Sicherheitstraces durchführen

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/nas-audit/perform-security-traces-task.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Sicherheitstraces durchführen . . . 1
ONTAP Sicherheitsüberprüfungen durchführen . . . 1
Erstellen von Security-Trace-Filtern in ONTAP SVMs . . . 1
Informationen zu Sicherheitsverfolgungsfiltern in ONTAP SVMs . . . 3
Anzeige der Sicherheitsverfolgungsergebnisse in ONTAP SVMs . . . 4
Sicherheitsverfolgungsfilter auf ONTAP SVMs ändern . . . 6
Sicherheits-Tracefilter auf ONTAP SVMs löschen . . . 7
Sicherheitsverfolgungsdatensätze auf ONTAP SVMs löschen . . . 8
Alle Sicherheitsverfolgungsdatensätze auf ONTAP SVMs löschen . . . 9

Sicherheitstraces durchführen

ONTAP Sicherheitsüberprüfungen durchführen

Die Durchführung einer Sicherheitsverfolgung umfasst das Erstellen eines Sicherheitsverfolgungsfilters, das Überprüfen der Filterkriterien, das Generieren von Zugriffsanfragen auf einem SMB- oder NFS-Client, die den Filterkriterien entsprechen, und das Anzeigen der Ergebnisse.

Nachdem Sie die Verwendung eines Sicherheitsfilters zur Erfassung von Protokollinformationen abgeschlossen haben, kann der Filter angepasst und wiederverwendet oder deaktiviert werden, falls er nicht mehr benötigt wird. Nach Ansicht und Analyse der Filterprotokollergebnisse können diese gelöscht werden, wenn sie nicht mehr benötigt werden.

Erstellen von Security-Trace-Filtern in ONTAP SVMs

Sie können Sicherheits-Trace-Filter erstellen, die SMB- und NFS-Client-Operationen auf Storage Virtual Machines (SVMs) erkennen und alle Zugriffsprüfungen protokollieren, die dem Filter entsprechen. Die Ergebnisse dieser Sicherheits-Traces können zur Validierung der Konfiguration oder zur Fehlerbehebung bei Zugriffsproblemen verwendet werden.

Über diese Aufgabe

Für den Befehl zum Erstellen des vserver security trace filter sind zwei Parameter erforderlich:

Erforderliche Parameter	Beschreibung
`-vserver vserver_name`	*SVM Name* Der Name der SVM, die die Dateien oder Ordner enthält, auf welche der Sicherheitsverfolgungsfilter angewendet werden soll.
`-index index_number`	*Filterindexnummer* Die Indexnummer, die Sie auf den Filter anwenden möchten. Pro SVM sind maximal 10 Trace-Filter zulässig. Die zulässigen Werte für diesen Parameter sind 1 bis 10.

Eine Reihe optionaler Filterparameter ermöglicht es Ihnen, den Sicherheitstrace-Filter anzupassen, sodass die von der Sicherheitstrace erzeugten Ergebnisse eingegrenzt werden können:

Filterparameter	Beschreibung
`-client-ip IP_Address`	Dieser Filter legt die IP-Adresse fest, von der aus der Benutzer auf die SVM zugreift.

`-path path`	Dieser Filter gibt den Pfad an, auf den der Berechtigungsverfolgungsfilter angewendet wird. Der Wert für `-path` kann eines der folgenden Formate verwenden: • Der vollständige Pfad, beginnend beim Stammverzeichnis der Freigabe oder des Exports • Ein Teilpfad, relativ zum Stammverzeichnis der Freigabe Im Pfadwert sind Verzeichnistrennzeichen im NFS-Stil beziehungsweise UNIX-Stil zu verwenden.
`-windows-name win_user_name` oder `-unix -name``unix_user_name`	Sie können entweder den Windows-Benutzernamen oder den UNIX-Benutzernamen angeben, dessen Zugriffsanfragen Sie verfolgen möchten. Die Variable „Benutzername“ unterscheidet nicht zwischen Groß- und Kleinschreibung. Es kann nicht gleichzeitig ein Windows-Benutzername und ein UNIX-Benutzername im selben Filter angegeben werden. Auch wenn SMB- und NFS-Zugriffsereignisse nachverfolgt werden können, könnten der zugeordnete UNIX-Benutzer und die zugeordneten UNIX-Benutzergruppen bei Zugriffsprüfungen auf gemischte oder UNIX-Sicherheitsstil-Daten verwendet werden.
`-trace-allow {yes`	`no}`
Das Tracing für Ablehnungsereignisse ist für einen Security Trace-Filter immer aktiviert. Optional ist das Tracing von Zulassungsereignissen möglich. Zum Tracing von Zulassungsereignissen wird dieser Parameter auf `yes` gesetzt.	`-enabled {enabled`
`disabled}`	Sie können den Security Trace Filter aktivieren oder deaktivieren. Standardmäßig ist der Security Trace Filter aktiviert.
`-time-enabled integer`	Sie können eine Zeitüberschreitung für den Filter festlegen, nach deren Ablauf er deaktiviert wird.

Schritte

1. Einen Sicherheits-Trace-Filter erstellen:

   ```
   vserver security trace filter create -vserver vserver_name -index
   index_numberfilter_parameters
   ```

   `filter_parameters` ist eine Liste optionaler Filterparameter.

   Weitere Informationen zu `vserver security trace filter create` finden sich in der "ONTAP-Befehlsreferenz".

2. Der Eintrag des Sicherheitsverfolgungsfilters wird überprüft:

   ```
   vserver security trace filter show -vserver vserver_name -index index_number
   ```

Beispiele

Der folgende Befehl erstellt einen Security Trace-Filter für jeden Benutzer, der von der IP-Adresse 10.10.10.7 auf eine Datei mit einem Freigabepfad `\\server\share1\dir1\dir2\file.txt` zugreift. Der Filter verwendet einen vollständigen Pfad für die `-path` Option. Die IP-Adresse des Clients, die für den Zugriff auf die Daten verwendet wird, ist 10.10.10.7. Der Filter läuft nach 30 Minuten ab.

```
cluster1::> vserver security trace filter create -vserver vs1 -index 1
-path /dir1/dir2/file.txt -time-enabled 30 -client-ip 10.10.10.7
cluster1::> vserver security trace filter show -index 1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    10.10.10.7   /dir1/dir2/file.txt          no       -
```

Der folgende Befehl erstellt einen Security-Trace-Filter mit einem relativen Pfad für die `-path` Option. Der Filter verfolgt den Dateizugriff eines Windows-Benutzers namens „joe“. Joe greift auf eine Datei mit einem Freigabepfad `\\server\share1\dir1\dir2\file.txt` zu. Der Filter protokolliert Zulassungs- und Ablehnungsereignisse.

```
cluster1::> vserver security trace filter create -vserver vs1 -index 2
-path /dir1/dir2/file.txt -trace-allow yes -windows-name mydomain\joe

cluster1::> vserver security trace filter show -vserver vs1 -index 2
                              Vserver: vs1
                         Filter Index: 2
            Client IP Address to Match: -
                                 Path: /dir1/dir2/file.txt
                  Windows User Name: mydomain\joe
                     UNIX User Name: -
                  Trace Allow Events: yes
                     Filter Enabled: enabled
             Minutes Filter is Enabled: 60
```

Informationen zu Sicherheitsverfolgungsfiltern in ONTAP SVMs

Zeigen Sie die Details des Security Trace Filters auf Ihrer Storage Virtual Machine (SVM) an, um die Zugriffsvorgänge zu identifizieren, die jeder Filter nachverfolgt.

System Manager

Ab ONTAP 9.6 können Sie den System Manager verwenden, um den Dateizugriff auf der SVM nachzuverfolgen.

Schritte

1. Öffnen Sie das System Manager dashboard.
2. Wählen Sie unter **Cluster Storage VMs** aus.
3. Wählen Sie ⋮ für die passende SVM aus.
4. Wählen Sie **Trace file access**.
5. Stellen Sie das Protokoll für den Dateizugriff auf **SMB/CIFS** oder **NFS** ein.
6. Geben Sie den **User name** ein.
7. Geben Sie die **Client IP address** ein.
8. Optional können Sie eine oder mehrere der folgenden Optionen auswählen:
   a. Wählen Sie **Trace particular path**, um die Datei oder den Dateipfad anzugeben, der verfolgt werden soll.
   b. Wählen Sie **Nur Zugriff verweigerte Einträge anzeigen**, um die Ablaufverfolgung auf Zugriff verweigerte Ereignisse zu beschränken.
9. Wählen Sie **Start tracing** aus.

CLI

Verwenden Sie die CLI, um den Dateizugriff auf der SVM zu verfolgen.

Schritt

1. Informationen zu den Einträgen des Sicherheitsverfolgungsfilters lassen sich mit dem `vserver security trace filter show` Befehl anzeigen.

   Weitere Informationen zu `vserver security trace filter show` finden sich in der "ONTAP-Befehlsreferenz".

Beispiele

Der folgende Befehl zeigt Informationen zu allen Security Trace-Filtern auf SVM vs1 an:

```
cluster1::> vserver security trace filter show -vserver vs1
Vserver  Index   Client-IP            Path            Trace-Allow
Windows-Name
-------- -----  -----------  ----------------------   -----------
-------------
vs1        1    -            /dir1/dir2/file.txt          yes      -
vs1        2    -            /dir3/dir4/                  no
mydomain\joe
```

Anzeige der Sicherheitsverfolgungsergebnisse in ONTAP SVMs

Sie können die Ergebnisse der Sicherheitsverfolgung anzeigen, die für Dateivorgänge generiert wurden, die den Sicherheitsverfolgungsfiltern entsprechen. Die Ergebnisse können zur Validierung Ihrer Dateizugriffssicherheitskonfiguration oder zur

Fehlerbehebung bei SMB- und NFS-Dateizugriffsproblemen verwendet werden.

Bevor Sie beginnen

Ein aktivierter Sicherheitstrace-Filter muss vorhanden sein und es müssen Vorgänge von einem SMB- oder NFS-Client durchgeführt worden sein, der dem Sicherheitstrace-Filter entspricht, um Sicherheitstrace-Ergebnisse zu generieren.

Über diese Aufgabe

Sie können eine Zusammenfassung aller Sicherheitstrace-Ergebnisse anzeigen oder die angezeigten Informationen durch Angabe optionaler Parameter anpassen. Dies kann hilfreich sein, wenn die Sicherheitstrace-Ergebnisse eine große Anzahl von Datensätzen enthalten.

Wenn Sie keinen der optionalen Parameter angeben, wird Folgendes angezeigt:

- Name der Storage Virtual Machine (SVM)
- Knotenname
- Sicherheits-Trace-Indexnummer
- Sicherheitsstil
- Pfad
- Grund
- Benutzername

  Der Benutzername wird abhängig von der Konfiguration des Trace-Filters angezeigt:

Wenn der Filter konfiguriert ist…	Dann…
Mit einem UNIX-Benutzernamen	Das Ergebnis der Sicherheitsüberwachung zeigt den UNIX-Benutzernamen an.
Mit einem Windows-Benutzernamen	Das Ergebnis der Sicherheitsüberwachung zeigt den Windows-Benutzernamen an.
Ohne Benutzernamen	Das Ergebnis der Sicherheitsüberwachung zeigt den Windows-Benutzernamen an.

Sie können die Ausgabe mithilfe optionaler Parameter anpassen. Zu den optionalen Parametern, mit denen Sie die in der Befehlsausgabe zurückgegebenen Ergebnisse eingrenzen können, gehören unter anderem die folgenden:

Optionaler Parameter	Beschreibung
`-fields field_name, ...`	Zeigt die Ausgabe in den von Ihnen ausgewählten Feldern an. Sie können diesen Parameter entweder allein oder in Kombination mit anderen optionalen Parametern verwenden.
`-instance`	Zeigt detaillierte Informationen zu Security Trace-Ereignissen an. Mit diesem Parameter und weiteren optionalen Parametern werden detaillierte Informationen zu bestimmten Filterergebnissen angezeigt.
`-node node_name`	Zeigt nur Informationen zu Ereignissen auf dem angegebenen Knoten an.
`-vserver vserver_name`	Zeigt nur Informationen über Ereignisse auf der angegebenen SVM an.

`-index integer`	Zeigt Informationen zu den Ereignissen an, die durch den Filter entsprechend der angegebenen Indexnummer aufgetreten sind.
`-client-ip IP_address`	Zeigt Informationen zu den Ereignissen, die infolge des Dateizugriffs von der angegebenen Client-IP-Adresse aufgetreten sind.
`-path path`	Zeigt Informationen zu den Ereignissen an, die infolge des Dateizugriffs auf den angegebenen Pfad aufgetreten sind.
`-user-name user_name`	Zeigt Informationen zu den Ereignissen an, die infolge des Dateizugriffs durch den angegebenen Windows- oder UNIX-Benutzer aufgetreten sind.
`-security-style security_style`	Zeigt Informationen über die Ereignisse an, die auf Dateisystemen mit dem angegebenen Sicherheitsstil aufgetreten sind.

Weitere Informationen zu anderen optionalen Parametern finden sich in der "ONTAP-Befehlsreferenz".

Schritt

1. Sicherheits-Trace-Filter-Ergebnisse werden mit dem `vserver security trace trace-result show` Befehl angezeigt.

   ```
   vserver security trace trace-result show -user-name domain\user
   ```

   ```
   Vserver: vs1

   Node     Index   Filter Details          Reason
   -------- ------- ---------------------  ----------------------------
   node1    3       User:domain\user       Access denied by explicit ACE
                    Security Style:mixed
                    Path:/dir1/dir2/

   node1    5       User:domain\user       Access denied by explicit ACE
                    Security Style:unix
                    Path:/dir1/
   ```

Sicherheitsverfolgungsfilter auf ONTAP SVMs ändern

Wenn die optionalen Filterparameter geändert werden sollen, die zur Bestimmung der zu protokollierenden Zugriffsereignisse verwendet werden, können bestehende Sicherheits-Trace-Filter modifiziert werden.

Über diese Aufgabe

Sie müssen den zu ändernden Sicherheitsverfolgungsfilter identifizieren, indem Sie den Namen der Storage Virtual Machine (SVM), auf die der Filter angewendet wird, und die Indexnummer des Filters angeben. Alle optionalen Filterparameter können geändert werden.

Schritte

1. Ändern eines Security Trace-Filters:

```
vserver security trace filter modify -vserver vserver_name -index
index_numberfilter_parameters
```

- `vserver_name` ist der Name der SVM, auf die ein Sicherheits-Trace-Filter angewendet werden soll.
- `index_number` ist die Indexnummer, die auf den Filter angewendet werden soll. Die zulässigen Werte für diesen Parameter sind 1 bis 10.
- `filter_parameters` ist eine Liste optionaler Filterparameter.

2. Der Eintrag des Sicherheitsverfolgungsfilters wird überprüft:

```
vserver security trace filter show -vserver vserver_name -index index_number
```

Beispiel

Der folgende Befehl ändert den Sicherheits-Trace-Filter mit der Indexnummer 1. Der Filter protokolliert Ereignisse für jeden Benutzer, der auf eine Datei mit einem Freigabepfad `\\server\share1\dir1\dir2\file.txt` von einer beliebigen IP-Adresse aus zugreift. Der Filter verwendet einen vollständigen Pfad für die `-path` Option. Der Filter protokolliert Zulassungs- und Ablehnungsereignisse.

```
cluster1::> vserver security trace filter modify -vserver vs1 -index 1
-path /dir1/dir2/file.txt -trace-allow yes

cluster1::> vserver security trace filter show -vserver vs1 -index 1
                                Vserver: vs1
                           Filter Index: 1
              Client IP Address to Match: -
                                    Path: /dir1/dir2/file.txt
                     Windows User Name: -
                        UNIX User Name: -
                    Trace Allow Events: yes
                        Filter Enabled: enabled
               Minutes Filter is Enabled: 60
```

Sicherheits-Tracefilter auf ONTAP SVMs löschen

Wenn ein Sicherheitsverfolgungsfiltereintrag nicht mehr benötigt wird, kann er gelöscht werden. Da maximal 10 Sicherheitsverfolgungsfilter pro Storage Virtual Machine (SVM) möglich sind, ermöglicht das Löschen nicht benötigter Filter das Erstellen neuer Filter, wenn das Maximum erreicht ist.

Über diese Aufgabe

Um den zu löschenden Security Trace-Filter eindeutig zu identifizieren, sind die folgenden Angaben erforderlich:

- Der Name der SVM, auf die der Trace-Filter angewendet wird
- Die Filterindexnummer des Trace-Filters

Schritte

1. Die Filterindexnummer des Security Trace Filtereintrags, der gelöscht werden soll, identifizieren:

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        1    -            /dir1/dir2/file.txt          yes      -
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

2. Mit den Informationen zur Filterindexnummer aus dem vorherigen Schritt den Filtereintrag löschen:

   ```
   vserver security trace filter delete -vserver vserver_name -index index_number

   vserver security trace filter delete -vserver vs1 -index 1
   ```

3. Es wird überprüft, ob der Eintrag des Sicherheitsverfolgungsfilters gelöscht wurde:

   ```
   vserver security trace filter show -vserver vserver_name

   vserver security trace filter show -vserver vs1
   ```

   ```
   Vserver  Index   Client-IP            Path            Trace-Allow
   Windows-Name
   -------- -----  -----------  ----------------------   -----------
   -------------
   vs1        2    -            /dir3/dir4/                  no
   mydomain\joe
   ```

Sicherheitsverfolgungsdatensätze auf ONTAP SVMs löschen

Nachdem ein Filter-Trace-Datensatz zur Überprüfung der Dateizugriffssicherheit oder zur Fehlerbehebung bei Zugriffsproblemen von SMB- oder NFS-Clients verwendet wurde, kann der Security-Trace-Datensatz aus dem Security-Trace-Protokoll gelöscht werden.

Über diese Aufgabe

Bevor Sie einen Sicherheitsverfolgungsdatensatz löschen können, muss die Sequenznummer des Datensatzes bekannt sein.

Jede Storage Virtual Machine (SVM) kann maximal 128 Trace-Datensätze speichern. Wenn die

maximale Anzahl auf der SVM erreicht ist, werden die ältesten Trace-Datensätze automatisch gelöscht, sobald neue hinzugefügt werden. Wenn das manuelle Löschen von Trace-Datensätzen auf dieser SVM vermieden werden soll, kann ONTAP die ältesten Trace-Ergebnisse nach Erreichen des Maximums automatisch löschen, um Platz für neue Ergebnisse zu schaffen.

Schritte

1. Die Sequenznummer des Datensatzes, der gelöscht werden soll, identifizieren:

   ```
   vserver security trace trace-result show -vserver vserver_name -instance
   ```

2. Den Sicherheitsprotokolleintrag löschen:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name -seqnum integer

   vserver security trace trace-result delete -vserver vs1 -node node1 -seqnum
   999
   ```

   - `-node node_name` ist der Name des Cluster-Knotens, auf dem das persistente Tracing-Ereignis aufgetreten ist, das gelöscht werden soll.

     Dies ist ein Pflichtparameter.

   - `-vserver vserver_name` ist der Name der SVM, auf der das persistente Tracing-Ereignis aufgetreten ist, das gelöscht werden soll.

     Dies ist ein Pflichtparameter.

   - `-seqnum integer` ist die Sequenznummer des Protokollereignisses, das gelöscht werden soll.

     Dies ist ein Pflichtparameter.

Alle Sicherheitsverfolgungsdatensätze auf ONTAP SVMs löschen

Wenn keine der vorhandenen Security-Trace-Datensätze beibehalten werden soll, ist das Löschen aller Datensätze auf einem Knoten mit einem einzigen Befehl möglich.

Schritt

1. Alle Sicherheitsverfolgungsdatensätze löschen:

   ```
   vserver security trace trace-result delete -node node_name -vserver
   vserver_name *
   ```

   - `-node node_name` ist der Name des Cluster-Knotens, auf dem das persistente Tracing-Ereignis aufgetreten ist, das gelöscht werden soll.
   - `-vserver vserver_name` ist der Name der Storage Virtual Machine (SVM), auf der das persistente Tracing-Ereignis aufgetreten ist, das gelöscht werden soll.

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.