



Configura las integraciones y los servicios de NetApp Console

NetApp Console local deployment

NetApp
August 10, 2026

Tabla de contenidos

- Configura las integraciones y los servicios de NetApp Console 1
 - Integra la implementación local de NetApp Console con Active Directory 1
 - Antes de empezar 1
 - Desactivar o activar una integración con Active Directory 2
 - Eliminar una integración con Active Directory 2
 - Conecta tu LLM y activa el asistente de NetApp Console en la implementación local de NetApp Console . . 3
 - Reúne todo lo que necesites antes de conectar un LLM 3
 - Conecta un LLM a la implementación local de NetApp Console 4
 - Comprueba que la integración de LLM funcione 4
 - Protege las credenciales y supervisa el uso de los modelos de lenguaje grande (LLM) 4
 - Soluciona problemas de la integración de LLM en la implementación local de NetApp Console 5
 - Soluciona rápido los problemas de integración de Triage LLM 5
 - Solucionar problemas según los síntomas 5
 - Responde ante la divulgación o el uso indebido de credenciales de LLM 6
 - Configura los canales de entrega de notificaciones en la implementación local de NetApp Console 6
 - Configura un servidor de correo electrónico 7
 - Configura un webhook 8

Configura las integraciones y los servicios de NetApp Console

Integra la implementación local de NetApp Console con Active Directory

Integra la implementación local de NetApp Console con Active Directory para el inicio de sesión respaldado por directorio y la búsqueda de usuarios. Usa tu servicio de directorio para autenticar a los usuarios y luego asígnale acceso en la implementación local de NetApp Console.

Roles de acceso necesarios

Superadministrador o administrador de la organización. ["Conoce los roles de acceso"](#).

Cuando integras con Active Directory, la implementación local de Console autentica a los usuarios a través de tu directorio existente. Después de agregar un usuario del directorio, asígnale roles de acceso a Console para controlar a qué puede acceder ese usuario.

La integración con Active Directory también te ayuda a cumplir los requisitos de cumplimiento al aplicar tus controles, registros de auditoría y políticas existentes al acceso local de Console.



- La integración con Active Directory no crea grupos federados, no sincroniza las asignaciones de grupos del directorio y no concede acceso automáticamente. Los administradores siguen añadiendo usuarios del directorio a la organización y asignando roles en la implementación local de Console.
- Solo se admite una integración con Active Directory a la vez. Una vez configurada una integración, el botón **Add integration** queda desactivado. Para cambiar a otro directorio, primero debes desactivar o eliminar la integración existente.
- Los usuarios del directorio no configuran ni usan la autenticación multifactor (MFA). La implementación local de NetApp Console solo admite MFA para usuarios locales. ["Aprende a gestionar la configuración de seguridad de los miembros"](#).

Antes de empezar

Antes de integrar con Active Directory, comprueba que tienes:

- Un dominio de Active Directory y credenciales que permitan consultar el directorio
- La dirección del servidor LDAP y el nombre distintivo (DN) base del árbol de directorios
- Acceso de red desde la implementación local de Console a tu servidor LDAP en el puerto 389 (LDAP) o 636 (LDAPS)
- Certificados SSL/TLS, si tienes pensado utilizar LDAPS

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Directory services** para abrir la página Federations.
3. Selecciona **Add integration**.

4. Introduce los datos de conexión de tu servidor de Active Directory:
 - Un nombre descriptivo para la integración.
 - El **host LDAP**: nombre de host o dirección IP de tu servidor LDAP. Si hay varios servidores, introduce el principal.
 - El puerto: 389 para LDAP o 636 para LDAPS.
 - El **tiempo de espera de conexión** en milisegundos. El valor predeterminado es 1000 ms.
5. Selecciona **Usar SSL/TLS** para utilizar LDAPS. Asegúrate de que tu servidor LDAP sea compatible con LDAPS y que NetApp Console pueda acceder a los certificados necesarios.
6. Comprueba la conexión. Si falla, comprueba el host LDAP, el puerto, la conectividad de red y los certificados SSL/TLS.
7. Después de que la prueba finalice con éxito, introduce los datos del directorio y del usuario:
 - **Enlace al DN base**: Introduce el DN de enlace de la cuenta LDAP/AD que esta aplicación utilizará para conectarse al directorio, e introduce la credencial de enlace (contraseña) de dicha cuenta. NetApp Console utiliza estos datos para establecer el enlace con LDAP y validar la conexión.
 - **DN de usuario**: una cuenta de usuario con permiso para consultar el directorio. Por ejemplo, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Selecciona **Add** para guardar la integración.

Después de que termines

Después de guardar la integración, añade usuarios de directorio a tu organización y asígnale roles. Debes configurar y habilitar al menos una integración con Active Directory antes de poder añadir usuarios de directorio. ["Aprende a añadir usuarios del directorio y a asignarles roles"](#).

Desactivar o activar una integración con Active Directory

Desactiva una integración para suspender temporalmente la autenticación basada en un directorio sin eliminar la configuración. Cuando desactivas un servicio de directorio, los usuarios de ese directorio no pueden iniciar sesión a través del directorio.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Directory services** para abrir la página Federations.
3. En la lista de integraciones, busca la integración y selecciona el menú de acciones de esa fila.
4. Selecciona **Desactivar** para suspender la integración o **Activar** para restablecerla.

Eliminar una integración con Active Directory

Elimina una integración para borrar de forma permanente la configuración del servicio de directorio. Antes de eliminar, revisa cualquier advertencia sobre los usuarios del directorio que están vinculados a la integración, ya que su acceso se verá afectado.

Pasos

1. Selecciona **Administración > Identidad y acceso**.
2. Selecciona **Directory services** para abrir la página Federations.
3. En la lista de integraciones, busca la integración y selecciona el menú de acciones de esa fila.
4. Selecciona **Eliminar** y confirma la eliminación.

Conecta tu LLM y activa el asistente de NetApp Console en la implementación local de NetApp Console

Conecta tu modelo de lenguaje a gran escala (LLM) a NetApp Console en una implementación local para habilitar el asistente de la Console y la gestión del almacenamiento asistida por IA.



Esta documentación sobre cómo conectar un modelo de lenguaje grande (LLM) al asistente de la Console para habilitar funciones de IA se ofrece como una versión preliminar tecnológica. Con esta versión preliminar, NetApp se reserva el derecho a modificar los detalles de la oferta, los contenidos y el calendario antes de su disponibilidad general.

Roles de acceso necesarios

Superadministrador o administrador de la organización. ["Conoce los roles de acceso"](#).

Después de la configuración, los usuarios abren el asistente de la consola desde el panel de control y eligen un modo de acceso:

- En el modo **Solo lectura**, el asistente responde a las preguntas y ofrece orientación sin realizar cambios.
- En el modo **lectura/escritura**, el asistente puede realizar acciones en la infraestructura de almacenamiento. Muestra los detalles para revisión y confirmación antes de cada cambio. Para operaciones asíncronas, como la creación de volúmenes, crea una tarea que los usuarios pueden consultar desde el asistente.

Para conectar tu LLM, selecciona una ruta de proveedor, introduce los datos del endpoint y la clave de API, y luego selecciona un modelo en **Administración > Herramientas de IA**. Las acciones del asistente se mantienen dentro de tus políticas de almacenamiento y los controles de acceso basados en roles.

Reúne todo lo que necesites antes de conectar un LLM

Antes de conectar tu LLM, reúne lo siguiente:

- Tu elección del tipo de proveedor: OpenAI o OpenAI-compatible. ["Infórmate sobre las opciones de proveedores."](#)
- Una clave API válida para la ruta del proveedor que selecciones.
- La URL del endpoint para la ruta de tu proveedor.
- La URL de tu proxy o gateway, si tu organización lo requiere.
- Tu nombre de usuario o identificador de inicio de sesión único (SSO) para la cuenta del proveedor de LLM, si es necesario.
- Acceso a la red desde la implementación local de Console al endpoint seleccionado.
- Clases de almacenamiento y controles de acceso basados en roles para las acciones del asistente que planeas permitir.

Para obtener más información sobre los modelos compatibles, consulta ["Infórmate sobre los proveedores y modelos de LLM compatibles en la implementación local de NetApp Console"](#).

Conecta un LLM a la implementación local de NetApp Console

Introduce la configuración del proveedor, la clave API y el modelo para conectar tu LLM a la implementación local de Console.

Pasos

1. Inicia sesión en la consola local de NetApp Console.
2. Selecciona **Administración > Herramientas de IA**.
3. Selecciona el menú y, a continuación, selecciona **Editar**.
4. En **Tipo de proveedor**, selecciona un tipo de proveedor.

["Infórmate sobre la integración de LLM en la implementación local de NetApp Console"](#).

5. Si se te pide un endpoint del proveedor, introduce la URL del endpoint para la ruta del proveedor que seleccionaste.
6. Introduce la URL del proxy o de la puerta de enlace y las credenciales.
7. En el campo **Nombre de usuario**, introduce tu nombre de usuario o tu ID de SSO si la ruta de tu proveedor así lo requiere.
8. En el campo **Clave API**, pega la clave API de la ruta del proveedor que hayas seleccionado.
9. Selecciona un modelo de la lista.
10. Revisa la configuración y, a continuación, selecciona **Guardar**.

Si falla el proceso de guardado o la prueba, verifica el tipo de proveedor, la URL del endpoint, la clave de API y el modelo seleccionado, y luego vuelve a intentarlo.

["Soluciona los problemas de tu integración con el LLM"](#).

Comprueba que la integración de LLM funcione

Después de guardar la configuración, verifica la disponibilidad y el comportamiento del asistente.

Pasos

1. Comprueba que el botón **Asistente de la consola** aparece en el panel de control de implementación local de la NetApp Console.
2. Abre el asistente en modo **Solo lectura** y ejecuta una consulta básica.
3. Abre el asistente en modo **lectura/escritura** y confirma que las acciones que modifican el almacenamiento requieran la confirmación del usuario antes de ejecutarse.
4. Comprueba que los usuarios que necesitan flujos de trabajo de acciones dispongan de los controles de acceso basados en roles necesarios.

Una vez completada la validación, los usuarios pueden abrir el asistente de la Console desde el panel de control y describir las tareas en lenguaje sencillo. Para ver ejemplos de uso y flujos de trabajo de los usuarios finales, consulta ["Usa el asistente de NetApp Console"](#).

Protege las credenciales y supervisa el uso de los modelos de lenguaje grande (LLM)

- Siempre que sea posible, utiliza una clave API dedicada para la integración con la implementación local de

Console.

- Rota las claves de la API según la política de tu organización.
- Restringe quién puede editar la configuración de las herramientas de IA solo a los roles de administrador necesarios.
- Supervisa el uso de la API por parte de los proveedores y las alertas para detectar actividad anómala o picos de costes.

Soluciona problemas de la integración de LLM en la implementación local de NetApp Console

Utiliza este flujo de clasificación rápida para diagnosticar y resolver problemas habituales de integración de LLM en NetApp Console en una implementación local.



Esta documentación sobre cómo conectar un modelo de lenguaje grande (LLM) al asistente de la Consola para habilitar funciones de IA se ofrece como una versión preliminar tecnológica. Con esta versión preliminar, NetApp se reserva el derecho a modificar los detalles de la oferta, los contenidos y el calendario antes de su disponibilidad general.

Si aún no has completado la configuración, consulta ["Conecta tu LLM y activa el asistente de NetApp Console"](#).

Soluciona rápido los problemas de integración de Triage LLM

1. Valida la configuración de las herramientas de IA en **Administración > Herramientas de IA**.

Confirma el tipo de proveedor, la URL del endpoint, la clave de API, el modelo seleccionado y el acceso a la red de salida.

2. Comprueba la disponibilidad del asistente en el panel de control.

Comprueba que el botón **Console assistant** aparezca para los usuarios y las organizaciones previstos.

3. Valida el comportamiento en tiempo de ejecución.

Realiza una solicitud sencilla de solo lectura y comprueba la accesibilidad del endpoint del proveedor, la disponibilidad del modelo y el estado del servicio del proveedor.

Solucionar problemas según los síntomas

Síntoma	Causa probable	Qué hay que comprobar	Próxima acción
Guardar o probar falla en AI Tools	Incompatibilidad de configuración o conectividad	Tipo de proveedor, URL del punto final, formato de la clave de API, modelo seleccionado y acceso saliente	Corrige el valor que no supera la validación y vuelve a guardar

Síntoma	Causa probable	Qué hay que comprobar	Próxima acción
Falta el botón Console assistant	Estado de integración inadecuado, incompatibilidad de la organización o incompatibilidad de RBAC	Guardado exitoso de herramientas de IA, estado de integración, organización actual y rol de acceso esperado	Actualiza la sesión y verifica con una cuenta de administrador que sepas que funciona correctamente
El asistente se abre pero la solicitud falla	Problema con el proveedor o con la ruta de ejecución	Accesibilidad del endpoint, disponibilidad del modelo en ese endpoint, límites del proveedor y estado temporal del proveedor	Vuelve a intentarlo tras solucionar la incompatibilidad entre el endpoint y el modelo o los problemas de límite por parte del proveedor.
La respuesta del asistente es lenta o irregular	Tamaño de la solicitud, rendimiento del endpoint o inestabilidad de la red/proxy	Prueba breve de respuesta, estado del servicio del proveedor y estabilidad de la red/proxy	Utiliza una instrucción más breve, prueba con otro modelo compatible y estabiliza la red o el enrutamiento del proxy

Responde ante la divulgación o el uso indebido de credenciales de LLM

Si sospechas que se ha filtrado una clave API o que se ha producido un uso no autorizado:

1. Revoca la clave API existente en el sistema de tu proveedor.
2. Crea una nueva clave de API.
3. Actualiza la clave en **Administración > Herramientas de IA**.
4. Verifica que la reconexión se realizó correctamente con una prueba de asistente de solo lectura.

Configura los canales de entrega de notificaciones en la implementación local de NetApp Console

En una implementación local de NetApp Console, puedes configurar varios canales para las notificaciones de alertas, incluyendo correo electrónico y webhooks.

Roles de acceso necesarios

Superadministrador o administrador de la organización. ["Conoce los roles de acceso"](#).

De forma predeterminada, la implementación local de Console muestra las notificaciones a través de su sistema de notificaciones integrado. Configurar canales de entrega adicionales te permite recibir notificaciones de la forma que mejor se adapte a tu flujo de trabajo.

Puedes enviar todas las notificaciones a través de los mismos canales o utilizar canales diferentes para distintos tipos de notificaciones. Por ejemplo, podrías enviar alertas urgentes sobre el almacenamiento por correo electrónico, mientras que el resto de alertas se redirigen a una herramienta de monitorización de terceros mediante un webhook.

Una vez que hayas configurado los canales de envío de notificaciones, puedes configurar las reglas de

notificación y asignarlas a los distintos canales. ["Aprende a configurar las reglas de notificación"](#).

Configura un servidor de correo electrónico

Cuando configuras un servidor de correo electrónico, la implementación local de Console envía notificaciones, alertas e invitaciones a usuarios a través de él. La implementación local de Console es compatible con servidores de correo electrónico SMTP, que pueden ser tu servidor de correo corporativo existente o un servicio de correo electrónico de terceros.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuraciones del sistema.
3. En la sección **Servidor de correo electrónico**, selecciona **Configurar**.
4. Introduce los datos de conexión de tu servidor de correo electrónico:
 - Agrega un nombre de remitente y una dirección de correo electrónico de remitente.
 - El **host SMTP**: nombre de host o dirección IP de tu servidor SMTP. Si tienes varios servidores, introduce el principal.
 - Selecciona el protocolo de conexión en la lista desplegable **Seguridad de la conexión**. El puerto ya está configurado y es de solo lectura: 25 para SMTP con STARTTLS o 465 para SMTPS.

SMTPS (puerto 465) establece una conexión cifrada de forma inmediata y se recomienda para entornos donde la seguridad es importante. STARTTLS (puerto 25) actualiza desde una conexión no cifrada y puede volver a la transmisión no cifrada si falla la negociación del cifrado.
5. Selecciona **Test email** para enviar un correo de prueba al destinatario que indiques.
6. Después de que la prueba finalice con éxito, selecciona **Guardar** para guardar la configuración.

Si la prueba falla, vuelve a verificar la configuración que introdujiste y asegúrate de que la implementación local de Console tenga acceso a la red del servidor de correo electrónico.

Actualizar la configuración de un servidor de correo electrónico

Puedes actualizar la configuración de un servidor de correo electrónico ya existente si quieres usar otro servidor de correo electrónico.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuraciones del sistema.
3. En la sección **Servidor de correo electrónico**, selecciona **Configurar**.
4. Selecciona **Borrar campos** para borrar la configuración actual.
5. Introduce los nuevos datos de conexión de tu servidor de correo electrónico.
6. Selecciona **Test email** para enviar un correo de prueba al destinatario que indiques.
7. Después de que la prueba se realice con éxito, selecciona **Guardar** para guardar la nueva configuración.

Si la prueba falla, vuelve a verificar la configuración que introdujiste y asegúrate de que la implementación local de Console tenga acceso a la red del servidor de correo electrónico.

Eliminar la configuración de un servidor de correo electrónico

Puedes eliminar la configuración del servidor de correo electrónico si ya no quieres que la implementación local de Console envíe correos electrónicos.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuración de sistemas.
3. En la sección **Servidor de correo electrónico**, selecciona **Configurar**.
4. Selecciona **Borrar campos** para borrar la configuración actual.
5. Selecciona **Guardar** para guardar la configuración borrada, lo que elimina la configuración del servidor de correo electrónico de la implementación local de Console.

Configura un webhook

Configura webhooks para enviar notificaciones desde la implementación local de Console a otras herramientas o servicios. Puedes configurar varios webhooks, cada uno apuntando a un endpoint diferente. Por ejemplo, uno para un SIEM y otro para un servicio de avisos de guardia.

Después de crear un webhook, los usuarios con el rol de Storage admin pueden asignarlo a reglas de alerta específicas. Por ejemplo, pueden enviar alertas críticas por correo electrónico mientras envían todas las alertas a una herramienta de monitorización de terceros a través de un webhook.



La implementación local de la consola no aplica control de acceso a los endpoints de webhook. Cualquier usuario o sistema que pueda acceder a la URL del endpoint recibe los datos de la alerta. Asegúrate de que el acceso a la aplicación receptora esté restringido a los usuarios autorizados mediante los propios controles de acceso de esa aplicación.

Antes de empezar

Confirma que la implementación local de Console pueda comunicarse con la aplicación receptora a través de la red y recopila la URL del endpoint, el método HTTP y cualquier detalle de autenticación o certificado que requiera esa aplicación.

Pasos

1. Selecciona **Administración > Consola**.
2. Selecciona **Configuración** para abrir la página de configuraciones del sistema.
3. En la sección **Integración de webhooks**, selecciona **Configurar**.
4. Introduce los datos necesarios para el webhook:
 - Un nombre descriptivo para el webhook.
 - La URL del punto final proporcionada por la aplicación receptora.
 - Método HTTP
 - Opcional: un certificado autofirmado en formato PEM.
 - Cualquier encabezado o secreto requerido (credenciales de autenticación).
 - El formato que se debe utilizar al enviar el webhook. Se admiten JSON y OTEL (OpenTelemetry).

Utiliza JSON para webhooks de uso general y puntos finales REST personalizados. Utiliza OTEL para plataformas de observabilidad que consumen de forma nativa señales de OpenTelemetry, como

Grafana u otros colectores compatibles con OpenTelemetry.

5. Selecciona **Probar webhook** para comprobar la conexión del webhook y asegurarte de que la implementación local de Console puede enviar mensajes correctamente a la aplicación receptora.
6. Después de que la prueba se realice correctamente, selecciona **Guardar** para crear el webhook.

Una vez que guardes el webhook, estará disponible para que los usuarios lo seleccionen donde se admitan webhooks, como en las opciones de entrega de alertas. ["Descubre cómo crear reglas de alerta y asignar webhooks para el envío de alertas."](#)

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.