



Configurar la interfaz de BMC (SG6000)

StorageGRID

NetApp
April 10, 2024

Tabla de contenidos

- Configurar la interfaz de BMC (SG6000) 1
 - Cambie la contraseña raíz de la interfaz de BMC 1
 - Establezca la dirección IP para el puerto de administración de BMC 2
 - Acceda a la interfaz de BMC 4
 - Configurar los ajustes SNMP para el controlador SG6000-CN 6
 - Configure notificaciones por correo electrónico para las alertas 7

Configurar la interfaz de BMC (SG6000)

La interfaz de usuario del controlador de administración de la placa base (BMC) del controlador SG6000-CN proporciona información de estado sobre el hardware y permite configurar los ajustes SNMP y otras opciones para el controlador SG6000-CN.

Cambie la contraseña raíz de la interfaz de BMC

Por motivos de seguridad, debe cambiar la contraseña del usuario raíz del BMC.

Lo que necesitará

- El cliente de gestión está usando un [navegador web compatible](#).

Acerca de esta tarea

Al instalar el dispositivo por primera vez, el BMC utiliza una contraseña predeterminada para el usuario raíz (root/calvin). Debe cambiar la contraseña del usuario raíz para proteger el sistema.

Pasos

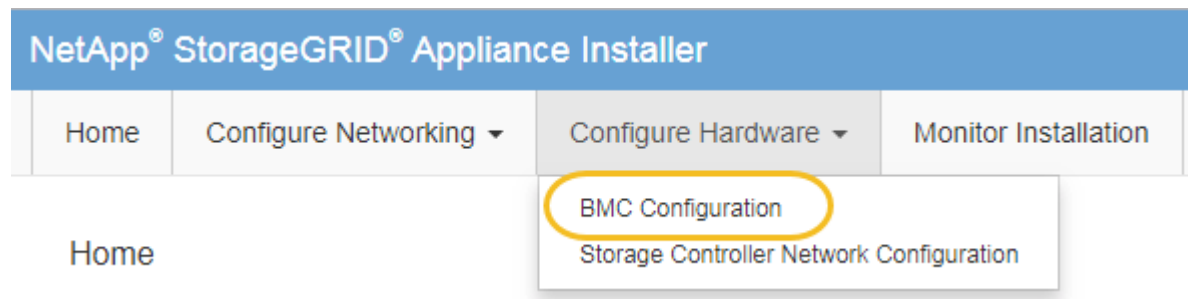
- Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID:

`https://Appliance_Controller_IP:8443`

Para *Appliance_Controller_IP*, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

Aparece la página de inicio del instalador de dispositivos de StorageGRID.

- Seleccione **Configurar hardware Configuración de BMC**.



Aparece la página Configuración de la controladora de gestión de placa base.

- Introduzca una nueva contraseña para la cuenta raíz en los dos campos proporcionados.

Baseboard Management Controller Configuration

User Settings

Root Password
Confirm Root Password

4. Haga clic en **Guardar**.

Establezca la dirección IP para el puerto de administración de BMC

Para poder acceder a la interfaz del BMC, debe configurar la dirección IP del puerto de administración del BMC en el controlador SG6000-CN.

Lo que necesitará

- El cliente de gestión está usando un [navegador web compatible](#).
- Está usando cualquier cliente de gestión que pueda conectarse a una red StorageGRID.
- El puerto de gestión del BMC está conectado a la red de gestión que tiene previsto utilizar.



Acerca de esta tarea

Para fines de soporte, el puerto de gestión del BMC permite un acceso bajo al hardware.



Solo debe conectar este puerto a una red de gestión interna segura y de confianza. Si no hay ninguna red disponible, deje el puerto BMC desconectado o bloqueado, a menos que el soporte técnico solicite una conexión a BMC.

Pasos

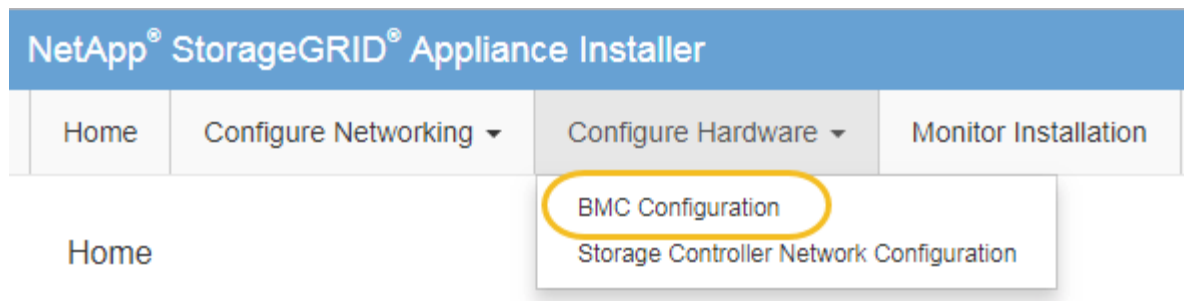
1. Desde el cliente, introduzca la URL del instalador de dispositivos de StorageGRID:

`https://SG6000-CN_Controller_IP:8443`

Para SG6000-CN_Controller_IP, Utilice la dirección IP del dispositivo en cualquier red StorageGRID.

Aparece la página de inicio del instalador de dispositivos de StorageGRID.

2. Seleccione **Configurar hardware Configuración de BMC**.



Aparece la página Configuración de la controladora de gestión de placa base.

3. Anote la dirección IPv4 que se muestra automáticamente.

DHCP es el método predeterminado para asignar una dirección IP a este puerto.



Puede que los valores de DHCP deban tardar varios minutos en aparecer.

Baseboard Management Controller Configuration

LAN IP Settings

IP Assignment	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
MAC Address	d8:c4:97:28:50:62
IPv4 Address (CIDR)	10.224.3.225/21
Default gateway	10.224.0.1

Cancel	Save
--------	------

4. De manera opcional, establezca una dirección IP estática para el puerto de gestión del BMC.



Debe asignar una IP estática al puerto de gestión de BMC o una concesión permanente para la dirección en el servidor DHCP.

- Seleccione **estático**.
- Introduzca la dirección IPv4 mediante la notación CIDR.
- Introduzca la pasarela predeterminada.

LAN IP Settings

IP Assignment	<input checked="" type="radio"/> Static <input type="radio"/> DHCP
MAC Address	d8:c4:97:28:50:62
IPv4 Address (CIDR)	10.224.3.225/21
Default gateway	10.224.0.1

Cancel Save

d. Haga clic en **Guardar**.

Puede que los cambios se apliquen en unos minutos.

Acceda a la interfaz de BMC

Puede acceder a la interfaz del BMC en el controlador SG6000-CN utilizando la dirección DHCP o IP estática para el puerto de administración del BMC.

Lo que necesitará

- El puerto de administración de BMC del controlador SG6000-CN está conectado a la red de administración que se va a utilizar.



- El cliente de gestión está usando un [navegador web compatible](#).

Pasos

1. Introduzca la dirección URL de la interfaz del BMC:

`https://BMC_Port_IP`

Para *BMC_Port_IP*, Utilice la dirección IP estática o DHCP para el puerto de administración del BMC.

Aparece la página de inicio de sesión de BMC.



Si aún no ha configurado BMC_Port_IP, siga las instrucciones de [Configurar la interfaz de BMC \(SG6000\)](#). Si no puede seguir este procedimiento debido a un problema de hardware y aún no ha configurado una dirección IP de BMC, es posible que aún pueda acceder al BMC. De forma predeterminada, el BMC obtiene una dirección IP mediante DHCP. Si DHCP está activado en la red BMC, el administrador de red puede proporcionar la dirección IP asignada al BMC MAC, que se imprime en la etiqueta situada en la parte frontal del controlador SG6000-CN. Si DHCP no está habilitado en la red BMC, el BMC no responderá después de unos minutos y se asignará la IP estática predeterminada 192.168.0.120. Es posible que necesite conectar su portátil directamente al puerto BMC y cambiar la configuración de red para asignar una IP a su portátil 192.168.0.200/24, para navegar a 192.168.0.120.

2. Introduzca el nombre de usuario y la contraseña de raíz con la contraseña que estableció al usuario [se ha cambiado la contraseña raíz predeterminada](#):

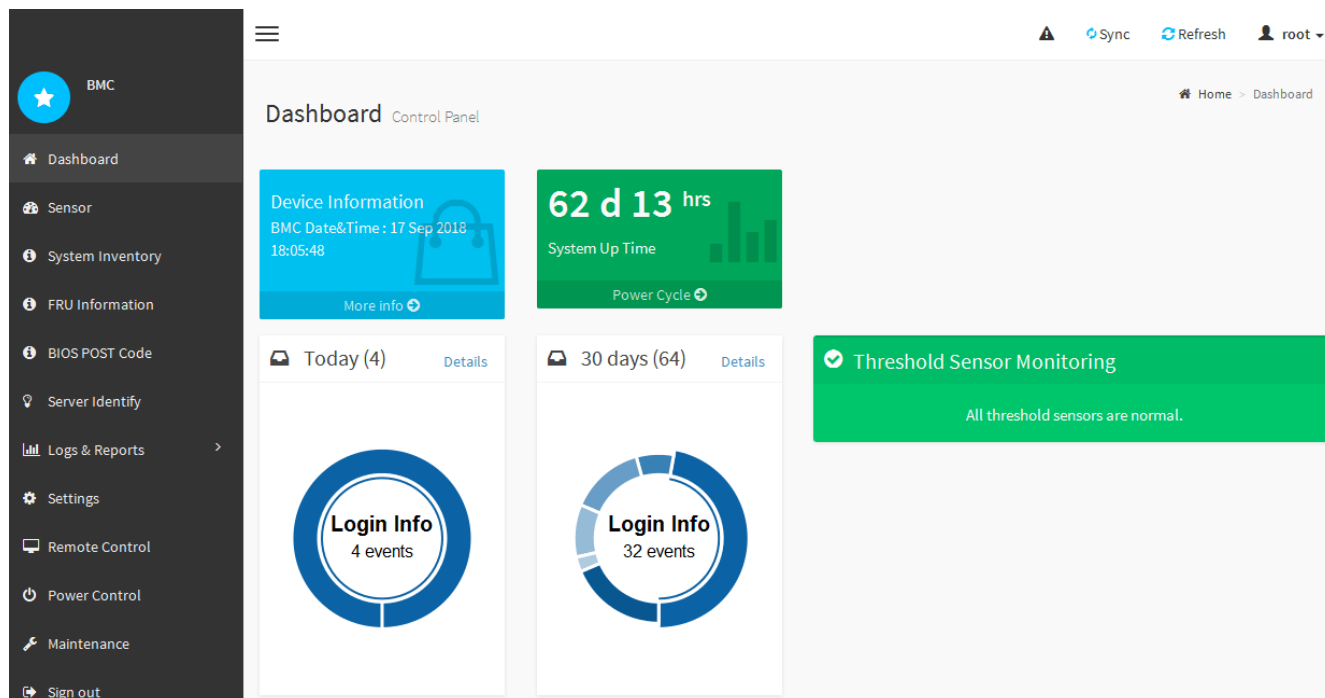


☐ Remember Username

[Sign me in](#)

[I forgot my password](#)

3. Seleccione **Iniciar sesión**.



4. Opcionalmente, cree usuarios adicionales seleccionando **Ajustes Gestión de usuarios** y haciendo clic en cualquier usuario "desactivado".



Cuando los usuarios inician sesión por primera vez, es posible que se les pida que cambien su contraseña para aumentar la seguridad.

Configurar los ajustes SNMP para el controlador SG6000-CN

Si está familiarizado con la configuración de SNMP para el hardware, puede utilizar la interfaz BMC para configurar los ajustes SNMP para el controlador SG6000-CN. Puede proporcionar cadenas de comunidad seguras, habilitar capturas SNMP y especificar hasta cinco destinos SNMP.

Lo que necesitará

- Sabe cómo acceder al panel de BMC.
- Tiene experiencia en la configuración de la configuración de SNMP para el equipo SNMPv1-v2c.



Es posible que los ajustes de BMC realizados por este procedimiento no se conserven si el SG6000-CN falla y se tiene que sustituir. Asegúrese de que tiene un registro de todos los ajustes que ha aplicado, para que se puedan volver a aplicar fácilmente después de reemplazar el hardware si es necesario.

Pasos

1. En el panel del BMC, seleccione **Ajustes Ajustes SNMP**.
2. En la página SNMP Settings (Configuración SNMP), seleccione **Enable SNMP V1/V2** (Activar SNMP V1/V2*) y, a continuación, proporcione una cadena de comunidad de sólo lectura y una cadena de comunidad de lectura y escritura.

La cadena de comunidad de sólo lectura es como un ID de usuario o una contraseña. Debe cambiar este valor para evitar que los intrusos obtengan información acerca de la configuración de la red. La cadena de comunidad de lectura y escritura protege el dispositivo contra cambios no autorizados.

3. Opcionalmente, seleccione **Activar solapamiento** e introduzca la información necesaria.



Introduzca la IP de destino para cada captura SNMP mediante una dirección IP. No se admiten los nombres de dominio completos.

Habilite las capturas si desea que el controlador SG6000-CN envíe notificaciones inmediatas a una consola SNMP cuando se encuentre en un estado inusual. Los traps pueden indicar que se han superado los fallos de hardware de varios componentes o umbrales de temperatura.

4. Opcionalmente, haga clic en **Enviar captura de prueba** para probar la configuración.
5. Si la configuración es correcta, haga clic en **Guardar**.

Configure notificaciones por correo electrónico para las alertas

Si desea que las notificaciones de correo electrónico se envíen cuando se produzcan alertas, debe utilizar la interfaz de BMC para configurar las opciones SMTP, los usuarios, los destinos LAN, las directivas de alerta y los filtros de eventos.



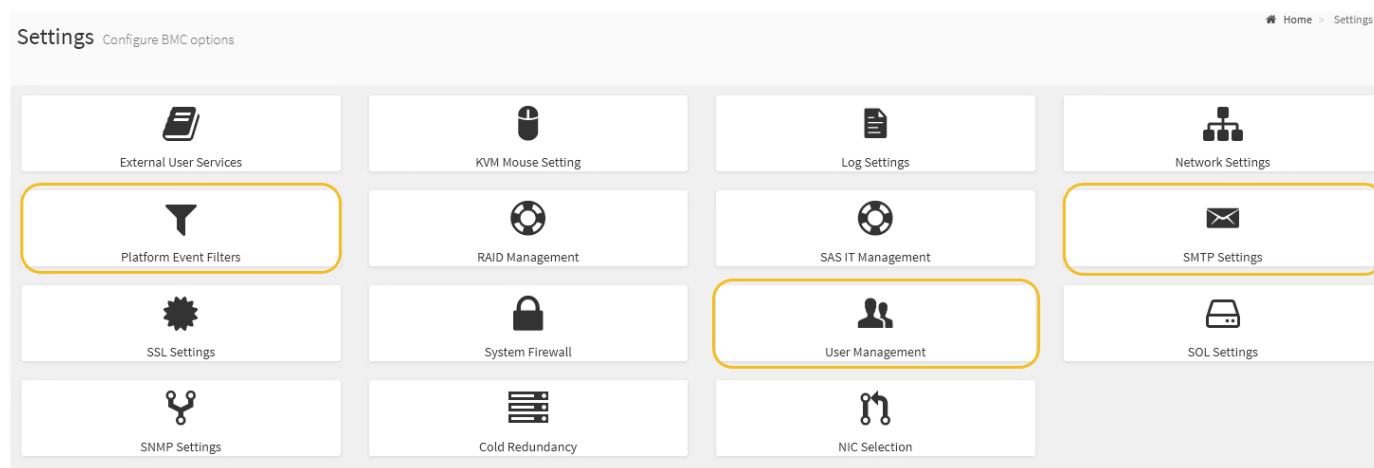
Es posible que los ajustes de BMC realizados por este procedimiento no se conserven si el SG6000-CN falla y se tiene que sustituir. Asegúrese de que tiene un registro de todos los ajustes que ha aplicado, para que se puedan volver a aplicar fácilmente después de reemplazar el hardware si es necesario.

Lo que necesitará

Sabe cómo acceder al panel de BMC.

Acerca de esta tarea

En la interfaz del BMC, utilice las opciones **Configuración SMTP**, **Administración de usuarios** y **Filtros de sucesos de plataforma** de la página Configuración para configurar notificaciones por correo electrónico.



Pasos

1. Configure los ajustes de SMTP.
 - a. Seleccione **Ajustes Ajustes SMTP**.
 - b. Para el ID de correo electrónico del remitente, introduzca una dirección de correo electrónico válida.

Esta dirección de correo electrónico se proporciona como dirección de origen cuando el BMC envía correo electrónico.

2. Configurar los usuarios para que reciban alertas.
 - a. En el panel de control del BMC, seleccione **Configuración Administración de usuarios**.
 - b. Añada al menos un usuario para recibir notificaciones de alerta.

La dirección de correo electrónico que configure para un usuario es la dirección a la que el BMC envía notificaciones de alerta. Por ejemplo, puede agregar un usuario genérico, como «usuario de notificación» y utilizar la dirección de correo electrónico de una lista de distribución de correo electrónico del equipo de soporte técnico.

3. Configure el destino de LAN para las alertas.
 - a. Seleccione **Ajustes Filtros de sucesos de plataforma Destinos LAN**.
 - b. Configure al menos un destino de LAN.
 - Seleccione **correo electrónico** como tipo de destino.
 - En Nombre de usuario de BMC, seleccione un nombre de usuario que haya añadido anteriormente.
 - Si agregó varios usuarios y desea que todos reciban mensajes de correo electrónico de notificación, debe agregar un destino LAN para cada usuario.
 - c. Envía una alerta de prueba.

4. Configurar directivas de alerta para poder definir cuándo y dónde envía alertas el BMC.
 - a. Seleccione **Configuración Filtros de sucesos de plataforma Directivas de alerta**.
 - b. Configure al menos una directiva de alerta para cada destino de LAN.
 - Para número de grupo de directivas, seleccione **1**.
 - Para Acción de directiva, seleccione **siempre enviar alerta a este destino**.
 - Para el canal LAN, seleccione **1**.
 - En el Selector de destinos, seleccione el destino LAN de la directiva.

5. Configurar filtros de eventos para dirigir las alertas de diferentes tipos de eventos a los usuarios correspondientes.
 - a. Seleccione **Ajustes Filtros de sucesos de plataforma Filtros de sucesos**.
 - b. Para el número de grupo de políticas de alerta, introduzca **1**.
 - c. Cree filtros para cada evento del que desee que se notifique al grupo de directivas de alerta.
 - Puede crear filtros de eventos para acciones de alimentación, eventos de sensor específicos o todos los eventos.
 - Si no está seguro de qué eventos debe supervisar, seleccione **todos los sensores** para el tipo de sensor y **todos los eventos** para las opciones de evento. Si recibe notificaciones no deseadas, puede cambiar sus selecciones más adelante.

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.