



Opérations ONTAP et liaison Lambda (composant VPC client)

Information Security for Workload Factory

NetApp
September 16, 2026

Sommaire

- Opérations ONTAP et liaison Lambda (composant VPC client) 1
 - Découvrez le lien Lambda pour NetApp Workload Factory 1
 - Architecture de sécurité des liens 1
 - Lien Lambda versus NetApp Console agent 2
 - Informations connexes 2
- Ports et appels Lambda pour NetApp Workload Factory 3
 - Types de requêtes 3
 - Limites du réseau sortant 3
 - Workload Factory appelle Lambda link 3
 - Informations connexes 3
- Autorisations IAM liées à Lambda pour NetApp Workload Factory 4
 - autorisations du rôle d'exécution Lambda 4
 - Autorisations d'invocation de Workload Factory 4
- Cycle de vie des liens Lambda pour NetApp Workload Factory 4
 - Points de contrôle du cycle de vie 5

Opérations ONTAP et liaison Lambda (composant VPC client)

Découvrez le lien Lambda pour NetApp Workload Factory

NetApp Workload Factory utilise un *link*, une fonction AWS Lambda déployée dans votre VPC, pour maintenir les opérations natives ONTAP à l'intérieur des limites de votre compte AWS lorsque l'API Amazon FSx for NetApp ONTAP n'expose pas ces opérations. Le link s'exécute dans vos sous-réseaux et groupes de sécurité, de sorte que le composant d'exécution reste au sein de votre environnement AWS. Workload Factory invoque le link uniquement pour les opérations qui nécessitent un accès direct à ONTAP plutôt qu'une API de service AWS disponible. Il compare l'architecture du link avec le profil de sécurité et opérationnel de l'agent NetApp Console.

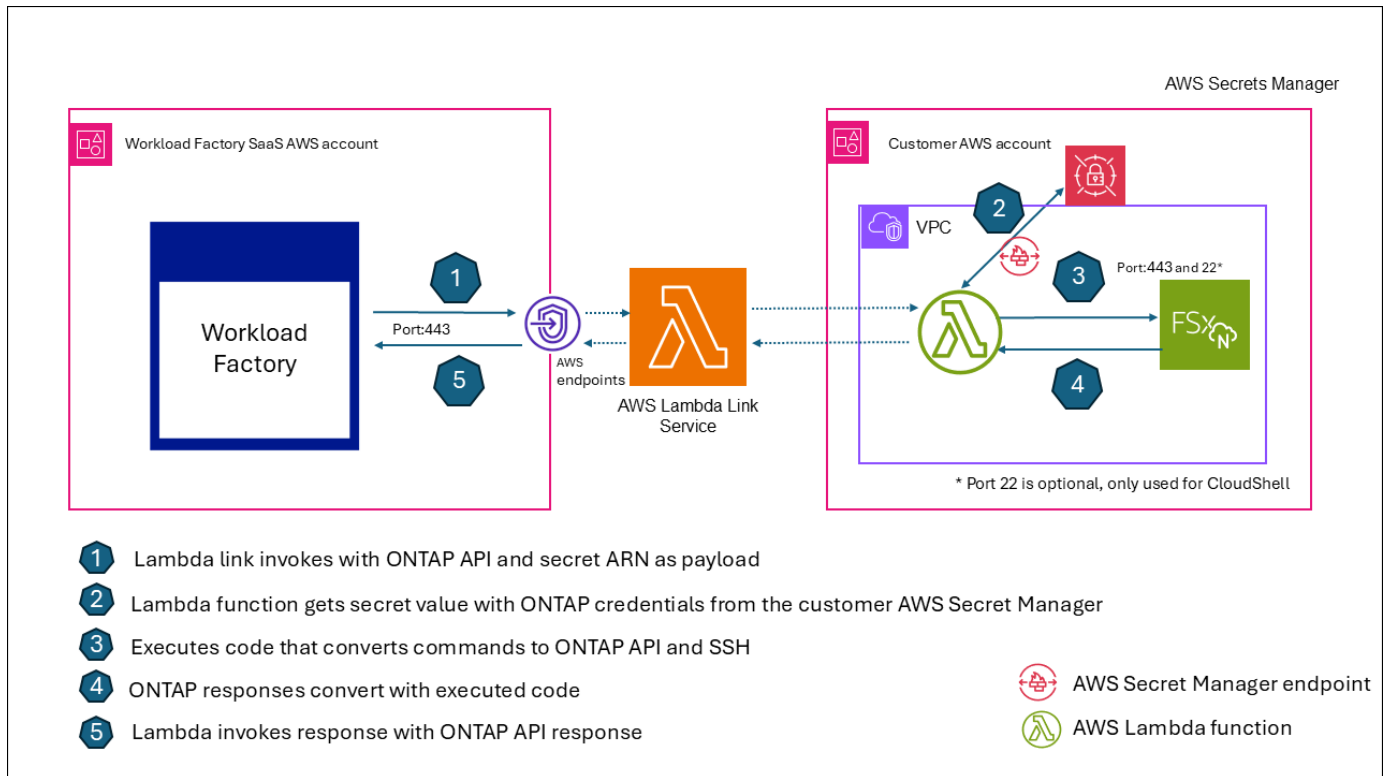
Architecture de sécurité des liens

Un lien Workload Factory crée une relation de confiance et une connectivité indirecte entre un compte Workload Factory et un ou plusieurs systèmes de fichiers FSx for ONTAP.

Le tableau suivant présente une vue d'ensemble de l'architecture de sécurité des liens Lambda. Utilisez ces informations pour comprendre comment la fonction Lambda est déployée et exécutée dans votre compte AWS, y compris sa configuration réseau, son environnement d'exécution et ses limites opérationnelles.

Propriété	Détail
Calcul	AWS Lambda (image conteneur)
Durée d'exécution	Node.js 22
Déploiement	CloudFormation stack dans votre compte AWS
Placement VPC	Vos sous-réseaux, vos groupes de sécurité
Délai d'attente	10 secondes par invocation
Invocation	Synchrone (RequestResponse)
Type de package	Image du conteneur (provenant de NetApp ECR)

Le schéma suivant illustre l'architecture de sécurité de la liaison Lambda.



Lien Lambda versus NetApp Console agent

Le lien Lambda et l'agent NetApp Console ont des objectifs différents et présentent des implications différentes en matière de sécurité et d'exploitation.

Dimension	Lien (basé sur Lambda)	NetApp Console agent (basé sur VM/Pods)
Modèle d'exécution	Sans serveur (AWS Lambda), déployé par le client	Machines virtuelles/conteneurs déployés par le client ; exécute des pods de service NetApp console
Portée principale	Opérations REST du plan de contrôle ONTAP (uniquement lorsque les API AWS ne prennent pas en charge l'opération)	Orchestration et prise en charge des services de données
Support des services de données	N'héberge pas de services de données	Peut héberger des services de données (exécute des pods de service NetApp console)
Frais généraux d'exploitation	Pas de machine virtuelle toujours active	Gestion du cycle de vie des machines virtuelles et mises à niveau

Informations connexes

Pour obtenir la carte complète de la connectivité inter-systèmes, veuillez vous référer à "[Chemins de connectivité et de confiance pour NetApp Workload Factory](#)".

Ports et appels Lambda pour NetApp Workload Factory

NetApp Workload Factory utilise les limites de requêtes et de ports Lambda pour définir la connectivité sortante requise et l'invocation autorisée par IAM. La liaison prend en charge les requêtes HTTPS vers le point de terminaison de gestion ONTAP, les commandes SSH en lecture seule pour les diagnostics et les contrôles d'intégrité. Toute la connectivité est sortante depuis la liaison au sein de votre VPC, aucune connectivité entrante ni aucun point de terminaison exposé ne sont donc requis. Workload Factory invoque la liaison via l'API AWS Lambda en utilisant une autorisation basée sur IAM.

Types de requêtes

- HTTPS (ONTAP REST API) : relaie les appels HTTPS vers le point de terminaison de gestion ONTAP (port 443) pour les opérations sur les volumes, les machines virtuelles de stockage et les clusters.
- SSH (ONTAP CLI) : exécute des commandes ONTAP CLI en lecture seule sur le port 22 pour les diagnostics et les données de performance.
- Bilan de santé : renvoie l'état et les fonctionnalités prises en charge.

Limites du réseau sortant

Direction	Port	Destination	But
Sortant	443	Adresse IP de gestion ONTAP (dans votre VPC)	opérations de l'API REST
Sortant	22	Adresse IP de gestion ONTAP (dans votre VPC)	Commandes SSH CLI
Sortant	443	Point de terminaison AWS Secrets Manager (facultatif)	Récupération des informations d'identification lors de l'utilisation de Secrets Manager

Aucune connectivité entrante n'est requise. Le lien n'expose aucun point de terminaison. Workload Factory l'appelle en utilisant l'API `lambda:InvokeFunction` AWS.

Workload Factory appelle Lambda link

Workload Factory appelle le lien Lambda via l'API AWS Lambda (`lambda:InvokeFunction`) en utilisant une autorisation basée sur IAM.

La charge utile de l'invocation contient :

- point de terminaison de gestion ONTAP cible (IP/nom d'hôte)
- opération à effectuer (chemin d'accès à l'API REST ou commande SSH)
- informations d'authentification (identifiants intégrés ou référence ARN de Secrets Manager)

Informations connexes

Pour obtenir la carte complète de la connectivité inter-systèmes, veuillez vous référer à ["connectivité et chemins de confiance pour NetApp Workload Factory"](#).

Autorisations IAM liées à Lambda pour NetApp Workload Factory

NetApp Workload Factory utilise les limites d'autorisation de lien Lambda pour définir l'accès IAM requis pour l'exécution de Lambda et l'invocation de Workload Factory. Ces autorisations sont facultatives, mais elles sont requises pour les opérations natives ONTAP. Lorsque vous configurez la prise en charge de Secrets Manager, le lien récupère les identifiants ONTAP directement depuis votre AWS Secrets Manager lors de l'exécution, et le mot de passe ne transite qu'au sein de votre VPC, de Secrets Manager à la fonction Lambda, puis au point de terminaison ONTAP.

Pour connaître les exigences relatives au chemin de requête et au port, veuillez vous référer à ["Ports et appels de liaison Lambda"](#).

autorisations du rôle d'exécution Lambda

Le rôle d'exécution Lambda requiert les autorisations suivantes lors du déploiement d'un lien dans votre VPC :

Autorisation	But
ec2:CreateNetworkInterface / ec2:DescribeNetworkInterfaces / ec2>DeleteNetworkInterface	Mise en réseau Lambda standard attachée à un VPC
ec2:AssignPrivatelpAddresses / ec2:UnassignPrivatelpAddresses	Gestion des adresses IP VPC ENI
secretsmanager : GetSecretValue (limité à FSxSecret*)	Récupérer les identifiants ONTAP (uniquement lorsque Secrets Manager est activé)
CloudWatch Logs (politique gérée)	Journalisation de l'exécution Lambda

Autorisations d'invocation de Workload Factory

La stratégie basée sur les ressources du lien Lambda accorde au principal de service Workload Factory les autorisations suivantes :

Autorisation	But
lambda:InvokeFunction	Exécutez la fonction Lambda
lambda:GetFunction	Contrôles de santé et d'état
lambda:UpdateFunctionCode	Mises à niveau de version (mises à jour d'image)
lambda:GetFunctionConfiguration	Vérification de la configuration

Cycle de vie des liens Lambda pour NetApp Workload Factory

NetApp Workload Factory utilise les contrôles de cycle de vie des liens Lambda pour gérer le déploiement, la surveillance de l'état et les mises à jour contrôlées des images,

avec une exposition opérationnelle minimale. Vous pouvez mettre à jour l'image conteneur du lien Lambda pour déployer des améliorations ou des correctifs de sécurité sans redéployer la pile Amazon CloudFormation, en utilisant l'`lambda:UpdateFunctionCode` autorisation. Les contrôles de cycle de vie définissent également comment surveiller l'état du lien et supprimer le lien Lambda ainsi que ses ressources associées lorsqu'ils ne sont plus nécessaires.

Points de contrôle du cycle de vie

- Déploiement : automatisé via Amazon CloudFormation ou déploiement de pile Terraform
- Surveillance : des contrôles d'intégrité détectent les problèmes de connectivité ; des compteurs de défaillance suivent la fiabilité
- Suppression : la suppression de la pile CloudFormation supprime la Lambda et les ressources associées de votre compte AWS

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.