Modèle de sécurité et responsabilités

Information Security for Workload Factory

NetApp
September 16, 2026

Sommaire

Modèle de sécurité et responsabilités

Découvrez le modèle de sécurité de NetApp Workload Factory

NetApp Workload Factory est une plateforme de contrôle SaaS qui vous aide à gérer et à optimiser les charges de travail exécutées sur Amazon FSx for NetApp ONTAP dans votre environnement AWS. Les résultats en matière de sécurité dépendent des responsabilités partagées entre NetApp, AWS et votre organisation.

Modèle de sécurité de haut niveau

- Workload Factory utilise un modèle d'assume-role IAM pour obtenir des identifiants temporaires AWS STS afin d'appeler les API AWS de votre compte.
- Certains flux de travail nécessitent des opérations natives ONTAP qui ne sont pas exposées via les API AWS ; vous pouvez exécuter ces opérations dans votre VPC à l'aide de composants d'exécution déployés par le client (par exemple, Lambda link).
- Les signaux d'observabilité (métriques, télémétrie et enregistrements opérationnels) prennent en charge la surveillance opérationnelle et les investigations.

Questions clés de révision

- De quel accès Workload Factory a-t-il besoin sur votre compte AWS (rôle de confiance + autorisations) ?
- Quels chemins d'exécution s'appliquent à vos flux de travail prévus (AWS API uniquement ou opérations natives ONTAP via un composant VPC) ?
- Quelles catégories de données sont gérées (configuration/métadonnées, journaux/événements opérationnels, télémétrie) et où sont-elles stockées ?
- Quels sont les signaux de surveillance existants et quelles sont leurs caractéristiques de rétention ?

Et ensuite

- "Limites de responsabilité partagée pour NetApp Workload Factory"
- "Chemins de connectivité et de confiance pour NetApp Workload Factory"
- "Niveaux d'autorisation de privilège minimal pour NetApp Workload Factory"

Limites de responsabilité partagée pour NetApp Workload Factory

NetApp Workload Factory la responsabilité de la sécurité est partagée entre NetApp (exploitation SaaS), AWS (infrastructure cloud et services gérés) et vous (configuration client). Comprendre où commencent et finissent les responsabilités de chaque partie vous aide à configurer correctement votre environnement AWS et à éviter les failles de sécurité. Ces limites clarifient ce que NetApp exploite, ce qu'AWS sécurise et ce que vous devez configurer et maintenir vous-même.

NetApp responsabilités (côté service)

NetApp est responsable de l'exploitation et de la sécurité de la plateforme SaaS Workload Factory. Cela inclut la gestion côté service des références de configuration stockées et des données opérationnelles.

Responsabilités AWS (plateforme cloud)

AWS est responsable de la sécurité de l'infrastructure cloud et des services gérés utilisés par votre déploiement et vos flux de travail (par exemple, IAM/STS, FSx for ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda et les primitives de réseau).

Responsabilités du client (votre configuration)

Vous êtes responsable de :

- Rôles IAM AWS, politiques de confiance et autorisations de moindre privilège
- Contrôles VPC (sous-réseaux, groupes de sécurité, routage, points de terminaison et sortie)
- Gouvernance des identifiants (y compris les identifiants ONTAP si vos flux de travail l'exigent)
- Décisions relatives au chiffrement et à la gestion des clés (par exemple, clés KMS gérées par le client en option pour FSx for ONTAP)
- Surveillance, alertes, politiques de rétention et processus de réponse aux incidents

Preuves à recueillir

- Relation de confiance du rôle IAM (y compris la condition d'identifiant externe)
- Sélection du niveau d'autorisation IAM et artefacts de stratégie
- Décision relative aux limites du réseau (API AWS uniquement ou composant d'exécution VPC tel qu'un lien Lambda)
- Décisions en matière d'observabilité et attentes en matière de rétention
- Décision d'activation de l'IA (les diagnostics d'IA sont activés par défaut, sauf s'ils sont explicitement désactivés)

NetApp Workload Factory workflow de sécurité d'intégration

L'intégration à NetApp Workload Factory établit un accès sécurisé à votre environnement AWS avant que vous ne commenciez à utiliser le produit. Ce processus combine la configuration de la confiance AWS, la définition du périmètre des autorisations, la configuration de la connectivité, la vérification de l'observabilité et l'activation optionnelle des diagnostics IA.

Étape 1 : Déterminez votre posture d'intégration

- Identifiez les comptes AWS et les limites de l'environnement (par exemple, séparation entre production et hors production).
- Identifier les flux de travail requis (découverte en lecture seule vs provisionnement vs opérations natives ONTAP).

- Décidez s'il convient de déployer des composants d'exécution VPC (par exemple, un lien Lambda) en fonction des besoins du flux de travail.
- Décidez si vous souhaitez activer les diagnostics IA (activés par défaut).

Informations connexes

- "Types d'identifiants"
- "Aperçu du lien Lambda"
- "Aperçu des contrôles IA"

Étape 2 : Établir la confiance et l'accès à AWS

1. Déployez un rôle IAM dans votre compte AWS.
2. Assomption du rôle de passerelle à l'aide d'un identifiant externe dans la politique de confiance.
3. Enregistrez l'ARN du rôle et l'ID externe dans Workload Factory.

Informations connexes

"Intégration de compte AWS"

Étape 3 : Appliquez les permissions minimales

1. Sélectionnez le niveau d'autorisation minimal qui prend en charge vos flux de travail prévus.
2. Vérifiez que les politiques de session par requête limitent les actions à l'opération en cours d'exécution.

Informations connexes

"Niveaux d'autorisation de privilège minimal pour NetApp Workload Factory".

Étape 4 : Configurez la connectivité et les limites du VPC (si nécessaire)

1. Validez les chemins réseau requis vers les points de terminaison AWS.
2. Si vous avez besoin d'opérations natives ONTAP, déployez et validez l'option d'exécution appropriée dans votre VPC.

Informations connexes

- "Chemins de connectivité et de confiance pour NetApp Workload Factory"
- "Options d'exécution ONTAP pour NetApp Workload Factory"

Étape 5 : Vérifiez l'observabilité

1. Confirmez que les indicateurs et les données de télémétrie sont collectés et conservés comme prévu.
2. Confirmez que vous pouvez accéder aux enregistrements opérationnels nécessaires au dépannage et aux enquêtes.

Informations connexes

- "Aperçu de l'observabilité pour NetApp Workload Factory"
- "Métriques et télémétrie pour NetApp Workload Factory"

Étape 6 : Activer les diagnostics IA (facultatif)

Les diagnostics par IA sont activés par défaut. Si vous les activez, assurez-vous de respecter les prérequis et limitez les autorisations au minimum nécessaire.

Informations connexes

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

Conformité et posture de sécurité pour NetApp Workload Factory

NetApp Workload Factory est conçu en accordant une importance primordiale à la conformité et à la sécurité. Toutes les charges de travail dans Workload Factory s'exécutent sur Amazon FSx for NetApp ONTAP. En plus de "fonctionnalités de sécurité AWS", NetApp Workload Factory dispose de "Conformité SOC2 Type 1, SOC2 Type 2 et HIPAA".

Amazon FSx for NetApp ONTAP for NetApp Workload Factory est une "Solution AWS pour le déploiement d'applications d'entreprise" et suit les bonnes pratiques AWS Well-Architected.

Informations sur le copyright

Informations sur les marques commerciales