Identidad, credenciales y privilegio mínimo

Information Security for Workload Factory

NetApp
September 16, 2026

Tabla de contenidos

Identidad, credenciales y privilegio mínimo

Integración de cuentas de AWS para NetApp Workload Factory

Workload Factory utiliza AWS `sts:AssumeRole` para obtener credenciales temporales para tu cuenta de AWS, así que las claves de acceso de AWS a largo plazo no son almacenadas por el servicio. Durante la incorporación, configuras un rol de IAM que Workload Factory puede asumir para operaciones aprobadas de la API de AWS, usando un ID externo para ayudar a evitar el acceso no autorizado entre cuentas. Luego, Workload Factory usa las credenciales de corta duración resultantes en tiempo de ejecución, que AWS caduca automáticamente después de cada sesión.

Configuración de la cuenta de AWS

Para permitir que Workload Factory acceda a tu cuenta de AWS:

1. Implementa un rol de IAM en tu cuenta de AWS (utilizando CloudFormation o de forma manual).
2. Asegúrate de que la política de confianza del rol permita que el service principal de Workload Factory lo asuma, controlado por un ID externo.
3. Utiliza un identificador externo como identificador secreto único (UUID v4) compartido exclusivamente entre el cliente y Workload Factory.

   Incorpóralo como condición en la política de confianza de tu rol de IAM (`sts:ExternalId`).

   El identificador externo evita los ataques de «confused deputy». En un modelo de acceso entre cuentas, un atacante que descubra el ARN de un rol de un cliente no puede asumir ese rol sin poseer también el identificador externo correspondiente. AWS recomienda este patrón para el acceso entre cuentas de terceros. Para obtener más información, consulta la página de documentación de AWS IAM "Acceso a cuentas de AWS propiedad de terceros".

   El identificador externo se genera una sola vez durante el proceso de incorporación de credenciales y se almacena cifrado junto con el ARN del rol en una base de datos de Workload Factory.
4. Registra el ARN del rol y el ID externo en Workload Factory.

Duración

Durante la ejecución, Workload Factory asume tu rol de IAM para obtener credenciales de corta duración para cada operación de la API de AWS:

1. Workload Factory realiza una llamada a `sts:AssumeRole` con el ARN de tu rol y el ID externo.
2. AWS devuelve credenciales temporales (clave de acceso, clave secreta y token de sesión).
3. Workload Factory utiliza las credenciales temporales para las operaciones de la API de AWS en tu cuenta.
4. Las credenciales caducan automáticamente (por defecto, una hora).

Cómo circulan las credenciales de AWS a través de NetApp Workload Factory

El flujo de credenciales de AWS describe cómo NetApp Workload Factory gestiona los identificadores de rol, los ID externos y las credenciales de AWS STS de corta duración durante la incorporación y las operaciones en tiempo de ejecución. Durante la configuración inicial, creas un rol de IAM en tu cuenta de AWS y configuras una política de confianza que requiere el servicio principal de Workload Factory y el ID externo correcto. En tiempo de ejecución, Workload Factory utiliza el ARN del rol almacenado y el ID externo para solicitar credenciales temporales limitadas por una política de sesión por solicitud, y reutiliza las credenciales almacenadas en caché hasta que expiran.

Configuración única

Para una configuración inicial, el proceso es el siguiente:

Pasos

1. Inicias una pila de CloudFormation o creas manualmente un rol de IAM en tu cuenta de AWS.
2. La política de confianza de roles de IAM especifica dos condiciones:
   a. Solo la entidad de servicio de Workload Factory puede asumirlo.
   b. La persona que llama debe presentar el ID externo correcto.
3. Workload Factory almacena el ARN del rol y el identificador externo (cifrado) en su base de datos.

Tiempo de ejecución (cada operación de la API)

Durante la ejecución, Workload Factory utiliza el ARN del rol almacenado y el ID externo para obtener credenciales temporales de AWS STS para cada operación de API. El flujo es el siguiente:

Pasos

1. Workload Factory recupera el ARN del rol y el ID externo almacenados en MySQL.
2. Comprueba en Redis si hay un conjunto almacenado en caché de credenciales temporales de AWS STS para este rol.
3. Cuando se produce una falta de acierto en la caché, Workload Factory llama a `sts:AssumeRole` con el ARN del rol y el ID externo. La llamada incluye una política de sesión en línea por solicitud que restringe los permisos únicamente a las acciones específicas de AWS necesarias para esa operación.
4. AWS STS devuelve credenciales temporales (access key ID, secret access key, session token) con una marca de tiempo de expiración.
5. Workload Factory almacena estas credenciales en caché en Redis y las utiliza para llamar a las API de AWS de destino.
6. Si se produce una coincidencia en la caché, Workload Factory omite la llamada a STS y utiliza directamente las credenciales almacenadas en caché.

Política de sesión

Cada llamada STS incluye una política de sesión integrada cuyo ámbito se limita a las acciones mínimas requeridas en AWS.

Información relacionada

- "Niveles de permisos de menor privilegio"

Retención de credenciales de AWS para NetApp Workload Factory

Workload Factory garantiza la seguridad en la gestión de credenciales mediante credenciales STS de AWS de corta duración, metadatos de roles cifrados y un comportamiento de retención limitado. El modelo de credenciales separa los metadatos de roles conservados de las credenciales temporales de AWS utilizadas para las operaciones de API. Las credenciales temporales se almacenan en caché solo durante un periodo limitado y caducan automáticamente según las normas de AWS. Al eliminar una credencial, se impide que Workload Factory obtenga nuevas credenciales para la cuenta, mientras que las credenciales almacenadas en caché caducan poco después.

Comportamientos clave

- Workload Factory no almacena claves de acceso de AWS a largo plazo.

  Workload Factory solo almacena un puntero (ARN de rol) y un secreto compartido (ID externo). Ninguno de los dos permite por sí solo el acceso a AWS.

- Las credenciales temporales de AWS STS tienen una duración máxima fija de una hora (impuesta por AWS).

  Workload Factory los almacena en caché en Redis durante un máximo de 30 minutos antes de forzar una nueva llamada a STS.

- Si a un conjunto de credenciales almacenado en caché le quedan menos de 15 minutos de validez, Workload Factory lo descarta y obtiene uno nuevo.
- La eliminación de las credenciales por parte del cliente revoca inmediatamente la capacidad de Workload Factory para acceder a esa cuenta.

  La siguiente llamada a AssumeRole falla, y las credenciales almacenadas en caché caducan en cuestión de minutos.

Resumen de retención y almacenamiento

Datos	Lugar de almacenamiento	Duración de retención	¿Caduca automáticamente?	Método de eliminación
ARN del rol de IAM + ID externo	MySQL (cifrado en reposo)	Indefinido (se conserva hasta que el cliente lo elimine expresamente)	No	El cliente hace clic en «Eliminar credencial» en la interfaz de usuario

Datos	Lugar de almacenamiento	Duración de retención	¿Caduca automáticamente?	Método de eliminación
Credenciales temporales de AWS STS (clave de acceso + secreto + token de sesión)	Redis (caché en memoria)	Máximo 30 minutos (TTL de la caché). Las credenciales STS subyacentes son válidas hasta una hora (AWS por defecto). La caché elimina los datos cinco minutos antes de que caduquen como margen de seguridad.	Sí (Redis elimina automáticamente los datos al vencimiento del TTL; AWS aplica el vencimiento de las credenciales de AWS)	Automático
Contraseña de administrador de ONTAP	MySQL (cifrado de envoltura AES-256-CBC mediante KMS)	Indefinido (se almacena hasta que el cliente elimine la credencial o borre el sistema de archivos)	No	El cliente elimina la credencial o la eliminación del sistema de archivos activa la limpieza
Contraseña de ONTAP descifrada (texto sin cifrar)	Solo en memoria (nunca se guarda en disco ni en caché)	Duración de una sola solicitud (milisegundos)	Sí (la memoria se libera una vez finalizada la solicitud)	Automático

Controles de seguridad

- El identificador externo evita los ataques de deputy confusos.
- Las políticas de sesión aplican el principio de privilegios mínimos por solicitud.
- Workload Factory actualiza las credenciales temporales de AWS STS de corta duración antes de los periodos de caducidad que suponen un riesgo.
- El manejo de las regiones y los tipos de cuenta es diferente para los entornos Standard, GovCloud y China.
- Workload Factory nunca almacena claves de acceso de AWS a largo plazo.
- Workload Factory nunca modifica los permisos de tu rol de IAM.
- Workload Factory nunca supera los permisos concedidos por la política de tu rol.
- Las políticas de sesión solo pueden restringir los permisos; Workload Factory nunca los amplía.

Tipos de credenciales para NetApp Workload Factory

NetAppWorkload Factory utiliza un modelo de credenciales separadas para diferenciar los permisos del plano de control de AWS del acceso administrativo directo a ONTAP. El rol de IAM de AWS autentica a Workload Factory ante las API de AWS para operaciones como la gestión del sistema de archivos, la gestión de backup y la detección de recursos. Las credenciales de ONTAP autentican el acceso directo al punto final de gestión de ONTAP mediante un enlace Lambda para operaciones que requieren configuración administrativa o diagnósticos. Algunos flujos de trabajo requieren ambos tipos de credenciales cuando combinan operaciones de la API de AWS con tareas directas de gestión de ONTAP.

Tipos de credenciales

La siguiente tabla resume los dos tipos de credenciales que se utilizan en Workload Factory y sus respectivos objetivos de autenticación.

Tipo de credencial	Se autentica en	Se utiliza para
Credenciales de AWS (AssumeRole)	API de AWS	Todas las operaciones que se realizan a través de la API del servicio AWS FSx
Credenciales de ONTAP (contraseña de admin)	Punto final de gestión de ONTAP	Operaciones que requieren acceso directo a la API de REST de ONTAP o a la CLI

Operaciones de AWS que solo requieren credenciales

Estas operaciones interactúan exclusivamente con las API de AWS y solo requieren el rol de IAM:

- Creación y eliminación de sistemas de archivos
- Cambios en la capacidad y el rendimiento del sistema de archivos
- Creación y gestión de backup
- Detección de VPC, subred y grupo de seguridad
- Enumeración de claves KMS
- CloudWatch recuperación de métricas
- Consultas de Cost Explorer
- Gestión de etiquetas mediante la API de FSx

Operaciones solo con credenciales de ONTAP

Estas operaciones se comunican directamente con el punto final de gestión de ONTAP a través del enlace Lambda y requieren credenciales de administrador de ONTAP:

- Configuración de la política de QoS a nivel de volumen
- Política de exportación y gestión de reglas
- Configuración del protocolo de storage VM (NFS, CIFS, iSCSI)
- Gestión de igroup y LUN

- SnapMirror (configuración de replicación)
- Gestión de políticas de Snapshot (a nivel de ONTAP)
- Diagnóstico del rendimiento (estadísticas de QoS, desglose de la latencia)
- Recuperación y análisis de eventos EMS
- Supervisión del estado de la protección contra ransomware
- Gestión de FlexCache
- Consultas sobre interfaces de red (LIF)

Operaciones que requieren credenciales tanto de AWS como de ONTAP

Flujo de trabajo	Credencial de AWS utilizada para	Credencial de ONTAP utilizada para
Análisis de eventos basado en inteligencia artificial	Invoca Bedrock, describe el sistema de archivos	Recupera eventos de EMS y ejecuta diagnósticos usando SSH
Creación del sistema de archivos con la configuración de la storage VM	Crear sistema de archivos (API de AWS)	Configura los protocolos de las máquinas virtuales de almacenamiento (ONTAP REST)
Creación de volúmenes con política de exportación	Crear volumen (AWS API)	Configura reglas de política de exportación (ONTAP REST)
Gestión de la capacidad de almacenamiento	Actualizar la capacidad del sistema de archivos (AWS API)	Comprobar la utilización del agregado (ONTAP SSH)

Información relacionada

- "Opciones de ejecución de ONTAP"
- "Descripción general de Lambda link"

Opciones de almacenamiento de credenciales para NetApp Workload Factory

NetApp Workload Factory admite patrones de gestión de credenciales que preservan el principio de privilegio mínimo y reducen la exposición de los secretos administrativos de ONTAP. Las funciones de diagnóstico impulsadas por IA utilizan credenciales de ONTAP de solo lectura cuando están disponibles, así el agente de diagnóstico puede observar y diagnosticar sin modificar el entorno de almacenamiento. Puedes usar almacenamiento cifrado gestionado por Workload Factory o guardar la contraseña de ONTAP en AWS Secrets Manager y darle a Workload Factory una referencia. La elección afecta dónde se almacena la contraseña, cómo se cifra y cómo gestionas requisitos como la compatibilidad con GovCloud y la rotación de credenciales.

Modelo de acceso de solo lectura a ONTAP

Para funciones basadas en IA, como el análisis de eventos y el diagnóstico de latencia, Workload Factory utiliza credenciales ONTAP de solo lectura cuando están disponibles. El modelo de credenciales de solo

lectura garantiza que el agente de diagnóstico de IA no pueda realizar modificaciones en tu entorno de almacenamiento; solo puede observar y diagnosticar.

Comparativa de opciones de almacenamiento de credenciales

Credenciales AWS

Las credenciales de AWS siempre se asumen a través de un rol de IAM. Workload Factory puede gestionar la información del rol internamente o consultarla en AWS Secrets Manager.

Opción	Credenciales AWS	Qué se almacena	Cifrado
Workload Factory gestionado	ARN del rol de IAM + ID externo	ARN del rol de IAM + ID externo	El ARN del rol no es confidencial (se almacena tal cual)

Credenciales ONTAP

Workload Factory puede gestionar las credenciales de ONTAP internamente con almacenamiento cifrado o hacer referencia a ellas desde AWS Secrets Manager. La elección afecta cómo se almacena, se cifra y se rota la contraseña.

Se requieren credenciales de ONTAP para que Workload Factory interactúe con las API del sistema de archivos ONTAP a través de un "Enlace Lambda".

Opción	Credenciales ONTAP	Qué se almacena	Cifrado
Workload Factory gestionado	Contraseña (cifrada)	Contraseña de administrador de ONTAP (cifrada)	La contraseña de ONTAP utiliza cifrado de envolvente AES-256
AWS Secrets Manager	Referencia ARN de Secrets Manager	Secrets Manager ARN	Secrets ARN no es un secreto (se almacena tal cual); AWS Secrets Manager cifra el secreto en tu cuenta

Consideraciones adicionales

GovCloud requisito

Se utiliza un rol IAM estándar; las credenciales de ONTAP deben usar Secrets Manager (no se permite el almacenamiento de contraseñas).

Rotación

Las políticas de roles se han actualizado en tu cuenta. Actualiza la contraseña de ONTAP en Workload Factory (opción gestionada) o rótala en AWS Secrets Manager.

Niveles de permisos de menor privilegio para NetApp Workload Factory

Puedes restringir los permisos de IAM de Workload Factory en cualquier momento para

ajustarlos a los requisitos de privilegio mínimo, como limitar el acceso a recursos específicos (ARNs) y aplicar condiciones de IAM, por ejemplo, etiquetas y rangos CIDR.

Modelo de permisos por niveles

Workload Factory utiliza un modelo de permisos por niveles que se ajusta al principio de menor privilegio. Tú eliges qué niveles de capacidades deseas habilitar al añadir credenciales de AWS. Puedes empezar con un acceso de solo lectura y ampliarlo según sea necesario.

Workload Factory concede todos los permisos a través de un rol de IAM en tu cuenta de AWS, que asume mediante STS con un identificador externo.

Workload Factory amplía aún más el alcance de cada llamada a la API mediante una política de sesión integrada.

En la consola de Workload Factory, la función de chat con IA *Ask Me* te ayuda a ajustar los permisos de forma segura, sugiriéndote opciones de restricción y generando una política actualizada para aplicar en AWS.

Concesión de permisos

Al añadir credenciales de AWS a Workload Factory, puedes elegir qué niveles de permisos deseas habilitar. Puedes habilitar o deshabilitar los niveles en cualquier momento.

Los niveles son acumulativos: al activar un nivel superior, se activan automáticamente todos los niveles inferiores.

Controles de seguridad

- Identificador externo (protección contra la confusión de cargos)
- Políticas de sesión por operación (privilegio mínimo por solicitud)
- Condiciones basadas en etiquetas (modificaciones de los grupos de seguridad limitadas a los recursos creados por Workload Factory)
- Ámbito de ARN secreto (acceso a Secrets Manager restringido a `FSxSecret*`)
- Validación de permisos en tiempo de ejecución (falta acción/recurso reportado para remediación específica)

Documentación sobre permisos

La referencia principal para los permisos de Workload Factory es la "Referencia sobre permisos" en la documentación de configuración y administración de Workload Factory. Aquí puedes encontrar información sobre los impactos de eliminar permisos de las políticas de IAM de almacenamiento.

Permisos de supervisión de Amazon CloudWatch para NetApp Workload Factory

Los permisos de supervisión de Amazon CloudWatch son opcionales en NetApp Workload Factory y solo se aplican cuando despliegas la pila de supervisión independiente. La pila de supervisión proporciona visibilidad operativa al recopilar métricas del sistema de archivos, publicar registros de eventos, gestionar paneles y

alarmas de CloudWatch y enviar notificaciones de alerta a través de Amazon SNS. La pila también requiere acceso para recuperar las credenciales de ONTAP cuando se necesiten para la supervisión.

Permisos necesarios de supervisión de CloudWatch

Se requieren los siguientes permisos para la pila de monitorización opcional:

Permiso	Propósito
fsx:Describe* / fsx:ListTagsForResource	Recopila métricas del sistema de archivos
cloudwatch:PutMetricData / cloudwatch:PutDashboard / cloudwatch:PutMetricAlarm / cloudwatch:DescribeAlarms / cloudwatch:Delete*	Gestiona paneles de control y alarmas
registros:CreateLogGroup / registros:CreateLogStream / registros:PutLogEvents	Publicar registros de eventos
sns:Publish	Enviar notificaciones de alerta
secretsmanager:GetSecretValue	Recupera las credenciales de ONTAP para la supervisión

Información de copyright

Información de la marca comercial