



데이터 거버넌스, 개인정보 보호 및 라이프사이클 Information Security for Workload Factory

NetApp
September 16, 2026

목차

데이터 거버넌스, 개인정보 보호 및 라이프사이클	1
NetApp Workload Factory의 데이터 처리 및 상주	1
Workload Factory에서 처리하는 데이터 클래스	1
Workload Factory에서 유지되는 데이터 클래스	1
정보가 보관되는 위치	1
정보 보관 기간	2
VPC에서 어떤 정보가 유출됩니까?	2
구성 및 메타데이터 수집 범위	3
NetApp Workload Factory용 암호화 및 키 관리	6
FSx용 KMS 저장 데이터 암호화 범위	7
자격 증명 보호(서비스 측 봉투 암호화)	7
NetApp Workload Factory 계정 삭제	8

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 옵션"](#)
- ["NetApp Workload Factory용 AI 톨 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."](#)

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.