



AWS

Cloud Manager 3.8

NetApp
March 25, 2024

Inhalt

- AWS 1
 - AWS Zugangsdaten und Berechtigungen 1
 - Verwalten von AWS Anmeldedaten und Abonnements für Cloud Manager 4

AWS

AWS Zugangsdaten und Berechtigungen

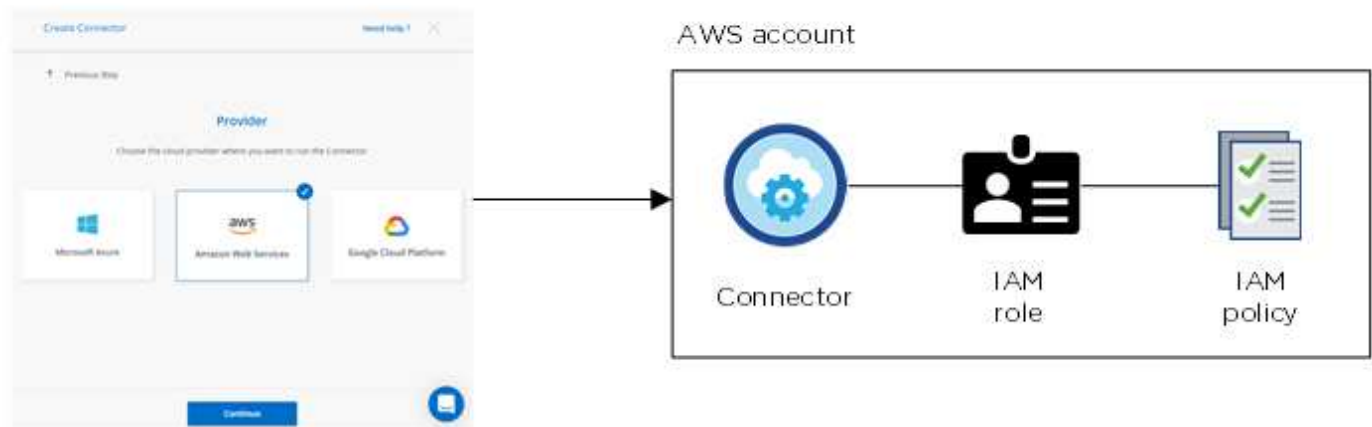
Mit Cloud Manager können Sie die AWS Zugangsdaten auswählen, die Sie bei der Implementierung von Cloud Volumes ONTAP verwenden möchten. Alle Cloud Volumes ONTAP Systeme können über die ersten AWS Zugangsdaten implementiert oder zusätzliche Anmeldedaten hinzugefügt werden.

Erste AWS Zugangsdaten

Wenn Sie einen Connector von Cloud Manager bereitstellen, müssen Sie ein AWS-Konto mit Berechtigungen zum Starten der Connector-Instanz verwenden. Die erforderlichen Berechtigungen werden im aufgeführt ["Connector-Implementierungsrichtlinie für AWS"](#).

Wenn Cloud Manager die Connector-Instanz in AWS startet, erstellt sie eine IAM-Rolle und ein Instanzprofil für die Instanz. Zudem wird eine Richtlinie angehängt, die Cloud Manager Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. ["Überprüfen Sie, wie Cloud Manager die Berechtigungen verwendet"](#).

Cloud Manager



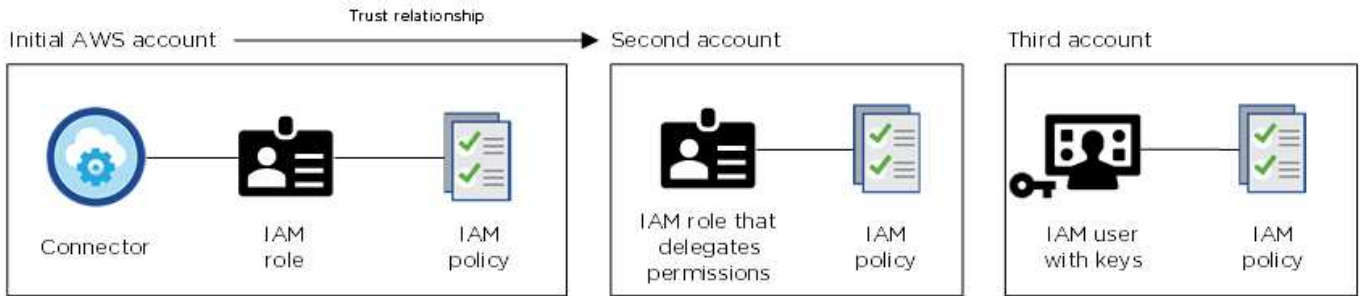
Cloud Manager wählt die AWS Zugangsdaten standardmäßig aus, wenn Sie eine neue Arbeitsumgebung für Cloud Volumes ONTAP erstellen:

Details & Credentials			
Instance Profile	XXXXXXXXXXXX	QA Subscription	Edit Credentials
Credentials	Account ID	Marketplace Subscription	

Zusätzliche AWS Zugangsdaten

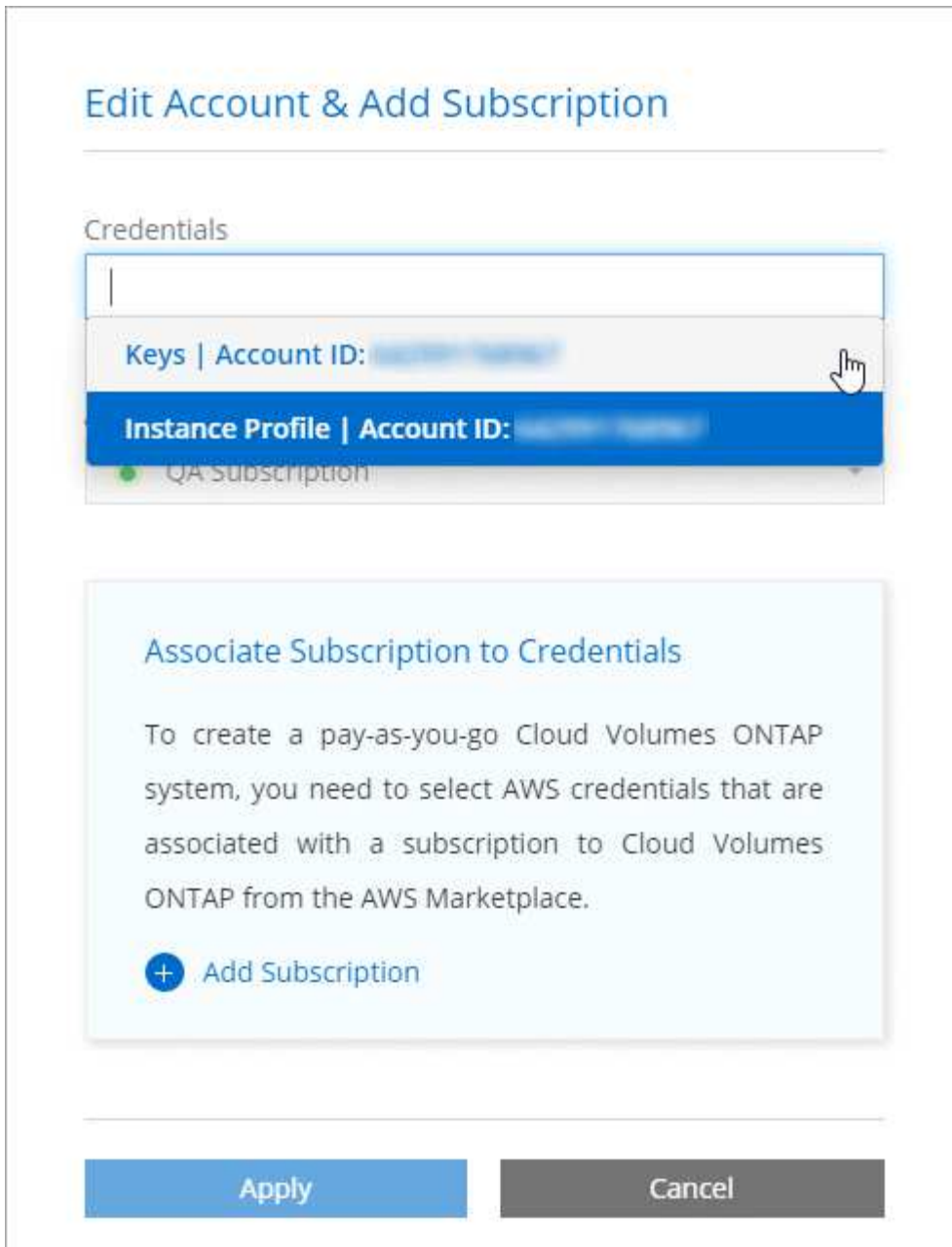
Wenn Sie Cloud Volumes ONTAP in verschiedenen AWS Accounts starten möchten, haben Sie eine der Möglichkeiten ["AWS Schlüssel für einen IAM-Benutzer oder den ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen"](#). Die folgende Abbildung zeigt zwei zusätzliche Konten: Eines mit Berechtigungen über

eine IAM-Rolle in einem vertrauenswürdigen Konto und ein weiteres über die AWS Schlüssel eines IAM-Benutzers:



Das würden Sie dann tun ["Fügen Sie die Kontoanmeldeinformationen zu Cloud Manager hinzu"](#) Indem Sie den Amazon Resource Name (ARN) der IAM-Rolle oder die AWS-Schlüssel für den IAM-Benutzer angeben.

Nachdem Sie einen weiteren Satz von Anmeldeinformationen hinzugefügt haben, können Sie zu ihnen wechseln, wenn Sie eine neue Arbeitsumgebung erstellen:



Wie sieht es mit Marketplace-Implementierungen und On-Premises-Implementierungen aus?

In den obigen Abschnitten wird die empfohlene Implementierungsmethode für den Connector, der aus Cloud Manager stammt, beschrieben. Sie können auch einen Connector in AWS von der bereitstellen "[AWS Marketplace](#)" Und das können Sie auch "[Installieren Sie den Steckverbinder vor Ort](#)".

Wenn Sie den Marktplatz nutzen, werden Berechtigungen auf die gleiche Weise bereitgestellt. Sie müssen lediglich die IAM-Rolle manuell erstellen und einrichten und dann Berechtigungen für weitere Konten bereitstellen.

Bei On-Premises-Implementierungen können nicht eine IAM-Rolle für das Cloud Manager-System eingerichtet werden, Sie können aber Berechtigungen wie bei zusätzlichen AWS-Konten bereitstellen.

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Wie oben beschrieben, können Sie mit Cloud Manager AWS Zugangsdaten auf verschiedene Arten bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder AWS-Zugriffsschlüssel.

Bei den ersten beiden Optionen verwendet Cloud Manager den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dies ist die Best Practice, also automatisch und sicher.

Wenn Sie Cloud Manager mit AWS-Zugriffsschlüsseln bereitstellen, sollten Sie die Schlüssel drehen, indem Sie sie in Cloud Manager in einem regelmäßigen Intervall aktualisieren. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Verwalten von AWS Anmeldedaten und Abonnements für Cloud Manager

Wenn Sie ein Cloud Volumes ONTAP System erstellen, müssen Sie die AWS Zugangsdaten und das Abonnement auswählen, die mit diesem System verwendet werden sollen. Wenn Sie mehrere AWS-Abonnements verwalten, können Sie jedes davon auf der Seite „Anmeldeinformationen“ verschiedenen AWS Zugangsdaten zuweisen.

Bevor Sie Cloud Manager mit AWS Zugangsdaten ergänzen, müssen Sie die erforderlichen Berechtigungen für dieses Konto bereitstellen. Mit den Berechtigungen kann Cloud Manager Ressourcen und Prozesse innerhalb dieses AWS Kontos verwalten. Wie Sie die Berechtigungen bereitstellen, hängt davon ab, ob Sie Cloud Manager mit AWS Schlüsseln oder dem ARN einer Rolle in einem vertrauenswürdigen Konto bereitstellen möchten.



Bei der Bereitstellung eines Connectors von Cloud Manager fügte Cloud Manager automatisch AWS Zugangsdaten für das Konto hinzu, in dem Sie den Connector implementiert haben. Dieses erste Konto wird nicht hinzugefügt, wenn Sie die Connector-Software manuell auf einem vorhandenen System installiert haben. ["Weitere Informationen zu AWS Zugangsdaten und Berechtigungen"](#).

Auswahl

- [Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln](#)
- [Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten](#)

Wie kann ich meine AWS Zugangsdaten sicher drehen?

Mit Cloud Manager können Sie AWS Zugangsdaten auf verschiedene Arten bereitstellen: Eine mit der Connector-Instanz verknüpfte IAM-Rolle, eine IAM-Rolle in einem vertrauenswürdigen Konto oder die Bereitstellung von AWS Zugriffsschlüssel. "[Weitere Informationen zu AWS Zugangsdaten und Berechtigungen](#)".

Bei den ersten beiden Optionen verwendet Cloud Manager den AWS Security Token Service, um temporäre Anmeldedaten zu erhalten, die sich ständig drehen. Dieser Prozess gilt als Best Practice, also automatisch und sicher.

Wenn Sie Cloud Manager mit AWS-Zugriffsschlüsseln bereitstellen, sollten Sie die Schlüssel drehen, indem Sie sie in Cloud Manager in einem regelmäßigen Intervall aktualisieren. Es handelt sich hierbei um einen vollständig manuellen Prozess.

Erteilen von Berechtigungen durch die Bereitstellung von AWS Schlüsseln

Wenn Sie Cloud Manager mit AWS Schlüsseln für einen IAM-Benutzer bereitstellen möchten, müssen Sie diesem Benutzer die erforderlichen Berechtigungen erteilen. Die Cloud Manager IAM-Richtlinie definiert die AWS-Aktionen und -Ressourcen, die Cloud Manager verwenden darf.

Schritte

1. Laden Sie die IAM-Richtlinie von Cloud Manager aus herunter "[Seite „Cloud Manager Policies“ aufgeführt](#)".
2. Erstellen Sie über die IAM-Konsole Ihre eigene Richtlinie, indem Sie den Text aus der Cloud Manager IAM-Richtlinie kopieren und einfügen.

["AWS Dokumentation: Erstellung von IAM-Richtlinien"](#)

3. Hängen Sie die Richtlinie an eine IAM-Rolle oder einen IAM-Benutzer an.
 - "[AWS Documentation: Erstellung von IAM-Rollen](#)"
 - "[AWS Dokumentation: Hinzufügen und Entfernen von IAM-Richtlinien](#)"

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. [Sie können es jetzt zu Cloud Manager hinzufügen](#).

Gewährung von Berechtigungen durch Annahme von IAM-Rollen in anderen Konten

Sie können eine Vertrauensbeziehung zwischen dem Quell-AWS-Konto einrichten, in dem Sie die Connector-Instanz und anderen AWS-Konten mithilfe von IAM-Rollen bereitgestellt haben. Dann würden Sie Cloud Manager über die vertrauenswürdigen Konten mit dem ARN der IAM-Rollen versorgen.

Schritte

1. Rufen Sie das Zielkonto auf, in dem Sie Cloud Volumes ONTAP bereitstellen und eine IAM-Rolle erstellen möchten, indem Sie **ein weiteres AWS-Konto** auswählen.

Gehen Sie wie folgt vor:

- Geben Sie die ID des Kontos ein, auf dem sich die Connector-Instanz befindet.

- Hängen Sie die Cloud Manager IAM-Richtlinie an, die über die erhältlich ist ["Seite „Cloud Manager Policies“ aufgeführt"](#).

Create role



Select type of trusted entity

AWS service EC2, Lambda and others.	Another AWS account Belonging to you or 3rd party	Web identity Cognito or any OpenID provider	SAML 2.0 federation Your corporate directory
---	---	---	--

Allows entities in other accounts to perform actions in this account. [Learn more](#)

Specify accounts that can use this role

Account ID*

- Options** Require external ID (Best practice when a third party will assume this role)
 Require MFA ⓘ

2. Gehen Sie zum Quellkonto, auf dem sich die Konnektorinstanz befindet, und wählen Sie die IAM-Rolle aus, die an die Instanz angehängt ist.
 - a. Klicken Sie auf **Richtlinien anhängen** und dann auf **Richtlinien erstellen**.
 - b. Erstellen Sie eine Richtlinie, die die Aktion „STS:AssumeRole“ und den ARN der Rolle umfasst, die Sie im Zielkonto erstellt haben.

Beispiel

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": "sts:AssumeRole",
    "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
  }
}
```

Ergebnis

Das Konto verfügt nun über die erforderlichen Berechtigungen. [Sie können es jetzt zu Cloud Manager hinzufügen](#).

AWS Zugangsdaten zu Cloud Manager hinzufügen

Nachdem Sie ein AWS Konto mit den erforderlichen Berechtigungen eingerichtet haben, können Sie die Anmeldedaten für dieses Konto bei Cloud Manager hinzufügen. Damit können Sie Cloud Volumes ONTAP Systeme in diesem Konto starten.

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie

Anmeldeinformationen.



2. Klicken Sie auf **Anmeldedaten hinzufügen** und wählen Sie **AWS**.
3. Bereitstellen von AWS Schlüsseln oder dem ARN einer vertrauenswürdigen IAM-Rolle
4. Bestätigen Sie, dass die Richtlinienanforderungen erfüllt wurden, und klicken Sie auf **Weiter**.
5. Wählen Sie das Pay-as-you-go-Abonnement aus, das Sie mit den Anmeldedaten verknüpfen möchten, oder klicken Sie auf **Abonnement hinzufügen**, wenn Sie noch nicht über ein Abonnement verfügen.

Um ein Pay-as-you-go Cloud Volumes ONTAP System zu erstellen, müssen AWS Zugangsdaten über den AWS Marketplace mit einem Abonnement für Cloud Volumes ONTAP verknüpft werden.

6. Klicken Sie Auf **Hinzufügen**.

Ergebnis

Sie können jetzt bei der Erstellung einer neuen Arbeitsumgebung auf eine andere Gruppe von Anmeldeinformationen von der Seite Details und Anmeldeinformationen wechseln:

Edit Account & Add Subscription

Credentials

Keys Account ID: [REDACTED]
Instance Profile Account ID: [REDACTED]
QA Subscription

Associate Subscription to Credentials

To create a pay-as-you-go Cloud Volumes ONTAP system, you need to select AWS credentials that are associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

[+ Add Subscription](#)

Apply

Cancel

Verknüpfen eines AWS Abonnements mit den Zugangsdaten

Nachdem Sie Ihre AWS Zugangsdaten zu Cloud Manager hinzugefügt haben, können Sie ein AWS Marketplace Abonnement mit diesen Anmeldedaten verknüpfen. Mithilfe des Abonnements können Sie ein nutzungsbasiertes Cloud Volumes ONTAP System erstellen und andere NetApp Cloud-Services nutzen.

Es gibt zwei Szenarien, in denen Sie ein AWS Marketplace-Abonnement verknüpfen können, nachdem Sie bereits die Anmeldedaten zu Cloud Manager hinzugefügt haben:

- Sie haben ein Abonnement nicht zugeordnet, wenn Sie zum ersten Mal die Anmeldedaten zu Cloud Manager hinzugefügt haben.
- Sie möchten ein vorhandenes AWS Marketplace Abonnement durch ein neues Abonnement ersetzen.

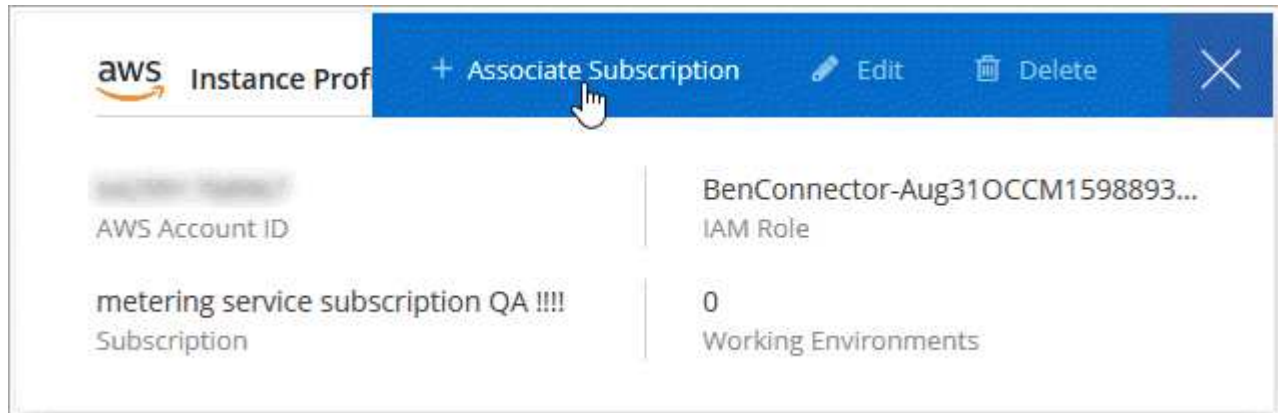
Was Sie benötigen

Sie müssen einen Konnektor erstellen, bevor Sie Cloud Manager-Einstellungen ändern können. ["Erfahren Sie,](#)

wie".

Schritte

1. Klicken Sie oben rechts in der Cloud Manager-Konsole auf das Symbol Einstellungen und wählen Sie **Anmeldeinformationen**.
2. Bewegen Sie den Mauszeiger über einen Satz von Anmeldeinformationen, und klicken Sie auf das Aktivitätsmenü.
3. Klicken Sie im Menü auf **Abonnement verknüpfen**.



4. Wählen Sie ein Abonnement aus der Down-Liste aus, oder klicken Sie auf **Abonnement hinzufügen** und befolgen Sie die Schritte, um ein neues Abonnement zu erstellen.

► https://docs.netapp.com/de-de/occm38//media/video_subscribing_aws.mp4 (video)

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.