	• ストレージ評価（最適化） • インベントリ	表示、計画、分析
Workload Factory が現在のロググループを取得し、Workload Factory によって作成されたロググループの保持が設定されていることを確認することを許可します。	ログ:DescriptionLogGroups	• ストレージ評価（最適化） • インベントリ	表示、計画、分析
Workload Factory が作成したロググループに 1 日間の保持ポリシーを設定できるようにして、SSM コマンド出力のログ ストリームの不要な蓄積を回避します。	ログ:PutRetentionPolicy	• ストレージ評価（最適化） • インベントリ	表示、計画、分析
カスタマーSNSのトピックを一覧表示し、WLMDBバックエンドSNSおよびカスタマーSNS（選択されている場合）に公開します。	SNS:リストトピック	導入	表示、計画、分析
	SNS：公開	導入	データベースホストの作成
プロビジョニングされたSQLインスタンスに対して検出スクリプトを実行し、FSx for ONTAPでサポートされるAWSリージョンの最新のリストを取得するために必要なSSM権限。	SSM：PutComplianceItems	導入	データベースホストの作成
	SSM：PutConfigurePackageResult	導入	データベースホストの作成
	SSM：PutInventory	導入	データベースホストの作成
	SSM：UpdateAssociationStatus	導入	データベースホストの作成
	SSM：UpdateInstanceAssociationStatus	導入	データベースホストの作成
	SSM：UpdateInstanceInformation	導入	データベースホストの作成
	ssmmessages:CreateControlChannel	導入	データベースホストの作成
	ssmmessages:データチャネルの作成	導入	データベースホストの作成
	ssmmessages:OpenControlChannel	導入	データベースホストの作成
	ssmmessages:OpenDataChannel	導入	データベースホストの作成

目的	アクション	使用先	許可ポリシー
成功または失敗時にCloudFormationスタックに信号を送信します。	CloudFormation：SignalResource [1]	導入	データベースホストの作成
テンプレートによって作成されたEC2ロールをEC2のインスタンスプロファイルに追加して、EC2上のスクリプトが展開に必要なリソースにアクセスできるようにします。	IAM：AddRoleToInstanceProfile	導入	データベースホストの作成
EC2のインスタンスプロファイルを作成し、作成したEC2ロールを割り当てます。	IAM：CreateInstanceProfile	導入	データベースホストの作成
以下の権限を持つテンプレートを使用してEC2ロールを作成する	IAM：CREATEROLE	導入	データベースホストの作成
EC2サービスにリンクされたロールの作成	IAM：CreateServiceLinkedRole[2]	導入	データベースホストの作成
検証ノード専用に導入時に作成されたインスタンスプロファイルを削除する	IAM：DeleteInstanceProfile	導入	データベースホストの作成
ロールとポリシーの詳細を取得して権限のギャップを特定し、導入のための検証を実施	IAM：GetPolicy	導入	データベースホストの作成
	IAM：GetPolicyVersion	導入	データベースホストの作成
	IAM：GetRole	導入	データベースホストの作成
	IAM：GetRolePolicy	導入	データベースホストの作成
	IAM：GetUser	導入	データベースホストの作成
作成したロールをEC2インスタンスに渡す	IAM：PassRole[3]	導入	データベースホストの作成
作成したEC2ロールに必要な権限を含むポリシーを追加します。	IAM：PutRolePolicy	導入	データベースホストの作成
プロビジョニングされたEC2インスタンスプロファイルからロールを切り離す	IAM：RemoveRoleFromInstanceProfile	導入	データベースホストの作成
ワークロードの処理をシミュレートして使用可能な権限を検証し、必要なAWSアカウントの権限と比較	IAM：SimulatePrincipalPolicy	導入	全て
エラーログ分析に使用できる基礎モデルを取得する	Bedrock：GetFoundationModelAvailability	エラーログ分析	表示、計画、分析

目的	アクション	使用先	許可ポリシー
エラーログ分析のために Amazon Bedrock で利用可能なインターフェースプロファイルを一覧表示する	Bedrock: ListInferenceProfiles	エラーログ分析	表示、計画、分析

1. アクセス許可は、WLMDBで始まるリソースに制限されます。
2. IAM：AWSServiceNameによって制限される「IAM：CreateServiceLinkedRole」：ec2.amazonaws.com"*
3. 「IAM：PassRole」は「IAM：PassedToService」によって制限されます：ec2.amazonaws.com"*

生成**AI**ワークロードの権限

VMware ワークロードの IAM ポリシーは、運用モードに基づいて、パブリック クラウド環境内のリソースとプロセスを管理するために Workload Factory for VMware に必要な権限を提供します。

GenAI IAM ポリシーは、読み取り/書き込み 権限でのみ使用できます。

- 読み取り/書き込み: 実行に必要な検証済みの権限を持つ割り当てられた認証情報を使用して、お客様に代わって AWS で操作を実行し、自動化します。

生成AIワークロードのIAMポリシー

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

次の表に、生成AIワークロードの権限の詳細を示します。

生成**AI**ワークロードの権限の一覧

目的	アクション	使用先	許可ポリシー
導入時と再構築時にAIエンジンCloudFormationスタックを作成	CloudFormation：CreateStack	導入	読み取り / 書き込み
AIエンジンCloudFormationスタックを作成	CloudFormation：DescribeStack	導入	読み取り / 書き込み
AIエンジン導入ウィザードのリージョンを表示する	EC2: DescribeRegions (説明領域	導入	読み取り / 書き込み
AIエンジンタグを表示	EC2: DescribeTags (説明タグ)	導入	読み取り / 書き込み
S3バケットの一覧	S3 ： ListAllMyBuckets	導入	読み取り / 書き込み
AIエンジンスタックを作成する前にVPCエンドポイントをリスト表示	EC2：CreateVpcEndpoint	導入	読み取り / 書き込み
導入時と再構築時のAIエンジンスタックの作成時にAIエンジンセキュリティグループを作成	EC2：CreateSecurityGroup	導入	読み取り / 書き込み
導入および再構築処理中にAIエンジンスタックの作成によって作成されたリソースにタグを付ける	ec2：CreateTags	導入	読み取り / 書き込み
暗号化されたイベントをAIエンジンスタックからWLMAIバックエンドにパブリッシュする	KMS：GenerateDataKey	導入	読み取り / 書き込み
	KMS：復号化	導入	読み取り / 書き込み
イベントとカスタムリソースをAIエンジンスタックからWLMAIバックエンドにパブリッシュする	SNS：公開	導入	読み取り / 書き込み
[List VPC during AI engine deployment]ウィザード	EC2: DescribeVpcs	導入	読み取り / 書き込み
AIエンジン導入ウィザードでサブネットを一覧表示する	EC2: DescribeSubnets	導入	読み取り / 書き込み
AIエンジンの導入時と再構築時にルーティングテーブルを取得	EC2: DescribeRouteTables	導入	読み取り / 書き込み
AIエンジン導入ウィザードでのキーペアの一覧表示	EC2：DescribeKeyPairs	導入	読み取り / 書き込み
AIエンジンスタックの作成中にセキュリティグループをリスト表示する（プライベートエンドポイントでセキュリティグループを検索する）	EC2: DescribeSecurityGroups	導入	読み取り / 書き込み

目的	アクション	使用先	許可ポリシー
VPCエンドポイントを取得して、AIエンジンの導入時に作成する必要があるかどうかを判断する	EC2: DescribeVpcEndpoints	導入	読み取り / 書き込み
Amazon Q Businessアプリケーションを挙げる	qbusiness：ListApplications	導入	読み取り / 書き込み
インスタンスを表示してAIエンジンの状態を確認する	EC2: DescribeInstances	トラブルシューティング	読み取り / 書き込み
導入時と再構築時のAIエンジンスタック作成時のイメージをリスト表示	EC2: DescribeImages	導入	読み取り / 書き込み
導入および再構築処理中のAIインスタンススタックの作成中に、AIインスタンスとプライベートエンドポイントセキュリティグループを作成および更新	EC2: RevokeSecurityGroupEgress	導入	読み取り / 書き込み
	EC2: RevokeSecurityGroupIngress	導入	読み取り / 書き込み
導入および再構築処理中にCloudFormationスタックの作成中にAIエンジンを実行	EC2：RunInstances	導入	読み取り / 書き込み
導入時や再構築時のスタック作成時に、セキュリティグループを追加してAIエンジンのルールを変更	ec2：AuthorizeSecurityGroupEgress	導入	読み取り / 書き込み
	ec2：AuthorizeSecurityGroupIngress	導入	読み取り / 書き込み
基本モデルのいずれかに対してチャットリクエストを開始する	Bedrock：InvokeModelWithResponseStream	導入	読み取り / 書き込み
基礎モデルのチャット/埋め込みリクエストの開始	Bedrock：InvokeModel	導入	読み取り / 書き込み
リージョンで使用可能な基盤モデルを表示する	Bedrock: ListFoundationModels	導入	読み取り / 書き込み
基盤モデルに関する情報を取得する	Bedrock：GetFoundationModel	導入	読み取り / 書き込み
基盤モデルへのアクセスを確認	Bedrock：GetFoundationModelAvailability	導入	読み取り / 書き込み
導入と再構築の処理中にAmazon CloudWatchロググループを作成する必要があることを確認	ログ:DescriptionLogGroups	導入	読み取り / 書き込み
AIエンジンウィザードでFSxとAmazon Bedrockをサポートするリージョンを取得	SSM：GetParametersByPath	導入	読み取り / 書き込み
導入時と再構築時にAIエンジンを導入するための最新のAmazon Linuxイメージを入手	SSM：GetParameters	導入	読み取り / 書き込み

目的	アクション	使用先	許可ポリシー
AIエンジンに送信されたコマンドからSSM応答を取得する	SSM：GetCommandInvocation	導入	読み取り / 書き込み
AIエンジンへのSSM接続を確認する	SSM:sendCommand	導入	読み取り / 書き込み
	SSM：GetConnectionStatus	導入	読み取り / 書き込み
導入および再構築処理中のスタック作成時にAIエンジンインスタンスプロファイルを作成	IAM：CREATEROLE	導入	読み取り / 書き込み
	IAM：CreateInstanceProfile	導入	読み取り / 書き込み
	IAM：AddRoleToInstanceProfile	導入	読み取り / 書き込み
	IAM：PutRolePolicy	導入	読み取り / 書き込み
	IAM：GetRolePolicy	導入	読み取り / 書き込み
	IAM：GetRole	導入	読み取り / 書き込み
	IAM：TagRole	導入	読み取り / 書き込み
	IAM：PassRole	導入	読み取り / 書き込み
ワークロードの処理をシミュレートして使用可能な権限を検証し、必要なAWSアカウントの権限と比較	IAM：SimulatePrincipalPolicy	導入	読み取り / 書き込み
「ナレッジベースの作成」ウィザードでFSx for ONTAPファイルシステムを確認する	FSx：Description	ナレッジベースの作成	読み取り / 書き込み
「ナレッジベースの作成」ウィザードでFSx for ONTAPファイルシステムのボリュームを確認する	FSx：DescriptionFileSystems	ナレッジベースの作成	読み取り / 書き込み
再構築処理中にAIエンジンを基盤としたナレッジベースを管理	FSx：ListTagsForResource	トラブルシューティング	読み取り / 書き込み
「ナレッジベースの作成」ウィザードでFSx for ONTAPファイルシステムStorage Virtual Machineを確認する	FSx：DescriptionStorageVirtualMachines	導入	読み取り / 書き込み
ナレッジベースを新しいインスタンスに移動	FSx：UntagResource	トラブルシューティング	読み取り / 書き込み
再構築時にAIエンジンに関するナレッジベースを管理	FSx：TagResource	トラブルシューティング	読み取り / 書き込み

目的	アクション	使用先	許可ポリシー
SSMシークレット（ECRトークン、CIFSクレデンシャル、テナンシーサービスアカウントキー）をセキュアな方法で保存	SSM:getParameter	導入	読み取り / 書き込み
	SSM：PutParameter	導入	読み取り / 書き込み
導入と再構築の処理中に、AIエンジンのログをAmazon CloudWatchロググループに送信	ログ:CreateLogGroup	導入	読み取り / 書き込み
	ログ:PutRetentionPolicy	導入	読み取り / 書き込み
AIエンジンのログをAmazon CloudWatchロググループに送信する	ログ:TagResource	トラブルシューティング	読み取り / 書き込み
Amazon CloudWatchからSSMの応答を取得する（応答が長すぎる場合）	ログ:DescriptionLogStreams	トラブルシューティング	読み取り / 書き込み
Amazon CloudWatchからSSMの応答を入手	ログ:GetLogEvents	トラブルシューティング	読み取り / 書き込み
デプロイおよび再構築処理中のスタック作成時に、Amazon Bedrockログ用のAmazon CloudWatchロググループを作成する	ログ:CreateLogGroup	導入	読み取り / 書き込み
	ログ:PutRetentionPolicy	導入	読み取り / 書き込み
	ログ:TagResource	導入	読み取り / 書き込み
モデルの推論プロファイルをリスト表示	Bedrock: ListInferenceProfiles	トラブルシューティング	読み取り / 書き込み

VMwareワークロードの権限

VMware ワークロードでは、次の権限ポリシーから選択できます。

- 表示、計画、分析: EVS 仮想化環境のインベントリを表示し、システムの Well-Architected 分析を取得して、コスト削減を検討します。
- データストアのデプロイと接続: 推奨される VM レイアウトを Amazon EVS、Amazon EC2、または VMware Cloud on AWS vSphere クラスターにデプロイし、カスタマイズされたAmazon FSx for NetApp ONTAPファイルシステムを外部データストアとして使用します。

必要な IAM ポリシーを表示するには、権限ポリシーを選択します。

VMwareワークロードのIAMポリシー

表示、計画、分析

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

データストアの展開と接続

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

次の表に、VMwareワークロードの権限の詳細を示します。

VMwareワークロードの権限の一覧

目的	アクション	使用先	許可ポリシー
プロビジョニングされたノードのセキュリティグループを接続してルールを変更する	ec2 ：AuthorizeSecurityGroupIngress	導入	データストアの展開と接続
EBSボリュームを作成する	FSx：ボリュームの作成	導入	データストアの展開と接続
VMwareワークロードによって作成されたFSx for NetApp ONTAPリソースのカスタム値にタグを付ける	FSx：TagResource	導入	データストアの展開と接続
CloudFormationテンプレートの作成と検証	CloudFormation：CreateStack	導入	データストアの展開と接続
作成したインスタンスのタグとネットワークセキュリティを管理します。	EC2：CreateSecurityGroup	導入	データストアの展開と接続
作成したインスタンスの開始	EC2：RunInstances	導入	データストアの展開と接続
EC2インスタンスの詳細を取得	EC2: DescribeInstances	インベントリ	データストアの展開と接続
展開および再構築操作中のスタック作成中のイメージのリスト表示	EC2: DescribeImages	インベントリ	データストアの展開と接続
VPC に関連付けられた DHCP オプション セットの構成の詳細を表示します	ec2:Dhcpオプションの説明	インベントリ	表示、計画、分析
選択した環境内のVPCを取得して導入フォームに記入	EC2: DescribeVpcs	• 導入 • インベントリ	表示、計画、分析
選択した環境のサブネットを取得して導入フォームに記入	EC2: DescribeSubnets	• 導入 • インベントリ	表示、計画、分析
選択した環境のセキュリティグループを取得して、展開フォームに入力します。	EC2: DescribeSecurityGroups	導入	表示、計画、分析
選択した環境のアベイラビリティゾーンを取得する	EC2：説明AvailabilityZones	• 導入 • インベントリ	表示、計画、分析
Amazon FSx for NetApp ONTAPのサポートリージョンを取得	EC2: DescribeRegions (説明領域	導入	表示、計画、分析

目的	アクション	使用先	許可ポリシー
Amazon FSx for NetApp ONTAP の暗号化に使用するKMSキーのエイリアスを取得する	KMS：エイリアスを確認する	導入	表示、計画、分析
Amazon FSx for NetApp ONTAP の暗号化に使用するKMSキーを入手	KMS：ListKeys	導入	表示、計画、分析
Amazon FSx for NetApp ONTAP の暗号化に使用するKMSキーの有効期限の詳細を取得	KMS:説明キー	導入	表示、計画、分析
AWS Secrets Manager でシークレットを一覧表示する	secretsmanager:ListSecrets	インベントリ	表示、計画、分析
Amazon EVSから環境のリストを取得する	evs:ListEnvironments	インベントリ	表示、計画、分析
特定の Amazon EVS 環境に関する詳細情報を取得する	evs:環境を取得する	インベントリ	表示、計画、分析
Amazon EVS 環境に関連付けられた VLAN を一覧表示する	evs:環境Vlansのリスト	インベントリ	表示、計画、分析
プロビジョニングに必要なAmazon FSx for NetApp ONTAPリソースを作成する	FSx：CreateFileSystem	導入	データストアの展開と接続
	FSx：CreateStorageVirtualMachine	導入	データストアの展開と接続
	FSx：ボリュームの作成	• 導入 • カンリシヨリ	データストアの展開と接続
Amazon FSx for NetApp ONTAP の詳細	FSx：説明*	• 導入 • インベントリ • カンリシヨリ • コスト削減の詳細	データストアの展開と接続

目的	アクション	使用先	許可ポリシー
KMSの主要な詳細情報を入手し、Amazon FSx for NetApp ONTAPの暗号化に使用	KMS：CreateGrant	導入	データストアの展開と接続
	KMS：説明*	導入	表示、計画、分析
	KMS：リスト*	導入	表示、計画、分析
	KMS：復号化	導入	データストアの展開と接続
	KMS：GenerateDataKey	導入	データストアの展開と接続
カスタマーSNSのトピックを一覧表示し、WLMVMCバックエンドSNSおよびカスタマーSNS（選択されている場合）に公開します。	SNS：公開	導入	データストアの展開と接続
ワークロードの処理をシミュレートして使用可能な権限を検証し、必要なAWSアカウントの権限と比較	IAM：SimulatePrincipalPolicy	導入	• データストアの展開と接続 • 表示、計画、分析

変更ログ

権限が追加および削除されると、以下のセクションにそれらの権限が表示されます。

2025年2月1日

ストレージ ワークロードに次の権限が追加されました。

- `s3:TagResource`
- `s3:ListTagsForResource`
- `s3:UntagResource`
- `s3tables:CreateTableBucket`
- `s3tables:ListTables`
- `s3tables:GetTable`
- `s3tables:GetTableMetadataLocation`
- `s3tables:CreateTable`
- `s3tables:GetNamespace`
- `s3tables:PutTableData`
- `s3tables:CreateNamespace`

- s3tables:GetTableData
- s3tables:ListNamespaces
- s3tables:ListTableBuckets
- s3tables:GetTableBucket
- s3tables:UpdateTableMetadataLocation
- s3tables:ListTagsForResource
- s3tables:TagResource
- s3:GetObjectTagging
- s3:ListBucket

2025年12月4日

ストレージ ワークロードに次の権限が追加されました。

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

2025年11月27日

ストレージ ワークロードに次の権限が追加されました。

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

2025年11月2日

ストレージ、データベース ワークロード、および VMware ワークロードの権限ポリシー「読み取り専用」および「読み取り/書き込み」が置き換えられ、権限の割り当てにおける細分性と柔軟性が向上しました。

2025年10月5日

以下の権限は GenAI から削除され、現在は GenAI エンジンによって処理されます。

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

2025年6月29日

データベースの 読み取り専用 モードで次の権限が利用できるようになりました。 `cloudwatch:GetMetricData` 。

2025年6月3日

GenAI の 読み取り/書き込み モードで次の権限が利用できるようになりました。 `s3:ListAllMyBuckets` 。

2025年5月4日

GenAI の 読み取り/書き込み モードで次の権限が利用できるようになりました。 `qbusiness:ListApplications` 。

データベースの 読み取り専用 モードで、次の権限が使用できるようになりました。

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

データベースの 読み取り/書き込み モードで次の権限が利用できるようになりました。 `logs:PutRetentionPolicy` 。

2025年4月2日

データベースの 読み取り専用 モードで次の権限が利用できるようになりました。 `ssm:DescribeInstanceInformation` 。

2025年3月30日

生成AIワークロード権限の更新

GenAI の 読み取り/書き込みモード では、次の権限が利用できるようになりました。

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

GenAI の 読み取り/書き込みモード から次の権限が削除されました: `Bedrock:GetFoundationModel` 。

IAM：SimulatePrincipalPolicy権限の更新

その `iam:SimulatePrincipalPolicy`追加の AWS アカウント認証情報を追加するとき、または Workload Factory コンソールから新しいワークロード機能を追加するときに自動アクセス許可チェックを有効にすると、アクセス許可はすべてのワークロードアクセス許可ポリシーの一部になります。この権限は、ワークロード操作をシミュレートし、Workload Factory からリソースをデプロイする前に、必要な AWS アカウント権限があるかどうかを確認します。このチェックを有効にすると、失敗した操作からリソースをクリーンアップしたり、不足している権限を追加したりするために必要な時間と労力が削減されます。

2025年3月2日

GenAI の 読み取り/書き込み モードで次の権限が利用できるようになりました。
`bedrock:GetFoundationModel` 。

2025年2月3日

データベースの 読み取り専用 モードで次の権限が利用できるようになりました。
`iam:SimulatePrincipalPolicy` 。

著作権に関する情報

商標に関する情報