Arquitectura y conectividad

Information Security for Workload Factory

NetApp
September 16, 2026

Tabla de contenidos

Arquitectura y conectividad

Vías de conectividad y confianza para NetApp Workload Factory

NetApp Workload Factory se comunica con las API de AWS, los recursos de la cuenta de AWS del cliente, el enlace Lambda de AWS y Amazon Bedrock, cada uno con sus propios protocolos, puertos y métodos de autenticación. Estas conexiones se organizan en grupos que separan el plano de gestión de AWS, el plano de datos de ONTAP y el tráfico del enlace Lambda, para que puedas evaluar los límites de confianza de forma independiente.

Vías de conectividad

Workload Factory establece varias rutas de conectividad distintas, cada una de las cuales cumple un propósito específico en la detección, el aprovisionamiento y la gestión de tus recursos de AWS y ONTAP. Algunas rutas se originan en el propio Workload Factory utilizando credenciales de AWS asumidas, mientras que otras pasan por Lambda link, que opera dentro de tu VPC para acceder a los endpoints de gestión de ONTAP sin exponerlos públicamente. Una ruta opcional hacia Amazon Bedrock admite diagnósticos asistidos por IA y solo está activa cuando tu organización habilita esa función.

En las siguientes secciones se describe cada una de las rutas, incluyendo las API de AWS u ONTAP implicadas, las credenciales o el método de autenticación utilizados y cualquier condición que determine si la ruta está activa. Comprender estas rutas te ayuda a evaluar qué acceso a la red y qué permisos requiere Workload Factory, y dónde los datos cruzan los límites de la cuenta o de la VPC.

Workload Factory a las API de AWS

Workload Factory utiliza `DescribeFileSystems`, `DescribeVolumes`, `CreateVolume`, `UpdateVolume`, `DeleteVolume`, `CreateFileSystem`, `CreateBackup`, `DescribeBackups` y las API de EC2/VPC para la detección de subredes y grupos de seguridad.

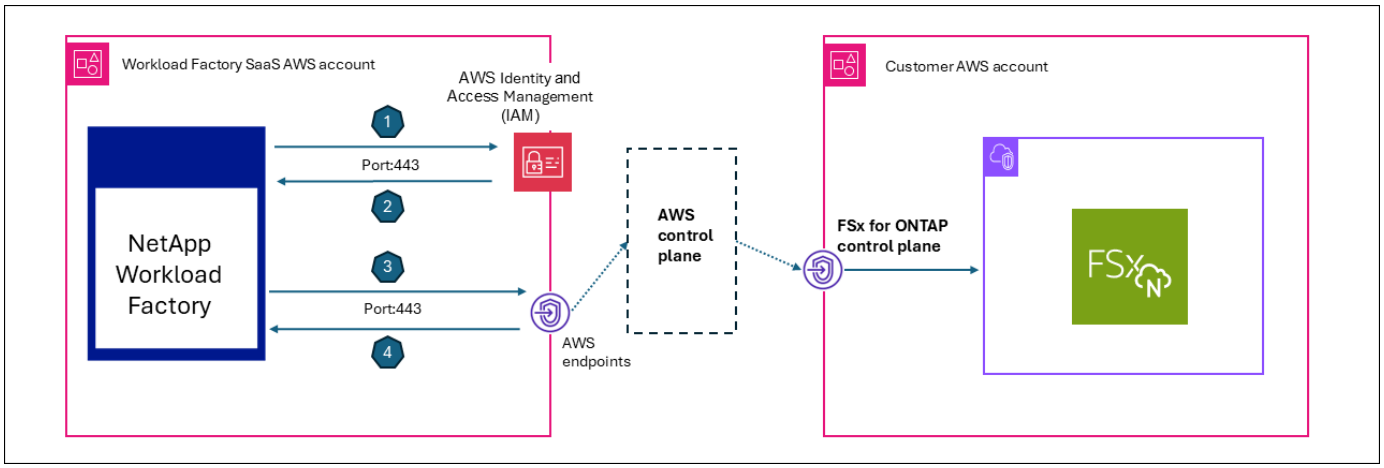
- El servicio de recopilación realiza un escaneo aproximadamente cada cinco horas.
- Las operaciones CRUD se ejecutan bajo demanda.
- Todas las llamadas utilizan credenciales temporales asumidas por STS con un identificador externo.

Workload Factory a los recursos de la cuenta de AWS del cliente (orquestación y automatización)

Workload Factory interactúa con AWS para comunicarse y crear recursos. La orquestación y la automatización ocurren de varias maneras.

- Plantillas de AWS CloudFormation: Workload Factory utiliza plantillas de AWS CloudFormation para crear recursos como roles y sistemas de archivos. Por ejemplo, cuando creas un sistema de archivos en la interfaz de usuario, Workload Factory accede directamente a CloudFormation y te redirige a tu cuenta de AWS.
- Llamadas a la API de AWS: Workload Factory utiliza llamadas a la API de AWS (STS `AssumeRole`) para enviar comandos de API para actividades relacionadas con FSx for ONTAP.
- AWS Lambda: Workload Factory utiliza CloudFormation para implementar una función de AWS Lambda para el enlace que se comunica con ONTAP.

El siguiente diagrama muestra cómo Workload Factory utiliza una relación de confianza entre una cuenta de AWS de NetApp y cuentas de AWS de clientes con sistemas de archivos FSx for ONTAP.



1. Workload Factory solicita AWS STS `AssumeRole`, usando el identificador externo específico del cliente del servicio AWS IAM.
2. El servicio IAM de AWS recupera un rol y crea una sesión.
3. Workload Factory envía una solicitud de API de AWS con permisos de sesión.
4. Workload Factory recibe una respuesta de la API de AWS procedente del plano de control de FSx for ONTAP.

Enlace de Lambda al punto final de gestión de ONTAP

Los enlaces Lambda se ejecutan dentro de la VPC del cliente para permitir el acceso a subredes privadas sin exponer ONTAP públicamente. Toda la conectividad desde el enlace hasta el punto final de gestión de ONTAP es exclusivamente de salida, por lo que no se requiere conectividad de entrada ni puntos finales expuestos. El enlace se utiliza únicamente para operaciones nativas de ONTAP que la API de Amazon FSx para NetApp ONTAP no expone.

Workload Factory utiliza los siguientes protocolos para las operaciones relacionadas con volúmenes, máquinas virtuales de almacenamiento y clústeres, y para los datos de diagnóstico y rendimiento de solo lectura:

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

Enlace de Lambda a AWS Secrets Manager (recuperación de credenciales de ONTAP)

Se utiliza únicamente cuando las credenciales de administrador de ONTAP se almacenan en AWS Secrets Manager (alternativa: credenciales cifradas en Workload Factory mediante cifrado de sobre).

- El proxy-forwarder pasa `x-aws-secret-arn` (codificado en Base64) en los encabezados.
- Lambda link llama a `GetSecretValue` en el momento de la ejecución para recuperar la contraseña.

De este modo, la contraseña permanece dentro de los límites de tu cuenta y se evita que se transmita desde Workload Factory.

Componentes de Workload Factory y específicos del cliente a Amazon Bedrock (diagnósticos de IA)

Esta ruta solo se utiliza cuando están activados los diagnósticos de IA.

- Event Analyzer utiliza esta ruta para el análisis del EMS y el diagnóstico de la latencia.
- Bedrock se ejecuta con tus credenciales asumidas y el ARN de tu perfil de inferencia, por lo que los datos no fluyen a la cuenta de NetApp.

Los datos enviados a Bedrock pueden incluir eventos JSON de EMS, estadísticas de calidad de servicio (QoS), configuración de volumen, datos agregados e información de los nodos. La ruta solo está activa cuando se ha configurado un perfil de inferencia por organización ((`ai_analyzer_config` tabla).

Grupos de conexión (protocolos, puertos y autenticación)

Grupo A — Ruta de confianza del plano de gestión de AWS (credenciales supuestas)

Conexión	Protocolo	Puerto	Dirección	Autenticación	Justificación
STS AssumeRole	HTTPS	443	WF → AWS STS (cuenta de cliente)	Credenciales de IAM + ExternalId	Obtener credenciales temporales entre cuentas
API de FSx (Describe/Create/Update/Delete)	HTTPS	443	WF → endpoint de AWS FSx (región del cliente)	Credenciales temporales de STS	Gestión del ciclo de vida del sistema de archivos y del volumen
API de EC2/VPC	HTTPS	443	WF → punto de conexión de AWS EC2	Credenciales temporales de STS	Detección de grupos de seguridad, subredes y VPC
API de CloudFormation	HTTPS	443	WF → Punto de conexión de AWS CFN	Credenciales temporales de STS	Implementación de la pila para roles de IAM y aprovisionamiento de FSx
Secrets Manager GetSecretValue	HTTPS	443	WF → endpoint de AWS Secrets Manager (cuenta del cliente)	Credenciales temporales de STS	Recuperar la contraseña de administrador de ONTAP (cuando está almacenada en Secrets Manager)
KMS cifrado/descifrado	HTTPS	443	WF → endpoint de AWS KMS	Credenciales temporales de STS	Operaciones con claves de cifrado de volumen

Todas las llamadas a la API de AWS utilizan el endpoint regional del cliente y pueden enrutarse a través de endpoints de VPC si están configurados.

Grupo B — Plano de datos de ONTAP

El plano de datos de ONTAP siempre se proxya a través de Lambda link; los servicios de Workload Factory nunca se conectan directamente a ONTAP.

Conexión	Protocolo	Puerto	Dirección	Autenticación	Justificación
API de REST de ONTAP	HTTPS	443	Enlace (VPC del cliente) → LIF de gestión de ONTAP	Autenticación básica (nombre de usuario/contraseña) o ARN de Secrets Manager	Configuración de clúster, volumen y máquina virtual de almacenamiento; QoS; eventos EMS; estado ARP
Interfaz de línea de comandos SSH de ONTAP	SSH	22	Enlace (VPC del cliente) → LIF de gestión de ONTAP	Autenticación mediante contraseña	Comandos de diagnóstico (estadísticas de QoS, df, registros de eventos, eficiencia)

Estrategia de enrutamiento (orden de prioridad) para el proxy-forwarder:

1. Encabezado explícito `x-link-id`: consultar el ARN de Lambda en la base de datos
2. ID de destino (ID del sistema de archivos FSx): encuentra el enlace asociado
3. ID del agente de la consola: ruta a través del intermediario de mensajes hasta el agente de la consola

Grupo C — Enlace de AWS Lambda (implementado en tu VPC)

Conexión	Protocolo	Puerto	Dirección	Autenticación	Justificación
Invocar Lambda	HTTPS (SDK de AWS)	443	WF → API de AWS Lambda (cuenta del cliente)	IAM (`lambda:InvokeFunction`)	Ejecutar comandos ONTAP REST/SSH desde la VPC del cliente
Lambda → ONTAP	HTTPS + SSH	443, 22	Lambda (VPC del cliente) → LIF de gestión de ONTAP	Autenticación básica / contraseña	Acceso desde una subred privada a ONTAP sin exposición pública

Grupo D — Agente de NetApp Console (EC2 en tu VPC, solo salida)

Conexión	Protocolo	Puerto	Dirección	Autenticación	Justificación
Sondeo de agentes	HTTPS	443	Agente de consola (VPC del cliente) → Broker de mensajes de WF	Token de portador (scope de occm-access)	Sondeo prolongado para comandos ONTAP pendientes (tiempo de espera de 7 segundos; se reconecta)
Respuesta del agente	HTTPS	443	Agente de consola (VPC del cliente) → Broker de mensajes de WF	Token Bearer	Devuelve los resultados del comando ONTAP (opcionalmente comprimidos con zlib)
Agente de consola → ONTAP	HTTPS + SSH	443, 22	Agente de consola (VPC del cliente) → LIF de gestión de ONTAP	Autenticación básica / contraseña	Ejecuta operaciones ONTAP a través de un proxy

Diseño clave: Workload Factory nunca inicia conexiones entrantes hacia el agente de la Console. El trabajo se

pone en cola en los flujos de Redis; el agente de la Console consulta `GET /messagebroker/v1/requests` y responde con `POST /messagebroker/v1/responses`.

Grupo E — Funciones de devolución de llamada de recursos personalizados de CloudFormation

Conexión	Protocolo	Puerto	Dirección	Autenticación	Justificación
CloudFormation → WF Lambda	HTTPS	443	CloudFormation (cliente) → WF Lambda (NetApp)	Token JWT + token de referencia	Informa sobre el estado de creación del rol de IAM y devuelve el ARN del rol
ONTAP CloudFormation Resource Provider → Enlace	HTTPS	443	CloudFormation recurso Lambda (cliente) → enlace Lambda (cliente)	IAM	Crear, actualizar o eliminar recursos de ONTAP durante las operaciones de la pila

Resumen: requisitos de red para tu VPC

Componente	Entrada	Salida
FSx para ONTAP	Puertos 443 y 22 del grupo de seguridad de Link Lambda o del agente Console	N/A
Enlace Lambda	Ninguno	Puerto 443 (ONTAP, AWS APIs) y puerto 22 (ONTAP SSH)
Agente de consola EC2	Ninguno	Puerto 443 (endpoints de WF, ONTAP, API de AWS) y puerto 22 (SSH de ONTAP)
Puntos de conexión de VPC (opcional)	N/A	STS, FSx, S3, Secrets Manager, Lambda, CloudFormation

No se requiere acceso a Internet entrante para ningún componente de la VPC del cliente. Todas las conexiones son iniciadas desde el interior (sondeo del agente de la consola) o se invocan a través de las API de servicios de AWS (Lambda Invoke).

Opciones de ejecución de ONTAP para NetApp Workload Factory

Algunos flujos de trabajo de NetApp Workload Factory requieren operaciones nativas de ONTAP que no están disponibles a través de las API de AWS. Workload Factory ofrece dos opciones de ejecución que mantienen estas operaciones dentro de los límites de tu cuenta de AWS: un enlace Lambda que ejecuta operaciones de ONTAP desde dentro de tu VPC y un NetApp Console Agent que utiliza conectividad solo de salida desde una instancia de EC2. Ambas opciones te permiten realizar las operaciones de ONTAP necesarias mientras mantienes las decisiones sobre red, credenciales y ciclo de vida dentro de tu modelo de seguridad.

Opciones de ejecución

Enlace de Lambda (AWS Lambda en tu VPC)

Ejecuta diagnósticos ONTAP REST y ONTAP CLI de solo lectura desde tu VPC, sin exponer ONTAP públicamente.

NetApp Console Agent (EC2 en tu VPC, solo salida)

Ejecuta operaciones ONTAP a través de un proxy, en las que el agente inicia las conexiones salientes y Workload Factory nunca inicia conexiones entrantes hacia el agente.

Consideraciones de seguridad

- Límites de red: confirma los puertos de salida necesarios (443/22) y los destinos.
- Límites de las credenciales: decide si las credenciales de ONTAP se almacenan en Workload Factory (con cifrado de envoltura) o se consultan desde AWS Secrets Manager.
- Auditabilidad: confirma los registros operativos de la actividad y los fallos de los componentes.
- Gestión del ciclo de vida: confirma cómo ocurren las actualizaciones y la eliminación.

Información relacionada

- "Descripción general de Lambda link para NetApp Workload Factory"
- "Vías de conectividad y confianza para NetApp Workload Factory"
- "Cifrado y gestión de claves para NetApp Workload Factory"

Información de copyright

Información de la marca comercial