アイデンティティ、資格情報、そして最小限の特権

Information Security for Workload Factory

NetApp
September 16, 2026

目次

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