



Asistente de IA Ask Me

Information Security for Workload Factory

NetApp

September 16, 2026

Tabla de contenidos

- Asistente de IA Ask Me 1
 - Arquitectura de seguridad de Ask Me para NetApp Workload Factory 1
 - Arquitectura RAG en Ask Me 1
 - Seguridad de comandos en varias capas 1
 - Aislamiento de datos de modelos y privacidad 1
 - Uso de herramientas y seguridad agénica 2
 - Control de acceso de Ask Me para NetApp Workload Factory 2
 - Autenticación 2
 - Protección de credenciales y gestión de secretos 2
 - Seguridad de la infraestructura 2
 - Modos de ejecución de Ask Me para NetApp Workload Factory 3
 - Salvaguardas para la ejecución de herramientas 3
 - Controles de salida 3
 - Consúltame sobre la privacidad y la disponibilidad de NetApp Workload Factory 3
 - Tratamiento de datos y privacidad 4
 - Controles de disponibilidad y aislamiento 4

Asistente de IA Ask Me

Arquitectura de seguridad de Ask Me para NetApp Workload Factory

Ask Me es un asistente potenciado por IA generativa integrado en NetApp Workload Factory. Ofrece asistencia conversacional en tiempo real para temas de Amazon FSx for NetApp ONTAP y Workload Factory. Las respuestas se basan en documentación verificada de NetApp, y Ask Me no puede acceder a internet pública ni usar datos de clientes para entrenar el modelo. Varias capas de seguridad ayudan a bloquear consultas maliciosas, limitar las respuestas a los dominios admitidos y evitar que la entrada del usuario sobrescriba las instrucciones del sistema. Cuando Ask Me usa herramientas, los límites de autorización, la aplicación de consultas de solo lectura, un entorno temporal de pruebas y el registro de auditoría ayudan a restringir y monitorear la ejecución.

Puedes desactivar Ask Me en cualquier momento a través de la configuración de **Administración** de Workload Factory, lo que desactiva el asistente para tu cuenta de usuario. ["Obtén más información sobre cómo gestionar las funciones de GenAI."](#)

Arquitectura RAG en Ask Me

Ask Me utiliza la generación aumentada por recuperación (RAG).

- Base de conocimientos seleccionada: las respuestas se basan en un corpus gestionado de documentación verificada y publicada de NetApp.
- Puntuación y filtrado de recuperación: solo se incluye en el contexto del modelo el contenido que resulta suficientemente relevante.
- Sin acceso a Internet: el modelo no puede recuperar, navegar ni extraer contenido externo.
- Atribución de fuentes: las respuestas incluyen referencias a los documentos fuente utilizados.

Seguridad de comandos en varias capas

- Capa 1: El clasificador de seguridad (LLM-as-a-judge) bloquea las consultas maliciosas (inyección de comandos, escalada de privilegios, exfiltración de datos, ingeniería social, incumplimientos de políticas).

El sistema registra las consultas bloqueadas, y el modelo generativo nunca las ve.

- Nivel 2: El refuerzo de las indicaciones del sistema impide que la entrada del usuario anule las instrucciones del sistema.
- Capa 3: el ámbito del dominio limita las respuestas a los temas de FSx ONTAP y Workload Factory.
- Capa 4: El control del uso de herramientas valida los parámetros y ejecuta consultas en un entorno aislado reforzado; el modelo no puede ejecutar operaciones arbitrarias.

Aislamiento de datos de modelos y privacidad

- No se ha realizado ningún entrenamiento de modelos con datos de clientes
- Aislamiento a nivel de solicitud (sin fuga de datos entre inquilinos)

- Contexto de conversación con ámbito de sesión y historial limitado
- Sin memoria persistente de modelos
- Infraestructura de inferencia gestionada

Uso de herramientas y seguridad agénica

- Herramientas con ámbito de autorización (se aplican los límites de permisos de usuario)
- Tiempos de espera estrictos para la ejecución de herramientas
- Entorno de pruebas efímero, con ámbito de sesión para los datos recuperados
- Aplicación de consultas de solo lectura mediante allowlisting
- Auditabilidad de las llamadas a herramientas mediante el ocultamiento de parámetros confidenciales

Control de acceso de Ask Me para NetApp Workload Factory

En NetApp Workload Factory, la seguridad de acceso a Ask Me se centra en sesiones autenticadas, responsabilidad a nivel de usuario y gestión protegida de secretos durante las operaciones en tiempo de ejecución. Los controles de autenticación validan cada sesión y asocian las interacciones con un usuario específico. Las credenciales confidenciales se recuperan de un almacén de secretos gestionado en tiempo de ejecución y se ocultan en los registros. El servicio también aplica controles de infraestructura, incluyendo la ejecución de contenedores sin privilegios de root y una lista restringida de permitidos para CORS.

Autenticación

- Autenticación mediante JWT firmado con validación criptográfica (incluyendo comprobaciones de destinatario, emisor y algoritmo como RS256)
- Autenticación gestionada por middleware en el límite del servicio
- Delimitar el ámbito de identidad del usuario para que las interacciones se puedan atribuir a un usuario concreto

Protección de credenciales y gestión de secretos

- Almacenamiento seguro en un almacén de secretos: las credenciales confidenciales que utiliza el servicio se almacenan en un almacén de secretos gestionado y se recuperan en tiempo de ejecución. No se almacena ningún secreto en el código de la aplicación, en los archivos de configuración ni en las imágenes de contenedor.
- Limpieza de registros: los valores sensibles (credenciales, tokens, contraseñas, claves de acceso, certificados) se eliminan de los registros antes de que se escriban.

Seguridad de la infraestructura

- Ejecución de contenedores sin privilegios de root
- CORS restringido a una lista explícita de dominios de confianza NetApp

Modos de ejecución de Ask Me para NetApp Workload Factory

NetApp Workload Factory ofrece varios modos de ejecución para Ask Me, cada uno con diferentes características de seguridad y privacidad. Cuando Ask Me utiliza integraciones con herramientas, por ejemplo, al consultar los propios recursos de Workload Factory del cliente, la ejecución de las herramientas se controla mediante medidas de seguridad por capas. La ejecución habilitada por herramientas opera dentro de los permisos del usuario autenticado y aplica límites a la duración y al alcance de cada operación. Los datos recuperados permanecen en un entorno de pruebas de sesión efímero que bloquea el acceso externo y se destruye cuando finaliza la sesión. Los controles independientes de solicitudes y código imponen consultas de solo lectura, mientras que los registros de auditoría capturan la actividad de la herramienta con los valores sensibles ocultos.

Salvaguardas para la ejecución de herramientas

- Las herramientas con ámbito de autorización funcionan dentro de los permisos del usuario autenticado.
- El tiempo de espera de ejecución de la herramienta limita las operaciones de larga duración.
- El entorno de pruebas de datos efímeros almacena los datos recuperados por las herramientas en el ámbito de la sesión, bloquea el acceso externo, las operaciones de E/S de archivos, las llamadas de red y la carga de extensiones a nivel del motor, y se elimina cuando finaliza la sesión.
- La aplicación de consultas de solo lectura valida las consultas generadas mediante una lista de permitidos muy estricta.
- La seguridad basada en mensajes de aviso y la basada en código se aplican de forma independiente.
- La herramienta de auditabilidad registra el nombre de la herramienta, los parámetros, las marcas de tiempo y el estado del resultado, con el ocultamiento de los valores confidenciales.

Controles de salida

- Aplicación del límite de tokens
- Salida determinista para operaciones de clasificación o críticas para la seguridad (temperatura 0)
- Transmisión con finalización anticipada y limpieza

Consúltame sobre la privacidad y la disponibilidad de NetApp Workload Factory

En NetApp Workload Factory, los controles de privacidad de Ask Me limitan la exposición de los datos, mantienen aislado el procesamiento de las sesiones y preservan los límites de privacidad en las interacciones de los usuarios. Tus entradas son procesadas por un servicio de IA gestionado que no las utiliza para entrenar ni mejorar modelos base. Los datos de operaciones recuperados permanecen en un almacenamiento efímero en memoria durante toda la sesión y no se conservan ni se comparten. Una cadena de reserva multimodelo que abarca varias regiones de la nube garantiza la disponibilidad cuando el modelo principal está limitado o no está disponible, mientras que se aplican los

mismos controles de seguridad en todos los modelos de reserva.

Tratamiento de datos y privacidad

- Datos de usuario en las indicaciones: procesados por un servicio de IA gestionado que no utiliza tus entradas para entrenar ni mejorar los modelos base.
- Contenido de la base de conocimientos: solo documentación seleccionada y publicada de NetApp; tus datos no están incluidos.
- Datos operativos: se recuperan solo cuando un usuario consulta sus propios recursos; se almacenan de forma efímera en la memoria durante la sesión y no se guardan ni se comparten.
- Registro de auditoría: se registran los metadatos de las consultas (ID de usuario anonimizado, marcas de tiempo, duraciones), con los campos sensibles eliminados.
- Datos de comentarios: se almacenan por separado y se vinculan a un identificador de consulta, no a información que permita identificar personalmente más allá del identificador de usuario anonimizado.

Controles de disponibilidad y aislamiento

Ask Me utiliza una cadena de respaldo multimodelo que abarca varias regiones en la nube.

Si el modelo principal se ve limitado o no está disponible, el sistema puede recurrir a modelos alternativos.

Todos los modelos están sujetos a los mismos controles de seguridad, refuerzo de las indicaciones del sistema y garantías de aislamiento.

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.