Gouvernance des données, confidentialité et cycle de vie

Information Security for Workload Factory

NetApp
September 16, 2026

Sommaire

Gouvernance des données, confidentialité et cycle de vie

Gestion et résidence des données pour NetApp Workload Factory

NetApp Workload Factory organise la gestion des données en catégories qui décrivent les données opérationnelles traitées par le service, la manière dont chaque classe de données s'intègre au modèle de sécurité, l'emplacement de stockage des données, la durée de leur conservation et si elles quittent ou non l'environnement client. Les principales classes de données comprennent la configuration et les métadonnées, les journaux et événements opérationnels, ainsi que la télémétrie. Les données conservées peuvent inclure des instantanés de configuration FSx for ONTAP, des références d'identifiant, des données d'utilisation et de coût de l'IA, des enregistrements d'audit et des caches de réponses temporaires. Les emplacements de stockage et de traitement varient selon le type de données : certaines informations restent dans le compte AWS du client, tandis que d'autres données opérationnelles sont stockées dans le compte NetApp.

Classes de données gérées par NetApp Workload Factory

Workload Factory gère les classes de données suivantes :

- Configuration et métadonnées
- Journaux et événements opérationnels
- Télémétrie

Classes de données conservées par Workload Factory

Workload Factory conserve les données suivantes :

- Instantanés de configuration FSx (actualisés à chaque analyse)
- Références d'identifiants ONTAP, ou éléments d'identifiants chiffrés avec le chiffrement par enveloppe KMS (selon le mode d'identifiant sélectionné)
- Métriques EDA
- Modèles CloudFormation (en-tête de 7 jours `Expires`)
- données sur l'utilisation et le coût de l'IA
- Registres d'audit
- Caches Redis (réponses FSx) avec un TTL de 20 minutes

Où les informations sont conservées

Compte AWS

- Les mots de passe d'administrateur ONTAP sont stockés dans votre AWS Secrets Manager.
- Amazon Bedrock traite l'inférence IA (analyse EMS) en utilisant votre ARN de profil d'inférence via un rôle STS assumé au sein de votre compte AWS.

Compte NetApp

- Configurations FSx, plans d'équilibrage, configurations ARP et limites d'utilisation de l'IA
- Identifiants AWS STS temporaires (mis en cache dans Redis), caches de réponses, verrous et état de déploiement
- CloudFormation/Modèles Terraform, descripteurs de configuration WAD et rapports compressés
- Mesure de l'utilisation de l'IA et indicateurs de performance des collecteurs
- Métriques agrégées EDA
- Pistes d'audit des actions
- traces OpenTelemetry

Considérations régionales

- Stocké dans les régions où le service Amazon Bedrock est disponible.
- NetApp internal fonctionne dans `us-east-1` et `us-west-2`.

Durée de conservation des informations

Cette section résume les catégories de rétention. Consultez les pages liées pour connaître les valeurs détaillées et le comportement des politiques.

- Conservation des identifiants et des identifiants temporaires AWS STS :"Conservation des identifiants pour NetApp Workload Factory"
- Conservation des indicateurs opérationnels et des données de télémétrie : "Référence des métriques et de la télémétrie pour NetApp Workload Factory"
- Conservation des enregistrements d'audit : régie par la politique de conservation de la NetApp Console (non contrôlée par NetApp Workload Factory)

Quelles informations quittent le VPC

Cette section récapitule les catégories de données sortantes. Consultez les pages liées pour obtenir des informations détaillées au niveau du protocole et des fonctionnalités.

Trafic du plan de gestion vers le service Workload Factory

Pour les opérations de gestion, la configuration FSx, les métadonnées des volumes, les identifiants de ressources et les commandes opérationnelles transitent via HTTPS vers le niveau de service NetApp Workload Factory.

Enregistrements d'audit vers le service d'audit de la NetApp Console

Chaque opération suivie envoie les informations suivantes :

- `accountId`
- `actionName`
- `status`
- `resourceId`
- `userId`
- `requestData`
- `responseData`
- `timestamps`
- `IP address`
- `workspaceId`

trafic d'analyse IA

Les événements du système de gestion des urgences (EMS) FSx for ONTAP, les données de latence et les journaux d'erreurs soumis pour les diagnostics d'IA transitent par Amazon Bedrock via votre compte AWS en utilisant votre profil d'inférence configuré, de sorte que ce trafic reste dans votre environnement plutôt que d'atteindre les systèmes NetApp.

Pour plus d'informations sur le trafic d'analyse de l'IA, consultez :

- "Aperçu des contrôles d'IA pour NetApp Workload Factory"
- "Activation de Bedrock pour les diagnostics IA de NetApp Workload Factory"
- "Limites des outils d'IA pour NetApp Workload Factory"

trafic de l'API du service AWS

Consultez "connectivité et chemins de confiance pour NetApp Workload Factory".

Collecte de données télémétriques et de métriques

Consultez le "référence des métriques et de la télémétrie".

Étendue de la configuration et de la collecte des métadonnées

Niveau du système de fichiers

- Configuration du système de fichiers (type de déploiement Gen1/Gen2, capacité de débit, capacité de stockage, type de stockage)
- Sous-réseau préféré, groupes de sécurité, configuration VPC
- Métadonnées de la clé de chiffrement KMS
- Étiquettes du système de fichiers
- Statut du cycle de vie du système de fichiers
- Paramètres de la fenêtre de maintenance

Niveau de volume (complet)

- Identité et état : nom du volume, UUID, type (rw/dp/ls), style (FlexVol®/FlexGroup), état (en ligne/hors ligne/restreint), heure de création
- Capacité : taille totale, utilisée, disponible, physique utilisée, pourcentage utilisé, encombrement SSD, encombrement du pool de capacité, octets de données inactifs/pourcentage
- Classification par niveaux : politique (all/auto/none/snapshot_only), nombre minimum de jours de refroidissement
- QoS : nom de la règle QoS attribuée
- Configuration du NAS : chemin de jonction, règles d'export, autorisations UNIX, style de sécurité (unix/ntfs/mixte)
- Instantanés : taille/pourcentage/utilisation de la réserve d'instantanés, paramètres de suppression automatique
- Efficacité des données : type/état de compression, déduplication, compactage, économies d'espace
- Dimensionnement automatique : mode (agrandir/agrandir_réduire/désactivé), taille min/max, seuils d'agrandissement/réduction
- SnapLock : type (compliance/enterprise/non_snaplock), périodes de rétention (min/max/par défaut), période de validation automatique
- Clonage : volume parent/instantané/VM de stockage, est FlexClone, état de fractionnement
- Inodes/fichiers : nombre maximal possible, nombre maximal configuré, nombre utilisé
- Chiffrement : état activé/désactivé
- Heure d'accès : mise à jour atime activée/désactivée et période de mise à jour
- SnapMirror : état de protection, types de destination (cloud/ONTAP)
- FlexGroup rééquilibrage : pourcentage de déséquilibre, seuil maximal
- Mouvement de volume : agrégat de destination, état du mouvement
- Type d'extrémité FlexCache® : none/cache/origin
- Étiquettes : étiquettes de volume au niveau ONTAP

Données Snapshot

- Nom de l'instantané, UUID, heure de création, heure d'expiration
- Taille en octets
- SnapMirror étiquette
- SnapLock état d'expiration et de verrouillage
- État (valide/invalide/partiel)
- Commentaires des utilisateurs
- Politiques d'instantané : nom, état activé, planification des copies (nombre, période de conservation, nom de la planification, préfixe, SnapMirror label)

Politiques d'export

- Nom de la stratégie, ID, machine virtuelle de stockage associée
- Règles : liste de protocoles (NFS/CIFS/FlexCache®), critères de correspondance client, règles de lecture

seule, règles de lecture/écriture, règles de superutilisateur, index/priorité de règle

- SUID, création de périphérique, mode chown, mappage d'utilisateur anonyme, paramètres de sécurité NTFS UNIX

Points d'accès S3

- État du cycle de vie (disponible/en cours de création/en cours de suppression/échec/mauvaise configuration)
- Date de création, ARN, alias, nom
- Utilisateur propriétaire des fichiers et type (UNIX/WINDOWS)
- Configuration réseau (accès Internet vs accès VPC, ID VPC)
- Balises AWS
- Activation de l'analyse des métadonnées, activation de la journalisation, CloudTrail ARN

Protection anti-ransomware (ARP)

Workload Factory collecte à la fois l'état de la configuration et les détails des événements :

- État par volume (activé/désactivé/test à blanc/en pause)
- Probabilité d'attaque (nulle/faible/modérée/élevée)
- Rapports d'attaque avec horodatage
- Paramètres de détection : seuils d'extension de fichier, augmentation du taux de renommage (%), augmentation du taux d'entropie (%), augmentation du taux de création/suppression de fichiers (%)
- Fichiers suspects : chemin d'accès du fichier, nom du fichier, format du fichier, heure suspecte, volume associé

Réplication / SnapMirror

- UUID de relation, état, état de santé
- Source et destination (machine virtuelle de stockage, chemin, cluster)
- Statistiques de transfert (octets transférés, durée, heure de fin, état)
- Politique (nom, type : asynchrone/synchrone/continu)
- Réglage du débit
- Temps de latence
- Raisons d'état non sain (message et code)
- Erreurs de transfert actuelles

iGroups

- Nom, UUID, protocole (FCP/iSCSI/mixte), type de système d'exploitation
- Initiateurs (IQN/WWPN), état de connectivité, dernière heure de détection
- Mappages LUN (numéro d'unité logique, détails du LUN)

LUN

- Nom, UUID, numéro de série, type de système d'exploitation, état d'activation
- Taille, espace utilisé, paramètres de provisionnement fin
- Emplacement (volume, nœud, chemin d'unité logique)
- Paramètre de suppression automatique
- État du conteneur, statut mappé, statut en lecture seule
- politique QoS
- Indicateurs de performance (IOPS, latence, débit par lecture/écriture/total)
- Adhésion au groupe de cohérence

FlexCache®

- Volume d'origine/VM de stockage/cluster, taille du cache, chemin
- Écriture différée activée, état du cache DR
- Configuration de dimensionnement relatif
- Préremplir les chemins de répertoire
- État de la connexion entre le cache et l'origine

Niveau de la machine virtuelle de stockage

- Nom, UUID, état (en cours d'exécution/arrêté), sous-type
- Protocoles activés/autorisés (NFS, CIFS, iSCSI, FCP, NVMe, S3)
- Serveurs DNS et domaines
- Configuration du commutateur de service de noms (passwd, group, hosts, etc.)
- Interfaces IP (nom, adresse IP, services)
- Agrégats affectés
- État du volume anti-ransomware par défaut
- Paramètres d'application de l'espace
- Relations entre pairs (applications, état, cluster distant/storage VM)

Niveau agrégat / stockage

- Nom de l'agrégat, UUID, état, état RAID
- Stockage par blocs : nombre de disques, taille RAID, espace disponible/utilisé/total, espace physique utilisé
- Stockage cloud utilisé
- Efficacité : ratio, utilisé logiquement, économies
- Chiffrement, miroir, paramètres SnapLock
- Métriques de performance (IOPS, latence, débit)

Métriques d'utilisation (EDA)

- Fréquence de collecte : toutes les 12 heures pour la capacité/le débit ; toutes les 20 minutes pour la latence
- Granularité : normalisée à environ 60 points de données par intervalle de temps
- Détails relatifs à la conservation et au stockage : "Référence des métriques et de la télémétrie"

Chiffrement et gestion des clés pour NetApp Workload Factory

NetApp Workload Factory utilise le chiffrement au repos et définit clairement les responsabilités de gestion des clés entre Workload Factory et les services AWS. Pour les systèmes de fichiers Amazon FSx for NetApp ONTAP, vous pouvez choisir votre propre clé AWS KMS ou utiliser la clé par défaut gérée par AWS, et FSx for ONTAP effectue les opérations cryptographiques avec cette clé. Workload Factory utilise également le chiffrement enveloppe pour protéger les identifiants ONTAP stockés.

Étendue du chiffrement au repos KMS pour FSx

Lors de la création d'un système de fichiers FSx for ONTAP via Workload Factory, vous pouvez éventuellement spécifier votre propre clé AWS KMS pour le chiffrement des données au repos. Si vous ne spécifiez pas de clé, Workload Factory utilise la clé FSx par défaut gérée par AWS.

Ce qui est chiffré

Toutes les données stockées sur les volumes EBS sous-jacents qui prennent en charge le système de fichiers FSx for ONTAP (chiffrement AWS FSx au repos).

Propriété de la clé

La clé KMS se trouve dans votre compte AWS.

Autorisations requises pour la sélection et l'utilisation des clés

Workload Factory nécessite :

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant` (pour permettre au service FSx for ONTAP d'utiliser la clé)

Modèle d'accès par clé

Workload Factory ne chiffre ni ne déchiffre directement les données avec votre clé KMS. Il transmet l'identifiant de la clé à l'API Amazon FSx for NetApp ONTAP lors de la création du système de fichiers ; Amazon FSx for NetApp ONTAP effectue les opérations cryptographiques.

Protection des identifiants (chiffrement enveloppe côté service)

Lorsque vous stockez des identifiants ONTAP (mots de passe administrateur) via Workload Factory, ils sont protégés à l'aide du chiffrement par enveloppe avant d'être enregistrés.

Méthode de chiffrement

AES-256-CBC avec une clé de chiffrement (DEK) unique par enregistrement d'identifiant.

Flux de chiffrement d'enveloppe

1. Une clé DEK unique de 256 bits est générée par identifiant.
2. Le DEK chiffre l'identifiant (mot de passe).
3. Le DEK lui-même est chiffré avec une clé racine et stocké avec l'identifiant chiffré.
4. Le DEK en clair n'est jamais stocké.

Contexte de chiffrement

Chaque clé de données est liée cryptographiquement à son identifiant spécifique, empêchant la réutilisation de la clé entre les enregistrements.

Alternative : AWS Secrets Manager

Au lieu de stocker les mots de passe chiffrés dans le service, vous pouvez stocker les identifiants ONTAP dans AWS Secrets Manager dans votre propre compte. Workload Factory ne voit ni ne stocke jamais le mot de passe ; il transmet l'ARN de Secrets Manager à Lambda link, qui récupère le mot de passe lors de l'exécution au sein de votre VPC.

AWS Secrets Manager est requis pour les comptes GovCloud.

NetApp Workload Factory suppression de compte

La suppression d'un compte n'est pas une opération en libre-service ; il s'agit d'un processus de désactivation qui concerne à la fois le service Workload Factory et les ressources de votre compte AWS. Le nettoyage comprend la suppression sécurisée de toutes les données associées au compte Workload Factory, aux systèmes de fichiers FSx for ONTAP, aux identifiants, aux liens, aux canaux de notification et aux ressources IAM, AWS Lambda et Amazon CloudWatch associées. Cette opération est irréversible.

Lorsque vous devez supprimer votre compte Workload Factory, vous devez "contactez le support NetApp."