



BMC-Schnittstelle konfigurieren (SG6000)

StorageGRID

NetApp
October 03, 2025

This PDF was generated from <https://docs.netapp.com/de-de/storagegrid-116/sg6000/changing-root-password-for-bmc-interface-sg6000.html> on October 03, 2025. Always check docs.netapp.com for the latest.

Inhalt

- BMC-Schnittstelle konfigurieren (SG6000) 1
 - Ändern Sie das 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 4
 - Konfigurieren Sie SNMP-Einstellungen für SG6000-CN Controller 6
 - Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein 7

BMC-Schnittstelle konfigurieren (SG6000)

Die Benutzeroberfläche für den Baseboard Management Controller (BMC) auf dem SG6000-CN Controller bietet Statusinformationen über die Hardware und ermöglicht die Konfiguration von SNMP-Einstellungen und anderen Optionen für den SG6000-CN Controller.

Ändern Sie das Root-Passwort für die BMC-Schnittstelle

Aus Sicherheitsgründen müssen Sie das Kennwort für den Root-Benutzer von BMC ändern.

Was Sie benötigen

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

Über diese Aufgabe

Bei der ersten Installation des Geräts verwendet der BMC ein Standardpasswort für den Root-Benutzer (root/calvin). Sie müssen das Passwort für den Root-Benutzer ändern, um Ihr System zu sichern.

Schritte

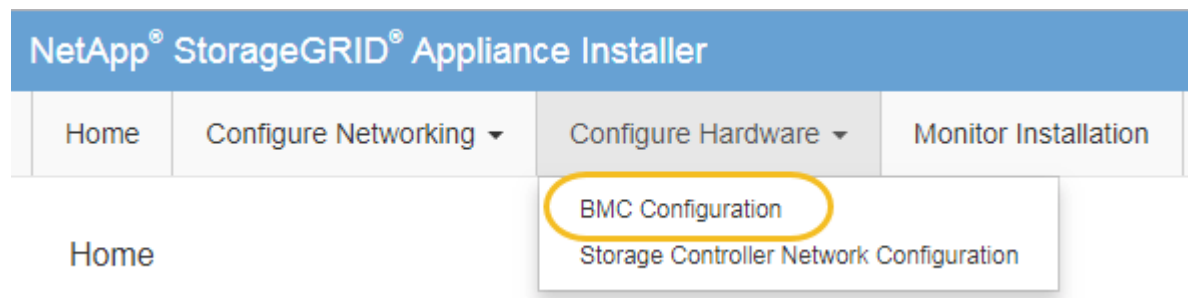
1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:

`https://Appliance_Controller_IP:8443`

Für *Appliance_Controller_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 Root-Konto ein.

Baseboard Management Controller Configuration

User Settings

Root Password

.....

Confirm Root Password

.....

4. Klicken Sie Auf **Speichern**.

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

Bevor Sie auf die BMC-Schnittstelle zugreifen können, müssen Sie die IP-Adresse für den BMC-Management-Port des SG6000-CN-Controllers konfigurieren.

Was Sie benötigen

- 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.



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.

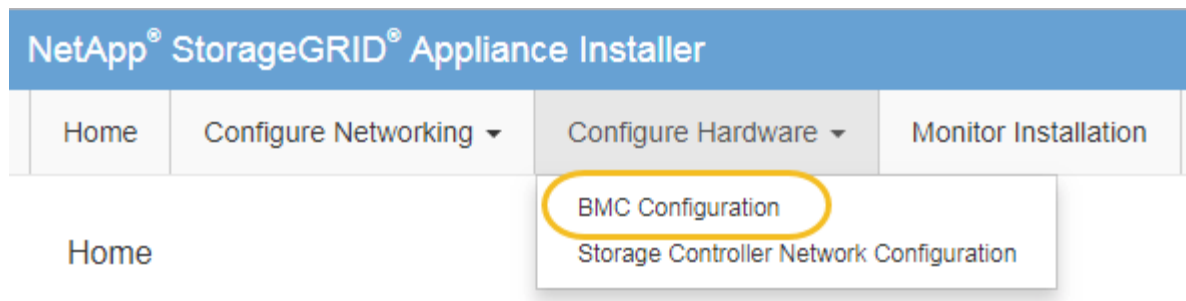
Schritte

1. Geben Sie auf dem Client die URL für den StorageGRID-Appliance-Installer ein:
`https://SG6000-CN_Controller_IP:8443`

Für SG6000-CN_Controller_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	☐ Static ☒ 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. 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.

- Wählen Sie **Statisch**.
- Geben Sie die IPv4-Adresse unter Verwendung der CIDR-Schreibweise ein.
- Geben Sie das Standard-Gateway ein.

LAN IP Settings

IP Assignment	☒ Static ☐ 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. Klicken Sie Auf **Speichern**.

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

Greifen Sie auf die BMC-Schnittstelle zu

Sie können über die DHCP- oder statische IP-Adresse für den BMC-Management-Port auf die BMC-Schnittstelle des SG6000-CN-Controllers zugreifen.

Was Sie benötigen

- Der BMC-Management-Port des SG6000-CN Controllers ist mit dem Managementnetzwerk verbunden, das Sie verwenden möchten.



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

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 [BMC-Schnittstelle konfigurieren \(SG6000\)](#). 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 SG6000-CN-Controllers gedruckt 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 Root-Benutzernamen und das Kennwort ein, das Sie bei der Eingabe des Passworts festgelegt haben [Das Standard-Root-Passwort wurde geändert](#):

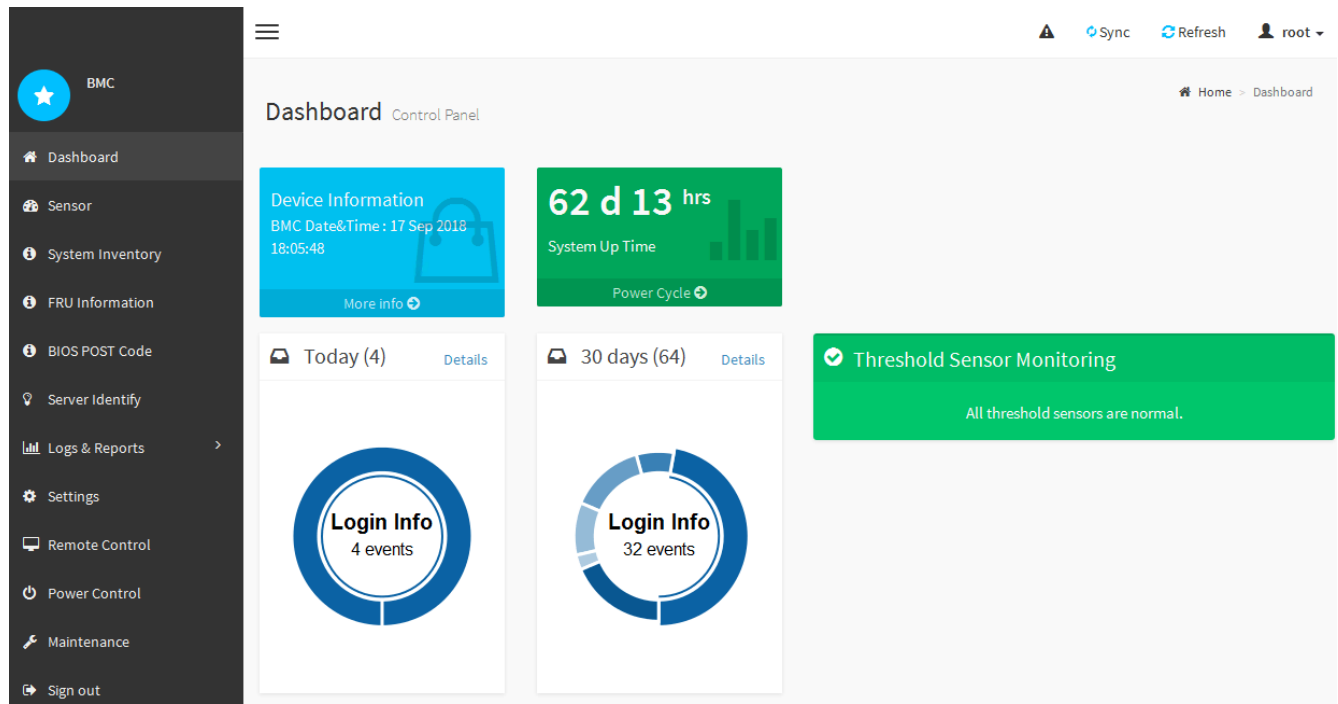


☐ Remember Username

Sign me in

[I forgot my password](#)

3. Wählen Sie **Sign me in** aus.



- 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 SNMP-Einstellungen für SG6000-CN Controller

Wenn Sie mit der Konfiguration von SNMP für Hardware vertraut sind, können Sie die SNMP-Einstellungen für den SG6000-CN-Controller über die BMC-Schnittstelle konfigurieren. Sie können sichere Community-Strings bereitstellen, SNMP-Trap aktivieren und bis zu fünf SNMP-Ziele angeben.

Was Sie benötigen

- 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 dieses Verfahren vorgenommenen BMC-Einstellungen bleiben möglicherweise nicht erhalten, wenn das SG6000-CN 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

- Wählen Sie im BMC-Dashboard **Einstellungen SNMP-Einstellungen** aus.
- 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 Domain-Namen werden nicht unterstützt.

Aktivieren Sie Traps, wenn der SG6000-CN-Controller sofortige Benachrichtigungen an eine SNMP-Konsole senden soll, wenn sie sich in einem ungewöhnlichen Zustand befindet. Traps können zeigen, dass Hardwareausfälle von verschiedenen Komponenten oder Temperaturschwellenwerten überschritten werden.

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

Richten Sie E-Mail-Benachrichtigungen für Warnmeldungen ein

Wenn E-Mail-Benachrichtigungen gesendet werden sollen, wenn Warnmeldungen auftreten, müssen Sie SMTP-Einstellungen, Benutzer, LAN-Ziele, Warnrichtlinien und Ereignisfilter über die BMC-Schnittstelle konfigurieren.



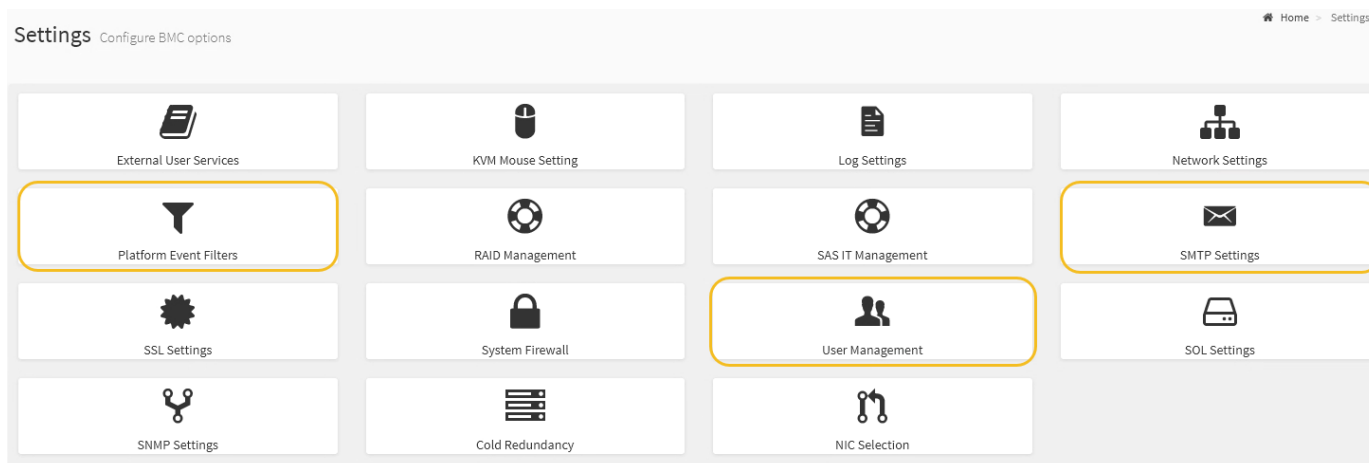
Die durch dieses Verfahren vorgenommenen BMC-Einstellungen bleiben möglicherweise nicht erhalten, wenn das SG6000-CN ausfällt und ersetzt werden muss. Stellen Sie sicher, dass Sie über eine Aufzeichnung aller Einstellungen verfügen, die Sie angewendet haben, so dass sie nach einem Hardware-Austausch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

Was Sie benötigen

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 SMTP-Einstellungen.

- a. Wählen Sie **Einstellungen SMTP-Einstellungen**.
- b. 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.

- a. Wählen Sie im BMC-Dashboard **Einstellungen Benutzerverwaltung** aus.
- b. 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.

- a. Wählen Sie **Einstellungen Plattformereignisfilter LAN-Ziele**.
- b. 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 alle Benutzer Benachrichtigungen erhalten möchten, müssen Sie für jeden Benutzer ein LAN-Ziel hinzufügen.
- c. Eine Testwarnung senden.

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

- a. Wählen Sie **Einstellungen Plattformereignisfilter Benachrichtigungsrichtlinien**.
- b. 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 © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.