Identité, identifiants et principe du moindre privilège

Information Security for Workload Factory

NetApp
September 16, 2026

Sommaire

Identité, identifiants et principe du moindre privilège

Intégration de compte AWS pour NetApp Workload Factory

Workload Factory utilise AWS `sts:AssumeRole` pour obtenir des identifiants temporaires pour votre compte AWS, de sorte que les clés d'accès AWS à long terme ne sont pas stockées par le service. Lors de l'intégration, vous configurez un rôle IAM que Workload Factory peut assumer pour les opérations d'API AWS approuvées, en utilisant un ID externe afin d'aider à prévenir tout accès inter-comptes non autorisé. Workload Factory utilise ensuite les identifiants temporaires générés lors de l'exécution, qu'AWS expire automatiquement à la fin de chaque session.

Configuration du compte AWS

Pour permettre à Workload Factory d'accéder à votre compte AWS :

1. Déployez un rôle IAM dans votre compte AWS (en utilisant CloudFormation ou manuellement).
2. Assurez-vous que la politique d'approbation des rôles permette au principal de service de Workload Factory de l'assumer, sous condition d'un ID externe.
3. Utilisez un identifiant externe comme identifiant secret unique (UUID v4) partagé exclusivement entre le client et Workload Factory.

   Intégrez-le comme condition dans votre politique d'approbation de rôle IAM (`sts:ExternalId`).

   L'identifiant externe empêche les attaques par usurpation d'identité. Dans un modèle d'accès inter-comptes, un attaquant qui découvre l'ARN du rôle d'un client ne peut pas assumer ce rôle sans posséder également l'identifiant externe correspondant. AWS recommande ce modèle pour l'accès inter-comptes par des tiers. Pour plus d'informations, consultez la page de documentation AWS IAM "Accès aux comptes AWS appartenant à des tiers".

   L'identifiant externe est généré une seule fois lors de l'intégration des identifiants et est stocké de manière chiffrée avec l'ARN du rôle dans une base de données Workload Factory.
4. Enregistrez l'ARN du rôle et l'ID externe dans Workload Factory.

Durée d'exécution

Lors de l'exécution, Workload Factory assume votre rôle IAM pour obtenir des identifiants temporaires pour chaque opération d'API AWS :

1. Workload Factory effectue des appels `sts:AssumeRole` avec l'ARN de votre rôle et l'ID externe.
2. AWS renvoie des identifiants temporaires (clé d'accès, clé secrète et jeton de session).
3. Workload Factory utilise les identifiants temporaires pour les opérations d'API AWS dans votre compte.
4. Les identifiants expirent automatiquement (par défaut, une heure).

Comment les identifiants AWS transitent par NetApp Workload Factory

Le flux d'identifiants AWS décrit comment NetApp Workload Factory gère les identifiants de rôle, les ID externes et les identifiants AWS STS temporaires lors de l'intégration et des opérations d'exécution. Lors de la configuration initiale, vous créez un rôle IAM dans votre compte AWS et configurez une stratégie d'approbation qui exige le principal de service Workload Factory et l'ID externe approprié. Lors de l'exécution, Workload Factory utilise l'ARN du rôle et l'ID externe stockés pour demander des identifiants temporaires limités par une stratégie de session par requête, et réutilise les identifiants mis en cache jusqu'à leur expiration.

Configuration unique

Pour une configuration unique, le processus est le suivant :

Étapes

1. Vous lancez une pile CloudFormation ou créez manuellement un rôle IAM dans votre compte AWS.
2. La politique d'approbation du rôle IAM spécifie deux conditions :
   a. Seul le principal de service de Workload Factory peut l'assumer.
   b. L'appelant doit présenter l'identifiant externe correct.
3. Workload Factory stocke l'ARN du rôle et l'ID externe (chiffrés) dans sa base de données.

Exécution (chaque opération API)

Lors de l'exécution, Workload Factory utilise l'ARN du rôle enregistré et l'ID externe pour obtenir des identifiants AWS STS temporaires pour chaque opération d'API. Le flux est le suivant :

Étapes

1. Workload Factory récupère l'ARN du rôle stocké et l'ID externe depuis MySQL.
2. Il vérifie dans Redis la présence d'un ensemble mis en cache d'identifiants AWS STS temporaires pour ce rôle.
3. En cas d'absence de données dans le cache, Workload Factory effectue un appel `sts:AssumeRole` avec l'ARN du rôle et l'ID externe. Cet appel inclut une stratégie de session intégrée par requête qui limite les autorisations aux seules actions AWS nécessaires pour cette opération.
4. AWS STS renvoie des identifiants temporaires (ID de clé d'accès, clé d'accès secrète, jeton de session) avec un horodatage d'expiration.
5. Workload Factory met ces identifiants en cache dans Redis et les utilise pour appeler les API AWS cibles.
6. En cas d'accès au cache, NetApp Workload Factory ignore l'appel STS et utilise directement les identifiants mis en cache.

Politique de session

Chaque appel STS inclut une politique de session intégrée limitée aux actions AWS minimales requises.

Informations connexes

- "Niveaux d'autorisation de privilège minimal"

Rétention des identifiants AWS pour NetApp Workload Factory

Workload Factory sécurise la gestion des identifiants grâce à des identifiants AWS STS à courte durée de vie, des métadonnées de rôle chiffrées et un comportement de rétention limité. Le modèle d'identifiants sépare les métadonnées de rôle conservées des identifiants AWS temporaires utilisés pour les opérations d'API. Les identifiants temporaires sont mis en cache uniquement pour une période limitée et expirent automatiquement sous l'application des règles AWS. La suppression d'un identifiant empêche Workload Factory d'obtenir de nouveaux identifiants pour le compte, tandis que les identifiants mis en cache expirent peu après.

Comportements clés

- Workload Factory ne stocke pas les clés d'accès AWS à long terme.

  Workload Factory ne stocke qu'un pointeur (ARN du rôle) et un secret partagé (identifiant externe). Aucun des deux ne permet d'accorder l'accès à AWS de manière autonome.

- Les identifiants AWS STS temporaires ont une durée de vie maximale stricte d'une heure (imposée par AWS).

  Workload Factory les met en cache dans Redis pendant 30 minutes maximum avant de forcer un nouvel appel STS.

- Si un ensemble d'identifiants mis en cache a une durée de vie restante inférieure à 15 minutes, Workload Factory le supprime et en obtient un nouveau.
- La suppression des identifiants par le client révoque immédiatement la possibilité pour Workload Factory d'accéder à ce compte.

  Le prochain appel AssumeRole échoue, et les identifiants mis en cache expirent dans les minutes qui suivent.

Résumé de la conservation et du stockage

Données	Lieu de stockage	Durée de rétention	Expiration automatique ?	Méthode de suppression
ARN du rôle IAM + ID externe	MySQL (chiffré au repos)	Indéfinie (conservée jusqu'à ce que le client la supprime explicitement)	Non	Le client clique sur « Supprimer identifiant » dans l'interface utilisateur

Données	Lieu de stockage	Durée de rétention	Expiration automatique ?	Méthode de suppression
Identifiants AWS STS temporaires (clé d'accès + secret + jeton de session)	Redis (cache en mémoire)	Maximum 30 minutes (TTL du cache). Les identifiants STS sous-jacents sont valides jusqu'à une heure (valeur par défaut AWS). Le cache est évincé cinq minutes avant l'expiration par mesure de sécurité.	Oui (Redis supprime automatiquement selon le TTL ; l'expiration des identifiants AWS est appliquée par AWS)	Automatique
Mot de passe administrateur ONTAP	MySQL (chiffrement enveloppe AES-256-CBC utilisant KMS)	Indéfinie (conservée jusqu'à ce que le client supprime l'identifiant ou supprime le système de fichiers)	Non	Le client supprime l'identifiant, ou la suppression du système de fichiers déclenche un nettoyage
Mot de passe ONTAP déchiffré (texte en clair)	En mémoire uniquement (jamais écrit sur disque ni en cache)	Durée d'une requête unique (millisecondes)	Oui (collecté par le ramasse-miettes après la fin de la requête)	Automatique

Contrôles de sécurité

- L'identifiant externe empêche les attaques de type « confused deputy ».
- Les politiques de session appliquent le principe du moindre privilège par requête.
- Workload Factory actualise les identifiants AWS STS temporaires de courte durée avant les périodes d'expiration à risque.
- La gestion régionale et du type de compte diffère pour les environnements Standard, GovCloud et Chine.
- Workload Factory ne stocke jamais les clés d'accès AWS à long terme.
- Workload Factory ne modifie jamais les autorisations de votre rôle IAM.
- Workload Factory ne dépasse jamais les autorisations accordées par votre politique de rôle.
- Les politiques de session peuvent uniquement réduire les autorisations ; Workload Factory ne les étend jamais.

Types d’identifiants pour NetApp Workload Factory

NetAppWorkload Factory utilise un modèle d’identifiants séparés pour dissocier les autorisations du plan de contrôle AWS de l’accès administratif direct à ONTAP. Le rôle AWS IAM authentifie Workload Factory auprès des API AWS pour des opérations telles que la gestion du système de fichiers, la gestion des sauvegardes et la découverte des ressources. Les identifiants ONTAP authentifient l’accès direct au point de gestion ONTAP avec un lien Lambda pour les opérations nécessitant une configuration administrative ou des diagnostics. Certains workflows requièrent les deux types d’identifiants lorsqu’ils combinent des opérations sur les API AWS avec des tâches de gestion directe d’ONTAP.

Types d’identifiants

Le tableau suivant récapitule les deux types d’identifiants utilisés dans Workload Factory et leurs cibles d’authentification respectives.

Type d’identifiant	S’authentifie auprès de	Utilisé pour
Identifiants AWS (AssumeRole)	API AWS	Toutes les opérations qui transitent par l’API du service AWS FSx
Identifiants ONTAP (mot de passe administrateur)	Point de terminaison de gestion ONTAP	Opérations nécessitant un accès direct à l’API REST ONTAP ou à l’interface de ligne de commande (CLI) ONTAP

Opérations AWS nécessitant uniquement un identifiant

Ces opérations interagissent exclusivement avec les API AWS et ne nécessitent que le rôle IAM :

- Création et suppression de système de fichiers
- Modifications de la capacité et du débit du système de fichiers
- Création et gestion des sauvegardes
- Découverte des VPC, des sous-réseaux et des groupes de sécurité
- énumération des clés KMS
- CloudWatch récupération des métriques
- Requêtes de Cost Explorer
- Gestion des balises à l’aide de l’API FSx

Opérations nécessitant uniquement des identifiants ONTAP

Ces opérations communiquent directement avec le point de terminaison de gestion ONTAP via le lien Lambda et nécessitent des identifiants d’administrateur ONTAP :

- Configuration de la politique QoS au niveau du volume
- Gestion des règles d’export
- Configuration du protocole de la machine virtuelle de stockage (NFS, CIFS, iSCSI)

- gestion des igroup et des LUN
- SnapMirror (réplication) configuration
- Gestion des politiques d'instantané (niveau ONTAP)
- Diagnostic des performances (statistiques QoS, analyse de la latence)
- Récupération et analyse des événements EMS
- Surveillance de l'état de la protection anti-ransomware
- Gestion de FlexCache®
- Requêtes d'interface réseau (LIF)

Opérations nécessitant à la fois des identifiants AWS et ONTAP

Flux de travail	identifiant AWS utilisé pour	Identifiant ONTAP utilisé pour
Analyse d'événements basée sur l'IA	Invoquer Bedrock, décrire le système de fichiers	Récupérez les événements EMS, exécutez des diagnostics via SSH
Création du système de fichiers avec configuration de la machine virtuelle de stockage	Créer un système de fichiers (API AWS)	Configurer les protocoles de la machine virtuelle de stockage (ONTAP REST)
Création de volume avec règles d'export	Créer un volume (API AWS)	Définir les règles d'export (ONTAP REST)
gestion de la capacité	Mettre à jour la capacité du système de fichiers (API AWS)	Vérifier l'utilisation de l'agrégat (ONTAP SSH)

Informations connexes

- "Options d'exécution ONTAP"
- "Aperçu du lien Lambda"

Options de stockage des identifiants pour NetApp Workload Factory

NetApp Workload Factory prend en charge des modèles de gestion des identifiants qui préservent le principe du moindre privilège et réduisent l'exposition des secrets d'administration ONTAP. Les fonctionnalités de diagnostic alimentées par l'IA utilisent des identifiants ONTAP en lecture seule lorsqu'ils sont disponibles, afin que l'agent de diagnostic puisse observer et diagnostiquer sans modifier l'environnement de stockage. Vous pouvez utiliser le stockage chiffré géré par Workload Factory ou stocker le mot de passe ONTAP dans AWS Secrets Manager et fournir une référence à Workload Factory. Ce choix influe sur l'emplacement de stockage du mot de passe, son chiffrement et la gestion des exigences telles que le support GovCloud et la rotation des identifiants.

Modèle d'accès ONTAP en lecture seule

Pour les fonctionnalités alimentées par l'IA, telles que l'analyse des événements et le diagnostic de latence, Workload Factory utilise des identifiants ONTAP en lecture seule lorsqu'ils sont disponibles. Le modèle

d’identifiant en lecture seule garantit que l’agent de diagnostic IA ne peut pas modifier votre environnement de stockage — il peut uniquement observer et diagnostiquer.

Comparaison des options de stockage des identifiants

Identifiants AWS

Les identifiants AWS sont toujours supposés via un rôle IAM. Workload Factory peut soit gérer les informations du rôle en interne, soit les référencer depuis AWS Secrets Manager.

Option	Identifiants AWS	Ce qui est stocké	Chiffrement
Workload Factory géré	ARN du rôle IAM + ID externe	ARN du rôle IAM + ID externe	L’ARN du rôle n’est pas un secret (stocké tel quel)

Identifiants ONTAP

Workload Factory peut gérer les identifiants ONTAP en interne grâce à un stockage chiffré ou les référencer depuis AWS Secrets Manager. Ce choix influe sur la manière dont le mot de passe est stocké, chiffré et renouvelé.

Les identifiants ONTAP sont requis pour que NetApp Workload Factory puisse interagir avec les API du système de fichiers ONTAP via un "Lien Lambda".

Option	Identifiants ONTAP	Ce qui est stocké	Chiffrement
Workload Factory géré	Mot de passe (chiffré)	Mot de passe administrateur ONTAP (chiffré)	Le mot de passe ONTAP utilise le chiffrement par enveloppe AES-256
AWS Secrets Manager	Référence ARN de Secrets Manager	ARN du Secrets Manager	L’ARN des secrets n’est pas un secret (stocké tel quel) ; AWS Secrets Manager chiffre le secret dans votre compte

Considérations supplémentaires

Exigence GovCloud

Le rôle IAM standard est utilisé ; les identifiants ONTAP doivent utiliser Secrets Manager (le stockage des mots de passe n’est pas autorisé).

Rotation

Les stratégies de rôle sont mises à jour dans votre compte. Mettez à jour le mot de passe ONTAP dans NetApp Workload Factory (option gérée) ou faites-le pivoter dans AWS Secrets Manager.

Niveaux d’autorisation de privilège minimal pour NetApp Workload Factory

Vous pouvez à tout moment restreindre les autorisations IAM de Workload Factory pour les aligner sur les exigences du moindre privilège, telles que la limitation de l’accès à des ressources spécifiques (ARN) et l’application de conditions IAM, par exemple des balises et des plages CIDR.

Modèle d’autorisation à plusieurs niveaux

Workload Factory utilise un modèle d’autorisations à plusieurs niveaux, conforme au principe du moindre privilège. Vous choisissez les niveaux de capacité à activer lors de l’ajout d’identifiants AWS. Vous pouvez commencer par la découverte en lecture seule et étendre selon vos besoins.

Workload Factory accorde toutes les autorisations via un rôle IAM dans votre compte AWS, qu’il assume via STS avec un ID externe.

Workload Factory limite davantage la portée de chaque appel d’API à l’aide d’une politique de session intégrée.

Dans la console Workload Factory, la fonctionnalité de chat IA *Ask Me* vous aide à affiner les autorisations en toute sécurité en suggérant des options de restriction et en générant une politique mise à jour à appliquer dans AWS.

Octroi des autorisations

Lorsque vous ajoutez des informations d’identification AWS à Workload Factory, vous pouvez choisir les niveaux d’autorisation à activer. Vous pouvez activer ou désactiver les niveaux à tout moment.

Les niveaux sont cumulatifs : activer un niveau supérieur active automatiquement tous les niveaux inférieurs.

Contrôles de sécurité

- ID externe (protection du confused deputy)
- Politiques de session par opération (principe du moindre privilège par requête)
- Conditions basées sur les balises (modifications des groupes de sécurité limitées aux ressources créées par Workload Factory)
- Portée de l’ARN secret (accès à Secrets Manager restreint à `FSxSecret*`)
- Validation des autorisations d’exécution (action/ressource manquante signalée pour correction ciblée)

Documentation relative aux autorisations

La référence principale concernant les autorisations de Workload Factory est la "référence des autorisations" dans la documentation d’installation et d’administration de Workload Factory. Vous pouvez trouver des informations sur les impacts de la suppression des autorisations dans les stratégies IAM de stockage dans cette référence.

Autorisations de surveillance Amazon CloudWatch pour NetApp Workload Factory

Les autorisations de surveillance Amazon CloudWatch sont facultatives dans NetApp Workload Factory et ne s'appliquent que lorsque vous déployez la pile de surveillance distincte. La pile de surveillance offre une visibilité opérationnelle en collectant les métriques du système de fichiers, en publiant les journaux d'événements, en gérant les tableaux de bord et les alarmes CloudWatch, et en envoyant des notifications d'alerte via Amazon SNS. La pile requiert également un accès pour récupérer les identifiants ONTAP lorsque cela est nécessaire pour la surveillance.

Autorisations de surveillance requises CloudWatch

Les autorisations suivantes sont requises pour la pile de surveillance optionnelle :

Autorisation	But
fsx:Describe* / fsx:ListTagsForResource	Collecter les métriques du système de fichiers
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	Gérer les tableaux de bord et les alarmes
logs : CreateLogGroup / logs : CreateLogStream / logs : PutLogEvents	Publier les journaux d'événements
sns:Publish	Envoyer des notifications d'alerte
secretsmanager :GetSecretValue	Récupérer les identifiants ONTAP pour la surveillance

Informations sur le copyright

Informations sur les marques commerciales