EMS-Ereignisbenachrichtigungen mit der CLI konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/error-messages/config-workflow-task.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

EMS-Ereignisbenachrichtigungen mit der CLI konfigurieren . . . 1
ONTAP EMS Konfigurationsworkflow . . . 1
Wichtige ONTAP EMS Ereignisse für den Versand von E-Mail-Benachrichtigungen konfigurieren . . . 2
Wichtige ONTAP EMS Ereignisse so konfigurieren, dass Benachrichtigungen an einen Syslog Server weitergeleitet werden . . . 3
ONTAP SNMP Traphosts für den Empfang von Ereignisbenachrichtigungen konfigurieren . . . 4
Wichtige ONTAP EMS-Ereignisse so konfigurieren, dass Benachrichtigungen an eine Webhook-Anwendung weitergeleitet werden . . . 4
Vorbereitung der Konfiguration der EMS Ereignisweiterleitung . . . 5
Ein Webhook-Ziel für die Verwendung von HTTP konfigurieren . . . 6
Ein Webhook-Ziel für die Verwendung von HTTPS konfigurieren . . . 6
Ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger Authentifizierung konfigurieren . . . 7

EMS-Ereignisbenachrichtigungen mit der CLI konfigurieren

ONTAP EMS Konfigurationsworkflow

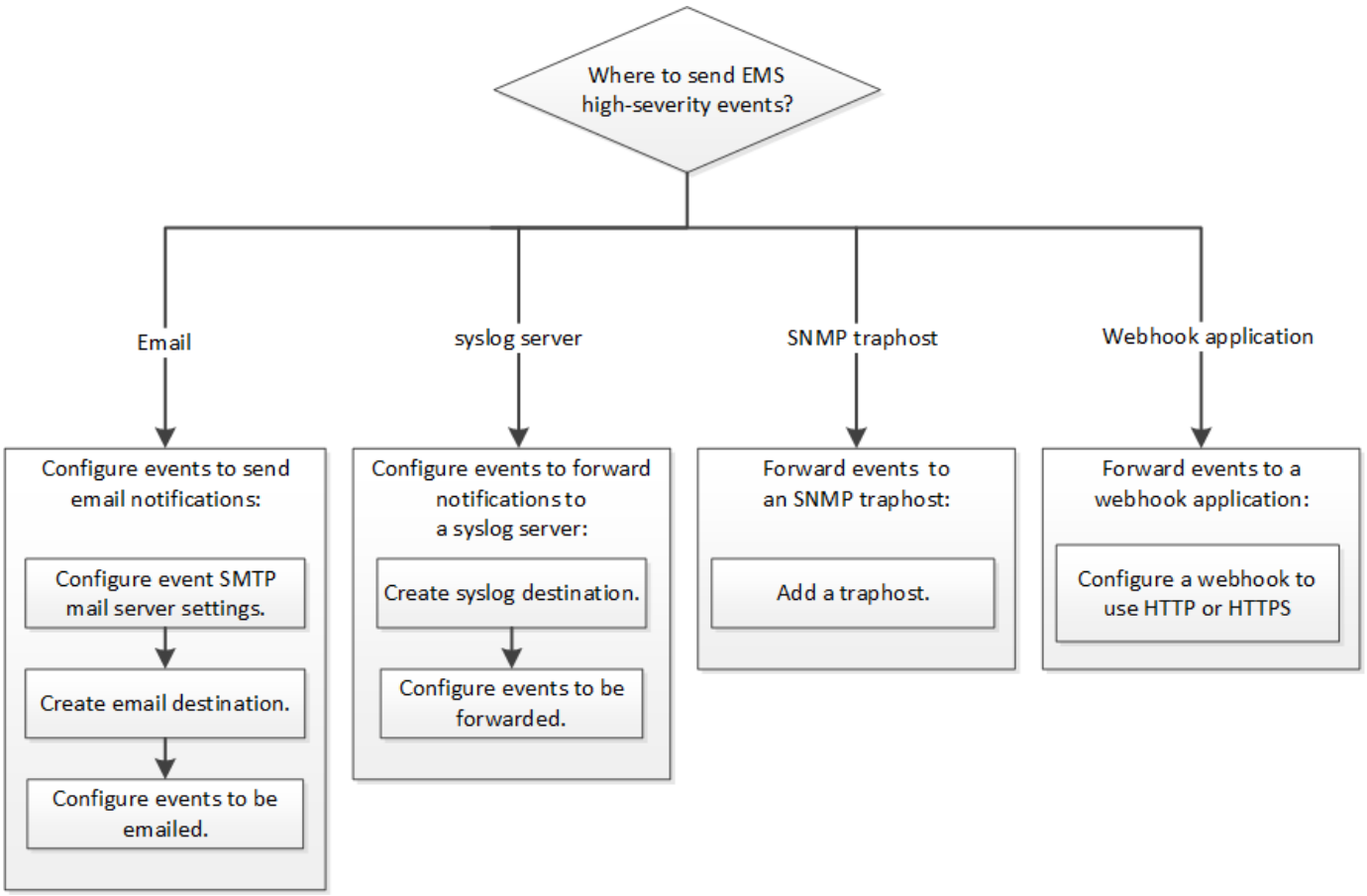
Wichtige EMS-Ereignisbenachrichtigungen müssen so konfiguriert werden, dass sie entweder per E-Mail, an einen Syslog-Server, an einen SNMP-Traphost oder an eine Webhook-Anwendung weitergeleitet werden. Dadurch lassen sich Systemunterbrechungen vermeiden, da rechtzeitig Korrekturmaßnahmen ergriffen werden können.

Über diese Aufgabe

Wenn Ihre Umgebung bereits einen Syslog-Server zum Aggregieren der protokollierten Ereignisse von anderen Systemen wie Servern und Anwendungen enthält, ist es einfacher, diesen Syslog-Server auch für wichtige Ereignisbenachrichtigungen von Speichersystemen zu verwenden.

Falls in Ihrer Umgebung noch kein Syslog-Server vorhanden ist, ist es einfacher, wichtige Ereignisbenachrichtigungen per E-Mail zu erhalten.

Wenn Sie Ereignisbenachrichtigungen bereits an einen SNMP-Traphost weiterleiten, kann es sinnvoll sein, diesen Traphost auf wichtige Ereignisse zu überwachen.



Auswahlmöglichkeiten

- EMS so einstellen, dass Ereignisbenachrichtigungen gesendet werden.

Wenn Sie möchten…	Weitere Informationen finden Sie unter …
Das EMS sendet wichtige Ereignisbenachrichtigungen an eine E-Mail-Adresse.	Wichtige EMS-Ereignisse für den Versand von E-Mail-Benachrichtigungen konfigurieren
Das EMS leitet wichtige Ereignisbenachrichtigungen an einen Syslog Server weiter.	Wichtige EMS-Ereignisse so konfigurieren, dass Benachrichtigungen an einen Syslog Server weitergeleitet werden
Wenn Sie möchten, dass EMS Ereignisbenachrichtigungen an einen SNMP-Traphost weiterleitet	SNMP-Traphosts für den Empfang von Ereignisbenachrichtigungen konfigurieren
Wenn Sie möchten, dass das EMS Ereignisbenachrichtigungen an eine Webhook Anwendung weiterleitet	Wichtige EMS-Ereignisse so konfigurieren, dass Benachrichtigungen an eine Webhook-Anwendung weitergeleitet werden

Wichtige ONTAP EMS Ereignisse für den Versand von E-Mail-Benachrichtigungen konfigurieren

Um E-Mail-Benachrichtigungen über die wichtigsten Ereignisse zu erhalten, muss das EMS so konfiguriert werden, dass E-Mail-Nachrichten für Ereignisse gesendet werden, die auf wichtige Aktivitäten hinweisen.

Bevor Sie beginnen

DNS muss auf dem Cluster konfiguriert sein, um die E-Mail-Adressen aufzulösen.

Über diese Aufgabe

Diese Aufgabe kann jederzeit während des Betriebs des Clusters durch Eingabe der Befehle in der ONTAP Befehlszeile ausgeführt werden.

Schritte

1. Die SMTP-Mailservereinstellungen für Ereignisse konfigurieren:

   ```
   event config modify -mail-server mailhost.your_domain -mail-from
   cluster_admin@your_domain
   ```

   Weitere Informationen zu `event config modify` finden sich in der "ONTAP-Befehlsreferenz".

2. Ein E-Mail-Ziel für Ereignisbenachrichtigungen erstellen:

   ```
   event notification destination create -name storage-admins -email
   your_email@your_domain
   ```

   Weitere Informationen zu `event notification destination create` finden sich in der "ONTAP-Befehlsreferenz".

3. Die wichtigen Ereignisse konfigurieren, für die E-Mail-Benachrichtigungen gesendet werden:

   ```
   event notification create -filter-name important-events -destinations storage-
   ```

`admins`

Weitere Informationen zu `event notification create` finden sich in der "ONTAP-Befehlsreferenz".

Wichtige ONTAP EMS Ereignisse so konfigurieren, dass Benachrichtigungen an einen Syslog Server weitergeleitet werden

Um Benachrichtigungen über die schwerwiegendsten Ereignisse auf einem Syslog-Server zu protokollieren, ist eine Konfiguration des EMS erforderlich, damit Benachrichtigungen für Ereignisse, die auf wichtige Aktivitäten hinweisen, weitergeleitet werden.

Bevor Sie beginnen

DNS muss auf dem Cluster konfiguriert sein, um den Namen des Syslog Servers aufzulösen.

Über diese Aufgabe

Falls in Ihrer Umgebung noch kein Syslog-Server für Ereignisbenachrichtigungen vorhanden ist, muss zunächst einer erstellt werden. Falls in Ihrer Umgebung bereits ein Syslog-Server zur Protokollierung von Ereignissen anderer Systeme existiert, kann dieser für wichtige Ereignisbenachrichtigungen verwendet werden.

Diese Aufgabe kann jederzeit durchgeführt werden, während der Cluster läuft, indem die Befehle in der ONTAP CLI eingegeben werden.

Ab ONTAP 9.12.1 können EMS-Ereignisse über das Transport Layer Security (TLS)-Protokoll an einen festgelegten Port eines entfernten Syslog-Servers gesendet werden. Zwei neue Parameter stehen zur Verfügung:

`tcp-encrypted`

Wenn `tcp-encrypted` für den `syslog-transport` angegeben ist, überprüft ONTAP die Identität des Zielhosts durch Validierung seines Zertifikats. Der Standardwert ist `udp-unencrypted`.

`syslog-port`

Der Standardwert `syslog-port` des Parameters hängt von der Einstellung des `syslog-transport` Parameters ab. Wenn `syslog-transport` auf `tcp-encrypted` gesetzt ist, hat `syslog-port` den Standardwert 6514.

Schritte

1. Ein Syslog-Serverziel für wichtige Ereignisse erstellen:

   `event notification destination create -name` *`syslog-ems`* `-syslog` *`syslog-server-address`* `-syslog-transport {udp-unencrypted|tcp-unencrypted|tcp-encrypted}`

   Ab ONTAP 9.12.1 können für `syslog-transport` die folgenden Werte angegeben werden:

   - `udp-unencrypted` - Benutzerdatengrammprotokoll ohne Sicherheit
   - `tcp-unencrypted` - Transmission Control Protocol ohne Sicherheitsvorkehrungen

- `tcp-encrypted` - Transmission Control Protocol mit Transport Layer Security (TLS)

  Das Standardprotokoll ist `udp-unencrypted`.

Weitere Informationen zu `event notification destination create` finden sich in der "ONTAP-Befehlsreferenz".

2. Die wichtigen Ereignisse werden so konfiguriert, dass Benachrichtigungen an den Syslog-Server weitergeleitet werden:

   `event notification create -filter-name` *`important-events`* `-destinations` *`syslog-ems`*

   Weitere Informationen zu `event notification create` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP SNMP Traphosts für den Empfang von Ereignisbenachrichtigungen konfigurieren

Um Ereignisbenachrichtigungen auf einem SNMP-Traphost zu erhalten, ist die Konfiguration eines Traphosts erforderlich.

Bevor Sie beginnen

- SNMP und SNMP Traps müssen auf dem Cluster aktiviert sein.

  SNMP und SNMP Traps sind standardmäßig aktiviert.

- DNS muss auf dem Cluster konfiguriert sein, um die Traphost-Namen aufzulösen.

Über diese Aufgabe

Wenn noch kein SNMP Traphost konfiguriert ist, um Ereignisbenachrichtigungen (SNMP Traps) zu empfangen, muss einer hinzugefügt werden.

Diese Aufgabe kann jederzeit während des Betriebs des Clusters durch Eingabe der Befehle in der ONTAP Befehlszeile ausgeführt werden.

Schritt

1. Falls in Ihrer Umgebung noch kein SNMP Traphost für den Empfang von Ereignisbenachrichtigungen konfiguriert ist, sollte einer hinzugefügt werden:

   `system snmp traphost add -peer-address` *`snmp_traphost_name`*

   Alle Ereignisbenachrichtigungen, die von SNMP standardmäßig unterstützt werden, werden an den SNMP traphost weitergeleitet.

Wichtige ONTAP EMS-Ereignisse so konfigurieren, dass Benachrichtigungen an eine Webhook-Anwendung weitergeleitet werden

Sie können ONTAP so konfigurieren, dass wichtige Ereignisbenachrichtigungen an eine

Webhook-Anwendung weitergeleitet werden. Die erforderlichen Konfigurationsschritte hängen vom gewählten Sicherheitsniveau ab.

Vorbereitung der Konfiguration der EMS Ereignisweiterleitung

Es gibt mehrere Konzepte und Anforderungen, die vor der Konfiguration von ONTAP zur Weiterleitung von Ereignisbenachrichtigungen an eine Webhook-Anwendung berücksichtigt werden sollten.

Webhook Anwendung

Sie benötigen eine Webhook-Anwendung, die ONTAP-Ereignisbenachrichtigungen empfangen kann. Ein Webhook ist eine benutzerdefinierte Callback-Routine, die die Funktionalität der Remote-Anwendung oder des Servers, auf dem sie ausgeführt wird, erweitert. Webhooks werden vom Client (in diesem Fall ONTAP) durch Senden einer HTTP-Anfrage an die Ziel-URL aufgerufen oder aktiviert. Konkret sendet ONTAP eine HTTP-POST-Anfrage an den Server, auf dem die Webhook-Anwendung gehostet wird, zusammen mit den Ereignisbenachrichtigungsdetails im XML-Format.

Sicherheitsoptionen

Je nachdem, wie das Transport Layer Security (TLS) Protokoll verwendet wird, stehen verschiedene Sicherheitsoptionen zur Verfügung. Die gewählte Option bestimmt die erforderliche ONTAP Konfiguration.

ⓘ TLS ist ein im Internet weit verbreitetes kryptografisches Protokoll. Es gewährleistet Vertraulichkeit, Datenintegrität und Authentifizierung mithilfe eines oder mehrerer öffentlicher Schlüsselzertifikate. Diese Zertifikate werden von vertrauenswürdigen Zertifizierungsstellen ausgestellt.

HTTP

HTTP kann für den Transport der Ereignisbenachrichtigungen verwendet werden. Mit dieser Konfiguration ist die Verbindung nicht sicher. Die Identitäten des ONTAP Client und der Webhook Anwendung werden nicht verifiziert. Außerdem ist der Netzwerkverkehr weder verschlüsselt noch geschützt. Siehe "Ein Webhook-Ziel für die Verwendung von HTTP konfigurieren" für die Konfigurationsdetails.

HTTPS

Zur zusätzlichen Sicherheit kann ein Zertifikat auf dem Server installiert werden, der die Webhook-Routine hostet. Das HTTPS-Protokoll wird von ONTAP verwendet, um die Identität des Webhook-Anwendungsservers zu überprüfen, und von beiden Parteien, um die Vertraulichkeit und Integrität des Netzwerkverkehrs sicherzustellen. Siehe "Ein Webhook-Ziel für die Verwendung von HTTPS konfigurieren" für die Konfigurationsdetails.

HTTPS mit gegenseitiger Authentifizierung

Die HTTPS-Sicherheit lässt sich weiter erhöhen, indem ein Clientzertifikat auf dem ONTAP-System installiert wird, das die Webhook-Anfragen sendet. Neben der Überprüfung der Identität des Webhook-Anwendungsservers durch ONTAP und dem Schutz des Netzwerkverkehrs überprüft die Webhook-Anwendung die Identität des ONTAP Clients. Diese gegenseitige Peer-Authentifizierung ist als *Mutual TLS* bekannt. Siehe "Ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger Authentifizierung konfigurieren" für die Konfigurationsdetails.

Verwandte Informationen

- "Das Transport Layer Security (TLS) Protokoll Version 1.3"

Ein Webhook-Ziel für die Verwendung von HTTP konfigurieren

ONTAP kann so konfiguriert werden, dass Ereignisbenachrichtigungen per HTTP an eine Webhook-Anwendung weitergeleitet werden. Dies ist die unsicherste, aber am einfachsten einzurichtende Option.

Schritte

1. Ein neues Ziel `restapi-ems` zum Empfangen der Ereignisse erstellen:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   http://<webhook-application>
   ```

   Im obigen Befehl muss das **HTTP**-Schema für das Ziel verwendet werden.

   Weitere Informationen zu `event notification destination create` finden sich in der "ONTAP-Befehlsreferenz".

2. Erstellen Sie eine Benachrichtigung, die den `important-events` Filter mit dem `restapi-ems` Ziel verknüpft:

   ```
   event notification create -filter-name important-events -destinations restapi-
   ems
   ```

   Weitere Informationen zu `event notification create` finden sich in der "ONTAP-Befehlsreferenz".

Ein Webhook-Ziel für die Verwendung von HTTPS konfigurieren

ONTAP kann so konfiguriert werden, dass Ereignisbenachrichtigungen per HTTPS an eine Webhook-Anwendung weitergeleitet werden. ONTAP verwendet das Serverzertifikat, um die Identität der Webhook-Anwendung zu bestätigen und den Netzwerkverkehr zu sichern.

Bevor Sie beginnen

- Ein privater Schlüssel und ein Zertifikat für den Webhook-Anwendungsserver werden generiert.
- Das Root-Zertifikat für die Installation in ONTAP bereithalten

Schritte

1. Installieren Sie den entsprechenden privaten Serverschlüssel und die Zertifikate auf dem Server, auf dem Ihre Webhook-Anwendung gehostet wird. Die genauen Konfigurationsschritte hängen vom jeweiligen Server ab.
2. Das Server-Root-Zertifikat in ONTAP installieren:

   ```
   security certificate install -type server-ca
   ```

   Der Befehl fordert das Zertifikat an.

3. Das `restapi-ems`Ziel zum Empfangen der Ereignisse erstellen:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application>
   ```

   Im obigen Befehl muss das **HTTPS**-Schema für das Ziel verwendet werden.

4. Erstellen Sie die Benachrichtigung, die den `important-events` Filter mit dem neuen `restapi-ems` Ziel

verknüpft:

```
event notification create -filter-name important-events -destinations restapi-ems
```

Ein Webhook-Ziel für die Verwendung von HTTPS mit gegenseitiger Authentifizierung konfigurieren

ONTAP kann so konfiguriert werden, dass Ereignisbenachrichtigungen an eine Webhook-Anwendung per HTTPS mit gegenseitiger Authentifizierung weitergeleitet werden. Bei dieser Konfiguration gibt es zwei Zertifikate. ONTAP verwendet das Serverzertifikat, um die Identität der Webhook-Anwendung zu bestätigen und den Netzwerkverkehr abzusichern. Zusätzlich verwendet die Anwendung, die den Webhook hostet, das Clientzertifikat, um die Identität des ONTAP Clients zu bestätigen.

Bevor Sie beginnen

Folgendes ist vor der Konfiguration von ONTAP erforderlich:

- Ein privater Schlüssel und ein Zertifikat für den Webhook-Anwendungsserver werden generiert.
- Das Root-Zertifikat für die Installation in ONTAP bereithalten
- Ein privater Schlüssel und ein Zertifikat für den ONTAP Client werden generiert.

Schritte

1. Führen Sie die ersten beiden Schritte der Aufgabe "Ein Webhook-Ziel für die Verwendung von HTTPS konfigurieren" aus, um das Serverzertifikat zu installieren, damit ONTAP die Identität des Servers verifizieren kann.
2. Die entsprechenden Stamm- und Zwischenzertifikate sind in der Webhook-Anwendung zu installieren, damit das Clientzertifikat validiert werden kann.
3. Das Clientzertifikat in ONTAP installieren:

   ```
   security certificate install -type client
   ```

   Der Befehl fragt nach dem privaten Schlüssel und dem Zertifikat.

4. Das `restapi-ems`Ziel zum Empfangen der Ereignisse erstellen:

   ```
   event notification destination create -name restapi-ems -rest-api-url
   https://<webhook-application> -certificate-authority <issuer of the client
   certificate> -certificate-serial <serial of the client certificate>
   ```

   Im obigen Befehl ist das Schema **HTTPS** für das Ziel zu verwenden.

5. Erstellen Sie die Benachrichtigung, die den `important-events` Filter mit dem neuen `restapi-ems` Ziel verknüpft:

   ```
   event notification create -filter-name important-events -destinations restapi-ems
   ```

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Copyright-Informationen

Copyright © 2026 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 IRGENDEINER 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.