Architecture et connectivité

Information Security for Workload Factory

NetApp
September 16, 2026

Sommaire

Architecture et connectivité

Chemins de connectivité et de confiance pour NetApp Workload Factory

NetApp Workload Factory communique avec les API AWS, les ressources du compte AWS du client, le lien AWS Lambda et Amazon Bedrock, chacun avec ses propres protocoles, ports et méthodes d'authentification. Ces connexions sont organisées en groupes qui séparent le plan de gestion AWS, le plan de données ONTAP et le trafic du lien Lambda, afin que vous puissiez évaluer indépendamment les limites de confiance.

Voies de connectivité

Workload Factory établit plusieurs chemins de connectivité distincts, chacun ayant une fonction spécifique pour la découverte, le provisionnement et la gestion de vos ressources AWS et ONTAP. Certains chemins proviennent de Workload Factory lui-même en utilisant des identifiants AWS assumés, tandis que d'autres passent par Lambda link, qui fonctionne à l'intérieur de votre VPC pour atteindre les points de terminaison de gestion ONTAP sans les exposer publiquement. Un chemin optionnel vers Amazon Bedrock prend en charge les diagnostics assistés par l'IA et n'est actif que lorsque votre organisation active cette fonctionnalité.

Les sections suivantes décrivent chaque chemin, y compris les API AWS ou ONTAP impliquées, les identifiants ou l'authentification utilisés, ainsi que les conditions qui déterminent si le chemin est actif. Comprendre ces chemins vous aide à évaluer les accès réseau et les autorisations requis par Workload Factory, et à identifier les points de passage des données entre comptes ou VPC.

Workload Factory vers les API AWS

Workload Factory utilise `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups` et les API EC2/VPC pour la découverte des sous-réseaux et des groupes de sécurité.

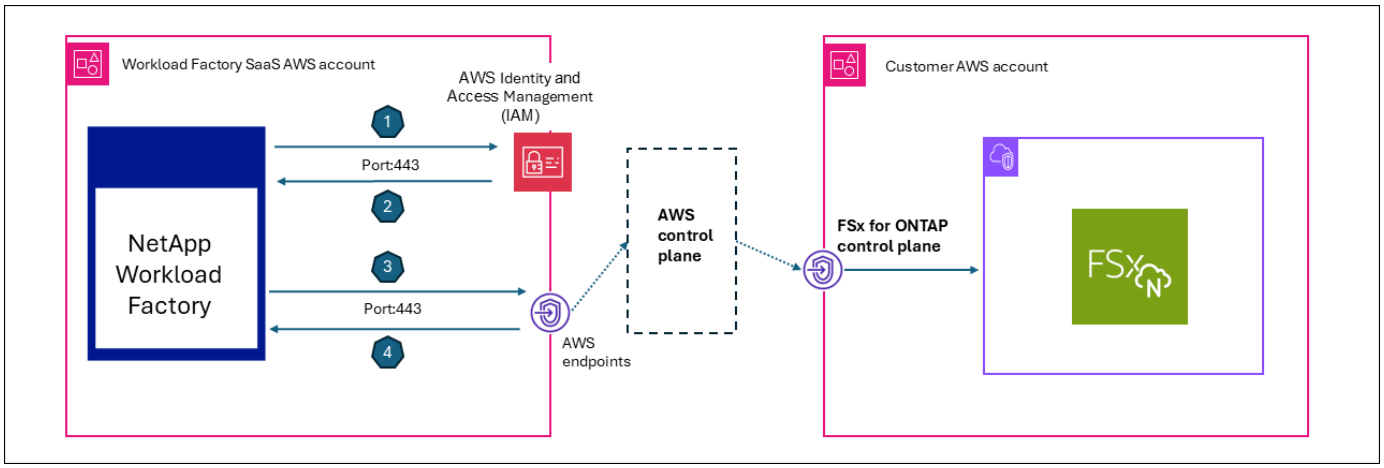
- Le service de collecte effectue des analyses environ toutes les cinq heures.
- Les opérations CRUD s'exécutent à la demande.
- Tous les appels utilisent des identifiants temporaires assumés par STS avec un identifiant externe.

Workload Factory vers les ressources du compte AWS du client (orchestration et automatisation)

Workload Factory interagit avec AWS pour communiquer et créer des ressources. L'orchestration et l'automatisation s'effectuent de plusieurs manières.

- Modèles AWS CloudFormation : Workload Factory utilise des modèles AWS CloudFormation pour créer des ressources telles que des rôles et des systèmes de fichiers. Par exemple, lorsque vous créez un système de fichiers dans l'interface utilisateur, Workload Factory appelle directement CloudFormation et vous redirige vers votre compte AWS.
- Appels d'API AWS : Workload Factory utilise des appels d'API AWS (STS `AssumeRole`) pour envoyer des commandes d'API pour les activités liées à FSx for ONTAP.
- AWS Lambda : Workload Factory utilise CloudFormation pour déployer une fonction AWS Lambda pour le lien qui communique avec ONTAP.

Le diagramme suivant montre comment Workload Factory utilise une relation de confiance entre un compte AWS NetApp et les comptes AWS des clients avec des systèmes de fichiers FSx for ONTAP.



1. Workload Factory demande à AWS STS `AssumeRole`, en utilisant un ID externe spécifique au client provenant du service AWS IAM.
2. Le service AWS IAM récupère un rôle et crée une session.
3. Workload Factory envoie une requête API AWS avec les autorisations de session.
4. Workload Factory reçoit une réponse de l'API AWS du plan de contrôle FSx for ONTAP.

Lien Lambda vers le point de terminaison de gestion ONTAP

Les liens Lambda s'exécutent au sein du VPC du client pour un accès au sous-réseau privé sans exposer ONTAP publiquement. Toute la connectivité du lien vers le point de terminaison de gestion ONTAP est uniquement sortante, aucune connectivité entrante ni point de terminaison exposé n'est donc requis. Le lien est utilisé uniquement pour les opérations natives ONTAP que l'API Amazon FSx for NetApp ONTAP n'expose pas.

Workload Factory utilise les protocoles suivants pour les opérations sur les volumes, les machines virtuelles de stockage et les clusters, ainsi que pour les données de diagnostic et de performance en lecture seule :

- HTTPS/443 (REST)
- SSH/22 (CLI)

Lien Lambda vers AWS Secrets Manager (récupération de l'identifiant ONTAP)

Utilisé uniquement lorsque les identifiants administrateur ONTAP sont stockés dans AWS Secrets Manager (alternative : identifiants chiffrés dans Workload Factory à l'aide du chiffrement par enveloppe).

- Le proxy-forwarder transmet `x-aws-secret-arn` (encodé en Base64) dans les en-têtes.
- Lambda link effectue des appels `GetSecretValue` lors de l'exécution pour récupérer le mot de passe.

Cela permet de conserver le mot de passe à l'intérieur du périmètre de votre compte et d'empêcher sa transmission depuis Workload Factory.

Composants Workload Factory et clients vers Amazon Bedrock (diagnostics IA)

Ce chemin n'est utilisé que lorsque les diagnostics d'IA sont activés.

- Event Analyzer utilise ce chemin pour l'analyse EMS et le diagnostic de latence.
- Bedrock s'exécute avec vos identifiants supposés et l'ARN du profil d'inférence, ainsi les données ne sont pas transférées vers le compte de NetApp.

Les données envoyées à Bedrock peuvent inclure des événements EMS au format JSON, des statistiques QoS, la configuration des volumes, des données agrégées et des informations sur les nœuds. Le chemin est actif uniquement lorsqu'un profil d'inférence est configuré par organisation (`ai_analyzer_config` table).

Groupes de connexion (protocoles, ports et authentification)

Groupe A — Chemin de confiance du plan de gestion AWS (identifiants supposés)

Connexion	Protocole	Port	Direction	Authentification	Justification
STS AssumeRole	HTTPS	443	WF → AWS STS (compte client)	Identifiants IAM + ExternalId	Obtenir des identifiants temporaires inter-comptes
API FSx (Décrire/Créer/Mettre à jour/Supprimer)	HTTPS	443	WF → Point de terminaison AWS FSx (région du client)	Identifiants temporaires STS	Gestion du cycle de vie des systèmes de fichiers et des volumes
API EC2/VPC	HTTPS	443	WF → Point de terminaison AWS EC2	Identifiants temporaires STS	Découverte des groupes de sécurité, des sous-réseaux et des VPC
API CloudFormation	HTTPS	443	WF → Point de terminaison AWS CFN	Identifiants temporaires STS	Déploiement de la pile pour les rôles IAM et le provisionnement FSx
Secrets Manager GetSecretValue	HTTPS	443	WF → Point de terminaison AWS Secrets Manager (compte client)	Identifiants temporaires STS	Récupérer le mot de passe d'administrateur ONTAP (lorsqu'il est stocké dans Secrets Manager)
Chiffrement/déchiffrement KMS	HTTPS	443	WF → Point de terminaison AWS KMS	Identifiants temporaires STS	Opérations sur la clé de chiffrement du volume

Tous les appels d'API AWS utilisent le point de terminaison régional du client et peuvent être acheminés via des points de terminaison VPC si ceux-ci sont configurés.

Groupe B — plan de données ONTAP

Le plan de données ONTAP est toujours acheminé via Lambda link ; les services Workload Factory ne se connectent jamais directement à ONTAP.

Connexion	Protocole	Port	Direction	Authentification	Justification
API REST ONTAP	HTTPS	443	Lien (VPC client) → LIF de gestion ONTAP	Authentification de base (nom d'utilisateur/mot de passe) ou ARN du Secrets Manager	Configuration du cluster, du volume et de la machine virtuelle de stockage ; QoS ; événements EMS ; état ARP
Interface de ligne de commande SSH ONTAP	SSH	22	Lien (VPC client) → LIF de gestion ONTAP	Authentification par mot de passe	Commandes de diagnostic (statistiques QoS, df, journaux d'événements, efficacité)

Stratégie de routage (ordre de priorité) pour le proxy-forwarder :

1. En-tête explicite `x-link-id` : rechercher l'ARN Lambda dans la base de données
2. ID cible (ID du système de fichiers FSx) : trouvez le lien associé
3. ID de l'agent de Console : acheminement via le courtier de messages vers l'agent de Console

Groupe C — Lien AWS Lambda (déployé dans votre VPC)

Connexion	Protocole	Port	Direction	Authentification	Justification
Invocation Lambda	HTTPS (AWS SDK)	443	WF → API AWS Lambda (compte client)	IAM (`lambda:InvokeFunction`)	Exécutez des commandes ONTAP REST/SSH depuis le VPC du client
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda (VPC client) → LIF de gestion ONTAP	Authentification de base / mot de passe	Accès au sous-réseau privé à ONTAP sans exposition publique

Groupe D — NetApp Console Agent (EC2 dans votre VPC, uniquement sortant)

Connexion	Protocole	Port	Direction	Authentification	Justification
Sondage des agents	HTTPS	443	Agent de console (VPC client) → Courtier de messages WF	Jeton porteur (portée occm-access)	Interrogation longue pour les commandes ONTAP en attente (délai d'expiration de 7 secondes ; reconnexions)
Réponse de l'agent	HTTPS	443	Agent de console (VPC client) → Courtier de messages WF	Jeton Bearer	Renvoie les résultats des commandes ONTAP (éventuellement compressés au format zlib)
Agent de console → ONTAP	HTTPS + SSH	443, 22	Agent de console (VPC client) → LIF de gestion ONTAP	Authentification de base / mot de passe	Exécutez des opérations ONTAP par proxy

Conception clé : Workload Factory n'initie jamais de connexions entrantes vers l'agent Console. Les tâches sont mises en file d'attente dans des flux Redis ; l'agent Console interroge `GET`

`/messagebroker/v1/requests` et répond avec `POST /messagebroker/v1/responses`.

Groupe E — CloudFormation callbacks de ressources personnalisées

Connexion	Protocole	Port	Direction	Authentification	Justification
CloudFormation → WF Lambda	HTTPS	443	CloudFormation (client) → WF Lambda (NetApp)	Jeton JWT + jeton de référence	Signalez l'état de création du rôle IAM et renvoyez l'ARN du rôle
ONTAP CloudFormation Resource Provider → Lien	HTTPS	443	CloudFormation resource Lambda (client) → Link Lambda (client)	IAM	Créer, mettre à jour ou supprimer des ressources ONTAP lors des opérations de pile

Résumé : exigences réseau pour votre VPC

Composant	Entrant	Sortant
FSx for ONTAP	Ports 443 et 22 du groupe de sécurité Link Lambda ou de l'agent Console	S/O
Lien Lambda	Aucune	Port 443 (ONTAP, API AWS) et port 22 (ONTAP SSH)
Agent de console EC2	Aucune	Port 443 (points de terminaison WF, ONTAP, API AWS) et port 22 (ONTAP SSH)
Points de terminaison VPC (facultatif)	S/O	STS, FSx, S3, Secrets Manager, Lambda, CloudFormation

Aucun accès Internet entrant n'est requis pour aucun composant du VPC client. Toutes les connexions sont soit initiées en sortie (interrogation de l'agent Console), soit invoquées via les API de service AWS (Lambda Invoke).

Options d'exécution ONTAP pour NetApp Workload Factory

Certains workflows NetApp Workload Factory nécessitent des opérations ONTAP natives qui ne sont pas exposées via les API AWS. Workload Factory propose deux options d'exécution permettant de maintenir ces opérations à l'intérieur de la limite de votre compte AWS : un lien Lambda qui exécute les opérations ONTAP depuis votre VPC, et un NetApp Console Agent qui utilise une connectivité sortante uniquement depuis une instance EC2. Les deux options vous permettent d'effectuer les opérations ONTAP requises tout en gardant les décisions concernant le réseau, les identifiants et le cycle de vie dans le cadre de votre modèle de sécurité.

Options d'exécution

Lien Lambda (AWS Lambda dans votre VPC)

Exécute les diagnostics ONTAP REST et ONTAP CLI en lecture seule depuis votre VPC, sans exposer ONTAP publiquement.

NetApp Console Agent (EC2 dans votre VPC, uniquement sortant)

Exécute des opérations ONTAP par proxy où l'agent initie des connexions sortantes et Workload Factory n'initie jamais de connexions entrantes vers l'agent.

Considérations de sécurité

- Limites du réseau : confirmez les ports de sortie requis (443/22) et les destinations.
- Limites des identifiants : décidez si les identifiants ONTAP sont stockés dans Workload Factory (chiffrés dans une enveloppe) ou référencés depuis AWS Secrets Manager.
- Auditabilité : confirmez les enregistrements opérationnels relatifs à l'activité et aux défaillances des composants.
- Gestion du cycle de vie : confirmez comment les mises à jour et les suppressions ont lieu.

Informations connexes

- "Aperçu du lien Lambda pour NetApp Workload Factory"
- "Chemins de connectivité et de confiance pour NetApp Workload Factory"
- "Chiffrement et gestion des clés pour NetApp Workload Factory"