



Fügen Sie einer S3-fähigen SVM Storage-Kapazität hinzu

ONTAP 9

NetApp
April 24, 2024

Inhalt

- Fügen Sie einer S3-fähigen SVM Storage-Kapazität hinzu 1
 - Erstellen eines Buckets 1
 - Erstellung eines Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration 5
 - Erstellen einer Bucket-Lifecycle-Management-Regel 9
 - Erstellen eines S3-Benutzers 13
 - Erstellen oder Ändern von S3-Gruppen 14
 - Schlüssel neu generieren und Aufbewahrungsfrist ändern 15

Fügen Sie einer S3-fähigen SVM Storage-Kapazität hinzu

Erstellen eines Buckets

S3 Objekte werden in *Buckets* aufbewahrt. Sie sind nicht als Dateien innerhalb eines Verzeichnisses in anderen Verzeichnissen verschachtelt.

Bevor Sie beginnen

Eine Storage-VM mit einem S3-Server muss bereits vorhanden sein.

Über diese Aufgabe

- Ab ONTAP 9.14.1 wurde die automatische Größenanpassung bei S3 FlexGroup Volumes beim Erstellen von Buckets aktiviert. So wird bei der Bucket-Erstellung auf vorhandenen und neuen FlexGroup Volumes keine übermäßige Kapazitätzuweisung mehr erreicht. Die Größe von FlexGroup Volumes wird anhand der folgenden Richtlinien auf die erforderliche Mindestgröße angepasst. Die erforderliche Mindestgröße ist die Gesamtgröße aller S3-Buckets in einem FlexGroup Volume.
 - Ab ONTAP 9.14.1 wird das FlexGroup Volume mit der minimal erforderlichen Größe erstellt, wenn ein S3-FlexGroup-Volume als Teil einer neuen Bucket-Erstellung erstellt wird.
 - Wenn ein S3-FlexGroup-Volume vor ONTAP 9.14.1 erstellt wurde, wird beim ersten, nach ONTAP 9.14.1 erstellten oder gelöschten Bucket das FlexGroup-Volume auf die minimal erforderliche Größe angepasst.
 - Wenn ein S3-FlexGroup-Volume vor ONTAP 9.14.1 erstellt wurde und bereits über die erforderliche Mindestgröße verfügt, bleibt beim Erstellen oder Löschen eines Buckets nach ONTAP 9.14.1 die Größe des S3-FlexGroup-Volumes erhalten.
- Storage-Service-Level sind vordefinierte Richtliniengruppen mit adaptiver Quality of Service (QoS) mit Standardeinstellungen wie *Value*, *Performance_* und *extreme*. Anstelle eines der standardmäßigen Storage-Service-Level können Sie auch eine individuelle QoS-Richtliniengruppe definieren und auf einen Bucket anwenden. Weitere Informationen zu Speicherservicedefinitionen finden Sie unter ["Definitionen von Storage-Services"](#). Weitere Informationen zum Leistungsmanagement finden Sie unter ["Performance Management"](#). Ab ONTAP 9.8 ist bei der Bereitstellung von Storage QoS standardmäßig aktiviert. Sie können die QoS deaktivieren oder während des Bereitstellungsprozesses oder zu einem späteren Zeitpunkt eine individuelle QoS-Richtlinie auswählen.
- Wenn Sie lokales Kapazitäts-Tiering konfigurieren, erstellen Sie Buckets und Benutzer in einer Daten-Storage-VM und nicht in der System-Storage-VM, auf der sich der S3 Server befindet.
- Für den Remote-Client-Zugriff müssen Sie Buckets in einer S3-fähigen Storage-VM konfigurieren. Wenn Sie einen Bucket in einer Storage-VM erstellen, die nicht S3-aktiviert ist, ist dieser nur für lokales Tiering verfügbar.
- Ab ONTAP 9.14.1 ist dies möglich ["Erstellung eines Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration"](#).
- Wenn Sie für die CLI einen Bucket erstellen, haben Sie zwei Bereitstellungsoptionen:
 - Lassen Sie ONTAP Select die zugrunde liegenden Aggregate und FlexGroup Komponenten (Standard)
 - ONTAP erstellt und konfiguriert ein FlexGroup-Volume für den ersten Bucket durch die automatische Auswahl der Aggregate. Er wählt automatisch das höchste Service-Level aus, das für Ihre Plattform verfügbar ist, oder Sie können das Storage-Service-Level angeben. Alle zusätzlichen Buckets, die Sie später in der Storage-VM hinzufügen, verfügen über dasselbe zugrunde liegende

FlexGroup Volume.

- Alternativ können Sie angeben, ob der Bucket für das Tiering verwendet wird. In diesem Fall versucht ONTAP, kostengünstige Medien mit optimaler Performance für die Tiered-Daten auszuwählen.
- Zudem wählen Sie die zugrunde liegenden Aggregate und FlexGroup-Komponenten aus (Optionen mit Advanced Privilege-Befehlen erforderlich): Sie können die Aggregate, auf denen der Bucket und das zugehörige FlexGroup Volume erstellt werden sollen, manuell auswählen und dann die Anzahl der Komponenten in jedem Aggregat angeben. Beim Hinzufügen weiterer Buckets:
 - Wenn Sie Aggregate und Komponenten für einen neuen Bucket angeben, wird für den neuen Bucket eine neue FlexGroup erstellt.
 - Wenn Sie keine Aggregate und Komponenten für einen neuen Bucket angeben, wird der neue Bucket zu einem vorhandenen FlexGroup hinzugefügt. Siehe [Management von FlexGroup Volumes](#) Finden Sie weitere Informationen.

Wenn bei der Erstellung eines Buckets Aggregate und Komponenten angegeben werden, werden keine QoS-Richtliniengruppen oder Benutzerdefiniert angewendet. Dies können Sie später mit dem `tun vserver object-store-server bucket modify` Befehl.

Siehe "[vserver Objekt-Store-Server Bucket ändern](#)" Finden Sie weitere Informationen.

Hinweis: Wenn Sie Eimer von Cloud Volumes ONTAP bedienen, sollten Sie das CLI-Verfahren verwenden. Es wird dringend empfohlen, die zugrunde liegenden Aggregate manuell auszuwählen, um sicherzustellen, dass sie nur einen Node verwenden. Die Verwendung von Aggregaten beider Nodes kann sich auf die Performance auswirken, da die Nodes sich in geografisch getrennten Verfügbarkeitszonen befinden und daher anfällig für Latenzprobleme sind.

Erstellen von S3 Buckets mit der ONTAP-CLI

1. Wenn Sie Aggregate und FlexGroup Komponenten selbst auswählen möchten, setzen Sie die Berechtigungsebene auf „Advanced“ (ansonsten reicht die Admin-Berechtigungsebene aus): `set -privilege advanced`
2. Erstellen eines Buckets:

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

Der Name der Storage VM kann entweder eine Daten-Storage-VM oder sein Cluster (Der Name der System-Storage-VM), wenn Sie lokales Tiering konfigurieren.

Wenn Sie keine Optionen angeben, erstellt ONTAP einen Bucket mit 800 GB mit dem Service Level auf das höchste für das System verfügbare Level.

Wenn ONTAP einen Bucket auf Basis der Performance oder Auslastung erstellen soll, verwenden Sie eine der folgenden Optionen:

- Service-Level

Nehmen Sie die auf `-storage-service-level` Option mit einem der folgenden Werte: `value`, `performance`, Oder `extreme`.

- tiering

Nehmen Sie die auf `-used-as-capacity-tier true` Option.

Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, verwenden Sie die folgenden Optionen:

- Der `-aggr-list` Der Parameter gibt die Liste der Aggregate an, die für FlexGroup Volume-Komponenten verwendet werden sollen.

Jeder Eintrag in der Liste erstellt eine Komponente im angegebenen Aggregat. Sie können ein Aggregat mehrmals angeben, damit mehrere Komponenten auf dem Aggregat erstellt werden.

Für eine konsistente Performance im FlexGroup Volume müssen alle Aggregate denselben Festplattentyp und dieselbe Konfiguration der RAID-Gruppen verwenden.

- Der `-aggr-list-multiplier` Parameter gibt die Anzahl der Wiederholungen über die Aggregate an, die mit dem aufgeführt sind `-aggr-list` Parameter beim Erstellen eines FlexGroup-Volumes.

Der Standardwert des `-aggr-list-multiplier` Der Parameter ist 4.

3. Fügen Sie bei Bedarf eine QoS-Richtliniengruppe hinzu:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
-group qos_policy_group
```

4. Überprüfen der Bucket-Erstellung:

```
vserver object-store-server bucket show [-instance]
```

Beispiel

Im folgenden Beispiel wird ein Bucket für Storage-VM erstellt `vs1` Der Größe 1TB Und Angabe des Aggregats:

```
cluster-1::*> vserver object-store-server bucket create -vserver
svm1.example.com -bucket testbucket -aggr-list aggr1 -size 1TB
```

Erstellung von S3 Buckets mit System Manager

1. Fügen Sie auf einer S3-fähigen Storage-VM einen neuen Bucket hinzu.

- Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
- Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.
 - Wenn Sie an dieser Stelle auf **Speichern** klicken, wird ein Bucket mit den folgenden Standardeinstellungen erstellt:
 - Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, bereits Gruppenrichtlinien sind gültig.



Sie sollten den S3-Root-Benutzer nicht zum Managen von ONTAP-Objekt-Storage und zur gemeinsamen Nutzung seiner Berechtigungen verwenden, da er unbegrenzten Zugriff auf den Objektspeicher hat. Erstellen Sie stattdessen einen Benutzer oder eine Gruppe mit Administratorrechten, die Sie zuweisen.

- Das Niveau der Servicequalität (Performance) ist das höchste für Ihr System verfügbare Niveau.
- Klicken Sie auf **Speichern**, um einen Bucket mit diesen Standardwerten zu erstellen.

Konfigurieren Sie zusätzliche Berechtigungen und Einschränkungen

Sie können auf **Weitere Optionen** klicken, um Einstellungen für Objektspernung, Benutzerberechtigungen und Leistungslevel zu konfigurieren, wenn Sie den Bucket konfigurieren, oder Sie können diese Einstellungen später ändern.

Wenn Sie beabsichtigen, den S3-Objektspeicher für FabricPool Tiering zu nutzen, sollten Sie die Wahl erwägen **für Tiering** zu verwenden (kostengünstige Medien mit optimaler Performance für die Tiered Data verwenden) anstatt ein Performance-Service-Level.

Wenn Sie die Versionierung für Ihre Objekte für eine spätere Wiederherstellung aktivieren möchten, wählen Sie **Versionierung aktivieren**. Die Versionierung ist standardmäßig aktiviert, wenn Sie die Objektspernung auf dem Bucket aktivieren. Informationen zur Objektversionierung finden Sie im ["Verwenden von Versionierung in S3 Buckets für Amazon"](#).

Ab Version 9.14.1 wird die Objektspernung in S3 Buckets unterstützt. Für die S3 Objektspernung ist eine standardmäßige SnapLock-Lizenz erforderlich. Diese Lizenz ist in enthalten ["ONTAP One"](#). Vor ONTAP One war die SnapLock-Lizenz im Paket für Sicherheit und Compliance enthalten. Das Paket „Sicherheit und Compliance“ wird nicht mehr angeboten, ist aber weiterhin gültig. Bestehende Kunden können diese Option wählen, obwohl sie derzeit nicht benötigt werden ["Upgrade auf ONTAP One"](#). Wenn Sie die Objektspernung für einen Bucket aktivieren, sollten Sie dies tun ["Vergewissern Sie sich, dass eine SnapLock-Lizenz installiert ist"](#). Wenn keine SnapLock-Lizenz installiert ist, müssen Sie dies tun ["Installieren"](#) Bevor Sie die Objektspernung aktivieren können. Wenn Sie die Installation der SnapLock-Lizenz überprüft haben, wählen Sie **enable object locking** aus, um Objekte in Ihrem Bucket vor dem Löschen oder Überschreiben zu schützen. Die Sperrung kann entweder für alle oder für bestimmte Objektversionen aktiviert werden und nur dann, wenn die SnapLock-Compliance-Uhr für die Cluster-Nodes initialisiert wird. Führen Sie hierzu folgende Schritte aus:

1. Wenn die SnapLock-Compliance-Uhr auf keinem Knoten des Clusters initialisiert wird, wird die Schaltfläche **SnapLock-Compliance-Uhr initialisieren** angezeigt. Klicken Sie auf **SnapLock-Compliance-Uhr initialisieren**, um die SnapLock-Compliance-Uhr auf den Clusterknoten zu initialisieren.
2. Wählen Sie den Modus **Governance**, um eine zeitbasierte Sperre zu aktivieren, die *Write Once, Read Many (WORM)* Berechtigungen für die Objekte erlaubt. Selbst im *Governance*-Modus können die Objekte von Administratorbenutzern mit bestimmten Berechtigungen gelöscht werden.
3. Wählen Sie **Compliance**-Modus, wenn Sie strengere Regeln für die Löschung und Aktualisierung der Objekte zuweisen möchten. In diesem Modus der Objektspernung können die Objekte nur nach Abschluss der angegebenen Aufbewahrungsfrist abgelaufen sein. Sofern keine Aufbewahrungsfrist festgelegt ist, bleiben die Objekte unbegrenzt gesperrt.
4. Geben Sie die Aufbewahrungsfrist für die Sperre in Tagen oder Jahren an, wenn die Verriegelung für einen bestimmten Zeitraum wirksam sein soll.



Das Sperren gilt für S3-Buckets mit Versionsangabe und ohne Versionsangabe. Objektspernung gilt nicht für NAS-Objekte.

Sie können Sicherungs- und Berechtigungseinstellungen sowie Performance Service Level für den Bucket konfigurieren.



Sie müssen bereits Benutzer und Gruppen erstellt haben, bevor Sie die Berechtigungen konfigurieren.

Weitere Informationen finden Sie unter ["Spiegelung für neuen Bucket erstellen"](#).

Überprüfen Sie den Zugriff auf den Bucket

Für S3-Client-Applikationen (ob ONTAP S3 oder eine externe Drittanbieterapplikation) können Sie Ihren Zugriff auf den neu erstellten Bucket überprüfen, indem Sie Folgendes eingeben:

- Das S3-Server-CA-Zertifikat.
- Der Zugriffsschlüssel und der geheime Schlüssel des Benutzers.
- Der FQDN-Name des S3-Servers und der Bucket-Name.

Erstellung eines Buckets auf einem gespiegelten oder nicht gespiegelten Aggregat in einer MetroCluster Konfiguration

Ab ONTAP 9.14.1 können Sie einen Bucket auf einem gespiegelten oder nicht gespiegelten Aggregat in MetroCluster FC- und IP-Konfigurationen bereitstellen.

Über diese Aufgabe

- Standardmäßig werden Buckets für gespiegelte Aggregate bereitgestellt.
- Dieselben Bereitstellungsrichtlinien wie in beschrieben ["Erstellen eines Buckets"](#) Anwenden bei der Erstellung eines Buckets in einer MetroCluster-Umgebung.
- Die folgenden S3-Objekt-Storage-Funktionen werden in MetroCluster Umgebungen **nicht** unterstützt:
 - S3 SnapMirror
 - S3 Bucket-Lifecycle-Management
 - S3-Objektsperre im **Compliance**-Modus



S3-Objektsperre im **Governance**-Modus wird unterstützt.

- Lokales FabricPool Tiering

Bevor Sie beginnen

Eine SVM, die einen S3-Server enthält, muss bereits vorhanden sein.

Erstellung von Buckets wird verarbeitet

CLI

1. Wenn Sie Aggregate und FlexGroup Komponenten selbst auswählen möchten, setzen Sie die Berechtigungsebene auf „Advanced“ (ansonsten reicht die Admin-Berechtigungsebene aus): `set -privilege advanced`
2. Erstellen eines Buckets:

```
vserver object-store-server bucket create -vserver <svm_name> -bucket  
<bucket_name> [-size integer[KB|MB|GB|TB|PB]] [-use-mirrored-aggregates  
true/false]
```

Stellen Sie die ein `-use-mirrored-aggregates` Option auf `true` Oder `false` Je nachdem, ob Sie ein gespiegeltes oder nicht gespiegeltes Aggregat verwenden möchten.



Standardmäßig wird der verwendet `-use-mirrored-aggregates` Die Option ist auf festgelegt `true`.

- Der SVM-Name muss eine Daten-SVM sein.
- Wenn Sie keine Optionen angeben, erstellt ONTAP einen Bucket mit 800 GB mit dem Service Level auf das höchste für das System verfügbare Level.
- Wenn ONTAP einen Bucket auf Basis der Performance oder Auslastung erstellen soll, verwenden Sie eine der folgenden Optionen:

- **Service-Level**

Nehmen Sie die auf `-storage-service-level` Option mit einem der folgenden Werte: `value`, `performance`, Oder `extreme`.

- **tiering**

Nehmen Sie die auf `-used-as-capacity-tier true` Option.

- Wenn Sie die Aggregate angeben möchten, auf denen das zugrunde liegende FlexGroup Volume erstellt werden soll, verwenden Sie die folgenden Optionen:
 - Der `-aggr-list` Der Parameter gibt die Liste der Aggregate an, die für FlexGroup Volume-Komponenten verwendet werden sollen.

Jeder Eintrag in der Liste erstellt eine Komponente im angegebenen Aggregat. Sie können ein Aggregat mehrmals angeben, damit mehrere Komponenten auf dem Aggregat erstellt werden.

Für eine konsistente Performance im FlexGroup Volume müssen alle Aggregate denselben Festplattentyp und dieselbe Konfiguration der RAID-Gruppen verwenden.

- Der `-aggr-list-multiplier` Parameter gibt die Anzahl der Wiederholungen über die Aggregate an, die mit dem aufgeführt sind `-aggr-list` Parameter beim Erstellen eines FlexGroup-Volumes.

Der Standardwert des `-aggr-list-multiplier` Der Parameter ist 4.

3. Fügen Sie bei Bedarf eine QoS-Richtliniengruppe hinzu:

```
vserver object-store-server bucket modify -bucket bucket_name -qos-policy
```



```
-group qos_policy_group
```

4. Überprüfen der Bucket-Erstellung:

```
vserver object-store-server bucket show [-instance]
```

Beispiel

Im folgenden Beispiel wird ein Bucket für SVM vs1 mit der Größe 1 TB auf einem gespiegelten Aggregat erstellt:

```
cluster-1::*> vserver object-store-server bucket create -vserver  
svml.example.com -bucket testbucket -size 1TB -use-mirrored-aggregates  
true
```


System Manager

1. Fügen Sie auf einer S3-fähigen Storage-VM einen neuen Bucket hinzu.
 - a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
 - b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus und geben Sie eine Größe ein.

Standardmäßig wird der Bucket auf einem gespiegelten Aggregat bereitgestellt. Wenn Sie einen Bucket auf einem nicht gespiegelten Aggregat erstellen möchten, wählen Sie **Weitere Optionen** und deaktivieren Sie das Kontrollkästchen **Use the SyncMirror Tier** unter **Schutz** wie im folgenden Bild gezeigt:

Add bucket

NAME

 To use this bucket from a remote cluster, configure S3 service on storage VM "vs1".

FOLDER (OPTIONAL)

Browse

Specify the folder to map to this bucket. [Know more](#)

CAPACITY

Size

GB

☐ Use tiering
If you select this option, the system will try to select low-cost media with optimal performance for the tiered data.

☐ Enable versioning
Versioning-enabled buckets allow you to recover objects that were accidentally deleted or overwritten. After versioning is enabled, it can't be disabled. However, you can suspend versioning.

PERFORMANCE SERVICE LEVEL

Value

Not sure? [Get help selecting type](#)

Permissions

☐ Copy access permissions from an existing bucket

Principal	Effect	Actions	Resources	Conditions
All users of this stor...	allow	ListBucket	*	

+ Add

Object locking

☐ Enable object locking
Object locking utilizes the "Write Once, Read Many" (WORM) model in which objects or their versions are protected from being deleted or overwritten during the specified retention period.

Protection

☒ Use the S3x3lination feature

Save

Cancel

- Wenn Sie an dieser Stelle auf **Speichern** klicken, wird ein Bucket mit den folgenden Standardeinstellungen erstellt:

- Benutzern wird kein Zugriff auf den Bucket gewährt, es sei denn, bereits Gruppenrichtlinien sind gültig.



Sie sollten den S3-Root-Benutzer nicht zum Managen von ONTAP-Objekt-Storage und zur gemeinsamen Nutzung seiner Berechtigungen verwenden, da er unbegrenzten Zugriff auf den Objektspeicher hat. Erstellen Sie stattdessen einen Benutzer oder eine Gruppe mit Administratorrechten, die Sie zuweisen.

- Das Niveau der Servicequalität (Performance) ist das höchste für Ihr System verfügbare Niveau.

- Sie können auf **Weitere Optionen** klicken, um Benutzerberechtigungen und Leistungslevel zu konfigurieren, wenn Sie den Bucket konfigurieren, oder Sie können diese Einstellungen später ändern.
 - Sie müssen bereits Benutzer und Gruppen erstellt haben, bevor Sie **Weitere Optionen** verwenden, um ihre Berechtigungen zu konfigurieren.
 - Wenn Sie beabsichtigen, den S3-Objektspeicher für FabricPool Tiering zu nutzen, sollten Sie die Wahl erwägen **für Tiering** zu verwenden (kostengünstige Medien mit optimaler Performance für die Tiered Data verwenden) anstatt ein Performance-Service-Level.
- 2. Überprüfen Sie bei S3-Client-Applikationen – einem anderen ONTAP System oder einer externen App von Drittanbietern – den Zugriff auf den neuen Bucket, indem Sie Folgendes eingeben:
 - Das S3-Server-CA-Zertifikat.
 - Der Zugriffsschlüssel und der Geheimschlüssel des Benutzers.
 - Der FQDN-Name des S3-Servers und der Bucket-Name.

Erstellen einer Bucket-Lifecycle-Management-Regel

Ab ONTAP 9.13.1 können Sie Lifecycle-Managementregeln erstellen, um Objekt-Lebenszyklen in Ihren S3 Buckets zu managen. Sie können Löschregeln für bestimmte Objekte in einem Bucket definieren und diese Bucket-Objekte durch diese Regeln ablaufen lassen. So können Sie Datenhaltungsanforderungen erfüllen und den gesamten S3 Objekt-Storage effizient managen.



Wenn die Objektsperre für Ihre Bucket-Objekte aktiviert ist, werden die Lifecycle-Management-Regeln für die Objektablauffrist nicht auf gesperrte Objekte angewendet. Informationen zur Objektsperre finden Sie unter "[Erstellen eines Buckets](#)".

Bevor Sie beginnen

Eine S3-fähige SVM mit einem S3-Server und einem Bucket muss bereits vorhanden sein. Siehe "[Erstellung einer SVM für S3](#)". Finden Sie weitere Informationen.

Über diese Aufgabe

Beim Erstellen von Lifecycle-Management-Regeln können Sie die folgenden Löschaktionen auf Ihre Bucket-Objekte anwenden:

- Löschen aktueller Versionen – Diese Aktion läuft Objekte ab, die durch die Regel identifiziert werden. Wenn die Versionierung auf dem Bucket aktiviert ist, sind alle abgelaufenen Objekte in S3 nicht verfügbar. Wenn die Versionierung nicht aktiviert ist, werden die Objekte durch diese Regel dauerhaft gelöscht. Die CLI-Aktion ist `Expiration`.
- Löschen nicht aktueller Versionen – Diese Aktion gibt an, wann S3 nicht aktuelle Objekte dauerhaft entfernen kann. Die CLI-Aktion ist `NoncurrentVersionExpiration`.
- Löschen abgelaufener Löschmarkierungen - Diese Aktion löscht abgelaufene Löschmarkierungen von Objekten. In versionierungsfähigen Buckets werden Objekte mit Löschmarkierungen zu den aktuellen Versionen der Objekte. Die Objekte werden nicht gelöscht, und es kann keine Aktion für sie ausgeführt werden. Diese Objekte sind abgelaufen, wenn ihnen keine aktuellen Versionen zugeordnet sind. Die CLI-Aktion ist `Expiration`.
- Löschen von unvollständigen mehrteiligen Uploads: Mit dieser Aktion wird die maximale Zeit (in Tagen)

festgelegt, die Sie zulassen möchten, dass mehrteilige Uploads noch ausgeführt werden. Danach werden sie gelöscht. Die CLI-Aktion ist `AbortIncompleteMultipartUpload`.

Die Vorgehensweise, die Sie befolgen, hängt von der verwendeten Schnittstelle ab. Bei ONTAP 9.13,1 müssen Sie die CLI verwenden. Ab ONTAP 9.14.1 können Sie auch System Manager verwenden.

Verwalten Sie Lifecycle Management-Regeln mit der CLI

Ab ONTAP 9.13.1 können Sie über die ONTAP CLI Lifecycle-Managementregeln erstellen, um Objekte in Ihren S3 Buckets ablaufen zu lassen.

Bevor Sie beginnen

Für die CLI müssen Sie die erforderlichen Felder für jeden Ablaufaktionstyp definieren, wenn Sie eine Bucket-Lebenszyklusverwaltungsregel erstellen. Diese Felder können nach der ersten Erstellung geändert werden. In der folgenden Tabelle werden die eindeutigen Felder für jeden Aktionstyp angezeigt.

Aktionstyp	Eindeutige Felder
NichtCurrentVersionAblauf	<ul style="list-style-type: none">• <code>-non-curr-days</code> - Anzahl der Tage, nach denen nicht aktuelle Versionen gelöscht werden• <code>-new-non-curr-versions</code> - Anzahl der neuesten nicht-aktuellen Versionen, die beibehalten werden sollen
Ablauf	<ul style="list-style-type: none">• <code>-obj-age-days</code> - Anzahl der Tage seit der Erstellung, nach denen die aktuelle Version der Objekte gelöscht werden kann• <code>-obj-exp-date</code> - Bestimmtes Datum, wann die Objekte ablaufen sollen• <code>-expired-obj-del-markers</code> - Löschen von Objektmarkierungen
AbortInsetteMultipartUpload	<ul style="list-style-type: none">• <code>-after-initiation-days</code> - Anzahl der Tage der Initiierung, nach denen der Upload abgebrochen werden kann

Damit die Bucket-Lifecycle-Management-Regel nur auf eine bestimmte Untergruppe von Objekten angewendet werden kann, müssen Administratoren beim Erstellen der Regel jeden Filter festlegen. Wenn diese Filter beim Erstellen der Regel nicht festgelegt werden, wird die Regel auf alle Objekte innerhalb des Buckets angewendet.

Alle Filter können nach der ersten Erstellung geändert werden *außer* für Folgendes:

- `-prefix`
- `-tags`
- `-obj-size-greater-than`
- `-obj-size-less-than`

Schritte

1. Verwenden Sie die `vserver object-store-server bucket lifecycle-management-rule create` Befehl mit den erforderlichen Feldern für Ihren Ablaufaktionstyp, um Ihre Bucket-Lifecycle-Management-Regel zu erstellen.

Beispiel

Mit dem folgenden Befehl wird eine Lebenszyklusverwaltungsregel für den Bucket „NonCurrentVersionExpiration“ erstellt:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
NonCurrentVersionExpiration -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -new-non-curr-versions <integer> -non-curr
-days <integer>
```

Beispiel

Mit dem folgenden Befehl wird eine Management-Regel für AblaufBucket-Lebenszyklus erstellt:

```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
Expiration -index <lifecycle_rule_index_integer> -is-enabled {true|false}
-prefix <object_name> -tags <text> -obj-size-greater-than
{<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -obj-age-days <integer> -obj-exp-date
<"MM/DD/YYYY HH:MM:SS"> -expired-obj-del-marker {true|false}
```

Beispiel

Mit dem folgenden Befehl wird eine AbortIncompleteMultipartUpload Bucket Lifecycle Management-Regel erstellt:


```
vserver object-store-server bucket lifecycle-management-rule create
-vserver <svm_name> -bucket <bucket_name> -rule-id <rule_name> -action
AbortIncompleteMultipartUpload -index <lifecycle_rule_index_integer> -is
-enabled {true|false} -prefix <object_name> -tags <text> -obj-size-greater
-than {<integer>[KB|MB|GB|TB|PB]} -obj-size-less-than
{<integer>[KB|MB|GB|TB|PB]} -after-initiation-days <integer>
```


Managen Sie Lifecycle Management-Regeln mit System Manager

Ab ONTAP 9.14.1 können Sie S3 Objekte mit System Manager ablaufen lassen. Sie können Lifecycle-Management-Regeln für Ihre S3-Objekte hinzufügen, bearbeiten und löschen. Darüber hinaus können Sie eine für einen Bucket erstellte Lebenszyklusregel importieren und für die Objekte in einem anderen Bucket nutzen. Sie können eine aktive Regel deaktivieren und später aktivieren.

Fügen Sie eine Lebenszyklusverwaltungsregel hinzu


1. Klicken Sie Auf **Speicher > Buckets**.

2. Wählen Sie den Bucket aus, für den Sie die Ablaufregel festlegen möchten.
3. Klicken Sie auf das  Und wählen Sie **Lebenszyklusregeln verwalten**.
4. Klicken Sie auf **Hinzufügen > Lebenszyklusregel**.
5. Fügen Sie auf der Seite Lebenszyklusregel hinzufügen den Namen der Regel hinzu.
6. Definieren Sie den Geltungsbereich der Regel, unabhängig davon, ob sie auf alle Objekte im Bucket oder auf bestimmte Objekte angewendet werden soll. Wenn Sie Objekte angeben möchten, fügen Sie mindestens eines der folgenden Filterkriterien hinzu:
 - a. **Präfix:** Geben Sie ein Präfix der Objektschlüsselnamen an, auf die die Regel angewendet werden soll. Normalerweise handelt es sich um den Pfad oder Ordner des Objekts. Sie können pro Regel ein Präfix eingeben. Sofern kein gültiges Präfix angegeben wird, gilt die Regel für alle Objekte in einem Bucket.
 - b. **Tags:** Geben Sie bis zu drei Schlüssel- und Wertpaare (Tags) für die Objekte an, auf die die Regel angewendet werden soll. Zum Filtern werden nur gültige Schlüssel verwendet. Der Wert ist optional. Wenn Sie jedoch Werte hinzufügen, stellen Sie sicher, dass Sie nur gültige Werte für die entsprechenden Schlüssel hinzufügen.
 - c. **Größe:** Sie können den Umfang zwischen der minimalen und maximalen Größe der Objekte begrenzen. Sie können einen oder beide Werte eingeben. Die Standardeinheit ist MiB.
7. Geben Sie die Aktion an:
 - a. **Die aktuelle Version von Objekten ablaufen lassen:** Legen Sie eine Regel fest, um alle aktuellen Objekte nach einer bestimmten Anzahl von Tagen seit ihrer Erstellung oder an einem bestimmten Datum dauerhaft nicht mehr verfügbar zu machen. Diese Option ist nicht verfügbar, wenn die Option **Delete Expired object delete Markers** ausgewählt ist.
 - b. **Nicht aktuelle Versionen dauerhaft löschen:** Geben Sie die Anzahl der Tage an, nach denen die Version nicht aktuell wird, und danach kann gelöscht werden, und die Anzahl der zu haltenden Versionen.
 - c. **Löschen abgelaufener Objektlösch-Marker:** Wählen Sie diese Aktion, um Objekte mit abgelaufenen Löschmarkierungen zu löschen, d.h. Marker ohne zugeordnetes aktuelles Objekt zu löschen.



Diese Option ist nicht mehr verfügbar, wenn Sie die Option **die aktuelle Version von Objekten ablaufen lassen** auswählen, die automatisch alle Objekte nach der Aufbewahrungsfrist löscht. Diese Option ist auch nicht mehr verfügbar, wenn Objekt-Tags zum Filtern verwendet werden.
- d. **Unvollständige mehrteilige Uploads löschen:** Legen Sie die Anzahl der Tage fest, nach denen unvollständige mehrteilige Uploads gelöscht werden sollen. Wenn die mehrteiligen Uploads, die gerade ausgeführt werden, innerhalb der angegebenen Aufbewahrungsfrist fehlschlagen, können Sie die unvollständigen mehrteiligen Uploads löschen. Diese Option ist nicht mehr verfügbar, wenn Objekt-Tags zum Filtern verwendet werden.
- e. Klicken Sie Auf **Speichern**.

Lebenszyklusregel importieren

1. Klicken Sie Auf **Speicher > Buckets**.
2. Wählen Sie den Bucket aus, für den Sie die Ablaufregel importieren möchten.
3. Klicken Sie auf das  Und wählen Sie **Lebenszyklusregeln verwalten**.
4. Klicken Sie auf **Hinzufügen > Regel importieren**.
5. Wählen Sie den Bucket aus, aus dem Sie die Regel importieren möchten. Die für den ausgewählten

Bucket definierten Lifecycle-Management-Regeln werden angezeigt.

6. Wählen Sie die Regel aus, die Sie importieren möchten. Sie haben die Möglichkeit, jeweils eine Regel auszuwählen, wobei die Standardauswahl die erste Regel ist.
7. Klicken Sie Auf **Import**.

Bearbeiten, löschen oder deaktivieren Sie eine Regel

Sie können nur die Lifecycle-Management-Aktionen bearbeiten, die der Regel zugeordnet sind. Wenn die Regel mit Objekt-Tags gefiltert wurde, stehen die Optionen **abgelaufene Objekte löschen** **Marker** und **unvollständige mehrteilige Uploads löschen** nicht zur Verfügung.

Wenn Sie eine Regel löschen, gilt diese Regel nicht mehr für zuvor zugeordnete Objekte.

1. Klicken Sie Auf **Speicher > Buckets**.
2. Wählen Sie den Bucket aus, für den Sie die Lifecycle-Management-Regel bearbeiten, löschen oder deaktivieren möchten.
3. Klicken Sie auf das **:** Und wählen Sie **Lebenszyklusregeln verwalten**.
4. Wählen Sie die gewünschte Regel aus. Sie können jeweils eine Regel bearbeiten und deaktivieren. Sie können mehrere Regeln auf einmal löschen.
5. Wählen Sie **Bearbeiten**, **Löschen** oder **Deaktivieren**, und schließen Sie das Verfahren ab.

Erstellen eines S3-Benutzers

Für alle ONTAP-Objektspeicher ist eine Benutzerautorisierung erforderlich, um die Konnektivität zu autorisierten Clients einzuschränken.

Bevor Sie beginnen.

Eine S3-fähige Storage-VM muss bereits vorhanden sein.

Über diese Aufgabe

Ein S3-Benutzer kann Zugriff auf jeden Bucket in einer Storage-VM erhalten. Wenn Sie einen S3-Benutzer erstellen, werden auch ein Zugriffsschlüssel und ein geheimer Schlüssel für den Benutzer generiert. Sie sollten zusammen mit dem FQDN des Objektspeichers und dem Bucket-Namen für den Benutzer freigegeben werden. Die Schlüssel eines S3-Benutzers können mit dem angezeigt werden `vserver object-store-server user show` Befehl.

Sie können S3 Benutzern in einer Bucket-Richtlinie oder einer Objekt-Server-Richtlinie spezifische Zugriffsberechtigungen zuweisen.



Wenn Sie einen neuen Objektspeicher-Server erstellen, erstellt ONTAP einen Root-Benutzer (UID 0), ein privilegierter Benutzer mit Zugriff auf alle Buckets. Anstatt ONTAP S3 als Root-Benutzer zu verwalten, empfiehlt NetApp, eine Admin-Benutzerrolle mit bestimmten Berechtigungen zu erstellen.

CLI

1. S3-Benutzer erstellen:

```
vserver object-store-server user create -vserver svm_name -user user_name  
-comment [-comment text] -key-time-to-live time
```


- Das Hinzufügen eines Kommentars ist optional.
- Ab ONTAP 9.14.1 können Sie den Zeitraum festlegen, für den der Schlüssel gültig sein wird -key-time-to-live Parameter. Sie können den Aufbewahrungszeitraum in diesem Format hinzufügen, um den Zeitraum anzugeben, nach dem der Zugriffsschlüssel abläuft:
P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W
Wenn Sie beispielsweise eine Aufbewahrungsfrist von einem Tag, zwei Stunden, drei Minuten und vier Sekunden eingeben möchten, geben Sie den Wert als P1DT2H3M4S. Sofern nicht angegeben, ist der Schlüssel für einen unbestimmten Zeitraum gültig.

Im folgenden Beispiel wird ein Benutzer mit dem Namen erstellt `sm_user1` Auf Storage-VM `vs0`, Mit einer Schlüsselaufbewahrungsfrist von einer Woche.

```
vserver object-store-server user create -vserver vs0 -user sm_user1  
-key-time-to-live P1W
```

2. Achten Sie darauf, den Zugriffsschlüssel und den geheimen Schlüssel zu speichern. Sie werden für den Zugriff von S3-Clients benötigt.

System Manager

1. Klicken Sie auf **Storage > Storage VMs**. Wählen Sie die Speicher-VM aus, zu der Sie einen Benutzer hinzufügen möchten, wählen Sie **Einstellungen** und klicken Sie dann auf  Unter S3.
2. Um einen Benutzer hinzuzufügen, klicken Sie auf **Benutzer > Hinzufügen**.
3. Geben Sie einen Namen für den Benutzer ein.
4. Ab ONTAP 9.14.1 können Sie den Aufbewahrungszeitraum der Zugriffsschlüssel festlegen, die für den Benutzer erstellt werden. Sie können den Aufbewahrungszeitraum in Tagen, Stunden, Minuten oder Sekunden angeben, nach denen die Schlüssel automatisch ablaufen. Standardmäßig ist der Wert auf festgelegt 0 Das bedeutet, dass der Schlüssel unbegrenzt gültig ist.
5. Klicken Sie Auf **Speichern**. Der Benutzer wird erstellt, und ein Zugriffsschlüssel und ein geheimer Schlüssel werden für den Benutzer generiert.
6. Laden Sie den Zugriffsschlüssel und den geheimen Schlüssel herunter, oder speichern Sie ihn. Sie werden für den Zugriff von S3-Clients benötigt.

Nächste Schritte

- [Erstellen oder Ändern von S3-Gruppen](#)

Erstellen oder Ändern von S3-Gruppen

Sie können den Bucket-Zugriff vereinfachen, indem Sie Benutzergruppen mit entsprechenden Zugriffsberechtigungen erstellen.

Bevor Sie beginnen

S3-Benutzer in einer S3-fähigen SVM müssen bereits vorhanden sein.

Über diese Aufgabe

Benutzern in einer S3-Gruppe kann Zugriff auf jeden Bucket in einer SVM, nicht aber auf mehrere SVMs gewährt werden. Gruppenzugriffsberechtigungen können auf zwei Arten konfiguriert werden:


- Auf Bucket-Ebene

Nachdem Sie eine Gruppe von S3-Benutzern erstellt haben, geben Sie in den Bucket-Richtlinienerklärungen Gruppenberechtigungen an, die nur auf diesen Bucket angewendet werden.

- Auf SVM-Ebene

Nach dem Erstellen einer Gruppe von S3-Benutzern geben Sie in der Gruppendefinition die Namen der Objektspeicherrichtlinien an. Diese Richtlinien bestimmen die Buckets und den Zugriff für die Gruppenmitglieder.

System Manager

1. Bearbeiten Sie den Speicher-VM: Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf  Unter S3.
2. Fügen Sie eine Gruppe hinzu: Wählen Sie **Gruppen** und dann **Hinzufügen**.
3. Geben Sie einen Gruppennamen ein, und wählen Sie aus einer Benutzerliste aus.
4. Sie können eine vorhandene Gruppenrichtlinie auswählen oder eine jetzt hinzufügen oder später eine Richtlinie hinzufügen.

CLI

1. Erstellen einer S3-Gruppe:

```
vserver object-store-server group create -vserver svm_name -name group_name  
-users user_name\(s\) [-policies policy_names] [-comment text\]`Der -  
policies Option kann in Konfigurationen mit nur einem Bucket in einem Objektspeicher  
weggelassen werden; der Gruppename kann der Bucket-Richtlinie hinzugefügt werden. Der  
-policies Option kann später mit der hinzugefügt werden vserver object-store-server  
group modify Befehl nach Erstellung der Objekt-Storage-Server-Richtlinien
```

Schlüssel neu generieren und Aufbewahrungsfrist ändern

Zugriffsschlüssel und geheime Schlüssel werden automatisch während der Erstellung von Benutzern generiert, um den S3-Client-Zugriff zu ermöglichen. Sie können Schlüssel für einen Benutzer neu generieren, wenn ein Schlüssel abgelaufen ist oder kompromittiert wurde.

Informationen zur Generierung von Zugriffsschlüsseln finden Sie unter ["Erstellen eines S3-Benutzers"](#).



CLI

1. Regenerieren Sie Zugriff und geheime Schlüssel für einen Benutzer, indem Sie den ausführen
`vserver object-store-server user regenerate-keys` **Befehl**.
2. Generierte Schlüssel sind standardmäßig für unbegrenzte Zeit gültig. Ab 9.14.1 können Sie die Aufbewahrungsfrist ändern, nach der die Schlüssel automatisch ablaufen. Sie können den Aufbewahrungszeitraum in diesem Format hinzufügen:
`P[<integer>D]T[<integer>H][<integer>M][<integer>S] | P<integer>W`
Wenn Sie beispielsweise eine Aufbewahrungsfrist von einem Tag, zwei Stunden, drei Minuten und vier Sekunden eingeben möchten, geben Sie den Wert als ein `P1DT2H3M4S`.

```
vserver object-store-server user regenerate-keys -vserver svm_name  
-user user -key-time-to-live 0
```

3. Speichern Sie den Zugriff und die geheimen Schlüssel. Sie werden für den Zugriff von S3-Clients benötigt.

System Manager

1. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
2. Klicken Sie auf der Registerkarte **Einstellungen** auf  In der Kachel **S3**.
3. Überprüfen Sie auf der Registerkarte **Users**, ob kein Zugriffsschlüssel vorhanden ist oder der Schlüssel für den Benutzer abgelaufen ist.
4. Wenn Sie den Schlüssel neu generieren möchten, klicken Sie auf  Klicken Sie neben dem Benutzer auf **Schlüssel neu generieren**.
5. Generierte Schlüssel sind standardmäßig für eine unbestimmte Zeit gültig. Ab 9.14.1 können Sie die Aufbewahrungsfrist ändern, nach der die Schlüssel automatisch ablaufen. Geben Sie den Aufbewahrungszeitraum in Tagen, Stunden, Minuten oder Sekunden ein.
6. Klicken Sie Auf **Speichern**. Der Schlüssel wird neu generiert. Jede Änderung der Schlüsselaufbewahrungsfrist tritt unmittelbar in Kraft.
7. Laden Sie den Zugriffsschlüssel und den geheimen Schlüssel herunter, oder speichern Sie ihn. Sie werden für den Zugriff von S3-Clients benötigt.

Copyright-Informationen

Copyright © 2024 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.