신원 확인, 자격 증명 및 최소 권한

Information Security for Workload Factory

NetApp
September 16, 2026

목차

신원 확인, 자격 증명 및 최소 권한

NetApp Workload Factory용 AWS 계정 통합

Workload Factory는 AWS `sts:AssumeRole`를 사용하여 사용자의 AWS 계정에 대한 임시 자격 증명을 가져오므로, 장기 AWS 액세스 키는 서비스에 저장되지 않습니다. 온보딩 과정에서 Workload Factory가 승인된 AWS API 작업에 사용할 수 있는 IAM 역할을 구성하며, 외부 ID를 사용하여 무단 계정 간 액세스를 방지합니다. Workload Factory는 런타임에 이렇게 생성된 단기 자격 증명을 사용하며, AWS는 각 세션이 종료된 후 해당 자격 증명을 자동으로 만료시킵니다.

AWS 계정 구성

Workload Factory가 AWS 계정에 액세스할 수 있도록 하려면 다음을 수행하십시오.

1. AWS 계정에 IAM 역할을 배포합니다(CloudFormation 사용 또는 수동으로).
2. 역할 신뢰 정책이 Workload Factory의 서비스 주체가 외부 ID를 통해 해당 역할을 수임할 수 있도록 허용하는지 확인하십시오.
3. 고객과 NetApp Workload Factory 간에만 공유되는 고유한 비밀 식별자(UUID v4)로 외부 ID를 사용하십시오.

   이를 IAM 역할 신뢰 정책의 조건으로 포함시키세요(`sts:ExternalId`).

   외부 ID는 혼동을 유발하는 대리인 공격을 방지합니다. 교차 계정 액세스 모델에서 공격자가 고객의 역할 ARN을 발견하더라도 해당 외부 ID가 없으면 해당 역할을 수임할 수 없습니다. AWS는 타사 교차 계정 액세스에 이 패턴을 권장합니다. 자세한 내용은 AWS IAM 설명서 페이지 "타사가 소유한 AWS 계정에 대한 액세스"를 참조하십시오.

   외부 ID는 자격 증명 등록 과정에서 한 번 생성되어 역할 ARN과 함께 암호화된 상태로 Workload Factory 데이터베이스에 저장됩니다.
4. Workload Factory에 역할 ARN과 외부 ID를 등록합니다.

런타임

런타임 시 Workload Factory는 사용자의 IAM 역할을 사용하여 각 AWS API 작업에 필요한 단기 자격 증명을 얻습니다.

1. Workload Factory는 사용자의 역할 ARN과 외부 ID를 사용하여 `sts:AssumeRole`을(를) 호출합니다.
2. AWS는 임시 자격 증명(액세스 키, 비밀 키 및 세션 토큰)을 반환합니다.
3. Workload Factory는 계정의 AWS API 작업에 임시 자격 증명을 사용합니다.
4. 자격 증명은 자동으로 만료됩니다(기본값은 1시간).

AWS 자격 증명이 NetApp Workload Factory를 통해 전달되는 방식

AWS 자격 증명 흐름은 NetApp Workload Factory가 온보딩 및 런타임 작업 중에 역할 식별자, 외부 ID 및 단기 AWS STS 자격 증명을 처리하는 방식을 설명합니다. 일회성 설정 시 AWS

계정에 IAM 역할을 생성하고 Workload Factory 서비스 주체와 올바른 외부 ID를 요구하는 신뢰 정책을 구성합니다. 런타임 시 Workload Factory는 저장된 역할 ARN과 외부 ID를 사용하여 요청별 세션 정책에 따라 범위가 지정된 임시 자격 증명을 요청하고, 캐시된 자격 증명은 만료될 때까지 재사용합니다.

일회성 설정

일회성 설정의 경우 절차는 다음과 같습니다.

단계

1. CloudFormation 스택을 시작하거나 AWS 계정에서 IAM 역할을 수동으로 생성합니다.
2. IAM 역할 신뢰 정책은 두 가지 조건을 명시합니다.
   a. Workload Factory의 서비스 주체만 이를 맡을 수 있습니다.
   b. 발신자는 올바른 외부 ID를 제시해야 합니다.
3. Workload Factory는 역할 ARN과 외부 ID(암호화됨)를 데이터베이스에 저장합니다.

런타임(모든 **API** 작업)

실행 시 Workload Factory는 저장된 역할 ARN과 외부 ID를 사용하여 각 API 작업에 대한 임시 AWS STS 자격 증명을 얻습니다. 흐름은 다음과 같습니다.

단계

1. Workload Factory는 MySQL에서 저장된 역할 ARN과 외부 ID를 검색합니다.
2. 이 작업은 해당 역할에 대한 임시 AWS STS 자격 증명 세트가 Redis에 캐시되어 있는지 확인합니다.
3. 캐시 미스 시 Workload Factory는 역할 ARN과 외부 ID를 사용하여 `sts:AssumeRole`를 호출합니다. 이 호출에는 요청별 인라인 세션 정책이 포함되어 해당 작업에 필요한 특정 AWS 작업에만 권한을 제한합니다.
4. AWS STS는 만료 타임스탬프가 포함된 임시 자격 증명(액세스 키 ID, 비밀 액세스 키, 세션 토큰)을 반환합니다.
5. Workload Factory는 이러한 자격 증명을 Redis에 캐시하고 이를 사용하여 대상 AWS API를 호출합니다.
6. 캐시 적중 시, Workload Factory는 STS 호출을 건너뛰고 캐시된 자격 증명을 직접 사용합니다.

세션 정책

각 STS 호출에는 최소한의 AWS 작업에만 적용되는 인라인 세션 정책이 포함됩니다.

관련 정보

- "최소 권한 계층"

NetApp Workload Factory 의 AWS 자격 증명 보존

Workload Factory는 수명이 짧은 AWS STS 자격 증명, 암호화된 역할 메타데이터 및 제한된 보존 정책을 통해 자격 증명 처리를 안전하게 관리합니다. 자격 증명 모델은 보존되는 역할 메타데이터와 API 작업에 사용되는 임시 AWS 자격 증명을 분리합니다. 임시 자격 증명은 제한된

기간 동안만 캐시되며 AWS 정책에 따라 자동으로 만료됩니다. 자격 증명을 삭제하면 Workload Factory는 해당 계정에 대한 새 자격 증명을 얻을 수 없으며, 캐시된 자격 증명은 그 후 얼마 지나지 않아 만료됩니다.

주요 동작

- Workload Factory는 AWS 액세스 키를 장기간 저장하지 않습니다.

  Workload Factory는 포인터(역할 ARN)와 공유 비밀 키(외부 ID)만 저장합니다. 이 두 가지 모두 자체적으로 AWS 액세스 권한을 부여하지는 않습니다.

- 임시 AWS STS 자격 증명은 최대 1시간 동안만 유효합니다(AWS에서 강제 적용).

  Workload Factory는 해당 데이터를 Redis에 최대 30분 동안 캐시한 후 새로운 STS 호출을 강제합니다.

- 캐시된 자격 증명 세트의 남은 시간이 15분 미만인 경우 Workload Factory는 해당 자격 증명 세트를 폐기하고 새 자격 증명 세트를 가져옵니다.
- 고객이 자격 증명을 삭제하면 Workload Factory가 해당 계정에 액세스할 수 있는 권한이 즉시 취소됩니다.

  다음 AssumeRole 호출이 실패하고 캐시된 자격 증명이 몇 분 내에 만료됩니다.

보존 및 저장 요약

데이터	저장 위치	보존 기간	자동 만료되나요?	삭제 방법
IAM 역할 ARN + 외부 ID	MySQL (저장 시 암호화됨)	무기한 (고객이 명시적으로 삭제할 때까지 저장됨)	아니요	고객이 사용자 인터페이스에서 "자격 증명 삭제"를 클릭합니다.
임시 AWS STS 자격 증명(액세스 키 + 비밀 키 + 세션 토큰)	Redis(인메모리 캐시)	최대 30분(캐시 TTL). 기본 STS 자격 증명은 최대 1시간 동안 유효합니다(AWS 기본값). 캐시는 안전 여유를 위해 만료 5분 전에 데이터를 삭제합니다.	예 (Redis TTL 자동 제거, AWS 자격 증명 만료는 AWS에서 적용)	자동
ONTAP 관리자 비밀번호	MySQL (KMS를 사용한 AES-256-CBC 봉투 암호화)	무기한 (고객이 자격 증명을 제거하거나 파일 시스템을 삭제할 때까지 저장됨)	아니요	고객이 자격 증명을 삭제하거나 파일 시스템 삭제로 인해 정리 작업이 트리거됩니다.
복호화된 ONTAP 암호(평문)	메모리에만 저장됩니다(디스크나 캐시에 기록되지 않음).	단일 요청 소요 시간(밀리초)	예 (요청 완료 후 가비지 컬렉션이 수행됩니다)	자동

보안 제어

- 외부 ID는 혼란스러운 대리인 공격을 방지합니다.
- 세션 정책은 요청별 최소 권한 원칙을 적용합니다.
- Workload Factory는 만료 위험이 높은 기간 전에 수명이 짧은 임시 AWS STS 자격 증명을 갱신합니다.
- Standard, GovCloud 및 China 환경에서는 지역 및 계정 유형별 처리 방식이 다릅니다.
- Workload Factory는 AWS 액세스 키를 장기간 저장하지 않습니다.
- Workload Factory는 IAM 역할의 권한을 절대 수정하지 않습니다.
- Workload Factory는 역할 정책에서 부여한 권한을 넘어서는 권한을 절대 행사하지 않습니다.
- 세션 정책은 권한을 축소할 뿐이며, NetApp Workload Factory는 권한을 확장하지 않습니다.

NetApp Workload Factory용 자격 증명 유형

NetAppWorkload Factory는 AWS 컨트롤 플레인 권한과 직접 ONTAP 관리 액세스를 분리하기 위해 분할 자격 증명 모델을 사용합니다. AWS IAM 역할은 파일 시스템 관리, 백업 관리, 리소스 검색 등의 작업을 위해 Workload Factory를 AWS API에 인증합니다. ONTAP 자격 증명은 관리 구성 또는 진단이 필요한 작업을 위해 Lambda 링크를 통해 ONTAP 관리 엔드포인트에 대한 직접 액세스를 인증합니다. 일부 워크플로는 AWS API 작업과 직접 ONTAP 관리 작업을 결합할 때 두 가지 유형의 자격 증명이 모두 필요합니다.

자격 증명 유형

다음 표는 Workload Factory에서 사용되는 두 가지 자격 증명 유형과 각각의 인증 대상을 요약한 것입니다.

자격 증명 유형	인증 대상	사용 대상
AWS 자격 증명(AssumeRole)	AWS API	AWS FSx 서비스 API를 통해 이루어지는 모든 작업
ONTAP 자격 증명(관리자 비밀번호)	ONTAP 관리 엔드포인트	ONTAP REST API 또는 CLI에 직접 액세스해야 하는 작업

AWS 자격 증명 전용 작업

이러한 작업은 AWS API와만 상호 작용하며 IAM 역할만 필요합니다.

- 파일 시스템 생성 및 삭제
- 파일 시스템 용량 및 처리량 변화
- 백업 생성 및 관리
- VPC, 서브넷 및 보안 그룹 검색
- KMS 키 열거
- CloudWatch 메트릭 검색
- Cost Explorer 쿼리

- FSx API를 사용한 태그 관리

ONTAP 자격 증명 전용 작업

이러한 작업은 Lambda 링크를 통해 ONTAP 관리 엔드포인트와 직접 통신하며 ONTAP 관리자 자격 증명이 필요합니다.

- 볼륨 레벨 QoS 정책 구성
- 엑스포트 정책 및 규칙 관리
- 스토리지 VM 프로토콜 구성(NFS, CIFS, iSCSI)
- igroup 및 LUN 관리
- SnapMirror (복제) 구성
- 스냅샷 정책 관리(ONTAP 수준)
- 성능 진단(QoS 통계, 지연 시간 분석)
- EMS 이벤트 검색 및 분석
- 랜섬웨어 방지 상태 모니터링
- FlexCache 관리
- 네트워크 인터페이스(LIF) 쿼리

AWS 및 ONTAP 자격 증명이 모두 필요한 작업

워크플로우	**AWS** 자격 증명 용도	**ONTAP** 자격 증명 용도
AI 기반 이벤트 분석	Bedrock 호출, 파일 시스템 설명	EMS 이벤트를 검색하고 SSH를 사용하여 진단을 실행합니다.
스토리지 VM 설정을 통한 파일 시스템 생성	파일 시스템 생성 (AWS API)	스토리지 VM 프로토콜 구성(ONTAP REST)
엑스포트 정책을 사용한 볼륨 생성	볼륨 생성(AWS API)	엑스포트 정책 규칙 설정(ONTAP REST)
스토리지 용량 관리	파일 시스템 용량 업데이트(AWS API)	애그리게이트 사용률 확인(ONTAP SSH)

관련 정보

- "ONTAP 실행 옵션"
- "Lambda 링크 개요"

NetApp Workload Factory 용 자격 증명 저장 옵션

NetApp Workload Factory는 최소 권한 원칙을 준수하고 ONTAP 관리 비밀 정보 노출을 최소화하는 자격 증명 처리 패턴을 지원합니다. AI 기반 진단 기능은 가능한 경우 읽기 전용 ONTAP 자격 증명을 사용하므로 진단 에이전트가 스토리지 환경을 수정하지 않고 관찰 및

진단할 수 있습니다. Workload Factory에서 관리하는 암호화된 스토리지를 사용하거나 AWS Secrets Manager에 ONTAP 암호를 저장하고 Workload Factory에 참조를 제공할 수 있습니다. 이 선택은 암호 저장 위치, 암호화 방식, GovCloud 지원 및 자격 증명 순환 등 요구 사항 관리 방식에 영향을 미칩니다.

읽기 전용 **ONTAP** 액세스 모델

이벤트 분석 및 지연 시간 진단과 같은 AI 기반 기능의 경우 Workload Factory는 사용 가능한 경우 읽기 전용 ONTAP 자격 증명을 사용합니다. 읽기 전용 자격 증명 모델을 통해 AI 진단 에이전트는 스토리지 환경을 수정할 수 없으며 관찰 및 진단만 수행할 수 있습니다.

자격 증명 저장 옵션 비교

AWS 자격 증명

AWS 자격 증명은 항상 IAM 역할을 통해 가정됩니다. Workload Factory는 역할 정보를 내부적으로 관리하거나 AWS Secrets Manager에서 참조할 수 있습니다.

옵션	**AWS** 자격 증명	저장된 내용	암호화
Workload Factory 관리	IAM 역할 ARN + 외부 ID	IAM 역할 ARN + 외부 ID	역할 ARN은 비밀이 아닙니다(있는 그대로 저장됩니다).

ONTAP 자격 증명

Workload Factory는 암호화된 스토리지를 사용하여 ONTAP 자격 증명을 내부적으로 관리하거나 AWS Secrets Manager에서 참조할 수 있습니다. 이 선택은 암호의 저장, 암호화 및 순환 방식에 영향을 미칩니다.

Workload Factory가 "Lambda 링크"을 통해 ONTAP 파일 시스템 API와 상호 작용하려면 ONTAP 자격 증명이 필요합니다.

옵션	**ONTAP** 자격 증명	저장된 내용	암호화
Workload Factory 관리	암호(암호화됨)	ONTAP 관리자 비밀번호(암호화됨)	ONTAP 비밀번호는 AES-256 봉투 암호화를 사용합니다
AWS Secrets Manager	Secrets Manager ARN 참조	Secrets Manager ARN	Secrets ARN은 비밀 정보(있는 그대로 저장됨)가 아닙니다. AWS Secrets Manager가 계정에 있는 비밀 정보를 암호화합니다.

추가 고려 사항

GovCloud 요구사항

표준 IAM 역할이 사용됩니다. ONTAP 자격 증명은 Secrets Manager를 사용해야 합니다(암호 저장은 허용되지 않음).

회전

계정의 역할 정책이 업데이트되었습니다. Workload Factory(관리형 옵션)에서 ONTAP 암호를 업데이트하거나 AWS Secrets Manager에서 암호를 교체하십시오.

NetApp Workload Factory의 최소 권한 권한 계층

특정 리소스(ARN)에 대한 액세스 제한, 태그 및 CIDR 범위 등 IAM 조건 적용 등 최소 권한 원칙에 맞춰 Workload Factory IAM 권한을 언제든지 제한할 수 있습니다.

계층형 권한 모델

Workload Factory는 최소 권한 원칙에 기반한 계층형 권한 모델을 사용합니다. AWS 자격 증명을 추가할 때 활성화할 기능 계층을 선택할 수 있습니다. 읽기 전용 검색으로 시작하여 필요에 따라 확장할 수 있습니다.

Workload Factory는 외부 ID를 사용하여 STS를 통해 가정하는 AWS 계정의 IAM 역할을 통해 모든 권한을 부여합니다.

Workload Factory는 인라인 세션 정책을 사용하여 각 API 호출의 범위를 더욱 세분화합니다.

Workload Factory 콘솔의 AI 챗봇 기능인 _Ask Me_는 제한 옵션을 제안하고 AWS에 적용할 업데이트된 정책을 생성하여 권한을 안전하게 세분화할 수 있도록 지원합니다.

권한 부여

Workload Factory에 AWS 자격 증명을 추가할 때 활성화할 권한 계층을 선택할 수 있습니다. 계층은 언제든지 활성화 또는 비활성화할 수 있습니다.

등급은 누적됩니다. 상위 등급을 활성화하면 하위 등급도 자동으로 모두 활성화됩니다.

보안 제어

- 외부 ID(혼동된 대리인 보호)
- 작업별 세션 정책(요청당 최소 권한)
- 태그 기반 조건(보안 그룹 수정은 Workload Factory에서 생성된 리소스로 제한됨)
- 비밀 ARN 범위 지정(Secrets Manager 액세스 제한 대상 `FSxSecret*`)
- 런타임 권한 유효성 검사(대상 해결을 위해 누락된 작업/리소스가 보고됨)

권한 문서

Workload Factory 권한에 대한 주요 참조는 Workload Factory 설정 및 관리 설명서의 "권한 참조"입니다. 스토리지 IAM 정책에서 권한을 제거할 경우 발생하는 영향에 대한 정보는 이 참조에서 확인할 수 있습니다.

NetApp Workload Factory용 Amazon CloudWatch 모니터링 권한

Amazon CloudWatch 모니터링 권한은 NetApp Workload Factory에서 선택 사항이며, 별도의

모니터링 스택을 배포할 때만 적용됩니다. 모니터링 스택은 파일 시스템 메트릭 수집, 이벤트 로그 게시, CloudWatch 대시보드 및 알람 관리, Amazon SNS를 통한 알림 전송 등을 통해 운영 가시성을 제공합니다. 또한 스택은 모니터링에 필요한 경우 ONTAP 자격 증명을 검색하기 위한 액세스 권한이 필요합니다.

필요한 **CloudWatch** 모니터링 권한

선택적 모니터링 스택을 사용하려면 다음과 같은 권한이 필요합니다.

권한	목적
fsx:Describe* / fsx:ListTagsForResource	파일 시스템 메트릭 수집
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	대시보드 및 알람 관리
logs:CreateLogGroup / logs:CreateLogStream / logs:PutLogEvents	이벤트 로그 게시
sns:Publish	경고 알림 전송
secretsmanager:GetSecretValue	모니터링을 위한 ONTAP 자격 증명 검색

저작권 정보

상표 정보