アーキテクチャと接続性

Information Security for Workload Factory

NetApp
September 16, 2026

目次

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。

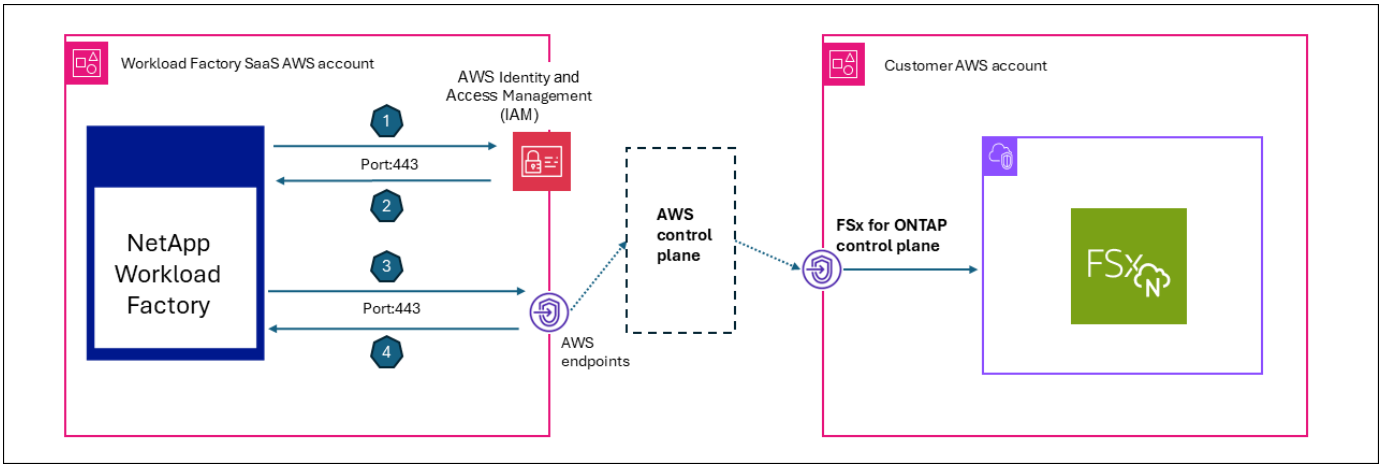
- 収集サービスは、約5時間ごとにスキャンを実行します。
- CRUD操作はオンデマンドで実行されます。
- すべての呼び出しは、外部IDを持つSTS が想定する一時的な認証情報を使用します。

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"

著作権に関する情報

商標に関する情報