NetApp Workload Factoryの情報セキュリティ

Information Security for Workload Factory

NetApp
September 16, 2026

目次

NetApp Workload Factoryの情報セキュリティについて学ぶ

情報セキュリティは、NetApp Workload Factory の設計と運用の中核をなす部分です。情報セキュリティ、クラウドプラットフォーム、ストレージの各チームは、これらの詳細情報を活用して、企業のセキュリティ要件をサポートする形で Workload Factory を評価・導入することができます。

Workload Factoryとは

Workload Factory は、Amazon FSx for NetApp ONTAP を使用して、ワークロード（ストレージ、VMware 移行、EDA プロジェクト、データベース環境など）を最適化および管理するための SaaS ライフサイクル管理プラットフォームです。お客様のワークロードは AWS 上で実行されます。

Workload Factory は、AWS を通じてネイティブに利用可能なすべての FSx for ONTAP 操作に AWS API を使用し、プラットフォームでサポートされているものの AWS API を通じてネイティブに利用できない Workload Factory 操作には ONTAP REST API を使用します。

このガイドで使用される基本的なセキュリティ原則

機密保持

ID管理、最小権限の原則、暗号化、ネットワーク境界の設定などを通じて、不正アクセスからデータを保護します。

整合性

権限範囲の設定、変更管理、および監査可能性を活用することで、システムと構成を不正な変更や意図しない変更から保護します。

使用の可否

堅牢なAWS設計と運用監視を通じて、承認されたユーザーがサービスとワークロードにアクセスできるようにします。

このガイドで取り上げる情報の種類

以下のセクションでは、企業のセキュリティ要件をサポートする形で Workload Factory を評価し、オンボードするのに役立つ情報を提供します。

1. セキュリティモデルと責任
   - "セキュリティモデルの概要"
   - "責任の共有範囲"
2. アーキテクチャと接続性
   - "接続性と信頼の経路"
   - "ONTAP実行オプション"
3. アイデンティティ、資格情報、そして最小限の特権

    - "AWSアカウントの統合"
    - "最小権限のアクセス許可階層"
4. データガバナンス、プライバシー、ライフサイクル
    - "データ処理とデータ所在地"
    - "アカウント削除チェックリスト"
5. 可観測性とモニタリング
    - "指標とテレメトリ"
6. AI制御とVPCコンポーネント
    - "AI制御の概要"
    - "Lambdaリンクの概要"

すぐに始める

- まずは_view、planning、analysis_（読み取り専用）の権限から始め、必要に応じて権限を拡張してください。
- AWS CloudTrail を使用して、統合ロールのアクティビティを検証します `sts:AssumeRole`。
- LambdaリンクまたはNetApp Consoleエージェントのデプロイを必要とするONTAPネイティブ操作が必要かどうかを事前に決定してください。
- 生成AIの使用が許可されているかどうか、また居住地の制約により単一リージョン推論プロファイルが必要かどうかを事前に決定してください。

セキュリティモデルと責任

NetApp Workload Factory のセキュリティモデルについて

NetApp Workload Factoryは、AWS環境でAmazon FSx for NetApp ONTAP上で実行されるワークロードの管理と最適化を支援するSaaSコントロールプレーンです。セキュリティの成果は、NetApp、AWS、およびお客様の組織間での責任共有によって決まります。

高レベルのセキュリティモデル

- Workload Factoryは、IAMのassume-roleモデルを使用して、お客様のアカウント内のAWS APIを呼び出すための一時的なAWS STS認証情報を取得します。
- ワークフローによっては、AWS API を通じて公開されていない ONTAP ネイティブの操作が必要となる場合があります。そのような操作は、お客様がデプロイした実行コンポーネント（Lambda リンクなど）を使用して、VPC 内で実行できます。
- 観測可能性シグナル（メトリクス、テレメトリ、運用記録）は、運用監視および調査をサポートします。

重要な復習問題

- Workload Factoryは、お客様のAWSアカウントに対してどのようなアクセス権限（ロールの信頼＋アクセス許可）を必要としますか？
- 想定されるワークフロー（AWS APIのみの操作、またはVPCコンポーネントを介したONTAPネイティブ操作）には、どの実行パスが適用されますか？
- どのようなデータカテゴリ（設定/メタデータ、運用ログ/イベント、テレメトリ）が処理され、それらはどこに保存されますか？
- どのような監視シグナルが存在し、それらの保持特性はどのようなものですか？

次の手順

- "NetApp Workload Factoryの共同責任の境界"
- "NetApp Workload Factory の接続性と信頼パス"
- "NetApp Workload Factoryの最小権限のアクセス許可階層"

NetApp Workload Factoryの共同責任の境界

NetApp Workload Factory のセキュリティ責任は、NetApp （SaaS運用）、AWS （クラウドインフラストラクチャおよびマネージドサービス）、およびお客様（顧客設定）の間で共有されます。各当事者の責任範囲を理解することで、AWS環境を正しく構成し、セキュリティ上のギャップを回避することができます。これらの境界線は、NetApp が運用するもの、AWS が保護するもの、およびお客様自身が設定・維持する必要があるものを明確にします。

NetAppの責任範囲（サービス側）

NetAppは、Workload Factory SaaSプラットフォームの運用とセキュリティ確保を担当しています。これには、保存された構成参照と運用データのサービス側での処理が含まれます。

AWSの責任範囲（クラウドプラットフォーム）

AWS は、デプロイメントやワークフローで使用されるクラウドインフラストラクチャとマネージドサービス（例：IAM/STS、FSx for ONTAP、CloudWatch、KMS、Secrets Manager、CloudFormation、Lambda、およびネットワークプリミティブ）のセキュリティに責任を負います。

お客様の責任（お客様の設定）

お客様は以下の責任を負います：

- AWS IAMロール、信頼ポリシー、および最小権限のアクセス許可
- VPCの制御（サブネット、セキュリティグループ、ルーティング、エンドポイント、およびエグレス）
- クレデンシャル管理（ワークフローで必要な場合は ONTAP クレデンシャルを含む）
- 暗号化とキー管理の決定（たとえば、FSx for ONTAP のオプションのカスタマー管理 KMS キー）
- 監視、アラート、データ保持ポリシー、およびインシデント対応プロセス

収集する証拠

- IAMロールの信頼関係（外部ID条件を含む）
- IAM権限階層の選択とポリシー成果物
- ネットワーク境界の決定（AWS APIのみか、LambdaリンクなどのVPC実行コンポーネントか）
- 可観測性に関する決定と保持に関する期待
- AI有効化の決定（AI診断は、明示的に無効化されない限り、デフォルトで有効になります）

NetApp Workload Factory オンボーディングセキュリティワークフロー

NetApp Workload Factoryへのオンボーディングは、製品の使用を開始する前に、お客様のAWS環境への安全なアクセスを確立します。このプロセスは、AWSの信頼設定、権限スコープの設定、接続性のセットアップ、可観測性の検証、およびオプションのAI診断の有効化を組み合わせたものです。

ステップ1：オンボーディングの方針を決定する

- AWSアカウントと環境境界（例：本番環境と非本番環境の分離）を特定します。
- 必要なワークフロー（読み取り専用の検出、プロビジョニング、ONTAPネイティブ操作）を特定します。
- ワークフローのニーズに基づいて、VPC実行コンポーネント（例：Lambda リンク）をデプロイするかどうかを決定します。

- AI診断を有効にするかどうかを決定します（デフォルトでは有効）。

関連情報

- "認証情報の種類"
- "Lambdaリンクの概要"
- "AI制御の概要"

ステップ2：AWSの信頼関係とアクセスを確立する

1. AWSアカウントにIAMロールをデプロイします。
2. 信頼ポリシーで外部IDを使用したゲートロールの引き受けを行います。
3. Workload Factory にロール ARN と外部 ID を登録します。

関連情報

"AWSアカウントの統合"

ステップ3：最小権限のアクセス許可を適用する

1. 想定するワークフローをサポートする最小限の権限レベルを選択してください。
2. リクエストごとのセッションポリシーによって、実行される操作に対するアクションが制限されていることを確認します。

関連情報

"NetApp Workload Factoryの最小権限のアクセス許可階層"。

ステップ4：接続性とVPC境界の設定（必要に応じて）

1. AWSエンドポイントへの必要なネットワークパスを検証します。
2. ONTAPネイティブ操作が必要な場合は、VPC内で適切な実行オプションをデプロイして検証してください。

関連情報

- "NetApp Workload Factory の接続性と信頼パス"
- "NetApp Workload FactoryにおけるONTAPの実行オプション"

ステップ5：可観測性の検証

1. メトリクスとテレメトリが想定どおりに収集および保持されていることを確認してください。
2. トラブルシューティングや調査に必要な運用記録にアクセスできることを確認してください。

関連情報

- "NetApp Workload Factoryの可観測性の概要"
- "NetApp Workload Factoryのメトリクスとテレメトリ"

ステップ6：AI診断を有効にする（オプション）

AI診断はデフォルトで有効になっています。これらを有効にする場合は、前提条件を満たしていること、および必要な最小限の権限範囲であることを確認してください。

関連情報

- "Bedrock の NetApp Workload Factory AI 診断へのオプトイン"
- "NetApp Workload FactoryにおけるAIツールの境界"

NetApp Workload Factoryのコンプライアンスとセキュリティ体制

NetApp Workload Factoryは、コンプライアンスとセキュリティを最優先事項として構築されています。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。"AWSセキュリティ機能"に加えて、NetApp Workload Factoryには"SOC2 Type 1、SOC2 Type 2、およびHIPAA準拠"があります。

Amazon FSx for NetApp ONTAP for NetApp Workload Factory は"エンタープライズアプリケーションをデプロイするためのAWSソリューション"であり、AWS Well-Architected のベストプラクティスに準拠しています。

アーキテクチャと接続性

NetApp Workload Factory の接続性と信頼パス

NetApp Workload Factoryは、AWS API、お客様のAWSアカウントリソース、AWS Lambdaリンク、およびAmazon Bedrockと通信しますが、それぞれ独自のプロトコル、ポート、および認証方法を使用します。これらの接続は、AWS管理プレーン、ONTAPデータプレーン、およびLambdaリンクトラフィックを分離するグループに整理されており、信頼境界を個別に評価できます。

接続経路

Workload Factory は、AWS および ONTAP リソースの検出、プロビジョニング、管理においてそれぞれ特定の目的を果たす、複数の異なる接続パスを確立します。一部のパスは想定される AWS 認証情報を使用して Workload Factory 自体から開始されますが、他のパスは VPC 内で動作する Lambda リンクを経由して実行され、ONTAP 管理エンドポイントを公開せずに到達します。Amazon Bedrock へのオプションのパスは、AI による診断をサポートしており、組織がその機能を有効にした場合にのみ有効になります。

次のセクションでは、各パスについて、関連する AWS または ONTAP API、使用される認証情報または認証方法、およびパスがアクティブかどうかを決定する条件を説明します。これらのパスを理解することで、Workload Factory が必要とするネットワーク アクセスと権限、およびデータがアカウントまたは VPC の境界を越える場所を評価できます。

Workload Factory から **AWS API** へ

Workload Factory は `DescribeFileSystems`、 `DescribeVolumes`、 `CreateVolume`、 `UpdateVolume`、 `DeleteVolume`、
`CreateFileSystem`、 `CreateBackup`、 `DescribeBackups`、およびEC2/VPC APIをサブネットとセキュリティグループの検出に使用します。

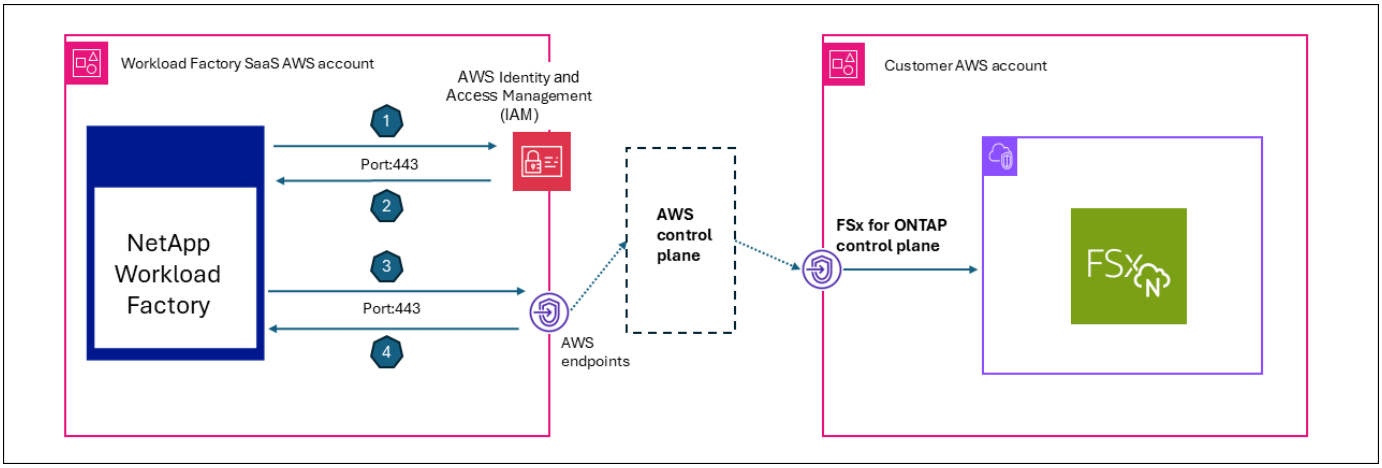
- 収集サービスは、約5時間ごとにスキャンを実行します。
- CRUD操作はオンデマンドで実行されます。
- すべての呼び出しは、外部IDを持つSTS が想定する一時的な認証情報を使用します。

Workload Factory からお客様の **AWS** アカウントリソースへ（オーケストレーションと自動化）

Workload Factory はAWSと連携して、リソースの通信と作成を行います。オーケストレーションと自動化は、いくつかの方法で行われます。

- AWS CloudFormation テンプレート：Workload Factory は AWS CloudFormation テンプレートを使用して、ロールやファイルシステムなどのリソースを作成します。たとえば、ユーザーインターフェースでファイルシステムを作成すると、Workload Factory は CloudFormation を直接呼び出し、お客様の AWS アカウントにリダイレクトします。
- AWS API 呼び出し：Workload Factory は AWS API 呼び出し（STS `AssumeRole`）を使用して、FSx for ONTAP 関連のアクティビティの API コマンドを送信します。
- AWS Lambda：Workload Factory はCloudFormationを使用して、ONTAP と通信するリンク用の AWS Lambda 関数をデプロイします。

次の図は、Workload Factory が NetApp AWS アカウントと、FSx for ONTAP ファイルシステムを持つお客様の AWS アカウントとの間の信頼関係をどのように使用するかを示しています。



1. Workload Factory は、AWS IAM サービスからのお客様に合わせた外部 ID を使用して、AWS STS をリクエストします `AssumeRole`。
2. AWS IAMサービスはロールを取得し、セッションを作成します。
3. Workload Factoryは、セッション権限を付与したAWS APIリクエストを発行します。
4. Workload Factory は、FSx for ONTAP コントロールプレーンから AWS API レスポンスを受け取ります。

Lambda から **ONTAP** 管理エンドポイントへのリンク

Lambda リンクは、お客様の VPC 内で実行され、ONTAP を外部に公開することなくプライベートサブネットへのアクセスを可能にします。リンクから ONTAP 管理エンドポイントへのすべての接続は送信専用であるため、受信接続や公開エンドポイントは必要ありません。このリンクは、Amazon FSx for NetApp ONTAP API が公開していない ONTAP ネイティブ操作にのみ使用されます。

Workload Factory は、ボリューム、ストレージ VM、クラスタ操作、および読み取り専用の診断データとパフォーマンスデータに対して、以下のプロトコルを使用します：

- HTTPS/443（REST）
- SSH/22（CLI）

AWS Secrets Manager への **Lambda** リンク（**ONTAP** 認証情報の取得）

ONTAP 管理者認証情報が AWS Secrets Manager に保存されている場合にのみ使用します（代替案：エンベロープ暗号化を使用して Workload Factory で暗号化された認証情報）。

- プロキシフォワーダーは、ヘッダー内で `x-aws-secret-arn`（Base64エンコード）を渡します。
- Lambdaは実行時に `GetSecretValue`をリンク呼び出しして、パスワードを取得します。

これにより、パスワードはアカウントの境界内に留まり、Workload Factoryからの送信が防止されます。

Workload Factory およびお客様コンポーネントから **Amazon Bedrock** （**AI**診断）

このパスは、AI診断が有効になっている場合にのみ使用されます。

- イベントアナライザーは、EMS分析およびレイテンシー診断のためにこのパスを使用します。
- Bedrockは想定される認証情報と推論プロファイルARNを使用して実行されるため、データはNetAppのアカウントに流れません。

Bedrockに送信されるデータには、EMSイベントJSON、QoS統計、ボリューム構成、集計データ、ノード情報などが含まれます。このパスは、組織ごとに推論プロファイルが構成されている場合にのみ有効になります(`ai_analyzer_config` テーブル）。

接続グループ（プロトコル、ポート、認証）

グループ**A — AWS**管理プレーンの信頼パス（想定される認証情報）

接続	**Protocol**	ポート	送受信方向	認証	**Justification**
STS AssumeRole	HTTPS	443	WF → AWS STS（お客様アカウント）	IAM認証情報 + ExternalId	一時的なクロスアカウント認証情報を取得する
FSx API（Describe/Create/Update/Delete）	HTTPS	443	WF → AWS FSx エンドポイント（お客様リージョン）	STS一時認証情報	ファイルシステムとボリュームのライフサイクル管理
EC2/VPC API	HTTPS	443	WF → AWS EC2 エンドポイント	STS一時認証情報	セキュリティグループ、サブネット、およびVPCの検出
CloudFormation API	HTTPS	443	WF → AWS CFN エンドポイント	STS一時認証情報	IAMロールとFSxプロビジョニングのためのスタック展開
Secrets Manager GetSecretValue	HTTPS	443	WF → AWS Secrets Manager エンドポイント（お客様アカウント）	STS一時認証情報	ONTAP 管理者パスワードの取得（Secrets Manager に保存されている場合）
KMS 暗号化 / 復号	HTTPS	443	WF → AWS KMS エンドポイント	STS一時認証情報	ボリューム暗号化キー操作

すべてのAWS API呼び出しは、お客様のリージョンエンドポイントを使用し、設定によってはVPCエンドポイントを経由してルーティングすることも可能です。

グループ**B — ONTAP**データプレーン

ONTAPデータプレーンは常に Lambda リンクを介してプロキシされます。Workload Factory サービスは ONTAP に直接接続することはありません。

接続	**Protocol**	ポート	送受信方向	認証	**Justification**
ONTAP REST API	HTTPS	443	リンク（顧客VPC）→ ONTAP 管理LIF	基本認証（ユーザー名/パスワード）またはSecrets Manager ARN	クラスタ、ボリューム、ストレージVM構成、QoS、EMSイベント、ARPステータス
ONTAP SSH CLI	SSH	22	リンク（顧客VPC）→ ONTAP 管理LIF	パスワード認証	診断コマンド（QoS統計、df、イベントログ、効率）

プロキシ転送装置のルーティング戦略（優先順位）：

1. 明示的 `x-link-id`ヘッダー：データベースから Lambda ARN を検索する
2. ターゲットID（FSx ファイルシステムID）：関連するリンクを見つける
3. コンソールエージェントID：メッセージブローカーを経由してコンソールエージェントにルーティングします

グループ**C — AWS Lambda**リンク（**VPC**内にデプロイ済み）

接続	**Protocol**	ポート	送受信方向	認証	**Justification**
Lambda Invoke	HTTPS（AWS SDK）	443	WF → AWS Lambda API（顧客アカウント）	IAM (`lambda:InvokeFunction`)	お客様のVPC内からONTAP REST/SSHコマンドを実行する
Lambda → ONTAP	HTTPS + SSH	443つまたは22つ	Lambda（顧客VPC）→ ONTAP管理LIF	基本認証／パスワード	パブリックに公開せずにONTAPへのプライベートサブネットアクセス

グループ**D — NetApp Console Agent**（お客様の**VPC**内の**EC2**、送信専用）

接続	**Protocol**	ポート	送受信方向	認証	**Justification**
エージェントポーリング	HTTPS	443	コンソールエージェント（顧客VPC）→WFメッセージブローカー	ベアラートークン（occm-accessスコープ）	保留中の ONTAP コマンドのロングポーリング（7秒タイムアウト、再接続）
エージェントの対応	HTTPS	443	コンソールエージェント（顧客VPC）→WFメッセージブローカー	ベアラートークン	ONTAPコマンドの実行結果を返す（オプションでzlib圧縮）
コンソールエージェント → ONTAP	HTTPS + SSH	443つまたは22つ	コンソールエージェント（顧客VPC）→ ONTAP管理LIF	基本認証／パスワード	プロキシ経由の ONTAP 操作を実行する

重要な設計：Workload Factory は、Console エージェントへのインバウンド接続を開始することはありません。作業は Redis ストリームにキューイングされ、Console エージェントがポーリング `GET

/messagebroker/v1/requests`して応答 `POST /messagebroker/v1/responses`します。

グループ**E — CloudFormation** カスタムリソースコールバック

接続	**Protocol**	ポート	送受信方向	認証	**Justification**
CloudFormation → WF Lambda	HTTPS	443	CloudFormation（お客様）→ WF Lambda （NetApp）	JWTトークン＋参照トークン	IAMロール作成ステータスを報告し、ロールARNを返送する
ONTAP CloudFormationリソースプロバイダー → リンク	HTTPS	443	CloudFormationリソース Lambda (顧客) → リンク Lambda (顧客)	IAM	スタック操作中に ONTAP リソースを作成／更新／削除する

概要：**VPC**のネットワーク要件

コンポーネント	インバウンド	アウトバウンド
FSx for ONTAP	Link Lambdaまたはコンソールエージェントのセキュリティグループからのポート443と22	該当なし
Lambdaのリンク	None	ポート443（ONTAP、AWS APIs）およびポート22（ONTAP SSH）
コンソールエージェント EC2	None	ポート443（WFエンドポイント、ONTAP、AWS APIs）およびポート22（ONTAP SSH）
VPCエンドポイント（オプション）	該当なし	STS、FSx、S3、Secrets Manager、Lambda、CloudFormation

顧客VPC内のどのコンポーネントも、インバウンドのインターネットアクセスを必要としません。すべての接続は、アウトバウンド開始（コンソールエージェントのポーリング）またはAWSサービスAPIを介した呼び出し（Lambda Invoke）のいずれかです。

NetApp Workload FactoryにおけるONTAPの実行オプション

いくつかの NetApp Workload Factory のワークフローでは、AWS API を通じて公開されていない ONTAP ネイティブの操作が必要です。Workload Factory は、これらの操作を AWS アカウントの境界内に留める 2 つの実行オプションを提供します：VPC 内から ONTAP 操作を実行する Lambda リンク、および EC2 インスタンスからの送信専用接続を使用する NetApp Console Agent です。どちらのオプションでも、ネットワーク、認証情報、ライフサイクルに関する決定事項をセキュリティモデルの範囲内に保ちながら、必要な ONTAP 操作を実行できます。

実行オプション

Lambdaリンク（**VPC**内の**AWS Lambda**）

VPC内からONTAP RESTおよび読み取り専用のONTAP CLI診断を実行しますが、ONTAPを外部に公開しません。

NetApp Console Agent（お客様の**VPC**内の**EC2**、送信専用）

プロキシされた ONTAP 処理を実行します。エージェントが発信接続を開始し、Workload Factory がエージェントへの着信接続を開始することはありません。

セキュリティに関する考慮事項

- ネットワーク境界：必要な送信ポート（443/22）と宛先を確認してください。
- 認証情報の境界：ONTAP 認証情報を Workload Factory に保存する（エンベロープ暗号化）か、AWS Secrets Manager から参照するかを決定します。
- 監査可能性：コンポーネントの動作および障害に関する運用記録を確認します。
- ライフサイクル管理：更新と削除がどのように行われるかを確認します。

関連情報

- "NetApp Workload FactoryのLambdaリンクの概要"
- "NetApp Workload Factory の接続性と信頼パス"
- "NetApp Workload Factoryの暗号化と暗号化キー管理"

アイデンティティ、資格情報、そして最小限の特権

AWS アカウントと NetApp Workload Factory の統合

Workload FactoryはAWS `sts:AssumeRole`を使用してAWSアカウントの一時的な認証情報を取得するため、長期的なAWSアクセスキーはサービスによって保存されません。オンボーディング時に、承認されたAWS API操作に対してWorkload Factoryが引き受けることができるIAMロールを設定します。この際、不正なクロスアカウントアクセスを防止するために、外部IDを使用します。Workload Factoryは、実行時に生成された有効期限の短い認証情報を使用します。この認証情報は、AWSによって各セッション終了後に自動的に期限切れとなります。

AWSアカウントの設定

Workload Factory が AWS アカウントにアクセスできるようにするには：

1. AWS アカウントに IAM ロールをデプロイします（CloudFormation または手動で）。
2. ロールの信頼ポリシーで、外部IDによってゲートされた上で、Workload Factory のサービスプリンシパルがそのロールを引き受けることができるようにしてください。
3. お客様と Workload Factory の間でのみ共有される一意の秘密識別子（UUID v4）として外部 ID を使用します。

   IAMロールの信頼ポリシーに条件として組み込む(`sts:ExternalId`）。

   外部IDは、混乱した代理人による攻撃を防ぎます。クロスアカウントアクセスモデルでは、攻撃者がお客様のロールARNを発見したとしても、対応する外部IDも所持していなければ、そのロールを引き受けることはできません。AWSは、サードパーティのクロスアカウントアクセスにはこのパターンを推奨しています。詳細については、AWS IAMのドキュメントページ"第三者が所有するAWSアカウントへのアクセス"を参照してください。

   外部IDは、クレデンシャルのオンボーディング時に一度生成され、Workload Factoryのデータベースにロール ARNとともに暗号化されて保存されます。

4. Workload Factory にロール ARN と外部 ID を登録します。

ランタイム

実行時に、Workload Factory はお客様の IAM ロールを引き受け、各 AWS API 操作に必要な短期間の認証情報を取得します。

1. Workload Factory がお客様のロール ARN と外部 ID を使用して `sts:AssumeRole`を呼び出します。
2. AWSは一時的な認証情報（アクセスキー、シークレットキー、セッショントークン）を返します。
3. Workload Factoryは、お客様のアカウントにおけるAWS API操作のために一時的な認証情報を使用します。
4. 認証情報は自動的に期限切れになります（デフォルトでは1時間）。

AWS認証情報が NetApp Workload Factory を経由してどのように流れるか

AWS 認証情報フローでは、NetApp Workload Factory は、オンボーディングおよび実行時操作中に、ロール識別子、外部 ID、および有効期限の短い AWS STS 認証情報を処理します。初回セットアップ時に、AWS アカウントに IAM ロールを作成し、Workload Factory のサービスプリンシパルと正しい外部 ID を必要とする信頼ポリシーを設定します。実行時、Workload Factory は保存されたロール ARN と外部 ID を使用して、リクエストごとのセッションポリシーによってスコープが設定された一時的な認証情報を要求し、キャッシュされた認証情報が期限切れになるまで再利用します。

一度限りの設定

初回設定の場合、手順は以下のとおりです。

手順

1. AWSアカウントでCloudFormationスタックを起動するか、IAMロールを手動で作成します。
2. IAMロール信頼ポリシーでは、次の2つの条件が指定されています：
   a. Workload Factory のサービスプリンシパルのみがこれを引き受けることができます。
   b. 発信者は正しい外部IDを提示する必要があります。
3. Workload Factoryは、ロールARNと外部ID（暗号化済み）をデータベースに保存します。

実行時（すべての**API**操作）

実行時、Workload Factory は保存されたロール ARN と外部 ID を使用して、各 API 操作の一時的な AWS STS 認証情報を取得します。流れは次のとおりです：

手順

1. Workload Factoryは、MySQLから保存されているロールARNと外部IDを取得します。
2. この機能は、Redisにキャッシュされた、このロール用の一時的なAWS STS認証情報セットを確認します。
3. キャッシュミスが発生すると、Workload Factory は `sts:AssumeRole`をロール ARN と外部 ID を使用して呼び出します。この呼び出しには、リクエストごとに適用されるインラインセッションポリシーが含まれており、その操作に必要な特定の AWS アクションのみに権限を制限します。
4. AWS STSは、有効期限タイムスタンプ付きの一時的な認証情報（アクセスキーID、シークレットアクセスキー、セッショントークン）を返します。
5. Workload Factoryはこれらの認証情報をRedisにキャッシュし、それらを使用して対象のAWS APIを呼び出します。
6. キャッシュ ヒット時、Workload Factory はSTS呼び出しをスキップし、キャッシュされた認証情報を直接使用します。

セッションポリシー

各STS呼び出しには、必要最小限のAWSアクションに限定されたインラインセッションポリシーが含まれて

います。

関連情報

- "最小権限のアクセス許可階層"

AWS認証情報の保持（NetApp Workload Factory）

Workload Factoryは、有効期限の短いAWS STS認証情報、暗号化されたロールメタデータ、および保持期間を限定した動作によって、認証情報の取り扱いを保護します。認証情報モデルは、保持されるロールメタデータと、API操作に使用される一時的なAWS認証情報を分離します。一時的な認証情報は限られた期間のみキャッシュされ、AWSの規定により自動的に期限切れとなります。認証情報を削除すると、Workload Factoryはそのアカウントの新しい認証情報を取得できなくなります。また、キャッシュされた認証情報はその後まもなく期限切れとなります。

主要な動作

- Workload Factoryは、長期的なAWSアクセスキーを保存しません。

  Workload Factory は、ポインタ（ロール ARN）と共有シークレット（外部 ID）のみを保存します。どちらも単独では AWS へのアクセス権を付与しません。

- 一時的なAWS STS認証情報には、AWSによって定められた最大1時間の有効期限があります。

  Workload Factory は、新しい STS 呼び出しを強制する前に、最大 30 分間、それらを Redis にキャッシュします。

- キャッシュされた認証情報セットの有効期限が15分未満になると、Workload Factoryはそれを破棄し、新しい認証情報を取得します。
- 顧客による認証情報の削除により、Workload Factory がそのアカウントにアクセスする権限は即座に失効します。

  次のAssumeRole呼び出しが失敗し、キャッシュされた認証情報は数分以内に期限切れになります。

保持および保管の概要

データ	保管場所	保持期間	自動期限切れ？	削除方法
IAMロールARN + 外部ID	MySQL（保存時は暗号化）	無期限（お客様が明示的に削除するまで保存されます）	×	顧客がUIで「認証情報を削除」をクリックする

データ	保管場所	保持期間	自動期限切れ？	削除方法
一時的なAWS STS認証情報（アクセスキー＋シークレット＋セッショントークン）	Redis（インメモリキャッシュ）	最大30分（キャッシュの有効期限）。基となるSTS認証情報は、最大1時間（AWSのデフォルト設定）有効です。キャッシュは安全マージンとして、有効期限の5分前に削除されます。	はい（Redis の TTL により自動的に削除されます。AWS認証情報の有効期限は AWS によって管理されます）	自動
ONTAP管理者パスワード	MySQL（KMSを使用したAES-256-CBCエンベロープ暗号化）	無期限（お客様が認証情報を削除するか、ファイルシステムを削除するまで保存される）	×	顧客が認証情報を削除するか、ファイルシステムの削除によってクリーンアップがトリガーされる
復号化されたONTAPパスワード（平文）	メモリ内のみ（ディスクやキャッシュには書き込まれません）	1回のリクエストにかかる時間（ミリ秒）	はい（リクエスト完了後にガベージコレクションされます）	自動

セキュリティ管理

- 外部IDは、混乱した代理攻撃を防ぎます。
- セッションポリシーは、リクエストごとに最小権限の原則を適用します。
- Workload Factory は、有効期限切れのリスクが高い期間が経過する前に、短期間有効な一時的な AWS STS 認証情報を更新します。
- Standard、GovCloud、および中国の環境では、リージョンとアカウントタイプの処理が異なります。
- Workload Factoryは、AWSの長期アクセスキーを一切保存しません。
- Workload Factory は、IAM ロールの権限を一切変更しません。
- Workload Factory は、ロールポリシーで付与された権限を超えて権限を昇格することはありません。
- セッションポリシーは権限を縮小することしかできず、Workload Factory が権限を拡大することはありません。

NetApp Workload Factoryの認証情報の種類

NetAppWorkload Factory は、AWS コントロールプレーンの権限と直接 ONTAP 管理者アクセスを分離するために、分割認証情報モデルを使用しています。AWS IAM ロール

は、ファイルシステム管理、バックアップ管理、リソース検出などの操作のために、Workload Factory を AWS API に対して認証します。ONTAP 認証情報は、管理設定や診断を必要とする操作のために、Lambda リンクを介して ONTAP 管理エンドポイントへの直接アクセスを認証します。一部のワークフローでは、AWS API 操作と直接 ONTAP 管理タスクを組み合わせる場合に、両方の認証情報タイプが必要になります。

認証情報の種類

以下の表は、Workload Factoryで使用される2種類の認証情報と、それぞれの認証対象をまとめたものです。

認証情報の種類	認証先	使用目的
AWS認証情報（AssumeRole）	AWS API	AWS FSxサービスAPIを経由するすべての操作
ONTAP認証情報（管理者パスワード）	ONTAP管理エンドポイント	直接 ONTAP REST API または CLI アクセスが必要な操作

AWS認証情報のみを使用する操作

これらの操作はAWS APIのみとやり取りし、IAMロールのみを必要とします。

- ファイルシステムの作成と削除
- ファイルシステムの容量とスループットの変化
- バックアップの作成と管理
- VPC、サブネット、およびセキュリティグループの検出
- KMSキーの列挙
- CloudWatch メトリクスの取得
- コストエクスプローラーのクエリ
- FSx API を使用したタグ管理

ONTAP認証情報のみの操作

これらの操作は、Lambda リンクを介して ONTAP 管理エンドポイントと直接通信し、ONTAP 管理者クレデンシャルが必要です：

- ボリュームレベルのQoSポリシー設定
- エクスポートポリシーとルールの管理
- ストレージVMプロトコル構成（NFS、CIFS、iSCSI）
- igroupとLUNの管理
- SnapMirror（レプリケーション）構成
- Snapshotポリシー管理（ONTAPレベル）
- パフォーマンス診断（QoS統計、レイテンシの内訳）
- EMSイベントの取得と分析

- ランサムウェア対策保護状況の監視
- FlexCache管理
- ネットワークインターフェース（LIF）クエリ

AWSとONTAPの両方のクレデンシャルを必要とする操作

ワークフロー	AWS認証情報の使用目的	ONTAPに使用される認証情報
AIを活用したイベント分析	Bedrock の呼び出し、ファイルシステムの説明	SSHを使用してEMSイベントを取得し、診断を実行する
ストレージVMセットアップによるファイルシステムの作成	ファイルシステムを作成する（AWS API）	ストレージ VM プロトコルを設定する（ONTAP REST）
エクスポートポリシーによるボリューム作成	ボリュームを作成する（AWS API）	エクスポートポリシールールを設定する（ONTAP REST）
ストレージ容量管理	ファイルシステムの容量を更新する（AWS API）	アグリゲートの使用率を確認する（ONTAP SSH）

関連情報

- "ONTAP実行オプション"
- "Lambdaリンクの概要"

NetApp Workload Factoryの認証情報の保存オプション

NetApp Workload Factory は、最小権限を維持し、ONTAP 管理シークレットの露出を低減する認証情報の処理パターンをサポートします。AI を活用した診断機能は、診断エージェントがストレージ環境を変更することなく監視および診断できるように、利用可能な場合は読み取り専用の ONTAP 認証情報を使用します。Workload Factory が管理する暗号化ストレージを使用するか、AWS Secrets Manager に ONTAP パスワードを保存して Workload Factory に参照情報を提供することができます。この選択は、パスワードの保存場所、暗号化方法、および GovCloud サポートや認証情報のローテーションなどの要件の管理方法に影響します。

読み取り専用ONTAPアクセスモデル

イベント分析やレイテンシー診断などのAIを活用した機能では、Workload Factoryは利用可能な場合に読み取り専用のONTAP認証情報を使用します。読み取り専用の認証情報モデルにより、AI診断エージェントはストレージ環境を変更することができず、監視と診断のみを行います。

認証情報保存オプションの比較

AWS クレデンシャル

AWS認証情報は常にIAMロールを通じて取得されます。Workload Factoryは、ロール情報を内部的に管理することも、AWS Secrets Managerから参照することもできます。

オプション	**AWS** クレデンシャル	何が保存されているか	暗号化
Workload Factory が管理	IAMロールARN + 外部ID	IAMロールARN + 外部ID	ロールARNは秘密情報ではありません（そのまま保存されます）

ONTAP クレデンシャル

Workload Factory は、ONTAP 認証情報を暗号化されたストレージに内部的に管理するか、AWS Secrets Manager から参照することができます。この選択は、パスワードの保存方法、暗号化方法、およびローテーション方法に影響します。

Workload Factory が "ラムダリンク" を通じて ONTAP ファイルシステム API と連携するには、ONTAP 認証情報が必要です。

オプション	**ONTAP** クレデンシャル	何が保存されているか	暗号化
Workload Factory が管理	パスワード（暗号化済み）	ONTAP管理者パスワード（暗号化済み）	ONTAPパスワードはAES-256エンベロープ暗号化を使用します
AWS Secrets Manager	Secrets Manager ARN リファレンス	Secrets Manager ARN	Secrets ARN はシークレットではありません（そのまま保存されます）。AWS Secrets Manager がアカウント内のシークレットを暗号化します。

その他の考慮事項

GovCloud 要件

標準のIAMロールが使用されます。ONTAP認証情報はSecrets Managerを使用する必要があります（パスワードの保存は許可されていません）。

回転

アカウント内のロールポリシーが更新されました。Workload Factory でONTAPパスワードを更新する（マネージドオプション）か、AWS Secrets Manager でパスワードをローテーションしてください。

NetApp Workload Factoryの最小権限のアクセス許可階層

Workload Factory の IAM 権限は、最小権限の要件に合わせていつでも制限できます。例えば、特定のリソース（ARN）へのアクセスを制限したり、タグや CIDR 範囲などの IAM 条件を適用したりできます。

階層型権限モデル

Workload Factoryは、最小権限の原則に沿った階層型権限モデルを採用しています。AWS認証情報を追加する際に、有効にする機能レベルを選択できます。読み取り専用の検出機能から始めて、必要に応じて拡張していくことができます。

Workload Factoryは、外部IDを使用してSTS経由で引き受けるAWSアカウント内のIAMロールを通じて、すべての権限を付与します。

Workload Factoryは、インラインセッションポリシーを使用して、各API呼び出しの範囲をさらに詳細に指定します。

Workload Factory コンソールでは、AI チャット機能 *Ask Me* が、制限オプションを提案し、AWS に適用する更新されたポリシーを生成することで、安全に権限を調整するのに役立ちます。

権限の付与

Workload FactoryにAWS認証情報を追加する際、有効にする権限レベルを選択できます。階層はいつでも有効または無効にできます。

階層は累積的です。上位の階層を有効にすると、下位のすべての階層も自動的に有効になります。

セキュリティ管理

- 外部ID（混乱した代理の保護）
- 操作ごとのセッションポリシー（リクエストごとの最小権限）
- タグベースの条件（セキュリティグループの変更は Workload Factory で作成されたリソースに限定される）
- シークレットARNスコープ（Secrets Managerへのアクセスを `FSxSecret*`に制限）
- 実行時権限の検証（対象を絞った修復のために不足しているアクション/リソースが報告されます）

権限に関するドキュメント

Workload Factory の権限に関する主な参照先は、Workload Factory のセットアップおよび管理に関するドキュメントの "権限リファレンス" です。ストレージ IAM ポリシーからアクセス許可を削除した場合の影響については、こちらの資料をご参照ください。

Amazon CloudWatch の NetApp Workload Factory に対する監視権限

Amazon CloudWatch の監視権限はオプションであり、NetApp Workload Factory では個別の監視スタックをデプロイする場合にのみ適用されます。監視スタックは、ファイルシステムメトリクスの収集、イベントログの公開、CloudWatch ダッシュボードとアラームの管理、および Amazon SNS を介したアラート通知の送信により、運用上の可視性を提供します。また、スタックは監視に必要な ONTAP 認証情報を取得するためのアクセスも必要とします。

必須の**CloudWatch**監視権限

オプションの監視スタックには、以下の権限が必要です。

アクセス許可	目的
fsx:Describe* / fsx:ListTagsForResource	ファイルシステムのメトリクスを収集する
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	ダッシュボードとアラームを管理する
logs:CreateLogGroup / logs:CreateLogStream / logs:PutLogEvents	イベントログを公開する
sns:Publish	アラート通知を送信する
secretsmanager:GetSecretValue	監視用のONTAP認証情報を取得する

データガバナンス、プライバシー、ライフサイクル

NetApp Workload Factoryのデータ処理とデータレジデンシー

NetApp Workload Factoryは、サービスが処理する運用データ、各データクラスがセキュリティモデルにどのように適合するか、データがどこに保存されるか、どのくらいの期間保持されるか、そしてデータが顧客環境から外部に持ち出されるかどうかを説明するカテゴリにデータ処理を整理します。主要なデータクラスには、構成情報とメタデータ、運用ログとイベント、およびテレメトリが含まれます。保持されるデータには、FSx for ONTAP構成スナップショット、認証情報参照、AIの使用状況とコストデータ、監査記録、および短期間有効な応答キャッシュが含まれる場合があります。ストレージと処理の場所はデータタイプによって異なります。一部の情報は顧客のAWSアカウントに残りますが、その他の運用データはNetAppアカウントに保存されます。

Workload Factoryによって処理されるデータクラス

NetApp Workload Factory は、以下のデータクラスを扱います。

- 設定とメタデータ
- 運用ログとイベント
- テレメトリー

Workload Factory が保持するデータクラス

Workload Factory は以下のデータを保持します：

- FSx構成スナップショット（スキャンごとに更新）
- ONTAP認証情報参照、またはKMSエンベロープ暗号化で暗号化された認証情報（選択された認証情報モードによる）
- EDAメトリクス
- CloudFormation テンプレート（7日間 `Expires` ヘッダー）
- AIの利用状況とコストデータ
- 監査記録
- Redis は（FSx の応答を）20 分の TTL でキャッシュします。

情報が保管される場所

AWSアカウント

- ONTAP管理者パスワードはAWS Secrets Managerに保存されます。
- Amazon Bedrock は、お客様の AWS アカウント内の STS が引き受けたロールを通じて、お客様の推論プロファイル ARN を使用して AI 推論（EMS 分析）を処理します。

NetAppアカウント

- FSx構成、バランスプラン、ARP構成、およびAI使用制限
- 一時的なAWS STS認証情報（Redisにキャッシュ）、レスポンスキャッシュ、ロック、およびデプロイメント状態
- CloudFormation/Terraformテンプレート、WAD構成記述子、および圧縮レポート
- AI使用状況計測とコレクターのパフォーマンス指標
- EDA集計指標
- アクション監査証跡
- OpenTelemetry トレース

地域に関する考慮事項

- Amazon Bedrockサービスが利用可能なリージョンに保存されます。
- NetApp 内部は `us-east-1`および `us-west-2`で動作します。

情報の保存期間

このセクションでは、保持対象となるカテゴリをまとめています。詳細な値とポリシーの動作については、リンク先のページを参照してください。

- 認証情報および一時的なAWS STS認証情報の保持："NetApp Workload Factoryの資格情報の保持"
- 運用指標およびテレメトリデータの保持："メトリクスとテレメトリのリファレンス（NetApp Workload Factory）"
- 監査記録の保持：NetApp Console の保持ポリシーによって管理されます（Workload Factory では制御されません）

VPCからどのような情報が流出するのか

このセクションでは、送信データのカテゴリをまとめています。プロトコルレベルおよび機能レベルの詳細については、リンク先のページを参照してください。

Workload Factoryサービスへの管理プレーントラフィック

管理操作においては、FSx構成、ボリュームメタデータ、リソース識別子、および操作コマンドはHTTPS経由でWorkload Factoryサービス層に送信されます。

NetApp Console 監査サービスへの監査レコード

追跡対象となるすべての操作は、以下の情報を送信します。

- `accountId`
- `actionName`
- `status`
- `resourceId`

- `userId`
- `requestData`
- `responseData`
- `timestamps`
- `IP address`
- `workspaceId`

AI分析トラフィック

FSx for ONTAP のAI診断のために送信される緊急管理システム（EMS）イベント、レイテンシデータ、およびエラーログは、設定済みの推論プロファイルを使用してAWSアカウント経由でAmazon Bedrockに転送されるため、このトラフィックはNetAppシステムに到達することなく、お客様の環境内に留まります。

AI分析トラフィックに関する詳細については、以下を参照してください。

- "NetApp Workload FactoryのAI制御の概要"
- "Bedrock の NetApp Workload Factory AI 診断へのオプトイン"
- "NetApp Workload FactoryにおけるAIツールの境界"

AWSサービス**API**トラフィック

"NetApp Workload Factoryの接続性と信頼パス"を参照してください。

テレメトリとメトリクスの収集

"メトリクスとテレメトリのリファレンス"を参照してください。

構成およびメタデータ収集の範囲

ファイルシステムレベル

- ファイルシステム構成（展開タイプ Gen1/Gen2、スループット容量、ストレージ容量、ストレージタイプ）
- 優先サブネット、セキュリティグループ、VPC構成
- KMS暗号化キーメタデータ
- ファイルシステムタグ
- ファイルシステムのライフサイクルステータス
- メンテナンスウィンドウの設定

ボリュームレベル（包括的）

- ID と状態：ボリューム名、UUID、タイプ （rw/dp/ls）、スタイル （FlexVol/FlexGroup）、状態 （オンライン/オフライン/制限付き）、作成時間
- 容量：合計サイズ、使用済み、利用可能、物理的に使用済み、使用率、SSD フットプリント、容量プール

フットプリント、非アクティブ データ バイト/パーセント

- 階層化：ポリシー （すべて/自動/なし/スナップショットのみ）、最低冷却日数
- QoS：割り当てられたQoSポリシー名
- NAS構成：ジャンクションパス、エクスポートポリシーの割り当て、UNIXパーミッション、セキュリティスタイル（unix/ntfs/mixed）
- スナップショット：スナップショットの予約サイズ/割合/使用率、自動削除設定
- データ効率：圧縮タイプ／状態、重複排除、コンパクション、スペース削減
- 自動サイズ調整：モード（grow/grow_shrink/off）、最小／最大サイズ、拡大／縮小しきい値
- SnapLock：タイプ（コンプライアンス/エンタープライズ/non_snaplock）、保持期間（最小/最大/デフォルト）、自動コミット期間
- クローン：親ボリューム / スナップショット / ストレージ VM、FlexCloneであるか、スプリット ステータス
- iノード/ファイル数：最大可能数、最大設定数、使用数
- 暗号化：有効/無効の状態
- アクセス時間：atime更新の有効/無効と更新期間
- SnapMirror：保護ステータス、デスティネーションタイプ（クラウド/ONTAP）
- FlexGroup リバランス：不均衡率、最大しきい値
- ボリューム移動：デスティネーションアグリゲート、移動状態
- FlexCacheエンドポイントタイプ：none/cache/origin
- タグ：ONTAPレベルのボリュームタグ

スナップショットデータ

- スナップショット名、UUID、作成日時、有効期限
- サイズ（バイト）
- SnapMirrorラベル
- SnapLock 有効期限とロック状態
- 状態（有効／無効／部分的）
- ユーザーコメント
- スナップショット ポリシー：名前、有効状態、スケジュール コピー（カウント、保持期間、スケジュール名、プレフィックス、SnapMirror ラベル）

エクスポート ポリシー

- ポリシー名、ID、関連付けられたストレージVM
- ルール：プロトコルリスト （NFS/CIFS/FlexCache）、クライアントのマッチパターン、読み取り専用ルール、読み取り / 書き込みルール、スーパーユーザールール、ルールインデックス/優先度
- SUID、デバイス作成、chownモード、匿名ユーザーマッピング、NTFS UNIXセキュリティ設定

S3アクセスポイント

- ライフサイクル状態（利用可能／作成中／削除中／失敗／設定ミス）
- 作成日時、ARN、エイリアス、名前
- ファイル所有者ユーザーと種類（UNIX/WINDOWS）
- ネットワーク構成（インターネットアクセスとVPCアクセス、VPC ID）
- AWSタグ
- メタデータスキャン有効化、ジャーナリング有効化、CloudTrail ARN

ランサムウェア対策（**ARP**）

Workload Factoryは、構成ステータスとイベントの詳細の両方を収集します。

- ボリュームごとの状態（有効／無効／dry_run／一時停止）
- 攻撃される可能性（なし／低い／中程度／高い）
- タイムスタンプ付き攻撃レポート
- 検出パラメータ：ファイル拡張子のしきい値、名前変更率の急増 %、エントロピー率の急増 %、ファイル作成 / 削除率の急増 %
- 疑わしいファイル：ファイルパス、ファイル名、ファイル形式、疑わしい時刻、関連ボリューム

レプリケーション **/ SnapMirror**

- リレーションシップUUID、状態、正常性ステータス
- ソースと宛先（ストレージVM、パス、クラスタ）
- 転送統計情報（転送バイト数、所要時間、終了時刻、状態）
- ポリシー（名前、タイプ：非同期/同期/継続的）
- スロットル設定
- 遅延時間
- 異常の理由（メッセージとコード）
- 現在の転送エラー

igroup

- 名前、UUID、プロトコル（FCP/iSCSI/混合）、OSタイプ
- イニシエータ（IQN/WWPN）、接続状態、最終確認時刻
- LUNマッピング（論理ユニット番号、LUNの詳細）

LUN

- 名前、UUID、シリアル番号、OSの種類、有効状態
- サイズ、使用容量、シンプロビジョニング設定
- 場所（ボリューム、ノード、論理ユニットパス）

- 自動削除設定
- コンテナの状態、マッピングされた状態、読み取り専用状態
- QoSポリシー
- パフォーマンス指標（IOPS、レイテンシ、読み取り / 書き込み / 合計別スループット）
- 整合性グループのメンバーシップ

FlexCache

- 元のボリューム/ストレージVM/クラスター、キャッシュサイズ、パス
- ライトバック有効、DRキャッシュステータス
- 相対サイズ設定
- ディレクトリパスを事前入力する
- キャッシュとオリジン間の接続状態

ストレージ**VM**レベル

- 名前、UUID、状態（実行中／停止中）、サブタイプ
- 有効/許可されているプロトコル（NFS、CIFS、iSCSI、FCP、NVMe、S3）
- DNSサーバーとドメイン
- 名前サービススイッチの設定（passwd、group、hostsなど）
- IPインターフェース（名前、IPアドレス、サービス）
- 割り当て済みアグリゲート
- ランサムウェア対策のデフォルトボリューム状態
- スペース適用設定
- ピア関係（アプリケーション、状態、リモートクラスタ／ストレージVM）

アグリゲート / ストレージレベル

- 集約名、UUID、状態、RAID状態
- ブロックストレージ：ディスク数、RAIDサイズ、使用可能/使用済み/合計容量、物理使用済み
- クラウドストレージの使用
- 効率：比率、論理使用量、削減量
- 暗号化、ミラー、SnapLock 設定
- パフォーマンス指標（IOPS、レイテンシ、スループット）

利用状況指標（**EDA**）

- データ収集頻度：容量/スループットは12時間ごと、レイテンシは20分ごと
- 粒度：時間範囲ごとに約 60 データポイントに正規化
- 保持および保管に関する詳細："メトリクスとテレメトリのリファレンス"

NetApp Workload Factoryの暗号化と暗号化キー管理

NetApp Workload Factoryは保存データの暗号化を使用し、Workload FactoryとAWSサービス全体にわたる明確なキー管理責任を定義しています。Amazon FSx for NetApp ONTAPファイルシステムの場合、独自のAWS KMSキーを選択するか、AWSが管理するデフォルトのキーを使用できます。また、FSx for ONTAPはそのキーを使用して暗号化操作を実行します。Workload Factoryは、保存されたONTAPクレデンシャルを保護するためにエンベロープ暗号化も使用しています。

FSxにおけるKMSの保存時暗号化範囲

Workload Factory を使用して FSx for ONTAP ファイルシステムを作成する場合、保存データの暗号化用に独自の AWS KMS キーをオプションで指定できます。キーを指定しない場合、Workload Factory は AWS が管理するデフォルトの FSx キーを使用します。

暗号化されるもの

基盤となる EBS ボリュームに保存されているすべてのデータは、FSx for ONTAP ファイルシステムをバックアップします（AWS FSx による保存時の暗号化）。

鍵の所有権

KMSキーはAWSアカウント内に存在します。

キーの選択と使用に必要な権限

Workload Factory には以下が必要です：

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant`（FSx for ONTAP サービスがキーを使用できるようにするため）

キーアクセスパターン

Workload Factoryは、お客様のKMSキーを使用してデータを直接暗号化または復号化することはありません。ファイルシステム作成時に、Amazon FSx for NetApp ONTAP APIにキーIDを渡します。暗号化処理はAmazon FSx for NetApp ONTAPが実行します。

認証情報保護（サービス側エンベロープ暗号化）

Workload Factory を使用して ONTAP クレデンシャル（管理者パスワード）を保存すると、永続化する前にエンベロープ暗号化を使用して保護されます。

暗号化方式

資格情報レコードごとに一意のデータ暗号化キー（DEK）を使用したAES-256-CBC。

エンベロープ暗号化フロー

1. 認証情報ごとに固有の256ビットDEKが生成されます。
2. DEKは認証情報（パスワード）を暗号化します。

3. DEK自体はルートキーで暗号化され、暗号化された認証情報とともに保存されます。
4. 平文のDEKは保存されません。

暗号化コンテキスト

各データキーは、特定の認証情報レコードに暗号学的に紐付けられており、レコード間でキーが再利用されるのを防いでいます。

代替案：**AWS Secrets Manager**

サービスに暗号化されたパスワードを保存する代わりに、ONTAP 認証情報をご自身のアカウントの AWS Secrets Manager に保存できます。Workload Factory はパスワードを一切認識したり保存したりしません。Secrets Manager の ARN を Lambda リンクに渡し、Lambda が実行時にお客様の VPC 内でパスワードを取得します。

AWS Secrets Manager は、GovCloud アカウントに必要です。

NetApp Workload Factoryアカウントの削除

アカウントの削除はセルフサービス操作ではありません。これは、Workload Factory サービスとAWSアカウント内のリソースの両方が関わるオフボーディングワークフローです。クリーンアップには、Workload Factory アカウント、FSx for ONTAP ファイルシステム、認証情報、リンク、通知チャネル、および関連するIAM、AWS Lambda、Amazon CloudWatch リソースに関連するデータの安全な削除が含まれます。この操作は元に戻すことができません。

Workload Factory アカウントを削除する必要がある場合は、"NetAppサポートにお問い合わせください。"

可観測性（ログ、メトリクス、テレメトリ）

NetApp Workload Factoryの可観測性について

可観測性シグナルは、運用監視、トラブルシューティング、および調査をサポートします。NetApp Workload Factoryの可観測性には、サービスの動作、AIの使用状況、およびWorkload Factoryを通じて実行されるアクションを可視化するメトリクス、テレメトリ、および運用記録が含まれます。テレメトリと運用記録は、内部監視と顧客向け監査の可視性をサポートし、トラッカーは、サポート対象の運用の進捗状況、ステータス、および詳細を確認するのに役立ちます。

テレメトリおよび運用記録

Workload Factoryは、以下のテレメトリおよび運用記録タイプを使用します：

- OpenTelemetry トレースは OTLP HTTP 経由で SigNoz にエクスポートされます（内部オブザーバビリティ）
- AIの使用状況計測（トークン数、モデルコスト）はAWS Timestreamに保存されます。
- NetApp Console監査記録（アクション名、ステータス、リクエスト／レスポンスのメタデータ、タイムスタンプ）

Workload Factoryにおける監査ログ

Workload Factoryには、監視機能であるTrackerが搭載されており、どの操作がいつ実行されているかを監視できます。Trackerを使用すると、FSx for ONTAPの進捗状況とステータス、クレデンシャル、およびリンク操作を追跡し、操作タスクとサブタスクの詳細を確認し、問題や障害を診断できます。

Trackerでは、いくつかの操作が可能です。ジョブは、期間（過去24時間、7日間、14日間、または30日間）、ワークロード、ステータス、およびユーザーでフィルタリングしたり、検索機能を使用してジョブを検索したり、ジョブテーブルをCSVファイルとしてダウンロードしたりできます。

- "Workload Factory の Tracker を使用して操作を監視する"

関連情報

- "NetApp Workload Factoryのメトリクスとテレメトリ"

NetApp Workload Factoryのメトリクスとテレメトリ

NetApp Workload Factory は、ボリュームレベルおよびファイルシステムレベルのメトリクスを収集して AWS CloudWatch に保存し、ストレージのパフォーマンスと容量に関する運用上の可視性を提供します。スループットなどの計算メトリクスは、これらの収集された値から導出されます。メトリクスの定義、収集頻度、更新動作、および保持の詳細をご確認ください。

含まれる指標

NetApp Workload Factoryは、運用ログとイベントに以下のメトリクスを使用します：

- ボリュームレベルのCloudWatchメトリクス（ボリュームごとに収集）
- ファイルシステムレベルのCloudWatchメトリクス（ファイルシステムごとに収集）
- 計算済みメトリクス
- 収集スケジュールと保管期間

運用指標について

計算されたメトリクスは、次の式を使用します：

- スループット（バイト/秒）=（NetworkSentBytes + NetworkReceivedBytes） / 期間

更新動作：

- ボリュームとクラスタのメトリクスは12時間ごとに更新されます。
- レイテンシの指標は20分ごとに更新されます。
- DynamoDB のアイテムは14日後に自動的に期限切れになります。

テレメトリデータ収集について

- OpenTelemetry トレースは OTLP HTTP 経由で SigNoz にエクスポートされます（内部オブザーバビリティ）
- AIの使用状況計測（トークン数、モデルコスト）はAWS Timestreamに保存されます。
- NetApp Console監査記録（アクション名、ステータス、リクエスト／レスポンスのメタデータ、タイムスタンプ）

ボリュームレベルの**CloudWatch**メトリクス（ボリュームごとに収集）

指標	**AWS CloudWatch** 名前	単位	測定対象
ボリュームストレージ容量	StorageCapacity	バイト	総プロビジョニング容量
ストレージ使用量	StorageUsed	バイト	実際に保存されたデータ
読み取られたデータバイト数	DataReadBytes	バイト	読み取りスループット
データ書き込みバイト数	DataWriteBytes	バイト	書き込みスループット
データ読み取り操作	DataReadOperations	数	Read IOPS
データ書き込み操作	DataWriteOperations	数	Write IOPS
メタデータ操作	MetadataOperations	数	メタデータIOPS
データ読み取り操作時間	DataReadOperationTime	秒	読み取りレイテンシ
データ書き込み操作時間	DataWriteOperationTime	秒	書き込みレイテンシ

指標	**AWS CloudWatch** 名前	単位	測定対象
メタデータ操作時間	MetadataOperationTime	秒	メタデータ遅延

ファイルシステムレベルの**CloudWatch**メトリクス

指標	**AWS CloudWatch** 名前	単位	測定対象
SSDストレージ容量	StorageCapacity	バイト	SSD階層の合計容量
SSDストレージ使用	StorageUsed（SSDティア）	バイト	SSD階層の消費量
使用された容量プール	StorageUsed（キャパシティプール）	バイト	容量プール消費量
CPU利用率	CPUUtilization	パーセント	ファイルサーバーCPU
SSDの容量利用率	StorageCapacityUtilization	パーセント	SSD階層の使用率
ネットワークスループット利用率	NetworkThroughputUtilization	パーセント	ネットワーク利用率
ディスクIOPS使用率	DiskIopsUtilization	パーセント	ディスクIOPS利用率
ディスクスループット利用率	FileServerDiskThroughputUtilization	パーセント	ディスクスループット利用率
ディスクIOPS使用率（サーバー）	FileServerDiskIopsUtilization	パーセント	サーバーディスクのIOPS利用率
ストレージ効率化による削減効果	StorageEfficiencySavings	バイト	効率化によりスペースを節約
ネットワーク受信	NetworkReceivedBytes	バイト	インバウンドネットワーク
ネットワーク送信	NetworkSentBytes	バイト	アウトバウンドネットワーク

収集スケジュールと保管期間

Time range	収集期間	データポイント	ストレージ	保持
1日	24分	約60	DynamoDB	14日間（TTL）
1週間	約2.8時間	約60	DynamoDB	14日間（TTL）
1ヶ月	12 時間	約60	DynamoDB	14日間（TTL）
3カ月	約1.5日	約60	DynamoDB	14日間（TTL）
1年	約6日間	約60	DynamoDB	14日間（TTL）

生成AIセキュリティ制御

NetApp Workload FactoryにおけるAIコントロールについて説明します

NetApp Workload Factoryには、モデルへのアクセス、データ範囲、および実行時動作に対するセキュリティ制御を適用しながら、診断を加速する生成AI機能が含まれています。

Workload Factoryは、デフォルトでAI診断を有効にしています。Workload Factoryの「管理」設定から、生成AI機能をいつでも無効にできます。"GenAI機能の管理方法について詳しくはこちらをご覧ください。"

セキュリティ関連のAI機能の概要

Workload Factoryは現在、生成AIを以下の機能に適用しています：

- Ask Me アシスタント（厳選された NetApp ドキュメントを用いた RAG、ソースに基づく回答）
- レイテンシ分析
- EMSイベント分析
- エラーログ分析

AI診断のためのAWS Bedrockの概要

Workload Factory は、AI推論にAmazon Bedrockを使用しています。推論処理は、お客様のAWSアカウント内で、お客様が設定した認証情報と推論プロファイルに基づいて実行されます。

関連情報

- "NetApp Workload Factory AI診断向けのAmazon Bedrockのオプトイン"
- "NetApp Workload FactoryにおけるAIツールの境界"
- "AIモデルのパラメータとNetApp Workload Factoryの課金"

NetApp Workload Factory AI診断向けのAmazon Bedrockのオプトイン

NetApp Workload FactoryのAI診断機能は、Amazon Bedrockを使用してイベントを分析し、この機能はデフォルトで有効になっています。Workload Factoryが選択したBedrockモデルを呼び出し、診断データを収集するには、IAM権限、推論プロファイル、およびSSH機能を備えた接続済みLambdaリンクを設定する必要があります。これらのコンポーネントのいずれかが欠落している場合、またはBedrock構成が削除された場合、AI診断は利用できなくなります。

AI診断はデフォルトで有効になっています。

開始する前に

- アカウントにAWS Bedrock推論プロファイルが含まれていることを確認してください。
- 診断データ収集のために、SSH機能を備えた接続済みのLambdaリンクが必要です。

手順

1. IAM ロールに Bedrock 権限を付与する：
    - `bedrock:InvokeModel`
    - `bedrock:InvokeModelWithResponseStream`
    - `bedrock:ListInferenceProfiles`
    - `bedrock:GetInferenceProfile`
2. Workload Factory の設定で、推論プロファイルの ARN を設定します。

前提条件となる要素が一つでも欠けている場合、システムは不足している具体的な要素を報告し、AI機能は非アクティブ状態のままになります。

AI診断を無効にする

AI診断を無効にするには：

- Bedrock の権限を IAM ロールから削除するか、
- Workload Factoryの設定でBedrockの設定を削除します。

AI診断は直ちに利用できなくなり、残留するデータ処理は発生しません。

地域および地域間推論プロファイル

Bedrock の推論は、推論プロファイルで指定された AWS リージョンで実行されます。リージョン間推論プロファイルを使用する場合、AWS は標準的な AWS Bedrock の動作に従って、プロファイルの設定で指定された任意のリージョンにリクエストをルーティングする可能性があります。データは AWS インフラストラクチャの外部に持ち出されません。

NetApp Workload FactoryにおけるAIツールの境界

NetApp Workload Factory は、AI 機能が AWS および ONTAP 環境とどのように連携するかについて厳格な境界を適用しているため、意図しない変更のリスクを負うことなく、AI による診断を信頼することができます。Amazon Bedrock は、変更コマンドをブロックし、サイズと実行によって出力を制限する読み取り専用の AWS CLI および ONTAP CLI 診断ツールを使用しており、使用されるデータはすべて一時的なものであり、NetApp Workload Factory または AWS によって保持されることはありません。

ツールの安全制御

ツール	機能	安全対策
AWS CLI（読み取り専用）	読み取り専用のAWS CLIコマンド（describe、list、get）を実行する	すべての変更動詞（作成、削除、変更、更新、配置、削除）をブロックします。1ステップあたり最大10個のコマンド。出力は20 KBで切り捨てられます。
ONTAP CLI（読み取り専用）	SSHを使用して読み取り専用のONTAP CLIコマンドを実行する	すべての変更動詞（削除、破壊、作成、変更、移動）をブロックします。出力は途中で途切れています。

エージェントは、リソースを変更、作成、または削除することはできません。観察と診断のみ実行できます。

データ保持とモデルトレーニングの境界

AWSのポリシーに基づき、Amazon Bedrockは、基盤モデルのトレーニングや改善のために、お客様の入力データや出力データを保存または使用することはありません。オンデマンド推論（Workload Factoryで使用）の場合、AWSはデータを一時的に処理し、レスポンスを返した後はデータを保持しません。

AIモデルのパラメータとNetApp Workload Factoryの課金

NetApp Workload Factoryは、AIガバナンスに関連するモデル構成、使用範囲、および課金範囲を定義します。設定されたモデルは決定論的なパラメータを使用し、一貫性のある分析結果をサポートするために構造化されたJSONを返します。AWSはAmazon Bedrockの推論処理費用をお客様のアカウントに請求しますが、Workload FactoryはAIの使用状況を追跡し、アカウントごとの月額コストを可視化します。これらのセクションでは、モデルのパラメータと、AIの利用に適用される制限について説明します。

モデルとパラメータ

パラメータ	**Value**
モデル	Anthropic Claude （クロスリージョン推論プロファイルを使用）
温度	0（決定論的、ランダム性なし）
最大出力トークン数	2,048
最大推論ステップ数	分析1件あたり15
出力形式	構造化JSON（概要、重大度、根本原因、是正措置）

請求および使用制限

- AWS は Bedrock の推論処理費用をお客様のアカウント（お客様の推論プロファイル、お客様の認証情報）に請求します。
- Workload Factoryは、AIの使用状況を内部で追跡します。
- Workload Factoryは、アカウントごとの月間コストを可視化します。

  "NetApp Workload Factoryでストレージコストを追跡する"

Ask Me AIアシスタント

NetApp Workload Factory の Ask Me セキュリティアーキテクチャ

Ask Me は、NetApp Workload Factory に組み込まれた生成AI搭載アシスタントです。Amazon FSx for NetApp ONTAP および Workload Factory のトピックに関するリアルタイムの会話サポートを提供します。回答は検証済みのNetAppドキュメントに基づいており、Ask Me は公開インターネットにアクセスしたり、顧客データを使用してモデルをトレーニングしたりすることはできません。複数のセキュリティ層により、悪意のあるクエリをブロックし、応答をサポート対象ドメインに限定し、ユーザー入力がシステム命令を上書きするのを防ぎます。Ask Me がツールを使用する場合、認証境界、読み取り専用クエリの強制、一時的なサンドボックス、および監査ログが、実行の制限と監視に役立ちます。

Workload Factory の 管理 設定からいつでも Ask Me を無効にできます。これにより、ユーザーアカウントのアシスタント機能が無効になります。"GenAI機能の管理方法について詳しくはこちらをご覧ください。"

Ask MeにおけるRAGアーキテクチャ

Ask Meは、検索拡張生成（RAG）を使用しています。

- 厳選されたナレッジベース：回答は、検証済みで公開された NetApp ドキュメントの管理されたコーパスに基づいています。
- 検索スコアリングとフィルタリング：モデルのコンテキストには、十分に関連性の高いコンテンツのみが含まれます。
- インターネットアクセスなし：モデルは外部コンテンツの取得、閲覧、またはスクレイピングができません。
- 出典の明記：回答には、使用した出典資料への参照が含まれます。

多層プロンプトセキュリティ

- レイヤー1：セキュリティ分類器（LLM-as-a-judge）は、悪意のあるクエリ（プロンプトインジェクション、権限昇格、データ漏洩、ソーシャルエンジニアリング、ポリシー違反）をブロックします。

  システムはブロックされたクエリをログに記録しますが、生成モデルはそれらを認識しません。

- レイヤー2：システムプロンプトの強化により、ユーザー入力がシステム命令を上書きすることを防止します。
- レイヤー 3：ドメインスコープにより、FSx ONTAP および Workload Factory のトピックへの応答が制限されます。
- レイヤー4：ツール使用ガバナンスはパラメータを検証し、強化されたサンドボックス内でクエリを実行します。モデルは任意の操作を実行できません。

モデルデータの分離とプライバシー

- 顧客データに基づくモデルトレーニングは行いません。

- リクエストレベルの分離（テナント間のデータ漏洩なし）
- セッションスコープの会話コンテキストと限定された履歴
- 永続的なモデルメモリはありません
- マネージド推論インフラストラクチャ

ツールの使用とエージェントのセキュリティ

- 認可スコープ付きツール（ユーザー権限の境界が適用される）
- 厳格なツール実行タイムアウト
- 取得したデータのための、一時的なセッションスコープのサンドボックス
- 許可リストによる読み取り専用クエリの強制
- 機密パラメータのスクラビングによるツール呼び出しの監査可能性

NetApp Workload Factory のアクセス制御について質問する

NetApp Workload Factory の Ask Me アクセスセキュリティは、認証済みセッション、ユーザーレベルの責任、および実行時操作中の保護された秘密情報の取り扱いに重点を置いています。認証制御は各セッションを検証し、操作を特定のユーザーに関連付けます。機密性の高い認証情報は、実行時に管理対象のシークレット保管庫から取得され、ログから削除されます。このサービスは、非ルートコンテナの実行や制限付き CORS 許可リストなど、インフラストラクチャ制御も適用します。

認証

- 暗号化検証（オーディエンス、発行者、RS256などのアルゴリズムチェックを含む）を備えた署名付きJWT認証
- サービス境界におけるミドルウェアによる認証
- ユーザーIDスコープにより、インタラクションを特定のユーザーに帰属させることができます

認証情報の保護と機密情報の取り扱い

- 安全な保管庫ストレージ：サービスで使用される機密性の高い認証情報は、管理されたシークレット保管庫に保存され、実行時に取得されます。アプリケーションコード、設定ファイル、またはコンテナイメージには、シークレットは一切保存されません。
- ログのスクラビング：機密情報（認証情報、トークン、パスワード、アクセスキー、証明書）は、ログに書き込まれる前に削除されます。

インフラストラクチャセキュリティ

- 非ルートコンテナの実行
- CORSは信頼できるNetAppドメインの明示的な許可リストに制限されています

Ask Me の実行モード（NetApp Workload Factory）

NetApp Workload Factoryは、Ask Meに対して複数の実行モードを提供しており、それぞれ異なるセキュリティおよびプライバシー特性を備えています。Ask Meがツール統合を使用する場合、例えばお客様自身のWorkload Factoryリソースにクエリを実行する場合、ツールの実行は多層的な安全対策によって制御されます。ツールによる実行は、認証されたユーザーの権限の範囲内で行われ、各操作の期間と範囲に制限が適用されます。取得されたデータは、外部からのアクセスを遮断する一時的なセッションサンドボックス内に保持され、セッションが終了すると破棄されます。独立したプロンプトとコード制御により読み取り専用のクエリが強制され、監査記録には機密値が削除されたツールアクティビティが記録されます。

ツール実行時の安全対策

- 認証済みユーザーの権限の範囲内で動作する、認可スコープ付きツールです。
- ツールの実行タイムアウトは、長時間実行される操作を制限します。
- 一時的なデータサンドボックスは、ツールによって取得されたデータをセッションスコープ内に保存し、エンジンレベルでの外部アクセス、ファイル I/O、ネットワーク呼び出し、および拡張機能の読み込みをブロックし、セッションが終了すると破棄されます。
- 読み取り専用クエリの強制適用は、厳格な許可リストを通じて生成されたクエリを検証します。
- プロンプトによるセキュリティとコードによるセキュリティは、それぞれ独立して適用されます。
- ツール呼び出しの監査可能性ログには、ツール名、パラメータ、タイムスタンプ、および結果ステータスが記録され、機密性の高い値はスクラビングされます。

出力制御

- トークン制限の適用
- 分類/セキュリティ上重要な操作のための決定論的出力（温度0）
- 早期終了とクリーンアップ機能を備えたストリーミング配信

NetApp Workload Factoryにおける「Ask Me」のプライバシーと可用性

NetApp Workload Factory の Ask Me プライバシー制御は、データ損失を制限し、セッション処理を分離して、ユーザーとのやり取りにおけるプライバシー境界を維持します。お客様の入力は、基盤モデルのトレーニングや改善には使用されない管理 AI サービスによって処理されます。取得された運用データは、セッション期間中、一時的なインメモリストレージに保持され、永続化または共有されることはありません。複数のクラウドリージョンにまたがるマルチモデルのフォールバックチェーンは、プライマリモデルが制限されたり利用できなくなったりした場合の可用性をサポートし、同じセキュリティ制御がフォールバックモデル全体に適用されます。

データ処理とプライバシー

- プロンプト内のユーザーデータ：管理されたAIサービスによって処理されますが、そのサービスはお客様の入力を基盤モデルのトレーニングや改善には使用しません。

- ナレッジベースコンテンツ：厳選・公開されたNetAppドキュメントのみ。お客様のデータは含まれません。
- 運用データ：ユーザーが自身のリソースを照会した場合にのみ取得され、セッション期間中は一時的なインメモリストレージに保持され、永続化または共有されることはありません。
- 監査ログ：クエリのメタデータ（匿名化されたユーザーID、タイムスタンプ、期間）がログに記録され、機密性の高いフィールドは削除されます。
- フィードバックデータ：匿名化されたユーザーID以外の個人を特定できる情報ではなく、クエリIDに紐づけられて別に保存されます。

可用性および隔離制御

Ask Meは、複数のクラウドリージョンにまたがるマルチモデルフォールバックチェーンを採用しています。

プライマリモデルがスロットリングされているか利用できない場合、システムは代替モデルにフェイルオーバーできます。

すべてのモデルは、同じセキュリティ管理、システムプロンプトの強化策、および隔離保証の対象となります。

ONTAP運用とLambdaリンク（顧客VPCコンポーネント）

NetApp Workload Factory の Lambda リンクについて

NetApp Workload Factory は、VPC にデプロイされた AWS Lambda 関数である *link* を使用して、Amazon FSx for NetApp ONTAP API がこれらの操作を公開していない場合でも、ONTAP ネイティブ操作を AWS アカウント境界内に保持します。このリンクはお客様のサブネットとセキュリティグループ内で実行されるため、実行コンポーネントはお客様の AWS 環境内に留まります。Workload Factory は、利用可能な AWS サービス API ではなく、ONTAP への直接アクセスが必要な操作に対してのみリンクを呼び出します。リンクのアーキテクチャを、NetApp Console エージェントのセキュリティおよび運用プロファイルと比較します。

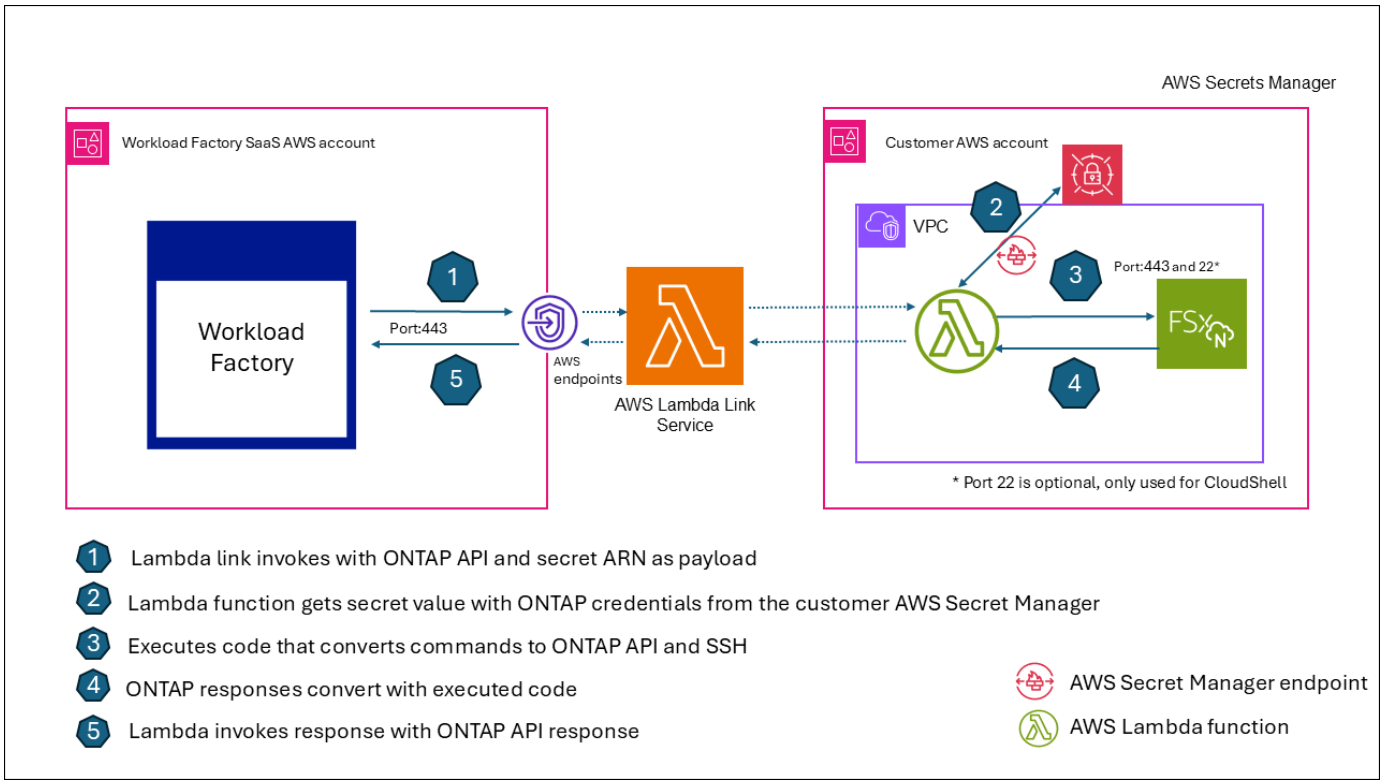
リンクセキュリティアーキテクチャ

Workload Factory リンクは、Workload Factory アカウントと 1 つ以上の FSx for ONTAP ファイルシステムとの間に信頼関係と間接的な接続を作成します。

以下の表は、Lambdaリンクのセキュリティアーキテクチャの概要を示しています。この情報を使用して、AWSアカウントにおけるLambda関数のデプロイおよび実行方法（ネットワーク構成、実行環境、運用上の制限など）を理解してください。

プロパティ	詳細
コンピューティング	AWS Lambda（コンテナイメージ）
ランタイム	Node.js 22
導入	CloudFormation AWS アカウントのスタック
VPCの配置	お客様のサブネット、お客様のセキュリティグループ
Timeout	呼び出しごとに10秒
呼び出し	同期（RequestResponse）
パッケージの種類	コンテナイメージ（NetApp ECR）

以下の図は、Lambdaリンクのセキュリティアーキテクチャを示しています。



Lambda link対NetApp Console agent

LambdaリンクとNetApp Consoleエージェントは、異なる目的を果たし、セキュリティおよび運用上の影響もそれぞれ異なります。

寸法	リンク（**Lambda**ベース）	**NetApp** コンソールエージェント（**VM/Pods** ベース）
ランタイムモデル	サーバーレス（AWS Lambda）、顧客によるデプロイ	顧客がデプロイしたVM/コンテナ。NetAppコンソールサービスポッドを実行します。
主な範囲	コントロールプレーン ONTAP REST 操作（AWS API が当該操作をサポートしていない場合のみ）	データサービスのオーケストレーションとサポート
データサービスサポート	データサービスは提供していません	データサービスをホストできます（NetApp コンソールサービスポッドを実行します）
運営上の諸経費	常時稼働のVMはありません	VMライフサイクル管理とアップグレード

関連情報

システム間の接続性マップ全体については、"NetApp Workload Factory の接続性と信頼パス"を参照してください。

NetApp Workload Factory向けのLambdaリンクのポートと呼び出し

NetApp Workload Factory は、Lambda リンク要求とポート境界を使用して、必要なアウトバウンド接続と IAM 認証済み呼び出しを定義します。このリンクは、ONTAP 管理エンドポイントへの HTTPS リクエスト、診断用の読み取り専用 SSH コマンド、およびヘルスチェックをサポートします。すべての接続は VPC 内のリンクからアウトバウンドで行われるため、インバウンド接続や公開エンドポイントは必要ありません。Workload Factory は、IAM ベースの認証を使用して AWS Lambda API 経由でリンクを呼び出します。

リクエストの種類

- HTTPS（ONTAP REST API）：HTTPS 呼び出しをボリューム、ストレージ VM、およびクラスタ操作のための ONTAP 管理エンドポイント（ポート 443）にプロキシします。
- SSH （ONTAP CLI）：診断およびパフォーマンスデータ取得のため、ポート22で読み取り専用の ONTAP CLI コマンドを実行します。
- ヘルスチェック：ステータスとサポートされている機能を返します。

アウトバウンドネットワーク境界

送受信方向	ポート	デスティネーション	目的
アウトバウンド	443	ONTAP管理用IPアドレス（VPC内）	REST API操作
アウトバウンド	22	ONTAP管理用IPアドレス（VPC内）	SSH CLIコマンド
アウトバウンド	443	AWS Secrets Managerエンドポイント（オプション）	Secrets Manager使用時の認証情報の取得

受信接続は不要です。このリンクはエンドポイントを公開していません。Workload Factory はAWS `lambda:InvokeFunction` APIを使用してそれを呼び出します。

Workload FactoryがLambdaリンクを呼び出します

Workload Factory は、IAM ベースの認証を使用して、AWS Lambda API (`lambda:InvokeFunction`）を介して Lambda リンクを呼び出します。

呼び出しペイロードには以下が含まれます：

- ターゲットONTAP管理エンドポイント（IPアドレス／ホスト名）
- 実行する操作（REST APIパスまたはSSHコマンド）
- 認証情報（インライン認証情報またはSecrets Manager ARN参照）

関連情報

システム間の接続性マップ全体については、"NetApp Workload Factoryの接続性と信頼パス"を参照してください。

Lambda リンクの IAM 権限（NetApp Workload Factory 用）

NetApp Workload Factory は、Lambda リンクのアクセス許可境界を使用して、Lambda の実行および Workload Factory の呼び出しに必要な IAM アクセスを定義します。これらの権限は任意ですが、ONTAP ネイティブ操作には必須です。Secrets Manager サポートを設定すると、リンクは実行時に AWS Secrets Manager から ONTAP 認証情報を直接取得し、パスワードは VPC 内でのみ転送されます。Secrets Manager から Lambda 関数、そして ONTAP エンドポイントへと転送されます。

リクエストパスとポートの要件については、"Lambdaリンクポートと呼び出し"を参照してください。

Lambda実行ロールの権限

VPC内にリンクをデプロイする際、Lambda実行ロールには以下の権限が必要です：

アクセス許可	目的
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	標準のVPC接続型Lambdaネットワーク
ec2:AssignPrivateIpAddresses / ec2:UnassignPrivateIpAddresses	VPC ENI IP管理
secretsmanager:GetSecretValue （FSxSecret* にスコープ設定）	ONTAP 認証情報の取得（Secrets Manager が有効になっている場合のみ）
CloudWatch ログ（管理ポリシー）	Lambda実行ログ

Workload Factory の呼び出し権限

Lambda リンクのリソースベースポリシーは、NetApp Workload Factory のサービスプリンシパルに次の権限を付与します：

アクセス許可	目的
lambda:InvokeFunction	Lambda関数を実行する
lambda:GetFunction	健康状態とステータスの確認
lambda:UpdateFunctionCode	バージョンアップグレード（イメージ更新）
lambda:GetFunctionConfiguration	構成検証

NetApp Workload FactoryのLambdaリンクのライフサイクル

NetApp Workload Factoryは、Lambdaリンクのライフサイクル制御を利用して、運用上

のリスクを最小限に抑えながら、デプロイメント、ヘルスモニタリング、および制御されたイメージ更新を管理します。Amazon CloudFormationスタックを再デプロイすることなく、 `lambda:UpdateFunctionCode`権限を使用して、Lambdaリンクコンテナイメージを更新し、改善点やセキュリティパッチをデプロイできます。ライフサイクル制御では、リンクの状態を監視する方法や、Lambdaリンクとその関連リソースが不要になったときに削除する方法も定義されます。

ライフサイクル管理ポイント

- デプロイ：Amazon CloudFormation または Terraform スタックのデプロイを介して自動化
- 監視：ヘルスチェックで接続の問題を検出し、障害カウンターで信頼性を追跡します。
- 削除：CloudFormation スタックを削除すると、AWS アカウントから Lambda と関連リソースが削除されます。

ナレッジとサポート

NetAppサポートへの登録

NetAppテクニカルサポートでサポートケースを開く前に、NetApp Support SiteアカウントをWorkload Factoryに追加し、サポートへの登録を行う必要があります。

NetApp Workload Factoryおよびそのストレージ ソリューションとサービスに特化したテクニカル サポートを受けるには、サポートへの登録が必要です。サポートへの登録は、Workload Factoryとは別のWebベースのコンソールであるNetApp Consoleから行う必要があります。

サポートに登録しても、クラウド プロバイダの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 プロバイダのファイルサービス、そのインフラストラクチャ、またはそのサービスを使用するソリューションに関するテクニカルサポートについては、該当製品のWorkload Factoryドキュメントの「Getting help」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の登録（NetApp Consoleのサポートリソースページにある20桁の960xxxxxxxxシリアル番号）は、お客様の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は登録が必要です。

登録することで、サポートチケットの発行や自動ケース生成などの機能を利用できるようになります。登録は、以下に説明するように NetApp Support Site （NSS） アカウントを NetApp Console に追加することで完了します。

NetAppサポートにお客様のアカウントを登録します

サポートに登録してサポートの利用権限を有効にするには、アカウント内の1人のユーザーが NetApp Support Site アカウントを NetApp Console のログインに関連付ける必要があります。NetApp サポートへの登録方法は、すでに NetApp Support Site （NSS）アカウントを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顧客

NSS アカウントをお持ちの NetApp のお客様は、NetApp Console からサポートに登録するだけで済みます。

手順

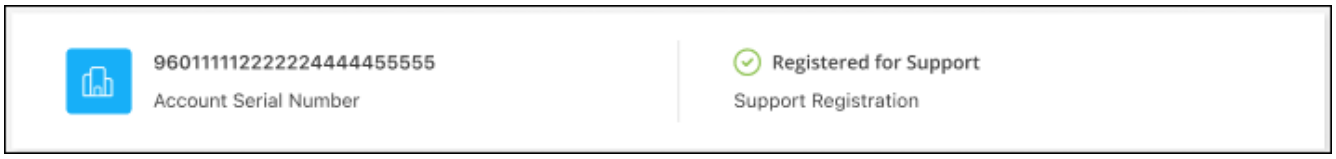
1. Workload Factory コンソールの右上で、*ヘルプ＞サポート*を選択します。

   このオプションを選択すると、新しいブラウザタブで NetApp Console 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、次に「認証情報」を選択します。
3. 「ユーザー認証情報」を選択します。
4. 「NSS認証情報の追加」を選択し、NetApp Support Site（NSS）認証プロンプトに従ってください。
5. 登録手続き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*を選択してくだ

さい。

「リソース」ページには、お客様のアカウントがサポート対象として登録されていることが表示されます。



他のNetApp Console ユーザーが NetApp Support Site アカウントを NetApp Console ログインに関連付けていない場合、同じサポート登録ステータスは表示されません。ただし、これはお客様の NetApp アカウントがサポート対象として登録されていないことを意味するわけではありません。アカウント内の少なくとも1人のユーザーがこれらの手順を完了していれば、アカウントは登録済みです。

既存顧客だが**NSS**アカウントは持っていない

既存のライセンスとシリアル番号をお持ちのNetAppの既存のお客様で、NSSアカウントをお持ちでない場合は、NSSアカウントを作成し、NetApp Consoleのログインに関連付ける必要があります。

手順

1. NetApp Support Site 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. 適切なユーザーレベルを選択してください。通常は **NetApp Customer/End User** です。
   b. シリアル番号フィールドには、上記で使用した NetApp アカウントシリアル番号（960xxxx）を必ずコピーしてください。これにより、アカウント処理が迅速化されます。
2. 新しい NSS アカウントを NetApp Console のログインに関連付けるには、NSSアカウントをお持ちの既存顧客 の手順を完了してください。

NetAppをご利用いただくのが初めての方へ

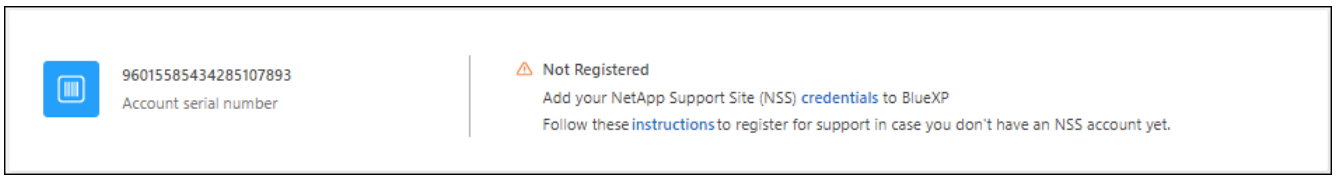
NetAppを初めてご利用になる方で、NSSアカウントをお持ちでない場合は、以下の手順に従ってください。

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 Console が開き、サポートダッシュボードが読み込まれます。

2. サポートリソースページからアカウントIDのシリアル番号をご確認ください。



3. "NetAppのサポート登録サイト"に移動し、*登録済みの NetApp のお客様ではありません*を選択します。
4. 必須項目（赤いアスタリスクが付いている項目）を入力してください。
5. 「Product Line」フィールドで「Cloud Manager」を選択し、該当する請求プロバイダーを選択してくだ

さい。

6. 上記のステップ2のアカウント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から、NetAppのグローバルデータプライバシーポリシーを読んだことを確認してください。

   この安全な取引を完了するために、ご提供いただいたメールアドレスに直ちにメールが送信されます。確認メールが数分以内に届かない場合は、迷惑メールフォルダをご確認ください。

7. メール本文から操作内容を確認してください。

   確認すると、リクエストが NetApp に送信され、NetApp Support Site アカウントを作成することをお勧めします。

8. NetApp Support Site 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. 適切なユーザーレベルを選択してください。通常は **NetApp Customer/End User** です。
   b. 必ず上記のアカウントシリアル番号（960xxxx）をコピーして、シリアル番号欄に入力してください。これにより、アカウント処理が迅速化されます。

終了後の操作

NetApp のサポート担当者がこのプロセス中にご連絡いたします。これは新規ユーザー向けの初回のみのオンボーディング手順です。

NetApp Support Site アカウントを取得したら、NSSアカウントをお持ちの既存顧客の手順を完了して、アカウントを NetApp Console ログインに関連付けてください。

Amazon FSx for NetApp ONTAP に関するヘルプを取得する（NetApp Workload Factory）

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）の記事やコミュニティフォーラムなど、充実した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が含まれています。

FSx for ONTAP のサポートを受ける

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する技術サポートについては、当該製品の Workload Factory ドキュメントにある「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とサービスに関する技術サポートを受けるには、以下のサポートオプションをご利用ください。

セルフサポートオプションを利用する

これらのオプションは、24時間年中無休で無料でご利用いただけます。

- ドキュメント

現在表示中の NetApp Workload Factory のドキュメントです。

- "ナレッジベース"

  NetApp Workload Factoryの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てください。

- "コミュニティ"

  NetApp 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開始したりしましょう。

NetApp サポートでケースを作成する

上記のセルフサポートオプションに加えて、サポートを有効化した後は、NetApp サポートスペシャリストと連携してあらゆる問題を解決することができます。

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。NetApp Support Siteの認証情報をWorkload Factoryのログインに関連付けてください。"サポートへの登録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 Console が開き、サポートダッシュボードが読み込まれます。

2. 「リソース」ページで、「テクニカルサポート」の下にある利用可能なオプションからいずれかを選択してください。

   a. 電話で担当者とお話しになりたい場合は、*お問い合わせください*を選択してください。netapp.com のページに移動し、お電話いただける電話番号が記載されています。

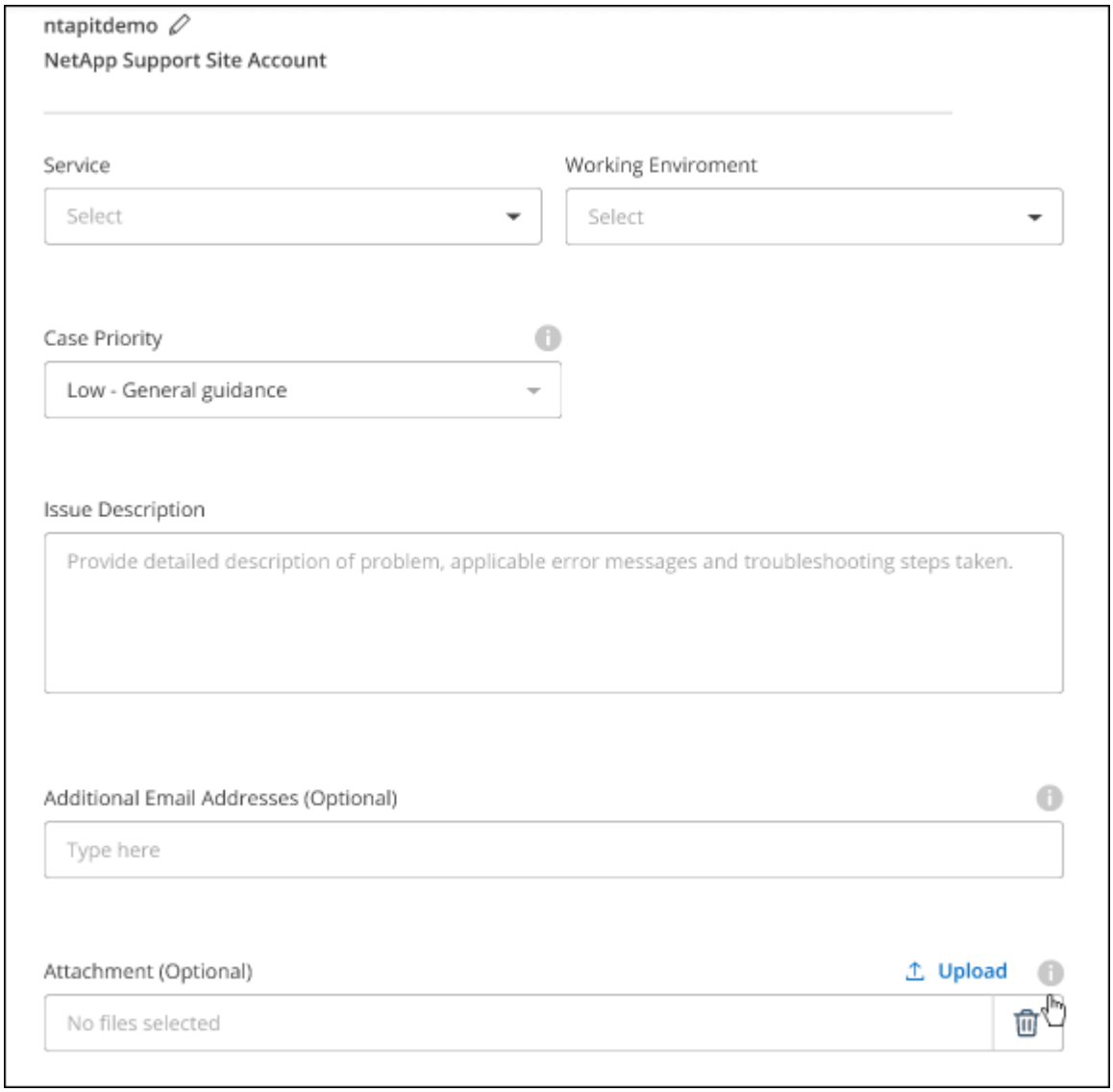
   b. 「ケースを作成」を選択して、NetApp サポートスペシャリストとのチケットを開きます：

      - サービス：**NetApp Workload Factory** を選択します。
      - ケースの優先度：ケースの優先度を低、中、高、または緊急から選択します。

        これらの優先事項に関する詳細については、フィールド名の横にある情報アイコンにマウスカーソルを合わせてください。

      - 事象の説明：問題の詳細な説明を、該当するエラーメッセージや実行したトラブルシューティング手順を含めて提供してください。
      - 追加のメールアドレス：この問題について他の方にも通知したい場合は、追加のメールアドレスを入力してください。
      - 添付ファイル（任意）：最大5つの添付ファイルを一度に1つずつアップロードできます。

        添付ファイルは1ファイルあたり25MBまでです。以下のファイル拡張子がサポートされています：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、およびcsv。



終了後の操作

サポートのケース番号が記載されたポップアップが表示されます。NetAppのサポート スペシャリストがお客様のケースを確認し、間もなくご連絡いたします。

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」という名前のアクションを探してください。一番右にある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した際に、以下のエラーメッセージが表示される場合があります。

「選択され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記録上の会社が、NetApp Console アカウントのシリアル番号（例：960xxxx）またはシステムシリアル番号と同じ記録上の会社でない可能性があることを意味します。以下のいずれかの方法でサポートを受けることができます。

- 製品内チャットを使用する
- 技術的な内容以外のケースを提出するには https://mysupport.netapp.com/site/help

サポート案件を管理する（プレビュー）

アクティブおよび解決済みのサポートケースは、NetApp Console から直接表示および管理できます。NSSアカウントおよび所属企業に関連付けられたケースを管理できます。

ケースマネジメント機能はプレビュー版として利用可能です。今後のリリースでは、このユーザー体験をさらに洗練させ、機能強化を加えていく予定です。製品内のチャット機能を使用して、フィードバックをお送りください。

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、2つの表示方法があります。
  - 左側の画面には、ご提供いただいたユーザー NSS アカウントで過去 3 ヶ月間にオープンされた案件の総数が表示されます。
  - 右側の画面には、ユーザーのNSSアカウントに基づいて、過去3か月間に貴社レベルで開設されたケースの総数が表示されます。

  表に表示されている結果は、選択したビューに関連する事例を反映しています。
- 関心のある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。その他の列は、ソート機能のみを提供します。

  詳細については、以下の手順をご覧ください。
- 案件ごとに、案件メモを更新したり、既に「クローズ済み」または「クローズ保留中」の状態になっていない案件をクローズしたりする機能を提供しています。

手順

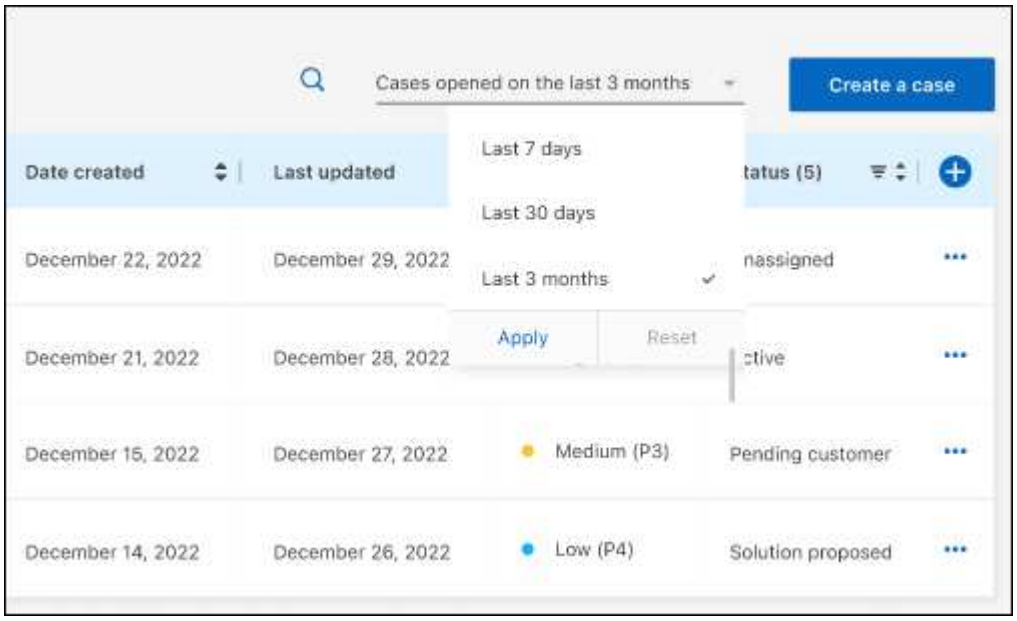
1. Workload Factory コンソールの右上で、*ヘルプ＞サポート*を選択します。

   このオプションを選択すると、NetApp Console が新しいブラウザタブで開き、サポートダッシュボードが読み込まれます。

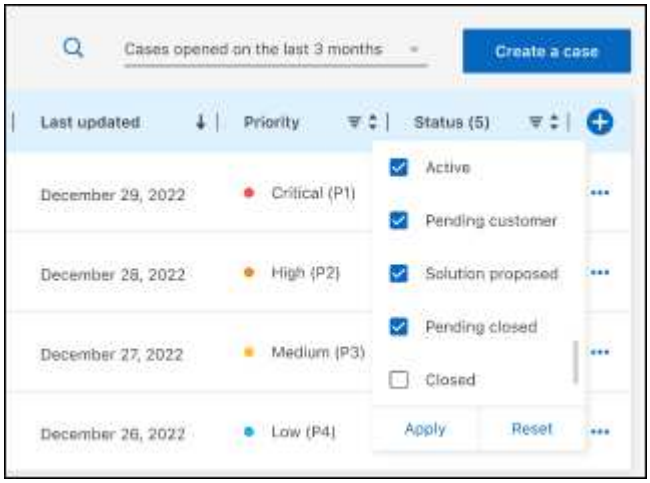
2. 「ケース管理」を選択し、プロンプトが表示されたら、NSSアカウントを NetApp Console に追加します。

   「ケース管理」ページには、お客様の NetApp Console ユーザーアカウントに関連付けられている NSS アカウントに関する未解決のケースが表示されます。これは、「NSS 管理」ページの最上部に表示されている NSS アカウントと同じものです。

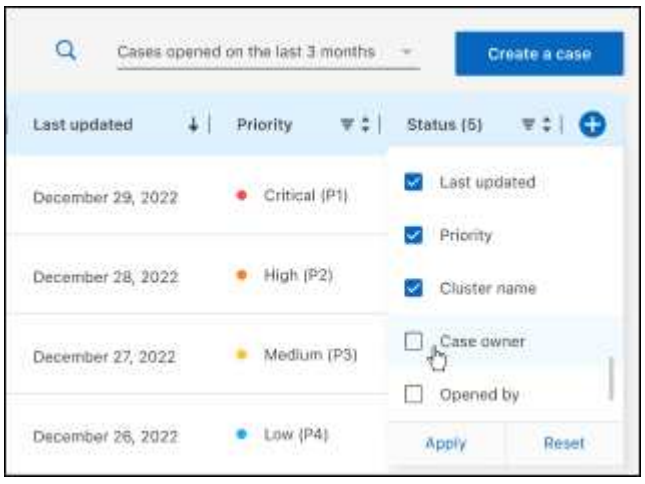
3. テーブルに表示される情報を必要に応じて変更できます。
   - *組織のケース*の下にある*表示*を選択すると、貴社に関連付けられているすべてのケースが表示されます。
   - 日付範囲を変更するには、正確な日付範囲を選択するか、別の期間を選択してください。



◦ 列の内容をフィルタリングします。



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

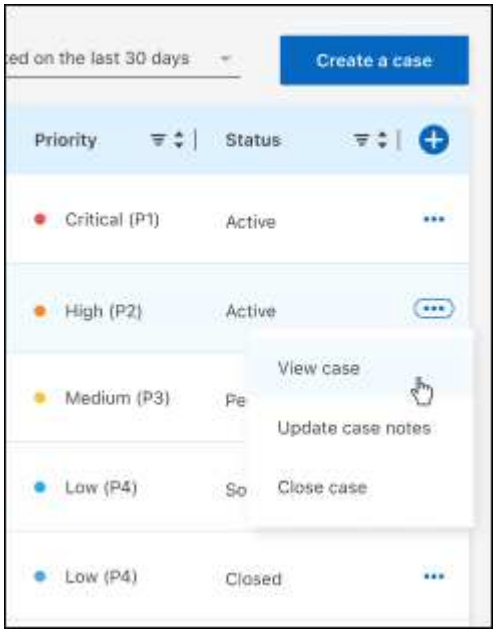


4. •••を選択し、利用可能なオプションのいずれかを選択して、既存のケースを管理します：

- ケースを表示：特定のケースに関する詳細情報を表示します。
- ケースメモの更新：問題に関する詳細情報を入力するか、*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てください。

  添付ファイルは1ファイルあたり25MBまでです。以下のファイル拡張子がサポートされています：txt、log、pdf、jpg/jpeg、rtf、doc/docx、xls/xlsx、およびcsv。

- ケースを閉じる：ケースを閉じる理由の詳細を入力し、*ケースを閉じる*を選択してください。



NetApp Workload Factoryの法的通知

法的通知から、著作権情報、商標、特許などを確認できます。

著作権

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

商標

NetApp、NetAppのロゴ、NetAppの商標一覧のページに掲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。

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

特許

現在NetAppが所有する特許の一覧は以下のページから閲覧できます。

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

通知ファイルは、NetAppソフトウェアで使用されるサードパーティの著作権とライセンスに関する情報を提供します。

"NetApp Workload Factory"

著作権に関する情報

商標に関する情報