



ONTAP 자동화

ONTAP Automation

NetApp
May 24, 2024

목차

ONTAP 자동화	1
ONTAP REST API 및 자동화의 새로운 기능	2
ONTAP 9.15.1	2
ONTAP 9.14.1	2
ONTAP 9.13.1	3
ONTAP 9.12.1	3
ONTAP 9.11.1	4
ONTAP 9.10.1	5
ONTAP 9.9.1	6
ONTAP 9.8	6
ONTAP 9.7	7
ONTAP 9.6	7
시작하십시오	9
ONTAP 자동화 옵션을 이해합니다	9
ONTAP REST API 액세스 방법	10
첫 번째 API 호출입니다	11
NetApp 연구소 리소스	11
ONTAP REST API를 참조하십시오	12
REST 구현 세부 정보	12
RBAC 보안	25
나머지 리소스 요약	31
워크플로우	52
워크플로우 사용을 준비하십시오	52
클러스터	55
NAS	59
네트워킹	69
보안	76
스토리지	90
지원	94
SVM	101
소프트웨어 도구	103
Python 클라이언트 라이브러리	103
PowerShell 툴킷	106
NetApp 관리 SDK	107
ONTAPI에서 REST API로 마이그레이션합니다	108
ONTAPI 비활성화	108
마이그레이션 고려 사항	108
ONTAPI를 REST API 매핑에 매핑	109
성능 카운터	109
툴 및 소프트웨어	132

블로그 기사를 참조하십시오	132
API 참조입니다	134
온라인으로 ONTAP API 참조 문서에 액세스합니다	134
Swagger UI를 통해 ONTAP API 참조 문서에 액세스합니다	134
자세한 정보	136
블로그 기사를 참조하십시오	136
비디오	137
기술 교육 및 이벤트	138
NetApp 기술 자료	138
법적 고지	139
저작권	139
상표	139
특허	139
개인 정보 보호 정책	139

ONTAP 자동화

ONTAP REST API 및 자동화의 새로운 기능

NetApp은 새로운 기능, 개선 사항 및 버그 수정을 제공하기 위해 ONTAP REST API를 정기적으로 업데이트합니다.



또한 를 검토해야 합니다 "[ONTAP 릴리즈 노트](#)" 알려진 제한 사항 또는 문제를 포함한 추가 정보

ONTAP 9.15.1

ONTAP 9.15.1은 ONTAP REST API의 기능을 계속 확장해 나가고 있습니다. 이 릴리스의 업데이트는 새로운 기능을 지원하는 세 개의 새로운 엔드포인트를 통해 비교적 소량입니다.

TLS를 통한 NFS

이 피처에는 세 개의 새 끝점이 있습니다. 이러한 API 호출을 실행하여 TLS 인터페이스를 통한 모든 NFS를 검색하고 UUID로 특정 인터페이스를 검색하고 TLS 인터페이스에 대한 구성 속성을 업데이트할 수 있습니다. 이러한 API 호출은 집합과 동일한 기능을 제공합니다 `vserver nfs tls interface` CLI 명령.



NFS over TLS는 ONTAP 9.15.1에서 공개 미리 보기로 제공됩니다. 미리 보기 오퍼링으로, 이 기능은 ONTAP 9.15.1을 사용하는 운영 워크로드에는 지원되지 않습니다.

ONTAP 9.14.1

ONTAP 9.14.1 릴리즈에는 ONTAP REST API의 기능을 계속 확장하는 24개 이상의 새로운 API 호출이 포함되어 있습니다. 이러한 끝점은 여러 가지 새로운 ONTAP 기능과 기존 기능에 대한 업데이트를 지원합니다. 이 릴리스에서는 주로 보안 개선 사항에 중점을 두지만 NAS, QoS 및 성능 메트릭의 개선 사항이 포함되어 있습니다.

보안

ONTAP 9.14.1에 도입된 두 가지 주요 보안 기능이 있습니다. OAuth 2.0(Open Authorization)은 ONTAP 스토리지 리소스에 대한 액세스를 제한하는 데 사용할 수 있는 토큰 기반 프레임워크입니다. REST API를 통해 ONTAP에 액세스하는 클라이언트와 함께 사용할 수 있습니다. REST API를 포함한 모든 ONTAP 관리 인터페이스를 사용하여 구성을 수행할 수 있습니다. ONTAP 9.14.1 릴리스에는 SSH 로그인에 대한 2단계 인증을 제공하는 Cisco Duo 지원도 포함되어 있습니다. Duo가 ONTAP 클러스터 또는 SVM 레벨에서 작동하도록 구성할 수 있습니다. 이 두 가지 새로운 기능 외에도 키 저장소에 대한 제어를 개선하기 위해 여러 개의 끝점이 추가되었습니다.

FPolicy 영구 스토리지

FPolicy는 ONTAP 정책 관리를 위한 플랫폼을 제공합니다. 이벤트 및 정책 엔진과 같은 다양한 구성 요소나 요소에 대한 컨테이너를 제공합니다. 이제 REST API를 사용하여 ONTAP FPolicy 구성 및 이벤트에 대한 영구 저장소를 구성하고 관리할 수 있습니다. 각 SVM에는 SVM 내 여러 정책에 대해 공유되는 하나의 영구 저장소가 있을 수 있습니다.

QoS 옵션

클러스터에 대한 QoS 옵션을 검색하고 설정할 수 있도록 두 개의 엔드포인트가 도입되었습니다. 예를 들어 백그라운드 작업에 사용 가능한 시스템 처리 리소스의 백분율을 예약할 수 있습니다.

성능 메트릭

ONTAP는 시스템의 작동 특성에 대한 통계 정보를 유지 관리합니다. 이 정보는 테이블과 행으로 구성된 데이터베이스 형식으로 표시됩니다. ONTAP 9.14.1에서는 파이버 채널, iSCSI, LUN, NVMe를 비롯한 여러 리소스

범주에 메트릭 데이터가 추가되었습니다. 이 추가 메트릭 데이터는 ONTAP REST API를 Data ONTAP API(ONTAPI 또는 ZAPI)와 패리티에 더 가깝게 제공합니다.

기타 개선 사항

사용자 환경에 따라 유용한 몇 가지 추가 개선 사항이 있습니다. 이러한 새 엔드포인트는 SAN 이니시에이터에 대한 액세스와 호스트 캐시 설정 제어를 개선하고 개별 AutoSupport 메시지에 대한 액세스를 활성화합니다.

ONTAP 9.13.1

ONTAP 9.13.1 ONTAP REST API의 기능을 20개 이상의 새로운 API 호출로 계속 확장하고 있습니다. 이러한 엔드포인트는 새로운 ONTAP 기능과 기존 기능의 향상된 기능을 지원합니다. 이 릴리즈에서는 보안, 리소스 관리, 향상된 SVM 구성 옵션, 성능 메트릭 등의 개선 사항에 중점을 둡니다.

리소스 태그 지정

태그를 사용하여 REST API 리소스를 그룹화할 수 있습니다. 이렇게 하면 특정 프로젝트 또는 조직 그룹 내의 관련 자원을 연결할 수 있습니다. 태그를 사용하면 리소스를 보다 효율적으로 구성 및 추적할 수 있습니다.

정합성 보장 그룹

ONTAP 9.13.1 성능 카운터 데이터의 가용성을 지속적으로 확장합니다. 이제 이 유형의 통계 정보에 액세스하여 정합성 보장 그룹의 기간별 성능 및 용량을 추적할 수 있습니다. 또한 정합성 보장 그룹 간의 상위-하위 관계를 구성 및 관리할 수 있는 향상된 기능도 포함되어 있습니다.

SVM당 DNS 구성

개별 SVM에 대해 DNS 도메인 및 서버 구성을 수행할 수 있도록 기존 DNS 엔드포인트를 확장하였습니다.

EMS 역할 구성

기존 EMS 지원 기능이 확장되어 역할에 할당된 역할 및 액세스 제어 구성을 관리할 수 있습니다. 이렇게 하면 역할 구성에 따라 이벤트 및 메시지를 제한하거나 필터링할 수 있습니다.

보안

REST API를 사용하여 SSH를 사용하여 ONTAP에 로그인하고 액세스하는 계정에 대해 TOTP(Time-Based One-Time Password) 프로필을 구성할 수 있습니다. 또한 키 관리자 끝점이 확장되어 지정된 키 관리 서버에서 복구 작업을 제공합니다.

SVM당 CIFS 구성

특정 SVM에 대한 구성을 업데이트할 수 있도록 기존 CIFS 엔드포인트가 확장되었습니다.

S3 버킷 규칙

기존 S3 버킷 끝점이 규칙 정의를 포함하도록 확장되었습니다. 각 규칙은 목록 오브젝트이며 버킷 내의 오브젝트에 대해 수행할 동작 집합을 정의합니다. 전체적으로 이러한 규칙을 통해 S3 버킷의 라이프사이클을 보다 효율적으로 관리할 수 있습니다.

ONTAP 9.12.1

ONTAP 9.12.1은 40개 이상의 새로운 API 호출을 통해 ONTAP REST API의 기능을 계속 확장하고 있습니다. 이러한 엔드포인트는 새로운 ONTAP 기능과 기존 기능의 향상된 기능을 지원합니다. 이 릴리즈는 보안 및 NAS 기능 향상에 중점을 둡니다.

보안 강화

Amazon Web Services에는 키 및 기타 비밀에 대한 보안 저장소를 제공하는 키 관리 서비스가 포함되어 있습니다. REST API를 통해 이 서비스에 액세스하여 ONTAP에서 클라우드에 암호화 키를 안전하게 저장할 수 있습니다. 또한 NetApp Storage Encryption에 사용되는 인증 키를 생성하고 나열할 수 있습니다.

Active Directory를 클릭합니다

ONTAP 클러스터에 대해 정의된 Active Directory 계정을 관리할 수 있습니다. 여기에는 새 계정 만들기와 계정 표시, 업데이트 및 삭제 작업이 포함됩니다.

CIFS 그룹 정책입니다

REST API는 CIFS 그룹 정책의 생성 및 관리를 지원하도록 개선되었습니다. 구성 정보는 모든 또는 특정 SVM에 적용되는 그룹 정책 개체를 통해 사용 및 관리됩니다.

ONTAP 9.11.1

ONTAP 9.11.1은 거의 100개의 새로운 API 호출을 통해 ONTAP REST API의 기능을 계속 확장하고 있습니다. 이러한 엔드포인트는 새로운 ONTAP 기능과 기존 기능의 향상된 기능을 지원합니다. 이 릴리즈에서는 고객이 Data ONTAP API(ONTAPI 또는 ZAPI)에서 ONTAP REST API로 마이그레이션할 수 있도록 지원합니다.

세분화된 RBAC

RBAC(ONTAP 역할 기반 액세스 제어) 기능이 더 세분화하여 개선되었습니다. REST API를 통해 필요에 따라 기존 역할을 사용하거나 새 사용자 지정 역할을 생성할 수 있습니다. 모든 역할은 하나 이상의 권한과 연결되며, 각 권한은 액세스 수준과 함께 REST API 호출 또는 CLI 명령을 식별합니다. 등의 REST 역할에 대해 새 액세스 수준을 사용할 수 있습니다 `read_create` 및 `read_modify`. 이러한 향상 기능은 Data ONTAP API(ONTAPI 또는 ZAPI)와 패리티를 제공하고 REST API로 고객 마이그레이션을 지원합니다. 을 참조하십시오 ["RBAC 보안"](#) 를 참조하십시오.

성능 카운터

이전 ONTAP 릴리즈에서는 시스템의 작동 특성에 대한 통계 정보를 유지했습니다. 9.11.1 릴리스 버전에서는 이 정보가 향상되어 이제 REST API를 통해 사용할 수 있습니다. 관리자 또는 자동화된 프로세스에서 데이터에 액세스하여 시스템 성능을 확인할 수 있습니다. 카운터 관리자 하위 시스템에서 유지 관리하는 통계 정보는 테이블 및 행을 사용하여 데이터베이스 형식으로 표시됩니다. 이러한 성능 향상을 통해 ONTAP REST API는 Data ONTAP API(ONTAPI 또는 ZAPI)와 패리티에 더 가깝게 됩니다.

애그리게이트 관리

ONTAP 스토리지 애그리게이트 관리가 향상되었습니다. 업데이트된 REST 엔드포인트를 사용하여 온라인 및 오프라인으로 애그리게이트를 이동하고 스페어를 관리할 수 있습니다.

IP 서브넷 기능입니다

ONTAP 네트워킹 기능이 IP 서브넷 지원을 포함하도록 확장되었습니다. REST API를 사용하면 ONTAP 클러스터 내에서 IP 서브넷의 구성 및 관리에 액세스할 수 있습니다.

여러 관리자 검증

여러 관리자 확인 기능은 ONTAP 명령 또는 작업에 대한 액세스를 보호하기 위한 유연한 인증 프레임워크를 제공합니다. 제한된 명령을 식별하는 규칙을 정의할 수 있습니다. 사용자가 특정 명령에 대한 액세스를 요청하면 여러 ONTAP 관리자가 적절한 승인을 부여할 수 있습니다.

SnapMirror의 향상된 기능

SnapMirror 기능은 예약을 비롯한 여러 영역에서 개선되었습니다. SnapVault 관계 패리티는 ONTAP 9.11.1과 DP 관계에 추가되었으며, REST API에서 사용할 수 있는 스로틀 기능은 Data ONTAP API(ONTAPI 또는 ZAPI)와 동일합니다. 이와 관련하여 대량 스냅샷 복사본을 생성 및 관리할 수 있는 지원이 제공됩니다.

지원합니다

ONTAP 스토리지 풀에 대한 액세스를 제공하기 위해 여러 엔드포인트가 추가되었습니다. 클러스터에서 스토리지 풀을 생성 및 나열하고 ID별로 특정 풀을 업데이트 및 삭제하는 기능이 지원됩니다.

이름 서비스 캐시 지원

ONTAP 이름 서비스는 성능 및 복원성을 향상시키는 캐싱을 지원하도록 개선되었습니다. 이제 REST API를 통해 이름 서비스 캐시 구성에 액세스할 수 있습니다. 호스트, UNIX 사용자, UNIX 그룹 및 넷그룹을 비롯한 여러 레벨에서 설정을 적용할 수 있습니다.

ONTAPI 보고 도구

ONTAPI 보고 도구는 고객과 파트너가 자신의 환경에서 ONTAPI 사용을 식별할 수 있도록 도와줍니다. Python 소프트웨어 외에도 NetApp Lab on Demand의 비디오 및 발전 지원도 제공됩니다. 이 둘은 ONTAPI에서 ONTAP REST API로 마이그레이션할 때 다른 리소스를 제공합니다.

ONTAP 9.10.1

ONTAP 9.10.1 ONTAP REST API의 기능은 계속 확장되고 있습니다. 새로운 ONTAP 기능과 기존 기능 향상을 지원하기 위해 100개 이상의 새로운 엔드포인트가 추가되었습니다. REST API의 향상된 기능에 대한 요약 정보가 아래에 나와 있습니다.

애플리케이션 정합성 보장 그룹

정합성 보장 그룹은 스냅샷과 같은 특정 작업을 수행할 때 함께 그룹화되는 볼륨 세트입니다. 이 기능은 단일 볼륨 작업에서 동일한 충돌 일관성 및 데이터 무결성을 단일 볼륨 작업으로 확장합니다. 대규모 다중 볼륨 워크로드 애플리케이션에 유용합니다.

SVM 마이그레이션

소스 클러스터에서 대상 클러스터로 SVM을 마이그레이션할 수 있습니다. 새 엔드포인트는 일시 중지, 재개, 상태 검색 및 마이그레이션 작업 중단 기능을 포함하여 완벽한 제어를 제공합니다.

파일 복제 및 관리

볼륨 레벨 파일 클론 복제 및 관리가 개선되었습니다. 새로운 REST 엔드포인트는 파일 이동, 복사 및 분할 작업을 지원합니다.

S3 감사 기능 향상

S3 이벤트에 대한 감사는 특정 S3 이벤트를 추적하고 기록할 수 있는 보안 개선입니다. S3 감사 이벤트 선택기는 버킷당 SVM 단위로 설정할 수 있습니다.

랜섬웨어 방어

ONTAP는 랜섬웨어 위협이 있을 가능성이 있는 파일을 감지합니다. 이러한 의심되는 파일의 목록을 검색할 수 있을 뿐 아니라 볼륨에서 제거할 수도 있습니다.

기타 보안 향상 기능

기존 프로토콜을 확장하고 새로운 기능을 도입하는 몇 가지 일반적인 보안 개선 사항이 있습니다. IPsec, 키 관리, SSH 구성 및 파일 권한이 개선되었습니다.

CIFS 도메인 및 로컬 그룹

CIFS 도메인에 대한 지원이 클러스터 및 SVM 레벨에서 추가되었습니다. 도메인 구성을 검색할 뿐만 아니라 기본 도메인 컨트롤러를 만들고 제거할 수도 있습니다.

볼륨 분석 확장

추가 엔드포인트를 통해 볼륨 분석 및 메트릭이 확장되어 상위 파일, 디렉토리 및 사용자를 지원합니다.

지원 개선 사항

몇 가지 새로운 기능을 통해 지원이 향상되었습니다. 자동 업데이트는 최신 소프트웨어 업데이트를 다운로드하고 적용하여 ONTAP 시스템을 최신 상태로 유지할 수 있습니다. 노드에서 생성된 메모리 코어 덤프를 검색하고 관리할 수도 있습니다.

ONTAP 9.9.1

ONTAP 9.9.1은 ONTAP REST API의 기능을 계속 확장합니다. SAN 포트 세트 및 SVM 파일 디렉토리 보안을 비롯한 기존 ONTAP 기능을 위한 새로운 API 엔드포인트가 있습니다. 또한 새로운 ONTAP 9.9.1 기능 및 향상된 기능을 지원하기 위해 끝점이 추가되었습니다. 또한 관련 문서도 개선되었습니다. 개선 사항에 대한 요약은 아래에 나와 있습니다.

ONTAP 9 REST API에 ONTAPI 매핑

ONTAP 자동화 코드를 REST API로 전환할 수 있도록 NetApp에서 API 매핑 문서를 제공합니다. 이 참조에는 ONTAPI 호출 목록과 각각에 해당하는 REST API 호출 목록이 포함되어 있습니다. 새 ONTAP 9.9.1 API 끝점을 포함하도록 매핑 문서가 업데이트되었습니다. 을 참조하십시오 ["ONTAPI를 REST API 매핑에 매핑"](#) 를 참조하십시오.

새로운 ONTAP 9.9.1 코어 기능의 API 엔드포인트

ONTAPI API를 통해 사용할 수 없는 새로운 ONTAP 9.9.1 기능이 REST API에 추가되었습니다. 여기에는 중첩된 igroup 및 Google Cloud Key Management Services에 대한 지원이 포함됩니다.

ONTAPI에서 REST로 전환하기 위한 지원이 향상되었습니다

기존 ONTAPI 호출의 더 많은 부분이 이제 상응하는 REST API 호출을 갖게 되었습니다. 여기에는 로컬 Unix 사용자 및 그룹, 클라이언트, SAN 포트 세트 및 볼륨 공간 속성 없이 NTFS 파일 보안 관리가 포함됩니다. 이러한 변경 사항은 업데이트된 ONTAPI to Rest 매핑 문서에도 포함되어 있습니다.

향상된 온라인 설명서

이제 ONTAP 온라인 설명서 참조 페이지에는 ONTAP 9.9.1의 새로운 기능을 포함하여 각 REST 엔드포인트 또는 매개 변수가 도입되었을 때 ONTAP 릴리스를 나타내는 레이블이 포함되어 있습니다.

ONTAP 9.8

ONTAP 9.8은 ONTAP REST API의 폭과 깊이를 크게 확장합니다. 이 솔루션에는 ONTAP 스토리지 시스템의 구축 및 관리를 자동화할 수 있도록 향상된 몇 가지 새로운 기능이 포함되어 있습니다. 또한 기존 ONTAPI API에서 REST로의 전환을 지원하기 위해 지원이 향상되었습니다.

ONTAP 9 REST API에 ONTAPI 매핑

ONTAPI 자동화를 업데이트할 수 있도록 NetApp에서는 하나 이상의 입력 매개 변수가 필요한 ONTAPI 호출 목록과 해당 호출을 동등한 ONTAP 9 REST API 호출에 대한 매핑을 제공합니다. 을 참조하십시오 ["ONTAPI를 REST API 매핑에 매핑"](#) 를 참조하십시오.

새로운 ONTAP 9.8 핵심 기능을 위한 API 엔드포인트

REST API에는 ONTAPI를 통해 사용할 수 없는 새로운 핵심 ONTAP 9.8 기능에 대한 지원이 추가되었습니다. 여기에는 ONTAP S3 버킷 및 서비스, SnapMirror 비즈니스 연속성 및 파일 시스템 분석에 대한 REST API 지원이 포함됩니다.

강화된 보안을 위한 지원 확대

Azure Key Vault, Google Cloud Key Management Services, IPSec 및 인증서 서명 요청 등의 여러 서비스와 프로토콜을 지원함으로써 보안이 향상되었습니다.

단순성 개선

ONTAP 9.8은 REST API를 사용하여 보다 효율적이고 현대적인 워크플로를 제공합니다. 예를 들어, OneClick 펌웨어 업데이트는 이제 여러 가지 유형의 펌웨어에서 사용할 수 있습니다.

향상된 온라인 설명서

이제 ONTAP 온라인 설명서 페이지에는 9.8의 새로운 기능을 포함하여 각 REST 엔드포인트 또는 매개 변수가 도입된 ONTAP 릴리스를 나타내는 레이블이 포함되어 있습니다.

ONTAPI에서 REST로 전환하기 위한 지원이 향상되었습니다

더 많은 레거시 ONTAPI 호출은 이제 상응하는 REST API를 갖습니다. 기존 ONTAPI 호출 대신 어떤 REST 엔드포인트를 사용해야 하는지 파악하는 데도 도움이 되는 문서도 제공됩니다.

성능 메트릭 확장

REST API의 성능 메트릭을 확장하여 몇 가지 새로운 스토리지 및 네트워크 객체를 포함시켰습니다.

ONTAP 9.7

ONTAP 9.7은 각각 여러 개의 REST 엔드포인트를 포함하는 세 가지 새로운 리소스 범주를 도입하여 ONTAP REST API의 기능 범위를 확장합니다.

- NDMP
- 오브젝트 저장소
- SnapLock

또한 ONTAP 9.7에서는 기존 리소스 범주 중 여러 개에 하나 이상의 새로운 REST 엔드포인트를 도입합니다.

- 클러스터
- NAS
- 네트워킹
- NVMe를 참조하십시오
- 산
- 보안
- 스토리지
- 지원

ONTAP 9.6

ONTAP 9.6은 ONTAP 9.4에 처음 도입된 REST API 지원을 크게 확장합니다. ONTAP 9.6 REST API는 대부분의 ONTAP 구성 및 관리 작업을 지원합니다.

ONTAP 9.6의 REST API에는 다음과 같은 주요 영역이 포함되어 있습니다.

- 클러스터 설정
- 프로토콜 구성
- 프로비저닝
- 성능 모니터링
- 데이터 보호
- 애플리케이션 인식 데이터 관리

시작하십시오

ONTAP 자동화 옵션을 이해합니다

ONTAP 스토리지 시스템의 구축과 관리를 자동화하는 몇 가지 옵션을 사용할 수 있습니다.

ONTAP REST API를 참조하십시오

ONTAP 9.6부터 ONTAP에는 스토리지 시스템의 배포 및 관리 자동화를 위한 기반을 제공하는 광범위한 REST API가 포함되어 있습니다. 그 이후로 REST API는 계속해서 확장 및 성숙되었습니다. 이제 ONTAP 구축 관리를 자동화할 때 선호하는 전략적 옵션을 제공합니다.

REST API에 기본적으로 액세스합니다

REST 클라이언트를 지원하는 모든 프로그래밍 언어를 사용하여 ONTAP REST API에 직접 액세스할 수 있습니다. Python, PowerShell, Java 등 다양한 언어가 제공됩니다.

REST를 사용하도록 레거시 ONTAPI 코드를 마이그레이션합니다

ONTAPI API(Zephyr API 또는 ZAPI)는 데이터 스토리지 관리 및 관리 작업의 자동화를 지원하기 위해 NetApp ONTAP 소프트웨어에 포함된 독창적인 호출 세트입니다. API는 의 일부입니다 ["NetApp 관리 SDK"](#). 향후 버전의 ONTAP에서는 ONTAPI 인터페이스가 비활성화될 것으로 예상됩니다. ONTAPI API를 사용하는 기존 코드가 있는 경우 ONTAPI에서 마이그레이션할 계획을 세워야 합니다. NetApp는 최신 ONTAP REST API를 사용하도록 코드를 변환할 수 있도록 지원합니다. 을 참조하십시오 ["ONTAPI에서 REST API로 마이그레이션합니다"](#) 를 참조하십시오.

클라이언트 소프트웨어 툴킷

NetApp는 ONTAP REST API를 추상화하여 자동화 코드를 더 쉽게 생성할 수 있는 클라이언트 툴킷을 제공합니다. 개발 언어 및 환경에 적합한 언어를 선택해야 합니다.

Python 클라이언트 라이브러리

Python 클라이언트 라이브러리는 스크립트를 작성하여 ONTAP REST API에 액세스할 때 사용할 수 있는 패키지입니다. 연결 관리, 비동기 요청 처리 및 예외 처리를 비롯한 여러 기본 서비스에 대한 지원을 제공합니다. Python 클라이언트 라이브러리를 사용하면 ONTAP 자동화 목표를 지원하는 강력한 코드를 빠르게 개발할 수 있습니다. 을 참조하십시오 ["Python 클라이언트 라이브러리"](#) 를 참조하십시오.

PowerShell 툴킷

NetApp.ONTAP PowerShell Toolkit을 사용하면 Windows 호스트에서 ONTAP 클러스터 관리를 자동화할 수 있습니다. 을 참조하십시오 ["PowerShell Toolkit 개요"](#) 를 참조하십시오.

자동화 프레임워크

여러 프레임워크 중 하나를 사용하여 자동화 코드를 만들고 배포할 수 있습니다

Ansible

Ansible은 프로비저닝, 구성 관리, 애플리케이션 배포를 지원하는 오픈 소스 소프트웨어 툴입니다. RedHat이 출시하고 이후 인수한 이후 계속 인기를 끌고 있습니다. NetApp은 고객이 ONTAP 스토리지 시스템 관리를 자동화하는 데 사용할 수 있는 Ansible 인증 모듈을 제공합니다. 을 참조하십시오 ["자세한 정보"](#) 및 ["NetApp Ansible DevOps 솔루션"](#) 자세한 내용은 를 참조하십시오.

BlueXP 자동화 카탈로그

넷앱 "BlueXP 자동화 카탈로그" 는 BlueXP 웹 사용자 인터페이스를 통해 제공됩니다. 이 카탈로그에서는 ONTAP를 다른 제품과 통합하고 배포하는 데 도움이 되는 패키지 솔루션에 액세스할 수 있습니다. 을 참조하십시오 "NetApp 자동화" 을 참조하십시오.

ONTAP REST API 액세스 방법

여러 가지 방법으로 ONTAP REST API에 액세스할 수 있습니다.

네트워크 고려 사항

다음 인터페이스를 통해 REST API에 연결할 수 있습니다.

- 클러스터 관리 LIF
- 노드 관리 LIF
- SVM 관리 LIF

사용할 LIF는 HTTPS 관리 프로토콜을 지원하도록 구성해야 합니다. 또한 네트워크의 방화벽 구성에서 HTTPS 트래픽을 허용해야 합니다.



클러스터 관리 LIF는 항상 사용해야 합니다. 이렇게 하면 모든 노드에서 API 요청의 로드 밸런싱을 수행하고 오프라인이거나 연결 문제가 발생하는 노드를 피할 수 있습니다. 여러 클러스터 관리 LIF가 구성된 경우 REST API에 액세스하는 것과 동일한 것입니다.

ONTAP API 온라인 설명서 페이지

ONTAP API 온라인 설명서 페이지는 웹 브라우저를 사용할 때 액세스 포인트를 제공합니다. 개별 API 호출을 직접 실행하는 방법을 제공하는 것 외에도 이 페이지에는 각 호출에 대한 입력 매개 변수 및 기타 옵션을 포함하여 API에 대한 자세한 설명이 포함되어 있습니다. API 호출은 기능 범주로 구성됩니다. 을 참조하십시오 "나머지 리소스 요약" 를 참조하십시오.

최신 버전의 API에 대한 설명서 페이지에 액세스하는 데 사용되는 URL 형식은 다음과 같습니다.

```
https://<cluster_mgmt_ip_address>/docs/api
```

사용자 정의 소프트웨어 및 도구

여러 가지 프로그래밍 언어 및 도구를 사용하여 ONTAP API에 액세스할 수 있습니다. Python, Java, Curl, PowerShell을 비롯한 다양한 옵션이 제공됩니다. API를 사용하는 프로그램, 스크립트 또는 도구는 REST 웹 서비스 클라이언트로 작동합니다. 프로그래밍 언어를 사용하면 API를 보다 심층적으로 이해할 수 있으며 ONTAP 관리를 자동화할 수 있습니다.

최신 버전의 API에 직접 액세스하는 데 사용되는 기본 URL의 형식은 다음과 같습니다.

```
https://<cluster_mgmt_ip_address>/api
```

여러 버전이 지원되는 특정 API 버전에 액세스하려면 URL 형식은 다음과 같습니다.

```
https://<cluster_mgmt_ip_address>/api/v1
```

첫 번째 API 호출입니다

간단한 curl 명령을 실행하여 ONTAP REST API를 사용하여 시작하고 가용성을 확인할 수 있습니다.

시작하기 전에

워크스테이션에서 curl 유틸리티를 사용할 수 있을 뿐 아니라 다음이 필요합니다.

- ONTAP 클러스터 관리 LIF의 IP 주소 또는 FQDN입니다
- ONTAP REST API 액세스 권한이 있는 계정의 ONTAP 자격 증명입니다



자격 증명에 특수 문자가 포함된 경우 사용 중인 셸에 따라 컬링할 수 있는 방식으로 해당 문자를 포맷해야 합니다. 예를 들어 각 특수 문자 앞에 백슬래시를 삽입하거나 전체 자격 증명 문자열을 큰따옴표로 묶을 수 있습니다.

단계

1. 로컬 워크스테이션의 명령줄 인터페이스에서 다음 명령을 실행합니다.

```
curl --request GET \  
"https://$FQDN_IP/api/cluster?fields=version" \  
--user username:password
```

◦ 예 *

```
curl --request GET "https://10.29.186.132/api/cluster?fields=version" --user  
admin:david123
```

작업을 마친 후

ONTAP 버전 정보는 JSON 형식으로 표시됩니다.

NetApp 연구소 리소스

NetApp는 ONTAP REST API 및 기타 관련 자동화 기술을 테스트할 수 있는 연구소 환경을 제공합니다.

를 클릭합니다 "[Lab on Demand의 약어로](#)" 는 NetApp 고객 및 파트너에게 제공됩니다. 로그인하여 실습 리소스를 사용하려면 유효한 자격 증명이 필요합니다. 필요한 경우 실습에서 *REST* 또는 기타 기술을 검색할 수 있습니다.

검토도 합니다 "[Lab on Demand를 준비하여 샘플 스크립트를 실행합니다](#)" 시작하십시오.

ONTAP REST API를 참조하십시오

REST 구현 세부 정보

REST 웹 서비스 기반

REST(Representational State Transfer)는 분산된 웹 애플리케이션을 만드는 스타일입니다. 웹 서비스 API의 설계에 적용될 경우 서버 기반 리소스를 노출하고 상태를 관리하기 위한 일련의 기술을 설정합니다. 이 솔루션은 메인스트림 프로토콜과 표준을 사용하여 ONTAP 클러스터 관리를 위한 유연한 기반을 제공합니다.



REST는 일반적인 기술과 모범 사례를 설정하지만 각 API의 세부 사항은 개발 과정에서 선택한 사항에 따라 다를 수 있습니다. ONTAP REST API를 라이브 구축과 함께 사용하기 전에 이 API의 설계 특성을 숙지해야 합니다.

리소스 및 상태 표시

리소스는 웹 기반 시스템의 기본 구성 요소입니다. REST 웹 서비스 응용 프로그램을 만들 때 초기 설계 작업은 다음과 같습니다.

- 시스템 또는 서버 기반 리소스 식별

모든 시스템은 리소스를 사용하고 유지합니다. 리소스는 파일, 비즈니스 트랜잭션, 프로세스 또는 관리 엔티티가 될 수 있습니다. REST 웹 서비스를 기반으로 애플리케이션을 설계하는 첫 번째 작업 중 하나는 리소스를 식별하는 것입니다.

- 자원 상태 및 연관된 상태 작업의 정의

리소스는 항상 한정된 수의 상태 중 하나에 있습니다. 상태 변경에 영향을 주는 데 사용되는 상태 및 관련 작업을 명확하게 정의해야 합니다.

URI 끝점

모든 REST 리소스는 잘 정의된 주소 지정 체계를 사용하여 정의되고 사용 가능해야 합니다. 리소스가 있고 식별된 끝점은 URI(Uniform Resource Identifier)를 사용합니다. URI는 네트워크의 각 리소스에 대해 고유한 이름을 만들기 위한 일반 프레임워크를 제공합니다. URL(Uniform Resource Locator)은 리소스를 식별하고 액세스하기 위해 웹 서비스와 함께 사용되는 URI 유형입니다. 일반적으로 리소스는 파일 디렉터리와 비슷한 계층적 구조로 표시됩니다.

HTTP 메시지

HTTP(Hypertext Transfer Protocol)는 웹 서비스 클라이언트 및 서버가 리소스에 대한 요청 및 응답 메시지를 교환하기 위해 사용하는 프로토콜입니다. 웹 서비스 응용 프로그램 설계의 일환으로 HTTP 메시드는 리소스 및 해당 상태 관리 작업에 매핑됩니다. HTTP는 상태 비저장입니다. 따라서 관련 요청 및 응답 집합을 하나의 트랜잭션으로 연결하려면 요청 및 응답 데이터 플로우와 함께 전달된 HTTP 헤더에 추가 정보가 포함되어야 합니다.

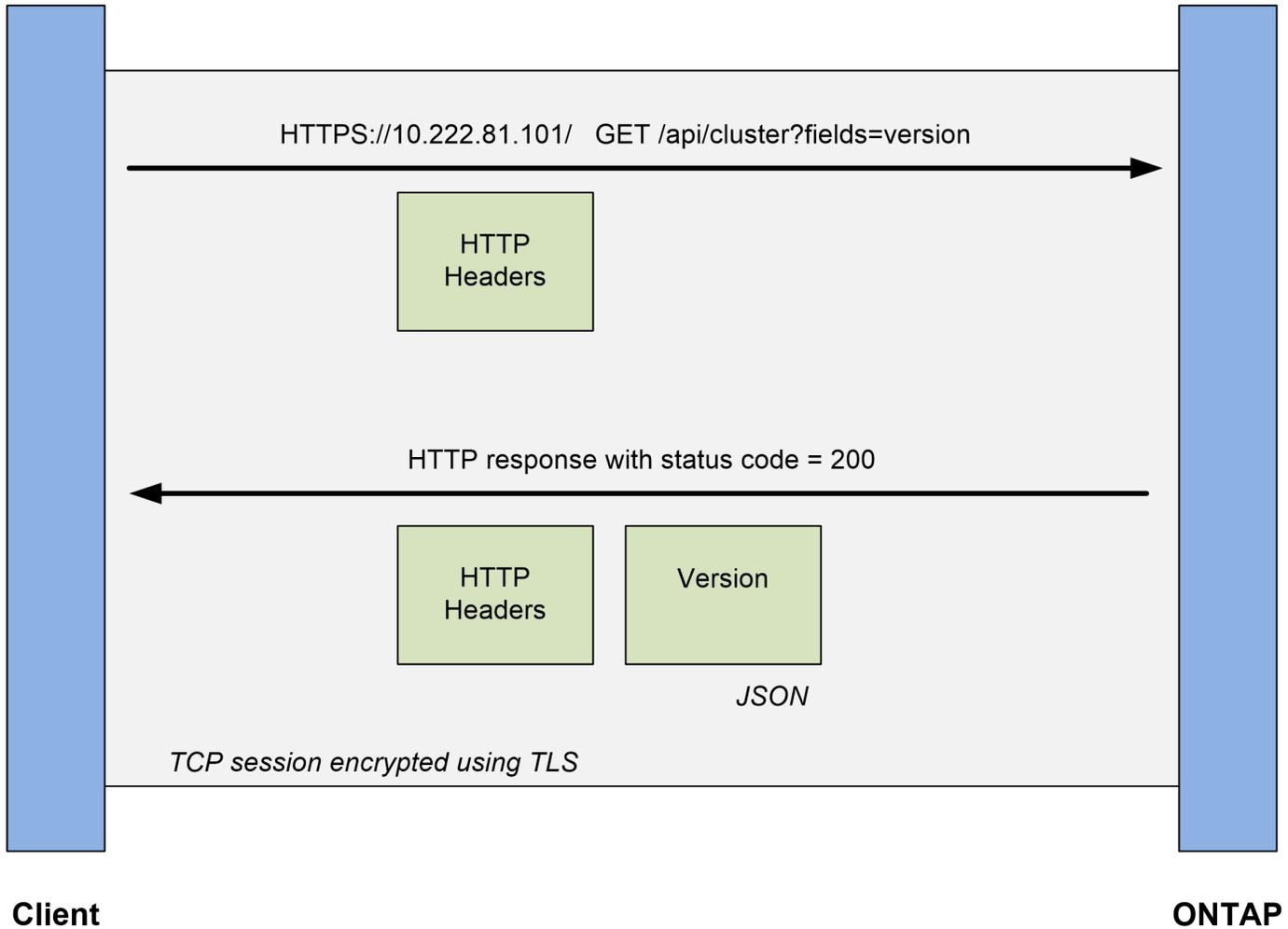
JSON 형식

여러 가지 방법으로 웹 서비스 클라이언트와 서버 간에 정보를 구성 및 전송할 수 있지만 가장 일반적인 옵션은 JSON(JavaScript Object Notation)입니다. JSON은 단순 데이터 구조를 일반 텍스트로 나타내는 업계 표준이며

리소스를 설명하는 상태 정보를 전송하는 데 사용됩니다. ONTAP REST API는 JSON을 사용하여 각 HTTP 요청 및 응답의 본문으로 전송되는 데이터를 포맷합니다.

일반적인 **REST API** 트랜잭션입니다

모든 API 트랜잭션은 HTTP 요청과 관련 응답으로 구성됩니다. 이 그림에서는 클러스터에서 사용하는 ONTAP 소프트웨어의 버전을 검색하는 방법을 보여 줍니다.



HTTP 요청

클라이언트에서 서버로 보낸 요청은 다음과 같이 구성됩니다.

- 동사 보기
- 클러스터의 URL 경로입니다
- 쿼리 매개 변수(필드)
- 승인을 포함한 요청 헤더

HTTP 응답입니다

서버에서 클라이언트로 전송되는 응답은 다음과 같이 구성됩니다.

- 상태 코드 200

- 응답 헤더
- 클러스터 소프트웨어 버전이 포함된 응답 본체입니다

기본 작동 특성

REST는 일반적인 기술과 모범 사례를 설정하지만 각 API의 세부 사항은 설계 선택에 따라 달라질 수 있습니다.

요청 및 응답 API 트랜잭션

모든 REST API 호출은 클라이언트에 대한 관련 응답을 생성하는 ONTAP 시스템에 대한 HTTP 요청으로 수행됩니다. 이 요청/응답 쌍은 API 트랜잭션으로 간주됩니다. API를 사용하기 전에 요청 및 응답 출력의 내용을 제어하는 데 사용할 수 있는 입력 변수에 대해 잘 알고 있어야 합니다.

CRUD 작업 지원

ONTAP REST API를 통해 사용 가능한 각 리소스는 CRUD 모델을 기반으로 액세스됩니다.

- 생성
- 읽기
- 업데이트
- 삭제

일부 리소스의 경우 일부 작업만 지원됩니다. 각 리소스에 대한 자세한 내용은 ONTAP 클러스터의 ONTAP API 설명서 페이지를 참조하십시오.

오브젝트 식별자

각 리소스 인스턴스 또는 개체는 만들 때 고유한 식별자가 할당됩니다. 대부분의 경우 식별자는 128비트 UUID입니다. 이러한 식별자는 특정 ONTAP 클러스터 내에서 전역적으로 고유합니다. 새 개체 인스턴스를 만드는 API 호출을 실행하면 연결된 ID 값이 있는 URL이 HTTP 응답의 위치 헤더에 있는 호출자에게 반환됩니다. 식별자를 추출하여 리소스 인스턴스를 참조할 때 후속 호출에 사용할 수 있습니다.



개체 식별자의 내용 및 내부 구조는 언제든지 변경할 수 있습니다. 관련 객체를 참조할 때는 필요한 경우 해당 API 호출에서만 식별자를 사용해야 합니다.

개체 인스턴스 및 컬렉션

API 호출은 리소스 경로 및 HTTP 메서드에 따라 특정 개체 인스턴스 또는 개체 컬렉션에 적용될 수 있습니다.

동기 및 비동기 작업

ONTAP는 클라이언트로부터 받은 HTTP 요청을 수행하는 두 가지 방법이 있습니다.

동기 처리

ONTAP는 요청을 즉시 수행하고 HTTP 상태 코드가 200 또는 201인 경우 응답한다.

get, head 및 options 메서드를 사용하는 모든 요청은 항상 동기적으로 수행됩니다. 또한 POST, 패치 및 삭제를

사용하는 요청은 2초 이내에 완료될 것으로 예상되는 경우 동기적으로 실행되도록 설계되었습니다.

비동기 처리

비동기 요청이 유효한 경우 ONTAP는 요청을 처리하기 위한 백그라운드 작업과 작업을 고정하기 위한 작업 개체를 만듭니다. 202 HTTP 상태는 작업 객체와 함께 호출자에게 반환됩니다. 최종 성공 또는 실패를 확인하려면 작업의 상태를 검색해야 합니다.

POST, 패치 및 삭제 메서드를 사용하는 요청은 완료하는 데 2초 이상 걸릴 것으로 예상되는 경우 비동기적으로 실행되도록 설계되었습니다.



를 클릭합니다 `return_timeout` 쿼리 매개 변수는 비동기 API 호출에 사용할 수 있으며 비동기 호출을 동기적으로 완료하도록 변환할 수 있습니다. 을 참조하십시오 ["작업 개체를 사용한 비동기 처리"](#) 를 참조하십시오.

보안

REST API와 함께 제공되는 보안은 주로 ONTAP에서 사용할 수 있는 기존 보안 기능을 기반으로 합니다. 다음 보안은 API에서 사용됩니다.

전송 계층 보안

클라이언트와 ONTAP LIF 간에 네트워크를 통해 전송되는 모든 트래픽은 ONTAP 구성 설정에 따라 TLS를 사용하여 암호화됩니다.

클라이언트 인증

ONTAP System Manager 및 네트워크 관리 SDK에서 사용할 수 있는 인증 옵션과 동일한 인증 옵션을 ONTAP REST API에서도 사용할 수 있습니다.

HTTP 인증

예를 들어, HTTP 레벨에서 ONTAP REST API에 직접 액세스하는 경우 아래에 설명된 대로 두 가지 인증 옵션이 있습니다. 각 경우에 HTTP 권한 부여 헤더를 만들어 각 요청에 포함시켜야 합니다.

옵션을 선택합니다	설명
HTTP 기본 인증	ONTAP 사용자 이름과 암호는 콜론으로 연결됩니다. 문자열은 base64로 변환되고 요청 헤더에 포함됩니다.
OAuth 2.0 을 참조하십시오	ONTAP 9.14부터 외부 권한 부여 서버에서 액세스 토큰을 요청하여 요청 헤더에 베어러 토큰으로 포함할 수 있습니다.

OAuth 2.0에 대한 자세한 내용과 ONTAP에서 구현하는 방법은 을 참조하십시오 ["ONTAP OAuth 2.0 구축 개요"](#). 도 참조하십시오 ["워크플로우 사용을 준비하십시오"](#) 이 사이트의 아래.

ONTAP 인증

ONTAP는 역할 기반 인증 모델을 구현합니다. ONTAP REST API 또는 API 설명서 페이지에 액세스할 때 사용하는 계정에 적절한 권한이 있어야 합니다.

API 요청을 제어하는 입력 변수입니다

HTTP 요청에 설정된 매개 변수와 변수를 통해 API 호출이 처리되는 방식을 제어할 수 있습니다.

HTTP 메서드

ONTAP REST API에서 지원하는 HTTP 메서드는 다음 표에 나와 있습니다.



모든 HTTP 메서드를 각 REST 끝점에서 사용할 수 있는 것은 아닙니다. 또한 컬렉션에서 패치와 삭제를 모두 사용할 수 있습니다. 자세한 내용은 `_개체 참조 및 액세스_` 를 참조하십시오.

HTTP 메소드	설명
가져오기	리소스 인스턴스 또는 컬렉션의 개체 속성을 검색합니다.
게시	제공된 입력을 기반으로 새 리소스 인스턴스를 만듭니다.
패치	제공된 입력에 따라 기존 리소스 인스턴스를 업데이트합니다.
삭제	기존 리소스 인스턴스를 삭제합니다.
머리	GET 요청을 효과적으로 발급하지만 HTTP 헤더만 반환합니다.
옵션	특정 끝점에서 지원되는 HTTP 메서드를 결정합니다.

경로 변수

각 REST API 호출에 사용되는 끝점 경로에는 다양한 식별자가 포함될 수 있습니다. 각 ID는 특정 리소스 인스턴스에 해당합니다. 예를 들어 클러스터 ID 및 SVM ID가 있습니다.

요청 헤더

HTTP 요청에 여러 개의 헤더를 포함해야 합니다.

콘텐츠 유형

요청 본문에 JSON이 포함된 경우 이 헤더를 `application/json`으로 설정해야 합니다.

수락

이 헤더는 `application/hal+json`으로 설정해야 한다. 대신 `application/json`으로 설정하면 다음 레코드 배치를 검색하는 데 필요한 링크를 제외하고 HAL 링크는 반환되지 않습니다. 이 두 값 외에 다른 머리가 있으면 응답에서 콘텐츠 형식 헤더의 기본값은 `application/hal+json`이 됩니다.

권한 부여

기본 인증은 base64 문자열로 인코딩된 사용자 이름과 암호로 설정되어야 합니다. 예를 들면 다음과 같습니다.

```
Authorization: Basic YWRtaW46cGV0ZXJzb24=.
```

요청 본문

요청 본문의 내용은 특정 호출에 따라 달라집니다. HTTP 요청 본문은 다음 중 하나로 구성됩니다.

- 입력 변수가 있는 JSON 개체입니다
- JSON 개체가 비어 있습니다

오브젝트 필터링

Get 메서드를 사용하여 API 호출을 실행할 때 쿼리 매개 변수를 사용하여 모든 특성을 기준으로 반환된 객체를 제한하거나 필터링할 수 있습니다.

쿼리 매개 변수 구문 분석 및 해석

하나 이상의 매개 변수 집합을 뒤에 오는 URL 문자열에 추가할 수 있습니다? 문자. 둘 이상의 매개 변수가 제공된 경우 쿼리 매개 변수는 을 기반으로 분할됩니다 & 문자. 매개 변수의 각 키와 값은 에서 분할됩니다 = 문자.

예를 들어 등호를 사용하여 정확히 일치하는 값을 지정할 수 있습니다.

```
<field>=<value>
```

보다 복잡한 쿼리의 경우 추가 연산자는 등호 뒤에 배치됩니다. 예를 들어 일부 값보다 크거나 같은 특정 필드를 기준으로 개체 집합을 선택하려면 쿼리는 다음과 같습니다.

```
<field>=>=<value>
```

필터링 연산자

위에 제공된 예제 외에 값 범위에 걸쳐 개체를 반환하는 추가 연산자를 사용할 수 있습니다. ONTAP REST API가 지원하는 필터링 연산자에 대한 요약은 아래 표와 같다.



설정되지 않은 필드는 일반적으로 일치하는 쿼리에서 제외됩니다.

운영자	설명
=	같음
를 누릅니다	보다 작음
를 누릅니다	보다 큼
=	보다 작거나 같음
>=	보다 크거나 같음
!	같지 않음
*	greedy 와일드카드

쿼리의 일부로 "null" 키워드 또는 "Negation"!null"을 사용하여 특정 필드가 설정되었는지 여부를 기준으로 개체 컬렉션을 반환할 수도 있습니다.

워크플로 예

이 사이트의 REST API 워크플로에 포함된 몇 가지 예가 아래에 나와 있습니다.

- ["디스크 나열"](#)

를 기준으로 필터링합니다 state 스페어 디스크를 선택하는 변수입니다.

특정 객체 필드를 요청하는 중입니다

기본적으로 Get을 사용하여 API 호출을 실행하면 HAL 자체 링크와 함께 개체나 개체를 고유하게 식별하는 특성만 반환됩니다. 이 최소 필드 집합은 각 개체의 키 역할을 하며 개체 유형에 따라 달라집니다. 다음과 같은 방법으로 '필드'

쿼리 매개 변수를 사용하여 추가 개체 속성을 선택할 수 있습니다.

- 공통 또는 표준 필드

가장 일반적으로 사용되는 객체 필드를 검색하려면 필드= * 를 지정합니다. 이러한 필드는 일반적으로 로컬 서버 메모리에 유지되거나 액세스에 필요한 처리가 거의 필요하지 않습니다. 이 속성은 URL 경로 키(UUID)로 GET를 사용한 후 개체에 대해 반환되는 속성과 동일합니다.

- 모든 필드

액세스 시 추가 서버 처리가 필요한 필드를 포함하여 모든 객체 필드를 검색하려면 필드=***를 지정합니다.

- 사용자 정의 필드 선택

필드=<field_name>'을 사용하여 원하는 필드를 정확하게 지정합니다. 여러 필드를 요청할 때는 공백 없이 심표를 사용하여 값을 구분해야 합니다.



가장 좋은 방법은 항상 원하는 특정 필드를 식별하는 것입니다. 필요한 경우 공통 필드 또는 모든 필드 집합만 검색해야 합니다. NetApp은 자체 성과 분석을 기반으로 공통으로 분류되어 있으며 'fields= *'를 사용하여 반환되는 필드를 결정합니다. 필드의 분류는 향후 릴리스에서 변경될 수 있습니다.

출력 집합에서 오브젝트 정렬

리소스 컬렉션의 레코드는 개체에서 정의한 기본 순서로 반환됩니다. 다음과 같이 필드 이름 및 정렬 방향을 가진 "ORDER_BY" 쿼리 매개 변수를 사용하여 순서를 변경할 수 있습니다.

'ORDER_BY=<필드 이름>ASC|desc'

예를 들어 유형 필드를 내림차순으로 정렬한 다음 ID를 오름차순으로 정렬할 수 있습니다.

order_by=desc, id asc를 입력합니다

다음 사항에 유의하십시오.

- 정렬 필드를 지정하지만 방향을 지정하지 않으면 값이 오름차순으로 정렬됩니다.
- 여러 매개 변수를 포함할 때는 필드를 심표로 구분해야 합니다.

컬렉션의 개체를 검색할 때 페이지 매김

Get 을 사용하여 API 호출을 실행하여 같은 형식의 개체 컬렉션에 액세스하면 ONTAP 는 두 가지 제약 조건에 따라 가능한 한 많은 개체를 반환합니다. 요청에 대한 추가 쿼리 매개 변수를 사용하여 이러한 각 제약 조건을 제어할 수 있습니다. 특정 GET 요청에 대한 첫 번째 제약 조건에 도달하면 요청이 종료되고 반환된 레코드 수가 제한됩니다.



모든 개체를 반복하기 전에 요청이 종료되면 응답에는 다음 레코드 배치를 검색하는 데 필요한 링크가 포함됩니다.

개체 수 제한

기본적으로 ONTAP 는 GET 요청에 대해 최대 10,000개의 오브젝트를 반환합니다. 이 제한은 max_records 쿼리 매개 변수를 사용하여 변경할 수 있습니다. 예를 들면 다음과 같습니다.

max_records=20

실제로 반환되는 개체 수는 관련 시간 제약 조건 및 시스템의 총 개체 수에 따라 실제 최대값보다 작을 수 있습니다.

객체를 검색하는 데 사용되는 시간 제한

기본적으로 ONTAP 는 GET 요청에 허용된 시간 내에 가능한 한 많은 오브젝트를 반환합니다. 기본 시간 초과는 15초입니다. RETURN_TIMEOUT' QUERY 파라미터를 이용하여 이 한계를 변경할 수 있다. 예를 들면 다음과 같습니다.

RETURN_TIMEOUT=5'입니다

실제로 반환되는 개체 수는 시스템의 총 개체 수와 개체 수에 대한 관련 제약 조건에 따라 최대 개체수보다 작을 수 있습니다.

결과 집합 축소

필요한 경우 이러한 두 매개 변수를 추가 쿼리 매개 변수와 결합하여 결과 집합의 범위를 좁힐 수 있습니다. 예를 들어, 지정된 시간 이후에 생성된 최대 10개의 EMS 이벤트가 반환됩니다.

time=> 2018-04-04T15:41:29.140265Z&max_records=10

여러 요청을 발행하여 객체를 통해 페이지를 이동할 수 있습니다. 이후의 각 API 호출은 마지막 결과 집합의 최신 이벤트를 기반으로 새 시간 값을 사용해야 합니다.

크기 속성

일부 API 호출과 특정 쿼리 매개 변수에 사용되는 입력 값은 숫자입니다. 정수(바이트)를 제공하는 대신 다음 표에 나와 있는 접미사를 선택적으로 사용할 수 있습니다.

접미사	설명
KB를 클릭합니다	KB 킬로바이트(1024바이트) 또는 키비바이트
MB	MB 메가바이트(KB x 1024바이트) 또는 메가바이트
GB	GB 기가바이트(MB x 1024바이트) 또는 기비바이트
TB	TB 테라바이트(GB x 1024바이트) 또는 테비바이트
PB	PB 페타바이트(TB x 1024바이트) 또는 페이비바이트

관련 정보

- ["개체 참조 및 액세스"](#)

API 응답을 해석합니다

각 API 요청은 클라이언트에 대한 응답을 다시 생성합니다. 응답을 검토하여 성공 여부를 확인하고 필요에 따라 추가 데이터를 검색해야 합니다.

HTTP 상태 코드입니다

ONTAP REST API에서 사용하는 HTTP 상태 코드는 다음과 같다.

코드	사유 구문	설명
200	좋습니다	새 개체를 만들지 않는 호출에 대한 성공 여부를 나타냅니다.
201	작성됨	객체가 성공적으로 생성되었습니다. 응답의 위치 헤더에는 개체의 고유 식별자가 포함됩니다.
202	수락됨	요청을 수행하기 위해 백그라운드 작업이 시작되었지만 아직 완료되지 않았습니다.
400	잘못된 요청입니다	요청 입력이 인식되지 않거나 부적절합니다.
401	권한이 없습니다	사용자 인증에 실패했습니다.
403	금지됨	인증 오류로 인해 액세스가 거부되었습니다.
404	찾을 수 없습니다	요청에서 참조되는 리소스가 없습니다.
405	메서드가 허용되지 않습니다	요청의 HTTP 메서드가 리소스에 대해 지원되지 않습니다.
409	충돌	다른 개체를 먼저 만들어야 하거나 요청된 개체가 이미 있으므로 개체를 만들지 못했습니다.
500입니다	내부 오류입니다	서버에서 일반적인 내부 오류가 발생했습니다.

응답 헤더

ONTAP에서 생성된 HTTP 응답에는 여러 헤더가 포함되어 있습니다.

위치

개체를 만들 때 위치 머리글에는 개체에 할당된 고유 식별자를 포함하여 새 개체에 대한 전체 URL이 포함됩니다.

콘텐츠 유형

이것은 보통 '응용 프로그램/JSON'입니다.

응답 바디

API 요청으로 인한 응답 본문의 내용은 객체, 처리 유형 및 요청의 성공 또는 실패에 따라 달라집니다. 응답은 항상 JSON으로 렌더링됩니다.

- 단일 개체

요청에 따라 필드 집합과 함께 단일 개체를 반환할 수 있습니다. 예를 들어, 가져오기를 사용하여 고유 식별자를 사용하여 클러스터의 선택된 속성을 검색할 수 있습니다.

- 여러 개의 개체

리소스 컬렉션의 여러 개체를 반환할 수 있습니다. 모든 경우에 사용되는 형식이 일관되게 있으며, 개체 인스턴스의 배열을 포함하는 레코드 및 레코드 수를 나타내는 num_records가 있습니다. 예를 들어, 특정 클러스터에 정의된 노드를 검색할 수 있습니다.

- 작업 객체

API 호출이 비동기적으로 처리되는 경우 백그라운드 작업을 고정하는 Job 개체가 반환됩니다. 예를 들어 클러스터 구성을 업데이트하는 데 사용되는 패치 요청은 비동기적으로 처리되고 작업 개체를 반환합니다.

- 오류 개체

오류가 발생하면 항상 Error 개체가 반환됩니다. 예를 들어, 클러스터에 대해 정의되지 않은 필드를 변경하려고 하면 오류가 발생합니다.

- JSON 개체가 비어 있습니다

경우에 따라 데이터가 반환되지 않고 응답 본문에 빈 JSON 개체가 포함되는 경우가 있습니다.

HAL 연결

ONTAP REST API는 HAL을 HATEOAS(Engine of Application State)로 Hypermedia를 지원하는 메커니즘으로 사용한다. 특정 리소스를 식별하는 객체 또는 속성이 반환되면 HAL로 인코딩된 링크도 포함되어 리소스에 대한 추가 세부 정보를 쉽게 찾아 확인할 수 있습니다.

오류

오류가 발생하면 응답 본문에 오류 객체가 반환됩니다.

형식

오류 개체의 형식은 다음과 같습니다.

```
"error": {  
  "message": "<string>",  
  "code": <integer>[,  
  "target": "<string>"]  
}
```

코드 값을 사용하여 일반 오류 유형 또는 범주를 확인하고 메시지를 사용하여 특정 오류를 확인할 수 있습니다. 사용 가능한 경우 대상 필드에는 오류와 관련된 특정 사용자 입력이 포함됩니다.

일반 오류 코드

일반적인 오류 코드는 다음 표에 설명되어 있습니다. 특정 API 호출에는 추가 오류 코드가 포함될 수 있습니다.

코드		설명
1	409	동일한 식별자를 가진 객체가 이미 있습니다.
2	400	필드 값이 잘못되었거나 누락되었거나 추가 필드가 제공되었습니다.
3	400	작업이 지원되지 않습니다.
4	405	지정된 식별자가 있는 개체를 찾을 수 없습니다.
6	403	요청 수행 권한이 거부되었습니다.
8	409	리소스가 사용 중입니다.

작업 개체를 사용한 비동기 처리

비동기적으로 실행되도록 설계된 API 요청을 실행하면 작업 객체가 항상 생성되어 호출자에게 반환됩니다. 이 작업에서는 요청을 처리하는 백그라운드 작업을 설명하고 앵커를 지정합니다. HTTP 상태 코드에 따라 작업의 상태를 검색하여 요청이 성공했는지 확인해야 합니다.

을 참조하십시오 **"API 참조입니다"** 비동기적으로 수행할 API 호출을 결정합니다.

요청 처리 방법 제어

RETURN_TIMEOUT' query 파라미터를 사용하면 비동기 API 호출 처리 방식을 제어할 수 있다. 이 매개 변수를 사용할 경우 두 가지 결과를 얻을 수 있습니다.

요청이 완료되기 전에 타이머가 만료됩니다

유효한 요청의 경우 ONTAP는 작업 객체와 함께 202 HTTP 상태 코드를 반환합니다. 요청이 성공적으로 완료되었는지 확인하려면 작업의 상태를 검색해야 합니다.

타이머가 만료되기 전에 요청이 완료되었습니다

요청이 유효하고 시간이 만료되기 전에 성공적으로 완료되면 ONTAP는 작업 객체와 함께 200 HTTP 상태 코드를 반환합니다. 요청이 200으로 표시된 대로 동기적으로 완료되므로 작업 상태를 검색할 필요가 없습니다.



RETURN_TIMEOUT 파라미터의 기본값은 0초입니다. 따라서 매개 변수를 포함하지 않으면 유효한 요청에 대해 202 HTTP 상태 코드가 항상 반환됩니다.

API 요청과 관련된 작업 객체를 쿼리합니다

HTTP 응답에서 반환된 작업 개체에는 여러 속성이 포함되어 있습니다. 후속 API 호출에서 state 속성을 쿼리하여 요청이 성공적으로 완료되었는지 확인할 수 있습니다. 작업 오브젝트는 항상 다음 상태 중 하나에 있습니다.

비단말기 상태입니다

- 대기열에 있습니다
- 실행 중입니다
- 일시 중지되었습니다

터미널 상태

- 성공
- 실패

비동기 요청을 실행하는 일반 절차입니다

다음 고급 절차를 사용하여 비동기 API 호출을 완료할 수 있습니다. 이 예제에서는 RETURN_TIMEOUT 매개변수가 사용되지 않거나 백그라운드 작업이 완료되기 전에 시간이 만료되는 것으로 가정합니다.

1. 비동기적으로 수행하도록 설계된 API 호출을 실행합니다.
2. 유효한 요청 수락을 나타내는 HTTP 응답 202 을 수신합니다.
3. 응답 본문에서 작업 객체의 식별자를 추출합니다.
4. 시간 지정 루프 내에서 각 사이클에서 다음을 수행합니다.

- a. 작업의 현재 상태를 가져옵니다.
 - b. 작업이 터미널 상태가 아닌 경우 루프를 다시 수행합니다.
5. 작업이 터미널 상태(성공, 실패)에 도달하면 중지합니다.

관련 정보

- ["클러스터 연락처를 업데이트합니다"](#)
- ["작업 인스턴스를 가져옵니다"](#)

개체 참조 및 액세스

ONTAP REST API를 통해 노출된 리소스 인스턴스 또는 개체는 여러 가지 방법으로 참조되고 액세스할 수 있습니다.

오브젝트 액세스 경로

높은 수준에서는 개체에 액세스할 때 두 가지 경로 유형이 있습니다.

- 기본

객체는 API 호출의 기본 또는 직접 타겟입니다.

- 외부

객체는 API 호출의 기본 참조가 아니라 기본 객체에서 연결됩니다. 따라서 이 개체는 외부 또는 다운스트림 개체이며 기본 개체의 필드를 통해 참조됩니다.

UUID를 사용하여 개체에 액세스

모든 개체에는 생성 시 고유한 식별자가 할당되며, 대부분의 경우 128비트 UUID입니다. 할당된 UUID 값은 변경할 수 없으며 ONTAP 내에서 내부적으로 사용되어 리소스에 액세스하고 관리할 수 있습니다. 따라서 UUID는 일반적으로 개체에 가장 빠르고 안정적으로 액세스할 수 있습니다.

대부분의 리소스 유형에서 UUID 값을 URL의 경로 키의 일부로 제공하여 특정 개체에 액세스할 수 있습니다. 예를 들어, 다음을 사용하여 노드 인스턴스 `"/cluster/nodes/{uuid}"`에 액세스할 수 있습니다

개체 속성을 사용하여 개체에 액세스

UUID 외에도 개체 속성을 사용하여 개체에 액세스할 수도 있습니다. 대부분의 경우 name 속성을 사용하면 편리합니다. 예를 들어, URL 문자열에 있는 다음 쿼리 매개 변수를 사용하여 노드 인스턴스에 대한 이름 `"/cluster/nodes?name=node_one"`을 기준으로 액세스할 수 있습니다. 쿼리 매개 변수 외에도 기본 개체의 속성을 통해 외부 개체에 액세스할 수 있습니다.

UUID 대신 이름이나 기타 속성을 사용하여 개체에 액세스할 수 있지만 다음과 같은 몇 가지 단점이 있습니다.

- 이름 필드는 변경할 수 없으며 변경할 수 있습니다. 개체에 액세스하기 전에 개체의 이름이 변경되면 잘못된 개체가 반환되거나 개체 액세스 오류가 발생합니다.



이 문제는 외부 개체의 POST 또는 패치 메서드나 기본 개체의 get 메서드에서 발생할 수 있습니다.

- ONTAP는 이름 필드를 해당 UUID로 변환해야 합니다. 이는 성능 문제가 될 수 있는 일종의 간접 액세스입니다.

특히 다음 중 하나 이상이 참일 경우 성능 저하가 발생할 수 있습니다.

- Get 메서드가 사용됩니다
- 큰 오브젝트 집합에 액세스합니다
- 복잡하거나 복잡한 쿼리가 사용됩니다

클러스터 및 SVM 컨텍스트 비교

클러스터와 SVM을 모두 지원하는 여러 개의 REST 엔드포인트가 있습니다. 이러한 엔드포인트 중 하나를 사용할 때 'scope=[svm|cluster]' 값을 통해 API 호출 컨텍스트를 나타낼 수 있습니다. 이 중 컨텍스트를 지원하는 엔드포인트의 예로는 IP 인터페이스 및 보안 역할이 있습니다.



범위 값에는 각 API 호출에 대해 제공된 속성을 기반으로 하는 기본값이 있습니다.

패치 사용 및 개체 모음에서 삭제

리소스 인스턴스에서 패치나 삭제를 지원하는 모든 REST 끝점은 개체 컬렉션에서 동일한 메서드를 지원합니다. 유일한 요구 사항은 URL 문자열의 쿼리 매개 변수를 통해 하나 이상의 필드를 제공해야 한다는 것입니다. 컬렉션을 통해 패치 또는 삭제를 실행하는 경우 이는 내부적으로 다음을 수행하는 것과 같습니다.

- 쿼리 기반 가져오기 - 컬렉션을 검색합니다
- 컬렉션의 각 개체에 대한 패치 또는 삭제 호출의 일련 번호 시퀀스입니다

작업 제한 시간은 기본값 15초로 RETURN_TIMEOUT으로 설정할 수 있다. 시간 초과 전에 완료되지 않은 경우 응답에는 다음 객체에 대한 링크가 포함됩니다. 작업을 계속하려면 다음 링크를 사용하여 동일한 HTTP 메서드를 다시 실행해야 합니다.

스토리지 리소스에 대한 성능 메트릭

ONTAP은 선택한 SVM 스토리지 오브젝트 및 프로토콜에 대한 성능 메트릭을 수집하고 REST API를 통해 이 정보를 보고합니다. 이 데이터를 사용하여 ONTAP 시스템의 성능을 모니터링할 수 있습니다.

특정 스토리지 오브젝트 또는 프로토콜에서 성능 데이터는 다음 세 가지 범주로 분류됩니다.

- IOPS
- 지연 시간
- 처리량

각 범주 내에서 다음 데이터 유형 중 하나 이상을 사용할 수 있습니다.

- 읽기(R)
- 쓰기(W)
- 기타(O)
- 합계(T)

다음 표에는 ONTAP REST API를 통해 사용할 수 있는 성능 데이터와 추가된 릴리즈가 요약되어 있습니다. 자세한 내용은 ONTAP 시스템의 REST API 온라인 설명서 페이지를 참조하십시오.

스토리지 오브젝트 또는 프로토콜입니다	IOPS	지연 시간	처리량	ONTAP 릴리즈
이더넷 포트	해당 없음	해당 없음	RWT	9.8
FC 포트	RWOT	RWOT	RWT	9.8
IP 인터페이스	해당 없음	해당 없음	RWT	9.8
FC 인터페이스	RWOT	RWOT	RWT	9.8
NVMe 네임스페이스	RWOT	RWOT	RWOT	9.8
qtree 통계	원시 RWOT	해당 없음	원시 RWOT	9.8
Volume FlexCache(볼륨 저장)	RWOT	RWOT	RWT	9.8
노드 - 프로세스 활용도	수치 값으로서 프로세스 활용	수치 값으로서 프로세스 활용	수치 값으로서 프로세스 활용	9.8
클라우드 볼륨	RWOT	RWOT	유연하지 않습니다	9.7
LUN을 클릭합니다	RWOT	RWOT	RWOT	9.7
집계	RWOT	RWOT	RWOT	9.7
SVM NFS 프로토콜	RWOT	RWOT	RWT	9.7
SVM CIFS 프로토콜	RWOT	RWOT	RWT	9.7
SVM FCP 프로토콜	RWOT	RWOT	RWT	9.7
SVM iSCSI 프로토콜	RWOT	RWOT	RWT	9.7
SVM NVMe 프로토콜	RWOT	RWOT	RWT	9.7
클러스터	RWOT	RWOT	RWOT	9.6
볼륨	RWOT	RWOT	RWOT	9.6

RBAC 보안

RBAC 보안 개요

ONTAP에는 강력하고 확장 가능한 RBAC(역할 기반 액세스 제어) 기능이 포함되어 있습니다. REST API 및 CLI를 통해 노출된 리소스에 대한 사용자의 액세스를 제어하는 역할을 각 계정에 다르게 할당할 수 있습니다. 이 역할은 다양한 ONTAP 사용자에 대해 서로 다른 수준의 관리 액세스를 정의합니다.



ONTAP RBAC 기능은 계속 확장되고 ONTAP 9.11.1(및 후속 릴리스)로 크게 향상되었습니다. 을 참조하십시오 ["RBAC 발전 요약"](#) 및 ["ONTAP REST API 및 자동화의 새로운 기능"](#) 를 참조하십시오.

ONTAP 역할

역할은 사용자가 수행할 수 있는 작업을 집합적으로 정의하는 권한 집합입니다. 각 권한은 특정 액세스 경로 및 관련 액세스 수준을 식별합니다. 역할은 사용자 계정에 할당되며 액세스 제어 결정을 내릴 때 ONTAP에 의해 적용됩니다.

역할 유형

역할에는 두 가지 유형이 있습니다. ONTAP이 발전함에 따라 다양한 환경에 맞게 조정되고 도입되었습니다.



각 유형의 역할을 사용할 때 장단점이 있습니다. 을 참조하십시오 ["역할 유형 비교"](#) 를 참조하십시오.

유형	설명
휴식	나머지 역할은 ONTAP 9.6으로 도입되었으며, REST API를 통해 ONTAP에 액세스하는 사용자에게 일반적으로 적용된다. REST 역할을 생성하면 기존의 <code>_mapping_role</code> 이 자동으로 생성됩니다.
기존	이는 ONTAP 9.6 이전에 포함된 레거시 역할입니다. ONTAP CLI 환경에 도입되었으며 RBAC 보안의 기본 요소로 계속 사용됩니다.

범위

모든 역할에는 해당 역할이 정의 및 적용되는 범위 또는 컨텍스트가 있습니다. 범위는 특정 역할이 사용되는 위치와 방법을 결정합니다.



ONTAP 사용자 계정에도 사용자 정의 및 사용 방법을 결정하는 유사한 범위가 있습니다.

범위	설명
클러스터	클러스터 범위가 있는 역할은 ONTAP 클러스터 레벨에 정의되어 있습니다. 클러스터 레벨 사용자 계정과 연결되어 있습니다.
SVM	SVM 범위를 갖는 역할은 특정 데이터 SVM에 대해 정의됩니다. 동일한 SVM의 사용자 계정에 할당됩니다.

역할 정의의 소스

ONTAP 역할은 두 가지 방법으로 정의할 수 있습니다.

역할 소스	설명
맞춤형	ONTAP 관리자는 사용자 지정 역할을 만들 수 있습니다. 이러한 역할은 특정 환경 및 보안 요구 사항에 맞게 조정할 수 있습니다.
내장	맞춤형 역할을 통해 더 많은 유연성을 제공할 뿐만 아니라, 클러스터 및 SVM 레벨에서 모두 사용할 수 있는 기본 제공 역할 세트가 있습니다. 이러한 역할은 미리 정의되어 있으며 일반적인 관리 작업에 사용할 수 있습니다.

역할 매핑 및 ONTAP 처리

사용 중인 ONTAP 릴리즈에 따라 전체 또는 거의 모든 REST API 호출이 하나 이상의 CLI 명령에 매핑됩니다. REST 역할을 만들면 기존 또는 레거시 역할도 만들어집니다. 이 * Mapped * 기존 역할은 해당 CLI 명령을 기반으로 하며 조작하거나 변경할 수 없습니다.



역 역할 매핑은 지원되지 않습니다. 즉, 기존 역할을 생성해도 해당 REST 역할은 발생하지 않습니다.

RBAC 발전 요약

기존 역할은 모든 ONTAP 9 릴리즈에 포함됩니다. 나머지 역할은 나중에 소개되었으며 아래 설명과 같이 발전했습니다.

ONTAP 9.6

REST API는 ONTAP 9.6과 함께 도입되었습니다. 나머지 역할도 이 릴리스에 포함되어 있습니다. 또한 REST 역할을 생성하면 이에 상응하는 기존 역할도 생성됩니다.

ONTAP 9.7 ~ 9.10.1

9.7에서 9.10.1까지의 각 ONTAP 릴리스에는 REST API의 향상된 기능이 포함되어 있습니다. 예를 들어, 각 릴리즈마다 다른 REST 엔드포인트가 추가되었습니다. 그러나 두 역할 유형의 생성 및 관리는 별개였습니다. 또한 ONTAP 9.10.1은 리소스 검증된 엔드포인트인 스냅샷 REST 엔드포인트 `/api/storage/volumes/{vol.uuid}/snapshots`에 대한 REST RBAC 지원을 추가했습니다.

ONTAP 9.11.1

이 릴리즈에서는 REST API를 사용하여 기존 역할을 구성 및 관리할 수 있는 기능이 추가되었습니다. REST 역할에 대한 추가 액세스 레벨도 추가되었습니다.

역할 및 사용자 작업

기본적인 RBAC 기능을 이해한 후에는 ONTAP 역할 및 사용자 작업을 시작할 수 있습니다.



을 참조하십시오 ["RBAC 워크플로"](#) ONTAP REST API를 사용하여 역할을 생성하고 사용하는 방법의 예를 참조하십시오.

관리 액세스

REST API 또는 명령줄 인터페이스를 통해 ONTAP 역할을 생성하고 관리할 수 있습니다. 액세스 세부 정보는 아래에 설명되어 있습니다.

REST API

RBAC 역할 및 사용자 계정으로 작업할 때 사용할 수 있는 여러 엔드포인트가 있습니다. 표의 처음 4개는 역할을 만들고 관리하는 데 사용됩니다. 마지막 두 가지는 사용자 계정을 만들고 관리하는 데 사용됩니다.



온라인으로 ONTAP에 액세스할 수 있습니다 ["API 참조입니다"](#) API 사용 방법의 예를 포함한 자세한 내용은 설명서를 참조하십시오.

엔드포인트	설명
<code>/security/roles'</code>	이 끝점을 사용하면 새 REST 역할을 만들 수 있습니다. ONTAP 9.11.1부터 기존 역할을 만들 수도 있습니다. 이 경우 ONTAP는 입력 매개 변수를 기반으로 역할 유형을 결정합니다. 정의된 역할 목록을 검색할 수도 있습니다.
<code>/security/roles/{owner.UUID}/{name}'</code>	특정 클러스터 또는 SVM 범위 역할을 검색하거나 삭제할 수 있습니다. UUID 값은 역할이 정의된 SVM(클러스터 또는 데이터 SVM)을 식별합니다. 이름 값은 역할의 이름입니다.

엔드포인트	설명
'/security/roles/{owner.UUID}/{name}/Privileges'	이 끝점을 사용하면 특정 역할에 대한 권한을 구성할 수 있습니다. 기본 제공 역할은 검색할 수 있지만 업데이트할 수는 없습니다. 자세한 내용은 ONTAP 릴리스의 API 참조 설명서를 참조하십시오.
'/security/roles/{owner.UUID}/{name}/Privileges/[path]'	특정 권한에 대한 액세스 수준 및 선택적 쿼리 값을 검색, 수정 및 삭제할 수 있습니다. 자세한 내용은 ONTAP 릴리스의 API 참조 설명서를 참조하십시오.
'/security/accounts'	이 엔드포인트를 사용하면 새 클러스터 또는 SVM 범위 사용자 계정을 생성할 수 있습니다. 계정이 작동하기 전에 몇 가지 유형의 정보를 포함시키거나 추가해야 합니다. 정의된 사용자 계정 목록을 검색할 수도 있습니다.
'/security/accounts/{owner.UUID}/{name}'	특정 클러스터 또는 SVM 범위 사용자 계정을 검색, 수정, 삭제할 수 있습니다. UUID 값은 사용자가 정의된 SVM(클러스터 또는 데이터 SVM)을 식별합니다. 이름 값은 계정의 이름입니다.

명령줄 인터페이스입니다

관련 ONTAP CLI 명령어는 다음과 같다. 모든 명령은 클러스터 수준에서 관리자 계정을 통해 액세스합니다.

명령	설명
보안 로그인	사용자 로그인을 만들고 관리하는 데 필요한 명령이 들어 있는 디렉토리입니다.
보안 로그인 REST 역할	사용자 로그인과 관련된 REST 역할을 생성하고 관리하는 데 필요한 명령이 들어 있는 디렉토리입니다.
'보안 로그인 역할	이 디렉터리는 사용자 로그인과 관련된 기존 역할을 만들고 관리하는 데 필요한 명령이 들어 있는 디렉토리입니다.

역할 정의

나머지 역할과 기존 역할은 일련의 특성을 통해 정의됩니다.

소유자 및 범위

역할은 ONTAP 클러스터 또는 클러스터 내의 특정 데이터 SVM에서 소유할 수 있습니다. 또한 소유자는 역할의 범위를 암시적으로 결정합니다.

고유한 이름입니다

모든 역할은 범위 내에서 고유한 이름을 가져야 합니다. 클러스터 역할의 이름은 ONTAP 클러스터 수준에서 고유해야 하며 SVM 역할은 특정 SVM 내에서 고유해야 합니다.



새로운 REST 역할의 이름은 기존 역할과 REST 역할 사이에서 고유해야 합니다. REST 역할을 생성하면 이름이 같은 새로운 기존 `_mapping_role`도 생성되기 때문입니다.

권한 집합

모든 역할에는 하나 이상의 권한이 포함됩니다. 각 권한은 특정 리소스 또는 명령과 연결된 액세스 레벨을 식별합니다.

권한

역할에는 하나 이상의 권한이 포함될 수 있습니다. 각 권한 정의는 튜플이며 특정 리소스 또는 작업에 대한 액세스 수준을 설정합니다.

리소스 경로입니다

리소스 경로는 REST 엔드포인트 또는 CLI 명령/명령 디렉토리 경로로 식별됩니다.

REST 엔드포인트

API 끝점이 REST 역할의 대상 리소스를 식별했습니다.

CLI 명령

CLI 명령은 기존 역할의 타겟을 식별합니다. 명령 디렉토리를 지정할 수도 있습니다. 그러면 ONTAP CLI 계층에 모든 다운로드 명령이 포함됩니다.

액세스 수준

액세스 수준은 특정 리소스 경로 또는 명령에 대한 역할의 액세스 유형을 정의합니다. 액세스 수준은 사전 정의된 키워드 집합을 통해 식별됩니다. 세 가지 액세스 수준이 ONTAP 9.6에 도입되었습니다. 기존 역할과 REST 역할 모두에 사용할 수 있습니다. 또한 ONTAP 9.11.1을 사용하여 세 가지 새로운 액세스 수준이 추가되었습니다. 이러한 새로운 액세스 수준은 REST 역할에만 사용할 수 있습니다.



액세스 수준은 CRUD 모델을 따릅니다. REST에서는 기본 HTTP 메서드(POST, GET, 패치, 삭제)를 기반으로 합니다. 해당 CLI 작업은 일반적으로 REST 작업(생성, 표시, 수정, 삭제)에 매핑됩니다.

액세스 수준	Rest 프리미티브	추가되었습니다	REST 역할만 해당
없음	해당 없음	9.6	아니요
읽기 전용	가져오기	9.6	아니요
모두	다운로드, POST, 패치, 삭제	9.6	아니요
read_create 를 참조하십시오	POST를 완료합니다	9.11.1	예
read_modify 를 참조하십시오	패치	9.11.1	예
READ_CREATE_MODIFY를 참조하십시오	GET, POST, 패치	9.11.1	예

선택적 쿼리입니다

기존 역할을 만들 때 * query * 값을 선택적으로 포함하여 명령 또는 명령 디렉터리에 적용할 수 있는 개체의 하위 집합을 식별할 수 있습니다.

기본 제공 역할 요약

ONTAP에는 클러스터 또는 SVM 레벨에서 사용할 수 있는 사전 정의된 여러 역할이 포함되어 있습니다.

클러스터 범위 역할

클러스터 범위에는 몇 가지 기본 제공 역할이 있습니다.

을 참조하십시오 ["클러스터 관리자를 위한 사전 정의된 역할"](#) 를 참조하십시오.

역할	설명
관리자	이 역할을 가진 관리자는 제한되지 않은 권한을 가지고 있으며 ONTAP 시스템에서 모든 작업을 수행할 수 있습니다. 모든 클러스터 레벨 및 SVM 레벨 리소스를 구성할 수 있습니다.
AutoSupport	이는 AutoSupport 계정에 맞게 조정된 특수 역할입니다.
백업	시스템을 백업해야 하는 백업 소프트웨어에 대한 특수 역할입니다.
SnapLock	이는 SnapLock 계정에 맞게 조정된 특수 역할입니다.
읽기 전용	이 역할을 가진 관리자는 클러스터 수준에서 모든 항목을 볼 수 있지만 변경할 수는 없습니다.
없음	관리 기능은 제공되지 않습니다.

SVM 범위 역할

SVM 범위에는 여러 가지 기본 제공 역할이 있습니다. vsadmin * 은 가장 일반적이고 강력한 기능에 대한 액세스를 제공합니다. 다음과 같은 특정 관리 작업에 맞게 조정된 추가 역할이 몇 가지 있습니다.

- vsadmin - 볼륨
- vsadmin - 프로토콜
- vsadmin - 백업
- vsadmin - SnapLock
- vsadmin - 읽기 전용입니다

을 참조하십시오 ["SVM 관리자를 위한 사전 정의된 역할"](#) 를 참조하십시오.

역할 유형 비교

REST * 역할 또는 * 기존 * 역할을 선택하기 전에 차이점을 알고 있어야 합니다. 두 역할 유형을 비교할 수 있는 몇 가지 방법은 아래에 설명되어 있습니다.



고급 또는 복잡한 RBAC 사용 사례의 경우 일반적으로 기존 역할을 사용해야 합니다.

사용자가 ONTAP에 액세스하는 방법

역할을 생성하기 전에 사용자가 ONTAP 시스템에 액세스하는 방법을 알아야 합니다. 이를 바탕으로 역할 유형을 결정할 수 있습니다.

액세스	추천 유형입니다
REST API만 해당	REST 역할은 REST API와 함께 사용하도록 설계되었습니다.
REST API 및 CLI	REST 역할을 정의하여 이에 상응하는 기존 역할을 생성할 수도 있습니다.
CLI만 해당됩니다	기존 역할을 생성할 수 있습니다.

REST 역할에 대해 정의된 액세스 경로는 REST 엔드포인트를 기반으로 합니다. 기존 역할의 액세스 경로는 CLI 명령 또는 명령 디렉토리를 기반으로 합니다. 또한 선택적 쿼리 매개 변수를 기존 역할과 함께 포함하여 명령 매개 변수 값에 따라 액세스를 추가로 제한할 수 있습니다.

나머지 리소스 요약

자원 범주 개요

ONTAP REST API를 통해 사용 가능한 리소스는 범주로 구성됩니다. 각 리소스 범주에는 간단한 설명과 함께 필요에 따라 추가적인 사용 고려 사항이 포함되어 있습니다.

요약에 설명된 나머지 리소스는 제품의 최신 버전을 기반으로 합니다. 이전 릴리스의 변경 사항에 대한 자세한 내용은 을 참조하십시오 ["ONTAP REST API의 새로운 기능"](#) 뿐만 아니라 ["ONTAP 릴리즈 노트"](#).



나머지 대부분의 끝점에서는 UUID 키를 경로 문자열의 일부로 포함하여 특정 개체 인스턴스를 액세스할 수 있습니다. 그러나 대부분의 경우 쿼리 매개 변수의 속성 값을 사용하여 개체에 액세스할 수도 있습니다.

관련 정보

- ["API 참조입니다"](#)

응용 프로그램

이러한 API 호출을 사용하여 ONTAP 응용 프로그램 리소스를 관리할 수 있습니다.

애플리케이션 스냅샷

애플리케이션은 언제든지 생성 또는 복구할 수 있는 스냅샷 복사본을 지원합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

응용 프로그램

ONTAP 애플리케이션은 템플릿, 애플리케이션, 구성 요소, 스냅샷 복사본을 포함한 유형에 따라 정렬됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

정합성 보장 그룹

정합성 보장 그룹은 스냅샷과 같은 특정 작업을 수행할 때 함께 그룹화되는 볼륨 세트입니다. 이 기능은 단일 볼륨 작업에서 동일한 충돌 일관성 및 데이터 무결성을 단일 볼륨 작업으로 확장합니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었으며 9.12로 업데이트되었습니다. ONTAP 9.13을 사용하여 메트릭 성능 및 용량 데이터를 검색하는 엔드포인트가 추가되었습니다.

정합성 보장 그룹 스냅샷

이러한 엔드포인트를 사용하여 일관성 그룹의 스냅샷을 복사, 생성, 인벤토리 및 복원할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

클라우드

이러한 API 호출을 사용하여 클라우드의 오브젝트 스토리지 리소스에 대한 연결을 관리할 수

있습니다.

타겟

타겟은 클라우드의 오브젝트 스토리지 리소스를 나타냅니다. 각 타겟에는 스토리지 리소스에 연결하는 데 필요한 구성 정보가 포함되어 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

클러스터

이러한 API 호출을 사용하여 ONTAP 클러스터와 관련 리소스를 관리할 수 있습니다.

용량 풀

용량 풀 라이선스 모델을 사용하면 공유 풀에서 각 클러스터 노드의 스토리지 용량을 라이선스할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

새시

새시는 클러스터를 지원하는 하드웨어 프레임워크입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

클러스터

ONTAP 클러스터에는 하나 이상의 노드와 스토리지 시스템을 정의하는 관련 구성 설정이 포함되어 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

카운터 테이블

ONTAP에 대한 다양한 통계 정보는 Counter Manager 서브시스템에서 캡처됩니다. 이 정보에 액세스하여 시스템 성능을 평가할 수 있습니다. 이 리소스 유형은 ONTAP 9.11에서 소개되었습니다.

펌웨어

펌웨어 업데이트 요청의 기록을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

작업

비동기 REST API 요청은 작업에 의해 고정된 백그라운드 작업을 사용하여 수행됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

사용권 인스턴스

각 라이선스는 별도의 패키지로 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

라이선스 관리자

ONTAP 클러스터와 연결된 각 라이선스 관리자 인스턴스와 관련된 구성 및 기타 정보를 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

추가 수익 실적

라이선스를 통해 특정 ONTAP 기능을 구현할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

중개자

중재자 인스턴스 추가 또는 제거를 포함하여 MetroCluster와 관련된 중재자를 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

MetroCluster

스위치오버 또는 스위치백 작업 실행을 비롯한 MetroCluster 배포를 생성하고 관리할 수 있습니다. 이 리소스 유형은

ONTAP 9.8에서 새롭게 추가되었으며 9.11로 업데이트되었습니다.

MetroCluster 진단 프로그램

MetroCluster 배포에서 진단 작업을 수행하고 결과를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

MetroCluster DR 그룹

MetroCluster DR 그룹과 관련된 작업을 수행할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

MetroCluster 상호 연결

MetroCluster 상호 연결 상태를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

MetroCluster 노드

MetroCluster 배포에서 개별 노드의 상태를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

MetroCluster 작업

MetroCluster 구성에 대해 최근에 실행된 작업의 목록을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

MetroCluster SVM

MetroCluster 구성에서 모든 SVM 쌍에 대한 정보를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

노드

ONTAP 클러스터는 하나 이상의 노드로 구성됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

NTP 키

NTP(네트워크 시간 프로토콜)는 ONTAP와 신뢰할 수 있는 외부 NTP 시간 서버 간에 공유 개인 키를 사용하도록 구성할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

NTP 서버

이러한 API 호출을 사용하여 외부 NTP 서버 및 키를 비롯한 ONTAP 네트워크 시간 프로토콜 설정을 구성할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

동료

피어 객체는 엔드포인트를 나타내고 클러스터 피어링 관계를 지원합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

성능 카운터

이전 ONTAP 릴리즈에서는 시스템의 작동 특성에 대한 통계 정보를 유지했습니다. 9.11.1 릴리스와 함께 정보가 향상되어 이제 REST API를 통해 사용할 수 있습니다. 이 기능은 ONTAP REST API를 Data ONTAP API(ONTAPI 또는 ZAPI)와 패리티에 더 가깝게 만듭니다. 이 자원 유형은 ONTAP 9.11에서 소개되었습니다.

리소스 태그

태그를 사용하여 REST API 리소스를 그룹화할 수 있습니다. 이렇게 하면 특정 프로젝트 또는 조직 그룹 내의 관련 자원을 연결할 수 있습니다. 태그를 사용하면 리소스를 보다 효율적으로 구성 및 추적할 수 있습니다. 이 리소스 유형은 ONTAP 9.13에서 도입되었습니다.

스케줄

일정을 사용하여 작업 수행을 자동화할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

센서

이러한 끝점을 사용하여 모든 플랫폼 환경 센서에 대한 세부 정보를 검색할 수 있습니다. 이 자원 유형은 ONTAP 9.11에서 소개되었습니다.

소프트웨어

ONTAP 클러스터에는 클러스터 소프트웨어 프로필, 소프트웨어 패키지 컬렉션, 소프트웨어 기록 컬렉션이 포함됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

웹

이러한 끝점을 사용하여 웹 서비스 구성을 업데이트하고 현재 구성을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

네임 서비스

이러한 API 호출을 사용하여 ONTAP에서 지원하는 이름 서비스를 관리할 수 있습니다.

캐시

ONTAP 이름 서비스는 캐싱을 지원하여 성능과 복원력을 높입니다. 이제 REST API를 통해 이름 서비스 캐시를 구성할 수 있습니다. 호스트, UNIX 사용자, UNIX 그룹 및 넷그룹을 비롯한 여러 레벨에서 설정을 적용할 수 있습니다. 이 자원 유형은 ONTAP 9.11에서 소개되었습니다.

DDNS

DDNS(동적 DNS) 정보를 표시하고 DDNS 하위 시스템을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

DNS

DNS는 네트워크에서 ONTAP 클러스터의 통합을 지원합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.13으로 개선되었습니다.

호스트 레코드입니다

이러한 끝점을 사용하면 지정된 호스트 이름의 IP 주소와 IP 주소의 호스트 이름을 표시할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

LDAP를 지원합니다

LDAP 서버를 사용하여 사용자 정보를 유지할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

LDAP 스키마

ONTAP에서 사용하는 LDAP 스키마를 생성, 수정 및 나열할 수 있습니다. 4개의 기본 스키마가 포함되어 있습니다. 이 자원 유형은 ONTAP 9.11에서 소개되었습니다.

로컬 호스트

이러한 끝점을 사용하여 호스트 이름에 대한 로컬 매핑을 표시하고 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

이름 매핑

이름 매핑을 사용하면 이름 도메인의 ID를 다른 이름 도메인으로 매핑할 수 있습니다. 예를 들어 CIFS에서 UNIX로,

Kerberos에서 UNIX로, UNIX에서 CIFS로 ID를 매핑할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

넷그룹 파일

넷그룹 파일 세부 정보를 검색하고 SVM용 파일을 삭제할 수 있습니다. 이 자원 유형은 ONTAP 9.11에서 소개되었습니다.

NIS를 선택합니다

NIS 서버를 사용하여 사용자 및 클라이언트 워크스테이션을 인증할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

Unix 사용자 및 그룹

로컬 UNIX 사용자 및 그룹은 이전 ONTAP 릴리즈의 일부였습니다. 그러나 이제 REST API에 지원이 추가되어 사용자와 그룹을 표시하고 관리할 수 있습니다. 이러한 REST 리소스 유형은 ONTAP 9.9에 도입되었으며 ONTAP 9.10으로 크게 향상되었습니다.

NAS

이러한 API 호출을 사용하여 클러스터와 SVM에 대한 CIFS 및 NFS 설정을 관리할 수 있습니다.

Active Directory를 클릭합니다

ONTAP 클러스터에 대해 정의된 Active Directory 계정을 관리할 수 있습니다. 여기에는 새 계정 만들기 및 계정 표시, 업데이트 및 삭제 작업이 포함됩니다. 이 지원은 ONTAP 9.12에 추가되었습니다.

감사

SVM에 대해 특정 CIFS 및 NFS 이벤트를 로깅하여 보안을 강화할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

감사 로그 리디렉션

NAS 감사 이벤트를 특정 SVM으로 리디렉션할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

CIFS 접속

설정된 CIFS 접속 목록을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

CIFS 도메인입니다

CIFS 도메인에 대한 지원이 클러스터 및 SVM 레벨에서 다양한 유형의 엔드포인트로 추가되었습니다. 도메인 구성을 검색할 뿐만 아니라 기본 도메인 컨트롤러를 만들고 제거할 수도 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었으며 ONTAP 9.13으로 향상되었습니다.

CIFS 그룹 정책입니다

CIFS 그룹 정책의 생성 및 관리를 지원하기 위해 엔드포인트가 추가되었습니다. 구성 정보는 모든 또는 특정 SVM에 적용되는 그룹 정책 개체를 통해 사용 및 관리됩니다. 이 지원은 ONTAP 9.12에 추가되었습니다.

CIFS 홈 디렉토리 검색 경로입니다

CIFS 서버의 SMB 사용자에게 대한 홈 디렉토리는 각 사용자에게 대한 개별 SMB 공유를 생성하지 않고 생성할 수 있습니다. 홈 디렉토리 검색 경로는 SVM 루트에서 연결되는 절대 경로 집합입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

CIFS 로컬 그룹

CIFS 서버는 공유, 파일 및 디렉토리 액세스 권한을 결정할 때 인증에 로컬 그룹을 사용할 수 있습니다. 이 리소스 유형은 ONTAP 9.9에서 도입되었으며 ONTAP 9.10으로 크게 확장되었습니다.

CIFS NetBIOS입니다

클러스터의 NetBIOS 연결에 대한 정보를 표시할 수 있습니다. 세부 정보에는 IP 주소 및 등록된 NetBIOS 이름이 포함됩니다. 이 정보는 이름 확인 문제를 해결하는 데 도움이 될 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

CIFS 서비스

CIFS 서버의 핵심 구성입니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다.

CIFS 세션 파일

여러 필터링 옵션을 기반으로 CIFS 세션에 대해 열려 있는 파일 목록을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

CIFS 세션

이 API를 사용하여 CIFS 세션에 대한 자세한 정보를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8 REST API에 도입되었으며 ONTAP 9.9로 향상되었습니다.

CIFS 새도 복사본

Microsoft 원격 볼륨 새도 복사본 서비스는 기존 Microsoft VSS 기능의 확장입니다. VSS 기능을 확장하여 SMB 공유의 새도우 복제를 지원합니다. 이 기능은 이제 ONTAP REST API를 통해 사용할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

CIFS 공유

CIFS 서버에 정의된 SMB 공유입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

CIFS는 **ACL**을 공유합니다

CIFS 공유의 폴더 및 파일에 대한 액세스를 제어하는 ACL(액세스 제어 목록)입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

CIFS UNIX symlink 매핑

CIFS와 UNIX 클라이언트 모두 동일한 데이터 저장소를 액세스할 수 있습니다. UNIX 클라이언트가 심볼 링크를 생성할 때 이러한 매핑은 CIFS 클라이언트를 지원하기 위해 다른 파일 또는 폴더에 대한 참조를 제공합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

CIFS 사용자 및 그룹 대량 가져오기

새로운 REST API 엔드포인트를 사용하여 CIFS 로컬 사용자, 그룹 및 그룹 구성원 정보를 대량으로 가져올 수 있을 뿐 아니라 요청 상태를 모니터링할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

파일 액세스 추적

이러한 API 호출을 사용하여 특정 파일에 대한 액세스를 추적할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

파일 보안 권한

이러한 API 호출을 사용하면 특정 파일이나 폴더에 대해 Windows 또는 Unix 사용자에게 부여된 유효한 권한을 표시할 수 있습니다. NTFS 파일 보안 및 감사 정책을 관리할 수도 있습니다. 이 리소스 유형은 ONTAP 9.8 REST API에 도입되었으며 ONTAP 9.9로 대폭 향상되었습니다.

FPolicy를 참조하십시오

FPolicy는 SVM에서 파일 액세스 이벤트를 모니터링 및 관리하는 데 사용되는 파일 액세스 알림 프레임워크입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

FPolicy 연결

이러한 엔드포인트를 사용하면 외부 FPolicy 서버의 연결 상태 정보를 표시하고 업데이트할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

FPolicy 엔진

FPolicy 엔진을 사용하여 파일 액세스 알림을 받는 외부 서버를 식별할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

FPolicy 이벤트

파일 액세스를 모니터링하는 방법 및 생성되는 이벤트를 식별하는 구성입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

FPolicy 영구 저장소

ONTAP FPolicy 구성 및 이벤트에 대한 영구 저장소를 구성하고 관리할 수 있습니다. 각 SVM에는 SVM 내 여러 정책에 대해 공유되는 하나의 영구 저장소가 있을 수 있습니다. 이 리소스 유형은 ONTAP 9.14에 도입되었습니다.

FPolicy 정책

FPolicy 엔진 및 이벤트를 포함한 FPolicy Framework의 요소에 대한 컨테이너입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

잠금

잠금은 여러 클라이언트가 동시에 같은 파일에 액세스하는 파일에 대한 동시 액세스에 제한을 적용하는 동기화 메커니즘입니다. 이러한 끝점을 사용하여 잠금을 검색하고 삭제할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

NFS 연결 클라이언트 맵

연결된 클라이언트에 대한 NFS 맵 정보는 새 엔드포인트를 통해 사용할 수 있습니다. 노드, SVM, IP 주소에 대한 세부 정보를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

NFS 연결 클라이언트

연결된 클라이언트 목록을 해당 연결 세부 정보와 함께 표시할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

NFS 익스포트 정책

NFS 익스포트를 설명하는 규칙을 포함한 정책입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

NFS Kerberos 인터페이스

Kerberos 인터페이스에 대한 구성 설정입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

NFS Kerberos 영역

Kerberos 영역의 구성 설정입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

TLS를 통한 NFS

이 리소스를 사용하면 TLS를 통한 NFS를 사용할 때 인터페이스 구성을 검색하고 업데이트할 수 있습니다. 이 리소스 유형은 ONTAP 9.15에 도입되었습니다.

NFS 서비스

NFS 서버의 핵심 구성입니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다.

오브젝트 저장소

S3 이벤트에 대한 감사는 특정 S3 이벤트를 추적하고 기록할 수 있는 보안 개선입니다. S3 감사 이벤트 선택기는 버킷당 SVM 단위로 설정할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

Vscan

바이러스 및 기타 악성 코드로부터 데이터를 보호하는 보안 기능입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

Vscan 온액세스 정책

Vscan 정책을 통해 클라이언트가 액세스할 때 파일 개체를 능동적으로 스캔할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

Vscan 주문형 정책

Vscan 정책을 사용하면 필요에 따라 또는 정해진 일정에 따라 파일 개체를 즉시 스캔할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

Vscan 스캐너 풀

ONTAP와 외부 바이러스 검사 서버 간의 연결을 관리하는 데 사용되는 일련의 속성입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

Vscan 서버 상태

외부 바이러스 검사 서버의 상태입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

NDMP

이러한 API 호출을 사용하여 NDMP 서비스를 관리할 수 있습니다.

NDMP 모드입니다

NDMP 운영 모드는 SVM 범위 또는 노드 범위가 될 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

NDMP 노드

노드의 NDMP 구성을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

NDMP 세션

특정 SVM 또는 노드에 대한 NDMP 세션 세부 정보를 검색하고 삭제할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

NDMP SVM

SVM의 NDMP 구성을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

NDMP SVM 사용자 암호

SVM 콘텐츠 내에서 특정 NDMP 사용자의 암호를 생성하고 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8 REST API에 도입되었으며 ONTAP 9.9로 향상되었습니다.

네트워킹

이러한 API 호출을 사용하여 클러스터와 함께 사용되는 물리적 및 논리적 네트워킹 리소스를 관리할 수 있습니다.

BGP 피어 그룹

Border Gateway Protocol 피어 그룹을 만들고 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

이더넷 브로드캐스트 도메인

이더넷 브로드캐스트 도메인은 동일한 물리적 네트워크에 속하는 것으로 보이는 물리적 포트 집합입니다. 모든 포트는 도메인의 포트 중 하나에서 브로드캐스트될 때 패킷을 수신합니다. 각 브로드캐스트 도메인은 IPspace의 일부입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

이더넷 포트

이더넷 포트는 물리적 또는 가상 네트워킹 엔드포인트입니다. 포트를 LAG(Link Aggregate Group)로 결합하거나 VLAN(Virtual LAN)을 사용하여 분리할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

이더넷 스위치 포트

이더넷 스위치의 포트 정보를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

이더넷 스위치

ONTAP 클러스터 또는 스토리지 네트워크에 사용되는 이더넷 스위치의 구성을 검색하거나 수정할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새롭게 추가되었으며 9.11로 업데이트되었습니다.

파이버 채널 패브릭

FC(파이버 채널) 패브릭 REST API 엔드포인트를 사용하여 FC 네트워크에 대한 정보를 검색할 수 있습니다. 여기에는 ONTAP 클러스터와 FC 패브릭 간 연결, 패브릭을 구성하는 스위치 및 활성 zoneset의 영역이 포함됩니다. 이 자원 유형은 ONTAP 9.11에서 소개되었습니다.

파이버 채널 인터페이스

파이버 채널 인터페이스는 SVM과 관련된 논리 엔드포인트입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다. ONTAP 9.14에 성능 메트릭 데이터 검색에 대한 지원이 추가되었습니다.

파이버 채널 포트

Fibre Channel 포트는 Fibre Channel 네트워크에 연결하는 데 사용되는 ONTAP 노드의 물리적 어댑터입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다. ONTAP 9.14에 성능 메트릭 데이터 검색에 대한 지원이 추가되었습니다.

HTTP 프록시

SVM 또는 클러스터 IPspace에 대해 HTTP 프록시를 구성할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

IP 인터페이스

논리 인터페이스(LIF)는 추가 구성 특성을 가진 IP 주소입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

IP 라우트

라우팅 테이블은 트래픽을 목적지로 전달하는 데 사용되는 IP 라우트의 모음입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

IP 서비스 정책

IP 서비스 정책은 특정 LIF에서 사용 가능한 서비스를 정의합니다. 서비스 정책은 SVM 또는 IPspace의 컨텍스트 내에서 구성할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

IP 서브넷

ONTAP 네트워킹 기능이 IP 서브넷을 지원하도록 확장되었습니다. REST API를 사용하면 ONTAP 클러스터 내에서 IP 서브넷의 구성 및 관리에 액세스할 수 있습니다. 이 자원 유형은 ONTAP 9.11에서 소개되었습니다.

IPspace

IPspace는 하나 이상의 SVM을 지원하는 네트워킹 공간을 생성합니다. IPspace를 상호 격리하여 보안 및 개인 정보 보호를 제공할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

NVMe를 참조하십시오

이러한 API 호출을 사용하여 비휘발성 메모리 익스프레스(NVMe)를 지원하는 리소스를 관리할 수 있습니다.

Fibre Channel 로그인

Fibre Channel 로그인 은 ONTAP에 로그인한 Fibre Channel 이니시에이터가 구성한 접속을 나타냅니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

네임스페이스

NVMe 네임스페이스는 NVMe over Fabrics 프로토콜을 사용하여 SVM에 연결된 호스트에 제공되는 주소 지정 가능한 논리 블록의 모음입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다. ONTAP 9.14에 성능 메트릭 데이터 검색에 대한 지원이 추가되었습니다.

NVMe 인터페이스

NVMe 인터페이스는 NVMe-oF(NVMe over Fabrics) 프로토콜을 지원하도록 구성된 네트워크 인터페이스입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

NVMe 서비스

NVMe 서비스는 SVM을 위한 NVMe 컨트롤러 타겟의 속성을 정의합니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다. ONTAP 9.14에 성능 메트릭 데이터 검색에 대한 지원이 추가되었습니다.

NVMe 하위 시스템 컨트롤러

NVMe 하위 시스템 컨트롤러는 호스트와 스토리지 솔루션 간의 동적 연결을 나타냅니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

NVMe 하위 시스템 맵

NVMe 하위 시스템 맵은 NVMe 서브시스템과 NVMe 네임스페이스를 연관한 것입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

NVMe 하위 시스템

NVMe 하위 시스템은 NVMe 연결 호스트 세트에 대한 구성 상태 및 네임스페이스 액세스 제어를 유지합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

오브젝트 저장소

이러한 API 호출을 사용하여 S3 기반 오브젝트 스토리지에 액세스할 수 있습니다.

버킷

버킷은 오브젝트의 컨테이너이며 오브젝트 이름 공간을 사용하여 구성됩니다. 각 S3 오브젝트 서버에는 여러 개의 버킷을 포함할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

서비스

서버 및 버킷 구성을 포함하여 ONTAP S3 구성을 생성 및 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

서비스 버킷

버킷은 오브젝트의 컨테이너이며 오브젝트 이름 공간을 사용하여 구성됩니다. 특정 S3 서버에 대한 버킷을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

S3 버킷 규칙

S3 버킷에는 규칙 정의가 포함될 수 있습니다. 각 규칙은 목록 오브젝트이며 버킷 내의 오브젝트에 대해 수행할 동작 집합을 정의합니다. 이 리소스 유형은 ONTAP 9.13에서 도입되었습니다.

S3 그룹

S3 사용자 그룹을 생성하고 그룹 수준에서 액세스 제어를 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

S3 정책

S3 정책을 만들고 이를 리소스와 연결하여 다양한 권한을 정의할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

사용자

S3 사용자 계정은 S3 서버에서 유지 관리됩니다. 사용자 계정은 키 쌍을 기반으로 하며 자신이 제어하는 버킷과 연결됩니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

산

이러한 API 호출을 사용하여 SAN(Storage Area Networking) 리소스를 관리할 수 있습니다.

Fibre Channel 로그인

Fibre Channel 로그인 ONTAP에 로그인한 Fibre Channel 이니시에이터에 의해 형성된 접속을 나타냅니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

파이버 채널 프로토콜 서비스

FCP(파이버 채널 프로토콜) 서비스는 SVM을 위한 파이버 채널 대상의 속성을 정의합니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다. ONTAP 9.14에 성능 메트릭 데이터 검색에 대한 지원이 추가되었습니다.

파이버 채널 WWPN 별칭

WWPN(World Wide Port Name)은 파이버 채널 포트를 고유하게 식별하는 64비트 값입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

igroup

이니시에이터 그룹(igroup)은 호스트 이니시에이터를 식별하는 파이버 채널 WWPN(전 세계 포트 이름), iSCSI IQN(정규화된 이름) 및 iSCSI EUI(확장된 고유 식별자)의 모음입니다. 이 리소스 유형은 원래 ONTAP 9.6에서 도입되었습니다.

중첩된 igroup은 ONTAP 9.9의 새로운 기능이며 REST API에도 지원이 추가되었습니다. 이 REST 리소스 유형은 ONTAP 9.9에 도입되었습니다.

이니시에이터

이니시에이터는 호스트 엔드포인트를 식별하는 FC(Fibre Channel) WWPN(World Wide Port Name), IQN(iSCSI Qualified Name) 또는 iSCSI EUI(Extended Unique Identifier)입니다. 클러스터 또는 특정 SVM에 대한 이니시에이터를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.14에 도입되었습니다.

iSCSI 자격 증명

iSCSI 자격 증명 객체에는 이니시에이터와 ONTAP에서 사용하는 인증 자격 증명이 포함되어 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

iSCSI 서비스

iSCSI 서비스는 SVM을 위한 iSCSI 타겟의 속성을 정의합니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다. ONTAP 9.14에 성능 메트릭 데이터 검색에 대한 지원이 추가되었습니다.

iSCSI 세션

iSCSI 세션은 iSCSI 이니시에이터와 iSCSI 타겟을 연결하는 하나 이상의 TCP 연결입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

LUN 특성입니다

LUN 특성은 LUN과 함께 선택적으로 저장할 수 있는 호출자 정의 이름/값 쌍입니다. 특성은 적은 양의 애플리케이션별 메타데이터를 저장하는 데 사용할 수 있으며 ONTAP에서 해석되지 않습니다. 엔드포인트를 사용하면 LUN의 특성을 생성, 업데이트, 삭제 및 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

LUN 매핑

LUN 매핑은 LUN과 이니시에이터 그룹 간의 연결입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

LUN은 보고 노드를 매핑합니다

보고 노드는 매핑된 LUN에 대한 네트워크 경로가 ONTAP의 선택적 LUN 맵(SLM) 기능의 일부로 SAN 프로토콜을 사용하여 광고되는 클러스터 노드입니다. 새 엔드포인트를 사용하면 LUN 매핑의 보고 노드를 추가, 제거 및 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

LUN을 클릭합니다

LUN은 SAN(Storage Area Network)에 있는 스토리지의 논리적 표현입니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다. ONTAP 9.14에 성능 메트릭 데이터 검색에 대한 지원이 추가되었습니다.

포트 세트

포트 세트는 _포트셋_ 스토리지 VM과 연결된 Fibre Channel 또는 iSCSI 네트워크 인터페이스의 모음입니다. 이 기능은 이전 릴리스의 ONTAP에 포함되어 있지만 이제 REST API에 지원이 추가되었습니다. 이 REST 리소스 유형은 ONTAP 9.9에 도입되었습니다.

VVol 바인딩

VVol(VMware Virtual Volume) 바인딩은 클래스 "protocol_endpoint"의 LUN과 클래스 "vVol"의 LUN 간의

연관입니다. VVOL 바인딩 REST API를 사용하여 VVOL 바인딩을 생성, 삭제 및 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

보안

이러한 API 호출을 사용하여 클러스터 및 SVM 보안 설정을 관리할 수 있습니다.

계정

클러스터 및 SVM에 대한 사용자 계정 모음이 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

계정 이름입니다

범위가 지정된 사용자 계정의 구성입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

Active Directory 프록시

Active Directory 서버에서 SVM 계정 정보를 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

랜섬웨어 방지

ONTAP는 랜섬웨어 위협이 있을 가능성이 있는 파일을 감지합니다. 여러 종류의 끝점이 있습니다. 이러한 의심되는 파일의 목록을 검색할 수 있을 뿐 아니라 볼륨에서 제거할 수도 있습니다. 이 리소스 유형은 ONTAP 9.10.1에서 도입되었습니다.

감사

감사 로그 파일에 기록되는 내용을 결정하는 설정입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

감사 대상

이러한 설정은 감사 로그 정보가 원격 시스템 또는 Splunk 서버로 전달되는 방식을 제어합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

감사 메시지

감사 로그 메시지를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

AWS KMS

Amazon Web Services에는 키 및 기타 비밀에 대한 보안 저장소를 제공하는 키 관리 서비스가 포함되어 있습니다. REST API를 통해 이 서비스에 액세스하여 ONTAP에서 클라우드에 암호화 키를 안전하게 저장할 수 있습니다. 또한 NetApp Storage Encryption에 사용되는 인증 키를 생성하고 나열할 수 있습니다. 이 지원은 ONTAP 9.12에 새로 추가되었습니다.

Azure 키 저장소

이 API 호출 집합을 사용하면 Azure 키 저장소를 사용하여 ONTAP 암호화 키를 저장할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

인증서

API 호출은 ONTAP에서 사용하는 인증서를 설치, 표시 및 삭제하는 데 사용할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

Cisco 듀오

Duo는 SSH 로그인에 대해 2단계 인증을 제공합니다. Duo가 ONTAP 클러스터 또는 SVM 레벨에서 작동하도록 구성할 수 있습니다. 이 리소스 유형은 ONTAP 9.14에 도입되었습니다.

클러스터 보안

클러스터 전체 보안의 세부 정보를 검색하고 특정 매개 변수를 업데이트할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

GCP KMS

이 API 호출 집합을 사용하면 Google 클라우드 플랫폼 키 관리 서비스를 사용하여 ONTAP 암호화 키를 저장하고 관리할 수 있습니다. 이 리소스 유형은 처음에 ONTAP 9.8 REST API에 도입되었습니다. 그러나 이 기능은 다시 설계되었으므로 ONTAP 9.9에서 새로운 리소스 유형을 사용하는 새로운 기능으로 간주됩니다.

IPsec

IPSec(인터넷 프로토콜 보안)은 기본 IP 네트워크를 통해 두 엔드포인트 간에 보안을 제공하는 프로토콜 모음입니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

IPsec CA 인증서

IPSec CA 인증서를 추가, 제거 및 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 새로 추가되었습니다.

IPsec 정책

이 API 호출 집합을 사용하여 IPSec 배포에 적용되는 정책을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

IPsec 보안 연결

이 API 호출 집합을 사용하여 IPSec 배포에 적용되는 보안 연결을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

키 관리자 구성

이러한 끝점을 사용하면 키 관리자에 대한 구성을 검색하고 업데이트할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 새로 추가되었습니다.

주요 관리자

키 관리자를 사용하면 ONTAP 내의 클라이언트 모듈이 안전하게 저장된 키를 사용할 수 있습니다. 이 리소스 유형은 ONTAP 9.6에 도입되었으며 ONTAP 9.7에 맞게 업데이트되었습니다. 인증 키를 지원하기 위해 ONTAP 9.12가 설치된 또 다른 업데이트가 있습니다. ONTAP 9.13에 복원 기능이 추가되었습니다.

키 저장소

키 저장소는 키 관리자의 유형을 설명합니다. 이 리소스 유형은 ONTAP 9.10에 새로 추가되었습니다. ONTAP 9.14에는 향상된 제어를 지원하는 끝점이 추가되었습니다.

LDAP 인증

이러한 API 호출은 클러스터 LDAP 서버 구성을 검색하고 관리하는 데 사용됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

로그인 메시지

ONTAP에서 사용하는 로그인 메시지를 표시하고 관리하는 데 사용됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

여러 관리자 검증

여러 관리자 확인 기능은 ONTAP 명령 또는 작업에 대한 액세스를 보호하기 위한 유연한 인증 프레임워크를 제공합니다. 다음 영역에서 액세스 정의, 요청 및 승인을 지원하는 새로운 엔드포인트가 17개 있습니다.

- 규칙
- 요청
- 승인 그룹

여러 관리자가 액세스를 승인할 수 있는 옵션을 제공하면 ONTAP 및 IT 환경의 보안이 향상됩니다. 이러한 자원 유형은 ONTAP 9.11에서 소개되었습니다.

NIS 인증

이러한 설정은 클러스터 NIS 서버 구성을 검색하고 관리하는 데 사용됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

OAuth 2.0 을 참조하십시오

OAuth 2.0(Open Authorization)은 ONTAP 스토리지 리소스에 대한 액세스를 제한하는 데 사용할 수 있는 토큰 기반 프레임워크입니다. REST API를 통해 ONTAP에 액세스하는 클라이언트와 함께 사용할 수 있습니다. REST API를 포함한 모든 ONTAP 관리 인터페이스를 사용하여 구성을 수행할 수 있습니다. 이 리소스 유형은 ONTAP 9.14에 도입되었습니다.

암호 인증

여기에는 사용자 계정의 암호를 변경하는 데 사용되는 API 호출도 포함됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

역할 인스턴스에 대한 권한입니다

특정 역할에 대한 권한을 관리합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

공개 키 인증

이러한 API 호출을 사용하여 사용자 계정에 대한 공개 키를 구성할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

역할

역할은 사용자 계정에 권한을 할당하는 방법을 제공합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

역할 인스턴스

역할의 특정 인스턴스입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

SAML 서비스 공급자

SAML 서비스 공급자의 구성을 표시하고 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

SSH를 클릭합니다

이러한 통화를 통해 SSH 구성을 설정할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

SSH SVM

이러한 엔드포인트를 사용하면 모든 SVM에 대한 SSH 보안 구성을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

TOTPS 를 참조하십시오

REST API를 사용하여 로그인 계정에 대해 TOTP(Time-Based One-Time Password) 프로필을 구성하고 SSH를 사용하여 ONTAP에 액세스할 수 있습니다. 이 리소스 유형은 ONTAP 9.13에서 도입되었습니다.

SnapLock

이러한 API 호출을 사용하여 ONTAP SnapLock 기능을 관리할 수 있습니다.

로그

SnapLock 로그 구조는 로그 레코드가 포함된 특정 볼륨의 디렉토리와 파일을 기반으로 합니다. 로그 파일은 최대 로그 크기에 따라 채워지고 보관됩니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

규정 준수 시계

준수 클록은 SnapLock 객체의 만료 시간을 결정합니다. 시계를 REST API 외부에서 초기화해야 하며 변경할 수 없습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

이벤트 보존

EBR(SnapLock 이벤트 기반 보존) 기능을 사용하여 이벤트 발생 후 파일이 유지되는 기간을 정의할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

파일 보존 및 권한 삭제

SnapLock에서 생성된 파일의 보존 시간을 관리할 수 있습니다. 필요한 경우 SnapLock 엔터프라이즈 볼륨에서 만료되지 않은 WORM 파일을 삭제할 수도 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.



삭제 작업을 실행할 수 있는 유일한 내장 역할은 vsadmin-SnapLock입니다.

파일 지문

유형 및 만료 날짜와 같은 파일 및 볼륨을 설명하는 핵심 정보를 보고 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

법적 증거 자료 보관

이러한 API 호출을 사용하여 소송 프로세스의 일부인 파일을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

SnapMirror를 참조하십시오

이러한 API 호출을 사용하여 SnapMirror 데이터 보호 기술을 관리할 수 있습니다.

정책

SnapMirror 정책은 관계에 적용되고 각 관계의 구성 특성 및 동작을 제어합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

관계

비동기 및 동기 관계 모두 필요한 데이터 전송 연결을 설정합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

관계가 전송됩니다

기존 SnapMirror 관계를 통해 SnapMirror 전송을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

스토리지

이러한 API 호출을 사용하여 물리적 스토리지와 논리적 스토리지를 관리할 수 있습니다.

메트릭을 취합합니다

특정 집계에 대한 기간별 메트릭 데이터를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다.

플렉스를 집계합니다

애그리게이트 내 WAFL 스토리지의 물리적 복사본 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

애그리게이트

Aggregate는 하나 이상의 RAID 그룹으로 구성됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

브리지

클러스터의 브리지를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.9에 도입되었습니다.

디스크

클러스터의 물리적 디스크입니다. 이 리소스 유형은 ONTAP 9.6에 도입되었으며 ONTAP 9.7 및 9.8로 업데이트되었습니다.

파일 클론

이러한 끝점을 사용하여 파일 클론을 만들고, 분할 상태를 검색하고, 분할 로드를 관리할 수 있습니다. 파일 클론 생성 엔드포인트 리소스는 ONTAP 9.6에서 처음 도입되었으며 ONTAP 9.8로 확장되었습니다. ONTAP 9.10으로 다시 크게 확장되었습니다.

파일이 이동합니다

이러한 REST API 엔드포인트를 사용하여 두 FlexVol 볼륨 간 또는 FlexGroup 볼륨 내에서 파일을 이동할 수 있습니다. 요청이 수락되면 진행 상황과 상태를 모니터링할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

FlexCache

이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

FlexCache 원점

FlexCache는 원본 볼륨의 영구 캐시입니다. 이 리소스 유형은 원래 ONTAP 9.6에서 도입되었습니다. HTTP 패치 방법을 통한 수정을 지원하기 위해 ONTAP 9.9 REST API로 지원이 향상되었습니다.

모니터링된 파일

추가 모니터링을 위해 특정 파일을 지정할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

풀

공유 스토리지 풀을 생성하고 클러스터에서 스토리지 풀을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

포트

클러스터의 스토리지 포트입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었으며 ONTAP 9.11.1로 향상되었습니다.

QoS 정책

서비스 품질 정책 구성 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

QoS 옵션

클러스터에 대한 QoS 옵션을 검색하고 설정할 수 있도록 엔드포인트가 도입되었습니다. 예를 들어 백그라운드 작업에 사용 가능한 시스템 처리 리소스의 백분율을 예약할 수 있습니다. 이 리소스 유형은 ONTAP 9.14에 도입되었습니다.

QoS 워크로드

QoS 워크로드는 QoS에서 추적하는 스토리지 개체를 나타냅니다. QoS 워크플로우를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

Qtree

이러한 API 호출을 사용하여 논리적으로 분리된 파일 시스템의 한 유형인 관리 qtree를 호출할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

할당량 보고서

파일 또는 공간 사용을 제한하거나 추적하는 기법인 할당량에 대한 보고 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

할당량 규칙

할당량을 적용하는 데 사용되는 규칙입니다. 이 리소스 유형은 ONTAP 9.6에서 도입되었으며 ONTAP 9.7로 업데이트되었습니다.

셀프

셀프 수: 클러스터 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

스냅샷 정책

스냅샷은 정책에 따라 생성됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

Snapshot 스케줄

스냅샷 스케줄을 제어할 수 있습니다. 이 리소스 유형은 ONTAP 9.8로 새롭게 재설계되었습니다.

스위치

클러스터의 스위치를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.9에 도입되었습니다.

테이프 장치

클러스터에서 테이프 디바이스를 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.9에 도입되었습니다.

가장 중요한 메트릭

상위 메트릭 엔드포인트를 사용하면 특정 메트릭으로 필터링된 볼륨의 활동을 확인할 수 있습니다. 클라이언트, 디렉토리, 파일 및 사용자를 기준으로 필터링을 수행할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

볼륨 효율성 정책

이러한 API 호출을 사용하여 전체 볼륨에 적용되는 효율성을 구성할 수 있습니다. 이 리소스 유형은 ONTAP 9.8에서 새로 추가되었습니다.

볼륨

논리 컨테이너는 클라이언트에 데이터를 제공하는 데 사용됩니다. 이 리소스 유형은 원래 ONTAP 9.6 REST API에서 도입되었습니다. API와 함께 사용되는 많은 매개변수 값이 ONTAP 9.9로 크게 확장되었으며, 여기에는 공간 관리에 사용되는 값이 포함됩니다.

볼륨 파일

볼륨의 특정 디렉토리에 대한 파일 및 디렉토리 목록을 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었으며 ONTAP 9.8로 업데이트되었습니다.

볼륨 스냅샷

볼륨에 대한 스냅샷입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

지원

이러한 API 호출을 사용하여 클러스터를 지원하는 데 사용되는 ONTAP 기능을 관리할 수 있습니다.

응용 프로그램 로그

독립 실행형 응용 프로그램은 POST 요청을 실행하여 ONTAP 시스템에서 EMS 이벤트 및 선택적으로 생성된 AutoSupport 패키지를 기록할 수 있습니다. 이 리소스 유형은 ONTAP 9.11.1에서 도입되었습니다.

자동 업데이트

자동 업데이트 기능은 최신 소프트웨어 업데이트를 다운로드하고 적용하여 ONTAP 시스템을 최신 상태로 유지합니다. 상태, 구성 및 업데이트를 포함하여 기능을 지원하는 여러 끝점 범주가 있습니다. 이러한 리소스 유형은 ONTAP 9.10에 도입되었습니다.

AutoSupport

AutoSupport는 오류와 함께 구성 및 상태 세부 정보를 수집하고 정보를 NetApp에 보고합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

AutoSupport 메시지

각 노드는 생성 및 검색할 수 있는 AutoSupport 메시지를 유지합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

구성 백업

이러한 API를 사용하여 현재 백업 설정을 검색하고 업데이트할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

구성 백업 작업

구성 백업 파일을 생성, 검색 및 삭제할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

코어 덤프

이러한 엔드포인트를 사용하여 클러스터 또는 노드에서 생성한 메모리 코어 덤프를 검색하고 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

있습니다

EMS(이벤트 관리 시스템)는 이벤트를 수집하고 하나 이상의 대상에 알림을 보냅니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

EMS 대상

EMS 대상은 알림을 보내는 방법과 위치를 결정합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

EMS 대상 인스턴스

EMS 대상 인스턴스는 유형 및 위치에 따라 정의됩니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

EMS 이벤트

클러스터에 대한 시스템 이벤트의 실시간 모음입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

EMS 필터

EMS 필터는 추가 처리가 필요한 이벤트를 종합적으로 식별합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

EMS가 인스턴스를 필터링합니다

EMS 필터 인스턴스는 이벤트에 적용되는 규칙의 모음입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

EMS 메시지

EMS 이벤트 카탈로그에 대한 액세스를 제공합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

EMS 역할 구성

EMS 지원 기능을 통해 역할에 할당된 역할 및 액세스 제어 구성을 관리할 수 있습니다. 이렇게 하면 역할 구성에 따라 이벤트 및 메시지를 제한하거나 필터링할 수 있습니다. 이 리소스 유형은 ONTAP 9.13에서 도입되었습니다.

필터 인스턴스에 대한 EMS 규칙

EMS 필터의 특정 인스턴스에 대해 규칙 목록을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

필터 인스턴스에 대한 EMS 규칙 인스턴스입니다

EMS 필터의 특정 인스턴스에 대한 개별 규칙입니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

SNMP를 선택합니다

클러스터에 대한 SNMP 및 트랩 작업을 설정하거나 해제할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

SNMP 트랩 호스트입니다

SNMP 트랩 호스트는 ONTAP에서 SNMP 트랩을 수신하도록 구성된 시스템입니다. 호스트를 검색하고 정의할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

SNMP 트랩 호스트 인스턴스입니다

특정 SNMP 트랩 호스트를 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

SNMP 사용자

SNMP 사용자를 정의하고 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

SNMP 사용자 인스턴스입니다

엔진 ID가 관리 SVM 또는 데이터 SVM과 관련된 특정 SNMP 사용자를 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.7에서 도입되었습니다.

SVM

이러한 API 호출을 사용하여 SVM(스토리지 가상 머신)을 관리할 수 있습니다.

마이그레이션

소스 클러스터에서 대상 클러스터로 SVM을 마이그레이션할 수 있습니다. 새 엔드포인트는 일시 중지, 재개, 상태 검색 및 마이그레이션 작업 중단 기능을 포함하여 완벽한 제어를 제공합니다. 이 리소스 유형은 ONTAP 9.10에서

도입되었습니다.

피어 권한

피어 권한을 할당하여 SVM 피어링 관계를 활성화할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

동료

피어링 관계는 SVM 간에 연결을 설정합니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

SVM

클러스터에 바인딩된 SVM을 관리할 수 있습니다. 이 리소스 유형은 ONTAP 9.6으로 도입되었습니다.

가장 중요한 메트릭

특정 SVM 인스턴스에 대한 추가 성능 메트릭 데이터에 액세스할 수 있습니다. 4개의 목록을 사용할 수 있으며 각 목록은 ONTAP FlexVol 및 FlexGroup 볼륨에 대한 최고의 I/O 활동을 제공합니다. 목록은 다음과 같습니다.

- 클라이언트
- 디렉토리
- 파일
- 사용자

이러한 자원 유형은 ONTAP 9.11에서 소개되었습니다.

웹

이러한 엔드포인트를 사용하여 각 데이터 SVM에 대한 웹 서비스 보안 구성을 업데이트하고 검색할 수 있습니다. 이 리소스 유형은 ONTAP 9.10에서 도입되었습니다.

워크플로우

워크플로우 사용을 준비하십시오

라이브 ONTAP 배포와 함께 사용하기 전에 워크플로의 구조와 형식을 잘 알고 있어야 합니다.



ONTAP 릴리스에서 사용하려는 워크플로에서 모든 API 호출을 지원하는지 확인해야 합니다. 을 참조하십시오 ["API 참조입니다"](#) 를 참조하십시오.

소개

Workflow _은(는) 특정 관리 작업 또는 목표를 달성하는 데 필요한 하나 이상의 단계 시퀀스입니다. ONTAP 워크플로에는 각 작업을 수행하는 데 필요한 핵심 단계와 매개 변수가 포함되어 있습니다. 이 서비스는 ONTAP 자동화 환경을 사용자 지정하기 위한 시작점을 제공합니다.

단계 유형

ONTAP 워크플로의 각 단계는 다음 유형 중 하나입니다.

- REST API 호출(curl 및 JSON 예 등의 세부 정보 포함)
- 다른 ONTAP 워크플로우를 수행하거나 호출합니다
- 기타 관련 작업(구성 결정 등)

REST API 호출

대부분의 워크플로 단계는 REST API 호출입니다. 이 단계에서는 curl 예제 및 기타 정보가 포함된 일반적인 형식을 사용합니다. 를 참조하십시오 ["API 참조입니다"](#) REST API 호출에 대한 자세한 내용은

단일 단계 워크플로우

워크플로는 한 단계만 포함할 수 있습니다. 이러한 _단일 단계 워크플로_는 여러 단계가 포함된 워크플로와 약간 다르게 형식이 지정됩니다. 예를 들어, 명시적인 단계 이름이 제거됩니다. 작업 또는 작업은 워크플로 제목에 따라 명확해야 합니다.

입력 변수

워크플로우는 최대한 일반화되도록 설계되어 모든 ONTAP 환경에서 사용할 수 있습니다. 이 점을 고려하여 REST API 호출은 curl 예제 및 기타 입력에 변수를 사용합니다. 그런 다음 REST API 호출을 다양한 ONTAP 환경에 쉽게 조정할 수 있습니다.

기본 URL 형식입니다

curl 또는 프로그래밍 언어를 통해 ONTAP REST API에 직접 액세스할 수 있습니다. 이 경우 기본 URL이 ONTAP 온라인 설명서 또는 System Manager에 액세스할 때 사용하는 URL과 다릅니다.

API에 직접 액세스할 때 도메인 또는 IP 주소에 *API* 를 추가해야 합니다. 예를 들면 다음과 같습니다.

<https://ontap.demo-example.com/api>

을 참조하십시오 ["ONTAP REST API 액세스 방법"](#) 를 참조하십시오.

공통 입력 매개변수

대부분의 REST API 호출에서 일반적으로 사용되는 몇 가지 입력 매개 변수가 있습니다. 이러한 매개 변수는 일반적으로 개별 워크플로에 설명되어 있지 않습니다. 매개 변수에 대해 잘 알고 있어야 합니다. 을 참조하십시오 ["API 요청을 제어하는 입력 변수입니다"](#) 를 참조하십시오.

특정 REST API 호출에 추가 매개 변수가 필요한 경우 각 워크플로에 대한 curl 예제에 대한 추가 입력 매개 변수 * 섹션에 해당 매개 변수가 포함됩니다.

변수 형식

워크플로우 예제에 사용되는 ID 값과 기타 변수는 불투명하며 ONTAP 클러스터마다 다를 수 있습니다. 예제의 가독성을 높이기 위해 실제 값은 사용되지 않습니다. 변수가 대신 사용됩니다. 일관된 형식과 예약된 이름을 기반으로 하는 이 접근 방식은 다음과 같은 이점을 제공합니다.

- curl 및 JSON 샘플은 읽기 쉽고 이해하기 쉽습니다.
- 모든 키워드가 동일한 형식을 사용하므로 빠르게 식별할 수 있습니다.
- 값을 복사하여 재사용할 수 없으므로 보안 노출이 없습니다.

변수 형식은 Bash 셸 환경에서 사용하도록 지정됩니다. 각 변수는 달러 기호로 시작하고 필요에 따라 큰따옴표로 묶습니다. 그러면 Bash에서 인식할 수 있습니다. 대문자는 이름에 일관되게 사용됩니다.

다음은 일반적인 변수 키워드 중 일부입니다. 이 목록은 완전하지 않으며 필요에 따라 추가 변수가 사용됩니다. 그들의 의미는 상황에 따라 분명해야 합니다.

키워드	유형	설명
\$FQDN_IP입니다	URL	ONTAP 관리 LIF의 정규화된 도메인 이름 또는 IP 주소
\$클러스터_ID	경로	API 작업이 실행되는 ONTAP 클러스터를 식별하는 UUIDv4 값입니다.
\$BASIC_AUTH입니다	머리글	HTTP 기본 인증에 사용되는 자격 증명 문자열입니다.

JSON 입력 예

POST 또는 패치를 사용하는 경우와 같은 일부 REST API 호출에는 요청 본문에 JSON 입력이 필요합니다. JSON 입력 예는 명확한 구별을 위해 컬링 예와 별도로 제시됩니다. JSON 입력 예제를 아래 설명된 기술 중 하나와 함께 사용할 수 있습니다.

로컬 파일에 저장

JSON 입력 예제를 파일로 복사하여 로컬에 저장할 수 있습니다. curl 명령은 를 사용하는 파일을 참조합니다 --data 로 파일 이름을 나타내는 값을 가진 매개 변수입니다 @ 접두어.

컬링 예제 다음에 터미널에 붙여 넣습니다

먼저 컬을 복사하여 터미널 셸에 붙여 넣어야 합니다. 그런 다음 예제를 편집하여 를 완전히 제거합니다 --data 끝에 매개 변수를 지정하고 로 바꿉니다 --data-raw 매개 변수. 마지막으로, 업데이트된 매개 변수가 있는 curl 명령 다음에 오도록 JSON 예제에 복사하여 붙여 넣습니다. 하나의 따옴표를 사용하여 JSON 입력 예제를 래핑해야 합니다.

인증 옵션

REST API에 사용할 수 있는 기본 인증 기술은 HTTP 기본 인증입니다. ONTAP 9.14부터 토큰 기반 인증 및 권한 부여와 함께 OAuth 2.0(Open Authorization) 프레임워크를 사용할 수도 있습니다.

HTTP 기본 인증

기본 인증을 사용할 때는 각 HTTP 요청에 사용자 자격 증명을 포함해야 합니다. 자격 증명을 보내는 방법에는 두 가지가 있습니다.

HTTP 요청 헤더를 생성합니다

수동으로 권한 부여 헤더를 생성하고 HTTP 요청에 포함할 수 있습니다. 이는 CLI에서 curl 명령을 사용하거나 자동화 코드와 함께 프로그래밍 언어를 사용할 때 수행할 수 있습니다. 개괄적인 단계는 다음과 같습니다.

1. 사용자 및 암호 값을 콜론으로 연결합니다.

```
admin:david123
```

2. 전체 문자열을 base64로 변환:

```
YWRtaW46ZGF2aWQxMjM=
```

3. 요청 헤더를 작성합니다.

```
Authorization: Basic YWRtaW46ZGF2aWQxMjM=
```

워크플로 컬링 예제에는 사용하기 전에 업데이트해야 하는 * \$BASIC_AUTH * 변수가 있는 이 헤더가 포함됩니다.

curl 매개 변수를 사용합니다

curl을 사용할 때 다른 옵션은 권한 부여 헤더를 제거하고 대신 curl * user * 매개 변수를 사용하는 것입니다. 예를 들면 다음과 같습니다.

```
--user username:password
```

사용자 환경에 적합한 자격 증명을 대체해야 합니다. 자격 증명은 base64로 인코딩되지 않습니다. 이 매개 변수를 사용하여 curl 명령을 실행하면 문자열이 인코딩되고 Authorization 헤더가 생성됩니다.

OAuth 2.0 을 참조하십시오

OAuth 2.0을 사용하는 경우 외부 인증 서버에서 액세스 토큰을 요청하고 각 HTTP 요청에 포함시켜야 합니다. 기본적인 상위 단계는 아래에 설명되어 있습니다. 도 참조하십시오 "[ONTAP OAuth 2.0 구축 개요](#)" OAuth 2.0에 대한 자세한 내용 및 ONTAP와 함께 사용하는 방법

ONTAP 환경을 준비합니다

REST API를 사용하여 ONTAP에 액세스하기 전에 ONTAP 환경을 준비하고 구성해야 합니다. 상위 수준에서는 다음과 같은 단계가 포함됩니다.

- ONTAP로 보호되는 리소스 및 클라이언트 식별
- 기존 ONTAP REST 역할 및 사용자 정의를 검토합니다
- 인증 서버를 설치하고 구성합니다

- 클라이언트 권한 부여 정의를 설계하고 구성합니다
- ONTAP를 구성하고 OAuth 2.0을 활성화합니다

액세스 토큰을 요청합니다

ONTAP 및 인증 서버가 정의되고 활성화되어 있으면 OAuth 2.0 토큰을 사용하여 REST API 호출을 수행할 수 있습니다. 첫 번째 단계는 인증 서버에서 액세스 토큰을 요청하는 것입니다. 이 작업은 서버에 기반한 여러 가지 다른 기술 중 하나를 사용하여 ONTAP 외부에서 수행됩니다. ONTAP는 액세스 토큰을 발급하거나 리디렉션을 수행하지 않습니다.

HTTP 요청 헤더를 생성합니다

액세스 토큰을 얻은 후 권한 부여 헤더를 생성하고 HTTP 요청에 포함할 수 있습니다. curl 또는 프로그래밍 언어를 사용하여 REST API에 액세스하든 관계없이 모든 클라이언트 요청에 헤더를 포함해야 합니다. 다음과 같이 헤더를 생성할 수 있습니다.

```
Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5cCIgOiAiSld ...
```

Bash와 함께 예제 사용

워크플로 컬 예제를 직접 사용하는 경우 해당 변수에 포함된 변수를 환경에 적합한 값으로 업데이트해야 합니다. 예제를 수동으로 편집하거나 아래 설명된 대로 Bash 셸을 사용하여 대신 사용할 수 있습니다.



Bash를 사용하면 curl 명령마다 한 번 설정하는 대신 셸 세션에서 한 번 변수 값을 설정할 수 있다는 이점이 있습니다.

단계

1. Linux 또는 유사한 운영 체제와 함께 제공되는 Bash 셸을 엽니다.
2. 실행할 컬링 예제에 포함된 변수 값을 설정합니다. 예를 들면 다음과 같습니다.

```
CLUSTER_ID=ce559b75-4145-11ee-b51a-005056aee9fb
```

3. 워크플로 페이지에서 컬링 예제를 복사하여 셸 터미널에 붙여 넣습니다.
4. Enter * 키를 누르면 다음 작업이 수행됩니다.
 - a. 설정한 변수 값으로 대체합니다
 - b. curl 명령을 실행합니다

클러스터

클러스터 구성을 가져옵니다

특정 필드를 포함하여 ONTAP 클러스터에 대한 구성을 검색할 수 있습니다. 이 작업은 클러스터의 상태를 평가하거나 구성을 업데이트하기 전에 수행할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/클러스터

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
필드	쿼리	아니요	반환할 값을 선택합니다. 예를 들면 다음과 같습니다 contact 및 version.

curl 예: 클러스터 연락처 정보를 검색합니다

이 예제에서는 단일 필드를 검색하는 방법을 보여 줍니다. 전체 클러스터 개체 및 구성을 가져오려면 `fields` 쿼리 매개 변수입니다.

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster?fields=contact" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "contact": "support@company-demo.com"
}
```

클러스터 연락처를 업데이트합니다

클러스터의 연락처 정보를 업데이트할 수 있습니다. 요청이 비동기적으로 처리되므로 연결된 백그라운드 작업이 성공적으로 완료되었는지 여부도 확인해야 합니다.

1단계: 클러스터 연락처 정보를 업데이트합니다

API 호출을 실행하여 클러스터 연락처 정보를 업데이트할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
패치	/api/클러스터

처리 유형

비동기식

컬의 예

```
curl --request PATCH \  
--location "https://$FQDN_IP/api/cluster" \  
--include \  
--header "Content-Type: application/json" \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "contact": "support@company-demo.com"  
}
```

JSON 출력 예

작업 객체가 반환됩니다. 다음 단계에서 사용할 작업 식별자를 저장해야 합니다.

```
{ "job": {  
  "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",  
  "_links": {  
    "self": {  
      "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"  
    }  
  }  
}
```

2단계: 작업 상태를 검색합니다

워크플로우를 수행합니다 ["작업 인스턴스를 가져옵니다"](#) 를 확인합니다 state 값은 입니다 success.

3단계: 클러스터 연락처 정보 확인

워크플로우를 수행합니다 ["클러스터 구성을 가져옵니다"](#). 를 설정해야 합니다 fields 에 쿼리 매개 변수 contact.

작업 인스턴스를 가져옵니다

특정 ONTAP 작업의 인스턴스를 검색할 수 있습니다. 일반적으로 이 작업을 수행하여 작업 및 관련 작업이 성공적으로 완료되었는지 확인할 수 있습니다.



일반적으로 비동기 요청을 실행한 후 제공되는 작업 개체의 UUID가 필요합니다. 검토도 합니다 "작업 개체를 사용한 비동기 처리" ONTAP 내부 작업으로 작업하기 전에

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/cluster/job/{uuid}

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$JOB_ID입니다	경로	예	요청되는 작업을 식별하는 데 필요합니다.

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/cluster/jobs/$JOB_ID" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

상태 값과 기타 필드는 반환된 작업 오브젝트에 포함됩니다. 이 예의 작업은 ONTAP 클러스터를 업데이트하는 과정에서 실행되었습니다.

```

{
  "uuid": "d877f5bb-3aa7-11e9-b6c6-005056a78c89",
  "description": "PATCH /api/cluster",
  "state": "success",
  "message": "success",
  "code": 0,
  "_links": {
    "self": {
      "href": "/api/cluster/jobs/d877f5bb-3aa7-11e9-b6c6-005056a78c89"
    }
  }
}

```

NAS

파일 보안 권한

파일 보안 및 감사 정책 관리 준비

ONTAP 클러스터 내에서 SVM을 통해 사용할 수 있는 파일에 대한 권한 및 감사 정책을 관리할 수 있습니다.

개요

ONTAP에서는 SACL(시스템 액세스 제어 목록) 및 DACL(임의 액세스 제어 목록)을 사용하여 파일 개체에 사용 권한을 할당합니다. ONTAP 9.9.1부터 REST API는 SACL 및 DACL 권한 관리를 지원합니다. API를 사용하여 파일 보안 권한 관리를 자동화할 수 있습니다. 대부분의 경우 여러 CLI 명령 또는 ONTAPI(ZAPI) 호출 대신 단일 REST API 호출을 사용할 수 있습니다.



9.9.1 이전 버전의 ONTAP 릴리스에서는 CLI 통과 기능을 사용하여 SACL 및 DACL 권한 관리를 자동화할 수 있습니다. 을 참조하십시오 ["마이그레이션 고려 사항"](#) 및 ["전용 CLI를 사용하면 ONTAP REST API를 통해 패스스루를 수행할 수 있습니다"](#) 를 참조하십시오.

REST API를 사용하여 ONTAP 파일 보안 서비스를 관리하는 방법을 보여주는 몇 가지 예제 워크플로우를 사용할 수 있습니다. 워크플로우를 사용하고 REST API 호출을 전송하기 전에 를 검토하십시오 ["워크플로우 사용을 준비하십시오"](#).

Python을 사용하는 경우 스크립트도 참조하십시오 ["file_security_permissions.py"](#) 일부 파일 보안 작업을 자동화하는 방법에 대한 예를 참조하십시오.

ONTAP REST API와 ONTAP CLI 명령 비교

대부분의 작업에서 ONTAP REST API를 사용할 경우 동일한 ONTAP CLI 명령 또는 ONTAPI(ZAPI) 호출보다 더 적은 수의 호출이 필요합니다. 아래 표에는 API 호출 목록과 각 작업에 필요한 CLI 명령 목록이 나와 있습니다.

ONTAP REST API를 참조하십시오	ONTAP CLI를 참조하십시오
'get/protocols/file-security/Effective-permissions/'	'vserver security file-directory show-Effective-permissions'를 선택합니다
'POST/PROTOCOLS/FILE-SECURITY/permissions/'	<ol style="list-style-type: none"> 1. 'vserver security file-directory NTFS create' 2. 'vserver security file-directory NTFS DACL add' 3. 'vserver security file-directory NTFS SACL add' 4. 'vserver security file-directory policy create'를 참조하십시오 5. 'vserver security file-directory policy task add' 6. 'vserver security file-directory apply'
'패치/프로토콜/파일-보안/권한/'	'vserver security file-directory NTFS modify'를 참조하십시오
삭제/프로토콜/파일-보안/권한/'	<ol style="list-style-type: none"> 1. 'vserver security file-directory NTFS DACL remove' 2. 'vserver security file-directory NTFS SACL remove'

관련 정보

- ["파일 권한을 보여 주는 Python 스크립트"](#)
- ["ONTAP REST API를 통해 파일 보안 권한 관리 간소화"](#)
- ["전용 CLI를 사용하면 ONTAP REST API를 통해 패스스루를 수행할 수 있습니다"](#)

파일에 대한 유효 사용 권한을 연습니다

특정 파일 또는 폴더에 대한 현재 유효 권한을 검색할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/protocols/file-security/effective-permissions/{svm.uuid}/{path}

처리 유형

동기식이다

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
curl --request GET \  
--location "https://$FQDN_IP/api/protocols/file-security/effective-  
permissions/$SVM_ID/$FILE_PATH" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "svm": {
    "uuid": "cf5f271a-1beb-11ea-8fad-005056bb645e",
    "name": "vs1"
  },
  "user": "administrator",
  "type": "windows",
  "path": "/",
  "share": {
    "path": "/"
  },
  "file_permission": [
    "read",
    "write",
    "append",
    "read_ea",
    "write_ea",
    "execute",
    "delete_child",
    "read_attributes",
    "write_attributes",
    "delete",
    "read_control",
    "write_dac",
    "write_owner",
    "synchronize",
    "system_security"
  ],
  "share_permission": [
    "read",
    "read_ea",
    "execute",
    "read_attributes",
    "read_control",
    "synchronize"
  ]
}
```

파일에 대한 감사 정보를 가져옵니다

특정 파일 또는 폴더에 대한 감사 정보를 검색할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형

동기식이다

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/protocols/file-
security/permissions/$SVM_ID/$FILE_PATH" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "svm": {
    "uuid": "9479099d-5b9f-11eb-9c4e-0050568e8682",
    "name": "vs1"
  },
  "path": "/parent",
  "owner": "BUILTIN\\Administrators",
  "group": "BUILTIN\\Administrators",
  "control_flags": "0x8014",
  "acls": [
    {
      "user": "BUILTIN\\Administrators",
      "access": "access_allow",
      "apply_to": {
        "files": true,
        "sub_folders": true,
        "this_folder": true
      },
      "advanced_rights": {
```

```

    "append_data": true,
    "delete": true,
    "delete_child": true,
    "execute_file": true,
    "full_control": true,
    "read_attr": true,
    "read_data": true,
    "read_ea": true,
    "read_perm": true,
    "write_attr": true,
    "write_data": true,
    "write_ea": true,
    "write_owner": true,
    "synchronize": true,
    "write_perm": true
  },
  "access_control": "file_directory"
},
{
  "user": "BUILTIN\\Users",
  "access": "access_allow",
  "apply_to": {
    "files": true,
    "sub_folders": true,
    "this_folder": true
  },
  "advanced_rights": {
    "append_data": true,
    "delete": true,
    "delete_child": true,
    "execute_file": true,
    "full_control": true,
    "read_attr": true,
    "read_data": true,
    "read_ea": true,
    "read_perm": true,
    "write_attr": true,
    "write_data": true,
    "write_ea": true,
    "write_owner": true,
    "synchronize": true,
    "write_perm": true
  },
  "access_control": "file_directory"
}
],

```

```

    "inode": 64,
    "security_style": "mixed",
    "effective_style": "ntfs",
    "dos_attributes": "10",
    "text_dos_attr": "----D---",
    "user_id": "0",
    "group_id": "0",
    "mode_bits": 777,
    "text_mode_bits": "rwxrwxrwx"
}

```

파일에 새 사용 권한을 적용합니다

특정 파일이나 폴더에 새 보안 설명자를 적용할 수 있습니다.

1단계: 새 사용 권한을 적용합니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형

비동기식

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \"acls\": [ { \"access\": \"access_allow\", \"advanced_rights\": { \"append_data\": true, \"delete\": true, \"delete_child\": true, \"execute_file\": true, \"full_control\": true, \"read_attr\": true, \"read_data\": true, \"read_ea\": true, \"read_perm\": true, \"write_attr\": true, \"write_data\": true, \"write_ea\": true, \"write_owner\": true, \"write_perm\": true }, \"apply_to\": { \"files\": true, \"sub_folders\": true, \"this_folder\": true }, \"user\": \"administrator\" } ], \"control_flags\": \"32788\", \"group\": \"S-1-5-21-2233347455-2266964949-1780268902-69700\", \"ignore_paths\": [ \"/parent/child2\" ], \"owner\": \"S-1-5-21-2233347455-2266964949-1780268902-69304\", \"propagation_mode\": \"propagate\"}'
```

JSON 출력 예

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

2단계: 작업 상태를 검색합니다

워크플로우를 수행합니다 "[작업 인스턴스를 가져옵니다](#)" 를 확인합니다 state 값은 입니다 success.

보안 설명자 정보를 업데이트합니다

기본 소유자, 그룹 또는 컨트롤 플래그를 포함하여 특정 파일 또는 폴더로 특정 보안 설명자를 업데이트할 수 있습니다.

1단계: 보안 설명자를 업데이트합니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
패치	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형
비동기식

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
curl --request POST --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ \"control_flags\": \"32788\", \"group\": \"everyone\", \"owner\": \"user1\"}'
```

JSON 출력 예

```
{
  "job": {
    "uuid": "6f89e612-5bbd-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/6f89e612-5bbd-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

2단계: 작업 상태를 검색합니다

워크플로우를 수행합니다 **"작업 인스턴스를 가져옵니다"** 를 확인합니다 state 값은 입니다 success.

액세스 제어 항목을 삭제합니다

특정 파일 또는 폴더에서 기존 ACE(액세스 제어 항목)를 삭제할 수 있습니다. 변경 내용이 자식 개체에 전파됩니다.

1단계: ACE를 삭제합니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
삭제	/api/protocols/file-security/permissions/{svm.uuid}/{path}

처리 유형

비동기식

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	파일이 포함된 SVM의 UUID입니다.
\$FILE_PATH입니다	경로	예	파일 또는 폴더의 경로입니다.

컬의 예

```
curl --request DELETE --location "https://$FQDN_IP/api/protocols/file-security/permissions/$SVM_ID/$FILE_PATH?return_timeout=0" --include --header "Accept */*" --header "Authorization: Basic $BASIC_AUTH" --data '{ "access": "access_allow", "apply_to": { "files": true, "sub_folders": true, "this_folder": true }, "ignore_paths": [ "/parent/child2" ], "propagation_mode": "propagate" }'
```

JSON 출력 예

```
{
  "job": {
    "uuid": "3015c294-5bbc-11eb-9c4e-0050568e8682",
    "_links": {
      "self": {
        "href": "/api/cluster/jobs/3015c294-5bbc-11eb-9c4e-0050568e8682"
      }
    }
  }
}
```

2단계: 작업 상태를 검색합니다

워크플로우를 수행합니다 "작업 인스턴스를 가져옵니다" 를 확인합니다 state 값은 입니다 success.

네트워킹

IP 인터페이스를 나열합니다

클러스터 및 SVM에 할당된 IP LIF를 검색할 수 있습니다. 이렇게 하면 네트워크 구성을 확인하거나 다른 LIF를 추가하려고 할 때 사용할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/network/ip/interfaces 를 참조하십시오

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
필드	쿼리	아니요	관련 구성 값의 제한된 목록을 반환합니다.

curl 예: 기본 구성 값으로 모든 LIF를 반환합니다

```
curl --request GET \  
--location "https://$FQDN_IP/api/network/ip/interfaces" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

curl 예: 4가지 특정 구성 값을 가진 모든 LIF를 반환합니다

```
curl --request GET \  
--location \  
"https://$FQDN_IP/api/network/ip/interfaces?fields=name,scope,svm.name,ip. \  
address" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "records": [
    {
      "uuid": "5ded9e38-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_mgmt1",
      "ip": {
        "address": "172.29.151.116"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/5ded9e38-999e-11ee-acad-005056ae6bd8"
        }
      }
    },
    {
      "uuid": "bb03c162-999e-11ee-acad-005056ae6bd8",
      "name": "cluster_mgmt",
      "ip": {
        "address": "172.29.186.156"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/bb03c162-999e-11ee-acad-005056ae6bd8"
        }
      }
    },
    {
      "uuid": "c5ffbd03-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_data1",
      "ip": {
        "address": "172.29.186.150"
      },
      "scope": "svm",
      "svm": {
        "name": "vs0"
      },
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/c5ffbd03-999e-11ee-acad-
```

```
005056ae6bd8"
  }
}
},
{
  "uuid": "c6612abe-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsrm-sr027o_data2",
  "ip": {
    "address": "172.29.186.151"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c6612abe-999e-11ee-acad-
005056ae6bd8"
    }
  }
},
{
  "uuid": "c6b21b94-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsrm-sr027o_data3",
  "ip": {
    "address": "172.29.186.152"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c6b21b94-999e-11ee-acad-
005056ae6bd8"
    }
  }
},
{
  "uuid": "c7025322-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsrm-sr027o_data4",
  "ip": {
    "address": "172.29.186.153"
  },
  "scope": "svm",
  "svm": {
```

```

    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c7025322-999e-11ee-acad-005056ae6bd8"
    }
  }
},
{
  "uuid": "c752cc66-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsimg-sr027o_data5",
  "ip": {
    "address": "172.29.186.154"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c752cc66-999e-11ee-acad-005056ae6bd8"
    }
  }
},
{
  "uuid": "c7a03719-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsimg-sr027o_data6",
  "ip": {
    "address": "172.29.186.155"
  },
  "scope": "svm",
  "svm": {
    "name": "vs0"
  },
  "_links": {
    "self": {
      "href": "/api/network/ip/interfaces/c7a03719-999e-11ee-acad-005056ae6bd8"
    }
  }
},
{
  "uuid": "ccd4c59c-999e-11ee-acad-005056ae6bd8",
  "name": "sti214-vsimg-sr027o_data4_inet6",

```

```

    "ip": {
      "address": "fd20:8b1e:b255:300f::ac5"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/ccd4c59c-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "d9144c30-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsim-sr027o_data6_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac7"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d9144c30-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "d961c13b-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsim-sr027o_data1_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac2"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d961c13b-999e-11ee-acad-005056ae6bd8"
      }
    }
  }
}

```

```

    }
  },
  {
    "uuid": "d9ac8d6a-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsrm-sr027o_data5_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac6"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d9ac8d6a-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "d9fc1a3-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsrm-sr027o_data2_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac3"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/d9fc1a3-999e-11ee-acad-005056ae6bd8"
      }
    }
  },
  {
    "uuid": "da4995a0-999e-11ee-acad-005056ae6bd8",
    "name": "sti214-vsrm-sr027o_data3_inet6",
    "ip": {
      "address": "fd20:8b1e:b255:300f::ac4"
    },
    "scope": "svm",
    "svm": {
      "name": "vs0"
    },
  },

```

```

    "_links": {
      "self": {
        "href": "/api/network/ip/interfaces/da4995a0-999e-11ee-acad-005056ae6bd8"
      }
    },
    {
      "uuid": "da9e7afd-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_cluster_mgmt_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:300f::ac8"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/da9e7afd-999e-11ee-acad-005056ae6bd8"
        }
      }
    },
    {
      "uuid": "e6db58b4-999e-11ee-acad-005056ae6bd8",
      "name": "sti214-vsrm-sr027o_mgmt1_inet6",
      "ip": {
        "address": "fd20:8b1e:b255:3008::1a0"
      },
      "scope": "cluster",
      "_links": {
        "self": {
          "href": "/api/network/ip/interfaces/e6db58b4-999e-11ee-acad-005056ae6bd8"
        }
      }
    }
  ],
  "num_records": 16,
  "_links": {
    "self": {
      "href":
"/api/network/ip/interfaces?fields=name,scope,svm.name,ip.address"
    }
  }
}

```

보안

계정

계정을 나열합니다

계정 목록을 검색할 수 있습니다. 보안 환경을 평가하거나 새 계정을 생성하기 전에 이 작업을 수행할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/security/accounts

처리 유형

동기식이다

컬의 예

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/accounts" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "records": [
    {
      "owner": {
        "uuid": "642573a8-9d14-11ee-9330-005056aed3de",
        "name": "vs0",
        "_links": {
          "self": {
            "href": "/api/svm/svms/642573a8-9d14-11ee-9330-005056aed3de"
          }
        }
      },
      "name": "vsadmin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/642573a8-9d14-11ee-9330-005056aed3de/vsadmin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "admin",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-005056aed3de/admin"
        }
      }
    },
    {
      "owner": {
        "uuid": "fdb6fe29-9d13-11ee-9330-005056aed3de",
        "name": "sti214nscluster-1"
      },
      "name": "autosupport",
      "_links": {
        "self": {
          "href": "/api/security/accounts/fdb6fe29-9d13-11ee-9330-
```

```

005056aed3de/autosupport"
    }
  }
},
"num_records": 3,
"_links": {
  "self": {
    "href": "/api/security/accounts"
  }
}
}

```

인증서 및 키

설치된 인증서를 나열합니다

ONTAP 클러스터에 설치된 인증서를 나열할 수 있습니다. 이렇게 하면 특정 인증서를 사용할 수 있는지 확인하거나 특정 인증서의 ID를 가져올 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/security/certificates 를 참조하십시오

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
Max_records(최대 레코드	쿼리	아니요	반환할 레코드 수를 지정합니다.

curl 예: 인증서 3개를 반환합니다

```

curl --request GET \
--location "https://$FQDN_IP/api/security/certificates?max_records=3" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"

```

JSON 출력 예

```
{
  "records": [
    {
      "uuid": "dad822c2-573c-11ee-a310-005056aecc29",
      "name": "vs0_17866DB5C933E2EA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/dad822c2-573c-11ee-a310-005056aecc29"
        }
      }
    },
    {
      "uuid": "7d8e5570-573c-11ee-a310-005056aecc29",
      "name": "BuypassClass3RootCA",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7d8e5570-573c-11ee-a310-005056aecc29"
        }
      }
    },
    {
      "uuid": "7dbb2191-573c-11ee-a310-005056aecc29",
      "name": "EntrustRootCertificationAuthority",
      "_links": {
        "self": {
          "href": "/api/security/certificates/7dbb2191-573c-11ee-a310-005056aecc29"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/security/certificates?max_records=3"
    },
    "next": {
      "href": "/api/security/certificates?start.svm_id=sti214nscluster-1&start.uuid=7dbb2191-573c-11ee-a310-005056aecc29&max_records=3"
    }
  }
}
```

인증서를 설치합니다

ONTAP 클러스터에 서명된 X.509 인증서를 설치할 수 있습니다. 강력한 인증이 필요한 ONTAP 기능이나 프로토콜을 구성할 때 이 작업을 수행할 수 있습니다.

시작하기 전에

설치할 인증서가 있어야 합니다. 또한 필요에 따라 중간 인증서가 설치되어 있는지 확인해야 합니다.



아래에 포함된 JSON 입력 예제를 사용하기 전에 를 업데이트해야 합니다 public_certificate 환경에 대한 인증서를 사용하여 얻을 수 있습니다.

1단계: 인증서를 설치합니다

API 호출을 실행하여 인증서를 설치할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/security/certificates 를 참조하십시오

curl 예: 클러스터 수준에서 루트 **CA** 인증서를 설치합니다

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/certificates" \  
--include \  
--header "Content-Type: application/json" \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{
  "type": "server_ca",
  "public_certificate":
    "-----BEGIN CERTIFICATE-----
MIID0TCCArkCFGYdznvTVvaY1VZPNfy4yCCyPph6MA0GCSqGSIb3DQEBCwUAMIGk
MQswCQYDVQQGEwJVUzELMAkGA1UECAwCTkMxDDAKBgNVBACMA1JUUDEWMBQGA1UE
CgwNT05UQVAgRXhhbXBsZTETMBEGA1UECwwKT05UQVAgOS4xNDEcMBoGA1UEAwWT
Ki5vbnRhcC1leGFtcGxlLmNvbTEvMC0GCSqGSIb3DQEJARYgZGF2aWQucGV0ZXJz
b25Ab250YXAtZXBhbXBsZS5jb20wHhcNMjMxMDA1MTUyOTE4WhcNMjMxMDA0MTUy
OTE4WjCBpDELMAkGA1UEBhMCMVVMxMCAzAJBGNVBAgMAk5DMQwwCgYDVQQHDANSVFAX
FjAUBGNVBAoMDU9OVEFQIEV4YW1wbGUuXzEzARBgNVBAsMCk9OVEFQIDkuMTQxHDAa
BgNVBAMMEyoub250YXAtZXBhbXBsZS5jb20xLzAtBgkqhkiG9w0BCQEWIGRhdm1k
LnBlldGVyc29uQG9udGFwLWV4YW1wbGUuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOc
AQ8AMIIBCgKCAQEAXQgy8mhb1Jhkf0D/MBodpZgW0aSp2jGbWJ+Zv2G8BXkp1762
dPHRkv1hnx9JvwkK4Dba05GiCiD5t3gjH/jUQMSFb+VwDbVmubVFnXjkm/4Q7sea
tMtA/ZpQdZbQFZ5RKtdWz7dzzPYEl2x8Q1Jc8Kh7NxERNMtgupGWZzn7mfXKYr4O
N/+vgahIhDibS8YK5rflw6bfmrik9E2D+PEab9DX/1DL5RX4tZ1H2OkyN2UxoBR6
Fq7l6n1Hi/5yR0OilxStN6s07EPoGak+KSlK4lq+EcIKRo0bP4mEQp8WMjJuiTkb
5MmeYoIpWEUgJK7S0M6Tp/3bTh2CST3AWxiNxQIDAQABMA0GCSqGSIb3DQEBCwUA
A4IBAQBfBqOuR0mYxdfRj930yIiRoDcoMzvo8cHGNUsuhnlBDnL203qhWEs97s0
mIy6zFMGnyNYa0t4i1cFsGDKP/JuljmYHjvv+2lHWnxHjTo7AOQCnXmQH5swoDbf
o1Vjqz8Oxz+PRJ+PA3dF5/8zqaAR6QreAN/iFR++6nUq1sbbM7w03tthBVMgo/h1
E9I2jVOZsqMFujm2CYfMs4XkZtrYmN6nZA8JcUpDjIWcAVbQYurMnna9r42oS3GB
WB/FE9n+P+FfJyHJ93KGcCXbH5RF2pi3wLlHilbvVuCjLRrhJ8U20I5mZoiXvAbc
IpYuBcuKXLwAarhDEacXttVjC+Bq
-----END CERTIFICATE-----"
}
```

2단계: 인증서가 설치되었는지 확인합니다

워크플로우를 수행합니다 "[설치된 인증서를 나열합니다](#)" 인증서를 사용할 수 있는지 확인합니다.

RBAC

RBAC를 사용하도록 준비합니다

ONTAP RBAC 기능은 환경에 따라 여러 가지 방법으로 사용할 수 있습니다. 이 섹션에서는 몇 가지 일반적인 시나리오를 워크플로우로 설명합니다. 각각의 경우 특정 보안 및 관리 목표에 중점을 둡니다.

역할을 생성하고 ONTAP 사용자 계정에 역할을 할당하기 전에 아래에 제시된 주요 보안 요구 사항 및 옵션을 검토하여 준비해야 합니다. 또한 에서 일반적인 워크플로 개념을 검토해야 합니다 "[워크플로우 사용을 준비하십시오](#)".

어떤 ONTAP 릴리스를 사용하고 있습니까?

ONTAP 릴리스는 사용 가능한 REST 엔드포인트 및 RBAC 기능을 결정합니다.

보호된 리소스 및 범위를 식별합니다

보호할 리소스 또는 명령과 범위(클러스터 또는 SVM)를 식별해야 합니다.

사용자는 어떤 액세스 권한을 가져야 하나요?

리소스 및 범위를 파악한 후에는 부여할 액세스 수준을 결정해야 합니다.

사용자는 **ONTAP**에 어떻게 액세스하나요?

사용자는 REST API 또는 CLI 또는 둘 다를 통해 ONTAP에 액세스할 수 있습니다.

기본 제공 역할 중 하나가 충분하니까, 아니면 사용자 지정 역할이 필요하니까?

기존 기본 제공 역할을 사용하는 것이 더 편리하지만 필요한 경우 새 사용자 지정 역할을 만들 수 있습니다.

어떤 유형의 역할이 필요하니까?

보안 요구 사항 및 ONTAP 액세스를 기반으로 REST 또는 기존 역할을 생성할지 여부를 선택해야 합니다.

역할을 생성합니다

SVM 볼륨 작업으로 액세스 제한

SVM 내에서 스토리지 볼륨 관리를 제한하는 역할을 정의할 수 있습니다.

이 워크플로 정보

먼저 복제를 제외한 모든 주요 볼륨 관리 기능에 액세스할 수 있도록 기존 역할이 생성됩니다. 역할은 다음과 같은 특성으로 정의됩니다.

- 가져오기, 생성, 수정 및 삭제를 포함한 모든 CRUD 볼륨 작업을 수행할 수 있습니다
- 볼륨 클론을 생성할 수 없습니다

그런 다음 필요에 따라 역할을 업데이트할 수 있습니다. 이 워크플로우에서는 두 번째 단계에서 사용자가 볼륨 클론을 생성할 수 있도록 역할이 변경됩니다.

1단계: 역할을 만듭니다

API 호출을 실행하여 RBAC 역할을 생성할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메서드와 엔드포인트를 사용합니다.

HTTP 메서드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "name": "role1",  
  "owner": {  
    "name": "cluster-1",  
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    { "path": "volume create", "access": "all" },  
    { "path": "volume delete", "access": "all" }  
  ]  
}
```

2단계: 역할을 업데이트합니다

API 호출을 실행하여 기존 역할을 업데이트할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메서드와 엔드포인트를 사용합니다.

HTTP 메서드	경로
게시	/API/보안/역할

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	역할 정의가 포함된 SVM의 UUID입니다.
\$ROLE_NAME입니다	경로	예	업데이트할 SVM 내에서 역할의 이름입니다.

컬의 예

```
curl --request POST \  
--location  
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/priveleges" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "path": "volume clone",  
  "access": "all"  
}
```

데이터 보호 관리 활성화

사용자에게 제한된 데이터 보호 기능을 제공할 수 있습니다.

이 워크플로 정보

생성된 전통적인 역할은 다음과 같은 특성을 가지고 정의됩니다.

- SnapMirror 관계를 업데이트할 뿐만 아니라 스냅샷을 생성 및 삭제할 수 있습니다
- 볼륨 또는 SVM과 같은 상위 레벨의 객체를 생성하거나 수정할 수 없습니다

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{
  "name": "role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "volume snapshot create", "access": "all"},
    {"path": "volume snapshot delete", "access": "all"},
    {"path": "volume show", "access": "readonly"},
    {"path": "vserver show", "access": "readonly"},
    {"path": "snapmirror show", "access": "readonly"},
    {"path": "snapmirror update", "access": "all"}
  ]
}
```

ONTAP 보고서 생성을 허용합니다

REST 역할을 생성하여 사용자에게 ONTAP 보고서를 생성할 수 있는 기능을 제공할 수 있습니다.

이 워크플로 정보

생성된 역할은 다음과 같은 특성으로 정의됩니다.

- 용량 및 성능(예: 볼륨, qtree, LUN, 애그리게이트, 노드, SnapMirror 관계 포함)
- 더 높은 수준의 오브젝트(예: 볼륨 또는 SVM)를 생성하거나 수정할 수 없음

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{
  "name": "rest_role1",
  "owner": {
    "name": "cluster-1",
    "uuid": "852d96be-f17c-11ec-9d19-005056bbad91"
  },
  "privileges": [
    {"path": "/api/storage/volumes", "access": "readonly"},
    {"path": "/api/storage/qtrees", "access": "readonly"},
    {"path": "/api/storage/luns", "access": "readonly"},
    {"path": "/api/storage/aggregates", "access": "readonly"},
    {"path": "/api/cluster/nodes", "access": "readonly"},
    {"path": "/api/snapmirror/relationships", "access": "readonly"},
    {"path": "/api/svm/svms", "access": "readonly"}
  ]
}
```

역할이 있는 사용자를 생성합니다

이 워크플로를 사용하여 연결된 REST 역할을 가진 사용자를 만들 수 있습니다.

이 워크플로 정보

이 워크플로에는 사용자 지정 REST 역할을 만들고 새 사용자 계정과 연결하는 데 필요한 일반적인 단계가 포함되어 있습니다. 사용자와 역할 모두 SVM 범위를 가지고 있으며 특정 데이터 SVM과 연관됩니다. 일부 단계는 선택 사항이거나 환경에 따라 변경해야 할 수 있습니다.

1단계: 클러스터의 데이터 **SVM**을 나열합니다

다음 REST API 호출을 수행하여 클러스터에 SVM을 표시합니다. 각 SVM의 UUID 및 이름은 출력에 제공됩니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/svm/sSVM

컬의 예

```
curl --request GET \
--location "https://$FQDN_IP/api/svm/svms?order_by=name" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

작업을 마친 후

새 사용자 및 역할을 생성할 목록에서 원하는 SVM을 선택합니다.

2단계: SVM에 정의된 사용자를 나열합니다

다음 REST API 호출을 수행하여 선택한 SVM에 정의된 사용자를 나열할 수 있습니다. 소유자 매개 변수를 통해 SVM을 식별할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/security/accounts

컬의 예

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/accounts?owner.name=dmp" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

작업을 마친 후

SVM에 이미 정의된 사용자를 기준으로 새 사용자의 이름을 선택합니다.

3단계: SVM에 정의된 REST 역할 나열

선택한 SVM에 정의된 역할을 나열하려면 다음 REST API 호출을 수행합니다. 소유자 매개 변수를 통해 SVM을 식별할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/API/보안/역할

컬의 예

```
curl --request GET \  
--location "https://$FQDN_IP/api/security/roles?owner.name=dmp" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

작업을 마친 후

SVM에 이미 정의된 역할에 따라 새 역할에 맞는 고유한 이름을 선택하십시오.

4단계: 사용자 지정 **REST** 역할을 만듭니다

SVM에서 맞춤형 REST API를 생성하여 다음 REST API 호출을 수행합니다. 이 역할에는 처음에 모든 액세스가 거부되도록 기본 액세스 권한을 *없음*으로 설정하는 하나의 권한만 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/API/보안/역할

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/security/roles" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "name": "dprole1",  
  "owner": {  
    "name": "dmp",  
    "uuid": "752d96be-f17c-11ec-9d19-005056bbad91"  
  },  
  "privileges": [  
    {"path": "/api", "access": "none"},  
  ]  
}
```

작업을 마친 후

필요에 따라 3단계를 다시 수행하여 새 역할을 표시합니다. ONTAP CLI에서 역할을 표시할 수도 있습니다.

5단계: 권한을 추가하여 역할을 업데이트합니다

필요에 따라 권한을 추가하여 역할을 수정하려면 다음 REST API 호출을 수행합니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/security/roles/{owner.uuid}/{name}/권한

컬링 예제에 대한 추가 입력 매개 변수

모든 REST API 호출에 공통되는 매개 변수 외에 다음 매개 변수가 이 단계의 cURL 예에도 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
\$SVM_ID입니다	경로	예	역할 정의가 포함된 SVM의 UUID입니다.
\$ROLE_NAME입니다	경로	예	업데이트할 SVM 내의 역할 이름입니다.

컬의 예

```
curl --request POST \
--location
"https://$FQDN_IP/api/security/roles/$SVM_ID/$ROLE_NAME/privileges" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON 입력 예

```
{
  "path": "/api/storage/volumes",
  "access": "readonly"
}
```

작업을 마친 후

필요에 따라 3단계를 다시 수행하여 새 역할을 표시합니다. ONTAP CLI에서 역할을 표시할 수도 있습니다.

6단계: 사용자 생성

사용자 계정 생성을 위해 다음 REST API 호출을 수행합니다. 위에서 생성한 * dprole1 * 역할은 새 사용자와 연결됩니다.



역할 없이 사용자를 만들 수 있습니다. 이 경우 사용자에게 기본 역할(둘 중 하나)이 할당됩니다 admin 또는 vsadmin) 사용자가 클러스터 또는 SVM 범위로 정의되었는지 여부에 따라 결정됩니다. 다른 역할을 할당하도록 사용자를 수정해야 합니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/security/accounts

컬의 예

```
curl --request POST \
--location "https://$FQDN_IP/api/security/accounts" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON 입력 예

```
{
  "owner": {"uuid": "daf84055-248f-11ed-a23d-005056ac4fe6"},
  "name": "david",
  "applications": [
    {"application": "ssh",
      "authentication_methods": ["password"],
      "second_authentication_method": "none"}
  ],
  "role": "dprole1",
  "password": "netapp123"
}
```

작업을 마친 후

새 사용자의 자격 증명을 사용하여 SVM 관리 인터페이스에 로그인할 수 있습니다.

스토리지

애그리게이트를 나열합니다

클러스터에서 애그리게이트 목록을 검색할 수 있습니다. 이를 통해 활용도와 성능을 평가할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/스토리지/디스크

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
node.name	쿼리	아니요	각 애그리게이트가 연결된 노드를 식별하는 데 사용될 수 있습니다.

curl 예: 기본 구성 값으로 모든 애그리게이트를 반환합니다

```
curl --request GET \  
--location "https://$FQDN_IP/api/storage/aggregates" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

curl 예: 특정 구성 값으로 모든 애그리게이트를 반환합니다

```
curl --request GET \  
--location "https://$FQDN_IP/api/storage/aggregates?fields=node.name" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "records": [
    {
      "uuid": "760d8137-fc59-47da-906a-cc28db0a1c1b",
      "name": "sti214_vsim_sr027o_aggr1",
      "node": {
        "name": "sti214-vsim-sr027o"
      },
      "_links": {
        "self": {
          "href": "/api/storage/aggregates/760d8137-fc59-47da-906a-cc28db0a1c1b"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/storage/aggregates?fields=node.name"
    }
  }
}
```

디스크를 나열합니다

클러스터에서 디스크 목록을 검색할 수 있습니다. 이렇게 하면 애그리게이트를 생성할 때 사용할 스페어를 하나 이상 찾을 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/스토리지/디스크

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
상태	쿼리	아니요	새 애그리게이트에 사용할 수 있는 스페어 디스크를 식별하는 데 사용할 수 있습니다.

curl 예: 모든 디스크를 반환합니다

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/disks" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

curl 예: 스페어 디스크를 반환합니다

```
curl --request GET \
--location "https://$FQDN_IP/api/storage/disks?state=spare" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "records": [
    {
      "name": "NET-1.20",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.20"
        }
      }
    },
    {
      "name": "NET-1.12",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.12"
        }
      }
    },
    {
      "name": "NET-1.7",
      "state": "spare",
      "_links": {
        "self": {
          "href": "/api/storage/disks/NET-1.7"
        }
      }
    }
  ],
  "num_records": 3,
  "_links": {
    "self": {
      "href": "/api/storage/disks?state=spare"
    }
  }
}
```

지원

있습니다

EMS 지원 서비스 관리 준비

ONTAP 클러스터에 대한 EMS(Event Management System) 처리를 설정하고 필요에 따라 EMS 메시지를 조회할 수 있다.

개요

ONTAP EMS 서비스 사용 방법을 보여 주는 몇 가지 예제 워크플로가 있습니다. 워크플로우를 사용하고 REST API 호출을 전송하기 전에 를 검토하십시오 ["워크플로우 사용을 준비하십시오"](#).

파이썬을 사용한다면, 성경도 참조하십시오 ["events.py"](#) 일부 EMS 관련 작업을 자동화하는 방법에 대한 예를 참조하십시오.

ONTAP REST API와 ONTAP CLI 명령 비교

대부분의 작업에서 ONTAP REST API를 사용할 경우 동일한 ONTAP CLI 명령보다 더 적은 수의 호출을 필요로 합니다. 아래 표에는 API 호출 목록과 각 작업에 필요한 CLI 명령 목록이 나와 있습니다.

ONTAP REST API를 참조하십시오	ONTAP CLI를 참조하십시오
GET/SUPPORT/EMS	이벤트 구성 쇼
POST/SUPPORT/EMS/목적지	1. 이벤트 알림 메시지 목적지 작성 2. 이벤트 알림 작성
'Get/support/EMS/events	이벤트 로그 쇼
'POST/support/EMS/filters	1. '이벤트 필터 생성 - 필터 이름 <filtername>' 2. '이벤트 필터 규칙 add-filter-name <filtername>'

관련 정보

- ["EMS를 설명하는 Python 스크립트"](#)
- ["ONTAP REST API: 심각도가 높은 이벤트 자동 알림"](#)

EMS 로그 이벤트 나열

모든 이벤트 알림 메시지 또는 특정 특성을 가진 메시지만 검색할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/support/ems/events 를 참조하십시오

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
필드	쿼리	아니요	응답에 포함할 특정 필드를 요청하는 데 사용됩니다.
Max_records(최대 레코드)	쿼리	아니요	단일 요청에서 반환되는 레코드 수를 제한하는 데 사용할 수 있습니다.
로그_메시지	쿼리	아니요	특정 텍스트 값을 검색하고 일치하는 메시지만 반환하는 데 사용됩니다.
message.severity	쿼리	아니요	반환된 메시지를 과 같은 특정 심각도의 메시지로 제한합니다 alert.

curl 예: 최신 메시지와 이름 값을 반환합니다

```
curl --request GET \  
--location \  
"https://$FQDN_IP/api/support/ems/events?fields=message.name&max_records=1" \  
\  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

curl 예: 특정 텍스트와 심각도가 포함된 메시지를 반환합니다

```
curl --request GET \  
--location \  
"https://$FQDN_IP/api/support/ems/events?log_message=*disk*&message.severity=alert" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "records": [
    {
      "node": {
        "name": "malha-vsimg1",
        "uuid": "da4f9e62-9de3-11ec-976a-005056b369de",
        "_links": {
          "self": {
            "href": "/api/cluster/nodes/da4f9e62-9de3-11ec-976a-005056b369de"
          }
        }
      },
      "index": 4602,
      "time": "2022-03-18T06:37:46-04:00",
      "message": {
        "severity": "alert",
        "name": "raid.autoPart.disabled"
      },
      "log_message": "raid.autoPart.disabled: Disk auto-partitioning is disabled on this system: the system needs a minimum of 4 usable internal hard disks.",
      "_links": {
        "self": {
          "href": "/api/support/ems/events/malha-vsimg1/4602"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href":
"/api/support/ems/events?log_message=*disk*&message.severity=alert&max_records=1"
    },
    "next": {
      "href": "/api/support/ems/events?start.keytime=2022-03-18T06%3A37%3A46-04%3A00&start.node.name=malha-vsimg1&start.index=4602&log_message=*disk*&message.severity=alert"
    }
  }
}
```

EMS 구성을 가져옵니다

ONTAP 클러스터에 대한 현재 EMS 구성을 조회할 수 있다. 구성을 업데이트하거나 새 EMS 알림을 생성하기 전에 이 작업을 수행할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/support/EMS

처리 유형

동기식이다

컬의 예

```
curl --request GET \  
--location "https://$FQDN_IP/api/support/ems" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{  
  "proxy_url": "https://proxyserver.mycompany.com",  
  "proxy_user": "proxy_user",  
  "mail_server": "mail@mycompany.com",  
  "_links": {  
    "self": {  
      "href": "/api/resourcelink"  
    }  
  },  
  "pubsub_enabled": "1",  
  "mail_from": "administrator@mycompany.com"  
}
```

EMS Notification을 생성한다

다음 워크플로를 사용하여 선택한 이벤트 메시지를 수신할 새 EMS 알림 대상을 만들 수 있습니다.

1단계: 시스템 전체 이메일 설정을 구성합니다

다음 API 호출을 실행하여 시스템 전체 이메일 설정을 구성할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
패치	/api/support/EMS

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
메일_보낸 사람	쿼리	예	를 설정합니다 from 알림 전자 메일 메시지의 필드입니다.
메일_서버	쿼리	예	대상 SMTP 메일 서버를 구성합니다.

컬의 예

```
curl --request PATCH \  
--location \  
"https://$FQDN_IP/api/support/ems?mail_from=administrator@mycompany.com&mail_server=mail@mycompany.com" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

2단계: 메시지 필터 정의

API 호출을 실행하여 메시지와 일치하는 필터 규칙을 정의할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/support/ems/filters 를 참조하십시오

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
필터	바디	예	필터 구성에 대한 값을 포함합니다.

컬의 예

```
curl --request POST \
--location "https://$FQDN_IP/api/support/ems/filters" \
--include \
--header "Accept: */*" \
--header "Authorization: Basic $BASIC_AUTH" \
--data @JSONinput
```

JSON 입력 예

```
{
  "name": "test-filter",
  "rules.type": ["include"],
  "rules.message_criteria.severities": ["emergency"]
}
```

3단계: 메시지 대상을 만듭니다

API 호출을 실행하여 메시지 대상을 생성할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
게시	/api/support/ems/destinations 를 참조하십시오

처리 유형

동기식이다

Curl 예제의 추가 입력 매개변수

모든 REST API 호출에서 일반적으로 사용되는 매개 변수 외에도 이 단계의 curl 예제에도 다음 매개 변수가 사용됩니다.

매개 변수	유형	필수 요소입니다	설명
대상 구성	바디	예	이벤트 대상에 대한 값을 포함합니다.

컬의 예

```
curl --request POST \  
--location "https://$FQDN_IP/api/support/ems/destinations" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH" \  
--data @JSONinput
```

JSON 입력 예

```
{  
  "name": "test-destination",  
  "type": "email",  
  "destination": "administrator@mycompany.com",  
  "filters.name": ["important-events"]  
}
```

SVM

SVM을 나열합니다

ONTAP 클러스터 내에 정의된 SVM(스토리지 가상 머신)을 표시할 수 있습니다. 이 작업은 특정 SVM의 식별자를 찾거나 새로운 SVM을 생성하기 전에 이름이 고유한지 확인할 때 수행할 수 있습니다.

HTTP 메서드 및 끝점입니다

이 REST API 호출은 다음과 같은 메소드와 엔드포인트를 사용합니다.

HTTP 메소드	경로
가져오기	/api/svm/sSVM

컬의 예

```
curl --request GET \  
--location "https://$FQDN_IP/api/svm/svms" \  
--include \  
--header "Accept: */*" \  
--header "Authorization: Basic $BASIC_AUTH"
```

JSON 출력 예

```
{
  "records": [
    {
      "uuid": "71bd74f8-40dc-11ee-b51a-005056aee9fa",
      "name": "vs0",
      "_links": {
        "self": {
          "href": "/api/svm/svms/71bd74f8-40dc-11ee-b51a-005056aee9fa"
        }
      }
    }
  ],
  "num_records": 1,
  "_links": {
    "self": {
      "href": "/api/svm/svms"
    }
  }
}
```

소프트웨어 도구

Python 클라이언트 라이브러리

Python 클라이언트 라이브러리 개요

NetApp ONTAP Python 클라이언트 라이브러리는 ONTAP REST API에 액세스하는 스크립트를 작성하고 사용하는 데 사용할 수 있는 패키지입니다. 연결 관리, 비동기 처리, 예외 처리 및 오류 메시지를 비롯한 여러 기본 서비스에 대한 지원을 제공합니다. Python 클라이언트 라이브러리를 사용하면 ONTAP 배포의 자동화를 지원하는 강력한 코드를 빠르게 개발할 수 있습니다.



NetApp은 코드 샘플 및 기타 유용한 정보가 포함된 GitHub 저장소를 유지합니다. Python 클라이언트 라이브러리를 사용하여 샘플에 액세스하려면 `_examples_folder`로 이동할 수 있습니다.

관련 정보

- ["ONTAP REST Python GitHub 리포지토리"](#)
- ["ONTAP REST Python 클라이언트 라이브러리 예"](#)

Python 클라이언트 라이브러리를 사용할 준비를 합니다

Python 클라이언트 라이브러리를 사용하기 전에 로컬 런타임 환경을 준비해야 합니다.

패키지 이름 및 버전

Python 클라이언트 라이브러리 패키지의 이름은 * NetApp-ONTAP * 입니다. 패키지에 연결된 버전은 ONTAP 릴리스 내의 클라이언트에 대한 부 버전과 함께 라이브러리가 생성된 ONTAP 주 버전 번호와 부 버전 번호의 조합입니다. 예를 들어 유효한 버전 번호에는 9.6.1, 9.6.2 및 9.7.1이 포함됩니다.

설치

PiP를 사용하여 Python Package Index(PyPi) 웹 사이트에서 NetApp_ONTAP 패키지를 설치해야 합니다.

ONTAP 릴리즈의 패키지 및 문서

9.6부터 시작되는 각 ONTAP 릴리스에는 PyPI 패키지와 관련 문서가 포함되어 있습니다. 을 참조하십시오 ["패키지 및 설명서"](#) 를 참조하십시오. 설치 요구 사항은 각 패키지와 함께 포함되며 다음과 같은 다양한 버전을 포함합니다.

- 파이썬
- 요청
- 요청 - 도구 벨트
- 마쉬멜로

패키지 및 설명서

Python 클라이언트 라이브러리는 9.6부터 각 ONTAP 릴리스에 사용할 수 있습니다. 사용 중인 ONTAP 릴리스에 따라 PyPI 패키지와 문서에 액세스해야 합니다.

ONTAP 9.15.1

- ["PyPI:NetApp ONTAP 9.15.1"](#)
- ["9.15.1용 NetApp PCL 문서"](#)

ONTAP 9.14.1

- ["PyPI:NetApp ONTAP 9.14.1"](#)
- ["9.14.1용 NetApp PCL 설명서"](#)

ONTAP 9.13.1

- ["PyPI: NetApp ONTAP 9.13.1"](#)
- ["9.13.1 용 NetApp PCL 설명서"](#)

ONTAP 9.12.1

- ["PyPI:NetApp ONTAP 9.12.1"](#)
- ["9.12.1용 NetApp PCL 문서"](#)

ONTAP 9.11.1

- ["PyPI:NetApp ONTAP 9.11.1"](#)
- ["9.11.1용 NetApp PCL 문서"](#)

ONTAP 9.10.1

- ["PyPI:NetApp ONTAP 9.10.1"](#)
- ["9.10.1용 NetApp PCL 설명서"](#)

ONTAP 9.9.1

- ["PyPI:NetApp ONTAP 9.9.1"](#)
- ["9.9.9.1용 NetApp PCL 문서"](#)

ONTAP 9.8

- ["PyPI:NetApp ONTAP 9.8"](#)
- ["9.8용 NetApp PCL 문서"](#)

ONTAP 9.7

- ["PyPI: NetApp ONTAP 9.7"](#)
- ["9.7용 NetApp PCL 설명서"](#)

ONTAP 9.6

- ["PyPI:NetApp ONTAP 9.6"](#)
- ["9.6용 NetApp PCL 문서"](#)

클러스터 구성을 검색하는 스크립트입니다

다음 스크립트는 Python 클라이언트 라이브러리를 사용하는 방법의 간단한 예를 제공합니다. CLI에서 Python 3을 사용하여 스크립트를 실행하여 ONTAP 클러스터 구성을 검색할 수 있습니다.

```

##-----
#
# Description: Python script to retrieve the cluster configuration.
#
# Usage example:
#
# python3 get_cluster.py
#
#
# (C) Copyright 2024 NetApp, Inc.
#
# This sample code is provided AS IS, with no support or warranties of
# any kind, including but not limited for warranties of merchantability
# or fitness of any kind, expressed or implied. Permission to use,
# reproduce, modify and create derivatives of the sample code is granted
# solely for the purpose of researching, designing, developing and
# testing a software application product for use with NetApp products,
# provided that the above copyright notice appears in all copies and
# that the software application product is distributed pursuant to terms
# no less restrictive than those set forth herein.
#
##-----
# For reading the password from the commandline
from getpass import getpass
# Global configuration for the library
from netapp_ontap import config
# Support for the connection to ONTAP
from netapp_ontap import HostConnection
# Specific API needed for this script
from netapp_ontap.resources import Cluster
# Create connection to the ONTAP management LIF
# (add verify=False if the certificate your cluster is serving is not
trusted)
conn = HostConnection(
    "<mgmt_ip>", username="admin", password=getpass("ONTAP admin password:
"),
)
# Set connection as the default for all API calls
config.CONNECTION = conn
# Create new cluster object
clus = Cluster()
# Issue REST API call
clus.get()
# Display the cluster configuration
print(clus)

```

블로그 기사를 참조하십시오

Python 클라이언트 라이브러리를 사용하는 방법을 더 잘 이해하는 데 도움이 되는 몇 가지 블로그 문서가 있습니다.

Python 클라이언트 라이브러리를 사용하여 **ONTAP REST API** 사용을 간소화합니다
이 블로그에서는 ONTAP 파이썬 클라이언트 라이브러리의 기능에 대해 소개합니다.

["www.netapp.com/blog/simplify-ontap-rest-api-consumption"](http://www.netapp.com/blog/simplify-ontap-rest-api-consumption)

ONTAP REST API 파이썬 클라이언트 라이브러리 시작하기

Python 클라이언트 라이브러리에 대한 자세한 내용을 다루는 3부작 블로그 시리즈입니다.

파트 1: ["NetApp.io/2020/06/09/ontap-rest-api-python-client-library-pt1"](http://NetApp.io/2020/06/09/ontap-rest-api-python-client-library-pt1)

2부: ["NetApp.io/2020/06/09/ontap-rest-api-python-client-library-pt2/"](http://NetApp.io/2020/06/09/ontap-rest-api-python-client-library-pt2/)

3부: ["NetApp.io/2020/06/09/ontap-rest-api-python-client-library-pt3"](http://NetApp.io/2020/06/09/ontap-rest-api-python-client-library-pt3)

PowerShell 툴킷

PowerShell Toolkit 개요

NetApp는 PowerShell을 사용하여 ONTAP 스토리지 시스템 관리를 지원합니다.

PowerShell을 사용합니다

PowerShell은 작업 자동화 및 구성 관리에 사용할 수 있는 Microsoft의 프로그램입니다. 여기에는 스크립트 언어뿐만 아니라 명령줄 셸 환경이 포함되어 있습니다.

NetApp ONTAP PowerShell 툴킷

NetApp입니다. ONTAP PowerShell 툴킷에는 NetApp ONTAP용 PowerShell 모듈이 포함되어 있습니다. 이 툴킷은 NetApp AFF 및 FAS 시스템, 일반 하드웨어 및 클라우드를 비롯한 다양한 환경에서 실행되는 ONTAP를 지원합니다. 이 모듈에는 Windows 호스트에서 스토리지 관리를 종합적으로 지원하는 2,400개 이상의 cmdlet이 포함되어 있습니다.

PowerShell Toolkit을 다운로드하여 설치합니다

NetApp ONTAP PowerShell 툴킷을 다운로드하고 설치하는 데 사용할 수 있는 두 가지 옵션이 있습니다.

NetApp 지원

PowerShell 툴킷은 다음 NetApp Support 사이트에서 다운로드할 수 있습니다.

<https://mysupport.netapp.com/site/tools/tool-eula/ontap-powershell-toolkit>

PowerShell 갤러리

PowerShell 툴킷은 PowerShell 갤러리에서 다운로드할 수 있습니다.

<https://www.powershellgallery.com/packages/NetApp.ONTAP/9.12.1.2302>

NetApp 관리 SDK

NetApp 관리 SDK는 ONTAP 스토리지를 모니터링하고 관리하는 애플리케이션을 개발하기 위한 일련의 ONTAPI API 호출 세트를 제공합니다. SDK는 OnCommand Workflow Automation 패키지와 함께 ONTAP 시스템 관리를 자동화하기 위한 노력을 지원합니다.



NetApp Manageability SDK 및 OnCommand Workflow Automation는 계속 지원되지만, ONTAP REST API는 ONTAP 시스템을 자동화할 때 사용하는 권장 전략적 기술입니다. 을 참조하십시오 ["ONTAPI 비활성화"](#) 를 참조하십시오.

SDK를 다운로드합니다

NetApp Support 사이트 에서 NetApp 관리 SDK를 다운로드할 수 있습니다. SDK는 클라이언트측에서 Python, PowerShell, C, C++, 자바, C#, VB. 네트, 루비. NetApp 관리 SDK에 대한 자세한 내용과 현재 사용 중인 ONTAP 버전에서 지원되는 방법은 상호 운용성 매트릭스 툴을 검토하십시오.

OnCommand Workflow Automation를 사용합니다

또한 SDK와 함께 제공되는 API를 사용하여 스크립트를 작성하지 않고도 관리 작업을 자동화할 수 있습니다. OnCommand Workflow Automation(OnCommand WFA)는 관리 작업을 구축하고 실행하기 위해 사전 패키징된 여러 워크플로우를 제공합니다. NetApp 스토리지 자동화 스토어 에서 OnCommand WFA 패키지를 다운로드할 수 있습니다.

관련 정보

- ["NetApp Support 사이트"](#)
- ["NetApp 상호 운용성 매트릭스 툴"](#)
- ["NetApp Manageability SDK 설명서"](#)
- ["OnCommand Workflow Automation 설명서 리소스"](#)
- ["NetApp 자동화 스토어"](#)

ONTAPI에서 REST API로 마이그레이션합니다

ONTAPI 비활성화

ONTAPI API(ZAPI)는 NetApp ONTAP 소프트웨어에 포함된 고유의 호출 세트입니다. API는 Network Manageability SDK를 통해 제공되며 데이터 스토리지 관리 및 관리 작업의 자동화를 지원합니다. 향후 버전의 ONTAP에서는 ONTAPI 인터페이스가 비활성화됩니다. ONTAPI를 사용하는 경우 ONTAP REST API로의 마이그레이션을 계획해야 합니다.

관련 정보

- ["ONTAP 자동화 옵션을 이해합니다"](#)
- ["CPC-00410 가용성 종료: ONTAPI"](#)
- ["CPC용 ZAPI에서 ONTAP REST API 변환에 대한 FAQ"](#)

마이그레이션 고려 사항

ONTAPI API(ZAPI) 또는 ONTAP CLI에서 ONTAP REST API로 마이그레이션하기 전에 몇 가지 문제를 고려해야 합니다.

일반적인 설계 차이점

ONTAP REST API 및 명령줄 인터페이스는 근본적으로 다른 디자인을 가지고 있습니다. CLI 명령 및 매개 변수는 REST API 호출에 직접 매핑되지 않습니다. 유사성이 있는 경우에도 입력 매개 변수의 세부 정보는 다를 수 있습니다. 예를 들어, 숫자 단위는 바이트로 지정하거나 접미사(예: KB)를 사용할 수 있습니다. 을 참조하십시오 ["API 요청을 제어하는 입력 변수입니다"](#) 및 ["API 참조입니다"](#) 를 참조하십시오.

REST API를 통해 표시되는 데이터 SVM

ONTAP은 다양한 유형의 SVM(스토리지 가상 머신)을 지원합니다. 하지만 ONTAP REST API를 통해 데이터 SVM만 직접 표시됩니다. REST API를 통해 클러스터와 노드를 설명하는 구성 정보를 사용할 수 있지만 클러스터와 노드는 별도의 SVM으로 취급되지 않습니다.

REST API를 통해 ONTAP CLI에 액세스합니다

ONTAP는 ONTAPI API 및 CLI 사용자가 ONTAP REST API로 전환할 때 ONTAP CLI에 액세스할 수 있는 REST 엔드포인트를 제공합니다. 이 통과 연결 기능을 사용하여 모든 CLI 명령을 실행할 수 있습니다. NetApp이 REST API의 격차를 파악하고 향후 ONTAP 릴리즈를 개선할 수 있도록 REST 엔드포인트의 사용이 AutoSupport 데이터로 반환됩니다.

CLI 명령을 실행하려면 다음과 같은 규칙에 따라 적절하게 구성된 REST API 호출을 해야 합니다.

- 리소스 경로
- 필드 이름
- HTTP 메서드

CLI 액세스를 위한 기본 리소스 경로는 `/private/cli`. REST API를 통해 CLI에 액세스하는 방법에 대한 자세한 내용은 ONTAP API 온라인 설명서 페이지를 참조하십시오. 또한 NetApp는 코드 샘플 및 기타 유용한 정보가 들어 있는 GitHub 리포지토리를 유지 관리합니다. 을 참조하십시오 ["ONTAP REST Python GitHub 리포지토리 - CLI passthrough 샘플"](#) 를 참조하십시오.

ONTAPI에서 SnapDiff 가용성 변경

ONTAP 9.10.1부터 SnapDiff v1 및 v2 ONTAPI 호출은 호출할 수 없습니다. SnapDiff v1 또는 v2 ONTAPI 호출을 호출하는 타사 응용 프로그램은 ONTAP 9.10.1부터 작동하지 않습니다. ONTAP 사용자는 ONTAP 9.10.1로 업그레이드하기 전에 백업 응용 프로그램이 SnapDiff v3 REST 호출을 지원하는지 확인해야 합니다.

ONTAP 릴리즈 간 SnapDiff API 가용성은 다음과 같이 정의됩니다.

- ONTAP 9.7 및 이전 릴리즈: v1 및 v2(ONTAPI만 해당)
- ONTAP 9.8–9.9.1:v1, v2 및 v3(ONTAPI와 REST API 모두)
- ONTAP 9.10.1:v3만 해당(REST API만 해당)

도 참조하십시오 ["ONTAP 릴리즈 노트"](#) 를 참조하십시오.

REST API 갭을 위해 ONTAPI를 제출하십시오

NetApp은 고객이 ONTAPI에서 ONTAP REST API로 마이그레이션할 수 있도록 지원하기 위해 노력하고 있습니다. REST API에 누락된 사항이 있는 경우 알려 주십시오. 에서 이러한 격차와 다른 아이디어를 제출할 수 있습니다 ["ONTAPI에서 REST API로"](#) 페이지.

ONTAPI를 REST API 매핑에 매핑

ONTAP REST API에는 대부분의 분야에서 ONTAPI와 동일한 기능이 포함되어 있습니다. NetApp은 ONTAPI 호출에서 동등한 REST API 호출로 매핑하는 방법을 설명하는 문서를 제공합니다.

API 매핑 설명서는 ONTAP 릴리즈에 따라 달라집니다.

- ["ONTAP 9.15.1"](#)
- ["ONTAP 9.14.1"](#)
- ["ONTAP 9.13.1"](#)
- ["ONTAP 9.12.1"](#)
- ["ONTAP 9.11.1"](#)
- ["ONTAP 9.10.1"](#)
- ["ONTAP 9.9.1"](#)
- ["ONTAP 9.8"](#)

성능 카운터

ONTAP 카운터 관리자는 각 ONTAP 시스템의 성능에 대한 광범위한 정보를 유지합니다. 이 데이터는 *performance* 카운터 세트에 내보내기되므로 ONTAP 시스템의 성능을 평가하고 성능

목표를 달성하는 데 사용할 수 있습니다.

ONTAP 성능 카운터에 액세스합니다

ONTAP 명령줄 인터페이스를 통해뿐만 아니라 두 개의 서로 다른 API를 사용하여 ONTAP 성능 카운터에 액세스할 수 있습니다.



ONTAP REST API는 ONTAP 구축 관리를 자동화할 때 선호되는 전략적 옵션입니다.

ONTAPI API를 참조하십시오

ONTAPI API는 NetApp Network Manageability SDK에서 사용할 수 있습니다. ONTAPI를 사용할 때 성능 카운터는 개체 컬렉션 내에서 정의됩니다. 각 객체는 시스템의 물리적 또는 가상 구성요소에 해당합니다. 시스템 구성에 따라 각 개체의 인스턴스가 하나 이상 있을 수 있습니다.

예를 들어, ONTAP 시스템에 4개의 물리적 디스크가 있는 경우의 인스턴스가 4개 있습니다 `disk` 각각 고유한 성능 카운터 집합이 있는 개체입니다. ONTAPI를 사용하여 각 디스크 인스턴스의 개별 카운터에 액세스할 수 있습니다.

ONTAP REST API를 참조하십시오

ONTAP 9.11.1부터 REST API를 통해 성능 데이터에 액세스할 수도 있습니다. 이 경우 성능 카운터는 ONTAPI 개체와 동일한 표로 구성됩니다. 각 테이블 행은 ONTAPI 개체의 인스턴스와 같습니다.

예를 들어, ONTAP 시스템에 4개의 물리 디스크가 있는 경우, 를 참조하십시오 `disk` 테이블에는 4개의 행이 포함됩니다. 각 행에 개별적으로 액세스할 수 있으며 해당 행의 필드나 열로 사용할 수 있는 자체 성능 카운터 집합이 포함되어 있습니다.

REST API 사용 준비

ONTAP REST API를 사용하여 성능 카운터에 액세스하기 전에 준비해야 합니다.

성능 카운터는 표로 정리되어 있습니다

ONTAPI 개체의 하위 집합은 ONTAP REST API를 통해 사용할 수 있으며 테이블로 표시됩니다. 예를 들어, ONTAPI * `hostadapter` * 개체는 REST API를 통해 * `host_adapter` * 테이블로 표시됩니다. 시스템의 각 호스트 어댑터는 자체 성능 카운터 세트가 있는 행입니다.

인스턴스 이름	성능 카운터					
host_adapter_1	TOTAL_READ_ops_1	TOTAL_WRITE_ops_1	바이트_읽기_1	바이트_쓰인_공간_1	MAX_LINK_D_ATA_RATE_1	RSCN_COUNT_1
Host_adapter_2	TOTAL_READ_ops_2	TOTAL_WRITE_ops_2	바이트_읽기_2	바이트_쓰인_공간_2	MAX_LINK_D_ATA_RATE_2	RSCN_COUNT_2
Host_adapter_3	TOTAL_READ_ops_3	TOTAL_WRITE_ops_3	바이트_읽기_3	바이트_쓰인_공간_3	MAX_LINK_D_ATA_RATE_3	RSCN_COUNT_3

나머지 끝점의 요약

ONTAP 성능 카운터 및 관련 테이블에 액세스할 수 있는 네 가지 주요 엔드포인트가 있습니다.



각 REST 끝점은 읽기 전용 액세스를 제공하며 * GET * HTTP 메서드만 지원합니다. 를 참조하십시오
"API 참조입니다" 를 참조하십시오.

- `*/cluster/counter/tables *`

카운터 테이블 및 해당 스키마 정의의 컬렉션을 반환합니다.

- `*/cluster/counter/tables/{name} *`

명명된 단일 카운터 테이블에 대한 정보를 반환합니다.

- `*/cluster/counter/tables/{counter_name}/rows *`

명명된 카운터 테이블의 행 컬렉션을 반환합니다.

- `*/cluster/counter/tables/{counter_name}/rows/{id} *`

명명된 카운터 테이블에서 특정 행을 반환합니다.

ONTAPI에서 REST API로 마이그레이션

NetApp은 ONTAPI에서 ONTAP REST API로 자동화 코드를 마이그레이션하기 위한 광범위한 지원을 제공합니다. 여기에는 지정된 ONTAPI 개체에 대한 REST API에서 사용할 수 있는 동등한 성능 카운터 테이블을 식별하는 문서가 포함됩니다.

사용 중인 ONTAP 릴리스에 따라 적절한 매핑 설명서를 참조하십시오.

- ["ONTAP 9.15.1 성능 카운터 매핑"](#)
- ["ONTAP 9.14.1 성능 카운터 매핑"](#)
- ["ONTAP 9.13.1 성능 카운터 매핑"](#)
- ["ONTAP 9.12.1 성능 카운터 매핑"](#)
- ["ONTAP 9.11.1 성능 카운터 매핑"](#)

ONTAP REST API를 시작합니다

다음 예제에서는 REST API를 사용하여 ONTAP 성능 카운터에 액세스하는 방법을 보여 줍니다. 여기에는 사용 가능한 테이블 목록을 검색하고 테이블 구조를 탐색하는 작업이 포함됩니다.

시작하기 전에

예제를 사용하기 전에 다음 정보를 검토하십시오.

ONTAP 자격 증명

암호를 포함한 ONTAP 관리자 계정이 필요합니다.

클러스터 관리 IP

ONTAP 시스템에 대해 구성된 클러스터 관리 IP 주소가 필요합니다.

모든 API 호출은 `get` 메서드를 사용합니다

아래에 포함된 모든 예제는 HTTP GET 메서드를 사용하여 정보를 검색하는 데만 사용할 수 있습니다.

변수 대체

각 curl 예제에는 대문자 및 괄호 텍스트로 표시된 하나 이상의 변수가 포함됩니다. 이러한 변수를 사용자 환경에 적합한 실제 값으로 바꿉니다.

예제는 끝점과 일치합니다

아래 예제 순서는 성능 카운터를 검색하는 데 사용할 수 있는 REST 끝점을 사용하는 방법을 보여 줍니다. 을 참조하십시오 [나머지 끝점의 요약](#) 를 참조하십시오.

예 1: 모든 성능 카운터 테이블

이 REST API 호출을 사용하여 사용 가능한 모든 카운터 관리자 테이블을 검색할 수 있습니다.

컬의 예

```
curl --request GET --user admin:<PASSWORD>  
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables'
```

```
{
  "records": [
    {
      "name": "copy_manager",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/copy_manager"
        }
      }
    },
    {
      "name": "copy_manager:constituent",
      "_links": {
        "self": {
          "href":
"/api/cluster/counter/tables/copy_manager%3Aconstituent"
        }
      }
    },
    {
      "name": "disk",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk"
        }
      }
    },
    {
      "name": "disk:constituent",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk%3Aconstituent"
        }
      }
    },
    {
      "name": "disk:raid_group",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/disk%3Araid_group"
        }
      }
    }
  ],
}
```

```

{
  "name": "external_cache",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/external_cache"
    }
  }
},
{
  "name": "fcp",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp"
    }
  }
},
{
  "name": "fcp:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp%3Anode"
    }
  }
},
{
  "name": "fcp_lif",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp_lif"
    }
  }
},
{
  "name": "fcp_lif:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp_lif%3Anode"
    }
  }
},
{
  "name": "fcp_lif:port",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/fcp_lif%3Aport"
    }
  }
}

```

```

    }
  },
  {
    "name": "fcp_lif:svm",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/fcp_lif%3Asvm"
      }
    }
  },
  {
    "name": "fcvi",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/fcvi"
      }
    }
  },
  {
    "name": "headroom_aggregate",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/headroom_aggregate"
      }
    }
  },
  {
    "name": "headroom_cpu",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/headroom_cpu"
      }
    }
  },
  {
    "name": "host_adapter",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/host_adapter"
      }
    }
  },
  {
    "name": "iscsi_lif",
    "_links": {
      "self": {

```

```

        "href": "/api/cluster/counter/tables/iscsi_lif"
    }
}
},
{
    "name": "iscsi_lif:node",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/iscsi_lif%3Anode"
        }
    }
},
{
    "name": "iscsi_lif:svm",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/iscsi_lif%3Asvm"
        }
    }
},
{
    "name": "lif",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/lif"
        }
    }
},
{
    "name": "lif:svm",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/lif%3Asvm"
        }
    }
},
{
    "name": "lun",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/lun"
        }
    }
},
{
    "name": "lun:constituent",

```

```

    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/lun%3Aconstituent"
      }
    }
  },
  {
    "name": "lun:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/lun%3Anode"
      }
    }
  },
  {
    "name": "namespace",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/namespace"
      }
    }
  },
  {
    "name": "namespace:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/namespace%3Aconstituent"
      }
    }
  },
  {
    "name": "nfs_v4_diag",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/nfs_v4_diag"
      }
    }
  },
  {
    "name": "nic_common",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/nic_common"
      }
    }
  }
},

```

```

{
  "name": "nvmf_lif",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif"
    }
  }
},
{
  "name": "nvmf_lif:constituent",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif%3Aconstituent"
    }
  }
},
{
  "name": "nvmf_lif:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif%3Anode"
    }
  }
},
{
  "name": "nvmf_lif:port",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/nvmf_lif%3Aport"
    }
  }
},
{
  "name": "object_store_client_op",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/object_store_client_op"
    }
  }
},
{
  "name": "path",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/path"
    }
  }
}

```

```

    }
  },
  {
    "name": "processor",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/processor"
      }
    }
  },
  {
    "name": "processor:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/processor%3Anode"
      }
    }
  },
  {
    "name": "qos",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/qos"
      }
    }
  },
  {
    "name": "qos:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/qos%3Aconstituent"
      }
    }
  },
  {
    "name": "qos:policy_group",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/qos%3Apolicy_group"
      }
    }
  },
  {
    "name": "qos_detail",
    "_links": {
      "self": {

```

```

        "href": "/api/cluster/counter/tables/qos_detail"
    }
}
},
{
    "name": "qos_detail_volume",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qos_detail_volume"
        }
    }
},
{
    "name": "qos_volume",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qos_volume"
        }
    }
},
{
    "name": "qos_volume:constituent",
    "_links": {
        "self": {
            "href":
"/api/cluster/counter/tables/qos_volume%3Aconstituent"
        }
    }
},
{
    "name": "qtree",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qtree"
        }
    }
},
{
    "name": "qtree:constituent",
    "_links": {
        "self": {
            "href": "/api/cluster/counter/tables/qtree%3Aconstituent"
        }
    }
},
{

```

```

    "name": "svm_cifs",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_cifs"
      }
    }
  },
  {
    "name": "svm_cifs:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_cifs%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_cifs:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_cifs%3Anode"
      }
    }
  },
  {
    "name": "svm_nfs_v3",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v3"
      }
    }
  },
  {
    "name": "svm_nfs_v3:constituent",
    "_links": {
      "self": {
        "href":
"/api/cluster/counter/tables/svm_nfs_v3%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_nfs_v3:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v3%3Anode"
      }
    }
  }
}

```

```

    }
  },
  {
    "name": "svm_nfs_v4",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v4"
      }
    }
  },
  {
    "name": "svm_nfs_v41",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v41"
      }
    }
  },
  {
    "name": "svm_nfs_v41:constituent",
    "_links": {
      "self": {
        "href":
"/api/cluster/counter/tables/svm_nfs_v41%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_nfs_v41:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v41%3Anode"
      }
    }
  },
  {
    "name": "svm_nfs_v42",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v42"
      }
    }
  },
  {
    "name": "svm_nfs_v42:constituent",
    "_links": {

```

```

    "self": {
      "href":
"/api/cluster/counter/tables/svm_nfs_v42%3Aconstituent"
    }
  },
  {
    "name": "svm_nfs_v42:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v42%3Anode"
      }
    }
  },
  {
    "name": "svm_nfs_v4:constituent",
    "_links": {
      "self": {
        "href":
"/api/cluster/counter/tables/svm_nfs_v4%3Aconstituent"
      }
    }
  },
  {
    "name": "svm_nfs_v4:node",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/svm_nfs_v4%3Anode"
      }
    }
  },
  {
    "name": "system",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/system"
      }
    }
  },
  {
    "name": "system:constituent",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/system%3Aconstituent"
      }
    }
  }
}

```

```

},
{
  "name": "system:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/system%3Anode"
    }
  }
},
{
  "name": "token_manager",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/token_manager"
    }
  }
},
{
  "name": "volume",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/volume"
    }
  }
},
{
  "name": "volume:node",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/volume%3Anode"
    }
  }
},
{
  "name": "volume:svm",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/volume%3Asvm"
    }
  }
},
{
  "name": "waf1",
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/waf1"
    }
  }
}

```

```

    }
  },
  {
    "name": "waf1_comp_aggr_vol_bin",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/waf1_comp_aggr_vol_bin"
      }
    }
  },
  {
    "name": "waf1_hya_per_aggregate",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/waf1_hya_per_aggregate"
      }
    }
  },
  {
    "name": "waf1_hya_sizer",
    "_links": {
      "self": {
        "href": "/api/cluster/counter/tables/waf1_hya_sizer"
      }
    }
  }
],
"num_records": 71,
"_links": {
  "self": {
    "href": "/api/cluster/counter/tables"
  }
}
}
}

```

예 2: 특정 테이블에 대한 고급 정보

이 REST API 호출을 사용하여 특정 테이블에 대한 설명과 메타데이터를 표시할 수 있습니다. 이 출력에는 테이블의 목적과 각 성능 카운터에 포함된 데이터 유형이 포함됩니다. 이 예에서는 * host_adapter * 테이블을 사용합니다.

컬의 예

```
curl --request GET --user admin:<PASSWORD>  
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter'
```

JSON 출력 예

```
{
  "name": "host_adapter",
  "description": "The host_adapter table reports activity on the Fibre Channel, Serial Attached SCSI, and parallel SCSI host adapters the storage system uses to connect to disks and tape drives.",
  "counter_schemas": [
    {
      "name": "bytes_read",
      "description": "Bytes read through a host adapter",
      "type": "rate",
      "unit": "per_sec"
    },
    {
      "name": "bytes_written",
      "description": "Bytes written through a host adapter",
      "type": "rate",
      "unit": "per_sec"
    },
    {
      "name": "max_link_data_rate",
      "description": "Max link data rate in Kilobytes per second for a host adapter",
      "type": "raw",
      "unit": "kb_per_sec"
    },
    {
      "name": "node.name",
      "description": "System node name",
      "type": "string",
      "unit": "none"
    },
    {
      "name": "rscn_count",
      "description": "Number of RSCN(s) received by the FC HBA",
      "type": "raw",
      "unit": "none"
    },
    {
      "name": "total_read_ops",
      "description": "Total number of reads on a host adapter",
      "type": "rate",
      "unit": "per_sec"
    }
  ],
}
```

```

    {
      "name": "total_write_ops",
      "description": "Total number of writes on a host adapter",
      "type": "rate",
      "unit": "per_sec"
    }
  ],
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter"
    }
  }
}

```

예 3: 특정 테이블의 모든 행

이 REST API 호출을 사용하여 테이블의 모든 행을 볼 수 있습니다. Counter Manager 개체의 인스턴스를 나타냅니다.

컬의 예

```

curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter/rows'

```

JSON 출력 예

```
{
  "records": [
    {
      "id": "dmp-adapter-01",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-01"
        }
      }
    },
    {
      "id": "dmp-adapter-02",
      "_links": {
        "self": {
          "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-02"
        }
      }
    }
  ],
  "num_records": 2,
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter/rows"
    }
  }
}
```

예제 4: 특정 테이블의 단일 행

이 REST API 호출을 사용하여 테이블의 특정 Counter Manager 인스턴스에 대한 성능 카운터 값을 볼 수 있습니다. 이 예에서는 호스트 어댑터 중 하나에 대한 성능 데이터가 요청됩니다.

컬의 예

```
curl --request GET --user admin:<PASSWORD>
'https://<ONTAP_IP_ADDRESS>/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-01'
```

JSON 출력 예



```

{
  "counter_table": {
    "name": "host_adapter"
  },
  "id": "dmp-adapter-01",
  "properties": [
    {
      "name": "node.name",
      "value": "dmp-node-01"
    }
  ],
  "counters": [
    {
      "name": "total_read_ops",
      "value": 25098
    },
    {
      "name": "total_write_ops",
      "value": 48925
    },
    {
      "name": "bytes_read",
      "value": 1003799680
    },
    {
      "name": "bytes_written",
      "value": 6900961600
    },
    {
      "name": "max_link_data_rate",
      "value": 0
    },
    {
      "name": "rscn_count",
      "value": 0
    }
  ],
  "_links": {
    "self": {
      "href": "/api/cluster/counter/tables/host_adapter/rows/dmp-adapter-01"
    }
  }
}

```

툴 및 소프트웨어

NetApp에서 샘플 Python 스크립트 및 기타 관련 소프트웨어를 제공하여 ONTAPI에서 ONTAP REST API로 마이그레이션하는 데 도움이 됩니다. 이 샘플들 중 가장 중요한 것은 아래에 설명되어 있습니다.



모든 Python 코드 샘플은 에서 사용할 수 있습니다 "[NetApp ONTAP REST Python](#)" GitHub 리포지토리.

ONTAPI 사용 보고 도구

ONTAPI 사용 보고 툴은 NetApp 프로페셔널 서비스, 고객 및 파트너가 ONTAP 환경에서 ONTAPI 사용을 식별할 수 있도록 설계되었습니다. 스크립트는 아래 표에 설명된 세 가지 사용 사례에 대해 제공됩니다.

스크립트	설명
apache_scraper.py	ONTAP 노드에 대해 실행된 ONTAPI 호출을 찾기 위한 Apache 로그 스크레이퍼입니다
session_stats.py	ONTAP에서 세션 통계 데이터를 검색하는 CLI 스크립트입니다
zapi_to_rest.py	전달된 ONTAPI 호출 및 속성의 나머지 세부 정보를 추출하기 위한 스크립트입니다

에 액세스할 수 있습니다 "[ONTAPI 사용 보고 도구](#)" 시작하십시오. 도 참조하십시오 "[데모](#)" 보고 도구 및 사용 방법

전용 CLI를 통과합니다

REST API는 ONTAP에서 사용할 수 있는 다양한 기능과 시설을 제공합니다. 그러나 REST API를 통해 ONTAP CLI에 직접 액세스하는 것이 유용한 경우가 있을 수 있습니다.

이 기능에 대한 소개는 를 참조하십시오 "[REST API를 통해 ONTAP CLI에 액세스합니다](#)". Python 샘플은 을 참조하십시오 "[REST CLI 통과 샘플입니다](#)".

Python 클라이언트 라이브러리

Python 클라이언트 라이브러리는 Python을 사용하여 ONTAP REST API에 설치하고 액세스하는 데 사용할 수 있는 패키지입니다. 이를 통해 ONTAP 배포를 자동화하기 위한 강력한 코드를 빠르게 개발할 수 있습니다.

Python 클라이언트 라이브러리에 대한 소개는 을 참조하십시오 "[Python 클라이언트 라이브러리 개요](#)". Python 샘플은 을 참조하십시오 "[Python 클라이언트 라이브러리의 예](#)".

ONTAP PowerShell 툴킷

NetApp.ONTAP PowerShell Toolkit에는 2,400개 이상의 cmdlet이 포함된 모듈로 로컬 PowerShell 환경을 개선합니다. 이를 통해 Windows 호스트용 코드를 빠르게 개발하여 ONTAP 배포를 자동화할 수 있습니다. 자세한 내용은 을 참조하십시오 "[PowerShell Toolkit 개요](#)".

블로그 기사를 참조하십시오

ONTAPI에서 ONTAP REST API로 마이그레이션하는 방법을 더 잘 이해하는 데 도움이 되는 몇

가지 블로그 문서가 있습니다.

ONTAPI - REST 매핑

NetApp은 매핑 문서를 통해 독점 ONTAPI API에서 ONTAP REST API로 이동할 수 있도록 지원합니다.

["NetApp.IO/2020/12/17/ontapi-to-rest-mapping"](https://netapp.io/2020/12/17/ontapi-to-rest-mapping)

ONTAP API에서 ONTAP REST API로 자동화 전환

REST API를 기반으로 ONTAP 자동화 환경을 변환하는 데 사용할 수 있는 몇 가지 기술이 있습니다.

["www.netapp.com/blog/transform-automation-ontap-rest-api"](https://www.netapp.com/blog/transform-automation-ontap-rest-api)

전용 CLI를 사용하면 **ONTAP REST API**를 통해 패스스루를 수행할 수 있습니다

CLI 및 ONTAP 사용자가 ONTAP REST API로 전환할 수 있도록 ONTAP는 모든 CLI 명령에 액세스하는 데 사용할 수 있는 전용 REST API 엔드포인트를 제공합니다.

["https://netapp.io/2020/11/09/private-cli-passthrough-ontap-rest-api"](https://netapp.io/2020/11/09/private-cli-passthrough-ontap-rest-api)

ONTAPI Usage Reporting Tool을 사용하여 ONTAPI에서 전환

NetApp은 고객과 파트너가 ONTAP REST API로 전환할 수 있도록 지원합니다.

["NetApp.IO/2022/03/21/Transitioning-from-ontapi-using-ontapi-usage-reporting-tool"](https://netapp.io/2022/03/21/Transitioning-from-ontapi-using-ontapi-usage-reporting-tool)

API 참조입니다

API 참조에는 HTTP 메서드, 입력 매개 변수 및 응답을 포함하여 ONTAP REST API 호출에 대한 세부 정보가 포함되어 있습니다. 이 전체 참조는 REST API를 사용하여 자동화 응용 프로그램을 개발할 때 유용합니다.



REST API 참조 문서는 ONTAP 릴리즈에 기반한 여러 사이트 중 하나에서 액세스할 수 있습니다. 해당 문서의 사본은 로컬 ONTAP 시스템의 Swagger UI를 통해서도 제공됩니다.

온라인으로 ONTAP API 참조 문서에 액세스합니다

아래 링크를 통해 ONTAP REST API 참조 설명서 사본에 액세스할 수 있습니다. 문서는 ONTAP 릴리스에서 관리합니다.

- ["ONTAP 9.15.1"](#)
- ["ONTAP 9.14.1"](#)
- ["ONTAP 9.13.1"](#)
- ["ONTAP 9.12.1"](#)
- ["ONTAP 9.11.1"](#)
- ["ONTAP 9.10.1"](#)
- ["ONTAP 9.9.1"](#)
- ["ONTAP 9.8"](#)
- ["ONTAP 9.7"](#)
- ["ONTAP 9.6"](#)

Swagger UI를 통해 ONTAP API 참조 문서에 액세스합니다

로컬 ONTAP 시스템에서 Swagger UI를 통해 ONTAP REST API 설명서에 액세스할 수 있습니다.

시작하기 전에

다음 항목이 있어야 합니다.

- ONTAP 클러스터 관리 LIF의 IP 주소 또는 호스트 이름입니다
- ONTAP REST API 액세스 권한이 있는 계정의 사용자 이름 및 암호

단계

1. 브라우저에 URL을 입력하고 * Enter * 를 누릅니다.

"https://<ip_address>/docs/api"

2. ONTAP 계정을 사용하여 로그인합니다.

ONTAP API 설명서 페이지는 하단의 주요 리소스 범주로 구성된 API 호출과 함께 표시됩니다.

3. 개별 API 호출의 예로 * cluster * 범주로 스크롤하고 * get/cluster * 를 클릭합니다.

자세한 정보

ONTAP 스토리지 시스템의 구축과 관리를 자동화하는 데 도움이 되는 몇 가지 추가 리소스가 있습니다.

블로그 기사를 참조하십시오

- 현재 ONTAP 자동화 기술에 대한 요약

["새로운 업계 표준이 도입되었습니다"](#)

- ONTAP REST API용 GitHub에서 Python 샘플 스크립트 액세스 및 사용 소개

["GitHub에서 샘플 스크립트를 사용해 보십시오"](#)

- CLI passthrough는 REST API를 사용하여 ONTAP CLI 명령을 실행하는 기술을 제공합니다.

["전용 CLI를 사용하면 ONTAP REST API를 통해 패스스루를 수행할 수 있습니다"](#)

- ONTAP 자동화를 위해 Ansible을 처음 사용하는 경우, 시작하는 것이 좋습니다.

["NetApp 및 Ansible 시작하기: Ansible을 설치하십시오"](#)

- ONTAP REST API를 사용하여 파일 보안 및 권한 관리를 탐색할 수 있습니다.

["ONTAP REST API를 통해 파일 보안 권한 관리 간소화"](#)

- ONTAP 이벤트를 모니터링하여 시스템 활동을 계속 파악할 수 있습니다. REST API를 사용하여 이러한 이벤트의 구성 및 관리를 자동화할 수 있습니다.

["ONTAP REST API: 심각도가 높은 이벤트 자동 알림"](#)

- REST API를 사용하여 RBAC 보안 환경의 일부로 역할 및 액세스 수준을 구성할 수 있습니다.

["ONTAP REST API를 사용한 RBAC\(역할 기반 액세스 제어\)"](#)

- NetApp는 ONTAP REST API를 사용하기 위한 Python 샘플 스크립트를 제공합니다.

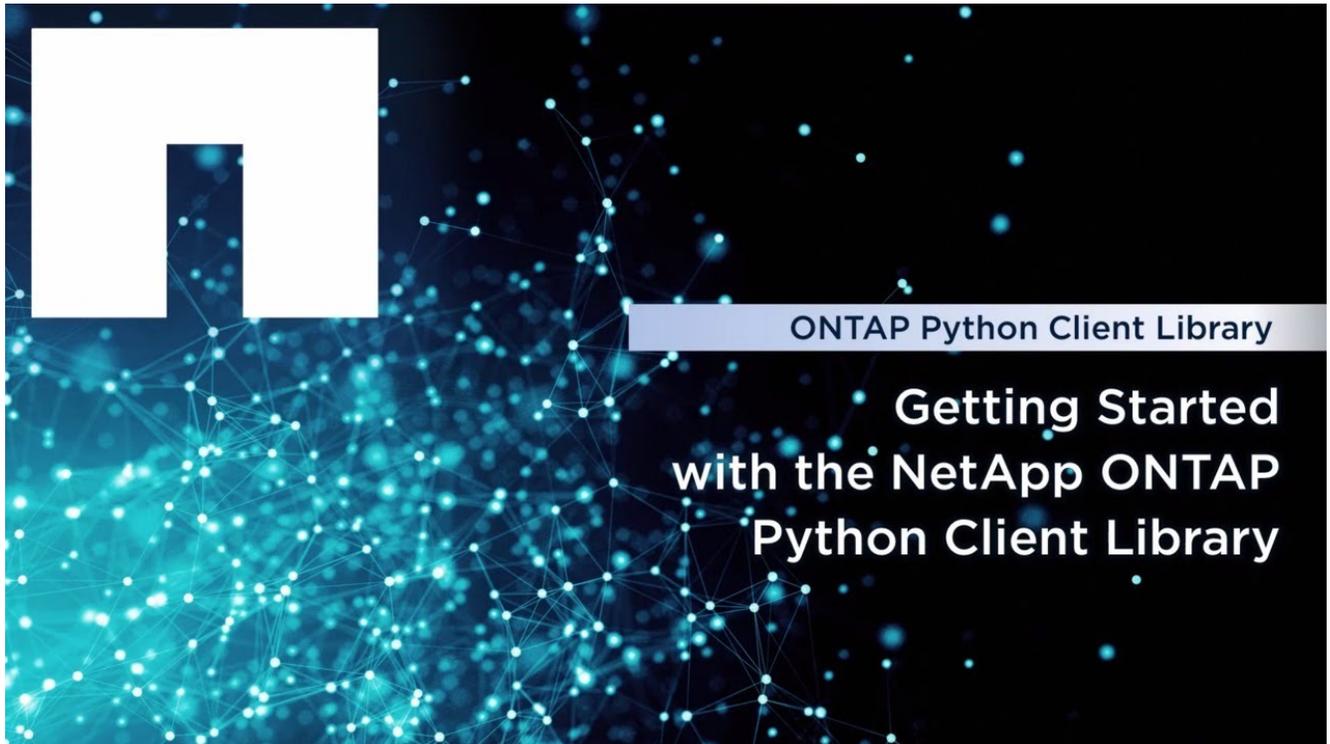
["ONTAP REST API Python 샘플 스크립트를 이제 GitHub에서 사용할 수 있습니다!"](#)

- 커피는 휴식 (6 에피소드).

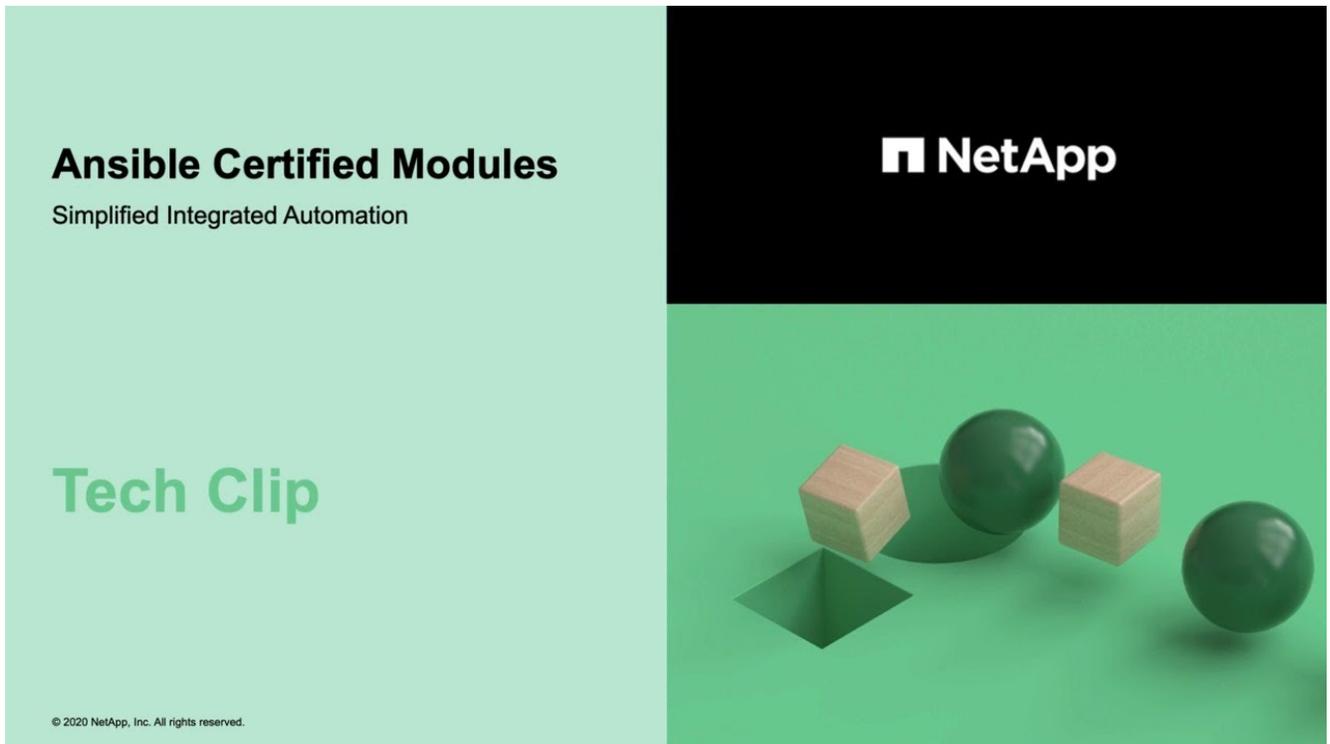
- ["ONTAP REST API 기초"](#)
- ["ONTAP REST API의 기능"](#)
- ["포스트맨을 사용하여 ONTAP REST에 대한 실습"](#)
- ["ONTAPI\(ZAPI\) 보고 도구"](#)
- ["전용 CLI 패스스루"](#)
- ["ONTAP 스토리지를 간편하게 자동화해 주는 5가지 강력한 기능!"](#)

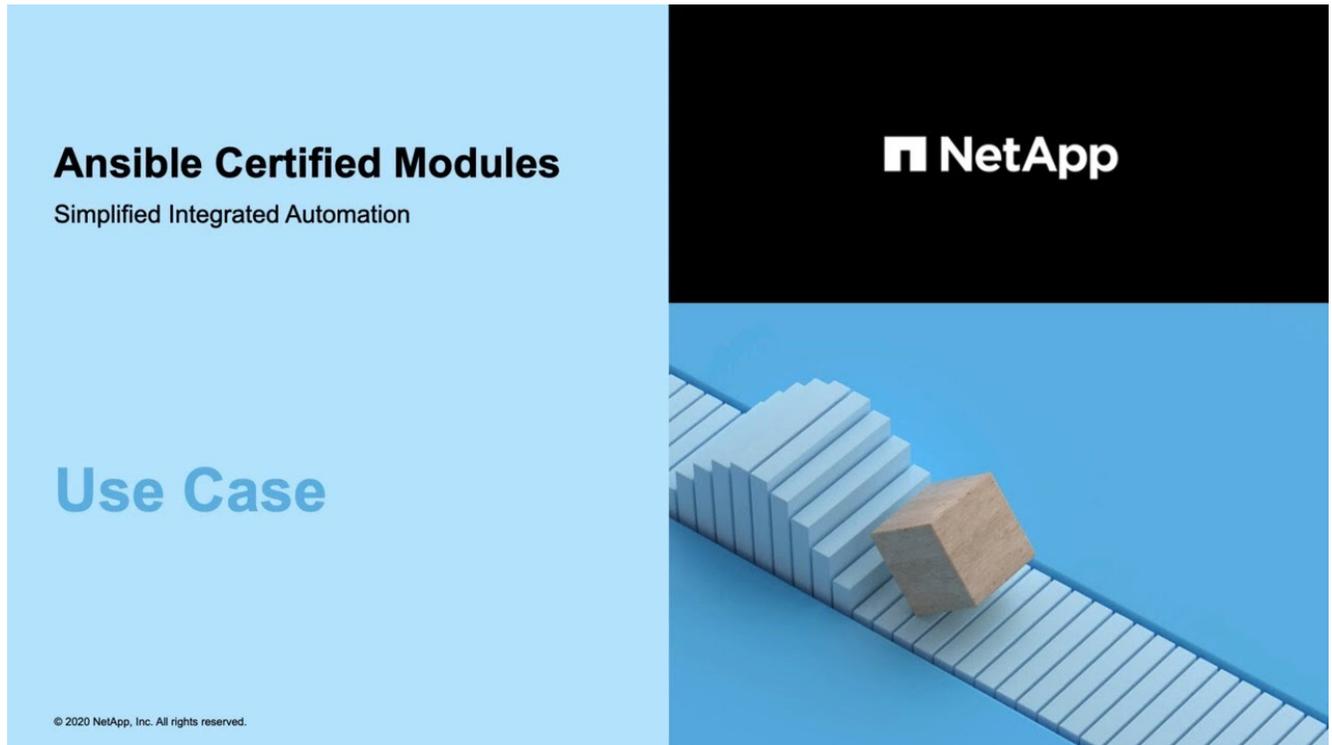
비디오

- NetApp Python 클라이언트 라이브러리에 대한 소개 및 라이브러리를 사용하여 코드 작성을 시작하는 방법



- Ansible 인증 모듈을 살펴보십시오.





- NetApp TechComm TV의 비디오 컬렉션입니다.

["NetApp ONTAP 관리를 자동화합니다"](#)

기술 교육 및 이벤트

- Insight 2022 프레젠테이션(26분)

["ONTAP REST API로 ONTAP 스토리지 관리를 현대화하십시오"](#)

- INSIGHT 2021 프레젠테이션(31분)

["NetApp ONTAP: REST API를 사용하여 시간을 절약하고 단순화합니다"](#)

- NetApp 학습 서비스:

["ONTAP REST API 및 Ansible을 사용하여 스토리지 관리 자동화"](#)

NetApp 기술 자료

- ONTAP REST API에 문제가 발생한 경우 NetApp에 보고할 수 있습니다.

["ONTAP REST API 및 ONTAP REST API Python 클라이언트 라이브러리의 문제를 보고하는 방법"](#)

- ONTAP REST API에서 기능 격차를 확인할 경우 API에 대한 새로운 기능을 요청할 수 있습니다.

["ONTAP REST API에 대한 기능을 요청하는 방법"](#)

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

개인 정보 보호 정책

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 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 라이선스와 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 라이선스도 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 라이선스를 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 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

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