



# **Management von Storage über REST-APIs**

## **Active IQ Unified Manager**

NetApp

March 26, 2025

This PDF was generated from <https://docs.netapp.com/de-de/active-iq-unified-manager-97/api-automation/reference-intended-audience-for-this-guide.html> on March 26, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Inhalt

Management von Storage über REST-APIs . . . . .	1
Erste Schritte mit Active IQ Unified Manager . . . . .	1
Zielgruppe für diesen Inhalt . . . . .	1
Active IQ Unified Manager API-Zugriff und Kategorien . . . . .	1
REST-Services in Active IQ Unified Manager angeboten . . . . .	2
API-Version in Active IQ Unified Manager . . . . .	3
Storage-Ressourcen in ONTAP . . . . .	4
REST-API-Zugriff und Authentifizierung in Active IQ Unified Manager . . . . .	5
REST-Zugriff . . . . .	5
Authentifizierung . . . . .	7
In Active IQ Unified Manager verwendete HTTP-Statuscodes . . . . .	7
Empfehlungen für die Verwendung der APIs für Active IQ Unified Manager . . . . .	9
Protokolle für die Fehlerbehebung . . . . .	9
Hallo API Server . . . . .	10
Unified Manager REST-APIs . . . . .	14
APIs für das Management von Datacentern . . . . .	14
Gateway-APIs . . . . .	18
Administrations-APIs . . . . .	21
Sicherheits-APIs . . . . .	23
API und asynchrone Prozesse für Job-Objekte . . . . .	24
APIs für das Management von Workloads . . . . .	26
Typische Workflows für das Storage-Management . . . . .	35
Allgemeines zu den in den Workflows verwendeten API-Aufrufen . . . . .	35
Bestimmen von Platzproblemen in Aggregaten . . . . .	35
Fehlerbehebung bei ONTAP Volumes mithilfe von Gateway-APIs . . . . .	37
Workflows für das Workload-Management . . . . .	41

# Management von Storage über REST-APIs

## Erste Schritte mit Active IQ Unified Manager

### Zielgruppe für diesen Inhalt

Die folgenden Themen sind für Entwickler bestimmt, die Applikationen erstellen, die über REST-APIs mit der Active IQ Unified Manager Software interface sind.

Storage-Administratoren und -Architekten. Diese Informationen bieten grundlegende Informationen dazu, wie die Unified Manager REST APIs verwendet werden können, um Client-Applikationen zum Managen und Überwachen von NetApp Storage-Systemen zu erstellen.

Sie sollten diese Informationen verwenden, wenn Sie den Storage-Provider, den ONTAP Cluster und Management-Administrations-APIs für das Management Ihres Storage verwenden möchten.

 Sie müssen eine der folgenden Rollen haben: Operator, Storage Administrator oder Application Administrator. Sie müssen die IP-Adresse oder den vollqualifizierten Domänennamen des Unified Manager Servers kennen, auf dem Sie die REST APIs ausführen möchten.

### Active IQ Unified Manager API-Zugriff und Kategorien

Die Active IQ Unified Manager APIs ermöglichen Ihnen das Management und die Bereitstellung von Storage-Objekten in Ihrer Umgebung. Sie können auch auf die Web-Benutzeroberfläche von Unified Manager zugreifen, um einige dieser Funktionen auszuführen.

#### Bauen einer URL für den direkten Zugriff AUF REST-APIs

Sie können die REST-APIs direkt über eine Programmiersprache wie Python, C#, C++, JavaScript, Und so weiter. Geben Sie den Hostnamen oder die IP-Adresse und die URL ein, um auf DIE REST-APIs im Format zuzugreifen

<https://<hostname>/api>

 Der Standardport ist 443. Sie können den Port wie für Ihre Umgebung erforderlich konfigurieren.

#### Zugriff auf die Online-API-Dokumentationsseite

Sie können auf die Seite *API Documentation* Referenzinhalt zugreifen, die zusammen mit dem Produkt verpackt ist, um die API-Dokumentation anzuzeigen, sowie manuell einen API-Aufruf (z. B. Swagger) auszuführen. Sie können diese Dokumentation über das Klicken auf die **Menüleiste > Hilfe-Schaltfläche > API-Dokumentation** aufrufen

Alternativ geben Sie den Hostnamen oder die IP-Adresse und die URL ein, um auf die REST-API-Seite im Format zuzugreifen

<https://<hostname>/docs/api>

## Kategorien

Die API-Aufrufe werden basierend auf den Bereichen oder Kategorien in funktionale Funktionen organisiert. Um eine bestimmte API zu finden, klicken Sie auf die entsprechende API-Kategorie.

DIE REST-APIs von Unified Manager helfen Ihnen bei der Durchführung von Administrations-, Monitoring- und Provisionierungsfunktionen. Die APIs sind in die folgenden Kategorien unterteilt.

- **Rechenzentrum**

Diese Kategorie enthält die APIs, mit denen Sie Ihre Datacenter-Storage-Objekte anzeigen und managen können. Die REST-APIs aus dieser Kategorie liefern Informationen über die Cluster, Nodes, Aggregate, Volumes, LUNs, File Shares, Namespaces und andere Elemente im Datacenter.

- \* Management-Server\*

Die APIs unter der Kategorie **Management-Server** enthalten die `jobs` API: Aufträge sind Vorgänge, die für die asynchrone Ausführung im Zusammenhang mit dem Management von Storage-Objekten oder Workloads auf Unified Manager geplant werden.

- \* Storage-Anbieter\*

Diese Kategorie enthält alle Bereitstellungs-APIs, die Sie für das Management und die Bereitstellung von File Shares, LUNs, Performance Service Levels und Richtlinien zur Storage-Effizienz benötigen. Die APIs ermöglichen außerdem die Konfiguration von Zugriffendpunkten, aktiven Verzeichnissen sowie die Zuweisung von Performance-Service-Leveln und Storage-Effizienzrichtlinien für Storage-Workloads.

## REST-Services in Active IQ Unified Manager angeboten

Vor der Verwendung der Active IQ Unified Manager-APIs sollten Sie sich über DIE REST-Services und -Vorgänge im Klaren sein, die angeboten werden.

Die Bereitstellungs- und Administrations-APIs, die für die Konfiguration des API-Servers verwendet werden, unterstützen die Vorgänge beim Lesen (ABRUFEN) oder Schreiben (POST, PATCH, LÖSCHEN). Im Folgenden sind einige Beispiele für GET-, PATCH-, POST- und LÖSCHVORGÄNGE aufgeführt, die von den APIs unterstützt werden:

- Beispiel FÜR GET: `GET /datacenter/cluster/clusters` Ruft Cluster-Details in Ihrem Datacenter ab. Die maximale Anzahl von Datensätzen, die vom zurückgegeben werden `GET` Der Vorgang ist 1000.



Mithilfe der APIs können Sie die Datensätze nach unterstützten Attributen filtern, sortieren und sortieren.

- Beispiel FÜR POST: `POST /datacenter/svm/svms` Erstellt eine benutzerdefinierte Storage Virtual Machine (SVM)
- Beispiel für PATCH: `PATCH /datacenter/svm/svms/{key}` Ändert die Eigenschaften einer SVM anhand eines eindeutigen Schlüssels.
- Beispiel FÜR LÖSCHEN: `DELETE /storage-provider/access-endpoints/{key}` Löscht einen Zugriffendpunkt von einer LUN, SVM oder Dateifreigabe mithilfe des eindeutigen Schlüssels.

DIE REST-Vorgänge, die mit den APIs ausgeführt werden können, hängen von der Rolle des Operators, des Storage-Administrators oder des Applikationsadministrators ab.

Benutzerrolle	Unterstützte REST-Methode
Operator	Schreibgeschützter Zugriff auf Daten. Benutzer mit dieser Rolle können alle GET-Anforderungen ausführen.
Storage-Administrator	Lesezugriff auf alle Daten. Benutzer mit dieser Rolle können alle GET-Anforderungen ausführen.  Zudem verfügen sie über Schreibzugriff (zur Ausführung VON ANFRAGEN ZU PATCHES und NACH DEM POSTEN und LÖSCHEN), um bestimmte Aktivitäten wie das Management von Storage-Serviceobjekten und Storage-Management-Optionen durchzuführen.
Applikationsadministrator	Lese- und Schreibzugriff auf alle Daten. Benutzer mit dieser Rolle können Anfragen FÜR alle Funktionen ABRUFEN, PATCHEN, VERÖFFENTLICHEN und LÖSCHEN.

Weitere Informationen zu allen REST-Vorgängen finden Sie in der Dokumentation [\\_Online API\\_](#).

## API-Version in Active IQ Unified Manager

DIE REST-API-URIs in Active IQ Unified Manager geben eine Versionsnummer an.

Beispiel: `/v2/datacenter/svm/svms`. Die Versionsnummer `v2` In `/v2/datacenter/svm/svms` Gibt die in einer bestimmten Version verwendete API-Version an. Die Versionsnummer minimiert die Auswirkungen von API-Änderungen auf die Client-Software durch das Senden einer Antwort, die der Client verarbeiten kann.

Der numerische Teil dieser Versionsnummer ist in Bezug auf Releases inkrementell. URIs mit einer Versionsnummer bieten eine konsistente Schnittstelle, die die Abwärtskompatibilität in zukünftigen Versionen beibehalten. Außerdem finden Sie die gleichen APIs auch ohne eine Version, zum Beispiel `/datacenter/svm/svms`, Das gibt die Basis-APIs ohne eine Version an. Die Basis-APIs sind immer die neueste Version der APIs.

 In der rechten oberen Ecke der Swagger-Schnittstelle können Sie die Version der zu verwendenden API auswählen. Die höchste Version ist standardmäßig ausgewählt. Es wird empfohlen, die höchste Version einer bestimmten API (im Hinblick auf die inkrementelle Ganzzahl) zu verwenden, die in der Unified Manager-Instanz verfügbar ist.

Für alle Anforderungen müssen Sie explizit die API-Version anfordern, die Sie verwenden möchten. Wenn die Versionsnummer angegeben ist, gibt der Dienst keine Antwortelemente zurück, die von Ihrer Anwendung nicht behandelt werden sollen. IM RUHEZUSTAND sollten Sie den Versionsparameter enthalten. Die früheren Versionen der APIs sind schließlich nach ein paar Releases veraltet. In diesem Release enthält der `v1` Die Version der APIs ist veraltet.

## Storage-Ressourcen in ONTAP

Die Storage-Ressourcen in ONTAP lassen sich grob in *physische Storage-Ressourcen* und *logische Storage-Ressourcen* klassifizieren. Um Ihre ONTAP-Systeme mit den in Active IQ Unified Manager bereitgestellten APIs effizient zu managen, müssen Sie das Storage-Ressourcenmodell und die Beziehung zwischen den verschiedenen Storage-Ressourcen kennen.

- **Physische Speicherressourcen**

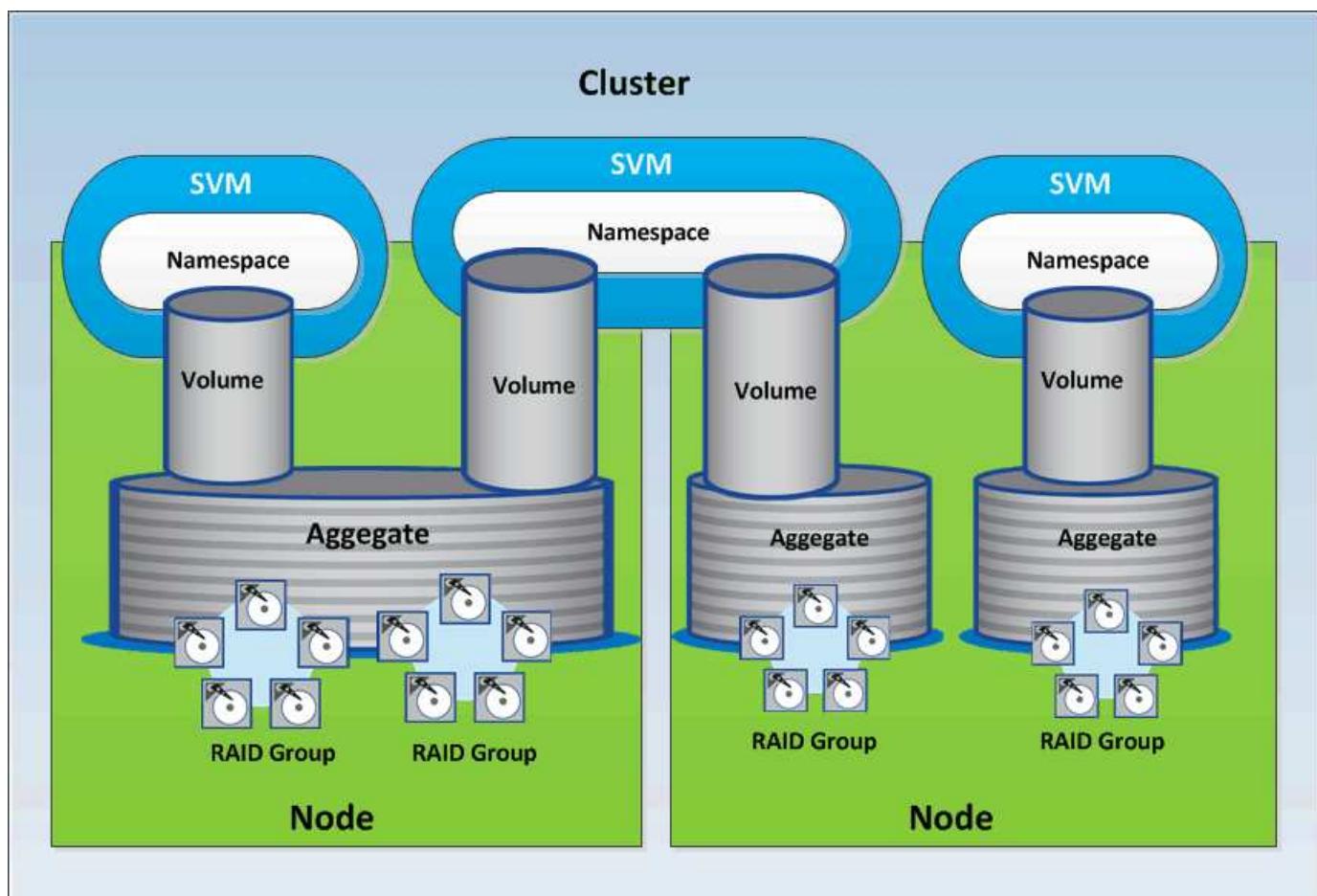
Bezieht sich auf die von ONTAP zur Verfügung gestellten physischen Speicherobjekte. Physische Storage-Ressourcen umfassen Festplatten, Cluster, Storage Controller, Nodes und Aggregate.

- **Logische Speicherressourcen**

Bezieht sich auf die von ONTAP bereitgestellten Storage-Ressourcen, die nicht an eine physische Ressource gebunden sind. Diese Ressourcen werden einer Storage Virtual Machine (SVM, ehemals Vserver) zugewiesen. Sie stehen unabhängig von spezifischen physischen Storage-Ressourcen wie Festplatten, Array-LUNs oder Aggregaten zur Verfügung.

Zu den logischen Storage-Ressourcen zählen Volumes aller Typen und qtrees sowie die Funktionen und Konfigurationen, die in diesen Ressourcen verwendet werden können, beispielsweise Snapshot Kopien, Deduplizierung, Komprimierung und Kontingente.

Die folgende Abbildung zeigt die Storage-Ressourcen in einem 2-Node Cluster:



# REST-API-Zugriff und Authentifizierung in Active IQ Unified Manager

Auf die Active IQ Unified Manager REST API kann über jeden Webbrowser oder eine Programmierplattform zugegriffen werden, um HTTP-Anfragen zu stellen. Unified Manager unterstützt den grundlegenden HTTP-Authentifizierungsmechanismus. Bevor Sie die UNIFIED Manager REST API aufrufen, müssen Sie einen Benutzer authentifizieren.

## REST-Zugriff

Sie können jeden Webbrowser oder jede Programmierplattform verwenden, die HTTP-Anfragen zum Zugriff auf die Unified Manager REST-API ausgeben. Nach der Anmeldung bei Unified Manager können Sie beispielsweise die URL in einen beliebigen Browser eingeben, um die Attribute aller Management-Stationen, wie beispielsweise der Name der Management Station, die Taste und die IP-Adresse, abzurufen.

- Anfrage

GET <https://<IP address/hostame>:<port number>/api/v2/datacenter/cluster/clusters>

- Antwort

```

        "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 Domain-Name (FQDN) des API-Servers.
- Port 443

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

Um HTTP-Anfragen aus einem Webbrower zu veröffentlichen, ZU PATCHEN und ZU LÖSCHEN, müssen Sie Browser-Plugins verwenden. Sie können auch über Skripting-Plattformen 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 ein selbstsigniertes SSL-Zertifikat zur Server-Überprüfung zur Verfügung. Dieses Zertifikat kann durch ein benutzerdefiniertes Zertifikat (oder ein CA-Zertifikat) ersetzt werden.

Sie müssen den Benutzerzugriff auf den API-Server konfigurieren, um die REST-APIs zu aufrufen. Die Benutzer können lokale Benutzer (Benutzerprofile, die in der lokalen Datenbank gespeichert sind) oder LDAP-Benutzer (wenn Sie den API-Server für die Authentifizierung über LDAP konfiguriert haben) sein. Sie können den Benutzerzugriff verwalten, indem Sie sich an der Benutzeroberfläche der Unified Manager Administration Console anmelden.

## In Active IQ Unified Manager verwendete HTTP-Statuscodes

Bei Ausführung der APIs oder bei der Fehlerbehebung sollten Sie die verschiedenen HTTP-Statuscodes und -Fehlercodes kennen, die von Active IQ Unified Manager-APIs verwendet werden.

In der folgenden Tabelle sind die Fehlercodes für die Authentifizierung aufgeführt:

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
200	OK	Wird bei der erfolgreichen Ausführung von synchronen API-Aufrufen zurückgegeben.
201	Erstellt	Erstellung neuer Ressourcen durch synchrone Anrufe, wie z. B. Konfiguration von Active Directory.

HTTP-Statuscode	Titel des Statuscodes	Beschreibung
202	Akzeptiert	Wird bei der erfolgreichen Ausführung von asynchronen Aufrufen für Bereitstellungsfunktionen zurückgegeben, z. B. Erstellen von LUNs und File Shares.
400	Ungültige Anforderung	Zeigt Fehler bei der Eingabevalidierung an. Der Benutzer muss die Eingaben korrigieren, z. B. gültige Schlüssel in einem Anforderungskörper.
401	Nicht autorisierte Anforderung	Sie sind nicht berechtigt, die Ressource/Unbefugte anzuzeigen.
403	Anfrage verweigert	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	Dieser Wert wird zurückgegeben, wenn der Benutzer zu viele Anfragen innerhalb eines bestimmten Zeitraums sendet.
500	Interner Serverfehler	Interner Serverfehler. Fehler beim Abrufen der Antwort vom Server. Dieser interne Serverfehler ist möglicherweise permanent oder nicht permanent. Beispiel: Wenn Sie ein ausführen GET Oder GET ALL Vorgang und Empfang dieses Fehlers. Es wird empfohlen, diesen Vorgang für mindestens fünf Wiederholungen zu wiederholen. Wenn es sich um einen permanenten Fehler handelt, ist der zurückgegebene Statuscode weiterhin 500. Wenn der Vorgang erfolgreich ist, wird der zurückgegebene Statuscode 200 zurückgegeben.

## Empfehlungen für die Verwendung der APIs für Active IQ Unified Manager

Bei Verwendung der APIs in Active IQ Unified Manager sollten Sie bestimmte empfohlene Methoden befolgen.

- Alle Arten von Antwortinhalten müssen für eine gültige Ausführung das folgende Format aufweisen:

application/json

- Die API-Versionsnummer steht nicht zur Produktversionsnummer. Sie sollten die neueste Version der für Ihre Unified Manager Instanz verfügbaren API verwenden. Weitere Informationen zu den Unified Manager API-Versionen finden Sie im Abschnitt „`reST API Versionierung in Active IQ Unified Manager`“.
- Beim Aktualisieren der Array-Werte mithilfe einer Unified Manager API müssen Sie die gesamte Zeichenfolge von Werten aktualisieren. Sie können einem Array keine Werte anhängen. Sie können nur ein vorhandenes Array ersetzen.
- Vermeiden Sie das Abfragen von Objekten, indem Sie eine Kombination aus Wildcard (\*) und Rohr („) des Filterbedieners verwenden. Es kann eine falsche Anzahl von Objekten abrufen.
- Beachten Sie, dass die `GET (Alle)` die Anforderung für eine beliebige API gibt maximal 1000 Datensätze zurück. Auch wenn Sie die Abfrage ausführen, indem Sie die einstellen `max_records` Parameter auf einen Wert über 1000, nur 1000 Datensätze werden zurückgegeben.
- Für administrative Aufgaben wird empfohlen, die Unified Manager-Benutzeroberfläche zu verwenden.

## Protokolle für die Fehlerbehebung

Mithilfe von Systemprotokollen können Sie die Ursachen eines Ausfalls und die Behebung von Problemen analysieren, die bei der Ausführung der APIs auftreten können.

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

Speicherort protokollieren	Nutzung
/var/log/ocie/access_log.log	Enthält alle API-Anrufdetails, z. B. den Benutzernamen des Benutzers, der die API aufruft, Startzeit, Ausführungszeit, Status und URL.  In dieser Protokolldatei können Sie die häufig verwendeten APIs überprüfen oder einen Fehler in jedem GUI-Workflow beheben. Sie können die Analyse auch anhand der Ausführungszeit skalieren.
/var/log/ocum/ocumserver.log	Enthält alle API-Ausführungsprotokolle.  Sie können diese Protokolldatei zur Fehlerbehebung und Fehlersuche bei API-Aufrufen verwenden.

Speicherort protokollieren	Nutzung
/var/log/ocie/server.log	<p>Enthält alle WildFly-Server-Bereitstellungen und Start/Stop-Service-bezogene Protokolle.</p> <p>Mithilfe dieser Protokolldatei können Sie die Ursache von Problemen ermitteln, die während des Starts, Stopps oder der Bereitstellung des Wildfly-Servers auftreten.</p>
/var/log/ocie/au.log	<p>Enthält Protokolle für die Erfassungseinheit.</p> <p>Sie können diese Protokolldatei verwenden, wenn Sie Objekte in ONTAP erstellt, geändert oder gelöscht haben, sie sich jedoch nicht für die Active IQ Unified Manager REST-APIs wiederspiegeln.</p>

## 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 enthält grundlegende Details zum API-Server im JSON-Format (nur der Server unterstützt `application/json` Format).

Der verwendete URI ist: <https://<hostname>/api/datacenter/svm/svms>. Dieser Beispielcode nimmt die folgenden Eingabeparameter auf:

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

Um REST-APIs aufzurufen, 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 Überlegungen zum Beispielcode:

- Verwendet eine HTTPS-Verbindung zu Active IQ Unified Manager, um den angegebenen REST-URI aufzurufen
- Ignoriert das von Active IQ Unified Manager bereitgestellte Zertifikat
- Überspringt die Überprüfung des Host-Namens während des Handshakes
- Verwendet `javax.net.ssl.HttpsURLConnection` Für eine URI-Verbindung
- Verwendet eine Bibliothek eines Drittanbieters (`org.apache.commons.codec.binary.Base64`) Für die Erstellung der Base64 kodierten Zeichenfolge in der HTTP-Grundauthentifizierung verwendet

Um den Beispielcode kompilieren und ausführen zu können, müssen Sie 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.HttpsURLConnection;
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 HttpsURLConnection
getAllTrustingHttpsURLConnection() {           HttpsURLConnection conn =
null;           try {           /* Creating a trust manager that does not
validate certificate chains */           TrustManager[]
trustAllCertificatesManager = 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() {
        boolean verify(String host, SSLSession
        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;
    }

}

```

## Unified Manager REST-APIs

DIE REST-APIs für Active IQ Unified Manager sind in diesem Abschnitt basierend auf ihren Kategorien aufgeführt.

Sie können die Online-Dokumentationsseite von Ihrer Unified Manager Instanz aus einsehen, die alle Einzelheiten zu jedem REST-API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder API-Aufruf, der in diesem Dokument aufgeführt oder beschrieben wird, enthält nur die Informationen, die Sie benötigen, um den Anruf auf der Dokumentationsseite zu finden. Nach dem Auffinden eines bestimmten API-Aufrufs können Sie die vollständigen Details dieses Anrufs überprüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und der Anforderungstypen.

Für jeden API-Aufruf in einem Workflow sind folgende Informationen enthalten, um den Anruf auf der Dokumentationsseite zu finden:

- Kategorie

Die API-Aufrufe werden auf der Dokumentationsseite in funktional bezogene Bereiche oder Kategorien unterteilt. Um einen bestimmten API-Aufruf zu finden, scrollen Sie nach unten auf der Seite und klicken Sie dann auf die entsprechende API-Kategorie.

- HTTP-Verb (Anruf)

Das HTTP-Verb identifiziert die Aktion, die für eine Ressource durchgeführt wird. Jeder API-Aufruf wird über ein einziges HTTP-Verb ausgeführt.

- Pfad

Der Pfad bestimmt die spezifische Ressource, die die Aktion als Teil der Durchführung eines Anrufs verwendet. Der Pfadstring wird an die Core-URL angehängt, um die vollständige URL zur Identifizierung der Ressource zu bilden.

## APIs für das Management von Datacentern

Die REST-APIs unter datacenter Kategorie stellt Informationen über die Cluster, Nodes, Aggregate, Volumes, LUNs, Fileshares, Namespaces und andere Elemente in

Ihrem Datacenter. Diese APIs sind für das Abfragen, Hinzufügen, Löschen oder Ändern der Konfiguration in Ihrem Datacenter verfügbar.

Die meisten dieser APIs sind GET-Aufrufe, die Cluster-übergreifende Aggregation mit Filter-, Sortier- und Paginierungsunterstützung bieten. Wenn sie diese APIs ausführen, geben sie Daten aus der Datenbank zurück. Daher müssen die neu erstellten Objekte durch den nächsten Erfassungszyklus entdeckt werden, damit sie in der Antwort angezeigt werden.

Wenn Sie die Details eines bestimmten Objekts abfragen möchten, müssen Sie die eindeutige ID dieses Objekts eingeben, um dessen Details anzuzeigen. Beispiel:

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters/4c6bf721-2e3f-11e9-a3e2-00a0985badbb" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

 Die CURL-Befehle, Beispiele, Anfragen und Antworten auf die APIs sind auf Ihrer Swagger API-Schnittstelle verfügbar. Sie können die Ergebnisse nach bestimmten Parametern filtern und sortieren, wie auf Swagger angegeben. Diese APIs ermöglichen die Filterung der Ergebnisse nach spezifischen Storage-Objekten wie Cluster, Volume oder Storage VM.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/cluster/clusters	Mit dieser Methode können Sie Details zu den ONTAP Clustern im gesamten Datacenter anzeigen.
	/datacenter/cluster/clusters/{key}	
GET	/datacenter/cluster/nodes	Mit dieser Methode können Sie die Details der Nodes im Datacenter anzeigen.
	/datacenter/cluster/nodes/{key}	
GET	/datacenter/protocols/cifs/shares	Mit dieser Methode können Sie Details zu den CIFS-Freigaben im Datacenter anzeigen.
	/datacenter/protocols/cifs/shares/{key}	

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/protocols/nfs/export-policies  /datacenter/protocols/nfs/export-policies/{key}	<p>Sie können diese Methode verwenden, um die Details der Exportrichtlinien für die unterstützten NFS-Dienste anzuzeigen.</p> <p>Sie können die Exportrichtlinien für eine Cluster- oder Storage-VM abfragen und den Richtlinienschlüssel für den Export zur Bereitstellung von NFS-Dateifreigaben verwenden. Weitere Informationen über das Zuweisen und erneute Verwenden von Exportrichtlinien für Workloads finden Sie unter „Provisioning von CIFS- und NFS-Dateifreigaben“.</p>
GET	/datacenter/storage/aggregates  /datacenter/storage/aggregates/{key}	Mit dieser Methode können Sie die Erfassung von Aggregaten im gesamten Datacenter einsehen, um Workloads darauf bereitzustellen oder das Monitoring zu überwachen.
GET	/datacenter/storage/luns  /datacenter/storage/luns/{key}	Mit dieser Methode können Sie die Erfassung von LUNs im gesamten Datacenter anzeigen.
GET	/datacenter/storage/qos/policies  /datacenter/storage/qos/policies/{key}	Mithilfe dieser Methode können Sie alle Details zu allen QoS-Richtlinien im Datacenter anzeigen und die Richtlinien nach Bedarf anwenden.
GET	/datacenter/storage/qtrees  /datacenter/storage/qtrees/{key}	Mit dieser Methode können Sie die qtree-Details im gesamten Datacenter anzeigen.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/storage/volumes  /datacenter/storage/volumes/{key}	Mit dieser Methode können Sie die Volume-Sammlungen im Datacenter anzeigen.
GET  POST  DELETE  PATCH	/datacenter/protocols/san/igroups  /datacenter/protocols/san/igroups/{key}	<p>Sie können Initiatorgruppen zuweisen, die für den Zugriff auf bestimmte LUN-Ziele autorisiert sind. Wenn eine vorhandene Initiatorgruppe vorhanden ist, können Sie sie zuweisen. Sie können auch Initiatorgruppen erstellen und sie den LUNs zuweisen.</p> <p>Sie können diese Methoden zum Abfragen, Erstellen, Löschen und Ändern von Initiatorgruppen verwenden.</p> <p>Hinweise:</p> <ul style="list-style-type: none"> <li>• POST: Beim Erstellen einer Initiatorgruppe können Sie die Speicher-VM angeben, auf der Sie Zugriff zuweisen möchten.</li> <li>• DELETE: Sie müssen den igroup-Schlüssel als Eingabeparameter angeben, um eine bestimmte igroup zu löschen. Wenn Sie einer LUN bereits eine Initiatorgruppe zugewiesen haben, können Sie diese Initiatorgruppe nicht löschen.</li> <li>• PATCH: Sie müssen den igroup-Schlüssel als Eingabeparameter angeben, um eine bestimmte igroup zu ändern. Sie müssen auch die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.</li> </ul>

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/svm/svms	Sie können diese Methoden verwenden, um Storage Virtual Machines (Storage VMs) anzuzeigen, zu erstellen, zu löschen und zu ändern.
POST	/datacenter/svm/svms/{key}	Hinweise: <ul style="list-style-type: none"><li>• POST: Sie müssen das Speicher-VM-Objekt eingeben, das Sie als Eingabeparameter erstellen möchten. Sie können eine benutzerdefinierte Storage-VM erstellen und anschließend erforderliche Eigenschaften zuweisen.</li></ul>
DELETE		 Wenn Sie die SLO-basierte Workload-Bereitstellung auf Ihrer Umgebung aktiviert und gleichzeitig die Storage VM erstellt haben, müssen Sie sicherstellen, dass alle Protokolle unterstützt werden, die für die Bereitstellung von LUNs und Dateifreigaben erforderlich sind, z. B. SMB/CIFS, NFS, FCP Und iSCSI. Die Bereitstellungs-Workflows können fehlschlagen, wenn die Storage-VM die erforderlichen Services nicht unterstützt. Es wird empfohlen, auf der Storage-VM auch die Services für die jeweiligen Workload-Typen zu aktivieren.
PATCH		 • DELETE: Sie müssen den Speicher-VM-Schlüssel bereitstellen, um eine bestimmte Speicher-VM zu löschen.
		 Wenn Sie die SLO-basierte Workload-Bereitstellung in Ihrer Umgebung aktiviert haben, kann diese Storage-VM nicht gelöscht werden, auf der Storage-Workloads bereitgestellt wurden. Wenn Sie eine Speicher-VM löschen, auf der ein CIFS/SMB-Server konfiguriert wurde, löscht diese API auch den CIFS/SMB-Server und die lokale Active Directory-Konfiguration. Der CIFS/SMB-Servername befindet sich jedoch weiterhin in der Active Directory-Konfiguration, die Sie manuell vom Active Directory-Server löschen müssen.
		 • PATCH: Sie müssen den Speicher-VM-Schlüssel zur Änderung einer bestimmten Speicher-VM zur Verfügung stellen. Sie müssen außerdem die Eigenschaften eingeben, die Sie aktualisieren möchten, zusammen mit ihren Werten.

## Gateway-APIs

Die Gateway-APIs bieten den Vorteil, dass Sie die Active IQ Unified Manager-Zugangsdaten verwenden können, um ONTAP REST-APIs und das Management von Storage-Objekten auszuführen. Diese APIs sind verfügbar, wenn die API-Gateway-Funktion über die Web-UI von Unified Manager aktiviert ist.

Unified Manager REST-APIs unterstützen nur einen ausgewählten Satz von Aktionen, die auf den Daten von Unified Manager ausgeführt werden sollen, d. h. ONTAP Cluster. Sie können die anderen Funktionen über ONTAP APIs nutzen. Durch die Gateway-APIs ist Unified Manager eine Pass-Through-Schnittstelle zum Tunneln aller API-Anfragen, die auf ONTAP Clustern ausgeführt werden sollen, ohne sich einzeln an die einzelnen Datacenter-Cluster anzumelden. Sie arbeitet als zentraler Managementpunkt bei der Ausführung der APIs auf den ONTAP Clustern, die von Ihrer Unified Manager Instanz gemanagt werden. Dank der API Gateway-Funktion kann Unified Manager als zentrale Managementoberfläche eingerichtet werden, über die Sie diverse ONTAP Cluster managen können, ohne sich dabei individuell anmelden zu müssen. Die Gateway-APIs ermöglichen es Ihnen, bei Unified Manager angemeldet zu bleiben und die ONTAP-Cluster zu managen, indem Sie ONTAP REST-API-Vorgänge ausführen.



Alle Benutzer können eine Abfrage mithilfe der ausführen GET Betrieb.  
Applikationsadministratoren können alle REST-Operationen für ONTAP ausführen.

Das Gateway fungiert als Proxy, um die API-Anforderungen zu Tunneln, indem die Header- und Body-Anfragen im gleichen Format wie in den ONTAP-APIs beibehalten werden. Kunden können ihre Unified Manager Anmelddaten verwenden und bestimmte Vorgänge ausführen, um ohne die individuellen Cluster-Anmelddaten zuzugreifen und das Management der ONTAP Cluster durchzuführen. Die Cluster-Authentifizierung und das Cluster-Management werden weiterhin gemanagt, allerdings werden die API-Anfragen umgeleitet, damit sie direkt auf dem spezifischen Cluster ausgeführt werden. Die Antwort der APIs ist die gleiche wie die Antwort, die von den jeweiligen ONTAP REST APIs zurückgegeben wird, die direkt von ONTAP ausgeführt werden.

HTTP-Verb	Pfad (URL)	Beschreibung
GET	/gateways	<p>Diese GET-Methode ruft die Liste aller von Unified Manager verwalteten Cluster ab, die Rest-Aufrufe von ONTAP unterstützen. Sie können die Cluster-Details überprüfen und auswählen, ob andere Methoden auf Basis der Cluster-UUID oder Universal Unique Identifier (UUID) ausgeführt werden sollen.</p> <p> Die Gateway-APIs rufen nur die von ONTAP 9.5 oder höher unterstützten Cluster ab und sind über HTTPS zu Unified Manager hinzugefügt.</p>

HTTP-Verb	Pfad (URL)	Beschreibung
GET	/gateways/{uuid}/{path}	Dies ist eine Single-Point-Proxy-API, die DEN POST- und LÖSCHVORGANG sowie DEN PATCH-Betrieb und DEN ZUGRIFF auf alle ONTAP REST-APIs unterstützt. Es gelten keine Einschränkungen für die API, sofern sie von ONTAP unterstützt wird. Die Tunneling- oder Proxy-Funktion kann nicht deaktiviert werden.
POST		
DELETE		
PATCH		
OPTIONS (Nicht verfügbar bei Swagger)		
HEAD (Nicht verfügbar bei Swagger)		<p>Der Wert für {uuid} Muss durch die Cluster-UUID ersetzt werden, für die der REST-Vorgang ausgeführt werden soll. Stellen Sie außerdem sicher, dass die UUID von dem Cluster gehört, das von ONTAP 9.5 oder höher unterstützt wird, und dass es über HTTPS zu Unified Manager hinzugefügt wird.</p> <p>{path} Muss durch die ONTAP REST-URL ersetzt werden. Sie müssen entfernen /api/ Über die URL anzeigen.</p>

## Allgemeines zum API-Gateway-Tunneling

Mithilfe der Gateway-APIs können Sie ONTAP-Objekte über Unified Manager managen. Unified Manager verwaltet die Cluster- und Authentifizierungsdetails und leitet die Anfragen an den REST-Endpunkt von ONTAP weiter. Die Gateway-API wandelt die URL und Hypermedia als Engine of Application State (HATEOAS)-Links im Header und Response Body mit der API-Gateway-Basis-URL um. Die Gateway-API fungiert als Proxy-Basis-URL, an die Sie die ONTAP-REST-URL anhängen und den erforderlichen ONTAP-REST-Endpunkt ausführen.

In diesem Beispiel lautet die Gateway-API (Proxy-Basis-URL): /gateways/{uuid}/

Die ONTAP-API wird verwendet: /storage/volumes. Sie müssen die Rest-URL der ONTAP-API als Wert für die hinzufügen path Parameter.



Stellen Sie beim Hinzufügen des Pfads sicher, dass Sie den „` entfernt haben/“ symbol at the beginning of the URL. For the API `/storage/volumes, Hinzufügen storage/volumes.

Die angehängte URL lautet: /gateways/{uuid}/storage/volumes

Bei Ausführung der GET Die generierte URL ist die folgende Operation:

GET https://<hostname>/api/gateways/<cluster\_UUID>/storage/volumes

Der /api Das Tag der ONTAP REST-URL wird in der angehängten URL entfernt und das für die Gateway-API beibehalten wird.

### **Befehl zum Curl-Beispiel**

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

Die API gibt die Liste der Storage Volumes in diesem Cluster zurück. Das Antwortformat entspricht dem, das Sie erhalten, wenn Sie dieselbe API von ONTAP ausführen. Die zurückgegebenen Statuscodes sind die ONTAP-REST-Statuscodes.

### **API-Umfang wird festgelegt**

Alle APIs weisen einen Kontext im Umfang des Clusters auf. APIs, die auf Storage-VMs basieren, haben auch den Cluster als Umfang, das heißt, die API-Vorgänge werden auf einer bestimmten Storage-VM innerhalb eines gemanagten Clusters ausgeführt. Wenn Sie den ausführen /gateways/{uuid}/{path} API, stellen Sie sicher, dass Sie die Cluster-UUID (Unified Manager Datasource UUID) für das Cluster eingeben, auf dem Sie den Vorgang ausführen. Um den Kontext für eine bestimmte Storage-VM in diesem Cluster einzustellen, geben Sie den Schlüssel für die Storage-VM als ein X-Dot-SVM-UUID Parameter oder der Name der Storage-VM als X-Dot-SVM-Name Parameter. Der Parameter wird als Filter im String-Header hinzugefügt und der Vorgang wird im Rahmen dieser Storage-VM innerhalb dieses Clusters ausgeführt.

### **Befehl zum Curl-Beispiel**

```
curl -X GET "https://<hostname>/api/gateways/e4f33f90-f75f-11e8-9ed9-00a098e3215f/storage/volume" -H "accept: application/hal+json" -H "X-Dot-SVM-UUID: d9c33ec0-5b61-11e9-8760-00a098e3215f" -H "Authorization: Basic <Base64EncodedCredentials>"
```

Weitere Informationen zur Verwendung von ONTAP REST-APIs finden Sie unter "[ONTAP REST-API-AUTOMATISIERUNG](#)".

## **Administrations-APIs**

Sie können die APIs unter verwenden `administration` Kategorie zum Ändern der Backup-Einstellungen, zur Überprüfung der Backup-Dateiinformationen und der Cluster-Zertifikate und zum Verwalten von ONTAP Clustern als Active IQ Unified Manager

## Datenquellen



Sie müssen die Anwendungsadministratorrolle besitzen, um diese Vorgänge ausführen zu können. Sie können diese Einstellungen auch über die Web-Benutzeroberfläche von Unified Manager konfigurieren.

HTTP-Verb	Pfad	Beschreibung
GET	/admin/backup-settings	Sie können das verwenden <code>GET</code> Methode zum Anzeigen der Einstellungen des in Unified Manager konfigurierten Backup-Zeitplans. Sie können Folgendes überprüfen:
PATCH	/admin/backup-settings	<ul style="list-style-type: none"><li>• Gibt an, ob der Zeitplan aktiviert oder deaktiviert ist</li><li>• Häufigkeit des geplanten Backups (täglich oder wöchentlich)</li><li>• Zum Zeitpunkt des Backups</li><li>• Maximale Anzahl an Backup-Dateien, die in der Applikation aufbewahrt werden sollen</li></ul> <p>Die Zeit des Backups befindet sich in der Server-Zeitzone.</p> <p>Die Backup-Einstellungen für die Datenbank sind standardmäßig in Unified Manager verfügbar, und Sie können keinen Backup-Zeitplan erstellen. Sie können jedoch die verwenden <code>PATCH</code> Methode zum Ändern der Standardeinstellungen.</p>
GET	/admin/backup-file-info	Eine Backup Dump-Datei wird jedes Mal erzeugt, wenn der Backup-Zeitplan für Unified Manager geändert wird. Mit dieser Methode können Sie überprüfen, ob die Sicherungsdatei gemäß den geänderten Backup-Einstellungen generiert wird und ob die Informationen in der Datei mit den geänderten Einstellungen übereinstimmen.

HTTP-Verb	Pfad	Beschreibung
GET	/admin/datasource-certificate	Sie können diese Methode verwenden, um das Datasource (Cluster)-Zertifikat aus dem Trust Store anzuzeigen. Bevor Sie ein ONTAP Cluster als Unified Manager-Datenquelle hinzufügen, ist eine Überprüfung des Zertifikats erforderlich.
GET	/admin/datasources/clusters	Sie können das verwenden GET Methode zum Abrufen der Details der Datenquellen (ONTAP Cluster), die von Unified Manager verwaltet werden.
POST	/admin/datasources/clusters/{key}	Sie können auch ein neues Cluster zu Unified Manager als Datenquelle hinzufügen. Zum Hinzufügen eines Clusters müssen Sie seinen Host-Namen, seinen Benutzernamen und sein Passwort kennen.
PATCH		
DELETE		Verwenden Sie den ONTAP-Clusterschlüssel zum Ändern und Löschen eines von Unified Manager als Datenquelle gemanagten Clusters.

## Sicherheits-APIs

Sie können die APIs in verwenden `security` Kategorie, um den Benutzerzugriff auf ausgewählte Clusterobjekte in Active IQ Unified Manager zu steuern. Sie können lokale Benutzer oder Datenbankbenutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Basierend auf den Berechtigungen der Rollen, die Sie den Benutzern zuweisen, können sie die Speicherobjekte verwalten oder die Daten in Unified Manager anzeigen.



Sie müssen die Anwendungsadministratorrolle besitzen, um diese Vorgänge ausführen zu können. Sie können diese Einstellungen auch über die Web-Benutzeroberfläche von Unified Manager konfigurieren.

Die APIs unter `security` Verwenden Sie die Kategorie `users` Parameter, das ist der Benutzername, und nicht der `key` Parameter als eindeutige Kennung für die Benutzereinheit.

HTTP-Verb	Pfad	Beschreibung
GET POST	/security/users /security/users	<p>Sie können diese Methoden verwenden, um Details zu Benutzern anzuzeigen oder neue Benutzer zu Unified Manager hinzuzufügen.</p> <p>Sie können den Benutzern basierend auf ihren Benutzertypen bestimmte Rollen hinzufügen. Beim Hinzufügen von Benutzern müssen Sie Passwörter für den lokalen Benutzer, den Wartungsbenuutzer und den Datenbankbenutzer bereitstellen.</p>
GET PATCH DELETE	/security/users/{name}	<p>Der GET Mit der Methode können Sie alle Details eines Benutzers abrufen, z. B. Name, E-Mail-Adresse, Rolle und Berechtigungstyp. Der PATCH Mit der Methode können Sie die Details aktualisieren. Der DELETE Mit der Methode können Sie den Benutzer entfernen.</p>

## API und asynchrone Prozesse für Job-Objekte

Die Kategorie Management-Server besteht aus der Jobs-API, die Informationen über die Jobs liefert, die während der Ausführung von Active IQ Unified Manager-APIs ausgeführt werden. Sie müssen wissen, wie die asynchrone Verarbeitung mit dem Job-Objekt funktioniert.

Einige der API-Aufrufe, insbesondere solche, die zum Hinzufügen oder Ändern von Ressourcen verwendet werden, können länger dauern als andere Anrufe. Unified Manager verarbeitet diese langfristigen Anforderungen asynchron.

### Asynchrone Anforderungen, die mit Job Object beschrieben werden

Nach einem API-Aufruf, der asynchron ausgeführt wird, weist der HTTP-Antwortcode 202 darauf hin, dass die Anforderung erfolgreich validiert und akzeptiert, aber noch nicht abgeschlossen wurde. Die Anforderung wird als Hintergrundaufgabe verarbeitet, die nach der ersten HTTP-Antwort auf den Client weiter ausgeführt wird. Die Antwort umfasst das Job-Objekt, das die Anfrage einschließlich der eindeutigen Kennung anverankert.

### Abfragen des mit einer API-Anforderung verknüpften Jobobjekts

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

- NORMAL

- WARNING
- PARTIAL\_FAILURES
- ERROR

Es gibt zwei Verfahren, die Sie beim Abfragen eines Jobobjekts verwenden können, um einen Terminalstatus für die Aufgabe zu erkennen: Erfolg oder Fehler:

- Standard-Abfrage: Der aktuelle Job-Status wird sofort zurückgegeben.
- Lange Abfrage: Wenn der Job-Status zu bewegt NORMAL, ERROR, Oder PARTIAL\_FAILURES.

### Schritte in einer asynchronen Anforderung

Sie können den folgenden grundlegenden Vorgang verwenden, um einen asynchronen API-Aufruf abzuschließen:

1. Geben Sie den asynchronen API-Aufruf aus.
2. Sie erhalten eine HTTP-Antwort 202, die darauf hinweist, dass die Anfrage erfolgreich angenommen wurde.
3. Extrahieren Sie die Kennung für das Job-Objekt aus dem Antwortkörper.
4. Warten Sie in einer Schleife, bis das Objekt Job den Terminalstatus erreicht hat NORMAL, ERROR, Oder PARTIAL\_FAILURES.
5. Überprüfen Sie den Terminalstatus des Jobs, und rufen Sie das Jobergebnis ab.

### Anzeigen Von Jobs

Im Active IQ Unified Manager werden Vorgänge wie das Hinzufügen und Ändern von Ressourcen durch synchrone und asynchrone API-Aufrufe durchgeführt. Aufrufe, die für die asynchrone Ausführung geplant sind, können von einem für diesen Aufruf erstellten Jobobjekt nachverfolgt werden. Jedes Jobobjekt verfügt über einen eindeutigen Schlüssel zur Identifizierung. Jedes Job-Objekt gibt die Job-Objekt-URI zurück, mit der Sie auf den Fortschritt des Jobs zugreifen und diesen verfolgen können. Sie können diese API zum Abrufen der Details jeder Ausführung verwenden.

Sie können alle Job-Objekte abfragen. Sie können auch die Job Key- und Job-Objektdetails verwenden, um die nächsten Vorgänge für die Ressourcen auszuführen.

#### Jobs anzeigen

Sie können diese Methode verwenden, um eine Liste aller Jobs zu erhalten. Der Antwortkörper besteht aus den Jobdetails aller Jobs. Sie können die Details eines bestimmten Job-Objekts auch anzeigen, indem Sie den Job-Schlüssel in der URI angeben. Der Antwortkörper besteht aus den Details, die durch die Taste Job identifiziert werden. In der Antwort wird das neueste Jobobjekt an die Spitze zurückgegeben. Wenn Sie ein bestimmtes Jobobjekt abfragen möchten, geben Sie die Job-ID des Jobs ein.

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management-server/jobs /management-server/jobs/{key}

## APIs für das Management von Workloads

Die hier beschriebenen APIs decken verschiedene Funktionen der Storage-Administration ab, z. B. das Anzeigen von Storage Workloads, das Erstellen von LUNs und Dateifreigaben, das Management von Performance Service Levels und Richtlinien für Storage-Effizienz sowie die Zuweisung von Richtlinien zu Storage Workloads.

### Anzeigen von Storage-Workloads

Mit den hier aufgeführten APIs können Sie eine konsolidierte Liste von Storage-Workloads für alle ONTAP Cluster im Datacenter anzeigen. Die APIs bieten auch eine Übersicht über die Anzahl der in Ihrer Active IQ Unified Manager Umgebung bereitgestellten Storage Workloads und ihre Kapazitäts- und IOPS-Statistiken (Performance).

### Anzeige von Storage-Workloads

Mithilfe der folgenden Methode können Sie alle Storage-Workloads in allen Clustern in Ihrem Datacenter anzeigen. Informationen zum Filtern der Antwort auf der Grundlage bestimmter Spalten finden Sie in der API-Referenzdokumentation, die in Ihrer Unified Manager Instanz verfügbar ist.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/workloads

### Anzeigen der Zusammenfassung der Speicher-Workloads

Anhand der folgenden Methode können Sie die genutzte Kapazität, verfügbare Kapazität, genutzte IOPS, verfügbare IOPS und Anzahl der von den einzelnen Performance-Service-Level gemanagten Storage Workloads bewerten. Die angezeigten Storage Workloads können für jede LUN, jede NFS-Dateifreigabe oder jede CIFS-Freigabe sein. Die API gibt einen Überblick über Storage-Workloads, einen Überblick über die vom Unified Manager bereitgestellten Storage-Workloads, eine Datacenter-Übersicht, eine Übersicht über die Gesamtzahl der verwendeten sowie den verfügbaren Speicherplatz und die IOPS im Datacenter, im Hinblick auf die zugewiesenen Performance-Service-Level. Die als Antwort auf diese API erhaltenen Informationen werden verwendet, um das Dashboard in die Benutzeroberfläche von Unified Manager einzufüllen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/workloads-summary

## Management von Zugriffendpunkten

Zugriffendpunkte oder logische Schnittstellen (LIFs) müssen erstellt werden, die für die Bereitstellung von Storage Virtual Machines (SVMs), LUNs und Dateifreigaben erforderlich sind. Sie können die Zugriffendpunkte für die SVMs, LUNs oder File Shares in der Active IQ Unified Manager Umgebung anzeigen, erstellen, ändern und löschen.

### Zugriffendpunkte anzeigen

Sie können eine Liste der Zugriffendpunkte in Ihrer Unified Manager-Umgebung mithilfe der folgenden Methode anzeigen. Um eine Liste der Zugriffendpunkte einer bestimmten SVM, LUN oder Dateifreigabe abzufragen, müssen Sie die eindeutige Kennung für die SVM, die LUN oder die Dateifreigabe eingeben. Sie können auch die eindeutige Taste für den Zugriffendpunkt eingeben, um die Details des jeweiligen Zugriffendpunkts abzurufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

### Fügen Sie Zugriffendpunkte hinzu

Sie können benutzerdefinierte Zugriffendpunkte erstellen und erforderliche Eigenschaften ihm zuweisen. Sie müssen die Details des Zugriffendpunkts eingeben, den Sie als Eingabeparameter erstellen möchten. Sie können diese API oder die System Manager- oder ONTAP-CLI verwenden, um auf jedem Node einen Zugriffsknoten zu erstellen. Für die Erstellung von Zugriffendpunkten werden sowohl IPv4- als auch IPv6-Adressen unterstützt.



Sie müssen Ihre SVM für die erfolgreiche Bereitstellung von LUNs und Dateifreigaben mit einer Mindestanzahl an Zugriffendpunkten pro Node konfigurieren. Sie sollten Ihre SVM mit mindestens zwei Zugriffendpunkten pro Node konfigurieren, die jeweils ein CIFS- und/oder NFS-Protokoll unterstützen, ein weiteres iSCSI- oder FCP-Protokoll.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/access-endpoints

### Zugriffsendpunkte löschen

Sie können einen bestimmten Zugriffendpunkt mithilfe der folgenden Methode löschen. Zum Löschen eines bestimmten Zugriffsparameters muss der Schlüssel für den Zugriffendpunkt als Eingabeparameter bereitgestellt werden.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	/storage-provider/access-endpoints/{key}

#### Zugriffsendpunkte ändern

Sie können einen Zugriffendpunkt ändern und seine Eigenschaften mithilfe der folgenden Methode aktualisieren. Zur Änderung eines bestimmten Zugriffendpunkts müssen Sie den Schlüssel für den Zugriffendpunkt angeben. Sie müssen außerdem die Eigenschaft eingeben, die Sie aktualisieren möchten, zusammen mit ihrem Wert.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	/storage-provider/access-endpoints/{key}

#### Verwalten der Active Directory-Zuordnung

Mithilfe der hier aufgeführten APIs können Sie die Active Directory-Zuordnungen auf der SVM managen, die für die Bereitstellung von CIFS-Freigaben auf den SVMs erforderlich sind. Active Directory-Zuordnungen müssen konfiguriert werden, um die SVMs mit ONTAP zuzuordnen.

#### Anzeigen von Active Directory-Zuordnungen

Sie können die Konfigurationsdetails der Active Directory-Zuordnungen für eine SVM über die folgende Methode anzeigen. Um die Active Directory-Zuordnungen auf einer SVM anzuzeigen, müssen Sie den SVM-Schlüssel eingeben. Um die Details einer bestimmten Zuordnung abfragen zu können, müssen Sie den Zuordnungsschlüssel eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/active-directories-mappings /storage-provider/active-directories-mappings/{key}

#### Fügen Sie die Active Directory-Zuordnung hinzu

Sie können Active Directory-Zuordnungen auf einer SVM mit der folgenden Methode erstellen. Sie müssen die Zuordnungsdetails als Eingabeparameter eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/active-directories-mappings

## Verwalten von Dateifreigaben

Über die hier aufgeführten APIs können CIFS-Freigaben und NFS-Dateifreigaben angezeigt, hinzugefügt und gelöscht werden. Mithilfe dieser APIs können Sie auch die Richtlinien für Performance Service Level und Storage-Effizienz für die Dateifreigaben zuweisen und ändern.

Vor dem Zuweisen von Storage muss die Virtual Machine mit den unterstützten Protokollen erstellt und bereitgestellt werden. Ebenso müssen die Storage-Effizienz-Richtlinien für die Zuweisung von Storage-Effizienz-Richtlinien zu File Shares erstellt werden, bevor Dateifreigaben erstellt werden können.

### Anzeigen von Dateifreigaben

Anhand der folgenden Methode können Sie alle in Ihrer Unified Manager Umgebung verfügbaren Storage Workloads anzeigen. Wenn Sie ein ONTAP Cluster als Datenquelle auf Active IQ Unified Manager hinzugefügt haben, werden die Storage-Workloads für diese Cluster automatisch Ihrer Unified Manager Instanz hinzugefügt. Diese API ruft alle Dateifreigaben automatisch ab und wird manuell Ihrer Unified Manager-Instanz hinzugefügt. Sie können die Details einer bestimmten Dateifreigabe anzeigen, indem Sie diese API mit dem Dateifreigabschlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/file-shares /storage-provider/file-shares/{key}

### Fügen Sie Dateifreigaben hinzu

Mit der folgenden Methode können Sie CIFS- und NFS-Dateifreigaben in Ihre SVM hinzufügen. Als Eingabeparameter müssen Sie die Details der Dateifreigabe eingeben, die Sie erstellen möchten. Sie können diese API nicht zum Erstellen von FlexGroups verwenden.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/file-shares



Je nachdem, ob die Parameter der Zugriffssteuerungsliste (ACL) oder der Parameter für die Exportrichtlinie zur Verfügung gestellt werden, werden CIFS-Shares oder NFS-Dateifreigaben erstellt. Wenn Sie die Werte für die ACL-Parameter nicht angeben, werden CIFS-Shares nicht erstellt und NFS-Shares werden standardmäßig erstellt, um Zugriff auf alle zu ermöglichen.

### Löschen von Dateifreigaben

Sie können die folgende Methode verwenden, um eine bestimmte Dateifreigabe zu löschen. Zum Löschen einer bestimmten Dateifreigabe müssen Sie den Freigabeschlüssel als Eingabeparameter eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	/storage-provider/file-shares/{key}

### Ändern von Dateifreigaben

Sie können die folgende Methode verwenden, um eine Dateifreigabe zu ändern und deren Eigenschaften zu aktualisieren.

Sie müssen den Dateifreigabschlüssel angeben, um eine bestimmte Dateifreigabe zu ändern. Außerdem müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.



Beachten Sie, dass Sie nur eine Eigenschaft bei einem einzelnen Aufruf dieser API aktualisieren können. Für mehrere Updates müssen Sie diese API so oft ausführen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	/storage-provider/file-shares/{key}

### Verwalten von LUNs

Mit den hier aufgeführten APIs können Sie LUNs auf den Storage Virtual Machines (Storage VMs) anzeigen, hinzufügen und löschen. Sie können auch Performance Service Level und Storage Efficiency Policies für die LUNs zuweisen und ändern.

Vor dem Zuweisen von Storage muss sichergestellt werden, dass die SVM mit den unterstützten Protokollen erstellt und bereitgestellt wurde. Gleiches gilt für das Zuweisen von Performance Service Levels zu den LUNs, bevor Sie die LUN erstellen.

#### Zeigen Sie LUNs an

Sie können die folgende Methode verwenden, um alle LUNs in Ihrer Unified Manager Umgebung anzuzeigen. Wenn Sie ein ONTAP Cluster als Datenquelle auf Active IQ Unified Manager hinzugefügt haben, werden die Storage-Workloads für diese Cluster automatisch Ihrer Unified Manager Instanz hinzugefügt. Diese API ruft alle LUNs automatisch ab und wird manuell zu Ihrer Unified Manager Instanz hinzugefügt. Sie können sich die Details einer bestimmten LUN anzeigen lassen, indem Sie diese API mit dem LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/luns /storage-provider/luns/{key}

#### Fügen Sie LUNs hinzu

Mit der folgenden Methode können Sie Ihren SVMs LUNs hinzufügen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/luns



Wenn Sie in Ihrer Curl-Anfrage einen Wert für den optionalen Parameter angeben `volume_name_tag` Im Input wird dieser Wert verwendet, während die Benennung des Volumes während der LUN-Erstellung verwendet wird. Mit diesem Tag kann das Volume einfach durchsucht werden. Wenn Sie den Volume-Schlüssel in der Anforderung angeben, wird das Tagging übersprungen.

#### LUNs löschen

Sie können eine bestimmte LUN mit der folgenden Methode löschen. Sie müssen den LUN-Schlüssel zum Löschen einer bestimmten LUN angeben.



Wenn Sie ein Volume in ONTAP erstellt und dann über Unified Manager auf diesem Volume bereitgestellt haben, wenn Sie alle LUNs mithilfe dieser API löschen, wird das Volume auch aus dem ONTAP Cluster gelöscht.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	/storage-provider/luns/{key}

#### LUNs ändern

Mit der folgenden Methode können Sie eine LUN ändern und ihre Eigenschaften aktualisieren. Sie müssen den LUN-Schlüssel angeben, um eine bestimmte LUN zu ändern. Sie müssen außerdem die LUN-Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben. Für die Aktualisierung von LUN-Arrays mithilfe dieser API sollten Sie die Empfehlungen unter „Empfehlungen zur Verwendung der APIs“ überprüfen.



Sie können nur eine Eigenschaft bei einem einzelnen Aufruf dieser API aktualisieren. Für mehrere Updates müssen Sie diese API so oft ausführen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	/storage-provider/luns/{key}

#### Managen Von Performance Service Levels

Sie können Performance-Service-Level mithilfe der Storage-Provider-APIs für auf Ihrer Active IQ Unified Manager anzeigen, erstellen, ändern und löschen.

##### Zeigen Sie Performance Service Level An

Mit der folgenden Methode können Sie die Performance-Service-Level für die Zuweisung zu Storage-Workloads anzeigen. Die API listet alle systemdefinierten und vom Benutzer erstellten Performance Service

Levels auf und ruft die Attribute aller Performance Service Levels ab. Wenn Sie einen bestimmten Performance-Service-Level abfragen möchten, müssen Sie die eindeutige ID des Performance-Service-Levels eingeben, um die entsprechenden Details abzurufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/performance-service-levels  /storage-provider/performance-service-levels/{key}

#### Performance-Service-Level Hinzufügen

Mithilfe der folgenden Methode können Sie benutzerdefinierte Performance-Service-Level erstellen und diesen Ihren Storage-Workloads zuweisen, wenn die vom System definierten Performance-Service-Level die erforderlichen Service Level-Ziele (SLOs) für die Storage-Workloads nicht erfüllen. Geben Sie die Details für die Leistungsstufe ein, die Sie erstellen möchten. Stellen Sie für die IOPS-Eigenschaften sicher, dass Sie einen gültigen Wertebereich eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/performance-service-levels

#### Performance-Service-Level Löschen

Sie können die folgende Methode verwenden, um einen bestimmten Leistungsservicelevel zu löschen. Ein Performance-Service-Level kann nicht gelöscht werden, wenn er einem Workload zugewiesen ist oder wenn es das einzige verfügbare Performance-Service-Level ist. Sie müssen die eindeutige ID des Performance Service Levels als Eingabeparameter angeben, um einen bestimmten Performance Service Level zu löschen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	/storage-provider/performance-service-levels/{key}

#### Ändern Sie Performance-Service-Level

Sie können die folgende Methode verwenden, um einen Performance-Service-Level zu ändern und seine Eigenschaften zu aktualisieren. Ein Performance-Service-Level, der systemdefiniert oder einem Workload zugewiesen ist, kann nicht geändert werden. Zum Ändern eines bestimmten Performance-Service-Levels müssen Sie die eindeutige ID des angeben. Sie müssen außerdem die IOPS-Eigenschaft, die Sie aktualisieren möchten, sowie einen gültigen Wert eingeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	/storage-provider/performance-service-levels/{key}

#### Anzeigen von Aggregatfunktionen auf Basis von Performance-Service-Leveln

Sie können die folgende Methode verwenden, um die Aggregatfunktionen auf Basis der Performance-Service-Level abzufragen. Diese API gibt die Liste der in Ihrem Datacenter verfügbaren Aggregate zurück und weist die Funktionen in Bezug auf die Performance-Service-Level an, die in diesen Aggregaten unterstützt werden können. Während Sie Workloads auf einem Volume bereitstellen, können Sie die Funktionen eines Aggregats anzeigen, um ein bestimmtes Performance Service Level zu unterstützen. Zudem können Sie Workloads basierend auf dieser Funktion bereitstellen. Die Angabe des Aggregats ist nur verfügbar, wenn Sie einen Workload mithilfe von APIs bereitstellen. Diese Funktion steht in der Web-Benutzeroberfläche von Unified Manager nicht zur Verfügung.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/aggregate-capabilities  /storage-provider/aggregate-capabilities/{key}

#### Management Von Richtlinien Zur Storage-Effizienz

Sie können Richtlinien zur Storage-Effizienz mithilfe der Storage-Provider-APIs anzeigen, erstellen, ändern und löschen.

Beachten Sie folgende Punkte:

- Beim Erstellen eines Workloads in Unified Manager ist es nicht erforderlich, eine Storage-Effizienz-Richtlinie zuzuweisen.
- Sie können die Zuweisung einer Storage-Effizienzrichtlinie zu einem Workload nicht aufheben, nachdem eine Richtlinie zugewiesen ist.
- Wenn bei einem Workload einige Storage-Einstellungen angegeben sind, die in ONTAP Volumes wie Deduplizierung und Komprimierung angegeben sind, können diese Einstellungen durch die in der Storage-Effizienzrichtlinie festgelegten Einstellungen überschrieben werden. Nach Hinzufügen der Storage Workloads auf Unified Manager sind diese Einstellungen möglich.



#### Zeigen Sie Richtlinien Zur Storage-Effizienz An

Sie können die folgenden Methoden verwenden, um die Storage-Effizienzrichtlinien anzuzeigen, bevor Sie sie Storage-Workloads zuweisen. Diese API enthält alle systemdefinierten sowie vom Benutzer erstellten Richtlinien zur Storage-Effizienz und ruft die Attribute aller Storage-Effizienzrichtlinien ab. Wenn Sie eine bestimmte Storage-Effizienz-Richtlinie abfragen möchten, müssen Sie die eindeutige ID der Richtlinie

eingeben, um deren Details abzurufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/storage-efficiency-policies /storage-provider/storage-efficiency-policies/{key}

#### Fügen Sie Storage-Effizienzrichtlinien Hinzu

Mithilfe der folgenden Methode können Sie benutzerdefinierte Storage-Effizienzrichtlinien erstellen und diesen Ihren Storage Workloads zuweisen, wenn die systemdefinierten Richtlinien die Bereitstellungsanforderungen für Ihre Storage-Workloads nicht erfüllen. Geben Sie die Details der Storage-Effizienz-Richtlinie ein, die Sie erstellen möchten, als Eingabeparameter ein.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/storage-efficiency-policies

#### Storage-Effizienzrichtlinien Löschen

Sie können eine bestimmte Storage-Effizienz-Richtlinie mit der folgenden Methode löschen: Sie können eine Richtlinie zur Storage-Effizienz nicht löschen, wenn sie einem Workload zugewiesen ist oder wenn sie die einzige verfügbare Richtlinie zur Storage-Effizienz ist. Sie müssen die eindeutige ID der Storage-Effizienz-Richtlinie als Eingabeparameter bereitstellen, um eine bestimmte Storage-Effizienz-Richtlinie zu löschen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	Löschen	/storage-provider/storage-efficiency-policies/{key}

#### Sie Können Die Storage-Effizienzrichtlinien Ändern

Sie können die folgende Methode verwenden, um eine Storage Efficiency Policy zu ändern und deren Eigenschaften zu aktualisieren. Sie können eine Storage-Effizienzrichtlinie, die systemdefiniert oder einem Workload zugewiesen ist, nicht ändern. Sie müssen die eindeutige ID der Storage-Effizienz-Richtlinie angeben, um eine bestimmte Storage-Effizienz-Richtlinie zu ändern. Zusätzlich müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert angeben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	/storage-provider/storage-efficiency-policies/{key}

# Typische Workflows für das Storage-Management

Die üblichen Workflows bieten Entwicklern von Client-Applikationen Beispiele dafür, wie Active IQ Unified Manager APIs von einer Client-Applikation aufgerufen werden können, um allgemeine Storage-Managementfunktionen auszuführen. Dieser Abschnitt enthält einige Beispiele-Workflows.

Die Workflows beschreiben einige der am häufigsten verwendeten Anwendungsfälle für das Storage-Management und geben Ihnen Beispielcodes an. Jede Aufgabe wird mit einem Workflow-Prozess beschrieben, der aus einem oder mehreren API-Aufrufen besteht.

## Allgemeines zu den in den Workflows verwendeten API-Aufrufen

Sie können die Online-Dokumentationsseite von Ihrer Unified Manager Instanz aus einsehen, die alle Einzelheiten zu jedem REST-API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder API-Aufruf, der in den Workflow-Proben in diesem Dokument verwendet wird, enthält nur die Informationen, die Sie benötigen, um den Anruf auf der Dokumentationsseite zu finden. Nach dem Auffinden eines bestimmten API-Aufrufs können Sie die vollständigen Details des Anrufs überprüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Aufruftyps.

Für jeden API-Aufruf in einem Workflow sind folgende Informationen enthalten, um den Anruf auf der Dokumentationsseite zu finden:

- Kategorie: Die API-Aufrufe werden auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien organisiert. Um einen bestimmten API-Aufruf zu finden, blättern Sie zum unteren Seitenrand und klicken Sie auf die entsprechende API-Kategorie.
- HTTP-Verb (Aufruf): Das HTTP-Verb identifiziert die Aktion, die auf einer Ressource ausgeführt wird. Jeder API-Aufruf wird über ein einziges HTTP-Verb ausgeführt.
- Pfad: Der Pfad bestimmt die spezifische Ressource, auf die die Aktion als Teil der Durchführung eines Anrufs gilt. Der Pfadstring wird an die Core-URL angehängt, um die vollständige URL zur Identifizierung der Ressource zu bilden.

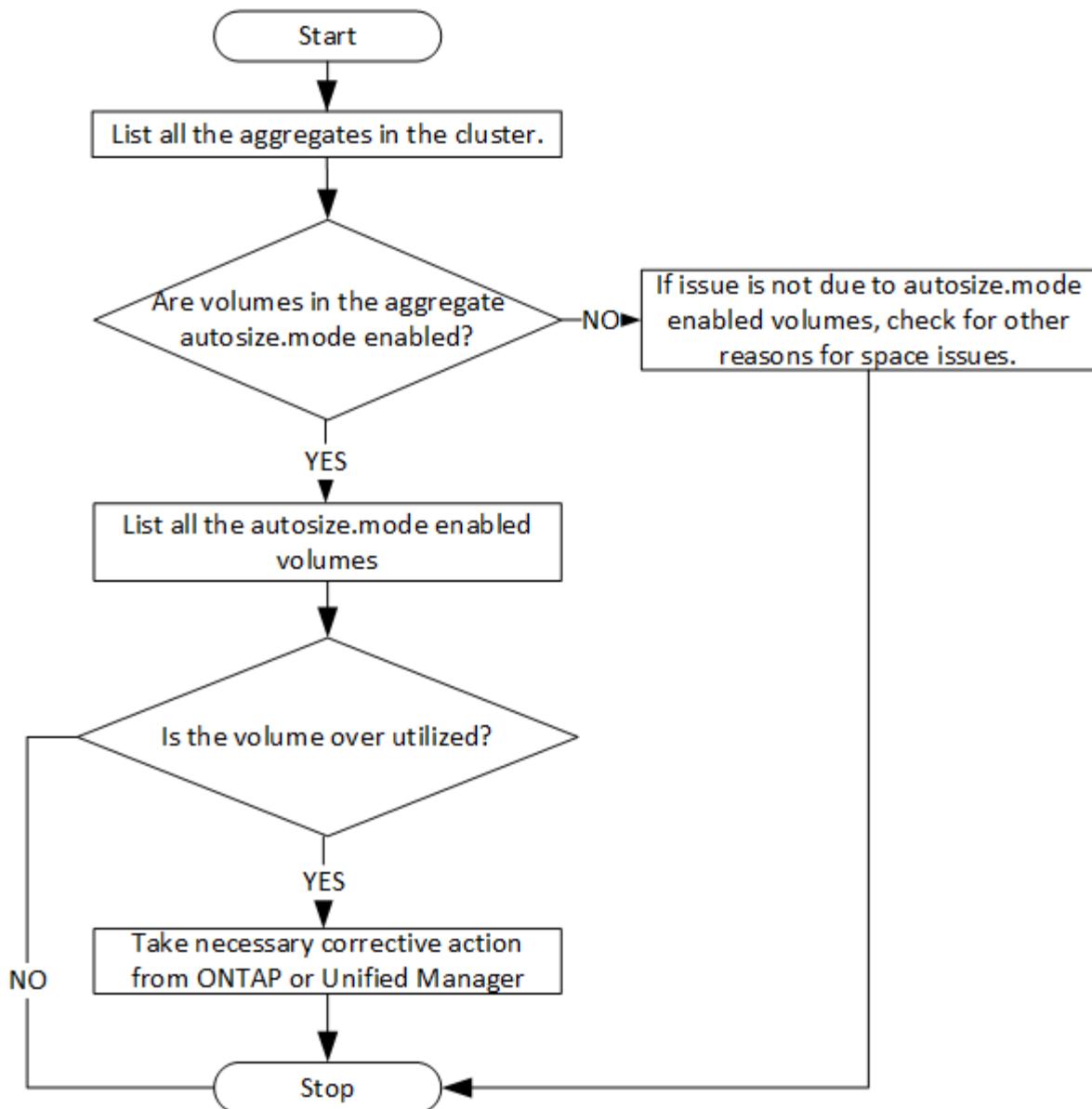
## Bestimmen von Platzproblemen in Aggregaten

Mit den Datacenter-APIs in Active IQ Unified Manager können Sie die Verfügbarkeit und Auslastung von Speicherplatz in Ihren Volumes überwachen. Sie können Platzprobleme in Ihrem Volume ermitteln und überlastete oder nicht ausgelastete Storage-Ressourcen identifizieren.

Die Datacenter-APIs für Aggregate rufen die relevanten Informationen über verfügbaren und belegten Speicherplatz sowie Einstellungen zur Speicherplatzersparnis ab. Sie können die abgerufenen Informationen auch anhand bestimmter Attribute filtern.

Eine Methode zur Bestimmung eines Speicherplatzmangels in Ihren Aggregaten ist es, festzustellen, ob in Ihrer Umgebung Volumes mit aktiviertem Autosize-Modus vorhanden sind. Anschließend sollten Sie ermitteln, welche Volumes zu viel genutzt werden, und Sie können Korrekturmaßnahmen vornehmen.

Das folgende Flussdiagramm zeigt den Prozess zum Abrufen von Informationen zu Volumes mit aktiviertem Autosize-Modus:



Es wird vorausgesetzt, dass die Cluster bereits im ONTAP erstellt und zu Unified Manager hinzugefügt wurden.

1. Beziehen Sie den Cluster-Schlüssel, es sei denn, Sie kennen den Wert:

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	/datacenter/cluster/clusters

2. Fragen Sie mit dem Cluster Key als Filterparameter die Aggregate auf diesem Cluster ab.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	/datacenter/storage/aggregates

3. Analysieren Sie als Antwort den Speicherplatznutzung der Aggregate und bestimmen Sie, welche Aggregate Platzprobleme aufweisen. Beziehen Sie für jedes Aggregat mit einem Platzproblem den Aggregatschlüssel aus der gleichen JSON-Ausgabe.
4. Filtern Sie mit jedem Aggregat-Schlüssel alle Volumes, die den Wert für das haben `autosize.mode` Parameter als `grow`.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	/datacenter/storage/volumes

5. Analyse der zu stark ausgelasteten Volumes
6. Führen Sie alle erforderlichen Korrekturmaßnahmen durch, z. B. das Verschieben des Volumes über Aggregate, um die Platzprobleme im Volume zu beheben. Sie können diese Aktionen über die ONTAP- oder die Unified Manager-Weboberfläche ausführen.

## Fehlerbehebung bei ONTAP Volumes mithilfe von Gateway-APIs

Die Gateway-APIs dienen als Gateway zum Aufrufen von ONTAP APIs, mit denen Informationen über Ihre ONTAP Storage-Objekte abgefragt und Korrekturmaßnahmen ergriffen werden, um die gemeldeten Probleme anzugehen.

Dieser Workflow greift auf einen Beispielfall zurück, in dem ein Ereignis angehoben wird, wenn ein ONTAP-Volume fast seine Kapazität erreicht. Im Workflow wird außerdem gezeigt, wie Sie das Problem beheben können, indem Sie eine Kombination aus Active IQ Unified Manager und ONTAP REST APIs aufrufen.

Bevor Sie die Workflow-Schritte ausführen, stellen Sie Folgendes sicher:

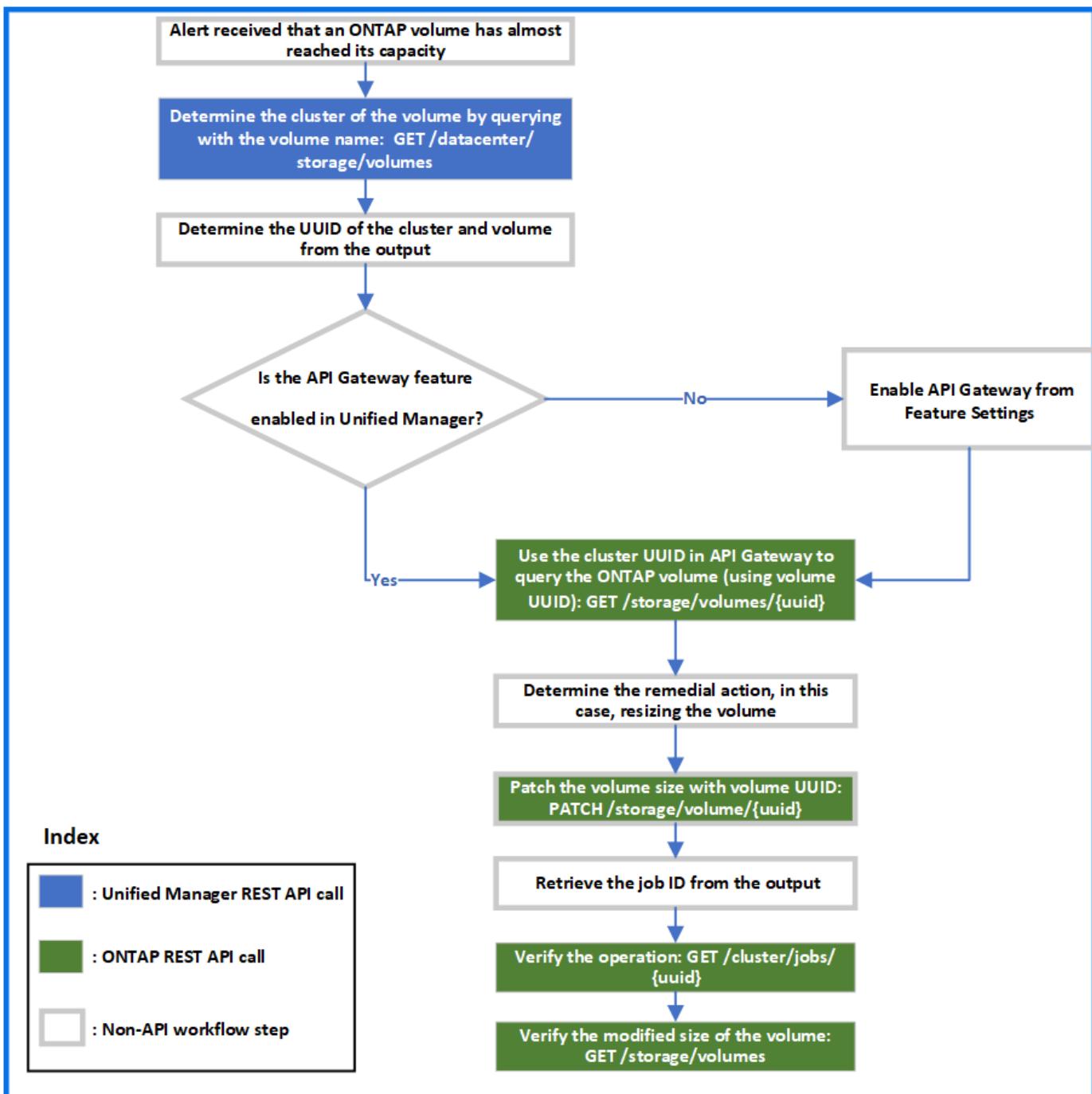
- Sie kennen die Gateway-APIs und deren Nutzung. Weitere Informationen finden Sie im Abschnitt „Gateway APIs“.

### Gateway-APIs



- Sie sind sich der Nutzung von ONTAP REST-APIs bewusst. Weitere Informationen zur Verwendung von ONTAP REST-APIs finden Sie unter ["ONTAP REST-API-AUTOMATISIERUNG"](#).
- Sie sind ein Anwendungsadministrator.
- Das Cluster, auf dem Sie die REST-API-Vorgänge ausführen möchten, wird von ONTAP 9.5 oder höher unterstützt, und das Cluster wird Unified Manager über HTTPS hinzugefügt.

Das folgende Diagramm zeigt jeden Schritt im Workflow zur Fehlerbehebung bei der Verwendung von ONTAP Volume-Kapazität.



Der Workflow umfasst die Anrufungspunkte sowohl von Unified Manager als auch von ONTAP REST-APIs.

1. Notieren Sie den Volume-Namen aus dem Ereignis, um die Kapazitätsauslastung des Volume zu benachrichtigen.
2. Durch Verwendung des Volume-Namens als Wert im `name` Parameter, Abfrage des Volumes durch Ausführung der folgenden Unified Manager API.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	/datacenter/storage/volumes

3. Abrufen der Cluster-UUID und Volume-UUID von der Ausgabe.
4. Navigieren Sie in der Web-UI von Unified Manager zu **Allgemein > Funktionseinstellungen > API Gateway**, um zu überprüfen, ob die API-Gateway-Funktion aktiviert ist. Sofern sie nicht aktiviert ist, werden die APIs unter dem angezeigten `gateway` Die Kategorie kann nicht aufgerufen werden. Aktivieren Sie die Funktion, wenn sie deaktiviert ist.
5. Verwenden Sie die Cluster-UUID zum Ausführen der ONTAP-API `/storage/volumes/{uuid}` Über das API-Gateway. Die Abfrage gibt die Volume-Details zurück, wenn die Volume-UUID als API-Parameter übergeben wird.

Zur Ausführung der ONTAP-APIs über das API-Gateway werden die Anmeldeinformationen für den Unified Manager zur internen Authentifizierung übergeben. Sie müssen keinen zusätzlichen Authentifizierungsschritt für den individuellen Cluster-Zugriff ausführen.

Kategorie	HTTP-Verb	Pfad
Unified Manager: gateway ONTAP: Storage	GET	Gateway-API: <code>/gateways/{uuid}/{path}</code>  ONTAP-API: <code>/storage/volumes/{uuid}</code>



In `/gateways/{uuid}/{path}`, Der Wert für `{uuid}` Muss durch die Cluster-UUID ersetzt werden, für die der REST-Vorgang ausgeführt werden soll. `{path}` Muss durch die ONTAP REST-URL ersetzt werden `/storage/volumes/{uuid}`.

Die angehängte URL lautet: `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

Bei Ausführung der GET Die generierte URL lautet:

GET `https://<hostname>/api/gateways/<cluster_UUID>/storage/volumes/{volume_uuid}`

#### Befehl zum Curl-Beispiel

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. Bestimmen Sie von der Ausgabe die zu ergriffende Größe, Nutzung und Abhilfemaßnahme. In diesem Workflow ist die Abhilfemaßnahme die Größe des Volumens.
7. Verwenden Sie die Cluster-UUID, und führen Sie die folgende ONTAP-API über das API-Gateway aus, um die Größe des Volumes zu ändern. Informationen zu den Eingabeparametern für das Gateway und ONTAP APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad
Unified Manager: gateway ONTAP: Storage	PATCH	Gateway-API: /gateways/{uuid}/{path}  ONTAP-API: /storage/volumes/{uuid}



Zusammen mit der Cluster-UUID und der Volume-UUID müssen Sie einen Wert für den eingeben `size` Parameter für die Größe des Volumens. Stellen Sie sicher, dass Sie den Wert *in Byte* eingeben. Wenn Sie beispielsweise die Größe eines Volumes von 100 GB auf 120 GB erhöhen möchten, geben Sie den Wert für den Parameter `size` Am Ende der Abfrage: `-d {"size": 128849018880}"`

### Befehl zum Curl-Beispiel

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H "accept: application/hal+json" -H "Authorization: Basic <Base64EncodedCredentials>" -d {"size": 128849018880}"
```

Die JSON-Ausgabe gibt eine Job-UUID zurück.

- Überprüfen Sie, ob der Job erfolgreich ausgeführt wurde, indem Sie die Job-UUID verwenden. Verwenden Sie die Cluster-UUID und Job-UUID, um die folgende ONTAP-API über das API-Gateway auszuführen. Informationen zu den Eingabeparametern für das Gateway und ONTAP APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad
Unified Manager: gateway ONTAP: Cluster	GET	Gateway-API: /gateways/{uuid}/{path}  ONTAP-API: /cluster/jobs/{uuid}

Die zurückgegebenen HTTP-Codes entsprechen den HTTP-Statuscodes der ONTAP REST-API.

- Führen Sie die folgende ONTAP API aus, um die Details des Volumes mit der Größe zu abfragen. Informationen zu den Eingabeparametern für das Gateway und ONTAP APIs finden Sie in Schritt 5.

Kategorie	HTTP-Verb	Pfad
Unified Manager: gateway ONTAP: Storage	GET	Gateway-API: /gateways/{uuid}/{path}  ONTAP-API: /storage/volumes/{uuid}

Die Ausgabe zeigt eine erhöhte Lautstärke von 120 GB an.

## Workflows für das Workload-Management

Mithilfe von Active IQ Unified Manager können Storage-Workloads (LUNs, NFS-Dateifreigaben und CIFS-Freigaben) bereitgestellt und geändert werden. Die Bereitstellung besteht aus mehreren Schritten: Von der Erstellung der Storage Virtual Machine (SVM) bis zur Anwendung von Performance Service Level- und Storage-Effizienz-Richtlinien auf die Storage Workloads. Das Ändern von Workloads besteht aus den Schritten zum Ändern spezifischer Parameter und zum Aktivieren zusätzlicher Funktionen für diese.

Die folgenden Workflows werden beschrieben:

- Workflow für die Bereitstellung von Storage Virtual Machines (SVMs) in Unified Manager



Dieser Workflow muss vor der Bereitstellung von LUNs oder File Shares auf Unified Manager durchgeführt werden.

- Bereitstellen von Dateifreigaben:
- Bereitstellung von LUNs:
- Ändern von LUNs und Dateifreigaben (mit dem Beispiel für die Aktualisierung des Parameters für Performance-Service-Level für die Storage-Workloads)
- Ändern einer NFS-Dateifreigabe zur Unterstützung des CIFS-Protokolls
- Änderung von Workloads für das Upgrade von QoS auf AQoS



Stellen Sie für jeden Bereitstellungs-Workflow (LUN und Dateifreigaben) sicher, dass Sie den Workflow zur Überprüfung der SVMs auf den Clustern abgeschlossen haben müssen.

Sie müssen auch die Empfehlungen und Einschränkungen lesen, bevor Sie jede API in den Workflows verwenden. Die relevanten Details der APIs sind in ihren einzelnen Abschnitten in den verwandten Konzepten und Referenzen aufgeführt.

### Überprüfung von SVMs auf Clustern

Bevor Sie Dateifreigaben oder LUNs bereitstellen, müssen Sie überprüfen, ob auf den Clustern Storage Virtual Machines (SVMs) erstellt wurden.



Beim Workflow wird vorausgesetzt, dass ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel erhalten wurde. Auf Clustern sollten die erforderlichen Lizenzen zur Bereitstellung von LUNs und File Shares vorhanden sein.

1. Überprüfen, ob auf dem Cluster eine SVM erstellt wurde.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	/datacenter/svm/svms /datacenter/svm/svms/{key}

### Stichprobe

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Erstellen Sie die SVM, falls der SVM-Schlüssel nicht zurückgegeben wird. Zum Erstellen der SVMs benötigen Sie den Cluster-Schlüssel, für den Sie die SVM bereitstellen. Sie müssen außerdem den SVM-Namen angeben. Auszuführende Schritte:

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	/datacenter/cluster/clusters /datacenter/cluster/clusters/{key}

Abrufen des Cluster-Schlüssels.

### Stichprobe

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

3. Holen Sie den Cluster-Schlüssel von der Ausgabe, und verwenden Sie ihn als Input für die Erstellung der SVM.



Vergewissern Sie sich bei der Erstellung der SVM, dass sie alle Protokolle unterstützt, die für die Bereitstellung von LUNs und File Shares benötigt werden, zum Beispiel CIFS, NFS, FCP Und iSCSI. Die Bereitstellungs-Workflows können fehlschlagen, wenn die SVM die erforderlichen Services nicht unterstützt. Es wird empfohlen, auch die Services für die jeweiligen Workload-Typen auf der SVM zu aktivieren.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	POST	/datacenter/svm/svms

### Stichprobe

Geben Sie die Details des SVM-Objekts als Eingabeparameter ein.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {}, \"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-9876567890123\", \"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-00a0986138f7\" } ], \"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\": \"string\", \"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" }, \"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-9876567890123\" }, \"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ], \"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] }, \"fcp\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true, \"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" }, \"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\": \"dataLif1\" }, { \"name\": \"exchange\" }, { \"enabled\": true }, { \"language\": \"c.utf_8\" }, { \"ad_domain\": \"string\", \"base_dn\": \"string\" }, { \"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ] } ], \"name\": \"svml\", \"nfs\": { \"enabled\": true }, \"nis\": { \"domain\": \"string\", \"enabled\": true }, \"servers\": [ \"string\" ], { \"enabled\": true }, { \"destination\": { \"address\": \"10.10.10.7\" }, \"netmask\": \"24\" }, { \"gateway\": \"string\" } ], { \"name\": \"default\" }, { \"state\": \"running\", \"subtype\": \"default\" } }
```

Die JSON-Ausgabe zeigt einen Objektschlüssel an, mit dem Sie die von Ihnen erstellte SVM überprüfen können.

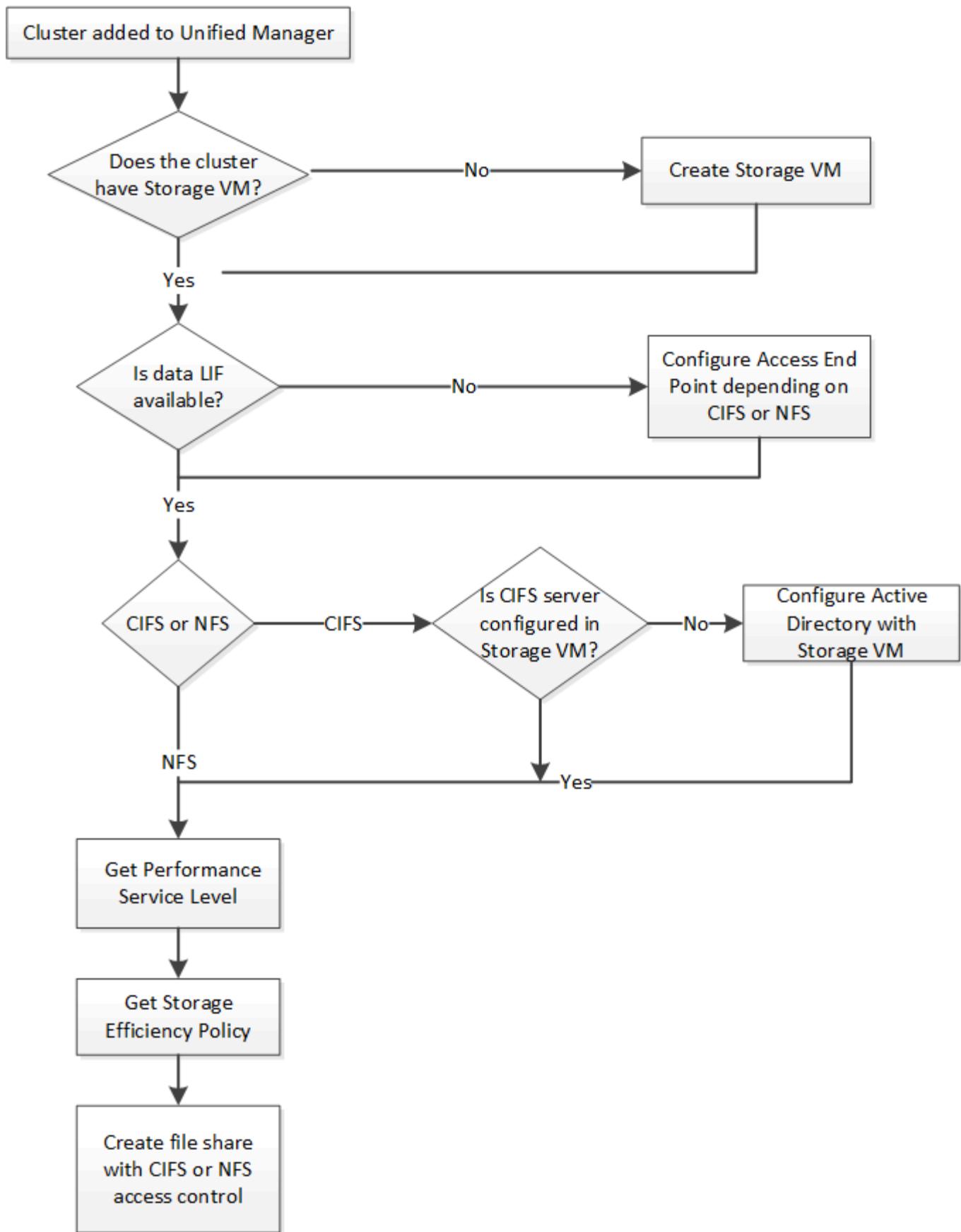
- Überprüfen Sie die SVM-Erstellung mithilfe des Jobobjektschlüssels für die Abfrage. Wenn die SVM erfolgreich erstellt wurde, wird der SVM-Schlüssel in der Antwort zurückgegeben.

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management-server/jobs/{key}

## Provisionierung von CIFS- und NFS-Dateifreigaben

Sie können CIFS-Freigaben und NFS-Dateifreigaben auf Ihren Storage Virtual Machines (SVMs) mithilfe der BereitstellungsAPIs, die als Teil von Active IQ Unified Manager bereitgestellt werden, bereitstellen. Dieser Bereitstellungs-Workflow zeigt die Schritte zum Abrufen der Schlüssel der SVMs, Performance Service Levels und Storage-Effizienz-Richtlinien, bevor die Dateifreigaben erstellt werden.

Das folgende Diagramm veranschaulicht die einzelnen Schritte eines Workflows zur Dateifreigabe. Das System umfasst die Bereitstellung von CIFS-Freigaben und NFS-Dateifreigaben.



Stellen Sie Folgendes sicher:

- Dem Unified Manager wurden ONTAP Cluster hinzugefügt, und der Clusterschlüssel ist abgerufen.
- Auf den Clustern wurden SVMs erstellt.
- Die SVMs unterstützen CIFS- und NFS-Services. Dateifreigaben können möglicherweise fehlschlagen, wenn die SVMs die erforderlichen Services nicht unterstützen.
- Der FCP Port ist online für die Port-Bereitstellung.

1. Ermitteln, ob Daten-LIFs oder Zugriffendpunkte auf der SVM verfügbar sind, auf der Sie die CIFS-Freigabe erstellen möchten. Rufen Sie die Liste der verfügbaren Zugriffendpunkte auf der SVM auf:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}

### Stichprobe

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Wenn Ihr Zugriffendpunkt in der Liste verfügbar ist, erhalten Sie den Schlüssel für den Access-Endpunkt, sonst erstellen Sie den Access-Endpunkt.



Stellen Sie sicher, dass Sie Zugriffendpunkte erstellen, auf denen das CIFS-Protokoll aktiviert ist. Die Bereitstellung von CIFS-Freigaben schlägt fehl, es sei denn, Sie haben einen Zugriffendpunkt erstellt, auf dem das CIFS-Protokoll aktiviert ist.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/access-endpoints

### Stichprobe

Sie müssen die Details des Zugriffendpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.

```

curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}

```

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie den von Ihnen erstellten Zugriffspunkt überprüfen können.

3. Überprüfen Sie den Zugriffspunkt:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management- server/jobs/{key}

4. Bestimmen Sie, ob Sie eine CIFS-Freigabe oder eine NFS-Dateifreigabe erstellen müssen. Führen Sie zum Erstellen von CIFS-Freigaben die folgenden Teilschritte aus:

- a. Legen Sie fest, ob der CIFS-Server für Ihre SVM konfiguriert ist, und ermitteln Sie, ob eine Active Directory-Zuordnung auf der SVM erstellt wird.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage- provider/active- directories-mappings

- b. Wenn die Active Directory-Zuordnung erstellt wird, ziehen Sie den Schlüssel, sonst erstellen Sie die Active Directory-Zuordnung auf der SVM.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage- provider/active- directories-mappings

## Stichprobe

Sie müssen die Details zum Erstellen der Active Directory-Zuordnung als Eingabeparameter eingeben.

```
curl -X POST "https://<hostname>/api/storage-provider/active-directories-mappings" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" { "_links": {}, "dns": "10.000.000.000", "domain": "example.com", "password": "string", "svm": { "key": "9f4dde-a-e395-11e9-b660-005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9" }, "username": "string" }
```

+ Dies ist ein synchroner Anruf, und Sie können die Erstellung der Active Directory-Zuordnung in der Ausgabe überprüfen. Im Fehlerfall wird die Fehlermeldung angezeigt, damit Sie die Anfrage beheben und erneut ausführen können.

5. Den SVM-Schlüssel für die SVM erhalten, auf der Sie die CIFS-Freigabe oder die NFS-Dateifreigabe erstellen möchten, wie im Workflow-Thema *ÜberprüfungsSVMs auf Clustern* beschrieben.
6. Erhalten Sie den Schlüssel für den Performance Service Level, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/performance-service-levels



Sie können die Details der vom System definierten Performance-Service-Level abrufen, indem Sie die einstellen `system_defined` Eingabeparameter an `true`. Holen Sie in der Ausgabe den Schlüssel des Performance Service Level, den Sie auf die Dateifreigabe anwenden möchten.

7. Sie können optional den Richtlinienschlüssel für die Storage-Effizienz für die Storage-Effizienzrichtlinie abrufen, den Sie auf die Dateifreigabe anwenden möchten, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/storage-efficiency-policies

8. Erstellen Sie die Dateifreigabe. Sie können eine Dateifreigabe erstellen, die sowohl CIFS als auch NFS unterstützt, indem Sie die Zugriffssteuerungsliste und die Exportrichtlinie angeben. Die folgenden Teilschritte enthalten Informationen, wenn Sie eine Dateifreigabe erstellen möchten, um nur eines der

Protokolle auf dem Volume zu unterstützen. Sie können auch eine NFS-Dateifreigabe aktualisieren, um die Zugriffssteuerungsliste einzuschließen, nachdem Sie die NFS-Freigabe erstellt haben. Informationen hierzu finden Sie im Thema „*Modifizieren von Storage Workloads*“.

- a. Wenn Sie nur eine CIFS-Freigabe erstellen möchten, sammeln Sie Informationen über die Zugriffssteuerungsliste (Access Control List, ACL). Geben Sie für die Erstellung der CIFS-Freigabe gültige Werte für die folgenden Eingabeparameter an. Für jede Benutzergruppe, die Sie zuweisen, wird bei der Bereitstellung einer CIFS/SMB-Freigabe eine ACL erstellt. Auf der Grundlage der von Ihnen für die ACL- und Active Directory-Zuordnung eingegebenen Werte werden die Zugriffssteuerung und Zuordnung für die CIFS-Freigabe bei ihrer Erstellung festgelegt.

#### Ein Curl-Befehl mit Beispielwerten

```
{  
  "access_control": {  
    "acl": [  
      {  
        "permission": "read",  
        "user_or_group": "everyone"  
      }  
    ],  
    "active_directory_mapping": {  
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"  
    },  
  },  
}
```

- b. Um nur eine NFS-Dateifreigabe zu erstellen, sammeln Sie die Informationen über die Exportrichtlinie. Geben Sie für die Erstellung der NFS-Dateifreigabe gültige Werte für die folgenden Eingabeparameter an. Auf Grundlage Ihrer Werte ist die Exportrichtlinie mit der NFS-Dateifreigabe verbunden, wenn sie erstellt wird.



Während Sie die NFS-Freigabe bereitstellen, können Sie entweder eine Exportrichtlinie erstellen, indem Sie alle erforderlichen Werte angeben oder den Schlüssel für die Exportrichtlinie angeben und eine vorhandene Exportrichtlinie wiederverwenden. Wenn Sie eine Exportrichtlinie für die Storage-VM wiederverwenden möchten, müssen Sie den Schlüssel für die Exportrichtlinie hinzufügen. Wenn Sie den Schlüssel nicht kennen, können Sie den Schlüssel für die Exportrichtlinie über abrufen `/datacenter/protocols/nfs/export-policies` API: Zum Erstellen einer neuen Richtlinie müssen Sie die Regeln eingeben, die im folgenden Beispiel angezeigt werden. Bei den eingegebenen Regeln versucht die API, nach einer vorhandenen Exportrichtlinie zu suchen, indem sie den Host, die Storage-VM und die Regeln anpasst. Wenn eine Exportrichtlinie vorhanden ist, wird sie verwendet. Andernfalls wird eine neue Exportrichtlinie erstellt.

#### Ein Curl-Befehl mit Beispielwerten

```

"export_policy": {
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name_tag": "ExportPolicyNameTag",
    "rules": [
        {
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ]
        }
    ]
}

```

Geben Sie nach der Konfiguration der Zugriffssteuerungsliste und der Exportrichtlinie die gültigen Werte für die obligatorischen Eingabeparameter für CIFS- und NFS-Dateifreigaben ein:



Die Richtlinie zur Storage-Effizienz ist ein optionaler Parameter zum Erstellen von Dateifreigaben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/file-shares

+ Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die von Ihnen erstellte Dateifreigabe überprüfen können.

9. Überprüfen Sie die Erstellung der Dateifreigabe, indem Sie den bei der Abfrage des Jobs zurückgegebenen Job-Objektschlüssel verwenden:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management-server/jobs/{key}

Am Ende der Antwort sehen Sie den Schlüssel der erstellten Dateifreigabe.

```

] ,
"job_results": [
{
    "name": "fileshareKey",
    "value": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
}
],
"_links": {
    "self": {
        "href": "/api/management-server/jobs/06a6148bf9e862df:-2611856e:16e8d47e722:-7f87"
    }
}
}

```

10. Überprüfen Sie die Erstellung der Dateifreigabe, indem Sie die folgende API mit dem zurückgegebenen Schlüssel ausführen:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/file-shares/{key}

#### Beispiel JSON-Ausgabe

Sie sehen, dass die POST-Methode von `/storage-provider/file-shares` Intern ruft alle für die einzelnen Funktionen erforderlichen APIs auf und erstellt das Objekt. Zum Beispiel ruft er die auf `/storage-provider/performance-service-levels/` API zum Zuweisen des Performance Service Levels in der Dateifreigabe.

```

{
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
    "name": "FileShare_377",
    "cluster": {
        "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
        "name": "AFFA300-206-68-70-72-74",
        "_links": {
            "self": {
                "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959"
            }
        }
    }
}
```

```

        }
    },
    "svm": {
        "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
        "name": "RRT_ritu_vs1",
        "_links": {
            "self": {
                "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-
8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-
00a098dcc959"
            }
        }
    },
    "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
    },
    "recommended_performance_service_level": {
        "key": null,
        "name": "Idle",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",

```

```
        "permission": "read"
    }
],
"export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 1,
            "protocols": [
                "nfs3",
                "nfs4"
            ],
            "ro_rule": [
                "sys"
            ],
            "rw_rule": [
                "sys"
            ],
            "superuser": [
                "none"
            ]
        },
        {
            "anonymous_user": "65534",
            "clients": [
                {
                    "match": "0.0.0.0/0"
                }
            ],
            "index": 2,
            "protocols": [
                "cifs"
            ],
            "ro_rule": [
                "ntlm"
            ],
            "rw_rule": [

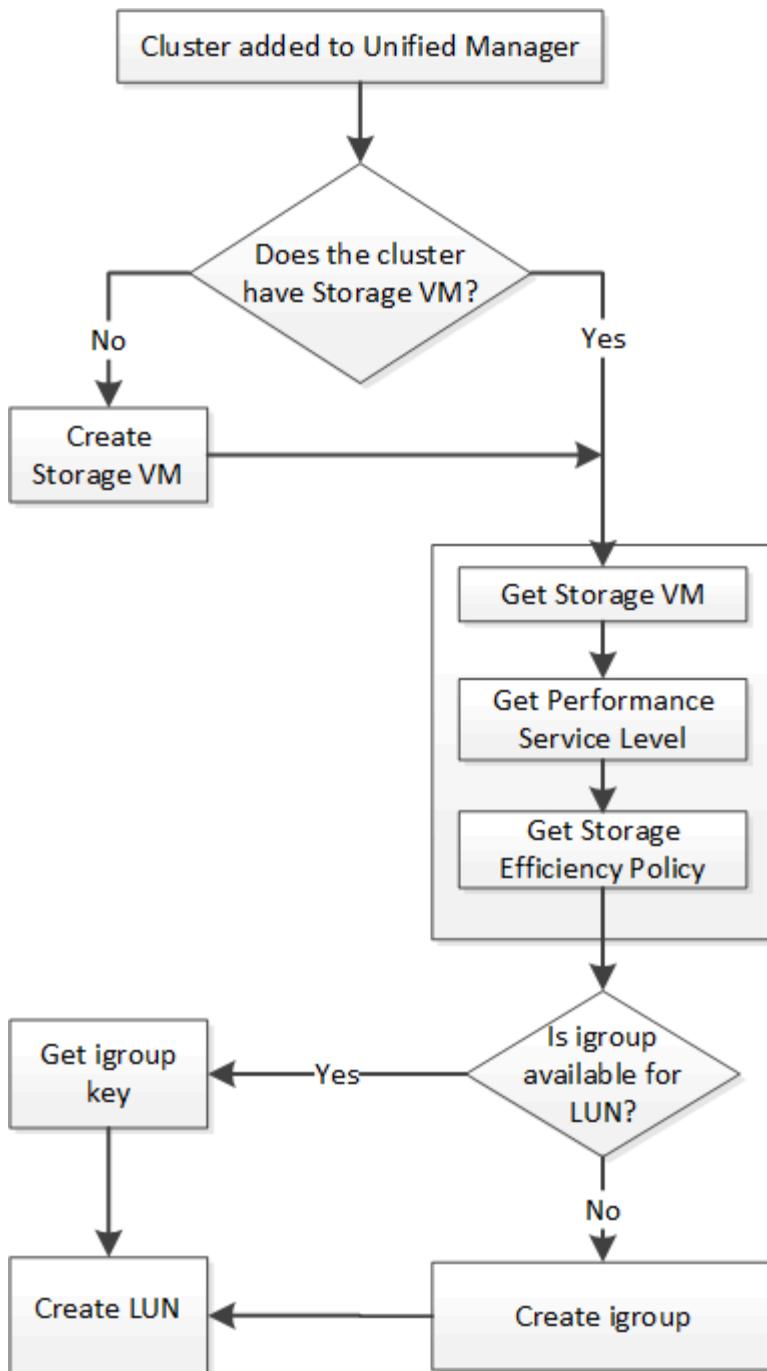
```

```
        "ntlm"
    ],
    "superuser": [
        "none"
    ]
}
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
    }
}
}
},
"_links": {
    "self": {
        "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
    }
}
}
```

## Bereitstellung von LUNs

Sie können LUNs auf Ihren Storage Virtual Machines (SVMs) bereitstellen, indem Sie die BereitstellungsAPIs verwenden, die als Teil von Active IQ Unified Manager zur Verfügung gestellt werden. Dieser Workflow zur Bereitstellung umfasst die Schritte zum Abrufen der Schlüssel der SVMs, Performance Service Levels und Storage-Effizienz-Richtlinien, bevor die LUN erstellt wird.

Im folgenden Diagramm sind die Schritte in einem Workflow zur Bereitstellung von LUNs dargestellt.



Bei diesem Workflow wird vorausgesetzt, dass die ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Beim Workflow wird auch davon ausgegangen, dass die SVMs bereits auf den Clustern erstellt wurden.

1. Den SVM-Schlüssel für die SVM erhalten, auf der Sie die LUN erstellen möchten, wie im Workflow-Thema „*Verifying SVMs on Cluster*“ beschrieben.
2. Erhalten Sie den Schlüssel für den Performance Service Level, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/performance-service-levels



Sie können die Details der vom System definierten Performance-Service-Level abrufen, indem Sie die einstellen `system_defined` Eingabeparameter an `true`. Holen Sie von der Ausgabe den Schlüssel des Performance Service Level, den Sie auf der LUN anwenden möchten.

3. Optional können Sie den Richtlinienschlüssel für die Storage-Effizienz für die Storage-Effizienzrichtlinie abrufen, die Sie auf der LUN anwenden möchten, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/storage-efficiency-policies

4. Legen Sie fest, ob Initiatorgruppen (Initiatorgruppen) erstellt wurden, um Ihnen den Zugriff auf das LUN-Ziel zu gewähren, das Sie erstellen möchten.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	GET	/datacenter/protocols/san/igroups /datacenter/protocols/san/igroups/{key}

Sie müssen den Parameterwert für die SVM eingeben, für die die Initiatorgruppe über einen autorisierten Zugriff verfügt. Wenn Sie außerdem eine bestimmte Initiatorgruppe abfragen möchten, geben Sie den Initiatorgruppennamen (Schlüssel) als Eingabeparameter ein.

5. Wenn Sie in der Ausgabe die Initiatorgruppe finden, der Sie Zugriff auf gewähren möchten, holen Sie den Schlüssel ein. Erstellen Sie andernfalls die Initiatorgruppe.

Kategorie	HTTP-Verb	Pfad
Rechenzentrum	POST	/datacenter/protocols/san/igroups

Sie müssen die Details der Initiatorgruppe, die Sie erstellen möchten, als Eingabeparameter eingeben. Dies ist ein synchroner Anruf, und Sie können die igrup-Erstellung in der Ausgabe überprüfen. Im Fehlerfall wird eine Meldung angezeigt, mit der Sie Fehler beheben und die API erneut ausführen können.

6. Erstellen Sie die LUN.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/luns

Stellen Sie zum Erstellen der LUN sicher, dass Sie die abgerufenen Werte als obligatorische Eingabeparameter hinzugefügt haben.



Die Richtlinie zur Storage-Effizienz ist ein optionaler Parameter zum Erstellen von LUNs.

## Stichprobe

Sie müssen als Eingabeparameter alle Details der LUN eingeben, die Sie erstellen möchten.

```
curl -X POST "https://<hostname>/api/storage-provider/luns" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d
  "{ \"name\": \"MigrationLunWithVol\", \"os_type\": \"windows\",
  \"performance_service_level\": { \"key\": \"7873dc0d-0ee5-11ea-82d7-fa163ea0eb69\" },
  \"space\": { \"size\": 1024000000 }, \"svm\": { \"key\": \"333fbefa-0ace-11ea-9d6d-00a09897cc15:type=vserver,uuid=4d462ec8-0f56-11ea-9d6d-00a09897cc15\" }
  } }
```

In der JSON-Ausgabe wird ein Objektschlüssel angezeigt, mit dem Sie die von Ihnen erstellte LUN überprüfen können.

- Überprüfen Sie die LUN-Erstellung, indem Sie den bei der Abfrage des Jobs zurückgegebenen Job-Objektschlüssel verwenden:

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management-server/jobs/{key}

Am Ende der Antwort wird der Schlüssel der erstellten LUN angezeigt.

```
{
  "name": "lunKey",
  "value": "key": "f963839f-0f95-11ea-9963-
00a098884af5:type=lun,uuid=71f3187e-bf19-4f34-ba34-b1736209b45a"
}
],
"_links": {
  "self": {
    "href": "/api/management-server/jobs/fa7c856d29e2b80f%3A-
8d3325d%3A16e9eb5ed6d%3A-548b"
  }
}
}
```

8. Überprüfen Sie die Erstellung der LUN, indem Sie die folgende API mit dem zurückgegebenen Schlüssel ausführen:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage- provider/luns/{key}

### Beispiel JSON-Ausgabe

Sie sehen, dass die POST-Methode von /storage-provider/luns Intern ruft alle für die einzelnen Funktionen erforderlichen APIs auf und erstellt das Objekt. Zum Beispiel ruft er die auf /storage-provider/performance-service-levels/ API zum Zuweisen des Performance Service Level auf der LUN.

```
{
  "key": "f963839f-0f95-11ea-9963-00a098884af5:type=lun,uuid=71f3187e-
bf19-4f34-ba34-b1736209b45a",
  "name": "/vol/NSLM_VOL_LUN_1574753881051/LunForTesting1",
  "uuid": "71f3187e-bf19-4f34-ba34-b1736209b45a",
  "cluster": {
    "uuid": "f963839f-0f95-11ea-9963-00a098884af5",
    "key": "f963839f-0f95-11ea-9963-
00a098884af5:type=cluster,uuid=f963839f-0f95-11ea-9963-00a098884af5",
    "name": "sti2552-4451574693410",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/f963839f-0f95-11ea-
9963-00a098884af5:type=cluster,uuid=f963839f-0f95-11ea-9963-
00a098884af5"
      }
    }
  }
}
```

```

} ,
"svm": {
    "uuid": "7754a99c-101f-11ea-9963-00a098884af5",
    "key": "f963839f-0f95-11ea-9963-
00a098884af5:type=vserver,uuid=7754a99c-101f-11ea-9963-00a098884af5",
    "name": "Testingsvm1",
    "_links": {
        "self": {
            "href": "/api/datacenter/svm/svms/f963839f-0f95-11ea-9963-
00a098884af5:type=vserver,uuid=7754a99c-101f-11ea-9963-00a098884af5"
        }
    }
},
"volume": {
    "uuid": "961778bb-2be9-4b4a-b8da-57c7026e52ad",
    "key": "f963839f-0f95-11ea-9963-
00a098884af5:type=volume,uuid=961778bb-2be9-4b4a-b8da-57c7026e52ad",
    "name": "NSLM_VOL_LUN_1574753881051",
    "_links": {
        "self": {
            "href": "/api/datacenter/storage/volumes/f963839f-0f95-11ea-
9963-00a098884af5:type=volume,uuid=961778bb-2be9-4b4a-b8da-57c7026e52ad"
        }
    }
},
"assigned_performance_service_level": {
    "key": "861f6e4d-0c35-11ea-9d73-fa163e706bc4",
    "name": "Value",
    "peak_iops": 75,
    "expected_iops": 75,
    "_links": {
        "self": {
            "href": "/api/storage-provider/performance-service-
levels/861f6e4d-0c35-11ea-9d73-fa163e706bc4"
        }
    }
},
"recommended_performance_service_level": {
    "key": null,
    "name": "Idle",
    "peak_iops": null,
    "expected_iops": null,
    "_links": {}
},
"assigned_storage_efficiency_policy": {
    "key": null,

```

```

        "name": "Unassigned",
        "_links": {}
    },
    "space": {
        "size": 1024458752
    },
    "os_type": "linux",
    "_links": {
        "self": {
            "href": "/api/storage-provider/luns/f963839f-0f95-11ea-9963-00a098884af5%3Atype%3Dlun%2Cuuid%3D71f3187e-bf19-4f34-ba34-b1736209b45a"
        }
    }
}

```

#### Fehlerbehebungsschritte für Fehler bei der LUN-Erstellung oder -Zuordnung

Beim Abschließen dieses Workflows wird möglicherweise immer noch ein Fehler bei der LUN-Erstellung angezeigt. Selbst wenn die LUN erfolgreich erstellt wird, schlägt die LUN-Zuordnung mit der Initiatorgruppe möglicherweise fehl, da eine SAN-LIF nicht verfügbar ist oder der Zugriffspunkt auf dem Node, auf dem Sie die LUN erstellen, nicht verfügbar ist. Bei einem Ausfall wird die folgende Meldung angezeigt:

The nodes <node\_name> and <partner\_node\_name> have no LIFs configured with the iSCSI or FCP protocol for Vserver <server\_name>. Use the access-endpoints API to create a LIF for the LUN.

Befolgen Sie diese Schritte zur Fehlerbehebung, um diesen Fehler zu umgehen.

1. Erstellen Sie einen Zugriffspunkt, der DAS iSCSI-/FCP-Protokoll auf der SVM unterstützt, auf der Sie die LUN erstellt haben.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	POST	/storage-provider/access-endpoints

#### Stichprobe

Sie müssen die Details des Zugriffspunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.



Stellen Sie sicher, dass Sie im Eingabeparameter den hinzugefügt haben `address` Um den Home-Node der LUN und des anzugeben `ha_address` Um den Partner-Node des Home-Node anzugeben. Bei diesem Vorgang werden sowohl auf dem Home-Node als auch auf dem Partner-Node Zugriffspunkte erstellt.

```

curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept:
    application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>" -d "{
\"data_protocols\": [ \"iscsi\" ], \"ip\": {
    \"address\": \"10.162.83.126\", \"ha_address\": \"10.142.83.126\",
\"netmask\": \"255.255.0.0\" }, \"lun\": { \"key\": \"e4f33f90-f75f-11e8-9ed9-00a098e3215f:type=lun,uuid=b8e0c1ae-0997-47c5-97d2-1677d3ec08ff\" },
\"name\": \"aep_example\" }"

```

2. Fragen Sie den Job mit dem in der JSON-Ausgabe zurückgegebenen Job-Objektschlüssel ab, um zu überprüfen, ob er erfolgreich ausgeführt wurde, um die Zugriffendpunkte auf der SVM hinzuzufügen und dass die iSCSI/FCP-Dienste auf der SVM aktiviert wurden.

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management-server/jobs/{key}

### Beispiel JSON-Ausgabe

Am Ende der Ausgabe sehen Sie den Schlüssel der erstellten Access-Endpunkte. In der folgenden Ausgabe, die "name": "accessEndpointKey" Der Wert gibt den Zugriffendpunkt an, der auf dem Home-Node der LUN erstellt wurde und für den der Schlüssel lautet 9c964258-14ef-11ea-95e2-00a098e32c28. Der "name": "accessEndpointHAKey" Der Wert gibt den Zugriffspunkt an, der auf dem Partner-Node des Home-Nodes erstellt wurde und für den der Schlüssel der Schlüssel ist 9d347006-14ef-11ea-8760-00a098e3215f.

```

"job_results": [
  {
    "name": "accessEndpointKey",
    "value": "e4f33f90-f75f-11e8-9ed9-
00a098e3215f:type=network_lif,lif_uuid=9c964258-14ef-11ea-95e2-
00a098e32c28"
  },
  {
    "name": "accessEndpointHAKey",
    "value": "e4f33f90-f75f-11e8-9ed9-
00a098e3215f:type=network_lif,lif_uuid=9d347006-14ef-11ea-8760-
00a098e3215f"
  }
],
"_links": {
  "self": {
    "href": "/api/management-server/jobs/71377eee0b25633%3A-
30a2dbfe%3A16ec620945d%3A-7f5a"
  }
}
}

```

3. Ändern Sie die LUN, um die Initiatorgruppenzuordnung zu aktualisieren. Weitere Informationen zur Änderung von Workflows finden Sie unter „Modifizieren von Storage-Workloads“.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	PATCH	/storage- provider/lun/{key}

Geben Sie in der Eingabe den Initiatorgruppenschlüssel an, mit dem Sie die LUN-Zuordnung aktualisieren möchten, zusammen mit dem LUN-Schlüssel.

### Stichprobe

```

curl -X PATCH "https://<hostname>/api/storage-provider/luns/e4f33f90-
f75f-11e8-9ed9-00a098e3215f%3Atype%3Dlun%2Cuuid%3Db8e0c1ae-0997-47c5-
97d2-1677d3ec08ff"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>" -d
"{
  \"lun_maps\": [
    {
      \"igroup\": {
        \"key\": \"e4f33f90-f75f-11e8-9ed9-
00a098e3215f:type=igroup,uuid=d19ec2fa-fec7-11e8-b23d-00a098e32c28\",
        \"logical_unit_number\": 3
      }
    }
  ]
}"

```

In der JSON-Ausgabe wird ein Objektschlüssel angezeigt, mit dem Sie überprüfen können, ob die Zuordnung erfolgreich ist.

4. Überprüfen Sie die LUN-Zuordnung, indem Sie mit dem LUN-Schlüssel abfragen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/luns/{key}

### Beispiel JSON-Ausgabe

In der Ausgabe sehen Sie, dass die LUN erfolgreich mit der Initiatorgruppe zugeordnet wurde (Schlüssel) d19ec2fa-fec7-11e8-b23d-00a098e32c28) Mit denen es ursprünglich bereitgestellt wurde.

```
{
  "key": "e4f33f90-f75f-11e8-9ed9-00a098e3215f:type=lun,uuid=b8e0c1ae-0997-47c5-97d2-1677d3ec08ff",
  "name": "/vol/NSLM_VOL_LUN_1575282642267/example_lun",
  "uuid": "b8e0c1ae-0997-47c5-97d2-1677d3ec08ff",
  "cluster": {
    "uuid": "e4f33f90-f75f-11e8-9ed9-00a098e3215f",
    "key": "e4f33f90-f75f-11e8-9ed9-00a098e3215f:type=cluster,uuid=e4f33f90-f75f-11e8-9ed9-00a098e3215f",
    "name": "umeng-aff220-01-02",
    "_links": {
      "self": {
        "href": "/api/datacenter/cluster/clusters/e4f33f90-f75f-11e8-9ed9-00a098e3215f:type=cluster,uuid=e4f33f90-f75f-11e8-9ed9-00a098e3215f"
      }
    }
  },
  "svm": {
    "uuid": "97f47088-fa8e-11e8-9ed9-00a098e3215f",
    "key": "e4f33f90-f75f-11e8-9ed9-00a098e3215f:type=vserver,uuid=97f47088-fa8e-11e8-9ed9-00a098e3215f",
    "name": "NSLM12_SVM_ritu",
    "_links": {
      "self": {
        "href": "/api/datacenter/svm/svms/e4f33f90-f75f-11e8-9ed9-00a098e3215f:type=vserver,uuid=97f47088-fa8e-11e8-9ed9-00a098e3215f"
      }
    }
  },
  "volume": {
    "uuid": "a1e09503-a478-43a0-8117-d25491840263",
    "key": "e4f33f90-f75f-11e8-9ed9-00a098e3215f:type=volume,uuid=a1e09503-a478-43a0-8117-d25491840263"
  }
}
```

```

    "key": "e4f33f90-f75f-11e8-9ed9-
00a098e3215f:type=volume,uuid=a1e09503-a478-43a0-8117-d25491840263",
    "name": "NSLM_VOL_LUN_1575282642267",
    "_links": {
        "self": {
            "href": "/api/datacenter/storage/volumes/e4f33f90-f75f-11e8-
9ed9-00a098e3215f:type=volume,uuid=a1e09503-a478-43a0-8117-d25491840263"
        }
    }
},
"lun_maps": [
{
    "igroup": {
        "uuid": "d19ec2fa-fec7-11e8-b23d-00a098e32c28",
        "key": "e4f33f90-f75f-11e8-9ed9-
00a098e3215f:type=igroup,uuid=d19ec2fa-fec7-11e8-b23d-00a098e32c28",
        "name": "lun55_igroup",
        "_links": {
            "self": {
                "href": "/api/datacenter/protocols/san/igroups/e4f33f90-
f75f-11e8-9ed9-00a098e3215f:type=igroup,uuid=d19ec2fa-fec7-11e8-b23d-
00a098e32c28"
            }
        }
    },
    "logical_unit_number": 3
}
],
"assigned_performance_service_level": {
    "key": "cf2aacda-10df-11ea-bbe6-fa163e599489",
    "name": "Value",
    "peak_iops": 75,
    "expected_iops": 75,
    "_links": {
        "self": {
            "href": "/api/storage-provider/performance-service-
levels/cf2aacda-10df-11ea-bbe6-fa163e599489"
        }
    }
},
"recommended_performance_service_level": {
    "key": null,
    "name": "Idle",
    "peak_iops": null,
    "expected_iops": null,
    "_links": {}
}

```

```

},
"assigned_storage_efficiency_policy": {
    "key": null,
    "name": "Unassigned",
    "_links": {}
},
"space": {
    "size": 1073741824
},
"os_type": "linux",
"_links": {
    "self": {
        "href": "/api/storage-provider/luns/e4f33f90-f75f-11e8-9ed9-00a098e3215f%3Atype%3Dlun%2Cuuid%3Db8e0c1ae-0997-47c5-97d2-1677d3ec08ff"
    }
}
}
}

```

## Änderung von Storage-Workloads

Das Ändern von Storage-Workloads besteht aus der Aktualisierung von LUNs oder File Shares mit fehlenden Parametern oder der Änderung der vorhandenen Parameter.

Dieser Workflow erläutert beispielhaft die Aktualisierung von Performance Service Levels für LUNs und File Shares.



Beim Workflow wird vorausgesetzt, dass die LUN oder Dateifreigabe mit Performance Service-Levels bereitgestellt wurde.

### Ändern von Dateifreigaben

Während Sie eine Dateifreigabe ändern, können Sie die folgenden Parameter aktualisieren:

- Kapazität oder Größe.
- „Online“- oder „Offline“-Einstellung.
- Storage-Effizienzrichtlinie.
- Performance Service Level:
- Einstellungen für die Zugriffssteuerungsliste (Access Control List, ACL).
- Einstellungen für Exportrichtlinien. Sie können auch die Parameter der Exportrichtlinie löschen und die Standardregeln für den (leeren) Export auf der Dateifreigabe zurücksetzen.



Während einer einzelnen API-Ausführung können Sie nur einen Parameter aktualisieren.

Dieses Verfahren beschreibt das Hinzufügen eines Performance Service Levels zu einer Dateifreigabe. Sie können das gleiche Verfahren zum Aktualisieren einer beliebigen anderen Dateifreigabe-Eigenschaft verwenden.

- Holen Sie sich den CIFS-Share oder den NFS-Dateifreigabschlüssel der Dateifreigabe, die Sie aktualisieren möchten. Diese API fragt alle Dateifreigaben in Ihrem Datacenter ab. Überspringen Sie diesen Schritt, wenn Sie den Dateifreigabeconkey bereits kennen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/file-shares

- Zeigen Sie die Details der Dateifreigabe an, indem Sie die folgende API mit dem von Ihnen erhaltenen Dateifreigabschlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/file-shares/{key}

Zeigen Sie die Details der Dateifreigabe in der Ausgabe an.

```
"assigned_performance_service_level": {
    "key": null,
    "name": "Unassigned",
    "peak_iops": null,
    "expected_iops": null,
    "_links": {}
},
```

- Holen Sie sich den Schlüssel für das Performance Service Level, das Sie für diese Dateifreigabe zuweisen möchten. Derzeit ist keine Richtlinie zugewiesen.

Kategorie	HTTP-Verb	Pfad
Performance Service Level	GET	/storage-provider/performance-service-levels



Sie können die Details der vom System definierten Performance-Service-Level abrufen, indem Sie die einstellen `system_defined` Eingabeparameter an `true`. Holen Sie in der Ausgabe den Schlüssel des Performance Service Level, den Sie auf die Dateifreigabe anwenden möchten.

- Wenden Sie den Performance Service Level auf der Dateifreigabe an.

Kategorie	HTTP-Verb	Pfad
Storage Provider	PATCH	/storage-provider/file-shares/{key}

In der Eingabe müssen Sie nur den Parameter angeben, den Sie aktualisieren möchten, zusammen mit dem Dateifreigabeschlüssel. In diesem Fall ist es der Schlüssel zum Performance Service Level.

### Stichprobe

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares" -H  
"accept: application/json" -H "Authorization: Basic  
<Base64EncodedCredentials>" -d  
"{"  
  \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-  
  fa163e82bbf2\" },  
}"
```

Die JSON-Ausgabe zeigt ein Job-Objekt an, mit dem Sie überprüfen können, ob die Zugriffspunkte auf den Home- und Partner-Nodes erfolgreich erstellt wurden.

5. Überprüfen Sie, ob der Performance Service Level zur Dateifreigabe hinzugefügt wurde, indem Sie den Job-Objektschlüssel verwenden, der in Ihrer Ausgabe angezeigt wird.

Kategorie	HTTP-Verb	Pfad
Management Server	GET	/management-server/jobs/{key}

Wenn Sie mit der ID des Job-Objekts abfragen, sehen Sie, ob die Dateifreigabe erfolgreich aktualisiert wurde. Beheben Sie bei einem Ausfall die Fehlerbehebung, und führen Sie die API erneut aus. Wenn die Datei erfolgreich erstellt wurde, fragen Sie die Dateifreigabe ab, um das geänderte Objekt anzuzeigen:

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/file-shares/{key}

Zeigen Sie die Details der Dateifreigabe in der Ausgabe an.

```
"assigned_performance_service_level": {  
  "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",  
  "name": "Value",  
  "peak_iops": 75,  
  "expected_iops": 75,  
  "_links": {  
    "self": {  
      "href": "/api/storage-provider/performance-service-  
      levels/1251e51b-069f-11ea-980d-fa163e82bbf2"  
    }  
  }  
}
```

## LUNs werden aktualisiert

Während Sie eine LUN aktualisieren, können Sie die folgenden Parameter ändern:

- Kapazität oder Größe
- „Online“- oder „Offline“-Einstellung
- Storage-Effizienzrichtlinie
- Performance Service Level
- LUN-Zuordnung



Während einer einzelnen API-Ausführung können Sie nur einen Parameter aktualisieren.

Bei diesem Verfahren wird das Hinzufügen eines Performance Service Levels zu einer LUN beschrieben. Sie können dasselbe Verfahren zum Aktualisieren jeder anderen LUN-Eigenschaft verwenden.

1. Holen Sie den LUN-Schlüssel der LUN, die Sie aktualisieren möchten. Diese API gibt Details zu allen LUNS in Ihrem Datacenter zurück. Überspringen Sie diesen Schritt, wenn Sie den LUN-Schlüssel bereits kennen.

Kategorie	HTTP-Verb	Pfad
Storage Provider	GET	/storage-provider/luns

2. Zeigen Sie die Details der LUN an, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Storage Provider	GET	/storage-provider/luns/{key}

Zeigen Sie die Details der LUN in der Ausgabe an. Sie sehen, dass dieser LUN kein Performance-Service-Level zugewiesen ist.

### Beispiel JSON-Ausgabe

```
"assigned_performance_service_level": {  
    "key": null,  
    "name": "Unassigned",  
    "peak_iops": null,  
    "expected_iops": null,  
    "_links": {}  
},
```

3. Erhalten Sie den Schlüssel für das Performance Service Level, das Sie der LUN zuweisen möchten.

Kategorie	HTTP-Verb	Pfad
Performance Service Level	GET	/storage-provider/performance-service-levels



Sie können die Details der vom System definierten Performance-Service-Level abrufen, indem Sie die einstellen `system_defined` Eingabeparameter an `true`. Holen Sie von der Ausgabe den Schlüssel des Performance Service Level, den Sie auf der LUN anwenden möchten.

#### 4. Wenden Sie den Performance Service Level auf der LUN an.

Kategorie	HTTP-Verb	Pfad
Storage Provider	PATCH	/storage-provider/lun/{key}

Sie müssen in der Eingabe nur den Parameter angeben, den Sie aktualisieren möchten, zusammen mit dem LUN-Schlüssel. In diesem Fall ist es der Schlüssel zum Performance Service Level.

#### Stichprobe

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-Type: application/json" -H "Authorization: Basic <Base64EncodedCredentials>" -d "{\"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-fa163e82bbf2\" }}
```

In der JSON-Ausgabe wird ein Objektschlüssel angezeigt, mit dem Sie die aktualisierte LUN überprüfen können.

#### 5. Zeigen Sie die Details der LUN an, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

Kategorie	HTTP-Verb	Pfad
Storage Provider	GET	/storage-provider/luns/{key}

Zeigen Sie die Details der LUN in der Ausgabe an. Sie sehen, dass dieser LUN das Performance-Service-Level zugewiesen ist.

#### Beispiel JSON-Ausgabe

```

"assigned_performance_service_level": {
    "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
    "name": "Value",
    "peak_iops": 75,
    "expected_iops": 75,
    "_links": {
        "self": {
            "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
        }
    }
}

```

## Ändern einer NFS-Dateifreigabe zur Unterstützung von CIFS

Sie können eine NFS-Dateifreigabe ändern, um CIFS-Protokoll zu unterstützen. Während der Erstellung von Dateifreigabe können sowohl ACL-Parameter (Access Control List) als auch Richtlinienregeln für den Export für dieselbe Dateifreigabe festgelegt werden. Wenn Sie jedoch CIFS auf demselben Volume aktivieren möchten, auf dem Sie eine NFS-Dateifreigabe erstellt haben, können Sie die ACL-Parameter auf dieser Dateifreigabe aktualisieren, um CIFS zu unterstützen.

### Bevor Sie beginnen

1. Eine NFS-Dateifreigabe muss nur mit den Details der Exportrichtlinie erstellt worden sein. Informationen hierzu finden Sie unter „*Managen von Dateifreigaben*“ und „*Ändern von Storage-Workloads*“.
2. Sie müssen über den Dateifreigabschlüssel verfügen, um diesen Vorgang ausführen zu können. Informationen zum Anzeigen von Details zur Dateifreigabe und zum Abrufen des Dateifreigabschlüssels mithilfe der Job-ID finden Sie unter *Provisioning CIFS and NFS File Shares*.

### Über diese Aufgabe

Dies gilt für eine NFS-Dateifreigabe, die Sie erstellt haben, indem Sie nur Richtlinien für den Export hinzufügen und nicht die ACL-Parameter. Sie ändern die NFS-Dateifreigabe, um die ACL-Parameter einzubeziehen.

### Schritte

1. Führen Sie auf der NFS-Dateifreigabe einen aus `PATCH` Operation mit den ACL-Details für den Zugriff auf CIFS.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	<code>PATCH</code>	<code>/storage-provider/file- shares</code>

### Stichprobe

Basierend auf den Zugriffsberechtigungen, die Sie der Benutzergruppe zuweisen, wird wie im folgenden Beispiel angezeigt eine ACL erstellt und der Dateifreigabe zugewiesen.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
  }
}
```

### Beispiel JSON-Ausgabe

Der Vorgang gibt die Job-ID des Jobs zurück, der das Update ausführt.

- Überprüfen Sie, ob die Parameter korrekt hinzugefügt wurden, indem Sie die Details zur Dateifreigabe für dieselbe Dateifreigabe abfragen.

Kategorie	HTTP-Verb	Pfad
Anbieter von Storage-Lösungen	GET	/storage-provider/file-shares/{key}

### Beispiel JSON-Ausgabe

```
"access_control": {
  "acl": [
    {
      "user_or_group": "everyone",
      "permission": "read"
    }
  ],
  "export_policy": {
    "id": 1460288880641,
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
    "name": "default",
    "rules": [
      {
        "anonymous_user": "65534",
        "clients": [
          {
            "match": "0.0.0.0/0"
          }
        ],
        "groups": [
          "everyone"
        ]
      }
    ]
  }
}
```

```

        "index": 1,
        "protocols": [
            "nfs3",
            "nfs4"
        ],
        "ro_rule": [
            "sys"
        ],
        "rw_rule": [
            "sys"
        ],
        "superuser": [
            "none"
        ]
    },
    {
        "anonymous_user": "65534",
        "clients": [
            {
                "match": "0.0.0.0/0"
            }
        ],
        "index": 2,
        "protocols": [
            "cifs"
        ],
        "ro_rule": [
            "ntlm"
        ],
        "rw_rule": [
            "ntlm"
        ],
        "superuser": [
            "none"
        ]
    }
],
"_links": {
    "self": {
        "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959?type=export_policy,uuid=1460288880641"
    }
}
}

```

```
  "_links": {
    "self": {
      "href": "/api/storage-provider/file-shares/7d5a59b3-953a-11e8-8857-00a098dcc959?type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
    }
  }
```

Sie können die ACL sehen, die zusammen mit der Exportrichtlinie in die gleiche Dateifreigabe zugewiesen wurde.

#### Änderung von Workloads für das Upgrade von QoS auf AQoS

Active IQ Unified Manager unterstützt sowohl herkömmliche QoS als auch AQoS (Adaptive QoS), die den von Unified Manager gemanagten Storage-Workloads zugeordnet sind.

Wenn Sie Ihre ONTAP-Cluster von 9.1 auf 9.3 (für Dateifreigaben) und 9.4 (für LUNs) aktualisieren, können Sie die traditionelle QoS der jeweiligen von Unified Manager verwalteten Workloads auf AQoS aktualisieren.

## 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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 VERTRÄGLICH 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.