NetApp Workload Factory의 정보 보안

Information Security for Workload Factory

NetApp
September 16, 2026

목차

NetApp Workload Factory의 정보 보안에 대해 알아보세요.

정보 보안은 NetApp Workload Factory 설계 및 운영의 핵심 요소입니다. 정보 보안, 클라우드 플랫폼 및 스토리지 팀은 이러한 세부 정보를 활용하여 기업 보안 요구 사항을 충족하는 방식으로 Workload Factory를 평가하고 도입할 수 있습니다.

Workload Factory란 무엇입니까

Workload Factory는 Amazon FSx for NetApp ONTAP를 사용하여 워크로드(예: 스토리지, VMware 마이그레이션, EDA 프로젝트, 데이터베이스 환경 등)를 최적화하고 관리하는 데 도움이 되도록 설계된 SaaS 수명 주기 관리 플랫폼입니다. 워크로드는 AWS에서 실행됩니다.

Workload Factory는 AWS를 통해 기본적으로 제공되는 모든 FSx for ONTAP 작업에 대해 AWS API를 사용하고, 플랫폼에서 지원되지만 AWS API를 통해 기본적으로 제공되지 않는 Workload Factory 작업에 대해서는 ONTAP REST API를 사용합니다.

이 가이드에서 사용된 핵심 보안 원칙

기밀 유지

신원 관리, 최소 권한 원칙, 암호화 및 네트워크 경계를 통해 무단 접근으로부터 데이터를 보호하십시오.

무결성

권한 범위 설정, 변경 제어 및 감사 기능을 사용하여 시스템과 구성을 무단 또는 의도치 않은 변경으로부터 보호하십시오.

가용성

AWS의 복원력 있는 설계와 운영 모니터링을 통해 승인된 사용자가 서비스 및 워크로드에 액세스할 수 있도록 보장합니다.

이 가이드에서 다루는 정보 유형

다음 섹션에서는 기업 보안 요구 사항을 충족하는 방식으로 Workload Factory를 평가하고 도입하는 데 도움이 되는 정보를 제공합니다.

1. 보안 모델 및 책임
   - "보안 모델 개요"
   - "공동 책임 범위"
2. 아키텍처 및 연결성
   - "연결성 및 신뢰 경로"
   - "ONTAP 실행 옵션"
3. 신원 확인, 자격 증명 및 최소 권한
   - "AWS 계정 연동"

    - "최소 권한 계층"
4. 데이터 거버넌스, 개인정보 보호 및 라이프사이클
    - "데이터 처리 및 상주"
    - "계정 삭제 체크리스트"
5. 관찰 가능성 및 모니터링
    - "측정항목 및 원격 측정"
6. AI 제어 및 VPC 구성 요소
    - "AI 제어 개요"
    - "Lambda 링크 개요"

빠르게 시작하기

- 먼저 보기, 계획 및 분석(읽기 전용) 권한으로 시작하고 필요에 따라 권한을 확장하십시오.
- AWS CloudTrail을 사용하여 `sts:AssumeRole` 통합 역할에 대한 활동을 검증하십시오.
- Lambda 링크 또는 NetApp Console 에이전트 배포가 필요한 ONTAP 네이티브 작업이 필요한지 여부를 사전에 결정하십시오.
- 생성형 AI가 허용되는지 여부와 거주지 제약 조건으로 인해 단일 지역 추론 프로필이 필요한지 여부를 사전에 결정하십시오.

보안 모델 및 책임

NetApp Workload Factory의 보안 모델에 대해 알아보십시오.

NetApp Workload Factory는 AWS 환경의 Amazon FSx for NetApp ONTAP에서 실행되는 워크로드를 관리하고 최적화하는 데 도움이 되는 SaaS 제어 플레인입니다. 보안 결과는 NetApp, AWS 및 조직 간의 공동 책임에 따라 달라집니다.

고수준 보안 모델

- Workload Factory는 IAM assume-role 모델을 사용하여 계정의 AWS API를 호출하기 위한 임시 AWS STS 자격 증명을 얻습니다.
- 일부 워크플로는 AWS API를 통해 노출되지 않는 ONTAP 네이티브 작업을 필요로 합니다. 이러한 작업은 고객이 배포한 실행 구성 요소(예: Lambda 링크)를 사용하여 VPC 내에서 실행할 수 있습니다.
- 관측 가능성 신호(측정 지표, 원격 측정 데이터 및 운영 기록)는 운영 모니터링 및 조사를 지원합니다.

주요 복습 질문

- Workload Factory는 AWS 계정에 대해 어떤 액세스 권한(역할 신뢰 + 권한)을 요구합니까?
- 의도하는 워크플로에 적용되는 실행 경로는 무엇입니까(AWS API 전용 또는 VPC 구성 요소를 통한 ONTAP 네이티브 작업)?
- 어떤 데이터 범주(구성/메타데이터, 운영 로그/이벤트, 텔레메트리)가 처리되며, 이러한 데이터는 어디에 저장됩니까?
- 어떤 모니터링 신호가 존재하며, 그 신호의 보존 특성은 무엇입니까?

다음 단계

- "NetApp Workload Factory의 공동 책임 경계"
- "NetApp Workload Factory의 연결 및 신뢰 경로"
- "NetApp Workload Factory의 최소 권한 권한 계층"

NetApp Workload Factory의 공동 책임 경계

NetApp Workload Factory의 보안 책임은 NetApp(SaaS 운영), AWS(클라우드 인프라 및 관리형 서비스), 그리고 고객(구성)이 공유합니다. 각 주체의 책임 범위를 명확히 이해하면 AWS 환경을 올바르게 구성하고 보안 취약점을 방지할 수 있습니다. 이러한 경계는 NetApp이 운영하는 부분, AWS가 보호하는 부분, 그리고 고객이 직접 구성하고 유지 관리해야 하는 부분을 명확히 합니다.

NetApp 책임 (서비스 측면)

NetApp은 Workload Factory SaaS 플랫폼의 운영 및 보안을 담당합니다. 여기에는 저장된 구성 참조 및 운영 데이터에 대한 서비스 측 처리가 포함됩니다.

AWS 관련 책임 (클라우드 플랫폼)

AWS는 배포 및 워크플로에서 사용하는 클라우드 인프라 및 관리형 서비스(IAM/STS, FSx for ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda 및 네트워킹 기본 요소 등)의 보안을 담당합니다.

고객 책임 사항 (사용자 구성)

귀하는 다음 사항에 대한 책임이 있습니다:

- AWS IAM 역할, 신뢰 정책 및 최소 권한 부여
- VPC 제어(서브넷, 보안 그룹, 라우팅, 엔드포인트 및 송신)
- 자격 증명 거버넌스(워크플로우에 필요한 경우 ONTAP 자격 증명 포함)
- 암호화 및 키 관리 결정 사항(예: FSx for ONTAP의 선택적 고객 관리 KMS 키)
- 모니터링, 경고, 보존 정책 및 사고 대응 프로세스

캡처할 증거

- IAM 역할 신뢰 관계(외부 ID 조건 포함)
- IAM 권한 계층 선택 및 정책 아티팩트
- 네트워크 경계 결정 (AWS API 전용 vs. Lambda 링크 등 VPC 실행 구성 요소)
- 관찰 가능성 결정 및 유지 기대치
- AI 활성화 결정 (AI 진단은 명시적으로 비활성화하지 않는 한 기본적으로 활성화됩니다)

NetApp Workload Factory 온보딩 보안 워크플로

NetApp Workload Factory 온보딩은 제품 사용을 시작하기 전에 AWS 환경에 대한 안전한 액세스를 설정하는 과정입니다. 이 프로세스에는 AWS 신뢰 구성, 권한 범위 설정, 연결 설정, 관찰 가능성 검증 및 선택적 AI 진단 활성화가 포함됩니다.

1단계: 온보딩 방식 결정

- AWS 계정 및 환경 경계(예: 프로덕션과 비프로덕션 분리)를 식별합니다.
- 필요한 워크플로(읽기 전용 검색, 프로비저닝, ONTAP 네이티브 작업)를 식별합니다.
- 워크플로 요구 사항에 따라 VPC 실행 구성 요소(예: Lambda 링크)를 배포할지 여부를 결정합니다.
- AI 진단 활성화 여부를 결정합니다(기본적으로 활성화됨).

관련 정보

- "자격 증명 유형"
- "Lambda 링크 개요"
- "AI 제어 개요"

2단계: AWS 신뢰 및 액세스 설정

1. AWS 계정에 IAM 역할을 배포합니다.
2. 신뢰 정책에서 외부 ID를 사용하여 게이트 역할 가정을 설정합니다.
3. Workload Factory에 역할 ARN과 외부 ID를 등록합니다.

관련 정보

"AWS 계정 연동"

3단계: 최소 권한 권한 적용

1. 원하는 워크플로를 지원하는 최소 권한 등급을 선택하십시오.
2. 요청별 세션 정책이 수행 중인 작업으로만 작업을 제한하는지 확인합니다.

관련 정보

"NetApp Workload Factory의 최소 권한 권한 계층".

4단계: 연결 및 VPC 경계 구성(필요한 경우)

1. AWS 엔드포인트에 필요한 네트워크 경로를 검증합니다.
2. ONTAP 네이티브 작업이 필요한 경우 VPC에 적절한 실행 옵션을 배포하고 유효성을 검사하십시오.

관련 정보

- "NetApp Workload Factory의 연결 및 신뢰 경로"
- "NetApp Workload Factory용 ONTAP 실행 옵션"

5단계: 관찰 가능성 검증

1. 측정 지표와 원격 측정 데이터가 예상대로 수집 및 보존되는지 확인하십시오.
2. 문제 해결 및 조사에 필요한 운영 기록에 접근할 수 있는지 확인하십시오.

관련 정보

- "NetApp Workload Factory의 관찰 가능성 개요"
- "NetApp Workload Factory의 메트릭 및 원격 측정"

6단계: AI 진단 활성화(선택 사항)

AI 진단은 기본적으로 활성화되어 있습니다. 이 기능을 활성화하는 경우 필수 조건을 충족하는지 확인하고 범위 권한을 필요한 최소한으로 설정하십시오.

관련 정보

- "Bedrock에서 NetApp Workload Factory AI 진단 옵트인"
- "NetApp Workload Factory용 AI 툴 경계"

NetApp Workload Factory의 규정 준수 및 보안 태세

NetApp Workload Factory는 규정 준수 및 보안을 핵심 우선순위로 삼아 구축되었습니다. Workload Factory의 모든 워크로드는 Amazon FSx for NetApp ONTAP에서 실행됩니다. 또한 "AWS 보안 기능", NetApp Workload Factory에는 "SOC2 Type 1, SOC2 Type 2 및 HIPAA 규정 준수"가 있습니다.

Amazon FSx for NetApp ONTAP for NetApp Workload Factory는 "기업용 애플리케이션 배포를 위한 AWS 솔루션 "이며, AWS Well-Architected 모범 사례를 따릅니다.

아키텍처 및 연결성

NetApp Workload Factory의 연결 및 신뢰 경로

NetApp Workload Factory는 AWS API, 고객 AWS 계정 리소스, AWS Lambda 링크 및 Amazon Bedrock과 통신하며, 각각 고유한 프로토콜, 포트 및 인증 방식을 사용합니다. 이러한 연결은 AWS 관리 평면, ONTAP 데이터 평면 및 Lambda 링크 트래픽을 분리하는 그룹으로 구성되어 있어 신뢰 경계를 독립적으로 평가할 수 있습니다.

연결 경로

Workload Factory는 AWS 및 ONTAP 리소스를 검색, 프로비저닝 및 관리하는 데 각각 특정한 목적을 가진 여러 개의 연결 경로를 설정합니다. 일부 경로는 가정된 AWS 자격 증명을 사용하여 Workload Factory 자체에서 시작되는 반면, 다른 경로는 VPC 내에서 작동하는 Lambda 링크를 통해 ONTAP 관리 엔드포인트에 공개적으로 노출하지 않고 접근합니다. Amazon Bedrock에 대한 선택적 경로는 AI 기반 진단을 지원하며, 조직에서 해당 기능을 활성화한 경우에만 작동합니다.

다음 섹션에서는 관련된 AWS 또는 ONTAP API, 사용되는 자격 증명 또는 인증, 그리고 경로 활성화 여부를 결정하는 조건을 포함하여 각 경로에 대해 설명합니다. 이러한 경로를 이해하면 Workload Factory에 필요한 네트워크 액세스 및 권한과 데이터가 계정 또는 VPC 경계를 넘는 지점을 평가하는 데 도움이 됩니다.

Workload Factory에서 **AWS API**로

Workload Factory는 서브넷 및 보안 그룹 검색을 위해 `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups`, EC2/VPC API를 사용합니다.

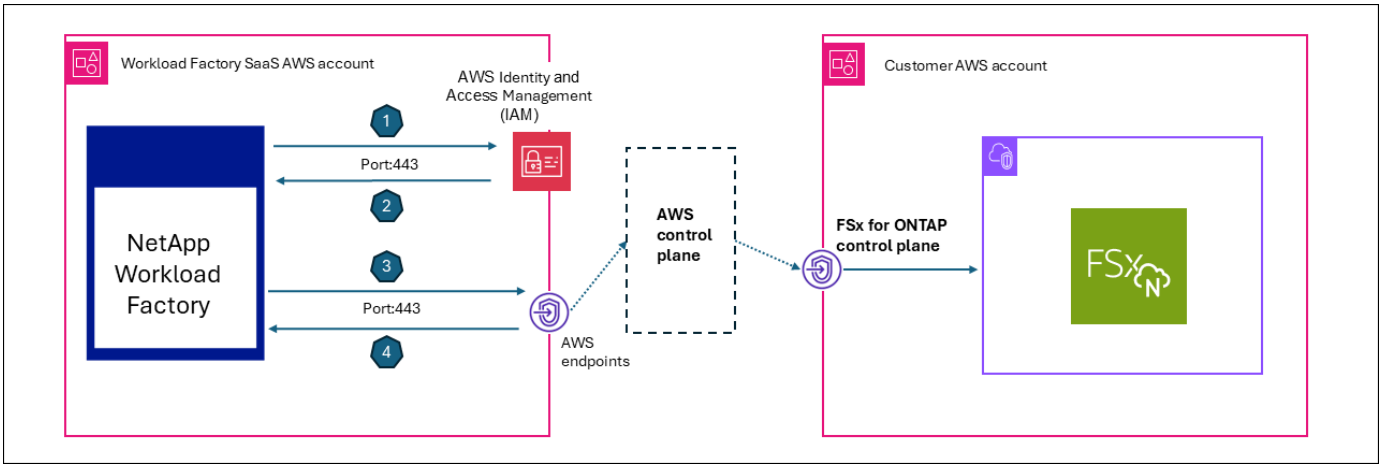
- 수집기 서비스는 약 5시간마다 스캔합니다.
- CRUD 작업은 필요에 따라 실행됩니다.
- 모든 호출은 외부 ID를 사용하는 STS 가정 임시 자격 증명을 사용합니다.

Workload Factory에서 고객 **AWS** 계정 리소스**(**오케스트레이션 및 자동화**)**로

Workload Factory는 AWS와 상호 작용하여 리소스를 통신하고 생성합니다. 오케스트레이션 및 자동화는 여러 가지 방식으로 이루어집니다.

- AWS CloudFormation 템플릿: Workload Factory는 AWS CloudFormation 템플릿을 사용하여 역할 및 파일 시스템과 같은 리소스를 생성합니다. 예를 들어 사용자 인터페이스에서 파일 시스템을 생성하면 Workload Factory가 CloudFormation을 직접 호출하고 사용자를 AWS 계정으로 리디렉션합니다.
- AWS API 호출: Workload Factory는 FSx for ONTAP 관련 활동을 위해 API 명령을 전송하기 위해 AWS API 호출(STS `AssumeRole`)을 사용합니다.
- AWS Lambda: Workload Factory는 CloudFormation을 사용하여 ONTAP와 통신하는 링크에 대한 AWS Lambda 함수를 배포합니다.

다음 다이어그램은 Workload Factory가 NetApp AWS 계정과 FSx for ONTAP 파일 시스템을 사용하는 고객 AWS 계정 간의 신뢰 관계를 활용하는 방식을 보여줍니다.



1. Workload Factory는 AWS IAM 서비스에서 제공하는 고객별 외부 ID를 사용하여 AWS STS `AssumeRole`에 요청을 보냅니다.
2. AWS IAM 서비스가 역할을 검색하고 세션을 생성합니다.
3. Workload Factory는 세션 권한을 사용하여 AWS API 요청을 보냅니다.
4. Workload Factory는 FSx for ONTAP 제어 플레인으로부터 AWS API 응답을 수신합니다.

ONTAP 관리 엔드포인트에 대한 **Lambda** 링크

Lambda 링크는 고객 VPC 내에서 실행되어 ONTAP을 공개적으로 노출하지 않고 프라이빗 서브넷에 액세스할 수 있도록 합니다. 링크에서 ONTAP 관리 엔드포인트로의 모든 연결은 아웃바운드 전용이므로 인바운드 연결이나 외부 엔드포인트는 필요하지 않습니다. 이 링크는 Amazon FSx for NetApp ONTAP API에서 노출하지 않는 ONTAP 네이티브 작업에만 사용됩니다.

Workload Factory는 볼륨, 스토리지 VM 및 클러스터 작업과 읽기 전용 진단 및 성능 데이터에 대해 다음과 같은 프로토콜을 사용합니다.

- HTTPS/443 (REST)
- SSH/22(CLI)

AWS Secrets Manager(ONTAP 자격 증명 검색**)**에 대한 **Lambda** 링크

ONTAP 관리자 자격 증명이 AWS Secrets Manager에 저장된 경우에만 사용됩니다(대안: Workload Factory에서 봉투 암호화를 사용하여 암호화된 자격 증명).

- 프록시 포워더는 헤더에 `x-aws-secret-arn` (Base64로 인코딩된) 값을 전달합니다.
- Lambda 링크는 실행 시점에 비밀번호를 검색하기 위해 `GetSecretValue`을(를) 호출합니다.

이렇게 하면 비밀번호가 계정 범위 내에 유지되고 Workload Factory에서 전송되는 것을 방지할 수 있습니다.

Workload Factory 및 고객 구성 요소와 **Amazon Bedrock(AI** 진단**)**

이 경로는 AI 진단이 활성화된 경우에만 사용됩니다.

- 이벤트 분석기는 EMS 분석 및 지연 시간 진단에 이 경로를 사용합니다.
- Bedrock은 사용자의 가상 자격 증명과 추론 프로필 ARN을 사용하여 실행되므로 데이터가 NetApp의 계정으로

전송되지 않습니다.

Bedrock으로 전송되는 데이터에는 EMS 이벤트 JSON, QoS 통계, 볼륨 구성, 집계 데이터 및 노드 정보가 포함될 수 있습니다. 이 경로는 조직 (`ai_analyzer_config` 테이블별로 추론 프로필이 구성된 경우에만 활성화됩니다.

연결 그룹(프로토콜, 포트 및 인증)

그룹 **A — AWS** 관리 평면 신뢰 경로(가정된 자격 증명)

연결	프로토콜	포트	방향	인증	정당화
STS AssumeRole	HTTPS	443	WF → AWS STS (고객 계정)	IAM 자격 증명 + ExternalId	임시 교차 계정 자격 증명 얻기
FSx API(Describe/Create/Update/Delete)	HTTPS	443	WF → AWS FSx 엔드포인트(고객 지역)	STS 임시 자격증명서	파일 시스템 및 볼륨 수명 주기 관리
EC2/VPC API	HTTPS	443	WF → AWS EC2 엔드포인트	STS 임시 자격증명서	보안 그룹, 서브넷 및 VPC 검색
CloudFormation API	HTTPS	443	WF → AWS CFN 엔드포인트	STS 임시 자격증명서	IAM 역할 및 FSx 프로비저닝을 위한 스택 배포
Secrets Manager GetSecretValue	HTTPS	443	WF → AWS Secrets Manager 엔드포인트(고객 계정)	STS 임시 자격증명서	ONTAP 관리자 암호 검색 (Secrets Manager에 저장된 경우)
KMS 암호화/복호화	HTTPS	443	WF → AWS KMS 엔드포인트	STS 임시 자격증명서	볼륨 암호화 키 작업

모든 AWS API 호출은 고객의 지역 엔드포인트를 사용하며, 구성된 경우 VPC 엔드포인트를 통해 라우팅될 수 있습니다.

그룹 **B — ONTAP** 데이터 플레인

ONTAP 데이터 플레인은 항상 Lambda 링크를 통해 프록시됩니다. Workload Factory 서비스는 ONTAP에 직접 연결되지 않습니다.

연결	프로토콜	포트	방향	인증	정당화
ONTAP REST API	HTTPS	443	링크(고객 VPC) → ONTAP 관리 LIF	기본 인증(사용자 이름/비밀번호) 또는 Secrets Manager ARN	클러스터, 볼륨 및 스토리지 VM 구성; QoS; EMS 이벤트; ARP 상태
ONTAP SSH CLI	SSH	22	링크(고객 VPC) → ONTAP 관리 LIF	비밀번호 인증	진단 명령(QoS 통계, df, 이벤트 로그, 효율성)

프록시 포워더의 라우팅 전략(우선순위):

1. 명시적 `x-link-id` 헤더: 데이터베이스에서 Lambda ARN을 조회합니다.
2. 대상 ID(FSx 파일 시스템 ID): 관련 링크 찾기

3. 콘솔 에이전트 ID: 메시지 브로커를 통해 콘솔 에이전트로 라우팅

그룹 **C — AWS Lambda** 링크**(VPC**에 배포됨**)**

연결	프로토콜	포트	방향	인증	정당화
Lambda 호출	HTTPS(AWS SDK)	443	WF → AWS Lambda API (고객 계정)	IAM (`lambda:InvokeFunction`)	고객 VPC 내에서 ONTAP REST/SSH 명령을 실행합니다.
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda(고객 VPC) → ONTAP 관리 LIF	기본 인증/비밀번호	공개적으로 노출되지 않고 ONTAP에 대한 프라이빗 서브넷 액세스

그룹 **D — NetApp Console Agent(VPC** 내 **EC2,** 아웃바운드 전용**)**

연결	프로토콜	포트	방향	인증	정당화
에이전트 폴링	HTTPS	443	콘솔 에이전트(고객 VPC) → WF 메시지 브로커	베어러 토큰(occm-access 범위)	대기 중인 ONTAP 명령을 확인하기 위한 장시간 폴링(7초 타임아웃, 재연결)
상담원 응답	HTTPS	443	콘솔 에이전트(고객 VPC) → WF 메시지 브로커	Bearer 토큰	ONTAP 명령 결과를 반환합니다(선택적으로 zlib으로 압축).
콘솔 에이전트 → ONTAP	HTTPS + SSH	443, 22	콘솔 에이전트(고객 VPC) → ONTAP 관리 LIF	기본 인증/비밀번호	프록시를 통해 ONTAP 작업을 실행합니다.

핵심 설계: Workload Factory는 Console 에이전트로의 인바운드 연결을 절대 시작하지 않습니다. 작업은 Redis 스트림에 대기열로 저장되며, Console 에이전트는 `GET /messagebroker/v1/requests` 폴링하고 `POST /messagebroker/v1/responses`로 응답합니다.

그룹 **E — CloudFormation** 사용자 지정 리소스 콜백

연결	프로토콜	포트	방향	인증	정당화
CloudFormation → WF Lambda	HTTPS	443	CloudFormation(고객) → WF Lambda(NetApp)	JWT 토큰 + 참조 토큰	IAM 역할 생성 상태를 보고하고 역할 ARN을 반환합니다.
ONTAP CloudFormation 리소스 공급자 → 링크	HTTPS	443	CloudFormation 리소스 Lambda(고객) → Lambda(고객) 연결	IAM	스택 작업 중 ONTAP 리소스 생성/업데이트/삭제

요약**: VPC**에 필요한 네트워크 요구 사항

구성 요소	인바운드	아웃바운드
FSx for ONTAP	Link Lambda 또는 콘솔 에이전트 보안 그룹의 포트 443 및 22	해당 없음
링크 람다	None	포트 443(ONTAP, AWS APIs) 및 포트 22(ONTAP SSH)
콘솔 에이전트 EC2	None	포트 443(WF 엔드포인트, ONTAP, AWS API) 및 포트 22(ONTAP SSH)
VPC 엔드포인트(선택 사항)	해당 없음	STS, FSx, S3, Secrets Manager, Lambda, CloudFormation

고객 VPC 내의 어떤 구성 요소에도 인바운드 인터넷 액세스가 필요하지 않습니다. 모든 연결은 아웃바운드 방식으로 시작되거나(콘솔 에이전트 폴링) AWS 서비스 API를 통해 호출됩니다(Lambda Invoke).

NetApp Workload Factory용 ONTAP 실행 옵션

일부 NetApp Workload Factory 워크플로는 AWS API를 통해 노출되지 않는 ONTAP 네이티브 작업을 필요로 합니다. Workload Factory는 이러한 작업을 AWS 계정 경계 내에서 수행할 수 있도록 두 가지 실행 옵션을 제공합니다. 하나는 VPC 내에서 ONTAP 작업을 실행하는 Lambda 링크이고, 다른 하나는 EC2 인스턴스에서 아웃바운드 연결만 사용하는 NetApp Console Agent입니다. 두 옵션 모두 네트워크, 자격 증명 및 수명 주기 관련 결정을 보안 모델 내에서 유지하면서 필요한 ONTAP 작업을 수행할 수 있도록 지원합니다.

실행 옵션

Lambda 링크 **(VPC** 내 **AWS Lambda)**

ONTAP를 공개적으로 노출하지 않고 VPC 내에서 ONTAP REST 및 읽기 전용 ONTAP CLI 진단을 실행합니다.

NetApp 콘솔 에이전트**(VPC** 내 **EC2** 인스턴스**,** 아웃바운드 전용**)**

에이전트가 아웃바운드 연결을 시작하고 Workload Factory가 에이전트로 인바운드 연결을 시작하지 않는 프록시된 ONTAP 작업을 실행합니다.

보안 고려 사항

- 네트워크 경계: 필요한 아웃바운드 포트(443/22) 및 목적지를 확인하십시오.
- 자격 증명 경계: ONTAP 자격 증명을 Workload Factory에 저장(봉투 암호화)할지 또는 AWS Secrets Manager에서 참조할지 결정합니다.
- 감사 가능성: 구성 요소 활동 및 오류에 대한 운영 기록을 확인합니다.
- 수명주기 관리: 업데이트 및 삭제가 어떻게 이루어지는지 확인합니다.

관련 정보

- "NetApp Workload Factory의 Lambda 링크 개요"

- "NetApp Workload Factory의 연결 및 신뢰 경로"
- "NetApp Workload Factory용 암호화 및 키 관리"

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

데이터 거버넌스, 개인정보 보호 및 라이프사이클

NetApp Workload Factory의 데이터 처리 및 상주

NetApp Workload Factory는 서비스에서 처리하는 운영 데이터, 각 데이터 클래스가 보안 모델에 어떻게 적용되는지, 데이터 저장 위치, 보존 기간, 그리고 데이터가 고객 환경 외부로 유출되는지 여부를 설명하는 범주별로 데이터 처리를 구성합니다. 주요 데이터 클래스에는 구성 및 메타데이터, 운영 로그 및 이벤트, 원격 측정 데이터가 포함됩니다. 보존되는 데이터에는 FSx for ONTAP 구성 스냅샷, 자격 증명 참조, AI 사용량 및 비용 데이터, 감사 기록, 단기 응답 캐시 등이 포함될 수 있습니다. 저장 및 처리 위치는 데이터 유형에 따라 다릅니다. 일부 정보는 고객의 AWS 계정에 유지되는 반면, 다른 운영 데이터는 NetApp 계정에 저장됩니다.

Workload Factory에서 처리하는 데이터 클래스

Workload Factory는 다음과 같은 데이터 클래스를 처리합니다.

- 구성 및 메타데이터
- 운영 로그 및 이벤트
- 원격 측정

Workload Factory에서 유지되는 데이터 클래스

Workload Factory는 다음 데이터를 저장합니다.

- FSx 구성 스냅샷(스캔할 때마다 새로 고쳐짐)
- ONTAP 자격 증명 참조 또는 KMS 봉투 암호화로 암호화된 자격 증명 자료(선택한 자격 증명 모드에 따라 다름)
- EDA 지표
- CloudFormation 템플릿(7일 `Expires` 헤더)
- AI 사용 및 비용 데이터
- 감사 기록
- TTL이 20분인 Redis 캐시(FSx 응답)

정보가 보관되는 위치

AWS 계정

- ONTAP 관리자 암호는 AWS Secrets Manager에 저장됩니다.
- Amazon Bedrock은 AWS 계정 내의 STS에서 위임한 역할을 통해 사용자의 추론 프로필 ARN을 사용하여 AI 추론(EMS 분석)을 처리합니다.

NetApp 계정

- FSx 구성, 균형 조정 계획, ARP 구성 및 AI 사용 제한

- 임시 AWS STS 자격 증명(Redis에 캐시됨), 응답 캐시, 잠금 및 배포 상태
- CloudFormation/Terraform 템플릿, WAD 구성 설명자 및 압축 보고서
- AI 사용량 측정 및 수집기 성능 지표
- EDA 집계 지표
- 작업 감사 추적
- OpenTelemetry 추적

지역적 고려사항

- Amazon Bedrock 서비스를 이용할 수 있는 지역에 저장됩니다.
- NetApp 내부는 `us-east-1` 및 `us-west-2`에서 운영됩니다.

정보 보관 기간

이 섹션에서는 보존 범주를 요약합니다. 자세한 값 및 정책 동작은 링크된 페이지를 참조하십시오.

- 자격 증명 및 임시 AWS STS 자격 증명 보존: "NetApp Workload Factory의 자격 증명 보존"
- 운영 지표 및 원격 측정 데이터 보존: "NetApp Workload Factory의 메트릭 및 원격 측정 참조"
- 감사 기록 보존: NetApp Console 보존 정책에 따라 관리됩니다(Workload Factory에서 제어하지 않음).

VPC에서 어떤 정보가 유출됩니까?

이 섹션에서는 송신 데이터 범주를 요약합니다. 프로토콜 수준 및 기능 수준의 자세한 내용은 링크된 페이지를 참조하십시오.

Workload Factory 서비스로 향하는 관리 플레인 트래픽

관리 작업의 경우 FSx 구성, 볼륨 메타데이터, 리소스 식별자 및 운영 명령은 HTTPS를 통해 Workload Factory 서비스 계층으로 전송됩니다.

NetApp Console 감사 서비스에 대한 감사 기록

추적되는 모든 작업은 다음 정보를 전송합니다.

- `accountId`
- `actionName`
- `status`
- `resourceId`
- `userId`
- `requestData`
- `responseData`
- `timestamps`

- `IP address`
- `workspaceId`

AI 분석 트래픽

FSx for ONTAP 긴급 관리 시스템(EMS) 이벤트, 지연 데이터 및 AI 진단을 위해 제출된 오류 로그는 구성된 추론 프로필을 사용하여 AWS 계정을 통해 Amazon Bedrock으로 전송되므로 이러한 트래픽은 NetApp 시스템에 도달하지 않고 사용자 환경 내에 유지됩니다.

AI 분석 트래픽에 대한 자세한 내용은 다음을 참조하십시오.

- "NetApp Workload Factory의 AI 제어 개요"
- "Bedrock에서 NetApp Workload Factory AI 진단 옵트인"
- "NetApp Workload Factory용 AI 툴 경계"

AWS 서비스 **API** 트래픽

자세한 내용은 "NetApp Workload Factory의 연결 및 신뢰 경로"을 참조하십시오.

원격 측정 및 지표 수집

"측정 지표 및 원격 측정 참조"을(를) 참조하십시오.

구성 및 메타데이터 수집 범위

파일 시스템 수준

- 파일 시스템 구성(배포 유형 Gen1/Gen2, 처리량 용량, 스토리지 용량, 저장 유형)
- 선호하는 서브넷, 보안 그룹, VPC 구성
- KMS 암호화 키 메타데이터
- 파일 시스템 태그
- 파일 시스템 수명 주기 상태
- 유지 관리 창 설정

볼륨 수준(종합)

- 식별 및 상태: 볼륨 이름, UUID, 유형(rw/dp/ls), 스타일(FlexVol/FlexGroup), 상태(온라인/오프라인/제한됨), 생성 시간
- 용량: 총 크기, 사용량, 사용 가능 용량, 물리적 사용량, 사용률, SSD 사용량, 용량 풀 사용량, 비활성 데이터 바이트/사용률
- 계층화: 정책(all/auto/none/snapshot_only), 최소 냉각 기간
- QoS: 할당된 QoS 정책 이름
- NAS 구성: 접합 경로, 내보내기 정책 할당, UNIX 권한, 보안 스타일(unix/ntfs/mixed)
- 스냅샷: 스냅샷 예약 크기/비율/사용량, 자동 삭제 설정

- 데이터 효율성: 압축 유형/상태, 중복 제거, 압축률 향상, 공간 절약
- 자동 크기 조정: 모드(grow/grow_shrink/off), 최소/최대 크기, 확대/축소 임계값
- SnapLock: 유형(규정 준수/엔터프라이즈/비 SnapLock), 보존 기간(최소/최대/기본값), 자동 커밋 기간
- 클론: 상위 볼륨/스냅샷/스토리지 VM, FlexClone, 분할 상태
- 이노드/파일: 최대 가능 개수, 최대 설정 개수, 사용 개수
- 암호화: 활성화/비활성화 상태
- 액세스 시간: atime 업데이트 활성화/비활성화 및 업데이트 주기
- SnapMirror: 보호 상태, 대상 유형(클라우드/ONTAP)
- FlexGroup 리밸런싱: 불균형 비율, 최대 임계값
- 볼륨 이동: 대상 애그리게이트, 이동 상태
- FlexCache 엔드포인트 유형: 없음/캐시/원본
- 태그: ONTAP 레벨 볼륨 태그

스냅샷 데이터

- 스냅샷 이름, UUID, 생성 시간, 만료 시간
- 크기(바이트)
- SnapMirror 레이블
- SnapLock 만료 및 잠금 상태
- 상태 (유효/무효/부분적)
- 사용자 댓글
- 스냅샷 정책: 이름, 활성화 상태, 예약된 복사본(개수, 보존 기간, 예약 이름, 접두사, SnapMirror 레이블)

엑스포트 정책

- 정책 이름, ID, 연결된 스토리지 VM
- 규칙: 프로토콜 목록(NFS/CIFS/FlexCache), 클라이언트 일치 패턴, 읽기 전용 규칙, 읽기/쓰기 규칙, 관리자 권한 규칙, 규칙 인덱스/우선순위
- SUID, 장치 생성, chown 모드, 익명 사용자 매핑, NTFS UNIX 보안 설정

S3 액세스 포인트

- 수명 주기 상태(사용 가능/생성 중/삭제 중/실패/잘못 구성됨)
- 생성 시간, ARN, 별칭, 이름
- 파일 소유자 사용자 및 유형(UNIX/WINDOWS)
- 네트워크 구성(인터넷 vs VPC 액세스, VPC ID)
- AWS 태그
- 메타데이터 스캔 활성화, 저널링 활성화, CloudTrail ARN

랜섬웨어 방지**(ARP)**

Workload Factory는 구성 상태와 이벤트 세부 정보를 모두 수집합니다.

- 볼륨별 상태(활성화/비활성화/dry_run/일시 중지)
- 공격 확률 (없음/낮음/중간/높음)
- 타임스탬프가 포함된 공격 보고서
- 탐지 매개변수: 파일 확장자 임계값, 이름 변경률 급증 %, 엔트로피 증가율 급증 %, 파일 생성/삭제율 급증 %
- 의심스러운 파일: 파일 경로, 파일 이름, 파일 형식, 의심 시간, 관련 볼륨

복제 **/ SnapMirror**

- 관계 UUID, 상태, 정상 상태
- 소스 및 대상(스토리지 VM, 경로, 클러스터)
- 전송 통계(전송된 바이트 수, 전송 시간, 종료 시간, 상태)
- 정책(이름, 유형: 비동기/동기/지속적)
- 스로틀 설정
- 지연 시간
- 비정상 이유(메시지 및 코드)
- 현재 전송 오류

iGroups

- 이름, UUID, 프로토콜(FCP/iSCSI/혼합), 운영 체제 유형
- 시작자(IQN/WWPN), 연결 상태, 마지막 접속 시간
- LUN 매핑(논리 장치 번호, LUN 세부 정보)

LUN

- 이름, UUID, 일련 번호, 운영 체제 유형, 활성화 상태
- 크기, 사용 공간, 씬 프로비저닝 설정
- 위치(볼륨, 노드, 논리 장치 경로)
- 자동 삭제 설정
- 컨테이너 상태, 매핑 상태, 읽기 전용 상태
- QoS 정책
- 성능 지표(IOPS, 지연 시간, 읽기/쓰기/총 처리량)
- 일관성 그룹 멤버십

FlexCache

- 원본 볼륨/스토리지 VM/클러스터, 캐시 크기, 경로

- 쓰기 백 활성화됨, DR 캐시 상태
- 상대적 크기 구성
- 디렉토리 경로 미리 채우기
- 캐시와 오리진 간의 연결 상태

스토리지 **VM** 수준

- 이름, UUID, 상태(실행 중/중지됨), 하위 유형
- 활성화/허용된 프로토콜(NFS, CIFS, iSCSI, FCP, NVMe, S3)
- DNS 서버 및 도메인
- 이름 서비스 스위치 구성(passwd, group, hosts 등)
- IP 인터페이스(이름, IP 주소, 서비스)
- 할당된 애그리게이트
- 랜섬웨어 방지 기본 볼륨 상태
- 공간 강제 설정
- 피어 관계(애플리케이션, 상태, 원격 클러스터/스토리지 VM)

애그리게이트/스토리지 레벨

- 애그리게이트 이름, UUID, 상태, RAID 상태
- 블록 스토리지: 디스크 개수, RAID 크기, 사용 가능/사용량/총 공간, 물리적 사용량
- 클라우드 스토리지 사용
- 효율성: 비율, 논리적 사용, 절감액
- 암호화, 미러링, SnapLock 설정
- 성능 지표(IOPS, 지연 시간, 처리량)

활용도 지표**(EDA)**

- 데이터 수집 주기: 용량/처리량의 경우 12시간마다, 지연 시간의 경우 20분마다
- 세분성: 시간 범위당 약 60개의 데이터 포인트로 정규화됨
- 보존 및 저장 세부 정보: "측정 지표 및 원격 측정 참조"

NetApp Workload Factory용 암호화 및 키 관리

NetApp Workload Factory는 저장 시 암호화를 사용하며 Workload Factory 및 AWS 서비스 전반에 걸쳐 명확한 키 관리 책임을 정의합니다. Amazon FSx for NetApp ONTAP 파일 시스템의 경우, 사용자가 직접 AWS KMS 키를 선택하거나 AWS에서 관리하는 기본 키를 사용할 수 있으며, FSx for ONTAP는 해당 키를 사용하여 암호화 작업을 수행합니다. Workload Factory는 또한 봉투 암호화를 사용하여 저장된 ONTAP 자격 증명을 보호합니다.

FSx용 KMS 저장 데이터 암호화 범위

Workload Factory를 통해 FSx for ONTAP 파일 시스템을 생성할 때, 선택적으로 저장 데이터 암호화를 위한 자체 AWS KMS 키를 지정할 수 있습니다. 키를 지정하지 않으면 Workload Factory는 AWS에서 관리하는 기본 FSx 키를 사용합니다.

암호화된 것은 무엇입니까**?**

FSx for ONTAP 파일 시스템을 지원하는 기본 EBS 볼륨에 저장된 모든 데이터(AWS FSx 저장 데이터 암호화).

키 소유권

KMS 키는 AWS 계정에 있습니다.

키 선택 및 사용에 필요한 권한

Workload Factory에 필요한 사항:

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant` (FSx for ONTAP 서비스에서 키를 사용할 수 있도록 하기 위함)

주요 액세스 패턴

Workload Factory는 KMS 키를 사용하여 데이터를 직접 암호화하거나 복호화하지 않습니다. 파일 시스템 생성 중에 Amazon FSx for NetApp ONTAP API로 키 ID를 전달하며, Amazon FSx for NetApp ONTAP이 암호화 작업을 수행합니다.

자격 증명 보호(서비스 측 봉투 암호화)

Workload Factory를 통해 ONTAP 자격 증명(관리자 암호)을 저장할 때, 해당 자격 증명은 저장하기 전에 봉투 암호화를 사용하여 보호됩니다.

암호화 방식

자격 증명 레코드당 고유한 데이터 암호화 키(DEK)를 사용하는 AES-256-CBC입니다.

봉투 암호화 흐름

1. 자격 증명마다 고유한 256비트 DEK가 생성됩니다.
2. DEK는 자격 증명(비밀번호)을 암호화합니다.
3. DEK 자체는 루트 키로 암호화되어 암호화된 자격 증명과 함께 저장됩니다.
4. 평문 DEK는 절대 저장되지 않습니다.

암호화 컨텍스트

각 데이터 키는 특정 자격 증명 레코드에 암호학적으로 연결되어 있어 레코드 간 키 재사용을 방지합니다.

대안**: AWS Secrets Manager**

암호화된 암호를 서비스에 저장하는 대신, ONTAP 자격 증명을 사용자 계정의 AWS Secrets Manager에 저장할 수 있습니다. Workload Factory는 암호를 보거나 저장하지 않으며, Secrets Manager ARN을 Lambda 링크로 전달하여 VPC 내에서 런타임에 암호를 검색합니다.

GovCloud 계정에는 AWS Secrets Manager가 필요합니다.

NetApp Workload Factory 계정 삭제

계정 삭제는 셀프 서비스가 아니며, Workload Factory 서비스와 AWS 계정의 리소스를 모두 포함하는 오프보딩 워크플로입니다. 정리 작업에는 Workload Factory 계정, FSx for ONTAP 파일 시스템, 자격 증명, 링크, 알림 채널, 관련 IAM, AWS Lambda 및 Amazon CloudWatch 리소스와 연결된 모든 데이터가 안전하게 제거되는 작업이 포함됩니다. 이 작업은 되돌릴 수 없습니다.

Workload Factory 계정을 제거해야 할 경우 "NetApp 지원팀에 문의하십시오."

관찰 가능성(로그, 메트릭, 원격 측정)

NetApp Workload Factory의 관찰 가능성에 대해 알아보십시오.

관찰 가능성 신호는 운영 모니터링, 문제 해결 및 조사에 도움이 됩니다. NetApp Workload Factory에서 관찰 가능성은 서비스 동작, AI 사용량 및 Workload Factory를 통해 수행된 작업에 대한 가시성을 제공하는 메트릭, 원격 측정 데이터 및 운영 기록을 포함합니다. 원격 측정 데이터와 운영 기록은 내부 모니터링 및 고객 대상 감사 가시성을 지원하며, Tracker를 통해 지원되는 작업의 진행 상황, 상태 및 세부 정보를 검토할 수 있습니다.

원격 측정 및 운영 기록

Workload Factory는 다음과 같은 원격 측정 및 운영 기록 유형을 사용합니다.

- OpenTelemetry 추적 데이터가 OTLP HTTP를 통해 SigNoz(내부 관찰 가능 도구)로 내보내졌습니다.
- AI 사용량 측정(토큰 수, 모델 비용)은 AWS Timestream에 저장됩니다.
- NetApp Console 감사 기록(작업 이름, 상태, 요청/응답 메타데이터, 타임스탬프)

Workload Factory의 감사 로깅

Workload Factory는 실행 중인 작업과 실행 시간을 모니터링할 수 있는 모니터링 기능인 Tracker를 제공합니다. Tracker를 사용하면 FSx for ONTAP, 자격 증명 및 링크 작업의 진행 상황과 상태를 추적하고, 작업 및 하위 작업에 대한 세부 정보를 검토하고, 문제 또는 오류를 진단할 수 있습니다.

트래커에서는 다양한 작업을 수행할 수 있습니다. 기간(최근 24시간, 7일, 14일 또는 30일), 작업량, 상태 및 사용자별로 작업을 필터링할 수 있고, 검색 기능을 사용하여 작업을 찾을 수 있으며, 작업 테이블을 CSV 파일로 다운로드할 수 있습니다.

- "Workload Factory에서 Tracker를 사용하여 작업 모니터링"

관련 정보

- "NetApp Workload Factory의 메트릭 및 원격 측정"

NetApp Workload Factory의 메트릭 및 원격 측정

NetApp Workload Factory는 볼륨 수준 및 파일 시스템 수준의 메트릭을 수집하여 AWS CloudWatch에 저장함으로써 스토리지 성능 및 스토리지 용량에 대한 운영 가시성을 제공합니다. 처리량 등 계산된 메트릭은 이러한 수집된 값을 기반으로 생성됩니다. 메트릭 정의, 수집 주기, 새로 고침 동작 및 보존 기간에 대한 자세한 내용을 확인하세요.

포함된 지표

NetApp Workload Factory는 운영 로그 및 이벤트에 대해 다음과 같은 메트릭을 사용합니다.

- 볼륨 수준 CloudWatch 메트릭(볼륨별로 수집됨)

- 파일 시스템 수준의 CloudWatch 메트릭(파일 시스템별로 수집됨)
- 계산된 지표
- 수집 일정 및 보존

운영 지표에 관하여

계산된 지표는 다음 공식을 사용합니다.

- 처리량(바이트/초) = (NetworkSentBytes + NetworkReceivedBytes) / 기간

새로 고침 동작:

- 볼륨 및 클러스터 메트릭은 12시간마다 새로 고쳐집니다.
- 지연 시간 측정값은 20분마다 갱신됩니다.
- DynamoDB 항목은 14일 후 자동으로 만료됩니다.

원격 측정 데이터 수집 정보

- OpenTelemetry 추적 데이터가 OTLP HTTP를 통해 SigNoz(내부 관찰 가능 도구)로 내보내졌습니다.
- AI 사용량 측정(토큰 수, 모델 비용)은 AWS Timestream에 저장됩니다.
- NetApp Console 감사 기록(작업 이름, 상태, 요청/응답 메타데이터, 타임스탬프)

볼륨 수준 **CloudWatch** 메트릭(볼륨별로 수집됨)

메트릭	**AWS CloudWatch** 이름	단위	측정하는 것
볼륨 스토리지 용량	StorageCapacity	바이트	총 프로비저닝된 용량
사용된 스토리지	StorageUsed	바이트	실제 데이터 저장됨
읽은 데이터 바이트	DataReadBytes	바이트	읽기 처리량
데이터 쓰기 바이트	DataWriteBytes	바이트	쓰기 처리량
데이터 읽기 작업	DataReadOperations	개수	읽기 IOPS
데이터 쓰기 작업	DataWriteOperations	개수	쓰기 IOPS
메타데이터 작업	MetadataOperations	개수	메타데이터 IOPS
데이터 읽기 작업 시간	DataReadOperationTime	초	읽기 지연 시간
데이터 쓰기 작업 시간	DataWriteOperationTime	초	쓰기 지연 시간
메타데이터 작업 시간	MetadataOperationTime	초	메타데이터 지연 시간

파일 시스템 수준의 **CloudWatch** 지표

메트릭	**AWS CloudWatch** 이름	단위	측정하는 것
SSD 스토리지 용량	StorageCapacity	바이트	총 SSD 계층 용량
SSD 스토리지 사용	StorageUsed(SSD 계층)	바이트	SSD 계층 소비량

메트릭	**AWS CloudWatch** 이름	단위	측정하는 것
용량 풀 사용됨	StorageUsed(용량 풀)	바이트	용량 풀 소비
CPU 사용률	CPUUtilization	퍼센트	파일 서버 CPU
SSD 용량 활용률	StorageCapacityUtilization	퍼센트	SSD 티어 사용률
네트워크 처리량 활용	NetworkThroughputUtilization	퍼센트	네트워크 활용률
디스크 IOPS 사용률	DiskIopsUtilization	퍼센트	디스크 IOPS 사용률
디스크 처리량 활용률	FileServerDiskThroughputUtilization	퍼센트	디스크 처리량 활용률
디스크 IOPS 사용률(서버)	FileServerDiskIopsUtilization	퍼센트	서버 디스크 IOPS 사용률
스토리지 효율성 절감	StorageEfficiencySavings	바이트	효율성으로 공간 절약
네트워크 수신됨	NetworkReceivedBytes	바이트	인바운드 네트워크
네트워크 전송됨	NetworkSentBytes	바이트	아웃바운드 네트워크

수집 일정 및 보존

시간 범위	수집 기간	데이터 포인트	스토리지	보유
1일	24분	~60	DynamoDB	14일(TTL)
1주일	약 2.8시간	~60	DynamoDB	14일(TTL)
1개월	12시간	~60	DynamoDB	14일(TTL)
3개월	약 1.5일	~60	DynamoDB	14일(TTL)
1년	약 6일	~60	DynamoDB	14일(TTL)

생성형 AI 보안 제어

NetApp Workload Factory의 AI 제어 기능에 대해 알아보십시오.

NetApp Workload Factory는 모델 액세스, 데이터 범위 및 런타임 동작에 대한 보안 제어를 강화하면서 진단 속도를 높이는 생성형 AI 기능을 포함합니다.

Workload Factory는 기본적으로 AI 진단을 활성화합니다. Workload Factory **Administration** 설정에서 언제든지 생성형 AI 기능을 비활성화할 수 있습니다. "GenAI 기능 관리에 대해 자세히 알아보십시오."

보안 범위 AI 기능 개요

Workload Factory는 현재 다음과 같은 기능에 생성형 AI를 적용하고 있습니다.

- Ask Me 어시스턴트(엄선된 NetApp 문서와 함께 RAG를 사용하여 소스 기반 응답 제공)
- 지연 시간 분석
- EMS 이벤트 분석
- 오류 로그 분석

AI 진단을 위한 AWS Bedrock 개요

Workload Factory는 AI 추론을 위해 Amazon Bedrock을 사용합니다. 추론은 구성된 자격 증명 및 추론 프로필을 사용하여 AWS 계정에서 실행됩니다.

관련 정보

- "Amazon Bedrock에서 NetApp Workload Factory AI 진단 옵트인"
- "NetApp Workload Factory용 AI 툴 경계"
- "NetApp Workload Factory용 AI 모델 파라미터 및 청구"

Amazon Bedrock에서 NetApp Workload Factory AI 진단 옵트인

NetApp Workload Factory의 AI 진단은 Amazon Bedrock을 사용하여 이벤트를 분석하며, 이 기능은 기본적으로 활성화되어 있습니다. Workload Factory에서 선택한 Bedrock 모델을 호출하고 진단 데이터를 수집하려면 IAM 권한, 추론 프로필, 그리고 SSH 기능을 갖춘 연결된 Lambda 링크를 구성해야 합니다. 이러한 구성 요소 중 하나라도 누락되었거나 Bedrock 구성이 제거되면 AI 진단을 사용할 수 없게 됩니다.

AI 진단은 기본적으로 활성화되어 있습니다.

시작하기 전에

- 계정에 AWS Bedrock 추론 프로필이 포함되어 있는지 확인하십시오.

- 진단 데이터 수집을 위해 SSH 기능이 있는 연결된 Lambda 링크를 보유합니다.

단계

1. IAM 역할에서 Bedrock 권한을 부여합니다.
   - `bedrock:InvokeModel`
   - `bedrock:InvokeModelWithResponseStream`
   - `bedrock:ListInferenceProfiles`
   - `bedrock:GetInferenceProfile`
2. Workload Factory 설정에서 추론 프로파일 ARN을 구성하십시오.

필수 구성 요소 중 하나라도 누락된 경우 시스템은 누락된 구성 요소를 구체적으로 보고하고 AI 기능은 비활성화된 상태로 유지됩니다.

AI 진단 비활성화

AI 진단을 비활성화하려면:

- IAM 역할에서 Bedrock 권한을 제거하거나
- Workload Factory 설정에서 Bedrock 구성을 삭제합니다.

AI 진단을 즉시 사용할 수 없게 되며, 잔여 데이터 처리는 발생하지 않습니다.

지역 및 지역 간 추론 프로필

Bedrock 추론은 추론 프로필에 지정된 AWS 리전에서 실행됩니다. 교차 리전 추론 프로필을 사용하는 경우, AWS는 표준 AWS Bedrock 동작에 따라 프로필 구성에 있는 모든 리전으로 요청을 라우팅할 수 있습니다. 데이터는 AWS 인프라를 벗어나지 않습니다.

NetApp Workload Factory용 AI 툴 경계

NetApp Workload Factory는 AI 기능이 AWS 및 ONTAP 환경과 상호 작용하는 방식에 엄격한 제한을 두므로 의도치 않은 변경 위험 없이 AI 기반 진단을 신뢰할 수 있습니다. Amazon Bedrock은 변경 명령을 차단하고 크기 및 실행 시간으로 출력을 제한하는 읽기 전용 AWS CLI 및 ONTAP CLI 진단 툴을 사용하며, 사용되는 모든 데이터는 일시적이며 NetApp Workload Factory 또는 AWS에 보관되지 않습니다.

툴 안전 제어

툴	기능	안전 제어 장치
AWS CLI (읽기 전용)	읽기 전용 AWS CLI 명령(describe, list, get)을 실행합니다.	생성, 삭제, 수정, 업데이트, 추가, 제거 등 모든 변경 동사를 차단합니다. 단계당 최대 10개의 명령만 허용됩니다. 출력 크기는 20KB에서 잘립니다.
ONTAP CLI (읽기 전용)	SSH를 사용하여 읽기 전용 ONTAP CLI 명령을 실행합니다.	변경 동사(delete, destroy, create, modify, move)를 모두 차단합니다. 출력 내용이 잘립니다.

에이전트는 리소스를 수정, 생성 또는 삭제할 수 없습니다. 에이전트는 관찰 및 진단만 가능합니다.

데이터 보존 및 모델 훈련 경계

AWS 정책에 따라 Amazon Bedrock은 기본 모델을 학습하거나 개선하기 위해 사용자의 입력 및 출력을 저장하거나 사용하지 않습니다. 온디맨드 추론(Workload Factory에서 사용)의 경우, AWS는 데이터를 일시적으로 처리하며 응답을 반환한 후에는 데이터를 보관하지 않습니다.

NetApp Workload Factory용 AI 모델 파라미터 및 청구

NetApp Workload Factory는 AI 거버넌스와 관련된 모델 구성, 사용량 및 청구 범위를 정의합니다. 구성된 모델은 결정론적 매개변수를 사용하고 일관된 분석 결과를 지원하기 위해 구조화된 JSON을 반환합니다. AWS는 Amazon Bedrock 추론에 대한 비용을 사용자 계정으로 청구하며, Workload Factory는 AI 사용량을 추적하고 계정별 월별 비용을 투명하게 제공합니다. 이 섹션에서는 모델 매개변수와 AI 사용량에 적용되는 제한 사항에 대해 설명합니다.

모델 및 매개변수

매개변수	가치
모델	Anthropic Claude(교차 지역 추론 프로필 사용)
온도	0 (결정론적, 무작위성 없음)
최대 출력 토큰	2,048
최대 추론 단계	분석당 15개
출력 형식	구조화된 JSON (요약, 심각도, 근본 원인, 시정 조치)

청구 및 사용 한도

- AWS는 Bedrock 추론에 대한 비용을 사용자 계정(추론 프로필, 자격 증명)으로 청구합니다.
- Workload Factory는 AI 사용량을 내부적으로 추적합니다.
- Workload Factory는 계정별 월별 비용 현황을 제공합니다.

  "NetApp Workload Factory에서 스토리지 비용을 추적합니다"

Ask Me AI 어시스턴트

NetApp Workload Factory용 Ask Me 보안 아키텍처

Ask Me는 NetApp Workload Factory 내에 내장된 생성형 AI 기반 어시스턴트입니다. Amazon FSx for NetApp ONTAP 및 Workload Factory 주제에 대한 실시간 대화형 지원을 제공합니다. 답변은 검증된 NetApp 문서를 기반으로 하며, Ask Me는 퍼블릭 인터넷에 액세스하거나 모델을 학습시키는 데 고객 데이터를 사용할 수 없습니다. 다중 보안 레이어는 악성 쿼리를 차단하고, 지원되는 도메인으로 답변을 제한하며, 사용자 입력이 시스템 지침을 재정의하지 못하도록 방지합니다. Ask Me가 툴을 사용할 때 권한 부여 경계, 읽기 전용 쿼리 적용, 임시 샌드박스 및

감사 로깅은 실행을 제한하고 모니터링하는 데 도움이 됩니다.

Workload Factory 관리 설정에서 언제든지 Ask Me를 옵트아웃할 수 있으며, 이렇게 하면 사용자 계정에 대한 어시스턴트가 비활성화됩니다. "GenAI 기능 관리에 대해 자세히 알아보십시오."

Ask Me의 **RAG** 아키텍처

Ask Me는 검색 증강 생성(RAG)을 사용합니다.

- 엄선된 지식 기반: 답변은 검증되고 게시된 NetApp 문서 모음을 기반으로 합니다.
- 검색 점수화 및 필터링: 충분히 관련성이 높은 콘텐츠만 모델 컨텍스트에 포함됩니다.
- 인터넷 접속 불가: 모델이 외부 콘텐츠를 가져오거나, 검색하거나, 스크래핑할 수 없습니다.
- 출처 표기: 답변에는 사용된 출처 문서에 대한 참조가 포함됩니다.

다중 계층 프롬프트 보안

- 1단계: 보안 분류기(LLM-as-a-judge)는 악의적인 쿼리(프롬프트 주입, 권한 상승, 데이터 유출, 소셜 엔지니어링, 정책 위반)를 차단합니다.

  시스템은 차단된 쿼리를 기록하지만, 생성 모델은 이를 전혀 인식하지 못합니다.

- 2단계: 시스템 프롬프트 강화는 사용자 입력이 시스템 명령을 덮어쓰는 것을 방지합니다.
- 레이어 3: 도메인 범위 지정으로 인해 FSx ONTAP 및 Workload Factory 주제에 대한 응답이 제한됩니다.
- 레이어 4: 툴 사용 거버넌스는 강화된 샌드박스에서 매개변수를 검증하고 쿼리를 실행합니다. 모델은 임의의 작업을 실행할 수 없습니다.

모델 데이터 격리 및 개인 정보 보호

- 고객 데이터를 사용한 모델 학습 없음
- 요청 수준 격리(테넌트 간 데이터 유출 방지)
- 제한된 기록을 가진 세션 범위의 대화 컨텍스트
- 영구적인 모델 메모리 없음
- 관리형 추론 인프라

툴 사용 및 에이전트 보안

- 권한 범위 기반 툴(사용자 권한 경계 적용)
- 엄격한 툴 실행 시간 제한
- 검색된 데이터를 위한 임시 세션 범위 샌드박스
- 허용 목록을 사용한 읽기 전용 쿼리 강제 적용
- 민감한 매개변수 스크러빙을 통한 툴 호출 감사 기능

NetApp Workload Factory용 Ask Me 액세스 제어

NetApp Workload Factory의 Ask Me 액세스 보안은 인증된 세션, 사용자 수준의 책임, 런타임 작업 중 보호된 비밀 키 처리에 중점을 둡니다. 인증 제어는 각 세션을 검증하고 상호 작용을 특정 사용자와 연결합니다. 민감한 자격 증명은 런타임에 관리되는 비밀 키 저장소에서 검색되고 로그에서 삭제됩니다. 또한 이 서비스는 루트 권한이 없는 컨테이너 실행 및 제한된 CORS 허용 목록을 포함한 인프라 제어를 적용합니다.

인증

- 대상, 발급자 및 RS256 등 알고리즘 검사를 포함한 암호화 검증을 통한 서명된 JWT 인증
- 서비스 경계에서 미들웨어를 이용한 인증
- 사용자 ID 범위를 지정하여 상호 작용이 특정 사용자에게 귀속되도록 합니다.

자격 증명 보호 및 기밀 처리

- 안전한 저장소: 서비스에서 사용하는 민감한 자격 증명은 관리형 비밀 저장소에 저장되며 런타임에 검색됩니다. 비밀 정보는 애플리케이션 코드, 구성 파일 또는 컨테이너 이미지에 저장되지 않습니다.
- 로그 정제: 민감한 값(자격 증명, 토큰, 암호, 액세스 키, 인증서)은 로그에 기록되기 전에 삭제됩니다.

인프라 보안

- 루트 권한이 없는 컨테이너 실행
- CORS는 신뢰할 수 있는 NetApp 도메인의 명시적인 허용 목록으로 제한됩니다.

NetApp Workload Factory의 Ask Me 실행 모드

NetApp Workload Factory는 Ask Me에 대해 서로 다른 보안 및 개인 정보 보호 특성을 가진 여러 실행 모드를 제공합니다. Ask Me가 툴 통합을 사용하는 경우(예: 고객의 Workload Factory 리소스를 쿼리하는 경우), 툴 실행은 계층화된 보안 조치를 통해 제어됩니다. 툴을 사용한 실행은 인증된 사용자의 권한 범위 내에서 작동하며 각 작업의 지속 시간과 범위에 제한이 적용됩니다. 검색된 데이터는 외부 액세스가 차단되는 임시 세션 샌드박스에 저장되며 세션이 종료되면 삭제됩니다. 독립적인 프롬프트 및 코드 제어를 통해 읽기 전용 쿼리가 적용되며, 감사 기록은 민감한 값이 삭제된 상태로 툴 활동을 기록합니다.

툴 실행 보호 장치

- 권한 범위 툴은 인증된 사용자의 권한 내에서 작동합니다.
- 툴 실행 시간 초과는 장시간 실행되는 작업을 제한합니다.
- 임시 데이터 샌드박스는 툴로 검색된 데이터를 세션 범위 내에 저장하고, 외부 액세스, 파일 I/O, 네트워크 호출 및 엔진 수준에서의 확장 프로그램 로딩을 차단하며, 세션이 종료되면 소멸됩니다.
- 읽기 전용 쿼리 강제 적용은 엄격한 허용 목록을 통해 생성된 쿼리의 유효성을 검사합니다.
- 프롬프트 적용 보안과 코드 적용 보안은 독립적으로 적용됩니다.
- 툴 호출 감사 기능은 툴 이름, 매개변수, 타임스탬프 및 결과 상태를 로깅하며, 민감한 값은 스크러빙됩니다.

출력 제어

- 토큰 제한 시행
- 분류/보안 중요 작업에 대한 결정론적 출력(온도 0)
- 조기 종료 및 정리 기능을 갖춘 스트리밍

NetApp Workload Factory용 Ask Me 개인 정보 보호 및 가용성

NetApp Workload Factory의 Ask Me 개인정보 보호 제어는 데이터 노출을 제한하고, 세션 처리를 격리하며, 사용자 상호 작용에 대한 개인정보 보호 경계를 유지합니다. 사용자의 입력은 관리형 AI 서비스에서 처리되며, 이 서비스는 해당 입력을 기본 모델 학습이나 개선에 사용하지 않습니다. 검색된 운영 데이터는 세션 기간 동안 임시 메모리 저장소에 보관되며 영구 저장되거나 공유되지 않습니다. 여러 클라우드 지역에 걸쳐 있는 멀티 모델 폴백 체인은 기본 모델의 성능 저하 또는 사용 불가 시에도 가용성을 보장하며, 폴백 모델에도 동일한 보안 제어가 적용됩니다.

데이터 처리 및 개인정보 보호

- 프롬프트에 포함된 사용자 데이터: 사용자의 입력을 기본 모델 학습 또는 개선에 사용하지 않는 관리형 AI 서비스에서 처리됩니다.
- 기술 자료 콘텐츠: 엄선되어 게시된 NetApp 문서만 포함되며, 사용자 데이터는 포함되지 않습니다.
- 운영 데이터: 사용자가 자신의 리소스를 조회할 때만 검색되며, 세션 기간 동안 임시 메모리 저장소에 보관되고 영구 저장되거나 공유되지 않습니다.
- 감사 로깅: 쿼리 메타데이터(익명 처리된 사용자 ID, 타임스탬프, 지속 시간)가 기록되며, 민감한 필드는 삭제됩니다.
- 피드백 데이터: 별도로 저장되며 쿼리 ID에 연결되고, 익명화된 사용자 ID 외의 개인 식별 정보와는 연결되지 않습니다.

가용성 및 격리 제어

Ask Me는 여러 클라우드 지역에 걸쳐 다중 모델 대체 체인을 사용합니다.

기본 모델이 조절되거나 사용할 수 없는 경우, 시스템은 대체 모델로 페일오버할 수 있습니다.

모든 모델은 동일한 보안 제어, 시스템 프롬프트 강화 및 격리 보장이 적용됩니다.

ONTAP 운영 및 Lambda 링크(고객 VPC 구성 요소)

NetApp Workload Factory용 Lambda 링크에 대해 알아봅니다.

NetApp Workload Factory는 Amazon FSx for NetApp ONTAP API에서 노출되지 않는 ONTAP 네이티브 작업을 AWS 계정 경계 내에서 유지하기 위해 VPC에 배포된 AWS Lambda 함수인 _link_를 사용합니다. 이 링크는 사용자의 서브넷 및 보안 그룹에서 실행되므로 실행 구성 요소는 AWS 환경 내에 유지됩니다. Workload Factory는 사용 가능한 AWS 서비스 API가 아닌 직접 ONTAP 액세스가 필요한 작업에 대해서만 이 링크를 호출합니다. 링크의 아키텍처를 NetApp Console 에이전트의 보안 및 운영 프로필과 비교합니다.

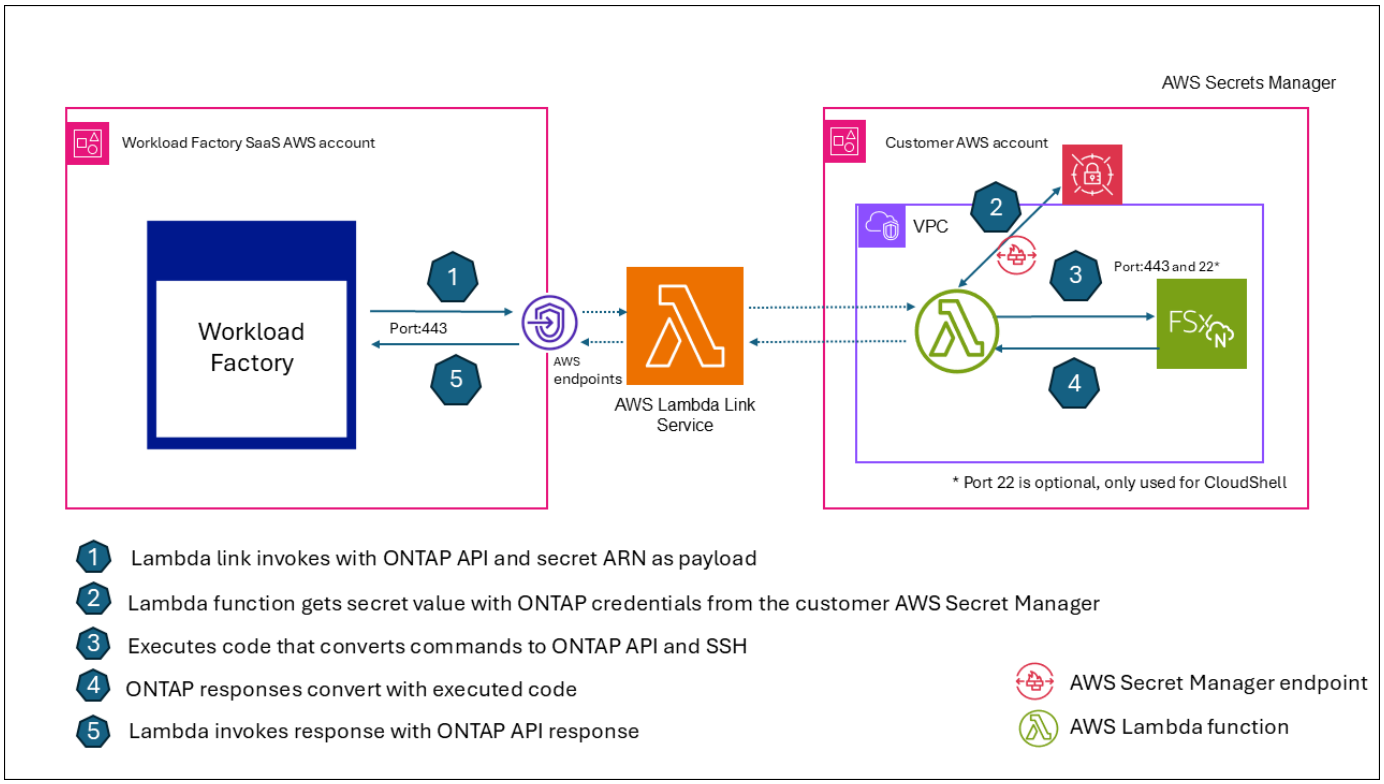
링크 보안 아키텍처

Workload Factory 링크는 Workload Factory 계정과 하나 이상의 FSx for ONTAP 파일 시스템 간에 신뢰 관계 및 간접 연결을 생성합니다.

다음 표는 Lambda 링크 보안 아키텍처에 대한 개요를 제공합니다. 이 정보를 활용하여 네트워킹 구성, 런타임 환경 및 운영 제한 사항 등 Lambda 함수가 AWS 계정에 배포되고 실행되는 방식을 이해하십시오.

속성	세부 정보
컴퓨팅	AWS Lambda(컨테이너 이미지)
런타임	Node.js 22
구축	CloudFormation AWS 계정의 스택
VPC 배치	귀하의 서브넷, 보안 그룹
시간 초과	호출당 10초
호출	동기식(RequestResponse)
패키지 유형	컨테이너 이미지(NetApp ECR에서 가져옴)

다음 다이어그램은 Lambda 링크의 보안 아키텍처를 보여줍니다.



Lambda 링크와 NetApp Console 에이전트 비교

Lambda 링크와 NetApp Console 에이전트는 서로 다른 목적을 가지고 있으며 보안 및 운영 측면에서 각기 다른 의미를 지닙니다.

차원	링크(Lambda 기반)	NetApp Console 에이전트(VM/Pod 기반)
런타임 모델	서버리스(AWS Lambda), 고객 배포	고객이 배포한 VM/컨테이너; NetApp 콘솔 서비스 Pod를 실행합니다.
주요 범위	컨트롤 플레인 ONTAP REST 작업(AWS API에서 해당 작업을 지원하지 않는 경우에만 해당)	데이터 서비스를 위한 오케스트레이션 및 지원 기능
데이터 서비스 지원	데이터 서비스를 호스팅하지 않습니다	데이터 서비스를 호스팅할 수 있습니다(NetApp 콘솔 서비스 Pod 실행)
운영 오버헤드	상시 가동 VM 없음	VM 수명 주기 관리 및 업그레이드

관련 정보

전체 시스템 간 연결성 맵은 "NetApp Workload Factory의 연결 및 신뢰 경로"을 참조하십시오.

NetApp Workload Factory의 Lambda 링크 포트 및 호출

NetApp Workload Factory는 Lambda 링크 요청 및 포트 경계를 사용하여 필요한 아웃바운드 연결과 IAM 인증 호출을 정의합니다. 이 링크는 ONTAP 관리 엔드포인트에 대한 HTTPS 요청, 진단을 위한 읽기 전용 SSH 명령 및 상태 확인을 지원합니다. 모든 연결은 VPC 내 링크에서 아웃바운드로 이루어지므로 인바운드 연결이나 외부 엔드포인트는 필요하지 않습니다.

Workload Factory는 IAM 기반 인증을 사용하여 AWS Lambda API를 통해 이 링크를 호출합니다.

요청 유형

- HTTPS(ONTAP REST API): 볼륨, 스토리지 VM 및 클러스터 작업을 위한 ONTAP 관리 엔드포인트(포트 443)에 대한 HTTPS 호출을 프록시합니다.
- SSH(ONTAP CLI): 진단 및 성능 데이터를 위해 포트 22에서 읽기 전용 ONTAP CLI 명령을 실행합니다.
- 상태 점검: 현재 상태 및 지원되는 기능을 반환합니다.

아웃바운드 네트워크 경계

방향	포트	목적지	목적
아웃바운드	443	ONTAP 관리 IP(VPC 내)	REST API 작업
아웃바운드	22	ONTAP 관리 IP(VPC 내)	SSH CLI 명령
아웃바운드	443	AWS Secrets Manager 엔드포인트(선택 사항)	Secrets Manager를 사용할 때 자격 증명 검색

별도의 인바운드 연결은 필요하지 않습니다. 해당 링크는 엔드포인트를 노출하지 않습니다. Workload Factory는 AWS `lambda:InvokeFunction` API를 사용하여 해당 링크를 호출합니다.

Workload Factory가 Lambda 링크를 호출합니다

Workload Factory는 IAM 기반 인증을 사용하여 AWS Lambda API(`lambda:InvokeFunction`)를 통해 Lambda 링크를 호출합니다.

호출 페이로드에는 다음 내용이 포함됩니다.

- 대상 ONTAP 관리 엔드포인트(IP/호스트 이름)
- 수행할 작업 (REST API 경로 또는 SSH 명령어)
- 인증 정보(인라인 자격 증명 또는 Secrets Manager ARN 참조)

관련 정보

전체 시스템 간 연결성 지도를 보려면 "NetApp Workload Factory의 연결 및 신뢰 경로"을 참조하십시오.

NetApp Workload Factory용 Lambda 링크 IAM 권한

NetApp Workload Factory는 Lambda 링크 권한 경계를 사용하여 Lambda 실행 및 Workload Factory 호출에 필요한 IAM 액세스를 정의합니다. 이러한 권한은 선택 사항이지만 ONTAP 네이티브 작업에는 필수입니다. Secrets Manager 지원을 구성하면 링크는 런타임에 AWS Secrets Manager에서 ONTAP 자격 증명을 직접 가져오며, 암호는 Secrets Manager에서 Lambda 함수로, 그리고 다시 ONTAP 엔드포인트로 VPC 내에서만 전송됩니다.

요청 경로 및 포트 요구 사항은 "Lambda 링크 포트 및 호출"을 참조하십시오.

Lambda 실행 역할 권한

Lambda 실행 역할은 VPC에 링크를 배포할 때 다음 권한이 필요합니다.

권한	목적
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2:DeleteNetworkInterface	표준 VPC 연결 Lambda 네트워킹
ec2:AssignPrivateIpAddresses / ec2:UnassignPrivateIpAddresses	VPC ENI IP 관리
secretsmanager:GetSecretValue (FSxSecret* 범위)	ONTAP 자격 증명 검색(Secrets Manager가 활성화된 경우에만)
CloudWatch Logs(관리형 정책)	Lambda 실행 로깅

Workload Factory 호출 권한

Lambda 링크 리소스 기반 정책은 Workload Factory 서비스 주체에게 다음과 같은 권한을 부여합니다.

권한	목적
lambda:InvokeFunction	Lambda를 실행합니다
lambda:GetFunction	상태 및 건강 점검
lambda:UpdateFunctionCode	버전 업그레이드(이미지 업데이트)
lambda:GetFunctionConfiguration	구성 검증

NetApp Workload Factory의 Lambda 링크 수명 주기

NetApp Workload Factory는 Lambda 링크 수명 주기 제어를 사용하여 배포, 상태 모니터링 및 제어된 이미지 업데이트를 최소한의 운영 노출로 관리합니다. Amazon CloudFormation 스택을 재배포하지 않고도 `lambda:UpdateFunctionCode` 권한을 사용하여 Lambda 링크 컨테이너 이미지를 업데이트하여 개선 사항이나 보안 패치를 배포할 수 있습니다. 수명 주기 제어는 링크 상태를 모니터링하고 더 이상 필요하지 않을 때 Lambda 링크 및 관련 리소스를 제거하는 방법도 정의합니다.

수명주기 제어 지점

- 배포: Amazon CloudFormation 또는 Terraform 스택 배포를 통해 자동화
- 모니터링: 상태 점검을 통해 연결 문제를 감지하고, 장애 카운터를 통해 안정성을 추적합니다.
- 삭제: CloudFormation 스택을 삭제하면 AWS 계정에서 Lambda 및 관련 리소스가 제거됩니다.

지식 및 지원

NetApp 지원에 등록

NetApp 기술 지원으로 지원 케이스를 열려면 먼저 NetApp Support Site 계정을 Workload Factory에 추가하고 지원을 등록해야 합니다.

NetApp Workload Factory 및 해당 스토리지 솔루션과 서비스에 대한 기술 지원을 받으려면 지원 등록이 필요합니다. Workload Factory와는 별도의 웹 기반 콘솔인 NetApp Console에서 지원을 등록해야 합니다.

지원 등록을 한다고 해서 클라우드 공급자 파일 서비스에 대한 NetApp 지원이 활성화되는 것은 아닙니다. 클라우드 공급자 파일 서비스, 해당 인프라 또는 해당 서비스를 사용하는 솔루션과 관련된 기술 지원은 해당 제품의 Workload Factory 설명서에 있는 "도움 받기" 섹션을 참조하십시오.

"Amazon FSx for ONTAP"

지원 등록 개요

계정 ID 지원 구독(NetApp 콘솔의 지원 리소스 페이지에 있는 20자리 일련 번호 960xxxxxxxxx)을 등록하면 해당 ID가 단일 지원 구독 ID로 사용됩니다. 각 NetApp 계정 수준 지원 구독은 모두 등록해야 합니다.

등록을 통해 지원 티켓 생성 및 자동 케이스 생성과 같은 기능을 사용할 수 있습니다. 등록은 아래 설명된 대로 NetApp Support Site(NSS) 계정을 NetApp Console에 추가하여 완료합니다.

NetApp 지원을 위한 계정 등록

지원을 등록하고 지원 권한을 활성화하려면 계정의 사용자 중 한 명이 NetApp Support Site 계정을 NetApp Console 로그인에 연결해야 합니다. NetApp 지원 등록 방법은 이미 NetApp Support Site(NSS) 계정이 있는지 여부에 따라 다릅니다.

NSS 계정을 보유한 기존 고객

NSS 계정을 보유한 NetApp 고객이라면 NetApp Console을 통해 지원을 등록하기만 하면 됩니다.

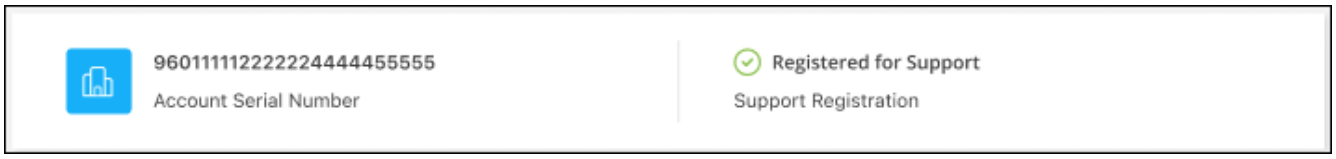
단계

1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택하십시오.

   이 옵션을 선택하면 새 브라우저 탭에서 NetApp Console이 열리고 지원 대시보드가 로드됩니다.

2. NetApp Console 메뉴에서 *관리*를 선택한 다음 *자격 증명*을 선택합니다.
3. *사용자 자격 증명*을 선택합니다.
4. *NSS 자격 증명 추가*를 선택하고 NetApp 지원 사이트(NSS) 인증 프롬프트를 따르십시오.
5. 등록 절차가 성공적으로 완료되었는지 확인하려면 도움말 아이콘을 선택한 다음 *지원*을 선택하세요.

   리소스 페이지에 계정이 지원 서비스에 등록되어 있음을 확인할 수 있습니다.



다른 NetApp Console 사용자가 NetApp Support Site 계정을 NetApp Console 로그인에 연결하지 않은 경우 동일한 지원 등록 상태를 볼 수 없습니다. 하지만 그렇다고 해서 귀하의 NetApp 계정이 지원에 등록되지 않았다는 의미는 아닙니다. 계정 내 사용자 중 한 명이라도 이 단계를 완료했다면 귀하의 계정은 등록된 것입니다.

기존 고객이지만 **NSS** 계정이 없습니다

기존 NetApp 고객으로 라이선스와 일련 번호는 있지만 NSS 계정이 없는 경우, NSS 계정을 생성하고 NetApp Console 로그인과 연결해야 합니다.

단계

1. NetApp 지원 사이트 계정을 생성하려면 다음을 완료하십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 적절한 사용자 레벨(일반적으로 **NetApp Customer/End User**)을 선택하십시오.
   b. 위에서 사용한 NetApp 계정 일련 번호(960xxxx)를 복사하여 일련 번호 필드에 입력하십시오. 이렇게 하면 계정 처리 속도가 빨라집니다.
2. NSS 계정을 보유한 기존 고객 아래의 단계를 완료하여 새 NSS 계정을 NetApp Console 로그인과 연결하십시오.

NetApp을 처음 사용하시나요

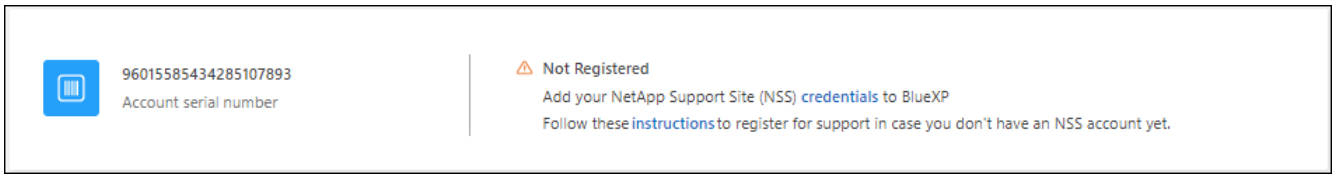
NetApp을 처음 사용하시거나 NSS 계정이 없으신 경우, 아래 각 단계를 따르십시오.

단계

1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택하십시오.

   이 옵션을 선택하면 새 브라우저 탭에서 NetApp Console이 열리고 지원 대시보드가 로드됩니다.

2. 지원 자료 페이지에서 계정 ID 일련 번호를 찾으십시오.



3. "NetApp의 지원 등록 사이트"로 이동하여 *저는 등록된 NetApp 고객이 아닙니다*를 선택하십시오.
4. 필수 입력 항목(빨간색 별표가 있는 항목)을 모두 입력하세요.
5. **Product Line** 필드에서 *Cloud Manager*를 선택한 다음 해당 청구 제공업체를 선택하십시오.
6. 위 2단계에서 계정 일련 번호를 복사하고 보안 검사를 완료한 다음 NetApp의 글로벌 데이터 개인정보 보호 정책을 읽었음을 확인하십시오.

   이 안전한 거래를 완료하기 위해 제공하신 이메일 주소로 즉시 이메일이 발송됩니다. 몇 분 안에 인증 이메일이 도착하지 않으면 스팸 폴더를 확인해 주세요.

7. 이메일 내에서 작업을 확인합니다.

확인을 클릭하면 NetApp에 요청이 제출되며 NetApp 지원 사이트 계정을 생성할 것을 권장합니다.

8. NetApp 지원 사이트 계정을 생성하려면 다음을 완료하십시오. "NetApp 지원 사이트 사용자 등록 양식"
   a. 적절한 사용자 레벨(일반적으로 **NetApp Customer/End User**)을 선택하십시오.
   b. 위에서 사용한 계정 일련 번호(960xxxx)를 복사하여 일련 번호 입력란에 붙여넣으십시오. 이렇게 하면 계정 처리 속도가 빨라집니다.

완료한 후

NetApp이 이 과정 중에 연락을 드릴 것입니다. 이는 신규 사용자를 위한 일회성 온보딩 절차입니다.

NetApp 지원 사이트 계정을 확보한 후, NSS 계정을 보유한 기존 고객 아래의 단계를 완료하여 해당 계정을 NetApp Console 로그인과 연결하십시오.

NetApp Workload Factory용 FSx for ONTAP에 대한 도움말 얻기

NetApp 은 Workload Factory 및 클라우드 서비스에 대해 다양한 방식으로 지원을 제공합니다. 기술 자료(KB) 문서와 커뮤니티 포럼 등 광범위한 무료 자가 지원 옵션을 연중무휴 24시간 이용할 수 있습니다. 지원 등록에는 웹 티켓팅을 통한 원격 기술 지원이 포함됩니다.

FSx for ONTAP 지원 받기

FSx for ONTAP, 해당 인프라 또는 해당 서비스를 사용하는 솔루션과 관련된 기술 지원은 해당 제품의 Workload Factory 설명서에 있는 "도움 받기" 섹션을 참조하십시오.

"Amazon FSx for ONTAP"

Workload Factory 및 해당 스토리지 솔루션과 서비스에 대한 기술 지원을 받으려면 아래에 설명된 지원 옵션을 사용하십시오.

셀프 지원 옵션 사용

이러한 옵션은 연중무휴 24시간 무료로 이용할 수 있습니다.

- 설명서

  현재 보고 계신 Workload Factory 문서입니다.

- "지식 기반"

  Workload Factory 기술 자료를 검색하여 문제 해결에 도움이 되는 문서를 찾아보십시오.

- "커뮤니티"

  Workload Factory 커뮤니티에 참여하여 진행 중인 토론을 팔로우하거나 새로운 토론을 시작하십시오.

NetApp 지원팀에 케이스 생성

위의 자가 지원 옵션 외에도 지원을 활성화한 후 NetApp 지원 전문가와 협력하여 문제를 해결할 수 있습니다.

시작하기 전에

케이스 생성 기능을 사용하려면 먼저 지원 등록을 해야 합니다. NetApp 지원 사이트 자격 증명을 Workload Factory 로그인과 연결하십시오. "지원 등록 방법을 알아보십시오".

단계

1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택하십시오.

   이 옵션을 선택하면 새 브라우저 탭에서 NetApp Console이 열리고 지원 대시보드가 로드됩니다.

2. 리소스 페이지에서 기술 지원 항목 아래에 있는 옵션 중 하나를 선택합니다.

   a. 전화 상담을 원하시면 *전화하기*를 선택하세요. netapp.com의 전화번호 목록 페이지로 이동합니다.

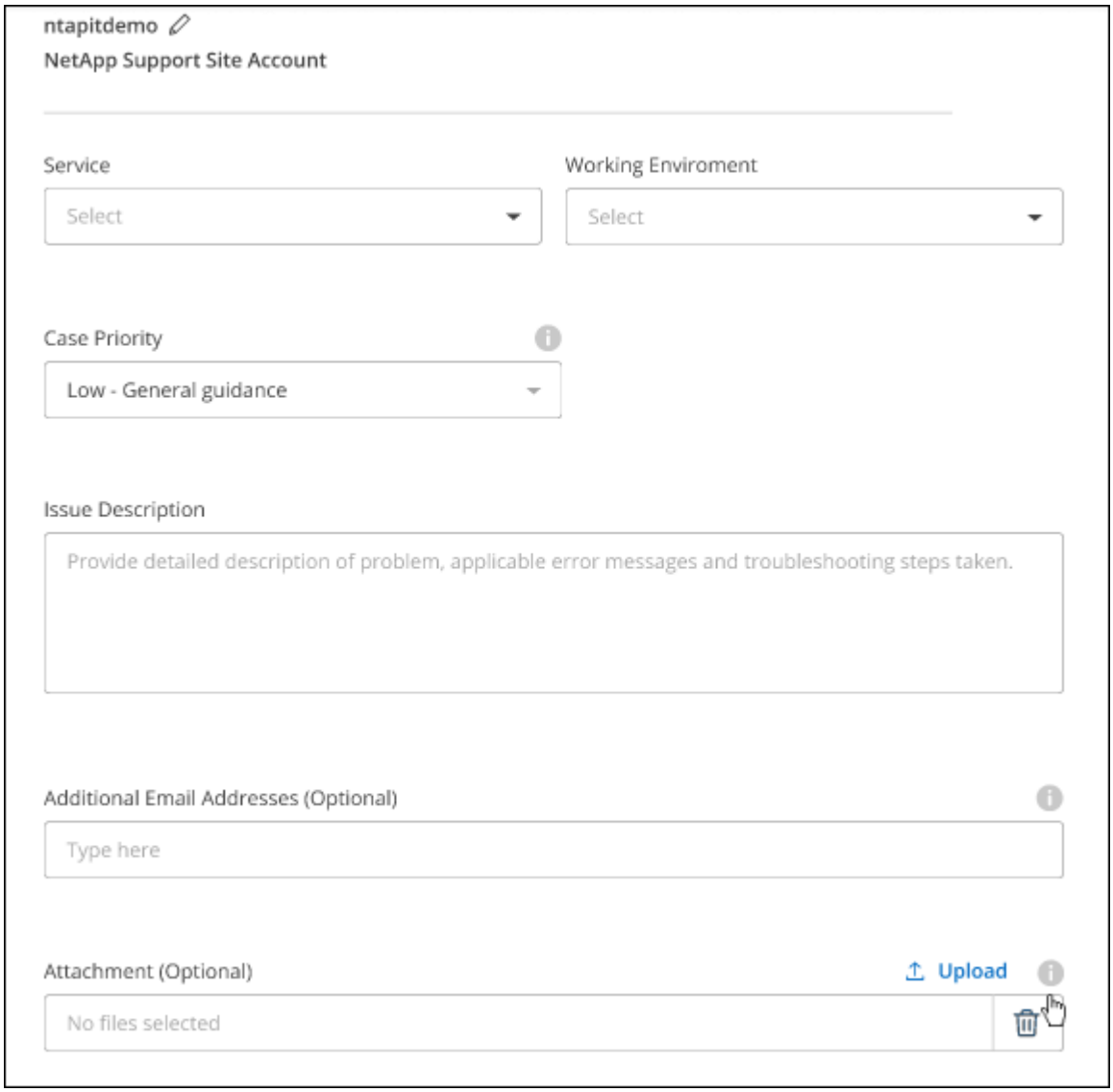
   b. NetApp 지원 전문가에게 티켓을 열려면 *케이스 생성*을 선택하세요:

      - 서비스: *Workload Factory*를 선택합니다.
      - **Case Priority**: 케이스의 우선순위를 낮음, 중간, 높음 또는 긴급 중에서 선택하십시오.

        이러한 우선순위에 대한 자세한 내용을 보려면 필드 이름 옆에 있는 정보 아이콘 위에 마우스를 올려놓으십시오.

      - 문제 설명: 발생한 문제에 대한 자세한 설명을 제공해 주십시오. 관련 오류 메시지 또는 수행한 문제 해결 단계를 포함해 주시기 바랍니다.
      - 추가 이메일 주소: 이 문제를 다른 사람에게 알리고 싶다면 추가 이메일 주소를 입력하십시오.
      - 첨부파일(선택 사항): 최대 5개의 첨부파일을 한 번에 하나씩 업로드할 수 있습니다.

        첨부 파일 크기는 파일당 25MB로 제한됩니다. 지원되는 파일 확장자는 txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv입니다.



완료한 후

지원 사례 번호가 포함된 팝업 창이 나타납니다. NetApp 지원 전문가가 귀하의 사례를 검토한 후 곧 연락드리겠습니다.

지원 사례 기록을 보려면 *설정 > 타임라인*을 선택하고 "지원 사례 생성"이라는 이름의 작업을 찾으세요. 맨 오른쪽에 있는 버튼을 클릭하면 해당 작업을 확장하여 세부 정보를 볼 수 있습니다.

케이스를 생성하려고 할 때 다음과 같은 오류 메시지가 나타날 수 있습니다.

"선택한 서비스에 대한 케이스를 생성할 권한이 없습니다."

이 오류는 NSS 계정과 해당 계정이 연결된 등록 회사가 NetApp Console 계정 일련 번호(예: 960xxxx) 또는 시스템 일련 번호에 대한 등록 회사와 일치하지 않음을 의미할 수 있습니다. 다음 옵션 중 하나를 사용하여 지원을 요청할 수 있습니다.

- 제품 내 채팅 기능을 사용하십시오
- 비기술적인 케이스를 제출하려면 https://mysupport.netapp.com/site/help

지원 사례 관리(미리 보기)

NetApp Console에서 활성 및 해결된 지원 사례를 직접 확인하고 관리할 수 있습니다. NSS 계정 및 회사와 관련된 사례를 관리할 수 있습니다.

사례 관리 기능은 미리 보기로 제공됩니다. 향후 릴리스에서 이 기능을 개선하고 향상된 기능을 추가할 예정입니다. 제품 내 채팅을 통해 의견을 보내주세요.

다음 사항에 유의하십시오.

- 페이지 상단의 사례 관리 대시보드는 두 가지 보기 방식을 제공합니다.
  - 왼쪽 화면에는 사용자께서 제공하신 NSS 계정으로 지난 3개월 동안 접수된 총 사건 수가 표시됩니다.
  - 오른쪽 화면에는 사용자 NSS 계정을 기준으로 회사 차원에서 지난 3개월 동안 접수된 총 사례 수가 표시됩니다.

  표에 표시된 결과는 사용자가 선택한 보기와 관련된 사례를 반영합니다.
- 원하는 열을 추가하거나 제거할 수 있으며, 우선순위 및 상태와 같은 열의 내용을 필터링할 수도 있습니다. 다른 열은 정렬 기능만 제공합니다.

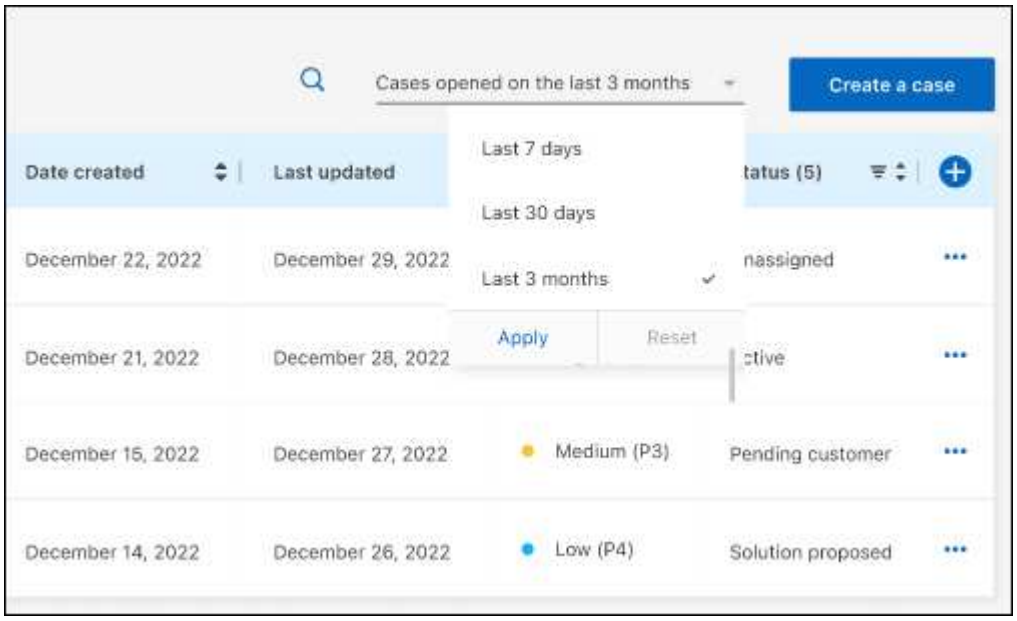
  자세한 내용은 아래 단계를 참조하십시오.
- 개별 케이스별로 케이스 노트를 업데이트하거나, 이미 '종료됨' 또는 '종료 예정' 상태가 아닌 케이스를 종료할 수 있는 기능을 제공합니다.

단계

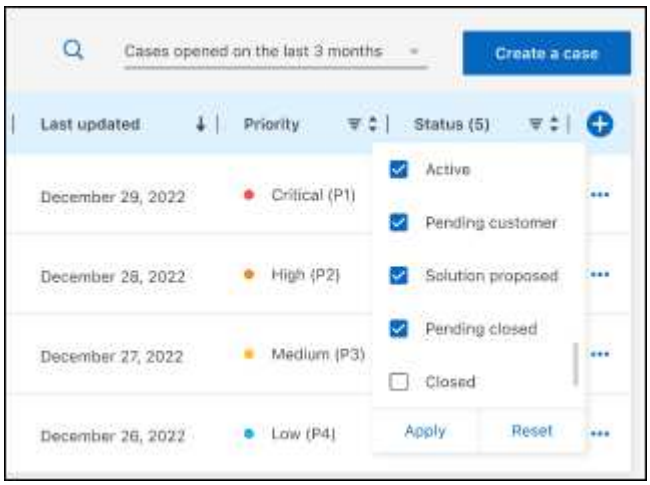
1. Workload Factory 콘솔의 오른쪽 상단에서 *도움말 > 지원*을 선택하십시오.

   이 옵션을 선택하면 NetApp Console이 새 브라우저 탭에서 열리고 지원 대시보드가 로드됩니다.
2. *케이스 관리*를 선택하고, 메시지가 표시되면 NSS 계정을 NetApp Console에 추가하십시오.

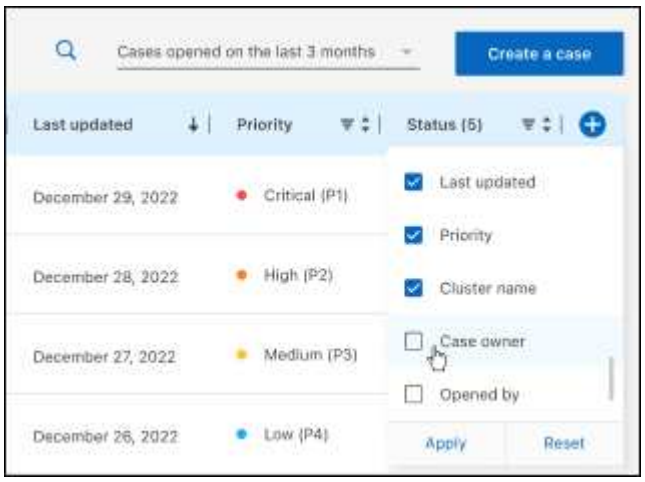
   케이스 관리 페이지에는 NetApp Console 사용자 계정과 연결된 NSS 계정과 관련된 미결 케이스가 표시됩니다. 이 NSS 계정은 **NSS** 관리 페이지 상단에 표시되는 계정과 동일합니다.
3. 표에 표시되는 정보를 선택적으로 수정할 수 있습니다.
   - *조직의 사례*에서 *보기*를 선택하면 회사와 관련된 모든 사례를 볼 수 있습니다.
   - 정확한 날짜 범위를 선택하거나 다른 기간을 선택하여 날짜 범위를 수정하십시오.



◦ 열의 내용을 필터링합니다.



◦ ⊕를 선택한 다음 표시할 열을 선택하여 표에 표시되는 열을 변경합니다.

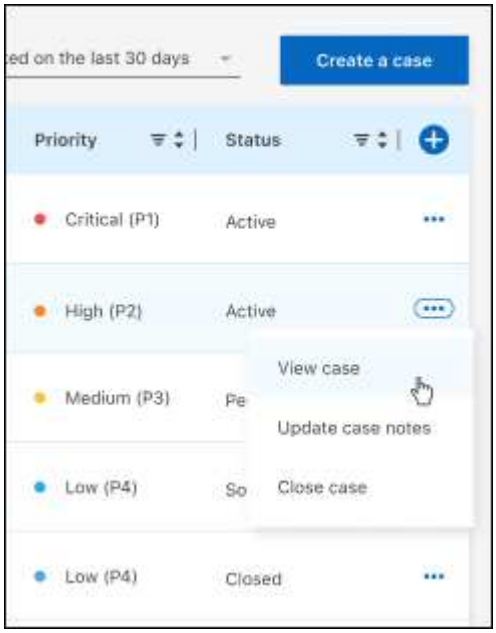


4. •••를 선택하고 사용 가능한 옵션 중 하나를 선택하여 기존 케이스를 관리합니다.

- 케이스 보기: 특정 케이스에 대한 전체 세부 정보를 봅니다.
- 사례 기록 업데이트: 문제에 대한 추가 정보를 입력하거나 *파일 업로드*를 선택하여 최대 5개의 파일을 첨부할 수 있습니다.

  첨부 파일 크기는 파일당 25MB로 제한됩니다. 지원되는 파일 확장자는 txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, csv입니다.

- 케이스 종결: 케이스를 종결하는 이유에 대한 세부 정보를 입력하고 *케이스 종결*을 선택하십시오.



NetApp Workload Factory 관련 법적 고지

법적 고지사항은 저작권 표시, 상표, 특허 등에 대한 접근을 제공합니다.

저작권

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

상표

NETAPP, NETAPP 로고 및 NetApp 상표 페이지에 나열된 마크는 NetApp, Inc.의 상표입니다. 다른 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

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

특허

NetApp이 소유한 특허의 현재 목록은 다음에서 확인할 수 있습니다:

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

개인정보 보호정책

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

오픈 소스

고지 파일에는 NetApp 소프트웨어에 사용된 타사 저작권 및 라이선스에 대한 정보가 포함되어 있습니다.

"NetApp Workload Factory"