



REST-API-Zugriff und Authentifizierung im Active IQ Unified Manager

Active IQ Unified Manager

NetApp
October 15, 2025

Inhalt

- REST-API-Zugriff und Authentifizierung im Active IQ Unified Manager 1
 - Authentifizierung 3
 - Im Active IQ Unified Manager verwendete HTTP-Statuscodes 3
 - Empfehlungen zur Verwendung der APIs für Active IQ Unified Manager 5
 - Protokolle zur Fehlerbehebung 5
 - Jobobjekte asynchrone Prozesse 6
 - Asynchrone Anforderungen, beschrieben mithilfe des Job-Objekts 6
 - Abfragen des mit einer API-Anforderung verknüpften Job-Objekts 7
 - Schritte in einer asynchronen Anfrage 7
 - Hallo API-Server. 7

REST-API-Zugriff und Authentifizierung im Active IQ Unified Manager

Auf die Active IQ Unified Manager REST-API kann über jeden REST-Client oder jede Programmierplattform zugegriffen werden, die HTTP-Anfragen mit einem grundlegenden HTTP-Authentifizierungsmechanismus ausgeben kann.

Eine Beispielanfrage und -antwort:

- **Anfrage**

```
GET
https://<IP
address/hostname>:<port_number>/api/v2/datacenter/cluster/clusters
```

- **Antwort**

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "name": "fas8040-206-21",
      "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "contact": null,
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33 UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "isSanOptimized": false,
      "management_ip": "10.226.207.25",
      "nodes": [
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "name": "fas8040-206-21-01",
          "_links": {
            "self": {
```

```

        "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
    },
    "location": null,
    "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
    },
    "model": "FAS8040",
    "uptime": 13924095,
    "serial_number": "701424000157"
},
{
    "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
    "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
    "name": "fas8040-206-21-02",
    "_links": {
        "self": {
            "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7"
        }
    },
    "location": null,
    "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
    },
    "model": "FAS8040",
    "uptime": 14012386,
    "serial_number": "701424000564"
}
],
"_links": {
    "self": {
        "href": "/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-

```

```

a3e2-00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-
00a0985badbb"
    }
  },

```

- ``IP address/hostname`` ist die IP-Adresse oder der vollqualifizierte Domänenname (FQDN) des API-Servers.
- Port 443

443 ist der Standard-HTTPS-Port. Sie können den HTTPS-Port bei Bedarf anpassen.

Um HTTP-Anfragen von einem Webbrowser aus zu stellen, müssen Sie REST-API-Browser-Plugins verwenden. Sie können auch über Skriptplattformen wie cURL und Perl auf die REST-API zugreifen.

Authentifizierung

Unified Manager unterstützt das grundlegende HTTP-Authentifizierungsschema für APIs. Für einen sicheren Informationsfluss (Anfrage und Antwort) sind die REST-APIs nur über HTTPS zugänglich. Der API-Server stellt allen Clients zur Serverüberprüfung ein selbstsigniertes SSL-Zertifikat zur Verfügung. Dieses Zertifikat kann durch ein benutzerdefiniertes Zertifikat (oder CA-Zertifikat) ersetzt werden.

Sie müssen den Benutzerzugriff auf den API-Server konfigurieren, um die REST-APIs aufzurufen. Bei den Benutzern kann es sich um lokale Benutzer (in der lokalen Datenbank gespeicherte Benutzerprofile) oder LDAP-Benutzer handeln (wenn Sie den API-Server für die Authentifizierung über LDAP konfiguriert haben). Sie können den Benutzerzugriff verwalten, indem Sie sich bei der Benutzeroberfläche der Unified Manager-Verwaltungskonsole anmelden.

Im Active IQ Unified Manager verwendete HTTP-Statuscodes

Beim Ausführen der APIs oder bei der Fehlerbehebung sollten Sie sich der verschiedenen HTTP-Statuscodes und Fehlercodes bewusst sein, die von den Active IQ Unified Manager -APIs verwendet werden.

In der folgenden Tabelle sind die Fehlercodes im Zusammenhang mit der Authentifizierung aufgeführt:

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
200	OK	Wird bei erfolgreicher Ausführung synchroner API-Aufrufe zurückgegeben.
201	Erstellt	Erstellung neuer Ressourcen durch synchrone Aufrufe, beispielsweise Konfiguration von Active Directory.

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
202	Akzeptiert	Wird bei erfolgreicher Ausführung asynchroner Aufrufe für Bereitstellungsfunktionen wie dem Erstellen von LUNs und Dateifreigaben zurückgegeben.
400	Ungültige Anfrage	Zeigt einen Fehler bei der Eingabevalidierung an. Der Benutzer muss die Eingaben korrigieren, beispielsweise gültige Schlüssel in einem Anforderungstext.
401	Nicht autorisierte Anfrage	Sie sind nicht berechtigt, die Ressource anzuzeigen/Nicht autorisiert.
403	Verbotene Anfrage	Der Zugriff auf die Ressource, die Sie erreichen wollten, ist verboten.
404	Ressource nicht gefunden	Die Ressource, die Sie erreichen wollten, wurde nicht gefunden.
405	Methode nicht zulässig	Methode nicht zulässig.
429	Zu viele Anfragen	Wird zurückgegeben, wenn der Benutzer innerhalb einer bestimmten Zeit zu viele Anfragen sendet.
500	Interner Serverfehler	Interner Serverfehler. Die Antwort vom Server konnte nicht abgerufen werden. Dieser interne Serverfehler kann dauerhaft sein, muss es aber nicht. Wenn Sie beispielsweise eine GET oder GET ALL Wenn Sie den Vorgang ausführen und diesen Fehler erhalten, wird empfohlen, diesen Vorgang mindestens fünfmal zu wiederholen. Handelt es sich um einen permanenten Fehler, lautet der zurückgegebene Statuscode weiterhin 500. Wenn der Vorgang erfolgreich ist, lautet der zurückgegebene Statuscode 200.

Empfehlungen zur Verwendung der APIs für Active IQ Unified Manager

Wenn Sie die APIs in Active IQ Unified Manager verwenden, sollten Sie bestimmte empfohlene Vorgehensweisen befolgen.

- Für eine gültige Ausführung müssen alle Antwortinhaltenstypen das folgende Format aufweisen:

```
application/json
```

- Die API-Versionsnummer hat nichts mit der Produktversionsnummer zu tun. Sie sollten die neueste Version der API verwenden, die für Ihre Unified Manager-Instanz verfügbar ist. Weitere Informationen zu den API-Versionen von Unified Manager finden Sie im Abschnitt „REST-API-Versionierung in Active IQ Unified Manager“.
- Beim Aktualisieren von Array-Werten mithilfe einer Unified Manager-API müssen Sie die gesamte Wertezeichenfolge aktualisieren. Sie können einem Array keine Werte anhängen. Sie können nur ein vorhandenes Array ersetzen.
- Sie können Filteroperatoren wie Pipe (|) und Platzhalter (*) für alle Abfrageparameter verwenden, mit Ausnahme von Doppelwerten, beispielsweise IOPS und Leistung in den Metrik-APIs.
- Vermeiden Sie die Abfrage von Objekten, indem Sie eine Kombination der Filteroperatoren Platzhalter (*) und Pipe (|) verwenden. Möglicherweise wird eine falsche Anzahl von Objekten abgerufen.
- Bei der Verwendung von Werten für Filter ist darauf zu achten, dass der Wert keine ? Charakter. Dies dient dazu, das Risiko einer SQL-Injection zu verringern.
- Beachten Sie, dass die GET (Alle) Anfragen für eine beliebige API geben maximal 1000 Datensätze zurück. Auch wenn Sie die Abfrage ausführen, indem Sie die `max_records` auf einen Wert über 1000 setzen, werden nur 1000 Datensätze zurückgegeben.
- Für die Durchführung administrativer Funktionen wird die Verwendung der Unified Manager-Benutzeroberfläche empfohlen.

Protokolle zur Fehlerbehebung

Mithilfe von Systemprotokollen können Sie die Ursachen von Fehlern analysieren und Probleme beheben, die beim Ausführen der APIs auftreten können.

Rufen Sie die Protokolle vom folgenden Speicherort ab, um Probleme im Zusammenhang mit den API-Aufrufen zu beheben.

Protokollspeicherort	Verwenden
/var/log/ocie/access_log.log	Enthält alle API-Aufrufdetails, wie etwa den Benutzernamen des Benutzers, der die API aufruft, Startzeit, Ausführungszeit, Status und URL. Sie können diese Protokolldatei verwenden, um die häufig verwendeten APIs zu überprüfen oder Fehler in jedem GUI-Workflow zu beheben. Sie können es auch verwenden, um Analysen basierend auf der Ausführungszeit zu skalieren.
/var/log/ocum/ocumserver.log	Enthält alle API-Ausführungsprotokolle. Sie können diese Protokolldatei zur Fehlerbehebung und zum Debuggen der API-Aufrufe verwenden.
/var/log/ocie/server.log	Enthält alle Wildfly-Serverbereitstellungen und Protokolle zum Starten/Stoppen des Dienstes. Mithilfe dieser Protokolldatei können Sie die Grundursache aller Probleme ermitteln, die beim Starten, Stoppen oder Bereitstellen des Wildfly-Servers auftreten.
/var/log/ocie/au.log	Enthält Protokolle zur Erfassungseinheit. Sie können diese Protokolldatei verwenden, wenn Sie Objekte in ONTAP erstellt, geändert oder gelöscht haben, diese jedoch nicht für die Active IQ Unified Manager REST-APIs berücksichtigt werden.

Jobobjekte asynchrone Prozesse

Active IQ Unified Manager bietet die `jobs` API, die Informationen zu den Jobs abrufen, die während der Ausführung anderer APIs ausgeführt werden. Sie müssen wissen, wie die asynchrone Verarbeitung mithilfe des Job-Objekts funktioniert.

Die Ausführung einiger API-Aufrufe, insbesondere jener zum Hinzufügen oder Ändern von Ressourcen, kann länger dauern als die Ausführung anderer Aufrufe. Unified Manager verarbeitet diese lang andauernden Anfragen asynchron.

Asynchrone Anforderungen, beschrieben mithilfe des Job-Objekts

Nach einem asynchron ausgeführten API-Aufruf zeigt der HTTP-Antwortcode 202 an, dass die Anfrage erfolgreich validiert und akzeptiert, aber noch nicht abgeschlossen wurde. Die Anfrage wird als Hintergrundaufgabe verarbeitet, die nach der ersten HTTP-Antwort an den Client weiterläuft. Die Antwort enthält das Job-Objekt, das die Anfrage verankert, einschließlich seiner eindeutigen Kennung.

Abfragen des mit einer API-Anforderung verknüpften Job-Objekts

Das in der HTTP-Antwort zurückgegebene Job-Objekt enthält mehrere Eigenschaften. Sie können die Status-eigenschaft abfragen, um festzustellen, ob die Anforderung erfolgreich abgeschlossen wurde. Ein Job-Objekt kann einen der folgenden Zustände aufweisen:

- NORMAL
- WARNING
- PARTIAL_FAILURES
- ERROR

Es gibt zwei Techniken, die Sie beim Abfragen eines Job-Objekts verwenden können, um einen Endzustand für die Aufgabe zu erkennen (entweder Erfolg oder Misserfolg):

- Standard-Polling-Anfrage: Der aktuelle Jobstatus wird sofort zurückgegeben.
- Lange Polling-Anforderung: Wenn der Job-Status wechselt zu NORMAL, ERROR, oder PARTIAL_FAILURES.

Schritte in einer asynchronen Anfrage

Sie können das folgende allgemeine Verfahren verwenden, um einen asynchronen API-Aufruf abzuschließen:

1. Führen Sie den asynchronen API-Aufruf aus.
2. Erhalten Sie eine HTTP-Antwort 202, die die erfolgreiche Annahme der Anfrage anzeigt.
3. Extrahieren Sie die Kennung für das Job-Objekt aus dem Antworttext.
4. Warten Sie innerhalb einer Schleife, bis das Job-Objekt den Endzustand erreicht NORMAL, ERROR, oder PARTIAL_FAILURES.
5. Überprüfen Sie den Endstatus des Jobs und rufen Sie das Jobergebnis ab.

Hallo API-Server

Der *Hello API-Server* ist ein Beispielprogramm, das zeigt, wie eine REST-API in Active IQ Unified Manager mit einem einfachen REST-Client aufgerufen wird. Das Beispielprogramm liefert Ihnen grundlegende Details zum API-Server im JSON-Format (der Server unterstützt nur application/json Format).

Die verwendete URI lautet: <https://<hostname>/api/datacenter/svm/svms>. Dieser Beispielcode verwendet die folgenden Eingabeparameter:

- Die IP-Adresse oder der FQDN des API-Servers
- Optional: Portnummer (Standard: 443)
- Benutzername
- Passwort
- Antwortformat(application/json)

Zum Aufrufen von REST-APIs können Sie auch andere Skripte wie Jersey und RESTEasy verwenden, um

einen Java-REST-Client für Active IQ Unified Manager zu schreiben. Beachten Sie die folgenden Hinweise zum Beispielcode:

- Verwendet eine HTTPS-Verbindung zum Active IQ Unified Manager, um die angegebene REST-URI aufzurufen
- Ignoriert das vom Active IQ Unified Manager bereitgestellte Zertifikat
- Überspringt die Hostnamenüberprüfung während des Handshakes
- Anwendung `javax.net.ssl.HttpURLConnection` für eine URI-Verbindung
- Verwendet eine Drittanbieterbibliothek(`org.apache.commons.codec.binary.Base64`) zum Erstellen der Base64-codierten Zeichenfolge, die in der HTTP-Basisauthentifizierung verwendet wird

Zum Kompilieren und Ausführen des Beispielcodes müssen Sie den Java-Compiler 1.8 oder höher verwenden.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
    necessary steps
     * to invoke the REST URI and show the response
    */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
```

```

        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpsURLConnection connection =
getAllTrustingHttpsURLConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
                System.exit(1);
            }
            System.out.println("Invoking API: " + server_url);
            connection.setRequestMethod("GET");
            connection.setRequestProperty("Accept", "application/" +
response_format);
            String authString = getAuthorizationString();
            connection.setRequestProperty("Authorization", "Basic " +
authString);
            if (connection.getResponseCode() != 200) {
                System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
+ connection.getResponseMessage());
                System.exit(1);
            }
            BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
            String response;
            System.out.println("Response:");
            while ((response = br.readLine()) != null) {
                System.out.println(response);
            }
            connection.disconnect();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    /* Print the usage of this sample code */ private static void
printUsage() {
        System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
        System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
        System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
    }

```

```

        System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
        String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
    * * Create a trust manager which accepts all certificates and * use
this trust
    * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
    * SSL Context and skip * server hostname verification during SSL
handshake. * *
    * Note: Trusting all certificates or skipping hostname verification *
is not
    * required for API Services to work. These are done here to * keep
this sample
    * REST Client code as simple as possible.
    */ private static HttpURLConnection
getAllTrustingHttpsURLConnection() {
    HttpURLConnection conn =
null;
    try {
        /* Creating a trust manager that does not
validate certificate chains */
        TrustManager[]
trustAllCertificatesManager = new
TrustManager[]{new
X509TrustManager() {
            public X509Certificate[] getAcceptedIssuers(){return null;}
            public void checkClientTrusted(X509Certificate[]
certs, String authType){}
            public void checkServerTrusted(X509Certificate[]
certs, String authType){}
        }};
        /* Initialize the
SSLContext with the all-trusting trust manager */
        SSLContext sslContext = SSLContext.getInstance("TLS");

```

```

sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));
        URL url = new URL(server_url);
        conn =
(HttpsURLConnection) url.openConnection();
        /* Do not perform an
actual hostname verification during SSL Handshake.
        Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {
        public
boolean verify(String host, SSLSession
        session) {
return true;
        }
});
        } catch (Exception e)
{
        e.printStackTrace();
        return conn;
        }

/*
 * * This forms the Base64 encoded string using the username and
password *
 * provided by the user. This is required for HTTP Basic
Authentication.
 */
private static String getAuthorizationString() {
    String userPassword = user + ":" + password;
    byte[] authEncodedBytes =
Base64.encodeBase64(userPassword.getBytes());
    String authString = new String(authEncodedBytes);
    return authString;
}

}

```

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 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.