아키텍처 및 연결성

Information Security for Workload Factory

NetApp
September 16, 2026

목차

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.

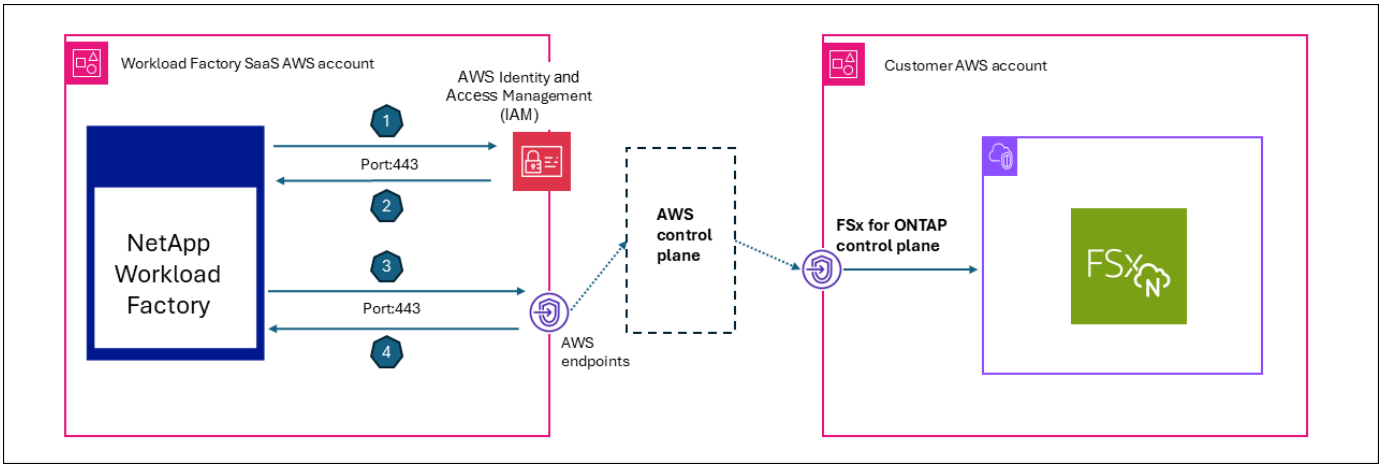
- 수집기 서비스는 약 5시간마다 스캔합니다.
- CRUD 작업은 필요에 따라 실행됩니다.
- 모든 호출은 외부 ID를 사용하는 STS 가정 임시 자격 증명을 사용합니다.

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"