Scannerpools konfigurieren

ONTAP 9

NetApp
September 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/antivirus/configure-scanner-pools-concept.html on September 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Scannerpools konfigurieren 1
Informationen zur Konfiguration von ONTAP Vscan Scannerpools 1
Einen ONTAP Vscan Scannerpool auf einem einzelnen Cluster erstellen 1
ONTAP Vscan Scannerpools in MetroCluster Konfigurationen erstellen 2
Eine Scannerrichtlinie auf einem einzelnen Cluster mit ONTAP Vscan anwenden 4
Scannerrichtlinien in MetroCluster ONTAP Vscan Konfigurationen anwenden 6
ONTAP Befehle zur Verwaltung von Scannerpools in Vscan 7

Scannerpools konfigurieren

Informationen zur Konfiguration von ONTAP Vscan Scannerpools

Ein Scanner Pool definiert die Vscan Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können. Eine Scanner Richtlinie legt fest, ob ein Scannerpool aktiv ist.

Wenn Sie auf einem SMB-Server eine Exportrichtlinie verwenden, müssen Sie jeden Vscan Server zur Exportrichtlinie hinzufügen.

Einen ONTAP Vscan Scannerpool auf einem einzelnen Cluster erstellen

Ein Scanner Pool definiert die Vscan Server und privilegierten Benutzer, die eine Verbindung zu SVMs herstellen können.

Bevor Sie beginnen

- SVMs und Vscan Server müssen sich in derselben Domäne oder in vertrauenswürdigen Domänen befinden.
- Ein ONTAP Antivirus Connector wird mit der Cluster Management-LIF konfiguriert.
- Die Liste der privilegierten Benutzer muss die Domäne und den Benutzernamen enthalten, die der Vscan Server für die Verbindung zur SVM verwendet.
- Sobald der Scannerpool konfiguriert ist, lässt sich der Verbindungsstatus zu den Servern überprüfen.

Schritte

1. Einen Scannerpool erstellen:

   ```
   vserver vscan scanner-pool create -vserver cluster_admin_SVM -scanner-pool
   scanner_pool -hostnames Vscan_server_hostnames -privileged-users
   privileged_users
   ```

   - Eine Cluster-Admin-SVM angeben.
   - Für jeden Vscan Server Hostnamen ist eine IP-Adresse oder ein FQDN anzugeben.
   - Die Domäne und den Benutzernamen für jeden privilegierten Benutzer angeben.

   Weitere Informationen zu `vserver vscan scanner-pool create` finden sich in der "ONTAP-Befehlsreferenz".

2. Es wird überprüft, ob der Scannerpool erstellt wurde:

   ```
   vserver vscan scanner-pool show -vserver cluster_admin_SVM -scanner-pool
   scanner_pool
   ```

   Der folgende Befehl zeigt die Details für den `SP`scanner-pool an:

```
cluster1::> vserver vscan scanner-pool show -vserver cluster_admin_SVM
-scanner-pool SP

                                    Vserver: cluster_admin_SVM
                                Scanner Pool: SP
                              Applied Policy: idle
                              Current Status: off
          Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: cluster
        List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

Sie können auch den `vserver vscan scanner-pool show` Befehl verwenden, um alle Scannerpools im Cluster anzuzeigen. Weitere Informationen zu `vserver vscan scanner-pool show` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Vscan Scannerpools in MetroCluster Konfigurationen erstellen

Sie müssen auf jedem Cluster in einer MetroCluster Konfiguration primäre und sekundäre Scannerpools erstellen, die den primären und sekundären SVMs auf dem Cluster entsprechen.

Bevor Sie beginnen

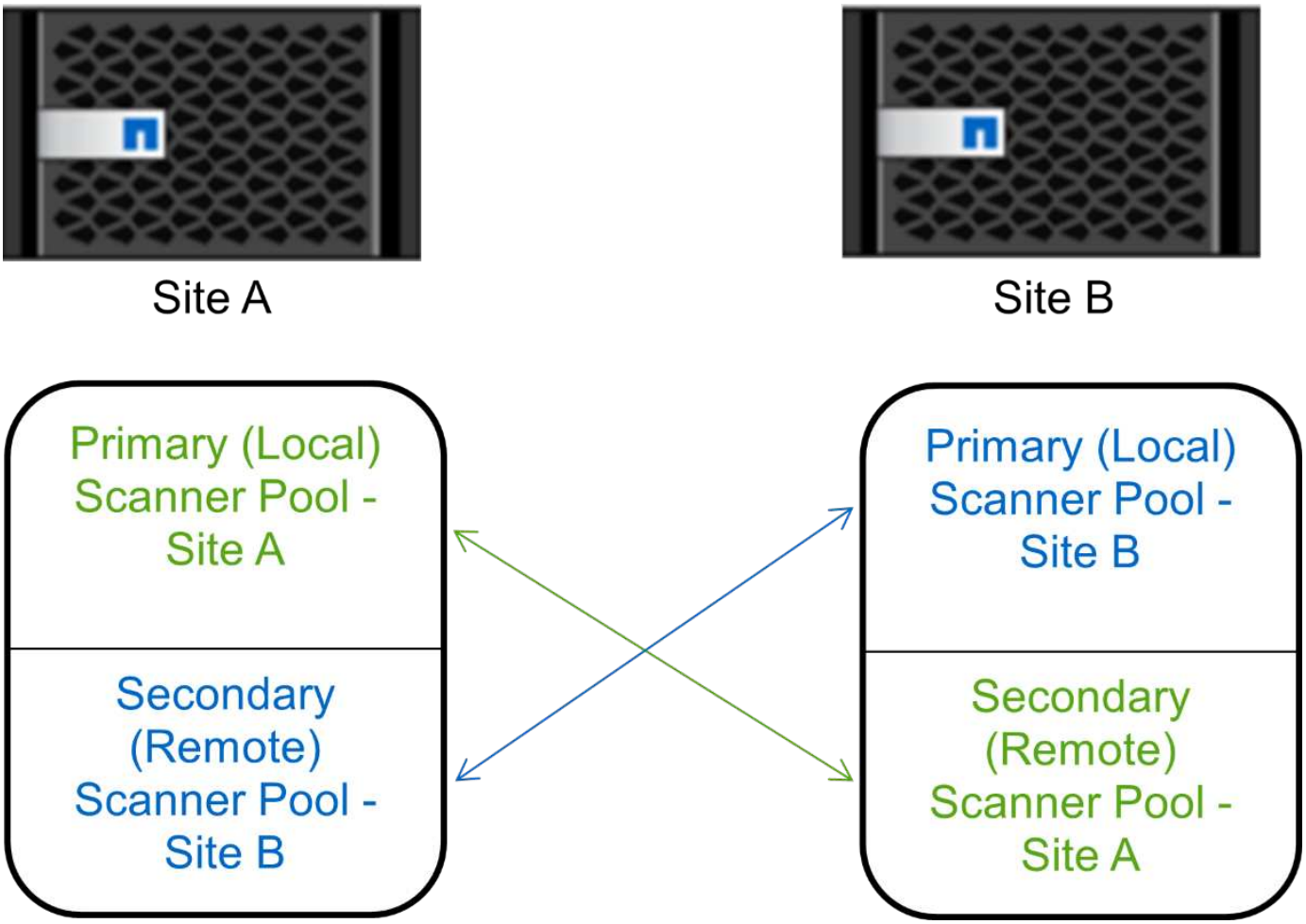
- SVMs und Vscan Server müssen sich in derselben Domäne oder in vertrauenswürdigen Domänen befinden.
- Für Scannerpools, die für eine einzelne SVM definiert sind, muss ONTAP Antivirus Connector mit dem SVM-Management-LIF oder dem SVM-Daten-LIF konfiguriert sein.
- Für Scannerpools, die für alle SVMs in einem Cluster definiert sind, muss ONTAP Antivirus Connector mit dem Cluster-Management-LIF konfiguriert sein.
- Die Liste der privilegierten Benutzer muss das Domänenbenutzerkonto enthalten, das der Vscan Server für die Verbindung zur SVM verwendet.
- Sobald der Scannerpool konfiguriert ist, lässt sich der Verbindungsstatus zu den Servern überprüfen.

Über diese Aufgabe

MetroCluster Konfigurationen schützen Daten durch die Implementierung zweier physisch getrennter, gespiegelter Cluster. Jeder Cluster repliziert synchron die Daten und die SVM-Konfiguration des anderen. Eine primäre SVM im lokalen Cluster stellt Daten bereit, wenn der Cluster online ist. Eine sekundäre SVM im lokalen Cluster stellt Daten bereit, wenn der entfernte Cluster offline ist.

Das bedeutet, dass Sie in einer MetroCluster Konfiguration auf jedem Cluster primäre und sekundäre Scannerpools erstellen müssen, der sekundäre Pool wird aktiv, wenn der Cluster beginnt, Daten vom sekundären SVM bereitzustellen. Für Disaster Recovery (DR) ist die Konfiguration ähnlich wie bei MetroCluster.

Diese Abbildung zeigt eine typische MetroCluster/DR Konfiguration.



Schritte

1. Einen Scannerpool erstellen:

```
vserver vscan scanner-pool create -vserver <data_SVM|cluster_admin_SVM>
-scanner-pool <scanner_pool> -hostnames <Vscan_server_hostnames> -privileged
-users <privileged_users>
```

   - Geben Sie eine Daten-SVM für einen Pool an, der für eine einzelne SVM definiert ist, und eine Cluster-Admin-SVM für einen Pool, der für alle SVMs in einem Cluster definiert ist.
   - Für jeden Vscan Server Hostnamen ist eine IP-Adresse oder ein FQDN anzugeben.
   - Die Domäne und den Benutzernamen für jeden privilegierten Benutzer angeben.

     Alle Scanner-Pools sind aus dem Cluster zu erstellen, das die primäre SVM enthält.

     Weitere Informationen zu `vserver vscan scanner-pool create` finden sich in der "ONTAP-Befehlsreferenz".

     Die folgenden Befehle erstellen primäre und sekundäre Scannerpools auf jedem Cluster in einer MetroCluster Konfiguration:

```
site_A::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_siteA -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

site_B::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool1_for_siteB -hostnames scan1 -privileged-users cifs
\u1,cifs\u2

site_A::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_siteA -hostnames scan2 -privileged-users cifs
\u1,cifs\u2

site_B::> vserver vscan scanner-pool create -vserver cifssvm1 -
scanner-pool pool2_for_siteB -hostnames scan2 -privileged-users cifs
\u1,cifs\u2
```

2. Es sollte überprüft werden, ob die Scannerpools erstellt wurden:

   `vserver vscan scanner-pool show -vserver <data_SVM|cluster_admin_SVM> -scanner -pool <scanner_pool>`

   Der folgende Befehl zeigt die Details für den Scannerpool an `pool1_for_siteA`:

```
site_A::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_siteA

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_siteA
                              Applied Policy: idle
                              Current Status: off
         Cluster on Which Policy Is Applied: -
                   Scanner Pool Config Owner: vserver
       List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   Sie können auch den `vserver vscan scanner-pool show`Befehl verwenden, um alle Scanner-Pools auf einer SVM anzuzeigen. Weitere Informationen zu `vserver vscan scanner-pool show` finden sich in der "ONTAP-Befehlsreferenz".

Eine Scannerrichtlinie auf einem einzelnen Cluster mit ONTAP Vscan anwenden

Eine Scanner Richtlinie legt fest, ob ein Scannerpool aktiv ist. Ein scanner-pool muss

aktiviert werden, bevor die darin definierten Vscan Server eine Verbindung zu einer SVM herstellen können.

Über diese Aufgabe

- Auf einen scanner-pool kann nur eine Scannerrichtlinie angewendet werden.
- Wenn Sie einen scanner-pool für alle SVMs in einem Cluster erstellt haben, muss auf jeder SVM individuell eine scanner-policy angewendet werden.

Schritte

1. Scannerrichtlinie anwenden:

   ```
   vserver vscan scanner-pool apply-policy -vserver data_SVM -scanner-pool
   scanner_pool -scanner-policy primary|secondary|idle -cluster
   cluster_to_apply_policy_on
   ```

   Eine Scannerrichtlinie kann einen der folgenden Werte haben:

   - `Primary`gibt an, dass der scanner-pool aktiv ist.
   - `Secondary`legt fest, dass der scanner-pool nur dann aktiv ist, wenn keiner der Vscan-Server im primären scanner-pool verbunden ist.
   - `Idle`gibt an, dass der scanner-pool inaktiv ist.

     Das folgende Beispiel zeigt, dass der Scanner-Pool mit dem Namen `SP` auf der `vs1` SVM aktiv ist:

   ```
   cluster1::> vserver vscan scanner-pool apply-policy -vserver vs1
   -scanner-pool SP  -scanner-policy primary
   ```

2. Es sollte überprüft werden, ob der scanner-pool aktiv ist:

   ```
   vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner
   -pool scanner_pool
   ```

   Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die Details für den `SP`scanner-pool an:

   ```
   cluster1::> vserver vscan scanner-pool show -vserver vs1 -scanner-pool
   SP

                                    Vserver: vs1
                                Scanner Pool: SP
                              Applied Policy: primary
                              Current Status: on
           Cluster on Which Policy Is Applied: cluster1
                    Scanner Pool Config Owner: vserver
         List of IPs of Allowed Vscan Servers: 1.1.1.1, 10.72.204.27
   ```

```
List of Host Names of Allowed Vscan Servers: 1.1.1.1, vmwin204-
27.fsct.nb
                    List of Privileged Users: cifs\u1, cifs\u2
```

Der `vserver vscan scanner-pool show-active` Befehl kann verwendet werden, um die aktiven scanner-pool auf einer SVM anzuzeigen. Weitere Informationen zu `vserver vscan scanner-pool show-active` finden sich in der "ONTAP-Befehlsreferenz".

Scannerrichtlinien in MetroCluster ONTAP Vscan Konfigurationen anwenden

Eine Scanner Richtlinie legt fest, ob ein Scannerpool aktiv ist. Einer scanner-pool-Policy muss auf die primären und sekundären scanner-pools auf jedem Cluster in einer MetroCluster Konfiguration angewendet werden.

Über diese Aufgabe

- Auf einen scanner-pool kann nur eine Scannerrichtlinie angewendet werden.
- Wenn Sie einen scanner-pool für alle SVMs in einem Cluster erstellt haben, muss auf jeder SVM individuell eine scanner-policy angewendet werden.
- Für die Notfallwiederherstellung und MetroCluster Konfigurationen ist es erforderlich, eine Scannerrichtlinie auf jeden scanner-pool im lokalen Cluster und im Remote Cluster anzuwenden.
- In der Richtlinie, die Sie für den lokalen Cluster erstellen, muss der lokale Cluster im `cluster` Parameter angegeben werden. In der Richtlinie, die Sie für den Remote Cluster erstellen, muss der Remote Cluster im `cluster` Parameter angegeben werden. Der Remote Cluster kann dann im Katastrophenfall die Virenprüfung übernehmen.

Schritte

1. Scannerrichtlinie anwenden:

   `vserver vscan scanner-pool apply-policy -vserver` *`data_SVM`* `-scanner-pool` *`scanner_pool`* `-scanner-policy primary|secondary|idle -cluster` *`cluster_to_apply_policy_on`*

   Weitere Informationen zu `vserver vscan scanner-pool apply-policy` finden sich in der "ONTAP-Befehlsreferenz".

   Eine Scannerrichtlinie kann einen der folgenden Werte haben:

   - `Primary`gibt an, dass der scanner-pool aktiv ist.
   - `Secondary`legt fest, dass der scanner-pool nur dann aktiv ist, wenn keiner der Vscan-Server im primären scanner-pool verbunden ist.
   - `Idle`gibt an, dass der scanner-pool inaktiv ist.

   > Alle Scannerrichtlinien müssen aus dem Cluster angewendet werden, das die primäre SVM enthält.

   Die folgenden Befehle wenden Scannerrichtlinien auf die primären und sekundären scanner-pool auf jedem Cluster in einer MetroCluster Konfiguration an:

```
cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site1 -scanner-policy primary -cluster cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site1 -scanner-policy secondary -cluster
cluster1

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool2_for_site2 -scanner-policy primary -cluster cluster2

cluster1::>vserver vscan scanner-pool apply-policy -vserver cifssvm1
-scanner-pool pool1_for_site2 -scanner-policy secondary -cluster
cluster2
```

2. Es sollte überprüft werden, ob der scanner-pool aktiv ist:

   `vserver vscan scanner-pool show -vserver data_SVM|cluster_admin_SVM -scanner -pool scanner_pool`

   Weitere Informationen zu `vserver vscan scanner-pool show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die Details für den Scannerpool an `pool1`:

```
cluster1::> vserver vscan scanner-pool show -vserver cifssvm1 -scanner
-pool pool1_for_site1

                                    Vserver: cifssvm1
                                Scanner Pool: pool1_for_site1
                             Applied Policy: primary
                             Current Status: on
          Cluster on Which Policy Is Applied: cluster1
                   Scanner Pool Config Owner: vserver
        List of IPs of Allowed Vscan Servers:
List of Host Names of Allowed Vscan Servers: scan1
                    List of Privileged Users: cifs\u1,cifs\u2
```

   Der `vserver vscan scanner-pool show-active` Befehl kann verwendet werden, um die aktiven scanner-pool auf einer SVM anzuzeigen. Weitere Informationen zu `vserver vscan scanner-pool show-active` finden sich in der "ONTAP-Befehlsreferenz".

ONTAP Befehle zur Verwaltung von Scannerpools in Vscan

Sie können Scannerpools bearbeiten und löschen sowie privilegierte Benutzer und Vscan Server für einen Scannerpool verwalten. Zusammenfassende Informationen zum

Scannerpool sind ebenfalls einsehbar.

Wenn Sie möchten…	Führen Sie den folgenden Befehl aus…
Einen Scannerpool ändern	`vserver vscan scanner-pool modify`
Einen Scannerpool löschen	`vserver vscan scanner-pool delete`
Privilegierte Benutzer zu einem Scannerpool hinzufügen	`vserver vscan scanner-pool privileged-users add`
Privilegierte Benutzer aus einem Scanner Pool entfernen	`vserver vscan scanner-pool privileged-users remove`
Vscan-Server zu einem Scannerpool hinzufügen	`vserver vscan scanner-pool servers add`
Vscan Server aus einem Scannerpool entfernen	`vserver vscan scanner-pool servers remove`
Zusammenfassung und Details für einen Scannerpool anzeigen	`vserver vscan scanner-pool show`
Privilegierte Benutzer für einen Scanner-Pool anzeigen	`vserver vscan scanner-pool privileged-users show`
Vscan Server für alle Scannerpools anzeigen	`vserver vscan scanner-pool servers show`

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

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.