Storage mithilfe von REST APIs verwalten

Active IQ Unified Manager

NetApp
November 13, 2026

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

Inhalt

Storage mithilfe von REST APIs verwalten . . . 1
Erste Schritte mit Active IQ Unified Manager . . . 1
Erste Schritte mit Active IQ Unified Manager REST APIs . . . 1
Vorgesehene Benutzer der Active IQ Unified Manager REST APIs . . . 1
API-Zugriff und Kategorien in Active IQ Unified Manager verwalten . . . 1
REST Services verstehen, die in Active IQ Unified Manager angeboten werden . . . 3
API-Versionsnummern in Active IQ Unified Manager verstehen . . . 3
Verständnis des ONTAP Speicherressourcenmodells in Active IQ Unified Manager . . . 4
Zugriff über REST API und Authentifizierung in Active IQ Unified Manager . . . 5
Zugriff auf REST APIs und Authentifizierung in Active IQ Unified Manager . . . 5
Informationen zu den HTTP-Statuscodes von Active IQ Unified Manager . . . 8
Empfohlene Vorgehensweisen für die Verwendung von Active IQ Unified Manager APIs . . . 9
Fehlerbehebung mithilfe von Systemprotokollen in Active IQ Unified Manager . . . 10
Informationen dazu, wie Active IQ Unified Manager Jobobjekte für die asynchrone Verarbeitung verwendet . . . 10
Informationen zum Hello API Server Beispielprogramm in Active IQ Unified Manager . . . 11
Unified Manager REST-APIs . . . 15
Kategorien für Active IQ Unified Manager REST APIs verstehen . . . 15
Verwaltung von Speicherobjekten in einem Rechenzentrum mithilfe von APIs in Active IQ Unified Manager . . . 16
Zugriff auf ONTAP APIs über Proxyzugriff in Active IQ Unified Manager . . . 22
Administrative Aufgaben mithilfe von APIs in Active IQ Unified Manager ausführen . . . 25
Benutzerverwaltung in Active IQ Unified Manager mithilfe von APIs . . . 27
Leistungsmetriken mithilfe von APIs in Active IQ Unified Manager anzeigen . . . 28
Aufträge und Systemdetails können über APIs in Active IQ Unified Manager angezeigt werden . . . 38
Verwaltung von Ereignissen und Warnmeldungen mithilfe von APIs in Active IQ Unified Manager . . . 39
Arbeitslasten verwalten . . . 43
Gängige Arbeitsabläufe für das Storage Management . . . 51
Informationen zu gängigen API-Workflows für die Speicherverwaltung in Active IQ Unified Manager . . . 51
Ermittlung von Speicherplatzproblemen in Aggregaten mithilfe der Active IQ Unified Manager APIs . . . 52
Probleme mit Speicherobjekten mithilfe der Event-APIs von Active IQ Unified Manager ermitteln . . . 54
Fehlerbehebung bei ONTAP Volumes mithilfe der Active IQ Unified Manager Gateway APIs . . . 55
Workflows für das Workload-Management . . . 58

Storage mithilfe von REST APIs verwalten

Erste Schritte mit Active IQ Unified Manager

Erste Schritte mit Active IQ Unified Manager REST APIs

Active IQ Unified Manager bietet eine Reihe von APIs zum Managen Ihrer Storage Ressourcen auf den unterstützten Storage Systemen über eine RESTful-Webservice-Schnittstelle für beliebige Drittanbieterintegrationen.

In diesen Abschnitten finden Sie Informationen zu den Unified Manager APIs, Beispiel-Workflows zur Behebung spezifischer Probleme sowie Beispielcode. Mithilfe dieser Informationen können Sie RESTful-Clients von NetApp Manageability-Softwarelösungen für das Management von NetApp Systemen erstellen. Die APIs basieren auf dem Architekturstil Representational State Transfer (REST). Alle vier REST-Operationen Create, Read, Update und Delete, auch als CRUD bezeichnet, werden unterstützt.

Zusätzliche Ressourcen und Details zu den Vorteilen der Active IQ Unified Manager REST API finden Sie unter "Active IQ Unified Manager".

Vorgesehene Benutzer der Active IQ Unified Manager REST APIs

Die hier behandelten Themen richten sich an Entwickler, die Applikationen erstellen, die über REST-APIs mit der Active IQ Unified Manager Software interagieren.

Storage Administratoren und -Architekten können diese Informationen nutzen, um ein grundlegendes Verständnis dafür zu erlangen, wie die Unified Manager REST APIs zum Erstellen von Client Applikationen für das Managen und Überwachen von NetApp Storage Systemen verwendet werden können.

Diese Informationen sind relevant, wenn Sie den Storage-Provider, ONTAP cluster und Management-Administrations-APIs zum Managen Ihres Storage verwenden möchten.

> Sie müssen über eine der folgenden Rollen verfügen: Operator, Storage Administrator oder Application Administrator. Sie müssen die IP-Adresse oder die vollqualifizierte Domain des Unified Manager Servers kennen, auf dem Sie die REST APIs ausführen möchten.

API-Zugriff und Kategorien in Active IQ Unified Manager verwalten

Mit den Active IQ Unified Manager APIs können Sie Storage-Objekte in Ihrer Umgebung managen und provisionieren. Einige dieser Funktionen sind auch über die Unified Manager Web-UI zugänglich.

Eine URL für den direkten Zugriff auf REST-APIs erstellen

Sie können über eine Programmiersprache wie Python, C#, C++++, JavaScript usw. direkt auf die REST APIs zugreifen. Für den Zugriff auf die REST APIs werden der Hostname oder die IP-Adresse und die URL im folgenden Format eingegeben

https://<hostname>/api

> Der Standardport ist 443. Sie können den Port entsprechend Ihrer Umgebung konfigurieren.

Zugriff auf die Online-API-Dokumentationsseite

Sie können die mit dem Produkt bereitgestellte Referenzinhaltsseite *API Documentation* aufrufen, um die API-Dokumentation anzuzeigen und einen API-Aufruf manuell auszuführen, beispielsweise über die Schnittstelle Swagger. Der Zugriff auf diese Dokumentation erfolgt über **Menu Bar** > **Help button** > **API Documentation**.

Alternativ können Sie den Hostnamen oder die IP-Adresse und die URL für den Zugriff auf die REST API-Seite im folgenden Format eingeben

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

Kategorien

Die API-Aufrufe sind funktional nach Bereichen oder Kategorien organisiert. Eine bestimmte API lässt sich über die entsprechende API-Kategorie auffinden.

Die mit Unified Manager bereitgestellten REST-APIs unterstützen Sie bei administrativen, Überwachungs- und Provisionierungsfunktionen. Die APIs sind in folgende Kategorien unterteilt.

- **Datacenter**

  Diese Kategorie umfasst die APIs, die Sie bei der Storage-Verwaltung und -Analyse im Datacenter mithilfe von Tools wie Work Flow Automation und Ansible unterstützen. Die REST-APIs dieser Kategorie liefern Informationen über Cluster, Knoten, Aggregate, Volumes, LUNs, Dateifreigaben, Namespaces und andere Elemente in Ihrem Datacenter.

- **Management-Server**

  Die APIs in der Kategorie **management-server** umfassen die `jobs, system,` und `events` APIs. Jobs sind Operationen, die für die asynchrone Ausführung geplant sind und mit dem Managen von Storage Objekten oder Workloads in Unified Manager zusammenhängen. Die `events` API gibt Ereignisse in Ihrem Datacenter zurück, und die `system` API gibt die Details der Unified Manager Instanz zurück.

- **storage-provider**

  Diese Kategorie enthält alle APIs für die Provisionierung, die für das Managen und die Provisionierung von Dateifreigaben, LUNs, Performance Service Levels und Storage-Effizienzrichtlinien erforderlich sind. Die APIs ermöglichen außerdem die Konfiguration von Zugriffsendpunkten und Active Directories sowie die Zuweisung von Performance Service Levels und Storage-Effizienzrichtlinien zu Storage-Workloads.

- **Verwaltung**

  Diese Kategorie enthält die APIs, die für die Ausführung administrativer Aufgaben verwendet werden, z. B. für die Pflege der Sicherungseinstellungen, das Anzeigen von Truststore-Zertifikaten für die Unified Manager Datenquellen und das Managen von ONTAP Clustern als Datenquellen für Unified Manager.

- **Gateway**

  Unified Manager ermöglicht es Ihnen, ONTAP REST-APIs über die APIs in der Gateway-Kategorie aufzurufen und die Storage Objekte in Ihrem Datacenter zu managen.

- **Sicherheit**

  Diese Kategorie enthält APIs zum Managen von Unified Manager Benutzern.

REST Services verstehen, die in Active IQ Unified Manager angeboten werden

Sie sollten sich mit den angebotenen REST Services und Operationen vertraut machen, bevor Sie die Active IQ Unified Manager APIs verwenden.

Die Provisionierungs- und Verwaltungs-APIs, die zur Konfiguration des API-Servers verwendet werden, unterstützen Lese- (GET) oder Schreibvorgänge (POST, PATCH, DELETE). Im Folgenden sind einige Beispiele für die von den APIs unterstützten GET-, PATCH-, POST- und DELETE-Operationen aufgeführt:

- Beispiel für GET: `GET /datacenter/cluster/clusters` ruft Clusterdetails in Ihrem Datacenter ab. Die maximale Anzahl der Datensätze, die von der `GET` Operation zurückgegeben wird, beträgt 1000.

> Die APIs ermöglichen Ihnen, die Datensätze nach unterstützten Attributen zu filtern, zu sortieren und zu ordnen.

- 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 mithilfe ihres eindeutigen Schlüssels.
- Beispiel für DELETE: `DELETE /storage-provider/access-endpoints/{key}` löscht einen Zugriffsendpunkt von einer LUN, SVM oder Dateifreigabe mithilfe seines eindeutigen Schlüssels.

Die mit den APIs ausführbaren REST-Operationen hängen von der Rolle des Benutzers Operator, Storage Administrator oder Application Administrator ab.

Benutzerrolle	Unterstützte REST-Methode
Operator	Schreibgeschützter Zugriff auf die Daten. Benutzer mit dieser Rolle können alle GET-Anfragen ausführen.
Storage-Administrator	Lesezugriff auf alle Daten. Benutzer mit dieser Rolle können alle GET-Anfragen ausführen. Darüber hinaus verfügen sie über Schreibzugriff (zum Ausführen von PATCH-, POST- und DELETE-Anfragen), um bestimmte Aktivitäten auszuführen, z. B. das Managen von Storage Service Objekten und Storage Management Optionen.
Anwendungsadministrator	Lese- und Schreibzugriff auf alle Daten. Benutzer mit dieser Rolle können GET-, PATCH-, POST- und DELETE-Anfragen für alle Funktionen ausführen.

Weitere Informationen zu allen REST-Operationen enthält die *Online API Dokumentation*.

API-Versionsnummern in Active IQ Unified Manager verstehen

Die REST-API-URIs in Active IQ Unified Manager enthalten eine Versionsnummer. Zum 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, indem eine Antwort zurückgegeben wird, die der Client verarbeiten

kann.

Der numerische Teil dieser Versionsnummer wird im Verhältnis zu Releases fortlaufend erhöht. URIs mit einer Versionsnummer bieten eine konsistente Schnittstelle, die in zukünftigen Releases die Abwärtskompatibilität beibehält. Dieselben APIs finden Sie auch ohne Versionsangabe, zum Beispiel `/datacenter/svm/svms`, die die Basis-APIs ohne Version kennzeichnen. Die Basis-APIs sind immer die neueste Version der APIs.

> In der oberen rechten Ecke Ihrer Swagger-Oberfläche können Sie die zu verwendende API-Version auswählen. Standardmäßig ist die höchste Version ausgewählt. Es wird empfohlen, die höchste verfügbare Version der jeweiligen API (bezogen auf die fortlaufende Versionsnummer) in Ihrer Unified Manager-Instanz zu verwenden.

Bei allen Anfragen ist die gewünschte API-Version explizit anzugeben. Wenn die Versionsnummer angegeben ist, liefert der Dienst keine Antwortelemente zurück, die Ihre Applikation nicht verarbeiten kann. In REST-Anfragen sollte der Versionsparameter angegeben werden. Ältere Versionen der APIs werden nach einigen Releases schließlich als veraltet markiert. In diesem Release ist die `v1`Version der APIs veraltet.

Verständnis des ONTAP Speicherressourcenmodells in Active IQ Unified Manager

Die Storage Ressourcen in ONTAP lassen sich grob in *physische Storage Ressourcen* und *logische Storage Ressourcen* unterteilen. Für ein effektives Management Ihrer ONTAP Systeme mithilfe der in Active IQ Unified Manager bereitgestellten APIs ist ein Verständnis des Storage Ressourcenmodells und der Beziehungen zwischen den verschiedenen Storage Ressourcen erforderlich.

- **Physische Storage Ressourcen**

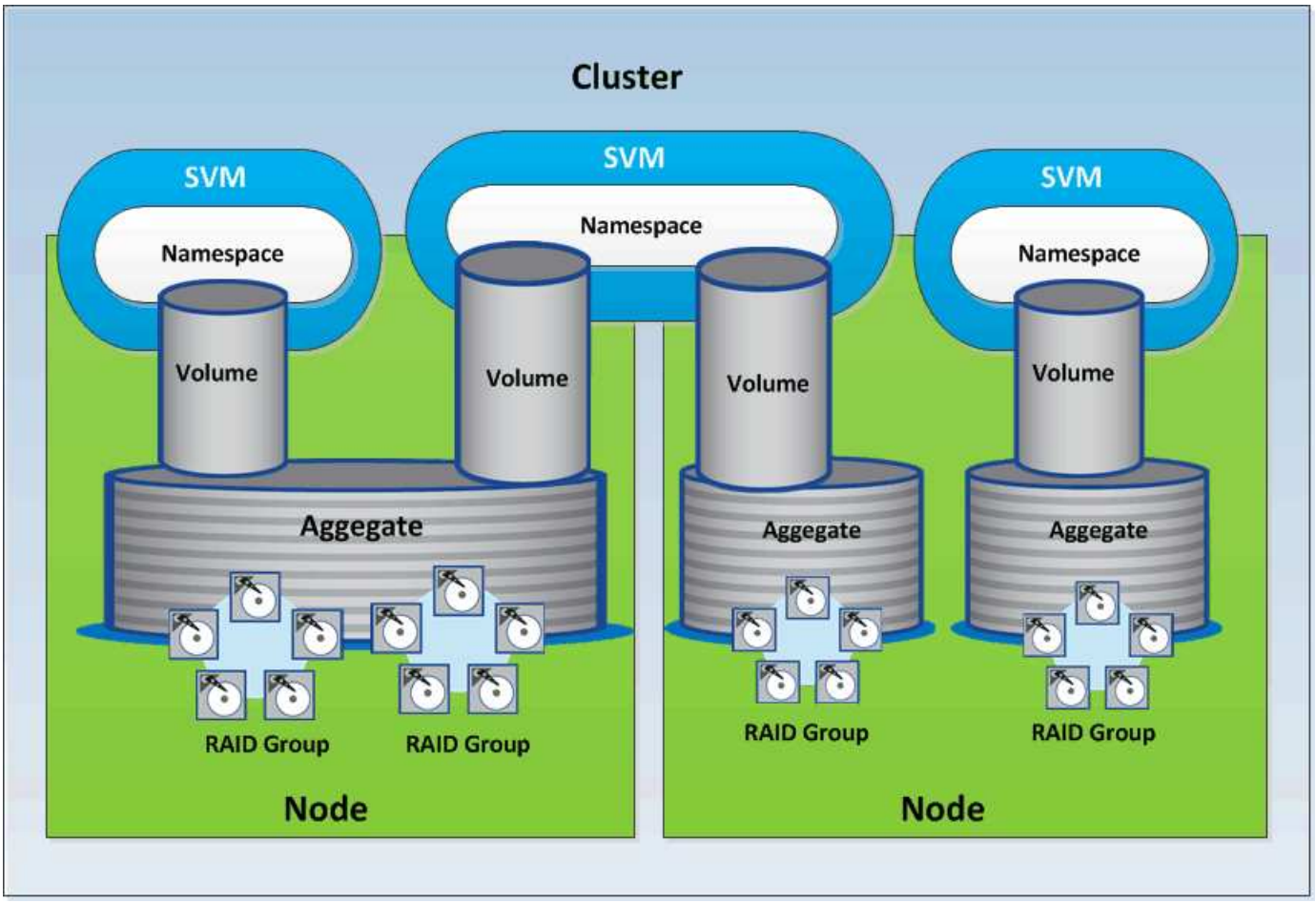
  Bezieht sich auf die physischen Storage Objekte, die von ONTAP bereitgestellt werden. Zu den physischen Storage Ressourcen gehören Festplatten, Cluster, Storage Controller, Knoten und Aggregate.

- **Logische Storage-Ressourcen**

  Bezeichnet die von ONTAP bereitgestellten Storage Ressourcen, die nicht an eine physische Ressource gebunden sind. Diese Ressourcen sind einer Storage Virtual Machine (SVM, ehemals Vserver) zugeordnet und existieren unabhängig von einer spezifischen physischen Storage Ressource wie einer Festplatte, einer Array LUN oder einem Aggregat.

  Zu den logischen Storage-Ressourcen gehören Volumes aller Typen und qtrees sowie die Funktionen und Konfigurationen, die mit diesen Ressourcen verwendet werden können, wie z. B. Snapshot Kopien, Deduplizierung, Komprimierung und Quotas.

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



Zugriff über REST API und Authentifizierung in Active IQ Unified Manager

Zugriff auf REST APIs und Authentifizierung in Active IQ Unified Manager

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

Beispiel einer Anfrage und Antwort:

- **Anfrage**

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

- **Antwort**

```
{
  "records": [
```

```
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "name": "fas8040-206-21",
      "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "contact": null,
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "isSanOptimized": false,
      "management_ip": "10.226.207.25",
      "nodes": [
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
          "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "name": "fas8040-206-21-01",
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 13924095,
          "serial_number": "701424000157"
        },
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
```

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

- *IP address/hostname* ist die IP-Adresse oder die vollqualifizierte Domain (FQDN) des API-Servers.
- Port 443

443 ist der Standardport für HTTPS. Sie können den HTTPS Port bei Bedarf anpassen.
Zum Senden von HTTP-Anfragen aus einem Webbrowser ist die Verwendung von REST API Browser Plugins erforderlich. Der Zugriff auf die REST API ist auch über Skriptplattformen wie cURL und Perl möglich.

Authentifizierung

Unified Manager unterstützt das grundlegende HTTP-Authentifizierungsschema für APIs. Für einen sicheren Informationsfluss (Anfrage und Antwort) sind die REST-APIs nur über HTTPS zugänglich. Der API-Server stellt allen Clients zur Serververifizierung ein selbstsigniertes SSL-Zertifikat bereit. 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 aufzurufen. Die Benutzer können lokale Benutzer (Benutzerprofile in der lokalen Datenbank) oder LDAP-Benutzer sein (sofern

Sie den API-Server für die Authentifizierung über LDAP konfiguriert haben). Der Benutzerzugriff lässt sich verwalten, wenn Sie sich an der Benutzeroberfläche der Unified Manager Administration Console anmelden.

Informationen zu den HTTP-Statuscodes von Active IQ Unified Manager

Beim Ausführen der APIs oder bei der Fehlerbehebung ist es wichtig, die verschiedenen HTTP-Statuscodes und Fehlercodes zu kennen, die von Active IQ Unified Manager APIs verwendet werden.

Die folgende Tabelle listet die Fehlercodes im Zusammenhang mit der Authentifizierung auf:

HTTP-Statuscode	Statuscode-Titel	Beschreibung
200	OK	Wird bei erfolgreicher Ausführung synchroner API-Aufrufe zurückgegeben.
201	Erstellt	Erstellung neuer Ressourcen durch synchrone Aufrufe, wie z. B. die Konfiguration von Active Directory.
202	Akzeptiert	Wird bei erfolgreicher Ausführung asynchroner Aufrufe für Provisionierungsfunktionen wie das Erstellen von LUNs und Dateifreigaben zurückgegeben.
400	Ungültige Anforderung	Weist auf einen Fehler bei der Eingabevalidierung hin. Die Eingaben müssen korrigiert werden, beispielsweise durch die Verwendung gültiger Schlüssel in einem Anfragetext.
401	Nicht autorisierte Anforderung	Sie sind nicht berechtigt, die Ressource anzuzeigen/Nicht autorisiert.
403	Verbotene Anfrage	Der Zugriff auf die Ressource, die Sie erreichen wollten, ist nicht zulässig.
404	Ressource nicht gefunden	Die Ressource, die Sie erreichen wollten, wurde nicht gefunden.
405	Methode nicht zulässig	Methode nicht zulässig.
429	Zu viele Anfragen	Wird zurückgegeben, wenn der Benutzer innerhalb einer bestimmten Zeit zu viele Anfragen sendet.

HTTP-Statuscode	Statuscode-Titel	Beschreibung
500	Interner Serverfehler	Interner Serverfehler. Es konnte keine Antwort vom Server empfangen werden. Dieser interne Serverfehler kann dauerhaft sein oder auch nicht. Wenn Sie beispielsweise einen `GET` oder `GET ALL` Vorgang ausführen und diesen Fehler erhalten, wird empfohlen, den Vorgang mindestens fünfmal zu wiederholen. Wenn es sich um einen dauerhaften Fehler handelt, bleibt der zurückgegebene Statuscode 500. Wenn der Vorgang erfolgreich ist, lautet der zurückgegebene Statuscode 200.

Empfohlene Vorgehensweisen für die Verwendung von Active IQ Unified Manager APIs

Bei der Verwendung der APIs in Active IQ Unified Manager sollten Sie bestimmte empfohlene Vorgehensweisen beachten.

- Für eine gültige Ausführung müssen alle Antwortinhalte folgendes Format aufweisen:

```
application/json
```

- Die API-Versionsnummer steht in keinem Zusammenhang mit der Produktversionsnummer. Sie sollten die neueste Version der API verwenden, die für Ihre Unified Manager Instanz verfügbar ist. Weitere Informationen zu Unified Manager API-Versionen finden Sie im Abschnitt “REST API versioning in Active IQ Unified Manager”.
- Beim Aktualisieren von Array-Werten mithilfe der Unified Manager API muss die gesamte Zeichenfolge der Werte aktualisiert werden. Es ist nicht möglich, Werte an ein Array anzuhängen. Ein vorhandenes Array kann lediglich ersetzt werden.
- Sie können Filteroperatoren wie Pipe (|) und Wildcard (*) für alle Abfrageparameter verwenden, außer für Double-Werte, zum Beispiel IOPS und Performance in den metrics APIs.
- Von Abfragen von Objekten mit einer Kombination der Filteroperatoren Wildcard (*) und Pipe (|) ist abzuraten. Dabei könnte eine falsche Anzahl von Objekten abgerufen werden.
- Bei der Verwendung von Werten für Filter ist sicherzustellen, dass der Wert keine `?`Zeichen enthält. Dies dient der Verringerung des Risikos von SQL-Injection.
- Es ist zu beachten, dass die `GET` (all)-Anfrage für jede API maximal 1000 Datensätze zurückgibt. Auch wenn die Abfrage mit dem `max_records` Parameter auf einen Wert über 1000 gesetzt wird, werden nur 1000 Datensätze zurückgegeben.
- Für die Durchführung administrativer Funktionen empfiehlt sich die Verwendung der Unified Manager UI.

Fehlerbehebung mithilfe von Systemprotokollen in Active IQ Unified Manager

Systemprotokolle ermöglichen es Ihnen, die Ursachen von Fehlern zu analysieren und Probleme bei der Fehlerbehebung zu untersuchen, die beim Ausführen der APIs auftreten können.

Für die Fehlerbehebung bei Problemen im Zusammenhang mit den API-Aufrufen sind die Protokolle am folgenden Speicherort abrufbar.

Protokollspeicherort	Verwenden
`/var/log/ocie/access_log.log`	Enthält alle Details zum API-Aufruf, wie z. B. den Benutzernamen des Benutzers, der die API aufruft, Startzeit, Ausführungszeit, Status und URL. Mithilfe dieser Protokolldatei können Sie die häufig genutzten APIs überprüfen oder Fehler bei jedem GUI-Workflow beheben. Außerdem können Sie sie auf Grundlage der Ausführungszeit zur Skalierung von Analysen verwenden.
`/var/log/ocum/ocumserver.log`	Enthält alle API-Ausführungsprotokolle. Mit dieser Protokolldatei können Sie Fehler bei den API-Aufrufen beheben und die API-Aufrufe debuggen.
`/var/log/ocie/server.log`	Enthält alle Wildfly Server Deployments und Protokolle zu Services für Start/Stopp. Mithilfe dieser Protokolldatei können Sie die Grundursache von Problemen ermitteln, die beim Starten, Stoppen oder Deployment des Wildfly Servers auftreten.
`/var/log/ocie/au.log`	Enthält Protokolle im Zusammenhang mit der Acquisition Unit. Sie können diese Protokolldatei verwenden, wenn Sie in ONTAP Objekte erstellt, geändert oder gelöscht haben, diese Änderungen jedoch nicht in den Active IQ Unified Manager REST APIs berücksichtigt werden.

Informationen dazu, wie Active IQ Unified Manager Jobobjekte für die asynchrone Verarbeitung verwendet

Active IQ Unified Manager stellt die `jobs`API bereit, die Informationen über die während der Ausführung anderer APIs ausgeführten Jobs abruft. Kenntnisse darüber, wie die asynchrone Verarbeitung mithilfe des Job-Objekts funktioniert, sind erforderlich.

Einige API-Aufrufe, insbesondere solche zum Hinzufügen oder Ändern von Ressourcen, können länger dauern als andere. Unified Manager verarbeitet diese zeitaufwändigen Anfragen asynchron.

Asynchrone Anfragen werden mithilfe des Job-Objekts beschrieben.

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

Abfrage des Job-Objekts, das einer API-Anfrage zugeordnet ist

Das in der HTTP-Antwort zurückgegebene Job-Objekt enthält mehrere Eigenschaften. Sie können die Eigenschaft state abfragen, um festzustellen, ob die Anfrage erfolgreich abgeschlossen wurde. Ein Job-Objekt kann sich in einem der folgenden Zustände befinden:

- `NORMAL`
- `WARNING`
- `PARTIAL_FAILURES`
- `ERROR`

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

- Bei einer Standard-Abfrage wird der aktuelle Jobstatus sofort zurückgegeben.
- Long Polling-Anfrage: Wenn sich der Jobstatus zu `NORMAL, ERROR,` oder `PARTIAL_FAILURES.` ändert

Schritte bei einer asynchronen Anfrage

Sie können die folgende allgemeine Vorgehensweise verwenden, um einen asynchronen API-Aufruf durchzuführen:

1. Führe den asynchronen API-Aufruf aus.
2. Sie erhalten eine HTTP-Antwort 202, die die erfolgreiche Annahme der Anfrage signalisiert.
3. Extrahieren Sie die Kennung für das Job-Objekt aus dem Antworttext.
4. Innerhalb einer Schleife auf das Erreichen des Endzustands durch das Job-Objekt `NORMAL, ERROR,` oder `PARTIAL_FAILURES.` warten
5. Überprüfung des Endstatus des Jobs und Abruf des Jobergebnisses.

Informationen zum Hello API Server Beispielprogramm in Active IQ Unified Manager

Der Hello API server ist ein Beispielprogramm, das zeigt, wie eine REST API in Active IQ Unified Manager mit einem einfachen REST Client aufgerufen wird. Das Beispielprogramm liefert grundlegende Informationen über den API Server im JSON Format (der Server unterstützt nur `application/json`Format).

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

- Die IP-Adresse oder der FQDN des API-Servers

- Optional: Portnummer (Standard: 443)
- Benutzername
- Passwort
- Antwortformat (`application/json`)

Zum Aufrufen von REST-APIs können Sie auch andere Skripte wie Jersey und RESTEasy verwenden, um einen Java-REST-Client für Active IQ Unified Manager zu schreiben. Die folgenden Hinweise zum Beispielcode sollten beachtet werden:

- Verwendet eine HTTPS-Verbindung zu Active IQ Unified Manager, um die angegebene REST-URI aufzurufen
- Ignoriert das von Active IQ Unified Manager bereitgestellte Zertifikat
- Überspringt die Hostnamenüberprüfung während des Handschlags
- Verwendet `javax.net.ssl.HttpsURLConnection` für eine URI-Verbindung
- Verwendet eine Drittanbieter-Bibliothek (`org.apache.commons.codec.binary.Base64`) zum Erstellen der Base64-kodierten Zeichenkette, die bei der HTTP-Basisauthentifizierung verwendet wird

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

```
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                    TrustManager[]{new
X509TrustManager(){
```

```
     public X509Certificate[] getAcceptedIssuers(){return  null;}
     public void checkClientTrusted(X509Certificate[]
certs, String authType){}
     public void checkServerTrusted(X509Certificate[]
certs, String authType){}            }};            /* Initialize the
SSLContext with the all-trusting trust manager */
     SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));            URL url = new URL(server_url);            conn =
(HttpsURLConnection) url.openConnection();            /* Do not perform an
actual hostname verification during SSL Handshake.            Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {               public
boolean verify(String host, SSLSession                        session) {
return true;               }            });        } catch (Exception e)
{            e.printStackTrace();        }        return conn;    }

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

}
```

Unified Manager REST-APIs

Kategorien für Active IQ Unified Manager REST APIs verstehen

In diesem Abschnitt sind die REST APIs für Active IQ Unified Manager nach Kategorien aufgeführt.

Sie können in Ihrer Unified Manager Instanz die Online-Dokumentationsseite anzeigen, die die Details zu jedem REST API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder in diesem Dokument aufgeführte oder beschriebene API-Aufruf enthält nur die Informationen, die Sie benötigen, um den Aufruf auf der Dokumentationsseite zu finden. Nachdem Sie einen bestimmten API-Aufruf gefunden haben, können Sie die vollständigen Details dieses Aufrufs prüfen, einschließlich der

Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Typs der Anforderungsverarbeitung.

Die folgenden Informationen sind für jeden API-Aufruf innerhalb eines Workflows enthalten, um den Aufruf auf der Dokumentationsseite zu finden:

- Kategorie

  Die API-Aufrufe sind auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien unterteilt. Einen bestimmten API-Aufruf finden Sie, wenn Sie bis zum Ende der Seite scrollen und anschließend auf die entsprechende API-Kategorie klicken.

- HTTP-Verb (Aufruf)

  Das HTTP-Verb identifiziert die an einer Ressource ausgeführte Aktion. Jeder API-Aufruf erfolgt über ein einzelnes HTTP-Verb.

- Pfad

  Der Pfad bestimmt die spezifische Ressource, die die Aktion im Rahmen eines Aufrufs verwendet. Die Pfadzeichenfolge wird an die Kern-URL angehängt, um die vollständige URL zu bilden, die die Ressource identifiziert.

Verwaltung von Speicherobjekten in einem Rechenzentrum mithilfe von APIs in Active IQ Unified Manager

Die REST-APIs in der `datacenter` Kategorie ermöglichen Ihnen das Managen der Storage Objekte in Ihrem Datacenter, wie z. B. Cluster, Knoten, Aggregate, Storage VMs, Volumes, LUNs, Dateifreigaben und Namespaces. Diese APIs stehen zum Abfragen der Konfiguration der Objekte zur Verfügung, während einige von ihnen das Hinzufügen, Löschen oder Ändern dieser Objekte ermöglichen.

Die meisten dieser APIs sind GET-Aufrufe, die clusterübergreifende Aggregation mit Unterstützung für Filtern, Sortieren und Paginierung bereitstellen. Bei der Ausführung dieser APIs geben sie Daten aus der Datenbank zurück. Daher müssen neu erstellte Objekte im nächsten Datenabrufzyklus erkannt werden, damit sie in der Antwort erscheinen.

Um die Details eines bestimmten Objekts abzufragen, müssen Sie die eindeutige ID dieses Objekts eingeben, um dessen Details anzuzeigen. Informationen zu Metriken und Analysen der Storage Objekte finden Sie beispielsweise unter "Anzeigen von Performance-Kennzahlen".

```
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 zu den APIs sind über Ihre Swagger API Schnittstelle verfügbar. Sie können die Ergebnisse anhand bestimmter Parameter filtern und sortieren, wie in Swagger angegeben. Diese APIs ermöglichen es Ihnen, die Ergebnisse nach bestimmten Storage Objekten wie Cluster, Volume oder Storage VM zu filtern.

APIs für Storage-Objekte in Ihrem Datacenter

HTTP-Verb	Pfad	Beschreibung

GET	`/datacenter/cluster/clusters`
	
	`/datacenter/cluster/clusters/{key}`
		Mit dieser Methode lassen sich die Details der ONTAP Cluster im gesamten Datacenter anzeigen. Die API liefert Informationen wie die IPv4- oder IPv6-Adresse des Clusters, Informationen über den Node, z. B. den Systemstatus des Node, die Performance Kapazität und das High Availability (HA) Paar, und gibt an, ob der Cluster ein All SAN Array ist.

GET	`/datacenter/cluster/licensing/licenses` `/datacenter/cluster/licensing/licenses/{key}`	Diese Funktion liefert Details zu den auf den Clustern in Ihrem Datacenter installierten Lizenzen. Sie können Ihre Ergebnisse anhand der erforderlichen Kriterien filtern. Informationen wie der Lizenzschlüssel, der Clusterschlüssel, das Ablaufdatum und der Lizenzumfang werden angezeigt. Sie können einen Lizenzschlüssel eingeben, um die Details einer bestimmten Lizenz abzurufen.

GET	`/datacenter/cluster/nodes`
	
	`/datacenter/cluster/nodes/{key}`
		Mit dieser Methode können Sie die Details der Knoten im Datacenter anzeigen. Sie können Informationen über den Cluster, den Systemstatus des Knotens, die Performancekapazität und das High Availability (HA)-Paar des Knotens anzeigen.

GET	`/datacenter/protocols/cifs/shares`
	
	`/datacenter/protocols/cifs/shares/{key}`
		Mit dieser Methode können Sie die Details der CIFS-Freigaben im Datacenter anzeigen. Neben Cluster-, SVM- und Volume-Details werden auch Informationen zur Access Control List (ACL) zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/protocols/nfs/export-policies /datacenter/protocols/nfs/export-policies/{key}	Mit dieser Methode können Sie die Details der Exportrichtlinien für die unterstützten NFS Services anzeigen. Sie können die Exportrichtlinien für einen Cluster oder eine Storage VM abfragen und den Exportrichtlinienschlüssel für die Provisionierung von NFS-Dateifreigaben wiederverwenden. Weitere Informationen zum Zuweisen und Wiederverwenden von Exportrichtlinien für Workloads finden Sie unter “Provisioning CIFS and NFS file shares”.
GET	/datacenter/storage/aggregates /datacenter/storage/aggregates/{key}	Mit dieser Methode können Sie die Sammlung der Aggregate im Datacenter oder ein bestimmtes Aggregat anzeigen, um Workloads darauf zu provisionieren oder sie zu überwachen. Informationen wie Cluster- und Knotendetails, die genutzte Performance-Kapazität, der verfügbare und verwendete Speicherplatz sowie die Storage-Effizienz werden zurückgegeben.
GET	/datacenter/storage/luns /datacenter/storage/luns/{key}	Mit dieser Methode lässt sich die Sammlung von LUNs im gesamten Datacenter anzeigen. Informationen zur LUN, wie Cluster- und SVM-Details, QoS-Richtlinien und Initiatorgruppen, lassen sich anzeigen.
GET	/datacenter/storage/qos/policies /datacenter/storage/qos/policies/{key}	Mit dieser Methode können Sie die Details aller QoS Richtlinien anzeigen, die für die Storage Objekte im Datacenter gelten. Informationen wie die Cluster- und SVM-Details, die Details der festen oder adaptiven Richtlinie sowie die Anzahl der Objekte, für die diese Richtlinie gilt, werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/storage/qtrees /datacenter/storage/qtrees/{key}	Mit dieser Methode können Sie die Qtree-Details im gesamten Datacenter für alle FlexVol Volumes oder FlexGroup Volumes anzeigen. Informationen wie die Cluster- und SVM-Details, das FlexVol Volume und die Exportrichtlinie werden zurückgegeben.
GET	/datacenter/storage/volumes /datacenter/storage/volumes/{key}	Mit dieser Methode lässt sich die Sammlung von Volumes im Datacenter anzeigen. Informationen über die Volumes, z. B. SVM- und Clusterdetails, QoS- und Exportrichtlinien sowie dazu, ob das Volume vom Typ Lesen/Schreiben, Datenschutz oder Lastverteilung ist, werden zurückgegeben. Für FlexVol- und FlexClone-Volumes können Sie die Informationen zu den jeweiligen Aggregaten anzeigen. Für ein FlexGroup-Volume gibt die Abfrage die Liste der zugehörigen Aggregate zurück.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/protocols/san/igroups`
	
	`/datacenter/protocols/san/igroups/{key}`
		Sie können Initiatorgruppen (igroups) zuweisen, die zum Zugriff auf bestimmte LUN-Ziele berechtigt sind. Falls bereits eine Initiatorgruppe vorhanden ist, können Sie diese zuweisen. Alternativ können Sie igroups erstellen und sie den LUNs zuordnen.
		
		Mit diesen Methoden können Sie Initiatorgruppen abfragen, erstellen, löschen bzw. ändern.
		
		Wichtige Punkte:
		
		• `POST:`Beim Erstellen einer Initiatorgruppe können Sie die Storage VM festlegen, auf der Sie den Zugriff zuweisen möchten.
		• `DELETE:` Zum Löschen einer bestimmten Initiatorgruppe muss der Schlüssel der Initiatorgruppe als Eingabeparameter angegeben werden. Wenn einer LUN bereits eine Initiatorgruppe zugewiesen wurde, kann diese Initiatorgruppe nicht gelöscht werden.
		• `PATCH:` Als Eingabeparameter muss der Schlüssel der Initiatorgruppe angegeben werden, um eine bestimmte Initiatorgruppe zu ändern. Außerdem müssen Sie die Eigenschaft eingeben, die aktualisiert werden soll, sowie deren Wert.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
	`/datacenter/svm/svms`
	
	`/datacenter/svm/svms/{key}`
		Mit diesen Methoden können Sie Storage Virtual Machines (storage VMs) anzeigen, erstellen, löschen und ändern.
		
		• `POST`: Sie müssen das Storage VM-Objekt, das Sie erstellen möchten, als Eingabeparameter angeben. Sie können eine benutzerdefinierte Storage VM erstellen und ihr anschließend die erforderlichen Eigenschaften zuweisen.
		• `DELETE`: Zum Löschen einer bestimmten Storage VM müssen Sie den Storage VM Schlüssel angeben.
		• `PATCH:`Sie müssen den Storage VM-Schlüssel angeben, um eine bestimmte Storage VM zu ändern. Außerdem müssen Sie die Eigenschaften, die Sie aktualisieren möchten, zusammen mit ihren Werten eingeben.

Wichtige Punkte:

Wenn in Ihrer Umgebung die SLO-basierte Workload Provisionierung aktiviert ist, muss beim Erstellen der Storage VM sichergestellt sein, dass sie alle Protokolle unterstützt, die für die Provisionierung von LUNs und Dateifreigaben darauf erforderlich sind, z. B. CIFS oder SMB, NFS, FCP und iSCSI. Die Provisionierung Workflows können fehlschlagen, wenn die Storage VM die erforderlichen Services nicht unterstützt. Es wird empfohlen, die Services für die jeweiligen Workload-Typen ebenfalls auf der Storage VM zu aktivieren.

Wenn Sie die SLO-basierte Workload Provisionierung in Ihrer Umgebung aktiviert haben, können Sie die Storage VM, auf der Storage Workloads provisioniert wurden, nicht löschen. Wenn Sie eine Storage VM löschen, auf der ein CIFS- oder SMB-Server konfiguriert wurde, löscht diese API auch den CIFS- oder SMB-Server sowie die lokale Active Directory-Konfiguration. Der Name des CIFS- oder SMB-Servers bleibt jedoch in der Active Directory-Konfiguration bestehen, und Sie müssen ihn manuell vom Active Directory-Server löschen.

APIs für Netzwerkelemente in Ihrem Datacenter

Die folgenden APIs in der Kategorie Datacenter rufen Informationen über die Ports und Netzwerkschnittstellen in Ihrer Umgebung ab, insbesondere über die FC-Ports, FC-Schnittstellen, Ethernet-Ports und IP-Schnittstellen.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/ethernet/ports /datacenter/network/ethernet/ports/{key}	Ruft Informationen zu allen Ethernet-Ports in Ihrer Datacenter-Umgebung ab. Mit einem Portschlüssel als Eingabeparameter können Sie die Informationen dieses spezifischen Ports anzeigen. Abgerufen werden unter anderem Clusterdetails, die Broadcast-Domäne, Portdetails wie Status, Geschwindigkeit und Typ sowie die Information, ob der Port aktiviert ist.
GET	/datacenter/network/fc/interfaces /datacenter/network/fc/interfaces/{key}	Mit dieser Methode können Sie die Details der FC-Schnittstellen in Ihrer Datacenter-Umgebung anzeigen. Mit einem Schnittstellenschlüssel als Eingabeparameter können Sie die Informationen zu dieser spezifischen Schnittstelle anzeigen. Dabei werden Informationen wie Clusterdetails, Details zum Home-Knoten und Details zum Home-Port abgerufen.
GET	/datacenter/network/fc/ports /datacenter/network/fc/ports/{key}	Ruft Informationen zu allen FC-Ports ab, die in den Knoten Ihrer Datacenter-Umgebung verwendet werden. Mit einem Portschlüssel als Eingabeparameter können Sie die Informationen des jeweiligen Ports anzeigen. Abgerufen werden unter anderem Clusterdetails, Portbeschreibung, unterstütztes Protokoll und Portstatus.
GET	/datacenter/network/ip/interfaces /datacenter/network/ip/interfaces/{key}	Mit dieser Methode lassen sich die Details der IP-Schnittstellen in Ihrer Datacenter-Umgebung anzeigen. Mit einem Schnittstellenschlüssel als Eingabeparameter lassen sich die Informationen zu dieser spezifischen Schnittstelle anzeigen. Dabei werden Informationen wie Clusterdetails, IPspace-Details, Home-Node-Details und die Angabe, ob Failover aktiviert ist, abgerufen.

Zugriff auf ONTAP APIs über Proxyzugriff in Active IQ Unified Manager

Die Gateway-APIs bieten Ihnen den Vorteil, die Anmeldeinformationen von Active IQ

Unified Manager zum Ausführen von ONTAP REST APIs und zum Managen von Storage Objekten zu verwenden. Diese APIs sind verfügbar, wenn die API Gateway Funktion in der Unified Manager Web-UI aktiviert ist.

Unified Manager REST APIs unterstützen nur eine begrenzte Anzahl von Aktionen, die auf den Unified Manager Datenquellen, also ONTAP Clustern, ausgeführt werden können. Die anderen Funktionen sind über ONTAP APIs verfügbar. Die Gateway APIs ermöglichen Unified Manager, als Durchleitungsoberfläche für das Tunneln aller API-Anforderungen an die von ihm verwalteten ONTAP Cluster zu dienen, ohne dass eine separate Anmeldung bei jedem einzelnen Datacenter Cluster erforderlich ist. Es dient als zentraler Verwaltungspunkt für die Ausführung der APIs über die von Ihrer Unified Manager Instanz verwalteten ONTAP Cluster. Die API Gateway Funktion ermöglicht Unified Manager, als zentrale Kontrollebene zu dienen, über die mehrere ONTAP Cluster gemanagt werden können, ohne dass eine einzelne Anmeldung bei jedem Cluster erforderlich ist. Die Gateway APIs ermöglichen es, in Unified Manager angemeldet zu bleiben und die ONTAP Cluster durch Ausführen von ONTAP REST API Vorgängen zu managen.

Alle Benutzer können Abfragen mittels der GET-Operation ausführen. Anwendungsadministratoren können alle ONTAP REST-Operationen ausführen.

Das Gateway fungiert als Proxy, um die API-Anfragen zu tunneln, indem es Header und Body der Anfragen im gleichen Format wie in den ONTAP APIs beibehält. Sie können Ihre Unified Manager Anmeldedaten verwenden und die spezifischen Vorgänge ausführen, um auf die ONTAP Cluster zuzugreifen und sie zu managen, ohne Anmeldedaten einzelner Cluster angeben zu müssen. Es übernimmt weiterhin die Cluster-Authentifizierung und das Cluster-Management, leitet die API-Anfragen jedoch so um, dass sie direkt auf dem jeweiligen Cluster ausgeführt werden. Die von den APIs zurückgegebene Antwort entspricht der Antwort der entsprechenden ONTAP REST APIs, die direkt von ONTAP ausgeführt werden.

HTTP-Verb	Pfad (URL)	Beschreibung
`GET`	`/gateways`	Diese GET-Methode ruft die Liste aller von Unified Manager gemanagten Cluster ab, die ONTAP REST-Aufrufe unterstützen. Sie können die Clusterdetails überprüfen und anhand der Cluster-UUID oder der Universal Unique Identifier (UUID) weitere Methoden ausführen. Die Gateway-APIs rufen nur die Cluster ab, die von ONTAP 9.5 oder höher unterstützt und über HTTPS zu Unified Manager hinzugefügt wurden.

HTTP-Verb	Pfad (URL)	Beschreibung

`GET`
 	
`POST`
 	
`DELETE`
 	
`PATCH`
 	
`OPTIONS` (nicht auf Swagger verfügbar)
 	
`HEAD` (nicht auf Swagger verfügbar)
	`/gateways/{uuid}/{path}`
	
	Der Wert für {uuid} muss durch die Cluster UUID ersetzt werden, auf der die REST Operation ausgeführt werden soll. Es ist außerdem sicherzustellen, dass die UUID zu einem von ONTAP 9.5 oder höher unterstützten Cluster gehört und über HTTPS zu Unified Manager hinzugefügt wurde. {path} muss durch die ONTAP REST URL ersetzt werden. Aus der URL muss `/api/` entfernt werden.
		Dies ist eine zentrale Proxy-API, die POST-, DELETE-, PATCH- und GET-Anfragen für alle ONTAP REST-APIs unterstützt. Für keine der APIs gelten Einschränkungen, solange sie von ONTAP unterstützt werden. Die Tunneling- bzw. Proxy-Funktionalität kann nicht deaktiviert werden.
		
		Die `OPTIONS`Methode gibt alle Operationen zurück, die von einer ONTAP REST API unterstützt werden. Wenn eine ONTAP API beispielsweise nur die `GET`Operation unterstützt, liefert die Ausführung der `OPTIONS`Methode über diese Gateway-API `GET`als Antwort. Diese Methode wird von Swagger nicht unterstützt, kann aber mit anderen API-Tools ausgeführt werden.
		
		Die `OPTIONS` Methode bestimmt, ob eine Ressource verfügbar ist. Dieser Vorgang kann verwendet werden, um die Metadaten zu einer Ressource in den HTTP-Antwortheadern anzuzeigen. Diese Methode wird von Swagger nicht unterstützt, kann jedoch mit anderen API-Tools ausgeführt werden.

Grundlagen des API Gateway Tunneling

Die Gateway APIs ermöglichen es, ONTAP Objekte über Unified Manager zu managen. Unified Manager managt die Cluster und Authentifizierungsdetails und leitet die Anfragen an den ONTAP REST Endpunkt weiter. Die Gateway API transformiert die URL und die Hypermedia as the Engine of Application State (HATEOAS) Links im Header und im Antworttext mit der Basis URL des API Gateway. Die Gateway API fungiert als Proxy Basis URL, an die die ONTAP REST URL angehängt wird und über die der erforderliche ONTAP REST Endpunkt ausgeführt wird.

Damit eine ONTAP API über das API Gateway erfolgreich ausgeführt werden kann, muss die API von der Version des ONTAP Clusters unterstützt werden, auf dem sie ausgeführt wird. Die Ausführung einer API, die auf dem ONTAP Cluster nicht unterstützt wird, liefert keine Ergebnisse.

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

Die verwendete ONTAP API lautet: `/storage/volumes`. Die ONTAP API REST URL wird als Wert für den

Pfadparameter angegeben.

> Beim Hinzufügen des Pfads ist sicherzustellen, dass “/” symbol at the beginning of the URL. For the API `/storage/volumes`, add `storage/volumes`. entfernt wurde.

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

Beim Ausführen des `GET` Vorgangs wird folgende URL generiert:
`GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes`

Das `/api` Tag der ONTAP REST URL wird in der angehängten URL entfernt, und das für die gateway API wird beibehalten.

Beispiel für einen cURL-Befehl

```
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 in ONTAP ausführen. Die zurückgegebenen Statuscodes sind die ONTAP REST-Statuscodes.

API-Bereich festlegen

Alle APIs haben einen Kontext, der innerhalb des Clusters festgelegt ist. APIs, die auf Basis von Storage VMs arbeiten, haben ebenfalls den Cluster als Geltungsbereich, das heißt, die API-Operationen werden auf einer bestimmten Storage VM innerhalb eines verwalteten Clusters ausgeführt. Beim Ausführen der `/gateways/{uuid}/{path}` API ist darauf zu achten, dass die Cluster UUID (Unified Manager datasource UUID) für den Cluster eingegeben wird, auf dem die Operation ausgeführt wird. Zum Festlegen des Kontexts auf eine bestimmte Storage VM innerhalb dieses Clusters ist der Storage VM Schlüssel als Parameter X-Dot-SVM-UUID oder der Storage VM Name als Parameter X-Dot-SVM-Name einzugeben. Der Parameter wird als Filter im String-Header hinzugefügt, und die Operation wird innerhalb des Geltungsbereichs dieser Storage VM in diesem Cluster ausgeführt.

Beispiel für einen cURL-Befehl

```
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"

Administrative Aufgaben mithilfe von APIs in Active IQ Unified Manager ausführen

Sie können die APIs der Kategorie `administration` verwenden, um

Sicherungseinstellungen zu ändern, die Informationen zur Sicherungsdatei und Clusterzertifikate zu überprüfen und ONTAP Cluster auch als Active IQ Unified Manager Datenquellen zu managen.

Sie benötigen die Rolle Application Administrator, um diese Vorgänge auszuführen. Alternativ können Sie die Web-Benutzeroberfläche von Unified Manager verwenden, um diese Einstellungen zu konfigurieren.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`PATCH`
	`/admin/backup-settings`
	
	`/admin/backup-settings`
		Mit der `GET`Methode können Sie die Einstellungen des in Unified Manager standardmäßig konfigurierten Sicherungszeitplans anzeigen. Sie können Folgendes überprüfen:
		• Ob der Zeitplan aktiviert oder deaktiviert ist
		• Häufigkeit der geplanten Datensicherung (täglich oder wöchentlich)
		• Zeitpunkt der Datensicherung
		• Maximale Anzahl der Backup-Dateien, die in der Applikation aufbewahrt werden sollten
		
		Die Uhrzeit der Datensicherung wird in der Zeitzone des Servers angegeben.
		
		Die Einstellungen für die Datenbanksicherung sind in Unified Manager standardmäßig verfügbar, und es lässt sich kein Sicherungszeitplan erstellen. Die Standardeinstellungen lassen sich jedoch mit der `PATCH`Methode ändern.

`GET`	`/admin/backup-file-info`	Bei jeder Änderung des Sicherungsplans für Unified Manager wird eine Sicherungsdumpdatei generiert. Mit dieser Methode können Sie überprüfen, ob die Sicherungsdatei gemäß den geänderten Sicherungseinstellungen generiert wurde und ob die Informationen in der Datei mit den geänderten Einstellungen übereinstimmen.

HTTP-Verb	Pfad	Beschreibung
GET	/admin/datasource-certificate	Mit dieser Methode können Sie das Datenquellenzertifikat (Clusterzertifikat) aus dem Truststore anzeigen. Die Validierung des Zertifikats ist erforderlich, bevor ein ONTAP Cluster als Unified Manager Datenquelle hinzugefügt wird.
GET POST PATCH DELETE	/admin/datasources/clusters /admin/datasources/clusters/{key}	Mit der GET Methode können Sie die Details der von Unified Manager gemanagten Datenquellen (ONTAP Cluster) abrufen. Sie können Unified Manager auch einen neuen Cluster als Datenquelle hinzufügen. Zum Hinzufügen eines Clusters benötigen Sie dessen Hostnamen, Benutzernamen und Passwort. Zum Ändern und Löschen eines Clusters, das von Unified Manager als Datenquelle gemanagt wird, dient der ONTAP Clusterschlüssel.

Benutzerverwaltung in Active IQ Unified Manager mithilfe von APIs

Mit den APIs in der security Kategorie können Sie den Benutzerzugriff auf ausgewählte Clusterobjekte in Active IQ Unified Manager 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 diese die Storage Objekte managen oder die Daten in Unified Manager anzeigen.

Sie benötigen die Rolle Application Administrator, um diese Vorgänge auszuführen. Alternativ können Sie die Web-Benutzeroberfläche von Unified Manager verwenden, um diese Einstellungen zu konfigurieren.

Die APIs unter der security Kategorie verwenden den Parameter users, also den Benutzernamen, und nicht den Parameter key als eindeutigen Bezeichner für die Benutzerentität.

HTTP-Verb	Pfad	Beschreibung

`GET`
 	
`POST`
	`/security/users`
	
	`/security/users`
		Mit diesen Methoden können Sie Details zu Benutzern abrufen oder neue Benutzer zu Unified Manager hinzufügen.
		
		Sie können Benutzern basierend auf ihren Benutzertypen spezifische Rollen zuweisen. Beim Hinzufügen von Benutzern müssen Sie Passwörter für den lokalen Benutzer, den Wartungsbenutzer und den Datenbankbenutzer angeben.

`GET`
 	
`PATCH`
 	
`DELETE`
	`/security/users/{name}`	Mit der GET-Methode lassen sich alle Details eines Benutzers abrufen, z. B. Name, E-Mail-Adresse, Rolle und Berechtigungstyp. Mit der PATCH-Methode lassen sich die Details aktualisieren. Mit der DELETE-Methode lässt sich der Benutzer entfernen.

Leistungsmetriken mithilfe von APIs in Active IQ Unified Manager anzeigen

Active IQ Unified Manager stellt Ihnen eine Reihe von APIs unter der `/datacenter` Kategorie zur Verfügung, mit denen Sie die Performance-Daten Ihrer Cluster und Storage Objekte in einem Datacenter anzeigen können. Diese APIs rufen die Performance-Daten der verschiedenen Storage Objekte wie Cluster, Nodes, LUNs, Volumes, Aggregate, Storage VMs, FC-Schnittstellen, FC-Ports, Ethernet-Ports und IP-Schnittstellen ab.

Die `/metrics` und `/analytics` APIs bieten unterschiedliche Ansichten der Performance-Metriken, mit denen Sie für die folgenden Storage Objekte in Ihrem Datacenter verschiedene Detailebenen aufschlüsseln können:

- Cluster
- Knoten
- Storage VMs
- Aggregate
- Volumes
- LUNs
- FC Schnittstellen
- FC-Ports
- Ethernet-Ports
- IP Schnittstellen

Die folgende Tabelle vergleicht die `/metrics` und `/analytics` APIs hinsichtlich der Details der abgerufenen Performance-Daten.

Kennzahlen	Analysen
Performancedetails für ein einzelnes Objekt. Beispielsweise erfordert die `/datacenter/cluster/clusters/{key}/metrics` API die Eingabe des Cluster-Schlüssels als Pfadparameter, um die Metriken für diesen spezifischen Cluster abzurufen.	Performance-Details für mehrere Objekte desselben Typs in einem Datacenter. Beispielsweise ruft die `/datacenter/cluster/clusters/analytics` API die kollektiven Metriken aller Cluster in einem Datacenter ab.
Performance-Kennzahlenbeispiel für ein Storage-Objekt basierend auf dem Zeitintervallparameter für den Abruf.	Der aggregierte Gesamtwert der Performance für einen bestimmten Typ von Storageobjekt über einen bestimmten Zeitraum (mehr als 72 Stunden).
Der Abruf umfasst grundlegende Details des Objekts, beispielsweise zu einem Knoten oder Cluster.	Es werden keine spezifischen Details abgerufen.
Akkumulierte Zählerwerte wie Minimum, Maximum, 95. Perzentil und die durchschnittlichen Performance Werte über einen Zeitraum werden für ein einzelnes Objekt abgerufen, z. B. Lese-, Schreib-, Gesamt- und andere Zähler.	Für alle Objekte desselben Typs wird ein einzelner aggregierter Wert angezeigt.

Kennzahlen	Analysen
Der Zeitbereich und die Abtastdaten basieren auf dem folgenden Zeitplan: der Zeitbereich für die Daten. Beispiele sind 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m. Bei einem Bereich von mehr als 3 Tagen (72 hr) werden 1-Stunden-Abtastwerte verwendet, andernfalls 5-Minuten-Abtastwerte. Der Zeitraum für jeden Zeitbereich ist wie folgt: • 1h: Messwerte der letzten Stunde, in 5-Minuten-Intervallen erfasst. • 12h: Messwerte der letzten 12 Stunden, im Abstand von 5 Minuten erfasst. • 1d: Messwerte des letzten Tages, im Abstand von 5 Minuten erfasst. • 2d: Metriken der letzten 2 Tage, im 5-Minuten-Intervall erfasst. • 3d: Metriken der letzten 3 Tage, erfasst in einem 5-Minuten-Intervall. • 15d: Kennzahlen der letzten 15 Tage, erfasst über 1 Stunde. • 1w: Kennzahlen der letzten Woche, erfasst über einen Zeitraum von einer Stunde. • 1m: Kennzahlen des letzten Monats, über 1 Stunde erfasst. • 2m: Kennzahlen der letzten 2 Monate, erfasst über 1 Stunde. • 3m: Metriken der letzten 3 Monate, erfasst über 1 Stunde. • 6m: Kennzahlen der letzten 6 Monate, im Abstand von 1 Stunde erfasst. Verfügbare Werte: 1h, 12h, 1d, 2d, 3d, 15d, 1w, 1m, 2m, 3m, 6m Standardwert: 1h	Über 72 Stunden. Die Dauer, über die diese Stichprobe berechnet wird, wird im ISO-8601-Standardformat dargestellt.

Beispielausgabe für Metrik-APIs

Beispielsweise ruft die `/datacenter/cluster/nodes/{key}/metrics` API unter anderem die folgenden Details für einen Node ab:

Der Wert 95. Perzentil in der Zusammenfassung gibt an, dass 95 % der für den Zeitraum gesammelten Proben einen Zählerwert aufweisen, der kleiner ist als der als 95. Perzentil angegebene Wert.

```
{
```

```
      "iops": {
        "local": {
          "other": 100.53,
          "read": 100.53,
          "total": 100.53,
          "write": 100.53
        },
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "latency": {
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "performance_capacity": {
        "available_iops_percent": 0,
        "free_percent": 0,
        "system_workload_percent": 0,
        "used_percent": 0,
        "user_workload_percent": 0
      },
      "throughput": {
        "other": 100.53,
        "read": 100.53,
        "total": 100.53,
        "write": 100.53
      },
      "timestamp": "2018-01-01T12:00:00-04:00",
      "utilization_percent": 0
    }
  ],
  "start_time": "2018-01-01T12:00:00-04:00",
  "summary": {
    "iops": {
      "local_iops": {
        "other": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "read": {
```

```
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "total": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        },
        "write": {
          "95th_percentile": 28,
          "avg": 28,
          "max": 28,
          "min": 5
        }
      },
```

Beispielausgabe für Analyse-APIs

Beispielsweise ruft die `/datacenter/cluster/nodes/analytics` API unter anderem die folgenden Werte für alle Knoten ab:

```
{     "iops": 1.7471,
      "latency": 60.0933,
      "throughput": 5548.4678,
      "utilization_percent": 4.8569,
      "period": 72,
      "performance_capacity": {
        "used_percent": 5.475,
        "available_iops_percent": 168350
      },
      "node": {
        "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a",
        "uuid": "95f94e8d-8b4e-11e9-8974-00a098e0219a",
        "name": "ocum-infinity-01",
        "_links": {
          "self": {
            "href": "/api/datacenter/cluster/nodes/37387241-8b57-11e9-8974-
00a098e0219a:type=cluster_node,uuid=95f94e8d-8b4e-11e9-8974-00a098e0219a"
          }
        }
      },
      "cluster": {
```

```
        "key": "37387241-8b57-11e9-8974-
00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a",
        "uuid": "37387241-8b57-11e9-8974-00a098e0219a",
        "name": "ocum-infinity",
        "_links": {
          "self": {
            "href": "/api/datacenter/cluster/clusters/37387241-8b57-11e9-
8974-00a098e0219a:type=cluster,uuid=37387241-8b57-11e9-8974-00a098e0219a"
          },
      "_links": {
        "self": {
          "href": "/api/datacenter/cluster/nodes/analytics"
        }
      }
    },
```

Liste der verfügbaren APIs

Die folgende Tabelle beschreibt die `/metrics` und `/analytics` APIs im Detail.

> Die von diesen APIs zurückgegebenen IOPS- und Performance-Metriken sind Double-Werte, zum Beispiel `100.53`. Das Filtern dieser Gleitkommawerte anhand der Pipe-Zeichen (|) und Platzhalterzeichen (*) wird nicht unterstützt.

HTTP-Verb	Pfad	Beschreibung
`GET`	`/datacenter/cluster/clusters/{key}/metrics`	Ruft Performance-Daten (Stichproben und Zusammenfassung) für einen Cluster ab, der durch den Eingabeparameter des Cluster-Schlüssels angegeben wird. Informationen wie der Cluster-Schlüssel und die UUID, der Zeitraum, IOPS, der Durchsatz und die Anzahl der Stichproben werden zurückgegeben.
`GET`	`/datacenter/cluster/clusters/analytics`	Ruft Performance-Metriken auf hoher Ebene für alle Cluster in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung
GET	`/datacenter/cluster/nodes/{key}/metrics`	Performance-Daten (Stichprobe und Zusammenfassung) für einen Knoten, der durch den Eingabeparameter des Knotenschlüssels angegeben ist, werden abgerufen. Informationen wie die Knoten-UUID, der Zeitraum, eine Zusammenfassung der IOPS, des Durchsatzes, der Latenz und der Performance, die Anzahl der erfassten Stichproben und die prozentuale Auslastung werden zurückgegeben.
GET	`/datacenter/cluster/nodes/analytics`	Es werden Performance-Metriken auf hoher Ebene für alle Knoten in einem Datacenter abgerufen. Die Ergebnisse lassen sich anhand der gewünschten Kriterien filtern. Informationen wie Knoten- und Clusterschlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.
GET	`/datacenter/storage/aggregates/{key}/metrics`	Ruft Performance-Daten (Stichproben und Zusammenfassung) für ein durch den Eingabeparameter des Aggregatschlüssels angegebenes Aggregat ab. Informationen wie der Zeitraum, eine Zusammenfassung der IOPS, Latenz, Durchsatz und Performance-Kapazität, die Anzahl der für jeden Zähler erfassten Stichproben und der Prozentsatz der Auslastung werden zurückgegeben.
GET	`/datacenter/storage/aggregates/analytics`	Ruft übergeordnete Performance-Metriken für alle Aggregate in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Informationen wie Aggregat- und Clusterschlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.

HTTP-Verb	Pfad	Beschreibung

GET	`/datacenter/storage/luns/{key}/metrics`
	
	`/datacenter/storage/volumes/{key}/metrics`
		Es werden Performance-Daten (Messwerte und Zusammenfassung) für eine LUN oder eine Dateifreigabe (Volume) abgerufen, die durch den Eingabeparameter des LUN- oder Volume-Schlüssels angegeben ist. Informationen wie die Zusammenfassung der minimalen, maximalen und durchschnittlichen Werte für Lese-, Schreib- und Gesamt-IOPS, Latenz und Durchsatz sowie die Anzahl der für jeden Zähler erfassten Messwerte werden zurückgegeben.

GET	`/datacenter/storage/luns/analytics`
	
	`/datacenter/storage/volumes/analytics`
		Ruft übergeordnete Performance-Metriken für alle LUNs oder Volumes in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Informationen wie Storage VM- und Cluster-Schlüssel sowie Werte wie aggregierte IOPS, Durchsatz und der Erfassungszeitraum (in Stunden) werden zurückgegeben.

GET	`/datacenter/svm/svms/{key}/metrics`	Ruft Performance-Daten (Stichprobe und Zusammenfassung) für eine Storage VM ab, die durch den Eingabeparameter des Storage VM-Schlüssels angegeben wird. Eine Zusammenfassung der IOPS basierend auf jedem unterstützten Protokoll, wie z. B. `nvmf, fcp, iscsi,` und `nfs`, des Durchsatzes, der Latenz und der Anzahl der erfassten Stichproben wird zurückgegeben.
GET	`/datacenter/svm/svms/analytics`	Ruft allgemeine Performance-Metriken für alle Storage VMs in einem Datacenter ab. Sie können Ihre Ergebnisse anhand der gewünschten Kriterien filtern. Die Rückgabe umfasst Informationen wie die Storage VM UUID, aggregierte IOPS, Latenz, Durchsatz und den Erfassungszeitraum (in Stunden).

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/ethernet/ports/{key}/metrics	Ruft die Performance-Metriken für einen bestimmten Ethernet-Port ab, der durch den Eingabeparameter des Portschlüssels angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben ist, gibt die API die akkumulierten Zähler zurück, etwa minimale, maximale und durchschnittliche Performance-Werte für diesen Zeitraum.
GET	/datacenter/network/ethernet/ports/analytics	Abgerufen werden die wichtigsten Performance Kennzahlen aller Ethernet-Ports in Ihrer Datacenter-Umgebung. Informationen wie Cluster- und Node-Schlüssel und UUID, Durchsatz, Erfassungszeitraum und Auslastungsgrad der Ports werden zurückgegeben. Die Ergebnisse können anhand der verfügbaren Parameter gefiltert werden, z. B. nach Portschlüssel, Auslastungsgrad, Cluster- und Node-Name sowie UUID.
GET	/datacenter/network/fc/interfaces/{key}/metrics	Ruft die Performance-Kennzahlen für eine bestimmte Netzwerk-FC-Schnittstelle ab, die durch den Eingabeparameter des Schnittstellenschlüssels angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben wird, gibt die API die akkumulierten Zähler zurück, z. B. minimale, maximale und durchschnittliche Performance-Werte über den Zeitraum.
GET	/datacenter/network/fc/interfaces/analytics	Ruft die allgemeinen Performance Kennzahlen für alle Ethernet-Ports in Ihrer Datacenter-Umgebung ab. Informationen wie Cluster- und FC-Schnittstellenschlüssel und -UUID, Durchsatz, IOPS, Latenz und Storage VM werden zurückgegeben. Die Ergebnisse können anhand der verfügbaren Parameter gefiltert werden, z. B. nach Cluster- und FC-Schnittstellenname und -UUID, Storage VM, Durchsatz usw.

HTTP-Verb	Pfad	Beschreibung
GET	/datacenter/network/fc/ports/{key}/metrics	Ruft die Performance Kennzahlen für einen bestimmten FC-Port ab, der durch den Eingabeparameter des Port-Key angegeben wird. Wenn ein Intervall (Zeitbereich) aus dem unterstützten Bereich angegeben wird, gibt die API die akkumulierten Zähler zurück, z. B. minimale, maximale und durchschnittliche Performance Werte über den Zeitraum.
GET	/datacenter/network/fc/ports/analytics	Es werden die wichtigsten Performance-Kennzahlen für alle FC-Ports in Ihrer Datacenter-Umgebung abgerufen. Informationen wie Cluster- und Node-Schlüssel und -UUID, Durchsatz, Erfassungszeitraum und Auslastungsgrad der Ports werden zurückgegeben. Die Ergebnisse können anhand der verfügbaren Parameter gefiltert werden, z. B. nach Port-Schlüssel, Auslastungsgrad, Cluster- und Node-Name und -UUID usw.
GET	/datacenter/network/ip/interfaces/{key}/metrics	Ruft die Performance-Kennzahlen einer Netzwerk-IP-Schnittstelle gemäß dem Eingabeparameter des Schnittstellelschlüssels ab. Bei Angabe eines Intervalls (Zeitbereichs) aus dem unterstützten Bereich liefert die API Informationen wie die Anzahl der Messwerte, akkumulierte Zählerstände, den Durchsatz sowie die Anzahl der empfangenen und gesendeten Pakete.
GET	/datacenter/network/ip/interfaces/analytics	Die wichtigsten Performance-Kennzahlen aller Netzwerk-IP-Schnittstellen in Ihrer Datacenter-Umgebung werden abgerufen. Informationen wie der Cluster- und IP-Schnittstellen-Schlüssel und die UUID sowie Durchsatz, IOPS und Latenz werden zurückgegeben. Das Ergebnis lässt sich anhand der verfügbaren Parameter filtern, z. B. nach Cluster- und IP-Schnittstellenname und UUID, IOPS, Latenz, Durchsatz usw.

Aufträge und Systemdetails können über APIs in Active IQ Unified Manager angezeigt werden

Sie können die `jobs` API in der `management-server` Kategorie verwenden, um die Ausführungsdetails asynchroner Operationen anzuzeigen. Die `system` API in der `management-server` Kategorie ermöglicht Ihnen die Anzeige der Instanzdetails in Ihrer Active IQ Unified Manager Umgebung.

Jobs anzeigen

In Active IQ Unified Manager werden Vorgänge wie das Hinzufügen und Ändern von Ressourcen über synchrone und asynchrone API-Aufrufe ausgeführt. Aufrufe, die zur asynchronen Ausführung geplant sind, lassen sich über ein für diesen Aufruf erstelltes Job-Objekt nachverfolgen. Jedes Job-Objekt besitzt einen eindeutigen Schlüssel zur Identifizierung. Jedes Job-Objekt gibt die Job-Objekt-URI zurück, über die auf den Job zugegriffen und sein Fortschritt verfolgt werden kann. Mit dieser API lassen sich die Details jeder Ausführung abrufen.

Mithilfe dieser API können Sie alle Jobobjekte Ihres Datacenter einschließlich historischer Daten abfragen. Standardmäßig werden bei einer Abfrage aller Jobs die Details der letzten 20 Jobs angezeigt, die über die Web-Oberfläche und die API-Schnittstelle ausgelöst wurden. Die integrierten Filter können zum Anzeigen bestimmter Jobs verwendet werden. Sie können auch den Job key verwenden, um die Details eines bestimmten Jobs abzufragen und die nächsten Operationen auf den Ressourcen auszuführen.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/jobs`	Gibt die Job-Details aller Jobs zurück. Ohne Sortierung wird das zuletzt übermittelte Job-Objekt oben angezeigt.
Management-Server	GET	`/management-server/jobs/{key}` Zum Anzeigen der spezifischen Details dieses Jobs den Job-Schlüssel des Job-Objekts eingeben.	Gibt die Details des spezifischen Job-Objekts zurück.

Systemdetails anzeigen

Mithilfe der `/management-server/system` API können Sie die instanzspezifischen Details Ihrer Unified Manager Umgebung abfragen. Die API liefert Informationen über das Produkt und die Services, wie z. B. die auf Ihrem System installierte Version von Unified Manager, die UUID, den Herstellernamen, das Host-Betriebssystem sowie Namen, Beschreibung und Status der auf der Unified Manager Instanz ausgeführten Services.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/system`	Für die Ausführung dieser API sind keine Eingabeparameter erforderlich. Standardmäßig gibt das System die Systemdetails der aktuellen Unified Manager Instanz zurück.

Verwaltung von Ereignissen und Warnmeldungen mithilfe von APIs in Active IQ Unified Manager

Die APIs `events`, `alerts` und `scripts` in der Kategorie `management-server` ermöglichen Ihnen, die Ereignisse, Warnungen und die mit den Warnungen verbundenen Skripte in Ihrer Active IQ Unified Manager Umgebung zu managen.

Ereignisse anzeigen und ändern

Unified Manager empfängt die Ereignisse, die auf ONTAP für die von Unified Manager überwachten und verwalteten Cluster generiert werden. Mithilfe dieser APIs können Sie die für Ihre Cluster generierten Ereignisse anzeigen, beheben und aktualisieren.

Durch Ausführen der `GET`Methode für die `/management-server/events`API lassen sich die Ereignisse in Ihrem Datacenter einschließlich historischer Daten abfragen. Mit den integrierten Filtern wie Name, Impact-Level, Impact-Bereich, Schweregrad, Status, Ressourcenname und Ressourcentyp lassen sich bestimmte Ereignisse anzeigen. Die Parameter für Ressourcentyp und Bereich geben Informationen über das Storage Objekt zurück, auf dem das Ereignis aufgetreten ist, und der Impact-Bereich gibt Informationen über das Problem zurück, für das das Ereignis ausgelöst wird, z. B. Verfügbarkeit, Kapazität, Konfiguration, Sicherheit, Schutz und Performance.

Durch Ausführen des PATCH-Vorgangs für diese API können Sie den Workflow zur Behebung des Ereignisses aktivieren. Sie können ein Ereignis sich selbst oder einem anderen Benutzer zuweisen und den Empfang des Ereignisses bestätigen. Nachdem Sie die Schritte auf den Ressourcen zur Behebung des Problems durchgeführt haben, das das Ereignis ausgelöst hat, können Sie diese API verwenden, um das Ereignis als gelöst zu markieren.

Weitere Informationen zu Ereignissen finden Sie unter "Informationen zu Active IQ Plattformereignissen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/events` `/management-server/events/{key}`	Wenn Sie die Methode „Get ALL“ ausführen, enthält der Antworttext die Ereignisdetails aller Ereignisse in Ihrem Datacenter. Wenn Sie die Ereignisdetails anhand eines bestimmten Schlüssels abrufen, können Sie die Details eines bestimmten Ereignisses anzeigen und die nächsten Operationen für die Ressourcen ausführen. Der Antworttext enthält die Details dieses Ereignisses.
Management-Server	PATCH	`management-server/events/{key}`	Mit dieser API lässt sich ein Ereignis zuweisen oder der Status in „Bestätigt“ oder „Abgeschlossen“ ändern. Diese Methode kann auch verwendet werden, um das Ereignis Ihnen selbst oder einem anderen Benutzer zuzuweisen. Es handelt sich um einen synchronen Vorgang.

Benachrichtigungen verwalten

Ereignisse werden automatisch und kontinuierlich generiert. Unified Manager generiert eine Warnung nur dann, wenn ein Ereignis bestimmte Filterkriterien erfüllt. Sie können die Ereignisse auswählen, für die Warnungen generiert werden sollen. Mithilfe der `/management-server/alerts` API lassen sich Warnungen so konfigurieren, dass automatisch Benachrichtigungen gesendet werden, wenn bestimmte Ereignisse oder Ereignisse bestimmter Schweregrade auftreten.

Weitere Informationen zu Warnmeldungen finden Sie unter "Informationen zu Benachrichtigungen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/alerts` `/management-server/alerts/{key}`	Sie können mithilfe des Warnungsschlüssels alle vorhandenen Warnmeldungen in Ihrer Umgebung oder eine bestimmte Warnmeldung abfragen. Sie können Informationen zu den in Ihrer Umgebung generierten Warnmeldungen anzeigen, z. B. die Beschreibung der Warnmeldung, die Aktion, die E-Mail-Adresse, an die die Benachrichtigung gesendet wird, sowie Ereignis und Schweregrad.
Management-Server	POST	`/management-server/alerts`	Mit dieser Methode können Sie Warnungen für bestimmte Ereignisse hinzufügen. Sie müssen den Warnungsnamen, die physische oder logische Ressource bzw. das Ereignis, für das die Warnung gilt, den Aktivierungsstatus der Warnung und die Verwendung von SNMP-Traps angeben. Optional können Sie weitere Details hinzufügen, für die die Warnung ausgelöst werden soll, z. B. die Aktion, die E-Mail-Adresse für Benachrichtigungen, die Skriptdetails (falls Sie ein Warnungsskript verwenden) usw.

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	PATCH und DELETE	`management-server/events/{key}`	Mithilfe dieser Methoden können Sie bestimmte Benachrichtigungen bearbeiten und löschen. Sie können verschiedene Attribute ändern, z. B. Beschreibung, Name sowie die Aktivierung und Deaktivierung der Benachrichtigung. Sie können eine Benachrichtigung löschen, sobald sie nicht mehr benötigt wird.

Beachten Sie bei der Auswahl einer Ressource zum Hinzufügen einer Warnung, dass die Auswahl eines Clusters als Ressource nicht automatisch die Storage Objekte innerhalb dieses Clusters auswählt. Wenn Sie beispielsweise eine Warnung für alle kritischen Ereignisse aller Cluster erstellen, erhalten Sie nur Warnungen für kritische Clusterereignisse. Sie erhalten keine Warnungen für kritische Ereignisse auf Knoten, Aggregaten usw.

Skripte managen

Mithilfe der `/management-server/scripts`API können Sie eine Warnung mit einem Skript verknüpfen, das bei Auslösung der Warnung ausgeführt wird. Skripte ermöglichen die automatische Änderung oder Aktualisierung mehrerer Storage Objekte in Unified Manager. Das Skript ist einer Warnung zugeordnet. Wenn ein Ereignis eine Warnung auslöst, wird das Skript ausgeführt. Sie können benutzerdefinierte Skripte hochladen und ihre Ausführung testen, wenn eine Warnung generiert wird. Sie können eine Warnung mit Ihrem Skript verknüpfen, sodass das Skript ausgeführt wird, wenn in Unified Manager für ein Ereignis eine Warnung ausgelöst wird.

Weitere Informationen zu Skripten finden Sie unter "Skripte managen".

Kategorie	HTTP-Verb	Pfad	Beschreibung
Management-Server	GET	`/management-server/scripts`	Mit dieser API lassen sich alle vorhandenen Skripte in Ihrer Umgebung abfragen. Mit den Standardfilter- und Sortierfunktionen lassen sich nur bestimmte Skripte anzeigen.
Management-Server	POST	`/management-server/scripts`	Mit dieser API kann eine Beschreibung für das Skript hinzugefügt und die mit einer Warnung verknüpfte Skriptdatei hochgeladen werden.

Arbeitslasten verwalten

Speicherworkloads mithilfe von APIs in Active IQ Unified Manager anzeigen

Die hier aufgeführten APIs ermöglichen die Anzeige einer konsolidierten Liste von Storage Workloads für alle ONTAP Cluster in Ihrem Datacenter. Die APIs bieten außerdem eine Übersicht über die Anzahl der in Ihrer Active IQ Unified Manager Umgebung provisionierten Storage Workloads sowie über deren Kapazitäts- und Performance-Statistiken (IOPS).

Storage Workloads anzeigen

Sie können die folgende Methode verwenden, um alle Storage Workloads in allen Clustern in Ihrem Datacenter anzuzeigen. Informationen zum Filtern der Antwort anhand bestimmter Spalten finden Sie in der API-Referenzdokumentation Ihrer Unified Manager Instanz.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/workloads`

Zusammenfassung der Storage Workloads anzeigen

Mit der folgenden Methode können die genutzte Kapazität, die verfügbare Kapazität, die genutzten IOPS, die verfügbaren IOPS sowie die Anzahl der von jedem Performance Service Level gemanagten Storage Workloads bewertet werden. Die angezeigten Storage Workloads können sich auf beliebige LUNs, NFS-Dateifreigaben oder CIFS-Freigaben beziehen. Die API bietet eine Übersicht über die Storage Workloads, eine Übersicht über die vom Unified Manager provisionierten Storage Workloads, eine Datacenter Übersicht sowie eine Übersicht über den gesamten, genutzten und verfügbaren Speicherplatz und die IOPS im Datacenter in Bezug auf die zugewiesenen Performance Service Levels. Die als Antwort auf diese API empfangenen Informationen werden zum Ausfüllen des Dashboards in der Unified Manager Benutzeroberfläche verwendet.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/workloads-summary`

Verwaltung von Zugriffsendpunkten mithilfe von APIs in Active IQ Unified Manager

Sie müssen Zugriffsendpunkte oder logische Schnittstellen (LIFs) erstellen, die für die Provisionierung von Storage Virtual Machines (SVMs), LUNs und Dateifreigaben erforderlich sind. In Ihrer Active IQ Unified Manager Umgebung können Sie die Zugriffsendpunkte für die SVMs, LUNs oder Dateifreigaben anzeigen, erstellen, ändern und löschen.

Zugriffsendpunkte anzeigen

Eine Liste der Zugriffs-Endpunkte in Ihrer Unified Manager Umgebung kann mit der folgenden Methode angezeigt werden. Zum Abfragen einer Liste von Zugriffs-Endpunkten einer bestimmten SVM, LUN oder Dateifreigabe ist die Eingabe der eindeutigen Kennung für die SVM, LUN oder Dateifreigabe erforderlich. Außerdem kann der eindeutige Schlüssel des Zugriffs-Endpunkts eingegeben werden, um die Details des jeweiligen Zugriffs-Endpunkts abzurufen.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/access-endpoints`
		
		`/storage-provider/access-endpoints/{key}`

Zugriffsendpunkte hinzufügen

Sie können benutzerdefinierte Zugriffsendpunkte erstellen und ihnen die erforderlichen Eigenschaften zuweisen. Als Eingabeparameter sind die Details des Zugriffsendpunkts anzugeben, den Sie erstellen möchten. Für die Erstellung eines Zugriffsendpunkts auf jedem Node können diese API, der System Manager oder die ONTAP CLI verwendet werden. Sowohl IPv4- als auch IPv6-Adressen werden für die Erstellung von Zugriffsendpunkten unterstützt.

> Für die erfolgreiche Provisionierung von LUNs und Dateifreigaben müssen Sie Ihre SVM mit einer Mindestanzahl an Zugriffspunkten pro Knoten konfigurieren. Sie sollten Ihre SVM mit mindestens zwei Zugriffspunkten pro Knoten konfigurieren, von denen einer das CIFS- und/oder NFS-Protokoll und der andere das iSCSI- oder FCP-Protokoll unterstützt.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/access-endpoints`

Zugriffs-Endpunkte löschen

Ein bestimmter Zugriffsendpunkt kann mit der folgenden Methode gelöscht werden. Zum Löschen eines bestimmten Zugriffsendpunkts muss der Schlüssel des Zugriffsendpunkts als Eingabeparameter angegeben werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/access-endpoints/{key}`

Zugriffsendpunkte ändern

Sie können einen Zugriffsendpunkt ändern und seine Eigenschaften aktualisieren, indem Sie die folgende Methode verwenden. Sie müssen den Schlüssel des Zugriffs-Endpunkts angeben, um einen bestimmten Zugriffsendpunkt zu ändern. Außerdem müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert eingeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/access-endpoints/{key}`

Verwalten von Active Directory Zuordnungen mithilfe von APIs in Active IQ Unified Manager

Mithilfe der hier aufgeführten APIs können Sie die Active Directory-Zuordnungen auf den SVMs managen, die für die Provisionierung von CIFS-Freigaben auf den SVMs

erforderlich sind. Active Directory-Zuordnungen müssen für die Zuordnung der SVMs mit ONTAP konfiguriert werden.

Anzeigen von Active Directory-Zuordnungen

Die Konfigurationsdetails der Active Directory-Zuordnungen für eine SVM lassen sich mit der folgenden Methode anzeigen. Zum Anzeigen der Active Directory-Zuordnungen auf einer SVM ist die Eingabe des SVM-Schlüssels erforderlich. Zum Abfragen der Details einer bestimmten Zuordnung ist die Eingabe des Zuordnungsschlüssels erforderlich.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/active-directories-mappings`
		
		`/storage-provider/active-directories-mappings/{key}`

Hinzufügen der Active Directory Zuordnung

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

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/active-directories-mappings`

Dateifreigaben können mithilfe von APIs in Active IQ Unified Manager verwaltet werden

Mit der `/storage-provider/file-shares`API können Sie die CIFS- und NFS-Dateifreigabe-Volumes in Ihrer Datacenter-Umgebung anzeigen, hinzufügen, ändern und löschen.

Vor der Provisionierung der Dateifreigabevolumes ist sicherzustellen, dass die SVM erstellt und mit den unterstützten Protokollen provisioniert wurde. Wenn bei der Provisionierung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zugewiesen werden, sollten die PSLs bzw. SEPs vor dem Erstellen der Dateifreigaben erstellt werden.

Dateifreigaben anzeigen

Mit der folgenden Methode lassen sich die in Ihrer Unified Manager Umgebung verfügbaren Dateifreigabe-Volumes anzeigen. Wenn Sie einen ONTAP Cluster als Datenquelle in Active IQ Unified Manager hinzugefügt haben, werden die Storage-Workloads dieser Cluster Ihrer Unified Manager Instanz automatisch hinzugefügt. Diese API ruft die Dateifreigaben ab, die Ihrer Unified Manager Instanz automatisch und manuell hinzugefügt wurden. Die Details einer bestimmten Dateifreigabe lassen sich anzeigen, indem diese API mit dem Dateifreigabeschlüssel ausgeführt wird.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/file-shares`
		
		`/storage-provider/file-shares/{key}`

Dateifreigaben hinzufügen

Die folgende Methode ermöglicht das Hinzufügen von CIFS- und NFS-Dateifreigaben in Ihrer SVM. Als Eingabeparameter werden die Details der Dateifreigabe benötigt, die erstellt werden soll. Diese API kann nicht zum Hinzufügen von FlexGroup Volumes verwendet werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/file-shares`

> Je nachdem, ob die Parameter der Zugriffssteuerungsliste (ACL) oder die Parameter der Exportrichtlinie angegeben werden, werden CIFS-Freigaben oder NFS-Dateifreigaben erstellt. Wenn Sie keine Werte für die ACL-Parameter angeben, werden keine CIFS-Freigaben erstellt, und standardmäßig werden NFS-Freigaben erstellt, die allen Zugriff gewähren.

Erstellen von Datensicherungsvolumes: Wenn Sie Dateifreigaben zu Ihrer SVM hinzufügen, ist der Typ des Volumes, das standardmäßig eingebunden wird, `rw`(Lesen/Schreiben). Für die Erstellung von Datensicherungsvolumes (DP-Volumes) ist `dp` als Wert für den `type` Parameter anzugeben.

Löschen von Dateifreigaben

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

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

Dateifreigaben ändern

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

Um eine bestimmte Dateifreigabe zu ändern, benötigen Sie den Dateifreigabeschlüssel. Zusätzlich müssen Sie die zu aktualisierende Eigenschaft sowie deren Wert angeben.

> Es ist zu beachten, dass Sie mit einem einzigen Aufruf dieser API nur eine Eigenschaft aktualisieren können. Für mehrere Aktualisierungen muss diese API entsprechend oft ausgeführt werden.

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

Verwaltung von LUNs mithilfe von APIs in Active IQ Unified Manager

Mit der `/storage-provider/luns` API können Sie die LUNs in Ihrer Datacenter-Umgebung anzeigen, hinzufügen, ändern und löschen.

Vor der Provisionierung der LUNs ist sicherzustellen, dass die SVM erstellt und mit den unterstützten Protokollen provisioniert wurde. Wenn bei der Provisionierung Performance Service Levels (PSLs) oder Storage Efficiency Policies (SEPs) zugewiesen werden, sollten die PSLs bzw. SEPs vor der Erstellung der LUN erstellt werden.

LUNs anzeigen

Mit der folgenden Methode lassen sich die LUNs in Ihrer Unified Manager Umgebung anzeigen. Wenn Sie einen ONTAP Cluster als Datenquelle in Active IQ Unified Manager hinzugefügt haben, werden die Storage Workloads für diese Cluster automatisch Ihrer Unified Manager Instanz hinzugefügt. Diese API ruft alle LUNs ab, die Ihrer Unified Manager Instanz automatisch und manuell hinzugefügt wurden. Die Details einer bestimmten LUN lassen sich anzeigen, indem diese API mit dem LUN Schlüssel ausgeführt wird.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/luns`
		
		`/storage-provider/luns/{key}`

LUNs hinzufügen

Sie können die folgende Methode verwenden, um Ihren SVMs LUNs hinzuzufügen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/luns`

Wenn Sie in Ihrer cURL-Anfrage einen Wert für den optionalen Parameter volume_name_tag in der Eingabe angeben, wird dieser Wert bei der Benennung des Volumes während der LUN-Erstellung verwendet. Dieses Tag erleichtert die Suche nach dem Volume. Wenn Sie den Volume-Schlüssel in der Anfrage angeben, wird die Tag-Vergabe übersprungen.

LUNs löschen

Sie können die folgende Methode verwenden, um eine bestimmte LUN zu löschen. Sie müssen den LUN-Schlüssel angeben, um eine bestimmte LUN zu löschen.

Wenn Sie in ONTAP ein Volume erstellt und anschließend über Unified Manager LUNs auf diesem Volume bereitgestellt haben, wird beim Löschen aller LUNs mithilfe dieser API auch das Volume aus dem ONTAP Cluster gelöscht.

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

LUNs modifizieren

Sie können die folgende Methode verwenden, um eine LUN zu ändern und ihre Eigenschaften zu aktualisieren. Sie müssen den LUN-Schlüssel angeben, um eine bestimmte LUN zu ändern. Außerdem müssen Sie die LUN-Eigenschaft, die Sie aktualisieren möchten, sowie ihren Wert eingeben. Für die Aktualisierung von LUN-Arrays mithilfe dieser API sollten Sie die Empfehlungen unter “Empfehlungen für die Verwendung der APIs” beachten.

Sie können mit einem einzigen Aufruf dieser API nur eine Eigenschaft aktualisieren. Für mehrere Aktualisierungen müssen Sie die API entsprechend oft ausführen.

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

Verwaltung von Performance Service Levels mithilfe von APIs in Active IQ Unified Manager

Sie können Performance Service Levels mithilfe der Storage Provider APIs auf Ihrem Active IQ Unified Manager anzeigen, erstellen, ändern und löschen.

Performance Service Levels anzeigen

Mit der folgenden Methode lassen sich die Performance Service Levels anzeigen, um sie Storage Workloads zuzuweisen. Die API listet alle systemdefinierten und benutzererstellten Performance Service Levels auf und ruft die Attribute aller Performance Service Levels ab. Wenn ein bestimmtes Performance Service Level abgefragt werden soll, muss die eindeutige ID des Performance Service Levels eingegeben werden, um dessen Details abzurufen.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/performance-service-levels`
		
		`/storage-provider/performance-service-levels/{key}`

Hinzufügen von Performance Service Levels

Sie können die folgende Methode verwenden, um benutzerdefinierte Performance Service Levels zu erstellen und sie Ihren Storage Workloads zuzuweisen, wenn die systemdefinierten Performance Service Levels die erforderlichen Service Level Objectives (SLOs) für die Storage Workloads nicht erfüllen. Anschließend erfolgt die Eingabe der Details für das Performance Service Level, das erstellt werden soll. Bei den IOPS-Eigenschaften muss ein gültiger Wertebereich eingegeben werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/performance-service-levels`

Löschen von Performance Service Levels

Sie können mit der folgenden Methode ein bestimmtes Performance Service Level löschen. Ein Performance Service Level kann nicht gelöscht werden, wenn es einer Workload zugewiesen ist oder wenn es das einzige verfügbare Performance Service Level ist. Zum Löschen eines bestimmten Performance Service Level müssen Sie dessen eindeutige ID als Eingabeparameter angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/performance-service-levels/{key}`

Performance Service Levels ändern

Sie können die folgende Methode verwenden, um ein Performance Service Level zu ändern und dessen Eigenschaften zu aktualisieren. Systemdefinierte oder einem Workload zugewiesene Performance Service Level können nicht geändert werden. Um ein bestimmtes Performance Service Level zu ändern, benötigen Sie die eindeutige ID. Außerdem müssen Sie die zu aktualisierende IOPS-Eigenschaft sowie einen gültigen Wert angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/performance-service-levels/{key}`

Anzeige der Aggregate-Funktionen basierend auf Performance Service Levels

Sie können die folgende Methode verwenden, um die Aggregatfunktionen basierend auf Performance Service Levels abzufragen. Diese API gibt die Liste der in Ihrem Datacenter verfügbaren Aggregate zurück und zeigt die Funktionen im Hinblick auf die Performance Service Levels an, die von diesen Aggregaten unterstützt werden können. Bei der Provisionierung von Workloads auf einem Volume können Sie die Fähigkeit eines Aggregats anzeigen, ein bestimmtes Performance Service Level zu unterstützen, und Workloads auf der Grundlage dieser Fähigkeit provisionieren. Die Möglichkeit, das Aggregat anzugeben, ist nur verfügbar, wenn Sie einen Workload mithilfe von APIs provisionieren. Diese Funktionalität ist in der Unified Manager web UI nicht verfügbar.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/aggregate-capabilities`
		
		`/storage-provider/aggregate-capabilities/{key}`

Verwaltung von Speichereffizienzrichtlinien mithilfe von APIs in Active IQ Unified Manager

Sie können Speichereffizienzrichtlinien mithilfe der Storage APIs des Speicheranbieters anzeigen, erstellen, ändern und löschen.

Folgende Punkte sind zu beachten:

- Es ist nicht zwingend erforderlich, beim Erstellen einer Arbeitslast auf Unified Manager eine Speichereffizienzrichtlinie zuzuweisen.
- Eine Storage-Effizienzrichtlinie kann nicht von einer Arbeitslast entfernt werden, nachdem ihr eine Richtlinie zugewiesen wurde.
- Wenn für einen Workload bestimmte Storage Einstellungen auf ONTAP Volumes festgelegt sind, wie z. B. Deduplizierung und Komprimierung, können diese Einstellungen durch die in der Storage Efficiency Policy angegebenen Einstellungen überschrieben werden, die Sie beim Hinzufügen der Storage Workloads in Unified Manager anwenden.

Anzeigen von Storage-Effizienzrichtlinien

Sie können die Speichereffizienzrichtlinien mithilfe der folgenden Methode anzeigen, bevor Sie sie Storage Workloads zuweisen. Diese API listet alle systemdefinierten und benutzerdefinierten Speichereffizienzrichtlinien auf und ruft deren Attribute ab. Um eine bestimmte Speichereffizienzrichtlinie abzufragen, müssen Sie deren eindeutige ID eingeben, um deren Details abzurufen.

Kategorie	HTTP-Verb	Pfad

Storage-Provider	GET	`/storage-provider/storage-efficiency-policies`
		
		`/storage-provider/storage-efficiency-policies/{key}`

Hinzufügen von Storage-Effizienzrichtlinien

Mit der folgenden Methode lassen sich benutzerdefinierte Speichereffizienzrichtlinien erstellen und Ihren Storage-Workloads zuweisen, wenn die systemdefinierten Richtlinien die Anforderungen an die Provisionierung Ihrer Storage-Workloads nicht erfüllen. Als Eingabeparameter dienen die Details der Speichereffizienzrichtlinie, die erstellt werden soll.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/storage-efficiency-policies`

Storage-Effizienzrichtlinien löschen

Mit der folgenden Methode kann eine bestimmte Storage Efficiency Policy gelöscht werden. Eine Storage Efficiency Policy kann nicht gelöscht werden, wenn sie einem Workload zugewiesen ist oder wenn sie die einzige verfügbare Storage Efficiency Policy ist. Zum Löschen einer bestimmten Storage Efficiency Policy muss ihre eindeutige ID als Eingabeparameter angegeben werden.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	LÖSCHEN	`/storage-provider/storage-efficiency-policies/{key}`

Storage-Effizienzrichtlinien ändern

Sie können die folgende Methode verwenden, um eine Storage Efficiency Policy zu ändern und ihre Eigenschaften zu aktualisieren. Eine Storage Efficiency Policy, die systemdefiniert ist oder einem Workload zugewiesen wurde, kann nicht geändert werden. Um eine bestimmte Storage Efficiency Policy zu ändern, müssen Sie die eindeutige ID der Storage Efficiency Policy angeben. Zusätzlich müssen Sie die Eigenschaft, die Sie aktualisieren möchten, zusammen mit ihrem Wert angeben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/storage-efficiency-policies/{key}`

Gängige Arbeitsabläufe für das Storage Management

Informationen zu gängigen API-Workflows für die Speicherverwaltung in Active IQ Unified Manager

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

Die Workflows beschreiben einige der häufig verwendeten Anwendungsfälle für das Storage-Management sowie Beispielcode zur Verwendung. Jede Aufgabe wird anhand eines Workflow-Prozesses beschrieben, der aus einem oder mehreren API-Aufrufen besteht.

Die in den Workflows verwendeten API-Aufrufe verstehen

Sie können von Ihrer Unified Manager Instanz aus die Seite der Online-Dokumentation anzeigen, die die Details zu jedem REST API-Aufruf enthält. Dieses Dokument wiederholt die Details der Online-Dokumentation nicht. Jeder API-Aufruf, der in den Workflow-Beispielen in diesem Dokument verwendet wird, enthält nur die Informationen, die Sie benötigen, um den Aufruf auf der Dokumentationsseite zu finden. Nachdem Sie einen bestimmten API-Aufruf gefunden haben, können Sie die vollständigen Details des Aufrufs prüfen, einschließlich der Eingabeparameter, Ausgabeformate, HTTP-Statuscodes und des Typs der Anfrageverarbeitung.

Die folgenden Informationen sind für jeden API-Aufruf innerhalb eines Workflows enthalten, um den Aufruf auf der Dokumentationsseite zu finden:

- Kategorie: Die API-Aufrufe sind auf der Dokumentationsseite in funktional verwandte Bereiche oder Kategorien unterteilt. Ein bestimmter API-Aufruf kann durch Scrollen zum Seitenende und Klicken auf die entsprechende API-Kategorie gefunden werden.
- HTTP-Verb (Aufruf): Das HTTP-Verb identifiziert die Aktion, die an einer Ressource ausgeführt wird. Jeder API-Aufruf wird über ein einzelnes HTTP-Verb ausgeführt.
- Pfad: Der Pfad bestimmt die spezifische Ressource, auf die sich die Aktion im Rahmen eines Aufrufs

bezieht. Die Pfadzeichenfolge wird an die Core-URL angehängt, um die vollständige URL zu bilden, die die Ressource identifiziert.

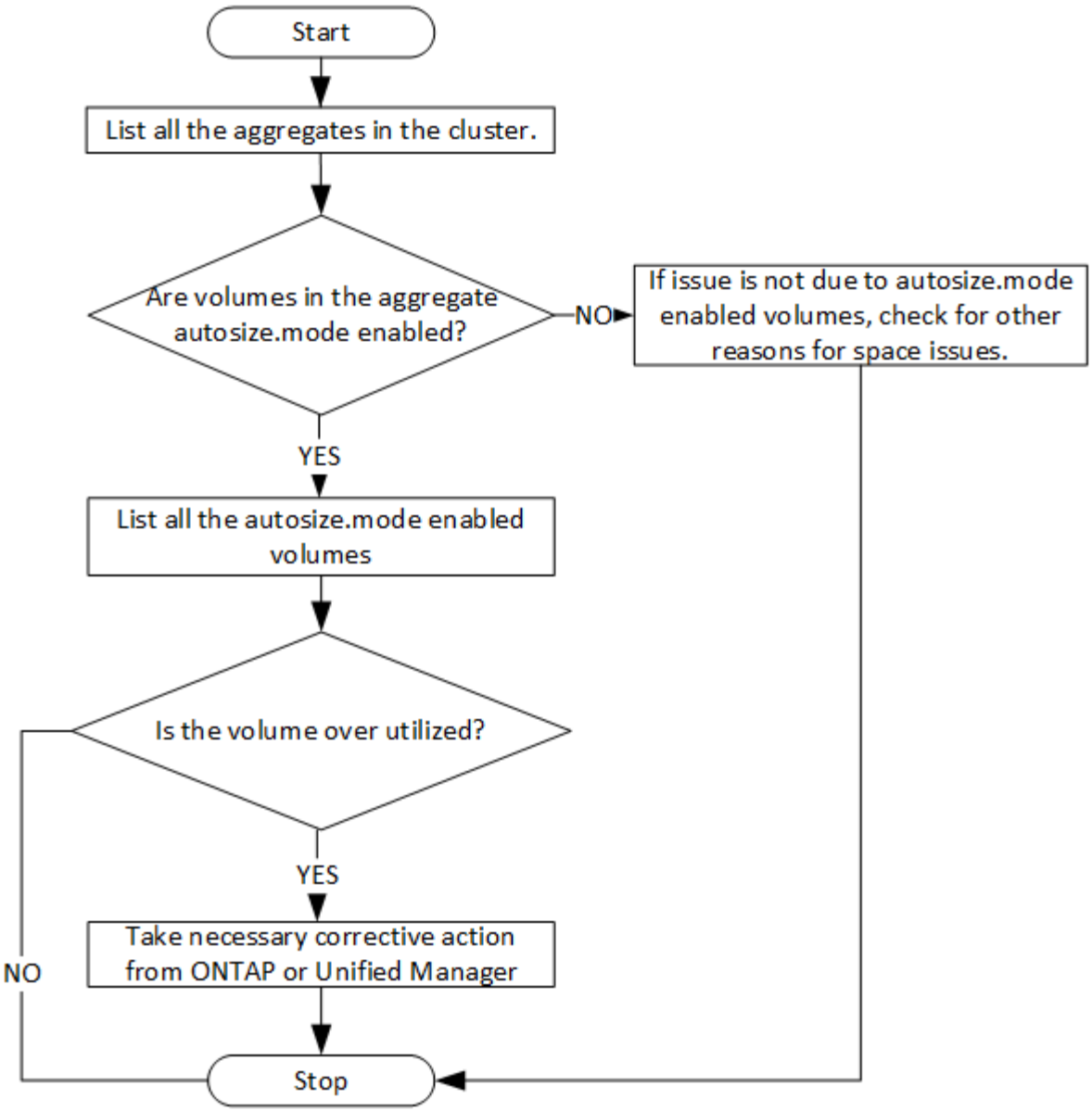
Ermittlung von Speicherplatzproblemen in Aggregaten mithilfe der Active IQ Unified Manager APIs

Mit den Datacenter-APIs in Active IQ Unified Manager kann die Verfügbarkeit und Auslastung des Speicherplatzes in Ihren Volumes überwacht werden. Speicherplatzprobleme in Ihren Volumes können ermittelt und über- oder unterausgelastete Storage-Ressourcen identifiziert werden.

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

Eine Möglichkeit, Speicherplatzmangel in Ihren Aggregaten festzustellen, besteht darin, zu überprüfen, ob in Ihrer Umgebung Volumes mit aktiviertem Modus für die automatische Größenanpassung vorhanden sind. Anschließend folgt die Identifizierung der Volumes, die übermäßig ausgelastet sind, sowie gegebenenfalls die Durchführung von Korrekturmaßnahmen.

Das folgende Flussdiagramm veranschaulicht den Prozess des Abrufens von Informationen über Volumes mit aktivierter automatischer Größenanpassung:



Dieser Ablauf setzt voraus, dass die Cluster bereits in ONTAP erstellt und zu Unified Manager hinzugefügt wurden.

1. Ermittlung des Cluster-Schlüssels, sofern der Wert nicht bekannt ist:

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/cluster/clusters`

2. Unter Verwendung des Cluster-Schlüssels als Filterparameter fragt die Abfrage die Aggregate auf diesem Cluster ab.

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/storage/aggregates`

3. Anhand der Antwort ist die Speicherplatznutzung der Aggregate zu analysieren und festzustellen, welche Aggregate Speicherplatzprobleme aufweisen. Für jedes Aggregat mit Speicherplatzproblem ist der Aggregatschlüssel aus derselben JSON-Ausgabe zu ermitteln.
4. Mithilfe jedes Aggregatschlüssels werden alle Volumes gefiltert, deren Wert für den Parameter autosize.mode als `grow`.

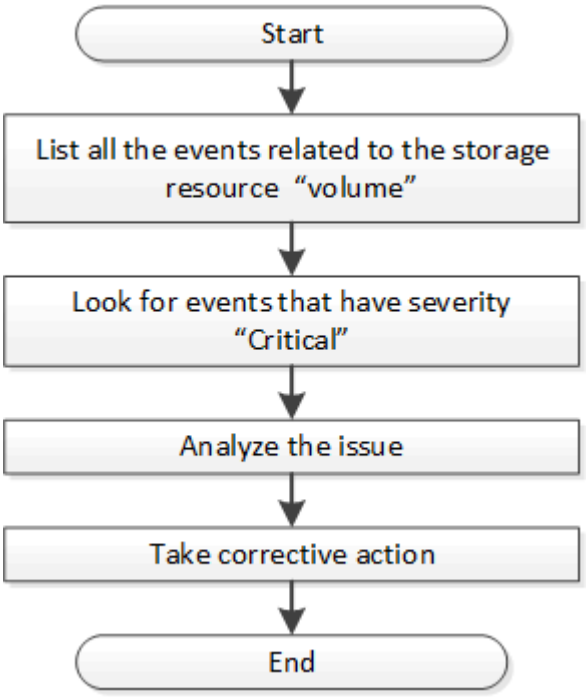
Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/storage/volumes`

5. Es erfolgt eine Analyse, welche Volumes übermäßig genutzt werden.
6. Zur Behebung der Speicherplatzprobleme in Ihrem Volume sind gegebenenfalls Korrekturmaßnahmen erforderlich, z. B. das Verschieben des Volumes auf andere Aggregate. Diese Aktionen können über ONTAP oder die Unified Manager Web-Benutzeroberfläche ausgeführt werden.

Probleme mit Speicherobjekten mithilfe der Event-APIs von Active IQ Unified Manager ermitteln

Wenn ein Storageobjekt in Ihrem Datacenter einen Schwellenwert überschreitet, erhalten Sie eine Benachrichtigung über dieses Ereignis. Mithilfe dieser Benachrichtigung können Sie das Problem analysieren und mithilfe der `events` APIs Korrekturmaßnahmen ergreifen.

Dieser Workflow verwendet das Beispiel eines Volume als Ressourcenobjekt. Mithilfe der `events` APIs können Sie die Liste der Ereignisse abrufen, die mit einem Volume verknüpft sind, die kritischen Probleme für dieses Volume analysieren und anschließend Korrekturmaßnahmen ergreifen, um das Problem zu beheben.



Mit den folgenden Schritten lassen sich die Probleme in Ihrem Volume ermitteln, bevor Korrekturmaßnahmen ergriffen werden.

Schritte

1. Analyse der kritischen Active IQ Unified Manager Ereignisbenachrichtigungen für die Volumes in Ihrem Datacenter.
2. Die Abfrage aller Ereignisse für die Volumes erfolgt mithilfe der folgenden Parameter in der API /management-server/events: `"resource_type": "volume" "severity": "critical"`

Kategorie	HTTP-Verb	Pfad
Management-Server	GET	/management-server/events

3. Die Ausgabe kann angezeigt und die Probleme in den spezifischen Volumes analysiert werden.
4. Die erforderlichen Maßnahmen zur Behebung der Probleme können mithilfe der Unified Manager REST APIs oder der Web UI durchgeführt werden.

Fehlerbehebung bei ONTAP Volumes mithilfe der Active IQ Unified Manager Gateway APIs

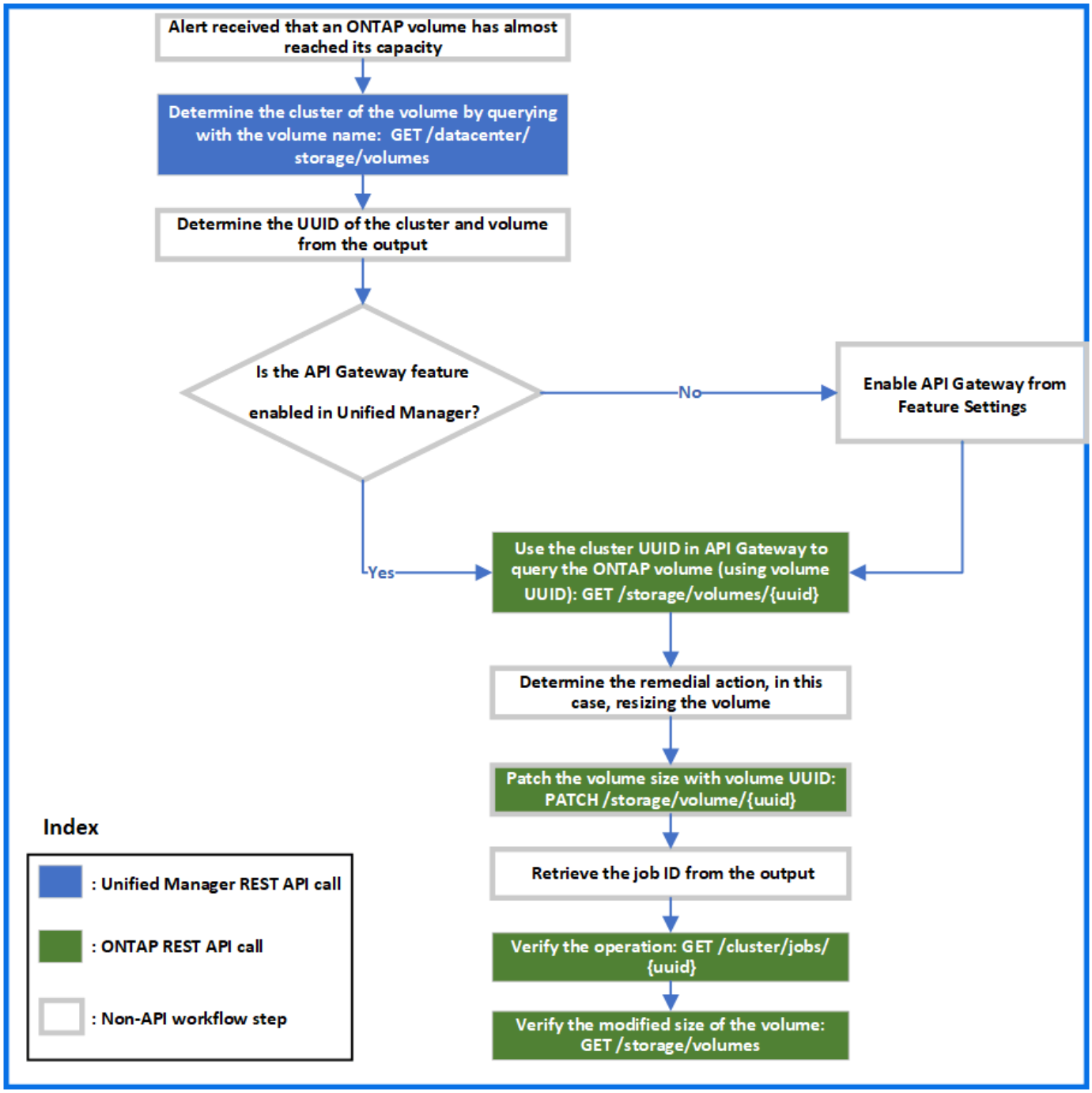
Die Gateway-APIs fungieren als Schnittstelle, um ONTAP-APIs aufzurufen, Informationen über Ihre ONTAP Storage-Objekte abzufragen und Abhilfemaßnahmen zu ergreifen, um die gemeldeten Probleme zu beheben.

Dieser Workflow behandelt einen beispielhaften Anwendungsfall, in dem ein Ereignis ausgelöst wird, wenn ein ONTAP Volume seine Kapazität fast erreicht. Der Workflow zeigt außerdem, wie dieses Problem durch den Aufruf einer Kombination aus Active IQ Unified Manager und ONTAP REST-APIs behoben werden kann.

Vor dem Ausführen der Workflow-Schritte müssen die folgenden Voraussetzungen erfüllt sein:

- Sie kennen die Gateway-APIs und deren Verwendung. Informationen dazu finden Sie unter "Zugriff auf ONTAP APIs über Proxy-Zugriff".
- Sie sind mit der Verwendung von ONTAP REST APIs vertraut. Informationen zur Verwendung von ONTAP REST APIs sind unter "ONTAP Automatisierungsdokumentation" verfügbar.
- Sie sind ein Anwendungsadministrator.
- Auf dem Cluster, auf dem Sie die REST API Vorgänge ausführen möchten, muss ONTAP 9.5 oder höher ausgeführt werden, und der Cluster muss über HTTPS zu Unified Manager hinzugefügt werden.

Das folgende Diagramm veranschaulicht jeden Schritt im Workflow zur Fehlerbehebung bei Problemen mit der Kapazitätsauslastung von ONTAP Volumes.



Der Workflow umfasst die Aufrufpunkte sowohl von Unified Manager als auch der ONTAP REST APIs.

1. Der Volumennamen aus dem Ereignis, das die Kapazitätsauslastung des Volumes meldet, ist zu beachten.
2. Für die Abfrage des Volume mit dem Volumennamen als Wert im Parameter „name“ steht die folgende Unified Manager API zur Verfügung.

Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/storage/volumes`

3. Aus der Ausgabe lassen sich die Cluster-UUID und die Volume-UUID entnehmen.

4. In der Web-Benutzeroberfläche von Unified Manager kann unter **Allgemein** > **Funktionseinstellungen** > **API Gateway** überprüft werden, ob die API Gateway Funktion aktiviert ist. Solange sie nicht aktiviert ist, stehen die APIs der Gateway Kategorie nicht zum Aufrufen zur Verfügung. Falls die Funktion deaktiviert ist, sollte sie aktiviert werden.
5. Die Cluster-UUID ermöglicht das Ausführen der ONTAP API `/storage/volumes/{uuid}` über API gateway. Die Abfrage gibt die Volume-Details zurück, wenn die Volume-UUID als API-Parameter übergeben wird.

   Für die Ausführung der ONTAP APIs über API gateway werden die Unified Manager Anmeldeinformationen intern zur Authentifizierung übergeben, sodass kein zusätzlicher Authentifizierungsschritt für den Zugriff auf einzelne Cluster erforderlich ist.

Kategorie	HTTP-Verb	Pfad

Unified Manager: Gateway
 	
ONTAP: Storage
	GET	Gateway-API:
		`/gateways/{uuid}/{path}`
		
		ONTAP API:
		`/storage/volumes/{uuid}`

   In /gateways/{uuid}/{path} muss der Wert für {uuid} durch die Cluster-UUID ersetzt werden, auf der die REST-Operation ausgeführt werden soll. {path} muss durch die ONTAP REST-URL /storage/volumes/{uuid} ersetzt werden.

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

   Beim Ausführen der GET-Operation wird folgende URL generiert:
   `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

   Beispiel für einen cURL-Befehl

```
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. Anhand der Ausgabe lassen sich Größe, Nutzung und die zu ergreifende Abhilfemaßnahme bestimmen. In diesem Workflow besteht die ergriffene Abhilfemaßnahme in der Anpassung der Größe des Volume.
7. Für die Größenanpassung des Volumes sind die Cluster UUID und die Ausführung der folgenden ONTAP API über das API Gateway erforderlich. Informationen zu den Eingabeparametern für das Gateway und die 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}`

Neben der Cluster UUID und der Volume UUID muss für die Größenänderung des Volumes ein Wert für den Parameter size eingegeben werden. Wichtig ist, dass der Wert in Byte angegeben wird. Wenn beispielsweise die Größe eines Volumes von 100 GB auf 120 GB erhöht werden soll, wird der Wert für den Parameter size am Ende der Abfrage angegeben: `-d {\"size\": 128849018880}"`

Beispiel für einen cURL-Befehl

```
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.

8. Anhand der Job-UUID lässt sich überprüfen, ob der Job erfolgreich ausgeführt wurde. Die folgende ONTAP API kann über das API-Gateway mit der Cluster-UUID und der Job-UUID ausgeführt werden. 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.

9. Die folgende ONTAP API dient zum Abfragen der Details des vergrößerten Volumes. Informationen zu den Eingabeparametern für das gateway und die ONTAP APIs sind in Schritt 5 enthalten.

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 Volumengröße von 120 GB an.

Workflows für das Workload-Management

Bereitstellung und Änderung von Speicherworkloads in Active IQ Unified Manager

Mit Active IQ Unified Manager können Sie Storage Workloads (LUNs, NFS-Dateifreigaben und CIFS-Freigaben) provisionieren und modifizieren. Die Provisionierung umfasst mehrere Schritte, von der Erstellung der Storage Virtual Machine (SVM) bis zur

Anwendung von Performance Service Level und Storage Efficiency Policies auf die Storage Workloads. Das Modifizieren von Workloads umfasst die Schritte zum Ändern spezifischer Parameter und zum Aktivieren zusätzlicher Funktionen für diese.

Folgende Arbeitsabläufe werden beschrieben:

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

  Dieser Workflow muss vor der Provisionierung von LUNs oder Dateifreigaben auf Unified Manager durchgeführt werden.

- Provisionierung von Dateifreigaben.
- Provisionierung von LUNs.
- Ändern von LUNs und Dateifreigaben (anhand des Beispiels zum Aktualisieren des Parameters „Performance Service Level“ für die Storage Workloads).
- Ändern einer NFS-Dateifreigabe zur Unterstützung des CIFS-Protokolls
- Arbeitslasten ändern, um QoS auf AQoS zu aktualisieren

Für jeden Provisionierungsworkflow (LUNs und Dateifreigaben) ist der Abschluss des Workflows zur Überprüfung der SVMs auf den Clustern erforderlich.

Vor der Verwendung der einzelnen APIs in den Workflows ist außerdem die Lektüre der Empfehlungen und Einschränkungen erforderlich. Die entsprechenden Details zu den APIs sind in den jeweiligen Abschnitten der zugehörigen Konzepte und Referenzen verfügbar.

SVMs auf ONTAP Clustern mithilfe der Active IQ Unified Manager APIs überprüfen

Vor der Provisionierung von Dateifreigaben oder LUNs sollte geprüft werden, ob auf den Clustern Storage Virtual Machines (SVMs) erstellt wurden.

Der Workflow setzt voraus, dass ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Die Cluster müssen über die erforderlichen Lizenzen für die Provisionierung von LUNs und Dateifreigaben verfügen.

1. Es ist zu prüfen, ob im Cluster eine SVM erstellt wurde.

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

Beispiel cURL

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

2. Wenn der SVM-Schlüssel nicht zurückgegeben wird, muss die SVM erstellt werden. Zum Erstellen der

SVMs benötigen Sie den Clusterschlüssel, auf dem Sie die SVM provisionieren. Außerdem müssen Sie den SVM-Namen angeben. Die folgenden Schritte sind auszuführen.

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

Ermittlung des Cluster-Schlüssels.

Beispiel cURL

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

3. Der Cluster-Schlüssel aus der Ausgabe dient anschließend als Eingabe für die Erstellung der SVM.

> Beim Erstellen der SVM muss sichergestellt werden, dass sie alle für die Provisionierung von LUNs und Dateifreigaben erforderlichen Protokolle unterstützt, z. B. CIFS, NFS, FCP und iSCSI. Die Provisionierungs-Workflows können fehlschlagen, wenn die SVM die erforderlichen Services nicht unterstützt. Es wird empfohlen, die Services für die jeweiligen Workload-Typen ebenfalls auf der SVM zu aktivieren.

Kategorie	HTTP-Verb	Pfad
Datacenter	POST	`/datacenter/svm/svms`

Beispiel cURL

Die Details des SVM-Objekts sind als Eingabeparameter anzugeben.

```
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\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

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

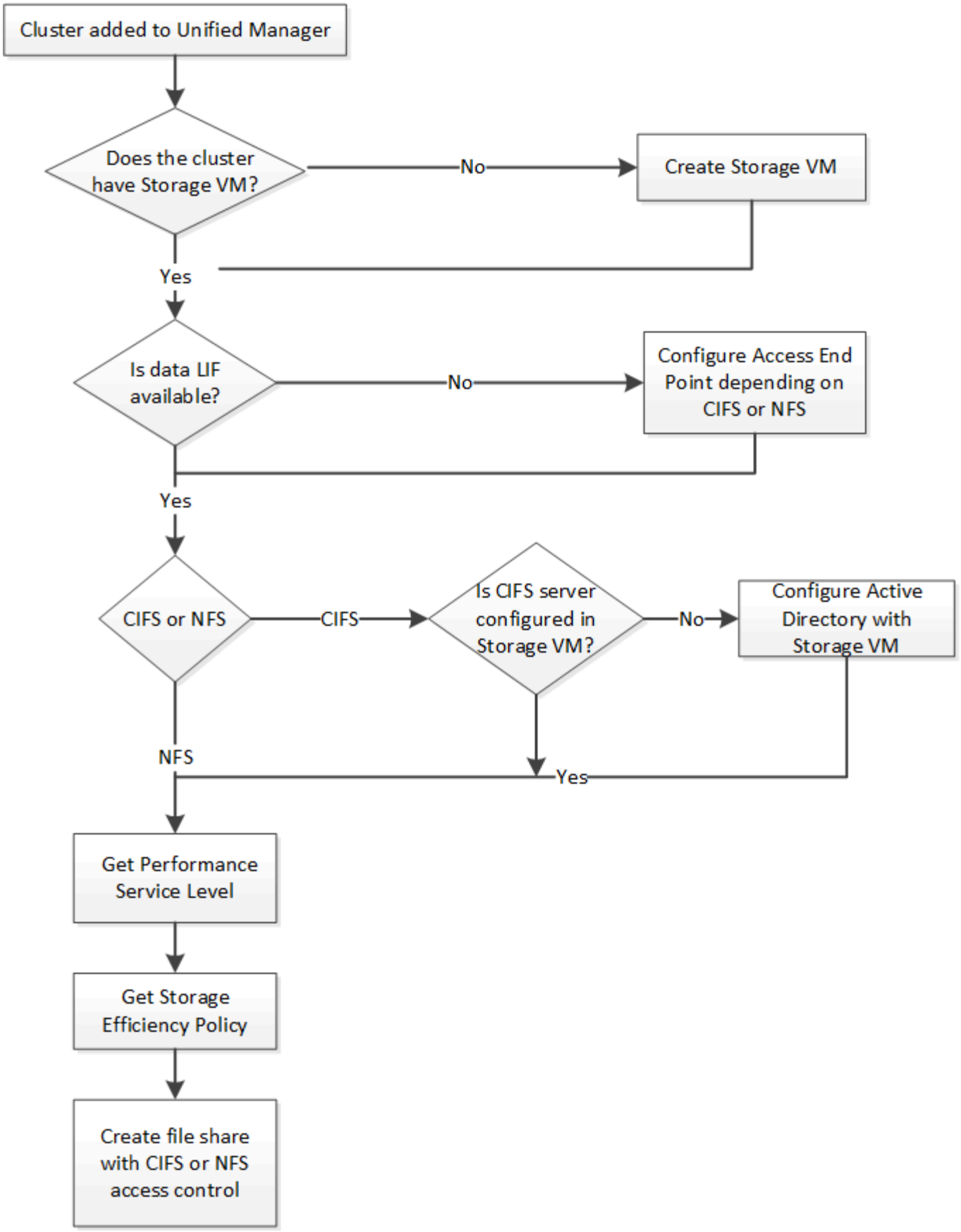
4. Die Überprüfung der SVM-Erstellung erfolgt mithilfe des Jobobjektschlüssels für die Abfrage. Bei erfolgreicher Erstellung der SVM wird der SVM-Schlüssel in der Antwort zurückgegeben.

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

Bereitstellung von CIFS- und NFS-Dateifreigaben mithilfe von Active IQ Unified Manager APIs

Sie können CIFS-Freigaben und NFS-Dateifreigaben auf Ihren Storage Virtual Machines (SVMs) mithilfe der Provisionierungs-APIs provisionieren, die als Teil von Active IQ Unified Manager bereitgestellt werden. Dieser Provisionierungs-Workflow beschreibt die Schritte zum Abrufen der Schlüssel der SVMs, der Performance Service Levels und der Storage Efficiency Policies vor dem Erstellen der Dateifreigaben.

Das folgende Diagramm veranschaulicht jeden Schritt in einem Workflow zur Provisionierung von Dateifreigaben. Es umfasst die Provisionierung sowohl von CIFS-Freigaben als auch von NFS-Dateifreigaben.



Stellen Sie Folgendes sicher:

- ONTAP Cluster wurden zu Unified Manager hinzugefügt, und der Clusterschlüssel wurde abgerufen.
- Auf den Clustern wurden SVMs erstellt.
- Die SVMs unterstützen CIFS- und NFS-Services. Die Provisionierung von Dateifreigaben kann fehlschlagen, wenn die SVMs die erforderlichen Services nicht unterstützen.
- Der FCP-Port ist für die Port-Provisionierung online.

1. Es ist festzustellen, ob auf der SVM, auf der die CIFS-Freigabe erstellt werden soll, Data LIFs oder Zugriffs-Endpunkte verfügbar sind. Die Liste der auf der SVM verfügbaren Zugriffs-Endpunkte:

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}`

Beispiel cURL

```
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. Sofern Ihr Zugriffsendpunkt in der Liste verfügbar ist, erfolgt der Abruf des Schlüssels des Zugriffsendpunkts, andernfalls die Erstellung des Zugriffsendpunkts.

Es muss sichergestellt werden, dass Zugriffs-Endpunkte erstellt werden, auf denen das CIFS-Protokoll aktiviert ist. Die Provisionierung von CIFS-Freigaben schlägt fehl, wenn kein Zugriffs-Endpunkt mit aktiviertem CIFS-Protokoll erstellt wurde.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/access-endpoints`

Beispiel cURL

Sie müssen die Details des Zugriffsendpunkts, 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 Zugriffs-Endpunkt überprüfen können.

3. Überprüfung des Zugriffs-Endpunkts:

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

4. Es ist zu ermitteln, ob eine CIFS-Freigabe oder eine NFS-Dateifreigabe erstellt werden muss. Für die Erstellung von CIFS-Freigaben gelten die folgenden Unterschritte:

   a. Es ist festzustellen, ob der CIFS-Server auf Ihrer SVM konfiguriert ist, das heißt, ob auf der SVM eine Active Directory-Zuordnung eingerichtet ist.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/active-directories-mappings`

   b. Wenn die Active Directory-Zuordnung erstellt wurde, ist der Schlüssel zu verwenden, andernfalls ist die Active Directory-Zuordnung auf der SVM zu erstellen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/active-directories-mappings`

Beispiel cURL

Als Eingabeparameter sind die Details zum Erstellen der Active Directory Zuordnung anzugeben.

```
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\": \"9f4ddea-e395-11e9-b660-
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

+ Dies ist ein synchroner Aufruf, und die Erstellung der Active Directory-Zuordnung lässt sich in der Ausgabe überprüfen. Im Fehlerfall wird eine Fehlermeldung angezeigt, anhand derer sich das Problem beheben und die Anfrage erneut ausführen lässt.

5. Die Ermittlung des SVM-Schlüssels für die SVM, auf der die CIFS-Freigabe oder die NFS-Dateifreigabe erstellt werden soll, erfolgt wie im Workflow-Thema *Verifying SVMs on clusters* beschrieben.
6. Den Schlüssel für das Performance Service Level erhalten Sie, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den `system_defined` Eingabeparameter auf `true` „true“ setzen. In der Ausgabe befindet sich der Schlüssel des Performance Service Levels, das Sie auf die Dateifreigabe anwenden möchten.

7. Optional können Sie den Schlüssel der Storage Efficiency Policy, die Sie auf die Dateifreigabe anwenden möchten, abrufen, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort extrahieren.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/storage-efficiency-policies`

8. Erstellung der 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, die auf dem Volume nur eines der Protokolle unterstützt. Sie können eine NFS-Dateifreigabe auch aktualisieren, um die Zugriffssteuerungsliste einzuschließen, nachdem Sie die NFS-Freigabe erstellt haben. Informationen dazu enthält das Thema *Modifying storage workloads*.

   a. Für die Erstellung nur einer CIFS-Freigabe werden die Informationen zur Zugriffssteuerungsliste (ACL) benötigt. Für die Erstellung der CIFS-Freigabe sind für die folgenden Eingabeparameter gültige Werte anzugeben. Für jede Benutzergruppe, die zugewiesen wird, wird beim Provisionieren einer CIFS/SMB-Freigabe eine ACL erstellt. Anhand der für ACL und Active Directory-Zuordnung eingegebenen Werte werden Zugriffskontrolle 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. Für die Erstellung nur einer NFS-Dateifreigabe sind die Informationen zur Exportrichtlinie erforderlich. Für die Erstellung der NFS-Dateifreigabe sind für die folgenden Eingabeparameter gültige Werte erforderlich. Anhand dieser Werte wird die Exportrichtlinie bei der Erstellung mit der NFS-Dateifreigabe verknüpft.

> Bei der Provisionierung der NFS-Freigabe können Sie entweder eine Exportrichtlinie erstellen, indem Sie alle erforderlichen Werte angeben, oder den Exportrichtlinienschlüssel angeben und eine bestehende Exportrichtlinie wiederverwenden. Wenn Sie eine Exportrichtlinie für die Storage VM wiederverwenden möchten, müssen Sie den Exportrichtlinienschlüssel hinzufügen. Falls Sie den Schlüssel nicht kennen, können Sie den Exportrichtlinienschlüssel über die `/datacenter/protocols/nfs/export-policies` API abrufen. Zum Erstellen einer neuen Richtlinie müssen Sie die Regeln wie im folgenden Beispiel gezeigt eingeben. Anhand der eingegebenen Regeln versucht die API, eine bestehende Exportrichtlinie zu finden, indem sie Host, Storage VM und Regeln abgleicht. Wenn bereits 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"
            }
```

Nach der Konfiguration der Zugriffssteuerungsliste und der Exportrichtlinie sind die gültigen Werte für die obligatorischen Eingabeparameter sowohl für CIFS- als auch für NFS-Dateifreigaben anzugeben:

> Storage Efficiency Policy ist ein optionaler Parameter für die Erstellung von Dateifreigaben.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/file-shares`

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem sich die erstellte Dateifreigabe überprüfen lässt . Die Erstellung der Dateifreigabe lässt sich mithilfe des Job-Objektschlüssels überprüfen, der bei der Abfrage des Jobs zurückgegeben wird:

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"
        }
    }
}
```

1. Zur Überprüfung der Erstellung der Dateifreigabe wird die folgende API mit dem zurückgegebenen Schlüssel ausgeführt:

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

   Beispielhafte JSON-Ausgabe

   Es ist ersichtlich, dass die POST-Methode `/storage-provider/file-shares`intern alle für die einzelnen Funktionen erforderlichen APIs aufruft und das Objekt erstellt. Beispielsweise ruft sie die `/storage-provider/performance-service-levels/`API auf, um das Performance Service Level der Dateifreigabe zuzuweisen.

   ```
   {
       "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": {}
```

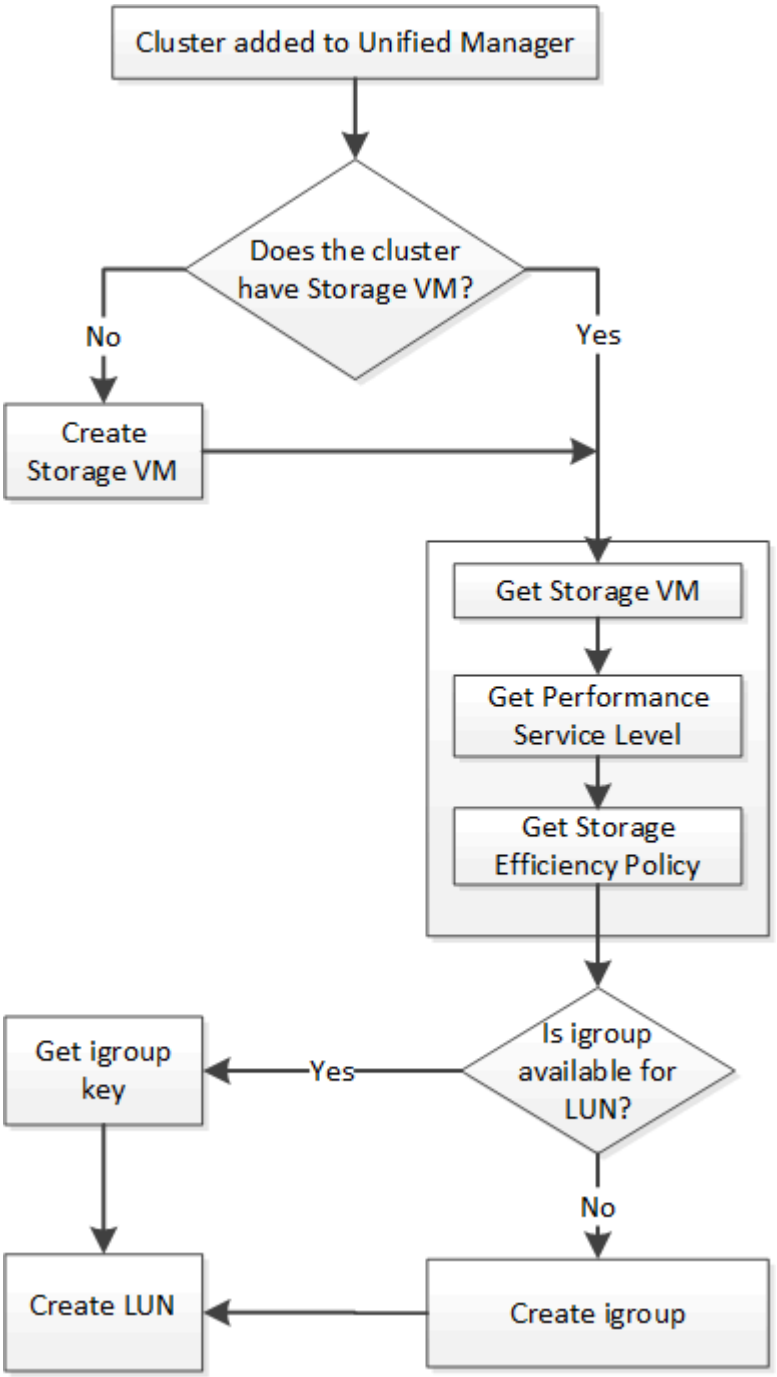
```
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "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 mithilfe der Active IQ Unified Manager APIs

Sie können LUNs auf Ihren Storage Virtual Machines (SVMs) mithilfe der als Teil von Active IQ Unified Manager bereitgestellten Provisionierungs-APIs provisionieren. Dieser Provisionierungs-Workflow beschreibt die Schritte zum Abrufen der Schlüssel der SVMs, der Performance Service Levels und der Storage Efficiency Policies vor dem Erstellen der LUN.

Das folgende Diagramm veranschaulicht die Schritte in einem LUN-Provisionierungs-Workflow.



Dieser Workflow setzt voraus, dass die ONTAP Cluster zu Unified Manager hinzugefügt wurden und der Clusterschlüssel abgerufen wurde. Der Workflow setzt außerdem voraus, dass die SVMs bereits auf den Clustern erstellt wurden.

1. Den SVM-Schlüssel für die SVM, auf der die LUN erstellt werden soll, finden Sie im Workflow-Thema *Verifying SVMs on clusters*.
2. Den Schlüssel für das Performance Service Level erhalten Sie, indem Sie die folgende API ausführen und den Schlüssel aus der Antwort abrufen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/performance-service-levels`

Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den `system_defined` Eingabeparameter auf `true` setzen. Aus der Ausgabe kann der Schlüssel des Performance Service Levels ermittelt werden, das Sie auf die LUN anwenden möchten.

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

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/storage-efficiency-policies`

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

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

Erforderlich ist die Eingabe des Parameterwerts, der die SVM angibt, für die die Initiatorgruppe autorisierten Zugriff hat. Wenn außerdem eine bestimmte Initiatorgruppe abgefragt werden soll, ist der Name der Initiatorgruppe (Schlüssel) als Eingabeparameter anzugeben.

5. Wenn sich in der Ausgabe die Initiatorgruppe finden lässt, der Sie Zugriff gewähren möchten, können Sie den Schlüssel abrufen. Andernfalls kann die Initiatorgruppe erstellt werden.

Kategorie	HTTP-Verb	Pfad
Datacenter	POST	`/datacenter/protocols/san/igroups`

Als Eingabeparameter sind die Details der Initiatorgruppe anzugeben, die erstellt werden soll. Dies ist ein synchroner Aufruf, und die Erstellung der Initiatorgruppe kann in der Ausgabe überprüft werden. Im Fehlerfall erscheint eine Meldung, die bei der Fehlerbehebung und beim erneuten Ausführen der API unterstützt.

6. Die LUN wird erstellt.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/luns`

Beim Erstellen der LUN ist sicherzustellen, dass die abgerufenen Werte als obligatorische Eingabeparameter hinzugefügt wurden.

Die Speichereffizienzrichtlinie ist ein optionaler Parameter für die Erstellung von LUNs.

Beispiel cURL

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

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

7. Die Überprüfung der LUN-Erstellung erfolgt mithilfe des Job-Objektschlüssels, der bei der Abfrage des Jobs zurückgegeben wird:

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

Am Ende der Antwort ist der Schlüssel der erstellten LUN sichtbar.

8. Die Erstellung der LUN kann überprüft werden, indem die folgende API mit dem zurückgegebenen Schlüssel ausgeführt wird:

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

Beispielhafte JSON-Ausgabe

Es zeigt sich, dass die POST-Methode `/storage-provider/luns`intern alle für die einzelnen Funktionen erforderlichen APIs aufruft und das Objekt erstellt. Beispielsweise ruft sie die `/storage-provider/performance-service-levels/` API zum Zuweisen des Performance Service Level auf der LUN auf.

== Schritte zur Fehlerbehebung bei Fehlern in der LUN-Erstellung oder -Zuordnung

Nach Abschluss dieses Workflows kann es dennoch zu einem Fehler bei der LUN-Erstellung kommen. Selbst wenn die LUN erfolgreich erstellt wurde, kann die Zuordnung der LUN zur Initiatorgruppe aufgrund einer nicht verfügbaren SAN-LIF oder eines Zugriffsendpunkts auf dem Knoten, auf dem die LUN erstellt wird, fehlschlagen. Im Fehlerfall 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.
```

Die folgenden Schritte zur Fehlerbehebung dienen dazu, diesen Fehler zu umgehen.

1. Erforderlich ist ein Zugriffsendpunkt auf der SVM, auf der Sie versucht haben, die LUN zu erstellen, der das ISCSI/FCP-Protokoll unterstützt.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	POST	`/storage-provider/access-endpoints`

Beispiel cURL

Sie müssen die Details des Zugriffs-Endpunkts, den Sie erstellen möchten, als Eingabeparameter eingeben.

> Stellen Sie sicher, dass Sie im Eingabeparameter die Adresse hinzugefügt haben, um den Home-Node der LUN anzugeben, sowie die ha_address, um den Partner-Node des Home-Node anzugeben. Bei der Ausführung dieses Vorgangs werden Zugriffsendpunkte sowohl auf dem Home-Node als auch auf dem Partner-Node erstellt.

2. Anhand des im JSON-Output zurückgegebenen Job-Objektschlüssels lässt sich überprüfen, dass der Job erfolgreich ausgeführt wurde, um die Zugriffs-Endpunkte auf der SVM hinzuzufügen, und dass die iSCSI/FCP Services auf der SVM aktiviert wurden.

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

Beispielhafte JSON-Ausgabe

Am Ende der Ausgabe ist der Schlüssel der erstellten Zugriffs-Endpunkte zu sehen. In der folgenden Ausgabe gibt der Wert "name": "accessEndpointKey" den Zugriffs-Endpunkt an, der auf dem Home-Knoten der LUN erstellt wurde und dessen Schlüssel 9c964258-14ef-11ea-95e2-00a098e32c28 lautet. Der Wert "name": "accessEndpointHAKey" gibt den Zugriffs-Endpunkt an, der auf dem Partnerknoten des Home-Knotens erstellt wurde und dessen Schlüssel 9d347006-14ef-11ea-8760-00a098e3215f lautet.

3. Die LUN wird geändert, um die Zuordnung der Initiatorgruppe zu aktualisieren. Weitere Informationen zur Workflow-Änderung finden Sie unter „`Modifying storage workloads`“.

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

Die Eingabe umfasst den Initiatorgruppe-Schlüssel, mit dem die LUN-Zuordnung aktualisiert werden soll, sowie den LUN-Schlüssel.

Beispiel cURL

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie überprüfen können, ob die Zuordnung erfolgreich war.

4. Die LUN-Zuordnung lässt sich durch eine Abfrage mit dem LUN-Schlüssel überprüfen.

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

Beispielhafte JSON-Ausgabe

In der Ausgabe können Sie sehen, dass die LUN erfolgreich der Initiatorgruppe (Schlüssel d19ec2fa-fec7-11e8-b23d-00a098e32c28) zugeordnet wurde, mit der sie ursprünglich provisioniert wurde.

Storage Workloads modifizieren

Das Ändern von Speicherworkloads mithilfe von APIs in Active IQ Unified Manager

Das Ändern von Storage-Workloads umfasst das Aktualisieren von LUNs oder Dateifreigaben mit fehlenden Parametern oder das Ändern der vorhandenen Parameter.

Dieser Workflow verwendet das Beispiel der Aktualisierung von Performance Service Levels für LUNs und Dateifreigaben.

Der Workflow setzt voraus, dass die LUN oder die Dateifreigabe mit Performance Service Levels provisioniert wurde.

Dateifreigaben ändern

Beim Bearbeiten einer Dateifreigabe können Sie die folgenden Parameter aktualisieren:

- Kapazität oder Größe.
- Online- oder Offline-Einstellung.
- Richtlinie zur Speichereffizienz.
- Performance-Service-Level.
- Einstellungen der Zugriffssteuerungsliste (ACL).
- Exportrichtlinieneinstellungen. Sie können auch Exportrichtlinienparameter löschen und die standardmäßigen (leeren) Exportrichtlinienregeln für die Dateifreigabe wiederherstellen.

Bei einem einzelnen API-Lauf kann nur ein Parameter aktualisiert werden.

Dieses Verfahren beschreibt das Hinzufügen eines Performance Service Level zu einer Dateifreigabe. Dasselbe Verfahren kann auch zum Aktualisieren jeder anderen Eigenschaft einer Dateifreigabe verwendet werden.

1. Der CIFS- oder NFS-Dateifreigabeschlüssel der Dateifreigabe, die Sie aktualisieren möchten, muss ermittelt werden. Mit dieser API werden alle Dateifreigaben in Ihrem Datacenter abgefragt. Dieser Schritt kann übersprungen werden, wenn Ihnen der Dateifreigabeschlüssel bereits bekannt ist.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	GET	`/storage-provider/file-shares`

2. Die Details der Dateifreigabe können Sie anzeigen, indem Sie die folgende API mit dem Dateifreigabeschlüssel ausführen, den Sie erhalten haben.

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

In der Ausgabe sind die Details der Dateifreigabe zu sehen.

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

3. Benötigt wird der Schlüssel für die Performance Service Level, die dieser Dateifreigabe zugewiesen werden soll. Derzeit ist ihr keine Richtlinie zugewiesen.

Kategorie	HTTP-Verb	Pfad
Performance-Servicelevels	GET	`/storage-provider/performance-service-levels`

> Die Details der systemdefinierten Performance Service Levels können durch Setzen des `system_defined` Eingabeparameters auf `true` abgerufen werden. Der Ausgabe ist der Schlüssel des Performance Service Level zu entnehmen, der auf die Dateifreigabe angewendet werden soll.

4. Performance Service Level auf die Dateifreigabe anwenden.

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 handelt es sich um den Schlüssel des Performance Service Level.

Beispiel cURL

```
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 überprüft werden kann, ob die Zugriffsendpunkte auf den Home- und Partnerknoten erfolgreich erstellt wurden.

5. Anhand des in Ihrer Ausgabe angezeigten Jobobjektschlüssels lässt sich überprüfen, ob der Dateifreigabe das Leistungsdienstniveau hinzugefügt wurde.

Kategorie	HTTP-Verb	Pfad
Verwaltungsserver	GET	`/management-server/jobs/{key}`

Bei einer Abfrage über die ID des Job-Objekts ist erkennbar, ob die Dateifreigabe erfolgreich aktualisiert wurde. Im Fehlerfall empfiehlt sich eine Fehlerbehebung mit anschließender erneuter Ausführung der API. Nach erfolgreicher Erstellung lässt sich die Dateifreigabe abfragen, um das geänderte Objekt anzuzeigen:

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

In der Ausgabe sind die Details der Dateifreigabe zu sehen.

```
"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"
            }
        }
```

Aktualisierung von LUNs

Beim Aktualisieren einer LUN können Sie die folgenden Parameter ändern:

- Kapazität oder Größe
- Online- oder Offline-Einstellung
- Richtlinie zur Storage-Effizienz
- Performance-Service-Level
- LUN erfassen

Bei einem einzelnen API-Lauf kann nur ein Parameter aktualisiert werden.

Dieses Verfahren beschreibt das Hinzufügen eines Performance Service Level zu einer LUN. Dasselbe Verfahren kann auch für die Aktualisierung jeder anderen LUN-Eigenschaft verwendet werden.

1. Der LUN-Schlüssel der LUN, die aktualisiert werden soll, ist zu ermitteln. Diese API liefert Details zu allen LUNs in Ihrem Datacenter. Dieser Schritt kann übersprungen werden, wenn der LUN-Schlüssel bereits bekannt ist.

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

2. Die Details der LUN können Sie anzeigen, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

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

   Die Details der LUN können Sie in der Ausgabe einsehen. Sie sehen, dass dieser LUN kein Performance Service Level zugewiesen ist.

   Beispielhafte JSON-Ausgabe

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

3. Benötigt wird der Schlüssel für das Performance Service Level, das der LUN zugewiesen werden soll.

Kategorie	HTTP-Verb	Pfad
Performance-Servicelevels	GET	`/storage-provider/performance-service-levels`

   Sie können die Details der systemdefinierten Performance Service Levels abrufen, indem Sie den `system_defined` Eingabeparameter auf `true` setzen. Aus der Ausgabe kann der Schlüssel des Performance Service Levels ermittelt werden, das Sie auf die LUN anwenden möchten.

4. Das Performance Service Level auf die LUN anwenden.

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

In der Eingabe müssen Sie lediglich den zu aktualisierenden Parameter sowie den LUN-Schlüssel angeben. In diesem Fall handelt es sich um den Schlüssel des Performance Service Level.

Beispiel cURL

```
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\" }"
```

Die JSON-Ausgabe zeigt einen Job-Objektschlüssel an, mit dem Sie die aktualisierte LUN überprüfen können.

5. Die Details der LUN können Sie anzeigen, indem Sie die folgende API mit dem erhaltenen LUN-Schlüssel ausführen.

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

Die Details der LUN können Sie in der Ausgabe einsehen. Dort sehen Sie, dass dieser LUN das Performance Service Level zugewiesen ist.

Beispielhafte 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 mithilfe der Active IQ Unified Manager APIs

Sie können eine NFS-Dateifreigabe ändern, damit sie das CIFS-Protokoll unterstützt. Bei der Erstellung der Dateifreigabe können sowohl Parameter der Zugriffssteuerungsliste (ACL) als auch Exportrichtlinienregeln für dieselbe Dateifreigabe angegeben werden. Wenn Sie CIFS jedoch auf demselben Volume aktivieren möchten, auf dem Sie eine NFS-Dateifreigabe erstellt haben, können Sie die ACL-Parameter dieser Dateifreigabe aktualisieren, damit sie CIFS unterstützt.

Bevor Sie beginnen

1. Eine NFS-Dateifreigabe muss bereits nur mit den Exportrichtliniendetails erstellt worden sein. Informationen dazu enthalten *Managing file shares* und *Modifying storage workloads*.
2. Für diesen Vorgang benötigen Sie den Dateifreigabeschlüssel. Informationen zum Anzeigen von Dateifreigabedetails und zum Abrufen des Dateifreigabeschlüssels mithilfe der Job ID finden Sie unter „Bereitstellen von CIFS- und NFS-Dateifreigaben“.

Dies gilt für eine NFS-Dateifreigabe, die Sie erstellt haben, indem Sie nur Exportrichtlinienregeln und keine ACL-Parameter hinzugefügt haben. Sie ändern die NFS-Dateifreigabe, sodass die ACL-Parameter einbezogen werden.

Schritte

1. Auf der NFS-Dateifreigabe erfolgt ein `PATCH`Vorgang mit den ACL-Details, um CIFS-Zugriff zuzulassen.

Kategorie	HTTP-Verb	Pfad
Storage-Provider	PATCH	`/storage-provider/file-shares`

Beispiel cURL

Basierend auf den Zugriffsrechten, die Sie der Benutzergruppe zuweisen, wird, wie im folgenden Beispiel dargestellt, 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"
    }
```

Beispielhafte JSON-Ausgabe

Die Operation gibt die Job-ID des Jobs zurück, der das Update ausführt.

2. Ob die Parameter korrekt hinzugefügt wurden, lässt sich durch Abfrage der Details der Dateifreigabe für dieselbe Dateifreigabe verifizieren.

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

Beispielhafte 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"
                        }
                    ],
                    "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 zusammen mit der Exportrichtlinie für dieselbe Dateifreigabe sehen.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.