Gestionar servicios web

ONTAP 9

NetApp
February 12, 2026

Tabla de contenidos

Gestionar servicios web

Información general sobre los servicios web de Manage

Puede habilitar o deshabilitar un servicio web para el clúster o una máquina virtual de almacenamiento (SVM), mostrar la configuración de los servicios web y controlar si los usuarios de un rol pueden acceder a un servicio web.

Puede gestionar los servicios web para el clúster o una SVM de las siguientes formas:

- Activación o desactivación de un servicio Web específico
- Especificar si el acceso a un servicio Web está restringido a sólo HTTP (SSL) cifrado
- Mostrar la disponibilidad de los servicios web
- Permitir o rechazar a los usuarios de una función acceder a un servicio web
- Mostrar los roles que pueden tener acceso a un servicio Web

Para que un usuario pueda acceder a un servicio web, se deben cumplir todas las siguientes condiciones:

- Se debe autenticar al usuario.

  Por ejemplo, un servicio Web puede solicitar un nombre de usuario y una contraseña. La respuesta del usuario debe coincidir con una cuenta válida.

- Debe configurarse el usuario con el método de acceso correcto.

  La autenticación sólo se realiza correctamente para los usuarios con el método de acceso correcto para el servicio web dado. Para el servicio web de la API de ONTAP `ontapi`), los usuarios deben tener el `ontapi` método de acceso. Para todos los demás servicios web, los usuarios deben tener el `http` método de acceso.

  > `security login`Los comandos se usan para gestionar los métodos de acceso y los métodos de autenticación de los usuarios.

- El servicio web debe estar configurado para permitir la función de control de acceso del usuario.

  > Los `vserver services web access` comandos se utilizan para controlar el acceso de un rol a un servicio web.

Si hay un firewall habilitado, la política de firewall para el LIF que se utilizará para los servicios web debe configurarse para permitir HTTP o HTTPS.

Si utiliza HTTPS para el acceso a servicios web, debe habilitar SSL para el clúster o la SVM que ofrece el servicio web, y debe proporcionar un certificado digital para el clúster o la SVM.

Administrar el acceso a los servicios web de ONTAP

Un servicio web es una aplicación a la que los usuarios pueden acceder mediante HTTP o HTTPS. El administrador de clúster puede configurar el motor de protocolo web, configurar SSL, habilitar un servicio web y permitir que los usuarios de un rol accedan a un servicio web.

A partir de ONTAP 9.6, se admiten los siguientes servicios web:

- Infraestructura de Procesador de Servicios (`spi`)

  Este servicio hace que los archivos de registro, volcado de memoria y MIB de un nodo estén disponibles para el acceso HTTP o HTTPS a través de la LIF de gestión de clústeres o de una LIF de gestión de nodos. El valor predeterminado es `enabled`.

  Cuando se recibe una solicitud para acceder a los archivos de registro o a los archivos de volcado de núcleo de un nodo, el `spi` El servicio web crea automáticamente un punto de montaje desde un nodo al volumen raíz de otro nodo donde residen los archivos. No es necesario crear el punto de montaje manualmente.

- API de ONTAP (`ontapi`)

  Este servicio le permite ejecutar API de ONTAP para ejecutar funciones administrativas con un programa remoto. El valor predeterminado es `enabled`.

  Es posible que este servicio sea necesario para algunas herramientas de administración externas. Por ejemplo, si utiliza System Manager, debe dejar este servicio habilitado.

- Descubrimiento Data ONTAP (`disco`)

  Este servicio permite que las aplicaciones de administración externas puedan detectar el clúster en la red. El valor predeterminado es `enabled`.

- Diagnósticos de Soporte (`supdiag`)

  Este servicio controla el acceso a un entorno privilegiado en el sistema para ayudar al análisis y resolución de problemas. El valor predeterminado es `disabled`. Debe habilitar este servicio solo cuando lo indique el soporte técnico.

- System (`sysmgr`Manager)

  Este servicio controla la disponibilidad de System Manager, que se incluye con ONTAP. El valor predeterminado es `enabled`. Este servicio solo es compatible en el clúster.

- Actualización del controlador de administración de la placa base (BMC) del firmware (`FW_BMC`)

  Este servicio le permite descargar archivos de firmware de BMC. El valor predeterminado es `enabled`.

- Documentación de ONTAP (`docs`)

  Este servicio proporciona acceso a la documentación de ONTAP. El valor predeterminado es `enabled`.

- API RESTful de ONTAP (`docs_api`)

  Este servicio proporciona acceso a la documentación de la API RESTful de ONTAP. El valor predeterminado es `enabled`.

- Carga y descarga de archivos (`fud`)

  Este servicio ofrece carga y descarga de archivos. El valor predeterminado es `enabled`.

- Mensajería ONTAP (`ontapmsg`)

  Este servicio admite una interfaz de publicación y suscripción que le permite suscribirse a eventos. El valor predeterminado es `enabled`.

- Portal ONTAP (`portal`)

  Este servicio implementa la puerta de enlace en un servidor virtual. El valor predeterminado es `enabled`.

- Interfaz ONTAP RESTful (`rest`)

  Este servicio es compatible con una interfaz RESTful que se utiliza para gestionar de forma remota todos los elementos de la infraestructura de clúster. El valor predeterminado es `enabled`.

- Soporte del proveedor de servicios de lenguaje de marcado de aserción de seguridad (SAML) (`saml`)

  Este servicio proporciona recursos para admitir el proveedor de servicios SAML. El valor predeterminado es `enabled`.

- Proveedor de Servicios SAML (`saml-sp`)

  Este servicio ofrece servicios como metadatos del SP y el servicio de consumidor de aserción al proveedor de servicios. El valor predeterminado es `enabled`.

A partir de ONTAP 9.7, se admiten los siguientes servicios adicionales:

- Archivos de Copia de Seguridad de Configuración (`backups`)

  Este servicio permite descargar archivos de copia de seguridad de configuración. El valor predeterminado es `enabled`.

- Seguridad ONTAP (`security`)

  Este servicio admite la gestión de token de CSRF para una autenticación mejorada. El valor predeterminado es `enabled`.

Administre el motor de protocolo web en ONTAP

Puede configurar el motor de protocolo web en el clúster para controlar si se permite el acceso web y qué versiones SSL se pueden utilizar. También puede mostrar los ajustes de configuración del motor de protocolo web.

Puede gestionar el motor de protocolo web en el nivel de clúster de las siguientes formas:

- Puede especificar si los clientes remotos pueden utilizar HTTP o HTTPS para acceder al contenido del servicio web mediante `system services web modify` el comando con el `-external` parámetro.
- Puede especificar si se debe utilizar SSLv3 para un acceso web seguro mediante `security config modify` el comando con el `-supported-protocol` parámetro. De forma predeterminada, SSLv3 está deshabilitado. La seguridad de la capa de transporte 1.0 (TLSv1.0) está habilitada y se puede desactivar si es necesario.

  Obtenga más información sobre `security config modify` en el "Referencia de comandos del ONTAP".

- Puede habilitar el modo de cumplimiento del estándar de procesamiento de información federal (FIPS) 140-2 para las interfaces de servicio web del plano de control de todo el clúster.

  De manera predeterminada, el modo de cumplimiento de FIPS 140-2 está deshabilitado.

  - **Cuando el modo de cumplimiento FIPS 140-2 está desactivado**, puede habilitar el modo de cumplimiento FIPS 140-2 estableciendo el `is-fips-enabled` parámetro en `true` para el `security config modify` comando y, a continuación, usando el `security config show` comando para confirmar el estado en línea.
  - **Cuando el modo de cumplimiento FIPS 140-2 está activado**
    - A partir de ONTAP 9.11.1, TLSv1, TLSv1,1 y SSLv3 están deshabilitados, y solo TSLv1,2 y TSLv1,3 permanecen habilitados. Afecta a otros sistemas y comunicaciones internos y externos a ONTAP 9. Si habilita el modo de cumplimiento FIPS 140-2 y, a continuación, se deshabilita TLSv1, TLSv1.1 y SSLv3. TLSv1,2 o TLSv1,3 permanecerán habilitados según la configuración anterior.
    - Para las versiones de ONTAP anteriores a 9.11.1, tanto TLSv1 como SSLv3 están deshabilitados y sólo TLSv1.1 y TLSv1.2 permanecen habilitados. ONTAP evita que habilite TLSv1 y SSLv3 cuando el modo de cumplimiento FIPS 140-2 está habilitado. Si activa el modo de cumplimiento FIPS 140-2 y lo deshabilita posteriormente, TLSv1 y SSLv3 permanecen deshabilitados, pero TLSv1.2 o TLSv1.1 y TLSv1.2 se habilitan en función de la configuración anterior.
- Puede mostrar la configuración de la seguridad de todo el clúster mediante `system security config show` el comando.

  Obtenga más información sobre `security config show` en el "Referencia de comandos del ONTAP".

Si el firewall está habilitado, debe configurarse la política de firewall de la interfaz lógica (LIF) que se utilizará para los servicios web para permitir el acceso HTTP o HTTPS.

Si utiliza HTTPS para acceder a servicios web, debe habilitar también SSL para el clúster o la máquina virtual de almacenamiento (SVM) que ofrezca el servicio web, y debe proporcionar un certificado digital para el clúster o la SVM.

En las configuraciones de MetroCluster, los cambios de configuración que realice para el motor de protocolo web de un clúster no se replican en el clúster de partners.

Comandos ONTAP para administrar el motor de protocolo web

Los `system services web` comandos se utilizan para administrar el motor del protocolo web. Utilice los `system services firewall policy create` `network interface modify` comandos y para permitir que las solicitudes de acceso web pasen por el firewall.

Si desea…	Se usa este comando…
Configure el motor de protocolo web en el nivel de clúster: • Habilite o deshabilite el motor de protocolo web del clúster • Habilite o deshabilite SSLv3 para el clúster • Habilitar o deshabilitar el cumplimiento de la normativa FIPS 140-2 para servicios web seguros (HTTPS)	`system services web modify`
Muestre la configuración del motor de protocolo web en el nivel del clúster, determine si los protocolos web son funcionales en todo el clúster y muestre si el cumplimiento con FIPS 140-2 está habilitado y en línea	`system services web show`
Muestre la configuración del motor de protocolo web en el nivel del nodo y la actividad de la manipulación del servicio web de los nodos del clúster	`system services web node show`
Cree una política de firewall o agregue un servicio de protocolo HTTP o HTTPS a una política de firewall existente para permitir que las solicitudes de acceso web se atraviese por el firewall	`system services firewall policy create` La configuración `-service` del parámetro en `http` o `https` permite que las solicitudes de acceso web pasen por el firewall.
Asociar una política de firewall a una LIF	`network interface modify` Puede usar el `-firewall-policy` parámetro para modificar la política de firewall de una LIF.

Información relacionada

- "modificación de la interfaz de red"

Configurar el acceso a los servicios web de ONTAP

Al configurar el acceso a los servicios web, los usuarios autorizados pueden usar HTTP

o HTTPS para acceder al contenido del servicio en el clúster o una máquina virtual de almacenamiento (SVM).

Pasos

1. Si hay un firewall habilitado, asegúrese de que el acceso HTTP o HTTPS esté configurado en la política de firewall para la LIF que se utilizará para los servicios web:

   Puede comprobar si un firewall está activado mediante el `system services firewall show` comando.

   a. Para verificar que HTTP o HTTPS está configurado en la política de firewall, utilice el `system services firewall policy show` comando.

      `-service`El parámetro `system services firewall policy create` del comando se establece en `http` o `https` para habilitar la política para admitir el acceso web.

   b. Para verificar que la política de firewall que admite HTTP o HTTPS está asociada a la LIF que proporciona servicios web, utilice `network interface show` el comando con el `-firewall-policy` parámetro.

      Obtenga más información sobre `network interface show` en el "Referencia de comandos del ONTAP".

      Utilice `network interface modify` el comando con `-firewall-policy` el parámetro para poner la política de firewall en vigencia para una LIF.

   Obtenga más información sobre `network interface modify` en el "Referencia de comandos del ONTAP".

2. Para configurar el motor de protocolo web a nivel de clúster y hacer que el contenido del servicio web sea accesible, utilice el `system services web modify` comando.
3. Si planea utilizar servicios web seguros (HTTPS), habilite SSL y proporcione información de certificado digital para el clúster o la SVM mediante `security ssl modify` el comando.

   Obtenga más información sobre `security ssl modify` en el "Referencia de comandos del ONTAP".

4. Para habilitar un servicio web para el clúster o la SVM, utilice `vserver services web modify` el comando.

   Debe repetir este paso para cada servicio que desee habilitar para el clúster o la SVM.

5. Para autorizar un rol para acceder a servicios web en el clúster o SVM, utilice `vserver services web access create` el comando.

   La función que concede acceso ya debe existir. Puede mostrar los roles existentes mediante `security login role show` el comando o crear roles nuevos mediante `security login role create` el comando.

   Obtenga más información sobre `security login role show` y `security login role create` en

el "Referencia de comandos del ONTAP".

6. Para un rol autorizado a acceder a un servicio web, asegúrese de que sus usuarios también estén configurados con el método de acceso correcto comprobando la salida del `security login show` comando.

   Para acceder al servicio web de la API de ONTAP `ontapi`), se debe configurar un usuario con el `ontapi` método de acceso. Para acceder a todos los demás servicios web, se debe configurar un usuario con el `http` método de acceso.

   Obtenga más información sobre `security login show` en el "Referencia de comandos del ONTAP".

   Utilice `security login create` el comando para agregar un método de acceso para un usuario. Obtenga más información sobre `security login create` en el "Referencia de comandos del ONTAP".

Comandos ONTAP para administrar servicios web

Los `vserver services web` comandos se utilizan para gestionar la disponibilidad de servicios web para el clúster o una máquina virtual de almacenamiento (SVM). Los `vserver services web access` comandos se utilizan para controlar el acceso de un rol a un servicio web.

Si desea…	Se usa este comando…
Configure un servicio web para el clúster o ANSVM: • Activar o desactivar un servicio Web • Especifique si sólo se puede utilizar HTTPS para acceder a un servicio web	`vserver services web modify`
Muestre la configuración y la disponibilidad de servicios web del clúster o ANSVM	`vserver services web show`
Autorice a un rol para acceder a un servicio web en el clúster o anSVM	`vserver services web access create`
Muestre los roles que están autorizados a acceder a los servicios web en el clúster o anSVM	`vserver services web access show`
Evite que un rol acceda a un servicio web en el clúster o anSVM	`vserver services web access delete`

Información relacionada

"Referencia de comandos del ONTAP"

Comandos para administrar puntos de montaje en nodos ONTAP

`spi`El servicio web crea automáticamente un punto de montaje desde un nodo al volumen raíz de otro nodo tras una solicitud para acceder a los archivos de registro o los archivos principales del nodo. Aunque no necesita gestionar manualmente los puntos de montaje, puede hacerlo mediante los `system node root-mount` comandos.

Si desea…	Se usa este comando…
Crear manualmente un punto de montaje desde un nodo al volumen raíz de otro nodo	`system node root-mount create` Sólo puede existir un único punto de montaje entre un nodo y otro.
Muestra los puntos de montaje existentes en los nodos del clúster, incluida la hora en la que se creó un punto de montaje y su estado actual	`system node root-mount show`
Elimine un punto de montaje de un nodo a el volumen raíz de otro nodo y obligue las conexiones al punto de montaje a cerrarse	`system node root-mount delete`

Información relacionada

"Referencia de comandos del ONTAP"

Administrar SSL en ONTAP

Utilice `security ssl` los comandos para gestionar el protocolo SSL para el clúster o una máquina virtual de almacenamiento (SVM). El protocolo SSL mejora la seguridad del acceso web mediante el uso de un certificado digital para establecer una conexión cifrada entre un servidor web y un navegador.

Puede gestionar SSL para el clúster o una máquina virtual de almacenamiento (SVM) de las siguientes maneras:

- Habilitar SSL
- Generar e instalar un certificado digital y asociarlo con el clúster o SVM
- Mostrar la configuración SSL para ver si SSL se ha habilitado y, si está disponible, el nombre del certificado SSL
- Configurar políticas de firewall para el clúster o SVM para que las solicitudes de acceso web puedan atravesarse
- Definición de las versiones SSL que se pueden utilizar
- Restringir el acceso sólo a solicitudes HTTPS para un servicio Web

Comandos para gestionar SSL

Los `security ssl` comandos se utilizan para gestionar el protocolo SSL para el clúster o una máquina virtual de almacenamiento (SVM).

Si desea…	Se usa este comando…
Habilite SSL para el clúster o una SVM y asocie un certificado digital con él	`security ssl modify`
Muestre la configuración de SSL y el nombre de certificado para el clúster o una SVM	`security ssl show`

Obtenga más información sobre `security ssl modify` y `security ssl show` en el "Referencia de comandos del ONTAP".

Utilice HSTS para servicios web de ONTAP

La Seguridad de Transporte Estricta HTTP (HSTS) es un mecanismo de política de seguridad web que ayuda a proteger los sitios web contra ataques de intermediario, como la degradación de protocolos y el secuestro de cookies. Al implementar el uso de HTTPS, HSTS garantiza el cifrado de todas las comunicaciones entre el navegador del usuario y el servidor. A partir de ONTAP 9.17.1, ONTAP puede implementar conexiones HTTPS para ONTAP servicios web.

> El navegador web solo aplica HSTS tras establecer una conexión HTTPS segura inicial con ONTAP. Si el navegador no establece una conexión segura inicial, no se aplicará HSTS. Consulte la documentación de su navegador para obtener información sobre la administración de HSTS.

Acerca de esta tarea

- Para la versión 9.17.1 y posteriores, HSTS está habilitado de forma predeterminada para los clústeres de ONTAP recién instalados. Al actualizar a la versión 9.17.1, HSTS no está habilitado de forma predeterminada. Debe habilitar HSTS después de la actualización.
- HSTS es compatible con todos "Servicios web de ONTAP" .

Antes de empezar

- Se requieren privilegios avanzados para las siguientes tareas.

Mostrar configuración de HSTS

Puede mostrar la configuración actual de HSTS para verificar si está habilitada y ver la configuración de edad máxima.

Pasos

1. Utilice el `system services web show` Comando para mostrar la configuración actual de los servicios web, incluida la configuración HSTS:

```
cluster-1::system services web*> show

                   External Web Services: true
                               HTTP Port: 80
                              HTTPS Port: 443
                         Protocol Status: online
                     Per Address Limit: 80
                    Wait Queue Capacity: 192
                           HTTP Enabled: true
                 CSRF Protection Enabled: true
Maximum Number of Concurrent CSRF Tokens: 500
       CSRF Token Idle Timeout (Seconds): 900
   CSRF Token Absolute Timeout (Seconds): 0
          Allow Web Management via Cloud: true
Enforce Network Interface Service-Policy: -
                           HSTS Enabled: true
                  HSTS max age (Seconds): 63072000
```

Habilitar HSTS y establecer la edad máxima

A partir de ONTAP 9.17.1, HSTS está habilitado de forma predeterminada en los nuevos clústeres de ONTAP . Si actualiza un clúster existente a la versión 9.17.1 o posterior, deberá habilitar HSTS manualmente para forzar el uso de HTTPS. Puede habilitar HSTS y establecer la antigüedad máxima. Puede cambiar la antigüedad máxima en cualquier momento si HSTS está habilitado. Una vez habilitado HSTS, los navegadores comenzarán a forzar las conexiones seguras solo después de establecer una conexión segura inicial.

Pasos

1. Utilice el `system services web modify` Comando para habilitar HSTS o modificar la edad máxima:

```
system services web modify -hsts-enabled true -hsts-max-age <seconds>
```

`-hsts-max-age` Especifica el tiempo en segundos que el navegador recordará aplicar HTTPS. El valor predeterminado es 63072000 segundos (dos años).

Deshabilitar HSTS

Los navegadores guardan la configuración de edad máxima de HSTS con cada conexión y continúan implementando HSTS durante todo el proceso, incluso si HSTS está deshabilitado en ONTAP. El navegador tardará hasta alcanzar la edad máxima configurada para dejar de implementar HSTS después de su deshabilitación. Si durante este tiempo no se puede establecer una conexión segura, los navegadores que implementan HSTS no permitirán el acceso a los servicios web de ONTAP hasta que se resuelva el problema o expire la edad máxima del navegador.

Pasos

1. Desactivar HSTS mediante el `system services web modify` dominio:

```
system services web modify -hsts-enabled false
```

Información relacionada

"RFC 6797 - Seguridad de transporte estricta HTTP (HSTS)"

Solucionar problemas de acceso al servicio web de ONTAP

Los errores de configuración provocan problemas de acceso al servicio web. Puede resolver los errores garantizando que la LIF, la política de firewall, el motor de protocolo web, los servicios web, los certificados digitales, y la autorización de acceso del usuario está configurada correctamente.

La tabla siguiente le ayuda a identificar y solucionar errores de configuración del servicio web:

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Su navegador web devuelve un `unable to connect failure to establish a connection` error OR cuando intenta acceder a un servicio web.	Es posible que el LIF se haya configurado incorrectamente.	Asegúrese de que puede hacer ping al LIF que proporciona el servicio web. Usted utiliza `network ping` el comando para hacer ping a una LIF.

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Es posible que el firewall esté configurado incorrectamente.	Asegúrese de que se haya configurado una política de firewall para que sea compatible con HTTP o HTTPS y de que la política esté asignada a la LIF que proporciona el servicio web. Los `system services firewall policy` comandos se utilizan para administrar las políticas de firewall. Puede utilizar `network interface modify` el comando con `-firewall -policy` el parámetro para asociar una política a una LIF.	Es posible que el motor de protocolo web esté desactivado.
Asegúrese de que el motor de protocolo web está activado para que los servicios web estén accesibles. `system services web`Los comandos se usan para administrar el motor de protocolo web del clúster.	Su navegador web devuelve un `not found` error cuando intenta acceder a un servicio web.	Es posible que el servicio web esté desactivado.

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Asegúrese de que todos los servicios web a los que desea permitir el acceso están habilitados individualmente. El `vserver services web modify` comando se utiliza para habilitar un servicio web para el acceso.	El explorador Web no puede iniciar sesión en un servicio Web con el nombre de cuenta y la contraseña de un usuario.	El usuario no se puede autenticar, el método de acceso no es correcto o el usuario no está autorizado a acceder al servicio web.
Asegúrese de que la cuenta de usuario exista y esté configurada con el método de acceso y el método de autenticación correctos. Asimismo, asegúrese de que la función del usuario está autorizada para acceder al servicio web. Los `security login` comandos se utilizan para administrar las cuentas de usuario y sus métodos de acceso y métodos de autenticación. Para acceder al servicio web de la API de ONTAP se requiere `ontapi` el método de acceso. El acceso a todos los demás servicios web requiere el `http` método de acceso. Los `vserver services web access` comandos se utilizan para gestionar el acceso de un rol a un servicio web.	Se conecta al servicio web con HTTPS y el explorador web indica que la conexión se ha interrumpido.	Es posible que no tenga habilitado SSL en el clúster ni la SVM que proporciona el servicio web.

Este problema de acceso…	Se produce debido a este error de configuración…	Para solucionar el error…
Compruebe que el clúster o la SVM tengan habilitada SSL y que el certificado digital sea válido. Los `security ssl` comandos se utilizan para administrar la configuración SSL para servidores HTTP y `security certificate show` el comando para mostrar información de certificados digitales.	Se conecta al servicio web mediante HTTPS y el navegador web indica que la conexión no es de confianza.	Es posible que utilice un certificado digital autofirmado.

Información relacionada

- "¿Cuáles son las mejores prácticas para la configuración de red para ONTAP?"
- "ping de red"
- "modificación de la interfaz de red"
- "Generación de certificado de seguridad CSR"
- "instalación del certificado de seguridad"
- "Mostrar certificado de seguridad"
- "seguridad SSL"

Información de copyright

Información de la marca comercial