



# **Gobernanza de datos, privacidad y ciclo de vida**

## **Information Security for Workload Factory**

NetApp  
September 16, 2026

# Tabla de contenidos

- Gobernanza de datos, privacidad y ciclo de vida ..... 1
  - Gestión y residencia de datos para NetApp Workload Factory ..... 1
    - Clases de datos gestionadas por Workload Factory ..... 1
    - Clases de datos conservadas por Workload Factory ..... 1
    - Dónde se conserva la información. .... 1
    - Durante cuánto tiempo se conserva la información. .... 2
    - Qué información sale de la VPC ..... 2
    - Ámbito de configuración y recopilación de metadatos. .... 3
  - Cifrado y gestión de claves para NetApp Workload Factory ..... 6
    - Ámbito de cifrado en reposo de KMS para FSx. .... 7
    - Protección de credenciales (cifrado de envoltura del lado del servidor) ..... 7
  - NetApp eliminación de la cuenta de Workload Factory ..... 8

# Gobernanza de datos, privacidad y ciclo de vida

## Gestión y residencia de datos para NetApp Workload Factory

NetApp Workload Factory organiza el manejo de datos en categorías que describen los datos de operaciones que procesa el servicio, cómo encaja cada clase de datos en el modelo de seguridad, dónde se almacenan los datos, cuánto tiempo se conservan y si salen del entorno del cliente. Las principales clases de datos incluyen la configuración y los metadatos, los registros y eventos operativos, y la telemetría. Los datos conservados pueden incluir instantáneas de configuración de FSx for ONTAP, referencias de credenciales, datos de uso y coste de IA, registros de auditoría y cachés de respuesta de corta duración. Las ubicaciones de almacenamiento y procesamiento varían según el tipo de datos: parte de la información permanece en la cuenta de AWS del cliente, mientras que otros datos de operaciones se almacenan en la cuenta de NetApp.

### Clases de datos gestionadas por Workload Factory

Workload Factory gestiona las siguientes clases de datos:

- Configuración y metadatos
- Registros operativos y eventos
- Telemetría

### Clases de datos conservadas por Workload Factory

Workload Factory almacena los siguientes datos:

- Instantáneas de configuración de FSx (actualizadas en cada escaneo)
- Referencias de credenciales de ONTAP o material de credenciales cifrado con el cifrado de envoltura de KMS (dependiendo del modo de credenciales seleccionado)
- Métricas de EDA
- CloudFormation plantillas (7 días `Expires` encabezado)
- Datos sobre el uso y el coste de la IA
- Registros de auditoría
- Redis almacena en caché (respuestas de FSx) con un TTL de 20 minutos

### Dónde se conserva la información

#### Cuenta de AWS

- Las contraseñas de administrador de ONTAP se almacenan en tu AWS Secrets Manager.
- Amazon Bedrock procesa la inferencia de IA (análisis EMS) utilizando el ARN de tu perfil de inferencia a través de un rol asumido por STS dentro de tu cuenta de AWS.

## Cuenta de NetApp

- Configuraciones de FSx, planes de equilibrio, configuraciones de ARP y límites de uso de IA
- Credenciales temporales de AWS STS (almacenadas en caché en Redis), cachés de respuestas, bloqueos y estado de la implementación
- CloudFormation/plantillas de Terraform, descriptores de configuración WAD e informes comprimidos
- Medición del uso de la IA y métricas de rendimiento del colector
- Métricas agregadas de EDA
- Registros de auditoría de acciones
- OpenTelemetry trazas

## Consideraciones relativas a la región

- Almacenados en regiones donde el servicio Amazon Bedrock está disponible.
- NetApp internal opera en `us-east-1` y `us-west-2`.

## Durante cuánto tiempo se conserva la información

Esta sección resume las categorías de retención. Consulta las páginas enlazadas para ver los valores detallados y el comportamiento de la política de retención.

- Retención de credenciales y de credenciales temporales de AWS STS: ["Conservación de credenciales para NetApp Workload Factory"](#)
- Retención de métricas operativas y de telemetría: ["Referencia sobre métricas y telemetría para NetApp Workload Factory"](#)
- Conservación de registros de auditoría: gobernada por la política de retención de la NetApp Console (no controlada por Workload Factory)

## Qué información sale de la VPC

Esta sección resume las categorías de datos salientes. Consulta las páginas enlazadas para obtener más detalles a nivel de protocolo y de funciones.

## Tráfico del plano de gestión hacia el servicio Workload Factory

En lo que respecta a las operaciones de gestión, la configuración de FSx, los metadatos de los volúmenes, los identificadores de recursos y los comandos operativos fluyen por HTTPS hacia el nivel de servicio de Workload Factory.

## Registros de auditoría en el NetApp Console Audit Service

Cada operación registrada envía la siguiente información:

- `accountId`
- `actionName`
- `status`
- `resourceId`

- `userId`
- `requestData`
- `responseData`
- `timestamps`
- `IP address`
- `workspaceId`

## **Análisis del tráfico mediante IA**

Los eventos del Sistema de Gestión de Emergencias (EMS) de FSx for ONTAP, los datos de latencia y los registros de errores enviados para el diagnóstico mediante IA se transmiten a Amazon Bedrock a través de tu cuenta de AWS utilizando tu perfil de inferencia configurado, así que este tráfico permanece dentro de tu entorno en lugar de llegar a los sistemas de NetApp.

Para obtener más información sobre el análisis del tráfico mediante IA, consulta:

- ["Descripción general de los controles de IA para NetApp Workload Factory"](#)
- ["Inclusión voluntaria de Bedrock para diagnósticos de IA de NetApp Workload Factory"](#)
- ["Límites de las herramientas de IA para NetApp Workload Factory"](#)

## **Tráfico de la API de servicio de AWS**

Consulta ["conectividad y rutas de confianza para NetApp Workload Factory"](#).

## **Recopilación de telemetría y métricas**

Consulta el ["Referencia sobre métricas y telemetría"](#).

# **Ámbito de configuración y recopilación de metadatos**

## **Nivel del sistema de archivos**

- Configuración del sistema de archivos (tipo de implementación Gen1/Gen2, capacidad de rendimiento, capacidad de almacenamiento, tipo de almacenamiento)
- Subred preferida, grupos de seguridad, configuración de VPC
- Metadatos de la clave de cifrado de KMS
- Etiquetas del sistema de archivos
- Estado del ciclo de vida del sistema de archivos
- Configuración de la ventana de mantenimiento

## **Nivel de volumen (completo)**

- Identidad y estado: nombre del volumen, UUID, tipo (rw/dp/lis), estilo (FlexVol/FlexGroup), estado (en línea/fuera de línea/restringido), hora de creación
- Capacidad: tamaño total, utilizada, disponible, utilizada físicamente, porcentaje utilizado, espacio ocupado por SSD, espacio ocupado por el grupo de capacidad, bytes de datos inactivos/porcentaje

- Clasificación por niveles: política (all/auto/none/snapshot\_only), días mínimos de enfriamiento
- QoS: nombre de la política de QoS asignada
- Configuración de NAS: ruta de enlace, asignación de políticas de exportación, permisos UNIX, estilo de seguridad (unix/ntfs/mixto)
- Instantáneas: tamaño de la reserva de snapshot, porcentaje/espacio utilizado, configuración de autodelete
- Eficiencia de los datos: tipo/estado de compresión, deduplicación, compactación, ahorro de espacio
- Tamaño automático: modo (aumentar/aumentar\_reducir/desactivado), tamaño mínimo/máximo, umbrales de aumento/reducción
- SnapLock: tipo (cumplimiento/empresa/sin\_snaplock), períodos de retención (mín/máx/por defecto), período de autocommit
- Clon: volumen primario/instantánea/máquina virtual de almacenamiento, es FlexClone, estado de división
- Inodos/archivos: máximo posible, máximo configurado, número utilizado
- Cifrado: estado activado/desactivado
- Tiempo de acceso: actualización de atime activada/desactivada y periodo de actualización
- SnapMirror: estado de protección, tipos de destino (nube/ONTAP)
- FlexGroup reequilibrio: porcentaje de desequilibrio, umbral máximo
- Movimiento de volumen: agregado de destino, estado del movimiento
- FlexCache tipo de endpoint: ninguno/caché/origen
- Etiquetas: etiquetas de volumen a nivel de ONTAP

### **Datos de la instantánea**

- Nombre de la instantánea, UUID, hora de creación, hora de caducidad
- Tamaño en bytes
- SnapMirror etiqueta
- SnapLock caducidad y estado de bloqueo
- Estado (válido/invalid/parcial)
- Comentarios de los usuarios
- Políticas de Snapshot: nombre, estado de activación, programación de copias (número, periodo de retención, nombre de la programación, prefijo, etiqueta de SnapMirror)

### **Políticas de exportación**

- Nombre de la política, ID, máquina virtual de almacenamiento asociada
- Reglas: lista de protocolos (NFS/CIFS/FlexCache), patrones de coincidencia de clientes, reglas de solo lectura, reglas de lectura/escritura, reglas de superusuario, índice/prioridad de reglas
- SUID, creación de dispositivos, modo chown, asignación de usuarios anónimos, ajustes de seguridad de NTFS para UNIX

### **Puntos de acceso S3**

- Estado del ciclo de vida (disponible/creando/eliminando/fallido/mal configurado)
- Fecha de creación, ARN, alias, nombre

- Usuario propietario de los archivos y tipo (UNIX/WINDOWS)
- Configuración de red (acceso a Internet vs acceso a VPC, ID de VPC)
- Etiquetas AWS
- Activación del análisis de metadatos, activación del registro en diario, ARN de CloudTrail

### **Protección contra ransomware (ARP)**

Workload Factory recopila tanto el estado de la configuración como los detalles de los eventos:

- Estado por volumen (activado/desactivado/simulación/en pausa)
- Probabilidad de ataque (ninguna/baja/moderada/alta)
- Informes de ataques con marcas de tiempo
- Parámetros de detección: umbrales de extensión de archivo, aumento de la tasa de cambio de nombre %, aumento de la tasa de entropía %, aumento de la tasa de creación/eliminación de archivos %
- Archivos sospechosos: ruta del archivo, nombre del archivo, formato del archivo, hora de sospecha, volumen asociado

### **Replicación / SnapMirror**

- UUID de la relación, estado, estado de salud
- Origen y destino (máquina virtual de almacenamiento, ruta, clúster)
- Estadísticas de transferencia (bytes transferidos, duración, hora de finalización, estado)
- Política (nombre, tipo: asíncrono/síncrono/continuo)
- Ajuste del acelerador
- Tiempo de retraso
- Motivos poco saludables (mensaje y código)
- Errores actuales de transferencia

### **iGroups**

- Nombre, UUID, protocolo (FCP/iSCSI/mixto), tipo de sistema operativo
- Iniciadores (IQN/WWPN), estado de conectividad, hora de la última vez visto
- Asignaciones de LUN (número de unidad lógica, detalles del LUN)

### **LUN**

- Nombre, UUID, número de serie, tipo de sistema operativo, estado habilitado
- Tamaño, espacio utilizado, configuración de thin provisioning
- Ubicación (volumen, nodo, ruta de la unidad lógica)
- Configuración de eliminación automática
- Estado del contenedor, estado asignado, estado de solo lectura
- Política de calidad de servicio (QoS)
- Métricas de rendimiento (IOPS, latencia, rendimiento por lectura/escritura/total)

- Pertenencia a un grupo de coherencia

## **FlexCache**

- Volumen de origen/máquina virtual de almacenamiento/clúster, tamaño de caché, ruta
- Reescritura activada, estado de la caché DR
- Configuración del tamaño relativo
- Rellenar automáticamente las rutas de los directorios
- Estado de la conexión entre la caché y el origen

## **Nivel de máquina virtual de almacenamiento**

- Nombre, UUID, estado (en ejecución/detenido), subtipo
- Protocolos habilitados/admitidos (NFS, CIFS, iSCSI, FCP, NVMe, S3)
- Servidores DNS y dominios
- Configuración del switch de servicio de nombres (passwd, group, hosts, etc.)
- Interfaces IP (nombre, dirección IP, servicios)
- Agregados asignados
- Estado predeterminado del volumen anti-ransomware
- Configuración de la aplicación de espacio
- Relaciones entre iguales (aplicaciones, estado, clúster remoto/máquina virtual de almacenamiento)

## **Nivel de agregado / de almacenamiento**

- Nombre del agregado, UUID, estado, estado del RAID
- Almacenamiento en bloque: número de discos, tamaño de RAID, espacio disponible/ocupado/total, espacio físico ocupado
- Almacenamiento en la nube utilizado
- Eficiencia: ratio, uso lógico, ahorro
- Cifrado, espejo, configuración de SnapLock
- Métricas de rendimiento (IOPS, latencia, rendimiento)

## **Métricas de utilización (EDA)**

- Frecuencia de recogida: cada 12 horas para capacidad/rendimiento; cada 20 minutos para latencia
- Granularidad: normalizada a aproximadamente 60 puntos de datos por intervalo de tiempo
- Detalles de retención y almacenamiento: ["Referencia sobre métricas y telemetría"](#)

# **Cifrado y gestión de claves para NetApp Workload Factory**

NetApp Workload Factory utiliza cifrado en reposo y define claramente las responsabilidades de gestión de claves tanto en Workload Factory como en los servicios de AWS. Para los sistemas de archivos Amazon FSx for NetApp ONTAP, puedes elegir tu propia clave de AWS KMS o usar la clave predeterminada gestionada por AWS, y FSx

for ONTAP realiza las operaciones criptográficas con esa clave. Workload Factory también utiliza cifrado de envoltente para proteger las credenciales de ONTAP almacenadas.

## Ámbito de cifrado en reposo de KMS para FSx

Al crear un sistema de archivos FSx for ONTAP a través de Workload Factory, puedes especificar, si lo deseas, tu propia clave de AWS KMS para el cifrado de datos en reposo. Si no especificas una clave, Workload Factory utiliza la clave FSx predeterminada gestionada por AWS.

### Qué está cifrado

Todos los datos almacenados en los volúmenes de EBS subyacentes que respaldan el sistema de archivos FSx for ONTAP (cifrado en reposo de AWS FSx).

### Titularidad de las claves

La clave KMS se encuentra en tu cuenta de AWS.

### Permisos necesarios para la selección y el uso de claves

Workload Factory requiere:

- `kms:DescribeKey`
- `kms:ListKeys`
- `kms:ListAliases`
- `kms:CreateGrant` (para permitir que el servicio FSx for ONTAP utilice la clave)

### Patrón de acceso clave

Workload Factory nunca cifra ni descifra directamente los datos con tu clave KMS. Pasa el ID de la clave a la API de Amazon FSx for NetApp ONTAP durante la creación del sistema de archivos; Amazon FSx for NetApp ONTAP realiza las operaciones criptográficas.

## Protección de credenciales (cifrado de envoltura del lado del servidor)

Cuando almacenas credenciales de ONTAP (contraseñas de administrador) a través de Workload Factory, las protege usando cifrado de sobre antes de guardarlas de forma permanente.

### Método de cifrado

AES-256-CBC con una clave de cifrado de datos (DEK) única para cada registro de credencial.

### Flujo de cifrado de sobre

1. Se genera una DEK única de 256 bits por cada credencial.
2. El DEK cifra la credencial (contraseña).
3. El propio DEK está cifrado con una clave raíz y se almacena junto con la credencial cifrada.
4. El DEK en texto sin cifrar nunca se almacena.

### Contexto de cifrado

Cada clave de datos está vinculada criptográficamente a su registro de credenciales específico, lo que impide la reutilización de la clave en distintos registros.

### Alternativa: AWS Secrets Manager

En lugar de almacenar contraseñas cifradas en el servicio, puedes guardar las credenciales de ONTAP en AWS Secrets Manager en tu propia cuenta. Workload Factory nunca ve ni almacena la contraseña; pasa el ARN de Secrets Manager a Lambda link, que recupera la contraseña en tiempo de ejecución dentro de tu VPC.



AWS Secrets Manager es obligatorio para las cuentas de GovCloud.

## NetApp eliminación de la cuenta de Workload Factory

La eliminación de la cuenta no es una operación de autoservicio; es un proceso de baja que implica tanto el servicio Workload Factory como los recursos en tu cuenta de AWS. La limpieza incluye eliminar de forma segura cualquier dato asociado con la cuenta de Workload Factory, los sistemas de archivos FSx for ONTAP, las credenciales, los enlaces, los canales de notificación y los recursos relacionados de IAM, AWS Lambda y Amazon CloudWatch. La operación es irreversible.

Cuando necesites eliminar tu cuenta de Workload Factory, debes ["Ponte en contacto con el soporte de NetApp."](#)

## Información de copyright

Copyright © 2026 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.