Verwalten der Authentifizierung

Active IQ Unified Manager 9.11

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-911/config/task_edit_authentication_servers.html on October 16, 2025. Always check docs.netapp.com for the latest.

Inhalt

Verwalten der Authentifizierung . . . 1
- Bearbeiten von Authentifizierungsservern . . . 1
- Authentifizierungsserver werden gelöscht . . . 1
- Authentifizierung mit Active Directory oder OpenLDAP . . . 2
- Audit-Protokollierung . . . 2
  - Audit-Protokolle werden konfiguriert . . . 3
  - Aktivieren der Fernprotokollierung von Audit-Protokollen . . . 4
- Seite „Remote Authentication“ . . . 5
  - Bereich Authentifizierungsserver . . . 7

Verwalten der Authentifizierung

Sie können die Authentifizierung mit LDAP oder Active Directory auf dem Unified Manager-Server aktivieren und so konfigurieren, dass sie mit Ihren Servern zur Authentifizierung von Remote-Benutzern verwendet werden kann.

Informationen zur Aktivierung der Fernauthentifizierung, zum Einrichten von Authentifizierungsdiensten und zum Hinzufügen von Authentifizierungsseviern finden Sie im vorherigen Abschnitt unter **Konfigurieren von Unified Manager zum Senden von Benachrichtigungen**.

Bearbeiten von Authentifizierungsservern

Sie können den Port ändern, den der Unified Manager-Server für die Kommunikation mit Ihrem Authentifizierungsserver verwendet.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Aktivieren Sie das Kontrollkästchen * Nested Group Lookup* deaktivieren.
3. Wählen Sie im Bereich **Authentifizierungsserver** den Authentifizierungsserver aus, den Sie bearbeiten möchten, und klicken Sie dann auf **Bearbeiten**.
4. Bearbeiten Sie im Dialogfeld **Authentifizierungsserver bearbeiten** die Portdetails.
5. Klicken Sie Auf **Speichern**.

Authentifizierungsserver werden gelöscht

Sie können einen Authentifizierungsserver löschen, wenn Sie verhindern möchten, dass der Unified Manager-Server mit dem Authentifizierungsserver kommuniziert. Wenn Sie beispielsweise einen Authentifizierungsserver ändern möchten, mit dem der Verwaltungsserver kommuniziert, können Sie den Authentifizierungsserver löschen und einen neuen Authentifizierungsserver hinzufügen.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Wenn Sie einen Authentifizierungsserver löschen, können Remote-Benutzer oder -Gruppen des Authentifizierungsservers nicht mehr auf Unified Manager zugreifen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Remote Authentication**.
2. Wählen Sie einen oder mehrere Authentifizierungsserver aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie auf **Ja**, um die Löschanforderung zu bestätigen.

Wenn die Option **Sichere Verbindung verwenden** aktiviert ist, werden die mit dem Authentifizierungsserver verknüpften Zertifikate zusammen mit dem Authentifizierungsserver gelöscht.

Authentifizierung mit Active Directory oder OpenLDAP

Sie können die Remote-Authentifizierung auf dem Verwaltungsserver aktivieren und den Verwaltungsserver so konfigurieren, dass er mit Ihren Authentifizierungsservern kommunizieren kann, damit Benutzer innerhalb der Authentifizierungsserver auf Unified Manager zugreifen können.

Sie können einen der folgenden vordefinierten Authentifizierungsservices verwenden oder Ihren eigenen Authentifizierungsservice angeben:

- Microsoft Active Directory

  Sie können Microsoft Lightweight Directory Services nicht verwenden.

- OpenLDAP

Sie können den erforderlichen Authentifizierungsservice auswählen und die entsprechenden Authentifizierungsserver hinzufügen, damit die Remote-Benutzer im Authentifizierungsserver auf Unified Manager zugreifen können. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet. Der Verwaltungsserver verwendet das Lightweight Directory Access Protocol (LDAP) zur Authentifizierung von Remote-Benutzern innerhalb des konfigurierten Authentifizierungsservers.

Für lokale Benutzer, die in Unified Manager erstellt werden, behält der Verwaltungsserver eine eigene Datenbank mit Benutzernamen und Kennwörtern. Der Verwaltungsserver führt die Authentifizierung durch und verwendet Active Directory oder OpenLDAP nicht zur Authentifizierung.

Audit-Protokollierung

Sie können erkennen, ob die Audit-Protokolle unter Verwendung von Audit-Protokollen kompromittiert wurden. Alle von einem Benutzer durchgeführten Aktivitäten werden überwacht und in den Audit-Protokollen protokolliert. Die Audits werden für alle Benutzerschnittstellen und öffentlich exponierte APIs' Funktionalitäten von Active IQ Unified Manager durchgeführt.

Sie können die Ansicht Überwachungsprotokoll: Dateiansicht verwenden, um alle in Ihrem Active IQ Unified Manager verfügbaren Audit-Log-Dateien anzuzeigen und darauf zuzugreifen. Die Dateien im Audit Log: File View werden basierend auf ihrem Erstellungsdatum aufgelistet. In dieser Ansicht werden Informationen über das gesamte Überwachungsprotokoll angezeigt, das von der Installation oder dem Upgrade auf die im System vorhandenen Protokolle erfasst wird. Wenn Sie in Unified Manager eine Aktion ausführen, werden die Informationen aktualisiert und stehen in den Protokollen zur Verfügung. Der Status jeder Protokolldatei wird mit dem Attribut „`File Integrity Status`“ erfasst, das aktiv überwacht wird, um Manipulation oder Löschung der Protokolldatei zu erkennen. Die Audit-Protokolle können einen der folgenden Status haben, wenn die Audit-Protokolle im System verfügbar sind:

Bundesland	Beschreibung
AKTIV	Datei, in der Protokolle aktuell protokolliert werden.
NORMAL	Datei, die inaktiv, komprimiert und im System gespeichert ist.
MANIPULIERT	Datei, die von einem Benutzer kompromittiert wurde, der die Datei manuell bearbeitet hat.
MANUELL_LÖSCHEN	Datei, die von einem autorisierten Benutzer gelöscht wurde.
ROLLOVER_DELETE	Datei, die aufgrund von Rolling Off auf der Grundlage Rolling Configuration Policy gelöscht wurde.
UNEXPECTED_DELETE	Datei, die aus unbekannten Gründen gelöscht wurde.

Die Seite „Prüfprotokoll“ enthält die folgenden Befehlsschaltflächen:

- Konfigurieren
- Löschen
- Download

Mit der Schaltfläche **DELETE** können Sie alle in der Ansicht Audit Logs aufgeführten Audit-Protokolle löschen. Sie können ein Audit-Protokoll löschen und optional einen Grund angeben, die Datei zu löschen, was in Zukunft hilft, ein gültiges Löschen zu bestimmen. Die SPALTE GRUND enthält den Grund und den Namen des Benutzers, der den Löschvorgang durchgeführt hat.

Das Löschen einer Protokolldatei führt zum Löschen der Datei aus dem System, der Eintrag in der DB-Tabelle wird jedoch nicht gelöscht.

Sie können die Audit-Protokolle von Active IQ Unified Manager mit der Schaltfläche **DOWNLOAD** im Bereich Audit-Protokolle herunterladen und die Audit-Log-Dateien exportieren. Die Dateien, die als „`NORMAL`“ oder „`MANIPULIERT`“ markiert sind, werden komprimiert heruntergeladen `.gzip` Formatieren.

Wenn ein komplettes AutoSupport Bundle generiert wird, enthält das Support Bundle sowohl archivierte als auch aktive Audit-Log-Dateien. Wenn aber ein Light Support Bundle erzeugt wird, enthält es nur die aktiven Audit-Protokolle. Die archivierten Prüfprotokolle sind nicht enthalten.

Audit-Protokolle werden konfiguriert

Sie können die Schaltfläche **Konfigurieren** im Bereich Audit Logs verwenden, um die Rolling Policy für Audit Log-Dateien zu konfigurieren und auch die Remote-Protokollierung für die Audit-Protokolle zu aktivieren.

Sie können die Werte in den AUFBEWAHRUNGSTAGEN **MAX-DATEIGRÖSSE** und **AUDIT-LOGBUCH** entsprechend der gewünschten Menge und Häufigkeit der Daten festlegen, die Sie im System speichern möchten. Der Wert im Feld **GESAMTE LOGGRÖSSE DES AUDITS** ist die Größe der gesamten Audit-Log-

Daten im System. Die Roll-Over-Richtlinie wird durch die Werte im Feld **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** und **TOTAL AUDIT LOG SIZE** bestimmt. Wenn die Größe des Backups des Revisionsprotokolls den in **GESAMT-AUDIT-LOG-GRÖSSE** konfigurierten Wert erreicht, wird die zuerst archivierte Datei gelöscht. Das bedeutet, dass die älteste Datei gelöscht wird. Der Dateieintrag ist jedoch weiterhin in der Datenbank verfügbar und wird als „`Rollover Delete`“ markiert. Der **AUDIT LOG RETENTION DAYS**-Wert gilt für die Anzahl der Tage, an denen die Audit Log-Dateien aufbewahrt werden. Jede Datei, die älter als der in diesem Feld eingestellte Wert ist, wird über gerollt.

Schritte

1. Klicken Sie Auf **Prüfprotokolle** > **Konfigurieren**.
2. Geben Sie die Werte in den * MAX-DATEIGRÖSSEN*, **GESAMT-AUDIT-LOG-GRÖSSE** und **AUDIT-LOG-AUFBEWAHRUNGSTAGE** ein.

   Wenn Sie die Fernprotokollierung aktivieren möchten, wählen Sie die Option **Remote Logging aktivieren**.

Aktivieren der Fernprotokollierung von Audit-Protokollen

Aktivieren Sie das Kontrollkästchen **Remote-Protokollierung aktivieren** im Dialogfeld Audit-Protokolle konfigurieren, um die Remote-Audit-Protokollierung zu aktivieren. Mit dieser Funktion können Sie Überwachungsprotokolle an einen Remote Syslog-Server übertragen. Auf diese Weise können Sie Ihre Audit-Protokolle verwalten, wenn es Platzbeschränkungen gibt.

Die Remote-Protokollierung von Audit-Protokollen bietet ein manipulationssicheres Backup, falls die Audit-Log-Dateien auf dem Active IQ Unified Manager Server manipuliert werden.

Schritte

1. Aktivieren Sie im Dialogfeld **Audit Logs konfigurieren** das Kontrollkästchen **Remote Logging aktivieren**.

   Zusätzliche Felder zum Konfigurieren der Remote-Protokollierung werden angezeigt.

2. Geben Sie den **HOSTNAME** und den **PORT** des Remoteserver ein, mit dem Sie eine Verbindung herstellen möchten.
3. Klicken Sie im Feld **SERVER CA ZERTIFIKAT** auf **DURCHSUCHEN**, um ein öffentliches Zertifikat des Zielservers auszuwählen.

   Das Zertifikat sollte in hochgeladen werden `.pem` Formatieren. Dieses Zertifikat sollte vom Ziel-Syslog-Server abgerufen werden und sollte nicht abgelaufen sein. Das Zertifikat sollte den ausgewählten „`hostname`“ als Teil des enthalten `SubjectAltName` (SAN)-Attribut.

4. Geben Sie die Werte für die folgenden Felder ein: **CHARSET**, **VERBINDUNGS-TIMEOUT**, **VERBINDUNGSVERZÖGERUNG**.

   Für diese Felder sollten die Werte in Millisekunden angegeben werden.

5. Wählen Sie das erforderliche Syslog-Format und die TLS-Protokollversion in den Feldern **FORMAT** und **PROTOKOLL** aus.
6. Aktivieren Sie das Kontrollkästchen **Client Authentication** aktivieren, wenn für den Ziel-Syslog-Server eine zertifikatbasierte Authentifizierung erforderlich ist.

   Sie müssen das Clientauthentifizierungszertifikat herunterladen und auf den Syslog-Server hochladen,

bevor Sie die Konfiguration des Überwachungsprotokolls speichern. Andernfalls schlägt die Verbindung fehl. Je nach Typ des Syslog-Servers müssen Sie möglicherweise einen Hash des Client-Authentifizierungszertifikats erstellen.

Beispiel: Syslog-ng erfordert, dass mit dem Befehl ein <Hash> des Zertifikats erstellt wird `openssl x509 -noout -hash -in cert.pem`, Und dann sollten Sie symbolisch das Clientauthentifizierungszertifikat mit einer Datei verknüpfen, die nach dem <Hash> .0 benannt ist.

7. Klicken Sie auf **Speichern**, um die Verbindung mit Ihrem Server zu konfigurieren und die Fernprotokollierung zu aktivieren.

   Sie werden zur Seite Audit Logs weitergeleitet.

Seite „Remote Authentication“

Mithilfe der Seite Remote Authentication kann Unified Manager für die Kommunikation mit Ihrem Authentifizierungsserver konfiguriert werden, um Remote-Benutzer zu authentifizieren, die versuchen, sich in der Web-UI von Unified Manager anzumelden.

Sie müssen über die Rolle „Anwendungsadministrator“ oder „Speicheradministrator“ verfügen.

Nachdem Sie das Kontrollkästchen Remote-Authentifizierung aktivieren aktiviert haben, können Sie die Remote-Authentifizierung über einen Authentifizierungsserver aktivieren.

- **Authentifizierungsdienst**

  Ermöglicht Ihnen, den Verwaltungsserver so zu konfigurieren, dass Benutzer in Verzeichnisdienstanbietern wie Active Directory, OpenLDAP authentifiziert werden oder dass Sie Ihren eigenen Authentifizierungsmechanismus festlegen. Sie können einen Authentifizierungsservice nur festlegen, wenn Sie die Remote-Authentifizierung aktiviert haben.

  - **Active Directory**
    - Administratorname

      Gibt den Administratornamen des Authentifizierungsservers an.

    - Passwort

      Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

    - Name Der Basisstation

      Gibt den Speicherort der Remote-Benutzer im Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**.

    - Deaktivieren Sie Die Suche Nach Verschachtelter Gruppe

      Gibt an, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Diese Option ist standardmäßig deaktiviert. Wenn Sie Active Directory verwenden, können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

- Verwenden Sie Secure Connection

  Gibt den Authentifizierungsservice an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

- **OpenLDAP**
  - Distinguished Name Binden

    Gibt den Distinguished BIND-Namen an, der zusammen mit dem angegebenen Basisnamen zum Suchen von Remote-Benutzern im Authentifizierungsserver verwendet wird.

  - Kennwort Binden

    Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

  - Name Der Basisstation

    Gibt den Speicherort der Remote-Benutzer im Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**.

  - Verwenden Sie Secure Connection

    Gibt an, dass Secure LDAP für die Kommunikation mit LDAPS-Authentifizierungsservern verwendet wird.

- **Andere**
  - Distinguished Name Binden

    Gibt den Distinguished BIND-Namen an, der zusammen mit dem angegebenen Basisnamen verwendet wird, um Remote-Benutzer auf dem von Ihnen konfigurierten Authentifizierungsserver zu finden.

  - Kennwort Binden

    Gibt das Kennwort für den Zugriff auf den Authentifizierungsserver an.

  - Name Der Basisstation

    Gibt den Speicherort der Remote-Benutzer im Authentifizierungsserver an. Wenn beispielsweise der Domänenname des Authentifizierungsservers ou@domain.com lautet, dann ist der Name der Basisunterscheidungder **cn=ou,dc=Domain,dc=com**.

  - Protokollversion

    Gibt die LDAP-Version (Lightweight Directory Access Protocol) an, die von Ihrem Authentifizierungsserver unterstützt wird. Sie können festlegen, ob die Protokollversion automatisch erkannt werden muss oder ob die Version auf 2 oder 3 eingestellt werden muss.

  - Attribut Benutzername

    Gibt den Namen des Attributs im Authentifizierungsserver an, der Benutzeranmeldungsnamen enthält, die vom Verwaltungsserver authentifiziert werden sollen.

  - Eigenschaft „Gruppenmitgliedschaft“

Gibt einen Wert an, der die Mitgliedschaft der Managementservergruppe Remote-Benutzern auf der Grundlage eines im Authentifizierungsserver des Benutzers angegebenen Attributs und Wertes zuweist.

- UGID

  Wenn die Remote-Benutzer als Mitglieder einer Gruppe OfUniqueNames-Objekt im Authentifizierungsserver enthalten sind, können Sie mit dieser Option die Mitgliedschaft der Management-Servergruppe den Remotebenutzern basierend auf einem bestimmten Attribut in dieser GroupOfUniqueNames-Objekt zuweisen.

- Deaktivieren Sie Die Suche Nach Verschachtelter Gruppe

  Gibt an, ob die Option für die Suche nach verschachtelten Gruppen aktiviert oder deaktiviert werden soll. Diese Option ist standardmäßig deaktiviert. Wenn Sie Active Directory verwenden, können Sie die Authentifizierung beschleunigen, indem Sie die Unterstützung für verschachtelte Gruppen deaktivieren.

- Mitglied

  Gibt den Attributnamen an, den Ihr Authentifizierungsserver zum Speichern von Informationen über die einzelnen Mitglieder einer Gruppe verwendet.

- Benutzerobjektklasse

  Gibt die Objektklasse eines Benutzers im Remote-Authentifizierungsserver an.

- Objektklasse Gruppieren

  Gibt die Objektklasse aller Gruppen im Remote-Authentifizierungsserver an.

- Verwenden Sie Secure Connection

  Gibt den Authentifizierungsservice an, der für die Kommunikation mit Authentifizierungsservern verwendet wird.

> Wenn Sie den Authentifizierungsservice ändern möchten, müssen Sie sicherstellen, dass Sie alle vorhandenen Authentifizierungsserver löschen und neue Authentifizierungsserver hinzufügen.

Bereich Authentifizierungsserver

Im Bereich Authentifizierungsserver werden die Authentifizierungsserver angezeigt, mit denen der Verwaltungsserver kommuniziert, um Remotebenutzer zu finden und zu authentifizieren. Die Anmeldeinformationen für Remote-Benutzer oder -Gruppen werden vom Authentifizierungsserver verwaltet.

- **Befehlsschaltflächen**

  Ermöglicht das Hinzufügen, Bearbeiten oder Löschen von Authentifizierungsservern.

  - Zusatz

    Ermöglicht das Hinzufügen eines Authentifizierungsservers.

Wenn der neue Authentifizierungsserver Teil eines Hochverfügbarkeitspaars ist (unter Verwendung derselben Datenbank), können Sie auch den Authentifizierungsserver des Partners hinzufügen. Dadurch kann der Management-Server mit dem Partner kommunizieren, wenn einer der Authentifizierungsserver nicht erreichbar ist.

  - Bearbeiten

    Ermöglicht die Bearbeitung der Einstellungen für einen ausgewählten Authentifizierungsserver.

  - Löschen

    Löscht die ausgewählten Authentifizierungsserver.

- **Name oder IP-Adresse**

  Zeigt den Hostnamen oder die IP-Adresse des Authentifizierungsservers an, der zur Authentifizierung des Benutzers auf dem Verwaltungsserver verwendet wird.

- **Port**

  Zeigt die Portnummer des Authentifizierungsservers an.

- **Testauthentifizierung**

  Mit dieser Schaltfläche wird die Konfiguration Ihres Authentifizierungsservers durch Authentifizierung eines Remotebenutzers oder einer -Gruppe validiert.

  Wenn Sie beim Testen nur den Benutzernamen angeben, sucht der Verwaltungsserver im Authentifizierungsserver nach dem Remote-Benutzer, authentifiziert den Benutzer jedoch nicht. Wenn Sie sowohl den Benutzernamen als auch das Passwort angeben, sucht der Verwaltungsserver den Remote-Benutzer und authentifiziert diesen.

  Sie können die Authentifizierung nicht testen, wenn die Remote-Authentifizierung deaktiviert ist.

Copyright-Informationen

Copyright © 2025 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.