Modelo de seguridad y responsabilidades

Information Security for Workload Factory

NetApp
September 16, 2026

Tabla de contenidos

Modelo de seguridad y responsabilidades

Conoce el modelo de seguridad de NetApp Workload Factory

NetApp Workload Factory es un plano de control SaaS que te ayuda a gestionar y optimizar las cargas de trabajo que se ejecutan en Amazon FSx for NetApp ONTAP en tu entorno de AWS. Los resultados en materia de seguridad dependen de las responsabilidades compartidas entre NetApp, AWS y tu organización.

Modelo de seguridad a grandes rasgos

- Workload Factory utiliza un modelo de asumir rol de IAM para obtener credenciales temporales de AWS STS para llamar a las API de AWS en tu cuenta.
- Algunos flujos de trabajo requieren operaciones nativas de ONTAP que no están disponibles a través de las API de AWS; puedes ejecutar esas operaciones dentro de tu VPC utilizando componentes de ejecución implementados por el cliente (por ejemplo, Lambda link).
- Las señales de observabilidad (métricas, telemetría y registros operativos) facilitan la supervisión operativa y las investigaciones.

Preguntas clave de la revisión

- ¿Qué acceso necesita Workload Factory a tu cuenta de AWS (confianza de rol + permisos)?
- ¿Qué vías de ejecución se aplican a los flujos de trabajo que tienes previstos (solo API de AWS u operaciones nativas de ONTAP a través de un componente de VPC)?
- ¿Qué categorías de datos se gestionan (configuración/metadatos, registros operativos/eventos, telemetría) y dónde se almacenan?
- ¿Qué señales de monitorización existen y cuáles son sus características de retención?

Qué sigue

- "Límites de responsabilidad compartida para NetApp Workload Factory"
- "Vías de conectividad y confianza para NetApp Workload Factory"
- "Niveles de permisos de menor privilegio para NetApp Workload Factory"

Límites de responsabilidad compartida para NetApp Workload Factory

NetApp Workload Factory tiene una responsabilidad de seguridad compartida entre NetApp (operación SaaS), AWS (infraestructura en la nube y servicios gestionados) y tú (configuración del cliente). Entender dónde empiezan y terminan las responsabilidades de cada parte te ayuda a configurar correctamente tu entorno de AWS y evitar brechas de seguridad. Estos límites aclaran qué opera NetApp, qué protege AWS y qué debes configurar y mantener tú mismo.

NetApp responsabilidades (lado del servicio)

NetApp se encarga de operar y asegurar la plataforma SaaS Workload Factory. Esto incluye la gestión del lado del servicio de las referencias de configuración almacenadas y los datos operativos.

Responsabilidades de AWS (plataforma en la nube)

AWS es responsable de la seguridad de la infraestructura en la nube y de los servicios gestionados que utilizan tu implementación y tus flujos de trabajo (por ejemplo, IAM/STS, FSx for ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda y los componentes básicos de red).

Responsabilidades del cliente (tu configuración)

Eres responsable de:

- Roles de AWS IAM, políticas de confianza y permisos de privilegios mínimos
- Controles de VPC (subredes, grupos de seguridad, enrutamiento, endpoints y egress)
- Gobernanza de credenciales (incluidas las credenciales de ONTAP si así lo requieren tus flujos de trabajo)
- Decisiones relativas al cifrado y la gestión de claves (por ejemplo, claves KMS opcionales gestionadas por el cliente para FSx for ONTAP)
- Supervisión, alertas, políticas de retención y procesos de respuesta ante incidentes

Evidencia que hay que recopilar

- Relación de confianza de roles de IAM (incluida la condición de external ID)
- Selección del nivel de permisos de IAM y artefactos de políticas
- Decisión sobre los límites de la red (solo API de AWS vs un componente de ejecución de VPC como Lambda link)
- Decisiones sobre la observabilidad y expectativas de retención
- Decisión sobre la activación de la IA (los diagnósticos de IA están activados por defecto a menos que se desactiven explícitamente)

NetApp flujo de trabajo de seguridad de incorporación a Workload Factory

La incorporación a NetApp Workload Factory establece un acceso seguro a tu entorno de AWS antes de que comiences a utilizar el producto. El proceso combina la configuración de confianza de AWS, la delimitación de permisos, la configuración de la conectividad, la verificación de la observabilidad y la activación opcional de diagnósticos de IA.

Paso 1: Decide tu postura de incorporación

- Identifica las cuentas de AWS y los límites del entorno (por ejemplo, separación entre prod y no prod).
- Identifica los flujos de trabajo necesarios (descubrimiento de solo lectura vs aprovisionamiento vs operaciones nativas de ONTAP).
- Decide si deseas implementar componentes de ejecución de VPC (por ejemplo, Lambda link) en función de las necesidades del flujo de trabajo.

- Decide si quieres activar el diagnóstico mediante IA (activado por defecto).

Información relacionada

- "Tipos de credenciales"
- "Descripción general de Lambda link"
- "Resumen de los controles de IA"

Paso 2: Establece la relación de confianza y el acceso a AWS

1. Implementa un rol de IAM en tu cuenta de AWS.
2. Asunción de un rol de gate mediante un identificador externo en la política de confianza.
3. Registra el ARN del rol y el ID externo en Workload Factory.

Información relacionada

"Integración de la cuenta de AWS"

Paso 3: aplica el principio del mínimo privilegio

1. Selecciona el nivel mínimo de permisos que admita tus flujos de trabajo previstos.
2. Comprueba que las políticas de sesión por solicitud limiten las acciones a la operación que se está realizando.

Información relacionada

"Niveles de permisos de menor privilegio para NetApp Workload Factory".

Paso 4: Configura la conectividad y los límites de la VPC (según sea necesario)

1. Valida las rutas de red necesarias para los endpoints de AWS.
2. Si necesitas operaciones nativas de ONTAP, implementa y verifica la opción de ejecución adecuada en tu VPC.

Información relacionada

- "Vías de conectividad y confianza para NetApp Workload Factory"
- "Opciones de ejecución de ONTAP para NetApp Workload Factory"

Paso 5: verifica la observabilidad

1. Comprueba que las métricas y los datos de telemetría se recopilan y conservan según lo previsto.
2. Asegúrate de que puedes acceder a los registros operativos necesarios para la resolución de problemas y las investigaciones.

Información relacionada

- "Descripción general de la observabilidad para NetApp Workload Factory"
- "Métricas y telemetría para NetApp Workload Factory"

Paso 6: activar el diagnóstico mediante IA (opcional)

Los diagnósticos de IA están activados de forma predeterminada. Si los activas, comprueba que cumples los

requisitos previos y que los permisos de ámbito se limitan al mínimo necesario.

Información relacionada

- "Inclusión voluntaria de Bedrock para diagnósticos de IA de NetApp Workload Factory"
- "Límites de las herramientas de IA para NetApp Workload Factory"

Cumplimiento y postura de seguridad para NetApp Workload Factory

NetApp Workload Factory se ha diseñado teniendo como prioridades fundamentales el cumplimiento normativo y la seguridad. Todas las cargas de trabajo de Workload Factory se ejecutan en Amazon FSx for NetApp ONTAP. Además de "Funciones de seguridad de AWS", NetApp Workload Factory cuenta con "SOC2 Type 1, SOC2 Type 2 e HIPAA compliance".

Amazon FSx para NetApp ONTAP para NetApp Workload Factory es un "Solución de AWS para la implementación de aplicaciones empresariales" y sigue las prácticas recomendadas de AWS Well-Architected.

Información de copyright

Información de la marca comercial