REST API를 사용하여 스토리지 관리

Active IQ Unified Manager 9.10

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager-910/api-automation/reference_intended_audience_for_this_guide.html on October 16, 2025. Always check docs.netapp.com for the latest.

목차

REST API를 사용하여 스토리지 관리 1
Active IQ Unified Manager REST API 시작하기 1
이 콘텐츠의 대상 1
Active IQ Unified Manager API 액세스 및 범주 1
Active IQ Unified Manager에서 제공되는 REST 서비스 2
Active IQ Unified Manager의 API 버전입니다 3
ONTAP의 스토리지 리소스 4
Active IQ Unified Manager에서 REST API 액세스 및 인증 5
인증 7
Active IQ Unified Manager에서 사용되는 HTTP 상태 코드입니다 8
Active IQ Unified Manager용 API 사용을 위한 권장 사항 9
문제 해결을 위한 로그 9
작업 객체 비동기 프로세스 10
Hello API 서버 11
Unified Manager REST API 15
데이터 센터의 스토리지 오브젝트 관리 15
프록시 액세스를 통해 ONTAP API 액세스 20
관리 작업을 수행합니다 22
사용자 관리 24
성능 메트릭 보기 25
작업 및 시스템 세부 정보 보기 32
이벤트 및 경고 관리 33
워크로드 관리 35
스토리지 관리를 위한 공통 워크플로우 43
워크플로에 사용되는 API 호출 이해 43
애그리게이트에서 공간 문제를 확인하는 중입니다 44
이벤트를 사용하여 스토리지 개체의 문제 확인 45
게이트웨이 API를 사용하여 ONTAP 볼륨 문제 해결 46
워크로드 관리를 위한 워크플로우 50

REST API를 사용하여 스토리지 관리

Active IQ Unified Manager REST API 시작하기

Active IQ Unified Manager은 타사 통합을 위해 RESTful 웹 서비스 인터페이스를 통해 지원되는 스토리지 시스템에서 스토리지 리소스를 관리하는 일련의 API를 제공합니다.

이 항목에서는 Unified Manager API에 대한 정보, 특정 문제를 해결하기 위한 샘플 워크플로우 및 일부 샘플 코드에 대해 설명합니다. 이 정보를 사용하여 NetApp 시스템 관리를 위한 NetApp 관리 효율 소프트웨어 솔루션의 RESTful 클라이언트를 생성할 수 있습니다. API는 REST(Representational State Transfer) 아키텍처 스타일을 기반으로 합니다. CRUD라고도 하는 4개의 REST 작업 모두 생성, 읽기, 업데이트 및 삭제가 지원됩니다.

이 콘텐츠의 대상

이 항목은 REST API를 통해 Active IQ Unified Manager 소프트웨어와 상호 작용하는 응용 프로그램을 만드는 개발자를 위한 것입니다.

스토리지 관리자 및 설계자는 이 정보를 참조하여 Unified Manager REST API를 사용하여 클라이언트 애플리케이션을 구축하고 NetApp 스토리지 시스템을 관리 및 모니터링하는 방법을 기본적으로 이해할 수 있습니다.

스토리지 공급자, ONTAP 클러스터 및 관리 관리 관리 API를 사용하여 스토리지를 관리하려면 이 정보를 사용해야 합니다.

> 운영자, 스토리지 관리자 또는 애플리케이션 관리자 역할 중 하나가 있어야 합니다. REST API를 실행할 Unified Manager 서버의 IP 주소 또는 정규화된 도메인 이름을 알아야 합니다.

Active IQ Unified Manager API 액세스 및 범주

Active IQ Unified Manager API를 사용하면 사용자 환경에서 스토리지 객체를 관리 및 프로비저닝할 수 있습니다. 또한 Unified Manager 웹 UI에 액세스하여 이러한 기능 중 일부를 수행할 수도 있습니다.

REST API에 직접 액세스하기 위한 **URL**을 생성하는 중입니다

Python, C#, C++, JavaScript 등 프로그래밍 언어를 통해 REST API에 직접 액세스할 수 있습니다. 기타 REST API에 액세스할 호스트 이름 또는 IP 주소와 URL을 형식으로 입력합니다

https://<hostname>/api+ 를 참조하십시오

> 기본 포트는 443입니다. 사용자 환경에서 필요에 따라 포트를 구성할 수 있습니다.

온라인 **API** 설명서 페이지 액세스

제품과 함께 제공되는 _API Documentation_reference 콘텐츠 페이지에 액세스하여 API 설명서를 표시하고 인터페이스(예: Swagger)에서 API 호출을 수동으로 실행할 수 있습니다. 이 설명서는 * 메뉴 모음 * > * 도움말 버튼 * > * API 문서 * 를 클릭하여 액세스할 수 있습니다

또는 호스트 이름 또는 IP 주소와 URL을 입력하여 REST API 페이지에 액세스합니다

https://<hostname>/docs/api/+ 를 참조하십시오

범주

API 호출은 영역 또는 범주를 기반으로 기능적으로 구성됩니다. 특정 API를 찾으려면 해당 API 범주를 클릭합니다.

Unified Manager와 함께 제공되는 REST API를 사용하여 관리, 모니터링 및 프로비저닝 기능을 수행할 수 있습니다. API는 다음 범주로 그룹화됩니다.

- * 데이터 센터 *

  이 범주에는 Work Flow Automation 및 Ansible과 같은 툴을 사용하여 데이터 센터 스토리지 관리 및 분석에 도움이 되는 API가 포함됩니다. 이 범주의 REST API는 클러스터, 노드, 애그리게이트, 볼륨, LUN, 데이터 센터의 파일 공유, 네임스페이스 및 기타 요소

- * 관리 - 서버 *

  관리-서버* 범주의 API에는 작업, 시스템, 이벤트 API가 포함됩니다. 작업은 Unified Manager에서 스토리지 오브젝트 또는 워크로드를 관리하는 것과 관련하여 비동기식 실행을 위해 예약된 작업입니다. 'events' API는 데이터 센터의 이벤트를 반환하고, 'system' API는 Unified Manager 인스턴스 세부 정보를 반환합니다.

- 스토리지 공급자 *

  이 범주에는 파일 공유, LUN, 성능 서비스 레벨 및 스토리지 효율성 정책을 관리 및 프로비저닝하는 데 필요한 모든 프로비저닝 API가 포함됩니다. 또한 API를 사용하면 액세스 엔드포인트, Active Directory를 구성할 수 있을 뿐 아니라 스토리지 워크로드에 성능 서비스 수준 및 스토리지 효율성 정책을 할당할 수 있습니다.

- * 관리 *

  이 범주에는 백업 설정 유지 관리, Unified Manager 데이터 소스의 신뢰 저장소 인증서 보기, ONTAP 클러스터를 Unified Manager의 데이터 소스로 관리하는 등 관리 작업을 실행하는 데 사용되는 API가 포함됩니다.

- * 게이트웨이 *

  Unified Manager를 사용하면 게이트웨이 범주의 API를 통해 ONTAP REST API를 호출하고 데이터 센터의 스토리지 객체를 관리할 수 있습니다.

- 보안 *

  이 범주에는 Unified Manager 사용자 관리를 위한 API가 포함됩니다.

Active IQ Unified Manager에서 제공되는 REST 서비스

Active IQ Unified Manager API를 사용하기 전에 제공되는 REST 서비스 및 작업을 알고 있어야 합니다.

API 서버를 구성하는 데 사용되는 프로비저닝 및 관리 API는 읽기(GET) 또는 쓰기(POST, 패치, 삭제) 작업을 지원합니다. 다음은 API에서 지원하는 GET, 패치, POST 및 삭제 작업의 몇 가지 예입니다.

- Get:'Get/DataCenter/cluster/cluster'는 데이터 센터의 클러스터 세부 정보를 검색합니다. Get 작업에 의해

반환되는 최대 레코드 수는 1000개입니다.

API를 사용하면 지원되는 속성별로 레코드를 필터링, 정렬 및 정렬할 수 있습니다.

- POST의 예: 'POST/DataCenter/svm/sSVM'은 맞춤형 SVM(Storage Virtual Machine)을 생성합니다.
- 패치 예: 'patch/datacenter/svm/sSVM/{key}'는 고유한 키를 사용하여 SVM의 속성을 수정합니다.
- 예: 삭제/storage-provider/access-endpoints/{key}'는 고유 키를 사용하여 LUN, SVM 또는 파일 공유에서 액세스 끝점을 삭제합니다.

API를 사용하여 수행할 수 있는 나머지 작업은 운영자, 스토리지 관리자 또는 애플리케이션 관리자 사용자의 역할에 따라 다릅니다.

사용자 역할	**REST** 방식 지원
운영자	데이터에 대한 읽기 전용 액세스. 이 역할을 가진 사용자는 모든 GET 요청을 실행할 수 있습니다.
스토리지 관리자	모든 데이터에 대한 읽기 액세스. 이 역할을 가진 사용자는 모든 GET 요청을 실행할 수 있습니다. 또한 패치, POST 및 삭제 요청을 실행하기 위한 쓰기 액세스 권한이 있어 관리, 스토리지 서비스 개체 및 스토리지 관리 옵션과 같은 특정 작업을 수행할 수 있습니다.
응용 프로그램 관리자	모든 데이터에 대한 읽기 및 쓰기 액세스 이 역할을 가진 사용자는 모든 기능에 대한 GET, 패치, POST 및 삭제 요청을 실행할 수 있습니다.

모든 REST 작업에 대한 자세한 내용은 _Online API 설명서_를 참조하십시오.

Active IQ Unified Manager의 API 버전입니다

Active IQ Unified Manager의 REST API URI는 버전 번호를 지정합니다. 예: '/v2/datacenter/svm/sSVM. /v2/datacenter/svm/sSVM의 버전 번호 "v2"는 특정 릴리즈에서 사용되는 API 버전을 나타냅니다. 버전 번호는 클라이언트가 처리할 수 있는 응답을 다시 전송하여 API 변경이 클라이언트 소프트웨어에 미치는 영향을 최소화합니다.

이 버전 번호의 숫자 부분은 릴리스에 대해 증분됩니다. 버전 번호가 있는 URI는 향후 릴리스에서 이전 버전과의 호환성을 유지하는 일관된 인터페이스를 제공합니다. 버전 없이 기본 API를 나타내는 /datacenter/svm/sSVM과 같은 버전 없이 동일한 API를 찾을 수도 있습니다. 기본 API는 항상 최신 버전의 API입니다.

Swagger 인터페이스의 오른쪽 상단에서 사용할 API 버전을 선택할 수 있습니다. 가장 높은 버전이 기본적으로 선택됩니다. Unified Manager 인스턴스에서 사용 가능한 증분 정수와 관련하여 가장 높은 버전의 특정 API를 사용하는 것이 좋습니다.

모든 요청에 대해 사용할 API 버전을 명시적으로 요청해야 합니다. 버전 번호가 지정되면 서비스는 응용 프로그램이 처리하도록 설계되지 않은 응답 요소를 반환하지 않습니다. REST 요청에는 version 매개 변수를 포함해야 합니다. 이전

버전의 API는 몇 번의 릴리즈 이후 더 이상 사용되지 않습니다. 이번 릴리즈에서는 v1 버전의 API가 더 이상 사용되지 않습니다.

ONTAP의 스토리지 리소스

ONTAP의 스토리지 리소스는 크게 물리적 스토리지 리소스 및 _논리적 스토리지 리소스로 분류할 수 있습니다. _ Active IQ Unified Manager에서 제공하는 API를 사용하여 ONTAP 시스템을 효과적으로 관리하려면 스토리지 리소스 모델 및 다양한 스토리지 리소스 간의 관계를 이해해야 합니다.

- 물리적 스토리지 리소스 *

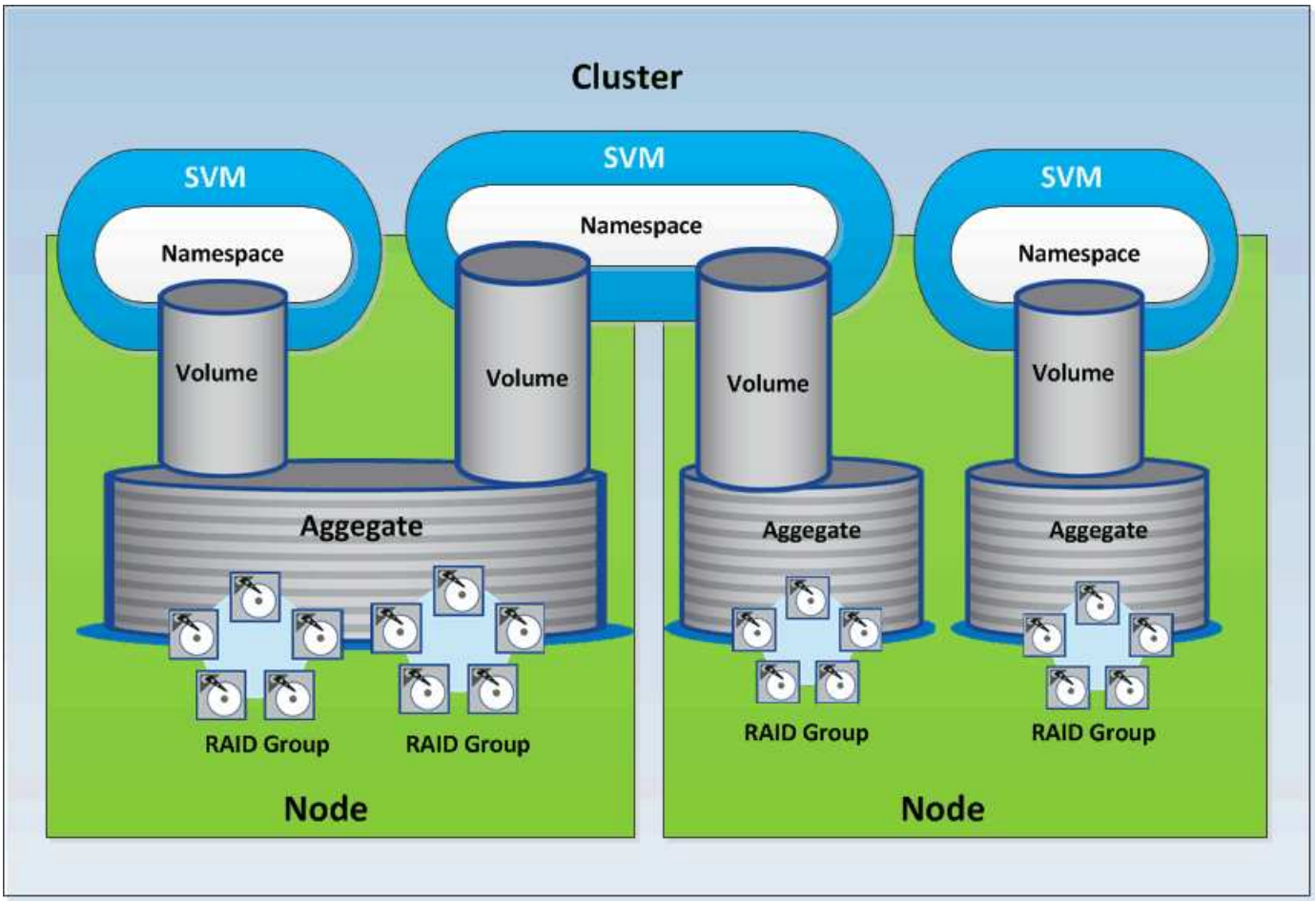
  ONTAP에서 제공하는 물리적 스토리지 객체를 나타냅니다. 물리적 스토리지 리소스에는 디스크, 클러스터, 스토리지 컨트롤러, 노드 및 애그리게이트가 포함됩니다.

- * 논리적 스토리지 리소스 *

  물리적 리소스에 연결되지 않은 ONTAP에서 제공하는 스토리지 리소스를 말합니다. 이러한 리소스는 스토리지 가상 머신(SVM, 이전의 Vserver)과 연결되며, 디스크, 어레이 LUN 또는 애그리게이트와 같은 특정 물리적 스토리지 리소스와 독립적으로 존재하게 됩니다.

  논리적 스토리지 리소스에는 모든 유형과 Qtree의 볼륨뿐 아니라 스냅샷 복사본, 중복제거, 압축, 할당량 등과 같은 리소스에 사용할 수 있는 기능 및 구성이 포함됩니다.

다음 그림에서는 2노드 클러스터의 스토리지 리소스를 보여 줍니다.



Active IQ Unified Manager에서 REST API 액세스 및 인증

Active IQ Unified Manager REST API는 기본적인 HTTP 인증 메커니즘을 통해 HTTP 요청을 실행할 수 있는 REST 클라이언트 또는 프로그래밍 플랫폼을 사용하여 액세스할 수 있습니다.

샘플 요청 및 응답:

- * 요청 *

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

- * 응답 *

```
{
  "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*'은(는) API 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다.
- 포트 443

  443은 기본 HTTPS 포트입니다. 필요한 경우 HTTPS 포트를 사용자 지정할 수 있습니다.

웹 브라우저에서 HTTP 요청을 실행하려면 REST API 브라우저 플러그인을 사용해야 합니다. CURL 및 Perl과 같은 스크립팅 플랫폼을 사용하여 REST API에 액세스할 수도 있습니다.

인증

Unified Manager는 API에 대한 기본 HTTP 인증 체계를 지원합니다. 보안 정보 흐름(요청 및 응답)을 위해 REST API는 HTTPS를 통해서만 액세스할 수 있습니다. API 서버는 서버 확인을 위해 모든 클라이언트에 자체 서명된 SSL 인증서를 제공합니다. 이 인증서는 사용자 지정 인증서(또는 CA 인증서)로 대체될 수 있습니다.

REST API를 호출하려면 API 서버에 대한 사용자 액세스를 구성해야 합니다. 사용자는 로컬 사용자(로컬 데이터베이스에 저장된 사용자 프로필) 또는 LDAP 사용자(LDAP를 통해 인증하도록 API 서버를 구성한 경우)일 수 있습니다. Unified Manager Administration Console 사용자 인터페이스에 로그인하여 사용자 액세스를 관리할 수 있습니다.

Active IQ Unified Manager에서 사용되는 HTTP 상태 코드입니다

API를 실행하거나 문제를 해결하는 동안 Active IQ Unified Manager API에서 사용되는 다양한 HTTP 상태 코드 및 오류 코드를 알고 있어야 합니다.

다음 표에는 인증과 관련된 오류 코드가 정리되어 있습니다.

HTTP 상태 코드입니다	상태 코드 제목	설명
200	좋습니다	동기 API 호출이 성공적으로 실행될 때 반환됩니다.
201	작성됨	Active Directory 구성과 같은 동기 호출을 통해 새 리소스 생성
202	수락됨	LUN 및 파일 공유 생성과 같은 프로비저닝 기능에 대한 비동기 호출을 성공적으로 실행할 때 반환됩니다.
400	잘못된 요청입니다	입력 유효성 검사 실패를 나타냅니다. 사용자는 요청 본문의 유효한 키와 같은 입력을 수정해야 합니다.
401	권한이 없는 요청입니다	리소스를 볼 수 있는 권한이 없습니다.
403	금지된 요청입니다	연결하려는 리소스에 대한 액세스는 금지됩니다.
404	리소스를 찾을 수 없습니다	연결하려는 리소스를 찾을 수 없습니다.
405	메서드가 허용되지 않습니다	메서드가 허용되지 않습니다.
429	요청이 너무 많습니다	사용자가 특정 시간 내에 너무 많은 요청을 보낼 때 반환됩니다.
500입니다	내부 서버 오류입니다	내부 서버 오류입니다. 서버에서 응답을 가져오지 못했습니다. 이 내부 서버 오류는 영구적인 오류일 수도 있고 그렇지 않을 수도 있습니다. 예를 들어, 'Get' 또는 'Get All' 작업을 실행하고 이 오류를 수신하는 경우 최소 5회 이상 이 작업을 반복할 것을 권장합니다. 영구적인 오류인 경우 반환되는 상태 코드는 계속 500입니다. 작업이 성공하면 반환되는 상태 코드는 200입니다.

Active IQ Unified Manager용 **API** 사용을 위한 권장 사항

Active IQ Unified Manager에서 API를 사용하는 경우 특정 권장 방법을 따라야 합니다.

- 유효한 실행을 위해서는 모든 응답 콘텐츠 형식이 다음 형식이어야 합니다.

```
application/json
```

- API 버전 번호가 제품 버전 번호와 관련이 없습니다. Unified Manager 인스턴스에 사용할 수 있는 최신 버전의 API를 사용해야 합니다. Unified Manager API 버전에 대한 자세한 내용은 "Active IQ Unified Manager의 'reST API vers버전 관리' 섹션을 참조하십시오.
- Unified Manager API를 사용하여 어레이 값을 업데이트하는 동안 값의 전체 문자열을 업데이트해야 합니다. 배열에 값을 추가할 수 없습니다. 기존 어레이만 교체할 수 있습니다.
- 메트릭 API의 IOPS 및 성능 등 이중 값을 제외한 모든 쿼리 매개 변수에 파이프(|) 및 와일드 카드(+ *+)와 같은 필터 연산자를 사용할 수 있습니다.
- 필터 연산자 와일드 카드(+ *+)와 파이프(|)를 함께 사용하여 개체를 쿼리하지 마십시오. 잘못된 개체 수를 검색할 수 있습니다.
- 필터 값을 사용할 때 값에 '?'가 포함되어 있지 않은지 확인합니다 문자. 이는 SQL 주입의 위험을 완화하기 위한 것입니다.
- 모든 API에 대한 'Get'(All) 요청은 최대 1000개의 레코드를 반환합니다. max_records' 매개 변수를 1000보다 큰 값으로 설정하여 쿼리를 실행해도 1000개의 레코드만 반환됩니다.
- 관리 기능을 수행하려면 Unified Manager UI를 사용하는 것이 좋습니다.

문제 해결을 위한 로그

시스템 로그를 사용하면 API를 실행하는 동안 발생할 수 있는 장애 원인과 문제 해결을 분석할 수 있습니다.

다음 위치에서 로그를 검색하여 API 호출과 관련된 문제를 해결합니다.

로그 위치	사용
'/var/log/socie/access_log.log'	API 호출, 시작 시간, 실행 시간, 상태 및 URL을 호출하는 사용자의 사용자 이름과 같은 모든 API 호출 세부 정보를 포함합니다. 이 로그 파일을 사용하여 자주 사용하는 API를 확인하거나 GUI 워크플로우를 해결할 수 있습니다. 또한 실행 시간을 기준으로 분석을 확장할 수도 있습니다.
'/var/log/ocum/ocumserver.log'	모든 API 실행 로그를 포함합니다. 이 로그 파일을 사용하여 API 호출 문제를 해결하고 디버깅할 수 있습니다.

로그 위치	사용
'/var/log/socie/server.log'	모든 Wildfly 서버 배포 및 서비스 시작/중지 관련 로그를 포함합니다. 이 로그 파일을 사용하여 Wildfly 서버의 시작, 중지 또는 배포 중에 발생하는 문제의 근본 원인을 찾을 수 있습니다.
'/var/log/socie/au.log'	획득 장치 관련 로그를 포함합니다. ONTAP에서 개체를 생성, 수정 또는 삭제했지만 Active IQ Unified Manager REST API에 반영되지 않은 경우 이 로그 파일을 사용할 수 있습니다.

작업 객체 비동기 프로세스

Active IQ Unified Manager는 다른 API를 실행하면서 수행된 작업에 대한 정보를 검색하는 jobs API를 제공한다. 작업 개체를 사용하여 비동기 처리가 작동하는 방식을 알아야 합니다.

일부 API 호출, 특히 리소스를 추가하거나 수정하는 데 사용되는 호출은 다른 호출보다 완료하는 데 시간이 오래 걸릴 수 있습니다. Unified Manager는 오래 실행되는 이러한 요청을 비동기식으로 처리합니다.

작업 개체를 사용하여 설명된 비동기 요청

비동기적으로 실행되는 API 호출을 수행한 후 HTTP 응답 코드 202는 요청이 성공적으로 유효성 확인 및 승인되었지만 아직 완료되지 않았음을 나타냅니다. 요청은 클라이언트에 대한 초기 HTTP 응답 후 계속 실행되는 백그라운드 작업으로 처리됩니다. 응답에는 고유한 식별자를 포함하여 요청을 고정하는 작업 객체가 포함됩니다.

API 요청과 관련된 작업 객체를 쿼리합니다

HTTP 응답에서 반환된 작업 개체에는 여러 속성이 포함되어 있습니다. 상태 속성을 쿼리하여 요청이 성공적으로 완료되었는지 확인할 수 있습니다. 작업 오브젝트는 다음 상태 중 하나일 수 있습니다.

- '정상'입니다
- 경고
- partial_failures를 선택합니다
- "오류"

작업 개체를 폴링하여 작업의 터미널 상태를 감지할 때 성공 또는 실패 등 두 가지 방법을 사용할 수 있습니다.

- 표준 폴링 요청: 현재 작업 상태가 즉시 반환됩니다.
- 긴 폴링 요청: 작업 상태가 정상, 오류 또는 partial_failures로 이동하는 경우

비동기 요청의 단계입니다

다음 고급 절차를 사용하여 비동기 API 호출을 완료할 수 있습니다.

1. 비동기 API 호출을 실행합니다.

2. 요청을 성공적으로 수락했음을 나타내는 HTTP 응답 202 을 수신합니다.
3. 응답 본문에서 작업 객체의 식별자를 추출합니다.
4. 루프 내에서 작업 객체가 터미널 상태인 정상, 오류 또는 partial_failures에 도달할 때까지 기다립니다
5. 작업의 터미널 상태를 확인하고 작업 결과를 가져옵니다.

Hello API 서버

Hello API server_는 간단한 REST 클라이언트를 사용하여 Active IQ Unified Manager에서 REST API를 호출하는 방법을 보여 주는 샘플 프로그램입니다. 샘플 프로그램은 JSON 형식의 API 서버에 대한 기본적인 세부 정보를 제공합니다(서버는 'application/json' 형식만 지원).

사용되는 URI는 https://<hostname>/api/datacenter/svm/svms.` 이다 이 샘플 코드는 다음과 같은 입력 매개 변수를 사용합니다.

- API 서버 IP 주소 또는 FQDN
- 선택 사항: 포트 번호(기본값: 443)
- 사용자 이름입니다
- 암호
- 응답 형식('application/json')

REST API를 호출하려면 Jersey 및 RESTEasy와 같은 다른 스크립트를 사용하여 Active IQ Unified Manager용 Java REST 클라이언트를 작성할 수도 있습니다. 샘플 코드에 대한 다음 고려 사항을 숙지해야 합니다.

- Active IQ Unified Manager에 대한 HTTPS 연결을 사용하여 지정된 REST URI를 호출합니다
- Active IQ Unified Manager에서 제공한 인증서를 무시합니다
- 핸드셰이크 중에 호스트 이름 확인을 건너뜁니다
- URI 연결을 위해 javax.net.ssl.HttpsURLConnection` 사용
- HTTP 기본 인증에 사용되는 Base64 인코딩 문자열을 구성하는 데 타사 라이브러리('org.apache.commons.codec.binary.Base64` 사용합니다

샘플 코드를 컴파일하고 실행하려면 Java 컴파일러 1.8 이상을 사용해야 합니다.

```
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 API

Active IQ Unified Manager용 REST API는 범주를 기준으로 이 섹션에 나열됩니다.

모든 REST API 호출에 대한 세부 정보가 포함된 Unified Manager 인스턴스에서 온라인 설명서 페이지를 볼 수 있습니다. 이 문서에서는 온라인 설명서의 세부 사항을 반복하지 않습니다. 이 문서에 나열되거나 설명된 각 API 호출에는 문서 페이지에서 통화를 찾는 데 필요한 정보만 포함됩니다. 특정 API 호출을 찾은 후 입력 매개 변수, 출력 형식, HTTP 상태 코드 및 요청 처리 유형을 포함하여 해당 호출의 전체 세부 정보를 검토할 수 있습니다.

문서 페이지에서 호출을 쉽게 찾을 수 있도록 워크플로 내의 각 API 호출에 대해 다음 정보가 포함되어 있습니다.

- 범주

  API 호출은 문서 페이지에서 기능적으로 관련된 영역이나 범주로 구성됩니다. 특정 API 호출을 찾으려면 페이지 아래쪽으로 스크롤한 다음 해당 API 범주를 클릭합니다.

- HTTP 동사(호출)

  HTTP 동사는 리소스에 대해 수행되는 작업을 식별합니다. 각 API 호출은 단일 HTTP 동사를 통해 실행됩니다.

- 경로

  경로는 호출 수행의 일부로 작업이 사용하는 특정 리소스를 결정합니다. 경로 문자열이 핵심 URL에 추가되어 리소스를 식별하는 전체 URL을 구성합니다.

데이터 센터의 스토리지 오브젝트 관리

데이터센터 범주의 REST API를 사용하면 클러스터, 노드, 애그리게이트, 스토리지 VM과 같은 데이터 센터의 스토리지 객체를 관리할 수 있습니다. 볼륨, LUN, 파일 공유 및 네임스페이스. 이러한 API는 개체의 구성을 쿼리하는 데 사용할 수 있는 반면, 일부 API를 사용하면 이러한 개체를 추가, 삭제 또는 수정하는 작업을 수행할 수 있습니다.

이러한 API의 대부분은 필터링, 정렬 및 페이지 매김 지원을 통해 클러스터 간 집계를 제공하는 호출을 받습니다. 이러한 API를 실행하면 데이터베이스에서 데이터가 반환됩니다. 따라서 다음 획득 주기에 따라 새로 생성된 객체를 검색한 후 응답해야 합니다.

특정 개체의 세부 정보를 쿼리하려면 해당 개체의 고유 ID를 입력하여 세부 정보를 확인해야 합니다. 예를 들어, 스토리지 오브젝트의 메트릭 및 분석 정보는 를 참조하십시오 "성능 메트릭 보기".

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

API에 대한 curl 명령, 예제, 요청 및 응답은 Swagger API 인터페이스에서 사용할 수 있습니다. Swagger에 표시된 특정 매개 변수를 기준으로 결과를 필터링하고 주문할 수 있습니다. 이러한 API를 사용하면 클러스터, 볼륨 또는 스토리지 VM과 같은 특정 스토리지 개체의 결과를 필터링할 수 있습니다.

데이터 센터의 스토리지 오브젝트를 위한 **API**

HTTP 동사	경로	설명
"내려가세요	'/datacenter/cluster/cluster' '/datacenter/cluster/clusters/{key}'	이 방법을 사용하여 데이터 센터 전체에서 ONTAP 클러스터의 세부 정보를 볼 수 있습니다. API는 클러스터의 IPv4 또는 IPv6 주소, 노드 상태, 성능 용량, HA(High Availability) 쌍 등의 노드 정보 및 클러스터가 모든 SAN 스토리지인지 여부를 표시합니다.
"내려가세요	'/datacenter/cluster/licenses/licenses/datacenter/cluster/licenses/licenses/{key}'	데이터 센터의 클러스터에 설치된 라이센스의 세부 정보를 반환합니다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 라이센스 키, 클러스터 키, 만료 날짜 및 라이센스 범위와 같은 정보가 반환됩니다. 라이센스 키를 입력하여 특정 라이센스의 세부 정보를 검색할 수 있습니다.
"내려가세요	'/datacenter/cluster/nodes' '/datacenter/cluster/nodes/{key}'	이 방법을 사용하여 데이터 센터의 노드 세부 정보를 볼 수 있습니다. 노드의 클러스터, 노드 상태, 성능 용량, HA(고가용성) 쌍에 대한 정보를 볼 수 있습니다.
"내려가세요	'/datacenter/protocols/cifs/공유' '/datacenter/protocols/cifs/공유/{key}'	이 방법을 사용하여 데이터 센터에서 CIFS 공유의 세부 정보를 볼 수 있습니다. 클러스터, SVM, 볼륨 세부 정보 외에도 액세스 제어 목록(ACL)에 대한 정보도 반환됩니다.
"내려가세요	'/datacenter/protocols/nfs/export-policies' '/datacenter/protocols/nfs/export-policies/{key}'	이 방법을 사용하여 지원되는 NFS 서비스에 대한 엑스포트 정책의 세부 정보를 볼 수 있습니다. 클러스터 또는 스토리지 VM에 대한 엑스포트 정책을 쿼리하고 NFS 파일 공유를 프로비저닝하기 위해 엑스포트 정책 키를 재사용할 수 있습니다. 작업 부하에 대한 내보내기 정책 할당 및 재사용에 대한 자세한 내용은 "'CIFS 및 NFS 파일 공유 프로비저닝'을 참조하십시오.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/storage/aggregate' '/datacenter/storage/aggregate/{key}'	이 방법을 사용하여 데이터 센터의 애그리게이트 컬렉션 또는 이러한 애그리게이트나 모니터링을 위한 특정 애그리게이트를 볼 수 있습니다. 클러스터 및 노드 세부 정보, 사용된 성능 용량, 사용 가능한 공간 및 사용된 공간, 스토리지 효율성 등의 정보가 반환됩니다.
"내려가세요	'/datacenter/storage/LUNs' '/datacenter/storage/LUNs/{key}'	이 방법을 사용하여 전체 데이터 센터에서 LUN 컬렉션을 볼 수 있습니다. 클러스터 및 SVM 세부 정보, QoS 정책, igroup 같은 LUN에 대한 정보를 볼 수 있습니다.
"내려가세요	'/datacenter/storage/qos/policies' '/datacenter/storage/qos/policies/{key}'	이 방법을 사용하여 데이터 센터의 스토리지 오브젝트에 해당하는 모든 QoS 정책의 세부 정보를 볼 수 있습니다. 클러스터 및 SVM 세부 정보, 고정 또는 적응형 정책 세부 정보, 해당 정책에 해당하는 오브젝트 수와 같은 정보가 반환됩니다.
"내려가세요	'/datacenter/storage/qtree' '/datacenter/storage/qtree/{key}'	이 방법을 사용하여 모든 FlexVol 볼륨 또는 FlexGroup 볼륨의 데이터 센터 전체에서 qtree 세부 정보를 볼 수 있습니다. 클러스터 및 SVM 세부 정보, FlexVol 볼륨, 엑스포트 정책과 같은 정보가 반환됩니다.
"내려가세요	'/datacenter/storage/volumes' '/datacenter/storage/volumes/{key}'	이 방법을 사용하여 데이터 센터의 볼륨 컬렉션을 볼 수 있습니다. 볼륨이 읽기-쓰기 유형인지, 데이터 보호 또는 로드 공유인지에 관계없이 SVM 및 클러스터 세부 정보, QoS 및 엑스포트 정책과 같은 볼륨 정보가 반환됩니다. FlexVol 및 FlexClone 볼륨의 경우 해당 애그리게이트에 대한 정보를 볼 수 있습니다. FlexGroup 볼륨의 경우 쿼리는 구성요소 애그리게이트 목록을 반환합니다.

HTTP 동사	경로	설명
"내려가세요 POST를 누릅니다 "삭제" 패치	'/datacenter/protocols/san/igroup' '/datacenter/protocols/san/igroup/{key}'	특정 LUN 타겟에 액세스할 수 있는 권한이 있는 이니시에이터 그룹(igroup)을 할당할 수 있습니다. 기존 igroup이 있으면 할당할 수 있습니다. 또한 igroup을 생성하여 LUN에 할당할 수 있습니다. 이러한 방법을 사용하여 각각 igroup을 쿼리, 생성, 삭제 및 수정할 수 있습니다. 참고 사항: • "POST:"igroup을 생성하는 동안 액세스를 할당할 스토리지 VM을 지정할 수 있습니다. • 삭제: 특정 igroup을 삭제하려면 iGroup 키를 입력 매개 변수로 제공해야 합니다. LUN에 igroup을 이미 할당한 경우에는 해당 igroup을 삭제할 수 없습니다. • '패치:' 특정 igroup을 수정하려면 igroup 키를 입력 매개 변수로 제공해야 합니다. 또한 업데이트할 속성과 해당 값을 입력해야 합니다.
"내려가세요 POST를 누릅니다 "삭제" 패치	'/datacenter/svm/sSVM' '/datacenter/svm/sSVM/{key}'	이러한 방법을 사용하여 스토리지 가상 머신(스토리지 VM)을 확인, 생성, 삭제 및 수정할 수 있습니다. • "POST:"입력 매개 변수로 생성하려는 스토리지 VM 객체를 입력해야 합니다. 사용자 지정 스토리지 VM을 생성한 다음 여기에 필요한 속성을 할당할 수 있습니다. • 삭제: 특정 스토리지 VM을 삭제하려면 스토리지 VM 키를 제공해야 합니다. • 패치: 특정 스토리지 VM을 수정하려면 스토리지 VM 키를 제공해야 합니다. 또한 업데이트할 속성과 해당 값을 입력해야 합니다.

참고 사항:

스토리지 VM을 생성하는 동안 환경에서 SLO 기반 워크로드 프로비저닝을 설정한 경우 CIFS 또는 SMB, NFS, FCP, NFS, FCP 등 LUN 및 파일 공유에 대한 프로비저닝에 필요한 모든 프로토콜을 지원해야 합니다. 및 iSCSI를 지원합니다. 스토리지 VM이 필요한 서비스를 지원하지 않으면 프로비저닝 워크플로우가 실패할 수 있습니다. 각 워크로드 유형에 대한 서비스도 스토리지 VM에서 사용하도록 설정하는 것이 좋습니다.

환경에서 SLO 기반 워크로드 프로비저닝을 설정한 경우 스토리지 워크로드가 프로비저닝된 스토리지 VM을 삭제할 수 없습니다. CIFS 또는 SMB 서버가 구성된 스토리지 VM을 삭제하면 이 API는 로컬 Active Directory 구성과 함께 CIFS 또는 SMB 서버도 삭제합니다. 그러나 CIFS 또는 SMB 서버 이름은 Active Directory 서버에서 수동으로 삭제해야 하는 Active Directory 구성에 계속 포함됩니다.

데이터 센터의 네트워크 요소를 위한 **API**입니다

데이터 센터 범주의 다음 API는 작업 환경의 포트 및 네트워크 인터페이스, 특히 FC 포트, FC 인터페이스, 이더넷 포트 및 IP 인터페이스에 대한 정보를 검색합니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/network/ethernet/ports' '/datacenter/network/ethernet/ports/{key}'	데이터 센터 환경의 모든 이더넷 포트에 대한 정보를 검색합니다. 포트 키를 입력 매개 변수로 사용하여 특정 포트의 정보를 볼 수 있습니다. 클러스터 세부 정보, 브로드캐스트 도메인, 상태, 속도 등의 포트 세부 정보 를 입력하고 포트의 활성화 여부를 검색합니다.
"내려가세요	'/datacenter/network/fc/interfaces' '/datacenter/network/fc/interface/{key}'	이 방법을 사용하여 데이터 센터 환경에서 FC 인터페이스의 세부 정보를 볼 수 있습니다. 인터페이스 키를 입력 매개 변수로 사용하면 해당 특정 인터페이스의 정보를 볼 수 있습니다. 클러스터 세부 정보, 홈 노드 세부 정보, 홈 포트 세부 정보 등의 정보가 검색됩니다.
"내려가세요	'/datacenter/network/fc/ports' '/datacenter/network/fc/ports/{key}'	이 명령어는 데이터 센터 환경의 노드에 사용되는 모든 FC 포트에 대한 정보를 조회한다. 포트 키를 입력 매개 변수로 사용하여 특정 포트의 정보를 볼 수 있습니다. 클러스터 세부 정보, 포트 설명, 지원되는 프로토콜 및 포트 상태와 같은 정보가 검색됩니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/network/ip/interfaces' '/datacenter/network/ip/interfaces/{key}'	이 방법을 사용하여 데이터 센터 환경에서 IP 인터페이스의 세부 정보를 볼 수 있습니다. 인터페이스 키를 입력 매개 변수로 사용하면 해당 특정 인터페이스의 정보를 볼 수 있습니다. 클러스터 세부 정보, IPspace 세부 정보, 홈 노드 세부 정보, 페일오버 활성화 여부 등의 정보가 검색됩니다.

프록시 액세스를 통해 **ONTAP API** 액세스

게이트웨이 API를 사용하면 Active IQ Unified Manager 자격 증명을 사용하여 ONTAP REST API를 실행하고 스토리지 객체를 관리할 수 있습니다. 이러한 API는 Unified Manager 웹 UI에서 API 게이트웨이 기능을 사용하도록 설정한 경우 사용할 수 있습니다.

Unified Manager REST API는 ONTAP 클러스터인 Unified Manager 데이터 소스에 대해 수행할 작업을 선택할 수만 지원합니다. ONTAP API를 통해 다른 기능을 사용할 수 있습니다. 게이트웨이 API를 통해 Unified Manager는 각 데이터 센터 클러스터에 개별적으로 로그인하지 않고 ONTAP 클러스터에서 수행할 모든 API 요청을 터널링하는 통과 인터페이스가 됩니다. Unified Manager 인스턴스에서 관리되는 ONTAP 클러스터에서 API를 실행하기 위한 단일 관리 지점으로 작동합니다. API 게이트웨이 기능을 사용하면 Unified Manager가 단일 제어 플레인이 될 수 있으므로 개별적으로 로그인하지 않고도 여러 ONTAP 클러스터를 관리할 수 있습니다. 게이트웨이 API를 사용하면 ONTAP REST API 작업을 실행하여 Unified Manager에 로그인 상태를 유지하고 ONTAP 클러스터를 관리할 수 있습니다.

ⓘ 모든 사용자는 가져오기 작업을 사용하여 쿼리를 실행할 수 있습니다. 애플리케이션 관리자는 모든 ONTAP REST 작업을 실행할 수 있습니다.

게이트웨이는 ONTAP API와 동일한 형식으로 헤더와 본문 요청을 유지함으로써 API 요청을 터널링하기 위한 프록시 역할을 합니다. Unified Manager 자격 증명을 사용하여 개별 클러스터 자격 증명을 전달하지 않고 ONTAP 클러스터에 액세스하고 이를 관리하는 특정 작업을 실행할 수 있습니다. 클러스터 인증 및 클러스터 관리를 계속 관리하지만 API 요청을 특정 클러스터에서 직접 실행하도록 리디렉션합니다. API가 반환하는 응답은 ONTAP에서 직접 실행되는 각 ONTAP REST API가 반환하는 응답과 동일합니다.

HTTP 동사	경로(URL)	설명
"내려가세요	`/ 관문’	이 Get 메서드는 ONTAP REST 호출을 지원하는 Unified Manager에서 관리하는 모든 클러스터의 목록을 검색합니다. 클러스터 세부 정보를 확인하고 클러스터 UUID 또는 UUID(Universal Unique Identifier)를 기반으로 다른 방법을 실행하도록 선택할 수 있습니다. 게이트웨이 API는 ONTAP 9.5 이상에서 지원되는 클러스터만 검색하고 HTTPS를 통해 Unified Manager에 추가됩니다.
"내려가세요 POST를 누릅니다 "삭제" 패치 '옵션'(Swagger에서 사용할 수 없음) "헤드"(Swagger에서 사용할 수 없음)	'/gateways/{uuid}/{path}' {uuid}의 값을 나머지 작업을 수행할 클러스터 UUID로 바꿔야 합니다. 또한 ONTAP 9.5 이상에서 지원되는 클러스터의 UUID가 있고 HTTPS를 통해 Unified Manager에 추가되었는지 확인합니다. {path}은(는) ONTAP REST URL로 대체되어야 합니다. URL에서 '/api/'를 제거해야 합니다.	이 API는 모든 ONTAP REST API에 대해 POST, 삭제, 패치 작업 및 GET를 지원하는 단일 지점 프록시 API입니다. API가 ONTAP에서 지원하는 한 어떠한 API에도 제한 사항이 적용되지 않습니다. 터널링 또는 프록시 기능을 비활성화할 수 없습니다. 'options' 메서드는 ONTAP REST API에서 지원하는 모든 작업을 반환합니다. 예를 들어, ONTAP API가 GET 작업만 지원하는 경우 이 gateway API를 사용하여 options 메소드를 실행하면 get이 응답으로 반환됩니다. 이 방법은 Swagger에서 지원되지 않지만 다른 API 도구에서 수행할 수 있습니다. 옵션 방법은 리소스를 사용할 수 있는지 여부를 결정합니다. 이 작업을 사용하여 HTTP 응답 헤더에서 리소스에 대한 메타데이터를 볼 수 있습니다. 이 방법은 Swagger에서 지원되지 않지만 다른 API 도구에서 수행할 수 있습니다.

API 게이트웨이 터널링 이해

게이트웨이 API를 사용하면 Unified Manager를 통해 ONTAP 개체를 관리할 수 있습니다. Unified Manager는 클러스터 및 인증 세부 정보를 관리하고 요청을 ONTAP REST 끝점으로 리디렉션합니다. 게이트웨이 API는 URL과 Hypermedia를 API 게이트웨이 기본 URL을 사용하여 헤더 및 응답 본문의 HATEOAS(Engine of Application State)

링크로 변환합니다. 게이트웨이 API는 ONTAP REST URL을 추가하고 필요한 ONTAP REST 엔드포인트를 실행하는 프록시 기본 URL 역할을 합니다.

이 예에서 게이트웨이 API(프록시 기본 URL)는 '/gateway/{uuid}/'입니다

ONTAP API는 '/storage/volumes'입니다. ONTAP API REST URL을 PATH 매개 변수의 값으로 추가해야 합니다.

> 경로를 추가하는 동안 URL의 시작 부분에서 ""/" 기호를 제거했는지 확인합니다. API/ 스토리지/ 볼륨의 경우 ' 스토리지/ 볼륨 추가 '를 선택합니다

추가된 URL은 '/geways/{uuuid}/storage/volumes'입니다

'Get' 작업을 실행할 때 생성된 URL은
'GETtps://<hostname\>/API/gateways/<cluster_UUID\>/storage/volumes'입니다

추가된 URL에서 ONTAP REST URL의 '/API' 태그가 제거되고 게이트웨이 API의 태그가 유지됩니다.

- 샘플 curl 명령 *

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

API는 해당 클러스터의 스토리지 볼륨 목록을 반환합니다. 응답 형식은 ONTAP에서 동일한 API를 실행할 때 받는 형식과 동일합니다. 반환된 상태 코드는 ONTAP REST 상태 코드입니다.

API 범위 설정

모든 API에는 클러스터 범위 내에 컨텍스트 세트가 있습니다. 스토리지 VM을 기반으로 작동하는 API도 클러스터를 범위로 가지고 있습니다. 즉, API 작업은 관리되는 클러스터 내의 특정 스토리지 VM에서 수행됩니다. '/gateways/{uuid}/{path}' API를 실행할 때 작업을 실행하는 클러스터의 클러스터 UUID(Unified Manager 데이터 소스 UUID)를 입력해야 합니다. 해당 클러스터 내의 특정 스토리지 VM으로 컨텍스트를 설정하려면 스토리지 VM 키를 X-Dot-SVM-UUID 매개 변수로 입력하거나 스토리지 VM 이름을 X-Dot-SVM-Name 매개 변수로 입력합니다. 매개 변수는 문자열 헤더의 필터로 추가되며 작업이 해당 클러스터 내의 스토리지 VM 범위 내에서 실행됩니다.

- 샘플 curl 명령 *

```
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>"
```

ONTAP REST API 사용에 대한 자세한 내용은 를 참조하십시오 "ONTAP REST API 자동화"

관리 작업을 수행합니다

관리 범주의 API를 사용하여 백업 설정을 수정하고, 백업 파일 정보와 클러스터 인증서를

확인하고, ONTAP 클러스터를 Active IQ Unified Manager 데이터 소스로 관리할 수 있습니다.

이러한 작업을 실행하려면 애플리케이션 관리자 역할이 있어야 합니다. Unified Manager 웹 UI를 사용하여 이러한 설정을 구성할 수도 있습니다.

HTTP 동사	경로	설명
"내려가세요 패치	'/admin/backup-settings' '/admin/backup-settings'	기본적으로 Unified Manager에 구성된 백업 스케줄의 설정을 보려면 'Get' 메서드를 사용합니다. 다음을 확인할 수 있습니다. • 스케줄이 설정되었는지 여부를 나타냅니다 • 예약된 백업 빈도(매일 또는 매주) • 백업 시간입니다 • 응용 프로그램에 보존되어야 하는 최대 백업 파일 수입니다 백업 시간이 서버 시간대에 있습니다. 데이터베이스 백업 설정은 기본적으로 Unified Manager에서 사용할 수 있으며 백업 일정을 만들 수는 없습니다. 그러나 패치 방식을 사용하여 기본 설정을 수정할 수 있습니다.
"내려가세요	'/admin/backup-file-info'	Unified Manager에 대한 백업 스케줄이 수정될 때마다 백업 덤프 파일이 생성됩니다. 이 방법을 사용하여 수정된 백업 설정에 따라 백업 파일이 생성되었는지, 파일의 정보가 수정된 설정과 일치하는지 여부를 확인할 수 있습니다.
"내려가세요	'/admin/datasource-certificate'	이 메서드를 사용하여 트러스트 저장소에서 데이터 소스(클러스터) 인증서를 볼 수 있습니다. ONTAP 클러스터를 Unified Manager 데이터 소스로 추가하기 전에 인증서 검증이 필요합니다.

HTTP 동사	경로	설명
"내려가세요 POST를 누릅니다 패치 "삭제"	'/admin/datasources/cluster' "/admin/datasources/cluster/{key}"	'Get' 메서드를 사용하면 Unified Manager에서 관리하는 데이터 소스(ONTAP 클러스터)의 세부 정보를 검색할 수 있습니다. 새 클러스터를 Unified Manager에 데이터 소스로 추가할 수도 있습니다. 클러스터를 추가하려면 해당 호스트 이름, 사용자 이름 및 암호를 알아야 합니다. Unified Manager에서 데이터 소스로 관리되는 클러스터를 수정 및 삭제하려면 ONTAP 클러스터 키를 사용합니다.

사용자 관리

'보안' 범주의 API를 사용하여 Active IQ Unified Manager에서 선택한 클러스터 개체에 대한 사용자 액세스를 제어할 수 있습니다. 로컬 사용자 또는 데이터베이스 사용자를 추가할 수 있습니다. 인증 서버에 속하는 원격 사용자 또는 그룹을 추가할 수도 있습니다. 사용자에게 할당한 역할의 권한에 따라 스토리지 객체를 관리하거나 Unified Manager에서 데이터를 볼 수 있습니다.

이러한 작업을 실행하려면 애플리케이션 관리자 역할이 있어야 합니다. Unified Manager 웹 UI를 사용하여 이러한 설정을 구성할 수도 있습니다.

'보안' 범주의 API는 사용자 매개 변수인 USERS 매개 변수를 사용하며 키 매개 변수는 사용자 엔터티의 고유 식별자로 사용하지 않습니다.

HTTP 동사	경로	설명
"내려가세요 POST를 누릅니다	'/security/users' '/security/users'	이러한 방법을 사용하여 사용자의 세부 정보를 확인하거나 Unified Manager에 새 사용자를 추가할 수 있습니다. 사용자 유형에 따라 특정 역할을 사용자에게 추가할 수 있습니다. 사용자를 추가하는 동안 로컬 사용자, 유지 관리 사용자 및 데이터베이스 사용자에 대한 암호를 제공해야 합니다.

HTTP 동사	경로	설명
"내려가세요 패치 "삭제"	'/security/users/{name}'	Get 메서드를 사용하면 이름, 전자 메일 주소, 역할, 권한 부여 유형 등 사용자의 모든 세부 정보를 검색할 수 있습니다. 패치 방법을 사용하면 세부 정보를 업데이트할 수 있습니다. 삭제 방법을 사용하면 사용자를 제거할 수 있습니다.

성능 메트릭 보기

Active IQ Unified Manager는 데이터 센터에서 클러스터의 성능 데이터와 스토리지 객체를 볼 수 있도록 하는 '/datacenter' 범주 아래에 API 세트를 제공합니다. 이들 API는 클러스터, 노드, LUN, 볼륨, 애그리게이트, 데이터 저장소, 데이터 저장소, 데이터 저장소, 스토리지 VM, FC 인터페이스, FC 포트, 이더넷 포트 및 IP 인터페이스.

'/metrics' 및 '/analytics' API는 성능 메트릭에 대한 다양한 뷰를 제공하므로 데이터 센터에서 다음과 같은 스토리지 객체에 대한 세부 정보를 다양한 수준으로 드릴다운할 수 있습니다.

- 클러스터
- 노드
- 스토리지 VM
- 애그리게이트
- 볼륨
- LUN을 클릭합니다
- FC 인터페이스
- FC 포트
- 이더넷 포트
- IP 인터페이스

다음 표는 검색된 성능 데이터의 세부 사항을 기준으로 '/metrics'와 '/analytics' API를 비교한 것입니다.

메트릭	분석
단일 객체에 대한 성능 세부 정보입니다. 예를 들어, "/datacenter/cluster/clusters/{key}/metrics" API를 사용하려면 해당 클러스터의 메트릭을 검색하기 위한 경로 매개 변수로 클러스터 키를 입력해야 합니다.	데이터 센터에서 동일한 유형의 여러 객체에 대한 성능 세부 정보입니다. 예를 들어, '/datacenter/cluster/clusters/analytics' API는 데이터 센터에 있는 모든 클러스터의 집합적 메트릭을 검색합니다.
검색할 시간 간격 매개 변수를 기반으로 스토리지 객체에 대한 성능 메트릭 샘플	특정 기간(72시간 이상) 동안 특정 유형의 스토리지 객체에 대한 높은 수준의 누적 성능 값입니다.

메트릭	분석
노드나 클러스터의 세부 정보와 같이 개체의 기본 세부 정보가 검색됩니다.	특정 세부 정보가 검색되지 않습니다.

메트릭	분석
최소, 최대, 95번째 백분위수 및 특정 기간 동안의 평균 성능 값과 같은 누적 카운터는 읽기, 쓰기, 합계 및 기타 카운터 등의 단일 개체에 대해 검색됩니다. 예를 들어, '/datacenter/cluster/nodes/{key}/metrics' API는 노드에 대해 다음과 같은 세부 정보를 검색합니다. 요약 값의 95 백분위수는 해당 기간 동안 수집된 샘플의 95%가 95 백분위수로 지정된 값보다 작은 카운터 값을 가졌음을 나타냅니다.	동일한 형식의 모든 개체에 대해 집계된 단일 값이 표시됩니다. 예를 들어, '/datacenter/cluster/nodes/analytics' API는 모든 노드에 대해 다음 값(다른 값 중)을 검색합니다.

{
"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
	{
	"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": {

메트릭	분석
시간 범위 및 예제 데이터는 데이터의 시간 범위인 다음 일정을 기반으로 합니다. 예: 1h, 12h, 1d, 2D, 3D, 15d, 1W, 1m, 2m, 3m, 6개월 범위가 3일(72시간)을 초과하는 경우 1시간 샘플이 수집되고, 그렇지 않은 경우 5분 샘플이 제공됩니다. 각 시간 범위의 기간은 다음과 같습니다. • 1시간: 5분 동안 샘플링한 최근 시간에 대한 메트릭입니다. • 12h: 5분 동안 샘플링한 최근 12시간 동안의 메트릭입니다. • 1D: 5분 동안 샘플링한 가장 최근 날짜의 메트릭 • 2D: 5분 동안 샘플링한 최근 2일간의 메트릭 • 3D: 5분 동안 가장 최근 3일간 샘플링한 메트릭스. • 15d: 1시간 동안 샘플링한 최근 15일간의 지표. • 1W: 1시간 동안 샘플링한 가장 최근 주에 대한 메트릭입니다. • 1m: 1시간 이상 샘플링한 가장 최근 달의 측정 지표입니다. • 2M: 1시간 동안 샘플링한 최근 2개월 동안의 메트릭 • 3M: 1시간 동안 샘플링한 최근 3개월 동안의 지표. • 6M: 1시간 동안 가장 최근 6개월 동안 샘플링한 수치. 사용 가능한 값: 1h, 12h, 1d, 2D, 3D, 15d, 1W, 1m, 2m, 3m, 6개월 기본값: 1h	72시간 이상. 이 샘플이 계산되는 기간은 ISO-8601 표준 형식으로 표시됩니다.


```
            "min": 5
        }
    },
```


다음 표에는 '/metrics'와 '/analytics' API가 자세히 나와 있습니다.

이러한 API에서 반환되는 IOPS와 성능 메트릭은 100.53과 같이 두 배의 값입니다. 파이프(|)와 와일드카드(*) 문자로 이러한 부동 값 필터링은 지원되지 않습니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/cluster/clusters/{key}/metrics'	이 명령어는 cluster key의 input 매개변수로 지정한 cluster의 성능 데이터(샘플 및 요약)를 조회한다. 클러스터 키 및 UUID, 시간 범위, IOPS, 처리량, 샘플 수와 같은 정보가 반환됩니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/cluster/cluster/analytics'	이 명령어는 데이터 센터의 모든 클러스터에 대한 고성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 집계된 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.
"내려가세요	'/datacenter/cluster/nodes/{key}/metrics'	노드 키의 input 매개 변수로 지정된 노드의 성능 데이터(샘플 및 요약)를 검색합니다. 노드 UUID, 시간 범위, IOPS 요약, 처리량, 지연 시간 및 성능, 수집된 샘플 수, 활용도와 같은 정보가 반환됩니다.
"내려가세요	'/datacenter/cluster/nodes/analytics'	이 명령어는 데이터 센터 내 모든 노드에 대해 높은 수준의 성능 지표를 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 노드 및 클러스터 키와 같은 정보와 집계된 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.
"내려가세요	'/datacenter/storage/aggregate/{key}/metrics'	이 명령어는 aggregate key의 input parameter로 지정된 aggregate에 대한 성능 데이터(sample, summary)를 조회한다. 시간 범위, IOPS 요약, 지연 시간, 처리량 및 성능 용량, 각 카운터에 대해 수집된 샘플 수, 사용된 비율 등의 정보가 반환됩니다.
"내려가세요	'/datacenter/storage/aggregate/analytics'	이 명령어는 데이터 센터의 모든 애그리게이트를 위한 높은 수준의 성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 집계 및 클러스터 키와 같은 정보와 집계 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.
"내려가세요	'/datacenter/storage/LUNs/{key}/metrics' '/datacenter/storage/volumes/{key}/metrics'	LUN 또는 볼륨 키의 입력 매개 변수로 지정한 LUN 또는 파일 공유(볼륨)의 성능 데이터(샘플 및 요약)를 검색합니다. 읽기, 쓰기 및 총 IOPS, 지연 시간, 처리량의 최소, 최대 및 평균에 대한 요약과 같은 정보 각 카운터에 대해 수집된 샘플의 수가 반환됩니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/storage/LUNs/analytics' '/datacenter/storage/volumes/analytics'	이 명령어는 데이터 센터의 모든 LUN 또는 볼륨에 대해 높은 수준의 성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 스토리지 VM 및 클러스터 키와 같은 정보와 집계 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.
"내려가세요	'/datacenter/svm/sSVM/{key}/metrics'	스토리지 VM 키의 입력 매개 변수로 지정한 스토리지 VM의 성능 데이터(샘플 및 요약)를 검색합니다. nvmf, fcp, iscsi, NFS, 처리량 등 지원되는 각 프로토콜을 기반으로 한 IOPS 요약 지연 시간 및 수집된 샘플의 수가 반환됩니다.
"내려가세요	'/datacenter/svm/sSVM/analytics'	이 명령어는 데이터 센터에 있는 모든 스토리지 VM에 대한 높은 수준의 성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 스토리지 VM UUID, 집계된 IOPS, 지연 시간, 처리량 및 수집 기간(시간)과 같은 정보가 반환됩니다.
"내려가세요	'/datacenter/network/ethernet/ports/{key}/metrics'	이 명령어는 Port Key의 INPUT 파라미터로 지정된 특정 Ethernet Port에 대한 성능 메트릭을 조회한다. 지원되는 범위에서 간격(시간 범위)을 제공하면 API는 시간 동안 누적된 카운터(예: 최소값, 최대값 및 평균 성능 값)를 반환합니다.
"내려가세요	'/datacenter/network/ethernet/ports/analytics'	이 명령어는 데이터 센터 환경의 모든 이더넷 포트에 대한 고성능 지표를 조회한다. 클러스터 및 노드 키 및 UUID, 처리량, 수집 기간, 포트의 사용률 등의 정보가 반환됩니다. 포트 키, 사용률, 클러스터 및 노드 이름, UUID 등과 같은 사용 가능한 매개 변수를 사용하여 결과를 필터링할 수 있습니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/network/fc/interface/{key}/metrics'	이 명령어는 interface key의 input parameter로 지정된 특정 network FC interface에 대한 성능 메트릭을 조회한다. 지원되는 범위에서 간격(시간 범위)을 제공하면 API는 시간 동안 누적된 카운터(예: 최소값, 최대값 및 평균 성능 값)를 반환합니다.
"내려가세요	'/datacenter/network/fc/interface/analytics'	이 명령어는 데이터 센터 환경의 모든 이더넷 포트에 대한 고성능 지표를 조회한다. 클러스터 및 FC 인터페이스 키와 UUID, 처리량, IOPS, 지연 시간, 스토리지 VM 등의 정보가 반환됩니다. 클러스터 및 FC 인터페이스 이름 및 UUID, 스토리지 VM, 처리량 등과 같은 사용 가능한 매개 변수를 사용하여 결과를 필터링할 수 있습니다.
"내려가세요	'/datacenter/network/fc/ports/{key}/metrics'	이 명령어는 포트 키의 입력 매개 변수로 지정한 특정 FC 포트의 성능 메트릭을 조회한다. 지원되는 범위에서 간격(시간 범위)을 제공하면 API는 시간 동안 누적된 카운터(예: 최소값, 최대값 및 평균 성능 값)를 반환합니다.
"내려가세요	'/datacenter/network/fc/ports/analytics'	이 명령어는 데이터 센터 환경의 모든 FC 포트에 대한 개략적인 성능 메트릭을 조회한다. 클러스터 및 노드 키 및 UUID, 처리량, 수집 기간, 포트의 사용률 등의 정보가 반환됩니다. 포트 키, 사용률, 클러스터 및 노드 이름, UUID 등과 같은 사용 가능한 매개 변수를 사용하여 결과를 필터링할 수 있습니다.
"내려가세요	'/datacenter/network/ip/interface/{key}/metrics'	이 명령어는 interface key의 input parameter에 의해 지정된 네트워크 IP interface에 대한 성능 메트릭을 조회한다. 지원 범위에서 간격(시간 범위)이 제공된 경우 API는 샘플 수, 누적 카운터, 처리량 및 송수신 패킷 수와 같은 정보를 반환합니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/network/ip/interfaces/analytics'	이 명령어는 데이터 센터 환경의 모든 네트워크 IP 인터페이스에 대한 높은 수준의 성능 지표를 조회한다. 클러스터 및 IP 인터페이스 키와 UUID, 처리량, IOPS, 지연 시간 등의 정보가 반환됩니다. 클러스터 및 IP 인터페이스 이름 및 UUID, IOPS, 지연 시간, 처리량 등과 같은 사용 가능한 매개 변수를 사용하여 결과를 필터링할 수 있습니다.

작업 및 시스템 세부 정보 보기

Management-server 범주에서 jobs API를 사용하여 비동기 작업의 실행 세부 정보를 볼 수 있습니다. '관리 서버' 범주의 '시스템' API를 사용하면 Active IQ Unified Manager 환경에서 인스턴스 세부 정보를 볼 수 있습니다.

작업 보기

Active IQ Unified Manager에서는 리소스를 추가 및 수정하는 등의 작업이 동기 및 비동기 API 호출에 의해 수행됩니다. 비동기 실행을 위해 예약된 호출은 해당 호출에 대해 만들어진 Job 개체에서 추적할 수 있습니다. 각 작업 오브젝트에는 식별을 위한 고유한 키가 있습니다. 각 작업 개체는 작업 진행률을 액세스하고 추적할 수 있도록 작업 개체 URI를 반환합니다. 이 API를 사용하여 각 실행의 세부 정보를 검색할 수 있습니다.

이 API를 사용하면 내역 데이터를 포함하여 데이터 센터의 모든 작업 객체를 쿼리할 수 있습니다. 기본적으로 모든 작업을 쿼리하면 웹 UI 및 API 인터페이스를 통해 트리거된 마지막 20개 작업의 세부 정보가 반환됩니다. 내장된 필터를 사용하여 특정 작업을 봅니다. 작업 키를 사용하여 특정 작업의 세부 정보를 쿼리하고 리소스에 대한 다음 작업 집합을 실행할 수도 있습니다.

범주	**HTTP** 동사	경로	설명
관리 - 서버	가져오기	(/management-server/jobs)	모든 작업의 작업 세부 정보를 반환합니다. 정렬 순서가 없으면 마지막으로 제출한 작업 객체가 맨 위에 반환됩니다.
관리 - 서버	가져오기	'/management-server/jobs/{key}' 해당 작업의 특정 세부 정보를 보려면 작업 오브젝트의 작업 키를 입력합니다.	특정 작업 오브젝트의 세부 정보를 반환합니다.

시스템 세부 정보 보기

'/management-server/system' API를 사용하여 Unified Manager 환경의 인스턴스별 세부 정보를 쿼리할 수 있습니다.

API는 시스템에 설치된 Unified Manager 버전, UUID, 공급업체 이름, 호스트 OS, 이름 등과 같은 제품 및 서비스에 대한 정보를 반환합니다. Unified Manager 인스턴스에서 실행 중인 서비스에 대한 설명 및 상태

범주	**HTTP** 동사	경로	설명
관리 - 서버	가져오기	(/management-server/system)	이 API를 실행하는 데 필요한 입력 매개 변수가 없습니다. 현재 Unified Manager 인스턴스의 시스템 세부 정보가 기본적으로 반환됩니다.

이벤트 및 경고 관리

'관리 서버' 범주의 '이벤트', '경고', '스크립트' API를 사용하면 Active IQ Unified Manager 환경의 알림과 관련된 이벤트, 알림 및 스크립트를 관리할 수 있습니다.

이벤트 보기 및 수정

Unified Manager는 ONTAP에서 Unified Manager가 모니터링 및 관리하는 클러스터에 대해 생성되는 이벤트를 수신합니다. 이러한 API를 사용하면 클러스터에 대해 생성된 이벤트를 보고 해당 이벤트를 확인 및 업데이트할 수 있습니다.

/management-server/events' API에 대한 get 메소드를 실행하면 내역 데이터를 포함하여 데이터 센터의 이벤트를 쿼리할 수 있습니다. 이름, 영향 수준, 영향 영역, 심각도, 특정 이벤트를 보려면 상태, 리소스 이름 및 리소스 유형 을 참조하십시오. 리소스 유형 및 영역 매개 변수는 이벤트가 발생한 스토리지 객체에 대한 정보를 반환하고 영향 영역은 가용성, 용량, 구성, 보안 등과 같이 이벤트가 발생한 문제에 대한 정보를 반환합니다. 성능과 보호 기능을 모두 제공합니다.

이 API에 대한 패치 작업을 실행하여 이벤트에 대한 해결 워크플로우를 활성화할 수 있습니다. 본인 또는 다른 사용자에게 이벤트를 할당하고 이벤트 수신을 확인할 수 있습니다. 리소스에 대한 단계를 수행하여 이벤트를 트리거한 문제를 해결할 때 이 API를 사용하여 이벤트를 Resolved로 표시할 수 있습니다.

이벤트에 대한 자세한 내용은 를 참조하십시오 "이벤트 관리"

범주	**HTTP** 동사	경로	설명
관리 - 서버	가져오기	'/management-server/events'/management-server/events/{key}'	모두 가져오기 메서드를 실행할 때 응답 본문은 데이터 센터의 모든 이벤트에 대한 이벤트 세부 정보로 구성됩니다. 특정 키로 이벤트 세부 정보를 검색할 때 특정 이벤트의 세부 정보를 보고 리소스에 대한 다음 작업 집합을 실행할 수 있습니다. 응답 본문은 해당 이벤트의 세부 정보로 구성됩니다.

범주	**HTTP** 동사	경로	설명
관리 - 서버	패치	'Management-server/events/{key}'	이 API를 실행하여 이벤트를 할당하거나 상태를 확인됨 또는 해결됨 으로 변경합니다. 또한 이 메서드를 사용하여 사용자나 다른 사용자에게 이벤트를 할당할 수도 있습니다. 동기식 작업입니다.

알림 관리

이벤트는 자동으로 연속적으로 생성됩니다. Unified Manager는 이벤트가 특정 필터 조건을 충족할 경우에만 알림을 생성합니다. 알림을 생성할 이벤트를 선택할 수 있습니다. '/management-server/alerts' API를 사용하면 특정 심각도 유형의 특정 이벤트 또는 이벤트가 발생할 때 알림을 자동으로 보내도록 알림을 구성할 수 있습니다.

알림에 대한 자세한 내용은 을 참조하십시오 "알림 관리"

범주	**HTTP** 동사	경로	설명
관리 - 서버	가져오기	'/management-server/alerts"/management-server/alerts/{key}'	경고 키를 사용하여 사용자 환경 또는 특정 알림에 있는 기존 경고를 모두 쿼리합니다. 알림 설명, 작업, 알림을 보낼 e-메일 ID, 이벤트, 심각도 등 사용자 환경에서 생성된 알림에 대한 정보를 볼 수 있습니다.
관리 - 서버	게시	'/management-server/alerts'	이 방법을 사용하면 특정 이벤트에 대한 알림을 추가할 수 있습니다. 경고 이름, 물리적 또는 논리적 리소스 또는 경고를 적용할 수 있는 이벤트, 경고가 설정되었는지 여부 및 SNMP 트랩을 발행하는지 여부를 추가해야 합니다. 알림 스크립트를 추가하는 경우 작업, 알림 이메일 ID, 스크립트 세부 정보 등과 같이 알림을 생성할 추가 세부 정보를 추가할 수 있습니다.

범주	**HTTP** 동사	경로	설명
관리 - 서버	패치 및 삭제	'Management-server/events/{key}'	이러한 방법을 사용하여 특정 경고를 수정 및 삭제할 수 있습니다. 설명, 이름, 알림 설정 및 해제 등 다양한 속성을 수정할 수 있습니다. 알림이 더 이상 필요하지 않은 경우 알림을 삭제할 수 있습니다.

알림을 추가할 리소스를 선택할 때는 클러스터를 리소스로 선택해도 해당 클러스터 내의 스토리지 객체가 자동으로 선택되지는 않습니다. 예를 들어, 모든 클러스터에 대한 모든 중요 이벤트에 대한 알림을 생성하는 경우 클러스터 중요 이벤트에 대한 알림만 받게 됩니다. 노드, 애그리게이트 등의 중요 이벤트에 대한 알림을 받지 못합니다.

스크립트 관리

'/management-server/scripts' API를 사용하면 경고가 트리거될 때 실행되는 스크립트와 알림을 연결할 수도 있습니다. 스크립트를 사용하여 Unified Manager에서 여러 스토리지 오브젝트를 자동으로 수정 또는 업데이트할 수 있습니다. 스크립트가 경고와 연결되어 있습니다. 이벤트가 경고를 트리거하면 스크립트가 실행됩니다. 사용자 지정 스크립트를 업로드하고 경고가 생성될 때 해당 스크립트를 테스트할 수 있습니다. 알림을 스크립트에 연결하여 Unified Manager의 이벤트에 대한 알림이 발생할 때 스크립트가 실행되도록 할 수 있습니다.

스크립트에 대한 자세한 내용은 을 참조하십시오 "스크립트 관리"

범주	**HTTP** 동사	경로	설명
관리 - 서버	가져오기	'/management-server/scripts'	이 API를 사용하여 사용자 환경의 모든 기존 스크립트를 쿼리합니다. 특정 스크립트만 보려면 표준 필터 및 작업별 순서를 사용합니다.
관리 - 서버	게시	'/management-server/scripts'	이 API를 사용하여 스크립트에 대한 설명을 추가하고 경고와 관련된 스크립트 파일을 업로드합니다.

워크로드 관리

여기에 설명된 API는 스토리지 워크로드 보기, LUN 및 파일 공유 생성, 성능 서비스 수준 및 스토리지 효율성 정책 관리, 스토리지 작업 부하에 대한 정책 할당 등 스토리지 관리의 다양한 기능에 대해 다룹니다.

스토리지 워크로드 보기

여기에 나열된 API를 사용하여 데이터 센터의 모든 ONTAP 클러스터에 대한 스토리지 워크로드 통합 목록을 볼 수 있습니다. 또한, API는 Active IQ Unified Manager 환경에 프로비저닝된 스토리지 워크로드 수와 해당 용량 및 성능(IOPS) 통계를 간략하게 보여줍니다.

스토리지 워크로드를 봅니다

다음 방법을 사용하여 데이터 센터의 모든 클러스터에서 모든 스토리지 워크로드를 볼 수 있습니다. 특정 열을 기준으로 응답을 필터링하는 방법에 대한 자세한 내용은 Unified Manager 인스턴스에서 사용할 수 있는 API 참조 설명서를 참조하십시오.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/워크로드'

스토리지 워크로드 요약 보기

다음 방법을 사용하여 각 성능 서비스 수준에서 관리되는 사용된 용량, 사용 가능한 용량, 사용된 IOPS, 사용 가능한 IOPS 및 스토리지 워크로드 수를 평가할 수 있습니다. 표시된 스토리지 워크로드는 모든 LUN, NFS 파일 공유 또는 CIFS 공유에 대해 수행할 수 있습니다. 이 API는 스토리지 워크로드 개요, Unified Manager에서 프로비저닝한 스토리지 워크로드 개요, 데이터 센터 개요, 할당된 성능 서비스 수준과 관련하여 데이터 센터의 총 공간, 사용된 공간 및 사용 가능한 공간 및 IOPS를 제공합니다. 이 API에 대한 응답으로 받은 정보는 Unified Manager UI에서 대시보드를 채우는 데 사용됩니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/워크로드 -summary'

액세스 엔드포인트 관리

SVM(Storage Virtual Machine), LUN 및 파일 공유를 프로비저닝하는 데 필요한 액세스 엔드포인트 또는 논리 인터페이스(LIF)를 생성해야 합니다. Active IQ Unified Manager 환경에서 SVM, LUN 또는 파일 공유에 대한 액세스 엔드포인트를 확인, 생성, 수정 및 삭제할 수 있습니다.

액세스 끝점을 봅니다

다음 방법을 사용하여 Unified Manager 환경의 액세스 끝점 목록을 볼 수 있습니다. 특정 SVM, LUN 또는 파일 공유의 액세스 끝점 목록을 쿼리하려면 SVM, LUN 또는 파일 공유에 대한 고유 식별자를 입력해야 합니다. 고유한 액세스 끝점 키를 입력하여 특정 액세스 끝점의 세부 정보를 검색할 수도 있습니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/access-endpoints' '/storage-provider/access-endpoints/{key}'

액세스 끝점을 추가합니다

사용자 정의 액세스 끝점을 만들고 필요한 속성을 할당할 수 있습니다. 입력 매개 변수로 생성하려는 액세스 끝점의 세부 정보를 입력해야 합니다. 이 API 또는 System Manager 또는 ONTAP CLI를 사용하여 각 노드에 액세스 엔드포인트를 생성할 수 있습니다. IPv4 및 IPv6 주소가 모두 액세스 엔드포인트 생성에 지원됩니다.

LUN 및 파일 공유를 성공적으로 프로비저닝하려면 노드당 최소 액세스 엔드포인트 수로 SVM을 구성해야 합니다. 노드당 두 개 이상의 액세스 엔드포인트, CIFS 및/또는 NFS 프로토콜을 지원하는 프로토콜, iSCSI 또는 FCP 프로토콜을 사용하여 SVM을 구성해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/storage-provider/access-endpoints'

액세스 끝점을 삭제합니다

다음 방법을 사용하여 특정 액세스 끝점을 삭제할 수 있습니다. 액세스 끝점 키를 입력 매개 변수로 제공하여 특정 액세스 끝점을 삭제해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	삭제	'/storage-provider/access-endpoints/{key}'

액세스 끝점을 수정합니다

다음 메서드를 사용하여 액세스 끝점을 수정하고 해당 속성을 업데이트할 수 있습니다. 특정 액세스 끝점을 수정하려면 액세스 끝점 키를 제공해야 합니다. 또한 업데이트할 속성과 해당 값을 입력해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	패치	'/storage-provider/access-endpoints/{key}'

Active Directory 매핑 관리

여기에 나열된 API를 사용하여 SVM에서 CIFS 공유를 프로비저닝하는 데 필요한 SVM에서 Active Directory 매핑을 관리할 수 있습니다. SVM을 ONTAP에 매핑하기 위해 Active Directory 매핑을 구성해야 합니다.

Active Directory 매핑을 봅니다

다음 방법을 사용하여 SVM에 대한 Active Directory 매핑의 구성 세부 정보를 볼 수 있습니다. SVM에서 Active Directory 매핑을 보려면 SVM 키를 입력해야 합니다. 특정 매핑의 세부 정보를 쿼리하려면 매핑 키를 입력해야 합니다.

범주	HTTP 동사	경로
제공합니다	가져오기	'/storage-provider/active-directories-mappings' '/storage-provider/active-directories-mappings/{key}'

Active Directory 매핑을 추가합니다

다음 방법을 사용하여 SVM에 Active Directory 매핑을 생성할 수 있습니다. 입력 매개 변수로 매핑 세부 정보를 입력해야 합니다.

범주	HTTP 동사	경로
제공합니다	게시	'/storage-provider/active-directories-mappings'

파일 공유 관리

데이터 센터 환경에서 '/storage-provider/file-share' API를 사용하여 CIFS 및 NFS 파일 공유 볼륨을 확인, 추가, 수정 및 삭제할 수 있습니다.

파일 공유 볼륨을 프로비저닝하기 전에 SVM이 지원 프로토콜을 통해 생성되고 프로비저닝되었는지 확인합니다. 프로비저닝 중에 PSL(Performance Service Levels) 또는 CDP(Storage Efficiency Policies)를 할당하는 경우 파일 공유를 생성하기 전에 PSL 또는 SRP를 생성해야 합니다.

파일 공유를 봅니다

다음 방법을 사용하여 Unified Manager 환경에서 사용 가능한 파일 공유 볼륨을 볼 수 있습니다. ONTAP 클러스터를 Active IQ Unified Manager의 데이터 소스로 추가하면 해당 클러스터의 스토리지 워크로드가 Unified Manager 인스턴스에 자동으로 추가됩니다. 이 API는 자동으로 파일 공유를 검색하고 Unified Manager 인스턴스에 수동으로 추가합니다. 이 API를 파일 공유 키로 실행하여 특정 파일 공유의 세부 정보를 볼 수 있습니다.

범주	HTTP 동사	경로
제공합니다	가져오기	'/storage-provider/file-공유' '/storage-provider/file-공유/{key}'

파일 공유를 추가합니다

다음 방법을 사용하여 SVM에 CIFS 및 NFS 파일 공유를 추가할 수 있습니다. 만들려는 파일 공유의 세부 정보를 입력 매개 변수로 입력해야 합니다. FlexGroup 볼륨을 추가하는 데 이 API를 사용할 수 없습니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/storage-provider/file-공유'

ACL(액세스 제어 목록) 매개 변수 또는 엑스포트 정책 매개 변수의 제공 여부에 따라 CIFS 공유 또는 NFS 파일 공유가 생성됩니다. ACL 매개 변수의 값을 제공하지 않으면 CIFS 공유가 생성되지 않고 기본적으로 NFS 공유가 생성되므로 모든 에 액세스할 수 있습니다.

- 데이터 보호 볼륨 생성 *: SVM에 파일 공유를 추가하면 기본적으로 마운트된 볼륨 유형은 "RW"(읽기-쓰기)입니다. 데이터 보호(DP) 볼륨을 생성하려면 'type' 매개 변수의 값으로 dp를 지정합니다.

파일 공유를 삭제합니다

다음 방법을 사용하여 특정 파일 공유를 삭제할 수 있습니다. 특정 파일 공유를 삭제하려면 파일 공유 키를 입력 매개 변수로 입력해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	삭제	'/storage-provider/file-공유/{key}'

파일 공유를 수정합니다

다음 메서드를 사용하여 파일 공유를 수정하고 해당 속성을 업데이트할 수 있습니다.

특정 파일 공유를 수정하려면 파일 공유 키를 제공해야 합니다. 또한 업데이트할 속성과 해당 값을 입력해야 합니다.

이 API를 한 번 호출할 때 하나의 속성만 업데이트할 수 있습니다. 여러 업데이트를 하려면 이 API를 여러 번 실행해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	패치	'/storage-provider/file-공유/{key}'

LUN 관리

'/storage-provider/LUNs' API를 사용하여 데이터 센터 환경에서 LUN을 확인, 추가, 수정 및 삭제할 수 있습니다.

LUN을 프로비저닝하기 전에 SVM이 지원되는 프로토콜을 사용하여 생성되고 프로비저닝되었는지 확인합니다. 프로비저닝 중에 PSL(Performance Service Levels) 또는 CDP(Storage Efficiency Policies)를 할당하는 경우 LUN을 생성하기 전에 PSL 또는 SRP를 생성해야 합니다.

LUN을 봅니다

다음 방법을 사용하여 Unified Manager 환경에서 LUN을 볼 수 있습니다. ONTAP 클러스터를 Active IQ Unified Manager의 데이터 소스로 추가하면 해당 클러스터의 스토리지 워크로드가 Unified Manager 인스턴스에 자동으로 추가됩니다. 이 API는 모든 LUN을 자동으로 검색하고 Unified Manager 인스턴스에 수동으로 추가합니다. 이 API를 LUN 키와 함께 실행하여 특정 LUN의 세부 정보를 볼 수 있습니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/LUN' '/storage-provider/LUNs/{key}'

LUN을 추가합니다

다음 방법을 사용하여 SVM에 LUN을 추가할 수 있습니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/스토리지 공급자/LUN'

curl 요청에서 입력에 선택적 매개 변수 volume_name_tag 값을 제공하면 LUN 생성 중에 볼륨의 이름을 지정하는 동안 해당 값이 사용됩니다. 이 태그를 사용하면 볼륨을 쉽게 검색할 수 있습니다. 요청에 볼륨 키를 제공하면 태그 지정이 생략됩니다.

LUN을 삭제합니다

다음 방법을 사용하여 특정 LUN을 삭제할 수 있습니다. 특정 LUN을 삭제하려면 LUN 키를 제공해야 합니다.

ONTAP에서 볼륨을 생성한 다음 해당 볼륨의 Unified Manager를 통해 LUN을 프로비저닝한 경우 이 API를 사용하여 모든 LUN을 삭제하면 볼륨도 ONTAP 클러스터에서 삭제됩니다.

범주	**HTTP** 동사	경로
제공합니다	삭제	'/storage-provider/LUNs/{key}'

LUN을 수정합니다

다음 방법을 사용하여 LUN을 수정하고 해당 속성을 업데이트할 수 있습니다. 특정 LUN을 수정하려면 LUN 키를 제공해야 합니다. 업데이트할 LUN 속성과 해당 값도 입력해야 합니다. 이 API를 사용하여 LUN 어레이를 업데이트하려면 '"API 사용 권장 사항"'의 권장 사항을 검토해야 합니다.

이 API를 한 번 호출할 때 하나의 속성만 업데이트할 수 있습니다. 여러 업데이트를 하려면 이 API를 여러 번 실행해야 합니다.

범주	HTTP 동사	경로
제공합니다	패치	'/storage-provider/LUNs/{key}'

성능 서비스 수준 관리

Active IQ Unified Manager에서 스토리지 공급자 API를 사용하여 성능 서비스 수준을 확인, 생성, 수정 및 삭제할 수 있습니다.

성능 서비스 수준을 봅니다

다음 방법을 사용하여 스토리지 워크로드에 할당할 성능 서비스 수준을 볼 수 있습니다. API는 시스템 정의 및 사용자가 생성한 모든 성능 서비스 수준을 나열하고 모든 성능 서비스 수준의 특성을 검색합니다. 특정 성능 서비스 수준을 쿼리하려면 성능 서비스 수준의 고유 ID를 입력하여 세부 정보를 검색해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/성능 서비스 수준' '/storage-provider/performance-service-levels/{key}'

성능 서비스 수준 추가

시스템 정의 성능 서비스 수준이 스토리지 워크로드의 SLO(서비스 수준 목표)를 충족하지 못하는 경우 다음 방법을 사용하여 맞춤형 성능 서비스 수준을 생성하고 이를 스토리지 워크로드에 할당할 수 있습니다. 생성하려는 성능 서비스 수준에 대한 세부 정보를 입력합니다. IOPS 속성의 경우 유효한 값 범위를 입력해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/스토리지 공급자/성능 서비스 수준'

성능 서비스 수준을 삭제합니다

다음 방법을 사용하여 특정 성능 서비스 수준을 삭제할 수 있습니다. 워크로드에 할당된 경우 또는 사용 가능한 유일한 성능 서비스 레벨인 경우 성능 서비스 레벨을 삭제할 수 없습니다. 특정 성능 서비스 수준을 삭제하려면 입력 매개 변수로 성능 서비스 수준의 고유 ID를 제공해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	삭제	'/storage-provider/performance-service-levels/{key}'

성능 서비스 수준을 수정합니다

다음 메서드를 사용하여 성능 서비스 수준을 수정하고 해당 속성을 업데이트할 수 있습니다. 시스템 정의이거나 워크로드에 할당된 성능 서비스 수준은 수정할 수 없습니다. 특정 성능 서비스 수준을 수정하려면 의 고유 ID를 제공해야 합니다. 또한 업데이트할 IOPS 속성과 유효한 값을 입력해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	패치	'/storage-provider/performance-service-levels/{key}'

성능 서비스 수준에 따라 집계 기능 보기

다음 방법을 사용하여 성능 서비스 수준에 따라 집계 기능을 쿼리할 수 있습니다. 이 API는 데이터 센터에서 사용할 수 있는 애그리게이트 목록을 반환하고 해당 애그리게이트에서 지원되는 성능 서비스 수준과 관련된 기능을 나타냅니다. 볼륨에서 워크로드를 프로비저닝하는 동안 특정 성능 서비스 수준을 지원하는 애그리게이트의 기능을 확인하고 해당

기능을 기준으로 워크로드를 프로비저닝할 수 있습니다. Aggregate를 지정하는 기능은 API를 사용하여 워크로드를 프로비저닝할 때만 사용할 수 있습니다. 이 기능은 Unified Manager 웹 UI에서 사용할 수 없습니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/집계 기능' '/storage-provider/aggregate-capabilities/{key}'

스토리지 효율성 정책 관리

스토리지 공급자 API를 사용하여 스토리지 효율성 정책을 확인, 생성, 수정 및 삭제할 수 있습니다.

다음 사항을 참고하십시오.

- Unified Manager에서 워크로드를 생성하는 동안 스토리지 효율성 정책을 할당할 필요는 없습니다.
- 정책이 할당된 후에는 워크로드에서 스토리지 효율성 정책을 할당 취소할 수 없습니다.
- ONTAP 볼륨에 중복제거 및 압축과 같은 일부 스토리지 설정이 지정된 워크로드의 경우, Unified Manager에서 스토리지 워크로드를 추가할 때 적용할 스토리지 효율성 정책에 지정된 설정으로 해당 설정을 덮어쓸 수 있습니다.

스토리지 효율성 정책을 봅니다

스토리지 워크로드에 할당하기 전에 다음 방법을 사용하여 스토리지 효율성 정책을 볼 수 있습니다. 이 API는 시스템 정의 및 사용자 생성 스토리지 효율성 정책을 모두 나열하고 모든 스토리지 효율성 정책의 특성을 검색합니다. 특정 스토리지 효율성 정책을 쿼리하려면 정책의 고유 ID를 입력하여 세부 정보를 검색해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/스토리지 효율성 - 정책' '/storage-provider/storage-Efficiency-policies/{key}'

스토리지 효율성 정책을 추가합니다

다음 방법을 사용하여 맞춤형 스토리지 효율성 정책을 생성하고 시스템 정의 정책이 스토리지 워크로드의 프로비저닝 요구사항을 충족하지 않는 경우 스토리지 워크로드에 할당할 수 있습니다. 생성할 스토리지 효율성 정책의 세부 정보를 입력 매개 변수로 입력합니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/스토리지 공급자/스토리지 효율성 - 정책'

스토리지 효율성 정책을 삭제합니다

다음 방법을 사용하여 특정 스토리지 효율성 정책을 삭제할 수 있습니다. 스토리지 효율성 정책이 워크로드에 할당되어 있거나 사용 가능한 유일한 스토리지 효율성 정책인 경우에는 스토리지 효율성 정책을 삭제할 수 없습니다. 특정 스토리지 효율성 정책을 삭제하려면 입력 매개 변수로 스토리지 효율성 정책의 고유 ID를 제공해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	삭제	'/storage-provider/storage-Efficiency-policies/{key}'

스토리지 효율성 정책을 수정합니다

다음 방법을 사용하여 스토리지 효율성 정책을 수정하고 해당 속성을 업데이트할 수 있습니다. 시스템 정의이거나 워크로드에 할당된 스토리지 효율성 정책은 수정할 수 없습니다. 특정 스토리지 효율성 정책을 수정하려면 스토리지 효율성 정책의 고유 ID를 제공해야 합니다. 또한 업데이트할 속성과 해당 값을 제공해야 합니다.

범주	**HTTP** 동사	경로
제공합니다	패치	'/storage-provider/storage-Efficiency-policies/{key}'

스토리지 관리를 위한 공통 워크플로우

공통 워크플로우를 통해 클라이언트 애플리케이션 개발자는 클라이언트 애플리케이션이 Active IQ Unified Manager API를 사용하여 일반적인 스토리지 관리 기능을 실행하는 방법의 예를 볼 수 있습니다. 이 섹션에서는 이러한 샘플 워크플로 중 일부를 다룹니다.

워크플로는 일반적으로 사용되는 일부 저장소 관리 사용 사례와 사용할 샘플 코드를 설명합니다. 각 작업은 하나 이상의 API 호출로 구성된 워크플로 프로세스를 사용하여 설명됩니다.

워크플로에 사용되는 **API** 호출 이해

모든 REST API 호출에 대한 세부 정보가 포함된 Unified Manager 인스턴스에서 온라인 설명서 페이지를 볼 수 있습니다. 이 문서에서는 온라인 설명서의 세부 사항을 반복하지 않습니다. 이 문서의 워크플로 샘플에 사용되는 각 API 호출에는 문서 페이지에서 호출을 찾는 데 필요한 정보만 포함됩니다. 특정 API 호출을 찾은 후에는 입력 매개 변수, 출력 형식, HTTP 상태 코드 및 요청 처리 유형을 비롯한 전체 호출 세부 정보를 검토할 수 있습니다.

문서 페이지에서 호출을 쉽게 찾을 수 있도록 워크플로 내의 각 API 호출에 대해 다음 정보가 포함되어 있습니다.

- 범주: API 호출은 문서 페이지에서 기능적으로 관련된 영역이나 범주로 구성됩니다. 특정 API 호출을 찾으려면 페이지 하단으로 스크롤하여 해당 API 범주를 클릭합니다.
- HTTP 동사(호출): HTTP 동사는 리소스에 대해 수행되는 작업을 식별합니다. 각 API 호출은 단일 HTTP 동사를 통해 실행됩니다.
- 경로: 경로는 호출을 수행하는 과정에서 작업이 적용되는 특정 리소스를 결정합니다. 경로 문자열이 핵심 URL에 추가되어 리소스를 식별하는 전체 URL을 구성합니다.

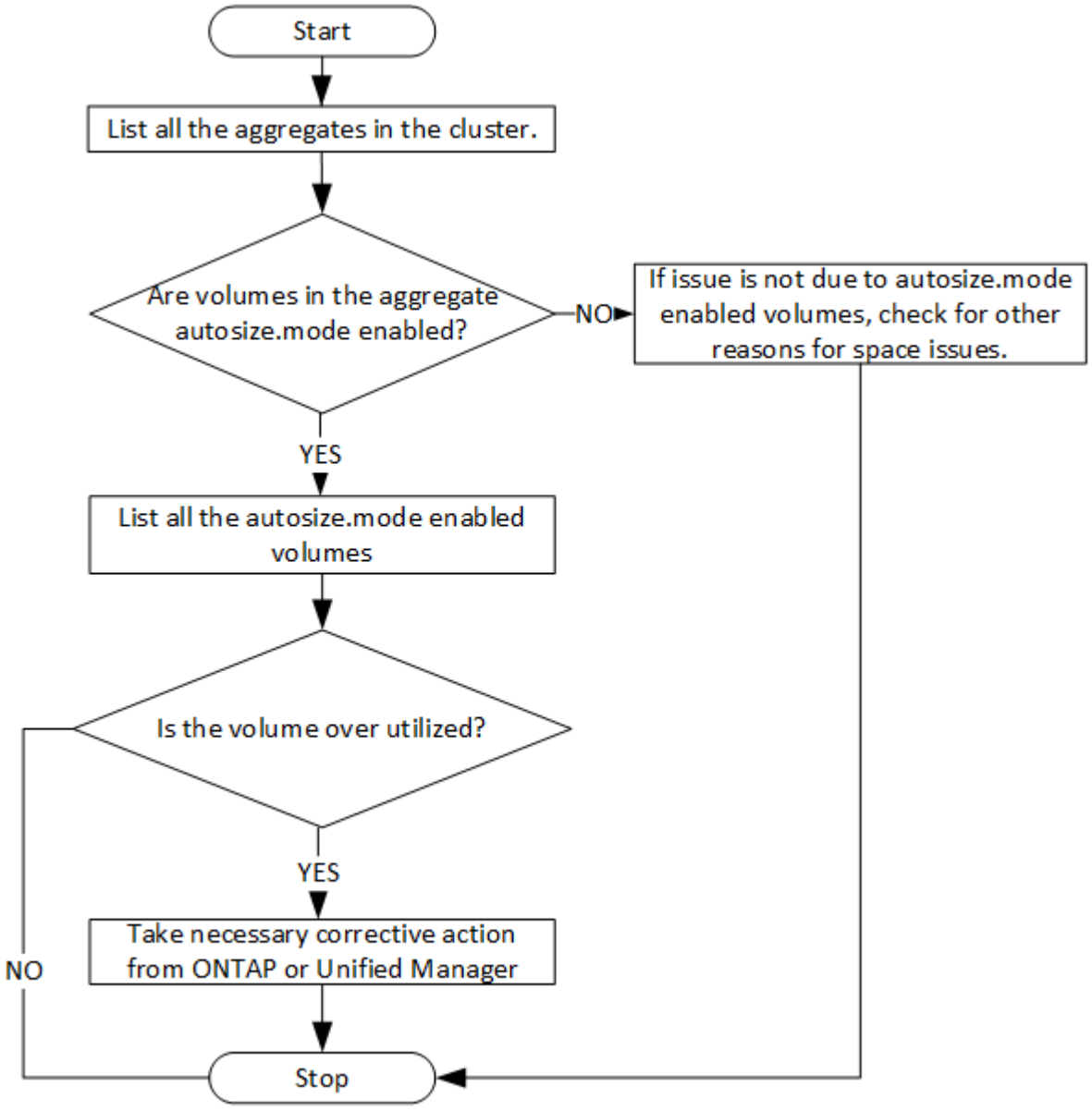
애그리게이트에서 공간 문제를 확인하는 중입니다

Active IQ Unified Manager의 데이터 센터 API를 사용하여 볼륨의 공간 가용성과 활용률을 모니터링할 수 있습니다. 볼륨의 공간 문제를 확인하고 과도하게 활용되거나 제대로 활용되지 않는 스토리지 리소스를 식별할 수 있습니다.

애그리게이트를 위한 데이터 센터 API는 사용 가능한 공간 및 사용된 공간에 대한 관련 정보를 검색하고 공간 절약 효율성 설정을 검색합니다. 또한 지정된 속성을 기반으로 검색된 정보를 필터링할 수 있습니다.

자동 크기 조정 모드를 사용하는 환경에 볼륨이 있는지 여부를 확인하는 한 가지 방법은 Aggregate의 공간 부족을 확인하는 것입니다. 그런 다음 과도하게 사용되는 볼륨을 식별하고 수정 조치를 수행해야 합니다.

다음 순서도는 자동 크기 조정 모드가 활성화된 볼륨에 대한 정보를 검색하는 프로세스를 보여 줍니다.



이 플로우에서는 클러스터가 ONTAP에서 이미 생성되어 Unified Manager에 추가되었다고 가정합니다.

1. 값을 모르는 경우 클러스터 키를 얻습니다.

범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/cluster/cluster'

2. 클러스터 키를 필터 매개 변수로 사용하여 해당 클러스터의 애그리게이트를 쿼리합니다.

범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/storage/aggregate'

3. 응답에서 애그리게이트의 공간 사용을 분석하고 공간 문제가 있는 애그리게이트를 결정합니다. 공간 문제가 있는 각 애그리게이트의 경우 동일한 JSON 출력에서 애그리게이트 키를 가져옵니다.
4. 각 집계 키를 사용하여 AutoSize.mode 매개 변수의 값이 있는 모든 볼륨을 'grow'로 필터링합니다

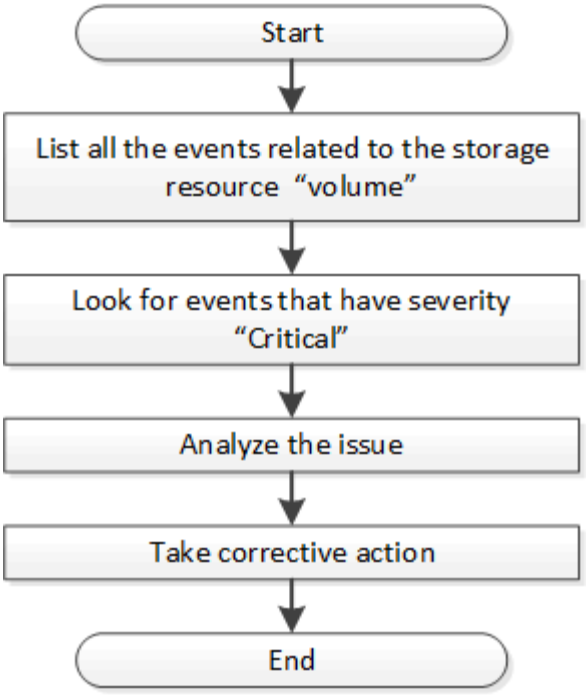
범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/storage/volumes'

5. 과도하게 사용되고 있는 볼륨을 분석합니다.
6. Aggregate 간에 볼륨을 이동하는 것과 같은 필요한 수정 조치를 수행하여 볼륨의 공간 문제를 해결할 수 있습니다. ONTAP 또는 Unified Manager 웹 UI에서 이러한 작업을 수행할 수 있습니다.

이벤트를 사용하여 스토리지 개체의 문제 확인

데이터 센터의 스토리지 객체가 임계값을 넘어가면 해당 이벤트에 대한 알림을 받습니다. 이 알림을 통해 문제를 분석하고 "이벤트" API를 사용하여 수정 조치를 취할 수 있습니다.

이 워크플로우에서는 볼륨의 예를 리소스 객체로 사용합니다. '이벤트' API를 사용하여 볼륨과 관련된 이벤트 목록을 검색하고 해당 볼륨에 대한 중요 문제를 분석한 다음 수정 조치를 수행하여 문제를 해결할 수 있습니다.



개선 단계를 수행하기 전에 볼륨의 문제를 확인하려면 다음 단계를 수행하십시오.

단계

1. 데이터 센터의 볼륨에 대한 중요 Active IQ Unified Manager 이벤트 알림을 분석합니다.
2. /management-server/events API:" * resource_type":"volume *""" * severity":"critical *""에서 다음 매개 변수를 사용하여 볼륨에 대한 모든 이벤트를 쿼리합니다

범주	**HTTP** 동사	경로
관리 - 서버	가져오기	/management - 서버/이벤트입니다

3. 출력을 보고 특정 볼륨의 문제를 분석합니다.
4. Unified Manager REST API 또는 웹 UI를 사용하여 필요한 작업을 수행하여 문제를 해결할 수 있습니다.

게이트웨이 **API**를 사용하여 **ONTAP** 볼륨 문제 해결

게이트웨이 API는 ONTAP API를 호출하여 ONTAP 스토리지 객체에 대한 정보를 쿼리하고 보고된 문제를 해결하기 위한 조치를 취하는 게이트웨이 역할을 합니다.

이 워크플로우에서는 ONTAP 볼륨이 거의 용량에 도달할 때 이벤트가 발생하는 샘플 사용 사례를 따릅니다. 또한 워크플로에서는 Active IQ Unified Manager 및 ONTAP REST API의 조합을 호출하여 이 문제를 해결하는 방법도 보여 줍니다.

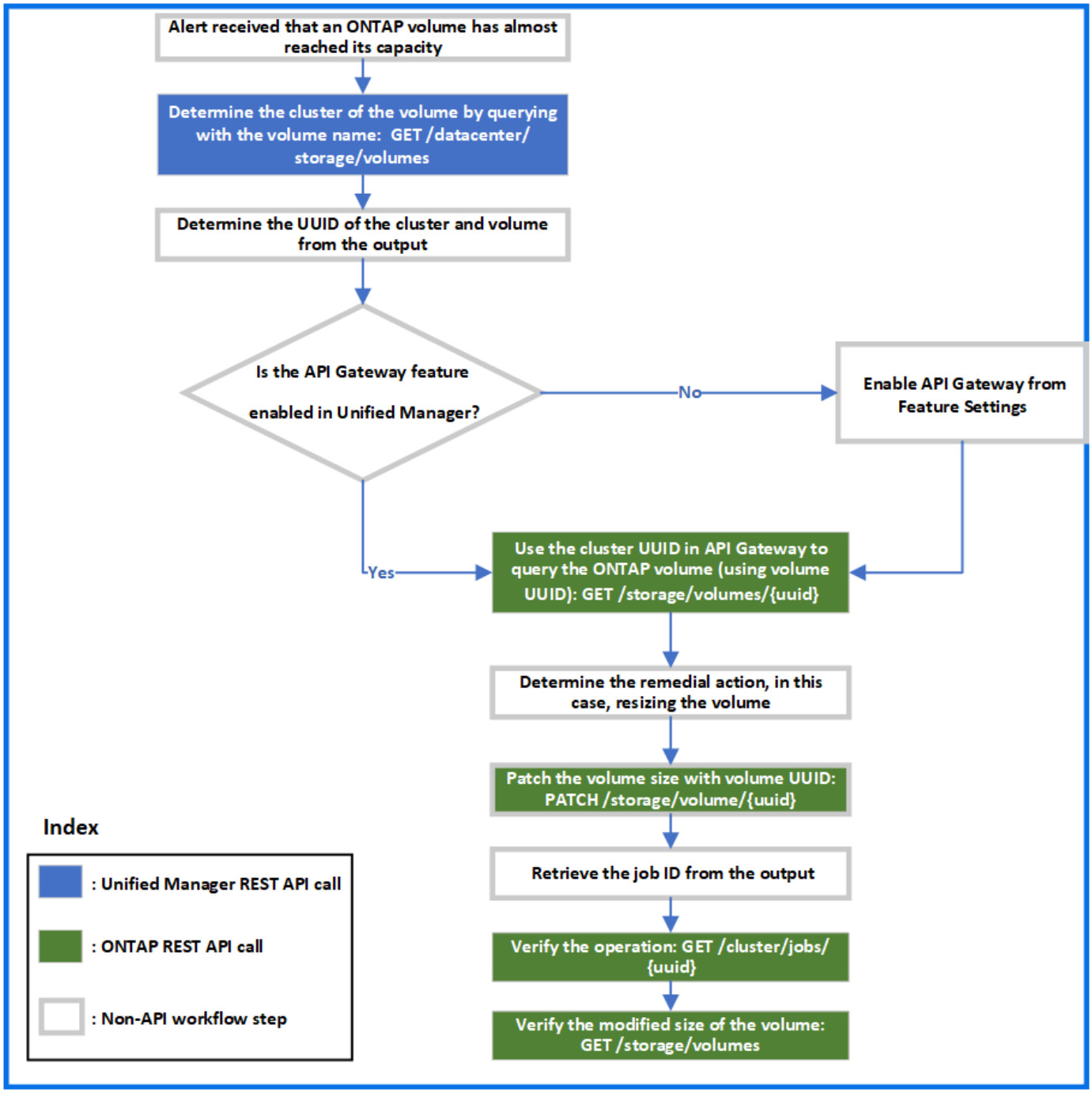
워크플로 단계를 실행하기 전에 다음 사항을 확인하십시오.

- 게이트웨이 API와 게이트웨이 API의 사용 방법을 알고 있습니다. 자세한 내용은 ""게이트웨이 API"" 섹션을 참조하십시오.

  "프록시 액세스를 통해 ONTAP API 액세스"

- ONTAP REST API의 사용에 대해 잘 알고 있습니다. ONTAP REST API 사용에 대한 자세한 내용은 를 참조하십시오https://docs.netapp.com/us-en/ontap-automation/index.html["ONTAP 자동화 문서"].
- 귀하는 애플리케이션 관리자입니다.
- REST API 작업을 실행하려는 클러스터는 ONTAP 9.5 이상에서 지원되며 HTTPS를 통해 Unified Manager에 추가됩니다.

다음 다이어그램은 ONTAP 볼륨 용량 사용 문제를 해결하기 위한 워크플로의 각 단계를 보여줍니다.



워크플로우에서 Unified Manager와 ONTAP REST API의 호출 포인트를 모두 지원합니다.

1. 볼륨 용량 사용률을 알리는 이벤트의 볼륨 이름을 기록합니다.
2. name 매개 변수의 값으로 볼륨 이름을 사용하여 다음 Unified Manager API를 실행하여 볼륨을 쿼리합니다.

범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/storage/volumes'

3. 출력에서 클러스터 UUID 및 볼륨 UUID를 검색합니다.
4. Unified Manager 웹 UI에서 * 일반 * > * 기능 설정 * > * API 게이트웨이 * 로 이동하여 API 게이트웨이 기능이

활성화되었는지 확인합니다. 사용하도록 설정되어 있지 않으면 게이트웨이 범주 아래의 API를 사용하여 를 호출할 수 없습니다. 기능이 비활성화된 경우 활성화합니다.

5. 클러스터 UUID를 사용하여 API 게이트웨이를 통해 ONTAP API/'storage/volumes/{uuid}'를 실행합니다. 이 쿼리는 볼륨 UUID가 API 매개 변수로 전달될 때 볼륨 세부 정보를 반환합니다.

   API 게이트웨이를 통해 ONTAP API를 실행하는 경우, Unified Manager 자격 증명은 인증을 위해 내부적으로 전달되며, 개별 클러스터 액세스를 위한 추가 인증 단계를 실행할 필요가 없습니다.

범주	**HTTP** 동사	경로
Unified Manager: 게이트웨이 ONTAP: 스토리지	가져오기	게이트웨이 API: "/geways/{uuid}/{path}" ONTAP API: "/storage/volumes/{uuuid}"

   /gateways/{uuid}/{path}에서 {uuid}의 값을 REST 작업을 수행할 클러스터 UUID로 바꿔야 합니다. {path}은(는) ONTAP REST URL/storage/volumes/{uuid}로 대체되어야 합니다.

   추가된 URL은 '/geways/{cluster_uuuid}/storage/volumes/{volume_uuuid}'입니다

   GET 작업을 실행할 때 생성된 URL은 'GETtps://<hostname\>/API/게이트웨이/<cluster_UUID\>/storage/volumes/{volume_uuuid}'입니다

   ◦ 샘플 curl 명령 *

```
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. 출력에서 취할 크기, 사용량 및 개선 조치를 결정합니다. 이 워크플로우에서 취한 개선 조치는 볼륨의 크기를 조정하는 것입니다.
7. 클러스터 UUID를 사용하고 API 게이트웨이를 통해 다음 ONTAP API를 실행하여 볼륨의 크기를 조정합니다. 게이트웨이 및 ONTAP API의 입력 매개 변수에 대한 자세한 내용은 5단계를 참조하십시오.

범주	**HTTP** 동사	경로
Unified Manager: 게이트웨이 ONTAP: 스토리지	패치	게이트웨이 API: "/geways/{uuid}/{path}" ONTAP API: "/storage/volumes/{uuuid}"

   클러스터 UUID 및 볼륨 UUID와 함께 볼륨 크기를 조정할 수 있는 크기 매개 변수의 값을 입력해야 합니다. bytes _ 의 값을 입력해야 합니다. 예를 들어, 볼륨 크기를 100GB에서 120GB로 늘리려면 쿼리 끝에 "-d{\"size\":128849018880}""의 매개 변수 크기 값을 입력합니다

◦ 샘플 curl 명령 *

```
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}"
```

+ JSON 출력은 작업 UUID를 반환합니다.

8. 작업 UUID를 사용하여 작업이 성공적으로 실행되었는지 확인합니다. 클러스터 UUID와 작업 UUID를 사용하여 API 게이트웨이를 통해 다음 ONTAP API를 실행할 수 있습니다. 게이트웨이 및 ONTAP API의 입력 매개 변수에 대한 자세한 내용은 5단계를 참조하십시오.

범주	**HTTP** 동사	경로
Unified Manager: 게이트웨이 ONTAP: 클러스터	가져오기	게이트웨이 API: "/geways/{uuid}/{path}" ONTAP API: "/cluster/jobs/{uuid}"

반환되는 HTTP 코드는 ONTAP REST API HTTP 상태 코드와 동일합니다.

9. 다음 ONTAP API를 실행하여 크기 조정된 볼륨의 세부 정보를 쿼리합니다. 게이트웨이 및 ONTAP API의 입력 매개 변수에 대한 자세한 내용은 5단계를 참조하십시오.

범주	**HTTP** 동사	경로
Unified Manager: 게이트웨이 ONTAP: 스토리지	가져오기	게이트웨이 API: "/geways/{uuid}/{path}" ONTAP API: "/storage/volumes/{uuuid}"

출력에는 120GB의 증가된 볼륨 크기가 표시됩니다.

워크로드 관리를 위한 워크플로우

Active IQ Unified Manager를 사용하면 스토리지 워크로드(LUN, NFS 파일 공유, CIFS 공유)를 프로비저닝하고 수정할 수 있습니다. 프로비저닝은 SVM(Storage Virtual Machine) 생성부터 스토리지 워크로드에 성능 서비스 수준 및 스토리지 효율성 정책을 적용하는 단계에 이르기까지 여러 단계로 구성됩니다. 워크로드 수정은 특정 매개 변수를 수정하고 추가 기능을 사용하기 위한 단계로 구성됩니다.

다음 워크플로에 대해 설명합니다.

- Unified Manager에서 SVM(Storage Virtual Machine)을 프로비저닝할 수 있는 워크플로우

Unified Manager에서 LUN 또는 파일 공유를 프로비저닝하기 전에 이 워크플로우를 수행해야 합니다.

- 파일 공유를 프로비저닝 중입니다.
- LUN 프로비저닝
- LUN 및 파일 공유 수정(예: 스토리지 워크로드에 대한 성능 서비스 레벨 매개 변수 업데이트)
- CIFS 프로토콜을 지원하도록 NFS 파일 공유를 수정합니다
- QoS를 AQoS로 업그레이드하기 위해 워크로드 수정

각 프로비저닝 워크플로우(LUN 및 파일 공유)에 대해 클러스터에서 SVM을 확인하기 위한 워크플로우를 완료해야 합니다.

또한 워크플로우에서 각 API를 사용하기 전에 권장 사항 및 제한 사항을 읽어야 합니다. API의 관련 세부 정보는 관련 개념 및 참조에 나열된 각 섹션에서 확인할 수 있습니다.

클러스터에서 **SVM** 확인

파일 공유 또는 LUN을 프로비저닝하기 전에 클러스터에 SVM(Storage Virtual Machine)이 생성되어 있는지 확인해야 합니다.

워크플로우에서 ONTAP 클러스터가 Unified Manager에 추가되었으며 클러스터 키가 있다고 가정합니다. 클러스터에는 LUN 및 파일 공유를 프로비저닝하는 데 필요한 라이센스가 있어야 합니다.

1. 클러스터에 SVM이 생성되었는지 확인합니다.

범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/svm/sSVM'//datacenter/svm/sSVM/{key}'

◦ 샘플 컬 *

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

2. SVM 키가 반환되지 않으면 SVM을 생성합니다. SVM을 생성하려면 SVM을 프로비저닝할 클러스터 키가 필요합니다. SVM 이름을 지정해야 합니다. 다음 단계를 수행합니다.

범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/cluster/cluster''/datacenter/cluster/cluster/{key}'

클러스터 키를 가져옵니다.

◦ 샘플 컬 *

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

3. 출력에서 클러스터 키를 가져온 다음 SVM 생성을 위한 입력으로 사용합니다.

SVM을 생성하는 동안 LUN 및 파일 공유를 프로비저닝하는 데 필요한 프로토콜(예: CIFS, NFS, FCP, 및 iSCSI를 지원합니다. SVM이 필요한 서비스를 지원하지 않으면 프로비저닝 워크플로우가 실패할 수 있습니다. 각 워크로드 유형에 대한 서비스도 SVM에서 활성화하는 것이 좋습니다.

범주	**HTTP** 동사	경로
데이터 센터	게시	'/datacenter/svm/sSVM'

◦ 샘플 컬 *

SVM 객체 세부 정보를 입력 매개 변수로 입력합니다.

```
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\"}"
```

+ JSON 출력에는 생성한 SVM을 확인하는 데 사용할 수 있는 작업 오브젝트 키가 표시됩니다.

4. 쿼리에 작업 오브젝트 키를 사용하여 SVM 생성을 확인합니다. SVM이 성공적으로 생성되면 응답 시 SVM 키가 반환됩니다.

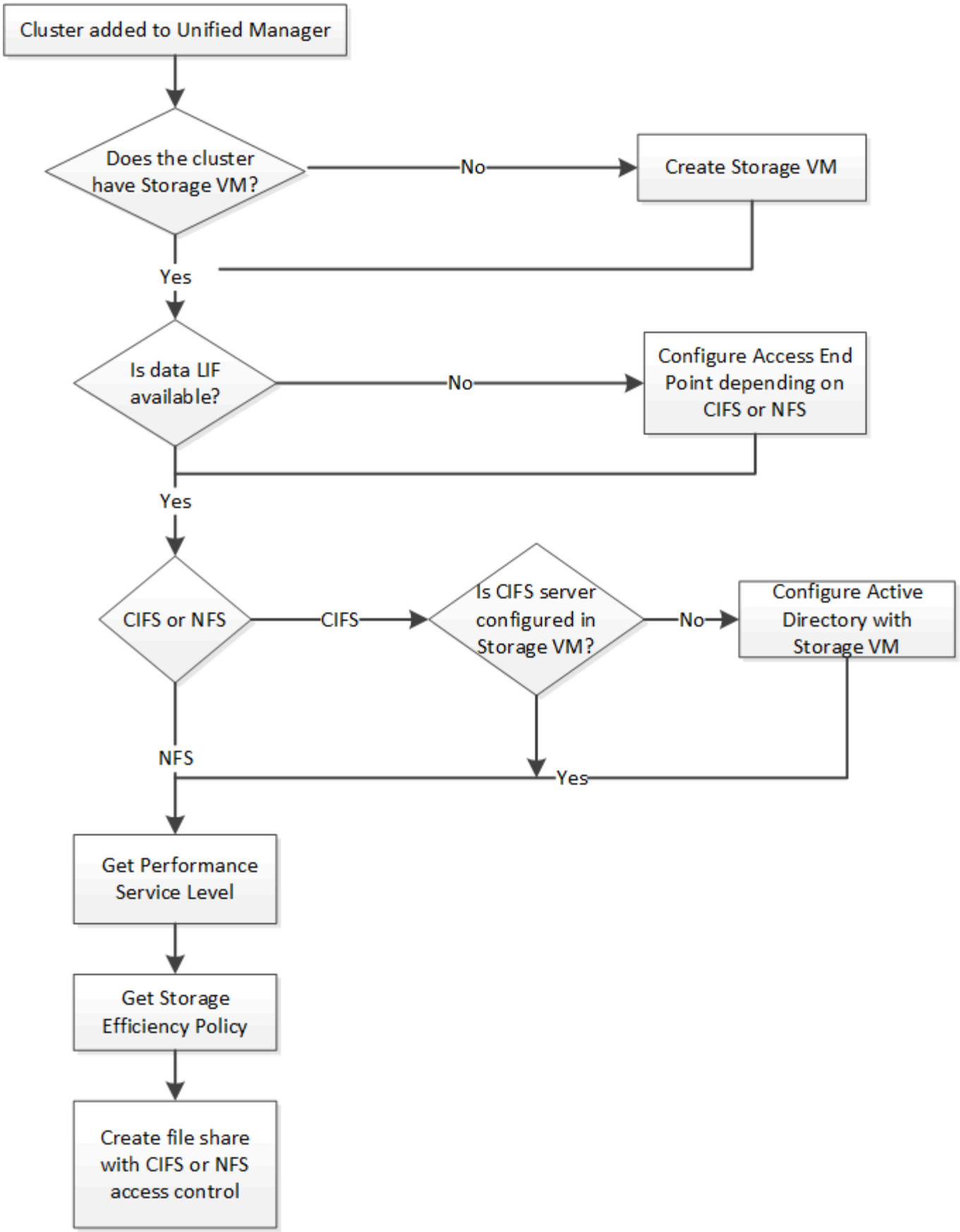
범주	**HTTP** 동사	경로
관리 - 서버	가져오기	'/management-server/jobs/{key}'

CIFS 및 **NFS** 파일 공유를 프로비저닝합니다

Active IQ Unified Manager의 일부로 제공되는 프로비저닝 API를 사용하여 SVM(스토리지 가상 머신)에서 CIFS 공유 및 NFS 파일 공유를 프로비저닝할 수 있습니다. 이 프로비저닝 워크플로에서는 파일 공유를 생성하기 전에 SVM의 키, 성능 서비스 수준 및 스토리지 효율성

정책을 검색하는 단계에 대해 자세히 설명합니다.

다음 다이어그램은 파일 공유 프로비저닝 워크플로우의 각 단계를 보여 줍니다. CIFS 공유와 NFS 파일 공유를 모두 프로비저닝합니다.


Cluster added to Unified Manager
Does the cluster have Storage VM?
No
Create Storage VM
Yes
Is data LIF available?
No
Configure Access End Point depending on CIFS or NFS
Yes
CIFS or NFS
CIFS
Is CIFS server configured in Storage VM?
No
Configure Active Directory with Storage VM
NFS
Yes
Get Performance Service Level
Get Storage Efficiency Policy
Create file share with CIFS or NFS access control

다음을 확인합니다.

- ONTAP 클러스터가 Unified Manager에 추가되고 클러스터 키가 확보되었습니다.
- SVM이 클러스터에 생성되었습니다.
- SVM은 CIFS 및 NFS 서비스를 지원합니다. SVM이 필요한 서비스를 지원하지 않으면 파일 공유 프로비저닝이 실패할 수 있습니다.
- 포트 프로비저닝을 위해 FCP 포트가 온라인 상태입니다.

1. CIFS 공유를 생성하려는 SVM에서 Data LIF 또는 액세스 엔드포인트를 사용할 수 있는지 확인합니다. SVM에서 사용 가능한 액세스 엔드포인트 목록을 확인하십시오.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/access-endpoints'/ 스토리지 -provider/access-endpoints/{key}'

◦ 샘플 컬 *

```
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. 액세스 끝점을 목록에서 사용할 수 있는 경우 액세스 끝점 키를 가져옵니다. 그렇지 않으면 액세스 끝점을 만듭니다.

CIFS 프로토콜이 설정된 액세스 엔드포인트를 생성해야 합니다. CIFS 프로토콜이 설정된 액세스 엔드포인트를 생성하지 않으면 CIFS 공유 프로비저닝이 실패합니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/storage-provider/access-endpoints'

◦ 샘플 컬 *

생성하려는 액세스 끝점의 세부 정보를 입력 매개 변수로 입력해야 합니다.

```
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}"
```

+ JSON 출력에는 사용자가 생성한 액세스 엔드포인트를 확인하는 데 사용할 수 있는 작업 객체 키가 표시됩니다.

3. 액세스 엔드포인트 확인:

범주	**HTTP** 동사	경로
관리 - 서버	가져오기	'/management-server/jobs/{key}'

4. CIFS 공유를 생성해야 하는지 또는 NFS 파일 공유를 생성해야 하는지 확인합니다. CIFS 공유를 생성하려면 다음 하위 단계를 수행하십시오.

   a. SVM에 CIFS 서버가 구성되어 있는지 확인합니다. 그런 다음 Active Directory 매핑이 SVM에 생성되는지 여부를 확인합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/active-directories-mappings'

   b. Active Directory 매핑이 생성된 경우 키를 사용하고, 그렇지 않으면 SVM에서 Active Directory 매핑을 생성합니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/storage-provider/active-directories-mappings'

- 샘플 컬 *

입력 매개 변수로 Active Directory 매핑을 만들기 위한 세부 정보를 입력해야 합니다.

```
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\"}"
```

+ 이 호출은 동기 호출이며 출력에서 Active Directory 매핑이 생성되었는지 확인할 수 있습니다. 오류가 발생하면 문제를 해결하고 요청을 다시 실행할 수 있는 오류 메시지가 표시됩니다.

5. cifs 공유 또는 NFS 파일 공유를 생성하려는 SVM을 위한 SVM 키를 얻습니다. 자세한 내용은 _Verifying SVM on clusters_workflow 항목을 참조하십시오.
6. 다음 API를 실행하고 응답에서 키를 검색하여 성능 서비스 수준의 키를 얻습니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/성능 서비스 수준'

System_Defined 입력 파라미터를 true로 설정하여 시스템 정의 Performance Service 레벨의 세부 정보를 조회할 수 있다. 출력에서 파일 공유에 적용할 성능 서비스 수준의 키를 가져옵니다.

7. 필요한 경우 다음 API를 실행하고 응답에서 키를 검색하여 파일 공유에 적용할 스토리지 효율성 정책에 대한 스토리지 효율성 정책 키를 가져옵니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/스토리지 효율성 - 정책'

8. 파일 공유를 생성합니다. 액세스 제어 목록 및 엑스포트 정책을 지정하여 CIFS와 NFS를 모두 지원하는 파일 공유를 생성할 수 있습니다. 다음 하위 단계는 볼륨에서 프로토콜 중 하나만 지원하기 위해 파일 공유를 생성하려는 경우에 정보를 제공합니다. NFS 공유를 생성한 후 액세스 제어 목록을 포함하도록 NFS 파일 공유를 업데이트할 수도 있습니다. 자세한 내용은 _스토리지 워크로드 수정_항목을 참조하십시오.

   a. CIFS 공유만 생성하려면 ACL(액세스 제어 목록)에 대한 정보를 수집합니다. CIFS 공유를 생성하려면 다음 입력 매개 변수에 유효한 값을 제공하십시오. 할당한 각 사용자 그룹에 대해 CIFS/SMB 공유가 프로비저닝될 때 ACL이 생성됩니다. ACL 및 Active Directory 매핑에 대해 입력한 값에 따라 CIFS 공유가 생성될 때 액세스 제어 및 매핑이 결정됩니다.

      - 예제 값이 있는 curl 명령 *

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

b. NFS 파일 공유만 생성하려면 엑스포트 정책에 대한 정보를 수집합니다. NFS 파일 공유를 생성하려면 다음 입력 매개 변수에 유효한 값을 제공하십시오. 값에 따라 내보내기 정책은 생성될 때 NFS 파일 공유에 첨부됩니다.

NFS 공유를 프로비저닝하는 동안 필요한 모든 값을 제공하여 엑스포트 정책을 생성하거나 엑스포트 정책 키를 제공하고 기존 엑스포트 정책을 재사용할 수 있습니다. 스토리지 VM에 대한 엑스포트 정책을 재사용하려면 엑스포트 정책 키를 추가해야 합니다. 키를 모르는 경우 '/datacenter/protocols/nfs/export-policies' API를 사용하여 내보내기 정책 키를 검색할 수 있습니다. 새 정책을 만들려면 다음 샘플에 표시된 대로 규칙을 입력해야 합니다. 입력한 규칙의 경우 API는 호스트, 스토리지 VM 및 규칙을 일치시켜 기존 엑스포트 정책을 검색합니다. 기존 엑스포트 정책이 있는 경우 사용 그렇지 않으면 새 엑스포트 정책이 생성됩니다.

- 예제 값이 있는 curl 명령 *

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

액세스 제어 목록 및 엑스포트 정책을 구성한 후 CIFS 및 NFS 파일 공유에 대한 필수 입력 매개 변수의 유효한 값을 제공합니다.

스토리지 효율성 정책은 파일 공유를 생성하는 선택적 매개 변수입니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/storage-provider/file-공유'

JSON 출력에는 사용자가 생성한 파일 공유를 확인하는 데 사용할 수 있는 작업 객체 키가 표시됩니다. . 작업 쿼리에 반환된 작업 객체 키를 사용하여 파일 공유 생성을 확인합니다.

범주	**HTTP** 동사	경로
관리 - 서버	가져오기	'/management-server/jobs/{key}'

응답이 끝나면 생성된 파일 공유의 키가 표시됩니다.

```
    ],
    "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. 반환된 키를 사용하여 다음 API를 실행하여 파일 공유가 생성되었는지 확인합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/file-공유/{key}'

◦ JSON 출력 샘플 *

'/storage-provider/file-공유'의 POST 메서드가 내부적으로 각 함수에 필요한 모든 API를 호출하고 객체를 생성하는 것을 알 수 있습니다. 예를 들어 파일 공유에 성능 서비스 수준을 할당하기 위해 '/storage-provider/performance-service-level/' API를 호출합니다.

```
{
    "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,
```

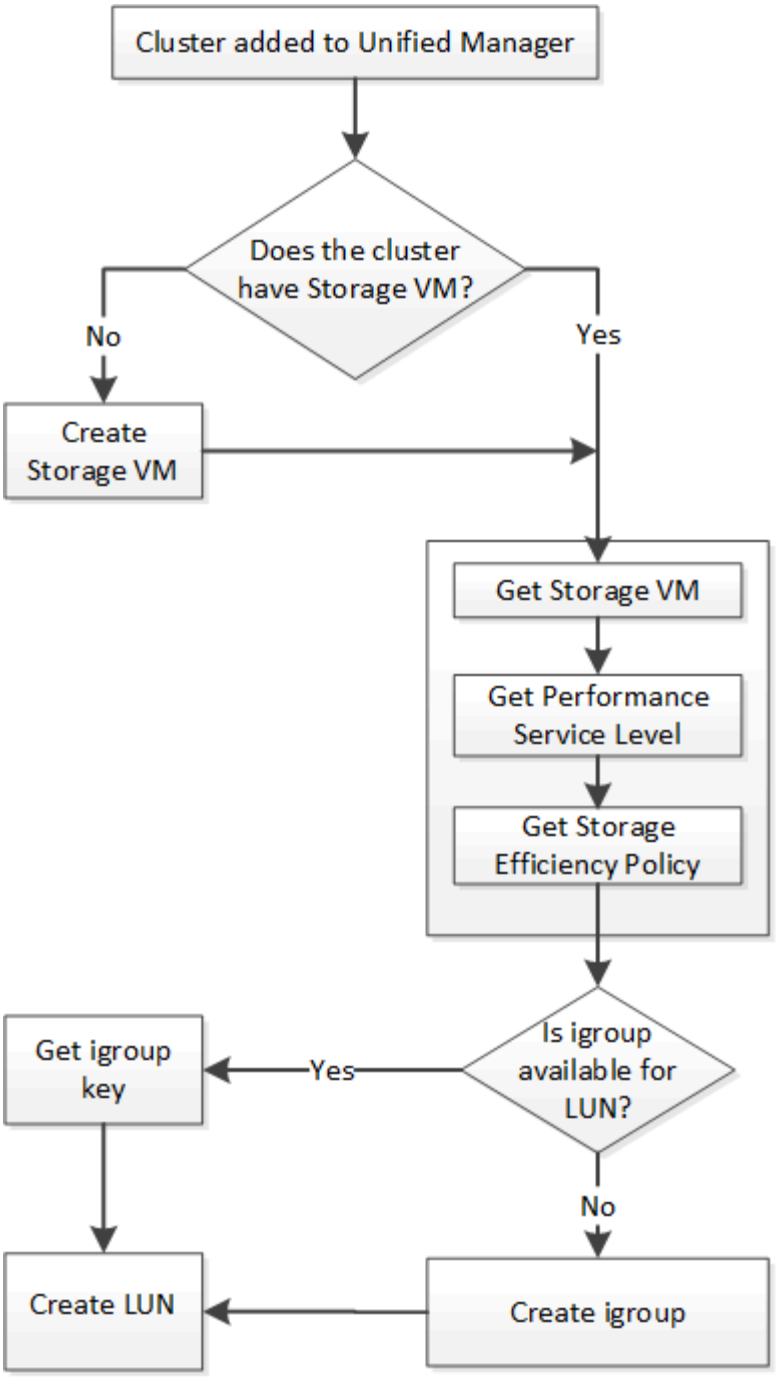
```
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "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"
        }
    }
}
```

LUN 프로비저닝

Active IQ Unified Manager의 일부로 제공되는 프로비저닝 API를 사용하여 SVM(스토리지 가상 머신)에서 LUN을 프로비저닝할 수 있습니다. 이 프로비저닝 워크플로에서는 LUN을 생성하기 전에 SVM의 키, 성능 서비스 수준 및 스토리지 효율성 정책을 검색하는 단계에 대해 자세히 설명합니다.

다음 다이어그램에서는 LUN 프로비저닝 워크플로우의 단계를 보여 줍니다.



이 워크플로우에서는 ONTAP 클러스터가 Unified Manager에 추가되었으며 클러스터 키를 얻었다고 가정합니다. 또한 이 워크플로우에서는 SVM이 클러스터에 이미 생성되어 있다고 가정합니다.

1. lun을 생성할 SVM용 SVM 키를 확인하십시오. 자세한 내용은 _Verifying SVM on clusters_workflow 항목을 참조하십시오.
2. 다음 API를 실행하고 응답에서 키를 검색하여 성능 서비스 수준의 키를 얻습니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/성능 서비스 수준'

System_Defined 입력 파라미터를 true로 설정하여 시스템 정의 Performance Service 레벨의 세부 정보를 조회할 수 있다. 출력에서 LUN에 적용할 성능 서비스 수준의 키를 얻습니다.

3. 필요한 경우 다음 API를 실행하고 응답에서 키를 검색하여 LUN에 적용할 스토리지 효율성 정책에 대한 스토리지 효율성 정책 키를 가져옵니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/스토리지 공급자/스토리지 효율성 - 정책'

4. 생성할 LUN 타겟에 대한 액세스 권한을 부여하기 위해 이니시에이터 그룹(igroup)이 생성되었는지 확인합니다.

범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/protocols/san/igroup'/datacenter/protocols/san/igroup/{key}'

igroup이 액세스를 허가한 SVM을 나타내는 매개 변수 값을 입력해야 합니다. 또한, 특정 igroup을 쿼리하려면 igroup 이름(키)을 입력 매개 변수로 입력합니다.

5. 출력에서 액세스를 허용할 igroup을 찾은 경우 키를 가져옵니다. 그렇지 않으면 igroup을 생성합니다.

범주	**HTTP** 동사	경로
데이터 센터	게시	'/datacenter/protocols/san/igroup'

입력 매개 변수로 생성하려는 igroup의 세부 정보를 입력해야 합니다. 이는 동기식 호출이며 출력에서 igroup 작성을 확인할 수 있습니다. 오류가 발생하면 API 문제를 해결하고 다시 실행할 수 있는 메시지가 표시됩니다.

6. LUN을 생성합니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/스토리지 공급자/LUN'

LUN을 생성하려면 검색된 값을 필수 입력 매개 변수로 추가해야 합니다.

스토리지 효율성 정책은 LUN 생성을 위한 선택적 매개 변수입니다.

◦ 샘플 컬 *

입력 매개 변수로 생성할 LUN의 모든 세부 정보를 입력해야 합니다.

웜뱃: 추출 #1

JSON 출력에는 생성한 LUN을 확인하는 데 사용할 수 있는 작업 오브젝트 키가 표시됩니다.

7. 작업 쿼리에 반환된 작업 객체 키를 사용하여 LUN 생성을 확인합니다.

범주	**HTTP** 동사	경로
관리 - 서버	가져오기	'/management-server/jobs/{key}'

응답이 끝나면 생성된 LUN의 키가 표시됩니다.

웜뱃: 추출 #2

8. 반환된 키를 사용하여 다음 API를 실행하여 LUN이 생성되었는지 확인합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/LUNs/{key}'

◦ JSON 출력 샘플 *

'/storage-provider/LUNs'의 POST 메서드가 내부적으로 각 함수에 필요한 모든 API를 호출하고 객체를 생성하는 것을 알 수 있습니다. 예를 들어 LUN에 성능 서비스 수준을 할당하기 위해 '/storage-provider/performance-service-level/' API를 호출합니다.

웜뱃: 추출 #3

LUN 생성 또는 매핑에서 장애가 발생한 경우 문제 해결 단계

이 워크플로우를 완료해도 LUN 생성에 장애가 발생할 수 있습니다. LUN을 성공적으로 생성하더라도 LUN을 생성하는 노드에서 SAN LIF 또는 액세스 엔드포인트를 사용할 수 없기 때문에 igroup 기반 LUN 매핑에서 실패할 수 있습니다. 오류가 발생한 경우 다음 메시지가 표시됩니다.

```
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.
```

이 문제를 해결하려면 다음 문제 해결 단계를 수행하십시오.

1. LUN을 생성하려는 SVM에서 iSCSI/FCP 프로토콜을 지원하는 액세스 엔드포인트를 생성합니다.

범주	**HTTP** 동사	경로
제공합니다	게시	'/storage-provider/access-endpoints'

◦ 샘플 컬 *

입력 매개 변수로 만들려는 액세스 끝점의 세부 정보를 입력해야 합니다.

input 매개 변수에서 LUN의 홈 노드를 나타내는 주소를 추가했으며 홈 노드의 파트너 노드를 나타내는 ha_address를 추가했는지 확인합니다. 이 작업을 실행하면 홈 노드와 파트너 노드 모두에 액세스 끝점이 생성됩니다.

+ 웜뱃: Extract #4

2. JSON 출력에서 반환된 Job 객체 키를 사용하여 작업을 쿼리하여 SVM에서 액세스 엔드포인트를 추가하고 SVM에서 iSCSI/FCP 서비스가 활성화되었는지 확인합니다.

범주	**HTTP** 동사	경로
관리 - 서버	가져오기	'/management-server/jobs/{key}'

◦ JSON 출력 샘플 *

출력 끝에 생성된 액세스 끝점의 키를 볼 수 있습니다. 다음 출력에서 "name":"accessEndpointKey" 값은 키가 9c964258-14ef-11ea-95e2-00a098e32c28인 LUN의 홈 노드에 생성된 액세스 끝점을 나타냅니다. "name":"accessEndpointHAKey" 값은 키가 9d347006-14ef-11ea-8760-00a098e3215f인 홈 노드의 파트너 노드에 생성된 액세스 끝점을 나타냅니다.

웜뱃: Extract #5

3. LUN을 수정하여 igroup 매핑을 업데이트합니다. 워크플로우 수정에 대한 자세한 내용은 ""스토리지 워크로드 수정""을 참조하십시오.

범주	**HTTP** 동사	경로
제공합니다	패치	'/storage-provider/lun/{key}'

입력에서 LUN 매핑을 업데이트할 igroup 키를 LUN 키와 함께 지정합니다.

◦ 샘플 컬 *

웜뱃: Extract #6

JSON 출력에는 매핑이 성공했는지 확인하는 데 사용할 수 있는 작업 오브젝트 키가 표시됩니다.

4. LUN 키를 사용하여 쿼리하여 LUN 매핑을 확인합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/LUNs/{key}'

◦ JSON 출력 샘플 *

출력에서 LUN이 처음에 프로비저닝한 igroup(키 d19ec2fa-fatec7-11e8-b23d-00a098e32c28)과 성공적으로 매핑되었음을 확인할 수 있습니다.

웜뱃: Extract #7

스토리지 워크로드 수정은 누락된 매개 변수를 사용하여 LUN 또는 파일 공유를 업데이트하거나 기존 매개 변수를 변경하는 작업으로 구성됩니다.

이 워크플로우에서는 LUN 및 파일 공유에 대한 성능 서비스 수준을 업데이트하는 예제를 제공합니다.

워크플로우에서는 LUN 또는 파일 공유가 성능 서비스 수준으로 프로비저닝되었다고 가정합니다.

파일 공유를 수정하는 중입니다

파일 공유를 수정하는 동안 다음 매개 변수를 업데이트할 수 있습니다.

- 용량 또는 크기입니다.
- 온라인 또는 오프라인 설정.
- 스토리지 효율성 정책:
- 성능 서비스 수준.
- ACL(액세스 제어 목록) 설정
- 정책 설정을 내보냅니다. 또한 내보내기 정책 매개 변수를 삭제하고 파일 공유에서 기본(비어 있음) 엑스포트 정책 규칙을 되돌릴 수도 있습니다.

단일 API를 실행하는 동안 매개 변수를 하나만 업데이트할 수 있습니다.

이 절차에서는 파일 공유에 성능 서비스 수준을 추가하는 방법에 대해 설명합니다. 다른 파일 공유 속성을 업데이트하는 경우에도 동일한 절차를 사용할 수 있습니다.

1. 업데이트할 파일 공유의 CIFS 공유 또는 NFS 파일 공유 키를 가져옵니다. 이 API는 데이터 센터의 모든 파일 공유를 쿼리합니다. 파일 공유 키를 이미 알고 있는 경우 이 단계를 건너뜁니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/file-공유'

2. 가져온 파일 공유 키와 다음 API를 실행하여 파일 공유의 세부 정보를 봅니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/file-공유/{key}'

출력에서 파일 공유의 세부 정보를 봅니다.

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

3. 이 파일 공유에 할당할 성능 서비스 수준의 키를 얻습니다. 현재 할당된 정책이 없습니다.

범주	**HTTP** 동사	경로
성능 서비스 레벨	가져오기	'/스토리지 공급자/성능 서비스 수준'

System_Defined 입력 파라미터를 true로 설정하여 시스템 정의 Performance Service 레벨의 세부 정보를 조회할 수 있다. 출력에서 파일 공유에 적용할 성능 서비스 수준의 키를 가져옵니다.

4. 파일 공유에 성능 서비스 수준을 적용합니다.

범주	**HTTP** 동사	경로
스토리지 공급자	패치	'/storage-provider/file-공유/{key}'

입력에서 업데이트할 매개 변수만 파일 공유 키와 함께 지정해야 합니다. 이 경우 성능 서비스 수준의 핵심입니다.

◦ 샘플 컬 *

```
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\" },
}"
```

+ JSON 출력에는 홈 및 파트너 노드의 액세스 끝점이 성공적으로 생성되었는지 확인하는 데 사용할 수 있는 작업 객체가 표시됩니다.

5. 출력에 표시된 작업 객체 키를 사용하여 성능 서비스 수준이 파일 공유에 추가되었는지 확인합니다.

범주	**HTTP** 동사	경로
관리 서버	가져오기	'/management-server/jobs/{key}'

작업 객체의 ID로 쿼리하면 파일 공유가 성공적으로 업데이트되었는지 여부를 확인할 수 있습니다. 장애가 발생한

경우, 장애 해결 후 API를 다시 실행한다. 성공적으로 생성되면 파일 공유를 쿼리하여 수정된 객체를 확인합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/file-공유/{key}'

출력에서 파일 공유의 세부 정보를 봅니다.

```
"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"
            }
        }
```

LUN을 업데이트하는 중입니다

LUN을 업데이트하는 동안 다음 매개 변수를 수정할 수 있습니다.

- 용량 또는 크기입니다
- 온라인 또는 오프라인 설정
- 스토리지 효율성 정책
- 성능 서비스 수준
- LUN 매핑

단일 API를 실행하는 동안 매개 변수를 하나만 업데이트할 수 있습니다.

이 절차에서는 LUN에 성능 서비스 수준을 추가하는 방법에 대해 설명합니다. 다른 LUN 속성을 업데이트하는 경우에도 동일한 절차를 사용할 수 있습니다.

1. 업데이트할 LUN의 LUN 키를 가져옵니다. 이 API는 데이터 센터의 모든 LUN에 대한 세부 정보를 반환합니다. LUN 키를 이미 알고 있는 경우 이 단계를 건너뜁니다.

범주	**HTTP** 동사	경로
스토리지 공급자	가져오기	'/스토리지 공급자/LUN'

2. 가져온 LUN 키와 함께 다음 API를 실행하여 LUN의 세부 정보를 봅니다.

범주	**HTTP** 동사	경로
스토리지 공급자	가져오기	'/storage-provider/LUNs/{key}'

출력에서 LUN의 세부 정보를 봅니다. 이 LUN에 성능 서비스 수준이 할당되지 않은 것을 확인할 수 있습니다.

◦ JSON 출력 샘플 *

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

3. LUN에 할당할 성능 서비스 수준의 키를 얻습니다.

범주	**HTTP** 동사	경로
성능 서비스 레벨	가져오기	'/스토리지 공급자/성능 서비스 수준'

System_Defined 입력 파라미터를 true로 설정하여 시스템 정의 Performance Service 레벨의 세부 정보를 조회할 수 있다. 출력에서 LUN에 적용할 성능 서비스 수준의 키를 얻습니다.

4. LUN에 성능 서비스 수준을 적용합니다.

범주	**HTTP** 동사	경로
스토리지 공급자	패치	'/storage-provider/lun/{key}'

입력에서 LUN 키와 함께 업데이트할 매개 변수만 지정해야 합니다. 이 경우 성능 서비스 수준의 핵심입니다.

◦ 샘플 컬 *

```
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\" }"
```

+ JSON 출력에는 업데이트된 LUN을 확인하는 데 사용할 수 있는 작업 오브젝트 키가 표시됩니다.

5. 가져온 LUN 키와 함께 다음 API를 실행하여 LUN의 세부 정보를 봅니다.

범주	**HTTP** 동사	경로
스토리지 공급자	가져오기	'/storage-provider/LUNs/{key}'

출력에서 LUN의 세부 정보를 봅니다. 이 LUN에 성능 서비스 수준이 할당된 것을 확인할 수 있습니다.

◦ JSON 출력 샘플 *

```
     "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"
            }
```

CIFS를 지원하도록 **NFS** 파일 공유를 수정합니다

CIFS 프로토콜을 지원하도록 NFS 파일 공유를 수정할 수 있습니다. 파일 공유를 생성하는 동안 동일한 파일 공유에 대한 ACL(액세스 제어 목록) 매개 변수와 엑스포트 정책 규칙을 모두 지정할 수 있습니다. 그러나 NFS 파일 공유를 생성한 볼륨에서 CIFS를 설정하려면 해당 파일 공유에서 CIFS를 지원하도록 ACL 매개 변수를 업데이트할 수 있습니다.

- 필요한 것 *

1. NFS 파일 공유는 엑스포트 정책 세부 정보만 사용하여 생성해야 합니다. 자세한 내용은 _ 파일 공유 관리 _ 및 _ 스토리지 워크로드 수정 _ 을(를) 참조하십시오.
2. 이 작업을 실행하려면 파일 공유 키가 있어야 합니다. 파일 공유 세부 정보를 보고 작업 ID를 사용하여 파일 공유 키를 검색하는 방법에 대한 자세한 내용은 _ CIFS 및 NFS 파일 공유 _ 을(를) 참조하십시오.

이는 ACL 매개 변수가 아닌 엑스포트 정책 규칙만 추가하여 생성한 NFS 파일 공유에 적용할 수 있습니다. ACL 매개 변수를 포함하도록 NFS 파일 공유를 수정합니다.

단계

1. NFS 파일 공유에서 CIFS 액세스를 허용하기 위한 ACL 세부 정보로 '패치' 작업을 수행합니다.

범주	**HTTP** 동사	경로
제공합니다	패치	'/storage-provider/file-공유'

◦ 샘플 컬 *

다음 샘플에 표시된 것처럼 사용자 그룹에 할당한 액세스 권한에 따라 ACL이 생성되고 파일 공유에 할당됩니다.

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

◦ JSON 출력 샘플 *

이 작업은 업데이트를 실행하는 작업의 작업 ID를 반환합니다.

2. 동일한 파일 공유에 대한 파일 공유 세부 정보를 쿼리하여 매개 변수가 올바르게 추가되었는지 확인합니다.

범주	**HTTP** 동사	경로
제공합니다	가져오기	'/storage-provider/file-공유/{key}'

◦ JSON 출력 샘플 *

```
"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"
        }
    }
```

+ 동일한 파일 공유에 대한 내보내기 정책과 함께 할당된 ACL을 볼 수 있습니다.

저작권 정보

Copyright © 2025 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이센스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이센스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이센스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 http://www.netapp.com/TM에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.