Proxy de servicios web

E-Series Systems

NetApp
June 14, 2024

Tabla de contenidos

Proxy de servicios web

Información general sobre el proxy de servicios web de SANtricity

El proxy de servicios web de SANtricity es un servidor API RESTful que se instala por separado en un sistema host para gestionar cientos de sistemas de almacenamiento E-Series de NetApp nuevos y heredados. El proxy incluye Unified Manager de SANtricity, que es una interfaz basada en web que ofrece funciones similares.

Información general de la instalación

La instalación y la configuración de Web Services Proxy implica los siguientes pasos:

1. "Revise los requisitos de instalación y actualización".
2. "Descargue e instale el archivo Web Services Proxy".
3. "Inicie sesión en API y Unified Manager".
4. "Configure el proxy de servicios web".

Obtenga más información

- Unified Manager: La instalación del proxy incluye Unified Manager de SANtricity, una interfaz web que proporciona acceso de configuración a los nuevos sistemas de almacenamiento E-Series y EF-Series. Para obtener más información, consulte la ayuda en línea de Unified Manager, que está disponible en su interfaz de usuario o en "Sitio de documentación del software SANtricity".
- Repositorio de GitHub: GitHub contiene un repositorio de la colección y organización de scripts de muestra que ilustra el uso de la API de servicios web de SANtricity de NetApp. Para acceder al repositorio, consulte "Ejemplos de WebServices de NetApp".
- Transferencia de estado representacional (REST): Servicios web es una API RESTful que proporciona acceso a prácticamente todas las funcionalidades de gestión de SANtricity, por lo que debería estar familiarizado con los conceptos DE REST. Para obtener más información, consulte "Estilos arquitectónicos y el diseño de arquitecturas de software basadas en red".
- Notación de objetos JavaScript (JSON) — debido a que los datos dentro de los servicios web están codificados a través de JSON, debe estar familiarizado con los conceptos de programación JSON. Para obtener más información, consulte "Presentamos JSON".

Obtenga más información acerca de los servicios web

Información general sobre los servicios web y Unified Manager

Antes de instalar y configurar el proxy de servicios web, lea la información general de servicios web y Unified Manager de SANtricity.

Servicios Web

Servicios web es una interfaz de programación de aplicaciones (API) que permite configurar, gestionar y supervisar sistemas de almacenamiento E-Series y EF-Series de NetApp. Al emitir solicitudes de API, podrá

completar flujos de trabajo como la configuración, el aprovisionamiento y la supervisión del rendimiento de los sistemas de almacenamiento E-Series.

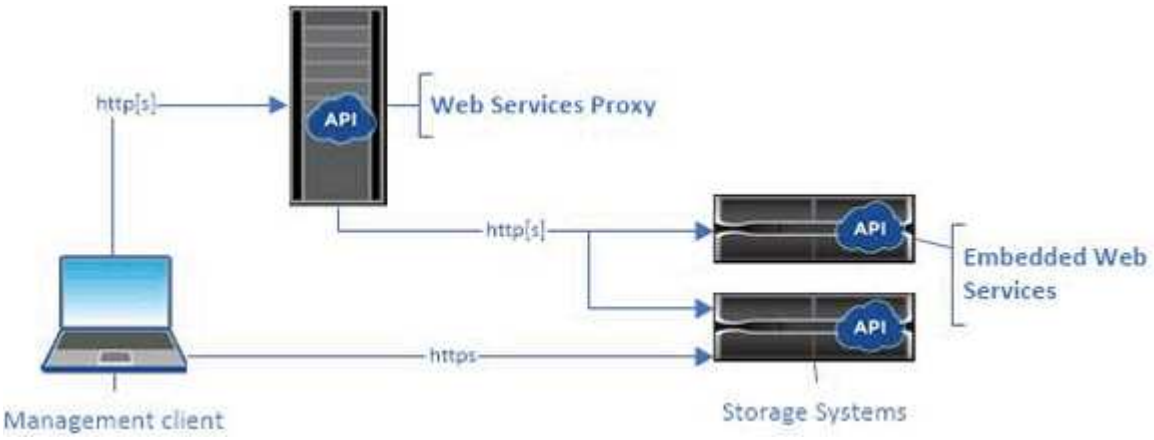
Al usar la API de servicios web para gestionar sistemas de almacenamiento, debe estar familiarizado con lo siguiente:

- Notación de objetos JavaScript (JSON): Debido a que los datos dentro de los servicios web están codificados a través de JSON, debe estar familiarizado con los conceptos de programación de JSON. Para obtener más información, consulte "Presentamos JSON".
- Transferencia de estado representacional (REST): Servicios web es una API RESTful que proporciona acceso a prácticamente todas las funcionalidades de gestión de SANtricity, por lo que debería estar familiarizado con los conceptos DE REST. Para obtener más información, consulte "Estilos arquitectónicos y el diseño de arquitecturas de software basadas en red".
- Conceptos del lenguaje de programación: Java y Python son los lenguajes de programación más comunes que se usan con la API de servicios web, pero cualquier lenguaje de programación que pueda realizar solicitudes HTTP es suficiente para la interacción de API.

Web Services está disponible en dos implementaciones:

- **Integrado**: Se integra Un servidor API RESTful en cada controladora de un sistema de almacenamiento E2800/EF280 que ejecuta SANtricity 11.30 de NetApp o versiones posteriores, un E5700/EF570 que ejecuta SANtricity 11.40 o versiones posteriores, y un EF300 o EF600 que ejecuta SANtricity 11.60 o versiones posteriores. No es necesario realizar ninguna instalación.
- **Proxy** — el proxy de servicios web de SANtricity es un servidor API RESTful instalado por separado en un servidor Windows o Linux. Esta aplicación basada en host puede gestionar cientos de sistemas de almacenamiento E-Series de NetApp nuevos y heredados. En general, debe usar el proxy para redes con más de 10 sistemas de almacenamiento. El proxy puede manejar numerosas solicitudes de forma más eficiente que la API integrada.

El núcleo de la API está disponible en ambas implementaciones.



La tabla siguiente proporciona una comparación entre el proxy y la versión incrustada.

Consideración	Proxy	Integrado
Instalación	Requiere un sistema host (Linux o Windows). El proxy se puede descargar en la "Sitio de soporte de NetApp" o encendido "DockerHub".	No se requiere instalación ni habilitación.
Seguridad	Configuración mínima de seguridad de forma predeterminada. La configuración de seguridad es baja para que los desarrolladores puedan empezar a usar la API de forma rápida y sencilla. Si lo desea, puede configurar el proxy con el mismo perfil de seguridad que la versión incrustada.	Configuración de alta seguridad de forma predeterminada. La configuración de seguridad es alta porque la API se ejecuta directamente en las controladoras. Por ejemplo, no permite el acceso HTTP y deshabilita todos los protocolos de cifrado SSL y TLS anteriores para HTTPS.
Gestión centralizada	Gestiona todos los sistemas de almacenamiento desde un servidor.	Gestiona únicamente el controlador en el que está integrado.

Unified Manager

El paquete de instalación proxy incluye Unified Manager, una interfaz web que proporciona acceso a la configuración de los nuevos sistemas de almacenamiento E-Series y EF-Series, como E2800, E5700, EF300 y EF600.

En Unified Manager, puede realizar las siguientes operaciones en lote:

- Vea el estado de varios sistemas de almacenamiento desde una vista central
- Detectar varios sistemas de almacenamiento en la red
- Importe la configuración de un sistema de almacenamiento a varios sistemas
- Actualizar el firmware para varios sistemas de almacenamiento

Compatibilidad y restricciones

Las siguientes restricciones y compatibilidad se aplican al uso del proxy de servicios web.

Consideración	Compatibilidad o restricción
Soporte HTTP	El proxy de servicios web permite el uso de HTTP o HTTPS. (La versión incrustada de Web Services requiere HTTPS por motivos de seguridad.)

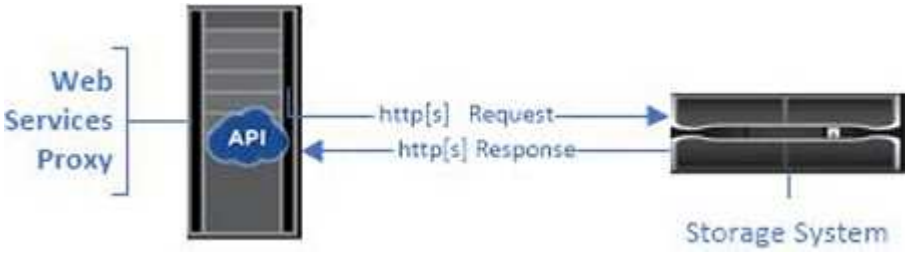
Consideración	Compatibilidad o restricción
Firmware y sistemas de almacenamiento	El proxy de servicios web puede gestionar todos los sistemas de almacenamiento E-Series, incluida una combinación de sistemas anteriores y las últimas versiones de E2800, EF280, E5700, EF570, EF300, Y sistemas de las series EF600.
Compatibilidad con IP	El proxy de servicios web es compatible con el protocolo IPv4 o con el protocolo IPv6. Es posible que se produzca un error en el protocolo IPv6 cuando el proxy de servicios web intenta detectar automáticamente la dirección de gestión de la configuración de la controladora. Entre las posibles causas del fallo se encuentran problemas durante el reenvío de direcciones IP o la activación de IPv6 en los sistemas de almacenamiento, pero no en el servidor.
Restricciones de nombres de archivo de NVSRAM	El proxy de servicios web utiliza nombres de archivo NVSRAM para identificar la información de la versión con precisión. Por lo tanto, no se pueden cambiar los nombres de los archivos NVSRAM cuando se utilizan con el proxy de servicios web. Es posible que el proxy de servicios web no reconozca un archivo NVSRAM cuyo nombre ha cambiado como un archivo de firmware válido.
Web Symbol	Symbol Web es una URL en la API REST. Proporciona acceso a casi todas las llamadas con símbolos. La función Symbol forma parte de la siguiente URL: `http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function` Los sistemas de almacenamiento con deshabilitado Symbol se admiten a través del proxy de servicios web.

Conceptos básicos de API

En la API de servicios web, las comunicaciones HTTP implican un ciclo de solicitud y respuesta.

Elementos de URL en las solicitudes

Independientemente del lenguaje de programación o la herramienta utilizada, cada llamada a la API de servicios web tiene una estructura similar, con una dirección URL, un verbo HTTP y un encabezado Accept.



Todas las solicitudes incluyen una dirección URL, como en el ejemplo siguiente, y contienen los elementos descritos en la tabla.

```
https://webservices.name.com:8443/devmgr/v2/storage-systems
```

Zona	Descripción
Transporte HTTP `https://`	El proxy de servicios web permite el uso de HTTP o HTTPS. Los servicios web integrados requieren HTTPS por motivos de seguridad.
Puerto y URL básicos `webservices.name.com:8443`	Cada solicitud debe enrutarse correctamente a una instancia activa de Web Services. Se requiere el FQDN (nombre de dominio completo) o la dirección IP de la instancia, junto con el puerto de escucha. De forma predeterminada, Web Services se comunica a través del puerto 8080 (para HTTP) y el puerto 8443 (para HTTPS). Para el proxy de servicios web, ambos puertos se pueden cambiar durante la instalación del proxy o en el archivo wsconfig.xml. La contención de puertos es común en los hosts de centro de datos que ejecutan diversas aplicaciones de gestión. En el caso de los servicios web integrados, no se puede cambiar el puerto de la controladora; de forma predeterminada, se establece en el puerto 8443 para conexiones seguras.

Zona	Descripción
Ruta API `devmgr/v2/storage-systems`	Se realiza una solicitud a un recurso DE REST o un extremo específico dentro de la API de servicios web. La mayoría de los extremos tienen el siguiente formato: `devmgr/v2/<resource>/[id]` La ruta API consta de tres partes: • `devmgr` (Administrador de dispositivos) es el espacio de nombres de la API de servicios web. • `v2` Indica la versión de la API a la que tiene acceso. También puede utilizar `utils` para acceder a los extremos de inicio de sesión. • `storage-systems` es una categoría de la documentación.

Verbos HTTP admitidos

Los verbos HTTP admitidos incluyen GET, POST y DELETE:

- Las solicitudes GET se utilizan para solicitudes de sólo lectura.
- LAS solicitudes POST se utilizan para crear y actualizar objetos, así como para solicitudes de lectura que podrían tener implicaciones de seguridad.
- Las solicitudes DE ELIMINACIÓN suelen utilizarse para quitar un objeto de la gestión, quitar un objeto por completo o restablecer el estado del objeto.

Actualmente, la API de servicios web no admite PUT ni PARCHE. En su lugar, puede usar POST para proporcionar la funcionalidad típica de estos verbos.

Aceptar encabezados

Al devolver un cuerpo de la solicitud, Web Services devuelve los datos en formato JSON (a menos que se especifique lo contrario). Algunos clientes solicitan por defecto "'text/html'" o algo similar. En estos casos, la API responde con un código HTTP 406, indicando que no puede proporcionar datos en este formato. Como práctica recomendada, debe definir el encabezado Accept como "'Application/json'" para los casos en los que espere JSON como tipo de respuesta. En otros casos en los que no se devuelve un cuerpo de respuesta (por ejemplo, ELIMINAR), siempre que el encabezado Accept no provoque ningún efecto no intencional.

Respuestas

Cuando se realiza una solicitud a la API, una respuesta devuelve dos partes fundamentales de información:

- Código de estado HTTP: Indica si la solicitud se ha realizado correctamente.
- Cuerpo de respuesta opcional — normalmente proporciona un cuerpo JSON que representa el estado del recurso o un cuerpo que proporciona más detalles sobre la naturaleza de un fallo.

Debe comprobar el código de estado y la cabecera de tipo de contenido para determinar el aspecto del cuerpo

de respuesta resultante. Para los códigos de estado HTTP 200-203 y 422, Web Services devuelve un cuerpo JSON con la respuesta. Para otros códigos de estado HTTP, Web Services generalmente no devuelve un cuerpo JSON adicional, ya sea porque la especificación no lo permite (204) o porque el estado es autoexplicativo. En la tabla se enumeran los códigos de estado HTTP comunes y las definiciones. También indica si la información asociada con cada código HTTP se devuelve en un cuerpo JSON.

Código de estado HTTP	Descripción	Cuerpo JSON
200 DE ACUERDO	Indica una respuesta correcta.	Sí
201 creado	Indica que se creó un objeto. Este código se utiliza en unos pocos casos excepcionales en lugar de un estado de 200.	Sí
202 aceptado	Indica que la solicitud se acepta para su procesamiento como una solicitud asíncrona, pero debe realizar una solicitud posterior para obtener el resultado real.	Sí
203 Información no autoritativa	Similar a una respuesta de 200, pero Web Services no puede garantizar que los datos estén actualizados (por ejemplo, solo los datos en caché están disponibles en este momento).	Sí
204 sin contenido	Indica una operación correcta, pero no hay cuerpo de respuesta.	No
400 solicitud incorrecta	Indica que el cuerpo JSON proporcionado en la solicitud no es válido.	No
401 no autorizado	Indica que se ha producido un error de autenticación. No se han proporcionado credenciales o el nombre de usuario o la contraseña no son válidos.	No
403 Prohibido	Un error de autorización, que indica que el usuario autenticado no tiene permiso para acceder al extremo solicitado.	No

Código de estado HTTP	Descripción	Cuerpo JSON
404 no encontrado	Indica que no se pudo ubicar el recurso solicitado. Este código es válido para API no existentes o recursos no existentes solicitados por el identificador.	No
422 entidad no procesable	Indica que por lo general, la solicitud está bien formada, pero los parámetros de entrada no son válidos o el estado del sistema de almacenamiento no permite que los servicios web satisfagan la solicitud.	Sí
424 Dependencia con error	Se utiliza en el proxy de servicios web para indicar que no se puede acceder al sistema de almacenamiento solicitado en ese momento. Por lo tanto, Web Services no puede satisfacer la solicitud.	No
429 demasiadas solicitudes	Indica que se ha superado el límite de solicitudes y que se debe volver a intentar más tarde.	No

Scripts de ejemplo

GitHub contiene un repositorio de la colección y la organización de scripts de muestra que ilustra el uso de la API de servicios web de SANtricity de NetApp. Para acceder al repositorio, consulte "Ejemplos de WebServices de NetApp".

Términos y conceptos

Los siguientes términos se utilizan en el proxy de servicios web.

Duración	Definición
API	Una interfaz de programación de aplicaciones (API) es un conjunto de protocolos y métodos que permiten a los desarrolladores comunicarse con los dispositivos. La API de servicios web se utiliza para comunicarse con los sistemas de almacenamiento E-Series.

Duración	Definición
ASUP	La función AutoSupport (ASUP) recoge datos en un bundle de soporte al cliente y envía automáticamente el archivo de mensaje al soporte técnico para la solución de problemas remota y el análisis de problemas.
Extremo	Los extremos son funciones que están disponibles en la API. Un extremo incluye un verbo HTTP, más la ruta de URI. En Web Services, los extremos pueden ejecutar tareas como detectar sistemas de almacenamiento y crear volúmenes.
HTTP Verbo	Un verbo HTTP es una acción correspondiente para un punto final, como la recuperación y la creación de datos. En Servicios Web, los verbos HTTP incluyen POST, GET y DELETE.
JSON	La notación de objetos JavaScript (JSON) es un formato de datos estructurado muy similar a XML, que utiliza un formato mínimo de lectura. Los datos en los servicios web están codificados a través de JSON.
REST/RESTful	La transferencia de estado representacional (REST) es una especificación suelta que define un estilo arquitectónico para una API. Dado que la mayoría de las API DE DESCANSO no cumplen plenamente la especificación, se las describe como «MUY COMPLETAS» o «similar AL TÉRMINO». En general, una API "MUY COMPLETA" es independiente de los lenguajes de programación y tiene las siguientes características: • Basado en HTTP, que sigue la semántica general del protocolo • Productor y consumidor de datos estructurados (JSON, XML, etc.) • Orientado a objetos (a diferencia de orientado a la operación) Servicios web es una API RESTful que proporciona acceso a prácticamente todas las funcionalidades de gestión de SANtricity.
sistema de almacenamiento	Un sistema de almacenamiento es una cabina E-Series que incluye bandejas, controladoras, unidades, software y firmware.

Duración	Definición
API Symbol	Symbol es una API heredada para gestionar los sistemas de almacenamiento E-Series. La implementación subyacente de la API de servicios web utiliza Symbol.
Servicios Web	Web Services es una API que NetApp ha sido diseñada para que los desarrolladores gestionen los sistemas de almacenamiento E-Series. Existen dos implementaciones de Web Services: Integradas en el controlador y un proxy independiente que se puede instalar en Linux o Windows.

Instalar y configurar

Revise los requisitos de instalación y actualización

Antes de instalar Web Services Proxy, revise los requisitos de instalación y actualice sus consideraciones.

Requisitos de instalación

Puede instalar y configurar el proxy de servicios web en un sistema host Windows o Linux.

La instalación de proxy incluye los siguientes requisitos.

Requisito	Descripción
Limitaciones de nombre de host	Asegúrese de que el nombre de host del servidor donde planea instalar el proxy de servicios web contiene sólo letras ASCII, dígitos numéricos y guiones (-). Este requisito se debe a una limitación de Java keytool, que se utiliza para generar un certificado autofirmado para el servidor. Si el nombre de host del servidor contiene otros caracteres, como un guión bajo (_), el servidor web no se iniciará después de la instalación.
Sistemas operativos	Puede instalar el proxy en los sistemas operativos siguientes: • Linux • Windows Para obtener una lista completa de los sistemas operativos y la compatibilidad del firmware, consulte "Herramienta de matriz de interoperabilidad de NetApp".

Requisito	Descripción
Linux: Consideraciones adicionales	Las bibliotecas Linux Standard base (init-functions) son necesarias para que el servidor web funcione correctamente. Debe instalar los paquetes lsb/insserv para el sistema operativo. Para obtener más información, consulte la sección "Paquetes adicionales necesarios" del archivo Readme.
Múltiples instancias	Sólo puede instalar una instancia de proxy de servicios web en un servidor; sin embargo, puede instalar el proxy en varios servidores de la red.
Planificación de la capacidad	El proxy de servicios web requiere un espacio adecuado para el registro. Asegúrese de que su sistema cumpla los siguientes requisitos de espacio en disco disponibles: • Espacio necesario para la instalación — 275 MB • Espacio mínimo de registro — 200 MB • Memoria del sistema — 2 GB; el espacio en el montón es 1 GB de forma predeterminada Puede utilizar una herramienta de supervisión de espacio en disco para verificar el espacio disponible en la unidad de disco para el almacenamiento persistente y el registro.
Licencia	El proxy de servicios web es un producto gratuito e independiente que no requiere una clave de licencia. Sin embargo, se aplican los derechos de autor y las condiciones de servicio aplicables. Si está instalando el proxy en modo gráfico o consola, debe aceptar el Contrato de licencia para el usuario final (EULA).

Consideraciones de renovación

Si está actualizando desde una versión anterior, tenga en cuenta que algunos elementos se conservan o se eliminan.

- Para el proxy de servicios web, se conservan los ajustes de configuración anteriores. Esta configuración incluye contraseñas de usuario, todos los sistemas de almacenamiento detectados, certificados de servidor, certificados de confianza y configuración de tiempo de ejecución del servidor.
- En el caso de Unified Manager, se quitan todos los archivos de sistema operativo SANtricity cargados anteriormente en el repositorio durante la actualización.

Instale o actualice el archivo proxy de servicios web

La instalación implica descargar el archivo y, a continuación, instalar el paquete proxy en un servidor Linux o Windows. También puede actualizar el proxy utilizando estas instrucciones.

Descargue los archivos del proxy de servicios web

Podrás descargar el archivo de instalación y el archivo Léame de la página de descarga de software del sitio de soporte de NetApp.

El paquete de descarga incluye el proxy de servicios web y la interfaz de Unified Manager.

Pasos

1. Vaya a. "Soporte de NetApp: Descargas".
2. Seleccione **E-Series SANtricity Web Services Proxy**.
3. Siga las instrucciones para descargar el archivo. Asegúrese de seleccionar el paquete de descarga correcto para su servidor (por ejemplo, EXE para Windows; BIN o RPM para Linux).
4. Descargue el archivo de instalación en el servidor donde desea instalar el proxy y Unified Manager.

Instale en servidores Windows o Linux

Puede instalar Web Services Proxy y Unified Manager mediante uno de tres modos (gráfica, consola o silenciosa) o utilizando un archivo RPM (sólo Linux).

Antes de empezar

- "Revise los requisitos de la instalación".
- Asegúrese de haber descargado el archivo de instalación correcto (EXE para Windows; BIN para Linux) en el servidor en el que desea instalar el proxy y Unified Manager.

Instalación en modo gráfico

Puede ejecutar la instalación en modo gráfico para Windows o Linux. En el modo gráfico, las instrucciones aparecen en una interfaz de estilo Windows.

Pasos

1. Acceda a la carpeta en la que descargó el archivo de instalación.
2. Inicie la instalación de Windows o Linux de la siguiente manera:

   - Windows — haga doble clic en el archivo de instalación:

     `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`

   - Linux — ejecute el siguiente comando: `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

     En los nombres de archivo anteriores, `nn.nn.nn.nnnn` representa el número de versión.

   Se inicia el proceso de instalación y se muestra la pantalla de bienvenida de NetApp SANtricity Web Services Proxy + Unified Manager.

3. Siga las instrucciones que aparecen en pantalla.

   Durante la instalación, se le pedirá que habilite varias funciones e introduzca algunos parámetros de configuración. Si es necesario, puede cambiar cualquiera de estas selecciones posteriormente en los archivos de configuración.

Durante una actualización, no se le solicitan los parámetros de configuración.

4. Cuando aparezca el mensaje servidor web iniciado, haga clic en **Aceptar** para completar la instalación.

   Aparece el cuadro de diálogo instalar completo.

5. Haga clic en las casillas de verificación si desea iniciar Unified Manager o la documentación de API interactiva y, a continuación, haga clic en **hecho**.

Instale en modo de consola

Puede ejecutar la instalación en modo de consola para Windows o Linux. En el modo Consola, las indicaciones aparecen en la ventana de terminal.

Pasos

1. Ejecute el siguiente comando: `<install filename> -i console`

   En el comando anterior, `<install filename>` representa el nombre del archivo de instalación del proxy que ha descargado (por ejemplo: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

   Para cancelar la instalación en cualquier momento durante el proceso de instalación, escriba `QUIT` en el símbolo del sistema.

   Se inicia el proceso de instalación y aparece el mensaje iniciando el instalador — Introducción .

2. Siga las instrucciones que aparecen en pantalla.

   Durante la instalación, se le pedirá que habilite varias funciones e introduzca algunos parámetros de configuración. Si es necesario, puede cambiar cualquiera de estas selecciones posteriormente en los archivos de configuración.

   Durante una actualización, no se le solicitan los parámetros de configuración.

3. Una vez finalizada la instalación, pulse **Intro** para salir del instalador.

Instalación en modo silencioso

Puede ejecutar la instalación en modo silencioso para Windows o Linux. En el modo silencioso, no aparecen mensajes de retorno ni secuencias de comandos en la ventana de terminal.

Pasos

1. Ejecute el siguiente comando: `<install filename> -i silent`

   En el comando anterior, `<install filename>` representa el nombre del archivo de instalación del proxy que ha descargado (por ejemplo: `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Pulse **Intro**.

   El proceso de instalación puede tardar varios minutos en completarse. Después de una instalación correcta, aparece un símbolo del sistema en la ventana de terminal.

RPM Command install (instalación DE comando RPM) (sólo Linux)

En el caso de los sistemas Linux que son compatibles con el sistema de gestión de paquetes RPM, puede instalar el proxy de servicios web mediante un archivo RPM opcional.

Pasos

1. Descargue el archivo RPM en el servidor en el que desea instalar el proxy y Unified Manager.
2. Abra una ventana de terminal.
3. Introduzca el siguiente comando:

   ```
   rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
   ```

   En el comando anterior, `nn.nn.nn.nnnn` representa el número de versión.

   El proceso de instalación puede tardar varios minutos en completarse. Después de una instalación correcta, aparece un símbolo del sistema en la ventana de terminal.

Inicie sesión en API y Unified Manager

Web Services incluye documentación de API, que permite interactuar directamente con la API DE REST. También incluye Unified Manager, una interfaz basada en navegador para gestionar varios sistemas de almacenamiento E-Series.

Inicie sesión en la API de servicios web

Después de instalar el proxy de servicios web, puede acceder a la documentación de API interactiva en un explorador.

La documentación de API se ejecuta con cada instancia de Web Services, y también está disponible en formato PDF estático del sitio de soporte de NetApp. Para tener acceso a la versión interactiva, abra un explorador e introduzca la URL que indica dónde reside Web Services (una controladora para la versión incrustada o un servidor para el proxy).

La API de servicios web implementa la especificación OpenAPI (originalmente llamada especificación Swagger).

Para el inicio de sesión inicial, se utilizan las credenciales "admin". "Admin" es considerado un súper administrador con acceso a todas las funciones y funciones.

Pasos

1. Abra un explorador.
2. Introduzca la dirección URL para la implementación de proxy o incrustado:

   - Integrado: `https://<controller>:<port>/devmgr/docs/`

     En esta URL, `<controller>` Es la dirección IP o el FQDN de la controladora y. `<port>` es el número de puerto de gestión de la controladora (el valor predeterminado es 8443).

   - Proxy: `http[s]://<server>:<port>/devmgr/docs/`

En esta URL, `<server>` Es la dirección IP o FQDN del servidor donde está instalado el proxy, y. `<port>` Es el número de puerto de escucha (el número predeterminado es 8080 para HTTP y 8443 para HTTPS).

> Si el puerto de escucha ya está en uso, el proxy detecta el conflicto y le solicita que elija un puerto de escucha diferente.

La documentación de API se abre en el explorador.

3. Cuando se abra la documentación interactiva de la API, vaya al menú desplegable situado en la parte superior derecha de la página y seleccione **utils**.
4. Haga clic en la categoría **Login** para ver los puntos finales disponibles.
5. Haga clic en el punto final **POST: /Login** y, a continuación, haga clic en **probar con ello**.
6. Si inicia sesión por primera vez, introduzca admin como nombre de usuario y contraseña.
7. Haga clic en **Ejecutar**.
8. Para acceder a los extremos para la administración de almacenamiento, vaya al menú desplegable de la parte superior derecha y seleccione **v2**.

   Se muestran las categorías de alto nivel de los puntos finales. Puede desplazarse por la documentación de API tal y como se describe en la tabla.

Zona	Descripción
Menú desplegable	En la parte superior derecha de la página, un menú desplegable proporciona opciones para cambiar entre la versión 2 de la documentación de API (V2), la interfaz de símbolos (Symbol V2) y las utilidades API (utils) para iniciar sesión. Dado que la versión 1 de la documentación de API era una versión preliminar y no estaba disponible de forma general, V1 no se incluye en el menú desplegable.
Categorías	La documentación de API está organizada por categorías de alto nivel (por ejemplo, Administración, Configuración). Haga clic en una categoría para ver los puntos finales relacionados.
Puntos finales	Seleccione un punto final para ver sus rutas de URL, los parámetros necesarios, los cuerpos de respuesta y los códigos de estado que es probable que las direcciones URL devuelvan.

Zona	Descripción
Pruébelo	Interactúe directamente con el punto final haciendo clic en **Inténtelo**. Este botón se proporciona en cada una de las vistas ampliadas de los puntos finales. Al hacer clic en el botón, aparecen campos para introducir parámetros (si corresponde). A continuación, puede introducir valores y hacer clic en **Ejecutar**. La documentación interactiva utiliza JavaScript para realizar la solicitud directamente a la API; no es una solicitud de prueba.

Inicie sesión en Unified Manager

Después de instalar el proxy de servicios web, puede acceder a Unified Manager para gestionar varios sistemas de almacenamiento en una interfaz web.

Para acceder a Unified Manager, abra un explorador e introduzca la URL donde está instalado el proxy. Se admiten los siguientes exploradores en las versiones mencionadas.

Navegador	Versión mínima
Google Chrome	79
Internet Explorer de Microsoft	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

Pasos

1. Abra un explorador e introduzca la siguiente URL:

   `http[s]://<server>:<port>/um`

   En esta URL, `<server>` Representa la dirección IP o el FQDN del servidor donde está instalado el proxy de servicios web, y. `<port>` Representa el número de puerto de escucha (el número predeterminado es 8080 para HTTP y 8443 para HTTPS).

   Se abrirá la página de inicio de sesión en Unified Manager.

2. Si inicia sesión por primera vez, introduzca `admin` para el nombre de usuario, y después establecer y confirmar una contraseña para el usuario administrador.

La contraseña puede tener hasta 30 caracteres. Para obtener más información sobre usuarios y contraseñas, consulte la sección Access Management de la ayuda en línea de Unified Manager.

Configure el proxy de servicios web

Es posible modificar la configuración del proxy de servicios web para cumplir con los requisitos operativos y de rendimiento únicos del entorno.

Detenga o reinicie el servidor web

El servicio de WebServer se inicia durante la instalación y se ejecuta en segundo plano. Durante algunas tareas de configuración, es posible que necesite detener o reiniciar el servicio de WebServer.

Pasos

1. Debe realizar una de las siguientes acciones:

   - Para Windows, vaya al menú **Inicio**, seleccione menú:Herramientas administrativas[Servicios], busque **Servicios Web de SANtricity de NetApp** y, a continuación, seleccione **Detener** o **Reiniciar**.
   - Para Linux, elija el método para detener y reiniciar el servidor web para la versión del sistema operativo. Durante la instalación, un cuadro de diálogo emergente indicó lo que se inició el daemon. Por ejemplo:

     ```
     web_services_proxy webserver installed and started. You can interact with it
     using systemctl start|stop|restart|status web_services_proxy.service
     ```

   El método más común para interactuar con el servicio es mediante el uso `systemctl` comandos.

Resolver conflictos de puerto

Si el proxy de servicios web está en ejecución mientras otra aplicación está disponible en el puerto o la dirección definidos, puede resolver el conflicto de puerto en el archivo wsconfig.xml.1.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:

   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy

2. Agregue la siguiente línea al archivo wsconfig.xml, en el que *n* es el número de puerto:

   ```
   <sslport clientauth="request">*n*</sslport>
   <port>n</port>
   ```

   En la siguiente tabla, se muestran los atributos que controlan los puertos HTTP y HTTPS.

Nombre	Descripción	Nodo principal	Atributos	Obligatorio
gestión de	El nodo raíz para la configuración	Nulo	Versión: La versión del esquema de configuración es actualmente 1.0.	Sí
puerto de sslport	El puerto TCP para escuchar las solicitudes SSL. El valor predeterminado es 8443.	gestión de	Clientauth	No
puerto	El puerto TCP para escuchar la solicitud HTTP, por defecto es 8080.	gestión de	-	No

3. Guarde y cierre el archivo.
4. Reinicie el servicio Webserver para que el cambio surta efecto.

Configuración de balanceo de carga y/o alta disponibilidad

Para usar el proxy de servicios web en una configuración altamente disponible (ha), se puede configurar el balanceo de carga. En una configuración de alta disponibilidad, normalmente un solo nodo recibe todas las solicitudes mientras los demás están en espera o las solicitudes se equilibran de carga en todos los nodos.

El proxy de servicios web puede existir en un entorno altamente disponible (ha), con la mayoría de las API funcionando correctamente independientemente del destinatario de la solicitud. Las etiquetas y carpetas de metadatos son dos excepciones, ya que las etiquetas y las carpetas se almacenan en una base de datos local y no se comparten entre instancias del proxy de servicios web.

Sin embargo, existen algunos problemas de sincronización conocidos que se producen en un pequeño porcentaje de solicitudes. Específicamente, una instancia del proxy puede tener datos más nuevos más rápidamente que una segunda instancia para una ventana pequeña. El proxy de servicios web incluye una configuración especial que elimina este problema de sincronización. Esta opción no está habilitada de forma predeterminada, ya que aumenta la cantidad de tiempo que se tarda en atender las solicitudes de servicio (para la consistencia de datos). Para habilitar esta opción, debe agregar una propiedad a un archivo .INI (para Windows) o a un archivo .SH (para Linux).

Pasos

1. Debe realizar una de las siguientes acciones:
   - Windows: Abra el archivo appserver64.ini y, a continuación, agregue `Dload-balance.enabled=true` propiedad.

     Por ejemplo: `vmarg.7=-Dload-balance.enabled=true`
   - Linux: Abra el archivo webserver.sh y, a continuación, agregue el `Dload-balance.enabled=true` propiedad.

Por ejemplo: `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`

2. Guarde los cambios.
3. Reinicie el servicio Webserver para que el cambio surta efecto.

Desactivar el símbolo HTTPS

Puede deshabilitar los comandos Symbol (ajuste predeterminado) y enviar comandos a través de una llamada a procedimiento remoto (RPC). Esta configuración se puede cambiar en el archivo wsconfig.xml.

De forma predeterminada, el proxy de servicios web envía comandos Symbol a través de HTTPS para todos los sistemas de almacenamiento serie E2800 y E5700 que ejecutan las versiones 08.40 o posteriores de SANtricity OS. Los comandos Symbol enviados a través de HTTPS se autentican en el sistema de almacenamiento. Si es necesario, puede deshabilitar la compatibilidad con símbolos HTTPS y enviar comandos a través de RPC. Siempre que se configura un símbolo a través de RPC, todos los comandos pasivos al sistema de almacenamiento están habilitados sin autenticación.

> Cuando se utiliza Symbol mediante RPC, el proxy de servicios web no se puede conectar a sistemas con el puerto de gestión de Symbol deshabilitado.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. En la `devicemgt.symbolclientstrategy` entrada, sustituya la `httpsPreferred` valor con `rpcOnly`.

   Por ejemplo:

   ```
   <env key="devicemgt.symbolclientstrategy">rpcOnly</env>
   ```

3. Guarde el archivo.

Configurar el uso compartido de recursos de origen cruzado

Puede configurar el uso compartido de recursos de origen cruzado (CORS), que es un mecanismo que utiliza encabezados HTTP adicionales para proporcionar una aplicación web que se ejecuta en un origen para tener permiso para acceder a recursos seleccionados desde un servidor de un origen diferente.

CORS es manejado por el archivo cors.cfg ubicado en el directorio de trabajo. La configuración de CORS está abierta de forma predeterminada, por lo que el acceso entre dominios no está restringido.

Si no hay ningún archivo de configuración, CORS está abierto. Pero si el archivo cors.cfg está presente, entonces se utiliza. Si el archivo cors.cfg está vacío, no puede realizar una solicitud CORS.

Pasos

1. Abra el archivo cors.cfg, que se encuentra en el directorio de trabajo.
2. Agregue las líneas deseadas al archivo.

   Cada línea del archivo de configuración CORS es un patrón de expresión regular que debe coincidir. El encabezado de origen debe coincidir con una línea del archivo cors.cfgl. Si cualquier patrón de línea

coincide con el encabezado de origen, se permite la solicitud. Se compara el origen completo, no sólo el elemento host.

3. Guarde el archivo.

Las solicitudes se coinciden en el host y según el protocolo, como el siguiente:

- Coincidir localhost con cualquier protocolo — `*localhost*`
- Match localhost sólo para HTTPS — `https://localhost*`

Desinstale el proxy de servicios web

Para quitar Web Services Proxy y Unified Manager, puede utilizar cualquier modo (archivo gráfico, consola, silencioso o RPM), independientemente del método que haya utilizado para instalar el proxy.

Desinstalación en modo gráfico

Puede ejecutar la desinstalación en modo gráfico para Windows o Linux. En el modo gráfico, las instrucciones aparecen en una interfaz de estilo Windows.

Pasos

1. Inicie la desinstalación para Windows o Linux de la siguiente manera:
   - Windows — vaya al directorio que contiene el archivo de desinstalación_web_Services_proxy. El directorio predeterminado se encuentra en la siguiente ubicación: C:/Program Files/NetApp/SANtricity Web Services Proxy/. Haga doble clic `uninstall_web_services_proxy.exe`.

     Como alternativa, puede ir al menú:Panel de control[programas > Desinstalar un programa] y, a continuación, seleccionar "proxy de servicios web de SANtricity de NetApp".

   - Linux — vaya al directorio que contiene el archivo de desinstalación del proxy de servicios web. El directorio predeterminado se encuentra en la siguiente ubicación: `/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`
2. Ejecute el siguiente comando:

   ```
   uninstall_web_services_proxy -i gui
   ```

   Aparece la pantalla de bienvenida del proxy de servicios web de SANtricity.

3. En el cuadro de diálogo Desinstalar, haga clic en **Desinstalar**.

   Aparece la barra de progreso Desinstalador y muestra el progreso.

4. Cuando aparezca el mensaje Uninstall Complete (desinstalación completa), haga clic en **Done** (Listo).

Desinstalación en modo de consola

Puede ejecutar la desinstalación en modo de consola para Windows o Linux. En el modo Consola, las indicaciones aparecen en la ventana de terminal.

Pasos

1. Vaya al directorio uninstall_web_Services_proxy.
2. Ejecute el siguiente comando:

   ```
   uninstall_web_services_proxy -i console
   ```

   Se inicia el proceso de desinstalación.

3. Cuando la desinstalación haya finalizado, pulse **Intro** para salir del instalador.

Desinstalación en modo silencioso

Puede ejecutar la desinstalación en modo silencioso para Windows o Linux. En el modo silencioso, no aparecen mensajes de retorno ni secuencias de comandos en la ventana de terminal.

Pasos

1. Vaya al directorio uninstall_web_Services_proxy.
2. Ejecute el siguiente comando:

   ```
   uninstall_web_services_proxy -i silent
   ```

   El proceso de desinstalación se ejecuta, pero no aparecen mensajes de retorno ni secuencias de comandos en la ventana del terminal. Una vez que el proxy de servicios web se ha desinstalado correctamente, aparece un símbolo del sistema en la ventana de terminal.

COMANDO RPM desinstal (sólo Linux)

Puede utilizar un comando RPM para desinstalar el proxy de servicios web de un sistema Linux.

Pasos

1. Abra una ventana de terminal.
2. Introduzca la siguiente línea de comandos:

   ```
   rpm -e santricity_webservices
   ```

   > El proceso de desinstalación podría dejar archivos que no formaban parte de la instalación original. Elimine manualmente estos archivos para quitar Web Services Proxy completamente.

Gestione el acceso de usuarios en el proxy de servicios web

Es posible gestionar el acceso de los usuarios a la API de servicios web y Unified Manager con fines de seguridad.

Información general sobre la gestión de acceso

La gestión de acceso incluye inicios de sesión basados en roles, cifrado de contraseña, autenticación básica e integración LDAP.

Acceso basado en funciones

El control de acceso basado en roles (RBAC) asocia usuarios predefinidos con roles. Cada función otorga permisos a un nivel específico de funcionalidad.

En la siguiente tabla se describe cada rol.

Función	Descripción
security.admin	SSL y gestión de certificados.
storage.admin	Acceso completo de lectura/escritura a la configuración del sistema de almacenamiento.
storage.monitor	Acceso de solo lectura para ver los datos del sistema de almacenamiento.
support.admin	Acceso a todos los recursos de hardware en los sistemas de almacenamiento y operaciones de soporte como la recuperación de AutoSupport (ASUP).

Las cuentas de usuario predeterminadas se definen en el archivo users.propertiesl. Se pueden cambiar cuentas de usuario modificando directamente el archivo users.properties o mediante las funciones Access Management en Unified Manager.

En la siguiente tabla, se enumeran los inicios de sesión de usuario disponibles para el proxy de servicios web.

Inicio de sesión de usuario predefinido	Descripción
admin	Un súper administrador que tiene acceso a todas las funciones e incluye todas las funciones. Para Unified Manager, debe establecer la contraseña en el inicio de sesión por primera vez.
Reducida	El administrador responsable de todo el aprovisionamiento de almacenamiento. Este usuario incluye los siguientes roles: Storage.admin, support.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
seguridad	El usuario responsable de la configuración de seguridad. Este usuario incluye los siguientes roles: Security.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
soporte técnico	El usuario responsable de los recursos de hardware, los datos de fallos y las actualizaciones de firmware. Este usuario incluye los siguientes roles: Support.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.

Inicio de sesión de usuario predefinido	Descripción
supervisar	Un usuario con acceso de solo lectura al sistema. Este usuario incluye únicamente el rol Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
rw (heredado para matrices antiguas)	el usuario rw (lectura/escritura) incluye los siguientes roles: Storage.admin, support.admin y Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.
ro (heredado para cabinas antiguas)	El usuario ro (solo lectura) incluye únicamente el rol Storage.monitor. Esta cuenta está deshabilitada hasta que se defina una contraseña.

Cifrado de contraseñas

Para cada contraseña, puede aplicar un proceso de cifrado adicional mediante la codificación de contraseña SHA256 existente. Este proceso de cifrado adicional aplica un conjunto aleatorio de bytes a cada contraseña (Salt) para cada cifrado hash SHA256. El cifrado SHA256 salado se aplica a todas las contraseñas recién creadas.

Antes de la versión 3.0 de Web Services Proxy, las contraseñas se cifraban sólo mediante hash SHA256. Todas las contraseñas cifradas SHA256 sólo hash conservan esta codificación y siguen siendo válidas en el archivo users.properties. Sin embargo, las contraseñas cifradas SHA256 sólo hash no son tan seguras como las contraseñas con cifrado SHA256 con salado.

Autenticación básica

De forma predeterminada, la autenticación básica está habilitada, lo que significa que el servidor devuelve un desafío de autenticación básico. Esta configuración se puede cambiar en el archivo wsconfig.xml.

LDAP

El proxy de servicios web habilita un protocolo ligero de acceso a directorios (LDAP), un protocolo de aplicación para acceder a servicios distribuidos de información de directorio y mantenerlos. La integración LDAP permite la autenticación de usuarios y la asignación de roles a grupos.

Para obtener información sobre la configuración de la funcionalidad LDAP, consulte las opciones de configuración en la interfaz de Unified Manager o en la sección LDAP de la documentación de API interactiva.

Configurar el acceso del usuario

Para gestionar el acceso de los usuarios, se puede aplicar cifrado adicional a las contraseñas, configurar la autenticación básica y definir el acceso basado en roles.

Aplicar cifrado adicional a las contraseñas

Para obtener el nivel más alto de seguridad, puede aplicar cifrado adicional a las contraseñas mediante la codificación de contraseña SHA256 existente.

Este proceso de cifrado adicional aplica un conjunto aleatorio de bytes a cada contraseña (Salt) para cada cifrado hash SHA256. El cifrado SHA256 salado se aplica a todas las contraseñas recién creadas.

Pasos

1. Abra el archivo users.properties, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Vuelva a introducir la contraseña cifrada como texto sin formato.
3. Ejecute el `securepasswds` Utilidad de línea de comandos para volver a cifrar la contraseña o simplemente reiniciar el proxy de servicios web. Esta utilidad se instala en el directorio raíz de instalación del proxy de servicios web.

> Como alternativa, es posible saldar y hash de contraseñas de usuario local siempre que se realice la edición de contraseñas mediante Unified Manager.

Configurar la autenticación básica

La autenticación básica predeterminada está habilitada, lo que significa que el servidor devuelve un desafío de autenticación básico. Si lo desea, puede cambiar esa configuración en el archivo wsconfig.xmll.

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Modifique la siguiente línea del archivo especificando false (no habilitado) o true (activado).

   Por ejemplo: `<env key="enable-basic-auth">true</env>`
3. Guarde el archivo.
4. Reinicie el servicio Webserver para que el cambio surta efecto.

Configure el acceso basado en roles

Para limitar el acceso de los usuarios a funciones específicas, puede modificar qué roles se especifican para cada cuenta de usuario.

El proxy de servicios web incluye el control de acceso basado en roles (RBAC), en el cual los roles están asociados con usuarios predefinidos. Cada función otorga permisos a un nivel específico de funcionalidad. Puede cambiar los roles asignados a las cuentas de usuario modificando directamente el archivo users.properties.

> También es posible cambiar las cuentas de usuario mediante Access Management en Unified Manager. Para obtener más información, consulte la ayuda en línea disponible con Unified Manager.

Pasos

1. Abra el archivo users.properties, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_Services_proxy/data/config
2. Busque la línea de la cuenta de usuario que desea modificar (almacenamiento, seguridad, supervisión, soporte, rw, o ro).

No modifique el usuario administrador. Se trata de un superusuario con acceso a todas las funciones.

3. Añada o quite los roles especificados, según lo desee.

   Entre los roles, se incluyen:

   - Security.admin — SSL y gestión de certificados.
   - Storage.admin — acceso completo de lectura/escritura a la configuración del sistema de almacenamiento.
   - Storage.monitor — acceso de solo lectura para ver los datos del sistema de almacenamiento.
   - Support.admin — brinda acceso a todos los recursos de hardware en los sistemas de almacenamiento y a operaciones de soporte como la recuperación AutoSupport (ASUP).

     El rol Storage.monitor se requiere para todos los usuarios, incluido el administrador.

4. Guarde el archivo.

Gestione la seguridad y los certificados en el proxy de servicios web

Para obtener seguridad en el proxy de servicios web, es posible especificar una designación de puerto SSL y gestionar certificados. Los certificados identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes.

Habilite SSL

El proxy de servicios web utiliza Secure Sockets Layer (SSL) para obtener seguridad, que se habilita durante la instalación. Puede cambiar la designación de puerto SSL en el archivo wsconfig.xml.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Añada o cambie el número de puerto SSL, de forma similar al ejemplo siguiente:

```
<sslport clientauth="request">8443</sslport>
```

Resultado

Cuando el servidor se inicia con SSL configurado, el servidor busca los archivos del almacén de claves y del almacén de confianza.

- Si el servidor no encuentra un almacén de claves, el servidor utiliza la dirección IP de la primera dirección IPv4 no loopback detectada para generar un almacén de claves y, a continuación, añadir un certificado autofirmado al almacén de claves.

- Si el servidor no encuentra un almacén de confianza o no se especifica el almacén de confianza, el servidor utiliza el almacén de claves como almacén de confianza.

Omitir la validación del certificado

Para admitir conexiones seguras, el proxy de servicios web valida los certificados de los sistemas de almacenamiento con sus propios certificados de confianza. Si es necesario, puede especificar que el proxy omita esa validación antes de conectarse a los sistemas de almacenamiento.

Antes de empezar

- Todas las conexiones a los sistemas de almacenamiento deben ser seguras.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Introduzca `true` en la `trust.all.arrays` entrada, como se muestra en el ejemplo:

```
<env key="trust.all.arrays">true</env>
```

3. Guarde el archivo.

Genere e importe un certificado de gestión de host

Los certificados identifican propietarios de sitios web para lograr conexiones seguras entre servidores y clientes. Para generar e importar certificados de una entidad de certificación (CA) para el sistema host donde está instalado el proxy de servicios web, puede usar extremos de API.

Para gestionar los certificados para el sistema host, debe realizar las siguientes tareas con la API:

- Cree una solicitud de firma de certificación (CSR) para el sistema host.
- Envíe el archivo CSR a una CA y espere que la autoridad envíe los archivos de certificado.
- Importe los certificados firmados al sistema host.

> También puede gestionar los certificados en la interfaz de Unified Manager. Para obtener más información, consulte la ayuda en línea disponible en Unified Manager.

Pasos

1. Inicie sesión en la "Documentación de API interactiva".
2. Vaya al menú desplegable de la parte superior derecha y seleccione **v2**.
3. Expanda el enlace **Administración** y desplácese hacia abajo hasta los puntos finales **/certificados**.
4. Genere el archivo CSR:
   a. Seleccione **POST:/certificates** y, a continuación, seleccione **probar**.

      El servidor web regenera un certificado autofirmado. A continuación, puede introducir información en los campos para definir el nombre común, la organización, la unidad de organización, el código alternativo y otra información utilizada para generar la CSR.

b. Agregue la información necesaria en el panel **valores de ejemplo** para generar un certificado de CA válido y, a continuación, ejecute los comandos.

> No llame a **POST:/certificates** o **POST:/certificates/reset** otra vez, o debe regenerar la CSR. Al llamar a **POST:/certificates** o **POST:/certificates/reset**, está generando un nuevo certificado autofirmado con una nueva clave privada. Si envía una CSR generada antes del último restablecimiento de la clave privada en el servidor, el nuevo certificado de seguridad no funciona. Debe generar una nueva CSR y solicitar un certificado de CA nuevo.

c. Ejecute el extremo **GET:/certificates/Server** para confirmar que el estado actual del certificado es el certificado autofirmado con la información agregada del comando **POST:/certificates**.

   El certificado de servidor (indicado por el alias `jetty`) sigue siendo auto-firmado en este punto.

d. Expanda el extremo **POST:/certificates/export**, seleccione **Inténtelo**, introduzca un nombre de archivo para el archivo CSR y, a continuación, haga clic en **Ejecutar**.

5. Copie y pegue el `fileUrl` En una nueva pestaña del explorador para descargar el archivo CSR y enviar el archivo CSR a una CA válida para solicitar una nueva cadena de certificados de servidor web.
6. Cuando la CA emita una nueva cadena de certificados, use una herramienta del administrador de certificados para extraer los certificados de servidor web, intermedios y raíz, y, a continuación, los importe al servidor del proxy de servicios web:
   a. Expanda el extremo **POST:/sslconfig/Server** y seleccione **probar fuera**.
   b. Introduzca un nombre para el certificado raíz de CA en el campo **alias**.
   c. Seleccione **false** en el campo **placaceMainServerCertificate**.
   d. Vaya a y seleccione el nuevo certificado raíz de CA.
   e. Haga clic en **Ejecutar**.
   f. Confirme que la carga del certificado se ha realizado correctamente.
   g. Repita el procedimiento de carga del certificado de CA para el certificado intermedio de CA.
   h. Repita el procedimiento de carga del certificado para el nuevo archivo de certificado de seguridad del servidor web, excepto en este paso, seleccione **true** en el menú desplegable **placeeMainServerCertificate**.
   i. Confirme que la importación del certificado de seguridad del servidor web se ha realizado correctamente.
   j. Para confirmar que los nuevos certificados raíz, intermedios y de servidor web están disponibles en el almacén de claves, ejecute **GET:/certificates/Server**.
7. Seleccione y expanda el punto final **POST:/certificates/reload** y, a continuación, seleccione **probar**. Cuando se le solicite, si desea reiniciar ambos controladores o no, seleccione **falso**. ("Verdadero" sólo se aplica en el caso de los controladores de matriz doble.) Haga clic en **Ejecutar**.

   El punto final **/certificates/reload** normalmente devuelve una respuesta http 202 correcta. Sin embargo, la recarga del almacén de confianza del servidor web y los certificados del almacén de claves crean una condición de carrera entre el proceso de API y el proceso de recarga de certificados del servidor web. En raras ocasiones, la recarga de certificados del servidor web puede superar el procesamiento de la API. En este caso, la recarga parece fallar aunque se haya completado correctamente. Si esto ocurre, continúe con el siguiente paso de todos modos. Si la recarga realmente falló, el siguiente paso también falla.

8. Cierre la sesión de explorador actual con el proxy de servicios web, abra una sesión de explorador nueva

y confirme que se puede establecer una nueva conexión con el proxy de servicios web.

Mediante el uso de una sesión de exploración incognito o en privado, puede abrir una conexión al servidor sin utilizar los datos guardados de sesiones de exploración anteriores.

Gestione los sistemas de almacenamiento mediante Web Services Proxy

Para gestionar los sistemas de almacenamiento en la red, primero debe detectarlos y después añadirlos a la lista de gestión.

Detectar sistemas de almacenamiento

Es posible establecer la detección automática o detectar manualmente los sistemas de almacenamiento.

Detección automática de sistemas de almacenamiento

Se puede especificar que los sistemas de almacenamiento se detecten automáticamente en la red mediante la modificación de la configuración del archivo wsconfig.xml. De manera predeterminada, la detección automática de IPv6 está deshabilitada y IPv4 está habilitada.

Solo debe proporcionar una dirección IP o DNS de gestión para añadir un sistema de almacenamiento. El servidor detecta automáticamente todas las rutas de administración cuando las rutas no están configuradas o las rutas están configuradas y podridas.

> Si intenta utilizar un protocolo IPv6 para detectar automáticamente sistemas de almacenamiento de la configuración de la controladora después de establecer una conexión inicial, es posible que se produzca un error en el proceso. Entre las posibles causas de este fallo se encuentran problemas durante el reenvío de direcciones IP o la activación de IPv6 en los sistemas de almacenamiento, pero no la activación en el servidor.

Antes de empezar

Antes de habilitar la configuración de detección IPv6, compruebe que la infraestructura admite conectividad IPv6 con los sistemas de almacenamiento para mitigar cualquier problema de conexión.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. En las cadenas de detección automática, cambie la configuración desde `true` para `false`, según se desee. Vea el ejemplo siguiente.

```
<env key="autodiscover.ipv6.enable">true</env>
```

Cuando las rutas están configuradas, pero no configuradas para que el servidor pueda enrutar a las direcciones, se producen errores intermitentes de conexión. Si no puede configurar las direcciones IP para que se puedan enrutar desde el host, desactive la detección automática (cambie la configuración a. `false`).

3. Guarde el archivo.

Detectar y añadir sistemas de almacenamiento con extremos API

Puede usar extremos de API para detectar y añadir sistemas de almacenamiento en la lista gestionada. Este procedimiento crea una conexión de gestión entre el sistema de almacenamiento y la API.

En esta tarea, se describe cómo detectar y añadir sistemas de almacenamiento mediante la API DE REST, para poder gestionar estos sistemas en la documentación de API interactiva. Sin embargo, es posible que se desee gestionar sistemas de almacenamiento en Unified Manager, que proporciona una interfaz fácil de usar. Para obtener más información, consulte la ayuda en línea disponible con Unified Manager.

Antes de empezar

Para los sistemas de almacenamiento con SANtricity versión 11.30 y posteriores, debe habilitarse la interfaz de gestión heredada para Symbol en la interfaz de SANtricity System Manager. De lo contrario, los extremos de detección se fallarán. Para encontrar este ajuste, abra System Manager y vaya a MENU:Configuración[sistema > Configuración adicional > Cambiar interfaz de gestión].

Pasos

1. Inicie sesión en la "Documentación de API interactiva".
2. Detecte los sistemas de almacenamiento:

   a. En la documentación de la API, asegúrese de que **V2** está seleccionado en la lista desplegable y, a continuación, expanda la categoría **sistemas de almacenamiento**.

   b. Haga clic en el punto final **POST: /Discovery** y, a continuación, haga clic en **Inténtelo**.

   c. Introduzca los parámetros como se describe en la tabla.

IP inicial IP final
Reemplace string por el rango de direcciones IP inicial y final para uno o más sistemas de almacenamiento en la red.
UseAgents
Establezca este valor en: • True = utilizar agentes en banda para la exploración de red. • False = no utilice agentes en banda para la exploración de red.
ConnectionTimeout

Introduzca los segundos permitidos para la exploración antes de que se agote el tiempo de espera de la conexión.	
MaxPortsToUse	
Introduzca un número máximo de puertos utilizados para la exploración de red.	

d. Haga clic en **Ejecutar**.

Las acciones de API se ejecutan sin las peticiones del usuario.

El proceso de detección se ejecuta en segundo plano.

a. Asegúrese de que el código devuelve un 202.

b. En **cuerpo de respuesta**, busque el valor devuelto para el Id. De solicitud. Necesita el ID de solicitud para ver los resultados en el siguiente paso.

3. Vea los resultados de la detección de la siguiente manera:

a. Haga clic en el punto final **GET: /Discovery** y, a continuación, haga clic en **Inténtelo**.

b. Introduzca el ID de solicitud del paso anterior. Si deja el **ID de solicitud** en blanco, el extremo tomará por defecto el último ID de solicitud ejecutado.

c. Haga clic en **Ejecutar**.

d. Asegúrese de que el código devuelve 200.

e. En el cuerpo de respuesta, busque su ID de solicitud y las cadenas de sistemas de almacenamiento. Las cadenas tienen un aspecto similar al siguiente ejemplo:

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. Escriba los valores para wwn, etiqueta e direcciones IP. Se necesitan para el siguiente paso.

4. Añada los sistemas de almacenamiento de la siguiente manera:

a. Haga clic en el extremo **POST: /Storage-system** y, a continuación, haga clic en **probar fuera**.

b. Introduzca los parámetros como se describe en la tabla.

id
Introduzca un nombre único para este sistema de almacenamiento. Puede introducir la etiqueta (que se muestra en LA respuesta DE GET: /Discovery), pero el nombre puede ser cualquier cadena que elija. Si no proporciona un valor para este campo, Web Services asigna automáticamente un identificador exclusivo.
ControladorAddresses
Introduzca las direcciones IP que se muestran en la respuesta PARA GET: /Discovery. En el caso de controladoras dobles, las direcciones IP deben separarse con una coma. Por ejemplo: `"IP address 1","IP address 2"`
validar
Introduzca `true`, Para recibir la confirmación de que los servicios Web se pueden conectar al sistema de almacenamiento.
contraseña
Introduzca la contraseña de administración para el sistema de almacenamiento.
wwn
Introduzca el WWN del sistema de almacenamiento (se muestra en la respuesta PARA GET: /Discovery).

c. Quite todas las cadenas después `"enableTrace": true`, de forma que todo el conjunto de cadenas sea similar al ejemplo siguiente:

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

d. Haga clic en **Ejecutar**.

e. Asegúrese de que la respuesta de código es 201, lo que indica que el punto final se ha ejecutado correctamente.

El punto final **Post: /Storage-systems** está en cola. Puede ver los resultados utilizando el extremo **GET: /Storage-systems** en el siguiente paso.

5. Confirme la adición de la lista de la siguiente manera:
   a. Haga clic en el extremo **GET: /Storage-system**.

      No es necesario ningún parámetro.

   b. Haga clic en **Ejecutar**.
   c. Asegúrese de que la respuesta de código es 200, lo que indica que el punto final se ha ejecutado correctamente.
   d. En el cuerpo de respuesta, busque la información del sistema de almacenamiento. Los valores devueltos indican que se agregó correctamente a la lista de cabinas gestionadas, de forma similar al siguiente ejemplo:

```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```

Escale verticalmente el número de sistemas de almacenamiento gestionados

De forma predeterminada, la API puede gestionar hasta 100 sistemas de almacenamiento. Si necesita administrar más, debe mejorar los requisitos de memoria para el servidor.

El servidor está configurado para utilizar 512 MB de memoria. Por cada 100 sistemas de almacenamiento adicionales de la red, añada 250 MB a ese número. No añada más memoria de la que tiene físicamente. Deje suficiente espacio adicional para su sistema operativo y otras aplicaciones.

El tamaño predeterminado de la caché es de 8,192 eventos. El uso aproximado de datos de la caché de eventos MEL es de 1 MB por cada 8,192 eventos. Por tanto, si se conservan los valores predeterminados, el uso de caché debe ser de 1 MB aproximadamente para un sistema de almacenamiento.

Además de la memoria, el proxy utiliza puertos de red para cada sistema de almacenamiento. Linux y Windows consideran los puertos de red como identificadores de archivos. Como medida de seguridad, la mayoría de los sistemas operativos limitan el número de identificadores de archivos abiertos que un proceso o un usuario pueden tener abiertos al mismo tiempo. Especialmente en entornos Linux, donde se considera que las conexiones TCP abiertas son identificadores de archivos, el proxy de servicios web puede superar fácilmente este límite. Dado que la corrección depende del sistema, debe consultar la documentación del sistema operativo para obtener información sobre cómo elevar este valor.

Pasos

1. Debe realizar una de las siguientes acciones:
   - En Windows, vaya al archivo appserver64.init. Localizar la línea, `vmarg.3=-Xmx512M`
   - En Linux, vaya al archivo webserver.shl. Localizar la línea, `JAVA_OPTIONS="-Xmx512M"`
2. Para aumentar la memoria, reemplace `512` Con la memoria deseada en MB.
3. Guarde el archivo.

Administrar el sondeo automático para las estadísticas del proxy de servicios web

Es posible configurar el sondeo automático para todas las estadísticas de disco y volumen en sistemas de almacenamiento detectados.

Descripción general de las estadísticas

Las estadísticas proporcionan información acerca de las tasas de recogida de datos y el rendimiento de los sistemas de almacenamiento.

El proxy de servicios web proporciona acceso a los siguientes tipos de estadísticas:

- Estadísticas sin procesar — total de contadores para puntos de datos en el momento de la recopilación de datos. Las estadísticas sin configurar se pueden utilizar para operaciones de lectura totales o operaciones de escritura totales.
- Estadísticas analizadas: Información calculada para un intervalo. Los ejemplos de estadísticas analizadas son operaciones de entrada/salida (IOPS) de lectura por segundo o rendimiento de escritura.

Las estadísticas sin procesar son lineales y normalmente requieren al menos dos puntos de datos recopilados para derivar datos utilizables de ellos. Las estadísticas analizadas son una derivación de las estadísticas sin procesar, que proporcionan mediciones importantes. Muchos valores que pueden derivarse de las estadísticas sin configurar se muestran en un formato utilizable y momento específico en las estadísticas analizadas para su comodidad.

Es posible recuperar las estadísticas sin procesar independientemente de si el sondeo automático está habilitado o no. Puede agregar el `usecache=true` Cadena de consulta al final de la URL para recuperar las estadísticas en caché del último sondeo. El uso de resultados almacenados en la caché aumenta significativamente el rendimiento de la recuperación de estadísticas. Sin embargo, varias llamadas a una velocidad igual o inferior a la caché de intervalos de sondeo configurada recuperan los mismos datos.

Funcionalidad de estadísticas

El proxy de servicios web proporciona extremos API que permiten recuperar estadísticas sin configurar y analizadas de la controladora y la interfaz desde los modelos de hardware y las versiones de software compatibles.

API de estadísticas sin procesar

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

API de estadísticas analizadas

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

Estas URL recuperan las estadísticas analizadas de la última encuesta y sólo están disponibles cuando se activa el sondeo. Estas direcciones URL incluyen los siguientes datos de entrada y salida:

- Operaciones por segundo
- Rendimiento en megabytes por segundo
- Tiempos de respuesta en milisegundos

Los cálculos se basan en las diferencias entre las iteraciones estadísticas de sondeo, que son las medidas más comunes de rendimiento de almacenamiento. Estas estadísticas son preferibles a las estadísticas no analizadas.

> Cuando se inicia el sistema, no hay ninguna recopilación de estadísticas anterior que utilizar para calcular las diversas métricas, por lo que las estadísticas analizadas requieren al menos un ciclo de sondeo tras el inicio para devolver los datos. Además, si se restablecen los contadores acumulativos, el siguiente ciclo de sondeo tendrá números impredecibles para los datos.

Configurar intervalos de sondeo

Para configurar los intervalos de sondeo, modifique el archivo wsconfig.xml para especificar un intervalo de sondeo en segundos.

> Debido a que las estadísticas se almacenan en la memoria caché, es posible que observe un aumento de aproximadamente 1.5 MB de uso de memoria para cada sistema de almacenamiento.

Antes de empezar

- El proxy debe detectar los sistemas de almacenamiento.

Pasos

1. Abra el archivo wsconfig.xml, ubicado en:
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_Services_proxy
2. Añada la siguiente línea dentro del `<env-entries>` etiquetar, en el que `n` es el número de segundos para el intervalo entre las solicitudes de sondeo:

   ```
   <env key="stats.poll.interval">n</env>
   ```

   Por ejemplo, si se introduce 60, el sondeo comienza a intervalos de 60 segundos. Es decir, el sistema solicita que el sondeo comience 60 segundos después de haber finalizado el periodo de sondeo anterior (independientemente de la duración del periodo de sondeo anterior). Todas las estadísticas están impresas con el tiempo exacto en que fueron recuperadas. El sistema utiliza la Marca de tiempo o la diferencia de tiempo en la que se basa el cálculo de 60 segundos.

3. Guarde el archivo.

Gestione AutoSupport mediante Web Services Proxy

Es posible configurar AutoSupport (ASUP), que recoge datos y luego envía automáticamente esos datos al soporte técnico para la solución de problemas y el análisis de problemas remotos.

Información general de AutoSupport (ASUP)

La función AutoSupport (ASUP) transmite automáticamente los mensajes a NetApp en función de criterios manuales o basados en programaciones.

Cada mensaje de AutoSupport es una colección de archivos de registro, datos de configuración, datos de estado y métricas de rendimiento. De forma predeterminada, AutoSupport transmite los archivos de la siguiente tabla al equipo de soporte de NetApp una vez por semana.

Nombre de archivo	Descripción
x-headers-data.txt	Archivo .txt que contiene la información del encabezado X.
manifest.xml	Archivo .xml en el que se detalla el contenido del mensaje.
arraydata.xml	Un archivo .xml que contiene la lista de datos persistentes del cliente.
appserver-config.txt	Archivo .txt que contiene datos de configuración del servidor de aplicaciones.
wsconfig.txt	Archivo .txt que contiene los datos de configuración del servicio web.

Nombre de archivo	Descripción
host-info.txt	Un archivo .txt que contiene información sobre el entorno del host.
server-logs.7z	Archivo .7z que contiene cada archivo de registro de servidor web disponible.
client-info.txt	Archivo .txt con pares de clave/valor arbitrarios para contadores específicos de aplicaciones como búsquedas de método y de página web.
webservices-profile.json	Estos archivos contienen datos de perfil de WebServices y datos estadísticos de control de Jersey. De forma predeterminada, las estadísticas de supervisión de Jersey están habilitadas. Puede habilitarlos y deshabilitarlos en el archivo wsconfig.xml de la siguiente manera: • Habilitar: `<env key="enable.jersey.statistics">true</env>` • Desactivar: `<env key="enable.jersey.statistics">false</env>`

Configure AutoSupport

AutoSupport está habilitado de forma predeterminada en la instalación; sin embargo, puede cambiar esa configuración o modificar los tipos de entrega.

Habilite o deshabilite AutoSupport

La función AutoSupport está habilitada o deshabilitada durante la instalación inicial del proxy de servicios web, pero puede cambiar esa configuración en el archivo ASUPConfig.

Puede habilitar o deshabilitar AutoSupport a través del archivo ASUPConfig.xml, como se describe en los pasos siguientes. Como alternativa, puede activar o desactivar esta función a través de la API mediante **Configuración** y **POST/asup** y, a continuación, introduciendo "verdadero" o "falso".

1. Abra el archivo ASUPConfig.xml en el directorio de trabajo.
2. Busque las líneas de <asupdata enable="Boolean_value" timestamp="timestamp">
3. Introduzca `true` (activar) o. `false` (desactivar). Por ejemplo:

```
<asupdata enabled="false" timestamp="0">
```

   La entrada de Marca de hora es superflua.

4. Guarde el archivo.

Configurar el método de entrega de AutoSupport

Es posible configurar la función AutoSupport para que use los métodos de entrega HTTPS, HTTP o SMTP. HTTPS es el método de entrega predeterminado.

1. Acceda al archivo ASUPConfig.xml del directorio de trabajo.
2. En la cadena, `<delivery type="n">`, escriba 1, 2 o 3 como se describe en la tabla:

Valor	Descripción
1	**HTTPS** (predeterminado) <delivery type="1">
2	**HTTP** <delivery type="2">

3	**SMTP** — para configurar correctamente el tipo de entrega de AutoSupport a SMTP, debe incluir la dirección del servidor de correo SMTP, junto con los correos electrónicos del remitente y del usuario destinatario, de forma similar al ejemplo siguiente:
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`

Información de copyright

Información de la marca comercial