NetAppワークロード ファクトリーのセットアップおよび管理ドキュメント

Setup and administration

NetApp
March 02, 2026

This PDF was generated from https://docs.netapp.com/ja-jp/workload-setup-admin/index.html on March 02, 2026. Always check docs.netapp.com for the latest.

目次

NetAppワークロード ファクトリーのセットアップおよび管理ドキュメント 1
リリースノート 2
NetApp Workload Factory 管理機能の新機能 2
2026年3月1日 2
2026年2月1日 2
2026年1月4日 3
2025年11月27日 3
2025年10月6日 3
2025年10月5日 4
2025年9月9日 4
2025年6月29日 4
2025年5月4日 4
2025年3月30日 5
2025年2月2日 5
2025年1月22日 5
2025年1月5日 5
2024年11月11日 6
2024年9月1日 6
2024 年 8 月 4 日 7
2024年7月7日 7
はじめに 8
基本事項をご確認ください 8
NetAppワークロードファクトリーについて学ぶ 8
コンソールエクスペリエンス 12
NetApp Workload Factory の権限 13
NetApp Workload Factory のクイックスタート 63
NetApp Workload Factory にサインアップ 63
ワークロードファクトリーにサインアップ 64
Workload Factoryのアカウントに他のユーザーを招待する 66
Workload FactoryにAWS認証情報を追加する 66
概要 66
AWS クレデンシャル 67
アカウントへのクレデンシャルの手動追加 67
CloudFormationを使用してアカウントにクレデンシャルを追加する 70
NetApp Workload Factoryでワークロードを最適化 73
ワークロードファクトリーの管理 74
NetAppワークロードファクトリーにログイン 74
サービスアカウントの管理 74
サービスアカウントを作成します 75

サービスアカウントを削除します 76
適切に設計されたワークロードを構築および運用する 76
仕組み 77
なぜそれが重要なのか 77
Workload Factory を使って誤った構成を検出し修正しましょう 77
ストレージワークロードのベストプラクティスと推奨事項 77
データベースワークロードのベストプラクティスと推奨事項 80
EVS ワークロードのベストプラクティスと推奨事項 84
関連情報 85
NetApp Workload Factory 通知を構成する 85
通知の種類とメッセージ 86
ワークロードファクトリーの通知を構成する 88
Amazon SNSトピックを購読する 89
通知をフィルタリングします 89
Codeboxを使用したタスクの自動化 91
コードボックス自動化の詳細 91
NetApp Workload Factory の自動化に Codebox を使用する 92
NetApp Workload Factory で CloudShell を使用する 95
タスクの内容 96
CloudShellコマンド 96
開始する前に 97
CloudShellを導入する 97
CloudShellセッションタブの名前変更 99
CloudShellセッションタブの複製 99
CloudShellセッションのタブを閉じる 100
CloudShellセッションタブの分割 100
CloudShellセッションの設定の更新 100
NetApp Workload Factory から資格情報を削除する 101
知識とサポート 102
サポートに登録します 102
サポート登録の概要 102
NetAppサポートのアカウントを登録する 102
ヘルプを表示します 104
FSx for ONTAPのサポートを利用する 104
セルフサポートオプションを使用します 104
ネットアップサポートと一緒にケースを作成します 105
サポートケースの管理（プレビュー） 107
NetApp Workload Factory に関する法的通知 110
著作権 110
商標 110
特許 110

プライバシーポリシー 110
オープンソース 110

NetAppワークロード ファクトリーのセットアップおよび管理ドキュメント

リリースノート

NetApp Workload Factory 管理機能の新機能

Workload Factory 管理機能の新機能（クラウド プロバイダーの資格情報、Codebox の機能強化など）について説明します。

2026年3月1日

Workload Factory で新しい **Ask Me** ブックマークが利用可能になりました

Workload Factory コンソールのすべての画面に新しい Ask Me ブックマークを追加しました。この改善により、ヘルプが必要なときにいつでも Ask Me に簡単かつ迅速にアクセスできるようになります。Ask Me は AI アシスタントであり、独自のワークロード環境について質問したり、環境から直接パーソナライズされた分析情報を取得したり、以前の会話を参照したりすることができます。

新しいブックマークをクリックすると、どのページからでも Ask Me を開くことができます。現在の作業を中断することなく、サイドパネルで Ask me を起動し、現在行っている作業に関連する簡単な説明と推奨事項を提供します。

"Ask Meの詳細"

2026年2月1日

適切に設計されたアップデート

NetApp Workload Factory には、Elastic VMware Service（EVS）ワークロード向けの Well-Architected 評価が含まれており、ストレージおよびデータベース ワークロードの新しい構成が追加されています。

- **VMware** ワークロード NetApp Workload Factory は、適切に設計された Amazon Elastic VMware Service（EVS） ワークロードを運用するためのベストプラクティスと推奨事項を提供します。

  "適切に設計されたEVS構成を実装する"

- ストレージワークロード ストレージワークロードのWell-Architected機能にいくつかの新しい構成が追加され、ストレージのパフォーマンスとコストをより深く理解できるようになりました。
  - Storage VM論理レポート
  - キャッシュボリュームのサイズを最適化する
  - 孤立したブロックデバイス

    "Storage ワークロードに適したファイルシステム構成を実装する"

- データベース ワークロード Workload Factory for Databases には、Direct NFS（dNFS）を有効にして設定し、I/O パフォーマンスを向上させ、ホストとストレージ システムの負荷を軽減するための、Oracle の新しいストレージ構成が含まれています。
  - dNFSの有効化
  - dNFS 一貫性のある IP 解決

- dNFS設定ファイル
- dNFS `nosharecache`

  "適切に設計されたデータベースワークロードを実装する"

Storage の新しい権限

S3 アクセスポイントの管理を強化するために、Storage ワークロードに新しい権限が追加されました。

"アクセス権参照変更ログ"

2026年1月4日

Ask me AIアシスタントのホームページ統合

Workload Factory コンソールのホームページには Ask me AI アシスタントが組み込まれており、独自のストレージ資産について質問したり、環境から直接パーソナライズされた分析情報を取得したり、以前の会話を参照したりすることができます。コンソールを離れることなく、「Ask me」と対話してワークロードを理解し、問題をトラブルシューティングし、Workload Factory について詳しく知ることができます。

2025年11月27日

ストレージの権限の更新

FSx for ONTAP EMS イベント アナライザーは、*operations and remediation* 権限ポリシーの次の Amazon Bedrock 権限を使用して、ストレージ ワークロードのイベント データを取得します。

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

"アクセス権参照変更ログ"

2025年10月6日

BlueXP workload factoryが**NetApp**ワークロードファクトリーに

BlueXP は、データ インフラストラクチャの管理における役割をより適切に反映するために、名前が変更され、再設計されました。その結果、 BlueXP workload factoryの名前がNetAppワークロード ファクトリーに変更されました。

MCP との **Ask Me** 統合

Workload Factory の AI アシスタントである Ask Me は、Model Context Protocol (MCP) と統合されています。 MCP を使用することで、Ask Me は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。

2025年10月5日

ストレージの新しい通知

NetApp Workload Factory 通知サービスには、ストレージの Well-Architected の問題に関する通知が含まれています。

"NetApp Workload Factory の通知"

2025年9月9日

ストレージの新しい通知

BlueXP workload factory通知サービスには、ストレージの自動容量管理に関する通知が含まれています。

"BlueXP workload factoryの通知"

2025年6月29日

データベースの権限の更新

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` 。

"アクセス権参照変更ログ"

BlueXPワークロードファクトリー通知サービスのサポート

BlueXP ワークロードファクトリー通知サービスを使用すると、ワークロードファクトリーは BlueXP アラートサービスまたは Amazon SNS トピックに通知を送信できます。BlueXPアラートに送信された通知は、BlueXP アラートパネルに表示されます。ワークロードファクトリーが Amazon SNS トピックに通知を発行すると、トピックのサブスクライバー（ユーザーや他のアプリケーションなど）は、トピックに設定されたエンドポイント（E メールや SMS メッセージなど）で通知を受け取ります。

"BlueXPワークロードファクトリー通知を構成する"

2025年5月4日

CloudShellオートコンプリートのサポート

BlueXP ワークロードファクトリCloudShellを使用している場合は、コマンドの入力を開始してTabキーを押すと、使用可能なオプションが表示されます。複数の候補が存在する場合は、CLIに候補のリストが表示されます。この機能は、エラーを最小限に抑え、コマンド実行を高速化することで、生産性を向上させます。

権限に関する用語を更新

ワークロード ファクトリのユーザー インターフェースとドキュメントでは、読み取り権限を示すために「読み取り専用」を使用し、自動化権限を示すために「読み取り/書き込み」を使用するようになりました。

2025年3月30日

ONTAP CLIコマンドについて、**AI**によって生成されたエラー応答が**CloudShell**で報告される

CloudShellを使用している場合、ONTAP CLIコマンドを発行してエラーが発生するたびに、失敗の説明、失敗の原因、詳細な解決策を含むAI生成のエラー応答を取得できます。

"CloudShellを使用"

IAM：SimulatePermissionPolicy権限の更新

AWSアカウントのクレデンシャルを追加したり、生成AIワークロードなどの新しいワークロード機能を追加したりするときに、ワークロードファクトリコンソールから権限を管理できるようになりまし`iam:SimulatePrincipalPolicy`た。

"アクセス権参照変更ログ"

2025年2月2日

BlueXP Workload Factoryコンソールで**CloudShell**を使用可能

CloudShellは、BlueXP ワークロードファクトリコンソールのどこからでも使用できます。CloudShellを使用すると、BlueXP アカウントで提供したAWSとONTAPのクレデンシャルを使用して、シェルに似た環境でAWS CLIコマンドまたはONTAP CLIコマンドを実行できます。

"CloudShellを使用"

データベースの権限の更新

データベースの_read_modeで次の権限を使用できるようになりました `iam:SimulatePrincipalPolicy`。

"アクセス権参照変更ログ"

2025年1月22日

BlueXP ワークロードの工場出荷時の権限

ストレージ環境の検出から、ストレージ内のファイルシステムや 生成AIワークロードのナレッジベースなどのAWSリソースの導入まで、BlueXP ワークロードファクトリでさまざまな処理を実行するために使用される権限を確認できるようになりました。ストレージ、データベース、VMware、生成AIの各ワークロードのIAMポリシーと権限を表示できます。

"BlueXP ワークロードの工場出荷時の権限"

2025年1月5日

BlueXP Workload Factoryでのサービスアカウントのサポート

BlueXP ワークロードファクトリでサービスアカウントがサポートされるようになりました。サービスアカウントを作成して、インフラの運用を自動化するマシンユーザとして機能させることができます。

"サービスアカウントを作成および管理します"

2024年11月11日

BlueXP コンソールにワークロードを工場出荷時に統合

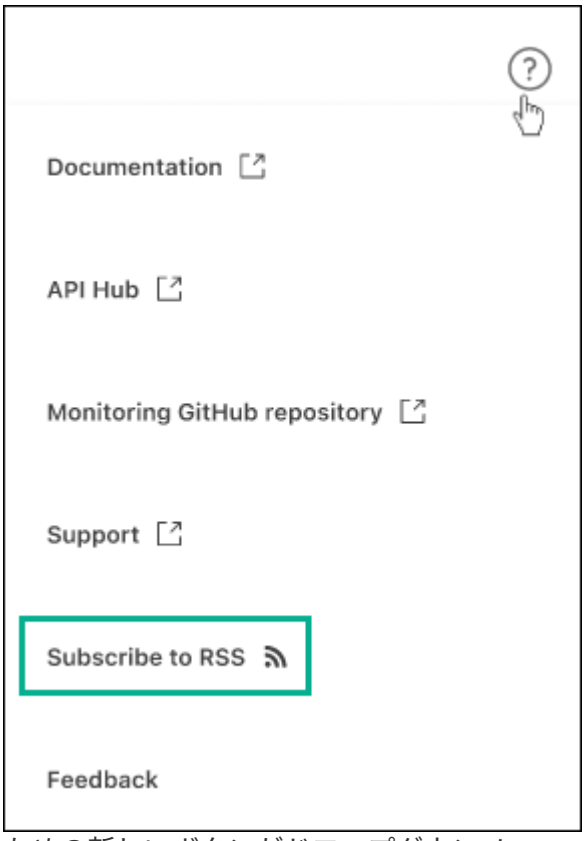
これで、からワークロードファクトリを使用できるようになり"BlueXPコンソール"ます。BlueXP コンソールエクスペリエンスは、ワークロードファクトリコンソールと同じ機能を提供します。

"BlueXP コンソールからワークロードファクトリにアクセスする方法"

2024年9月1日

RSSサブスクリプション

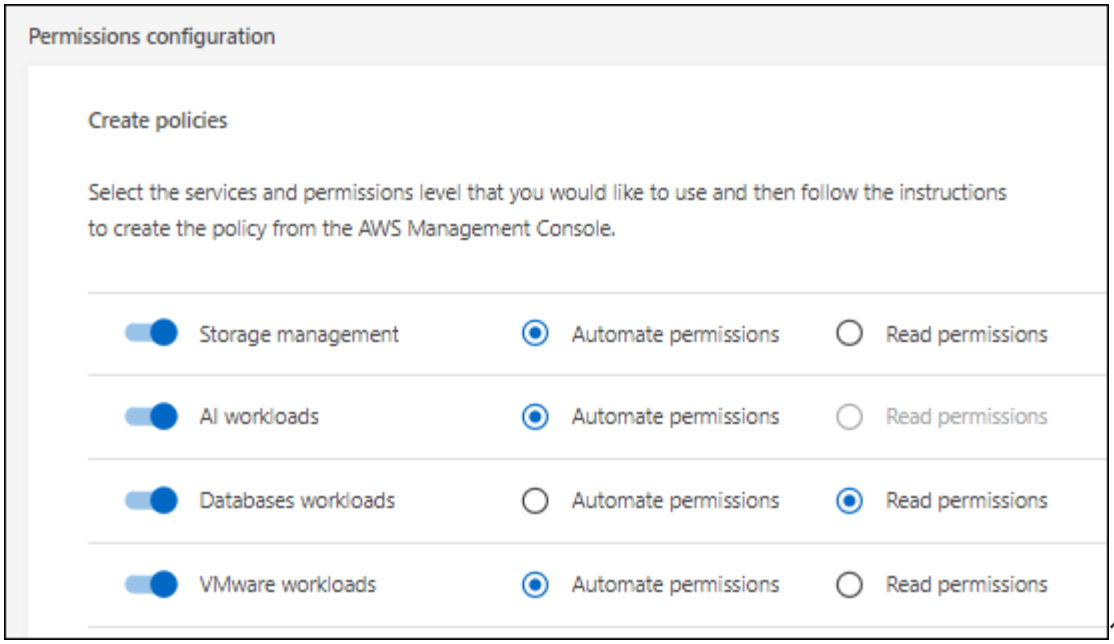
RSSサブスクリプションは、から利用でき"ワークロードファクトリコンソール"ます。RSSフィードを使用すると、BlueXP ワークロードファクトリの変化を簡単に把握して把握できます。



ドロップダウンメニューのスクリーンショットRSSを購読するための新しいボタンがドロップダウンメニューにオプションとして表示されます。"]

ワークロードごとに**1**つの権限ポリシーをサポート

ワークロード工場でAWSクレデンシャルを追加する際に、ワークロードとストレージ管理ごとに読み取りモードまたは自動モードのいずれか1つの権限ポリシーを選択できるようになりました。



ページの権限設定セクションのスクリーンショット。ストレージ管理、AIワークロード、データベースワークロード、VMwareワークロードの権限ポリシーの読み取りまたは自動化を選択できます。"]

"ワークロードファクトリへのAWSクレデンシャルの追加"

2024 年 8 月 4 日

Terraformのサポート

Terraformは、Amazon FSx for NetApp ONTAPファイルシステムの導入とStorage VMの作成で利用できます。セットアップガイドと管理ガイドに、CodeboxからTerraformを使用する方法が記載されました。

"コードボックスからTerraformを使用"

2024年7月7日

BlueXP Workload Factoryの初回リリース

BlueXP 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するために設計された、強力なライフサイクル管理プラットフォームです。ワークロードファクトリと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。

はじめに

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。

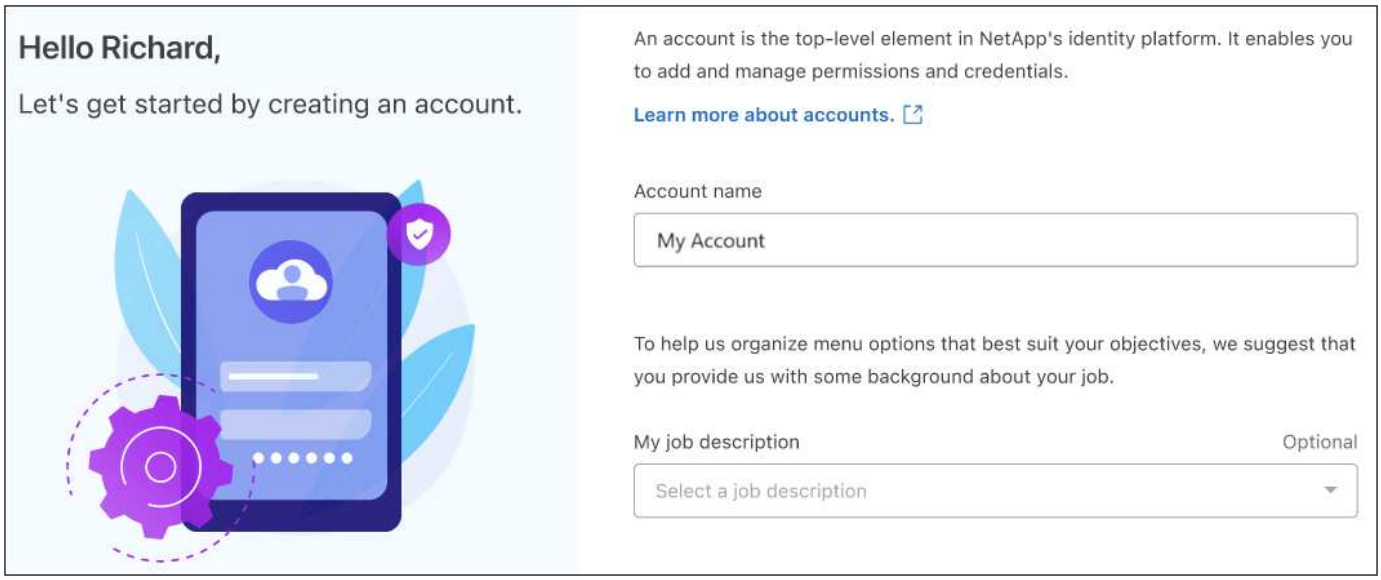
ソフトウェアサービス

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。

データベースワークロードのIAMポリシー

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。

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` 。

NetApp Workload Factory のクイックスタート

NetApp Workload Factory の使用を開始するには、サインアップしてアカウントを作成し、Workload Factory が AWS リソースを直接管理できるように認証情報を追加し、Amazon FSx for NetApp ONTAPを使用してワークロードを最適化します。

NetApp Workload Factory は、Web ベースのコンソールからクラウド サービスとしてユーザーがアクセスできます。始める前に、以下のことを理解しておく必要があります。"ワークロードファクトリー" 。

1 サインアップしてアカウントを作成する

に行く "ワークロードファクトリーコンソール"サインアップしてアカウントを作成してください。

"サインアップしてアカウントを作成する方法について説明します"です。

2 **Workload Factory**に**AWS**認証情報を追加する

この手順はオプションです。AWS アカウントにアクセスするための認証情報を追加しなくても、Workload Factory を使用できます。 Workload Factory に AWS 認証情報を追加すると、FSx for ONTAPファイルシステムの作成と管理、およびデータベースや GenAI などの特定のワークロードの導入と管理に必要な権限が Workload Factory アカウントに付与されます。

"アカウントにクレデンシャルを追加する方法"です。

3 **FSx for ONTAP**でワークロードを最適化

サインアップしてアカウントを作成し、オプションで AWS 認証情報を追加したら、Workload Factory を使用して FSx for ONTAPでワークロードを最適化できるようになります。

"FSx for ONTAPでワークロードを最適化" 。

NetApp Workload Factory にサインアップ

NetApp Workload Factory には、Web ベースのコンソールからアクセスできます。Workload Factory を使い始めるときの最初のステップは、既存のNetAppサポート サイトの認証情報を使用してサインアップするか、 NetAppクラウド ログインを作成することです。

他のユーザーを Workload Factory アカウントに招待して、Workload Factory にアクセスして使用できるようにすることもできます。

ワークロードファクトリーにサインアップ

次のいずれかのオプションを使用して Workload Factory にサインアップできます。

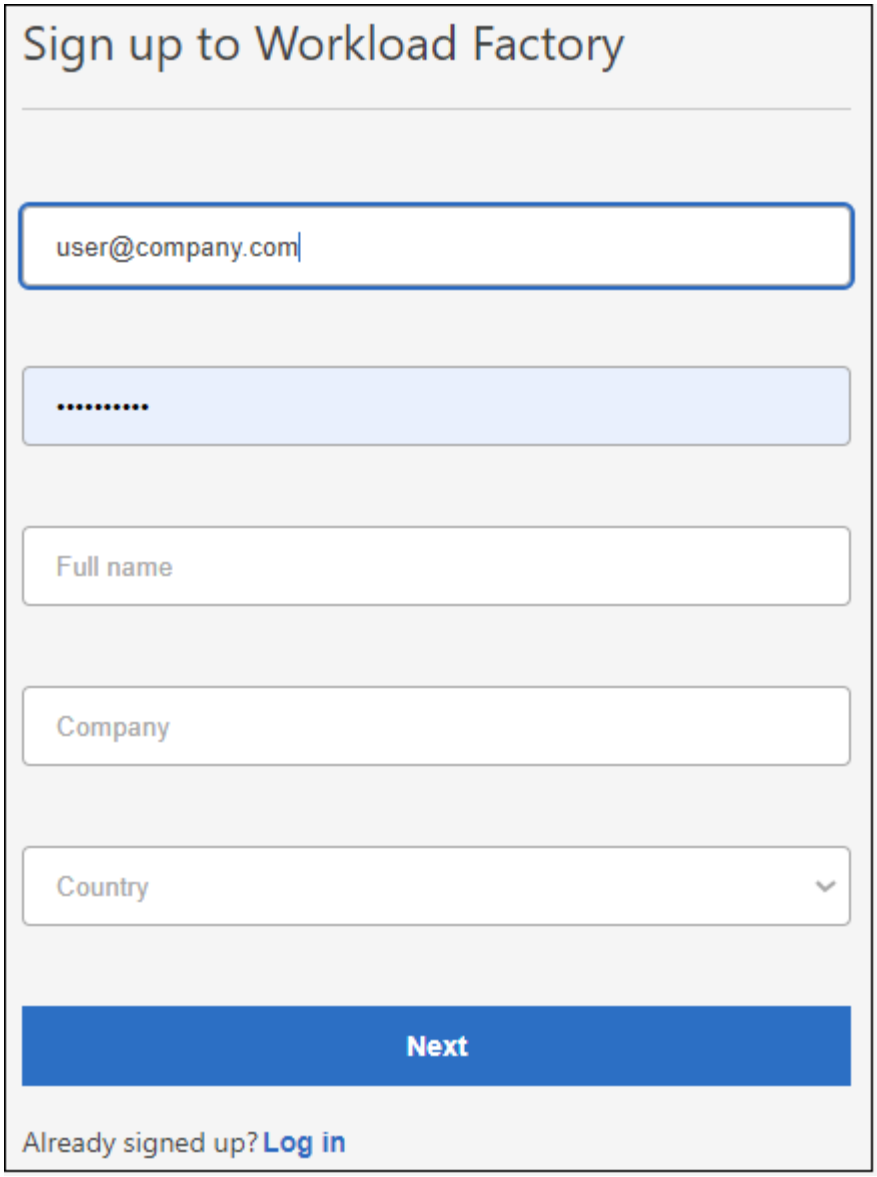
- 既存のNetApp Support Site （NSS）のクレデンシャルを必要に応じて変更
- Eメールアドレスとパスワードを指定してネットアップクラウドにログインします

手順

1. ウェブブラウザを開いて、 "ワークロードファクトリーコンソール"
2. NetApp Support Site アカウントをお持ちの場合は、*ログイン*ページでNSSアカウントに関連付けられているメールアドレスを直接入力してください。

   NSS アカウントをお持ちの場合は、サインアップ ページをスキップできます。 Workload Factory では、この初期ログインの一環としてサインアップが行われます。

3. NSSアカウントをお持ちでなく、ネットアップクラウドログインを作成して登録する場合は、*[Sign Up]* を選択します。



4. [サインアップ]ページで、NetAppクラウドログインを作成するために必要な情報を入力し、*[次へ]*を選択します。

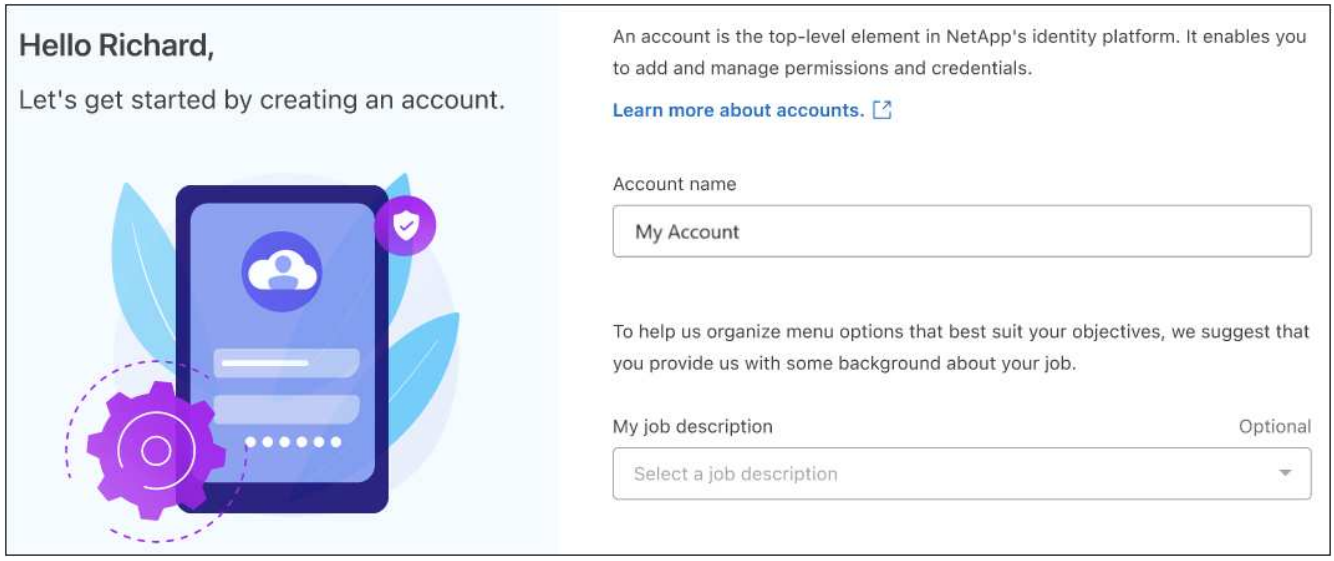
   サインアップフォームでは、英語の文字のみを使用できます。

5. 会社の詳細情報を入力し、*サインアップ*を選択します。
6. Eメールアドレスの確認手順が記載されたNetAppからのEメールが受信トレイに届いていることを確認します。

   この手順はログインする前に必要です。

7. プロンプトが表示されたら、エンドユーザライセンス契約を確認し、条項に同意して* Continue *を選択します。
8. [アカウント]ページで、アカウントの名前を入力し、必要に応じてジョブの説明を選択します。

   アカウントは、ネットアップのアイデンティティプラットフォームの最上位レベルの要素であり、権限とクレデンシャルを追加および管理できます。



ページのスクリーンショット。"]

9. *作成*を選択すると、ワークロード ファクトリーのホームページが表示されます。

結果

これで、Workload Factory のログインとアカウントが作成されました。あなたはアカウント管理者とみなされ、すべての Workload Factory 機能にアクセスできます。

Workload Factoryのアカウントに他のユーザーを招待する

アカウント管理者は、他のユーザーを Workload Factory アカウントに招待して、Workload Factory にアクセスして使用できるようにすることができます。アカウント管理はNetApp Consoleからのみ可能です。

NetApp Consoleのドキュメントを参照してください。 "メンバー（ユーザーアカウント）を追加する方法を学ぶ"、Workload Factory アカウントに追加します。

結果

招待されたユーザーには、Workload Factory アカウントに参加するための手順が記載されたメールが届きます。

Workload FactoryにAWS認証情報を追加する

AWS 認証情報を追加および管理して、 NetApp Workload Factory が AWS アカウントでクラウド リソースを展開および管理するために必要な権限を持つようにします。

概要

認証情報ページから、既存の Workload Factory アカウントに AWS 認証情報を追加できます。これにより、AWS 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必要な権限が Workload Factory に付与されます。

クレデンシャルは、次の2つの方法で追加できます。

- 手動: Workload Factory で認証情報を追加しながら、AWS アカウントに IAM ポリシーと IAM ロールを作成します。

- 自動的に:権限に関する最小限の情報を取得し、CloudFormationスタックを使用して資格情報のIAMポリシーと役割を作成します。

AWS クレデンシャル

AWS Assumeロールのクレデンシャルの登録フローは次のように設計されています。

- では、使用するワークロード機能を指定し、選択内容に応じてIAMポリシーの要件を指定できるため、AWSアカウントの権限をより適切に調整できます。
- 特定のワークロード機能をオプトインまたはオプトアウトするときに、付与されたAWSアカウントの権限を調整できます。
- AWSコンソールで適用できるカスタマイズされたJSONポリシーファイルを提供することで、IAMポリシーの手動作成を簡易化します。
- AWS CloudFormationスタックを使用して必要なIAMポリシーとロールの作成を自動化するオプションをユーザに提供することで、クレデンシャルの登録プロセスをさらに簡易化します。
- AWSベースのシークレット管理バックエンドにFSx for ONTAPサービスのクレデンシャルを格納できるようにすることで、クレデンシャルをAWSクラウドエコシステムの境界内に格納することを強く希望するFSx for ONTAPユーザとの連携が強化されます。

1つ以上の**AWS**クレデンシャル

最初の Workload Factory 機能を使用する場合は、それらのワークロード機能に必要な権限を使用して資格情報を作成する必要があります。認証情報は Workload Factory に追加しますが、IAM ロールとポリシーを作成するには AWS マネジメントコンソールにアクセスする必要があります。これらの資格情報は、Workload Factory のあらゆる機能を使用するときにアカウント内で利用できるようになります。

AWS 認証情報の初期セットには、1 つの機能または複数の機能に対する IAM アクセス許可ポリシーを含めることができます。それはあなたのビジネス要件によって異なります。

Workload Factory に複数の AWS 認証情報セットを追加すると、FSx for ONTAPファイルシステム、FSx for ONTAPへのデータベースのデプロイ、VMware ワークロードの移行など、追加機能を使用するために必要な追加の権限が提供されます。

アカウントへのクレデンシャルの手動追加

Workload Factory に AWS 認証情報を手動で追加して、独自のワークロードを実行するために使用する AWS リソースを管理するために必要な権限を Workload Factory アカウントに付与できます。追加する認証情報の各セットには、使用するワークロード機能に基づく 1 つ以上の IAM ポリシーと、アカウントに割り当てられた IAM ロールが含まれます。

> Workload Factory コンソールまたはNetAppコンソールから、アカウントに AWS 認証情報を追加できます。

クレデンシャルの作成には、次の3つの要素があります。

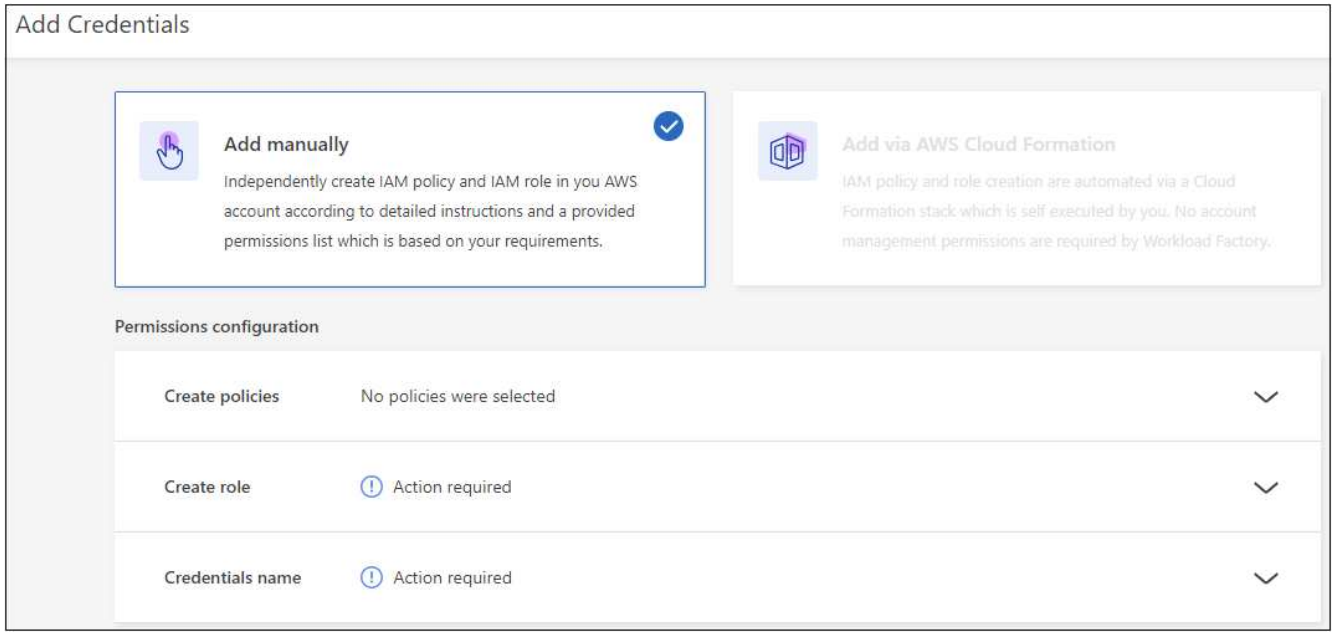
- 使用するサービスと権限レベルを選択し、AWS管理コンソールからIAMポリシーを作成します。
- AWS管理コンソールからIAMロールを作成します。
- Workload Factory から名前を入力し、資格情報を追加します。

開始する前に

AWSアカウントにログインするにはクレデンシャルが必要です。

手順

1. ログイン "ワークロードファクトリーコンソール"。
2. メニューから*管理*を選択し、次に*資格情報*を選択します。
3. [クレデンシャル]ページで、*[クレデンシャルの追加]*を選択します。
4. [クレデンシャルの追加]ページで*[手動で追加]*を選択し、次の手順に従って_Permissions configuration_の各セクションを完了します。



手順**1**：ワークロードの機能を選択し、**IAM**ポリシーを作成する

このセクションでは、これらのクレデンシャルの一部として管理できるワークロード機能のタイプと、各ワークロードに対して有効にする権限を選択します。選択した各ワークロードのポリシー権限をCodeboxからコピーし、AWSアカウント内のAWS管理コンソールに追加してポリシーを作成する必要があります。

手順

1. [ポリシーの作成]*セクションで、これらのクレデンシャルに含めるワークロード機能をそれぞれ有効にします。

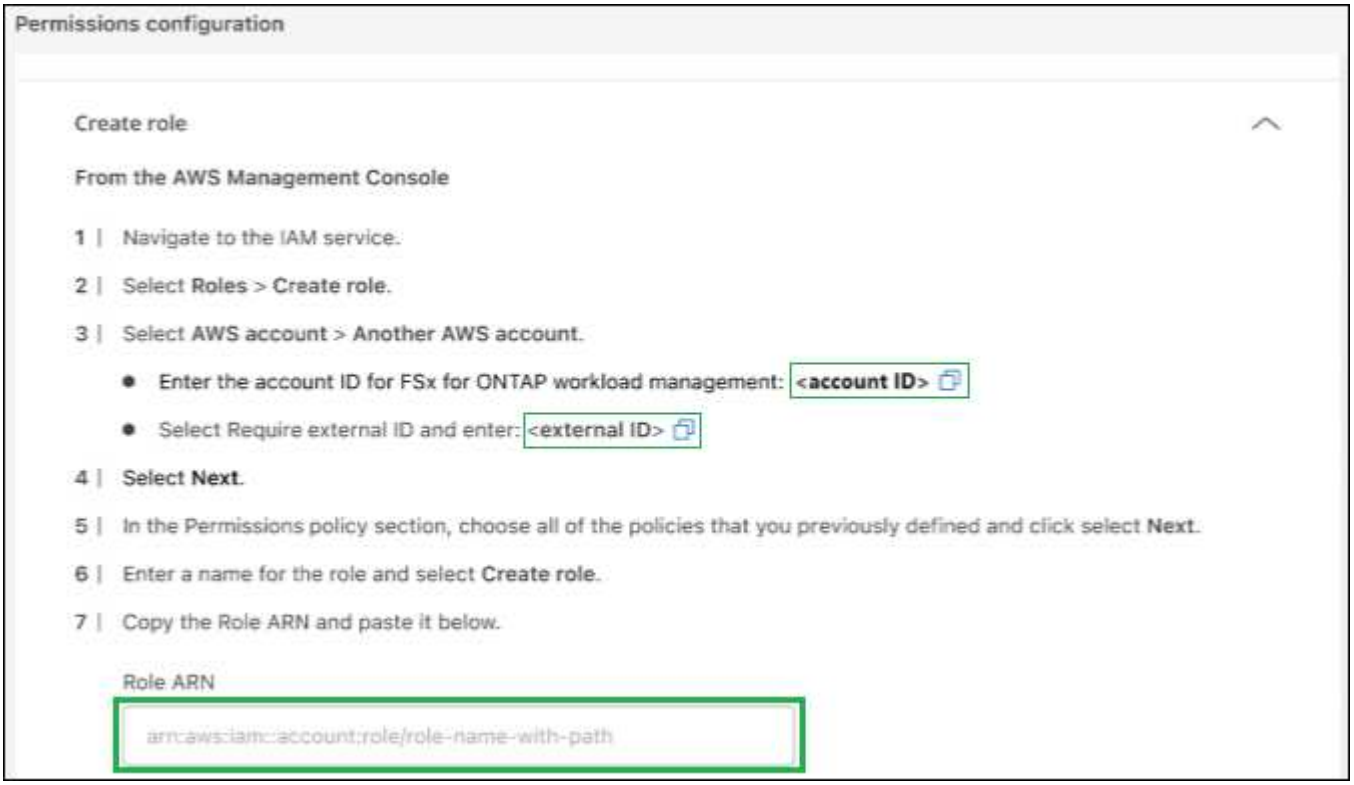
   あとから機能を追加できるので、導入と管理が必要なワークロードを選択するだけです。

2. 権限ポリシーを選択できるワークロード機能の場合は、これらの資格情報で使用できる権限のタイプを選択します。
3. オプション：[自動権限チェックを有効にする]*を選択して、ワークロードの処理を完了するために必要なAWSアカウントの権限があるかどうかを確認します。チェックを有効にすると、権限ポリシーにが追加され `iam:SimulatePrincipalPolicy permission`ます。この権限の目的は、権限のみを確認することです。クレデンシャルを追加したあとにこの権限を削除することもできますが、処理が一部しか成功しないようにリソースが作成されないようにしたり、必要なリソースの手動クリーンアップを行わないようにするために、

4. [コードボックス]ウィンドウで、最初のIAMポリシーの権限をコピーします。
5. 別のブラウザウィンドウを開き、AWS管理コンソールでAWSアカウントにログインします。
6. IAMサービスを開き、* Policies **>** Create Policy *を選択します。
7. ファイルタイプとしてJSONを選択し、手順3でコピーした権限を貼り付けて* Next *を選択します。
8. ポリシーの名前を入力し、*[ポリシーの作成]*を選択します。
9. 手順1で複数のワークロード機能を選択した場合は、これらの手順を繰り返して、ワークロード権限のセットごとにポリシーを作成します。

手順**2**：ポリシーを使用する**IAM**ロールを作成する

このセクションでは、作成した権限とポリシーを含む、Workload Factory が引き受ける IAM ロールを設定します。



手順

1. AWS管理コンソールで、*[Roles]>[Create Role]*を選択します。
2. 信頼されるエンティティのタイプ * で、 * AWS アカウント * を選択します。
   a. 別の **AWS** アカウント を選択し、Workload Factory UI から FSx for ONTAPワークロード管理のアカウント ID をコピーして貼り付けます。
   b. 必須の外部 **ID** を選択し、Workload Factory UI から外部 ID をコピーして貼り付けます。
3. 「 * 次へ * 」を選択します。
4. [アクセス許可ポリシー]セクションで、以前に定義したすべてのポリシーを選択し、*[次へ]*を選択します。
5. ロールの名前を入力し、*[ロールの作成]*を選択します。

6. ロールARNをコピーします。
7. Workload Factory の [認証情報の追加] ページに戻り、[権限の設定] の下の [ロールの作成] セクションを展開して、[ロール *ARN*] フィールドに ARN を貼り付けます。

手順**3**：名前を入力してクレデンシャルを追加

最後のステップは、Workload Factory で資格情報の名前を入力することです。

手順

1. Workload Factory の [資格情報の追加] ページで、[権限の構成] の下の [資格情報の名前] を展開します。
2. これらのクレデンシャルに使用する名前を入力します。
3. [追加]*を選択してクレデンシャルを作成します。

結果

クレデンシャルが作成され、[Credentials]ページに戻ります。

CloudFormationを使用してアカウントにクレデンシャルを追加する

使用する Workload Factory 機能を選択し、AWS アカウントで AWS CloudFormation スタックを起動することで、AWS CloudFormation スタックを使用して Workload Factory に AWS 認証情報を追加できます。CloudFormation は、選択したワークロード機能に基づいて IAM ポリシーと IAM ロールを作成します。

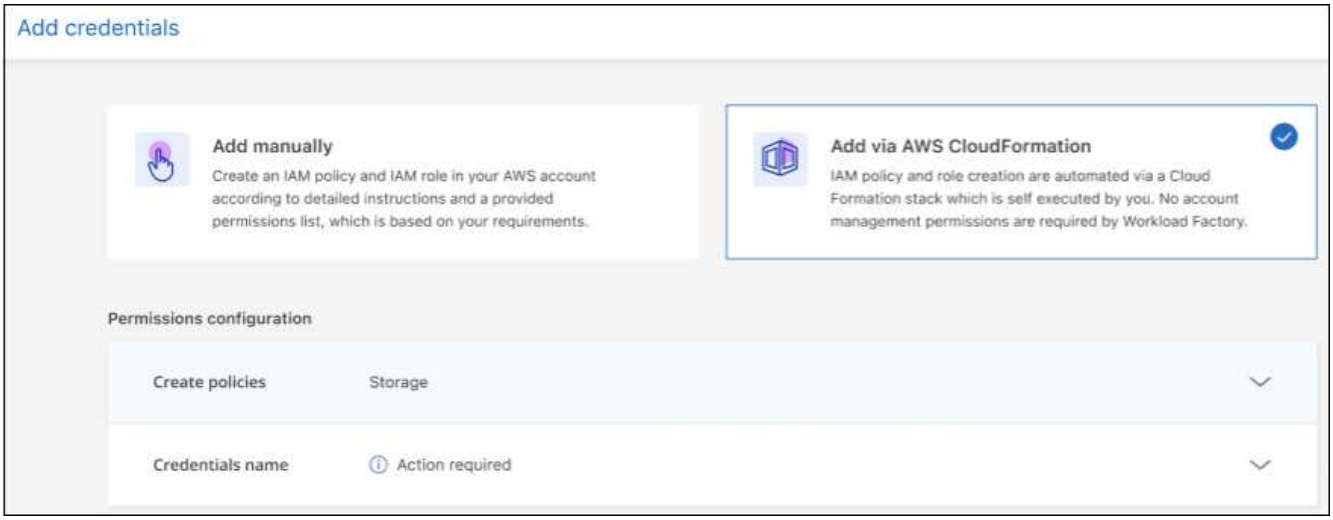
開始する前に

- AWSアカウントにログインするにはクレデンシャルが必要です。
- CloudFormationスタックを使用してクレデンシャルを追加する場合は、AWSアカウントで次の権限が必要です。

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

手順

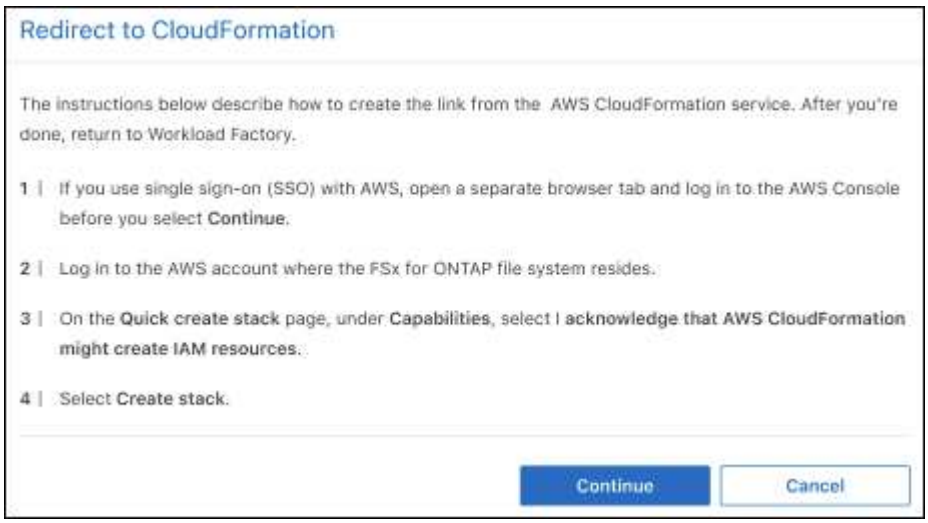
1. ログイン "ワークロードファクトリーコンソール"。
2. メニューから*管理*を選択し、次に*資格情報*を選択します。
3. [クレデンシャル]ページで、*[クレデンシャルの追加]*を選択します。
4. [Add via AWS CloudFormation]*を選択します。



5. [ポリシーの作成]*で、これらのクレデンシャルに含める各ワークロード機能を有効にし、各ワークロードの権限レベルを選択します。

   あとから機能を追加できるので、導入と管理が必要なワークロードを選択するだけです。

6. オプション：[自動権限チェックを有効にする]*を選択して、ワークロードの処理を完了するために必要なAWSアカウントの権限があるかどうかを確認します。チェックを有効にすると、権限ポリシーに権限が追加され `iam:SimulatePrincipalPolicy` ます。この権限の目的は、権限のみを確認することです。クレデンシャルを追加したあとにこの権限を削除することもできますが、処理が一部しか成功しないようにリソースが作成されないようにしたり、必要なリソースの手動クリーンアップを行わないようにするために、
7. [クレデンシャル名]*で、これらのクレデンシャルに使用する名前を入力します。
8. AWS CloudFormationからクレデンシャルを追加します。
   a. [Add]*（または[Redirect to CloudFormation]*を選択）を選択すると、[Redirect to CloudFormation]ページが表示されます。



   b. AWSでシングルサインオン（SSO）を使用している場合は、別のブラウザタブを開き、AWSコンソールにログインしてから*[続行]*を選択します。

      FSx for ONTAPファイルシステムが配置されているAWSアカウントにログインする必要があります。

c. [Redirect to CloudFormation]ページから[Continue]*を選択します。

d. [Quick create stack]ページの[Capabilities]で、*[I acknowledge that AWS CloudFormation might create IAM resources]*を選択します。

e. [スタックの作成]*を選択します。

f. ワークロード ファクトリーに戻り、資格情報ページを監視して、新しい資格情報が進行中であること、または追加されたことを確認します。

NetApp Workload Factoryでワークロードを最適化

ログインしてNetApp Workload Factory をセットアップしたら、 Amazon FSx for ONTAPファイルシステムの作成、FSx for ONTAP ファイルシステムへのデータベースのデプロイ、FSx for ONTAPファイルシステムを外部データストアとして使用して仮想マシン構成を VMware Cloud on AWS に移行するなど、いくつかのONTAP Factory 機能を使い始めることができます。

- "NetApp ONTAP 対応の Amazon FSX"

  FSx for ONTAPをストレージインフラとして使用することで、現在のデータ資産を評価して分析し、コスト削減の可能性を探ります。また、ベストプラクティスに基づいてFSx for ONTAP環境をプロビジョニングしてテンプレート化し、高度な管理機能を利用できます。

- "データベースワークロード"

  AWS上の既存のデータベース資産の検出、FSx for ONTAPへの移行によるコスト削減の可能性の評価、最適化のためのベストプラクティスが組み込まれたエンドツーエンドのデータベース導入、CI / CDパイプライン向けのシンクローニングの自動化が可能です。

- "玄愛"

  Retrieval-Augmented Generation（RAG）インフラを導入、管理して、AIアプリケーションの精度と独自性を向上させます。データのセキュリティとコンプライアンスが組み込まれたFSx for ONTAPに関するRAGナレッジベースを作成できます。

- "VMwareワークロード"

  スマートな推奨事項と自動修正により、移行と運用を合理化できます。効率的なバックアップと堅牢なディザスタリカバリを導入VMの監視とトラブルシューティング

- "EDAワークロード"

  複数のファイルシステムにわたって FSx for ONTAPを最適化し、自動化されたストレージ パラメータ管理を通じてパフォーマンスを向上させ、運用コストを削減します。

ワークロードファクトリーの管理

NetAppワークロードファクトリーにログイン

NetApp Workload Factory にサインアップすると、Web ベースのコンソールからいつでもログインして、ワークロードと FSx for ONTAPファイル システムの管理を開始できます。

タスクの内容

次のいずれかのオプションを使用して、Workload Factory の Web ベース コンソールにログインできます。

- 既存のNetApp Support Site （NSS）のクレデンシャルを必要に応じて変更
- Eメールアドレスとパスワードを使用したネットアップクラウドへのログイン

手順

1. ウェブブラウザを開いて、 "ワークロードファクトリーコンソール" 。
2. [ログイン*]ページで、ログインに関連付けられている電子メールアドレスを入力します。
3. ログインに関連付けられている認証方法に応じて、クレデンシャルの入力を求められます。
   - ネットアップクラウドクレデンシャル：パスワードを入力します
   - フェデレーテッドユーザ：フェデレーテッドアイデンティティクレデンシャルを入力します
   - NetApp Support Site アカウント：NetApp Support Site クレデンシャルを入力します
4. [ログイン]*を選択します。

   過去に正常にログインしたことがある場合は、Workload Factory のホームページが表示され、デフォルトのアカウントを使用することになります。

   初めてログインする場合は、*アカウント*ページが表示されます。

   - 1つのアカウントのメンバーである場合は、*続行*を選択します。
   - 複数のアカウントのメンバーである場合は、アカウントを選択して*続行*を選択します。

結果

これでログインし、Workload Factory を使用して FSx for ONTAPファイルシステムとワークロードを管理できるようになりました。

サービスアカウントの管理

サービスアカウントを作成して、インフラの運用を自動化するマシンユーザとして機能させます。サービスアカウントへのアクセス権は、いつでも無効にしたり変更したりできます。

タスクの内容

サービス アカウントは、 NetAppが提供するマルチテナント機能です。アカウント管理者は、サービス アカ

ウントの作成、アクセスの制御、サービス アカウントの削除を行います。サービス アカウントは、NetAppコンソールまたはNetApp Workload Factory コンソールで管理できます。

クライアント シークレットを再作成できるNetAppコンソールでのサービス アカウントの管理とは異なり、Workload Factory ではサービス アカウントの作成と削除のみがサポートされます。 NetApp Workload Factoryコンソールで特定のサービスアカウントのクライアントシークレットを再作成する場合は、サービスアカウントの削除 、 その後新規作成。

サービスアカウントは、パスワードではなくクライアントIDとシークレットを認証に使用します。クライアントIDとシークレットは、アカウント管理者が変更を決定するまで修正されます。サービスアカウントを使用するには、アクセストークンを生成するためにクライアントIDとシークレットが必要です。そうしないとアクセスできません。アクセストークンは短命であり、数時間しか使用できないことに注意してください。

開始する前に

NetAppコンソールでサービス アカウントを作成するか、Workload Factory コンソールでサービス アカウントを作成するかを決定します。若干の違いはございます。次の手順では、Workload Factory コンソールでサービス アカウントを管理する方法について説明します。

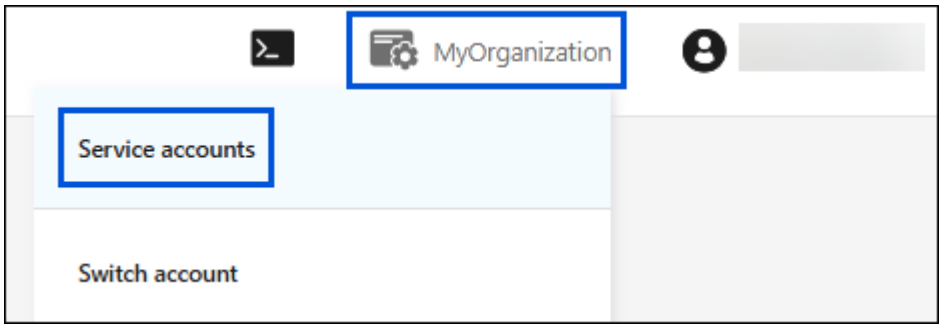
NetAppコンソールでサービスアカウントを管理するには、"アイデンティティとアクセス管理の仕組みを学ぶ" そして"IAM メンバーを追加して権限を管理する方法を学びます"。

サービスアカウントを作成します

サービス アカウントを作成すると、Workload Factory を使用すると、サービス アカウントのクライアント ID とクライアント シークレットをコピーまたはダウンロードできます。このキー ペアは、Workload Factory による認証に使用されます。

手順

1. Workload Factoryコンソールで、**[Account]***アイコンを選択し、[Service accounts]*を選択します。



2. [サービスアカウント]ページで、[サービスアカウントの作成]*を選択します。
3. Create service account（サービスアカウントの作成）ダイアログで、* Service account name（サービスアカウント名）*フィールドにサービスアカウントの名前を入力します。

   role は、 account admin *として事前に選択されています。

4. 「 * Continue * 」を選択します。
5. クライアント ID とクライアントシークレットをコピーまたはダウンロードします。

   クライアント シークレットは 1 回だけ表示され、Workload Factory によってどこにも保存されません。秘密をコピーまたはダウンロードして安全に保管してください。

6. オプションで、クライアント資格情報交換を実行して、Auth0 管理 API のアクセストークンを取得できます。リフレッシュトークンの生成に関する情報については、"NetApp Console APIドキュメント"を参照してください。

   curl の例は、クライアント ID とシークレットを取得し、API を使用して時間制限のあるアクセストークンを生成する方法を示しています。トークンは、NetApp Workload Factory API への数時間のアクセスを提供します。

   ```
   {
   "audience": "https://api.cloud.netapp.com",
   "grant_type": "client_credentials",
   "client_id": "ck2MGBU9LeWCpWlhqyaeximrCmdrNQRm",
   "client_secret": "pEleXhAsyf-HXHW5UaFx-
   Ek1tFT3MKZIEszhVuy6eHePHCwgXkiQT0El_g-WYLUu"
   }
   ```

   出力をhttps://netapp-cloud-account.auth0.com/oauth/tokenに投稿してアクセストークンを取得します。

7. [閉じる（ Close ）] を選択します。

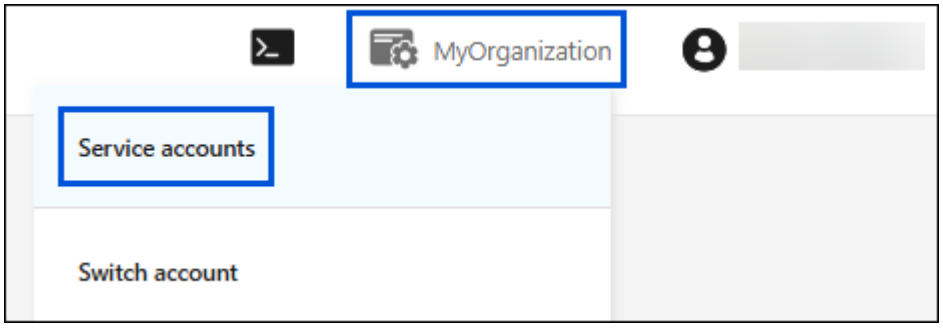
新しいサービスアカウントが作成され、[サービスアカウント]ページに表示されます。

サービスアカウントを削除します

不要になったサービスアカウントを削除します。

手順

1. Workload Factoryコンソールで、**[Account]***アイコンを選択し、[Service accounts]*を選択します。



2. サービス アカウント ページで、アクション メニューを選択し、削除 を選択します。
3. [サービスアカウントの削除]ダイアログで、テキストボックスに「* delete *」と入力します。
4. 削除*を選択して削除を確定します。

適切に設計されたワークロードを構築および運用する

Amazon FSx for NetApp ONTAP用のNetApp管理スイートである 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、ストレージとデータベースのワークロードの毎日の分析、推奨事項、自動修正を提供し、健全なワークロード操作を促進します。このプロセスを自動化することで、Workload Factory は人的エラーを最小限に抑え、ワークロード管理の一貫性を確保します。

仕組み

Workload Factory は、Amazon FSx for NetApp ONTAP ファイルシステム、Microsoft SQL Server、および Oracle データベースのデプロイメントを毎日分析します。分析により、適切に設計されたステータス、インサイト、推奨事項が提供されます。ベストプラクティスを満たし、効率的に運用できるように構成の問題を自動的に修正できます。

毎日の分析が完了すると、デプロイメントの Well-architected ダッシュボードに構成が「最適化済み」または「最適化されていない」として表示されます。全体的な最適化スコア、カテゴリ別の構成の問題、構成の問題と推奨事項のリストが表示されます。構成の問題に関する推奨事項を確認できます。一部の問題は Workload Factory によって自動的に修正できますが、その他の問題は手動での介入が必要です。この場合、Workload Factory は、推奨される変更を実装するのに役立つ詳細な手順を提供します。

ご使用の環境に適用されない構成の分析を無視することができます。これにより、不要なアラートや不正確な最適化結果を回避できます。特定の構成分析を無視すると、Workload Factory ではその構成が全体の最適化スコアに含められません。

なぜそれが重要なのか

Workload Factory は、継続的な評価と推奨事項の洞察および修復を組み合わせることで、大規模なストレージまたはデータベース環境にベストプラクティスを適用します。自動修正により人為的エラーが削減され、統一された管理が確保され、パフォーマンスと信頼性が維持されます。Workload Factory コンソールに適用された修正により、人為的エラーが削減され、統一された管理が保証されます。自動化により、構成が正しく適用され、維持され、ワークロードインフラストラクチャ全体のパフォーマンスと信頼性が維持されます。

Workload Factory を使って誤った構成を検出し修正しましょう

Workload Factoryを使い始めるには、サインアップして認証情報を追加し、接続を確立してAWSリソースを管理し、Amazon FSx for NetApp ONTAPを使用してワークロードを最適化します。

"クイックスタート"

ストレージワークロードのベストプラクティスと推奨事項

Workload Factoryはストレージ構成を評価し、ONTAP構成のベストプラクティスとAWS Well-Architected Frameworkへの準拠について詳細なビューを提供します。評価では改善と修正も推奨されます。

Well-Architected 分析では、フレームワークの次の柱に従って構成を分類します: 信頼性、セキュリティ、運用上の卓越性、コスト最適化、および パフォーマンス効率。

信頼性

信頼性により、中断が発生した場合でも、ワークロードが意図した機能を正しく一貫して実行することが保証されます。

- * ONTAPバックアップ用に FSx をスケジュールする*

  FSx for ONTAP：ボリュームをバックアップすることで、データ保持とコンプライアンスのニーズをサポートします。FSx for ONTAP バックアップを使用して、データの自動バックアップと保持を設定します。

- ローカルスナップショットをスケジュールする

  効率的なバックアップと迅速な復元のためにローカル スナップショットをスケジュールします。スナップショットは、ボリュームの即時のポイントインタイムのイメージです。

- クロスリージョンレプリケーション

  クロスリージョンレプリケーションにより、データが別の AWS リージョンにレプリケートされ、データの耐久性と可用性が向上します。Workload Factory では、災害復旧とコンプライアンスを支援するために、クロスリージョンレプリケーションを設定することを推奨しています。

- データ複製を設定する

  データの信頼性を高めるために、データを同じリージョンまたは別のリージョンの FSx for ONTAPファイルシステムに複製できます。ファイル システム間での移行、災害復旧、長期保存をサポートするために、データ レプリケーションを設定します。

- **SSD**容量のしきい値を増やす

  SSD ストレージ層の容量は、継続的に 80% の使用率を超えてはなりません。これにより、容量プールのストレージ層へのデータの読み取りと書き込みに影響が及ぶ可能性があり、ファイル システムのスループット容量にも影響が及ぶ可能性があります。容量が不足すると、データ ボリュームが読み取り専用になり、新しいデータを書き込もうとするサービスが失敗する可能性があります。

- データの信頼性を確保するためにラベルを一致させる

  データの信頼性を確保するには、ソース ボリュームのスナップショット ポリシー ラベルとレプリケーション ポリシー ラベルが一致している必要があります。

- ファイル容量のしきい値を増やす

  ボリューム容量の制限に達しないように、ファイル容量のしきい値を上げる必要があります。ファイル容量 (i ノード) が少ないと、ボリュームに追加データを書き込むことができなくなります。Workload Factory では、利用可能なファイル容量の使用率を継続的に 80% 未満に抑えることを推奨しています。ボリューム内に新しいファイルを作成するには、使用可能なファイル容量が必要です。

セキュリティ

セキュリティでは、リスク評価と軽減戦略を通じてデータ、システム、資産を保護することに重点が置かれます。

- **ARP/AI**を有効にする

  NetApp Autonomous Ransomware Protection with AI（ARP/AI）は、ボリュームをランサムウェアの脅威から保護するのに役立ちます。Workload Factory では、すべてのボリュームに対して ARP/AI を有効にすることをお勧めします。

- ボリュームへの不正アクセス

iSCSI を使用してアプリケーション データを提供するボリュームでは、NAS アクセスを並行して許可しないでください。Workload Factory では、iSCSI プロトコル経由でアクセスされるボリュームを、追加のプロトコルに制限することを推奨しています。

オペレーションの卓越性

運用の卓越性は、最適なアーキテクチャとビジネス価値の提供に重点を置いています。

- 自動容量管理を有効にする

  SSD 層がしきい値を超えないように定期的に確認するには、自動容量管理を有効にする必要があります。

- ボリューム容量使用率しきい値

  Workload Factory では、ボリューム容量の使用率が継続的に 80% を超えないようにすることを推奨しています。これにより、アプリケーションへのデータの読み取りと書き込みに影響する可能性があります。ボリューム容量の増加は、ボリュームの自動拡張機能を使用して手動で行うことも、自動で行うこともできます。

- ボリューム使用率がほぼ満杯に近づいています

  ボリュームの容量がいっぱいに近づいた場合、Workload Factory は、潜在的なアプリケーションの中断を回避するためにボリューム容量を増やすアクションを実行することを推奨します。

- キャッシュ関係書き込みモード

  最適なパフォーマンスを得るために、Workload Factory はワークロードに最適なキャッシュ リレーションシップ書き込みモードを推奨します。ライトアラウンド モードでは、小さなファイルで読み取りが多いワークロードのパフォーマンスが向上しますが、ライトバック モードでは、大きなファイルで書き込みが多いワークロードのパフォーマンスが向上します。

- キャッシュボリュームのサイズを最適化

  Workload Factory では、最適なサイズを維持し、ホットデータにキャッシュを集中させて効率を最大限に高めるために、ボリュームの自動サイズ調整とキャッシュボリュームのスクラブを有効にすることを推奨しています。

- **Storage VM**論理レポート

  Workload Factory では、ボリュームレベルでのストレージ使用状況をより適切に把握できるように、ストレージ VM のデフォルトのレポート設定を論理に設定することをお勧めします。

コスト最適化

コストの最適化により、コストを低く抑えながらビジネスの価値を最大限に高めることができます。

- コールドデータを階層化して**TCO**を最適化

  SSD ストレージ層の使用率を削減するには、コールド データ階層化を有効にする必要があります。すべてのボリュームに階層化ポリシーを適用することをお勧めします。FSx for ONTAP はデータを継続的にスキャンしてコールドデータを検出し、中断することなく容量ストレージプール層に移動します。

- ストレージ効率を向上

  ストレージ使用率を最適化し、SSD 層のコストを削減するには、ストレージ効率 (圧縮、圧縮、重複排除) を有効にする必要があります。

- 不要なスナップショットとバックアップの削除

  不要になったスナップショットとバックアップは、コストを削減するために削除する必要があります。

- 非アクティブなブロックデバイス

  ブロックデバイスが7日間使用されなかった場合、Workload Factoryはブロックデバイスデータをアーカイブするか、未使用のブロックデバイスを削除してコストを削減することを推奨します。

データベースワークロードのベストプラクティスと推奨事項

Workload Factory は、適切に設計されたデータベース ワークロードを運用するためのベスト プラクティスと推奨事項のセットを提供します。Well-Architected 分析では、ストレージのサイズ設定、ストレージ レイアウト、ストレージ構成、コンピューティング、アプリケーション (SQL Server)、および回復力に関連するMicrosoft SQL Serverおよび Oracle データベースの構成と設定を評価します。

ストレージのサイズ

- ストレージ層

  最高のストレージパフォーマンスを得るには、プライマリSSD階層にFSx for ONTAPボリュームを作成します。容量プール階層を使用すると、パフォーマンスが低下し、レイテンシが増加する可能性があります。

- ファイルシステムのヘッドルーム

  ストレージパフォーマンスを最適化するには、ファイルシステム容量をボリュームの合計サイズの1.35倍に設定します。

  ファイル システムのヘッドルーム パーセンテージは次のとおりです。

  - 不足: < 35%
  - 最適化: 35〜100%
  - 過剰プロビジョニング: > 100%

- ログドライブのサイズ

  ログ ドライブがいっぱいになることで発生するトランザクションのロールバック、データベースの使用不可、データ破損、パフォーマンスの低下などの問題を防ぐために、SQL Server ログ ドライブの正確なサイズ設定と定期的な監視を確実に実行します。

  ログ ドライブのサイズの割合は次のとおりです。

  - 不足: < 20%
  - 最適化: 20〜30%

    - 過剰プロビジョニング: > 30%

- **TempDB** ドライブのサイズ

  パフォーマンスを最適化し、全体的な安定性を維持するために、SQL Server TempDB の正確なサイズ設定と定期的な監視を確実に実行します。適切に構成された TempDB は、パフォーマンスの問題や不安定さを防ぎます。スペースが不足したり競合が多発したりすると、クエリの速度低下、アプリケーションのタイムアウト、システムクラッシュが発生する可能性があります。

  TempDB ドライブ サイズの割合は次のとおりです。

    - 不足: < 10%
    - 最適化: 10〜20%
    - 過剰プロビジョニング: > 20%

ストレージレイアウト

- データファイル（**.mdf**）の配置

  データファイルとログファイルを別のドライブに分離することで、パフォーマンスが向上し、独立したバックアップスケジュールが有効になり、リストア機能が向上します。小規模なデータベースの場合は、データとログのLUNパスを異なるボリュームに分離します。この分離は、複数の大規模なデータベース（> 500 GiB）で必要です。

- ログファイル（**.ldf**）の配置

  データファイルとログファイルを別のドライブに分離することで、パフォーマンスが向上し、独立したバックアップスケジュールが有効になり、リストア機能が向上します。小規模なデータベースの場合は、データとログのLUNパスを異なるボリュームに分離します。この分離は、複数の大規模なデータベース（> 500 GiB）で必要です。

- **TempDB** の配置

  TempDB を専用のドライブに配置することで、TempDB I/O を分離し、他のデータベースからの I/O 競合を回避します。この最適化により、SQL Server の全体的なパフォーマンスと安定性が向上します。これを怠ると、重大な I/O ボトルネック、クエリ パフォーマンスの低下、システムの不安定化が発生する可能性があります。

ストレージ構成

- * ONTAP構成*

エンティティ	設定	推奨事項
Volume	• シンプロビジョニング (-space-guarantee = none) • 自動サイズ設定オン • 自動サイズモード = 拡大 • 部分準備金 = 0% • スナップショットコピーリザーブ = 0% • スナップショットの自動削除（ボリューム/古いものから） • スペース管理の試行を最初に実行 = volume_grow	ストレージ効率とコスト効率を最適化するには、FSx for ONTAPボリュームのシンプロビジョニング、自動サイズ設定、およびスペース管理オプションを設定します。シン プロビジョニングを行わないと、ストレージは事前に割り当てられるため、非効率的な使用と過剰プロビジョニングによるコストの増加につながります。静的割り当てでは未使用の容量に対して料金が発生し、経費が増加します。動的割り当てが行われないため、スケーラビリティと柔軟性が低下し、パフォーマンスに影響を及ぼします。また、スペースの再利用を行わないと、削除されたデータがスペースを占有し、効率が低下します。
Volume	• 階層化ポリシー = スナップショットのみ • 階層化最小冷却日数 = 7	最適なデータベース パフォーマンスとコスト効率を実現するために、Workload Factory ではスナップショットのみを容量層に移動することを推奨しています。この戦略により、コストを削減しながら高いパフォーマンスが保証されます。特に、7 日以上経過したスナップショットを階層化することをお勧めします。
LUN	OSの種類 = windows_2008	ONTAP LUN OS タイプ値は、I/O アライメントを実現するために、オペレーティングシステムのパーティションスキームと一致する必要があります。構成が正しくない場合、パフォーマンスが最適にならない可能性があります。
LUN	スペース予約が有効	スペース リザベーションを有効にすると、 ONTAP はボリューム内に十分なスペースを予約し、ディスク スペース不足のために LUN への書き込みが失敗しないようにします。
LUN	スペース割り当てが有効	このオプションにより、ボリュームがいっぱいになって書き込みを受け付けなくなったときに、FSx for ONTAPが EC2 ホストに通知するようになります。この設定により、EC2 ホスト上の SQL Server がデータを削除したときに、FSx for ONTAPが自動的にスペースを再利用することも可能になります。無効にすると、書き込みが失敗する可能性があり、スペースが効率的に利用されない可能性があります。

- **Windows** ストレージ構成

エンティティ	設定	推奨事項
Microsoft マルチパス I/O (MPIO)	• ステータス = 有効 • ポリシー = ラウンドロビン • セッション数 = 5	FSx for ONTAPでプロビジョニングされた基盤となる LUN を持つ EC2 上のMicrosoft SQL Serverデータベースの最適な稼働時間とデータアクセスの一貫性を確保するために、Workload Factory では、マルチパス I/O (MPIO) を有効にして設定することを推奨しています。MPIO は FSx for ONTAPへの複数のパスを提供し、回復力とパフォーマンスの両方を強化します。このベスト プラクティスは、コンポーネントに障害が発生した場合でもデータ アクセスを維持することで、潜在的なデータ損失やダウンタイムを防ぎます。
アロケーションユニットサイズ	NTFSアロケーションユニットサイズ = 64K	NTFSアロケーションユニットサイズを64Kに設定すると、ディスクスペースをより有効に活用し、断片化を減らし、ファイルの読み取り / 書き込みパフォーマンスを向上させることができます。これを適切に構成しないと、ディスクの使用効率が低下し、パフォーマンスが低下する可能性があります。

コンピューティング

- コンピューティングの適正化

  SQL Server EC2 インスタンスの最適なパフォーマンスとコスト効率を確保するには、ワークロードの需要に基づいて適切なサイズを設定することをお勧めします。現在のインスタンスが不足している場合は、アップグレードすると CPU、メモリ、I/O 容量が強化されます。過剰にプロビジョニングされている場合は、ダウングレードすることでパフォーマンスを維持しながらコストを削減できます。

- オペレーティング システム パッチ

  Workload Factory では、セキュリティを確保し、 SQL Server データベースを脆弱性から保護し、システムの信頼性を向上させるために、最新のパッチを適用することを推奨しています。

- ネットワークアダプタの設定

  Microsoft SQL Serverインスタンスで最適なネットワーク パフォーマンスを得るには、受信側スケーリング (RSS) を正確に構成することが不可欠です。RSS はネットワーク処理を複数のプロセッサに分散し、ボトルネックを防止してシステム パフォーマンスを向上させます。Workload Factory では、次の RSS 設定を推奨しています。

  - TCP オフロード機能を無効にする: すべての TCP オフロード機能が無効になっていることを確認します。
  - 受信キューの数: vCPU が 8 を超える場合は 8 に設定します。vCPU が 8 以下の場合は、vCPU の数に設定します。
  - RSS プロファイル: NUMAStatic に設定します。
  - ベースプロセッサ番号: 2 に設定します。

    これらの設定に従うと、Microsoft SQL Serverインスタンスのパフォーマンスと信頼性が向上します。

本番環境に変更を加える前に、推奨設定をテストしてパフォーマンスの向上を確認することをお勧めします。

アプリケーション **(SQL Server)**

- ライセンス

  SQL Server ライセンスの評価と推奨は、ホスト レベルで提供されます。

  最適化されていません: データベース インフラストラクチャが、支払っている商用ソフトウェア ライセンスの機能をまったく使用していないことを Workload Factory が検出した場合、ライセンスは「最適化されていない」とみなされます。最適化されていないライセンスでは、不必要なコストが発生する可能性があります。

  最適化: データベースの商用ソフトウェア ライセンスがパフォーマンス要件を満たしている場合、ライセンスは「最適化」されているとみなされます。

- * Microsoft SQL Serverパッチ*

  Workload Factory では、セキュリティを確保し、 SQL Server データベースを脆弱性から保護し、システムの信頼性を向上させるために、最新のパッチを適用することを推奨しています。

- マックスドップ

  並行処理のバランスをとることでクエリのパフォーマンスを最適化するには、最大並列度 (MAXDOP) を設定します。正確な MAXDOP 構成により、パフォーマンスと効率が向上します。通常、MAXDOP を 4、8、または 16 に設定すると、ほとんどのユース ケースで最適な結果が得られます。ワークロードをテストし、CXPACKET などの並列処理関連の待機タイプを監視することをお勧めします。

信頼性

- * ONTAPバックアップ用に FSx をスケジュールする*

  Microsoft SQL Server ボリュームのバックアップは、データ保持とコンプライアンス要件をサポートするために不可欠です。FSx for ONTAP バックアップを使用して、SQL Server データの自動バックアップと保持を設定します。

- ローカルスナップショットをスケジュールする

  効率的なバックアップと迅速な復元のためにローカル スナップショットをスケジュールします。スナップショットは、ボリュームの即時のポイントインタイムのイメージです。

- クロスリージョンレプリケーション

  クロスリージョンレプリケーションにより、データが別の AWS リージョンにレプリケートされ、データの耐久性と可用性が向上します。Workload Factory では、災害復旧とコンプライアンスを支援するために、クロスリージョンレプリケーションを設定することを推奨しています。

EVS ワークロードのベストプラクティスと推奨事項

Workload Factory は、適切に設計された Amazon Elastic VMware Service （EVS）ワークロードを運用するた

めのベストプラクティスと推奨事項を提供します。Well-Architected 分析では、EVS 構成を評価して、VMware 環境が信頼性、セキュリティ、運用の卓越性、コストの最適化、パフォーマンス効率に最適化されていることを確認します。VMware の Well-Architected ステータスタブでは、EVS 環境に Well-Architected のベストプラクティスを実装するのに役立つ分析情報と推奨事項が見つかります。

Well-Architected 分析では、フレームワークの次の柱である 信頼性 と セキュリティ に基づいて構成を分類します。

信頼性

信頼性により、中断が発生した場合でも、ワークロードが意図した機能を正しく一貫して実行することが保証されます。

- **EVS**環境の回復力

  EVS クラスタノードがパーティション配置グループ全体に適切に分散されていることを確認します。すべてのノードは、4 つ以上のパーティションで構成された単一のパーティション配置グループのメンバーである必要があります。パーティションを適切に配置することで、EVS クラスタノードが AWS アベイラビリティゾーン内の障害が分離された複数のハードウェアパーティションに分散されます。不整合により、パーティションに障害が発生した場合に、処理能力が大幅に低下したり、ダウンタイムが発生する可能性があります。

セキュリティ

セキュリティでは、リスク評価と軽減戦略を通じてデータ、システム、資産を保護することに重点が置かれます。

- クラスタノード管理

  EVS クラスタノードに適切な EC2 停止および終了保護が設定されていることを確認します。EVS ESXi ノードは、vCenter またはその他の VMware レベルの管理ツールを使用してのみ管理する必要があります。適切な EC2 レベルの保護がないと、EC2 コンソールからノードが誤って停止または終了される可能性があり、仮想マシンのデータが使用できなくなったり、データが失われたりする可能性があります。

関連情報

- "ONTAPファイルシステム向けに適切に設計された FSx を実装する"
- "適切に設計されたデータベースワークロードを実装する"
- "適切に設計されたEVS構成を実装する"

NetApp Workload Factory 通知を構成する

NetApp Workload Factory 通知サービスを設定して、 NetAppコンソールまたは Amazon SNS トピックにアラートとして通知を送信できます。コンソール エージェントまたはリンクが展開されている場合、アラートとして送信された通知はNetAppコンソールに表示されます。 Workload Factory が Amazon SNS トピックに通知を発行すると、トピックのサブスクライバー (ユーザーや他のアプリケーションなど) は、トピックに設定されたエンドポイント (電子メールや SMS メッセージなど) で通知を受信します。

通知の種類とメッセージ

Workload Factory は次のイベントの通知を送信します。

イベント	製品説明	通知のタイプ	重大度	ワークロード	リソースタイプ
アカウント内の一部のデータベースインスタンスは適切に設計されていません	アカウント内のすべての Microsoft SQL Server インスタンスは、well-architected の問題について分析されています。このイベントの説明には、適切に設計されたインスタンスと最適化されていないインスタンスの数が表示されます。 Workload Factory コンソールから、データベース インベントリ内の well-architected ステータスの調査結果と推奨事項を確認します。	優れた設計	推奨事項	データベース	Microsoft SQL Serverインスタンス
Microsoft SQL Server/PostgreSQL サーバーの展開に成功しました	Microsoft SQL Server または PostgreSQL ホストのデプロイに成功しました。詳細については、ジョブ監視を参照してください。	導入	成功	データベース	FSx for ONTAP、DBホスト
Microsoft SQL Server/PostgreSQL サーバーの展開に失敗しました	Microsoft SQL Server または PostgreSQL ホストのデプロイに失敗しました。詳細については、ジョブ監視を参照してください。	導入	エラー	データベース	FSx for ONTAP、DBホスト

イベント	製品説明	通知のタイプ	重大度	ワークロード	リソースタイプ
レプリケーション関係の作成に失敗しました	SnapMirrorレプリケーション関係の作成に失敗しました。詳細については、Tracker をご覧ください。	レプリケーション	致命的	一般的な保管	ONTAP向け FSx
FSx for ONTAP の作成失敗	FSx for ONTAP ファイル システムの作成プロセスが失敗しました。詳細については、Tracker をご覧ください。	FSx for ONTAP ファイルシステムアクション	致命的	一般的な保管	ONTAP向け FSx
自動SSD容量またはinodeにより成功率が向上する	最近の自動容量管理更新中に、FSx for ONTAPファイルシステムによって SSD 容量またはボリューム inode のいずれかが正常に増加しました。詳細については、Tracker をご覧ください。	容量管理	成功	一般的な保管	FSx for ONTAP ファイル
自動SSD容量またはinodeの障害増加	最近の自動容量管理更新中に、FSx for ONTAPファイルシステムは SSD 容量またはボリューム inode を増やすことができませんでした。詳細については、Tracker をご覧ください。	容量管理	致命的	一般的な保管	ONTAPファイルシステム用の FSx

イベント	製品説明	通知のタイプ	重大度	ワークロード	リソースタイプ
FSx for ONTAP の問題が検出されました	すべての FSx for ONTAPファイルシステムについて、well-architected の問題について分析されています。スキャンにより 1 つ以上の問題が検出されました。詳細については、Workload Factory コンソールのストレージダッシュボードの well-architected 分析を確認してください。	適切に設計された分析	推奨事項	一般的な保管	ONTAPファイルシステム用の FSx
FSx for ONTAP の自動容量管理イベント	FSx for ONTAP ファイル システムの SSD パフォーマンス層が、警告しきい値の容量/パーセンテージ合計に達しました。	容量管理	警告	一般的な保管	ONTAPファイルシステム用の FSx
FSx for ONTAP の自動 inode 管理イベント	FSx for ONTAP ボリュームの inode 数が、警告しきい値の数/パーセンテージの合計に達しました。	容量管理	警告	一般的な保管	ONTAPファイルシステム用の FSx

ワークロードファクトリーの通知を構成する

NetAppコンソールまたは Workload Factory コンソールを使用して、Workload Factory 通知を構成します。NetAppコンソールを使用する場合は、 NetAppコンソールまたは Amazon SNS トピックにアラートとして通知を送信するように Workload Factory を設定できます。 NetAppコンソールの 通知設定 から通知を設定できます。

開始する前に

- Amazon SNS コンソールまたは AWS CLI を使用して、Amazon SNS を設定し、Amazon SNS トピックを作成する必要があります。
- Workload Factory は **Standard** トピック タイプをサポートしていることに注意してください。このタイプのトピックでは、通知が受信順にサブスクライバーに送信されるとは限りません。そのため、重要な通知や緊急の通知がある場合は、この点を考慮してください。

NetAppコンソールからの通知を構成する

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、管理、*通知設定*の順に選択します。
3. 通知設定ページで、次の操作を行います。
   a. オプション: NetAppコンソールで通知を送信するように Workload Factory を構成するには、*NetAppコンソール通知を有効にする* を選択します。
   b. *SNS通知を有効にする*を選択します。
   c. Amazon SNS コンソールから Amazon SNS を設定するには、指示に従います。

      トピックを作成したら、トピック ARN をコピーして、通知設定*ページの ***SNS** トピック **ARN** フィールドに入力します。
4. テスト通知を送信して構成を確認した後、[適用] を選択します。

結果

Workload Factory は、指定した Amazon SNS トピックに通知を送信するように設定されています。

Workload Factory コンソールから通知を構成する

手順

1. ログイン"ワークロードファクトリーコンソール"。
2. Workload Factory コンソール メニューから、ワークロード、管理、*通知設定*の順に選択します。
3. *SNS通知を有効にする*を選択します。
4. Amazon SNS コンソールから Amazon SNS を設定するには、指示に従います。
5. テスト通知を送信して構成を確認した後、[適用] を選択します。

結果

Workload Factory は、指定した Amazon SNS トピックに通知を送信するように設定されています。

Amazon SNSトピックを購読する

トピックに通知を送信するようにWorkload Factoryを設定したら、 "説明書" Amazon SNS ドキュメントの手順に従ってトピックをサブスクライブし、Workload Factory から通知を受信できるようにします。

通知をフィルタリングします

通知にフィルターを適用することで、不要な通知トラフィックを削減し、特定のユーザーに対して特定の通知タイプをターゲットにすることができます。これは、SNS 通知用の Amazon SNS ポリシーと、 NetAppコンソールの通知設定を使用して実行できます。

Amazon SNS通知をフィルタリングする

Amazon SNS トピックをサブスクライブすると、デフォルトでそのトピックに公開されたすべての通知を受

信します。トピックから特定の通知のみを受信する場合は、フィルター ポリシーを使用して、受信する通知を制御できます。フィルタポリシーにより、Amazon SNS はフィルタポリシーに一致する通知のみをサブスクライバーに配信します。

Amazon SNS 通知は、次の基準でフィルタリングできます。

製品説明	フィルターポリシーフィールド名	可能な値
リソースタイプ	`resourceType`	• `DB` • `Microsoft SQL Server host` • `PostgreSQL Server host`
ワークロード	`workload`	`WLMDB`
優先度	`priority`	• `Success` • `Info` • `Recommendation` • `Warning` • `Error` • `Critical`
通知のタイプ	`notificationType`	• `Deployment` • `Well-architected`

手順

1. Amazon SNS コンソールで、SNS トピックのサブスクリプションの詳細を編集します。
2. サブスクリプション フィルター ポリシー 領域で、メッセージ属性 でフィルターすることを選択します。
3. サブスクリプション フィルター ポリシー オプションを有効にします。
4. **JSON** エディター ボックスに JSON フィルター ポリシーを入力します。

   たとえば、次の JSON フィルター ポリシーは、WLMDB ワークロードに関連し、優先度が成功またはエラーであり、Well-architected ステータスの詳細を提供する Microsoft SQL Server リソースからの通知を受け入れます。

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

5. *変更を保存*を選択します。

その他のフィルタポリシーの例については、以下を参照してください。 "Amazon SNS のフィルターポリシーの例" 。

フィルタポリシーの作成の詳細については、 "Amazon SNSのドキュメント" 。

NetAppコンソールで通知をフィルタリングする

NetAppコンソールの通知設定を使用すると、コンソールで受信する通知を重大度レベル (重大、情報、警告など) でフィルタリングできます。

コンソールでの通知のフィルタリングの詳細については、 "NetAppコンソールのドキュメント" 。

Codeboxを使用したタスクの自動化

コードボックス自動化の詳細

Codebox は、開発者と DevOps がNetApp 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。 Codebox は Workload Factory の権限ポリシーに準拠しており、実行準備のための明確なパスを設定するとともに、将来の迅速な再利用のための自動化カタログを提供します。

Codeboxの機能

Codeboxには、次の2つの主要なIAC機能があります。

- _Codeboxビューア_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からエントリと選択を一致させることで、特定のジョブフロー操作によって生成されるIACを表示します。Codebox Viewerは、ナビゲーションと分析を容易にするためにカラーコーディングをサポートしていますが、編集は許可されておらず、オートメーションカタログへのコードのコピーまたは保存のみが許可されています。
- _Codebox Automation Catalog_保存されているすべてのIACジョブを表示し、将来の使用に備えて簡単に参照できるようにします。自動カタログジョブはテンプレートとして保存され、適用されるリソースのコンテキストで表示されます。

さらに、Workload Factory の認証情報を設定すると、Codebox は IAM ポリシーの作成に必要な AWS 権限を動的に表示します。使用する予定の Workload Factory 機能 (データベース、AI、FSx for ONTAPなど) ごとに権限が提供され、カスタマイズ可能です。 Codebox から権限をコピーし、AWS マネジメントコンソールに貼り付けるだけで、Workload Factory にワークロードを管理するための適切な権限が付与されます。

サポートされるコード形式

サポートされているコード形式は次のとおりです。

- ワークロードファクトリー REST API
- AWS CLI
- AWS CloudFormation
- テラフォーム

関連情報

"Codeboxの使用方法"です。

"ワークロードファクトリー REST API ドキュメント" 。

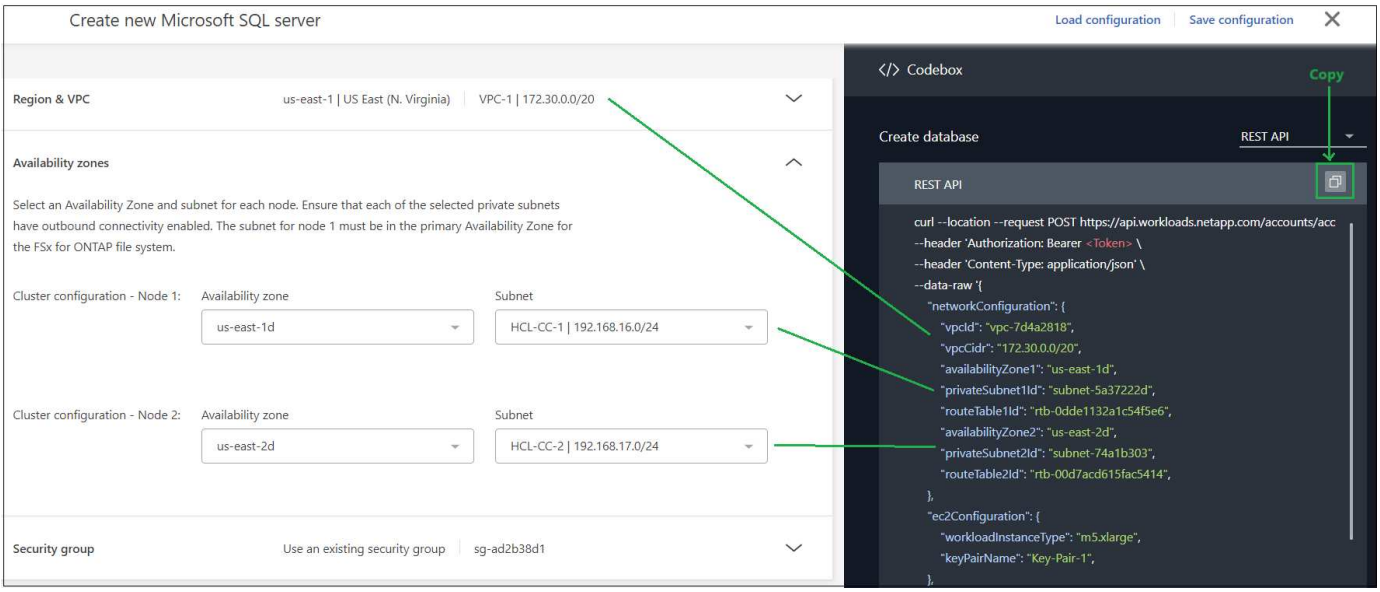
NetApp Workload Factory の自動化に Codebox を使用する

Codebox を使用すると、 NetApp 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できます。 Workload Factory REST API、AWS CLI、AWS CloudFormation を使用して使用および実行できるコードを生成できます。

Codebox は、各ユーザーの Workload Factory アカウントに提供される AWS 権限に基づいてコードに適切なデータを入力することで、Workload Factory の権限ポリシーに準拠しています。コードはテンプレートのように使用でき、不足している情報 (資格情報など) を入力したり、コードを実行する前に特定のデータをカスタマイズしたりできます。

Codeboxの使用方法

Workload Factory UI ウィザードに値を入力すると、各フィールドの入力が完了すると Codebox でデータの更新を確認できます。ウィザードを完了した後、ページの下部にある*作成*ボタンを選択する前に、構成を構築するために必要なコードをキャプチャするために、Codebox にコピーします。たとえば、新しい Microsoft SQL Server を作成するときのこのスクリーンショットには、VPC とアベイラビリティーゾーンのウィザードエントリと、REST API 実装の Codebox 内の同等のエントリが表示されています。



一部のコード形式では、ダウンロード ボタンを選択して、コードをファイルに保存し、別のシステムに持ち込むこともできます。必要に応じて、ダウンロード後にコードを編集して、他の AWS アカウントに適合させることができます。

Codeboxから**CloudFormation**コードを使用

Codebox から生成された CloudFormation コードをコピーし、AWS アカウントで Amazon Web Services CloudFormation スタックを起動できます。 CloudFormation は、Workload Factory UI で定義したアクションを実行します。

CloudFormation コードを使用する手順は、FSx for ONTAPファイルシステムをデプロイするのか、アカウント認証情報を作成するのか、それとも他の Workload Factory アクションを実行するのかによって異なる場合があります。

CloudFormationによって生成されたYAMLファイル内のコードは、セキュリティ上の理由から7日後に期限切れになります。

開始する前に

- AWSアカウントにログインするにはクレデンシャルが必要です。
- CloudFormationスタックを使用するには、次のユーザー権限が必要です。

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

手順

1. Workload Factory コンソールを使用して実行する操作を定義したら、コードボックス内のコードをコピーします。
2. [Redirect to CloudFormation]*を選択すると、[Redirect to CloudFormation]ページが表示されます。
3. 別のブラウザウィンドウを開き、AWS管理コンソールにログインします。
4. [Redirect to CloudFormation]ページから[Continue]*を選択します。
5. コードを実行するAWSアカウントにログインします。
6. [Quick create stack]ページの[Capabilities]で、*[I acknowledge that AWS CloudFormation may…]*を選択します。
7. [スタックの作成]*を選択します。
8. AWS または Workload Factory から進行状況を監視します。

Codeboxから REST APIコードを使用する

Codebox から生成された 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できます。

APIは、curlをサポートし、インターネットに接続された任意のホストから実行できます。

認証トークンはCodeboxでは非表示になっていますが、API呼び出しをコピーして貼り付けると入力されます。

手順

1. Workload Factory コンソールを使用して実行する操作を定義したら、Codebox に API コードをコピーします。
2. コードを貼り付けて、ホストシステムで実行します。

Codeboxから AWS CLIコードを使用

Codeboxから生成されたAmazon Web Services CLIを使用して、FSx for ONTAPファイルシステムやその他のAWSリソースを導入および管理できます。

手順

1. Workload Factory コンソールを使用して実行する操作を定義したら、Codebox に AWS CLI をコピーします。
2. 別のブラウザウィンドウを開き、AWS管理コンソールにログインします。
3. コードを貼り付けて実行します。

コードボックスから**Terraform**を使用

Terraformを使用して、FSx for ONTAPファイルシステムやその他のAWSリソースを導入、管理できます。

開始する前に

- Terraformがインストールされているシステム(Windows/Mac/Linux)が必要です。
- AWSアカウントにログインするにはクレデンシャルが必要です。

手順

1. Workload Factory コンソールを使用して実行する操作を定義したら、Codebox から Terraform コードをダウンロードします。
2. ダウンロードしたスクリプトアーカイブをTerraformがインストールされているシステムにコピーします。
3. zipファイルを展開し、README.mdファイルの手順に従います。

NetApp Workload Factory で CloudShell を使用する

CloudShell を開いて、 NetApp Workload Factory コンソールのどこからでも AWS またはONTAP CLI コマンドを実行します。

タスクの内容

CloudShell を使用すると、Workload Factory コンソール内からシェルのような環境で AWS CLI コマンドまたはONTAP CLI コマンドを実行できます。ブラウザでターミナル セッションをシミュレートし、ターミナル機能を提供し、Workload Factory のバックエンドを通じてメッセージをプロキシします。これにより、 NetApp アカウントで提供した AWS 認証情報とONTAP認証情報を使用できるようになります。

CloudShellには次の機能があります。

- 複数のCloudShellセッション：複数のCloudShellセッションを一度に展開して、複数のコマンドシーケンスを並行して発行します。
- 複数のビュー：CloudShellタブセッションを分割して、2つ以上のタブを水平または垂直に同時に表示できるようにします。
- セッション名の変更:必要に応じてセッション名を変更
- Last session content persistence（前回のセッションのコンテンツの永続性）：誤って閉じた場合は、最後のセッションを再度開きます。
- 設定の環境設定:フォントサイズと出力タイプの変更
- ONTAP CLIコマンドに対するAIが生成するエラー応答
- オートコンプリートのサポート：コマンドの入力を開始し、* Tab *キーを使用して使用可能なオプションを表示します。

CloudShellコマンド

CloudShell GUIインターフェイス内で、と入力して使用可能なCloudShellコマンドを表示できます `help`。コマンドを実行すると `help`、次のリファレンスが表示されます。

製品説明

NetApp CloudShell は、 NetApp Workload Factory に組み込まれた GUI インターフェイスであり、シェルのような環境で AWS CLI コマンドまたはONTAP CLI コマンドを実行できます。ブラウザでターミナル セッションをシミュレートし、ターミナル機能を提供し、Workload Factory のバックエンドを通じてメッセージをプロキシします。これにより、 NetAppアカウントで提供した AWS 認証情報とONTAP認証情報を使用できるようになります。

使用可能なコマンド

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

コンテキスト

各ターミナルセッションは、クレデンシャル、リージョン、およびオプションでFSx for ONTAPファイルシステムという特定のコンテキストで実行されます。

+ すべての AWS コマンドは、提供されたコンテキストで実行されます。 AWS コマンドは、提供された認証情報に指定されたリージョンでの権限がある場合にのみ成功します。

+ ONTAPコマンドをオプションで指定できます `fsxId`。あなたが `fsxId`個別のONTAPコマンドを使用する場

合、この ID はコンテキスト内の ID をオーバーライドします。ターミナルセッションにFSx for ONTAPファイルシステムIDコンテキストがない場合は、以下を提供する必要があります。 `fsxId`各ONTAPコマンドとともに。

+ 異なるコンテキストの詳細を更新するには、次の操作を行います。 * 資格情報を変更するには：「using credentials <credentialId>」 * リージョンを変更するには：「using region <regionCode>」 * ONTAPファイルシステムの FSx を変更するには：「using fsx <fileSystemId>」

アイテムの表示

- 使用可能な認証情報を表示するには："show credentials"
- 利用可能な地域を表示するには:"show regions"
- コマンド履歴を表示するには："show history"

変数

変数の設定と使用例を次に示します。変数の値にスペースが含まれている場合は、引用符で囲んで設定してください。

+ * 変数を設定するには: $<variable> = <value> * 変数を使用するには: $<variable> * 変数を設定する例: $svm1 = svm123 * 変数を使用する例: --fsx FileSystem-1 volumes show --vserver $svm1 * 文字列値で変数を設定する例 $comment1 = "スペースを含むコメント"

運用者

パイプ、バックグラウンド実行 `&`、リダイレクト `>`などのシェル演算子は `|`サポートされていません。これらの演算子を含めると、コマンドの実行は失敗します。

開始する前に

CloudShellは、AWSクレデンシャルのコンテキストで機能します。CloudShellを使用するには、AWSクレデンシャルを少なくとも1つ指定する必要があります。

> CloudShellを使用すると、AWSまたはONTAPの任意のCLIコマンドを実行できます。ただし、FSx for ONTAPファイルシステムのコンテキスト内で作業する場合は、必ず次のコマンドを実行してください。 `using fsx <file-system-name>`

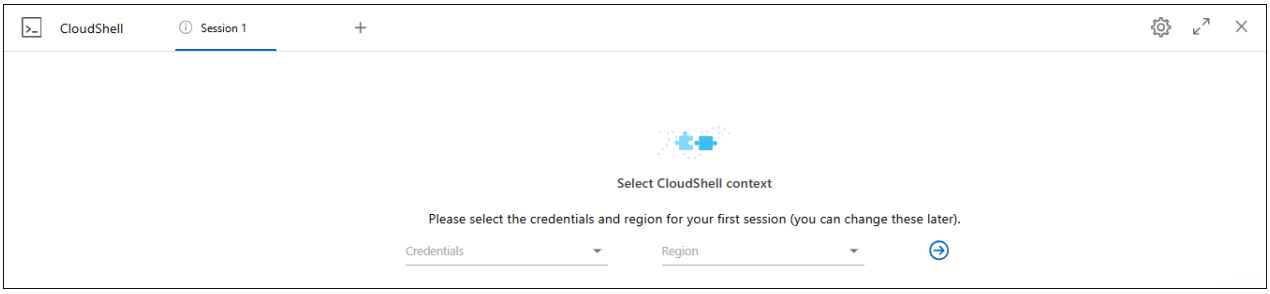
CloudShellを導入する

CloudShell は、 NetApp Workload Factory コンソールのどこからでもデプロイできます。 NetAppコンソールから CloudShell をデプロイすることもできます。

Workload Factory コンソールからデプロイする

手順

1. ログイン "ワークロードファクトリーコンソール"。
2. メニューから、[管理]、[CloudShell] の順に選択します。
3. [CloudShell]ウィンドウで、CloudShellセッションのクレデンシャルとリージョンを選択し、矢印を選択して続行します。



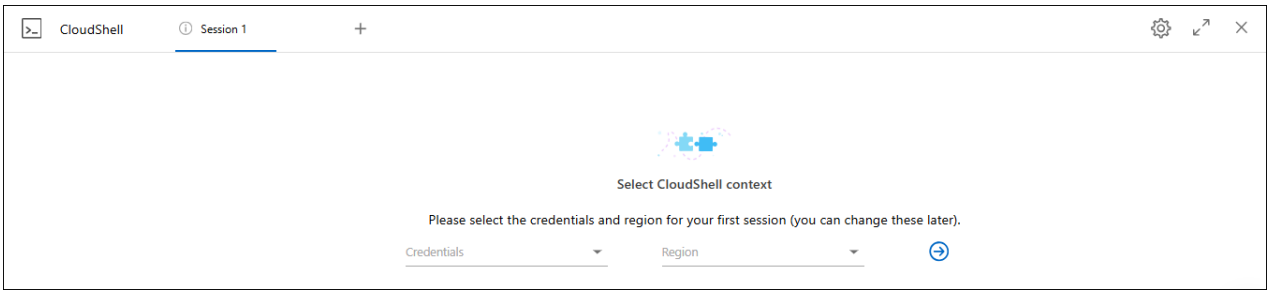
4. と入力し `help`て使用可能なコマンドと手順を表示するか、次のCLIリファレンスマニュアルを参照してCloudShellコマンドください。
   - "AWS CLIリファレンス"：FSx for ONTAPに関連するコマンドについては、* FSx *を選択します。
   - "ONTAP CLIリファレンス"
5. CloudShellセッション内でコマンドを発行します。

   ONTAP CLIコマンドの実行後にエラーが発生した場合は、電球のアイコンを選択すると、AIによって生成された簡単なエラー応答と、障害の説明、障害の原因、および詳細な解決策が表示されます。詳細については、*[続きを読む]*を選択してください。

NetAppコンソールから導入

手順

1. ログイン"NetAppコンソール"。
2. メニューから、*ワークロード*を選択し、次に*管理*を選択します。
3. 管理メニューから*CloudShell*を選択します。
4. [CloudShell]ウィンドウで、CloudShellセッションのクレデンシャルとリージョンを選択し、矢印を選択して続行します。



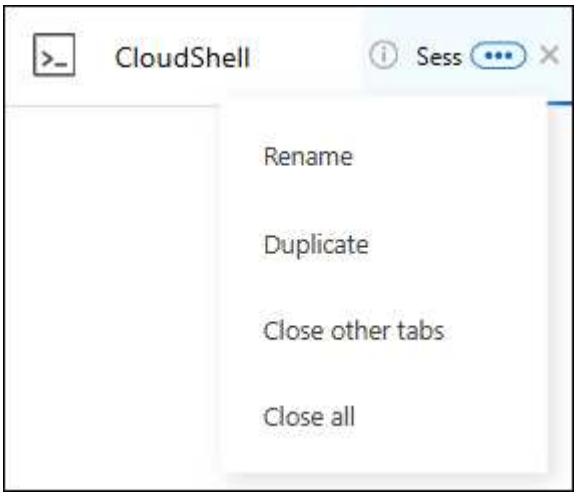
5. と入力し `help`て使用可能なCloudShellコマンドとその手順を表示するか、使用可能なコマンドについては次のCLIリファレンスドキュメントを参照してください。

- "AWS CLIリファレンス"：FSx for ONTAPに関連するコマンドについては、* FSx *を選択します。
- "ONTAP CLIリファレンス"

6. CloudShellセッション内でコマンドを発行します。

   ONTAP CLIコマンドの実行後にエラーが発生した場合は、電球のアイコンを選択すると、AIによって生成された簡単なエラー応答と、障害の説明、障害の原因、および詳細な解決策が表示されます。詳細については、*[続きを読む]*を選択してください。

このスクリーンショットに表示されている CloudShell タスクは、開いている CloudShell セッション タブのアクション メニューを選択することで完了できます。各タスクの手順は次のとおりです。



CloudShellセッションタブの名前変更

CloudShellセッションタブの名前を変更して、セッションを識別しやすくすることができます。

手順

1. CloudShell セッション タブのアクション メニューを選択します。
2. [名前の変更 *] を選択します。
3. セッションタブの新しい名前を入力し、タブ名の外側をクリックして新しい名前を設定します。

結果

CloudShellセッションタブに新しい名前が表示されます。

CloudShellセッションタブの複製

CloudShellセッションタブを複製して、同じ名前、クレデンシャル、およびリージョンを持つ新しいセッションを作成できます。元のタブのコードは、複製されたタブでは複製されません。

手順

1. CloudShell セッション タブのアクション メニューを選択します。
2. [複製]*を選択します。

結果

新しいタブが元のタブと同じ名前で表示されます。

CloudShellセッションのタブを閉じる

CloudShellタブを一度に1つずつ閉じたり、作業していない他のタブを閉じたり、すべてのタブを一度に閉じることができます。

手順

1. CloudShell セッション タブのアクション メニューを選択します。
2. 次のいずれかを選択します。
    - [CloudShell]タブウィンドウで[X]を選択して、一度に1つのタブを閉じます。
    - 作業中のタブを除く、開いている他のすべてのタブを閉じるには、*[他のタブを閉じる]*を選択します。
    - すべてのタブを閉じるには、*すべてのタブを閉じる*を選択します。

結果

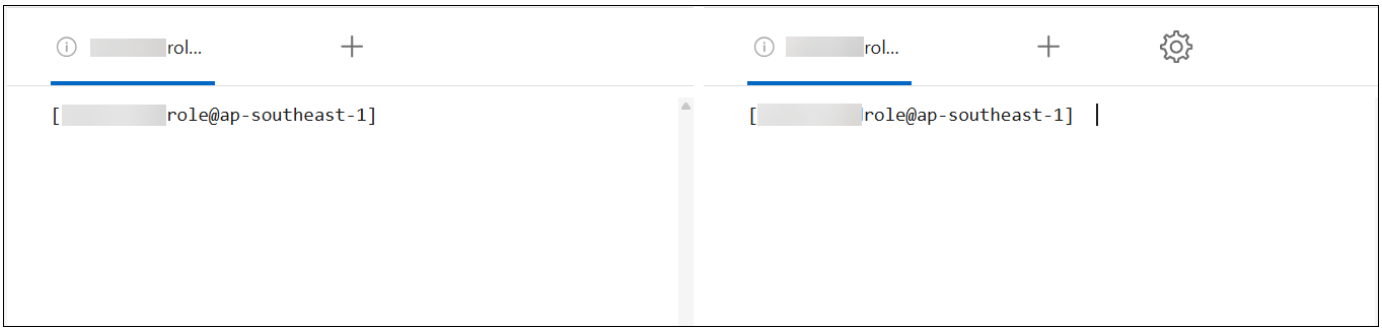
選択したCloudShellセッションタブが閉じます。

CloudShellセッションタブの分割

CloudShellセッションのタブを分割して、複数のタブを同時に表示できます。

ステップ

CloudShellウィンドウの上部、下部、左、または右にCloudShellセッションタブをドラッグアンドドロップして、ビューを分割します。



CloudShellセッションの設定の更新

CloudShellセッションのフォントおよび出力タイプの設定を更新できます。

手順

1. CloudShellセッションをデプロイします。
2. [CloudShell]タブで、設定アイコンを選択します。

    設定ダイアログが表示されます。

3. 必要に応じてフォントサイズと出力タイプを更新します。

> エンリッチ化された出力は、JSONオブジェクトとテーブルの書式設定に適用されます。その他の出力はすべてプレーンテキストで表示されます。

4. * 適用 * を選択します。

結果

CloudShell設定が更新されます。

NetApp Workload Factory から資格情報を削除する

資格情報セットが不要になった場合は、Workload Factory から削除できます。 FSx for ONTAPファイル システムに関連付けられていない認証情報のみを削除できます。

手順

1. いずれかを使用してログインし"コンソールエクスペリエンス"ます。
2. メニューから*管理*を選択し、次に*資格情報*を選択します。
3. *資格情報*ページで、次の操作を行います。
   - Workload Factory コンソールで、資格情報セットのアクション メニューを選択し、[削除] を選択します。*削除*を選択して確認します。
   - NetAppコンソールで、資格情報セットのアクション メニューを選択し、[削除] を選択します。*削除*を選択して確認します。

知識とサポート

サポートに登録します

NetApp Workload Factory とそのストレージ ソリューションおよびサービスに固有のテクニカル サポートを受けるには、サポート登録が必要です。Workload Factory とは別の Web ベースのコンソールであるNetAppコンソールからサポートに登録する必要があります。

サポートに登録しても、クラウド プロバイダー ファイル サービスに対するNetAppサポートは有効になりません。クラウド プロバイダーのファイル サービス、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品の Workload Factory ドキュメントの「ヘルプの取得」を参照してください。

"Amazon FSx for ONTAP"

サポート登録の概要

アカウント ID サポート サブスクリプション (NetAppコンソールの [サポート リソース] ページにある 20 桁の 960xxxxxxxxx シリアル番号) を登録すると、単一のサポート サブスクリプション ID として機能します。各NetAppアカウント レベルのサポート サブスクリプションを登録する必要があります。

登録すると、サポート チケットの開設やケースの自動生成などの機能が有効になります。登録は、以下の説明に従ってNetAppコンソールにNetAppサポート サイト (NSS) アカウントを追加することで完了します。

NetAppサポートのアカウントを登録する

サポートに登録し、サポート資格を有効にするには、アカウント内の 1 人のユーザーがNetAppサポート サイト アカウントをNetAppコンソール ログインに関連付ける必要があります。NetAppサポートに登録する方法は、 NetAppサポート サイト (NSS) アカウントをすでにお持ちかどうかによって異なります。

NSSアカウントをお持ちの既存のお客様

NSS アカウントをお持ちのNetApp のお客様の場合は、 NetAppコンソールからサポートに登録するだけです。

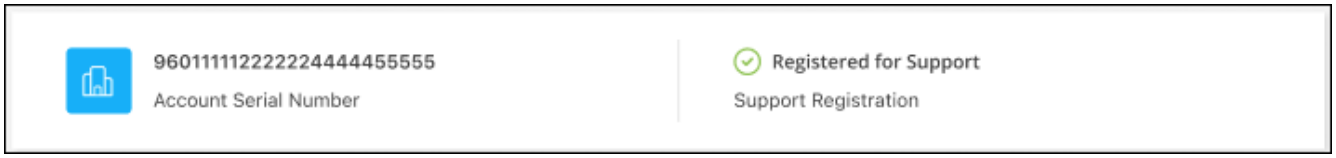
手順

1. Workload Factory コンソールの右上で、[ヘルプ] > [サポート] を選択します。

   このオプションを選択すると、新しいブラウザ タブでNetAppコンソールが開き、サポート ダッシュボードが読み込まれます。

2. NetAppコンソール メニューから、管理 を選択し、資格情報 を選択します。
3. [ユーザクレデンシャル]*を選択します。
4. [NSSクレデンシャルの追加]*を選択し、NetApp Support Site（NSS）認証プロンプトに従います。
5. 登録プロセスが正常に完了したことを確認するには、[ヘルプ]アイコンを選択し、*[サポート]*を選択します。

[リソース]ページに、アカウントがサポートに登録されていることが表示されます。



NetAppコンソール ログインにNetAppサポート サイト アカウントを関連づけていない場合、他のNetAppコンソール ユーザーには同じサポート登録ステータスが表示されません。ただし、これはNetAppアカウントがサポートに登録されていないことを意味するものではありません。アカウント内の 1 人のユーザーがこれらの手順を実行していれば、アカウントは登録済みになります。

NSSアカウントを持たない既存のお客様

既存のNetApp顧客であり、既存のライセンスとシリアル番号を持っているものの、NSS アカウントを持っていない場合は、NSS アカウントを作成し、それをNetAppコンソール ログインに関連付ける必要があります。

手順

1. NetAppサポートサイトのアカウントを作成するには、 "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. 上記で使用したNetAppアカウントのシリアル番号 (960xxxx) を必ずシリアル番号フィールドにコピーしてください。これにより、アカウント処理が高速化されます。
2. 以下の手順を実行して、新しいNSSアカウントをNetAppコンソールログインに関連付けます。NSSアカウントをお持ちの既存のお客様 。

ネットアップのソリューションを初めて導入する場合は

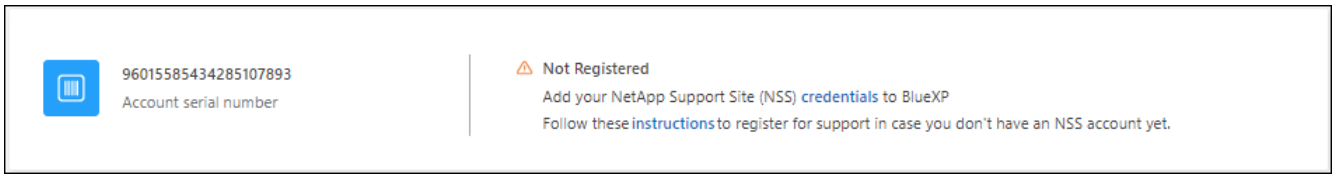
ネットアップ製品を初めてご利用になり、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

手順

1. Workload Factory コンソールの右上で、[ヘルプ] > [サポート] を選択します。

   このオプションを選択すると、新しいブラウザ タブでNetAppコンソールが開き、サポート ダッシュボードが読み込まれます。

2. [Support Resources]ページでアカウントIDのシリアル番号を確認します。



メニューのスクリーンショット。サポートは最初に表示されるオプションです"]

3. [I am not a registered NetApp Customer]に移動して "ネットアップサポート登録サイト" 選択します。
4. 必須フィールドに入力します（赤いアスタリスクのフィールド）。
5. [製品ライン（Product Line ）]フィールドで、[Cloud Manager *]を選択し、該当する課金プロバイダーを

選択します。

6. 上記の手順2からアカウントのシリアル番号をコピーし、セキュリティチェックを完了して、ネットアップのグローバルデータプライバシーポリシーを確認します。

   この安全なトランザクションを完了するために、メールボックスに電子メールがすぐに送信されます。確認メールが数分で届かない場合は、必ずスパムフォルダを確認してください。

7. Eメールからアクションを確認します。

   確認ではネットアップにリクエストが送信され、NetApp Support Site アカウントを作成することを推奨します。

8. NetAppサポートサイトのアカウントを作成するには、 "NetApp Support Site ユーザー登録フォーム"
   a. 適切なユーザレベルを選択してください。通常は*ネットアップのお客様/エンドユーザ*がこれに該当します。
   b. シリアル番号フィールドには、上記のアカウントのシリアル番号（960xxxx）を必ずコピーしてください。これにより、アカウント処理が高速化されます。

終了後

このプロセスについては、ネットアップからご連絡ください。これは、新規ユーザ向けの1回限りのオンボーディング演習です。

NetAppサポートサイトのアカウントを取得したら、以下の手順を実行して、アカウントをNetAppコンソールのログインに関連付けます。NSSアカウントをお持ちの既存のお客様 。

ヘルプを表示します

NetApp は、Workload Factory とそのクラウド サービスをさまざまな方法でサポートします。ナレッジベース (KB) 記事やコミュニティ フォーラムなど、広範な無料のセルフサポート オプションが 24 時間 365 日ご利用いただけます。サポート登録には、Webチケットによるリモートテクニカルサポートも含まれます。

FSx for ONTAPのサポートを利用する

FSx for ONTAP、そのインフラストラクチャ、またはサービスを使用するソリューションに関連するテクニカル サポートについては、その製品の Workload Factory ドキュメントの「ヘルプの取得」を参照してください。

"Amazon FSx for ONTAP"

Workload Factoryおよびそのストレージソリューションおよびサービスに固有のテクニカルサポートを受けるには、以下に説明するサポートオプションを使用してください。

セルフサポートオプションを使用します

次のオプションは、 1 日 24 時間、週 7 日間無料でご利用いただけます。

- ドキュメント

現在表示している Workload Factory のドキュメント。

- "ナレッジベース"

  Workload Factory ナレッジベースを検索して、問題のトラブルシューティングに役立つ記事を見つけます。

- "コミュニティ"

  Workload Factory コミュニティに参加して、進行中のディスカッションをフォローしたり、新しいディスカッションを作成したりしてください。

ネットアップサポートと一緒にケースを作成します

上記のセルフサポートオプションに加え、サポートを有効にしたあとで問題が発生した場合は、ネットアップサポートの担当者と相談して解決できます。

始める前に

*ケースの作成*機能を使用するには、まずサポートに登録する必要があります。NetAppNetAppサイトの資格情報を Workload Factory ログインに関連付けます。"サポートに登録する方法について説明します" 。

手順

1. Workload Factory コンソールの右上で、[ヘルプ] > [サポート] を選択します。

   このオプションを選択すると、新しいブラウザ タブでNetAppコンソールが開き、サポート ダッシュボードが読み込まれます。

2. [**Resources**]ページで、[Technical Support]で次のいずれかのオプションを選択します。

   a. 電話で誰かと話をしたい場合は、*[電話]*を選択します。netapp.comのページに移動し、電話番号が表示されます。

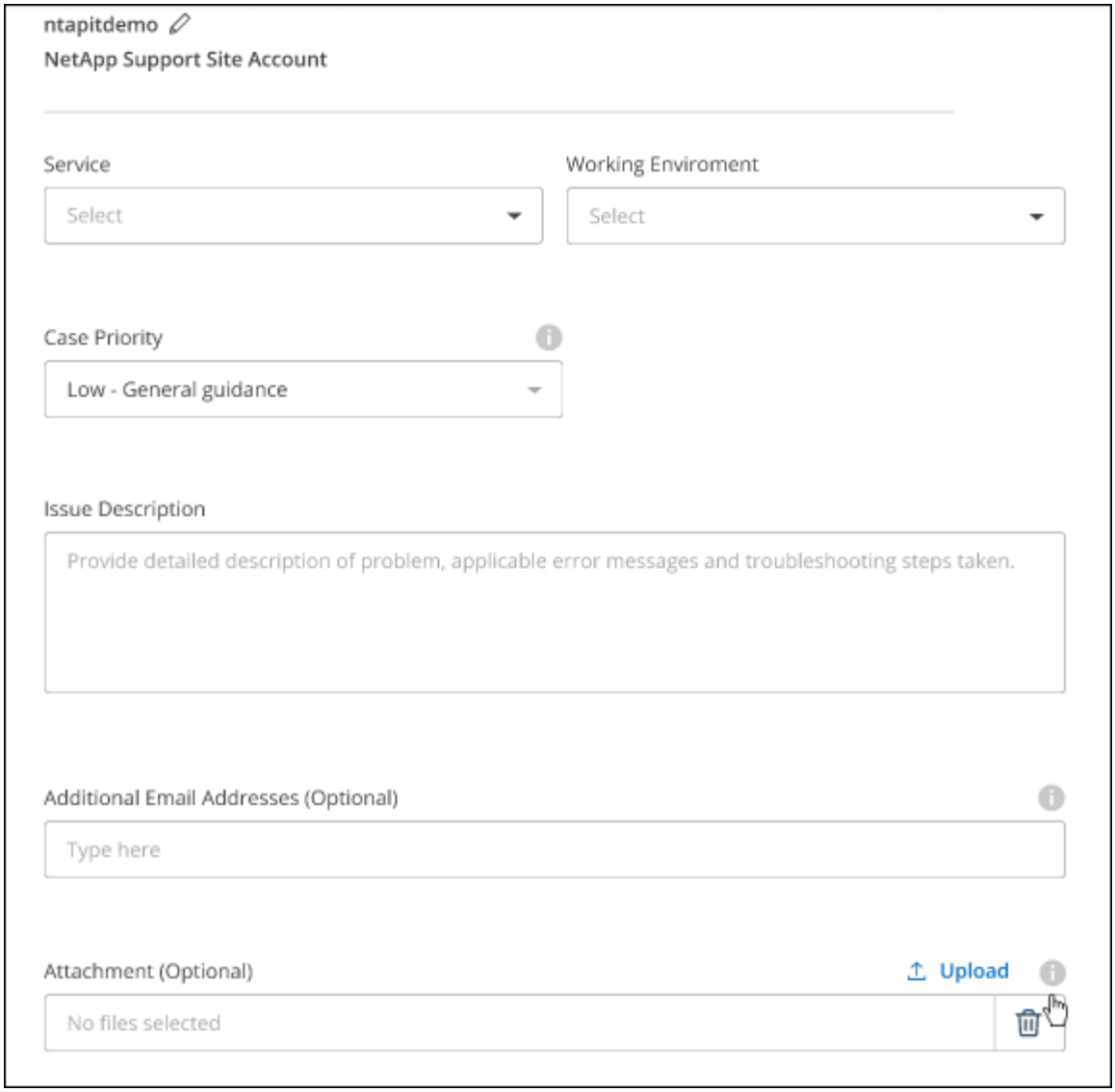
   b. [ケースの作成]*を選択して、NetAppサポートスペシャリストとのチケットをオープンします。

      - * Service ： Workload Factory *を選択します。
      - ケース優先度：ケースの優先度を選択します。優先度は、[低]、[中]、[高]、[クリティカル]のいずれかになります。

        これらの優先度の詳細を確認するには、フィールド名の横にある情報アイコンの上にマウスポインタを合わせます。

      - *事象の説明 *：実行したエラーメッセージやトラブルシューティング手順など、問題の詳細な概要 を入力します。
      - その他のメールアドレス：この問題 を他のユーザーに知らせる場合は、追加のメールアドレスを入力します。
      - 添付ファイル（オプション）：一度に1つずつ、最大5つの添付ファイルをアップロードできます。

        添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。



終了後

ポップアップにサポートケース番号が表示されます。ネットアップのサポート担当者がケースを確認し、すぐに対応させていただきます。

サポートケースの履歴を確認するには、*[設定]>[タイムライン]*を選択し、「サポートケースの作成」というアクションを検索します。右端のボタンをクリックすると、アクションを展開して詳細を表示できます。

ケースを作成しようとすると、次のエラーメッセージが表示される場合があります。

"選択したサービスに対してケースを作成する権限がありません"

このエラーは、NSS アカウントとそれに関連付けられているレコード会社が、 NetAppコンソール アカウントのシリアル番号のレコード会社と同じではないことを意味している可能性があります (つまり、960xxxx) またはシステムのシリアル番号。次のいずれかのオプションを使用してサポートを求めることができます。

- 製品内のチャットを使用します
- テクニカル以外のケースを https://mysupport.netapp.com/site/help

サポートケースの管理（プレビュー）

アクティブなサポート ケースと解決済みのサポート ケースをNetAppコンソールから直接表示および管理できます。NSS アカウントおよび会社に関連付けられたケースを管理できます。

ケース管理はプレビューとして使用できます。今後のリリースでは、この点をさらに改良し、機能を強化する予定です。製品内のチャットでご意見をお寄せください。

次の点に注意してください。

- ページ上部のケース管理ダッシュボードには、次の2つのビューがあります。
  - 左側のビューには、指定したユーザNSSアカウントによって過去3カ月間にオープンされたケースの総数が表示されます。
  - 右側のビューには、ユーザのNSSアカウントに基づいて、過去3カ月間にオープンしたケースの総数が会社レベルで表示されます。

  テーブルの結果には、選択したビューに関連するケースが反映されます。

- 目的の列を追加または削除したり、[優先度]や[ステータス]などの列の内容をフィルタリングしたりできます。他の列には、並べ替え機能だけがあります。

  詳細については、以下の手順を参照してください。

- ケースごとに、ケースノートを更新したり、ステータスが「Closed」または「Pending Closed」でないケースをクローズしたりすることができます。

手順

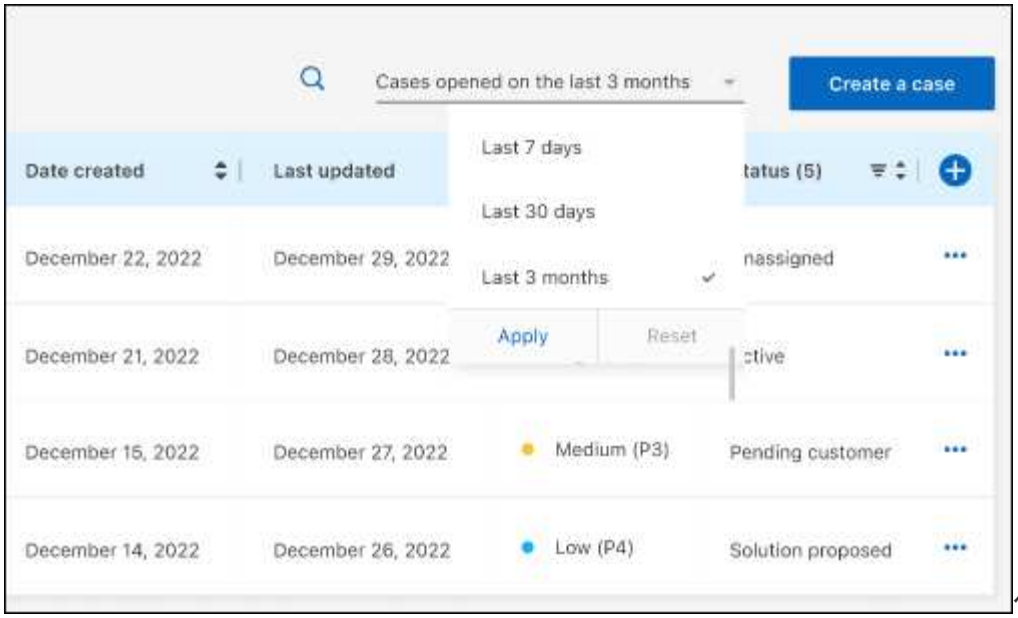
1. Workload Factory コンソールの右上で、[ヘルプ] > [サポート] を選択します。

   このオプションを選択すると、 NetAppコンソールの新しいブラウザ タブが開き、サポート ダッシュボードが読み込まれます。

2. *ケース管理*を選択し、プロンプトが表示されたら、NSS アカウントをNetAppコンソールに追加します。

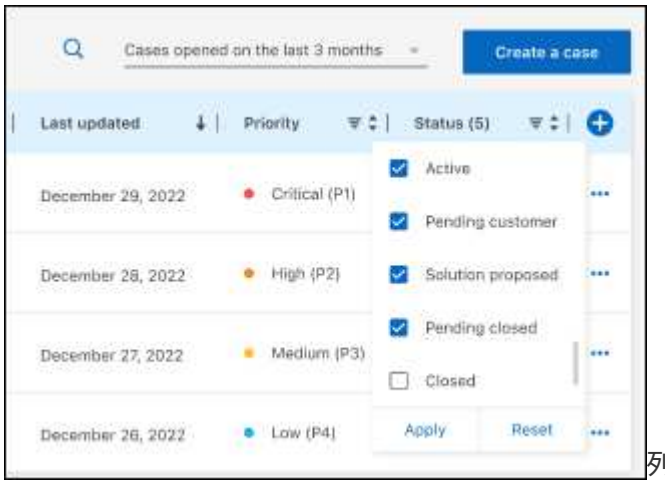
   ケース管理 ページには、 NetAppコンソール ユーザー アカウントに関連付けられている NSS アカウントに関連するオープン ケースが表示されます。これは、**NSS** 管理 ページの上部に表示される NSS アカウントと同じです。

3. 必要に応じて、テーブルに表示される情報を変更します。
   - [Organization’s Cases]*で[View]*を選択すると、会社に関連付けられているすべてのケースが表示されます。
   - 正確な日付範囲を選択するか、別の期間を選択して、日付範囲を変更します。



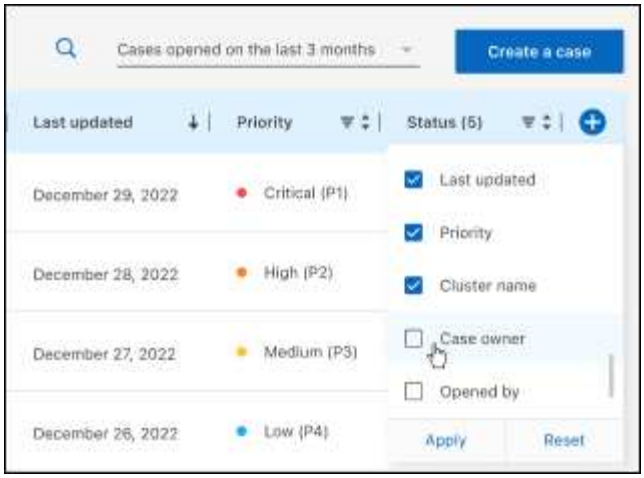
ページのテーブルの上にあるオプションのスクリーンショット。正確な日付範囲、または過去7日、30日、または3カ月を選択できます。"]

- 列の内容をフィルタリングします。



列のフィルタオプションのスクリーンショット。[Active]や[Closed]など、特定のステータスに一致するケースを除外できます。"]

- テーブルに表示される列を変更するには、を選択し、表示する列を選択します。

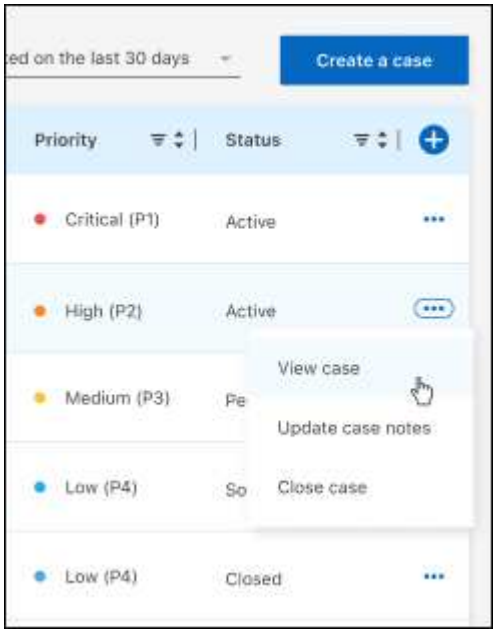


4. 使用可能なオプションのいずれかを選択して、既存のケースを管理し ••• ます。

   - ケースの表示:特定のケースの詳細を表示します。
   - ケースノートの更新：問題の詳細を入力するか、*ファイルのアップロード*を選択して最大5つのファイルを添付します。

     添付ファイルはファイルあたり25 MBに制限されています。サポートされているファイル拡張子は、txt、log、pdf、jpg/jpeg、rtf、 doc/docx、xls/xlsx、およびcsv。

   - ケースをクローズ：ケースをクローズする理由の詳細を入力し、*ケースをクローズ*を選択します。



NetApp Workload Factory に関する法的通知

法的通知では、著作権に関する声明、商標、特許などにアクセスできます。

著作権

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

商標

NetApp、NetAppのロゴ、およびNetAppの商標ページに記載されているマークは、NetApp、Inc.の商標です。その他の会社名および製品名は、それを所有する各社の商標である場合があります。

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

特許

NetAppが所有する特許の最新リストは、次のサイトで参照できます。

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

プライバシーポリシー

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

オープンソース

通知ファイルには、ネットアップソフトウェアで使用されるサードパーティの著作権およびライセンスに関する情報が記載されています。

"NetAppワークロード ファクトリー"

著作権に関する情報

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S.このドキュメントは著作権によって保護されています。著作権所有者の書面による事前承諾がある場合を除き、画像媒体、電子媒体、および写真複写、記録媒体、テープ媒体、電子検索システムへの組み込みを含む機械媒体など、いかなる形式および方法による複製も禁止します。

ネットアップの著作物から派生したソフトウェアは、次に示す使用許諾条項および免責条項の対象となります。

このソフトウェアは、ネットアップによって「現状のまま」提供されています。ネットアップは明示的な保証、または商品性および特定目的に対する適合性の暗示的保証を含み、かつこれに限定されないいかなる暗示的な保証も行いません。ネットアップは、代替品または代替サービスの調達、使用不能、データ損失、利益損失、業務中断を含み、かつこれに限定されない、このソフトウェアの使用により生じたすべての直接的損害、間接的損害、偶発的損害、特別損害、懲罰的損害、必然的損害の発生に対して、損失の発生の可能性が通知されていたとしても、その発生理由、根拠とする責任論、契約の有無、厳格責任、不法行為（過失またはそうでない場合を含む）にかかわらず、一切の責任を負いません。

ネットアップは、ここに記載されているすべての製品に対する変更を随時、予告なく行う権利を保有します。ネットアップによる明示的な書面による合意がある場合を除き、ここに記載されている製品の使用により生じる責任および義務に対して、ネットアップは責任を負いません。この製品の使用または購入は、ネットアップの特許権、商標権、または他の知的所有権に基づくライセンスの供与とはみなされません。

このマニュアルに記載されている製品は、1つ以上の米国特許、その他の国の特許、および出願中の特許によって保護されている場合があります。

権利の制限について：政府による使用、複製、開示は、DFARS 252.227-7013（2014年2月）およびFAR 5252.227-19（2007年12月）のRights in Technical Data -Noncommercial Items（技術データ - 非商用品目に関する諸権利）条項の(b)(3)項、に規定された制限が適用されます。

本書に含まれるデータは商用製品および / または商用サービス（FAR 2.101の定義に基づく）に関係し、データの所有権はNetApp, Inc.にあります。本契約に基づき提供されるすべてのネットアップの技術データおよびコンピュータ ソフトウェアは、商用目的であり、私費のみで開発されたものです。米国政府は本データに対し、非独占的かつ移転およびサブライセンス不可で、全世界を対象とする取り消し不能の制限付き使用権を有し、本データの提供の根拠となった米国政府契約に関連し、当該契約の裏付けとする場合にのみ本データを使用できます。前述の場合を除き、NetApp, Inc.の書面による許可を事前に得ることなく、本データを使用、開示、転載、改変するほか、上演または展示することはできません。国防総省にかかる米国政府のデータ使用権については、DFARS 252.227-7015(b)項（2014年2月）で定められた権利のみが認められます。

商標に関する情報

NetApp、NetAppのロゴ、http://www.netapp.com/TMに記載されているマークは、NetApp, Inc.の商標です。その他の会社名と製品名は、それを所有する各社の商標である場合があります。