Gängige Arbeitsabläufe für das Storage Management

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_workflow_intro.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Gängige Arbeitsabläufe für das Storage Management . . . 1
Informationen zu gängigen API-Workflows für die Speicherverwaltung in Active IQ Unified Manager . . . 1
Die in den Workflows verwendeten API-Aufrufe verstehen . . . 1
Ermittlung von Speicherplatzproblemen in Aggregaten mithilfe der Active IQ Unified Manager APIs . . . 1
Probleme mit Speicherobjekten mithilfe der Event-APIs von Active IQ Unified Manager ermitteln . . . 3
Fehlerbehebung bei ONTAP Volumes mithilfe der Active IQ Unified Manager Gateway APIs . . . 4
Workflows für das Workload-Management . . . 8
Bereitstellung und Änderung von Speicherworkloads in Active IQ Unified Manager . . . 8
SVMs auf ONTAP Clustern mithilfe der Active IQ Unified Manager APIs überprüfen . . . 8
Bereitstellung von CIFS- und NFS-Dateifreigaben mithilfe von Active IQ Unified Manager APIs . . . 11
Bereitstellung von LUNs mithilfe der Active IQ Unified Manager APIs . . . 20
Storage Workloads modifizieren . . . 25

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.

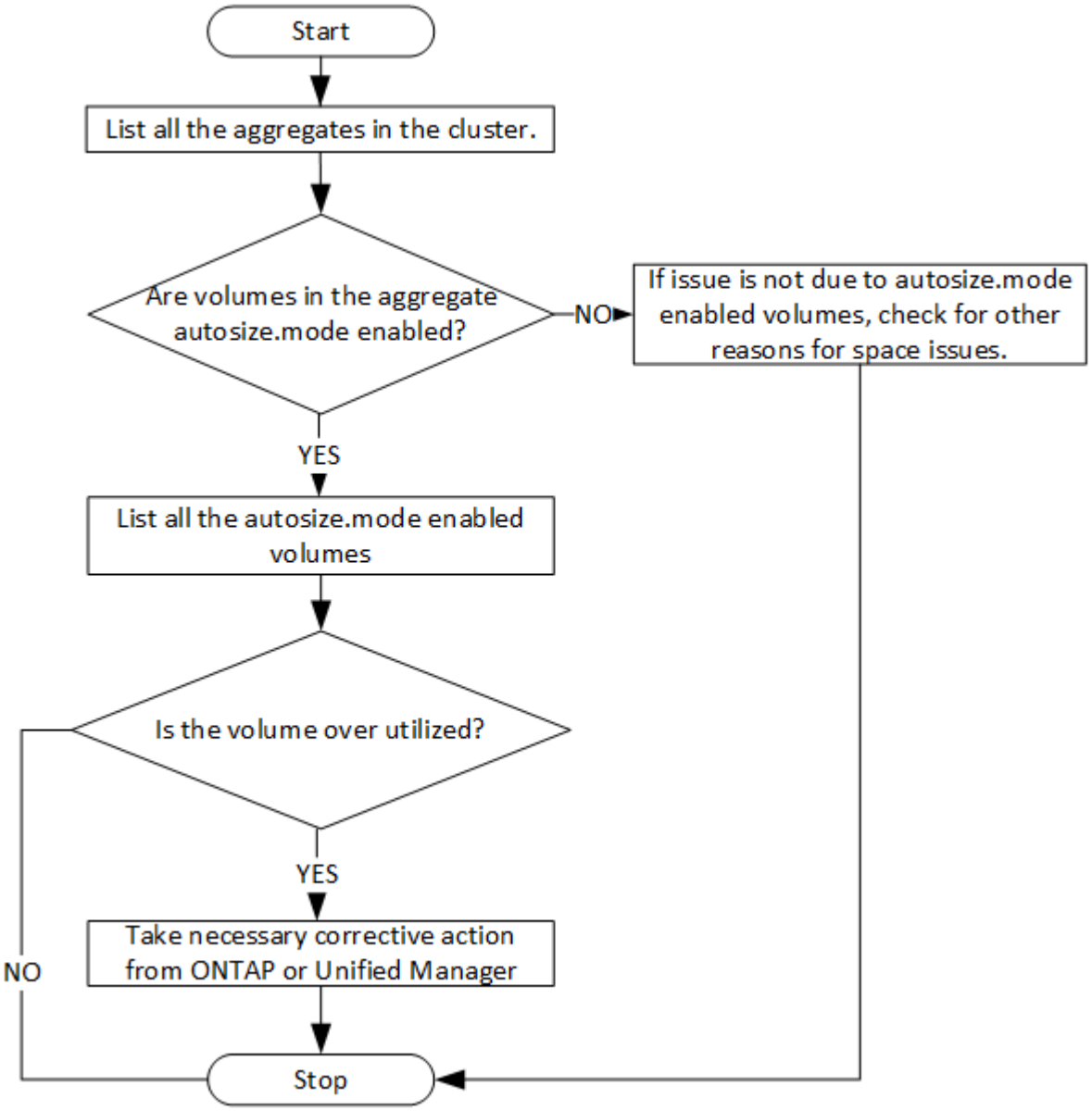
Ermittlung von Speicherplatzproblemen in Aggregaten mithilfe der Active IQ Unified Manager APIs

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`.

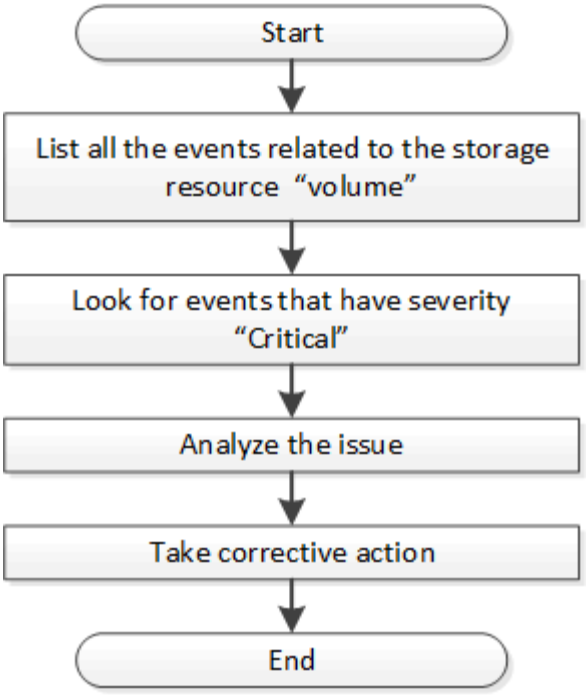
Kategorie	HTTP-Verb	Pfad
Datacenter	GET	`/datacenter/storage/volumes`

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

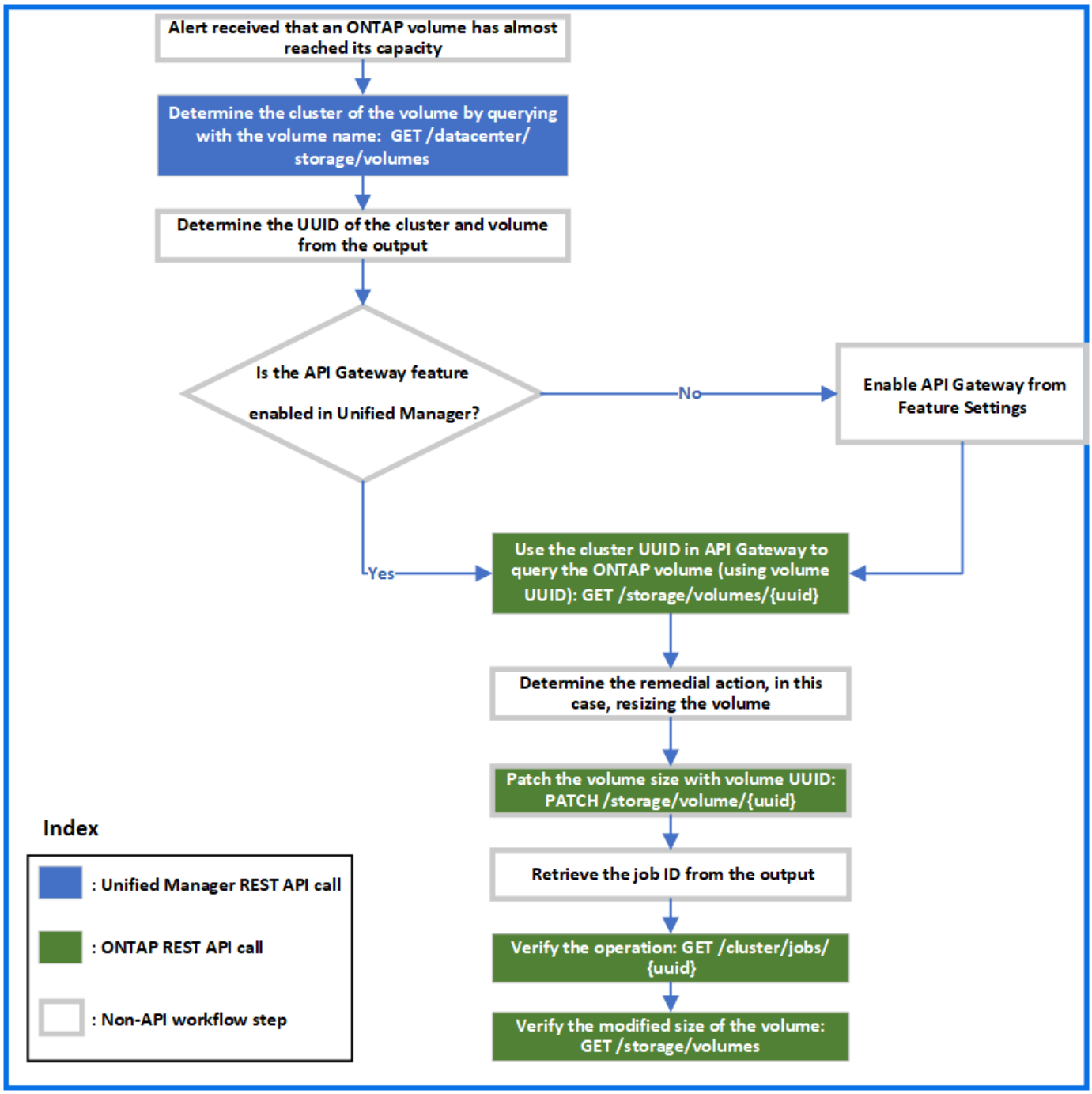
Die Gateway-APIs fungieren als Schnittstelle, um ONTAP-APIs aufzurufen, Informationen über Ihre ONTAP Storage-Objekte abzufragen und Abhilfemaßnahmen zu ergreifen, um die gemeldeten Probleme zu beheben.

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.

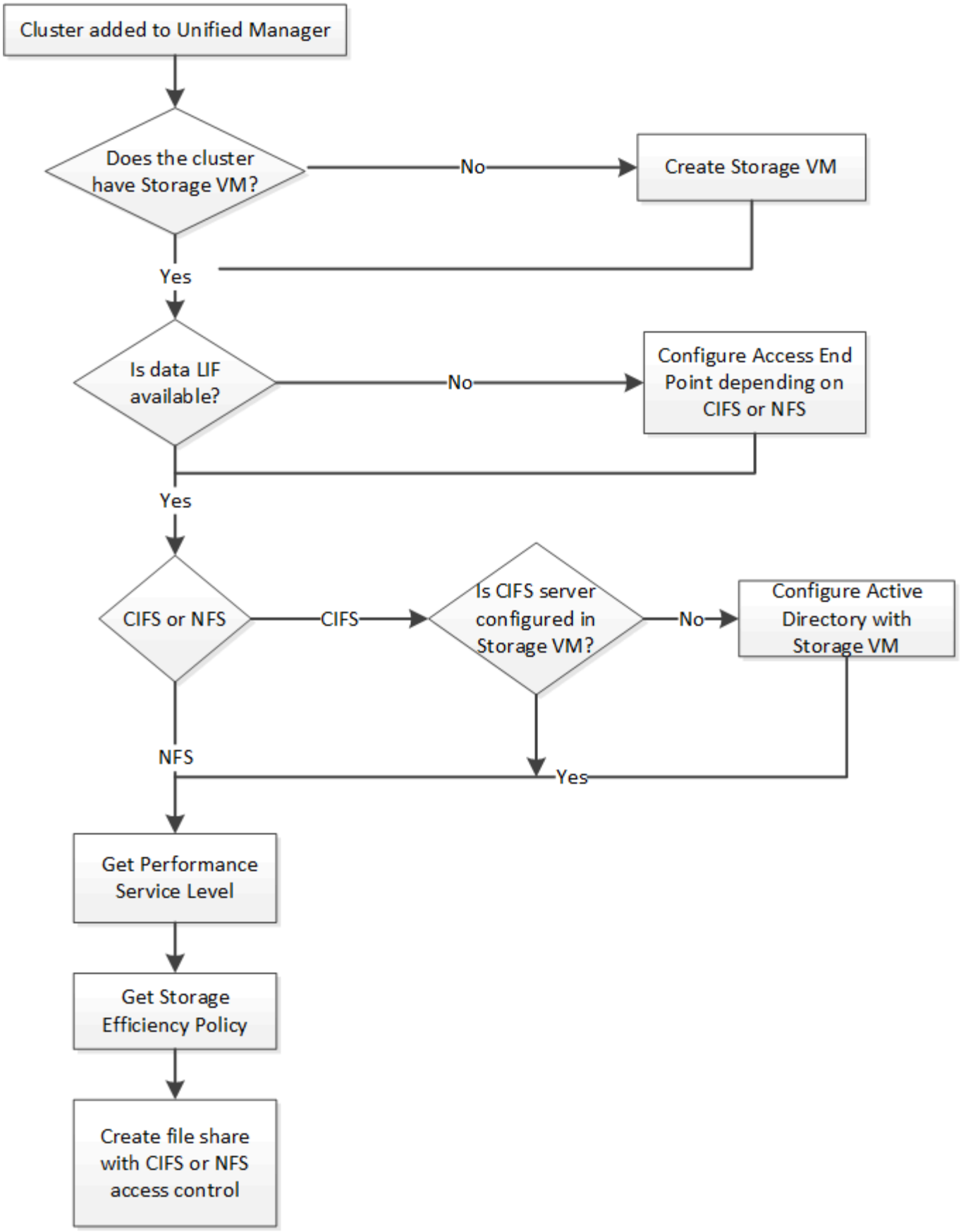
4. Die Überprüfung der SVM-Erstellung erfolgt mithilfe des Jobobjektschlüssels für die Abfrage. Bei erfolgreicher Erstellung der SVM wird der SVM-Schlüssel in der Antwort zurückgegeben.

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": {}
```

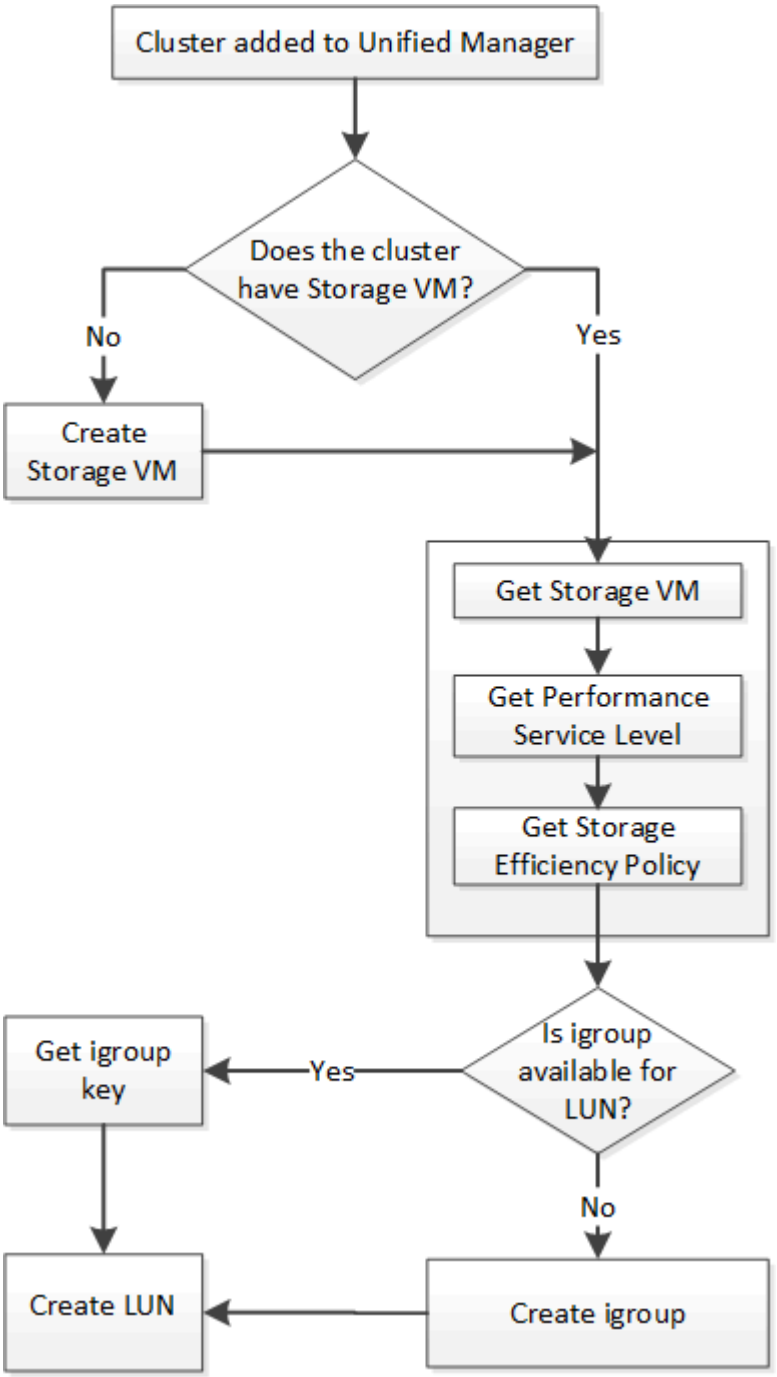
```
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "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.