Governance dei dati, privacy e ciclo di vita

Information Security for Workload Factory

NetApp
September 16, 2026

Sommario

Governance dei dati, privacy e ciclo di vita

Gestione e residenza dei dati per NetApp Workload Factory

NetApp Workload Factory organizza la gestione dei dati in categorie che descrivono i dati operativi elaborati dal servizio, come ogni classe di dati si inserisce nel modello di sicurezza, dove vengono archiviati i dati, per quanto tempo vengono conservati e se escono dall'ambiente del cliente. Le classi di dati principali includono configurazione e metadati, log ed eventi operativi e telemetria. I dati conservati possono includere snapshot di configurazione di FSx for ONTAP, riferimenti alle credenziali, dati di utilizzo e di costo dell'AI, record di audit e cache di risposta di breve durata. Le posizioni di archiviazione ed elaborazione variano in base al tipo di dati: alcune informazioni rimangono nell'account AWS del cliente, mentre altri dati operativi vengono archiviati nell'account NetApp.

Classi di dati gestite da Workload Factory

Workload Factory gestisce le seguenti classi di dati:

- Configurazione e metadati
- Registri operativi ed eventi
- Telemetria

Classi di dati conservate da Workload Factory

Workload Factory conserva i seguenti dati:

- Snapshot della configurazione di FSx (aggiornati a ogni scansione)
- Riferimenti alle credenziali ONTAP o materiale delle credenziali crittografato con busta di crittografia KMS (a seconda della modalità di credenziali selezionata)
- metriche EDA
- Template CloudFormation (header a 7 giorni `Expires`)
- Dati sull'utilizzo e sui costi dell'intelligenza artificiale
- Registri di controllo
- Cache Redis (risposte FSx) con un TTL di 20 minuti

Dove sono conservate le informazioni

Account AWS

- Le password di amministrazione di ONTAP sono memorizzate in AWS Secrets Manager.
- Amazon Bedrock elabora l'inferenza AI (analisi EMS) utilizzando l'ARN del tuo profilo di inferenza tramite un ruolo assunto da STS all'interno del tuo account AWS.

Account NetApp

- Configurazioni FSx, piani di bilanciamento, configurazioni ARP e limiti di utilizzo dell'AI
- Credenziali AWS STS temporanee (memorizzate nella cache di Redis), cache delle risposte, blocchi e stato di distribuzione
- CloudFormation/Modelli Terraform, descrittori di configurazione WAD e report compressi
- Misurazione dell'utilizzo dell'IA e metriche sulle prestazioni del collector
- metriche aggregate EDA
- Tracce di audit delle azioni
- tracce OpenTelemetry

Considerazioni regionali

- Archiviato nelle regioni in cui è disponibile il servizio Amazon Bedrock.
- NetApp opera internamente in `us-east-1` e `us-west-2`.

Per quanto tempo vengono conservate le informazioni

Questa sezione riassume le categorie di conservazione. Per i valori dettagliati e il comportamento delle policy, consulta le pagine collegate.

- Conservazione delle credenziali e delle credenziali temporanee AWS STS: "Conservazione delle credenziali per NetApp Workload Factory"
- Conservazione delle metriche operative e dei dati di telemetria: "Riferimento a metriche e telemetria per NetApp Workload Factory"
- Conservazione dei record di audit: regolata dalla policy di conservazione della NetApp Console (non controllata da Workload Factory)

Quali informazioni escono dalla VPC

Questa sezione riassume le categorie di dati outbound. Per i dettagli a livello di protocollo e di funzionalità, consulta le pagine collegate.

Traffico del piano di gestione verso il servizio Workload Factory

Per le operazioni di gestione, la configurazione di FSx, i metadati del volume, gli identificatori delle risorse e i comandi operativi fluiscono tramite HTTPS al livello di servizio di Workload Factory.

Registri di controllo al servizio di controllo della NetApp Console

Ogni operazione tracciata invia le seguenti informazioni:

- `accountId`
- `actionName`
- `status`
- `resourceId`
- `userId`

- `requestData`
- `responseData`
- `timestamps`
- `IP address`
- `workspaceId`

Analisi del traffico AI

Gli eventi del sistema di gestione delle emergenze (EMS) di FSx for ONTAP, i dati di latenza e i log degli errori inviati per la diagnostica AI viaggiano verso Amazon Bedrock tramite il tuo account AWS utilizzando il profilo di inferenza configurato, così questo traffico rimane all'interno del tuo ambiente invece di raggiungere i sistemi NetApp.

Per ulteriori informazioni sul traffico di analisi AI, consulta:

- "Panoramica dei controlli AI per NetApp Workload Factory"
- "Bedrock opt-in per la diagnostica AI di NetApp Workload Factory"
- "Limiti degli strumenti di intelligenza artificiale per NetApp Workload Factory"

traffico API del servizio AWS

Fai riferimento a "Connettività e percorsi di fiducia per NetApp Workload Factory".

Raccolta di dati di telemetria e metriche

Fai riferimento a "metriche e telemetria: riferimento".

Ambito di configurazione e raccolta dei metadati

Livello del file system

- Configurazione del file system (tipo di deployment Gen1/Gen2, throughput, capacità di archiviazione, tipo di storage)
- Sottorete preferita, gruppi di sicurezza, configurazione VPC
- Metadati della chiave di crittografia KMS
- Tag del file system
- Stato del ciclo di vita del file system
- Impostazioni finestra di manutenzione

Livello del volume (completo)

- Identità e stato: nome volume, UUID, tipo (rw/dp/ls), stile (FlexVol/FlexGroup), stato (online/offline/limitato), ora di creazione
- Capacità: dimensione totale, utilizzata, disponibile, utilizzata fisicamente, % di utilizzo, impronta SSD, impronta del capacity pool, byte di dati inattivi/%
- Tiering: policy (tutti/auto/nessuno/solo snapshot), giorni minimi di raffreddamento
- QoS: nome della policy QoS assegnata

- Configurazione NAS: percorso di giunzione, assegnazione della policy di esportazione, permessi UNIX, stile di sicurezza (unix/ntfs/mixed)
- Snapshot: dimensione/percentuale/utilizzo della riserva snapshot, impostazioni di autodelete
- Efficienza dei dati: tipo/stato di compressione, deduplicazione, compaction, risparmio di spazio
- Ridimensionamento automatico: modalità (ingrandimento/ingrandimento_riduzione/disattivato), dimensioni min/max, soglie di ingrandimento/riduzione
- SnapLock: tipo (compliance/enterprise/non_snaplock), periodi di conservazione (min/max/predefinito), periodo di autocommit
- Clona: volume d'origine/snapshot/storage VM, è FlexClone, stato di split
- Inode/file: massimo possibile, massimo configurato, numero utilizzato
- Crittografia: stato abilitato/disabilitato
- Tempo di accesso: aggiornamento atime abilitato/disabilitato e periodo di aggiornamento
- SnapMirror: stato di protezione, tipi di destinazione (cloud/ONTAP)
- FlexGroup ribilanciamento: percentuale di squilibrio, soglia massima
- Movimento volume: aggregato di destinazione, stato del movimento
- FlexCache endpoint tipo: nessuno/cache/origine
- Tag: tag di volume a livello ONTAP

Dati Snapshot

- Nome Snapshot, UUID, ora di creazione, ora di scadenza
- Dimensione in byte
- etichetta SnapMirror
- Stato di scadenza e di blocco di SnapLock
- Stato (valido/non valido/parziale)
- Commenti degli utenti
- Criteri di snapshot: nome, stato di attivazione, pianificazione delle copie (conteggio, periodo di conservazione, nome della pianificazione, prefisso, SnapMirror label)

Politiche di esportazione

- Nome policy, ID, storage VM associata
- Regole: elenco protocolli (NFS/CIFS/FlexCache), modelli di corrispondenza client, regole di sola lettura, regole di lettura/scrittura, regole superutente, indice/priorità delle regole
- SUID, creazione del dispositivo, modalità chown, mappatura utente anonimo, impostazioni di sicurezza NTFS UNIX

Punti di accesso S3

- Stato del ciclo di vita (disponibile/creazione/eliminazione/non riuscito/configurato in modo errato)
- Ora di creazione, ARN, alias, nome
- Proprietario del file, utente e tipo (UNIX/WINDOWS)
- Configurazione di rete (accesso Internet vs VPC, ID VPC)

- Tag AWS
- Abilitazione della scansione dei metadati, abilitazione del journaling, CloudTrail ARN

Protezione anti-ransomware (ARP)

Workload Factory raccoglie sia lo stato di configurazione che i dettagli degli eventi:

- Stato per volume (abilitato/disabilitato/dry_run/in pausa)
- Probabilità di attacco (nessuna/bassa/moderata/alta)
- Rapporti di attacco con timestamp
- Parametri di rilevamento: soglie di estensione dei file, aumento % del tasso di ridenominazione, aumento % del tasso di entropia, aumento % del tasso di creazione/eliminazione dei file
- File sospetti: percorso del file, nome del file, formato del file, ora del sospetto, volume associato

Replica / SnapMirror

- UUID relazione, stato, stato di salute
- Origine e destinazione (storage VM, percorso, cluster)
- Statistiche di trasferimento (byte trasferiti, durata, ora di fine, stato)
- Policy (nome, tipo: asincrona/sincrona/continua)
- Impostazione del throttle
- tempo di latenza
- Motivi di non integrità (messaggio e codice)
- Errori di trasferimento attuali

iGroups

- Nome, UUID, protocollo (FCP/iSCSI/misto), tipo di sistema operativo
- Iniziatori (IQN/WWPN), stato di connettività, ultima volta visto
- Mappature LUN (logical unit number, dettagli LUN)

LUN

- Nome, UUID, numero di serie, tipo di sistema operativo, stato abilitato
- Dimensioni, spazio utilizzato, impostazioni di thin provisioning
- Posizione (volume, nodo, percorso dell’unità logica)
- Impostazione di eliminazione automatica
- Stato del container, stato mappato, stato di sola lettura
- Policy QoS
- Metriche delle prestazioni (IOPS, latenza, throughput per lettura/scrittura/totale)
- Appartenenza al gruppo di coerenza

FlexCache

- Volume d'origine/VM di storage/cluster, dimensione della cache, percorso
- Scrittura abilitata, stato della cache DR
- Configurazione dimensionale relativa
- Precompila i percorsi delle directory
- Stato della connessione tra cache e origine

Livello Storage VM

- Nome, UUID, stato (in esecuzione/arrestato), sottotipo
- Protocolli abilitati/consentiti (NFS, CIFS, iSCSI, FCP, NVMe, S3)
- Server DNS e domini
- Configurazione dello switch dei servizi dei nomi (passwd, group, hosts, ecc.)
- Interfacce IP (nome, indirizzo IP, servizi)
- Aggregati assegnati
- Stato predefinito del volume anti-ransomware
- Impostazioni di applicazione dello spazio
- Relazioni tra pari (applicazioni, stato, cluster/VM di storage remoti)

Livello aggregato/di storage

- Nome aggregato, UUID, stato, stato RAID
- Archiviazione a blocchi: numero di dischi, dimensione RAID, spazio disponibile/utilizzato/totale, spazio fisico utilizzato
- Archiviazione cloud utilizzata
- Efficienza: rapporto, logico utilizzato, risparmi
- Crittografia, mirror, impostazioni SnapLock
- metriche delle prestazioni (IOPS, latenza, throughput)

Metriche di utilizzo (EDA)

- Frequenza di raccolta: ogni 12 ore per capacità/throughput; ogni 20 minuti per latenza
- Granularità: normalizzata a circa 60 punti dati per intervallo di tempo
- Dettagli relativi alla conservazione e all'archiviazione: "Riferimento a metriche e telemetria"

Crittografia e gestione delle chiavi per NetApp Workload Factory

NetApp Workload Factory utilizza la crittografia dei dati a riposo e definisce chiare responsabilità di gestione delle chiavi tra Workload Factory e i servizi AWS. Per i file system Amazon FSx for NetApp ONTAP, puoi scegliere la tua chiave AWS KMS oppure usare la chiave predefinita gestita da AWS, e FSx for ONTAP esegue le operazioni

crittografiche con quella chiave. Workload Factory utilizza anche la crittografia a busta per proteggere le credenziali ONTAP memorizzate.

Ambito di crittografia a riposo KMS per FSx

Quando crei un file system FSx for ONTAP tramite Workload Factory, puoi opzionalmente specificare la tua chiave AWS KMS per la crittografia dei dati a riposo. Se non specifichi una chiave, Workload Factory usa la chiave FSx predefinita gestita da AWS.

Cosa è crittografato

Tutti i dati memorizzati sui volumi EBS sottostanti che supportano il file system FSx for ONTAP (crittografia AWS FSx a riposo).

Proprietà della chiave

La chiave KMS risiede nel tuo account AWS.

Autorizzazioni necessarie per la selezione e l'utilizzo della chiave

Workload Factory richiede:

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant` (per consentire al servizio FSx for ONTAP di utilizzare la chiave)

Schema di accesso chiave

Workload Factory non crittografa né decrittografa mai direttamente i dati con la tua chiave KMS. Passa l'ID della chiave all'API di Amazon FSx for NetApp ONTAP durante la creazione del file system; Amazon FSx for NetApp ONTAP esegue le operazioni crittografiche.

Protezione delle credenziali (crittografia dell'envelope lato servizio)

Quando memorizzi le credenziali ONTAP (password di amministratore) tramite Workload Factory, vengono protette utilizzando la crittografia a busta prima di essere salvate.

Metodo di crittografia

AES-256-CBC con una chiave di crittografia dei dati (DEK) univoca per ogni record di credenziali.

Flusso di crittografia della busta

1. Per ogni credenziale viene generato un DEK univoco a 256 bit.
2. Il DEK crittografa la credenziale (password).
3. Il DEK stesso è crittografato con una chiave root e memorizzato insieme alla credenziale crittografata.
4. Il testo in chiaro DEK non viene mai memorizzato.

Contesto di crittografia

Ogni chiave dati è crittograficamente associata al suo specifico record di credenziali, impedendo il riutilizzo della chiave tra record.

Alternativa: AWS Secrets Manager

Anziché memorizzare le password crittografate nel servizio, puoi archiviare le credenziali ONTAP in AWS

Secrets Manager nel tuo account. Workload Factory non vede né memorizza mai la password; passa l'ARN di Secrets Manager al collegamento Lambda, che recupera la password durante l'esecuzione all'interno della tua VPC.

AWS Secrets Manager è necessario per gli account GovCloud.

NetApp Workload Factory eliminazione account

L'eliminazione dell'account non è un'operazione self-service; si tratta di un flusso di lavoro di dismissione che coinvolge sia il servizio Workload Factory sia le risorse presenti nel tuo account AWS. La pulizia include la rimozione sicura di tutti i dati associati all'account Workload Factory, ai file system FSx for ONTAP, alle credenziali, ai collegamenti, ai canali di notifica e alle relative risorse IAM, AWS Lambda e Amazon CloudWatch. L'operazione è irreversibile.

Quando devi rimuovere il tuo account Workload Factory, devi "Contatta l'assistenza NetApp."

Informazioni sul copyright

Informazioni sul marchio commerciale