# Cluster verwalten

## Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/storage-mgmt/concept_how_discovery_process_works.html on November 13, 2026. Always check docs.netapp.com for the latest.

# Inhalt

Cluster verwalten . . . . . 1
Informationen zur Funktionsweise des Cluster-Erkennungsprozesses in Active IQ Unified Manager . . . . . 1
Liste der von Active IQ Unified Manager überwachten Cluster . . . . . 2
Cluster zu Active IQ Unified Manager hinzufügen . . . . . 2
Bearbeiten der Clustereinstellungen in Active IQ Unified Manager . . . . . 5
Entfernung von Clustern aus Active IQ Unified Manager . . . . . 5
Cluster in Active IQ Unified Manager erneut erkennen . . . . . 6

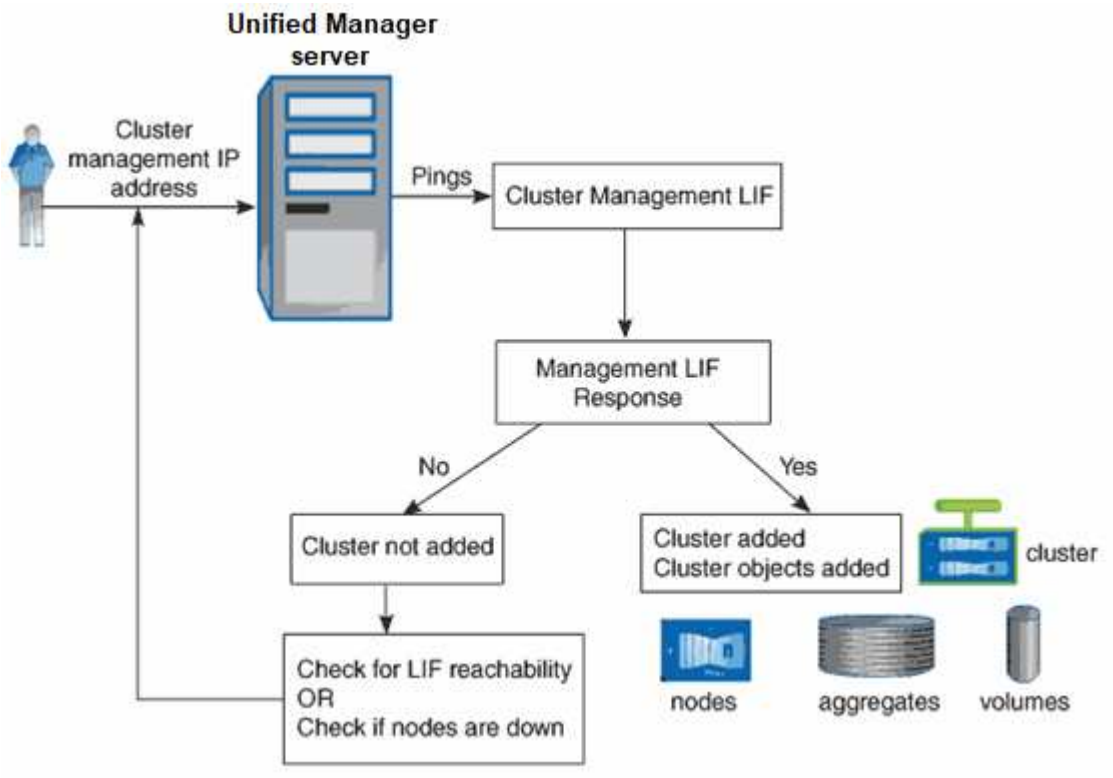
# Cluster verwalten

## Informationen zur Funktionsweise des Cluster-Erkennungsprozesses in Active IQ Unified Manager

Nachdem Sie einen Cluster zu Unified Manager hinzugefügt haben, erkennt der Server die Clusterobjekte und fügt sie seiner Datenbank hinzu. Das Verständnis der Funktionsweise dieses Erkennungsprozesses unterstützt Sie beim Managen der Cluster Ihres Unternehmens und ihrer Objekte.

Das Überwachungsintervall für die Erfassung von Clusterkonfigurationsinformationen beträgt 15 Minuten. Nachdem Sie beispielsweise einen Cluster hinzugefügt haben, dauert es 15 Minuten, bis die Clusterobjekte in der Unified Manager UI angezeigt werden. Dieser Zeitraum gilt auch für Änderungen an einem Cluster. Wenn Sie beispielsweise zwei neue Volumes zu einer SVM in einem Cluster hinzufügen, werden diese neuen Objekte nach dem nächsten Abfrageintervall, das bis zu 15 Minuten betragen kann, in der UI angezeigt.

Die folgende Abbildung veranschaulicht den Entdeckungsprozess:




Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Erfassung der Datenkontinuität gesammelt. Diese Funktion stellt Ihnen unmittelbar nach dem Hinzufügen eines Clusters Performance-Informationen für mehr als zwei Wochen zur Verfügung. Nach Abschluss des Erfassungszyklus für die Datenkontinuität werden standardmäßig alle fünf Minuten Echtzeit-Performance-Daten für den Cluster erfasst.

Da die Erfassung von 15 Tagen Performance-Daten CPU-intensiv ist, wird empfohlen, die Hinzufügung neuer Cluster zeitlich zu staffeln, damit die Abfragen zur Erfassung der

Datenkontinuität nicht gleichzeitig auf zu vielen Clustern ausgeführt werden.

# Liste der von Active IQ Unified Manager überwachten Cluster

Auf der Seite „Cluster Setup“ können Sie Ihre Clusterübersicht einsehen. Dort finden Sie Details zu den Clustern, wie z. B. deren Name, IP-Adresse und Kommunikationsstatus.

**Bevor Sie beginnen**

Sie benötigen die Rolle „Operator“, „Application Administrator“ oder „Storage Administrator“.

**Schritt**

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.

   Alle Cluster in Ihrer vom Unified Manager gemanagten Storage-Umgebung werden angezeigt. Die Clusterliste ist nach der Spalte für den Schweregrad des Erfassungsstatus sortiert. Durch Klicken auf eine Spaltenüberschrift können die Cluster nach verschiedenen Spalten sortiert werden.

# Cluster zu Active IQ Unified Manager hinzufügen

Sie können Active IQ Unified Manager einen Cluster hinzufügen, damit Sie den Cluster überwachen können. Dies umfasst die Möglichkeit, Clusterinformationen wie den Systemstatus, die Kapazität, die Performance und die Konfiguration des Clusters abzurufen, damit Sie auftretende Probleme erkennen und beheben können.

**Bevor Sie beginnen**

- Sie benötigen die Rolle des Anwendungsadministrators oder die Rolle des Storage-Administrators.
- Sie benötigen folgende Informationen:
  - Unified Manager unterstützt lokale ONTAP Cluster, ONTAP Select, Cloud Volumes ONTAP.
  - Sie benötigen den Hostnamen oder die Cluster-Management-IP-Adresse (IPv4 oder IPv6) für den Cluster.

    Bei Verwendung des Hostnamens muss dieser zur Clusterverwaltungs-IP-Adresse für die Clusterverwaltungs-LIF aufgelöst werden. Bei Verwendung einer Knotenverwaltungs-LIF schlägt der Vorgang fehl.
  - Sie benötigen den Benutzernamen und das Passwort, um auf den Cluster zugreifen zu können.

    Dieses Konto muss die Rolle *admin* besitzen, wobei der Anwendungszugriff auf *ontapi*, *amqp*, *console* und *http* festgelegt sein muss.
  - Sie müssen die Portnummer kennen, um sich über das HTTPS-Protokoll mit dem Cluster zu verbinden (typischerweise Port 443).
  - Auf dem Cluster muss ONTAP Softwareversion 9.9 oder höher ausgeführt werden.
  - Auf dem Unified Manager Server muss ausreichend Speicherplatz vorhanden sein. Das Hinzufügen eines Clusters zum Server ist nicht möglich, wenn bereits mehr als 90 % des Speicherplatzes belegt sind.

- Sie verfügen über die erforderlichen Zertifikate:

  **SSL-Zertifikat (HTTPS)**: Dieses Zertifikat gehört Unified Manager. Bei einer Neuinstallation von Unified Manager wird standardmäßig ein selbstsigniertes SSL-Zertifikat (HTTPS) generiert. NetApp empfiehlt, es für mehr Sicherheit auf ein von einer Zertifizierungsstelle signiertes Zertifikat umzustellen. Wenn das Serverzertifikat abläuft, sollten Sie es neu generieren und Unified Manager neu starten, damit die Services das neue Zertifikat übernehmen. Weitere Informationen zum Regenerieren von SSL-Zertifikaten enthält "Generieren eines HTTPS-Sicherheitszertifikats".

  **EMS-Zertifikat**: Dieses Zertifikat gehört dem Unified Manager. Es dient zur Authentifizierung von EMS-Benachrichtigungen, die von ONTAP empfangen werden.

  **Zertifikate für die gegenseitige TLS-Kommunikation**: Werden während der gegenseitigen TLS-Kommunikation zwischen Unified Manager und ONTAP verwendet. Die zertifikatbasierte Authentifizierung ist für einen Cluster abhängig von der ONTAP Version aktiviert. Wenn auf einem Cluster eine ONTAP Version niedriger als 9.5 ausgeführt wird, ist die zertifikatbasierte Authentifizierung nicht aktiviert.

  Die zertifikatbasierte Authentifizierung ist für einen Cluster nicht automatisch aktiviert, wenn Sie eine ältere Version von Unified Manager aktualisieren. Sie können sie jedoch aktivieren, indem Sie die Clusterdetails ändern und speichern. Wenn das Zertifikat abläuft, müssen Sie es neu generieren, um das neue Zertifikat einzubinden. Weitere Informationen zum Anzeigen und Neugenerieren des Zertifikats finden Sie unter "Cluster bearbeiten".

  - Über die Web-Benutzeroberfläche lässt sich ein Cluster hinzufügen, und die zertifikatbasierte Authentifizierung wird dabei automatisch aktiviert.
  - Sie können einen Cluster über Unified Manager CLI hinzufügen, die zertifikatbasierte Authentifizierung ist standardmäßig nicht aktiviert. Wenn Sie einen Cluster mit Unified Manager CLI hinzufügen, müssen Sie den Cluster anschließend über Unified Manager UI bearbeiten. Unter "Unterstützte Unified Manager CLI-Befehle" finden Sie Informationen zum Hinzufügen eines Clusters mit Unified Manager CLI.
  - Wenn die zertifikatbasierte Authentifizierung für einen Cluster aktiviert ist und Sie das Backup von Unified Manager auf einem Server erstellen und es auf einem anderen Unified Manager Server wiederherstellen, bei dem Hostname oder IP-Adresse geändert wurden, kann die Überwachung des Clusters fehlschlagen. Zur Vermeidung dieses Fehlers empfiehlt sich das Bearbeiten und Speichern der Clusterdetails. Weitere Informationen zum Bearbeiten von Clusterdetails finden Sie unter "Cluster bearbeiten".
  - Auf Cluster-Level fügt die Active IQ Schnittstelle zwei neue Benutzergruppeneinträge für das Authentifizierungsverfahren „cert“ hinzu.

  + **Clusterzertifikate**: Dieses Zertifikat gehört ONTAP. Sie können keinen Cluster mit einem abgelaufenen Zertifikat zu Unified Manager hinzufügen. Wenn das Zertifikat bereits abgelaufen ist, müssen Sie es vor dem Hinzufügen des Clusters neu generieren. Informationen zur Zertifikatserstellung finden Sie im entsprechenden Knowledge-Base-Artikel "Erneuern eines ONTAP selbstsignierten Zertifikats in der System Manager Benutzeroberfläche".

- Eine einzelne Instanz von Unified Manager kann eine bestimmte Anzahl von Knoten unterstützen. Wenn Sie eine Umgebung überwachen müssen, die die unterstützte Knotenanzahl überschreitet, müssen Sie eine zusätzliche Instanz von Unified Manager installieren, um einige der Cluster zu überwachen. Die Liste der unterstützten Knotenanzahl finden Sie in der "Unified Manager Best Practices-Leitfaden".

**Schritte**

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite „Cluster Setup“ ist **Add** auszuwählen.
3. Im Dialogfeld „Cluster hinzufügen“ werden die erforderlichen Werte wie erforderlich angegeben; anschließend wird auf **Submit** geklickt.
4. Im Dialogfeld „Host autorisieren“ kann über **Zertifikat anzeigen** die Zertifikatsinformation zum Cluster angezeigt werden.
5. Klicken Sie auf **Ja**.

   Nach dem Speichern der Clusterdetails können Sie das Zertifikat für die gegenseitige TLS-Kommunikation für einen Cluster einsehen.

   Wenn die zertifikatbasierte Authentifizierung nicht aktiviert ist, prüft Unified Manager das Zertifikat nur beim erstmaligen Hinzufügen des Clusters. Unified Manager prüft das Zertifikat nicht bei jedem API-Aufruf an ONTAP.

Nachdem alle Objekte für einen neuen Cluster erkannt wurden, beginnt Unified Manager mit der Erfassung historischer Performance-Daten der letzten 15 Tage. Diese Statistiken werden mithilfe der Funktion zur Erfassung der Datenkontinuität gesammelt. Diese Funktion stellt Ihnen unmittelbar nach dem Hinzufügen eines Clusters Performance-Informationen für mehr als zwei Wochen zur Verfügung. Nach Abschluss des Erfassungszyklus für die Datenkontinuität werden standardmäßig alle fünf Minuten Echtzeit-Performance-Daten für den Cluster erfasst.

- Die Erfassung von 15 Tagen Performance-Daten ist CPU-intensiv. NetApp empfiehlt, das Hinzufügen neuer Cluster zeitlich zu staffeln, damit die Abfragen zur Erfassung der Datenkontinuität nicht gleichzeitig auf zu vielen Clustern ausgeführt werden. Wenn Sie Unified Manager während des Zeitraums der Erfassung der Datenkontinuität neu starten, wird die Erfassung angehalten, und in den Performance-Diagrammen werden Lücken für den fehlenden Zeitraum angezeigt.
- Beim Hinzufügen eines ONTAP Clusters ab Version 9.14.1 erfolgt die Kommunikation über die Cloud-Agent-Funktion. ONTAP erstellt automatisch einen internen Servicekonto-Benutzer mit schreibgeschützten Berechtigungen (z. B. clus-agent-xxxx). Unified Manager stellt die Datenerfassung von diesen Clustern ein, wenn der `clus-agent` Benutzer gelöscht wird.

Falls Sie eine Fehlermeldung erhalten, dass Sie den Cluster nicht hinzufügen können, kann eines der folgenden Probleme vorliegen:

- Wenn die Uhren auf den beiden Systemen nicht synchronisiert sind und das Startdatum des Unified Manager HTTPS-Zertifikats nach dem Datum auf dem Cluster liegt. Die Uhren müssen mithilfe von NTP oder einem ähnlichen Dienst synchronisiert sein.
- Wenn die maximale Anzahl an EMS-Benachrichtigungszielen im Cluster erreicht ist, kann die Unified Manager Adresse nicht hinzugefügt werden. Standardmäßig können im Cluster nur 20 EMS-Benachrichtigungsziele definiert werden.

**Verwandte Informationen**

"Hinzufügen von Benutzern"

"Anzeigen der Clusterliste und Details"

"Installation eines von einer CA signierten und zurückgegebenen HTTPS-Zertifikats"

# Bearbeiten der Clustereinstellungen in Active IQ Unified Manager

Über das Dialogfeld „Cluster bearbeiten“ können Sie die Einstellungen eines bestehenden Clusters ändern, z. B. den Hostnamen oder die IP-Adresse, den Benutzernamen, das Passwort und den Port.

**Bevor Sie beginnen**

Sie benötigen die Rolle des Anwendungsadministrators oder die Rolle des Storage-Administrators.

Ab Unified Manager 9.7 können Cluster nur noch über HTTPS hinzugefügt werden.

**Schritte**

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite **Cluster Setup** erfolgt die Auswahl des Clusters, den Sie bearbeiten möchten; anschließend klicken Sie auf **Edit**.
3. Im Dialogfeld **Edit Cluster** lassen sich die Werte bei Bedarf ändern. + Wenn die Details für einen zu Unified Manager hinzugefügten Cluster geändert wurden, können die Zertifikatsdetails für die Mutual TLS-Kommunikation abhängig von der ONTAP Version angezeigt werden. Weitere Informationen zur ONTAP Version finden Sie unter "Zertifikate für die gegenseitige TLS-Kommunikation". + Die Zertifikatsdetails können über **Certificate Details** angezeigt werden. Wenn das Zertifikat abgelaufen ist, lässt sich das neue Zertifikat über die Schaltfläche **Regenerate** einbinden.
4. Anschließend **Absenden** auswählen.
5. Im Dialogfeld „Host autorisieren“ kann über **Zertifikat anzeigen** die Zertifikatsinformation zum Cluster angezeigt werden.
6. Klicken Sie auf **Ja**.

**Verwandte Informationen**

"Hinzufügen von Benutzern"

"Anzeigen der Clusterliste und Details"

# Entfernung von Clustern aus Active IQ Unified Manager

Sie können einen Cluster aus Unified Manager über die Seite „Cluster Setup“ entfernen. Beispielsweise können Sie einen Cluster entfernen, wenn die Clustererkennung fehlschlägt oder wenn Sie ein Storage-System stilllegen möchten.

**Bevor Sie beginnen**

Sie benötigen die Rolle des Anwendungsadministrators oder die Rolle des Storage-Administrators.

Diese Aufgabe entfernt den ausgewählten Cluster aus Unified Manager. Nach dem Entfernen eines Clusters überwacht Unified Manager ihn nicht mehr. Die bei dem entfernten Cluster registrierte Instanz von Unified Manager wird ebenfalls von dem Cluster abgemeldet.

Durch das Entfernen eines Clusters werden auch alle zugehörigen Storage-Objekte, Verlaufsdaten, Storage Services und alle zugehörigen Ereignisse aus Unified Manager gelöscht. Diese Änderungen werden nach dem

nächsten Datenerfassungszyklus auf den Inventar- und Detailseiten angezeigt.

> Sie müssen einen Cluster aus Unified Manager entfernen, bevor Sie ihn außer Betrieb nehmen. Wenn der Cluster bereits offline oder nicht erreichbar ist, wenn Sie versuchen, ihn zu entfernen, kann Unified Manager nicht mit dem Cluster kommunizieren, um den Anwendungsdatensatz und die konfigurierten Event Management System (EMS) Abonnements zu entfernen. Dies kann dazu führen, dass der Entfernungsprozess fehlschlägt oder nicht mehr reagiert, bevor er abgeschlossen ist.

**Schritte**

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite „Cluster Setup“ wählen Sie den Cluster aus, der entfernt werden soll, und klicken anschließend auf **Remove**.
3. Im Meldungsdialogfeld **Remove Data Source** wird durch Klicken auf **Remove** die Entfernungsanforderung bestätigt.

**Verwandte Informationen**

"Hinzufügen von Benutzern"

"Anzeigen der Clusterliste und Details"

# Cluster in Active IQ Unified Manager erneut erkennen

Auf der Seite „Cluster Setup“ kann ein Cluster manuell erneut identifiziert werden, um die neuesten Informationen über den Systemstatus, den Überwachungsstatus und den Performance-Status des Clusters zu erhalten.

Sie können einen Cluster manuell erneut identifizieren, wenn Sie den Cluster aktualisieren möchten, beispielsweise durch Erhöhen der Größe eines Aggregats, wenn nicht genügend Speicherplatz vorhanden ist, und wenn Unified Manager die von Ihnen vorgenommenen Änderungen identifizieren soll.

Wenn Unified Manager mit OnCommand Workflow Automation (WFA) gekoppelt ist, löst die Kopplung die erneute Erfassung der von WFA zwischengespeicherten Daten aus.

**Schritte**

1. Auswahl im linken Navigationsbereich: **Storage Management** > **Cluster Setup**.
2. Auf der Seite **Cluster Setup** erfolgt die Auswahl von **Rediscover**.

   Unified Manager identifiziert den ausgewählten Cluster erneut und zeigt den aktuellen Systemstatus und Performance-Status an.

**Verwandte Informationen**

"Anzeigen der Clusterliste und Details"

**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.