



# Uso de la supervisión de SNMP

## StorageGRID 11.5

NetApp  
April 11, 2024

# Tabla de contenidos

- Uso de la supervisión de SNMP ..... 1
  - Funcionalidades ..... 1
  - Compatibilidad con versiones de SNMP ..... 1
  - Limitaciones ..... 2
  - Acceso a la MIB ..... 2
  - Configuración del agente SNMP ..... 2
  - Actualización del agente SNMP ..... 13

# Uso de la supervisión de SNMP

Si desea supervisar StorageGRID mediante el protocolo simple de gestión de redes (SNMP), debe configurar el agente SNMP que se incluye con StorageGRID.

- ["Configuración del agente SNMP"](#)
- ["Actualización del agente SNMP"](#)

## Funcionalidades

Cada nodo StorageGRID ejecuta un agente SNMP, o un daemon, que proporciona una base de datos de información de gestión (MIB). El MIB de StorageGRID contiene definiciones de tablas y notificaciones para alertas y alarmas. El MIB también contiene información de descripción del sistema, como la plataforma y el número de modelo de cada nodo. Cada nodo StorageGRID también admite un subconjunto de objetos MIB-II.

Inicialmente, SNMP está deshabilitado en todos los nodos. Al configurar el agente SNMP, todos los nodos StorageGRID reciben la misma configuración.

El agente SNMP de StorageGRID admite las tres versiones del protocolo SNMP. Proporciona acceso MIB de solo lectura para consultas, y puede enviar dos tipos de notificaciones condicionadas por eventos a un sistema de gestión:

- **Trampas** son notificaciones enviadas por el agente SNMP que no requieren el reconocimiento del sistema de administración. Los traps sirven para notificar al sistema de gestión que algo ha sucedido dentro de StorageGRID, por ejemplo, que se activa una alerta.

Las tres versiones de SNMP admiten capturas.

- **Informa** es similar a las trampas, pero requieren el reconocimiento del sistema de administración. Si el agente SNMP no recibe un acuse de recibo en un periodo de tiempo determinado, vuelve a enviar el informe hasta que se reciba un acuse de recibo o se haya alcanzado el valor de reintento máximo.

Las informa son compatibles con SNMPv2c y SNMPv3.

Las notificaciones Trap e INFORM se envían en los siguientes casos:

- Una alerta predeterminada o personalizada se activa en cualquier nivel de gravedad. Para suprimir las notificaciones SNMP de una alerta, debe configurar un silencio para la alerta. Las notificaciones de alerta se envían mediante el nodo de administrador que esté configurado para que sea el remitente preferido.
- Ciertas alarmas (sistema heredado) se activan a niveles de gravedad especificados o superiores.



Las notificaciones SNMP no se envían para cada alarma ni para cada gravedad de alarma.

## Compatibilidad con versiones de SNMP

La tabla proporciona un resumen a grandes rasgos de lo que se admite para cada versión de SNMP.

	<b>SNMPv1</b>	<b>SNMPv2c</b>	<b>SNMPv3</b>
Consultas	Consultas MIB de solo lectura	Consultas MIB de solo lectura	Consultas MIB de solo lectura
Consulta de autenticación	Cadena de comunidad	Cadena de comunidad	Usuario del modelo de seguridad basado en el usuario (USM)
Notificaciones	Sólo capturas	Atrapa e informa	Atrapa e informa
Autenticación de notificaciones	Comunidad de capturas predeterminada o una cadena de comunidad personalizada para cada destino de capturas	Comunidad de capturas predeterminada o una cadena de comunidad personalizada para cada destino de capturas	Usuario USM en cada destino de captura

## Limitaciones

- StorageGRID admite acceso MIB de solo lectura. No se admite el acceso de lectura y escritura.
- Todos los nodos de la cuadrícula reciben la misma configuración.
- SNMPv3: StorageGRID no admite el modo de soporte para transporte (TSM).
- SNMPv3: El único protocolo de autenticación compatible es SHA (HMAC-SHA-96).
- SNMPv3: El único protocolo de privacidad compatible es AES.

## Acceso a la MIB

Puede acceder al archivo de definición MIB en la siguiente ubicación en cualquier nodo StorageGRID:

/Usr/share/snmp/mibs/NETAPP-STORAGEGRID-MIB.txt

### Información relacionada

["Referencia de alertas"](#)

["Referencia de alarmas \(sistema heredado\)"](#)

["Alarmas que generan notificaciones SNMP \(sistema heredado\)"](#)

["Silenciar notificaciones de alerta"](#)

## Configuración del agente SNMP

Puede configurar el agente SNMP de StorageGRID si desea usar un sistema de administración SNMP de terceros para el acceso MIB de solo lectura y las notificaciones.

### Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.

- Debe tener el permiso acceso raíz.

### Acerca de esta tarea

El agente SNMP de StorageGRID admite las tres versiones del protocolo SNMP. Puede configurar el agente para una o más versiones.

### Pasos

1. Seleccione **Configuración > Supervisión > Agente SNMP**.

Aparece la página Agente SNMP.

#### SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.

Enable SNMP 

2. Para activar el agente SNMP en todos los nodos de cuadrícula, active la casilla de verificación **Activar SNMP**.

Aparecen los campos para configurar un agente SNMP.

## SNMP Agent

You can configure SNMP for read-only MIB access and notifications. SNMPv1, SNMPv2c, SNMPv3 are supported. For SNMPv3, only User Security Model (USM) authentication is supported. All nodes in the grid share the same SNMP configuration.

Enable SNMP

System Contact

System Location

Enable SNMP Agent Notifications

Enable Authentication Traps

---

### Community Strings

Default Trap Community

Read-Only Community

String 1  +

---

### Other Configurations

Agent Addresses (0)   USM Users (0)   Trap Destinations (0)

+ Create   Edit   x Remove

Internet Protocol	Transport Protocol	StorageGRID Network	Port
No results found.			

[Save](#)

3. En el campo **Contacto del sistema**, introduzca el valor que desea que StorageGRID proporcione en los mensajes SNMP para sysContact.

El Contacto del sistema normalmente es una dirección de correo electrónico. El valor que proporcione se aplicará a todos los nodos del sistema StorageGRID. **Contacto del sistema** puede tener un máximo de 255 caracteres.

4. En el campo **ubicación del sistema**, introduzca el valor que desea que StorageGRID proporcione en los mensajes SNMP para sysLocation.

La ubicación del sistema puede ser cualquier información útil para identificar dónde se encuentra el sistema StorageGRID. Por ejemplo, puede utilizar la dirección de una instalación. El valor que proporcione se aplicará a todos los nodos del sistema StorageGRID. **Ubicación del sistema** puede tener un máximo de 255 caracteres.

5. Mantenga seleccionada la casilla de verificación **Activar notificaciones de agente SNMP** si desea que el agente SNMP de StorageGRID envíe notificaciones de captura e informe.

Si esta casilla de verificación no está seleccionada, el agente SNMP admite acceso MIB de sólo lectura, pero no envía ninguna notificación SNMP.

6. Active la casilla de verificación **Activar capturas de autenticación** si desea que el agente SNMP de

StorageGRID envíe una captura de autenticación si recibe un mensaje de protocolo autenticado incorrectamente.

7. Si utiliza SNMPv1 o SNMPv2c, complete la sección Community Strings.

Los campos de esta sección se utilizan para la autenticación basada en la comunidad en SNMPv1 o SNMPv2c. Estos campos no se aplican a SNMPv3.

- a. En el campo **Default Trap Community**, introduzca opcionalmente la cadena de comunidad predeterminada que desea utilizar para los destinos de captura.

Según sea necesario, puede proporcionar una cadena de comunidad diferente ("personalizada") cuando usted lo necesite [definir un destino de captura específico](#).

**La comunidad de solapamientos predeterminada** puede tener un máximo de 32 caracteres y no puede contener caracteres en espacios en blanco.

- b. Para **Comunidad de sólo lectura**, introduzca una o más cadenas de comunidad para permitir el acceso MIB de sólo lectura en direcciones de agente IPv4 e IPv6. Haga clic en el signo más **+** para agregar varias cadenas.

Cuando el sistema de gestión consulta el MIB de StorageGRID, envía una cadena de comunidad. Si la cadena de comunidad coincide con uno de los valores especificados aquí, el agente SNMP envía una respuesta al sistema de administración.

Cada cadena de comunidad puede tener un máximo de 32 caracteres y no puede contener caracteres en blanco. Se permiten hasta cinco cadenas.



Para garantizar la seguridad de su sistema StorageGRID, no utilice "public" como cadena de la comunidad. Si no introduce una cadena de comunidad, el agente SNMP utiliza el identificador de grid del sistema StorageGRID como la cadena de comunidad.

8. Si lo desea, seleccione la ficha direcciones del agente en la sección otras configuraciones.

Utilice esta pestaña para especificar una o más «direcciones de escucha». Éstas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas. Cada dirección del agente incluye un protocolo de Internet, un protocolo de transporte, una red StorageGRID y, opcionalmente, un puerto.

Si no configura una dirección de agente, la dirección de escucha predeterminada es el puerto UDP 161 en todas las redes StorageGRID.

- a. Haga clic en **Crear**.

Aparece el cuadro de diálogo Crear dirección del agente.

### Create Agent Address

Internet Protocol  IPv4  IPv6

Transport Protocol  UDP  TCP

StorageGRID Network:

Port:

- b. Para **Internet Protocol**, seleccione si esta dirección utilizará IPv4 o IPv6.
- De forma predeterminada, SNMP utiliza IPv4.
- c. Para **Protocolo de transporte**, seleccione si esta dirección utilizará UDP o TCP.
- De forma predeterminada, SNMP utiliza UDP.
- d. En el campo **Red StorageGRID**, seleccione en qué red StorageGRID se recibirá la consulta.
- Redes de grid, administración y cliente: StorageGRID debería escuchar las consultas SNMP en las tres redes.
  - Red Grid
  - Red de administración
  - Red cliente



Para garantizar la seguridad de las comunicaciones de cliente con StorageGRID, no debe crear una dirección de agente para la red de cliente.

- e. En el campo **Puerto**, introduzca opcionalmente el número de puerto en el que debe escuchar el agente SNMP.

El puerto UDP predeterminado para un agente SNMP es 161, pero puede introducir cualquier número de puerto no utilizado.



Al guardar el agente SNMP, StorageGRID abre automáticamente los puertos de dirección del agente en el firewall interno. Debe asegurarse de que cualquier firewall externo permita el acceso a estos puertos.

- f. Haga clic en **Crear**.

La dirección del agente se crea y se agrega a la tabla.



## Other Configurations

Agent Addresses (2)

USM Users (2)

Trap Destinations (2)

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

9. Si utiliza SNMPv3, seleccione la pestaña usuarios USM en la sección Other Configurations.

Use esta pestaña para definir los usuarios USM que están autorizados a consultar el MIB o a recibir capturas e informes.




Este paso no se aplica si sólo utiliza SNMPv1 o SNMPv2c.


a. Haga clic en **Crear**.


Se muestra el cuadro de diálogo Create USM User.

## Create USM User

Username


Read-Only MIB Access 

Authoritative Engine ID 

Security Level   authPriv  authNoPriv

---

### Authentication


Protocol  SHA

Password

Confirm Password

---

### Privacy

Protocol  AES

Password

Confirm Password

b. Introduzca un **Nombre de usuario** único para este usuario USM.

Los nombres de usuario tienen un máximo de 32 caracteres y no pueden contener caracteres en blanco. No se puede cambiar el nombre de usuario una vez creado el usuario.

c. Active la casilla de verificación **acceso MIB de sólo lectura** si este usuario debe tener acceso de sólo lectura a la MIB.

Si selecciona **acceso MIB de sólo lectura**, el campo **ID de motor autorizado** está desactivado.



Los usuarios USM que tengan acceso a MIB de solo lectura no pueden tener ID de motor.

d. Si este usuario se va a utilizar en un destino de informe, introduzca el **ID de motor autorizado** para

este usuario.



Los destinos de INFORM SNMPv3 deben tener usuarios con ID de motor. El destino de la captura SNMPv3 no puede tener usuarios con ID de motor.

El ID de motor autorizado puede ser de 5 a 32 bytes en hexadecimal.

e. Seleccione un nivel de seguridad para el usuario USM.

- **Authpriv:** Este usuario se comunica con autenticación y privacidad (cifrado). Debe especificar un protocolo y una contraseña de autenticación, y un protocolo y una contraseña de privacidad.
- **AuthNoprivilegios:** Este usuario se comunica con autenticación y sin privacidad (sin cifrado). Debe especificar un protocolo de autenticación y una contraseña.

f. Introduzca y confirme la contraseña que utilizará este usuario para la autenticación.



El único protocolo de autenticación compatible es SHA (HMAC-SHA-96).

g. Si ha seleccionado **authpriv**, introduzca y confirme la contraseña que este usuario utilizará para la privacidad.



El único protocolo de privacidad compatible es AES.

h. Haga clic en **Crear**.

El usuario USM se crea y se añade a la tabla.

#### Other Configurations

Agent Addresses (2)

USM Users (3)

Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	✓	authNoPriv	
<input type="radio"/>	user1		authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3		authPriv	59D39E801256

10. en la sección Other Configurations, seleccione la pestaña Trap Destinations.

La pestaña Destinos de captura permite definir uno o varios destinos para las notificaciones de capturas StorageGRID o informar. Al activar el agente SNMP y hacer clic en **Guardar**, StorageGRID comienza a enviar notificaciones a cada destino definido. Las notificaciones se envían cuando se activan alertas y alarmas. También se envían notificaciones estándar para las entidades MIB-II admitidas (por ejemplo, ifdown y coldStart).

a. Haga clic en **Crear**.

Se muestra el cuadro de diálogo Crear destino de captura.

### Create Trap Destination

Version  SNMPv1  SNMPv2C  SNMPv3

Type  Trap

Host

Port

Protocol   UDP  TCP

Community String   Use the default trap community: No default found  
(Specify the default on the SNMP Agent page.)  
 Use a custom community string

Custom Community String

- b. En el campo **Versión**, seleccione la versión de SNMP que se utilizará para esta notificación.
- c. Complete el formulario en función de la versión seleccionada

Versión	Especifique esta información
SNMPv1	<p><b>Nota:</b> para SNMPv1, el agente SNMP sólo puede enviar capturas. No se admiten los informes.</p> <ol style="list-style-type: none"> <li>i. En el campo <b>Host</b>, introduzca una dirección IPv4 o IPv6 (o FQDN) para recibir la captura.</li> <li>ii. Para <b>Puerto</b>, utilice el valor predeterminado (162), a menos que deba utilizar otro valor. (162 es el puerto estándar para las capturas SNMP).</li> <li>iii. Para <b>Protocolo</b>, utilice el valor predeterminado (UDP). También admite TCP. (UDP es el protocolo de captura SNMP estándar).</li> <li>iv. Utilice la comunidad de capturas predeterminada, si se especificó una en la página Agente SNMP, o introduzca una cadena de comunidad personalizada para este destino de captura.</li> </ol> <p>La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.</p>
SNMPv2c	<ol style="list-style-type: none"> <li>i. Seleccione si el destino se utilizará para los solapamientos o para los informes.</li> <li>ii. En el campo <b>Host</b>, introduzca una dirección IPv4 o IPv6 (o FQDN) para recibir la captura.</li> <li>iii. Para <b>Puerto</b>, utilice el valor predeterminado (162), a menos que deba utilizar otro valor. (162 es el puerto estándar para las capturas SNMP).</li> <li>iv. Para <b>Protocolo</b>, utilice el valor predeterminado (UDP). También admite TCP. (UDP es el protocolo de captura SNMP estándar).</li> <li>v. Utilice la comunidad de capturas predeterminada, si se especificó una en la página Agente SNMP, o introduzca una cadena de comunidad personalizada para este destino de captura.</li> </ol> <p>La cadena de comunidad personalizada puede tener un máximo de 32 caracteres y no puede contener espacios en blanco.</p>

Versión	Especifique esta información
SNMPv3	<ul style="list-style-type: none"> <li>i. Seleccione si el destino se utilizará para los solapamientos o para los informes.</li> <li>ii. En el campo <b>Host</b>, introduzca una dirección IPv4 o IPv6 (o FQDN) para recibir la captura.</li> <li>iii. Para <b>Puerto</b>, utilice el valor predeterminado (162), a menos que deba utilizar otro valor. (162 es el puerto estándar para las capturas SNMP).</li> <li>iv. Para <b>Protocolo</b>, utilice el valor predeterminado (UDP). También admite TCP. (UDP es el protocolo de captura SNMP estándar).</li> <li>v. Seleccione el usuario USM que se utilizará para la autenticación. <ul style="list-style-type: none"> <li>◦ Si ha seleccionado <b>Trap</b>, sólo se mostrarán los usuarios USM sin identificación de motor autorizada.</li> <li>◦ Si ha seleccionado <b>INFORM</b>, sólo se mostrarán los usuarios USM con ID de motor autoritativos.</li> </ul> </li> </ul>

d. Haga clic en **Crear**.

El destino de captura se crea y se añade a la tabla.

#### Other Configurations

Agent Addresses (1)
USM Users (2)
Trap Destinations (2)

**+** Create
 Edit
**×** Remove

Version	Type	Host	Port	Protocol	Community/USM User
<input type="radio"/> SNMPv3	Trap	local		UDP	User: Read only user
<input type="radio"/> SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user

11. Cuando haya completado la configuración del agente SNMP, haga clic en **Guardar**

La nueva configuración del agente SNMP se activa.

#### Información relacionada

["Silenciar notificaciones de alerta"](#)

# Actualización del agente SNMP

Puede que desee deshabilitar las notificaciones SNMP, actualizar cadenas de comunidad, o añadir o quitar direcciones de agente, usuarios USM y destinos de capturas.

## Lo que necesitará

- Debe iniciar sesión en Grid Manager mediante un explorador compatible.
- Debe tener el permiso acceso raíz.

## Acerca de esta tarea

Siempre que actualice la configuración del agente SNMP, tenga en cuenta que debe hacer clic en **Guardar** en la parte inferior de la página Agente SNMP para confirmar los cambios realizados en cada ficha.

## Pasos

1. Seleccione **Configuración > Supervisión > Agente SNMP**.

Aparece la página Agente SNMP.

2. Si desea desactivar el agente SNMP en todos los nodos de cuadrícula, desactive la casilla de verificación **Activar SNMP** y haga clic en **Guardar**.

El agente SNMP está deshabilitado para todos los nodos de grid. Si después vuelve a habilitar el agente, se conserva cualquier configuración de SNMP anterior.

3. Si lo desea, actualice los valores introducidos para **Contacto del sistema y ubicación del sistema**.
4. Opcionalmente, anule la selección de la casilla de verificación **Activar notificaciones de agente SNMP** si ya no desea que el agente SNMP de StorageGRID envíe notificaciones de captura e informe.

Cuando esta casilla de verificación está desactivada, el agente SNMP admite acceso MIB de sólo lectura, pero no envía ninguna notificación SNMP.

5. Opcionalmente, anule la selección de la casilla de verificación **Activar capturas de autenticación** si ya no desea que el agente SNMP de StorageGRID envíe una captura de autenticación cuando reciba un mensaje de protocolo autenticado incorrectamente.
6. Si utiliza SNMPv1 o SNMPv2c, puede actualizar opcionalmente la sección Community Strings.

Los campos de esta sección se utilizan para la autenticación basada en la comunidad en SNMPv1 o SNMPv2c. Estos campos no se aplican a SNMPv3.



Si desea quitar la cadena de comunidad predeterminada, primero debe asegurarse de que todos los destinos de capturas utilicen una cadena de comunidad personalizada.

7. Si desea actualizar las direcciones del agente, seleccione la ficha direcciones del agente en la sección otras configuraciones.

## Other Configurations

Agent Addresses (2)    USM Users (2)    Trap Destinations (2)

	Internet Protocol	Transport Protocol	StorageGRID Network	Port
<input type="radio"/>	IPv4	UDP	Grid Network	161
<input checked="" type="radio"/>	IPv4	UDP	Admin Network	161

Utilice esta pestaña para especificar una o más «direcciones de escucha». Éstas son las direcciones StorageGRID en las que el agente SNMP puede recibir consultas. Cada dirección de agente incluye un protocolo de Internet, un protocolo de transporte, una red StorageGRID y un puerto.

- Para agregar una dirección de agente, haga clic en **Crear**. A continuación, consulte el paso correspondiente a las direcciones del agente en las instrucciones para configurar el agente SNMP.
  - Para editar una dirección de agente, seleccione el botón de opción de la dirección y haga clic en **Editar**. A continuación, consulte el paso correspondiente a las direcciones del agente en las instrucciones para configurar el agente SNMP.
  - Para eliminar una dirección de agente, seleccione el botón de opción de la dirección y haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar esta dirección.
  - Para confirmar los cambios, haga clic en **Guardar** en la parte inferior de la página Agente SNMP.
8. Si desea actualizar usuarios de USM, seleccione la pestaña usuarios de USM en la sección Other Configurations.

## Other Configurations

Agent Addresses (2)    USM Users (3)    Trap Destinations (2)

	Username	Read-Only MIB Access	Security Level	Authoritative Engine ID
<input type="radio"/>	user2	<input checked="" type="checkbox"/>	authNoPriv	
<input type="radio"/>	user1	<input type="checkbox"/>	authNoPriv	B3A73C2F3D6
<input checked="" type="radio"/>	user3	<input type="checkbox"/>	authPriv	59D39E801256

Use esta pestaña para definir los usuarios USM que están autorizados a consultar el MIB o a recibir capturas e informes.

- Para añadir un usuario USM, haga clic en **Crear**. A continuación, consulte el paso para los usuarios de USM en las instrucciones para configurar el agente de SNMP.
- Para editar un usuario USM, seleccione el botón de opción del usuario y haga clic en **Editar**. A



continuación, consulte el paso para los usuarios de USM en las instrucciones para configurar el agente de SNMP.

El nombre de usuario de un usuario USM existente no se puede cambiar. Si necesita cambiar un nombre de usuario, debe eliminar el usuario y crear uno nuevo.



Si agrega o quita un identificador de motor autorizado de un usuario y ese usuario está seleccionado actualmente para un destino, debe editar o quitar el destino, como se describe en el paso [Destino de capturas SNMP](#). De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

- c. Para eliminar un usuario USM, seleccione el botón de opción del usuario y haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar este usuario.



Si el usuario que quitó está actualmente seleccionado para un destino de captura, debe editar o quitar el destino, como se describe en el paso [Destino de capturas SNMP](#). De lo contrario, se produce un error de validación al guardar la configuración del agente SNMP.

### Error

422: Unprocessable Entity

Validation failed. Please check the values you entered for errors.

Undefined trap destination usmUser 'user1'

OK

- a. Para confirmar los cambios, haga clic en **Guardar** en la parte inferior de la página Agente SNMP.

- 1. Si desea actualizar destinos de capturas, seleccione la pestaña Destinos de capturas en la sección otras configuraciones.

#### Other Configurations

Agent Addresses (1)

USM Users (2)

Trap Destinations (2)

Create Edit Remove

	Version	Type	Host	Port	Protocol	Community/USM User
<input type="radio"/>	SNMPv3	Trap	local		UDP	User: Read only user
<input type="radio"/>	SNMPv3	Inform	10.10.10.10	162	UDP	User: Inform user

La pestaña Destinos de captura permite definir uno o varios destinos para las notificaciones de capturas StorageGRID o informar. Al activar el agente SNMP y hacer clic en **Guardar**, StorageGRID comienza a enviar notificaciones a cada destino definido. Las notificaciones se envían cuando se activan alertas y alarmas. También se envían notificaciones estándar para las entidades MIB-II admitidas (por ejemplo,

ifdown y coldStart).

- a. Para agregar un destino de captura, haga clic en **Crear**. A continuación, consulte el paso para los destinos de capturas en las instrucciones para configurar el agente SNMP.
  - b. Para editar un destino de captura, seleccione el botón de opción del usuario y haga clic en **Editar**. A continuación, consulte el paso para los destinos de capturas en las instrucciones para configurar el agente SNMP.
  - c. Para eliminar un destino de captura, seleccione el botón de opción del destino y haga clic en **Quitar**. A continuación, haga clic en **Aceptar** para confirmar que desea eliminar este destino.
  - d. Para confirmar los cambios, haga clic en **Guardar** en la parte inferior de la página Agente SNMP.
2. Cuando haya actualizado la configuración del agente SNMP, haga clic en **Guardar**.

#### **Información relacionada**

["Configuración del agente SNMP"](#)

## Información de copyright

Copyright © 2024 NetApp, Inc. Todos los derechos reservados. Imprimido en EE. UU. No se puede reproducir este documento protegido por copyright ni parte del mismo de ninguna forma ni por ningún medio (gráfico, electrónico o mecánico, incluidas fotocopias, grabaciones o almacenamiento en un sistema de recuperación electrónico) sin la autorización previa y por escrito del propietario del copyright.

El software derivado del material de NetApp con copyright está sujeto a la siguiente licencia y exención de responsabilidad:

ESTE SOFTWARE LO PROPORCIONA NETAPP «TAL CUAL» Y SIN NINGUNA GARANTÍA EXPRESA O IMPLÍCITA, INCLUYENDO, SIN LIMITAR, LAS GARANTÍAS IMPLÍCITAS DE COMERCIALIZACIÓN O IDONEIDAD PARA UN FIN CONCRETO, CUYA RESPONSABILIDAD QUEDA EXIMIDA POR EL PRESENTE DOCUMENTO. EN NINGÚN CASO NETAPP SERÁ RESPONSABLE DE NINGÚN DAÑO DIRECTO, INDIRECTO, ESPECIAL, EJEMPLAR O RESULTANTE (INCLUYENDO, ENTRE OTROS, LA OBTENCIÓN DE BIENES O SERVICIOS SUSTITUTIVOS, PÉRDIDA DE USO, DE DATOS O DE BENEFICIOS, O INTERRUPCIÓN DE LA ACTIVIDAD EMPRESARIAL) CUALQUIERA SEA EL MODO EN EL QUE SE PRODUJERON Y LA TEORÍA DE RESPONSABILIDAD QUE SE APLIQUE, YA SEA EN CONTRATO, RESPONSABILIDAD OBJETIVA O AGRAVIO (INCLUIDA LA NEGLIGENCIA U OTRO TIPO), QUE SURJAN DE ALGÚN MODO DEL USO DE ESTE SOFTWARE, INCLUSO SI HUBIEREN SIDO ADVERTIDOS DE LA POSIBILIDAD DE TALES DAÑOS.

NetApp se reserva el derecho de modificar cualquiera de los productos aquí descritos en cualquier momento y sin aviso previo. NetApp no asume ningún tipo de responsabilidad que surja del uso de los productos aquí descritos, excepto aquello expresamente acordado por escrito por parte de NetApp. El uso o adquisición de este producto no lleva implícita ninguna licencia con derechos de patente, de marcas comerciales o cualquier otro derecho de propiedad intelectual de NetApp.

Es posible que el producto que se describe en este manual esté protegido por una o más patentes de EE. UU., patentes extranjeras o solicitudes pendientes.

LEYENDA DE DERECHOS LIMITADOS: el uso, la copia o la divulgación por parte del gobierno están sujetos a las restricciones establecidas en el subpárrafo (b)(3) de los derechos de datos técnicos y productos no comerciales de DFARS 252.227-7013 (FEB de 2014) y FAR 52.227-19 (DIC de 2007).

Los datos aquí contenidos pertenecen a un producto comercial o servicio comercial (como se define en FAR 2.101) y son propiedad de NetApp, Inc. Todos los datos técnicos y el software informático de NetApp que se proporcionan en este Acuerdo tienen una naturaleza comercial y se han desarrollado exclusivamente con fondos privados. El Gobierno de EE. UU. tiene una licencia limitada, irrevocable, no exclusiva, no transferible, no sublicenciable y de alcance mundial para utilizar los Datos en relación con el contrato del Gobierno de los Estados Unidos bajo el cual se proporcionaron los Datos. Excepto que aquí se disponga lo contrario, los Datos no se pueden utilizar, desvelar, reproducir, modificar, interpretar o mostrar sin la previa aprobación por escrito de NetApp, Inc. Los derechos de licencia del Gobierno de los Estados Unidos de América y su Departamento de Defensa se limitan a los derechos identificados en la cláusula 252.227-7015(b) de la sección DFARS (FEB de 2014).

## Información de la marca comercial

NETAPP, el logotipo de NETAPP y las marcas que constan en <http://www.netapp.com/TM> son marcas comerciales de NetApp, Inc. El resto de nombres de empresa y de producto pueden ser marcas comerciales de sus respectivos propietarios.