



Konfiguration der BMC-Schnittstelle (SGF6112, SG6000, SG100 und SG1000)

StorageGRID 11.7

NetApp
April 12, 2024

Inhalt

- Konfiguration der BMC-Schnittstelle (SGF6112, SG6000, SG100 und SG1000) 1
- BMC-Schnittstelle: Überblick (SGF6112, SG6000, SG100 und SG1000) 1
- Ändern Sie das Admin- oder Root-Passwort für die BMC-Schnittstelle 1
- Legen Sie die IP-Adresse für den BMC-Managementport fest 2
- Greifen Sie auf die BMC-Schnittstelle zu 5
- Konfigurieren Sie die SNMP-Einstellungen für BMC 6
- E-Mail-Benachrichtigungen für BMC-Warnungen einrichten 7

Konfiguration der BMC-Schnittstelle (SGF6112, SG6000, SG100 und SG1000)

BMC-Schnittstelle: Überblick (SGF6112, SG6000, SG100 und SG1000)

Die Benutzeroberfläche des Baseboard Management Controllers (BMC) auf der SGF6112-, SG6000- oder Services-Appliance liefert Statusinformationen zur Hardware und ermöglicht Ihnen die Konfiguration von SNMP-Einstellungen und anderen Optionen für die Appliances.

Gehen Sie wie folgt vor, um den BMC bei der Installation des Geräts zu konfigurieren:

- ["Ändern Sie das Admin- oder Root-Passwort für die BMC-Schnittstelle"](#)
- ["Legen Sie die IP-Adresse für den BMC-Managementport fest"](#)
- ["Greifen Sie auf die BMC-Schnittstelle zu"](#)
- ["Konfigurieren Sie die SNMP-Einstellungen"](#)
- ["E-Mail-Benachrichtigungen für BMC-Warnungen einrichten"](#)

Wenn die Appliance bereits in einem Grid installiert wurde und StorageGRID-Software ausgeführt wird, gehen Sie wie folgt vor:



- ["Stellen Sie das Gerät in den Wartungsmodus"](#) Um auf das Installationsprogramm für die StorageGRID Appliance zuzugreifen.
- Siehe ["Legen Sie die IP-Adresse für den BMC-Managementport fest"](#) Für Informationen über den Zugriff auf die BMC-Schnittstelle mithilfe des StorageGRID-Appliance-Installationsprogramms.

Ändern Sie das Admin- oder Root-Passwort für die BMC-Schnittstelle

Aus Sicherheitsgründen müssen Sie das Kennwort für den Admin- oder Root-Benutzer des BMC ändern.

Bevor Sie beginnen

Der Management-Client verwendet ein ["Unterstützter Webbrowser"](#).

Über diese Aufgabe

Wenn Sie die Appliance zum ersten Mal installieren, verwendet der BMC ein Standardkennwort für den Admin- oder Root-Benutzer. Sie müssen das Passwort für den Administrator oder Root-Benutzer ändern, um Ihr System zu sichern.

Der Standardbenutzer hängt davon ab, wann Sie Ihre StorageGRID-Appliance installiert haben. Der Standardbenutzer ist **admin** für neue Installationen und **root** für ältere Installationen.

Schritte

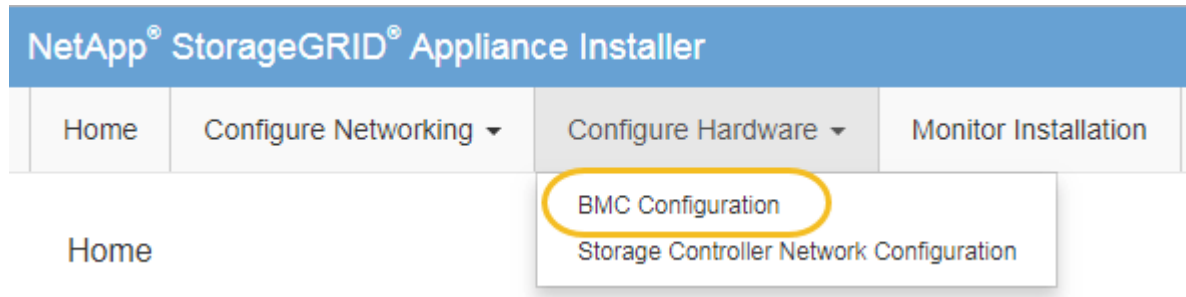
1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:

https://Appliance_IP:8443

Für *Appliance_IP*, Verwenden Sie die IP-Adresse für die Appliance in einem beliebigen StorageGRID-Netzwerk.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Hardware konfigurieren > BMC-Konfiguration**.



Die Seite Baseboard Management Controller Configuration wird angezeigt.

3. Geben Sie in den beiden Feldern ein neues Passwort für das Admin- oder Root-Konto ein.

4. Klicken Sie Auf **Speichern**.

Legen Sie die IP-Adresse für den BMC-Managementport fest

Bevor Sie auf die BMC-Schnittstelle zugreifen können, konfigurieren Sie die IP-Adresse für den BMC-Verwaltungsport auf den SGF6112-, SG6000-CN-Controllern oder Service-Appliances.

Wenn Sie mit ConfigBuilder eine JSON-Datei erstellen, können Sie IP-Adressen automatisch konfigurieren. Siehe "[Automatisierung der Appliance-Installation und -Konfiguration](#)".

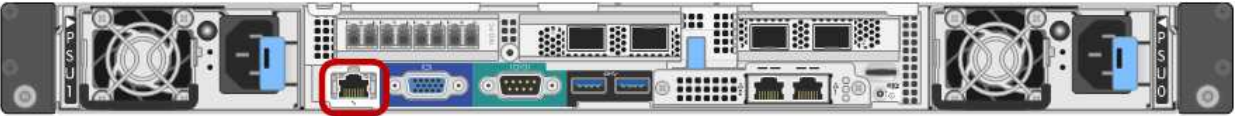
Bevor Sie beginnen

- Der Management-Client verwendet ein "[Unterstützter Webbrowser](#)".
- Sie verwenden jeden Management-Client, der eine Verbindung zu einem StorageGRID-Netzwerk herstellen kann.
- Der BMC-Management-Port ist mit dem Managementnetzwerk verbunden, das Sie verwenden möchten.

SG6112



SG6000



SG1000



SG100



Über diese Aufgabe

Zu Support-Zwecken ermöglicht der BMC-Management-Port einen niedrigen Hardwarezugriff.



Sie sollten diesen Port nur mit einem sicheren, vertrauenswürdigen, internen Managementnetzwerk verbinden. Wenn kein solches Netzwerk verfügbar ist, lassen Sie den BMC-Port nicht verbunden oder blockiert, es sei denn, eine BMC-Verbindung wird vom technischen Support angefordert.

Schritte

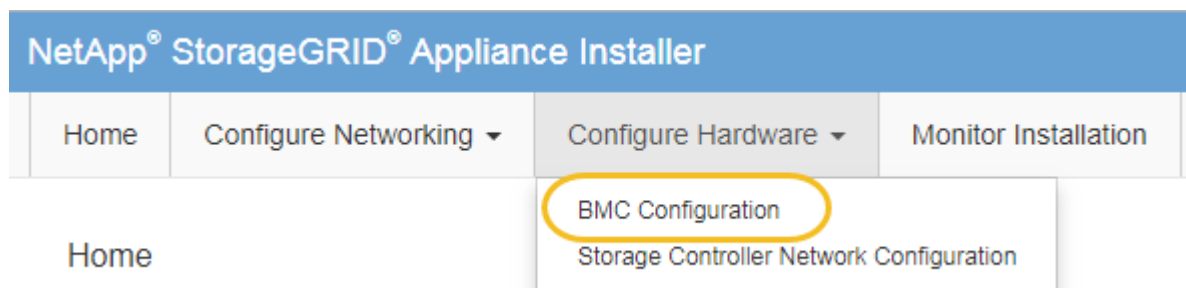
1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:

`https://Appliance_IP:8443`

Für `Appliance_IP`, Verwenden Sie die IP-Adresse für die Appliance in einem beliebigen StorageGRID-Netzwerk.

Die Startseite des StorageGRID-Appliance-Installationsprogramms wird angezeigt.

2. Wählen Sie **Hardware konfigurieren > BMC-Konfiguration**.



Die Seite Baseboard Management Controller Configuration wird angezeigt.

3. Notieren Sie sich die automatisch angezeigte IPv4-Adresse.

DHCP ist die Standardmethode zum Zuweisen einer IP-Adresse zu diesem Port.



Es kann einige Minuten dauern, bis die DHCP-Werte angezeigt werden.

Baseboard Management Controller Configuration

LAN IP Settings

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

4. Legen Sie optional eine statische IP-Adresse für den BMC-Verwaltungsport fest.



Sie sollten entweder eine statische IP für den BMC-Verwaltungsport zuweisen oder einen permanenten Leasing für die Adresse auf dem DHCP-Server zuweisen.

a. Wählen Sie **Statisch**.

b. Geben Sie die IPv4-Adresse unter Verwendung der CIDR-Schreibweise ein.

c. Geben Sie das Standard-Gateway ein.

Baseboard Management Controller Configuration

LAN IP Settings

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

d. Klicken Sie Auf **Speichern**.

Es kann einige Minuten dauern, bis Ihre Änderungen angewendet werden.

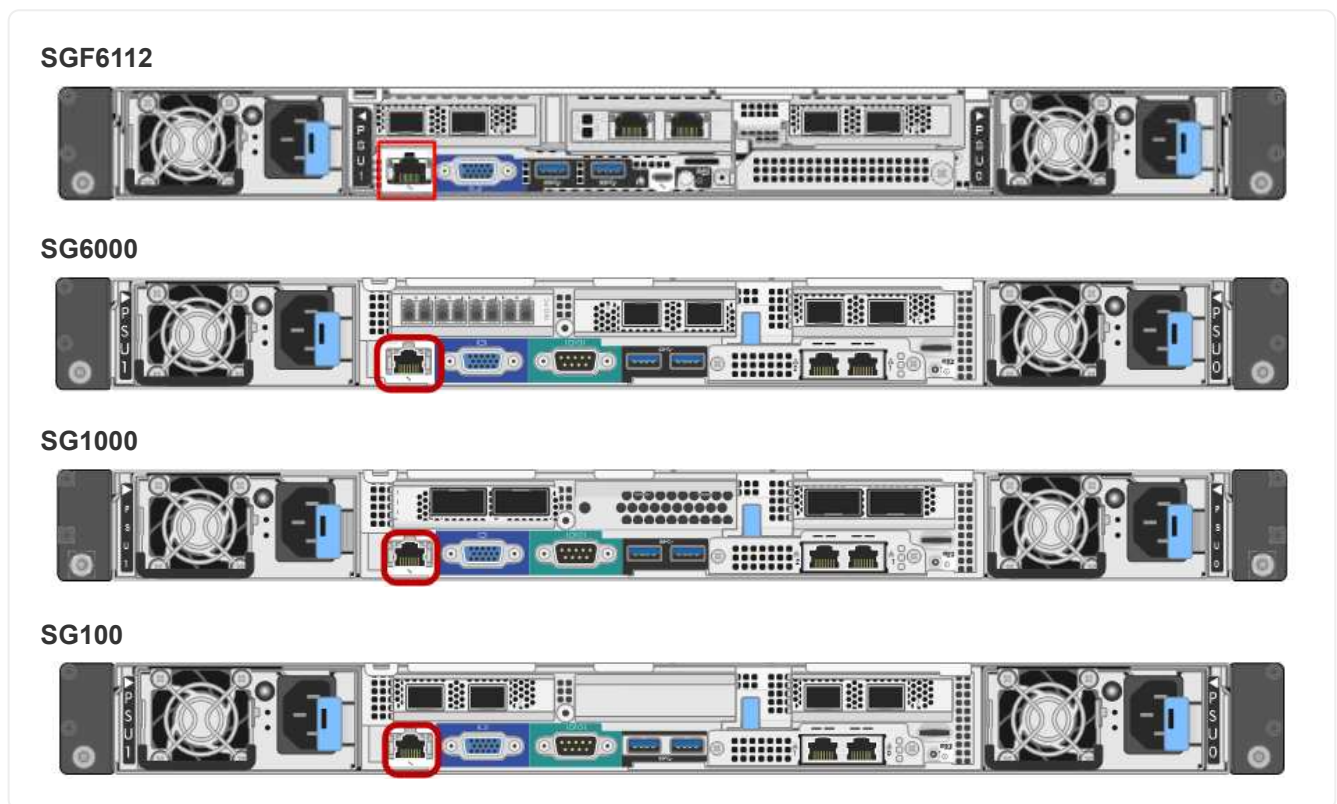
Greifen Sie auf die BMC-Schnittstelle zu

Sie können auf die BMC-Schnittstelle über die DHCP- oder statische IP-Adresse für den BMC-Verwaltungsport auf den folgenden Appliance-Modellen zugreifen:

- SGF6112
- SG6000
- SG1000
- SG100

Bevor Sie beginnen

- Der Management-Client verwendet ein "[Unterstützter Webbrowser](#)".
- Der BMC-Managementport der Appliance ist mit dem zu verwendenden Managementnetzwerk verbunden.



Schritte

1. Geben Sie die URL für die BMC-Schnittstelle ein:

`https://BMC_Port_IP`

Für *BMC_Port_IP*, Verwenden Sie die DHCP- oder statische IP-Adresse für den BMC-Management-Port.

Die BMC-Anmeldeseite wird angezeigt.



Wenn Sie noch nicht konfiguriert haben `BMC_Port_IP`, Folgen Sie den Anweisungen in "[Konfigurieren Sie die BMC-Schnittstelle](#)". Wenn Sie diese Vorgehensweise aufgrund eines Hardwareproblems nicht ausführen können und noch keine BMC-IP-Adresse konfiguriert haben, können Sie möglicherweise weiterhin auf den BMC zugreifen. Standardmäßig erhält der BMC über DHCP eine IP-Adresse. Wenn DHCP im BMC-Netzwerk aktiviert ist, kann Ihr Netzwerkadministrator die dem BMC-MAC zugewiesene IP-Adresse angeben, die auf dem Etikett auf der Vorderseite des Geräts aufgedruckt ist. Wenn DHCP im BMC-Netzwerk nicht aktiviert ist, reagiert der BMC nach einigen Minuten nicht und weist sich selbst die standardmäßige statische IP zu `192.168.0.120`. Möglicherweise müssen Sie Ihren Laptop direkt mit dem BMC-Port verbinden und die Netzwerkeinstellung ändern, um Ihrem Laptop eine IP-Adresse wie zuzuweisen `192.168.0.200/24`, Um zu suchen `192.168.0.120`.

2. Geben Sie den Admin- oder Root-Benutzernamen und das Passwort ein. Geben Sie dabei das Passwort ein, das Sie bei Ihrer Einstellung festgelegt haben "[Das Standard-Root-Passwort wurde geändert](#)":



Der Standardbenutzer hängt davon ab, wann Sie Ihre StorageGRID-Appliance installiert haben. Der Standardbenutzer ist **admin** für neue Installationen und **root** für ältere Installationen.

3. Wählen Sie **Sign me in** aus.

4. Erstellen Sie optional weitere Benutzer, indem Sie **Einstellungen > Benutzerverwaltung** wählen und auf einen beliebigen Benutzer "disabled" klicken.



Wenn sich Benutzer zum ersten Mal anmelden, werden sie möglicherweise aufgefordert, ihr Passwort zu ändern, um die Sicherheit zu erhöhen.

Konfigurieren Sie die SNMP-Einstellungen für BMC

Wenn Sie mit der Konfiguration von SNMP für Hardware vertraut sind, können Sie die

SNMP-Einstellungen für die SGF6112-, SG6000- und Service-Appliances über die BMC-Schnittstelle konfigurieren. Sie können sichere Community-Strings bereitstellen, SNMP-Trap aktivieren und bis zu fünf SNMP-Ziele angeben.

Bevor Sie beginnen

- Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.
- Sie haben Erfahrung in der Konfiguration von SNMP-Einstellungen für SNMPv1-v2c Geräte.



Die durch diese Vorgehensweise vorgenommenen BMC-Einstellungen bleiben möglicherweise nicht erhalten, wenn das Gerät ausfällt und ersetzt werden muss. Stellen Sie sicher, dass Sie über eine Aufzeichnung aller Einstellungen verfügen, die Sie angewendet haben, so dass sie nach einem Hardware-Austausch bei Bedarf leicht wieder angewendet werden können.

Schritte

1. Wählen Sie im BMC-Dashboard **Einstellungen** > **SNMP-Einstellungen** aus.
2. Wählen Sie auf der Seite SNMP-Einstellungen die Option **SNMP V1/V2** aktivieren und geben Sie dann eine schreibgeschützte Community-Zeichenfolge und eine Read-Write Community-Zeichenfolge an.

Die schreibgeschützte Community-Zeichenfolge ist wie eine Benutzer-ID oder ein Passwort. Sie sollten diesen Wert ändern, um zu verhindern, dass Eindringlinge Informationen über Ihr Netzwerk-Setup erhalten. Die Lese-Schreib-Community-Zeichenfolge schützt das Gerät vor nicht autorisierten Änderungen.

3. Wählen Sie optional **Trap aktivieren** aus, und geben Sie die erforderlichen Informationen ein.



Geben Sie die Ziel-IP für jeden SNMP-Trap unter Verwendung einer IP-Adresse ein. Vollständig qualifizierte Domännennamen werden nicht unterstützt.

Aktivieren Sie Traps, wenn die Appliance sofortige Benachrichtigungen an eine SNMP-Konsole senden soll, wenn sie sich in einem ungewöhnlichen Zustand befindet. Je nach Gerät können Traps auf Hardwareausfälle verschiedener Komponenten, auf Verbindungsabstände, Temperaturschwellenwerte oder hohen Datenverkehr hinweisen.

4. Klicken Sie optional auf **Test-Trap senden**, um Ihre Einstellungen zu testen.
5. Wenn die Einstellungen korrekt sind, klicken Sie auf **Speichern**.

E-Mail-Benachrichtigungen für BMC-Warnungen einrichten

Wenn Sie möchten, dass E-Mail-Benachrichtigungen bei Auftreten von Warnungen gesendet werden, verwenden Sie die BMC-Schnittstelle, um SMTP-Einstellungen, Benutzer, LAN-Ziele, Warnungsrichtlinien und Ereignisfilter zu konfigurieren.



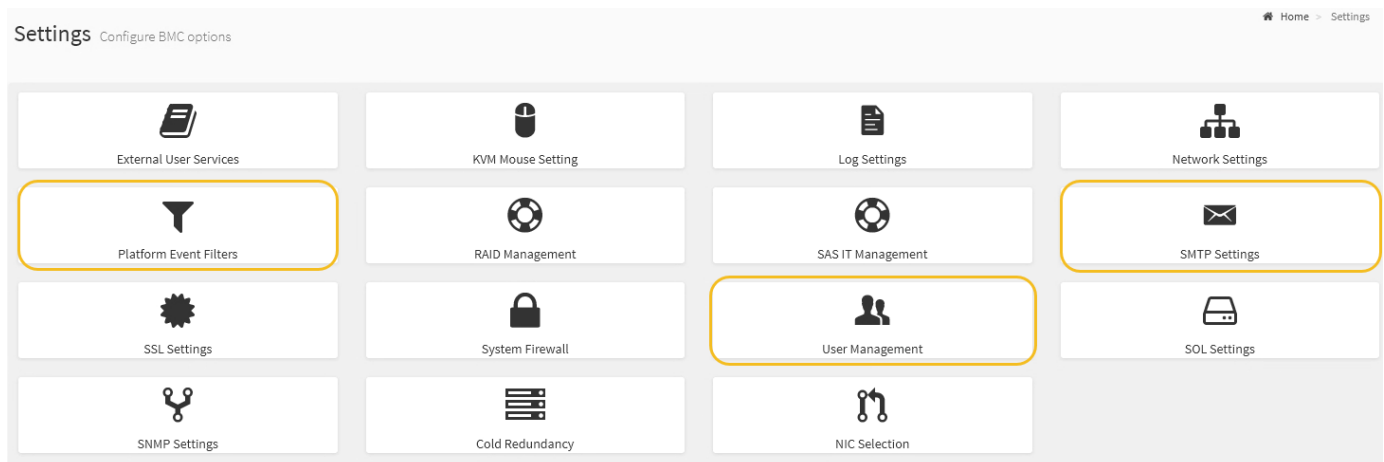
BMC-Einstellungen, die durch dieses Verfahren vorgenommen werden, bleiben möglicherweise nicht erhalten, wenn der SG6000-CN-Controller oder die Services-Apliance ausfällt und ersetzt werden muss. Stellen Sie sicher, dass Sie über eine Aufzeichnung aller Einstellungen verfügen, die Sie angewendet haben, so dass sie nach einem Hardware-Austausch bei Bedarf leicht wieder angewendet werden können.

Bevor Sie beginnen

Wissen Sie, wie Sie auf das BMC-Dashboard zugreifen können.

Über diese Aufgabe

In der BMC-Schnittstelle verwenden Sie die Optionen **SMTP-Einstellungen**, **Benutzerverwaltung** und **Platform Event Filters** auf der Seite Einstellungen, um E-Mail-Benachrichtigungen zu konfigurieren.



Schritte

1. "Konfigurieren Sie die SNMP-Einstellungen für BMC".

- Wählen Sie **Einstellungen > SMTP-Einstellungen**.
- Geben Sie für die Absender-E-Mail-ID eine gültige E-Mail-Adresse ein.

Diese E-Mail-Adresse wird als von-Adresse angegeben, wenn der BMC E-Mail sendet.

2. Richten Sie Benutzer für den Empfang von Warnungen ein.

- Wählen Sie im BMC-Dashboard die Option **Einstellungen > Benutzerverwaltung** aus.
- Fügen Sie mindestens einen Benutzer hinzu, um Benachrichtigungen zu erhalten.

Die für einen Benutzer konfigurierte E-Mail-Adresse ist die Adresse, an die BMC Warnmeldungen sendet. Sie können beispielsweise einen generischen Benutzer wie „notification-user,“ hinzufügen und die E-Mail-Adresse einer E-Mail-Verteilerliste für das technische Support-Team verwenden.

3. Konfigurieren Sie das LAN-Ziel für Meldungen.

- Wählen Sie **Einstellungen > Plattformereignisfilter > LAN-Ziele**.
- Konfigurieren Sie mindestens ein LAN-Ziel.
 - Wählen Sie als Zieltyp **E-Mail** aus.
 - Wählen Sie für BMC-Benutzername einen Benutzernamen aus, den Sie zuvor hinzugefügt haben.
 - Wenn Sie mehrere Benutzer hinzugefügt haben und möchten, dass alle von ihnen Benachrichtigungs-E-Mails erhalten, fügen Sie für jeden Benutzer ein LAN-Ziel hinzu.
- Eine Testwarnung senden.

4. Konfigurieren von Meldungsrichtlinien, um festzulegen, wann und wo BMC Alarme sendet

- Wählen Sie **Einstellungen > Plattformereignisfilter > Benachrichtigungsrichtlinien** Aus.
- Konfigurieren Sie mindestens eine Meldungsrichtlinie für jedes LAN-Ziel.
 - Wählen Sie für die Policengruppennummer **1** aus.
 - Wählen Sie für Policy Action *** immer Warnung an dieses Ziel senden*** aus.

- Wählen Sie für LAN-Kanal **1** aus.
 - Wählen Sie in der Zielauswahl das LAN-Ziel für die Richtlinie aus.
5. Ereignisfilter konfigurieren, um Warnmeldungen für verschiedene Ereignistypen an die entsprechenden Benutzer zu leiten.
- a. Wählen Sie **Einstellungen > Plattformereignisfilter > Ereignisfilter**.
 - b. Geben Sie für die Nummer der Meldungsrichtlinie **1** ein.
 - c. Erstellen Sie Filter für jedes Ereignis, über das die Meldungsrichtlinie-Gruppe benachrichtigt werden soll.
 - Sie können Ereignisfilter für Energieaktionen, bestimmte Sensorereignisse oder alle Ereignisse erstellen.
 - Wenn Sie unsicher sind, welche Ereignisse überwacht werden sollen, wählen Sie **Alle Sensoren** für den Sensortyp und **Alle Ereignisse** für Ereignisoptionen. Wenn Sie unerwünschte Benachrichtigungen erhalten, können Sie Ihre Auswahl später ändern.

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFT SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGEND EINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.