Active IQ Unified Manager 문서

Active IQ Unified Manager 9.14

NetApp
March 07, 2024

This PDF was generated from https://docs.netapp.com/ko-kr/active-iq-unified-manager/index.html on March 07, 2024. Always check docs.netapp.com for the latest.

목차

Active IQ Unified Manager 문서 . . . 1
릴리스 정보 . . . 2
시작하십시오 . . . 3
VMware 설치를 위한 빠른 시작 지침 . . . 3
Linux 설치를 위한 빠른 시작 지침 . . . 4
Windows 설치를 위한 빠른 시작 지침 . . . 5
VMware vSphere 시스템에 Unified Manager를 설치합니다 . . . 7
Active IQ Unified Manager 소개 . . . 7
Unified Manager 설치 요구 사항 . . . 8
Unified Manager 소프트웨어의 설치, 업그레이드 및 제거 . . . 15
Linux 시스템에 Unified Manager를 설치합니다 . . . 24
Active IQ Unified Manager 소개 . . . 24
Unified Manager 설치 요구 사항 . . . 25
Unified Manager 소프트웨어의 설치, 업그레이드 및 제거 . . . 33
Windows 시스템에 Unified Manager를 설치합니다 . . . 53
Active IQ Unified Manager 소개 . . . 53
Unified Manager 설치 요구 사항 . . . 54
Unified Manager 소프트웨어의 설치, 업그레이드 및 제거 . . . 61
구성 및 관리 작업을 수행합니다 . . . 71
Active IQ Unified Manager 구성 . . . 71
Unified Manager 백업 구성 . . . 90
기능 설정 관리 . . . 90
유지보수 콘솔 사용 . . . 93
사용자 액세스 관리 . . . 106
SAML 인증 설정 관리 . . . 113
인증 관리 . . . 119
보안 인증서 관리 . . . 126
스토리지 모니터링 및 관리 . . . 133
Active IQ Unified Manager 소개 . . . 133
사용자 인터페이스 이해 . . . 136
대시보드에서 클러스터 모니터링 및 관리 . . . 143
클러스터 관리 . . . 153
VMware 가상 인프라스트럭처 모니터링 . . . 158
워크로드 프로비저닝 및 관리 . . . 167
MetroCluster 구성 관리 및 모니터링 . . . 182
할당량 관리 . . . 189
문제 해결 . . . 196
이벤트 및 알림을 관리합니다 . . . 203
이벤트 관리 . . . 203

- 알림 관리 289
- 스크립트 관리 303

클러스터 성능을 모니터링하고 관리합니다 313
- Active IQ Unified Manager 성능 모니터링 소개 313
- Unified Manager GUI에서 성능 워크플로우 탐색 316
- 대시보드에서 클러스터 성능 모니터링 326
- 워크로드 분석기를 사용하여 워크로드 문제 해결 328
- 성능 클러스터 랜딩 페이지에서 클러스터 성능을 모니터링합니다 330
- 성능 인벤토리 페이지를 사용하여 성능 모니터링 335
- 성능 탐색기 페이지를 사용하여 성능 모니터링 345
- QoS 정책 그룹 정보를 사용하여 성능 관리 363
- 성능 용량 및 사용 가능한 IOPS 정보를 사용하여 성능 관리 369
- 노드 장애 조치 계획 페이지의 이해 및 사용 376
- 데이터 수집 및 워크로드 성능 모니터링 380
- 성능 이벤트 및 경고 이해 387
- 성능 임계값 관리 397
- 성능 이벤트 분석 407
- 성능 이벤트 해결 421
- Unified Manager Server와 외부 데이터 공급자 간의 연결 설정 435

클러스터 상태를 모니터링하고 관리합니다 440
- Active IQ Unified Manager 상태 모니터링 소개 440
- 클러스터 및 클러스터 객체 상태 관리 및 모니터링 442
- 공통 Unified Manager 상태 워크플로우 및 작업 456

데이터 보호 및 복원 579
- 보호 관계 생성, 모니터링 및 문제 해결 579
- 보호 관계 관리 및 모니터링 591

사용자 정의 보고서를 생성합니다 665
- Unified Manager 보고 665
- 보고서 작업 670
- 보고서 예약 678
- 샘플 사용자 지정 보고서 683
- Microsoft Excel 보고서 예제 699

REST API를 사용하여 스토리지 관리 710
- Active IQ Unified Manager REST API 시작하기 710
- Active IQ Unified Manager에서 REST API 액세스 및 인증 714
- Unified Manager REST API 724
- 스토리지 관리를 위한 공통 API 워크플로우 753

법적 고지 786
- 저작권 786
- 상표 786
- 특허 786

개인 정보 보호 정책 786
오픈 소스 786

Active IQ Unified Manager 문서

릴리스 정보

Active IQ Unified Manager 9.14의 새로운 기능, 제한 사항 및 알려진 문제에 대한 요약을 제공합니다.

자세한 내용은 를 참조하십시오 "Active IQ Unified Manager 릴리즈 노트".

시작하십시오

VMware 설치를 위한 빠른 시작 지침

를 다운로드할 수 있습니다 `.tar` 루트 인증서가 포함된 파일, a `README` 파일, 및 `OVA` Unified Manager를 가상 어플라이언스로 구축하여 파일 및 구축

시스템 요구 사항

- 운영 체제: VMware ESXi 7.0 및 8.0
- RAM: 12GB
- CPU: 총 9572MHz
- 사용 가능한 디스크 공간: 5GB(씬 프로비저닝), 152GB(일반 프로비저닝)

시스템 요구 사항에 대한 자세한 내용은 를 참조하십시오 "Unified Manager 설치 요구 사항" 및 "상호 운용성 매트릭스".

Active IQ Unified Manager를 설치하는 중입니다

설치 프로그램을 다운로드합니다

1. 를 다운로드합니다 `.tar` 루트 인증서가 포함된 파일, a `README` 파일, 및 `OVA` 파일.
2. 파일을 vSphere Client에서 액세스할 수 있는 로컬 디렉토리 또는 네트워크 디렉토리에 저장합니다.
3. 를 다운로드한 디렉토리 `.tar` 파일에서 를 입력합니다 `tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz` 명령. + 필수 요소입니다 `OVA` 파일, 루트 인증서 및 입니다 `README` 타겟 디렉토리에 파일 압축이 풀립니다.

무결성을 확인합니다

의 무결성을 확인할 수 있습니다 `OVA` 에 나와 있는 단계에 따라 파일을 엽니다 `README` 파일.

Unified Manager를 설치합니다

1. vSphere Client에서 * File > Deploy OVF Template * 을 클릭합니다.
2. OVA 파일을 찾아 마법사를 사용하여 ESXi 서버에 가상 어플라이언스를 구축합니다.
3. 검토 세부 정보 페이지의 게시자 섹션에서 메시지를 표시합니다 `Entrust Code Signing - OVCS2 (Trusted certificate)` 다운로드한 의 무결성을 확인합니다 `OVA` 파일. 을 클릭합니다 `Entrust Code Signing - OVCS2 (Invalid certificate)`에서 VMware vCenter Server를 7.0U3E 이상 버전으로 업그레이드합니다.
4. 템플릿 사용자 정의 페이지의 속성 탭에서 수행 중인 설치 유형에 필요한 필드를 입력합니다.
   - 정적 구성의 경우 모든 필드에 필수 정보를 입력합니다. Secondary DNS* 필드에 대한 정보를 추가할 필요가 없습니다.
   - IPv4를 사용하는 DHCP의 경우 필드에 정보를 추가하지 마십시오.
   - IPv6을 사용하는 DHCP의 경우 “자동 IPv6 주소 지정 활성화” 상자를 선택합니다. 다른 필드에 정보를 추가하지 마십시오.

5. VM의 전원을 켭니다.
6. 콘솔 탭을 클릭하여 초기 부팅 프로세스를 봅니다.
7. 시간대를 구성합니다.
8. Unified Manager 유지보수 사용자 이름과 암호를 입력합니다.

설치가 끝나면 Unified Manager 웹 UI에 연결할 정보가 표시됩니다.

Linux 설치를 위한 빠른 시작 지침

설치 패키지를 다운로드하여 물리적 또는 가상 Red Hat Enterprise Linux 또는 CentOS 플랫폼에 Unified Manager를 설치할 수 있습니다.

시스템 요구 사항

- 운영 체제: Red Hat Enterprise Linux 버전 7.x 및 8.8에서 8.8까지 또는 x86_64 아키텍처 기반의 CentOS 버전 7.x로, OS 설치 프로그램의 * Software Selection * 옵션에서 "GUI 기반 서버" 기본 환경을 사용하여 설치됩니다
- RAM: 12GB, CPU: 총 9572MHz
- 사용 가능한 디스크 공간: '/opt/netapp/data' 디렉토리에 100GB, 루트 파티션에 50GB 디스크 공간이 있습니다. 별도로 마운트된 '/opt' 및 '/var/log' 디렉토리의 경우, '/opt'에 15GB가 있고, '/var/log'에 16GB가 있고, '/tmp'에 10GB의 여유 공간이 있는지 확인하십시오.

시스템 요구 사항에 대한 자세한 내용과 보안 사이트에 제품을 설치하는 방법에 대한 자세한 내용은 을 참조하십시오 "Unified Manager 설치 요구 사항" 및 "상호 운용성 매트릭스".

Active IQ Unified Manager를 설치하는 중입니다

설치 프로그램을 다운로드합니다

1. 를 다운로드합니다 `ActiveIQUnifiedManager-<version>.zip` 코드 서명 인증서와 함께 설치 패키지 (`.pem`) 및 디지털 서명 (`.sig`)를 클릭합니다.
2. 설치 파일을 다운로드한 디렉토리에서 다음을 실행합니다.

   '#unzip ActiveIQUnifiedManager-<version>.zip'

무결성을 확인합니다

다음 명령을 실행하여 설치 프로그램 패키지의 무결성을 확인합니다.

- 실행 `openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem > <public_key_file_name>` 코드 서명 인증서의 공개 키로 파일을 만들려면
- 실행 `openssl dgst -sha256 -verify <public_key_file_name> -signature <signature_file_name> ActiveIQUnifiedManager-<version>.zip` 설치 프로그램 패키지의 서명을 확인합니다.

리포지토리 구성을 확인합니다

Red Hat Enterprise Linux 또는 CentOS 리포지토리를 구성하는 절차는 사이트에 따라 다릅니다. 설치 패키지에 포함된 "pre_install_check.sh" 스크립트를 사용하여 운영 체제의 구성을 확인할 수 있습니다. 시스템이 인터넷에 연결되어 있는 경우 Red Hat Enterprise Linux 또는 CentOS 리포지토리를 설정하는 지침이 자동으로 제공됩니다.

'#sudo./pre_install_check.sh'

Unified Manager를 설치합니다

Unified Manager는 'yum' 유틸리티를 사용하여 소프트웨어와 종속 소프트웨어를 설치합니다. Red Hat Enterprise Linux 또는 CentOS의 이미지가 다양하기 때문에 설치된 패키지는 이미지에 있는 소프트웨어에 따라 다릅니다. yum 유틸리티는 설치할 종속 소프트웨어 패키지를 결정합니다. 종속 소프트웨어 패키지에 대한 자세한 내용은 를 참조하십시오 "Linux 소프트웨어 및 설치 요구 사항".

Unified Manager를 설치하려면 설치 파일의 압축이 풀린 디렉토리에서 루트 사용자 또는 'SUDO'를 사용하여 다음 명령을 실행합니다.

'#yum install netapp-um <version>.x86_64.rpm'

또는

'%sudo yum install netapp-um <version>.x86_64.rpm'

설치가 끝나면 Unified Manager 웹 UI에 연결할 정보가 표시됩니다. 웹 UI에 연결할 수 없는 경우, 포트 443 제한 사항에 대한 자세한 내용은 소프트웨어와 함께 제공된 'reADME' 파일을 참조하십시오.

Windows 설치를 위한 빠른 시작 지침

설치 패키지를 다운로드하고 Unified Manager를 설치하여 데이터 스토리지 용량, 가용성, 성능 및 보호 문제를 모니터링하고 문제를 해결할 수 있습니다.

시스템 요구 사항

- 운영 체제
  - Microsoft Windows Server 2019 Standard 및 Datacenter Edition
  - Microsoft Windows Server 2022 Standard 및 Datacenter Edition

    Unified Manager는 64비트 Windows 운영 체제에서 다음 언어로 지원됩니다.

  - 영어
  - 일본어
  - 중국어 간체
- RAM: 12GB
- CPU: 총 9572MHz
- 사용 가능한 디스크 공간: 설치 디렉토리를 위한 100GB 디스크 공간, MySQL 데이터 디렉토리를 위한 50GB의 디스크 공간

시스템 요구 사항에 대한 자세한 내용은 를 참조하십시오 "Unified Manager 설치 요구 사항" 및 "상호 운용성 매트릭스".

Active IQ Unified Manager를 설치하는 중입니다

설치 프로그램을 다운로드합니다

1. 'ActiveIQUnifiedManager-<version>.exe' 설치 패키지를 다운로드합니다.
2. 설치 파일을 대상 시스템의 디렉토리에 복사합니다.

Unified Manager를 설치합니다

Unified Manager를 설치하려면 Microsoft .NET 4.5.2 이상 버전이 설치되어 있어야 합니다. 설치 프로세스 중에 Unified Manager가 필요에 따라 다른 타사 패키지를 설치합니다. 종속 소프트웨어 패키지에 대한 자세한 내용은 를 참조하십시오 "Windows 소프트웨어 및 설치 요구 사항".

1. 기본 로컬 관리자 계정을 사용하여 Windows에 로그인합니다.
2. 설치 파일을 다운로드한 디렉토리에서 마우스 오른쪽 버튼을 클릭하여 Unified Manager 실행 파일(.exe)을 관리자로 실행합니다.
3. 메시지가 표시되면 사용자 이름과 암호를 입력하여 Unified Manager 유지보수 사용자를 생성합니다.
4. 데이터베이스 연결 마법사에서 MySQL 루트 암호를 입력합니다.
5. 나머지 메시지에 따라 설치를 완료합니다.
6. 설치가 끝나면 * Finish * 를 클릭하면 Unified Manager 웹 UI가 표시됩니다.

VMware vSphere 시스템에 Unified Manager를 설치합니다

Active IQ Unified Manager 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태 및 성능을 모니터링 및 관리할 수 있습니다. Unified Manager를 Linux 서버, Windows 서버 또는 VMware 호스트의 가상 어플라이언스에 구축할 수 있습니다.

설치를 완료하고 관리할 클러스터를 추가한 후에는 Unified Manager에서 모니터링되는 스토리지 시스템의 용량, 가용성, 보호 및 성능 상태를 표시하는 그래픽 인터페이스를 제공합니다.

- 관련 정보 *

"NetApp 상호 운용성 매트릭스 툴"

Unified Manager 서버의 기능

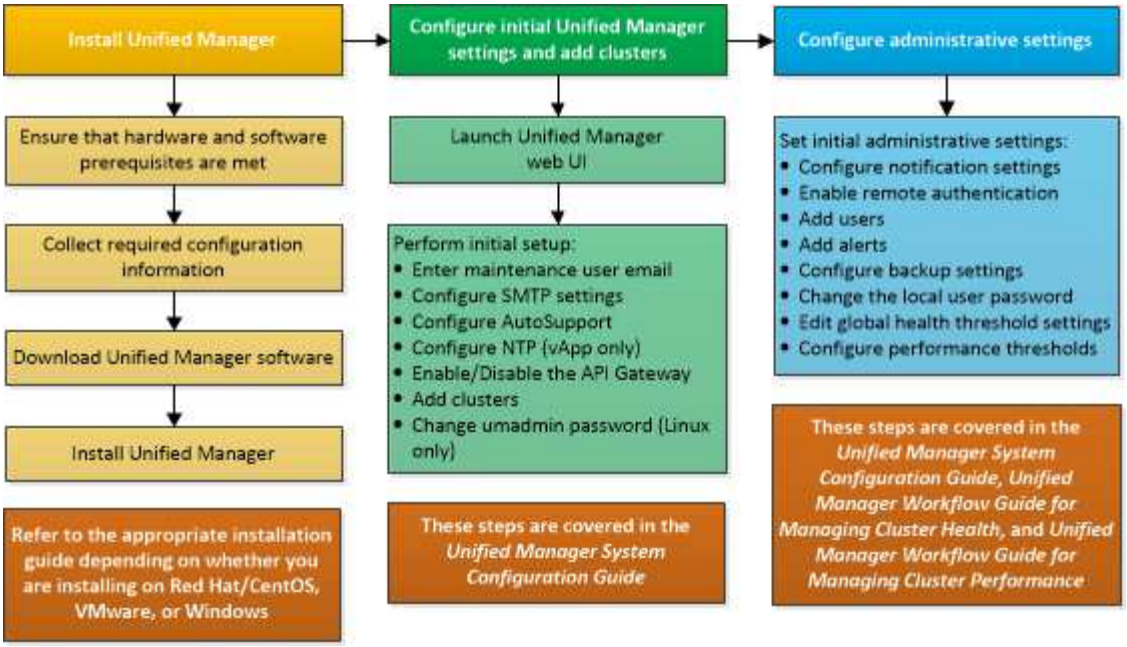
Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스 및 애플리케이션 서버로 구성됩니다. 검색, 모니터링, RBAC(역할 기반 액세스 제어), 감사, 로깅 등의 인프라 서비스를 제공합니다.

Unified Manager는 클러스터 정보를 수집하고, 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터 문제가 있는지 확인합니다.

설치 순서 개요

설치 워크플로우에서 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.

이 섹션에서는 아래 워크플로에 표시된 각 항목에 대해 설명합니다.



Unified Manager 설치 요구 사항

설치 프로세스를 시작하기 전에 Unified Manager를 설치할 서버가 특정 소프트웨어, 하드웨어, CPU 및 메모리 요구 사항을 충족하는지 확인하십시오.

NetApp은 Unified Manager 애플리케이션 코드의 수정을 지원하지 않습니다. Unified Manager 서버에 보안 조치를 적용해야 하는 경우 Unified Manager가 설치된 운영 체제를 변경해야 합니다.

Unified Manager 서버에 보안 조치를 적용하는 방법에 대한 자세한 내용은 기술 자료 문서를 참조하십시오.

"Clustered Data ONTAP을 위해 Active IQ Unified Manager에 적용된 보안 조치에 대한 지원 가능성"

- 관련 정보 *

자세한 내용은 을 참조하십시오 "NetApp 상호 운용성 매트릭스 툴"

가상 인프라 및 하드웨어 시스템 요구 사항

가상 인프라 또는 물리적 시스템에 Unified Manager를 설치하려면 메모리, CPU 및 디스크 공간에 대한 최소 요구사항을 충족해야 합니다.

다음 표에는 메모리, CPU 및 디스크 공간 리소스에 권장되는 값이 나와 있습니다. 이러한 값은 Unified Manager가 허용 가능한 성능 수준을 충족할 수 있도록 검증을 받았습니다.

하드웨어 구성	권장 설정
RAM	12GB(최소 요구 사항 8GB)
프로세서	CPU 4개

하드웨어 구성	권장 설정
CPU 사이클 용량입니다	총 9572MHz(최소 요구 사항 9572MHz)
사용 가능한 디스크 공간	• 5GB(씬 프로비저닝) • 152GB(씩 프로비저닝)

적은 용량의 메모리가 있는 시스템에 Unified Manager를 설치할 수 있지만 권장되는 12GB RAM을 사용하면 최적의 성능을 위해 충분한 메모리를 사용할 수 있으며, 따라서 시스템이 구성 증가에 따라 추가 클러스터 및 스토리지 오브젝트를 수용할 수 있습니다. Unified Manager가 구축된 VM에서 메모리 제한을 설정하지 말아야 하며, 시스템에서 할당된 메모리를 소프트웨어가 활용하지 못하는 기능(예: 풍선 벌루닝)을 사용하면 안 됩니다.

또한 Unified Manager의 두 번째 인스턴스를 설치하기 전에 Unified Manager의 단일 인스턴스에서 모니터링할 수 있는 노드 수에 제한이 있습니다. 자세한 내용은 을 참조하십시오 "Unified Manager 모범 사례 가이드".

메모리 페이지 스와핑은 시스템 및 관리 응용 프로그램의 성능에 부정적인 영향을 줍니다. 전체 호스트 활용률로 인해 CPU 리소스를 사용하지 않는 경우 성능이 저하될 수 있습니다.

전용 요구사항

Unified Manager를 설치하는 물리적 또는 가상 시스템은 Unified Manager에만 사용해야 하며 다른 애플리케이션과 공유해서는 안 됩니다. 다른 애플리케이션은 시스템 리소스를 소모하며 Unified Manager의 성능을 크게 줄일 수 있습니다.

백업에 필요한 공간 요구 사항

Unified Manager 백업 및 복원 기능을 사용하려면 "데이터" 디렉토리나 디스크에 150GB의 공간이 있도록 추가 용량을 할당합니다. 백업은 로컬 대상 또는 원격 대상에 쓸 수 있습니다. 모범 사례는 최소 150GB의 공간이 있는 Unified Manager 호스트 시스템 외부의 원격 위치를 식별하는 것입니다.

호스트 접속 구성 요구 사항

Unified Manager를 설치하는 물리적 시스템 또는 가상 시스템은 호스트 자체에서 호스트 이름을 성공적으로 "핑"할 수 있도록 구성해야 합니다. IPv6 구성의 경우 Unified Manager 설치가 성공적으로 수행되도록 호스트 이름에 대한 ping6(ping6)이 성공했는지 확인해야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 제품 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트의 이름을 지정합니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 얻어야 합니다.

사용자가 FQDN(정규화된 도메인 이름) 또는 IP 주소를 사용하는 대신 짧은 이름을 사용하여 Unified Manager에 액세스할 수 있도록 하려는 경우 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 해석해야 합니다.

VMware 소프트웨어 및 설치 요구 사항

Unified Manager를 설치하는 VMware vSphere 시스템에는 특정 버전의 운영 체제와 지원 소프트웨어가 필요합니다.

운영 체제 소프트웨어

지원되는 VMware ESXi 버전은 다음과 같습니다.

- ESXi 7.0 및 8.0

VMware vSphere 시스템의 Unified Manager OVA는 내부적으로 Debian OS 11(bullseye)을 실행합니다. 지원되는 ESXi 서버 버전에서 지원할 수 있는 가상 머신 하드웨어 버전에 대한 자세한 내용은 VMware 설명서를 참조하십시오.

지원되는 vSphere 버전은 다음과 같습니다.

- VMware vCenter Server 7.0 및 8.0

지원되는 ESXi 버전의 전체 및 최신 목록은 상호 운용성 매트릭스 를 참조하십시오.

"mysupport.netapp.com/matrix"

VMware ESXi 서버 시간은 가상 어플라이언스가 올바르게 작동할 수 있도록 NTP 서버 시간과 동일해야 합니다. VMware ESXi 서버 시간을 NTP 서버 시간과 동기화하면 시간 오류가 방지됩니다.

설치 요구 사항

Unified Manager 가상 어플라이언스에 대한 VMware High Availability가 지원됩니다.

ONTAP 소프트웨어를 실행 중인 스토리지 시스템에 NFS 데이터 저장소를 구축하는 경우 NetApp NFS Plug-in for VMware VAAI를 사용하여 일반 프로비저닝을 사용합니다.

리소스 부족으로 High Availability 지원 환경을 사용하여 배포가 실패하는 경우 VM 다시 시작 우선 순위를 비활성화하고 호스트 격리 응답 전원을 켠 상태로 두어 클러스터 기능 가상 머신 옵션을 수정해야 할 수 있습니다.

Unified Manager를 설치 또는 업그레이드하는 동안 필요한 타사 소프트웨어 및 보안 패치가 VMware vSphere 시스템에 자동으로 설치 또는 업그레이드됩니다. Unified Manager 설치 및 업그레이드 프로세스에서 이러한 구성요소를 제어하므로 타사 구성요소를 독립적으로 설치 또는 업그레이드하려고 하면 안 됩니다.

지원되는 브라우저

Unified Manager 웹 UI에 액세스하려면 지원되는 브라우저를 사용하십시오.

상호 운용성 매트릭스에는 지원되는 브라우저 버전 목록이 있습니다.

"mysupport.netapp.com/matrix"

모든 브라우저의 경우 팝업 차단기를 비활성화하면 소프트웨어 기능이 제대로 표시됩니다.

IdP(ID 공급자)가 사용자를 인증할 수 있도록 SAML 인증을 위해 Unified Manager를 구성하려면 IDP에서 지원하는 브라우저 목록도 확인해야 합니다.

프로토콜 및 포트 요구 사항

필요한 포트와 프로토콜을 사용하면 Unified Manager 서버와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간에 통신할 수 있습니다.

Unified Manager 서버에 대한 연결

일반적으로 기본 포트는 항상 사용되므로 Unified Manager 웹 UI에 연결할 때 포트 번호를 지정할 필요가 없습니다. 예를 들어, Unified Manager가 항상 기본 포트에서 실행하려고 하므로 "https://<host>:443` 대신 "https://<host>` 를 입력할 수 있습니다.

Unified Manager 서버는 특정 프로토콜을 사용하여 다음 인터페이스에 액세스합니다.

인터페이스	프로토콜	포트	설명
Unified Manager 웹 UI	HTTP	80	Unified Manager 웹 UI에 액세스하는 데 사용되며 보안 포트 443으로 자동으로 리디렉션됩니다.
API를 사용하는 Unified Manager 웹 UI 및 프로그램	HTTPS	443	Unified Manager 웹 UI에 안전하게 액세스하거나 API 호출을 하는 데 사용되며 HTTPS를 통해서만 API 호출을 수행할 수 있습니다.
유지보수 콘솔	SSH/SFTP	22	유지보수 콘솔에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
Linux 명령줄	SSH/SFTP	22	Red Hat Enterprise Linux 또는 CentOS 명령줄에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
Syslog를 클릭합니다	UDP입니다	514	ONTAP 시스템에서 서브스크립션 기반 EMS 메시지에 액세스하고 메시지를 기반으로 이벤트를 생성하는 데 사용됩니다.
휴식	HTTPS	9443	인증된 ONTAP 시스템에서 실시간 REST API 기반 EMS 이벤트에 액세스하는 데 사용됩니다.

MySQL의 기본 포트 3306은 VMware vSphere 시스템에 Unified Manager를 설치하는 동안 localhost로 제한됩니다. 이전 구성이 유지되는 업그레이드 시나리오에는 영향을 주지 않습니다. 이 구성은 수정할 수 있으며 을 사용하여 다른 호스트에서 연결을 사용할 수 있습니다 `Control access to MySQL port 3306` 옵션을 설정할 수 있습니다. 자세한 내용은 을 참조하십시오 "추가 메뉴 옵션". HTTP 및 HTTPS 통신에 사용되는 포트(포트 80 및 443)는 Unified Manager 유지 관리 콘솔을 사용하여 변경할 수 있습니다. 자세한 내용은 을 참조하십시오 "유지보수 콘솔 메뉴".

Unified Manager 서버와의 연결입니다

Unified Manager Server와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 활성화하는 포트를 열도록 방화벽을 구성해야 합니다. 포트가 열려 있지 않으면 통신이 실패합니다.

환경에 따라 Unified Manager 서버가 특정 대상에 연결하는 데 사용하는 포트와 프로토콜을 수정할 수 있습니다.

Unified Manager 서버는 다음 프로토콜과 포트를 사용하여 관리형 스토리지 시스템, 서버 및 기타 구성 요소에 연결합니다.

목적지	프로토콜	포트	설명
수행할 수 있습니다	HTTPS	443/TCP	스토리지 시스템을 모니터링 및 관리하는 데 사용됩니다. 이 포트 또는 다른 포트를 사용하여 VMware vCenter Server 또는 ESXi Server에 연결하는 경우 해당 포트를 사용할 수 있고 보안 사이트에 연결할 수 있는지 확인합니다.
수행할 수 있습니다	NDMP	10000/TCP	특정 스냅샷 복원 작업에 사용됩니다.
AutoSupport 서버	HTTPS	443	AutoSupport 정보를 전송하는 데 사용됩니다. 이 기능을 수행하려면 인터넷 액세스가 필요합니다.

목적지	프로토콜	포트	설명
인증 서버	LDAP를 지원합니다	389	인증 요청, 사용자 및 그룹 조회 요청을 하는 데 사용됩니다.
LDAPS	636	보안 LDAP 통신에 사용됩니다.	메일 서버
SMTP	25	경고 알림 이메일을 보내는 데 사용됩니다.	SNMP 트랩 보낸 사람
SNMPv1 또는 SNMPv3	162/UDP	알림 SNMP 트랩을 보내는 데 사용됩니다.	외부 데이터 공급자 서버
TCP	2003년	Graphite와 같은 외부 데이터 공급자에게 성능 데이터를 보내는 데 사용됩니다.	NTP 서버

워크시트를 작성합니다

Unified Manager를 설치 및 구성하기 전에 환경에 대한 정보를 즉시 확인할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

Unified Manager를 설치하는 데 필요한 세부 정보

소프트웨어가 배포되는 시스템입니다	귀사의 가치
ESXi 서버 IP 주소입니다	
호스트 정규화된 도메인 이름입니다	
호스트 IP 주소입니다	
네트워크 마스크	
게이트웨이 IP 주소입니다	
기본 DNS 주소입니다	
보조 DNS 주소입니다	

소프트웨어가 배포되는 시스템입니다	귀사의 가치
도메인 검색	
유지보수 사용자 이름입니다	
유지보수 사용자 암호입니다	

Unified Manager 구성 정보

설치 후 Unified Manager를 구성하기 위한 세부 정보 일부 값은 구성에 따라 선택 사항입니다.

설정	귀사의 가치
유지보수 사용자 이메일 주소	
NTP 서버	
SMTP 서버 호스트 이름 또는 IP 주소입니다	
SMTP 사용자 이름입니다	
SMTP 암호	
SMTP 포트	25(기본값)
알림 알림이 전송되는 이메일입니다	
인증 서버 호스트 이름 또는 IP 주소입니다	
Active Directory 관리자 이름 또는 LDAP 바인드 고유 이름입니다	
Active Directory 암호 또는 LDAP 바인딩 암호입니다	
인증 서버 기본 고유 이름입니다	
ID 공급자(IDP) URL입니다	
IdP(Identity Provider) 메타데이터	
SNMP 트랩 대상 호스트 IP 주소입니다	
SNMP 포트	

클러스터 정보

Unified Manager를 사용하여 관리하는 스토리지 시스템의 세부 정보입니다.

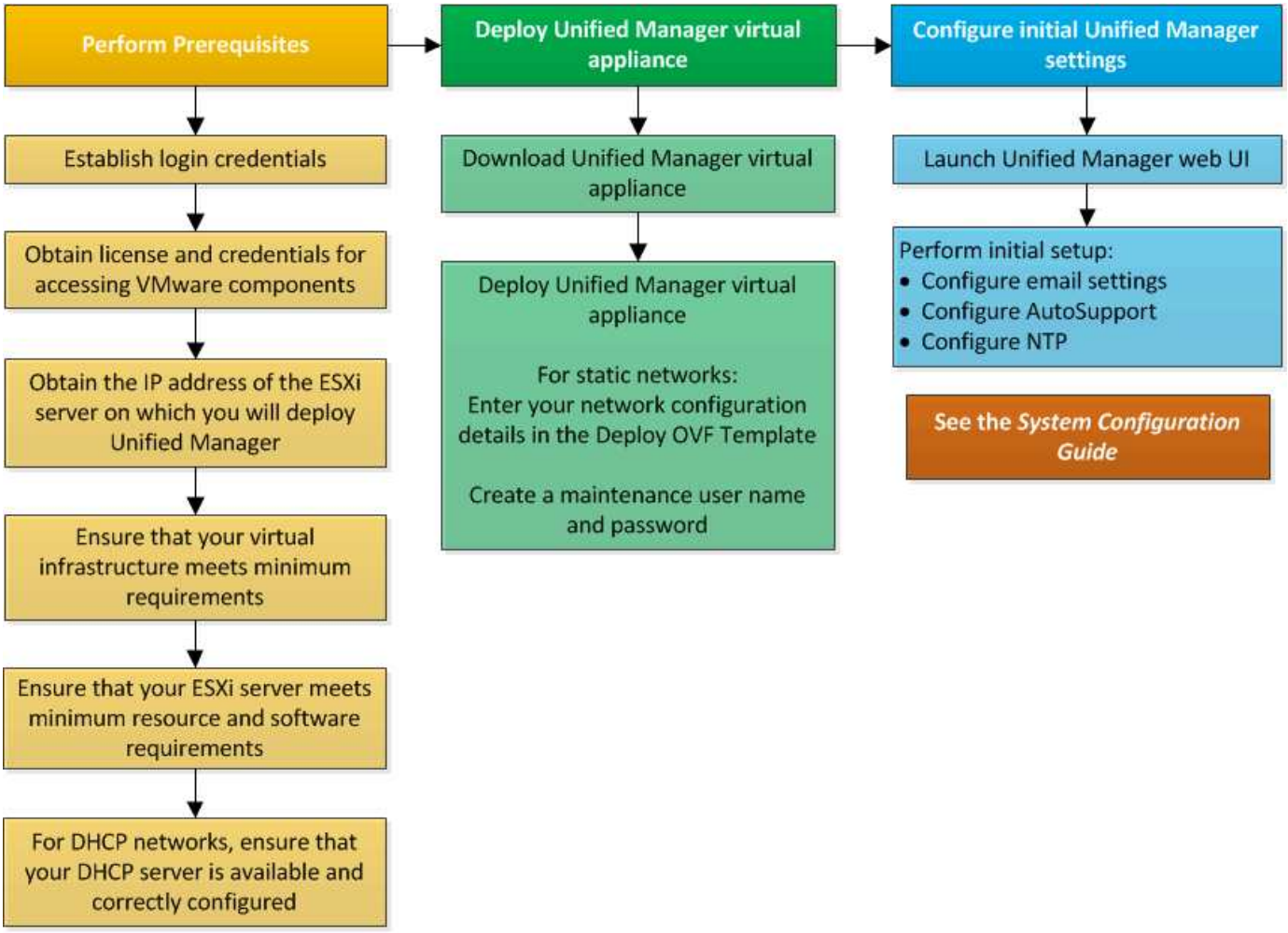
클러스터 **1/N**	귀사의 가치
호스트 이름 또는 클러스터 관리 IP 주소입니다	
ONTAP 관리자 사용자 이름입니다 관리자가 "admin" 역할을 할당받아야 합니다.	
ONTAP 관리자 암호입니다	
프로토콜	HTTPS

Unified Manager 소프트웨어의 설치, 업그레이드 및 제거

VMware vSphere 시스템에서는 Unified Manager를 설치하거나, 최신 버전의 소프트웨어로 업그레이드하거나, vApp(Unified Manager 가상 어플라이언스)을 제거할 수 있습니다.

배포 프로세스 개요

구축 워크플로우에서는 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.



Unified Manager 구축

Unified Manager를 구축하려면 소프트웨어 다운로드, 가상 어플라이언스 구축, 유지보수 사용자 이름 및 암호 생성, 웹 UI에서 초기 설정 작업이 포함됩니다.

- 필요한 것 *
- 구축을 위한 시스템 요구 사항을 확인하고 완료해야 합니다.

  을 참조하십시오 "시스템 요구 사항".

- 다음 정보가 있는지 확인하십시오.
  - NetApp Support 사이트의 로그인 자격 증명
  - VMware vCenter Server 및 vSphere Web Client에 액세스하기 위한 자격 증명
  - Unified Manager 가상 어플라이언스를 구축하고 있는 ESXi 서버의 IP 주소입니다
  - 데이터 저장소의 스토리지 공간 및 메모리 요구 사항과 같은 데이터 센터에 대한 세부 정보입니다
  - IPv6 주소 지정을 사용할 계획이라면 호스트에서 IPv6를 활성화해야 합니다.

Unified Manager를 VMware ESXi 서버에 가상 어플라이언스로 구축할 수 있습니다.

SSH를 사용하지 않고 VMware 콘솔을 사용하여 유지보수 콘솔에 액세스해야 합니다.

Unified Manager 9.8부터 VMware Tools는 Open VM Tools("오픈 VM 도구")로 대체되었습니다. Unified Manager 설치 패키지에 개방형 VM-Tools가 포함되어 있으므로 설치 시 VMware Tools를 더 이상 설치할 필요가 없습니다.

배포 및 초기 설정을 완료한 후 클러스터를 추가하거나 유지 관리 콘솔에서 추가 네트워크 설정을 구성한 다음 웹 UI에 액세스할 수 있습니다.

단계

1. 의 단계를 따릅니다 "Unified Manager 다운로드".
2. 또한 의 단계를 따릅니다 "Unified Manager 가상 어플라이언스를 구축합니다".

Unified Manager 설치 파일을 다운로드하는 중입니다

NetApp Support 사이트에서 Unified Manager 설치 파일을 다운로드하여 Unified Manager를 가상 어플라이언스로 구축할 수 있습니다.

- 필요한 것 *

NetApp Support 사이트에 대한 로그인 자격 증명이 있어야 합니다.

설치 파일은 입니다 `.tar` 루트 인증서가 포함된 파일, a `README` 파일, 및 `OVA` 가상 어플라이언스에 대해 구성된 Unified Manager 소프트웨어가 포함된 파일입니다.

단계

1. NetApp Support 사이트에 로그인하고 Unified Manager의 다운로드 페이지로 이동합니다.

   "NetApp Support 사이트"

2. Unified Manager의 필수 버전을 선택하고 최종 사용자 라이센스 계약(EULA)에 동의합니다.
3. 를 다운로드하고 저장합니다 `.tar` vSphere Client에서 액세스할 수 있는 로컬 디렉토리 또는 네트워크 디렉토리에 VMware vSphere 설치를 위한 파일입니다.
4. 체크섬을 확인하여 소프트웨어가 올바르게 다운로드되었는지 확인합니다.
5. 를 다운로드한 디렉토리로 이동합니다 `.tar` 를 입력하고 터미널 창에 다음 명령을 입력하여 Unified Manager 번들을 확장합니다.

   ```
   tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
   ```

   필수 요소입니다 `OVA` 파일, 루트 인증서 및 입니다 `README` Unified Manager용 파일의 압축이 대상 디렉토리에 풀립니다.

6. 의 무결성을 확인합니다 `OVA` 에 나와 있는 단계에 따라 파일을 엽니다 `README` 파일.

Unified Manager 가상 어플라이언스 구축

설치 파일을 다운로드한 후에는 Unified Manager를 가상 어플라이언스로 구축할 수 있습니다. vSphere Web Client를 사용하여 ESXi 서버에 가상 어플라이언스를 구축합니다. 가상

어플라이언스를 구축하면 가상 머신이 생성됩니다.

- 필요한 것 *

시스템 요구 사항을 검토해야 합니다. Unified Manager 가상 어플라이언스를 구축하기 전에 필요에 따라 변경하십시오.

을 참조하십시오 "가상 인프라 요구 사항".

을 참조하십시오 "VMware 소프트웨어 및 설치 요구 사항".

DHCP(Dynamic Host Configuration Protocol)를 사용하는 경우 DHCP 서버를 사용할 수 있고 DHCP 및 가상 머신(VM) 네트워크 어댑터 구성이 올바른지 확인합니다. DHCP는 기본적으로 구성됩니다.

정적 네트워킹 구성을 사용하는 경우 IP 주소가 동일한 서브넷에 복제되지 않고 적절한 DNS 서버 항목이 구성되었는지 확인합니다.

가상 어플라이언스를 구축하기 전에 다음 정보를 확인하십시오.

- VMware vCenter Server 및 vSphere Web Client에 액세스하기 위한 자격 증명
- Unified Manager 가상 어플라이언스를 구축하고 있는 ESXi 서버의 IP 주소입니다
- 스토리지 공간의 가용성과 같은 데이터 센터에 대한 세부 정보
- DHCP를 사용하지 않는 경우 연결하려는 네트워킹 장치의 IPv4 또는 IPv6 주소를 확인합니다.
  - 호스트의 FQDN(정규화된 도메인 이름)입니다
  - 호스트의 IP 주소입니다
  - 네트워크 마스크
  - 기본 게이트웨이의 IP 주소입니다
  - 기본 및 보조 DNS 주소
  - 도메인 검색

Unified Manager 9.8부터 VMware Tools는 Open VM Tools("*open-vm-tools*")로 대체되었습니다. Unified Manager 설치 패키지에 '*open-vm-tools*'이 포함되어 있으므로 설치 프로세스의 일부로 VMware Tools를 설치할 필요가 없습니다.

가상 어플라이언스가 배포되면 HTTPS 액세스를 위한 고유한 자체 서명 인증서가 생성됩니다. Unified Manager 웹 UI에 액세스할 때 신뢰할 수 없는 인증서에 대한 브라우저 경고가 표시될 수 있습니다.

Unified Manager 가상 어플라이언스에 대한 VMware High Availability가 지원됩니다.

단계

1. vSphere Client에서 * File * > * Deploy OVF Template * 을 클릭합니다.
2. Deploy OVF Template 마법사를 완료하여 Unified Manager 가상 어플라이언스를 구축합니다.

   검토 세부 정보 페이지에서 다음을 수행합니다.

   - Publisher 섹션의 세부 정보를 확인합니다. Entrust Code Signing - OVCS2(신뢰할 수 있는 인증서) * 메시지는 다운로드한 의 무결성을 확인합니다 `OVA` 파일. + * Entrust Code Signing - OVCS2 (Invalid certificate) * 메시지가 표시되면 VMware vCenter Server를 7.0U3E 이상 버전으로 업그레이드합니다.

템플릿 사용자 지정 페이지에서 다음을 수행합니다.

- DHCP 및 IPv4 주소 지정을 사용하는 경우 모든 필드를 비워 둡니다.
- DHCP 및 IPv6 주소 지정을 사용할 때 ""자동 IPv6 주소 지정 활성화"" 확인란을 선택하고 다른 모든 필드는 비워 둡니다.
- 정적 네트워크 구성을 사용하려면 이 페이지의 필드를 완성하면 배포 중에 이러한 설정이 적용됩니다. IP 주소가 배포된 호스트에 고유하고, 이미 사용 중이 아니며, 유효한 DNS 항목이 있는지 확인합니다.

3. Unified Manager 가상 어플라이언스를 ESXi 서버에 구축한 후 VM을 마우스 오른쪽 버튼으로 클릭하고 * Power On * 을 선택하여 VM의 전원을 켭니다.

   리소스 부족으로 전원 켜기 작업이 실패하면 리소스를 추가한 다음 설치를 다시 시도하십시오.

4. Console * 탭을 클릭합니다.

   초기 부팅 프로세스를 완료하는 데 몇 분 정도 걸립니다.

5. 시간대를 구성하려면 VM 콘솔 창에 표시된 대로 지리적 지역 및 도시 또는 지역을 입력합니다.

   표시되는 모든 날짜 정보는 관리되는 장치의 표준 시간대 설정에 관계없이 Unified Manager에 대해 구성된 표준 시간대를 사용합니다. 스토리지 시스템과 관리 서버가 동일한 NTP 서버로 구성되어 있는 경우 다르게 나타나더라도 동일한 인스턴트 서버를 나타냅니다. 예를 들어, 관리 서버의 표준 시간대가 아닌 다른 시간대를 사용하여 구성된 장치를 사용하여 스냅샷 복사본을 생성하는 경우 관리 서버 시간이 타임스탬프입니다.

6. DHCP 서비스를 사용할 수 없거나 정적 네트워크 구성에 대한 세부 정보에 오류가 있는 경우 다음 옵션 중 하나를 선택합니다.

사용하는 경우...	다음을 수행하십시오.
DHCP를 선택합니다	DHCP 재시도 * 를 선택합니다. DHCP를 사용할 계획이라면 DHCP가 올바르게 구성되어 있는지 확인해야 합니다. DHCP 지원 네트워크를 사용하는 경우 FQDN 및 DNS 서버 항목이 가상 어플라이언스에 자동으로 제공됩니다. DHCP가 DNS로 제대로 구성되어 있지 않으면 호스트 이름 ""UnifiedManager""가 자동으로 할당되어 보안 인증서와 연결됩니다. DHCP 지원 네트워크를 설정하지 않은 경우 네트워킹 구성 정보를 수동으로 입력해야 합니다.
정적 네트워크 구성	a. 정적 네트워크 구성에 대한 세부 정보를 입력하십시오 * 를 선택합니다. 구성 프로세스를 완료하는 데 몇 분 정도 소요됩니다. b. 입력한 값을 확인하고 * Y * 를 선택합니다.

7. 프롬프트에서 유지보수 사용자 이름을 입력한 다음 * Enter * 를 클릭합니다.

유지보수 사용자 이름은 a-z의 문자로 시작하고 그 뒤에 -, a-z 또는 0-9의 조합을 입력해야 합니다.

8. 프롬프트에서 암호를 입력한 다음 * Enter * 를 클릭합니다.

   VM 콘솔에는 Unified Manager 웹 UI의 URL이 표시됩니다.

웹 UI에 액세스하여 에 설명된 대로 Unified Manager의 초기 설정을 수행할 수 있습니다 "Active IQ Unified Manager 구성".

Unified Manager 업그레이드

릴리스 9.12 또는 9.13에서만 Active IQ Unified Manager를 릴리스 9.14로 업그레이드할 수 있습니다.

업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없습니다. Unified Manager를 업그레이드하기 전에 실행 중인 작업을 완료해야 합니다.

Unified Manager가 OnCommand Workflow Automation 인스턴스와 페어링되어 있고 두 제품 모두에 사용할 수 있는 새로운 소프트웨어 버전이 있는 경우 두 제품의 연결을 끊고 업그레이드를 수행한 후 새 Workflow Automation 연결을 설정해야 합니다. 제품 중 하나로 업그레이드하는 경우, 업그레이드 후에 Workflow Automation에 로그인하여 Unified Manager에서 데이터를 아직 취득하고 있는지 확인해야 합니다.

단계

1. 의 단계를 따릅니다 "Unified Manager ISO 이미지를 다운로드합니다".
2. 또한 에 설명된 단계를 따릅니다 "Unified Manager 업그레이드".

Unified Manager 버전에 지원되는 업그레이드 경로

Active IQ Unified Manager는 각 버전에 대한 특정 업그레이드 경로를 지원합니다.

모든 버전의 Unified Manager에서 이후 버전으로 업그레이드할 수 있는 것은 아닙니다. Unified Manager 업그레이드는 N-2 모델로 제한되어 있으며, 이는 모든 플랫폼의 다음 2개 릴리즈 내에서만 업그레이드할 수 있음을 의미합니다. 예를 들어, Unified Manager 9.12와 9.13에서만 Unified Manager 9.14로 업그레이드할 수 있습니다.

지원되는 버전보다 이전 버전을 실행 중인 경우 Unified Manager 인스턴스를 지원되는 버전 중 하나로 먼저 업그레이드한 다음 현재 버전으로 업그레이드해야 합니다.

예를 들어, 설치된 버전이 Unified Manager 9.9이고 Unified Manager 9.14로 업그레이드하려면 일련의 업그레이드를 수행해야 합니다.

샘플 업그레이드 경로**:**

1. 업그레이드 9.9 → 9.11
2. 업그레이드 9.11 → 9.13
3. 업그레이드 9.13 → 9.14

업그레이드 경로 매트릭스에 대한 자세한 내용은 다음을 참조하십시오 "기술 자료(KB) 문서".

Unified Manager 업그레이드 파일을 다운로드하는 중입니다

Unified Manager를 업그레이드하기 전에 NetApp Support 사이트에서 Unified Manager 업그레이드 파일을 다운로드하십시오.

- 필요한 것 *

NetApp Support 사이트에 대한 로그인 자격 증명이 있어야 합니다.

단계

1. NetApp Support 사이트 에 로그인합니다.

   "NetApp Support 사이트"

2. VMware vSphere에서 Unified Manager를 업그레이드하기 위한 다운로드 페이지로 이동합니다.
3. 업그레이드를 위해 '.iso' 이미지를 다운로드하여 vSphere Client에서 액세스할 수 있는 로컬 디렉토리 또는 네트워크 디렉토리에 저장합니다.
4. 체크섬을 확인하여 소프트웨어가 올바르게 다운로드되었는지 확인합니다.

Unified Manager 가상 어플라이언스 업그레이드

Active IQ Unified Manager 가상 어플라이언스는 9.12 또는 9.13에서 9.14로 업그레이드할 수 있습니다.

- 필요한 것 *

다음을 확인합니다.

- 업그레이드 파일인 ISO 이미지를 NetApp Support 사이트에서 다운로드했습니다.
- Unified Manager를 업그레이드하는 시스템은 시스템 및 소프트웨어 요구사항을 충족합니다.

  을 참조하십시오 "가상 인프라 요구 사항".

  을 참조하십시오 "VMware 소프트웨어 및 설치 요구 사항".

- vSphere 6.5 이상 사용자의 경우 VMware Remote Console(VMRC)을 설치했습니다.
- 업그레이드하는 동안 성능 데이터를 13개월 동안 유지하기 위한 이전 기본 설정을 유지할지 아니면 6개월로 변경할지 묻는 메시지가 표시될 수 있습니다. 확인 시, 기록 성능 데이터는 6개월 후에 삭제됩니다.
- 다음 정보가 있습니다.
  - NetApp Support 사이트의 로그인 자격 증명
  - VMware vCenter Server 및 vSphere Web Client에 액세스하기 위한 자격 증명
  - Unified Manager 유지보수 사용자의 자격 증명

업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없습니다. Unified Manager를 업그레이드하기 전에 실행 중인 작업을 완료해야 합니다.

Workflow Automation과 Unified Manager가 페어링된 경우 Workflow Automation에서 호스트 이름을 수동으로

업데이트해야 합니다.

단계

1. vSphere Client에서 * Home * > * Inventory * > * VMs and Templates * 를 클릭합니다.
2. Unified Manager 가상 어플라이언스가 설치된 가상 머신(VM)을 선택합니다.
3. Unified Manager VM이 실행 중인 경우 * 요약 * > * 명령 * > * 게스트 종료 * 로 이동합니다.
4. 애플리케이션 정합성 보장 백업을 생성하기 위해 Unified Manager VM의 스냅샷 또는 클론 같은 백업 복사본을 생성합니다.
5. vSphere Client에서 Unified Manager VM의 전원을 켭니다.
6. VMware Remote Console을 시작합니다.
7. CDROM * 아이콘을 클릭하고 * 디스크 이미지 파일에 연결 (.iso) * 을 선택합니다.
8. 'ActiveIQUnifiedManager-<version>-virtual-update.iso' 파일을 선택하고 * Open * 을 클릭합니다.
9. Console * 탭을 클릭합니다.
10. Unified Manager 유지보수 콘솔에 로그인합니다.
11. 주 메뉴에서 * 업그레이드 * 를 선택합니다.

    업그레이드 프로세스 중에 Unified Manager를 사용할 수 없으며 작업이 완료된 후 다시 시작된다는 메시지가 표시됩니다.

12. 계속하려면 y를 입력하십시오.

    가상 어플라이언스가 상주하는 가상 머신을 백업하도록 알리는 경고가 표시됩니다.

13. 계속하려면 y를 입력하십시오.

    업그레이드 프로세스와 Unified Manager 서비스를 다시 시작하는 데 몇 분 정도 걸릴 수 있습니다.

14. 계속하려면 아무 키나 누르십시오.

    유지보수 콘솔에서 자동으로 로그아웃됩니다.

15. * 선택 사항: * 유지보수 콘솔에 로그인하여 Unified Manager 버전을 확인합니다.

지원되는 웹 브라우저의 새 창에서 웹 UI를 시작하고 로그인하여 Unified Manager의 업그레이드된 버전을 사용할 수 있습니다. UI에서 작업을 수행하기 전에 검색 프로세스가 완료될 때까지 기다려야 합니다.

Unified Manager 가상 머신을 재시작합니다

유지보수 콘솔에서 Unified Manager 가상 머신(VM)을 다시 시작할 수 있습니다. 새 보안 인증서를 생성한 후 또는 VM에 문제가 있는 경우 VM을 다시 시작해야 합니다.

- 필요한 것 *
- 가상 어플라이언스의 전원이 켜져 있어야 합니다.
- 유지보수 사용자로 Unified Manager 유지보수 콘솔에 로그인해야 합니다.

VMware * Restart Guest * 옵션을 사용하여 vSphere에서 가상 머신을 재시작할 수도 있습니다.

단계

1. 유지보수 콘솔에서 * 시스템 구성 * > * 가상 시스템 재부팅 * 을 선택합니다.
2. 브라우저에서 Unified Manager 웹 UI를 시작하고 로그인합니다.
    ◦ 관련 정보 *

"VMware vSphere PowerCLI cmdlet 참조: 재시작 - VMGuest"

Unified Manager를 제거하는 중입니다

Unified Manager 소프트웨어가 설치된 가상 머신(VM)을 제거하여 Unified Manager를 제거할 수 있습니다.

- 필요한 것 *
- VMware vCenter Server 및 vSphere Web Client에 액세스하기 위한 자격 증명이 있어야 합니다.
- Unified Manager 서버와 Workflow Automation 서버의 활성 연결은 모두 종료되어야 합니다.
- 가상 머신(VM)을 제거하기 전에 모든 클러스터(데이터 소스)를 Unified Manager 서버에서 제거해야 합니다.

단계

1. Unified Manager 유지보수 콘솔을 사용하여 Unified Manager 서버가 외부 데이터 공급자에 대해 활성 상태로 연결되어 있지 않은지 확인합니다.
2. vSphere Client에서 * Home * > * Inventory * > * VMs and Templates * 를 클릭합니다.
3. 제거할 VM을 선택하고 * 요약 * 탭을 클릭합니다.
4. VM이 실행 중인 경우 * 전원 * > * 게스트 종료 * 를 클릭합니다.
5. 제거할 VM을 마우스 오른쪽 단추로 클릭하고 * 디스크에서 삭제 * 를 클릭합니다.

Linux 시스템에 Unified Manager를 설치합니다

Active IQ Unified Manager 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태 및 성능을 모니터링 및 관리할 수 있습니다. Unified Manager를 Linux 서버, Windows 서버 또는 VMware 호스트의 vApp(가상 어플라이언스)에 구축할 수 있습니다.

설치를 완료하고 관리할 클러스터를 추가한 후에는 Unified Manager에서 모니터링되는 스토리지 시스템의 용량, 가용성, 보호 및 성능 상태를 표시하는 그래픽 인터페이스를 제공합니다.

- 관련 정보 *

"NetApp 상호 운용성 매트릭스 툴"

Unified Manager 서버의 기능

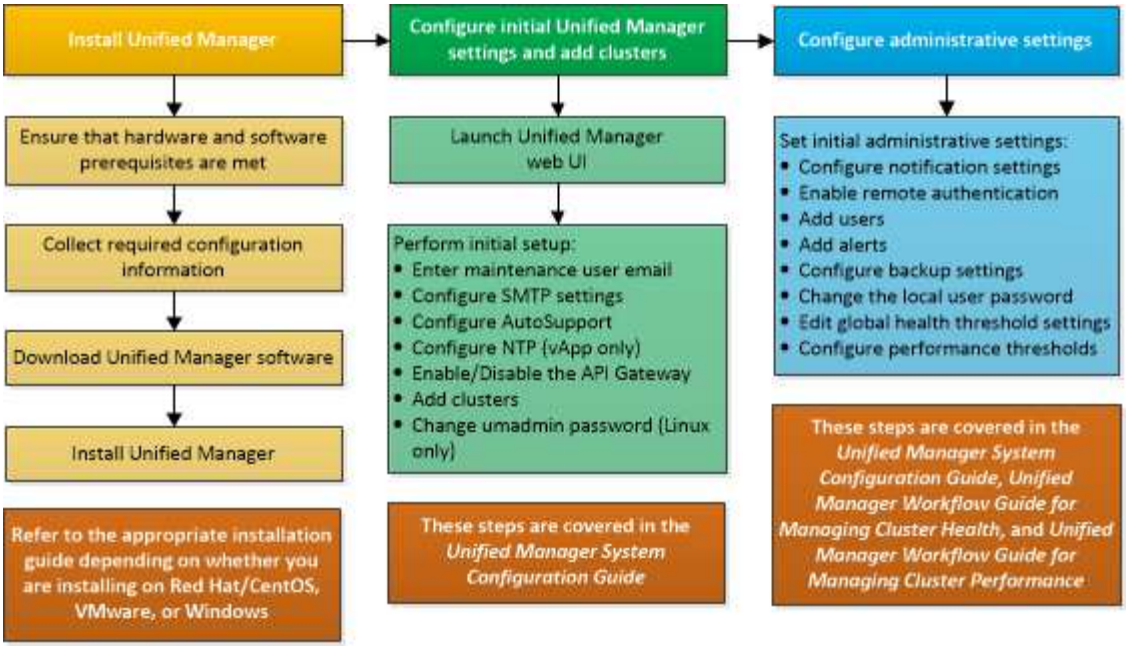
Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스 및 애플리케이션 서버로 구성됩니다. 검색, 모니터링, RBAC(역할 기반 액세스 제어), 감사, 로깅 등의 인프라 서비스를 제공합니다.

Unified Manager는 클러스터 정보를 수집하고, 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터 문제가 있는지 확인합니다.

설치 순서 개요

설치 워크플로우에서 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.

이 섹션에서는 아래 워크플로에 표시된 각 항목에 대해 설명합니다.



Unified Manager 설치 요구 사항

설치 프로세스를 시작하기 전에 Unified Manager를 설치할 서버가 특정 소프트웨어, 하드웨어, CPU 및 메모리 요구 사항을 충족하는지 확인하십시오.

NetApp은 Unified Manager 애플리케이션 코드의 수정을 지원하지 않습니다. Unified Manager 서버에 보안 조치를 적용해야 하는 경우 Unified Manager가 설치된 운영 체제를 변경해야 합니다.

Unified Manager 서버에 보안 조치를 적용하는 방법에 대한 자세한 내용은 기술 자료 문서를 참조하십시오.

"Clustered Data ONTAP을 위해 Active IQ Unified Manager에 적용된 보안 조치에 대한 지원 가능성"

- 관련 정보 *

"NetApp 상호 운용성 매트릭스 툴"

가상 인프라 및 하드웨어 시스템 요구 사항

가상 인프라 또는 물리적 시스템에 Unified Manager를 설치하려면 메모리, CPU 및 디스크 공간에 대한 최소 요구사항을 충족해야 합니다.

다음 표에는 메모리, CPU 및 디스크 공간 리소스에 권장되는 값이 나와 있습니다. 이러한 값은 Unified Manager가 허용 가능한 성능 수준을 충족할 수 있도록 검증을 받았습니다.

하드웨어 구성	권장 설정
RAM	12GB(최소 요구 사항 8GB)
프로세서	CPU 4개

하드웨어 구성	권장 설정
CPU 사이클 용량입니다	총 9572MHz(최소 요구 사항 9572MHz)
사용 가능한 디스크 공간	150GB로, 다음과 같이 용량이 할당됩니다. • 루트 파티션에 50GB가 할당됩니다 • LVM 드라이브 또는 타겟 시스템에 연결된 별도의 로컬 디스크에 마운트된 '/opt/netapp/data' 디렉토리에 할당된 사용 가능한 디스크 공간 100GB입니다 별도로 마운트된 '/opt' 및 '/var/log' 디렉토리의 경우, '/opt'에 15GB가 있고 '/var/log'에 16GB의 여유 공간이 있는지 확인하십시오. '/tmp' 디렉토리에 최소 10GB의 여유 공간이 있어야 합니다.

적은 용량의 메모리가 있는 시스템에 Unified Manager를 설치할 수 있지만 권장되는 12GB RAM을 사용하면 최적의 성능을 위해 충분한 메모리를 사용할 수 있으며, 따라서 시스템이 구성 증가에 따라 추가 클러스터 및 스토리지 오브젝트를 수용할 수 있습니다. Unified Manager가 구축된 VM에서 메모리 제한을 설정하지 말아야 하며, 시스템에서 할당된 메모리를 소프트웨어가 활용하지 못하는 기능(예: 풍선 벌루닝)을 사용하면 안 됩니다.

또한 Unified Manager의 두 번째 인스턴스를 설치하기 전에 Unified Manager의 단일 인스턴스에서 모니터링할 수 있는 노드 수에 제한이 있습니다. 자세한 내용은 _모범 사례 가이드_를 참조하십시오.

"기술 보고서 4621: Unified Manager 모범 사례 가이드"

메모리 페이지 스와핑은 시스템 및 관리 응용 프로그램의 성능에 부정적인 영향을 줍니다. 전체 호스트 활용률로 인해 CPU 리소스를 사용하지 않는 경우 성능이 저하될 수 있습니다.

전용 요구사항

Unified Manager를 설치하는 물리적 또는 가상 시스템은 Unified Manager에만 사용해야 하며 다른 애플리케이션과 공유해서는 안 됩니다. 다른 애플리케이션은 시스템 리소스를 소모하며 Unified Manager의 성능을 크게 줄일 수 있습니다.

백업에 필요한 공간 요구 사항

Unified Manager 백업 및 복원 기능을 사용하려면 "데이터" 디렉토리나 디스크에 150GB의 공간이 있도록 추가 용량을 할당합니다. 백업은 로컬 대상 또는 원격 대상에 쓸 수 있습니다. 모범 사례는 최소 150GB의 공간이 있는 Unified Manager 호스트 시스템 외부의 원격 위치를 식별하는 것입니다.

호스트 접속 구성 요구 사항

Unified Manager를 설치하는 물리적 시스템 또는 가상 시스템은 호스트 자체에서 호스트 이름을 성공적으로 "핑"할 수 있도록 구성해야 합니다. IPv6 구성의 경우 Unified Manager 설치가 성공적으로 수행되도록 호스트 이름에 대한 ping6(ping6)이 성공했는지 확인해야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 제품 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP

주소를 구성한 경우 네트워크 호스트의 이름을 지정합니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 얻어야 합니다.

사용자가 FQDN(정규화된 도메인 이름) 또는 IP 주소를 사용하는 대신 짧은 이름을 사용하여 Unified Manager에 액세스할 수 있도록 하려는 경우 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 해석해야 합니다.

Linux 소프트웨어 및 설치 요구 사항

Unified Manager를 설치하는 Linux 시스템에는 특정 버전의 운영 체제 및 지원 소프트웨어가 필요합니다.

운영 체제 소프트웨어

Linux 시스템에는 다음 버전의 운영 체제와 지원 소프트웨어가 설치되어 있어야 합니다.

- x86_64 아키텍처 기반 Red Hat Enterprise Linux 버전 7.x 및 8.8에서 8.8까지.
- x86_64 아키텍처 기반 CentOS 버전 7.x CentOS 스트림은 지원되지 않습니다.

지원되는 Red Hat Enterprise Linux 및 CentOS 버전의 전체 최신 목록은 상호 운용성 매트릭스를 참조하십시오.

"mysupport.netapp.com/matrix"

서버는 Unified Manager 실행 전용으로 사용되어야 합니다. 서버에 다른 응용 프로그램을 설치할 수 없습니다. 회사 규정으로 인해 Qualys와 같은 취약점 검사가 Linux 시스템에 설치될 수 있습니다. 설치가 실패하지 않도록 Unified Manager를 설치하기 전에 취약점 검사기를 비활성화해야 합니다.

타사 소프트웨어

Unified Manager는 WildFly 웹 서버에 구축되어 있습니다. WildFly 26.1.3은 Unified Manager와 함께 번들로 제공되며 구성됩니다.

다음 타사 패키지는 필수이지만 Unified Manager에 포함되어 있지 않습니다. 이러한 패키지는 다음 섹션에서 설명한 대로 리포지토리를 구성한 경우 설치 중에 'yum' 설치 관리자에 의해 자동으로 설치됩니다.

- MySQL Community Edition 버전 8.0.34(MySQL 리포지토리에서).
- OpenJDK 버전 11.0.21(Red Hat Extra Enterprise Linux Server 리포지토리에서 제공)
- Python 3.6.x
- p7zip 버전 16.02 이상(Enterprise Linux용 Red Hat Extra Packages 리포지토리)

타사 소프트웨어를 업그레이드하기 전에 Unified Manager를 실행 중인 인스턴스를 종료해야 합니다. 타사 소프트웨어 설치가 완료되면 Unified Manager를 다시 시작할 수 있습니다.

사용자 인증 요구 사항

Linux 시스템에 Unified Manager를 설치하는 작업은 루트 사용자 또는 비루트 사용자가 'sudo' 명령을 사용하여 수행할 수 있습니다.

설치 요구 사항

Red Hat Enterprise Linux 또는 CentOS를 설치하는 모범 사례와 시스템에 연결된 리포지토리를 설치하는 방법은 다음과 같습니다. 다르게 설치 또는 구성되거나 오프 프레미스(클라우드)를 배포한 시스템은 추가 단계가 필요할 수 있으며, Unified Manager가 이러한 배포에서 제대로 실행되지 않을 수 있습니다.

- Red Hat 모범 사례에 따라 Red Hat Enterprise Linux 또는 CentOS를 설치해야 하며, "GUI 기반 서버" 기본 환경을 선택해야 하는 다음 기본 옵션을 선택해야 합니다.
- Red Hat Enterprise Linux 또는 CentOS에 Unified Manager를 설치하는 동안 설치 프로그램이 필요한 모든 소프트웨어 종속성을 액세스하고 설치할 수 있도록 해당 저장소에 대한 액세스 권한이 시스템에 있어야 합니다.
- 'yum' 설치 관리자가 Red Hat Enterprise Linux 리포지토리에서 종속 소프트웨어를 찾으려면 Red Hat Enterprise Linux 설치 중에 또는 유효한 Red Hat 서브스크립션을 사용하여 시스템을 등록해야 합니다.

  Red Hat 서브스크립션 관리자에 대한 자세한 내용은 Red Hat 설명서를 참조하십시오.

- 시스템에 필요한 타사 유틸리티를 설치하려면 EPEL(Enterprise Linux) 리포지토리용 추가 패키지를 활성화해야 합니다.

  EPEL 리포지토리가 시스템에 구성되어 있지 않은 경우 리포지토리를 수동으로 다운로드하고 구성해야 합니다.

  을 참조하십시오 "EPEL 리포지토리를 수동으로 구성합니다".

- 올바른 버전의 MySQL이 설치되어 있지 않은 경우 MySQL 리포지토리를 활성화하여 시스템에 MySQL 소프트웨어를 성공적으로 설치해야 합니다.

  MySQL 리포지토리가 시스템에 구성되어 있지 않은 경우 리포지토리를 수동으로 다운로드하고 구성해야 합니다.

  을 참조하십시오 "MySQL 리포지토리를 수동으로 구성합니다".

시스템에 인터넷 액세스가 없고 저장소가 인터넷에 연결된 시스템에서 연결되지 않은 시스템으로 미러링되지 않은 경우 설치 지침에 따라 시스템의 외부 소프트웨어 종속성을 결정해야 합니다. 그런 다음 필요한 소프트웨어를 인터넷에 연결된 시스템에 다운로드하고 Unified Manager를 설치할 시스템에 .rpm 파일을 복사할 수 있습니다. 아티팩트 및 패키지를 다운로드하려면 "yum install" 명령을 사용해야 합니다. 두 시스템이 동일한 운영 체제 버전을 실행하고 있고 해당 서브스크립션 라이센스가 적절한 Red Hat Enterprise Linux 또는 CentOS 버전인지 확인해야 합니다.

> ⓘ 여기에 나열된 리포지토리가 아닌 리포지토리에서 필요한 타사 소프트웨어를 설치해서는 안 됩니다. Red Hat 리포지토리에서 설치되는 소프트웨어는 Red Hat Enterprise Linux용으로 명시적으로 설계되었으며 Red Hat 모범 사례(디렉터리 레이아웃, 권한 등)를 준수합니다. 다른 지역의 소프트웨어는 이러한 지침을 따르지 않을 수 있으며, 이로 인해 Unified Manager 설치가 실패하거나 향후 업그레이드에 문제가 발생할 수 있습니다.

포트 **443** 요구 사항

Red Hat Enterprise Linux 및 CentOS의 일반 이미지는 포트 443에 대한 외부 액세스를 차단할 수 있습니다. 이러한 제한으로 인해 Unified Manager를 설치한 후 관리자 웹 UI에 연결할 수 없을 수 있습니다. 다음 명령을 실행하면 일반 Red Hat Enterprise Linux 또는 CentOS 시스템의 모든 외부 사용자 및 애플리케이션에 대한 포트 443에 액세스할 수 있습니다.

`#firewall-cmd—zone=public—add-port=443/tcp—permanent;firewall-cmd—reload'

"GUI가 있는 서버" 기본 환경에서 Red Hat Enterprise Linux 및 CentOS를 설치해야 합니다. Unified Manager 설치

지침에 사용되는 명령을 제공합니다. 다른 기본 환경에서는 설치를 검증 또는 완료하기 위해 추가 명령을 설치해야 할 수도 있습니다. 시스템에서 firewall-cmd를 사용할 수 없는 경우 다음 명령을 실행하여 설치해야 합니다.

'#sudo yum install firewalld'

명령을 실행하기 전에 IT 부서에 문의하여 보안 정책에 다른 절차가 필요한지 확인하십시오.

CentOS 및 Red Hat 시스템에서는 THP(Transparent 거대한 페이지)를 비활성화해야 합니다. 이 옵션을 사용하면 특정 프로세스에서 너무 많은 메모리를 사용하고 프로세스가 종료될 때 Unified Manager를 종료하는 경우가 있습니다.

지원되는 브라우저

Unified Manager 웹 UI에 액세스하려면 지원되는 브라우저를 사용하십시오.

상호 운용성 매트릭스에는 지원되는 브라우저 버전 목록이 있습니다.

"mysupport.netapp.com/matrix"

모든 브라우저의 경우 팝업 차단기를 비활성화하면 소프트웨어 기능이 제대로 표시됩니다.

IdP(ID 공급자)가 사용자를 인증할 수 있도록 SAML 인증을 위해 Unified Manager를 구성하려면 IDP에서 지원하는 브라우저 목록도 확인해야 합니다.

프로토콜 및 포트 요구 사항

필요한 포트와 프로토콜을 사용하면 Unified Manager 서버와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간에 통신할 수 있습니다.

Unified Manager 서버에 대한 연결

일반적으로 기본 포트는 항상 사용되므로 Unified Manager 웹 UI에 연결할 때 포트 번호를 지정할 필요가 없습니다. 예를 들어, Unified Manager가 항상 기본 포트에서 실행하려고 하므로 "https://<host>:443` 대신 "https://<host>` 를 입력할 수 있습니다.

Unified Manager 서버는 특정 프로토콜을 사용하여 다음 인터페이스에 액세스합니다.

인터페이스	프로토콜	포트	설명
Unified Manager 웹 UI	HTTP	80	Unified Manager 웹 UI에 액세스하는 데 사용되며 보안 포트 443으로 자동으로 리디렉션됩니다.
API를 사용하는 Unified Manager 웹 UI 및 프로그램	HTTPS	443	Unified Manager 웹 UI에 안전하게 액세스하거나 API 호출을 하는 데 사용되며 HTTPS를 통해서만 API 호출을 수행할 수 있습니다.

인터페이스	프로토콜	포트	설명
유지보수 콘솔	SSH/SFTP	22	유지보수 콘솔에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
Linux 명령줄	SSH/SFTP	22	Red Hat Enterprise Linux 또는 CentOS 명령줄에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
MySQL 데이터베이스	MySQL	3306	OnCommand 및 OnCommand Workflow Automation API Services에서 Unified Manager에 액세스할 수 있도록 설정하는 데 사용됩니다.
Syslog를 클릭합니다	UDP입니다	514	ONTAP 시스템에서 서브스크립션 기반 EMS 메시지에 액세스하고 메시지를 기반으로 이벤트를 생성하는 데 사용됩니다.
휴식	HTTPS	9443	인증된 ONTAP 시스템에서 실시간 REST API 기반 EMS 이벤트에 액세스하는 데 사용됩니다.

MySQL의 기본 포트 3306은 Linux 시스템에 Unified Manager를 설치하는 동안 localhost로 제한됩니다. 이전 구성이 유지되는 업그레이드 시나리오에는 영향을 주지 않습니다. 이 구성은 수정할 수 있으며 을 사용하여 다른 호스트에서 연결을 사용할 수 있습니다 `Control access to MySQL port 3306` 옵션을 설정할 수 있습니다. 자세한 내용은 을 참조하십시오 "추가 메뉴 옵션". HTTP 및 HTTPS 통신에 사용되는 포트(포트 80 및 443)는 Unified Manager 유지 관리 콘솔을 사용하여 변경할 수 있습니다. 자세한 내용은 을 참조하십시오 "유지보수 콘솔 메뉴".

Unified Manager 서버와의 연결입니다

Unified Manager Server와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 활성화하는 포트를 열도록 방화벽을 구성해야 합니다. 포트가 열려 있지 않으면 통신이 실패합니다.

환경에 따라 Unified Manager 서버가 특정 대상에 연결하는 데 사용하는 포트와 프로토콜을 수정할 수 있습니다.

Unified Manager 서버는 다음 프로토콜과 포트를 사용하여 관리형 스토리지 시스템, 서버 및 기타 구성 요소에 연결합니다.

목적지	프로토콜	포트	설명
수행할 수 있습니다	HTTPS	443/TCP	스토리지 시스템을 모니터링 및 관리하는 데 사용됩니다.
수행할 수 있습니다	NDMP	10000/TCP	특정 스냅샷 복원 작업에 사용됩니다.
AutoSupport 서버	HTTPS	443	AutoSupport 정보를 전송하는 데 사용됩니다. 이 기능을 수행하려면 인터넷 액세스가 필요합니다.
인증 서버	LDAP를 지원합니다	389	인증 요청, 사용자 및 그룹 조회 요청을 하는 데 사용됩니다.
LDAPS	636	보안 LDAP 통신에 사용됩니다.	메일 서버
SMTP	25	경고 알림 이메일을 보내는 데 사용됩니다.	SNMP 트랩 보낸 사람
SNMPv1 또는 SNMPv3	162/UDP	알림 SNMP 트랩을 보내는 데 사용됩니다.	외부 데이터 공급자 서버
TCP	2003년	Graphite와 같은 외부 데이터 공급자에게 성능 데이터를 보내는 데 사용됩니다.	NTP 서버

워크시트를 작성합니다

Unified Manager를 설치 및 구성하기 전에 환경에 대한 정보를 즉시 확인할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

Unified Manager를 설치하는 데 필요한 세부 정보

소프트웨어가 배포되는 시스템입니다	귀사의 가치
호스트 정규화된 도메인 이름입니다	
호스트 IP 주소입니다	

소프트웨어가 배포되는 시스템입니다	귀사의 가치
네트워크 마스크	
게이트웨이 IP 주소입니다	
기본 DNS 주소입니다	
보조 DNS 주소입니다	
도메인 검색	
유지보수 사용자 이름입니다	
유지보수 사용자 암호입니다	

Unified Manager 구성 정보

설치 후 Unified Manager를 구성하기 위한 세부 정보 일부 값은 구성에 따라 선택 사항입니다.

설정	귀사의 가치
유지보수 사용자 이메일 주소	
SMTP 서버 호스트 이름 또는 IP 주소입니다	
SMTP 사용자 이름입니다	
SMTP 암호	
SMTP 포트	25(기본값)
알림 알림이 전송되는 이메일입니다	
인증 서버 호스트 이름 또는 IP 주소입니다	
Active Directory 관리자 이름 또는 LDAP 바인드 고유 이름입니다	
Active Directory 암호 또는 LDAP 바인딩 암호입니다	
인증 서버 기본 고유 이름입니다	
ID 공급자(IDP) URL입니다	

설정	귀사의 가치
IdP(Identity Provider) 메타데이터	
SNMP 트랩 대상 호스트 IP 주소입니다	
SNMP 포트	

클러스터 정보

Unified Manager를 사용하여 관리하는 스토리지 시스템의 세부 정보입니다.

클러스터 **1/N**	귀사의 가치
호스트 이름 또는 클러스터 관리 IP 주소입니다	
ONTAP 관리자 사용자 이름입니다 관리자가 "admin" 역할을 할당받아야 합니다.	
ONTAP 관리자 암호입니다	
프로토콜	HTTPS

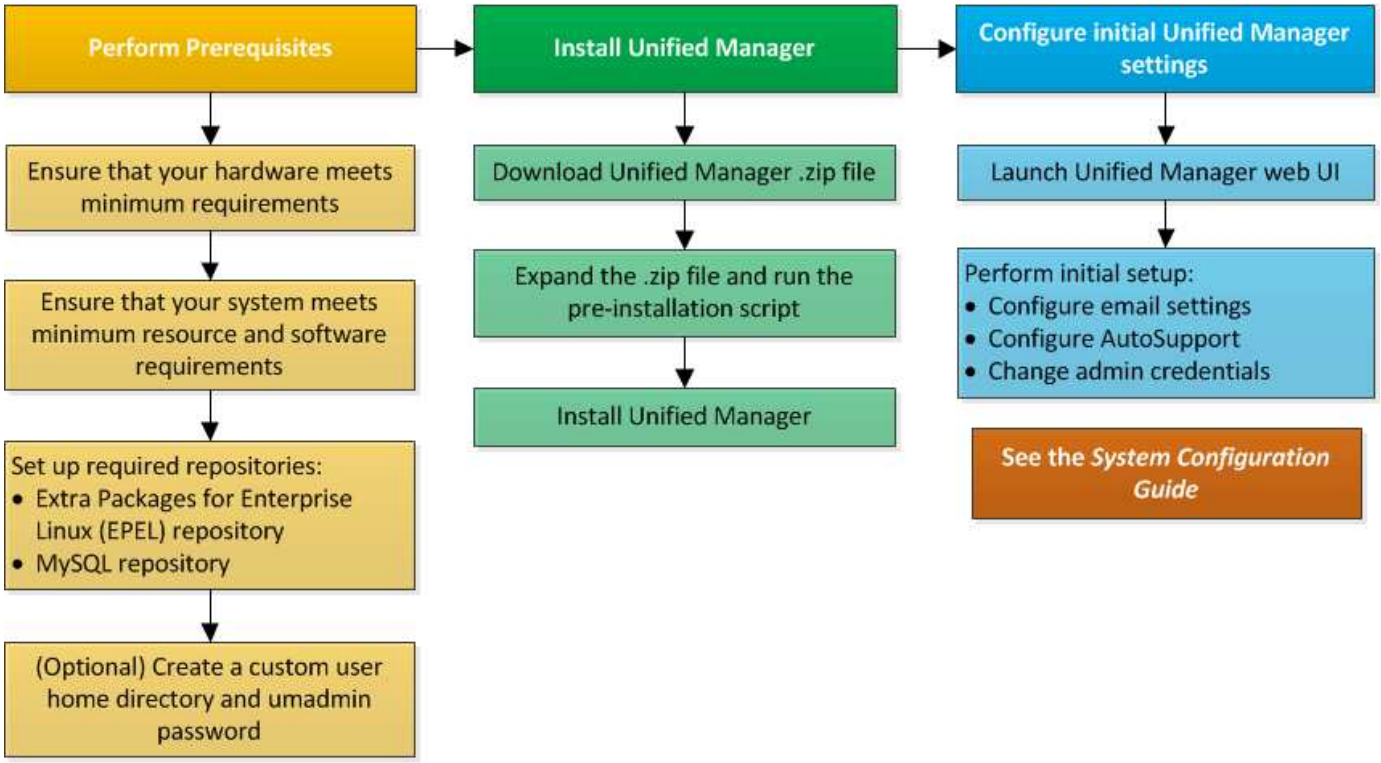
Unified Manager 소프트웨어의 설치, 업그레이드 및 제거

Linux 시스템에서는 Unified Manager 소프트웨어를 설치하거나, 최신 버전의 소프트웨어로 업그레이드하거나, Unified Manager를 제거할 수 있습니다.

Unified Manager는 Red Hat Enterprise Linux 또는 CentOS 서버에 설치할 수 있습니다. Unified Manager를 설치하는 Linux 서버는 물리적 시스템이나 VMware ESXi, Microsoft Hyper-V 또는 Citrix XenServer에서 실행되는 가상 머신에서 실행될 수 있습니다.

설치 프로세스 개요

설치 워크플로우에서 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.



필요한 소프트웨어 리포지토리를 설정합니다

설치 프로그램이 필요한 모든 소프트웨어 종속성을 액세스하고 설치할 수 있도록 시스템에 특정 저장소에 대한 액세스 권한이 있어야 합니다.

EPEL 리포지토리를 수동으로 구성합니다

Unified Manager를 설치하는 시스템에 EPEL(Enterprise Linux) 리포지토리용 추가 패키지에 대한 액세스 권한이 없는 경우, 설치를 성공적으로 수행하려면 리포지토리를 수동으로 다운로드하고 구성해야 합니다.

EPEL 리포지토리는 시스템에 설치해야 하는 필수 타사 유틸리티에 대한 액세스를 제공합니다. Red Hat Enterprise Linux 또는 CentOS 시스템에 Unified Manager를 설치할 때 EPEL 리포지토리를 사용합니다.

단계

1. 설치를 위해 EPEL 리포지토리를 다운로드합니다. Red Hat Enterprise Linux 7의 경우 다음 위치에서 다운로드하십시오.

   "와우와 https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm`[]

   버전 8의 경우 다음에서 다운로드하십시오.

   "와우와 https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm`[]

2. EPEL 리포지토리 구성:

   "yum install EPEL-release-latest-<version>.narch.rpm'

Red Hat Enterprise Linux 8 시스템의 경우, 모듈식 RPM 패키지(예: '*javapackages-filesystem-<version>.module.rpm*')가 있는 내부 저장소가 있는 경우, 동일한 리포지토리에서 모듈식 패키지에 대한 메타데이터도 사용할 수 있도록 합니다.

MySQL 리포지토리를 수동으로 구성합니다

Unified Manager를 설치하는 시스템에 MySQL Community Edition 저장소에 대한 액세스 권한이 없는 경우, 설치를 성공적으로 수행하려면 리포지토리를 수동으로 다운로드하여 구성해야 합니다.

MySQL 리포지토리는 시스템에 설치해야 하는 필수 MySQL 소프트웨어에 대한 액세스를 제공합니다.

시스템에 인터넷이 연결되어 있지 않으면 이 작업이 실패할 수 있습니다. Unified Manager를 설치하는 시스템에 인터넷에 액세스할 수 없는 경우 MySQL 설명서를 참조하십시오.

단계

1. 설치를 위해 적절한 MySQL 리포지토리를 다운로드합니다. Red Hat Enterprise Linux 7의 경우 다음 위치에서 다운로드하십시오.

   "와우와 http://repo.mysql.com/yum/mysql-8.0-community/el/7/x86_64/mysql80-community-release-el7-3.noarch.rpm`[]

   버전 8의 경우 다음에서 다운로드하십시오.

   "와우와 http://repo.mysql.com/yum/mysql-8.0-community/el/8/x86_64/mysql80-community-release-el8-1.noarch.rpm`[]

2. MySQL 리포지토리 구성:

   'yum install mysql80 -community-release-<version>.nocarch.rpm'

Red Hat Enterprise Linux 8 시스템의 경우, Java-11-openjdk, p7zip 및 AppStream 리포지토리에서 제공하는 기타 소프트웨어 패키지가 있는 내부 저장소가 있는 경우 AppStream 리포지토리를 비활성화하고 MySQL Community Server를 설치해야 합니다. 다음 명령을 실행합니다.

```
# sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install  mysql-community-server
```

키 누락 또는 키 불일치에 대한 오류가 발생하고 설치에 실패한 경우 다음 단계를 수행하십시오.

- 연결된 시스템에서 다음 명령을 실행하여 업데이트된 MySQL 키를 가져옵니다.

```
rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-<xxxx>

for example:

rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022
```

- 인터넷에 연결되지 않은 시스템에서는 gpgcheck=0으로 표시하여 MySQL repo 파일을 업데이트하고 gpgcheck를 비활성화합니다.

NFS 및 CIFS 공유에 대한 SELinux 요구 사항

NAS 또는 SAN 장치에 '/opt/netapp' 또는 '/opt/netapp/data'를 마운트하고 SELinux를 활성화한 경우 몇 가지 고려 사항을 염두에 두어야 합니다.

루트 파일 시스템이 아닌 다른 곳에서 '/opt/netapp' 또는 '/opt/netapp/data'를 마운트하고 사용자 환경에서 SELinux를 활성화한 경우 마운트된 디렉토리에 대한 올바른 컨텍스트를 설정해야 합니다. 사용자 환경의 해당 시나리오에 대해 올바른 SELinux 컨텍스트를 설정하고 확인하려면 다음 단계를 수행하십시오.

SELinux 컨텍스트 구성 시기 `/opt/netapp/data` 탑재됩니다

시스템에 '/opt/netapp/data'를 마운트하고 SELinux가 'Enforcing'으로 설정된 경우, 데이터베이스 파일 위치의 기본 컨텍스트 요소인 '/opt/netapp/data'에 대한 SELinux context type이 'mysqld_db_t'로 설정되어 있는지 확인하십시오.

1. 다음 명령을 실행하여 컨텍스트를 확인합니다.

   'ls-dZ/opt/netapp/data'

   샘플 출력:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0
   /opt/netapp/data
   ```

   이 출력에서 컨텍스트는 ddefault_t입니다. 이 컨텍스트를 mysqld_db_t로 변경해야 합니다.

2. 다음 단계를 수행하여 '/opt/netapp/data'를 마운트한 방법에 따라 컨텍스트를 설정합니다.

   a. 다음 명령을 실행하여 컨텍스트를 로 설정합니다 `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp/data"`
   `` `restorecon -R -v /opt/netapp/data ``

   b. '/etc/fstab'에서 '/opt/netapp/data'를 구성한 경우 '/etc/fstab' 파일을 편집해야 합니다. '/opt/netapp/data/' 마운트 옵션의 경우 MySQL 레이블을 다음과 같이 추가합니다.

   'CONTEXT=system_u:object_r:mysqld_db_t:s0'

   c. 컨텍스트를 설정하려면 '/opt/netapp/data/'를 마운트 해제하고 다시 마운트하십시오.

   d. 직접 NFS 마운트가 있는 경우 다음 명령을 실행하여 컨텍스트를 mysqld_db_t로 설정합니다.

   '<nfsshare>:/<mountpoint>/opt/netapp/data-o context=system_u:object_r:mysqld_db_t:s0'

3. 컨텍스트가 올바르게 설정되었는지 확인합니다.

'ls-dZ/opt/netapp/data/'

샘플 출력:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/
```

SELinux 컨텍스트 구성 시기 `/opt/netapp` 이**(**가**)** 장착된 경우 및 입니다 `/opt/netapp/data/` 또한 별도로 장착됩니다

이 시나리오에서는 먼저 이전 섹션에서 설명한 대로 '/opt/netapp/data/'의 컨텍스트를 설정해야 합니다. '/opt/netapp/data/'에 대한 올바른 컨텍스트를 설정한 후 부모 디렉토리 '/opt/netapp'에 SELinux 컨텍스트가 ' file_t'로 설정되어 있지 않은지 확인합니다.

단계

1. 다음 명령을 실행하여 컨텍스트를 확인합니다.

   'ls-dZ/opt/netapp'

   샘플 출력:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:file_t:s0 /opt/netapp
   ```

   이 출력에서 컨텍스트는 file_t가 변경되어야 합니다. 다음 명령어를 실행하면 해당 컨텍스트가 usr_t로 설정됩니다. 보안 요구 사항에 따라 context를 file_t 이외의 값으로 설정할 수 있습니다.

2. 다음 단계를 수행하여 '/opt/NetApp'을(를) 마운트한 방법에 따라 컨텍스트를 설정합니다.

   a. 다음 명령을 실행하여 컨텍스트를 설정합니다.

```
semanage fcontext -a -t usr_t "/opt/netapp"
restorecon -v /opt/netapp
```

1. '/etc/fstab'에서 '/opt/netapp'를 구성한 경우 '/etc/fstab' 파일을 편집해야 합니다. '/opt/netapp' 마운트 옵션에 MySQL 레이블을 다음과 같이 추가합니다.

   'CONTEXT=system_u:object_r:usr_t:s0'

2. 마운트 해제한 다음 컨텍스트를 사용하도록 다시 `/opt/netapp'을 마운트합니다.
3. 직접 NFS 마운트가 있는 경우 다음 명령을 실행하여 컨텍스트를 설정합니다.

   mount <nfsshare>:/<mountpoint>/opt/netapp-o context=system_u:object_r:usr_t:s0'

   a. 컨텍스트가 올바르게 설정되었는지 확인합니다.

      'ls-dZ/opt/netapp'

   샘플 출력입니다

```
drwxr-xr-x. mysql root unconfined_u:object_r:usr_t:s0 /opt/netapp
```

SELinux 컨텍스트 구성 시기 `/opt/netapp` 이**(**가**)** 장착된 경우 및 입니다 `/opt/netapp/data/` 은**(**는**)** 별도로 마운트되지 않습니다

시스템에 '/opt/netapp'를 마운트하고 SELinux가 'Enforcing'으로 설정된 경우, 데이터베이스 파일 위치의 기본 컨텍스트 요소인 '/opt/NetApp'에 대한 SELinux context type이 mysqld_db_t'로 설정되어 있는지 확인하십시오.

단계

1. 다음 명령을 실행하여 컨텍스트를 확인합니다.

   'ls-dZ/opt/netapp'

   샘플 출력:

   ```
   drwxr-xr-x. mysql root unconfined_u:object_r:default_t:s0 /opt/netapp
   ```

   이 출력에서 컨텍스트는 ddefault_t입니다. 이 컨텍스트를 mysqld_db_t로 변경해야 합니다.

2. 다음 단계를 수행하여 '/opt/NetApp'을(를) 마운트한 방법에 따라 컨텍스트를 설정합니다.

   a. 다음 명령을 실행하여 컨텍스트를 로 설정합니다 `mysqld_db_t`:
   `semanage fcontext -a -t mysqld_db_t "/opt/netapp"`
   `` `restorecon -R -v /opt/netapp ``

   b. '/etc/fstab'에서 '/opt/netapp'를 구성한 경우 '/etc/fstab' 파일을 편집합니다. '/opt/netapp/'mount option에 mysql label을 'context=system_u:object_r:mysqld_db_t:s0'으로 추가한다

   c. 마운트 해제한 다음 컨텍스트를 사용하도록 다시 `/opt/netapp/'를 마운트합니다.

   d. 직접 NFS 마운트가 있는 경우 다음 명령을 실행하여 컨텍스트를 mysqld_db_t"로 설정합니다. mount <nfsshare>:/<mountpoint>/opt/netapp-o context=system_u:object_r:mysqld_db_t:s0"

3. 컨텍스트가 올바르게 설정되었는지 확인합니다.

'ls-dZ/opt/netapp/'

샘플 출력:

```
drwxr-xr-x. mysql root unconfined_u:object_r:mysqld_db_t:s0 /opt/netapp/
```

Linux 시스템에 Unified Manager 설치

Unified Manager를 다운로드하고 설치하는 단계는 설치 시나리오에 따라 다르다는 점을 이해하는 것이 중요합니다.

설치 전에 사용자 정의 사용자 홈 디렉토리 및 **umadmin** 암호를 생성합니다

Unified Manager를 설치하기 전에 사용자 지정 홈 디렉터리를 만들고 사용자 고유의 umadmin 사용자 암호를 정의할 수 있습니다. 이 작업은 선택 사항이지만 일부 사이트에서는 Unified Manager 설치 기본 설정을 재정의할 수 있는 유연성을 필요로 할 수 있습니다.

- 필요한 것 *
- 시스템은 에 설명된 요구 사항을 충족해야 합니다 "하드웨어 시스템 요구 사항".
- Red Hat Enterprise Linux 또는 CentOS 시스템에 루트 사용자로 로그인할 수 있어야 합니다.

기본 Unified Manager 설치는 다음 작업을 수행합니다.

- 홈 디렉토리로 '/home/umadmin'을 사용하여 umadmin 사용자를 생성합니다.
- 기본 암호 ""admin""을 umadmin 사용자에게 할당합니다.

일부 설치 환경에서는 '/home'에 대한 액세스가 제한되므로 설치가 실패합니다. 다른 위치에 홈 디렉토리를 생성해야 합니다. 또한 일부 사이트에는 암호 복잡성에 대한 규칙이 있거나 설치 프로그램에서 설정하는 대신 로컬 관리자가 암호를 설정해야 할 수 있습니다.

설치 환경에서 이러한 설치 기본 설정을 재정의해야 하는 경우 다음 단계에 따라 사용자 지정 홈 디렉터리를 만들고 umadmin 사용자의 암호를 정의합니다.

설치 전에 이 정보를 정의하면 설치 스크립트가 이러한 설정을 검색하고 설치 기본 설정을 사용하는 대신 정의된 값을 사용합니다.

또한 기본 Unified Manager 설치에는 '/etc/sudoers.d/' 디렉토리의 sudoers 파일('ocum_sudoers' 및 'socie_sudoers')에 있는 umadmin 사용자가 포함됩니다. 보안 정책 또는 일부 보안 모니터링 도구로 인해 환경에서 이 콘텐츠를 제거하는 경우 다시 추가해야 합니다. 일부 Unified Manager 작업에서는 sudo 권한이 필요하므로 sudoers 구성을 유지해야 합니다.

사용자 환경의 보안 정책이 Unified Manager 유지 관리 사용자에 대한 sudo 권한을 제한하지 않아야 합니다. 권한이 제한된 경우 일부 Unified Manager 작업이 실패할 수 있습니다. 성공적으로 설치한 후 umadmin 사용자로 로그인하면 다음 sudo 명령을 실행할 수 있는지 확인합니다.

'SUDO systemctl status socie'

이 명령은 오류 없이 해당 상태인 socie 서비스를 반환해야 합니다.

단계

1. 서버에 루트 사용자로 로그인합니다.
2. "유지보수"라는 umadmin 그룹 계정을 만듭니다.

   그룹추가 유지 보수

3. 선택한 홈 디렉토리 아래의 유지보수 그룹에서 사용자 계정 ""umadmin""을 생성합니다.

   'adduser — home <home_directory\> -g maintenance umadmin'

4. umadmin 암호 정의:

'passwd umadmin'

umadmin 사용자의 새 암호 문자열을 입력하라는 메시지가 표시됩니다.

Unified Manager를 설치한 후에는 umadmin 사용자 로그인 셸을 지정해야 합니다.

Unified Manager 다운로드 중

Unified Manager를 설치하려면 NetApp Support 사이트에서 Unified Manager '.zip' 파일을 다운로드해야 합니다.

- 필요한 것 *

NetApp Support 사이트에 대한 로그인 자격 증명이 있어야 합니다.

Red Hat Enterprise Linux 및 CentOS 시스템에 대해 동일한 Unified Manager 설치 패키지를 다운로드합니다.

단계

1. NetApp Support 사이트에 로그인하고 Unified Manager의 다운로드 페이지로 이동합니다.

   "NetApp Support 사이트"

2. Unified Manager의 필수 버전을 선택하고 최종 사용자 라이센스 계약(EULA)에 동의합니다.
3. Linux용 Unified Manager 설치 프로그램 파일을 다운로드하고 대상 시스템의 디렉토리에 .zip 파일을 저장합니다.

   ◦ Red Hat Enterprise Linux 시스템에 맞는 설치 관리자 파일 버전을 다운로드했는지 확인합니다. Red Hat Enterprise Linux 7 또는 8이 설치되어 있는지 여부에 따라 Unified Manager '.zip' 파일의 적절한 버전을 다운로드해야 합니다.

   ◦ 코드 서명 인증서를 다운로드할 것을 권장합니다 (`.pem`) 및 디지털 서명 (`.sig`)를 참조하십시오 `.zip` 파일.

4. 다운로드한 소프트웨어의 무결성 체크섬을 확인합니다.
5. 코드 서명 인증서와 디지털 서명을 다운로드한 경우 설치 프로그램 파일의 무결성을 확인할 수 있습니다. 다음 명령을 사용하여 설치 프로그램 파일의 무결성을 확인할 수 있습니다.

   ◦ 이 명령은 코드 서명 인증서에서 공개 키로 파일을 만듭니다.

   ```
   openssl x509 -pubkey -noout -in AIQUM-RHEL-CLIENT-INTER-ROOT.pem >
   <public_key_file_name>
   ```

   ▪ 여기서 * AIQUM-RHEL-CLIENT-INTER-ROOT.PEM * 은 코드 서명 인증서가 들어 있는 파일입니다.

   ◦ 이 명령은 설치 프로그램 파일의 서명을 확인합니다.

   ```
   openssl dgst -sha256 -verify <public_key_file_name> -signature
   <signature_file_name> ActiveIQUnifiedManager-<version>.zip
   ```

메시지가 와 유사합니다 `Verified Ok` 설치 프로그램 파일을 사용해도 안전한지 확인합니다.

Unified Manager 설치 중

Unified Manager를 물리적 또는 가상 Red Hat Enterprise Linux 또는 CentOS 플랫폼에 설치할 수 있습니다.

- 필요한 것 *
- Unified Manager를 설치할 시스템은 시스템 및 소프트웨어 요구사항을 충족해야 합니다.

  을 참조하십시오 "하드웨어 시스템 요구 사항".

  을 참조하십시오 "Linux 소프트웨어 및 설치 요구 사항".

- NetApp Support 사이트에서 대상 시스템으로 Unified Manager '.zip' 파일을 다운로드해야 합니다.
- 다운로드한 의 무결성을 확인해야 합니다 `.zip` 파일.
- 지원되는 웹 브라우저가 있어야 합니다.
- 터미널 에뮬레이션 소프트웨어에 scrollback이 활성화되어 있어야 합니다.

Red Hat Enterprise Linux 또는 CentOS 시스템에는 필요한 지원 소프트웨어(Java, MySQL, 추가 유틸리티)의 모든 필수 버전이 설치되어 있거나, 필요한 소프트웨어 중 일부만 설치되어 있거나, 필요한 소프트웨어가 설치되지 않은 새로 설치된 시스템일 수 있습니다.

단계

1. Unified Manager를 설치할 서버에 로그인합니다.
2. 적절한 명령을 입력하여 설치를 지원하기 위해 타겟 시스템에 설치 또는 업그레이드해야 할 소프트웨어를 평가합니다.

필수 소프트웨어 및 최소 버전	명령을 사용하여 소프트웨어 및 버전을 확인합니다
OpenJDK 버전 11.0.21	자바 버전
MySQL 8.0.34 커뮤니티 에디션	"rpm-qa
grep-i mysql"을 참조하십시오	p7zip 16.02
"rpm-qa	grep p7zip"

3. 설치된 MySQL 버전이 MySQL 8.0.34 Community Edition보다 이전 버전인 경우 다음 명령을 입력하여 제거합니다.

   "rpm -e <mysql_package_name>"를 입력합니다

   종속성 오류가 발생하면 구성 요소를 제거하려면 '--nodeps' 옵션을 추가해야 합니다.

4. 설치 '.zip' 파일을 다운로드한 디렉토리로 이동하여 Unified Manager 번들을 확장합니다.

'ActiveIQUnifiedManager-<*version*>.zip의 압축을 풉니다.

Unified Manager에 필요한 '.rpm' 모듈의 압축이 대상 디렉토리에 풀립니다.

5. 디렉토리에서 다음 모듈을 사용할 수 있는지 확인합니다.

   "ls *.rpm"

   'netapp-um <version>.x86_64.rpm'

6. 설치 전 스크립트를 실행하여 Unified Manager 설치와 충돌할 수 있는 시스템 구성 설정이나 설치된 소프트웨어가 없는지 확인합니다.

   'SUDO./PRE_INSTALL_CHECK.sh'를 선택합니다

   사전 설치 스크립트는 시스템에 유효한 Red Hat Enterprise Linux 서브스크립션이 있으며 필요한 소프트웨어 저장소에 대한 액세스 권한이 있는지 확인합니다. 스크립트에서 문제가 식별되면 Unified Manager를 설치하기 전에 문제를 해결해야 합니다.

   Red Hat Enterprise Linux 8 시스템의 경우 JDK 11-OpenJDK, p7zip 및 AppStream 리포지토리에서 제공하는 기타 소프트웨어 패키지가 있는 내부 저장소가 있는 경우 AppStream 리포지토리를 비활성화하고 MySQL Community Server를 설치해야 합니다. 다음 명령을 실행합니다.

   ```
   # sudo yum --disablerepo=rhel-8-for-x86_64-appstream-rpms install
   mysql-community-server
   ```

7. * 선택 사항:* 시스템이 인터넷에 연결되어 있지 않은 경우에만 7단계를 수행해야 하며 설치에 필요한 패키지를 수동으로 다운로드해야 합니다. 시스템에 인터넷 액세스가 있고 필요한 모든 패키지를 사용할 수 있는 경우 8단계로 이동합니다. 인터넷에 연결되어 있지 않거나 Red Hat Enterprise Linux 리포지토리를 사용하지 않는 시스템의 경우 다음 단계를 수행하여 필요한 패키지가 있는지 확인한 다음 해당 패키지를 다운로드하십시오.

   a. Unified Manager를 설치할 시스템에서 사용 가능한 패키지 및 사용할 수 없는 패키지 목록은 +를 참조하십시오
      `yum install netapp-um<version>.x86_64.rpm --assumeno`

      ""설치 중:"" 섹션의 항목은 현재 디렉터리에서 사용할 수 있는 패키지이며 ""종속성 설치:"" 섹션의 항목은 시스템에 없는 패키지입니다.

   b. 인터넷에 액세스할 수 있는 시스템에서 누락된 패키지를 다운로드합니다.

      "yum install <package_name>--downloadonly—downlodaddr=.'

      > 플러그인 ""yum-plugin-downloadonly""가 Red Hat Enterprise Linux 시스템에서 항상 활성화되어 있는 것은 아니므로 "yum install yum-plugin-downloadonly"를 설치하지 않고 패키지를 다운로드하도록 기능을 설정해야 할 수 있습니다

   a. 인터넷 연결 시스템에서 설치 시스템으로 누락된 패키지를 복사합니다.

8. 루트 사용자 또는 'SUDO'를 사용하여 다음 명령을 실행하여 소프트웨어를 설치합니다.

   'yum install netapp-um <version>.x86_64.rpm'

   이 명령은 .rpm 패키지, 기타 필요한 지원 소프트웨어 및 Unified Manager 소프트웨어를 설치합니다.

GPG NOKEY 오류로 인해 설치가 실패하는 경우 를 사용합니다 `rpm --import` URL에서 키를 가져오려면:

`rpm --import https://repo.mysql.com/RPM-GPG-KEY-mysql-2022`

> 다른 명령(예: rpm-ivh)을 사용하여 설치를 시도하지 마십시오. Red Hat Enterprise Linux 또는 CentOS 시스템에 Unified Manager를 성공적으로 설치하려면 모든 Unified Manager 파일과 관련 파일이 특정 순서로 특정 디렉토리 구조에 설치되어 있어야 합니다. 이 디렉토리 구조는 "yum install NetApp -um <version>.x86_64.rpm" 명령에 의해 자동으로 적용됩니다.

9. 설치 메시지 직후에 표시되는 이메일 알림은 무시하십시오.

   e-메일은 초기 cron 작업 실패를 루트 사용자에게 알려 주며 설치에 부정적인 영향을 주지 않습니다.

10. 설치 메시지가 완료된 후 Unified Manager 웹 UI의 IP 주소 또는 URL, 유지보수 사용자 이름(umadmin), 기본 암호가 표시되는 메시지가 표시될 때까지 메시지를 다시 스크롤합니다.

    이 메시지는 다음과 유사합니다.

```
Active IQ Unified Manager installed successfully.
Use a web browser and one of the following URL(s) to configure and
access the Unified Manager GUI.
https://default_ip_address/    (if using IPv4)
https://[default_ip_address]/  (if using IPv6)
https://fully_qualified_domain_name/

Log in to Unified Manager in a web browser by using following details:
  username: umadmin
  password: admin
```

11. IP 주소 또는 URL, 할당된 사용자 이름(umadmin) 및 현재 암호를 기록합니다.
12. Unified Manager를 설치하기 전에 사용자 지정 홈 디렉터리를 사용하여 umadmin 사용자 계정을 만든 경우 umadmin 사용자 로그인 셸을 지정해야 합니다.

    'usermod -s /bin/maintenance-user-shell.sh umadmin'

에 설명된 대로 웹 UI에 액세스하여 umadmin 사용자의 기본 암호를 변경하고 Unified Manager의 초기 설정을 수행합니다 "Active IQ Unified Manager 구성". umadmin 사용자의 기본 암호를 변경해야 합니다.

Unified Manager 설치 중에 생성한 사용자입니다

Red Hat Enterprise Linux 또는 CentOS에 Unified Manager를 설치하면 Unified Manager 및 타사 유틸리티인 umadmin, JBoss 및 MySQL이 다음 사용자를 생성합니다.

- * umadmin *

  Unified Manager에 처음 로그인하는 데 사용됩니다. 이 사용자에게는 "애플리케이션 관리자" 사용자 역할이 할당되며 "유지보수 사용자" 유형으로 구성됩니다. 이 사용자는 Unified Manager를 통해 생성됩니다.

- * JBoss *

  JBoss 유틸리티와 관련된 Unified Manager 서비스를 실행하는 데 사용됩니다. 이 사용자는 Unified Manager를 통해 생성됩니다.

- * MySQL *

  Unified Manager의 MySQL 데이터베이스 쿼리를 실행하는 데 사용됩니다. 이 사용자는 MySQL 타사 유틸리티에 의해 생성됩니다.

Unified Manager는 이러한 사용자 외에도 유지 관리, JBoss 및 MySQL 같은 해당 그룹도 생성합니다. 유지 관리 및 JBoss 그룹은 Unified Manager에 의해 생성되고 MySQL 그룹은 타사 유틸리티에 의해 생성됩니다.

Unified Manager를 설치하기 전에 사용자 지정 홈 디렉터리를 만들고 사용자 고유의 umadmin 사용자 암호를 정의한 경우 설치 프로그램에서 유지보수 그룹 또는 umadmin 사용자를 다시 생성하지 않습니다.

JBoss 암호 변경

설치 중에 설정된 인스턴스별 JBoss 암호를 재설정할 수 있습니다. 사이트에 Unified Manager 설치 설정을 재정의하는 데 이 보안 기능이 필요한 경우 암호를 선택적으로 재설정할 수 있습니다. 이 작업은 JBoss가 MySQL에 액세스하는 데 사용하는 암호도 변경합니다.

- Unified Manager가 설치된 Red Hat Enterprise Linux 또는 CentOS 시스템에 대한 루트 사용자 액세스 권한이 있어야 합니다.
- 디렉토리 '/opt/netapp/Essentials/bin'에서 NetApp에서 제공한 password.sh' 스크립트에 액세스할 수 있어야 합니다.

단계

1. 시스템에서 루트 사용자로 로그인합니다.
2. 다음 명령을 표시된 순서대로 입력하여 Unified Manager 서비스를 중지합니다.

   '스타치틀스조우'

   '스ystemtl stop socie'

   연결된 MySQL 소프트웨어를 중지하지 마십시오.

3. 다음 명령을 입력하여 암호 변경 프로세스를 시작합니다.

   '/opt/netapp/essentials/bin/password.sh resetJBossPassword'

4. 메시지가 표시되면 새 JBoss 암호를 입력한 다음 다시 입력하여 확인합니다.

   암호는 8자에서 16자 사이여야 하며 숫자, 대문자, 소문자 및 다음 특수 문자 중 하나 이상을 포함해야 합니다.

   '!@%^ * -_=[]:<>.?/~+'

5. 스크립트가 완료되면 다음 명령을 표시된 순서대로 입력하여 Unified Manager 서비스를 시작합니다.

'스타ctl start socie'입니다

'신조 시작 조숙자'

6. 모든 서비스가 시작되면 Unified Manager UI에 로그인할 수 있습니다.

Red Hat Enterprise Linux 또는 CentOS에서 Unified Manager 업그레이드

새로운 버전이 출시되면 Unified Manager를 업그레이드할 수 있습니다.

NetApp에서 제공하는 Unified Manager 소프트웨어의 패치 릴리즈는 새로운 릴리즈와 동일한 절차를 사용하여 설치됩니다.

Unified Manager가 OnCommand Workflow Automation 인스턴스와 페어링되어 있고 두 제품 모두에 사용할 수 있는 새로운 소프트웨어 버전이 있는 경우 두 제품의 연결을 끊고 업그레이드를 수행한 후 새 Workflow Automation 연결을 설정해야 합니다. 제품 중 하나로 업그레이드하는 경우, 업그레이드 후에 Workflow Automation에 로그인하여 Unified Manager에서 데이터를 아직 취득하고 있는지 확인해야 합니다.

Unified Manager 버전에 지원되는 업그레이드 경로

Active IQ Unified Manager는 각 버전에 대한 특정 업그레이드 경로를 지원합니다.

모든 버전의 Unified Manager에서 이후 버전으로 업그레이드할 수 있는 것은 아닙니다. Unified Manager 업그레이드는 N-2 모델로 제한되어 있으며, 이는 모든 플랫폼의 다음 2개 릴리즈 내에서만 업그레이드할 수 있음을 의미합니다. 예를 들어, Unified Manager 9.12와 9.13에서만 Unified Manager 9.14로 업그레이드할 수 있습니다.

지원되는 버전보다 이전 버전을 실행 중인 경우 Unified Manager 인스턴스를 지원되는 버전 중 하나로 먼저 업그레이드한 다음 현재 버전으로 업그레이드해야 합니다.

예를 들어, 설치된 버전이 Unified Manager 9.9이고 Unified Manager 9.14로 업그레이드하려면 일련의 업그레이드를 수행해야 합니다.

샘플 업그레이드 경로:

1. 업그레이드 9.9 → 9.11
2. 업그레이드 9.11 → 9.13
3. 업그레이드 9.13 → 9.14

업그레이드 경로 매트릭스에 대한 자세한 내용은 다음을 참조하십시오 "기술 자료(KB) 문서".

Unified Manager 업그레이드

Linux 플랫폼에서 설치 파일을 다운로드하여 실행하면 Unified Manager 9.12 또는 9.13에서 9.14로 업그레이드할 수 있습니다.

- 필요한 것 *
- Unified Manager를 업그레이드하는 시스템은 시스템 및 소프트웨어 요구사항을 충족해야 합니다.

  을 참조하십시오 "하드웨어 시스템 요구 사항".

  을 참조하십시오 "Linux 소프트웨어 및 설치 요구 사항".

- Red Hat Enterprise Linux Subscription Manager에 가입해야 합니다.
- Unified Manager를 업그레이드하기 전에 올바른 버전의 OpenJDK를 설치하거나 업그레이드해야 합니다.

  을 참조하십시오 "Linux에서 JRE 업그레이드".

- 업그레이드 중에 문제가 발생할 경우 데이터 손실을 방지하려면 Unified Manager 데이터베이스의 백업을 생성해야 합니다. 에서 백업 파일을 이동하는 것이 좋습니다 `/opt/netapp/data` 외부 위치에 대한 디렉터리입니다.
- 업그레이드하는 동안 성능 데이터를 13개월 동안 유지하기 위한 이전 기본 설정을 유지할지 아니면 6개월로 변경할지 묻는 메시지가 표시될 수 있습니다. 확인 시, 기록 성능 데이터는 6개월 후에 삭제됩니다.
- 업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없으므로 실행 중인 작업을 모두 완료해야 합니다.
- MySQL Community Edition은 Unified Manager 업그레이드 중에 자동으로 업그레이드됩니다. 시스템에 설치된 MySQL 버전이 8.0.34 이전인 경우 Unified Manager 업그레이드 프로세스에서 MySQL을 8.0.34로 자동 업그레이드합니다.

단계

1. 대상 Red Hat Enterprise Linux 또는 CentOS 서버에 로그인합니다.
2. 서버에 Unified Manager 번들을 다운로드합니다.

   을 참조하십시오 "Linux용 Unified Manager 다운로드 중".

3. 타겟 디렉토리로 이동하고 Unified Manager 번들을 확장합니다.

   'ActiveIQUnifiedManager-<version>.zip의 압축을 풉니다.

   Unified Manager에 필요한 RPM 모듈의 압축이 대상 디렉토리에 풀립니다.

4. 디렉토리에서 다음 모듈을 사용할 수 있는지 확인합니다.

   "ls *.rpm"

   'netapp-um <version>.x86_64.rpm'

5. 사전 설치 스크립트를 실행하여 업그레이드와 충돌할 수 있는 시스템 구성 설정이나 설치된 소프트웨어가 없는지 확인합니다.

   'SUDO./PRE_INSTALL_CHECK.sh'를 선택합니다

   사전 설치 스크립트는 시스템에 유효한 Red Hat Enterprise Linux 서브스크립션이 있으며 필요한 소프트웨어 저장소에 대한 액세스 권한이 있는지 확인합니다. 스크립트에서 문제가 식별되면 문제를 해결하고 업그레이드를 계속 수행해야 합니다.

   누락된 패키지가 발견되면 에 설명된 단계를 수행합니다 "누락된 패키지에 대해 수행할 추가 단계입니다". 누락된 패키지가 없는 경우 다음 단계를 계속합니다.

6. 다음 스크립트를 사용하여 Unified Manager 업그레이드:

   업그레이드.sh

   이 스크립트는 RPM 모듈을 자동으로 실행하여 필요한 지원 소프트웨어 및 실행 중인 Unified Manager 모듈을 업그레이드합니다. 또한 업그레이드 스크립트는 업그레이드와 충돌할 수 있는 시스템 구성 설정이나 설치된

소프트웨어가 있는지 확인합니다. 스크립트에서 문제가 식별되면 Unified Manager를 업그레이드하기 전에 문제를 해결해야 합니다. Unified Manager를 업그레이드하기 전에 _net-snmp_와 같은 패키지를 이전에 설치한 경우 MySQL 종속성이 업그레이드 중에 패키지를 제거할 수 있습니다. 계속 사용하려면 패키지를 수동으로 다시 설치해야 합니다.

7. 업그레이드가 완료된 후 Unified Manager 웹 UI의 IP 주소 또는 URL, 유지보수 사용자 이름(umadmin) 및 기본 암호가 표시된 메시지가 나타날 때까지 메시지를 다시 스크롤합니다.

   이 메시지는 다음과 유사합니다.

```
Active IQ Unified Manager upgraded successfully.
Use a web browser and one of the following URLs to access the Unified
Manager GUI:

https://default_ip_address/    (if using IPv4)
https://[default_ip_address]/  (if using IPv6)
https://fully_qualified_domain_name/
```

지원되는 웹 브라우저의 새 창에 지정된 IP 주소 또는 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음, 앞서 설정한 유지보수 사용자 이름(umadmin) 및 암호를 사용하여 로그인합니다.

누락된 패키지에 대해 수행할 추가 단계입니다

업그레이드 중 사이트에서 누락된 패키지가 발견되거나 시스템이 인터넷에 연결되어 있지 않거나 Red Hat Enterprise Linux 리포지토리를 사용하지 않는 경우 다음 단계를 수행하여 필요한 패키지가 있는지 확인하고 패키지를 다운로드하십시오.

이러한 단계는 주 절차의 _5_단계 이후에 수행해야 합니다. 이 절차를 수행하면 Unified Manager가 업그레이드되며 업그레이드를 위해 추가 단계를 실행할 필요가 없습니다.

1. 사용 가능한 패키지 및 사용할 수 없는 패키지 목록을 봅니다.

   'yum install netapp-um <version>.x86_64.rpm --assulmeno'

   ""설치 중:"" 섹션의 항목은 현재 디렉터리에서 사용할 수 있는 패키지이며 ""종속성 설치:"" 섹션의 항목은 시스템에 없는 패키지입니다.

2. 인터넷에 액세스할 수 있는 다른 시스템에서 다음 명령을 실행하여 누락된 패키지를 다운로드합니다.

   "yum install package_name — downloadonly — downlopaddr=.'

   패키지는 '--downlodaddr='으로 지정된 디렉토리에 다운로드됩니다.

   플러그인 ""yum-plugin-downloadonly""가 Red Hat Enterprise Linux 시스템에서 항상 활성화되어 있는 것은 아니므로 패키지를 설치하지 않고 패키지를 다운로드할 수 있도록 기능을 설정해야 할 수 있습니다.

   'yum install yum-plugin-downloadonly

3. 다운로드한 패키지를 설치 시스템에서 Unified Manager 번들의 압축을 푼 디렉토리에 복사합니다.

4. 디렉토리를 해당 디렉토리로 변경하고 다음 명령을 실행하여 누락된 패키지를 해당 종속성에 따라 설치합니다.

   'yum install *.rpm'입니다

5. Unified Manager 서버를 시작합니다. 다음 명령을 실행합니다.

   '스타ctl start socie'입니다

   '신조 시작 조숙자'

이 프로세스는 Unified Manager 업그레이드 프로세스를 완료합니다. 지원되는 웹 브라우저의 새 창에 지정된 IP 주소 또는 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음, 앞서 설정한 유지보수 사용자 이름(umadmin) 및 암호를 사용하여 로그인합니다.

Red Hat Enterprise Linux 7.x에서 **8.x**로 호스트 **OS** 업그레이드

이전에 Red Hat Enterprise Linux 7.x 시스템에 Unified Manager를 설치했으며 Red Hat Enterprise Linux 8.x로 업그레이드해야 하는 경우 이 항목에 나열된 절차 중 하나를 따라야 합니다. 두 경우 모두 Red Hat Enterprise Linux 7.x 시스템에서 Unified Manager 백업을 생성한 다음 Red Hat Enterprise Linux 8.x 시스템으로 백업을 복원해야 합니다. 지원되는 Red Hat Enterprise Linux 버전은 8.0에서 8.7입니다.

아래 나열된 두 옵션의 차이점은 한 가지 경우에서 Unified Manager 복원을 새 8.x 서버로 수행하고 다른 경우에는 동일한 서버에서 복원 작업을 수행하고 있다는 것입니다.

이 작업을 수행하려면 Red Hat Enterprise Linux 7.x 시스템에 Unified Manager의 백업을 만들어야 하므로 전체 업그레이드 프로세스를 완료할 준비가 된 경우에만 Unified Manager가 가장 짧은 기간 동안 오프라인 상태가 되도록 백업을 만들어야 합니다. 수집된 데이터의 격차가 Unified Manager UI에 나타나는 것은 Red Hat Enterprise Linux 7.x 시스템이 종료되는 기간이며 새로운 Red Hat Enterprise Linux 8.x가 시작되기 전입니다.

을 참조하십시오 "백업 및 복원 작업 관리" 백업 및 복원 프로세스에 대한 자세한 지침을 검토해야 하는 경우

Red Hat Enterprise Linux 8.x 소프트웨어를 설치할 수 있는 예비 시스템이 있는 경우, Red Hat Enterprise Linux 7.x 시스템을 사용할 수 있는 동안 해당 시스템에서 Unified Manager 복원을 수행할 수 있도록 다음 단계를 따르십시오.

1. Red Hat Enterprise Linux 8.x 소프트웨어로 새 서버를 설치하고 구성합니다.

   을 참조하십시오 "Linux 소프트웨어 및 설치 요구 사항".

2. Red Hat Enterprise Linux 8.x 시스템에서 기존 Red Hat Enterprise Linux 7.x 시스템에 있는 것과 동일한 버전의 Unified Manager 소프트웨어를 설치합니다.

   을 참조하십시오 "Linux에 Unified Manager 설치".

   설치가 완료되면 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마십시오. 백업 파일은 복원 프로세스 중에 이 정보를 채웁니다.

3. Red Hat Enterprise Linux 7.x 시스템의 웹 UI의 관리 메뉴에서 Unified Manager 백업을 만든 다음 백업 파일(.7z 파일)과 데이터베이스 리포지토리 디렉토리("/database-dumps-repo" 하위 디렉토리)의 내용을 외부 위치로 복사합니다.
4. Red Hat Enterprise Linux 7.x 시스템에서 Unified Manager를 종료합니다.

5. Red Hat Enterprise Linux 8.x 시스템에서 백업 파일(.7z)을 외부 위치에서 '/opt/netapp/data/ocum-backup/'으로, 데이터베이스 리포지토리 파일을 '/ocum-backup' 디렉토리 아래의 '/database-dumps-repo' 하위 디렉토리로 복사합니다.
6. 다음 명령을 입력하여 백업 파일에서 Unified Manager 데이터베이스를 복원합니다.

   "um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>'
7. 웹 브라우저에 IP 주소 또는 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음 시스템에 로그인합니다.

시스템이 올바르게 작동하는지 확인한 후에는 Red Hat Enterprise Linux 7.x 시스템에서 Unified Manager를 제거할 수 있습니다.

- 동일한 서버에서 호스트 OS 업그레이드 *

Red Hat Enterprise Linux 8.x 소프트웨어를 설치할 수 있는 예비 시스템이 없는 경우 다음 단계를 따르십시오.

1. 웹 UI의 관리 메뉴에서 Unified Manager 백업을 생성한 다음 백업 파일(.7z' 파일)과 데이터베이스 저장소 디렉터리('/database-dumps-repo' 하위 디렉터리)의 내용을 외부 위치로 복사합니다.
2. 시스템에서 Red Hat Enterprise Linux 7.x 이미지를 제거하고 시스템을 완전히 초기화하십시오.
3. 동일한 시스템에 Red Hat Enterprise Linux 8.x 소프트웨어를 설치하고 구성합니다.

   을 참조하십시오 "Linux 소프트웨어 및 설치 요구 사항".
4. Red Hat Enterprise Linux 8.x 시스템에서 Red Hat Enterprise Linux 7.x 시스템에 있는 것과 동일한 버전의 Unified Manager 소프트웨어를 설치합니다.

   을 참조하십시오 "Linux에 Unified Manager 설치".

   설치가 완료되면 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마십시오. 백업 파일은 복원 프로세스 중에 이 정보를 채웁니다.
5. 외부 위치에서 '/opt/netapp/data/ocum-backup/'으로 백업 파일('.7z')을 복사하고 데이터베이스 저장소 파일은 '/ocum-backup' 디렉토리 아래의 '/database-dumps-repo' 하위 디렉토리로 복사합니다.
6. 다음 명령을 입력하여 백업 파일에서 Unified Manager 데이터베이스를 복원합니다.

   "um backup restore -f /opt/netapp/data/ocum-backup/<backup_file_name>'
7. 웹 브라우저에 IP 주소 또는 URL을 입력하여 Unified Manager 웹 UI를 시작한 다음 시스템에 로그인합니다.

Unified Manager 설치 후 타사 제품 업그레이드

Unified Manager가 Linux 시스템에 이미 설치되어 있는 경우 JRE와 같은 타사 제품을 업그레이드할 수 있습니다.

이러한 타사 제품을 개발하는 회사는 정기적으로 보안 취약점을 보고합니다. 사용자 일정에 따라 이 소프트웨어의 새 버전으로 업그레이드할 수 있습니다.

Linux에서 OpenJDK 업그레이드

Unified Manager가 설치된 Linux 서버에서 최신 버전의 OpenJDK로 업그레이드하여 보안

취약점에 대한 수정 사항을 확인할 수 있습니다.

- 필요한 것 *

Unified Manager가 설치된 Linux 시스템에 대한 루트 권한이 있어야 합니다.

릴리스 제품군 내에서 OpenJDK 릴리스를 업데이트할 수 있습니다. 예를 들어 OpenJDK 11.0.14에서 OpenJDK 11.0.17로 업그레이드할 수 있지만 OpenJDK 11에서 OpenJDK 12로 직접 업데이트할 수는 없습니다.

단계

1. Unified Manager 호스트 시스템에서 루트 사용자로 로그인합니다.
2. 대상 시스템에 적절한 버전의 OpenJDK(64비트)를 다운로드합니다.
3. Unified Manager 서비스 중지:

   '스타치틀스조우'

   '스ystemtl stop socie'

4. 시스템에 최신 OpenJDK를 설치합니다.
5. Unified Manager 서비스 시작:

   '스타ctl start socie'입니다

   '신조 시작 조숙자'

Unified Manager를 다시 시작하는 중입니다

구성을 변경한 후 Unified Manager를 다시 시작해야 할 수 있습니다.

- 필요한 것 *

Unified Manager가 설치된 Red Hat Enterprise Linux 또는 CentOS 서버에 대한 루트 사용자 액세스 권한이 있어야 합니다.

단계

1. Unified Manager 서비스를 다시 시작할 서버에 루트 사용자로 로그인합니다.
2. Unified Manager 서비스 및 관련 MySQL 서비스를 다음 순서로 중지합니다.

   '스타치틀스조우'

   '스ystemtl stop socie'

   '스타emctl stop mysqld'

3. MySQL 및 Unified Manager 서비스를 다음 순서대로 시작합니다.

   '스타emctl start mysqld'

   '스타ctl start socie'입니다

'신조 시작 조숙자'

`mysqld` MySQL Server를 시작 및 중지하는 데 필요한 데몬 프로그램입니다.

Unified Manager를 제거하는 중입니다

단일 명령으로 Red Hat Enterprise Linux 또는 CentOS 호스트에서 Unified Manager를 중지하고 제거할 수 있습니다.

- 필요한 것 *
- Unified Manager를 제거할 서버에 대한 루트 사용자 액세스 권한이 있어야 합니다.
- Linux 시스템에서 SELinux(Security-Enhanced Linux)를 비활성화해야 합니다. 을 사용하여 SELinux 런타임 모드를 ""허용""으로 변경합니다 `setenforce 0` 명령.
- 소프트웨어를 제거하기 전에 모든 클러스터(데이터 소스)를 Unified Manager 서버에서 제거해야 합니다.
- MySQL 포트 3306을 허용하거나 차단할 수 있도록 만들어진 방화벽 규칙을 수동으로 삭제해야 합니다. 방화벽 규칙은 자동으로 삭제되지 않습니다.

단계

1. Unified Manager를 제거할 서버에 루트 사용자로 로그인합니다.
2. 서버에서 Unified Manager를 중지하고 제거합니다.

   "rpm -e NetApp -um"

   이 단계에서는 관련된 모든 NetApp RPM 패키지를 제거합니다. Java, MySQL 및 p7zip 같은 필수 소프트웨어 모듈은 제거하지 않습니다.

3. * 선택 사항: * 필요한 경우 Java, MySQL 및 p7zip 같은 지원 소프트웨어 모듈을 제거합니다.

   rpm -e p7zip mysql -community -client mysql -community -server mysql -common mysql -community -libs java -x. y

이 작업이 완료되면 소프트웨어가 제거됩니다. 제거 후 "/opt/netapp/data" 디렉토리의 모든 데이터가 "/opt/netapp/data/backup" 폴더로 이동됩니다. Unified Manager를 제거하면 Java 및 MySQL 패키지도 제거됩니다. 단, 시스템의 다른 애플리케이션에서 패키지가 필요하고 사용되지 않습니다. 그러나 MySQL 데이터는 삭제되지 않습니다.

사용자 지정 **umadmin** 사용자 및 유지보수 그룹을 제거합니다

Unified Manager를 설치하기 전에 사용자 지정 홈 디렉터리를 만들어 자신의 umadmin 사용자 및 유지보수 계정을 정의한 경우 Unified Manager를 제거한 후 이러한 항목을 제거해야 합니다.

표준 Unified Manager 설치 제거를 사용해도 사용자 정의 umadmin 사용자 및 유지보수 계정은 제거되지 않습니다. 이러한 항목은 수동으로 삭제해야 합니다.

단계

1. Red Hat Enterprise Linux 서버에 루트 사용자로 로그인합니다.

2. umadmin 사용자를 삭제합니다.

   'userdel umadmin'

3. 유지보수 그룹을 삭제합니다.

   그룹델 유지보수

Windows 시스템에 Unified Manager를 설치합니다

Active IQ Unified Manager 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태 및 성능을 모니터링 및 관리할 수 있습니다. Unified Manager를 Linux 서버, Windows 서버 또는 VMware 호스트의 가상 어플라이언스에 구축할 수 있습니다.

설치를 완료하고 관리할 클러스터를 추가한 후에는 Unified Manager에서 모니터링되는 스토리지 시스템의 용량, 가용성, 보호 및 성능 상태를 표시하는 그래픽 인터페이스를 제공합니다.

- 관련 정보 *

"NetApp 상호 운용성 매트릭스 툴"

Unified Manager 서버의 기능

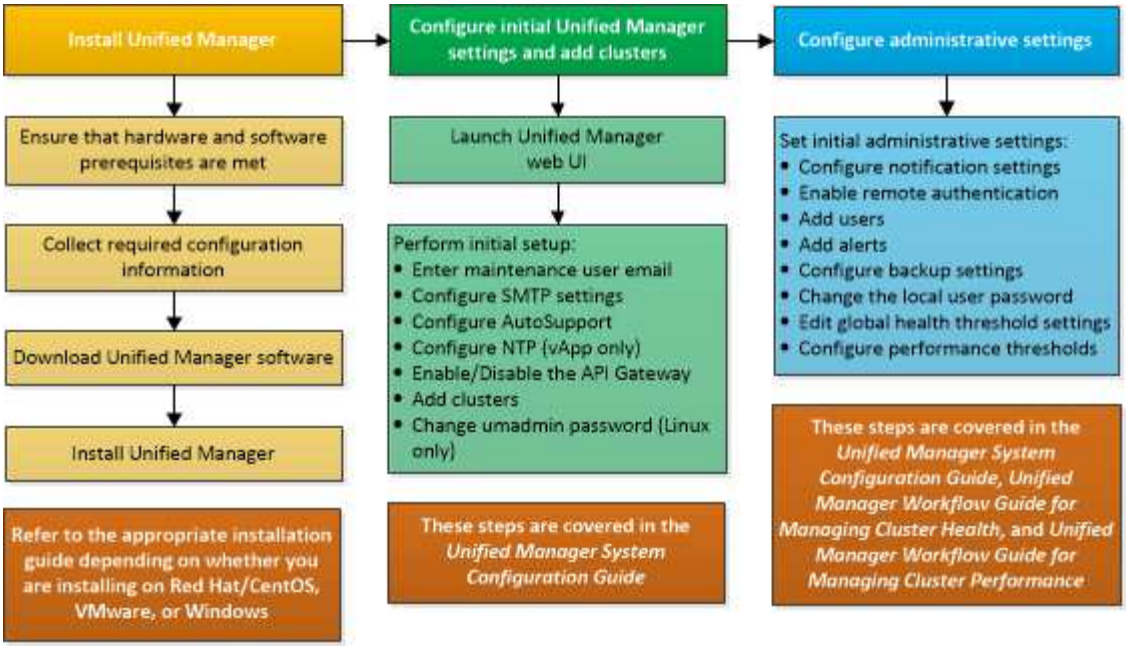
Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스 및 애플리케이션 서버로 구성됩니다. 검색, 모니터링, RBAC(역할 기반 액세스 제어), 감사, 로깅 등의 인프라 서비스를 제공합니다.

Unified Manager는 클러스터 정보를 수집하고, 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터 문제가 있는지 확인합니다.

설치 순서 개요

설치 워크플로우에서 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.

이 섹션에서는 아래 워크플로에 표시된 각 항목에 대해 설명합니다.



Unified Manager 설치 요구 사항

설치 프로세스를 시작하기 전에 Unified Manager를 설치할 서버가 특정 소프트웨어, 하드웨어, CPU 및 메모리 요구 사항을 충족하는지 확인하십시오.

NetApp은 Unified Manager 애플리케이션 코드의 수정을 지원하지 않습니다. Unified Manager 서버에 보안 조치를 적용해야 하는 경우 Unified Manager가 설치된 운영 체제를 변경해야 합니다.

Unified Manager 서버에 보안 조치를 적용하는 방법에 대한 자세한 내용은 기술 자료 문서를 참조하십시오.

"Clustered Data ONTAP을 위해 Active IQ Unified Manager에 적용된 보안 조치에 대한 지원 가능성"

- 관련 정보 *

"NetApp 상호 운용성 매트릭스 툴"

가상 인프라 및 하드웨어 시스템 요구 사항

가상 인프라 또는 물리적 시스템에 Unified Manager를 설치하려면 메모리, CPU 및 디스크 공간에 대한 최소 요구사항을 충족해야 합니다.

다음 표에는 메모리, CPU 및 디스크 공간 리소스에 권장되는 값이 나와 있습니다. 이러한 값은 Unified Manager가 허용 가능한 성능 수준을 충족할 수 있도록 검증을 받았습니다.

하드웨어 구성	권장 설정
RAM	12GB(최소 요구 사항 8GB)
프로세서	CPU 4개

하드웨어 구성	권장 설정
CPU 사이클 용량입니다	총 9572MHz(최소 요구 사항 9572MHz)
사용 가능한 디스크 공간	150GB로, 다음과 같이 용량이 할당됩니다. • 설치 디렉토리를 위한 100GB의 디스크 공간 • MySQL 데이터 디렉토리용 50GB의 디스크 공간

적은 용량의 메모리가 있는 시스템에 Unified Manager를 설치할 수 있지만 권장되는 12GB RAM을 사용하면 최적의 성능을 위해 충분한 메모리를 사용할 수 있으며, 따라서 시스템이 구성 증가에 따라 추가 클러스터 및 스토리지 오브젝트를 수용할 수 있습니다. Unified Manager가 구축된 VM에서 메모리 제한을 설정하지 말아야 하며, 시스템에서 할당된 메모리를 소프트웨어가 활용하지 못하는 기능(예: 풍선 벌루닝)을 사용하면 안 됩니다.

또한 Unified Manager의 두 번째 인스턴스를 설치하기 전에 Unified Manager의 단일 인스턴스에서 모니터링할 수 있는 노드 수에 제한이 있습니다. 자세한 내용은 _모범 사례 가이드_를 참조하십시오.

"기술 보고서 4621: Unified Manager 모범 사례 가이드"

메모리 페이지 스와핑은 시스템 및 관리 응용 프로그램의 성능에 부정적인 영향을 줍니다. 전체 호스트 활용률로 인해 CPU 리소스를 사용하지 않는 경우 성능이 저하될 수 있습니다.

전용 요구사항

Unified Manager를 설치하는 물리적 또는 가상 시스템은 Unified Manager에만 사용해야 하며 다른 애플리케이션과 공유해서는 안 됩니다. 다른 애플리케이션은 시스템 리소스를 소모하며 Unified Manager의 성능을 크게 줄일 수 있습니다.

백업에 필요한 공간 요구 사항

Unified Manager 백업 및 복원 기능을 사용하려면 "데이터" 디렉토리나 디스크에 150GB의 공간이 있도록 추가 용량을 할당합니다. 백업은 로컬 대상 또는 원격 대상에 쓸 수 있습니다. 모범 사례는 최소 150GB의 공간이 있는 Unified Manager 호스트 시스템 외부의 원격 위치를 식별하는 것입니다.

호스트 접속 구성 요구 사항

Unified Manager를 설치하는 물리적 시스템 또는 가상 시스템은 호스트 자체에서 호스트 이름을 성공적으로 "핑"할 수 있도록 구성해야 합니다. IPv6 구성의 경우 Unified Manager 설치가 성공적으로 수행되도록 호스트 이름에 대한 ping6(ping6)이 성공했는지 확인해야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 제품 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트의 이름을 지정합니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 얻어야 합니다.

사용자가 FQDN(정규화된 도메인 이름) 또는 IP 주소를 사용하는 대신 짧은 이름을 사용하여 Unified Manager에 액세스할 수 있도록 하려는 경우 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 해석해야 합니다.

Windows 소프트웨어 및 설치 요구 사항

Windows에 Unified Manager를 성공적으로 설치하려면 Unified Manager가 설치된 시스템이

소프트웨어 요구사항을 충족하는지 확인해야 합니다.

운영 체제 소프트웨어

Unified Manager는 다음 Windows 에디션에 설치할 수 있습니다.

- Microsoft Windows Server 2019 Standard 및 Datacenter Edition
- Microsoft Windows Server 2022 Standard 및 Datacenter Edition

Unified Manager는 64비트 Windows 운영 체제에서 다음 언어로 지원됩니다.

- 영어
- 일본어
- 중국어 간체

지원되는 Windows 버전의 전체 최신 목록은 상호 운용성 매트릭스 를 참조하십시오.

"mysupport.netapp.com/matrix"

NetApp은 Microsoft SCCM(System Center Configuration Manager)과 같은 타사 툴을 사용하여 Unified Manager 설치를 지원하지 않습니다.

서버는 Unified Manager 실행 전용으로 사용되어야 합니다. 서버에 다른 응용 프로그램을 설치할 수 없습니다. 회사 규정에 따라 Windows 시스템에 안티바이러스 소프트웨어가 설치되어 있을 수 있습니다. 설치 실패를 방지하려면 Unified Manager를 설치하기 전에 바이러스 백신 소프트웨어를 비활성화해야 합니다.

타사 소프트웨어

다음 타사 패키지는 Unified Manager와 함께 번들로 제공됩니다. 타사 패키지가 시스템에 설치되어 있지 않은 경우, Unified Manager에서 이를 설치의 일부로 설치합니다.

- Microsoft Visual C++ 2015 재배포 가능 패키지 버전 14.26.28720.3
- Microsoft Visual C++ Visual Studio 2013 버전 12.0.40660.0용 재배포 가능 패키지
- MySQL Community Edition 버전 8.0.34
- 파이썬 3.11.6
- OpenJDK 버전 11.0.20
- p7zip 버전 23.01 이상

Unified Manager 9.5부터 OpenJDK는 Unified Manager 설치 패키지에 제공되어 자동으로 설치됩니다. Oracle Java는 Unified Manager 9.5부터 지원되지 않습니다.

MySQL이 사전 설치된 경우 다음 사항을 확인해야 합니다.

- 기본 포트를 사용하고 있습니다.
- 샘플 데이터베이스가 설치되지 않았습니다.
- 서비스명은 MYSQL8.

Unified Manager는 WildFly 웹 서버에 구축되어 있습니다. WildFly 26.1.3은 Unified Manager와 함께 번들로 제공되며 구성됩니다.

타사 소프트웨어를 업그레이드하기 전에 Unified Manager를 실행 중인 인스턴스를 종료해야 합니다. 타사 소프트웨어 설치가 완료되면 Unified Manager를 다시 시작할 수 있습니다.

설치 요구 사항

- Microsoft .NET 4.5.2 이상이 설치되어 있어야 합니다.
- 임시 디렉터리는 설치 파일 압축을 풀 수 있도록 2GB의 디스크 공간으로 구성해야 합니다. 디렉토리가 생성되었는지 확인하려면 명령줄 인터페이스에서 ' echo %temp% ' 명령을 실행합니다
- Unified Manager MSI 파일을 캐시하려면 Windows 드라이브에 2GB의 디스크 공간을 예약해야 합니다.
- Unified Manager를 설치할 Microsoft Windows Server는 호스트 이름 및 FQDN에 대한 "ping" 응답이 성공하도록 FQDN(정규화된 도메인 이름)으로 구성해야 합니다.
- Microsoft IIS Worldwide 웹 게시 서비스를 비활성화하고 포트 80 및 443이 사용 가능한지 확인해야 합니다.
- 설치 중에 ""Windows Installer RDS 호환성""에 대한 원격 데스크톱 세션 호스트 설정이 비활성화되어 있는지 확인해야 합니다.
- UDP 포트 514는 사용 가능한 상태여야 하며 다른 서비스에서 사용하지 않아야 합니다.
- Unified Manager를 설치하기 전에 시스템에서 모든 바이러스 백신 소프트웨어를 비활성화해야 합니다. 설치가 완료된 후 바이러스 백신 검사에서 다음 경로를 수동으로 제외해야 합니다.
  - Unified Manager 데이터 디렉토리(예: 'C:\ProgramData\NetApp\OnCommandAppData\'
  - Unified Manager 설치 디렉토리(예: '\C:\Program Files\NetApp\'
  - MySQL 데이터 디렉터리(예: 'C:\ProgramData\MySQL\MySQLServerData')

지원되는 브라우저

Unified Manager 웹 UI에 액세스하려면 지원되는 브라우저를 사용하십시오.

상호 운용성 매트릭스에는 지원되는 브라우저 버전 목록이 있습니다.

"mysupport.netapp.com/matrix"

모든 브라우저의 경우 팝업 차단기를 비활성화하면 소프트웨어 기능이 제대로 표시됩니다.

IdP(ID 공급자)가 사용자를 인증할 수 있도록 SAML 인증을 위해 Unified Manager를 구성하려면 IDP에서 지원하는 브라우저 목록도 확인해야 합니다.

프로토콜 및 포트 요구 사항

필요한 포트와 프로토콜을 사용하면 Unified Manager 서버와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간에 통신할 수 있습니다.

Unified Manager 서버에 대한 연결

일반적으로 기본 포트는 항상 사용되므로 Unified Manager 웹 UI에 연결할 때 포트 번호를 지정할 필요가 없습니다.

예를 들어, Unified Manager가 항상 기본 포트에서 실행하려고 하므로 "https://<host>:443` 대신 "https://<host>` 를 입력할 수 있습니다.

Unified Manager 서버는 특정 프로토콜을 사용하여 다음 인터페이스에 액세스합니다.

인터페이스	프로토콜	포트	설명
Unified Manager 웹 UI	HTTP	80	Unified Manager 웹 UI에 액세스하는 데 사용되며 보안 포트 443으로 자동으로 리디렉션됩니다.
API를 사용하는 Unified Manager 웹 UI 및 프로그램	HTTPS	443	Unified Manager 웹 UI에 안전하게 액세스하거나 API 호출을 하는 데 사용되며 HTTPS를 통해서만 API 호출을 수행할 수 있습니다.
유지보수 콘솔	SSH/SFTP	22	유지보수 콘솔에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
Linux 명령줄	SSH/SFTP	22	Red Hat Enterprise Linux 또는 CentOS 명령줄에 액세스하고 지원 번들을 검색하는 데 사용됩니다.
Syslog를 클릭합니다	UDP입니다	514	ONTAP 시스템에서 서브스크립션 기반 EMS 메시지에 액세스하고 메시지를 기반으로 이벤트를 생성하는 데 사용됩니다.
휴식	HTTPS	9443	인증된 ONTAP 시스템에서 실시간 REST API 기반 EMS 이벤트에 액세스하는 데 사용됩니다.
MySQL 데이터베이스	MySQL	3306	OnCommand 및 OnCommand Workflow Automation API Services에서 Unified Manager에 액세스할 수 있도록 설정하는 데 사용됩니다.

MySQL의 기본 포트 3306은 Windows 시스템에 Unified Manager를 설치하는 동안 localhost로 제한됩니다. 설치가 완료되면 방화벽에서 MySQL 포트 3306에 대한 액세스를 제한합니다. 이전 구성이 유지되는 업그레이드 시나리오에는 영향을 주지 않습니다. 이 구성은 수정할 수 있으며 을 사용하여 다른 호스트에서 연결을 사용할 수 있습니다 `Control access to MySQL port 3306` 옵션을 설정할 수 있습니다. 자세한 내용은 을 참조하십시오 "추가 메뉴 옵션". HTTP 및 HTTPS 통신에 사용되는 포트(포트 80 및 443)는 Unified Manager 유지 관리 콘솔을 사용하여 변경할 수 있습니다. 자세한 내용은 을 참조하십시오 "Active IQ Unified Manager 구성".

Unified Manager 서버와의 연결입니다

Unified Manager Server와 관리되는 스토리지 시스템, 서버 및 기타 구성 요소 간의 통신을 활성화하는 포트를 열도록 방화벽을 구성해야 합니다. 포트가 열려 있지 않으면 통신이 실패합니다.

환경에 따라 Unified Manager 서버가 특정 대상에 연결하는 데 사용하는 포트와 프로토콜을 수정할 수 있습니다.

Unified Manager 서버는 다음 프로토콜과 포트를 사용하여 관리형 스토리지 시스템, 서버 및 기타 구성 요소에 연결합니다.

목적지	프로토콜	포트	설명
수행할 수 있습니다	HTTPS	443/TCP	스토리지 시스템을 모니터링 및 관리하는 데 사용됩니다.
수행할 수 있습니다	NDMP	10000/TCP	특정 스냅샷 복원 작업에 사용됩니다.
AutoSupport 서버	HTTPS	443	AutoSupport 정보를 전송하는 데 사용됩니다. 이 기능을 수행하려면 인터넷 액세스가 필요합니다.
인증 서버	LDAP를 지원합니다	389	인증 요청, 사용자 및 그룹 조회 요청을 하는 데 사용됩니다.
LDAPS	636	보안 LDAP 통신에 사용됩니다.	메일 서버
SMTP	25	경고 알림 이메일을 보내는 데 사용됩니다.	SNMP 트랩 보낸 사람
SNMPv1 또는 SNMPv3	162/UDP	알림 SNMP 트랩을 보내는 데 사용됩니다.	외부 데이터 공급자 서버
TCP	2003년	Graphite와 같은 외부 데이터 공급자에게 성능 데이터를 보내는 데 사용됩니다.	NTP 서버

워크시트를 작성합니다

Unified Manager를 설치 및 구성하기 전에 환경에 대한 정보를 즉시 확인할 수 있어야 합니다. 워크시트에 정보를 기록할 수 있습니다.

Unified Manager 설치 정보

Unified Manager를 설치하는 데 필요한 세부 정보

소프트웨어가 배포되는 시스템입니다	귀사의 가치
호스트 정규화된 도메인 이름입니다	
호스트 IP 주소입니다	
네트워크 마스크	
게이트웨이 IP 주소입니다	
기본 DNS 주소입니다	
보조 DNS 주소입니다	
도메인 검색	
유지보수 사용자 이름입니다	
유지보수 사용자 암호입니다	

Unified Manager 구성 정보

설치 후 Unified Manager를 구성하기 위한 세부 정보 일부 값은 구성에 따라 선택 사항입니다.

설정	귀사의 가치
유지보수 사용자 이메일 주소	
SMTP 서버 호스트 이름 또는 IP 주소입니다	
SMTP 사용자 이름입니다	
SMTP 암호	
SMTP 포트	25(기본값)

설정	귀사의 가치
알림 알림이 전송되는 이메일입니다	
인증 서버 호스트 이름 또는 IP 주소입니다	
Active Directory 관리자 이름 또는 LDAP 바인드 고유 이름입니다	
Active Directory 암호 또는 LDAP 바인딩 암호입니다	
인증 서버 기본 고유 이름입니다	
ID 공급자(IDP) URL입니다	
IdP(Identity Provider) 메타데이터	
SNMP 트랩 대상 호스트 IP 주소입니다	
SNMP 포트	

클러스터 정보

Unified Manager를 사용하여 관리하는 스토리지 시스템의 세부 정보입니다.

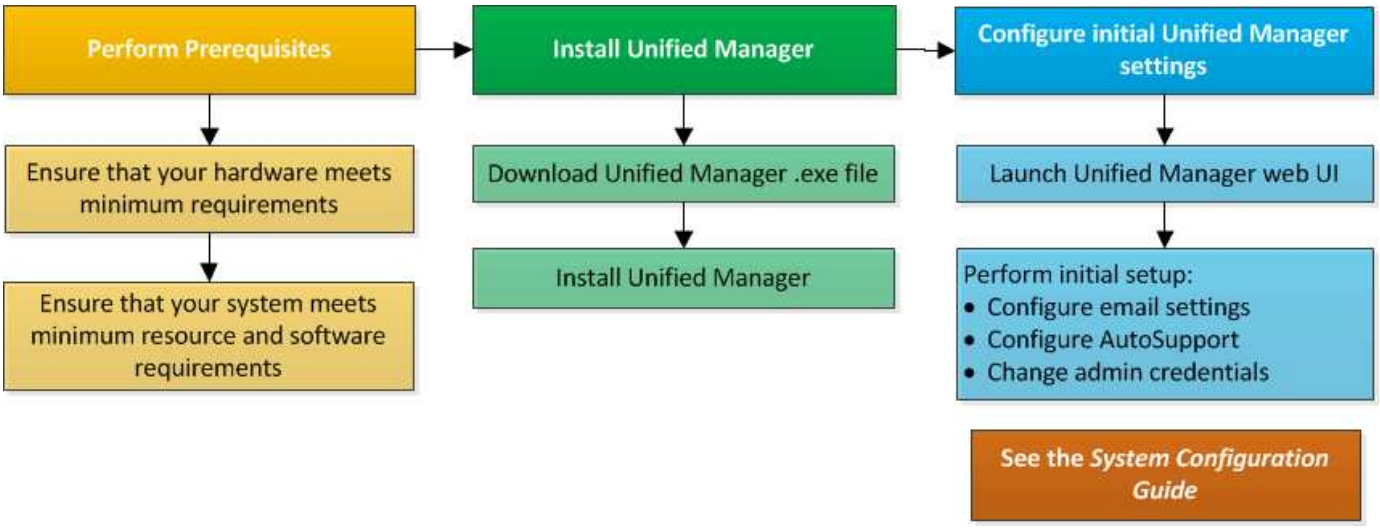
클러스터 **1/N**	귀사의 가치
호스트 이름 또는 클러스터 관리 IP 주소입니다	
ONTAP 관리자 사용자 이름입니다 관리자가 "admin" 역할을 할당받아야 합니다.	
ONTAP 관리자 암호입니다	
프로토콜	HTTPS

Unified Manager 소프트웨어의 설치, 업그레이드 및 제거

Unified Manager를 설치하거나, 최신 버전으로 업그레이드하거나, Unified Manager 애플리케이션을 제거할 수 있습니다.

설치 프로세스 개요

설치 워크플로우에서 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.



Windows에 Unified Manager 설치

Windows에서 Unified Manager를 다운로드하고 설치하는 일련의 단계를 이해하는 것이 중요합니다.

Unified Manager 설치 중

Unified Manager를 설치하여 데이터 스토리지의 용량, 가용성, 성능 및 보호 문제를 모니터링하고 문제를 해결할 수 있습니다.

- 필요한 것 *
- Unified Manager를 설치하려는 시스템은 시스템 및 소프트웨어 요구사항을 충족해야 합니다.

  을 참조하십시오 "하드웨어 시스템 요구 사항".

  을 참조하십시오 "Windows 소프트웨어 및 설치 요구 사항".

  Unified Manager 9.5부터 OpenJDK는 설치 패키지에 제공되어 자동으로 설치됩니다. Oracle Java는 Unified Manager 9.5부터 지원되지 않습니다.

- Windows 관리자 권한이 있어야 합니다. 사용자 이름이 느낌표 ""!""로 시작하지 않는지 확인합니다. 설치를 실행 중인 사용자의 이름이 ""!"(으로)로 시작하는 경우 Unified Manager 설치가 실패할 수 있습니다.
- 지원되는 웹 브라우저가 있어야 합니다.
- Unified Manager 유지보수 사용자 암호는 8자에서 20자 사이여야 하며, 대문자 또는 소문자, 숫자 및 특수 문자를 포함해야 합니다.
- 유지보수 사용자 또는 MySQL 루트 사용자의 암호 문자열에는 다음과 같은 특수 문자가 허용되지 않습니다: ""%,=&<>|^\/()[];:

  다음 특수 문자를 사용할 수 있습니다.~! @#$ * -? . {}

단계

1. 기본 로컬 관리자 계정을 사용하여 Windows에 로그인합니다.
2. NetApp Support 사이트에 로그인하고 Unified Manager의 다운로드 페이지로 이동합니다.

   "NetApp Support 사이트"

3. Unified Manager의 필수 버전을 선택하고 최종 사용자 라이센스 계약(EULA)에 동의합니다.
4. Unified Manager Windows 설치 파일을 Windows 시스템의 대상 디렉토리에 다운로드합니다.
5. 설치 파일이 있는 디렉터리로 이동합니다.
6. 마우스 오른쪽 단추를 클릭하고 Unified Manager 설치 관리자 실행 파일(.exe) 파일을 관리자로 실행합니다.

   Unified Manager에서 누락되거나 미리 설치된 타사 패키지를 감지하여 나열합니다. 필요한 타사 패키지가 시스템에 설치되어 있지 않은 경우, Unified Manager에서 설치 시 타사 패키지를 설치합니다.

7. 다음 * 을 클릭합니다.
8. 사용자 이름과 암호를 입력하여 유지보수 사용자를 생성합니다.
9. 데이터베이스 연결 마법사에서 MySQL 루트 암호를 입력합니다.
10. Unified Manager 설치 디렉토리 및 MySQL 데이터 디렉토리의 새 위치를 지정하려면 * 변경 * 을 클릭합니다.

    설치 디렉토리를 변경하지 않으면 Unified Manager가 기본 설치 디렉토리에 설치됩니다.

11. 다음 * 을 클릭합니다.
12. Shield 설치 준비 완료 마법사에서 * 설치 * 를 클릭합니다.
13. 설치가 완료되면 * Finish * 를 클릭합니다.
14. Windows 시스템에 안티바이러스 소프트웨어가 설치되어 있는 경우 설치가 완료된 후 바이러스 백신 검사에서 다음 경로를 수동으로 제외하십시오.
    - Unified Manager 데이터 디렉토리입니다
    - Unified Manager 설치 디렉토리
    - MySQL 데이터 디렉토리

설치 시 여러 디렉토리가 생성됩니다.

- 설치 디렉토리

  이 디렉토리는 설치 중에 지정한 Unified Manager의 루트 디렉토리입니다. 예: 'C:\Program Files\NetApp\'

- MySQL 데이터 디렉토리

  MySQL 데이터베이스가 저장되는 디렉토리이며 설치 중에 지정한 디렉토리입니다. 예: 'C:\ProgramData\MySQL\MySQLServerData\'

- Java 디렉토리입니다

  OpenJDK가 설치된 디렉토리입니다. 예: 'C:\Program Files\NetApp\JDK\'

- Unified Manager 애플리케이션 데이터 디렉토리(appDataDir)

  이 디렉터리는 응용 프로그램에서 생성한 모든 데이터가 저장되는 디렉터리입니다. 여기에는 로그, 지원 번들, 백업 및 기타 모든 추가 데이터가 포함됩니다. 예: 'C:\ProgramData\NetApp\OnCommandAppData\'

웹 UI에 액세스하여 에 설명된 대로 Unified Manager의 초기 설정을 수행할 수 있습니다 "Active IQ Unified Manager 구성".

Unified Manager의 자동 설치 수행

명령줄 인터페이스를 사용하여 사용자 개입 없이 Unified Manager를 설치할 수 있습니다. 키 값 쌍의 매개 변수를 전달하여 무인 설치를 완료할 수 있습니다.

단계

1. 기본 로컬 관리자 계정을 사용하여 Windows 명령줄 인터페이스에 로그인합니다.
2. Unified Manager를 설치할 위치로 이동하고 다음 옵션 중 하나를 선택합니다.

옵션을 선택합니다	지침
타사 패키지가 사전 설치된 경우	'ActiveIQUnifiedManager-x.y.exe /V" mysql_password=mysql_password INSTALLDIR=\"설치 디렉토리\" mysql_data_DIR=\"mysql 데이터 디렉토리\" maintenance_password=maintenance_password maintenance_username=maintenance_username/qn/l * v CompletePathForLogFile" • 예: * ' ActiveIQUnifiedManager.exe /s/v " mysql_password = netapp21! INSTALLDIR=\"C:\Program Files\NetApp\"MySQL_DATA_DIR=\"C:\ProgramData\MySQL\MySQLServer\" maintenance_password=* maintenance_username=admin/qn/l * v C:\install.log""

옵션을 선택합니다	지침
타사 패키지가 설치되지 않은 경우	'ActiveIQUnifiedManager-x.y.exe /V" mysql_password=mysql_password INSTALLDIR=\"설치 디렉터리\" mysql_data_DIR=\"mysql 데이터 디렉터리\" maintenance_password=maintenance_password maintenance_username=maintenance_username/QR/l * v CompletePathForLogFile" • 예: * ' ActiveIQUnifiedManager.exe /s/v " mysql_password = netapp21! INSTALLDIR=\"C:\Program Files\NetApp\"MySQL_DATA_DIR=\"C:\ProgramData\MySQL\MySQLServer\" maintenance_password=* maintenance_username=admin/QR/l * v C:\install.log""

'/QR' 옵션은 사용자 인터페이스 감소로 자동 모드를 활성화합니다. 기본 사용자 인터페이스가 표시되어 설치 진행률을 보여 줍니다. 입력 메시지가 표시되지 않습니다. JRE, MySQL, 7zip 등의 타사 패키지가 사전 설치되지 않은 경우 '/QR' 옵션을 사용해야 합니다. 타사 패키지가 설치되지 않은 서버에서 '/qn' 옵션을 사용하면 설치가 실패합니다.

'/qn' 옵션은 사용자 인터페이스 없이 자동 모드를 활성화합니다. 설치 중에 사용자 인터페이스 또는 세부 정보가 표시되지 않습니다. 타사 패키지가 설치되지 않은 경우 '/qn' 옵션을 사용하면 안 됩니다.

3. 다음 URL을 사용하여 Unified Manager 웹 사용자 인터페이스에 로그인합니다.

   'https://IP 주소'

JBoss 암호 변경

설치 중에 설정된 인스턴스별 JBoss 암호를 재설정할 수 있습니다. 사이트에 Unified Manager 설치 설정을 재정의하는 데 이 보안 기능이 필요한 경우 암호를 선택적으로 재설정할 수 있습니다. 이 작업은 JBoss가 MySQL에 액세스하는 데 사용하는 암호도 변경합니다.

- 필요한 것 *
- Unified Manager가 설치된 시스템에 대한 Windows 관리자 권한이 있어야 합니다.
- MySQL root 사용자의 암호가 있어야 합니다.
- NetApp에서 제공한 password.bat" 스크립트에 디렉토리에서 액세스할 수 있어야 합니다

  'C:\Program Files\NetApp\Essentials\bin'을 선택합니다.

단계

1. Unified Manager 호스트 시스템에서 admin 사용자로 로그인합니다.

2. Windows 서비스 콘솔을 사용하여 다음 Unified Manager 서비스를 중지합니다.
   - NetApp Active IQ 구입 서비스(Ocie-au)
   - NetApp Active IQ 관리 서버 서비스(Oncommanddsvc)
3. password.bat 스크립트를 실행하여 암호 변경 프로세스를 시작합니다.

   'C:\Program Files\NetApp\Essentials\bin> password.bat resetJBossPassword'를 참조하십시오
4. 메시지가 표시되면 MySQL root 사용자 암호를 입력합니다.
5. 메시지가 표시되면 새 JBoss 사용자 암호를 입력한 다음 확인을 위해 다시 입력합니다.

   암호는 8자에서 16자 사이여야 하며 숫자, 대문자, 소문자 및 다음 특수 문자 중 하나 이상을 포함해야 합니다.

   '!@%^ * -_=[]:<>.?/~+'
6. 스크립트가 완료되면 Windows 서비스 콘솔을 사용하여 Unified Manager 서비스를 시작합니다.
   - NetApp Active IQ 관리 서버 서비스(Oncommanddsvc)
   - NetApp Active IQ 구입 서비스(Ocie-au)
7. 모든 서비스가 시작되면 Unified Manager UI에 로그인할 수 있습니다.

Unified Manager 버전에 지원되는 업그레이드 경로

Active IQ Unified Manager는 각 버전에 대한 특정 업그레이드 경로를 지원합니다.

모든 버전의 Unified Manager에서 이후 버전으로 업그레이드할 수 있는 것은 아닙니다. Unified Manager 업그레이드는 N-2 모델로 제한되어 있으며, 이는 모든 플랫폼의 다음 2개 릴리즈 내에서만 업그레이드할 수 있음을 의미합니다. 예를 들어, Unified Manager 9.12와 9.13에서만 Unified Manager 9.14로 업그레이드할 수 있습니다.

지원되는 버전보다 이전 버전을 실행 중인 경우 Unified Manager 인스턴스를 지원되는 버전 중 하나로 먼저 업그레이드한 다음 현재 버전으로 업그레이드해야 합니다.

예를 들어, 설치된 버전이 Unified Manager 9.9이고 Unified Manager 9.14로 업그레이드하려면 일련의 업그레이드를 수행해야 합니다.

샘플 업그레이드 경로**:**

1. 업그레이드 9.9 → 9.11
2. 업그레이드 9.11 → 9.13
3. 업그레이드 9.13 → 9.14

업그레이드 경로 매트릭스에 대한 자세한 내용은 다음을 참조하십시오 "기술 자료(KB) 문서".

Unified Manager 업그레이드

Windows 플랫폼에서 설치 파일을 다운로드하여 실행하면 Unified Manager 9.12 또는 9.13을 9.14로 업그레이드할 수 있습니다.

- 필요한 것 *

- Unified Manager를 업그레이드하는 시스템은 시스템 및 소프트웨어 요구사항을 충족해야 합니다.

  을 참조하십시오 "하드웨어 시스템 요구 사항".

  을 참조하십시오 "Windows 소프트웨어 및 설치 요구 사항".

  Unified Manager 9.5부터 OpenJDK는 설치 패키지에 제공되어 자동으로 설치됩니다. Oracle Java는 Unified Manager 9.5부터 지원되지 않습니다.

  업그레이드를 시작하기 전에 시스템에 Microsoft .NET 4.5.2 이상이 설치되어 있는지 확인하십시오.

- MySQL Community Edition은 Unified Manager 업그레이드 중에 자동으로 업그레이드됩니다. 시스템에 설치된 MySQL 버전이 8.0.34 이전인 경우 Unified Manager 업그레이드 프로세스에서 MySQL을 8.0.34로 자동 업그레이드합니다. MySQL 이전 버전의 독립 실행형 업그레이드를 8.0.34로 실행하면 안 됩니다.
- Windows 관리자 권한이 있어야 합니다. 사용자 이름이 느낌표 ""!""로 시작하지 않는지 확인합니다. 설치를 실행 중인 사용자의 이름이 ""!"(으로)로 시작하는 경우 Unified Manager 설치가 실패할 수 있습니다.
- NetApp Support 사이트에 로그인하려면 유효한 자격 증명이 있어야 합니다.
- 업그레이드 중에 문제가 발생할 경우 데이터 손실을 방지하려면 Unified Manager 시스템의 백업을 생성해야 합니다.
- 업그레이드를 수행할 수 있는 충분한 디스크 공간이 있어야 합니다.

  설치 드라이브의 사용 가능한 공간은 데이터 디렉토리의 크기보다 2.5GB가 커야 합니다. 사용 가능한 공간이 충분하지 않은 경우 업그레이드를 중지하고 추가할 공간의 양을 나타내는 오류 메시지를 표시합니다.

- 업그레이드하는 동안 성능 데이터를 13개월 동안 유지하기 위한 이전 기본 설정을 유지할지 아니면 6개월로 변경할지 묻는 메시지가 표시될 수 있습니다. 확인 시 6개월 후의 성능 기록 데이터가 삭제됩니다.
- 업그레이드하기 전에 _<InstallDir>\JDK_and_MySQL Data Directory_에서 열려 있는 파일이나 폴더를 닫아야 합니다.
- Windows 시스템에 안티바이러스 소프트웨어가 설치되어 있는 경우 Unified Manager 업그레이드가 실패할 수 있습니다. Unified Manager를 업그레이드하기 전에 시스템에서 모든 바이러스 검사 소프트웨어를 비활성화해야 합니다.

업그레이드 프로세스 중에는 Unified Manager를 사용할 수 없습니다. Unified Manager를 업그레이드하기 전에 실행 중인 작업을 완료해야 합니다.

Unified Manager가 OnCommand Workflow Automation 인스턴스와 페어링되어 있고 두 제품 모두에 사용할 수 있는 새로운 소프트웨어 버전이 있는 경우 두 제품의 연결을 끊고 업그레이드를 수행한 후 새 Workflow Automation 연결을 설정해야 합니다. 제품 중 하나로 업그레이드하는 경우, 업그레이드 후에 Workflow Automation에 로그인하여 Unified Manager에서 데이터를 아직 취득하고 있는지 확인해야 합니다.

단계

1. NetApp Support 사이트에 로그인하고 Unified Manager의 다운로드 페이지로 이동합니다.

   "NetApp Support 사이트".

2. Unified Manager의 필수 버전을 선택하고 최종 사용자 라이센스 계약(EULA)에 동의합니다.
3. Unified Manager Windows 설치 파일을 Windows 시스템의 대상 디렉토리에 다운로드합니다.

4. 마우스 오른쪽 단추를 클릭하고 Unified Manager 설치 관리자 실행 파일(.exe) 파일을 관리자로 실행합니다.

   Unified Manager에 다음 메시지가 표시됩니다.

   ```
   This setup will perform an upgrade of Unified Manager. Do you want to
   continue?
   ```

5. 예 * 를 클릭한 후 * 다음 * 을 클릭합니다.
6. 설치 중에 설정된 MySQL8 루트 암호를 입력하고 * 다음 * 을 클릭합니다.
7. 지원되는 웹 브라우저의 새 창에서 웹 UI를 시작하고 로그인하여 Unified Manager의 업그레이드된 버전을 사용하십시오.
8. Windows 시스템에 안티바이러스 소프트웨어가 설치되어 있는 경우 업그레이드가 완료된 후 바이러스 백신 검사에서 다음 경로를 수동으로 제외해야 합니다.
   - Unified Manager 데이터 디렉토리입니다
   - Unified Manager 설치 디렉토리
   - MySQL 데이터 디렉토리

Unified Manager의 자동 업그레이드를 수행하려면 'ActiveIQUnifiedManager-<version\>.exe/s/v "MySQL_PASSWORD=<PASSWORD>/qn/l * v <system_drive>:\install.log" 명령을 실행합니다

타사 제품 업그레이드

Windows 시스템에 설치된 경우 Unified Manager에서 JRE와 같은 타사 제품을 업그레이드할 수 있습니다.

이러한 타사 제품을 개발하는 회사는 정기적으로 보안 취약점을 보고합니다. 사용자 일정에 따라 이 소프트웨어의 새 버전으로 업그레이드할 수 있습니다.

OpenJDK 업그레이드 중

Unified Manager가 설치된 Windows 서버에서 최신 버전의 OpenJDK로 업그레이드하여 보안 취약점에 대한 수정 사항을 확인할 수 있습니다.

- 필요한 것 *

Unified Manager가 설치된 시스템에 대한 Windows 관리자 권한이 있어야 합니다.

릴리스 제품군 내에서 OpenJDK 릴리스를 업데이트할 수 있습니다. 예를 들어 OpenJDK 11.0.16에서 OpenJDK 11.0.18로 업그레이드할 수 있지만 OpenJDK 11에서 OpenJDK 12로 직접 업데이트할 수는 없습니다.

단계

1. Unified Manager 호스트 시스템에서 admin 사용자로 로그인합니다.
2. OpenJDK 사이트에서 대상 시스템으로 적절한 버전의 OpenJDK(64비트)를 다운로드합니다.

   예를 들어, 다운로드 를 선택합니다 `jdk-11.0.18_windows-x64_bin.zip from`

https://www.oracle.com/in/java/technologies/javase/jdk11-archive-downloads.html.

> 파일을 다운로드하려면 Oracle 계정이 필요합니다. Oracle 계정이 없는 경우 로 이동합니다 "Oracle 계정 로그인" 페이지를 만듭니다.

3. Windows 서비스 콘솔을 사용하여 다음 Unified Manager 서비스를 중지합니다.
   - NetApp Active IQ 구입 서비스(Ocie-au)
   - NetApp Active IQ 관리 서버 서비스(Oncommanddsvc)
4. zip 파일을 확장합니다.
5. 결과로 생성된 디렉토리와 파일을 복사합니다 `jdk` 디렉터리(예: `jdk-11.0.18` Java가 설치된 위치로 이동합니다. 예: `C:\Program Files\NetApp\JDK\`
6. Windows 서비스 콘솔을 사용하여 Unified Manager 서비스를 시작합니다.
   - NetApp Active IQ 관리 서버 서비스(Oncommanddsvc)
   - NetApp Active IQ 구입 서비스(Ocie-au)

Unified Manager를 다시 시작하는 중입니다

구성을 변경한 후 Unified Manager를 다시 시작해야 할 수 있습니다.

- 필요한 것 *

Windows 관리자 권한이 있어야 합니다.

단계

1. 기본 로컬 관리자 계정을 사용하여 Windows에 로그인합니다.
2. Unified Manager 서비스 중지:

시작...	다음 순서대로 서비스를 중지합니다.
명령줄	a. '스탑 치아우' b. '스탑 온commanddsvc'
Microsoft 서비스 관리자	a. NetApp Active IQ 구입 서비스(Ocie-au) b. NetApp Active IQ 관리 서버 서비스(Oncommanddsvc)

3. Unified Manager 서비스 시작:

시작...	다음 순서로 서비스를 시작합니다.
명령줄	a. 'sc start Oncommanddsvc'를 선택합니다 b. 'sc start socie-au'를 선택합니다

시작...	다음 순서로 서비스를 시작합니다.
Microsoft 서비스 관리자	a. NetApp Active IQ 관리 서버 서비스(Oncommanddsvc) b. NetApp Active IQ 구입 서비스(Ocie-au)

Unified Manager 제거 중

프로그램 및 기능 마법사를 사용하거나 명령줄 인터페이스에서 자동 제거를 수행하여 Unified Manager를 제거할 수 있습니다.

- 필요한 것 *
- Windows 관리자 권한이 있어야 합니다.
- 소프트웨어를 제거하기 전에 모든 클러스터(데이터 소스)를 Unified Manager 서버에서 제거해야 합니다.
- MySQL 포트 3306을 허용하거나 차단할 수 있도록 만들어진 방화벽 규칙을 수동으로 삭제해야 합니다. 방화벽 규칙은 자동으로 삭제되지 않습니다.

단계

1. 다음 옵션 중 하나를 선택하여 Unified Manager를 제거합니다.
   - 프로그램 및 기능 * 마법사에서 Unified Manager를 제거하는 경우 다음 단계를 수행하십시오.
     i. 제어판 * > * 프로그램 및 기능 * 으로 이동합니다.
     ii. Active IQ Unified Manager 를 선택하고 * 제거 * 를 클릭합니다.
   - 명령줄에서 Unified Manager를 제거하는 경우 다음 단계를 수행하십시오.
     i. 관리자 권한을 사용하여 Windows 명령줄에 로그인합니다.
     ii. Active IQ Unified Manager 디렉토리로 이동하여 다음 명령을 실행합니다.

     'msiexec /x{A78760DB-7EC0-4305-97dB-E4A89CDFF4E1} /qn/l * v%systemdrive%\UmUninstall.log'

     서버에서 UAC(사용자 계정 컨트롤)가 활성화되어 있고 도메인 사용자로 로그인한 경우 명령줄 제거 방법을 사용해야 합니다.

   Unified Manager가 시스템에서 제거되었습니다.
2. Unified Manager 설치 제거 중에 제거되지 않은 다음 타사 패키지 및 데이터를 제거합니다.
   - 타사 패키지: JRE, MySQL, Microsoft Visual C 및 #43;+ 2015 재배포 가능 파일, Python, 7zip
   - Unified Manager에서 생성된 MySQL 애플리케이션 데이터
   - 응용 프로그램 로그 및 응용 프로그램 데이터 디렉터리의 내용

구성 및 관리 작업을 수행합니다

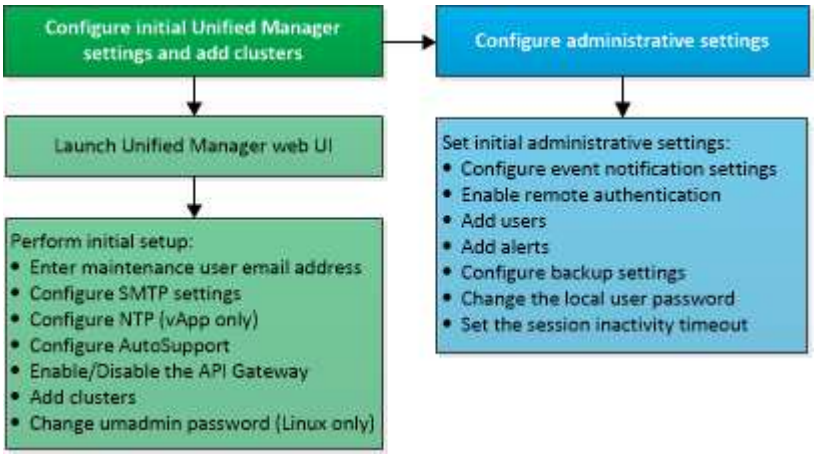
Active IQ Unified Manager 구성

Active IQ Unified Manager(이전의 OnCommand Unified Manager)을 설치한 후 웹 UI에 액세스하려면 초기 설정(첫 번째 환경 마법사라고도 함)을 완료해야 합니다. 그런 다음 클러스터 추가, 원격 인증 구성, 사용자 추가 및 알림 추가와 같은 추가 구성 작업을 수행할 수 있습니다.

이 설명서에 설명된 일부 절차는 Unified Manager 인스턴스의 초기 설정을 완료하는 데 필요합니다. 다른 절차는 새 인스턴스에 설정하는 데 유용하거나 ONTAP 시스템의 정기적인 모니터링을 시작하기 전에 알아야 할 구성 설정을 권장합니다.

구성 시퀀스의 개요

구성 워크플로우에서 Unified Manager를 사용하기 전에 수행해야 하는 작업에 대해 설명합니다.



Unified Manager 웹 UI에 액세스

Unified Manager를 설치한 후에는 웹 UI에 액세스하여 Unified Manager를 설정하여 ONTAP 시스템 모니터링을 시작할 수 있습니다.

- 필요한 것 *
- 웹 UI에 처음 액세스하는 경우 유지 관리 사용자(또는 Linux 설치의 경우 umadmin 사용자)로 로그인해야 합니다.
- 사용자가 FQDN(정규화된 도메인 이름) 또는 IP 주소를 사용하는 대신 짧은 이름을 사용하여 Unified Manager에 액세스하도록 허용하려면 네트워크 구성에서 이 짧은 이름을 유효한 FQDN으로 해석해야 합니다.
- 서버에서 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에서 인증서를 신뢰할 수 없다는 경고를 표시할 수 있습니다. 액세스를 계속할 위험을 확인하거나 서버 인증을 위해 CA(인증 기관) 서명 디지털 인증서를 설치할 수 있습니다.

단계

1. 설치 마지막에 표시되는 URL을 사용하여 브라우저에서 Unified Manager 웹 UI를 시작합니다. URL은 Unified Manager 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다.

   링크는 다음과 같은 형식으로 되어 있습니다: 'https://URL`.

2. 유지보수 사용자 자격 증명을 사용하여 Unified Manager 웹 UI에 로그인합니다.

한 시간 내에 웹 UI에 세 번 연속해서 로그인을 실패하면 시스템이 잠기므로 시스템 관리자에게 문의해야 합니다. 이 옵션은 로컬 사용자에게만 적용됩니다.

Unified Manager 웹 UI의 초기 설정 수행

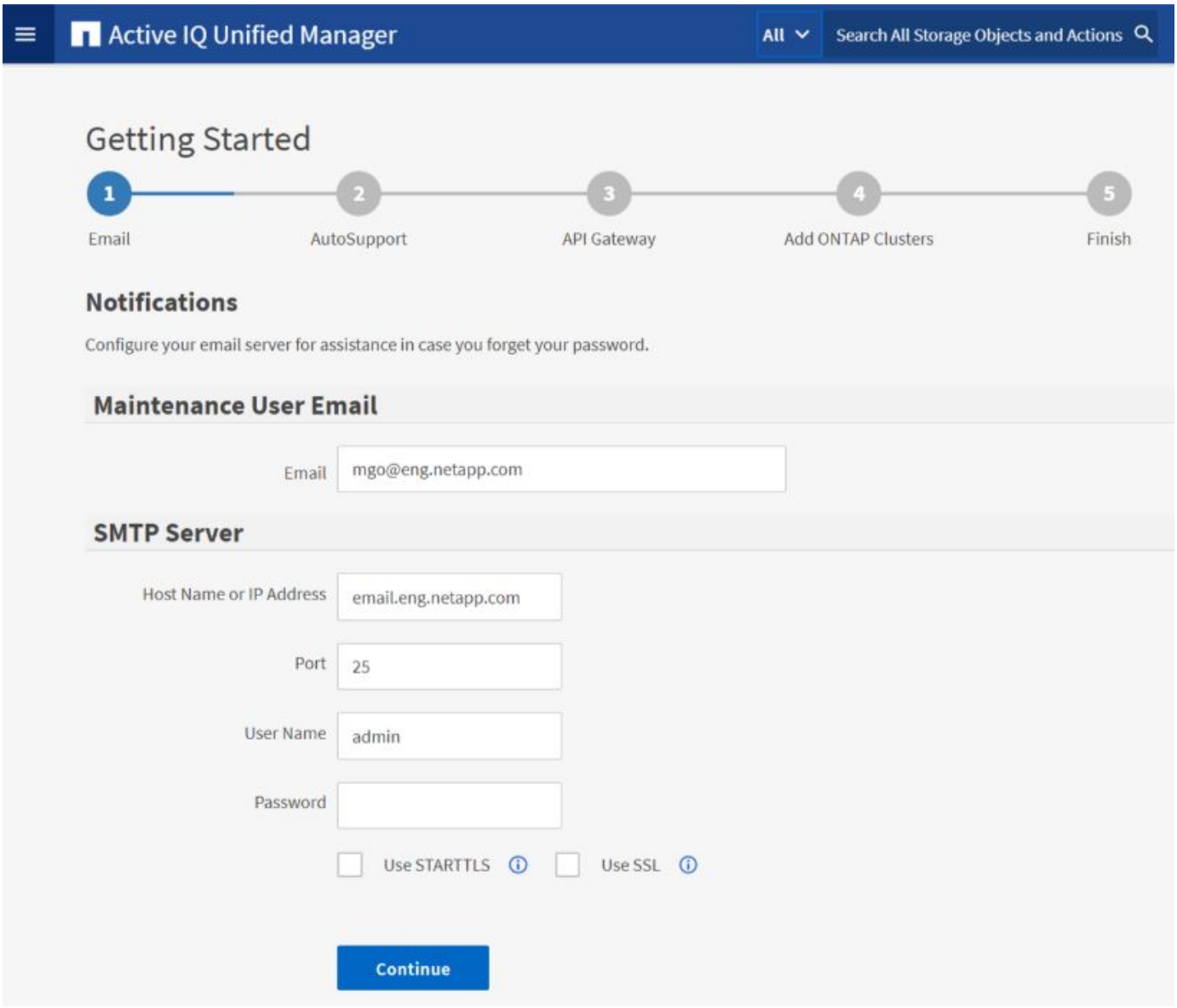
Unified Manager를 사용하려면 먼저 NTP 서버, 유지보수 사용자 이메일 주소, SMTP 서버 호스트 및 ONTAP 클러스터 추가를 포함한 초기 설정 옵션을 구성해야 합니다.

- 필요한 것 *

다음 작업을 수행해야 합니다.

- 설치 후 제공된 URL을 사용하여 Unified Manager 웹 UI를 실행했습니다
- 설치 중에 생성된 유지보수 사용자 이름 및 암호(Linux 설치의 경우 umadmin 사용자)를 사용하여 로그인했습니다

Active IQ Unified Manager 시작 페이지는 웹 UI에 처음 액세스할 때만 나타납니다. 아래 페이지는 VMware 설치 페이지입니다.



나중에 이 옵션 중 하나를 변경하려면 Unified Manager의 왼쪽 탐색 창에서 일반 옵션에서 원하는 옵션을 선택합니다. NTP 설정은 VMware 설치에만 해당되며 나중에 Unified Manager 유지보수 콘솔을 사용하여 변경할 수 있습니다.

단계

1. Active IQ Unified Manager 초기 설정 페이지에서 유지보수 사용자 e-메일 주소, SMTP 서버 호스트 이름 및 추가 SMTP 옵션, NTP 서버(VMware 설치만 해당)를 입력합니다. 그런 다음 * 계속 * 을 클릭합니다.

   STARTTLS* 또는 * SSL* 사용 옵션을 선택한 경우 * 계속 * 단추를 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 수락하여 웹 UI의 초기 설정 설정을 계속합니다.

2. AutoSupport 페이지에서 * 동의 및 계속 * 을 클릭하여 AutoSupport 메시지를 Unified Manager에서 NetAppActive IQ로 보낼 수 있습니다.

   AutoSupport 콘텐츠를 전송하기 위해 인터넷 액세스를 제공할 프록시를 지정해야 하거나 AutoSupport를 비활성화하려면 웹 UI에서 * 일반 * > * AutoSupport * 옵션을 사용하십시오.

3. Red Hat 및 CentOS 시스템에서 umadmin 사용자 암호를 기본 ""admin" 문자열에서 개인 문자열로 변경합니다.

4. API 게이트웨이 설정 페이지에서 ONTAP REST API를 사용하여 모니터링하려는 ONTAP 클러스터를 Unified Manager에서 관리할 수 있도록 하는 API 게이트웨이 기능을 사용할지 여부를 선택합니다. 그런 다음 * 계속 * 을 클릭합니다.

   웹 UI의 나중에 * 일반 * > * 기능 설정 * > * API 게이트웨이 * 에서 이 설정을 활성화하거나 비활성화할 수 있습니다. API에 대한 자세한 내용은 를 참조하십시오 "Active IQ Unified Manager REST API 시작하기".

5. Unified Manager에서 관리할 클러스터를 추가하고 * 다음 * 을 클릭합니다. 관리하려는 각 클러스터마다 사용자 이름 및 암호 자격 증명과 함께 호스트 이름 또는 클러스터 관리 IP 주소(IPv4 또는 IPv6)가 있어야 합니다. 사용자는 ""admin" 역할을 가지고 있어야 합니다.

   이 단계는 선택 사항입니다. 웹 UI의 나중에 * 스토리지 관리 * > * 클러스터 설정 * 에서 클러스터를 추가할 수 있습니다.

6. 요약 페이지에서 모든 설정이 올바른지 확인하고 * 마침 * 을 클릭합니다.

시작하기 페이지가 닫히고 Unified Manager 대시보드 페이지가 표시됩니다.

클러스터 추가

클러스터를 모니터링할 수 있도록 Active IQ Unified Manager에 클러스터를 추가할 수 있습니다. 여기에는 발생할 수 있는 문제를 찾아 해결할 수 있도록 클러스터의 상태, 용량, 성능, 구성 등과 같은 클러스터 정보를 가져오는 기능도 포함됩니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 다음 정보가 있어야 합니다.
  - Unified Manager는 사내 ONTAP 클러스터, ONTAP Select, Cloud Volumes ONTAP를 지원합니다.
  - 호스트 이름 또는 클러스터 관리 IP 주소입니다

    호스트 이름은 Unified Manager가 클러스터에 연결하는 데 사용하는 FQDN 또는 짧은 이름입니다. 호스트 이름이 클러스터 관리 IP 주소로 확인되어야 합니다.

  클러스터 관리 IP 주소는 관리 스토리지 가상 시스템(SVM)의 클러스터 관리 LIF여야 합니다. 노드 관리 LIF를 사용하면 작업이 실패합니다.

  - 클러스터에서 ONTAP 버전 9.1 소프트웨어 이상을 실행해야 합니다.
  - ONTAP 관리자 사용자 이름 및 암호

    이 계정에는 응용 프로그램 액세스 권한이 *ontapi*, *console* 및 _http_로 설정된 _admin_역할이 있어야 합니다.

  - HTTPS 프로토콜을 사용하여 클러스터에 연결할 포트 번호(일반적으로 포트 443)
  - 필요한 인증서가 있습니다.
- SSL(HTTPS) 인증서 *: 이 인증서는 Unified Manager에서 소유합니다. Unified Manager를 새로 설치하면 자체 서명된 기본 SSL(HTTPS) 인증서가 생성됩니다. 보안을 강화하기 위해 CA 서명 인증서로 업그레이드하는 것이 좋습니다. 서버 인증서가 만료되면 해당 인증서를 다시 생성하고 Unified Manager를 다시 시작하여 새 인증서를 통합하는 서비스를 수행해야 합니다. SSL 인증서 재생성에 대한 자세한 내용은 을 참조하십시오 "HTTPS 보안 인증서를 생성하는 중입니다".

- EMS 인증서 *: 이 인증서는 Unified Manager에서 소유합니다. ONTAP로부터 수신한 EMS 알림에 대한 인증 중에 사용된다.
- 상호 TLS 통신을 위한 인증서 *: Unified Manager와 ONTAP 간의 상호 TLS 통신 중에 사용됩니다. 인증서 기반 인증은 ONTAP 버전에 따라 클러스터에 대해 설정됩니다. ONTAP 버전을 실행하는 클러스터가 9.5보다 낮은 경우 인증서 기반 인증이 활성화되지 않습니다.

  이전 버전의 Unified Manager를 업데이트하는 경우 클러스터에 대해 인증서 기반 인증이 자동으로 활성화되지 않습니다. 그러나 클러스터 세부 정보를 수정 및 저장하여 이 기능을 사용하도록 설정할 수 있습니다. 인증서가 만료되면 인증서를 다시 생성하여 새 인증서를 통합해야 합니다. 인증서 보기 및 재생에 대한 자세한 내용은 을 참조하십시오 "클러스터 편집".

  ◦ 웹 UI에서 클러스터를 추가할 수 있으며 인증서 기반 인증이 자동으로 활성화됩니다.

  ◦ Unified Manager CLI를 통해 클러스터를 추가할 수 있으며, 인증서 기반 인증은 기본적으로 사용되지 않습니다. Unified Manager CLI를 사용하여 클러스터를 추가하는 경우 Unified Manager UI를 사용하여 클러스터를 편집해야 합니다. 확인할 수 있습니다 "지원되는 Unified Manager CLI 명령" 을 사용하여 Unified Manager CLI를 사용하여 클러스터를 추가합니다.

  ◦ 클러스터에 대해 인증서 기반 인증을 사용하고 서버에서 Unified Manager 백업을 수행한 후 호스트 이름 또는 IP 주소가 변경된 다른 Unified Manager 서버로 복원하면 클러스터 모니터링이 실패할 수 있습니다. 이 문제를 방지하려면 클러스터 세부 정보를 편집하고 저장합니다. 클러스터 세부 정보 편집에 대한 자세한 내용은 을 참조하십시오 "클러스터 편집".

- 클러스터 인증서 *: 이 인증서는 ONTAP에서 소유합니다. 만료된 인증서가 있는 클러스터는 Unified Manager에 추가할 수 없으며, 인증서가 이미 만료된 경우 클러스터를 추가하기 전에 다시 생성해야 합니다. 인증서 생성에 대한 자세한 내용은 기술 자료(KB) 문서를 참조하십시오 "System Manager 사용자 인터페이스에서 ONTAP 자체 서명된 인증서를 갱신하는 방법".
- Unified Manager 서버에 적절한 공간이 있어야 합니다. 데이터베이스 디렉토리의 공간이 이미 90% 이상 사용된 경우 서버에 클러스터를 추가할 수 없습니다.

MetroCluster 구성의 경우 로컬 클러스터와 원격 클러스터를 모두 추가해야 하며 클러스터가 올바르게 구성되어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.
2. 클러스터 설정 페이지에서 * 추가 * 를 클릭합니다.
3. 클러스터 추가 대화 상자에서 클러스터의 호스트 이름 또는 IP 주소, 사용자 이름, 암호 및 포트 번호와 같은 필수 값을 지정합니다.

   클러스터 관리 IP 주소를 IPv6에서 IPv4로, 또는 IPv4에서 IPv6로 변경할 수 있습니다. 새 IP 주소는 다음 모니터링 주기가 완료된 후 클러스터 그리드 및 클러스터 구성 페이지에 반영됩니다.

4. 제출 * 을 클릭합니다.
5. 호스트 인증 대화 상자에서 * 인증서 보기 * 를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
6. 예 * 를 클릭합니다.

   클러스터 세부 정보를 저장한 후에는 클러스터의 상호 TLS 통신에 대한 인증서를 볼 수 있습니다.

   인증서 기반 인증이 활성화되지 않은 경우 Unified Manager는 클러스터가 처음에 추가될 때만 인증서를 확인합니다. Unified Manager에서는 ONTAP에 대한 각 API 호출의 인증서를 확인하지 않습니다.

새 클러스터의 모든 객체가 검색된 후 Unified Manager가 이전 15일 동안 기간별 성능 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능은 클러스터를 추가한 직후 2주 이상의 클러스터 성능 정보를 제공합니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.

15일간의 성능 데이터 수집은 CPU를 많이 사용하므로 데이터 연속성 수집 폴이 너무 많은 클러스터에서 동시에 실행되지 않도록 새 클러스터를 추가하는 시차를 두는 것이 좋습니다. 또한, 데이터 연속성 수집 기간 동안 Unified Manager를 다시 시작하면 수집이 중단되고 성능 차트의 누락된 시간 간격이 표시됩니다.

클러스터를 추가할 수 없다는 오류 메시지가 표시되면 두 시스템의 시계가 동기화되지 않았는지, Unified Manager HTTPS 인증서 시작 날짜가 클러스터의 날짜 이후인지 확인합니다. NTP 또는 이와 유사한 서비스를 사용하여 시계가 동기화되었는지 확인해야 합니다.

- 관련 정보 *

"서명되고 반환된 HTTPS 인증서를 설치하는 중입니다"

경고 알림을 보내도록 **Unified Manager** 구성

Unified Manager에서 사용자 환경의 이벤트에 대한 알림을 보내도록 구성할 수 있습니다. 알림을 보내려면 먼저 몇 가지 다른 Unified Manager 옵션을 구성해야 합니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

Unified Manager를 구축하고 초기 구성을 완료한 후에는 이벤트 수신 시 알림을 트리거하고 알림 e-메일 또는 SNMP 트랩을 생성하도록 환경을 구성하는 것이 좋습니다.

단계

1. "이벤트 알림 설정을 구성합니다".

   사용자 환경에서 특정 이벤트가 발생할 때 알림 알림을 보내려면 SMTP 서버를 구성하고 알림 알림을 보낼 이메일 주소를 제공해야 합니다. SNMP 트랩을 사용하려면 해당 옵션을 선택하고 필요한 정보를 제공할 수 있습니다.

2. "원격 인증을 사용합니다".

   원격 LDAP 또는 Active Directory 사용자가 Unified Manager 인스턴스에 액세스하여 경고 알림을 받으려면 원격 인증을 설정해야 합니다.

3. "인증 서버를 추가합니다".

   인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있도록 인증 서버를 추가할 수 있습니다.

4. "사용자 추가".

   여러 가지 유형의 로컬 또는 원격 사용자를 추가하고 특정 역할을 할당할 수 있습니다. 알림을 생성할 때 사용자에게 경고 알림을 보내도록 할당합니다.

5. "알림을 추가합니다".

알림을 보낼 e-메일 주소를 추가하고 알림을 받을 사용자를 추가했으며 네트워크 설정을 구성했으며 사용자 환경에 필요한 SMTP 및 SNMP 옵션을 구성한 후 알림을 할당할 수 있습니다.

이벤트 알림 설정을 구성하는 중입니다

이벤트가 생성되거나 이벤트가 사용자에게 할당될 때 알림을 보내도록 Unified Manager를 구성할 수 있습니다. 알림을 보내는 데 사용되는 SMTP 서버를 구성할 수 있으며, 다양한 알림 메커니즘을 설정할 수 있습니다. 예를 들어, 알림 알림을 e-메일 또는 SNMP 트랩으로 보낼 수 있습니다.

- 필요한 것 *

다음 정보가 있어야 합니다.

- 알림 메시지가 전송되는 이메일 주소입니다

  보낸 알림 알림의 ""보낸 사람" 필드에 이메일 주소가 나타납니다. 어떤 이유로든 이메일을 전달할 수 없는 경우 이 이메일 주소는 배달 불가능한 메일의 받는 사람으로도 사용됩니다.

- SMTP 서버 호스트 이름 및 서버에 액세스하기 위한 사용자 이름 및 암호
- SNMP 버전, 아웃바운드 트랩 포트, 커뮤니티 및 기타 필수 SNMP 구성 값과 함께 SNMP 트랩을 수신할 트랩 대상 호스트의 호스트 이름 또는 IP 주소입니다

  여러 트랩 대상을 지정하려면 각 호스트를 쉼표로 구분합니다. 이 경우 버전 및 아웃바운드 트랩 포트와 같은 다른 모든 SNMP 설정은 목록의 모든 호스트에 대해 동일해야 합니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 알림 * 을 클릭합니다.
2. 알림 페이지에서 적절한 설정을 구성합니다.
   - 참고: *
     - 보낸 사람 주소에 "ActiveIQUnifiedManager@localhost.com" 주소가 미리 입력된 경우, 모든 이메일 알림이 성공적으로 전송되도록 실제 작업 이메일 주소로 변경해야 합니다.
     - SMTP 서버의 호스트 이름을 확인할 수 없는 경우 호스트 이름 대신 SMTP 서버의 IP 주소(IPv4 또는 IPv6)를 지정할 수 있습니다.
3. 저장 * 을 클릭합니다.
4. STARTTLS* 또는 * SSL* 사용 옵션을 선택한 경우 * 저장 * 단추를 클릭하면 인증서 페이지가 표시됩니다. 인증서 세부 정보를 확인하고 인증서를 수락하여 알림 설정을 저장합니다.

   인증서 세부 정보 보기 * 단추를 클릭하여 인증서 세부 정보를 볼 수 있습니다. 기존 인증서가 만료된 경우 * STARTTLS * 또는 * SSL * 사용 상자의 선택을 취소하고 알림 설정을 저장한 다음 * STARTTLS * 또는 * SSL * 사용 상자를 다시 선택하여 새 인증서를 봅니다.

Unified Manager 서버가 인증 서버와 통신할 수 있도록 원격 인증을 설정할 수 있습니다. 인증 서버 사용자는 Unified Manager 그래픽 인터페이스에 액세스하여 스토리지 객체와 데이터를 관리할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

Unified Manager 서버는 인증 서버에 직접 연결되어 있어야 합니다. SSSD(System Security Services Daemon) 또는 NSLCD(Name Service LDAP Caching Daemon)와 같은 로컬 LDAP 클라이언트를 비활성화해야 합니다.

Open LDAP 또는 Active Directory를 사용하여 원격 인증을 설정할 수 있습니다. 원격 인증이 비활성화되어 있으면 원격 사용자가 Unified Manager에 액세스할 수 없습니다.

원격 인증은 LDAP 및 LDAPS(Secure LDAP)를 통해 지원됩니다. Unified Manager에서는 비보안 통신의 기본 포트로 389를 사용하고 보안 통신의 기본 포트는 636을 사용합니다.

사용자를 인증하는 데 사용되는 인증서는 X.509 형식을 따라야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 원격 인증 활성화… * 확인란을 선택합니다.
3. 인증 서비스 필드에서 서비스 유형을 선택하고 인증 서비스를 구성합니다.

인증 유형...	다음 정보를 입력합니다...
Active Directory를 클릭합니다	• 인증 서버 관리자 이름은 다음 형식 중 하나입니다. ◦ domainname\username’입니다 ◦ 'username@domainname’입니다 ◦ '고유 이름 바인딩'(적절한 LDAP 표기법 사용) • 관리자 암호입니다 • 기본 고유 이름(적절한 LDAP 표기법 사용)
LDAP를 엽니다	• 적절한 LDAP 표시법으로 고유 이름 바인딩 • 암호를 바인딩합니다 • 기본 고유 이름입니다

Active Directory 사용자의 인증에 오랜 시간이 걸리거나 시간이 걸리는 경우 인증 서버가 응답하는 데 시간이 오래 걸릴 수 있습니다. Unified Manager에서 중첩된 그룹에 대한 지원을 사용하지 않도록 설정하면 인증 시간이 줄어들 수 있습니다.

인증 서버에 대해 보안 연결 사용 옵션을 선택하면 Unified Manager는 SSL(Secure Sockets Layer) 프로토콜을

사용하여 인증 서버와 통신합니다.

4. * 선택 사항: * 인증 서버를 추가하고 인증을 테스트합니다.
5. 저장 * 을 클릭합니다.

원격 인증에서 중첩 그룹을 해제합니다

원격 인증이 활성화된 경우 그룹 구성원이 아닌 개별 사용자만 Unified Manager에 원격으로 인증할 수 있도록 중첩된 그룹 인증을 비활성화할 수 있습니다. Active Directory 인증 응답 시간을 향상시키려면 중첩된 그룹을 사용하지 않도록 설정할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 역할이 있어야 합니다.
- 중첩된 그룹을 사용하지 않도록 설정하는 것은 Active Directory를 사용하는 경우에만 적용됩니다.

Unified Manager에서 중첩된 그룹에 대한 지원을 사용하지 않도록 설정하면 인증 시간이 줄어들 수 있습니다. 중첩된 그룹 지원이 비활성화되어 있고 원격 그룹이 Unified Manager에 추가된 경우, 개별 사용자는 Unified Manager에 인증할 원격 그룹의 구성원이어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 중첩 그룹 조회 사용 안 함 * 에 대한 확인란을 선택합니다.
3. 저장 * 을 클릭합니다.

인증 서비스 설정 중

인증 서비스를 사용하면 Unified Manager에 대한 액세스를 제공하기 전에 인증 서버에서 원격 사용자 또는 원격 그룹을 인증할 수 있습니다. 사전 정의된 인증 서비스(예: Active Directory 또는 OpenLDAP)를 사용하거나 고유한 인증 메커니즘을 구성하여 사용자를 인증할 수 있습니다.

- 필요한 것 *
- 원격 인증을 활성화해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 다음 인증 서비스 중 하나를 선택합니다.

다음을 선택한 경우...	다음을 수행하십시오.
Active Directory를 클릭합니다	a. 관리자 이름과 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com +인 경우 기본 고유 이름은 * cn=ou, dc=domain, dc=com * 입니다.
OpenLDAP를 클릭합니다	a. 바인딩 고유 이름 및 바인딩 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com +인 경우 기본 고유 이름은 * cn=ou, dc=domain, dc=com * 입니다.
기타	a. 바인딩 고유 이름 및 바인딩 암호를 입력합니다. b. 인증 서버의 기본 고유 이름을 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com +인 경우 기본 고유 이름은 * cn=ou, dc=domain, dc=com * 입니다. c. 인증 서버에서 지원하는 LDAP 프로토콜 버전을 지정합니다. d. 사용자 이름, 그룹 구성원 자격, 사용자 그룹 및 구성원 특성을 입력합니다.

인증 서비스를 수정하려면 기존 인증 서버를 삭제한 다음 새 인증 서버를 추가해야 합니다.

3. 저장 * 을 클릭합니다.

인증 서버 추가

인증 서버를 추가하고 관리 서버에서 원격 인증을 설정하여 인증 서버 내의 원격 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다.

- 필요한 것 *
- 다음 정보를 사용할 수 있어야 합니다.
  - 인증 서버의 호스트 이름 또는 IP 주소입니다
  - 인증 서버의 포트 번호입니다
- 관리 서버가 인증 서버의 원격 사용자 또는 그룹을 인증할 수 있도록 원격 인증을 활성화하고 인증 서비스를 구성해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

추가하려는 인증 서버가 동일한 데이터베이스를 사용하는 고가용성(HA) 쌍의 일부인 경우 파트너 인증 서버를 추가할 수도 있습니다. 이렇게 하면 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 보안 연결 사용 * 옵션을 활성화 또는 비활성화합니다.

원하는 작업	다음을 수행하십시오.
활성화	a. 보안 연결 사용 * 옵션을 선택합니다. b. Authentication Servers 영역에서 * Add * 를 클릭합니다. c. Add Authentication Server 대화 상자에서 서버의 인증 이름 또는 IP 주소(IPv4 또는 IPv6)를 입력합니다. d. 호스트 권한 부여 대화 상자에서 인증서 보기를 클릭합니다. e. 인증서 보기 대화 상자에서 인증서 정보를 확인한 다음 * 닫기 * 를 클릭합니다. f. 호스트 권한 부여 대화 상자에서 * 예 * 를 클릭합니다. 보안 연결 인증 사용 * 옵션을 활성화하면 Unified Manager가 인증 서버와 통신하고 인증서를 표시합니다. Unified Manager는 보안 통신을 위한 기본 포트로 636을 사용하고 비보안 통신을 위한 포트 번호 389를 사용합니다.
비활성화합니다	a. 보안 연결 사용 * 옵션의 선택을 취소합니다. b. Authentication Servers 영역에서 * Add * 를 클릭합니다. c. Add Authentication Server 대화 상자에서 서버의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 포트 세부 정보를 지정합니다. d. 추가 * 를 클릭합니다.

추가한 인증 서버가 Servers 영역에 표시됩니다.

3. 테스트 인증을 수행하여 추가한 인증 서버에서 사용자를 인증할 수 있는지 확인합니다.

인증 서버의 구성을 테스트하는 중입니다

관리 서버가 인증 서버와 통신할 수 있는지 확인하기 위해 인증 서버 구성을 검증할 수 있습니다.

인증 서버에서 원격 사용자 또는 원격 그룹을 검색하고 구성된 설정을 사용하여 인증하여 구성을 확인할 수 있습니다.

- 필요한 것 *
- Unified Manager 서버가 원격 사용자 또는 원격 그룹을 인증할 수 있도록 원격 인증을 설정하고 인증 서비스를 구성해야 합니다.
- 관리 서버가 이러한 서버에서 원격 사용자 또는 원격 그룹을 검색하고 인증할 수 있도록 인증 서버를 추가해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

인증 서비스가 Active Directory로 설정되어 있고 인증 서버의 기본 그룹에 속하는 원격 사용자의 인증을 확인하는 경우 기본 그룹에 대한 정보가 인증 결과에 표시되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 인증 테스트 * 를 클릭합니다.
3. 사용자 테스트 대화 상자에서 원격 사용자의 사용자 이름 및 암호 또는 원격 그룹의 사용자 이름을 지정한 다음 * 테스트 * 를 클릭합니다.

   원격 그룹을 인증하는 경우 암호를 입력하지 않아야 합니다.

알림 추가

특정 이벤트가 생성될 때 알림을 표시하도록 알림을 구성할 수 있습니다. 단일 리소스, 리소스 그룹 또는 특정 심각도 유형의 이벤트에 대한 알림을 구성할 수 있습니다. 알림을 받을 빈도를 지정하고 스크립트를 알림에 연결할 수 있습니다.

- 필요한 것 *
- Active IQ Unified Manager 서버가 이러한 설정을 사용하여 이벤트가 생성될 때 사용자에게 알림을 보낼 수 있도록 하려면 사용자 e-메일 주소, SMTP 서버 및 SNMP 트랩 호스트와 같은 알림 설정을 구성해야 합니다.
- 알림을 트리거할 리소스 및 이벤트와 알림을 보낼 사용자의 사용자 이름 또는 이메일 주소를 알고 있어야 합니다.
- 이벤트를 기반으로 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여기서 설명하는 대로 알림 설정 페이지에서 알림을 생성할 뿐만 아니라 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. 경고 설정 페이지에서 * 추가 * 를 클릭합니다.
3. 경고 추가 대화 상자에서 * 이름 * 을 클릭하고 경고의 이름과 설명을 입력합니다.
4. 리소스 * 를 클릭하고 경고에 포함되거나 제외될 리소스를 선택합니다.

이름 포함 * 필드에서 텍스트 문자열을 지정하여 리소스 그룹을 선택하여 필터를 설정할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 자원 목록에는 필터 규칙과 일치하는 자원만 표시됩니다. 지정하는 텍스트 문자열은 대/소문자를 구분합니다.

자원이 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 제외된 리소스와 관련된 이벤트에 대해서는 알림이 생성되지 않습니다.

5. 이벤트 * 를 클릭하고 알림을 트리거할 이벤트 이름 또는 이벤트 심각도 유형을 기반으로 이벤트를 선택합니다.

   둘 이상의 이벤트를 선택하려면 Ctrl 키를 누른 상태에서 원하는 항목을 선택합니다.

6. Actions * 를 클릭하고 알릴 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신기로 전송할지 여부를 선택한 다음, 경고가 생성될 때 실행할 스크립트를 할당합니다.

   사용자에 대해 지정된 전자 메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 전자 메일 주소가 이전에 선택한 사용자에게 더 이상 매핑되지 않으므로 이름 필드가 비어 있습니다. 또한 사용자 페이지에서 선택한 사용자의 전자 메일 주소를 수정한 경우 선택한 사용자에 대해 수정된 전자 메일 주소가 업데이트되지 않습니다.

   SNMP 트랩을 통해 사용자에게 알리도록 선택할 수도 있습니다.

7. 저장 * 을 클릭합니다.

알림 추가 예

이 예제에서는 다음 요구 사항을 충족하는 알림을 생성하는 방법을 보여 줍니다.

- 알림 이름: 상태 테스트
- 리소스: 이름에 ""abc""가 포함된 모든 볼륨을 포함하며 이름에 ""xyz""가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요한 상태 이벤트를 포함합니다
- 작업: "sample@domain.com", ""테스트"" 스크립트를 포함하며, 사용자는 15분마다 통지를 받아야 합니다

경고 추가 대화 상자에서 다음 단계를 수행합니다.

단계

1. 이름 * 을 클릭하고 * 알림 이름 * 필드에 * 상태 테스트 * 를 입력합니다.
2. 리소스 * 를 클릭하고 포함 탭의 드롭다운 목록에서 * 볼륨 * 을 선택합니다.
   a. 이름이 ""abc""인 볼륨을 표시하려면 * Name Contains * 필드에 * abc * 를 입력합니다.
   b. 를 선택합니다[All Volumes whose name contains 'abc']Available Resources 영역에서 + * 를 선택한 다음 Selected Resources 영역으로 이동합니다.
   c. 제외 * 를 클릭하고 * 이름 포함 * 필드에 * xyz * 를 입력한 다음 * 추가 * 를 클릭합니다.
3. 이벤트 * 를 클릭하고 이벤트 심각도 필드에서 * 긴급 * 을 선택합니다.
4. Matching Events 영역에서 * All Critical Events * 를 선택하고 Selected Events 영역으로 이동합니다.
5. Actions * 를 클릭하고 Alert these users 필드에 * sample@domain.com * 를 입력합니다.
6. 15분마다 사용자에게 알리려면 * 15분마다 알림 * 을 선택합니다.

지정된 시간 동안 수신자에게 반복적으로 알림을 보내도록 알림을 구성할 수 있습니다. 알림에 대해 이벤트 알림이 활성화되는 시간을 결정해야 합니다.

7. 실행할 스크립트 선택 메뉴에서 * 테스트 * 스크립트를 선택합니다.
8. 저장 * 을 클릭합니다.

로컬 사용자 암호 변경

잠재적인 보안 위험을 방지하기 위해 로컬 사용자 로그인 암호를 변경할 수 있습니다.

- 필요한 것 *

로컬 사용자로 로그인해야 합니다.

유지보수 사용자 및 원격 사용자의 암호는 다음 단계를 사용하여 변경할 수 없습니다. 원격 사용자 암호를 변경하려면 암호 관리자에게 문의하십시오. 유지보수 사용자 암호를 변경하려면 를 참조하십시오 "유지보수 콘솔 사용".

단계

1. Unified Manager에 로그인합니다.
2. 상단 메뉴 모음에서 사용자 아이콘을 클릭한 다음 * 암호 변경 * 을 클릭합니다.

   원격 사용자인 경우 * 암호 변경 * 옵션이 표시되지 않습니다.

3. 암호 변경 대화 상자에서 현재 암호와 새 암호를 입력합니다.
4. 저장 * 을 클릭합니다.

Unified Manager가 고가용성 구성으로 구성된 경우 설정의 두 번째 노드에서 암호를 변경해야 합니다. 두 인스턴스 모두 동일한 암호를 사용해야 합니다.

세션 비활성 시간 초과 설정

Unified Manager의 비활성 시간 초과 값을 지정하여 특정 시간 이후에 세션이 자동으로 종료되도록 할 수 있습니다. 기본적으로 시간 초과는 4,320분(72시간)으로 설정됩니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

이 설정은 로그인한 모든 사용자 세션에 영향을 줍니다.

SAML(Security Assertion Markup Language) 인증을 활성화한 경우에는 이 옵션을 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 기능 설정 * 을 클릭합니다.
2. 기능 설정 * 페이지에서 다음 옵션 중 하나를 선택하여 비활성 시간 초과를 지정합니다.

원하는 작업	다음을 수행하십시오.
세션이 자동으로 닫히지 않도록 설정된 시간 제한이 없습니다	Inactivity Timeout * (비활성 시간 초과 *) 패널에서 슬라이더 버튼을 왼쪽(꺼짐)으로 이동하고 * Apply * (적용 *)를 클릭합니다.
시간 초과 값으로 특정 시간(분)을 설정합니다	Inactivity Timeout * (비활성 시간 초과 *) 패널에서 슬라이더 버튼을 오른쪽(켜짐)으로 이동하고 비활성 시간 초과 값을 분 단위로 지정한 다음 * Apply * (적용 *)를 클릭합니다.

Unified Manager 호스트 이름을 변경하는 중입니다

경우에 따라 Unified Manager를 설치한 시스템의 호스트 이름을 변경할 수도 있습니다. 예를 들어, 호스트 이름을 유형, 작업 그룹 또는 모니터링되는 클러스터 그룹별로 Unified Manager 서버를 더 쉽게 식별하도록 변경할 수 있습니다.

호스트 이름을 변경하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat 또는 CentOS Linux 서버 또는 Microsoft Windows 서버에서 실행 중인지 여부에 따라 다릅니다.

Unified Manager 가상 어플라이언스 호스트 이름을 변경하는 중입니다

Unified Manager 가상 어플라이언스를 처음 구축할 때 네트워크 호스트에 이름이 할당됩니다. 배포 후 호스트 이름을 변경할 수 있습니다. 호스트 이름을 변경하는 경우 HTTPS 인증서도 다시 생성해야 합니다.

- 필요한 것 *

이러한 작업을 수행하려면 Unified Manager에 유지보수 사용자로 로그인하거나 애플리케이션 관리자 역할이 할당되어 있어야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 Unified Manager 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트의 이름을 지정했을 것입니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS에서 호스트 이름을 가져와야 합니다. DHCP 또는 DNS가 제대로 구성되지 않은 경우 호스트 이름 ""Unified Manager""가 자동으로 할당되어 보안 인증서와 연결됩니다.

호스트 이름이 할당된 방식에 관계없이 호스트 이름을 변경하고 새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려는 경우 새 보안 인증서를 생성해야 합니다.

호스트 이름 대신 서버의 IP 주소를 사용하여 웹 UI에 액세스하는 경우 호스트 이름을 변경할 경우 새 인증서를 생성할 필요가 없습니다. 그러나 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 인증서를 업데이트하는 것이 가장 좋습니다.

Unified Manager에서 호스트 이름을 변경하는 경우 WFA(OnCommand Workflow Automation)에서 호스트 이름을 수동으로 업데이트해야 합니다. 호스트 이름은 WFA에서 자동으로 업데이트되지 않습니다.

새 인증서는 Unified Manager 가상 머신을 다시 시작할 때까지 적용되지 않습니다.

단계

1. HTTPS 보안 인증서를 생성합니다

   새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려면 HTTPS 인증서를 다시 생성하여 새 호스트 이름과 연결해야 합니다.

2. Unified Manager 가상 머신을 다시 시작합니다

   HTTPS 인증서를 다시 생성한 후 Unified Manager 가상 머신을 다시 시작해야 합니다.

HTTPS 보안 인증서를 생성하는 중입니다

Active IQ Unified Manager를 처음 설치하면 기본 HTTPS 인증서가 설치됩니다. 기존 인증서를 대체하는 새 HTTPS 보안 인증서를 생성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

고유 이름(DN)에 더 나은 값을 사용하거나 키 크기를 더 늘리거나 만료 기간을 연장하거나 현재 인증서가 만료된 경우와 같이 인증서를 다시 생성해야 하는 이유는 여러 가지가 있습니다.

Unified Manager 웹 UI에 액세스할 수 없는 경우 유지보수 콘솔을 사용하여 동일한 값으로 HTTPS 인증서를 다시 생성할 수 있습니다. 인증서를 재생성하는 동안 키 크기와 키의 유효 기간을 정의할 수 있습니다. 유지보수 콘솔에서 '서버 인증서 재설정' 옵션을 사용하는 경우 397일 동안 유효한 새 HTTPS 인증서가 생성됩니다. 이 인증서에는 2048비트 크기의 RSA 키가 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * HTTPS 인증서 * 를 클릭합니다.
2. HTTPS 인증서 다시 생성 * 을 클릭합니다.

   HTTPS 인증서 재생성 대화 상자가 표시됩니다.

3. 인증서를 생성하는 방법에 따라 다음 옵션 중 하나를 선택합니다.

원하는 작업	수행할 작업...
현재 값을 사용하여 인증서를 다시 생성합니다	현재 인증서 특성을 사용하여 다시 생성 * 옵션을 클릭합니다.

원하는 작업	수행할 작업...
다른 값을 사용하여 인증서를 생성합니다	현재 인증서 특성 업데이트 * 옵션을 클릭합니다. 새 값을 입력하지 않으면 일반 이름 및 대체 이름 필드에 기존 인증서의 값이 사용됩니다. "공통 이름"은 호스트의 FQDN으로 설정되어야 합니다. 다른 필드에는 값이 필요하지 않지만 전자 메일, 회사, 부서 등의 값을 입력할 수 있습니다. 인증서에 해당 값을 채우려는 경우 시/도/Country를 선택합니다. 사용 가능한 키 크기(키 알고리즘은 ""RSA"")와 유효 기간 중에서 선택할 수도 있습니다. • 키 크기에 허용되는 값은 2048 3072 4096입니다. • 유효 기간은 최소 1일에서 최대 36500일입니다. 유효 기간 36500일이 허용되지만 유효 기간은 397일 또는 13개월을 넘지 않는 것이 좋습니다. 397일 이상의 유효 기간을 선택하고 이 인증서에 대해 CSR을 내보내고 잘 알려진 CA가 서명한 경우 CA에서 반환한 서명된 인증서의 유효 기간이 397일로 줄어듭니다. • 인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 "로컬 식별 정보 제외(예: localhost)" 확인란을 선택할 수 있습니다. 이 확인란을 선택하면 필드에 입력한 항목만 대체 이름 필드에 사용됩니다. 공백으로 두면 결과 인증서에 대체 이름 필드가 전혀 없습니다.

4. 예 * 를 클릭하여 인증서를 다시 생성합니다.
5. 새 인증서가 적용되도록 Unified Manager 서버를 다시 시작합니다.
6. HTTPS 인증서를 확인하여 새 인증서 정보를 확인합니다.

Unified Manager 가상 머신을 재시작합니다

Unified Manager의 유지보수 콘솔에서 가상 머신을 재시작할 수 있습니다. 새 보안 인증서를 생성한 후 또는 가상 시스템에 문제가 있는 경우 를 다시 시작해야 합니다.

- 필요한 것 *

가상 어플라이언스의 전원이 켜져 있습니다.

유지보수 사용자로 유지보수 콘솔에 로그인한 경우

또한 * Restart Guest * 옵션을 사용하여 vSphere에서 가상 머신을 재시작할 수 있습니다. 자세한 내용은 VMware 설명서를 참조하십시오.

단계

1. 유지보수 콘솔에 액세스합니다.
2. 시스템 구성 * > * 가상 시스템 재부팅 * 을 선택합니다.

Linux 시스템에서 Unified Manager 호스트 이름 변경

경우에 따라 Unified Manager를 설치한 Red Hat Enterprise Linux 또는 CentOS 시스템의 호스트 이름을 변경할 수 있습니다. 예를 들어 Linux 시스템을 나열할 때 호스트 이름을 Unified Manager 서버를 유형, 작업 그룹 또는 모니터링되는 클러스터 그룹별로 더 쉽게 식별하도록 변경할 수 있습니다.

- 필요한 것 *

Unified Manager가 설치된 Linux 시스템에 대한 루트 사용자 액세스 권한이 있어야 합니다.

호스트 이름(또는 호스트 IP 주소)을 사용하여 Unified Manager 웹 UI에 액세스할 수 있습니다. 배포 중에 네트워크에 대한 정적 IP 주소를 구성한 경우 네트워크 호스트의 이름을 지정했을 것입니다. DHCP를 사용하여 네트워크를 구성한 경우 DNS 서버에서 호스트 이름을 가져와야 합니다.

호스트 이름이 할당된 방식에 관계없이 호스트 이름을 변경하고 새 호스트 이름을 사용하여 Unified Manager 웹 UI에 액세스하려는 경우 새 보안 인증서를 생성해야 합니다.

호스트 이름 대신 서버의 IP 주소를 사용하여 웹 UI에 액세스하는 경우 호스트 이름을 변경할 경우 새 인증서를 생성할 필요가 없습니다. 그러나 인증서의 호스트 이름이 실제 호스트 이름과 일치하도록 인증서를 업데이트하는 것이 가장 좋습니다. 새 인증서는 Linux 시스템을 다시 시작할 때까지 적용되지 않습니다.

Unified Manager에서 호스트 이름을 변경하는 경우 WFA(OnCommand Workflow Automation)에서 호스트 이름을 수동으로 업데이트해야 합니다. 호스트 이름은 WFA에서 자동으로 업데이트되지 않습니다.

단계

1. 수정할 Unified Manager 시스템의 루트 사용자로 로그인합니다.
2. 다음 명령을 입력하여 Unified Manager 소프트웨어 및 관련 MySQL 소프트웨어를 중지합니다.

   '신조토 스탑 조숙조 신비주의자'

3. Linux의 hostnamectl 명령을 사용하여 호스트 이름을 변경합니다.

   'hostnamectl set-hostname new_FQDN’입니다

   hostnamectl set-hostname nuhost.corp.widget.com

4. 서버에 대한 HTTPS 인증서를 다시 생성합니다.

   '/opt/netapp/essentials/bin/cert.sh create'

5. 네트워크 서비스를 다시 시작합니다.

'Service network restart(서비스 네트워크 재시작)'

6. 서비스가 다시 시작된 후 새 호스트 이름이 스스로 ping을 수행할 수 있는지 확인합니다.

   'ping new_hostname'입니다

   "ping nuhost"

   이 명령은 원래 호스트 이름에 대해 이전에 설정된 것과 동일한 IP 주소를 반환해야 합니다.

7. 호스트 이름 변경을 완료하고 확인한 후 다음 명령을 입력하여 Unified Manager를 다시 시작합니다.

   신출호 신비사회 시작

정책 기반 스토리지 관리 설정 및 해제

Unified Manager 9.7부터 ONTAP 클러스터에 스토리지 워크로드(볼륨 및 LUN)를 프로비저닝하고 지정된 성능 서비스 수준에 따라 해당 워크로드를 관리할 수 있습니다. 이 기능은 ONTAP System Manager에서 워크로드를 생성하고 QoS 정책을 연결하는 것과 비슷하지만, Unified Manager를 사용하여 적용할 경우 Unified Manager 인스턴스가 모니터링하는 모든 클러스터에서 워크로드를 프로비저닝하고 관리할 수 있습니다.

애플리케이션 관리자 역할이 있어야 합니다.

이 옵션은 기본적으로 활성화되어 있지만 Unified Manager를 사용하여 워크로드를 프로비저닝하고 관리하지 않으려는 경우 비활성화할 수 있습니다.

이 옵션을 활성화하면 사용자 인터페이스에 많은 새 항목이 제공됩니다.

새 콘텐츠	위치
새로운 워크로드를 프로비저닝하는 데 필요한 페이지입니다	일반 작업 * > * 프로비저닝 * 에서 사용할 수 있습니다
성능 서비스 수준 정책을 생성하는 페이지입니다	설정 * > * 정책 * > * 성능 서비스 수준 * 에서 사용할 수 있습니다
성능 스토리지 효율성 정책을 생성하는 페이지입니다	설정 * > * 정책 * > * 스토리지 효율성 * 에서 사용할 수 있습니다
현재 워크로드 성능 및 워크로드 IOPS를 설명하는 패널	대시보드에서 사용할 수 있습니다

이러한 페이지 및 이 기능에 대한 자세한 내용은 제품의 온라인 도움말을 참조하십시오.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 기능 설정 * 을 클릭합니다.
2. 기능 설정 * 페이지에서 다음 옵션 중 하나를 선택하여 정책 기반 스토리지 관리를 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
정책 기반 스토리지 관리를 해제합니다	Policy-based storage management * (정책 기반 저장소 관리 *) 패널에서 슬라이더 버튼을 왼쪽으로 이동합니다.
정책 기반 스토리지 관리 설정	Policy-based storage management * (정책 기반 저장소 관리 *) 패널에서 슬라이더 버튼을 오른쪽으로 이동합니다.

Unified Manager 백업 구성

호스트 시스템과 를 통해 유지보수 콘솔에서 수행할 구성 단계 세트를 통해 Unified Manager의 백업 기능을 구성할 수 있습니다.

구성 단계에 대한 자세한 내용은 를 참조하십시오 "백업 및 복원 작업 관리".

기능 설정 관리

기능 설정 페이지에서 Active IQ Unified Manager의 특정 기능을 활성화 및 비활성화할 수 있습니다. 여기에는 정책에 따라 스토리지 객체 생성 및 관리, API 게이트웨이 및 로그인 배너 활성화, 알림 관리를 위한 스크립트 업로드, 비활성 시간에 따른 웹 UI 세션 시간 초과, Active IQ 플랫폼 이벤트 수신 비활성화 등이 포함됩니다.

기능 설정 페이지는 응용 프로그램 관리자 역할을 가진 사용자만 사용할 수 있습니다.

스크립트 업로드에 대한 자세한 내용은 을 참조하십시오 "스크립트 업로드 활성화 및 비활성화".

정책 기반 스토리지 관리 설정

정책 기반 스토리지 관리 * 옵션을 사용하면 서비스 수준 목표(SLO)를 기준으로 스토리지를 관리할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 활성화하면 Active IQ Unified Manager 인스턴스에 추가된 ONTAP 클러스터에서 스토리지 워크로드를 프로비저닝하고 할당된 성능 서비스 수준 및 스토리지 효율성 정책을 기반으로 이러한 워크로드를 관리할 수 있습니다.

이 기능은 * 일반 * > * 기능 설정 * > * 정책 기반 스토리지 관리 * 에서 활성화 또는 비활성화할 수 있습니다. 이 기능을 활성화하면 다음 페이지를 작동 및 모니터링할 수 있습니다.

- 프로비저닝(스토리지 워크로드 프로비저닝)
- * 정책 * > * 성능 서비스 수준 *
- * 정책 * > * 스토리지 효율성 *
- 클러스터 설정 페이지의 성능 서비스 수준별로 관리되는 작업 부하 열
- Dashboard * 의 워크로드 성능 패널입니다

화면에서 성능 서비스 수준 및 스토리지 효율성 정책을 생성하고 스토리지 워크로드를 프로비저닝할 수 있습니다. 또한, 할당된 성능 서비스 수준과 부적합 사항을 준수하는 스토리지 워크로드를 모니터링할 수 있습니다. 또한 워크로드 성능 및 워크로드 IOPS 패널을 사용하면 프로비저닝된 스토리지 워크로드를 기준으로 데이터 센터 전체의 클러스터에서 사용 가능한 총 용량 및 성능(IOPS)을 평가할 수 있습니다.

이 기능을 활성화한 후 Unified Manager REST API를 실행하여 이러한 기능 중 일부를 * Menu Bar * > * Help 버튼 * > * API Documentation * > * storage-provider * 범주에서 수행할 수 있습니다. 또는 호스트 이름 또는 IP 주소와 URL을 입력하여 REST API 페이지에 액세스할 수 있습니다. 형식은 https://<hostname>/docs/api/ 입니다

API에 대한 자세한 내용은 를 참조하십시오 "Active IQ Unified Manager REST API 시작하기".

API 게이트웨이 활성화 중

API 게이트웨이 기능을 통해 Active IQ Unified Manager는 개별적으로 로그인하지 않고도 여러 ONTAP 클러스터를 관리할 수 있는 단일 제어 플레인이 될 수 있습니다.

Unified Manager에 처음 로그인할 때 나타나는 구성 페이지에서 이 기능을 사용하도록 설정할 수 있습니다. 또는 * 일반 * > * 기능 설정 * > * API 게이트웨이 * 에서 이 기능을 활성화 또는 비활성화할 수 있습니다.

Unified Manager REST API는 ONTAP REST API와 다르며, ONTAP REST API를 사용하여 모든 기능을 사용할 수 있는 것은 아닙니다. 그러나 Unified Manager에 노출되지 않은 특정 기능을 관리하기 위해 ONTAP API에 액세스해야 하는 특정 비즈니스 요구 사항이 있는 경우 API 게이트웨이 기능을 설정하고 ONTAP API를 실행할 수 있습니다. 게이트웨이는 ONTAP API와 동일한 형식으로 헤더와 본문 요청을 유지함으로써 API 요청을 터널링하기 위한 프록시 역할을 합니다. Unified Manager 자격 증명을 사용하고 특정 API를 실행하여 개별 클러스터 자격 증명을 전달하지 않고 ONTAP 클러스터에 액세스하고 관리할 수 있습니다. Unified Manager는 Unified Manager 인스턴스에서 관리되는 ONTAP 클러스터에서 API를 실행하기 위한 단일 관리 지점 역할을 수행합니다. API가 반환하는 응답은 ONTAP에서 직접 실행되는 각 ONTAP REST API가 반환하는 응답과 동일합니다.

이 기능을 활성화한 후 * 메뉴 모음 * > * 도움말 버튼 * > * API 문서 * > * 게이트웨이 * 범주에서 Unified Manager REST API를 실행할 수 있습니다. 또는 호스트 이름 또는 IP 주소와 URL을 입력하여 REST API 페이지에 액세스할 수 있습니다 https://<hostname>/docs/api/`

API에 대한 자세한 내용은 를 참조하십시오 "Active IQ Unified Manager REST API 시작하기".

비활성 시간 초과 지정

Active IQ Unified Manager에 대한 비활성 시간 초과 값을 지정할 수 있습니다. 지정된 시간 동안 사용하지 않으면 응용 프로그램이 자동으로 로그아웃됩니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 비활성화하거나 * 일반 * > * 기능 설정 * > * 비활성 시간 제한 * 에서 시간을 수정할 수 있습니다. 이 기능을 활성화하면 * 로그아웃 후 * 필드에 비활성 시간 제한(분 단위)을 지정해야 합니다. 이 시간 이후에는 시스템이 자동으로 로그아웃됩니다. 기본값은 4320분(72시간)입니다.

SAML(Security Assertion Markup Language) 인증을 활성화한 경우에는 이 옵션을 사용할 수 없습니다.

Active IQ 포털 이벤트 활성화

Active IQ 포털 이벤트 활성화 또는 비활성화 여부를 지정할 수 있습니다. 이 설정을 사용하면

Active IQ 포털에서 시스템 구성, 케이블 연결 등에 대한 추가 이벤트를 검색하고 표시할 수 있습니다. 이 옵션은 기본적으로 활성화되어 있습니다.

이 기능을 활성화하면 Active IQ Unified Manager는 Active IQ 포털에서 검색된 이벤트를 표시합니다. 이러한 이벤트는 모니터링되는 모든 스토리지 시스템에서 생성되는 AutoSupport 메시지에 대해 일련의 규칙을 실행하여 생성됩니다. 이러한 이벤트는 다른 Unified Manager 이벤트와 다르며, 시스템 구성, 케이블 연결, 모범 사례 및 가용성 문제와 관련된 사고 또는 위험을 식별합니다.

이 기능은 * 일반 * > * 기능 설정 * > * Active IQ 포털 이벤트 * 에서 활성화 또는 비활성화할 수 있습니다. 외부 네트워크에 액세스할 수 없는 사이트에서는 * 스토리지 관리 * > * 이벤트 설정 * > * 업로드 규칙 * 에서 수동으로 규칙을 업로드해야 합니다.

이 기능은 기본적으로 활성화되어 있습니다. 이 기능을 사용하지 않도록 설정하면 Active IQ 이벤트가 검색되지 않고 Unified Manager에 표시되지 않습니다. 이 기능을 비활성화하면 Unified Manager가 해당 클러스터 시간대의 사전 정의된 시간 00:15에서 클러스터에서 Active IQ 이벤트를 수신할 수 있습니다.

규정 준수를 위한 보안 설정 활성화 및 비활성화

기능 설정 페이지의 * 보안 대시보드 * 패널에 있는 * 사용자 정의 * 버튼을 사용하여 Unified Manager에서 규정 준수 모니터링을 위한 보안 매개 변수를 활성화 또는 비활성화할 수 있습니다.

이 페이지에서 설정 또는 사용하지 않도록 설정하면 Unified Manager에서 클러스터 및 스토리지 VM의 전반적인 규정 준수 상태가 적용됩니다. 선택한 항목에 따라 클러스터 인벤토리 페이지의 * 보안: 모든 클러스터 * 보기와 스토리지 VM 인벤토리 페이지의 * 보안: 모든 스토리지 VM * 보기에 해당 열이 표시됩니다.

관리자 역할을 가진 사용자만 이러한 설정을 편집할 수 있습니다.

ONTAP 클러스터, 스토리지 VM 및 볼륨의 보안 기준은 에 정의된 권장 사항을 기준으로 평가됩니다 "Security Hardening Guide for NetApp ONTAP 9 을 참조하십시오". 대시보드와 보안 페이지의 보안 패널에는 클러스터, 스토리지 VM 및 볼륨의 기본 보안 준수 상태가 표시됩니다. 보안 이벤트도 생성되고 보안 위반이 있는 클러스터 및 스토리지 VM에 대해 관리 작업이 활성화됩니다.

보안 설정 사용자 지정

ONTAP 환경에 적용할 수 있는 규정 준수 모니터링 설정을 사용자 지정하려면 다음 단계를 수행하십시오.

단계

1. 일반 > 기능 설정 > 보안 대시보드 > 사용자 지정 * 을 클릭합니다. 보안 대시보드 설정 사용자 지정 * 팝업이 나타납니다.

   설정 또는 해제하는 보안 규정 준수 매개 변수는 클러스터 및 스토리지 VM 화면의 기본 보안 보기, 보고서 및 예약된 보고서에 직접 영향을 줄 수 있습니다. 보안 매개 변수를 수정하기 전에 이러한 화면에서 Excel 보고서를 업로드한 경우 다운로드한 Excel 보고서에 오류가 있을 수 있습니다.

2. ONTAP 클러스터에 대한 사용자 정의 설정을 활성화 또는 비활성화하려면 * 클러스터 * 에서 필요한 일반 설정을 선택합니다. 클러스터 규정 준수를 사용자 지정하는 옵션에 대한 자세한 내용은 을 참조하십시오 "클러스터 규정 준수 범주".
3. 스토리지 VM에 대한 사용자 지정 설정을 활성화하거나 비활성화하려면 * 스토리지 VM * 에서 필요한 일반 설정을 선택합니다. 스토리지 VM 규정 준수를 사용자 지정하는 옵션에 대한 자세한 내용은 를 참조하십시오 "스토리지 VM

규정 준수 범주".

AutoSupport 및 인증 설정 사용자 지정

AutoSupport 설정 * 섹션에서 AutoSupport에서 ONTAP 메시지를 보내는 데 HTTPS 전송을 사용할지 여부를 지정할 수 있습니다.

인증 설정 * 섹션에서 기본 ONTAP 관리자 사용자에 대해 Unified Manager 알림을 발생하도록 설정할 수 있습니다.

스크립트 업로드 활성화 및 비활성화

스크립트를 Unified Manager에 업로드하여 실행할 수 있는 기능은 기본적으로 활성화되어 있습니다. 보안상의 이유로 조직에서 이 작업을 허용하지 않으려는 경우 이 기능을 사용하지 않도록 설정할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 기능 설정 * 을 클릭합니다.
2. 기능 설정 * 페이지에서 다음 옵션 중 하나를 선택하여 스크립팅을 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
스크립트를 사용하지 않도록 설정합니다	Script Upload* 패널에서 슬라이더 단추를 왼쪽으로 이동합니다.
스크립트를 사용하도록 설정합니다	Script Upload* 패널에서 슬라이더 단추를 오른쪽으로 이동합니다.

로그인 배너 추가 중

로그인 배너를 추가하면 조직에서 시스템에 액세스할 수 있는 사용자, 로그인 및 로그아웃 시 사용 약관 등의 정보를 표시할 수 있습니다.

스토리지 운영자 또는 관리자와 같은 모든 사용자는 로그인, 로그아웃 및 세션 시간 초과 중에 이 로그인 배너 팝업을 볼 수 있습니다.

유지보수 콘솔 사용

유지보수 콘솔을 사용하여 네트워크 설정을 구성하고, Unified Manager가 설치된 시스템을 구성 및 관리하고, 기타 유지보수 작업을 수행하여 발생할 수 있는 문제를 예방하고 해결할 수 있습니다.

유지보수 콘솔에서 제공하는 기능은 무엇입니까

Unified Manager 유지보수 콘솔을 사용하면 Unified Manager 시스템의 설정을 유지하고 문제 발생을 방지하기 위해 필요한 모든 변경을 수행할 수 있습니다.

Unified Manager를 설치한 운영 체제에 따라 유지보수 콘솔에서 다음 기능을 제공합니다.

- 특히 Unified Manager 웹 인터페이스를 사용할 수 없는 경우, 가상 어플라이언스 관련 문제를 해결합니다
- 최신 버전의 Unified Manager로 업그레이드하십시오
- 기술 지원 팀에 보낼 지원 번들을 생성합니다
- 네트워크 설정을 구성합니다
- 유지보수 사용자 암호를 변경합니다
- 외부 데이터 공급자에 연결하여 성능 통계를 보냅니다
- 성능 데이터 수집 내부 변경
- 이전에 백업한 버전에서 Unified Manager 데이터베이스 및 구성 설정을 복원합니다.

유지 관리 사용자가 수행하는 작업

유지 관리 사용자는 Red Hat Enterprise Linux 또는 CentOS 시스템에 Unified Manager를 설치하는 동안 생성됩니다. 유지보수 사용자 이름은 "'umadmin" 사용자입니다. 유지 관리 사용자는 웹 UI에서 응용 프로그램 관리자 역할을 가지고 있으며, 사용자는 후속 사용자를 만들고 해당 역할을 할당할 수 있습니다.

유지보수 사용자 또는 umadmin 사용자도 Unified Manager 유지보수 콘솔에 액세스할 수 있습니다.

진단 사용자 기능

진단 액세스의 목적은 기술 지원 부서에서 문제 해결을 지원하도록 하는 것입니다. 기술 지원 부서의 지시가 있을 때만 사용해야 합니다.

진단 사용자는 문제 해결을 위해 기술 지원 부서의 지시가 있을 때 OS 레벨 명령을 실행할 수 있습니다.

유지보수 콘솔 액세스

Unified Manager 사용자 인터페이스가 작동 중이 아니거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우, 유지보수 콘솔에 액세스하여 Unified Manager 시스템을 관리할 수 있습니다.

- 필요한 것 *

Unified Manager를 설치하고 구성해야 합니다.

15분 동안 비활성 상태가 지속되면 유지보수 콘솔에서 로그아웃합니다.

VMware에 설치된 경우 VMware 콘솔을 통해 유지 관리 사용자로 이미 로그인한 경우에는 Secure Shell을 사용하여 동시에 로그인할 수 없습니다.

단계

1. 다음 단계에 따라 유지보수 콘솔에 액세스합니다.

이 운영 체제에서...	다음 단계를 따르십시오...
VMware	a. Secure Shell을 사용하여 Unified Manager 가상 어플라이언스의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. b. 유지보수 사용자 이름과 암호를 사용하여 유지보수 콘솔에 로그인합니다.
리눅스	a. Secure Shell을 사용하여 Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. b. 유지보수 사용자(umadmin) 이름 및 암호를 사용하여 시스템에 로그인합니다. c. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.
Windows	a. 관리자 자격 증명을 사용하여 Unified Manager 시스템에 로그인합니다. b. Windows 관리자로 PowerShell을 실행합니다. c. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.

Unified Manager 유지보수 콘솔 메뉴가 표시됩니다.

vSphere VM 콘솔을 사용하여 유지 관리 콘솔 액세스

Unified Manager 사용자 인터페이스가 작동 중이 아니거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우 유지보수 콘솔에 액세스하여 가상 어플라이언스를 재구성할 수 있습니다.

- 필요한 것 *
- 유지 보수 사용자여야 합니다.
- 유지보수 콘솔에 액세스하려면 가상 어플라이언스의 전원을 켜야 합니다.

단계

1. vSphere Client에서 Unified Manager 가상 어플라이언스를 찾습니다.
2. Console * 탭을 클릭합니다.

3. 콘솔 창 내부를 클릭하여 로그인합니다.
4. 사용자 이름 및 암호를 사용하여 유지보수 콘솔에 로그인합니다.

   15분 동안 비활성 상태가 지속되면 유지보수 콘솔에서 로그아웃합니다.

유지보수 콘솔 메뉴

유지보수 콘솔은 Unified Manager 서버의 특수 기능 및 구성 설정을 유지 관리 및 관리할 수 있는 다양한 메뉴로 구성되어 있습니다.

Unified Manager를 설치한 운영 체제에 따라 유지보수 콘솔은 다음 메뉴로 구성됩니다.

- Unified Manager 업그레이드(VMware만 해당)
- 네트워크 구성(VMware만 해당)
- 시스템 구성(VMware만 해당)
  a. 지원/진단
  b. 서버 인증서를 재설정합니다
  c. 외부 데이터 공급자
  d. 백업 복원
  e. 성능 폴링 간격 구성
  f. SAML 인증을 비활성화합니다
  g. 애플리케이션 포트 보기/변경
  h. 디버그 로그 구성
  i. MySQL 포트 3306에 대한 액세스를 제어합니다
  j. Exit(종료)

특정 메뉴 옵션에 액세스하기 위해 목록에서 번호를 선택합니다. 예를 들어 백업 및 복원의 경우 _4_를 선택합니다.

네트워크 구성 메뉴

네트워크 구성 메뉴를 사용하여 네트워크 설정을 관리할 수 있습니다. Unified Manager 사용자 인터페이스를 사용할 수 없는 경우 이 메뉴를 사용해야 합니다.

Unified Manager가 Red Hat Enterprise Linux, CentOS 또는 Microsoft Windows에 설치된 경우에는 이 메뉴를 사용할 수 없습니다.

다음 메뉴를 선택할 수 있습니다.

- * IP 주소 설정 표시 *

  IP 주소, 네트워크, 브로드캐스트 주소, 넷마스크, 게이트웨이를 포함하여 가상 어플라이언스에 대한 현재 네트워크 설정을 표시합니다. DNS 서버가 있습니다.

- * IP 주소 설정 변경 *

  IP 주소, 넷마스크, 게이트웨이 또는 DNS 서버를 포함하여 가상 어플라이언스에 대한 네트워크 설정을 변경할 수 있습니다. 유지보수 콘솔을 사용하여 네트워크 설정을 DHCP에서 정적 네트워킹으로 전환하는 경우 호스트 이름을 편집할 수 없습니다. 변경 사항을 적용하려면 * 변경 사항 커밋 * 을 선택해야 합니다.

- * 도메인 이름 검색 설정 표시 *

  호스트 이름을 확인하는 데 사용되는 도메인 이름 검색 목록을 표시합니다.

- * 도메인 이름 검색 설정 변경 *

  호스트 이름을 확인할 때 검색할 도메인 이름을 변경할 수 있습니다. 변경 사항을 적용하려면 * 변경 사항 커밋 * 을 선택해야 합니다.

- * 정적 라우트 표시 *

  현재 정적 네트워크 경로를 표시합니다.

- * 정적 라우트 변경 *

  정적 네트워크 경로를 추가하거나 삭제할 수 있습니다. 변경 사항을 적용하려면 * 변경 사항 커밋 * 을 선택해야 합니다.

  ◦ * 루트 추가 *

    정적 경로를 추가할 수 있습니다.

  ◦ * 루트 삭제 *

    정적 라우트를 삭제할 수 있습니다.

  ◦ * 뒤로 *

    기본 메뉴 * 로 돌아갑니다.

  ◦ * 종료 *

    유지보수 콘솔을 종료합니다.

- * 네트워크 인터페이스 비활성화 *

  사용 가능한 네트워크 인터페이스를 비활성화합니다. 하나의 네트워크 인터페이스만 사용할 수 있는 경우에는 비활성화할 수 없습니다. 변경 사항을 적용하려면 * 변경 사항 커밋 * 을 선택해야 합니다.

- * 네트워크 인터페이스 사용 *

  사용 가능한 네트워크 인터페이스를 활성화합니다. 변경 사항을 적용하려면 * 변경 사항 커밋 * 을 선택해야 합니다.

- * 변경 사항을 커밋합니다 *

  가상 어플라이언스의 네트워크 설정에 대한 변경 사항을 적용합니다. 변경 사항을 적용하려면 이 옵션을 선택해야 합니다. 그렇지 않으면 변경 내용이 적용되지 않습니다.

- * 호스트에 Ping *

  IP 주소 변경 또는 DNS 구성을 확인하기 위해 타겟 호스트에 ping을 보냅니다.

- * 기본 설정으로 복원 *

  모든 설정을 출하 시 기본값으로 재설정합니다. 변경 사항을 적용하려면 * 변경 사항 커밋 * 을 선택해야 합니다.

- * 뒤로 *

  기본 메뉴 * 로 돌아갑니다.

- * 종료 *

  유지보수 콘솔을 종료합니다.

System Configuration(시스템 구성**)** 메뉴

시스템 구성 메뉴를 사용하면 서버 상태 보기, 가상 시스템 재부팅 및 종료 등의 다양한 옵션을 제공하여 가상 어플라이언스를 관리할 수 있습니다.

Unified Manager가 Linux 또는 Microsoft Windows 시스템에 설치된 경우 이 메뉴에서 ""Unified Manager 백업에서 복원" 옵션만 사용할 수 있습니다.

다음 메뉴를 선택할 수 있습니다.

- * 서버 상태 표시 *

  현재 서버 상태를 표시합니다. 상태 옵션에는 실행 중 및 실행 중이 아닙니다.

  서버가 실행되고 있지 않으면 기술 지원 부서에 문의해야 할 수 있습니다.

- * 가상 머신을 재부팅합니다 *

  가상 시스템을 재부팅하여 모든 서비스를 중지합니다. 재부팅 후 가상 머신과 서비스가 다시 시작됩니다.

- * 가상 머신 종료 *

  가상 머신을 종료하고 모든 서비스를 중지합니다.

  이 옵션은 가상 시스템 콘솔에서만 선택할 수 있습니다.

- * <로그인한 사용자> 사용자 암호 변경 *

  현재 로그인한 사용자의 암호를 변경합니다. 이 암호는 유지 관리 사용자만 될 수 있습니다.

- * 데이터 디스크 크기 증가 *

  가상 시스템에서 데이터 디스크(디스크 3)의 크기를 늘립니다.

- * 스왑 디스크 크기 증가 *

가상 시스템에서 스왑 디스크(디스크 2)의 크기를 늘립니다.

- * 시간대 변경 *

  시간대를 사용자의 위치로 변경합니다.

- * NTP 서버 변경 *

  IP 주소 또는 FQDN(정규화된 도메인 이름)과 같은 NTP 서버 설정을 변경합니다.

- * NTP 서비스 변경 *

  NTP와 스ystemd-timesyncd 서비스 간을 전환합니다.

- * Unified Manager Backup에서 복원 *

  Unified Manager 데이터베이스와 구성 설정을 이전에 백업된 버전에서 복원합니다.

- * 서버 인증서 재설정 * 을 선택합니다

  서버 보안 인증서를 재설정합니다.

- * 호스트 이름 변경 *

  가상 어플라이언스가 설치된 호스트의 이름을 변경합니다.

- * 뒤로 *

  시스템 구성 메뉴를 종료하고 주 메뉴로 돌아갑니다.

- * 종료 *

  유지보수 콘솔 메뉴를 종료합니다.

지원 및 진단 메뉴

지원 및 진단 메뉴를 사용하면 문제 해결 지원을 위해 기술 지원 부서에 보낼 수 있는 지원 번들을 생성할 수 있습니다.

다음 메뉴 옵션을 사용할 수 있습니다.

- * Light Support Bundle * 생성

  에서는 30일 동안의 로그 및 구성 데이터베이스 레코드를 포함하는 경량 지원 번들을 생성할 수 있습니다. 성능 데이터, 획득 기록 파일 및 서버 힙 덤프는 제외됩니다.

- * 지원 번들 생성 *

  진단 사용자의 홈 디렉토리에 진단 정보가 포함된 전체 지원 번들(7-Zip 파일)을 생성할 수 있습니다. 시스템이 인터넷에 연결되어 있는 경우 지원 번들을 NetApp에 업로드할 수도 있습니다.

  이 파일에는 AutoSupport 메시지에서 생성된 정보, Unified Manager 데이터베이스의 콘텐츠, Unified Manager

서버 내부 구성 요소에 대한 자세한 데이터, 일반적으로 AutoSupport 메시지 또는 경량 지원 번들에 포함되지 않은 자세한 레벨의 로그가 포함됩니다.

추가 메뉴 옵션

다음 메뉴 옵션을 사용하여 Unified Manager 서버에서 다양한 관리 작업을 수행할 수 있습니다.

다음 메뉴를 선택할 수 있습니다.

- * 서버 인증서 재설정 * 을 선택합니다

  HTTPS 서버 인증서를 재생성합니다.

  Unified Manager GUI에서 * 일반 * > * HTTPS 인증서 * > * HTTPS 인증서 다시 생성 * 을 클릭하여 서버 인증서를 다시 생성할 수 있습니다.

- * SAML 인증 비활성화 *

  ID 공급자(IDP)가 Unified Manager GUI에 액세스하는 사용자에 대해 로그인 인증을 더 이상 제공하지 않도록 SAML 인증을 비활성화합니다. 이 콘솔 옵션은 일반적으로 IDP 서버 또는 SAML 구성 문제로 인해 사용자가 Unified Manager GUI에 액세스하지 못하게 되는 경우에 사용됩니다.

- * 외부 데이터 공급자 *

  Unified Manager를 외부 데이터 공급자에 연결하는 옵션을 제공합니다. 연결을 설정하면 성능 데이터가 외부 서버로 전송되므로 스토리지 성능 전문가가 타사 소프트웨어를 사용하여 성능 메트릭을 차트로 작성할 수 있습니다. 다음 옵션이 표시됩니다.

  - * Display Server Configuration * — 외부 데이터 공급자에 대한 현재 연결 및 구성 설정을 표시합니다.
  - * 서버 연결 추가/수정 * — 외부 데이터 공급자에 대한 새 연결 설정을 입력하거나 기존 설정을 변경할 수 있습니다.
  - * 서버 구성 수정 * — 외부 데이터 공급자에 대한 새 구성 설정을 입력하거나 기존 설정을 변경할 수 있습니다.
  - * 서버 연결 삭제 * — 외부 데이터 공급자에 대한 연결을 삭제합니다.

    연결이 삭제된 후 Unified Manager는 외부 서버와의 연결이 끊어집니다.

- * 백업 복원 *

  자세한 내용은 의 항목을 참조하십시오 "백업 및 복원 작업 관리".

- * 성능 폴링 간격 구성 *

  Unified Manager가 클러스터에서 성능 통계 데이터를 수집하는 빈도를 구성할 수 있는 옵션을 제공합니다. 기본 수집 간격은 5분입니다.

  대규모 클러스터의 컬렉션이 적시에 완료되지 않는 경우 이 간격을 10분 또는 15분으로 변경할 수 있습니다.

- * 응용 프로그램 포트 보기/변경 *

  Unified Manager에서 보안에 필요한 경우 HTTP 및 HTTPS 프로토콜에 사용하는 기본 포트를 변경하는 옵션을 제공합니다. 기본 포트는 HTTP의 경우 80이고 HTTPS의 경우 443입니다.

- * MySQL 포트 3306 * 에 대한 액세스를 제어합니다

  기본 MySQL 포트 3306에 대한 호스트 액세스를 제어합니다. 보안상의 이유로 Linux, Windows 및 VMware vSphere 시스템에 Unified Manager를 새로 설치하는 동안에만 이 포트를 통한 액세스가 localhost로 제한됩니다. 이 옵션을 사용하면 로컬 호스트 및 원격 호스트 간에 이 포트의 표시 여부를 전환할 수 있습니다. 즉, 사용자 환경에서 localhost만 사용하도록 설정된 경우 이 포트를 원격 호스트에서도 사용할 수 있도록 설정할 수 있습니다. 또는 모든 호스트에 대해 활성화된 경우 이 포트의 액세스를 localhost 전용으로 제한할 수 있습니다. 이전에 원격 호스트에서 액세스가 설정된 경우 구성은 업그레이드 시나리오에서 유지됩니다. 포트 표시 여부를 토글한 후 Windows 시스템의 방화벽 설정을 확인하고 MySQL 포트 3306에 대한 액세스를 제한하도록 설정이 구성된 경우 방화벽 설정을 비활성화해야 합니다.

- * 종료 *

  유지보수 콘솔 메뉴를 종료합니다.

Windows에서 유지 관리 사용자 암호 변경

필요한 경우 Unified Manager 유지보수 사용자 암호를 변경할 수 있습니다.

단계

1. Unified Manager 웹 UI 로그인 페이지에서 * 암호를 잊으셨습니까 * 를 클릭합니다.

   암호를 재설정할 사용자의 이름을 묻는 페이지가 표시됩니다.

2. 사용자 이름을 입력하고 * 제출 * 을 클릭합니다.

   암호를 재설정할 수 있는 링크가 포함된 이메일이 해당 사용자 이름에 대해 정의된 이메일 주소로 전송됩니다.

3. 이메일에서 * 비밀번호 재설정 링크 * 를 클릭하고 새 비밀번호를 정의합니다.
4. 웹 UI로 돌아가 새 암호를 사용하여 Unified Manager에 로그인합니다.

Linux 시스템에서 umadmin 암호 변경

보안상의 이유로 설치 프로세스를 완료한 후 즉시 Unified Manager umadmin 사용자의 기본 암호를 변경해야 합니다. 필요한 경우 나중에 언제든지 암호를 다시 변경할 수 있습니다.

- 필요한 것 *
- Unified Manager는 Red Hat Enterprise Linux 또는 CentOS Linux 시스템에 설치해야 합니다.
- Unified Manager가 설치된 Linux 시스템에 대한 루트 사용자 자격 증명이 있어야 합니다.

단계

1. Unified Manager가 실행 중인 Linux 시스템의 루트 사용자로 로그인합니다.
2. umadmin 암호 변경:

   'passwd umadmin'

   umadmin 사용자의 새 암호를 입력하라는 메시지가 표시됩니다.

Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 포트를 변경합니다

Unified Manager가 HTTP 및 HTTPS 프로토콜에 사용하는 기본 포트는 보안에 필요한 경우 설치 후 변경할 수 있습니다. 기본 포트는 HTTP의 경우 80이고 HTTPS의 경우 443입니다.

- 필요한 것 *

Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.

Mozilla Firefox 또는 Google Chrome 브라우저를 사용할 때 안전하지 않은 것으로 간주되는 포트가 있습니다. HTTP 및 HTTPS 트래픽에 새 포트 번호를 할당하기 전에 브라우저를 통해 확인하십시오. 안전하지 않은 포트를 선택하면 시스템에 액세스할 수 없게 될 수 있으므로 고객 지원 센터에 문의하여 문제를 해결해야 합니다.

포트를 변경한 후에는 Unified Manager 인스턴스가 자동으로 다시 시작되므로 시스템을 잠시 중단해 보십시오.

1. SSH를 사용하여 Unified Manager 호스트에 대한 유지보수 사용자로 로그인합니다.

   Unified Managermaintenance 콘솔 프롬프트가 표시됩니다.

2. 응용 프로그램 포트 보기/변경 * 이라고 표시된 메뉴 옵션의 번호를 입력한 다음 Enter 키를 누릅니다.
3. 메시지가 표시되면 유지보수 사용자 암호를 다시 입력합니다.
4. HTTP 및 HTTPS 포트의 새 포트 번호를 입력한 다음 Enter 키를 누릅니다.

   포트 번호를 비워 두면 프로토콜의 기본 포트가 할당됩니다.

   지금 포트를 변경하고 Unified Manager를 다시 시작할지 묻는 메시지가 표시됩니다.

5. 포트를 변경하고 Unified Manager를 다시 시작하려면 * y * 를 입력합니다.
6. 유지보수 콘솔을 종료합니다.

변경 후에는 Unified Manager 웹 UI에 액세스할 수 있도록 URL에 새 포트 번호를 포함해야 합니다(예: https://host.company.com:1234, https://12.13.14.15:1122 또는 https://[2001:db8:0:1]:2123).

네트워크 인터페이스를 추가하는 중입니다

네트워크 트래픽을 분리해야 하는 경우 새 네트워크 인터페이스를 추가할 수 있습니다.

- 필요한 것 *

vSphere를 사용하여 가상 어플라이언스에 네트워크 인터페이스를 추가해야 합니다.

가상 어플라이언스의 전원을 켜야 합니다.

Unified Manager가 Red Hat Enterprise Linux 또는 Microsoft Windows에 설치된 경우에는 이 작업을 수행할 수 없습니다.

단계

1. vSphere 콘솔 주 메뉴에서 * 시스템 구성 * > * 운영 체제 재부팅 * 을 선택합니다.

   재부팅 후 유지보수 콘솔은 새로 추가된 네트워크 인터페이스를 감지할 수 있습니다.

2. 유지보수 콘솔에 액세스합니다.
3. Network Configuration * > * Enable Network Interface * 를 선택합니다.
4. 새 네트워크 인터페이스를 선택하고 * Enter * 를 누릅니다.

   eth1 * 을 선택하고 * Enter * 를 누릅니다.

5. y * 를 입력하여 네트워크 인터페이스를 활성화합니다.
6. 네트워크 설정을 입력합니다.

   정적 인터페이스를 사용하는 경우 또는 DHCP가 감지되지 않는 경우 네트워크 설정을 입력하라는 메시지가 표시됩니다.

   네트워크 설정을 입력하면 자동으로 * 네트워크 구성 * 메뉴로 돌아갑니다.

7. 변경 사항 커밋 * 을 선택합니다.

   네트워크 인터페이스를 추가하려면 변경 사항을 커밋해야 합니다.

Unified Manager 데이터베이스 디렉토리에 디스크 공간 추가

Unified Manager 데이터베이스 디렉토리에는 ONTAP 시스템에서 수집된 모든 상태 및 성능 데이터가 포함되어 있습니다. 경우에 따라 데이터베이스 디렉토리의 크기를 늘려야 할 수 있습니다.

예를 들어, Unified Manager가 각 클러스터에 노드가 많은 수의 클러스터에서 데이터를 수집하는 경우 데이터베이스 디렉토리가 가득 찰 수 있습니다. 데이터베이스 디렉토리가 90% 찼을 때 경고 이벤트가 수신되고 디렉토리가 95% 찼을 때 중요한 이벤트가 발생합니다.

디렉토리가 95% 꽉 찬 후 클러스터에서 추가 데이터가 수집되지 않습니다.

데이터 디렉토리에 용량을 추가하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat 또는 CentOS Linux 서버 또는 Microsoft Windows 서버에서 실행 중인지 여부에 따라 다릅니다.

Linux 호스트의 데이터 디렉토리에 공간을 추가합니다

처음에 Linux 호스트를 설정한 다음 Unified Manager를 설치할 때 Unified Manager를 지원하기 위해 '/opt/netapp/data' 디렉토리에 디스크 공간을 충분히 할당한 경우, '/opt/netapp/data' 디렉토리에서 디스크 공간을 늘려서 설치 후 디스크 공간을 추가할 수 있습니다.

- 필요한 것 *

Unified Manager가 설치된 Red Hat Enterprise Linux 또는 CentOS Linux 시스템에 대한 루트 사용자 액세스 권한이 있어야 합니다.

데이터 디렉토리 크기를 늘리기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가할 Linux 시스템에 루트 사용자로 로그인합니다.
2. Unified Manager 서비스 및 관련 MySQL 소프트웨어를 표시된 순서대로 중지합니다.

   '신조토 스탑 조숙조 신비주의자'

3. 현재 '/opt/netapp/data' 디렉토리에 데이터를 포함할 디스크 공간이 충분한 임시 백업 폴더(예: /backup-data')를 생성합니다.
4. 기존 '/opt/netapp/data' 디렉토리의 컨텐츠 및 권한 구성을 백업 데이터 디렉토리에 복사합니다.

   'cp-arp/opt/netapp/data/ * /backup-data

5. SE Linux가 활성화된 경우:

   a. 기존 '/opt/netapp/data' 폴더의 폴더에 대한 SE Linux 유형을 가져옵니다.

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
echo $se_type
mysqld_db_t
```

   a. chcon 명령을 실행하여 백업 디렉토리에 대한 SE Linux 유형을 설정합니다.

      'chcon-R—type=mysqld_db_t/backup-data

6. '/opt/netapp/data' 디렉터리의 내용을 제거합니다.
   a. 'cd/opt/netapp/data'
   b. rm-rf *
7. LVM 명령을 사용하거나 추가 디스크를 추가하여 '/opt/netapp/data' 디렉토리의 크기를 최소 150GB로 확장합니다.

   디스크에서 '/opt/netapp/data'를 생성한 경우 NFS 또는 CIFS 공유로 '/opt/netapp/data'를 마운트하지 마십시오. 이 경우 디스크 공간을 확장하려고 하면 'resize', 'extend' 같은 일부 LVM 명령이 예상대로 작동하지 않을 수 있기 때문입니다.

8. '/opt/netapp/data' 디렉토리 소유자(MySQL) 및 그룹(root)이 변경되지 않았는지 확인합니다.

   'ls-ltr/opt/netapp/|grep data'

   시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. SE Linux가 활성화된 경우, '/opt/netapp/data' 디렉토리의 컨텍스트가 mysqld_db_t로 설정되어 있는지 확인합니다.

   a. 'touch/opt/netapp/data/abc

   b. 'ls-Z/opt/netapp/data/abc

      시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. 이 추가 파일이 나중에 데이터베이스 오류를 발생시키지 않도록 abc 파일을 삭제합니다.
11. 백업 데이터의 내용을 확장된 '/opt/netapp/data' 디렉토리로 다시 복사합니다.

    'cp-arp/backup-data/ * /opt/netapp/data/'

12. SE Linux가 활성화된 경우 다음 명령을 실행합니다.

    'chcon-R—type=mysqld_db_t/opt/netapp/data

13. MySQL 서비스를 시작합니다.

    '스타emctl start mysqld'

14. MySQL 서비스가 시작된 후 다음 순서대로 socie 및 socieau 서비스를 시작합니다.

    '신조 시작 조숙자'

15. 모든 서비스가 시작된 후 백업 폴더 "/backup-data"를 삭제합니다.

    'rm-rf/backup-data

VMware 가상 머신의 데이터 디스크에 공간 추가

Unified Manager 데이터베이스의 데이터 디스크 공간을 늘려야 하는 경우, Unified Manager 유지보수 콘솔을 사용하여 디스크 공간을 늘려서 설치 후 용량을 추가할 수 있습니다.

- 필요한 것 *
- vSphere Client에 대한 액세스 권한이 있어야 합니다.
- 가상 머신에 로컬에 저장된 스냅샷이 없어야 합니다.
- 유지보수 사용자 자격 증명이 있어야 합니다.

가상 디스크의 크기를 늘리기 전에 가상 시스템을 백업하는 것이 좋습니다.

단계

1. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 데이터 디스크 용량을 디스크 3에 추가합니다. 자세한 내용은 VMware 설명서를 참조하십시오.

드문 경우지만 Unified Manager 배포에서는 ""하드 디스크 3"" 대신 ""하드 디스크 2""를 데이터 디스크에 사용합니다. 구축 과정에서 이 문제가 발생한 경우 더 큰 디스크의 공간을 늘리십시오. 데이터 디스크는 항상 다른 디스크보다 더 많은 공간을 갖게 됩니다.

2. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 * Console * 탭을 선택합니다.
3. 콘솔 창을 클릭한 다음 사용자 이름과 암호를 사용하여 유지보수 콘솔에 로그인합니다.
4. 주 메뉴에서 * 시스템 구성 * 옵션의 번호를 입력합니다.
5. 시스템 구성 메뉴에서 * 데이터 디스크 크기 증가 * 옵션에 대한 번호를 입력합니다.

Microsoft Windows 서버의 논리 드라이브에 공간 추가

Unified Manager 데이터베이스의 디스크 공간을 늘려야 하는 경우 Unified Manager가 설치된 논리 드라이브에 용량을 추가할 수 있습니다.

- 필요한 것 *

Windows 관리자 권한이 있어야 합니다.

디스크 공간을 추가하기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가할 Windows 서버에 관리자로 로그인합니다.
2. 공간을 더 추가하는 데 사용할 방법에 해당하는 단계를 따릅니다.

옵션을 선택합니다	설명
물리적 서버에서 Unified Manager 서버가 설치된 논리 드라이브에 용량을 추가합니다.	Microsoft 항목의 단계를 따릅니다. "기본 볼륨을 확장합니다"
물리적 서버에서 하드 디스크 드라이브를 추가합니다.	Microsoft 항목의 단계를 따릅니다. "하드 디스크 드라이브 추가"
가상 머신에서 디스크 파티션의 크기를 늘립니다.	VMware 항목의 단계를 따릅니다. "디스크 파티션 크기 늘리기"

사용자 액세스 관리

역할을 생성하고 Active IQ Unified Manager에 대한 사용자 액세스를 제어하는 기능을 할당할 수 있습니다. Unified Manager 내에서 선택한 개체에 액세스하는 데 필요한 기능이 있는 사용자를 식별할 수 있습니다. 이러한 역할 및 기능을 가진 사용자만 Unified Manager의 개체를 관리할 수 있습니다.

사용자 추가

사용자 페이지를 사용하여 로컬 사용자 또는 데이터베이스 사용자를 추가할 수 있습니다. 인증 서버에 속하는 원격 사용자 또는 그룹을 추가할 수도 있습니다. 이러한 사용자에게 역할을 할당할 수 있으며 역할의 권한에 따라 사용자는 Unified Manager를 사용하여 스토리지 객체 및 데이터를 관리하거나 데이터베이스의 데이터를 볼 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 역할이 있어야 합니다.
- 원격 사용자 또는 그룹을 추가하려면 원격 인증을 사용하고 인증 서버를 구성해야 합니다.
- IdP(Identity Provider)가 그래픽 인터페이스에 액세스하는 사용자를 인증하도록 SAML 인증을 구성하려면 이러한 사용자가 "최종" 사용자로 정의되어 있는지 확인하십시오.

  SAML 인증이 활성화된 경우 ""local"" 또는 " main유지보수" 유형의 사용자는 UI에 액세스할 수 없습니다.

Windows Active Directory에서 그룹을 추가하면 중첩된 하위 그룹이 비활성화되지 않는 한 모든 직접 구성원과 중첩된 하위 그룹이 Unified Manager에 인증할 수 있습니다. OpenLDAP 또는 기타 인증 서비스에서 그룹을 추가하는 경우 해당 그룹의 직접 구성원만 Unified Manager에 인증할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 사용자 * 를 클릭합니다.
2. 사용자 페이지에서 * 추가 * 를 클릭합니다.
3. 사용자 추가 대화 상자에서 추가할 사용자 유형을 선택하고 필요한 정보를 입력합니다.

   필수 사용자 정보를 입력할 때는 해당 사용자에게 고유한 이메일 주소를 지정해야 합니다. 여러 사용자가 공유하는 전자 메일 주소는 지정하지 않아야 합니다.

4. 추가 * 를 클릭합니다.

데이터베이스 사용자 생성

Workflow Automation과 Unified Manager 간의 연결을 지원하거나 데이터베이스 보기에 액세스하려면 먼저 Unified Manager 웹 UI에서 통합 스키마 또는 보고서 스키마 역할을 사용하여 데이터베이스 사용자를 만들어야 합니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

데이터베이스 사용자는 Workflow Automation과 통합되어 보고서 관련 데이터베이스 뷰에 액세스할 수 있습니다. 데이터베이스 사용자는 Unified Manager 웹 UI 또는 유지보수 콘솔에 액세스할 수 없으며 API 호출을 실행할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 사용자 * 를 클릭합니다.
2. 사용자 페이지에서 * 추가 * 를 클릭합니다.

3. 사용자 추가 대화 상자의 * 유형 * 드롭다운 목록에서 * 데이터베이스 사용자 * 를 선택합니다.
4. 데이터베이스 사용자의 이름과 암호를 입력합니다.
5. 역할 * 드롭다운 목록에서 적절한 역할을 선택합니다.

만약...	이 역할을 선택하십시오
Unified Manager와 워크플로우 자동화 연결	통합 스키마
보고 및 기타 데이터베이스 보기에 액세스	보고서 스키마

6. 추가 * 를 클릭합니다.

사용자 설정 편집

각 사용자에게 지정된 전자 메일 주소 및 역할과 같은 사용자 설정을 편집할 수 있습니다. 예를 들어 스토리지 운영자 사용자의 역할을 변경하고 스토리지 관리자 권한을 사용자에게 할당할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

사용자에게 할당된 역할을 수정하면 다음 작업 중 하나가 발생할 때 변경 사항이 적용됩니다.

- 사용자가 로그아웃한 후 Unified Manager에 다시 로그인합니다.
- 24시간의 세션 시간 제한에 도달했습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 사용자 * 를 클릭합니다.
2. 사용자 페이지에서 설정을 편집할 사용자를 선택하고 * 편집 * 을 클릭합니다.
3. 사용자 편집 대화 상자에서 사용자에 대해 지정된 적절한 설정을 편집합니다.
4. 저장 * 을 클릭합니다.

사용자 보기

사용자 페이지에서 Unified Manager를 사용하여 스토리지 오브젝트 및 데이터를 관리하는 사용자 목록을 볼 수 있습니다. 사용자 이름, 사용자 유형, 전자 메일 주소, 사용자에게 할당된 역할 등 사용자에 대한 세부 정보를 볼 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 사용자 * 를 클릭합니다.

사용자 또는 그룹을 삭제하는 중입니다

특정 사용자가 Unified Manager에 액세스하지 못하도록 관리 서버 데이터베이스에서 사용자를 한 명 이상 삭제할 수 있습니다. 그룹의 모든 사용자가 더 이상 관리 서버에 액세스할 수 없도록 그룹을 삭제할 수도 있습니다.

- 필요한 것 *
- 원격 그룹을 삭제하는 경우 원격 그룹의 사용자에게 할당된 이벤트를 다시 할당해야 합니다.

  로컬 사용자 또는 원격 사용자를 삭제하는 경우 이러한 사용자에게 할당된 이벤트는 자동으로 할당되지 않습니다.

- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 사용자 * 를 클릭합니다.
2. 사용자 페이지에서 삭제할 사용자 또는 그룹을 선택한 다음 * 삭제 * 를 클릭합니다.
3. 예 * 를 클릭하여 삭제를 확인합니다.

RBAC란 무엇입니까

RBAC(역할 기반 액세스 제어)에서는 Active IQ Unified Manager 서버의 다양한 기능과 리소스에 액세스할 수 있는 사용자를 제어하는 기능을 제공합니다.

역할 기반 액세스 제어의 역할

역할 기반 액세스 제어(RBAC)를 통해 관리자는 역할을 정의하여 사용자 그룹을 관리할 수 있습니다. 선택한 관리자에게 특정 기능에 대한 액세스를 제한해야 하는 경우 해당 관리자에 대한 관리자 계정을 설정해야 합니다. 관리자가 볼 수 있는 정보와 관리자가 수행할 수 있는 작업을 제한하려면 사용자가 만든 관리자 계정에 역할을 적용해야 합니다.

관리 서버는 사용자 로그인 및 역할 권한에 RBAC를 사용합니다. 관리 사용자 액세스에 대한 관리 서버의 기본 설정을 변경하지 않은 경우 로그인할 필요가 없습니다.

특정 권한이 필요한 작업을 시작하면 관리 서버에 로그인하라는 메시지가 표시됩니다. 예를 들어 관리자 계정을 만들려면 응용 프로그램 관리자 계정 액세스 권한으로 로그인해야 합니다.

사용자 유형 정의

사용자 유형은 사용자가 보유하는 계정의 종류를 지정하며 원격 사용자, 원격 그룹, 로컬 사용자, 데이터베이스 사용자 및 유지 보수 사용자를 포함합니다. 이러한 각 유형에는 관리자 역할을 가진 사용자가 할당하는 고유한 역할이 있습니다.

Unified Manager 사용자 유형은 다음과 같습니다.

- * 유지보수 사용자 *

  Unified Manager의 초기 구성 중에 생성됩니다. 그러면 유지 보수 사용자가 추가 사용자를 생성하고 역할을

할당합니다. 유지보수 사용자는 유지보수 콘솔에 액세스할 수 있는 유일한 사용자입니다. Unified Manager를 Red Hat Enterprise Linux 또는 CentOS 시스템에 설치하면 유지 관리 사용자에게 사용자 이름 ""umadmin""이 지정됩니다.

- * 로컬 사용자 *

  Unified Manager UI에 액세스하고 유지보수 사용자 또는 애플리케이션 관리자 역할을 가진 사용자가 제공하는 역할에 따라 기능을 수행합니다.

- * 원격 그룹 *

  인증 서버에 저장된 자격 증명을 사용하여 Unified Manager UI에 액세스하는 사용자 그룹입니다. 이 계정의 이름은 인증 서버에 저장된 그룹의 이름과 일치해야 합니다. 원격 그룹 내의 모든 사용자는 개별 사용자 자격 증명을 사용하여 Unified Manager UI에 액세스할 수 있습니다. 원격 그룹은 할당된 역할에 따라 기능을 수행할 수 있습니다.

- * 원격 사용자 *

  인증 서버에 저장된 자격 증명을 사용하여 Unified Manager UI에 액세스합니다. 원격 사용자는 유지보수 사용자 또는 애플리케이션 관리자 역할을 가진 사용자가 제공한 역할에 따라 기능을 수행합니다.

- * 데이터베이스 사용자 *

  Unified Manager 데이터베이스의 데이터에 읽기 전용으로 액세스하고 Unified Manager 웹 인터페이스 또는 유지보수 콘솔에 액세스할 수 없으며 API 호출을 실행할 수 없습니다.

사용자 역할의 정의

유지보수 사용자 또는 애플리케이션 관리자는 모든 사용자에게 역할을 할당합니다. 각 역할에는 특정 권한이 포함됩니다. Unified Manager에서 수행할 수 있는 작업의 범위는 할당된 역할 및 역할에 포함된 권한에 따라 다릅니다.

Unified Manager에는 다음과 같은 사전 정의된 사용자 역할이 포함되어 있습니다.

- * 연산자 *

  기록 및 용량 추세를 비롯하여 Unified Manager에서 수집한 스토리지 시스템 정보 및 기타 데이터를 확인합니다. 스토리지 운영자는 이 역할을 사용하여 이벤트에 대한 메모를 확인, 할당, 확인, 해결 및 추가할 수 있습니다.

- * 스토리지 관리자 *

  Unified Manager 내에서 스토리지 관리 작업을 구성합니다. 스토리지 관리자는 이 역할을 통해 임계값을 구성하고 알림 및 기타 스토리지 관리 관련 옵션 및 정책을 생성할 수 있습니다.

- * 응용 프로그램 관리자 *

  스토리지 관리와 관련 없는 설정을 구성합니다. 이 역할을 통해 사용자, 보안 인증서, 데이터베이스 액세스 및 인증을 포함한 관리 옵션을 관리할 수 있습니다. SMTP, 네트워킹 및 AutoSupport.

  Linux 시스템에 Unified Manager를 설치하면 애플리케이션 관리자 역할을 가진 초기 사용자 이름이 자동으로 ""umadmin""으로 지정됩니다.

- * 통합 스키마 *

  WFA(Unified Manager)와 OnCommand Workflow Automation(Unified Manager)를 통합할 수 있도록 Unified Manager 데이터베이스 보기에 대한 읽기 전용 액세스를 지원합니다.

- * 보고서 스키마 *

  이 역할은 Unified Manager 데이터베이스에서 직접 보고 및 기타 데이터베이스 뷰에 대한 읽기 전용 액세스를 지원합니다. 볼 수 있는 데이터베이스는 다음과 같습니다.

  - NetApp_모델_뷰
  - netapp_performance
  - ocum
  - ocum_report 를 참조하십시오
  - ocum_report_bRT
  - OPM
  - 스케일로토르

Unified Manager 사용자 역할 및 기능

할당된 사용자 역할에 따라 Unified Manager에서 수행할 수 있는 작업을 결정할 수 있습니다.

다음 표에는 각 사용자 역할이 수행할 수 있는 기능이 나와 있습니다.

기능	운영자	스토리지 관리자	응용 프로그램 관리자	통합 스키마	보고서 스키마
스토리지 시스템 정보를 봅니다	•	•	•	•	•
기록 및 용량 추세와 같은 다른 데이터를 봅니다	•	•	•	•	•
이벤트 보기, 할당 및 해결	•	•	•		
SVM 협회 및 리소스 풀과 같은 스토리지 서비스 객체를 확인합니다	•	•	•		
임계값 정책을 봅니다	•	•	•		

기능	운영자	스토리지 관리자	응용 프로그램 관리자	통합 스키마	보고서 스키마
SVM 협회 및 리소스 풀과 같은 스토리지 서비스 객체를 관리합니다		•	•		
알림을 정의합니다		•	•		
스토리지 관리 옵션을 관리합니다		•	•		
스토리지 관리 정책 관리		•	•		
사용자 관리			•		
관리 옵션을 관리합니다			•		
임계값 정책을 정의합니다			•		
데이터베이스 액세스를 관리합니다			•		
WFA와의 통합을 관리하고 데이터베이스 뷰에 대한 액세스를 제공합니다				•	
보고서 예약 및 저장		•	•		
관리 조치로부터 "Fix it" 작업을 실행합니다		•	•		
데이터베이스 보기에 대한 읽기 전용 액세스를 제공합니다					•

SAML 인증 설정 관리

원격 인증 설정을 구성한 후에는 SAML(Security Assertion Markup Language) 인증을 설정하여 원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 IDP(Secure Identity Provider)에 의해 인증되도록 할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자 및 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지보수 콘솔에 액세스하는 사용자에게 영향을 주지 않습니다.

ID 공급자 요구 사항

ID 공급자(IDP)를 사용하여 모든 원격 사용자에 대해 SAML 인증을 수행하도록 Unified Manager를 구성하는 경우 Unified Manager에 성공적으로 연결되도록 몇 가지 필수 구성 설정을 알고 있어야 합니다.

IDP 서버에 Unified Manager URI 및 메타데이터를 입력해야 합니다. 이 정보는 Unified ManagerSAML 인증 페이지에서 복사할 수 있습니다. Unified Manager는 SAML(Security Assertion Markup Language) 표준의 서비스 공급자(SP)로 간주됩니다.

지원되는 암호화 표준

- AES(고급 암호화 표준): AES-128 및 AES-256
- 보안 해시 알고리즘(SHA): SHA-1 및 SHA-256

검증된 **ID** 공급자

- 시바볼레스
- ADFS(Active Directory Federation Services)

ADFS 구성 요구 사항

- Unified Manager가 이 기반 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 청구 규칙을 다음 순서로 정의해야 합니다.

청구 규칙	값
SAM-계정-이름	이름 ID입니다
SAM-계정-이름	urn:OID: 0.9.2342.19200300.100.1.1
토큰 그룹 — 비정규화된 이름	urn:OID: 1.3.6.1.4.1.5923.1.5.1.1

- 인증 방법을 ""양식 인증""으로 설정해야 합니다. 그렇지 않을 경우 Unified Manager에서 로그아웃할 때 사용자에게 오류가 발생할 수 있습니다. 다음 단계를 수행하십시오.
  a. ADFS 관리 콘솔을 엽니다.

b. 왼쪽 트리 뷰에서 Authentication Policies 폴더를 클릭합니다.

c. 오른쪽의 작업 에서 글로벌 기본 인증 정책 편집 을 클릭합니다.

d. 인트라넷 인증 방법을 기본값인 "Windows 인증" 대신 " 양식 인증"으로 설정합니다.

- 경우에 따라 Unified Manager 보안 인증서가 CA 서명되면 IDP를 통한 로그인이 거부됩니다. 이 문제를 해결하기 위한 두 가지 해결 방법이 있습니다.
  - 링크에 나와 있는 지침에 따라 연결된 CA 인증자에 대한 ADFS 서버의 해지 확인을 비활성화합니다.

    "신뢰할 수 있는 당사자 신뢰에 따라 해지 확인을 비활성화합니다"

  - CA 서버가 ADFS 서버 내에 상주하여 Unified Manager 서버 인증서 요청에 서명하도록 합니다.

기타 구성 요구 사항

- Unified Manager 시간 차이는 5분으로 설정되어 있으므로 IDP 서버와 Unified Manager 서버 간의 시간 차이는 5분 이내이거나 인증이 실패합니다.

SAML 인증을 사용하도록 설정합니다

SAML(Security Assertion Markup Language) 인증을 사용하면 원격 사용자가 Unified Manager 웹 UI에 액세스하기 전에 IDP(Secure Identity Provider)에서 인증을 받을 수 있습니다.

- 필요한 것 *
- 원격 인증을 구성하고 성공적으로 수행되었는지 확인해야 합니다.
- 애플리케이션 관리자 역할을 사용하여 하나 이상의 원격 사용자 또는 원격 그룹을 만들어야 합니다.
- IDP(Identity Provider)는 Unified Manager에서 지원해야 하며 구성해야 합니다.
- IDP URL 및 메타데이터가 있어야 합니다.
- IDP 서버에 대한 액세스 권한이 있어야 합니다.

Unified Manager에서 SAML 인증을 설정한 후에는 IDP가 Unified Manager 서버 호스트 정보로 구성될 때까지 사용자가 그래픽 사용자 인터페이스에 액세스할 수 없습니다. 따라서 구성 프로세스를 시작하기 전에 연결의 두 부분을 모두 완료할 수 있도록 준비해야 합니다. IDP는 Unified Manager를 구성하기 전이나 후에 구성할 수 있습니다.

SAML 인증이 활성화된 후에는 원격 사용자만 Unified Manager 그래픽 사용자 인터페이스에 액세스할 수 있습니다. 로컬 사용자 및 유지 관리 사용자는 UI에 액세스할 수 없습니다. 이 구성은 유지보수 콘솔, Unified Manager 명령 또는 ZAPI에 액세스하는 사용자에게는 영향을 주지 않습니다.

이 페이지에서 SAML 구성을 완료하면 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * SAML 인증 * 을 클릭합니다.
2. SAML 인증 활성화 * 확인란을 선택합니다.

   IDP 연결을 구성하는 데 필요한 필드가 표시됩니다.

3. Unified Manager 서버를 IDP 서버에 연결하는 데 필요한 IDP URI 및 IDP 메타데이터를 입력합니다.

   IDP 서버에 Unified Manager 서버에서 직접 액세스할 수 있는 경우 IDP URI를 입력한 후 * Fetch IDP Metadata * 버튼을 클릭하여 IDP 메타데이터 필드를 자동으로 채울 수 있습니다.

4. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.

   이 정보를 사용하여 IDP 서버를 구성할 수 있습니다.

5. 저장 * 을 클릭합니다.

   구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

6. 확인 및 로그아웃 * 을 클릭하면 Unified Manager가 다시 시작됩니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 Unified Manager 로그인 페이지 대신 IDP 로그인 페이지에 자격 증명을 입력합니다.

아직 완료되지 않은 경우 IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.

ID 공급자로 ADFS를 사용하는 경우 Unified Manager GUI는 ADFS 시간 제한을 적용하지 않으며 Unified Manager 세션 시간 제한에 도달할 때까지 계속 작동합니다. GUI 세션 시간 초과는 * 일반 * > * 기능 설정 * > * 비활성 시간 초과 * 를 클릭하여 변경할 수 있습니다.

SAML 인증에 사용되는 ID 공급자를 변경합니다

Unified Manager에서 원격 사용자를 인증하는 데 사용하는 IDP(ID 공급자)를 변경할 수 있습니다.

- 필요한 것 *
- IDP URL 및 메타데이터가 있어야 합니다.
- IDP에 대한 액세스 권한이 있어야 합니다.

Unified Manager를 구성하기 전이나 후에 새 IDP를 구성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * SAML 인증 * 을 클릭합니다.
2. Unified Manager 서버를 IDP에 연결하는 데 필요한 새 IDP URI 및 IDP 메타데이터를 입력합니다.

   IDP가 Unified Manager 서버에서 직접 액세스할 수 있는 경우 IDP URL을 입력한 후 * Fetch IDP Metadata * 버튼을 클릭하여 IDP 메타데이터 필드를 자동으로 채울 수 있습니다.

3. Unified Manager 메타데이터 URI를 복사하거나 메타데이터를 XML 텍스트 파일에 저장합니다.
4. 구성 저장 * 을 클릭합니다.

   구성을 변경할 것인지 확인하는 메시지 상자가 표시됩니다.

5. 확인 * 을 클릭합니다.

새 IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.

다음에 권한이 있는 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 이전 IDP 로그인 페이지 대신 새 IDP 로그인 페이지에 자격 증명을 입력합니다.

Unified Manager 보안 인증서 변경 후 SAML 인증 설정을 업데이트하는 중입니다

Unified Manager 서버에 설치된 HTTPS 보안 인증서를 변경하려면 SAML 인증 구성 설정을 업데이트해야 합니다. 호스트 시스템의 이름을 바꾸거나 호스트 시스템에 새 IP 주소를 할당하거나 시스템에 대한 보안 인증서를 수동으로 변경하면 인증서가 업데이트됩니다.

보안 인증서가 변경되고 Unified Manager 서버가 다시 시작되면 SAML 인증이 작동하지 않고 사용자가 Unified Manager 그래픽 인터페이스에 액세스할 수 없습니다. 사용자 인터페이스에 대한 액세스를 다시 활성화하려면 IDP 서버 및 Unified Manager 서버 모두에서 SAML 인증 설정을 업데이트해야 합니다.

단계

1. 유지보수 콘솔에 로그인합니다.
2. 주 메뉴 * 에서 * SAML 인증 비활성화 * 옵션에 대한 번호를 입력합니다.

   SAML 인증을 비활성화하고 Unified Manager를 다시 시작할지 확인하는 메시지가 표시됩니다.

3. 업데이트된 FQDN 또는 IP 주소를 사용하여 Unified Manager 사용자 인터페이스를 시작하고, 업데이트된 서버 인증서를 브라우저에 적용하고, 유지 관리 사용자 자격 증명을 사용하여 로그인합니다.
4. 설정/인증 * 페이지에서 * SAML 인증 * 탭을 선택하고 IDP 연결을 구성합니다.
5. Unified Manager 호스트 메타데이터 URI를 복사하거나 호스트 메타데이터를 XML 텍스트 파일에 저장합니다.
6. 저장 * 을 클릭합니다.

   구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

7. 확인 및 로그아웃 * 을 클릭하면 Unified Manager가 다시 시작됩니다.
8. IDP 서버에 액세스한 다음 Unified Manager 서버 URI 및 메타데이터를 입력하여 구성을 완료합니다.

ID 공급자	구성 단계
고급	a. ADFS 관리 GUI에서 기존 기반 당사자 신뢰 항목을 삭제합니다. b. 업데이트된 Unified Manager 서버의 'saML_sp_metadata.xml'을 사용하여 새로운 신뢰할 수 있는 당사자 항목을 추가합니다. c. Unified Manager가 이 기반 당사자 신뢰 항목에 대한 ADFS SAML 응답을 구문 분석하는 데 필요한 세 가지 클레임 규칙을 정의합니다. d. ADFS Windows 서비스를 다시 시작합니다.

ID 공급자	구성 단계
시바볼레스	a. Unified Manager 서버의 새 FQDN을 attribute-filter.xml과 reying-party.xml 파일로 업데이트합니다. b. Apache Tomcat 웹 서버를 다시 시작하고 포트 8005가 온라인 상태가 될 때까지 기다립니다.

9. Unified Manager에 로그인하고 IdP를 통해 SAML 인증이 예상대로 작동하는지 확인합니다.

SAML 인증을 사용하지 않도록 설정합니다

Unified Manager 웹 UI에 로그인하기 전에 IDP(Secure Identity Provider)를 통해 원격 사용자 인증을 중지하려면 SAML 인증을 사용하지 않도록 설정할 수 있습니다. SAML 인증이 비활성화된 경우 Active Directory 또는 LDAP와 같이 구성된 디렉토리 서비스 공급자가 로그온 인증을 수행합니다.

SAML 인증을 비활성화하면 로컬 사용자 및 유지 관리 사용자가 구성된 원격 사용자 외에 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

그래픽 사용자 인터페이스에 액세스할 수 없는 경우 Unified Manager 유지보수 콘솔을 사용하여 SAML 인증을 비활성화할 수도 있습니다.

SAML 인증이 비활성화된 후 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * SAML 인증 * 을 클릭합니다.
2. SAML 인증 활성화 * 확인란의 선택을 취소합니다.
3. 저장 * 을 클릭합니다.

   구성을 완료하고 Unified Manager를 다시 시작할지 확인하는 메시지 상자가 표시됩니다.

4. 확인 및 로그아웃 * 을 클릭하면 Unified Manager가 다시 시작됩니다.

다음 번에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 IDP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력합니다.

IDP에 액세스하고 Unified Manager 서버 URI 및 메타데이터를 삭제합니다.

유지 관리 콘솔에서 SAML 인증을 사용하지 않도록 설정합니다

Unified Manager GUI에 액세스할 수 없는 경우 유지보수 콘솔에서 SAML 인증을 비활성화해야 할 수 있습니다. 이는 구성이 잘못되거나 IDP에 액세스할 수 없는 경우에 발생할 수 있습니다.

- 필요한 것 *

유지보수 사용자로서 유지보수 콘솔에 액세스할 수 있어야 합니다.

SAML 인증이 비활성화된 경우 Active Directory 또는 LDAP와 같이 구성된 디렉토리 서비스 공급자가 로그온 인증을 수행합니다. 로컬 사용자 및 유지 관리 사용자는 구성된 원격 사용자 외에도 그래픽 사용자 인터페이스에 액세스할 수 있습니다.

UI의 설정/인증 페이지에서 SAML 인증을 비활성화할 수도 있습니다.

SAML 인증이 비활성화된 후 Unified Manager가 자동으로 다시 시작됩니다.

단계

1. 유지보수 콘솔에 로그인합니다.
2. 주 메뉴 * 에서 * SAML 인증 비활성화 * 옵션에 대한 번호를 입력합니다.

   SAML 인증을 비활성화하고 Unified Manager를 다시 시작할지 확인하는 메시지가 표시됩니다.

3. y * 를 입력한 다음 Enter 키를 누르면 Unified Manager가 다시 시작됩니다.

다음 번에 원격 사용자가 Unified Manager 그래픽 인터페이스에 액세스하려고 할 때 IDP 로그인 페이지 대신 Unified Manager 로그인 페이지에 자격 증명을 입력합니다.

필요한 경우 IDP에 액세스하고 Unified Manager 서버 URL 및 메타데이터를 삭제합니다.

SAML 인증 페이지

SAML 인증 페이지를 사용하면 Unified Manager 웹 UI에 로그인하기 전에 IdP(Secure Identity Provider)를 통해 SAML을 사용하여 원격 사용자를 인증하도록 Unified Manager를 구성할 수 있습니다.

- SAML 구성을 생성하거나 수정하려면 애플리케이션 관리자 역할이 있어야 합니다.
- 원격 인증을 구성해야 합니다.
- 하나 이상의 원격 사용자 또는 원격 그룹을 구성해야 합니다.

원격 인증 및 원격 사용자를 구성한 후 SAML 인증 활성화 확인란을 선택하여 보안 ID 공급자를 사용하여 인증을 활성화할 수 있습니다.

- * IDP URI *

  Unified Manager 서버에서 IDP에 액세스하기 위한 URI입니다. URI의 예는 다음과 같습니다.

  ADFS 예제 URI:

  (https://win2016-dc.ntap2016.local/federationmetadata/2007-06/federationmetadata.xml`)

  Shibboleth 예제 URI:

  (https://centos7.ntap2016.local/idp/shibboleth`)

- * IDP 메타데이터 *

  XML 형식의 IDP 메타데이터

Unified Manager 서버에서 IDP URL에 액세스할 수 있는 경우 * Fetch IDP Metadata * 버튼을 클릭하여 이 필드를 채울 수 있습니다.

- * 호스트 시스템(FQDN) *

  설치 중에 정의된 Unified Manager 호스트 시스템의 FQDN입니다. 필요한 경우 이 값을 변경할 수 있습니다.

- * 호스트 URI *

  IDP에서 Unified Manager 호스트 시스템에 액세스하기 위한 URI입니다.

- * 호스트 메타데이터 *

  XML 형식의 호스트 시스템 메타데이터

인증 관리

Unified Manager 서버에서 LDAP 또는 Active Directory를 사용하여 인증을 설정하고 서버와 함께 작동하도록 구성하여 원격 사용자를 인증할 수 있습니다.

원격 인증 활성화, 인증 서비스 설정 및 인증 서버 추가에 대한 자세한 내용은 * Unified Manager에서 경고 알림을 보내도록 구성 * 의 이전 섹션을 참조하십시오.

인증 서버 편집

Unified Manager 서버가 인증 서버와 통신하는 데 사용하는 포트를 변경할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 중첩된 그룹 조회 사용 안 함 * 상자를 선택합니다.
3. Authentication Servers * 영역에서 편집할 인증 서버를 선택한 다음 * Edit * 를 클릭합니다.
4. 인증 서버 편집 * 대화 상자에서 포트 세부 정보를 편집합니다.
5. 저장 * 을 클릭합니다.

인증 서버를 삭제하는 중입니다

Unified Manager 서버가 인증 서버와 통신하지 못하도록 하려면 인증 서버를 삭제할 수 있습니다. 예를 들어 관리 서버가 통신하는 인증 서버를 변경하려는 경우 인증 서버를 삭제하고 새 인증 서버를 추가할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

인증 서버를 삭제하면 인증 서버의 원격 사용자 또는 그룹이 Unified Manager에 더 이상 액세스할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
2. 삭제할 인증 서버를 하나 이상 선택한 다음 * 삭제 * 를 클릭합니다.
3. 예 * 를 클릭하여 삭제 요청을 확인합니다.

   보안 연결 사용 * 옵션을 활성화하면 인증 서버와 연관된 인증서가 인증 서버와 함께 삭제됩니다.

Active Directory 또는 OpenLDAP를 사용한 인증

관리 서버에서 원격 인증을 사용하도록 설정하고 인증 서버 내의 사용자가 Unified Manager에 액세스할 수 있도록 인증 서버와 통신하도록 관리 서버를 구성할 수 있습니다.

다음 미리 정의된 인증 서비스 중 하나를 사용하거나 고유한 인증 서비스를 지정할 수 있습니다.

- Microsoft Active Directory를 클릭합니다

  Microsoft Lightweight Directory Services는 사용할 수 없습니다.

- OpenLDAP를 클릭합니다

필요한 인증 서비스를 선택하고 적절한 인증 서버를 추가하여 인증 서버의 원격 사용자가 Unified Manager에 액세스할 수 있도록 할 수 있습니다. 원격 사용자 또는 그룹에 대한 자격 증명은 인증 서버에서 관리합니다. 관리 서버는 LDAP(Lightweight Directory Access Protocol)를 사용하여 구성된 인증 서버 내에서 원격 사용자를 인증합니다.

Unified Manager에서 만든 로컬 사용자의 경우 관리 서버에서 사용자 이름과 암호 데이터베이스를 자체적으로 유지 관리합니다. 관리 서버는 인증을 수행하고 Active Directory 또는 OpenLDAP를 인증에 사용하지 않습니다.

로깅 감사

감사 로그를 사용하여 감사 로그가 손상되었는지 여부를 감지할 수 있습니다. 사용자가 수행하는 모든 작업은 감사 로그에 모니터링 및 기록됩니다. 감사는 Active IQ Unified Manager의 모든 사용자 인터페이스 및 공개적으로 노출된 API 기능에 대해 수행됩니다.

감사 로그: 파일 보기 * 를 사용하여 Active IQ Unified Manager에서 사용 가능한 모든 감사 로그 파일을 보고 액세스할 수 있습니다. Audit Log: File View(감사 로그: 파일 보기)의 파일은 생성 날짜를 기준으로 나열됩니다. 이 보기에는 설치 또는 업그레이드 시 캡처된 모든 감사 로그의 정보가 시스템에 있는 것으로 표시됩니다. Unified Manager에서 작업을 수행할 때마다 정보가 업데이트되고 로그에서 사용할 수 있습니다. 각 로그 파일의 상태는 로그 파일의 변조 또는 삭제를 감지하기 위해 능동적으로 모니터링되는 ""파일 무결성 상태"" 속성을 사용하여 캡처됩니다. 시스템에서 감사 로그를 사용할 수 있는 경우 감사 로그에 다음 상태 중 하나가 포함될 수 있습니다.

상태	설명
활성	로그가 현재 로그되고 있는 파일입니다.
정상	비활성, 압축 및 시스템에 저장된 파일입니다.

상태	설명
변조되었습니다	파일을 수동으로 편집한 사용자에 의해 손상된 파일입니다.
manual_delete(수동 삭제)	권한이 있는 사용자가 삭제한 파일입니다.
롤오버_삭제	롤링 구성 정책에 따라 롤오프로 인해 삭제된 파일입니다.
Unexpected_delete를 선택합니다	알 수 없는 이유로 삭제된 파일입니다.

감사 로그 페이지에는 다음과 같은 명령 단추가 있습니다.

- 구성
- 삭제
- 다운로드

delete * 버튼을 사용하면 Audit Logs 보기에 나열된 감사 로그를 삭제할 수 있습니다. 감사 로그를 삭제하고 나중에 유효한 삭제를 확인하는 데 도움이 되는 파일을 삭제할 이유를 선택적으로 제공할 수 있습니다. Reason 열에는 삭제 작업을 수행한 사용자의 이름과 함께 이유가 나열됩니다.

로그 파일을 삭제하면 시스템에서 파일이 삭제되지만 DB 테이블의 항목은 삭제되지 않습니다.

감사 로그 섹션의 * 다운로드 * 버튼을 사용하여 Active IQ Unified Manager에서 감사 로그를 다운로드하고 감사 로그 파일을 내보낼 수 있습니다. "보통" 또는 "무단 변경"으로 표시된 파일은 압축된 .gzip 형식으로 다운로드됩니다.

감사 로그 파일은 주기적으로 보관되며 참조를 위해 데이터베이스에 저장됩니다. 보관 전에 보안 및 무결성을 유지하기 위해 감사 로그에 디지털 서명됩니다.

전체 AutoSupport 번들이 생성되면 지원 번들에는 아카이빙 및 액티브 감사 로그 파일이 모두 포함됩니다. 하지만 간단한 지원 번들이 생성되면 활성 감사 로그만 포함됩니다. 보관된 감사 로그는 포함되지 않습니다.

감사 로그 구성

감사 로그 섹션의 * 구성 * 버튼을 사용하여 감사 로그 파일에 대한 롤링 정책을 구성하고 감사 로그에 대한 원격 로깅을 활성화할 수 있습니다.

시스템에 저장할 데이터의 양과 빈도에 따라 * MAX 파일 크기 * 및 * 감사 로그 보존 일 * 의 값을 설정할 수 있습니다. 필드 * 총 감사 로그 크기 * 의 값은 시스템에 있는 총 감사 로그 데이터의 크기입니다. 롤오버 정책은 * 감사 로그 보존 기간 *, * 최대 파일 크기 * 및 * 총 감사 로그 크기 * 필드의 값에 따라 결정됩니다. 감사 로그 백업의 크기가 * TOTAL AUDIT LOG SIZE * 에 구성된 값에 도달하면 먼저 아카이빙된 파일이 삭제됩니다. 즉, 가장 오래된 파일이 삭제됩니다. 그러나 파일 항목은 데이터베이스에서 계속 사용할 수 있으며 ""롤오버 삭제""로 표시됩니다. 감사 로그 보존 기간 * 값은 감사 로그 파일이 보존되는 일수입니다. 이 필드에 설정된 값보다 오래된 파일은 롤오버됩니다.

단계

1. 감사 로그 * >> * 구성 * 을 클릭합니다.
2. 최대 파일 크기 *, * 총 감사 로그 크기 * 및 * 감사 로그 보존 기간 * 에 값을 입력합니다.

원격 로깅을 활성화하려면 * 원격 로깅 사용 * 을 선택해야 합니다.

감사 로그의 원격 로깅을 사용하도록 설정합니다

감사 로그 구성 대화 상자에서 * 원격 로깅 사용 * 확인란을 선택하여 원격 감사 로깅을 활성화할 수 있습니다. 이 기능을 사용하여 감사 로그를 원격 Syslog 서버로 전송할 수 있습니다. 이렇게 하면 공간 제약 조건이 있을 때 감사 로그를 관리할 수 있습니다.

감사 로그의 원격 로깅은 Active IQ Unified Manager 서버의 감사 로그 파일이 변조될 경우에 대비하여 변조 불가능한 백업을 제공합니다.

단계

1. 감사 로그 구성 * 대화 상자에서 * 원격 로깅 사용 * 확인란을 선택합니다.

   원격 로깅을 구성하는 추가 필드가 표시됩니다.

2. 연결할 원격 서버의 * HOSTNAME * 및 * 포트 * 를 입력합니다.
3. server CA certificate * 필드에서 * browse * 를 클릭하여 대상 서버의 공용 인증서를 선택합니다.

   인증서는 '.pem' 형식으로 업로드되어야 합니다. 이 인증서는 대상 Syslog 서버에서 받아야 하며 만료되지 않아야 합니다. 인증서는 선택한 "hostname"을 'subjectAltName'(SAN) 속성의 일부로 포함해야 합니다.

4. * CHARSET *, * CONNECTION TIMEOUT *, * 재연결 지연 * 필드에 값을 입력합니다.

   이러한 필드의 값은 밀리초 단위입니다.

5. 필요한 Syslog 형식과 TLS 프로토콜 버전을 * format * 및 * protocol * 필드에서 선택합니다.
6. 대상 Syslog 서버에 인증서 기반 인증이 필요한 경우 * 클라이언트 인증 활성화 * 확인란을 선택합니다.

   감사 로그 구성을 저장하기 전에 클라이언트 인증 인증서를 다운로드하여 Syslog 서버에 업로드해야 합니다. 그렇지 않으면 연결이 실패합니다. Syslog 서버의 유형에 따라 클라이언트 인증 인증서의 해시를 만들어야 할 수도 있습니다.

   예: syslog-ng를 사용하려면 ' openssl x509 -noout -hash -in cert.pem' 명령을 사용하여 인증서의 <hash>를 만들어야 합니다. 그런 다음 클라이언트 인증 인증서를 <hash>.0 뒤에 명명된 파일에 상징적으로 연결해야 합니다.

7. 저장 * 을 클릭하여 서버와의 연결을 구성하고 원격 로깅을 활성화합니다.

   감사 로그 페이지로 리디렉션됩니다.

> 연결 시간 초과 * 값은 구성에 영향을 줄 수 있습니다. 설정에 정의된 값보다 응답하는 데 시간이 오래 걸리는 경우 연결 오류로 인해 구성 오류가 발생할 수 있습니다. 성공적으로 연결하려면 * 연결 시간 초과 * 값을 늘리고 구성을 다시 시도하십시오.

원격 인증 페이지

원격 인증 페이지를 사용하여 Unified Manager 웹 UI에 로그인하려는 원격 사용자를 인증하도록 Unified Manager를 인증 서버와 통신하도록 구성할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

원격 인증 활성화 확인란을 선택한 후 인증 서버를 사용하여 원격 인증을 활성화할 수 있습니다.

- * 인증 서비스 *

  Active Directory, OpenLDAP 등의 디렉터리 서비스 공급자에서 사용자를 인증하도록 관리 서버를 구성하거나 고유한 인증 메커니즘을 지정할 수 있습니다. 원격 인증을 설정한 경우에만 인증 서비스를 지정할 수 있습니다.

  - * Active Directory *
    - 관리자 이름

      인증 서버의 관리자 이름을 지정합니다.

    - 암호

      인증 서버에 액세스할 암호를 지정합니다.

    - 기본 고유 이름

      인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com +인 경우 기본 고유 이름은 * cn=ou, dc=domain, dc=com * 입니다.

    - 중첩된 그룹 조회를 비활성화합니다

      중첩 그룹 조회 옵션을 사용할지 여부를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩된 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

    - 보안 연결을 사용합니다

      인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.

  - * OpenLDAP *
    - 고유 이름 바인딩

      인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인딩 고유 이름을 지정합니다.

    - 바인딩 암호

      인증 서버에 액세스할 암호를 지정합니다.

    - 기본 고유 이름

      인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com +인 경우 기본 고유 이름은 * cn=ou, dc=domain, dc=com * 입니다.

    - 보안 연결을 사용합니다

      LDAP 인증 서버와 통신하는 데 Secure LDAP를 사용하도록 지정합니다.

  - 기타 *

- 고유 이름 바인딩

  구성한 인증 서버에서 원격 사용자를 찾기 위해 기본 고유 이름과 함께 사용되는 바인딩 고유 이름을 지정합니다.

- 바인딩 암호

  인증 서버에 액세스할 암호를 지정합니다.

- 기본 고유 이름

  인증 서버에서 원격 사용자의 위치를 지정합니다. 예를 들어 인증 서버의 도메인 이름이 +ou@domain.com +인 경우 기본 고유 이름은 * cn=ou, dc=domain, dc=com * 입니다.

- 프로토콜 버전

  인증 서버에서 지원하는 LDAP(Lightweight Directory Access Protocol) 버전을 지정합니다. 프로토콜 버전을 자동으로 감지할지 또는 버전을 2나 3으로 설정할지 지정할 수 있습니다.

- 사용자 이름 특성

  관리 서버에서 인증할 사용자 로그인 이름이 포함된 인증 서버의 속성 이름을 지정합니다.

- 그룹 구성원 자격 특성

  사용자의 인증 서버에 지정된 속성 및 값을 기반으로 관리 서버 그룹 구성원 자격을 원격 사용자에게 할당하는 값을 지정합니다.

- UGID

  원격 사용자가 인증 서버에 groupOfUniqueNames 개체의 구성원으로 포함된 경우 이 옵션을 사용하면 해당 groupOfUniqueNames 개체의 지정된 속성에 따라 관리 서버 그룹 구성원을 원격 사용자에게 할당할 수 있습니다.

- 중첩된 그룹 조회를 비활성화합니다

  중첩 그룹 조회 옵션을 사용할지 여부를 지정합니다. 기본적으로 이 옵션은 비활성화되어 있습니다. Active Directory를 사용하는 경우 중첩된 그룹에 대한 지원을 비활성화하여 인증 속도를 높일 수 있습니다.

- 회원

  인증 서버가 그룹의 개별 구성원에 대한 정보를 저장하는 데 사용하는 속성 이름을 지정합니다.

- 사용자 객체 클래스

  원격 인증 서버에 있는 사용자의 개체 클래스를 지정합니다.

- 그룹 객체 클래스

  원격 인증 서버에 있는 모든 그룹의 객체 클래스를 지정합니다.

Member, *User* 개체 클래스 및 *Group* 개체 클래스 속성에 입력하는 값은 Active Directory, OpenLDAP 및 LDAP 구성에 추가된 값과 같아야 합니다. 그렇지 않으면 인증에 실패할 수 있습니다.

- 보안 연결을 사용합니다

  인증 서버와 통신하는 데 사용되는 인증 서비스를 지정합니다.

인증 서비스를 수정하려면 기존 인증 서버를 삭제하고 새 인증 서버를 추가해야 합니다.

Authentication Servers 영역

인증 서버 영역에는 관리 서버가 원격 사용자를 찾고 인증하기 위해 통신하는 인증 서버가 표시됩니다. 원격 사용자 또는 그룹에 대한 자격 증명은 인증 서버에서 관리합니다.

- * 명령 버튼 *

  인증 서버를 추가, 편집 또는 삭제할 수 있습니다.

  ◦ 추가

  인증 서버를 추가할 수 있습니다.

  추가하려는 인증 서버가 같은 데이터베이스를 사용하는 고가용성 쌍의 일부인 경우 파트너 인증 서버를 추가할 수도 있습니다. 이렇게 하면 인증 서버 중 하나에 연결할 수 없을 때 관리 서버가 파트너와 통신할 수 있습니다.

  ◦ 편집

  선택한 인증 서버에 대한 설정을 편집할 수 있습니다.

  ◦ 삭제

  선택한 인증 서버를 삭제합니다.

- * 이름 또는 IP 주소 *

  관리 서버에서 사용자를 인증하는 데 사용되는 인증 서버의 호스트 이름 또는 IP 주소를 표시합니다.

- * 포트 *

  인증 서버의 포트 번호를 표시합니다.

- * 인증 테스트 *

  이 단추는 원격 사용자 또는 그룹을 인증하여 인증 서버 구성을 확인합니다.

  테스트하는 동안 사용자 이름만 지정하면 관리 서버가 인증 서버에서 원격 사용자를 검색하지만 사용자를 인증하지는 않습니다. 사용자 이름과 암호를 모두 지정하면 관리 서버가 원격 사용자를 검색하고 인증합니다.

  원격 인증이 비활성화되어 있으면 인증을 테스트할 수 없습니다.

보안 인증서 관리

Unified Manager 서버에서 HTTPS를 구성하여 보안 연결을 통해 클러스터를 모니터링하고 관리할 수 있습니다.

HTTPS 보안 인증서 보기

HTTPS 인증서 세부 정보를 브라우저에서 검색된 인증서와 비교하여 브라우저가 Unified Manager에 암호화된 연결을 가로채 가로채지 않도록 할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

인증서를 보면 다시 생성된 인증서의 내용을 확인하거나 Unified Manager에 액세스할 수 있는 주체 대체 이름(SAN)을 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * HTTPS 인증서 * 를 클릭합니다.

   HTTPS 인증서는 페이지 맨 위에 표시됩니다

HTTPS 인증서 페이지에 표시된 것보다 보안 인증서에 대한 자세한 정보를 보려면 브라우저에서 연결 인증서를 볼 수 있습니다.

HTTPS 인증서 서명 요청을 다운로드하는 중입니다

서명할 인증 기관에 파일을 제공할 수 있도록 현재 HTTPS 보안 인증서에 대한 인증 서명 요청을 다운로드할 수 있습니다. CA 서명 인증서는 끼어들기 공격을 방지하고 자체 서명된 인증서보다 향상된 보안 보호를 제공합니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * HTTPS 인증서 * 를 클릭합니다.
2. HTTPS 인증서 서명 요청 다운로드 * 를 클릭합니다.
3. '<hostname>.csr' 파일을 저장합니다.

서명하도록 인증 기관에 파일을 제공한 다음 서명된 인증서를 설치할 수 있습니다.

서명되고 반환된 HTTPS 인증서를 설치하는 중입니다

인증 기관이 서명하여 반환한 후에 보안 인증서를 업로드 및 설치할 수 있습니다. 업로드 및 설치하는 파일은 자체 서명된 기존 인증서의 서명된 버전이어야 합니다. CA 서명 인증서는 끼어들기 공격을 방지하고 자체 서명된 인증서보다 더 나은 보안 보호를 제공합니다.

• 필요한 것 *

다음 작업을 완료해야 합니다.

- 인증서 서명 요청 파일을 다운로드하고 인증 기관에서 서명했습니다
- 인증서 체인을 PEM 형식으로 저장했습니다
- 중간 인증서를 비롯하여 Unified Manager 서버 인증서에서 루트 서명 인증서까지 체인에 있는 모든 인증서가 포함됩니다

애플리케이션 관리자 역할이 있어야 합니다.

CSR이 생성된 인증서의 유효 기간이 397일 이상인 경우 CA가 인증서를 서명 및 반환하기 전에 유효 기간을 397일로 줄입니다

단계

1. 왼쪽 탐색 창에서 * 일반 * > * HTTPS 인증서 * 를 클릭합니다.
2. HTTPS 인증서 설치 * 를 클릭합니다.
3. 표시되는 대화 상자에서 * 파일 선택… * 을 클릭하여 업로드할 파일을 찾습니다.
4. 파일을 선택한 다음 * 설치 * 를 클릭하여 파일을 설치합니다.

   자세한 내용은 을 참조하십시오 "외부 도구를 사용하여 생성된 HTTPS 인증서 설치".

인증서 체인의 예

다음 예제에서는 인증서 체인 파일이 표시되는 방법을 보여 줍니다.

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

외부 도구를 사용하여 생성된 **HTTPS** 인증서 설치

자체 서명 또는 CA 서명된 인증서를 설치할 수 있으며 OpenSSL, BoringSSL, LetsEncrypt와 같은 외부 도구를 사용하여 생성할 수 있습니다.

이러한 인증서는 외부에서 생성된 공개-개인 키 쌍이므로 인증서 체인과 함께 개인 키를 로드해야 합니다. 허용된 키 쌍

알고리즘은 "RSA"와 "EC"입니다. HTTPS 인증서 설치 * 옵션은 일반 섹션의 HTTPS 인증서 페이지에서 사용할 수 있습니다. 업로드하는 파일은 다음과 같은 입력 형식이어야 합니다.

1. Active IQ Unified Manager 호스트에 속한 서버의 개인 키입니다
2. 개인 키와 일치하는 서버의 인증서입니다
3. 위의 인증서에 서명하는 데 사용되는 루트까지 CA의 인증서가 반대입니다

EC 키 쌍을 사용하여 인증서를 로드하는 형식입니다

허용되는 곡선은 프리메256v1, 에코384r1입니다. 외부에서 생성된 EC 쌍이 있는 인증서 샘플:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

RSA 키 쌍을 사용하여 인증서를 로드하는 형식입니다

호스트 인증서에 속하는 RSA 키 쌍에 허용되는 키 크기는 2048, 3072 및 4096입니다. 외부에서 생성된 * RSA 키 쌍이 포함된 인증서 *:

```
-----BEGIN RSA PRIVATE KEY-----
 <RSA private key of Server>
 -----END RSA PRIVATE KEY-----
 -----BEGIN CERTIFICATE-----
 <Server certificate>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #1 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Intermediate certificate #2 (if present)>
 -----END CERTIFICATE-----
 -----BEGIN CERTIFICATE-----
 <Root signing certificate>
 -----END CERTIFICATE-----
```

인증서가 업로드되면 Active IQ Unified Manager 인스턴스를 다시 시작하여 변경 내용을 적용해야 합니다.

외부에서 생성된 인증서를 업로드하는 동안 확인합니다

시스템은 외부 툴을 사용하여 생성된 인증서를 업로드하는 동안 검사를 수행합니다. 확인 중 하나라도 실패하면 인증서가 거부됩니다. 또한 제품 내에서 CSR에서 생성된 인증서 및 외부 도구를 사용하여 생성된 인증서에 대한 유효성 검사가 포함되어 있습니다.

- 입력의 개인 키는 입력의 호스트 인증서에 대해 유효성이 검사됩니다.
- 호스트 인증서의 CN(일반 이름)이 호스트의 FQDN에 대해 확인됩니다.
- 호스트 인증서의 CN(일반 이름)은 비어 있거나 비어 있어서는 안 되며 localhost로 설정해서는 안 됩니다.
- 유효 시작 날짜는 미래일 수 없으며 인증서의 유효 기간이 과거일 수 없습니다.
- 중간 CA 또는 CA가 있는 경우 인증서의 유효 시작 날짜는 미래일 수 없으며 유효 기간 만료 날짜는 과거일 수 없습니다.

입력의 개인 키는 암호화해서는 안 됩니다. 암호화된 개인 키가 있으면 시스템에서 거부됩니다.

예 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

예 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

예 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

인증서 설치에 실패한 경우 기술 자료(KB) 문서:
"ActiveIQ Unified Manager에서 외부에서 생성된 인증서를 설치하지 못했습니다"

인증서 관리에 대한 페이지 설명입니다

HTTPS 인증서 페이지를 사용하여 현재 보안 인증서를 보고 새 HTTPS 인증서를 생성할 수 있습니다.

HTTPS 인증서 페이지

HTTPS 인증서 페이지에서는 현재 보안 인증서를 보거나, 인증서 서명 요청을 다운로드하거나, 자체 서명된 새 HTTPS 인증서를 생성하거나, 새 HTTPS 인증서를 설치할 수 있습니다.

자체 서명된 새 HTTPS 인증서를 생성하지 않은 경우 이 페이지에 나타나는 인증서는 설치 중에 생성된 인증서입니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * HTTPS 인증서 서명 요청 다운로드 *

  현재 설치된 HTTPS 인증서에 대한 인증 요청을 다운로드합니다. 브라우저에서 <hostname>.csr 파일을 저장하라는 메시지를 표시하면 서명할 인증 기관에 파일을 제공할 수 있습니다.

- * HTTPS 인증서 설치 *

  인증 기관이 서명하여 반환한 후에 보안 인증서를 업로드 및 설치할 수 있습니다. 관리 서버를 다시 시작한 후 새 인증서가 적용됩니다.

- * HTTPS 인증서 재생성 *

  현재 보안 인증서를 대체하는 자체 서명된 새 HTTPS 인증서를 생성할 수 있습니다. 새 인증서는 Unified Manager를 다시 시작한 후에 적용됩니다.

HTTPS 인증서 재생성 대화 상자

HTTPS 인증서 다시 생성 대화 상자에서는 보안 정보를 사용자 지정한 다음 해당 정보로 새 HTTPS 인증서를 생성할 수 있습니다.

현재 인증서 정보가 이 페이지에 나타납니다.

""현재 인증서 특성을 사용하여 재생성" 및 ""현재 인증서 특성 업데이트" 선택 항목을 사용하면 현재 정보로 인증서를 다시 생성하거나 새 정보로 인증서를 생성할 수 있습니다.

- * 일반 이름 *

  필수 요소입니다. 보안하려는 FQDN(정규화된 도메인 이름)입니다.

  Unified Manager 고가용성 구성에서 가상 IP 주소를 사용합니다.

- * 이메일 *

  선택 사항. 조직에 연락할 이메일 주소. 일반적으로 인증서 관리자 또는 IT 부서의 이메일 주소입니다.

- * 회사 *

  선택 사항. 일반적으로 회사의 통합 이름입니다.

- * 부서 *

  선택 사항. 회사의 부서 이름입니다.

- * 시 *

  선택 사항. 회사의 도시 위치입니다.

- * 시/도 *

  선택 사항. 회사의 시/도 위치(약어로 표시되지 않음)입니다.

- * 국가 *

  선택 사항. 회사의 국가 위치입니다. 이 코드는 일반적으로 해당 국가의 2자리 ISO 코드입니다.

- * 대체 이름 *

  필수 요소입니다. 기존 localhost 또는 기타 네트워크 주소 외에 이 서버에 액세스하는 데 사용할 수 있는 추가, 비기본 도메인 이름입니다. 각 대체 이름을 쉼표로 구분합니다.

  인증서의 대체 이름 필드에서 로컬 식별 정보를 제거하려면 "'로컬 식별 정보 제외(예: localhost)'" 확인란을 선택합니다. 이 확인란을 선택하면 필드에 입력한 항목만 대체 이름 필드에 사용됩니다. 공백으로 두면 결과 인증서에 대체 이름 필드가 전혀 없습니다.

- * 키 크기(키 알고리즘: RSA) *

  키 알고리즘은 RSA로 설정됩니다. 2048, 3072 또는 4096비트의 키 크기 중 하나를 선택할 수 있습니다. 기본 키 크기는 2048비트로 설정됩니다.

- * 유효 기간 *

  기본 유효 기간은 397일입니다. 이전 버전에서 업그레이드한 경우 이전 인증서 유효성이 변경되지 않은 상태로 표시될 수 있습니다.

자세한 내용은 을 참조하십시오 "HTTPS 인증서를 생성하는 중입니다".

스토리지 모니터링 및 관리

Active IQ Unified Manager 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하면 단일 인터페이스에서 ONTAP 스토리지 시스템의 상태 및 성능을 모니터링 및 관리할 수 있습니다.

Unified Manager는 다음과 같은 기능을 제공합니다.

- ONTAP 소프트웨어와 함께 설치된 시스템에 대한 검색, 모니터링 및 알림
- 환경의 용량, 보안 및 성능 상태를 보여주는 대시보드
- 향상된 알림, 이벤트 및 임계값 인프라
- IOPS(작업), MBps(처리량), 지연 시간(응답 시간), 활용률을 비롯한 시간별 워크로드 작업을 그래프로 표시합니다. 성능 용량 및 캐시 비율입니다.
- 클러스터 구성 요소를 과도하게 사용하는 워크로드 및 늘어난 활동에 의해 성능이 영향을 받는 워크로드를 식별합니다.
- 에서는 특정 인시던트 및 이벤트를 해결하기 위해 수행할 수 있는 권장 수정 조치를 제공하고, 일부 이벤트의 경우 문제를 즉시 해결할 수 있도록 "Fix it" 버튼을 제공합니다.
- OnCommand Workflow Automation와 통합하여 자동화된 보호 워크플로우 실행
- Unified Manager에서 직접 LUN 또는 파일 공유와 같은 새 워크로드를 생성하고 성능 서비스 레벨을 할당하여 해당 워크로드를 사용하는 애플리케이션에 액세스하는 사용자의 성능 및 스토리지 목표를 정의할 수 있습니다.

Active IQ Unified Manager 상태 모니터링 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하면 중앙 집중식 사용자 인터페이스를 통해 ONTAP 소프트웨어를 실행하는 수많은 시스템을 모니터링할 수 있습니다. Unified Manager 서버 인프라는 확장성, 지원 가능성 및 향상된 모니터링 및 알림 기능을 제공합니다.

Unified Manager의 주요 기능으로는 모니터링, 경고, 클러스터의 가용성 및 용량 관리, 보호 기능 관리, 진단 데이터의 번들 구성, 기술 지원 부서에 전송 등이 있습니다.

Unified Manager를 사용하여 클러스터를 모니터링할 수 있습니다. 클러스터에서 문제가 발생하면 Unified Manager가 이벤트를 통해 해당 문제의 세부 정보를 통지합니다. 또한 일부 이벤트는 문제를 해결하기 위해 취할 수 있는 개선 조치를 제공합니다. 문제가 발생할 때 전자 메일 및 SNMP 트랩을 통해 알림을 받도록 이벤트에 대한 알림을 구성할 수 있습니다.

Unified Manager를 사용하여 스토리지 객체를 주석과 연계하여 사용자 환경의 스토리지 객체를 관리할 수 있습니다. 맞춤형 주석을 생성하고 규칙을 통해 클러스터, SVM(스토리지 가상 머신), 볼륨을 주석과 함께 동적으로 연결할 수 있습니다.

또한 용량 및 상태 차트에 제공된 정보를 사용하여 각 클러스터 개체에 대한 클러스터 개체의 스토리지 요구 사항을 계획할 수 있습니다.

물리적 및 논리적 용량

Unified Manager에서는 ONTAP 스토리지 객체에 사용되는 물리적/논리적 공간의 개념을 사용합니다.

- 물리적 용량: 물리적 공간은 볼륨에 사용된 스토리지의 물리적 블록을 나타냅니다. "물리적 사용 용량"은 일반적으로 중복 제거 및 압축과 같은 스토리지 효율성 기능에서 데이터 감소로 인해 논리적 사용 용량보다 작습니다.
- 논리적 용량: 논리적 공간은 볼륨의 사용 가능한 공간(논리적 블록)을 나타냅니다. 논리적 공간은 중복제거 또는 압축 결과를 고려하지 않고 이론적 공간을 사용할 수 있는 방법을 나타냅니다. "사용된 논리적 공간"은 사용된 물리적 공간과 함께 구성된 스토리지 효율성 기능(예: 중복제거 및 압축)의 절약 효과를 더한 것입니다. 이 측정치는 데이터 압축과 물리적 공간의 기타 감소량을 반영하지 않기 때문에 물리적 사용된 용량보다 더 크게 표시되는 경우가 많습니다. 따라서 총 논리적 용량이 프로비저닝된 공간보다 클 수 있습니다.

용량 측정 단위

Unified Manager에서는 1024바이트(2^{10})바이트의 이진 단위를 기준으로 스토리지 용량을 계산합니다. ONTAP 9.10.0 이전 버전에서는 이러한 유닛이 KB, MB, GB, TB 및 PB로 표시되었습니다. ONTAP 9.10.1부터는 Unified Manager에 KiB, MiB, GiB, TiB 및 PiB로 표시됩니다.

처리량에 사용되는 단위는 모든 ONTAP 릴리스에 대해 초당 킬로바이트(Kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps) 또는 초당 테라바이트(Tbps) 등으로 계속 사용됩니다.

용량 단위는 **ONTAP 9.10.0** 이하 버전에 대해 **Unified Manager**에 표시됩니다	**Unified Manager for ONTAP 9.10.1**에 용량 단위가 표시됩니다	계산	바이트 단위의 값입니다
KB를 클릭합니다	KiB	1024	1024바이트
MB	MIB	1024 * 1024	1,048,576바이트
GB	GiB	1024 * 1024 * 1024	1,073,741,824바이트
TB	TiB	1024 * 1024 * 1024	1,099,511,627,776바이트

Active IQ Unified Manager 성능 모니터링 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)은 NetApp ONTAP 소프트웨어를 실행하는 시스템에 대한 성능 모니터링 기능 및 이벤트 근본 원인 분석을 제공합니다.

Unified Manager를 사용하면 클러스터 구성 요소를 과도하게 사용하는 워크로드를 식별하고 클러스터에서 다른 워크로드의 성능을 줄일 수 있습니다. 성능 임계값 정책을 정의하여 특정 성능 카운터의 최대값을 지정하여 임계값이 위반될 때 이벤트가 생성되도록 할 수도 있습니다. Unified Manager를 사용하면 이러한 성능 이벤트를 경고하여 수정 조치를 취하고 성능을 정상 작동 수준으로 높일 수 있습니다. Unified Manager UI에서 이벤트를 보고 분석할 수 있습니다.

Unified Manager에서 두 가지 유형의 워크로드 성능을 모니터링합니다.

- 사용자 정의 워크로드

이러한 워크로드는 클러스터에서 생성한 FlexVol 볼륨과 FlexGroup 볼륨으로 구성됩니다.

- 시스템 정의 워크로드

  이러한 워크로드는 내부 시스템 작업으로 구성됩니다.

Unified Manager REST API 사용

Active IQ Unified Manager에서는 REST API를 사용하여 스토리지 환경을 모니터링 및 관리하는 방법에 대한 정보를 볼 수 있습니다. API를 사용하면 정책에 따라 스토리지 객체를 프로비저닝 및 관리할 수 있습니다.

Unified Manager가 지원하는 API 게이트웨이를 사용하여 모든 ONTAP 관리 클러스터에서 ONTAP API를 실행할 수도 있습니다.

Unified Manager REST API에 대한 자세한 내용은 를 참조하십시오 "Active IQ Unified Manager REST API 시작하기".

Unified Manager 서버의 기능

Unified Manager 서버 인프라는 데이터 수집 장치, 데이터베이스 및 애플리케이션 서버로 구성됩니다. 검색, 모니터링, RBAC(역할 기반 액세스 제어), 감사, 로깅 등의 인프라 서비스를 제공합니다.

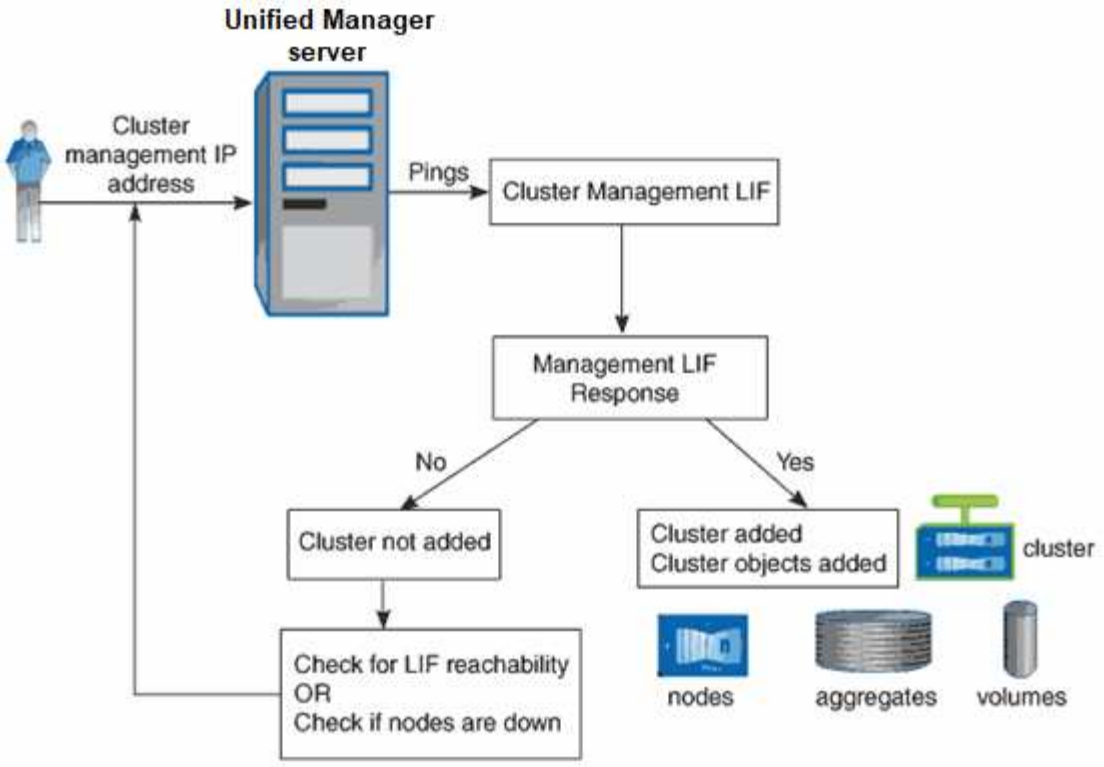
Unified Manager는 클러스터 정보를 수집하고, 데이터를 데이터베이스에 저장하고, 데이터를 분석하여 클러스터 문제가 있는지 확인합니다.

검색 프로세스의 작동 방식

클러스터를 Unified Manager에 추가한 후에는 서버에서 클러스터 개체를 검색하고 해당 개체를 데이터베이스에 추가합니다. 검색 프로세스가 작동하는 방식을 이해하면 조직의 클러스터와 개체를 관리하는 데 도움이 됩니다.

기본 모니터링 간격은 15분입니다. 클러스터를 Unified Manager 서버에 추가한 경우 Unified Manager UI에 클러스터 세부 정보를 표시하는 데 15분이 걸립니다.

다음 그림에서는 Active IQ Unified Manager의 검색 프로세스를 보여 줍니다.



사용자 인터페이스 이해

Unified Manager 사용자 인터페이스는 주로 모니터링된 개체를 한눈에 파악할 수 있는 대시보드로 구성되어 있습니다. 또한 사용자 인터페이스에서 모든 클러스터 객체를 볼 수 있습니다.

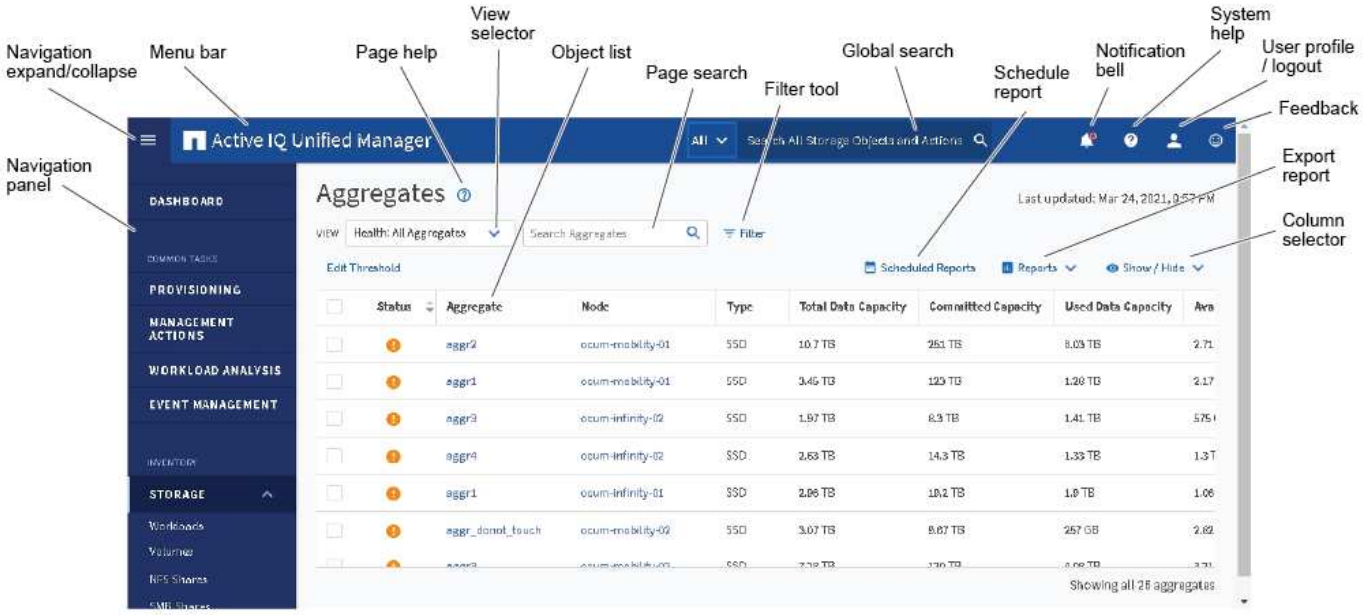
원하는 보기를 선택하고 필요에 따라 작업 버튼을 사용할 수 있습니다. 화면 구성은 Unified Manager를 시작할 때 필요한 모든 기능을 사용할 수 있도록 작업 공간에 저장됩니다. 그러나 한 보기에서 다른 보기로 이동한 다음 다시 탐색하면 보기가 동일하지 않을 수 있습니다.

일반적인 창 레이아웃

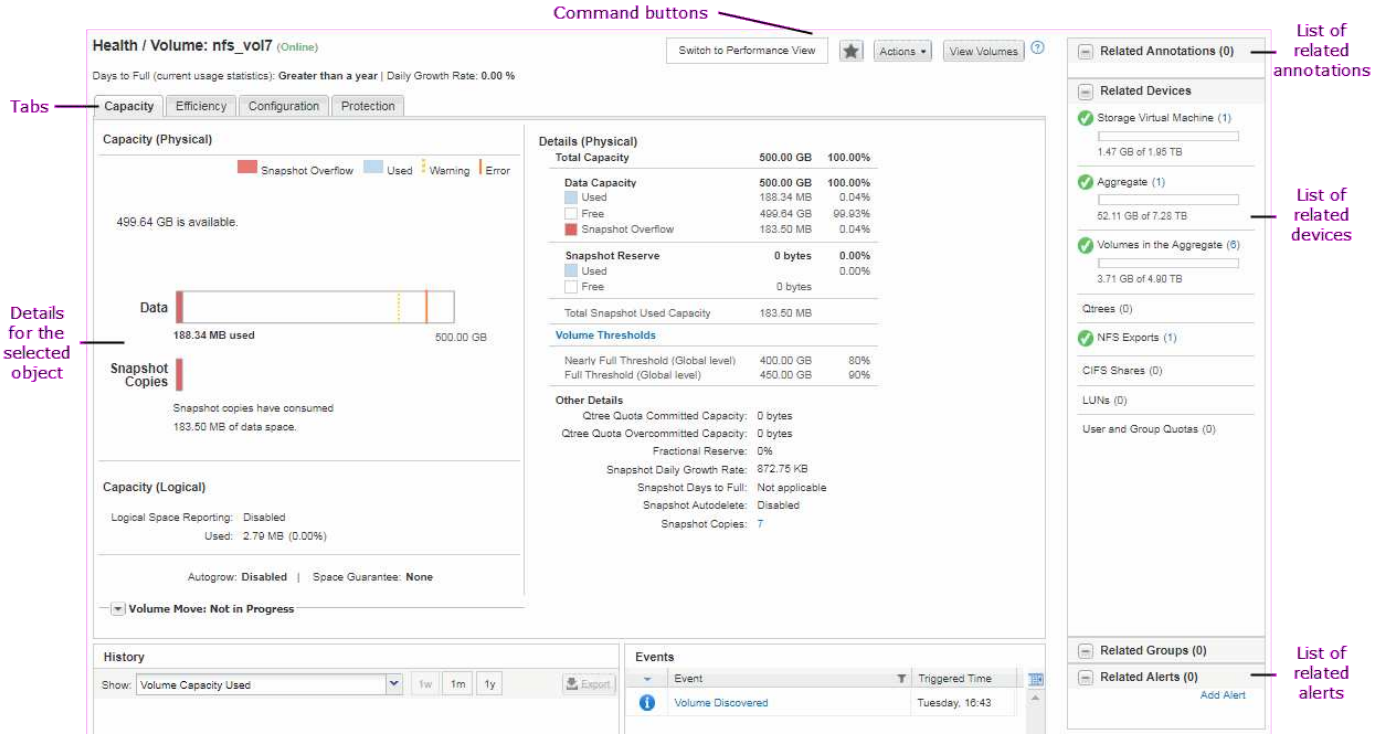
일반적인 창 레이아웃을 이해하면 Active IQ Unified Manager를 효율적으로 탐색하고 사용할 수 있습니다. 대부분의 Unified Manager 창은 두 가지 일반적인 레이아웃 중 하나, 즉 개체 목록 또는 세부 사항과 비슷합니다. 권장 디스플레이 설정은 최소 1280 x 1024 픽셀입니다.

모든 창에 다음 다이어그램의 모든 요소가 포함되는 것은 아닙니다.

개체 목록 창 레이아웃



개체 세부 정보 창 레이아웃



창 레이아웃 사용자 정의

Active IQ Unified Manager를 사용하면 스토리지 및 네트워크 개체 페이지의 정보 레이아웃을 사용자 지정할 수 있습니다. 창을 사용자 지정하여 볼 수 있는 데이터와 데이터의 표시 방법을 제어할 수 있습니다.

- * 정렬 *

열 머리글을 클릭하여 열 항목의 정렬 순서를 변경할 수 있습니다. 열 머리글을 클릭하면 정렬 화살표(및)가 해당 열에 나타납니다.

- * 필터링 *

  필터 아이콘( )를 사용하여 스토리지 및 네트워크 개체 페이지에 정보 표시를 사용자 지정하는 필터를 적용하여 제공된 조건과 일치하는 항목만 표시되도록 합니다. 필터 창에서 필터를 적용합니다.

  필터 창에서는 선택한 옵션을 기준으로 대부분의 열을 필터링할 수 있습니다. 예를 들어, 상태: 모든 볼륨 보기에서 필터 창을 사용하여 상태 에서 적절한 필터 옵션을 선택하여 오프라인 상태인 모든 볼륨을 표시할 수 있습니다.

  모든 목록의 용량 관련 열에는 항상 용량 데이터가 소수점 이하 두 자리로 반올림된 적절한 단위로 표시됩니다. 이는 용량 열을 필터링할 때도 적용됩니다. 예를 들어, Health: All aggregate(모든 집계) 보기의 Total Data Capacity(전체 데이터 용량) 열에서 필터를 사용하여 20.454GB보다 큰 데이터를 필터링하는 경우 실제 용량은 20.454GB로 표시됩니다. 마찬가지로 20.45GB 미만의 데이터를 필터링하는 경우 실제 용량은 20.449GB로 표시됩니다.

  Health: All aggregate(모든 집계) 보기의 Available Data %(사용 가능한 데이터 %) 열에서 필터를 사용하여 20.45% 이상의 데이터를 필터링하는 경우 실제 용량 20.454%가 20.45%로 표시됩니다. 마찬가지로 20.45% 미만의 데이터를 필터링하는 경우 실제 용량은 20.449%로 20.45%로 표시됩니다.

- * 열 숨기기 또는 표시 *

  열 표시 아이콘(* 표시/숨기기*)을 클릭하여 표시할 열을 선택할 수 있습니다. 적절한 열을 선택한 후 마우스를 사용하여 끌어서 순서를 다시 지정할 수 있습니다.

- * 검색 중 *

  검색 상자를 사용하여 특정 객체 속성을 검색하여 재고 페이지의 항목 목록을 구체화할 수 있습니다. 예를 들어, "cloud"를 입력하여 볼륨 인벤토리 페이지에 있는 볼륨 목록을 세분화하여 "cloud"라는 단어가 포함된 모든 볼륨을 볼 수 있습니다.

- * 데이터 내보내기 *

  보고서 * 버튼(또는 * 내보내기 * 버튼)을 클릭하여 데이터를 쉼표로 구분된 값 파일(.csv), 파일(.pdf), 문서 또는 Microsoft Excel(.xlsx) 파일로 내보내고 내보낸 데이터를 사용하여 보고서를 작성할 수 있습니다.

Unified Manager 도움말 사용

도움말에는 Active IQ Unified Manager에 포함된 모든 기능에 대한 정보가 포함되어 있습니다. 목차, 색인 또는 검색 도구를 사용하여 기능에 대한 정보와 사용 방법을 찾을 수 있습니다.

도움말은 각 탭과 Unified Manager 사용자 인터페이스의 메뉴 모음에서 사용할 수 있습니다.

도움말의 검색 도구가 일부 단어에서는 작동하지 않습니다.

- 특정 필드나 매개 변수에 대해 알아보려면 를 클릭합니다 .
- 모든 도움말 내용을 보려면 * 를 클릭합니다*> * 도움말/문서 * 를 선택합니다.

  탐색 창에서 목차의 일부를 확장하여 자세한 정보를 찾을 수 있습니다.

- 도움말 내용을 검색하려면 탐색 창에서 * 검색 * 탭을 클릭하고 찾으려는 단어 또는 일련의 단어를 입력한 다음 * 이동! * 을 클릭합니다
- 도움말 항목을 인쇄하려면 프린터 아이콘을 클릭합니다.

즐겨찾는 도움말 항목 북마크

도움말 즐겨찾기 탭에서 자주 사용하는 도움말 항목에 책갈피를 지정할 수 있습니다. 도움말 책갈피를 사용하면 자주 사용하는 항목에 빠르게 액세스할 수 있습니다.

단계

1. 즐겨찾기로 추가할 도움말 항목으로 이동합니다.
2. 즐겨찾기 * 를 클릭한 다음 * 추가 * 를 클릭합니다.

스토리지 객체를 검색하는 중입니다

특정 개체에 빠르게 액세스하려면 메뉴 모음 맨 위에 있는 * 모든 스토리지 개체 검색 * 필드를 사용합니다. 모든 개체에 대해 이 전역 검색 방법을 사용하면 유형별로 특정 개체를 빠르게 찾을 수 있습니다. 검색 결과는 스토리지 객체 유형별로 정렬되며 드롭다운 메뉴를 사용하여 객체별로 추가로 필터링할 수 있습니다.

- 필요한 것 *
- 이 작업을 수행하려면 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할 중 하나가 있어야 합니다.
- 유효한 검색에는 3자 이상의 문자가 포함되어야 합니다.

드롭다운 메뉴 값 "모두"를 사용할 경우 전체 검색은 모든 개체 범주에서 찾은 총 결과 수를 표시하며 각 개체 범주에 대해 최대 25개의 검색 결과를 표시합니다. 드롭다운 메뉴에서 특정 개체 유형을 선택하여 특정 개체 유형 내에서 검색을 구체화할 수 있습니다. 이 경우 반환된 목록은 상위 25개 객체로 제한되지 않습니다.

검색할 수 있는 객체 유형은 다음과 같습니다.

- 클러스터
- 노드
- 스토리지 VM
- 애그리게이트
- 볼륨
- Qtree
- SMB 공유
- NFS 공유
- 사용자 또는 그룹 할당량
- LUN을 클릭합니다
- NVMe 네임스페이스
- 이니시에이터 그룹

- 이니시에이터
- 정합성 보장 그룹

워크로드 이름을 입력하면 해당 볼륨 또는 LUN 범주 아래에 있는 워크로드 목록이 반환됩니다.

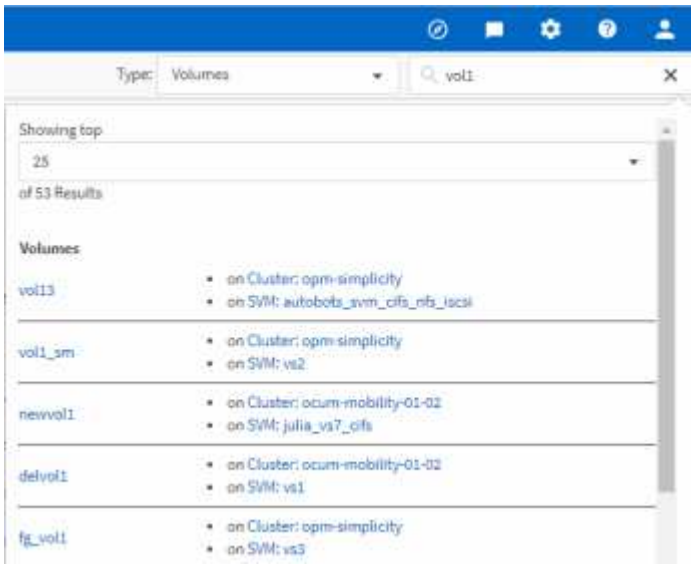
검색 결과에서 아무 개체나 클릭하여 해당 개체의 상태 세부 정보 페이지로 이동할 수 있습니다. 개체에 대한 직접 상태 페이지가 없으면 부모 개체의 상태 페이지가 표시됩니다. 예를 들어, 특정 LUN을 검색할 때 LUN이 있는 SVM 세부 정보 페이지가 표시됩니다.

포트 및 LIF는 글로벌 검색 창에서 검색할 수 없습니다.

단계

1. 메뉴에서 개체 유형을 선택하여 단일 개체 유형에 대한 검색 결과를 구체화합니다.
2. 모든 스토리지 객체 검색 * 필드에 객체 이름의 최소 3자를 입력하십시오.

   이 예제에서 드롭다운 상자에는 볼륨 개체 유형이 선택되어 있습니다. 모든 스토리지 객체 검색 * 필드에 "vol1"을 입력하면 이름에 이러한 문자가 포함된 모든 볼륨 목록이 표시됩니다.



스토리지 데이터를 보고서로 내보내기

다양한 출력 형식으로 저장소 데이터를 내보낸 다음 내보낸 데이터를 사용하여 보고서를 작성할 수 있습니다. 예를 들어 해결되지 않은 10개의 중요 이벤트가 있는 경우 이벤트 관리 인벤토리 페이지에서 데이터를 내보내서 보고서를 만든 다음 문제를 해결할 수 있는 관리자에게 보고서를 보낼 수 있습니다.

Storage * 및 * Network * 재고 페이지에서 ".csv" 파일, .xlsx" 파일 또는 ".pdf" 문서로 데이터를 내보내고 내보낸 데이터를 사용하여 보고서를 작성할 수 있습니다. 제품에는 .csv 또는 .pdf 파일만 생성할 수 있는 다른 위치가 있습니다.

단계

1. 다음 작업 중 하나를 수행합니다.

내보내려는 경우...	수행할 작업...
스토리지 객체 인벤토리 세부 정보입니다	왼쪽 탐색 메뉴에서 * 스토리지 * 또는 * 네트워크 * 를 클릭한 다음 스토리지 객체를 선택합니다. 시스템에서 제공하는 보기 중 하나 또는 사용자가 만든 사용자 지정 보기를 선택합니다.
QoS 정책 그룹 세부 정보	왼쪽 탐색 메뉴에서 * 스토리지 * > * QoS 정책 그룹 * 을 클릭합니다.
스토리지 용량 및 보호 기록 세부 정보	스토리지 * > * 애그리게이트 * 또는 * 스토리지 * > * 볼륨 * 을 클릭한 다음 단일 애그리게이트 또는 볼륨을 선택합니다.
이벤트 세부 정보	왼쪽 탐색 메뉴에서 * 이벤트 관리 * 를 클릭합니다.
스토리지 객체 10가지 성능 세부 정보	Storage * > * Clusters * > * Performance: All Clusters * 를 클릭한 다음 클러스터를 선택하고 * Top Performers * 탭을 선택합니다. 그런 다음 스토리지 오브젝트 및 성능 카운터를 선택합니다.

2. 보고서 * 버튼(또는 일부 UI 페이지의 * 내보내기 * 버튼)을 클릭합니다.
3. CSV * 다운로드, * PDF 다운로드 * 또는 * Excel * 다운로드 를 클릭하여 내보내기 요청을 확인합니다.

   Top Performers 탭에서 보고 있는 단일 클러스터의 통계 보고서 또는 데이터 센터의 모든 클러스터에 대한 통계 보고서를 다운로드할 수 있습니다.

   파일이 다운로드됩니다.

4. 해당 응용 프로그램에서 파일을 엽니다.
   - 관련 정보 *

"상태/클러스터 인벤토리 페이지입니다"

"보고서 예약"

재고 페이지 콘텐츠 필터링

Unified Manager에서 인벤토리 페이지 데이터를 필터링하여 특정 기준에 따라 데이터를 빠르게 찾을 수 있습니다. 필터링을 사용하면 Unified Manager 페이지의 콘텐츠 범위를 좁혀 원하는 결과만 표시할 수 있습니다. 따라서 관심 있는 데이터만 표시하는 매우 효율적인 방법이 제공됩니다.

필터링 * 을 사용하여 기본 설정에 따라 그리드 보기를 사용자 정의합니다. 사용 가능한 필터 옵션은 격자에서 보는 개체 유형을 기반으로 합니다. 필터가 현재 적용된 경우 필터 단추 오른쪽에 적용된 필터 수가 표시됩니다.

세 가지 유형의 필터 매개 변수가 지원됩니다.

매개 변수	검증
문자열(텍스트)	연산자는 * 포함 *, * 다음으로 시작 *, * 로 끝 *, * 포함하지 않음 * 입니다.
번호	연산자는 * 보다 * 큼, * 보다 작음 *, * 마지막 * 에서 * 사이 * 입니다.
Enum(텍스트)	연산자는 * 이고 * 는 * 입니다.

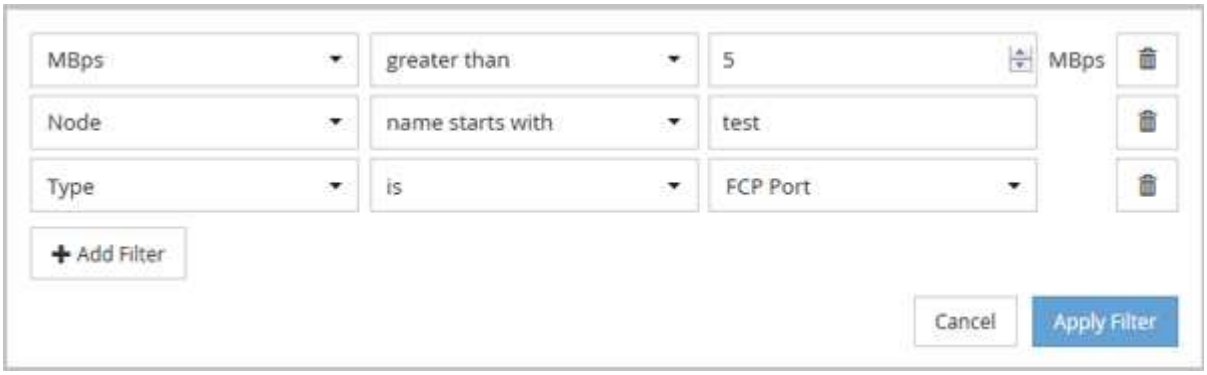
각 필터에는 열, 연산자 및 값 필드가 필요합니다. 사용 가능한 필터는 현재 페이지의 필터링 가능한 열을 반영합니다. 적용할 수 있는 최대 필터 수는 4개입니다. 필터링된 결과는 결합된 필터 매개 변수를 기반으로 합니다. 필터링된 결과는 현재 표시된 페이지뿐만 아니라 필터링된 검색의 모든 페이지에 적용됩니다.

필터링 패널을 사용하여 필터를 추가할 수 있습니다.

1. 페이지 맨 위에서 * 필터 * 버튼을 클릭합니다. Filtering(필터링) 패널이 표시됩니다.
2. 왼쪽 드롭다운 목록을 클릭하고 개체를 선택합니다(예: *Cluster* 또는 성능 카운터).
3. 가운데 드롭다운 목록을 클릭하고 사용할 연산자를 선택합니다.
4. 마지막 목록에서 값을 선택하거나 입력하여 해당 개체에 대한 필터를 완료합니다.
5. 다른 필터를 추가하려면 * + 필터 추가 * 를 클릭합니다. 추가 필터 필드가 표시됩니다. 위의 단계에 설명된 프로세스를 사용하여 이 필터를 완료합니다. 네 번째 필터를 추가하면 * + 필터 추가 * 버튼이 더 이상 표시되지 않습니다.
6. 필터 적용 * 을 클릭합니다. 필터 옵션이 그리드에 적용되고 필터 버튼 오른쪽에 필터 수가 표시됩니다.
7. 필터 패널을 사용하여 제거할 필터의 오른쪽에 있는 휴지통 아이콘을 클릭하여 개별 필터를 제거합니다.
8. 모든 필터를 제거하려면 필터링 패널 하단에 있는 * Reset * (재설정 *)을 클릭합니다.

필터링 예제

그림에는 3개의 필터가 있는 필터링 패널이 나와 있습니다. 최대 4개 이하의 필터가 있는 경우 * + 필터 추가 * 버튼이 표시됩니다.



필터 적용 * 을 클릭하면 필터링 패널이 닫히고 필터가 적용되고 적용된 필터 수가 표시됩니다(3)를 클릭합니다.

알림 표시에서 활성 이벤트 보기

알림 벨(🔔) 메뉴 모음에서는 Unified Manager가 추적하고 있는 가장 중요한 활성 이벤트를 빠르게 볼 수 있습니다.

활성 이벤트 목록을 사용하면 모든 클러스터에서 위험, 오류, 경고 및 업그레이드 이벤트의 총 수를 확인할 수 있습니다. 이 목록에는 이전 7일의 이벤트가 포함되며 정보 이벤트는 포함되지 않습니다. 링크를 클릭하여 가장 관심 있는 이벤트 목록을 표시할 수 있습니다.

클러스터에 연결할 수 없는 경우 Unified Manager에서 이 정보를 이 페이지에 표시합니다. 세부 정보 * 버튼을 클릭하면 연결할 수 없는 클러스터에 대한 자세한 정보를 볼 수 있습니다. 그러면 이벤트 세부 정보 페이지가 열립니다. 관리 스테이션의 공간 부족 또는 RAM과 같은 스케일 모니터링 문제도 이 페이지에 표시됩니다.

단계

1. 메뉴 모음에서 를 클릭합니다 🔔.
2. 활성 이벤트에 대한 세부 정보를 보려면 "2 Capacity" 또는 "4 Performance"와 같은 이벤트 텍스트 링크를 클릭합니다.

대시보드에서 클러스터 모니터링 및 관리

대시보드에서는 모니터링되는 ONTAP 시스템의 현재 상태에 대한 누적 정보를 한 눈에 확인할 수 있습니다. 대시보드에는 모니터링 중인 클러스터의 전체 용량, 성능 및 보안 상태를 평가할 수 있는 ""패널""이 있습니다.

또한 ONTAP 시스템 관리자나 ONTAP CLI를 사용할 필요 없이 Unified Manager 사용자 인터페이스에서 직접 해결할 수 있는 특정 ONTAP 문제가 있습니다.

대시보드 상단에서 패널이 모니터링되는 모든 클러스터에 대한 정보를 표시할지 또는 개별 클러스터에 대한 정보를 표시할지를 선택할 수 있습니다. 먼저 모든 클러스터의 상태를 확인한 다음 세부 정보를 보려는 개별 클러스터로 드릴다운할 수 있습니다.

ⓘ 아래 나열된 패널 중 일부는 구성에 따라 페이지에 나타나지 않을 수 있습니다.

패널	설명
관리 조치	Unified Manager에서 문제에 대한 단일 해결책을 진단하고 결정할 수 있으면 해당 해결 방법이 * Fix it * 버튼과 함께 이 패널에 표시됩니다.
용량	로컬 계층 및 클라우드 계층에 대한 총 용량 및 사용된 용량, 로컬 용량이 상한에 도달할 때까지 남은 일 수를 표시합니다.
성능 용량	각 클러스터의 성능 용량 값과 성능 용량이 상한에 도달할 때까지 남은 일 수를 표시합니다.

패널	설명
워크로드 IOPS	특정 IOPS 범위에서 현재 실행 중인 총 워크로드 수를 표시합니다.
워크로드 성능	정의된 각 성능 서비스 수준에 할당된 준수 및 부적합 워크로드의 총 수를 표시합니다.
보안	규정을 준수하거나 준수하지 않는 클러스터의 수, 규정을 준수하거나 준수하지 않는 SVM의 수, 암호화되거나 암호화되지 않은 볼륨의 수를 표시합니다.
보호	SVM-DR 관계로 보호되는 스토리지 VM 수, SnapMirror 관계에 의해 보호되는 볼륨, Snapshot으로 보호되는 볼륨 및 MetroCluster에 의해 보호되는 클러스터의 수를 표시합니다.
사용 개요	가장 높은 IOPS, 가장 높은 처리량(MBps) 또는 가장 많이 사용되는 물리적 용량에 따라 정렬된 클러스터를 표시합니다.

대시보드 페이지

대시보드 페이지에는 모니터링하는 클러스터의 높은 수준, 성능 및 보안 상태를 표시하는 "패널"이 있습니다. 또한 Unified Manager에서 특정 이벤트를 해결하기 위해 수행할 수 있는 수정 사항이 나열된 관리 작업 패널도 제공합니다.

또한 대부분의 패널에는 해당 범주의 활성 이벤트 수와 이전 24시간 동안 추가된 새 이벤트 수가 표시됩니다. 이 정보는 이벤트를 해결하기 위해 더 자세히 분석해야 할 클러스터를 결정하는 데 도움이 됩니다. 이벤트를 클릭하면 상위 이벤트가 표시되고 해당 범주의 활성 이벤트를 표시하도록 필터링된 이벤트 관리 인벤토리 페이지로 연결되는 링크가 제공됩니다.

대시보드 맨 위에서 패널이 모니터링되는 모든 클러스터("모든 클러스터")에 대한 정보를 표시할지 또는 개별 클러스터에 대한 정보를 표시할지 여부를 선택할 수 있습니다. 먼저 모든 클러스터의 상태를 확인한 다음 세부 정보를 보려는 개별 클러스터로 드릴다운할 수 있습니다.

아래 나열된 패널 중 일부는 구성에 따라 대시보드에 표시됩니다.

관리 작업 패널

Unified Manager에서 완벽하게 진단하고 한 가지 해결 방법을 제공할 수 있는 특정 문제가 있습니다. 사용 가능한 경우 이러한 해상도는 이 패널에 * Fix it * 또는 * Fix All * 버튼과 함께 표시됩니다. ONTAP System Manager 또는 ONTAP CLI를 사용하지 않고 Unified Manager에서 이러한 문제를 즉시 해결할 수 있습니다. 모든 문제를 보려면 참조 를 클릭합니다 "Unified Manager에서 직접 ONTAP 문제 해결" 를 참조하십시오.

용량 패널

모든 클러스터를 볼 때 이 패널에는 스토리지 효율성 절약 효과를 적용한 후의 물리적 사용 용량 및 각 클러스터에 대한 물리적 사용 가능한 용량(잠재적인 스토리지 효율성 절약 비율 제외)이 표시되며, 디스크가 꽉 찰 것으로 예상되는 일

수가 표시됩니다. 및 구성된 ONTAP 스토리지 효율성 설정을 기반으로 한 데이터 축소율(스냅샷 복사본 없음) 또한 구성된 모든 클라우드 계층에 사용된 용량도 나열됩니다. 막대 차트를 클릭하면 해당 클러스터의 애그리게이트 인벤토리 페이지로 이동합니다. "DAYS to Full" 텍스트를 클릭하면 남은 용량 일 수가 가장 적은 애그리게이트를 식별하는 메시지가 표시됩니다. 자세한 내용을 보려면 애그리게이트 이름을 클릭합니다.

단일 클러스터를 볼 때 이 패널에는 로컬 계층의 각 개별 디스크 유형과 클라우드 계층에 따라 정렬된 데이터 애그리게이트를 위한 물리적 사용 용량 및 물리적 사용 가능한 용량이 표시됩니다. 디스크 유형의 막대 차트를 클릭하면 해당 디스크 유형을 사용하는 볼륨의 볼륨 인벤토리 페이지로 이동합니다.

Performance Capacity 패널

모든 클러스터를 볼 때 이 패널에는 각 클러스터의 성능 용량 값(이전 1시간 동안의 평균 성능)과 성능 용량이 상한에 도달할 때까지 남은 일 수(일별 성장률 기준)가 표시됩니다. 막대 차트를 클릭하면 해당 클러스터의 노드 인벤토리 페이지로 이동합니다. 노드 인벤토리 페이지에는 이전 72시간 동안의 평균 성능 용량이 표시됩니다. "Days to Full" 텍스트를 클릭하면 남은 성능 용량이 가장 적은 노드를 식별하는 메시지가 표시됩니다. 자세한 내용을 보려면 노드 이름을 클릭하십시오.

단일 클러스터를 볼 때 이 패널에는 사용된 클러스터 성능 용량 비율, 총 IOPS 및 총 처리량(MB/s) 값과 이 세 가지 메트릭 각각이 상한에 도달할 때까지 남은 일 수가 표시됩니다.

워크로드 **IOPS** 패널

단일 클러스터를 볼 때 이 패널에는 특정 IOPS 범위에서 현재 실행 중인 총 워크로드 수가 표시되고, 차트 위에 커서를 놓으면 각 디스크 유형의 수를 나타냅니다.

워크로드 성능 패널

이 패널에는 각 PSL(Performance Service Level) 정책에 할당된 준수 및 부적합 워크로드의 총 수가 표시됩니다. 또한 PSL이 할당되지 않은 워크로드의 수도 표시됩니다. 막대 차트를 클릭하면 워크로드 페이지에서 해당 정책에 할당된 적합한 워크로드로 이동합니다. 막대 차트 다음에 나오는 숫자를 클릭하면 해당 정책에 할당된 준수 및 부적합 작업 부하로 이동합니다.

보안 패널

보안 패널은 현재 보기에 따라 모든 클러스터 또는 단일 클러스터에 대해 높은 수준의 보안 상태를 제공합니다. 이 패널은 다음을 표시합니다.

- 지난 24시간 동안 수신된 보안 이벤트 목록입니다. 이벤트 세부 정보 페이지에서 세부 정보를 보려면 이벤트를 클릭합니다
- 클러스터 보안 상태(준수 클러스터 및 비준수 클러스터 수)
- 스토리지 VM 보안 상태(호환 및 비준수 스토리지 VM 수)
- 볼륨 암호화 상태(암호화되거나 암호화되지 않은 볼륨의 수)
- 볼륨 안티 랜섬웨어 상태(랜섬웨어 방지 기능이 활성화 또는 비활성화된 볼륨 수)

준수 및 비준수 클러스터, 스토리지 VM, 암호화 및 암호화되지 않은 볼륨, 볼륨 안티 랜섬웨어 상태의 막대 차트를 클릭하여 해당 페이지로 이동하고 필터링된 클러스터, 스토리지 VM 및 볼륨의 보안 세부 정보를 볼 수 있습니다.

규정 준수는 을 기준으로 합니다 "ONTAP 9에 대한 NetApp 보안 강화 가이드". 패널 상단의 오른쪽 화살표를 클릭하여 보안 페이지의 모든 클러스터에 대한 보안 세부 정보를 봅니다. 자세한 내용은 을 참조하십시오"클러스터 및 스토리지 VM에 대한 자세한 보안 상태 보기".

데이터 보호 패널

이 패널에는 데이터 센터의 단일 또는 모든 클러스터에 대한 데이터 보호 요약이 표시됩니다. 이 창에는 ONTAP에서 최근 24시간 동안 발생한 총 데이터 보호 이벤트 수, MetroCluster 이벤트 및 활성 이벤트 수가 표시됩니다. 각 이벤트의 링크를 클릭하면 이벤트 세부 정보 페이지로 이동합니다. 이벤트 관리 인벤토리 페이지에서 * 모두 보기 * 링크를 클릭하여 모든 활성 보호 이벤트를 볼 수 있습니다. 패널에 다음이 표시됩니다.

- 스냅샷 복사본으로 보호되는 데이터 센터의 클러스터 또는 모든 클러스터에 있는 볼륨 수
- SnapMirror 관계로 보호되는 데이터 센터의 클러스터 또는 모든 클러스터에 있는 볼륨 수 SnapMirror 관계의 경우 소스 클러스터의 볼륨 수가 고려됩니다.
- IP 또는 FC를 통한 MetroCluster 구성으로 보호되는 데이터 센터의 클러스터 또는 모든 클러스터 수
- 지연 상태에 따른 RPO(SnapMirror 복구 지점 목표) 지연과의 볼륨 관계 수입니다.

마우스를 가져가면 해당 개수와 범례를 볼 수 있습니다. 패널 상단의 오른쪽 화살표를 클릭하여 데이터 보호 페이지의 단일 또는 모든 클러스터에 대한 세부 정보를 볼 수 있습니다. 또한 다음을 클릭할 수도 있습니다.

- 보호되지 않는 볼륨 및 스냅샷 복사본으로 보호되는 볼륨에 대한 막대 차트를 볼륨 페이지로 이동하여 세부 정보를 확인합니다.
- MetroCluster 구성으로 보호되거나 보호되지 않는 클러스터의 막대 차트는 클러스터 페이지로 이동하여 세부 정보를 봅니다.
- 모든 관계에 대한 막대 차트는 원본 클러스터를 기준으로 세부 정보가 필터링되는 관계 페이지로 이동합니다.

자세한 내용은 을 참조하십시오 "볼륨 보호 상태 보기".

사용 개요 패널

모든 클러스터를 볼 때 가장 높은 IOPS, 가장 높은 처리량(MB/s) 또는 가장 많이 사용되는 물리적 용량을 기준으로 정렬된 클러스터를 표시하도록 선택할 수 있습니다.

단일 클러스터를 볼 때 가장 높은 IOPS, 가장 높은 처리량(MB/s) 또는 가장 많이 사용되는 논리적 용량을 기준으로 워크로드를 정렬하도록 선택할 수 있습니다.

- 관련 정보 *

"Unified Manager 자동 수정을 사용하여 문제 해결"

"성능 이벤트에 대한 정보 표시"

"성능 용량 및 사용 가능한 IOPS 정보를 사용하여 성능 관리"

"볼륨/상태 세부 정보 페이지"

"성능 이벤트 분석 및 알림"

"이벤트 심각도 유형에 대한 설명입니다"

"성능 이벤트의 소스"

"클러스터 보안 목표 관리"

"성능 클러스터 랜딩 페이지에서 클러스터 성능을 모니터링합니다"

"성능 인벤토리 페이지를 사용하여 성능 모니터링"

Unified Manager에서 직접 ONTAP 문제 또는 기능 관리

ONTAP 시스템 관리자나 ONTAP CLI를 사용할 필요 없이 Unified Manager 사용자 인터페이스에서 특정 ONTAP 문제를 직접 수정하거나 특정 ONTAP 기능을 관리할 수 있습니다. ""관리 작업"" 옵션은 Unified Manager 이벤트를 발생시킨 여러 ONTAP 문제에 대한 수정 사항을 제공합니다.

왼쪽 탐색 창에서 * 관리 작업 * 옵션을 선택하여 관리 작업 페이지에서 직접 문제를 해결할 수 있습니다. 관리 작업은 왼쪽 탐색 메뉴의 대시보드, 이벤트 세부 정보 페이지 및 워크로드 분석 선택 항목에 있는 관리 작업 패널에서도 사용할 수 있습니다.

Unified Manager에서 완벽하게 진단하고 한 가지 해결 방법을 제공할 수 있는 특정 문제가 있습니다. 안티 랜섬웨어 모니터링과 같은 특정 ONTAP 기능에 대해 Unified Manager가 내부 점검을 수행하고 특정 조치를 권장합니다. 사용 가능한 경우 이러한 해결 방법은 [Fix it*] 단추로 관리 작업 에 표시됩니다. 문제를 해결하려면 * Fix it * 버튼을 클릭하십시오. 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

Unified Manager가 ONTAP 명령을 클러스터에 전송하여 요청된 수정을 실행합니다. 수정이 완료되면 이벤트가 폐기됩니다.

일부 관리 작업을 통해 * 모두 수정 * 버튼을 사용하여 여러 스토리지 개체에서 동일한 문제를 해결할 수 있습니다. 예를 들어, "볼륨 자동 확장 사용"에 대한 * 모든 * 관리 수정 작업을 클릭하여 해결할 수 있는 "볼륨 공간이 가득 참" 이벤트가 있는 볼륨 5개가 있을 수 있습니다. 한 번의 클릭으로 5개의 볼륨에서 이 문제를 해결할 수 있습니다.

자동 조정을 사용하여 관리할 수 있는 ONTAP 문제 및 기능에 대한 자세한 내용은 을 참조하십시오 "Unified Manager로 해결할 수 있는 문제".

Fix it 또는 Fix All 단추가 표시되면 어떤 옵션이 있는지 확인합니다

관리 작업 페이지에서는 Unified Manager가 이벤트를 통해 통보한 문제를 해결하기 위해 * Fix it * 또는 * Fix All * 버튼을 제공합니다.

필요한 경우 단추를 클릭하여 문제를 해결하는 것이 좋습니다. 하지만 Unified Manager에서 권장하는 대로 문제를 해결할지 잘 모를 경우 다음 작업을 수행할 수 있습니다.

무엇을 하시겠습니까?	* 작업 *
Unified Manager에서 식별된 모든 개체의 문제를 해결하도록 지원	모두 수정 * 단추를 클릭합니다.
현재 식별된 개체에 대한 문제를 해결하지 말고 이벤트가 다시 발생할 때까지 이 관리 동작을 숨기십시오.	아래쪽 화살표를 클릭하고 * 모두 무시 * 를 클릭합니다.
식별된 개체 중 일부에 대해서만 문제를 해결합니다.	관리 작업의 이름을 클릭하여 목록을 확장하고 모든 개별 * Fix it * 작업을 표시한 다음 개별 관리 작업을 수정 또는 설치 해제합니다.

무엇을 하시겠습니까?	조치
Unified Manager로 문제를 해결하도록 지원	Fix it * 버튼을 클릭합니다.
이 때 문제를 해결하고 이벤트가 다시 발생할 때까지 이 관리 작업을 숨기십시오.	아래쪽 화살표를 클릭하고 * Dismiss * 를 클릭합니다.
문제를 더 잘 이해할 수 있도록 이 이벤트에 대한 세부 정보를 표시합니다.	• Fix it * 버튼을 클릭하고 결과 대화 상자에 적용할 수정 사항을 검토합니다. • 아래쪽 화살표를 클릭하고 * 이벤트 세부 정보 보기 * 를 클릭하여 이벤트 세부 정보 페이지를 표시합니다. 그런 다음 문제를 해결하려면 이러한 결과 페이지 중 하나에서 * Fix it * 을 클릭합니다.
문제를 더 잘 이해할 수 있도록 이 스토리지 개체의 세부 정보를 표시합니다.	성능 탐색기 또는 상태 세부 정보 페이지에 세부 정보를 표시하려면 스토리지 개체의 이름을 클릭합니다.

경우에 따라 15분 구성 폴에 수정 사항이 반영됩니다. 구성 변경을 확인하고 이벤트가 폐기되는 데 최대 몇 시간이 걸릴 수도 있습니다.

완료 또는 진행 중인 관리 작업의 목록을 보려면 필터 아이콘을 클릭하고 * Completed * (완료됨 *) 또는 * In Progress * (진행 중 *)를 선택합니다.

모든 작업을 직렬로 수정함으로써 * In Progress * (진행 중 *) 패널을 볼 때 일부 개체는 Status * In Progress * (상태 * 진행 중 *)가 있는 반면, 다른 개체는 Status * Scheduled * (상태 * 예약됨 *)가 있는 것입니다. 이는 해당 개체가 계속 구현되기를 기다리고 있음을 의미합니다.

수정하도록 선택한 관리 작업의 상태를 봅니다

관리 작업 페이지에서 수정하도록 선택한 모든 관리 작업의 상태를 볼 수 있습니다. 대부분의 작업은 Unified Manager가 ONTAP 명령을 클러스터로 전송한 후 * completed * 로 거의 빠르게 표시됩니다. 그러나 볼륨 이동 등의 일부 작업은 시간이 오래 걸릴 수 있습니다.

관리 작업 페이지에는 다음 세 가지 필터를 사용할 수 있습니다.

- * 완료됨 * 에는 성공적으로 완료된 관리 작업과 실패한 관리 작업이 모두 표시됩니다. * 실패 * 작업은 문제를 수동으로 해결할 수 있도록 실패 이유를 제공합니다.
- * 진행 중 * 은 구현 중인 관리 작업과 구현될 예정인 관리 작업을 모두 표시합니다.
- * 권장 * 은 모니터링되는 모든 클러스터에 대해 현재 활성화된 모든 관리 작업을 표시합니다.

단계

1. 왼쪽 탐색 창에서 * 관리 작업 * 을 클릭합니다. 또는 을 클릭합니다 ⋮ 대시보드 * 의 * 관리 작업 * 패널 상단에서 보려는 보기를 선택합니다.

   관리 작업 페이지가 표시됩니다.

2. [설명*] 필드의 관리 작업 옆에 있는 캐럿 아이콘을 클릭하여 문제 및 문제 해결에 사용되는 명령에 대한 세부 정보를 볼 수 있습니다.
3. 실패한 * 작업을 보려면 * Completed * View(완료 * 보기)의 * Status *(상태 *) 열을 기준으로 정렬합니다. 이와 같은 용도로 * 필터 * 도구를 사용할 수 있습니다.
4. 실패한 관리 작업에 대한 자세한 정보를 보거나 권장 관리 작업을 수정하려는 경우 관리 작업 옆에 있는 캐럿 아이콘을 클릭한 후 확장된 영역에서 * 이벤트 세부 정보 보기 * 를 클릭할 수 있습니다. 해당 페이지에서 * Fix it * 버튼을 사용할 수 있습니다.

Unified Manager로 해결할 수 있는 문제

Active IQ Unified Manager의 자동 수정 기능을 사용하면 Unified Manager를 통해 특정 ONTAP 문제를 해결하거나 랜섬웨어 방지 모니터링과 같은 특정 ONTAP 기능을 효과적으로 관리할 수 있습니다.

이 표에서는 ONTAP 웹 UI의 * Fix it * 또는 * Fix All * 버튼을 통해 직접 관리할 수 있는 문제 또는 기능에 대해 설명합니다.

이벤트 이름 및 설명	관리 조치	**"Fix it"** 작업
볼륨 공간이 가득 찼습니다 볼륨에 공간이 거의 없어 용량 최대 임계값을 위반했습니다. 이 임계값은 기본적으로 볼륨 크기의 90%로 설정되어 있습니다.	볼륨 자동 확장 활성화	Unified Manager에서 볼륨 자동 확장이 이 볼륨에 구성되지 않음을 확인할 수 있으므로 이 기능을 사용하면 필요할 때 볼륨 용량이 증가합니다.
inode가 꽉 찼습니다 이 볼륨은 inode가 부족하며 새 파일을 수락할 수 없습니다.	볼륨의 inode 수를 늘립니다	볼륨의 inode 수를 2% 늘립니다.
스토리지 계층 정책 불일치가 발견되었습니다 볼륨에 비활성 데이터가 많이 있고 현재 계층화 정책이 "스냅샷 전용" 또는 "없음"으로 설정되어 있습니다.	자동 클라우드 계층화 지원	볼륨이 이미 FabricPool에 있으므로 비활성 데이터가 저비용 클라우드 계층으로 이동하도록 계층화 정책을 "자동"으로 변경합니다.
스토리지 계층 불일치가 발견되었습니다 볼륨에 비활성 데이터가 많이 있지만 클라우드 지원 스토리지 계층(FabricPool)에 상주하지 않는 경우	볼륨의 스토리지 계층을 변경합니다	볼륨을 클라우드 지원 스토리지 계층으로 이동하고 계층화 정책을 "자동"으로 설정하여 비활성 데이터를 클라우드 계층으로 이동합니다.

이벤트 이름 및 설명	관리 조치	**"Fix it"** 작업
감사 로그 사용 안 함 스토리지 VM에 대해 감사 로그가 설정되지 않았습니다	스토리지 VM에 대한 감사 로깅을 설정합니다	스토리지 VM에 대한 감사 로깅을 설정합니다. 스토리지 VM에는 이미 로컬 또는 원격 감사 로그 위치가 구성되어 있어야 합니다.
로그인 배너 사용 안 함 액세스 제한을 명확히 하여 보안을 강화하려면 클러스터의 로그인 배너를 활성화해야 합니다.	클러스터의 로그인 배너를 설정합니다	클러스터 로그인 배너를 "'권한 있는 사용자로 액세스 제한'으로 설정합니다.
로그인 배너 사용 안 함 스토리지 VM의 로그인 배너는 액세스 제한을 명확히 하여 보안을 강화하도록 설정해야 합니다.	스토리지 VM의 로그인 배너를 설정합니다	스토리지 VM 로그인 배너를 "권한이 있는 사용자로 액세스 제한"으로 설정합니다.
SSH가 보안 암호 를 사용하고 있습니다 "-CBC"라는 접미사가 있는 Cipherers는 안전하지 않은 것으로 간주됩니다.	클러스터에서 안전하지 않은 암호를 제거합니다	클러스터에서 AES192-CBC 및 aes128-CBC와 같은 안전하지 않은 암호를 제거합니다.
SSH가 보안 암호 를 사용하고 있습니다 "-CBC"라는 접미사가 있는 Cipherers는 안전하지 않은 것으로 간주됩니다.	스토리지 VM에서 안전하지 않은 암호를 제거합니다	스토리지 VM에서 AES192-CBC 및 aes128-CBC와 같은 안전하지 않은 암호를 제거합니다.
AutoSupport HTTPS 전송이 비활성화되었습니다 AutoSupport 메시지를 기술 지원 부서에 보내는 데 사용되는 전송 프로토콜을 암호화해야 합니다.	HTTPS를 AutoSupport 메시지의 전송 프로토콜로 설정합니다	HTTPS를 클러스터의 AutoSupport 메시지에 대한 전송 프로토콜로 설정합니다.
클러스터 로드 불균형 임계값이 위반되었습니다 클러스터의 노드 간에 로드가 균형 조정되지 않음을 나타냅니다. 이 이벤트는 노드 간 사용된 성능 용량의 차이가 30%를 초과할 때 생성됩니다.	클러스터 워크로드의 균형 조정	Unified Manager에서는 불균형을 줄이기 위해 한 노드에서 다른 노드로 이동하는 데 가장 적합한 볼륨을 식별한 후 볼륨을 이동합니다.

이벤트 이름 및 설명	관리 조치	**"Fix it"** 작업
클러스터 용량 불균형 임계값이 위반되었습니다 클러스터의 애그리게이트 간에 용량이 불균형임을 나타냅니다. 이 이벤트는 사용된 용량의 차이가 애그리게이트 간에 70% 이상일 때 생성됩니다.	클러스터 용량의 균형을 맞춥니다	Unified Manager에서는 불균형을 줄이기 위해 애그리게이트 간에 이동하는 데 가장 적합한 볼륨을 식별한 후 볼륨을 이동합니다.
사용된 성능 용량 임계값 위반 사용률이 1개 이상의 매우 높은 워크로드까지 감소하지 않을 경우 노드의 부하가 과도하게 사용될 수 있음을 나타냅니다. 이 이벤트는 사용된 노드 성능 용량이 12시간 이상 100% 이상인 경우 생성됩니다.	노드의 최대 부하 제한	Unified Manager는 가장 높은 IOPS를 가진 볼륨을 식별하고 기간별 예상 및 최대 IOPS 수준을 사용하여 QoS 정책을 적용하여 노드의 부하를 줄입니다.
동적 이벤트 경고 임계값이 위반되었습니다 일부 워크로드의 비정상적으로 높은 부하로 인해 노드가 이미 과부하된 상태로 작동하고 있음을 나타냅니다.	노드의 과부하 감소	Unified Manager는 가장 높은 IOPS를 가진 볼륨을 식별하고 기간별 예상 및 최대 IOPS 수준을 사용하여 QoS 정책을 적용하여 노드의 부하를 줄입니다.
테이크오버가 가능하지 않습니다 페일오버를 현재 사용할 수 없으므로 중단 또는 재부팅 중 노드의 리소스에 대한 액세스는 노드를 다시 사용할 수 있을 때까지 손실됩니다.	노드 페일오버 설정	Unified Manager가 적절한 명령을 전송하여 클러스터의 모든 노드에서 페일오버를 사용하도록 설정합니다.
옵션 cf.takeover.on_panic이 off로 구성됩니다 노드 쉘의 옵션 "cf.Takeover.on_panic"은 * off * 로 설정되어 HA 구성 시스템에서 문제를 일으킬 수 있습니다.	패닉 시 Takeover를 설정합니다	Unified Manager가 적절한 명령을 클러스터에 전송하여 이 설정을 * On * 으로 변경합니다.
nodesell 옵션 SnapMirror.enable을 비활성화합니다 이전 노드 쉘의 옵션 "SnapMirror.enable"은 * On * 으로 설정되어 ONTAP 9.3 이상으로 업그레이드한 후 부팅 중에 문제가 발생할 수 있습니다.	SnapMirror.enable 옵션을 off로 설정합니다	Unified Manager가 적절한 명령을 클러스터에 전송하여 이 설정을 * 꺼짐 * 으로 변경합니다.

이벤트 이름 및 설명	관리 조치	**"Fix it"** 작업
텔넷이 활성화되었습니다 텔넷이 안전하지 않고 암호화되지 않은 방식으로 데이터를 전달하므로 잠재적인 보안 문제를 나타냅니다.	텔넷을 비활성화합니다	Unified Manager가 텔넷을 사용하지 않도록 클러스터에 적절한 명령을 보냅니다.
스토리지 VM 안티 랜섬웨어 학습 구성 랜섬웨어 방지 모니터링 라이센스가 있는 클러스터를 주기적으로 확인합니다. 스토리지 VM이 해당 클러스터에서 NFS 또는 SMB 볼륨만 지원하는지 확인합니다.	스토리지 VM을 랜섬웨어 방지 모니터링의 '학습' 모드로 전환합니다	Unified Manager는 클러스터 관리 콘솔을 통해 스토리지 VM의 랜섬웨어 방지 모니터링을 '학습' 상태로 설정합니다. 스토리지 VM에서 생성된 모든 새 볼륨의 랜섬웨어 방지 모니터링은 학습 모드로 자동으로 이동됩니다. ONTAP는 이러한 지원을 통해 볼륨에서 활동 패턴을 학습하고 잠재적인 악성 공격으로 인한 이상 징후를 감지할 수 있습니다.
볼륨 안티 랜섬웨어 학습을 구성하십시오 랜섬웨어 방지 모니터링 라이센스가 있는 클러스터를 주기적으로 확인합니다. 볼륨이 해당 클러스터에서 NFS 또는 SMB 서비스만 지원하는지 확인합니다.	볼륨을 안티 랜섬웨어 모니터링의 '학습' 모드로 전환하십시오	Unified Manager는 클러스터 관리 콘솔을 통해 볼륨에 대한 안티 랜섬웨어 모니터링을 '학습' 상태로 설정합니다. ONTAP는 이러한 지원을 통해 볼륨에서 활동 패턴을 학습하고 잠재적인 악성 공격으로 인한 이상 징후를 감지할 수 있습니다.
볼륨 안티 랜섬웨어 기능을 활성화하십시오 랜섬웨어 방지 모니터링 라이센스가 있는 클러스터를 주기적으로 확인합니다. 볼륨이 45일 이상 안티 랜섬웨어 모니터링의 '학습' 모드에 있는지 여부를 감지하고 해당 볼륨을 액티브 모드로 전환할 가능성을 결정합니다.	볼륨을 랜섬웨어 방지 모니터링의 활성 모드로 설정합니다	Unified Manager는 클러스터 관리 콘솔을 통해 볼륨에 대한 안티 랜섬웨어 모니터링을 '활성'으로 설정합니다. ONTAP는 이러한 지원을 통해 볼륨에서 활동 패턴을 학습하고 잠재적인 악성 공격으로 인한 이상 징후를 탐지하고 데이터 보호 작업에 대한 경고를 생성할 수 있습니다.
볼륨 안티 랜섬웨어를 비활성화합니다 랜섬웨어 방지 모니터링 라이센스가 있는 클러스터를 주기적으로 확인합니다. 볼륨에서 액티브 안티 랜섬웨어 모니터링 중에 반복적인 알림을 감지합니다(예: 잠재적인 랜섬웨어 공격에 대한 여러 경고는 30일 이상 반환됨).	볼륨에 대한 랜섬웨어 방지 모니터링을 비활성화합니다	Unified Manager는 클러스터 관리 콘솔을 통해 볼륨에 대한 안티 랜섬웨어 모니터링을 비활성화합니다.

맞춤형 스크립트를 생성하여 알림에 연결하면 특정 이벤트에 대한 특정 작업을 수행할 수 있으며, 관리 작업 페이지 또는 Unified Manager 대시보드에서 사용할 수 있는 기본 관리 작업을 선택하지 않습니다.

이벤트 유형에 대한 특정 작업을 수행하고 Unified Manager에서 제공하는 관리 작업 기능의 일부로 수정하지 않도록 선택하면 특정 작업에 대한 사용자 지정 스크립트를 구성할 수 있습니다. 그런 다음 스크립트를 해당 이벤트 유형에 대한 알림과 연결하고 이러한 이벤트를 개별적으로 처리할 수 있습니다. 이 경우 관리 작업 페이지 또는 Unified Manager 대시보드에서 특정 이벤트 유형에 대한 관리 작업이 생성되지 않습니다.

클러스터 관리

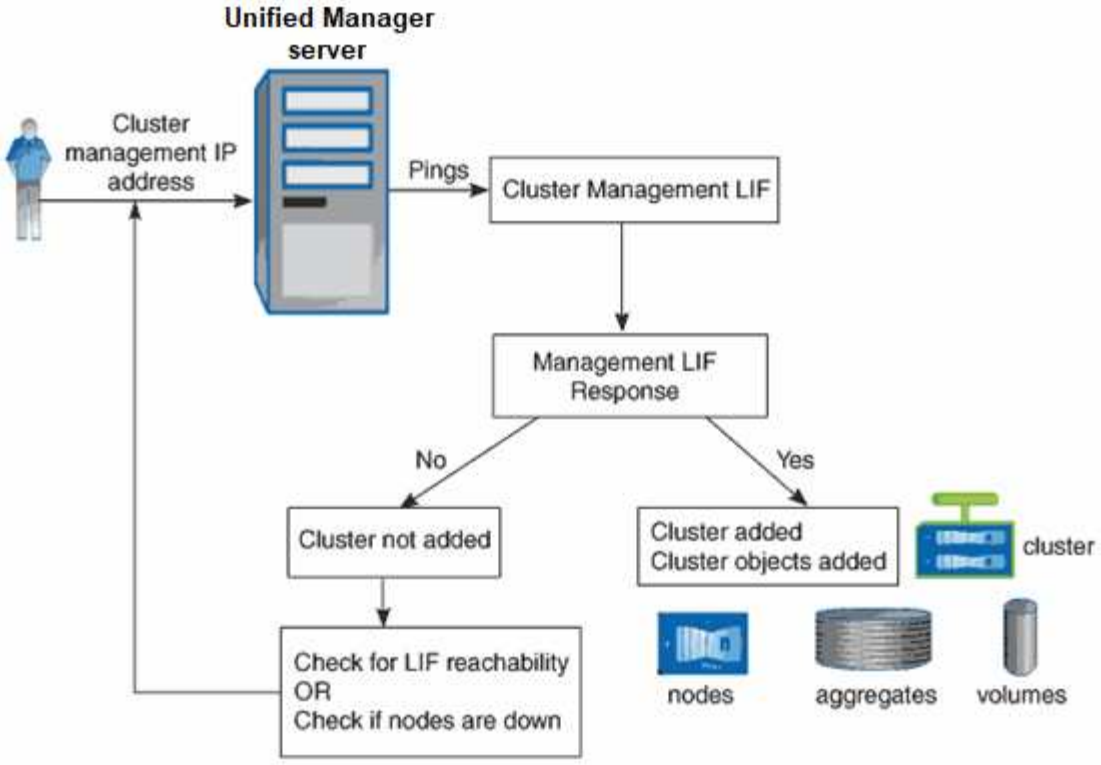
Unified Manager를 사용하여 클러스터를 모니터링, 추가, 편집, 제거하여 ONTAP 클러스터를 관리할 수 있습니다.

클러스터 검색 프로세스의 작동 방식

Unified Manager에 클러스터를 추가하면 서버에서 클러스터 개체를 검색하여 해당 데이터베이스에 추가합니다. 검색 프로세스가 작동하는 방식을 이해하면 조직의 클러스터와 개체를 관리하는 데 도움이 됩니다.

클러스터 구성 정보 수집을 위한 모니터링 간격은 15분입니다. 예를 들어, 클러스터를 추가한 후에는 15분 이내에 Unified Manager UI에 클러스터 객체를 표시할 수 있습니다. 이 기간은 클러스터를 변경할 때도 적용됩니다. 예를 들어, 클러스터의 SVM에 새 볼륨 2개를 추가하는 경우 다음 폴링 간격 후 UI에서 새로운 객체를 볼 수 있으며 이는 최대 15분이 될 수 있습니다.

다음 그림에서는 검색 프로세스를 보여 줍니다.



새 클러스터의 모든 객체가 검색된 후 Unified Manager가 이전 15일 동안 기간별 성능 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능은 클러스터를 추가한 직후 2주 이상의 클러스터 성능 정보를 제공합니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.

15일간의 성능 데이터 수집은 CPU를 많이 사용하므로 데이터 연속성 수집 폴이 너무 많은 클러스터에서 동시에 실행되지 않도록 새 클러스터를 추가하는 시차를 두는 것이 좋습니다.

모니터링되는 클러스터 목록 보기

클러스터 설정 페이지를 사용하여 클러스터 인벤토리를 볼 수 있습니다. 이름 또는 IP 주소, 통신 상태와 같은 클러스터에 대한 세부 정보를 볼 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.

   Unified Manager에서 관리하는 스토리지 환경의 모든 클러스터가 표시됩니다. 클러스터 목록은 컬렉션 상태 심각도 수준 열을 기준으로 정렬됩니다. 열 머리글을 클릭하여 클러스터를 다른 열을 기준으로 정렬할 수 있습니다.

클러스터 추가

클러스터를 모니터링할 수 있도록 Active IQ Unified Manager에 클러스터를 추가할 수 있습니다. 여기에는 발생할 수 있는 문제를 찾아 해결할 수 있도록 클러스터의 상태, 용량, 성능,

구성 등과 같은 클러스터 정보를 가져오는 기능도 포함됩니다.

- 필요한 것 *
- 애플리케이션 관리자 역할 또는 스토리지 관리자 역할이 있어야 합니다.
- 다음 정보가 있어야 합니다.
  - Unified Manager는 사내 ONTAP 클러스터, ONTAP Select, Cloud Volumes ONTAP를 지원합니다.
  - 클러스터에 대한 호스트 이름 또는 클러스터 관리 IP 주소(IPv4 또는 IPv6)가 있어야 합니다.

    호스트 이름을 사용할 때는 클러스터 관리 LIF의 클러스터 관리 IP 주소로 해석해야 합니다. 노드 관리 LIF를 사용하면 작업이 실패합니다.

  - 클러스터에 액세스하려면 사용자 이름과 암호가 있어야 합니다.

    이 계정에는 응용 프로그램 액세스 권한이 *ontapi*, *console* 및 _http_로 설정된 _admin_역할이 있어야 합니다.

  - HTTPS 프로토콜(일반적으로 포트 443)을 사용하여 클러스터에 연결하려면 포트 번호를 알아야 합니다.
  - 클러스터에서 ONTAP 버전 9.1 소프트웨어 이상을 실행해야 합니다.
  - Unified Manager 서버에 적절한 공간이 있어야 합니다. 90% 이상의 공간이 이미 사용된 경우 서버에 클러스터를 추가할 수 없습니다.
  - 필요한 인증서가 있습니다.
- SSL(HTTPS) 인증서 *: 이 인증서는 Unified Manager에서 소유합니다. Unified Manager를 새로 설치하면 자체 서명된 기본 SSL(HTTPS) 인증서가 생성됩니다. 보안을 강화하기 위해 CA 서명 인증서로 업그레이드하는 것이 좋습니다. 서버 인증서가 만료되면 해당 인증서를 다시 생성하고 Unified Manager를 다시 시작하여 새 인증서를 통합하는 서비스를 수행해야 합니다. SSL 인증서 재생성에 대한 자세한 내용은 을 참조하십시오 "HTTPS 보안 인증서를 생성하는 중입니다".
- EMS 인증서 *: 이 인증서는 Unified Manager에서 소유합니다. ONTAP로부터 수신한 EMS 알림에 대한 인증 중에 사용된다.
- 상호 TLS 통신을 위한 인증서 *: Unified Manager와 ONTAP 간의 상호 TLS 통신 중에 사용됩니다. 인증서 기반 인증은 ONTAP 버전에 따라 클러스터에 대해 설정됩니다. ONTAP 버전을 실행하는 클러스터가 9.5보다 낮은 경우 인증서 기반 인증이 활성화되지 않습니다.

  이전 버전의 Unified Manager를 업데이트하는 경우 클러스터에 대해 인증서 기반 인증이 자동으로 활성화되지 않습니다. 그러나 클러스터 세부 정보를 수정 및 저장하여 이 기능을 사용하도록 설정할 수 있습니다. 인증서가 만료되면 인증서를 다시 생성하여 새 인증서를 통합해야 합니다. 인증서 보기 및 재생에 대한 자세한 내용은 을 참조하십시오 "클러스터 편집".

  - 웹 UI에서 클러스터를 추가할 수 있으며 인증서 기반 인증이 자동으로 활성화됩니다.
  - Unified Manager CLI를 통해 클러스터를 추가할 수 있으며, 인증서 기반 인증은 기본적으로 사용되지 않습니다. Unified Manager CLI를 사용하여 클러스터를 추가하는 경우 Unified Manager UI를 사용하여 클러스터를 편집해야 합니다. 확인할 수 있습니다 "지원되는 Unified Manager CLI 명령" 을 사용하여 Unified Manager CLI를 사용하여 클러스터를 추가합니다.
  - 클러스터에 대해 인증서 기반 인증을 사용하고 서버에서 Unified Manager 백업을 수행한 후 호스트 이름 또는 IP 주소가 변경된 다른 Unified Manager 서버로 복원하면 클러스터 모니터링이 실패할 수 있습니다. 이 문제를 방지하려면 클러스터 세부 정보를 편집하고 저장합니다. 클러스터 세부 정보 편집에 대한 자세한 내용은 을 참조하십시오 "클러스터 편집".

- 클러스터 인증서 *: 이 인증서는 ONTAP에서 소유합니다. 만료된 인증서가 있는 클러스터는 Unified Manager에 추가할 수 없으며, 인증서가 이미 만료된 경우 클러스터를 추가하기 전에 다시 생성해야 합니다. 인증서 생성에 대한 자세한 내용은 기술 자료(KB) 문서를 참조하십시오 "System Manager 사용자 인터페이스에서 ONTAP 자체 서명된 인증서를 갱신하는 방법".
- Unified Manager의 단일 인스턴스에서 특정 수의 노드를 지원할 수 있습니다. 지원되는 노드 수를 초과하는 환경을 모니터링해야 하는 경우, 일부 클러스터를 모니터링하려면 Unified Manager의 추가 인스턴스를 설치해야 합니다. 지원되는 노드 수 목록을 보려면 를 참조하십시오 "Unified Manager 모범 사례 가이드".

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.
2. 클러스터 설정 페이지에서 * 추가 * 를 클릭합니다.
3. 클러스터 추가 대화 상자에서 필요에 따라 값을 지정한 다음 * 제출 * 을 클릭합니다.
4. 호스트 인증 대화 상자에서 * 인증서 보기 * 를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
5. 예 * 를 클릭합니다.

   클러스터 세부 정보를 저장한 후에는 클러스터의 상호 TLS 통신에 대한 인증서를 볼 수 있습니다.

   인증서 기반 인증이 활성화되지 않은 경우 Unified Manager는 클러스터가 처음에 추가될 때만 인증서를 확인합니다. Unified Manager에서는 ONTAP에 대한 각 API 호출의 인증서를 확인하지 않습니다.

새 클러스터의 모든 객체가 검색된 후 Unified Manager가 이전 15일 동안 기간별 성능 데이터를 수집하기 시작합니다. 이러한 통계는 데이터 연속성 수집 기능을 사용하여 수집됩니다. 이 기능은 클러스터를 추가한 직후 2주 이상의 클러스터 성능 정보를 제공합니다. 데이터 연속성 수집 주기가 완료되면 기본적으로 5분마다 실시간 클러스터 성능 데이터가 수집됩니다.

15일간의 성능 데이터 수집은 CPU를 많이 사용하므로 데이터 연속성 수집 폴이 너무 많은 클러스터에서 동시에 실행되지 않도록 새 클러스터를 추가하는 시차를 두는 것이 좋습니다. 또한, 데이터 연속성 수집 기간 동안 Unified Manager를 다시 시작하면 수집이 중단되고 성능 차트의 누락된 시간 간격이 표시됩니다.

클러스터를 추가할 수 없다는 오류 메시지가 표시되면 다음 문제가 있는지 확인하십시오.

- 두 시스템의 시계가 동기화되지 않고 Unified Manager HTTPS 인증서 시작 날짜가 클러스터의 날짜보다 이후인 경우 NTP 또는 이와 유사한 서비스를 사용하여 시계가 동기화되었는지 확인해야 합니다.
- 클러스터가 최대 EMS 알림 대상 수에 도달하면 Unified Manager 주소를 추가할 수 없습니다. 기본적으로 클러스터에 20개의 EMS 알림 대상만 정의할 수 있습니다.

- 관련 정보 *

"사용자 추가"

"클러스터 목록 및 세부 정보 보기"

"서명되고 반환된 HTTPS 인증서를 설치하는 중입니다"

클러스터 편집

클러스터 편집 대화 상자를 사용하여 호스트 이름 또는 IP 주소, 사용자 이름, 암호 및 포트와 같은 기존 클러스터의 설정을 수정할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할 또는 스토리지 관리자 역할이 있어야 합니다.

Unified Manager 9.7부터는 HTTPS만 사용하여 클러스터를 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.
2. 클러스터 설정 * 페이지에서 편집할 클러스터를 선택한 다음 * 편집 * 을 클릭합니다.
3. 클러스터 편집 * 대화 상자에서 필요에 따라 값을 수정합니다. +Unified Manager에 추가된 클러스터에 대한 세부 정보를 수정한 경우 ONTAP 버전에 따라 상호 TLS 통신에 대한 인증서 세부 정보를 볼 수 있습니다. ONTAP 버전에 대한 자세한 내용은 를 참조하십시오 "상호 TLS 통신용 인증서". + * 인증서 세부 정보 * 를 클릭하여 인증서 세부 정보를 볼 수 있습니다. 인증서가 만료된 경우 * 재생성 * 버튼을 클릭하여 새 인증서를 통합하십시오.
4. 제출 * 을 클릭합니다.
5. 호스트 인증 대화 상자에서 * 인증서 보기 * 를 클릭하여 클러스터에 대한 인증서 정보를 확인합니다.
6. 예 * 를 클릭합니다.
    - 관련 정보 *

"사용자 추가"

"클러스터 목록 및 세부 정보 보기"

클러스터를 제거하는 중입니다

클러스터 설정 페이지를 사용하여 Unified Manager에서 클러스터를 제거할 수 있습니다. 예를 들어, 클러스터 검색에 실패하거나 스토리지 시스템의 서비스를 해제하려는 경우 클러스터를 제거할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할 또는 스토리지 관리자 역할이 있어야 합니다.

이 작업을 수행하면 Unified Manager에서 선택한 클러스터가 제거됩니다. 클러스터가 제거된 후에는 더 이상 모니터링되지 않습니다. 제거된 클러스터에 등록된 Unified Manager의 인스턴스도 클러스터에서 등록 취소됩니다.

또한 클러스터를 제거하면 Unified Manager에서 해당 스토리지 오브젝트, 기간별 데이터, 스토리지 서비스 및 연결된 모든 이벤트가 삭제됩니다. 이러한 변경 사항은 다음 데이터 수집 주기 이후 재고 페이지 및 세부 정보 페이지에 반영됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.

2. 클러스터 설정 페이지에서 제거할 클러스터를 선택하고 * 제거 * 를 클릭합니다.
3. 데이터 소스 제거 * 메시지 대화 상자에서 * 제거 * 를 클릭하여 제거 요청을 확인합니다.
    ◦ 관련 정보 *

"사용자 추가"

"클러스터 목록 및 세부 정보 보기"

클러스터 재검색

클러스터의 상태, 모니터링 상태 및 성능 상태에 대한 최신 정보를 얻으려면 클러스터 설정 페이지에서 클러스터를 수동으로 다시 검색할 수 있습니다.

공간이 부족할 때 애그리게이트의 크기를 증가하는 것과 같이 클러스터를 업데이트하고 싶은 경우 클러스터를 수동으로 다시 검색할 수 있으며, Unified Manager에서 변경 사항을 검색하도록 할 수 있습니다.

Unified Manager를 WFA(OnCommand Workflow Automation)와 페어링하면 WFA에 의해 캐시된 데이터를 다시 취득하게 됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.
2. 클러스터 설정 * 페이지에서 * 재검색 * 을 클릭합니다.

    Unified Manager가 선택한 클러스터를 다시 검색하고 최신 상태 및 성능 상태를 표시합니다.

    ◦ 관련 정보 *

"클러스터 목록 및 세부 정보 보기"

VMware 가상 인프라스트럭처 모니터링

Active IQ Unified Manager는 가상 인프라의 가상 머신(VM)에 대한 가시성을 제공하며, 가상 환경에서 스토리지 및 성능 문제를 모니터링하고 문제를 해결할 수 있도록 지원합니다. 이 기능을 사용하여 스토리지 환경에서 지연 시간 문제가 있는지 또는 vCenter Server에 보고된 성능 이벤트가 있는지 확인할 수 있습니다.

ONTAP 기반의 일반적인 가상 인프라 구축에는 컴퓨팅, 네트워크 및 스토리지 계층 전체에 분산된 다양한 구성 요소가 있습니다. VM 애플리케이션의 성능 지연은 각 계층의 다양한 구성 요소에 의해 발생하는 지연 시간의 조합으로 인해 발생할 수 있습니다. 이 기능은 가상 환경에서 성능 문제를 분석하고 문제가 발생한 구성 요소를 파악해야 하는 스토리지 및 vCenter Server 관리자와 일반 IT 사용자에게 유용합니다.

이제 VMware 섹션의 vCenter 메뉴에서 vCenter Server에 액세스할 수 있습니다. 나열된 각 가상 머신의 PEEK 뷰에는 새 브라우저에서 vCenter Server를 실행하는 토폴로지 뷰에 * vCenter Server * 링크가 있습니다. 또한 * Expand Topology * 버튼을 사용하여 vCenter Server를 시작하고 * View in vCenter * 버튼을 클릭하여 vCenter Server에서 데이터 저장소를 볼 수도 있습니다.

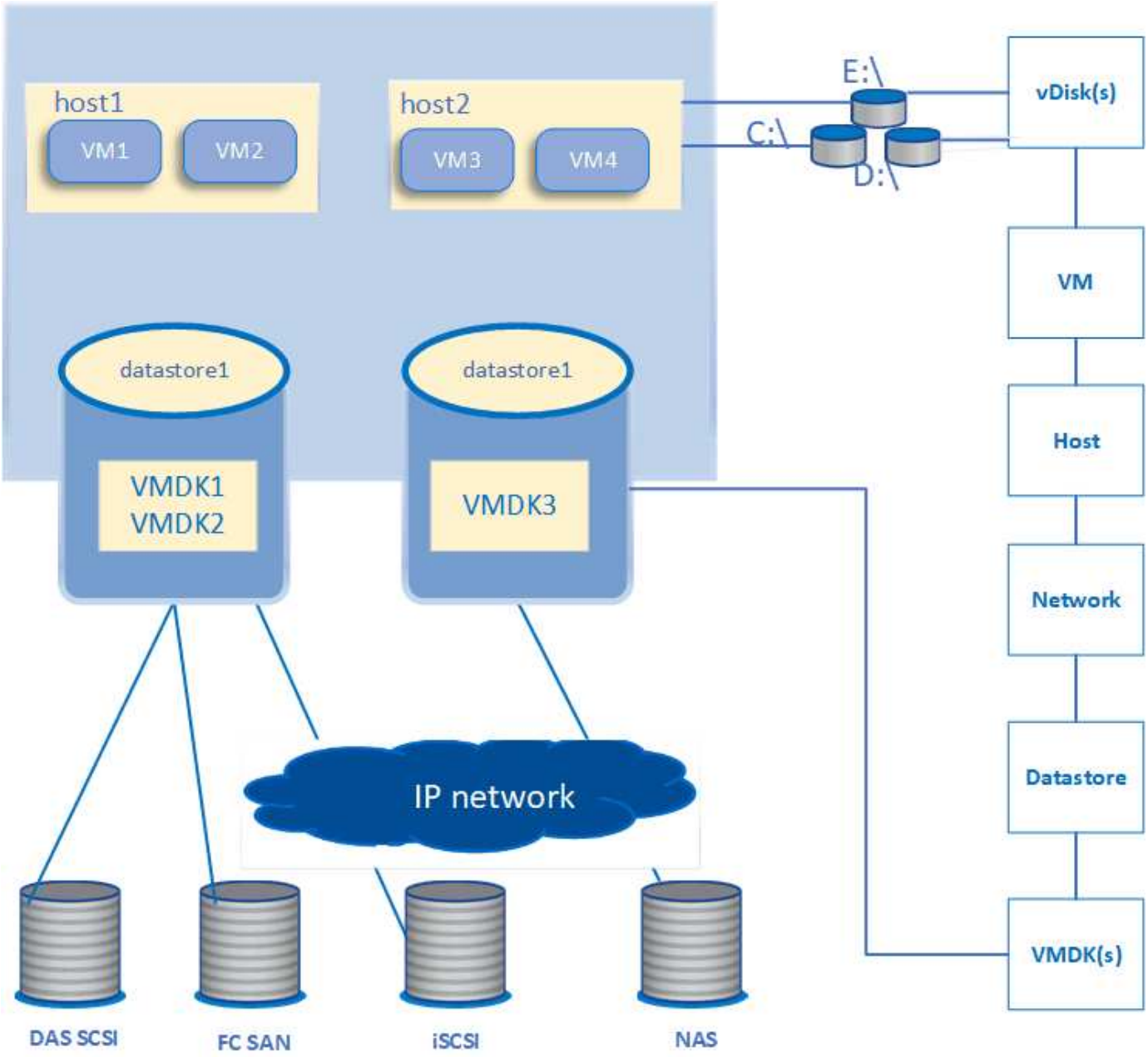
Unified Manager는 가상 환경의 기본 하위 시스템을 토폴로지 뷰에서 제공하므로 컴퓨팅 노드, 네트워크 또는 스토리지에서 지연 시간 문제가 발생했는지 여부를 확인할 수 있습니다. 또한 개선 단계를 수행하고 기본 문제를 해결하는 데 성능 지연이 발생하는 특정 개체를 중점적으로 보여 줍니다.

ONTAP 스토리지에 구축된 가상 인프라스트럭처에는 다음과 같은 객체가 포함됩니다.

- vCenter Server: 가상 환경에서 VMware VM, ESXi 호스트 및 모든 관련 구성 요소를 관리하기 위한 중앙 집중식 컨트롤 플레인 vCenter Server에 대한 자세한 내용은 VMware 설명서를 참조하십시오.
- 호스트: ESXi를 실행하는 물리적 또는 가상 시스템, VMware의 가상화 소프트웨어 및 VM을 호스팅합니다.
- 데이터 저장소: 데이터 저장소는 ESXi 호스트에 접속된 가상 스토리지 객체입니다. 데이터 저장소는 로그 파일, 스크립트, 구성 파일 및 가상 디스크와 같은 VM 파일의 저장소로 사용되는 LUN 또는 볼륨과 같은 ONTAP의 관리 가능한 스토리지 엔터티입니다. SAN 또는 IP 네트워크 연결을 통해 환경의 호스트에 연결됩니다. vCenter Server에 매핑된 ONTAP 외부의 데이터 저장소는 Unified Manager에서 지원되지 않거나 표시되지 않습니다.
- VM: VMware 가상 머신
- 가상 디스크: VMDK로 확장하는 VM에 속한 데이터 저장소의 가상 디스크 가상 디스크의 데이터는 해당 VMDK에 저장됩니다.
- VMDK: 가상 디스크에 대한 스토리지 공간을 제공하는 데이터 저장소의 가상 머신 디스크입니다. 각 가상 디스크에 해당하는 VMDK가 있습니다.

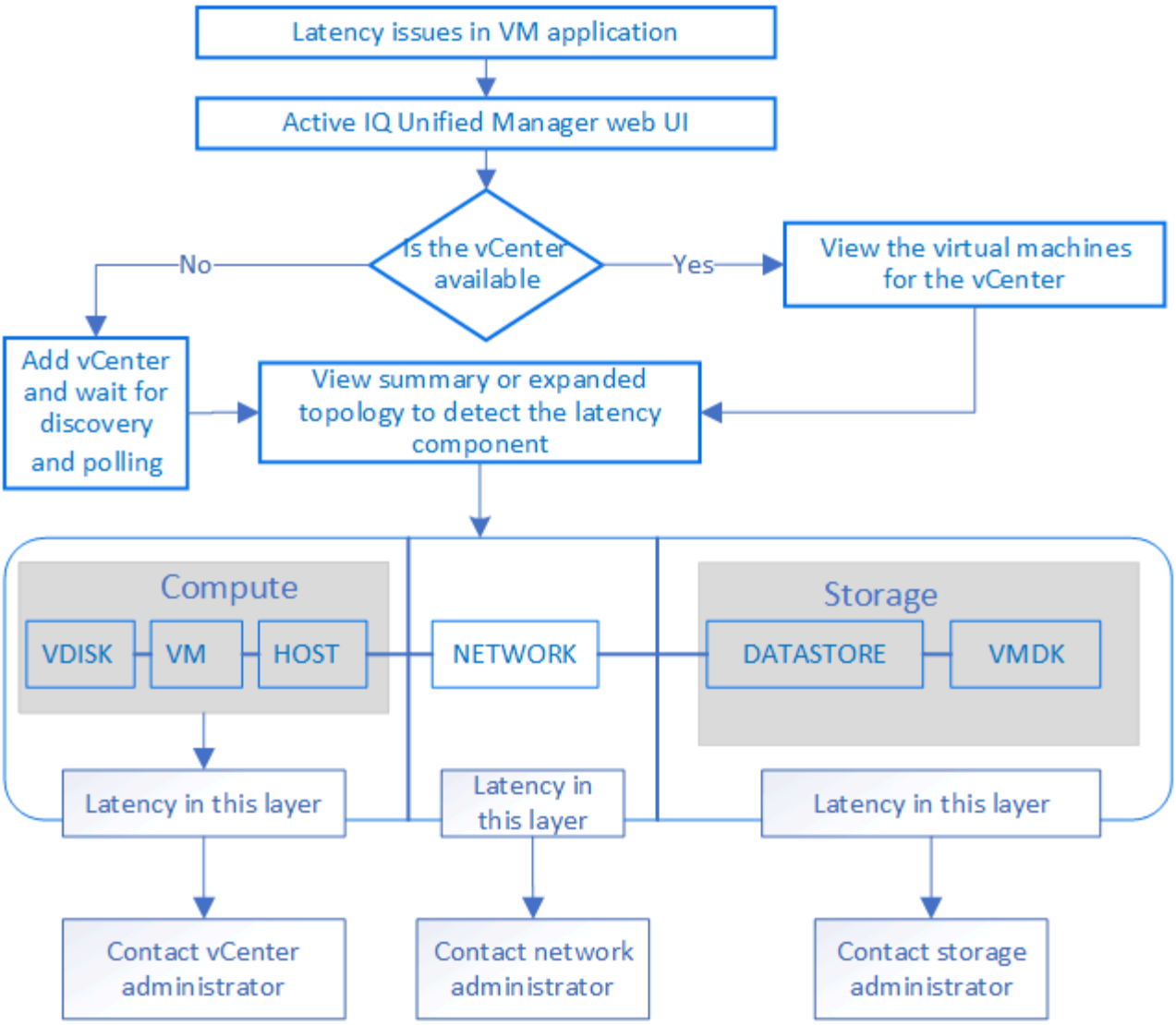
이러한 객체는 VM 토폴로지 뷰로 표시됩니다.

- ONTAP * 기반 VMware 가상화



- 사용자 워크플로 *

다음 다이어그램에서는 VM 토폴로지 뷰를 사용하는 일반적인 사용 사례를 보여 줍니다.



지원되지 않는 것은 무엇입니까

- ONTAP 외부에 있고 vCenter Server 인스턴스에 매핑된 데이터 저장소는 Unified Manager에서 지원되지 않습니다. 이러한 데이터 저장소에 가상 디스크가 있는 VM도 지원되지 않습니다.
- 여러 LUN에 걸쳐 있는 데이터 저장소는 지원되지 않습니다.
- 데이터 LIF(액세스 엔드포인트)를 매핑하기 위해 NAT(Network Address Translation)를 사용하는 데이터 저장소는 지원되지 않습니다.
- 여러 LIF 구성에서 동일한 IP 주소를 가진 서로 다른 클러스터에서 볼륨 또는 LUN을 데이터 저장소로 내보내는 기능은 Unified Manager에서 어떤 데이터 저장소가 어떤 클러스터에 속해 있는지 식별할 수 없으므로 지원되지 않습니다.

  예: 클러스터 A에 데이터 저장소 A가 있다고 가정합니다 데이터 저장소 A는 IP 주소가 동일한 데이터 LIF를 통해 내보내지며 VM A는 이 데이터 저장소에 생성됩니다. 마찬가지로 클러스터 B에도 데이터 저장소 B가 있습니다 데이터 저장소 B는 IP 주소 x.x.x.x 및 VM B가 동일한 데이터 LIF를 통해 데이터 저장소 B에서 내보내집니다 UM은 VM A 토폴로지의 데이터 저장소 A를 해당 ONTAP 볼륨/LUN에 매핑하거나 VM B를 매핑할 수 없습니다

- NAS 및 SAN 볼륨(VMFS의 경우 iSCSI 및 FCP)만 데이터 저장소로 지원되며, 가상 볼륨(VVol)은 지원되지 않습니다.

- iSCSI 가상 디스크만 지원됩니다. NVMe 및 SATA 유형의 가상 디스크는 지원되지 않습니다.
- 뷰를 사용하면 다양한 부품의 성능을 분석하기 위한 보고서를 생성할 수 없습니다.
- Unified Manager의 가상 인프라에만 지원되는 스토리지 가상 머신(스토리지 VM) DR(재해 복구) 설정의 경우, 전환 및 스위치백 시나리오에서 활성 LUN을 가리키도록 vCenter Server에서 구성을 수동으로 변경해야 합니다. 수동 개입 없이 해당 데이터 저장소에 액세스할 수 없게 됩니다.

vCenter Server 보기 및 추가

VM(가상 머신)의 성능을 확인하고 문제를 해결하려면 관련 vCenter Server를 Active IQ Unified Manager 인스턴스에 추가해야 합니다.

- 필요한 것 *

vCenter Server를 추가하거나 보기 전에 다음을 확인하십시오.

- vCenter Server 이름을 알고 있습니다.
- vCenter Server의 IP 주소를 알고 있고 필요한 자격 증명을 가지고 있습니다. 자격 증명은 vCenter Server 관리자 또는 vCenter Server에 대한 읽기 전용 액세스 권한이 있는 루트 사용자여야 합니다.
- 추가하려는 vCenter Server는 vSphere 6.5 이상을 실행합니다.

  VMware ESXi 및 vCenter Server용 Unified Manager 지원은 영어 및 일본어로 제공됩니다.

- vCenter Server의 데이터 수집 설정은 모니터링되는 모든 객체에 대해 필요한 메트릭 수집 수준을 보장하기 위해 통계 수준 '*Level 3*'로 설정됩니다. 간격은 '_5분 _'이어야 하며 저장 기간은 '_1일 _'이어야 합니다.

  자세한 내용은 VMware 설명서의 _ vSphere 모니터링 및 성능 가이드 _ 의 "데이터 수집 수준" 섹션을 참조하십시오.

- 지연 시간 값을 성공적으로 계산할 수 있도록 vCenter Server의 지연 시간 값은 마이크로초 단위가 아니라 밀리초 단위로 구성됩니다.
- vCenter Server에 데이터 저장소를 추가하는 동안 호스트의 IP 주소 또는 FQDN(정규화된 도메인 이름)을 모두 사용할 수 있습니다. FQDN을 추가하는 경우 Unified Manager 서버에서 도메인 이름을 확인할 수 있는지 확인합니다. 예를 들어, Linux 설치의 경우 도메인 이름이 에 추가되었는지 확인합니다 `/etc/resolv.conf` 파일.
- vCenter Server의 현재 시간이 vCenter Server 시간대와 동기화되어 있습니다.
- 성공적인 검색을 위해 vCenter Server에 연결할 수 있습니다.
- vCenter Server를 Unified Manager에 추가할 때 VMware SDK에 대한 읽기 액세스 권한이 있습니다. 이는 구성 폴링에 필요합니다.

추가 및 검색된 모든 vCenter Server에 대해 Unified Manager는 vCenter Server 및 ESXi Server 세부 정보, ONTAP 매핑, 데이터 저장소 세부 정보 및 호스팅되는 VM 수와 같은 구성 데이터를 수집합니다. 또한 구성 요소의 성능 메트릭을 수집합니다.

단계

1. VMware * > * vCenter * 로 이동하여 목록에서 vCenter Server를 사용할 수 있는지 확인합니다.

vCenter Server를 사용할 수 없는 경우 vCenter Server를 추가해야 합니다.

a. 추가 * 를 클릭합니다.

b. vCenter Server에 대한 올바른 IP 주소를 추가하고 디바이스에 연결할 수 있는지 확인합니다.

c. vCenter Server에 대한 읽기 전용 액세스 권한이 있는 관리자 또는 루트 사용자의 사용자 이름 및 암호를 추가합니다.

d. 기본 443 이외의 포트를 사용하는 경우 사용자 지정 포트 번호를 추가합니다.

e. 저장 * 을 클릭합니다.

검색이 완료되면 서버 인증서가 표시되어 수락됩니다.

인증서를 수락하면 vCenter Server가 사용 가능한 vCenter Server 목록에 추가됩니다. 장치를 추가해도 연결된 VM의 데이터 수집은 되지 않으며 예약된 간격으로 수집이 수행됩니다.

2. vCenter Server가 * vCenters * 페이지에서 사용 가능한 경우 * Status * 필드 위로 마우스를 가져가 vCenter Server가 예상대로 수행되는지 또는 경고 또는 오류가 있는지 여부를 표시하여 해당 상태를 확인합니다.

vCenter Server를 추가하면 다음 상태를 볼 수 있습니다. 그러나 vCenter Server를 추가하여 정확하게 반영되려면 해당 VM의 성능 및 지연 시간 데이터가 1시간 정도 걸릴 수 있습니다.

◦ 녹색: "Normal" - vCenter Server가 검색되었으며 성능 메트릭이 성공적으로 수집되었음을 나타냅니다

◦ 노란색: "Warning"(예: vCenter Server의 통계 수준이 각 객체에 대한 통계를 얻기 위해 3 이상으로 설정되지 않은 경우)

◦ 주황색: "오류"(예외, 구성 데이터 수집 실패 또는 vCenter Server에 연결할 수 없음 등의 내부 오류 표시) 열 표시 아이콘(* 표시/숨기기*)을 클릭하여 vCenter Server 상태에 대한 상태 메시지를 보고 문제를 해결할 수 있습니다.

3. vCenter Server에 연결할 수 없거나 자격 증명이 변경된 경우 * vCenter * > * Edit * 를 선택하여 vCenter Server 세부 정보를 편집합니다.

4. VMware vCenter Server * 편집 페이지에서 필요한 내용을 변경합니다.

5. 저장 * 을 클릭합니다.

◦ vCenter Server 데이터 수집이 시작됩니다 *

vCenter Server는 20초 간의 실시간 성능 데이터 샘플을 수집하여 최대 5분 분량의 샘플을 취합합니다. Unified Manager의 성능 데이터 수집 일정은 vCenter Server의 기본 설정을 기반으로 합니다. Unified Manager는 vCenter Server에서 얻은 5분 샘플을 처리하고, 가상 디스크, VM 및 호스트에 대한 IOPS 및 지연 시간의 시간별 평균을 계산합니다. 데이터 저장소의 경우 Unified Manager는 ONTAP에서 얻은 샘플에서 IOPS 및 지연 시간의 시간별 평균을 계산합니다. 이러한 값은 시간 맨 위에 표시됩니다. vCenter Server를 추가한 직후에 성능 메트릭을 사용할 수 없으며 다음 시간이 시작될 때만 사용할 수 있습니다. 성능 데이터 폴링은 구성 데이터 수집 주기를 완료하는 데 시작됩니다.

vCenter Server 구성 데이터를 폴링하기 위해 Unified Manager는 클러스터 구성 데이터를 수집하는 것과 동일한 스케줄을 따릅니다. vCenter Server 구성 및 성능 데이터 수집 스케줄에 대한 자세한 내용은 "클러스터 구성 및 성능 데이터 수집 작업"을 참조하십시오.

- 관련 정보 *

"클러스터 구성 및 성능 데이터 수집 작업"

vCenter Server를 제거하는 중입니다

Active IQ Unified Manager 인스턴스에서 vCenter Server를 제거할 수 있습니다. 예를 들어 vCenter Server 검색이 실패하거나 더 이상 필요하지 않은 경우 vCenter Server를 제거할 수 있습니다.

vCenter Server를 제거하면 해당 vCenter에 호스팅된 모든 VM(가상 머신)과 해당 구성 데이터도 삭제됩니다. vCenter Server가 제거되면 연결된 객체 및 기록 데이터와 함께 더 이상 모니터링되지 않습니다. 이러한 변경 사항은 vCenter 및 가상 머신 인벤토리 페이지에 반영됩니다.

- 필요한 것 *

vCenter Server를 제거하기 전에 다음을 확인하십시오.

- 애플리케이션 관리자 역할 또는 스토리지 관리자 역할이 있습니다.
- vCenter Server 이름 및 이와 관련된 각 IP 주소를 알고 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * VMware > vCenter * 를 클릭합니다.
2. vCenter 페이지에서 제거할 vCenter Server를 선택하고 * Remove * 를 클릭합니다.
3. vCenter 제거 * 메시지 대화 상자에서 * 확인 * 을 클릭하여 제거 요청을 확인합니다.

가상 머신 모니터링

가상 머신(VM) 애플리케이션에서 지연 시간 문제가 발생하는 경우 VM을 모니터링하여 원인을 분석하고 문제를 해결해야 할 수 있습니다. VM은 vCenter Server와 VM 스토리지를 호스팅하는 ONTAP 클러스터를 Unified Manager에 추가할 때 사용할 수 있습니다.

VM의 세부 정보는 * VMware * >> * 가상 머신 * 페이지에서 확인할 수 있습니다. 가용성, 상태, 사용된 용량 및 할당된 용량, 네트워크 지연 시간, VM, 데이터 저장소 및 호스트의 IOPS 및 지연 시간 등의 정보가 표시됩니다. 여러 데이터 저장소를 지원하는 VM의 경우 그리드는 지연 시간이 가장 짧은 데이터 저장소의 메트릭을 표시하며, 추가 데이터 저장소를 나타내는 별표 아이콘(*)을 표시합니다. 아이콘을 클릭하면 추가 데이터 저장소의 메트릭이 표시됩니다. 이러한 열 중 일부는 정렬 및 필터링에 사용할 수 없습니다.

VM 및 해당 세부 정보를 보려면 ONTAP 클러스터의 검색(폴링 또는 메트릭 수집)을 완료해야 합니다. 클러스터가 Unified Manager에서 제거되면 다음 번 검색 주기 이후 VM을 더 이상 사용할 수 없습니다.

이 페이지에서 VM의 세부 토폴로지를 볼 수도 있습니다. 이 토폴로지에는 VM에 연결된 호스트, 가상 디스크 및 데이터 저장소와 같은 VM과 관련된 구성 요소가 표시됩니다. 토폴로지 뷰는 특정 계층의 기본 구성 요소를 다음 순서로 표시합니다. * 가상 디스크 * > * VM * > * 호스트 * > * 네트워크 * > * 데이터 저장소 * > * VMDK *.

토폴로지 측면에서 I/O 경로와 구성 요소 레벨 지연 시간을 확인하고 스토리지가 성능 문제의 원인인지 여부를 식별할 수 있습니다. 토폴로지의 요약 보기에는 I/O 경로가 표시되며, 문제 해결 단계를 결정할 때 IOPS 및 지연 시간 문제가 있는 구성 요소가 강조 표시됩니다. 또한 각 구성 요소를 별도로 설명하는 토폴로지와 해당 구성 요소의 지연 시간을 볼 수 있습니다. 계층을 통해 강조 표시된 I/O 경로를 결정하기 위해 구성 요소를 선택할 수 있습니다.

요약 토폴로지 보기

요약 토폴로지에서 VM을 확인하여 성능 문제를 확인하려면 다음을 수행합니다.

1. VMware * > * 가상 머신 * 으로 이동합니다.
2. 검색 상자에 VM 이름을 입력하여 VM을 검색합니다. 필터 * 버튼을 클릭하여 특정 기준에 따라 검색 결과를 필터링할 수도 있습니다. 그러나 VM을 찾을 수 없는 경우 해당 vCenter Server가 추가 및 검색되었는지 확인합니다.

> vCenter Server는 특수 문자(예: %, &, *, $, #, @,!,\, /,:, *,?,"",<,>, |,;,') VM, 클러스터, 데이터 저장소, 폴더, 또는 파일. VMware vCenter Server 및 ESX/ESXi Server는 표시 이름에 사용되는 특수 문자를 이스케이프하지 않습니다. 하지만 Unified Manager에서 이름을 처리하면 이름이 다르게 표시됩니다. 예를 들어, Unified Manager에서 vCenter Server의 "%$VC_AIQUM_CLONE_191124%"라는 VM이 "%25$VC_AIQUM_CLONE_191124% 25"로 표시됩니다. 이름에 특수 문자가 포함된 VM을 쿼리할 때 이 문제를 기록해 두어야 합니다.

3. VM의 상태를 확인합니다. VM 상태는 vCenter Server에서 검색됩니다. 다음 상태를 사용할 수 있습니다. 이러한 상태에 대한 자세한 내용은 VMware 설명서를 참조하십시오.
   - 정상
   - 경고
   - 경고
   - 모니터링되지 않음
   - 알 수 없음
4. VM 옆의 아래쪽 화살표를 클릭하여 컴퓨팅, 네트워크 및 스토리지 계층 전체에서 구성 요소 토폴로지에 대한 요약 보기를 표시합니다. 지연 시간 문제가 있는 노드가 강조 표시됩니다. 요약 보기에는 구성 요소의 지연 시간이 가장 짧습니다. 예를 들어, VM에 가상 디스크가 두 개 이상 있는 경우 이 보기에는 모든 가상 디스크 중에서 지연 시간이 가장 짧은 가상 디스크가 표시됩니다.
5. 일정 기간 동안 데이터 저장소의 지연 시간 및 처리량을 분석하려면 데이터 저장소 개체 아이콘 위에 있는 * Workload Analyzer * 버튼을 클릭합니다. 워크로드 분석 페이지로 이동하여 시간 범위를 선택하고 데이터 저장소의 성능 차트를 확인할 수 있습니다. 워크로드 분석기에 대한 자세한 내용은 _ 워크로드 분석기를 사용한 워크로드 문제 해결 _ 을(를) 참조하십시오.

확장된 토폴로지 보기

VM의 확장된 토폴로지를 확인하여 각 구성 요소별로 드릴다운할 수 있습니다.

단계

1. 요약 토폴로지 보기에서 * 토폴로지 확장 * 을 클릭합니다. 각 구성 요소의 상세한 토폴로지와 각 개체의 지연 시간 번호를 별도로 확인할 수 있습니다. 데이터 저장소 또는 VMDK에 여러 노드 같은 범주에 여러 노드가 있는 경우 지연 시간이 가장 짧은 노드는 빨간색으로 강조 표시됩니다.
2. 특정 객체의 입출력 경로를 확인하려면 해당 객체를 클릭하여 입출력 경로와 해당 매핑을 확인하십시오. 예를 들어, 가상 디스크의 매핑을 보려면 가상 디스크를 클릭하여 해당 VMDK에 대한 강조 표시된 매핑을 확인합니다. 이러한 구성 요소의 성능이 저하될 경우 ONTAP에서 더 많은 데이터를 수집하고 문제를 해결할 수 있습니다.

> vmdks에 대한 메트릭은 보고되지 않습니다. 토폴로지에서는 VMDK 이름만 표시되고 메트릭은 표시되지 않습니다.

◦ 관련 정보 *

"워크로드 분석기를 사용하여 워크로드 문제 해결"

재해 복구 설정에서 가상 인프라 보기

MetroCluster 구성 또는 스토리지 가상 시스템(스토리지 VM) SVM DR(재해 복구) 설정에서 호스팅되는 데이터 저장소의 구성 및 성능 메트릭을 확인할 수 있습니다.

Unified Manager에서는 vCenter Server에서 데이터 저장소로 연결된 MetroCluster 구성에서 NAS 볼륨 또는 LUN을 볼 수 있습니다. MetroCluster 구성에서 호스팅되는 데이터스토어는 표준 환경에서 데이터스토어와 동일한 토폴로지 뷰로 표시됩니다.

vCenter Server의 데이터 저장소에 매핑된 스토리지 VM 재해 복구 구성의 NAS 볼륨 또는 LUN도 볼 수 있습니다.

MetroCluster 구성에서 데이터 저장소 보기

MetroCluster 구성에서 데이터 저장소를 보기 전에 다음 사전 요구 사항을 확인하십시오.

- 스위치오버 및 스위치백을 수행할 경우 HA 쌍의 기본 및 보조 클러스터와 vCenter Server의 검색이 완료됩니다.
- HA 쌍의 운영 클러스터와 보조 클러스터와 vCenter Server는 Unified Manager를 통해 관리해야 합니다.
- ONTAP 및 vCenter Server에서 필요한 설정을 완료해야 합니다. 자세한 내용은 ONTAP 및 vCenter 설명서를 참조하십시오.

  "ONTAP 9 문서 센터"

데이터 저장소를 보려면 다음 단계를 수행하십시오.

1. VMware * > * Virtual Machines * 페이지에서 데이터 저장소를 호스팅하는 VM을 클릭합니다. 워크로드 분석기 * 또는 데이터 저장소 객체 링크를 클릭합니다. 표준 시나리오에서는 볼륨 또는 LUN을 호스팅하는 운영 사이트가 예상대로 작동하는 경우 기본 사이트의 SVM 클러스터 세부 정보를 볼 수 있습니다.
2. 재해 발생 시 데이터 저장소 링크는 보조 클러스터에 있는 볼륨 또는 LUN의 성능 메트릭을 가리킵니다. 이는 클러스터의 다음 주기 및 가상 서버 검색(획득)이 완료된 후에 반영됩니다.
3. 스위치백을 성공적으로 완료한 후 데이터 저장소 링크는 운영 클러스터에 있는 볼륨 또는 LUN의 성능 메트릭을 다시 반영합니다. 이는 클러스터의 다음 주기 및 가상 서버 검색이 완료된 후에 반영됩니다.

스토리지 **VM** 재해 복구 구성에서 데이터 저장소 보기

스토리지 VM 재해 복구 구성에서 데이터 저장소를 보기 전에 다음 사전 요구 사항을 확인하십시오.

- 스위치오버 및 스위치백을 수행할 경우 HA 쌍의 기본 및 보조 클러스터와 vCenter Server의 검색이 완료됩니다.
- 소스 및 타겟 클러스터와 스토리지 VM 피어는 모두 Unified Manager를 통해 관리해야 합니다.
- ONTAP 및 vCenter Server에서 필요한 설정을 완료해야 합니다.
  - NAS(NFS 및 VMFS) 데이터 저장소의 경우 재해가 발생할 경우 보조 스토리지 VM을 가져와 데이터 LIF 및 경로 확인, vCenter Server에서 손실된 연결 설정 및 VM 시작 단계가 포함됩니다.

    기본 사이트로 스위치백을 수행할 경우 기본 사이트에서 데이터 제공을 시작하기 전에 볼륨 간 데이터를

동기화해야 합니다.

- SAN(iSCSI 및 FC for VMFS) 데이터 저장소의 경우 vCenter Server는 마운트된 LUN을 VMFS 형식으로 포맷합니다. 재해 발생 시 보조 스토리지 VM을 가져와 데이터 LIF 및 경로를 확인하는 단계가 포함됩니다. iSCSI 타겟 IP가 운영 LIF와 다른 경우 수동으로 추가해야 합니다. 새 LUN은 호스트의 스토리지 어댑터의 iSCSI 어댑터 아래에 디바이스로 사용할 수 있어야 합니다. 그런 다음 새 LUN이 있는 새 VMFS 데이터 저장소를 생성하고 이전 VM을 새 이름으로 등록해야 합니다. VM이 실행 중이어야 합니다.

  복구 시 볼륨 간 데이터를 동기화해야 합니다. 새 VMFS 데이터 저장소는 LUN과 새 이름으로 등록된 이전 VM을 사용하여 다시 생성해야 합니다.

  설정에 대한 자세한 내용은 ONTAP and vCenter Server 설명서를 참조하십시오.

"ONTAP 9 문서 센터"

데이터 저장소를 보려면 다음 단계를 수행하십시오.

1. VMware * > * Virtual Machines * 페이지에서 데이터 저장소를 호스팅하는 VM 인벤토리를 클릭합니다. 데이터 저장소 객체 링크를 클릭합니다. 표준 시나리오에서는 운영 스토리지 VM에 있는 볼륨 및 LUN의 성능 데이터를 확인할 수 있습니다.
2. 재해 발생 시 보조 스토리지 VM으로 연속적으로 전환하는 데이터 저장소 링크는 보조 스토리지 VM에 있는 볼륨 또는 LUN의 성능 메트릭을 가리킵니다. 이는 클러스터의 다음 주기 및 가상 서버 검색(획득)이 완료된 후에 반영됩니다.
3. 스위치백을 성공적으로 완료한 후 데이터 저장소 링크는 운영 스토리지 VM의 볼륨 또는 LUN의 성능 메트릭을 다시 반영합니다. 이는 클러스터의 다음 주기 및 가상 서버 검색이 완료된 후에 반영됩니다.

지원되지 않는 시나리오입니다

- MetroCluster 구성의 경우 다음과 같은 제한 사항에 유의하십시오.
  - 정상과 위시WER의 군집들만 잡게 됩니다. partial_switchover, partial_스위치백, not_reachable 등의 다른 상태는 지원되지 않습니다.
  - ASO(Automatic Switch over)가 설정되어 있지 않으면 운영 클러스터가 다운되면 보조 클러스터를 검색할 수 없으며 토폴로지가 운영 클러스터의 볼륨 또는 LUN을 계속 가리킵니다.
- 스토리지 VM 재해 복구 구성의 경우 다음 제한 사항에 유의하십시오.
  - SAN 스토리지 환경에 대해 SRM(Site Recovery Manager) 또는 SRA(Storage Replication Adapter)가 활성화된 구성은 지원되지 않습니다.

워크로드 프로비저닝 및 관리

Active IQ Unified Manager의 액티브 관리 기능은 데이터 센터에서 스토리지 워크로드를 프로비저닝, 모니터링 및 관리하기 위한 성능 서비스 수준, 스토리지 효율성 정책 및 스토리지 공급자 API를 제공합니다.

Unified Manager는 이 기능을 기본적으로 제공합니다. 이 기능을 사용하지 않으려면 * 스토리지 관리 * > * 기능 설정 * 에서 비활성화할 수 있습니다.

사용하도록 설정된 경우, Unified Manager 인스턴스에서 관리하는 ONTAP 클러스터에서 워크로드를 프로비저닝할 수

있습니다. 또한 워크로드에 성능 서비스 수준 및 스토리지 효율성 정책과 같은 정책을 할당하고 이러한 정책을 기반으로 스토리지 환경을 관리할 수도 있습니다.

이 기능을 사용하면 다음 기능을 사용할 수 있습니다.

- 추가된 클러스터에서 스토리지 워크로드를 자동으로 검색하여 스토리지 워크로드를 쉽게 평가하고 구축할 수 있습니다
- NFS 및 CIFS 프로토콜을 지원하는 NAS 워크로드를 프로비저닝합니다
- iSCSI 및 FCP 프로토콜을 지원하는 SAN 워크로드 프로비저닝
- 동일한 파일 공유에서 NFS 및 CIFS 프로토콜을 모두 지원합니다
- 성능 서비스 수준 및 스토리지 효율성 정책 관리
- 스토리지 워크로드에 성능 서비스 수준 및 스토리지 효율성 정책 할당

UI의 왼쪽 창에 있는 * Provisioning *, * Storage * > * 워크로드 * 및 * Policies * 옵션을 사용하여 다양한 구성을 수정할 수 있습니다.

다음 옵션을 사용하여 다음 기능을 수행할 수 있습니다.

- 스토리지 * > * 워크로드 * 페이지에서 스토리지 워크로드를 확인합니다
- 워크로드 프로비저닝 페이지에서 스토리지 워크로드를 생성합니다
- 정책에서 성능 서비스 수준을 생성하고 관리합니다
- 정책에서 스토리지 효율성 정책을 생성하고 관리합니다
- 워크로드 페이지에서 스토리지 워크로드에 정책 할당
- 관련 정보 *

"정책 기반 스토리지 관리"

워크로드 개요

워크로드는 볼륨 또는 LUN과 같은 스토리지 개체의 입출력 작업을 나타냅니다. 스토리지가 프로비저닝되는 방식은 예상되는 워크로드 요구 사항을 기반으로 합니다. 워크로드 통계는 스토리지 오브젝트 간에 트래픽이 있는 경우에만 Active IQ Unified Manager에서 추적합니다. 예를 들어 워크로드 IOPS 및 지연 시간 값은 사용자가 데이터베이스 또는 이메일 애플리케이션을 시작한 후에 사용할 수 있습니다.

워크로드 페이지에는 Unified Manager에서 관리하는 ONTAP 클러스터의 스토리지 워크로드가 요약되어 있습니다. Performance Service Level을 준수하는 스토리지 워크로드와 부적합 스토리지 워크로드에 대한 누적 요약 정보를 제공합니다. 또한 데이터 센터 전반에서 클러스터의 총, 사용 가능, 사용된 용량 및 성능(IOPS)을 평가할 수 있습니다.

어떤 성능 서비스 레벨에서든 부적합, 사용 불가능 또는 관리되지 않는 스토리지 워크로드의 수를 평가하고 적합성, 용량 사용 및 IOPS를 보장하기 위해 필요한 조치를 취하는 것이 좋습니다.

워크로드 페이지에는 다음 두 섹션이 있습니다.

- 워크로드 개요: Unified Manager가 관리하는 ONTAP 클러스터의 스토리지 워크로드 수를 간략하게 설명합니다.

- 데이터 센터 개요: 데이터 센터 내 스토리지 워크로드의 용량 및 IOPS에 대한 개요를 제공합니다. 관련 데이터는 데이터 센터 레벨 및 개인에 대해 표시됩니다.

워크로드 개요 섹션을 참조하십시오

워크로드 개요 섹션에서는 스토리지 워크로드에 대한 요약 정보를 제공합니다. 스토리지 워크로드의 상태는 할당되고 할당되지 않은 성능 서비스 수준에 따라 표시됩니다.

- * 할당됨 *: 성능 서비스 수준이 할당된 스토리지 워크로드에 대해 다음 상태가 보고됩니다.
  - * 준수 *: 스토리지 워크로드의 성능은 할당된 성능 서비스 수준을 기준으로 합니다. 스토리지 워크로드가 관련 성능 서비스 수준에 정의된 임계값 지연 시간 내에 있으면 ""준수""로 표시됩니다. 적합 워크로드는 파란색으로 표시됩니다.
  - * 부적합 *: 스토리지 워크로드의 지연 시간이 관련 성능 서비스 수준에 정의된 임계값 지연 시간을 초과할 경우 성능 모니터링 중에 스토리지 워크로드가 ""부적합""으로 표시됩니다. 부적합 워크로드는 주황색으로 표시됩니다.
  - * 사용할 수 없음 *: 스토리지 워크로드가 오프라인이거나 해당 클러스터에 연결할 수 없는 경우 ""사용할 수 없음""으로 표시됩니다. 사용할 수 없는 워크로드는 빨간색으로 표시됩니다.
- * 할당되지 않음 *: 성능 서비스 수준이 할당되지 않은 스토리지 워크로드는 ""할당되지 않음""으로 보고됩니다. 숫자는 정보 아이콘을 통해 전달됩니다.

총 워크로드 수는 할당되고 할당되지 않은 워크로드의 합계입니다.

이 섹션에 표시된 총 워크로드 수를 클릭하고 워크로드 페이지에서 볼 수 있습니다.

성능 서비스 수준별 준수 하위 섹션에는 사용 가능한 총 스토리지 워크로드 수가 표시됩니다.

- 각 유형의 성과 서비스 수준 준수
- 할당된 성능 수준과 권장 성능 서비스 수준이 일치하지 않습니다

데이터 센터 개요 섹션을 참조하십시오

데이터 센터 개요 섹션에서는 데이터 센터의 모든 클러스터에서 사용 가능한 용량과 사용된 용량 및 IOPS를 그래픽으로 보여 줍니다. 이 데이터를 사용하여 스토리지 워크로드의 용량과 IOPS를 관리해야 합니다. 이 섹션에는 모든 클러스터에서 스토리지 워크로드에 대한 다음 정보도 표시됩니다.

- 데이터 센터의 모든 클러스터에 대한 총 용량, 사용 가능 용량 및 사용된 용량입니다
- 데이터 센터의 모든 클러스터에 대해 사용 가능한 총 IOPS와 사용된 IOPS
- 각 성능 서비스 수준에 따라 사용 가능한 용량과 사용된 용량
- 각 성능 서비스 수준에 기반한 사용 가능한 IOPS 및 사용된 IOPS
- 성능 서비스 수준이 할당되지 않은 워크로드에서 사용하는 총 공간 및 IOPS
- 성능 서비스 수준을 기준으로 데이터 센터 용량과 성능을 계산하는 방법 *

사용된 용량과 IOPS는 클러스터에 있는 모든 스토리지 워크로드의 사용된 총 용량과 성능을 기준으로 검색됩니다.

사용 가능한 IOPS는 노드의 예상 지연 시간과 권장 성능 서비스 수준을 기준으로 계산됩니다. 여기에는 예상 지연 시간이 자신만의 예상 지연 시간보다 작거나 같은 모든 성능 서비스 수준에 대해 사용 가능한 IOPS가 포함됩니다.

가용 용량은 애그리게이트에서 예상되는 지연 시간과 권장되는 성능 서비스 수준을 기준으로 계산됩니다. 여기에는 예상 지연 시간이 예상 대기 시간보다 작거나 같은 모든 Performance Service 수준에 사용할 수 있는 용량이 포함됩니다.

워크로드 보기

Unified Manager에 클러스터를 추가하면 각 클러스터의 스토리지 워크로드가 자동으로 검색되어 워크로드 페이지에 표시됩니다.

Unified Manager는 스토리지 워크로드에서 I/O 작업이 시작된 후에만 권장 PSL(권장 PSL)에 대한 워크로드를 분석하기 시작합니다.

FlexGroup 볼륨 및 구성 요소에서는 제외됩니다.

워크로드 개요

워크로드 개요 페이지에는 데이터 센터의 워크로드 개요와 데이터 센터의 공간 및 성능 개요가 표시됩니다.

- * 워크로드 개요 * 패널: 총 워크로드 수와 PSL이 할당되어 있거나 없는 워크로드 수를 표시합니다. 각 PSL에 대한 작업 부하 수의 분할도 표시됩니다. 개수를 클릭하면 필터링된 워크로드가 있는 * 모든 워크로드 * 보기로 이동합니다. 또한 시스템 권장 사항을 따르지 않는 작업 부하의 수를 보고 * 시스템 권장 PSL 할당 * 버튼을 클릭하여 시스템 권장 PSL을 할당할 수 있습니다.
- * 데이터 센터 개요 * 패널: 데이터 센터의 사용 가능한 공간과 사용된 공간(TiB) 및 성능(IOPS)을 표시합니다. 또한 각 PSL에서 사용 가능한 공간과 사용된 공간(TiB) 및 모든 워크로드의 성능(IOPS)이 표시됩니다.

모든 워크로드 보기

스토리지 > 워크로드 > 모든 워크로드 * 페이지에는 Unified Manager에서 관리하는 ONTAP 클러스터와 관련된 스토리지 워크로드가 나열됩니다.

I/O 작업이 없는 새로 발견된 스토리지 워크로드의 경우 I/O를 기다리는 중입니다. 스토리지 워크로드에서 I/O 작업이 시작되면 Unified Manager가 분석을 시작하고 워크로드 상태가 ""학습…""으로 변경됩니다. 분석이 완료되면(I/O 작업 시작 후 24시간 이내) 스토리지 워크로드에 권장되는 PSL이 표시됩니다.

또한 이 페이지에서는 스토리지 워크로드에 CDP(스토리지 효율성 정책) 및 PSL(성능 서비스 수준)을 할당할 수 있습니다. 여러 작업을 수행할 수 있습니다.

- 스토리지 워크로드를 추가하거나 프로비저닝
- 워크로드 목록을 보고 필터링합니다
- 스토리지 워크로드에 PSL 할당
- 시스템 권장 PSL을 평가하고 작업 부하에 할당합니다
- 스토리지 워크로드에 CDP를 할당합니다

스토리지 워크로드 추가 또는 프로비저닝

지원되는 LUN(iSCSI 및 FCP 프로토콜 모두 지원), NFS 파일 공유 및 SMB 공유에 스토리지 워크로드를 추가하거나 프로비저닝할 수 있습니다.

단계

1. 스토리지 > 워크로드 > 모든 워크로드 > 생성 * 을 클릭합니다.

2. 워크로드 생성: 자세한 내용은 을 참조하십시오 "워크로드 프로비저닝 및 관리".

워크로드 보기 및 필터링

모든 워크로드 화면에서 데이터 센터의 모든 워크로드를 확인하거나 PSL 또는 이름을 기준으로 특정 스토리지 워크로드를 검색할 수 있습니다. 필터 아이콘을 사용하여 검색에 대한 특정 조건을 입력할 수 있습니다. 호스트 클러스터나 스토리지 VM과 같은 다양한 필터 조건으로 검색할 수 있습니다. Capacity Total * 옵션을 사용하면 워크로드의 총 용량(MB 단위)으로 필터링할 수 있습니다. 그러나 이 경우 총 용량이 바이트 레벨에서 비교되기 때문에 반환되는 워크로드 수가 달라질 수 있습니다.

각 워크로드에 대해 호스트 클러스터 및 스토리지 VM과 같은 정보가 할당된 PSL 및 SEP와 함께 표시됩니다.

또한 이 페이지에서는 워크로드의 성능 세부 정보를 볼 수 있습니다. 열 선택/주문 * 버튼을 클릭하고 표시할 특정 열을 선택하여 워크로드의 IOPS, 용량, 지연 시간에 대한 자세한 정보를 볼 수 있습니다. 성능 보기 열에는 워크로드에 대한 평균 및 최대 IOPS가 표시되며, 워크로드 분석기 아이콘을 클릭하여 자세한 IOPS 분석을 볼 수 있습니다.

워크로드에 대한 성능 및 용량 기준 분석

IOPS 분석 * 팝업의 * 워크로드 분석 * 버튼을 누르면 워크로드 분석 페이지로 이동합니다. 이 페이지에서 시간 범위를 선택하고 선택한 워크로드의 지연 시간, 처리량 및 용량 추세를 확인할 수 있습니다. 워크로드 분석기에 대한 자세한 내용은 을 참조하십시오 "워크로드 분석기를 사용하여 워크로드 문제 해결".

성능 보기 * 열에서 막대 차트 아이콘을 클릭하여 문제 해결에 도움이 되는 작업 부하에 대한 성능 정보를 볼 수 있습니다. 워크로드 분석 페이지에서 성능 및 용량 차트를 보고 객체를 분석하려면 * 워크로드 분석 * 버튼을 클릭합니다.

자세한 내용은 을 참조하십시오 "워크로드 분석기가 표시하는 데이터는 무엇입니까".

작업 부하에 정책 할당

다양한 탐색 옵션을 사용하여 모든 워크로드 페이지의 스토리지 워크로드에 CDP(스토리지 효율성 정책) 및 PSL(성능 서비스 수준)을 할당할 수 있습니다.

단일 워크로드에 정책 할당

PSL 또는 SEP 또는 둘 모두를 단일 작업 부하에 할당할 수 있습니다. 다음 단계를 수행하십시오.

1. 워크로드를 선택합니다.
2. 행 옆에 있는 편집 아이콘을 클릭한 다음 * 편집 * 을 클릭합니다.

   할당된 성능 서비스 수준 * 및 * 스토리지 효율성 정책 * 필드가 활성화됩니다.

3. 필요한 PSL 또는 SEP 또는 둘 다를 선택합니다.
4. 확인 아이콘을 클릭하여 변경 사항을 적용합니다.

ⓘ 워크로드를 선택하고 * 추가 작업 * 을 클릭하여 정책을 할당할 수도 있습니다.

여러 스토리지 워크로드에 정책 할당

여러 스토리지 작업 부하에 PSL 또는 SEP를 함께 할당할 수 있습니다. 다음 단계를 수행하십시오.

1. 정책을 할당할 워크로드의 확인란을 선택하거나 데이터 센터의 모든 워크로드를 선택합니다.
2. 추가 작업 * 을 클릭합니다.
3. PSL을 할당하려면 * 성능 서비스 수준 할당 * 을 선택합니다. SEP를 할당하려면 * 스토리지 효율성 정책 할당 * 을 선택합니다. 정책을 선택할 수 있는 팝업이 표시됩니다.
4. 적절한 정책을 선택하고 * 적용 * 을 클릭합니다. 정책이 할당된 워크로드 수가 표시됩니다. 정책이 할당되지 않은 워크로드도 원인과 함께 나열됩니다.

선택한 워크로드 수에 따라 워크로드를 대량으로 정책을 적용하는 데 시간이 걸릴 수 있습니다. 백그라운드 * 실행 버튼을 클릭하여 백그라운드에서 작업이 실행되는 동안 다른 작업을 계속할 수 있습니다. 대량 할당이 완료되면 완료 상태를 볼 수 있습니다. 여러 작업 부하에 PSL을 적용하는 경우 이전 대량 할당 작업이 실행 중일 때 다른 요청을 트리거할 수 없습니다.

작업 부하에 시스템 권장 **PSL** 할당

PSL이 할당되지 않았거나 할당된 PSL이 시스템 권장 사항과 일치하지 않는 데이터 센터의 스토리지 워크로드에 시스템 권장 PSL을 할당할 수 있습니다. 이 기능을 사용하려면 * 시스템 권장 PSL 할당 * 버튼을 클릭합니다. 특정 워크로드를 선택할 필요가 없습니다.

권장 사항은 내부적으로 시스템 분석에 의해 결정되며, IOPS 및 기타 매개 변수가 사용 가능한 모든 PSL의 정의와 일치하지 않는 워크로드의 경우 건너뜁니다. 입출력 대기 중 및 학습 상태의 스토리지 워크로드도 제외됩니다.

Unified Manager에서 워크로드 이름을 찾아 시스템 분석을 재정의하고 워크로드에 대해 다른 PSL을 추천하도록 하는 특수 키워드가 있습니다. 작업 부하는 이름에 ""ora""가 있으면 **Extreme Performance** PSL을 사용하는 것이 좋습니다. 작업 부하에는 이름에 ""VM""이라는 글자가 있으면 성능 PSL을 사용하는 것이 좋습니다.

또한 기술 자료(KB) 문서를 참조하십시오 "ActiveIQ Unified Manager '시스템 권장 성능 서비스 레벨 할당'은 워크로드가 매우 가변적인 워크로드에 대해 적응하지 못합니다"

파일 공유 볼륨 프로비저닝

프로비저닝 워크로드 페이지에서 기존 클러스터 및 스토리지 가상 머신(스토리지 VM)에서 CIFS/SMB 및 NFS 프로토콜을 지원하는 파일 공유 볼륨을 생성할 수 있습니다.

- 필요한 것 *
- 스토리지 VM에 파일 공유 볼륨을 프로비저닝할 수 있는 공간이 있어야 합니다.
- 스토리지 VM에서 SMB 및 NFS 서비스 중 하나 또는 둘 다 활성화해야 합니다.
- 작업 부하에서 PSL(Performance Service Level) 및 SEP(Storage Efficiency Policy)를 선택하고 할당하려면 워크로드를 생성하기 전에 정책을 생성해야 합니다.

단계

1. Provision Workload * 페이지에서 생성할 워크로드 이름을 추가한 다음 Available 목록에서 클러스터를 선택합니다.
2. 선택한 클러스터에 따라 * 스토리지 VM * 필드가 해당 클러스터에 대해 사용 가능한 스토리지 VM을 필터링합니다. 목록에서 필요한 스토리지 VM을 선택합니다.

   스토리지 VM에서 지원되는 SMB 및 NFS 서비스에 따라 호스트 정보 섹션에서 NAS 옵션이 설정됩니다.

3. 스토리지 및 최적화 섹션에서 스토리지 용량 및 PSL을 할당하고 선택적으로 워크로드에 대한 SEP를 할당합니다.

   SEP에 대한 사양은 LUN에 할당되며 PSL에 대한 정의는 생성 시 워크로드에 적용됩니다.

4. 작업 부하에 할당한 PSL을 적용하려면 * 성능 제한 강제 적용 * 확인란을 선택합니다.

   작업 부하에 PSL을 할당하면 워크로드가 생성되는 총계를 통해 해당 정책에 정의된 성능 및 용량 목표를 지원할 수 있습니다. 예를 들어, 워크로드에 "최고 성능" PSL이 할당된 경우 워크로드를 프로비저닝할 집계 시 SSD 스토리지와 같은 "최고 성능" 정책의 성능 및 용량 목표를 지원할 수 있어야 합니다.

   ⓘ 이 확인란을 선택하지 않으면 PSL이 작업 부하에 적용되지 않고 대시보드의 작업 부하 상태가 미할당 상태로 나타납니다.

5. NAS * 옵션을 선택합니다.

   nas * 옵션이 설정되어 있지 않으면 선택한 스토리지 VM이 SMB 또는 NFS를 지원하는지 확인하십시오.

   ⓘ 스토리지 VM이 SMB 및 NFS 서비스 모두에 대해 활성화된 경우 * Share by NFS * 및 * Share by SMB * 확인란을 선택하고 NFS 및 SMB 프로토콜을 모두 지원하는 파일 공유를 생성할 수 있습니다. SMB 또는 CIFS 공유를 생성하려면 해당 확인란만 선택합니다.

6. NFS 파일 공유 볼륨의 경우 파일 공유 볼륨을 액세스할 호스트 또는 네트워크의 IP 주소를 지정합니다. 여러 호스트에 대해 쉼표로 구분된 값을 입력할 수 있습니다.

   호스트 IP 주소를 추가할 때 호스트 세부 정보를 스토리지 VM과 일치시키기 위해 내부 검사가 실행되고 해당 호스트에 대한 엑스포트 정책이 생성되거나 기존 정책이 있는 경우 다시 사용됩니다. 동일한 호스트에 대해 여러 개의 NFS 공유가 생성된 경우 동일한 호스트에 대해 사용 가능한 내보내기 정책이 모든 파일 공유에 다시 사용됩니다. API를 사용하여 NFS 공유를 프로비저닝할 때 개별 정책의 규칙을 지정하거나 특정 정책 키를 제공하여 정책을 재사용하는 기능을 사용할 수 있습니다.

7. SMB 공유의 경우 SMB 공유에 액세스할 수 있는 사용자 또는 사용자 그룹을 지정하고 필요한 권한을 할당합니다. 각 사용자 그룹에 대해 파일 공유를 생성하는 동안 새 ACL(액세스 제어 목록)이 생성됩니다.
8. 저장 * 을 클릭합니다.

   스토리지 워크로드 목록에 워크로드가 추가됩니다.

LUN 프로비저닝

프로비저닝 워크로드 페이지에서 기존 클러스터와 스토리지 가상 머신(스토리지 VM)에서 CIFS/SMB 및 NFS 프로토콜을 지원하는 LUN을 생성할 수 있습니다.

- 필요한 것 *
- 스토리지 VM에 LUN 프로비저닝을 위한 공간이 있어야 합니다.
- LUN을 생성하는 스토리지 VM에서 iSCSI와 FCP를 모두 사용하도록 설정해야 합니다.
- 작업 부하에서 PSL(Performance Service Level) 및 SEP(Storage Efficiency Policy)를 선택하고 할당하려면 워크로드를 생성하기 전에 정책을 생성해야 합니다.

단계

1. Provision Workload * 페이지에서 생성할 워크로드 이름을 추가한 다음 Available 목록에서 클러스터를 선택합니다.

   선택한 클러스터에 따라 * 스토리지 VM * 필드가 해당 클러스터에 대해 사용 가능한 스토리지 VM을 필터링합니다.

2. iSCSI 및 FCP 서비스를 지원하는 목록에서 스토리지 VM을 선택합니다.

   선택한 내용에 따라 호스트 정보 섹션에서 SAN 옵션이 활성화됩니다.

3. 스토리지 및 최적화 * 섹션에서 스토리지 용량 및 PSL을 할당하고 선택적으로 워크로드에 대한 SEP를 할당합니다.

   SEP에 대한 사양은 LUN에 할당되며 PSL에 대한 정의는 생성 시 워크로드에 적용됩니다.

4. 작업량에 할당된 PSL을 적용하려는 경우 * 성능 제한 적용 * 확인란을 선택합니다.

   작업 부하에 PSL을 할당하면 워크로드가 생성되는 총계를 통해 해당 정책에 정의된 성능 및 용량 목표를 지원할 수 있습니다. 예를 들어, 워크로드에 "최고 성능" PSL이 할당된 경우 워크로드를 프로비저닝할 집계 시 SSD 스토리지와 같은 "최고 성능" 정책의 성능 및 용량 목표를 지원할 수 있어야 합니다.

   > ⓘ 이 확인란을 선택하지 않으면 PSL이 작업 부하에 적용되지 않고 대시보드의 작업 부하 상태가 '할당되지 않음'으로 나타납니다.

5. SAN * 옵션을 선택합니다. SAN * 옵션이 설정되어 있지 않으면 선택한 스토리지 VM이 iSCSI 및 FCP를 지원하는지 확인하십시오.
6. 호스트 OS를 선택합니다.
7. LUN에 대한 이니시에이터의 액세스를 제어할 호스트 매핑을 지정합니다. 기존 이니시에이터 그룹(igroup)을 지정하거나 새 igroup을 정의 및 매핑할 수 있습니다.

   > ⓘ LUN을 프로비저닝하는 동안 새로운 igroup을 생성하는 경우 다음 검색 주기(최대 15분)까지 기다려야 합니다. 따라서 사용 가능한 igroup 목록에서 기존 igroup을 사용하는 것이 좋습니다.

   새 igroup을 생성하려면 * Create a new initiator group * 버튼을 선택하고 igroup에 대한 정보를 입력합니다.

8. 저장 * 을 클릭합니다.

   LUN이 스토리지 워크로드 목록에 추가됩니다.

성능 서비스 레벨

PSL(성능 서비스 수준)을 사용하면 작업 부하에 대한 성능 및 스토리지 목표를 정의할 수 있습니다. 처음에 워크로드를 생성할 때 또는 작업 부하를 편집하여 작업 부하에 PSL을 할당할 수 있습니다.

스토리지 리소스의 관리 및 모니터링은 SLO(서비스 수준 목표)를 기준으로 합니다. SLO는 필요한 성능 및 용량을 기준으로 한 서비스 수준 계약에 의해 정의됩니다. Unified Manager에서 SLO는 NetApp 스토리지에서 실행되는 애플리케이션의 PSL 정의를 참조합니다. 스토리지 서비스는 기본 리소스의 성능과 활용률을 기준으로 차별화됩니다. PSL은 스토리지 서비스 목표에 대한 설명입니다. PSL을 사용하면 스토리지 공급업체가 워크로드의 성능 및 용량 목표를 지정할 수 있습니다. 작업 부하에 PSL을 할당하면 ONTAP의 해당 작업 부하가 성능 및 용량 목표에 따라 관리됩니다. 각 PSL은 최대, 예상 및 절대 최소 IOPS와 예상 지연 시간에 따라 결정됩니다.

Unified Manager에는 다음과 같은 유형의 PSL이 있습니다.

- * 시스템 정의 *: Unified Manager는 변경할 수 없는 몇 가지 미리 정의된 정책을 제공합니다. 사전 정의된 PSL은 다음과 같습니다.
  - 최고 성능
  - 성능
  - 값

    최고 성능, 성능 및 가치 PSL은 데이터 센터의 일반적인 스토리지 워크로드 대부분에 적용할 수 있습니다.

  또한 Unified Manager는 데이터베이스 애플리케이션에 3가지 성능 서비스 수준을 제공합니다. 이러한 PSL은 폭발적으로 증가하는 IOPS를 지원하는 매우 높은 성능의 PSL로, 처리량이 가장 많은 데이터베이스 애플리케이션에 적합합니다.

  - 데이터베이스 로그의 경우 극한입니다
  - 데이터베이스 공유 데이터의 경우 매우 높음
  - 데이터베이스 데이터의 경우 매우 높음
- * 사용자 정의 *: 사전 정의된 성능 서비스 수준이 요구 사항을 충족하지 않는 경우, 필요에 따라 새로운 PSL을 생성할 수 있습니다. 자세한 내용은 을 참조하십시오 "성능 서비스 수준 생성 및 편집".
- 익스트림 * 그 이상 *: 익스트림 PSL은 IOP가 Extreme보다 높은 워크로드에 권장되는 시스템 권장 PSL입니다. 워크로드는 IOPS, 용량 및 지연 시간을 기준으로 내부적으로 분석되며, * Storage > 워크로드 > 모든 워크로드 * 화면에서 이러한 각 워크로드에 대해 Extreme PSL 이상을 사용하는 것이 좋습니다. 최적의 성능을 보장하기 위해 작업 부하에 PSL을 적용할 수 있습니다.

  워크로드의 IOPS 매개 변수는 워크로드 동작에 따라 동적으로 생성되고, 'Beyond Extreme<number-(peak IOPS/TB)><number(expected IOPS/TB)>' 형식으로 Beyond Extreme PSL의 이름에 추가됩니다. 예를 들어, 시스템에서 최대 및 예상 IOP를 각각 106345 및 37929로 결정하는 경우, 해당 워크로드에 대해 생성되는 익스트림 PSL보다 더 높은 이름은 Extreme 106345 37929입니다. 시스템에서 이러한 PSL을 권장하지만 워크로드에 PSL을 할당할 때는 유형에 "사용자 정의"로 레이블이 지정됩니다.

PSL을 할당하여 작업 부하 관리

PSL은 * Policies * > * Performance Service Levels * 페이지에서, 그리고 스토리지 공급자 API를 사용하여 액세스할 수 있습니다. 스토리지 작업 부하를 개별적으로 관리할 필요가 없으며 PSL을 할당하여 스토리지 작업 부하를 관리하는 것이 편리합니다. 모든 수정 사항은 개별적으로 관리하는 대신 다른 PSL을 다시 할당하여 관리할 수도 있습니다. Unified Manager를 사용하면 내부 평가 및 권장사항을 기반으로 워크로드에 PSL을 할당할 수 있습니다.

워크로드에 시스템 권장 PSL을 할당하는 방법에 대한 자세한 내용은 을 참조하십시오 "작업 부하에 시스템 권장 PSL 할당"

성능 서비스 수준 페이지에는 사용 가능한 PSL 정책이 나열되며 이를 추가, 편집 및 삭제할 수 있습니다.

시스템 정의 PSL이나 현재 워크로드에 할당된 PSL은 수정할 수 없습니다. 작업 부하에 할당된 PSL이나 사용 가능한 PSL만 삭제할 수는 없습니다.

이 페이지에는 다음 정보가 표시됩니다.

필드에 입력합니다	설명
이름	PSL의 이름입니다.
유형	정책이 시스템 정의인지 사용자 정의인지 여부
예상 IOPS/TB	애플리케이션이 LUN 또는 파일 공유에 대해 수행해야 하는 최소 IOPS 수입니다. 예상 IOPS는 할당된 스토리지 개체 크기를 기준으로 할당된 최소 예상 IOPS를 지정합니다.
최대 IOPS/TB	애플리케이션이 LUN 또는 파일 공유에서 수행할 수 있는 최대 IOPS 수입니다. 최대 IOPS는 할당된 스토리지 객체 크기 또는 사용된 스토리지 객체 크기를 기준으로 할당된 최대 IOPS를 지정합니다. 최대 IOPS는 할당 정책을 기반으로 합니다. 할당 정책은 할당 공간 또는 사용된 공간입니다. 할당 정책을 allocated-space로 설정하면 peak IOPS는 스토리지 객체의 크기에 따라 계산됩니다. 할당 정책이 사용된 공간으로 설정된 경우, 스토리지 효율성을 고려하여 최대 IOPS는 스토리지 객체에 저장된 데이터의 양을 기준으로 계산됩니다. 기본적으로 할당 정책은 사용된 공간으로 설정됩니다.

필드에 입력합니다	설명
절대 최소 IOPS	예상 IOPS가 이 값보다 작은 경우 절대 최소 IOPS가 재정의로 사용됩니다. 시스템 정의 PSL의 기본값은 다음과 같습니다. • 최고 성능: 예상 IOPS >= 6144/TB인 경우 절대 최소 IOPS = 1000 • 성능: 예상 IOPS >= 2048/TB 및 < 6144/TB인 경우 절대 최소 IOPS = 500 • 값: 예상 IOPS >= 128/TB 및 < 2048/TB인 경우 절대 최소 IOPS = 75 시스템 정의 데이터베이스 PSL의 기본값은 다음과 같습니다. • 데이터베이스 로그의 경우 매우 높음: 예상 IOPS >= 22528, 절대 최소 IOPS = 4000 • 데이터베이스 공유 데이터의 경우 매우 높음: 예상 IOPS > = 16384, 절대 최소 IOPS = 2000 • 데이터베이스 데이터의 경우 매우 높음: 예상 IOPS >= 12288이면 절대 최소 IOPS = 2000입니다 사용자 지정 PSL에 대한 절대 최소 IOPS의 값이 클수록 최대 75000이 될 수 있습니다. 낮은 값은 다음과 같이 계산됩니다. 1000/예상 지연 시간
예상되는 지연 시간	스토리지 IOPS에 대한 예상 지연 시간(밀리초/밀리초/작업).
용량	클러스터에서 사용 가능한 총 용량 및 사용된 용량입니다.
워크로드	PSL에 할당된 스토리지 워크로드 수입니다.

ONTAP 클러스터에서 피크 IOPS와 예상 IOPS가 일관된 차별화된 성능을 달성하는 데 어떤 도움이 되는지 알아보려면 다음 KB 문서를 참조하십시오.https://kb.netapp.com/Advice_and_Troubleshooting/Data_Infrastructure_Management/Active_IQ_Unified_Manager/What_is_Performance_Budgeting%3F["성능 예산이란 무엇입니까?"]

작업 부하에 대해 생성된 이벤트가 **PSL**에서 정의한 임계값을 초과합니다

워크로드가 이전 시간 중 예상 지연 시간 값을 30%까지 초과할 경우 Unified Manager에서 다음 이벤트 중 하나를 생성하여 잠재적 성능 문제를 알립니다.

- 워크로드 볼륨 지연 임계값 성능 서비스 수준 정책에 정의된 대로 위반됩니다
- 워크로드 LUN 지연 임계값 성능 서비스 수준 정책에 정의된 위반

워크로드를 분석하여 지연 시간 값이 더 큰 원인이 될 수 있는 것이 무엇인지 확인할 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- "볼륨 이벤트"
- "성능 임계값 정책이 위반될 경우 발생하는 현상"
- "Unified Manager에서 워크로드 지연 시간을 사용하여 성능 문제를 식별하는 방법"
- "어떤 성능 이벤트가 있는지 확인합니다"

시스템 정의 **PSL**

다음 표에는 시스템 정의 PSL에 대한 정보가 나와 있습니다.

성능 서비스 수준	설명 및 사용 사례	예상 지연 시간**(ms/op)**	최대 **IOPS**	예상 **IOPS**	절대 최소 **IOPS**
최고 성능	매우 짧은 지연 시간으로 매우 높은 처리량을 제공합니다 지연 시간에 민감한 애플리케이션에 적합합니다	1	12288	6144	1000입니다
성능	짧은 지연 시간으로 높은 처리량을 제공합니다 데이터베이스 및 가상화 애플리케이션에 적합합니다	2	4096	2048	500입니다
값	높은 스토리지 용량과 적절한 지연 시간을 제공합니다 이메일, 웹 콘텐츠, 파일 공유, 백업 타겟 등의 대용량 애플리케이션에 적합합니다	17	512	128	75를

성능 서비스 수준	설명 및 사용 사례	예상 지연 시간**(ms/op)**	최대 **IOPS**	예상 **IOPS**	절대 최소 **IOPS**
데이터베이스 로그의 경우 극한입니다	가장 짧은 지연 시간으로 최대 처리량을 제공합니다. 데이터베이스 로그를 지원하는 데이터베이스 애플리케이션에 적합합니다. 이 PSL은 데이터베이스 로그가 폭발적으로 증가하고 로깅이 지속적으로 요구되기 때문에 가장 높은 처리량을 제공합니다.	1	45056	22528	4,000
데이터베이스 공유 데이터의 경우 매우 높음	가장 짧은 지연 시간으로 매우 높은 처리량을 제공합니다. 공통 데이터 저장소에 저장되지만 데이터베이스 간에 공유되는 데이터베이스 애플리케이션 데이터에 적합합니다.	1	32768	16384)를 참조하십시오	2000년
데이터베이스 데이터의 경우 매우 높음	가장 짧은 지연 시간으로 높은 처리량을 제공합니다. 데이터베이스 테이블 정보 및 메타데이터와 같은 데이터베이스 애플리케이션 데이터에 적합합니다.	1	24576)을 참조하십시오	12288	2000년

시스템 정의 성능 서비스 수준이 워크로드 요구 사항과 일치하지 않으면 워크로드에 최적화된 자체 성능 서비스 수준을 생성할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 역할이 있어야 합니다.
- 성능 서비스 수준 이름은 고유해야 하며 다음과 같은 예약된 키워드를 사용할 수 없습니다.

  프라임, 익스트림, 퍼포먼스, 가치, 미할당, 배움, 유휴, 기본값, 없음.

스토리지를 액세스할 애플리케이션에 필요한 서비스 수준 목표를 정의하여 성능 서비스 수준 페이지에서 사용자 지정 성능 서비스 수준을 생성하고 편집할 수 있습니다.

현재 워크로드에 할당된 성능 서비스 수준은 수정할 수 없습니다.

단계

1. 왼쪽 탐색 창의 * 설정 * 아래에서 * 정책 * > * 성능 서비스 수준 * 을 선택합니다.
2. 성능 서비스 수준* 페이지에서 새 성능 서비스 수준을 생성할지 또는 기존 성능 서비스 수준을 편집할지 여부에 따라 적절한 단추를 클릭합니다.

대상...	다음 단계를 따르십시오...
새 성능 서비스 레벨을 생성합니다	추가 * 를 클릭합니다.
기존 성능 서비스 수준을 편집합니다	기존 성능 서비스 수준을 선택한 다음 * 편집 * 을 클릭합니다.

   성능 서비스 수준을 추가하거나 편집할 페이지가 표시됩니다.

3. 성능 목표를 지정하여 성능 서비스 수준을 사용자 지정한 다음 * 제출 * 을 클릭하여 성능 서비스 수준을 저장합니다.

새 성능 서비스 레벨 또는 변경된 성능 서비스 레벨을 워크로드 페이지 또는 새 워크로드를 프로비저닝할 때 워크로드(LUN, NFS 파일 공유, CIFS 공유)에 적용할 수 있습니다.

스토리지 효율성 정책 관리

SEP(Storage Efficiency Policy)를 사용하면 워크로드의 스토리지 효율성 특성을 정의할 수 있습니다. 처음에 워크로드를 생성할 때 또는 나중에 워크로드를 편집하여 워크로드에 SEP를 할당할 수 있습니다.

스토리지 효율성에는 스토리지 활용률을 높이고 스토리지 비용을 절감하는 씬 프로비저닝, 중복제거, 데이터 압축 등의 기술 사용이 포함됩니다. SRP를 생성하는 동안 이러한 공간 절약 기술을 개별적으로 또는 함께 사용하여 스토리지 효율성을 극대화할 수 있습니다. 정책을 스토리지 워크로드와 연결하면 지정된 정책 설정이 해당 정책에 할당됩니다. Unified Manager를 사용하면 시스템 정의 및 사용자 정의 SRP를 할당하여 데이터 센터의 스토리지 리소스를 최적화할 수 있습니다.

Unified Manager는 두 가지 시스템 정의 CDP, 즉 High와 Low를 제공합니다. 이러한 CDP는 데이터 센터의 스토리지 워크로드 대부분에 적용할 수 있지만, 시스템 정의 CDP가 요구사항을 충족하지 않는 경우 자체 정책을 생성할 수 있습니다.

시스템 정의 SEP 또는 현재 워크로드에 할당된 SEP는 수정할 수 없습니다. 워크로드에 할당된 SEP를 삭제할 수 없으며, 사용 가능한 SEP만 있는 경우 삭제할 수 없습니다.

Storage Efficiency Policies 페이지에는 사용 가능한 SRP가 나열되며, 사용자 지정된 SRP를 추가, 편집 및 삭제할 수 있습니다. 이 페이지에는 다음 정보가 표시됩니다.

필드에 입력합니다	설명
이름	SEP의 이름입니다.
유형	정책이 시스템 정의인지 사용자 정의인지 여부
공간 예약	볼륨이 씬 프로비저닝되었는지 아니면 일반 프로비저닝되었는지 여부
중복 제거	워크로드에 중복 제거가 설정되었는지 여부: • 인라인: 데이터 중복 제거는 워크로드에 기록되는 동안 발생합니다 • 배경: 작업 부하에서 중복 제거가 발생합니다 • 해제: 워크로드에서 중복 제거가 해제되어 있습니다
압축	워크로드에 데이터 압축이 활성화되어 있는지 여부: • 인라인: 워크로드에 쓰는 동안 데이터 압축이 발생합니다 • 배경: 작업 부하에서 데이터 압축이 발생합니다 • 비활성화: 작업 부하에서 데이터 압축이 비활성화됩니다
워크로드	SEP에 할당된 스토리지 워크로드 수입니다

맞춤형 스토리지 효율성 정책을 생성하기 위한 지침입니다

기존 SRP가 스토리지 워크로드의 정책 요구사항을 충족하지 않는 경우 맞춤형 SEP를 생성할 수 있습니다. 그러나 스토리지 워크로드에 시스템 정의 CDP를 사용하고 필요한 경우 맞춤형 SRP만 생성하는 것이 좋습니다.

모든 워크로드 페이지와 볼륨/상태 세부 정보 페이지에서 워크로드에 할당된 SEP를 볼 수 있습니다. 대시보드 및 용량 :모든 클러스터 보기의 용량 패널에서 이러한 스토리지 효율성을 기준으로 클러스터 레벨 데이터 축소율(스냅샷 복사본 없음)을 볼 수 있습니다.

스토리지 효율성 정책 생성 및 편집

시스템 정의 스토리지 효율성 정책이 워크로드 요구사항에 맞지 않을 경우 워크로드에 최적화된

자체 스토리지 효율성 정책을 생성할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 역할이 있어야 합니다.
- 스토리지 효율성 정책 이름은 고유해야 하며 다음과 같은 예약된 키워드를 사용할 수 없습니다.

  고, 저, 미지정, 학습, 유휴, '기본'과 '없음'이 있습니다.

스토리지 효율성 정책 페이지에서 스토리지에 액세스할 애플리케이션에 필요한 스토리지 효율성 특성을 정의하여 사용자 지정 스토리지 효율성 정책을 생성하고 편집할 수 있습니다.

현재 워크로드에 할당된 스토리지 효율성 정책은 수정할 수 없습니다.

단계

1. 왼쪽 탐색 창의 * 설정 * 아래에서 * 정책 * > * 스토리지 효율성 * 을 선택합니다.
2. 스토리지 효율성 정책 * 페이지에서 새 스토리지 효율성 정책을 생성할지 또는 기존 스토리지 효율성 정책을 편집할지 여부에 따라 적절한 버튼을 클릭합니다.

대상...	다음 단계를 따르십시오...
새 스토리지 효율성 정책을 생성합니다	추가 * 를 클릭합니다
기존 스토리지 효율성 정책을 편집합니다	기존 스토리지 효율성 정책을 선택하고 * Edit * 를 클릭합니다

   스토리지 효율성 정책을 추가하거나 편집할 페이지가 표시됩니다.

3. 스토리지 효율성 특성을 지정하여 스토리지 효율성 정책을 사용자 지정한 다음 * 제출 * 을 클릭하여 스토리지 효율성 정책을 저장합니다.

새 스토리지 효율성 정책 또는 변경된 스토리지 효율성 정책을 워크로드 페이지 또는 새 워크로드를 프로비저닝할 때 워크로드(LUN, NFS 파일 공유, CIFS 공유)에 적용할 수 있습니다.

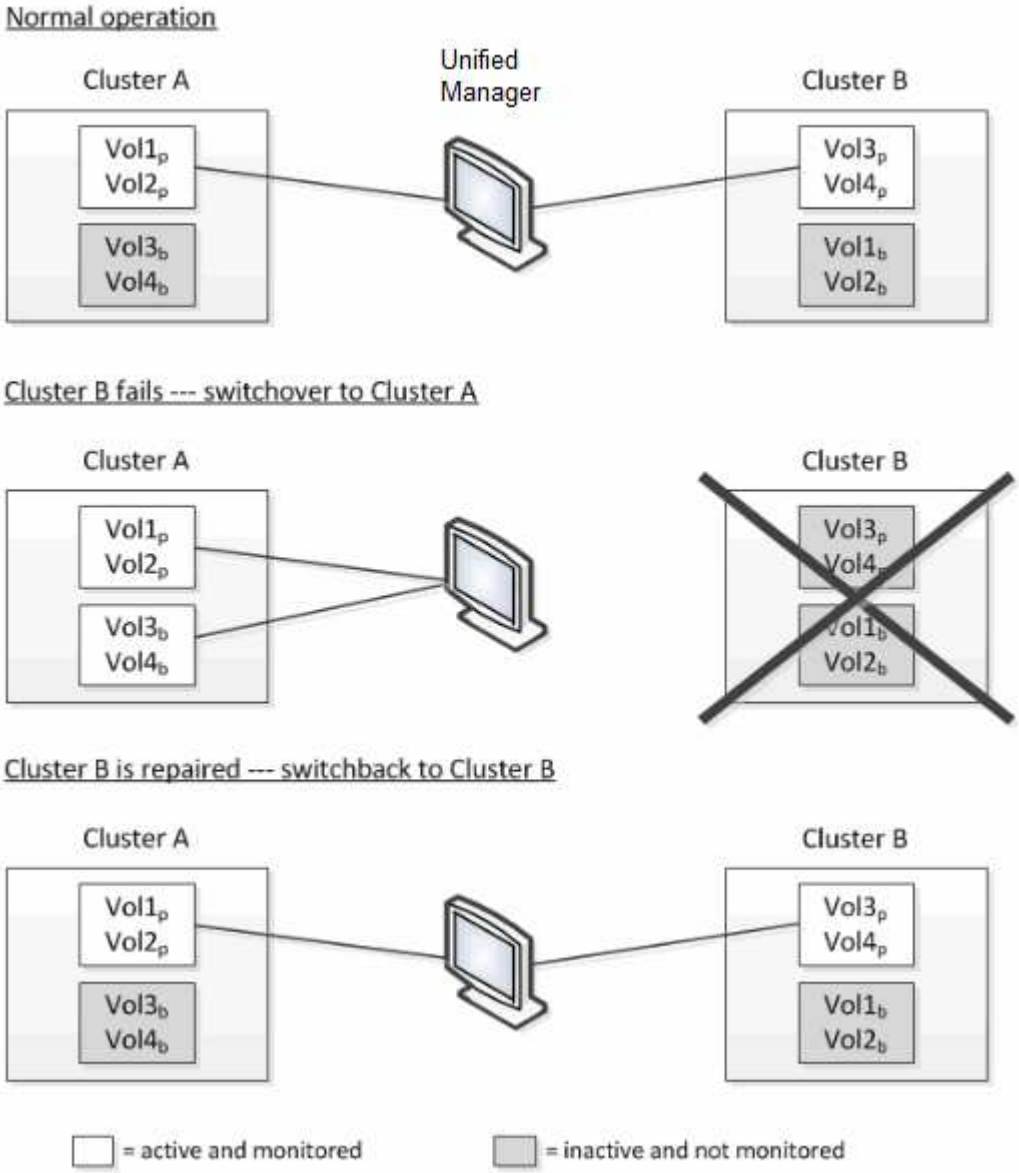
MetroCluster 구성 관리 및 모니터링

Unified Manager 웹 UI에서 MetroCluster 구성에 대한 모니터링 지원을 통해 FC 및 IP 구성을 통해 MetroCluster의 연결 문제를 확인할 수 있습니다. 연결 문제를 조기에 발견할 경우 MetroCluster 구성을 효과적으로 관리할 수 있습니다.

스위치오버 및 스위치백 중 볼륨 동작

스위치오버 또는 스위치백을 트리거하는 이벤트는 활성 볼륨을 재해 복구 그룹의 다른 클러스터로 이동합니다. 활성 상태이고 클라이언트에 데이터를 제공하는 클러스터의 볼륨이 중지되고 다른 클러스터의 볼륨이 활성화되며 데이터 제공을 시작합니다. Unified Manager는 활성 상태이고 실행 중인 볼륨만 모니터링합니다.

볼륨이 한 클러스터에서 다른 클러스터로 이동되므로 두 클러스터를 모두 모니터링하는 것이 좋습니다. Unified Manager의 단일 인스턴스가 MetroCluster 구성에서 두 클러스터를 모두 모니터링할 수 있지만, 두 위치 간 거리가 필요한 경우 두 Unified Manager 인스턴스를 사용하여 두 클러스터를 모니터링해야 하는 경우도 있습니다. 다음 그림에서는 Unified Manager의 단일 인스턴스를 보여 줍니다.



이름에 p 가 있는 볼륨은 기본 볼륨을 나타내고, 이름에 b 가 있는 볼륨은 SnapMirror에서 만든 미러링된 백업 볼륨입니다.

정상 작동 시:

- 클러스터 A에는 Vol1p와 Vol2p의 두 개의 활성 볼륨이 있습니다.
- 클러스터 B에는 Vol3p와 Vol4p의 두 개의 활성 볼륨이 있습니다.
- 클러스터 A에는 Vol3b와 Vol4b의 두 개의 비활성 볼륨이 있습니다.
- 클러스터 B에는 Vol1b와 Vol2b라는 두 개의 비활성 볼륨이 있습니다.

각 활성 볼륨(통계, 이벤트 등)에 대한 정보는 Unified Manager에서 수집합니다. Vol1p 및 Vol2p 통계는 클러스터 A에 의해 수집되고 Vol3p 및 Vol4p 통계는 클러스터 B에 의해 수집됩니다

심각한 장애가 발생하면 클러스터 B에서 클러스터 A로 활성 볼륨이 전환됩니다.

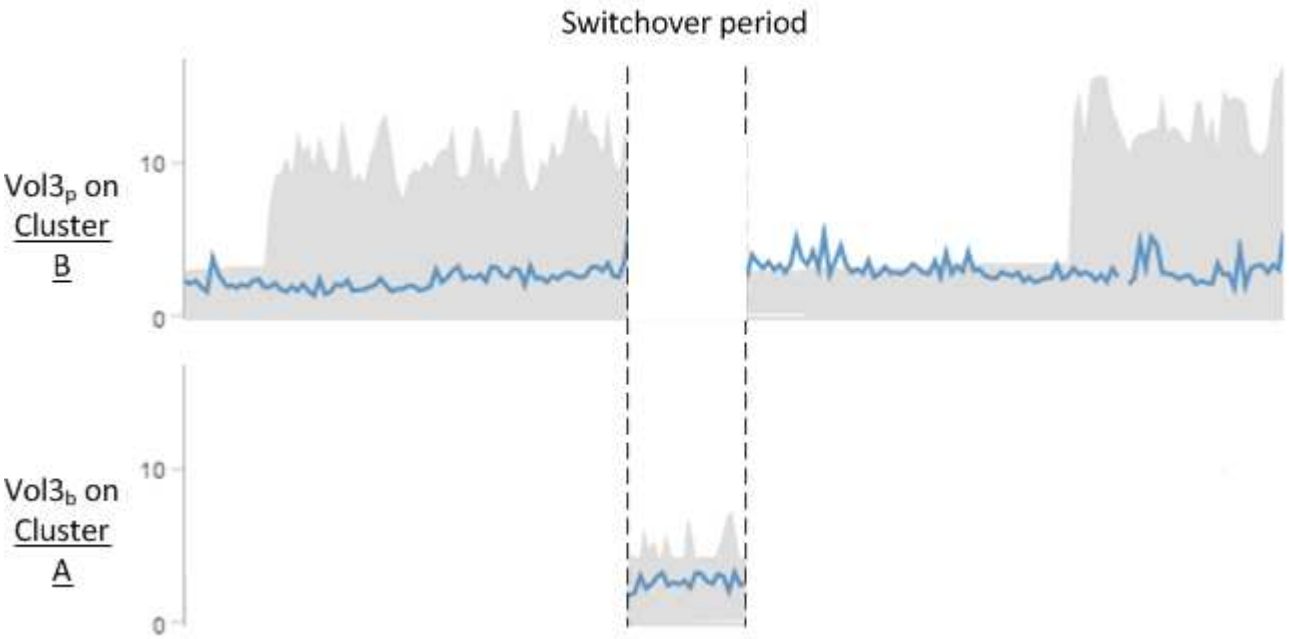
- 클러스터 A에는 Vol1p, Vol2p, Vol3b 및 Vol4b의 4개의 활성 볼륨이 있습니다.
- 클러스터 B에는 Vol3p, Vol4p, Vol1b 및 Vol2b의 4개의 비활성 볼륨이 있습니다.

정상 작동 중에 각 활성 볼륨과 관련된 정보가 Unified Manager에서 수집됩니다. 그러나 이 경우 Vol1p 및 Vol2p 통계는 클러스터 A에 의해 수집되고 Vol3b 및 Vol4b 통계도 클러스터 A에 의해 수집됩니다

Vol3p와 Vol3b는 서로 다른 클러스터에 있으므로 동일한 볼륨이 아닙니다. Vol3p용 Unified Manager의 정보는 Vol3b와 다릅니다.

- 클러스터 A로 전환하는 동안 Vol3p 통계 및 이벤트가 표시되지 않습니다.
- 첫 번째 스위치오버에서는 Vol3b가 기록 정보가 없는 새 볼륨으로 보입니다.

클러스터 B가 복구되고 스위치백 이 수행되면 클러스터 B에서 Vol3p가 다시 활성화되며, 전환 중에 기간별 통계 및 기간의 통계 차이가 표시됩니다. Vol3b는 다른 전환이 발생할 때까지 클러스터 A에서 볼 수 없습니다.



- 스위치백 후 클러스터 A의 Vol3b와 같이 비활성 상태인 MetroCluster 볼륨은 "'이 볼륨이 삭제되었습니다.' 메시지로 식별됩니다. 이 볼륨은 실제로 삭제되지 않지만 활성 볼륨이 아니기 때문에 현재 Unified Manager에서 모니터링되지 않습니다.
- 단일 Unified Manager가 MetroCluster 구성에서 두 클러스터를 모두 모니터링하는 경우, 볼륨 검색은 해당 시점에 활성 상태인 볼륨에 대한 정보를 반환합니다. 예를 들어, "Vol3"을 검색하면 클러스터 A에서 전환이 발생하고 Vol3이 활성 상태가 되면 클러스터 A의 Vol3b에 대한 통계 및 이벤트가 반환됩니다

FC를 통한 MetroCluster 구성에 대한 클러스터 연결 상태 정의

FC를 통한 MetroCluster 구성의 클러스터 간 접속은 Optimal(최적), Impacted(영향) 또는 Down(중단) 상태 중 하나일 수 있습니다. 연결 상태를 이해하면 MetroCluster 구성을 효과적으로 관리할 수 있습니다.

연결 상태	설명	아이콘이 표시됩니다
최적	MetroCluster 구성에서 클러스터 간 접속은 정상입니다.	
영향을 받습니다	하나 이상의 오류로 인해 장애 조치 가용성 상태가 저하되지만 MetroCluster 구성의 두 클러스터가 여전히 작동 중입니다. 예를 들어, ISL 링크가 다운되거나, 인터클러스터 IP 링크가 다운되거나, 파트너 클러스터에 연결할 수 없는 경우	
아래로	MetroCluster 구성에서 클러스터 간 연결이 다운된 이유는 클러스터 중 하나 또는 둘 모두가 다운되었거나 클러스터가 페일오버 모드에 있기 때문입니다. 예를 들어, 재해 또는 테스트 목적으로 계획된 전환이 있는 경우 파트너 클러스터가 중단된 경우	오류 발생 시 전환: 전환 성공:

FC를 통한 MetroCluster의 데이터 미러링 상태 정의

FC 기반 MetroCluster 구성은 데이터 미러링을 제공하며 전체 사이트를 사용할 수 없게 될 경우 페일오버를 시작할 수 있는 추가적인 기능을 제공합니다. FC를 통한 MetroCluster 구성의 클러스터 간 데이터 미러링 상태는 정상 또는 미러링을 사용할 수 없음이 될 수 있습니다. 상태를 이해하면 MetroCluster 구성을 효과적으로 관리할 수 있습니다.

데이터 미러링 상태	설명	아이콘이 표시됩니다
정상	MetroCluster 구성에서 클러스터 간 데이터 미러링은 정상입니다.	

데이터 미러링 상태	설명	아이콘이 표시됩니다
미러링을 사용할 수 없습니다	스위치오버로 인해 MetroCluster 구성에서 클러스터 간 데이터 미러링을 사용할 수 없습니다. 예를 들어, 재해 또는 테스트 목적으로 계획된 전환이 있는 경우 파트너 클러스터가 중단된 경우	오류 발생 시 전환: 전환 성공:

MetroCluster 구성 모니터링

MetroCluster 구성에서 연결 문제를 모니터링할 수 있습니다. 세부 정보에는 클러스터 내의 구성 요소 및 연결 상태와 MetroCluster 구성의 클러스터 간 연결 상태가 포함됩니다. 여기에서는 MetroCluster over FC 및 MetroCluster over IP 구성으로 보호되는 클러스터에서 연결 문제를 모니터링하는 방법을 알아봅니다.

Active IQ Unified Manager 왼쪽 탐색 창에서 다음 뷰에서 MetroCluster 구성을 모니터링할 수 있습니다.

- * 스토리지 * > * 클러스터 * > * 보호:MetroCluster * 보기
- * 보호 * > * 관계 * > * 관계: MetroCluster * 보기

Unified Manager에서는 시스템 상태 알림을 사용하여 MetroCluster 구성의 구성요소 및 연결 상태를 표시합니다.

- 필요한 것 *
- MetroCluster 구성의 로컬 및 원격 클러스터를 모두 Active IQ Unified Manager에 추가해야 합니다.
- MetroCluster over IP 구성에서 중재자를 지원하는 경우 해당 API를 통해 중재자를 구성하고 클러스터에 추가해야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

FC를 통한 MetroCluster 구성의 연결 문제 모니터링

MetroCluster over FC 구성의 클러스터의 경우 연결 차트가 * 클러스터/상태 * 세부 정보 페이지에 표시됩니다. 다음 단계를 수행합니다.

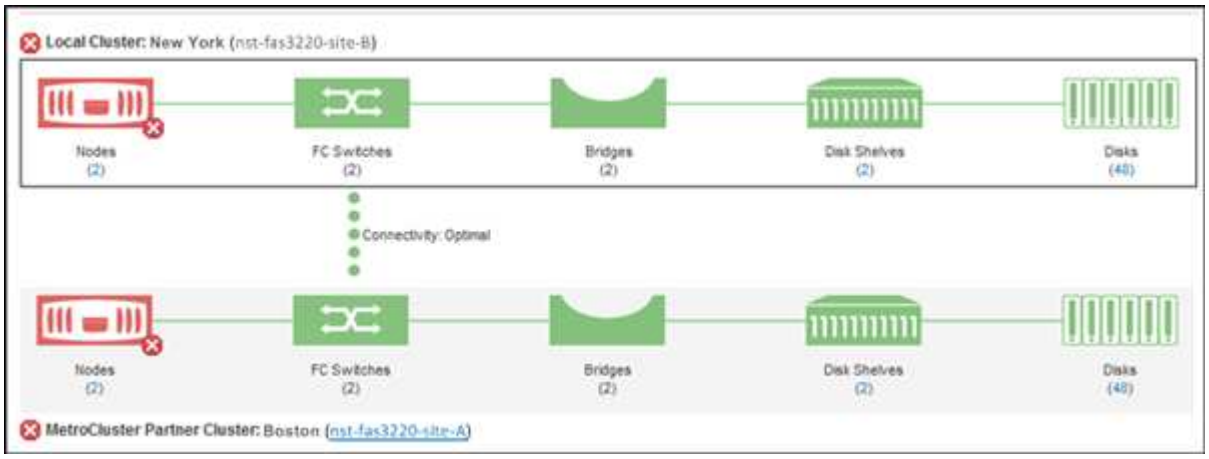
단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.

   모니터링되는 모든 클러스터의 목록이 표시됩니다.

2. 보호: MetroCluster * 보기에서 FC를 통한 MetroCluster 구성 세부 정보를 확인할 클러스터 이름을 클릭합니다. 또는 MetroCluster 구성에서 클러스터로 필터링할 수 있습니다.

3. 클러스터/상태 * 세부 정보 페이지에서 * MetroCluster 연결 * 탭을 클릭합니다. MetroCluster 연결 * 탭은 FC를 통한 MetroCluster 구성에만 사용할 수 있습니다.



MetroCluster 구성의 토폴로지가 해당 클러스터 오브젝트 영역에 표시됩니다. 클러스터/상태 세부 정보 페이지에 표시된 정보를 사용하여 연결 문제를 해결할 수 있습니다. 예를 들어, 노드와 클러스터 내 스위치 간의 연결이 다운된 경우 다음 아이콘이 표시됩니다.

아이콘 위로 포인터를 이동하면 생성된 이벤트에 대한 자세한 정보를 볼 수 있습니다.

MetroCluster 구성에서 연결 문제를 발견한 경우, System Manager에 로그인하거나 ONTAP CLI에 액세스하여 문제를 해결해야 합니다.

클러스터 상태를 확인하는 방법에 대한 자세한 내용은 를 참조하십시오 "FC를 통한 MetroCluster 구성의 클러스터 상태 확인".

MetroCluster over IP 구성에서 연결 문제를 모니터링합니다

MetroCluster over IP 구성의 클러스터의 경우 연결 차트가 * 클러스터 * 페이지에 표시됩니다. 다음 단계를 수행합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.

   모니터링되는 모든 클러스터의 목록이 표시됩니다.

2. Protection:MetroClusters * 보기에서 IP를 통한 MetroCluster 구성 세부 정보를 확인할 클러스터 이름을 클릭합니다. 또는 MetroCluster 구성에서 클러스터로 필터링할 수 있습니다.
3. 캐럿을 클릭하여 행을 확장합니다 v 아이콘을 클릭합니다. 캐럿 아이콘은 IP를 통한 MetroCluster 구성에 의해 보호되는 클러스터에만 표시됩니다.

   소스 및 미러 사이트의 토폴로지와 연결에 사용되는 중재자를 볼 수 있습니다. 다음 정보를 볼 수 있습니다.

   - 사이트 간 연결
   - 두 사이트 모두에서 상태 및 가용성 문제가 있는 경우
   - 중재자 관련 문제

◦ 복제 관련 문제입니다.

다음과 같은 상태가 보고됩니다. 위험(), 오류() 또는 보통()를 클릭합니다. 또한 동일한 토폴로지에서 운영 데이터와 미러 데이터의 애그리게이트 데이터 복제 상태를 볼 수 있습니다.

다음 다이어그램에서 소스와 대상 클러스터 간의 사이트 간 연결을 사용할 수 없고 이들 클러스터 간의 중재자가 구성되지 않은 것을 확인할 수 있습니다.

4. 상태 아이콘을 클릭합니다. 오류 정의가 포함된 메시지가 표시됩니다. MetroCluster over IP 구성에서 문제에 대한 이벤트가 발생한 경우 메시지에서 * 이벤트 보기 * 단추를 클릭하여 이벤트 세부 정보를 볼 수 있습니다. 문제와 이벤트를 해결하면 이 토폴로지의 상태 아이콘이 정상(로 바뀝니다)를 클릭합니다.
5. 자세한 구성 정보는 * 클러스터/상태 * 세부 정보 페이지의 * 구성 * 탭에 있는 * MetroCluster 개요 * 및 * 보호 * 섹션에서 확인할 수 있습니다.

IP 기반 MetroCluster 구성에만 * 클러스터 * 페이지에서 클러스터 토폴로지를 볼 수 있습니다. FC 기반 MetroCluster 구성의 클러스터의 경우 * 클러스터/상태 * 세부 정보 페이지의 * MetroCluster 연결 * 탭에 토폴로지가 표시됩니다.

- 관련 정보 *
- "클러스터/상태 세부 정보 페이지"
- 관계: MetroCluster * 보기에 대한 자세한 내용은 을 참조하십시오 "MetroCluster 구성 모니터링".
- 관계: 지난 1개월 전송 상태* 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 최근 1개월 전송 상태 보기".
- 관계: 지난 1개월 전송 속도* 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 최근 1개월 전송 속도 보기".
- 관계: 모든 관계 * 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 모든 관계 보기".

MetroCluster 복제 모니터링

데이터를 미러링하는 동안 논리 연결의 전체 상태를 모니터링하고 진단할 수 있습니다. 애그리게이트, 노드, 스토리지 가상 머신 등과 같은 클러스터 구성 요소의 미러링을 중단하는

문제 또는 위험을 식별할 수 있습니다.

Unified Manager는 시스템 상태 알림을 사용하여 MetroCluster 구성에서 구성 요소 및 연결 상태를 모니터링합니다.

- 필요한 것 *

MetroCluster 구성의 로컬 클러스터와 원격 클러스터를 모두 Unified Manager에 추가해야 합니다

IP를 통한 **MetroCluster** 구성에 대한 복제 보기

MetroCluster over IP 구성의 경우 Unified Manager의 왼쪽 탐색 창에서 다음 뷰에서 IP를 통해 MetroCluster로 보호되는 클러스터의 토폴로지 피킹 뷰(topology peeking view)에 데이터 복제 상태가 표시됩니다.

- * 스토리지 * > * 클러스터 * > * 보호:MetroCluster * 보기
- * 보호 * > * 관계 * > * 관계: MetroCluster * 보기

자세한 내용은 을 참조하십시오 "MetroCluster over IP의 연결 문제를 모니터링합니다".

FC를 통한 **MetroCluster** 구성에 대한 복제 보기

다음 단계에 따라 MetroCluster over FC 구성의 데이터 복제에 문제가 있는지 확인합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.

   모니터링되는 클러스터의 목록이 표시됩니다.

2. 상태: 모든 클러스터 * 보기에서 MetroCluster 복제 세부 정보를 보려는 클러스터의 이름을 클릭합니다. 클러스터 /상태 세부 정보 * 페이지에서 * MetroCluster 복제 * 탭을 클릭합니다.

   복제할 MetroCluster 구성의 토폴로지는 데이터가 미러링되는 원격 사이트에 대한 정보와 함께 해당 클러스터 개체 영역의 로컬 사이트에 표시됩니다. 아이콘 위로 포인터를 이동하면 생성된 이벤트에 대한 자세한 정보를 볼 수 있습니다.

클러스터/상태 세부 정보 페이지에 표시된 정보를 사용하여 복제 문제를 해결할 수 있습니다. MetroCluster 구성에서 미러링 문제를 발견한 경우, System Manager에 로그인하거나 ONTAP CLI에 액세스하여 문제를 해결해야 합니다.

- 관련 정보 *

"클러스터/상태 세부 정보 페이지"

할당량 관리

사용자 및 그룹 할당량을 사용하여 사용자 또는 사용자 그룹이 사용할 수 있는 디스크 공간 또는 파일 수를 제한할 수 있습니다. 디스크 및 파일 사용, 디스크에 설정된 다양한 제한 등 사용자 및 사용자 그룹 할당량 정보를 볼 수 있습니다.

할당량 제한이란 무엇입니까

사용자 할당량 제한이란 Unified Manager 서버가 사용자의 공간 사용량이 제한에 도달했는지 또는 사용자의 할당량에 의해 설정된 한도에 도달했는지 여부를 평가하는 데 사용하는 값입니다. 소프트 제한값을 초과하거나 하드 제한값에 도달하면 Unified Manager 서버가 사용자 할당량 이벤트를 생성합니다.

기본적으로 Unified Manager 서버는 할당량 소프트 제한값을 초과했거나 할당량 하드 제한값에 도달했으며 사용자 할당량 이벤트가 구성된 사용자에게 알림 이메일을 보냅니다. 응용 프로그램 관리자 역할을 가진 사용자는 지정된 받는 사람에게 사용자 또는 사용자 그룹 할당량 이벤트를 알리는 경고를 구성할 수 있습니다.

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 할당량 제한을 지정할 수 있습니다.

사용자 및 사용자 그룹 할당량 보기

스토리지 VM/상태 세부 정보 페이지에는 SVM에 구성된 사용자 및 사용자 그룹 할당량에 대한 정보가 표시됩니다. 사용자 또는 사용자 그룹의 이름, 디스크 및 파일에 설정된 제한, 사용된 디스크 및 파일 공간, 알림을 위한 이메일 주소를 볼 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 스토리지 VM * 을 클릭합니다.
2. 상태: 모든 스토리지 VM * 보기에서 스토리지 VM을 선택한 다음 * 사용자 및 그룹 할당량 * 탭을 클릭합니다.
    - 관련 정보 *

"사용자 추가"

전자 메일 주소를 생성하는 규칙을 만듭니다

클러스터, SVM(스토리지 가상 머신), 볼륨, Qtree, 사용자 또는 사용자 그룹과 연결된 사용자 할당량을 기준으로 이메일 주소를 지정하는 규칙을 생성할 수 있습니다. 할당량 위반이 발생하면 지정된 이메일 주소로 알림이 전송됩니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 사용자 및 그룹 할당량 이메일 주소 생성 규칙 페이지의 지침을 검토해야 합니다.

할당량 이메일 주소에 대한 규칙을 정의하고 이를 실행할 순서대로 입력해야 합니다. 예를 들어 abc@xyz.com 전자 메일 주소를 사용하여 abc에 대한 할당량 위반에 대한 알림을 받고 다른 모든 그룹에 대해 전자 메일 주소 dl-$group@$domain을 사용하려면 규칙이 다음 순서로 나열되어야 합니다.

- 만약 ($user=='abc')이면 abc@xyz.com 입니다
- IF($group== *) dl-$group@$domain

지정한 규칙에 대한 조건이 충족되지 않으면 기본 규칙이 사용됩니다.

($USER_OR_GROUP===*)인 경우 $USER_OR_GROUP@$domain

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 할당량 이메일 규칙 * 을 클릭합니다.
2. 기준에 따라 규칙을 입력합니다.
3. 규칙 구문의 유효성을 검사하려면 * Validate * 를 클릭합니다.

   규칙 구문이 잘못된 경우 오류 메시지가 표시됩니다. 구문을 수정하고 * Validate * 를 다시 클릭해야 합니다.

4. 저장 * 을 클릭합니다.
5. 생성한 e-메일 주소가 Storage * VM/Health * 세부 정보 페이지의 * 사용자 및 그룹 할당량 * 탭에 표시되는지 확인합니다.

사용자 및 사용자 그룹 할당량에 대한 **e-**메일 알림 형식을 생성합니다

할당량 관련 문제(소프트 제한값 위반 또는 하드 제한값에 도달함)가 있을 때 사용자 또는 사용자 그룹에 전송되는 이메일에 대한 알림 형식을 생성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 할당량 이메일 형식 * 을 클릭합니다.
2. From *, * Subject * 및 * Email Details * 필드에 세부 정보를 입력하거나 수정합니다.
3. 미리 보기 * 를 클릭하여 이메일 알림을 미리 봅니다.
4. 미리보기 창을 닫으려면 * 닫기 * 를 클릭합니다.
5. 필요한 경우 이메일 알림의 내용을 수정합니다.
6. 저장 * 을 클릭합니다.

사용자 및 그룹 할당량 이메일 주소 편집

클러스터, SVM(스토리지 가상 머신), 볼륨, Qtree, 사용자 또는 사용자 그룹과 연결된 사용자 할당량을 기준으로 이메일 주소를 수정할 수 있습니다. 사용자 및 그룹 할당량 이메일 주소 생성 규칙 대화 상자에서 지정한 규칙에 의해 생성된 이메일 주소를 무시하려면 이메일 주소를 수정할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 을(를) 검토해야 합니다 "규칙 작성 지침".

전자 메일 주소를 편집하는 경우 사용자 및 그룹 할당량 전자 메일 주소를 생성하는 규칙이 더 이상 할당량에 적용되지 않습니다. 지정한 규칙에 의해 생성된 이메일 주소로 알림을 보내려면 이메일 주소를 삭제하고 변경 내용을 저장해야

합니다.

단계

1. 왼쪽 탐색 창에서 * Storage * > * SVM * 을 클릭합니다.
2. 상태: 모든 스토리지 VM * 보기에서 SVM을 선택한 다음 * 사용자 및 그룹 할당량 * 탭을 클릭합니다.
3. 탭 행 아래에 있는 * 이메일 주소 편집 * 을 클릭합니다.
4. 이메일 주소 편집 * 대화 상자에서 적절한 조치를 수행합니다.

만약...	그러면...
지정한 규칙에 의해 생성된 이메일 주소로 알림을 전송하고자 합니다	a. 이메일 주소 * 필드에서 이메일 주소를 삭제합니다. b. 저장 * 을 클릭합니다. c. F5 키를 눌러 전자 메일 주소 편집 대화 상자를 다시 로드하여 브라우저를 새로 고칩니다. 지정한 규칙에 의해 생성된 이메일 주소는 * 이메일 주소 * 필드에 표시됩니다.
알림을 지정된 이메일 주소로 전송하려는 경우	a. 이메일 주소 * 필드에서 이메일 주소를 수정합니다. b. 저장 * 을 클릭합니다. 사용자 및 그룹 할당량 e-메일 주소를 생성하는 규칙은 더 이상 할당량에 적용되지 않습니다.

할당량에 대한 자세한 정보

할당량에 대한 개념을 이해하면 사용자 할당량과 사용자 그룹 할당량을 효율적으로 관리할 수 있습니다.

할당량 프로세스 개요

할당량은 소프트 또는 하드일 수 있습니다. 소프트 할당량을 사용하면 ONTAP에서 지정된 제한을 초과할 때 알림을 보내고, 하드 할당량을 사용하면 지정된 제한을 초과할 때 쓰기 작업이 성공하지 못합니다.

ONTAP가 사용자 또는 사용자 그룹으로부터 FlexVol 볼륨에 쓰기 요청을 수신하면 사용자 또는 사용자 그룹의 해당 볼륨에서 할당량이 활성화되었는지 확인하고 다음을 확인합니다.

- 하드 제한값에 도달할지 여부

  yes인 경우 하드 제한값에 도달하고 하드 할당량 알림이 전송되면 쓰기 작업이 실패합니다.

- 소프트 제한값을 위반할지 여부

  yes인 경우 소프트 제한값이 위반되고 소프트 할당량 알림이 전송되면 쓰기 작업이 성공합니다.

- 쓰기 작업이 소프트 제한값을 초과하지 않는지 여부

예 인 경우 쓰기 작업이 성공하고 알림이 전송되지 않습니다.

할당량 정보

할당량을 통해 사용자, 그룹 또는 qtree가 사용하는 파일 수와 디스크 공간을 제한하거나 추적할 수 있습니다. '/etc/quotas' 파일을 사용하여 할당량을 지정합니다. 할당량은 특정 볼륨 또는 qtree에 적용됩니다.

할당량을 사용하는 이유

할당량을 사용하여 FlexVol 볼륨의 리소스 사용량을 제한하거나, 리소스 사용량이 특정 수준에 도달할 때 알림을 제공하거나, 리소스 사용량을 추적할 수 있습니다.

다음과 같은 이유로 할당량을 지정합니다.

- 사용자 또는 그룹에서 사용할 수 있거나 qtree에 포함될 수 있는 디스크 공간 또는 파일 수를 제한합니다
- 제한을 적용하지 않고 사용자, 그룹 또는 qtree에서 사용되는 파일 수나 디스크 공간을 추적합니다
- 디스크 사용량이나 파일 사용량이 높을 때 사용자에게 경고합니다

할당량 대화 상자에 대한 설명입니다

상태: 모든 스토리지 VM 보기의 사용자 및 그룹 할당량 탭에서 적절한 옵션을 사용하여 할당량 관련 문제가 발생할 때 전송되는 e-메일 알림의 형식을 구성하고 사용자 할당량을 기준으로 e-메일 주소를 지정하는 규칙을 구성할 수 있습니다.

이메일 알림 형식 페이지

e-메일 알림 형식 페이지에는 할당량 관련 문제(소프트 제한값 위반 또는 하드 제한값에 도달함)가 있을 때 사용자 또는 사용자 그룹에 전송되는 e-메일의 규칙이 표시됩니다.

e-메일 알림은 다음 사용자 또는 사용자 그룹 할당량 이벤트가 생성된 경우에만 전송됩니다. 사용자 또는 그룹 할당량 디스크 공간 소프트 제한값 위반, 사용자 또는 그룹 할당량 파일 개수 소프트 제한값 위반, 사용자 또는 그룹 할당량 디스크 공간 하드 제한값에 도달했거나 사용자 또는 그룹 할당량 파일 개수의 하드 제한값에 도달했습니다.

- * 보낸 사람 *

  E-mail을 보낼 때 사용할 수 있는 E-mail 주소를 표시합니다. 기본적으로 이 주소는 알림 페이지로 지정된 전자 메일 주소입니다.

- * 제목 *

  알림 이메일의 제목을 표시합니다.

- * 이메일 세부 정보 *

  알림 E-mail의 텍스트를 표시합니다. 요구 사항에 따라 텍스트를 수정할 수 있습니다. 예를 들어 할당량 특성과 관련된 정보를 제공하고 키워드 수를 줄일 수 있습니다. 그러나 키워드를 수정하면 안 됩니다.

유효한 키워드는 다음과 같습니다.

- $EVENT_NAME

  이메일 알림을 발생시킨 이벤트 이름을 지정합니다.

- $quota_target입니다

  할당량을 적용할 수 있는 qtree 또는 볼륨을 지정합니다.

- $quota_used_percent

  사용자 또는 사용자 그룹에서 사용하는 디스크 하드 제한값, 디스크 소프트 제한값, 파일 하드 제한값 또는 파일 소프트 제한값의 백분율을 지정합니다.

- $quota_limit입니다

  사용자 또는 사용자 그룹이 도달한 디스크 하드 제한이나 파일 하드 제한값을 지정하고 다음 이벤트 중 하나가 생성됩니다.

  - 사용자 또는 그룹 할당량 디스크 공간 하드 제한값에 도달했습니다
  - 사용자 또는 그룹 할당량 디스크 공간 소프트 제한값에 도달했습니다
  - 사용자 또는 그룹 할당량 파일 개수의 하드 제한값에 도달했습니다
  - 사용자 또는 그룹 할당량 파일 개수 소프트 제한값에 도달했습니다

- $quota_used

  사용된 디스크 공간 또는 사용자 또는 사용자 그룹이 생성한 파일 수를 지정합니다.

- $quota_user

  사용자 또는 사용자 그룹 이름을 지정합니다.

명령 버튼

명령 버튼을 사용하여 이메일 알림 형식의 변경 사항을 미리 보거나 저장하거나 취소할 수 있습니다.

- * 미리보기 *

  알림 E-mail의 미리보기를 표시합니다.

- * 출하 시 기본값으로 복원 *

  알림 형식을 공장 출하 시 기본값으로 복원할 수 있습니다.

- * 저장 *

  알림 형식에 대한 변경 내용을 저장합니다.

사용자 및 그룹 할당량 이메일 주소 생성 규칙 페이지에서는 클러스터, SVM, 볼륨, Qtree, 사용자, 애플리케이션 등과 관련된 사용자 할당량을 기준으로 이메일 주소를 지정하는 규칙을 또는 사용자 그룹. 할당량이 침해되면 지정된 e-메일 주소로 알림이 전송됩니다.

규칙 영역

할당량 이메일 주소에 대한 규칙을 정의해야 합니다. 규칙을 설명하기 위해 설명을 추가할 수도 있습니다.

규칙 정의 방법

규칙을 실행할 순서대로 입력해야 합니다. 첫 번째 규칙의 조건이 충족되면 이 규칙에 따라 이메일 주소가 생성됩니다. 조건이 충족되지 않으면 다음 규칙에 대한 조건이 고려됩니다. 각 줄에는 별도의 규칙이 나열됩니다. 기본 규칙은 목록의 마지막 규칙입니다. 규칙의 우선 순위 순서를 변경할 수 있습니다. 그러나 기본 규칙의 순서는 변경할 수 없습니다.

예를 들어, 이메일 주소 qtree1@xyz.com 를 사용하여 qtree1 에 대한 할당량 위반 알림을 받고 다른 모든 qtree에 대해 이메일 주소 admin@xyz.com 를 사용하려면 규칙이 다음 순서로 나열되어야 합니다.

- ($qtree =='qtree1')인 경우 qtree1@xyz.com 으로 제출하시기 바랍니다
- ($qtree == *)인 경우 admin@xyz.com 으로 제출하시기 바랍니다

지정한 규칙에 대한 조건이 충족되지 않으면 기본 규칙이 사용됩니다.

($USER_OR_GROUP===*)인 경우 $USER_OR_GROUP@$domain

두 명 이상의 사용자가 동일한 할당량을 사용하는 경우 사용자 이름이 쉼표로 구분된 값으로 표시되며 이 규칙은 할당량에 적용되지 않습니다.

설명을 추가하는 방법

규칙을 설명하기 위해 설명을 추가할 수 있습니다. 각 설명의 시작 시에 #을 사용해야 하며 각 줄에는 별도의 설명이 나열됩니다.

규칙 구문

규칙 구문은 다음 중 하나여야 합니다.

- IF(`valid variableoperator *`)를 클릭합니다 `email ID@domain name`

  IF는 키워드이고 소문자로 되어 있습니다. 연산자는 == 입니다. e-메일 ID에는 모든 문자, 유효한 변수 $USER_OR_GROUP, $USER 또는 $GROUP 또는 문자 및 유효한 변수 $USER_OR_GROUP, $USER 또는 $GROUP의 조합이 포함될 수 있습니다. 도메인 이름에는 임의의 문자, 유효한 변수 $domain 또는 임의의 문자와 유효한 변수 $domain의 조합이 포함될 수 있습니다. 유효한 변수는 대문자나 소문자일 수 있지만 둘 다 함께 사용할 수는 없습니다. 예를 들어 $domain과 $domain은 유효하지만 $Domain은 유효한 변수가 아닙니다.

- IF(`valid variableoperator` `string`)를 클릭합니다 `email ID@domain name`

  IF는 키워드이고 소문자입니다. 연산자는 또는 == 를 포함할 수 있습니다. e-메일 ID에는 모든 문자, 유효한 변수 $USER_OR_GROUP, $USER 또는 $GROUP 또는 문자 및 유효한 변수 $USER_OR_GROUP, $USER 또는 $GROUP의 조합이 포함될 수 있습니다. 도메인 이름에는 임의의 문자, 유효한 변수 $domain 또는 임의의 문자와 유효한 변수 $domain의 조합이 포함될 수 있습니다. 유효한 변수는 대문자나 소문자일 수 있지만 둘 다 함께 사용할

수는 없습니다. 예를 들어 $domain과 $domain은 유효하지만 $Domain은 유효한 변수가 아닙니다.

명령 버튼

명령 단추를 사용하면 생성된 규칙을 저장, 확인 또는 취소할 수 있습니다.

- * 검증 *

  생성된 규칙의 구문을 검증합니다. 유효성 검사 중에 오류가 발생하면 오류를 생성하는 규칙과 오류 메시지가 함께 표시됩니다.

- * 출하 시 기본값으로 복원 *

  주소 규칙을 출하 시 기본값으로 복원할 수 있습니다.

- * 저장 *

  규칙 구문의 유효성을 검사하고 오류가 없는 경우 규칙을 저장합니다. 유효성 검사 중에 오류가 발생하면 오류를 생성하는 규칙과 오류 메시지가 함께 표시됩니다.

문제 해결

문제 해결 정보는 Unified Manager를 사용할 때 발생하는 문제를 식별하고 해결하는 데 도움이 됩니다.

Unified Manager 데이터베이스 디렉토리에 디스크 공간 추가

Unified Manager 데이터베이스 디렉토리에는 ONTAP 시스템에서 수집된 모든 상태 및 성능 데이터가 포함되어 있습니다. 경우에 따라 데이터베이스 디렉토리의 크기를 늘려야 할 수 있습니다.

예를 들어, Unified Manager가 각 클러스터에 노드가 많은 수의 클러스터에서 데이터를 수집하는 경우 데이터베이스 디렉토리가 가득 찰 수 있습니다. 데이터베이스 디렉토리가 90% 찼을 때 경고 이벤트가 수신되고 디렉토리가 95% 찼을 때 중요한 이벤트가 발생합니다.

디렉토리가 95% 꽉 찬 후 클러스터에서 추가 데이터가 수집되지 않습니다.

데이터 디렉토리에 용량을 추가하는 데 필요한 단계는 Unified Manager가 VMware ESXi 서버, Red Hat 또는 CentOS Linux 서버 또는 Microsoft Windows 서버에서 실행 중인지 여부에 따라 다릅니다.

VMware 가상 머신의 데이터 디스크에 공간 추가

Unified Manager 데이터베이스의 데이터 디스크 공간을 늘려야 하는 경우, Unified Manager 유지보수 콘솔을 사용하여 디스크 공간을 늘려서 설치 후 용량을 추가할 수 있습니다.

- 필요한 것 *
- vSphere Client에 대한 액세스 권한이 있어야 합니다.

- 가상 머신에 로컬에 저장된 스냅샷이 없어야 합니다.
- 유지보수 사용자 자격 증명이 있어야 합니다.

가상 디스크의 크기를 늘리기 전에 가상 시스템을 백업하는 것이 좋습니다.

단계

1. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 데이터 디스크 용량을 디스크 3에 추가합니다. 자세한 내용은 VMware 설명서를 참조하십시오.

   드물지만 Unified Manager 배포에서 "하드 디스크 3" 대신 데이터 디스크에 "하드 디스크 2"를 사용하는 경우가 있습니다. 구축 과정에서 이 문제가 발생한 경우 더 큰 디스크의 공간을 늘리십시오. 데이터 디스크는 항상 다른 디스크보다 더 많은 공간을 갖게 됩니다.

2. vSphere 클라이언트에서 Unified Manager 가상 머신을 선택한 다음 * Console * 탭을 선택합니다.
3. 콘솔 창을 클릭한 다음 사용자 이름과 암호를 사용하여 유지보수 콘솔에 로그인합니다.
4. 주 메뉴 * 에서 * 시스템 구성 * 옵션의 번호를 입력합니다.
5. 시스템 구성 메뉴 * 에서 * 데이터 디스크 크기 증가 * 옵션의 숫자를 입력합니다.

Linux 호스트의 데이터 디렉토리에 공간을 추가합니다

처음에 Linux 호스트를 설정한 다음 Unified Manager를 설치할 때 Unified Manager를 지원하기 위해 '/opt/netapp/data' 디렉토리에 디스크 공간을 충분히 할당한 경우, '/opt/netapp/data' 디렉토리에서 디스크 공간을 늘려서 설치 후 디스크 공간을 추가할 수 있습니다.

- 필요한 것 *

Unified Manager가 설치된 Red Hat Enterprise Linux 또는 CentOS Linux 시스템에 대한 루트 사용자 액세스 권한이 있어야 합니다.

데이터 디렉토리 크기를 늘리기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가할 Linux 시스템에 루트 사용자로 로그인합니다.
2. 'emctl stop socieau sociqld'와 같은 순서로 Unified Manager 서비스와 관련 MySQL 소프트웨어를 중지합니다
3. 현재 '/opt/netapp/data' 디렉토리에 데이터를 포함할 디스크 공간이 충분한 임시 백업 폴더(예: /backup-data')를 생성합니다.
4. 기존 '/opt/netapp/data' 디렉토리의 컨텐츠 및 권한 구성을 백업 데이터 디렉토리에 복사합니다.

   'cp-arp/opt/netapp/data/ * /backup-data

5. SE Linux가 활성화된 경우:

   a. 기존 '/opt/netapp/data' 폴더의 폴더에 대한 SE Linux 유형을 가져옵니다.

      ```
      se_type=`ls -Z /opt/netapp/data| awk '{print $4}'| awk -F: '{print $3}'|
      head -1
      ```

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
echo $se_type
mysqld_db_t
```

a. "chcon" 명령을 실행하여 백업 디렉토리에 대한 SE Linux 유형을 설정합니다.

'chcon-R—type=mysqld_db_t/backup-data

6. '/opt/netapp/data' 디렉터리의 내용을 제거합니다.
   a. 'cd/opt/netapp/data'
   b. rm-rf *
7. LVM 명령을 사용하거나 추가 디스크를 추가하여 '/opt/netapp/data' 디렉토리의 크기를 최소 150GB로 확장합니다.

> 디스크에서 '/opt/netapp/data'를 생성한 경우 NFS 또는 CIFS 공유로 '/opt/netapp/data'를 마운트하지 마십시오. 이 경우 디스크 공간을 확장하려고 하면 'resize', 'extend' 같은 일부 LVM 명령이 예상대로 작동하지 않을 수 있기 때문입니다.

8. '/opt/netapp/data' 디렉토리 소유자(MySQL) 및 그룹(root)이 변경되지 않았는지 확인합니다.

'ls-ltr/opt/netapp/|grep data'

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. SE Linux가 활성화된 경우, '/opt/netapp/data' 디렉토리의 컨텍스트가 mysqld_db_t로 설정되어 있는지 확인합니다.
   a. 'touch/opt/netapp/data/abc
   b. 'ls-Z/opt/netapp/data/abc

시스템은 다음과 유사한 확인 메시지를 반환합니다.

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. 이 불필요한 파일로 인해 나중에 데이터베이스 오류가 발생하지 않도록 'abc' 파일을 삭제합니다.
11. "backup-data"의 내용을 다시 확장된 "opt/netapp/data" 디렉토리로 복사합니다.

'cp-arp/backup-data/ * /opt/netapp/data/'

12. SE Linux가 활성화된 경우 다음 명령을 실행합니다.

'chcon-R—type=mysqld_db_t/opt/netapp/data

13. MySQL 서비스를 시작합니다.

    '스타emctl start mysqld'

14. MySQL 서비스가 시작된 후 다음 순서대로 socie 및 socieau 서비스를 시작합니다.

    '신조 시작 조숙자'

15. 모든 서비스가 시작된 후 백업 폴더 "/backup-data"를 삭제합니다.

    'rm-rf/backup-data

Microsoft Windows 서버의 논리 드라이브에 공간 추가

Unified Manager 데이터베이스의 디스크 공간을 늘려야 하는 경우 Unified Manager가 설치된 논리 드라이브에 용량을 추가할 수 있습니다.

- 필요한 것 *

Windows 관리자 권한이 있어야 합니다.

디스크 공간을 추가하기 전에 Unified Manager 데이터베이스를 백업하는 것이 좋습니다.

단계

1. 디스크 공간을 추가할 Windows 서버에 관리자로 로그인합니다.
2. 공간을 더 추가하는 데 사용할 방법에 해당하는 단계를 따릅니다.

옵션을 선택합니다	설명
물리적 서버에서 Unified Manager 서버가 설치된 논리 드라이브에 용량을 추가합니다.	Microsoft 항목의 단계를 따릅니다. "기본 볼륨을 확장합니다"
물리적 서버에서 하드 디스크 드라이브를 추가합니다.	Microsoft 항목의 단계를 따릅니다. "하드 디스크 드라이브 추가"
가상 머신에서 디스크 파티션의 크기를 늘립니다.	VMware 항목의 단계를 따릅니다. "디스크 파티션 크기 늘리기"

성능 통계 수집 주기 변경

성능 통계에 대한 기본 수집 간격은 5분입니다. 대규모 클러스터의 컬렉션이 기본 시간 내에 마중되지 않으면 이 간격을 10 또는 15분으로 변경할 수 있습니다. 이 설정은 Unified Manager의 이 인스턴스가 모니터링하는 모든 클러스터의 통계 모음에 영향을 줍니다.

- 필요한 것 *

Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.

성능 통계 수집 시간이 정시에 마무리되지 않는 문제는 "Unable to s일관되게 collect from cluster <cluster_name> or Data collection is too long long long on cluster <cluster_name>"이라는 배너 메시지가 표시됩니다

통계 수집 문제로 인해 필요한 경우에만 수집 간격을 변경해야 합니다. 다른 이유로 이 설정을 변경하지 마십시오.

> 이 값을 5분의 기본 설정에서 변경하면 Unified Manager에서 보고하는 성능 이벤트의 수와 빈도에 영향을 줄 수 있습니다. 예를 들어, 시스템 정의 성능 임계값은 정책이 30분 동안 초과될 때 이벤트를 트리거합니다. 5분 컬렉션을 사용하는 경우 6개의 연속 컬렉션에 대해 정책을 초과해야 합니다. 15분 컬렉션의 경우 두 수집 기간 동안 정책을 초과해야 합니다.

클러스터 설정 페이지 하단의 메시지는 현재 통계 데이터 수집 간격을 나타냅니다.

단계

1. SSH를 사용하여 Unified Manager 호스트에 대한 유지보수 사용자로 로그인합니다.

   Unified Managermaintenance 콘솔 프롬프트가 표시됩니다.

2. 성능 폴링 간격 구성 * 이라고 표시된 메뉴 옵션의 번호를 입력한 다음 Enter 키를 누릅니다.
3. 메시지가 표시되면 유지보수 사용자 암호를 다시 입력합니다.
4. 설정할 새 폴링 간격의 숫자를 입력한 다음 Enter 키를 누릅니다.

Unified Manager 수집 간격을 10분 또는 15분으로 변경하고, 외부 데이터 공급자(예: Graphite)에 현재 연결되어 있는 경우, 데이터 공급자의 전송 간격을 Unified Manager 수집 간격보다 크거나 같도록 변경해야 합니다.

Unified Manager가 이벤트 및 성능 데이터를 유지하는 기간을 변경합니다

기본적으로 Unified Manager는 모니터링되는 모든 클러스터에 대해 6개월 동안 이벤트 데이터 및 성능 데이터를 저장합니다. 이 시간이 지나면 새 데이터를 저장할 공간을 만들기 위해 오래된 데이터가 자동으로 삭제됩니다. 이 기본 일정은 대부분의 구성에서 잘 작동하지만, 많은 클러스터와 노드가 있는 매우 큰 구성에서는 Unified Manager가 최적으로 작동하도록 보존 기간을 줄여야 할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

데이터 보존 페이지에서 이러한 두 가지 데이터 유형의 보존 기간을 변경할 수 있습니다. 이러한 설정은 Unified Manager의 이 인스턴스가 모니터링하는 모든 클러스터의 데이터 보존에 영향을 줍니다.

> Unified Manager는 5분마다 성능 통계를 수집합니다. 매일 5분 통계가 매시간 성능 통계로 요약됩니다. 이 기능을 사용하면 30일 동안 5분 동안의 기간별 성능 데이터와 6개월 분량의 시간별 요약 성능 데이터를 유지할 수 있습니다(기본값).

공간이 부족하거나 백업 및 기타 작업을 완료하는 데 시간이 매우 오래 걸리는 경우에만 보존 기간을 줄여야 합니다. 보존 기간을 줄이면 다음과 같은 효과가 있습니다.

- 자정 이후 이전 성능 데이터가 Unified Manager 데이터베이스에서 삭제됩니다.

- 이전 이벤트 데이터가 Unified Manager 데이터베이스에서 즉시 삭제됩니다.
- 보존 기간 이전의 이벤트는 더 이상 사용자 인터페이스에서 볼 수 없습니다.
- UI에서 시간별 성능 통계가 표시되는 위치는 보존 기간 전에 비어 있습니다.
- 이벤트 보존 기간이 성능 데이터 보존 기간을 초과하는 경우 성능 슬라이더 아래에 오래된 성능 이벤트에 연결된 차트의 데이터가 백업되지 않을 수 있다는 메시지가 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * Policies * > * Data Retention * 을 클릭합니다.
2. Data Retention * 페이지의 Event Retention 또는 Performance Data Retention 영역에서 슬라이더 도구를 선택하고 데이터를 보존할 개월 수로 이동한 다음 * Save * 를 클릭합니다.

알 수 없는 인증 오류입니다

원격 사용자 또는 그룹을 추가, 편집, 삭제 또는 테스트하는 등 인증 관련 작업을 수행하는 경우 알 수 없는 인증 오류 메시지가 표시될 수 있습니다

- 원인 *

이 문제는 다음 옵션에 대해 잘못된 값을 설정한 경우 발생할 수 있습니다.

- Active Directory 인증 서비스의 관리자 이름입니다
- OpenLDAP 인증 서비스의 고유 이름을 바인딩합니다
- 시정 조치 *
  1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
  2. 선택한 인증 서비스에 따라 관리자 이름 또는 고유 이름 바인딩에 대한 적절한 정보를 입력합니다.
  3. 인증 테스트 * 를 클릭하여 지정한 세부 정보로 인증을 테스트합니다.
  4. 저장 * 을 클릭합니다.

사용자를 찾을 수 없습니다

원격 사용자 또는 그룹을 추가, 편집, 삭제 또는 테스트하는 등 인증 관련 작업을 수행하는 경우 사용자를 찾을 수 없습니다. 라는 오류 메시지가 표시됩니다

- 원인 *

이 문제는 사용자가 AD 서버 또는 LDAP 서버에 있고 기본 고유 이름을 잘못된 값으로 설정한 경우 발생할 수 있습니다.

- 시정 조치 *
  1. 왼쪽 탐색 창에서 * 일반 * > * 원격 인증 * 을 클릭합니다.
  2. 기본 고유 이름에 대한 적절한 정보를 입력합니다.
  3. 저장 * 을 클릭합니다.

다른 인증 서비스를 사용하여 **LDAP**를 추가하는 데 문제가 있습니다

인증 서비스로 다른 사용자를 선택하면 사용자 및 그룹 개체 클래스는 이전에 선택한 템플릿의 값을 유지합니다. LDAP 서버가 동일한 값을 사용하지 않으면 작업이 실패할 수 있습니다.

- 원인 *

사용자가 OpenLDAP에서 올바르게 구성되지 않았습니다.

- 시정 조치 *

다음 해결 방법 중 하나를 사용하여 이 문제를 수동으로 해결할 수 있습니다.

LDAP 사용자 객체 클래스와 그룹 객체 클래스가 각각 사용자 및 그룹인 경우 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 일반 > * 원격 인증 * 을 클릭합니다.
2. 인증 서비스 * 드롭다운 메뉴에서 * Active Directory * 를 선택한 다음 * 기타 * 를 선택합니다.
3. 텍스트 필드를 작성합니다.

LDAP 사용자 객체 클래스와 그룹 객체 클래스가 각각 posixAccount 및 posixGroup인 경우 다음 단계를 수행하십시오.

1. 왼쪽 탐색 창에서 일반 > * 원격 인증 * 을 클릭합니다.
2. Authentication Service * (인증 서비스 *) 드롭다운 메뉴에서 * OpenLDAP * 를 선택한 다음 * Others * 를 선택합니다.
3. 텍스트 필드를 작성합니다.

처음 두 가지 해결 방법이 적용되지 않으면 옵션 집합 API를 호출하여 auth.ldap.userObjectClass` 및 auth.ldap.groupObjectClass` 옵션을 올바른 값으로 설정합니다.

이벤트 및 알림을 관리합니다

이벤트 관리

이벤트는 모니터링되는 클러스터의 문제를 식별하는 데 도움이 됩니다.

Active IQ 플랫폼 이벤트란 무엇입니까

Unified Manager는 Active IQ 플랫폼에서 검색된 이벤트를 표시할 수 있습니다. 이러한 이벤트는 Unified Manager가 모니터링하는 모든 스토리지 시스템에서 생성되는 AutoSupport 메시지에 대해 일련의 규칙을 실행하여 생성됩니다.

자세한 내용은 을 참조하십시오 "Active IQ 플랫폼 이벤트 생성 방법".

Unified Manager는 새 규칙 파일을 자동으로 확인하고 새 규칙이 있을 때만 새 파일을 다운로드합니다. 외부 네트워크에 액세스할 수 없는 사이트에서는 * 스토리지 관리 * > * 이벤트 설정 * > * 규칙 업로드 * 에서 수동으로 규칙을 업로드해야 합니다.

Active IQ 이벤트는 기존 Unified Manager 이벤트와 중복되지 않으며 시스템 구성, 케이블 연결, 모범 사례 및 가용성 문제와 관련된 인시던트나 위험을 식별합니다.

플랫폼 이벤트 활성화에 대한 자세한 내용은 을 참조하십시오 "Active IQ 포털 이벤트 활성화". 규칙 파일 업로드에 대한 자세한 내용은 을 참조하십시오 "새 Active IQ 규칙 파일을 업로드하는 중입니다".

NetApp Active IQ는 예측 분석 및 능동적 지원을 제공하여 NetApp 하이브리드 클라우드 전반에서 스토리지 시스템 운영을 최적화하는 클라우드 기반 서비스입니다. 을 참조하십시오 "NetApp Active IQ를 참조하십시오" 를 참조하십시오.

이벤트 관리 시스템 이벤트란 무엇입니까

EMS(이벤트 관리 시스템)는 ONTAP 커널의 여러 부분에서 이벤트 데이터를 수집하고 이벤트 전달 메커니즘을 제공합니다. 이러한 ONTAP 이벤트는 Unified Manager에서 EMS 이벤트로 보고할 수 있습니다. 중앙 집중식 모니터링 및 관리를 통해 이러한 EMS 이벤트를 기반으로 중요한 EMS 이벤트 및 경고 알림을 간편하게 구성할 수 있습니다.

Unified Manager에 클러스터를 추가하면 Unified Manager 주소가 클러스터에 알림 대상으로 추가됩니다. EMS 이벤트는 클러스터에서 이벤트가 발생하는 즉시 보고됩니다.

Unified Manager에서 EMS 이벤트를 수신하는 방법에는 두 가지가 있습니다.

- 특정 수의 중요한 EMS 이벤트가 자동으로 보고됩니다.
- 개별 EMS 이벤트를 구독할 수 있습니다.

Unified Manager에서 생성되는 EMS 이벤트는 이벤트가 생성된 방법에 따라 다르게 보고됩니다.

기능	자동 **EMS** 메시지	등록된 **EMS** 메시지
사용 가능한 EMS 이벤트입니다	EMS 이벤트의 하위 집합입니다	모든 EMS 이벤트
EMS가 트리거될 때 메시지 이름입니다	Unified Manager 이벤트 이름(EMS 이벤트 이름에서 변환됨)	"Error EMS Received(오류 EMS 수신)" 형식의 비특이적. 상세 메시지는 실제 EMS 이벤트의 도트 표기 형식을 제공한다
메시지가 수신되었습니다	클러스터가 검색되는 즉시	필요한 각 EMS 이벤트를 Unified Manager에 추가한 후 다음 15분 폴링 주기가 지나면
이벤트 수명 주기	다른 Unified Manager 이벤트와 동일: 새 상태, 확인됨 상태, 해결된 상태 및 폐기 상태	이벤트가 생성된 후 15분 후에 클러스터를 새로 고친 후 EMS 이벤트가 더 이상 사용되지 않습니다
Unified Manager 다운타임 동안 이벤트를 캡처합니다	예. 시스템이 시작되면 각 클러스터와 통신하여 누락된 이벤트를 획득합니다	아니요
이벤트 세부 정보	제안된 수정 조치를 ONTAP에서 직접 가져와 일관된 해결 방법을 제공합니다	이벤트 세부 정보 페이지에서 수정 조치를 사용할 수 없습니다

새로운 자동 EMS 이벤트 중 일부는 이전 이벤트가 해결되었음을 나타내는 정보 이벤트입니다. 예를 들어, "FlexGroup 구성 요소공간 상태 모두 확인" 정보 이벤트는 "FlexGroup 구성 요소에는 공간 문제가 있음" 오류 이벤트가 해결되었음을 나타냅니다. 다른 이벤트 심각도 유형과 동일한 이벤트 수명 주기를 사용하여 정보 이벤트를 관리할 수 없지만 동일한 볼륨에서 또 다른 "속도 문제" 오류 이벤트가 발생하면 이벤트가 자동으로 폐기됩니다.

Unified Manager에 자동으로 추가되는 **EMS** 이벤트입니다

다음 ONTAP EMS 이벤트가 Unified Manager에 자동으로 추가됩니다. 이러한 이벤트는 Unified Manager가 모니터링하는 모든 클러스터에서 트리거될 때 생성됩니다.

ONTAP 9.5 이상의 소프트웨어를 실행 중인 클러스터를 모니터링할 때 다음과 같은 EMS 이벤트를 사용할 수 있습니다.

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
애그리게이트 재배치에 대한 클라우드 계층 액세스가 거부되었습니다	arl.netra.ca.check.failed	집계	오류
스토리지 페일오버 중 애그리게이트 재배치에 대한 클라우드 계층 액세스가 거부되었습니다	gb.netra.ca.check.failed	집계	오류

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
FabricPool 미러 복제 재동기화가 완료되었습니다	wafl.ca.resync.complete	클러스터	오류
FabricPool 공간이 거의 찼습니다	거의 다 찼습니다	클러스터	오류
NVMe - 유예 기간 시작됨	nvmf.graceperiod.start	클러스터	경고
NVMe - 유예 기간 활성	nvmf.graceperiod.active	클러스터	경고
NVMe - 유예 기간이 만료되었습니다	nvmf.graceperiod.expired	클러스터	경고
LUN이 제거되었습니다	lun.destroy	LUN을 클릭합니다	정보
Cloud AWS MetaDataConnFail	Cloud.AWS.metadataConnFail입니다	노드	오류
클라우드 AWS IAMCredsExpired	Cloud.AWS.iamCredsExpired를 참조하십시오	노드	오류
클라우드 AWS IAMCredsInvalid	Cloud.AWS.iamCredsInvalid	노드	오류
Cloud AWS IAMCredsNotFound 를 참조하십시오	Cloud.AWS.iamCredsNotFound 를 참조하십시오	노드	오류
Cloud AWS IAMCredsNotInitialized를 참조하십시오	Cloud.AWS.iamNotInitialized를 초기화합니다	노드	정보
Cloud AWS IAMRoleInvalid	Cloud.AWS.iamRoleInvalid	노드	오류
Cloud AWS IAMRoleNotFound를 참조하십시오	Cloud.AWS.iamRoleNotFound 를 참조하십시오	노드	오류
클라우드 계층 호스트를 확인할 수 없습니다	objstore.host.unresolable을 선택합니다	노드	오류
클라우드 계층 간 클러스터 LIF가 다운되었습니다	objstore.interclusterlifDown	노드	오류

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
요청 불일치 클라우드 계층 서명	OSC.signaturemismatch.(OSCC.sign	노드	오류
NFSv4 풀 중 하나가 소진되었습니다	Nblade.nfsV4PoolExhaust	노드	심각
QoS 모니터 메모리 최대 용량	QoS.MONITOR.MEMOR Y.MEMORY	노드	오류
QoS Monitor 메모리가 잠졌습니다	QoS.MONITOR.MEMOR Y.abated를 참조하십시오	노드	정보
NVMeNS 제거	NVMeNS.destroy	네임스페이스	정보
NVMeNS 온라인	오프라인, NVMeNS	네임스페이스	정보
NVMeNS 오프라인	온라인, NVMeNS	네임스페이스	정보
데이터 보호 공간 부족	데이터 보호. 공간 부족	네임스페이스	경고
동기식 복제가 동기화되지 않았습니다	sms.status.out.of.sync	SnapMirror 관계	경고
동기식 복제가 복구되었습니다	sms.status.in.sync	SnapMirror 관계	정보
동기 복제 자동 재동기화에 실패했습니다	SMS.resync.attempt.failed 를 참조하십시오	SnapMirror 관계	오류
많은 CIFS 접속	Nblade.cifsManyAuhs를 참조하십시오	SVM	오류
최대 CIFS 접속이 초과되었습니다	nblade.cifsMaxOpenSam eFile을 참조하십시오	SVM	오류
사용자당 최대 CIFS 연결 수를 초과했습니다	Nblade.cifsMaxSessPerU srConn	SVM	오류
CIFS NetBIOS 이름이 충돌합니다	nblade.cifsNbNameConfli ctt	SVM	오류
존재하지 않는 CIFS 공유를 연결하려고 시도합니다	Nblade.cifsNoPrivShare	SVM	심각

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
CIFS 섀도우 복제본 작업이 실패했습니다	cifs.shadowcopy.실패	SVM	오류
AV 서버에서 바이러스가 발견되었습니다	Nblade.vscanVirusDetected 를 참조하십시오	SVM	오류
바이러스 검사를 위한 AV 서버 연결이 없습니다	Nblade.vscanNoScannerConn을 참조하십시오	SVM	심각
등록된 AV 서버가 없습니다	NBlade.vscanNoRegdScanner	SVM	오류
응답이 없는 AV 서버 연결	NBlade.vscanConnInactive	SVM	정보
AV 서버가 새 스캔 요청을 수락하기에 너무 사용 중입니다	NBlade.vscanConnBackPressure	SVM	오류
권한이 없는 사용자가 AV 서버를 시도합니다	Nblade.vscanBadUserPrivaccess를 참조하십시오	SVM	오류
FlexGroup 구성요소에 공간 문제가 있습니다	flexgroup.flexpodues.space.문제로 이동합니다	볼륨	오류
FlexGroup 구성 요소인 공간 상태가 모두 정상입니다	flexgroup.성분.space.status.all.ok	볼륨	정보
FlexGroup 구성 요소에는 inode 문제가 있습니다	flexgroup.constituents.have.inodes.issues	볼륨	오류
FlexGroup 구성 요소에서는 inode 상태가 모두 정상입니다	flexgroup.constituents.inodes.status.all.ok	볼륨	정보
볼륨 논리 공간이 거의 찼습니다	monitor.vol.nearFull.inc.sav	볼륨	경고
볼륨 논리적 공간이 가득 찼습니다	monitor.vol.full.inc.sav	볼륨	오류
볼륨 논리적 공간이 정상입니다	monitor.vol.one.ok.inc.sav	볼륨	정보

Unified Manager 이벤트 이름입니다	**EMS** 이벤트 이름입니다	영향을 받는 리소스입니다	**Unified Manager**의 심각도
WAFL 볼륨 자동 크기 조정 실패	wafl.vol.autoSize.fail	볼륨	오류
WAFL 볼륨 자동 크기 조정이 완료되었습니다	wafl.vol.autoSize.done	볼륨	정보
WAFL readdir 파일 작업 시간 초과	WAFL.readdir.expired를 참조하십시오	볼륨	오류

ONTAP EMS 이벤트 가입

ONTAP 소프트웨어가 설치된 시스템에서 생성되는 EMS(이벤트 관리 시스템) 이벤트를 구독하여 받을 수 있습니다. EMS 이벤트의 하위 집합이 Unified Manager에 자동으로 보고되지만 이러한 이벤트에 가입한 경우에만 추가 EMS 이벤트가 보고됩니다.

- 필요한 것 *

Unified Manager에 이미 추가된 EMS 이벤트를 자동으로 구독하지 마십시오. 동일한 문제에 대해 두 개의 이벤트를 수신할 때 혼란이 발생할 수 있습니다.

EMS 이벤트 수에 관계없이 구독할 수 있습니다. 구독하는 모든 이벤트의 유효성을 검증하며, 검증된 이벤트만 Unified Manager에서 모니터링하는 클러스터에 적용됩니다. _ONTAP 9 EMS 이벤트 카탈로그_는 지정된 버전의 ONTAP 9 소프트웨어에 대한 모든 EMS 메시지에 대한 자세한 정보를 제공합니다. 해당 이벤트 목록을 보려면 ONTAP 9 제품 설명서 페이지에서 해당 버전의 _EMS 이벤트 카탈로그_를 찾으십시오.

"ONTAP 9 제품 라이브러리"

구독하는 ONTAP EMS 이벤트에 대한 알림을 구성할 수 있으며 이러한 이벤트에 대해 실행할 사용자 지정 스크립트를 만들 수 있습니다.

구독한 ONTAP EMS 이벤트를 수신하지 않으면 클러스터의 DNS 구성에 문제가 발생하여 클러스터가 Unified Manager 서버에 도달하지 못할 수 있습니다. 이 문제를 해결하려면 클러스터 관리자가 클러스터의 DNS 구성을 수정한 다음 Unified Manager를 다시 시작해야 합니다. 이렇게 하면 보류 중인 EMS 이벤트가 Unified Manager 서버로 플러시됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 이벤트 설정 * 을 클릭합니다.
2. 이벤트 설정 페이지에서 * EMS 이벤트 가입 * 버튼을 클릭합니다.
3. EMS 이벤트 가입 대화 상자에서 가입하려는 ONTAP EMS 이벤트의 이름을 입력합니다.

   ONTAP 클러스터 쉘에서 가입할 수 있는 EMS 이벤트의 이름을 보려면 'event route show' 명령(ONTAP 9 이전) 또는 'event catalog show' 명령(ONTAP 9 이상)을 사용할 수 있습니다.

   "Active IQ Unified Manager에서 ONTAP EMS 이벤트 가입으로부터 알림을 구성 및 수신하는 방법"

4. 추가 * 를 클릭합니다.

EMS 이벤트는 가입된 EMS 이벤트 목록에 추가되지만, 해당 to Cluster 열에 추가한 EMS 이벤트에 대한 상태가 ""Unknown""으로 표시됩니다.

5. Save and Close * 를 클릭하여 EMS 이벤트 구독을 클러스터에 등록합니다.
6. EMS 이벤트 가입 * 을 다시 클릭합니다.

   추가한 EMS 이벤트에 대해 클러스터에 적용 가능한 열에 ""예"" 상태가 표시됩니다.

   상태가 "예"가 아닌 경우 ONTAP EMS 이벤트 이름의 철자를 확인합니다. 이름을 잘못 입력한 경우 잘못된 이벤트를 제거한 다음 이벤트를 다시 추가해야 합니다.

ONTAP EMS 이벤트가 발생하면 이벤트 페이지에 이벤트가 표시됩니다. Event details 페이지에서 EMS 이벤트에 대한 세부 정보를 볼 이벤트를 선택할 수 있다. 이벤트 처리를 관리하거나 이벤트에 대한 알림을 생성할 수도 있습니다.

이벤트 수신 시 발생하는 현상

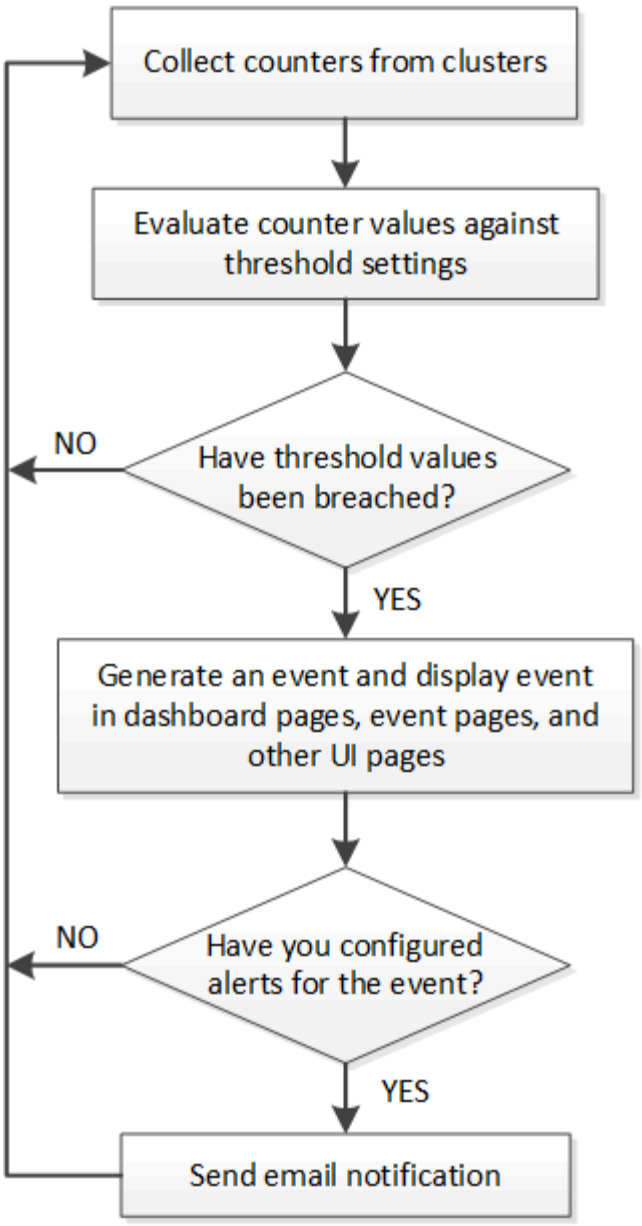
Unified Manager에서 이벤트를 수신하면 대시보드 페이지, 이벤트 관리 인벤토리 페이지, 클러스터/성능 페이지의 요약 및 탐색기 탭, 개체별 인벤토리 페이지(예: 볼륨/상태 인벤토리 페이지)에 표시됩니다.

Unified Manager에서 동일한 클러스터 구성 요소에 대해 같은 이벤트가 여러 번 지속적으로 발생하는 것을 감지한 경우 모든 경우를 별도의 이벤트가 아닌 단일 이벤트로 처리합니다. 이벤트 지속 시간이 증가하여 이벤트가 여전히 활성 상태임을 나타냅니다.

경고 설정 페이지의 설정 구성 방법에 따라 다른 사용자에게 이러한 이벤트에 대해 알릴 수 있습니다. 알림으로 인해 다음 작업이 시작됩니다.

- 이벤트에 대한 e-메일을 모든 Unified Manager Administrator 사용자에게 보낼 수 있습니다.
- 이벤트를 추가 e-메일 수신자에게 보낼 수 있습니다.
- SNMP 트랩을 트랩 수신기로 보낼 수 있습니다.
- 작업을 수행하기 위해 사용자 지정 스크립트를 실행할 수 있습니다.

이 워크플로는 다음 다이어그램에 표시됩니다.



이벤트 및 이벤트 세부 정보 보기

Unified Manager에서 트리거된 이벤트에 대한 세부 정보를 확인하여 수정 조치를 취할 수 있습니다. 예를 들어, 상태 이벤트 Volume Offline이 있는 경우 해당 이벤트를 클릭하여 세부 정보를 확인하고 수정 조치를 수행할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트 세부 정보에는 이벤트 소스, 이벤트 원인 및 이벤트와 관련된 메모 등의 정보가 포함됩니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.

   기본적으로 모든 활성 이벤트 보기에는 영향 수준의 인시던트 또는 위험이 있는 이전 7일 동안 생성된 새 이벤트 및

확인된(활성) 이벤트가 표시됩니다.

2. 용량 이벤트 또는 성능 이벤트와 같은 특정 이벤트 범주를 보려면 * View * 를 클릭하고 이벤트 유형 메뉴에서 선택합니다.
3. 세부 정보를 보려는 이벤트 이름을 클릭합니다.

   이벤트 세부 정보가 이벤트 세부 정보 페이지에 표시됩니다.

할당되지 않은 이벤트 보기

할당되지 않은 이벤트를 확인한 다음 각 이벤트를 해결할 수 있는 사용자에게 할당할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.

   기본적으로 새 이벤트와 확인된 이벤트는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. Filters * 창에서 * Assigned to * 영역에서 * Unassigned * 필터 옵션을 선택합니다.

이벤트 확인 및 해결

이벤트 생성 문제에 대한 작업을 시작하기 전에 이벤트 확인을 통해 반복 경고 알림을 계속 받지 않도록 해야 합니다. 특정 이벤트에 대해 수정 조치를 취한 후 해당 이벤트를 '해결됨'으로 표시해야 합니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여러 이벤트를 동시에 확인하고 해결할 수 있습니다.

정보 이벤트는 승인할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.
2. 이벤트 목록에서 다음 작업을 수행하여 이벤트를 확인합니다.

원하는 작업	수행할 작업...
단일 이벤트를 확인하고 해결된 것으로 표시합니다	a. 이벤트 이름을 클릭합니다. b. 이벤트 세부 정보 페이지에서 이벤트의 원인을 확인합니다. c. 확인 * 을 클릭합니다. d. 적절한 수정 조치를 취하십시오. e. 해결됨으로 표시 * 를 클릭합니다.
여러 이벤트를 확인하고 해결된 것으로 표시합니다	a. 각 이벤트 세부 정보 페이지에서 이벤트의 원인을 확인합니다. b. 이벤트를 선택합니다. c. 확인 * 을 클릭합니다. d. 적절한 수정 조치를 취하십시오. e. 해결됨으로 표시 * 를 클릭합니다.

이벤트를 Resolved 로 표시하면 이벤트가 Resolved 이벤트 목록으로 이동합니다.

3. * 선택 사항 *: * 참고 및 업데이트 * 영역에서 이벤트 처리 방법에 대한 메모를 추가한 다음 * 게시 * 를 클릭합니다.

특정 사용자에게 이벤트 할당

할당되지 않은 이벤트를 사용자 자신 또는 원격 사용자를 포함한 다른 사용자에게 할당할 수 있습니다. 필요한 경우 할당된 이벤트를 다른 사용자에게 재할당할 수 있습니다. 예를 들어, 스토리지 개체에서 자주 문제가 발생하는 경우 이러한 문제에 대한 이벤트를 해당 개체를 관리하는 사용자에게 할당할 수 있습니다.

- 필요한 것 *
- 사용자 이름과 이메일 ID가 올바르게 구성되어 있어야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.
2. 이벤트 관리 * 인벤토리 페이지에서 할당할 하나 이상의 이벤트를 선택합니다.
3. 다음 옵션 중 하나를 선택하여 이벤트를 할당합니다.

이벤트를 다음에 할당하려면...	다음을 수행하십시오.
직접	Assign to * > * Me * 를 클릭합니다.

이벤트를 다음에 할당하려면...	다음을 수행하십시오.
다른 사용자	a. Assign to * > * another user * 를 클릭합니다. b. 소유자 할당 대화 상자에서 사용자 이름을 입력하거나 드롭다운 목록에서 사용자를 선택합니다. c. 할당 * 을 클릭합니다. 사용자에게 이메일 알림이 전송됩니다. 사용자 이름을 입력하지 않거나 드롭다운 목록에서 사용자를 선택하고 * 배정 * 을 클릭하면 이벤트가 미할당 상태로 유지됩니다.

원치 않는 이벤트 비활성화

모든 이벤트는 기본적으로 활성화됩니다. 사용자 환경에서 중요하지 않은 이벤트에 대한 알림이 발생하지 않도록 이벤트를 전역적으로 비활성화할 수 있습니다. 알림 수신을 다시 시작하려는 경우 비활성화된 이벤트를 활성화할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트를 사용하지 않도록 설정하면 시스템에서 이전에 생성된 이벤트가 사용되지 않는 것으로 표시되고 이러한 이벤트에 대해 구성된 알림이 트리거되지 않습니다. 비활성화된 이벤트를 활성화하면 다음 모니터링 주기부터 이러한 이벤트에 대한 알림이 생성됩니다.

개체에 대한 이벤트(예: "vol offline" 이벤트)를 해제한 다음 나중에 이 이벤트를 사용하면 Unified Manager는 이벤트가 비활성 상태일 때 오프라인 상태인 개체에 대한 새 이벤트를 생성하지 않습니다. Unified Manager는 이벤트가 다시 활성화된 후 오브젝트 상태가 변경된 경우에만 새 이벤트를 생성합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 이벤트 설정 * 을 클릭합니다.
2. 이벤트 설정 * 페이지에서 다음 옵션 중 하나를 선택하여 이벤트를 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
이벤트를 비활성화합니다	a. 비활성화 * 를 클릭합니다. b. 이벤트 사용 안 함 대화 상자에서 이벤트 심각도를 선택합니다. c. 이벤트 일치 열에서 이벤트 심각도에 따라 비활성화할 이벤트를 선택한 다음 오른쪽 화살표를 클릭하여 해당 이벤트를 이벤트 사용 안 함 열로 이동합니다. d. 저장 후 닫기 * 를 클릭합니다. e. 사용하지 않도록 설정한 이벤트가 이벤트 설정 페이지의 목록 보기에 표시되는지 확인합니다.
이벤트 활성화	a. 활성화할 이벤트 또는 이벤트의 확인란을 선택합니다. b. 사용 * 을 클릭합니다.

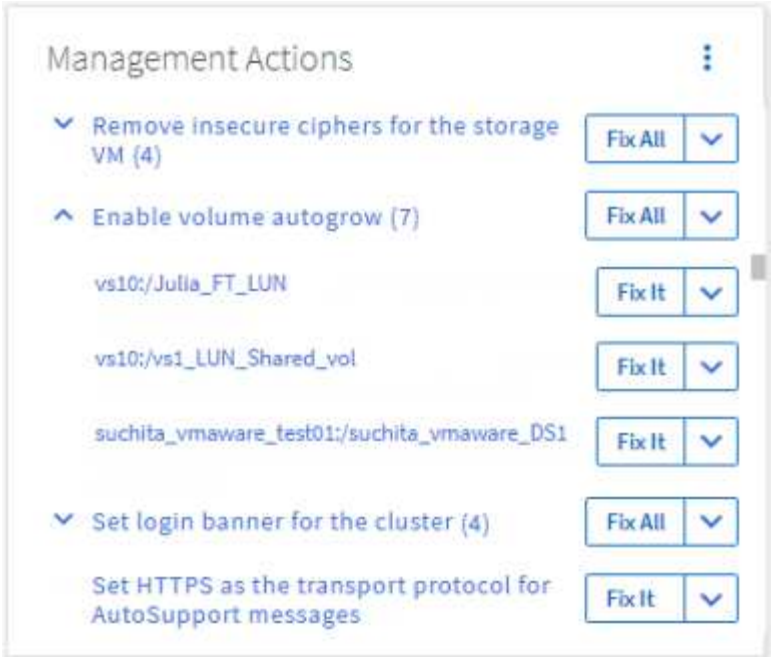
Unified Manager 자동 조정을 사용하여 문제 해결

Unified Manager에서 철저히 진단하고 * Fix it * 버튼을 사용하여 단일 해결책을 제공할 수 있는 특정 이벤트가 있습니다. 사용 가능한 경우 이러한 해결 방법은 Dashboard, Event Details 페이지 및 왼쪽 탐색 메뉴의 Workload Analysis 선택 항목에 표시됩니다.

대부분의 이벤트는 이벤트 세부 정보 페이지에 표시될 수 있는 다양한 해결 방법이 있으므로 ONTAP System Manager 또는 ONTAP CLI를 사용하여 최상의 솔루션을 구현할 수 있습니다. Unified Manager에서 문제를 해결할 수 있는 단일 해결책이 있다고 판단하여 ONTAP CLI 명령을 사용하여 해결할 수 있다고 판단한 경우 * Fix it * 작업을 사용할 수 있습니다.

단계

1. 대시보드 * 에서 수정할 수 있는 이벤트를 보려면 * 대시보드 * 를 클릭합니다.



2. Unified Manager로 해결할 수 있는 문제를 해결하려면 * Fix it * 버튼을 클릭합니다. 여러 개체에 존재하는 문제를 해결하려면 * 모두 수정 * 버튼을 클릭합니다.

자동 수정 기능으로 해결할 수 있는 문제에 대한 자세한 내용은 을 참조하십시오 "Unified Manager로 해결할 수 있는 문제".

Active IQ 이벤트 보고 활성화 및 비활성화

Active IQ 플랫폼 이벤트는 기본적으로 Unified Manager 사용자 인터페이스에 생성되고 표시됩니다. 이러한 이벤트가 너무 "노이즈"이거나 Unified Manager에서 이러한 이벤트를 보고 싶지 않은 경우, 이러한 이벤트가 생성되지 않도록 설정할 수 있습니다. 이러한 알림 수신을 다시 시작하려면 나중에 해당 알림을 사용하도록 설정할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

이 기능을 사용하지 않도록 설정하면 Unified Manager에서 Active IQ 플랫폼 이벤트 수신을 즉시 중지합니다.

이 기능을 사용하도록 설정하면 Unified Manager가 클러스터 시간대를 기준으로 자정 직후 Active IQ 플랫폼 이벤트를 수신하기 시작합니다. 시작 시간은 Unified Manager가 각 클러스터에서 AutoSupport 메시지를 수신하는 시점을 기준으로 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 기능 설정 * 을 클릭합니다.
2. 기능 설정 * 페이지에서 다음 옵션 중 하나를 선택하여 Active IQ 플랫폼 이벤트를 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
Active IQ 플랫폼 이벤트를 비활성화합니다	Active IQ 포털 이벤트 * 패널에서 슬라이더 버튼을 왼쪽으로 이동합니다.
Active IQ 플랫폼 이벤트를 활성화합니다	Active IQ 포털 이벤트 * 패널에서 슬라이더 버튼을 오른쪽으로 이동합니다.

새 **Active IQ** 규칙 파일을 업로드하는 중입니다

Unified Manager는 새로운 Active IQ 이벤트(규칙) 파일을 자동으로 확인하고 새로운 규칙이 있을 때 새 파일을 다운로드합니다. 그러나 외부 네트워크에 액세스할 수 없는 사이트에서는 규칙 파일을 수동으로 업로드해야 합니다.

Active IQ 규칙은 CA(Config Advisor) 보안 규칙이라고도 합니다.

네트워크에 연결하지 않고 Unified Manager를 사이트의 특정 릴리즈로 설치 또는 업그레이드하는 경우 번들 Active IQ 규칙을 자동으로 업로드할 수 있습니다. 하지만 NetApp Support 사이트에서 매월 약 한 번 새로운 규칙 파일을 다운로드하여 업데이트된 이벤트가 생성되고 스토리지 시스템이 최적의 상태로 계속 작동하도록 하는 것이 좋습니다.

- 필요한 것 *
- Active IQ 포털 이벤트 보고를 활성화해야 합니다. 이 기능은 기본적으로 활성화되어 있습니다. 자세한 내용은 을 참조하십시오 "Active IQ 포털 이벤트 활성화".
- NetApp Support 사이트에서 규칙 파일을 다운로드해야 합니다.

  규칙 파일은 다음 위치에 있습니다. https://mysupport.netapp.com/api/content-service/staticcontents/content/public/tools/unifiedmanager/ca/secure_rules.zip

단계

1. 네트워크 액세스가 가능한 컴퓨터에서 NetApp Support 사이트로 이동하여 현재 규칙 파일 '.zip'을 다운로드합니다.

   번들 규칙 패키지에는 규칙 저장소, 데이터 소스 및 NetApp KB 문서가 포함되어 있습니다.

   Windows 시스템의 경우 네트워크에 연결되지 않은 사이트에서 NetApp KB 문서가 기본적으로 설치 프로그램과 함께 번들로 제공되지 않습니다. 지원 사이트에서 _secure_rules.zip_파일을 다운로드하고 업로드하여 모든 규칙에 대한 KB 문서를 볼 수 있습니다.

2. 보안 영역으로 가져올 수 있는 일부 미디어로 규칙 파일을 전송한 다음 보안 영역의 시스템에 복사합니다.
3. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 이벤트 설정 * 을 클릭합니다.
4. 이벤트 설정 * 페이지에서 * 규칙 업로드 * 버튼을 클릭합니다.
5. Upload Rules * (규칙 업로드 *) 대화 상자에서 다운로드한 규칙 '.zip' 파일을 찾아 선택하고 * Upload * (업로드 *)를 클릭합니다.

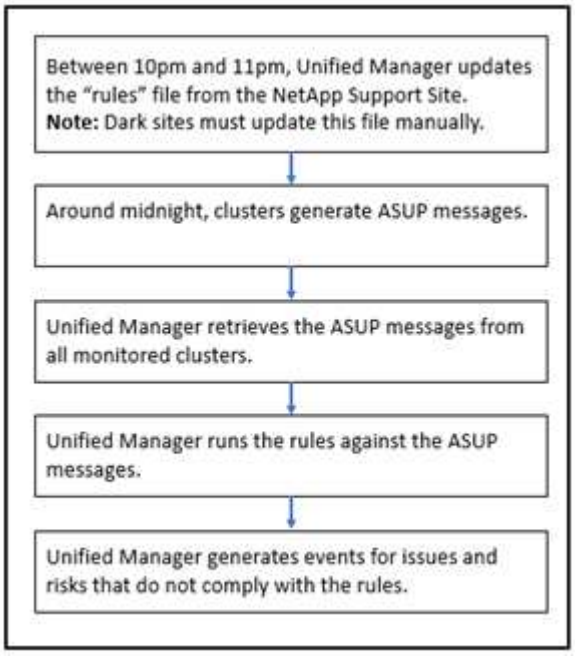
   이 과정은 몇 분 정도 걸릴 수 있습니다.

규칙 파일의 압축이 Unified Manager 서버에서 풀립니다. 자정 이후 관리 클러스터에서 AutoSupport 파일이 생성되면 Unified Manager에서 규칙 파일에 대해 클러스터를 확인하고 필요에 따라 새로운 위험 및 인시던트 이벤트를 생성합니다.

자세한 내용은 다음 기술 자료(KB) 문서를 참조하십시오. "Active IQ Unified Manager에서 AIQCASecure 규칙을 수동으로 업데이트하는 방법".

Active IQ 플랫폼 이벤트 생성 방법

Active IQ 플랫폼 인시던트 및 위험은 다음 다이어그램에 표시된 대로 Unified Manager 이벤트로 변환됩니다.

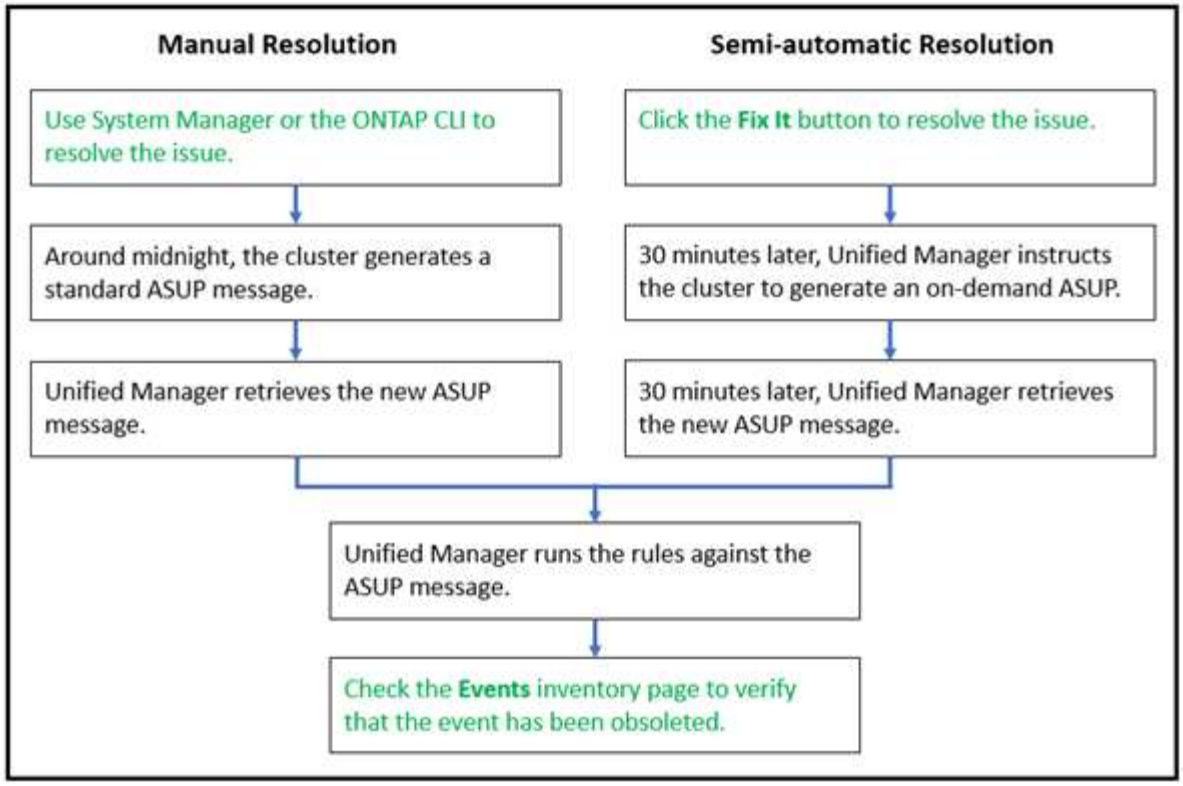


보시다시피 Active IQ 플랫폼에서 컴파일된 규칙 파일은 최신 상태로 유지되고, 클러스터 AutoSupport 메시지가 매일 생성되고, Unified Manager에서 매일 이벤트 목록을 업데이트합니다.

Active IQ 플랫폼 이벤트 해결

Active IQ 플랫폼 문제 및 위험은 해결을 위해 다른 사용자에게 할당할 수 있고 사용 가능한 상태가 동일하므로 다른 Unified Manager 이벤트와 비슷합니다. 그러나 * Fix it * 버튼을 사용하여 이러한 유형의 이벤트를 해결할 경우 몇 시간 내에 해결 여부를 확인할 수 있습니다.

다음 다이어그램에서는 Active IQ 플랫폼에서 생성된 이벤트를 확인할 때 취해야 하는 조치(녹색)와 유니파이드 관리자가 수행하는 조치(검정색)를 보여 줍니다.



수동 해결을 수행할 때 문제를 해결하려면 System Manager 또는 ONTAP 명령줄 인터페이스에 로그인해야 합니다. 자정에만 클러스터에서 새 AutoSupport 메시지가 생성된 후에만 문제를 확인할 수 있습니다.

Fix it* 단추를 사용하여 반자동 해결을 수행할 때 몇 시간 내에 수정이 성공했는지 확인할 수 있습니다.

이벤트 보존 설정을 구성하는 중입니다

이벤트가 자동으로 삭제되기 전에 Unified Manager 서버에 유지되는 기간(월)을 지정할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

6개월 이상 이벤트를 보존하면 서버 성능에 영향을 줄 수 있으며 권장하지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 데이터 보존 * 을 클릭합니다.
2. Data Retention * 페이지의 Event Retention 영역에서 슬라이더를 선택하고 이벤트를 보존할 개월 수로 이동한 다음 * Save * 를 클릭합니다.

Unified Manager의 유지 관리 기간은 얼마입니까

Unified Manager 유지 관리 창을 정의하여 클러스터 유지 관리를 예약하고 원치 않는 알림이 쏟아지는 것을 원치 않는 경우 특정 기간 동안 이벤트와 알림을 표시하지 않을 수 있습니다.

유지 보수 기간이 시작되면 "Object Maintenance Window Started" 이벤트가 이벤트 관리 인벤토리 페이지에

게시됩니다. 이 이벤트는 유지 보수 기간이 종료되면 자동으로 폐기됩니다.

유지 관리 창에서는 해당 클러스터의 모든 개체와 관련된 이벤트가 여전히 생성되지만 UI 페이지에는 표시되지 않으며 이러한 이벤트에 대한 알림이나 다른 유형의 알림도 전송되지 않습니다. 하지만 이벤트 관리 인벤토리 페이지에서 보기 옵션 중 하나를 선택하면 유지보수 윈도우 동안 모든 스토리지 개체에 대해 생성된 이벤트를 볼 수 있습니다.

나중에 시작하도록 유지 관리 창을 예약하고, 예약된 유지 관리 창의 시작 및 종료 시간을 변경하고, 예약된 유지 관리 창을 취소할 수 있습니다.

클러스터 이벤트 알림을 사용하지 않도록 유지 관리 창을 예약하는 중입니다

예를 들어, 클러스터를 업그레이드하거나 노드 중 하나를 이동하기 위해 클러스터에 대해 계획된 다운타임이 있는 경우 Unified Manager 유지보수 윈도우를 예약하여 해당 기간 동안 일반적으로 생성되는 이벤트 및 알림을 억제할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

유지보수 윈도우 중에 해당 클러스터의 모든 오브젝트와 관련된 이벤트는 계속 생성되지만 이벤트 페이지에는 표시되지 않으며 이러한 이벤트에 대한 경고 또는 기타 유형의 알림은 전송되지 않습니다.

유지보수 시간에 입력하는 시간은 Unified Manager 서버의 시간을 기준으로 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.
2. 클러스터의 * 유지보수 모드 * 열에서 슬라이더 버튼을 선택하고 오른쪽으로 이동합니다.

   캘린더 창이 표시됩니다.

3. 유지 관리 창의 시작 및 종료 날짜와 시간을 선택하고 * 적용 * 을 클릭합니다.

   슬라이더 단추 옆에 "예약됨" 메시지가 나타납니다.

시작 시간에 도달하면 클러스터가 유지보수 모드로 전환되고 "Object Maintenance Window Started" 이벤트가 생성됩니다.

예약된 유지 관리 창 변경 또는 취소

Unified Manager 유지보수 윈도우를 향후 발생하도록 구성한 경우, 시작 및 종료 시간을 변경하거나 유지보수 윈도우 발생을 취소할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

현재 실행 중인 유지보수 윈도우를 취소하면 예약된 유지보수 윈도우 종료 시간 전에 클러스터 유지보수를 완료하고 클러스터에서 이벤트 및 경고를 다시 수신하려는 경우에 유용합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 클러스터 설정 * 을 클릭합니다.
2. 클러스터의 * 유지보수 모드 * 열에서 다음을 수행합니다.

원하는 작업	이 단계를 수행합니다...
예약된 유지 보수 기간의 기간을 변경합니다	a. 슬라이더 단추 옆에 있는 "예약됨" 텍스트를 클릭합니다. b. 시작 및/또는 종료 날짜와 시간을 변경하고 * 적용 * 을 클릭합니다.
활성 유지 관리 창의 길이를 확장합니다	a. 슬라이더 단추 옆에 있는 "Active(활성)" 텍스트를 클릭합니다. b. 종료 날짜 및 시간을 변경하고 * 적용 * 을 클릭합니다.
예약된 유지 관리 창을 취소합니다	슬라이더 버튼을 선택하고 왼쪽으로 이동합니다.
활성 유지 보수 창을 취소합니다	슬라이더 버튼을 선택하고 왼쪽으로 이동합니다.

유지보수 윈도우 중 발생한 이벤트 보기

필요한 경우 Unified Manager 유지보수 윈도우 동안 모든 스토리지 오브젝트에 대해 생성된 이벤트를 볼 수 있습니다. 대부분의 이벤트는 유지 보수 기간이 완료되고 모든 시스템 리소스가 백업 및 실행되면 Obsolete 상태로 표시됩니다.

- 필요한 것 *

이벤트를 사용하려면 먼저 하나 이상의 유지보수 윈도우를 완료해야 합니다.

유지보수 기간 동안 발생한 이벤트는 기본적으로 이벤트 관리 인벤토리 페이지에 나타나지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 * 를 클릭합니다.

   기본적으로 모든 활성(신규 및 확인됨) 이벤트가 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 창에서 * 유지 관리 중에 생성된 모든 이벤트 * 옵션을 선택합니다.

   모든 유지 보수 기간 세션 및 모든 클러스터에서 지난 7일 동안 트리거된 이벤트 목록이 표시됩니다.

3. 단일 클러스터에 대한 여러 유지 관리 기간이 있는 경우 * Triggered Time * 캘린더 아이콘을 클릭하고 보려는 유지 관리 창 이벤트의 기간을 선택할 수 있습니다.

호스트 시스템 리소스 이벤트 관리

Unified Manager에는 Unified Manager가 설치된 호스트 시스템의 리소스 문제를 모니터링하는 서비스가 포함되어 있습니다. 사용 가능한 디스크 공간 부족 또는 호스트 시스템의 메모리 부족과

같은 문제는 UI 상단에 배너 메시지로 표시되는 관리 스테이션 이벤트를 트리거할 수 있습니다.

관리 스테이션 이벤트는 Unified Manager가 설치된 호스트 시스템의 문제를 나타냅니다. 관리 스테이션 문제의 예로는 호스트 시스템에서 부족한 디스크 공간, Unified Manager가 정기적인 데이터 수집 주기를 누락한 경우, 다음 컬렉션 폴링이 시작되었으므로 통계 분석의 완료되지 않은 경우 또는 늦게 완료되는 경우 등이 있습니다.

다른 모든 Unified Manager 이벤트 메시지와 달리 이러한 특정 관리 스테이션 경고 및 중요 이벤트는 배너 메시지에 표시됩니다.

단계

1. 관리 스테이션 이벤트 정보를 보려면 다음 작업을 수행하십시오.

원하는 작업	수행할 작업...
이벤트 세부 정보를 봅니다	이벤트 배너를 클릭하면 문제에 대한 권장 솔루션이 포함된 이벤트 세부 정보 페이지가 표시됩니다.
모든 관리 스테이션 이벤트를 봅니다	a. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다. b. 이벤트 관리 인벤토리 페이지의 필터 창에서 소스 유형 목록에서 관리 스테이션 상자를 클릭합니다.

이벤트에 대한 자세한 정보

이벤트에 대한 개념을 이해하면 클러스터 및 클러스터 객체를 효율적으로 관리하고 경고를 적절하게 정의할 수 있습니다.

이벤트 상태 정의

이벤트의 상태는 적절한 수정 조치가 필요한지 여부를 식별하는 데 도움이 됩니다. 이벤트는 New, Acknowledged, Resolved 또는 Obsolete가 될 수 있습니다. 새 이벤트와 승인된 이벤트 모두 활성 이벤트로 간주됩니다.

이벤트 상태는 다음과 같습니다.

- * 신규 *

  새 이벤트의 상태입니다.

- * 확인됨 *

  사용자가 이벤트를 승인했을 때의 상태입니다.

- * 해결됨 *

  해결됨으로 표시된 이벤트의 상태입니다.

- * 사용되지 않음 *

  자동으로 수정되거나 이벤트의 원인이 더 이상 유효하지 않은 경우의 이벤트 상태입니다.

더 이상 사용되지 않는 이벤트를 확인하거나 확인할 수 없습니다.

이벤트의 여러 가지 상태 예

다음 예제에서는 수동 및 자동 이벤트 상태의 변화를 보여 줍니다.

이벤트 클러스터에 연결할 수 없음 이 트리거되면 이벤트 상태는 새로 만들기 입니다. 이벤트를 확인하면 이벤트 상태가 확인으로 변경됩니다. 적절한 수정 조치를 취했다면 해당 이벤트를 '해결됨'으로 표시해야 합니다. 그런 다음 이벤트 상태가 Resolved 로 변경됩니다.

정전 때문에 Cluster Not Reachable 이벤트가 발생한 경우 전원이 복구되면 클러스터가 관리자 개입 없이 작동을 시작합니다. 따라서 Cluster Not Reachable 이벤트가 더 이상 유효하지 않으며 이벤트 상태가 다음 모니터링 주기에서 Obsolete로 변경됩니다.

이벤트가 Obsolete 또는 Resolved 상태인 경우 Unified Manager에서 알림을 보냅니다. 알림의 전자 메일 제목 줄 및 전자 메일 콘텐츠는 이벤트 상태에 대한 정보를 제공합니다. SNMP 트랩에는 이벤트 상태에 대한 정보도 포함되어 있습니다.

이벤트 심각도 유형에 대한 설명입니다

각 이벤트는 심각도 유형과 연관되어 있으므로 즉각적인 수정 조치가 필요한 이벤트의 우선순위를 지정하는 데 도움이 됩니다.

- * 심각 *

  수정 조치를 즉시 취하지 않으면 서비스가 중단될 수 있는 문제가 발생했습니다.

  성능에 중요한 이벤트는 사용자 정의 임계값에서만 전송됩니다.

- * 오류 *

  이벤트 소스가 여전히 수행되고 있지만 서비스 중단을 방지하기 위해 수정 조치가 필요합니다.

- * 경고 *

  이벤트 소스에서 사용자가 인식해야 하는 상황이 발생했거나 클러스터 개체의 성능 카운터가 정상 범위를 벗어났고 모니터링하여 심각도에 도달하지 않았는지 확인해야 합니다. 이러한 심각도 때문에 서비스가 중단되지 않으며 즉각적인 수정 조치가 필요하지 않을 수 있습니다.

  성능 경고 이벤트는 사용자 정의, 시스템 정의 또는 동적 임계값에서 전송됩니다.

- * 정보 *

  이 이벤트는 새 개체가 검색되거나 사용자 작업이 수행될 때 발생합니다. 예를 들어, 스토리지 객체가 삭제되거나 구성이 변경된 경우 심각도 유형 정보가 있는 이벤트가 생성됩니다.

  정보 이벤트는 구성 변경을 감지하면 ONTAP에서 직접 전송됩니다.

이벤트 영향 수준에 대한 설명입니다

각 이벤트는 영향 수준(인시던트, 위험, 이벤트 또는 업그레이드)과 연결되어 즉각적인 수정 조치가 필요한 이벤트의 우선 순위를 지정하는 데 도움이 됩니다.

- * 사건 *

  인시던트는 클러스터에서 클라이언트에 데이터 제공을 중지하고 데이터를 저장하기 위한 공간이 부족한 상황을 말합니다. 사고의 영향 수준이 가장 심각한 이벤트는 입니다. 서비스 중단을 방지하기 위해 즉각적인 수정 조치를 취해야 합니다.

- * 위험 *

  리스크는 클러스터에서 클라이언트에 데이터 제공을 중지하고 데이터를 저장하기 위한 공간이 부족하게 되는 일련의 이벤트입니다. 위험 수준이 영향을 미치는 이벤트는 서비스 중단을 일으킬 수 있습니다. 수정 조치가 필요할 수 있습니다.

- * 이벤트 *

  이벤트는 스토리지 객체 및 해당 속성의 상태 또는 상태 변경입니다. 이벤트의 영향 레벨이 있는 이벤트는 정보를 제공할 뿐만 아니라 수정 조치가 필요하지 않습니다.

- * 업그레이드 *

  업그레이드 이벤트는 Active IQ 플랫폼에서 보고되는 특정 유형의 이벤트입니다. 이러한 이벤트는 문제 해결을 위해 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어(보안 권장 사항)를 업그레이드해야 하는 문제를 식별합니다. 이러한 문제 중 일부에 대해 즉각적인 수정 조치를 수행해야 하는 경우도 있지만, 다른 문제로 인해 예정된 다음 유지 관리 작업이 완료될 때까지 기다릴 수 있습니다.

이벤트 영향 영역에 대한 설명입니다

이벤트는 6가지 영향 영역(가용성, 용량, 구성, 성능, 보호, 및 보안)을 통해 귀하가 책임을 지는 이벤트의 유형에 집중할 수 있습니다.

- * 가용성 *

  가용성 이벤트는 스토리지 객체가 오프라인 상태가 되거나, 프로토콜 서비스가 다운되거나, 스토리지 페일오버 문제가 발생하거나, 하드웨어 문제가 발생한 경우 이를 알립니다.

- * 용량 *

  용량 이벤트는 애그리게이트, 볼륨, LUN 또는 네임스페이스가 크기 임계값에 도달하거나 도달하지 않았거나 사용자 환경에서 증가 속도가 비정상적인 경우 이를 알려줍니다.

- * 구성 *

  구성 이벤트는 스토리지 객체의 검색, 삭제, 추가, 제거 또는 이름을 알려 줍니다. 구성 이벤트는 이벤트 및 정보의 심각도 수준에 영향을 줍니다.

- * 성능 *

  성능 이벤트는 클러스터에서 리소스, 구성 또는 활동 상태에 대해 알림을 발생하므로, 모니터링되는 스토리지

개체의 데이터 스토리지 입력 또는 검색 속도에 악영향을 미칠 수 있습니다.

- * 보호 *

  보호 이벤트는 SnapMirror 관계, 대상 용량 문제, SnapVault 관계 문제 또는 보호 작업 관련 문제와 관련된 사고 또는 위험을 알려줍니다. 2차 볼륨 및 보호 관계를 호스팅하는 모든 ONTAP 오브젝트(특히 애그리게이트, 볼륨 및 SVM)는 보호 영향 영역에서 분류됩니다.

- * 보안 *

  보안 이벤트는 에 정의된 매개 변수를 기반으로 ONTAP 클러스터, SVM(스토리지 가상 머신) 및 볼륨의 보안 수준을 알려줍니다 "ONTAP 9에 대한 NetApp 보안 강화 가이드".

  또한 이 영역에는 Active IQ 플랫폼에서 보고된 업그레이드 이벤트가 포함됩니다.

개체 상태 계산 방법

개체 상태는 현재 New 또는 Acknowledged 상태를 보유한 가장 심각한 이벤트에 의해 결정됩니다. 예를 들어, 개체 상태가 Error 인 경우 개체의 이벤트 중 하나에 오류 심각도 유형이 있습니다. 수정 조치를 취하면 이벤트 상태가 해결됨 으로 이동합니다.

동적 성능 이벤트 차트 세부 정보

동적 성능 이벤트의 경우 이벤트 세부 정보 페이지의 시스템 진단 섹션에 경합 중인 클러스터 구성 요소의 사용 또는 지연 시간이 가장 긴 최상위 워크로드가 나열됩니다.

성능 통계는 이벤트가 마지막으로 분석된 시간까지 성능 이벤트가 감지된 시간을 기준으로 합니다. 또한 차트에는 경합 중인 클러스터 구성 요소에 대한 기간별 성능 통계도 표시됩니다.

예를 들어, 구성 요소의 사용률이 높은 워크로드를 식별하여 사용률이 낮은 구성 요소로 이동할 워크로드를 결정할 수 있습니다. 워크로드를 이동하면 현재 구성 요소에 대한 작업 양이 줄어들고 구성 요소의 경합이 발생할 수 있습니다. 이 섹션의 맨 위에는 이벤트가 감지되어 마지막으로 분석된 시간 및 날짜 범위가 있습니다. 활성 이벤트(새 이벤트 또는 승인된 이벤트)의 경우 마지막으로 분석된 시간이 업데이트됩니다.

지연 시간 및 활동 차트에는 커서를 차트 위에 놓으면 최상위 워크로드의 이름이 표시됩니다. 차트 오른쪽의 워크로드 유형 메뉴를 클릭하면 *Sharks*, *bullies*, 또는 *inuss* 등의 이벤트 역할에 따라 워크로드를 정렬할 수 있으며 경합 중인 클러스터 구성 요소의 지연 시간 및 사용 현황에 대한 세부 정보를 표시합니다. 실제 값을 예상 값과 비교하여 워크로드가 예상 지연 시간 또는 사용 범위를 벗어난 시점을 확인할 수 있습니다. 자세한 내용은 을 참조하십시오 "Unified Manager에서 모니터링하는 워크로드의 유형입니다".

> 지연 시간이 최대 편차로 정렬되면 사용자 정의 워크로드에만 지연 시간이 적용되므로 시스템 정의 워크로드가 표에 표시되지 않습니다. 지연 시간이 매우 짧은 워크로드는 테이블에 표시되지 않습니다.

동적 성능 임계값에 대한 자세한 내용은 를 참조하십시오 "동적 성능 임계값에서 이벤트 분석".

Unified Manager에서 워크로드의 순위를 결정하고 정렬 순서를 결정하는 방법에 대한 자세한 내용은 을 참조하십시오 "Unified Manager에서 이벤트에 대한 성능 영향을 확인하는 방법".

그래프의 데이터는 이벤트를 마지막으로 분석하기 전에 24시간 동안의 성능 통계를 보여줍니다. 각 워크로드의 실제 값과 예상 값은 워크로드가 발생한 시간을 기준으로 합니다. 예를 들어, 이벤트가 감지된 후 워크로드가 이벤트에 포함될 수 있으므로 이벤트 감지 시 성능 통계가 값과 일치하지 않을 수 있습니다. 기본적으로 워크로드는 지연 시간의 최대

(최고) 편차별로 정렬됩니다.

Unified Manager에서는 최대 30일간 5분간 기간별 성능 및 이벤트 데이터를 유지할 수 있으므로, 30일이 경과되지 않은 경우 성능 데이터가 표시되지 않습니다.

- * 워크로드 정렬 열 *
  - * 지연 시간 차트 *

    마지막 분석 동안 워크로드의 지연 시간에 이벤트가 미치는 영향을 표시합니다.
  - * 구성 요소 사용 열 *

    경합하는 클러스터 구성 요소의 워크로드 사용에 대한 세부 정보를 표시합니다. 그래프에서 실제 사용량은 파란색 선입니다. 빨간색 막대는 감지 시간부터 마지막으로 분석된 시간까지 이벤트 지속 시간을 강조 표시합니다. 자세한 내용은 을 참조하십시오 "워크로드 성능 측정 값".

    네트워크 구성요소의 경우, 네트워크 성능 통계는 클러스터 외부의 활동에서 얻을 수 있기 때문에 이 열은 표시되지 않습니다.
  - * 구성 요소 사용 *

    QoS 정책 그룹 구성 요소에 대한 네트워크 처리, 데이터 처리 및 집계 구성 요소 또는 작업 내역(백분율)의 사용률 기록을 표시합니다. 네트워크 또는 상호 연결 구성 요소에 대한 차트는 표시되지 않습니다. 통계를 가리켜 특정 시점의 사용 통계를 볼 수 있습니다.
  - * 총 쓰기 MB/s 기록 *

    MetroCluster 리소스 구성 요소의 경우 MetroCluster 구성에서 파트너 클러스터로 미러링되는 모든 볼륨 워크로드의 총 쓰기 처리량(MB/sec)을 표시합니다.
  - * 이벤트 기록 *

    경합이 발생한 부품의 과거 이벤트를 나타내기 위해 빨간색 음영으로 표시된 선을 표시합니다. 사용되지 않는 이벤트의 경우 선택한 이벤트가 감지되기 전과 해결된 이후에 발생한 이벤트가 차트에 표시됩니다.

Unified Manager에서 구성 변경이 감지되었습니다

Unified Manager는 클러스터의 구성 변경 사항을 모니터링하여 변경이 성능 이벤트의 원인인지 또는 기여 원인인지 여부를 결정합니다. 성능 탐색기 페이지에 변경 이벤트 아이콘(●)을 클릭하여 변경이 감지된 날짜와 시간을 표시합니다.

성능 탐색기 페이지와 워크로드 분석 페이지에서 성능 차트를 검토하여 변경 이벤트가 선택한 클러스터 개체의 성능에 영향을 미치는지 여부를 확인할 수 있습니다. 성능 이벤트와 거의 동시에 변경이 감지된 경우, 변경으로 인해 이벤트 알림이 트리거되었을 수 있습니다.

Unified Manager는 정보 이벤트로 분류되는 다음 변경 이벤트를 감지할 수 있습니다.

- 볼륨이 애그리게이트 간에 이동합니다.

  Unified Manager는 이동이 진행 중이거나 완료 또는 실패했는지 감지할 수 있습니다. 볼륨 이동 중에 Unified

Manager가 다운된 경우, 볼륨이 백업될 때 볼륨 이동을 감지하고 해당 볼륨 이동을 위한 변경 이벤트를 표시합니다.

- 모니터링되는 하나 이상의 워크로드 변경이 포함된 QoS 정책 그룹의 처리량(MB/s 또는 IOPS) 제한

  정책 그룹 제한을 변경하면 지연 시간(응답 시간)이 간헐적으로 급증할 수 있으며, 이 경우 정책 그룹에 대한 이벤트도 트리거될 수 있습니다. 지연 시간이 점차 정상으로 돌아오며 급증으로 인한 이벤트는 더 이상 사용되지 않습니다.

- HA 쌍의 노드는 파트너 노드의 스토리지를 이어받거나 해당 노드를 다시 제공합니다.

  Unified Manager는 테이크오버, 부분 인수 또는 반환 작업이 완료된 시기를 감지할 수 있습니다. 패닉이 발생한 노드가 테이크오버로 인해 Unified Manager에서 이벤트를 감지하지 못하는 경우

- ONTAP 업그레이드 또는 되돌리기 작업이 성공적으로 완료되었습니다.

  이전 버전과 새 버전이 표시됩니다.

이벤트 및 심각도 유형 목록입니다

이벤트 목록을 사용하면 Unified Manager에서 볼 수 있는 각 이벤트의 이벤트 범주, 이벤트 이름 및 심각도 유형을 보다 잘 알 수 있습니다. 이벤트는 개체 범주에 따라 사전순으로 나열됩니다.

이벤트를 집계합니다

집계 이벤트는 잠재적 문제를 모니터링할 수 있도록 집계 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
오프라인 애그리게이트(ocumaggregateStateOffline)	사고	집계	심각
집계 실패(문서 집계 실패)	사고	집계	심각
Aggregate Restricted(문서 집계 제한상태)	위험입니다	집계	경고
Aggregate Reconstructing(ocumEvtAggregateRaidStateReconstructing)	위험입니다	집계	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
애그리게이트 성능 저하(document gagregateRaidStateDegraded)	위험입니다	집계	경고
클라우드 계층에 부분적으로 연결 가능(ocEventCloudTierPartiallyReachable)	위험입니다	집계	경고
Cloud Tier Unreachable(문서 클라우드연락할 수 없음)	위험입니다	집계	오류
애그리게이트 재배치에 대한 클라우드 계층 액세스 거부됨 * (arlNetraCaCheckFailed)	위험입니다	집계	오류
스토리지 페일오버 중 애그리게이트 재배치에 대한 클라우드 계층 액세스가 거부됨 * (gbNetraCaCheckFailed)	위험입니다	집계	오류
MetroCluster 집계 왼쪽(ocumEvtMetroCluster AggregateLeftBehind)	위험입니다	집계	오류
MetroCluster 애그리게이트 미러링 성능 저하(ocumEvtMetroCluster및 AggregateMirrorDegraded)	위험입니다	집계	오류

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
애그리게이트 공간 거의 가득 참(ocumEvtAggregateNearlyFull)	위험입니다	집계	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
전체 애그리게이트 공간(ocumEvtAggregateFull)	위험입니다	집계	오류
전체(ocumEvtAggregateDaysUntilFullSoon)까지 일 집계	위험입니다	집계	오류
OverCommitted 집계(ocumEvtAggregateOverCommitted)	위험입니다	집계	오류
거의 커밋됨 집계(문서 집계)(ocumEvtAggregateAlmostOverCommitted)	위험입니다	집계	경고
전체 스냅숏 예비 공간 집계(ocumEvtAggregateSnapReserveFull)	위험입니다	집계	경고
애그리게이트 성장률 비정상(ocumEvtgeggateGrowthRateAbnormal)	위험입니다	집계	경고

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
검색된 애그리게이트(해당 없음)	이벤트	집계	정보
이름이 바뀐 애그리게이트(해당 없음)	이벤트	집계	정보
삭제된 애그리게이트(해당 없음)	이벤트	노드	정보

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
애그리게이트 IOPS 중요 임계값 위반(문서 애그리게이트게이트ateIops Incident)	사고	집계	심각

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
애그리게이트 IOPS 경고 임계값 위반(문서 집계.ifssWarning)	위험입니다	집계	경고
애그리게이트 MB/s 심각한 임계값 침해(문서 집계 ateMbpsIncident)	사고	집계	심각
애그리게이트 MB/s 경고 임계값 위반(문서 집계.MbpsWarning)	위험입니다	집계	경고
지연 시간에 심각한 임계값 위반(문서 집계 atrencyIncident)	사고	집계	심각
애그리게이트 지연 경고 임계값 위반(문서 집계 LatencyWarning)	위험입니다	집계	경고
사용된 총 성능 용량 위험 임계값 위반(문서 집계 성능 용량 PerfCapacityUsedIncident)	사고	집계	심각
사용된 총 성능 용량 경고 임계값 위반(문서 집계 성능 용량 사용 용량 사용 경고)	위험입니다	집계	경고
총 활용률 주요 임계값 위반(문서 집계 활용률인시던트)	사고	집계	심각
애그리게이트 활용률 경고 임계값 위반(문서 집계 활용률경고)	위험입니다	집계	경고
과도하게 사용된 임계값 침해(문서 집계 디스크OverUtilizedWarning)	위험입니다	집계	경고
집계 동적 임계값 위반(문서 집계 DynamicEventWarning)	위험입니다	집계	경고

클러스터 이벤트입니다

클러스터 이벤트는 클러스터의 상태에 대한 정보를 제공하므로 클러스터에서 잠재적인 문제가 있는지 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 이름, 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
클러스터에 스페어 디스크 부족(문서 DisksNot예비품)	위험입니다	클러스터	경고
클러스터에 연결할 수 없음(문서 클러스터연결할 수 없음)	위험입니다	클러스터	오류
클러스터 모니터링 실패(문서 클러스터 모니터링 실패)	위험입니다	클러스터	경고
클러스터 FabricPool 라이센스 용량 제한 위반(문서 ExternalCapacityTierSpaceFull)	위험입니다	클러스터	경고
NVMe - 유예 기간 시작됨 *(nvmfGracePeriodStart)	위험입니다	클러스터	경고
NVMe-of Grace Period Active *(nvmfGracePeriodActive)	위험입니다	클러스터	경고
NVMe - 유예 기간 만료 *(nvmfGracePeriodExpired)	위험입니다	클러스터	경고
개체 유지 관리 창 시작됨(objectMaintenanceWindowStarted)	이벤트	클러스터	심각
개체 유지 관리 창 종료됨(objectMaintenanceWindowEnded)	이벤트	클러스터	정보

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
MetroCluster 스페어 디스크 남음(document.SpareDiskLeftBehind)	위험입니다	클러스터	오류
MetroCluster 자동 비계획 전환 비활성화(문서 MccAutomaticUnplanneSwitchOverDisabled)	위험입니다	클러스터	경고
클러스터 사용자 암호가 변경되었습니다. * (cluster.passwd.changed)	이벤트	클러스터	정보

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
클러스터 용량 불균형 임계값 위반(문서 ConformanceNodeImbalanceWarning)	위험입니다	클러스터	경고
클러스터 클라우드 계층 계획(클러스터CloudTierPlanningWarning)	위험입니다	클러스터	경고
FabricPool 미러 복제 재동기화 완료 * (awflCaResyncComplete)	이벤트	클러스터	경고
FabricPool 공간 거의 다 찼음 * (faboolNearlyFull)	위험입니다	클러스터	오류

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
추가된 노드(해당 없음)	이벤트	클러스터	정보
제거된 노드(해당 없음)	이벤트	클러스터	정보
클러스터 제거됨(해당 없음)	이벤트	클러스터	정보

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
클러스터 추가 실패(해당 없음)	이벤트	클러스터	오류
클러스터 이름이 변경됨(해당 없음)	이벤트	클러스터	정보
비상 EMS 수신(해당 없음)	이벤트	클러스터	심각
Critical EMS 수신 (해당 없음)	이벤트	클러스터	심각
경고 EMS 수신(해당 없음)	이벤트	클러스터	오류
오류 EMS 수신(해당 없음)	이벤트	클러스터	경고
경고 EMS 수신(해당 없음)	이벤트	클러스터	경고
디버그 EMS 수신(해당 없음)	이벤트	클러스터	경고
EMS 수신 통지(해당 없음)	이벤트	클러스터	경고
정보 EMS 수신(해당 없음)	이벤트	클러스터	경고

ONTAP EMS 이벤트는 세 가지 Unified Manager 이벤트 심각도 수준으로 분류됩니다.

Unified Manager 이벤트 심각도 레벨	ONTAP EMS 이벤트 심각도 수준
심각	비상 상황 심각
오류	경고
경고	오류 경고 디버그 주의 정보 제공

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
클러스터 로드 불균형 임계값 위반()	위험입니다	클러스터	경고
클러스터 IOPS 중요 임계값 위반(문서 클러스터사고)	사고	클러스터	심각
클러스터 IOPS 경고 임계값 위반(문서 클러스터경고)	위험입니다	클러스터	경고
클러스터 MB/s 심각한 임계값 위반(문서 클러스터인시던트)	사고	클러스터	심각
클러스터 MB/s 경고 임계값 위반(문서 클러스터 MbpsWarning)	위험입니다	클러스터	경고
클러스터 동적 임계값 위반(문서 ClusterDynamicEventWarning)	위험입니다	클러스터	경고

충격 영역: 보안

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
AutoSupport HTTPS 전송 비활성화됨(ocumClusterASUPHttpsConfiguredDisabled)	위험입니다	클러스터	경고
로그 전달 암호화되지 않음(ocumClusterAuditLogUnencrypted)	위험입니다	클러스터	경고
기본 로컬 관리자 사용(문서 클러스터 기본 관리자 사용)	위험입니다	클러스터	경고
FIPS 모드 비활성화(ocumClusterFipsDisabled)	위험입니다	클러스터	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
로그인 배너 사용 안 함(ocumClusterLoginBannerDisabled)	위험입니다	클러스터	경고
로그인 배너 변경됨(ocumClusterLoginBannerChanged)	위험입니다	클러스터	경고
로그 전달 대상 변경됨(문서 LogForwardinationsChanged)	위험입니다	클러스터	경고
NTP 서버 이름이 변경되었습니다(ocntpServerNamesChanged).	위험입니다	클러스터	경고
NTP 서버 개수가 낮음(securityConfigNTPServerCountLowRisk)	위험입니다	클러스터	경고
클러스터 피어 통신이 암호화되지 않음(ocumClusterPeerEncryptionDisabled)	위험입니다	클러스터	경고
SSH가 안전하지 않은 암호(ClusterSSHInsecure)를 사용 중	위험입니다	클러스터	경고
텔넷 프로토콜 사용(ocumClusterTelnetEnabled)	위험입니다	클러스터	경고
일부 ONTAP 사용자 계정의 암호는 덜 안전한 MD5 해시 기능(ocument ClusterMD5PasswordHashUsed)을 사용합니다.	위험입니다	클러스터	경고
클러스터가 자체 서명된 인증서(ocumClusterSelfSignedCertificate)를 사용합니다.	위험입니다	클러스터	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
클러스터 원격 셸이 활성화됨(문서 클러스터 비활성화됨)	위험입니다	클러스터	경고
클러스터 인증서가 곧 만료됩니다(ocumartClusterCertificateAboutToExpire).	위험입니다	클러스터	경고
클러스터 인증서 만료(문서 클러스터 인증서 만료됨)	위험입니다	클러스터	오류

디스크 이벤트입니다

디스크 이벤트는 잠재적인 문제를 모니터링할 수 있도록 디스크 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
플래시 디스크 - 스페어 블록이 거의 사용됨(문서 클러스터 FlashDiskFewerSpareBlockError)	위험입니다	클러스터	오류
플래시 디스크 - 스페어 블록 없음(doctClusterFlashDiskNoSpareBlockCritical)	사고	클러스터	심각
할당되지 않은 일부 디스크(ocumEvtClusterUnassignedDisksome)	위험입니다	클러스터	경고
일부 실패한 디스크(문서 DisksSomeFailed)	사고	클러스터	심각

엔클로저 이벤트

엔클로저 이벤트는 데이터 센터에서 디스크 쉘프 엔클로저의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
디스크 쉘프 팬 실패(문서 쉘프 팬 실패)	사고	스토리지 쉘프	심각
디스크 쉘프 전원 공급 장치 실패(문서 쉘프 PowerSupplyFailed)	사고	스토리지 쉘프	심각
디스크 쉘프 다중 경로가 구성되지 않음(문서 DiskShelf ConnectivityNotInMultiPath) 이 이벤트는 다음 항목에 적용되지 않습니다. • MetroCluster 구성에 있는 클러스터 • FAS2554, FAS2552, FAS2520 및 FAS2240의 플랫폼을 기반으로 합니다	위험입니다	노드	경고
디스크 쉘프 경로 오류(문서 디스크 쉘프 연결경로 장애)	위험입니다	스토리지 쉘프	경고

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
검색된 디스크 쉘프(해당 없음)	이벤트	노드	정보
디스크 쉘프 제거됨(해당 없음)	이벤트	노드	정보

팬 이벤트

팬 이벤트는 데이터 센터의 노드에 있는 상태 팬에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
하나 이상의 팬 실패(문서 FansOneOrMoreFailed)	사고	노드	심각

플래시 카드 이벤트입니다

플래시 카드 이벤트는 잠재적 문제를 모니터링할 수 있도록 데이터 센터의 노드에 설치된 플래시 카드의 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
오프라인 플래시 카드(ocumEvtFlashCardOffline)	사고	노드	심각

inode 이벤트입니다

inode 이벤트는 inode가 꽉 찼거나 거의 꽉 찼을 때 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
inode가 거의 꽉 참(문서 없음 - 전체)	위험입니다	볼륨	경고
Inode Full(문서 없음)	위험입니다	볼륨	오류

네트워크 인터페이스**(LIF)** 이벤트입니다

네트워크 인터페이스 이벤트는 잠재적인 문제를 모니터링할 수 있도록 네트워크 인터페이스(LIF) 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
네트워크 인터페이스 상태 작동 중지(ocumEvtLifStatusDown)	위험입니다	인터페이스	오류
FC/FCoE 네트워크 인터페이스 상태 다운(문서 FCLifStatusDown)	위험입니다	인터페이스	오류
네트워크 인터페이스 장애 조치를 수행할 수 없습니다(문서: LiftFailoverNotPosable).	위험입니다	인터페이스	경고
네트워크 인터페이스가 홈 포트에 없음(문서 번호: EvtLifNotAtHomePort)	위험입니다	인터페이스	경고

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
네트워크 인터페이스 경로가 구성되지 않음(해당 없음)	이벤트	인터페이스	정보

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
네트워크 인터페이스 MB/s 심각한 임계값 위반(문서 네트워크 수명 장애)	사고	인터페이스	심각
네트워크 인터페이스 MB/s 경고 임계값 위반(문서 네트워크 수명 경고)	위험입니다	인터페이스	경고
FC 네트워크 인터페이스 MB/s 심각한 임계값 위반(문서 FcpLifmbpsIncident)	사고	인터페이스	심각
FC 네트워크 인터페이스 MB/s 경고 임계값 위반(문서 수명경고)	위험입니다	인터페이스	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
NVMf FC 네트워크 인터페이스 MB/s 중요 임계값 위반(문서 NvmfcLifmpsIncident)	사고	인터페이스	심각
NVMf FC 네트워크 인터페이스 MB/s 경고 임계값 위반(문서 NvmfcLifmpsWarning)	위험입니다	인터페이스	경고

LUN 이벤트입니다

LUN 이벤트는 잠재적 문제를 모니터링할 수 있도록 LUN 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
LUN 오프라인(documartLunOffline)	사고	LUN을 클릭합니다	심각
LUN 제거 * (lunDestroy)	이벤트	LUN을 클릭합니다	정보
igroup에서 지원되지 않는 운영 체제와 매핑된 LUN(i.UnsupportedOsType)	사고	LUN을 클릭합니다	경고
LUN 액세스를 위한 단일 활성 경로(doctLunSingleActivePath)	위험입니다	LUN을 클릭합니다	경고
LUN에 액세스할 수 있는 활성 경로 없음(문서 LunNotReachable)	사고	LUN을 클릭합니다	심각
LUN에 액세스하기 위한 최적화된 경로 없음(문서 LunOptimizedPathInactive)	위험입니다	LUN을 클릭합니다	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
HA 파트너의 LUN에 액세스할 수 있는 경로 없음(문서,룬하파비활성)	위험입니다	LUN을 클릭합니다	경고
HA 쌍 중 한 노드에서 LUN에 액세스하는 경로가 없음(ocumuntLunNodePathStatusDown)	위험입니다	LUN을 클릭합니다	오류

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
LUN 스냅샷 복사본을 위한 공간 부족(Documents LunSnapshotNotPosable)	위험입니다	볼륨	경고

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
igroup에서 지원되지 않는 운영 체제와 매핑된 LUN(i.UnsupportedOsType)	위험입니다	LUN을 클릭합니다	경고

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
LUN IOPS 중요 임계값 위반(문서 및 장애)	사고	LUN을 클릭합니다	심각
LUN IOPS 경고 임계값 위반(문서 경고)	위험입니다	LUN을 클릭합니다	경고
LUN MB/s 심각한 임계값 위반(문서 LunMbpsIncident)	사고	LUN을 클릭합니다	심각
LUN MB/s 경고 임계값 위반(문서 LunMbpsWarning)	위험입니다	LUN을 클릭합니다	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
LUN 지연 시간 ms/op 중요 임계값 위반(LunocatencyIncident)	사고	LUN을 클릭합니다	심각
LUN 지연 시간 ms/op 경고 임계값 위반(LunocatencyWarning)	위험입니다	LUN을 클릭합니다	경고
LUN 지연 시간 및 IOPS 중요 임계값 위반(문서 LatrencyIsopsIncident)	사고	LUN을 클릭합니다	심각
LUN 지연 시간 및 IOPS 경고 임계값 위반(문서 라트encyIsopsWarning)	위험입니다	LUN을 클릭합니다	경고
LUN 지연 시간 및 MB/s 심각한 임계값 위반(문서 LunLatencyMbpsIncident)	사고	LUN을 클릭합니다	심각
LUN 지연 시간 및 MB/s 경고 임계값 위반(문서 LunLatencyMbpsWarning)	위험입니다	LUN을 클릭합니다	경고
LUN 지연 시간 및 총 성능 용량 사용된 위험 임계값 위반(문서 LunLatencyAggregatePerfCapacityUsedIncident)	사고	LUN을 클릭합니다	심각
LUN 지연 시간 및 집계 성능 사용된 용량 경고 임계값 위반(문서 LunLatencyAggregatePerfCapacityUsedWarning)	위험입니다	LUN을 클릭합니다	경고
LUN 지연 시간 및 애그리게이트 활용률 주요 임계값 위반(LunocatencyAggregateUtilationIncident)	사고	LUN을 클릭합니다	심각
LUN 지연 및 애그리게이트 활용률 경고 임계값 위반(LunocatencyAggregateUtilationWarning)	위험입니다	LUN을 클릭합니다	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
LUN 지연 시간 및 노드 성능 용량 사용 심각한 임계값 위반(문서 LunatencyNodePerfCapacityUsedIncident)	사고	LUN을 클릭합니다	심각
LUN 지연 시간 및 노드 성능 사용된 용량 경고 임계값 위반(문서 LunatencyNodePerfCapacityUsedWarning)	위험입니다	LUN을 클릭합니다	경고
LUN 지연 시간 및 노드 성능 용량 사용 - 테이크오버가 중요 임계값 위반(문서 LunLatencyAggregatePerfCapacityUsedTakeoverIncident)	사고	LUN을 클릭합니다	심각
사용된 LUN 지연 시간 및 노드 성능 용량 - 테이크오버 경고 임계값 위반(문서 LunLatencyAggregatePerfCapacityUsedTakeoverWarning)	위험입니다	LUN을 클릭합니다	경고
LUN 지연 시간 및 노드 활용률 주요 임계값 위반(LunocrencyNodeUtilationIncident)	사고	LUN을 클릭합니다	심각
LUN 지연 및 노드 활용률 경고 임계값 위반(LunocrencyNodeUtilationWarning)	위험입니다	LUN을 클릭합니다	경고
QoS LUN 최대 IOPS 경고 임계값 위반(문서 QosLunMaxIopsWarning)	위험입니다	LUN을 클릭합니다	경고
QoS LUN 최대 MB/s 경고 임계값 위반(문서 QosLunMaxMbpsWarning)	위험입니다	LUN을 클릭합니다	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
워크로드 LUN 지연 임계값 성능 서비스 수준 정책에 정의된 위반(문서 ConformanceLatencyWarning)	위험입니다	LUN을 클릭합니다	경고

관리 스테이션 이벤트입니다

관리 스테이션 이벤트는 Unified Manager가 설치된 서버의 상태에 대한 정보를 제공하므로 사용자가 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
관리 서버 디스크 공간이 거의 찼습니다(문서 UnifiedManagerDiskSpaceNearlyFull).	위험입니다	관리 스테이션	경고
관리 서버 디스크 공간이 가득 참(문서 UnifiedManagerDiskSpaceFull)	사고	관리 스테이션	심각
메모리 부족 관리 서버(문서 UnifiedManagerMemoryLow)	위험입니다	관리 스테이션	경고
관리 서버의 메모리가 거의 부족합니다(문서 UnifiedManagerMemoryAlmostOut).	사고	관리 스테이션	심각
MySQL 로그 파일 크기 증가, 다시 시작 필요(문서 MysqlLogFileSizeWarning)	사고	관리 스테이션	경고
총 감사 로그 크기 할당이 가득 찼습니다	위험입니다	관리 스테이션	경고
Syslog Server 인증서가 곧 만료됩니다	위험입니다	관리 스테이션	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
Syslog 서버 인증서가 만료되었습니다	위험입니다	관리 스테이션	오류
감사 로그 파일이 변경되었습니다	위험입니다	관리 스테이션	경고
감사 로그 파일이 삭제되었습니다	위험입니다	관리 스테이션	경고
Syslog 서버 연결 오류입니다	위험입니다	관리 스테이션	오류
Syslog 서버 구성이 변경되었습니다	이벤트	관리 스테이션	경고

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
성능 데이터 분석이 영향을 받음(documtUnifiedManagerDataMissingAnalyze)	위험입니다	관리 스테이션	경고
성능 데이터 수집이 영향을 받음(document.UnifiedManagerDataMissingCollection)	사고	관리 스테이션	심각

이 마지막 2가지 성능 이벤트는 Unified Manager 7.2에만 사용할 수 있습니다. 이러한 이벤트 중 하나가 새 상태에 있는 경우, 새 버전의 Unified Manager 소프트웨어로 업그레이드하면 이벤트가 자동으로 삭제되지 않습니다. 이벤트를 수동으로 Resolved 상태로 이동해야 합니다.

MetroCluster 브리지 이벤트입니다

MetroCluster 브리지 이벤트는 브리지 상태에 대한 정보를 제공하므로 FC를 통한 MetroCluster 구성에서 발생할 수 있는 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
Bridge Unreachable(문서 BridgeUnreachable)	사고	MetroCluster 브리지	심각

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
브리지 온도 비정상(문서 BridgeTemperatureAbnormal)	사고	MetroCluster 브리지	심각

MetroCluster 연결 이벤트입니다

연결 이벤트는 클러스터의 구성 요소와 MetroCluster over FC 및 MetroCluster over IP 구성의 클러스터 간 연결에 대한 정보를 제공하므로 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

두 구성 모두에서 공통되는 이벤트입니다

이러한 연결 이벤트는 FC 기반 MetroCluster 및 IP 기반 MetroCluster 구성에서 모두 공통입니다.

영향 영역**:** 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
MetroCluster 파트너 간의 모든 링크 다운(document.MetroClusterTM-AllLinksBetweenPartnersDown)	사고	MetroCluster 관계	심각
피어링 네트워크를 통해 MetroCluster 파트너에게 연결할 수 없음(doctMetroCluster소프트웨어 파트너스NotReachableOverPeeringNetwork)	사고	MetroCluster 관계	심각
영향을 받는 MetroCluster 재해 복구 기능(문서 MetroCluster MetroCluster MetroCluster: 영향 받음)	위험입니다	MetroCluster 관계	심각
MetroCluster 구성이 전환됨(문서 MetroCluster MetroCluster MetroCluster에 영향을 받음)	위험입니다	MetroCluster 관계	경고

FC를 통한 MetroCluster 구성

이러한 이벤트는 FC를 통한 MetroCluster 구성과 관련이 있습니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
모든 스위치 간 링크 다운(documenttMetroClusterTMAllISLBetweenSwitchesDown)	사고	MetroCluster 스위치 간 연결	심각
FC-SAS 브리지와 스토리지 스택 연결 연결 해제(문서 BridgeSasPortDown)	사고	MetroCluster 브리지 스택 연결	심각
MetroCluster 구성이 부분적으로 전환됨(documptMetroCluster MetroCluster소프트웨어 영향받음)	위험입니다	MetroCluster 관계	오류
노드에서 FC 스위치까지 모든 FC-VI 상호 연결 링크 다운(문서 MccNodeSwitchFcviLinksDown)	사고	MetroCluster 노드 스위치 연결	심각
노드-FC 스위치 하나 이상의 FC-이니시에이터 링크 다운(문서 EvtMccNodeSwitchFcLinksOneOrMoreDown)	위험입니다	MetroCluster 노드 스위치 연결	경고
노드에서 FC 스위치로 모든 FC Initiator 링크 다운(문서 MccNodeSwitchFcLinksDown)	사고	MetroCluster 노드 스위치 연결	심각
FC-SAS 브리지 FC 링크로 전환 다운됨(문서 MccSwitchBridgeFcLinksDown)	사고	MetroCluster 스위치 브리지 연결	심각
노드 간 모든 FC VI 상호 연결 링크 다운(문서 MccInterNodeLinksDown)	사고	노드 간 연결입니다	심각

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
노드 간 하나 이상의 FC VI 상호 연결 링크 다운(document MccInterNodeLinksOneOrMoreDown)	위험입니다	노드 간 연결입니다	경고
노드-브리지 링크 다운(문서:EvtMccNodeBridgeLinksDown)	사고	노드 브리지 연결	심각
노드에서 스토리지까지 모든 SAS 링크 다운(문서 MccNodeStackLinksDown)	사고	노드 스택 연결	심각
스토리지 스택에 대한 노드 하나 이상의 SAS 링크 다운(문서 MccNodeStackLinksOneOrMoreDown)	위험입니다	노드 스택 연결	경고

IP를 통한 MetroCluster 구성

이러한 이벤트는 IP를 통한 MetroCluster 구성과 관련이 있습니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
MetroCluster IP 사이트 간 연결 상태가 다운됨(mcIntersiteconectivityStatusDown)	위험입니다	MetroCluster 관계	심각
MetroCluster-IP 노드에서 스위치 연결로 오프라인(mcIpPortStatusOffline)	위험입니다	노드	오류

MetroCluster 스위치 이벤트입니다

FC를 통한 MetroCluster 구성에 대한 MetroCluster 스위치 이벤트를 통해 MetroCluster 스위치의 상태에 대한 정보를 얻을 수 있으므로 잠재적 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
스위치 온도 비정상(ocumEvtSwitchTemperatureAbnormal)	사고	MetroCluster 스위치	심각
스위치에 연결할 수 없음(문서 SwitchUnreachable)	사고	MetroCluster 스위치	심각
팬 전환 실패(문서 교환 OneOrMoreFailed)	사고	MetroCluster 스위치	심각
전원 공급 장치 전환 실패(문서 SwitchPowerSuppliesOneOrMoreFailed)	사고	MetroCluster 스위치	심각
스위치 온도 센서 실패(문서 SwitchTemperatureSensorFailed) 이 이벤트는 Cisco 스위치에만 적용됩니다.	사고	MetroCluster 스위치	심각

NVMe 네임스페이스 이벤트입니다

NVMe 네임스페이스 이벤트는 잠재적 문제를 모니터링할 수 있도록 네임스페이스의 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
NVMeNS 오프라인 *(nvmeNamespaceStatusOffline)	이벤트	네임스페이스	정보
NVMeNS 온라인 *(nvmeNamespaceStatusOnline)	이벤트	네임스페이스	정보

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
스페이스 * 의 NVMeNS(nvmeNamespaceOutOfSpace)	위험입니다	네임스페이스	경고
NVMeNS Destroy * (nvmeNamespaceDestroy)	이벤트	네임스페이스	정보

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
NVMe 네임스페이스 IOPS 주요 임계값 위반(문서 NvmeNamespaceIopsIncident)	사고	네임스페이스	심각
NVMe 네임스페이스 IOPS 경고 임계값 위반(문서 NvmeNamespaceIopsWarning)	위험입니다	네임스페이스	경고
NVMe 네임스페이스 MB/s 심각한 임계값 위반(문서 NvmeNamespaceMbpsIncident)	사고	네임스페이스	심각
NVMe 네임스페이스 MB/s 경고 임계값 위반(문서 NvmeNamespaceMbpsWarning)	위험입니다	네임스페이스	경고
NVMe 네임스페이스 지연 시간 ms/op 중요 임계값 위반(ocumNmeNamespaceLatencyIncident)	사고	네임스페이스	심각
NVMe 네임스페이스 지연 시간 ms/op 경고 임계값 위반(문서 NvmeNamespaceLatencyWarning)	위험입니다	네임스페이스	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
NVMe 네임스페이스 지연 시간 및 IOPS 중요 임계값 위반(문서 NvmeNamespaceLatencyIsopsIncident)	사고	네임스페이스	심각
NVMe 네임스페이스 지연 및 IOPS 경고 임계값 위반(문서 NvmeNamespaceLatencyIsopsWarning)	위험입니다	네임스페이스	경고
NVMe 네임스페이스 지연 시간 및 MB/s 심각한 임계값 위반(문서 NvmeNamespaceLatencyMbpsIncident)	사고	네임스페이스	심각
NVMe 네임스페이스 지연 및 MB/s 경고 임계값 위반(문서 NvmeNamespaceLatencyMbpsWarning)	위험입니다	네임스페이스	경고

노드 이벤트입니다

노드 이벤트는 잠재적 문제를 모니터링할 수 있도록 노드 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
노드 루트 볼륨 공간이 거의 가득 참(Documents ClusterNodeRootVolumeSpaceNearlyFull)	위험입니다	노드	경고
Cloud AWS MetaDataConnFail *(ocumCloudawsMetadataConnFail)	위험입니다	노드	오류

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
Cloud AWS IAMCredsExpired * (CloudocumsIamCredsExpired)(클라우드 AWS IAMCredsExpired)	위험입니다	노드	오류
Cloud AWS IAMCredsInvalid * (CloudocumsIamCredsInvalid)	위험입니다	노드	오류
Cloud AWS IAMCredsNotFound * (ocumCloudAwsIamCredsNotFound)	위험입니다	노드	오류
Cloud AWS IAMCredsNotInitialized * (ocumCloudsIamCredsNotInitialized)	이벤트	노드	정보
Cloud AWS IAMRoleInvalid * (CloudocumeIamRoleInvalid)	위험입니다	노드	오류
Cloud AWS IAMRoleNotFound * (ocumCloudAwsIamRoleNotFound)	위험입니다	노드	오류
클라우드 계층 호스트 해결할 수 없음 * (문서 ObjstoreHostUnresolable)	위험입니다	노드	오류
클라우드 계층 간 클러스터 LIF 다운 * (ocumobstoreInterClusterLif다운)	위험입니다	노드	오류
NFSv4 풀 중 하나가 소진됨 * (nbladeNfsv4PoolEXhaust)	사고	노드	심각

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
요청 불일치 클라우드 계층 서명 * (osSignatureMismatch)	위험입니다	노드	오류

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
QoS 모니터 메모리 최대 * (ocQosMonitorMemoryMaxed)	위험입니다	노드	오류
QoS 모니터 메모리 abated * (문서 QosMonitorMemoryAbated)	이벤트	노드	정보

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
노드 이름 변경됨(해당 없음)	이벤트	노드	정보

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
노드 IOPS 중요 임계값 위반(문서 노드인시던트)	사고	노드	심각
노드 IOPS 경고 임계값 위반(문서 노드 경고)	위험입니다	노드	경고
노드 MB/s 심각한 임계값 위반(문서 노드 MbpsIncident)	사고	노드	심각
노드 MB/s 경고 임계값 위반(문서 노드 MbpsWarning)	위험입니다	노드	경고
노드 지연 시간 ms/op 중요 임계값 위반(문서 노드 LatencyIncident)	사고	노드	심각

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
노드 지연 ms/op 경고 임계값 위반(문서 LatencyWarning)	위험입니다	노드	경고
노드 성능 용량 사용된 중요 임계값 위반(문서 성능 용량 UsedIncident)	사고	노드	심각
사용된 노드 성능 용량 경고 임계값 위반(문서 성능 용량 UsedWarning)	위험입니다	노드	경고
사용된 노드 성능 용량 - 테이크오버가 중요 임계값 위반(문서 성능 용량 성능용량 UsedTakeOverIncident)	사고	노드	심각
사용된 노드 성능 용량 - 조건 경고 임계값 위반(문서 PerfCapacityUsedTakeOverWarning)	위험입니다	노드	경고
노드 활용률 주요 임계값 위반(ocumNodeUtilationIncident)	사고	노드	심각
노드 활용률 경고 임계값 위반(ocumNodeUtilizationWarning)	위험입니다	노드	경고
노드 HA Pair 과도하게 사용된 임계값 침해(문서 노드 HaairOverUtilizedInformation)	이벤트	노드	정보
노드 디스크 조각 모음 임계값 위반(documentDiskFragmentationWarning)	위험입니다	노드	경고
사용된 성능 임계값 위반(문서 오버유틸리티경고)	위험입니다	노드	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
노드 동적 임계값 위반(문서 노드 DynamicEventWarning)	위험입니다	노드	경고

충격 영역: 보안

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
권고 ID: NTAP - <*Advisory ID*>(문서)	위험입니다	노드	심각

NVRAM 배터리 이벤트입니다

NVRAM 배터리 이벤트는 잠재적인 문제를 모니터링할 수 있도록 배터리 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
NVRAM 배터리 부족(문서 번호: NvramBatteryLow)	위험입니다	노드	경고
NVRAM 배터리 방전(문서 번호:	위험입니다	노드	오류
NVRAM 배터리가 과도하게 충전됨(문서 번호: NvramBatteryOverChared)	사고	노드	심각

포트 이벤트입니다

포트 이벤트는 클러스터 포트에 대한 상태를 제공하므로 포트가 중단되었는지 여부와 같이 포트의 변경 또는 문제를 모니터링할 수 있습니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
포트 상태 다운(ocumEvtPortStatusDown)	사고	노드	심각

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
네트워크 포트 MB/s 심각한 임계값 위반(문서 네트워크 포트인시던트)	사고	포트	심각
네트워크 포트 MB/s 경고 임계값 위반(문서 네트워크 포트 MbpsWarning)	위험입니다	포트	경고
FCP 포트 MB/s 중요 임계값 위반(문서 FcpPortMbpsIncident)	사고	포트	심각
FCP 포트 MB/s 경고 임계값 위반(문서 FcpPortMbpsWarning)	위험입니다	포트	경고
네트워크 포트 활용률 주요 임계값 위반(문서 네트워크활용도 유틸리티 인시던트)	사고	포트	심각
네트워크 포트 사용률 경고 임계값 위반(문서 네트워크활용도 경고)	위험입니다	포트	경고
FCP 포트 활용률 주요 임계값 위반(문서 FcpPortUtilizationIncident)	사고	포트	심각
FCP 포트 활용률 경고 임계값 위반(문서 FcpPortUtilizationWarning)	위험입니다	포트	경고

전원 공급 장치 이벤트입니다

전원 공급 장치 이벤트는 잠재적인 문제를 모니터링할 수 있도록 하드웨어 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
하나 이상의 전원 공급 장치 실패(문서 PowerSupplyOneOrMore Failed)	사고	노드	심각

보호 이벤트

보호 이벤트는 작업이 실패했거나 중단되었는지 여부를 알려 사용자가 문제를 모니터링할 수 있도록 합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 보호

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
보호 작업 실패(문서 보호작업 실패)	사고	볼륨 또는 스토리지 서비스	심각
보호 작업이 중단됨(문서 보호작업 중단됨)	위험입니다	볼륨 또는 스토리지 서비스	경고

Qtree 이벤트

Qtree 이벤트에서는 qtree 용량 및 파일/디스크 제한에 대한 정보를 제공하므로 잠재적 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
qtree 공간이 거의 가득 참(문서:QtreeSpaceNearlyFull)	위험입니다	qtree입니다	경고
Qtree 공간 가득 참(문서 QtreeSpaceFull)	위험입니다	qtree입니다	오류
qtree 공간 정상(ocumEvtQtreeSpaceThresholdOk)	이벤트	qtree입니다	정보
Qtree 파일 하드 제한값에 도달함(문서:문서:파일 하드 제한다시 참조)	사고	qtree입니다	심각

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
Qtree 파일 소프트 제한값 위반(doctQtreeFilesSoftLimitBached)	위험입니다	qtree입니다	경고
Qtree 공간 하드 제한값에 도달함(문서:문서:공간 하드 제한재분리)	사고	qtree입니다	심각
Qtree 공간 소프트 제한값 위반(문서:문서 공간 스페이스바 제한도달됨)	위험입니다	qtree입니다	경고

서비스 프로세서 이벤트입니다

서비스 프로세서 이벤트는 잠재적인 문제를 모니터링할 수 있도록 프로세서의 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
서비스 프로세서가 구성되지 않음(문서 서비스프로세서구성 안 됨)	위험입니다	노드	경고
서비스 프로세서 오프라인(ocumEvtServiceProcessorOffline)	위험입니다	노드	오류

SnapMirror 관계 이벤트입니다

SnapMirror 관계 이벤트는 비동기식 및 동기식 SnapMirror 관계의 상태에 대한 정보를 제공하여 잠재적 문제를 모니터링할 수 있습니다. 비동기식 SnapMirror 관계 이벤트는 스토리지 VM 및 볼륨 모두에 대해 생성되지만 동기식 SnapMirror 관계 이벤트는 볼륨 관계에 대해서만 생성됩니다. 스토리지 VM 재해 복구 관계의 일부인 구성요소 볼륨에 대해 생성된 이벤트가 없습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 보호

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

SnapMirror 관계 이벤트는 스토리지 VM 재해 복구로 보호되는 스토리지 VM에 대해 생성되지만 구성요소 개체 관계에는 생성되지 않습니다.

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
미러 복제 비정상(문서 Snap미러로RelationshipUnHealthy)	위험입니다	SnapMirror 관계	경고
미러 복제 부분 해제(ocumEvtSnap미러로RelationshipStateBrokenoff)	위험입니다	SnapMirror 관계	오류
미러 복제 초기화 실패(ocumEvtSnap미러로RelationshipInitializeFailed)	위험입니다	SnapMirror 관계	오류
미러 복제 업데이트 실패(ocumEvtSnap미러로RelationshipUpdateFailed)	위험입니다	SnapMirror 관계	오류
미러 복제 지연 오류(문서1 SnapMirror RelationshipLagError)	위험입니다	SnapMirror 관계	오류
미러 복제 지연 경고(문서 SnapMirror RelationshipLagWarning)	위험입니다	SnapMirror 관계	경고
미러 복제 재동기화 실패(문서 Snap 미러란RelationshipResyncFailed)	위험입니다	SnapMirror 관계	오류
동기식 복제 동기화 중단 *(syncSnap미러로RelationshipOutofsync)	위험입니다	SnapMirror 관계	경고
동기식 복제 복구 *(syncSnap미러로RelationshipInSync)	이벤트	SnapMirror 관계	정보
동기 복제 자동 재동기화 실패 * (syncSnap 미러로RelationshipAutoSyncRetryFailed)	위험입니다	SnapMirror 관계	오류

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
ONTAP 중재자가 클러스터에 추가됨(snap미러orMediatorAdded)	이벤트	클러스터	정보
클러스터에서 ONTAP 중재자가 제거되었습니다(snap미러orMediatorRemoved).	이벤트	클러스터	정보
클러스터에서 ONTAP 중재자를 연결할 수 없습니다(snap미러orMediatorUnreachable).	위험입니다	중재자	경고
ONTAP 중재자를 클러스터에서 액세스할 수 없습니다(snap미러orMediatorMisConfigured).	위험입니다	중재자	오류
ONTAP 중재자 연결이 다시 설정되었으며 SMBC(snap미러orMediatorInQuorum)에 대해 다시 동기화되고 준비되었습니다.	이벤트	중재자	정보

비동기식 미러 및 볼트 관계 이벤트입니다

비동기식 미러 및 볼트 관계 이벤트는 비동기식 SnapMirror 및 볼트 관계의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있도록 합니다. 볼륨 및 스토리지 VM 보호 관계 모두에 대해 비동기식 미러 및 볼트 관계 이벤트가 지원됩니다. 그러나 저장소 VM 재해 복구에는 볼트 관계만 지원되지 않습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 보호

또한 스토리지 VM 재해 복구에서 보호되지만 구성요소 오브젝트 관계에서는 보호되지 않는 스토리지 VM에 대해 SnapMirror 및 Vault 관계 이벤트가 생성됩니다.

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
비동기 미러와 볼트가 비정상(문서 대칭 복사됨 RelationshipUnhealthy)	위험입니다	SnapMirror 관계	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
비동기 미러 및 볼트 연결이 끊어짐(문서:EvtMirrorVaultRelationshipStateBrokenoff)	위험입니다	SnapMirror 관계	오류
비동기 미러 및 볼트 초기화 실패(문서 대칭 복사 VaultRelationshipInitializeFailed)	위험입니다	SnapMirror 관계	오류
비동기 미러 및 볼트 업데이트 실패(문서 대칭 복사. RelationshipUpdateFailed)	위험입니다	SnapMirror 관계	오류
비동기 미러 및 볼트 지연 오류(문서 대칭 복사. RelationshipLagError)	위험입니다	SnapMirror 관계	오류
비동기 미러 및 볼트 지연 경고(문서 대칭 복사. RelationshipLagWarning)	위험입니다	SnapMirror 관계	경고
비동기 미러 및 볼트 재동기화 실패(문서 대칭 복사. RelationshipResyncFailed)	위험입니다	SnapMirror 관계	오류

"SnapMirror 업데이트 실패" 이벤트가 Active IQ 포털(Config Advisor)에 의해 발생합니다.

스냅샷 이벤트

스냅샷 이벤트는 스냅샷의 상태에 대한 정보를 제공하여 스냅샷을 모니터링하여 잠재적인 문제를 파악할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 이름, 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
스냅샷 자동 삭제 사용 안 함(해당 없음)	이벤트	볼륨	정보

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
스냅샷 자동 삭제 사용(해당 없음)	이벤트	볼륨	정보
스냅샷 자동 삭제 구성 수정됨(해당 없음)	이벤트	볼륨	정보

SnapVault 관계 이벤트입니다

SnapVault 관계 이벤트는 잠재적 문제를 모니터링할 수 있도록 SnapVault 관계 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 보호

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
비동기 볼트 비정상(문서 SnapVaultRelationshipUnHealthy)	위험입니다	SnapMirror 관계	경고
비동기 볼트 끊어진 부분(document SnapVaultRelationshipStateBrokenoff)	위험입니다	SnapMirror 관계	오류
비동기 볼트 초기화 실패(문서 SnapVaultRelationshipInitializeFailed)	위험입니다	SnapMirror 관계	오류
비동기 볼트 업데이트 실패(문서 SnapVaultRelationshipUpdateFailed)	위험입니다	SnapMirror 관계	오류
비동기 볼트 지연 오류(ocumEvtSnapVaultRelationshipLagError)	위험입니다	SnapMirror 관계	오류
비동기 볼트 지연 경고(문서 SnapCenter VaultRelationshipLagWarning)	위험입니다	SnapMirror 관계	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
비동기 볼트 재동기화 실패(문서 SnapvaultRelationshipResyncFailed)	위험입니다	SnapMirror 관계	오류

스토리지 페일오버 설정 이벤트입니다

SFO(Storage Failover) 설정 이벤트는 잠재적인 문제를 모니터링할 수 있도록 스토리지 페일오버가 비활성화되었는지 구성되지 않는지에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
스토리지 페일오버 상호 연결 하나 이상의 링크 다운(EvtSpoInterconnectOneOrMoreLinksDown)	위험입니다	노드	경고
스토리지 장애 조치 비활성화됨(문서 클릭 설정 비활성화됨)	위험입니다	노드	오류
저장소 장애 조치가 구성되지 않았습니다(문서 SfingSettingsNotConfiged).	위험입니다	노드	오류
스토리지 페일오버 상태 - 테이크오버가(Document SfocStateTakeover)	위험입니다	노드	경고
스토리지 페일오버 상태 - 부분 기브백(문서 반론 파티션)	위험입니다	노드	오류
스토리지 페일오버 노드 상태 다운(ocumotSfodeStatusDown)	위험입니다	노드	오류
스토리지 페일오버 테이크오버가 가능하지 않음(문서 중 테이크오버가 불가함)	위험입니다	노드	오류

스토리지 서비스 이벤트입니다

스토리지 서비스 이벤트는 잠재적 문제를 모니터링할 수 있도록 스토리지 서비스의 생성 및 구독에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
스토리지 서비스 생성됨(해당 없음)	이벤트	스토리지 서비스	정보
스토리지 서비스 가입됨(해당 없음)	이벤트	스토리지 서비스	정보
스토리지 서비스 구독 취소됨(해당 없음)	이벤트	스토리지 서비스	정보

충격 영역: 보호

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
관리 SnapMirror RelationshipocumEvtStorageServiceUnsupportedRelationshipDeletion 의 예기치 않은 삭제	위험입니다	스토리지 서비스	경고
스토리지 서비스 구성원 볼륨의 예기치 않은 삭제(doctStorageServiceUnexpectedVolumeDeletion)	사고	스토리지 서비스	심각

스토리지 쉘프 이벤트

스토리지 쉘프 이벤트는 스토리지 쉘프가 비정상적인지 여부를 알려므로 잠재적 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
비정상 전압 범위(ocumEvtShortVoltageAbnormal)	위험입니다	스토리지 쉘프	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
비정상 전류 범위(ocumEvttCurrentAbnormal)	위험입니다	스토리지 쉘프	경고
비정상 온도(문서 쉘프 템플릿\n정보)	위험입니다	스토리지 쉘프	경고

스토리지 **VM** 이벤트입니다

스토리지 VM(SVM이라고도 함) 이벤트는 스토리지 VM(SVM)의 상태에 대한 정보를 제공하여 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
SVM CIFS 서비스 중단(문서 VserverCifsServiceStatusDown)	사고	SVM	심각
SVM CIFS 서비스가 구성되지 않음(해당 없음)	이벤트	SVM	정보
존재하지 않는 CIFS 공유 * 연결 시도(nbladeCifsNoPrivShare)	사고	SVM	심각
CIFS NetBIOS 이름 충돌 *(nbladeCifsNbNameConflict)	위험입니다	SVM	오류
CIFS 섀도우 복제본 작업 실패 *(cifsShadowCopyFailure)	위험입니다	SVM	오류
많은 CIFS 연결 *(nbladeCifsManyAuhs)	위험입니다	SVM	오류

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
최대 CIFS 연결이 초과되었습니다 * (nbladeCifsMaxOpenSameFile)	위험입니다	SVM	오류
사용자당 최대 CIFS 연결 수 초과 * (nbladeCifsMaxSessPerUsrConn)	위험입니다	SVM	오류
SVM FC/FCoE 서비스 중단(문서 VserverFcServiceStatusDown)	사고	SVM	심각
SVM iSCSI 서비스 중단(문서 VserverIscsiServiceStatusDown)	사고	SVM	심각
SVM NFS 서비스 중지(ocumEvtVserverNfsServiceStatusDown)	사고	SVM	심각
SVM FC/FCoE 서비스가 구성되지 않음(해당 없음)	이벤트	SVM	정보
SVM iSCSI 서비스가 구성되지 않음(해당 없음)	이벤트	SVM	정보
SVM NFS 서비스가 구성되지 않음(해당 없음)	이벤트	SVM	정보
SVM 중지됨(ocumvserverDown)	위험입니다	SVM	경고
AV 서버 사용 중(Too Busy to Accept New Scan Request) * (nbladvscanConnBackPressure)	위험입니다	SVM	오류

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
바이러스 검사를 위한 AV 서버 연결 없음 * (nbladeVscanNoScannerConn)	사고	SVM	심각
등록된 AV 서버 없음 * (nbladeVscanNoRegdScanner)	위험입니다	SVM	오류
무응답 AV 서버 연결 * (nbladeVscanConnInactive)	이벤트	SVM	정보
AV 서버 무단 사용자 시도 * (nbladvscanBadUserPrivAccess)	위험입니다	SVM	오류
AV 서버에서 바이러스 발견 * (nbladvscanVirusDetected)	위험입니다	SVM	오류

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
SVM 발견됨(해당 없음)	이벤트	SVM	정보
SVM 삭제됨(해당 없음)	이벤트	클러스터	정보
이름이 바뀐 SVM(해당 없음)	이벤트	SVM	정보

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
SVM IOPS 중요 임계값 위반(문서 vmIopsIncident)	사고	SVM	심각
SVM IOPS 경고 임계값 위반(문서 vmIopsWarning)	위험입니다	SVM	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
SVM MB/s 심각한 임계값 위반(문서 vmMbpsIncident)	사고	SVM	심각
SVM MB/s 경고 임계값 위반(문서 vmMbpsWarning)	위험입니다	SVM	경고
SVM 지연 시간 중요 임계값 위반(문서 vmLatencyIncident)	사고	SVM	심각
SVM 지연 경고 임계값 위반(문서 SSmLatencyWarning)	위험입니다	SVM	경고

충격 영역: 보안

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
감사 로그 비활성화(ocumVserverAuditLogDisabled)	위험입니다	SVM	경고
로그인 배너 비활성화됨(ocumVserverLoginBannerDisabled)	위험입니다	SVM	경고
SSH가 안전하지 않은 암호화(ocumVserverSSHInsecure)를 사용 중	위험입니다	SVM	경고
로그인 배너 변경됨(ocumVserverLoginBannerChanged)	위험입니다	SVM	경고
스토리지 VM의 랜섬웨어 방지 모니터링이 비활성화됨(AntansomwareSvmStateDisabled)	위험입니다	SVM	경고
스토리지 VM의 랜섬웨어 방지 모니터링이 활성화됨(학습 모드)(antiRansomwareSvmStateDryrun)	이벤트	SVM	정보

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
랜섬웨어 방지 모니터링에 적합한 스토리지 VM(학습 모드)(ocumEvtSvmArwCaniddate)	이벤트	SVM	정보

사용자 및 그룹 할당량 이벤트입니다

사용자 및 그룹 할당량 이벤트는 잠재적 문제를 모니터링할 수 있도록 사용자 및 사용자 그룹 할당량의 용량 및 파일 및 디스크 제한에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
사용자 또는 그룹 할당량 디스크 공간 소프트 제한값 위반(문서 EvtUserOrGroupQuotaDiskSpaceSoftLimitBreached)	위험입니다	사용자 또는 그룹 할당량	경고
사용자 또는 그룹 할당량 디스크 공간 하드 제한값에 도달함(문서 EvtUserOrGroupQuotaDiskSpaceHardLimitReached)	사고	사용자 또는 그룹 할당량	심각
사용자 또는 그룹 할당량 파일 개수 소프트 제한값 위반(documtUserOrGroupQuotaFileCountSoftLimitBreached)	위험입니다	사용자 또는 그룹 할당량	경고
사용자 또는 그룹 할당량 파일 개수의 하드 제한값에 도달했습니다(문서 EvtUserOrGroupQuotaFileCountHardLimitReached).	사고	사용자 또는 그룹 할당량	심각

볼륨 이벤트

볼륨 이벤트는 잠재적인 문제를 모니터링할 수 있는 볼륨 상태에 대한 정보를 제공합니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 이름, 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

별표(*)는 Unified Manager 이벤트로 변환된 EMS 이벤트를 나타냅니다.

영향 영역: 가용성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨 제한(문서 볼륨 제한)	위험입니다	볼륨	경고
볼륨 오프라인(documVolumeOffline)	사고	볼륨	심각
부분적으로 사용 가능한 볼륨(문서 볼륨 PartiallyAvailable)	위험입니다	볼륨	오류
볼륨 마운트 해제됨(해당 없음)	이벤트	볼륨	정보
마운트된 볼륨(해당 없음)	이벤트	볼륨	정보
볼륨 다시 마운트(해당 없음)	이벤트	볼륨	정보
Volume Junction Path Inactive(문서 JunctVolumeJunctionPathInactive)	위험입니다	볼륨	경고
볼륨 자동 크기 사용(해당 없음)	이벤트	볼륨	정보
Volume Autosize(볼륨 자동 크기) - Disabled(사용 안 함)(해당 없음)	이벤트	볼륨	정보
볼륨 자동 크기 최대 용량 수정됨(해당 없음)	이벤트	볼륨	정보
볼륨 자동 크기 증분 크기 수정됨(해당 없음)	이벤트	볼륨	정보

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
씬 프로비저닝된 볼륨 공간 위험(ocumThinProvisionVolumeSpaceAtRisk)	위험입니다	볼륨	경고
볼륨 효율성 작업 오류(문서 볼륨효율성 OperationError)	위험입니다	볼륨	오류
볼륨 공간이 가득 참(문서 볼륨 전체)	위험입니다	볼륨	오류
볼륨 공간이 거의 가득 참(문서 볼륨 NearlyFull)	위험입니다	볼륨	경고
Volume Logical Space Full *(volumeLogicalSpaceFull)	위험입니다	볼륨	오류
볼륨 논리적 공간이 거의 가득 참 *(volumeLogicalSpaceNearlyFull)	위험입니다	볼륨	경고
볼륨 논리적 공간 정상 *(volumeLogicalSpaceAllOK)	이벤트	볼륨	정보
볼륨 스냅숏 예비 공간 가득 참(문서 스냅샷전체)	위험입니다	볼륨	경고
Snapshot 복사본이 너무 많음(문서 스냅샷모든)	위험입니다	볼륨	오류
볼륨 Qtree 할당량이 커밋됨(문서 볼륨 QtreeQuotaOverCommitted)	위험입니다	볼륨	오류
볼륨 Qtree 할당량이 거의 커밋됨(documotVolumeQtreeQuotaAlmostOverCommitted)	위험입니다	볼륨	경고
용적 증가율 비정상(ocumVolumeGrowthRateAbnormal)	위험입니다	볼륨	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
가득 차기까지 남은 볼륨 일 수(ocumVolumeDaysUntilFullSoon)	위험입니다	볼륨	오류
볼륨 공간 보장 비활성화됨(해당 없음)	이벤트	볼륨	정보
볼륨 공간 보장 사용(해당 없음)	이벤트	볼륨	정보
볼륨 공간 보장 수정됨(해당 없음)	이벤트	볼륨	정보
볼륨 스냅숏 예비 기간(전체(Documents VolumeSnapshotReserveDaysUntilFullSoon)	위험입니다	볼륨	오류
FlexGroup 구성 요소 공간 문제 *(flexGroupConstitutsHaveSpaceIssues)	위험입니다	볼륨	오류
FlexGroup 구성 요소 공간 상태 모두 정상 *(flexGroupConstitutsSpaceStatusAllOK)	이벤트	볼륨	정보
FlexGroup 구성 요소 inode 문제 *(flexGroupConstitutsHaveintesIssues)	위험입니다	볼륨	오류
FlexGroup 구성 요소 inode 상태 모두 정상 *(flexGroupConstituentsInudesStatusAllOK)	이벤트	볼륨	정보
WAFL 볼륨 자동 크기 조정 실패 *(waflVolAutoSizeFail)	위험입니다	볼륨	오류
WAFL 볼륨 자동 크기 조정 완료 *(waflVolAutoSizeDone)	이벤트	볼륨	정보

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
FlexGroup 볼륨이 80% 이상 활용되었습니다 *	사고	볼륨	오류
FlexGroup 볼륨이 90% 이상 활용되었습니다 *	사고	볼륨	심각
볼륨 스토리지 효율성 이상(ocumVolumeAbnormalStorageEfficencyWarning)	위험입니다	볼륨	경고
볼륨 스냅샷 예비 공간 활용도가 낮음(볼륨 스냅샷 예비 공간 활용도가 낮음 경고)	이벤트	볼륨	경고
볼륨 스냅샷 예비 공간 활용도가 낮음(볼륨 스냅샷 예비 공간 활용도가 낮음)	이벤트	볼륨	경고

충격 영역: 구성

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨 이름 변경(해당 없음)	이벤트	볼륨	정보
검색된 볼륨(해당 없음)	이벤트	볼륨	정보
볼륨 삭제됨(해당 없음)	이벤트	볼륨	정보

충격 영역: 성능

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
QoS 볼륨 최대 IOPS 경고 임계값 위반(문서 QosVolumeMaxIopsWarning)	위험입니다	볼륨	경고
QoS 볼륨 최대 MB/s 경고 임계값 위반(문서 QosVolumeMaxMbpsWarning)	위험입니다	볼륨	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
QoS 볼륨 최대 IOPS/TB 경고 임계값 위반(문서 QosVolumeMaxIopsPerTbWarning)	위험입니다	볼륨	경고
워크로드 볼륨 지연 임계값 성능 서비스 수준 정책에 정의된 위반(문서 ConformanceLatencyWarning)	위험입니다	볼륨	경고
볼륨 IOPS 중요 임계값 위반(문서 VolumeIopsIncident)	사고	볼륨	심각
볼륨 IOPS 경고 임계값 위반(문서 볼륨 경고)	위험입니다	볼륨	경고
볼륨 MB/s 심각한 임계값 위반(문서 볼륨 MbpsIncident)	사고	볼륨	심각
볼륨 MB/s 경고 임계값 위반(문서 볼륨 MbpsWarning)	위험입니다	볼륨	경고
볼륨 지연 시간 ms/op 중요 임계값 위반(VolumeLatencyIncident)	사고	볼륨	심각
볼륨 지연 시간 ms/op 경고 임계값 위반(VolumeLatencyWarning)	위험입니다	볼륨	경고
볼륨 캐시 비적중 비율 위험 임계값 위반(문서 VolumeCacheMisssRatioIncident)	사고	볼륨	심각
볼륨 캐시 비적중 비율 경고 임계값 위반(문서 VolumeCacheMisssRatioWarning)	위험입니다	볼륨	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨 지연 시간 및 IOPS 중요 임계값 위반(문서 라티encyIsopsIncident)	사고	볼륨	심각
볼륨 지연 시간 및 IOPS 경고 임계값 위반(문서 LatencyIsopsWarning)	위험입니다	볼륨	경고
볼륨 지연 시간 및 MB/s 심각한 임계값 위반(VolumeLatencyMbpsIncident)	사고	볼륨	심각
볼륨 지연 시간 및 MB/s 경고 임계값 위반(VolumeLatencyMbpsWarning)	위험입니다	볼륨	경고
볼륨 지연 시간 및 집계 성능 사용된 심각한 임계값 위반(문서 LatencyAggregatePerfCapacityUsedIncident)	사고	볼륨	심각
볼륨 지연 및 집계 성능 사용된 용량 경고 임계값 위반(문서 LatencyAggregatePerfCapacityUsedWarning)	위험입니다	볼륨	경고
볼륨 지연 및 애그리게이트 활용률 주요 임계값 위반(VolumeLatencyAggregateUtilationIncident)	사고	볼륨	심각
볼륨 지연 및 애그리게이트 활용률 경고 임계값 위반(VolumeLatencyAggregateUtilationWarning)	위험입니다	볼륨	경고
볼륨 지연 시간 및 노드 성능 용량 사용 심각한 임계값 위반(문서 라티노드 PerfCapacityUsedIncident)	사고	볼륨	심각

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨 지연 및 노드 성능 사용된 용량 경고 임계값 위반(문서 LatencyNodePerfCapacityUsedWarning)	위험입니다	볼륨	경고
사용된 볼륨 지연 시간 및 노드 성능 용량 - 테이크오버가 중요 임계값 위반(문서 LatencyAggregatePerfCapacityUsedTakeoverIncident)	사고	볼륨	심각
사용된 볼륨 지연 시간 및 노드 성능 용량 - 테이크오버 경고 임계값 위반(문서 LatencyAggregatePerfCapacityUsedTakeoverWarning)	위험입니다	볼륨	경고
볼륨 지연 시간 및 노드 활용률 주요 임계값 위반(VolumeLatencyNodeUtilationIncident)	사고	볼륨	심각
볼륨 지연 및 노드 활용률 경고 임계값 위반(VolumeLatencyNodeUtilationWarning)	위험입니다	볼륨	경고

충격 영역: 보안

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨 안티 랜섬웨어 모니터링이 활성화됨(액티브 모드)(안티란소마wareVolumeStateEnabled)	이벤트	볼륨	정보
볼륨 랜섬웨어 방지 모니터링이 비활성화됨(AntRansomwareVolumeStateDisabled)	위험입니다	볼륨	경고

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨 안티 랜섬웨어 모니터링이 활성화됨(학습 모드)(antiRansomwareVolumeStateDryrun)	이벤트	볼륨	정보
볼륨 랜섬웨어 방지 모니터링이 일시 중지됨(학습 모드)(antRansomwareVolumeVolumeStateDryrunPaused)	위험입니다	볼륨	경고
볼륨 랜섬웨어 방지 모니터링이 일시 중지됨(활성 모드)(안티란소마wareVolumeStateEnablePaused)	위험입니다	볼륨	경고
볼륨 안티 랜섬웨어 모니터링이 비활성화(안티란소모레볼륨StateDisableInProgress)	위험입니다	볼륨	경고
랜섬웨어 활동 표시(callHomeRansomwareActivitySeen)	사고	볼륨	심각
랜섬웨어 방지 모니터링에 적합한 볼륨(학습 모드)(ocumVolumeArwCandidATE)	이벤트	볼륨	정보
랜섬웨어 방지 모니터링에 적합한 볼륨(액티브 모드)(ocumVolumeSuitedForActiveAntiRansomwareDetection)	위험입니다	볼륨	경고
볼륨에서 예기치 않은 트래픽 방지 경고(antispansomwareFeatureNoisyVolume)가 발생합니다.	위험입니다	볼륨	경고

충격 영역: 데이터 보호

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨에 로컬 스냅샷 보호 기능이 부족합니다(볼륨 \로컬 보호경고).	위험입니다	볼륨	경고
볼륨에 로컬 스냅샷 보호 기능이 부족합니다(볼륨\LocalProtectionCleared).	위험입니다	볼륨	경고

볼륨 이동 상태 이벤트입니다

볼륨 이동 상태 이벤트는 볼륨 이동 상태를 알려서 잠재적인 문제를 모니터링할 수 있습니다. 이벤트는 영향 영역별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준, 소스 유형 및 심각도를 포함합니다.

충격 영역: 용량

이벤트 이름(트랩 이름)	충격 수준	소스 유형	심각도입니다
볼륨 이동 상태: 진행 중(해당 없음)	이벤트	볼륨	정보
볼륨 이동 상태 - 실패(문서 볼륨 이동 실패)	위험입니다	볼륨	오류
볼륨 이동 상태: 완료됨(해당 없음)	이벤트	볼륨	정보
볼륨 이동 - 컷오버 지연(문서 VolumeCutoverDeferred)	위험입니다	볼륨	경고

이벤트 창 및 대화 상자에 대한 설명입니다

이벤트는 환경의 모든 문제를 알려 줍니다. 이벤트 관리 인벤토리 페이지와 이벤트 세부 정보 페이지를 사용하여 모든 이벤트를 모니터링할 수 있습니다. 알림 설정 옵션 대화 상자를 사용하여 알림을 구성할 수 있습니다. 이벤트 설정 페이지를 사용하여 이벤트를 비활성화하거나 활성화할 수 있습니다.

알림 페이지

이벤트가 생성되거나 사용자에게 할당된 경우 알림을 보내도록 Unified Manager 서버를 구성할 수 있습니다. 알림 메커니즘을 구성할 수도 있습니다. 예를 들어, 알림을 e-메일 또는 SNMP 트랩으로 보낼 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이메일

이 영역에서 알림 알림에 대한 다음 이메일 설정을 구성할 수 있습니다.

- * 보내는 사람 주소 *

  경고 알림을 보낼 e-메일 주소를 지정합니다. 이 값은 공유 시 보고서의 보내는 사람 주소로도 사용됩니다. 발신 주소에 "ActiveIQUnifiedManager@localhost.com" 주소가 미리 입력된 경우, 모든 이메일 알림이 성공적으로 전송되도록 실제 작업 이메일 주소로 변경해야 합니다.

SMTP 서버

이 영역에서 다음 SMTP 서버 설정을 구성할 수 있습니다.

- * 호스트 이름 또는 IP 주소 *

  지정된 수신자에게 알림 알림을 보내는 데 사용되는 SMTP 호스트 서버의 호스트 이름을 지정합니다.

- * 사용자 이름 *

  SMTP 사용자 이름을 지정합니다. SMTP 사용자 이름은 SMTP 서버에서 SMTPAUTH가 활성화된 경우에만 필요합니다.

- * 암호 *

  SMTP 암호를 지정합니다. SMTP 사용자 이름은 SMTP 서버에서 SMTPAUTH가 활성화된 경우에만 필요합니다.

- * 포트 *

  SMTP 호스트 서버가 경고 알림을 보내는 데 사용하는 포트를 지정합니다.

  기본값은 25입니다.

- * 시작/TLS * 를 사용합니다

  이 상자를 선택하면 TLS/SSL 프로토콜(start_tls 및 StartTLS라고도 함)을 사용하여 SMTP 서버와 관리 서버 간의 보안 통신을 제공합니다.

- * SSL 사용 *

  이 확인란을 선택하면 SSL 프로토콜을 사용하여 SMTP 서버와 관리 서버 간의 보안 통신이 제공됩니다.

SNMP를 선택합니다

이 영역에서 다음 SNMP 트랩 설정을 구성할 수 있습니다.

- * 버전 *

  필요한 보안 유형에 따라 사용할 SNMP 버전을 지정합니다. 옵션에는 버전 1, 버전 3, 인증을 사용하는 버전 3, 인증 및 암호화를 사용하는 버전 3이 포함됩니다. 기본값은 버전 1입니다.

- * 트랩 대상 호스트 *

  관리 서버에서 보낸 SNMP 트랩을 수신하는 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)를 지정합니다. 여러 트랩 대상을 지정하려면 각 호스트를 쉼표로 구분합니다.

  "버전" 및 "아웃바운드 포트"와 같은 다른 모든 SNMP 설정은 목록의 모든 호스트에 대해 동일해야 합니다.

- * 아웃바운드 트랩 포트 *

  SNMP 서버가 관리 서버에서 보내는 트랩을 수신하는 포트를 지정합니다.

  기본값은 162입니다.

- * 커뮤니티 *

  호스트에 액세스할 커뮤니티 문자열입니다.

- * 엔진 ID *

  SNMP 에이전트의 고유 식별자를 지정하며 관리 서버에서 자동으로 생성됩니다. 엔진 ID는 SNMP 버전 3, 인증을 사용하는 SNMP 버전 3, 인증 및 암호화를 사용하는 SNMP 버전 3에서 사용할 수 있습니다.

- * 사용자 이름 *

  SNMP 사용자 이름을 지정합니다. 사용자 이름은 SNMP 버전 3, 인증을 사용하는 SNMP 버전 3, 인증 및 암호화를 사용하는 SNMP 버전 3에서 사용할 수 있습니다.

- * 인증 프로토콜 *

  사용자를 인증하는 데 사용되는 프로토콜을 지정합니다. 프로토콜 옵션에는 MD5 및 SHA가 포함됩니다. MD5가 기본값입니다. 인증 프로토콜은 인증 및 암호화 기능이 있는 SNMP 버전 3 및 SNMP 버전 3에서 사용할 수 있습니다.

- * 인증 암호 *

  사용자를 인증할 때 사용되는 암호를 지정합니다. 인증 암호는 인증 및 암호화 기능이 있는 SNMP 버전 3 및 인증 및 SNMP 버전 3에서 사용할 수 있습니다.

- * 개인 정보 보호 프로토콜 *

  SNMP 메시지를 암호화하는 데 사용되는 개인 정보 보호 프로토콜을 지정합니다. 프로토콜 옵션에는 AES 128과 DES가 있습니다. 기본값은 AES 128입니다. 개인 정보 보호 프로토콜은 인증 및 암호화 기능이 있는 SNMP 버전 3에서 사용할 수 있습니다.

- * 개인 정보 보호 암호 *

  개인 정보 보호 프로토콜을 사용할 때 암호를 지정합니다. 개인 정보 보호 암호는 인증 및 암호화 기능이 있는 SNMP 버전 3에서 사용할 수 있습니다.

SNMP 개체 및 트랩에 대한 자세한 내용은 를 다운로드할 수 있습니다 "Active IQ Unified Manager MIB" NetApp Support 사이트에서.

이벤트 관리 인벤토리 페이지입니다

이벤트 관리 인벤토리 페이지에서는 현재 이벤트와 해당 속성의 목록을 볼 수 있습니다. 이벤트 확인, 해결 및 할당과 같은 작업을 수행할 수 있습니다. 특정 이벤트에 대한 알림을 추가할 수도 있습니다.

이 페이지의 정보는 5분마다 자동으로 새로 고쳐지므로 최신 새 이벤트가 표시됩니다.

부품 필터링

이벤트 목록에 표시되는 정보를 사용자 지정할 수 있습니다. 다음 구성 요소를 사용하여 표시되는 이벤트 목록을 구체화할 수 있습니다.

- 미리 정의된 필터 선택 목록에서 선택할 수 있는 보기 메뉴

  여기에는 모든 활성(새 이벤트 및 확인된 이벤트), 활성 성능 이벤트, 나에게 할당된 이벤트(로그인한 사용자) 및 모든 유지 관리 기간 동안 생성된 모든 이벤트가 포함됩니다.

- 전체 또는 부분 용어를 입력하여 이벤트 목록을 구체화하는 검색 창
- 사용 가능한 모든 필드 및 필드 속성에서 선택하여 이벤트 목록을 구체화할 수 있도록 필터 창을 시작하는 필터 단추.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 할당 대상 *

  이벤트를 할당할 사용자를 선택할 수 있습니다. 사용자에게 이벤트를 할당하면 사용자 이름과 이벤트를 할당한 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다.

  - 나

    현재 로그인한 사용자에게 이벤트를 할당합니다.

  - 다른 사용자

    다른 사용자에게 이벤트를 할당하거나 다시 할당할 수 있는 소유자 할당 대화 상자를 표시합니다. 소유권 필드를 비워 두면 이벤트 할당을 취소할 수도 있습니다.

- * 확인 *

  선택한 이벤트를 확인합니다.

  이벤트를 확인하면 사용자 이름과 이벤트를 확인한 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다. 이벤트를 승인하면 해당 이벤트를 관리할 책임이 있습니다.

  정보 이벤트는 승인할 수 없습니다.

- * 해결됨으로 표시 *

  이벤트 상태를 Resolved 로 변경할 수 있습니다.

이벤트를 해결할 때 사용자 이름과 이벤트를 해결한 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다. 이벤트에 대한 수정 조치를 취한 후에는 해당 이벤트를 '해결됨'으로 표시해야 합니다.

- * 알림 추가 *

  선택한 이벤트에 대한 경고를 추가할 수 있는 경고 추가 대화 상자를 표시합니다.

- * 보고서 *

  현재 이벤트 보기의 세부 정보를 쉼표로 구분된 값(.csv) 파일 또는 PDF 문서로 내보낼 수 있습니다.

- * 열 선택기 표시/숨기기 *

  페이지에 표시되는 열을 선택하고 표시되는 순서를 선택할 수 있습니다.

이벤트 목록

트리거된 시간별로 정렬된 모든 이벤트의 세부 정보를 표시합니다.

기본적으로 모든 활성 이벤트 보기가 표시되어 이전 7일 동안 인시던트 또는 위험의 영향 수준을 가진 새 이벤트 및 승인된 이벤트를 표시합니다.

- * 트리거 시간 *

  이벤트가 생성된 시간입니다.

- * 심각도 *

  이벤트 심각도: Critical(), 오류(), 경고() 및 정보()를 클릭합니다.

- * 시/도 *

  이벤트 상태는 New, Acknowledged, Resolved 또는 Obsolete입니다.

- * 영향력 수준 *

  이벤트 영향 수준: 인시던트, 위험, 이벤트 또는 업그레이드.

- * 충격 영역 *

  이벤트 영향 영역: 가용성, 용량, 성능, 보호, 구성, 있습니다.

- * 이름 *

  이벤트 이름입니다. 이름을 선택하여 해당 이벤트에 대한 이벤트 세부 정보 페이지를 표시할 수 있습니다.

- * 출처 *

  이벤트가 발생한 객체의 이름입니다. 이름을 선택하여 해당 개체의 상태 또는 성능 세부 정보 페이지를 표시할 수 있습니다.

  공유 QoS 정책 위반이 발생하는 경우 이 필드에는 최대 IOPS 또는 MB/s를 소비하는 워크로드 객체만 표시됩니다.

이 정책을 사용하는 추가 워크로드가 이벤트 세부 정보 페이지에 표시됩니다.

- * 소스 유형 *

  이벤트가 연결된 객체 유형(예: 스토리지 VM, 볼륨 또는 Qtree)

- * 할당 대상 *

  이벤트가 할당된 사용자의 이름입니다.

- * 이벤트 원본 *

  이벤트가 "Active IQ 포털" 또는 "Active IQ Unified Manager"에서 발생한 것인지 여부.

- * 주석 이름 *

  스토리지 객체에 할당된 주석의 이름입니다.

- * 참고 *

  이벤트에 대해 추가되는 메모 수입니다.

- * 일 우수 *

  이벤트가 처음 생성된 이후 발생한 일 수입니다.

- * 할당된 시간 *

  이벤트가 사용자에게 할당된 이후 경과된 시간입니다. 경과된 시간이 주를 초과하면 이벤트가 사용자에게 할당된 타임스탬프가 표시됩니다.

- * 에 의해 승인됨

  이벤트를 확인한 사용자의 이름입니다. 이벤트가 확인되지 않으면 필드가 비어 있습니다.

- * 확인된 시간 *

  이벤트가 확인된 이후 경과된 시간입니다. 경과된 시간이 주를 초과하면 이벤트가 확인된 타임스탬프가 표시됩니다.

- * 해결자 *

  이벤트를 해결한 사용자의 이름입니다. 이벤트가 해결되지 않으면 필드가 비어 있습니다.

- * 해결 시간 *

  이벤트가 해결된 이후 경과된 시간입니다. 경과된 시간이 주를 초과하면 이벤트가 해결된 타임스탬프가 표시됩니다.

- * Obsoleted Time(관찰 시간) *

  이벤트 상태가 폐기로 된 시간입니다.

이벤트 세부 정보 페이지에서 이벤트 심각도, 영향 수준, 영향 영역 및 이벤트 소스와 같은 선택한 이벤트의 세부 정보를 볼 수 있습니다. 문제 해결을 위해 가능한 해결 방법에 대한 추가 정보도 볼 수 있습니다.

- * 이벤트 이름 *

  이벤트의 이름과 이벤트가 마지막으로 표시된 시간입니다.

  비성능 이벤트의 경우 이벤트가 New 또는 Acknowledged 상태에 있는 동안에는 마지막으로 본 정보를 알 수 없으므로 숨겨집니다.

- * 이벤트 설명 *

  이벤트에 대한 간략한 설명입니다.

  경우에 따라 이벤트 설명에 이벤트가 트리거되는 이유가 제공됩니다.

- * 경합의 요소 *

  동적 성능 이벤트의 경우 이 섹션에는 클러스터의 논리적 및 물리적 구성요소를 나타내는 아이콘이 표시됩니다. 구성 요소의 경합이 발생한 경우 해당 아이콘이 빨간색 원으로 강조 표시됩니다.

  여기에 표시된 구성 요소에 대한 설명은 _Cluster 구성 요소 및 구성 요소가 경합이 가능한 이유_를 참조하십시오.

이벤트 정보, 시스템 진단 및 권장 조치 섹션은 기타 항목에서 설명합니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 메모 아이콘 *

  이벤트에 대한 메모를 추가하거나 업데이트하고 다른 사용자가 남긴 모든 메모를 검토할 수 있습니다.

- 작업 메뉴 *
- * 나에게 할당 *

  사용자에게 이벤트를 할당합니다.

- 다른 사람에게 할당 *

  소유자 할당 대화 상자를 엽니다. 이 대화 상자에서 다른 사용자에게 이벤트를 할당하거나 다시 할당할 수 있습니다.

  사용자에게 이벤트를 할당하면 사용자의 이름과 이벤트가 할당된 시간이 선택한 이벤트의 이벤트 목록에 추가됩니다.

  소유권 필드를 비워 두면 이벤트 할당을 취소할 수도 있습니다.

- * 확인 *

반복 경고 알림을 계속 수신하지 않도록 선택한 이벤트를 확인합니다.

이벤트를 확인하면 선택한 이벤트의 이벤트 목록(에 의해 확인됨)에 사용자 이름과 이벤트가 추가됩니다. 이벤트를 인지하면 해당 이벤트를 관리할 책임이 있습니다.

- * 해결됨으로 표시 *

  이벤트 상태를 Resolved 로 변경할 수 있습니다.

  이벤트를 해결할 때 사용자 이름과 이벤트를 해결한 시간이 선택한 이벤트의 이벤트 목록(에서 해결)에 추가됩니다. 이벤트에 대한 수정 조치를 취한 후에는 해당 이벤트를 '해결됨'으로 표시해야 합니다.

- * 알림 추가 *

  선택한 이벤트에 대한 경고를 추가할 수 있는 경고 추가 대화 상자를 표시합니다.

이벤트 정보 섹션이 표시되는 내용

이벤트 세부 정보 페이지의 이벤트 정보 섹션을 사용하여 이벤트 심각도, 영향 수준, 영향 영역 및 이벤트 소스와 같이 선택한 이벤트에 대한 세부 정보를 볼 수 있습니다.

이벤트 유형에 적용할 수 없는 필드는 숨겨집니다. 다음 이벤트 세부 정보를 볼 수 있습니다.

- * 이벤트 트리거 시간 *

  이벤트가 생성된 시간입니다.

- * 시/도 *

  이벤트 상태는 New, Acknowledged, Resolved 또는 Obsolete입니다.

- * Obsoleted 원인 *

  예를 들어, 이벤트를 폐기하도록 만든 작업이 해결되었습니다.

- * 이벤트 기간 *

  활성(새 이벤트 및 확인된 이벤트) 이벤트의 경우 감지 시간과 이벤트가 마지막으로 분석된 시간 사이의 시간입니다. 사용되지 않는 이벤트의 경우 감지 간격과 이벤트가 해결된 시간입니다.

  이 필드는 모든 성능 이벤트 및 기타 이벤트 유형의 경우 해당 이벤트가 해결되거나 폐기된 후에만 표시됩니다.

- * 마지막 표시 *

  이벤트가 마지막으로 활성 상태로 표시된 날짜 및 시간입니다.

  성능 이벤트의 경우 이벤트가 활성 상태인 동안 성능 데이터를 새로 수집한 후 이 필드가 업데이트되므로 이 값은 이벤트 트리거 시간보다 최근일 수 있습니다. 다른 유형의 이벤트의 경우 New 또는 Acknowledged 상태인 경우 이 콘텐츠는 업데이트되지 않으므로 필드가 숨겨집니다.

- * 심각도 *

이벤트 심각도: Critical(), 오류(), 경고() 및 정보()를 클릭합니다.

- * 영향력 수준 *

  이벤트 영향 수준: 인시던트, 위험, 이벤트 또는 업그레이드.

- * 충격 영역 *

  이벤트 영향 영역: 가용성, 용량, 성능, 보호, 구성, 있습니다.

- * 출처 *

  이벤트가 발생한 객체의 이름입니다.

  공유 QoS 정책 이벤트에 대한 세부 정보를 볼 때 최대 IOPS 또는 MBPS를 소비하는 최대 3개의 워크로드 객체가 이 필드에 나열됩니다.

  소스 이름 링크를 클릭하여 해당 개체의 상태 또는 성능 세부 정보 페이지를 표시할 수 있습니다.

- * 소스 주석 *

  이벤트가 연결된 개체의 주석 이름과 값을 표시합니다.

  이 필드는 클러스터, SVM 및 볼륨의 상태 이벤트에 대해서만 표시됩니다.

- * 소스 그룹 *

  영향을 받는 개체가 구성원으로 있는 모든 그룹의 이름을 표시합니다.

  이 필드는 클러스터, SVM 및 볼륨의 상태 이벤트에 대해서만 표시됩니다.

- * 소스 유형 *

  이벤트가 연결된 오브젝트 유형(예: SVM, 볼륨 또는 Qtree)입니다.

- * 클러스터 *

  이벤트가 발생한 클러스터의 이름입니다.

  클러스터 이름 링크를 클릭하여 해당 클러스터의 상태 또는 성능 세부 정보 페이지를 표시할 수 있습니다.

- * 영향 받는 개체 수 *

  이벤트의 영향을 받는 개체 수입니다.

  개체 링크를 클릭하면 현재 이 이벤트의 영향을 받는 개체로 채워진 인벤토리 페이지가 표시됩니다.

  이 필드는 성능 이벤트에 대해서만 표시됩니다.

- * 영향 받는 볼륨 *

  이 이벤트의 영향을 받는 볼륨 수입니다.

이 필드는 노드 또는 애그리게이트의 성능 이벤트에 대해서만 표시됩니다.

- * 트리거된 정책 *

  이벤트를 발행한 임계값 정책의 이름입니다.

  정책 이름 위에 커서를 올려 놓으면 임계값 정책의 세부 정보를 볼 수 있습니다. 적응형 QoS 정책의 경우 정의된 정책, 블록 크기, 할당 유형(할당된 공간 또는 사용된 공간)도 표시됩니다.

  이 필드는 성능 이벤트에 대해서만 표시됩니다.

- * 규칙 ID *

  Active IQ 플랫폼 이벤트의 경우 이벤트 생성을 위해 트리거된 규칙의 수입니다.

- * 에 의해 승인됨

  이벤트를 인지한 사람의 이름 및 이벤트를 인지한 시간입니다.

- * 해결자 *

  이벤트를 해결한 사람의 이름 및 이벤트가 해결된 시간입니다.

- * 할당 대상 *

  이벤트 작업에 배정된 사람의 이름입니다.

- * 경고 설정 *

  알림에 대한 다음 정보가 표시됩니다.

  ◦ 선택한 이벤트와 관련된 경고가 없으면 * 알림 추가 * 링크가 표시됩니다.

    링크를 클릭하여 경고 추가 대화 상자를 열 수 있습니다.

  ◦ 선택한 이벤트와 관련된 경고가 하나 있는 경우 경고 이름이 표시됩니다.

    링크를 클릭하여 알림 편집 대화 상자를 열 수 있습니다.

  ◦ 선택한 이벤트와 관련된 알림이 두 개 이상 있는 경우 경고 수가 표시됩니다.

    링크를 클릭하여 경고 설정 페이지를 열면 이러한 경고에 대한 자세한 정보를 볼 수 있습니다.

  비활성화된 경고는 표시되지 않습니다.

- * 마지막 알림 전송 *

  가장 최근 알림 메시지가 전송된 날짜 및 시간입니다.

- * 전송 기준 *

  e-메일 또는 SNMP 트랩이라는 경고 알림을 보내는 데 사용된 메커니즘입니다.

- * 이전 스크립트 실행 *

  알림이 생성될 때 실행된 스크립트의 이름입니다.

권장 조치 섹션이 표시되는 내용

이벤트 세부 정보 페이지의 권장 조치 섹션에서는 이벤트에 대해 가능한 원인을 제공하고 사용자가 직접 이벤트를 해결할 수 있도록 몇 가지 조치를 제안합니다. 제안된 작업은 위반된 이벤트 유형 또는 임계값 유형에 따라 사용자 정의됩니다.

이 영역은 일부 이벤트 유형에 대해서만 표시됩니다.

경우에 따라 특정 작업 수행 지침을 포함하여 제안된 여러 작업에 대한 추가 정보를 참조하는 * 도움말 * 링크가 페이지에 제공됩니다. 그 중에는 Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI 명령 또는 이러한 툴의 조합을 사용하는 것도 포함될 수 있습니다.

이 이벤트를 해결하기 위한 지침으로만 여기에서 제안하는 조치를 고려해야 합니다. 이 이벤트를 해결하기 위해 취하는 조치는 사용자 환경의 컨텍스트를 기반으로 해야 합니다.

객체 및 이벤트를 자세히 분석하려면 * 워크로드 분석 * 버튼을 클릭하여 워크로드 분석 페이지를 표시합니다.

Unified Manager에서 완벽하게 진단하고 단일 해결책을 제공할 수 있는 특별한 이벤트가 있습니다. 사용 가능한 경우 해당 해상도는 * Fix it * 버튼과 함께 표시됩니다. Unified Manager에서 이벤트를 발생시키는 문제를 해결하도록 하려면 이 버튼을 클릭합니다.

Active IQ 플랫폼 이벤트의 경우 이 섹션에는 문제 및 가능한 해결책을 설명하는 NetApp 기술 자료 문서(있는 경우)에 대한 링크가 포함될 수 있습니다. 외부 네트워크에 액세스할 수 없는 사이트에서는 Knowledgebase 문서의 PDF가 로컬로 열립니다. PDF는 Unified Manager 인스턴스로 수동으로 다운로드하는 규칙 파일의 일부입니다.

시스템 진단**(System Diagnosis)** 섹션이 표시되는 내용

이벤트 세부 정보 페이지의 시스템 진단 섹션에서는 이벤트에 대한 책임이 있을 수 있는 문제를 진단하는 데 도움이 되는 정보를 제공합니다.

이 영역은 일부 이벤트에 대해서만 표시됩니다.

일부 성능 이벤트는 트리거된 특정 이벤트와 관련된 차트를 제공합니다. 일반적으로 IOPS 또는 MBps 차트와 이전 10일 동안의 지연 시간 차트가 포함됩니다. 이렇게 정렬하면 이벤트가 활성 상태일 때 지연 시간에 가장 영향을 주거나 지연 시간의 영향을 받는 스토리지 구성 요소를 확인할 수 있습니다.

동적 성능 이벤트의 경우 다음 차트가 표시됩니다.

- 워크로드 지연 시간 - 경합 중인 구성 요소의 주요 피해자, 불리 또는 상어 워크로드에 대한 지연 시간 기록을 표시합니다.
- 워크로드 활동 - 경합이 발생한 클러스터 구성 요소의 워크로드 사용에 대한 세부 정보를 표시합니다.
- 리소스 활동 - 경합이 발생한 클러스터 구성 요소에 대한 기간별 성능 통계를 표시합니다.

일부 클러스터 구성 요소의 경합이 있을 때 다른 차트가 표시됩니다.

다른 이벤트는 시스템이 스토리지 객체에서 수행 중인 분석 유형에 대한 간단한 설명을 제공합니다. 경우에 따라 여러

성능 카운터를 분석하는 시스템 정의 성능 정책에 대해 분석한 각 구성 요소별로 하나 이상의 줄이 있을 수 있습니다. 이 시나리오에서는 진단 옆에 특정 진단에서 문제가 발견되었는지 여부를 나타내는 녹색 또는 빨간색 아이콘이 표시됩니다.

이벤트 설정 페이지

이벤트 설정 페이지에는 비활성화된 이벤트 목록이 표시되며 연결된 개체 유형 및 이벤트 심각도와 같은 정보가 제공됩니다. 또한 이벤트를 전역적으로 비활성화하거나 활성화하는 등의 작업을 수행할 수도 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있는 경우에만 이 페이지에 액세스할 수 있습니다.

명령 버튼

명령 단추를 사용하여 선택한 이벤트에 대해 다음 작업을 수행할 수 있습니다.

- * 비활성화 *

  이벤트 사용 안 함 대화 상자를 시작합니다. 이 대화 상자에서 이벤트를 사용하지 않도록 설정할 수 있습니다.

- * 활성화 *

  이전에 비활성화하도록 선택한 이벤트를 활성화합니다.

- * 규칙 업로드 *

  외부 네트워크 액세스 권한이 없는 사이트에서 Active IQ 규칙 파일을 Unified Manager에 수동으로 업로드할 수 있도록 규칙 업로드 대화 상자를 시작합니다. 이 규칙은 AutoSupport 플랫폼에서 정의한 시스템 구성, 케이블 연결, 모범 사례 및 가용성에 대한 이벤트를 생성하기 위해 클러스터 Active IQ 메시지에 대해 실행됩니다.

- * EMS 이벤트 가입 *

  모니터링 중인 클러스터에서 특정 EMS(Event Management System) 이벤트를 수신할 수 있도록 구독할 수 있는 EMS 이벤트 등록 대화 상자를 시작합니다. EMS는 클러스터에서 발생하는 이벤트에 대한 정보를 수집합니다. 가입된 EMS 이벤트에 대한 알림을 수신하면 Unified Manager 이벤트가 적절한 심각도로 생성됩니다.

목록 보기

목록 보기는 비활성화된 이벤트에 대한 정보를 표 형식으로 표시합니다. 열 필터를 사용하여 표시되는 데이터를 사용자 지정할 수 있습니다.

- * 이벤트 *

  비활성화된 이벤트의 이름을 표시합니다.

- * 심각도 *

  이벤트의 심각도를 표시합니다. 심각성은 Critical, Error, Warning 또는 Information 일 수 있습니다.

- * 소스 유형 *

  이벤트가 생성되는 소스 유형을 표시합니다.

이벤트 비활성화 대화 상자

이벤트 사용 안 함 대화 상자에는 이벤트를 사용하지 않도록 설정할 수 있는 이벤트 유형 목록이 표시됩니다. 특정 심각도 또는 이벤트 세트에 따라 이벤트 유형에 대한 이벤트를 사용하지 않도록 설정할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트 속성 영역

이벤트 속성 영역에는 다음 이벤트 속성이 지정됩니다.

- * 이벤트 심각도 *

  심각성, 오류, 경고 또는 정보 등의 심각도 유형을 기반으로 이벤트를 선택할 수 있습니다.

- * 이벤트 이름에 * 가 포함되어 있습니다

  지정한 문자가 포함된 이름의 이벤트를 필터링할 수 있습니다.

- * 일치하는 이벤트 *

  이벤트 심각도 유형과 지정한 텍스트 문자열과 일치하는 이벤트 목록을 표시합니다.

- * 이벤트 비활성화 *

  비활성화하기 위해 선택한 이벤트 목록을 표시합니다.

  이벤트 심각도와 이벤트 이름도 표시됩니다.

명령 버튼

명령 단추를 사용하여 선택한 이벤트에 대해 다음 작업을 수행할 수 있습니다.

- * 저장 후 닫기 *

  이벤트 유형을 비활성화하고 대화 상자를 닫습니다.

- * 취소 *

  변경 내용을 취소하고 대화 상자를 닫습니다.

알림 관리

특정 심각도 유형의 특정 이벤트 또는 이벤트가 발생할 때 알림을 자동으로 보내도록 알림을 구성할 수 있습니다. 경고가 트리거될 때 실행되는 스크립트와 알림을 연결할 수도 있습니다.

경고란 무엇입니까

이벤트는 계속 발생하지만 Unified Manager는 이벤트가 지정된 필터 기준을 충족할 경우에만 알림을 생성합니다. 공간 임계값이 초과되거나 개체가 오프라인 상태가 되는 경우와 같이 알림을 생성할 이벤트를 선택할 수 있습니다. 경고가 트리거될 때 실행되는 스크립트와 알림을 연결할 수도 있습니다.

필터 조건에는 개체 클래스, 이름 또는 이벤트 심각도가 포함됩니다.

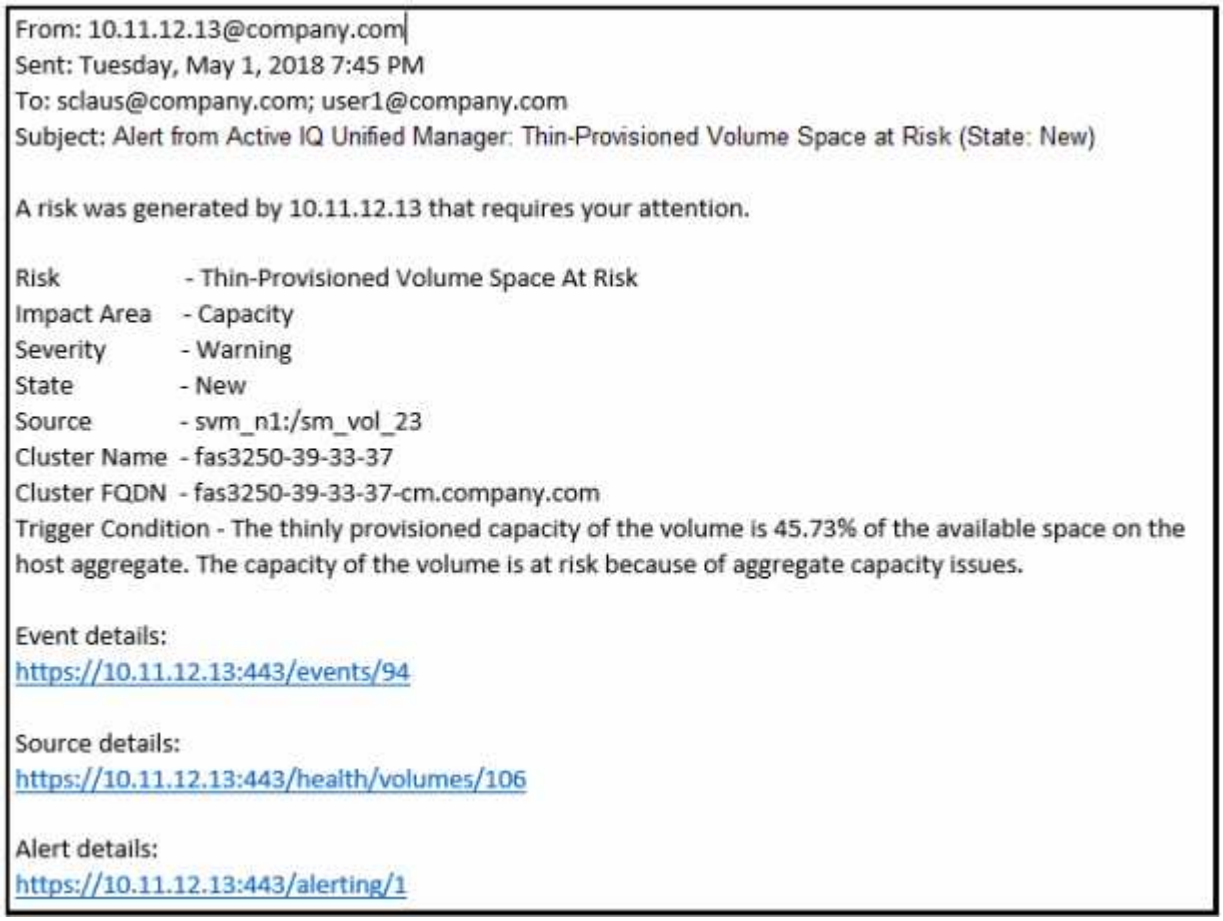
경고 이메일에 포함된 정보

Unified Manager 경고 이메일은 이벤트 유형, 이벤트의 심각도, 이벤트를 발생시키는 위반된 정책 또는 임계값의 이름, 이벤트에 대한 설명을 제공합니다. 또한 전자 메일 메시지에는 UI에서 이벤트의 세부 정보 페이지를 볼 수 있는 각 이벤트에 대한 하이퍼링크도 제공됩니다.

알림 이메일은 알림 수신을 신청한 모든 사용자에게 전송됩니다.

수집 기간 동안 성능 카운터 또는 용량 값이 크게 변경되면 동일한 임계값 정책에 대해 긴급 이벤트와 경고 이벤트가 동시에 트리거될 수 있습니다. 이 경우 경고 이벤트에 대한 이메일 1개와 중요 이벤트에 대한 이메일 1개가 제공됩니다. 그 이유는 Unified Manager를 사용하면 경고 및 심각한 임계값 위반에 대한 경고를 받기 위해 별도로 등록할 수 있기 때문입니다.

다음은 알림 이메일의 예입니다.


From: 10.11.12.13@company.com
Sent: Tuesday, May 1, 2018 7:45 PM
To: sclaus@company.com; user1@company.com
Subject: Alert from Active IQ Unified Manager: Thin-Provisioned Volume Space at Risk (State: New)

A risk was generated by 10.11.12.13 that requires your attention.

Risk - Thin-Provisioned Volume Space At Risk
Impact Area - Capacity
Severity - Warning
State - New
Source - svm_n1:/sm_vol_23
Cluster Name - fas3250-39-33-37
Cluster FQDN - fas3250-39-33-37-cm.company.com
Trigger Condition - The thinly provisioned capacity of the volume is 45.73% of the available space on the host aggregate. The capacity of the volume is at risk because of aggregate capacity issues.

Event details:
https://10.11.12.13:443/events/94

Source details:
https://10.11.12.13:443/health/volumes/106

Alert details:
https://10.11.12.13:443/alerting/1

알림 추가

특정 이벤트가 생성될 때 알림을 표시하도록 알림을 구성할 수 있습니다. 단일 리소스, 리소스 그룹 또는 특정 심각도 유형의 이벤트에 대한 알림을 구성할 수 있습니다. 알림을 받을 빈도를 지정하고 스크립트를 알림에 연결할 수 있습니다.

- 필요한 것 *
- Active IQ Unified Manager 서버가 이러한 설정을 사용하여 이벤트가 생성될 때 사용자에게 알림을 보낼 수 있도록 하려면 사용자 e-메일 주소, SMTP 서버 및 SNMP 트랩 호스트와 같은 알림 설정을 구성해야 합니다.
- 알림을 트리거할 리소스 및 이벤트와 알림을 보낼 사용자의 사용자 이름 또는 이메일 주소를 알고 있어야 합니다.
- 이벤트를 기반으로 스크립트를 실행하려면 스크립트 페이지를 사용하여 Unified Manager에 스크립트를 추가해야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

여기서 설명하는 대로 알림 설정 페이지에서 알림을 생성할 뿐만 아니라 이벤트를 수신한 후 이벤트 세부 정보 페이지에서 직접 알림을 생성할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 * Add * 를 클릭합니다.
3. 경고 추가 * 대화 상자에서 * 이름 * 을 클릭하고 경고의 이름과 설명을 입력합니다.
4. 리소스 * 를 클릭하고 경고에 포함되거나 제외될 리소스를 선택합니다.

   이름 포함 * 필드에서 텍스트 문자열을 지정하여 리소스 그룹을 선택하여 필터를 설정할 수 있습니다. 지정한 텍스트 문자열을 기준으로 사용 가능한 자원 목록에는 필터 규칙과 일치하는 자원만 표시됩니다. 지정하는 텍스트 문자열은 대/소문자를 구분합니다.

   자원이 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 제외된 리소스와 관련된 이벤트에 대해서는 알림이 생성되지 않습니다.

5. 이벤트 * 를 클릭하고 알림을 트리거할 이벤트 이름 또는 이벤트 심각도 유형을 기반으로 이벤트를 선택합니다.

   둘 이상의 이벤트를 선택하려면 Ctrl 키를 누른 상태에서 원하는 항목을 선택합니다.

6. Actions * 를 클릭하고 알릴 사용자를 선택하고, 알림 빈도를 선택하고, SNMP 트랩을 트랩 수신기로 전송할지 여부를 선택한 다음, 경고가 생성될 때 실행할 스크립트를 할당합니다.

   사용자에 대해 지정된 전자 메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 전자 메일 주소가 이전에 선택한 사용자에게 더 이상 매핑되지 않으므로 이름 필드가 비어 있습니다. 또한 사용자 페이지에서 선택한 사용자의 전자 메일 주소를 수정한 경우 선택한 사용자에 대해 수정된 전자 메일 주소가 업데이트되지 않습니다.

   SNMP 트랩을 통해 사용자에게 알리도록 선택할 수도 있습니다.

7. 저장 * 을 클릭합니다.

알림 추가 예

이 예제에서는 다음 요구 사항을 충족하는 알림을 생성하는 방법을 보여 줍니다.

- 알림 이름: 상태 테스트
- 리소스: 이름에 "abc"가 포함된 모든 볼륨을 포함하며 이름에 "xyz"가 포함된 모든 볼륨을 제외합니다.
- 이벤트: 모든 중요한 상태 이벤트를 포함합니다
- 작업: "sample@domain.com", "테스트" 스크립트를 포함하며 사용자에게 15분마다 알림을 받아야 합니다

경고 추가 대화 상자에서 다음 단계를 수행합니다.

1. Name * 을 클릭하고 * Alert Name * 필드에 * 'HealthTest' * 를 입력합니다.
2. 리소스 * 를 클릭하고 포함 탭의 드롭다운 목록에서 * 볼륨 * 을 선택합니다.
   a. 이름이 "abc"인 볼륨을 표시하려면 * Name Contains * 필드에 * "abc" * 를 입력합니다.
   b. 를 선택합니다[All Volumes whose name contains 'abc']Available Resources 영역에서 + * 를 선택한 다음 Selected Resources 영역으로 이동합니다.
   c. Exclude * 를 클릭하고 * Name Contains * 필드에 * "xyz" * 를 입력한 다음 * Add * 를 클릭합니다.
3. 이벤트 * 를 클릭하고 이벤트 심각도 필드에서 * 긴급 * 을 선택합니다.
4. Matching Events 영역에서 * All Critical Events * 를 선택하고 Selected Events 영역으로 이동합니다.
5. 작업 * 을 클릭하고 다음 사용자에게 알림 필드에 *'ample@domain.com' * 를 입력합니다.
6. 15분마다 사용자에게 알리려면 * 15분마다 알림 * 을 선택합니다.

   지정된 시간 동안 수신자에게 반복적으로 알림을 보내도록 알림을 구성할 수 있습니다. 알림에 대해 이벤트 알림이 활성화되는 시간을 결정해야 합니다.

7. 실행할 스크립트 선택 메뉴에서 * 테스트 * 스크립트를 선택합니다.
8. 저장 * 을 클릭합니다.

알림 추가 지침

클러스터, 노드, 애그리게이트 또는 볼륨, 특정 심각도 유형의 이벤트 등 리소스를 기반으로 하는 알림을 추가할 수 있습니다. 모범 사례로서, 객체가 속한 클러스터를 추가한 후 중요 객체에 대한 알림을 추가할 수 있습니다.

다음 지침 및 고려 사항을 사용하여 알림을 생성하여 시스템을 효과적으로 관리할 수 있습니다.

- 경고 설명입니다

  알림을 효과적으로 추적할 수 있도록 알림에 대한 설명을 제공해야 합니다.

- 리소스

  어떤 물리적 또는 논리적 리소스에 경고가 필요한지 결정해야 합니다. 필요에 따라 자원을 포함하거나 제외할 수 있습니다. 예를 들어, 경고를 구성하여 애그리게이트를 면밀히 모니터링하려면 리소스 목록에서 필요한 애그리게이트를 선택해야 합니다.

자원 범주를 선택한 경우(예: *)<<All User or Group Quotas>> * 를 선택하면 해당 범주의 모든 객체에 대한 알림을 받게 됩니다.

> 클러스터를 리소스로 선택해도 해당 클러스터 내의 스토리지 객체는 자동으로 선택되지는 않습니다. 예를 들어, 모든 클러스터에 대해 모든 중요 이벤트에 대한 알림을 생성하는 경우 클러스터 중요 이벤트에 대한 알림만 받게 됩니다. 노드, 애그리게이트 등의 중요 이벤트에 대한 알림을 받지 못합니다.

- 이벤트 심각도입니다

  지정된 심각도 유형(Critical, Error, Warning)의 이벤트가 경고를 트리거할지, 트리거할 경우 어떤 심각도 유형을 트리거할지 결정해야 합니다.

- 선택한 이벤트

  생성된 이벤트 유형에 따라 알림을 추가하는 경우 경고가 필요한 이벤트를 결정해야 합니다.

  이벤트 심각도를 선택했지만 개별 이벤트를 선택하지 않은 경우("선택한 이벤트" 열을 비워 두면) 범주에 있는 모든 이벤트에 대한 알림을 받게 됩니다.

- 작업

  알림을 받는 사용자의 사용자 이름과 이메일 주소를 제공해야 합니다. SNMP 트랩을 알림 모드로 지정할 수도 있습니다. 알림을 생성할 때 실행되도록 알림을 통해 스크립트를 연결할 수 있습니다.

- 알림 빈도

  지정된 시간 동안 수신자에게 알림을 반복적으로 보내도록 알림을 구성할 수 있습니다. 알림에 대해 이벤트 알림이 활성화되는 시간을 결정해야 합니다. 이벤트 알림이 이벤트가 확인될 때까지 반복되도록 하려면 알림을 반복할 빈도를 결정해야 합니다.

- 스크립트를 실행합니다

  스크립트를 경고와 연결할 수 있습니다. 경고가 생성될 때 스크립트가 실행됩니다.

성능 이벤트에 대한 알림 추가

Unified Manager에서 수신한 다른 이벤트처럼 개별 성능 이벤트에 대한 알림을 구성할 수 있습니다. 또한 모든 성능 이벤트를 동일하게 처리하고 동일한 사용자에게 이메일을 전송하려는 경우, 중요한 이벤트 또는 경고 성능 이벤트가 트리거될 때 단일 알림을 생성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 예는 모든 중요한 지연 시간, IOPS 및 MBPS 이벤트에 대한 이벤트를 생성하는 방법을 보여줍니다. 이 동일한 방법을 사용하여 모든 성능 카운터와 모든 경고 이벤트에서 이벤트를 선택할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.

2. Alert Setup * 페이지에서 * Add * 를 클릭합니다.
3. 경고 추가 * 대화 상자에서 * 이름 * 을 클릭하고 경고의 이름과 설명을 입력합니다.
4. 리소스 * 페이지에서 리소스를 선택하지 마십시오.

   리소스를 선택하지 않으면 모든 클러스터, 애그리게이트, 볼륨 등에 경고가 적용되고 해당 이벤트가 수신됩니다.

5. 이벤트 * 를 클릭하고 다음 작업을 수행합니다.
   a. 이벤트 심각도 목록에서 * 긴급 * 을 선택합니다.
   b. Event Name Contains 필드에 * "latency" * 를 입력한 다음 화살표를 클릭하여 일치하는 모든 이벤트를 선택합니다.
   c. 이벤트 이름 포함 필드에 * "IOPS" * 를 입력한 다음 화살표를 클릭하여 일치하는 모든 이벤트를 선택합니다.
   d. 이벤트 이름 포함 필드에 * mbps * 를 입력한 다음 화살표를 클릭하여 일치하는 모든 이벤트를 선택합니다.
6. Actions * 를 클릭한 다음 * Alert these users * 필드에서 경고 이메일을 수신할 사용자의 이름을 선택합니다.
7. SNMP 트랩을 발행하고 스크립트를 실행하기 위해 이 페이지의 다른 옵션을 구성합니다.
8. 저장 * 을 클릭합니다.

알림 테스트 중

경고를 테스트하여 올바르게 구성되었는지 확인할 수 있습니다. 이벤트가 트리거되면 알림이 생성되고 구성된 수신자에게 경고 이메일이 전송됩니다. 테스트 알림을 사용하여 알림이 전송되었는지, 스크립트가 실행되는지 여부를 확인할 수 있습니다.

- 필요한 것 *
- 받는 사람, SMTP 서버 및 SNMP 트랩의 전자 메일 주소와 같은 알림 설정을 구성해야 합니다.

  Unified Manager 서버는 이러한 설정을 사용하여 이벤트가 생성될 때 사용자에게 알림을 보낼 수 있습니다.

- 경고가 생성될 때 스크립트를 할당하고 스크립트를 실행하도록 구성해야 합니다.
- 애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 테스트할 경고를 선택한 다음 * Test * 를 클릭합니다.

   경고를 생성하는 동안 지정한 이메일 주소로 테스트 알림 이메일이 전송됩니다.

해결된 이벤트 및 사용되지 않는 이벤트에 대한 알림을 설정 및 해제할 수 있습니다

알림을 보내도록 구성한 모든 이벤트의 경우 해당 이벤트가 새 상태, 확인된 이벤트, 해결된 이벤트 및 폐기 상태의 모든 사용 가능한 상태로 전환될 때 알림 메시지가 전송됩니다. 이벤트가 Resolved 및 Obsolete 상태로 이동할 때 이벤트에 대한 알림을 받지 않으려면 전역 설정을 구성하여 알림을 표시하지 않도록 할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

기본적으로 알림은 Resolved 및 Obsolete 상태로 이동할 때 이벤트에 대해 전송되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup* 페이지에서 항목 옆에 있는 슬라이더 컨트롤을 사용하여 다음 작업 중 하나를 수행합니다. * 해결됨 및 폐기 이벤트에 대한 경고 *:

대상...	수행할 작업...
이벤트가 해결되거나 폐기됨에 따라 알림 전송을 중지합니다	슬라이더 컨트롤을 왼쪽으로 이동합니다
이벤트가 해결되거나 폐기됨에 따라 알림 전송을 시작합니다	슬라이더 컨트롤을 오른쪽으로 이동합니다

알림 생성에서 재해 복구 대상 볼륨 제외

볼륨 경고를 구성할 때 경고 대화 상자에서 볼륨 또는 볼륨 그룹을 식별하는 문자열을 지정할 수 있습니다. 그러나 SVM에 대한 재해 복구를 구성했다면 소스 볼륨과 타겟 볼륨의 이름이 동일하므로 두 볼륨에 대한 알림이 제공됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대상 SVM의 이름이 인 볼륨을 제외하고 재해 복구 대상 볼륨에 대한 알림을 비활성화할 수 있습니다. 볼륨 이벤트의 식별자에는 SVM 이름과 볼륨 이름이 "<svm_name>:/<volume_name>" 형식으로 포함되어 있으므로 이 작업이 가능합니다.

아래 예에서는 1차 SVM "VS1"에서 볼륨 "vol1"에 대한 경고를 생성하지만 SVM "VS1-DR"에서 이름이 같은 볼륨에서 알림이 생성되지 않도록 하는 방법을 보여줍니다.

경고 추가 대화 상자에서 다음 단계를 수행합니다.

단계

1. 이름 * 을 클릭하고 알림의 이름과 설명을 입력합니다.
2. 리소스 * 를 클릭한 다음 * 포함 * 탭을 선택합니다.
   a. 드롭다운 목록에서 * Volume * 을 선택한 다음 * Name Contains * 필드에 * "vol1" * 를 입력하여 이름에 "vol1"이 포함된 볼륨을 표시합니다.
   b. 를 선택합니다[All Volumes whose name contains 'vol1']Available Resources * 영역에서 + * 를 선택한 다음 * Selected Resources * 영역으로 이동합니다.
3. Exclude *(제외 *) 탭을 선택하고 * Volume *(볼륨 *)을 선택한 다음 * Name Contains *(이름 포함 *) 필드에 * "VS1-DR" * 을 입력한 다음 * Add * (추가 *)를 클릭합니다.

SVM "VS1-DR"에서 볼륨 "vol1"에 대해 알림이 생성되지 않습니다.

4. Events * 를 클릭하고 볼륨에 적용할 이벤트 또는 이벤트를 선택합니다.
5. Actions * 를 클릭한 다음 * Alert these users * 필드에서 경고 이메일을 수신할 사용자의 이름을 선택합니다.
6. SNMP 트랩을 실행하고 스크립트를 실행하도록 이 페이지의 다른 옵션을 구성한 다음 * 저장 * 을 클릭합니다.

경고 보기

경고 설정 페이지에서 다양한 이벤트에 대해 생성된 경고 목록을 볼 수 있습니다. 또한 알림 설명, 알림 방법 및 빈도, 알림을 트리거하는 이벤트, 알림을 e-메일 받는 사람, 클러스터, 애그리게이트, 볼륨과 같은 영향을 받는 리소스 등의 알림 속성을 볼 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.

   경고 목록이 경고 설정 페이지에 표시됩니다.

알림 편집

알림이 연결된 리소스, 이벤트, 수신자, 알림 옵션, 알림 빈도 등의 알림 속성을 편집할 수 있습니다. 관련 스크립트로 제공됩니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 편집할 경고를 선택하고 * Edit * 를 클릭합니다.
3. Edit Alert * (경고 편집 *) 대화 상자에서 이름, 리소스, 이벤트 및 작업 섹션을 편집합니다. 필요에 따라.

   경고와 관련된 스크립트를 변경하거나 제거할 수 있습니다.

4. 저장 * 을 클릭합니다.

알림을 삭제하는 중입니다

더 이상 필요하지 않은 알림은 삭제할 수 있습니다. 예를 들어, Unified Manager에서 해당 리소스를 더 이상 모니터링하지 않을 때 특정 리소스에 대해 생성한 알림을 삭제할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 삭제할 경고를 선택하고 * Delete * 를 클릭합니다.
3. 예 * 를 클릭하여 삭제 요청을 확인합니다.

경고 창 및 대화 상자에 대한 설명입니다

경고 추가 대화 상자를 사용하여 이벤트에 대한 알림을 받도록 알림을 구성해야 합니다. 경고 설정 페이지에서 경고 목록을 볼 수도 있습니다.

경고 설정 페이지

경고 설정 페이지에는 경고 목록이 표시되고 경고 이름, 상태, 알림 방법 및 알림 빈도에 대한 정보가 표시됩니다. 이 페이지에서 경고를 추가, 편집, 제거, 활성화 또는 비활성화할 수도 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

명령 버튼

- * 추가 *

  새 경고를 추가할 수 있는 경고 추가 대화 상자를 표시합니다.

- * 편집 *

  선택한 경고를 편집할 수 있는 Edit Alert(경고 편집) 대화 상자를 표시합니다.

- * 삭제 *

  선택한 경고를 삭제합니다.

- * 활성화 *

  선택한 경고를 사용하여 알림을 보낼 수 있습니다.

- * 비활성화 *

  알림 전송을 일시적으로 중지하려는 경우 선택한 알림을 비활성화합니다.

- * 테스트 *

  선택한 경고를 테스트하여 추가 또는 편집한 후 구성을 확인합니다.

- * 해결된 이벤트 및 사용되지 않는 이벤트에 대한 경고 *

  이벤트가 Resolved 또는 Obsolete 상태로 이동할 때 알림 전송을 활성화 또는 비활성화할 수 있습니다. 이렇게 하면 사용자가 불필요한 알림을 받지 않도록 할 수 있습니다.

목록 보기

목록 보기는 생성된 알림에 대한 정보를 표 형식으로 표시합니다. 열 필터를 사용하여 표시되는 데이터를 사용자 지정할 수 있습니다. 알림을 선택하여 세부 정보 영역에서 자세한 정보를 볼 수도 있습니다.

- * 상태 *

  알림이 설정되었는지 여부를 지정합니다( ) 또는 사용 안 함( )를 클릭합니다.

- * 알림 *

  알림의 이름을 표시합니다.

- * 설명 *

  경고에 대한 설명을 표시합니다.

- * 알림 방법 *

  경고에 대해 선택된 알림 방법을 표시합니다. 이메일 또는 SNMP 트랩을 통해 사용자에게 알릴 수 있습니다.

- * 알림 빈도 *

  이벤트가 확인, 해결 또는 폐기 상태로 이동할 때까지 관리 서버가 계속해서 알림을 보내는 빈도(분)를 지정합니다.

세부 정보 영역

세부 정보 영역에는 선택한 알림에 대한 자세한 정보가 표시됩니다.

- * 경고 이름 *

  알림의 이름을 표시합니다.

- * 경고 설명 *

  경고에 대한 설명을 표시합니다.

- * 이벤트 *

  알림을 트리거할 이벤트를 표시합니다.

- * 리소스 *

  알림을 트리거할 리소스를 표시합니다.

- * 포함 *

  알림을 트리거할 리소스 그룹을 표시합니다.

- * 제외 *

  경고를 트리거하지 않을 리소스 그룹을 표시합니다.

- * 알림 방법 *

  경고에 대한 알림 방법을 표시합니다.

- * 알림 빈도 *

  이벤트가 확인, 해결 또는 폐기 상태로 이동할 때까지 관리 서버가 경고 알림을 계속 보내는 빈도를 표시합니다.

- * 스크립트 이름 *

  선택한 경고와 연결된 스크립트의 이름을 표시합니다. 이 스크립트는 경고가 생성될 때 실행됩니다.

- * 이메일 수신자 *

  알림 알림을 받는 사용자의 전자 메일 주소를 표시합니다.

경고 추가 대화 상자

알림을 생성하여 특정 이벤트가 생성될 때 알림을 받을 수 있으므로 문제를 신속하게 해결하고 환경에 미치는 영향을 최소화할 수 있습니다. 단일 리소스 또는 리소스 집합, 특정 심각도 유형의 이벤트에 대한 알림을 생성할 수 있습니다. 알림 방법 및 알림 빈도를 지정할 수도 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이름

이 영역에서 알림의 이름과 설명을 지정할 수 있습니다.

- * 경고 이름 *

  경고 이름을 지정할 수 있습니다.

- * 경고 설명 *

  경고에 대한 설명을 지정할 수 있습니다.

리소스

이 영역에서는 알림을 트리거할 동적 규칙에 따라 개별 리소스를 선택하거나 리소스를 그룹화할 수 있습니다. _dynamic rule_은 지정한 텍스트 문자열을 기준으로 필터링된 자원 집합입니다. 드롭다운 목록에서 리소스 유형을 선택하여 자원을 검색하거나 정확한 자원 이름을 지정하여 특정 자원을 표시할 수 있습니다.

스토리지 객체 세부 정보 페이지에서 알림을 생성하는 경우 스토리지 객체가 알림에 자동으로 포함됩니다.

- * 포함 *

  경고를 트리거할 리소스를 포함할 수 있습니다. 문자열과 일치하는 리소스를 그룹화하는 텍스트 문자열을 지정하고 경고에 포함할 이 그룹을 선택할 수 있습니다. 예를 들어 이름이 "abc" 문자열을 포함하는 모든 볼륨을 그룹화할 수 있습니다.

- * 제외 *

알림을 트리거하지 않을 리소스를 제외할 수 있습니다. 예를 들어 이름이 "xyz" 문자열을 포함하는 모든 볼륨을 제외할 수 있습니다.

제외 탭은 특정 자원 유형의 모든 자원(예: +)을 선택한 경우에만 표시됩니다[All Volumes] 또는 [All Volumes whose name contains 'xyz']를 누릅니다.

자원이 지정한 포함 및 제외 규칙을 모두 준수하는 경우 제외 규칙이 포함 규칙보다 우선하며 이벤트에 대해 알림이 생성되지 않습니다.

이벤트

이 영역에서 알림을 생성할 이벤트를 선택할 수 있습니다. 특정 심각도 또는 이벤트 집합을 기반으로 이벤트에 대한 알림을 생성할 수 있습니다.

둘 이상의 이벤트를 선택하려면 Ctrl 키를 누른 상태에서 선택해야 합니다.

- * 이벤트 심각도 *

  심각도 유형을 기반으로 이벤트를 선택할 수 있습니다. 심각도 유형은 위험, 오류 또는 경고일 수 있습니다.

- * 이벤트 이름에 * 가 포함되어 있습니다

  이름에 지정된 문자가 포함된 이벤트를 선택할 수 있습니다.

작업

이 영역에서는 알림이 트리거될 때 알릴 사용자를 지정할 수 있습니다. 알림 방법 및 알림 빈도를 지정할 수도 있습니다.

- * 이 사용자에게 알림 *

  알림을 수신할 사용자의 이메일 주소 또는 사용자 이름을 지정할 수 있습니다.

  사용자에 대해 지정된 전자 메일 주소를 수정하고 편집을 위해 알림을 다시 열면 수정된 전자 메일 주소가 이전에 선택한 사용자에게 더 이상 매핑되지 않으므로 이름 필드가 비어 있습니다. 또한 사용자 페이지에서 선택한 사용자의 전자 메일 주소를 수정한 경우 선택한 사용자에 대해 수정된 전자 메일 주소가 업데이트되지 않습니다.

- * 알림 빈도 *

  이벤트를 확인, 확인 또는 폐기 상태로 이동할 때까지 관리 서버가 알림을 보내는 빈도를 지정할 수 있습니다.

  다음 알림 방법을 선택할 수 있습니다.

  - 한 번만 알립니다
  - 지정된 빈도로 알립니다
  - 지정된 시간 범위 내에 지정된 빈도로 알립니다

- * SNMP 트랩 * 을 실행합니다

  이 상자를 선택하면 SNMP 트랩을 전역적으로 구성된 SNMP 호스트로 전송할지 여부를 지정할 수 있습니다.

- * 스크립트 실행 *

알림에 사용자 지정 스크립트를 추가할 수 있습니다. 이 스크립트는 경고가 생성될 때 실행됩니다.

사용자 인터페이스에서 이 기능을 사용할 수 없는 경우 관리자가 해당 기능을 비활성화했기 때문입니다. 필요한 경우 * 스토리지 관리 * > * 기능 설정 * 에서 이 기능을 활성화할 수 있습니다.

명령 버튼

- * 저장 *

  알림을 생성하고 대화 상자를 닫습니다.

- * 취소 *

  변경 내용을 취소하고 대화 상자를 닫습니다.

알림 편집 대화 상자

경고가 연결된 리소스, 이벤트, 스크립트 및 알림 옵션을 비롯한 알림 속성을 편집할 수 있습니다.

이름

이 영역에서 알림의 이름과 설명을 편집할 수 있습니다.

- * 경고 이름 *

  경고 이름을 편집할 수 있습니다.

- * 경고 설명 *

  경고에 대한 설명을 지정할 수 있습니다.

- * 경고 상태 *

  경고를 활성화 또는 비활성화할 수 있습니다.

리소스

이 영역에서는 알림을 트리거할 동적 규칙에 따라 개별 리소스를 선택하거나 리소스를 그룹화할 수 있습니다. 드롭다운 목록에서 리소스 유형을 선택하여 자원을 검색하거나 정확한 자원 이름을 지정하여 특정 자원을 표시할 수 있습니다.

- * 포함 *

  경고를 트리거할 리소스를 포함할 수 있습니다. 문자열과 일치하는 리소스를 그룹화하는 텍스트 문자열을 지정하고 경고에 포함할 이 그룹을 선택할 수 있습니다. 예를 들어 이름이 ""vol0"" 문자열을 포함하는 모든 볼륨을 그룹화할 수 있습니다.

- * 제외 *

  알림을 트리거하지 않을 리소스를 제외할 수 있습니다. 예를 들어 이름이 ""xyz"" 문자열을 포함하는 모든 볼륨을 제외할 수 있습니다.

제외 탭은 특정 자원 유형의 모든 자원(예: +)을 선택한 경우에만 표시됩니다[All Volumes]또는 +[All Volumes whose name contains 'xyz']를 누릅니다.

이벤트

이 영역에서 알림을 트리거할 이벤트를 선택할 수 있습니다. 특정 심각도 또는 이벤트 세트에 따라 이벤트에 대한 알림을 트리거할 수 있습니다.

- * 이벤트 심각도 *

  심각도 유형을 기반으로 이벤트를 선택할 수 있습니다. 심각도 유형은 위험, 오류 또는 경고일 수 있습니다.

- * 이벤트 이름에 * 가 포함되어 있습니다

  지정한 문자가 포함된 이름의 이벤트를 선택할 수 있습니다.

작업

이 영역에서 알림 방법 및 알림 빈도를 지정할 수 있습니다.

- * 이 사용자에게 알림 *

  이메일 주소 또는 사용자 이름을 편집하거나 알림을 수신할 새 이메일 주소 또는 사용자 이름을 지정할 수 있습니다.

- * 알림 빈도 *

  이벤트를 확인, 해결 또는 폐기 상태로 이동할 때까지 관리 서버가 알림을 보내는 빈도를 편집할 수 있습니다.

  다음 알림 방법을 선택할 수 있습니다.

  - 한 번만 알립니다
  - 지정된 빈도로 알립니다
  - 지정된 시간 범위 내에 지정된 빈도로 알립니다

- * SNMP 트랩 * 을 실행합니다

  SNMP 트랩을 전역적으로 구성된 SNMP 호스트로 전송할지 여부를 지정할 수 있습니다.

- * 스크립트 실행 *

  스크립트를 경고와 연결할 수 있습니다. 이 스크립트는 경고가 생성될 때 실행됩니다.

명령 버튼

- * 저장 *

  변경 사항을 저장하고 대화 상자를 닫습니다.

- * 취소 *

변경 내용을 취소하고 대화 상자를 닫습니다.

스크립트 관리

스크립트를 사용하여 Unified Manager에서 여러 스토리지 오브젝트를 자동으로 수정 또는 업데이트할 수 있습니다. 스크립트가 경고와 연결되어 있습니다. 이벤트가 경고를 트리거하면 스크립트가 실행됩니다. 사용자 지정 스크립트를 업로드하고 경고가 생성될 때 해당 스크립트를 테스트할 수 있습니다.

스크립트를 Unified Manager에 업로드하여 실행할 수 있는 기능은 기본적으로 활성화되어 있습니다. 보안상의 이유로 조직에서 이 기능을 허용하지 않으려는 경우 * 스토리지 관리 * > * 기능 설정 * 에서 이 기능을 비활성화할 수 있습니다.

- 관련 정보 *

"스크립트 업로드 기능을 활성화 및 비활성화합니다"

스크립트가 경고와 함께 작동하는 방식

알림을 스크립트에 연결하여 Unified Manager의 이벤트에 대한 알림이 발생할 때 스크립트가 실행되도록 할 수 있습니다. 스크립트를 사용하여 스토리지 오브젝트 문제를 해결하거나 이벤트를 생성하고 있는 스토리지 오브젝트를 식별할 수 있습니다.

Unified Manager에서 이벤트에 대한 알림이 생성되면 지정된 수신자에게 알림 이메일이 전송됩니다. 경고와 스크립트를 연결한 경우 스크립트가 실행됩니다. 알림 e-메일에서 스크립트에 전달된 인수의 세부 정보를 확인할 수 있습니다.

사용자 지정 스크립트를 만들어 특정 이벤트 유형에 대한 경고와 연결한 경우 해당 이벤트 유형에 대한 사용자 지정 스크립트를 기반으로 작업이 수행되며, 관리 작업 페이지나 Unified Manager 대시보드에서 기본적으로 * Fix it * 작업을 사용할 수 없습니다.

스크립트는 실행에 다음 인수를 사용합니다.

- ``eventID'
- - 'EventName'
- -"eventSeverity"
- -eventSourceID
- - "eventSourceName"입니다
- -eventSourceType
- -'eventState'입니다
- 'EventArgs'입니다

스크립트의 인수를 사용하여 관련 이벤트 정보를 수집하거나 스토리지 객체를 수정할 수 있습니다.

스크립트에서 인수를 가져오는 예제

```
`print "$ARGV[0] : $ARGV[1]\n"`
`print "$ARGV[7] : $ARGV[8]\n"`
```

경고가 생성되면 이 스크립트가 실행되고 다음 출력이 표시됩니다.

```
-`eventID : 290`
-`eventSourceID : 4138`
```

스크립트 추가

Unified Manager에 스크립트를 추가하고 스크립트를 알림에 연결할 수 있습니다. 이러한 스크립트는 경고가 생성될 때 자동으로 실행되며, 이벤트를 생성할 스토리지 개체에 대한 정보를 가져올 수 있습니다.

- 필요한 것 *
- Unified Manager 서버에 추가할 스크립트를 작성하여 저장해야 합니다.
- 스크립트에 지원되는 파일 형식은 Perl, Shell, PowerShell, Python 및 .bat입니다.

Unified Manager가 설치된 플랫폼입니다	지원되는 언어
VMware	Perl 및 Shell 스크립트
리눅스	Perl, Python 및 Shell 스크립트
Windows	PowerShell, Perl, Python 및 .bat 스크립트

  - Perl 스크립트의 경우, Perl을 Unified Manager 서버에 설치해야 합니다. VMware 설치의 경우 Perl 5가 기본적으로 설치되며 스크립트는 Perl 5가 지원하는 것만 지원합니다. Unified Manager 후에 Perl이 설치된 경우 Unified Manager 서버를 다시 시작해야 합니다.
  - PowerShell 스크립트의 경우 스크립트를 실행할 수 있도록 Windows 서버에 적절한 PowerShell 실행 정책을 설정해야 합니다.

  스크립트가 알림 스크립트 진행률을 추적하기 위해 로그 파일을 생성할 경우 Unified Manager 설치 폴더 내 로그 파일이 생성되지 않도록 해야 합니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

사용자 지정 스크립트를 업로드하고 알림에 대한 이벤트 세부 정보를 수집할 수 있습니다.

사용자 인터페이스에서 이 기능을 사용할 수 없는 경우 관리자가 해당 기능을 비활성화했기 때문입니다. 필요한 경우 * 스토리지 관리 * > * 기능 설정 * 에서 이 기능을 활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 스크립트 * 를 클릭합니다.
2. 스크립트 * 페이지에서 * 추가 * 를 클릭합니다.
3. 스크립트 * 추가 대화 상자에서 * 찾아보기 * 를 클릭하여 스크립트 파일을 선택합니다.
4. 선택한 스크립트에 대한 설명을 입력합니다.
5. 추가 * 를 클릭합니다.
    ◦ 관련 정보 *

"스크립트 업로드 기능을 활성화 및 비활성화합니다"

스크립트를 삭제하는 중입니다

스크립트가 더 이상 필요하지 않거나 유효하지 않은 경우 Unified Manager에서 스크립트를 삭제할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스크립트는 경고와 연관되지 않아야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 스크립트 * 를 클릭합니다.
2. 스크립트 * 페이지에서 삭제할 스크립트를 선택한 다음 * 삭제 * 를 클릭합니다.
3. 경고 * 대화 상자에서 * 예 * 를 클릭하여 삭제를 확인합니다.

스크립트 실행 테스트 중

스토리지 객체에 대한 알림이 생성될 때 스크립트가 올바르게 실행되는지 확인할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 지원되는 파일 형식의 스크립트를 Unified Manager에 업로드해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 스크립트 * 를 클릭합니다.
2. 스크립트 * 페이지에서 테스트 스크립트를 추가합니다.
3. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
4. Alert Setup* 페이지에서 다음 작업 중 하나를 수행합니다.

대상...	수행할 작업...
알림을 추가합니다	a. 추가 * 를 클릭합니다. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.

대상...	수행할 작업...
알림을 편집합니다	a. 알림을 선택한 다음 * 편집 * 을 클릭합니다. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.

5. 저장 * 을 클릭합니다.
6. Alert Setup * 페이지에서 추가하거나 수정한 알림을 선택한 다음 * Test * 를 클릭합니다.

   이 스크립트는 "-test" 인수를 사용하여 실행되며 알림을 만들 때 지정된 e-메일 주소로 알림 알림이 전송됩니다.

지원되는 **Unified Manager CLI** 명령

스토리지 관리자는 CLI 명령을 사용하여 클러스터, 애그리게이트, 볼륨 등의 스토리지 개체에 대한 쿼리를 수행할 수 있습니다. qtree 및 LUN, CLI 명령을 사용하여 Unified Manager 내부 데이터베이스와 ONTAP 데이터베이스를 쿼리할 수 있습니다. 작업 시작 또는 종료 시 실행되는 스크립트에서 CLI 명령을 사용하거나 경고가 트리거될 때 실행할 수도 있습니다.

모든 명령에는 'um CLI login' 명령어와 유효한 사용자 이름 및 인증 패스워드가 선행되어야 한다.

um run_command를 실행하려면 계정에 _console_application 액세스 권한이 있는지 확인하십시오.

CLI 명령	설명	출력
'um CLI login -u <username>[-p <password>]'	CLI에 로그인합니다. 보안 관련 문제 때문에 "-u" 옵션 다음에 사용자 이름만 입력해야 합니다. 이러한 방식으로 사용하면 암호를 입력하라는 메시지가 표시되며 암호는 기록 또는 프로세스 테이블에서 캡처되지 않습니다. 이 세션은 로그인 후 3시간 후에 만료되며, 그 이후에는 사용자가 다시 로그인해야 합니다.	해당 메시지를 표시합니다.
um CLI 로그아웃	CLI에서 로그아웃합니다.	해당 메시지를 표시합니다.
염원이다	모든 1단계 하위 명령을 표시합니다.	모든 1단계 하위 명령을 표시합니다.
'<um run cmd[-t<timeout>]<cluster><command>'	하나 이상의 호스트에서 명령을 실행하는 가장 간단한 방법입니다. ONTAP에서 작업을 가져오기 또는 수행하기 위해 주로 알림 스크립팅에 사용됩니다. 선택적 timeout 인수는 클라이언트에서 명령이 완료될 수 있는 최대 시간 제한(초)을 설정합니다. 기본값은 0(계속 대기)입니다.	ONTAP로부터 수신한 경우

CLI 명령	설명	출력
'um run query <sql command>'	SQL 쿼리를 실행합니다. 데이터베이스에서 읽은 쿼리만 허용됩니다. 업데이트, 삽입 또는 삭제 작업은 지원되지 않습니다.	결과는 표 형식으로 표시됩니다. 빈 집합이 반환되거나 구문 오류 또는 잘못된 요청이 있으면 적절한 오류 메시지가 표시됩니다.
"um datasource add -u <username> -P <password>[-t <protocol>][-p <port>] <hostname-or -ip>'	관리되는 스토리지 시스템 목록에 데이터 소스를 추가합니다. 데이터 소스는 스토리지 시스템에 대한 접속 방식을 설명합니다. 데이터 소스를 추가할 때 -u(사용자 이름) 및 -P(암호) 옵션을 지정해야 합니다. t(프로토콜) 옵션은 클러스터(http 또는 https)와 통신하는 데 사용되는 프로토콜을 지정합니다. 프로토콜을 지정하지 않으면 두 프로토콜 모두 -p(포트) 옵션이 클러스터와 통신하는 데 사용되는 포트를 지정합니다. 포트를 지정하지 않으면 해당 프로토콜의 기본값이 시도됩니다. 이 명령은 스토리지 관리자만 실행할 수 있습니다.	사용자에게 인증서를 수락하라는 메시지가 표시되고 해당 메시지가 인쇄됩니다.
'<datasource-id>' 데이터 소스 목록 [<datasource-id>]'	관리되는 스토리지 시스템의 데이터 소스를 표시합니다.	'ID Address Port, Protocol Acquisition Status, Analysis Status, Communication Status, Acquisition Message, 및 분석 메시지'를 참조하십시오.
'<datasource modify[-h<hostname-or-ip>] [-u<username>] [-P<password>] [-t<protocol>] [-p <port>] <datasource-id>'	하나 이상의 데이터 소스 옵션을 수정합니다. 스토리지 관리자만 실행할 수 있습니다.	해당 메시지를 표시합니다.
'um datasource remove <datasource-id>'	Unified Manager에서 데이터 소스(클러스터)를 제거합니다.	해당 메시지를 표시합니다.
'<옵션 목록[<옵션>.]	에는 set 명령을 사용하여 구성할 수 있는 모든 옵션이 나와 있습니다.	이름, 값, 기본값, 다시 시작 필요 등의 값을 표 형식으로 표시합니다
``um option set <option-name>=<option-value>[<option-name>=<option-value>…]	하나 이상의 옵션을 설정합니다. 명령은 스토리지 관리자만 실행할 수 있습니다.	해당 메시지를 표시합니다.
UM 버전	Unified Manager 소프트웨어 버전을 표시합니다.	버전 ("9.6")

CLI 명령	설명	출력
``um LUN list[-q][-ObjectType<object-id>]'	지정된 객체에서 필터링한 후 LUN을 나열합니다. q는 헤더를 표시하지 않는 모든 명령에 적용할 수 있습니다. ObjectType은 LUN, qtree, 클러스터, 볼륨, 할당량, 또는 svm. 예를 들면 다음과 같습니다. • "um LUN list-cluster 1" * 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령을 실행하면 클러스터 내의 모든 LUN이 ID 1로 나열됩니다.	표 형식으로 ID와 LUN 경로를 표시합니다
"um svm list[-q][-ObjectType<object-id>]'	지정된 객체에서 필터링한 후 스토리지 VM을 나열합니다. ObjectType은 LUN, qtree, 클러스터, 볼륨, 할당량, 또는 svm. 예를 들면 다음과 같습니다. • "um svm list-cluster 1' 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령을 실행하면 클러스터 내의 모든 스토리지 VM이 ID 1로 나열됩니다.	Name과 Cluster ID를 표 형식으로 표시합니다
"um qtree list[-q][-ObjectType<object-id>]'	지정된 객체에서 필터링한 후 qtree를 나열합니다. q는 헤더를 표시하지 않는 모든 명령에 적용할 수 있습니다. ObjectType은 LUN, qtree, 클러스터, 볼륨, 할당량, 또는 svm. 예를 들면 다음과 같습니다. • 'um qtree list-cluster 1' 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 명령은 클러스터 내의 모든 qtree를 ID 1로 나열합니다.	표 형식으로 Qtree ID와 Qtree Name의 값을 표시합니다

CLI 명령	설명	출력
'<um disk list[-q][-ObjectType<object-id>]'	지정된 개체에서 필터링한 후 디스크를 나열합니다. ObjectType은 디스크, 집계, 노드 또는 클러스터일 수 있습니다. 예를 들면 다음과 같습니다. • "um disk list - cluster 1" * 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령을 실행하면 클러스터 내의 모든 디스크가 ID 1과 함께 나열됩니다.	다음 값을 표 형식 "ObjectType and object-id"로 표시합니다.
``um 클러스터 목록[-q][-ObjectType<object-id>]'	지정된 개체에서 필터링한 후 클러스터가 나열됩니다. ObjectType은 디스크, 집계, 노드, 클러스터, LUN, Qtree, 볼륨, 할당량 또는 svm. 예를 들면 다음과 같습니다. • 'um cluster list-aggr 1' 이 예제에서 "-aggr"은 objectType이고 "1"은 objectId입니다. 이 명령을 실행하면 ID가 1인 애그리게이트가 속해 있는 클러스터가 나열됩니다.	Name, Full Name, Serial Number, DataSource ID, Last Refresh Time, 및 리소스 키'를 선택합니다.
"um cluster node list[-q][-ObjectType<object-id>]'	지정된 객체에서 필터링한 후 클러스터 노드를 나열합니다. ObjectType은 디스크, 집계, 노드 또는 클러스터일 수 있습니다. 예를 들면 다음과 같습니다. • 'um cluster node list-cluster 1' 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 명령은 클러스터 내의 모든 노드를 ID 1로 나열합니다.	다음 값을 표 형식 '이름 및 클러스터 ID'로 표시합니다.

CLI 명령	설명	출력
'<um volume list[-q][-ObjectType<object-id>]'	지정된 개체에서 필터링한 후 볼륨을 나열합니다. ObjectType은 LUN, qtree, 클러스터, 볼륨, 할당량, SVM 또는 애그리게이트. 예를 들면 다음과 같습니다. • 'um volume list-cluster 1' 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령을 실행하면 클러스터 내의 모든 볼륨이 ID 1로 나열됩니다.	다음 값을 표 형식 '볼륨 ID 및 볼륨 이름'으로 표시합니다.
"um quota user list[-q][-ObjectType<object-id>]'	지정된 개체에서 필터링한 후 할당량 사용자를 나열합니다. ObjectType은 qtree, 클러스터, 볼륨, 할당량 또는 svm일 수 있습니다. 예를 들면 다음과 같습니다. • 'um quota user list-cluster 1' 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령을 실행하면 클러스터 내의 모든 할당량 사용자에게 ID가 1로 표시됩니다.	ID, 이름, SID, 이메일 등 표 형식으로 다음 값을 표시합니다.
"um aggr list[-q][-ObjectType<object-id>]'	지정된 개체에서 필터링한 후 애그리게이트를 나열합니다. ObjectType은 디스크, 집계, 노드, 클러스터 또는 볼륨일 수 있습니다. 예를 들면 다음과 같습니다. • 'um aggr list-cluster 1' 이 예제에서 "-cluster"는 objectType이고 "1"은 objectId입니다. 이 명령을 실행하면 클러스터 내의 모든 애그리게이트가 ID 1로 나열됩니다.	다음 값을 표 형식 '애그리게이트 ID 및 애그리게이트 이름'으로 표시합니다.
'um event ack <event-ids>'	하나 이상의 이벤트를 승인합니다.	해당 메시지를 표시합니다.
'<event-ids>'um event resolve<event-ids>'	하나 이상의 이벤트를 확인합니다.	해당 메시지를 표시합니다.
'<사용자 이름><event-id>' 이벤트가 발생합니다	사용자에게 이벤트를 할당합니다.	해당 메시지를 표시합니다.

CLI 명령	설명	출력
'<um event list[-s<source>][-S<event-state-filter-list>.] [<event-id>.]	시스템 또는 사용자가 생성한 이벤트를 나열합니다. 소스, 상태 및 ID를 기준으로 이벤트를 필터링합니다.	표 형식 '소스, 소스 유형, 이름, 심각도, 상태'로 다음 값을 표시합니다. User and Timestamp'(사용자 및 타임스탬프)를 선택합니다.
'um backup restore -f <backup_file_path_and_name>'	7z 파일을 사용하여 MySQL 데이터베이스 백업을 복원합니다.	해당 메시지를 표시합니다.

스크립트 창 및 대화 상자에 대한 설명입니다

스크립트 페이지에서는 Unified Manager에 스크립트를 추가할 수 있습니다.

스크립트 페이지

스크립트 페이지에서는 Unified Manager에 사용자 지정 스크립트를 추가할 수 있습니다. 이러한 스크립트를 경고와 연결하여 스토리지 객체를 자동으로 재구성할 수 있습니다.

스크립트 페이지에서는 Unified Manager에서 스크립트를 추가하거나 삭제할 수 있습니다.

명령 버튼

- * 추가 *

  스크립트를 추가할 수 있는 스크립트 추가 대화 상자를 표시합니다.

- * 삭제 *

  선택한 스크립트를 삭제합니다.

목록 보기

목록 보기에는 Unified Manager에 추가한 스크립트가 표 형식으로 표시됩니다.

- * 이름 *

  스크립트의 이름을 표시합니다.

- * 설명 *

  스크립트에 대한 설명을 표시합니다.

스크립트 추가 대화 상자

스크립트 추가 대화 상자에서 Unified Manager에 스크립트를 추가할 수 있습니다. 스토리지 객체에 대해 생성된 이벤트를 자동으로 확인하도록 스크립트로 알림을 구성할 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

- * 스크립트 파일 * 을 선택합니다

  경고에 대한 스크립트를 선택할 수 있습니다.

- * 설명 *

  스크립트에 대한 설명을 지정할 수 있습니다.

클러스터 성능을 모니터링하고 관리합니다

Active IQ Unified Manager 성능 모니터링 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)은 NetApp ONTAP 소프트웨어를 실행하는 시스템에 대한 성능 모니터링 기능 및 이벤트 근본 원인 분석을 제공합니다.

Unified Manager를 사용하면 클러스터 구성 요소를 과도하게 사용하는 워크로드를 식별하고 클러스터에서 다른 워크로드의 성능을 줄일 수 있습니다. 성능 임계값 정책을 정의하여 특정 성능 카운터의 최대값을 지정하여 임계값이 위반될 때 이벤트가 생성되도록 할 수도 있습니다. Unified Manager를 사용하면 이러한 성능 이벤트를 경고하여 수정 조치를 취하고 성능을 정상 작동 수준으로 높일 수 있습니다. Unified Manager UI에서 이벤트를 보고 분석할 수 있습니다.

Unified Manager에서 두 가지 유형의 워크로드 성능을 모니터링합니다.

- 사용자 정의 워크로드

  이러한 워크로드는 클러스터에서 생성한 FlexVol 볼륨과 FlexGroup 볼륨으로 구성됩니다.

- 시스템 정의 워크로드

  이러한 워크로드는 내부 시스템 작업으로 구성됩니다.

Unified Manager 성능 모니터링 기능

Unified Manager는 ONTAP 소프트웨어를 실행하는 시스템에서 성능 통계를 수집하고 분석합니다. 동적 성능 임계값과 사용자 정의 성능 임계값을 사용하여 많은 클러스터 구성 요소에 대해 다양한 성능 카운터를 모니터링합니다.

응답 시간(지연 시간)이 높으면 예를 들어, 스토리지 객체(예: 볼륨)가 정상보다 느리게 작동하고 있음을 나타냅니다. 또한 이 문제는 볼륨을 사용하는 클라이언트 응용 프로그램의 성능이 저하되었음을 나타냅니다. Unified Manager는 성능 문제가 있는 스토리지 구성요소를 식별하고 성능 문제를 해결하기 위해 수행할 수 있는 권장 조치 목록을 제공합니다.

Unified Manager에는 다음과 같은 기능이 포함되어 있습니다.

- ONTAP 소프트웨어를 실행하는 시스템에서 워크로드 성능 통계를 모니터링 및 분석합니다.
- 클러스터, 노드, 애그리게이트, 포트, SVM에 대한 성능 카운터 추적 볼륨, LUN, NVMe 네임스페이스 및 네트워크 인터페이스(LIF)
- IOPS(작업), MB/s(처리량), 지연 시간(응답 시간), 사용률, 성능 용량 및 캐시 비율입니다.
- 임계값을 위반할 때 이벤트를 트리거하고 이메일 경고를 보내는 사용자 정의 성능 임계값 정책을 생성할 수 있습니다.
- 시스템 정의 임계값과 동적 성능 임계값을 사용하여 워크로드 활동을 파악하고 성능 문제를 알립니다.
- 볼륨 및 LUN에 적용되는 QoS(서비스 품질) 정책 및 PSL(성능 서비스 수준 정책)을 식별합니다.
- 경합 중인 클러스터 구성 요소를 명확하게 식별합니다.

- 클러스터 구성 요소를 과도하게 사용하는 워크로드 및 늘어난 활동에 의해 성능이 영향을 받는 워크로드를 식별합니다.

스토리지 시스템 성능을 관리하는 데 사용되는 **Unified Manager** 인터페이스

이 섹션에는 Active IQ Unified Manager에서 데이터 스토리지 용량, 가용성 및 보호 문제를 해결하기 위해 제공하는 두 가지 사용자 인터페이스에 대한 정보가 포함되어 있습니다. UI 두 개는 Unified Manager 웹 UI와 유지보수 콘솔입니다.

Unified Manager의 보호 기능을 사용하려면 WFA(OnCommand Workflow Automation)도 설치 및 구성해야 합니다.

Unified Manager 웹 **UI**

관리자는 Unified Manager 웹 UI를 사용하여 데이터 스토리지 용량, 가용성 및 보호와 관련된 클러스터 문제를 모니터링하고 해결할 수 있습니다.

다음 섹션에서는 관리자가 Unified Manager 웹 UI에 표시되는 스토리지 용량, 데이터 가용성 또는 보호 문제를 해결하기 위해 수행할 수 있는 몇 가지 일반적인 워크플로우에 대해 설명합니다.

유지보수 콘솔

관리자는 Unified Manager 유지보수 콘솔을 사용하여 Unified Manager 서버 자체와 관련된 운영 체제 문제, 버전 업그레이드 문제, 사용자 액세스 문제, 네트워크 문제를 모니터링, 진단, 해결할 수 있습니다. Unified Manager 웹 UI를 사용할 수 없는 경우에는 유지보수 콘솔만 Unified Manager에 액세스할 수 있습니다.

이 정보를 사용하여 유지보수 콘솔에 액세스하고 Unified Manager 서버 기능과 관련된 문제를 해결할 수 있습니다.

클러스터 구성 및 성능 데이터 수집 작업

클러스터 구성 data_의 수집 간격은 15분입니다. 예를 들어, 클러스터를 추가한 후에는 15분 이내에 Unified Manager UI에 클러스터 세부 정보를 표시할 수 있습니다. 이 간격은 클러스터에 대한 변경에도 적용됩니다.

예를 들어, 클러스터의 SVM에 새 볼륨 2개를 추가하는 경우 다음 폴링 간격 후 UI에서 새로운 객체를 볼 수 있으며 이는 최대 15분이 될 수 있습니다.

Unified Manager는 5분마다 모니터링되는 모든 클러스터에서 current_performance 통계를 수집합니다. 이 데이터를 분석하여 성능 이벤트 및 잠재적 문제를 식별합니다. 또한 30일 동안 5분 동안의 기간별 성능 데이터와 180일 동안의 기간별 성능 데이터를 유지합니다. 이를 통해 현재 달의 매우 세부적인 성능 세부 정보와 최대 1년의 일반적인 성능 추세를 볼 수 있습니다.

컬렉션 폴은 몇 분 간격으로 오프셋되므로 모든 클러스터의 데이터가 동시에 전송되지 않아 성능에 영향을 줄 수 있습니다.

다음 표에서는 Unified Manager가 수행하는 수집 활동에 대해 설명합니다.

활동입니다	시간 간격입니다	설명
성능 통계 폴링	5분마다	각 클러스터에서 실시간 성능 데이터 수집

활동입니다	시간 간격입니다	설명
통계 분석	5분마다	모든 통계 폴링 후에 Unified Manager는 수집된 데이터를 사용자 정의, 시스템 정의 및 동적 임계값과 비교합니다. 성능 임계값이 위반된 경우 Unified Manager는 이벤트를 생성하고 지정된 사용자에게 해당 e-메일을 보냅니다(구성된 경우).
구성 폴링	15분마다	각 클러스터에서 세부 인벤토리 정보를 수집하여 모든 스토리지 오브젝트(노드, SVM, 볼륨 등)를 식별합니다.
요약	매시간	에서는 최신 12개의 5분 성능 데이터 컬렉션을 시간별 평균으로 요약합니다. 매시간 평균 값은 일부 UI 페이지에서 사용되며 180일 동안 유지됩니다.
예측 분석 및 데이터 정리	매일 자정이 지나면	클러스터 데이터를 분석하여 향후 24시간 동안 볼륨 지연 시간 및 IOPS에 대한 동적 임계값을 설정합니다. 30일이 지난 5분 동안의 성능 데이터를 데이터베이스에서 삭제합니다.
데이터 잘라내기	매일 오전 2시 이후	180일이 지난 이벤트 및 180일이 지난 동적 임계값을 데이터베이스에서 삭제합니다.
데이터 잘라내기	매일 오전 3시 30분 이후	180일이 지난 1시간 동안의 성능 데이터를 데이터베이스에서 삭제합니다.

데이터 연속성 수집 주기는 얼마입니까

데이터 연속성 수집 주기는 기본적으로 5분마다 실행되는 실시간 클러스터 성능 수집 주기를 벗어나 성능 데이터를 검색합니다. Unified Manager는 데이터 연속성 컬렉션을 통해 실시간 데이터를 수집할 수 없을 때 발생하는 통계 데이터의 격차를 해소합니다.

Unified Manager는 다음과 같은 이벤트가 발생할 경우 기간별 성능 데이터에 대한 데이터 연속성 수집 폴링을 수행합니다.

- 클러스터는 처음에 Unified Manager에 추가됩니다.

  Unified Manager는 이전 15일 동안의 기간별 성능 데이터를 수집합니다. 따라서 클러스터를 추가한 후 몇 시간 이내에 클러스터에 대한 2주간의 기간별 성능 정보를 볼 수 있습니다.

  또한 시스템 정의 임계값 이벤트가 있는 경우 이전 기간에 대해 보고됩니다.

- 현재 성능 데이터 수집 주기가 정해진 시간에 완료되지 않습니다.

  실시간 성능 폴링이 5분 수집 기간을 초과할 경우 데이터 연속성 수집 주기가 시작되어 누락된 정보를 수집합니다. Data Continuity 수집 기능이 없으면 다음 수집 기간을 건너뜁니다.

- Unified Manager는 일정 기간 동안 액세스할 수 없었던 적이 있으며 다음과 같은 상황에서 온라인 상태로 돌아갑니다.
  - 다시 시작되었습니다.
  - 소프트웨어 업그레이드 또는 백업 파일 생성 중에 종료되었습니다.
  - 네트워크 중단이 복구됩니다.
- 클러스터가 일정 기간 동안 액세스할 수 없게 된 경우 다음과 같은 상황에서 온라인 상태로 돌아갑니다.
  - 네트워크 중단이 복구됩니다.
  - WAN 연결이 느리면 정상적인 성능 데이터 수집이 지연됩니다.

데이터 연속성 수집 주기는 최대 24시간의 기록 데이터를 수집할 수 있습니다. Unified Manager가 24시간 이상 중단된 경우, UI 페이지에 성능 데이터의 차이가 나타납니다.

데이터 연속성 수집 주기와 실시간 데이터 수집 주기를 동시에 실행할 수 없습니다. 실시간 성능 데이터 수집이 시작되기 전에 데이터 연속성 수집 주기를 완료해야 합니다. 1시간 이상의 기록 데이터를 취합하기 위해 데이터 연속성 수집이 필요한 경우 알림 창 맨 위에 해당 클러스터의 배너 메시지가 표시됩니다.

수집된 데이터 및 이벤트에서 타임스탬프가 의미하는 것입니다

수집된 상태 및 성능 데이터에 표시되거나 이벤트 감지 시간으로 표시되는 타임스탬프는 ONTAP 클러스터 시간을 기반으로 하며 웹 브라우저에 설정된 표준 시간대로 조정됩니다.

NTP(네트워크 시간 프로토콜) 서버를 사용하여 Unified Manager 서버, ONTAP 클러스터 및 웹 브라우저의 시간을 동기화하는 것이 좋습니다.

특정 클러스터에 대해 타임스탬프가 잘못된 것으로 표시되는 경우 클러스터 시간이 올바르게 설정되었는지 확인할 수 있습니다.

Unified Manager GUI에서 성능 워크플로우 탐색

Unified Manager 인터페이스는 성능 정보를 수집하고 표시하기 위한 여러 페이지를 제공합니다. 왼쪽 탐색 패널을 사용하여 GUI의 페이지로 이동하고 페이지의 탭과 링크를 사용하여 정보를 보고 구성할 수 있습니다.

다음 페이지를 모두 사용하여 클러스터 성능 정보를 모니터링하고 문제를 해결할 수 있습니다.

- 대시보드 페이지
- 스토리지 및 네트워크 객체 인벤토리 페이지
- 스토리지 객체 세부 정보 페이지(성능 탐색기 포함)
- 구성 및 설정 페이지
- 이벤트 페이지

UI에 로그인합니다

지원되는 웹 브라우저를 사용하여 Unified Manager UI에 로그인할 수 있습니다.

- 필요한 것 *
- 웹 브라우저는 최소 요구 사항을 충족해야 합니다.

  에서 상호 운용성 매트릭스 를 참조하십시오 "mysupport.netapp.com/matrix" 를 참조하십시오.

- Unified Manager 서버의 IP 주소 또는 URL이 있어야 합니다.

1시간 동안 사용하지 않으면 세션에서 자동으로 로그아웃됩니다. 이 기간은 * 일반 * > * 기능 설정 * 에서 구성할 수 있습니다.

단계

1. 웹 브라우저에 URL을 입력합니다. 여기서 URL은 Unified Manager 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다.
   - IPv4의 경우: "https://URL/`
   - IPv6의 경우:'https://[URL]/`

서버에서 자체 서명된 디지털 인증서를 사용하는 경우 브라우저에서 인증서를 신뢰할 수 없다는 경고를 표시할 수 있습니다. 액세스를 계속할 위험을 확인하거나 서버 인증을 위해 CA(인증 기관) 서명 디지털 인증서를 설치할 수 있습니다. . 로그인 화면에서 사용자 이름과 암호를 입력합니다.

SAML 인증을 사용하여 Unified Manager 사용자 인터페이스에 로그인할 수 있는 경우 Unified Manager 로그인 페이지 대신 IdP(Identity Provider) 로그인 페이지에 자격 증명을 입력합니다.

대시보드 페이지가 표시됩니다.

Unified Manager 서버가 초기화되지 않은 경우 새 브라우저 창에 첫 번째 환경 마법사가 표시됩니다. 이메일 알림을 보낼 초기 이메일 수신자, 이메일 통신을 처리할 SMTP 서버, AutoSupport가 Unified Manager 설치에 대한 정보를 기술 지원 부서에 보낼 수 있도록 설정되어 있는지 여부를 입력해야 합니다. 이 정보를 완료하면 Unified Manager UI가 나타납니다.

그래픽 인터페이스 및 탐색 경로

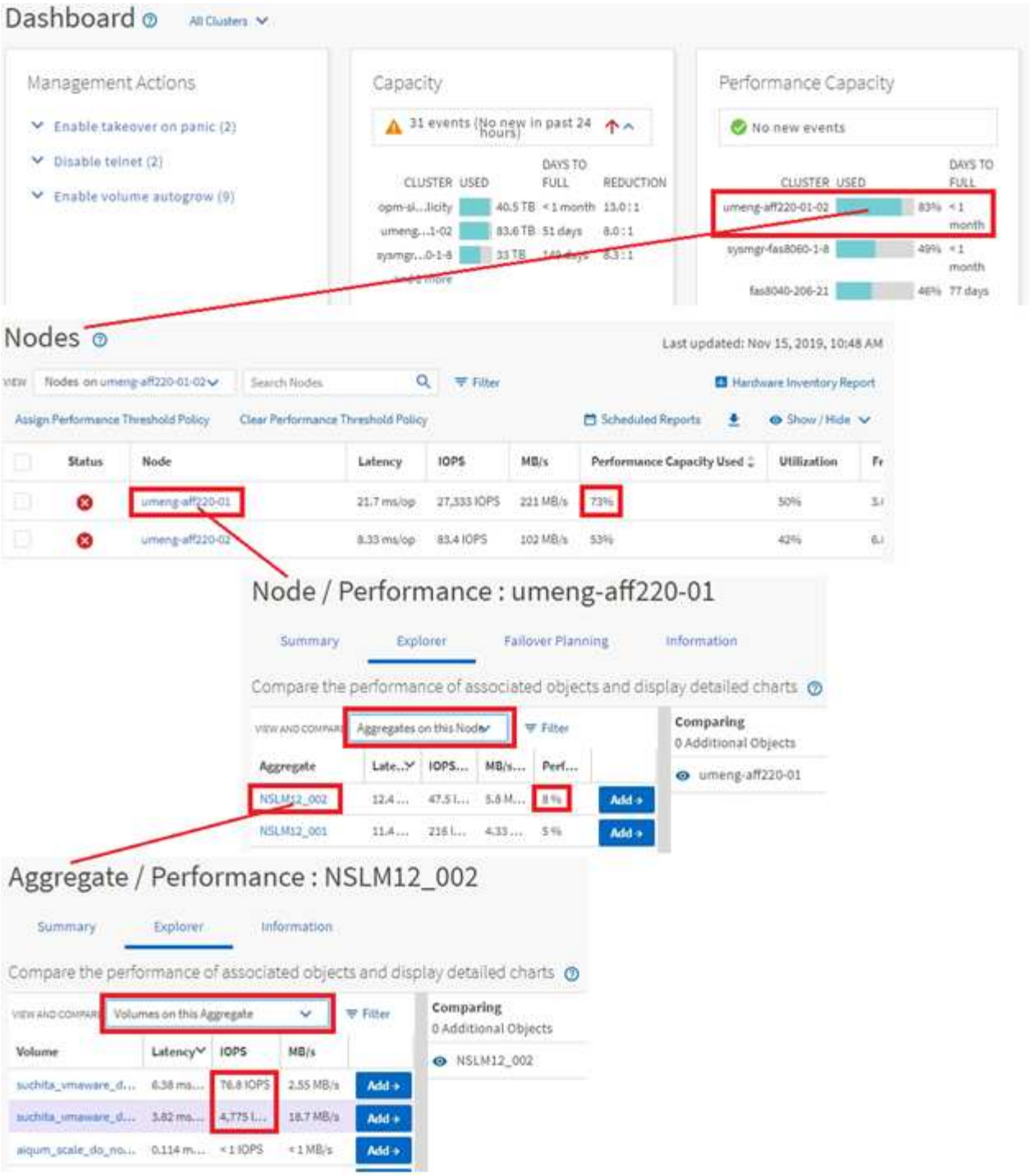
Unified Manager는 유연성이 탁월하며 다양한 방법으로 여러 작업을 수행할 수 있습니다. Unified Manager에서 작업하는 경우 다양한 탐색 경로를 찾을 수 있습니다. 가능한 모든 탐색 조합을 표시할 수 있는 것은 아니지만 몇 가지 일반적인 시나리오에 익숙해야 합니다.

Unified Manager가 관리하는 모든 클러스터의 모든 개체의 성능을 모니터링할 수 있습니다. 스토리지 객체를 모니터링하면 클러스터 및 객체 성능에 대한 개요와 성능 이벤트 모니터링 기능을 제공합니다. 성능과 이벤트를 한 수준 높게 보거나 개체 성능 및 성능 이벤트에 대한 세부 정보를 추가로 조사할 수 있습니다.

다음은 가능한 여러 클러스터 객체 탐색의 한 예입니다.

1. 대시보드 페이지에서 Performance Capacity 패널의 세부 정보를 검토하여 가장 높은 성능 용량을 사용하는 클러스터를 식별하고 막대 차트를 클릭하여 해당 클러스터의 노드 목록으로 이동합니다.
2. 사용된 성능 용량이 가장 높은 노드를 식별하고 해당 노드를 클릭합니다.
3. 노드/성능 탐색기 페이지의 보기 및 비교 메뉴에서 이 노드의 * 집계 * 를 클릭합니다.
4. 가장 높은 성능 용량을 사용하고 있는 애그리게이트를 파악하고 해당 애그리게이트를 클릭합니다.
5. 집계/성능 탐색기 페이지의 보기 및 비교 메뉴에서 * 이 집계 볼륨 * 을 클릭합니다.
6. 가장 높은 IOPS를 사용하는 볼륨을 식별합니다.

이러한 볼륨을 조사하여 QoS 정책 또는 성능 서비스 수준 정책을 적용해야 하는지 또는 정책 설정을 변경해야 하는지 여부를 확인해야 합니다. 그래야 해당 볼륨에서 클러스터의 IOPS가 크게 사용되지 않습니다.



클러스터 성능 탐색을 모니터링합니다

Unified Manager에서 관리하는 모든 클러스터의 성능을 모니터링할 수 있습니다. 클러스터 모니터링은 클러스터 및 오브젝트 성능에 대한 개요를 제공하고 성능 이벤트 모니터링을 포함합니다. 성능 및 이벤트를 높은 수준에서 확인하거나 클러스터 및 오브젝트 성능 및 성능 이벤트에 대한 세부 정보를 자세히 조사할 수 있습니다.

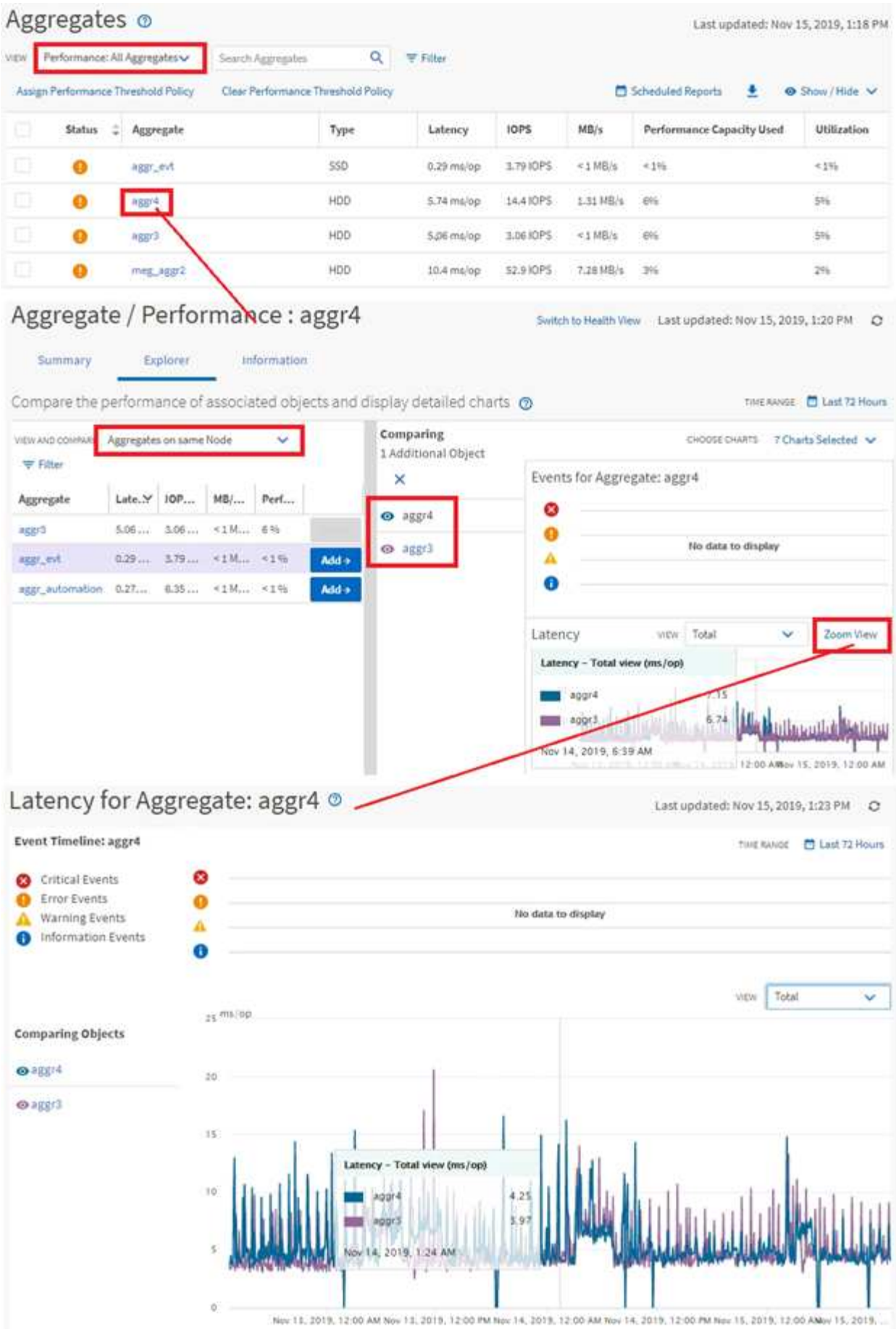
다음은 가능한 여러 클러스터 성능 탐색 경로의 한 가지 예입니다.

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.

2. 해당 애그리게이트의 성능에 대한 정보를 보려면 Performance: All 애그리게이트 뷰를 선택합니다.
3. 조사할 집계 이름을 확인하고 해당 집계 이름을 클릭하여 집계/성능 탐색기 페이지로 이동합니다.
4. 필요한 경우 보기 및 비교 메뉴에서 이 집계와 비교할 다른 개체를 선택한 다음 비교 창에 개체 중 하나를 추가합니다.

   두 객체에 대한 통계가 비교를 위해 카운터 차트에 표시됩니다.

5. 탐색기 페이지 오른쪽의 비교 창에서 카운터 차트 중 하나에서 * 확대/축소 보기 * 를 클릭하여 해당 애그리게이트의 성능 기록에 대한 세부 정보를 봅니다.


Aggregates
Last updated: Nov 15, 2019, 1:18 PM
VIEW
Performance: All Aggregates
Search Aggregates
Filter
Assign Performance Threshold Policy
Clear Performance Threshold Policy
Scheduled Reports
Show / Hide
Status
Aggregate
Type
Latency
IOPS
MB/s
Performance Capacity Used
Utilization
aggr_evt
SSD
0.29 ms/op
3.79 IOPS
< 1 MB/s
< 1%
aggr4
HDD
5.74 ms/op
14.4 IOPS
1.31 MB/s
6%
5%
aggr3
HDD
5.06 ms/op
3.06 IOPS
< 1 MB/s
6%
5%
meg_aggr2
HDD
10.4 ms/op
52.9 IOPS
7.28 MB/s
3%
2%
Aggregate / Performance : aggr4
Switch to Health View
Last updated: Nov 15, 2019, 1:20 PM
Summary
Explorer
Information
Compare the performance of associated objects and display detailed charts
TIME RANGE
Last 72 Hours
VIEW AND COMPARE
Aggregates on same Node
Filter
Aggregate
Late...
IOP...
MB/...
Perf...
aggr3
5.06 ...
3.06 ...
< 1 M...
6 %
aggr_evt
0.29 ...
3.79 ...
< 1 M...
< 1 %
Add
aggr_automation
0.27...
6.35 ...
< 1 M...
< 1 %
Add
Comparing
1 Additional Object
CHOOSE CHARTS
7 Charts Selected
aggr4
aggr3
Events for Aggregate: aggr4
No data to display
Latency
VIEW
Total
Zoom View
Latency – Total view (ms/op)
aggr4
7.15
aggr3
6.74
Nov 14, 2019, 6:39 AM
12:00 AM
Nov 15, 2019, 12:00 AM
Latency for Aggregate: aggr4
Last updated: Nov 15, 2019, 1:23 PM
Event Timeline: aggr4
TIME RANGE
Last 72 Hours
Critical Events
Error Events
Warning Events
Information Events
No data to display
VIEW
Total
Comparing Objects
aggr4
aggr3
25
ms/op
20
15
10
5
0
Latency – Total view (ms/op)
aggr4
4.25
aggr3
3.97
Nov 14, 2019, 1:24 AM
Nov 13, 2019, 12:00 AM
Nov 13, 2019, 12:00 PM
Nov 14, 2019, 12:00 AM
Nov 14, 2019, 12:00 PM
Nov 15, 2019, 12:00 AM
Nov 15, 2019,

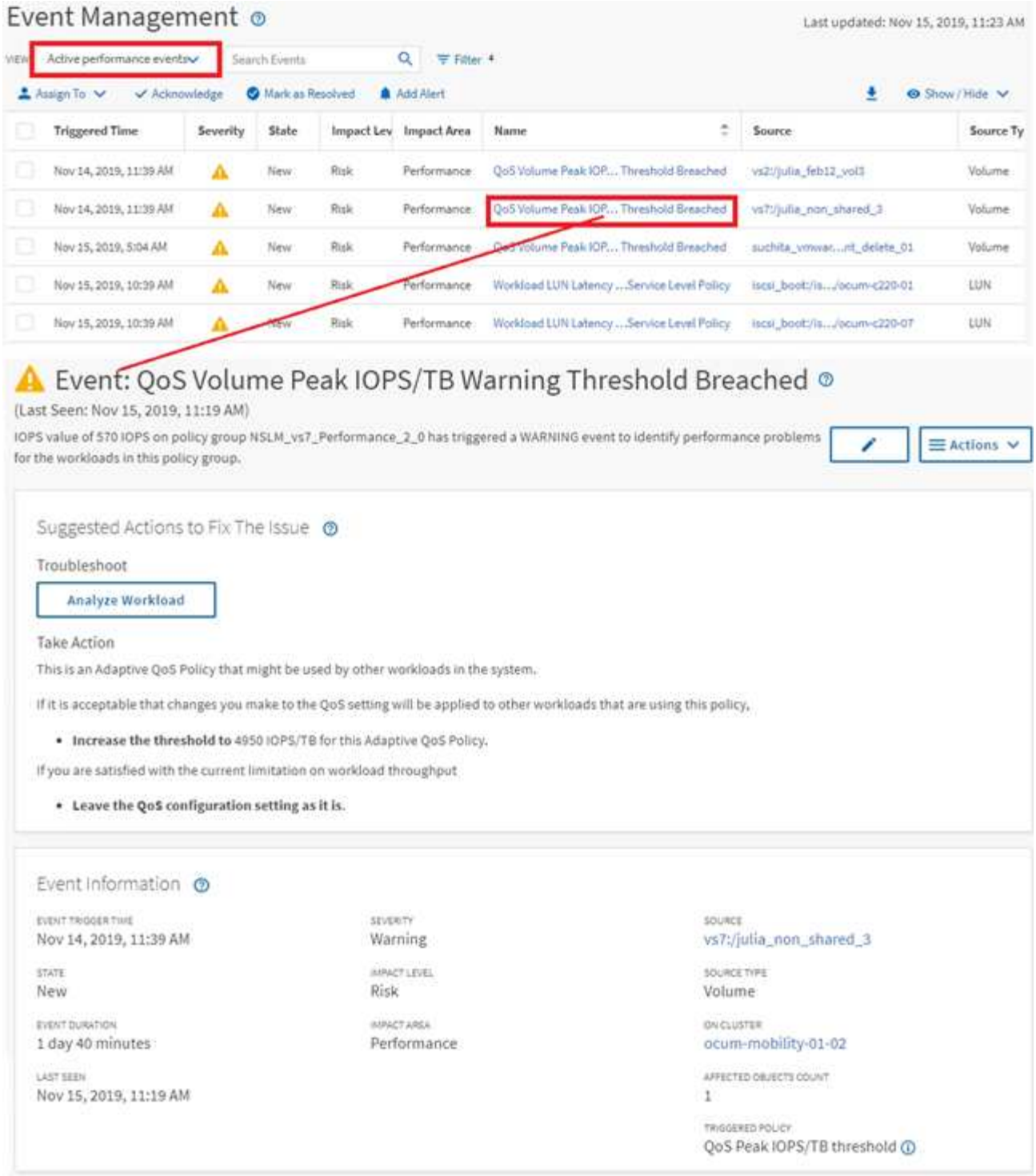
Unified Manager 이벤트 세부 정보 페이지에서는 성능 이벤트에 대한 세부 정보를 제공합니다. 이 기능은 성능 이벤트, 문제 해결 및 시스템 성능 미세 조정 시 유용합니다.

성능 이벤트 유형에 따라 두 가지 유형의 이벤트 세부 정보 페이지 중 하나가 표시될 수 있습니다.

- 사용자 정의 임계값 및 시스템 정의 임계값 정책 이벤트에 대한 이벤트 세부 정보 페이지입니다
- 동적 임계값 정책 이벤트에 대한 이벤트 세부 정보 페이지입니다

다음은 이벤트 조사 탐색의 한 예입니다.

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.
2. 보기 메뉴에서 * 활성 성능 이벤트 * 를 클릭합니다.
3. 조사할 이벤트의 이름을 클릭하면 이벤트 세부 정보 페이지가 표시됩니다.
4. 이벤트에 대한 설명 을 보고 제안 조치(있는 경우)를 검토하여 문제 해결에 도움이 될 수 있는 이벤트에 대한 자세한 정보를 봅니다. 분석 워크로드 * 버튼을 클릭하여 상세한 성능 차트를 표시하여 문제를 보다 상세하게 분석할 수 있습니다.



스토리지 객체를 검색하는 중입니다

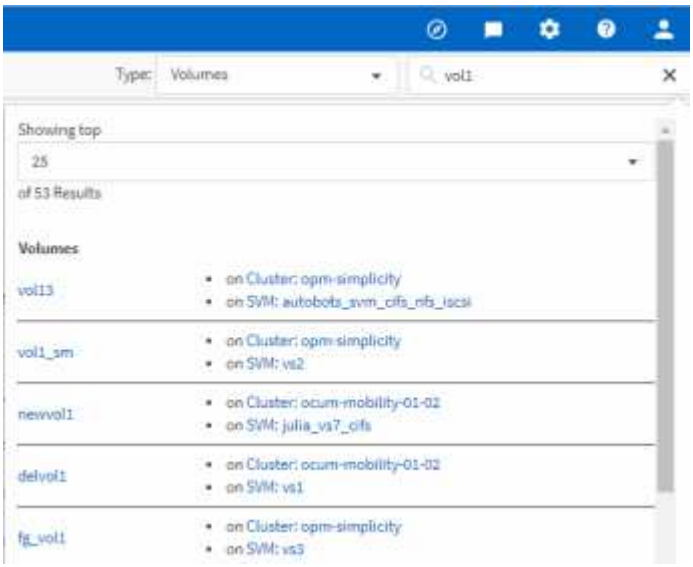
특정 개체에 빠르게 액세스하려면 메뉴 모음 맨 위에 있는 * 모든 스토리지 개체 검색 * 필드를 사용합니다. 모든 개체에 대해 이 전역 검색 방법을 사용하면 유형별로 특정 개체를 빠르게 찾을 수 있습니다. 검색 결과는 스토리지 객체 유형별로 정렬되며 드롭다운 메뉴를 사용하여 필터링할 수 있습니다. 유효한 검색에는 3자 이상의 문자가 포함되어야 합니다.

전체 검색에는 총 결과 수가 표시되지만 상위 25개 검색 결과만 액세스할 수 있습니다. 따라서 빠르게 찾을 항목을 알고 있으면 전역 검색 기능을 특정 항목을 찾는 바로 가기 도구로 생각할 수 있습니다. 전체 검색 결과의 경우 객체 재고

페이지 및 관련 필터링 기능을 사용하여 검색할 수 있습니다.

드롭다운 상자를 클릭하고 * All * 을 선택하여 모든 오브젝트 및 이벤트를 동시에 검색할 수 있습니다. 또는 드롭다운 상자를 클릭하여 개체 유형을 지정할 수 있습니다. 모든 스토리지 객체 검색 * 필드에 객체 또는 이벤트 이름의 최소 3자를 입력한 다음 * Enter * 를 눌러 다음과 같은 검색 결과를 표시합니다.

- 클러스터:클러스터 이름
- 노드:노드 이름
- 애그리게이트: 애그리게이트 이름
- SVM: SVM 이름
- 볼륨: 볼륨 이름
- LUN: LUN 경로



LIF 및 포트는 글로벌 검색 창에서 검색할 수 없습니다.

이 예제에서 드롭다운 상자에는 볼륨 개체 유형이 선택되어 있습니다. Search All Storage Objects * 필드에 ""vol""을 입력하면 이름에 해당 문자가 포함된 모든 볼륨 목록이 표시됩니다. 개체 검색의 경우 검색 결과를 클릭하여 해당 개체의 성능 탐색기 페이지로 이동할 수 있습니다. 이벤트 검색의 경우 검색 결과에서 항목을 클릭하면 이벤트 세부 정보 페이지로 이동합니다.

재고 페이지 콘텐츠 필터링

Unified Manager에서 인벤토리 페이지 데이터를 필터링하여 특정 기준에 따라 데이터를 빠르게 찾을 수 있습니다. 필터링을 사용하면 Unified Manager 페이지의 콘텐츠 범위를 좁혀 원하는 결과만 표시할 수 있습니다. 따라서 관심 있는 데이터만 표시하는 매우 효율적인 방법이 제공됩니다.

필터링 * 을 사용하여 기본 설정에 따라 그리드 보기를 사용자 정의합니다. 사용 가능한 필터 옵션은 격자에서 보는 개체 유형을 기반으로 합니다. 필터가 현재 적용된 경우 필터 단추 오른쪽에 적용된 필터 수가 표시됩니다.

세 가지 유형의 필터 매개 변수가 지원됩니다.

매개 변수	검증
문자열(텍스트)	연산자는 * 포함 *, * 다음으로 시작 *, * 로 끝 *, * 포함하지 않음 * 입니다.
번호	연산자는 * 보다 * 큼, * 보다 작음 *, * 마지막 * 에서 * 사이 * 입니다.
Enum(텍스트)	연산자는 * 이고 * 는 * 입니다.

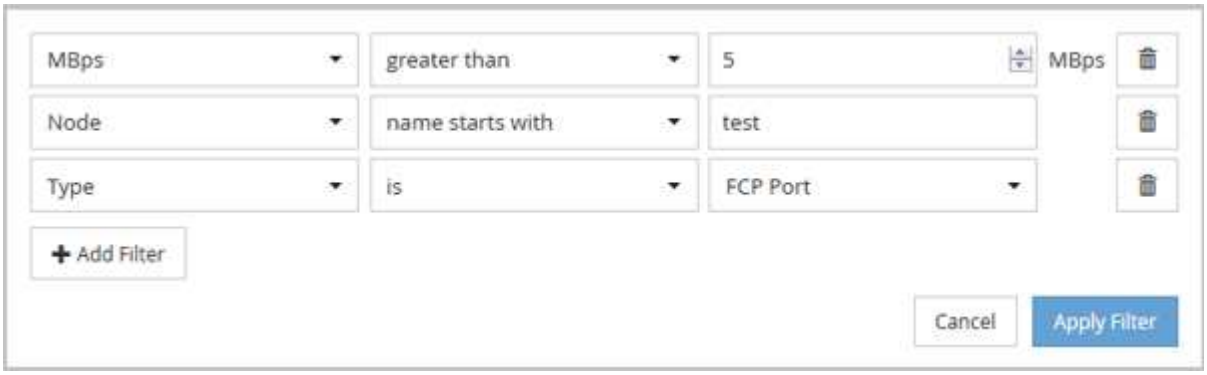
각 필터에는 열, 연산자 및 값 필드가 필요합니다. 사용 가능한 필터는 현재 페이지의 필터링 가능한 열을 반영합니다. 적용할 수 있는 최대 필터 수는 4개입니다. 필터링된 결과는 결합된 필터 매개 변수를 기반으로 합니다. 필터링된 결과는 현재 표시된 페이지뿐만 아니라 필터링된 검색의 모든 페이지에 적용됩니다.

필터링 패널을 사용하여 필터를 추가할 수 있습니다.

1. 페이지 맨 위에서 * 필터 * 버튼을 클릭합니다. Filtering(필터링) 패널이 표시됩니다.
2. 왼쪽 드롭다운 목록을 클릭하고 개체를 선택합니다(예: *Cluster* 또는 성능 카운터).
3. 가운데 드롭다운 목록을 클릭하고 사용할 연산자를 선택합니다.
4. 마지막 목록에서 값을 선택하거나 입력하여 해당 개체에 대한 필터를 완료합니다.
5. 다른 필터를 추가하려면 * + 필터 추가 * 를 클릭합니다. 추가 필터 필드가 표시됩니다. 위의 단계에 설명된 프로세스를 사용하여 이 필터를 완료합니다. 네 번째 필터를 추가하면 * + 필터 추가 * 버튼이 더 이상 표시되지 않습니다.
6. 필터 적용 * 을 클릭합니다. 필터 옵션이 그리드에 적용되고 필터 버튼 오른쪽에 필터 수가 표시됩니다.
7. 필터 패널을 사용하여 제거할 필터의 오른쪽에 있는 휴지통 아이콘을 클릭하여 개별 필터를 제거합니다.
8. 모든 필터를 제거하려면 필터링 패널 하단에 있는 * Reset * (재설정 *)을 클릭합니다.

필터링 예제

그림에는 3개의 필터가 있는 필터링 패널이 나와 있습니다. 최대 4개 이하의 필터가 있는 경우 * + 필터 추가 * 버튼이 표시됩니다.



필터 적용 * 을 클릭하면 필터링 패널이 닫히고 필터가 적용되고 적용된 필터 수가 표시됩니다(3)를 클릭합니다.

대시보드에서 클러스터 성능 모니터링

Unified Manager 대시보드에서는 이 Unified Manager 인스턴스에서 모니터링하는 모든 클러스터의 높은 성능 상태를 표시하는 몇 가지 패널을 제공합니다. 이를 통해 관리되는 클러스터의 전반적인 성능을 평가하고 식별된 특정 이벤트를 신속하게 확인, 검색 또는 할당할 수 있습니다.

대시보드의 성능 패널 이해

Unified Manager 대시보드에서는 사용자 환경에서 모니터링 중인 모든 클러스터의 고성능 상태를 표시하는 몇 가지 패널을 제공합니다. 모든 클러스터 또는 개별 클러스터의 상태를 볼 수 있습니다.

성능 정보를 표시하는 것 외에도 대부분의 패널에는 해당 범주의 활성 이벤트 수와 이전 24시간 동안 추가된 새 이벤트 수가 표시됩니다. 이 정보는 보고된 이벤트를 해결하기 위해 더 자세히 분석해야 할 클러스터를 결정하는 데 도움이 됩니다. 이벤트를 클릭하면 상위 몇 개의 이벤트가 표시되고 해당 범주의 이벤트를 표시하도록 필터링된 이벤트 관리 인벤토리 페이지로 연결되는 링크가 제공됩니다.

다음 패널은 성능 상태를 제공합니다.

- * 성능 용량 패널 *

  모든 클러스터를 볼 때 이 패널에는 각 클러스터의 성능 용량 값(이전 1시간 동안의 평균 성능)과 성능 용량이 상한에 도달할 때까지 남은 일 수(일별 성장률 기준)가 표시됩니다. 막대 차트를 클릭하면 해당 클러스터의 노드 인벤토리 페이지로 이동합니다. 노드 인벤토리 페이지에는 이전 72시간 동안의 평균 성능 용량이 표시되므로 이 값이 대시보드 값과 일치하지 않을 수 있습니다.

  단일 클러스터를 볼 때 이 패널에는 클러스터 성능 용량, 총 IOPS 및 총 처리량 값이 표시됩니다.

- * 워크로드 IOPS 패널 *

  워크로드 활성 관리가 활성화되고 단일 클러스터를 볼 때 이 패널에는 특정 IOPS 범위에서 현재 실행 중인 총 워크로드 수가 표시됩니다.

- * 워크로드 성능 패널 *

  워크로드 활성 관리가 활성화된 경우 이 패널에는 정의된 각 성능 서비스 수준에 할당된 준수 및 부적합 워크로드의 총 수가 표시됩니다. 막대 차트를 클릭하면 워크로드 페이지에서 해당 정책에 할당된 워크로드로 이동합니다.

- * 사용 개요 패널 *

  모든 클러스터를 볼 때 가장 높은 IOPS 또는 처리량(MB/s)별로 정렬된 클러스터를 표시하도록 선택할 수 있습니다.

  단일 클러스터를 볼 때 해당 클러스터의 워크로드를 가장 높은 IOPS 또는 처리량(MB/s)별로 정렬하도록 선택할 수 있습니다.

성능 배너 메시지 및 설명

Unified Manager에서 알림 페이지(알림 벨)에 배너 메시지를 표시하여 특정 클러스터의 상태

문제를 알릴 수 있습니다.

배너 메시지입니다	설명	해상도
"cluster_cluster_name_에서 성능 데이터가 수집되지 않습니다. 이 문제를 해결하려면 Unified Manager를 다시 시작하십시오	Unified Manager 컬렉션 서비스가 중지되었으며 어떠한 클러스터에서도 성능 데이터가 수집되고 있지 않습니다.	이 문제를 해결하려면 Unified Manager를 다시 시작하십시오. 이렇게 해도 문제가 해결되지 않으면 기술 지원 부서에 문의하십시오.
Cluster_cluster_name_에서 기록 데이터가 x 시간 이상 수집되고 있습니다. 현재 데이터 수집은 모든 기록 데이터가 수집된 후에 시작됩니다	실시간 클러스터 성능 수집 주기 외부에서 성능 데이터를 검색하기 위해 현재 데이터 연속성 수집 주기가 실행되고 있습니다.	별도의 조치가 필요하지 않습니다. 데이터 연속성 수집 주기가 완료된 후 현재 성능 데이터가 수집됩니다. 데이터 연속성 수집 주기는 새 클러스터가 추가되거나 Unified Manager에서 어떤 이유로 현재 성능 데이터를 수집할 수 없을 때 실행됩니다.

성능 통계 수집 주기 변경

성능 통계에 대한 기본 수집 간격은 5분입니다. 대규모 클러스터의 컬렉션이 기본 시간 내에 마중되지 않으면 이 간격을 10 또는 15분으로 변경할 수 있습니다. 이 설정은 Unified Manager의 이 인스턴스가 모니터링하는 모든 클러스터의 통계 모음에 영향을 줍니다.

- 필요한 것 *

Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.

성능 통계 수집 시간이 정시에 마무리되지 않는 문제는 "Unable to s일관되게 collect from cluster <cluster_name>" 배너 메시지 또는 "data collection is too long long long on cluster <cluster_name>"으로 표시됩니다.

통계 수집 문제로 인해 필요한 경우에만 수집 간격을 변경해야 합니다. 다른 이유로 이 설정을 변경하지 마십시오.

이 값을 5분의 기본 설정에서 변경하면 Unified Manager에서 보고하는 성능 이벤트의 수와 빈도에 영향을 줄 수 있습니다. 예를 들어, 시스템 정의 성능 임계값은 정책이 30분 동안 초과될 때 이벤트를 트리거합니다. 5분 컬렉션을 사용하는 경우 6개의 연속 컬렉션에 대해 정책을 초과해야 합니다. 15분 컬렉션의 경우 두 수집 기간 동안 정책을 초과해야 합니다.

클러스터 설정 페이지 하단의 메시지는 현재 통계 데이터 수집 간격을 나타냅니다.

단계

1. SSH를 사용하여 Unified Manager 호스트에 대한 유지보수 사용자로 로그인합니다.

   Unified Manager 유지보수 콘솔 프롬프트가 표시됩니다.

2. 성능 폴링 간격 구성 * 이라고 표시된 메뉴 옵션의 번호를 입력한 다음 Enter 키를 누릅니다.
3. 메시지가 표시되면 유지보수 사용자 암호를 다시 입력합니다.
4. 설정할 새 폴링 간격의 숫자를 입력한 다음 Enter 키를 누릅니다.

Unified Manager 수집 간격을 10분 또는 15분으로 변경하고, 외부 데이터 공급자(예: Graphite)에 현재 연결되어 있는 경우, 데이터 공급자의 전송 간격을 Unified Manager 수집 간격보다 크거나 같도록 변경해야 합니다.

워크로드 분석기를 사용하여 워크로드 문제 해결

워크로드 분석기는 단일 페이지의 단일 작업 부하에 대한 중요한 상태 및 성능 기준을 볼 수 있는 방법을 제공하여 문제 해결을 지원합니다. 워크로드에 대한 모든 현재 및 이전 이벤트를 보면 워크로드에 현재 성능 또는 용량 문제가 있는 이유를 보다 잘 알 수 있습니다.

또한 이 툴을 사용하면 스토리지가 애플리케이션의 성능 문제의 원인인지 또는 네트워킹 또는 기타 관련 문제로 인한 문제인지 여부를 확인하는 데 도움이 될 수 있습니다.

사용자 인터페이스의 다양한 위치에서 이 기능을 시작할 수 있습니다.

- 왼쪽 탐색 메뉴에서 Workload Analysis를 선택합니다
- 이벤트 세부 정보 페이지에서 * 워크로드 분석 * 버튼을 클릭합니다
- 모든 워크로드 인벤토리 페이지(볼륨, LUN, 워크로드, NFS 공유 또는 SMB/CIFS 공유)에서 자세히 아이콘을 클릭합니다 그런 다음 * 워크로드 분석 * 을 누릅니다
- 가상 머신 페이지에서 데이터 저장소 객체에서 * Analyze Workload * 버튼을 클릭합니다

왼쪽 탐색 메뉴에서 도구를 시작하면 분석할 작업 부하의 이름을 입력하고 문제를 해결할 시간 범위를 선택할 수 있습니다. 워크로드 또는 가상 머신 인벤토리 페이지에서 툴을 실행하면 워크로드 이름이 자동으로 채워지고 워크로드의 데이터가 기본 2시간 범위로 표시됩니다. 이벤트 세부 정보 페이지에서 툴을 시작하면 워크로드 이름이 자동으로 채워지고 10일 동안의 데이터가 표시됩니다.

워크로드 분석기가 표시하는 데이터는 무엇입니까

워크로드 분석기 페이지에는 작업 부하에 영향을 줄 수 있는 현재 이벤트에 대한 정보, 이벤트를 발생시키는 문제를 잠재적으로 해결할 수 있는 권장 사항, 성능 및 용량 기록 분석을 위한 차트가 표시됩니다.

페이지 위쪽에서 분석할 워크로드(볼륨 또는 LUN)의 이름과 통계를 보려는 기간을 지정합니다. 더 짧거나 긴 기간을 보려면 언제든지 기간을 변경할 수 있습니다.

페이지의 다른 영역에는 분석 결과와 성능 및 용량 차트가 표시됩니다.

LUN에 대한 워크로드 차트는 볼륨에 대한 해당 차트와 같은 수준의 통계를 제공하지 않으므로 이러한 두 유형의 워크로드를 분석할 때 차이가 있음을 알 수 있습니다.

- * 이벤트 요약 영역 *

  시간 경과에 따라 발생한 이벤트의 수와 유형에 대한 간략한 개요를 표시합니다. 다양한 영향 영역(예: 성능 및 용량)의 이벤트가 있는 경우 이 정보가 표시되므로 관심 있는 이벤트 유형에 대한 세부 정보를 선택할 수 있습니다. 이벤트 유형 을 클릭하여 이벤트 이름 목록을 표시합니다.

  해당 기간 동안 이벤트가 하나만 있는 경우 일부 이벤트에 대해 문제 해결을 위한 권장 사항 목록이 표시됩니다.

- * 이벤트 타임라인 *

지정된 기간 동안 발생한 모든 이벤트를 표시합니다. 각 이벤트 위에 커서를 올려 놓으면 이벤트 이름이 표시됩니다.

이벤트 세부 정보 페이지에서 * 워크로드 분석 * 버튼을 클릭하여 이 페이지에 도착한 경우 선택한 이벤트의 아이콘이 더 크게 표시되어 이벤트를 확인할 수 있습니다.

- * 성능 차트 영역 *

  선택한 기간을 기준으로 지연 시간, 처리량(IOPS 및 MB/s 모두) 및 사용률(노드 및 애그리게이트 모두)에 대한 차트를 표시합니다. 성능 세부 정보 보기 링크를 클릭하면 추가 분석을 수행할 경우에 대비하여 작업 부하에 대한 성능 탐색기 페이지가 표시됩니다.

  - * 지연 시간 * 선택한 기간 동안 워크로드의 지연 시간을 표시합니다. 이 차트에는 다음과 같은 세 가지 보기가 있습니다.
    - * 총 * 지연 시간
    - * Breakdown * 지연 시간(읽기, 쓰기 및 기타 프로세스로 구분)
    - * 클러스터 구성 요소 * 지연 시간(클러스터 구성 요소별로 표시)

을 참조하십시오 "클러스터 구성 요소 및 구성 요소의 경합이 발생할 수 있는 이유" 에 표시되는 클러스터 구성 요소에 대한 설명이 나와 있습니다. *** Throughput *** 선택한 기간 동안 워크로드의 **IOPS** 및 **MB/s** 처리량을 모두 표시합니다**.** 이 차트에는 다음 네 가지 보기가 있습니다**.** * 총 * 처리량 ***** 처리량 분석 ***** 처리량**(**읽기**,** 쓰기 및 기타 프로세스로 구분**)** * 클라우드 처리량 * (클라우드에 데이터를 쓰고 클라우드에서 데이터를 읽는 데 사용되는 MB/s; 용량을 클라우드에 계층화하는 워크로드의 경우)***** 예측 ***** 을 사용한 **IOPS * (**기간 동안 예상되는 상위 및 하위 **IOPS** 처리량 값의 예측**)** 이 차트에는 서비스 품질**(QoS)** 최대 및 최소 처리량 임계값 설정도 표시됩니다**(**구성된 경우**).** 따라서 시스템이 **QoS** 정책을 사용하여 의도적으로 처리량을 제한하는 위치를 확인할 수 있습니다**.** * Utilization * 선택한 기간 동안 워크로드가 실행되는 집계 및 노드에 대한 활용률을 표시합니다. 여기에서 애그리게이트 또는 노드의 활용률이 너무 높은것을 확인할 수 있으며 이로 인해 지연 시간이 길어질 수 있습니다. FlexGroup 볼륨을 분석할 때 활용도 차트에 여러 노드와 여러 애그리게이트가 나열됩니다.

- * 용량 차트 영역 *

  워크로드의 지난 1개월 동안의 데이터 용량 및 스냅샷 용량에 대한 차트를 표시합니다.

  볼륨의 경우 View capacity details(용량 세부 정보 보기) 링크를 클릭하여 추가 분석을 수행하려는 경우 워크로드의 Health Details(상태 세부 정보) 페이지를 표시할 수 있습니다. LUN에 대한 상태 세부 정보 페이지가 없으므로 LUN에서 이 링크를 제공하지 않습니다.

  - * Capacity View * 는 작업 부하에 할당된 총 사용 가능한 공간과 모든 NetApp 최적화 후 논리적 사용 공간을 표시합니다.
  - * 스냅샷 뷰 * 는 스냅샷 복사본에 예약된 총 공간과 현재 사용 중인 공간을 표시합니다. LUN은 스냅샷 보기를 제공하지 않습니다.
  - * Cloud Tier View * 는 로컬 성능 계층에서 사용되는 용량과 클라우드 계층에서 사용되는 용량을 표시합니다. 이러한 차트에는 이 워크로드에 대한 용량이 가득 차기까지의 남은 예상 시간이 포함됩니다. 이 정보는 과거 사용량을 기준으로 하며 최소 10일 이상의 데이터가 필요합니다. 유니파이드 관리자는 30일 이내에 용량을 유지할 경우 스토리지를 ""거의 꽉 참""으로 식별합니다.

워크로드 분석기는 언제 사용해야 합니다

일반적으로 워크로드 분석기를 사용하여 사용자가 보고한 지연 시간 문제를 해결하거나, 보고된 이벤트 또는 경고를 보다 철저히 분석하거나, 비정상적으로 작동하는 워크로드를 탐색할 수 있습니다.

사용자가 사용 중인 애플리케이션이 매우 느리게 실행된다고 문의한 경우, 애플리케이션이 실행되는 워크로드의 지연 시간, 처리량 및 활용률 차트를 확인하여 스토리지가 성능 문제의 원인인지 파악할 수 있습니다. 용량 차트를 사용하여 용량의 85% 이상이 사용된 ONTAP 시스템으로 인해 성능 문제가 발생할 수 있으므로 용량 수준이 낮은지 확인할 수 있습니다. 이 차트는 문제가 스토리지 또는 네트워킹 또는 기타 관련 문제로 인해 발생하는지 확인하는 데 도움이 됩니다.

Unified Manager가 성능 이벤트를 생성한 후 문제의 원인을 보다 철저히 검토하려면 이벤트 세부 정보 페이지에서 * 워크로드 분석 * 버튼을 클릭하여 워크로드 분석기를 시작하여 지연 시간, 처리량, 처리량 등을 조사할 수 있습니다. 및 용량 동향을 파악합니다.

워크로드 인벤토리 페이지(볼륨, LUN, 워크로드, NFS 공유 또는 SMB/CIFS 공유)를 볼 때 워크로드가 비정상적으로 작동하는 것으로 보이는 경우 자세히 아이콘을 클릭할 수 있습니다 ⋮ 그런 다음 * 워크로드 분석 * 을 클릭하여 워크로드 분석 페이지를 열어 워크로드를 더 자세히 검토합니다.

워크로드 분석기를 사용합니다

사용자 인터페이스에서 워크로드 분석기를 시작하는 방법은 여러 가지가 있습니다. 여기에서는 왼쪽 탐색 창에서 도구를 시작하는 방법을 설명합니다.

단계

1. 왼쪽 탐색 창에서 * 워크로드 분석 * 을 클릭합니다.

   워크로드 분석 페이지가 표시됩니다.

2. 워크로드 이름을 알고 있는 경우 이름을 입력합니다. 전체 이름을 모르는 경우 최소 3자를 입력하면 문자열과 일치하는 워크로드 목록이 표시됩니다.
3. 기본 2시간 이상의 통계를 보려면 시간 범위를 선택하고 * 적용 * 을 클릭합니다.
4. 요약 영역을 보고 해당 기간 동안 발생한 이벤트를 확인합니다.
5. 성능 및 용량 차트를 보고 메트릭이 언제 비정상적인지 확인하고 비정상적인 항목에 이벤트가 있는지 확인합니다.

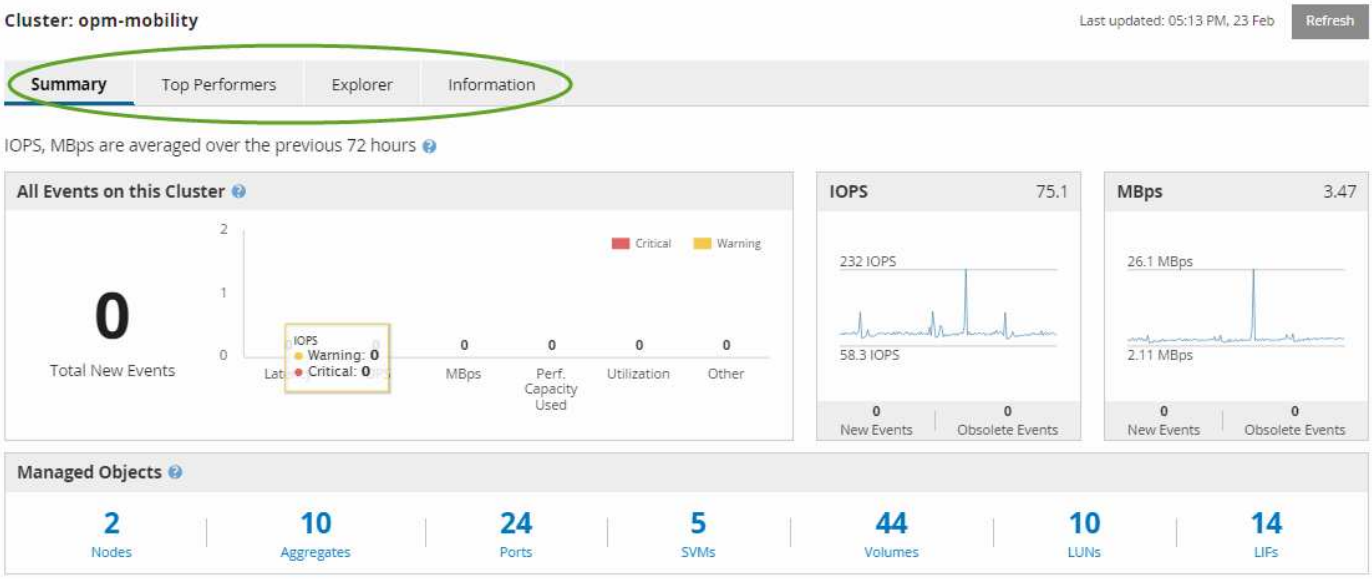
성능 클러스터 랜딩 페이지에서 클러스터 성능을 모니터링합니다

Performance Cluster Landing 페이지는 Unified Manager 인스턴스에서 모니터링되고 있는 선택된 클러스터의 고성능 상태를 표시합니다. 이 페이지에서는 특정 클러스터의 전반적인 성능을 평가하고 식별된 클러스터별 이벤트를 신속하게 확인, 검색 또는 할당할 수 있습니다.

성능 클러스터 랜딩 페이지 이해

성능 클러스터 랜딩 페이지는 선택한 클러스터에 대한 높은 수준의 성능 개요를 제공하며 클러스터 내 상위 10개 개체의 성능 상태를 강조합니다. 성능 문제는 이 클러스터의 모든 이벤트 패널에 페이지 맨 위에 표시됩니다.

Performance Cluster 랜딩 페이지에서는 Unified Manager 인스턴스에서 관리되는 각 클러스터에 대한 간략한 개요를 제공합니다. 이 페이지에서는 이벤트와 성능에 대한 정보를 제공하고 클러스터를 모니터링하고 문제를 해결할 수 있습니다. 다음 이미지는 OPM-mobility라는 클러스터에 대한 성능 클러스터 랜딩 페이지의 예를 보여줍니다.



클러스터 요약 페이지의 이벤트 수가 성능 이벤트 인벤토리 페이지의 이벤트 수와 일치하지 않을 수 있습니다. 이는 복합 임계값 정책이 위반된 경우 클러스터 요약 페이지에 지연 시간 및 활용률 막대에 각각 하나의 이벤트가 표시될 수 있는 반면 성능 이벤트 인벤토리 페이지에는 조합 정책이 위반된 경우 하나의 이벤트만 표시될 수 있기 때문입니다.

Unified Manager에서 클러스터를 관리할 수 없는 경우, 페이지 위쪽의 클러스터 이름 오른쪽에 상태 * 제거됨 * 이 표시됩니다.

성능 클러스터 랜딩 페이지 를 참조하십시오

성능 클러스터 랜딩 페이지에는 선택한 클러스터의 고성능 상태가 표시됩니다. 이 페이지에서는 선택한 클러스터의 스토리지 오브젝트에 대한 각 성능 카운터의 전체 세부 정보를 액세스할 수 있습니다.

성능 클러스터 랜딩 페이지에는 클러스터 세부 정보를 4개의 정보 영역으로 구분하는 4개의 탭이 있습니다.

- 요약 페이지
  - 클러스터 이벤트 창
  - MB/s 및 IOPS 성능 차트
  - 관리 개체 창
- 우수 성과 페이지
- 탐색 페이지
- 정보 페이지

성능 클러스터 요약 페이지

Performance Cluster Summary 페이지에는 클러스터에 대한 활성 이벤트, IOPS 성능 및 MB/s 성능이 요약되어 있습니다. 이 페이지에는 클러스터에 있는 스토리지 객체의 총 개수도 포함됩니다.

클러스터 성능 이벤트 창에는 클러스터에 대한 성능 통계 및 모든 활성 이벤트가 표시됩니다. 이 기능은 클러스터와 모든 클러스터 관련 성능 및 이벤트를 모니터링할 때 가장 유용합니다.

이 클러스터 창의 모든 이벤트입니다

이 클러스터의 모든 이벤트 창에는 지난 72시간 동안 발생한 모든 활성 클러스터 성능 이벤트가 표시됩니다. 총 활성 이벤트가 맨 왼쪽에 표시됩니다. 이 숫자는 이 클러스터의 모든 스토리지 객체에 대한 모든 신규 및 승인된 이벤트의 합계를 나타냅니다. 총 활성 이벤트 링크를 클릭하여 이벤트 인벤토리 페이지로 이동할 수 있습니다. 이 페이지는 이러한 이벤트를 표시하도록 필터링되어 있습니다.

클러스터의 총 활성 이벤트 막대 그래프에는 활성 위험 및 경고 이벤트의 총 수가 표시됩니다.

- 지연 시간(노드, 애그리게이트, SVM, 볼륨, LUN의 합계, 및 네임스페이스)
- IOPS(클러스터, 노드, 애그리게이트, SVM, 볼륨, LUN 및 네임스페이스)
- MB/s(클러스터, 노드, 애그리게이트, SVM, 볼륨 합계) LUN, 네임스페이스, 포트 및 LIF)
- 사용된 성능 용량(노드 및 애그리게이트의 총 수)
- 사용률(노드, 애그리게이트 및 포트의 총 수)
- 기타(볼륨의 캐시 비적중 비율)

목록에는 사용자 정의 임계값 정책, 시스템 정의 임계값 정책 및 동적 임계값에서 트리거되는 활성 성능 이벤트가 포함되어 있습니다.

그래프 데이터(수직 카운터 바)가 빨간색 (), 심각 이벤트 및 황색()를 참조하십시오. 각 수직 카운터 바 위에 커서를 놓으면 실제 유형과 이벤트 수가 표시됩니다. 새로 고침 * 을 클릭하여 카운터 패널 데이터를 업데이트할 수 있습니다.

범례에서 * Critical * 및 * Warning * 아이콘을 클릭하여 Total Active Events 성능 그래프에서 중대 및 경고 이벤트를 표시하거나 숨길 수 있습니다. 특정 이벤트 유형을 숨기면 범례 아이콘이 회색으로 표시됩니다.

카운터 패널

카운터 패널에는 이전 72시간 동안의 클러스터 활동 및 성능 이벤트가 표시되며 다음 카운터가 포함됩니다.

- * IOPS 카운터 패널 *

  IOPS는 초당 입출력 작업 수로 클러스터의 작동 속도를 나타냅니다. 이 카운터 패널에서는 이전 72시간 동안의 클러스터 IOPS 상태에 대한 간략한 개요를 제공합니다. 그래프 추이 행 위에 커서를 놓으면 특정 시간의 IOPS 값을 볼 수 있습니다.

- MB/s 카운터 패널 *

  MB/s는 클러스터에서 또는 클러스터에서 전송된 데이터의 양을 초당 메가바이트 단위로 나타냅니다. 이 카운터 패널에서는 이전 72시간 동안의 클러스터의 MB/s 상태에 대한 개괄적인 개요를 제공합니다. 그래프 추세 선 위에 커서를 놓으면 특정 시간에 대한 MB/s 값을 볼 수 있습니다.

회색 막대의 차트 오른쪽 위에 있는 숫자는 지난 72시간 동안의 평균 값입니다. 추세 선 그래프의 맨 아래 및 맨 위에 표시되는 숫자는 지난 72시간 동안의 최소값 및 최대값입니다. 차트 아래의 회색 표시줄에는 지난 72시간 동안의 활성(새 이벤트 및 확인된) 이벤트 수와 사용되지 않는 이벤트의 수가 포함됩니다.

카운터 패널에는 두 가지 유형의 이벤트가 있습니다.

- * 활성 *

  성능 이벤트가 현재 활성 상태(새 이벤트 또는 확인된 이벤트)임을 나타냅니다. 이벤트를 발생시키는 문제가 자체적으로 해결되지 않았거나 해결되지 않았습니다. 스토리지 개체의 성능 카운터는 성능 임계값보다 높게 유지됩니다.

- * 사용되지 않음 *

  이벤트가 더 이상 활성 상태가 아님을 나타냅니다. 이벤트를 발생시키는 문제가 자체적으로 해결되었거나 해결되었습니다. 스토리지 개체의 성능 카운터가 더 이상 성능 임계값을 초과하지 않습니다.

활성 이벤트 * 의 경우 이벤트가 하나 있는 경우 이벤트 아이콘 위에 커서를 놓고 이벤트 번호를 클릭하여 해당 이벤트 세부 정보 페이지로 연결할 수 있습니다. 이벤트가 두 개 이상 있는 경우 * 모든 이벤트 보기 * 를 클릭하여 이벤트 인벤토리 페이지를 표시할 수 있습니다. 이벤트 인벤토리 페이지는 선택한 개체 카운터 유형에 대한 모든 이벤트를 표시하도록 필터링됩니다.

관리 개체 창

성능 요약 정보 탭의 관리 대상 개체 창에는 클러스터에 대한 스토리지 개체 유형과 카운트의 최상위 개요가 표시됩니다. 이 창에서는 각 클러스터에 있는 개체의 상태를 추적할 수 있습니다.

관리되는 개체 수는 마지막 컬렉션 기간의 시점 데이터입니다. 새 오브젝트는 15분 간격으로 검색됩니다.

개체 유형에 대해 연결된 번호를 클릭하면 해당 개체 유형에 대한 개체 성능 인벤토리 페이지가 표시됩니다. 객체 인벤토리 페이지는 이 클러스터의 객체만 표시하도록 필터링됩니다.

관리되는 개체는 다음과 같습니다.

- * 노드 *

  클러스터의 물리적 시스템

- * 애그리게이트 *

  보호 및 프로비저닝을 위해 단일 유닛으로 관리할 수 있는 여러 RAID(Redundant Array of Independent Disks) 그룹 집합입니다.

- 포트 *

  네트워크의 다른 장치에 연결하는 데 사용되는 노드의 물리적 연결 지점입니다.

- 스토리지 VM *

  고유한 네트워크 주소를 통해 네트워크 액세스를 제공하는 가상 시스템. SVM은 별개의 네임스페이스에서 데이터를 제공할 수 있으며 클러스터의 나머지 부분과는 별도로 관리할 수 있습니다.

- 볼륨 *

  지원되는 하나 이상의 액세스 프로토콜을 통해 액세스 가능한 사용자 데이터를 보유하는 논리적 엔티티입니다. 이 개수에는 FlexVol 볼륨과 FlexGroup 볼륨이 모두 포함되며 FlexGroup 구성 요소는 포함되지 않습니다.

- LUN *

  FC(Fibre Channel) 논리 유닛 또는 iSCSI 논리 유닛의 식별자입니다. 논리 유닛은 일반적으로 저장소 볼륨에 해당하며 컴퓨터 운영 체제 내에서 장치로 표시됩니다.

- * 네트워크 인터페이스 *

  노드에 대한 네트워크 액세스 포인트를 나타내는 논리 네트워크 인터페이스입니다. 카운트에는 모든 인터페이스 유형이 포함됩니다.

우수 성과 페이지

우수 성과 페이지에는 선택한 성능 카운터에 따라 성능이 가장 높은 스토리지 객체 또는 성능이 가장 낮은 스토리지 객체가 표시됩니다. 예를 들어, 스토리지 VM 범주에서 IOPS가 가장 높고 지연 시간이 가장 긴 SVM이나 가장 낮은 MB/s를 표시할 수 있습니다 또한 이 페이지는 상위 성과자가 진행 중인 성과 이벤트(신규 또는 확인됨)를 가지고 있는지도 보여줍니다.

우수 성과 기업 페이지에는 각 개체 중 최대 10개가 표시됩니다. 볼륨 개체에는 FlexVol 볼륨과 FlexGroup 볼륨이 모두 포함되어 있습니다.

- * 시간 범위 *

  상위 성과자를 볼 시간 범위를 선택할 수 있습니다. 선택한 시간 범위는 모든 스토리지 객체에 적용됩니다. 사용 가능한 시간 범위:

  ◦ 지난 시간
  ◦ 최근 24시간
  ◦ 최근 72시간(기본값)
  ◦ 최근 7일

- * 미터법 *

  다른 카운터를 선택하려면 * Metric * 메뉴를 클릭합니다. 카운터 옵션은 개체 형식에 고유합니다. 예를 들어, * Volumes * 개체에 사용할 수 있는 카운터는 * 지연 시간 *, * IOPS * 및 * MB/s * 입니다. 카운터를 변경하면 선택한 카운터를 기준으로 최상위 성과자와 함께 패널 데이터가 다시 로드됩니다.

  사용 가능한 카운터:

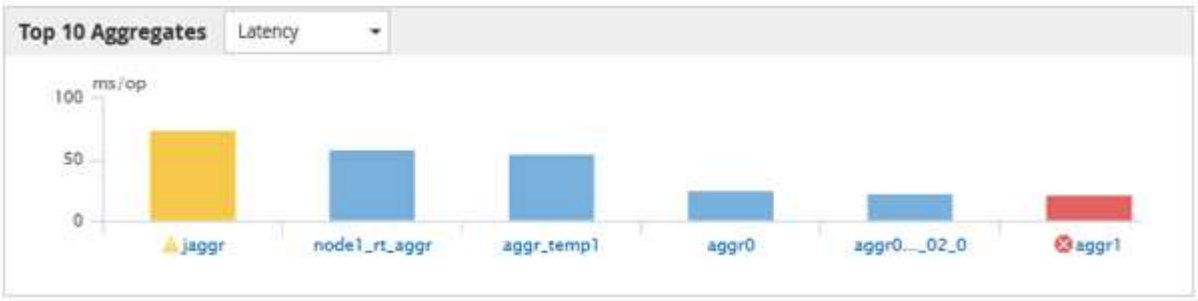
  ◦ 지연 시간
  ◦ IOPS
  ◦ MB/s
  ◦ 사용된 성능 용량(노드 및 애그리게이트의 경우)
  ◦ 활용률(노드 및 애그리게이트)

- * 정렬 *

  정렬 * 메뉴를 클릭하여 선택한 개체 및 카운터에 대한 오름차순 또는 내림차순 정렬을 선택합니다. 옵션은 * Highest(최고) - Lowest(최저) *, * Lowest(최저) - Highest(최고) * 입니다 이러한 옵션을 사용하면 성능이 가장 좋은 오브젝트나 성능이 가장 낮은 오브젝트를 볼 수 있습니다.

- * 카운터 바 *

  그래프의 카운터 막대는 각 개체의 성능 통계를 표시하며, 해당 항목의 표시줄로 표시됩니다. 막대 그래프는 색상으로 구분됩니다. 카운터가 성능 임계값을 위반하지 않으면 카운터 막대가 파란색으로 표시됩니다. 임계값 위반이 활성화된 경우(새 이벤트 또는 승인된 이벤트) 해당 이벤트의 색으로 경고 이벤트가 노란색으로 표시됩니다 ( ), 및 위험 이벤트가 빨간색( )를 클릭합니다. 임계값 위반은 경고 및 중요 이벤트에 대한 심각도 이벤트 표시기 아이콘으로 표시됩니다.



  각 그래프에 대해 X축은 선택한 객체 유형에 대해 최상위 성과자를 표시합니다. Y 축에는 선택한 카운터에 적용할 수 있는 단위가 표시됩니다. 각 세로 막대 그래프 요소 아래에 있는 개체 이름 링크를 클릭하면 선택한 개체의 성능 랜딩 페이지로 이동합니다.

- * 심각도 이벤트 표시기 *

  활성 심각(.)에 대한 객체 이름 왼쪽에 * 심각도 이벤트 * 표시기 아이콘이 표시됩니다( ) 또는 경고( ) 상위 성과자 그래프의 이벤트. 다음을 보려면 * 심각도 이벤트 * 표시 아이콘을 클릭하십시오.

  - * 하나의 이벤트 *

    해당 이벤트의 이벤트 세부 정보 페이지로 이동합니다.

  - * 두 개 이상의 이벤트 *

    선택한 개체에 대한 모든 이벤트를 표시하도록 필터링되는 이벤트 인벤토리 페이지로 이동합니다.

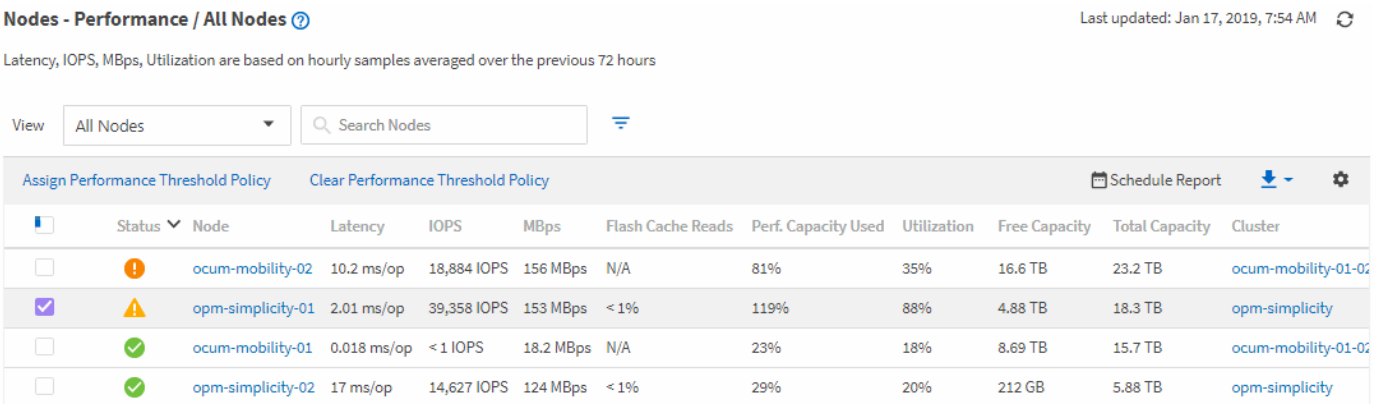
- * 내보내기 버튼 *

  카운터 모음에 나타나는 데이터가 포함된 '.csv' 파일을 만듭니다. 보고 있는 단일 클러스터나 데이터 센터의 모든 클러스터에 대해 파일을 생성하도록 선택할 수 있습니다.

성능 인벤토리 페이지를 사용하여 성능 모니터링

오브젝트 인벤토리 성능 페이지에는 오브젝트 유형 범주 내의 모든 오브젝트에 대한 성능 정보, 성능 이벤트 및 오브젝트 상태가 표시됩니다. 클러스터 내에서 모든 노드 또는 모든 볼륨과 같은 각 개체의 성능 상태를 한눈에 파악할 수 있습니다.

오브젝트 인벤토리 성능 페이지는 오브젝트 상태에 대한 높은 수준의 개요를 제공하여 모든 오브젝트의 전반적인 성능을 평가하고 오브젝트 성능 데이터를 비교할 수 있도록 합니다. 검색, 정렬 및 필터링을 통해 개체 재고 페이지의 내용을 구체화할 수 있습니다. 이 기능은 성능 문제가 있는 개체를 신속하게 찾고 문제 해결 프로세스를 시작할 수 있으므로 개체 성능을 모니터링하고 관리할 때 유용합니다.



기본적으로 성능 인벤토리 페이지의 개체는 개체 성능 중요도에 따라 정렬됩니다. 새로운 심각한 성능 이벤트가 발생한 객체가 먼저 나열되고 경고 이벤트가 있는 객체가 두 번째로 나열됩니다. 이를 통해 해결해야 할 문제를 시각적으로 즉시 확인할 수 있습니다. 모든 성능 데이터는 평균 72시간을 기준으로 합니다.

객체 이름 열에서 객체 이름을 클릭하여 객체 재고 성능 페이지에서 객체 세부 정보 페이지로 쉽게 이동할 수 있습니다. 예를 들어 성능/모든 노드 인벤토리 페이지에서 * 노드 * 열에서 노드 개체를 클릭합니다. 개체 세부 정보 페이지는 활성 이벤트의 side-by-side 비교를 포함하여 선택한 개체에 대한 자세한 정보와 세부 정보를 제공합니다.

모든 스토리지 객체에 대한 성능 인벤토리 페이지 보기

성능 인벤토리 페이지를 사용하여 클러스터, 애그리게이트, 볼륨 등과 같이 사용 가능한 각 스토리지 개체에 대한 성능 정보 요약을 확인할 수 있습니다. 성능 개체 세부 정보 페이지에 연결하여 특정 개체에 대한 자세한 정보를 볼 수 있습니다.

기본적으로 보기 페이지의 개체는 이벤트 중요도에 따라 정렬됩니다. 중요한 이벤트가 있는 개체가 먼저 나열되고 경고 이벤트가 있는 개체는 두 번째로 나열됩니다. 이를 통해 해결해야 할 문제를 시각적으로 즉시 확인할 수 있습니다.

이 페이지에서 데이터는 * Reports * 버튼을 사용하여 쉼표로 구분된 값(".csv") 파일, Microsoft Excel 파일(".xlsx") 또는 (".pdf") 문서로 내보낸 다음 내보낸 데이터를 사용하여 보고서를 작성할 수 있습니다. 또한 페이지를 사용자 정의한 다음 * Scheduled Reports * 버튼을 사용하여 정기적으로 보고서를 만들고 이메일로 전송할 수 있도록 예약할 수 있습니다.

이러한 페이지의 모든 필드는 사용자 정의 보기 및 보고서에서 사용할 수 있습니다. 일부 필드는 관련 페이지에 연결되어 보다 상세한 보기를 제공합니다.

성능: 모든 클러스터 보기

Performance:All Clusters 보기에는 Unified Manager 인스턴스에서 모니터링하는 각 클러스터의 성능 이벤트, 데이터 및 구성 정보에 대한 개요가 표시됩니다. 이 페이지에서는 클러스터의 성능을 모니터링하고 성능 문제 및 임계값 이벤트를 해결할 수 있습니다.

성능 임계값 정책 할당 * 및 * 성능 임계값 정책 지우기 * 버튼을 사용하여 개체 인벤토리 페이지의 모든 개체에 성능 임계값 정책을 할당하거나 삭제할 수 있습니다.

다음은 Performance:All Clusters 보기의 몇 가지 중요한 필드입니다.

- 클러스터 FQDN: 클러스터의 FQDN(정규화된 도메인 이름)입니다.
- IOPS: 클러스터의 초당 입출력 작업 수

- MB/s: 클러스터에서 처리량(MiB/초 단위)입니다.
- 용량 필드: 가용 용량 및 총 용량(GiB)
- 호스트 이름 또는 IP 주소: 클러스터 관리 LIF의 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)입니다.
- OS 버전: 클러스터에 설치된 ONTAP 소프트웨어 버전입니다.

> 다른 버전의 ONTAP 소프트웨어가 클러스터의 노드에 설치된 경우 가장 낮은 버전 번호가 표시됩니다. 성능: 모든 노드 보기에서 각 노드에 설치된 ONTAP 버전을 볼 수 있습니다.

- 임계값 정책: 이 스토리지 개체에서 활성 상태인 사용자 정의 성능 임계값 정책 또는 정책입니다. 줄임표(…)가 포함된 정책 이름 위에 커서를 놓으면 전체 정책 이름 또는 할당된 정책 이름 목록을 볼 수 있습니다. 맨 왼쪽에 있는 확인란을 클릭하여 하나 이상의 개체를 선택할 때까지 성능 임계값 정책 할당 및 성능 임계값 정책 지우기 버튼이 비활성화 상태로 유지됩니다.

성능**:** 모든 볼륨 보기

Performance:All Volumes 뷰에는 Unified Manager 인스턴스에서 모니터링되는 각 FlexVol 볼륨 및 FlexGroup 볼륨에 대한 성능 이벤트, 카운터 데이터 및 구성 정보의 개요가 표시됩니다. 따라서 볼륨의 성능을 빠르게 모니터링하고 성능 문제 및 임계값 이벤트를 해결할 수 있습니다.

특정 개체의 대기 시간과 처리량을 분석하려면 자세히 옵션 단추를 클릭합니다 ⋮ 그런 다음 * 워크로드 분석 * 을 통해 워크로드 분석 페이지에서 성능 및 용량 차트를 확인할 수 있습니다. System Manager에 대한 유효한 자격 증명이 있는 경우 System Manager에서 세부 정보를 볼 수 있습니다.

> 데이터 보호(DP) 볼륨의 경우 사용자 생성 트래픽에 대한 카운터 값만 표시됩니다. 루트 볼륨은 이 페이지에 표시되지 않습니다.

다음은 Performance:All Volumes 보기의 몇 가지 중요한 필드입니다.

- 스타일: FlexVol 또는 FlexGroup.
- 지연 시간: FlexVol 볼륨의 경우 모든 I/O 요청에 대한 볼륨의 평균 응답 시간으로, 작업당 밀리초 단위로 표시됩니다. FlexGroup 볼륨의 경우 이 지연 시간이 모든 구성 볼륨의 평균 지연 시간입니다.
- IOPS/TB: 워크로드에서 소비하는 총 공간(TB)을 기준으로 초당 처리되는 입출력 작업의 수입니다. 이 카운터는 지정된 양의 스토리지 용량으로 제공할 수 있는 성능을 측정합니다.
- IOPS: FlexVol 볼륨의 경우 볼륨에 대한 초당 입출력 작업 수입니다. FlexGroup 볼륨의 경우 모든 구성 볼륨의 IOPS 합계입니다.
- MB/s: FlexVol 볼륨의 경우 초당 메가바이트 단위로 측정되는 볼륨의 처리량입니다. FlexGroup 볼륨의 경우 모든 구성 볼륨의 MB/s 합계입니다.
- 용량 필드: 가용 용량 및 총 용량(GiB)

자세한 내용은 다음 링크를 참조하십시오.

- "스토리지 객체에 성능 임계값 정책 할당"
- "스토리지 개체에서 성능 임계값 정책 제거"
- "Unified Manager에서 모니터링하는 워크로드의 유형입니다"
- "특정 볼륨 또는 LUN에 적용된 QoS 정책 그룹 설정 보기"

- "데이터를 클라우드에 계층화하도록 Unified Manager의 권장 사항 이해"
- "성능 차트를 확인하여 동일한 QoS 정책 그룹에 있는 볼륨 또는 LUN을 비교합니다"

성능: 모든 애그리게이트 보기

Performance:All 애그리게이트 뷰에는 Unified Manager 인스턴스에서 모니터링하는 각 애그리게이트의 성능 이벤트, 데이터 및 구성 정보의 개요가 표시됩니다. 이 페이지에서는 애그리게이트의 성능을 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다.

다음은 Performance:All aggregate 보기의 몇 가지 중요한 필드입니다.

- 유형: 집계 유형:
  - HDD
  - 하이브리드. HDD와 SSD를 결합하지만 Flash Pool은 활성화되지 않았습니다.
  - 하이브리드(Flash Pool) HDD와 SSD의 결합과 Flash Pool이 설정되었습니다.
  - SSD를 지원합니다
  - SSD(FabricPool): SSD와 클라우드 계층을 결합합니다
  - HDD(FabricPool). HDD와 클라우드 계층 결합
  - VMDisk(SDS): 가상 머신 내의 가상 디스크
  - VMDisk(FabricPool). 가상 디스크와 클라우드 계층을 결합합니다
  - LUN(FlexArray)
- Inactive Data Reporting(비활성 데이터 보고): 이 집계에서 비활성 데이터 보고 기능을 활성화 또는 비활성화할지 여부를 나타냅니다. 이 애그리게이트의 볼륨을 활성화하면 Performance:All Volumes 뷰에 콜드 데이터의 양이 표시됩니다. ONTAP 버전이 비활성 데이터 보고를 지원하지 않는 경우 이 필드의 값은 "N/A"입니다.
- 임계값 정책: 이 스토리지 개체에서 활성 상태인 사용자 정의 성능 임계값 정책 또는 정책입니다. 줄임표(…)가 포함된 정책 이름 위에 커서를 놓으면 전체 정책 이름 또는 할당된 정책 이름 목록을 볼 수 있습니다. 맨 왼쪽에 있는 확인란을 클릭하여 하나 이상의 개체를 선택할 때까지 성능 임계값 정책 할당 및 성능 임계값 정책 지우기 버튼이 비활성화 상태로 유지됩니다. 자세한 내용은 다음 링크를 참조하십시오.
- "스토리지 객체에 성능 임계값 정책 할당"
- "스토리지 개체에서 성능 임계값 정책 제거"

성능: 모든 노드 보기

Performance:All Nodes 보기에는 Unified Manager 인스턴스에서 모니터링하는 각 노드에 대한 성능 이벤트, 데이터 및 구성 정보의 개요가 표시됩니다. 따라서 노드의 성능을 빠르게 모니터링하고 성능 문제와 임계값 이벤트를 해결할 수 있습니다.

Flash Cache 읽기는 디스크에서 반환된 것이 아니라 캐시에서 처리된 노드의 읽기 작업 비율을 반환합니다. Flash Cache 데이터는 노드에 대해서만 표시되며 Flash Cache 모듈이 노드에 설치된 경우에만 표시됩니다.

보고서 * 메뉴에서 * 하드웨어 인벤토리 보고서 * 옵션은 Unified Manager와 관리 중인 클러스터가 외부 네트워크 연결이 없는 사이트에 설치될 때 제공됩니다. 이 버튼은 하드웨어 모델 번호 및 일련 번호, 디스크 유형 및 개수, 설치된 라이센스 등과 같은 클러스터 및 노드 정보의 전체 목록을 포함하는 .csv 파일을 생성합니다. 이 보고 기능은 NetApp Active IQ 플랫폼에 연결되지 않은 보안 사이트 내에서 계약을 갱신하는 데 유용합니다. 성능 임계값 정책 할당 * 및 *

성능 임계값 정책 지우기 * 버튼을 사용하여 개체 인벤토리 페이지의 모든 개체에 성능 임계값 정책을 할당하거나 삭제할 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- "스토리지 객체에 성능 임계값 정책 할당"
- "스토리지 개체에서 성능 임계값 정책 제거"
- "계약 갱신을 위한 하드웨어 인벤토리 보고서를 생성하는 중입니다"

성능**:** 모든 스토리지 **VM** 보기

성능: 모든 스토리지 VM 뷰에는 Unified Manager 인스턴스에서 모니터링되는 각 SVM(스토리지 가상 머신)의 성능 이벤트, 데이터 및 구성 정보에 대한 개요가 표시됩니다. 따라서 SVM의 성능을 빠르게 모니터링하고 성능 문제 및 임계값 이벤트를 해결할 수 있습니다. 이 페이지의 지연 시간 필드는 모든 I/O 요청에 대한 평균 응답 시간을 밀리초 단위로 표시합니다.

이 페이지에 나열된 SVM에는 데이터 및 클러스터 SVM만 포함됩니다. Unified Manager는 관리 또는 노드 SVM을 사용하거나 표시하지 않습니다.

자세한 내용은 다음 링크를 참조하십시오.

- "스토리지 객체에 성능 임계값 정책 할당"
- "스토리지 개체에서 성능 임계값 정책 제거"

성능**:** 모든 **LUN** 보기

Performance: All LUNs 보기에는 Unified Manager 인스턴스에서 모니터링되는 각 LUN에 대한 성능 이벤트, 데이터 및 구성 정보의 개요가 표시됩니다. 이를 통해 LUN의 성능을 빠르게 모니터링하고 성능 문제 및 임계값 이벤트를 해결할 수 있습니다.

특정 개체의 대기 시간과 처리량을 분석하려면 자세히 아이콘을 클릭합니다 ⋮그런 다음 * 워크로드 분석 * 을 실행하여 * 워크로드 분석 * 페이지에서 성능 및 용량 차트를 확인할 수 있습니다.

자세한 내용은 다음 링크를 참조하십시오.

- "정합성 보장 그룹 관계에서 LUN 모니터링"
- "LUN 프로비저닝"
- "스토리지 객체에 성능 임계값 정책 할당"
- "스토리지 개체에서 성능 임계값 정책 제거"
- "동일한 QoS 정책 그룹에 있는 볼륨 또는 LUN 보기".
- "특정 볼륨 또는 LUN에 적용된 QoS 정책 그룹 설정 보기"
- "API를 사용하여 LUN 프로비저닝"

성능**:** 모든 **NVMe** 네임스페이스 보기

Performance:All NVMe Namespaces 뷰에는 Unified Manager 인스턴스에서 모니터링되는 각 NVMe 네임스페이스에 대한 성능 이벤트, 데이터 및 구성 정보의 개요가 표시됩니다. 이렇게 하면 네임스페이스의 성능과

상태를 빠르게 모니터링하고 문제 및 임계값 이벤트를 해결할 수 있습니다.

다른 정보 중 다음과 같은 정보가 보고됩니다. Namespace 의 현재 상태입니다. * 오프라인 - 네임스페이스에 대한 읽기 또는 쓰기 액세스가 허용되지 않습니다. * 온라인 - 네임스페이스에 대한 읽기 및 쓰기 액세스가 허용됩니다. * NVFail - NVRAM 장애로 인해 네임스페이스가 자동으로 오프라인 상태로 전환되었습니다. * 공간 오류 - 네임스페이스에서 공간이 부족합니다.

자세한 내용은 다음 링크를 참조하십시오.

- "스토리지 객체에 성능 임계값 정책 할당"
- "스토리지 개체에서 성능 임계값 정책 제거"

성능: 모든 네트워크 인터페이스 보기

성능: 모든 네트워크 인터페이스 뷰는 Unified Manager의 이 인스턴스에서 모니터링되는 각 네트워크 인터페이스(LIF)에 대한 성능 이벤트, 데이터 및 구성 정보의 개요를 표시합니다. 이 페이지에서는 인터페이스 성능을 빠르게 모니터링하고 성능 문제 및 임계값 이벤트를 해결할 수 있습니다. 다음은 Performance:All Network Interfaces 보기의 몇 가지 중요한 필드입니다.

- IOPS: 초당 입출력 작업 수입니다. IOPS는 NFS LIF 및 CIFS LIF에는 적용되지 않으며 이러한 유형에 대해 N/A로 표시됩니다.
- 지연 시간: 모든 I/O 요청에 대한 평균 응답 시간으로, 작업 당 밀리초 단위로 표시됩니다. 지연 시간은 NFS LIF 및 CIFS LIF에는 적용되지 않으며 이러한 유형에 대해 N/A로 표시됩니다.
- 홈 위치: 인터페이스의 홈 위치로, 노드 이름 및 포트 이름으로 표시되며 콜론(:)으로 구분됩니다. 위치가 줄임표(…)로 표시되는 경우 위치 이름 위에 커서를 놓으면 전체 위치를 볼 수 있습니다.
- 현재 위치: 노드 이름 및 포트 이름으로 표시되며 콜론(:)으로 구분된 인터페이스의 현재 위치입니다. 위치가 줄임표(…)로 표시되는 경우 위치 이름 위에 커서를 놓으면 전체 위치를 볼 수 있습니다.
- 역할: 인터페이스 역할: 데이터, 클러스터, 노드 관리 또는 인터클러스터.

이 페이지에 표시되는 인터페이스에는 데이터 LIF, 클러스터 LIF, 노드 관리 LIF 및 인터클러스터 LIF가 있습니다. Unified Manager는 시스템 LIF를 사용하거나 표시하지 않습니다.

성능: 모든 포트 보기

성능: 모든 포트 보기에는 Unified Manager 인스턴스가 모니터링하는 각 포트의 성능 이벤트, 데이터 및 구성 정보가 개괄적으로 표시됩니다. 따라서 포트의 성능을 빠르게 모니터링하고 성능 문제 및 임계값 이벤트를 해결할 수 있습니다. 포트 역할의 경우 네트워크 포트 기능이 데이터 또는 클러스터라는 형식으로 표시됩니다. FCP 포트의 역할은 있을 수 없으며 해당 역할은 N/A로 표시됩니다

성능 카운터 값은 물리적 포트에만 표시됩니다. 카운터 값은 VLAN 또는 인터페이스 그룹에 대해 표시되지 않습니다.

자세한 내용은 다음 링크를 참조하십시오.

- "스토리지 객체에 성능 임계값 정책 할당"
- "스토리지 개체에서 성능 임계값 정책 제거"

성능**: QoS** 정책 그룹 보기

QoS 정책 그룹 보기에는 Unified Manager에서 모니터링하는 클러스터에서 사용할 수 있는 QoS 정책 그룹이 표시됩니다. 여기에는 기존 QoS 정책, 적응형 QoS 정책, 그리고 성능 서비스 수준을 사용하여 할당된 QoS 정책이 포함됩니다.

다음은 Performance:QoS Policy Groups 뷰의 몇 가지 중요한 필드입니다.

- QoS 정책 그룹: QoS 정책 그룹의 이름입니다. Unified Manager 9.7 이상으로 가져온 NSLM(NetApp Service Level Manager) 1.3 정책의 경우, 여기에 표시된 이름은 SVM 이름 및 NSLM에 성능 서비스 수준이 정의되어 있는 경우 이름에 포함되지 않은 기타 정보를 포함합니다. 예를 들어, "NSLM_vs6_Performance_2_0"이라는 이름은 SVM "vs6"에서 생성된 NSLM 시스템 정의 "성능" PSL 정책이며 예상되는 지연 시간은 "2ms/op"입니다.
- SVM: QoS 정책 그룹이 속하는 스토리지 VM(SVM) 스토리지 VM 이름을 클릭하여 해당 스토리지 VM의 세부 정보 페이지로 이동할 수 있습니다. 이 스토리지 VM 유형이 클러스터를 나타내므로 관리 스토리지 VM에서 QoS 정책이 생성된 경우 이 필드는 비어 있습니다.
- 최소 처리량: 정책 그룹이 제공할 수 있는 최소 처리량(IOPS)입니다. 적응형 정책의 경우 할당된 스토리지 개체 크기를 기준으로 볼륨 또는 LUN에 할당된 TB당 최소 예상 IOPS입니다.
- 최대 처리량: 정책 그룹이 초과하지 않아야 하는 처리량(IOPS 및/또는 MB/s)입니다. 이 필드가 비어 있으면 ONTAP에 정의된 최대값이 무한함을 의미합니다. 적응형 정책의 경우 할당된 스토리지 개체 크기 또는 사용된 스토리지 개체 크기를 기준으로 볼륨 또는 LUN에 할당된 TB당 가능한 최대 IOPS입니다.
- 절대 최소 IOPS: 적응형 정책의 경우 예상되는 IOPS가 이 값보다 작을 때 재정의로 사용되는 절대 최소 IOPS 값입니다.
- 블록 크기: QoS 적응형 정책에 지정된 블록 크기입니다.
- 최소 할당: "할당된 공간" 또는 "사용된 공간"을 사용하여 최대 처리량(피크) IOPS를 결정합니다.
- 예상 지연 시간: 스토리지 입출력 작업에 대해 예상되는 평균 지연 시간입니다.
- 공유: 기존 QoS 정책의 경우 정책 그룹에 정의된 처리량 값이 여러 오브젝트 간에 공유되는지 여부입니다.
- Associated Objects: QoS 정책 그룹에 할당된 워크로드 수입니다. 확장 단추( ) QoS 정책 그룹 이름 옆에 있는 을 클릭하여 정책 그룹에 대한 자세한 정보를 봅니다.
- Allocated Capacity: QoS 정책 그룹에 있는 오브젝트가 현재 사용하고 있는 공간의 크기입니다.
- Associated Objects: QoS 정책 그룹에 할당된 워크로드 수로, 볼륨 및 LUN으로 구분됩니다. 번호를 클릭하여 선택한 볼륨 또는 LUN에 대한 자세한 정보를 제공하는 페이지로 이동할 수 있습니다.

자세한 내용은 의 항목을 참조하십시오 "QoS 정책 그룹 정보를 사용하여 성능 관리".

성능 재고 페이지 콘텐츠 구체화

성능 개체의 인벤토리 페이지에는 개체 인벤토리 데이터 콘텐츠를 세밀하게 조정하는 데 도움이 되는 도구가 포함되어 있으므로 특정 데이터를 빠르고 쉽게 찾을 수 있습니다.

성능 개체 인벤토리 페이지에 포함된 정보는 대개 여러 페이지에 걸쳐 매우 광범위할 수 있습니다. 이러한 종류의 포괄적인 데이터는 성능 모니터링, 추적 및 개선에 뛰어나지만 특정 데이터를 찾으려면 원하는 데이터를 빠르게 찾을 수 있는 도구가 필요합니다. 따라서 성능 개체 인벤토리 페이지에는 검색, 정렬 및 필터링 기능이 포함되어 있습니다. 또한 검색 및 필터링이 함께 작동하여 결과를 더욱 좁힐 수 있습니다.

객체 재고 퍼포먼스 페이지에서 검색 중입니다

개체 인벤토리 성능 페이지에서 문자열을 검색할 수 있습니다. 페이지 오른쪽 위에 있는 * 검색 * 필드를 사용하여 개체 이름 또는 정책 이름을 기반으로 데이터를 빠르게 찾을 수 있습니다. 따라서 특정 객체 및 관련 데이터를 빠르게 찾거나 정책을 신속하게 찾고 관련 정책 객체 데이터를 볼 수 있습니다.

단계

1. 검색 요구 사항에 따라 다음 옵션 중 하나를 수행합니다.

찾는 방법...	이 항목 입력...
특정 개체	개체 이름을 * 검색 * 필드에 입력하고 * 검색 * 을 클릭합니다. 검색한 개체와 관련 데이터가 표시됩니다.
사용자 정의 성능 임계값 정책	정책 이름의 전체 또는 일부를 * 검색 * 필드에 입력하고 * 검색 * 을 클릭합니다. 검색한 정책에 할당된 객체가 표시됩니다.

객체 재고 퍼포먼스 페이지에서 정렬

객체 재고 퍼포먼스 페이지의 모든 데이터를 오름차순 또는 내림차순으로 정렬할 수 있습니다. 이를 통해 성능을 검사하거나 문제 해결 프로세스를 시작할 때 유용한 객체 재고 데이터를 빠르게 찾을 수 있습니다.

선택한 정렬 열은 강조 표시된 열 머리글 이름과 이름 오른쪽의 정렬 방향을 나타내는 화살표 아이콘으로 표시됩니다. 위쪽 화살표는 오름차순을 나타내고 아래쪽 화살표는 내림차순을 나타냅니다. 기본 정렬 순서는 * 상태 * (이벤트 중요도)로 내림차순으로 표시되며, 가장 중요한 성능 이벤트가 먼저 나열됩니다.

단계

1. 열 이름을 클릭하여 열의 정렬 순서를 오름차순 또는 내림차순으로 전환할 수 있습니다.

   객체 재고 퍼포먼스 페이지 내용은 선택한 열을 기준으로 오름차순 또는 내림차순으로 정렬됩니다.

개체 인벤토리 성능 페이지에서 데이터 필터링

객체 재고 퍼포먼스 페이지에서 데이터를 필터링하여 특정 기준에 따라 데이터를 빠르게 찾을 수 있습니다. 필터링을 사용하면 개체 재고 퍼포먼스 페이지의 내용을 좁혀 지정한 결과만 표시할 수 있습니다. 따라서 관심 있는 성능 데이터만 표시하는 매우 효율적인 방법이 제공됩니다.

필터링 패널을 사용하여 기본 설정에 따라 그리드 보기를 사용자 정의할 수 있습니다. 사용 가능한 필터 옵션은 격자에서 보는 개체 유형을 기반으로 합니다. 필터가 현재 적용된 경우 필터 단추 오른쪽에 적용된 필터 수가 표시됩니다.

세 가지 유형의 필터 매개 변수가 지원됩니다.

매개 변수	검증
문자열(텍스트)	연산자는 * 포함 *, * 다음으로 시작 *, * 로 끝 *, * 포함하지 않음 * 입니다.
번호	연산자는 * 보다 * 큼, * 보다 작음 *, * 마지막 * 에서 * 사이 * 입니다.
Enum(텍스트)	연산자는 * 이고 * 는 * 입니다.

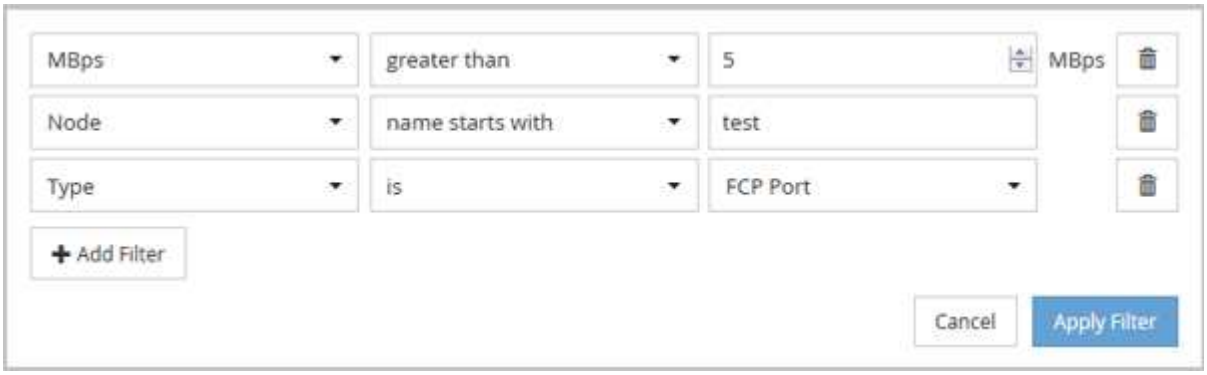
각 필터에는 열, 연산자 및 값 필드가 필요합니다. 사용 가능한 필터는 현재 페이지의 필터링 가능한 열을 반영합니다. 적용할 수 있는 최대 필터 수는 4개입니다. 필터링된 결과는 결합된 필터 매개 변수를 기반으로 합니다. 필터링된 결과는 현재 표시된 페이지뿐만 아니라 필터링된 검색의 모든 페이지에 적용됩니다.

필터링 패널을 사용하여 필터를 추가할 수 있습니다.

1. 페이지 맨 위에서 * 필터 * 버튼을 클릭합니다. Filtering(필터링) 패널이 표시됩니다.
2. 왼쪽 드롭다운 목록을 클릭하고 개체를 선택합니다(예: *Cluster* 또는 성능 카운터).
3. 가운데 드롭다운 목록을 클릭하고 사용할 연산자를 선택합니다.
4. 마지막 목록에서 값을 선택하거나 입력하여 해당 개체에 대한 필터를 완료합니다.
5. 다른 필터를 추가하려면 * + 필터 추가 * 를 클릭합니다. 추가 필터 필드가 표시됩니다. 위의 단계에 설명된 프로세스를 사용하여 이 필터를 완료합니다. 네 번째 필터를 추가하면 * + 필터 추가 * 버튼이 더 이상 표시되지 않습니다.
6. 필터 적용 * 을 클릭합니다. 필터 옵션이 그리드에 적용되고 필터 버튼 오른쪽에 필터 수가 표시됩니다.
7. 필터 패널을 사용하여 제거할 필터의 오른쪽에 있는 휴지통 아이콘을 클릭하여 개별 필터를 제거합니다.
8. 모든 필터를 제거하려면 필터링 패널 하단에 있는 * Reset * (재설정 *)을 클릭합니다.

필터링 예제

그림에는 3개의 필터가 있는 필터링 패널이 나와 있습니다. 최대 4개 이하의 필터가 있는 경우 * + 필터 추가 * 버튼이 표시됩니다.



필터 적용 * 을 클릭하면 필터링 패널이 닫히고 필터가 적용되고 적용된 필터 수가 표시됩니다(3)를 클릭합니다.

데이터를 클라우드에 계층화하도록 **Unified Manager**의 권장 사항 이해

Performance: All Volumes(성능: 모든 볼륨) 보기에는 비활성(콜드) 상태인 볼륨에 저장된 사용자 데이터의 크기와 관련된 정보가 표시됩니다. 경우에 따라 Unified Manager에서 FabricPool 지원 애그리게이트의 클라우드 계층(클라우드 공급자 또는 StorageGRID)에 비활성 데이터를 계층화함으로써 이점을 얻을 수 있는 특정 볼륨을 식별합니다.

FabricPool는 ONTAP 9.2에서 소개된 것으로, ONTAP 소프트웨어 9.2 이전 버전을 사용하는 경우 데이터를 계층화하려면 ONTAP 소프트웨어를 업그레이드해야 하는 Unified Manager의 권장사항이 됩니다. 또한 ONTAP 9.4에 ' * auto * ' 계층화 정책이 도입되었으며 ' * all * ' 계층화 정책이 ONTAP 9.6에 도입되었으므로 자동 계층화 정책을 사용하는 것이 권장된다면 ONTAP 9.4 이상으로 업그레이드해야 합니다.

성능: 모든 볼륨 보기는 비활성 데이터를 클라우드 계층으로 이동하여 스토리지 시스템의 디스크 사용률을 높이고 성능 계층의 공간을 절약할 수 있는지 여부에 대한 정보를 제공합니다.

- * 계층화 정책 *

  계층화 정책은 볼륨의 데이터가 성능 계층에 유지되는지 또는 일부 데이터가 성능 계층에서 클라우드 계층으로 이동되는지 여부를 결정합니다.

  이 필드의 값은 볼륨이 현재 FabricPool 애그리게이트에 없는 경우에도 볼륨에 설정된 계층화 정책을 나타냅니다. 계층화 정책은 볼륨이 FabricPool 애그리게이트에 있는 경우에만 적용됩니다.

- * 콜드 데이터 *

  콜드 데이터는 비활성(콜드) 상태인 볼륨에 저장된 사용자 데이터의 크기를 표시합니다.

  ONTAP 9.4 이상 소프트웨어를 사용할 때만 여기에 값이 표시됩니다. 볼륨이 배포된 집계에 ' * inactive data reporting parameter * '가 ' * enabled * '로 설정되어 있어야 하기 때문입니다. 그리고 최소 냉각 일수 임계값이 충족되었습니다(' * 스냅샷 전용 *' 또는 ' * 자동 *' 계층화 정책을 사용하는 볼륨의 경우). 그렇지 않으면 값이 ""N/A""로 표시됩니다.

- * 클라우드 권장사항 *

  볼륨의 데이터 활동에 대한 정보가 충분히 수집되면 Unified Manager에서 아무런 조치가 필요하지 않는지, 아니면 비활성 데이터를 클라우드 계층으로 계층화하여 성능 계층의 공간을 절약할 수 있는지 확인할 수 있습니다.

콜드 데이터 필드는 15분마다 업데이트되지만, 콜드 데이터 분석이 볼륨에 대해 수행되는 7일마다 클라우드 권장 사항 필드가 업데이트됩니다. 따라서 필드 간에 정확한 양의 콜드 데이터가 다를 수 있습니다. 클라우드 권장 사항 필드에는 분석이 실행된 날짜가 표시됩니다.

비활성 데이터 보고가 활성화되면 Cold Data(콜드 데이터) 필드에 정확한 양의 비활성 데이터가 표시됩니다. 비활성 데이터 보고 기능이 없으면 Unified Manager는 성능 통계를 사용하여 데이터가 볼륨에 비활성 상태인지 확인합니다. 이 경우 비활성 데이터의 양은 Cold Data(콜드 데이터) 필드에 표시되지 않지만, 커서를 * Tier * 라는 단어 위로 가져가면 클라우드 권장 사항을 볼 수 있습니다.

다음과 같은 클라우드 권장 사항이 표시됩니다.

- * 학습 *. 권장 사항을 만들 데이터가 충분하지 않습니다.

- * 계층 *. 분석 결과, 볼륨에 비활성(콜드) 데이터가 포함되어 있고 해당 데이터를 클라우드 계층으로 이동하도록 볼륨을 구성해야 합니다. 경우에 따라 먼저 볼륨을 FabricPool 지원 애그리게이트로 이동해야 할 수 있습니다. 볼륨이 이미 FabricPool 애그리게이트에 있는 경우에는 계층화 정책만 변경하면 됩니다.
- * 작업 없음 *. 볼륨에 비활성 데이터가 거의 없거나 FabricPool 애그리게이트에 "자동" 계층화 정책으로 이미 설정되어 있거나 볼륨이 데이터 보호 볼륨입니다. 이 값은 볼륨이 오프라인이거나 MetroCluster 구성에서 사용 중일 때도 표시됩니다.

볼륨을 이동하거나 볼륨 계층화 정책 또는 애그리게이트 비활성 데이터 보고 설정을 변경하려면 ONTAP System Manager, ONTAP CLI 명령 또는 이러한 툴의 조합을 사용합니다.

애플리케이션 관리자 또는 스토리지 관리자 역할로 Unified Manager에 로그인한 경우, * 계층 * 이라는 단어 위에 커서를 올리면 클라우드 권장 사항에서 * 볼륨 구성 * 링크를 사용할 수 있습니다. 이 버튼을 클릭하여 System Manager에서 Volumes 페이지를 열어 권장 사항을 변경합니다.

성능 탐색기 페이지를 사용하여 성능 모니터링

성능 탐색기 페이지에는 클러스터의 각 개체 성능에 대한 자세한 정보가 표시됩니다. 이 페이지에서는 모든 클러스터 개체의 성능을 자세하게 보여 주기 때문에 다양한 기간에 걸쳐 특정 개체의 성능 데이터를 선택하고 비교할 수 있습니다.

또한 모든 개체의 전체 성능을 평가하고 오브젝트 성능 데이터를 side-by-side 형식으로 비교할 수도 있습니다.

루트 개체 이해

루트 개체는 다른 개체를 비교할 때 기준이 되는 기준점입니다. 이를 통해 다른 개체의 데이터를 루트 개체와 보고 비교할 수 있으며 성능 데이터 분석을 제공하여 개체 성능 문제를 해결하고 향상할 수 있습니다.

루트 개체 이름이 비교 창 맨 위에 표시됩니다. 추가 개체는 루트 개체 아래에 표시됩니다. 비교 창에 추가할 수 있는 추가 개체 수에 제한이 없지만 루트 개체는 하나만 허용됩니다. 루트 개체의 데이터는 카운터 차트 창의 그래프에 자동으로 표시됩니다.

루트 개체는 변경할 수 없으며 항상 보고 있는 개체 페이지로 설정됩니다. 예를 들어, 볼륨1의 볼륨 성능 탐색기 페이지를 열면 볼륨1이 루트 개체이므로 변경할 수 없습니다. 다른 루트 개체와 비교하려면 개체의 링크를 클릭하고 해당 랜딩 페이지를 열어야 합니다.

이벤트 및 임계값은 루트 객체에 대해서만 표시됩니다.

필터링을 적용하여 그리드의 상관 오브젝트 목록을 줄입니다

필터링을 사용하면 그리드에서 더 작고 잘 정의된 개체 하위 집합을 표시할 수 있습니다. 예를 들어, 그리드에 볼륨이 25개 있는 경우 필터링을 사용하면 처리량이 90Mbps 미만이거나 지연 시간이 1ms/op보다 큰 볼륨만 볼 수 있습니다.

상관 오브젝트에 대한 시간 범위 지정

성능 탐색기 페이지의 시간 범위 선택기를 사용하면 개체 데이터 비교의 시간 범위를 지정할 수

있습니다. 시간 범위를 지정하면 성능 탐색기 페이지의 내용이 구체화되어 지정한 시간 범위 내의 개체 데이터만 표시됩니다.

시간 범위를 구체화하면 관심 있는 성능 데이터만 효율적으로 표시할 수 있습니다. 미리 정의된 시간 범위를 선택하거나 사용자 지정 시간 범위를 지정할 수 있습니다. 기본 시간 범위는 이전 72시간입니다.

미리 정의된 시간 범위 선택

사전 정의된 시간 범위를 선택하면 클러스터 오브젝트 성능 데이터를 볼 때 데이터 출력을 사용자 지정하고 초점을 맞출 수 있는 빠르고 효율적인 방법이 있습니다. 미리 정의된 시간 범위를 선택하면 최대 13개월까지 데이터를 사용할 수 있습니다.

단계

1. Performance Explorer * 페이지 오른쪽 상단에서 * 시간 범위 * 를 클릭합니다.
2. Time Range Selection* 패널의 오른쪽에서 미리 정의된 시간 범위를 선택합니다.
3. 범위 적용 * 을 클릭합니다.

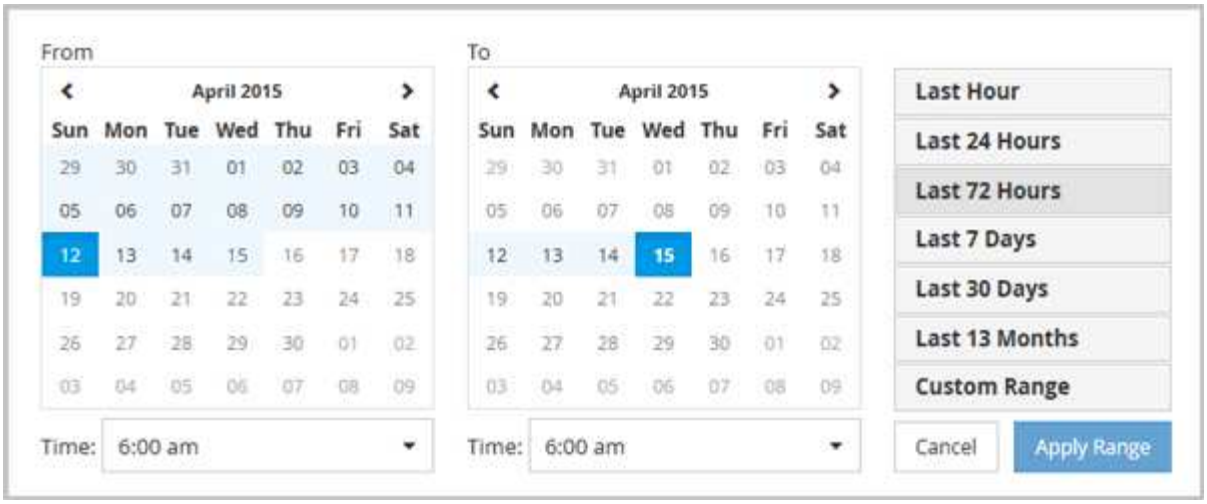
사용자 지정 시간 범위 지정

성능 탐색기 페이지에서 성능 데이터의 날짜 및 시간 범위를 지정할 수 있습니다. 사용자 지정 시간 범위를 지정하면 클러스터 오브젝트 데이터를 정제할 때 미리 정의된 시간 범위를 사용할 때보다 더 많은 유연성을 제공합니다.

1시간에서 390일 사이의 시간 범위를 선택할 수 있습니다. 13개월은 매월 30일로 계산되므로 390일입니다. 날짜 및 시간 범위를 지정하면 보다 자세한 정보를 얻을 수 있으며 특정 성능 이벤트 또는 일련의 이벤트를 확대할 수 있습니다. 또한 시간 범위를 지정하면 날짜 및 시간 범위를 지정하면 성능 이벤트 관련 데이터를 보다 자세하게 표시할 수 있으므로 잠재적인 성능 문제를 해결하는 데 도움이 됩니다. [시간 범위*] 컨트롤을 사용하여 미리 정의된 날짜 및 시간 범위를 선택하거나 최대 390일의 사용자 지정 날짜 및 시간 범위를 지정할 수 있습니다. 미리 정의된 시간 범위의 버튼은 * Last Hour * 에서 * Last 13 Months * 까지 다양합니다.

지난 13개월 * 옵션을 선택하거나 30일을 초과하는 사용자 지정 날짜 범위를 지정하면 30일이 넘는 기간 동안 표시되는 성능 데이터가 5분 데이터 폴링이 아닌 시간별 평균을 사용하여 차트로 작성된다는 알림 대화 상자가 표시됩니다. 따라서 타임라인 시각적 세분화가 손실될 수 있습니다. 대화 상자에서 * 다시 표시 안 함 * 옵션을 클릭하면 * 지난 13개월 * 옵션을 선택하거나 30일을 초과하는 사용자 지정 날짜 범위를 지정하면 메시지가 나타나지 않습니다. 시간 범위에 오늘부터 30일이 넘는 시간/날짜가 포함된 경우 요약 데이터도 더 작은 시간 범위에 적용됩니다.

시간 범위(사용자 지정 또는 미리 정의된 시간)를 선택할 때 30일 이하의 시간 범위는 5분 간격 데이터 샘플을 기준으로 합니다. 30일을 초과하는 시간 범위는 1시간 간격 데이터 샘플을 기준으로 합니다.



1. Time Range * (시간 범위 *) 드롭다운 상자를 클릭하면 Time Range (시간 범위) 패널이 표시됩니다.
2. 미리 정의된 시간 범위를 선택하려면 * Time Range * (시간 범위) 패널 오른쪽에 있는 * Last… * (마지막… *) 버튼 중 하나를 클릭합니다. 미리 정의된 시간 범위를 선택하면 최대 13개월까지 데이터를 사용할 수 있습니다. 선택한 미리 정의된 시간 범위 단추가 강조 표시되고 해당 날짜 및 시간이 달력 및 시간 선택기에 표시됩니다.
3. 사용자 지정 날짜 범위를 선택하려면 왼쪽의 * From * 달력에서 시작 날짜를 클릭합니다. 일정에서 앞으로 또는 뒤로 이동하려면 * < * 또는 * > * 를 클릭합니다. 종료 날짜를 지정하려면 오른쪽의 * to * 달력에서 날짜를 클릭합니다. 다른 종료 날짜를 지정하지 않는 한 기본 종료 날짜는 오늘입니다. Time Range(시간 범위) 패널 오른쪽에 있는 * Custom Range *(사용자 지정 범위 *) 버튼이 강조 표시되어 사용자 지정 날짜 범위를 선택했음을 나타냅니다.
4. 사용자 지정 시간 범위를 선택하려면 * From * 달력 아래의 * Time * 컨트롤을 클릭하고 시작 시간을 선택합니다. 종료 시간을 지정하려면 오른쪽의 * to * 달력 아래에 있는 * Time * 컨트롤을 클릭하고 종료 시간을 선택합니다. Time Range(시간 범위) 패널 오른쪽에 있는 * Custom Range *(사용자 지정 범위 *) 버튼이 강조 표시되어 사용자 지정 시간 범위를 선택했음을 나타냅니다.
5. 선택적으로 미리 정의된 날짜 범위를 선택할 때 시작 및 종료 시간을 지정할 수 있습니다. 앞서 설명한 대로 미리 정의된 날짜 범위를 선택한 다음 앞서 설명한 시작 및 종료 시간을 선택합니다. 선택한 날짜가 달력에서 강조 표시되고 지정된 시작 및 종료 시간이 * 시간 * 컨트롤에 표시되고 * 사용자 지정 범위 * 버튼이 강조 표시됩니다.
6. 날짜 및 시간 범위를 선택한 후 * 범위 적용 * 을 클릭합니다. 해당 시간 범위의 성능 통계는 차트와 이벤트 타임라인에 표시됩니다.

비교 그래프 작성을 위해 상관 오브젝트 목록을 정의합니다

카운터 차트 창에서 데이터 및 성능 비교에 대한 상호 연결된 개체의 목록을 정의할 수 있습니다. 예를 들어, SVM(스토리지 가상 시스템)에 성능 문제가 발생하는 경우 SVM의 모든 볼륨을 비교하여 문제를 일으킬 수 있는 볼륨을 식별할 수 있습니다.

상관 오브젝트 격자의 모든 오브젝트를 비교 및 카운터 차트 창에 추가할 수 있습니다. 따라서 여러 오브젝트 및 루트 객체의 데이터를 보고 비교할 수 있습니다. 상관 오브젝트 그리드에 객체를 추가하거나 상관 오브젝트 그리드에서 객체를 제거할 수 있지만 비교 창의 루트 객체는 제거할 수 없습니다.

비교 창에 많은 개체를 추가하면 성능에 부정적인 영향을 줄 수 있습니다. 성능을 유지하려면 데이터 비교를 위해 제한된 수의 차트를 선택해야 합니다.

단계

1. 개체 그리드에서 추가할 개체를 찾고 * 추가 * 단추를 클릭합니다.

Add * (추가 *) 버튼이 회색으로 바뀌고 비교 창의 추가 개체 목록에 개체가 추가됩니다. 오브젝트의 데이터는 Counter Charts 창의 그래프에 추가됩니다. 개체의 눈 아이콘( )는 그래프의 오브젝트 데이터 추세 선 색상과 일치합니다.

2. * 선택 사항: * 선택한 개체의 데이터를 숨기거나 표시합니다.

수행할 작업...	이 작업 수행...
선택한 개체를 숨깁니다	선택한 개체의 눈 아이콘( )를 선택합니다. 개체의 데이터가 숨겨지고 해당 개체의 눈 아이콘이 회색으로 바뀝니다.
숨겨진 개체를 표시합니다	비교 창에서 선택한 개체의 회색 눈 아이콘을 클릭합니다. 눈 아이콘이 원래 색으로 돌아가고 개체 데이터가 카운터 차트 창의 그래프에 다시 추가됩니다.

3. * 선택 사항: * 비교 * 창에서 선택한 개체를 제거합니다.

수행할 작업...	이 작업 수행...
선택한 개체를 제거합니다	비교 창에서 선택한 개체의 이름 위로 마우스를 가져가 개체 제거 단추(* X*)를 표시한 다음 단추를 클릭합니다. 비교 창에서 개체가 제거되고 카운터 차트에서 해당 데이터가 지워집니다.
선택한 개체를 모두 제거합니다	비교 창 맨 위에 있는 모든 개체 제거 단추(* X*)를 클릭합니다. 루트 개체만 남겨두고 선택한 모든 개체와 해당 데이터가 제거됩니다.

카운터 차트 이해

카운터 차트 창의 차트를 사용하면 루트 개체 및 상호 연결된 개체 표에서 추가한 개체의 성능 데이터를 보고 비교할 수 있습니다. 이를 통해 성능 추세를 파악하고 성능 문제를 격리 및 해결할 수 있습니다.

기본적으로 표시되는 카운터 차트는 이벤트, 지연 시간, IOPS 및 MBPS입니다. 활용도, 사용된 성능 용량, 사용 가능한 IOPS, IOPS/TB 및 캐시 비적중 비율 중에서 선택할 수 있는 옵션 차트입니다. 또한 지연 시간, IOPS, MBps 및 사용된 성능 용량 차트에 대한 총 값 또는 분석 값을 표시하도록 선택할 수 있습니다.

성능 탐색기에는 스토리지 개체에서 해당 카운터 차트를 모두 지원하는지 여부와 같은 특정 카운터 차트가 기본적으로 표시됩니다. 카운터가 지원되지 않으면 카운터 차트가 비어 있고 '<object>에 적용할 수 없음' 메시지가 표시됩니다.

차트는 비교 창에서 선택한 모든 개체와 루트 개체의 성능 추세를 표시합니다. 각 차트의 데이터는 다음과 같이 정렬됩니다.

- * X 축 *

지정된 기간을 표시합니다. 시간 범위를 지정하지 않은 경우 기본값은 이전 72시간 기간입니다.

- * Y 축 *

  선택한 오브젝트 또는 오브젝트에 고유한 카운터 단위를 표시합니다.

추세 선 색상은 비교 창에 표시된 개체 이름의 색상과 일치합니다. 추세 선 위에 커서를 놓으면 해당 지점에 대한 시간 및 값에 대한 세부 정보를 볼 수 있습니다.

차트 내의 특정 기간을 조사하려면 다음 방법 중 하나를 사용합니다.

- 카운터 차트 창을 확장하여 페이지 너비를 넓히려면 * < * 버튼을 사용합니다.
- 커서를 사용하여(돋보기로 전환 시) 차트에서 해당 영역에 초점을 맞추고 확대할 기간을 선택합니다. 차트 확대/축소 원래대로를 클릭하여 차트를 기본 시간 값으로 되돌릴 수 있습니다.
- 확대/축소 보기 * 버튼을 사용하면 확장된 세부 정보와 임계값 표시기가 포함된 큰 단일 카운터 차트를 표시할 수 있습니다.

때때로 추세선의 간격이 표시됩니다. 격차의 경우 Unified Manager가 스토리지 시스템에서 성능 데이터를 수집하지 못했거나 Unified Manager가 중단되었을 수 있습니다.

성능 카운터 차트의 유형입니다

선택한 스토리지 개체의 카운터 값을 표시하는 표준 성능 차트가 있습니다. 각 분석 결과 카운터 차트는 읽기, 쓰기 및 기타 범주로 구분된 총 값을 표시합니다. 또한 일부 분석 카운터 차트는 확대/축소 보기에 차트가 표시될 때 추가 세부 정보를 표시합니다.

다음 표에서는 사용 가능한 성능 카운터 차트를 보여 줍니다.

사용 가능한 차트	차트 설명
이벤트	루트 개체에 대한 통계 차트와 관련된 중요, 오류, 경고 및 정보 이벤트를 표시합니다. 성능 이벤트와 함께 상태 이벤트가 표시되어 성능이 영향을 받을 수 있는 이유를 완벽하게 파악할 수 있습니다.
지연 시간 - 합계	애플리케이션 요청에 응답하는 데 필요한 밀리초 수입니다. 평균 지연 시간 값은 I/O 가중치입니다.
지연 시간 - 분류	지연 시간 합계 에 표시된 것과 동일한 정보이지만, 성능 데이터는 읽기, 쓰기 및 기타 지연 시간으로 구분됩니다. 이 차트 옵션은 선택한 오브젝트가 SVM, 노드, 애그리게이트, 볼륨, LUN인 경우에만 적용됩니다. 네임스페이스입니다.
지연 시간 - 클러스터 구성 요소	지연 시간 합계에 표시되는 것과 동일한 정보이지만, 성능 데이터가 클러스터 구성 요소별로 지연 시간으로 분리되어 있습니다. 이 차트 옵션은 선택한 개체가 볼륨일 때만 적용됩니다.

사용 가능한 차트	차트 설명
IOPS - 합계	초당 처리되는 입출력 작업 수입니다. 노드에 대해 ""합계"를 선택하면 로컬 또는 원격 노드에 있을 수 있는 이 노드를 통해 이동하는 데이터의 IOPS가 표시되고 ""합계(로컬)"를 선택하면 현재 노드에만 있는 데이터의 IOPS가 표시됩니다.
IOPS - 분류	IOPS Total에 표시된 것과 동일한 정보이지만, 성능 데이터는 읽기, 쓰기 및 기타 IOPS로 구분됩니다. 이 차트 옵션은 선택한 오브젝트가 SVM, 노드, 애그리게이트, 볼륨, LUN인 경우에만 적용됩니다. 네임스페이스입니다. Zoom(확대/축소) 보기에 표시된 볼륨 차트는 ONTAP에서 구성된 경우 QoS 최소 및 최대 처리량 값을 표시합니다. 노드에 대해 표시되는 경우 ""고장""을 선택하면 로컬 또는 원격 노드에 있을 수 있는 이 노드를 통해 이동하는 데이터에 대한 IOPS 분석 결과가 표시되고 ""고장(로컬)""을 선택하면 현재 노드에만 있는 데이터에 대한 IOPS 분석 결과가 표시됩니다.
IOPS - 프로토콜	IOPS Total에 표시된 것과 동일한 정보이지만 성능 데이터는 CIFS, NFS, FCP, NVMe 및 iSCSI 프로토콜 트래픽에 대한 개별 차트로 구분됩니다. 이 차트 옵션은 선택한 개체가 SVM 인 경우에만 적용됩니다.
IOPS/TB - 합계	워크로드에서 소비하는 총 공간(TB)을 기준으로 초당 처리되는 입출력 작업의 수입니다. I/O 밀도라고도 하는 이 카운터는 지정된 양의 스토리지 용량으로 제공할 수 있는 성능을 측정합니다. Zoom(확대/축소) 보기에 표시된 볼륨 차트에는 ONTAP에서 구성된 경우 QoS 예상 및 최대 처리량 값이 표시됩니다. 이 차트 옵션은 선택한 개체가 볼륨일 때만 적용됩니다.
MB/s - 합계	오브젝트에서 초당 전송된 데이터 크기(MB)입니다.

사용 가능한 차트	차트 설명
MB/s - 고장	MB/s 차트에 표시되는 것과 동일한 정보이지만 처리량 데이터가 디스크 읽기, Flash Cache 읽기, 쓰기 등으로 분리되어 있습니다. Zoom(확대/축소) 보기에 표시되는 볼륨 차트는 ONTAP에서 구성된 경우 QoS 최대 처리량 값을 표시합니다. 이 차트 옵션은 선택한 오브젝트가 SVM, 노드, 애그리게이트, 볼륨, LUN인 경우에만 적용됩니다. 네임스페이스입니다. Flash Cache 데이터는 노드에 대해서만 표시되며 Flash Cache 모듈이 노드에 설치된 경우에만 표시됩니다.
사용된 성능 용량 - 합계	노드 또는 애그리게이트에 사용되고 있는 성능 용량의 비율입니다.
사용된 성능 용량 - 분류	성능 용량 사용 데이터를 사용자 프로토콜과 시스템 백그라운드 프로세스로 분리합니다. 또한 여유 성능 용량이 표시됩니다.
사용 가능한 IOPS - 합계	이 개체에서 현재 사용 가능한(사용 가능) 초당 입출력 작업 수입니다. 이 수치는 Unified Manager에서 해당 객체가 수행할 수 있는 총 IOPS에서 현재 사용된 IOPS를 뺀 결과입니다. 이 차트 옵션은 선택한 개체가 노드 또는 집합인 경우에만 적용됩니다.
Utilization - 총	사용 중인 개체의 사용 가능한 리소스 백분율입니다. 사용률은 노드의 노드 활용률, 애그리게이트의 디스크 활용률, 포트의 대역폭 활용률을 나타냅니다. 이 차트 옵션은 선택한 오브젝트가 노드, 애그리게이트 또는 포트인 경우에만 적용됩니다.
캐시 비적중 비율 - 합계	캐시에서 반환되지 않고 디스크에서 반환된 클라이언트 애플리케이션의 읽기 요청 비율입니다. 이 차트 옵션은 선택한 개체가 볼륨일 때만 적용됩니다.

표시할 성능 차트를 선택합니다

차트 선택 드롭다운 목록을 사용하면 카운터 차트 창에 표시할 성능 카운터 차트 종류를 선택할 수 있습니다. 따라서 성능 요구 사항에 따라 특정 데이터와 카운터를 볼 수 있습니다.

단계

1. Counter Charts * 창에서 * Charts * 선택 드롭다운 목록을 클릭합니다.
2. 차트 추가 또는 제거:

대상...	수행할 작업...
개별 차트를 추가하거나 제거합니다	표시하거나 숨길 차트 옆의 확인란을 클릭합니다
모든 차트를 추가합니다	모두 선택 * 을 클릭합니다
모든 차트를 제거합니다	모두 선택 취소 * 를 클릭합니다

차트 선택 항목이 Counter Charts(카운터 차트) 창에 표시됩니다. 차트를 추가할 때 차트 선택 드롭다운 목록에 나열된 차트 순서와 일치하도록 새 차트가 카운터 차트 창에 삽입됩니다. 추가 차트를 선택하려면 추가로 스크롤해야 할 수도 있습니다.

카운터 차트 창 확장

차트를 더 크고 읽기 쉽게 만들 수 있도록 카운터 차트 창을 확장할 수 있습니다.

카운터의 비교 개체와 시간 범위를 정의한 후에는 더 큰 카운터 차트 창을 볼 수 있습니다. 성능 탐색기 창의 중간에 있는 * < * 버튼을 사용하여 창을 확장합니다.

단계

1. Counter Charts * 창을 확장하거나 축소합니다.

대상...	수행할 작업...
페이지 너비에 맞게 Counter Charts(카운터 차트) 창을 확장합니다	• < * 버튼을 클릭합니다
카운터 차트 창을 페이지의 오른쪽 반으로 줄입니다	• > * 버튼을 클릭합니다

카운터 차트 포커스를 짧은 기간으로 변경합니다

마우스를 사용하여 카운터 차트 창 또는 카운터 차트 확대/축소 보기 창에서 특정 기간에 초점을 맞출 시간 범위를 줄일 수 있습니다. 이를 통해 성능 데이터, 이벤트 및 임계값 일정의 모든 부분에 대한 보다 세부적이고 미세한 보기를 확인할 수 있습니다.

- 필요한 것 *

커서가 돋보기 모양으로 변경되어 이 기능이 활성화되었음을 나타내야 합니다.

타임라인을 변경하여 더 세밀한 디스플레이에 해당하는 값을 표시하는 이 기능을 사용할 경우 * 시간 범위 * 선택기의 시간 및 날짜 범위는 차트의 원래 값에서 변경되지 않습니다.

단계

1. 특정 기간을 확대하려면 돋보기 사용을 클릭하고 마우스를 드래그하여 자세히 보려는 영역을 강조 표시합니다.

   선택한 기간의 카운터 값이 카운터 차트를 채웁니다.

2. 시간 범위* 선택기에 설정된 원래 시간으로 돌아가려면 * 차트 확대/축소 재설정 * 버튼을 클릭합니다.

   카운터 차트는 원래 상태로 표시됩니다.

이벤트 타임라인에서 이벤트 세부 정보 보기

성능 탐색기의 이벤트 일정 창에서 모든 이벤트와 관련 세부 정보를 볼 수 있습니다. 이 방법은 지정된 시간 범위 동안 루트 개체에서 발생한 모든 상태 및 성능 이벤트를 빠르고 효율적으로 보는 방법으로 성능 문제를 해결할 때 유용할 수 있습니다.

이벤트 타임라인 창에는 선택한 시간 범위 동안 루트 개체에서 발생한 중요, 오류, 경고 및 정보 이벤트가 표시됩니다. 각 이벤트 심각도에는 고유한 타임라인이 있습니다. 단일 및 여러 이벤트는 시각표에서 이벤트 점으로 표시됩니다. 이벤트 점 위에 커서를 놓으면 이벤트 세부 정보를 볼 수 있습니다. 여러 이벤트의 시각적 세분화를 높이려면 시간 범위를 줄일 수 있습니다. 이렇게 하면 여러 이벤트가 단일 이벤트로 분산되므로 각 이벤트를 별도로 보고 조사할 수 있습니다.

이벤트 시각표의 각 성능 이벤트 점은 이벤트 타임라인 아래에 표시되는 카운터 차트 추세선의 해당 급증을 사용하여 세로로 배열됩니다. 따라서 이벤트와 전체 성능 간에 직접적인 시각적 상관 관계가 형성됩니다. 상태 이벤트는 타임라인에도 표시되지만 이러한 유형의 이벤트가 성능 차트 중 하나에서 급증한 것과 반드시 일치하지는 않습니다.

단계

1. 이벤트 시각표 * 창에서 타임라인의 이벤트 점 위에 커서를 놓으면 해당 이벤트 지점의 이벤트 또는 이벤트 요약을 볼 수 있습니다.

   팝업 대화 상자에는 이벤트 유형, 이벤트가 발생한 날짜 및 시간, 상태 및 이벤트 기간에 대한 정보가 표시됩니다.

2. 하나의 이벤트 또는 여러 이벤트에 대한 전체 이벤트 세부 정보 보기:

수행할 작업...	이...
단일 이벤트에 대한 세부 정보를 봅니다	• 팝업 대화 상자에서 이벤트 세부 정보 * 를 봅니다.
여러 이벤트에 대한 세부 정보를 봅니다	• 팝업 대화 상자에서 이벤트 세부 정보 * 를 봅니다. 다중 이벤트 대화 상자에서 단일 이벤트를 클릭하면 해당 이벤트 세부 정보 페이지가 표시됩니다.

카운터 차트 확대/축소 보기

카운터 차트는 지정된 기간 동안 성능 세부 정보를 확대할 수 있는 확대/축소 보기를 제공합니다. 이렇게 하면 성능 세부 정보와 이벤트를 훨씬 더 세부적으로 확인할 수 있으므로 성능 문제를 해결할 때 유용합니다.

확대/축소 보기에 표시된 일부 분석 차트는 차트가 확대/축소 보기에 없을 때 표시되는 것보다 더 많은 정보를 제공합니다. 예를 들어 IOPS, IOPS/TB 및 MBPS 분석 차트 확대/축소 보기 페이지는 ONTAP에 설정된 볼륨 및 LUN에 대한 QoS 정책 값을 표시합니다.

시스템 정의 성능 임계값 정책의 경우 "노드 리소스 초과 사용" 및 "QoS 처리량 제한 위반" 정책만 * 정책 * 목록에서 사용할 수 있습니다. 현재 다른 시스템 정의 임계값 정책을 사용할 수 없습니다.

카운터 차트 확대/축소 보기 표시

Counter Charts Zoom View(카운터 차트 확대/축소 보기)는 선택한 카운터 차트 및 관련 타임라인에 대한 세부 정보를 제공합니다. 이렇게 하면 카운터 차트 데이터가 확대되어 성능 이벤트와 그 근본 원인을 보다 선명하게 볼 수 있습니다.

모든 카운터 차트에 대해 카운터 차트 확대/축소 보기를 표시할 수 있습니다.

단계

1. 선택한 차트를 새 브라우저 창으로 열려면 * 확대/축소 보기 * 를 클릭합니다.
2. 분석 차트를 보고 있는 경우 * 확대/축소 보기 * 를 클릭하면 분석 차트가 확대/축소 보기에 표시됩니다. 보기 옵션을 변경하려면 확대/축소 보기에서 * 전체 * 를 선택할 수 있습니다.

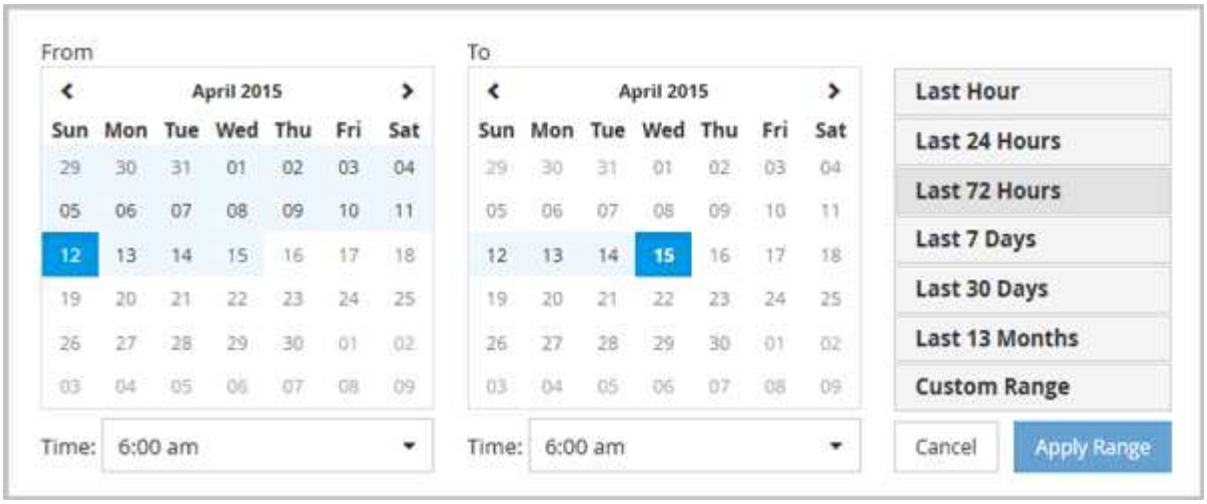
확대/축소 보기에서 시간 범위 지정

Counter Charts Zoom View 창의 * Time Range * 컨트롤을 사용하면 선택한 차트의 날짜 및 시간 범위를 지정할 수 있습니다. 이를 통해 사전 설정된 시간 범위 또는 사용자 지정 시간 범위를 기반으로 특정 데이터를 빠르게 찾을 수 있습니다.

1시간에서 390일 사이의 시간 범위를 선택할 수 있습니다. 13개월은 매월 30일로 계산되므로 390일입니다. 날짜 및 시간 범위를 지정하면 보다 자세한 정보를 얻을 수 있으며 특정 성능 이벤트 또는 일련의 이벤트를 확대할 수 있습니다. 또한 시간 범위를 지정하면 날짜 및 시간 범위를 지정하면 성능 이벤트 관련 데이터를 보다 자세하게 표시할 수 있으므로 잠재적인 성능 문제를 해결하는 데 도움이 됩니다. [시간 범위*] 컨트롤을 사용하여 미리 정의된 날짜 및 시간 범위를 선택하거나 최대 390일의 사용자 지정 날짜 및 시간 범위를 지정할 수 있습니다. 미리 정의된 시간 범위의 버튼은 * Last Hour * 에서 * Last 13 Months * 까지 다양합니다.

지난 13개월 * 옵션을 선택하거나 30일을 초과하는 사용자 지정 날짜 범위를 지정하면 30일이 넘는 기간 동안 표시되는 성능 데이터가 5분 데이터 폴링이 아닌 시간별 평균을 사용하여 차트로 작성된다는 알림 대화 상자가 표시됩니다. 따라서 타임라인 시각적 세분화가 손실될 수 있습니다. 대화 상자에서 * 다시 표시 안 함 * 옵션을 클릭하면 * 지난 13개월 * 옵션을 선택하거나 30일을 초과하는 사용자 지정 날짜 범위를 지정하면 메시지가 나타나지 않습니다. 시간 범위에 오늘부터 30일이 넘는 시간/날짜가 포함된 경우 요약 데이터도 더 작은 시간 범위에 적용됩니다.

시간 범위(사용자 지정 또는 미리 정의된 시간)를 선택할 때 30일 이하의 시간 범위는 5분 간격 데이터 샘플을 기준으로 합니다. 30일을 초과하는 시간 범위는 1시간 간격 데이터 샘플을 기준으로 합니다.



1. Time Range * (시간 범위 *) 드롭다운 상자를 클릭하면 Time Range (시간 범위) 패널이 표시됩니다.
2. 미리 정의된 시간 범위를 선택하려면 * Time Range * (시간 범위) 패널 오른쪽에 있는 * Last… * (마지막… *) 버튼 중 하나를 클릭합니다. 미리 정의된 시간 범위를 선택하면 최대 13개월까지 데이터를 사용할 수 있습니다. 선택한 미리 정의된 시간 범위 단추가 강조 표시되고 해당 날짜 및 시간이 달력 및 시간 선택기에 표시됩니다.
3. 사용자 지정 날짜 범위를 선택하려면 왼쪽의 * From * 달력에서 시작 날짜를 클릭합니다. 일정에서 앞으로 또는 뒤로 이동하려면 * < * 또는 * > * 를 클릭합니다. 종료 날짜를 지정하려면 오른쪽의 * to * 달력에서 날짜를 클릭합니다. 다른 종료 날짜를 지정하지 않는 한 기본 종료 날짜는 오늘입니다. Time Range(시간 범위) 패널 오른쪽에 있는 * Custom Range *(사용자 지정 범위 *) 버튼이 강조 표시되어 사용자 지정 날짜 범위를 선택했음을 나타냅니다.
4. 사용자 지정 시간 범위를 선택하려면 * From * 달력 아래의 * Time * 컨트롤을 클릭하고 시작 시간을 선택합니다. 종료 시간을 지정하려면 오른쪽의 * to * 달력 아래에 있는 * Time * 컨트롤을 클릭하고 종료 시간을 선택합니다. Time Range(시간 범위) 패널 오른쪽에 있는 * Custom Range *(사용자 지정 범위 *) 버튼이 강조 표시되어 사용자 지정 시간 범위를 선택했음을 나타냅니다.
5. 선택적으로 미리 정의된 날짜 범위를 선택할 때 시작 및 종료 시간을 지정할 수 있습니다. 앞서 설명한 대로 미리 정의된 날짜 범위를 선택한 다음 앞서 설명한 시작 및 종료 시간을 선택합니다. 선택한 날짜가 달력에서 강조 표시되고 지정된 시작 및 종료 시간이 * 시간 * 컨트롤에 표시되고 * 사용자 지정 범위 * 버튼이 강조 표시됩니다.
6. 날짜 및 시간 범위를 선택한 후 * 범위 적용 * 을 클릭합니다. 해당 시간 범위의 성능 통계는 차트와 이벤트 타임라인에 표시됩니다.

카운터 차트 확대/축소 보기에서 성능 임계값 선택

Counter Charts Zoom View에서 임계값을 적용하면 성능 임계값 이벤트가 발생한 상황을 자세히 볼 수 있습니다. 이를 통해 임계값을 적용하거나 제거하고 결과를 즉시 볼 수 있으므로 문제 해결이 다음 단계가 되어야 하는지 여부를 결정할 때 도움이 될 수 있습니다.

카운터 차트 확대/축소 보기에서 임계값을 선택하면 성능 임계값 이벤트에 대한 정확한 데이터를 볼 수 있습니다. Counter Charts Zoom View의 * Policies * (정책 *) 영역에 나타나는 모든 임계값을 적용할 수 있습니다.

카운터 차트 확대/축소 보기에서 개체에 한 번에 하나의 정책만 적용할 수 있습니다.

단계

1. 를 선택하거나 선택을 취소합니다 정책과 연결되어 있습니다.

   선택한 임계값이 Counter Charts Zoom View(카운터 차트 확대/축소 보기)에 적용됩니다. 위험 임계값은 빨간색 선으로 표시되고 경고 임계값은 노란색 선으로 표시됩니다.

클러스터 구성 요소별 볼륨 지연 시간 보기

볼륨 성능 탐색기 페이지를 사용하여 볼륨에 대한 자세한 지연 시간 정보를 볼 수 있습니다. 지연 시간 - 총 카운터 차트는 볼륨의 총 지연 시간을 보여 주며 지연 시간 - 장애 카운터 차트는 볼륨에 대한 읽기 및 쓰기 지연 시간의 영향을 확인하는 데 유용합니다.

또한 지연 시간 - 클러스터 구성 요소 차트에는 각 클러스터 구성 요소의 지연 시간을 상세하게 비교하여 각 구성 요소가 볼륨의 총 지연 시간에 어떻게 기여하는지 확인할 수 있습니다. 다음 클러스터 구성 요소가 표시됩니다.

- 네트워크
- QoS 제한 최대
- 최소 QoS 제한
- 네트워크 처리
- 클러스터 인터커넥트
- 데이터 처리
- 집계 작업
- 볼륨 활성화
- MetroCluster 리소스
- 클라우드 지연 시간
- SnapMirror를 동기화합니다

단계

1. 선택한 볼륨의 * Volume Performance Explorer * 페이지의 지연 시간 차트의 드롭다운 메뉴에서 * 클러스터 구성 요소 * 를 선택합니다.

   지연 시간 - 클러스터 구성 요소 차트가 표시됩니다.

2. 더 큰 버전의 차트를 보려면 * 확대/축소 보기 * 를 선택합니다.

   클러스터 구성 요소 비교 차트가 표시됩니다. 을 선택 취소하거나 선택하여 비교를 제한할 수 있습니다 각 클러스터 구성요소와 연결되어 있습니다.

3. 특정 값을 보려면 커서를 차트 영역으로 이동하여 팝업 창을 확인합니다.

프로토콜별 **SVM IOPS** 트래픽 보기

성능/SVM 탐색기 페이지를 사용하여 SVM에 대한 자세한 IOPS 정보를 볼 수 있습니다. IOPS - 총 카운터 차트는 SVM의 총 IOPS 사용량을 보여 주며 IOPS - 분석 카운터 차트는 SVM에 대한 읽기, 쓰기 및 기타 IOPS의 영향을 확인하는 데 유용합니다.

또한 IOPS-프로토콜 차트에서는 SVM에서 사용 중인 각 프로토콜의 IOPS 트래픽을 자세하게 비교하여 보여줍니다. 다음 프로토콜을 사용할 수 있습니다.

- CIFS를 선택합니다
- NFS 를 참조하십시오

- FCP
- iSCSI
- NVMe를 참조하십시오

단계

1. 선택한 SVM에 대한 * 성능/SVM 탐색기 * 페이지의 IOPS 차트에서 드롭다운 메뉴에서 * 프로토콜 * 을 선택합니다.

   IOPS - 프로토콜 차트가 표시됩니다.

2. 더 큰 버전의 차트를 보려면 * 확대/축소 보기 * 를 선택합니다.

   IOPS 고급 프로토콜 비교 차트가 표시됩니다. 을 선택 취소하거나 선택하여 비교를 제한할 수 있습니다 이는 프로토콜과 관련이 있습니다.

3. 특정 값을 보려면 커서를 차트 중 하나의 차트 영역으로 이동하여 팝업 창을 표시합니다.

볼륨 및 **LUN** 지연 시간 차트를 확인하여 성능 보장 검증

"성능 보장" 프로그램에 가입한 볼륨 및 LUN을 확인하여 지연 시간이 보장된 수준을 초과하지 않았는지 확인할 수 있습니다.

지연 시간 성능 보장은 작동 당 밀리초를 초과해서는 안 됩니다. 기본 5분 성능 수집 기간이 아닌 시간당 평균을 기반으로 합니다.

단계

1. 성능: 모든 볼륨 * 보기 또는 * 성능: 모든 LUN * 보기에서 관심 있는 볼륨 또는 LUN을 선택합니다.
2. 선택한 볼륨 또는 LUN에 대한 * Performance Explorer * 페이지의 * 선택기에서 * 시간별 평균 * 을 선택합니다.

   5분 컬렉션이 시간 평균으로 대체되면 지연 시간 차트의 가로 줄에 부드러운 선이 표시됩니다.

3. 성능 보장 하에 같은 aggregate에 다른 볼륨이 있는 경우, 해당 볼륨을 추가하여 지연 시간 값을 동일한 차트로 볼 수 있습니다.

모든 **SAN** 어레이 클러스터의 성능 보기

성능: 모든 클러스터 보기를 사용하여 모든 SAN 어레이 클러스터의 성능 상태를 표시할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

성능: 모든 클러스터 보기 및 자세한 내용은 클러스터/성능 탐색기 페이지에서 모든 SAN 어레이 클러스터에 대한 개요 정보를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.
2. 상태: 모든 클러스터 * 보기에 ""개인 정보" 열이 표시되어 있는지 확인하거나 * 표시/숨기기 * 컨트롤을 사용하여

추가하십시오.

이 열에는 모든 SAN 어레이 클러스터에 대한 ""모든 SAN 어레이""가 표시됩니다.

3. 해당 클러스터의 성능에 대한 정보를 보려면 * Performance: All Clusters * 보기를 선택합니다.

   All SAN 어레이 클러스터의 성능 정보를 봅니다.

4. 이러한 클러스터의 성능에 대한 자세한 정보를 보려면 All SAN Array 클러스터의 이름을 클릭합니다.
5. Explorer * 탭을 클릭합니다.
6. 클러스터/성능 탐색기 * 페이지의 * 보기 및 비교 * 메뉴에서 이 클러스터의 * 노드 * 를 선택합니다.

   이 클러스터에서 두 노드의 성능 통계를 비교하여 두 노드의 로드가 거의 동일한지 확인할 수 있습니다. 두 노드 간에 큰 차이가 있을 경우 차트에 두 번째 노드를 추가하고 더 긴 기간 동안 값을 비교하여 구성 문제를 식별할 수 있습니다.

로컬 노드에만 있는 워크로드를 기준으로 노드 **IOPS** 보기

노드 IOPS 카운터 차트는 네트워크 LIF를 사용하여 로컬 노드를 통해서만 원격 노드의 볼륨에 읽기/쓰기 작업을 수행할 수 있는 작업을 강조 표시할 수 있습니다. IOPS - ""Total (Local)" 및 ""Breakdown (Local)" 차트는 현재 노드에서만 로컬 볼륨에 있는 데이터의 IOPS를 표시합니다.

이러한 카운터 차트의 ""로컬"" 버전은 로컬 볼륨에 상주하는 데이터의 통계만 표시하므로 성능 용량 및 활용도에 대한 노드 차트와 비슷합니다.

이러한 카운터 차트의 ""로컬" 버전을 이러한 카운터 차트의 일반 전체 버전과 비교하여 원격 노드의 볼륨에 액세스하기 위해 로컬 노드를 통해 많은 트래픽이 이동하는지 확인할 수 있습니다. 이 상황은 원격 노드의 볼륨에 도달하기 위해 로컬 노드를 통과하는 작업이 너무 많은 경우 노드의 높은 활용도로 인해 성능 문제가 발생할 수 있습니다. 이 경우 볼륨을 로컬 노드로 이동하거나 해당 볼륨에 액세스하는 호스트의 트래픽을 연결할 수 있는 원격 노드에 LIF를 생성할 수 있습니다.

단계

1. 선택한 노드의 * 성능/노드 탐색기 * 페이지의 IOPS 차트의 드롭다운 메뉴에서 * 합계 * 를 선택합니다.

   IOPS - 합계 차트가 표시됩니다.

2. 확대/축소 보기 * 를 클릭하여 새 브라우저 탭에 더 큰 버전의 차트를 표시합니다.
3. 성능/노드 탐색기 * 페이지로 돌아가 IOPS 차트의 드롭다운 메뉴에서 * Total (Local) * 을 선택합니다.

   IOPS - 합계(로컬) 차트가 표시됩니다.

4. 확대/축소 보기 * 를 클릭하여 새 브라우저 탭에 더 큰 버전의 차트를 표시합니다.
5. 두 차트를 서로 나란히 보고 IOPS 값이 상당히 다르게 나타나는 영역을 확인합니다.
6. 이 영역 위로 커서를 이동하여 특정 시점의 로컬 IOPS와 총 IOPS를 비교합니다.

개체 랜딩 페이지의 구성 요소입니다

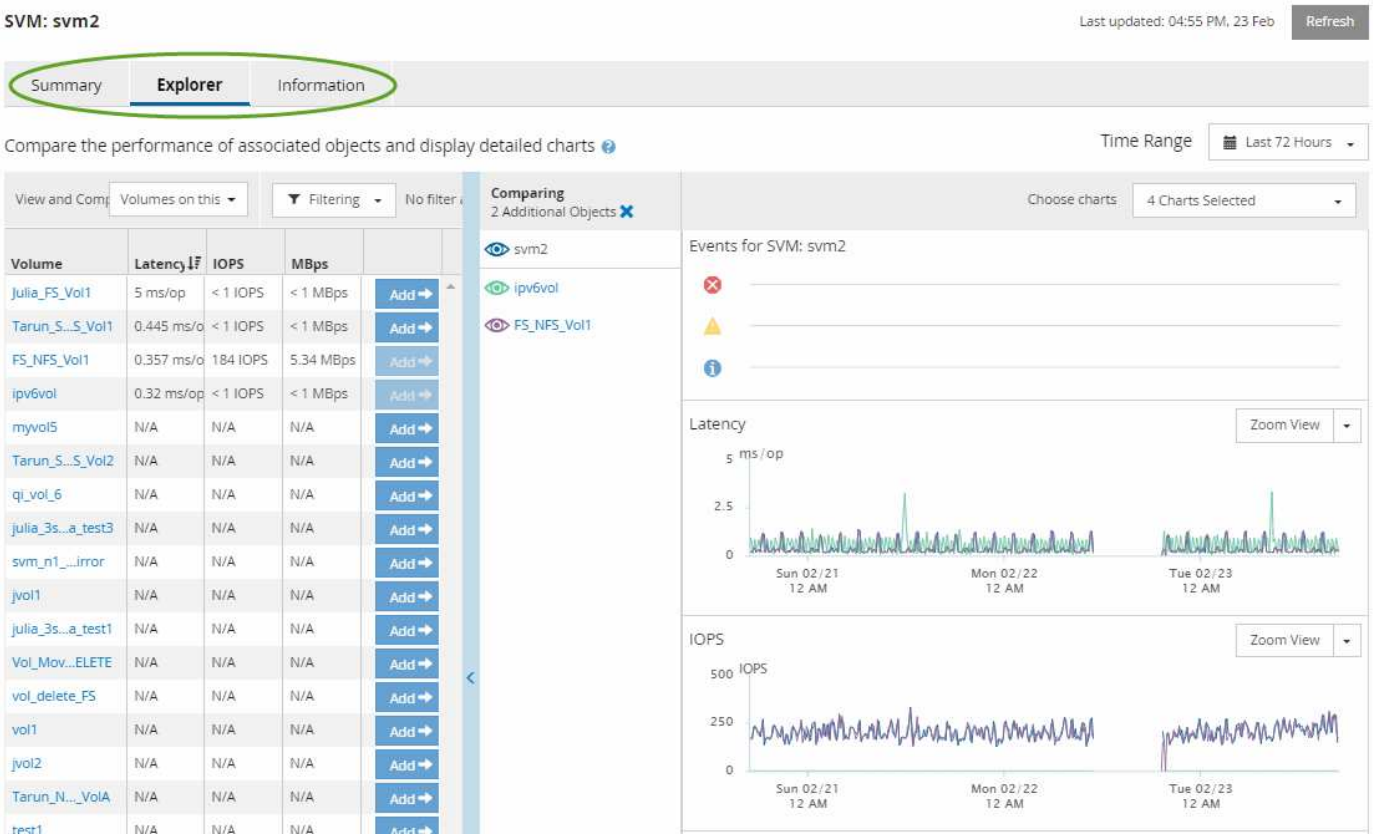
개체 랜딩 페이지에서는 모든 위험, 경고 및 정보 이벤트에 대한 세부 정보를 제공합니다. 이

기능을 사용하면 모든 클러스터 개체의 성능을 자세하게 확인할 수 있으므로 여러 기간에 걸쳐 개별 개체를 선택하고 비교할 수 있습니다.

개체 랜딩 페이지를 사용하면 모든 개체의 전반적인 성능을 검사하고 개체 성능 데이터를 나란히 비교할 수 있습니다. 이 기능은 성능을 평가할 때와 이벤트 문제를 해결할 때 유용합니다.

카운터 요약 패널 및 카운터 차트에 표시되는 데이터는 5분 샘플링 간격을 기준으로 합니다. 페이지 왼쪽의 개체 인벤토리 그리드에 표시되는 데이터는 1시간 샘플링 간격을 기준으로 합니다.

다음 그림에서는 탐색기 정보를 표시하는 개체 랜딩 페이지의 예를 보여 줍니다.



표시되는 스토리지 개체에 따라 개체 랜딩 페이지에는 개체에 대한 성능 데이터를 제공하는 다음 탭이 있을 수 있습니다.

- 요약

  이전 72시간 동안의 개체당 이벤트와 성능을 포함하는 3개 또는 4개의 카운터 차트를 표시합니다. 여기에는 해당 기간 동안의 높은 값과 낮은 값을 보여 주는 추세 선이 포함됩니다.

- 탐색기

  현재 개체와 관련된 스토리지 개체의 그리드를 표시하여 현재 개체의 성능 값을 관련 개체의 성능 값과 비교할 수 있도록 합니다. 이 탭에는 최대 11개의 카운터 차트와 시간 범위 선택기가 포함되어 있어 다양한 비교를 수행할 수 있습니다.

- 정보

  설치된 ONTAP 소프트웨어 버전, HA 파트너 이름, 포트 및 LIF 수를 비롯하여 스토리지 개체에 대한 성능 저하 구성 특성의 값을 표시합니다.

- 우수 성과 기업

  클러스터의 경우: 선택한 성능 카운터를 기준으로 가장 높은 성능 또는 가장 낮은 성능을 가진 스토리지 객체를 표시합니다.

- 장애 조치 계획

  노드의 경우: 노드의 HA 파트너에 장애가 발생할 경우 노드에 대한 성능 영향의 추정치를 표시합니다.

- 세부 정보

  볼륨: 선택한 볼륨 워크로드에 대한 모든 I/O 작업 및 작업에 대한 자세한 성능 통계를 표시합니다. 이 탭은 FlexGroup 볼륨, FlexVol 볼륨 및 FlexGroups의 구성요소에 대해 사용할 수 있습니다.

요약 페이지

요약 페이지에는 이전 72시간 동안의 개체별 이벤트 및 성능에 대한 세부 정보가 포함된 카운터 차트가 표시됩니다. 이 데이터는 자동으로 새로 고쳐지지 않지만 마지막 페이지 로드 시점의 최신 데이터입니다. 요약 페이지의 차트는 "더 자세히 살펴봐야 합니까?"라는 질문에 답합니다

차트 및 카운터 통계

요약 차트는 지난 72시간 동안의 간략한 상위 수준 개요를 제공하고 추가 조사가 필요한 가능한 문제를 식별하는 데 도움이 됩니다.

요약 페이지 카운터 통계가 그래프로 표시됩니다.

그래프의 추세선 위에 커서를 놓으면 특정 시점의 카운터 값을 볼 수 있습니다. 또한 요약 차트에는 다음 카운터에 대한 이전 72시간 동안의 활성 위험 및 경고 이벤트의 총 개수가 표시됩니다.

- * 지연 시간 *

  모든 I/O 요청에 대한 평균 응답 시간으로, 작업당 밀리초 단위로 표시됩니다.

  모든 개체 유형에 대해 표시됩니다.

- IOPS *

  평균 작동 속도, 초당 입력/출력 작업으로 표현됨.

  모든 개체 유형에 대해 표시됩니다.

- MB/s *

  초당 메가바이트 단위로 표시되는 평균 처리량입니다.

  모든 개체 유형에 대해 표시됩니다.

- * 사용된 성능 용량 *

  노드 또는 애그리게이트에 사용되고 있는 성능 용량의 비율입니다.

노드 및 애그리게이트에만 표시됩니다.

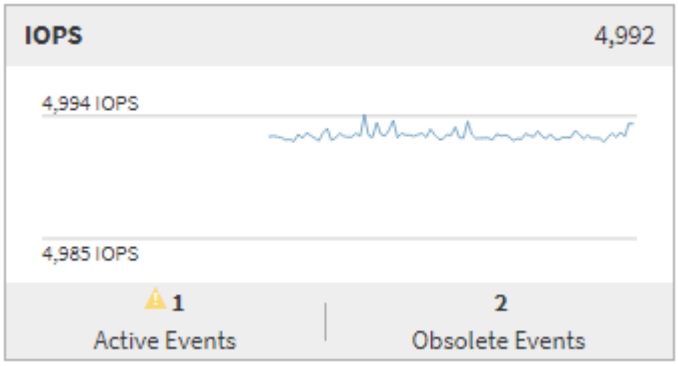
- * 활용률 *

  노드 및 애그리게이트의 개체 활용률 또는 포트의 대역폭 활용률

  노드, 애그리게이트 및 포트에 대해서만 표시됩니다.

활성 이벤트에 대한 이벤트 수 위에 커서를 놓으면 이벤트 유형과 수가 표시됩니다. 위험 이벤트는 빨간색(🟥), 경고 이벤트가 노란색(🟨)를 클릭합니다.

회색 막대의 차트 오른쪽 위에 있는 숫자는 지난 72시간 동안의 평균 값입니다. 추세 선 그래프의 맨 아래 및 맨 위에 표시되는 숫자는 지난 72시간 동안의 최소값 및 최대값입니다. 차트 아래의 회색 표시줄에는 지난 72시간 동안의 활성(새 이벤트 및 확인된) 이벤트 수와 사용되지 않는 이벤트의 수가 포함됩니다.



- * 지연 시간 카운터 차트 *

  지연 시간 카운터 차트는 이전 72시간 동안의 오브젝트 지연 시간에 대한 간략한 개요를 제공합니다. 지연 시간은 모든 I/O 요청에 대한 평균 응답 시간을 나타내며, 고려 중인 클러스터 스토리지 구성 요소의 데이터 패킷 또는 블록에서 경험되는 작업, 서비스 시간, 대기 시간 또는 둘 다에 대해 밀리초 단위로 표시됩니다.

- 상위(카운터 값): * 머리글의 숫자는 이전 72시간 기간의 평균을 표시합니다.
- 중간(성능 그래프): * 그래프 하단의 숫자는 가장 짧은 지연 시간을 표시하고 그래프 상단의 숫자는 이전 72시간 동안의 가장 높은 지연 시간을 표시합니다. 그래프 추이 선 위에 커서를 놓으면 특정 시간의 지연 시간 값을 볼 수 있습니다.
- bottom (events): * 마우스 커서를 가져가면 이벤트의 세부 정보가 팝업으로 표시됩니다. 전체 이벤트 세부 정보를 보려면 그래프 아래의 * 활성 이벤트 * 링크를 클릭하여 이벤트 인벤토리 페이지로 이동합니다.
- * IOPS 카운터 차트 *

  IOPS 카운터 차트는 이전 72시간 동안의 객체 IOPS 상태에 대한 상위 수준의 개요를 제공합니다. IOPS는 초당 입출력 작업 수로 스토리지 시스템의 속도를 나타냅니다.

- 상위(카운터 값): * 머리글의 숫자는 이전 72시간 기간의 평균을 표시합니다.
- 중간(성능 그래프): * 그래프 하단의 숫자는 가장 낮은 IOPS를 표시하며 그래프 상단의 숫자는 이전 72시간 동안의 가장 높은 IOPS를 표시합니다. 그래프 추세 선 위에 커서를 놓으면 특정 시간의 IOPS 값이 표시됩니다.
- bottom (events): * 마우스 커서를 가져가면 이벤트의 세부 정보가 팝업으로 표시됩니다. 전체 이벤트 세부 정보를 보려면 그래프 아래의 * 활성 이벤트 * 링크를 클릭하여 이벤트 인벤토리 페이지로 이동합니다.
- MB/s 카운터 차트 *

MB/s 카운터 차트는 객체 MB/s 성능을 표시하고 오브젝트에서 초당 메가바이트 단위로 얼마나 많은 데이터가 전송되었는지 나타냅니다. MB/s 카운터 차트는 이전 72시간 동안의 객체 MB/s 상태에 대한 개괄적인 개요를 제공합니다.

- 맨 위(카운터 값): * 머리글의 숫자는 이전 72시간 동안의 평균 MB/s 수를 표시합니다.

  중간(성능 그래프): * 그래프 하단의 값은 가장 낮은 MB/s 수를 표시하며 그래프 상단의 값은 이전 72시간 동안의 가장 높은 MB/s 수를 표시합니다. 그래프 추세선 위에 커서를 놓으면 특정 시간에 대한 MB/s 값을 볼 수 있습니다.

- bottom (events): * 마우스 커서를 가져가면 이벤트의 세부 정보가 팝업으로 표시됩니다. 전체 이벤트 세부 정보를 보려면 그래프 아래의 * 활성 이벤트 * 링크를 클릭하여 이벤트 인벤토리 페이지로 이동합니다.
- * 사용된 성능 용량 카운터 차트 *

  사용된 성능 용량 카운터 차트에는 개체에서 사용 중인 성능 용량의 백분율이 표시됩니다.

- 상위(카운터 값): * 헤더의 숫자는 지난 72시간 동안의 평균 사용된 성능 용량을 표시합니다.
- 중간(성능 그래프): * 그래프 하단의 값은 사용된 성능 용량 비율이 가장 낮은 값을 표시하고 그래프 상단의 값은 이전 72시간 동안의 사용된 성능 용량 중 가장 높은 비율을 표시합니다. 그래프 추이 선 위에 커서를 놓으면 특정 시간에 사용된 성능 용량 값을 볼 수 있습니다.
- bottom (events): * 마우스 커서를 가져가면 이벤트의 세부 정보가 팝업으로 표시됩니다. 전체 이벤트 세부 정보를 보려면 그래프 아래의 * 활성 이벤트 * 링크를 클릭하여 이벤트 인벤토리 페이지로 이동합니다.
- * 활용률 카운터 차트 *

  사용률 카운터 차트에는 개체 사용률 백분율이 표시됩니다. Utilization counter 차트는 지난 72시간 동안의 객체 또는 대역폭 활용도의 백분율에 대한 상위 수준의 개요를 제공합니다.

- 상위(카운터 값): * 헤더의 숫자는 지난 72시간 동안의 평균 사용률을 표시합니다.
- 중간(성능 그래프): * 그래프 하단의 값은 가장 낮은 사용률을 표시하며 그래프 상단의 값은 이전 72시간 동안의 가장 높은 사용률을 표시합니다. 그래프 추세 선 위에 커서를 놓으면 특정 시간의 사용률 값이 표시됩니다.
- bottom (events): * 마우스 커서를 가져가면 이벤트의 세부 정보가 팝업으로 표시됩니다. 전체 이벤트 세부 정보를 보려면 그래프 아래의 * 활성 이벤트 * 링크를 클릭하여 이벤트 인벤토리 페이지로 이동합니다.

이벤트

해당되는 경우 이벤트 기록 테이블에는 해당 개체에서 가장 최근에 발생한 이벤트가 나열됩니다. 이벤트 이름을 클릭하면 이벤트 세부 정보 페이지에 이벤트의 세부 정보가 표시됩니다.

성능 탐색기 페이지의 구성 요소입니다

Performance Explorer 페이지에서는 클러스터에서 유사한 개체의 성능을 비교할 수 있습니다(예: 클러스터의 모든 볼륨). 이 기능은 성능 이벤트 문제를 해결하고 개체 성능을 미세 조정할 때 유용합니다. 개체를 다른 개체 비교에 대한 기준선인 루트 개체와 비교할 수도 있습니다.

상태 보기로 전환 * 단추를 클릭하여 이 개체의 상태 세부 정보 페이지를 표시할 수 있습니다. 경우에 따라 문제를 해결할 때 도움이 될 수 있는 이 개체의 스토리지 구성 설정에 대한 중요한 정보를 알 수 있습니다.

성능 탐색기 페이지에는 클러스터 개체 목록과 해당 성능 데이터가 표시됩니다. 이 페이지에는 동일한 유형의 모든 클러스터 객체(예: 볼륨 및 해당 객체별 성능 통계)가 표 형식으로 표시됩니다. 이 보기에서는 클러스터 개체 성능에 대한 효율적인 개요를 제공합니다.

테이블의 셀에 ""N/A""가 표시되면 해당 개체에 대한 입출력이 없기 때문에 해당 카운터의 값을 사용할 수 없음을 의미합니다.

성능 탐색기 페이지에는 다음과 같은 구성 요소가 포함되어 있습니다.

- * 시간 범위 *

  개체 데이터의 시간 범위를 선택할 수 있습니다.

  미리 정의된 범위를 선택하거나 사용자 지정 시간 범위를 지정할 수 있습니다.

- * 보기 및 비교 *

  그리드에 표시되는 상관 오브젝트 유형을 선택할 수 있습니다.

  사용 가능한 옵션은 루트 개체 유형과 사용 가능한 데이터에 따라 다릅니다. 보기 및 비교 드롭다운 목록을 클릭하여 개체 유형을 선택할 수 있습니다. 선택한 개체 유형이 목록에 표시됩니다.

- * 필터링 *

  기본 설정에 따라 수신 데이터의 양을 줄일 수 있습니다.

  개체 데이터에 적용되는 필터(예: IOPS가 4보다 큼)를 만들 수 있습니다. 최대 4개의 필터를 동시에 추가할 수 있습니다.

- * 비교 *

  루트 오브젝트와 비교하기 위해 선택한 오브젝트의 목록을 표시합니다.

  비교 창의 개체에 대한 데이터가 카운터 차트에 표시됩니다.

- * 통계 보기: *

  볼륨 및 LUN의 경우 각 수집 주기(기본값 5분) 이후에 통계를 표시할지 또는 통계가 시간 평균으로 표시되는지 여부를 선택할 수 있습니다. 이 기능을 사용하면 NetApp "성능 보장" 프로그램을 지원하는 지연 시간 차트를 확인할 수 있습니다.

- * 카운터 차트 *

  각 오브젝트 성능 범주에 대해 그래프로 작성된 데이터를 표시합니다.

  일반적으로 기본적으로 3개 또는 4개의 차트만 표시됩니다. 차트 선택 구성 요소를 사용하면 추가 차트를 표시하거나 특정 차트를 숨길 수 있습니다. 이벤트 타임라인을 표시하거나 숨기도록 선택할 수도 있습니다.

- * 이벤트 타임라인 *

  시간 범위 구성 요소에서 선택한 시간 표시 막대에 걸쳐 발생하는 성능 및 상태 이벤트를 표시합니다.

QoS 정책 그룹 정보를 사용하여 성능 관리

Unified Manager를 사용하면 모니터링 중인 모든 클러스터에서 사용할 수 있는 서비스

품질(QoS) 정책 그룹을 확인할 수 있습니다. ONTAP 소프트웨어(System Manager 또는 ONTAP CLI) 또는 Unified Manager 성능 서비스 수준 정책을 사용하여 정책을 정의했을 수 있습니다. 또한 Unified Manager에는 QoS 정책 그룹이 할당된 볼륨 및 LUN이 표시됩니다.

QoS 설정 조정에 대한 자세한 내용은 을 참조하십시오 "성능 관리 개요"

스토리지 **QoS**로 워크로드 처리량을 제어하는 방법

QoS(서비스 품질) 정책 그룹을 생성하여 포함된 워크로드의 IOPS(초당 I/O) 또는 처리량(MB/s) 제한을 제어할 수 있습니다. 워크로드가 기본 정책 그룹과 같이 설정된 제한이 없는 정책 그룹에 있거나 설정된 제한이 사용자의 요구 사항을 충족하지 않는 경우, 제한을 늘리거나 워크로드를 원하는 제한이 있는 새 정책 그룹 또는 기존 정책 그룹으로 이동할 수 있습니다.

"기존" QoS 정책 그룹은 단일 볼륨 또는 LUN과 같은 개별 워크로드에 할당할 수 있습니다. 이 경우 워크로드는 최대 처리량 제한을 사용할 수 있습니다. QoS 정책 그룹도 여러 워크로드에 할당할 수 있으며, 이 경우 처리량 제한이 워크로드 간에 "공유"됩니다. 예를 들어, 3개의 워크로드에 할당된 9,000 IOPS의 QoS 제한은 결합된 IOPS가 9,000 IOPS를 초과하지 않도록 제한됩니다.

또한 개별 워크로드 또는 여러 워크로드에 "Adaptive" QoS 정책 그룹을 할당할 수 있습니다. 그러나 여러 워크로드에 할당된 경우에도 각 워크로드는 처리량 값을 다른 워크로드와 공유하는 대신 최대 처리량 제한을 받습니다. 또한 적응형 QoS 정책은 볼륨 크기 및 워크로드별로 처리량 설정을 자동으로 조정하여 볼륨 크기에 따라 IOPS와 테라바이트의 비율을 유지합니다. 예를 들어, 적응형 QoS 정책에서 최대값이 5,000 IOPS/TB로 설정된 경우 10TB 볼륨의 처리량은 최대 50,000 IOPS입니다. 나중에 볼륨 크기를 20TB로 조정하는 경우 적응형 QoS는 최대 100,000 IOPS로 조정합니다.

ONTAP 9.5부터 적응형 QoS 정책을 정의할 때 블록 크기를 포함할 수 있습니다. 따라서 워크로드가 매우 큰 블록 크기를 사용하고 궁극적으로 높은 처리량을 사용하는 경우, IOPS/TB 임계값에서 MB/s 임계값으로 정책이 효과적으로 변환됩니다.

공유 그룹 QoS 정책의 경우 정책 그룹에 있는 모든 워크로드의 IOPS 또는 MB/s가 설정된 한도를 초과할 경우 정책 그룹은 워크로드를 조절하여 작업을 제한함으로써 정책 그룹의 모든 워크로드의 성능을 저하시할 수 있습니다. 정책 그룹 임계치 조절에 의해 동적 성능 이벤트가 생성되는 경우 이벤트 설명에 관련된 정책 그룹의 이름이 표시됩니다.

Performance: All Volumes 뷰에서 영향을 받는 볼륨을 IOPS 및 MB/s로 정렬하여 이벤트가 발생한 가장 높은 사용률이 있는 워크로드를 확인할 수 있습니다. 성능/볼륨 탐색기 페이지에서 볼륨의 다른 볼륨 또는 LUN을 선택하여 영향을 받는 워크로드 IOPS 또는 MBPS 처리량 사용량과 비교할 수 있습니다.

노드 리소스를 과도하게 사용하는 워크로드를 보다 제한적인 정책 그룹 설정에 할당하면 정책 그룹은 워크로드를 조절하여 해당 노드의 리소스 사용을 줄일 수 있습니다. 그러나 작업 부하에서 더 많은 노드 리소스를 사용할 수 있도록 하려면 정책 그룹의 값을 늘릴 수 있습니다.

System Manager, ONTAP 명령 또는 Unified Manager 성능 서비스 수준을 사용하여 다음 작업을 비롯한 정책 그룹을 관리할 수 있습니다.

- 정책 그룹을 생성하는 중입니다
- 정책 그룹에서 워크로드 추가 또는 제거
- 정책 그룹 간에 워크로드 이동
- 정책 그룹의 처리량 제한을 변경합니다
- 워크로드를 다른 애그리게이트 및/또는 노드로 이동

모든 클러스터에서 사용 가능한 모든 **QoS** 정책 그룹 보기

Unified Manager에서 모니터링하는 클러스터에서 사용 가능한 모든 QoS 정책 그룹의 목록을 표시할 수 있습니다. 여기에는 기존 QoS 정책, 적응형 QoS 정책, Unified Manager Performance Service Level 정책에서 관리하는 QoS 정책이 포함됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * QoS 정책 그룹 * 을 클릭합니다.

   성능: 기존 QoS 정책 그룹 보기가 기본적으로 표시됩니다.

2. 사용 가능한 각 기존 QoS 정책 그룹에 대한 자세한 구성 설정을 봅니다.
3. 확장 단추( ) QoS 정책 그룹 이름 옆에 있는 을 클릭하여 정책 그룹에 대한 자세한 정보를 봅니다.
4. 보기 메뉴에서 추가 옵션 중 하나를 선택하여 모든 적응형 QoS 정책 그룹을 보거나 Unified Manager Performance Service 레벨을 사용하여 생성한 모든 QoS 정책 그룹을 확인합니다.

동일한 **QoS** 정책 그룹에 있는 볼륨 또는 **LUN** 보기

동일한 QoS 정책 그룹에 할당된 볼륨 및 LUN의 목록을 표시할 수 있습니다.

여러 볼륨 간에 "공유"되는 기존 QoS 정책 그룹의 경우 특정 볼륨이 정책 그룹에 대해 정의된 처리량을 과도하게 사용하고 있는지 확인하는 데 도움이 될 수 있습니다. 다른 볼륨에 부정적인 영향을 주지 않고 정책 그룹에 다른 볼륨을 추가할 수 있는지 결정하는 데도 도움이 됩니다.

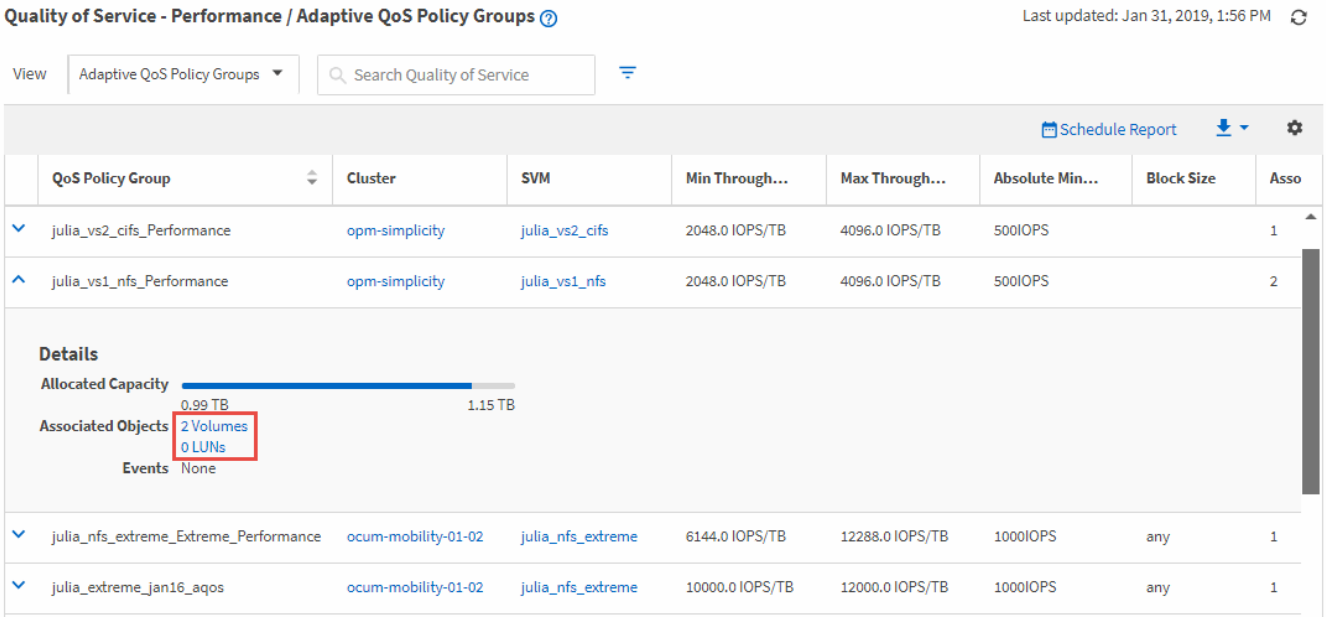
적응형 QoS 정책과 Unified Manager Performance Service 레벨 정책의 경우, 정책 그룹을 사용 중인 모든 볼륨 또는 LUN을 볼 때 QoS 정책의 구성 설정을 변경한 경우 영향을 받을 개체를 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * QoS 정책 그룹 * 을 클릭합니다.

   성능: 기존 QoS 정책 그룹 보기가 기본적으로 표시됩니다.

2. 기존 정책 그룹에 관심이 있는 경우 이 페이지를 계속 참조하십시오. 그렇지 않으면 추가 보기 옵션 중 하나를 선택하여 모든 적응형 QoS 정책 그룹 또는 Unified Manager Performance Service 레벨에 의해 생성된 모든 QoS 정책 그룹을 표시합니다.
3. 관심 있는 QoS 정책에서 확장 단추(를 클릭합니다) QoS 정책 그룹 이름 옆에 있는 을 클릭하여 자세한 내용을 봅니다.



4. 이 QoS 정책을 사용하여 객체를 보려면 Volumes 또는 LUN 링크를 클릭합니다.

   볼륨 또는 LUN의 성능 인벤토리 페이지는 QoS 정책을 사용하는 개체의 정렬된 목록과 함께 표시됩니다.

특정 볼륨 또는 **LUN**에 적용된 **QoS** 정책 그룹 설정 보기

볼륨 및 LUN에 적용된 QoS 정책 그룹을 볼 수 있으며, 성능/QoS 정책 그룹 보기에 연결하여 각 QoS 정책에 대한 자세한 구성 설정을 표시할 수 있습니다.

볼륨에 적용된 QoS 정책을 확인하는 단계는 다음과 같습니다. LUN에 대해 이 정보를 확인하는 단계도 비슷합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.

   Health: All Volumes(상태: 모든 볼륨) 보기가 기본적으로 표시됩니다.

2. 보기 메뉴에서 * 성능:QoS 정책 그룹의 볼륨 * 을 선택합니다.
3. 검토할 볼륨을 찾아 * QoS 정책 그룹 * 열이 표시될 때까지 오른쪽으로 스크롤합니다.
4. QoS 정책 그룹 이름을 클릭합니다.

   해당 서비스 품질 페이지는 기존 QoS 정책, 적응형 QoS 정책 또는 Unified Manager Performance Service 레벨을 사용하여 생성된 QoS 정책에 따라 표시됩니다.

5. QoS 정책 그룹에 대한 자세한 구성 설정을 봅니다.
6. 확장 단추( ) QoS 정책 그룹 이름 옆에 있는 을 클릭하여 정책 그룹에 대한 자세한 정보를 봅니다.

성능 차트를 확인하여 동일한 **QoS** 정책 그룹에 있는 볼륨 또는 **LUN**을 비교합니다

동일한 QoS 정책 그룹에 속한 볼륨 및 LUN을 확인한 다음 단일 IOPS, MB/s 또는 IOPS/TB 차트의 성능을 비교하여 문제를 식별할 수 있습니다.

동일한 QoS 정책 그룹에서 볼륨의 성능을 비교하는 단계는 아래에 나와 있습니다. LUN에 대해 이 정보를 확인하는 단계도 비슷합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.

   Health: All Volumes(상태: 모든 볼륨) 보기가 기본적으로 표시됩니다.

2. 보기 메뉴에서 * 성능:QoS 정책 그룹의 볼륨 * 을 선택합니다.
3. 검토할 볼륨의 이름을 클릭합니다.

   볼륨에 대한 성능 탐색기 페이지가 표시됩니다.

4. 보기 및 비교 메뉴에서 * 동일한 QoS 정책 그룹의 볼륨 * 을 선택합니다.

   동일한 QoS 정책을 공유하는 다른 볼륨은 아래 표에 나와 있습니다.

5. 차트에서 선택한 모든 볼륨의 IOPS, MB/s, IOPS/TB 및 기타 성능 카운터를 비교할 수 있도록 해당 볼륨을 차트에 추가하려면 * 추가 * 버튼을 클릭합니다.

   시간 범위를 변경하여 기본 72시간이 아닌 다른 시간 간격에 대한 성능을 볼 수 있습니다.

처리량 차트에 표시되는 **QoS** 정책의 유형

성능 탐색기 및 워크로드 분석 IOPS, IOPS/TB 및 MB/s 차트에서 볼륨 또는 LUN에 적용된 ONTAP 정의 서비스 품질(QoS) 정책 설정을 볼 수 있습니다. 차트에 표시되는 정보는 워크로드에 적용된 QoS 정책 유형에 따라 달라집니다.

처리량 최대(""피크") 설정은 워크로드가 사용할 수 있는 최대 처리량을 정의하므로 시스템 리소스에 대한 경쟁 워크로드에 대한 영향을 제한합니다. 처리량 최소(또는 ""예상됨") 설정은 중요 워크로드가 경쟁 워크로드의 요구에 관계없이 최소 처리량 목표를 충족하도록 워크로드에 사용 가능한 최소 처리량을 정의합니다.

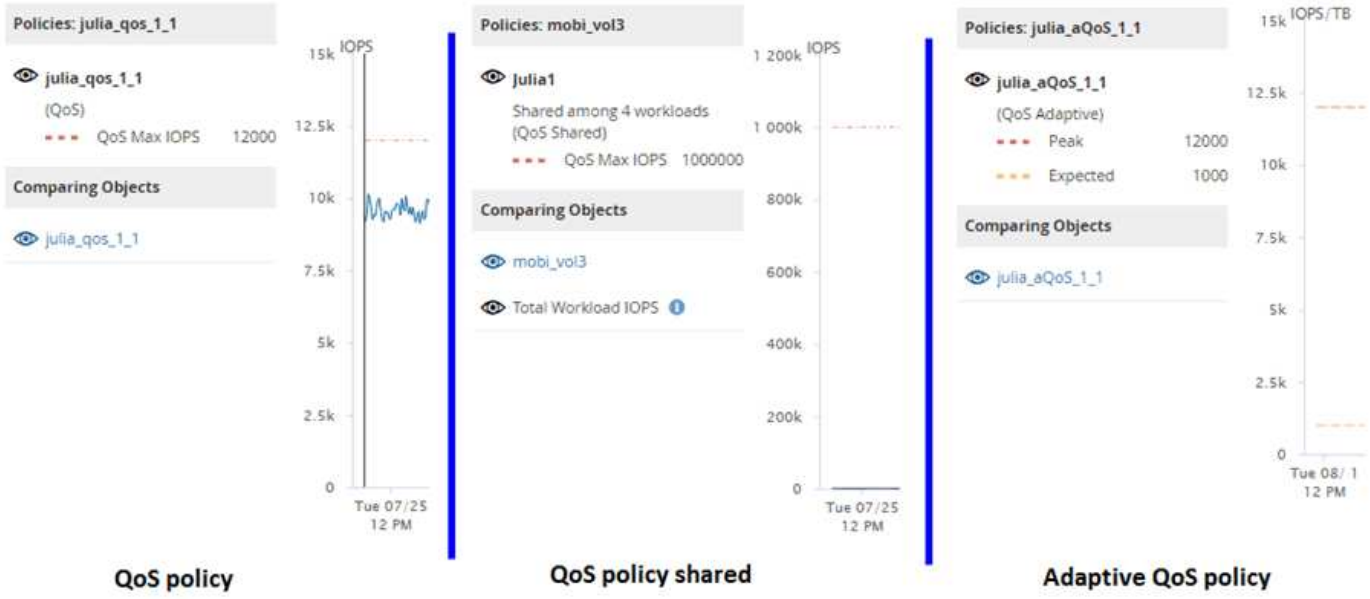
IOPS 및 MB/s에 대한 공유 및 비공유 QoS 정책은 "minimum" 및 "mixum"이라는 용어를 사용하여 바닥과 천장을 정의합니다. ONTAP 9.3에 도입된 IOPS/TB에 대한 적응형 QoS 정책은 "예상됨" 및 "피크"라는 용어를 사용하여 바닥과 천장을 정의합니다.

ONTAP를 사용하면 QoS 정책의 두 가지 유형을 만들 수 있지만, 워크로드에 QoS 정책이 적용되는 방식에 따라 성능 차트에 QoS 정책이 표시되는 방법에는 세 가지가 있습니다.

정책 유형입니다	기능	**Unified Manager** 인터페이스에 대한 표시기입니다
단일 워크로드에 할당된 QoS 공유 정책 또는 단일 워크로드 또는 여러 워크로드에 할당된 QoS 비공유 정책	각 워크로드는 지정된 처리량 설정을 사용할 수 있습니다	"'(QoS)' 표시
여러 워크로드에 할당된 QoS 공유 정책입니다	모든 워크로드는 지정된 처리량 설정을 공유합니다	"'(QoS Shared)' 표시

정책 유형입니다	기능	**Unified Manager** 인터페이스에 대한 표시기입니다
단일 워크로드 또는 여러 워크로드에 할당된 적응형 QoS 정책	각 워크로드는 지정된 처리량 설정을 사용할 수 있습니다	"'(QoS Adaptive)' 표시

다음 그림에서는 세 가지 옵션이 카운터 차트에 표시되는 방법의 예를 보여 줍니다.



IOPS에 정의된 일반 QoS 정책이 워크로드의 IOPS/TB 차트에 표시되면 ONTAP는 IOPS 값을 IOPS/TB 값으로 변환하고 Unified Manager는 IOPS/TB 차트에 해당 정책을 "QoS, IOPS로 정의됨" 텍스트와 함께 표시합니다.

IOPS/TB에 정의된 적응형 QoS 정책이 워크로드의 IOPS 차트에 표시되면 ONTAP는 IOPS/TB 값을 IOPS 값으로 변환하고 Unified Manager는 IOPS 차트에 해당 정책을 "QoS Adaptive-Used" 텍스트와 함께 표시합니다. 최대 IOPS 할당 설정의 구성 방식에 따라 IOPS/TB에 정의된 IOPS/TB 또는 "QoS Adaptive-Allocated, IOPS/TB"로 정의됩니다. 할당 설정이 "allocated-space"로 설정되면, 최대 IOPS는 볼륨의 크기를 기준으로 계산됩니다. 할당 설정이 ""사용된 공간""으로 설정되면 저장소 효율성을 고려하여 볼륨에 저장된 데이터의 양을 기준으로 피크 IOPS가 계산됩니다.

IOPS/TB 차트에는 볼륨에서 사용하는 논리적 용량이 128GB보다 크거나 같은 경우에만 성능 데이터가 표시됩니다. 선택한 기간 동안 사용된 용량이 128GB보다 낮아지면 차트에는 간격이 표시됩니다.

Performance Explorer에서 워크로드 **QoS** 최소 및 최대 설정 보기

성능 탐색기 차트에서 볼륨 또는 LUN에 대한 ONTAP 정의 서비스 품질(QoS) 정책 설정을 볼 수 있습니다. 최대 처리량 설정은 경쟁 워크로드가 시스템 리소스에 미치는 영향을 제한합니다. 처리량 최소 설정은 중요 워크로드가 서로 경합하는 워크로드에 대한 요구 사항에 관계없이 최소 처리량 목표를 충족하도록 보장합니다.

QoS 처리량 "최소" 및 "최대" IOPS 및 MB/s 설정은 ONTAP에서 구성한 경우에만 카운터 차트에 표시됩니다. 최소 처리량 설정은 ONTAP 9.2 이상 소프트웨어를 실행하는 시스템, AFF 시스템에서만 사용할 수 있으며 지금은 IOPS에만 설정할 수 있습니다.

적응형 QoS 정책은 ONTAP 9.3부터 사용할 수 있으며 IOPS 대신 IOPS/TB를 사용하여 표현됩니다. 이러한 정책은

볼륨 크기, 워크로드 당 QoS 정책 값을 자동으로 조정하므로 볼륨 크기에 따라 IOPS와 TB의 비율을 유지합니다. 적응형 QoS 정책 그룹은 볼륨에만 적용할 수 있습니다. QoS 용어인 "예상됨""과 "피크"는 QoS 정책 적용에 최소값과 최대값이 아닌 적응성 QoS 정책에 사용됩니다.

Unified Manager에서는 이전 시간의 각 성능 수집 기간 동안 워크로드 처리량이 정의된 QoS 최대 정책 설정을 초과할 경우 QoS 정책 위반에 대한 경고 이벤트를 생성합니다. 각 수집 기간 동안 짧은 기간 동안만 워크로드 처리 성능이 QoS 임계값을 초과할 수 있지만 Unified Manager는 차트에 수집 기간 동안 ""평균"" 처리량을 표시합니다. 따라서 워크로드의 처리량이 차트에 표시된 정책 임계값을 넘을 수 없는 동안 QoS 이벤트가 발생할 수 있습니다.

단계

1. 선택한 볼륨 또는 LUN에 대한 * Performance Explorer * 페이지에서 QoS 상한 및 하한 설정을 보려면 다음 작업을 수행하십시오.

원하는 작업	수행할 작업...
IOPS 한도 보기(QoS 최대)	IOPS 합계 또는 분석 차트에서 * 확대/축소 보기 * 를 클릭합니다.
MB/s 천장을 봅니다(QoS 최대).	MB/s 합계 또는 분석 차트에서 * 확대/축소 보기 * 를 클릭합니다.
IOPS 최저값 보기(QoS min)	IOPS 합계 또는 분석 차트에서 * 확대/축소 보기 * 를 클릭합니다.
IOPS/TB 한도 보기(QoS 피크)	볼륨의 경우 IOPS/TB 차트에서 * Zoom View * 를 클릭합니다.
IOPS/TB 설치 공간 보기(QoS 예상)	볼륨의 경우 IOPS/TB 차트에서 * Zoom View * 를 클릭합니다.

   점선으로 표시된 수평선은 ONTAP에 설정된 최대 또는 최소 처리량 값을 나타냅니다. QoS 값에 대한 변경 사항이 구현된 시점을 확인할 수도 있습니다.

2. QoS 설정과 비교하여 특정 IOPS 및 MB/s 값을 보려면 커서를 차트 영역으로 이동하여 팝업 창을 확인합니다.

특정 볼륨 또는 LUN의 IOPS 또는 MB/s가 매우 높고 시스템 리소스를 강조하는 경우, System Manager 또는 ONTAP CLI를 사용하여 QoS 설정을 조정하여 해당 워크로드가 다른 워크로드의 성능에 영향을 미치지 않도록 할 수 있습니다.

QoS 설정 조정에 대한 자세한 내용은 을 참조하십시오 "성능 관리 개요"

성능 용량 및 사용 가능한 IOPS 정보를 사용하여 성능 관리

_성능 용량_은 리소스의 유용한 성능을 초과하지 않고 자원을 얼마나 많이 활용할 수 있는지 나타냅니다. 기존 성능 카운터를 사용하여 보면 지연 시간이 문제가 되기 전에 성능 용량은 노드 또는 애그리게이트의 활용률을 극대화하는 데 사용됩니다.

Unified Manager는 각 클러스터의 노드 및 애그리게이트로부터 성능 용량 통계를 수집합니다. _ 사용된 성능 용량은 현재 사용 중인 성능 용량의 백분율이고, _ performance capacity free _ 는 아직 사용 가능한 성능 용량의 비율입니다.

여유 성능 용량은 사용 가능한 리소스의 비율을 제공하지만, _Available IOPS_는 최대 성능 용량에 도달하기 전에 리소스에 추가할 수 있는 IOPS 수를 나타냅니다. 이 메트릭을 사용하면 미리 정해진 IOPS 수의 워크로드를 리소스에 추가할 수 있습니다.

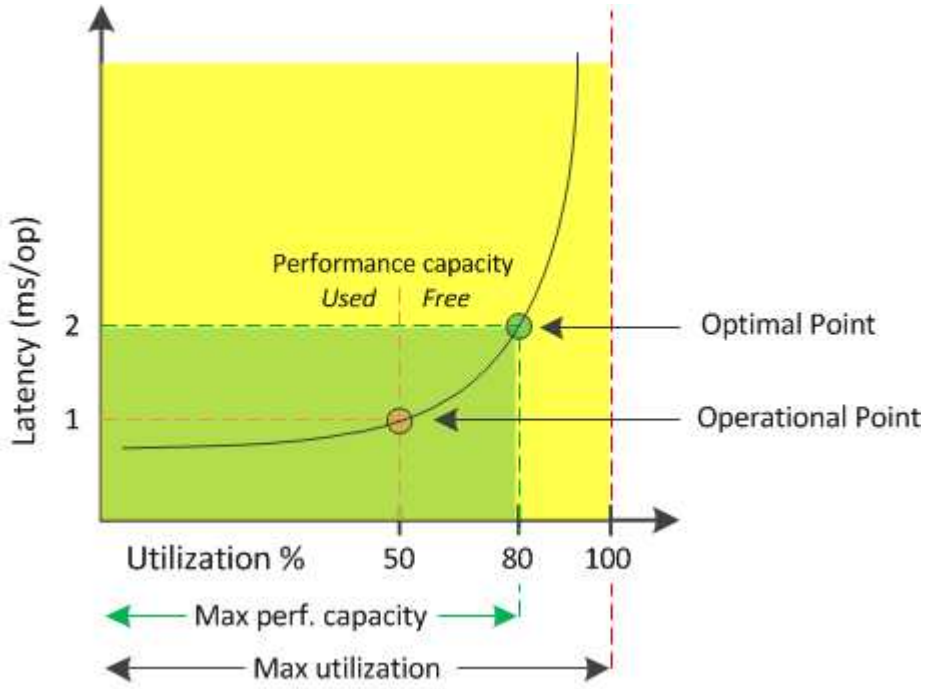
성능 용량 정보를 모니터링하면 다음과 같은 이점이 있습니다.

- 워크플로우 프로비저닝 및 밸런싱 지원
- 노드를 오버로딩하거나 리소스를 최적의 포인트 이상으로 과도하게 투입하는 것을 방지함으로써 문제 해결 필요성을 줄여줍니다.
- 추가 저장 장비가 필요할 수 있는 곳을 정확하게 파악할 수 있습니다.

사용된 성능 용량이 무엇입니까

사용된 성능 용량 카운터를 사용하면 노드 성능이 저하되거나 워크로드가 증가할 경우 성능이 저하될 수 있는 지점에 도달하는지 여부를 식별할 수 있습니다. 또한 특정 기간 동안 노드 또는 애그리게이트를 현재 초과 사용하고 있는지도 확인할 수 있습니다. 사용된 성능 용량은 활용도와 유사하지만, 이전 용량은 특정 워크로드에 대해 물리적 리소스에서 사용 가능한 성능 기능에 대한 보다 자세한 정보를 제공합니다.

사용된 최적의 성능 용량은 노드 또는 애그리게이트의 활용률이 최적의 지연 시간(응답 시간)이 있으며 효율적인 사용 중인 지점입니다. 다음 그림에서는 Aggregate에 대한 샘플 지연 시간 및 활용률 곡선이 표시되어 있습니다.



이 예제에서 _operational point_는 aggregate가 현재 50% 사용률로 작동하고 있으며 지연 시간은 1.0ms/op인 것을 식별합니다. Unified Manager는 aggregate에서 얻은 통계를 기반으로 이 애그리게이트에 사용할 수 있는 추가 성능 용량을 결정합니다. 이 예에서 _optimal point_는 aggregate가 80% 활용률이고 지연 시간이 2.0ms/op인 시점을 가리킵니다. 따라서 이 애그리게이트에 볼륨 및 LUN을 추가하여 시스템을 보다 효율적으로 사용할 수 있습니다.

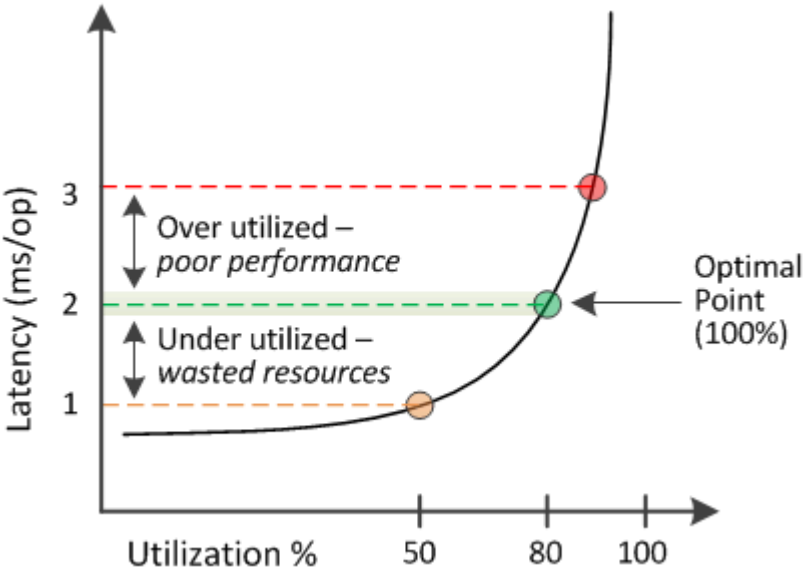
성능 용량이 지연 시간에 미치는 영향을 증가하므로 사용된 성능 카운터는 "활용률" 카운터보다 더 많은 수가 될 것으로 예상됩니다. 예를 들어, 노드 또는 애그리게이트의 사용량이 70%인 경우 지연 시간 값에 따라 성능 용량 값이 80%~100% 범위에 있을 수 있습니다.

그러나 대시보드 페이지에서 활용률 카운터가 더 높을 수 있는 경우도 있습니다. 대시보드는 각 컬렉션 기간에 현재 카운터 값을 새로 고치므로 이는 정상적인 현상이며 Unified Manager 사용자 인터페이스의 다른 페이지와 같이 일정 기간 동안 평균을 표시하지 않습니다. 사용된 성능 용량은 일정 기간 동안의 평균 성능 지표로서 가장 많이 사용되는 반면, 사용률 카운터는 리소스의 즉각적인 사용을 결정하는 데 가장 적합합니다.

사용된 성능 용량이 갖는 의미

사용된 성능 용량은 현재 과도하게 사용하거나 활용도가 낮은 노드와 애그리게이트를 식별하는 데 도움이 됩니다. 따라서 스토리지 리소스를 더욱 효율적으로 사용하기 위해 워크로드를 재배포할 수 있습니다.

다음 그림에서는 리소스의 지연 시간 및 활용률 곡선을 보여 주고, 현재 작업 지점이 위치할 수 있는 세 가지 영역을 컬러 점으로 식별합니다.



- 100과 같은 비율로 사용된 성능 용량이 최적의 위치에 있습니다.

  현재 리소스가 효율적으로 사용되고 있습니다.

- 사용된 성능 용량이 100을 넘으면 노드 또는 애그리게이트의 활용률이 초과되며 워크로드가 최적의 성능을 발휘함을 나타냅니다.

  리소스에 새 워크로드를 추가할 필요가 없으며 기존 워크로드를 재배포해야 할 수도 있습니다.

- 사용된 성능 용량이 100% 미만이면 노드 또는 애그리게이트의 활용률이 낮으므로 리소스가 효율적으로 사용되지 않음을 나타냅니다.

  리소스에 더 많은 워크로드를 추가할 수 있습니다.

사용률과 달리 사용된 성능 용량은 100%를 초과할 수 있습니다. 최대 비율은 없지만 리소스가 과도하게 사용되는 경우 리소스가 일반적으로 110%~140% 범위에 있게 됩니다. 백분율이 높을수록 심각한 문제가 있는 자원을 나타냅니다.

사용 가능한 **IOPS**는 무엇입니까

사용 가능한 IOPS 카운터는 리소스가 제한에 도달하기 전에 노드나 애그리게이트에 추가할 수 있는 IOPS의 남은 수를 식별합니다.

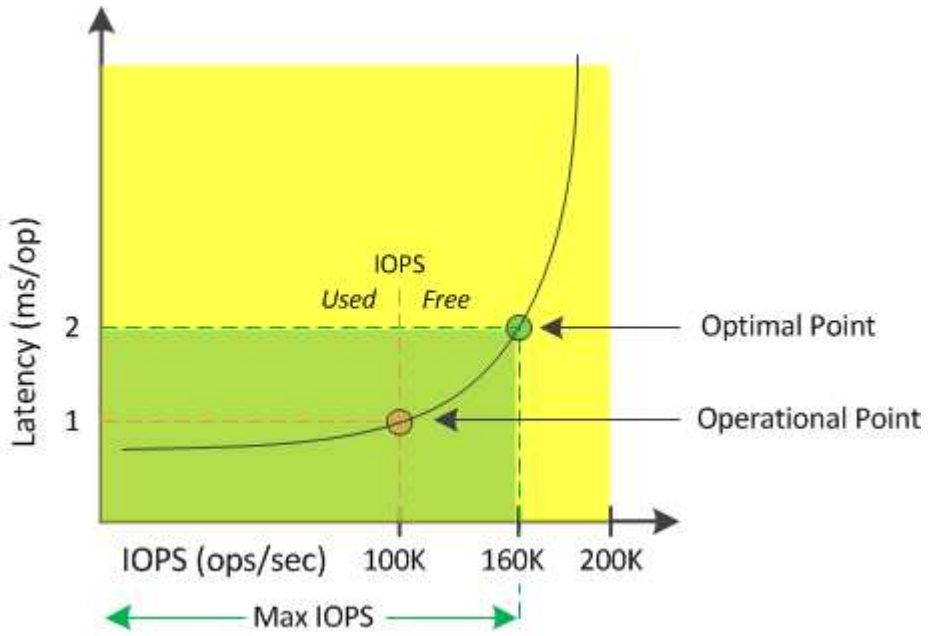
노드가 제공할 수 있는 총 IOPS는 노드의 물리적 특성(예: CPU 수, CPU 속도 및 RAM 용량)을 기반으로 합니다. Aggregate가 제공할 수 있는 총 IOPS는 디스크의 물리적 속성(예: SATA, SAS 또는 SSD 디스크)을 기반으로 합니다.

Aggregate에 있는 모든 볼륨의 총 IOPS가 애그리게이트의 총 IOPS와 일치하지 않을 수 있습니다. 이에 대해서는 다음 기술 자료 문서 KB에서 설명합니다 "Aggregate의 모든 볼륨 IOPS의 합이 Aggregate IOP와 일치하지 않는 이유는 무엇입니까?"

성능 가용 용량 카운터는 사용 가능한 리소스의 백분율을 제공하지만, 사용 가능한 IOPS 카운터는 최대 성능 용량에 도달하기 전에 리소스에 추가할 수 있는 IOPS(워크로드)의 정확한 수를 보여 줍니다.

예를 들어, FAS2520 및 FAS8060 스토리지 시스템 쌍을 사용하는 경우, 여유 성능 용량이 30%라는 것은 여유 성능 용량이 있음을 의미합니다. 하지만 이 가치는 해당 노드에 구축할 수 있는 더 많은 워크로드를 파악할 수 없습니다. 사용 가능한 IOPS 카운터는 FAS8060에서 500 IOPS를 사용할 수 있지만, FAS2520에서는 100 IOPS만 사용할 수 있다는 것을 보여 줄 수 있습니다.

다음 그림에서는 노드에 대한 IOPS 곡선 대비 지연 시간의 예를 보여 줍니다.



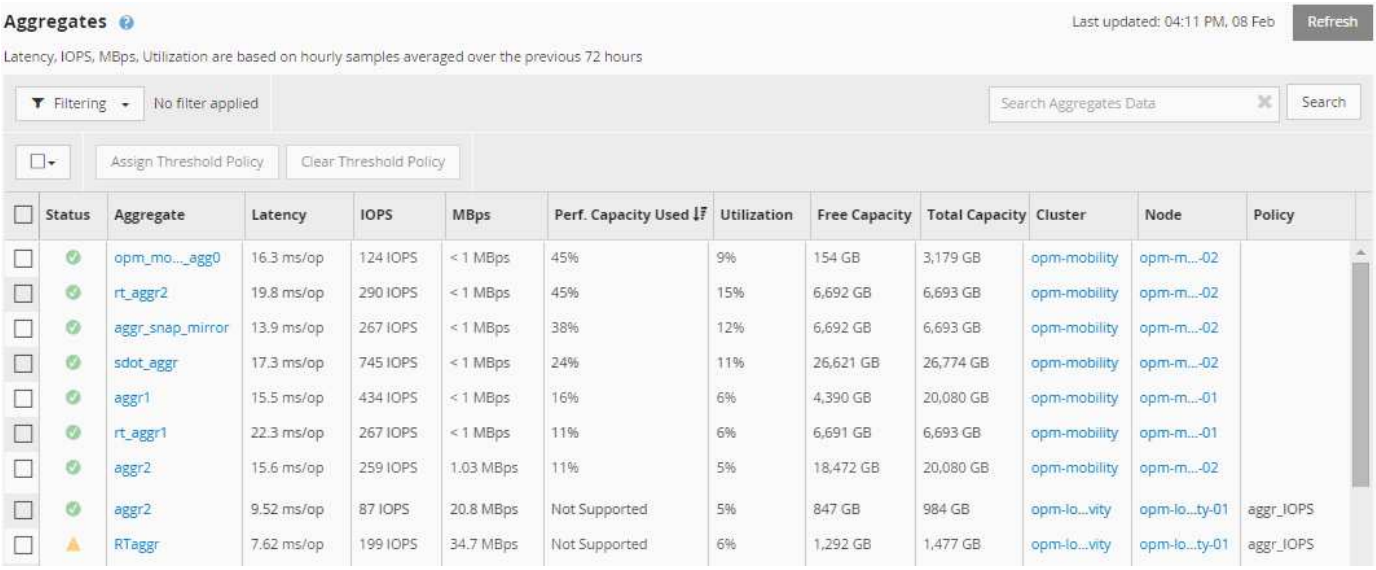
리소스가 제공할 수 있는 최대 IOPS 수는 사용된 성능 용량이 100%(최적의 포인트)일 때의 IOPS 수입니다. 운영 포인트는 노드가 현재 100K IOPS에서 작동하고 있으며 지연 시간은 1.0ms/op인 것을 식별합니다. Unified Manager는 노드에서 수집한 통계를 기반으로 노드의 최대 IOPS가 160K임을 확인합니다. 즉, 사용 가능한 IOPS는 60K입니다. 따라서 시스템을 더 효율적으로 사용할 수 있도록 이 노드에 워크로드를 더 추가할 수 있습니다.

리소스에 최소 사용자 활동이 있는 경우 CPU 코어당 약 4,500IOPS를 기준으로 일반 워크로드를 가정하여 사용 가능한 IOPS 값이 계산됩니다. 그 이유는 Unified Manager에 제공된 워크로드의 특성을 정확하게 추정하는 데이터가 없기 때문입니다.

사용된 노드 및 총 성능 용량 값 보기

모든 노드 또는 클러스터의 모든 애그리게이트에 대해 사용된 성능 용량 값을 모니터링하거나 단일 노드 또는 애그리게이트에 대한 세부 정보를 볼 수 있습니다.

사용된 성능 용량 값은 대시보드, 성능 인벤토리 페이지, 우수 성과 기록자 페이지, 임계값 정책 만들기 페이지, 성능 탐색기 페이지 및 세부 정보 차트에 표시됩니다. 예를 들어, Performance: All aggregate 페이지는 모든 애그리게이트에 사용된 성능 용량 값을 확인하는 데 사용되는 Performance Capacity 열을 제공합니다.



Status	Aggregate	Latency	IOPS	MBps	Perf. Capacity Used	Utilization	Free Capacity	Total Capacity	Cluster	Node	Policy
	opm_mo..._agg0	16.3 ms/op	124 IOPS	< 1 MBps	45%	9%	154 GB	3,179 GB	opm-mobility	opm-m...-02	
	rt_aggr2	19.8 ms/op	290 IOPS	< 1 MBps	45%	15%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	aggr_snap_mirror	13.9 ms/op	267 IOPS	< 1 MBps	38%	12%	6,692 GB	6,693 GB	opm-mobility	opm-m...-02	
	sdot_aggr	17.3 ms/op	745 IOPS	< 1 MBps	24%	11%	26,621 GB	26,774 GB	opm-mobility	opm-m...-02	
	aggr1	15.5 ms/op	434 IOPS	< 1 MBps	16%	6%	4,390 GB	20,080 GB	opm-mobility	opm-m...-01	
	rt_aggr1	22.3 ms/op	267 IOPS	< 1 MBps	11%	6%	6,691 GB	6,693 GB	opm-mobility	opm-m...-01	
	aggr2	15.6 ms/op	259 IOPS	1.03 MBps	11%	5%	18,472 GB	20,080 GB	opm-mobility	opm-m...-02	
	aggr2	9.52 ms/op	87 IOPS	20.8 MBps	Not Supported	5%	847 GB	984 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS
	RTaggr	7.62 ms/op	199 IOPS	34.7 MBps	Not Supported	6%	1,292 GB	1,477 GB	opm-lo...vity	opm-lo...ty-01	aggr_IOPS

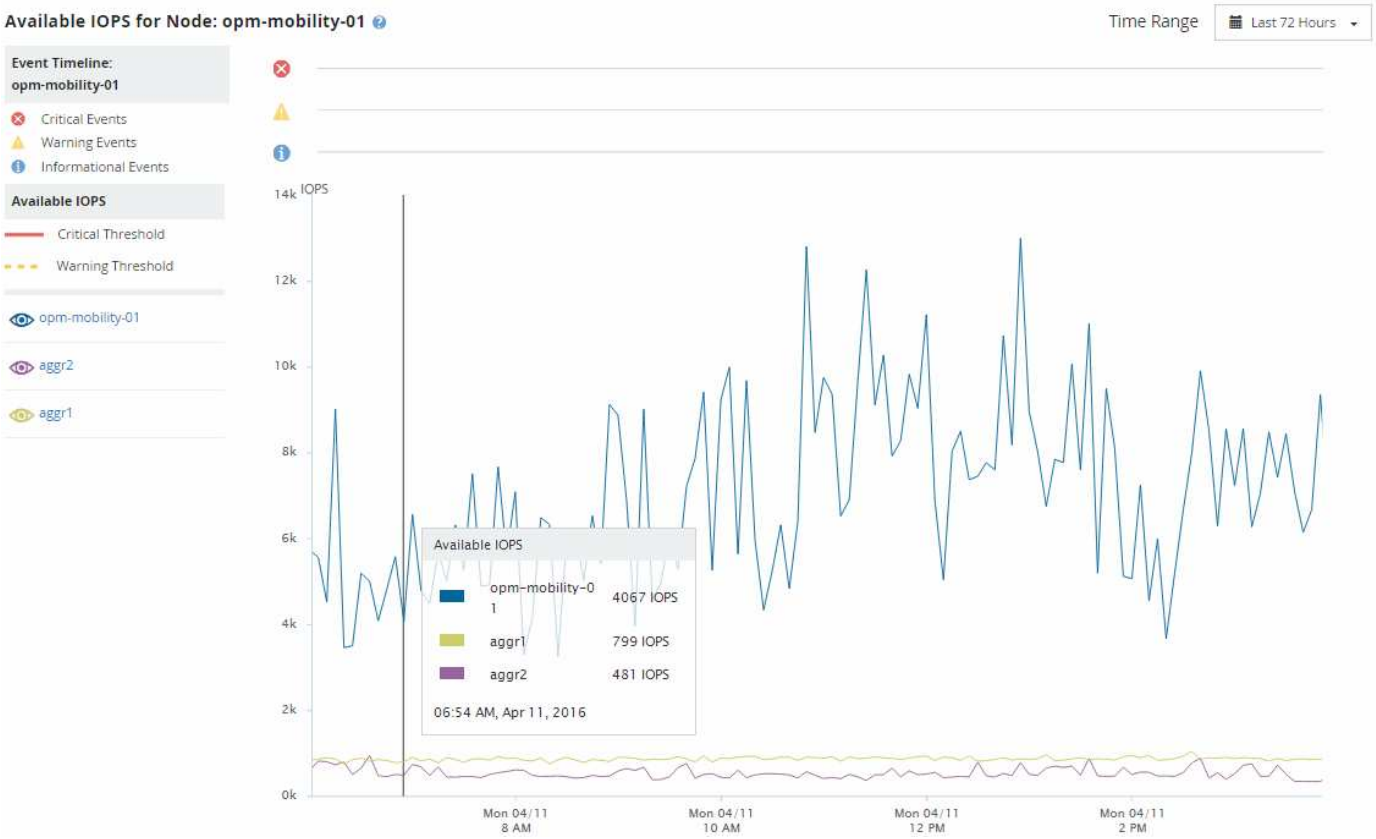
사용된 성능 용량 카운터를 모니터링하면 다음을 식별할 수 있습니다.

- 모든 클러스터에서 노드나 애그리게이트가 사용된 용량이 고성능 용량인지 여부
- 모든 클러스터에서 노드 또는 애그리게이트에 활성 성능 용량이 사용된 이벤트가 있는지 여부
- 클러스터에서 사용된 성능 용량이 가장 높고 그 용량이 가장 낮은 노드 및 애그리게이트
- 지연 시간 및 활용률 카운터 값은 사용된 성능 용량이 큰 노드 또는 애그리게이트와 함께 사용됩니다
- 노드 중 하나에 장애가 발생할 경우 HA 쌍에서 노드의 성능 용량이 사용되는 값에 영향을 미칩니다
- Aggregate에서 사용 중인 볼륨 및 LUN의 사용량이 가장 많고 성능 용량이 높은 값을 사용합니다

노드 및 애그리게이트 가용 **IOPS** 값 보기

모든 노드 또는 클러스터의 모든 애그리게이트에 대해 사용 가능한 IOPS 값을 모니터링하거나 단일 노드 또는 애그리게이트에 대한 세부 정보를 볼 수 있습니다.

사용 가능한 IOPS 값은 성능 인벤토리 페이지와 성능 탐색기 페이지 차트에서 노드 및 애그리게이트로 표시됩니다. 예를 들어, 노드/성능 탐색기 페이지에서 노드를 볼 때 목록에서 ""사용 가능한 IOPS"" 카운터 차트를 선택하면 해당 노드에서 사용 가능한 IOPS 값과 여러 애그리게이트를 비교할 수 있습니다.



사용 가능한 IOPS 카운터를 모니터링하여 다음을 식별할 수 있습니다.

- 사용 가능한 IOPS 값이 가장 큰 노드 또는 애그리게이트를 사용하여 향후 워크로드를 구축할 위치를 결정할 수 있습니다.
- 사용 가능한 최소 IOPS 값이 있는 노드 또는 애그리게이트는 향후 성능 문제가 발생할 수 있도록 모니터링해야 하는 리소스를 식별합니다.
- 가용 IOPS 값이 작은 애그리게이트에서 가장 많이 사용되는 볼륨 및 LUN

성능 용량 카운터 차트를 확인하여 문제를 파악합니다

성능 탐색기 페이지에서 노드 및 애그리게이트에 사용된 성능 용량 차트를 확인할 수 있습니다. 따라서 특정 기간 동안 선택한 노드 및 애그리게이트에 대한 자세한 성능 용량 데이터를 볼 수 있습니다.

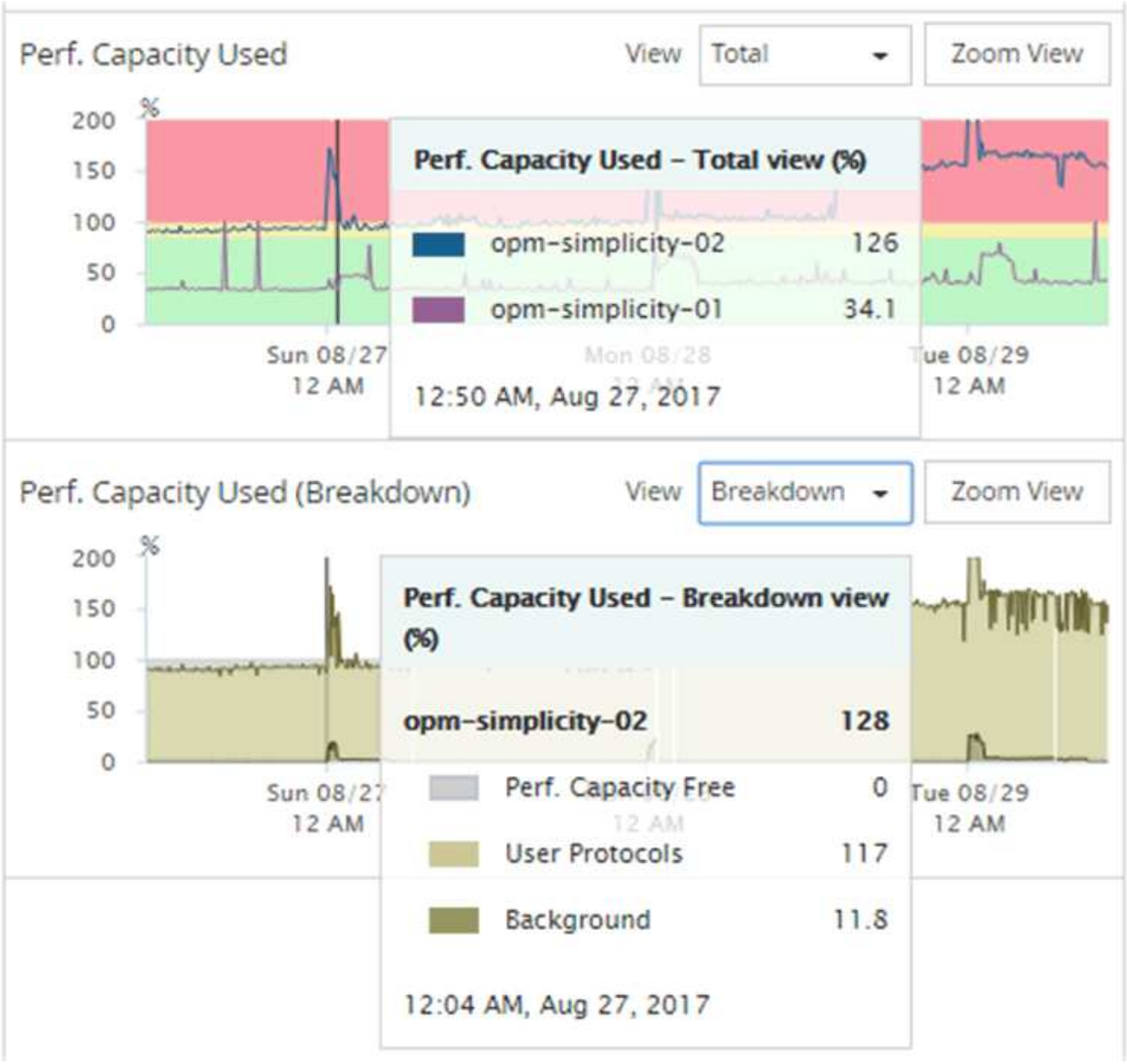
표준 카운터 차트에는 선택한 노드 또는 애그리게이트에 사용된 성능 용량 값이 표시됩니다. 분석 결과 카운터 차트는 사용자 프로토콜과 백그라운드 시스템 프로세스를 기준으로 사용 현황으로 구분된 루트 객체의 총 성능 용량 값을 표시합니다. 또한 여유 성능 용량도 표시됩니다.

> 시스템 및 데이터 관리와 관련된 일부 백그라운드 작업은 사용자 작업 부하로 식별되고 사용자 프로토콜로 분류되기 때문에 이러한 프로세스가 실행될 때 사용자 프로토콜 백분율이 인위적으로 높게 나타날 수 있습니다. 이러한 프로세스는 일반적으로 클러스터 사용량이 적은 자정부터 실행됩니다. 자정 무렵에 사용자 프로토콜 작업이 급증하는 경우 클러스터 백업 작업 또는 다른 백그라운드 작업이 해당 시간에 실행되도록 구성되었는지 확인합니다.

단계

1. 노드 또는 애그리게이트 * 랜딩 * 페이지에서 * 탐색기 * 탭을 선택합니다.
2. Counter Charts * 창에서 * Charts * 를 클릭하고 * Perf를 선택합니다. 사용된 용량 * 차트.
3. 차트를 볼 수 있을 때까지 아래로 스크롤합니다.

   표준 차트의 색상은 개체가 최적 범위(노란색)에 있을 때, 개체가 충분히 활용되지 않을 때(녹색), 그리고 개체가 과활용(빨간색)될 때 표시됩니다. 분석 차트에는 루트 객체에 대한 자세한 성능 용량 세부 정보만 표시됩니다.



4. 두 차트를 모두 전체 크기 형식으로 보려면 * 확대/축소 보기 * 를 클릭합니다.

   이러한 방식으로 여러 카운터 차트를 별도의 창에서 열어 동일한 기간 동안 사용된 성능 용량과 IOPS 또는 MBPS 값을 비교할 수 있습니다.

성능 용량에 사용된 성능 임계값 조건

노드 또는 애그리게이트에 사용된 성능 용량이 정의된 성능 용량 사용 임계값 설정을 초과할 경우

이벤트가 트리거되도록 사용자 정의 성능 임계값 정책을 생성할 수 있습니다.

또한 "사용된 성능 용량 인수" 임계값 정책으로 노드를 구성할 수 있습니다. 이 임계값 정책은 HA 쌍에서 두 노드 모두에 대해 사용된 성능 통계를 합산하여 다른 노드에 장애가 발생할 경우 두 노드 중 하나에 충분한 용량이 없는지 확인합니다. 페일오버 중 워크로드가 두 파트너 노드 워크로드의 조합이기 때문에 테이크오버 정책을 사용하는 것과 동일한 성능 용량이 두 노드에 적용될 수 있습니다.

이와 동등하게 사용되는 이 성능 용량은 일반적으로 노드 간에 적용됩니다. 하지만 페일오버 파트너를 통해 노드 중 하나에 대해 전달되는 노드 간 트래픽이 훨씬 더 많은 경우, 한 파트너 노드에서 모든 워크로드를 실행할 때 사용되는 총 성능 용량이 노드 장애 노드에 따라 약간 다를 수 있습니다.

사용된 성능 용량 조건은 LUN 및 볼륨에 대한 임계값을 정의할 때 조합 임계값 정책을 생성하기 위해 보조 성능 임계값 설정으로 사용될 수도 있습니다. 사용된 성능 용량 조건은 볼륨 또는 LUN이 상주하는 애그리게이트 또는 노드에 적용됩니다. 예를 들어 다음 조건을 사용하여 조합 임계값 정책을 만들 수 있습니다.

스토리지 객체	성능 카운터	경고 임계값	위험 임계값	기간
볼륨	지연 시간	15ms/운영	25ms/운영	20분
집계	사용된 성능 용량입니다	80%	95%	

조합 임계값 정책은 전체 기간 동안 두 조건이 모두 위반되는 경우에만 이벤트가 생성됩니다.

카운터를 사용하여 성능을 관리합니다

일반적으로 조직은 사용량이 가장 많은 시간에 대한 수요를 지원하기 위해 추가 성능 용량을 예약하면서 리소스가 효율적으로 사용되도록 100퍼센트 미만의 성능 용량을 사용하여 운영하려고 합니다. 임계값 정책을 사용하여 고성능 용량 사용 값에 대한 알림이 전송되는 시기를 사용자 지정할 수 있습니다.

성과 요구사항에 따라 특정 목표를 설정할 수 있습니다. 예를 들어 금융 서비스 기업은 적시에 거래를 실행할 수 있도록 더 많은 성능 용량을 확보할 수 있습니다. 이러한 회사에서는 70-80% 범위에서 사용된 성능 용량을 설정할 수 있습니다. 마진이 적은 제조 기업은 IT 비용을 보다 효율적으로 관리하기 위해 성능에 위험을 감수할 경우 성능 용량을 더 적게 예약할 수 있습니다. 이러한 회사는 사용된 성능 임계값을 85-95% 범위로 설정할 수 있습니다.

사용된 성능 용량이 사용자 정의 임계값 정책에서 설정된 비율을 초과하면 Unified Manager에서 경고 이메일을 보내고 이벤트를 이벤트 인벤토리 페이지에 추가합니다. 따라서 성능에 영향을 미치기 전에 잠재적 문제를 관리할 수 있습니다. 이러한 이벤트는 노드와 애그리게이트 내에서 워크로드를 이동하고 변경해야 하는 표시기도 사용할 수 있습니다.

노드 장애 조치 계획 페이지의 이해 및 사용

성능/노드 페일오버 계획 페이지에서는 노드의 고가용성(HA) 파트너 노드에 장애가 발생할 경우 노드에 대한 성능 영향을 예측합니다. Unified Manager는 HA 쌍 내 노드의 기간별 성능을 기준으로 추정합니다.

페일오버의 성능 영향을 예측하면 다음 시나리오에서 계획을 수립하는 데 도움이 됩니다.

- 페일오버로 인해 테이크오버 노드의 예상 성능이 허용되지 않는 수준으로 꾸준히 저하되면 페일오버 문제로 인한 성능 영향을 줄이기 위한 수정 조치를 고려해 볼 수 있습니다.
- 수동 페일오버를 시작하여 하드웨어 유지 관리 작업을 수행하기 전에 페일오버가 테이크오버 노드의 성능에 미치는 영향을 예측하여 작업을 수행하는 데 가장 적합한 시간을 결정할 수 있습니다.

노드 장애 조치 계획 페이지를 사용하여 수정 조치를 결정합니다

성능/노드 장애 조치 계획 페이지에 표시되는 정보를 기반으로, 장애 조치가 HA 쌍의 성능을 허용 수준 아래로 떨어뜨지 않도록 조치를 취할 수 있습니다.

예를 들어, 페일오버의 예상 성능 영향을 줄이려면 HA 쌍의 노드에서 일부 볼륨 또는 LUN을 클러스터의 다른 노드로 이동할 수 있습니다. 이렇게 하면 운영 노드가 페일오버 후에도 계속해서 적절한 성능을 제공할 수 있습니다.

노드 장애 조치 계획 페이지의 구성 요소입니다

성능/노드 장애 조치 계획 페이지의 구성 요소는 그리드 및 비교 창에 표시됩니다. 이 섹션에서는 노드 페일오버가 테이크오버 노드의 성능에 미치는 영향을 평가할 수 있습니다.

성능 통계 그리드

성능/노드 장애 조치 계획 페이지에는 지연 시간, IOPS, 활용도 및 사용된 성능 용량에 대한 통계가 포함된 그리드가 표시됩니다.

> 이 페이지와 성능/노드 성능 탐색기 페이지에 표시되는 지연 시간 및 IOPS 값이 일치하지 않을 수 있습니다. 다른 성능 카운터를 사용하여 노드 페일오버를 예측하는 값을 계산하기 때문입니다.

그리드에서 각 노드에는 다음 역할 중 하나가 할당됩니다.

- 기본

  파트너가 장애가 발생할 경우 HA 파트너에게 인계되는 노드입니다. 루트 개체는 항상 기본 노드입니다.

- 파트너

  페일오버 시나리오에서 장애가 발생한 노드입니다.

- 예상 인수

  운영 노드와 동일합니다. 이 노드에 대해 표시되는 성능 통계는 장애가 발생한 파트너가 테이크오버한 후 테이크오버 노드의 성능을 보여줍니다.

> 테이크오버 노드의 워크로드는 페일오버 후 두 노드의 결합된 워크로드와 동일하나, 예상 테이크오버에 대한 통계는 운영 노드와 파트너 노드의 통계를 합하지 않습니다. 예를 들어 운영 노드의 지연 시간이 2ms/op 이고 파트너 노드의 지연 시간이 3ms/op인 경우 예상 테이크오버의 지연 시간은 4ms/opp일 수 있습니다. 이 값은 Unified Manager에서 수행하는 계산입니다.

파트너 노드의 이름을 클릭하여 루트 객체가 되도록 할 수 있습니다. 성능/노드 성능 탐색기 페이지가 표시되면 * 장애 조치 계획 * 탭을 클릭하여 이 노드 장애 시나리오에서 성능이 어떻게 변경되는지 확인할 수 있습니다. 예를 들어, Node1이 기본 노드이고 Node2가 파트너 노드인 경우 Node2를 클릭하여 기본 노드로 설정할 수 있습니다. 이렇게

하면 장애가 발생한 노드에 따라 예상 성능이 어떻게 변경되는지 확인할 수 있습니다.

비교 창

다음 목록에서는 기본적으로 비교 창에 표시되는 구성 요소에 대해 설명합니다.

- * 이벤트 차트 *

  성능/노드 성능 탐색기 페이지의 형식과 동일한 형식으로 표시됩니다. 운영 노드에만 해당됩니다.

- * 카운터 차트 *

  이 표에는 그리드에 표시된 성능 카운터에 대한 기간별 통계가 표시됩니다. 각 차트에서 예상 테이크오버에 대한 그래프는 특정 시간에 페일오버가 발생한 경우의 예상 성능을 보여 줍니다.

  예를 들어, Utilization 차트가 오전 11시에 예상 테이크오버에 대해 73%를 표시한다고 가정해 보겠습니다 2월 8일. 해당 시점에 페일오버가 발생한 경우 테이크오버 노드의 활용률은 73%였습니다.

  기간별 통계를 사용하면 페일오버를 시작할 최적의 시간을 찾아 테이크오버 노드의 오버로드 가능성을 최소화할 수 있습니다. 테이크오버 노드의 예상 성능이 허용되는 경우에만 페일오버를 예약할 수 있습니다.

기본적으로 루트 객체와 파트너 노드에 대한 통계가 비교 창에 표시됩니다. 성능/노드 성능 탐색기 페이지와 달리 이 페이지에는 통계 비교를 위해 객체를 추가할 수 있는 * 추가 * 버튼이 표시되지 않습니다.

성능/노드 성능 탐색기 페이지에서 수행하는 것과 동일한 방식으로 비교 창을 사용자 지정할 수 있습니다. 다음 목록에서는 차트를 사용자 지정하는 예를 보여 줍니다.

- 노드 이름을 클릭하여 카운터 차트에서 노드의 통계를 표시하거나 숨깁니다.
- 확대/축소 보기 * 를 클릭하여 새 창에 특정 카운터에 대한 세부 차트를 표시합니다.

노드 장애 조치 계획 페이지에서 임계값 정책 사용

잠재적 장애 조치가 테이크오버 노드의 성능을 허용할 수 없는 수준으로 떨어뜨릴 경우 성능/노드 장애 조치 계획 페이지에서 알림을 받을 수 있도록 노드 임계값 정책을 생성할 수 있습니다.

"노드 HA 쌍 초과 사용"이라는 시스템 정의 성능 임계값 정책은 임계값이 6개의 연속 수집 기간(30분)에 걸쳐 위반될 경우 경고 이벤트를 생성합니다. HA 쌍에서 노드의 결합된 성능 용량이 200%를 초과하면 임계값이 위반된 것으로 간주됩니다.

시스템 정의 임계값 정책의 이벤트는 페일오버로 인해 테이크오버 노드의 지연 시간이 허용되지 않는 수준으로 증가한다는 사실을 알립니다. 특정 노드에 대해 이 정책에 의해 생성된 이벤트가 표시되면 해당 노드의 성능/노드 장애 조치 계획 페이지로 이동하여 페일오버로 인한 예상 지연 시간 값을 볼 수 있습니다.

이 시스템 정의 임계값 정책을 사용하는 것 외에도 ""Performance Capacity Used - Takover"" 카운터를 사용하여 임계값 정책을 생성한 다음 선택한 노드에 정책을 적용할 수 있습니다. 임계값을 200%보다 낮게 지정하면 시스템 정의 정책의 임계값이 위반되기 전에 이벤트를 받을 수 있습니다. 시스템 정의 정책 이벤트가 생성되기 전에 알림을 받으려면 임계값을 초과하는 최소 기간을 30분 미만으로 지정할 수도 있습니다.

예를 들어, HA 쌍에서 노드의 결합된 성능 용량이 175%를 10분 이상 초과하면 경고 이벤트를 생성하도록 임계값 정책을 정의할 수 있습니다. 이 정책을 Node1과 Node2에 적용할 수 있습니다. Node2는 HA 쌍을 형성합니다. Node1 또는 Node2에 대한 경고 이벤트 알림을 수신한 후 해당 노드에 대한 성능/노드 페일오버 계획 페이지를 보고 테이크오버

노드에 대한 예상 성능 영향을 평가할 수 있습니다. 페일오버가 발생하는 경우 테이크오버 노드에 과부하가 발생하지 않도록 수정 조치를 취할 수 있습니다. 노드에 사용된 결합된 성능 용량이 200% 미만이면 테이크오버 노드의 지연 시간이 허용되지 않는 레벨에 도달하지 않습니다. 이는 페일오버 중에 발생하는 경우에도 마찬가지입니다.

장애 조치 계획에 사용된 성능 용량 분석 차트를 사용합니다

상세 사용된 성능 용량 - 분석 차트는 운영 노드와 파트너 노드에 사용된 성능 용량을 보여 줍니다. 또한 예상 테이크오버의 노드에서 사용 가능한 성능 용량도 표시됩니다. 이 정보를 통해 파트너 노드에 장애가 발생할 경우 성능 문제가 있는지 여부를 확인할 수 있습니다.

이 분석 차트는 노드에 사용된 총 성능 용량을 보여 줄 뿐 아니라 각 노드의 값을 사용자 프로토콜 및 백그라운드 프로세스로 나눕니다.

- 사용자 프로토콜은 사용자 애플리케이션과 클러스터 간의 I/O 작업입니다.
- 백그라운드 프로세스는 스토리지 효율성, 데이터 복제 및 시스템 상태와 관련된 내부 시스템 프로세스입니다.

이러한 추가 세부 정보 수준을 통해 성능 문제가 사용자 애플리케이션 작업 또는 중복 제거, RAID 재구성, 디스크 스크러빙 및 SnapMirror 복사본과 같은 백그라운드 시스템 프로세스로 인해 발생하는지 여부를 확인할 수 있습니다.

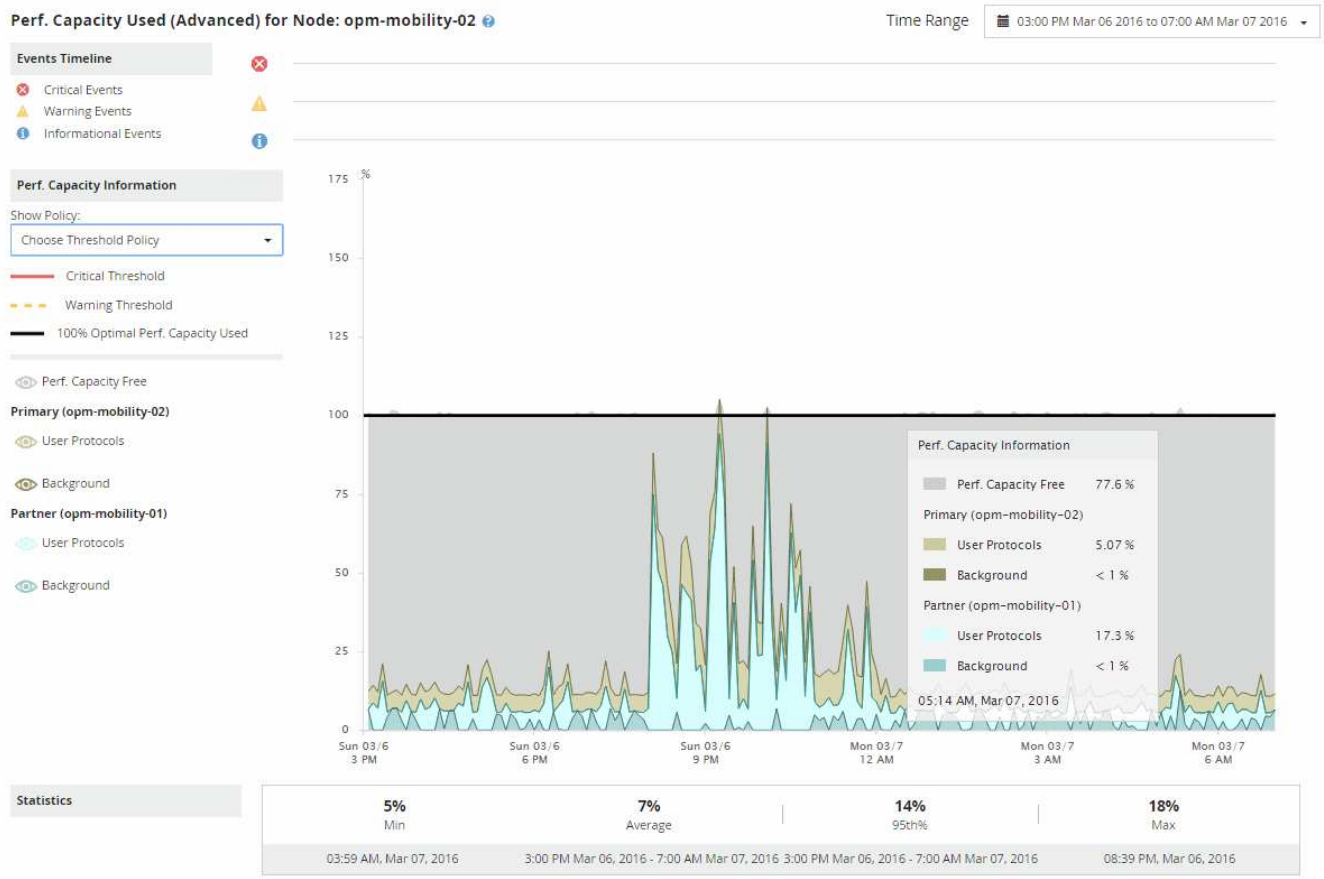
단계

1. 예상 대체품 노드로 사용할 노드의 * 성능/노드 장애 조치 계획 * 페이지로 이동합니다.
2. 시간 범위 * 선택기에서 카운터 그리드와 카운터 차트에 기록 통계가 표시되는 기간을 선택합니다.

   기본 노드, 파트너 노드 및 예상 대체 노드에 대한 통계를 포함하는 카운터 차트가 표시됩니다.

3. Charts * 선택 목록에서 * Perf를 선택합니다. 사용된 용량 *.
4. 성능 Capacity Used * 차트에서 * Breakdown * 을 선택하고 * Zoom View * 를 클릭합니다.

   성능 세부 정보 차트 사용된 용량이 표시됩니다.



5. 상세 차트 위로 커서를 이동하면 팝업 창에서 사용된 성능 용량이 표시됩니다.

   성능 Capacity Free Percentage는 예상 테이크오버에서 사용할 수 있는 성능 용량입니다. 페일오버 후 테이크오버 노드에 남은 성능 용량이 얼마나 되는지 나타냅니다. 페일오버가 0%인 경우 테이크오버 노드의 지연 시간이 허용되지 않는 수준으로 증가합니다.

6. 성능 용량이 낮은 가용 용량을 방지하기 위해 수정 조치를 취하는 것이 좋습니다.

   노드 유지 관리에 대한 페일오버를 시작하려면 성능 가용 용량 비율이 0이 아닐 때 파트너 노드에 장애가 발생할 시간을 선택합니다.

데이터 수집 및 워크로드 성능 모니터링

Unified Manager는 5분마다 워크로드 작업을 수집 및 분석하여 성능 이벤트를 식별하고, 15분마다 구성 변경을 감지합니다. 이 기능은 5분 동안의 기간별 성능 및 이벤트 데이터를 최대 30일까지 유지하며 이 데이터를 사용하여 모니터링되는 모든 워크로드에 대해 예측 가능한 지연 시간 범위를 예측합니다.

Unified Manager는 분석을 시작하기 전에, 그리고 워크로드 분석 페이지와 이벤트 세부 정보 페이지에 I/O 응답 시간에 대한 지연 시간 예측을 표시할 수 있도록 최소 3일간의 워크로드 활동을 수집해야 합니다. 이 활동이 수집되는 동안 지연 시간 예측은 워크로드 활동에서 발생하는 모든 변경 사항을 표시하지 않습니다. Unified Manager는 3일간의 활동을 수집한 후 오전 12시에 24시간마다 지연 시간 예측을 조정하여 워크로드 활동 변화를 반영하고 보다 정확한 동적 성능 임계값을 설정합니다.

Unified Manager가 워크로드를 모니터링하는 처음 4일 동안에는 마지막 데이터 수집 이후 24시간이 경과해도 지연

시간 차트에 해당 워크로드의 지연 시간 예측이 표시되지 않습니다. 마지막 컬렉션 이전에 감지된 이벤트는 계속 사용할 수 있습니다.

DST(일광 절약 시간)는 시스템 시간을 변경하여 모니터링되는 워크로드의 성능 통계에 대한 지연 시간 예측을 변경합니다. Unified Manager가 즉시 지연 시간 예측을 수정하기 시작하므로, 완료하는 데 약 15일이 소요됩니다. 이때 Unified Manager를 계속 사용할 수 있지만, Unified Manager에서는 지연 시간 예측을 사용하여 동적 이벤트를 감지하므로 일부 이벤트는 정확하지 않을 수 있습니다. 시간 변경 전에 감지된 이벤트는 영향을 받지 않습니다.

Unified Manager에서 모니터링하는 워크로드의 유형입니다

Unified Manager를 사용하여 사용자 정의 워크로드와 시스템 정의라는 두 가지 유형의 워크로드의 성능을 모니터링할 수 있습니다.

- * _ 사용자 정의 워크로드 _ *

  애플리케이션에서 클러스터로 I/O 처리량 이러한 프로세스는 읽기 및 쓰기 요청과 관련된 프로세스입니다. 볼륨, LUN, NFS 공유, SMB/CIFS 공유, 워크로드는 사용자 정의 워크로드입니다.

  Unified Manager는 클러스터의 워크로드 활동만 모니터링합니다. 애플리케이션, 클라이언트 또는 애플리케이션과 클러스터 간의 경로는 모니터링하지 않습니다.

  다음 중 하나 이상이 워크로드에 대해 참인 경우 Unified Manager에서 모니터링할 수 없습니다.

  - 읽기 전용 모드의 데이터 보호(DP) 복사본입니다. (DP 볼륨은 사용자가 생성한 트래픽을 모니터링합니다.)
  - 오프라인 데이터 클론입니다.
  - MetroCluster 구성에서 미러링된 볼륨입니다.

- *시스템 정의 워크로드 *

  다음을 비롯하여 스토리지 효율성, 데이터 복제 및 시스템 상태와 관련된 내부 프로세스:

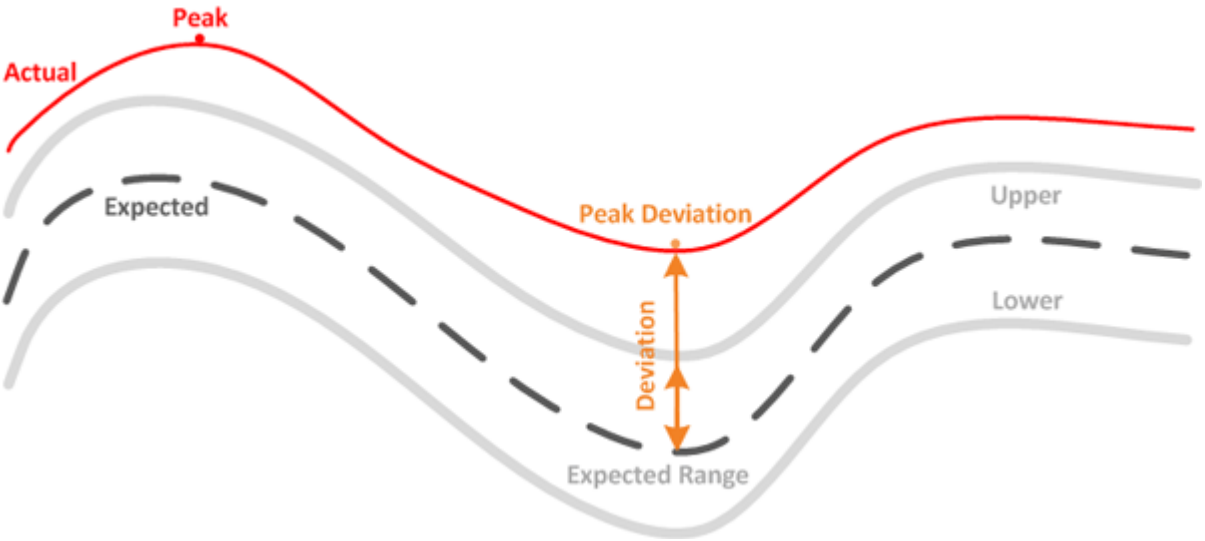
  - 중복 제거와 같은 스토리지 효율성
  - RAID 재구성, 디스크 스크러빙 등을 포함하는 디스크 상태
  - SnapMirror 복사본과 같은 데이터 복제 기능을 제공합니다
  - 관리 활동
  - 다양한 WAFL 작업을 포함하는 파일 시스템 상태입니다
  - WAFL 스캔과 같은 파일 시스템 스캐너입니다
  - 오프로드 스토리지 효율성 작업을 VMware 호스트에서 수행하는 등의 복제 오프로드
  - 볼륨 이동, 데이터 압축 등과 같은 시스템 상태입니다
  - 모니터링되지 않은 볼륨

시스템 정의 워크로드의 성능 데이터는 해당 워크로드에서 사용되는 클러스터 구성 요소의 경합이 발생한 경우에만 GUI에 표시됩니다. 예를 들어, GUI에서 성능 데이터를 보기 위해 시스템 정의 워크로드의 이름을 검색할 수 없습니다.

워크로드 성능 측정 값

Unified Manager는 기간별, 예상 통계 값을 기준으로 클러스터에서 워크로드의 성능을 측정하고, 해당 워크로드의 지연 시간 예측을 보여 줍니다. 또한 실제 워크로드의 통계 값을 지연 시간 예측과 비교하여 워크로드 성능이 너무 높거나 낮은 시기를 판단합니다. 예상대로 작동하지 않는 워크로드는 동적 성능 이벤트를 트리거하여 사용자에게 알립니다.

다음 그림에서 실제 값(빨간색)은 시간 프레임의 실제 성능 통계를 나타냅니다. 실제 값이 성능 임계값을 초과했습니다. 즉, 지연 시간 예측의 상한입니다. 피크는 시간 프레임에서 가장 높은 실제 값입니다. 편차는 예상 값(예측)과 실제 값 사이의 변화를 측정하는 반면, 최대 편차는 예상 값과 실제 값 사이의 가장 큰 변화를 나타냅니다.



다음 표에는 워크로드 성능 측정값이 나와 있습니다.

측정	설명
활동입니다	정책 그룹의 워크로드에 사용되는 QoS 제한의 백분율입니다. Unified Manager에서 볼륨 추가 또는 제거, QoS 제한 변경 등 정책 그룹의 변경 사항이 감지되면 실제 값과 예상 값이 설정 제한의 100%를 초과할 수 있습니다. 값이 설정 한계의 100%를 초과하면 100%를 초과하는 것으로 표시됩니다. 값이 설정 한계의 1% 미만이면 1% 미만으로 표시됩니다.
실제	지정된 워크로드의 특정 시간에 측정된 성능 값입니다.

측정	설명
편차	예상 값과 실제 값 간의 변경 실제 값에서 예상 값을 뺀 값을 예상 범위의 상한 값에서 예상 값을 뺀 비율입니다. 음의 편차 값은 워크로드 성능이 예상보다 낮음을 나타내고, 양의 편차 값은 워크로드 성능이 예상보다 높음을 나타냅니다.
필요합니다	예상 값은 지정된 워크로드에 대한 기간별 성능 데이터 분석을 기반으로 산출됩니다. Unified Manager는 이러한 통계 값을 분석하여 예상 값 범위(지연 시간 예측)를 결정합니다.
지연 시간 예측(예상 범위)	지연 시간 예측은 특정 시간에 있을 것으로 예상되는 상한 및 하한 성능 값을 예측한 것입니다. 워크로드 지연 시간의 경우 상한값이 성능 임계값을 구성합니다. 실제 값이 성능 임계값을 넘어가면 Unified Manager가 동적 성능 이벤트를 트리거합니다.
피크	일정 기간 동안 측정된 최대 값입니다.
피크 편차	일정 기간 동안 측정된 최대 편차 값입니다.
큐 길이	상호 연결 구성 요소에서 대기 중인 보류 중인 입출력 요청 수입니다.
활용률	네트워크 처리, 데이터 처리 및 집계 구성 요소의 경우 일정 기간 동안 워크로드 작업을 완료하는 데 걸리는 시간의 백분율입니다. 예를 들어, 네트워크 처리 또는 데이터 처리 구성 요소가 I/O 요청을 처리하거나 읽기 또는 쓰기 요청을 이행하는 aggregate에 대한 시간의 백분율입니다.
쓰기 처리량	로컬 클러스터의 워크로드부터 MetroCluster 구성의 파트너 클러스터까지 초당 메가바이트(MB/s)의 쓰기 처리량

예상되는 성능 범위는 얼마입니까

지연 시간 예측은 특정 시간에 있을 것으로 예상되는 상한 및 하한 성능 값을 예측한 것입니다. 워크로드 지연 시간의 경우 상한값이 성능 임계값을 구성합니다. 실제 값이 성능 임계값을 넘어가면 Unified Manager가 동적 성능 이벤트를 트리거합니다.

예를 들어, 정규 업무 시간 동안 오전 9시 사이에 있습니다 대부분의 직원은 오전 9시부터 오후 5시까지 이메일을 확인할 수 있습니다 오전 10시 30분 이메일 서버에 대한 수요가 증가하면 이 기간 동안 백엔드 스토리지의 워크로드 활동이 증가합니다. 직원들은 이메일 클라이언트에서 느린 응답 시간을 알아차릴 수 있습니다.

점심 시간 동안 오후 12시 사이에 오후 1시 그리고 오후 5시 이후 업무가 끝날 때 대부분의 직원들은 컴퓨터에서 떨어져

있을 가능성이 높습니다. 일반적으로 이메일 서버에 대한 수요가 감소하므로 백엔드 스토리지에 대한 요구도 감소합니다. 또는 오후 5시 이후에 시작되는 스토리지 백업 또는 바이러스 검사 등의 예약된 워크로드 작업이 있을 수 있습니다 백 엔드 스토리지에서의 활동을 늘려줍니다.

워크로드 활동의 증가 및 감소는 몇 일 동안 작업의 예상 범위(지연 시간 예측)를 결정합니다. 워크로드의 범위는 상한 및 하단으로 결정됩니다. 개체의 실제 워크로드 활동이 상한 또는 하위의 경계를 벗어나 일정 기간 동안 경계 외부에 있는 경우, 개체가 초과 사용 또는 과소사용됨을 나타낼 수 있습니다.

지연 시간 예측 구성 방법

Unified Manager에서 분석을 시작하기 전에, 그리고 GUI에 I/O 응답 시간에 대한 지연 시간 예측을 표시할 수 있으려면 최소 3일간의 워크로드 활동을 수집해야 합니다. 필요한 최소 데이터 수집은 워크로드 활동에서 발생하는 모든 변경 사항을 고려하지 않습니다. Unified Manager는 처음 3일 동안의 활동을 수집한 후 24시간마다 오전 12시에 지연 시간 예측을 조정합니다 워크로드 활동 변화를 반영하고 보다 정확한 동적 성능 임계값을 설정합니다.

DST(일광 절약 시간)는 시스템 시간을 변경하여 모니터링되는 워크로드의 성능 통계에 대한 지연 시간 예측을 변경합니다. Unified Manager가 즉시 지연 시간 예측을 수정하기 시작하므로, 완료하는 데 약 15일이 소요됩니다. 이때 Unified Manager를 계속 사용할 수 있지만, Unified Manager에서는 지연 시간 예측을 사용하여 동적 이벤트를 감지하므로 일부 이벤트는 정확하지 않을 수 있습니다. 시간 변경 전에 감지된 이벤트는 영향을 받지 않습니다.

성능 분석에 지연 시간 예측을 사용하는 방법

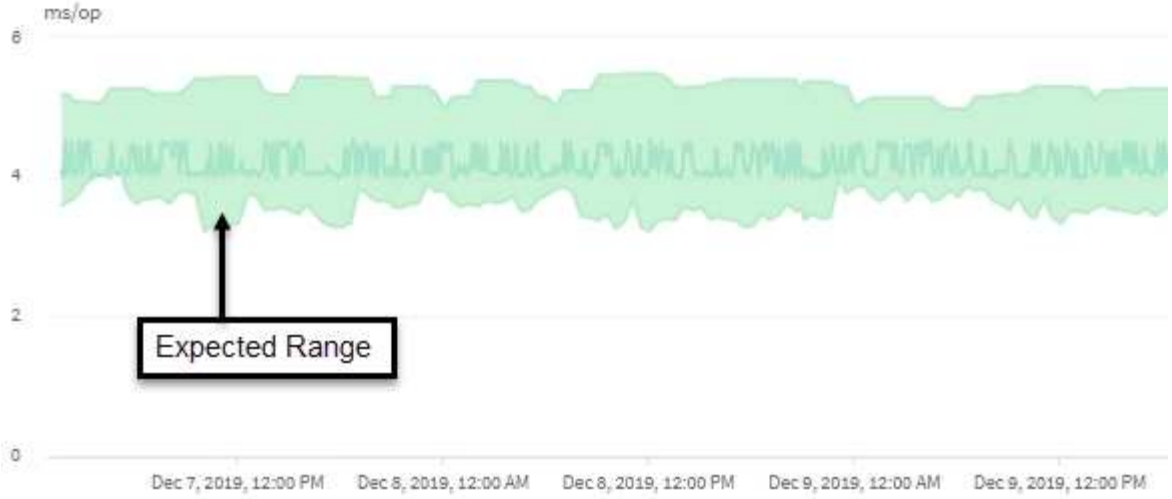
Unified Manager는 지연 시간 예측을 사용하여 모니터링되는 워크로드의 일반적인 I/O 지연 시간(응답 시간) 작업을 나타냅니다. 또한 워크로드의 실제 지연 시간이 지연 시간 예측 상한을 초과할 때 알림을 표시합니다. 그러면 동적 성능 이벤트가 트리거되어 성능 문제를 분석하고 해결 조치를 취할 수 있습니다.

지연 시간 예측은 워크로드의 성능 기준을 설정합니다. 시간이 지남에 따라 Unified Manager는 과거의 성능 측정값을 학습하여 워크로드에 대한 예상 성능 및 활동 수준을 예측합니다. 예상 범위의 상한은 동적 성능 임계값을 설정합니다. Unified Manager에서는 기준을 사용하여 실제 지연 시간이 임계값보다 높거나 낮거나 예상 범위를 벗어나는 시간을 결정합니다. 실제 값과 예상 값을 비교하여 워크로드에 대한 성능 프로필을 생성합니다.

클러스터 구성 요소의 경합으로 인해 워크로드의 실제 지연 시간이 동적 성능 임계값을 초과할 경우 지연 시간이 늘어나고 워크로드 성능이 예상보다 느려집니다. 동일한 클러스터 구성 요소를 공유하는 다른 워크로드의 성능도 예상보다 느릴 수 있습니다.

Unified Manager는 임계값 교차 이벤트를 분석하고 활동이 성능 이벤트인지 여부를 확인합니다. 몇 시간 등 긴 시간 동안 높은 워크로드 활동이 일관되게 유지되는 경우 Unified Manager는 해당 작업을 정상으로 간주하고 지연 시간 예측을 동적으로 조정하여 새로운 동적 성능 임계값을 구성합니다.

일부 워크로드는 활동이 일관되게 낮은 경우가 있으며, 지연 시간에 대한 대기 시간 예측은 시간이 지남에 따라 변화율이 높지 않습니다. 성능 이벤트를 분석하는 동안 이벤트 수를 최소화하기 위해 Unified Manager는 작업 및 지연 시간이 예상보다 훨씬 긴 작업량이 적은 볼륨에 대해서만 이벤트를 트리거합니다.



이 예에서 볼륨의 지연 시간은 지연 시간 예측(회색으로, 작업당 3.5밀리초(ms/op)이 가장 낮고 5.5ms/op이 가장 높은 것으로 표시됩니다. 네트워크 트래픽이 간헐적으로 급증하거나 클러스터 구성 요소의 경합으로 인해 실제 지연 시간이 갑자기 10ms/op로 증가하는 경우, 지연 시간이 예상을 초과하고 동적 성능 임계값을 초과하게 됩니다.

네트워크 트래픽이 감소하거나 클러스터 구성 요소의 경합이 더 이상 발생하지 않으면 지연 시간이 예상 지연 시간 내에서 반환됩니다. 지연 시간이 10ms/op 이상 지속될 경우 문제를 해결하기 위해 수정 조치를 취해야 할 수 있습니다.

Unified Manager에서 워크로드 지연 시간을 사용하여 성능 문제를 식별하는 방법

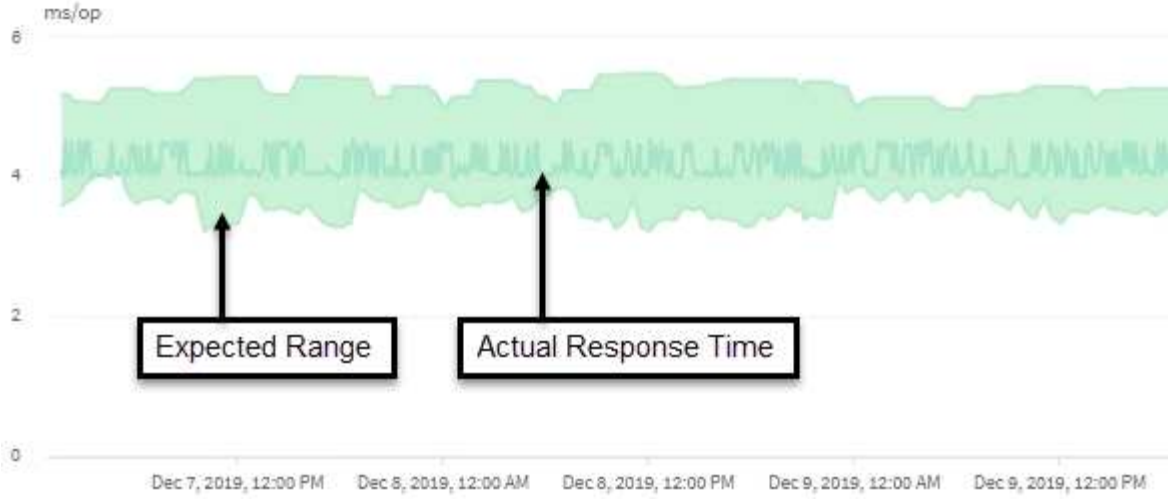
워크로드 지연 시간(응답 시간)은 클러스터의 볼륨이 클라이언트 애플리케이션의 I/O 요청에 응답하는 데 걸리는 시간입니다. Unified Manager는 지연 시간을 사용하여 성능 이벤트를 감지하고 경고합니다.

지연 시간이 높다는 것은 애플리케이션의 클러스터 볼륨 요청이 평소보다 더 오래 걸린다는 의미입니다. 하나 이상의 클러스터 구성 요소에 대한 경합으로 인해 클러스터 자체에 높은 지연 시간의 원인이 있을 수 있습니다. 또한 네트워크 병목 현상, 애플리케이션을 호스팅하는 클라이언트의 문제 또는 애플리케이션 자체 문제 등 클러스터 외부의 문제로 인해 지연 시간이 길어질 수 있습니다.

Unified Manager는 클러스터의 워크로드 활동만 모니터링합니다. 애플리케이션, 클라이언트 또는 애플리케이션과 클러스터 간의 경로는 모니터링하지 않습니다.

백업을 만들거나 중복 제거를 실행하는 것과 같이 클러스터에서 다른 워크로드에서 공유되는 클러스터 구성 요소의 요구를 증가시키는 작업은 또한 높은 지연 시간을 유발할 수 있습니다. 실제 지연 시간이 예상 범위(지연 시간 예측)의 동적 성능 임계값을 초과하는 경우 Unified Manager가 이벤트를 분석하여 해결해야 할 성능 이벤트인지 확인합니다. 지연 시간은 작업당 밀리초(ms/op)로 측정됩니다.

워크로드 분석 페이지의 총 지연 시간 차트에서 지연 시간 통계를 분석하여 읽기 및 쓰기 요청과 같은 개별 프로세스의 활동이 전체 지연 시간 통계와 어떻게 비교되는지 확인할 수 있습니다. 비교를 통해 가장 활동이 많은 작업이나 특정 작업이 볼륨의 지연 시간에 영향을 주는 비정상적인 활동을 가지고 있는지 여부를 확인할 수 있습니다. 성능 이벤트를 분석할 때 지연 시간 통계를 사용하여 클러스터의 문제로 인해 이벤트가 발생했는지 여부를 확인할 수 있습니다. 또한 이벤트와 관련된 특정 워크로드 활동이나 클러스터 구성 요소를 식별할 수도 있습니다.



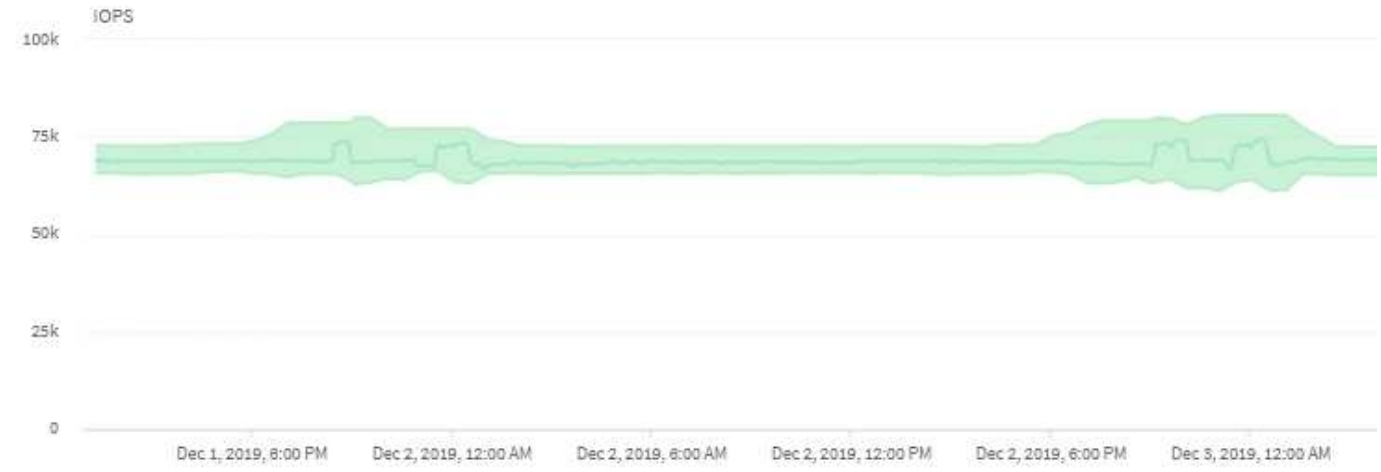
이 예에서는 지연 시간 차트를 보여 줍니다. 실제 응답 시간(지연 시간) 작업은 파란색 선으로, 지연 시간 예측(예상 범위)은 녹색입니다.

Unified Manager에서 데이터를 수집할 수 없을 경우 파란 선 안에 공백이 있을 수 있습니다. 이 문제는 클러스터 또는 볼륨에 연결할 수 없거나, 해당 시간 동안 Unified Manager를 껐거나, 수집 시간이 5분 이상 소요되었기 때문에 발생할 수 있습니다.

클러스터 작업이 워크로드 지연 시간에 미치는 영향

운영(IOPS)은 클러스터에서 모든 사용자 정의 및 시스템 정의 워크로드의 작업을 나타냅니다. IOPS 통계는 백업 또는 중복제거 실행 등과 같은 클러스터 프로세스가 워크로드 지연 시간(응답 시간)에 영향을 미치는지, 또는 성능 이벤트의 원인인지 여부를 파악하는 데 도움이 됩니다.

성능 이벤트를 분석할 때 IOPS 통계를 사용하여 성능 이벤트가 클러스터 문제로 인해 발생했는지 여부를 확인할 수 있습니다. 성과 이벤트의 주요 기여 요인이 되었을 수 있는 특정 워크로드 활동을 식별할 수 있습니다. IOPS는 초당 작업 수(ops/초)로 측정됩니다.



이 예에서는 IOPS 차트를 보여 줍니다. 실제 작업 통계는 파란색 선으로, 운영 통계의 IOPS 예측은 녹색입니다.

클러스터가 과부하된 경우 Unified Manager에서 "Cluster_cluster_name_"에 Data 수집이 너무 오래 걸립니다."라는 메시지를 표시할 수 있습니다. 즉, Unified Manager에서 분석할 수 있는 통계가 충분히 수집되지 않았습니다. 통계를 수집할 수 있도록 클러스터에서 사용하는 리소스를 줄여야 합니다.

MetroCluster 구성의 성능 모니터링

Unified Manager를 사용하면 MetroCluster 구성에서 클러스터 간 쓰기 처리량을 모니터링하여 쓰기 처리량이 많은 워크로드를 식별할 수 있습니다.

이러한 고성능 워크로드에 따라 로컬 클러스터의 다른 볼륨에 높은 I/O 응답 시간이 발생하는 경우 Unified Manager가 성능 이벤트를 트리거하여 사용자에게 알립니다.

Unified Manager는 MetroCluster 구성의 클러스터를 개별 클러스터로 처리합니다. 파트너이거나 쓰기 처리량을 각 클러스터와 상관시킬 수 있는 클러스터는 서로 구분되지 않습니다.

MetroCluster 구성의 로컬 클러스터가 데이터를 파트너 클러스터에 미러링하면 데이터가 NVRAM에 기록된 다음 ISL(Interswitch Link)을 통해 원격 애그리게이트로 전송됩니다. Unified Manager는 NVRAM을 분석하고, 높은 쓰기 처리량이 NVRAM을 지나치게 활용하여 NVRAM의 경합을 일으키는 워크로드를 파악합니다.

응답 시간의 편차가 성능 임계값을 초과하는 워크로드를 _DISPINGITERS_라고 하며 NVRAM에 대한 쓰기 처리량의 편차가 평소보다 높아 경합을 일으키는 워크로드를 _bullies_라고 합니다. 쓰기 요청만 파트너 클러스터에 미러링되므로 Unified Manager에서는 읽기 처리량을 분석하지 않습니다.

다음 화면에서 해당 LUN 및 볼륨의 워크로드를 분석하여 MetroCluster 구성에서 클러스터의 처리량을 확인할 수 있습니다. 클러스터를 통해 결과를 필터링할 수 있습니다. 왼쪽 탐색 창에서 다음을 수행합니다.

- * 스토리지 > 클러스터 > 성능: 모든 클러스터 * 보기. 을 참조하십시오
- * 스토리지 > 볼륨 > 성능: 모든 볼륨 * 보기.
- * 스토리지 > LUN > 성능: 모든 LUN * 보기.
- * 워크로드 분석 > 모든 워크로드 *
- 관련 정보 *

"성능 이벤트 분석 및 알림"

"MetroCluster 구성에 대한 성능 이벤트 분석"

"성능 이벤트와 관련된 워크로드의 역할"

"성능 이벤트와 관련된 피해자의 워크로드 파악"

"성능 이벤트와 관련된 대규모 워크로드 식별"

"성능 이벤트와 관련된 shark 워크로드 식별"

성능 이벤트 및 경고 이해

성능 이벤트는 클러스터의 워크로드 성능과 관련된 이벤트입니다. 응답 시간이 느린 워크로드를 식별하는 데 도움이 됩니다. 동시에 발생한 상태 이벤트와 함께 응답 시간 저하의 원인이 될 수

있거나 원인이 될 수 있는 문제를 파악할 수 있습니다.

Unified Manager에서 동일한 클러스터 구성 요소에 대해 같은 이벤트가 여러 번 감지되면 모든 이벤트가 별도의 이벤트가 아닌 단일 이벤트로 처리됩니다.

특정 심각도 유형의 성능 이벤트가 발생할 때 자동으로 e-메일 알림을 보내도록 알림을 구성할 수 있습니다.

성능 이벤트의 소스

성능 이벤트는 클러스터의 워크로드 성능과 관련된 문제입니다. 응답 시간이 느려 스토리지 객체를 식별하는 데 도움이 되며, 이를 지연 시간이라고도 합니다. 동시에 발생한 다른 상태 이벤트와 함께 응답 시간을 지연시켰거나 이로 인해 발생한 문제를 파악할 수 있습니다.

Unified Manager는 다음 소스에서 성능 이벤트를 수신합니다.

- * 사용자 정의 성능 임계값 정책 이벤트 *

  설정한 사용자 지정 임계값을 기반으로 성능 문제가 발생합니다. 성능 카운터의 임계값이 위반되었을 때 이벤트가 생성되도록 애그리게이트 및 볼륨 등의 스토리지 개체에 대한 성능 임계값 정책을 구성합니다.

  이러한 이벤트를 수신하려면 성능 임계값 정책을 정의하고 스토리지 개체에 할당해야 합니다.

- * 시스템 정의 성능 임계값 정책 이벤트 *

  시스템 정의된 임계값을 기반으로 하는 성능 문제입니다. 이러한 임계값 정책은 일반적인 성능 문제를 해결하기 위해 Unified Manager 설치에 포함됩니다.

  이러한 임계값 정책은 기본적으로 활성화되어 있으며 클러스터를 추가한 직후에 이벤트를 볼 수 있습니다.

- * 동적 성능 임계값 이벤트 *

  성능 문제는 IT 인프라에서 발생하는 장애 또는 오류 또는 클러스터 리소스를 과도하게 활용하는 워크로드의 결과입니다. 이러한 이벤트의 원인은 일정 기간 동안 자체적으로 해결되거나 수리 또는 구성 변경으로 해결될 수 있는 간단한 문제일 수 있습니다. 동적 임계값 이벤트는 공유 클러스터 구성 요소를 많이 사용하는 다른 워크로드로 인해 ONTAP 시스템의 워크로드가 느려졌음을 나타냅니다.

  이러한 임계값은 기본적으로 설정되어 있으며 새 클러스터에서 데이터를 수집한 후 3일이 지나면 이벤트가 표시될 수 있습니다.

성능 이벤트 심각도 유형

각 성능 이벤트는 심각도 유형과 관련되어 있으므로 즉각적인 수정 조치가 필요한 이벤트의 우선 순위를 지정하는 데 도움이 됩니다.

- * 심각 *

  수정 조치를 즉시 취하지 않을 경우 서비스 중단으로 이어질 수 있는 성능 이벤트가 발생했습니다.

  중요 이벤트는 사용자 정의 임계값에서만 전송됩니다.

- * 경고 *

  클러스터 개체의 성능 카운터가 정상 범위를 벗어났고 모니터링하여 심각도에 도달하지 않도록 해야 합니다. 이러한 심각도 때문에 서비스가 중단되지 않으며 즉각적인 수정 조치가 필요하지 않을 수 있습니다.

  경고 이벤트는 사용자 정의, 시스템 정의 또는 동적 임계값에서 전송됩니다.

- * 정보 *

  이 이벤트는 새 개체가 검색되거나 사용자 작업이 수행될 때 발생합니다. 예를 들어, 스토리지 객체가 삭제되거나 구성이 변경된 경우 심각도 유형 정보가 있는 이벤트가 생성됩니다.

  정보 이벤트는 구성 변경을 감지하면 ONTAP에서 직접 전송됩니다.

자세한 내용은 다음 링크를 참조하십시오.

- "이벤트 수신 시 발생하는 현상"
- "경고 이메일에 포함된 정보"
- "알림 추가"
- "성능 이벤트에 대한 알림 추가"

Unified Manager에서 구성 변경이 감지되었습니다

Unified Manager는 클러스터의 구성 변경 사항을 모니터링하여 변경이 성능 이벤트의 원인인지 또는 기여 원인인지 여부를 결정합니다. 성능 탐색기 페이지에 변경 이벤트 아이콘( )을 클릭하여 변경이 감지된 날짜와 시간을 표시합니다.

성능 탐색기 페이지와 워크로드 분석 페이지에서 성능 차트를 검토하여 변경 이벤트가 선택한 클러스터 개체의 성능에 영향을 미치는지 여부를 확인할 수 있습니다. 성능 이벤트와 거의 동시에 변경이 감지된 경우, 변경으로 인해 이벤트 알림이 트리거되었을 수 있습니다.

Unified Manager는 정보 이벤트로 분류되는 다음 변경 이벤트를 감지할 수 있습니다.

- 볼륨이 애그리게이트 간에 이동합니다.

  Unified Manager는 이동이 진행 중이거나 완료 또는 실패했는지 감지할 수 있습니다. 볼륨 이동 중에 Unified Manager가 다운된 경우, 볼륨이 백업될 때 볼륨 이동을 감지하고 해당 볼륨 이동을 위한 변경 이벤트를 표시합니다.

- 모니터링되는 하나 이상의 워크로드 변경이 포함된 QoS 정책 그룹의 처리량(MB/s 또는 IOPS) 제한

  정책 그룹 제한을 변경하면 지연 시간(응답 시간)이 간헐적으로 급증할 수 있으며, 이 경우 정책 그룹에 대한 이벤트도 트리거될 수 있습니다. 지연 시간이 점차 정상으로 돌아오며 급증으로 인한 이벤트는 더 이상 사용되지 않습니다.

- HA 쌍의 노드는 파트너 노드의 스토리지를 이어받거나 해당 노드를 다시 제공합니다.

  Unified Manager는 테이크오버, 부분 인수 또는 반환 작업이 완료된 시기를 감지할 수 있습니다. 패닉이 발생한 노드가 테이크오버로 인해 Unified Manager에서 이벤트를 감지하지 못하는 경우

- ONTAP 업그레이드 또는 되돌리기 작업이 성공적으로 완료되었습니다.

이전 버전과 새 버전이 표시됩니다.

시스템 정의 성능 임계값 정책의 유형입니다

Unified Manager는 클러스터 성능을 모니터링하고 이벤트를 자동으로 생성하는 몇 가지 표준 임계값 정책을 제공합니다. 이러한 정책은 기본적으로 사용하도록 설정되어 있으며 모니터링되는 성능 임계값이 위반될 때 경고 또는 정보 이벤트를 생성합니다.

Cloud Volumes ONTAP, ONTAP Edge 또는 ONTAP Select 시스템에서는 시스템 정의 성능 임계값 정책이 사용되지 않습니다.

시스템 정의 성능 임계값 정책에서 불필요한 이벤트를 수신하는 경우 이벤트 설정 페이지에서 개별 정책에 대한 이벤트를 비활성화할 수 있습니다.

클러스터 임계값 정책

기본적으로 시스템 정의 클러스터 성능 임계값 정책은 Unified Manager가 모니터링하는 모든 클러스터에 할당됩니다.

- * 클러스터 로드 불균형 *

  한 노드가 클러스터의 다른 노드보다 훨씬 더 높은 부하에서 작동 중이고 따라서 워크로드 지연 시간에 영향을 줄 수 있는 상황을 식별합니다.

  이는 클러스터의 모든 노드에 사용된 성능 용량 값을 비교하여 어떤 노드도 24시간 이상 30% 임계값을 초과하는지 여부를 확인하는 방식으로 실행됩니다. 이것은 경고 이벤트입니다.

- * 클러스터 용량 불균형 *

  하나의 애그리게이트에서 클러스터의 다른 애그리게이트보다 훨씬 더 많은 용량이 사용되고 있으므로 작업에 필요한 공간에 영향을 줄 수 있는 상황을 식별합니다.

  이는 클러스터 내의 모든 애그리게이트에서 사용된 용량 값을 비교하여 애그리게이트 간에 70%의 차이가 있는지 여부를 확인하는 방식으로 실행됩니다. 이것은 경고 이벤트입니다.

노드 임계값 정책

기본적으로 시스템 정의 노드 성능 임계값 정책은 Unified Manager가 모니터링하는 클러스터의 모든 노드에 할당됩니다.

- * 사용된 성능 용량 임계값 위반 *

  단일 노드가 운영 효율성 한계를 초과하여 작동하고 따라서 워크로드 지연 시간에 영향을 미칠 수 있는 상황을 식별합니다.

  이는 성능 용량의 100% 이상을 12시간 이상 사용하는 노드를 찾는 것입니다. 이것은 경고 이벤트입니다.

- * 노드 HA Pair 초과 활용 *

  HA 쌍 노드가 HA 쌍 운영 효율성 한계를 초과하여 작동하는 상황을 식별합니다.

이 작업을 위해 HA 쌍의 두 노드에 사용된 성능 용량을 확인합니다. 두 노드에서 사용하는 결합된 성능 용량이 12시간 이상 200%를 초과하면 컨트롤러 페일오버가 워크로드 지연 시간에 영향을 미칩니다. 이것은 정보 이벤트입니다.

- * 노드 디스크 조각화 *

  Aggregate의 디스크 또는 디스크가 조각화되어 주요 시스템 서비스가 느려지고 노드의 워크로드 지연 시간에 영향을 줄 수 있는 상황을 식별합니다.

  노드의 모든 애그리게이트에서 특정 읽기 및 쓰기 작업 비율을 살펴보면 이 작업이 수행됩니다. 이 정책은 SyncMirror 재동기화 중에 또는 디스크 스크럽 작업 중에 오류가 발견된 경우에도 트리거될 수 있습니다. 이것은 경고 이벤트입니다.

  ⓘ "'노드 디스크 조각화' 정책은 HDD 전용 애그리게이트를 분석하지만, Flash Pool, SSD, FabricPool 애그리게이트는 분석되지 않습니다.

임계값 정책을 집계합니다

시스템 정의 애그리게이트의 성능 임계값 정책은 기본적으로 Unified Manager가 모니터링하는 클러스터의 모든 애그리게이트로 할당됩니다.

- * 과도하게 사용된 디스크 집계 *

  애그리게이트는 운영 효율성 한계를 초과하여 작동하는 상황을 식별하여 워크로드 지연 시간에 영향을 줄 수 있습니다. 이 방법을 통해 aggregate에서 디스크가 30분 이상 95% 이상 활용되는 애그리게이트를 찾을 수 있습니다. 이 다중 조건 정책은 다음 분석을 수행하여 문제의 원인을 파악합니다.

  - 현재 백그라운드 유지 관리 작업을 진행 중인 aggregate의 디스크가 있습니까?

    디스크 재구성, 디스크 스크럽, SyncMirror 재동기화 및 재패리티가 디스크에 실행될 수 있는 일부 백그라운드 유지 관리 작업입니다.

  - 디스크 쉘프 파이버 채널 인터커넥트에 통신 병목 현상이 있습니까?
  - Aggregate에 사용 가능한 용량이 너무 적습니까? 세 하위 정책 중 하나 이상의 정책이 위반된 것으로 간주되는 경우에만 이 정책에 대해 경고 이벤트가 발생합니다. Aggregate의 디스크가 95% 이상 사용된 경우 성능 이벤트가 트리거되지 않습니다.

ⓘ "'Aggregate disks over-활용되는' 정책은 HDD 전용 애그리게이트 및 Flash Pool(하이브리드) 애그리게이트를 분석하며, SSD와 FabricPool 애그리게이트는 분석되지 않습니다.

워크로드 지연 임계값 정책

시스템 정의 워크로드 지연 임계값 정책은 ""예상 지연 시간" 값이 정의된 성능 서비스 수준 정책이 구성된 모든 워크로드에 할당됩니다.

- * 워크로드 볼륨/LUN 지연 임계값 성능 서비스 수준 * 에서 정의한 대로 위반됩니다

  "예상 지연 시간" 제한을 초과했으며 워크로드 성능에 영향을 주는 볼륨(파일 공유) 및 LUN을 식별합니다. 이것은 경고 이벤트입니다.

  이는 이전 시간 동안 예상 지연 시간 값을 30% 초과한 워크로드를 찾는 것입니다.

QoS 임계값 정책

시스템 정의 QoS 성능 임계값 정책은 ONTAP QoS 최대 처리량 정책(IOPS, IOPS/TB 또는 MB/s)이 구성된 모든 워크로드에 할당됩니다. Unified Manager가 워크로드 처리량 값이 구성된 QoS 값보다 15% 작은 경우 이벤트를 트리거합니다.

- * QoS 최대 IOPS 또는 MB/s 임계값 *

  QoS 최대 IOPS 또는 MB/s 처리량 한도를 초과했으며 워크로드 지연 시간에 영향을 주는 볼륨 및 LUN을 식별합니다. 이것은 경고 이벤트입니다.

  단일 워크로드가 정책 그룹에 할당되면 이전 시간의 각 수집 기간 동안 할당된 QoS 정책 그룹에 정의된 최대 처리량 임계값을 초과한 워크로드를 찾습니다.

  여러 워크로드가 단일 QoS 정책을 공유하는 경우 정책에 있는 모든 워크로드의 IOPS 또는 MB/s를 추가하고 이 임계값을 확인하여 해당 작업을 수행합니다.

- * QoS 최대 IOPS/TB 또는 IOPS/TB, 블록 크기 임계값 *

  적응형 QoS 최대 IOPS/TB 처리량 한도(또는 블록 크기 제한이 있는 IOPS/TB)를 초과했으며 워크로드 지연 시간에 영향을 주는 볼륨을 식별합니다. 이것은 경고 이벤트입니다.

  이렇게 하려면 적응형 QoS 정책에 정의된 최대 IOPS/TB 임계값을 각 볼륨의 크기를 기준으로 QoS 최대 IOPS 값으로 변환한 다음, 이전 시간의 각 성능 수집 기간 동안 QoS 최대 IOPS를 초과한 볼륨을 찾습니다.

  이 정책은 클러스터가 ONTAP 9.3 이상 소프트웨어와 함께 설치된 경우에만 볼륨에 적용됩니다.

  적응형 QoS 정책에 ""블록 크기"" 요소가 정의되면 각 볼륨의 크기에 따라 임계값이 QoS 최대 MB/s 값으로 변환됩니다. 그런 다음 이전 시간 동안 각 성능 수집 기간 동안 QoS 최대 MB/s를 초과한 볼륨을 찾습니다.

  이 정책은 클러스터가 ONTAP 9.5 이상 소프트웨어와 함께 설치된 경우에만 볼륨에 적용됩니다.

성능 이벤트 분석 및 알림

성능 이벤트는 클러스터 구성 요소의 경합으로 인해 발생하는 워크로드의 I/O 성능 문제를 알려줍니다. Unified Manager에서 이벤트를 분석하여 관련 워크로드, 경합 중인 구성 요소 및 문제가 여전히 해결해야 할 문제인지 여부를 파악합니다.

Unified Manager는 클러스터의 볼륨에 대한 I/O 지연 시간(응답 시간) 및 IOPS(작업)를 모니터링합니다. 예를 들어, 다른 워크로드가 클러스터 구성 요소를 과도하게 사용하면 구성 요소의 경합이 발생할 수 있으며, 워크로드 수요를 충족하기 위해 최적의 레벨에서 성능을 발휘할 수 없습니다. 동일한 구성요소를 사용하는 다른 워크로드의 성능이 영향을 받을 수 있어 지연 시간이 증가할 수 있습니다. 지연 시간이 동적 성능 임계값을 초과하는 경우 Unified Manager가 성능 이벤트를 트리거하여 사용자에게 알립니다.

이벤트 분석

Unified Manager는 이전 15일간의 성능 통계를 사용하여 피해자 워크로드, 불특정 워크로드 및 이벤트와 관련된 클러스터 구성 요소를 파악합니다.

- 지연 시간이 동적 성능 임계값을 초과한 피해자 워크로드 파악, 즉 지연 시간 예측의 상한값

- HDD 또는 Flash Pool 하이브리드 애그리게이트(로컬 계층)의 볼륨의 경우, 지연 시간이 5밀리초(ms)보다 크고 IOPS가 초당 10개 이상의 작업(ops/sec)인 경우에만 이벤트가 트리거됩니다.
- All-SSD 애그리게이트 또는 FabricPool 애그리게이트(클라우드 계층)의 볼륨의 경우, 지연 시간이 1ms 미만이고 IOPS가 100 ops/sec를 초과할 경우에만 이벤트가 트리거됩니다

- 경합하는 클러스터 구성 요소를 식별합니다.

  클러스터 인터커넥트의 피해자 워크로드 지연 시간이 1ms 이상이면 Unified Manager는 이를 중요한 것으로 간주하고 클러스터 인터커넥트에 대한 이벤트를 트리거합니다.

- 클러스터 구성 요소를 과도하게 사용하여 경합을 일으키는 대규모 워크로드를 식별합니다.
- 클러스터 구성 요소의 활용도 또는 활동 편차에 따라 관련 워크로드의 순위를 매기하여 클러스터 구성 요소의 사용 빈도가 가장 높고 가장 큰 영향을 받는 피해자를 결정합니다.

이벤트는 잠시 동안 발생할 수 있으며, 사용 중인 구성 요소가 더 이상 충돌하지 않으면 이벤트가 자동으로 보정됩니다. 연속 이벤트는 5분 간격 내에 동일한 클러스터 구성 요소에 대해 다시 발생하고 활성 상태로 유지되는 이벤트입니다. 지속적인 이벤트의 경우, Unified Manager는 두 번의 연속 분석 간격 동안 동일한 이벤트를 감지한 후 알림을 트리거합니다.

이벤트가 해결되면 Unified Manager에서 볼륨에 대한 이전 성능 문제 레코드의 일부로 계속 사용할 수 있습니다. 각 이벤트에는 이벤트 유형과 관련된 볼륨, 클러스터 및 클러스터 구성 요소를 식별하는 고유한 ID가 있습니다.

단일 볼륨은 동시에 여러 이벤트에 참여할 수 있습니다.

이벤트 상태입니다

이벤트는 다음 상태 중 하나일 수 있습니다.

- * 활성 *

  성능 이벤트가 현재 활성 상태(새 이벤트 또는 확인된 이벤트)임을 나타냅니다. 이벤트를 발생시키는 문제가 자체적으로 해결되지 않았거나 해결되지 않았습니다. 스토리지 개체의 성능 카운터는 성능 임계값보다 높게 유지됩니다.

- * 사용되지 않음 *

  이벤트가 더 이상 활성 상태가 아님을 나타냅니다. 이벤트를 발생시키는 문제가 자체적으로 해결되었거나 해결되었습니다. 스토리지 개체의 성능 카운터가 더 이상 성능 임계값을 초과하지 않습니다.

이벤트 알림

이벤트는 대시보드 페이지와 사용자 인터페이스의 다른 여러 페이지에 표시되며, 이러한 이벤트에 대한 알림은 지정된 이메일 주소로 전송됩니다. 이벤트에 대한 자세한 분석 정보를 보고 이벤트 세부 정보 페이지 및 워크로드 분석 페이지에서 해결 방법을 확인할 수 있습니다.

이벤트 상호 작용

이벤트 세부 정보 페이지와 워크로드 분석 페이지에서 다음과 같은 방법으로 이벤트와 상호 작용할 수 있습니다.

- 이벤트 위로 마우스를 이동하면 이벤트가 감지된 날짜와 시간을 표시하는 메시지가 표시됩니다.

동일한 기간에 여러 이벤트가 있는 경우 메시지에 이벤트 수가 표시됩니다.

- 단일 이벤트를 클릭하면 관련된 클러스터 구성 요소를 비롯하여 이벤트에 대한 자세한 정보를 보여 주는 대화 상자가 표시됩니다.

  경합이 발생한 구성 요소에 동그라미가 표시되며 빨간색으로 강조 표시됩니다. 전체 분석 보기 * 를 클릭하여 이벤트 세부 정보 페이지에서 전체 분석을 볼 수 있습니다. 같은 기간에 여러 이벤트가 있는 경우 대화 상자에 가장 최근의 세 이벤트에 대한 세부 정보가 표시됩니다. 이벤트를 클릭하여 이벤트 세부 정보 페이지에서 이벤트 분석을 볼 수 있습니다.

Unified Manager에서 이벤트에 대한 성능 영향을 확인하는 방법

Unified Manager에서는 작업 부하에 대한 활동, 활용률, 쓰기 처리량, 클러스터 구성요소 사용량, I/O 지연 시간(응답 시간)의 편차를 사용하여 워크로드 성능에 미치는 영향 수준을 결정합니다. 이 정보는 이벤트 세부 정보 페이지에서 각 워크로드의 역할 및 순위를 결정합니다.

Unified Manager는 워크로드에서 마지막으로 분석된 값을 예상 범위(지연 시간 예측)와 비교합니다. 마지막으로 분석한 값과 예상 값 범위 간의 차이는 이벤트의 성능에 가장 큰 영향을 준 워크로드를 식별합니다.

예를 들어, 클러스터에 워크로드 A와 워크로드 B의 두 워크로드가 포함되어 있다고 가정해 보겠습니다 워크로드 A에 대한 지연 예측은 작업당 5-10밀리초(ms/op)이며 실제 지연 시간은 대개 약 7ms/op입니다. 워크로드 B에 대한 대기 시간은 10-20ms/op이고 실제 대기 시간은 대개 약 15ms/opp입니다. 두 워크로드 모두 예상 지연 시간 내에 처리되었습니다. 클러스터의 경합으로 인해 두 워크로드의 지연 시간이 40ms/op로 증가하여 지연 시간 예측 상한인 동적 성능 임계값을 초과하고 이벤트를 트리거합니다. 워크로드 A의 경우 예상 값에서 성능 임계값보다 높은 값으로 지연 시간의 편차는 약 33ms/op이고 워크로드 B의 편차는 약 25ms/opp입니다. 두 워크로드의 지연 시간이 40ms/op로 급증하지만, 워크로드 A의 지연 시간이 33ms/opp에서 지연 시간의 편차가 더 높으므로 성능에 더 큰 영향을 미쳤습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에서 클러스터 구성 요소의 활동, 활용률 또는 처리량의 편차를 기준으로 워크로드를 정렬할 수 있습니다. 지연 시간별로 워크로드를 정렬할 수도 있습니다. 정렬 옵션을 선택하면 Unified Manager에서 이벤트가 예상 값에서 감지되어 워크로드 정렬 순서를 결정하기 때문에 활동, 활용률, 처리량, 지연 시간의 편차를 분석합니다. 지연 시간의 경우 빨간색 점(🔴)는 피해자 워크로드에 의한 성능 임계값 및 지연 시간에 대한 후속 영향을 나타냅니다. 각 빨간색 점은 지연 시간의 편차가 더 높음을 나타냅니다. 이를 통해 이벤트의 지연 시간이 가장 큰 영향을 받은 피해자의 워크로드를 파악할 수 있습니다.

클러스터 구성 요소 및 구성 요소의 경합이 발생할 수 있는 이유

클러스터 구성 요소의 경합이 발생할 때 클러스터 성능 문제를 식별할 수 있습니다. 구성 요소를 사용하는 워크로드의 성능이 느려지고 클라이언트 요청에 대한 응답 시간(지연 시간)이 증가하여 Unified Manager에서 이벤트가 트리거됩니다.

경합이 발생한 구성 요소는 최적 수준에서 수행할 수 없습니다. 성능이 저하되었으며, _ 피해자라고 하는 다른 클러스터 구성 요소와 워크로드의 성능이 지연 시간을 증가했을 수 있습니다. 구성 요소의 경합을 줄이려면 작업 부하를 줄이거나 작업 처리 능력을 높여 성능이 정상 수준으로 돌아가도록 해야 합니다. Unified Manager는 5분 간격으로 워크로드 성능을 수집 및 분석하므로, 클러스터 구성 요소가 지속적으로 초과 사용되는 경우에만 감지합니다. 5분 간격 동안 짧은 시간 동안만 지속되는 일시적인 과사용량 급증은 감지되지 않습니다.

예를 들어, 스토리지 aggregate에서 발생하는 경합이 발생할 수 있습니다. 그 이유는 하나 이상의 워크로드가 I/O 요청을 이행하기 위해 경합하기 때문입니다. Aggregate의 다른 워크로드에 영향을 줄 수 있으므로 성능이 저하될 수 있습니다. 애그리게이트에서 수행하는 작업의 양을 줄이기 위해 하나 이상의 워크로드를 사용량이 적은 애그리게이트 또는 노드로 이동하여 현재 애그리게이트의 전체 워크로드 요구사항을 줄이는 것과 같은 다양한 단계를 수행할 수

있습니다. QoS 정책 그룹의 경우 처리량 제한을 조정하거나 워크로드를 다른 정책 그룹으로 이동하여 워크로드가 더 이상 제한되지 않도록 할 수 있습니다.

Unified Manager에서 다음 클러스터 구성 요소를 모니터링하여 경합 상태를 경고합니다.

- 네트워크 *

  클러스터의 외부 네트워킹 프로토콜에 의한 I/O 요청 대기 시간을 나타냅니다. 대기 시간은 클러스터가 입출력 요청에 응답하기 전에 ""전송 준비"" 트랜잭션이 완료될 때까지 기다리는 데 걸리는 시간입니다. 네트워크 구성 요소의 경합이 발생한 경우, 프로토콜 계층에서 대기 시간이 길면 하나 이상의 워크로드 지연 시간에 영향을 미치게 됩니다.

- * 네트워크 처리 *

  프로토콜 계층과 클러스터 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 이벤트가 감지된 이후 네트워크 처리를 처리하는 노드가 변경되었을 수 있습니다. 네트워크 처리 구성 요소의 경합이 발생한 경우, 네트워크 처리 노드의 높은 사용률이 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

  액티브-액티브 구성에서 모든 SAN 어레이 클러스터를 사용할 경우 두 노드에 대해 네트워크 처리 지연 시간 값이 표시되므로 노드가 로드를 균등하게 공유하고 있는지 확인할 수 있습니다.

- * QoS 제한 최대 *

  워크로드에 할당된 스토리지 QoS(Quality of Service) 정책 그룹의 최대 처리량(최대) 설정을 나타냅니다. 정책 그룹 구성 요소의 경합이 발생한 경우 정책 그룹의 모든 워크로드가 설정된 처리량 제한에 따라 조절되고, 이로 인해 하나 이상의 워크로드 지연 시간이 영향을 받습니다.

- * QoS 제한 최소 *

  다른 워크로드에 할당된 QoS 처리량 최소(예상) 설정으로 인해 워크로드의 지연 시간을 나타냅니다. 특정 워크로드에 설정된 QoS 최소값이 대부분의 대역폭을 사용하여 보장된 처리량을 보장하는 경우, 다른 워크로드의 임계치가 조절되고 더 많은 지연 시간이 표시됩니다.

- 클러스터 인터커넥트 *

  클러스터된 노드가 물리적으로 연결된 케이블과 어댑터를 나타냅니다. 클러스터 인터커넥트 구성 요소의 경합이 발생한 경우, 클러스터 인터커넥트에서 I/O 요청이 있을 때까지 대기 시간이 길어 하나 이상의 워크로드 지연 시간에 영향을 미치게 됩니다.

- * 데이터 처리 *

  는 클러스터와 워크로드를 포함하는 스토리지 애그리게이트 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 이벤트가 감지된 이후 데이터 처리를 처리하는 노드가 변경될 수 있습니다. 데이터 처리 구성 요소의 경합이 발생한 경우, 데이터 처리 노드의 높은 활용률이 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

- * 볼륨 활성화 *

  모든 활성 볼륨의 사용량을 추적하는 프로세스를 나타냅니다. 1,000개 이상의 볼륨이 활성 상태인 대규모 환경에서는 이 프로세스에서 노드를 통해 동시에 리소스에 액세스해야 하는 중요 볼륨의 수를 추적합니다. 동시 활성 볼륨 수가 권장되는 최대 임계값을 초과하면 중요하지 않은 볼륨 중 일부에서 여기에 나와 있는 지연 시간이 발생합니다.

- * MetroCluster 리소스 *

  MetroCluster 구성에서 클러스터 간 데이터를 미러링하는 데 사용되는 NVRAM 및 ISL(Interswitch Link)을 비롯한 MetroCluster 리소스를 나타냅니다. MetroCluster 구성 요소의 경합이 발생한 경우, 로컬 클러스터의 워크로드로부터 높은 쓰기 처리량을 의미하거나 링크 상태 문제가 로컬 클러스터에 있는 하나 이상의 워크로드 지연 시간에 영향을 줍니다. 클러스터가 MetroCluster 구성에 없으면 이 아이콘이 표시되지 않습니다.

- * 애그리게이트 또는 SSD 애그리게이트 운영 *

  워크로드가 실행되는 스토리지 애그리게이트를 나타냅니다. 애그리게이트 구성 요소의 경합이 발생할 경우, 애그리게이트의 활용률이 높아지면 하나 이상의 워크로드 지연 시간에 영향을 미치게 됩니다. Aggregate는 모든 HDD 또는 HDD와 SSD(Flash Pool 애그리게이트)의 혼합 또는 HDD와 클라우드 계층(FabricPool 애그리게이트)의 혼합 요소로 이루어집니다. 'SSD Aggregate'는 모든 SSD(All-Flash 애그리게이트) 또는 SSD와 클라우드 계층(FabricPool 애그리게이트)의 혼합으로 구성됩니다.

- * 클라우드 지연 시간 *

  클러스터 및 사용자 데이터가 저장되는 클라우드 계층 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 클라우드 지연 시간 구성 요소의 경합이 발생할 경우, 클라우드 계층에서 호스팅되는 볼륨의 대량 읽기가 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

- SnapMirror * 를 동기화합니다

  SnapMirror Synchronous 관계의 기본 볼륨에서 보조 볼륨으로 사용자 데이터를 복제하는 것과 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 동기식 SnapMirror 구성 요소의 경합이 발생한 경우, SnapMirror Synchronous 작업의 활동이 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

성능 이벤트와 관련된 워크로드의 역할

Unified Manager에서는 역할을 사용하여 성능 이벤트에서 워크로드가 어떻게 관여하는지 파악합니다. 희생자, 폭리, 상어 등의 역할을 합니다. 사용자 정의 워크로드는 동시에 피해자이고 괴롭히는 상어가 될 수 있습니다.

역할	설명
피해자	클러스터 구성 요소를 과도하게 사용하는 bullies라는 다른 워크로드로 인해 성능이 저하된 사용자 정의 워크로드 사용자 정의 워크로드만 피해자로 식별됩니다. Unified Manager에서는 지연 시간 편차가 있는 워크로드를 식별하는데, 이 경우 이벤트 중에 실제 지연 시간이 지연 시간 예측(예상 범위)에서 크게 증가했습니다.
괴롭습니다	클러스터 구성 요소를 과도하게 사용하여 피해자라고 하는 다른 워크로드의 성능을 저하시킨 사용자 정의 또는 시스템 정의 워크로드입니다. Unified Manager에서는 클러스터 구성 요소의 사용 편차에 따라 대규모 워크로드를 식별하며, 이벤트 중에는 예상 사용 범위에서 실제 사용량이 크게 증가했습니다.

역할	설명
상어	이벤트에 관여하는 모든 워크로드에 비해 클러스터 구성 요소를 가장 많이 사용하는 사용자 정의 워크로드입니다. Unified Manager에서는 이벤트 중에 클러스터 구성 요소를 사용하여 shark 워크로드를 식별합니다.

클러스터의 워크로드는 네트워크 및 데이터 처리를 위한 애그리게이트 및 CPU와 같은 여러 클러스터 구성 요소를 공유할 수 있습니다. 볼륨과 같은 워크로드가 클러스터 구성 요소의 사용량을 구성 요소가 워크로드 수요를 효율적으로 충족할 수 없는 시점으로 증가하면 구성 요소의 경합이 발생합니다. 클러스터 구성 요소를 과도하게 사용하는 워크로드는 부담스러운 워크로드와 이러한 구성 요소를 공유하며 성능에 큰 영향을 미치는 다른 워크로드는 이 피해자들입니다. 중복 제거 또는 Snapshot 복사본과 같은 시스템 정의 워크로드의 작업도 ""불링""으로 에스컬레이션될 수 있습니다.

Unified Manager에서 이벤트를 감지하면 해당 이벤트를 발생시킨 대규모 워크로드, 경합하는 클러스터 구성 요소, 워크로드가 폭증하여 성능이 저하된 워크로드를 비롯하여 관련된 모든 워크로드와 클러스터 구성 요소를 파악합니다.

Unified Manager에서 대규모 워크로드를 식별할 수 없는 경우 피해자 워크로드와 관련된 클러스터 구성 요소에 대한 알림만 제공됩니다.

Unified Manager를 사용하면 워크로드가 불룩한 경우 이를 식별하고 동일한 워크로드가 불룩한 워크로드가 되는 시기를 파악할 수 있습니다. 워크로드는 그 자체로 부담스러운 것이 될 수 있습니다. 예를 들어, 정책 그룹 제한으로 인해 성능이 높은 워크로드의 임계치가 조절되면 정책 그룹의 모든 워크로드가 그 자체를 포함하여 제한됩니다. 지속적인 성과 이벤트의 피해자 또는 괴롭히는 워크로드는 역할을 변경하거나 더 이상 이벤트에 참가하지 않을 수 있습니다.

성능 임계값 관리

성능 임계값 정책을 사용하면 Unified Manager에서 이벤트를 생성하는 시점을 확인하여 시스템 관리자에게 워크로드 성능에 영향을 줄 수 있는 문제를 알릴 수 있습니다. 이러한 임계값 정책을 _user-defined_performance 임계값이라고 합니다.

이 릴리즈에서는 사용자 정의, 시스템 정의 및 동적 성능 임계값을 지원합니다. Unified Manager는 동적 및 시스템 정의 성능 임계값을 사용하여 워크로드 활동을 분석하여 적절한 임계값을 결정합니다. 사용자 정의 임계값을 사용하면 여러 성능 카운터 및 여러 스토리지 개체에 대한 최대 성능 한도를 정의할 수 있습니다.

시스템 정의 성능 임계값 및 동적 성능 임계값은 Unified Manager에서 설정하며 구성할 수 없습니다. 시스템 정의 성능 임계값 정책에서 불필요한 이벤트를 수신하는 경우 이벤트 설정 페이지에서 개별 정책을 사용하지 않도록 설정할 수 있습니다.

사용자 정의 성능 임계값 정책의 작동 방식

스토리지 오브젝트(예: 애그리게이트 및 볼륨)에 대한 성능 임계값 정책을 설정하여 이벤트를 스토리지 관리자에게 보내 클러스터에 성능 문제가 발생하고 있음을 알릴 수 있습니다.

스토리지 객체에 대한 성능 임계값 정책을 생성하는 방법은 다음과 같습니다.

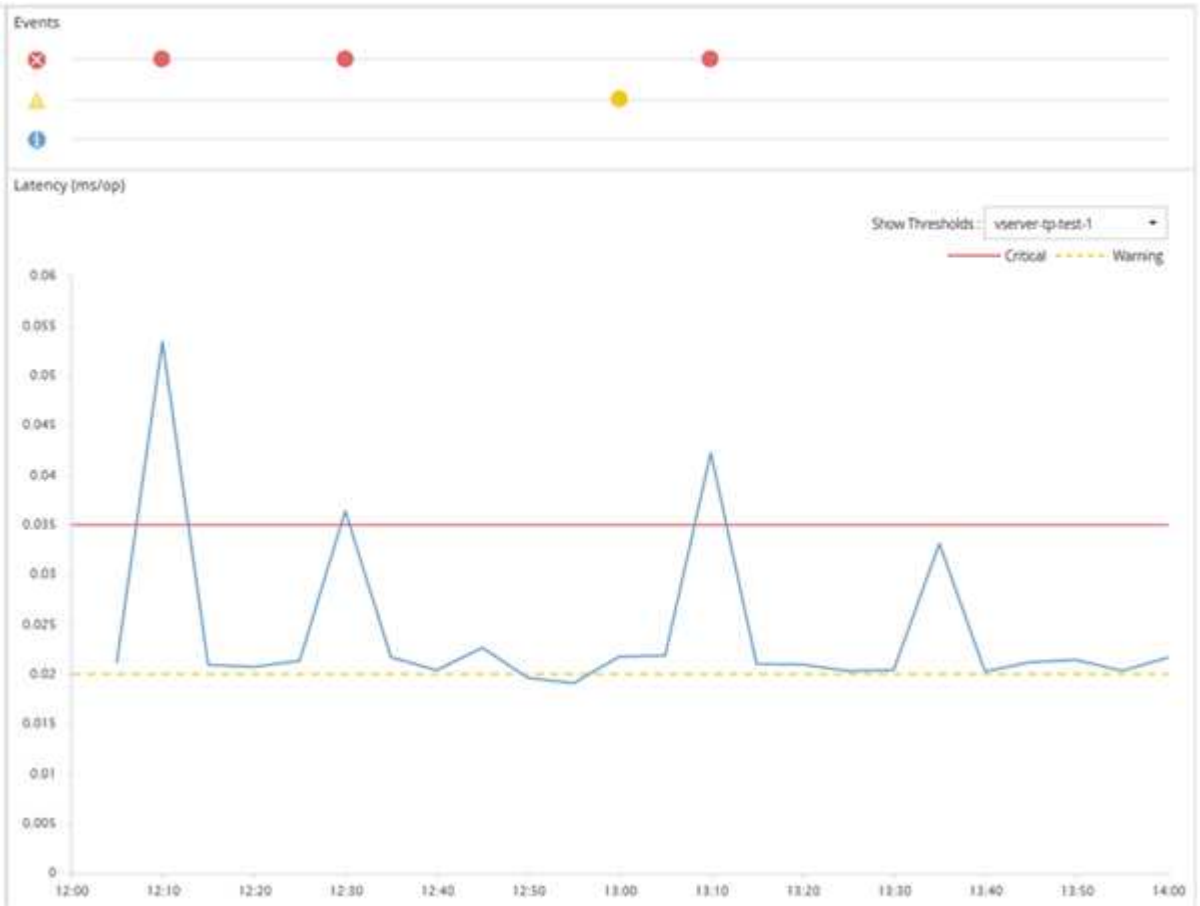
- 스토리지 객체를 선택합니다
- 해당 객체와 연결된 성능 카운터 선택

- 경고 및 심각한 상황으로 간주되는 성능 카운터 상한을 정의하는 값을 지정합니다
- 카운터가 상한을 초과할 기간을 정의하는 기간을 지정합니다

예를 들어, 볼륨에 대한 성능 임계값 정책을 설정하여 해당 볼륨에 대한 IOPS가 10분 동안 초당 750작업을 초과할 때마다 중요한 이벤트 알림을 받을 수 있습니다. 이 동일한 임계값 정책은 IOPS가 10분 동안 초당 500개 작업을 초과할 때 경고 이벤트를 보내도록 지정할 수도 있습니다.

현재 릴리즈에서는 카운터 값이 임계값 설정을 초과할 때 이벤트를 전송하는 임계값을 제공합니다. 카운터 값이 임계값 설정 아래로 떨어지면 이벤트를 전송하는 임계값을 설정할 수 없습니다.

여기에 표시된 카운터 차트 예는 경고 임계값(노란색 아이콘)이 1:00에 위반되었으며 중요 임계값(빨간색 아이콘)이 12:10, 12:30 및 1:10에 위반되었음을 나타냅니다.



임계값 위반은 지정된 기간 동안 연속적으로 발생해야 합니다. 어떤 이유로든 임계값이 제한 값 아래로 떨어지면 후속 위반은 새로운 기간의 시작으로 간주됩니다.

일부 클러스터 개체와 성능 카운터를 사용하면 이벤트가 생성되기 전에 두 개의 성능 카운터가 최대 제한을 초과하도록 하는 조합 임계값 정책을 만들 수 있습니다. 예를 들어, 다음 기준을 사용하여 임계값 정책을 생성할 수 있습니다.

클러스터 객체	성능 카운터	경고 임계값	위험 임계값	기간
볼륨	지연 시간	10밀리초	20밀리초	15분
집계	활용률	65%	85%	

두 클러스터 객체를 사용하는 임계값 정책은 두 조건이 모두 위반된 경우에만 이벤트가 생성됩니다. 예를 들어 표에 정의된 임계값 정책을 사용할 수 있습니다.

볼륨 지연 시간이 평균인 경우...	그리고 애그리게이트 디스크 활용률은...	그러면...
15밀리초	50%	보고된 이벤트가 없습니다.
15밀리초	75%	경고 이벤트가 보고됩니다.
25밀리초	75%	경고 이벤트가 보고됩니다.
25밀리초	90%	긴급 이벤트가 보고됩니다.

성능 임계값 정책이 위반될 경우 발생하는 현상

기간에 지정된 시간 동안 카운터 값이 정의된 성능 임계값을 초과하면 임계값이 위반되고 이벤트가 보고됩니다.

이 이벤트로 인해 다음 작업이 시작됩니다.

- 이벤트는 대시보드, 성능 클러스터 요약 페이지, 이벤트 페이지 및 개체별 성능 인벤토리 페이지에 표시됩니다.
- (선택 사항) 이벤트에 대한 e-메일 알림을 하나 이상의 e-메일 수신자에게 보낼 수 있으며 SNMP 트랩을 트랩 수신기로 보낼 수 있습니다.
- (선택 사항) 스토리지 객체를 자동으로 수정 또는 업데이트하기 위해 스크립트를 실행할 수 있습니다.

첫 번째 작업은 항상 실행됩니다. 경고 설정 페이지에서 옵션 작업을 수행할지 여부를 구성합니다. 경고 또는 위험 임계값 정책이 위반되는지 여부에 따라 고유한 작업을 정의할 수 있습니다.

스토리지 객체에 대한 성능 임계값 정책 위반이 발생한 후 카운터 값이 임계값 아래로 떨어질 때까지 해당 정책에 대해 더 이상 이벤트가 생성되지 않으며, 이때 해당 제한에 대한 기간이 재설정됩니다. 임계값이 계속 초과되는 동안 이벤트의 종료 시간은 지속적으로 업데이트되어 이 이벤트가 진행 중인 것을 반영합니다.

임계값 이벤트는 심각도 및 정책 정의와 관련된 정보를 캡처하거나 중지하여 나중에 임계값 정책이 수정되더라도 이벤트와 함께 고유한 임계값 정보가 표시되도록 합니다.

임계값을 사용하여 추적할 수 있는 성능 카운터

IOPS 및 MB/s와 같은 일부 일반적인 성능 카운터는 모든 스토리지 개체에 대해 임계값을 설정할 수 있습니다. 특정 스토리지 객체에 대해서만 임계값을 설정할 수 있는 다른 카운터가 있습니다.

사용 가능한 성능 카운터

스토리지 객체	성능 카운터	설명
클러스터	IOPS	클러스터에서 초당 처리하는 평균 입출력 작업 수입니다.

스토리지 객체	성능 카운터	설명
MB/s	이 클러스터와 초당 전송된 평균 데이터 크기(MB)입니다.	노드
IOPS	노드가 초당 처리하는 평균 입출력 작업 수입니다.	MB/s
이 노드와 초당 전송된 평균 데이터 크기(MB)입니다.	지연 시간	노드가 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.
활용률	사용 중인 노드의 CPU 및 RAM의 평균 백분율입니다.	사용된 성능 용량
노드에서 사용 중인 성능 용량의 평균 백분율입니다.	사용된 성능 용량 - 테이크오버입니다	노드에서 사용 중인 성능 용량과 파트너 노드의 성능 용량에 대한 평균 비율입니다.
집계	IOPS	초당 집계 프로세스가 수행하는 평균 입출력 작업 수입니다.
MB/s	이 애그리게이트로부터 초당 전송되는 평균 데이터 크기(MB)입니다.	지연 시간
집계가 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.	활용률	사용 중인 애그리게이트 디스크의 평균 백분율입니다.
사용된 성능 용량	애그리게이트에서 사용 중인 성능 용량의 평균 백분율입니다.	스토리지 VM
IOPS	SVM 프로세스가 초당 수행하는 평균 입출력 작업 수입니다.	MB/s
이 SVM과 초당 전송된 평균 데이터 크기(MB)입니다.	지연 시간	SVM이 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)
볼륨	IOPS	볼륨 프로세스가 초당 처리하는 평균 입출력 작업 수입니다.
MB/s	이 볼륨으로부터 초당 전송된 평균 데이터 크기(MB)입니다.	지연 시간
볼륨이 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.	캐시 비적중 비율입니다	캐시에서 반환되지 않고 볼륨에서 반환되는 클라이언트 애플리케이션의 읽기 요청 평균 비율입니다.

스토리지 객체	성능 카운터	설명
LUN을 클릭합니다	IOPS	LUN이 초당 처리하는 평균 입출력 작업 수입니다.
MB/s	이 LUN과 초당 전송된 평균 데이터 크기(MB)입니다.	지연 시간
LUN이 애플리케이션 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.	네임스페이스	IOPS
네임스페이스 프로세스가 초당 처리하는 평균 입출력 작업 수입니다.	MB/s	이 네임스페이스에서 초당 전송된 평균 데이터 크기(MB)입니다.
지연 시간	네임스페이스가 응용 프로그램 요청에 응답하는 데 걸리는 평균 시간(밀리초)입니다.	포트
대역폭 사용률	사용 중인 포트의 가용 대역폭에 대한 평균 백분율입니다.	MB/s
이 포트와 초당 전송된 평균 데이터 크기(MB)입니다.	네트워크 인터페이스(LIF)	MB/s

조합 임계값 정책에 사용할 수 있는 개체 및 카운터

일부 성능 카운터만 조합 정책에서 함께 사용할 수 있습니다. 기본 및 보조 성능 카운터를 지정할 때 두 성능 카운터는 모두 이벤트가 생성되기 전에 최대 제한을 초과해야 합니다.

운영 스토리지 오브젝트 및 카운터	**2**차 스토리지 오브젝트 및 카운터
볼륨 지연 시간	볼륨 IOPS
볼륨 MB/s	애그리게이트 활용률
사용된 총 성능 용량	노드 활용률
사용된 노드 성능 용량입니다	사용된 노드 성능 용량 - 테이크오버입니다
LUN 지연 시간	LUN IOPS입니다
LUN MB/s	애그리게이트 활용률
사용된 총 성능 용량	노드 활용률

운영 스토리지 오브젝트 및 카운터	2차 스토리지 오브젝트 및 카운터
사용된 노드 성능 용량입니다	사용된 노드 성능 용량 - 테이크오버입니다

볼륨 조합 정책이 FlexVol 볼륨 대신 FlexGroup 볼륨에 적용되는 경우 ""볼륨 IOPS"" 및 ""볼륨 MB/s"" 속성만 보조 카운터로 선택할 수 있습니다. 임계값 정책에 노드 또는 애그리게이트 특성 중 하나가 포함된 경우 정책이 FlexGroup 볼륨에 적용되지 않으며 이 사례를 설명하는 오류 메시지가 표시됩니다. 그 이유는 FlexGroup 볼륨이 둘 이상의 노드 또는 애그리게이트에 있을 수 있기 때문입니다.

사용자 정의 성능 임계값 정책 생성

성능 카운터가 특정 값을 초과할 때 알림이 전송되도록 스토리지 객체에 대한 성능 임계값 정책을 생성합니다. 이벤트 알림에서 클러스터에 성능 문제가 발생한 것을 확인할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

성능 임계값 정책 생성 페이지에서 임계값을 입력하여 성능 임계값 정책을 생성합니다. 이 페이지의 모든 정책 값을 정의하여 새 정책을 생성하거나 기존 정책의 복사본을 만들고 복사본의 값(*cloning*)을 변경할 수 있습니다.

유효한 임계값은 숫자로 0.001에서 10,000,000 사이, 백분율의 경우 0.001에서 100 사이, 사용된 성능 용량의 백분율 값은 0.001에서 200 사이입니다.

현재 릴리즈에서는 카운터 값이 임계값 설정을 초과할 때 이벤트를 전송하는 임계값을 제공합니다. 카운터 값이 임계값 설정 아래로 떨어지면 이벤트를 전송하는 임계값을 설정할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 임계값 * > * 성능 * 을 선택합니다.

   성능 임계값 페이지가 표시됩니다.

2. 새 정책을 구축할지 또는 비슷한 정책을 클론 복제하고 클론 복제된 버전을 수정할지 여부에 따라 적절한 버튼을 클릭합니다.

대상...	클릭...
새 정책을 생성합니다	• 생성 *
기존 정책의 클론을 생성합니다	기존 정책을 선택하고 * Clone * 을 클릭합니다

   성능 임계값 정책 생성 페이지 또는 성능 임계값 정책 복제 페이지가 표시됩니다.

3. 특정 스토리지 개체에 설정할 성능 카운터 임계값을 지정하여 임계값 정책을 정의합니다.

   a. 스토리지 객체 유형을 선택하고 정책의 이름과 설명을 지정합니다.

   b. 추적할 성능 카운터를 선택하고 Warning 및 Critical 이벤트를 정의하는 제한 값을 지정합니다.

최소한 하나의 경고 또는 하나의 위험 한도를 정의해야 합니다. 두 가지 제한 유형을 모두 정의할 필요는 없습니다.

c. 필요한 경우 보조 성능 카운터를 선택하고 Warning 및 Critical 이벤트에 대한 제한 값을 지정합니다.

보조 카운터를 포함하면 두 카운터가 모두 임계값을 위반하고 이벤트가 보고되기 전에 제한 값을 초과해야 합니다. 조합 정책을 사용하여 특정 개체 및 카운터만 구성할 수 있습니다.

d. 이벤트를 전송하기 위해 제한 값을 위반해야 하는 기간을 선택합니다.

기존 정책을 복제할 때 정책의 새 이름을 입력해야 합니다.

4. 저장 * 을 클릭하여 정책을 저장합니다.

성능 임계값 페이지로 돌아갑니다. 페이지 맨 위에 있는 성공 메시지는 임계값 정책이 생성되었음을 확인하고 스토리지 개체에 새 정책을 즉시 적용할 수 있도록 해당 개체 유형에 대한 인벤토리 페이지에 대한 링크를 제공합니다.

현재 스토리지 객체에 새 임계값 정책을 적용하려면 * Go to object_type now * 링크를 클릭하여 인벤토리 페이지로 이동할 수 있습니다.

스토리지 객체에 성능 임계값 정책 할당

성능 카운터 값이 정책 설정을 초과할 경우 Unified Manager에서 이벤트를 보고하도록 스토리지 개체에 사용자 정의 성능 임계값 정책을 할당합니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

객체에 적용할 성능 임계값 정책 또는 정책이 있어야 합니다.

개체 또는 개체 그룹에 한 번에 하나의 성능 정책만 적용할 수 있습니다.

각 스토리지 개체에 최대 3개의 임계값 정책을 할당할 수 있습니다. 여러 개체에 정책을 할당할 때 개체에 이미 최대 개수의 정책이 할당된 경우 Unified Manager에서 다음 작업을 수행합니다.

- 최대 값에 도달하지 않은 선택한 모든 개체에 정책을 적용합니다
- 최대 정책 수에 도달한 객체를 무시합니다
- 정책이 모든 개체에 할당되지 않았다는 메시지를 표시합니다

단계

1. 스토리지 개체의 성능 인벤토리 페이지에서 임계값 정책을 할당할 개체를 선택합니다.

임계값을 할당하려면...	클릭...
단일 개체입니다	해당 개체의 왼쪽에 있는 확인란.
여러 개의 개체	각 개체의 왼쪽에 있는 확인란.

임계값을 할당하려면...	클릭...
페이지의 모든 개체	를 클릭합니다 ☐▾ 드롭다운 상자에서 * 이 페이지의 모든 개체 선택 * 을 선택합니다.
동일한 유형의 모든 개체	를 클릭합니다 ☐▾ 드롭다운 상자에서 * 모든 개체 선택 * 을 선택합니다.

정렬 및 필터링 기능을 사용하여 인벤토리 페이지의 개체 목록을 구체화하여 여러 개체에 임계값 정책을 쉽게 적용할 수 있습니다.

2. 선택한 다음 * 성능 임계값 정책 할당 * 을 클릭합니다.

   성능 임계값 정책 할당 페이지가 표시되어 해당 특정 유형의 스토리지 오브젝트에 대한 임계값 정책 목록을 보여 줍니다.

3. 각 정책을 클릭하여 성능 임계값 설정에 대한 세부 정보를 표시하여 올바른 임계값 정책을 선택했는지 확인합니다.
4. 적절한 임계값 정책을 선택한 후 * 정책 할당 * 을 클릭합니다.

   페이지 맨 위에 있는 성공 메시지는 임계값 정책이 개체 또는 개체에 할당되었음을 확인하고 이 개체 및 정책에 대한 경고 설정을 구성할 수 있도록 경고 페이지에 대한 링크를 제공합니다.

특정 성능 이벤트가 생성되었음을 알리기 위해 e-메일을 통해 또는 SNMP 트랩으로 알림을 보내려면 경고 설정 페이지에서 경고 설정을 구성해야 합니다.

성능 임계값 정책 보기

성능 임계값 페이지에서 현재 정의된 모든 성능 임계값 정책을 볼 수 있습니다.

임계값 정책 목록은 정책 이름을 기준으로 사전순으로 정렬되며 모든 유형의 스토리지 객체에 대한 정책이 포함됩니다. 열 머리글을 클릭하여 해당 열을 기준으로 정책을 정렬할 수 있습니다. 특정 정책을 찾고 있는 경우 필터 및 검색 메커니즘을 사용하여 인벤토리 목록에 나타나는 임계값 정책 목록을 구체화합니다.

정책 이름 및 조건 이름 위에 커서를 놓으면 정책의 구성 세부 정보를 볼 수 있습니다. 또한 제공된 버튼을 사용하여 사용자 정의 임계값 정책을 생성, 클론 복제, 편집 및 삭제할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 임계값 * > * 성능 * 을 선택합니다.

   성능 임계값 페이지가 표시됩니다.

사용자 정의 성능 임계값 정책 편집

기존 성능 임계값 정책에 대한 임계값 설정을 편집할 수 있습니다. 이 기능은 특정 임계값 조건에 대해 너무 많거나 적은 경고를 수신하는 경우 유용할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

기존 임계값 정책에 대해 모니터링되는 스토리지 개체의 유형이나 정책 이름은 변경할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 임계값 * > * 성능 * 을 선택합니다.

   성능 임계값 페이지가 표시됩니다.

2. 변경할 임계값 정책을 선택하고 * 편집 * 을 클릭합니다.

   성능 임계값 정책 편집 페이지가 표시됩니다.

3. 임계값 정책을 변경하고 * Save * 를 클릭합니다.

   성능 임계값 페이지로 돌아갑니다.

변경 사항은 저장되면 정책을 사용하는 모든 스토리지 객체에서 즉시 업데이트됩니다.

정책의 변경 유형에 따라 경고 설정 페이지의 정책을 사용하는 개체에 대해 구성된 알림 설정을 검토할 수 있습니다.

스토리지 개체에서 성능 임계값 정책 제거

Unified Manager에서 성능 카운터 값을 더 이상 모니터링하지 않으려는 경우 스토리지 개체에서 사용자 정의 성능 임계값 정책을 제거할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

선택한 개체에서 한 번에 하나의 정책만 제거할 수 있습니다.

목록에서 둘 이상의 개체를 선택하여 여러 스토리지 개체에서 임계값 정책을 제거할 수 있습니다.

단계

1. 스토리지 객체의 * inventory * 페이지에서 성능 임계값 정책이 하나 이상 적용된 객체를 하나 이상 선택합니다.

임계값을 지우려면...	수행할 작업...
단일 개체입니다	해당 개체의 왼쪽에 있는 확인란을 선택합니다.
여러 개의 개체	각 개체의 왼쪽에 있는 확인란을 선택합니다.
페이지의 모든 개체	을 클릭합니다 열 머리글에 표시됩니다.

2. 성능 임계값 정책 지우기 * 를 클릭합니다.

   Clear Threshold Policy(임계값 정책 지우기) 페이지가 표시되며, 이 페이지에는 스토리지 객체에 현재 할당된 임계값 정책 목록이 표시됩니다.

3. 개체에서 제거할 임계값 정책을 선택하고 * 정책 지우기 * 를 클릭합니다.

   임계값 정책을 선택하면 해당 정책을 선택했는지 확인할 수 있도록 정책의 세부 정보가 표시됩니다.

성능 임계값 정책이 변경되면 어떻게 됩니까

기존 성능 임계값 정책의 카운터 값 또는 기간을 조정하면 정책 변경 사항이 정책을 사용하는 모든 스토리지 개체에 적용됩니다. 새로운 설정이 즉시 적용되어 Unified Manager에서 새로 수집된 모든 성능 데이터에 대한 성능 카운터 값과 새 임계값 설정을 비교하기 시작합니다.

변경된 임계값 정책을 사용하는 객체에 대해 활성화된 이벤트가 있는 경우 해당 이벤트는 폐기된 것으로 표시되고 임계값 정책은 카운터를 새로 정의된 임계값 정책으로 모니터링하기 시작합니다.

Counter Charts Detailed View에서 임계값이 적용된 카운터를 볼 때 위험 및 경고 임계값 선은 현재 임계값 설정을 반영합니다. 이전 임계값 설정이 적용되었을 때 기록 데이터를 보는 경우에도 이 페이지에는 원래 임계값 설정이 나타나지 않습니다.

이전 임계값 설정이 Counter Charts Detailed View에 나타나지 않기 때문에 현재 임계값 라인 아래에 나타나는 기록 이벤트를 볼 수 있습니다.

오브젝트를 이동할 때 성능 임계값 정책이 어떻게 되는지 확인합니다

성능 임계값 정책은 스토리지 개체에 할당되므로 개체를 이동할 경우 이동을 완료한 후에도 할당된 모든 임계값 정책이 개체에 연결된 상태로 유지됩니다. 예를 들어, 볼륨 또는 LUN을 다른 애그리게이트로 이동하는 경우 임계값 정책은 새 애그리게이트에 있는 볼륨 또는 LUN에 대해 여전히 활성 상태입니다.

임계값 정책에 대한 보조 카운터 조건이 있는 경우(예: 결합 정책) - 예를 들어 aggregate 또는 노드에 추가 조건이 할당된 경우 - 보조 카운터 조건이 볼륨 또는 LUN이 이동된 새 Aggregate 또는 노드에 적용됩니다.

변경된 임계값 정책을 사용하는 객체에 대해 새 활성 이벤트가 존재하는 경우 해당 이벤트는 폐기된 것으로 표시되고 임계값 정책은 카운터를 새로 정의된 임계값 정책으로 모니터링하기 시작합니다.

볼륨 이동 작업을 수행하면 ONTAP에서 정보 변경 이벤트를 보냅니다. 성능 탐색기 페이지의 이벤트 타임라인과 워크로드 분석 페이지에 변경 이벤트 아이콘이 표시되어 이동 작업이 완료된 시간을 나타냅니다.

개체를 다른 클러스터로 이동하는 경우 사용자 정의 임계값 정책이 개체에서 제거됩니다. 필요한 경우 이동 작업이 완료된 후 개체에 임계값 정책을 할당해야 합니다. 그러나 동적 및 시스템 정의 임계값 정책은 새 클러스터로 이동된 후 개체에 자동으로 적용됩니다.

HA 테이크오버 및 반환 중 임계값 정책 기능

고가용성(HA) 구성에서 테이크오버 또는 반환 작업이 발생하는 경우 한 노드에서 다른 노드로 이동된 객체는 수동 이동 작업과 동일한 방식으로 임계값 정책을 유지합니다. Unified Manager에서는 15분마다 클러스터 구성의 변경 사항을 확인하기 때문에, 클러스터 구성을 다음에 폴링할 때까지 새 노드로 전환할 때 미치는 영향이 식별되지 않습니다.

테이크오버와 반환 작업이 15분 구성 변경 수집 기간 내에 발생하는 경우 성능 통계가 한 노드에서 다른 노드로 이동하지 않는 것을 확인할 수 있습니다.

애그리게이트 재배치 중 임계값 정책 기능

'Aggregate relocation start' 명령을 사용하여 하나의 노드에서 다른 노드로 애그리게이트를 이동하는 경우 단일 임계값 정책과 조합 임계값 정책이 모든 객체에 유지되고 임계값 정책의 노드 부분이 새 노드에 적용됩니다.

MetroCluster 절체 시 **Threshold** 정책 기능

MetroCluster 구성에서 클러스터 간에 이동하는 오브젝트에는 사용자 정의 임계값 정책 설정이 유지되지 않습니다. 필요한 경우 파트너 클러스터로 이동한 볼륨 및 LUN에 임계값 정책을 적용할 수 있습니다. 오브젝트가 원래 클러스터로 다시 이동되면 사용자 정의 임계값 정책이 자동으로 다시 적용됩니다.

자세한 내용은 을 참조하십시오 "스위치오버 및 스위치백 중 볼륨 동작".

성능 이벤트 분석

성능 이벤트를 분석하여 감지된 시기, 활성 상태(신규 또는 확인됨) 또는 폐기 여부, 관련 워크로드 및 클러스터 구성 요소, 이벤트를 자체적으로 해결하는 옵션을 파악할 수 있습니다.

성능 이벤트에 대한 정보 표시

이벤트 관리 인벤토리 페이지를 사용하여 Unified Manager에서 모니터링하는 클러스터의 모든 성능 이벤트 목록을 볼 수 있습니다. 이 정보를 보면 가장 중요한 이벤트를 확인한 다음 세부 정보로 드릴다운하여 이벤트의 원인을 확인할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트 목록은 감지된 시간에 따라 정렬되며 가장 최근의 이벤트가 먼저 나열됩니다. 열 머리글을 클릭하여 해당 열을 기준으로 이벤트를 정렬할 수 있습니다. 예를 들어, 상태 열을 기준으로 정렬하여 심각도별로 이벤트를 볼 수 있습니다. 특정 이벤트 또는 특정 유형의 이벤트를 찾는 경우 필터 및 검색 메커니즘을 사용하여 목록에 나타나는 이벤트 목록을 구체화할 수 있습니다.

모든 소스의 이벤트가 이 페이지에 표시됩니다.

- 사용자 정의 성능 임계값 정책
- 시스템 정의 성능 임계값 정책
- 동적 성능 임계값

이벤트 유형 열에는 이벤트의 소스가 나열됩니다. 이벤트를 선택하여 이벤트 세부 정보 페이지에서 이벤트에 대한 세부 정보를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.
2. 보기 메뉴에서 * 활성 성능 이벤트 * 를 선택합니다.

   이 페이지에는 지난 7일 동안 생성된 모든 New 및 Acknowledged Performance 이벤트가 표시됩니다.

3. 분석할 이벤트를 찾아 이벤트 이름을 클릭합니다.

이벤트에 대한 세부 정보 페이지가 표시됩니다.

> 또한 성능 탐색기 페이지 및 경고 전자 메일에서 이벤트 이름 링크를 클릭하여 이벤트의 세부 정보 페이지를 표시할 수도 있습니다.

사용자 정의 성능 임계값의 이벤트 분석

사용자 정의 임계값에서 생성된 이벤트는 집계 또는 볼륨과 같은 특정 스토리지 개체의 성능 카운터가 정책에 정의된 임계값을 초과했음을 나타냅니다. 이는 클러스터 개체에 성능 문제가 발생했음을 나타냅니다.

이벤트 세부 정보 페이지를 사용하여 성능 이벤트를 분석하고 필요한 경우 수정 조치를 취하여 성능을 정상 상태로 되돌릴 수 있습니다.

사용자 정의 성능 임계값 이벤트에 응답

Unified Manager를 사용하면 성능 카운터가 사용자 정의 경고 또는 중요 임계값을 초과하여 성능 이벤트를 조사할 수 있습니다. Unified Manager를 사용하여 클러스터 구성 요소의 상태를 검사하여 구성 요소에서 감지된 최근 상태 이벤트가 성능 이벤트에 기여했는지 확인할 수도 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새 성능 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 이벤트를 발생시킨 임계값 위반을 설명하는 * Description * 을 검토합니다.

   예를 들어 "'456 ms/op의 지연 시간 값이 400 ms/op의 임계값 설정에 따라 경고 이벤트를 트리거했습니다' 메시지는 객체에 대한 지연 경고 이벤트가 발생했음을 나타냅니다.

3. 정책 이름 위에 커서를 올려 놓으면 이벤트를 트리거한 임계값 정책에 대한 세부 정보가 표시됩니다.

   여기에는 정책 이름, 평가 중인 성능 카운터, 중요 이벤트 또는 경고 이벤트로 간주하기 위해 위반되어야 하는 카운터 값, 카운터가 값을 초과해야 하는 기간이 포함됩니다.

4. 이벤트 트리거 시간 * 을 메모하여 이 이벤트에 영향을 줄 수 있는 다른 이벤트가 동시에 발생했는지 여부를 조사할 수 있습니다.
5. 아래 옵션 중 하나를 따라 이벤트를 추가로 조사하여 성능 문제를 해결하기 위해 조치를 수행해야 하는지 여부를 확인합니다.

옵션을 선택합니다	가능한 조사 조치
원본 개체 이름을 클릭하여 해당 개체의 탐색기 페이지를 표시합니다.	이 페이지에서는 오브젝트 세부 정보를 확인하고 이 오브젝트를 다른 유사한 스토리지 오브젝트와 비교하여 다른 스토리지 오브젝트의 성능 문제가 동시에 있는지 확인할 수 있습니다. 예를 들어, 같은 애그리게이트의 다른 볼륨에도 성능 문제가 있는지 확인합니다.
클러스터 이름을 클릭하여 클러스터 요약 페이지를 표시합니다.	이 페이지에서는 이 객체가 상주하는 클러스터에 대한 세부 정보를 볼 수 있어 다른 성능 문제가 동시에 발생했는지 여부를 확인할 수 있습니다.

시스템 정의 성능 임계값에서 이벤트 분석

시스템 정의 성능 임계값에서 생성된 이벤트는 특정 스토리지 개체의 성능 카운터 또는 성능 카운터 집합이 시스템 정의 정책의 임계값을 초과했음을 나타냅니다. 이는 Aggregate 또는 노드와 같은 스토리지 개체에 성능 문제가 있음을 나타냅니다.

이벤트 세부 정보 페이지를 사용하여 성능 이벤트를 분석하고 필요한 경우 수정 조치를 취하여 성능을 정상 상태로 되돌릴 수 있습니다.

Cloud Volumes ONTAP, ONTAP Edge 또는 ONTAP Select 시스템에서는 시스템 정의 임계값 정책이 사용되지 않습니다.

시스템 정의 성능 임계값 이벤트에 응답

Unified Manager를 사용하면 성능 카운터가 시스템 정의 경고 임계값을 초과하여 성능 이벤트로 인해 발생한 성능 이벤트를 조사할 수 있습니다. Unified Manager를 사용하여 클러스터 구성 요소의 상태를 점검하여 구성 요소에서 감지된 최근 이벤트가 성능 이벤트에 기여했는지 확인할 수도 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새 성능 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 이벤트를 발생시킨 임계값 위반을 설명하는 * Description * 을 검토합니다.

   예를 들어 "'노드 사용률 값 90%가 임계값 설정인 85%를 기반으로 경고 이벤트를 트리거했습니다' 메시지는 클러스터 객체에 대한 노드 사용률 경고 이벤트가 발생했음을 나타냅니다.

3. 이벤트 트리거 시간 * 을 메모하여 이 이벤트에 영향을 줄 수 있는 다른 이벤트가 동시에 발생했는지 여부를 조사할 수 있습니다.
4. 시스템 진단 * 에서 시스템 정의 정책이 클러스터 개체에 대해 수행하는 분석 유형에 대한 간략한 설명을 검토합니다.

일부 이벤트의 경우 진단 옆에 녹색 또는 빨간색 아이콘이 표시되어 특정 진단에서 문제가 발견되었는지 여부를 나타냅니다. 다른 형식의 시스템 정의 이벤트 카운터 차트에는 개체의 성능이 표시됩니다.

5. [권장 조치] * 에서 [이 일을 하도록 도와주세요 *] 링크를 클릭하여 성능 이벤트를 직접 해결 및 시도하기 위해 수행할 수 있는 권장 조치를 확인하십시오.

QoS 정책 그룹 성능 이벤트에 응답

Unified Manager는 워크로드 처리량(IOPS, IOPS/TB 또는 MBps)이 정의된 ONTAP QoS 정책 설정을 초과하고 워크로드 지연 시간에 영향을 미칠 경우 QoS 정책 경고 이벤트를 생성합니다. 많은 워크로드가 지연 시간의 영향을 받기 전에 이러한 시스템 정의 이벤트를 통해 잠재적 성능 문제를 해결할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성능 이벤트, 확인된 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.

Unified Manager는 이전 시간의 각 성능 수집 기간 동안 워크로드 처리량이 정의된 QoS 정책 설정을 초과할 경우 QoS 정책 위반에 대한 경고 이벤트를 생성합니다. 각 수집 기간 동안 짧은 기간 동안만 워크로드 처리 성능이 QoS 임계값을 초과할 수 있지만 Unified Manager에서는 차트에 수집 기간 동안 ""평균"" 처리량만 표시합니다. 따라서 워크로드의 처리량이 차트에 표시된 정책 임계값을 넘을 수 없는 경우 QoS 이벤트가 발생할 수 있습니다.

System Manager 또는 ONTAP 명령을 사용하여 다음 작업을 비롯한 정책 그룹을 관리할 수 있습니다.

- 워크로드에 대한 새 정책 그룹 생성
- 정책 그룹에서 워크로드 추가 또는 제거
- 정책 그룹 간에 워크로드 이동
- 정책 그룹의 처리량 제한을 변경합니다
- 워크로드를 다른 Aggregate 또는 노드로 이동

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 이벤트를 발생시킨 임계값 위반을 설명하는 * Description * 을 검토합니다.

   예를 들어 ""vol1_NFS1에서 1,352 IOPS의 IOPS 값이 경고 이벤트를 트리거하여 워크로드에 대한 잠재적인 성능 문제를 식별했습니다." 메시지는 볼륨 vol1_NFS1에서 QoS Max IOPS 이벤트가 발생했음을 나타냅니다.

3. 이벤트 발생 시기 및 이벤트 활성 기간에 대한 자세한 내용은 * 이벤트 정보 * 섹션을 참조하십시오.

   또한 QoS 정책의 처리량을 공유하는 볼륨 또는 LUN의 경우 가장 높은 IOPS 또는 MBPS를 소비하는 상위 3개 워크로드의 이름을 확인할 수 있습니다.

4. System Diagnosis * 섹션에서 총 평균 IOPS 또는 MBps(이벤트에 따라 다름)에 대한 차트와 지연 시간에 대한 차트의 두 차트를 검토합니다. 이렇게 정렬하면 워크로드가 QoS 최대 제한에 근접했을 때 지연 시간에 가장 영향을 미치는 클러스터 구성 요소를 확인할 수 있습니다.

   공유 QoS 정책 이벤트의 경우 처리량 차트에 상위 3개 워크로드가 표시됩니다. QoS 정책을 공유하는 워크로드가 3개 이상이면 추가 워크로드가 ""기타 워크로드" 범주에 추가됩니다. 또한 지연 시간 차트에는 QoS 정책에 포함되는

모든 워크로드의 평균 지연 시간이 표시됩니다.

적응형 QoS 정책 이벤트의 경우 IOPS 및 MBPS 차트는 볼륨 크기에 따라 ONTAP이 할당된 IOPS/TB 임계값 정책에서 변환한 IOPS 또는 MBPS 값을 표시합니다.

5. 제안 조치 * 섹션에서 제안 사항을 검토하고 작업 부하 대기 시간의 증가를 방지하기 위해 수행해야 할 조치를 결정합니다.

   필요한 경우 * 도움말 * 버튼을 클릭하여 성능 이벤트 해결을 위해 수행할 수 있는 권장 조치에 대한 자세한 내용을 확인하십시오.

블록 크기가 정의된 적응형 **QoS** 정책의 이벤트 이해

적응형 QoS 정책 그룹은 볼륨 크기에 따라 처리량 상한 또는 하한 을 자동으로 확장하며, 볼륨 크기에 따라 IOPS와 TB의 비율을 유지합니다. ONTAP 9.5부터 QoS 정책에 블록 크기를 지정하여 MB/s 임계값을 동시에 효과적으로 적용할 수 있습니다.

적응형 QoS 정책에 IOPS 임계값을 할당하면 각 워크로드에서 발생하는 작업 수만 제한됩니다. 워크로드를 생성하는 클라이언트에 설정된 블록 크기에 따라 일부 IOPS에는 훨씬 더 많은 데이터가 포함되므로 작업을 처리하는 노드에 부담이 훨씬 커집니다.

워크로드에 대한 MB/s 값은 다음 공식을 사용하여 생성됩니다.

```
MB/s = (IOPS * Block Size) / 1000
```

워크로드가 평균 3,000 IOPS이고 클라이언트의 블록 크기가 32KB로 설정된 경우 이 워크로드에 대한 유효 MB/s는 96입니다. 이 동일한 워크로드가 평균 3,000 IOPS이고 클라이언트의 블록 크기가 48KB로 설정된 경우 이 워크로드에 대한 유효 MB/s는 144입니다. 블록 크기가 클 경우 노드가 50% 더 많은 데이터를 처리하고 있음을 알 수 있습니다.

블록 크기가 정의된 다음 적응형 QoS 정책과 클라이언트에서 설정된 블록 크기를 기반으로 이벤트가 트리거되는 방식을 살펴보겠습니다.

정책을 생성하고 블록 크기 32KB로 최대 처리량을 2,500 IOPS/TB로 설정합니다. 이 경우 사용된 용량이 1TB인 볼륨의 경우 MB/s 임계값을 80MB/s(2500 IOPS * 32KB)/1000으로 효과적으로 설정합니다. 처리량 값이 정의된 임계값보다 10% 작은 경우 Unified Manager에서 경고 이벤트를 생성합니다. 이벤트는 다음과 같은 상황에서 생성됩니다.

사용된 용량	처리량이 이 수를 초과하면 이벤트가 생성됩니다.	
	IOPS	MB/s
1TB	2,250 IOPS	72MB/s
2TB입니다	4,500IOPS	144MB/s
5TB	11,250 IOPS	360MB/s

볼륨에서 2TB의 사용 가능한 공간을 사용하고 IOPS가 4,000이고 클라이언트에서 QoS 블록 크기가 32KB로 설정된 경우 MB/PS 처리량은 128Mb/s(4,000IOPS * 32KB)/1000입니다. 이 시나리오에서는 2TB의 공간을 사용하는 볼륨의

임계값 미만에서 4,000 IOPS와 128 MB/s가 모두 사용되기 때문에 이벤트가 생성되지 않습니다.

볼륨에서 2TB의 사용 가능한 공간을 사용하고 IOPS가 4,000이고 클라이언트에서 QoS 블록 크기가 64KB로 설정된 경우 MB/s 처리량은 256MB/s(4,000IOPS * 64KB)/1000입니다. 이 경우 4,000 IOPS가 이벤트를 생성하지 않지만 256MB/s의 값이 144MB/s의 임계값을 초과하며 이벤트가 생성됩니다.

따라서 블록 크기를 포함하는 적응형 QoS 정책에 대한 MB/s 위반으로 이벤트가 트리거되면 이벤트 세부 정보 페이지의 시스템 진단 섹션에 MB/s 차트가 표시됩니다. 적응형 QoS 정책에 대한 IOPS 위반으로 이벤트가 트리거되면 시스템 진단 섹션에 IOPS 차트가 표시됩니다. IOPS와 MB/s 모두에 대해 위반이 발생한 경우 두 가지 이벤트가 발생합니다.

QoS 설정 조정에 대한 자세한 내용은 을 참조하십시오 "성능 관리 개요".

노드 리소스가 과도하게 사용된 성능 이벤트에 응답

Unified Manager에서는 단일 노드가 운영 효율성 한계를 초과하여 작동하고 워크로드 지연 시간에 영향을 줄 수 있는 경우 노드 리소스가 과도하게 사용되는 경고 이벤트를 생성합니다. 많은 워크로드가 지연 시간의 영향을 받기 전에 이러한 시스템 정의 이벤트를 통해 잠재적 성능 문제를 해결할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새 성능 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.

Unified Manager에서는 성능 용량의 100% 이상을 30분 이상 사용하는 노드를 찾으므로 노드 리소스가 과도하게 사용된 정책 위반에 대한 경고 이벤트를 생성합니다.

System Manager 또는 ONTAP 명령을 사용하여 다음 작업을 포함하여 이러한 유형의 성능 문제를 해결할 수 있습니다.

- 시스템 리소스를 과도하게 사용하는 볼륨 또는 LUN에 QoS 정책 생성 및 적용
- 워크로드가 적용된 정책 그룹의 QoS 최대 처리량 제한을 줄입니다
- 워크로드를 다른 Aggregate 또는 노드로 이동
- 노드에 디스크를 추가하거나 더 빠른 CPU와 더 많은 RAM이 있는 노드로 업그레이드하여 용량을 늘릴 수 있습니다

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 이벤트를 발생시킨 임계값 위반을 설명하는 * Description * 을 검토합니다.

   예를 들어, ""Perf. Simplicity-02의 139%의 Capacity Used Value는 데이터 처리 유닛에서 발생 가능한 성능 문제를 파악하기 위한 경고 이벤트를 발생시켰습니다.""노드 심플리시티-02의 성능 용량이 과도하게 사용되고 노드 성능에 영향을 미친다는 것을 나타냅니다.

3. System Diagnosis * 섹션에서 노드에 사용된 성능 용량에 대한 차트 1개, 최상위 워크로드에 사용되는 평균 스토리지 IOPS에 대한 차트 1개, 상위 워크로드의 지연 시간에 대한 차트 1개를 검토합니다. 이렇게 정렬하면 노드에서 지연 시간의 원인이 되는 워크로드를 확인할 수 있습니다.

   IOPS 차트 위로 커서를 이동하면 QoS 정책이 적용된 워크로드와 적용되지 않는 워크로드를 확인할 수 있습니다.

4. 제안 조치 * 섹션에서 제안 사항을 검토하고 작업 부하 대기 시간의 증가를 방지하기 위해 수행해야 할 조치를 결정합니다.

   필요한 경우 * 도움말 * 버튼을 클릭하여 성능 이벤트 해결을 위해 수행할 수 있는 권장 조치에 대한 자세한 내용을 확인하십시오.

클러스터 불균형 성능 이벤트에 대한 대응

Unified Manager는 클러스터의 한 노드가 다른 노드보다 훨씬 더 높은 부하에서 작동 중일 때 클러스터 불균형 경고 이벤트를 발생시키며, 이로 인해 워크로드 지연 시간에 영향을 줄 수 있습니다. 많은 워크로드가 지연 시간의 영향을 받기 전에 이러한 시스템 정의 이벤트를 통해 잠재적 성능 문제를 해결할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

Unified Manager에서 클러스터의 모든 노드에 대해 사용된 성능 용량과 노드 간 로드 차이가 30%인지 비교하여 클러스터 불균형 임계값 정책 위반에 대한 경고 이벤트를 생성합니다.

다음 단계를 수행하면 고성능 워크로드를 사용률이 낮은 노드로 이동할 수 있는 다음 리소스를 식별할 수 있습니다.

- 활용이 떨어지는 동일한 클러스터의 노드
- 가장 활용도가 낮은 새 노드의 Aggregate
- 현재 노드에서 가장 높은 성능을 보이는 볼륨입니다

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 * 세부 정보 페이지를 표시합니다.
2. 이벤트를 발생시킨 임계값 위반을 설명하는 * Description * 을 검토합니다.

   예를 들어 "'사용된 성능 용량 카운터'는 클러스터 Dallas-1-8 노드 간의 로드 차이를 나타내며 시스템 임계값인 30%를 기준으로 경고 이벤트를 발생시켰습니다."라는 메시지는 노드 중 하나의 성능 용량이 과도하게 사용되고 노드 성능에 영향을 미친다는 것을 나타냅니다.

3. 제안된 작업 * 의 텍스트를 검토하여 고성능 용량 사용 값이 있는 노드에서 사용된 성능 용량이 가장 낮은 노드로 고성능 볼륨을 이동합니다.
4. 사용된 용량이 가장 높고 가장 낮은 노드를 식별합니다.
   a. 이벤트 정보 * 섹션에서 소스 클러스터의 이름을 클릭합니다.
   b. 클러스터/성능 요약 * 페이지의 * 관리되는 개체 * 영역에서 * 노드 * 를 클릭합니다.
   c. Nodes * inventory 페이지에서 * Performance Capacity Used * 열을 기준으로 노드를 정렬합니다.
   d. 사용된 성능 용량이 가장 높고 가장 낮은 노드를 식별하고 해당 이름을 기록합니다.
5. 사용된 성능 용량이 가장 높은 노드에서 최대 IOPS를 사용하여 볼륨을 식별합니다.
   a. 사용된 성능 용량이 가장 높은 노드를 클릭합니다.
   b. 노드/성능 탐색기 * 페이지의 * 보기 및 비교 * 메뉴에서 이 노드의 * 집계 * 를 선택합니다.

c. 사용된 성능 용량이 가장 높은 애그리게이트를 클릭합니다.

d. Aggregate/Performance Explorer * 페이지의 * 보기 및 비교 * 메뉴에서 * 이 애그리게이트에 있는 볼륨 * 을 선택합니다.

e. IOPS * 열을 기준으로 볼륨을 정렬하고, 최대 IOPS와 볼륨이 상주하는 애그리게이트의 이름을 사용하여 볼륨의 이름을 기록합니다.

6. 사용된 성능 용량이 가장 낮은 노드에서 사용률이 가장 낮은 애그리게이트 식별:

a. 스토리지 * > * 애그리게이트 * 를 클릭하여 * 애그리게이트 * 재고 페이지를 표시합니다.

b. 성능: 모든 애그리게이트 * 보기를 선택합니다.

c. 필터 * 버튼을 클릭하고 4단계에서 적어 내려는 성능 용량 사용 값이 가장 낮은 노드 이름과 ""노드""가 같은 필터를 추가합니다.

d. 사용된 성능 용량이 가장 낮은 애그리게이트의 이름을 기록합니다.

7. 오버로드된 노드에서 새 노드의 사용률이 낮은 것으로 확인된 애그리게이트로 볼륨을 이동합니다.

ONTAP 시스템 관리자, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 툴의 조합을 사용하여 이동 작업을 수행할 수 있습니다.

며칠 후 이 클러스터에서 동일한 클러스터 불균형 이벤트가 발생하는지 확인합니다.

동적 성능 임계값에서 이벤트 분석

동적 임계값에서 생성된 이벤트는 워크로드의 실제 응답 시간(지연 시간)이 예상 응답 시간 범위에 비해 너무 높거나 낮음을 나타냅니다. 이벤트 세부 정보 페이지를 사용하여 성능 이벤트를 분석하고 필요한 경우 수정 조치를 취하여 성능을 정상 상태로 되돌릴 수 있습니다.

동적 성능 임계값은 Cloud Volumes ONTAP, ONTAP Edge 또는 ONTAP Select 시스템에서는 사용할 수 없습니다.

동적 성능 이벤트와 관련된 피해자 워크로드 파악

Unified Manager에서 경합으로 인해 발생한 스토리지 구성요소의 응답 시간(지연 시간)에서 가장 큰 편차가 있는 볼륨 워크로드를 식별할 수 있습니다. 이러한 워크로드를 식별하면 액세스하는 클라이언트 애플리케이션이 평소보다 느리게 작동하는 이유를 이해하는 데 도움이 됩니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 동적 성능 이벤트, 확인된 이벤트 또는 사용되지 않는 동적 성능 이벤트가 있어야 합니다.

이벤트 세부 정보 페이지에는 사용자 정의 워크로드 및 시스템 정의 워크로드 목록이 표시되며, 이 목록은 구성 요소의 활동 또는 사용량의 최고 편차로 순위가 매겨지거나 이벤트에 의해 가장 많이 영향을 받습니다. 이 값은 Unified Manager가 이벤트를 감지하여 마지막으로 분석한 결과를 기준으로 한 피크를 기반으로 합니다.

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.

2. 워크로드 지연 시간 및 워크로드 활동 차트에서 * 피해자 워크로드 * 를 선택합니다.
3. 차트 위에 커서를 올려 놓으면 구성 요소에 영향을 주는 최상위 사용자 정의 워크로드와 대상 워크로드의 이름이 표시됩니다.

동적 성능 이벤트와 관련된 대규모 워크로드 식별

Unified Manager에서 경합 중인 클러스터 구성 요소의 사용 편차가 가장 큰 워크로드를 식별할 수 있습니다. 이러한 워크로드를 식별하면 클러스터의 특정 볼륨에서 응답 시간(지연 시간)이 느려지는 이유를 이해하는 데 도움이 됩니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 동적 성능 이벤트, 확인된 이벤트 또는 사용되지 않는 동적 성능 이벤트가 있어야 합니다.

이벤트 세부 정보 페이지에는 구성 요소의 최대 사용량이나 이벤트의 영향을 가장 많이 받는 작업량에 따라 순위가 지정된 사용자 정의 및 시스템 정의 작업 부하 목록이 표시됩니다. 이 값은 Unified Manager가 이벤트를 감지하여 마지막으로 분석한 결과를 기준으로 한 피크를 기반으로 합니다.

단계

1. 이벤트에 대한 정보를 보려면 이벤트 세부 정보 페이지를 표시합니다.
2. 워크로드 지연 시간 및 워크로드 활동 차트에서 * Bully Workload * 를 선택합니다.
3. 차트 위에 커서를 올려 놓으면 구성 요소에 영향을 주는 사용자 정의 상위 워크로드가 표시됩니다.

동적 성능 이벤트와 관련된 **shark** 워크로드 식별

Unified Manager에서 경합 중인 스토리지 구성 요소에 대해 사용 시 가장 편차가 큰 워크로드를 식별할 수 있습니다. 이러한 워크로드를 식별하면 활용도가 낮은 클러스터로 이동해야 하는지 여부를 결정하는 데 도움이 됩니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성능 동적 이벤트가 있거나, 확인되거나, 사용되지 않는 성능 동적 이벤트가 있습니다.

이벤트 세부 정보 페이지에는 구성 요소의 최대 사용량이나 이벤트의 영향을 가장 많이 받는 작업량에 따라 순위가 지정된 사용자 정의 및 시스템 정의 작업 부하 목록이 표시됩니다. 이 값은 Unified Manager가 이벤트를 감지하여 마지막으로 분석한 결과를 기준으로 한 피크를 기반으로 합니다.

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 워크로드 지연 시간 및 워크로드 활동 차트에서 * Shark 워크로드 * 를 선택합니다.
3. 차트 위에 커서를 올려 놓으면 구성 요소에 영향을 미치는 최상위 사용자 정의 워크로드와 Shark 워크로드의 이름이 표시됩니다.

MetroCluster 구성에 대한 성능 이벤트 분석

Unified Manager를 사용하여 MetroCluster 구성의 성능 이벤트를 분석할 수 있습니다. 이벤트와 관련된 워크로드를 식별하고 해결을 위해 제안된 작업을 검토할 수 있습니다.

MetroCluster 성능 이벤트는 클러스터 간 ISL(Interswitch Link)을 과도하게 활용하는 _bully_워크로드 또는 링크 상태 문제로 인해 발생할 수 있습니다. Unified Manager는 파트너 클러스터의 성능 이벤트를 고려하지 않고 MetroCluster 구성에서 각 클러스터를 독립적으로 모니터링합니다.

MetroCluster 구성에서 두 클러스터의 성능 이벤트도 Unified Manager 대시보드 페이지에 표시됩니다. Unified Manager의 상태 페이지를 보고 각 클러스터의 상태를 확인하고 상태를 확인할 수도 있습니다.

MetroCluster 구성에서 클러스터의 동적 성능 이벤트 분석

Unified Manager를 사용하면 성능 이벤트가 감지된 MetroCluster 구성에서 클러스터를 분석할 수 있습니다. 관련된 클러스터 이름, 이벤트 감지 시간 및 _bully_and_d피해자_작업 부하를 식별할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- MetroCluster 구성에 대한 새로운 성능 이벤트, 확인된 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.
- MetroCluster 구성의 두 클러스터는 동일한 Unified Manager 인스턴스에서 모니터링해야 합니다.

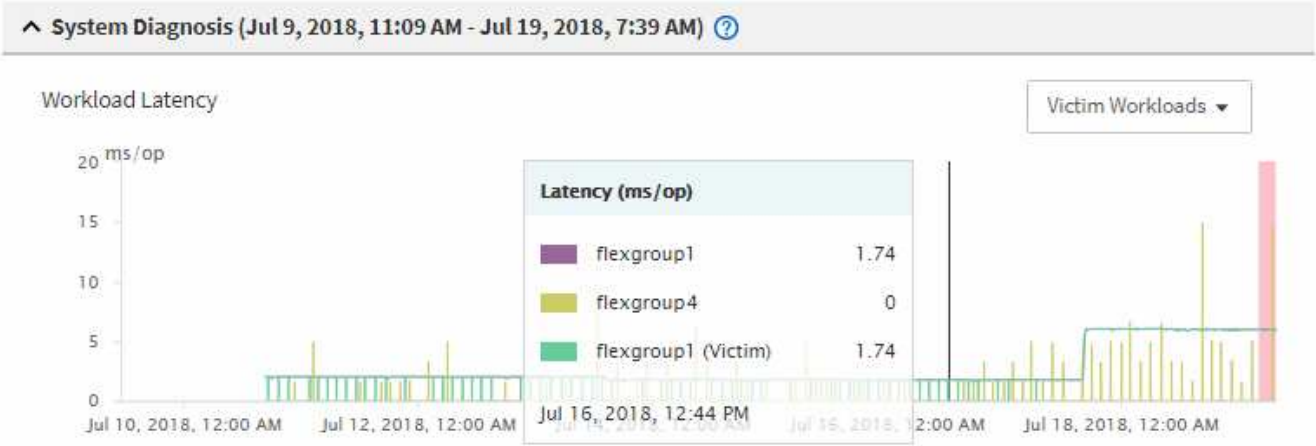
단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 이벤트 설명을 검토하여 관련된 워크로드의 이름과 관련 워크로드의 수를 확인합니다.

   이 예에서 MetroCluster 리소스 아이콘은 빨간색이며 MetroCluster 리소스 경합이 발생했음을 나타냅니다. 아이콘 위에 커서를 놓으면 아이콘에 대한 설명이 표시됩니다.

3. 클러스터 이름과 이벤트 감지 시간을 기록해 둡니다. 이 정보를 사용하여 파트너 클러스터의 성능 이벤트를 분석할 수 있습니다.
4. 차트에서 _d피해자_워크로드 를 검토하여 응답 시간이 성능 임계값보다 높음을 확인합니다.

   이 예에서는 희생자 워크로드가 호버 텍스트에 표시됩니다. 지연 시간 차트는 관련된 피해자 워크로드에 대해 일관된 지연 시간 패턴을 고수준으로 표시합니다. 비정상적인 지연 시간으로 인해 이벤트가 트리거되었지만, 일관된 지연 시간 패턴을 통해 워크로드가 예상 범위 내에서 수행되고 있음을 알 수 있지만 I/O가 급증하면 지연 시간이 늘어나고 이벤트가 트리거됩니다.



최근에 이러한 볼륨 워크로드에 액세스하는 클라이언트에 애플리케이션을 설치하고 해당 애플리케이션에서 많은 양의 I/O를 보내면 지연 시간이 증가할 것으로 예상할 수 있습니다. 워크로드의 지연 시간이 예상 범위 내로 돌아오며 이벤트 상태가 폐기로 변경되고 30분 이상 이 상태로 지속되면 이벤트를 무시할 수 있습니다. 이벤트가 진행 중이며 새 상태로 남아 있는 경우 더 자세히 조사하여 다른 문제로 인해 이벤트가 발생했는지 여부를 확인할 수 있습니다.

5. 워크로드 처리량 차트에서 * Bully Workload * 를 선택하여 워크로드가 불룩한 워크로드를 표시합니다.

   대규모 워크로드가 있을 경우 MetroCluster 리소스를 과도하게 활용하여 로컬 클러스터에 있는 하나 이상의 워크로드에 의해 이벤트가 발생했을 수 있습니다. 워크로드가 큰 경우 쓰기 처리량(MB/s)이 편차가 높습니다.

   이 차트는 워크로드의 쓰기 처리량(MB/s) 패턴을 높은 수준으로 표시합니다. 쓰기 MB/s 패턴을 검토하여 비정상적인 처리량을 파악할 수 있습니다. 이는 워크로드가 MetroCluster 리소스를 과도하게 활용하고 있음을 나타낼 수 있습니다.

   문제가 있는 워크로드가 이벤트와 관련되지 않은 경우, 해당 이벤트는 클러스터 간 연결 상태 문제 또는 파트너 클러스터의 성능 문제로 인해 발생한 것일 수 있습니다. Unified Manager를 사용하여 MetroCluster 구성에서 두 클러스터의 상태를 확인할 수 있습니다. Unified Manager를 사용하여 파트너 클러스터의 성능 이벤트를 확인하고 분석할 수도 있습니다.

MetroCluster 구성에서 원격 클러스터에 대한 동적 성능 이벤트 분석

Unified Manager를 사용하여 MetroCluster 구성에서 원격 클러스터의 동적 성능 이벤트를 분석할 수 있습니다. 분석을 통해 원격 클러스터의 이벤트로 인해 파트너 클러스터의 이벤트가 발생했는지 여부를 확인할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- MetroCluster 구성에서 로컬 클러스터의 성능 이벤트를 분석하고 이벤트 감지 시간을 확인해야 합니다.
- 성능 이벤트와 관련된 로컬 클러스터와 파트너 클러스터의 상태를 확인하고 파트너 클러스터의 이름을 얻어야 합니다.

단계

1. 파트너 클러스터를 모니터링 중인 Unified Manager 인스턴스에 로그인합니다.
2. 왼쪽 탐색 창에서 * 이벤트 * 를 클릭하여 이벤트 목록을 표시합니다.

3. Time Range * 선택기에서 * Last Hour * 를 선택한 다음 * Apply Range * 를 클릭합니다.
4. 필터링 * 선택기의 왼쪽 드롭다운 메뉴에서 * 클러스터 * 를 선택하고 텍스트 필드에 파트너 클러스터의 이름을 입력한 다음 * 필터 적용 * 을 클릭합니다.

   지난 1시간 동안 선택한 클러스터에 대한 이벤트가 없을 경우 이는 이벤트가 파트너에 감지된 시간 동안 클러스터에서 성능 문제가 발생하지 않았음을 나타냅니다.

5. 선택한 클러스터에 지난 1시간 동안 감지된 이벤트가 있는 경우 이벤트 감지 시간과 로컬 클러스터의 이벤트에 대한 이벤트 감지 시간을 비교합니다.

   이러한 이벤트로 인해 워크로드가 불룩하게 발생하여 데이터 처리 구성 요소에서 경합이 발생하는 경우, 이러한 불리 중 하나 이상이 로컬 클러스터에서 이벤트를 유발했을 수 있습니다. 이벤트를 클릭하여 분석하고 이벤트 세부 정보 페이지에서 해결 시 제안된 작업을 검토할 수 있습니다.

   대규모 워크로드가 관련되지 않은 경우 로컬 클러스터에서 성능 이벤트가 발생하지는 않았습니다.

QoS 정책 그룹 임계치 조절로 인해 발생하는 동적 성능 이벤트에 대한 응답

Unified Manager를 사용하면 QoS(서비스 품질) 정책 그룹의 워크로드 처리량 제한(MB/s)으로 인해 발생하는 성능 이벤트를 조사할 수 있습니다. 임계치 조절을 통해 정책 그룹에 있는 볼륨 워크로드의 응답 시간(지연 시간)이 증가했습니다. 이벤트 정보를 사용하여 임계치 조절을 중지하기 위해 정책 그룹에 대한 새로운 제한이 필요한지 여부를 결정할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성능 이벤트, 확인된 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 임계치 조절에 의해 영향을 받는 워크로드의 이름을 표시하는 * 설명 * 을 읽습니다.

   임계치 조절을 통해 워크로드를 스스로 희생시킬 수 있으므로 설명은 피해자와 괴롭힘을 가진 환자에 대해 동일한 워크로드를 표시할 수 있습니다.

3. 텍스트 편집기와 같은 응용 프로그램을 사용하여 볼륨의 이름을 기록합니다.

   볼륨 이름을 검색하여 나중에 찾을 수 있습니다.

4. 워크로드 지연 시간 및 워크로드 활용률 차트에서 * Bully Workload * 를 선택합니다.
5. 차트 위에 커서를 올려 놓으면 정책 그룹에 영향을 주는 최상위 사용자 정의 워크로드가 표시됩니다.

   목록의 맨 위에 있는 작업 부하는 편차가 가장 높고 스로틀링이 발생합니다. 이 활동은 각 워크로드에서 사용하는 정책 그룹 제한의 백분율입니다.

6. Suggested Actions * 영역에서 상위 워크로드에 대한 * Analyze Workload * 버튼을 클릭합니다.
7. 워크로드 분석 페이지에서 지연 시간 차트를 설정하여 모든 클러스터 구성 요소를 확인하고 처리량 차트를 설정하여 분석 내역을 볼 수 있습니다.

분석 차트는 지연 시간 차트 및 IOPS 차트 아래에 표시됩니다.

8. 지연 시간 * 차트의 QoS 제한을 비교하여 이벤트 발생 시 지연 시간에 영향을 미치는 임계치 조절량을 확인하십시오.

   QoS 정책 그룹은 초당 최대 1,000개의 작업 처리량(op/sec)을 가지고 있으며, 이 처리 속도는 해당 그룹의 워크로드를 통틀어 초과할 수 없습니다. 이벤트 발생 시 정책 그룹의 워크로드는 초당 1,200회 이상의 처리 속도로 결합되어 정책 그룹이 작업을 다시 초당 1,000회 작업으로 제한했습니다

9. 읽기/쓰기 지연 시간 * 값을 * 읽기/쓰기/기타 * 값과 비교합니다.

   두 차트 모두 대기 시간이 긴 많은 읽기 요청 수가 표시되지만 요청 수와 쓰기 요청 대기 시간은 낮습니다. 이러한 값을 통해 처리량이 많을지 또는 지연 시간을 증가했는지 여부를 확인할 수 있습니다. 처리량 또는 작업에 정책 그룹 제한을 두기로 결정할 때 이러한 값을 사용할 수 있습니다.

10. ONTAP 시스템 관리자를 사용하여 정책 그룹의 현재 제한을 1300op/sec로 늘립니다
11. 하루 후 Unified Manager로 돌아가 3단계에서 기록한 워크로드를 * 워크로드 분석 * 페이지에 입력합니다.
12. 처리량 분석 차트를 선택합니다.

    읽기/쓰기/기타 차트가 표시됩니다.

13. 페이지 맨 위에서 커서를 이벤트 변경 아이콘( )를 클릭합니다.
14. 읽기/쓰기/기타 * 차트를 * 지연 시간 * 차트와 비교하십시오.

    읽기 및 쓰기 요청은 동일하지만 임계치 조절이 중지되고 지연 시간이 감소했습니다.

디스크 장애로 인한 동적 성능 이벤트에 대한 응답

Unified Manager를 사용하면 애그리게이트를 과도하게 활용하여 워크로드가 발생하는 성능 이벤트를 조사할 수 있습니다. 또한 Unified Manager를 사용하여 애그리게이트의 상태를 점검하여 성능 이벤트가 발생한 애그리게이트에서 감지된 최신 상태 이벤트가 있는지 확인할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성능 이벤트, 확인된 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 이벤트와 관련된 워크로드 및 경합의 클러스터 구성 요소에 대해 설명하는 * Description * 을 읽습니다.

   경합 중인 클러스터 구성 요소의 지연 시간에 영향을 받은 여러 개의 대상 볼륨이 있습니다. RAID 재구성 중에 장애가 발생한 디스크를 스페어 디스크로 교체하기 위한 애그리게이트는 경합 중인 클러스터 구성요소입니다. 경합의 부품 아래에서 집계 아이콘이 빨간색으로 강조 표시되고 집계 이름이 괄호 안에 표시됩니다.

3. 워크로드 활용률 차트에서 * Bully Workload * 를 선택합니다.
4. 차트 위에 커서를 올려 놓으면 구성 요소에 영향을 주는 상위 워크로드가 표시됩니다.

이벤트가 감지된 이후 최고 사용률이 가장 높은 상위 워크로드가 차트 상단에 표시됩니다. 가장 중요한 워크로드 중 하나는 RAID 재구성을 나타내는 시스템 정의 워크로드 디스크 상태 입니다. 재구성은 스페어 디스크로 애그리게이트를 재구성하는 작업과 관련된 내부 프로세스입니다. 디스크 상태 워크로드와 애그리게이트의 기타 워크로드가 서로 경합하면 애그리게이트와 관련 이벤트가 발생할 수 있습니다.

5. 디스크 상태 워크로드의 작업으로 인해 이벤트가 발생했는지 확인한 후 재구성이 완료될 때까지 약 30분 정도 기다린 후 Unified Manager가 이벤트를 분석하고 애그리게이션 경합이 아직 지속되는지 여부를 감지할 수 있도록 합니다.
6. 이벤트 세부 정보 * 를 새로 고칩니다.

   RAID 재구성이 완료된 후 상태가 폐기되어 이벤트가 해결되었음을 나타내는지 확인합니다.

7. 워크로드 활용률 차트에서 * Bully Workload * 를 선택하여 최대 활용률별 총 워크로드를 봅니다.
8. Suggested Actions * 영역에서 상위 워크로드에 대한 * Analyze Workload * 버튼을 클릭합니다.
9. Workload Analysis * 페이지에서 선택한 볼륨에 대한 마지막 24시간(1일)의 데이터를 표시할 시간 범위를 설정합니다.

   이벤트 타임라인에서 빨간색 점(🔴)는 디스크 오류 이벤트가 발생한 시기를 나타냅니다.

10. 노드 및 애그리게이트 활용도 차트에서 집계 라인만 유지되도록 노드 통계에 대한 줄을 숨깁니다.
11. 이 차트의 데이터를 * 지연 시간 * 차트의 이벤트 시점의 데이터와 비교합니다.

    이벤트 발생 시 애그리게이트 활용률은 RAID 재구성 프로세스로 인해 발생하는 높은 양의 읽기 및 쓰기 작업을 보여주며, 이로 인해 선택한 볼륨의 지연 시간이 증가합니다. 이벤트가 발생한 후 몇 시간이 지나면 읽기 및 쓰기와 지연 시간이 모두 감소되어 애그리게이트는 더 이상 경합이 발생하지 않음을 확인합니다.

HA 테이크오버 때문에 발생하는 동적 성능 이벤트에 대한 대응

Unified Manager를 사용하면 고가용성(HA) 쌍의 클러스터 노드에서 높은 데이터 처리로 인해 발생하는 성능 이벤트를 조사할 수 있습니다. Unified Manager를 사용하여 노드의 상태를 점검하여 노드에서 감지된 최신 상태 이벤트가 성능 이벤트에 기여했는지 확인할 수도 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 새로운 성능 이벤트, 확인된 이벤트 또는 사용되지 않는 성능 이벤트가 있어야 합니다.

단계

1. 이벤트에 대한 정보를 보려면 * 이벤트 세부 정보 * 페이지를 표시합니다.
2. 이벤트와 관련된 워크로드 및 경합의 클러스터 구성 요소에 대해 설명하는 * Description * 을 읽습니다.

   경합 중인 클러스터 구성 요소에 의해 지연 시간이 영향을 받은 피해자 볼륨이 한 개 있습니다. 파트너 노드에서 모든 워크로드를 인계받은 데이터 처리 노드는 경합이 발생한 클러스터 구성 요소입니다. Component in Contention(충돌 시 구성 요소) 아래에 데이터 처리 아이콘이 빨간색으로 강조 표시되고 이벤트 시 데이터 처리를 처리하고 있는 노드의 이름이 괄호 안에 표시됩니다.

3. 설명 * 에서 볼륨의 이름을 클릭합니다.

   볼륨 성능 탐색기 페이지가 표시됩니다. 페이지 위쪽의 이벤트 시간 줄에서 변경 이벤트 아이콘(🔵)은 Unified

Manager가 HA 테이크오버 시작을 감지한 시간을 나타냅니다.

4. HA 테이크오버 이벤트 변경 아이콘에 커서를 가져가면 HA 테이크오버 관련 세부 정보가 호버 텍스트로 표시됩니다.

   지연 시간 차트에서 이벤트는 HA 테이크오버 시간과 거의 동일한 시간의 높은 지연 시간으로 인해 선택한 볼륨이 성능 임계값을 초과했음을 나타냅니다.

5. 새 페이지에 지연 시간 차트를 표시하려면 * 확대/축소 보기 * 를 클릭합니다.
6. 보기 메뉴에서 * 클러스터 구성 요소 * 를 선택하여 클러스터 구성 요소별 총 지연 시간을 확인합니다.
7. HA 테이크오버 시작을 위한 변경 이벤트 아이콘에 마우스 커서를 놓고 데이터 처리 지연 시간을 총 지연 시간과 비교하십시오.

   HA 테이크오버 중 데이터 처리 노드의 워크로드 수요 증가로 데이터 처리가 급증했습니다. CPU 활용률이 증가하면서 지연 시간이 늘어나고 이벤트가 트리거되었습니다.

8. 장애가 발생한 노드를 해결한 후 ONTAP System Manager를 사용하여 HA 기브백을 수행하여 워크로드를 파트너 노드에서 고정 노드로 이동합니다.
9. HA 기브백이 완료된 후 Unified Manager에서 다음 구성 검색(약 15분)을 수행한 후 * 이벤트 관리 * 인벤토리 페이지에서 HA 테이크오버(HA)에 의해 트리거되는 이벤트 및 워크로드를 찾습니다.

   이제 HA 테이크오버에 의해 트리거된 이벤트에 대해 사용되지 않는 상태가 있으며 이는 이벤트가 해결되었음을 나타냅니다. 데이터 처리 구성 요소의 지연 시간이 감소되어 총 지연 시간이 감소했습니다. 선택한 볼륨이 현재 데이터 처리에 사용 중인 노드에서 이벤트를 해결했습니다.

성능 이벤트 해결

제안된 작업을 사용하여 직접 성능 이벤트를 시도하고 해결할 수 있습니다. 처음 세 가지 제안 사항은 항상 표시되며 네 번째 제안 아래에 있는 작업은 표시되는 이벤트 유형에 따라 달라집니다.

Help Me Do this* 링크는 특정 작업 수행에 대한 지침을 포함하여 각 권장 조치에 대한 추가 정보를 제공합니다. 그 중에는 Unified Manager, ONTAP System Manager, OnCommand Workflow Automation, ONTAP CLI 명령 또는 이러한 툴의 조합을 사용하는 것도 포함될 수 있습니다.

지연 시간이 예상 범위 내에 있는지 확인

클러스터 구성 요소의 경합이 발생하면 이 구성 요소를 사용하는 볼륨 워크로드에서 응답 시간(지연 시간)이 단축될 수 있습니다. 경합 중인 구성 요소에서 각 피해자 워크로드의 지연 시간을 검토하여 실제 지연 시간이 예상 범위 내에 있는지 확인할 수 있습니다. 볼륨 이름을 클릭하여 볼륨에 대한 내역 데이터를 볼 수도 있습니다.

성능 이벤트가 폐기 상태인 경우 이벤트에 관련된 각 피해자의 지연 시간이 예상 범위 내로 반환되었을 수 있습니다.

구성 변경이 워크로드 성능에 미치는 영향을 검토하십시오

장애 디스크, HA 페일오버 또는 이동한 볼륨과 같이 클러스터의 구성을 변경하면 볼륨 성능에 부정적인 영향을 미치고 대기 시간이 증가할 수 있습니다.

Unified Manager에서 워크로드 분석 페이지를 검토하여 최근 구성 변경이 발생한 시기를 확인하고 작업 및 지연 시간(응답 시간)과 비교하여 선택한 볼륨 워크로드에 대한 활동이 변경되었는지 확인할 수 있습니다.

Unified Manager의 성능 페이지에서는 제한된 수의 변경 이벤트만 감지할 수 있습니다. 상태 페이지에서는 구성 변경으로 인한 다른 이벤트에 대한 알림을 제공합니다. Unified Manager에서 볼륨을 검색하여 이벤트 기록을 볼 수 있습니다.

클라이언트측 워크로드 성능 향상을 위한 옵션

애플리케이션 또는 데이터베이스와 같은 클라이언트 워크로드가 성능 이벤트와 관련된 볼륨에 I/O를 보내고 있는지 확인하여 클라이언트 측 변경이 이벤트를 해결할 수 있는지 파악할 수 있습니다.

클러스터의 볼륨에 연결된 클라이언트가 I/O 요청을 늘릴 경우 클러스터가 더 열심히 작업하여 수요를 충족시켜야 합니다. 클러스터의 특정 볼륨에 대한 입출력 요청이 많은 클라이언트를 알고 있는 경우 볼륨에 액세스하는 클라이언트 수를 조정하거나 볼륨에 대한 I/O 양을 줄여 클러스터 성능을 향상시킬 수 있습니다. 볼륨이 구성원인 QoS 정책 그룹에 제한을 적용하거나 늘릴 수도 있습니다.

클라이언트 및 해당 애플리케이션을 조사하여 클라이언트가 평소보다 더 많은 입출력을 전송하는지 여부를 확인할 수 있습니다. 이로 인해 클러스터 구성 요소에서 충돌이 발생할 수 있습니다. 이벤트 세부 정보 페이지의 시스템 진단 섹션에 구성 요소를 사용하여 상위 볼륨 워크로드가 표시됩니다. 특정 볼륨에 액세스하는 클라이언트를 알고 있는 경우 클라이언트로 이동하여 클라이언트 하드웨어 또는 애플리케이션이 예상대로 작동하지 않는지 또는 평소보다 더 많은 작업을 수행하고 있는지 확인할 수 있습니다.

MetroCluster 구성에서는 로컬 클러스터의 볼륨에 대한 쓰기 요청이 원격 클러스터의 볼륨에 미러링됩니다. 로컬 클러스터의 소스 볼륨을 원격 클러스터의 대상 볼륨과 동기화하여 유지하면 MetroCluster 구성에서 두 클러스터의 수요가 증가할 수 있습니다. 이러한 미러링된 볼륨에 대한 쓰기 요청을 줄임으로써 클러스터는 더 적은 수의 동기화 작업을 수행할 수 있으므로 다른 워크로드에 대한 성능 영향이 줄어듭니다.

클라이언트 또는 네트워크 문제를 확인합니다

클러스터의 볼륨에 연결된 클라이언트가 I/O 요청을 늘릴 경우 클러스터가 더 열심히 작업하여 수요를 충족시켜야 합니다. 클러스터에 대한 수요 증가로 인해 구성 요소의 경합이 발생할 수 있으며, 해당 구성 요소를 사용하는 워크로드의 지연 시간이 늘어나고, Unified Manager에서 이벤트가 발생할 수 있습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에 구성 요소를 사용하여 상위 볼륨 워크로드가 표시됩니다. 특정 볼륨에 액세스하는 클라이언트를 알고 있는 경우 클라이언트로 이동하여 클라이언트 하드웨어 또는 애플리케이션이 예상대로 작동하지 않는지 또는 평소보다 더 많은 작업을 수행하고 있는지 확인할 수 있습니다. 도움이 필요하면 클라이언트 관리자 또는 애플리케이션 공급업체에 문의하십시오.

네트워크 인프라를 확인하여 클러스터와 연결된 클라이언트 간에 입출력 요청이 예상보다 느리게 수행되도록 했을 수 있는 하드웨어 문제, 병목 현상 또는 경쟁업체 워크로드가 있는지 확인할 수 있습니다. 도움이 필요하면 네트워크 관리자에게 문의하십시오.

QoS 정책 그룹의 다른 볼륨에서 활동이 비정상적으로 높았는지 확인합니다

활동이 가장 많이 변경되는 QoS(서비스 품질) 정책 그룹의 워크로드를 검토하여 둘 이상의 워크로드가 이벤트를 유발했는지 여부를 확인할 수 있습니다. 또한 다른 워크로드가 설정된 처리량 제한을 초과하지 않고 있는지 또는 해당 워크로드가 예상 활동 범위 내에 있는지 여부를

확인할 수 있습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에서는 활동에서 최대 편차별로 워크로드를 정렬하여 테이블 상단에 가장 높은 활동 변화가 있는 워크로드를 표시할 수 있습니다. 이러한 워크로드는 활동이 설정된 한도를 초과하고 이벤트를 유발했을 가능성이 있는 "불리"일 수 있습니다.

각 볼륨 워크로드의 워크로드 분석 페이지로 이동하여 IOPS 작업을 검토할 수 있습니다. 워크로드가 매우 높은 작업 기간을 갖는 경우 이벤트에 영향을 줄 수 있습니다. 워크로드에 대한 정책 그룹 설정을 변경하거나 워크로드를 다른 정책 그룹으로 이동할 수 있습니다.

ONTAP System Manager 또는 ONTAP CLI 명령을 사용하여 다음과 같이 정책 그룹을 관리할 수 있습니다.

- 정책 그룹을 생성합니다.
- 정책 그룹에서 워크로드를 추가하거나 제거합니다.
- 정책 그룹 간에 워크로드를 이동합니다.
- 정책 그룹의 처리량 제한을 변경합니다.

논리 인터페이스(LIF) 이동

LIF(논리 인터페이스)를 사용량이 적은 포트로 이동하면 로드 밸런싱을 개선하고, 유지보수 운영 및 성능 조정을 지원하고, 간접 액세스를 줄일 수 있습니다.

간접 액세스는 시스템 효율성을 줄일 수 있습니다. 볼륨 워크로드가 네트워크 처리 및 데이터 처리에 서로 다른 노드를 사용하는 경우 발생합니다. 간접 액세스를 줄이기 위해 LIF를 재배열할 수 있습니다. LIF에는 네트워크 처리 및 데이터 처리에 동일한 노드를 사용하도록 LIF를 이동하는 작업이 포함됩니다. ONTAP가 사용 중인 LIF를 다른 포트로 자동으로 이동하도록 로드 밸런싱을 구성하거나 LIF를 수동으로 이동할 수 있습니다.

* 혜택 *	* 고려 사항 *
• 로드 밸런싱 향상 • 간접 액세스를 줄입니다.	CIFS 공유에 연결된 LIF를 이동할 때 CIFS 공유에 액세스하는 클라이언트의 연결이 끊어집니다. CIFS 공유에 대한 읽기 또는 쓰기 요청이 모두 중단됩니다.

ONTAP 명령을 사용하여 로드 밸런싱을 구성합니다. 자세한 내용은 ONTAP 네트워킹 설명서를 참조하십시오.

ONTAP System Manager와 ONTAP CLI 명령을 사용하여 LIF를 수동으로 이동할 수 있습니다.

사용 빈도가 낮은 시간에 스토리지 효율성 작업을 실행합니다

영향을 받는 볼륨 워크로드의 사용량이 적을 때 실행할 스토리지 효율성 작업을 처리하는 정책 또는 일정을 수정할 수 있습니다.

스토리지 효율성 작업은 많은 양의 클러스터 CPU 리소스를 사용할 수 있으며 작업이 실행 중인 볼륨에 큰 역할을 할 수 있습니다. 스토리지 효율성 작업을 실행할 때 대상 볼륨의 활동이 동시에 많은 경우 지연 시간이 길어지면 이벤트가 트리거될 수 있습니다.

이벤트 세부 정보 페이지의 시스템 진단 섹션에는 작업 중 최대 편차별로 QoS 정책 그룹의 워크로드를 표시하여

워크로드가 불룩한 워크로드를 식별합니다. 테이블 상단 근처에 "스토리지 효율성"이 표시되면 이러한 작업이 피해자의 워크로드를 괴롭히는 것입니다. 워크로드 사용량이 적을 때 효율성 정책 또는 일정을 수정하여 실행할 경우 스토리지 효율성 작업으로 인해 클러스터에 경합이 발생하지 않도록 할 수 있습니다.

ONTAP 시스템 관리자를 사용하여 효율성 정책을 관리할 수 있습니다. ONTAP 명령을 사용하여 효율성 정책 및 일정을 관리할 수 있습니다.

스토리지 효율성에 대해 설명합니다

스토리지 효율성을 통해 최저 비용으로 최대 용량의 데이터를 저장할 수 있으며 빠른 데이터 증가를 수용하면서도 공간을 덜 사용할 수 있습니다. NetApp의 스토리지 효율성 전략은 핵심 ONTAP 운영 체제 및 WAFL(Write Anywhere File Layout) 파일 시스템이 제공하는 스토리지 가상화 및 유니파이드 스토리지의 내장된 기반을 기반으로 합니다.

스토리지 효율성에는 씬 프로비저닝, 스냅샷 복사본, 중복제거, 데이터 압축, FlexClone ®, SnapVault 및 볼륨 SnapMirror, RAID-DP, Flash Cache, Flash Pool 애그리게이트 및 FabricPool 지원 애그리게이트를 사용하는 씬 복제를 통해 스토리지 활용률을 높이고 스토리지 비용을 절감할 수 있습니다.

통합 스토리지 아키텍처를 사용하면 SAN(Storage Area Network), NAS(Network-Attached Storage) 및 보조 스토리지를 단일 플랫폼으로 효율적으로 통합할 수 있습니다.

Flash Pool 애그리게이트 또는 Flash Cache 및 RAID-DP 기술을 통해 구성된 SATA(Serial Advanced Technology Attachment) 드라이브와 같은 고밀도 디스크 드라이브를 사용하면 성능과 복원력에 영향을 주지 않고 효율성을 높일 수 있습니다.

FabricPool 지원 애그리게이트에는 ONTAP 9.8부터 시작하는 모든 SSD 애그리게이트 또는 HDD 애그리게이트와 클라우드 계층으로 지정한 오브젝트 저장소가 포함됩니다. FabricPool를 구성하면 데이터의 액세스 빈도 여부를 기준으로 저장할 스토리지 계층(로컬 계층 또는 클라우드 계층) 데이터를 관리할 수 있습니다.

씬 프로비저닝, 스냅샷 복사본, 중복제거, 데이터 압축, SnapVault 및 volume SnapMirror를 사용한 씬 복제 및 FlexClone과 같은 기술을 통해 비용을 더욱 절감할 수 있습니다. 이러한 기술을 개별적으로 또는 함께 사용하여 최대한의 스토리지 효율성을 달성할 수 있습니다.

디스크 추가 및 데이터 재할당

Aggregate에 디스크를 추가하면 스토리지 용량과 해당 애그리게이트의 성능을 높일 수 있습니다. 디스크를 추가한 후에는 추가한 디스크에 데이터를 재할당한 후에만 읽기 성능이 향상됩니다.

Unified Manager가 동적 임계값 또는 시스템 정의 성능 임계값에 의해 트리거된 애그리게이트 이벤트를 수신한 경우 다음 명령을 사용할 수 있습니다.

- 동적 임계값 이벤트를 수신한 경우 이벤트 세부 정보 페이지에서 경합된 애그리게이트를 나타내는 클러스터 구성 요소 아이콘이 빨간색으로 강조 표시됩니다.

  아이콘 아래의 괄호 안에 있는 는 디스크를 추가할 수 있는 애그리게이트를 식별하는 애그리게이트의 이름입니다.

- 시스템 정의 임계값 이벤트를 수신한 경우 이벤트 세부 정보 페이지에서 이벤트 설명 텍스트에 문제가 있는 애그리게이트의 이름이 나열됩니다.

  이 Aggregate에 디스크를 추가하고 데이터를 재할당할 수 있습니다.

Aggregate에 추가하는 디스크가 클러스터에 이미 존재해야 합니다. 클러스터에 사용 가능한 추가 디스크가 없는 경우 관리자에게 문의하거나 더 많은 디스크를 구매해야 할 수 있습니다. ONTAP System Manager 또는 ONTAP 명령을 사용하여 애그리게이트에 디스크를 추가할 수 있습니다.

HDD 및 Flash Pool 애그리게이트만 사용할 경우 데이터를 재할당해야 합니다. SSD 또는 FabricPool 애그리게이트에 데이터를 재할당하지 마십시오.

노드에서 **Flash Cache**를 사용하도록 설정하여 워크로드 성능을 향상하는 방법

클러스터의 각 노드에서 Flash Cache ™ 지능형 데이터 캐싱을 활성화하여 워크로드 성능을 높일 수 있습니다.

Flash Cache 모듈 또는 성능 가속화 모듈 PCIe 기반 메모리 모듈은 지능형 외부 읽기 캐시로 작동하는 랜덤 읽기 집약적인 워크로드의 성능을 최적화합니다. 이 하드웨어는 ONTAP의 WAFL 외부 캐시 소프트웨어 구성 요소와 함께 작동합니다.

Unified Manager의 이벤트 세부 정보 페이지에서 경합에 있는 애그리게이트를 나타내는 클러스터 구성 요소 아이콘이 빨간색으로 강조 표시됩니다. 아이콘 아래의 괄호 안에 있는 는 애그리게이트를 식별하는 애그리게이트의 이름입니다. Aggregate가 상주하는 노드에서 Flash Cache를 사용하도록 설정할 수 있습니다.

ONTAP System Manager나 ONTAP 명령을 사용하여 Flash Cache가 설치되어 있는지, 설정되어 있지 않은 경우 사용하도록 설정할 수 있습니다. 다음 명령은 특정 노드에서 Flash Cache가 설정되었는지 여부를 나타냅니다. " * cluster::> run local options flexscale.enable * "

Flash Cache 및 Flash Cache 사용에 대한 자세한 내용은 다음 기술 보고서를 참조하십시오.

"기술 보고서 3832: Flash Cache 모범 사례 가이드 를 참조하십시오"

스토리지 애그리게이트에서 **Flash Pool**을 사용하도록 설정하여 워크로드 성능을 향상하는 방법

애그리게이트에서 Flash Pool 기능을 활성화하여 워크로드 성능을 개선할 수 있습니다. Flash Pool은 HDD와 SSD를 모두 통합하는 애그리게이트입니다. HDD는 운영 스토리지에 사용되며 SSD는 고성능 읽기 및 쓰기 캐시를 제공하여 애그리게이트 성능을 향상합니다.

Unified Manager에서 이벤트 세부 정보 페이지에는 경합에 있는 애그리게이트의 이름이 표시됩니다. ONTAP System Manager 또는 ONTAP 명령을 사용하여 애그리게이트에 Flash Pool이 활성화되어 있는지 확인할 수 있습니다. SSD가 설치된 경우 명령줄 인터페이스를 사용하여 활성화할 수 있습니다. SSD가 설치된 경우 애그리게이트에서 다음 명령을 실행하여 Flash Pool이 활성화되었는지 확인할 수 있습니다. ' * cluster::::> 스토리지 애그리게이트 show-aggregate aggr_name-field Hybrid-enabled * '

이 명령에서 '_aggr_name _'은(는) 경합 중인 집계와 같은 집계 이름입니다.

Flash Pool 및 Flash Pool 사용에 대한 자세한 내용은 _Clustered Data ONTAP 물리적 스토리지 관리 가이드_를 참조하십시오.

MetroCluster 구성 상태 점검

Unified Manager를 사용하여 IP 또는 FC를 통한 MetroCluster 구성에서 클러스터의 상태를 검토할 수 있습니다. 상태 및 이벤트는 워크로드의 성능에 영향을 줄 수 있는 하드웨어 또는 소프트웨어 문제가 있는지 여부를 파악하는 데 도움이 됩니다.

이메일 경고를 보내도록 Unified Manager를 구성하는 경우 성능 이벤트에 원인이 될 수 있는 로컬 또는 원격 클러스터의 상태 문제가 있는지 이메일을 확인할 수 있습니다. Unified Manager GUI에서 * 이벤트 관리 * 를 선택하여 현재 이벤트 목록을 표시한 다음 필터를 사용하여 MetroCluster 구성 이벤트만 표시할 수 있습니다.

자세한 내용은 을 참조하십시오 "MetroCluster 구성에서 클러스터 상태 확인"

MetroCluster 구성 검증

MetroCluster 구성이 올바르게 설정되었는지 확인하여 FC 및 IP 구성을 통해 MetroCluster에서 미러링된 워크로드의 성능 문제를 방지할 수 있습니다. 또한 구성을 변경하거나 소프트웨어 또는 하드웨어 구성요소를 업그레이드하여 워크로드 성능을 향상할 수 있습니다.

을 참조하십시오 "MetroCluster 문서" FC(Fibre Channel) 스위치, 케이블 및 ISL(Inter-Switch Link)을 포함하여 MetroCluster 구성에서 클러스터를 설정하는 지침은 을 참조하십시오. 또한 로컬 및 원격 클러스터가 미러 볼륨 데이터와 통신할 수 있도록 MetroCluster 소프트웨어를 구성하는 데도 도움이 됩니다. IP를 통한 MetroCluster 설정에 대한 자세한 내용은 을 참조하십시오 "MetroCluster IP 구성을 설치합니다".

MetroCluster 구성과 의 요구 사항을 비교할 수 있습니다 "MetroCluster 문서" MetroCluster 구성에서 구성 요소를 변경하거나 업그레이드하면 워크로드 성능이 향상될 수 있는지 확인할 수 있습니다. 이 비교는 다음 질문에 대한 해답을 제공합니다.

- 컨트롤러가 워크로드에 적합합니까?
- 더 많은 처리량을 처리하기 위해 ISL 번들을 더 큰 대역폭으로 업그레이드해야 합니까?
- 대역폭을 늘리기 위해 스위치의 버퍼 대 버퍼 크레딧(BBC)을 조정할 수 있습니까?
- 워크로드에 SSD(Solid State Drive) 스토리지에 대한 쓰기 처리량이 높은 경우 처리량을 수용하기 위해 FC-to-SAS 브릿지를 업그레이드해야 합니까?
- 관련 정보 *
- MetroCluster 구성 요소 교체 또는 업그레이드에 대한 자세한 내용은 를 참조하십시오 "MetroCluster 문서".
- 컨트롤러 업그레이드에 대한 자세한 내용은 를 참조하십시오 "스위치오버 및 스위치백을 사용하여 MetroCluster FC 구성에서 컨트롤러 업그레이드" 및 "스위치오버 및 스위치백을 사용하여 MetroCluster IP 구성에서 컨트롤러 업그레이드"

워크로드를 다른 애그리게이트로 이동

Unified Manager를 사용하면 현재 워크로드가 있는 애그리게이트보다 덜 사용되는 애그리게이트를 식별할 수 있으며, 그런 다음 선택한 볼륨 또는 LUN을 해당 애그리게이트로 이동할 수 있습니다. 고성능 워크로드를 사용량이 낮은 Aggregate로 이동하거나 플래시 스토리지를 지원하는 Aggregate를 이동하면 워크로드가 보다 효율적으로 수행됩니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 현재 성능 문제가 있는 애그리게이트의 이름을 기록해야 합니다.
- Aggregate가 이벤트를 수신한 날짜 및 시간을 기록해야 합니다.
- Unified Manager에서 성능 데이터를 한 달 이상 수집 및 분석해야 합니다.

다음 단계를 수행하면 고성능 워크로드를 사용률이 낮은 Aggregate로 이동할 수 있도록 다음 리소스를 식별할 수 있습니다.

- 활용되지 않는 동일한 클러스터의 애그리게이트
- 현재 애그리게이트에서 가장 높은 성능을 보이는 볼륨

단계

1. 가장 활용도가 낮은 클러스터 내 애그리게이트 식별:
   a. 이벤트 * 세부 정보 페이지에서 애그리게이트로 구성된 클러스터의 이름을 클릭합니다.

      클러스터 세부 정보가 성능/클러스터 랜딩 페이지에 표시됩니다.

   b. 요약 * 페이지의 * 관리되는 개체 * 창에서 * 집계 * 를 클릭합니다.

      이 클러스터의 애그리게이트 목록이 표시됩니다.

   c. Utilization * 열을 클릭하여 가장 적게 사용된 순서대로 애그리게이트를 정렬합니다.

      또한 * 가용 용량 * 이 가장 큰 애그리게이트를 식별할 수 있습니다. 다음은 워크로드를 이동할 수 있는 잠재적 애그리게이트 목록입니다.

   d. 워크로드를 이동할 애그리게이트의 이름을 기록합니다.
2. 이벤트를 수신한 애그리게이트로부터 고성능 볼륨을 식별합니다.
   a. 성능 문제가 있는 애그리게이트를 클릭합니다.

      집계 세부 정보는 성능/집계 탐색기 페이지에 표시됩니다.

   b. 시간 범위 * 선택기에서 * 최근 30일 * 을 선택한 다음 * 범위 적용 * 을 클릭합니다.

      이렇게 하면 기본 72시간보다 더 긴 성능 기록 기간을 볼 수 있습니다. 지난 72시간 동안 많은 리소스를 사용하는 볼륨을 일관성 있게 이동하려고 합니다.

   c. 보기 및 비교 * 컨트롤에서 이 집계 * 의 * 볼륨 을 선택합니다.

      이 애그리게이트에 있는 FlexVol 볼륨 및 FlexGroup 구성 볼륨 목록이 표시됩니다.

   d. 가장 높은 성능이 필요한 볼륨을 확인하려면 가장 높은 MB/s와 가장 높은 IOPS 순으로 볼륨을 정렬합니다.
   e. 다른 aggregate로 이동하려는 볼륨의 이름을 기록합니다.
3. 사용률이 낮은 것으로 확인된 aggregate로 고성능 볼륨을 이동합니다.

   ONTAP 시스템 관리자, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 툴의 조합을 사용하여 이동 작업을 수행할 수 있습니다.

며칠 후 이 노드나 집합으로부터 동일한 유형의 이벤트를 받고 있는지 확인하십시오.

워크로드를 다른 노드로 이동

Unified Manager를 사용하면 현재 실행 중인 워크로드가 있는 노드보다 사용량이 적은 다른

노드의 애그리게이트를 식별할 수 있으며, 선택한 볼륨을 해당 애그리게이트로 이동할 수 있습니다. 사용량이 적은 노드의 aggregate로 고성능 워크로드를 이동하면 두 노드의 워크로드를 더 효율적으로 처리할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 현재 성능 문제가 있는 노드의 이름을 기록해야 합니다.
- 성능 이벤트를 수신한 날짜 및 시간을 기록해야 합니다.
- Unified Manager에서 성능 데이터를 한 달 이상 수집 및 분석해야 합니다.

이 절차를 사용하면 고성능 워크로드를 사용률이 낮은 노드로 이동할 수 있도록 다음 리소스를 식별할 수 있습니다.

- 동일한 클러스터에 있는 노드 중 사용 가능한 성능 용량이 가장 큰 노드
- 새 노드의 aggregate에서 사용 가능한 성능 용량이 가장 많습니다
- 현재 노드에서 가장 높은 성능을 보이는 볼륨입니다

단계

1. 사용 가능한 성능 용량이 가장 큰 클러스터 노드를 식별합니다.
   a. 이벤트 세부 정보 * 페이지에서 노드가 상주하는 클러스터의 이름을 클릭합니다.

      클러스터 세부 정보가 성능/클러스터 랜딩 페이지에 표시됩니다.

   b. 요약 * 탭의 * 관리 개체 * 창에서 * 노드 * 를 클릭합니다.

      이 클러스터의 노드 목록이 표시됩니다.

   c. Performance Capacity Used * 열을 클릭하여 사용된 최소 비율별로 노드를 정렬합니다.

      이 목록에는 워크로드를 이동할 수 있는 잠재적 노드 목록이 나와 있습니다.

   d. 워크로드를 이동할 노드의 이름을 기록합니다.
2. 가장 활용도가 낮은 새 노드의 애그리게이트 식별:
   a. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭하고 보기 메뉴에서 * 성능 * > * 모든 애그리게이트 * 를 선택합니다.

      성능: 모든 애그리게이트 보기가 표시됩니다.

   b. 필터링 * 을 클릭하고 왼쪽 드롭다운 메뉴에서 * 노드 * 를 선택한 다음 텍스트 필드에 노드 이름을 입력하고 * 필터 적용 * 을 클릭합니다.

      성능: 모든 애그리게이트 보기는 이 노드에서 사용할 수 있는 애그리게이트 목록과 함께 다시 표시됩니다.

   c. Performance Capacity Used * 열을 클릭하여 가장 적게 사용된 순서대로 애그리게이트를 정렬합니다.

      다음은 워크로드를 이동할 수 있는 잠재적 애그리게이트 목록입니다.

   d. 워크로드를 이동할 애그리게이트의 이름을 기록합니다.

3. 이벤트를 수신한 노드에서 고성능 워크로드 파악:
   a. 이벤트의 * 이벤트 세부 정보 * 페이지로 돌아갑니다.
   b. 영향을 받는 볼륨 * 필드에서 볼륨 수에 대한 링크를 클릭합니다.

      성능: 모든 볼륨 보기는 해당 노드에 있는 볼륨의 필터링된 목록과 함께 표시됩니다.

   c. Total Capacity * 열을 클릭하여 할당된 최대 공간으로 볼륨을 정렬합니다.

      이동할 수 있는 잠재적 볼륨 목록이 표시됩니다.

   d. 이동할 볼륨의 이름과 해당 볼륨이 있는 현재 애그리게이트의 이름을 기록합니다.
4. 새 노드에서 최대 가용 성능 용량이 있는 것으로 확인된 애그리게이트로 볼륨을 이동합니다.

   ONTAP 시스템 관리자, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 툴의 조합을 사용하여 이동 작업을 수행할 수 있습니다.

며칠 후 이 노드나 집합으로부터 동일한 유형의 이벤트를 받고 있는지 확인할 수 있습니다.

워크로드를 다른 노드의 **Aggregate**로 이동

Unified Manager를 사용하면 워크로드가 현재 실행 중인 노드보다 사용량이 적은 다른 노드의 애그리게이트를 식별할 수 있으며, 선택한 볼륨을 해당 애그리게이트로 이동할 수 있습니다. 사용량이 적은 노드의 aggregate로 고성능 워크로드를 이동하면 두 노드의 워크로드를 더 효율적으로 처리할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 현재 성능 문제가 있는 노드의 이름을 기록해야 합니다.
- 성능 이벤트를 수신한 날짜 및 시간을 기록해야 합니다.
- Unified Manager에서 성능 데이터를 한 달 이상 수집 및 분석해야 합니다.

다음 단계를 수행하면 고성능 워크로드를 사용률이 낮은 노드로 이동할 수 있는 다음 리소스를 식별할 수 있습니다.

- 활용이 떨어지는 동일한 클러스터의 노드
- 가장 활용도가 낮은 새 노드의 Aggregate
- 현재 노드에서 가장 높은 성능을 보이는 볼륨입니다

단계

1. 클러스터에서 가장 활용도가 낮은 노드를 식별합니다.
   a. 이벤트 * 세부 정보 페이지에서 노드가 상주하는 클러스터의 이름을 클릭합니다.

      클러스터 세부 정보가 성능/클러스터 랜딩 페이지에 표시됩니다.

   b. 요약 * 페이지의 * 관리 개체 * 창에서 * 노드 * 를 클릭합니다.

이 클러스터의 노드 목록이 표시됩니다.

c. Utilization * 열을 클릭하여 가장 활용도가 낮은 노드를 정렬합니다.

또한 * 여유 용량 * 이 가장 큰 노드를 식별할 수도 있습니다. 이 목록에는 워크로드를 이동할 수 있는 잠재적 노드 목록이 나와 있습니다.

d. 워크로드를 이동할 노드의 이름을 기록합니다.

2. 가장 활용도가 낮은 새 노드의 애그리게이트 식별:

a. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭하고 보기 메뉴에서 * 성능 * > * 모든 애그리게이트 * 를 선택합니다.

성능: 모든 애그리게이트 보기가 표시됩니다.

b. 필터링 * 을 클릭하고 왼쪽 드롭다운 메뉴에서 * 노드 * 를 선택한 다음 텍스트 필드에 노드 이름을 입력하고 * 필터 적용 * 을 클릭합니다.

성능: 모든 애그리게이트 보기는 이 노드에서 사용할 수 있는 애그리게이트 목록과 함께 다시 표시됩니다.

c. Utilization * 열을 클릭하여 가장 적게 사용된 순서대로 애그리게이트를 정렬합니다.

또한 * 가용 용량 * 이 가장 큰 애그리게이트를 식별할 수 있습니다. 다음은 워크로드를 이동할 수 있는 잠재적 애그리게이트 목록입니다.

d. 워크로드를 이동할 애그리게이트의 이름을 기록합니다.

3. 이벤트를 수신한 노드에서 고성능 워크로드 파악:

a. 이벤트에 대한 * 이벤트 * 세부 정보 페이지로 돌아갑니다.

b. 영향을 받는 볼륨 * 필드에서 볼륨 수에 대한 링크를 클릭합니다.

성능: 모든 볼륨 보기는 해당 노드에 있는 볼륨의 필터링된 목록과 함께 표시됩니다.

c. Total Capacity * 열을 클릭하여 할당된 최대 공간으로 볼륨을 정렬합니다.

이동할 수 있는 잠재적 볼륨 목록이 표시됩니다.

d. 이동할 볼륨의 이름과 해당 볼륨이 있는 현재 애그리게이트의 이름을 기록합니다.

4. 새 노드의 사용률이 낮은 것으로 확인된 애그리게이트로 볼륨을 이동합니다.

ONTAP 시스템 관리자, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 툴의 조합을 사용하여 이동 작업을 수행할 수 있습니다.

며칠 후 이 노드나 집합으로부터 동일한 유형의 이벤트를 받고 있는지 확인하십시오.

워크로드를 다른 **HA** 쌍의 노드로 이동

Unified Manager를 사용하면 현재 워크로드가 실행 중인 HA 쌍보다 더 많은 가용 성능 용량이 있는 다른 HA(고가용성) 쌍의 노드에서 애그리게이트를 식별할 수 있습니다. 그런 다음, 선택한 볼륨을 새 HA 쌍에서 애그리게이트로 이동할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 클러스터는 최소한 2개의 HA 쌍으로 구성되어야 합니다

  클러스터에 하나의 HA 쌍만 있는 경우에는 이 수정 프로세스를 사용할 수 없습니다.

- 현재 성능 문제가 있는 HA 쌍에 두 노드의 이름을 기록해야 합니다.
- 노드가 성능 이벤트를 수신한 날짜 및 시간을 기록해야 합니다.
- Unified Manager에서 성능 데이터를 한 달 이상 수집 및 분석해야 합니다.

고성능 워크로드를 여유 성능 용량이 더 많은 노드의 aggregate로 이동하면 두 노드의 워크로드를 더 효율적으로 처리할 수 있습니다. 이 절차를 통해 고성능 워크로드를 다른 HA 쌍의 여유 성능 용량이 더 큰 노드로 이동할 수 있도록 다음 리소스를 식별할 수 있습니다.

- 동일한 클러스터에 있는 다른 HA 쌍의 노드로, 최대 가용 성능 용량을 제공합니다
- 새 노드의 aggregate에서 사용 가능한 성능 용량이 가장 많습니다
- 현재 노드에서 가장 높은 성능을 보이는 볼륨

단계

1. 동일한 클러스터에서 다른 HA 쌍의 일부인 노드를 식별합니다.
   a. 이벤트 세부 정보 * 페이지에서 노드가 상주하는 클러스터의 이름을 클릭합니다.

      클러스터 세부 정보가 성능/클러스터 랜딩 페이지에 표시됩니다.

   b. 요약 * 페이지의 * 관리 개체 * 창에서 * 노드 * 를 클릭합니다.

      이 클러스터의 노드 목록은 성능:모든 노드 보기에 표시됩니다.

   c. 현재 성능 문제가 있는 HA Pair와 다른 HA 노드에 있는 노드의 이름을 적어둡니다.
2. 새 HA 쌍에서 사용 가능한 성능 용량이 가장 큰 노드 식별:
   a. 성능: 모든 노드 * 보기에서 * 사용된 성능 용량 * 열을 클릭하여 사용된 최소 비율별로 노드를 정렬합니다.

      이 목록에는 워크로드를 이동할 수 있는 잠재적 노드 목록이 나와 있습니다.

   b. 워크로드를 이동할 다른 HA 쌍의 노드 이름을 기록합니다.
3. 새 노드에서 사용 가능한 성능 용량이 가장 큰 Aggregate를 식별합니다.
   a. 성능: 모든 노드 * 보기에서 노드를 클릭합니다.

      노드 세부 정보가 성능/노드 탐색기 페이지에 표시됩니다.

   b. 보기 및 비교 * 메뉴에서 이 노드의 * 집계 * 를 선택합니다.

      이 노드의 애그리게이트는 그리드에 표시됩니다.

   c. Performance Capacity Used * 열을 클릭하여 가장 적게 사용된 순서대로 애그리게이트를 정렬합니다.

      다음은 워크로드를 이동할 수 있는 잠재적 애그리게이트 목록입니다.

d. 워크로드를 이동할 애그리게이트의 이름을 기록합니다.

4. 이벤트를 수신한 노드에서 고성능 워크로드 파악:

   a. 이벤트에 대한 * 이벤트 * 세부 정보 페이지로 돌아갑니다.

   b. 영향을 받는 볼륨 * 필드에서 첫 번째 노드의 볼륨 수에 대한 링크를 클릭합니다.

      성능: 모든 볼륨 보기는 해당 노드에 있는 볼륨의 필터링된 목록과 함께 표시됩니다.

   c. Total Capacity * 열을 클릭하여 할당된 최대 공간으로 볼륨을 정렬합니다.

      이동할 수 있는 잠재적 볼륨 목록이 표시됩니다.

   d. 이동할 볼륨의 이름과 해당 볼륨이 있는 현재 애그리게이트의 이름을 기록합니다.

   e. 이 이벤트의 일부인 두 번째 노드에 대해 4c 및 4D단계를 수행하여 해당 노드에서 이동할 수 있는 볼륨도 식별합니다.

5. 새 노드에서 최대 가용 성능 용량이 있는 것으로 확인된 애그리게이트로 볼륨을 이동합니다.

   ONTAP 시스템 관리자, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 툴의 조합을 사용하여 이동 작업을 수행할 수 있습니다.

며칠 후 이 노드나 집합으로부터 동일한 유형의 이벤트를 받고 있는지 확인할 수 있습니다.

워크로드를 다른 **HA** 쌍의 다른 노드로 이동

Unified Manager를 사용하면 현재 워크로드가 실행 중인 HA 쌍보다 사용량이 적은 다른 HA 쌍에서 노드의 애그리게이트를 식별할 수 있습니다. 그런 다음, 선택한 볼륨을 새 HA 쌍에서 애그리게이트로 이동할 수 있습니다. 사용량이 적은 노드의 aggregate로 고성능 워크로드를 이동하면 두 노드의 워크로드를 더 효율적으로 처리할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 클러스터는 최소한 2개의 HA 쌍으로 구성되어야 합니다. 클러스터에는 HA 쌍이 하나만 있으면 이 수정 프로세스를 사용할 수 없습니다.
- 현재 성능 문제가 있는 HA 쌍에 두 노드의 이름을 기록해야 합니다.
- 노드가 성능 이벤트를 수신한 날짜 및 시간을 기록해야 합니다.
- Unified Manager에서 성능 데이터를 한 달 이상 수집 및 분석해야 합니다.

다음 단계를 따르면 고성능 워크로드를 다른 HA Pair의 사용률이 낮은 노드로 이동할 수 있도록 다음 리소스를 식별할 수 있습니다.

- 활용되지 않는 동일한 클러스터에 있는 다른 HA 쌍의 노드
- 새로운 노드의 Aggregate가 가장 활용도가 낮습니다
- 현재 노드에서 가장 높은 성능을 보이는 볼륨

단계

1. 동일한 클러스터에서 다른 HA 쌍의 일부인 노드를 식별합니다.
   a. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭하고 보기 메뉴에서 * 성능 * > * 모든 클러스터 * 를 선택합니다.

      성능: 모든 클러스터 보기가 표시됩니다.

   b. 현재 클러스터의 * 노드 수 * 필드에서 번호를 클릭합니다.

      성능: 모든 노드 보기가 표시됩니다.

   c. 현재 성능 문제가 있는 HA Pair와 다른 HA 노드에 있는 노드의 이름을 적어둡니다.
2. 새로운 HA 쌍에서 가장 적게 사용되는 노드 식별
   a. Utilization * 열을 클릭하여 가장 활용도가 낮은 노드를 정렬합니다.

      또한 * 여유 용량 * 이 가장 큰 노드를 식별할 수도 있습니다. 이 목록에는 워크로드를 이동할 수 있는 잠재적 노드 목록이 나와 있습니다.

   b. 워크로드를 이동할 노드의 이름을 기록합니다.
3. 가장 활용도가 낮은 새 노드의 애그리게이트 식별:
   a. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭하고 보기 메뉴에서 * 성능 * > * 모든 애그리게이트 * 를 선택합니다.

      성능: 모든 애그리게이트 보기가 표시됩니다.

   b. 필터링 * 을 클릭하고 왼쪽 드롭다운 메뉴에서 * 노드 * 를 선택한 다음 텍스트 필드에 노드 이름을 입력하고 * 필터 적용 * 을 클릭합니다.

      성능: 모든 애그리게이트 보기는 이 노드에서 사용할 수 있는 애그리게이트 목록과 함께 다시 표시됩니다.

   c. Utilization * 열을 클릭하여 가장 적게 사용된 순서대로 애그리게이트를 정렬합니다.

      또한 * 가용 용량 * 이 가장 큰 애그리게이트를 식별할 수 있습니다. 다음은 워크로드를 이동할 수 있는 잠재적 애그리게이트 목록입니다.

   d. 워크로드를 이동할 애그리게이트의 이름을 기록합니다.
4. 이벤트를 수신한 노드에서 고성능 워크로드 파악:
   a. 이벤트에 대한 * 이벤트 * 세부 정보 페이지로 돌아갑니다.
   b. 영향을 받는 볼륨 * 필드에서 첫 번째 노드의 볼륨 수에 대한 링크를 클릭합니다.

      성능: 모든 볼륨 보기는 해당 노드에 있는 볼륨의 필터링된 목록과 함께 표시됩니다.

   c. Total Capacity * 열을 클릭하여 할당된 최대 공간으로 볼륨을 정렬합니다.

      이동할 수 있는 잠재적 볼륨 목록이 표시됩니다.

   d. 이동할 볼륨의 이름과 해당 볼륨이 있는 현재 애그리게이트의 이름을 기록합니다.
   e. 이 이벤트의 일부인 두 번째 노드에 대해 4c 및 4D단계를 수행하여 해당 노드에서 이동할 수 있는 볼륨도 식별합니다.

5. 새 노드의 사용률이 낮은 것으로 확인된 애그리게이트로 볼륨을 이동합니다.

   ONTAP 시스템 관리자, OnCommand Workflow Automation, ONTAP 명령 또는 이러한 툴의 조합을 사용하여 이동 작업을 수행할 수 있습니다.

며칠 후 이 노드나 집합으로부터 동일한 유형의 이벤트를 받고 있는지 확인하십시오.

QoS 정책 설정을 사용하여 이 노드에서 작업의 우선 순위를 지정합니다

QoS 정책 그룹에 포함된 워크로드에 대한 IOPS(초당 I/O) 또는 MBPS 처리량 한도를 제어할 수 있습니다. 워크로드가 기본 정책 그룹과 같이 설정된 제한이 없는 정책 그룹에 있거나 설정된 제한이 사용자의 요구 사항을 충족하지 않는 경우, 설정된 제한을 늘리거나 워크로드를 원하는 제한이 있는 새 정책 그룹 또는 기존 정책 그룹으로 이동할 수 있습니다.

노드의 성능 이벤트가 노드 리소스를 과도하게 사용하는 워크로드에 의해 발생하는 경우 이벤트 세부 정보 페이지의 이벤트 설명에 관련 볼륨 목록에 대한 링크가 표시됩니다. 성능/볼륨 페이지에서 영향을 받는 볼륨을 IOPS 및 MBPS 기준으로 정렬하여 이벤트가 발생한 가장 높은 사용률이 있는 워크로드를 확인할 수 있습니다.

노드 리소스를 과도하게 사용하는 볼륨을 보다 제한적인 정책 그룹 설정에 할당하면 정책 그룹은 워크로드를 조절하여 해당 노드의 리소스 사용을 줄일 수 있습니다.

ONTAP System Manager 또는 ONTAP 명령을 사용하여 다음 작업을 비롯한 정책 그룹을 관리할 수 있습니다.

- 정책 그룹을 생성하는 중입니다
- 정책 그룹에서 워크로드 추가 또는 제거
- 정책 그룹 간에 워크로드 이동
- 정책 그룹의 처리량 제한을 변경합니다

비활성 볼륨 및 LUN을 제거합니다

애그리게이트 가용 공간이 문제로 식별된 경우, 사용하지 않는 볼륨 및 LUN을 검색하여 Aggregate에서 삭제할 수 있습니다. 이렇게 하면 디스크 공간 부족 문제를 완화할 수 있습니다.

애그리게이트의 성능 이벤트가 디스크 공간이 부족하기 때문에 발생하는 경우 더 이상 사용되지 않는 볼륨 및 LUN을 확인할 수 있는 몇 가지 방법이 있습니다.

사용하지 않는 볼륨을 식별하려면 다음을 따르십시오.

- 이벤트 세부 정보 페이지에서 * 영향 받는 개체 수 * 필드는 영향을 받는 볼륨 목록을 표시하는 링크를 제공합니다.

  링크를 클릭하여 Performance: All Volumes(성능: 모든 볼륨) 보기에 볼륨을 표시합니다. 여기서 영향을 받는 볼륨을 * IOPS * 로 정렬하여 활성 상태가 아닌 볼륨을 확인할 수 있습니다.

사용되지 않는 LUN을 식별하려면 다음을 따르십시오.

1. 이벤트 세부 정보 페이지에서 이벤트가 발생한 애그리게이트의 이름을 기록합니다.
2. 왼쪽 탐색 창에서 * 스토리지 * > * LUN * 을 클릭하고 보기 메뉴에서 * 성능 * > * 모든 LUN * 을 선택합니다.

3. 필터링 * 을 클릭하고 왼쪽 드롭다운 메뉴에서 * 집계 * 를 선택한 다음 텍스트 필드에 집계 이름을 입력하고 * 필터 적용 * 을 클릭합니다.
4. 영향을 받는 LUN의 결과 목록을 * IOPS * 별로 정렬하여 활성 상태가 아닌 LUN을 확인합니다.

사용하지 않는 볼륨 및 LUN을 식별한 후 ONTAP System Manager 또는 ONTAP 명령을 사용하여 해당 개체를 삭제할 수 있습니다.

디스크를 추가하고 애그리게이트 레이아웃 재구성을 수행합니다

Aggregate에 디스크를 추가하면 스토리지 용량과 해당 애그리게이트의 성능을 높일 수 있습니다. 디스크를 추가한 후에는 Aggregate를 재구성한 후에만 성능이 향상됩니다.

이벤트 세부 정보 페이지에서 시스템 정의 임계값 이벤트를 수신하면 이벤트 설명 텍스트에 문제가 있는 애그리게이트의 이름이 나열됩니다. 이 애그리게이트에서 디스크를 추가하고 데이터를 재구성할 수 있습니다.

Aggregate에 추가하는 디스크가 클러스터에 이미 존재해야 합니다. 클러스터에 사용 가능한 추가 디스크가 없는 경우 관리자에게 문의하거나 더 많은 디스크를 구매해야 할 수 있습니다. ONTAP System Manager 또는 ONTAP 명령을 사용하여 애그리게이트에 디스크를 추가할 수 있습니다.

"기술 보고서 3838: 스토리지 서브시스템 구성 가이드"

Unified Manager Server와 외부 데이터 공급자 간의 연결 설정

Unified Manager Server와 외부 데이터 공급자 간의 연결을 통해 클러스터 성능 데이터를 외부 서버로 전송하여 스토리지 관리자가 타사 소프트웨어를 사용하여 성능 메트릭을 차트에 작성할 수 있도록 합니다.

Unified Manager 서버와 외부 데이터 공급자 간의 연결은 유지보수 콘솔의 ""외부 데이터 공급자"" 메뉴 옵션을 통해 설정됩니다.

외부 서버로 보낼 수 있는 성능 데이터

Unified Manager는 모니터링 하는 모든 클러스터에서 다양한 성능 데이터를 수집합니다. 특정 데이터 그룹을 외부 서버로 보낼 수 있습니다.

차트로 작성할 성능 데이터에 따라 다음 통계 그룹 중 하나를 보내도록 선택할 수 있습니다.

통계 그룹	데이터 포함	세부 정보
성능 모니터	다음 객체에 대한 높은 수준의 성능 통계: • LUN을 클릭합니다 • 볼륨	이 그룹은 모니터링되는 모든 클러스터의 모든 LUN 및 볼륨에 대해 총 IOPS 또는 지연 시간을 제공합니다. 이 그룹은 가장 적은 수의 통계를 제공합니다.

통계 그룹	데이터 포함	세부 정보
리소스 활용률	다음 객체에 대한 리소스 활용도 통계: • 노드 • 애그리게이트	이 그룹은 모니터링되는 모든 클러스터에서 노드에 대한 활용도 통계를 제공하고 물리적 리소스를 집계합니다. 또한 성능 모니터 그룹에서 수집된 통계도 제공합니다.
드릴다운	추적된 모든 객체에 대해 낮은 레벨의 읽기/쓰기 및 프로토콜별 통계: • 노드 • 애그리게이트 • LUN을 클릭합니다 • 볼륨 • 디스크 • LIF • 포트/NIC	이 그룹은 모니터링되는 모든 클러스터에서 추적된 7개의 객체 유형 모두에 대해 읽기/쓰기 및 프로토콜별 분석 기능을 제공합니다. 또한 Performance Monitor 그룹과 Resource Utilization 그룹에서 수집된 통계도 제공합니다. 이 그룹은 가장 많은 수의 통계를 제공합니다.

스토리지 시스템에서 클러스터 또는 클러스터 객체의 이름이 변경되면 기존 객체와 새 객체 모두 외부 서버("metric_path"라고 함)의 성능 데이터를 포함합니다. 두 오브젝트는 동일한 오브젝트와 연관되지 않습니다. 예를 들어, 볼륨 이름을 ""volume1_acct"에서 ""acct_vol1""로 변경하면 이전 볼륨에 대한 이전 성능 데이터와 새 볼륨에 대한 새 성능 데이터가 표시됩니다.

외부 데이터 공급자로 보낼 수 있는 모든 성능 카운터 목록은 기술 자료 문서 30096을 참조하십시오.

"Unified Manager 성능 카운터를 외부 데이터 공급자로 내보낼 수 있습니다"

Unified Manager로부터 성능 데이터를 수신하도록 Graphite 설정

흑연은 컴퓨터 시스템에서 성능 데이터를 수집하고 그래프로 작성하기 위한 개방형 소프트웨어 도구입니다. Unified Manager로부터 통계 데이터를 수신하려면 Graphite 서버 및 소프트웨어를 올바르게 구성해야 합니다.

NetApp은 Graphite 또는 다른 타사 툴의 특정 버전을 테스트하거나 검증하지 않습니다.

Graphite 서버는 Unified Manager로부터 볼륨에 대한 성능 데이터를 수신하지 않습니다.

설치 지침에 따라 Graphite를 설치한 후에는 Unified Manager에서 통계 데이터 전송을 지원하도록 다음과 같이 변경해야 합니다.

- '/opt/흑연/conf/carbon.conf' 파일에서, 분당 흑연 서버에서 생성할 수 있는 최대 파일 수를 *200*(' * MAX_cres_per_minute=200 *')로 설정해야 한다.

구성에 있는 클러스터 수와 보내기로 선택한 통계 개체에 따라 처음에 만들어야 하는 수천 개의 새 파일이 있을 수 있습니다. 분당 200개의 파일로 모든 메트릭 파일이 처음 생성되기까지 15분 이상이 걸릴 수 있습니다. 모든 고유한 메트릭 파일이 생성된 후에는 이 매개 변수가 더 이상 관련이 없습니다.

- IPv6 주소를 사용하여 배포된 서버에서 Graphite를 실행하는 경우 의 line_receiver_interface에 대한 값입니다 `/opt/graphite/conf/carbon.conf` 파일을 "'0.0.0.0'에서 ":"로 변경해야 합니다. (**`LINE_RECEIVER_INTERFACE = ::`**)
- '/opt/흑연/conf/storage-schemas.conf' 파일에서 'retutions' 매개변수를 사용하여 빈도를 5분으로 설정하고 보존 기간을 사용자 환경과 관련된 일수로 설정해야 합니다.

  보존 기간은 사용자 환경에서 허용하는 기간일 수 있지만 빈도 값은 최소 하나의 보존 설정에 대해 5분으로 설정되어야 합니다. 다음 예에서는 "pattern" 매개 변수를 사용하여 Unified Manager에 대한 섹션을 정의하며, 초기 빈도를 5분으로 설정하고 보존 기간을 100일로 설정합니다. " * [OPM] * "

  ``패턴=^NetApp - 성과\.. *'

  ``보존 = 5m:100d *'

  기본 공급업체 태그가 "NetApp-performance"에서 다른 태그로 변경되면 해당 변경 사항이 'pattern' 매개 변수에도 반영되어야 합니다.

Unified Manager 서버가 성능 데이터를 전송하려고 할 때 Graphite 서버를 사용할 수 없는 경우 데이터가 전송되지 않으며 수집된 데이터에 차이가 있습니다.

Unified Manager 서버에서 외부 데이터 공급자로의 연결 구성

Unified Manager에서 클러스터 성능 데이터를 외부 서버로 보낼 수 있습니다. 전송되는 통계 데이터의 유형 및 데이터가 전송되는 간격을 지정할 수 있습니다.

- 필요한 것 *
- Unified Manager 서버의 유지보수 콘솔에 로그인할 수 있는 권한이 있는 사용자 ID가 있어야 합니다.
- 외부 데이터 공급자에 대한 다음 정보가 있어야 합니다.
  - 서버 이름 또는 IP 주소(IPv4 또는 IPv6)
  - 서버 기본 포트(기본 포트 2003을 사용하지 않는 경우)
- Unified Manager 서버에서 통계 데이터를 수신할 수 있도록 원격 서버 및 타사 소프트웨어를 구성해야 합니다.
- 전송할 통계 그룹을 알아야 합니다.
  - Performance_indicator: 성능 모니터 통계
  - resource_Utilization: 리소스 활용도 및 성능 모니터 통계
  - 드릴다운: 모든 통계
- 통계를 전송할 시간 간격(5, 10 또는 15분)을 알아야 합니다

  기본적으로 Unified Manager는 5분 간격으로 통계를 수집합니다. 전송 간격을 10분(또는 15분)으로 설정하면 각 전송 중에 전송되는 데이터 양이 기본 5분 간격을 사용할 때보다 2배(또는 3배) 더 커집니다.

Unified Manager 성능 수집 간격을 10 또는 15분으로 변경하는 경우 전송 간격을 Unified Manager 수집 간격보다 크거나 같게 변경해야 합니다.

하나의 Unified Manager 서버와 하나의 외부 데이터 공급자 서버 간에 연결을 구성할 수 있습니다.

단계

1. Unified Manager 서버의 유지보수 콘솔에 유지보수 사용자로 로그인합니다.

   Unified Manager 유지보수 콘솔 프롬프트가 표시됩니다.

2. 유지보수 콘솔에서 * 외부 데이터 공급자 * 메뉴 옵션의 번호를 입력합니다.

   External Server Connection(외부 서버 연결) 메뉴가 표시됩니다.

3. 서버 연결 추가/수정 * 메뉴 옵션의 번호를 입력합니다.

   현재 서버 연결 정보가 표시됩니다.

4. 메시지가 표시되면 ' * y * '를 입력하여 계속합니다.
5. 메시지가 표시되면 대상 서버의 IP 주소 또는 이름과 서버 포트 정보(기본 포트 2003과 다른 경우)를 입력합니다.
6. 메시지가 표시되면 ' * y * '를 입력하여 입력한 정보가 올바른지 확인합니다.
7. 아무 키나 눌러 외부 서버 연결 메뉴로 돌아갑니다.
8. Modify Server Configuration *(서버 구성 수정 *) 메뉴 옵션의 번호를 입력합니다.

   현재 서버 구성 정보가 표시됩니다.

9. 메시지가 표시되면 ' * y * '를 입력하여 계속합니다.
10. 메시지가 표시되면 전송할 통계 유형, 통계가 전송되는 시간 간격 및 지금 통계 전송 활성화 여부를 입력합니다.

...	입력...
통계 그룹 ID이다	' * 0 * ' - performance_indicator(기본값) '* 1*'-resource_Utilization ' * 2 * ' - 드릴다운
공급업체 태그	외부 서버에 통계를 저장할 폴더의 설명 이름입니다. 기본 이름은 "'NetApp-performance"이지만 다른 값을 입력할 수 있습니다. 점선으로 표시된 표기법을 사용하여 계층적 폴더 구조를 정의할 수 있습니다. 예를 들어, ' * stats.performance.netapp*` 을 입력하면 통계가 * stats * > * performance * > * netapp * 에 표시됩니다.
전송 간격입니다	' * 5 * '(기본값), ' * 10 * ' 또는 ' * 15 *'분

...	입력...
활성화/비활성화합니다	'* 0*' - 비활성화 ' * 1 * ' - 활성화(기본값)

11. 메시지가 표시되면 ' * y * '를 입력하여 입력한 정보가 올바른지 확인합니다.
12. 아무 키나 눌러 외부 서버 연결 메뉴로 돌아갑니다.
13. 유지보수 콘솔을 종료하려면 ' * x * '를 입력합니다.

연결을 구성한 후에는 선택한 성능 데이터가 지정한 시간 간격에 따라 대상 서버로 전송됩니다. 외부 도구에 메트릭이 나타나기 시작하는 데 몇 분 정도 걸립니다. 메트릭 계층에서 새 메트릭을 보려면 브라우저를 새로 고쳐야 할 수 있습니다.

클러스터 상태를 모니터링하고 관리합니다

Active IQ Unified Manager 상태 모니터링 소개

Active IQ Unified Manager(이전의 OnCommand Unified Manager)를 사용하면 중앙 집중식 사용자 인터페이스를 통해 ONTAP 소프트웨어를 실행하는 수많은 시스템을 모니터링할 수 있습니다. Unified Manager 서버 인프라는 확장성, 지원 가능성 및 향상된 모니터링 및 알림 기능을 제공합니다.

Unified Manager의 주요 기능으로는 모니터링, 경고, 클러스터의 가용성 및 용량 관리, 보호 기능 관리, 진단 데이터의 번들 구성, 기술 지원 부서에 전송 등이 있습니다.

Unified Manager를 사용하여 클러스터를 모니터링할 수 있습니다. 클러스터에서 문제가 발생하면 Unified Manager가 이벤트를 통해 해당 문제의 세부 정보를 통지합니다. 또한 일부 이벤트는 문제를 해결하기 위해 취할 수 있는 개선 조치를 제공합니다. 문제가 발생할 때 전자 메일 및 SNMP 트랩을 통해 알림을 받도록 이벤트에 대한 알림을 구성할 수 있습니다.

Unified Manager를 사용하여 스토리지 객체를 주석과 연계하여 사용자 환경의 스토리지 객체를 관리할 수 있습니다. 맞춤형 주석을 생성하고 규칙을 통해 클러스터, SVM(스토리지 가상 머신), 볼륨을 주석과 함께 동적으로 연결할 수 있습니다.

또한 용량 및 상태 차트에 제공된 정보를 사용하여 각 클러스터 개체에 대한 클러스터 개체의 스토리지 요구 사항을 계획할 수 있습니다.

물리적 및 논리적 용량

Unified Manager에서는 ONTAP 스토리지 객체에 사용되는 물리적/논리적 공간의 개념을 사용합니다.

- 물리적 용량: 물리적 공간은 볼륨에 사용된 스토리지의 물리적 블록을 나타냅니다. "물리적 사용 용량"은 일반적으로 중복 제거 및 압축과 같은 스토리지 효율성 기능에서 데이터 감소로 인해 논리적 사용 용량보다 작습니다.
- 논리적 용량: 논리적 공간은 볼륨의 사용 가능한 공간(논리적 블록)을 나타냅니다. 논리적 공간은 중복제거 또는 압축 결과를 고려하지 않고 이론적 공간을 사용할 수 있는 방법을 나타냅니다. "사용된 논리적 공간"은 사용된 물리적 공간과 함께 구성된 스토리지 효율성 기능(예: 중복제거 및 압축)의 절약 효과를 더한 것입니다. 이 측정치는 데이터 압축과 물리적 공간의 기타 감소량을 반영하지 않기 때문에 물리적 사용된 용량보다 더 크게 표시되는 경우가 많습니다. 따라서 총 논리적 용량이 프로비저닝된 공간보다 클 수 있습니다.

용량 측정 단위

Unified Manager에서는 1024바이트(2^{10})바이트의 이진 단위를 기준으로 스토리지 용량을 계산합니다. ONTAP 9.10.0 이전 버전에서는 이러한 유닛이 KB, MB, GB, TB 및 PB로 표시되었습니다. ONTAP 9.10.1부터는 Unified Manager에 KiB, MiB, GiB, TiB 및 PiB로 표시됩니다.

처리량에 사용되는 단위는 모든 ONTAP 릴리스에 대해 초당 킬로바이트(Kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps) 또는 초당 테라바이트(Tbps) 등으로 계속 사용됩니다.

용량 단위는 **ONTAP 9.10.0** 이하 버전에 대해 **Unified Manager**에 표시됩니다	**Unified Manager for ONTAP 9.10.1**에 용량 단위가 표시됩니다	계산	바이트 단위의 값입니다
KB를 클릭합니다	KiB	1024	1024바이트
MB	MIB	1024 * 1024	1,048,576바이트
GB	GiB	1024 * 1024 * 1024	1,073,741,824바이트
TB	TiB	1024 * 1024 * 1024	1,099,511,627,776바이트

Unified Manager 상태 모니터링 기능

Unified Manager는 서버 인프라를 기반으로 확장성, 지원 가능성 및 향상된 모니터링 및 알림 기능을 제공합니다. Unified Manager는 ONTAP 소프트웨어를 실행하는 시스템의 모니터링을 지원합니다.

Unified Manager에는 다음과 같은 기능이 포함되어 있습니다.

- ONTAP 소프트웨어가 설치된 시스템에 대한 검색, 모니터링 및 알림:
  - 물리적 오브젝트: 노드, 디스크, 디스크 쉘프, SFO 쌍, 포트, Flash Cache가 있습니다
  - 논리적 오브젝트: 클러스터, SVM(스토리지 가상 머신), 애그리게이트, 볼륨, LUN, 네임스페이스, Qtree, LIF, 스냅샷 복사본, 접합 경로, NFS 공유, SMB 공유, 사용자 및 그룹 할당량, QoS 정책 그룹 및 이니시에이터 그룹
  - 프로토콜: CIFS, NFS, FC, iSCSI, NVMe, 및 FCoE를 지원합니다
  - 스토리지 효율성: SSD 애그리게이트, Flash Pool 애그리게이트, FabricPool 애그리게이트, 중복제거, 압축
  - 보호: SnapMirror 관계(동기식 및 비동기식) 및 SnapVault 관계
- 클러스터 검색 및 모니터링 상태 보기
- MetroCluster over FC 및 IP 구성: 클러스터 구성 요소의 구성, 문제 및 연결 상태 보기 및 모니터링 FC 기반 MetroCluster 구성을 위한 MetroCluster 스위치 및 브리지
- 향상된 알림, 이벤트 및 임계값 인프라
- LDAP, LDAPS, SAML 인증 및 로컬 사용자 지원
- RBAC(사전 정의된 역할 세트)
- AutoSupport 및 지원 번들
- 환경의 용량, 가용성, 보호 및 성능 상태를 보여 주는 향상된 대시보드
- 볼륨 이동 상호 운용성, 볼륨 이동 기록, 접합 경로 변경 내역
- 일부 실패한 디스크, MetroCluster 애그리게이트 미러링 성능 저하, 이벤트 뒤에 남겨진 MetroCluster 스페어 디스크 등과 같은 이벤트에 영향을 받는 리소스를 그래픽으로 표시하는 영향 범위의 영역입니다
- MetroCluster 이벤트의 효과를 표시하는 가능한 효과 영역입니다
- 일부 실패한 디스크, MetroCluster 애그리게이트 미러링 성능 저하 및 이벤트 뒤에 남겨진 MetroCluster 스페어 디스크와 같은 이벤트를 해결하기 위해 수행할 수 있는 작업을 표시하는 권장 해결 조치 영역

- Volume Offline 이벤트, Volume Restricted 이벤트 및 Thin-provisioned Volume Space at Risk 이벤트와 같은 이벤트에 영향을 미칠 수 있는 리소스를 표시하는 영향받는 영역입니다
- FlexVol 또는 FlexGroup 볼륨에서 SVM 지원
- 노드 루트 볼륨 모니터링 지원
- 재확보 가능한 공간 계산 및 스냅샷 복사본 삭제를 비롯한 향상된 스냅샷 복사본 모니터링
- 스토리지 객체에 대한 주석
- 물리적 및 논리적 용량, 활용률, 공간 절감, 성능, 관련 이벤트와 같은 스토리지 오브젝트 정보의 생성 및 관리를 보고합니다
- OnCommand Workflow Automation와 통합하여 워크플로우 실행

  스토리지 자동화 스토어에는 WFA(OnCommand Workflow Automation)와 함께 사용하도록 개발된 NetApp 인증 자동 스토리지 워크플로우 팩이 포함되어 있습니다. 팩을 다운로드한 다음 WFA로 가져와 실행할 수 있습니다. 자동화된 워크플로우는 여기에서 확인할 수 있습니다.

  "스토리지 자동화 스토어"

스토리지 시스템 상태를 관리하는 데 사용되는 **Unified Manager** 인터페이스

이 섹션에는 Active IQ Unified Manager에서 데이터 스토리지 용량, 가용성 및 보호 문제를 해결하기 위해 제공하는 두 가지 사용자 인터페이스에 대한 정보가 포함되어 있습니다. UI 두 개는 Unified Manager 웹 UI와 유지보수 콘솔입니다.

Unified Manager의 보호 기능을 사용하려면 WFA(OnCommand Workflow Automation)도 설치 및 구성해야 합니다.

Unified Manager 웹 **UI**

관리자는 Unified Manager 웹 UI를 사용하여 데이터 스토리지 용량, 가용성 및 보호와 관련된 클러스터 문제를 모니터링하고 해결할 수 있습니다.

다음 섹션에서는 관리자가 Unified Manager 웹 UI에 표시되는 스토리지 용량, 데이터 가용성 또는 보호 문제를 해결하기 위해 수행할 수 있는 몇 가지 일반적인 워크플로우에 대해 설명합니다.

유지보수 콘솔

관리자는 Unified Manager 유지보수 콘솔을 사용하여 Unified Manager 서버 자체와 관련된 운영 체제 문제, 버전 업그레이드 문제, 사용자 액세스 문제, 네트워크 문제를 모니터링, 진단, 해결할 수 있습니다. Unified Manager 웹 UI를 사용할 수 없는 경우에는 유지보수 콘솔만 Unified Manager에 액세스할 수 있습니다.

이 정보를 사용하여 유지보수 콘솔에 액세스하고 Unified Manager 서버 기능과 관련된 문제를 해결할 수 있습니다.

클러스터 및 클러스터 객체 상태 관리 및 모니터링

Unified Manager는 주기적인 API 쿼리 및 데이터 수집 엔진을 사용하여 클러스터에서 데이터를 수집합니다. Unified Manager 데이터베이스에 클러스터를 추가하면 가용성 및 용량 위험에 대한 클러스터를 모니터링하고 관리할 수 있습니다.

클러스터 모니터링 이해

Unified Manager 데이터베이스에 클러스터를 추가하여 가용성, 용량 및 기타 세부 정보(예: CPU 사용, 인터페이스 통계, 사용 가능한 디스크 공간, qtree 사용, 섀시 환경)를 클러스터에서 모니터링할 수 있습니다.

상태가 비정상이거나 사전 정의된 임계값이 위반되는 경우 이벤트가 생성됩니다. 그렇게 하도록 구성된 경우 Unified Manager는 이벤트가 경고를 트리거할 때 지정된 수신자에게 알림을 보냅니다.

노드 루트 볼륨 이해

Unified Manager를 사용하여 노드 루트 볼륨을 모니터링할 수 있습니다. 모범 사례는 노드 루트 볼륨에 노드가 중지되는 것을 방지할 수 있는 충분한 용량이 있어야 한다는 것입니다.

노드 루트 볼륨의 사용된 용량이 총 노드 루트 볼륨 용량의 80%를 초과하면 노드 루트 볼륨 공간 거의 꽉 참 이벤트가 생성됩니다. 알림을 받도록 이벤트에 대한 알림을 구성할 수 있습니다. ONTAP System Manager 또는 ONTAP CLI를 사용하여 노드가 중지되는 것을 방지하기 위해 적절한 조치를 취할 수 있습니다.

> 클러스터에서 ONTAP 9.14.1 버전 이상을 실행하는 경우에는 노드 루트 볼륨 모니터링 기능을 사용할 수 없습니다.

노드 루트 애그리게이트에 대한 이벤트 및 임계값 이해

Unified Manager를 사용하여 노드 루트 애그리게이트를 모니터링할 수 있습니다. 노드를 중단하는 것을 방지하기 위해 루트 애그리게이트에 루트 볼륨을 두껍게 프로비저닝하는 것이 가장 좋습니다.

기본적으로 용량 및 성능 이벤트는 루트 애그리게이트에 대해 생성되지 않습니다. 또한 Unified Manager에서 사용하는 임계값은 노드 루트 애그리게이트에 적용할 수 없습니다. 기술 지원 담당자만 생성할 이벤트에 대한 설정을 수정할 수 있습니다. 기술 지원 담당자가 설정을 수정하면 용량 임계값이 노드 루트 애그리게이트에 적용됩니다.

ONTAP System Manager 또는 ONTAP CLI를 사용하여 노드를 중단하는 것을 방지하기 위한 적절한 조치를 취할 수 있습니다.

> 클러스터에서 ONTAP 9.14.1 버전 이상을 실행하는 경우 노드 루트 애그리게이트 모니터링 기능을 사용할 수 없습니다.

쿼럼 및 **epsilon** 이해

쿼럼 및 epsilon은 클러스터 상태 및 기능의 중요한 측정치로서, 클러스터를 통해 잠재적인 통신 및 연결 문제를 해결하는 방법을 함께 나타냅니다.

_Quorum_은 완전히 작동하는 클러스터를 위한 전제 조건입니다. 클러스터가 쿼럼에 있으면 대부분의 노드가 정상 상태이며 서로 통신할 수 있습니다. 쿼럼이 손실되면 클러스터는 정상적인 클러스터 작업을 수행할 수 없게 됩니다. 모든 노드가 데이터의 단일 뷰를 공유하므로 한 번에 하나의 노드 집합만 쿼럼을 가질 수 있습니다. 따라서 서로 통신하지 않는 두 개의 노드가 서로 다른 방식으로 데이터를 수정할 수 있는 경우 더 이상 데이터를 단일 데이터 뷰로 조정할 수 없습니다.

클러스터의 각 노드는 하나의 노드 마스터를 선택하는 투표 프로토콜에 참여하며, 나머지 각 노드는 보조 노드입니다.

마스터 노드는 클러스터 전체에서 정보를 동기화하는 역할을 합니다. 쿼럼이 형성되면 투표가 계속된다. 마스터 노드가 오프라인이 되고 클러스터가 여전히 쿼럼에 있으면 새 마스터는 온라인 상태로 유지되는 노드에 의해 선택됩니다.

노드의 수가 짝수인 클러스터에서 타이 가능성이 있기 때문에 노드 하나에 epsilon이라는 추가 분수 투표 중량이 있습니다. 대규모 클러스터의 동일한 두 부분 간의 연결이 실패할 경우 epsilon이 포함된 노드 그룹은 모든 노드가 정상 상태라고 가정하고 quorum을 유지합니다. 예를 들어, 다음 그림에서는 노드 2개에 장애가 발생한 4노드 클러스터를 보여 줍니다. 그러나 남아 있는 노드 중 하나가 epsilon을 보유하기 때문에 양호한 노드의 대부분이 단순하지 않더라도 클러스터가 쿼럼에 남아 있습니다.

Epsilon은 클러스터를 생성할 때 첫 번째 노드에 자동으로 할당됩니다. epsilon이 있는 노드가 정상 상태가 아니거나 고가용성 파트너를 인수하거나 고가용성 파트너가 인수하는 경우 epsilon은 다른 HA 쌍의 정상 노드에 자동으로 재할당됩니다.

노드를 오프라인 상태로 전환하면 클러스터의 쿼럼 유지 기능에 영향을 줄 수 있습니다. 따라서 클러스터를 쿼럼에서 제외시키거나 quorum이 손실된 상태에서 한 번의 작동 중지가 발생하지 않는 작업을 시도할 경우 ONTAP에서 경고 메시지를 표시합니다. 클러스터 quorum-service options modify 명령을 고급 권한 수준에서 사용하여 quorum 경고 메시지를 비활성화할 수 있습니다.

일반적으로, 클러스터의 노드 간에 안정적인 연결을 가정하면 더 큰 클러스터는 더 작은 클러스터보다 더 안정적입니다. 노드 과반수의 단순한 정수에 epsilon을 더한 quorum 요구 사항은 노드 2개로 구성된 클러스터보다 노드 24개로 구성된 클러스터에서 유지하기가 더 쉽습니다.

2노드 클러스터는 쿼럼을 유지 관리하는 데 몇 가지 고유한 문제를 제시합니다. 2노드 클러스터는 어떠한 노드도 epsilon을 보유하지 않는 클러스터 HA를 사용합니다. 대신 두 노드는 모두 지속적으로 폴링되므로 하나의 노드에 장애가 발생할 경우 다른 노드가 데이터에 대한 읽기-쓰기 액세스 권한을 완벽하게 갖추고 논리 인터페이스 및 관리 기능에 액세스할 수 있습니다.

클러스터 목록 및 세부 정보 보기

상태: 모든 클러스터 보기를 사용하여 클러스터의 인벤토리를 볼 수 있습니다. Capacity:All Clusters 보기를 사용하면 모든 클러스터의 스토리지 용량 및 활용도에 대한 요약된 정보를 볼 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

또한 클러스터 상태, 용량, 구성, LIF, 노드 등과 같은 개별 클러스터에 대한 세부 정보를 볼 수 있습니다. 클러스터/상태 세부 정보 페이지를 사용하여 해당 클러스터의 디스크를 확인합니다.

상태: 모든 클러스터 보기, 용량: 모든 클러스터 보기 및 클러스터/상태 세부 정보 페이지의 세부 정보를 통해 스토리지를 계획할 수 있습니다. 예를 들어 새 Aggregate를 프로비저닝하기 전에 Health: All Clusters 보기에서 특정 클러스터를 선택하고 용량 세부 정보를 확인하여 클러스터에 필요한 공간이 있는지 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.
2. 보기 메뉴에서 * 상태: 모든 클러스터 * 보기를 선택하여 상태 정보를 보거나 * 용량: 모든 클러스터 * 보기를 선택하여 모든 클러스터의 스토리지 용량 및 활용도에 대한 세부 정보를 봅니다.
3. 클러스터 이름을 클릭하면 * Cluster/Health * 세부 정보 페이지에서 클러스터의 전체 세부 정보를 볼 수 있습니다.
    - 관련 정보 *
    - "클러스터/상태 세부 정보 페이지"
    - "성능: 모든 클러스터 보기"
    - "MetroCluster 구성 모니터링"
    - "클러스터 및 스토리지 VM의 보안 상태 보기"
    - "평가 대상 보안 기준"

MetroCluster 구성에서 클러스터 상태 확인

Active IQ Unified Manager(Unified Manager)를 사용하면 MetroCluster over FC 및 MetroCluster over IP 구성에서 클러스터의 운영 상태와 해당 구성요소를 확인할 수 있습니다. 클러스터가 Unified Manager에서 감지한 성능 이벤트에 참여한 경우 상태 를 통해 하드웨어 또는 소프트웨어 문제가 이벤트에 기여했는지 여부를 확인할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- MetroCluster 구성에 대한 성능 이벤트를 분석하고 관련 클러스터의 이름을 확인해야 합니다.
- FC와 IP를 통해 MetroCluster 구성의 두 클러스터는 동일한 Unified Manager 인스턴스에서 모니터링해야 합니다.

FC를 통한 MetroCluster 구성의 클러스터 상태 확인

FC를 통한 MetroCluster 구성의 클러스터 상태를 확인하려면 다음 단계를 따르십시오.

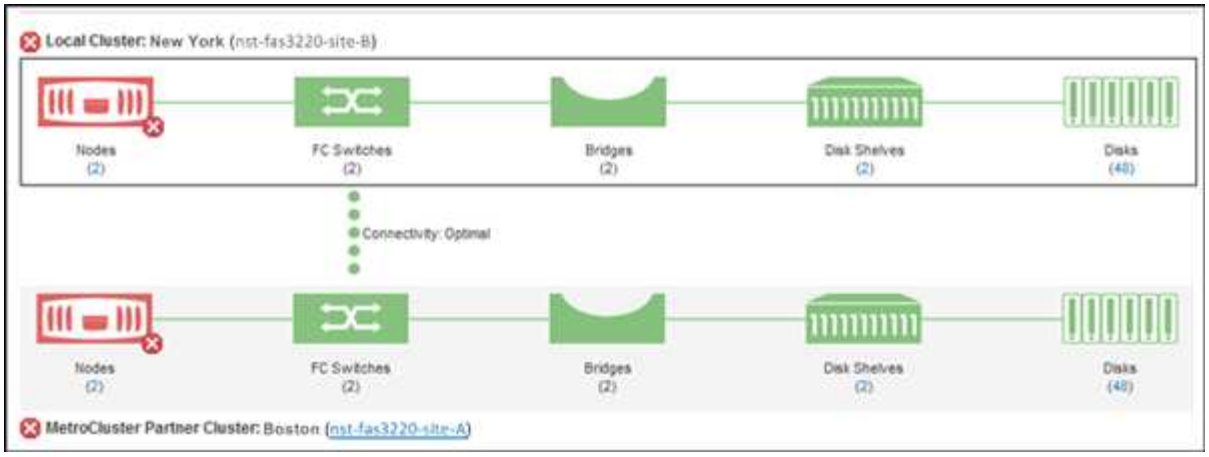
단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭하여 이벤트 목록을 표시합니다.
2. 필터 패널의 * 소스 유형 * 범주 아래에서 모든 MetroCluster 필터를 선택합니다. 모든 MetroCluster 구성에 대해 사용자 환경에서 발생한 모든 이벤트를 볼 수 있습니다.
3. MetroCluster 이벤트 옆에 있는 클러스터의 이름을 클릭합니다.

    MetroCluster 이벤트가 표시되지 않으면 검색 표시줄을 사용하여 FC를 통한 MetroCluster 구성과 관련된 이벤트와 관련된 클러스터의 이름을 검색할 수 있습니다.

    상태: 모든 클러스터 보기가 이벤트에 대한 자세한 정보와 함께 표시됩니다.

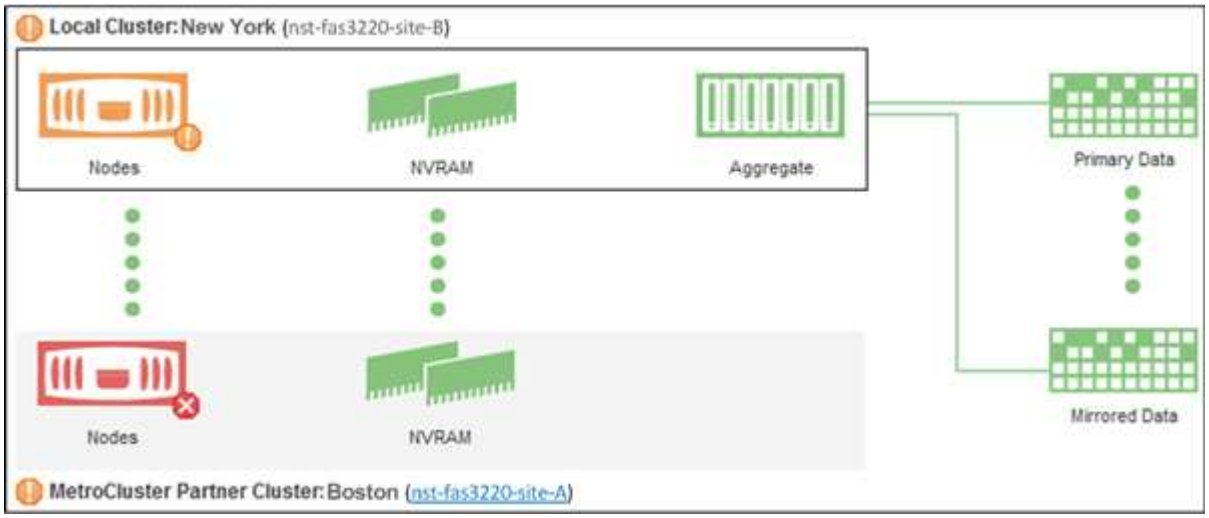
4. 선택한 클러스터와 파트너 클러스터 간의 연결 상태를 표시하려면 * MetroCluster 연결 * 탭을 선택합니다.



이 예에서는 로컬 클러스터와 파트너 클러스터의 이름과 구성 요소가 표시됩니다. 노란색 또는 빨간색 아이콘은 강조 표시된 구성 요소에 대한 상태 이벤트를 나타냅니다. 연결 아이콘은 클러스터 간의 링크를 나타냅니다. 마우스 커서를 아이콘에 갖다 대면 이벤트 정보를 표시하거나 아이콘을 클릭하여 이벤트를 표시할 수 있습니다. 두 클러스터의 상태 문제가 성능 이벤트에 영향을 줄 수 있습니다.

Unified Manager는 클러스터 간 링크의 NVRAM 구성 요소를 모니터링합니다. 로컬 또는 파트너 클러스터의 FC 스위치 아이콘 또는 연결 아이콘이 빨간색인 경우 링크 상태 문제로 인해 성능 이벤트가 발생했을 수 있습니다.

5. MetroCluster 복제 * 탭을 선택합니다.



이 예제에서 로컬 또는 파트너 클러스터의 NVRAM 아이콘이 노란색 또는 빨간색이면 NVRAM의 상태 문제로 인해 성능 이벤트가 발생했을 수 있습니다. 페이지에 빨간색 또는 노란색 아이콘이 없을 경우 파트너 클러스터의 성능 문제로 인해 성능 이벤트가 발생했을 수 있습니다.

MetroCluster over IP 구성에서 클러스터 상태 확인

MetroCluster over IP 구성에서 클러스터 상태를 확인하려면 다음 단계를 수행하십시오.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭하여 이벤트 목록을 표시합니다.
2. 필터 패널의 * 소스 유형 * 범주에서 을 선택합니다 `MetroCluster Relationship` 필터. 모든 MetroCluster 구성에 대해 사용자 환경에서 발생한 모든 이벤트를 볼 수 있습니다.

보고된 MetroCluster 이벤트를 볼 수 없는 경우 검색 표시줄을 사용하여 IP를 통한 MetroCluster 구성과 관련된 이벤트에 관련된 클러스터 이름을 검색할 수 있습니다.

3. 관련 MetroCluster 이벤트 옆에 있는 클러스터의 이름을 클릭합니다. 클러스터 페이지가 해당 클러스터의 세부 정보와 함께 표시됩니다. 상태 문제 확인에 대한 자세한 내용은 을 참조하십시오 "MetroCluster over IP 구성에서 연결 문제를 모니터링합니다".

모든 **SAN** 어레이 클러스터의 상태 및 용량 상태 보기

클러스터 인벤토리 페이지를 사용하여 모든 SAN 어레이 클러스터의 상태 및 용량 상태를 표시할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

상태: 모든 클러스터 보기 및 용량: 모든 클러스터 보기에서 모든 SAN 어레이 클러스터에 대한 개요 정보를 볼 수 있습니다. 또한 클러스터/상태 세부 정보 페이지에서 세부 정보를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.
2. 상태: 모든 클러스터 * 보기에 ""개인 정보" 열이 표시되어 있는지 확인하거나 * 표시/숨기기 * 컨트롤을 사용하여 추가하십시오.

   이 열에는 모든 SAN 어레이 클러스터에 대한 ""모든 SAN 어레이""가 표시됩니다.
3. 정보를 검토합니다.
4. 해당 클러스터의 스토리지 용량에 대한 정보를 보려면 Capacity:All Clusters 보기를 선택합니다.
5. 해당 클러스터의 상태 및 스토리지 용량에 대한 자세한 정보를 보려면 All SAN Array 클러스터의 이름을 클릭합니다.

   클러스터/상태 세부 정보 페이지의 상태, 용량 및 노드 탭에서 세부 정보를 봅니다

노드 목록 및 세부 정보 보기

상태: 모든 노드 보기를 사용하여 클러스터의 노드 목록을 볼 수 있습니다. 클러스터/상태 세부 정보 페이지를 사용하여 모니터링되는 클러스터의 일부인 노드에 대한 자세한 정보를 볼 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

노드 상태, 노드가 포함된 클러스터, 애그리게이트 용량 세부 정보(사용된 용량 및 총 용량), 물리적 용량 세부 정보(사용 가능, 스페어, 총 용량)와 같은 세부 정보를 볼 수 있습니다. HA 쌍, 디스크 쉘프 및 포트에 대한 정보도 얻을 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 노드 * 를 클릭합니다.
2. 상태: 모든 노드 * 보기에서 세부 정보를 보려는 노드를 클릭합니다.

   선택한 노드에 대한 자세한 정보가 클러스터/상태 세부 정보 페이지에 표시됩니다. 왼쪽 창에는 HA 쌍 목록이 표시됩니다. 기본적으로 HA Details는 열려 있어 HA 상태 세부 정보와 선택한 HA 쌍과 관련된 이벤트를 표시합니다.

3. 노드에 대한 다른 세부 정보를 보려면 적절한 작업을 수행합니다.

보기...	클릭...
디스크 쉘프 세부 정보	디스크 쉘프 *.
포트 관련 정보입니다	포트 *.

자세한 내용은 다음을 참조하십시오.

- "성능: 모든 노드 보기"
- "노드 및 애그리게이트 가용 IOPS 값 보기"
- "사용된 노드 및 총 성능 용량 값 보기"

계약 갱신을 위한 하드웨어 인벤토리 보고서를 생성하는 중입니다

하드웨어 모델 번호 및 일련 번호, 디스크 유형 및 개수, 설치된 라이센스 등 클러스터와 노드 정보의 전체 목록이 포함된 보고서를 생성할 수 있습니다. 이 보고서는 NetAppActive IQ 플랫폼에 연결되어 있지 않은 보안 사이트("표시" 사이트) 내의 계약 갱신을 위해 유용합니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 노드 * 를 클릭합니다.
2. 상태: 모든 노드 * 보기 또는 * 성능: 모든 노드 * 보기로 이동합니다.
3. Reports * > * > Hardware Inventory Report * 를 선택합니다.

   하드웨어 인벤토리 보고서는 현재 날짜를 기준으로 완전한 정보가 포함된 .csv 파일로 다운로드됩니다.

4. 계약 갱신을 위해 NetApp 지원 담당자에게 이 정보를 제공합니다.

스토리지 **VM** 목록 및 세부 정보 보기

상태: 모든 스토리지 VM 보기에서 스토리지 가상 시스템(SVM)의 인벤토리를 모니터링할 수 있습니다. 스토리지 VM/상태 세부 정보 페이지를 사용하여 모니터링되는 SVM에 대한 자세한 정보를 볼 수 있습니다.

• 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

SVM의 용량, 효율성, 구성과 같은 SVM 세부 정보를 확인할 수 있습니다. 관련 장치에 대한 정보와 해당 SVM에 대한 관련 경고를 볼 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 스토리지 VM * 을 클릭합니다.
2. 다음 방법 중 하나를 선택하여 SVM 세부 정보를 확인하십시오.
   - 모든 클러스터에 있는 모든 SVM의 상태에 대한 정보를 보려면 보기 메뉴에서 상태: 모든 스토리지 VM 보기 를 선택합니다.
   - 전체 세부 정보를 보려면 스토리지 VM 이름을 클릭합니다.

     세부 정보 대화 상자에서 * 세부 정보 보기 * 를 클릭하여 전체 세부 정보를 볼 수도 있습니다.
3. 최소 세부 정보 대화 상자에서 * 관련 항목 보기 * 를 클릭하여 SVM 관련 객체를 확인합니다.
   - 관련 정보 *
   - "스토리지 VM: 상태 세부 정보 페이지"
   - "성능: 모든 스토리지 VM 보기"
   - "보안: 랜섬웨어 차단 뷰"
   - "클러스터 및 스토리지 VM의 보안 상태 보기"
   - "관계: 모든 관계 보기"

집계 목록 및 세부 정보 보기

상태: 모든 집계 보기에서 집계 인벤토리를 모니터링할 수 있습니다. Capacity:All 애그리게이트 보기에서는 모든 클러스터에서 애그리게이트의 용량 및 활용률에 대한 정보를 볼 수 있습니다.

• 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

애그리게이트 용량 및 구성, 그리고 애그리게이트/상태 세부 정보 페이지에서 디스크 정보와 같은 세부 정보를 볼 수 있습니다. 필요한 경우 임계값 설정을 구성하기 전에 이러한 세부 정보를 사용할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. 다음 방법 중 하나를 선택하여 애그리게이트 세부 정보를 봅니다.
   - 모든 클러스터의 모든 집계 상태에 대한 정보를 보려면 보기 메뉴에서 상태: 모든 집계 보기 를 선택합니다.
   - 모든 클러스터의 모든 애그리게이트 용량 및 활용률에 대한 정보를 보려면 보기 메뉴에서 용량: 모든 애그리게이트 보기 를 선택합니다.
   - 전체 세부 정보를 보려면 애그리게이트 이름을 클릭합니다.

세부 정보 대화 상자에서 * 세부 정보 보기 * 를 클릭하여 전체 세부 정보를 볼 수도 있습니다.

3. Minimal details(최소 세부 정보) 대화 상자에서 * View related * (관련 항목 보기)를 클릭하여 집계와 관련된 개체를 봅니다.
   - 관련 정보 *
   - "집계/상태 세부 정보 페이지"
   - "성능: 모든 애그리게이트 보기"
   - "애그리게이트 용량 보고서 사용자 지정"

FabricPool 용량 정보 보기

용량 및 성능 인벤토리에서 클러스터, 애그리게이트 및 볼륨의 FabricPool 용량 정보와 이러한 개체에 대한 세부 정보 페이지를 볼 수 있습니다. 이 페이지에는 미러 계층이 구성된 경우 FabricPool 미러 정보도 표시됩니다.

이 페이지에는 로컬 성능 계층 및 클라우드 계층에서 사용 가능한 용량, 두 계층에서 사용 중인 용량, 애그리게이트가 클라우드 계층에 연결된 용량 등의 정보가 표시됩니다. 어떤 볼륨이 특정 정보를 클라우드 계층으로 이동하여 FabricPool 기능을 구현할지,

클라우드 계층이 다른 클라우드 공급자("미러 계층")로 미러링되면 두 클라우드 계층이 모두 애그리게이트/상태 세부 정보 페이지에 표시됩니다.

단계

1. 다음 중 하나를 수행합니다.

용량 정보를 보려면...	수행할 작업...
클러스터	a. Capacity: All Clusters(용량: 모든 클러스터) 보기에서 클러스터를 클릭합니다. b. 클러스터/상태 세부 정보 페이지에서 * 구성 * 탭을 클릭합니다. 이 화면에는 이 클러스터가 연결된 모든 클라우드 계층의 이름이 표시됩니다.

용량 정보를 보려면...	수행할 작업...
애그리게이트	a. Capacity:All Aggregates 보기에서 Type 필드에 "SSD(FabricPool)" 또는 "HDD(FabricPool)"가 표시된 애그리게이트를 클릭합니다. b. 집계/상태 세부 정보 페이지에서 * 용량 * 탭을 클릭합니다. 이 화면에는 클라우드 계층에서 사용된 총 용량이 표시됩니다. c. 디스크 정보 * 탭을 클릭합니다. 이 화면에는 클라우드 계층의 이름과 사용된 용량이 표시됩니다. d. Configuration * 탭을 클릭합니다. 이 화면에는 클라우드 계층의 이름과 클라우드 계층에 대한 기타 자세한 정보가 표시됩니다.
볼륨	a. Capacity:All Volumes 보기에서 "Tiering Policy" 필드에 정책 이름이 표시되는 볼륨을 클릭합니다. b. 볼륨/상태 세부 정보 페이지에서 * 구성 * 탭을 클릭합니다. 이 화면에는 볼륨에 할당된 FabricPool 계층화 정책의 이름이 표시됩니다.

2. Workload Analysis * 페이지에서 * Capacity Trend * 영역에서 ""클라우드 계층 보기"를 선택하여 이전 달의 로컬 성능 계층과 클라우드 계층에서 사용되는 용량을 확인할 수 있습니다.

FabricPool Aggregate에 대한 자세한 내용은 를 참조하십시오 "디스크 및 애그리게이트 개요".

스토리지 풀 세부 정보 보기

스토리지 풀의 세부 정보를 보고 스토리지 풀 상태, 총 캐시 및 사용 가능한 캐시, 사용된 할당 및 사용 가능한 할당을 모니터링할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. 애그리게이트 이름을 클릭합니다.

   선택한 애그리게이트의 세부 정보가 표시됩니다.

3. 디스크 정보 * 탭을 클릭합니다.

   자세한 디스크 정보가 표시됩니다.

   캐시 테이블은 선택한 애그리게이트에서 스토리지 풀을 사용 중인 경우에만 표시됩니다.

4. 캐시 테이블에서 포인터를 필요한 스토리지 풀의 이름 위로 이동합니다.

   스토리지 풀의 세부 정보가 표시됩니다.

볼륨 목록 및 세부 정보 보기

상태: 모든 볼륨 보기에서 볼륨 인벤토리를 모니터링할 수 있습니다. Capacity:All Volumes 보기를 사용하면 클러스터의 볼륨 용량 및 활용도에 대한 정보를 볼 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨/상태 세부 정보 페이지를 사용하여 볼륨의 용량, 효율성, 구성 및 보호를 비롯하여 모니터링되는 볼륨에 대한 자세한 정보를 볼 수도 있습니다. 특정 볼륨에 대한 관련 장치 및 관련 경고에 대한 정보도 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 다음 방법 중 하나를 선택하여 볼륨 세부 정보를 봅니다.
   - 클러스터의 볼륨 상태에 대한 자세한 정보를 보려면 보기 메뉴에서 상태: 모든 볼륨 보기를 선택합니다.
   - 클러스터의 볼륨 용량 및 활용도에 대한 자세한 정보를 보려면 보기 메뉴에서 용량: 모든 볼륨 보기를 선택합니다.
   - 전체 세부 정보를 보려면 볼륨 이름을 클릭합니다.

     세부 정보 대화 상자에서 * 세부 정보 보기 * 를 클릭하여 전체 세부 정보를 볼 수도 있습니다.
3. * 선택 사항: * 최소 세부 정보 대화 상자에서 * 관련 항목 보기 * 를 클릭하여 볼륨과 관련된 개체를 봅니다.
   - 관련 정보 *
   - "볼륨: 상태 세부 정보 페이지"
   - "성능: 모든 볼륨 보기"
   - "보안: 랜섬웨어 차단 뷰"
   - "볼륨 보호 관계 보기"
   - "보고서를 생성하여 사용 가능한 볼륨 용량 차트를 표시합니다"

NFS 공유에 대한 세부 정보 보기

상태, 볼륨과 연결된 경로(FlexGroup 볼륨 또는 FlexVol 볼륨), NFS 공유에 대한 클라이언트의 액세스 수준, 내보낸 볼륨에 대해 정의된 엑스포트 정책과 같은 모든 NFS 공유에 대한 세부

정보를 볼 수 있습니다. 상태: 모든 NFS 공유 보기를 사용하여 모니터링되는 모든 클러스터에서 모든 NFS 공유를 확인하고, 스토리지 VM/상태 세부 정보 페이지를 사용하여 특정 SVM(스토리지 가상 머신)의 모든 NFS 공유를 볼 수 있습니다.

- 필요한 것 *
- 클러스터에서 NFS 라이센스를 설정해야 합니다.
- NFS 공유를 지원하는 네트워크 인터페이스를 구성해야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 모든 NFS 공유를 표시할지, 아니면 특정 SVM에 대한 NFS 공유만 표시할지 여부에 따라 아래 단계를 수행합니다.

대상...	다음 단계를 따르십시오...
모든 NFS 공유를 표시합니다	스토리지 * > * NFS 공유 * 를 클릭합니다
단일 SVM에서 NFS 공유 보기	a. 스토리지 * > * 스토리지 VM * 을 클릭합니다 b. NFS 공유 세부 정보를 확인할 SVM을 클릭합니다. c. 스토리지 VM/상태 세부 정보 페이지에서 * NFS 공유 * 탭을 클릭합니다.

자세한 내용은 을 참조하십시오 "파일 공유 볼륨 프로비저닝" 및 "API를 사용하여 CIFS 및 NFS 파일 공유 프로비저닝".

SMB/CIFS 공유에 대한 세부 정보 보기

공유 이름, 연결 경로, 객체 포함, 보안 설정 및 공유에 대해 정의된 내보내기 정책과 같은 모든 SMB/CIFS 공유에 대한 세부 정보를 볼 수 있습니다. 상태: 모든 SMB 공유 보기를 사용하여 모니터링되는 모든 클러스터에서 모든 SMB 공유를 확인하고, 스토리지 VM/상태 세부 정보 페이지를 사용하여 특정 SVM(스토리지 가상 머신)의 모든 SMB 공유를 볼 수 있습니다.

- 필요한 것 *
- 클러스터에서 CIFS 라이센스를 설정해야 합니다.
- SMB/CIFS 공유를 지원하는 네트워크 인터페이스를 구성해야 합니다.
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

ⓘ 폴더의 공유가 표시되지 않습니다.

단계

1. 왼쪽 탐색 창에서 모든 SMB/CIFS 공유를 표시할지, 아니면 특정 SVM에 대한 공유만 표시할지 여부에 따라 아래 단계를 수행합니다.

대상...	다음 단계를 따르십시오...
모든 SMB/CIFS 공유를 표시합니다	스토리지 * > * SMB 공유 * 를 클릭합니다
단일 SVM에서 SMB/CIFS 공유 보기	a. 스토리지 * > * 스토리지 VM * 을 클릭합니다 b. SMB/CIFS 공유 세부 정보를 확인할 SVM을 클릭합니다. c. 스토리지 VM/상태 세부 정보 페이지에서 * SMB 공유 * 탭을 클릭합니다.

자세한 내용은 을 참조하십시오 "API를 사용하여 CIFS 및 NFS 파일 공유 프로비저닝".

스냅샷 복사본 목록 보기

선택한 볼륨의 스냅샷 복사본 목록을 볼 수 있습니다. 스냅샷 복사본 목록을 사용하여 하나 이상의 스냅샷 복사본이 삭제된 경우 재확보된 디스크 공간 크기를 계산할 수 있으며, 필요한 경우 스냅샷 복사본을 삭제할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스냅샷 복사본이 포함된 볼륨이 온라인 상태여야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 상태: 모든 볼륨 * 보기에서 보려는 스냅샷 복사본이 포함된 볼륨을 선택합니다.
3. 볼륨/상태 * 세부 정보 페이지에서 * 용량 * 탭을 클릭합니다.
4. Capacity * 탭의 * Details * 창에서 Other Details 섹션에서 * Snapshot Copies * 옆에 있는 링크를 클릭합니다.

   스냅샷 복사본 수는 스냅샷 복사본 목록을 표시하는 링크입니다.

   ◦ 관련 정보 *

"상태/볼륨 페이지입니다"

스냅샷 복사본 삭제

공간을 절약하거나 디스크 공간을 확보하기 위해 스냅샷 복사본을 삭제하거나, 더 이상 필요하지 않은 스냅샷 복사본을 삭제할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨이 온라인 상태여야 합니다.

사용 중이거나 잠겨 있는 스냅샷 복사본을 삭제하려면 사용 중인 애플리케이션에서 스냅샷 복사본을 릴리즈해야 합니다.

- FlexClone 볼륨이 해당 스냅샷 복사본을 사용 중인 경우 상위 볼륨의 기본 스냅샷 복사본을 삭제할 수 없습니다.

  기본 스냅샷 복사본은 FlexClone 볼륨을 만드는 데 사용되는 스냅샷 복사본이며 상위 볼륨에서 "사용 중" 및 애플리케이션 의존성 상태를 "사용 중, 클론"으로 표시합니다.

- SnapMirror 관계에 사용되는 잠긴 스냅샷 복사본은 삭제할 수 없습니다.

  스냅샷 복사본은 잠겨 있으며 다음 업데이트에 필요합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 상태: 모든 볼륨 * 보기에서 보려는 스냅샷 복사본이 포함된 볼륨을 선택합니다.

   스냅샷 복사본 목록이 표시됩니다.

3. 볼륨/상태 * 세부 정보 페이지에서 * 용량 * 탭을 클릭합니다.
4. Capacity * 탭의 * Details * 창에서 Other Details 섹션에서 * Snapshot Copies * 옆에 있는 링크를 클릭합니다.

   스냅샷 복사본 수는 스냅샷 복사본 목록을 표시하는 링크입니다.

5. Snapshot 복사본 * 보기에서 삭제할 스냅샷 복사본을 선택한 다음 * 선택 항목 삭제 * 를 클릭합니다.

스냅샷 복사본에 대한 재확보 가능한 공간 계산

하나 이상의 스냅샷 복사본이 삭제된 경우 회수할 수 있는 디스크 공간의 양을 계산할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 볼륨이 온라인 상태여야 합니다.
- 볼륨은 FlexVol 볼륨이어야 하며, FlexGroup 볼륨에서는 이 기능이 지원되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 상태: 모든 볼륨 * 보기에서 보려는 스냅샷 복사본이 포함된 볼륨을 선택합니다.

   스냅샷 복사본 목록이 표시됩니다.

3. 볼륨/상태 * 세부 정보 페이지에서 * 용량 * 탭을 클릭합니다.
4. Capacity * 탭의 * Details * 창에서 Other Details 섹션에서 * Snapshot Copies * 옆에 있는 링크를 클릭합니다.

   스냅샷 복사본 수는 스냅샷 복사본 목록을 표시하는 링크입니다.

5. Snapshot 복사본 * 보기에서 재확보 가능한 공간을 계산할 스냅샷 복사본을 선택합니다.
6. Calculate * 를 클릭합니다.

볼륨의 재확보 가능한 공간(백분율, KB, MB, GB 등)이 표시됩니다.

7. 반환 가능 공간을 다시 계산하려면 필요한 스냅샷 복사본을 선택하고 * 재계산 * 을 클릭합니다.

클러스터 객체 창 및 대화 상자에 대한 설명입니다

각 스토리지 오브젝트 페이지에서 모든 클러스터와 클러스터 오브젝트를 볼 수 있습니다. 해당 스토리지 객체 세부 정보 페이지에서 세부 정보를 볼 수도 있습니다. 이제 인벤토리의 다음 스토리지 및 보호 섹션에서 System Manager 사용자 인터페이스를 시작할 수 있습니다.

- 클러스터 인벤토리, 클러스터 상태 및 클러스터 성능 페이지를 표시합니다
- 인벤토리, 집계 상태 및 집계 성능 페이지
- 볼륨 인벤토리, 볼륨 상태 및 볼륨 성능 페이지
- 노드 인벤토리 및 노드 성능 페이지
- StorageVM 인벤토리, StorageVM 상태 및 StorageVM 성능 페이지
- 보호 관계 페이지

공통 **Unified Manager** 상태 워크플로우 및 작업

Unified Manager와 관련된 몇 가지 일반적인 관리 워크플로우 및 작업으로는 모니터링할 스토리지 클러스터 선택, 데이터 가용성, 용량 및 보호에 부정적인 영향을 미치는 조건 진단, 손실된 데이터 복원, 볼륨 구성 및 관리, 기술 지원(필요한 경우)에 진단 데이터를 번들로 제공 및 전송하는 작업이 있습니다.

스토리지 관리자는 Unified Manager를 사용하여 대시보드를 확인하고, 관리되는 스토리지 클러스터의 전체 용량, 가용성 및 보호 상태를 평가한 다음, 발생할 수 있는 특정 문제를 신속하게 식별, 검색, 진단 및 할당하여 해결할 수 있습니다.

스토리지 용량 또는 관리 대상 스토리지 오브젝트의 데이터 가용성에 영향을 미치는 클러스터, SVM(스토리지 가상 시스템), 볼륨 또는 FlexGroup 볼륨과 관련된 가장 중요한 문제는 대시보드 페이지의 시스템 상태 그래프 및 이벤트에 표시됩니다. 중요한 문제가 식별되면 이 페이지에서는 적절한 문제 해결 워크플로를 지원하는 링크를 제공합니다.

WFA(OnCommand Workflow Automation)와 같은 관련 관리 도구가 포함된 워크플로우에 Unified Manager를 포함하여 스토리지 리소스를 직접 구성할 수도 있습니다.

이 문서에서는 다음과 같은 관리 작업과 관련된 일반적인 워크플로에 대해 설명합니다.

- 가용성 문제 진단 및 관리

  하드웨어 장애 또는 스토리지 리소스 구성 문제로 인해 대시보드 페이지에 데이터 가용성 이벤트가 표시되는 경우 스토리지 관리자는 포함된 링크를 따라 영향을 받는 스토리지 리소스에 대한 연결 정보를 확인하고 문제 해결 조언을 확인하고 다른 관리자에게 문제 해결 방법을 할당할 수 있습니다.

- 성능 인시던트 구성 및 모니터링

  관리자는 모니터링 중인 스토리지 시스템 리소스의 성능을 모니터링하고 관리할 수 있습니다. 를 참조하십시오 "Active IQ Unified Manager 성능 모니터링 소개" 를 참조하십시오.

- 볼륨 용량 문제 진단 및 관리

  대시보드 페이지에 볼륨 스토리지 용량 문제가 표시되는 경우 스토리지 관리자는 포함된 링크를 따라 영향을 받는 볼륨의 스토리지 용량과 관련된 현재 및 과거 추세를 확인하고, 문제 해결 조언을 확인하고, 다른 관리자에게 문제 해결 방법을 할당할 수 있습니다.

- 보호 관계 문제 구성, 모니터링 및 진단

  보호 관계를 생성 및 구성한 후에는 스토리지 관리자가 보호 관계, 보호 관계의 현재 상태, 영향을 받는 관계에 대한 현재 및 과거의 보호 작업 성공 정보 및 문제 해결 조언과 관련된 잠재적인 문제를 볼 수 있습니다. 를 참조하십시오 "보호 관계 생성, 모니터링 및 문제 해결" 를 참조하십시오.

- 백업 파일을 생성하고 백업 파일에서 데이터를 복원합니다.
- 스토리지 객체를 주석과 연관

  스토리지 객체를 주석과 연결하여 스토리지 관리자는 스토리지 객체와 관련된 이벤트를 필터링하고 볼 수 있으므로 스토리지 관리자가 이벤트와 관련된 문제의 우선 순위를 지정하고 해결할 수 있습니다.

- REST API를 사용하여 Unified Manager에서 캡처한 상태, 용량 및 성능 정보를 확인하여 클러스터를 관리할 수 있습니다. 을 참조하십시오 "Active IQ Unified Manager REST API 시작하기" 를 참조하십시오.
- 기술 지원 팀에 지원 번들 보내기

  스토리지 관리자는 유지 관리 콘솔을 사용하여 지원 번들을 검색하고 기술 지원에 보낼 수 있습니다. 문제가 AutoSupport 메시지가 제공하는 것보다 더 자세한 진단 및 문제 해결이 필요한 경우 지원 번들을 기술 지원 부서에 보내야 합니다.

데이터 가용성 모니터링 및 문제 해결

Unified Manager는 권한이 있는 사용자가 저장된 데이터에 액세스할 수 있는 안정성을 모니터링하고, 해당 액세스를 차단하거나 방해하는 조건을 경고하며, 이러한 상태를 진단하고, 해결책을 할당 및 추적할 수 있도록 합니다.

이 섹션의 가용성 워크플로우 항목에서는 스토리지 관리자가 Unified Manager 웹 UI를 사용하여 데이터 가용성에 부정적인 영향을 미치는 하드웨어 및 소프트웨어 조건을 검색, 진단 및 할당하는 방법의 예를 설명합니다.

스토리지 페일오버 상호 연결 검색 및 해결 링크 다운 상태

이 워크플로우에서는 다운된 스토리지 페일오버 인터커넥트 링크 상태를 검색, 평가 및 해결하는 방법의 예를 제공합니다. 이 시나리오에서는 Unified Manager를 사용하여 노드에서 ONTAP 버전 업그레이드를 시작하기 전에 스토리지 페일오버 위험을 검사합니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

무중단 업그레이드 시도 중에 HA 쌍 노드 간 스토리지 페일오버 상호 연결이 실패할 경우 업그레이드가 실패합니다. 따라서 일반적으로 관리자는 업그레이드를 시작하기 전에 업그레이드 대상 클러스터 노드의 스토리지 페일오버 안정성을 모니터링하고 확인하는 것이 좋습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.
2. 이벤트 관리 * 재고 페이지에서 * 활성 가용성 이벤트 * 를 선택합니다.
3. 이벤트 관리 * 재고 페이지 * 이름 * 열의 맨 위에서 를 클릭합니다 텍스트 상자에 ' * failover'를 입력하여 이벤트를 스토리지 페일오버 관련 이벤트로 제한하십시오.

   스토리지 페일오버 조건과 관련된 모든 이전 이벤트가 표시됩니다.

   이 시나리오에서는 Unified Manager가 Availability Incidents 섹션에 "Storage Failover Interconnect One or More Links Down" 이벤트를 표시합니다.

4. 스토리지 페일오버와 관련된 하나 이상의 이벤트가 * Event Management * 인벤토리 페이지에 표시되는 경우 다음 단계를 수행하십시오.

   a. 이벤트 제목 링크를 클릭하여 해당 이벤트에 대한 이벤트 세부 정보를 표시합니다.

      이 예제에서는 이벤트 제목 "Storage Failover Interconnect One or more Links Down"을 클릭합니다.

   해당 이벤트에 대한 이벤트 세부 정보 페이지가 표시됩니다.

   a. 이벤트 세부 정보 페이지에서 다음 작업 중 하나 이상을 수행할 수 있습니다.
      - 원인 필드에서 오류 메시지를 검토하고 문제를 평가합니다.
      - 관리자에게 이벤트를 할당합니다.
      - 이벤트를 확인합니다.
        - 관련 정보 *

"이벤트 세부 정보 페이지"

"Unified Manager 사용자 역할 및 기능"

스토리지 페일오버 상호 연결에 대한 수정 조치를 수행하면 연결이 다운됩니다

스토리지 페일오버 관련 이벤트의 이벤트 세부 정보 페이지를 표시할 때 페이지의 요약 정보를 검토하여 이벤트의 긴급성, 문제의 가능한 원인 및 가능한 문제 해결 방법을 결정할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이 예제 시나리오에서는 이벤트 세부 정보 페이지에 제공된 이벤트 요약에 스토리지 페일오버 상호 연결 연결 연결 해제 상태에 대한 다음 정보가 포함됩니다.

```
Event: Storage Failover Interconnect One or More Links Down

Summary

Severity: Warning
State: New
Impact Level: Risk
Impact Area: Availability
Source: aardvark
Source Type: Node
Acknowledged By:
Resolved By:
Assigned To:
Cause: At least one storage failover interconnected link
       between the nodes aardvark and bonobo is down.
       RDMA interconnect is up (Link0 up, Link1 down)
```

예제 이벤트 정보는 HA 쌍 노드 aardvark와 bonobo 간의 스토리지 페일오버 상호 연결 링크 Link1이 중단되었지만 Apple과 Boy 사이의 link0이 활성 상태임을 나타냅니다. 하나의 링크가 활성화되었기 때문에 RDMA(원격 동적 메모리 액세스)가 계속 작동하고 있으며 스토리지 페일오버 작업을 계속 수행할 수 있습니다.

그러나 링크 장애 및 스토리지 페일오버 보호를 모두 완전히 비활성화하기 위해 Link1이 다운된 이유를 추가로 진단하기로 결정합니다.

단계

1. Event * details 페이지에서 Source 필드에 지정된 이벤트에 대한 링크를 클릭하여 스토리지 페일오버 상호 연결 링크 다운 상태와 관련된 다른 이벤트에 대한 자세한 정보를 얻을 수 있습니다.

   이 예제에서 이벤트의 소스는 aardvark라는 노드입니다. 이 노드 이름을 클릭하면 클러스터/상태 세부 정보 페이지의 노드 탭에 영향을 받는 HA 쌍, awardvark 및 bonobo에 대한 HA 세부 정보가 표시되고, 영향을 받는 HA 쌍에서 최근에 발생한 다른 이벤트가 표시됩니다.

2. 이벤트에 대한 자세한 내용은 * HA 세부 정보 * 를 참조하십시오.

   이 예제에서 관련 정보는 Events 테이블에 있습니다. 이 테이블에는 "스토리지 페일오버 연결 하나 이상의 링크 다운" 이벤트, 이벤트가 생성된 시간, 이 이벤트가 발생한 노드 등이 표시됩니다.

HA Details의 노드 위치 정보를 사용하여 영향을 받는 HA Pair 노드에서 스토리지 페일오버 문제의 물리적 검사 및 복구를 요청하거나 직접 수행합니다.

- 관련 정보 *

"이벤트 세부 정보 페이지"

"Unified Manager 사용자 역할 및 기능"

이 워크플로우에서는 Unified Manager가 이벤트 관리 인벤토리 페이지에 표시할 수 있는 볼륨 오프라인 이벤트를 평가하고 해결하는 방법의 예를 제공합니다. 이 시나리오에서는 Unified Manager를 사용하여 하나 이상의 볼륨 오프라인 이벤트 문제를 해결할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음과 같은 여러 가지 이유로 볼륨이 오프라인 상태로 보고될 수 있습니다.

- SVM 관리자가 볼륨을 오프라인으로 고의적으로 전환했습니다.
- 볼륨의 호스팅 클러스터 노드가 다운되고 HA 쌍 파트너에 대한 스토리지 페일오버도 실패합니다.
- 해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되었기 때문에 볼륨의 호스팅 스토리지 가상 시스템(SVM)이 중지됩니다.
- 2개의 RAID 디스크에서 동시에 발생한 장애로 인해 볼륨의 호스팅 애그리게이트는 다운되었습니다.

이벤트 관리 인벤토리 페이지와 클러스터/상태, 스토리지 VM/상태 및 볼륨/상태 세부 정보 페이지를 사용하여 이러한 가능성 중 하나 이상을 확인하거나 제거할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.
2. 이벤트 관리 * 재고 페이지에서 * 활성 가용성 이벤트 * 를 선택합니다.
3. 볼륨 오프라인 이벤트에 대해 표시되는 하이퍼텍스트 링크를 클릭합니다.

   가용성 인시던트에 대한 이벤트 세부 정보 페이지가 표시됩니다.

4. 이 페이지에서 SVM 관리자가 해당 볼륨을 오프라인으로 전환했음을 나타내는 메모가 있는지 확인합니다.
5. 이벤트 * 세부 정보 페이지에서 다음 작업 중 하나 이상에 대한 정보를 검토할 수 있습니다.
   - 원인 필드에 표시되는 정보를 검토하여 가능한 진단 지침을 확인합니다.

     이 예에서 원인 필드의 정보는 볼륨이 오프라인 상태임을 알려줍니다.

   - 참고 및 업데이트 영역에서 SVM 관리자가 문제의 볼륨을 오프라인으로 설정했음을 나타내는 표시를 확인하십시오.
   - 이벤트 소스(이 경우 오프라인으로 보고된 볼륨)를 클릭하여 해당 볼륨에 대한 자세한 정보를 확인합니다.
   - 관리자에게 이벤트를 할당합니다.
   - 이벤트를 확인하거나 해당하는 경우 해결됨으로 표시합니다.

볼륨 오프라인 상태에 대한 진단 작업을 수행합니다

오프라인 상태로 보고된 볼륨의 볼륨/상태 세부 정보 페이지로 이동한 후 볼륨 오프라인 상태를 진단하는 데 도움이 되는 추가 정보를 검색할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

오프라인으로 보고된 볼륨이 의도적으로 오프라인 상태로 전환되지 않은 경우 몇 가지 이유로 해당 볼륨이 오프라인 상태일 수 있습니다.

오프라인 볼륨의 볼륨/상태 세부 정보 페이지에서 시작하여 다른 페이지 및 창으로 이동하여 가능한 원인을 확인하거나 제거할 수 있습니다.

- 볼륨/상태 * 세부 정보 페이지 링크를 클릭하여 호스트 노드가 다운되어 있고 HA 쌍 파트너에 대한 스토리지 페일오버도 실패했으므로 볼륨이 오프라인 상태인지 확인합니다.

  을 참조하십시오 "볼륨 오프라인 상태가 다운 노드로 인해 발생했는지 확인".

- 볼륨/상태 * 세부 정보 페이지 링크를 클릭하여 볼륨이 오프라인 상태인지, 해당 SVM의 루트 볼륨을 호스팅하는 노드가 중단되어 해당 호스트 스토리지 가상 시스템(SVM)이 중지되었는지 확인합니다.

  을 참조하십시오 "노드가 중단되어 볼륨이 오프라인 상태인지, SVM이 중지되는지 확인".

- 볼륨/상태 * 세부 정보 페이지 링크를 클릭하여 해당 호스트 Aggregate의 손상된 디스크로 인해 볼륨이 오프라인 상태인지 확인합니다.

  을 참조하십시오 "Aggregate의 손상된 디스크로 인해 볼륨이 오프라인 상태인지 확인합니다".

- 관련 정보 *

"Unified Manager 사용자 역할 및 기능"

호스트 노드가 중단되어 볼륨이 오프라인 상태인지 확인합니다

Unified Manager 웹 UI를 사용하면 호스트 노드가 다운되어 있고 해당 HA 쌍 파트너에 대한 스토리지 페일오버가 성공하지 못하여 볼륨이 오프라인 상태가 될 가능성을 확인 또는 제거할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨 오프라인 상태가 호스팅 노드의 장애 및 후속 스토리지 페일오버 실패로 인해 발생하는지 확인하려면 다음 작업을 수행하십시오.

단계

1. 오프라인 볼륨의 * 볼륨/상태 * 세부 정보 페이지의 * 관련 장치 * 창에서 SVM 아래에 표시되는 하이퍼텍스트 링크를 찾아 클릭합니다.

   스토리지 VM/상태 세부 정보 페이지에는 오프라인 볼륨의 호스팅 스토리지 가상 시스템(SVM)에 대한 정보가 표시됩니다.

2. 스토리지 VM/상태 * 세부 정보 페이지의 * 관련 장치 * 창에서 볼륨 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.

   상태: 모든 볼륨 보기에는 SVM에서 호스팅하는 모든 볼륨에 대한 정보 테이블이 표시됩니다.

3. 상태: 모든 볼륨 * 뷰 상태 열 머리글에서 필터 기호를 클릭합니다 을 클릭한 다음 * 오프라인 * 옵션을 선택합니다.

   오프라인 상태인 SVM 볼륨만 나열됩니다.

4. 상태: 모든 볼륨 보기에서 그리드 기호를 클릭합니다 를 선택한 다음 * 클러스터 노드 * 옵션을 선택합니다.

   그리드 선택 상자에서 스크롤하여 * 클러스터 노드 * 옵션을 찾아야 할 수 있습니다.

   클러스터 노드 열이 볼륨 인벤토리에 추가되고 각 오프라인 볼륨을 호스팅하는 노드의 이름이 표시됩니다.

5. 상태: 모든 볼륨 * 보기에서 오프라인 볼륨의 목록을 찾은 다음 해당 클러스터 노드 열에서 호스팅 노드의 이름을 클릭합니다.

   클러스터/상태 세부 정보 페이지의 노드 탭에는 호스팅 노드가 속한 노드의 HA 쌍 상태가 표시됩니다. 호스팅 노드의 상태와 클러스터 페일오버 작업의 성공 여부가 디스플레이에 표시됩니다.

호스트 노드가 다운되어 있고 HA 쌍 파트너에 대한 스토리지 페일오버가 실패하여 볼륨 오프라인 상태가 존재하는지 확인한 후에는 해당 관리자 또는 운영자에게 연락하여 다운 노드를 수동으로 재시작하고 스토리지 페일오버 문제를 해결하십시오.

노드가 다운되어 볼륨이 오프라인 상태가 되고 해당 **SVM**이 중지되는지 확인

Unified Manager 웹 UI를 사용하면 SVM의 루트 볼륨을 호스팅하는 노드로 인해 SVM(호스트 스토리지 가상 머신)이 중지되어 볼륨이 오프라인 상태가 될 가능성을 확인 또는 제거할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

해당 SVM의 루트 볼륨을 호스팅하는 노드가 다운되었기 때문에 볼륨 오프라인 상태로 인해 호스트 SVM이 중지되었는지 확인하려면 다음 작업을 수행하십시오.

단계

1. 오프라인 볼륨의 * 볼륨/상태 * 세부 정보 페이지의 * 관련 장치 * 창에서 SVM 아래에 표시되는 하이퍼텍스트 링크를 찾아 클릭합니다.

   스토리지 VM/상태 세부 정보 페이지에는 호스팅 SVM의 "실행 중" 또는 "가동 중" 상태가 표시됩니다. SVM 상태가 실행 중이면 해당 SVM의 루트 볼륨을 호스팅하는 노드에 의해 볼륨 오프라인 상태가 발생하지 않습니다.

2. SVM 상태가 중지된 경우 * SVM 보기 * 를 클릭하여 호스팅 SVM의 중지 원인을 추가로 식별합니다.
3. 상태: 모든 스토리지 VM * 보기 SVM 열 머리글에서 필터 기호를 클릭합니다 그런 다음 중지된 SVM의 이름을 입력합니다.

   해당 SVM에 대한 정보가 표에 나와 있습니다.

4. 상태: 모든 스토리지 VM * 보기에서 을 클릭합니다 그런 다음 * 루트 볼륨 * 옵션을 선택합니다.

   루트 볼륨 열이 SVM 인벤토리에 추가되고 중지된 SVM의 루트 볼륨 이름이 표시됩니다.

5. 루트 볼륨 열에서 루트 볼륨의 이름을 클릭하여 해당 볼륨에 대한 * 스토리지 VM/상태 * 세부 정보 페이지를 표시합니다.

   SVM 루트 볼륨 상태가 (온라인)인 경우 해당 SVM의 루트 볼륨을 호스팅하는 노드가 중단되어 원래 볼륨 오프라인 상태가 발생하지 않습니다.

6. SVM 루트 볼륨의 상태가 (오프라인)인 경우 SVM 루트 볼륨의 볼륨/상태 세부 정보 페이지의 관련 장치 창에서 Aggregate에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.
7. Aggregate * Aggregate/Health * 세부 정보 페이지의 * Related Devices * 창에서 Node 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.

   클러스터/상태 세부 정보 페이지의 노드 탭에는 SVM 루트 볼륨의 호스팅 노드가 속하는 HA 노드 쌍의 상태가 표시됩니다. 노드 상태가 디스플레이에 표시됩니다.

볼륨 오프라인 상태가 해당 볼륨의 호스트 SVM 오프라인 상태로 인해 발생했는지 확인합니다. 오프라인 상태는 해당 SVM의 루트 볼륨을 호스팅하는 노드에 의해 유발됩니다. 그런 다음 해당 관리자 또는 운영자에게 연락하여 아래쪽 노드를 수동으로 재시작합니다.

Aggregate의 손상된 디스크로 인해 볼륨이 오프라인 상태인지 확인합니다

Unified Manager 웹 UI를 사용하면 RAID 디스크 문제로 인해 호스트 애그리게이트는 오프라인 상태가 되기 때문에 볼륨이 오프라인 상태가 될 가능성을 확인 또는 제거할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨 오프라인 상태가 호스팅 애그리게이트를 오프라인으로 전환하는 RAID 디스크 문제로 인한 것인지 확인하려면 다음 작업을 수행하십시오.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 관련 장치 * 창에서 집계 아래에 표시된 하이퍼텍스트 링크를 찾아 클릭합니다.

   집계/상태 세부 정보 페이지에는 호스팅 애그리게이트의 온라인 또는 오프라인 상태가 표시됩니다. 집계 상태가 온라인인 경우 RAID 디스크 문제는 볼륨이 오프라인 상태가 되는 원인이 아닙니다.

2. 집계 상태가 오프라인인 경우 * 디스크 정보 * 를 클릭하고 * 디스크 정보 * 탭의 * 이벤트 * 목록에서 손상된 디스크 이벤트를 찾습니다.
3. 손상된 디스크를 더 자세히 식별하려면 * Related Devices *(관련 장치 *) 창의 Node(노드) 아래에 표시된 하이퍼텍스트 링크를 클릭합니다.

   클러스터/상태 세부 정보 페이지가 표시됩니다.

4. Disks * 를 클릭한 다음 * Filters * 창에서 * Broken * 을 선택하여 손상된 상태의 모든 디스크를 나열합니다.

   깨진 상태의 디스크로 인해 호스트 애그리게이트의 오프라인 상태가 발생한 경우 해당 애그리게이트의 이름이 영향받는 애그리게이트 열에 표시됩니다.

손상된 RAID 디스크와 그로 인한 오프라인 호스트 집계로 인해 볼륨 오프라인 상태가 발생했는지 확인한 후 해당 관리자 또는 운영자에게 문의하여 손상된 디스크를 수동으로 교체하고 애그리게이트를 다시 온라인으로 전환합니다.

용량 문제 해결

이 워크플로우는 용량 문제를 해결하는 방법의 예를 제공합니다. 이 시나리오에서는 관리자나 운영자가 Unified ManagerDashboard 페이지에 액세스하여 모니터링되는 스토리지 개체에 용량 문제가 있는지 확인합니다. 문제의 가능한 원인과 해결 방법을 파악하려고 합니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대시보드 페이지에서 이벤트 드롭다운 목록 아래의 용량 패널에서 ""볼륨 공간이 가득 참"" 오류 이벤트를 찾습니다.

단계

1. Dashboard * 페이지의 * Capacity * 패널에서 Volume Space Full 오류 이벤트의 이름을 클릭합니다.

   오류에 대한 이벤트 세부 정보 페이지가 표시됩니다.

2. 이벤트 * 세부 정보 페이지에서 다음 작업 중 하나 이상을 수행할 수 있습니다.
   - 원인 필드의 오류 메시지를 검토하고 권장 해결 조치 아래에 있는 제안 사항을 클릭하여 가능한 해결 방법을 검토합니다.
   - 객체에 대한 세부 정보를 보려면 소스 필드에서 객체 이름(이 경우 볼륨)을 클릭합니다.
   - 이 이벤트에 대해 추가되었을 수 있는 참고 사항을 찾습니다.
   - 이벤트에 메모를 추가합니다.
   - 다른 사용자에게 이벤트를 할당합니다.
   - 이벤트를 확인합니다.
   - 이벤트를 Resolved 로 표시합니다.
     - 관련 정보 *

"이벤트 세부 정보 페이지"

전체 볼륨에 대해 제안된 개선 작업 수행

"Volume Space Full(볼륨 공간 부족)" 오류 이벤트가 발생한 후 이벤트 세부 정보 페이지에서 제안된 개선 조치를 검토하고 권장 조치 중 하나를 수행합니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

어떤 역할이라도 하는 사용자는 Unified Manager를 사용하는 이 워크플로우에서 모든 작업을 수행할 수 있습니다.

이 예에서는 Unified ManagerEvent Management 인벤토리 페이지에서 볼륨 공간 가득 참 오류 이벤트가 발생하고 이벤트 이름을 클릭했습니다.

전체 볼륨에 대해 수행할 수 있는 개선 조치는 다음과 같습니다.

- 볼륨에 대해 자동 확장, 중복제거 또는 압축을 사용하도록 설정합니다

- 볼륨 크기 조정 또는 이동
- 볼륨에서 데이터 삭제 또는 이동

이러한 모든 작업은 ONTAP System Manager 또는 ONTAP CLI에서 수행해야 하지만, Unified Manager를 사용하여 수행할 작업을 결정하는 데 필요한 정보를 찾을 수 있습니다.

단계

1. Event * details(이벤트 * 세부 정보) 페이지에서 Source(소스) 필드에서 볼륨 이름을 클릭하여 영향을 받는 볼륨에 대한 세부 정보를 봅니다.
2. 볼륨/상태 * 세부 정보 페이지에서 * 구성 * 을 클릭하면 볼륨에서 중복제거 및 압축이 이미 활성화되어 있음을 확인할 수 있습니다.

   볼륨 크기를 조정합니다.

3. Related Devices * 창에서 호스팅 애그리게이트의 이름을 클릭하여 애그리게이트로 더 큰 볼륨을 수용할 수 있는지 확인합니다.
4. Aggregate/Health * 세부 정보 페이지에는 전체 볼륨을 호스팅하는 aggregate에 커밋되지 않은 용량이 충분히 있으므로 ONTAP System Manager를 사용하여 볼륨 크기를 조정함으로써 더 많은 용량을 제공할 수 있습니다.

   ◦ 관련 정보 *

"이벤트 세부 정보 페이지"

상태 임계값 관리

모든 애그리게이트, 볼륨 및 qtree에 대한 글로벌 상태 임계값을 구성하여 상태 임계값 위반을 추적할 수 있습니다.

스토리지 용량 상태 임계값은 무엇입니까

스토리지 용량 상태 임계값은 Unified Manager 서버가 스토리지 오브젝트의 용량 문제를 보고하는 이벤트를 생성하는 지점입니다. 이러한 이벤트가 발생할 때마다 알림을 보내도록 알림을 구성할 수 있습니다.

모든 애그리게이트, 볼륨 및 qtree의 스토리지 용량 상태 임계값이 기본값으로 설정됩니다. 개체 또는 개체 그룹에 필요한 대로 설정을 변경할 수 있습니다.

전역 상태 임계값 설정 구성 중

용량, 증가, 스냅샷 예약, 할당량, inode에 대한 글로벌 상태 임계값 조건을 구성하여 애그리게이트, 볼륨 및 qtree 크기를 효과적으로 모니터링할 수 있습니다. 지연 임계값을 초과하는 이벤트를 생성하기 위한 설정을 편집할 수도 있습니다.

글로벌 상태 임계값 설정은 애그리게이트, 볼륨 등 연결되어 있는 모든 개체에 적용됩니다. 임계값을 넘어지면 이벤트가 생성되고 경고가 구성된 경우 경고 알림이 전송됩니다. 임계값 기본값은 권장 값으로 설정되지만 특정 요구에 맞게 이벤트 간격을 생성하도록 수정할 수 있습니다. 임계값이 변경되면 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

전역 상태 임계값 설정은 왼쪽 탐색 메뉴의 이벤트 임계값 섹션에서 액세스할 수 있습니다. 재고 페이지 또는 해당

객체의 세부 정보 페이지에서 개별 객체에 대한 임계값 설정을 수정할 수도 있습니다.

- 자세한 내용은 을 참조하십시오 "글로벌 애그리게이트 상태 임계값 구성".

  모든 애그리게이트의 용량, 증가 및 스냅샷 복사본에 대한 상태 임계값 설정을 구성하여 모든 임계값 위반을 추적할 수 있습니다.

- 자세한 내용은 을 참조하십시오 "글로벌 볼륨 상태 임계값을 구성하는 중입니다".

  용량, 스냅샷 복사본, qtree 할당량, 볼륨 증가, 덮어쓰기 예약 공간에 대한 상태 임계값 설정을 편집할 수 있습니다. 모든 볼륨에 대한 inode를 통해 임계값 위반을 추적할 수 있습니다.

- 자세한 내용은 을 참조하십시오 "글로벌 qtree 상태 임계값을 구성하는 중입니다".

  모든 qtree의 용량에 대한 상태 임계값 설정을 편집하여 모든 임계값 위반을 추적할 수 있습니다.

- 자세한 내용은 을 참조하십시오 "관리되지 않는 보호 관계에 대한 지연 상태 임계값 설정 편집".

  경고 또는 오류 지연 시간 비율을 늘리거나 줄이면 사용자의 요구에 더 적합한 간격으로 이벤트가 생성됩니다.

글로벌 애그리게이트 상태 임계값 구성

모든 애그리게이트에 대한 글로벌 상태 임계값을 구성하여 모든 임계값 위반을 추적할 수 있습니다. 임계값 위반에 대한 적절한 이벤트가 생성되고 이러한 이벤트를 기반으로 예방 조치를 취할 수 있습니다. 모니터링되는 모든 애그리게이트에 적용되는 임계값에 대한 모범 사례 설정을 기반으로 글로벌 값을 구성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

옵션을 전역적으로 구성하면 개체의 기본값이 수정됩니다. 그러나 개체 수준에서 기본값이 변경된 경우에는 글로벌 값이 수정되지 않습니다.

임계값 옵션은 더 나은 모니터링을 위한 기본값을 가지고 있지만, 환경의 요구 사항에 맞게 값을 변경할 수 있습니다.

Aggregate에 상주하는 볼륨에 대해 자동 ogrow를 사용하도록 설정하면 원래 볼륨 크기가 아닌 에서 설정된 최대 볼륨 크기에 따라 애그리게이트 용량 임계값이 위반된 것으로 간주됩니다.

상태 임계값은 노드의 루트 애그리게이트에 적용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 임계값 * > * 집계 * 를 클릭합니다.
2. 용량, 증가 및 스냅샷 복사본에 대한 적절한 임계값을 구성합니다.
3. 저장 * 을 클릭합니다.

◦ 관련 정보 *

"사용자 추가"

글로벌 볼륨 상태 임계값을 구성하는 중입니다

모든 볼륨에 대한 글로벌 상태 임계값을 구성하여 모든 임계값 위반을 추적할 수 있습니다. 상태 임계값 위반에 대한 적절한 이벤트가 생성되고 이러한 이벤트를 기반으로 예방 조치를 취할 수 있습니다. 모니터링되는 모든 볼륨에 적용되는 임계값에 대한 Best Practice 설정을 기반으로 글로벌 값을 구성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대부분의 임계값 옵션에는 더 나은 모니터링을 위한 기본값이 있습니다. 그러나 환경의 요구 사항에 맞게 값을 변경할 수 있습니다.

볼륨에 대해 Autogrow를 사용하도록 설정한 경우 원래 볼륨 크기를 기준으로 하지 않고 자동으로 설정된 최대 볼륨 크기에 따라 용량 임계값이 위반된 것으로 간주됩니다.

> 스냅샷 복사본 1000개의 기본값은 ONTAP 버전이 9.4 이상인 경우 FlexVol 볼륨에만, ONTAP 버전이 9.8 이상인 경우 FlexGroup 볼륨에만 적용됩니다. 이전 버전의 ONTAP 소프트웨어와 함께 설치된 클러스터의 경우 최대 250개의 스냅샷 복사본이 볼륨당 가능합니다. 이전 버전에서는 Unified Manager가 이 1000번(및 1000에서 250번 사이의 숫자)을 250으로 해석합니다. 즉, 스냅샷 복사본 수가 250개에 도달하면 계속 이벤트를 받게 됩니다. 이러한 이전 버전에 대해 이 임계값을 250개 미만으로 설정하려면 여기에서 상태: 모든 볼륨 보기 또는 볼륨/상태 세부 정보 페이지에서 임계값을 250개 이하로 설정해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 임계값 * > * 볼륨 * 을 클릭합니다.
2. 용량, 스냅샷 복사본, qtree 할당량, 볼륨 증가, inode에 대한 적절한 임계값을 구성합니다.
3. 저장 * 을 클릭합니다.

◦ 관련 정보 *

"사용자 추가"

글로벌 **qtree** 상태 임계값을 구성하는 중입니다

모든 qtree에 대한 글로벌 상태 임계값을 구성하여 모든 임계값 위반을 추적할 수 있습니다. 상태 임계값 위반에 대한 적절한 이벤트가 생성되고 이러한 이벤트를 기반으로 예방 조치를 취할 수 있습니다. 모니터링되는 모든 qtree에 적용되는 임계값에 대한 모범 사례 설정을 기반으로 글로벌 값을 구성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값 옵션은 더 나은 모니터링을 위한 기본값을 가지고 있지만, 환경의 요구 사항에 맞게 값을 변경할 수 있습니다.

Qtree 할당량 또는 기본 할당량이 qtree에 설정된 경우에만 qtree에 대한 이벤트가 생성됩니다. 사용자 할당량 또는 그룹 할당량에 정의된 공간이 임계값을 초과하면 이벤트가 생성되지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 임계값 * > * Qtree * 를 클릭합니다.
2. 적절한 용량 임계값을 구성합니다.
3. 저장 * 을 클릭합니다.

관리되지 않는 보호 관계에 대한 지연 임계값 설정 구성

관리되지 않는 보호 관계에 대한 전역 기본 지연 경고 및 오류 상태 임계값 설정을 편집하여 필요에 맞는 간격으로 이벤트가 생성됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

지연 시간은 정의된 전송 스케줄 간격보다 길지 않아야 합니다. 예를 들어, 전송 일정이 매시간 인 경우 지연 시간은 1시간 이상이어야 합니다. 지연 임계값은 지연 시간이 초과해서는 안 되는 비율을 지정합니다. 1시간의 예를 사용하여 지연 임계값이 150%로 정의된 경우 지연 시간이 1.5시간 이상일 때 이벤트를 받게 됩니다.

이 작업에 설명된 설정은 관리되지 않는 모든 보호 관계에 전체적으로 적용됩니다. 이 설정은 하나의 관리되지 않는 보호 관계에만 지정하고 적용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 임계값 * > * 관계 * 를 클릭합니다.
2. 필요에 따라 글로벌 기본 경고 또는 오류 지연 시간 비율을 늘리거나 줄입니다.
3. 지연 임계값 양에서 경고 또는 오류 이벤트가 트리거되지 않도록 하려면 * Enabled * (활성화 *) 옆의 확인란을 선택 취소합니다.
4. 저장 * 을 클릭합니다.

◦ 관련 정보 *

"사용자 추가"

개별 애그리게이트 상태 임계값 설정 편집

하나 이상의 Aggregate의 용량, 증가 및 스냅샷 복사본에 대한 상태 임계값 설정을 편집할 수 있습니다. 임계값이 초과되면 알림이 생성되고 알림이 수신됩니다. 이러한 알림은 생성된 이벤트를 기반으로 예방 조치를 취하는 데 도움이 됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값 변경에 따라 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

Aggregate에 상주하는 볼륨에 대해 자동 ogrow를 사용하도록 설정하면 원래 볼륨 크기가 아닌 에서 설정된 최대 볼륨 크기에 따라 애그리게이트 용량 임계값이 위반된 것으로 간주됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. 상태: 모든 애그리게이트 * 보기에서 하나 이상의 애그리게이트를 선택한 다음 * 임계값 편집 * 을 클릭합니다.
3. [집계 임계값 편집] * 대화 상자에서 적절한 확인란을 선택한 다음 설정을 수정하여 용량, 증가 또는 스냅샷 복사본 중 하나의 임계값 설정을 편집합니다.
4. 저장 * 을 클릭합니다.
    ◦ 관련 정보 *

"사용자 추가"

개별 볼륨 상태 임계값 설정 편집

하나 이상의 볼륨에 대한 볼륨 용량, 증가, 할당량 및 공간 예비 공간에 대한 상태 임계값 설정을 편집할 수 있습니다. 임계값이 초과되면 알림이 생성되고 알림이 수신됩니다. 이러한 알림은 생성된 이벤트를 기반으로 예방 조치를 취하는 데 도움이 됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값 변경에 따라 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

볼륨에 대해 Autogrow를 사용하도록 설정한 경우 원래 볼륨 크기를 기준으로 하지 않고 자동으로 설정된 최대 볼륨 크기에 따라 용량 임계값이 위반된 것으로 간주됩니다.

> 스냅샷 복사본 1000개의 기본값은 ONTAP 버전이 9.4 이상인 경우 FlexVol 볼륨에만, ONTAP 버전이 9.8 이상인 경우 FlexGroup 볼륨에만 적용됩니다. 이전 버전의 ONTAP 소프트웨어와 함께 설치된 클러스터의 경우 최대 250개의 스냅샷 복사본이 볼륨당 가능합니다. 이전 버전에서는 Unified Manager가 이 1000번(및 1000에서 250번 사이의 숫자)을 250으로 해석합니다. 즉, 스냅샷 복사본 수가 250개에 도달하면 계속 이벤트를 받게 됩니다. 이러한 이전 버전에 대해 이 임계값을 250개 미만으로 설정하려면 여기에서 상태: 모든 볼륨 보기 또는 볼륨/상태 세부 정보 페이지에서 임계값을 250개 이하로 설정해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 상태: 모든 볼륨 * 보기에서 하나 이상의 볼륨을 선택한 다음 * 임계값 편집 * 을 클릭합니다.
3. 볼륨 임계값 편집 * 대화 상자에서 적절한 확인란을 선택한 다음 설정을 수정하여 용량, 스냅샷 복사본, qtree 할당량, 증가 또는 inode 중 하나의 임계값 설정을 편집합니다.
4. 저장 * 을 클릭합니다.
    ◦ 관련 정보 *

"사용자 추가"

개별 **qtree** 상태 임계값 설정 편집

하나 이상의 qtree에 대한 qtree 용량의 상태 임계값 설정을 편집할 수 있습니다. 임계값이 초과되면 알림이 생성되고 알림이 수신됩니다. 이러한 알림은 생성된 이벤트를 기반으로 예방

조치를 취하는 데 도움이 됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

임계값 변경에 따라 다음 모니터링 주기에서 이벤트가 생성되거나 폐기됩니다.

단계

1. 왼쪽 탐색 창에서 * Storage * > * qtree * 를 클릭합니다.
2. Capacity:All qtree * 뷰에서 하나 이상의 qtree를 선택한 다음 * Edit Thresholds * 를 클릭합니다.
3. [Qtree 임계값 편집] * 대화 상자에서 선택한 qtree 또는 qtree의 용량 임계값을 변경하고 * [저장]을 클릭합니다.

스토리지 VM/상태 세부 정보 페이지의 qtree 탭에서 개별 qtree 임계값을 설정할 수도 있습니다.

클러스터 보안 목표 관리

Unified Manager는 ONTAP 9_에 대한_NetApp 보안 강화 가이드에 정의된 권장사항을 기반으로 ONTAP 클러스터, SVM(스토리지 가상 시스템), 볼륨이 얼마나 안전한지 식별하는 대시보드를 제공합니다.

보안 대시보드의 목표는 ONTAP 클러스터가 NetApp 권장 지침에 맞지 않는 영역을 보여서 이러한 잠재적 문제를 해결할 수 있도록 하는 것입니다. 대부분의 경우 ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 문제를 해결할 수 있습니다. 조직에서 모든 권장 사항을 따르지 않을 수 있으므로 변경할 필요가 없는 경우도 있습니다.

를 참조하십시오 "ONTAP 9에 대한 NetApp 보안 강화 가이드" (TR-4569)을 참조하십시오.

Unified Manager는 보안 상태를 보고하는 것 외에도 보안 위반 사례가 있는 클러스터 또는 SVM을 위한 보안 이벤트도 생성합니다. 이벤트 관리 인벤토리 페이지에서 이러한 문제를 추적하고 이러한 이벤트에 대한 알림을 구성하여 새로운 보안 이벤트가 발생할 때 스토리지 관리자에게 알릴 수 있습니다.

자세한 내용은 을 참조하십시오 "평가 대상 보안 기준".

평가 대상 보안 기준

일반적으로 ONTAP 클러스터, SVM(스토리지 가상 머신), 볼륨에 대한 보안 기준은 ONTAP 9_에 대한_NetApp 보안 강화 가이드에 정의된 권장사항을 기준으로 평가됩니다.

일부 보안 검사는 다음과 같습니다.

- 클러스터에서 SAML과 같은 보안 인증 방법을 사용하는지 여부
- 피어링된 클러스터의 통신이 암호화되었는지 여부
- 스토리지 VM에 감사 로그가 설정되었는지 여부
- 볼륨에 소프트웨어 또는 하드웨어 암호화가 활성화되어 있는지 여부

규정 준수 범주 및 에 대한 항목을 참조하십시오 "ONTAP 9에 대한 NetApp 보안 강화 가이드" 을 참조하십시오.

Active IQ 플랫폼에서 보고된 업그레이드 이벤트도 보안 이벤트로 간주됩니다. 이러한 이벤트는 문제 해결을 위해 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어(보안 권장 사항)를 업그레이드해야 하는 문제를 식별합니다. 이러한 이벤트는 보안 패널에 표시되지 않지만 이벤트 관리 인벤토리 페이지에서 사용할 수 있습니다.

자세한 내용은 을 참조하십시오 "클러스터 보안 목표 관리".

클러스터 규정 준수 범주

이 표에는 Unified Manager가 평가하는 클러스터 보안 규정 준수 매개 변수, NetApp 권장 사항 및 매개 변수가 불만 제기인지 여부와 관련된 클러스터의 전반적인 결정에 영향을 미치는지 여부가 정리되어 있습니다.

클러스터에서 규정을 준수하지 않는 SVM이 존재할 경우 클러스터의 규정 준수 값에 영향을 미칩니다. 따라서 클러스터 보안이 규정 준수 상태로 인식되기 전에 SVM에서 보안 문제를 해결해야 하는 경우도 있습니다.

아래 나열된 모든 매개변수가 모든 설치에 나타나는 것은 아닙니다. 예를 들어 피어링된 클러스터가 없거나 클러스터에서 AutoSupport를 비활성화한 경우 UI 페이지에 클러스터 피어링 또는 AutoSupport HTTPS 전송 항목이 표시되지 않습니다.

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
글로벌 FIPS	글로벌 FIPS(Federal Information Processing Standard) 140-2 준수 모드가 활성화되어 있는지 여부를 나타냅니다. FIPS가 활성화되면 TLSv1 및 SSLv3이 비활성화되고 TLSv1.1 및 TLSv1.2만 허용됩니다.	활성화됨	예
텔넷	시스템에 대한 텔넷 액세스가 활성화되었는지 여부를 나타냅니다. 보안 원격 액세스를 위해 SSH(Secure Shell)를 사용하는 것이 좋습니다.	사용 안 함	예
안전하지 않은 SSH 설정	SSH가 * CBC로 시작하는 암호 등의 안전하지 않은 암호를 사용하는지 여부를 나타냅니다.	아니요	예
로그인 배너	시스템에 액세스하는 사용자가 로그인 배너를 사용할 수 있는지 여부를 나타냅니다.	활성화됨	예

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
클러스터 피어링	피어링된 클러스터 간의 통신이 암호화되었는지 또는 암호화되지 않았음을 나타냅니다. 이 매개 변수를 준수하는 것으로 간주하려면 소스 클러스터와 대상 클러스터 모두에서 암호화를 구성해야 합니다.	암호화	예
Network Time Protocol의 약어입니다	클러스터에 구성된 NTP 서버가 하나 이상 있는지 여부를 나타냅니다. 이중화 및 최적의 서비스를 위해 최소 3개의 NTP 서버를 클러스터에 연결하는 것이 좋습니다.	구성됨	예
OCSP	ONTAP에 OCSP(온라인 인증서 상태 프로토콜)로 구성되지 않은 응용 프로그램이 있는지 여부를 나타내므로 통신이 암호화되지 않습니다. 비준수 애플리케이션이 나열됩니다.	활성화됨	아니요
원격 감사 로깅	로그 전달(Syslog)이 암호화되었는지 또는 암호화되지 않았음을 나타냅니다.	암호화	예
AutoSupport HTTPS 전송	HTTPS가 NetApp 지원으로 AutoSupport 메시지를 보내기 위한 기본 전송 프로토콜로 사용되는지 여부를 나타냅니다.	활성화됨	예
기본 관리자 사용자입니다	기본 관리자 사용자(기본 제공)가 활성화 또는 비활성화되었는지 여부를 나타냅니다. 불필요한 내장 계정을 잠금(비활성화)하는 것이 좋습니다.	사용 안 함	예

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
SAML 사용자	SAML이 구성되었는지 여부를 나타냅니다. SAML을 사용하면 SSO(Single Sign-On)에 대한 로그인 방법으로 MFA(Multi-Factor Authentication)를 구성할 수 있습니다.	아니요	아니요
Active Directory 사용자	Active Directory가 구성되었는지 여부를 나타냅니다. Active Directory 및 LDAP는 클러스터에 액세스하는 사용자가 선호하는 인증 메커니즘입니다.	아니요	아니요
LDAP 사용자	LDAP가 구성되었는지 여부를 나타냅니다. Active Directory 및 LDAP는 로컬 사용자를 통해 클러스터를 관리하는 사용자에게 권장되는 인증 메커니즘입니다.	아니요	아니요
인증서 사용자	인증서 사용자가 클러스터에 로그인하도록 구성되었는지 여부를 나타냅니다.	아니요	아니요
로컬 사용자	로컬 사용자가 클러스터에 로그인하도록 구성되었는지 여부를 나타냅니다.	아니요	아니요
원격 셸	RSH가 활성화되었는지 여부를 나타냅니다. 보안상의 이유로 RSH를 비활성화해야 합니다. 보안 원격 액세스를 위한 SSH(Secure Shell)가 권장됩니다.	사용 안 함	예

매개 변수	설명	권장 사항	클러스터 규정 준수에 영향을 줍니다
MD5가 사용 중입니다	ONTAP 사용자 계정이 덜 안전한 MD5 해시 기능을 사용하고 있는지 여부를 나타냅니다. MD5 해시 사용자 계정을 SHA-512와 같은 보다 안전한 암호화 해시 기능으로 마이그레이션하는 것이 좋습니다.	아니요	예
인증서 발급자 유형	사용된 디지털 인증서의 유형을 나타냅니다.	CA 서명	아니요

스토리지 **VM** 규정 준수 범주

이 표에서는 Unified Manager에서 평가하는 SVM(Storage Virtual Machine) 보안 규정 준수 기준, NetApp 권장 사항 및 매개 변수가 불만 사항이 아닌 SVM의 전반적인 결정에 영향을 미치는지 여부를 설명합니다.

매개 변수	설명	권장 사항	**SVM** 규정 준수에 영향을 줍니다
감사 로그	감사 로깅이 설정되었는지 여부를 나타냅니다.	활성화됨	예
안전하지 않은 SSH 설정	SSH가 secure cipherer를 사용하는지 여부(예: CBC * 로 시작하는 cipherers)를 나타냅니다.	아니요	예
로그인 배너	시스템에서 SVM에 액세스하는 사용자에 대해 로그인 배너가 활성화되어 있는지 또는 비활성화되어 있는지 여부를 나타냅니다.	활성화됨	예
LDAP 암호화	LDAP 암호화가 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요
NTLM 인증	NTLM 인증이 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요

매개 변수	설명	권장 사항	**SVM** 규정 준수에 영향을 줍니다
LDAP 페이로드 서명	LDAP 페이로드 서명이 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요
CHAP 설정	CHAP가 설정되었는지 여부를 나타냅니다.	활성화됨	아니요
Kerberos V5	Kerberos V5 인증이 활성화 또는 비활성화되었는지 여부를 나타냅니다.	활성화됨	아니요
NIS 인증	NIS 인증 사용이 구성되었는지 여부를 나타냅니다.	사용 안 함	아니요
FPolicy 상태가 활성 상태입니다	FPolicy가 생성되었는지 여부를 나타냅니다.	예	아니요
SMB 암호화가 활성화되었습니다	SMB 서명 및 봉인 기능이 활성화되어 있지 않음을 나타냅니다.	예	아니요
SMB 서명이 활성화되었습니다	SMB 서명이 설정되어 있지 않음을 나타냅니다.	예	아니요

볼륨 규정 준수 범주

이 표에서는 Unified Manager에서 볼륨 암호화 매개 변수를 평가하여, 볼륨의 데이터가 무단 사용자에 의해 액세스되지 않도록 적절히 보호되는지 여부를 확인합니다.

볼륨 암호화 매개 변수는 클러스터 또는 스토리지 VM의 규정 준수 여부에 영향을 주지 않습니다.

매개 변수	설명
소프트웨어가 암호화되었습니다	NVE(NetApp Volume Encryption) 또는 NAE(NetApp Aggregate Encryption) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨 수를 표시합니다.
하드웨어가 암호화되었습니다	NSE(NetApp Storage Encryption) 하드웨어 암호화를 사용하여 보호되는 볼륨 수를 표시합니다.
소프트웨어 및 하드웨어가 암호화되었습니다	소프트웨어 및 하드웨어 암호화로 보호되는 볼륨의 수를 표시합니다.

매개 변수	설명
암호화되지 않았습니다	암호화되지 않은 볼륨의 수를 표시합니다.

규정을 준수하지 않는 것은 무엇을 의미합니까

ONTAP 9_에 대한 NetApp 보안 강화 가이드에 정의된 권장사항을 기준으로 평가 중인 보안 기준이 충족되지 않을 경우 클러스터 및 SVM(스토리지 가상 시스템)이 적합하지 않은 것으로 간주됩니다. 또한 SVM이 규정을 준수하지 않는 것으로 플래그가 지정된 클러스터는 규정을 준수하지 않는 것으로 간주됩니다.

보안 카드의 상태 아이콘은 규정 준수와 관련하여 다음과 같은 의미를 가집니다.

- 매개 변수가 권장 구성으로 구성되어 있습니다.
- 매개 변수가 권장 구성으로 구성되지 않았습니다.
- - 클러스터에서 기능이 활성화되지 않았거나 매개 변수가 권장 구성으로 구성되지 않았습니다. 하지만 이 매개 변수는 개체의 규정 준수에 영향을 주지 않습니다.

볼륨 암호화 상태는 클러스터 또는 SVM이 규정을 준수하는지 여부를 나타내는 것이 아닙니다.

클러스터 및 스토리지 **VM**의 보안 상태 보기

Active IQ Unified Manager를 사용하면 환경의 스토리지 객체 보안 상태를 인터페이스의 여러 지점에서 확인할 수 있습니다. 정의된 매개 변수를 기반으로 정보 및 보고서를 수집 및 분석하고, 모니터링되는 클러스터와 스토리지 VM에서 의심스러운 동작 또는 승인되지 않은 시스템 변경을 감지할 수 있습니다.

보안 권장 사항은 을 참조하십시오 "ONTAP 9에 대한 NetApp 보안 강화 가이드"

보안 페이지에서 개체 수준 보안 상태를 봅니다

시스템 관리자는 * 보안 * 페이지를 사용하여 데이터 센터 및 사이트 수준에서 ONTAP 클러스터 및 스토리지 VM의 보안 강도에 대한 가시성을 확보할 수 있습니다. 지원되는 객체는 클러스터, 스토리지 VM 및 볼륨입니다. 다음 단계를 수행하십시오.

단계

1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다.
2. 모니터링되는 모든 클러스터에 대한 보안 상태를 볼 것인지 또는 단일 클러스터에 대한 보안 상태를 볼 것인지 여부에 따라 * All Clusters * 를 선택하거나 드롭다운 메뉴에서 단일 클러스터를 선택합니다.
3. Security * 패널에서 오른쪽 화살표를 클릭합니다. 보안 페이지가 표시됩니다.

막대 차트, 개수 및 '보고서 보기' 링크를 클릭하면 볼륨, 클러스터 또는 스토리지 VM 페이지로 이동하여 필요에 따라 해당 세부 정보를 보거나 보고서를 생성할 수 있습니다.

보안 페이지에는 다음 패널이 표시됩니다.

- * 클러스터 규정 준수 *: 데이터 센터에 있는 모든 클러스터의 보안 상태(규정을 준수하거나 준수하지 않는 클러스터

수)입니다

- * 스토리지 VM 규정 준수 *: 데이터 센터의 모든 스토리지 VM에 대한 보안 상태(규정을 준수하거나 준수하지 않는 스토리지 VM 수)입니다
- * 볼륨 암호화 *: 사용자 환경의 모든 볼륨에 대한 볼륨 암호화 상태(암호화되거나 암호화되지 않은 볼륨 수)입니다
- * Volume Anti-랜섬웨어 Status *: 사용자 환경의 모든 볼륨에서 보안 상태(랜섬웨어 방지 기능이 활성화된 볼륨 수 또는 비활성화된 볼륨 수)입니다
- * 클러스터 인증 및 인증서 *: SAML, Active Directory 등의 각 인증 방법을 사용하거나 인증서 및 로컬 인증을 통해 클러스터 수입니다. 또한 이 패널에는 인증서가 만료되었거나 60일 후에 만료되려고 하는 클러스터의 수가 표시됩니다.

클러스터 페이지에서 모든 클러스터의 보안 세부 정보를 봅니다

클러스터/보안 * 세부 정보 페이지에서는 클러스터 수준에서 보안 규정 준수 상태를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * Storage > Clusters * 를 클릭합니다.
2. 보기 > 보안 > 모든 클러스터 * 를 선택합니다.

글로벌 FIPS, Telnet, 비보안 SSH 설정, 로그인 배너, 네트워크 시간 프로토콜 등의 기본 보안 매개 변수 AutoSupport HTTPS 전송 과 클러스터 인증서 만료 상태가 표시됩니다.

를 클릭할 수 있습니다 ⋮ 추가 옵션 단추를 클릭하고 Unified Manager의 * 보안 * 페이지 또는 System Manager에서 보안 세부 정보를 표시하도록 선택합니다. System Manager에서 자세한 정보를 볼 수 있는 유효한 자격 증명이 있어야 합니다.

클러스터에 만료된 인증서가 있는 경우 * 클러스터 인증서 유효성 * 에서 "만료됨"을 클릭하고 System Manager(9.10.1 이상)에서 갱신할 수 있습니다. System Manager 인스턴스가 9.10.1 이전 릴리즈인 경우 '만료됨'을 클릭할 수 없습니다.

스토리지 **VM** 페이지에서 모든 클러스터의 보안 세부 정보를 봅니다

스토리지 VM/보안 * 세부 정보 페이지에서는 스토리지 VM 레벨의 보안 규정 준수 상태를 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 보기 > 보안 > 모든 스토리지 VM * 을 선택합니다. 보안 매개 변수가 있는 클러스터 목록이 표시됩니다.

스토리지 VM, 클러스터, 로그인 배너, 감사 로그, 보안되지 않은 SSH 설정 등의 보안 매개 변수를 확인하여 스토리지 VM의 보안 규정 준수를 기본적으로 볼 수 있습니다.

를 클릭할 수 있습니다 ⋮ 추가 옵션 단추를 클릭하고 Unified Manager의 * 보안 * 페이지 또는 System Manager에서 보안 세부 정보를 표시하도록 선택합니다. System Manager에서 자세한 정보를 볼 수 있는 유효한 자격 증명이 있어야 합니다.

볼륨 및 스토리지 VM에 대한 랜섬웨어 방지 보안에 대한 자세한 내용은 을 참조하십시오 "모든 볼륨 및 스토리지 VM의 랜섬웨어 방지 상태 보기".

소프트웨어 또는 펌웨어 업데이트가 필요할 수 있는 보안 이벤트 보기

"업그레이드"의 영향 영역이 있는 특정 보안 이벤트가 있습니다. 이러한 이벤트는 Active IQ 플랫폼에서 보고되며, 해결 방법을 통해 ONTAP 소프트웨어, 노드 펌웨어 또는 운영 체제 소프트웨어(보안 권장 사항)를 업그레이드해야 하는 문제를 식별합니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이러한 문제 중 일부에 대해 즉각적인 수정 조치를 수행해야 하는 경우도 있지만, 다른 문제로 인해 예정된 다음 유지 관리 작업이 완료될 때까지 기다릴 수 있습니다. 이러한 이벤트를 모두 보고 문제를 해결할 수 있는 사용자에게 할당할 수 있습니다. 또한 알림을 받지 않을 특정 보안 업그레이드 이벤트가 있는 경우 이 목록을 사용하면 해당 이벤트를 식별하여 비활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.

   기본적으로 모든 활성(신규 및 확인됨) 이벤트가 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 * 업그레이드 이벤트 * 를 선택합니다.

   이 페이지에는 모든 활성 업그레이드 보안 이벤트가 표시됩니다.

모든 클러스터에서 사용자 인증을 관리하는 방법 보기

보안 페이지에는 각 클러스터의 사용자를 인증하는 데 사용되는 인증 유형과 각 유형을 사용하여 클러스터에 액세스하는 사용자 수가 표시됩니다. 이렇게 하면 조직에서 정의한 대로 사용자 인증이 안전하게 수행되고 있는지 확인할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다.
2. 대시보드 상단의 드롭다운 메뉴에서 * All Clusters * 를 선택합니다.
3. 보안* 패널에서 오른쪽 화살표를 클릭하면 * 보안 * 페이지가 표시됩니다.
4. 각 인증 유형을 사용하여 시스템에 액세스하는 사용자 수를 보려면 * 클러스터 인증 * 카드를 확인하십시오.
5. 각 클러스터의 사용자를 인증하는 데 사용되는 인증 메커니즘을 보려면 * 클러스터 보안 * 카드를 확인하십시오.

시스템에 액세스하는 일부 사용자가 안전하지 않은 방법을 사용하거나 NetApp에서 권장하지 않는 방법을 사용하는 경우, 이 방법을 사용하지 않도록 설정할 수 있습니다.

모든 볼륨의 암호화 상태 보기

모든 볼륨의 목록과 현재 암호화 상태를 볼 수 있으므로 볼륨의 데이터가 무단 사용자가 액세스하지 못하도록 적절하게 보호되는지 여부를 확인할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨에 적용할 수 있는 암호화 유형은 다음과 같습니다.

- 소프트웨어 - NVE(NetApp Volume Encryption) 또는 NetApp NAE(Aggregate Encryption) 소프트웨어 암호화 솔루션을 사용하여 보호되는 볼륨
- Hardware - NSE(NetApp Storage Encryption) 하드웨어 암호화를 사용하여 보호되는 볼륨입니다.
- 소프트웨어 및 하드웨어 - 소프트웨어 및 하드웨어 암호화로 보호되는 볼륨입니다.
- 없음 - 암호화되지 않은 볼륨입니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 상태 * > * 볼륨 암호화 * 를 선택합니다
3. 상태: 볼륨 암호화 * 보기에서 * 암호화 유형 * 필드를 기준으로 정렬하거나 필터를 사용하여 특정 암호화 유형이 있거나 암호화되지 않은 볼륨(암호화 유형 ""없음")을 표시합니다.

모든 볼륨 및 스토리지 **VM**의 랜섬웨어 방지 상태 보기

모든 볼륨 및 스토리지 VM(SVM)의 목록과 현재 안티 랜섬웨어 상태를 볼 수 있으므로 볼륨 및 SVM의 데이터가 랜섬웨어 공격으로부터 적절히 보호되는지 확인할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다양한 안티 랜섬웨어 상태에 대한 자세한 내용은 를 참조하십시오 "ONTAP: 랜섬웨어 방지 지원".

랜섬웨어 방지 감지를 사용하여 모든 볼륨의 보안 세부 정보를 봅니다

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 상태 * > * 보안 * > * 랜섬웨어 방지 * 를 선택합니다
3. Security: Anti-랜섬웨어 * 보기에서 다양한 필드를 기준으로 정렬하거나 필터를 사용할 수 있습니다.

오프라인 볼륨, 제한된 볼륨, SnapLock 볼륨, FlexGroup 볼륨, FlexCache 볼륨 및 SAN 전용 볼륨, 중지된 스토리지 VM의 볼륨, 스토리지 VM의 루트 볼륨 또는 데이터 보호 볼륨.

랜섬웨어 방지 감지를 사용하여 모든 스토리지 **VM**의 보안 세부 정보를 봅니다

단계

1. 왼쪽 탐색 창에서 * 스토리지 > 스토리지 VM * 을 클릭합니다.
2. 보기 > 보안 > 랜섬웨어 방지 * 를 선택합니다. 랜섬웨어 방지 상태가 표시된 SVM 목록이 표시됩니다.

랜섬웨어 방지 모니터링은 NAS 프로토콜이 활성화되지 않은 스토리지 VM에서 지원되지 않습니다.

모든 활성 보안 이벤트 보기

모든 활성 보안 이벤트를 확인한 다음 문제를 해결할 수 있는 사용자에게 각 이벤트를 할당할 수 있습니다. 또한 수신하지 않을 특정 보안 이벤트가 있는 경우 이 목록을 사용하여 비활성화할 이벤트를 확인할 수 있습니다.

- 필요한 것 *

운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 이벤트 관리 * 를 클릭합니다.

   기본적으로 새 이벤트와 확인된 이벤트는 이벤트 관리 인벤토리 페이지에 표시됩니다.

2. 보기 메뉴에서 * 활성 보안 이벤트 * 를 선택합니다.

   이 페이지에는 지난 7일 동안 생성된 모든 새 보안 이벤트 및 확인된 보안 이벤트가 표시됩니다.

보안 이벤트에 대한 알림 추가

Unified Manager에서 수신한 다른 이벤트처럼 개별 보안 이벤트에 대한 알림을 구성할 수 있습니다. 또한 모든 보안 이벤트를 동일하게 처리하고 동일한 사용자에게 전자 메일을 보내려는 경우 보안 이벤트가 트리거되면 단일 알림을 생성하여 사용자에게 알릴 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 예제에서는 ""Telnet 프로토콜 사용"" 보안 이벤트에 대한 경고를 생성하는 방법을 보여 줍니다. 클러스터에 대한 원격 관리 액세스를 위해 텔넷 액세스가 구성된 경우 경고가 전송됩니다. 이와 동일한 방법을 사용하여 모든 보안 이벤트에 대한 알림을 만들 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
2. Alert Setup * 페이지에서 * Add * 를 클릭합니다.
3. 경고 추가 * 대화 상자에서 * 이름 * 을 클릭하고 경고의 이름과 설명을 입력합니다.
4. Resources * 를 클릭하고 이 경고를 활성화할 클러스터 또는 클러스터를 선택합니다.
5. 이벤트 * 를 클릭하고 다음 작업을 수행합니다.
   a. 이벤트 심각도 목록에서 * 경고 * 를 선택합니다.
   b. 일치하는 이벤트 목록에서 * 텔넷 프로토콜 사용 * 을 선택합니다.
6. Actions * 를 클릭한 다음 * Alert these users * 필드에서 경고 이메일을 수신할 사용자의 이름을 선택합니다.
7. 알림 빈도, SNMP 탭 실행 및 스크립트 실행을 위해 이 페이지의 다른 옵션을 구성합니다.
8. 저장 * 을 클릭합니다.

특정 보안 이벤트 비활성화

모든 이벤트는 기본적으로 활성화됩니다. 특정 이벤트를 비활성화하여 사용자 환경에서 중요하지 않은 이벤트에 대한 알림이 발생하지 않도록 할 수 있습니다. 알림 수신을 다시 시작하려면 사용하지 않는 이벤트를 설정할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이벤트를 사용하지 않도록 설정하면 시스템에서 이전에 생성된 이벤트가 사용되지 않는 것으로 표시되고 이러한 이벤트에 대해 구성된 알림이 트리거되지 않습니다. 비활성화된 이벤트를 활성화하면 다음 모니터링 주기부터 이러한 이벤트에 대한 알림이 생성됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 이벤트 설정 * 을 클릭합니다.
2. 이벤트 * 설정 페이지에서 다음 옵션 중 하나를 선택하여 이벤트를 비활성화하거나 활성화합니다.

원하는 작업	다음을 수행하십시오.
이벤트를 비활성화합니다	a. 비활성화 * 를 클릭합니다. b. 이벤트 비활성화 대화 상자에서 * 경고 * 심각도를 선택합니다. 모든 보안 이벤트의 범주입니다. c. 일치하는 이벤트 열에서 비활성화할 보안 이벤트를 선택한 다음 오른쪽 화살표를 클릭하여 해당 이벤트를 이벤트 사용 안 함 열로 이동합니다. d. 저장 후 닫기 * 를 클릭합니다. e. 사용하지 않도록 설정한 이벤트가 이벤트 설정 페이지의 목록 보기에 표시되는지 확인합니다.
이벤트 활성화	a. 비활성화된 이벤트 목록에서 다시 사용할 이벤트 또는 이벤트의 확인란을 선택합니다. b. 사용 * 을 클릭합니다.

보안 이벤트

보안 이벤트는 ONTAP 9_에 대한_NetApp 보안 강화 가이드에 정의된 매개 변수를 기반으로 ONTAP 클러스터, SVM(스토리지 가상 머신) 및 볼륨의 보안 상태에 대한 정보를 제공합니다. 이러한 이벤트는 잠재적 문제를 사용자에게 알려주기 때문에 심각도를 평가하고 필요한 경우 문제를 해결할 수 있습니다.

보안 이벤트는 소스 유형별로 그룹화되며 이벤트 및 트랩 이름, 영향 수준 및 심각도를 포함합니다. 이러한 이벤트는 클러스터 및 스토리지 VM 이벤트 범주에 표시됩니다.

백업 및 복원 작업 관리

Active IQ Unified Manager의 백업을 생성하고 복원 기능을 사용하여 시스템 장애 또는 데이터 손실 발생 시 동일한(로컬) 시스템이나 새(원격) 시스템에 백업을 복원할 수 있습니다.

Unified Manager를 설치한 운영 체제와 관리되는 클러스터 및 노드 수에 따라 세 가지 백업 및 복원 방법이 있습니다.

운영 체제	배포 규모	권장 백업 방법
VMware vSphere를 참조하십시오	모두	Unified Manager 가상 어플라이언스의 VMware 스냅샷
Red Hat Enterprise Linux 또는 CentOS Linux	작은 크기	Unified Manager MySQL 데이터베이스 덤프
	대형	Unified Manager 데이터베이스의 NetApp Snapshot
Microsoft Windows	작은 크기	Unified Manager MySQL 데이터베이스 덤프
	대형	iSCSI 프로토콜을 사용하는 Unified Manager 데이터베이스의 NetApp Snapshot

이러한 여러 가지 방법은 다음 섹션에서 설명합니다.

가상 어플라이언스의 **Unified Manager**에 대한 백업 및 복원

가상 어플라이언스에 설치된 Unified Manager의 백업 및 복원 모델은 전체 가상 애플리케이션의 이미지를 캡처하여 복원하는 것입니다.

다음 작업을 통해 가상 어플라이언스 백업을 완료할 수 있습니다.

1. VM의 전원을 끄고 Unified Manager 가상 어플라이언스의 VMware 스냅샷을 생성합니다.
2. 데이터 저장소에 NetApp Snapshot 복사본을 만들어 VMware 스냅샷을 캡처합니다.

   데이터 저장소가 ONTAP 소프트웨어를 실행하는 시스템에서 호스팅되지 않은 경우 스토리지 공급업체의 지침에 따라 VMware 스냅샷의 백업을 생성합니다.

3. NetApp 스냅샷 복사본 또는 그에 상응하는 스냅샷을 대체 스토리지에 복제합니다.
4. VMware 스냅샷을 삭제합니다.

이러한 작업을 사용하여 백업 일정을 구현하여 문제가 발생할 경우 Unified Manager 가상 어플라이언스를 보호해야 합니다.

VM을 복구하려면 생성한 VMware 스냅샷을 사용하여 VM을 백업 시점 상태로 복구할 수 있습니다.

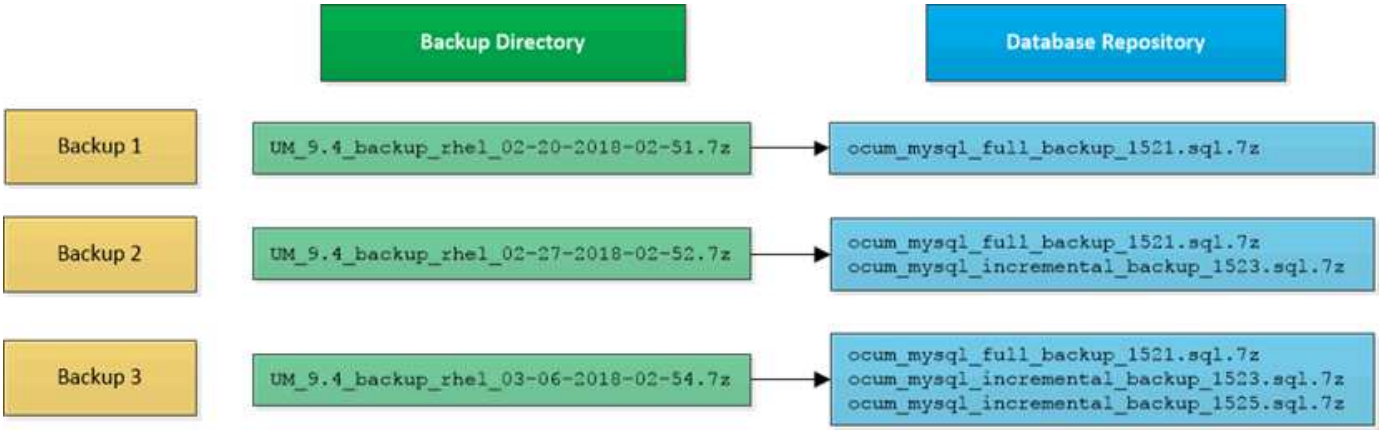
MySQL 데이터베이스 덤프를 사용하여 백업 및 복원

MySQL 데이터베이스 덤프 백업은 시스템 장애 또는 데이터 손실 시 사용할 수 있는 Active IQ Unified Manager 데이터베이스 및 구성 파일의 복사본입니다. 백업을 로컬 대상 또는 원격 대상에 기록하도록 예약할 수 있습니다. Active IQ Unified Manager 호스트 시스템 외부의 원격 위치를 정의하는 것이 좋습니다.

Linux 및 Windows 서버에 Unified Manager가 설치된 경우 MySQL 데이터베이스 덤프는 기본 백업 메커니즘입니다. 그러나 Unified Manager에서 많은 수의 클러스터와 노드를 관리하고 있거나 MySQL 백업을 완료하는 데 몇 시간이 걸리는 경우 Snapshot 복사본을 사용하여 백업할 수 있습니다. 이 기능은 Red Hat Enterprise Linux, CentOS Linux 시스템 및 Windows에서 사용할 수 있습니다.

데이터베이스 덤프 백업은 백업 디렉토리의 단일 파일과 데이터베이스 저장소 디렉토리에 있는 하나 이상의 파일로 구성됩니다. 백업 디렉토리의 파일은 백업을 다시 생성하는 데 필요한 데이터베이스 저장소 디렉토리에 있는 파일에 대한 포인터만 포함하므로 매우 작습니다.

데이터베이스 백업을 처음 생성할 때 단일 파일이 백업 디렉토리에 생성되고 전체 백업 파일이 데이터베이스 저장소 디렉터리에 생성됩니다. 다음에 백업을 생성할 때 백업 디렉토리에 단일 파일이 생성되고 전체 백업 파일과의 차이가 포함된 증분 백업 파일이 데이터베이스 저장소 디렉토리에 생성됩니다. 다음 그림과 같이 최대 보존 설정까지 추가 백업을 생성하면 이 프로세스가 계속됩니다.



이 두 디렉토리에 있는 백업 파일의 이름을 바꾸거나 제거하지 마십시오. 그렇지 않으면 이후의 복원 작업이 실패합니다.

백업 파일을 로컬 시스템에 쓰는 경우 전체 복원이 필요한 시스템 문제가 있는 경우 사용할 수 있도록 백업 파일을 원격 위치에 복사하는 프로세스를 시작해야 합니다.

백업 작업을 시작하기 전에 Active IQ Unified Manager는 무결성 검사를 수행하여 필요한 모든 백업 파일 및 백업 디렉토리가 존재하고 쓰기 가능한지 확인합니다. 또한 백업 파일을 생성할 수 있는 충분한 공간이 시스템에 있는지 확인합니다.

데이터베이스 덤프 백업에 대한 대상 및 스케줄 구성

Unified Manager 데이터베이스 덤프 백업 설정을 구성하여 데이터베이스 백업 경로, 보존 수 및 백업 일정을 설정할 수 있습니다. 매일 또는 매주 예약된 백업을 설정할 수 있습니다. 기본적으로 예약된 백업은 비활성화되어 있지만 백업 일정을 설정해야 합니다.

- 필요한 것 *

- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 백업 경로로 정의한 위치에서 최소 150GB의 공간을 사용할 수 있어야 합니다.

  Unified Manager 호스트 시스템 외부에 있는 원격 위치를 사용하는 것이 좋습니다.

- Linux 시스템에 Unified Manager가 설치되어 있고 MySQL 백업을 사용하는 경우 백업 디렉토리에 다음 사용 권한 및 소유권이 설정되어 있는지 확인하십시오.

  권한: 0750, 소유권: jboss: 유지 보수

- Unified Manager가 Windows 시스템에 설치되어 있고 MySQL 백업을 사용하는 경우 관리자만 백업 디렉토리에 액세스할 수 있어야 합니다.

첫 번째 백업은 전체 백업이므로 백업을 처음 수행할 때보다 더 많은 시간이 필요합니다. 전체 백업은 1GB가 넘고 3~4시간이 소요될 수 있습니다. 후속 백업은 증분 백업이므로 더 적은 시간이 필요합니다.

- 백업용으로 할당된 공간에 비해 증분 백업 파일 수가 너무 많은 경우 주기적으로 전체 백업을 수행하여 이전 백업과 해당 증분 파일을 대체할 수 있습니다. 다른 옵션으로 Snapshot 복사본을 사용하여 백업을 수행할 수 있습니다.
- 새 클러스터를 추가한 후 처음 15일 동안 수행된 백업은 성능 기록 데이터를 가져올 정도로 정확하지 않을 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 데이터베이스 백업 * 을 클릭합니다.
2. 데이터베이스 백업 * 페이지에서 * 백업 설정 * 을 클릭합니다.
3. 백업 경로, 보존 수 및 스케줄에 대한 적절한 값을 구성합니다.

   보존 수의 기본값은 10이며 무제한 백업을 생성하는 데 0을 사용할 수 있습니다.

4. Scheduled Daily * 또는 * Scheduled Weekly * 버튼을 선택한 후 일정 세부 정보를 지정합니다.
5. 적용 * 을 클릭합니다.

데이터베이스 덤프 백업 파일은 일정에 따라 생성됩니다. 데이터베이스 백업 페이지에서 사용 가능한 백업 파일을 볼 수 있습니다.

데이터베이스 복원이란 무엇입니까

MySQL 데이터베이스 복원은 기존의 Unified Manager 백업 파일을 동일한 또는 다른 Unified Manager 서버로 복원하는 프로세스입니다. Unified Manager 유지보수 콘솔에서 복원 작업을 수행합니다.

동일한(로컬) 시스템에서 복원 작업을 수행하고 백업 파일이 모두 로컬에 저장된 경우 기본 위치를 사용하여 복원 옵션을 실행할 수 있습니다. 다른 Unified Manager 시스템(원격 시스템)에서 복원 작업을 수행하는 경우 복원 옵션을 실행하기 전에 백업 파일을 보조 스토리지에서 로컬 디스크로 복사해야 합니다.

복원 프로세스 중에 Unified Manager에서 로그아웃됩니다. 복원 프로세스가 완료된 후 시스템에 로그인할 수 있습니다.

백업 이미지를 새 서버로 복원하는 경우 복원 작업이 완료된 후 새 HTTPS 보안 인증서를 생성하고 Unified Manager 서버를 다시 시작해야 합니다. 또한 백업 이미지를 새 서버로 복원할 때 필요한 경우 SAML 인증 설정을 다시 구성해야

합니다.

Unified Manager를 최신 버전의 소프트웨어로 업그레이드한 후에는 이전 백업 파일을 사용하여 이미지를 복원할 수 없습니다. 공간을 절약하기 위해 Unified Manager를 업그레이드할 때 최신 파일을 제외한 이전 백업 파일이 자동으로 제거됩니다.

- 관련 정보 *

"HTTPS 보안 인증서를 생성하는 중입니다"

"SAML 인증을 사용하도록 설정합니다"

"Active Directory 또는 OpenLDAP를 사용한 인증"

Linux 시스템에서 **MySQL** 데이터베이스 백업을 복원합니다

데이터 손실 또는 데이터 손상이 발생할 경우 Unified Manager를 최소한의 데이터 손실로 이전의 안정적인 상태로 복원할 수 있습니다. Unified Manager 유지 관리 콘솔을 사용하여 Unified Manager 데이터베이스를 로컬 또는 원격 Red Hat Enterprise Linux 또는 CentOS 시스템으로 복원할 수 있습니다.

- 필요한 것 *
- Unified Manager가 설치된 Linux 호스트에 대한 루트 사용자 자격 증명이 있어야 합니다.
- Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.
- Unified Manager 백업 파일과 데이터베이스 저장소 디렉터리의 내용을 복구 작업을 수행할 시스템에 복사해야 합니다.

  백업 파일을 기본 디렉토리 /data/ocum'-backup에 복사하는 것이 좋습니다. 데이터베이스 리포지토리 파일은 /'ocum-backup' 디렉토리 아래의 / database-dumps-repo 하위 디렉토리에 복사해야 합니다.

- 백업 파일은 반드시 .7z 형식이어야 합니다.

복원 기능은 플랫폼별 및 버전에 따라 다릅니다. Unified Manager 백업은 동일한 Unified Manager 버전에서만 복원할 수 있습니다. Linux 백업 파일 또는 가상 어플라이언스 백업 파일을 Red Hat Enterprise Linux 또는 CentOS 시스템으로 복원할 수 있습니다.

백업 폴더 이름에 공백이 포함된 경우 절대 경로 또는 상대 경로를 큰따옴표로 묶어야 합니다.

단계

1. 새 서버로 복원을 수행하는 경우 Unified Manager를 설치한 후 설치가 완료될 때 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마십시오. 백업 파일은 복원 프로세스 중에 이 정보를 채웁니다.
2. Secure Shell을 사용하여 Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다.
3. 유지보수 사용자(umadmin) 이름 및 암호를 사용하여 시스템에 로그인합니다.
4. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.
5. 유지보수 콘솔 * 메인 메뉴 * 에서 * 백업 복원 * 옵션의 번호를 입력합니다.
6. Restore MySQL Backup * 의 번호를 입력합니다.

7. 메시지가 표시되면 백업 파일의 절대 경로를 입력합니다.

```
Bundle to restore from: /data/ocum-
backup/UM_9.8.N151113.1348_backup_rhel_02-20-2020-04-45.7z
```

복원 작업이 완료되면 Unified Manager에 로그인할 수 있습니다.

백업을 복원한 후 OnCommand Workflow Automation 서버가 작동하지 않으면 다음 단계를 수행하십시오.

1. Workflow Automation 서버에서 Unified Manager 서버의 IP 주소를 최신 시스템을 가리키도록 변경합니다.
2. 1단계에서 획득에 실패한 경우 Unified Manager 서버에서 데이터베이스 암호를 재설정합니다.

Windows에서 **MySQL** 데이터베이스 백업을 복원합니다

데이터 손실 또는 데이터 손상이 발생할 경우 복원 기능을 사용하여 최소한의 손실로 Unified Manager를 이전의 안정적인 상태로 복원할 수 있습니다. Unified Manager 유지 관리 콘솔을 사용하여 Unified Manager MySQL 데이터베이스를 로컬 Windows 시스템 또는 원격 Windows 시스템으로 복원할 수 있습니다.

- 필요한 것 *
- Windows 관리자 권한이 있어야 합니다.
- Unified Manager 백업 파일과 데이터베이스 저장소 디렉터리의 내용을 복구 작업을 수행할 시스템에 복사해야 합니다.

  백업 파일을 기본 디렉터리 '\ProgramData\NetApp\OnCommandAppData\ocum\backup'에 복사하는 것이 좋습니다. 데이터베이스 리포지토리 파일은 '\backup' 디렉토리 아래의 '\database_dumps_repo' 하위 디렉토리에 복사해야 합니다.

- 백업 파일은 반드시 .7z 형식이어야 합니다.

복원 기능은 플랫폼별 및 버전에 따라 다릅니다. Unified Manager MySQL 백업은 동일한 Unified Manager 버전에서만 복원할 수 있고 Windows 백업은 Windows 플랫폼에서만 복원할 수 있습니다.

폴더 이름에 공백이 포함된 경우 백업 파일의 절대 경로 또는 상대 경로를 큰따옴표로 묶어야 합니다.

단계

1. 새 서버로 복원을 수행하는 경우 Unified Manager를 설치한 후 설치가 완료될 때 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마십시오. 백업 파일은 복원 프로세스 중에 이 정보를 채웁니다.
2. 관리자 자격 증명을 사용하여 Unified Manager 시스템에 로그인합니다.
3. Windows 관리자로 PowerShell 또는 명령 프롬프트를 시작합니다.
4. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.
5. 유지보수 콘솔 * 메인 메뉴 * 에서 * 백업 복원 * 옵션의 번호를 입력합니다.
6. Restore MySQL Backup * 의 번호를 입력합니다.
7. 메시지가 표시되면 백업 파일의 절대 경로를 입력합니다.

```
Bundle to restore from:
\ProgramData\NetApp\OnCommandAppData\ocum\backup\UM_9.8.N151118.2300_bac
kup_windows_02-20-2020-02-51.7z
```

복원 작업이 완료되면 Unified Manager에 로그인할 수 있습니다.

백업을 복원한 후 OnCommand Workflow Automation 서버가 작동하지 않으면 다음 단계를 수행하십시오.

1. Workflow Automation 서버에서 Unified Manager 서버의 IP 주소를 최신 시스템을 가리키도록 변경합니다.
2. 1단계에서 획득에 실패한 경우 Unified Manager 서버에서 데이터베이스 암호를 재설정합니다.

NetApp Snapshot을 사용한 백업 및 복원

NetApp 스냅샷 복사본은 시스템 장애 또는 데이터 손실 시 복원에 사용할 수 있는 Unified Manager 데이터베이스 및 구성 파일의 시점 이미지를 생성합니다. 항상 최신 복사본을 사용할 수 있도록 ONTAP 클러스터 중 하나의 볼륨에 정기적으로 스냅샷 복사본을 기록하도록 예약합니다.

가상 어플라이언스에 설치된 Active IQ Unified Manager에는 이 기능을 사용할 수 없습니다.

Linux에서 백업 구성

Active IQ Unified Manager가 Linux 시스템에 설치된 경우 NetApp Snapshot을 사용하여 백업 및 복원을 구성할 수 있습니다.

Snapshot 복사본은 보통 몇 분 정도밖에 걸리지 않으며, Unified Manager 데이터베이스가 매우 짧은 시간 동안 잠겨 있으므로 설치가 중단되는 것이 거의 없습니다. 마지막 스냅샷 복사본이 생성된 이후 파일에 대한 변경사항만 기록하므로 이미지는 최소한의 스토리지 공간을 소비하고 무시할 만한 성능 오버헤드를 발생시킵니다. ONTAP 클러스터에서 스냅샷이 생성되므로, 필요한 경우 SnapMirror와 같은 다른 NetApp 기능을 활용하여 2차 보호를 생성할 수 있습니다.

백업 작업을 시작하기 전에 Unified Manager에서 무결성 검사를 수행하여 대상 시스템을 사용할 수 있는지 확인합니다.

- 동일한 버전의 Active IQ Unified Manager에서만 스냅샷 복사본을 복원할 수 있습니다.

  예를 들어, Unified Manager 9.14에 백업을 생성한 경우 Unified Manager 9.14 시스템에서만 백업을 복원할 수 있습니다.

- 스냅샷 구성이 변경된 경우 스냅샷이 잘못될 수 있습니다.

스냅샷 복사본 위치를 구성하는 중입니다

ONTAP 시스템 관리자 또는 ONTAP CLI를 사용하여 ONTAP 클러스터 중 하나에서 스냅샷 복사본이 저장될 볼륨을 구성할 수 있습니다.

- 필요한 것 *

클러스터, 스토리지 VM 및 볼륨은 다음 요구사항을 충족해야 합니다.

- 클러스터 요구 사항:
  - ONTAP 9.3 이상을 설치해야 합니다
  - Unified Manager 서버와 지리적으로 가까운 곳에 있어야 합니다
  - Unified Manager를 통해 모니터링할 수 있지만 반드시 필요한 것은 아닙니다
- 스토리지 VM 요구 사항:
  - 이름 스위치와 이름 매핑은 ""파일""을 사용하도록 설정되어야 합니다.
  - 클라이언트 측 사용자와 일치하도록 생성된 로컬 사용자입니다
  - 모든 읽기/쓰기 권한이 선택되어 있는지 확인합니다
  - 수출 정책에서 슈퍼유저 액세스가 ""모두""로 설정되어 있는지 확인하십시오
  - Linux용 NetApp Snapshot용 NFS
  - NFSv4는 클라이언트 및 스토리지 VM에 지정된 NFS 서버 및 NFSv4 ID 도메인에서 설정해야 합니다
  - 이 볼륨은 Unified Manager/opt/NetApp/data 디렉토리의 최소 2배가 되어야 합니다

    du-sh/opt/netapp/data/ 명령을 사용하여 현재 크기를 확인합니다.
- 볼륨 요구 사항:
  - 이 볼륨은 Unified Manager/opt/NetApp/data 디렉토리의 최소 2배가 되어야 합니다
  - 보안 스타일을 UNIX로 설정해야 합니다
  - 로컬 스냅샷 정책을 해제해야 합니다
  - 볼륨 자동 크기 조정이 활성화되어야 합니다
  - 고성능 서비스 수준은 높은 IOPS와 낮은 지연 시간(예: "Extreme")을 가진 정책으로 설정해야 합니다.

NFS 볼륨을 생성하는 자세한 단계는 를 참조하십시오 "ONTAP 9에서 NFSv4를 구성하는 방법" 및 "ONTAP 9 NFS 구성 익스프레스 가이드 를 참조하십시오".

스냅샷 복사본의 대상 위치 지정

ONTAP 클러스터 중 하나에 이미 구성되어 있는 볼륨의 Active IQ Unified Manager 스냅샷 복사본에 대한 대상 위치를 구성해야 합니다. 유지보수 콘솔을 사용하여 위치를 정의해야 합니다.

- Active IQ Unified Manager가 설치된 Linux 호스트에 대한 루트 사용자 자격 증명이 있어야 합니다.
- Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.
- 클러스터 관리 IP 주소, 스토리지 VM 이름, 볼륨 이름 및 스토리지 시스템 사용자 이름과 암호가 있어야 합니다.
- Active IQ Unified Manager 호스트에 볼륨을 마운트해야 하며 마운트 경로가 있어야 합니다.

단계

1. 보안 셸을 사용하여 Active IQ Unified Manager 시스템의 IP 주소 또는 FQDN에 연결합니다.
2. 유지보수 사용자(umadmin) 이름 및 암호를 사용하여 시스템에 로그인합니다.

3. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.
4. 유지보수 콘솔 * 메인 메뉴 * 에서 * 백업 복원 * 옵션의 번호를 입력합니다.
5. Configure NetApp Snapshot Backup * 의 번호를 입력합니다.
6. NFS를 구성할 번호를 입력합니다.
7. 제공해야 할 정보를 검토한 다음 * 백업 구성 세부 정보 입력 * 에 대한 번호를 입력합니다.
8. 스냅샷을 기록할 볼륨을 식별하려면 클러스터 관리 인터페이스의 IP 주소, 스토리지 VM 이름, 볼륨 이름, LUN 이름, 스토리지 시스템 사용자 이름 및 암호, 마운트 경로를 입력합니다.
9. 이 정보를 확인하고 y를 입력합니다.

   시스템은 다음 작업을 수행합니다.

   ◦ 클러스터에 대한 연결을 설정합니다
   ◦ 모든 서비스를 중지합니다
   ◦ 볼륨에 새 디렉토리를 생성하고 Active IQ Unified Manager 데이터베이스 구성 파일을 복사합니다
   ◦ Active IQ Unified Manager에서 파일을 삭제하고 새 데이터베이스 디렉터리에 대한 symlink를 만듭니다
   ◦ 모든 서비스를 다시 시작합니다
10. 아직 시작하지 않은 경우 유지보수 콘솔을 종료하고 Active IQ Unified Manager 인터페이스를 시작하여 스냅샷 복사본에 대한 일정을 생성합니다.

Windows에서 백업을 구성합니다

Active IQ Unified Manager는 iSCSI 프로토콜을 사용하는 LUN의 도움으로 Windows 운영 체제에서 NetApp 스냅샷을 사용하여 백업 및 복원을 지원합니다.

모든 Unified Manager 서비스가 실행되는 동안 스냅샷 기반 백업을 수행할 수 있습니다. 백업이 전체 데이터베이스에 글로벌 읽기 잠금을 설정하면 동시 쓰기를 방지할 수 있으므로 스냅샷의 일부로 데이터베이스의 정합성이 보장되는 상태가 캡처됩니다. Windows OS에 설치된 Unified Manager 시스템에서 NetApp Snapshot을 사용하여 백업 및 복원을 수행하려면 먼저 유지보수 콘솔을 사용하여 Unified Manager 백업을 Snapshot에 구성해야 합니다.

Unified Manager에서 스냅샷 복사본을 생성하도록 구성하기 전에 다음 구성 작업을 수행해야 합니다.

- ONTAP 클러스터를 구성합니다
- Windows 호스트 시스템을 구성합니다

Windows의 백업 위치 구성

Windows에서 Unified Manager를 백업한 후 Snapshot 복사본을 저장할 볼륨을 구성해야 합니다.

- 필요한 것 *

클러스터, 스토리지 VM 및 볼륨은 다음 요구사항을 충족해야 합니다.

- 클러스터 요구 사항:
  ◦ ONTAP 9.3 이상을 설치해야 합니다

- Unified Manager 서버와 지리적으로 가까운 곳에 있어야 합니다
- Unified Manager에서 모니터링합니다

- 스토리지 VM 요구 사항:
  - ONTAP 클러스터의 iSCSI 접속 구성
  - 구성된 시스템에 대해 iSCSI 프로토콜을 활성화해야 합니다
  - 백업 구성을 위해서는 전용 볼륨과 LUN이 있어야 합니다. 선택한 볼륨에는 LUN이 하나만 포함되어야 하며 다른 볼륨은 없어야 합니다.
  - LUN 크기는 9.9 Active IQ Unified Manager에서 처리할 것으로 예상되는 데이터 크기의 2배 이상이어야 합니다.

    그러면 볼륨에도 동일한 크기 요구 사항이 설정됩니다.

  - 모든 읽기/쓰기 권한이 선택되어 있는지 확인합니다
  - 수출 정책에서 슈퍼유저 액세스가 ""모두""로 설정되어 있는지 확인하십시오
- 볼륨 및 LUN 요구 사항:
  - 이 볼륨은 Unified Manager MySQL 데이터 디렉토리의 최소 2배가 되어야 합니다.
  - 보안 스타일을 Windows로 설정해야 합니다
  - 로컬 스냅샷 정책을 해제해야 합니다
  - 볼륨 자동 크기 조정이 활성화되어야 합니다
  - 고성능 서비스 수준은 높은 IOPS와 낮은 지연 시간(예: "Extreme")을 가진 정책으로 설정해야 합니다.

ONTAP 클러스터를 구성하는 중입니다

ONTAP 시스템에서 스냅샷 복사본을 사용하여 Active IQ Unified Manager를 백업 및 복원하려면 먼저 Windows 클러스터에서 몇 가지 사전 구성 단계를 수행해야 합니다.

명령 프롬프트나 System Manager 사용자 인터페이스를 사용하여 ONTAP 클러스터를 구성할 수 있습니다. ONTAP 클러스터를 구성하려면 스토리지 VM에 iSCSI LIF로 할당할 수 있도록 데이터 LIF를 구성해야 합니다. 다음 단계는 System Manager 사용자 인터페이스를 사용하여 iSCSI 지원 스토리지 VM을 구성하는 것입니다. LIF가 아웃바운드 트래픽에 네트워크를 사용하는 방법을 제어하려면 이 스토리지 VM에 대한 정적 네트워크 경로를 구성해야 합니다.

백업 구성을 위해서는 전용 볼륨과 LUN이 있어야 합니다. 선택한 볼륨에 LUN이 하나만 포함되어야 합니다. LUN 크기는 Active IQ Unified Manager에서 처리할 수 있을 것으로 예상되는 데이터 크기의 2배 이상이어야 합니다.

다음 구성을 수행해야 합니다.

단계

1. iSCSI 지원 스토리지 VM을 구성하거나 동일한 구성을 가진 기존 스토리지 VM을 사용합니다.
2. 구성된 스토리지 VM에 대한 네트워크 라우트를 구성합니다.
3. 볼륨이 이 LUN 전용인지 확인하기 위해 적절한 용량의 볼륨과 내부의 단일 LUN을 구성합니다.

System Manager에서 LUN을 생성할 때 LUN 매핑을 해제하면 igroup이 삭제되고 복원이 실패할 수 있습니다. 이 시나리오를 방지하려면 LUN을 생성하는 동안 LUN이 명시적으로 생성되고 LUN이 매핑 해제될 때 삭제되지 않도록 해야 합니다.

4. 스토리지 VM에서 이니시에이터 그룹을 구성합니다.
5. 포트 세트를 구성합니다.
6. igroup을 포트셋 통합
7. LUN을 igroup에 매핑합니다.

Windows 호스트 시스템을 구성하는 중입니다

NetApp Snapshot을 사용하여 Active IQ Unified Manager를 백업 및 복원하려면 Windows 호스트 시스템을 구성해야 합니다. Windows 호스트 시스템에서 Microsoft iSCSI 초기자를 시작하려면 검색 표시줄에 ""iSCSI""를 입력하고 * iSCSI 초기자 * 를 클릭합니다.

- 필요한 것 *

호스트 시스템에서 이전 구성을 정리해야 합니다.

Windows를 새로 설치할 때 iSCSI 초기자를 시작하려고 하면 확인 메시지가 표시되고 확인 메시지가 표시되면 iSCSI 속성 대화 상자가 표시됩니다. 기존 Windows 설치인 경우 iSCSI 속성 대화 상자가 비활성이거나 연결을 시도하는 대상과 함께 표시됩니다. 따라서 Windows 호스트의 이전 구성이 모두 제거되었는지 확인해야 합니다.

단계

1. 호스트 시스템에서 이전 구성을 모두 정리합니다.
2. 대상 포털을 검색합니다.
3. 대상 포털에 연결합니다.
4. 대상 포털에 다중 경로를 사용하여 연결합니다.
5. 두 LIF를 모두 확인하십시오.
6. Windows 시스템에서 디바이스로 구성된 LUN을 검색합니다.
7. Windows에서 검색된 LUN을 새 볼륨 드라이브로 구성합니다.

Windows에서 스냅샷 복사본의 대상 위치 지정

ONTAP 클러스터 중 하나에 이미 구성되어 있는 볼륨의 Active IQ Unified Manager 스냅샷 복사본에 대한 대상 위치를 구성해야 합니다. 유지보수 콘솔을 사용하여 위치를 정의해야 합니다.

- Active IQ Unified Manager가 설치된 Windows 호스트에 대한 관리자 권한이 있어야 합니다.
- Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.
- 클러스터 관리 IP 주소, 스토리지 VM 이름, 볼륨 이름, LUN 이름 및 스토리지 시스템 사용자 이름과 암호가 있어야 합니다.
- Active IQ Unified Manager 호스트에 볼륨을 네트워크 드라이브로 마운트해야 하며 마운트 드라이브가 있어야 합니다.

단계

1. Power Shell을 사용하여 Active IQ Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다.
2. 유지보수 사용자(umadmin) 이름 및 암호를 사용하여 시스템에 로그인합니다.
3. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.
4. 유지보수 콘솔 * 메인 메뉴 * 에서 * 백업 복원 * 옵션의 번호를 입력합니다.
5. Configure NetApp Snapshot Backup * 의 번호를 입력합니다.
6. iSCSI를 구성할 번호를 입력합니다.
7. 제공해야 할 정보를 검토한 다음 * 백업 구성 세부 정보 입력 * 에 대한 번호를 입력합니다.
8. 스냅샷을 기록할 볼륨을 식별하려면 클러스터 관리 인터페이스의 IP 주소, 스토리지 VM 이름, 볼륨 이름, LUN 이름, 스토리지 시스템 사용자 이름 및 암호, 마운트 드라이브를 입력합니다.
9. 이 정보를 확인하고 y를 입력합니다.

   시스템은 다음 작업을 수행합니다.

   - 스토리지 VM이 검증되었습니다
   - 볼륨이 확인되었습니다
   - 드라이브 마운트 및 상태가 확인되었습니다
   - LUN 존재 및 상태입니다
   - 네트워크 드라이브가 있습니다
   - 마운트된 볼륨에 권장 공간(MySQL 데이터 디렉토리의 2배 이상)이 있는지 확인합니다
   - 볼륨의 전용 LUN에 해당하는 LUN 경로입니다
   - iGroup 이름입니다
   - 네트워크 드라이브가 마운트된 볼륨의 GUID입니다
   - ONTAP와 통신하는 데 사용되는 iSCSI 이니시에이터입니다
10. 유지보수 콘솔을 종료하고 Active IQ Unified Manager 인터페이스를 실행하여 스냅샷 복사본의 일정을 생성합니다.

유지보수 콘솔에서 **Snapshot** 복사본으로 백업을 구성합니다

스냅샷 복사본을 사용하여 Active IQ Unified Manager 백업을 수행하려면 유지보수 콘솔에서 몇 가지 구성 단계를 수행해야 합니다.

- 필요한 것 *

시스템에 대한 다음 세부 정보가 있어야 합니다.

- 클러스터 IP 주소입니다
- 스토리지 VM 이름입니다
- 볼륨 이름입니다
- LUN 이름입니다

- 마운트 경로
- 스토리지 시스템 자격 증명

단계

1. Unified Manager의 유지보수 콘솔에 액세스합니다.
2. 4 를 입력하여 * 백업 복원 * 을 선택합니다.
3. 2를 입력하여 NetApp Snapshot * 을 사용한 백업 및 복원을 선택합니다.

   백업 구성을 변경하려면 3을 입력하여 * NetApp Snapshot 백업 구성 업데이트 * 를 선택합니다. 암호만 업데이트할 수 있습니다.

4. 메뉴에서 1을 입력하여 * Configure NetApp Snapshot Backup * 을 선택합니다.
5. 1을 입력하여 필요한 정보를 제공합니다.
6. 유지보수 콘솔의 사용자 이름과 암호를 입력한 다음 LUN이 호스트에 마운트되었음을 확인합니다.

   그런 다음 이 프로세스에서 데이터 디렉토리, LUN 경로, 스토리지 VM, 볼륨, 공간 가용성 드라이브 등이 정답입니다. 백그라운드에서 진행 중인 작업은 다음과 같습니다.

   - 서비스가 중지되었습니다
   - 데이터베이스 디렉토리가 마운트된 스토리지로 이동됩니다
   - 데이터베이스 디렉토리가 삭제되고 symlink가 설정됩니다
   - Active IQ Unified Manager 인터페이스에서 구성이 완료되면 서비스가 다시 시작됩니다. 백업 유형은 NetApp Snapshot으로 수정되며 사용자 인터페이스에 데이터베이스 백업(스냅샷 기반)으로 반영됩니다.

백업 작업을 시작하기 전에 스냅샷 구성이 변경되었는지 확인해야 합니다. 스냅샷이 잘못될 수 있기 때문입니다. G 드라이브에서 백업을 구성하고 스냅샷을 촬영했다고 가정해 보겠습니다. 나중에 백업을 E 드라이브로 재구성하고 새 구성에 따라 데이터가 E 드라이브에 저장됩니다. G 드라이브에 있던 동안 생성된 스냅샷을 복원하려고 하면 G 드라이브가 존재하지 않는다는 오류와 함께 실패합니다.

Linux 및 **Windows**에 대한 백업 일정 정의

Unified Manager UI를 사용하여 Unified Manager 스냅샷 복사본이 생성되는 일정을 구성할 수 있습니다.

- 필요한 것 *
- 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스냅샷을 생성할 대상을 식별하려면 유지보수 콘솔에서 스냅샷 복사본을 생성하기 위한 설정을 구성해야 합니다.

Snapshot 복사본은 몇 분 내에 생성되며 Unified Manager 데이터베이스는 몇 초 동안만 잠깁니다.

새 클러스터를 추가한 후 처음 15일 동안 수행된 백업은 성능 기록 데이터를 가져올 정도로 정확하지 않을 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * 데이터베이스 백업 * 을 클릭합니다.

2. 데이터베이스 백업 * 페이지에서 * 백업 설정 * 을 클릭합니다.
3. Retention Count * 필드에 유지할 최대 스냅샷 복사본 수를 입력합니다.

   보존 수의 기본값은 10입니다. 최대 스냅샷 복사본 수는 클러스터의 ONTAP 소프트웨어 버전에 따라 결정됩니다. 이 필드를 비워 두면 ONTAP 버전에 관계없이 최대값을 구현할 수 있습니다.

4. Scheduled Daily * 또는 * Scheduled Weekly * 버튼을 선택한 후 일정 세부 정보를 지정합니다.
5. 적용 * 을 클릭합니다.

스냅샷 복사본은 일정에 따라 생성됩니다. 데이터베이스 백업 페이지에서 사용 가능한 백업 파일을 볼 수 있습니다.

이 볼륨과 스냅샷의 중요성으로 인해 이 볼륨에 대해 한두 개의 알림을 생성하여 다음 중 하나가 발생할 때 알림을 받을 수 있습니다.

- 볼륨 공간이 90% 찼습니다. 볼륨 공간이 가득 참 * 이벤트를 사용하여 경고를 설정합니다.

  ONTAP System Manager 또는 ONTAP CLI를 사용하여 볼륨에 용량을 추가하면 Unified Manager 데이터베이스의 공간이 부족하지 않게 됩니다.

- 스냅샷 수가 최대 수에 근접합니다. 이벤트 * 너무 많은 Snapshot 복사본 * 을 사용하여 알림을 설정합니다.

  ONTAP System Manager 또는 ONTAP CLI를 사용하여 이전 스냅샷을 삭제할 수 있으므로 항상 새 스냅샷 복사본을 저장할 공간이 있습니다.

경고 설정 페이지에서 경고를 구성합니다.

스냅샷 복사본을 사용하여 **Unified Manager** 복원

데이터 손실 또는 데이터 손상이 발생할 경우 Unified Manager를 최소한의 데이터 손실로 이전의 안정적인 상태로 복원할 수 있습니다. Unified Manager 유지보수 콘솔을 사용하여 Unified Manager 스냅샷 데이터베이스를 로컬 또는 원격 운영 체제로 복원할 수 있습니다.

- 필요한 것 *
- Linux 호스트에 대한 루트 사용자 자격 증명과 Unified Manager가 설치된 Windows 호스트 시스템에 대한 관리 권한이 있어야 합니다.
- Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.

복원 기능은 플랫폼별 및 버전에 따라 다릅니다. Unified Manager 백업은 동일한 Unified Manager 버전에서만 복원할 수 있습니다.

단계

1. Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다.
   - Linux: 보안 셸
   - Windows:Power Shell
2. 루트 사용자 자격 증명을 사용하여 시스템에 로그인합니다.
3. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.
4. 유지보수 콘솔 * 메인 메뉴 * 에서 * 백업 복원 * 옵션에 대해 4를 입력합니다.

5. 2를 입력하여 NetApp Snapshot * 을 사용하여 백업 및 복원을 선택합니다.

   새 서버로 복원을 수행하는 경우 Unified Manager를 설치한 후 설치가 완료될 때 UI를 실행하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마십시오. 1을 입력하여 * NetApp Snapshot Backup 구성 * 을 선택한 후, 원래 시스템에 있는 스냅샷 복사본의 설정을 구성합니다.

6. 3을 입력하여 NetApp Snapshot * 을 사용하여 복원 * 을 선택합니다.
7. Unified Manager를 복원할 스냅샷 복사본을 선택합니다. Enter * 를 누릅니다.
8. 복원 프로세스가 완료되면 Unified Manager 사용자 인터페이스에 로그인합니다.

백업을 복원한 후 Workflow Automation 서버가 작동하지 않으면 다음 단계를 수행하십시오.

1. Workflow Automation 서버에서 Unified Manager 서버의 IP 주소를 최신 시스템을 가리키도록 변경합니다.
2. 1단계에서 획득에 실패한 경우 Unified Manager 서버에서 데이터베이스 암호를 재설정합니다.

백업 유형 수정

Active IQ Unified Manager 시스템의 백업 유형을 변경하려면 유지보수 콘솔 옵션을 사용할 수 있습니다. NetApp Snapshot Backup * 구성 취소 옵션을 사용하면 MySQL 기반 백업으로 되돌아갈 수 있습니다.

- 필요한 것 *

Unified Manager 서버의 유지보수 콘솔에 로그인하려면 사용자 ID와 암호가 필요합니다.

단계

1. 유지보수 콘솔에 액세스합니다.
2. 백업 및 복원을 위해 * 메인 메뉴 * 에서 4 를 선택합니다.
3. 백업 및 복원 메뉴 * 에서 2를 선택합니다.
4. NetApp Snapshot Backup * 의 구성 취소 * 에 대해 4를 선택합니다.

   수행되는 작업이 표시됩니다. 즉, 서비스를 중지하고, symlink를 중단하고, 데이터를 스토리지에서 디렉터리로 이동한 다음 서비스를 다시 시작합니다.

   백업 방법이 수정된 후 백업 메커니즘이 스냅샷 복사본에서 기본 MySQL 백업으로 변경됩니다. 이 변경 사항은 일반 설정의 데이터베이스 백업 섹션에 나타납니다.

Unified Manager의 필요 시 백업

Active IQ Unified Manager 사용자 인터페이스를 사용하여 필요할 때마다 필요 시 백업을 생성할 수 있습니다. 필요 시 백업을 사용하면 기존 백업 방법을 사용하여 즉시 백업을 생성할 수 있습니다. 필요 시 백업은 MySQL과 NetApp Snapshot 기반 백업을 구분하지 않습니다.

데이터베이스 백업 페이지의 * 지금 백업 * 버튼을 사용하여 필요 시 백업을 수행할 수 있습니다. 필요 시 백업은 Active IQ Unified Manager에 대해 구성한 스케줄에 따라 달라지지 않습니다.

Unified Manager를 실행하는 호스트 운영 체제를 변경하려면 Unified Manager MySQL 데이터베이스 덤프 백업을 가상 어플라이언스에서 Red Hat Enterprise Linux 또는 CentOS Linux 시스템으로 복구할 수 있습니다.

- 필요한 것 *
- 가상 어플라이언스:
  - 운영자, 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
  - 복원 작업에 사용할 Unified Manager 유지보수 사용자의 이름을 알아야 합니다.
- Linux 시스템에서 다음을 수행합니다.
  - 의 지침에 따라 Linux 서버에 Unified Manager를 설치해야 합니다 "Linux 시스템에 Unified Manager 설치".
  - 이 서버의 Unified Manager 버전은 백업 파일을 사용하는 가상 어플라이언스의 버전과 동일해야 합니다.
  - 설치 후 Linux 시스템에서 UI를 시작하거나 클러스터, 사용자 또는 인증 설정을 구성하지 마십시오. 백업 파일은 복원 프로세스 중에 이 정보를 채웁니다.
  - Linux 호스트에 대한 루트 사용자 자격 증명이 있어야 합니다.

다음 단계에서는 가상 어플라이언스에 백업 파일을 생성하고 백업 파일을 Red Hat Enterprise Linux 또는 CentOS 시스템에 복사한 다음 데이터베이스 백업을 새 시스템으로 복원하는 방법을 설명합니다.

단계

1. 가상 어플라이언스에서 * 관리 * > * 데이터베이스 백업 * 을 클릭합니다.
2. 데이터베이스 백업 * 페이지에서 * 백업 설정 * 을 클릭합니다.
3. 백업 경로를 /jail/support로 변경합니다.
4. Schedule 섹션에서 * Scheduled Daily * 를 선택하고 현재 시간 이후 몇 분 동안 백업을 생성할 시간을 입력합니다.
5. 적용 * 을 클릭합니다.
6. 백업이 생성될 때까지 몇 시간 정도 기다립니다.

   전체 백업은 1GB가 넘고 완료하는 데 3~4시간이 걸릴 수 있습니다.

7. Unified Manager가 설치된 Linux 호스트에 루트 사용자로 로그인하고 SCP를 사용하여 가상 어플라이언스에 대한 지원/지원 파일에서 백업 파일을 복사합니다.' root@<rhel_server>:/#scp -r admin@<vapp_server_ip_address>:/support/ *

   'root@ocum_rhel-21:/#scp-r admin@10.10.10.10:/support/ *.

   /database-dumps-repo 하위 디렉터리에 .7z 백업 파일과 모든 .7z 리포지토리 파일을 복사했는지 확인합니다.

8. 명령 프롬프트에서 'um backup restore -f/<backup_file_path>/<backup_file_name>' 백업을 복구합니다

   'um backup restore-f/UM_9.7.N151113.1348_backup_UNIX_02-12-2019-04-16.7z

9. 복원 작업이 완료되면 Unified Manager 웹 UI에 로그인합니다.

다음 작업을 수행해야 합니다.

- 새 HTTPS 보안 인증서를 생성하고 Unified Manager 서버를 다시 시작합니다.
- Linux 시스템에 /jail/support 경로가 없기 때문에 백업 경로를 Linux 시스템의 기본 설정(/data/ocum-backup) 또는 선택한 새 경로로 변경합니다.
- WFA를 사용 중인 경우 Workflow Automation 연결의 양측을 다시 구성하십시오.
- SAML을 사용하는 경우 SAML 인증 설정을 다시 구성하십시오.

Linux 시스템에서 모든 기능이 예상대로 실행되고 있는지 확인한 후 Unified Manager 가상 어플라이언스를 종료 및 제거할 수 있습니다.

스크립트 관리

스크립트를 사용하여 Unified Manager에서 여러 스토리지 오브젝트를 자동으로 수정 또는 업데이트할 수 있습니다. 스크립트가 경고와 연결되어 있습니다. 이벤트가 경고를 트리거하면 스크립트가 실행됩니다. 사용자 지정 스크립트를 업로드하고 경고가 생성될 때 해당 스크립트를 테스트할 수 있습니다.

스크립트를 Unified Manager에 업로드하여 실행할 수 있는 기능은 기본적으로 활성화되어 있습니다. 보안상의 이유로 조직에서 이 기능을 허용하지 않으려는 경우 * 스토리지 관리 * > * 기능 설정 * 에서 이 기능을 비활성화할 수 있습니다.

스크립트가 경고와 함께 작동하는 방식

알림을 스크립트에 연결하여 Unified Manager의 이벤트에 대한 알림이 발생할 때 스크립트가 실행되도록 할 수 있습니다. 스크립트를 사용하여 스토리지 오브젝트 문제를 해결하거나 이벤트를 생성하고 있는 스토리지 오브젝트를 식별할 수 있습니다.

Unified Manager에서 이벤트에 대한 알림이 생성되면 지정된 수신자에게 알림 이메일이 전송됩니다. 경고와 스크립트를 연결한 경우 스크립트가 실행됩니다. 알림 e-메일에서 스크립트에 전달된 인수의 세부 정보를 확인할 수 있습니다.

사용자 지정 스크립트를 만들어 특정 이벤트 유형에 대한 경고와 연결한 경우 해당 이벤트 유형에 대한 사용자 지정 스크립트를 기반으로 작업이 수행되며, 관리 작업 페이지나 Unified Manager 대시보드에서 기본적으로 * Fix it * 작업을 사용할 수 없습니다.

스크립트는 실행에 다음 인수를 사용합니다.

- ``eventID’
- '- 이벤트 이름'
- '-eventSeverity’입니다
- '-eventSourceID’입니다
- '-eventSourceName’입니다
- '-eventSourceType’입니다
- '-eventState’입니다
- '-EventArgs'

스크립트의 인수를 사용하여 관련 이벤트 정보를 수집하거나 스토리지 객체를 수정할 수 있습니다.

스크립트에서 인수를 가져오는 예제

```
print "$ARGV[0] : $ARGV[1]\n"
print "$ARGV[7] : $ARGV[8]\n"
```

경고가 생성되면 이 스크립트가 실행되고 다음 출력이 표시됩니다.

```
-eventID : 290
-eventSourceID : 4138
```

스크립트 추가

Unified Manager에 스크립트를 추가하고 스크립트를 알림에 연결할 수 있습니다. 이러한 스크립트는 경고가 생성될 때 자동으로 실행되며, 이벤트를 생성할 스토리지 개체에 대한 정보를 가져올 수 있습니다.

- 필요한 것 *
- Unified Manager 서버에 추가할 스크립트를 작성하여 저장해야 합니다.
- 스크립트에 지원되는 파일 형식은 Perl, Shell, PowerShell, Python 및 .bat입니다.

Unified Manager가 설치된 플랫폼입니다	지원되는 언어
VMware	Perl 및 Shell 스크립트
리눅스	Perl, Python 및 Shell 스크립트
Windows	PowerShell, Perl, Python 및 .bat 스크립트

  - Perl 스크립트의 경우, Perl을 Unified Manager 서버에 설치해야 합니다. VMware 설치의 경우 Perl 5가 기본적으로 설치되며 스크립트는 Perl 5가 지원하는 것만 지원합니다. Unified Manager 후에 Perl이 설치된 경우 Unified Manager 서버를 다시 시작해야 합니다.
  - PowerShell 스크립트의 경우 스크립트를 실행할 수 있도록 Windows 서버에 적절한 PowerShell 실행 정책을 설정해야 합니다.

> ⓘ 스크립트가 알림 스크립트 진행률을 추적하기 위해 로그 파일을 생성할 경우 Unified Manager 설치 폴더 내 로그 파일이 생성되지 않도록 해야 합니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

사용자 지정 스크립트를 업로드하고 알림에 대한 이벤트 세부 정보를 수집할 수 있습니다.

> ⓘ 사용자 인터페이스에서 이 기능을 사용할 수 없는 경우 관리자가 해당 기능을 비활성화했기 때문입니다. 필요한 경우 * 스토리지 관리 * > * 기능 설정 * 에서 이 기능을 활성화할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 스크립트 * 를 클릭합니다.
2. 스크립트 * 페이지에서 * 추가 * 를 클릭합니다.
3. 스크립트 * 추가 대화 상자에서 * 찾아보기 * 를 클릭하여 스크립트 파일을 선택합니다.
4. 선택한 스크립트에 대한 설명을 입력합니다.
5. 추가 * 를 클릭합니다.

스크립트를 삭제하는 중입니다

스크립트가 더 이상 필요하지 않거나 유효하지 않은 경우 Unified Manager에서 스크립트를 삭제할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 스크립트는 경고와 연관되지 않아야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 스크립트 * 를 클릭합니다.
2. 스크립트 * 페이지에서 삭제할 스크립트를 선택한 다음 * 삭제 * 를 클릭합니다.
3. 경고 * 대화 상자에서 * 예 * 를 클릭하여 삭제를 확인합니다.

스크립트 실행 테스트 중

스토리지 객체에 대한 알림이 생성될 때 스크립트가 올바르게 실행되는지 확인할 수 있습니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 지원되는 파일 형식의 스크립트를 Unified Manager에 업로드해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 스크립트 * 를 클릭합니다.
2. 스크립트 페이지에서 테스트 스크립트를 추가합니다.
3. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 경고 설정 * 을 클릭합니다.
4. Alert Setup* 페이지에서 다음 작업 중 하나를 수행합니다.

대상...	수행할 작업...
알림을 추가합니다	a. 추가 * 를 클릭합니다. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.
알림을 편집합니다	a. 알림을 선택한 다음 * 편집 * 을 클릭합니다. b. 작업 섹션에서 알림을 테스트 스크립트와 연결합니다.

5. 저장 * 을 클릭합니다.
6. Alert Setup * 페이지에서 추가하거나 수정한 알림을 선택한 다음 * Test * 를 클릭합니다.

   스크립트는 ""-test" 인수를 사용하여 실행되며 알림을 만들 때 지정된 e-메일 주소로 알림 알림이 전송됩니다.

그룹 관리 및 모니터링

Unified Manager에서 그룹을 생성하여 스토리지 객체를 관리할 수 있습니다.

그룹 이해

Unified Manager에서 그룹을 생성하여 스토리지 객체를 관리할 수 있습니다. 그룹에 대한 개념 및 그룹 규칙을 사용하여 그룹에 스토리지 객체를 추가하는 방법을 이해하면 환경에서 스토리지 객체를 관리하는 데 도움이 됩니다.

그룹이란 무엇인가

그룹은 이기종 스토리지 오브젝트(클러스터, SVM 또는 볼륨)의 동적 모음입니다. Unified Manager에서 그룹을 생성하여 스토리지 객체 세트를 쉽게 관리할 수 있습니다. 그룹의 구성원은 특정 시점에 Unified Manager에서 모니터링하는 스토리지 개체에 따라 변경될 수 있습니다.

- 각 그룹에는 고유한 이름이 있습니다.
- 각 그룹에 대해 최소 하나의 그룹 규칙을 구성해야 합니다.
- 그룹을 둘 이상의 그룹 규칙과 연결할 수 있습니다.
- 각 그룹에는 클러스터, SVM 또는 볼륨과 같은 여러 유형의 스토리지 객체가 포함될 수 있습니다.
- 그룹 규칙이 생성될 때 또는 Unified Manager가 모니터링 주기를 완료할 때 에 따라 스토리지 객체가 그룹에 동적으로 추가됩니다.
- 볼륨에 대한 임계값 설정과 같은 그룹의 모든 스토리지 개체에 작업을 동시에 적용할 수 있습니다.

그룹 규칙이 그룹에 대해 작동하는 방식

그룹 규칙은 스토리지 오브젝트(볼륨, 클러스터 또는 SVM)를 특정 그룹에 포함할 수 있도록 정의하는 기준입니다. 조건 그룹 또는 조건을 사용하여 그룹에 대한 그룹 규칙을 정의할 수 있습니다.

- 그룹 규칙을 그룹에 연결해야 합니다.
- 그룹 규칙에 대한 개체 유형을 연결해야 합니다. 그룹 규칙에 대해 하나의 개체 유형만 연결됩니다.
- 스토리지 객체는 각 모니터링 주기 이후 또는 규칙을 생성, 편집 또는 삭제할 때 그룹에서 추가 또는 제거됩니다.
- 그룹 규칙에는 하나 이상의 조건 그룹이 있을 수 있으며 각 조건 그룹에는 하나 이상의 조건이 있을 수 있습니다.
- 스토리지 객체는 생성한 그룹 규칙에 따라 여러 그룹에 속할 수 있습니다.

조건

여러 조건 그룹을 만들 수 있으며 각 조건 그룹에는 하나 이상의 조건이 있을 수 있습니다. 그룹에 포함할 스토리지

객체를 지정하기 위해 그룹의 그룹 규칙에 정의된 모든 조건 그룹을 적용할 수 있습니다.

조건 그룹 내의 조건은 논리 AND를 사용하여 실행됩니다. 조건 그룹의 모든 조건을 충족해야 합니다. 그룹 규칙을 생성하거나 수정할 때 조건 그룹의 모든 조건을 충족하는 스토리지 객체만 적용, 선택 및 그룹화하는 조건이 생성됩니다. 그룹에 포함할 스토리지 오브젝트의 범위를 좁히려는 경우 조건 그룹 내에서 여러 조건을 사용할 수 있습니다.

다음 피연산자와 연산자를 사용하고 필요한 값을 지정하여 저장소 개체로 조건을 만들 수 있습니다.

스토리지 객체 유형입니다	적용 가능한 피연산자
볼륨	• 개체 이름 • 소유 클러스터 이름입니다 • 소유 SVM 이름 • 주석
SVM	• 개체 이름 • 소유 클러스터 이름입니다 • 주석
클러스터	• 개체 이름 • 주석

스토리지 개체의 피연산자로 주석을 선택하면 ""is"" 연산자를 사용할 수 있습니다. 다른 모든 피연산자의 경우 ""is"" 또는 ""Contains""를 연산자로 선택할 수 있습니다.

- 피연산자

  Unified Manager의 피연산자 목록은 선택한 개체 형식을 기반으로 변경됩니다. 이 목록에는 오브젝트 이름, 소유 클러스터 이름, SVM 이름 소유, Unified Manager에 정의한 주석이 포함됩니다.

- 운영자

  연산자 목록은 조건에 대해 선택한 피연산자를 기준으로 변경됩니다. Unified Manager에서 지원되는 운영자는 "is"와 "Contains"입니다.

  ""is"" 연산자를 선택하면 선택한 피연산자에 대해 제공된 값과 피연산자 값의 정확한 일치에 대한 조건이 계산됩니다.

  "포함" 연산자를 선택하면 다음 조건 중 하나를 충족하도록 조건이 평가됩니다.

  ◦ 피연산자 값은 선택한 피연산자에 대해 제공된 값과 정확히 일치합니다

  ◦ 피연산자 값은 선택한 피연산자에 대해 제공된 값을 포함합니다

- 값

  값 필드는 선택한 피연산자에 따라 변경됩니다.

조건이 있는 그룹 규칙의 예

다음 두 가지 조건이 있는 볼륨의 조건 그룹을 고려합니다.

- 이름에 "vol"이 포함되어 있습니다.
- SVM 이름은 "data_svm"입니다.

이 조건 그룹은 이름에 ""vol""이 포함되어 있고 이름이 ""data_svm""인 SVM에서 호스팅되는 모든 볼륨을 선택합니다.

조건 그룹

조건 그룹은 논리 OR를 사용하여 실행된 다음 스토리지 객체에 적용됩니다. 스토리지 객체가 그룹에 포함될 조건 그룹 중 하나를 만족해야 합니다. 모든 조건 그룹의 스토리지 객체가 결합됩니다. 조건 그룹을 사용하여 그룹에 포함할 스토리지 개체의 범위를 늘릴 수 있습니다.

조건 그룹이 있는 그룹 규칙의 예

볼륨별로 다음 두 가지 조건을 포함하는 두 개의 조건 그룹을 고려합니다.

- 조건 그룹 1
  - 이름에 "vol"이 포함되어 있습니다.
  - SVM 이름이 ""data_svm"" 조건 그룹 1은 이름에 "vol"이 포함된 모든 볼륨을 선택하고 SVM에서 "data_svm"이라는 이름으로 호스팅됩니다.
- 조건 그룹 2
  - 이름에 "vol"이 포함되어 있습니다.
  - 데이터 우선 순위의 주석 값은 ""위험"" 조건 그룹 2는 이름에 ""vol""을 포함하고 데이터 우선 순위 주석 값으로 ""위험""으로 주석이 붙은 모든 볼륨을 선택합니다.

이러한 두 조건 그룹이 포함된 그룹 규칙이 스토리지 객체에 적용되는 경우 선택한 그룹에 다음 스토리지 객체가 추가됩니다.

- 이름에 "vol"이 포함되어 있고 "data_svm"이라는 이름의 SVM에서 호스팅되는 모든 볼륨.
- 이름에 ""vol""이 포함되어 있고 데이터 우선 순위 주석 값 ""critical""이 주석으로 표시된 모든 볼륨.

그룹 작업이 스토리지 객체에서 작동하는 방식

그룹 작업은 그룹의 모든 스토리지 객체에 대해 수행되는 작업입니다. 예를 들어, 볼륨 임계값 그룹 작업을 구성하여 그룹에 있는 모든 볼륨의 볼륨 임계값을 동시에 변경할 수 있습니다.

그룹은 고유한 그룹 작업 유형을 지원합니다. 볼륨 상태 임계값 그룹 작업 유형이 하나만 있는 그룹을 가질 수 있습니다. 그러나 같은 그룹에 대해 다른 유형의 그룹 작업을 구성할 수 있습니다(사용 가능한 경우). 그룹 작업의 순위에 따라 스토리지 객체에 작업이 적용되는 순서가 결정됩니다. 스토리지 객체의 세부 정보 페이지는 스토리지 객체에 적용되는 그룹 작업에 대한 정보를 제공합니다.

고유한 그룹 작업의 예

그룹 G1 및 G2에 속하는 볼륨 A를 예로 들어 보겠습니다. 이러한 그룹에 대해 다음과 같은 볼륨 상태 임계값 그룹 작업이 구성됩니다.

- 볼륨 용량 구성을 위한 1순위 그룹 동작인 Change_capacity_threshold
- 볼륨의 Snapshot 복제본을 구성하기 위한 등급 2의 Change_snapshot_copies 그룹 작업입니다

Change_capacity_threshold 그룹 동작은 항상 Change_snapshot_copies 그룹 동작보다 우선하며 볼륨 A에 적용됩니다 Unified Manager가 모니터링 주기를 하나만 완료하면 볼륨 A의 상태 임계값 관련 이벤트가 'Change_capacity_threshold' 그룹 동작에 따라 다시 평가됩니다. G1 또는 G2 그룹에 대해 다른 볼륨 임계값 유형의 그룹 작업을 구성할 수 없습니다.

그룹 추가

클러스터, 볼륨 및 SVM(스토리지 가상 머신)을 결합한 그룹을 생성하여 관리를 용이하게 할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

그룹 규칙을 정의하여 그룹에서 구성원을 추가 또는 제거하고 그룹에 대한 그룹 작업을 수정할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 * 탭에서 * 추가 * 를 클릭합니다.
3. 그룹 추가 * 대화 상자에서 그룹의 이름과 설명을 입력합니다.
4. 추가 * 를 클릭합니다.

그룹 편집

Unified Manager에서 생성한 그룹의 이름과 설명을 편집할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이름을 업데이트하기 위해 그룹을 편집할 때 고유한 이름을 지정해야 합니다. 기존 그룹 이름은 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 * 탭에서 편집할 그룹을 선택한 다음 * 편집 * 을 클릭합니다.
3. 그룹 편집 * 대화 상자에서 그룹의 이름, 설명 또는 둘 다를 변경합니다.
4. 저장 * 을 클릭합니다.

그룹을 삭제하는 중입니다

그룹이 더 이상 필요하지 않은 경우 Unified Manager에서 그룹을 삭제할 수 있습니다.

- 필요한 것 *

- 삭제할 그룹에 연결된 그룹 규칙과 스토리지 오브젝트(클러스터, SVM 또는 볼륨)를 연결할 수 없습니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 * 탭에서 삭제할 그룹을 선택한 다음 * 삭제 * 를 클릭합니다.
3. 경고 * 대화 상자에서 * 예 * 를 클릭하여 삭제를 확인합니다.

   그룹을 삭제해도 그룹과 연결된 그룹 작업은 삭제되지 않습니다. 그러나 그룹이 삭제된 후에는 이러한 그룹 작업이 매핑 해제됩니다.

그룹 규칙 추가

그룹에 대해 그룹 규칙을 생성하여 볼륨, 클러스터 또는 SVM(스토리지 가상 머신)과 같은 스토리지 객체를 그룹에 동적으로 추가할 수 있습니다. 그룹 규칙을 만들려면 하나 이상의 조건을 가진 조건 그룹을 하나 이상 구성해야 합니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

현재 모니터링되는 스토리지 객체는 그룹 규칙이 생성되는 즉시 추가됩니다. 모니터링 주기가 완료된 후에만 새 객체가 추가됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 규칙 * 탭에서 * 추가 * 를 클릭합니다.
3. 그룹 규칙 추가 * 대화 상자에서 그룹 규칙의 이름을 지정합니다.
4. 대상 객체 유형 * 필드에서 그룹화할 스토리지 객체의 유형을 선택합니다.
5. 그룹 * 필드에서 그룹 규칙을 생성할 필수 그룹을 선택합니다.
6. 조건 * 섹션에서 다음 단계를 수행하여 조건, 조건 그룹 또는 둘 모두를 만듭니다.

만들려면	수행할 작업...
조건	a. 피연산자 목록에서 피연산자를 선택합니다. b. Contains * 또는 * is * 를 연산자로 선택합니다. c. 값을 입력하거나 사용 가능한 목록에서 값을 선택합니다.

만들려면	수행할 작업...
조건 그룹	a. 조건 그룹 추가 * 를 클릭합니다 b. 피연산자 목록에서 피연산자를 선택합니다. c. Contains * 또는 * is * 를 연산자로 선택합니다. d. 값을 입력하거나 사용 가능한 목록에서 값을 선택합니다. e. 필요한 경우 * 조건 추가 * 를 클릭하여 조건을 더 만들고 각 조건에 대해 a - d 단계를 반복합니다.

7. 추가 * 를 클릭합니다.

그룹 규칙 생성 예

그룹 규칙 추가 대화 상자에서 다음 단계를 수행하여 조건을 구성하고 조건 그룹을 추가하는 등의 그룹 규칙을 만듭니다.

단계

1. 그룹 규칙의 이름을 지정합니다.
2. 오브젝트 유형을 SVM(스토리지 가상 시스템)으로 선택합니다.
3. 그룹 목록에서 그룹을 선택합니다.
4. 조건 섹션에서 피연산자로 * 개체 이름 * 을 선택합니다.
5. 연산자로 * 포함 * 을 선택합니다.
6. 값을 'VM_DATA'로 입력합니다.
7. 조건 그룹 추가 * 를 클릭합니다.
8. 피연산자로 * 개체 이름 * 을 선택합니다.
9. 연산자로 * 포함 * 을 선택합니다.
10. 값을 'vol'로 입력합니다.
11. 조건 추가 * 를 클릭합니다.
12. 8단계에서 피연산자로 * data-priority * 를 선택하고 9단계의 연산자로 * 를, 10단계의 값으로 * critical * 을 선택하여 8단계에서 10단계까지 반복합니다.
13. 그룹 규칙의 조건을 만들려면 * 추가 * 를 클릭합니다.

그룹 규칙 편집 중

그룹 규칙을 편집하여 조건 그룹 및 조건 그룹 내의 조건을 수정하여 특정 그룹에 스토리지 객체를 추가하거나 제거할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 규칙 * 탭에서 편집할 그룹 규칙을 선택한 다음 * 편집 * 을 클릭합니다.
3. 그룹 규칙 편집 * 대화 상자에서 필요에 따라 그룹 규칙 이름, 관련 그룹 이름, 조건 그룹 및 조건을 변경합니다.

   그룹 규칙의 대상 개체 유형은 변경할 수 없습니다.

4. 저장 * 을 클릭합니다.

그룹 규칙을 삭제하는 중입니다

그룹 규칙이 더 이상 필요하지 않은 경우 Active IQ Unified Manager에서 그룹 규칙을 삭제할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

그룹 규칙이 삭제되면 연결된 스토리지 객체가 그룹에서 제거됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 규칙 * 탭에서 삭제할 그룹 규칙을 선택한 다음 * 삭제 * 를 클릭합니다.
3. 경고 * 대화 상자에서 * 예 * 를 클릭하여 삭제를 확인합니다.

그룹 작업을 추가하는 중입니다

그룹의 스토리지 객체에 적용할 그룹 작업을 구성할 수 있습니다. 그룹에 대한 작업을 구성하면 각 개체에 이러한 작업을 개별적으로 추가할 필요가 없으므로 시간을 절약할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 작업 * 탭에서 * 추가 * 를 클릭합니다.
3. 그룹 작업 추가 * 대화 상자에서 작업의 이름과 설명을 입력합니다.
4. Group * (그룹 *) 메뉴에서 작업을 구성할 그룹을 선택합니다.
5. Action Type * (작업 유형 *) 메뉴에서 작업 유형을 선택합니다.

   대화 상자가 확장되어 필요한 매개 변수를 사용하여 선택한 작업 유형을 구성할 수 있습니다.

6. 필요한 매개 변수에 적절한 값을 입력하여 그룹 작업을 구성합니다.
7. 추가 * 를 클릭합니다.

그룹 작업 편집

그룹 작업 이름, 설명, 관련 그룹 이름, 작업 유형의 매개 변수 등 Unified Manager에서 구성한 그룹 작업 매개 변수를 편집할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 작업 * 탭에서 편집할 그룹 작업을 선택한 다음 * 편집 * 을 클릭합니다.
3. 그룹 작업 편집 * 대화 상자에서 필요에 따라 그룹 작업 이름, 설명, 관련 그룹 이름 및 작업 유형의 매개 변수를 변경합니다.
4. 저장 * 을 클릭합니다.

그룹에 대한 볼륨 상태 임계값을 구성합니다

용량, 스냅샷 복사본, qtree 할당량, 증가 및 inode에 대한 그룹 레벨 볼륨 상태 임계값을 구성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

그룹 작업의 볼륨 상태 임계값 유형은 그룹의 볼륨에만 적용됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 작업 * 탭에서 * 추가 * 를 클릭합니다.
3. 그룹 작업의 이름과 설명을 입력합니다.
4. 그룹 * 드롭다운 상자에서 그룹 작업을 구성할 그룹을 선택합니다.
5. 볼륨 상태 임계값으로 * Action Type * 을 선택합니다.
6. 임계값을 설정할 범주를 선택합니다.
7. 상태 임계값에 필요한 값을 입력합니다.
8. 추가 * 를 클릭합니다.

그룹 작업을 삭제하는 중입니다

그룹 작업이 더 이상 필요하지 않은 경우 Unified Manager에서 그룹 작업을 삭제할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

볼륨 상태 임계값에 대한 그룹 작업을 삭제하면 글로벌 임계값이 해당 그룹의 스토리지 개체에 적용됩니다. 스토리지 개체에 설정된 개체 수준 상태 임계값은 영향을 받지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. 그룹 작업 * 탭에서 삭제할 그룹 작업을 선택한 다음 * 삭제 * 를 클릭합니다.
3. 경고 * 대화 상자에서 * 예 * 를 클릭하여 삭제를 확인합니다.

그룹 작업 순서 바꾸기

그룹의 스토리지 객체에 적용할 그룹 작업의 순서를 변경할 수 있습니다. 그룹 작업은 순위를 기준으로 스토리지 객체에 순차적으로 적용됩니다. 가장 낮은 순위는 마지막으로 구성한 그룹 동작에 할당됩니다. 요구 사항에 따라 그룹 작업의 순위를 변경할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단일 행 또는 여러 행을 선택한 다음 여러 끌어서 놓기 작업을 수행하여 그룹 작업의 순위를 변경할 수 있습니다. 그러나 다시 우선 순위를 적용하려면 그룹 작업 그리드에 변경 사항을 저장해야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 그룹 * 을 클릭합니다.
2. Group Actions * 탭에서 * Reorder * 를 클릭합니다.
3. 그룹 작업 다시 정렬 * 대화 상자에서 행을 끌어 놓아 그룹 작업의 순서를 필요에 따라 다시 정렬합니다.
4. 저장 * 을 클릭합니다.

주석을 사용하여 스토리지 오브젝트 이벤트 우선 순위 지정

주석 규칙을 생성하고 스토리지 객체에 적용하여 적용된 주석 유형과 우선 순위에 따라 해당 객체를 식별하고 필터링할 수 있습니다.

주석에 대한 자세한 이해

주석에 대한 개념을 이해하면 환경의 스토리지 오브젝트와 관련된 이벤트를 관리하는 데 도움이 됩니다.

주석 정의

주석은 다른 텍스트 문자열(값)에 할당된 텍스트 문자열(이름)입니다. 각 주석 이름 값 쌍은 주석 규칙을 사용하여 스토리지 오브젝트와 동적으로 연결될 수 있습니다. 스토리지 객체를 사전 정의된 주석과 연결할 때 해당 객체와 관련된 이벤트를 필터링하고 볼 수 있습니다. 클러스터, 볼륨 및 SVM(스토리지 가상 머신)에 주석을 적용할 수 있습니다.

각 주석 이름에는 여러 값이 있을 수 있으며 각 이름-값 쌍은 규칙을 통해 스토리지 개체와 연결될 수 있습니다.

예를 들어 "보스턴"과 "캐나다"라는 값으로 "데이터 센터"라는 주석을 만들 수 있습니다. 그런 다음 볼륨 v1에 "Boston" 값을 가진 "data-center" 주석을 적용할 수 있습니다. 볼륨 v1에서 "데이터 센터"라는 주석이 붙은 이벤트에 대해 경고가 생성되면 생성된 e-메일은 볼륨 위치 "보스턴"을 나타내며, 이를 통해 문제의 우선 순위를 지정하고 해결할 수 있습니다.

Unified Manager에서 주석 규칙이 작동하는 방식

주석 규칙은 스토리지 오브젝트(볼륨, 클러스터 또는 SVM(스토리지 가상 머신)에 주석을 다는 것을 정의하는 기준입니다. 조건 그룹 또는 조건을 사용하여 주석 규칙을 정의할 수 있습니다.

- 주석 규칙을 주석에 연결해야 합니다.
- 주석 규칙에 개체 유형을 연결해야 합니다. 주석 규칙에 대해 하나의 개체 유형만 연결할 수 있습니다.
- Unified Manager는 각 모니터링 주기가 끝난 후 또는 규칙이 생성, 편집, 삭제 또는 재정렬될 때 스토리지 개체에서 주석을 추가하거나 제거합니다.
- 주석 규칙에는 하나 이상의 조건 그룹이 있을 수 있으며 각 조건 그룹에는 하나 이상의 조건이 있을 수 있습니다.
- 스토리지 객체에는 여러 주석이 있을 수 있습니다. 특정 주석에 대한 주석 규칙은 규칙 조건에서 다른 주석을 사용하여 이미 주석이 추가된 개체에 다른 주석을 추가할 수도 있습니다.

조건

여러 조건 그룹을 만들 수 있으며 각 조건 그룹에는 하나 이상의 조건이 있을 수 있습니다. 스토리지 객체에 주석을 달려면 주석의 주석 규칙에 정의된 조건 그룹을 모두 적용할 수 있습니다.

조건 그룹 내의 조건은 논리 AND를 사용하여 실행됩니다. 조건 그룹의 모든 조건을 충족해야 합니다. 주석 규칙을 생성하거나 수정할 때 조건 그룹의 모든 조건을 충족하는 스토리지 객체만 적용, 선택 및 주석을 달 수 있는 조건이 생성됩니다. 주석을 추가할 스토리지 오브젝트의 범위를 좁히려는 경우 조건 그룹 내에서 여러 조건을 사용할 수 있습니다.

다음 피연산자와 연산자를 사용하고 필요한 값을 지정하여 저장소 개체로 조건을 만들 수 있습니다.

스토리지 객체 유형입니다	적용 가능한 피연산자
볼륨	• 개체 이름 • 소유 클러스터 이름입니다 • 소유 SVM 이름 • 주석
SVM	• 개체 이름 • 소유 클러스터 이름입니다 • 주석
클러스터	• 개체 이름 • 주석

스토리지 개체의 피연산자로 주석을 선택하면 ""is"" 연산자를 사용할 수 있습니다. 다른 모든 피연산자의 경우 ""is"" 또는 ""Contains""를 연산자로 선택할 수 있습니다. ""is"" 연산자를 선택하면 선택한 피연산자에 대해 제공된 값을

사용하여 피연산자 값과 정확히 일치하는 조건이 평가됩니다. "포함" 연산자를 선택하면 다음 조건 중 하나를 충족하도록 조건이 평가됩니다.

- 피연산자 값은 선택한 피연산자의 값과 정확히 일치합니다.
- 피연산자 값은 선택한 피연산자에 대해 제공된 값을 포함합니다.

조건이 있는 주석 규칙의 예

다음 두 가지 조건이 있는 볼륨에 대해 하나의 조건 그룹이 있는 주석 규칙을 고려합니다.

- 이름에 "vol"이 포함되어 있습니다.
- SVM 이름은 "data_svm"입니다.

이 주석 규칙은 이름에 ""vol""이 포함되어 있고 선택한 주석 및 주석 유형이 "data_svm"인 SVM에서 호스팅되는 모든 볼륨에 주석을 추가합니다.

조건 그룹

조건 그룹은 논리 OR를 사용하여 실행된 다음 스토리지 객체에 적용됩니다. 스토리지 객체는 주석을 추가할 조건 그룹 중 하나의 요구 사항을 충족해야 합니다. 모든 조건 그룹의 조건을 충족하는 스토리지 객체에는 주석이 추가됩니다. 조건 그룹을 사용하여 주석을 추가할 스토리지 오브젝트의 범위를 늘릴 수 있습니다.

조건 그룹이 있는 주석 규칙의 예

볼륨에 대해 두 개의 조건 그룹이 있는 주석 규칙을 고려합니다. 각 그룹에는 다음 두 가지 조건이 포함됩니다.

- 조건 그룹 1
  - 이름에 "vol"이 포함되어 있습니다.
  - SVM 이름은 ""data_svm"입니다. 이 조건 그룹은 이름에 ""vol""이 포함되어 있고 SVM에서 ""data_svm""이라는 이름으로 호스팅되는 모든 볼륨에 주석을 답니다.
- 조건 그룹 2
  - 이름에 "vol"이 포함되어 있습니다.
  - 데이터 우선 순위의 주석 값은 ""위험""입니다. 이 조건 그룹은 이름에 ""vol""을 포함하고 데이터 우선 순위 주석 값으로 ""위험""으로 주석 표시된 모든 볼륨에 주석을 답니다.

이러한 두 조건 그룹이 포함된 주석 규칙이 스토리지 객체에 적용되면 다음 스토리지 객체에 주석이 추가됩니다.

- 이름에 "vol"이 포함되어 있고 이름이 "data_svm"인 SVM에서 호스팅되는 모든 볼륨.
- 이름에 ""vol""이 포함되어 있고 데이터 우선 순위 주석 값이 ""critical""로 표시된 모든 볼륨.

사전 정의된 주석 값에 대한 설명입니다

- Data-priority * 는 미션 크리티컬, 높음, 낮음이라는 값을 가진 미리 정의된 주석입니다. 이러한 값을 사용하여 스토리지 객체에 포함된 데이터의 우선 순위에 따라 스토리지 객체에 주석을 달 수 있습니다. 미리 정의된 주석 값은 편집하거나 삭제할 수 없습니다.
- * 데이터 우선 순위: 미션 크리티컬 *

  이 주석은 미션 크리티컬 데이터가 포함된 스토리지 객체에 적용됩니다. 예를 들어, 운영 애플리케이션이 포함된

객체는 미션 크리티컬 객체로 간주될 수 있습니다.

- * 데이터 우선 순위: 높음 *

  이 주석은 우선 순위가 높은 데이터를 포함하는 스토리지 객체에 적용됩니다. 예를 들어, 비즈니스 애플리케이션을 호스팅하는 개체는 높은 우선 순위로 간주될 수 있습니다.

- * 데이터 우선 순위: 낮음 *

  이 주석은 낮은 우선 순위 데이터를 포함하는 스토리지 객체에 적용됩니다. 예를 들어, 백업 및 미러 대상과 같은 보조 스토리지에 있는 개체의 우선 순위가 낮을 수 있습니다.

동적으로 주석 추가

맞춤형 주석을 생성할 때 Unified Manager는 규칙에 따라 클러스터, SVM(스토리지 가상 머신), 볼륨을 주석과 동적으로 연결합니다. 이 규칙은 스토리지 객체에 주석을 자동으로 할당합니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 * 페이지에서 * 주석 추가 * 를 클릭합니다.
3. 주석 추가 * 대화 상자에서 주석에 대한 이름과 설명을 입력합니다.
4. 옵션: * 주석 값 * 섹션에서 * 추가 * 를 클릭하여 주석에 값을 추가합니다.
5. 저장 * 을 클릭합니다.

주석에 값 추가

주석에 값을 추가한 다음 저장 개체를 특정 주석 이름-값 쌍과 연결할 수 있습니다. 주석에 값을 추가하면 스토리지 객체를 보다 효과적으로 관리할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

미리 정의된 주석에는 값을 추가할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 * 페이지에서 값을 추가할 주석을 선택한 다음 * 값 * 섹션에서 * 추가 * 를 클릭합니다.
3. 주석 값 추가 * 대화 상자에서 주석 값을 지정합니다.

   지정한 값은 선택한 주석에 대해 고유해야 합니다.

4. 추가 * 를 클릭합니다.

주석 삭제

사용자 정의 주석 및 그 값이 더 이상 필요하지 않은 경우 삭제할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 주석 값은 다른 주석 또는 그룹 규칙에서 사용해서는 안 됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. Annotations * (주석 *) 탭에서 삭제할 주석을 선택합니다.

   선택한 주석의 세부 정보가 표시됩니다.

3. Actions * > * Delete * 를 클릭하여 선택한 주석과 해당 값을 삭제합니다.
4. 경고 대화 상자에서 * 예 * 를 클릭하여 삭제를 확인합니다.

주석 목록 및 세부 정보 보기

클러스터, 볼륨 및 SVM(스토리지 가상 머신)과 동적으로 연결되는 주석 목록을 볼 수 있습니다. 설명, 만든 사용자, 만든 날짜, 값, 규칙 등의 세부 정보를 볼 수도 있습니다. 및 주석과 연관된 개체.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. Annotations * (주석 *) 탭에서 주석 이름을 클릭하여 관련 세부 정보를 봅니다.

주석에서 값 삭제

해당 값이 주석에 더 이상 적용되지 않는 경우 사용자 정의 주석과 연관된 값을 삭제할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 주석 값은 주석 규칙 또는 그룹 규칙과 연관되지 않아야 합니다.

미리 정의된 주석에서는 값을 삭제할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 * 탭의 주석 목록에서 값을 삭제할 주석을 선택합니다.
3. 주석 * 탭의 * 값 * 영역에서 삭제할 값을 선택한 다음 * 삭제 * 를 클릭합니다.
4. 경고 * 대화 상자에서 * 예 * 를 클릭합니다.

   값이 삭제되고 선택한 주석의 값 목록에 더 이상 표시되지 않습니다.

주석 규칙 작성

Unified Manager에서 볼륨, 클러스터 또는 SVM(스토리지 가상 머신)과 같은 스토리지 객체를 동적으로 주석으로 달기 위해 사용하는 주석 규칙을 생성할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

현재 모니터링되는 스토리지 개체는 주석 규칙이 생성되는 즉시 주석으로 추가됩니다. 모니터링 주기가 완료된 후에만 새 객체에 주석이 추가됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 규칙 * 탭에서 * 추가 * 를 클릭합니다.
3. 주석 규칙 추가 * 대화 상자에서 주석 규칙 이름을 지정합니다.
4. Target Object Type * 필드에서 주석을 달 스토리지 객체 유형을 선택합니다.
5. Apply Annotation(주석 적용) * 필드에서 사용할 주석 및 주석 값을 선택합니다.
6. 조건 섹션에서 적절한 작업을 수행하여 조건, 조건 그룹 또는 둘 모두를 만듭니다.

생성 방법...	수행할 작업...
조건	a. 피연산자 목록에서 피연산자를 선택합니다. b. Contains * 또는 * is * 를 연산자로 선택합니다. c. 값을 입력하거나 사용 가능한 목록에서 값을 선택합니다.
조건 그룹	a. 조건 그룹 추가 * 를 클릭합니다. b. 피연산자 목록에서 피연산자를 선택합니다. c. Contains * 또는 * is * 를 연산자로 선택합니다. d. 값을 입력하거나 사용 가능한 목록에서 값을 선택합니다. e. 필요한 경우 * 조건 추가 * 를 클릭하여 조건을 더 만들고 각 조건에 대해 a - d 단계를 반복합니다.

7. 추가 * 를 클릭합니다.

주석 규칙 작성 예제

Add Annotation Rule(주석 규칙 추가) 대화 상자에서 다음 단계를 수행하여 조건 구성 및 조건 그룹 추가를 비롯한 주석 규칙을 생성합니다.

단계

1. 주석 규칙 이름을 지정합니다.

2. 대상 오브젝트 유형을 SVM(스토리지 가상 머신)으로 선택합니다.
3. 주석 목록에서 주석을 선택하고 값을 지정합니다.
4. 조건 섹션에서 피연산자로 * 개체 이름 * 을 선택합니다.
5. 연산자로 * 포함 * 을 선택합니다.
6. 값을 'VM_DATA'로 입력합니다.
7. 조건 그룹 추가 * 를 클릭합니다.
8. 피연산자로 * 개체 이름 * 을 선택합니다.
9. 연산자로 * 포함 * 을 선택합니다.
10. 값을 'vol'로 입력합니다.
11. 조건 추가 * 를 클릭합니다.
12. 8단계에서 피연산자로 * data-priority * 를 선택하고 9단계의 연산자로 * 를, 10단계의 값으로 * mission-critical * 을 선택하여 8단계에서 10단계까지 반복합니다.
13. 추가 * 를 클릭합니다.

개별 스토리지 객체에 수동으로 주석 추가

주석 규칙을 사용하지 않고 선택한 볼륨, 클러스터, SVM에 수동으로 주석을 달 수 있습니다. 단일 스토리지 오브젝트 또는 여러 스토리지 오브젝트에 주석을 추가하고 주석에 필요한 이름-값 쌍 조합을 지정할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 주석을 추가할 스토리지 객체로 이동합니다.

주석을 추가하려면...	수행할 작업...
클러스터	a. 스토리지 * > * 클러스터 * 를 클릭합니다. b. 하나 이상의 클러스터를 선택합니다.
볼륨	a. 스토리지 * > * 볼륨 * 을 클릭합니다. b. 하나 이상의 볼륨을 선택합니다.
SVM	a. 스토리지 * > * SVM * 을 클릭합니다. b. 하나 이상의 SVM을 선택합니다.

2. Annotate * (주석 달기 *)를 클릭하고 이름 값 쌍을 선택합니다.
3. 적용 * 을 클릭합니다.

주석 규칙 편집

주석 규칙을 편집하여 조건 그룹 내의 조건 그룹 및 조건을 수정하여 스토리지 개체에 주석을 추가하거나 스토리지 개체에서 주석을 제거할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

관련 주석 규칙을 편집할 때 주석이 스토리지 오브젝트에서 해제됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 규칙 * 탭에서 편집할 주석 규칙을 선택한 다음 * 작업 * > * 편집 * 을 클릭합니다.
3. Edit Annotation Rule * (주석 규칙 편집 *) 대화 상자에서 필요에 따라 규칙 이름, 주석 이름 및 값, 조건 그룹 및 조건을 변경합니다.

   주석 규칙의 대상 개체 유형은 변경할 수 없습니다.

4. 저장 * 을 클릭합니다.

주석 규칙 조건 구성

하나 이상의 조건을 구성하여 Unified Manager가 스토리지 개체에 적용하는 주석 규칙을 생성할 수 있습니다. 주석 규칙을 충족하는 스토리지 객체에는 규칙에 지정된 값으로 주석이 추가됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 규칙 * 탭에서 * 추가 * 를 클릭합니다.
3. 주석 규칙 추가 * 대화 상자에서 규칙 이름을 입력합니다.
4. 대상 개체 유형 목록에서 개체 유형을 하나 선택한 다음 목록에서 주석 이름과 값을 선택합니다.
5. 대화 상자의 * 조건 * 섹션에서 목록에서 피연산자와 연산자를 선택하고 조건 값을 입력하거나 * 조건 추가 * 를 클릭하여 새 조건을 만듭니다.
6. 저장 및 추가 * 를 클릭합니다.

주석 규칙 조건 구성의 예

개체 이름에 "svm_data"가 포함된 SVM 객체 유형의 조건을 고려하십시오.

주석 규칙 추가 대화 상자에서 다음 단계를 수행하여 조건을 구성합니다.

단계

1. 주석 규칙 이름을 입력합니다.

2. 대상 오브젝트 유형을 SVM으로 선택합니다.
3. 주석 목록에서 주석 및 값을 선택합니다.
4. 조건 * 필드에서 피연산자로 * 개체 이름 * 을 선택합니다.
5. 연산자로 * 포함 * 을 선택합니다.
6. 값을 'VM_DATA'로 입력합니다.
7. 추가 * 를 클릭합니다.

주석 규칙 삭제

규칙이 더 이상 필요하지 않은 경우 Active IQ Unified Manager에서 주석 규칙을 삭제할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

주석 규칙을 삭제하면 주석이 스토리지 오브젝트에서 분리되고 제거됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 규칙 * 탭에서 삭제할 주석 규칙을 선택한 다음 * 삭제 * 를 클릭합니다.
3. 경고 * 대화 상자에서 * 예 * 를 클릭하여 삭제를 확인합니다.

주석 규칙 순서 바꾸기

Unified Manager가 스토리지 개체에 주석 규칙을 적용하는 순서를 변경할 수 있습니다. 주석 규칙은 스토리지 객체의 순위에 따라 순차적으로 적용됩니다. 주석 규칙을 구성할 때 순위는 가장 낮습니다. 하지만 요구 사항에 따라 주석 규칙의 순위를 변경할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단일 행 또는 여러 행을 선택하고 여러 끌어서 놓기 작업을 수행하여 주석 규칙의 순위를 변경할 수 있습니다. 그러나 다시 우선 순위를 지정할 수 있도록 변경 사항을 저장해야 주석 규칙 탭에 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 관리 * > * 주석 * 을 클릭합니다.
2. 주석 규칙 * 탭에서 * 재정렬 * 을 클릭합니다.
3. 주석 규칙 순서 바꾸기 * 대화 상자에서 단일 행 또는 여러 행을 끌어서 주석 규칙 순서를 다시 정렬합니다.
4. 저장 * 을 클릭합니다.

   재정렬을 표시하려면 변경 사항을 저장해야 합니다.

웹 **UI** 및 유지 관리 콘솔을 통해 지원 번들 보내기

AutoSupport 메시지가 제공하는 것보다 더 자세한 진단 및 문제 해결이 필요한 문제의 경우 지원 번들을 보내야 합니다. Unified Manager 웹 UI 및 유지보수 콘솔을 사용하여 기술 지원 팀에 지원 번들을 보낼 수 있습니다.

Unified Manager에는 최대 2개의 완벽한 지원 번들과 3개의 경량 지원 번들이 한번에 저장됩니다.

- 관련 정보 *

"Unified Manager 사용자 역할 및 기능"

기술 지원 팀에 **AutoSupport** 메시지 및 지원 번들 보내기

AutoSupport 페이지에서는 사전 정의된 요청 시 AutoSupport 메시지를 기술 지원 팀에 전송하여 운영 환경을 올바르게 운영하고 환경의 무결성을 유지할 수 있도록 지원합니다. AutoSupport는 기본적으로 활성화되어 있으며NetApp Active IQ의 이점을 누릴 수 있도록 비활성화되어서는 안 됩니다.

Unified Manager 서버에 대한 진단 시스템 정보 및 세부 데이터를 필요한 경우 메시지로 보내거나, 주기적으로 메시지를 보내거나, 기술 지원 팀에 지원 번들을 생성하고 보낼 수 있습니다.

> 스토리지 관리자 역할을 가진 사용자는 주문형 AutoSupport 메시지 및 지원 번들을 생성하여 기술 지원으로 보낼 수 있습니다. 그러나 관리자 또는 유지 관리 사용자만 주기적인 AutoSupport를 활성화 또는 비활성화하고 HTTP 프록시 서버 설정 섹션에 설명된 대로 HTTP 설정을 구성할 수 있습니다. HTTP 프록시 서버를 사용해야 하는 환경에서는 스토리지 관리자가 주문형 AutoSupport 메시지 및 지원 번들을 기술 지원에 보내기 전에 구성을 완료해야 합니다.

주문형 **AutoSupport** 메시지 보내기

주문형 메시지를 생성하여 기술 지원 부서 또는 지정된 이메일 수신자 또는 두 사람에게 보낼 수 있습니다.

단계

1. 일반 * > * AutoSupport * 로 이동하여 다음 작업 중 하나 또는 모두를 수행합니다.
2. 기술 지원 부서에 AutoSupport 메시지를 보내려면 * 기술 지원 부서로 전송 * 확인란을 선택합니다.
3. 특정 이메일 수신자에게 AutoSupport 메시지를 보내려면 * 이메일 수신자에게 전송 * 확인란을 선택하고 수신자의 이메일 주소를 입력합니다.
4. 저장 * 을 클릭합니다.
5. AutoSupport 생성 및 전송 * 을 클릭합니다.

Periodic AutoSupport 활성화

정기적으로 문제 진단 및 해결을 위해 기술 지원 부서에 사전 정의된 특정 메시지를 보낼 수 있습니다. 이 기능은 기본적으로 활성화되어 있습니다. 비활성화된 경우 관리자 또는 유지 관리 사용자가 설정을 활성화할 수 있습니다.

단계

1. 일반 * > * AutoSupport * 로 이동합니다.

2. Periodic AutoSupport(주기적 데이터) 섹션에서 AutoSupport*에 주기적으로 Active IQ 데이터 전송 사용 확인란을 선택합니다.
3. 필요한 경우 HTTP 프록시 서버 설정 섹션에 설명된 대로 HTTP 프록시 서버의 이름, 포트 및 인증 정보를 정의합니다.
4. 저장 * 을 클릭합니다.

주문형 지원 번들 업로드

문제 해결 요구사항에 따라 지원 번들을 생성하고 기술 지원 팀에 보낼 수 있습니다. Unified Manager에서는 가장 최근에 생성된 2개의 지원 번들만 저장합니다. 이전 지원 번들은 시스템에서 삭제됩니다.

일부 지원 데이터 유형에서는 많은 양의 클러스터 리소스를 사용하거나 완료하는 데 시간이 오래 걸릴 수 있으므로 전체 지원 번들을 선택할 때 특정 데이터 유형을 포함하거나 제외하여 지원 번들 크기를 줄일 수 있습니다. 또한 30일 동안의 로그 및 구성 데이터베이스 레코드를 포함하는 경량 지원 번들을 생성할 수 있습니다. 성능 데이터, 획득 기록 파일 및 서버 힙 덤프는 제외됩니다.

단계

1. 일반 * > * AutoSupport * 로 이동합니다.
2. 주문형 지원 번들 섹션에서 * 지원 번들 생성 및 전송 * 을 클릭합니다.
3. 기술 지원 부서에 가벼운 지원 번들을 보내려면 지원 번들 생성 및 전송 팝업에서 가벼운 지원 번들 생성 확인란을 선택합니다.
4. 또는 전체 지원 번들을 보내려면 * 전체 지원 번들 생성 * 확인란을 선택합니다. 지원 번들에 포함하거나 제외할 특정 데이터 유형을 선택합니다.

   데이터 유형을 선택하지 않더라도 지원 번들은 다른 Unified Manager 데이터와 함께 생성됩니다.

5. 번들을 생성하여 기술 지원 부서에 보내려면 * 기술 지원 부서에 번들 보내기 * 확인란을 선택합니다. 이 확인란을 선택하지 않으면 번들은 Unified Manager 서버에 로컬로 생성되고 저장됩니다. 생성된 지원 번들은 나중에 VMware 시스템의 /support 디렉토리, Linux 시스템의 경우 '/opt/netapp/data/support/', Windows 시스템의 경우 'ProgramData\NetApp\OnCommandAppData\ocum\support'에서 사용할 수 있습니다.
6. 보내기 * 를 클릭합니다.

HTTP 프록시 서버 설정 중

사용자 환경에서 Unified Manager 서버로부터 직접 액세스할 수 없는 경우 AutoSupport 콘텐츠를 지원하도록 인터넷 액세스를 제공하는 프록시를 지정할 수 있습니다. 이 섹션은 관리자 및 유지 보수 사용자만 사용할 수 있습니다.

- * HTTP 프록시 사용 *

  HTTP 프록시로 사용 중인 서버를 식별하려면 이 확인란을 선택합니다.

  프록시 서버의 호스트 이름 또는 IP 주소와 서버 연결에 사용되는 포트 번호를 입력합니다.

- * 인증 사용 *

  HTTP 프록시로 사용 중인 서버에 액세스하기 위한 인증 정보를 제공해야 하는 경우 이 확인란을 선택합니다.

  HTTP 프록시로 인증하는 데 필요한 사용자 이름과 암호를 입력합니다.

기본 인증만 제공하는 HTTP 프록시는 지원되지 않습니다.

유지보수 콘솔 액세스

Unified Manager 사용자 인터페이스가 작동 중이 아니거나 사용자 인터페이스에서 사용할 수 없는 기능을 수행해야 하는 경우, 유지보수 콘솔에 액세스하여 Unified Manager 시스템을 관리할 수 있습니다.

- 필요한 것 *

Unified Manager를 설치하고 구성해야 합니다.

15분 동안 비활성 상태가 지속되면 유지보수 콘솔에서 로그아웃합니다.

VMware에 설치된 경우 VMware 콘솔을 통해 유지 관리 사용자로 이미 로그인한 경우에는 Secure Shell을 사용하여 동시에 로그인할 수 없습니다.

단계

1. 다음 단계에 따라 유지보수 콘솔에 액세스합니다.

이 운영 체제에서...	다음 단계를 따르십시오...
VMware	a. Secure Shell을 사용하여 Unified Manager 가상 어플라이언스의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. b. 유지보수 사용자 이름과 암호를 사용하여 유지보수 콘솔에 로그인합니다.
리눅스	a. Secure Shell을 사용하여 Unified Manager 시스템의 IP 주소 또는 정규화된 도메인 이름에 연결합니다. b. 유지보수 사용자(umadmin) 이름 및 암호를 사용하여 시스템에 로그인합니다. c. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.
Windows	a. 관리자 자격 증명을 사용하여 Unified Manager 시스템에 로그인합니다. b. Windows 관리자로 PowerShell을 실행합니다. c. mainf유지보수_console 명령을 입력하고 Enter 키를 누릅니다.

Unified Manager 유지보수 콘솔 메뉴가 표시됩니다.

문제 해결 지원을 위해 기술 지원 부서에 보낼 수 있도록 진단 정보가 포함된 지원 번들을 생성할 수 있습니다.

Unified Manager 9.8부터 Unified Manager 서버가 인터넷에 연결되어 있는 경우, 유지보수 콘솔에서 지원 번들을 NetApp에 업로드할 수도 있습니다.

- 필요한 것 *

유지보수 사용자로서 유지보수 콘솔에 액세스할 수 있어야 합니다.

일부 유형의 지원 데이터는 많은 양의 클러스터 리소스를 사용하거나 완료하는 데 시간이 오래 걸릴 수 있으므로, 전체 지원 번들을 선택할 때 포함 또는 제외할 데이터 유형을 지정하여 지원 번들 크기를 줄일 수 있습니다. 또한 30일 동안의 로그 및 구성 데이터베이스 레코드를 포함하는 경량 지원 번들을 생성할 수 있습니다. 성능 데이터, 획득 기록 파일 및 서버 힙 덤프는 제외됩니다.

Unified Manager에서는 가장 최근에 생성된 2개의 지원 번들만 저장합니다. 이전 지원 번들은 시스템에서 삭제됩니다.

단계

1. 유지보수 콘솔 * 주 메뉴 * 에서 * 지원/진단 * 을 선택합니다.
2. 지원 번들에서 원하는 세부 정보 수준에 따라 * Generate Light Support Bundle * 또는 * Generate Support Bundle * 을 선택합니다.
3. 전체 지원 번들을 선택하는 경우 지원 번들에 포함하거나 제외할 다음 데이터 유형을 선택하거나 선택 취소합니다.
   - * 데이터베이스 덤프 *

     MySQL Server 데이터베이스의 덤프.
   - * 힙 덤프 *

     기본 Unified Manager 서버 프로세스 상태의 스냅샷 이 옵션은 기본적으로 비활성화되어 있으며 고객 지원 부서에서 요청할 때만 선택해야 합니다.
   - * 촬영 녹화 *

     Unified Manager와 모니터링되는 클러스터 간의 모든 통신 내용을 기록하는 것입니다.

   모든 데이터 유형의 선택을 취소하면 지원 번들이 다른 Unified Manager 데이터와 함께 계속 생성됩니다.
4. 'g'를 입력한 다음 Enter 키를 눌러 지원 번들을 생성합니다.

   지원 번들 생성은 메모리를 많이 사용하는 작업이므로 지원 번들을 생성할지 확인하는 메시지가 표시됩니다.
5. 'y'를 입력한 다음 Enter 키를 눌러 지원 번들을 생성합니다.

   현재 지원 번들을 생성하지 않으려면 "n"을 입력한 다음 Enter 키를 누릅니다.
6. 전체 지원 번들에 데이터베이스 덤프 파일을 포함하는 경우 성능 통계를 포함할 기간을 지정하라는 메시지가 표시됩니다. 성능 통계를 포함시키면 많은 시간과 공간이 소요되므로 성능 통계를 포함하지 않고 데이터베이스를

덤프할 수도 있습니다.

a. YYYYMMDD 형식으로 시작 날짜를 입력합니다.

   예를 들어, 2021년 1월 1일에 20210101을 입력합니다. 성능 통계를 포함하지 않으려면 n을 입력합니다.

b. 오전 12시부터 통계 일수를 입력합니다 지정된 시작 날짜에.

   1부터 10까지의 숫자를 입력할 수 있습니다.

성능 통계를 포함하는 경우 성능 통계를 수집하는 기간이 표시됩니다.

7. 지원 번들이 생성되면 NetApp에 업로드할 것인지 묻는 메시지가 표시됩니다. y를 입력한 다음 Enter 키를 누릅니다.

   지원 케이스 번호를 입력하라는 메시지가 표시됩니다.

8. 케이스 번호가 이미 있는 경우 번호를 입력하고 Enter 키를 누릅니다. 그렇지 않으면 Enter 키를 누릅니다.

   지원 번들은 NetApp에 업로드됩니다.

Unified Manager 서버가 인터넷에 연결되어 있지 않거나 다른 이유로 지원 번들을 업로드할 수 없는 경우 검색할 수 있으며 수동으로 전송할 수 있습니다. SFTP 클라이언트를 사용하거나 UNIX 또는 Linux CLI 명령을 사용하여 검색할 수 있습니다. Windows 설치에서 RDP(원격 데스크톱)를 사용하여 지원 번들을 검색할 수 있습니다.

생성된 지원 번들은 VMware 시스템의 /support 디렉토리, Linux 시스템의 /opt/netapp/data/support/및 Windows 시스템의 ProgramData\NetApp\OnCommandAppData\ocum\support에 있습니다.

- 관련 정보 *

"Unified Manager 사용자 역할 및 기능"

Windows 클라이언트를 사용하여 지원 번들 검색

Windows 사용자인 경우, 툴을 다운로드하여 설치하면 Unified Manager 서버에서 지원 번들을 검색할 수 있습니다. 문제에 대한 보다 자세한 진단을 위해 기술 지원 부서에 지원 번들을 보낼 수 있습니다. FileZilla 또는 WinSCP는 사용할 수 있는 도구의 예입니다.

- 필요한 것 *

이 작업을 수행하려면 유지 관리 사용자여야 합니다.

SCP 또는 SFTP를 지원하는 도구를 사용해야 합니다.

단계

1. 지원 번들을 검색하기 위한 도구를 다운로드하고 설치합니다.
2. 도구를 엽니다.
3. SFTP를 통해 Unified Manager 관리 서버에 연결합니다.

   이 도구는 /support 디렉토리의 내용을 표시하며 기존의 모든 지원 번들을 볼 수 있습니다.

4. 복사할 지원 번들의 대상 디렉토리를 선택합니다.
5. 복사할 지원 번들을 선택하고 이 툴을 사용하여 Unified Manager 서버에서 로컬 시스템으로 파일을 복사합니다.

UNIX 또는 **Linux** 클라이언트를 사용하여 지원 번들 검색

UNIX 또는 Linux 사용자인 경우 Linux 클라이언트 서버에서 CLI(Command-Line Interface)를 사용하여 vApp에서 지원 번들을 검색할 수 있습니다. SCP 또는 SFTP를 사용하여 지원 번들을 검색할 수 있습니다.

- 필요한 것 *

이 작업을 수행하려면 유지 관리 사용자여야 합니다.

유지보수 콘솔을 사용하여 지원 번들을 생성하고 지원 번들 이름을 사용할 수 있어야 합니다.

단계

1. Linux 클라이언트 서버를 사용하여 텔넷 또는 콘솔을 통해 CLI에 액세스합니다.
2. /support' 디렉토리에 액세스합니다.
3. 다음 명령을 사용하여 지원 번들을 검색하고 로컬 디렉토리에 복사합니다.

사용 중인 경우...	그런 다음 다음 다음 명령을 사용합니다.
SCP를 선택합니다	'sp<maintenance-user>@<vapp-name-or-ip>:/support/support_bundle_file_name.7z<destination-directory>'
SFTP	'sftp<maintenance-user>@<vapp-name-or-ip>:/support/support_bundle_file_name.7z<destination-directory>'

   지원 번들은 유지보수 콘솔을 사용하여 생성할 때 제공됩니다.

4. 유지보수 사용자 암호를 입력합니다.

예

다음 예에서는 SCP를 사용하여 지원 번들을 검색합니다.

```
        `$ scp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
support_bundle_20160216_145359.7z   100%  119MB  11.9MB/s   00:10
```

다음 예에서는 SFTP를 사용하여 지원 번들을 검색합니다.

```
        `$ sftp
admin@10.10.12.69:/support/support_bundle_20160216_145359.7z .`
Password: `<maintenance_user_password>`
Connected to 10.228.212.69.
Fetching /support/support_bundle_20130216_145359.7z to
./support_bundle_20130216_145359.7z
/support/support_bundle_20160216_145359.7z
```

기술 지원 팀에 지원 번들 보내기

AutoSupport 메시지에서 제공하는 것보다 문제에 더 자세한 진단 및 문제 해결 정보가 필요한 경우 기술 지원 팀에 지원 번들을 보낼 수 있습니다.

- 필요한 것 *

기술 지원 팀에 지원 번들을 보내려면 지원 번들에 액세스할 수 있어야 합니다.

기술 지원 웹 사이트를 통해 생성된 케이스 번호가 있어야 합니다.

단계

1. NetApp Support 사이트에 로그인합니다.
2. 파일을 업로드합니다.

   "NetApp에 파일을 업로드하는 방법"

여러 워크플로와 관련된 작업 및 정보

Unified Manager에서 워크플로우에 대한 참고 사항을 추가 및 검토, 이벤트 할당, 이벤트 확인 및 해결, 볼륨, SVM(스토리지 가상 시스템), 애그리게이트, 애그리게이트 세부 정보 등을 포함하여 일부 작업과 참조 텍스트를 확인하여 워크플로우를 완료하는 데 도움이 되는 참조 텍스트도 있습니다. 등.

클러스터 구성 요소 및 구성 요소의 경합이 발생할 수 있는 이유

클러스터 구성 요소의 경합이 발생할 때 클러스터 성능 문제를 식별할 수 있습니다. 구성 요소를 사용하는 워크로드의 성능이 느려지고 클라이언트 요청에 대한 응답 시간(지연 시간)이 증가하여 Unified Manager에서 이벤트가 트리거됩니다.

경합이 발생한 구성 요소는 최적 수준에서 수행할 수 없습니다. 성능이 저하되었으며, _ 피해자라고 하는 다른 클러스터 구성 요소와 워크로드의 성능이 지연 시간을 증가했을 수 있습니다. 구성 요소의 경합을 줄이려면 작업 부하를 줄이거나 작업 처리 능력을 높여 성능이 정상 수준으로 돌아가도록 해야 합니다. Unified Manager는 5분 간격으로 워크로드 성능을 수집 및 분석하므로, 클러스터 구성 요소가 지속적으로 초과 사용되는 경우에만 감지합니다. 5분 간격 동안 짧은 시간 동안만 지속되는 일시적인 과사용량 급증은 감지되지 않습니다.

예를 들어, 스토리지 aggregate에서 발생하는 경합이 발생할 수 있습니다. 그 이유는 하나 이상의 워크로드가 I/O 요청을 이행하기 위해 경합하기 때문입니다. Aggregate의 다른 워크로드에 영향을 줄 수 있으므로 성능이 저하될 수

있습니다. 애그리게이트에서 수행하는 작업의 양을 줄이기 위해 하나 이상의 워크로드를 사용량이 적은 애그리게이트 또는 노드로 이동하여 현재 애그리게이트의 전체 워크로드 요구사항을 줄이는 것과 같은 다양한 단계를 수행할 수 있습니다. QoS 정책 그룹의 경우 처리량 제한을 조정하거나 워크로드를 다른 정책 그룹으로 이동하여 워크로드가 더 이상 제한되지 않도록 할 수 있습니다.

Unified Manager에서 다음 클러스터 구성 요소를 모니터링하여 경합 상태를 경고합니다.

- 네트워크 *

  클러스터의 외부 네트워킹 프로토콜에 의한 I/O 요청 대기 시간을 나타냅니다. 대기 시간은 클러스터가 입출력 요청에 응답하기 전에 ""전송 준비"" 트랜잭션이 완료될 때까지 기다리는 데 걸리는 시간입니다. 네트워크 구성 요소의 경합이 발생한 경우, 프로토콜 계층에서 대기 시간이 길면 하나 이상의 워크로드 지연 시간에 영향을 미치게 됩니다.

- * 네트워크 처리 *

  프로토콜 계층과 클러스터 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 이벤트가 감지된 이후 네트워크 처리를 처리하는 노드가 변경되었을 수 있습니다. 네트워크 처리 구성 요소의 경합이 발생한 경우, 네트워크 처리 노드의 높은 사용률이 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

  액티브-액티브 구성에서 모든 SAN 어레이 클러스터를 사용할 경우 두 노드에 대해 네트워크 처리 지연 시간 값이 표시되므로 노드가 로드를 균등하게 공유하고 있는지 확인할 수 있습니다.

- * QoS 제한 최대 *

  워크로드에 할당된 스토리지 QoS(Quality of Service) 정책 그룹의 최대 처리량(최대) 설정을 나타냅니다. 정책 그룹 구성 요소의 경합이 발생한 경우 정책 그룹의 모든 워크로드가 설정된 처리량 제한에 따라 조절되고, 이로 인해 하나 이상의 워크로드 지연 시간이 영향을 받습니다.

- * QoS 제한 최소 *

  다른 워크로드에 할당된 QoS 처리량 최소(예상) 설정으로 인해 워크로드의 지연 시간을 나타냅니다. 특정 워크로드에 설정된 QoS 최소값이 대부분의 대역폭을 사용하여 보장된 처리량을 보장하는 경우, 다른 워크로드의 임계치가 조절되고 더 많은 지연 시간이 표시됩니다.

- 클러스터 인터커넥트 *

  클러스터된 노드가 물리적으로 연결된 케이블과 어댑터를 나타냅니다. 클러스터 인터커넥트 구성 요소의 경합이 발생한 경우, 클러스터 인터커넥트에서 I/O 요청이 있을 때까지 대기 시간이 길어 하나 이상의 워크로드 지연 시간에 영향을 미치게 됩니다.

- * 데이터 처리 *

  는 클러스터와 워크로드를 포함하는 스토리지 애그리게이트 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 이벤트가 감지된 이후 데이터 처리를 처리하는 노드가 변경될 수 있습니다. 데이터 처리 구성 요소의 경합이 발생한 경우, 데이터 처리 노드의 높은 활용률이 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

- * 볼륨 활성화 *

  모든 활성 볼륨의 사용량을 추적하는 프로세스를 나타냅니다. 1,000개 이상의 볼륨이 활성 상태인 대규모 환경에서는 이 프로세스에서 노드를 통해 동시에 리소스에 액세스해야 하는 중요 볼륨의 수를 추적합니다. 동시 활성 볼륨 수가 권장되는 최대 임계값을 초과하면 중요하지 않은 볼륨 중 일부에서 여기에 나와 있는 지연 시간이 발생합니다.

- * MetroCluster 리소스 *

  MetroCluster 구성에서 클러스터 간 데이터를 미러링하는 데 사용되는 NVRAM 및 ISL(Interswitch Link)을 비롯한 MetroCluster 리소스를 나타냅니다. MetroCluster 구성 요소의 경합이 발생한 경우, 로컬 클러스터의 워크로드로부터 높은 쓰기 처리량을 의미하거나 링크 상태 문제가 로컬 클러스터에 있는 하나 이상의 워크로드 지연 시간에 영향을 줍니다. 클러스터가 MetroCluster 구성에 없으면 이 아이콘이 표시되지 않습니다.

- * 애그리게이트 또는 SSD 애그리게이트 운영 *

  워크로드가 실행되는 스토리지 애그리게이트를 나타냅니다. 애그리게이트 구성 요소의 경합이 발생할 경우, 애그리게이트의 활용률이 높아지면 하나 이상의 워크로드 지연 시간에 영향을 미치게 됩니다. Aggregate는 모든 HDD 또는 HDD와 SSD(Flash Pool 애그리게이트)의 혼합 또는 HDD와 클라우드 계층(FabricPool 애그리게이트)의 혼합 요소로 이루어집니다. 'SSD Aggregate'는 모든 SSD(All-Flash 애그리게이트) 또는 SSD와 클라우드 계층(FabricPool 애그리게이트)의 혼합으로 구성됩니다.

- * 클라우드 지연 시간 *

  클러스터 및 사용자 데이터가 저장되는 클라우드 계층 간의 I/O 처리와 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 클라우드 지연 시간 구성 요소의 경합이 발생할 경우, 클라우드 계층에서 호스팅되는 볼륨의 대량 읽기가 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

- SnapMirror * 를 동기화합니다

  SnapMirror Synchronous 관계의 기본 볼륨에서 보조 볼륨으로 사용자 데이터를 복제하는 것과 관련된 클러스터의 소프트웨어 구성요소를 나타냅니다. 동기식 SnapMirror 구성 요소의 경합이 발생한 경우, SnapMirror Synchronous 작업의 활동이 하나 이상의 워크로드 지연 시간에 영향을 미치고 있음을 의미합니다.

볼륨/상태 세부 정보 페이지

볼륨/상태 세부 정보 페이지를 사용하여 용량, 스토리지 효율성, 구성, 보호 등과 같은 선택한 볼륨에 대한 자세한 정보를 볼 수 있습니다. 주석 및 이벤트가 생성됩니다. 또한 해당 볼륨에 대한 관련 개체 및 관련 경고에 대한 정보를 볼 수 있습니다.

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

명령 버튼

명령 단추를 사용하여 선택한 볼륨에 대해 다음 작업을 수행할 수 있습니다.

- * 성능 보기로 전환 *

  볼륨/성능 세부 정보 페이지로 이동할 수 있습니다.

- * 조치 *

  - 경고 추가

    선택한 볼륨에 경고를 추가할 수 있습니다.

  - 임계값 편집

    선택한 볼륨의 임계값 설정을 수정할 수 있습니다.

◦ 주석 달기

선택한 볼륨에 주석을 달 수 있습니다.

◦ 보호

선택한 볼륨에 대해 SnapMirror 또는 SnapVault 관계를 생성할 수 있습니다.

◦ 관계

다음과 같은 보호 관계 작업을 실행할 수 있습니다.

- 편집

  기존 보호 관계에 대한 기존 SnapMirror 정책, 일정 및 최대 전송 속도를 변경할 수 있는 관계 편집 대화 상자를 시작합니다.

- 중단

  선택한 관계에 대해 진행 중인 전송을 중단합니다. 필요에 따라 기본 전송 이외의 전송을 위해 재시작 체크포인트를 제거할 수 있습니다. 기본 전송에 대한 체크포인트를 제거할 수 없습니다.

- 정지

  선택한 관계에 대해 예약된 업데이트를 일시적으로 비활성화합니다. 관계가 중지되기 전에 이미 진행 중인 전송을 완료해야 합니다.

- 휴식

  소스 볼륨과 타겟 볼륨 간의 관계를 끊은 후 대상을 읽기-쓰기 볼륨으로 변경합니다.

- 제거

  선택한 소스와 대상 간의 관계를 영구적으로 삭제합니다. 볼륨은 제거되지 않고 볼륨의 스냅샷 복사본은 제거되지 않습니다. 이 작업은 실행 취소할 수 없습니다.

- 다시 시작

  중지된 관계에 대해 예약된 전송을 활성화합니다. 다음 예약된 전송 간격에서 재시작 체크포인트가 있는 경우 해당 체크포인트가 사용됩니다.

- 재동기화

  이전에 끊어진 관계를 다시 동기화할 수 있습니다.

- 초기화/업데이트

  새 보호 관계에 대해 최초 베이스라인 전송을 수행하거나 관계가 이미 초기화된 경우 수동 업데이트를 수행할 수 있습니다.

- 재동기화

  는 소스를 원래 대상의 복사본으로 만들어 소스 및 대상의 기능을 반전하여 이전에 파손된 보호 관계를 다시

설정할 수 있도록 합니다. 소스의 콘텐츠는 대상의 컨텐츠로 덮어쓰여지고, 공통 스냅샷 복사본의 데이터보다 최신 데이터는 삭제됩니다.

◦ 복원

한 볼륨에서 다른 볼륨으로 데이터를 복원할 수 있습니다. 자세한 내용은 을 참조하십시오 "볼륨/상태 세부 정보 페이지를 사용하여 데이터를 복원합니다".

복원 단추와 관계 작업 단추는 동기 보호 관계에 있는 볼륨에는 사용할 수 없습니다.

- * 볼륨 보기 *

  Health:All Volumes 보기로 이동할 수 있습니다.

용량 탭

용량 탭에는 물리적 용량, 논리적 용량, 임계값 설정, 할당량 용량, 볼륨 이동 작업에 대한 정보 등 선택한 볼륨에 대한 세부 정보가 표시됩니다.

- * 물리적 용량 *

  에서는 볼륨의 물리적 용량을 자세히 설명합니다.

  ◦ 스냅샷 오버플로

  스냅샷 복사본에서 사용하는 데이터 공간을 표시합니다.

  ◦ 사용됨

  볼륨의 데이터에 사용된 공간을 표시합니다.

  ◦ 경고

  볼륨의 공간이 거의 꽉 찼음을 나타냅니다. 이 임계값이 위반되면 Space 거의 가득 참 이벤트가 생성됩니다.

  ◦ 오류

  볼륨의 공간이 가득 찼음을 나타냅니다. 이 임계값이 위반되면 Space Full 이벤트가 생성됩니다.

  ◦ 사용할 수 없습니다

  위험 시 씬 프로비저닝된 볼륨 공간 이벤트가 생성되고 씬 프로비저닝된 볼륨의 공간이 애그리게이트 용량 문제로 인해 위험에 처함을 나타냅니다. 사용할 수 없는 용량은 씬 프로비저닝된 볼륨에 대해서만 표시됩니다.

  ◦ 데이터 그래프

  볼륨의 총 데이터 용량과 사용된 데이터 용량을 표시합니다.

  자동 확장 이 설정된 경우 데이터 그래프에는 aggregate에서 사용 가능한 공간이 표시됩니다. 데이터 그래프에는 볼륨의 데이터에 사용할 수 있는 유효 스토리지 공간이 표시되며 다음 중 하나일 수 있습니다.

    ▪ 다음 조건에서 볼륨의 실제 데이터 용량입니다.

        - 자동 확장 이 비활성화되어 있습니다.
        - 자동 확장 지원 볼륨이 최대 크기에 도달했습니다.
        - 자동 확장 지원 프로비저닝된 볼륨은 더 이상 확장할 수 없습니다.
      - 최대 볼륨 크기를 고려한 후의 볼륨 데이터 용량(씬 프로비저닝된 볼륨 및 애그리게이트에 볼륨을 최대 크기에 도달할 수 있는 공간이 있는 경우)
      - 가능한 다음 자동 확장 크기를 고려한 후의 볼륨 데이터 용량(자동 확장 백분율 임계값이 있는 걸쭉한 프로비저닝 볼륨의 경우)
    - Snapshot 복사본 그래프

      이 그래프는 사용된 스냅샷 용량 또는 스냅샷 예약 공간이 0이 아닌 경우에만 표시됩니다.

  두 그래프에는 사용된 스냅샷 용량이 스냅샷 예약 용량을 초과하는 경우 스냅샷 용량이 스냅샷 예약 용량을 초과하는 용량이 표시됩니다.

- * 용량 논리 *

  볼륨의 논리적 공간 특성을 표시합니다. 논리적 공간은 ONTAP 스토리지 효율성 기술을 사용할 때의 절감 효과를 적용하지 않고 디스크에 저장 중인 데이터의 실제 크기를 나타냅니다.

    - 논리적 공간 보고

      볼륨에 논리적 공간 보고가 구성되어 있는지 여부를 표시합니다. 이 값은 Enabled, Disabled 또는 Not Applicable 중 선택할 수 있습니다. 이전 버전의 ONTAP 또는 논리적 공간 보고를 지원하지 않는 볼륨에 대해서는 "'해당 없음'"이 표시됩니다.

    - 사용됨

      볼륨의 데이터에서 사용 중인 논리적 공간의 양과 총 데이터 용량에 따라 사용된 논리적 공간의 비율을 표시합니다.

    - 논리적 공간 적용

      씬 프로비저닝된 볼륨에 대해 논리적 공간 적용이 구성되었는지 여부를 표시합니다. Enabled(활성화)로 설정하면 볼륨의 논리적 사용 크기가 현재 설정된 물리적 볼륨 크기보다 클 수 없습니다.

- * Autogrow *

  공간이 부족할 때 볼륨이 자동으로 증가하는지 여부를 표시합니다.

- * 공간 보장 *

  볼륨이 Aggregate에서 사용 가능한 블록을 제거할 때 FlexVol 볼륨 설정 컨트롤을 표시합니다. 그런 다음 이러한 블록을 볼륨의 파일에 쓸 수 있습니다. 공간 보장은 다음 중 하나로 설정할 수 있습니다.

    - 없음

      볼륨에 대해 공간 보장이 구성되지 않았습니다.

    - 파일

전체 크기의 적게 쓴 파일(예: LUN)이 보장됩니다.

◦ 볼륨

볼륨의 전체 크기가 보장됩니다.

◦ 부분

FlexCache 볼륨은 크기에 따라 공간을 예약합니다. FlexCache 볼륨의 크기가 100MB 이상인 경우 최소 공간 보장은 기본적으로 100MB로 설정됩니다. FlexCache 볼륨의 크기가 100MB 미만인 경우 최소 공간 보장이 FlexCache 볼륨의 크기로 설정됩니다. FlexCache 볼륨의 크기를 나중에 확장할 경우 최소 공간 보장이 증가하지 않습니다.

볼륨이 Data-Cache 유형인 경우 공간 보장이 Partial입니다.

- * 세부 정보(물리적) *

  볼륨의 물리적 특성을 표시합니다.

- * 총 용량 *

  볼륨의 총 물리적 용량을 표시합니다.

- * 데이터 용량 *

  볼륨에 사용된 물리적 공간(사용된 용량)과 볼륨에서 여전히 사용 가능한 물리적 공간(사용 가능한 용량)을 표시합니다. 이러한 값은 총 물리적 용량의 백분율로도 표시됩니다.

  씬 프로비저닝된 볼륨 공간 위험 이벤트가 씬 프로비저닝된 볼륨에 대해 생성된 경우, 볼륨에서 사용하는 공간(사용된 용량)과 볼륨에서 사용 가능하지만 사용할 수 없는 공간(사용할 수 없는 용량)이 집계 용량 문제로 인해 표시됩니다.

- * 스냅숏 예비 공간 *

  스냅샷 복사본(사용된 용량)에서 사용하는 공간 및 볼륨의 스냅샷 복사본(여유 용량)에 사용 가능한 공간이 표시됩니다. 이러한 값은 전체 스냅숏 예비 공간의 비율로도 표시됩니다.

  씬 프로비저닝된 볼륨 공간 위험 이벤트가 씬 프로비저닝된 볼륨에 대해 생성되는 경우, 스냅샷 복사본에서 사용하는 공간(사용된 용량) 및 볼륨에서 사용 가능한 공간 중 스냅샷 복사본을 만드는 데 사용할 수 없지만 사용할 수 없는 용량(사용할 수 없는 용량)입니다. 집계 용량 문제가 표시되므로

- * 볼륨 임계값 *

  다음 볼륨 용량 임계값을 표시합니다.

  ◦ 거의 꽉 참 임계값

  볼륨이 거의 꽉 찬 비율을 지정합니다.

  ◦ 전체 임계값

  볼륨이 꽉 찬 비율을 지정합니다.

- * 기타 세부 정보 *
  - 최대 크기 자동 확장

    볼륨이 자동으로 커질 수 있는 최대 크기를 표시합니다. 기본값은 생성 시 볼륨 크기의 120%입니다. 이 필드는 볼륨에 대해 자동 확장 이 활성화된 경우에만 표시됩니다.

  - Qtree 할당량 커밋 용량

    할당량에 예약된 공간을 표시합니다.

  - Qtree 할당량 초과 커밋 용량

    시스템에서 볼륨 Qtree 할당량 초과 커밋 이벤트를 생성하기 전에 사용할 수 있는 공간의 양을 표시합니다.

  - 분할 예약

    덮어쓰기 예약의 크기를 제어합니다. 기본적으로 부분 예약은 100으로 설정되어 있으며, 이는 필요한 예약 공간의 100%가 예약되므로 오브젝트를 덮어쓰기용으로 완전히 보호할 수 있음을 나타냅니다. 부분 예약이 100% 미만인 경우 해당 볼륨의 모든 공간 예약 파일에 대한 예약 공간이 분할 예약 비율로 줄어듭니다.

  - 스냅샷 일일 증가율

    선택한 볼륨의 스냅샷 복사본에서 24시간마다 발생하는 변경 사항(백분율 또는 KB, MB, GB 등)을 표시합니다.

  - 스냅샷 일수를 전체 로 설정합니다

    볼륨의 스냅샷 복사본에 예약된 공간이 지정된 임계값에 도달하기 전에 남은 예상 일 수를 표시합니다.

    Snapshot days to Full 필드는 볼륨의 스냅샷 복사본의 성장률이 0 또는 음수이거나 증가율을 계산할 데이터가 충분하지 않은 경우 해당 값이 표시되지 않습니다.

  - 스냅샷 자동 삭제

    Aggregate의 공간 부족으로 인해 볼륨에 쓸 수 없을 때 공간을 확보하기 위해 스냅샷 복사본을 자동으로 삭제할지 여부를 지정합니다.

  - Snapshot 복사본

    볼륨의 스냅샷 복사본에 대한 정보를 표시합니다.

    볼륨에 있는 스냅샷 복사본의 수가 링크로 표시됩니다. 이 링크를 클릭하면 볼륨 대화 상자에서 스냅샷 복사본이 열립니다. 이 대화 상자에는 스냅샷 복사본에 대한 세부 정보가 표시됩니다.

  스냅샷 복사본 수는 약 1시간마다 업데이트되지만 아이콘을 클릭하면 스냅샷 복사본 목록이 업데이트됩니다. 이로 인해 토폴로지에 표시된 스냅샷 복사본 수와 아이콘을 클릭할 때 나열되는 스냅샷 복사본 수가 다를 수 있습니다.

- * 볼륨 이동 *

  현재 또는 볼륨에서 수행된 마지막 볼륨 이동 작업의 상태와 진행 중인 볼륨 이동 작업의 현재 단계, 소스 애그리게이트, 대상 애그리게이트, 시작 시간, 종료 시간 등의 기타 세부 정보가 표시됩니다. 예상 종료 시간입니다.

  또한 선택한 볼륨에서 수행된 볼륨 이동 작업의 수도 표시됩니다. 볼륨 이동 내역 * 링크를 클릭하여 볼륨 이동

작업에 대한 자세한 정보를 볼 수 있습니다.

Configuration(구성) 탭

Configuration 탭에는 볼륨의 내보내기 정책, RAID 유형, 용량 및 스토리지 효율성 관련 기능과 같이 선택한 볼륨에 대한 세부 정보가 표시됩니다.

- * 개요 *
  - 전체 이름

    볼륨의 전체 이름을 표시합니다.

  - 애그리게이트

    볼륨이 상주하는 애그리게이트의 이름 또는 FlexGroup 볼륨이 상주하는 애그리게이트 수가 표시됩니다.

  - 계층화 정책

    볼륨이 FabricPool 지원 애그리게이트에 구축된 경우 볼륨에 대한 계층화 정책 세트를 표시합니다. 정책은 없음, 스냅샷 전용, 백업, 자동 또는 모두일 수 있습니다.

  - 스토리지 VM

    볼륨이 포함된 SVM의 이름을 표시합니다.

  - 접합 경로

    활성 또는 비활성일 수 있는 경로의 상태를 표시합니다. 볼륨이 마운트된 SVM의 경로도 표시됩니다. History * 링크를 클릭하면 교차점 경로에 대한 최근 5개의 변경 사항을 볼 수 있습니다.

  - 엑스포트 정책

    볼륨에 대해 생성된 엑스포트 정책의 이름을 표시합니다. 링크를 클릭하면 SVM에 속한 볼륨에서 엑스포트 정책, 인증 프로토콜 및 액세스 가능한 볼륨에 대한 세부 정보를 볼 수 있습니다.

  - 스타일

    볼륨 스타일을 표시합니다. 볼륨 스타일은 FlexVol 또는 FlexGroup가 될 수 있습니다.

  - 유형

    선택한 볼륨의 유형을 표시합니다. 볼륨 유형은 읽기/쓰기, 로드 공유, 데이터 보호, 데이터 캐시 또는 임시 유형이 될 수 있습니다.

  - RAID 유형

    선택한 볼륨의 RAID 유형을 표시합니다. RAID 유형은 RAID0, RAID4, RAID-DP 또는 RAID-TEC가 될 수 있습니다.

    FlexGroup 볼륨의 구성 볼륨은 유형이 다른 애그리게이트에 있을 수 있으므로 FlexGroups에 여러 RAID 유형이 표시될 수 있습니다.

- SnapLock 유형

  볼륨이 포함된 애그리게이트의 SnapLock Type이 표시됩니다.

- SnapLock 만료

  SnapLock 볼륨의 만료 날짜를 표시합니다.

- * 용량 *
  - 씬 프로비저닝

    볼륨에 대한 씬 프로비저닝이 구성되었는지 여부를 표시합니다.

  - 자동 확장

    유연한 볼륨이 애그리게이트 내에서 자동으로 증가하는지 여부를 표시합니다.

  - 스냅샷 자동 삭제

    Aggregate의 공간 부족으로 인해 볼륨에 쓸 수 없을 때 공간을 확보하기 위해 스냅샷 복사본을 자동으로 삭제할지 여부를 지정합니다.

  - 할당량

    볼륨에 대해 할당량을 설정할지 여부를 지정합니다.

- * 효율성 *
  - 압축

    압축을 사용할지 여부를 지정합니다.

  - 중복 제거

    중복 제거 설정 여부를 지정합니다.

  - 중복제거 모드

    볼륨에 대해 활성화된 중복 제거 작업이 수동, 예약 또는 정책 기반 작업인지 여부를 지정합니다. 모드가 예약됨으로 설정되어 있으면 작업 일정이 표시되고, 모드가 정책으로 설정되어 있으면 정책 이름이 표시됩니다.

  - 중복 제거 유형

    볼륨에서 실행 중인 중복 제거 작업의 유형을 지정합니다. 볼륨이 SnapVault 관계인 경우 표시되는 유형은 SnapVault입니다. 다른 볼륨에 대해서는 유형이 보통 으로 표시됩니다.

  - 스토리지 효율성 정책

    Unified Manager를 통해 이 볼륨에 할당된 스토리지 효율성 정책의 이름을 지정합니다. 이 정책은 압축 및 중복제거 설정을 제어할 수 있습니다.

- * 보호 *

◦ Snapshot 복사본

자동 스냅샷 복사본의 설정 여부를 지정합니다.

보호 탭

보호 탭에는 지연 정보, 관계 유형, 관계의 토폴로지 등 선택한 볼륨에 대한 보호 세부 정보가 표시됩니다.

- * 요약 *

  선택한 볼륨의 보호 관계(SnapMirror, SnapVault 또는 스토리지 VM DR) 속성을 표시합니다. 다른 관계 유형의 경우 관계 유형 속성만 표시됩니다. 운영 볼륨을 선택하면 관리형 및 로컬 스냅샷 복사본 정책만 표시됩니다. SnapMirror 및 SnapVault 관계에 대해 표시되는 속성은 다음과 같습니다.

  ◦ 소스 볼륨

  선택한 볼륨이 대상일 경우 선택한 볼륨의 소스 이름을 표시합니다.

  ◦ 지연 상태

  보호 관계에 대한 업데이트 또는 전송 지연 상태를 표시합니다. 상태는 오류, 경고 또는 위험 일 수 있습니다.

  지연 상태는 동기식 관계에는 적용되지 않습니다.

  ◦ 지연 기간

  미러의 데이터가 소스 뒤에 걸리는 시간을 표시합니다.

  ◦ 마지막으로 성공한 업데이트

  최근에 성공한 보호 업데이트의 날짜와 시간을 표시합니다.

  마지막으로 성공한 업데이트는 동기 관계에 적용되지 않습니다.

  ◦ 스토리지 서비스 구성원

  볼륨이 스토리지 서비스에 속해 있고 스토리지 서비스에 의해 관리되는지 여부를 나타내는 예 또는 아니요를 표시합니다.

  ◦ 버전에 상관없이 유연하게 복제

  백업 옵션과 함께 예, 예 또는 없음을 표시합니다. 예 - 소스 볼륨과 타겟 볼륨에서 서로 다른 버전의 ONTAP 소프트웨어를 실행 중인 경우에도 SnapMirror 복제가 가능합니다. 예. 백업 옵션을 사용하면 대상에 여러 버전의 백업 복사본을 유지할 수 있는 기능으로 SnapMirror 보호를 구현할 수 있습니다. None 버전에 상관없이 유연한 복제가 사용되지 않음을 나타냅니다.

  ◦ 관계 기능

  보호 관계에 사용할 수 있는 ONTAP 기능을 나타냅니다.

  ◦ 보호 서비스

  보호 파트너 애플리케이션에서 관계를 관리하는 경우 보호 서비스의 이름을 표시합니다.

◦ 관계 유형

비동기 미러, 비동기 볼트, 비동기 MirrorVault, StrictSync, 및 동기화 를 누릅니다.

◦ 관계 상태

SnapMirror 또는 SnapVault 관계의 상태를 표시합니다. 상태는 Uninitialized, SnapMired 또는 Broken-Off 일 수 있습니다. 소스 볼륨을 선택하면 관계 상태가 적용되지 않고 표시되지 않습니다.

◦ 전송 상태

보호 관계에 대한 전송 상태를 표시합니다. 전송 상태는 다음 중 하나일 수 있습니다.

- 중단 중

  SnapMirror 전송이 사용하도록 설정되어 있지만 체크포인트 제거가 포함된 전송 중단 작업이 진행 중입니다.

- 확인 중입니다

  대상 볼륨에 진단 검사가 진행 중이며 전송이 진행 중입니다.

- 마무리 중입니다

  SnapMirror 전송이 사용하도록 설정되었습니다. 이 볼륨은 현재 증분 SnapVault 전송을 위한 전송 후 단계에 있습니다.

- 유휴

  전송이 활성화되고 진행 중인 전송이 없습니다.

- In-Sync(동기화 중)

  동기 관계에 있는 두 볼륨의 데이터가 동기화됩니다.

- 동기화 중단

  대상 볼륨의 데이터가 소스 볼륨과 동기화되지 않습니다.

- 준비 중

  SnapMirror 전송이 사용하도록 설정되었습니다. 볼륨은 현재 증분 SnapVault 전송을 위한 전송 전 단계에 있습니다.

- 대기열에 있습니다

  SnapMirror 전송이 사용하도록 설정되었습니다. 진행 중인 전송이 없습니다.

- 정지되었습니다

  SnapMirror 전송이 비활성화되었습니다. 진행 중인 전송이 없습니다.

- 정지 중

SnapMirror 전송이 진행 중입니다. 추가 전송이 비활성화됩니다.

- 전송 중입니다

  SnapMirror 전송이 설정되고 전송 중입니다.

- 전환 중

  소스에서 대상 볼륨으로 데이터를 비동기적으로 전송하는 작업이 완료되고 동기식 작업으로 전환이 시작되었습니다.

- 대기 중

  SnapMirror 전송이 시작되었지만 연결된 일부 작업이 대기 중입니다.

◦ 최대 전송 속도

관계의 최대 전송 속도를 표시합니다. 최대 전송 속도는 초당 킬로바이트(Kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps) 또는 초당 테라바이트(Tbps)로 숫자 값이 될 수 있습니다. No Limit(제한 없음)가 표시되면 관계 간 기준선 전송이 무제한입니다.

◦ SnapMirror 정책

볼륨에 대한 보호 정책을 표시합니다. DPDefault 는 기본 비동기 미러 보호 정책을 나타내고, XDPDefault 는 기본 비동기 볼트 정책을 나타내고, DPSyncDefault 는 기본 비동기 MirrorVault 정책을 나타냅니다. StrictSync는 기본 Synchronous Strict 보호 정책을 나타내고, Sync는 기본 Synchronous 정책을 나타냅니다. 정책 이름을 클릭하면 다음 정보를 포함하여 해당 정책과 관련된 세부 정보를 볼 수 있습니다.

- 전송 우선 순위
- 액세스 시간 설정을 무시합니다
- 시도 횟수 제한
- 설명
- SnapMirror 레이블
- 보존 설정
- 실제 스냅샷 복사본
- 스냅샷 복사본 보존
- 보존 경고 임계값입니다
- 소스가 데이터 보호(DP) 볼륨인 계단식 SnapVault 관계에서 보존 설정이 없는 스냅샷 복사본은 "'s_created' 규칙만 적용됩니다.

◦ 업데이트 일정

관계에 할당된 SnapMirror 일정을 표시합니다. 정보 아이콘 위에 커서를 놓으면 일정 세부 정보가 표시됩니다.

◦ 로컬 스냅샷 정책

볼륨에 대한 스냅샷 복사본 정책을 표시합니다. 정책은 기본값, 없음 또는 사용자 지정 정책에 지정된 모든 이름입니다.

◦ 에 의해 보호됩니다

선택한 볼륨에 사용된 보호 유형을 표시합니다. 예를 들어, 볼륨이 정합성 보장 그룹 및 SnapMirror 볼륨 관계에 의해 보호되는 경우 이 필드에 SnapMirror와 정합성 보장 그룹이 모두 표시됩니다. 이 필드에는 통합 관계 상태를 볼 수 있도록 관계 페이지로 리디렉션하는 링크도 제공됩니다. 링크는 구성 관계에만 적용됩니다.

◦ 정합성 보장 그룹

SM-BC(SnapMirror Business Continuity) 관계에 의해 보호되는 볼륨의 경우 이 열에는 볼륨의 일관성 그룹이 표시됩니다.

- 뷰 *

선택한 볼륨의 보호 토폴로지를 표시합니다. 토폴로지에는 선택한 볼륨과 관련된 모든 볼륨의 그래픽 표현이 포함됩니다. 선택한 볼륨은 짙은 회색 테두리로 표시되며 토폴로지의 볼륨 간 선은 보호 관계 유형을 나타냅니다. 토폴로지에서 관계의 방향은 왼쪽부터 오른쪽, 왼쪽에는 각 관계의 소스와 오른쪽에는 대상이 표시됩니다.

이중 굵은 선 비동기 미러 관계를 지정하고, 하나의 굵은 선으로 비동기 볼트 관계를 지정하고, 두 개의 단일 선으로 비동기 MirrorVault 관계를 지정하고, 굵은 선과 굵은 선이 동기 관계를 지정합니다. 아래 표는 동기 관계가 StrictSync 또는 동기화인지 여부를 나타냅니다.

볼륨을 마우스 오른쪽 버튼으로 클릭하면 볼륨을 보호할지 또는 볼륨에 데이터를 복원할지 선택할 수 있는 메뉴가 표시됩니다. 관계를 마우스 오른쪽 단추로 클릭하면 편집, 중단, 중지, 중단, 제거 중 하나를 선택할 수 있는 메뉴가 표시됩니다. 또는 관계를 다시 시작합니다.

다음과 같은 경우에는 메뉴가 표시되지 않습니다.

◦ RBAC 설정에 따라 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우

◦ 볼륨이 동기식 보호 관계에 있는 경우

◦ 예를 들어, 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우) 토폴로지에서 다른 볼륨을 클릭하면 해당 볼륨에 대한 정보가 선택되고 표시됩니다. 물음표( ) 볼륨의 왼쪽 위 모서리에 있는 는 볼륨이 없거나 아직 검색되지 않았음을 나타냅니다. 용량 정보가 누락된 것으로 표시될 수도 있습니다. 물음표 위에 커서를 놓으면 교정 조치를 위한 제안 사항을 비롯한 추가 정보가 표시됩니다.

토폴로지에는 몇 가지 일반적인 토폴로지 템플릿 중 하나를 준수하는 경우 볼륨 용량, 지연 시간, 스냅샷 복사본 및 마지막으로 성공한 데이터 전송에 대한 정보가 표시됩니다. 토폴로지가 이러한 템플릿 중 하나를 준수하지 않을 경우 볼륨 지연 및 마지막으로 성공한 데이터 전송에 대한 정보가 토폴로지 아래의 관계 테이블에 표시됩니다. 이 경우 표에서 강조 표시된 행은 선택한 볼륨을 나타내고 토폴로지 뷰에서 파란색 점이 있는 굵은 선은 선택한 볼륨과 해당 소스 볼륨 간의 관계를 나타냅니다.

토폴로지 뷰에는 다음 정보가 포함됩니다.

- 용량

볼륨에 사용된 총 용량을 표시합니다. 토폴로지의 볼륨 위에 커서를 놓으면 현재 임계값 설정 대화 상자에 해당 볼륨에 대한 현재 경고 및 중요 임계값 설정이 표시됩니다. 현재 임계값 설정 대화 상자에서 * 임계값 편집 * 링크를 클릭하여 임계값 설정을 편집할 수도 있습니다. Capacity * 확인란의 선택을 취소하면 토폴로지의 모든 볼륨에 대한 모든 용량 정보가 숨겨집니다.

- 지연

수신 보호 관계의 지연 기간 및 지연 상태를 표시합니다. Lag * 확인란의 선택을 취소하면 토폴로지의 모든 볼륨에

대한 모든 지연 정보가 숨겨집니다. Lag * (지연 *) 확인란이 흐리게 표시되면 선택한 볼륨의 지연 정보가 토폴로지 아래의 관계 표와 모든 관련 볼륨의 지연 정보에 표시됩니다.

- 스냅샷

  볼륨에 사용 가능한 스냅샷 복사본의 수를 표시합니다. Snapshot * 확인란의 선택을 취소하면 토폴로지의 모든 볼륨에 대한 모든 스냅샷 복사본 정보가 숨겨집니다. 스냅샷 복사본 아이콘( )는 볼륨의 스냅샷 복사본 목록을 표시합니다. 아이콘 옆에 표시되는 스냅샷 복사본 수는 약 1시간마다 업데이트되지만 아이콘을 클릭하면 스냅샷 복사본 목록이 업데이트됩니다. 이로 인해 토폴로지에 표시된 스냅샷 복사본 수와 아이콘을 클릭할 때 나열되는 스냅샷 복사본 수가 다를 수 있습니다.

- 마지막으로 성공한 전송

  마지막으로 성공한 데이터 전송의 양, 기간, 시간 및 날짜를 표시합니다. 마지막으로 성공한 전송 * 확인란이 흐리게 표시되면 선택한 볼륨에 대한 마지막으로 성공한 전송 정보가 토폴로지 아래의 관계 표와 모든 관련 볼륨에 대한 마지막으로 성공한 전송 정보에 표시됩니다.

  - * 기록 *

    그래프에 선택된 볼륨에 대해 수신되는 SnapMirror 및 SnapVault 보호 관계의 기록이 표시됩니다. 수신 관계 지연 기간, 수신 관계 전송 기간, 수신 관계 전송 크기 등 세 가지 기록 그래프를 사용할 수 있습니다. 기록 정보는 대상 볼륨을 선택한 경우에만 표시됩니다. 기본 볼륨을 선택하면 그래프가 비어 있고 No data found(데이터를 찾을 수 없음) 메시지가 표시됩니다. 볼륨이 정합성 보장 그룹 및 SnapMirror 동기식 관계에 의해 보호되는 경우 관계 전송 기간 및 관계 전송 크기에 대한 정보가 표시되지 않습니다.

  기록 창 상단의 드롭다운 목록에서 그래프 유형을 선택할 수 있습니다. 또한 1주, 1개월 또는 1년을 선택하여 특정 기간에 대한 세부 정보를 볼 수도 있습니다. 기록 그래프는 추세를 식별하는 데 도움이 됩니다. 예를 들어, 많은 양의 데이터가 하루 또는 주 중 동시에 전송되거나 지연 경고 또는 지연 오류 임계값이 지속적으로 위반되는 경우 적절한 조치를 취할 수 있습니다. 또한 * 내보내기 * 버튼을 클릭하여 보고 있는 차트에 대한 보고서를 CSV 형식으로 만들 수 있습니다.

보호 기록 그래프에는 다음 정보가 표시됩니다.

- * 관계 지연 기간 *

  세로(y) 축에 초, 분 또는 시간을 표시하고 선택한 기간에 따라 가로(x) 축에 일, 월 또는 년을 표시합니다. y축의 상단 값은 x축에 표시된 기간 동안 도달한 최대 지연 기간을 나타냅니다. 그래프의 가로 주황색 선은 지연 오류 임계값을 나타내고, 가로 노란색 선은 지연 경고 임계값을 나타냅니다. 이러한 선 위에 커서를 놓으면 임계값 설정이 표시됩니다. 파란색 수평선은 지연 기간을 나타냅니다. 관심 영역 위에 커서를 놓으면 그래프에서 특정 지점의 세부 정보를 볼 수 있습니다.

- * 관계 이전 기간 *

  세로(y) 축에 초, 분 또는 시간을 표시하고 선택한 기간에 따라 가로(x) 축에 일, 월 또는 년을 표시합니다. y축의 상단 값은 x축에 표시된 기간 동안 도달한 최대 전송 기간을 나타냅니다. 커서를 관심 영역 위에 놓으면 그래프에서 특정 지점의 세부 정보를 볼 수 있습니다.

  ⓘ 동기식 보호 관계에 있는 볼륨에는 이 차트를 사용할 수 없습니다.

- * 전송된 관계 크기 *

  전송 크기에 따라 세로(y) 축에 바이트, 킬로바이트, 메가바이트 등을 표시하고 선택한 기간에 따라 가로(x) 축에 일,

월 또는 년을 표시합니다. y축의 상단 값은 x축에 표시된 기간 동안 도달한 최대 전송 크기를 나타냅니다. 관심 영역 위에 커서를 놓으면 그래프에서 특정 지점의 세부 정보를 볼 수 있습니다.

동기식 보호 관계에 있는 볼륨에는 이 차트를 사용할 수 없습니다.

기록 영역

History 영역에는 선택한 볼륨의 용량 및 공간 예약에 대한 정보를 제공하는 그래프가 표시됩니다. 또한 * 내보내기 * 버튼을 클릭하여 보고 있는 차트에 대한 보고서를 CSV 형식으로 만들 수 있습니다.

그래프가 비어 있을 수 있으며 일정 기간 동안 볼륨의 데이터 또는 상태가 변경되지 않은 상태로 유지될 때 No data found(데이터를 찾을 수 없음) 메시지가 표시됩니다.

기록 창 상단의 드롭다운 목록에서 그래프 유형을 선택할 수 있습니다. 또한 1주, 1개월 또는 1년을 선택하여 특정 기간에 대한 세부 정보를 볼 수도 있습니다. 기록 그래프는 추세를 식별하는 데 도움이 됩니다. 예를 들어, 볼륨 사용량이 거의 가득 찬 임계값을 지속적으로 초과하는 경우 적절한 조치를 취할 수 있습니다.

기록 그래프에는 다음 정보가 표시됩니다.

- * 사용된 볼륨 용량 *

  볼륨에서 사용된 용량과 사용 기록을 기준으로 볼륨 용량이 사용되는 추세를 바이트, 킬로바이트, 메가바이트 등의 행 그래프로 세로(y) 축에 표시합니다. 기간은 가로(x) 축에 표시됩니다. 주, 월 또는 연도의 기간을 선택할 수 있습니다. 특정 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다. 적절한 범례를 클릭하여 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, Volume Used Capacity(사용된 볼륨) 범례를 클릭하면 Volume Used Capacity(사용된 볼륨) 그래프 선이 숨겨집니다.

- * 사용된 볼륨 용량과 총 용량 *

  사용 기록을 기준으로 볼륨 용량이 사용되는 방식과 사용된 용량, 총 용량 및 중복제거 및 압축으로 절약한 공간 세부 정보를 바이트, 킬로바이트, 메가바이트, 메가바이트 단위로 선 그래프로 표시합니다. 그런 다음 세로(y) 축 위에 있습니다. 기간은 가로(x) 축에 표시됩니다. 주, 월 또는 연도의 기간을 선택할 수 있습니다. 특정 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다. 적절한 범례를 클릭하여 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, Trend Capacity Used 범례를 클릭하면 Trend Capacity Used 그래프 선이 숨겨집니다.

- * 사용된 볼륨 용량(%) *

  볼륨에서 사용된 용량과 사용 기록을 기준으로 볼륨 용량이 사용되는 추세를 세로(y) 축에서 선형 그래프(백분율)로 표시합니다. 기간은 가로(x) 축에 표시됩니다. 주, 월 또는 연도의 기간을 선택할 수 있습니다. 특정 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다. 적절한 범례를 클릭하여 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, Volume Used Capacity(사용된 볼륨) 범례를 클릭하면 Volume Used Capacity(사용된 볼륨) 그래프 선이 숨겨집니다.

- * 사용된 스냅샷 용량(%) *

  스냅샷 예약 및 스냅샷 경고 임계값을 선 그래프로 표시하고, 스냅샷 복사본에 사용되는 용량을 수직(y) 축으로 백분율로 표시합니다. 스냅샷 오버플로 는 다양한 색상으로 표시됩니다. 기간은 가로(x) 축에 표시됩니다. 주, 월 또는 연도의 기간을 선택할 수 있습니다. 특정 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다. 적절한 범례를 클릭하여 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, Snapshot Reserve 범례를 클릭하면 Snapshot Reserve(스냅숏 예비 공간) 그래프 선이 숨겨집니다.

이벤트 목록

이벤트 목록에는 새 이벤트와 승인된 이벤트에 대한 세부 정보가 표시됩니다.

- * 심각도 *

  이벤트의 심각도를 표시합니다.

- * 이벤트 *

  이벤트 이름을 표시합니다.

- * 트리거 시간 *

  이벤트가 생성된 후 경과한 시간을 표시합니다. 경과된 시간이 주를 초과하면 이벤트가 생성된 타임스탬프가 표시됩니다.

관련 주석 창

Related Annotations(관련 주석) 창에서는 선택한 볼륨과 관련된 주석 세부 정보를 볼 수 있습니다. 세부 정보에는 주석 이름과 볼륨에 적용된 주석 값이 포함됩니다. 관련 주석 창에서 수동 주석을 제거할 수도 있습니다.

관련 장치 창

Related Devices 창을 사용하면 볼륨과 관련된 SVM, 애그리게이트, qtree, LUN 및 스냅샷 복사본을 확인하고 이동할 수 있습니다.

- * 스토리지 가상 머신 *

  선택한 볼륨이 포함된 SVM의 용량 및 상태를 표시합니다.

- * 집계 *

  선택한 볼륨이 포함된 애그리게이트의 용량 및 상태가 표시됩니다. FlexGroup 볼륨의 경우 FlexGroup를 구성하는 애그리게이트 수가 나열됩니다.

- * 집계 볼륨 *

  선택한 볼륨의 상위 애그리게이트에 속한 모든 볼륨의 수와 용량을 표시합니다. 볼륨의 상태 또한 가장 높은 심각도 수준에 따라 표시됩니다. 예를 들어 aggregate에 10개의 볼륨이 포함되어 있고, 그 중 5개는 경고 상태를 표시하고 나머지 5개는 위험 상태를 표시하는 경우, 표시된 상태는 위험 입니다. 이 구성 요소는 FlexGroup 볼륨에 대해 표시되지 않습니다.

- * qtree *

  선택한 볼륨에 포함된 qtree 수와 선택한 볼륨에 포함된 할당량이 있는 Qtree 용량을 표시합니다. 할당량이 있는 qtree의 용량은 볼륨 데이터 용량과 관련하여 표시됩니다. qtree의 상태도 가장 높은 심각도 수준에 따라 표시됩니다. 예를 들어, 볼륨에 10개의 qtree, 5개의 경고 상태, 나머지 5개의 위험 상태가 표시되는 경우 상태는 긴급입니다.

- * NFS 공유 *

  볼륨과 연결된 NFS 공유의 수와 상태를 표시합니다.

- * SMB 공유 *

  SMB/CIFS 공유의 수와 상태를 표시합니다.

- LUN *

  선택한 볼륨에 있는 모든 LUN의 수와 총 크기를 표시합니다. 가장 높은 심각도 수준에 따라 LUN의 상태도 표시됩니다.

- * 사용자 및 그룹 할당량 *

  볼륨 및 해당 qtree와 관련된 사용자 및 사용자 그룹 할당량의 수와 상태를 표시합니다.

- FlexClone 볼륨 *

  선택한 볼륨의 복제된 모든 볼륨의 수와 용량을 표시합니다. 이 수와 용량은 선택한 볼륨에 복제된 볼륨이 포함된 경우에만 표시됩니다.

- * 상위 볼륨 *

  선택한 FlexClone 볼륨의 상위 볼륨의 이름과 용량을 표시합니다. 선택한 볼륨이 FlexClone 볼륨인 경우에만 상위 볼륨이 표시됩니다.

관련 그룹 창

Related Groups(관련 그룹) 창에서는 선택한 볼륨과 연결된 그룹 목록을 볼 수 있습니다.

관련 경고 창

Related Alerts 창에서는 선택한 볼륨에 대해 생성된 알림 목록을 볼 수 있습니다. 알림 추가 링크를 클릭하여 알림을 추가하거나 알림 이름을 클릭하여 기존 알림을 편집할 수도 있습니다.

스토리지 **VM**/상태 세부 정보 페이지

스토리지 VM/상태 세부 정보 페이지를 사용하여 상태, 용량, 구성, 데이터 정책, 논리 인터페이스(LIF), LUN, qtree, 사용자, 사용자 그룹 할당량 및 보호 세부 정보 또한 스토리지 VM에 대한 관련 개체 및 관련 경고에 대한 정보도 볼 수 있습니다.

데이터 스토리지 VM만 모니터링할 수 있습니다.

명령 버튼

명령 버튼을 사용하여 선택한 스토리지 VM에 대해 다음 작업을 수행할 수 있습니다.

- * 성능 보기로 전환 *

  스토리지 VM/성능 세부 정보 페이지로 이동할 수 있습니다.

- * 조치 *
  - 경고 추가

선택한 스토리지 VM에 경고를 추가할 수 있습니다.

◦ 주석 달기

선택한 스토리지 VM에 주석을 달 수 있습니다.

- * 스토리지 VM 보기 *

  상태: 모든 스토리지 VM 보기로 이동할 수 있습니다.

상태 탭

상태 탭에는 볼륨, 애그리게이트, NAS LIF, SAN LIF, LUN, 볼륨 등과 같은 다양한 개체의 데이터 가용성, 데이터 용량 및 보호 문제에 대한 자세한 정보가 표시됩니다. 프로토콜, 서비스, NFS 공유, CIFS 공유

개체의 그래프를 클릭하여 필터링된 개체 목록을 볼 수 있습니다. 예를 들어, 볼륨 용량 그래프를 클릭하면 경고를 표시하여 심각도와 관련된 용량 문제가 있는 볼륨 목록을 경고로 볼 수 있습니다.

- * 가용성 문제 *

  가용성 문제가 있는 오브젝트 및 가용성 관련 문제가 없는 오브젝트를 포함하여 총 오브젝트 수를 그래프로 표시합니다. 그래프의 색상은 문제의 서로 다른 심각도 수준을 나타냅니다. 그래프 아래의 정보는 스토리지 VM의 데이터 가용성에 영향을 미칠 수 있거나 이미 영향을 미친 가용성 문제에 대한 세부 정보를 제공합니다. 예를 들어, NAS LIF 및 다운된 SAN LIF와 오프라인 상태인 볼륨에 대한 정보가 표시됩니다.

  또한 현재 실행 중인 관련 프로토콜과 서비스, NFS 및 CIFS 공유의 수와 상태에 대한 정보를 볼 수 있습니다.

- * 용량 문제 *

  용량 문제가 있는 오브젝트 및 용량 관련 문제가 없는 오브젝트를 포함하여 총 오브젝트 수를 그래프로 표시합니다. 그래프의 색상은 문제의 서로 다른 심각도 수준을 나타냅니다. 아래 그래프는 스토리지 VM의 데이터 용량에 영향을 미치거나 이미 영향을 미칠 수 있는 용량 문제에 대한 세부 정보를 제공합니다. 예를 들어, 설정된 임계값을 초과할 가능성이 있는 애그리게이트에 대한 정보가 표시됩니다.

- * 보호 문제 *

  에서는 필드 대화 상자로 보호 문제가 있는 관계 및 보호 관련 문제가 없는 관계를 포함하여 총 관계 수를 표시하여 스토리지 VM 보호 관련 상태에 대한 간략한 개요를 제공합니다. 선택한 스토리지 VM에 대한 스토리지 VM DR 관계의 상태도 볼 수 있습니다. 스토리지 VM DR 관계 이벤트가 여기에 표시되고 이벤트를 클릭하면 이벤트 세부 정보 페이지로 이동합니다. 보호되지 않은 볼륨이 있는 경우 링크를 클릭하면 스토리지 VM에서 보호되지 않은 볼륨의 필터링된 목록을 볼 수 있는 상태: 모든 볼륨 보기로 이동합니다. 그래프의 색상은 문제의 서로 다른 심각도 수준을 나타냅니다. 그래프를 클릭하면 [관계: 모든 관계] 보기로 이동합니다. 이 보기에서 보호 관계 세부 정보의 필터링된 목록을 볼 수 있습니다. 아래 그래프는 스토리지 VM의 데이터 보호에 영향을 미치거나 이미 영향을 미칠 수 있는 보호 문제에 대한 세부 정보를 제공합니다. 예를 들어, Snapshot 복사본 예약 공간이 거의 가득 찼거나 SnapMirror 관계 지연 문제에 대한 정보가 표시됩니다.

용량 탭

용량 탭에는 선택된 SVM의 데이터 용량에 대한 자세한 정보가 표시됩니다.

FlexVol 볼륨 또는 FlexGroup 볼륨이 있는 스토리지 VM에 대해 다음 정보가 표시됩니다.

- * 용량 *

  Capacity 영역에는 모든 볼륨에서 할당된 사용된 용량과 사용 가능한 용량에 대한 세부 정보가 표시됩니다.

  - 총 용량

    스토리지 VM의 총 용량을 표시합니다.

  - 사용됨

    스토리지 VM에 속한 볼륨의 데이터가 사용하는 공간을 표시합니다.

  - 보장 사용 가능

    스토리지 VM의 볼륨에 사용할 수 있는 데이터에 대해 보장된 사용 가능한 공간을 표시합니다.

  - 보장 안 됨

    스토리지 VM에서 씬 프로비저닝된 볼륨에 할당된 데이터에 남아 있는 사용 가능한 공간을 표시합니다.

- * 용량 문제가 있는 볼륨 *

  Capacity Issues(용량 문제) 목록이 표 형식으로 용량 문제가 있는 볼륨에 대한 세부 정보를 표시합니다.

  - 상태

    볼륨에 표시된 심각도의 용량 관련 문제가 있음을 나타냅니다.

    용량 관련 이벤트 또는 볼륨에 대해 생성된 이벤트에 대한 자세한 정보를 보려면 상태 위로 포인터를 이동할 수 있습니다.

    단일 이벤트에 의해 볼륨 상태가 결정되는 경우 이벤트가 트리거된 이벤트 이름, 시간 및 날짜, 이벤트가 할당된 관리자의 이름 및 이벤트 원인과 같은 정보를 볼 수 있습니다. [상세정보 보기] * 버튼을 사용하여 이벤트에 대한 자세한 정보를 볼 수 있습니다.

    볼륨의 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우 상위 3개 이벤트는 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자의 이름 등의 정보와 함께 표시됩니다. 이벤트 이름을 클릭하면 이러한 각 이벤트에 대한 자세한 정보를 볼 수 있습니다. 생성된 이벤트 목록을 보려면 * 모든 이벤트 보기 * 링크를 클릭할 수도 있습니다.

    > 볼륨에는 동일한 심각도 또는 서로 다른 심각도의 여러 이벤트가 있을 수 있습니다. 그러나 가장 높은 심각도만 표시됩니다. 예를 들어, 볼륨에 오류 심각도와 경고 심각도의 이벤트가 두 개 있는 경우 오류 심각도만 표시됩니다.

  - 볼륨

    볼륨의 이름을 표시합니다.

  - 사용된 데이터 용량

    볼륨 용량 사용에 대한 정보(백분율)를 그래프로 표시합니다.

◦ 전체 백업 일수

볼륨이 전체 용량에 도달하기 전까지 남은 예상 일 수를 표시합니다.

◦ 씬 프로비저닝되었습니다

선택한 볼륨에 대해 공간 보장이 설정되어 있는지 여부를 표시합니다. 유효한 값은 Yes 및 No입니다

◦ 애그리게이트

FlexVol 볼륨의 경우 볼륨을 포함하는 애그리게이트의 이름을 표시합니다. FlexGroup 볼륨의 경우 FlexGroup에 사용되는 애그리게이트 수를 표시합니다.

Configuration(구성) 탭

구성 탭에는 클러스터, 루트 볼륨, 포함된 볼륨 유형(FlexVol 볼륨), 정책 및 스토리지 VM에서 생성된 보호 등 선택한 스토리지 VM에 대한 구성 세부 정보가 표시됩니다.

- * 개요 *
  - 클러스터

    스토리지 VM이 속한 클러스터의 이름을 표시합니다.

  - 허용된 볼륨 유형입니다

    스토리지 VM에서 생성할 수 있는 볼륨 유형을 표시합니다. 유형은 FlexVol 또는 FlexVol/FlexGroup입니다.

  - 루트 볼륨

    스토리지 VM의 루트 볼륨 이름을 표시합니다.

  - 허용된 프로토콜

    스토리지 VM에서 구성할 수 있는 프로토콜 유형을 표시합니다. 또한, 프로토콜이 작동 중임을 나타냅니다(), 아래쪽() 또는 이(가) 구성되지 않았습니다()를 클릭합니다.

- * 데이터 네트워크 인터페이스 *
  - NAS

    스토리지 VM과 연결된 NAS 인터페이스의 수를 표시합니다. 또한 인터페이스가 작동() 또는 아래쪽()를 클릭합니다.

  - 산

    스토리지 VM과 연결된 SAN 인터페이스 수를 표시합니다. 또한 인터페이스가 작동() 또는 아래쪽()를 클릭합니다.

  - FC-NVMe를 참조하십시오

    스토리지 VM과 연결된 FC-NVMe 인터페이스 수를 표시합니다. 또한 인터페이스가 작동() 또는 아래쪽()를 클릭합니다.

- * 관리 네트워크 인터페이스 *
  - 가용성

    스토리지 VM과 연결된 관리 인터페이스의 수를 표시합니다. 또한 관리 인터페이스가 작동( ) 또는 아래쪽( )를 클릭합니다.

- * 정책 *
  - 스냅샷 수

    스토리지 VM에 생성된 스냅샷 정책의 이름을 표시합니다.

  - 엑스포트 정책

    단일 정책이 생성된 경우 내보내기 정책의 이름을 표시하거나 여러 정책이 생성된 경우 내보내기 정책의 수를 표시합니다.

- * 보호 *
  - 스토리지 VM DR

    선택한 스토리지 VM이 보호되는지, 대상 또는 보호되지 않음인지 여부와 스토리지 VM이 보호되는 대상 이름을 표시합니다. 선택한 스토리지 VM이 대상으로 지정된 경우 소스 스토리지 VM의 세부 정보가 표시됩니다. 팬아웃의 경우 이 필드에는 스토리지 VM이 보호되는 총 대상 스토리지 VM 수가 표시됩니다. 개수 링크를 클릭하면 소스 스토리지 VM에서 필터링된 스토리지 VM 관계 그리드로 이동합니다.

  - 보호된 볼륨

    선택한 스토리지 VM의 보호된 볼륨 수가 총 볼륨 중 차지하는 수를 표시합니다. 대상 스토리지 VM을 보고 있는 경우 선택된 스토리지 VM의 대상 볼륨에 대한 링크 수입니다.

  - 보호되지 않는 볼륨

    선택한 스토리지 VM의 보호되지 않은 볼륨 수를 표시합니다.

- 서비스 *
  - 유형

    스토리지 VM에 구성된 서비스 유형을 표시합니다. 이 유형은 DNS(Domain Name System) 또는 NIS(Network Information Service)일 수 있습니다.

  - 상태

    작동 가능한 서비스 상태를 표시합니다( ), 아래쪽( ) 또는 구성되지 않음( )를 클릭합니다.

  - 도메인 이름

    NIS 서비스에 대한 DNS 서비스 또는 NIS 서버에 대한 DNS 서버의 FQDN(정규화된 도메인 이름)을 표시합니다. NIS 서버가 활성화되면 NIS 서버의 활성 FQDN이 표시됩니다. NIS 서버가 비활성화되면 모든 FQDN 목록이 표시됩니다.

  - IP 주소

DNS 또는 NIS 서버의 IP 주소를 표시합니다. NIS 서버가 활성화되면 NIS 서버의 활성 IP 주소가 표시됩니다. NIS 서버가 비활성화되면 모든 IP 주소 목록이 표시됩니다.

네트워크 인터페이스 탭

네트워크 인터페이스 탭에는 선택된 스토리지 VM에 생성된 데이터 네트워크 인터페이스(LIF)에 대한 세부 정보가 표시됩니다.

- * 네트워크 인터페이스 *

  선택한 스토리지 VM에 생성된 인터페이스의 이름을 표시합니다.

- * 작동 상태 *

  작동 가능한 인터페이스의 작동 상태를 표시합니다(), 아래쪽() 또는 알 수 없음()를 클릭합니다. 인터페이스의 작동 상태는 해당 물리적 포트의 상태에 따라 결정됩니다.

- * 관리 상태 *

  작동 가능한 인터페이스의 관리 상태를 표시합니다(), 아래쪽() 또는 알 수 없음()를 클릭합니다. 인터페이스의 관리 상태는 스토리지 관리자가 구성을 변경하거나 유지 관리를 위해 제어합니다. 관리 상태는 작동 상태와 다를 수 있습니다. 그러나 인터페이스의 관리 상태가 다운인 경우 기본적으로 작동 상태는 다운입니다.

- * IP 주소/WWPN *

  이더넷 인터페이스의 IP 주소와 FC LIF의 WWPN(World Wide Port Name)을 표시합니다.

- * 프로토콜 *

  CIFS, NFS, iSCSI, FC/FCoE 등과 같이 인터페이스에 지정된 데이터 프로토콜 목록을 표시합니다. FC-NVMe 및 FlexCache

- * 역할 *

  인터페이스 역할을 표시합니다. 역할은 데이터 또는 관리일 수 있습니다.

- * 홈 포트 *

  인터페이스가 원래 연결된 물리적 포트를 표시합니다.

- * 현재 포트 *

  인터페이스가 현재 연결되어 있는 물리적 포트를 표시합니다. 인터페이스가 마이그레이션되면 현재 포트가 홈 포트와 다를 수 있습니다.

- * 포트 세트 *

  인터페이스가 매핑되는 포트 세트를 표시합니다.

- * 페일오버 정책 *

  인터페이스에 대해 구성된 페일오버 정책을 표시합니다. NFS, CIFS 및 FlexCache 인터페이스의 경우 기본 페일오버 정책은 Next Available입니다. 페일오버 정책은 FC 및 iSCSI 인터페이스에 적용되지 않습니다.

- * 라우팅 그룹 *

  라우팅 그룹의 이름을 표시합니다. 라우팅 그룹 이름을 클릭하여 라우트와 대상 게이트웨이에 대한 자세한 정보를 볼 수 있습니다.

  라우팅 그룹은 ONTAP 8.3 이상에서 지원되지 않으므로 이러한 클러스터에 대해 빈 열이 표시됩니다.

- * 페일오버 그룹 *

  페일오버 그룹의 이름을 표시합니다.

qtree 탭

Qtree 탭에는 Qtree 및 할당량에 대한 세부 정보가 표시됩니다. 하나 이상의 qtree에 대한 qtree 용량의 상태 임계값 설정을 편집하려면 * 임계값 편집 * 버튼을 클릭합니다.

Export * 버튼을 사용하여 모니터링되는 모든 qtree의 세부 정보가 포함된 쉼표로 구분된 값(.csv) 파일을 생성합니다. CSV 파일로 내보낼 때 현재 스토리지 VM에 대한 Qtree 보고서, 현재 클러스터에 있는 모든 스토리지 VM에 대한 Qtree 보고서 또는 데이터 센터의 모든 클러스터에 대한 모든 스토리지 VM에 대한 Qtree 보고서를 만들도록 선택할 수 있습니다. 일부 추가 qtree 필드가 내보낸 CSV 파일에 나타납니다.

- * 상태 *

  qtree의 현재 상태를 표시합니다. 상태는 Critical(), 오류(), 경고() 또는 보통()를 클릭합니다.

  상태 아이콘 위로 포인터를 이동하면 qtree에 대해 생성된 이벤트 또는 이벤트에 대한 자세한 정보를 볼 수 있습니다.

  qtree 상태가 단일 이벤트로 결정되는 경우 이벤트 이름, 시간 및 이벤트 발생 날짜, 이벤트가 할당된 관리자 이름 및 이벤트 발생 원인 등의 정보를 볼 수 있습니다. View Details * 를 사용하여 이벤트에 대한 자세한 정보를 볼 수 있습니다.

  qtree의 상태가 동일한 심각도 수준의 여러 이벤트에 의해 결정되는 경우, 상위 3개 이벤트는 이벤트 이름, 이벤트 발생 시간 및 날짜, 이벤트가 할당된 관리자 이름 등의 정보와 함께 표시됩니다. 이벤트 이름을 클릭하면 이러한 각 이벤트에 대한 자세한 정보를 볼 수 있습니다. 또한 * 모든 이벤트 보기 * 를 사용하여 생성된 이벤트 목록을 볼 수 있습니다.

  > qtree에는 동일한 심각도 또는 여러 심각도의 여러 이벤트가 포함될 수 있습니다. 그러나 가장 높은 심각도만 표시됩니다. 예를 들어, qtree에 Error 와 Warning 의 심각도와 함께 두 개의 이벤트가 있는 경우 Error severity 만 표시됩니다.

- * Qtree *

  qtree의 이름이 표시됩니다.

- * 클러스터 *

  qtree가 포함된 클러스터의 이름을 표시합니다. 내보낸 CSV 파일에만 표시됩니다.

- * 스토리지 가상 머신 *

  qtree가 포함된 스토리지 가상 시스템(SVM) 이름을 표시합니다. 내보낸 CSV 파일에만 표시됩니다.

- * 볼륨 *

  qtree가 포함된 볼륨의 이름을 표시합니다.

  볼륨 이름 위로 포인터를 이동하면 볼륨에 대한 자세한 정보를 볼 수 있습니다.

- * 할당량 설정 *

  qtree에서 할당량이 설정되었는지 여부를 나타냅니다.

- * 할당량 유형 *

  사용자, 사용자 그룹 또는 qtree에 대한 할당량인지 여부를 지정합니다. 내보낸 CSV 파일에만 표시됩니다.

- * 사용자 또는 그룹 *

  사용자 또는 사용자 그룹의 이름을 표시합니다. 각 사용자 및 사용자 그룹에 대한 행이 여러 개 있습니다. 할당량 유형이 qtree가 아니거나 할당량이 설정되지 않은 경우 열은 비어 있습니다. 내보낸 CSV 파일에만 표시됩니다.

- * 사용된 디스크 % *

  사용된 디스크 공간의 비율을 표시합니다. 디스크 하드 제한값이 설정된 경우 이 값은 디스크 하드 제한값을 기준으로 합니다. 디스크 하드 제한없이 할당량이 설정된 경우 이 값은 볼륨 데이터 공간을 기준으로 합니다. 할당량이 설정되어 있지 않거나 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우 그리드 페이지에 ""해당 없음""이 표시되고 CSV 내보내기 데이터에서 필드가 비어 있습니다.

- * 디스크 하드 제한값 *

  qtree에 할당된 최대 디스크 공간 크기를 표시합니다. Unified Manager에서는 이 제한에 도달하고 추가 디스크 쓰기가 허용되지 않을 경우 중요한 이벤트를 생성합니다. 이 값은 디스크 하드 제한없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우 "무제한"으로 표시됩니다.

- * 디스크 소프트 제한값 *

  경고 이벤트가 생성되기 전에 qtree에 할당된 디스크 공간의 크기를 표시합니다. 이 값은 디스크 소프트 제한값 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 디스크 임계값 *

  디스크 공간에 설정된 임계값을 표시합니다. 이 값은 디스크 임계값 제한 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 사용된 파일 % *

  qtree에 사용된 파일의 백분율을 표시합니다. 파일 하드 제한값이 설정된 경우 이 값은 파일 하드 제한값을 기준으로 합니다. 파일 하드 제한값이 없는 할당량이 설정된 경우 값이 표시되지 않습니다. 할당량이 설정되어 있지 않거나 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우 그리드 페이지에 ""해당 없음""이 표시되고 CSV 내보내기 데이터에서 필드가 비어 있습니다.

- * 파일 하드 제한값 *

Qtree에서 허용되는 파일 수의 하드 제한값을 표시합니다. 이 값은 다음과 같은 조건에서 "Unlimited"로 표시됩니다. 파일 하드 제한없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우.

- * 파일 소프트 제한값 *

  Qtree에서 허용되는 파일 수의 소프트 제한값을 표시합니다. 이 값은 다음과 같은 조건에서 "Unlimited"로 표시됩니다. 파일 소프트 제한값 없이 할당량이 설정된 경우, 할당량이 설정되지 않은 경우 또는 qtree가 속한 볼륨에서 할당량이 꺼져 있는 경우. 기본적으로 이 열은 숨겨져 있습니다.

사용자 및 그룹 할당량 탭

선택한 스토리지 VM의 사용자 및 사용자 그룹 할당량에 대한 세부 정보를 표시합니다. 할당량 상태, 사용자 또는 사용자 그룹 이름, 디스크 및 파일에 설정된 소프트 및 하드 제한값, 사용된 디스크 공간 및 파일 수, 디스크 임계값 등의 정보를 볼 수 있습니다. 사용자 또는 사용자 그룹과 연결된 이메일 주소를 변경할 수도 있습니다.

- * 이메일 주소 편집 명령 버튼 *

  선택한 사용자 또는 사용자 그룹의 현재 전자 메일 주소를 표시하는 전자 메일 주소 편집 대화 상자를 엽니다. 이메일 주소를 수정할 수 있습니다. 이메일 주소 편집 필드가 비어 있는 경우 기본 규칙을 사용하여 선택한 사용자 또는 사용자 그룹에 대한 이메일 주소를 생성합니다.

  두 명 이상의 사용자가 동일한 할당량을 가진 경우 사용자 이름이 쉼표로 구분된 값으로 표시됩니다. 또한 기본 규칙은 이메일 주소를 생성하는 데 사용되지 않으므로 알림을 보낼 이메일 주소를 입력해야 합니다.

- * 이메일 규칙 구성 명령 버튼 *

  스토리지 VM에 구성된 사용자 또는 사용자 그룹 할당량에 대한 이메일 주소를 생성하기 위한 규칙을 생성하거나 수정할 수 있습니다. 할당량 위반이 발생하면 지정된 이메일 주소로 알림이 전송됩니다.

- * 상태 *

  할당량의 현재 상태를 표시합니다. 상태는 Critical(), 경고() 또는 보통()를 클릭합니다.

  상태 아이콘 위로 포인터를 이동하면 할당량에 대해 생성된 이벤트 또는 이벤트에 대한 자세한 정보를 볼 수 있습니다.

  할당량 상태가 단일 이벤트에 의해 결정되는 경우 이벤트가 트리거된 이벤트 이름, 시간 및 날짜, 이벤트가 할당된 관리자의 이름 및 이벤트 원인과 같은 정보를 볼 수 있습니다. View Details * 를 사용하여 이벤트에 대한 자세한 정보를 볼 수 있습니다.

  할당량 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우 상위 세 개의 이벤트는 이벤트 이름, 이벤트가 트리거된 시간 및 날짜, 이벤트가 할당된 관리자의 이름 등의 정보와 함께 표시됩니다. 이벤트 이름을 클릭하면 이러한 각 이벤트에 대한 자세한 정보를 볼 수 있습니다. 또한 * 모든 이벤트 보기 * 를 사용하여 생성된 이벤트 목록을 볼 수 있습니다.

  > 할당량은 동일한 심각도 또는 서로 다른 심각도의 여러 이벤트를 가질 수 있습니다. 그러나 가장 높은 심각도만 표시됩니다. 예를 들어 할당량에 Error 와 Warning 의 심각도를 가진 두 개의 이벤트가 있는 경우 Error 심각도만 표시됩니다.

- * 사용자 또는 그룹 *

사용자 또는 사용자 그룹의 이름을 표시합니다. 두 명 이상의 사용자가 동일한 할당량을 가진 경우 사용자 이름이 쉼표로 구분된 값으로 표시됩니다.

SecD 오류로 인해 ONTAP가 유효한 사용자 이름을 제공하지 않으면 이 값은 ""알 수 없음""으로 표시됩니다.

- * 유형 *

  사용자 또는 사용자 그룹에 대한 할당량인지 여부를 지정합니다.

- * 볼륨 또는 Qtree *

  사용자 또는 사용자 그룹 할당량이 지정된 볼륨 또는 qtree의 이름을 표시합니다.

  볼륨 또는 qtree의 이름 위로 포인터를 이동하여 볼륨 또는 qtree에 대한 자세한 정보를 볼 수 있습니다.

- * 사용된 디스크 % *

  사용된 디스크 공간의 비율을 표시합니다. 이 값은 디스크 하드 제한값이 없는 할당량이 설정된 경우 ""해당 없음""으로 표시됩니다.

- * 디스크 하드 제한값 *

  할당량에 할당된 최대 디스크 공간을 표시합니다. Unified Manager에서는 이 제한에 도달하고 추가 디스크 쓰기가 허용되지 않을 경우 중요한 이벤트를 생성합니다. 이 값은 디스크 하드 제한없이 할당량이 설정된 경우 "무제한"으로 표시됩니다.

- * 디스크 소프트 제한값 *

  경고 이벤트가 생성되기 전에 할당량에 할당된 디스크 공간의 양을 표시합니다. 이 값은 디스크 소프트 제한값 없이 할당량이 설정된 경우 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 디스크 임계값 *

  디스크 공간에 설정된 임계값을 표시합니다. 이 값은 디스크 임계값 제한 없이 할당량이 설정된 경우 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 사용된 파일 % *

  qtree에 사용된 파일의 백분율을 표시합니다. 파일 하드 제한값 없이 할당량이 설정된 경우 이 값은 ""해당 없음""으로 표시됩니다.

- * 파일 하드 제한값 *

  할당량에 허용된 파일 수에 대한 하드 제한값을 표시합니다. 파일 하드 제한없이 할당량이 설정된 경우 이 값은 "무제한"으로 표시됩니다.

- * 파일 소프트 제한값 *

  할당량에 허용된 파일 수에 대한 소프트 제한값을 표시합니다. 파일 소프트 제한값 없이 할당량이 설정된 경우 이 값은 "무제한"으로 표시됩니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 이메일 주소 *

할당량에 위반이 있을 때 알림을 보낼 사용자 또는 사용자 그룹의 이메일 주소를 표시합니다.

NFS Shares 탭

NFS 공유 탭에는 상태, 볼륨과 연결된 경로(FlexGroup 볼륨 또는 FlexVol 볼륨), NFS 공유에 대한 클라이언트의 액세스 수준, 내보낸 볼륨에 대해 정의된 내보내기 정책 등의 NFS 공유에 대한 정보가 표시됩니다. NFS 공유는 다음 조건에서 표시되지 않습니다. 볼륨이 마운트되어 있지 않거나 볼륨에 대한 엑스포트 정책과 연결된 프로토콜에 NFS 공유가 포함되지 않은 경우

- * 상태 *

  NFS 공유의 현재 상태를 표시합니다. 상태는 오류( ) 또는 보통( )를 클릭합니다.

- * 정크션 경로 *

  볼륨이 마운트되는 경로를 표시합니다. 명시적 NFS 엑스포트 정책이 qtree에 적용되는 경우, qtree를 액세스할 수 있는 볼륨의 경로가 열에 표시됩니다.

- * 정크션 경로 활성화 *

  마운트된 볼륨에 액세스할 경로가 활성 상태인지 비활성 상태인지 여부를 표시합니다.

- * 볼륨 또는 Qtree *

  NFS 엑스포트 정책이 적용되는 볼륨 또는 qtree의 이름을 표시합니다. 볼륨의 qtree에 NFS 엑스포트 정책이 적용되는 경우 볼륨과 qtree의 이름이 모두 표시됩니다.

  링크를 클릭하면 해당 세부 정보 페이지에서 개체에 대한 세부 정보를 볼 수 있습니다. 개체가 qtree인 경우 qtree 및 볼륨에 대한 링크가 표시됩니다.

- * 볼륨 상태 *

  내보내는 볼륨의 상태를 표시합니다. 상태는 오프라인, 온라인, 제한 또는 혼합일 수 있습니다.

  - 오프라인

    볼륨에 대한 읽기 또는 쓰기 액세스가 허용되지 않습니다.

  - 온라인

    볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

  - 제한

    패리티 재구성 같은 제한된 작업은 허용되지만 데이터 액세스는 허용되지 않습니다.

  - 혼합

    FlexGroup 볼륨의 구성요소가 동일한 상태가 아닙니다.

- * 보안 스타일 *

  내보낸 볼륨에 대한 액세스 권한을 표시합니다. 보안 스타일은 UNIX, Unified, NTFS 또는 Mixed일 수 있습니다.

◦ UNIX(NFS 클라이언트)

볼륨의 파일과 디렉토리에는 UNIX 권한이 있습니다.

◦ 통합

볼륨의 파일과 디렉토리에는 통합 보안 스타일이 있습니다.

◦ NTFS(CIFS 클라이언트)

볼륨의 파일과 디렉토리에는 Windows NTFS 권한이 있습니다.

◦ 혼합

볼륨의 파일 및 디렉토리에는 UNIX 사용 권한이나 Windows NTFS 사용 권한이 있을 수 있습니다.

- * UNIX 권한 *

  내보낸 볼륨에 대해 설정된 8진수 문자열 형식으로 UNIX 사용 권한 비트를 표시합니다. UNIX 스타일 사용 권한 비트와 유사합니다.

- * 정책 내보내기 *

  내보낸 볼륨에 대한 액세스 권한을 정의하는 규칙을 표시합니다. 링크를 클릭하면 인증 프로토콜 및 액세스 권한과 같은 엑스포트 정책과 관련된 규칙에 대한 세부 정보를 볼 수 있습니다.

SMB 공유 탭

선택한 스토리지 VM의 SMB 공유에 대한 정보를 표시합니다. SMB 공유의 상태, 공유 이름, 스토리지 VM과 연결된 경로, 공유의 접속 경로 상태, 객체 포함, 포함된 볼륨의 상태, 공유의 보안 데이터, 공유에 대해 정의된 내보내기 정책 등의 정보를 볼 수 있습니다. 또한 SMB 공유에 필요한 NFS 경로가 있는지 여부를 확인할 수도 있습니다.

폴더의 공유는 SMB 공유 탭에 표시되지 않습니다.

- * 사용자 매핑 보기 명령 버튼 *

  사용자 매핑 대화 상자를 시작합니다.

  스토리지 VM에 대한 사용자 매핑의 세부 정보를 볼 수 있습니다.

- * ACL 명령 버튼 표시 *

  공유에 대한 액세스 제어 대화 상자를 시작합니다.

  선택한 공유에 대한 사용자 및 권한 세부 정보를 볼 수 있습니다.

- * 상태 *

  공유의 현재 상태를 표시합니다. 상태는 정상( ) 또는 오류( )를 클릭합니다.

- * 공유 이름 *

SMB 공유의 이름을 표시합니다.

- * 경로 *

  공유가 생성된 접합 경로를 표시합니다.

- * 정크션 경로 활성화 *

  공유에 액세스할 경로가 활성 상태인지 비활성 상태인지 여부를 표시합니다.

- * 포함 개체 *

  공유가 속한 포함하는 객체의 이름을 표시합니다. 포함된 오브젝트는 볼륨 또는 qtree가 될 수 있습니다.

  링크를 클릭하면 해당 세부 정보 페이지에서 포함하는 객체에 대한 세부 정보를 볼 수 있습니다. 포함된 개체가 qtree인 경우 qtree와 볼륨 모두에 대한 링크가 표시됩니다.

- * 볼륨 상태 *

  내보내는 볼륨의 상태를 표시합니다. 상태는 오프라인, 온라인, 제한 또는 혼합일 수 있습니다.

  - 오프라인

    볼륨에 대한 읽기 또는 쓰기 액세스가 허용되지 않습니다.

  - 온라인

    볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

  - 제한

    패리티 재구성 같은 제한된 작업은 허용되지만 데이터 액세스는 허용되지 않습니다.

  - 혼합

    FlexGroup 볼륨의 구성요소가 동일한 상태가 아닙니다.

- * 보안 *

  내보낸 볼륨에 대한 액세스 권한을 표시합니다. 보안 스타일은 UNIX, Unified, NTFS 또는 Mixed일 수 있습니다.

  - UNIX(NFS 클라이언트)

    볼륨의 파일과 디렉토리에는 UNIX 권한이 있습니다.

  - 통합

    볼륨의 파일과 디렉토리에는 통합 보안 스타일이 있습니다.

  - NTFS(CIFS 클라이언트)

    볼륨의 파일과 디렉토리에는 Windows NTFS 권한이 있습니다.

◦ 혼합

볼륨의 파일 및 디렉토리에는 UNIX 사용 권한이나 Windows NTFS 사용 권한이 있을 수 있습니다.

- * 정책 내보내기 *

  공유에 적용할 수 있는 엑스포트 정책의 이름을 표시합니다. 스토리지 VM에 대해 엑스포트 정책이 지정되지 않은 경우 이 값은 Not Enabled로 표시됩니다.

  링크를 클릭하면 액세스 프로토콜 및 권한과 같은 엑스포트 정책과 관련된 규칙에 대한 세부 정보를 볼 수 있습니다. 선택한 스토리지 VM에 대해 엑스포트 정책이 비활성화되어 있으면 링크가 비활성화됩니다.

- * NFS에 해당 *

  공유에 해당하는 NFS가 있는지 여부를 지정합니다.

SAN 탭

선택한 스토리지 VM의 LUN, 이니시에이터 그룹 및 이니시에이터에 대한 세부 정보를 표시합니다. 기본적으로 LUN 보기가 표시됩니다. 이니시에이터 그룹 탭에서 이니시에이터 그룹에 대한 세부 정보와 이니시에이터 탭에서 이니시에이터에 대한 세부 정보를 볼 수 있습니다.

- LUN 탭 *

  선택한 스토리지 VM에 속한 LUN에 대한 세부 정보를 표시합니다. LUN 이름, LUN 상태(온라인 또는 오프라인), LUN이 포함된 파일 시스템(볼륨 또는 qtree)의 이름, 호스트 운영 체제의 유형, LUN의 총 데이터 용량 및 일련 번호와 같은 정보를 볼 수 있습니다. LUN 성능 열은 LUN/성능 세부 정보 페이지에 대한 링크를 제공합니다.

  LUN에서 씬 프로비저닝이 설정되었는지 여부와 LUN이 이니시에이터 그룹에 매핑되었는지 여부에 대한 정보도 볼 수 있습니다. 이니시에이터에 매핑된 경우 선택한 LUN에 매핑된 이니시에이터 그룹 및 이니시에이터를 볼 수 있습니다.

- * 이니시에이터 그룹 탭 *

  이니시에이터 그룹에 대한 세부 정보를 표시합니다. 이니시에이터 그룹의 이름, 액세스 상태, 그룹의 모든 이니시에이터에 사용되는 호스트 운영 체제의 유형, 지원되는 프로토콜과 같은 세부 정보를 볼 수 있습니다. 액세스 상태 열에서 링크를 클릭하면 이니시에이터 그룹의 현재 액세스 상태를 볼 수 있습니다.

  ◦ * 보통 *

    이니시에이터 그룹이 여러 액세스 경로에 연결되어 있습니다.

  ◦ * 단일 경로 *

    이니시에이터 그룹이 단일 액세스 경로에 연결됩니다.

  ◦ * 경로 없음 *

    이니시에이터 그룹에 연결된 액세스 경로가 없습니다.

    이니시에이터 그룹이 포트 세트를 통해 모든 인터페이스에 매핑되었는지 또는 특정 인터페이스에 매핑되었는지 확인할 수 있습니다. Mapped Interfaces 열에서 count 링크를 클릭하면 모든 인터페이스가 표시되거나 포트 세트의 특정 인터페이스가 표시됩니다. 대상 포털을 통해 매핑된 인터페이스는 표시되지 않습니다.

이니시에이터 그룹에 매핑된 총 이니시에이터 및 LUN 수가 표시됩니다.

또한 선택한 이니시에이터 그룹에 매핑된 LUN 및 이니시에이터를 볼 수도 있습니다.

- * 이니시에이터 탭 *

  선택한 스토리지 VM에 대해 이 이니시에이터에 매핑된 이니시에이터 그룹의 이름과 유형, 총 이니시에이터 그룹 수를 표시합니다.

```
initiator groups that are mapped to the selected initiator group.
```

관련 주석 창

Related Annotations(관련 주석) 창에서는 선택한 스토리지 VM과 관련된 주석 세부 정보를 볼 수 있습니다. 세부 정보에는 스토리지 VM에 적용되는 주석 이름 및 주석 값이 포함됩니다. 관련 주석 창에서 수동 주석을 제거할 수도 있습니다.

관련 장치 창

Related Devices 창에서는 스토리지 VM과 관련된 클러스터, 애그리게이트 및 볼륨을 볼 수 있습니다.

- * 클러스터 *

  스토리지 VM이 속한 클러스터의 상태를 표시합니다.

- * 애그리게이트 *

  선택한 스토리지 VM에 속하는 애그리게이트 수를 표시합니다. 최고 심각도 수준에 따라 애그리게이트의 상태도 표시됩니다. 예를 들어, 스토리지 VM에 10개의 애그리게이트가 포함되어 있는 경우 5개의 애그리게이트가 경고 상태를 표시하고 나머지 5개의 애그리게이트는 위험 상태를 표시하는 경우 표시된 상태는 심각입니다.

- * 할당된 애그리게이트 *

  스토리지 VM에 할당된 애그리게이트 수를 표시합니다. 최고 심각도 수준에 따라 애그리게이트의 상태도 표시됩니다.

- 볼륨 *

  선택한 스토리지 VM에 속한 볼륨의 수와 용량을 표시합니다. 볼륨의 상태 또한 가장 높은 심각도 수준에 따라 표시됩니다. 스토리지 VM에 FlexGroup 볼륨이 있는 경우 이 개수에는 FlexGroups가 포함되며 FlexGroup 구성 요소는 포함되지 않습니다.

관련 그룹 창

Related Groups 창에서는 선택한 스토리지 VM과 연결된 그룹 목록을 볼 수 있습니다.

관련 경고 창

관련 알림 창을 사용하면 선택한 스토리지 VM에 대해 생성된 알림 목록을 볼 수 있습니다. 또한 * Add Alert * (경고 추가 *) 링크를 클릭하여 경고를 추가하거나 경고 이름을 클릭하여 기존 경고를 편집할 수도 있습니다.

클러스터/상태 세부 정보 페이지

클러스터/상태 세부 정보 페이지에는 상태, 용량 및 구성 세부 정보와 같은 선택한 클러스터에 대한 자세한 정보가 표시됩니다. 또한 LIF(네트워크 인터페이스), 노드, 디스크, 관련 장치 및 클러스터에 대한 관련 경고에 대한 정보도 볼 수 있습니다.

클러스터 이름 옆의 상태(예: 양호)는 통신 상태, Unified Manager가 클러스터와 통신할 수 있는지 여부를 나타냅니다. 클러스터의 페일오버 상태 또는 전체 상태는 나타내지 않습니다.

명령 버튼

명령 버튼을 사용하여 선택한 클러스터에 대해 다음 작업을 수행할 수 있습니다.

- * 성능 보기로 전환 *

  클러스터/성능 세부 정보 페이지로 이동할 수 있습니다.

- * 조치 *

  - Add Alert(경고 추가): Add Alert(경고 추가) 대화 상자를 엽니다. 이 대화 상자에서 선택한 클러스터에 경고를 추가할 수 있습니다.
  - 재검색: 클러스터의 수동 업데이트를 시작하여 Unified Manager가 클러스터의 최근 변경 사항을 검색할 수 있습니다.

    Unified Manager가 OnCommand Workflow Automation와 페어링된 경우, 다시 검색 작업을 통해 WFA에서 캐시된 데이터를 다시 가져옵니다.

  재검색 작업이 시작된 후 작업 상태를 추적할 수 있도록 관련 작업 세부 정보에 대한 링크가 표시됩니다.

  - 주석: 선택한 클러스터에 주석을 달 수 있습니다.
- * 클러스터 보기 *

  상태: 모든 클러스터 보기로 이동할 수 있습니다.

상태 탭

노드, SVM, 애그리게이트 등과 같은 다양한 클러스터 오브젝트의 데이터 가용성 및 데이터 용량 문제에 대한 자세한 정보를 표시합니다. 가용성 문제는 클러스터 개체의 데이터 제공 기능과 관련이 있습니다. 용량 문제는 클러스터 객체의 데이터 저장 기능과 관련이 있습니다.

개체의 그래프를 클릭하여 필터링된 개체 목록을 볼 수 있습니다. 예를 들어, SVM 용량 그래프를 클릭하면 경고를 표시하여 필터링된 SVM 목록을 볼 수 있습니다. 이 목록에는 용량 문제가 있고 심각도 수준의 경고가 있는 SVM이 포함되어 있습니다. 경고를 표시하는 SVM 가용성 그래프를 클릭하여 심각도 수준의 경고 수준에서 가용성 문제가 있는 SVM 목록을 볼 수도 있습니다.

가용성 문제

가용성 문제와 가용성 관련 문제가 없는 오브젝트 등을 포함하여 총 오브젝트 수를 그래픽으로 표시합니다. 그래프의 색상은 문제의 서로 다른 심각도 수준을 나타냅니다. 그래프 아래의 정보는 클러스터의 데이터 가용성에 영향을 미칠 수 있거나 이미 영향을 미친 가용성 문제에 대한 세부 정보를 제공합니다. 예를 들어, 정보가 다운되는 디스크 쉘프 및 오프라인 상태인 애그리게이트에 대해 표시됩니다.

SFO 막대 그래프에 표시되는 데이터는 노드의 HA 상태를 기반으로 합니다. 다른 모든 막대 그래프에 대해 표시되는 데이터는 생성된 이벤트를 기준으로 계산됩니다.

용량 문제

용량 문제가 있는 오브젝트 및 용량 관련 문제가 없는 오브젝트를 포함하여 총 오브젝트 수를 그래픽으로 표시합니다. 그래프의 색상은 문제의 서로 다른 심각도 수준을 나타냅니다. 그래프 아래의 정보는 클러스터의 데이터 용량에 영향을 미치거나 이미 영향을 미친 용량 문제에 대한 세부 정보를 제공합니다. 예를 들어, 설정된 임계값을 초과할 가능성이 있는 애그리게이트에 대한 정보가 표시됩니다.

용량 탭

선택한 클러스터의 용량에 대한 자세한 정보를 표시합니다.

용량

할당된 모든 Aggregate의 사용 가능한 용량 및 사용 가능한 용량에 대한 데이터 용량 그래프를 표시합니다.

- 사용된 논리적 공간입니다

  ONTAP 스토리지 효율성 기술을 사용할 때의 절감 효과를 적용하지 않고도 이 클러스터의 모든 애그리게이트에 저장되어 있는 데이터의 실제 크기를 알 수 있습니다. 여기에는 스냅샷 복사본이 포함되지 않습니다.

- 데이터 축소

  는 Snapshot 복사본 없이 1.8:1과 같이 두 유효 자릿수의 비율을 표시합니다. 이 비율은 구성된 ONTAP 스토리지 효율성 설정을 기반으로 합니다.

- 사용됨

  모든 애그리게이트에서 데이터에 사용되는 물리적 용량입니다. 여기에는 패리티, 적합한 사이징 및 예약에 사용된 용량이 포함되지 않습니다.

- 사용 가능

  데이터에 사용 가능한 용량을 표시합니다.

- 예비 부품

  모든 스페어 디스크의 스토리지에 사용할 수 있는 저장 가능 용량을 표시합니다.

- 프로비저닝되었습니다

  모든 기본 볼륨에 대해 프로비저닝된 용량을 표시합니다.

세부 정보

사용된 용량과 사용 가능한 용량에 대한 자세한 정보를 표시합니다. 계산에서 루트 애그리게이트 데이터는 제외됩니다.

- 총 용량

  클러스터의 총 용량을 표시합니다. 여기에는 패리티에 할당된 용량이 포함되지 않습니다.

- 사용됨

  데이터가 사용하는 용량을 표시합니다. 여기에는 패리티, 적합한 사이징 및 예약에 사용된 용량이 포함되지 않습니다.

- 사용 가능

  데이터에 사용 가능한 용량을 표시합니다.

- 프로비저닝되었습니다

  모든 기본 볼륨에 대해 프로비저닝된 용량을 표시합니다.

- 예비 부품

  모든 스페어 디스크의 스토리지에 사용할 수 있는 저장 가능 용량을 표시합니다.

클라우드 계층

사용된 총 클라우드 계층 용량과 클러스터에서 FabricPool 지원 애그리게이트에 대해 연결된 각 클라우드 계층에 사용된 용량을 표시합니다. FabricPool는 라이센스가 있거나 라이센스가 부여되지 않은 것 중 하나입니다.

디스크 유형별 물리적 용량 브레이크아웃

디스크 유형별 물리적 용량 브레이크아웃 영역에는 클러스터에 있는 다양한 디스크 유형의 디스크 용량에 대한 자세한 정보가 표시됩니다. 디스크 유형을 클릭하면 디스크 탭에서 디스크 유형에 대한 자세한 정보를 볼 수 있습니다.

- 총 가용 용량

  데이터 디스크의 사용 가능한 용량과 여유 용량을 표시합니다.

- HDD

  클러스터에 있는 모든 HDD 데이터 디스크의 사용된 용량과 사용 가능한 용량을 그래픽으로 표시합니다. 점선은 HDD에 있는 데이터 디스크의 여유 용량을 나타냅니다.

- 플래시
  - SSD 데이터

    클러스터에서 SSD 데이터 디스크의 사용 가능한 용량과 용량을 그래픽으로 표시합니다.

  - SSD 캐시

    클러스터에 있는 SSD 캐시 디스크의 저장 가능 용량을 그래픽으로 표시합니다.

  - SSD 스페어

    클러스터에서 SSD, 데이터 및 캐시 디스크의 여유 용량을 그래픽으로 표시합니다.

- 할당되지 않은 디스크

  클러스터에서 할당되지 않은 디스크의 수를 표시합니다.

용량 문제가 있는 애그리게이트 목록

용량 위험 문제가 있는 애그리게이트의 사용된 용량 및 사용 가능한 용량에 대한 세부 정보가 표 형식으로 표시됩니다.

- 상태

  Aggregate에 특정 심각도의 용량 관련 문제가 있음을 나타냅니다.

  상태 위로 포인터를 이동하면 애그리게이트에 대해 생성된 이벤트 또는 이벤트에 대한 자세한 정보를 볼 수 있습니다.

  집계 상태가 단일 이벤트에 의해 결정되는 경우 이벤트가 트리거된 이벤트 이름, 시간 및 날짜, 이벤트가 할당된 관리자의 이름 및 이벤트 원인과 같은 정보를 볼 수 있습니다. 이벤트에 대한 자세한 정보를 보려면 * 세부 정보 보기 * 버튼을 클릭하십시오.

  집계 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우 상위 3개 이벤트는 이벤트 이름, 이벤트 트리거 시간 및 날짜, 이벤트가 할당된 관리자의 이름 등의 정보와 함께 표시됩니다. 이벤트 이름을 클릭하면 이러한 각 이벤트에 대한 자세한 정보를 볼 수 있습니다. 생성된 이벤트 목록을 보려면 * 모든 이벤트 보기 * 링크를 클릭할 수도 있습니다.

  > 애그리게이트에는 동일한 심각도 또는 서로 다른 심각도의 여러 용량 관련 이벤트가 있을 수 있습니다. 그러나 가장 높은 심각도만 표시됩니다. 예를 들어, 애그리게이트에 심각도 수준이 Error 와 Critical 인 두 개의 이벤트가 있는 경우 Critical 심각도만 표시됩니다.

- 집계

  애그리게이트의 이름을 표시합니다.

- 사용된 데이터 용량

  애그리게이트 용량 사용량에 대한 정보를 그래픽으로 표시합니다(백분율).

- 전체 백업 일수

  Aggregate가 전체 용량에 도달하기 전까지 남은 예상 일 수를 표시합니다.

Configuration(구성) 탭

IP 주소, 연락처 및 위치와 같이 선택한 클러스터에 대한 세부 정보를 표시합니다.

클러스터 개요

- 관리 인터페이스

  에는 Unified Manager가 클러스터에 연결하는 데 사용하는 클러스터 관리 LIF가 표시됩니다. 인터페이스의 작동 상태도 표시됩니다.

- 호스트 이름 또는 IP 주소입니다

  Unified Manager에서 클러스터에 연결하는 데 사용하는 클러스터 관리 LIF의 FQDN, 짧은 이름 또는 IP 주소를 표시합니다.

- FQDN

  클러스터의 FQDN(정규화된 도메인 이름)을 표시합니다.

- OS 버전

  클러스터에서 실행 중인 ONTAP 버전을 표시합니다. 클러스터의 노드가 서로 다른 버전의 ONTAP를 실행 중인 경우 가장 초기 ONTAP 버전이 표시됩니다.

- 연락처

  클러스터에 문제가 있을 경우 연락할 관리자에 대한 세부 정보를 표시합니다.

- 위치

  클러스터의 위치를 표시합니다.

- 성격

  이 클러스터가 모든 SAN 스토리지 구성 클러스터인지 확인합니다.

원격 클러스터 개요

MetroCluster 구성의 원격 클러스터에 대한 자세한 내용은 에 나와 있습니다. 이 정보는 MetroCluster 구성에 대해서만 표시됩니다.

- 클러스터

  원격 클러스터의 이름을 표시합니다. 클러스터 이름을 클릭하여 클러스터의 세부 정보 페이지로 이동할 수 있습니다.

- 호스트 이름 또는 IP 주소입니다

  원격 클러스터의 FQDN, 짧은 이름 또는 IP 주소를 표시합니다.

- 위치

  원격 클러스터의 위치를 표시합니다.

MetroCluster 개요

FC를 통한 MetroCluster 또는 IP를 통한 MetroCluster 구성의 로컬 클러스터에 대한 자세한 내용은 에 나와 있습니다. 이 정보는 FC 또는 IP를 통한 MetroCluster 구성에 대해서만 표시됩니다.

- 유형

  MetroCluster 형식이 2노드인지 4노드인지 표시합니다. MetroCluster over IP의 경우 4노드만 지원됩니다.

- 구성

  FC 및 IP를 통한 MetroCluster 구성을 표시하며 다음과 같은 값을 가질 수 있습니다.

FC * 용

- SAS 케이블을 사용하여 확장 구성
- FC-SAS 브리지로 확장 구성
- FC 스위치를 사용한 패브릭 구성

  4노드 MetroCluster의 경우 FC 스위치를 사용하는 패브릭 구성만 지원됩니다.

- IP * 용
- 이더넷 스위치를 사용하는 IP 구성(클러스터 구성 방식에 따라 L2 또는 L3)
  - 예상치 못한 자동 전환(AUSO)

    로컬 클러스터에 대해 자동 비계획 전환 활성화 여부를 표시합니다. 기본적으로 AUSO는 Unified Manager에서 2노드 MetroCluster 구성의 모든 클러스터에 대해 사용하도록 설정됩니다. 명령줄 인터페이스를 사용하여 AUSO 설정을 변경할 수 있습니다. 이 기능은 FC를 통한 MetroCluster에만 지원됩니다.

  - 전환 모드

    MetroCluster over IP 구성에 대한 전환 모드를 표시합니다. 사용 가능한 값은 다음과 같습니다. `Active`, `Negotiated Switchover`, 및 `Automatic Unplanned Switchover`.

노드

- 가용성

  작동 중인 노드 수( ) 또는 아래쪽( )를 클러스터에서 선택합니다.

- OS 버전

  노드가 실행 중인 ONTAP 버전과 특정 버전의 ONTAP를 실행하는 노드의 수를 표시합니다. 예를 들어 9.6(2), 9.3(1)은 두 노드가 ONTAP 9.6을 실행하고 한 노드는 ONTAP 9.3을 실행한다고 지정합니다.

스토리지 가상 머신

- 가용성

  에는 작동 중인 SVM의 수가 표시됩니다( ) 또는 아래쪽( )를 클러스터에서 선택합니다.

네트워크 인터페이스

- 가용성

  작동 중인 ( ) 비데이터 LIF의 수를 표시합니다) 또는 아래쪽( )를 클러스터에서 선택합니다.

- 클러스터 관리 인터페이스

  클러스터 관리 LIF의 수를 표시합니다.

- 노드 관리 인터페이스

  노드 관리 LIF의 수를 표시합니다.

- 클러스터 인터페이스

  클러스터 LIF의 수를 표시합니다.

- 인터클러스터 인터페이스

  인터클러스터 LIF의 수를 표시합니다.

프로토콜

- 데이터 프로토콜

  클러스터에 대해 활성화된 라이센스 데이터 프로토콜 목록을 표시합니다. 데이터 프로토콜에는 iSCSI, CIFS, NFS, NVMe 및 FC/FCoE가 포함됩니다.

보호

- 중개자

  클러스터가 중재자의 중재자와 연결 상태를 지원하는지 여부를 표시합니다. 중재자가 구성되었는지 여부를 나타내며, 구성된 경우 중개자의 상태가 표시됩니다.

  - 해당 없음

    클러스터에서 중재자를 지원하지 않는 경우에 표시됩니다.

  - 구성되지 않았습니다

    클러스터가 중재자를 지원하지만 중재자가 구성되지 않은 경우에 표시됩니다.

  - IP 주소

    클러스터가 중재자를 지원하고 중재자가 구성된 경우 표시됩니다. 중재자 상태는 색상으로 표시됩니다. 녹색 색은 중재자 상태에 도달할 수 있음을 나타냅니다. 빨간색은 중재자 상태에 도달할 수 없음을 나타냅니다.

클라우드 계층

에는 이 클러스터가 연결된 클라우드 계층의 이름이 나와 있습니다. 또한 유형(Amazon S3, Microsoft Azure Cloud, IBM Cloud Object Storage, Google Cloud Storage, Alibaba Cloud Object Storage, StorageGRID) 및 클라우드 계층 상태(사용 가능 또는 사용 불가능)도 나열됩니다.

MetroCluster 연결 탭

FC를 통한 MetroCluster 구성에서 클러스터 구성 요소의 문제 및 연결 상태를 표시합니다. 클러스터의 재해 복구 파트너에 문제가 있는 경우 클러스터가 빨간색 상자로 표시됩니다.

MetroCluster 접속 구성 탭은 MetroCluster over FC 구성에 있는 클러스터에만 표시됩니다.

원격 클러스터의 이름을 클릭하여 원격 클러스터의 세부 정보 페이지로 이동할 수 있습니다. 부품의 개수 링크를 클릭하여 부품의 세부 정보를 볼 수도 있습니다. 예를 들어, 클러스터에서 노드의 개수 링크를 클릭하면 클러스터의 세부 정보 페이지에 노드 탭이 표시됩니다. 원격 클러스터에서 디스크의 개수 링크를 클릭하면 원격 클러스터의 세부 정보 페이지에 디스크 탭이 표시됩니다.

8노드 MetroCluster 구성을 관리할 때 디스크 쉘프 구성요소의 카운트 링크를 클릭하면 기본 HA 쌍의 로컬 쉘프만 표시됩니다. 또한 다른 HA 쌍에 로컬 쉘프를 표시할 방법이 없습니다.

구성 요소 위로 포인터를 이동하면 문제가 발생한 경우 클러스터의 세부 정보 및 연결 상태를 확인하고 해당 문제와 관련하여 생성된 이벤트 또는 이벤트에 대한 자세한 정보를 볼 수 있습니다.

구성 요소 간 연결 문제의 상태가 단일 이벤트에 의해 결정되는 경우 이벤트가 트리거된 이벤트 이름, 시간 및 날짜, 이벤트가 할당된 관리자의 이름 및 이벤트 원인과 같은 정보를 볼 수 있습니다. View Details 버튼을 클릭하면 이벤트에 대한 자세한 정보를 볼 수 있습니다.

구성 요소 간 연결 문제의 상태가 동일한 심각도의 여러 이벤트에 의해 결정되는 경우 이벤트 이름, 이벤트 발생 시간 및 날짜, 이벤트가 할당된 관리자 이름 등의 정보와 함께 상위 세 개의 이벤트가 표시됩니다. 이벤트 이름을 클릭하면 이러한 각 이벤트에 대한 자세한 정보를 볼 수 있습니다. 생성된 이벤트 목록을 보려면 * 모든 이벤트 보기 * 링크를 클릭할 수도 있습니다.

MetroCluster 복제 탭

FC를 통해 MetroCluster 구성에서 복제되는 데이터의 상태를 표시합니다. MetroCluster 복제 탭을 사용하면 이미 피어링된 클러스터와 데이터를 동기식으로 미러링하여 데이터 보호를 보장할 수 있습니다. 클러스터의 재해 복구 파트너에 문제가 있는 경우 클러스터가 빨간색 상자로 표시됩니다.

MetroCluster 복제 탭은 FC를 통한 MetroCluster 구성에 있는 클러스터에만 표시됩니다.

MetroCluster 환경에서는 이 탭을 사용하여 원격 클러스터를 사용한 로컬 클러스터의 논리 연결과 피어링을 확인할 수 있습니다. 논리적 접속을 통해 클러스터 구성 요소의 객관적인 표현을 볼 수 있습니다. 이렇게 하면 메타데이터 및 데이터를 미러링하는 동안 발생할 수 있는 문제를 식별하는 데 도움이 됩니다.

MetroCluster 복제 탭에서 로컬 클러스터는 선택한 클러스터에 대한 자세한 그래픽 표시를 제공하고 MetroCluster 파트너가 원격 클러스터를 참조합니다.

네트워크 인터페이스 탭

선택한 클러스터에서 생성되는 모든 비데이터 LIF에 대한 세부 정보를 표시합니다.

네트워크 인터페이스

선택한 클러스터에 생성된 LIF의 이름을 표시합니다.

작동 상태

작동 가능한 인터페이스의 작동 상태를 표시합니다(↑), 아래쪽(↓) 또는 알 수 없음(?)를 클릭합니다. 네트워크 인터페이스의 작동 상태는 해당 물리적 포트의 상태에 따라 결정됩니다.

관리 상태

작동 가능한 인터페이스의 관리 상태를 표시합니다(↑), 아래쪽(↓) 또는 알 수 없음(?)를 클릭합니다. 구성을 변경하거나 유지 관리 중에 인터페이스의 관리 상태를 제어할 수 있습니다. 관리 상태는 작동 상태와 다를 수 있습니다.

그러나 LIF의 관리 상태가 다운인 경우 기본적으로 운영 상태가 다운됩니다.

IP 주소

인터페이스의 IP 주소를 표시합니다.

역할

인터페이스의 역할을 표시합니다. 가능한 역할은 Cluster-Management LIF, 노드 관리 LIF, 클러스터 LIF, 인터클러스터 LIF입니다.

홈 포트

인터페이스가 원래 연결된 물리적 포트를 표시합니다.

현재 포트

인터페이스가 현재 연결되어 있는 물리적 포트를 표시합니다. LIF 마이그레이션 후 현재 포트가 홈 포트와 다를 수 있습니다.

페일오버 정책

인터페이스에 대해 구성된 페일오버 정책을 표시합니다.

라우팅 그룹

라우팅 그룹의 이름을 표시합니다. 라우팅 그룹 이름을 클릭하여 라우트와 대상 게이트웨이에 대한 자세한 정보를 볼 수 있습니다.

라우팅 그룹은 ONTAP 8.3 이상에서 지원되지 않으므로 이러한 클러스터에 대해 빈 열이 표시됩니다.

페일오버 그룹

페일오버 그룹의 이름을 표시합니다.

노드 탭

선택한 클러스터의 노드에 대한 정보를 표시합니다. HA 쌍, 디스크 쉘프 및 포트에 대한 자세한 정보를 볼 수 있습니다.

HA 세부 정보

HA 쌍의 노드 상태와 상태를 그림으로 보여 줍니다. 노드의 상태는 다음과 같은 색상으로 표시됩니다.

- * 녹색 *

  노드가 작동 상태입니다.

- * 노란색 *

  노드가 파트너 노드를 인수했거나 노드에서 몇 가지 환경 문제를 겪고 있습니다.

- * 적색 *

노드가 다운되었습니다.

HA 쌍의 가용성에 대한 정보를 확인하고 위험을 방지하기 위해 필요한 조치를 취할 수 있습니다. 예를 들어 인수 작업이 가능한 경우 스토리지 페일오버가 가능한이라는 메시지가 표시됩니다.

팬, 전원 공급 장치, NVRAM 배터리, 플래시 카드 등과 같은 HA 쌍 및 해당 환경과 관련된 이벤트 목록을 볼 수 있습니다. 서비스 프로세서 및 디스크 쉘프 연결 이벤트가 트리거된 시간을 볼 수도 있습니다.

모델 번호와 같은 다른 노드 관련 정보를 볼 수 있습니다.

단일 노드 클러스터가 있는 경우 노드에 대한 세부 정보도 볼 수 있습니다.

디스크 쉘프

HA 쌍의 디스크 쉘프에 대한 정보를 표시합니다.

또한 디스크 쉘프 및 환경 구성요소에 대해 생성된 이벤트와 이벤트가 트리거된 시간을 볼 수 있습니다.

- * 쉘프 ID *

  디스크가 있는 쉘프의 ID를 표시합니다.

- * 구성 요소 상태 *

  전원 공급 장치, 팬, 온도 센서, 현재 센서, 디스크 연결 등과 같은 디스크 쉘프의 환경 세부 정보를 표시합니다. 및 전압 센서 환경 세부 정보는 다음과 같은 색상으로 아이콘으로 표시됩니다.

  ◦ * 녹색 *

    환경 구성 요소가 제대로 작동하고 있습니다.

  ◦ * 회색 *

    환경 부품에 사용할 수 있는 데이터가 없습니다.

  ◦ * 적색 *

    일부 환경 구성 요소가 다운되었습니다.

- * 시/도 *

  디스크 쉘프의 상태를 표시합니다. 가능한 상태는 오프라인, 온라인, 상태 없음, 초기화 필요, 누락, 및 알 수 없음.

- * 모델 *

  디스크 쉘프의 모델 번호를 표시합니다.

- * 로컬 디스크 쉘프 *

  디스크 쉘프가 로컬 클러스터에 있는지 또는 원격 클러스터에 있는지 여부를 나타냅니다. 이 열은 MetroCluster 구성의 클러스터에 대해서만 표시됩니다.

- * 고유 ID *

  디스크 쉘프의 고유 식별자를 표시합니다.

- * 펌웨어 버전 *

  디스크 쉘프의 펌웨어 버전을 표시합니다.

포트

연결된 FC, FCoE 및 이더넷 포트에 대한 정보를 표시합니다. 포트 아이콘을 클릭하여 포트 및 관련 LIF에 대한 세부 정보를 볼 수 있습니다.

포트에 대해 생성된 이벤트를 볼 수도 있습니다.

다음 포트 세부 정보를 볼 수 있습니다.

- 포트 ID입니다

  포트의 이름을 표시합니다. 예를 들어 포트 이름은 e0M, e0a 및 e0b일 수 있습니다.

- 역할

  포트의 역할을 표시합니다. 가능한 역할은 Cluster, Data, Intercluster, Node-Management 및 Undefined입니다.

- 유형

  포트에 사용되는 물리 계층 프로토콜을 표시합니다. 가능한 유형은 이더넷, Fibre Channel 및 FCoE입니다.

- WWPN입니다

  포트의 WWPN(World Wide Port Name)을 표시합니다.

- 펌웨어 개정

  FC/FCoE 포트의 펌웨어 버전을 표시합니다.

- 상태

  포트의 현재 상태를 표시합니다. 가능한 상태는 위로, 아래로, 링크가 연결되지 않음 또는 알 수 없음( )를 클릭합니다.

  이벤트 목록에서 포트 관련 이벤트를 볼 수 있습니다. 또한 LIF 이름, 운영 상태, IP 주소 또는 WWPN, 프로토콜, LIF와 연결된 SVM의 이름, 현재 포트, 페일오버 정책 및 페일오버 그룹 등과 같은 관련 LIF 세부 정보를 볼 수 있습니다.

디스크 탭을 클릭합니다

선택한 클러스터의 디스크에 대한 세부 정보를 표시합니다. 사용된 디스크 수, 스페어 디스크, 파손된 디스크 및 할당되지 않은 디스크 수와 같은 디스크 관련 정보를 볼 수 있습니다. 또한 디스크 이름, 디스크 유형 및 디스크의 소유자 노드와 같은 다른 세부 정보를 볼 수도 있습니다.

디스크 풀 요약

유효 유형(FCAL, SAS, SATA, mSATA, SSD, NVMe SSD, SSD 캡, 어레이 LUN 및 VMDISK)와 디스크의 상태를 확인합니다. 애그리게이트 수, 공유 디스크, 스페어 디스크, 파손된 디스크, 할당되지 않은 디스크, 및 지원되지 않는 디스크입니다. 유효한 디스크 유형 개수 링크를 클릭하면 선택한 상태 및 유효 유형의 디스크가 표시됩니다. 예를 들어, 디스크 상태 Broken 및 Effective 유형 SAS에 대한 카운트 링크를 클릭하면 디스크 상태가 Broken 이고 Effective Type SAS인 모든 디스크가 표시됩니다.

디스크

디스크 이름을 표시합니다.

RAID 그룹

RAID 그룹의 이름을 표시합니다.

소유자 노드

디스크가 속한 노드의 이름을 표시합니다. 디스크가 할당되지 않은 경우 이 열에 값이 표시되지 않습니다.

상태

디스크 상태를 표시합니다. Aggregate, Shared, Spare, Broken, Unassigned, 지원되지 않거나 알 수 없습니다. 기본적으로 이 열은 상태를 Broken, Unassigned, Unsupported, Spare, Aggregate, 및 공유 를 클릭합니다.

로컬 디스크

디스크가 로컬 클러스터인지 원격 클러스터인지 여부를 나타내는 예 또는 아니요를 표시합니다. 이 열은 MetroCluster 구성의 클러스터에 대해서만 표시됩니다.

위치

컨테이너 유형(예: 복사, 데이터 또는 패리티)을 기준으로 디스크의 위치를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

영향을 받는 애그리게이트

오류 발생 디스크로 인해 영향을 받는 애그리게이트 수를 표시합니다. 포인터를 개수 링크 위로 이동하여 영향을 받는 애그리게이트를 확인한 다음, 애그리게이트 이름을 클릭하여 애그리게이트의 세부 정보를 확인할 수 있습니다. 또한 애그리게이트 수를 클릭하여 상태: 모든 애그리게이트 보기에서 영향을 받는 애그리게이트 목록을 볼 수도 있습니다.

다음 경우에는 이 열에 값이 표시되지 않습니다.

- 깨진 디스크의 경우 해당 디스크가 포함된 클러스터를 Unified Manager에 추가합니다
- 오류가 발생한 디스크가 없는 경우

스토리지 풀

SSD가 속한 스토리지 풀의 이름을 표시합니다. 스토리지 풀 이름 위로 포인터를 이동하면 스토리지 풀의 세부 정보를 볼 수 있습니다.

저장 가능한 용량

사용 가능한 디스크 용량을 표시합니다.

물리적 용량

올바른 크기 조정 및 RAID 구성 전에 포맷되지 않은 원시 디스크의 용량을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

유형

디스크 유형(예: ATA, SATA, FCAL 또는 VMDISK)을 표시합니다.

유효 유형

ONTAP에서 할당한 디스크 유형을 표시합니다.

특정 ONTAP 디스크 유형은 Aggregate 및 스페어 관리 생성 및 추가 시 이에 상응하는 것으로 간주됩니다. ONTAP는 각 디스크 유형에 대해 유효한 디스크 유형을 할당합니다.

스페어 블록 사용량 **%**

SSD 디스크에서 사용된 스페어 블록의 백분율 표시 SSD 디스크가 아닌 디스크의 경우 이 열은 비어 있습니다.

정격 사용 수명 **%**

실제 SSD 사용량과 제조업체에서 예측한 SSD 수명을 기준으로 사용된 SSD의 예상 사용 시간을 백분율로 표시합니다. 값이 99보다 크면 예상 내구성이 사용되었지만 SSD 장애를 나타내는 것은 아닙니다. 값을 알 수 없으면 디스크가 생략됩니다.

펌웨어

디스크의 펌웨어 버전을 표시합니다.

RPM

디스크의 분당 회전수(RPM)를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

모델

디스크의 모델 번호를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

공급업체

디스크 공급업체의 이름을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

쉘프 **ID**입니다

디스크가 있는 쉘프의 ID를 표시합니다.

베이

디스크가 있는 베이의 ID를 표시합니다.

관련 주석 창

선택한 클러스터와 관련된 주석 세부 정보를 볼 수 있습니다. 세부 정보에는 클러스터에 적용되는 주석 이름 및 주석 값이 포함됩니다. 관련 주석 창에서 수동 주석을 제거할 수도 있습니다.

관련 장치 창

선택한 클러스터와 연결된 장치 세부 정보를 볼 수 있습니다.

세부 정보에는 디바이스 유형, 크기, 개수, 상태 등 클러스터에 연결된 디바이스의 속성이 포함됩니다. 개수 링크를 클릭하면 특정 장치에 대한 추가 분석을 수행할 수 있습니다.

MetroCluster 파트너 창을 사용하여 노드, 애그리게이트, SVM과 같은 관련 클러스터 구성요소와 함께 원격 MetroCluster 파트너에 대한 세부 정보를 확인할 수 있습니다. MetroCluster 파트너 창은 MetroCluster 구성의 클러스터에 대해서만 표시됩니다.

Related Devices 창을 사용하면 클러스터와 관련된 노드, SVM 및 애그리게이트를 확인하고 이동할 수 있습니다.

MetroCluster 파트너

MetroCluster 파트너의 상태를 표시합니다. 개수 링크를 사용하여 더 자세히 탐색하고 클러스터 구성 요소의 상태 및 용량에 대한 정보를 얻을 수 있습니다.

노드

선택한 클러스터에 속한 노드의 수, 용량, 상태를 표시합니다. 용량은 사용 가능한 용량을 초과하는 총 가용 용량을 나타냅니다.

스토리지 가상 머신

선택한 클러스터에 속한 SVM의 수를 표시합니다.

애그리게이트

선택한 클러스터에 속한 애그리게이트의 수, 용량 및 상태 정보가 표시됩니다.

관련 그룹 창

선택한 클러스터를 포함하는 그룹 목록을 볼 수 있습니다.

관련 경고 창

관련 경고 창을 사용하면 선택한 클러스터에 대한 경고 목록을 볼 수 있습니다. 알림 추가 링크를 클릭하여 알림을 추가하거나 알림 이름을 클릭하여 기존 알림을 편집할 수도 있습니다.

- 관련 정보 *

"볼륨 페이지"
"클러스터 목록 및 세부 정보 보기"

Aggregate/Health 세부 정보 페이지를 사용하면 용량, 디스크 정보, 구성 세부 정보 및 생성된 이벤트와 같은 선택한 애그리게이트에 대한 자세한 정보를 볼 수 있습니다. 또한 해당 애그리게이트의 관련 객체 및 관련 알림에 대한 정보도 볼 수 있습니다.

명령 버튼

FabricPool 지원 애그리게이트를 모니터링할 때 이 페이지의 약속된 값과 초과 약속된 값은 로컬 또는 성능 계층 용량에만 관련이 있습니다. 클라우드 계층에서 사용할 수 있는 공간의 양은 초과 커밋된 값에 반영되지 않습니다. 마찬가지로 애그리게이트 임계값은 로컬 성능 계층에만 관련이 있습니다.

명령 버튼을 사용하여 선택한 애그리게이트에 대해 다음 작업을 수행할 수 있습니다.

- * 성능 보기로 전환 *

  집계/성능 세부 정보 페이지로 이동할 수 있습니다.

- * 조치 *
  - 경고 추가

    선택한 애그리게이트에 경고를 추가할 수 있습니다.

  - 임계값 편집

    선택한 애그리게이트의 임계값 설정을 수정할 수 있습니다.

- * 집계 보기 *

  Health:All aggregate 보기로 이동할 수 있습니다.

용량 탭

용량 탭에는 용량, 임계값 및 일일 증가율과 같은 선택한 애그리게이트에 대한 자세한 정보가 표시됩니다.

기본적으로 용량 이벤트는 루트 애그리게이트에 대해 생성되지 않습니다. 또한 Unified Manager에서 사용하는 임계값은 노드 루트 애그리게이트에 적용할 수 없습니다. 기술 지원 담당자만 생성할 이벤트에 대한 설정을 수정할 수 있습니다. 기술 지원 담당자가 설정을 수정할 경우 임계값이 노드 루트 애그리게이트에 적용됩니다.

- * 용량 *

  데이터 용량 그래프 및 스냅샷 복사본 그래프를 표시합니다. 이 그래프에는 애그리게이트에 대한 용량 세부 정보가 표시됩니다.

  - 사용된 논리적 공간입니다

    ONTAP 스토리지 효율성 기술을 사용할 때의 절감 효과를 적용하지 않고 aggregate에 저장되는 데이터의 실제 크기입니다.

  - 사용됨

Aggregate의 데이터에 사용되는 물리적 용량입니다.

◦ 초과 커밋되었습니다

Aggregate의 공간이 초과 커밋되면 차트에 초과 커밋된 금액이 있는 플래그가 표시됩니다.

◦ 경고

경고 임계값이 설정된 위치에 점선이 표시됩니다. 즉, 애그리게이트의 공간이 거의 가득 찼습니다. 이 임계값이 위반되면 Space 거의 가득 참 이벤트가 생성됩니다.

◦ 오류

오류 임계값이 설정된 위치에 실선을 표시합니다. 즉, 애그리게이트의 공간이 가득 찼습니다. 이 임계값이 위반되면 Space Full 이벤트가 생성됩니다.

◦ Snapshot Copies 그래프입니다

이 그래프는 사용된 스냅샷 용량 또는 스냅샷 예약 공간이 0이 아닌 경우에만 표시됩니다.

두 그래프에는 사용된 스냅샷 용량이 스냅샷 예약 용량을 초과하는 경우 스냅샷 용량이 스냅샷 예약 용량을 초과하는 용량이 표시됩니다.

- * 클라우드 계층 *

FabricPool 지원 애그리게이트를 위해 클라우드 계층의 데이터에 사용되는 공간을 표시합니다. FabricPool는 라이센스가 있거나 라이센스가 부여되지 않은 것 중 하나입니다.

클라우드 계층이 다른 클라우드 공급자("미러 계층")로 미러링되면 두 클라우드 계층이 모두 여기에 표시됩니다.

- * 세부 정보 *

용량에 대한 자세한 정보를 표시합니다.

◦ 총 용량

Aggregate의 총 용량을 표시합니다.

◦ 데이터 용량

Aggregate에서 사용하는 공간(사용된 용량)과 Aggregate에서 사용 가능한 공간(사용 가능한 용량)을 표시합니다.

◦ 스냅숏 예비 공간

Aggregate의 사용 중인 스냅샷 용량과 사용 가능한 스냅샷 용량을 표시합니다.

◦ 과도하게 확정된 용량

애그리게이트 구매의사를 표시합니다. 오버커밋 덕분에 해당 스토리지가 현재 사용되고 있지 않는 한 해당 애그리게이트에서 실제로 사용할 수 있는 것보다 더 많은 스토리지를 제공할 수 있습니다. 씬 프로비저닝을 사용 중인 경우 애그리게이트의 총 볼륨 크기가 총 애그리게이트 용량을 초과할 수 있습니다.

Aggregate를 초과 커밋한 경우 사용 가능한 공간을 신중하게 모니터링하고 공간이 부족하여 쓰기 오류가 발생하지 않도록 필요에 따라 스토리지를 추가해야 합니다.

◦ 클라우드 계층

FabricPool 지원 애그리게이트를 위해 클라우드 계층의 데이터에 사용되는 공간을 표시합니다. FabricPool는 라이센스가 있거나 라이센스가 부여되지 않은 것 중 하나입니다. 클라우드 계층이 다른 클라우드 공급자(미러 계층)로 미러링되면 여기에 두 클라우드 계층이 모두 표시됩니다

◦ 총 캐시 공간

Flash Pool 애그리게이트에 추가된 SSD(Solid State Drive) 또는 할당 유닛의 총 공간을 표시합니다. 애그리게이트에 Flash Pool을 사용하도록 설정했지만 SSD를 추가하지 않은 경우 캐시 공간이 0KB로 표시됩니다.

이 필드는 Flash Pool이 Aggregate에 사용되지 않도록 설정된 경우 표시되지 않습니다.

◦ 임계값 집계

다음과 같은 총 용량 임계값을 표시합니다.

- 거의 꽉 참 임계값

  Aggregate가 거의 꽉 찬 비율을 지정합니다.

- 전체 임계값

  Aggregate가 가득 찬 비율을 지정합니다.

- 거의 커밋된 임계값

  Aggregate가 거의 커밋된 비율을 지정합니다.

- 초과 커밋된 임계값

  Aggregate가 초과 커밋되는 비율을 지정합니다.

◦ 기타 세부 정보: 일일 성장률

마지막 두 샘플 간의 변경 비율이 24시간 동안 지속되는 경우 애그리게이트에 사용된 디스크 공간을 표시합니다.

예를 들어, 애그리게이트에서는 오후 2시에 10GB 디스크 공간을 사용하고 오후 6시에 12GB를 사용하는 경우 이 애그리게이트의 일일 증가율(GB)은 2GB입니다.

◦ 볼륨 이동

현재 진행 중인 볼륨 이동 작업의 수를 표시합니다.

- 볼륨 출력

  Aggregate에서 외부로 이동 중인 볼륨의 수와 용량을 표시합니다.

링크를 클릭하면 볼륨 이름, 볼륨이 이동되는 애그리게이트, 볼륨 이동 작업의 상태, 예상 종료 시간 등의 자세한 정보를 볼 수 있습니다.

- 볼륨 in

  aggregate로 이동하는 볼륨의 수와 남은 용량을 표시합니다.

링크를 클릭하면 볼륨 이름, 볼륨이 이동되는 애그리게이트, 볼륨 이동 작업의 상태, 예상 종료 시간 등 자세한 정보를 볼 수 있습니다.

- 볼륨 이동 후 예상되는 사용 용량

  볼륨 이동 작업이 완료된 후 Aggregate에서 사용된 예상 공간(백분율, KB, MB, GB 등)을 표시합니다.

- * 용량 개요 - 볼륨 *

  애그리게이트에 포함된 볼륨의 용량에 대한 정보를 제공하는 그래프를 표시합니다. 볼륨에 사용된 공간(사용된 용량)과 볼륨에서 사용 가능한 공간(사용 가능한 용량)이 표시됩니다. 씬 프로비저닝된 볼륨 공간 위험 이벤트가 씬 프로비저닝된 볼륨에 대해 생성된 경우, 볼륨에서 사용하는 공간(사용된 용량)과 볼륨에서 사용 가능하지만 사용할 수 없는 공간(사용할 수 없는 용량)이 집계 용량 문제로 인해 표시됩니다.

  드롭다운 목록에서 보려는 그래프를 선택할 수 있습니다. 그래프에 표시된 데이터를 정렬하여 사용된 크기, 프로비저닝된 크기, 사용 가능한 용량, 가장 빠른 일일 증가율 및 가장 느린 증가율과 같은 세부 정보를 표시할 수 있습니다. Aggregate에 볼륨이 포함된 SVM(스토리지 가상 머신)을 기준으로 데이터를 필터링할 수 있습니다. 씬 프로비저닝된 볼륨에 대한 세부 정보도 볼 수 있습니다. 커서를 관심 영역 위에 놓으면 그래프에서 특정 지점의 세부 정보를 볼 수 있습니다. 기본적으로 그래프에는 aggregate에서 상위 30개 필터링된 볼륨이 표시됩니다.

디스크 정보 탭

선택한 애그리게이트의 디스크 유형 및 크기, 애그리게이트에 사용되는 디스크 유형을 비롯한 자세한 정보가 표시됩니다. 이 탭에는 RAID 그룹 및 사용된 디스크 유형(예: SAS, ATA, FCAL, SSD 또는 VMDISK)이 그래픽으로 표시됩니다. 패리티 디스크 및 데이터 디스크 위에 커서를 놓으면 디스크 베이, 쉘프 및 회전 속도와 같은 추가 정보를 볼 수 있습니다.

- * 데이터 *

  전용 데이터 디스크, 공유 데이터 디스크 또는 둘 다에 대한 세부 정보를 그래픽으로 표시합니다. 데이터 디스크에 공유 디스크가 포함되어 있으면 공유 디스크의 그래픽 세부 정보가 표시됩니다. 데이터 디스크에 전용 디스크와 공유 디스크가 포함되어 있으면 전용 데이터 디스크와 공유 데이터 디스크의 그래픽 세부 정보가 표시됩니다.

  - * RAID 세부 정보 *

    RAID 세부 정보는 전용 디스크에만 표시됩니다.

    - 유형

      RAID 유형(RAID0, RAID4, RAID-DP 또는 RAID-TEC)을 표시합니다.

    - 그룹 크기

      RAID 그룹에서 허용되는 최대 디스크 수를 표시합니다.

    - 그룹

Aggregate의 RAID 그룹 수를 표시합니다.

◦ * 사용된 디스크 *

▪ 유효 유형

데이터 디스크 유형(예: ATA, SATA, FCAL, SSD, 또는 VMDISK)를 참조하십시오.

▪ 데이터 디스크

애그리게이트에 할당된 데이터 디스크의 수와 용량을 표시합니다. Aggregate에 공유 디스크만 포함되어 있으면 데이터 디스크 세부 정보가 표시되지 않습니다.

▪ 패리티 디스크

애그리게이트에 할당된 패리티 디스크의 수와 용량을 표시합니다. 애그리게이트에 공유 디스크만 포함된 경우 패리티 디스크 세부 정보가 표시되지 않습니다.

▪ 공유 디스크

애그리게이트에 할당된 공유 데이터 디스크의 수와 용량을 표시합니다. 공유 디스크 세부 정보는 Aggregate에 공유 디스크가 포함된 경우에만 표시됩니다.

◦ 스페어 디스크 *

선택한 애그리게이트의 노드에 사용할 수 있는 스페어 데이터 디스크의 디스크 실제 유형, 개수 및 용량을 표시합니다.

파트너 노드로 Aggregate가 페일오버된 경우 Unified Manager는 Aggregate와 호환되는 스페어 디스크를 모두 표시하지 않습니다.

• SSD 캐시 *

전용 캐시 SSD 디스크 및 공유 캐시 SSD 디스크에 대한 자세한 내용은 에 나와 있습니다.

전용 캐시 SSD 디스크에 대한 다음 세부 정보가 표시됩니다.

◦ * RAID 세부 정보 *

▪ 유형

RAID 유형(RAID0, RAID4, RAID-DP 또는 RAID-TEC)을 표시합니다.

▪ 그룹 크기

RAID 그룹에서 허용되는 최대 디스크 수를 표시합니다.

▪ 그룹

Aggregate의 RAID 그룹 수를 표시합니다.

◦ * 사용된 디스크 *

▪ 유효 유형

Aggregate에서 캐시에 사용되는 디스크가 SSD 유형임을 나타냅니다.

- 데이터 디스크

  캐시에 대해 aggregate에 할당된 데이터 디스크의 수와 용량을 표시합니다.

- 패리티 디스크

  캐시에 대해 aggregate에 할당된 패리티 디스크의 수와 용량을 표시합니다.

◦ 스페어 디스크 *

선택한 애그리게이트의 노드에 사용할 수 있는 스페어 디스크의 디스크 실제 유형, 개수 및 용량을 표시합니다.

> 파트너 노드로 Aggregate가 페일오버된 경우 Unified Manager는 Aggregate와 호환되는 스페어 디스크를 모두 표시하지 않습니다.

에서는 공유 캐시에 대해 다음과 같은 세부 정보를 제공합니다.

◦ * 스토리지 풀 *

스토리지 풀의 이름을 표시합니다. 포인터를 스토리지 풀 이름 위로 이동하면 다음 세부 정보를 볼 수 있습니다.

- 상태

  스토리지 풀의 상태를 표시합니다. 이 상태는 정상 상태 또는 정상 상태가 될 수 있습니다.

- 총 할당

  스토리지 풀의 총 할당 유닛 및 크기를 표시합니다.

- 할당 단위 크기

  애그리게이트에 할당될 수 있는 스토리지 풀의 최소 공간을 표시합니다.

- 디스크

  스토리지 풀을 생성하는 데 사용된 디스크 수를 표시합니다. 스토리지 풀 열의 디스크 수와 해당 스토리지 풀의 디스크 정보 탭에 표시된 디스크 수가 일치하지 않으면 하나 이상의 디스크가 손상되고 스토리지 풀이 정상 상태가 아님을 나타냅니다.

- 사용된 할당

  애그리게이트에서 사용하는 할당 유닛의 수와 크기를 표시합니다. 애그리게이트 이름을 클릭하여 애그리게이트 세부 정보를 볼 수 있습니다.

- 사용 가능한 할당

  노드에 사용할 수 있는 할당 유닛의 수와 크기를 표시합니다. 노드 이름을 클릭하여 애그리게이트 세부 정보를 볼 수 있습니다.

◦ * 할당된 캐시 *

Aggregate에서 사용하는 할당 단위의 크기를 표시합니다.

◦ * 할당 단위 *

Aggregate에서 사용하는 할당 단위의 수를 표시합니다.

◦ 디스크 *

스토리지 풀에 포함된 디스크 수를 표시합니다.

◦ * 세부 정보 *

▪ 스토리지 풀

스토리지 풀 수를 표시합니다.

▪ 총 크기

스토리지 풀의 총 크기를 표시합니다.

- * 클라우드 계층 *

FabricPool 지원 애그리게이트를 구성한 경우 클라우드 계층의 이름을 표시하고 사용된 총 공간을 표시합니다. 클라우드 계층이 다른 클라우드 공급자(미러 계층)로 미러링되면 두 클라우드 계층에 대한 세부 정보가 여기에 표시됩니다

Configuration(구성) 탭

구성 탭에는 클러스터 노드, 블록 유형, RAID 유형, RAID 크기, RAID 그룹 개수 등 선택한 애그리게이트에 대한 세부 정보가 표시됩니다.

- * 개요 *

◦ 노드

선택한 Aggregate가 포함된 노드의 이름을 표시합니다.

◦ 블록 유형

애그리게이트의 블록 형식(32비트 또는 64비트)을 표시합니다.

◦ RAID 유형

RAID 유형(RAID0, RAID4, RAID-DP, RAID-TEC 또는 혼합 RAID)을 표시합니다.

◦ RAID 크기

RAID 그룹의 크기를 표시합니다.

◦ RAID 그룹

Aggregate의 RAID 그룹 수를 표시합니다.

◦ SnapLock 유형

Aggregate의 SnapLock Type을 표시합니다.

- * 클라우드 계층 *

FabricPool 지원 애그리게이트인 경우 클라우드 계층에 대한 세부 정보가 표시됩니다. 일부 필드는 스토리지 공급자에 따라 다릅니다. 클라우드 계층이 다른 클라우드 공급자("미러 계층")로 미러링되면 두 클라우드 계층이 모두 여기에 표시됩니다.

◦ 제공합니다

스토리지 공급자의 이름을 표시합니다(예: StorageGRID, Amazon S3, IBM Cloud Object Storage, Microsoft Azure Cloud, Google Cloud Storage 또는 Alibaba Cloud Object Storage).

◦ 이름

ONTAP에서 생성한 클라우드 계층의 이름을 표시합니다.

◦ 서버

클라우드 계층의 FQDN을 표시합니다.

◦ 포트

클라우드 공급자와 통신하는 데 사용되는 포트입니다.

◦ 키 또는 계정에 액세스합니다

클라우드 계층에 대한 액세스 키 또는 계정을 표시합니다.

◦ 컨테이너 이름

클라우드 계층의 버킷 또는 컨테이너 이름을 표시합니다.

◦ SSL

클라우드 계층에 대해 SSL 암호화를 사용할지 여부를 표시합니다.

기록 영역

History 영역에는 선택한 애그리게이트의 용량에 대한 정보를 제공하는 그래프가 표시됩니다. 또한 * 내보내기 * 버튼을 클릭하여 보고 있는 차트에 대한 보고서를 CSV 형식으로 만들 수 있습니다.

기록 창 상단의 드롭다운 목록에서 그래프 유형을 선택할 수 있습니다. 또한 1주, 1개월 또는 1년을 선택하여 특정 기간에 대한 세부 정보를 볼 수도 있습니다. 기록 그래프는 추세를 식별하는 데 도움이 됩니다. 예를 들어 집계 사용량이 거의 가득 찬 임계값을 지속적으로 위반할 경우 적절한 조치를 취할 수 있습니다.

기록 그래프에는 다음 정보가 표시됩니다.

- * 사용된 애그리게이트 용량(%) *

사용 기록을 기준으로 애그리게이트 용량이 사용되는 방식과 세로(y) 축에 대한 선형 그래프(백분율)로

애그리게이트 용량이 사용되는 추세를 표시합니다. 기간은 가로(x) 축에 표시됩니다. 주, 월 또는 연도의 기간을 선택할 수 있습니다. 특정 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다. 적절한 범례를 클릭하여 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, Capacity Used 범례를 클릭하면 Capacity Used 그래프 선이 숨겨집니다.

- * 사용된 애그리게이트 용량과 총 용량 비교 *

  사용 내역과 사용된 용량 및 총 용량을 바이트, 킬로바이트, 메가바이트 단위의 선 그래프로 사용하여 애그리게이트 용량이 사용되는 추세를 표시합니다. 그런 다음 세로(y) 축 위에 있습니다. 기간은 가로(x) 축에 표시됩니다. 주, 월 또는 연도의 기간을 선택할 수 있습니다. 특정 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다. 적절한 범례를 클릭하여 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어, Trend Capacity Used 범례를 클릭하면 Trend Capacity Used 그래프 선이 숨겨집니다.

- * 사용된 애그리게이트 용량(%) vs 커밋된 용량(%) *

  세로(y) 축에서 사용 내역과 커밋된 공간 및 선 그래프를 기준으로 애그리게이트 용량이 사용되는 추세를 백분율로 표시합니다. 기간은 가로(x) 축에 표시됩니다. 주, 월 또는 연도의 기간을 선택할 수 있습니다. 특정 영역 위에 커서를 놓으면 그래프의 특정 지점에 대한 세부 정보를 볼 수 있습니다. 적절한 범례를 클릭하여 선 그래프를 숨기거나 표시할 수 있습니다. 예를 들어 커밋된 공간 범례를 클릭하면 커밋된 공간 그래프 선이 숨겨집니다.

이벤트 목록

이벤트 목록에는 새 이벤트와 승인된 이벤트에 대한 세부 정보가 표시됩니다.

- * 심각도 *

  이벤트의 심각도를 표시합니다.

- * 이벤트 *

  이벤트 이름을 표시합니다.

- * 트리거 시간 *

  이벤트가 생성된 후 경과한 시간을 표시합니다. 경과된 시간이 주를 초과하면 이벤트가 생성된 시점의 타임스탬프가 표시됩니다.

관련 장치 창

Related Devices 창에서는 aggregate와 관련된 클러스터 노드, 볼륨 및 디스크를 볼 수 있습니다.

- * 노드 *

  Aggregate가 포함된 노드의 용량 및 상태를 표시합니다. 용량은 사용 가능한 용량을 초과하는 총 가용 용량을 나타냅니다.

- * 노드 내 애그리게이트 *

  선택한 애그리게이트가 포함된 클러스터 노드의 모든 애그리게이트 수와 용량이 표시됩니다. 최고 심각도 수준에 따라 애그리게이트의 상태도 표시됩니다. 예를 들어, 클러스터 노드에 10개의 애그리게이트가 포함되어 있는 경우 5개의 애그리게이트가 경고 상태를 표시하고 나머지 5개의 애그리게이트는 위험 상태로 표시됩니다.

- 볼륨 *

  애그리게이트에 있는 FlexVol 볼륨 및 FlexGroup 볼륨의 수와 용량을 표시합니다. 이 숫자는 FlexGroup 구성요소를 포함하지 않습니다. 볼륨의 상태 또한 가장 높은 심각도 수준에 따라 표시됩니다.

- * 리소스 풀 *

  Aggregate와 관련된 자원 풀을 표시합니다.

- 디스크 *

  선택한 Aggregate의 디스크 수를 표시합니다.

관련 경고 창

Related Alerts 창에서는 선택한 애그리게이트에 대해 생성된 알림 목록을 볼 수 있습니다. 알림 추가 링크를 클릭하여 알림을 추가하거나 알림 이름을 클릭하여 기존 알림을 편집할 수도 있습니다.

- 관련 정보 *

"스토리지 풀 세부 정보 보기"

데이터 보호 및 복원

보호 관계 생성, 모니터링 및 문제 해결

Unified Manager를 사용하면 보호 관계를 생성하고, 관리 대상 클러스터에 저장된 데이터의 미러 보호 및 백업 소산 보호를 모니터링 및 해결하고, 데이터를 덮어쓰거나 손실된 경우 데이터를 복원할 수 있습니다.

SnapMirror 보호 유형입니다

데이터 스토리지 토폴로지 구축에 따라 Unified Manager를 사용하여 다양한 유형의 SnapMirror 보호 관계를 구성할 수 있습니다. SnapMirror 보호의 모든 변형 기능은 페일오버 재해 복구 보호를 제공하지만 성능, 버전 유연성 및 다중 백업 복사본 보호에 있어 다른 기능을 제공합니다.

기존의 **SnapMirror** 비동기식 보호 관계

기존의 SnapMirror 비동기식 보호 기능은 소스 볼륨과 타겟 볼륨 간의 블록 복제 미러 보호 기능을 제공합니다.

기존 SnapMirror 관계에서는 미러 작업이 블록 복제를 기반으로 하므로 미러 작업이 대체 SnapMirror 관계보다 더 빠르게 실행됩니다. 그러나 기존 SnapMirror 보호에서는 동일한 주요 릴리즈(예: 버전 8.x에서 8.x 또는 9.x에서 9.x)내의 소스 볼륨과 동일한 부 버전 이상의 ONTAP 소프트웨어에서 타겟 볼륨을 실행해야 합니다. 대상이 이전 주 버전을 실행하고 있으므로 9.1 소스에서 9.0 대상으로 복제하는 것은 지원되지 않습니다.

버전에 상관없이 유연하게 복제할 수 있는 **SnapMirror** 비동기식 보호

버전에 상관없이 유연하게 복제할 수 있는 SnapMirror 비동기식 보호 기능은 소스 볼륨과 타겟 볼륨 간에 논리적 복제 미러 보호 기능을 제공합니다. 이는 서로 다른 버전의 ONTAP 8.3.1, 8.3.1에서 9.1, 9.2.2 에서 9.2 등)로 실행 중인 볼륨에서도 마찬가지입니다.

버전에 상관없이 유연하게 복제 가능한 SnapMirror 관계에서는 미러링 작업이 기존 SnapMirror 관계에서와 같이 빠르게 실행되지 않습니다.

느린 실행 속도 때문에 버전에 상관없이 유연하게 복제 보호를 지원하는 SnapMirror는 다음 중 하나를 구현하는 데 적합하지 않습니다.

- 소스 객체에는 보호할 파일이 1,000만 개 이상 있습니다.
- 보호 데이터에 대한 복구 지점 목표는 2시간 이하입니다. 즉, 대상에는 항상 소스의 데이터보다 2시간 이상 오래된 미러링된 복구 가능한 데이터가 포함되어 있어야 합니다.

나열된 상황 중 하나에서 기본 SnapMirror 보호의 신속한 블록 복제 기반 실행이 필요합니다.

버전에 상관없이 유연하게 복제 및 백업 옵션을 사용하는 **SnapMirror** 비동기 보호

버전에 상관없이 유연하게 복제 및 백업 옵션을 사용하는 SnapMirror 비동기 보호 기능은 소스 볼륨과 타겟 볼륨 간의 미러링 보호 기능과 미러링된 데이터의 여러 복사본을 대상에 저장하는 기능을 제공합니다.

스토리지 관리자는 소스에서 타겟으로 미러링되는 스냅샷 복사본을 지정할 수 있으며, 복사본이 소스에서 삭제되더라도 해당 복사본을 대상에서 보존할 기간을 지정할 수도 있습니다.

버전에 상관없이 유연한 복제 및 백업 옵션과 SnapMirror 관계를 사용하면 기존 SnapMirror 관계에서와 같이 미러링 작업이 신속하게 실행되지 않습니다.

SnapMirror 유니파이드 복제**(**미러링 및 소산**)**

SnapMirror 통합 복제를 사용하면 동일한 대상 볼륨에 재해 복구 및 아카이빙을 구성할 수 있습니다. SnapMirror와 마찬가지로 통합 데이터 보호는 처음 호출할 때 기본 전송을 수행합니다. 기본 통합 데이터 보호 정책 ""MirorAndVault""에 따른 기본 전송은 소스 볼륨의 스냅샷 복사본을 만든 다음, 해당 복사본과 데이터 블록이 대상 볼륨에 참조되도록 전송합니다. SnapVault와 마찬가지로, 통합 데이터 보호에도 이전 Snapshot 복사본이 기본 안에 포함되지 않습니다.

SnapMirror Synchronous 보호 및 엄격한 동기화

"사전" 동기화로 SnapMirror Synchronous를 활용하면 1차 볼륨과 2차 볼륨이 항상 서로 진정한 복제본으로 유지됩니다. 보조 볼륨에 데이터를 쓰려고 할 때 복제 실패가 발생하면 운영 볼륨에 대한 클라이언트 입출력이 중단됩니다.

SnapMirror Synchronous 보호 **-** 정기적인 동기화

"리큘러" 동기화를 통한 SnapMirror Synchronous 보호에서는 1차 볼륨과 2차 볼륨이 항상 서로 진정한 복사본일 필요가 없으며, 따라서 1차 볼륨의 가용성이 보장됩니다. 보조 볼륨에 데이터를 쓰려고 할 때 복제 실패가 발생하면 운영 볼륨과 보조 볼륨이 동기화되지 않고 클라이언트 입출력이 운영 볼륨으로 계속됩니다.

상태: 모든 볼륨 보기 또는 볼륨/상태 세부 정보 페이지에서 동기 보호 관계를 모니터링할 때는 복원 단추와 관계 작업 단추를 사용할 수 없습니다.

SnapMirror Synchronous 비즈니스 연속성

ONTAP 9.8 이상에서는 SnapMirror SM-BC(비즈니스 연속성) 기능을 사용할 수 있으며, 이 기능을 사용하여 LUN이 있는 애플리케이션을 보호할 수 있으므로 애플리케이션이 투명하게 페일오버할 수 있으므로 재해 발생 시 비즈니스 연속성을 보장할 수 있습니다.

Unified Manager에서 클러스터 및 스토리지 가상 머신에서 사용 가능한 CG(Consistency Group)를 위한 동기식 SnapMirror 관계를 검색하고 모니터링할 수 있습니다. SM-BC는 AFF 클러스터 또는 모든 ASA(SAN 어레이) 클러스터에서 지원되며, 운영 클러스터와 보조 클러스터는 AFF 또는 ASA가 될 수 있습니다. SM-BC는 iSCSI 또는 FCP LUN을 사용하여 애플리케이션을 보호합니다.

SM-BC 관계에 의해 보호되는 볼륨 및 LUN을 볼 때 보호 관계, 볼륨 인벤토리의 정합성 보장 그룹, 정합성 보장 그룹 관계의 보호 토폴로지 보기, 정합성 보장 그룹 관계에 대한 기간별 데이터 보기 등을 통합적으로 확인할 수 있습니다. 보고서를 다운로드할 수도 있습니다. 또한 정합성 보장 그룹 관계 요약, 정합성 보장 그룹 관계 검색 지원 및 정합성 보장 그룹에 의해 보호되는 볼륨에 대한 정보를 확인할 수 있습니다.

관계 페이지에서 소스 및 대상 스토리지 객체와 정합성 보장 그룹에 의해 보호되는 해당 관계의 보호를 정렬, 필터링 및 확장할 수도 있습니다.

SnapMirror Synchronous 비즈니스 연속성에 대한 자세한 내용은 을 참조하십시오 "SM-BC용 ONTAP 9 문서".

Unified Manager에서 보호 관계 설정

Unified Manager 및 OnCommand Workflow Automation를 사용하여 데이터를 보호하기 위해 SnapMirror 및 SnapVault 관계를 설정하기 위해 수행해야 하는 몇 가지 단계가 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 2개의 클러스터 또는 2개의 SVM(스토리지 가상 머신) 간에 피어 관계를 설정해야 합니다.
- OnCommand Workflow Automation을 Unified Manager와 통합해야 함:
  - "OnCommand Workflow Automation를 설정합니다".
  - "Workflow Automation에서 Unified Manager 데이터 소스 캐싱 검증".

단계

1. 만들려는 보호 관계 유형에 따라 다음 중 하나를 수행합니다.
   - "SnapMirror 보호 관계를 생성합니다".
   - "SnapVault 보호 관계를 생성합니다".
2. 관계에 대한 정책을 만들려면 만드는 관계 유형에 따라 다음 중 하나를 실행합니다.
   - "SnapVault 정책을 생성합니다".
   - "SnapMirror 정책을 생성합니다".
3. "SnapMirror 또는 SnapVault 일정을 생성합니다".

Workflow Automation과 **Unified Manager** 간 연결 구성

WFA(OnCommand Workflow Automation)와 Unified Manager 간에 보안 연결을 구성할 수 있습니다. Workflow Automation에 연결하면 SnapMirror 및 SnapVault 구성 워크플로우와 같은 보호 기능을 사용할 수 있으며 SnapMirror 관계를 관리하는 데 필요한 명령을 사용할 수 있습니다.

- 필요한 것 *
- Workflow Automation의 설치 버전은 5.1 이상이어야 합니다.

  WFA 5.1에는 "'Clustered Data ONTAP를 관리하기 위한 WFA 팩'이 포함되어 있으므로 NetApp Storage Automation Store에서 이 팩을 다운로드하여 이전에 필요한 WFA 서버에 별도로 설치할 필요가 없습니다. "ONTAP 관리를 위한 WFA 팩"
- WFA 및 Unified Manager 연결을 지원하려면 Unified Manager에서 생성한 데이터베이스 사용자의 이름이 있어야 합니다.

  이 데이터베이스 사용자에게 통합 스키마 사용자 역할이 할당되어야 합니다.
- Workflow Automation에서 관리자 역할 또는 설계자 역할을 할당해야 합니다.
- Workflow Automation 설정을 사용하려면 호스트 주소, 포트 번호 443, 사용자 이름 및 암호가 있어야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 일반 * > * Workflow Automation * 을 클릭합니다.
2. Workflow Automation 페이지 * 의 * 데이터베이스 사용자 * 영역에서 이름을 선택하고 Unified Manager 및

Workflow Automation 연결을 지원하기 위해 생성한 데이터베이스 사용자의 암호를 입력합니다.

3. 페이지의 * Workflow Automation Credentials * 영역에서 호스트 이름 또는 IP 주소(IPv4 또는 IPv6)와 Workflow Automation 설정의 사용자 이름 및 암호를 입력합니다.

   Unified Manager 서버 포트(포트 443)를 사용해야 합니다.

4. 저장 * 을 클릭합니다.
5. 자체 서명된 인증서를 사용하는 경우 * 예 * 를 클릭하여 보안 인증서를 승인합니다.

   Workflow Automation 페이지가 표시됩니다.

6. 웹 UI를 다시 로드하고 Workflow Automation 기능을 추가하려면 * 예 * 를 클릭합니다.

◦ 관련 정보 *

"NetApp 설명서: OnCommand Workflow Automation(최신 릴리즈)"

Workflow Automation에서 **Unified Manager** 데이터 소스 캐싱 검증

Workflow Automation에서 데이터 소스 획득이 성공적인지 확인하여 Unified Manager 데이터 소스 캐싱이 제대로 작동하는지 확인할 수 있습니다. Workflow Automation을 Unified Manager와 통합하면 통합 후 Workflow Automation 기능을 사용할 수 있는지 확인할 수 있습니다.

- 필요한 것 *

이 작업을 수행하려면 Workflow Automation에서 관리자 역할 또는 설계자 역할이 할당되어야 합니다.

단계

1. Workflow Automation UI에서 * Execution * > * Data Sources * 를 선택합니다.
2. Unified Manager 데이터 소스의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 * Acquire Now * 를 선택합니다.
3. 취득이 오류 없이 성공하는지 확인합니다.

   Workflow Automation을 Unified Manager와 성공적으로 통합하려면 구입 오류를 해결해야 합니다.

OnCommand Workflow Automation를 재설치하거나 업그레이드하면 어떻게 됩니까

OnCommand Workflow Automation를 재설치하거나 업그레이드하기 전에 OnCommand Workflow Automation와 Unified Manager 간의 연결을 먼저 제거하고 현재 실행 중이거나 예약된 모든 OnCommand Workflow Automation 작업이 중지되었는지 확인해야 합니다.

또한 OnCommand Workflow Automation에서 Unified Manager를 수동으로 삭제해야 합니다.

OnCommand Workflow Automation를 재설치하거나 업그레이드한 후에는 Unified Manager와의 연결을 다시 설정해야 합니다.

Unified Manager에서 **OnCommand Workflow Automation** 설정을 제거하는 중입니다

Workflow Automation을 더 이상 사용하지 않으려는 경우 Unified Manager에서 OnCommand Workflow Automation 설정을 제거할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창의 왼쪽 설정 메뉴에서 * 일반 * > * Workflow Automation * 을 클릭합니다.
2. Workflow Automation * 페이지에서 * 설정 제거 * 를 클릭합니다.

보호 관계 페일오버 및 페일백 수행

하드웨어 장애 또는 재해로 인해 보호 관계의 소스 볼륨이 비활성화되어 있는 경우, Unified Manager의 보호 관계 기능을 사용하여 보호 대상을 읽기/쓰기로 액세스하고 소스가 다시 온라인 상태가 될 때까지 해당 볼륨으로 페일오버할 수 있습니다. 그런 다음 데이터를 제공하는 데 사용할 수 있는 경우 원래 소스로 페일백할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 이 작업을 수행하려면 OnCommand Workflow Automation를 설정해야 합니다.

단계

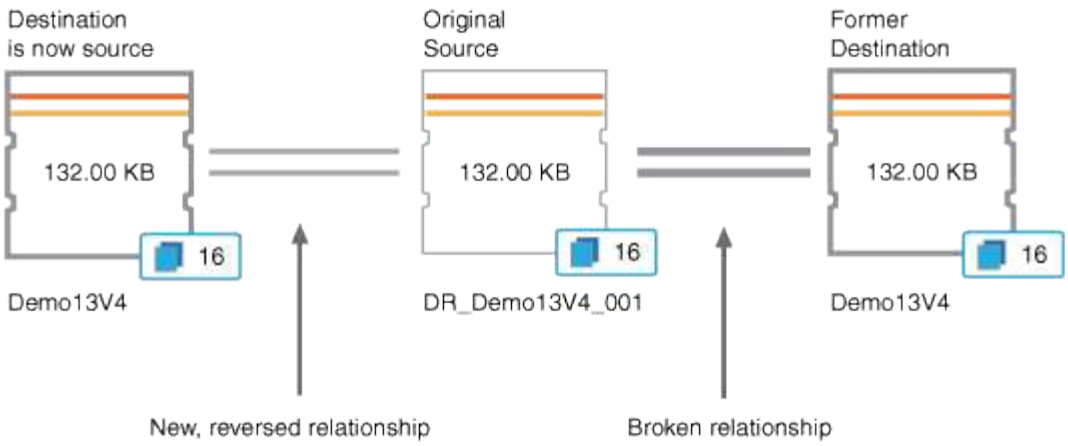
1. "SnapMirror 관계를 발전시킬 수 있습니다".

   대상을 데이터 보호 볼륨에서 읽기/쓰기 볼륨으로 변환하려면 먼저 관계를 끊어야 하며, 그 후에 관계를 반대로 전환해야 합니다.

2. "보호 관계를 반대로 설정합니다".

   원래 소스 볼륨을 다시 사용할 수 있는 경우 소스 볼륨을 복원하여 원래 보호 관계를 다시 설정할 수 있습니다. 소스를 복구하려면 먼저 소스를 이전 대상에 기록된 데이터와 동기화해야 합니다. 역방향 재동기화 작업을 사용하면 원래 관계의 역할을 바꾸고 소스 볼륨을 이전 대상과 동기화하여 새로운 보호 관계를 만들 수 있습니다. 새 관계에 대한 새 기본 스냅샷 복사본이 생성됩니다.

   역관계는 다중 구간 관계와 비슷합니다.



3. "역방향 SnapMirror 관계를 나눕니다".

   원본 소스 볼륨이 재동기화되어 데이터를 다시 제공할 수 있으면 중단 작업을 사용하여 역방향 관계를 끊어 보십시오.

4. "관계를 제거합니다".

   역방향 관계가 더 이상 필요하지 않으면 원래 관계를 다시 설정하기 전에 해당 관계를 제거해야 합니다.

5. "관계를 다시 동기화합니다".

   재동기화 작업을 사용하여 소스에서 대상으로 데이터를 동기화하고 원래 관계를 재설정합니다.

볼륨/상태 세부 정보 페이지에서 **SnapMirror** 관계 분리

볼륨/상태 세부 정보 페이지에서 보호 관계를 유지하고 SnapMirror 관계의 소스 볼륨과 타겟 볼륨 간의 데이터 전송을 중지할 수 있습니다. 데이터를 마이그레이션하거나, 재해 복구 또는 애플리케이션 테스트를 위해 관계를 끊을 수 있습니다. 대상 볼륨이 읽기-쓰기 볼륨으로 변경됩니다. SnapVault 관계를 끊을 수 없습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 분리할 SnapMirror 관계를 선택합니다.
2. 대상을 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 * Break * (휴식 *)를 선택합니다.

   [관계 분리] 대화상자가 표시됩니다.

3. 관계를 해제하려면 * 계속 * 을 클릭합니다.
4. 토폴로지에서 관계가 끊어졌는지 확인합니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 반대로 설정합니다

재해로 인해 보호 관계의 소스 볼륨이 비활성화되면 소스를 복구하거나 교체하는 동안 대상 볼륨을 사용하여 데이터를 읽기/쓰기로 변환하여 제공할 수 있습니다. 소스를 다시 사용하여 데이터를 수신할 수 있으면 역재동기화 작업을 사용하여 역방향의 관계를 설정하여 소스의 데이터를 읽기/쓰기 대상의 데이터와 동기화할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 관계가 SnapVault 관계여야 합니다.
- 보호 관계가 이미 있어야 합니다.
- 보호 관계가 끊어야 합니다.
- 소스와 대상이 모두 온라인 상태여야 합니다.
- 소스가 다른 데이터 보호 볼륨의 대상이 아니어야 합니다.
- 이 작업을 수행하면 공통 스냅샷 복사본의 데이터보다 최신 소스의 데이터가 삭제됩니다.
- 역재동기화 관계에 생성된 정책 및 스케줄은 원래 보호 관계에 있는 정책과 동일합니다.

  정책과 스케줄이 없으면 생성됩니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 소스와 대상을 반대로 이동할 SnapMirror 관계를 찾아 마우스 오른쪽 단추로 클릭합니다.
2. 메뉴에서 * Reverse Resync * 를 선택합니다.

   역방향 재동기화 대화 상자가 표시됩니다.

3. 역방향 재동기화* 대화 상자에 표시된 관계가 역방향 재동기화 작업을 수행할 관계인지 확인한 다음 * 제출 * 을 클릭합니다.

   역방향 재동기화 대화 상자가 닫히고 작업 링크가 볼륨/상태 세부 정보 페이지 맨 위에 표시됩니다.

4. * 선택 사항: * 볼륨/상태 * 세부 정보 페이지에서 * 작업 보기 * 를 클릭하여 각 역방향 재동기화 작업의 상태를 추적합니다.

   필터링된 작업 목록이 표시됩니다.

5. * 선택 사항: * 브라우저의 * 뒤로 * 화살표를 클릭하여 * 볼륨/상태 * 세부 정보 페이지로 돌아갑니다.

   모든 작업 작업이 성공적으로 완료되면 역방향 재동기화 작업이 완료됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 제거합니다

보호 관계를 제거하여 선택한 소스와 대상 간의 기존 관계를 영구적으로 삭제할 수 있습니다. 예를 들어 다른 대상을 사용하여 관계를 만들려는 경우 이 작업은 모든 메타데이터를 제거하므로

실행 취소할 수 없습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 제거할 SnapMirror 관계를 토폴로지 중에서 선택합니다.
2. 대상 이름을 마우스 오른쪽 단추로 클릭하고 메뉴에서 * 제거 * 를 선택합니다.

   관계 제거 대화 상자가 표시됩니다.

3. 관계를 제거하려면 * 계속 * 을 클릭합니다.

   볼륨/상태 세부 정보 페이지에서 관계가 제거됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 재동기화합니다

중단된 SnapMirror 또는 SnapVault 관계의 데이터를 다시 동기화한 다음 소스의 데이터가 대상의 데이터와 일치하도록 대상을 읽기/쓰기로 만들 수 있습니다. 소스 볼륨에서 필요한 공통 스냅샷 복사본이 삭제되어 SnapMirror 또는 SnapVault 업데이트가 실패하는 경우에도 재동기화할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- OnCommand Workflow Automation를 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 재동기화하려는 보호 관계를 토폴로지에서 찾아 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 * 재동기화 * 를 선택합니다.

   또는 * Actions * 메뉴에서 * Relationship * > * ResSynchronize * 를 선택하여 현재 세부 정보를 보고 있는 관계를 다시 동기화합니다.

   재동기화 대화 상자가 표시됩니다.

3. 재동기화 옵션 * 탭에서 전송 우선 순위 및 최대 전송 속도를 선택합니다.
4. 소스 스냅샷 복사본 * 을 클릭한 다음 * 스냅샷 복사본 * 열에서 * 기본값 * 을 클릭합니다.

   소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

5. 기본 스냅샷 복사본을 전송하지 않고 기존 스냅샷 복사본을 지정하려면 * 기존 스냅샷 복사본 * 을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
6. 제출 * 을 클릭합니다.

재동기화 대화 상자로 돌아갑니다.

7. 재동기화할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정할 다음 소스에 대해 * 기본값 * 을 클릭합니다.
8. Submit * 을 클릭하여 재동기화 작업을 시작합니다.

   재동기화 작업이 시작되고 볼륨/상태 세부 정보 페이지로 돌아가며 페이지 상단에 작업 링크가 표시됩니다.

9. * 선택 사항: * 볼륨/상태 세부 정보 * 페이지에서 * 작업 보기 * 를 클릭하여 각 재동기화 작업의 상태를 추적합니다.

   필터링된 작업 목록이 표시됩니다.

10. * 선택 사항: * 브라우저의 * 뒤로 * 화살표를 클릭하여 * 볼륨/상태 * 세부 정보 페이지로 돌아갑니다.

    모든 작업 작업이 성공적으로 완료되면 재동기화 작업이 완료됩니다.

보호 작업 실패 해결

이 워크플로우에서는 Unified Manager 대시보드에서 보호 작업 장애를 식별하고 해결하는 방법의 예를 제공합니다.

- 필요한 것 *

이 워크플로의 일부 작업에서는 관리자 역할을 사용하여 로그인해야 하므로 다양한 기능을 사용하는 데 필요한 역할에 익숙해야 합니다.

이 시나리오에서는 대시보드 페이지에 액세스하여 보호 작업에 문제가 있는지 확인합니다. 보호 인시던트 영역에서 볼륨에 보호 작업 실패 오류가 표시된 작업이 종료됨 인시던트가 있음을 알 수 있습니다. 이 오류를 조사하여 가능한 원인과 가능한 해결 방법을 결정합니다.

단계

1. Dashboard Unresolved Incidents and Risks 영역의 Protection Incidents 패널에서 * Protection job failed * 이벤트를 클릭합니다.

   이벤트에 연결된 텍스트는 "cluster2_src_svm:/cluster2_src_vol2 - 보호 작업 실패"와 같은 "object_name:/object_name - Error Name" 형식으로 기록됩니다.

   실패한 보호 작업에 대한 이벤트 세부 정보 페이지가 표시됩니다.

2. 요약 * 영역의 원인 필드에 있는 오류 메시지를 검토하여 문제를 확인하고 가능한 수정 조치를 평가합니다.

   을 참조하십시오 "문제 식별 및 실패한 보호 작업에 대한 수정 조치 수행".

문제 식별 및 실패한 보호 작업에 대한 수정 조치 수행

이벤트 세부 정보 페이지의 원인 필드에서 작업 실패 오류 메시지를 검토하고 스냅샷 복사본 오류로 인해 작업이 실패했는지 확인합니다. 그런 다음 볼륨/상태 세부 정보 페이지로 이동하여 추가 정보를 수집합니다.

• 필요한 것 *

애플리케이션 관리자 역할이 있어야 합니다.

이벤트 세부 정보 페이지의 원인 필드에 제공된 오류 메시지에는 실패한 작업에 대한 다음 텍스트가 포함되어 있습니다.

```
Protection Job Failed. Reason: (Transfer operation for
relationship 'cluster2_src_svm:cluster2_src_vol2->cluster3_dst_svm:
managed_svc2_vol3' ended unsuccessfully. Last error reported by
Data ONTAP: Failed to create Snapshot copy 0426cluster2_src_vol2snap
on volume cluster2_src_svm:cluster2_src_vol2. (CSM: An operation
failed due to an ONC RPC failure.)
Job Details
```

이 메시지는 다음 정보를 제공합니다.

- 백업 또는 미러 작업이 성공적으로 완료되지 않았습니다.

  이 작업에는 가상 서버 'cluster2_src_svm'의 소스 볼륨 'cluster2_src_vol2'와 가상 서버 'cluster3_dst_svm'의 대상 볼륨 'managed_svc2_vol3'의 보호 관계가 포함되었습니다.

- 소스 볼륨 'cluster2_src_svm:/cluster2_src_vol2'의 0426cluster2_src_vol2snap 스냅샷 복사 작업이 실패했습니다.

이 시나리오에서는 작업 실패의 원인 및 잠재적 시정 조치를 식별할 수 있습니다. 그러나 장애를 해결하려면 System Manager 웹 UI 또는 ONTAP CLI 명령에 액세스해야 합니다.

단계

1. 오류 메시지를 검토하고 소스 볼륨에서 스냅샷 복사본 작업이 실패했는지 확인하여 소스 볼륨에 문제가 있을 수 있음을 나타냅니다.

   선택적으로 오류 메시지 끝에 있는 * 작업 세부 정보 * 링크를 클릭할 수 있지만 이 시나리오의 목적상 그렇게 하지 않도록 선택할 수 있습니다.

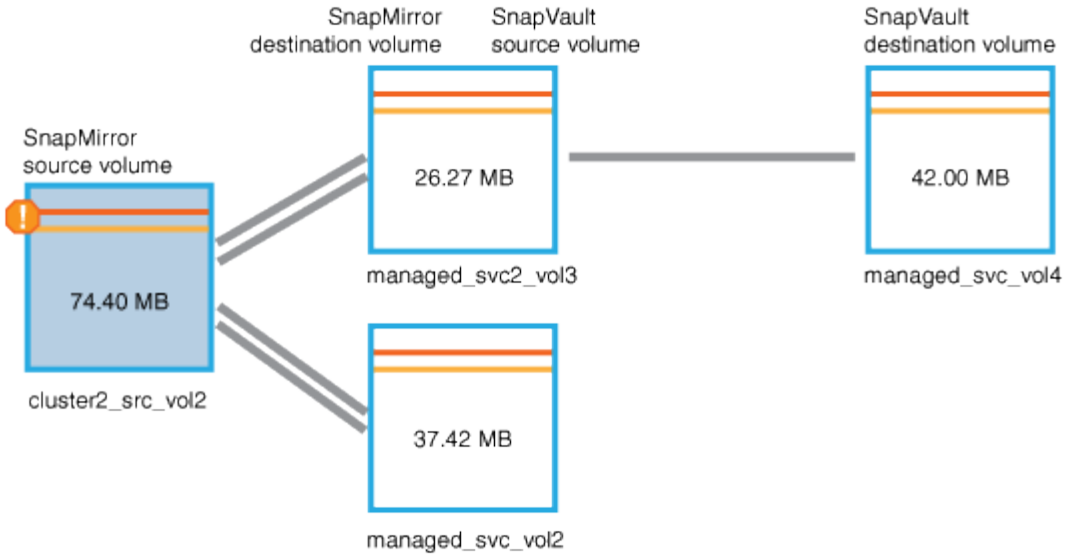
2. 이벤트 해결을 시도하기로 결정했으므로 다음을 수행합니다.
   a. 할당 대상 * 버튼을 클릭하고 메뉴에서 * Me * 를 선택합니다.
   b. 이벤트에 대한 경고가 설정된 경우 반복 알림 알림을 계속 수신하지 않도록 * 확인 * 버튼을 클릭합니다.
   c. 필요에 따라 이벤트에 대한 메모를 추가할 수도 있습니다.
3. 소스 볼륨에 대한 세부 정보를 보려면 * 요약 * 창에서 * 소스 * 필드를 클릭합니다.

   소스 * 필드에는 소스 객체의 이름이 들어 있습니다. 이 경우 스냅샷 복사본 작업이 예약된 볼륨입니다.

   'cluster2_src_vol2'에 대한 볼륨/상태 세부 정보 페이지가 표시되고 보호 탭의 내용이 표시됩니다.

4. 보호 토폴로지 그래프를 보면 토폴로지의 첫 번째 볼륨과 연관된 오류 아이콘이 표시됩니다. 이 아이콘은 SnapMirror 관계의 소스 볼륨입니다.

   소스 볼륨 아이콘에는 해당 볼륨에 대해 설정된 경고 및 오류 임계값을 나타내는 가로 막바도 있습니다.



5. 오류 아이콘 위에 커서를 놓으면 임계값 설정이 표시되고 볼륨이 용량 문제를 나타내는 오류 임계값을 초과했음을 확인하는 팝업 대화 상자가 표시됩니다.
6. 용량 * 탭을 클릭합니다.

   볼륨 'cluster2_src_vol2'에 대한 용량 정보가 표시됩니다.

7. 용량 * 패널에서 막대 그래프에 오류 아이콘이 표시됩니다. 이는 볼륨 용량이 볼륨에 설정된 임계값 수준을 초과했음을 나타냅니다.
8. 용량 그래프 아래에 볼륨 자동 확장 기능이 비활성화되어 있고 볼륨 공간 보장이 설정되어 있는 것을 볼 수 있습니다.

   자동 증가를 사용하도록 설정할 수 있지만 이 시나리오의 목적상 용량 문제를 해결하는 방법을 결정하기 전에 추가 조사를 하기로 결정합니다.

9. 아래로 스크롤하여 * 이벤트 * 목록으로 이동하여 보호 작업 실패, 전체 시점까지의 볼륨 일수 및 볼륨 공간 전체 이벤트가 생성되었는지 확인합니다.
10. Events* 목록에서 * Volume Space Full* 이벤트를 클릭하여 자세한 정보를 확인하고 이 이벤트가 용량 문제와 가장 관련이 있는 것으로 판단했습니다.

    이벤트 세부 정보 페이지에는 소스 볼륨의 볼륨 공간 가득 참 이벤트가 표시됩니다.

11. Summary * (요약 *) 영역에서 이벤트의 Cause 필드를 읽습니다. "90%로 설정된 전체 임계값이 위반됩니다. 47.50MB 중 45.38MB(95.54%)가 사용됩니다.
12. 요약 영역 아래에 권장 시정 조치가 표시됩니다.

    제안된 시정 조치는 일부 이벤트에 대해서만 표시되므로 모든 유형의 이벤트에 대해 이 영역이 표시되지 않습니다.

    볼륨 공간 가득 참 이벤트를 해결하기 위해 수행할 수 있는 권장 조치 목록을 클릭합니다.

    - 이 볼륨에 대해 자동 확장 기능을 활성화합니다.
    - 볼륨 크기를 조정합니다.
    - 이 볼륨에서 중복 제거를 설정하고 실행합니다.

◦ 이 볼륨에 대해 압축을 활성화하고 실행합니다.

13. 볼륨에 대해 자동 확장을 활성화하기로 결정했지만, 그렇게 하려면 상위 애그리게이트에 사용 가능한 공간과 현재 볼륨 증가율을 확인해야 합니다.

    a. Related Devices * 창에서 부모 집합인 cluster2_src_aggr1을 확인합니다.

    Aggregate의 이름을 클릭하면 Aggregate에 대한 자세한 정보를 볼 수 있습니다.

    Aggregate에 볼륨 자동 증가를 활성화할 수 있는 충분한 공간이 있는지 확인합니다.

    b. 페이지 상단에서 중요 인시던트를 나타내는 아이콘을 확인하고 아이콘 아래에 있는 텍스트를 검토합니다.

    "Days to Full: less than a day | Daily Growth Rate: 5.4%"를 결정합니다.

14. 시스템 관리자로 이동하거나 ONTAP CLI에 액세스하여 '볼륨 자동 확장' 옵션을 활성화하십시오.

    자동 확장 기능을 설정할 때 사용할 수 있도록 볼륨 및 애그리게이트 이름을 기록해 둡니다.

15. 용량 문제를 해결한 후 Unified Manager * Event * 세부 정보 페이지로 돌아가 이벤트를 '해결됨'으로 표시합니다.

지연 문제 해결

이 워크플로에서는 지연 문제를 해결하는 방법의 예를 제공합니다. 이 시나리오에서는 Unified ManagerDashboard 페이지에 액세스하는 관리자 또는 운영자로, 보호 관계에 문제가 있는지, 그리고 문제가 있는 경우 솔루션을 찾아야 합니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

대시보드 페이지에서는 해결되지 않은 인시던트 및 위험 영역을 살펴보고 보호 위험 아래의 보호 창에서 SnapMirror 지연 오류를 확인할 수 있습니다.

단계

1. 대시보드 * 페이지의 * 보호 * 창에서 SnapMirror 관계 지연 오류를 찾아 클릭합니다.

   LAG ERROR 이벤트에 대한 이벤트 세부 정보 페이지가 표시됩니다.

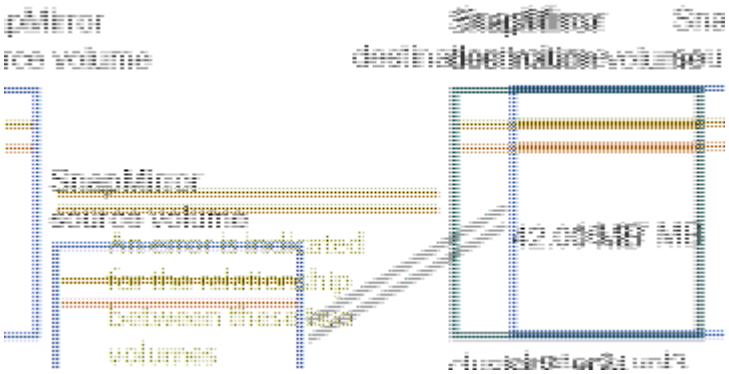
2. 이벤트 * 세부 정보 페이지에서 다음 작업 중 하나 이상을 수행할 수 있습니다.
   - Summary(요약) 영역의 Cause(원인) 필드에 있는 오류 메시지를 검토하여 제안된 수정 조치가 있는지 확인합니다.
   - 볼륨에 대한 세부 정보를 보려면 Summary(요약) 영역의 Source(소스) 필드에서 객체 이름(이 경우 볼륨)을 클릭합니다.
   - 이 이벤트에 대해 추가되었을 수 있는 참고 사항을 찾습니다.
   - 이벤트에 메모를 추가합니다.
   - 특정 사용자에게 이벤트를 할당합니다.
   - 이벤트를 확인하거나 해결합니다.

3. 이 시나리오에서는 * Summary * (요약 *) 영역의 Source (소스) 필드에서 객체 이름(이 경우 볼륨)을 클릭하여 볼륨에 대한 세부 정보를 확인할 수 있습니다.

   볼륨/상태 세부 정보 페이지의 보호 탭이 표시됩니다.

4. Protection * 탭에서 토폴로지 다이어그램을 살펴봅니다.

   지연 오류가 있는 볼륨은 3볼륨 SnapMirror 계단식 볼륨의 마지막 볼륨입니다. 선택한 볼륨의 윤곽선이 진한 회색으로 표시되고 소스 볼륨의 이중 주황색 선은 SnapMirror 관계 오류를 나타냅니다.



5. SnapMirror 캐스케이드의 각 볼륨을 클릭합니다.

   각 볼륨을 선택할 때 요약, 토폴로지, 기록, 이벤트, 관련 장치의 보호 정보 및 관련 경고 영역이 변경되어 선택한 볼륨과 관련된 세부 정보가 표시됩니다.

6. Summary * (요약 *) 영역을 보고 각 볼륨의 * Update Schedule * (업데이트 일정 *) 필드에 있는 정보 아이콘 위에 커서를 놓습니다.

   이 시나리오에서는 SnapMirror 정책이 DPDefault로, SnapMirror 일정은 시간 5분 후에 매시간 업데이트됩니다. 관계의 모든 볼륨이 동시에 SnapMirror 전송을 완료하려고 한다는 것을 알고 있습니다.

7. 지연 문제를 해결하기 위해 각 대상이 전송을 완료한 후 SnapMirror 전송을 시작할 수 있도록 다중 구간 볼륨 중 두 개에 대한 일정을 수정합니다.

보호 관계 관리 및 모니터링

Active IQ Unified Manager를 사용하면 보호 관계를 생성하고, 관리 대상 클러스터에서 SnapMirror 및 SnapVault 관계를 모니터링 및 해결하며, 데이터를 덮어쓰거나 손실할 때 데이터를 복원할 수 있습니다.

SnapMirror 작업의 경우 두 가지 복제 유형이 있습니다.

- 비동기식

  운영 볼륨에서 보조 볼륨으로의 복제는 스케줄에 따라 결정됩니다.

- 동기식이다

  복제는 운영 볼륨과 2차 볼륨에서 동시에 수행됩니다.

성능에 영향을 주지 않고 최대 10개의 보호 작업을 동시에 수행할 수 있습니다. 11 ~ 30개의 작업을 동시에 실행할 경우 성능에 약간의 영향을 줄 수 있습니다. 30개 이상의 작업을 동시에 실행하는 것은 권장되지 않습니다.

볼륨 보호 상태 보기

데이터 보호 페이지는 단일 클러스터의 모든 보호된 볼륨 또는 데이터 센터의 모든 클러스터에 대한 데이터 보호 세부 정보에 대한 종합적인 뷰를 제공합니다.

단계

1. 왼쪽 탐색 창에서 * 대시보드 * 를 클릭합니다.
2. 모니터링되는 모든 클러스터에 대한 데이터 보호 상태를 볼 것인지 또는 단일 클러스터에 대한 데이터 보호 상태를 볼 것인지 여부에 따라 * All Clusters * 를 선택하거나 드롭다운 메뉴에서 단일 클러스터를 선택합니다.
3. Data Protection 패널 상단의 오른쪽 화살표를 클릭합니다. 데이터 보호 * 페이지가 표시됩니다.

데이터 센터에서 단일 또는 모든 클러스터를 선택했는지 여부에 따라 이 페이지는 스냅샷 복사본 또는 SnapMirror 정책으로 보호되는 볼륨의 데이터 보호 상태를 표시하고 보호되지 않은 볼륨의 수도 표시합니다.

개별 클러스터 * 목록에서 클러스터를 선택하면 해당 클러스터에 있는 보호된 볼륨의 스냅샷 보호 및 SnapMirror 관계 상태가 표시됩니다.

이 페이지에서 이벤트를 클릭하면 이벤트 세부 정보 페이지로 이동합니다. 이벤트 관리 인벤토리 페이지에서 * 모두 보기 * 링크를 클릭하여 모든 활성 보호 이벤트를 볼 수 있습니다. 마우스를 가져가면 해당 개수와 범례를 볼 수 있습니다. 다음을 클릭할 수 있습니다.

- 보호되지 않는 볼륨 및 스냅샷 복사본으로 보호되는 볼륨에 대한 막대 차트를 볼륨 페이지로 이동하여 세부 정보를 확인합니다.
- 모든 관계에 대한 막대 차트는 원본 클러스터를 기준으로 세부 정보가 필터링되는 관계 페이지로 이동합니다.

스냅샷 복사본으로 보호되는 볼륨의 보호 상태를 봅니다

- Snapshot 복사본 개요 *: 다음과 같이 Snapshot 복사본으로 보호되는 볼륨에 대한 개요:
- Snapshot 복사본으로 보호되고 보호되지 않는 총 볼륨 수입니다.
- 스냅샷 복사본을 위해 예약 공간을 사용 중이거나 초과하는 총 볼륨 수입니다.
- Snapshot 복사본 분석 * 은 다음 정보를 자세히 설명합니다.
- 지난 24시간 동안 발생한 이벤트를 비롯하여 스냅샷 복사본에 대한 개별 이벤트입니다.
- 스냅샷 복사본으로 보호되고 보호되지 않는 볼륨에 대한 자세한 차트
- 예약된 스냅샷 복사본 용량을 사용, 사용하지 않음 및 위반한 볼륨
- 스냅샷 복사본 수를 기준으로 볼륨 수를 세분합니다.

Snapshot 복사본에 대해 메모할 사항입니다

- 스냅샷 복사본으로 보호되는 볼륨을 계산할 때는 소스 볼륨과 타겟 볼륨을 모두 고려합니다.
- 반환되는 스냅샷 복사본 수는 온라인 상태이고 사용 가능한 볼륨에 대해서만 제공됩니다.
- 스냅샷 복사본 수에 대한 그래프 범위는 동적입니다. 선택한 클러스터에 있는 스냅샷 수에 따라 생성됩니다.
- 볼륨을 보호됨 으로 고려하려면 볼륨의 스냅샷 복사본에 대한 일정을 설정해야 합니다.

- 스냅샷 복사본을 위한 예약 공간 값은 사용된 디스크 공간의 양을 확인하거나 하나 이상의 스냅샷 복사본이 삭제된 경우 재확보된 공간을 계산할 때 중요합니다.

SnapMirror 관계의 보호 상태를 봅니다

- SnapMirror 개요 *: 다음과 같이 SnapMirror 정책으로 보호되는 볼륨에 대한 개요:
- 볼륨 SnapMirror 관계, 스토리지 VM 재해 복구(SVM-DR), 조합 등 각 SnapMirror 정책으로 보호되는 볼륨 수
- 지연 상태에 따라 RPO(복구 시점 목표) 지연을 경험한 SnapMirror 관계의 총 수
- SnapMirror 분석 * 은 다음 정보를 자세히 설명합니다.
- 지난 24시간 동안 발생한 이벤트를 포함하여 SnapMirror 관계에 대해 발생한 개별 이벤트입니다
- 각 유형의 SnapMirror 정책으로 보호되는 볼륨 수입니다.
- 비동기 미러, 비동기 볼트, 비동기 MirrorVault, StricxtSync, SMBC(SnapMirror Business Continuity) 일관성 그룹 및 동기화와 같이 SnapMirror 관계 유형으로 보호되는 관계 수입니다.
- 건강하고 비정상적인 관계의 수.
- 볼륨 관계 카운트의 분할입니다. RPO 지연 시간 및 상태를 기준으로 차트를 전환할 수 있습니다.
- 관리되지 않는 관계에 대한 지연 임계값입니다. 설정 아이콘( )을 클릭하여 지연 임계값 설정을 구성합니다. 자세한 내용은 을 참조하십시오 "관리되지 않는 보호 관계에 대한 지연 임계값 설정 구성".

SnapMirror 관계에 대한 참고 사항을 나타냅니다

- SnapMirror 관계를 계산할 때는 읽기 및 쓰기가 가능한 소스 볼륨이 계산됩니다. 대상 및 루트 볼륨은 고려되지 않습니다.
- SnapMirror 관계의 경우 소스 클러스터에 대한 이벤트가 표시됩니다.
- SnapMirror 관계 개수에는 동일한 클러스터 또는 서로 다른 클러스터에 있는 소스 및 대상이 있는 볼륨 수가 포함됩니다.
- 데이터 복제에서 RPO 지연의 지연 시간은 SnapMirror 관계를 기준으로 합니다. 이 상태는 관계 임계치 설정에 따라 ok, warning, error로 분류된다. 상태를 보고 매개 변수가 예상대로 작동하는지 또는 문제를 해결해야 하는지 여부를 확인할 수 있습니다.
- 볼륨에 여러 SnapMirror 관계가 있는 경우 각 관계 유형이 RPO 지연에 대해 계산됩니다.
- 예를 들어, 관계가 끊어진 경우와 같이 소스와 대상 간의 데이터 복제 문제가 있는 경우 볼륨 관계는 좋지 않은 것으로 간주됩니다.

MetroCluster 구성으로 보호되는 클러스터 보기

데이터 보호 * 페이지의 * MetroCluster 보호 * 패널에는 사이트의 FC 또는 IP 구성을 통해 MetroCluster에 의해 보호되거나 보호되지 않는 클러스터의 수가 표시됩니다. 이 패널에서 막대 차트를 클릭하면 클러스터 페이지로 이동합니다. 클러스터 세부 정보는 보호되거나 보호되지 않는 클러스터를 기준으로 필터링됩니다. MetroCluster 구성 모니터링에 대한 자세한 내용은 을 참조하십시오 "MetroCluster 구성 모니터링".

볼륨 보호 관계 보기

관계: 모든 관계 보기 및 볼륨 관계 페이지에서 기존 볼륨 SnapMirror 및 SnapVault 관계의 상태를 볼 수 있습니다. 전송 및 지연 상태, 소스 및 대상 세부 정보, 스케줄 및 정책 정보 등의

보호 관계에 대한 세부 정보를 검토할 수도 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

이 페이지에서 관계 명령을 시작할 수도 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 모든 관계 * 를 선택합니다.

   관계: 모든 관계 보기가 표시됩니다.

3. 다음 방법 중 하나를 선택하여 볼륨 보호 세부 정보를 봅니다.

   ◦ 모든 볼륨 관계에 대한 현재 정보를 보려면 기본 * 모든 관계 * 페이지에 그대로 둡니다.

   ◦ 일정 기간 동안의 볼륨 전송 추세에 대한 자세한 정보를 보려면 보기 메뉴에서 관계: 최근 1개월 전송 상태 보기를 선택합니다.

   ◦ 볼륨 전송 활동에 대한 자세한 정보를 일 단위로 보려면 보기 메뉴에서 관계: 최근 1개월 전송 속도 보기를 선택합니다.

볼륨 전송 보기에는 비동기 관계의 볼륨에 대한 정보만 표시되며, 동기 관계의 볼륨은 표시되지 않습니다.

정합성 보장 그룹 관계에서 **LUN** 모니터링

ONTAP 환경에서 LUN을 사용하여 애플리케이션을 보호하기 위해 SM-BC(SnapMirror 비즈니스 연속성)를 지원하는 경우 Active IQ Unified Manager에서 해당 LUN을 보고 모니터링할 수 있습니다.

SM-BC는 SAN 환경의 페일오버 중에 RTO(복구 시간 목표)를 0으로 보장합니다. SM-BC를 지원하는 일반적인 구축 환경에서는 볼륨의 LUN이 정합성 보장 그룹 관계에 의해 보호됩니다.

이러한 운영 LUN과 보조 LUN은 복합 LUN이거나 UUID와 일련 번호가 같은 복제본 LUN 쌍입니다. 입출력 작업(읽기 및 쓰기 모두)은 이러한 복합 LUN의 소스 및 대상 사이트에서 멀티플렉싱되므로 투명성이 보장됩니다.

복합 LUN을 보려면 정합성 보장 그룹 관계의 일부인 LUN이 포함된 운영 클러스터와 보조 클러스터를 Unified Manager에서 추가하고 검색해야 합니다. iSCSI 및 FCP LUN만 지원됩니다.

SM-BC에 대한 자세한 내용은 를 참조하십시오 "SM-BC용 ONTAP 9 문서".

환경에서 복합 LUN을 보려면 다음 단계를 수행하십시오.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * LUN * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 모든 LUN * 을 선택합니다.

관계: 모든 LUN 보기가 표시됩니다.

LUN 이름, 볼륨, LUN을 호스팅하는 스토리지 VM, 클러스터, 일관성 그룹 및 파트너 LUN과 같은 LUN 세부 정보를 볼 수 있습니다. 각 구성 요소를 클릭하여 세부 보기로 드릴다운할 수 있습니다. 정합성 보장 그룹을 클릭하면 관계 페이지로 이동합니다.

파트너 LUN을 클릭하면 파트너 LUN이 호스팅되는 스토리지 VM에 대한 스토리지 VM 세부 정보 페이지의 SAN 탭에서 구성 세부 정보를 볼 수 있습니다. 이니시에이터, 이니시에이터 그룹 등의 정보와 파트너 LUN의 다른 측면이 표시됩니다.

사용자 환경에서 보호된 LUN에 대한 보고서를 정렬, 필터링, 생성 및 업로드하는 표준 그리드 레벨 기능을 수행할 수 있습니다.

상태**:** 모든 볼륨 보기에서 **SnapVault** 보호 관계 생성

상태: 모든 볼륨 보기를 사용하여 보호 목적으로 데이터 백업을 사용하도록 동일한 스토리지 VM에 있는 하나 이상의 볼륨에 대한 SnapVault 관계를 생성할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

다음과 같은 경우에는 * Protect * 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 상태: 모든 볼륨 * 보기에서 보호할 볼륨을 선택하고 * 보호 * 를 클릭합니다.

   또는 동일한 SVM(스토리지 가상 시스템)에서 여러 보호 관계를 생성하려면 Health:All Volumes(상태:모든 볼륨) 보기에서 하나 이상의 볼륨을 선택하고 도구 모음에서 * Protect * 를 클릭합니다.

3. 메뉴에서 * SnapVault * 를 선택합니다.

   보호 구성 대화 상자가 시작됩니다.

4. SnapVault * 를 클릭하여 * SnapVault * 탭을 보고 보조 볼륨 정보를 구성합니다.
5. 고급 * 을 클릭하여 필요에 따라 중복제거, 압축, 자동 확장, 공간 보장을 설정하고 * 적용 * 을 클릭합니다.
6. SnapVault* 탭의 * 대상 정보 * 영역과 * 관계 설정 * 영역을 입력합니다.
7. 적용 * 을 클릭합니다.

   Health:All Volumes 보기로 돌아갑니다.

8. 상태: 모든 볼륨 * 보기 상단에 있는 보호 구성 작업 링크를 클릭합니다.

   보호 관계를 하나만 생성하는 경우에는 작업 세부 정보 페이지가 표시되지만 둘 이상의 보호 관계를 생성하는

경우에는 보호 작업과 관련된 모든 작업의 필터링된 목록이 표시됩니다.

9. 다음 중 하나를 수행합니다.
   - 작업이 하나뿐인 경우 * 새로 고침 * 을 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 결정합니다.
   - 작업이 두 개 이상인 경우:
     i. 작업 목록에서 작업을 클릭합니다.
     ii. 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 확인하려면 * 새로 고침 * 을 클릭합니다.
     iii. 필터링된 목록으로 돌아가 다른 작업을 보려면 * 뒤로 * 버튼을 사용합니다.

볼륨/상태 세부 정보 페이지에서 **SnapVault** 보호 관계 생성

볼륨/상태 세부 정보 페이지를 사용하여 SnapVault 관계를 생성하면 볼륨에서 데이터 백업을 보호할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 이 작업을 수행하려면 Workflow Automation을 설정해야 합니다.

다음과 같은 경우에는 * Protect * 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 보호할 토폴로지 뷰의 볼륨을 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 * Protect * > * SnapVault * 를 선택합니다.

   보호 구성 대화 상자가 시작됩니다.

3. SnapVault * 를 클릭하여 * SnapVault * 탭을 보고 보조 리소스 정보를 구성합니다.
4. 고급 * 을 클릭하여 필요에 따라 중복제거, 압축, 자동 확장, 공간 보장을 설정하고 * 적용 * 을 클릭합니다.
5. 보호 구성 * 대화 상자에서 * 대상 정보 * 영역과 * 관계 설정 * 영역을 완료합니다.
6. 적용 * 을 클릭합니다.

   볼륨/상태 세부 정보 페이지로 돌아갑니다.

7. 볼륨/상태 * 세부 정보 페이지 상단의 보호 구성 작업 링크를 클릭합니다.

   작업 세부 정보 페이지가 표시됩니다.

8. 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 확인하려면 * 새로 고침 * 을 클릭합니다.

작업 작업이 완료되면 볼륨/상태 세부 정보 페이지 토폴로지 뷰에 새 관계가 표시됩니다.

상태**:** 모든 볼륨 보기에서 **SnapMirror** 보호 관계 생성

상태: 모든 볼륨 보기를 사용하면 동일한 스토리지 VM에서 둘 이상의 볼륨을 선택하여 여러 SnapMirror 보호 관계를 한 번에 생성할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

다음과 같은 경우에는 * Protect * 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

단계

1. 상태: 모든 볼륨 * 보기에서 보호할 볼륨을 선택합니다.

   또는 동일한 SVM에서 여러 보호 관계를 생성하려면 Health:All Volumes 보기에서 하나 이상의 볼륨을 선택하고 도구 모음에서 * Protect * > * SnapMirror * 를 클릭합니다.

   보호 구성 대화 상자가 표시됩니다.

2. SnapMirror * 탭을 보고 대상 정보를 구성하려면 * SnapMirror * 를 클릭합니다.
3. 필요에 따라 * 고급 * 을 클릭하여 공간 보장을 설정한 다음 * 적용 * 을 클릭합니다.
4. SnapMirror * 탭에서 * 대상 정보 * 영역과 * 관계 설정 * 영역을 완료합니다.
5. 적용 * 을 클릭합니다.

   Health:All Volumes 보기로 돌아갑니다.

6. 상태: 모든 볼륨 보기 * 의 맨 위에 있는 보호 구성 작업 링크를 클릭합니다.

   보호 관계를 하나만 생성하는 경우 작업 세부 정보 페이지가 표시되지만 둘 이상의 보호 관계를 생성하는 경우 보호 작업과 관련된 모든 작업 목록이 표시됩니다.

7. 다음 중 하나를 수행합니다.
   - 작업이 하나뿐인 경우 * 새로 고침 * 을 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 결정합니다.
   - 작업이 두 개 이상인 경우:
     i. 작업 목록에서 작업을 클릭합니다.
     ii. 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 확인하려면 * 새로 고침 * 을 클릭합니다.
     iii. 필터링된 목록으로 돌아가 다른 작업을 보려면 * 뒤로 * 버튼을 사용합니다.

구성 중에 지정한 대상 SVM에 따라, 고급 설정에서 지정한 옵션에 따라 SnapMirror 관계가 달라질 수 있습니다.

- 소스 볼륨과 동일한 버전 또는 최신 버전의 ONTAP에서 실행되는 타겟 SVM을 지정한 경우 블록 복제 기반 SnapMirror 관계가 기본 결과입니다.
- 소스 볼륨과 동일한 버전 또는 최신 버전의 ONTAP에서 실행되는 타겟 SVM을 지정했지만 고급 설정에서 버전에 상관없이 유연한 복제를 사용하도록 설정한 경우 유연한 복제를 사용하는 SnapMirror 관계가 됩니다.
- 이전 버전의 ONTAP에서 소스 볼륨의 SVM보다 실행되는 타겟 SVM을 지정하고 이전 버전에서 버전에 상관없이 유연한 복제를 지원하는 경우, 버전에 상관없이 유연한 복제를 사용하는 SnapMirror 관계가 자동으로 이루어집니다.

볼륨/상태 세부 정보 페이지에서 **SnapMirror** 보호 관계 생성

볼륨/상태 세부 정보 페이지를 사용하여 보호 목적으로 데이터 복제를 사용하도록 SnapMirror 관계를 만들 수 있습니다. SnapMirror 복제를 사용하면 소스의 데이터 손실 발생 시 대상 볼륨에서 데이터를 복원할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

다음과 같은 경우에는 * Protect * 메뉴가 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

성능에 영향을 주지 않고 최대 10개의 보호 작업을 동시에 수행할 수 있습니다. 11 ~ 30개의 작업을 동시에 실행할 경우 성능에 약간의 영향을 줄 수 있습니다. 30개 이상의 작업을 동시에 실행하는 것은 권장되지 않습니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 탭 * 에서 보호할 볼륨의 이름을 마우스 오른쪽 단추로 클릭합니다.
2. 메뉴에서 * 보호 * > * SnapMirror * 를 선택합니다.

   보호 구성 대화 상자가 표시됩니다.

3. SnapMirror * 탭을 보고 대상 정보를 구성하려면 * SnapMirror * 를 클릭합니다.
4. 필요에 따라 * 고급 * 을 클릭하여 공간 보장을 설정한 다음 * 적용 * 을 클릭합니다.
5. 보호 구성 * 대화 상자에서 * 대상 정보 * 영역과 * 관계 설정 * 영역을 완료합니다.
6. 적용 * 을 클릭합니다.

   볼륨/상태 세부 정보 페이지로 돌아갑니다.

7. 볼륨/상태 * 세부 정보 페이지 상단의 보호 구성 작업 링크를 클릭합니다.

   작업의 작업 및 세부 정보가 작업 세부 정보 페이지에 표시됩니다.

8. Job * details 페이지에서 * Refresh * 를 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업 완료 시기를 결정합니다.

9. 작업 작업이 완료되면 브라우저에서 * Back * 을 클릭하여 * Volume/Health * 세부 정보 페이지로 돌아갑니다.

   새 관계가 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

구성 중에 지정한 대상 SVM에 따라, 고급 설정에서 지정한 옵션에 따라 SnapMirror 관계가 달라질 수 있습니다.

- 소스 볼륨과 동일한 버전 또는 최신 버전의 ONTAP에서 실행되는 타겟 SVM을 지정한 경우 블록 복제 기반 SnapMirror 관계가 기본 결과입니다.
- 소스 볼륨과 동일한 버전 또는 최신 버전의 ONTAP에서 실행되는 타겟 SVM을 지정했지만 고급 설정에서 버전에 상관없이 유연한 복제를 사용하도록 설정한 경우 유연한 복제를 사용하는 SnapMirror 관계가 됩니다.
- 이전 버전의 ONTAP에서 실행되는 대상 SVM이나 이전 버전의 소스 볼륨보다 더 높은 버전을 사용하여 유연한 복제를 지원하는 경우에는 버전에 상관없이 유연한 복제를 사용하는 SnapMirror 관계가 자동으로 이루어집니다.

버전에 상관없이 유연하게 복제 가능한 **SnapMirror** 관계 생성

버전에 상관없이 유연하게 복제할 수 있는 SnapMirror 관계를 구축할 수 있습니다. 버전에 상관없이 유연하게 복제를 수행하면 소스 볼륨과 타겟 볼륨이 서로 다른 버전의 ONTAP에서 실행되는 경우에도 SnapMirror 보호를 구현할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 소스 및 타겟 SVM에는 각각 SnapMirror 라이센스가 활성화되어 있어야 합니다.
- 버전에 상관없이 유연하게 복제를 지원하는 ONTAP 소프트웨어 버전에서 소스 및 타겟 SVM을 각각 실행해야 합니다.

버전에 상관없이 복제 가능한 SnapMirror를 사용하면 모든 스토리지가 ONTAP의 단일 버전에서 실행되는 것이 아닌 이기종 스토리지 환경에서도 SnapMirror 보호를 구현할 수 있습니다. 하지만 버전에 상관없이 유연한 복제를 통해 SnapMirror에서 수행되는 미러링 작업은 기존 블록 복제 SnapMirror와 마찬가지로 빠르게 실행되지 않습니다.

단계

1. 보호할 볼륨에 대한 * 보호 구성 * 대화 상자를 표시합니다.
   - 볼륨/상태 세부 정보 페이지의 보호 탭을 보고 있는 경우 보호할 볼륨 이름이 있는 토폴로지 뷰를 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 * 보호 * > * SnapMirror * 를 선택합니다.
   - 상태: 모든 볼륨 보기를 보고 있는 경우 보호할 볼륨을 찾아 마우스 오른쪽 단추로 클릭한 다음 메뉴에서 * 보호 * > * SnapMirror * 를 선택합니다. 보호 구성 대화 상자가 표시됩니다.
2. SnapMirror * 탭을 보려면 * SnapMirror * 를 클릭하십시오.
3. 보호 구성 * 대화 상자에서 * 대상 정보 * 영역과 * 관계 설정 * 영역을 완료합니다.

   보호할 소스 볼륨보다 이전 버전의 ONTAP에서 실행되는 타겟 SVM을 지정하고 이전 버전에서 유연한 복제를 지원하는 경우 이 작업은 버전에 상관없이 유연한 복제를 통해 SnapMirror를 자동으로 구성합니다.

4. 소스 볼륨과 동일한 버전의 ONTAP에서 실행되는 타겟 SVM을 지정했지만 버전에 상관없이 유연한 복제로 SnapMirror를 구성하려면 * 고급 * 을 클릭하여 버전에 상관없이 복제를 활성화한 다음 * 적용 * 을 클릭합니다.
5. 적용 * 을 클릭합니다.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

6. 볼륨/상태 * 세부 정보 페이지 상단의 보호 구성 작업 링크를 클릭합니다.

   작업 태스크 및 세부 정보가 작업 세부 정보 페이지에 표시됩니다.

7. Job * details 페이지에서 * Refresh * 를 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업 완료 시기를 결정합니다.
8. 작업 작업이 완료되면 브라우저에서 * Back * 을 클릭하여 * Volume/Health * 세부 정보 페이지로 돌아갑니다.

   새 관계가 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

버전에 상관없이 유연하게 복제 가능한 백업 옵션을 사용하여 **SnapMirror** 관계 생성

버전에 상관없이 유연한 복제 및 백업 옵션 기능을 통해 SnapMirror 관계를 구축할 수 있습니다. 백업 옵션 기능을 사용하면 SnapMirror 보호를 구현하고 여러 버전의 백업 복사본을 대상 위치에 유지할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 소스 및 타겟 SVM에는 각각 SnapMirror 라이센스가 활성화되어 있어야 합니다.
- 소스 및 타겟 SVM에는 각각 SnapVault 라이센스가 활성화되어 있어야 합니다.
- 버전에 상관없이 유연하게 복제를 지원하는 ONTAP 소프트웨어 버전에서 소스 및 타겟 SVM을 각각 실행해야 합니다.

백업 옵션 기능을 사용하여 SnapMirror를 구성하면 볼륨 장애 조치 기능과 같은 SnapMirror 재해 복구 기능을 통해 데이터를 보호할 수 있으며 동시에 다중 백업 복사본 보호와 같은 SnapVault 기능을 제공할 수 있습니다.

단계

1. 보호할 볼륨에 대한 * 보호 구성 * 대화 상자를 표시합니다.
   - 볼륨/상태 세부 정보 페이지의 보호 탭을 보고 있는 경우, 보호할 볼륨의 이름을 토폴로지 뷰에서 마우스 오른쪽 버튼으로 클릭하고 메뉴에서 * 보호 * > * SnapMirror * 를 선택합니다.
   - 상태: 모든 볼륨 보기를 보고 있는 경우 보호할 볼륨을 찾아 마우스 오른쪽 단추로 클릭한 다음 메뉴에서 * 보호 * > * SnapMirror * 를 선택합니다. 보호 구성 대화 상자가 표시됩니다.
2. SnapMirror * 탭을 보려면 * SnapMirror * 를 클릭하십시오.
3. 보호 구성 * 대화 상자에서 * 대상 정보 * 영역과 * 관계 설정 * 영역을 완료합니다.
4. 고급 * 을 클릭하여 * 고급 대상 설정 * 대화 상자를 표시합니다.
5. 버전에 상관없이 복제 * 확인란을 아직 선택하지 않은 경우 지금 선택합니다.
6. 백업 옵션 기능을 활성화하려면 * with backup option * 확인란을 선택하고 * Apply * 를 클릭합니다.
7. 적용 * 을 클릭합니다.

   볼륨/상태 세부 정보 페이지로 돌아갑니다.

8. 볼륨/상태 * 세부 정보 페이지 상단의 보호 구성 작업 링크를 클릭합니다.

   작업 태스크 및 세부 정보가 작업 세부 정보 페이지에 표시됩니다.

9. Job * details 페이지에서 * Refresh * 를 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업 완료 시기를 결정합니다.
10. 작업 작업이 완료되면 브라우저에서 * Back * 을 클릭하여 * Volume/Health * 세부 정보 페이지로 돌아갑니다.

    새 관계가 볼륨/상태 세부 정보 페이지 토폴로지 보기에 표시됩니다.

대상 효율성 설정을 구성하는 중입니다

고급 대상 설정 대화 상자를 사용하여 보호 대상에서 중복제거, 압축, 자동 확장, 공간 보장과 같은 대상 효율성 설정을 구성할 수 있습니다. 대상 또는 보조 볼륨에서 공간 활용률을 최대화하려는 경우 이러한 설정을 사용합니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

기본적으로 효율성 설정은 소스 볼륨의 압축 설정과 일치하며 SnapVault 관계의 압축 설정은 기본적으로 비활성화되어 있습니다.

단계

1. 구성 중인 관계 유형에 따라 * 보호 구성 * 대화 상자에서 * SnapMirror * 탭 또는 * SnapVault * 탭을 클릭합니다.
2. Destination Information * 영역에서 * Advanced * 를 클릭합니다.

   고급 대상 설정 대화 상자가 열립니다.

3. 필요에 따라 중복제거, 압축, 자동 확장 및 공간 보장에 대한 효율성 설정을 사용하거나 사용하지 않도록 설정합니다.
4. 선택 사항을 저장하고 * 보호 구성 * 대화 상자로 돌아가려면 * 적용 * 을 클릭합니다.

SnapMirror 및 **SnapVault** 일정 생성

기본 또는 고급 SnapMirror 및 SnapVault 일정을 생성하여 데이터 변경 빈도에 따라 소스 또는 기본 볼륨에서 자동 데이터 보호 전송을 가능하게 할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료해야 합니다.
- 이 작업을 수행하려면 Workflow Automation을 설정해야 합니다.

단계

1. 보호 구성 * 대화 상자의 * SnapMirror * 탭 또는 * SnapVault * 탭에서 * 관계 설정 * 영역에서 * 일정 생성 * 링크를 클릭합니다.

   Create Schedule 대화상자가 표시됩니다.

2. [일정 이름] * 필드에 일정에 부여할 이름을 입력합니다.
3. 다음 중 하나를 선택합니다.
   - * 기본 *

     기본 간격 스타일 일정을 만들려면 선택합니다.

   - * 고급 *

     cron 스타일 일정을 만들려면 선택합니다.
4. Create * 를 클릭합니다.

   새 일정이 SnapMirror 일정 또는 SnapVault 일정 드롭다운 목록에 표시됩니다.

계단식 또는 팬아웃 관계를 생성하여 기존 보호 관계로부터 보호를 확장합니다

소스 볼륨에서 팬아웃 또는 기존 관계의 대상 볼륨에서 캐스케이드하여 기존 관계로부터 보호를 확장할 수 있습니다. 한 사이트에서 여러 사이트로 데이터를 복사하거나 더 많은 백업을 만들어 추가 보호 기능을 제공해야 하는 경우 이 작업을 수행할 수 있습니다.

모든 볼륨을 하나의 엔터티로 관리할 수 있도록 여러 볼륨을 포함하는 컨테이너인 일관성 그룹을 사용하여 보호 기능을 볼륨으로 확장할 수 있습니다. Unified Manager의 관계 페이지에서 SM-BC(SnapMirror Business Continuity) 일관성 그룹과 동기식 정합성 보장 그룹 관계를 볼 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 보호 * > * 관계 * 를 클릭합니다. 또는 볼륨 세부 정보 페이지에서 관계를 볼 수도 있습니다.
2. 볼륨 관계 * 페이지에서 보호를 확장할 SnapMirror 관계를 선택합니다.
3. 작업 표시줄에서 * 보호 확장 * 을 클릭합니다.
4. 소스에서 팬아웃 관계를 생성하는지 또는 대상에서 캐스케이드 관계를 생성하는지에 따라 메뉴에서 소스 * 또는 대상에서 * 를 선택합니다.
5. 생성하는 보호 관계 유형에 따라 SnapMirror * 또는 * with SnapVault * 를 선택합니다.

   보호 구성 * 대화 상자가 표시됩니다.

   이는 통합 관계/볼륨 관계 및 볼륨/상태 세부 정보 페이지에서 수행할 수 있습니다.
6. 보호 구성 * 대화 상자에 표시된 정보를 입력합니다.

볼륨 관계 페이지에서 보호 관계 편집

기존 보호 관계를 편집하여 최대 전송 속도, 보호 정책 또는 보호 스케줄을 변경할 수 있습니다.

관계를 편집하여 전송에 사용되는 대역폭을 줄이거나 데이터가 자주 변경되므로 예약된 전송 빈도를 늘릴 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

선택한 볼륨은 보호 관계 대상이어야 합니다. 소스 볼륨, 로드 공유 볼륨 또는 SnapMirror 또는 SnapVault 관계의 대상이 아닌 볼륨을 선택한 경우에는 관계를 편집할 수 없습니다.

단계

1. 볼륨 관계 * 페이지의 볼륨 목록에서 관계 설정을 편집할 동일한 SVM에 있는 하나 이상의 볼륨을 선택한 다음 도구 모음에서 * 편집 * 을 선택합니다.

   관계 편집 대화 상자가 표시됩니다.

2. [관계 편집] * 대화 상자에서 필요에 따라 최대 전송 속도, 보호 정책 또는 보호 일정을 편집합니다.
3. 적용 * 을 클릭합니다.

   변경 내용이 선택한 관계에 적용됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계 편집

기존 보호 관계를 편집하여 현재 최대 전송 속도, 보호 정책 또는 보호 스케줄을 변경할 수 있습니다. 관계를 편집하여 전송에 사용되는 대역폭을 줄이거나 데이터가 자주 변경되므로 예약된 전송 빈도를 늘릴 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설치하고 구성해야 합니다.

선택한 볼륨은 보호 관계 대상이어야 합니다. 소스 볼륨, 로드 공유 볼륨 또는 SnapMirror 또는 SnapVault 관계의 대상이 아닌 볼륨을 선택한 경우에는 관계를 편집할 수 없습니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 편집할 보호 관계를 토폴로지에서 찾아 마우스 오른쪽 버튼으로 클릭합니다.
2. 메뉴에서 * 편집 * 을 선택합니다.

   또는 * Actions * 메뉴에서 * Relationship * > * Edit * 를 선택하여 현재 세부 정보를 보고 있는 관계를 편집합니다.

   관계 편집 * 대화 상자가 표시됩니다.

3. 관계 편집 대화 상자에서 필요에 따라 최대 전송 속도, 보호 정책 또는 보호 스케줄을 편집합니다.
4. 적용 * 을 클릭합니다.

   변경 내용이 선택한 관계에 적용됩니다.

전송 효율성을 최대화할 수 있도록 **SnapMirror** 정책 생성

SnapMirror 정책을 생성하여 보호 관계에 대한 SnapMirror 전송 우선순위를 지정할 수 있습니다. SnapMirror 정책을 사용하면 우선 순위를 지정하여 소스에서 대상으로 전송 효율성을 극대화할 수 있으므로 우선순위가 낮은 전송이 일반 우선 순위 전송 후에 실행되도록 예약할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 이 작업에서는 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료한 것으로 가정합니다.

단계

1. 보호 구성 * 대화 상자의 * SnapMirror * 탭에서 * 관계 설정 * 영역의 * 정책 생성 * 링크를 클릭합니다.

   SnapMirror 정책 생성 대화 상자가 표시됩니다.

2. Policy Name * 필드에 정책을 지정할 이름을 입력합니다.
3. Transfer Priority * 필드에서 정책에 할당할 전송 우선 순위를 선택합니다.
4. Comment * (주석 *) 필드에 정책에 대한 선택적 설명을 입력합니다.
5. Create * 를 클릭합니다.

   새 정책이 SnapMirror 정책 드롭다운 목록에 표시됩니다.

전송 효율성을 극대화하기 위한 **SnapVault** 정책 생성

새 SnapVault 정책을 생성하여 SnapVault 전송의 우선 순위를 설정할 수 있습니다. 보호 관계에서 정책을 사용하여 운영 스토리지에서 2차 스토리지로 전송 효율성을 극대화할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 보호 구성 대화 상자에서 대상 정보 영역을 이미 완료해야 합니다.

단계

1. 보호 구성 * 대화 상자의 * SnapVault * 탭에서 * 관계 설정 * 영역의 * 정책 * 만들기 * 링크를 클릭합니다.

   SnapVault(측정) 탭이 표시됩니다.

2. Policy Name * 필드에 정책을 지정할 이름을 입력합니다.
3. 전송 우선순위 * 필드에서 정책에 할당할 전송 우선순위를 선택합니다.
4. * 선택 사항: * 설명 * 필드에 정책에 대한 설명을 입력합니다.

5. Replication Label * 영역에서 필요에 따라 복제 레이블을 추가하거나 편집합니다.
6. Create * 를 클릭합니다.

   새 정책이 정책 생성 드롭다운 목록에 표시됩니다.

볼륨 관계 페이지에서 활성 데이터 보호 전송을 중단합니다

진행 중인 SnapMirror 복제를 중지하려는 경우 활성 데이터 보호 전송을 중단할 수 있습니다. 기본 전송 이후에 전송을 위해 재시작 체크포인트를 지울 수도 있습니다. 볼륨 이동 같은 다른 작업과 충돌하는 경우 전송을 중단할 수 있습니다.

정합성 보장 그룹에 의해 보호되는 볼륨 관계는 중단할 수 없습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

중단 작업은 다음 경우에 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

기본 전송에 대해 재시작 체크포인트를 지울 수 없습니다.

단계

1. 하나 이상의 보호 관계에 대한 전송을 중단하려면 * 볼륨 관계 * 페이지에서 하나 이상의 볼륨을 선택하고 도구 모음에서 * 중단 * 을 클릭합니다.

   전송 중단 대화 상자가 표시됩니다.

2. 기본 전송이 아닌 전송에 대해 재시작 체크포인트를 지우려면 * 체크포인트 지우기 * 를 선택합니다.
3. 계속 * 을 클릭합니다.

   전송 중단 대화 상자가 닫히고 중단 작업의 상태가 작업 세부 정보에 대한 링크와 함께 볼륨 관계 페이지 맨 위에 표시됩니다.

4. * 선택 사항: * 세부 정보 보기 * 링크를 클릭하여 * 작업 * 세부 정보 페이지로 이동하여 자세한 내용을 확인하고 작업 진행 상황을 확인하십시오.

볼륨/상태 세부 정보 페이지에서 활성 데이터 보호 전송을 중단합니다

진행 중인 SnapMirror 복제를 중지하려는 경우 활성 데이터 보호 전송을 중단할 수 있습니다. 기본 전송이 아닌 경우 전송에 대한 재시작 체크포인트를 지울 수도 있습니다. 볼륨 이동 같은 다른 작업과 충돌하는 경우 전송을 중단할 수 있습니다.

정합성 보장 그룹에 의해 보호되는 볼륨 관계는 중단할 수 없습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

중단 작업은 다음 경우에 표시되지 않습니다.

- RBAC 설정에서 이 작업을 허용하지 않는 경우(예: 운영자 권한만 있는 경우
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

기본 전송에 대해 재시작 체크포인트를 지울 수 없습니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 중단하려는 데이터 전송에 대한 토폴로지 뷰의 관계를 마우스 오른쪽 버튼으로 클릭하고 * 중단 * 을 선택합니다.

   전송 중단 대화 상자가 표시됩니다.

2. 기본 전송이 아닌 전송에 대해 재시작 체크포인트를 지우려면 * 체크포인트 지우기 * 를 선택합니다.
3. 계속 * 을 클릭합니다.

   전송 중단 대화 상자가 닫히고 중단 작업의 상태가 작업 세부 정보에 대한 링크와 함께 볼륨/상태 세부 정보 페이지 맨 위에 표시됩니다.

4. * 선택 사항: * 세부 정보 보기 * 링크를 클릭하여 * 작업 * 세부 정보 페이지로 이동하여 자세한 내용을 확인하고 작업 진행 상황을 확인하십시오.
5. 각 작업 작업을 클릭하여 세부 정보를 봅니다.
6. 브라우저의 뒤로 화살표를 클릭하여 * 볼륨/상태 * 세부 정보 페이지로 돌아갑니다.

   모든 작업 작업이 성공적으로 완료되면 중단 작업이 완료됩니다.

볼륨 관계 페이지에서 보호 관계를 중지합니다

볼륨 관계 페이지에서 보호 관계를 중지하여 데이터 전송이 일시적으로 발생하지 않도록 할 수 있습니다. 데이터베이스가 포함된 SnapMirror 대상 볼륨의 스냅샷 복사본을 생성하려는 경우 관계를 중단시키고 스냅샷 복사본 작업 중에 해당 볼륨의 콘텐츠가 안정적으로 유지되도록 할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

다음 경우에는 일시 중지 작업이 표시되지 않습니다.

- RBAC 설정에 따라 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우
- 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우

- Workflow Automation 및 Unified Manager를 페어링하지 않은 경우

단계

1. 하나 이상의 보호 관계에 대한 전송을 중지하려면 * 볼륨 관계 * 페이지에서 하나 이상의 볼륨을 선택하고 도구 모음에서 * 정지 * 를 클릭합니다.

   정지 대화 상자가 표시됩니다.

2. 계속 * 을 클릭합니다.

   일시 중지 작업의 상태는 볼륨/상태 세부 정보 페이지 맨 위에 작업 세부 정보에 대한 링크와 함께 표시됩니다.

3. 자세한 내용 및 작업 진행 상황을 보려면 * 상세 정보 보기 * 링크를 클릭하여 * 작업 * 상세 정보 페이지로 이동하십시오.
4. * 선택 사항: * 브라우저의 * 뒤로 * 화살표를 클릭하여 * 볼륨 관계 * 페이지로 돌아갑니다.

   모든 작업 작업이 성공적으로 완료되면 중지 작업이 완료됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 중지합니다

보호 관계를 일시 중지하여 데이터 전송이 발생하지 않도록 할 수 있습니다. 데이터베이스가 포함된 SnapMirror 대상 볼륨의 스냅샷 복사본을 생성하려는 경우 관계를 중단시키고 스냅샷 복사본 중에 해당 볼륨의 콘텐츠가 안정적으로 유지되도록 할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

다음 경우에는 일시 중지 작업이 표시되지 않습니다.

- RBAC 설정에 따라 이 작업이 허용되지 않는 경우(예: 운영자 권한만 있는 경우
- 예를 들어, 볼륨 ID를 알 수 없는 경우(예: 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우
- Workflow Automation 및 Unified Manager를 페어링하지 않은 경우

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 중지하려는 보호 관계에 대한 토폴로지 보기의 관계를 마우스 오른쪽 단추로 클릭합니다.
2. 메뉴에서 * 정지 * 를 선택합니다.
3. 계속하려면 * 예 * 를 클릭하십시오.

   일시 중지 작업의 상태는 볼륨/상태 세부 정보 페이지 맨 위에 작업 세부 정보에 대한 링크와 함께 표시됩니다.

4. 자세한 내용 및 작업 진행 상황을 보려면 * 상세 정보 보기 * 링크를 클릭하여 * 작업 * 상세 정보 페이지로 이동하십시오.
5. * 선택 사항: * 브라우저의 뒤로 화살표를 클릭하여 * 볼륨/상태 * 세부 정보 페이지로 돌아갑니다.

모든 작업 작업이 성공적으로 완료되면 중지 작업이 완료됩니다.

볼륨 관계 페이지에서 **SnapMirror** 관계 분리

SnapMirror 관계의 소스 볼륨과 타겟 볼륨 간의 데이터 전송을 중지하려면 보호 관계를 중단할 수 있습니다. 데이터를 마이그레이션하거나, 재해 복구 또는 애플리케이션 테스트를 위해 관계를 끊을 수 있습니다. 대상 볼륨이 읽기/쓰기 볼륨으로 변경됩니다. SnapVault 관계를 끊을 수 없습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨 관계 * 페이지에서 데이터 전송을 중지할 보호 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 * 중단 * 을 클릭합니다.

   [관계 분리] 대화상자가 표시됩니다.

2. 관계를 해제하려면 * 계속 * 을 클릭합니다.
3. 볼륨 관계 * 페이지에서 * 관계 상태 * 열에서 관계가 끊어져 있는지 확인합니다.

   관계 상태 열은 기본적으로 숨겨져 있으므로 열 표시/숨기기 목록에서 선택해야 할 수 있습니다 .

볼륨 관계 페이지에서 보호 관계를 제거합니다

볼륨 관계 페이지에서 보호 관계를 제거하여 선택한 소스와 대상 간의 기존 관계를 영구적으로 삭제할 수 있습니다. 예를 들어 다른 대상을 사용하여 관계를 만들려는 경우 이 작업은 모든 메타데이터를 제거하므로 실행 취소할 수 없습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨 관계 * 페이지에서 제거할 보호 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 * 제거 * 를 클릭합니다.

   관계 제거 대화 상자가 표시됩니다.

2. 관계를 제거하려면 * 계속 * 을 클릭합니다.

   볼륨 관계 페이지에서 관계가 제거됩니다.

볼륨 관계 페이지에서 중지된 관계에서 예약된 전송을 다시 시작합니다

예약된 전송 발생을 중지하기 위해 관계를 중단한 후 * Resume * 을 사용하여 소스 또는 기본 볼륨의 데이터가 보호되도록 예약된 전송을 다시 활성화할 수 있습니다. 체크포인트가 있는 경우 다음 예약된 전송 간격에 다시 시작됩니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

전송을 재개할 일시 중지된 관계를 10개 이상 선택할 수 없습니다.

단계

1. 볼륨 * 관계 * 페이지에서 중지 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 * 재시작 * 을 클릭합니다.
2. Resume* 대화 상자에서 * Continue*를 클릭합니다.

   볼륨 관계 페이지로 돌아갑니다.

3. 관련 작업 작업을 보고 진행 상황을 추적하려면 * 볼륨 관계 * 페이지 상단에 표시되는 작업 링크를 클릭합니다.
4. 다음 중 하나를 수행합니다.
   - 하나의 작업만 표시되는 경우 작업 세부 정보 페이지에서 * 새로 고침 * 을 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 결정합니다.
   - 두 개 이상의 작업이 표시되는 경우
     i. 작업 페이지에서 세부 정보를 보려는 작업을 클릭합니다.
     ii. 작업 세부 정보 페이지에서 * 새로 고침 * 을 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업이 완료되는 시점을 결정합니다. 작업이 완료되면 다음 예약 전송 간격으로 데이터 전송이 다시 시작됩니다.

볼륨/상태 세부 정보 페이지에서 중지된 관계에서 예약된 전송을 재개합니다

예약된 전송 발생을 중지하기 위해 관계를 중지한 후 볼륨/상태 세부 정보 페이지에서 * Resume * 을 사용하여 소스 또는 기본 볼륨의 데이터가 보호되도록 예약된 전송을 다시 활성화할 수 있습니다. 체크포인트가 있는 경우 다음 예약된 전송 간격에 다시 시작됩니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 재개할 토폴로지 뷰를 마우스 오른쪽 버튼으로 클릭합니다.

   또는 * Actions * > * Relationship * 메뉴에서 * Resume * 을 선택합니다.

2. Resume* 대화 상자에서 * Continue*를 클릭합니다.

볼륨/상태 세부 정보 페이지로 돌아갑니다.

3. 관련 작업 작업을 보고 진행 상황을 추적하려면 * 볼륨/상태 * 세부 정보 페이지 상단에 표시되는 작업 링크를 클릭합니다.
4. Job * details 페이지에서 * Refresh * 를 클릭하여 보호 구성 작업과 관련된 작업 목록 및 작업 세부 정보를 업데이트하고 작업 완료 시기를 결정합니다.

   작업이 완료되면 다음 예약 전송 간격으로 데이터 전송이 재개됩니다.

볼륨 관계 페이지에서 보호 관계를 초기화 또는 업데이트합니다

볼륨 관계 페이지에서 새 보호 관계에 대한 초기 계획을 처음 전송할 수도 있고, 이미 초기화된 관계로 즉시 전송하기 위해 예정되지 않은 수동 증분 업데이트를 수행하려는 경우 관계를 업데이트할 수도 있습니다.

정합성 보장 그룹으로 보호되는 볼륨은 초기화하거나 업데이트할 수 없습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- OnCommand Workflow Automation를 설정해야 합니다.

단계

1. 볼륨 관계 * 페이지에서 볼륨을 마우스 오른쪽 단추로 클릭하고 업데이트하거나 초기화할 관계가 있는 볼륨을 하나 이상 선택한 다음 도구 모음에서 * 초기화/업데이트 * 를 클릭합니다.

   Initialize/Update * (초기화/업데이트 *) 대화 상자가 표시됩니다.

2. 전송 옵션 * 탭에서 전송 우선 순위 및 최대 전송 속도를 선택합니다.
3. 소스 스냅샷 복사본 * 을 클릭한 다음 * 스냅샷 복사본 * 열에서 * 기본값 * 을 클릭합니다.

   소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

4. 기본 스냅샷 복사본을 전송하지 않고 기존 스냅샷 복사본을 지정하려면 * 기존 스냅샷 복사본 * 을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
5. 제출 * 을 클릭합니다.

   Initialize/Update * 대화 상자로 돌아갑니다.

6. 초기화하거나 업데이트할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정할 다음 소스에 대해 * 기본값 * 을 클릭합니다.
7. 초기화 또는 업데이트 작업을 시작하려면 * 제출 * 을 클릭하십시오.

   초기화 또는 업데이트 작업이 시작되고 볼륨 관계 페이지로 돌아가며 페이지 상단에 작업 링크가 표시됩니다.

8. * 선택 사항: * 상태: 모든 볼륨 * 보기에서 * 작업 보기 * 를 클릭하여 각 초기화 또는 업데이트 작업의 상태를 추적합니다.

필터링된 작업 목록이 표시됩니다.

9. * 선택 사항: * 세부 정보를 보려면 각 작업을 클릭합니다.
10. * 선택 사항: * 브라우저의 * 뒤로 * 화살표를 클릭하여 * 볼륨 관계 * 페이지로 돌아갑니다.

    모든 작업이 성공적으로 완료되면 초기화 또는 업데이트 작업이 완료됩니다.

볼륨/상태 세부 정보 페이지에서 보호 관계를 초기화 또는 업데이트합니다

새 보호 관계에 대해 최초 베이스라인 전송을 수행하거나, 이미 초기화된 상태에서 데이터를 즉시 전송하기 위해 예정되지 않은 수동 증분 업데이트를 수행하려는 경우 관계를 업데이트할 수 있습니다.

- 참고 *: 정합성 보장 그룹으로 보호되는 볼륨은 초기화하거나 업데이트할 수 없습니다.
- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- OnCommand Workflow Automation를 설정해야 합니다.

단계

1. 볼륨/상태 * 세부 정보 페이지의 * 보호 * 탭에서 초기화하거나 업데이트할 보호 관계를 토폴로지에서 찾은 다음 마우스 오른쪽 단추로 클릭합니다.
2. 메뉴에서 * Initialize/Update * 를 선택합니다.

    또는 * Actions * 메뉴에서 * Relationship * > * Initialize/Update * 를 선택하여 현재 세부 정보를 보고 있는 관계를 초기화하거나 업데이트합니다.

    Initialize/Update(초기화/업데이트) 대화 상자가 표시됩니다.

3. 전송 옵션 * 탭에서 전송 우선 순위 및 최대 전송 속도를 선택합니다.
4. 소스 스냅샷 복사본 * 을 클릭한 다음 * 스냅샷 복사본 * 열에서 * 기본값 * 을 클릭합니다.

    소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

5. 기본 스냅샷 복사본을 전송하지 않고 기존 스냅샷 복사본을 지정하려면 * 기존 스냅샷 복사본 * 을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
6. 제출 * 을 클릭합니다.

    Initialize/Update(초기화/업데이트) 대화 상자로 돌아갑니다.

7. 초기화하거나 업데이트할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정할 다음 읽기/쓰기 소스에 대해 * 기본값 * 을 클릭합니다.

    데이터 보호 볼륨에 대해 다른 스냅샷 복사본을 선택할 수는 없습니다.

8. 초기화 또는 업데이트 작업을 시작하려면 * 제출 * 을 클릭하십시오.

    초기화 또는 업데이트 작업이 시작되고 볼륨/상태 세부 정보 페이지로 돌아가며 페이지 상단에 작업 링크가

표시됩니다.

9. * 선택 사항: * 볼륨/상태 * 세부 정보 페이지에서 * 작업 보기 * 를 클릭하여 각 초기화 또는 업데이트 작업의 상태를 추적합니다.

   필터링된 작업 목록이 표시됩니다.

10. * 선택 사항: * 세부 정보를 보려면 각 작업을 클릭합니다.
11. * 선택 사항: * 브라우저의 뒤로 화살표를 클릭하여 * 볼륨/상태 * 세부 정보 페이지로 돌아갑니다.

    모든 작업 작업이 성공적으로 완료되면 초기화 또는 업데이트 작업이 완료됩니다.

볼륨 관계 페이지에서 보호 관계를 재동기화합니다

볼륨 관계 페이지에서 소스 볼륨을 사용하지 않도록 설정한 이벤트에서 복구하거나 현재 소스를 다른 볼륨으로 변경하려는 경우 관계를 다시 동기화할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.

단계

1. 볼륨 관계 * 페이지에서 중지된 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 * 재동기화 * 를 클릭합니다.

   재동기화 대화 상자가 표시됩니다.

2. 재동기화 옵션 * 탭에서 전송 우선 순위 및 최대 전송 속도를 선택합니다.
3. 소스 스냅샷 복사본 * 을 클릭한 다음 * 스냅샷 복사본 * 열에서 * 기본값 * 을 클릭합니다.

   소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

4. 기본 스냅샷 복사본을 전송하지 않고 기존 스냅샷 복사본을 지정하려면 * 기존 스냅샷 복사본 * 을 클릭하고 목록에서 스냅샷 복사본을 선택합니다.
5. 제출 * 을 클릭합니다.

   재동기화 대화 상자로 돌아갑니다.

6. 재동기화할 소스를 두 개 이상 선택한 경우 기존 스냅샷 복사본을 지정할 다음 소스에 대해 * 기본값 * 을 클릭합니다.
7. Submit * 을 클릭하여 재동기화 작업을 시작합니다.

   재동기화 작업이 시작되고 볼륨 관계 페이지로 돌아가며 페이지 상단에 작업 링크가 표시됩니다.

8. * 선택 사항: * 볼륨 관계 * 페이지에서 * 작업 보기 * 를 클릭하여 각 재동기화 작업의 상태를 추적합니다.

   필터링된 작업 목록이 표시됩니다.

9. * 선택 사항: * 브라우저의 * 뒤로 * 화살표를 클릭하여 * 볼륨 관계 * 페이지로 돌아갑니다.

모든 작업 작업이 성공적으로 완료되면 재동기화 작업이 완료됩니다.

볼륨 관계 페이지에서 보호 관계를 반대로 설정합니다

재해로 인해 보호 관계의 소스 볼륨이 비활성화되면 소스를 복구하거나 교체하는 동안 대상 볼륨을 사용하여 데이터를 읽기/쓰기 볼륨으로 변환하여 제공할 수 있습니다. 소스를 다시 사용하여 데이터를 수신할 수 있으면 역재동기화 작업을 사용하여 역방향의 관계를 설정하여 소스의 데이터를 읽기/쓰기 대상의 데이터와 동기화할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- Workflow Automation을 설정해야 합니다.
- 관계가 SnapVault 관계여야 합니다.
- 보호 관계가 이미 있어야 합니다.
- 보호 관계가 끊어야 합니다.
- 소스와 대상이 모두 온라인 상태여야 합니다.
- 소스가 다른 데이터 보호 볼륨의 대상이 아니어야 합니다.
- 이 작업을 수행하면 공통 스냅샷 복사본의 데이터보다 최신 소스의 데이터가 삭제됩니다.
- 역재동기화 관계에 생성된 정책 및 스케줄은 원래 보호 관계에 있는 정책과 동일합니다.

  정책과 스케줄이 없으면 생성됩니다.

단계

1. 볼륨 관계 * 페이지에서 반전할 관계가 있는 볼륨을 하나 이상 선택하고 도구 모음에서 * 역재동기화 * 를 클릭합니다.

   역방향 재동기화 대화 상자가 표시됩니다.

2. 역방향 재동기화* 대화 상자에 표시된 관계가 역재동기화 작업을 수행할 관계인지 확인한 다음 * 제출 * 을 클릭합니다.

   역방향 재동기화 작업이 시작되고 볼륨 관계 페이지로 돌아가며 페이지 맨 위에 작업 링크가 표시됩니다.

3. * 선택 사항: * 볼륨 관계 * 페이지에서 * 작업 보기 * 를 클릭하여 각 역방향 재동기화 작업의 상태를 추적합니다.

   이 작업과 관련된 필터링된 작업 목록이 표시됩니다.

4. * 선택 사항: * 브라우저의 * 뒤로 * 화살표를 클릭하여 * 볼륨 관계 * 페이지로 돌아갑니다.

   모든 작업 작업이 성공적으로 완료되면 역방향 재동기화 작업이 완료됩니다.

볼륨 및 볼륨/상태 세부 정보 페이지를 사용하여 데이터를 복원합니다

볼륨 및 볼륨/상태 세부 정보 페이지의 복원 기능을 사용하여 스냅샷 복사본에서 덮어쓰기 또는

삭제된 파일, 디렉토리 또는 전체 볼륨을 복원할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 사항을 참고하십시오.

- NTFS 파일 스트림은 복원할 수 없습니다.
- 다음과 같은 경우에는 복원 옵션을 사용할 수 없습니다.
  - 볼륨 ID는 알 수 없습니다. 예를 들어, 인터클러스터 관계가 있고 대상 클러스터가 아직 검색되지 않은 경우입니다.
  - 볼륨은 SnapMirror Synchronous 복제에 대해 구성됩니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 > 볼륨 * 으로 이동합니다.
2. 볼륨을 선택하고 * 복원 * 버튼을 클릭합니다. 또는 볼륨을 클릭하여 * 볼륨/상태 세부 정보 > 작업 > 복원 * 으로 이동합니다. Restore(복원) 대화 상자가 표시됩니다. 이 페이지에 대한 자세한 내용은 을 참조하십시오 "복원 대화 상자".
3. 기본값과 다른 경우 데이터를 복원할 볼륨 및 스냅샷 복사본을 선택합니다.
4. 소스 LUN과 같이 복구할 항목을 선택합니다.

   전체 볼륨을 복원하거나 복원할 폴더 및 파일을 지정할 수 있습니다.
5. 선택한 항목을 복원할 위치를 * 원래 위치 * 또는 * 대체 기존 위치 * 중에서 선택합니다.
6. 기존 위치를 다른 위치로 선택하는 경우 다음 중 하나를 수행합니다.
   - Restore Path(복원 경로) 텍스트 필드에 데이터를 복원할 위치의 경로를 입력한 다음 * Select Directory(디렉터리 선택) * 를 클릭합니다.
   - 찾아보기 * 를 클릭하여 디렉터리 찾아보기 대화 상자를 시작하고 다음 단계를 완료합니다.
     i. 복원할 대상 클러스터, 스토리지 VM(SVM) 및 볼륨을 선택합니다.
     ii. 이름 테이블에서 복원해야 하는 디렉터리 이름을 선택합니다.
     iii. 디렉터리 선택 * 을 클릭합니다.
7. 복원 * 을 클릭합니다.

   복원 프로세스가 시작됩니다. 백엔드에서 작업을 생성하여 복원 프로세스를 완료합니다.
8. 작업 진행률을 보려면 왼쪽 탐색 창에서 * 보호 > 작업 * 으로 이동하여 작업 목록에서 복원 작업의 상태를 확인합니다.

NDMP 오류가 있는 Cloud Volumes ONTAP HA 클러스터 간에 복구 작업이 실패할 경우 대상이 소스 시스템의 클러스터 관리 LIF와 통신할 수 있도록 타겟 클러스터에 명시적 AWS 경로를 추가해야 할 수 있습니다. BlueXP를 사용하여 이 구성 단계를 수행합니다.

리소스 풀이란 무엇입니까

리소스 풀은 스토리지 관리자가 Unified Manager를 사용하여 생성한 애그리게이트 그룹이며, 백업 관리를 위해 파트너 애플리케이션에 프로비저닝을 제공합니다.

성능, 비용, 물리적 위치 또는 가용성 같은 속성을 기준으로 리소스를 풀링할 수 있습니다. 관련 리소스를 풀로 그룹화하면 풀을 단일 유닛으로 간주하여 모니터링하고 프로비저닝할 수 있습니다. 따라서 리소스 관리가 단순화되며 스토리지를 더 유연하고 효율적으로 사용할 수 있습니다.

2차 스토리지 프로비저닝 중에 Unified Manager는 다음 기준을 사용하여 리소스 풀에서 보호에 가장 적합한 애그리게이트를 결정합니다.

- Aggregate는 루트 애그리게이트가 아닌 데이터 애그리게이트로, 온라인 상태입니다.
- Aggregate는 ONTAP 버전이 소스 클러스터의 주요 버전보다 크거나 같은 대상 클러스터 노드에 있습니다.
- 애그리게이트에는 리소스 풀의 모든 애그리게이트에서 사용할 수 있는 가장 큰 공간이 있습니다.
- 대상 볼륨을 프로비저닝한 후 aggregate 공간이 거의 가득 차고 거의 초과된 임계값(글로벌 또는 로컬 임계값 중 해당하는 값)에 할당되고 있습니다.
- 대상 노드의 FlexVol 볼륨 수가 플랫폼 제한을 초과해서는 안 됩니다.

리소스 풀 생성

리소스 풀 생성 대화 상자를 사용하여 프로비저닝을 위해 애그리게이트를 그룹화할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

리소스 풀에는 서로 다른 클러스터의 애그리게이트가 포함될 수 있지만 동일한 애그리게이트는 서로 다른 리소스 풀에 속할 수 없습니다.

1. 왼쪽 탐색 창에서 * 보호 * > * 리소스 풀 * 을 클릭합니다.
2. 리소스 풀 * 페이지에서 * 생성 * 을 클릭합니다.
3. 리소스 풀 만들기 * 대화 상자의 지침에 따라 이름 및 설명을 제공하고 애그리게이트를 만들 리소스 풀에 구성원으로 추가합니다.

리소스 풀 편집

자원 그룹 이름과 설명을 변경하려는 경우 기존 자원 그룹을 편집할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

Edit * 버튼은 하나의 리소스 풀을 선택한 경우에만 활성화됩니다. 둘 이상의 리소스 풀을 선택하면 * Edit * 버튼이 비활성화됩니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 리소스 풀 * 을 클릭합니다.
2. 목록에서 리소스 풀 하나를 선택합니다.
3. 편집 * 을 클릭합니다.

   리소스 풀 편집 창이 표시됩니다.

4. 필요에 따라 리소스 풀 이름 및 설명을 편집합니다.
5. 저장 * 을 클릭합니다.

   새 이름과 설명이 리소스 풀 목록에 표시됩니다.

리소스 풀 인벤토리 보기

리소스 풀 페이지를 사용하여 리소스 풀 인벤토리를 보고 각 리소스 풀의 남은 용량을 모니터링할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 리소스 풀 * 을 클릭합니다.

   자원 그룹 인벤토리가 표시됩니다.

리소스 풀 구성원을 추가하는 중입니다

리소스 풀은 다수의 구성원 애그리게이트로 구성됩니다. 기존 리소스 풀에 애그리게이트를 추가하여 2차 볼륨 프로비저닝에 사용할 수 있는 공간 크기를 늘릴 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

리소스 풀에는 한 번에 200개 이상의 애그리게이트를 추가할 수 없습니다. 애그리게이트 대화 상자에 표시된 애그리게이트는 다른 리소스 풀에 속하지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 리소스 풀 * 을 클릭합니다.
2. 리소스 풀 * 목록에서 리소스 풀을 선택합니다.

   리소스 풀 구성원은 리소스 풀 목록 아래의 영역에 표시됩니다.

3. 자원 그룹 구성원 영역에서 * 추가 * 를 클릭합니다.

   애그리게이트 대화 상자가 표시됩니다.

4. 하나 이상의 애그리게이트를 선택합니다.
5. 추가 * 를 클릭합니다.

   대화 상자가 닫히고 선택한 리소스 풀의 구성원 목록에 애그리게이트가 표시됩니다.

리소스 풀에서 애그리게이트를 제거합니다

기존 리소스 풀에서 Aggregate를 제거할 수 있습니다. 예를 들어, 다른 용도로 Aggregate를 사용할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

리소스 풀 구성원은 리소스 풀을 선택한 경우에만 표시됩니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 리소스 풀 * 을 클릭합니다.
2. 구성원 애그리게이트를 제거할 리소스 풀을 선택합니다.

   구성원 집계 목록이 구성원 창에 표시됩니다.

3. 하나 이상의 애그리게이트를 선택합니다.

   제거 * 버튼이 활성화됩니다.

4. 제거 * 를 클릭합니다

   경고 대화 상자가 표시됩니다.

5. 계속하려면 * 예 * 를 클릭하십시오.

   선택한 애그리게이트가 구성원 창에서 제거됩니다.

리소스 풀을 삭제하는 중입니다

리소스 풀이 더 이상 필요하지 않으면 삭제할 수 있습니다. 예를 들어 리소스 풀 간에 구성원 애그리게이트를 재배포하여 원래 리소스 풀을 사용하지 않을 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

삭제 * 버튼은 하나 이상의 리소스 풀을 선택한 경우에만 활성화됩니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 리소스 풀 * 을 클릭합니다.
2. 삭제할 리소스 풀을 선택합니다.

3. 삭제 * 를 클릭합니다.

   리소스 풀이 리소스 풀 목록에서 제거되고 해당 애그리게이트가 구성원 목록에서 제거됩니다.

스토리지 **VM** 재해 복구 보호 관계 모니터링

Active IQ Unified Manager는 스토리지 VM 재해 복구 관계 모니터링을 지원하여 스토리지 VM 레벨의 세분화 수준으로 재해 복구를 제공합니다. 스토리지 VM 재해 복구를 사용하면 스토리지 VM의 구성 볼륨에 있는 데이터를 복구하고 스토리지 VM 구성을 복구할 수 있습니다.

스토리지 VM DR 관계는 소스 스토리지 VM에서 대상 스토리지 VM으로 생성되어 비동기식 재해 복구를 제공합니다. 클러스터 설정에 따라 데이터 볼륨과 함께 스토리지 VM 구성(네트워크 및 프로토콜 구성 제외)의 전체 또는 일부를 복제하도록 선택할 수 있습니다.

스토리지 VM 재해 복구 관계가 구성된 후 하드웨어 장애 또는 환경 재해로 인해 소스 스토리지 VM을 사용할 수 없게 되면 대상 스토리지 VM이 시작되어 운영 중단 없이 데이터에 액세스할 수 있습니다. 마찬가지로, 소스 스토리지 VM을 사용할 수 있게 되면 대상 스토리지 VM과 다시 동기화되고 소스가 다시 시작되어 데이터를 제공합니다. SnapMirror 명령을 사용하여 스토리지 VM 재해 복구 관계를 구성하고 관리할 수 있습니다.

관계 페이지를 사용하여 스토리지 **VM** 모니터링

인벤토리의 보호 섹션에 있는 관계 페이지에서 스토리지 VM 재해 복구 관계를 모니터링할 수 있습니다. 기본적으로 관계 페이지에는 구성 관계 필터가 적용될 때 최상위 관계만 나열됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

필터를 사용하여 스토리지 VM 재해 복구 관계를 볼 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 관계 * 를 클릭합니다.

   이 페이지에는 볼륨, 일관성 그룹 및 스토리지 VM 관계와 같은 모든 유형의 관계가 표시됩니다.

2. 필터 * 를 클릭한 다음 * 관계 개체 유형 * 및 * 스토리지 VM * 을 선택하여 스토리지 VM 재해 복구 관계만 표시합니다.
3. 필터 적용 * 을 클릭합니다.

   모든 보호 관계를 보려면 구성 관계 필터를 지워야 합니다.

   이 페이지에는 스토리지 VM 재해 복구 관계만 표시됩니다.

스토리지 **VM** 페이지에서 보호 관계 보기

스토리지 VM 페이지에서 기존 스토리지 VM의 재해 복구 관계 상태를 볼 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

전송 및 지연 상태, 소스 및 대상 세부 정보를 비롯한 보호 관계에 대한 세부 정보를 검토할 수도 있습니다. 보고서를 예약하거나 필요한 형식으로 기존 보고서를 다운로드할 수 있습니다. Show/Hide * (표시/숨기기 *) 버튼을 사용하면 기본적으로 표시되지 않으므로 보고서에 필요한 열을 추가할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 스토리지 VM * 을 클릭합니다.
2. 보기 * 메뉴에서 * 관계 * > * 모든 관계 * 를 선택합니다.

   관계: 모든 관계 보기가 구성된 모든 스토리지 VM과 함께 표시됩니다.

보호 상태에 따라 스토리지 **VM** 보기

인벤토리의 스토리지 VM 페이지를 사용하여 Active IQ Unified Manager의 모든 스토리지 VM을 보고 해당 보호 상태에 따라 스토리지 VM을 필터링할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

스토리지 VM의 보호 또는 보호 해제에 대한 정보를 제공하는 새 열 보호 역할이 스토리지 VM 보기에 추가됩니다.

ⓘ 소스 클러스터가 Active IQ Unified Manager에 추가되지 않으면 그리드에서 해당 클러스터와 관련된 모든 정보를 사용할 수 없습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 스토리지 VM * 을 클릭합니다.
2. view * 메뉴에서 * 상태 * > * 모든 스토리지 VM * 을 선택합니다.

   상태: 모든 스토리지 VM이 표시됩니다.

3. 다음 스토리지 VM 중 하나를 보려면 * Filter * 를 클릭합니다.

를 눌러 봅니다	필터 값
• 보호된 스토리지 VM *	• 보호 역할 * 은 * 보호됨 *
• 보호되지 않는 스토리지 VM *	• 보호 역할 * 은 * 보호되지 않음 * 입니다

ⓘ 보호된 스토리지 VM과 보호되지 않은 스토리지 VM을 동시에 볼 수 없습니다. 새 필터 옵션을 다시 적용하려면 기존 필터를 지워야 합니다.

4. 필터 적용 * 을 클릭합니다.

   Unsaved 보기에는 필터 선택에 따라 스토리지 VM 재해 복구에 의해 보호되거나 보호되지 않는 모든 스토리지 VM이 표시됩니다.

스토리지 **VM** 연결 이해

스토리지 가상 머신(스토리지 VM)은 리소스 선택 및 2차 볼륨 프로비저닝을 위해 파트너 애플리케이션이 사용하는 소스 스토리지 VM에서 대상 스토리지 VM으로 매핑되는 것입니다.

대상 스토리지 VM이 보조 대상인지 또는 3차 대상인지에 관계없이 소스 스토리지 VM과 대상 스토리지 VM 간에 연결이 생성됩니다. 2차 대상 스토리지 VM을 소스로 사용하여 3차 대상 스토리지 VM과 연결을 생성할 수 없습니다.

애플리케이션 관리자 또는 스토리지 관리자는 * 보호 * > * 스토리지 VM 연결 * 페이지에서 사용자 환경의 스토리지 VM 연결을 볼 수 있습니다.

SVM은 다음 세 가지 방법으로 연결할 수 있습니다.

- * 모든 스토리지 VM 연결 *: 운영 소스 스토리지 VM과 하나 이상의 타겟 SVM 간에 연결을 생성할 수 있습니다. 즉, 현재 보호가 필요한 모든 기존 SVM과 향후에 생성된 SVM이 지정된 타겟 SVM과 연결됩니다. 예를 들어, 서로 다른 위치에 있는 여러 소스의 애플리케이션을 한 위치의 하나 이상의 대상 SVM에 백업할 수 있습니다.
- * 특정 스토리지 VM 연결 *: 특정 소스 스토리지 VM과 하나 이상의 특정 타겟 SVM 간에 연결을 생성할 수 있습니다. 예를 들어, 데이터가 서로 분리되어 있어야 하는 여러 클라이언트에 스토리지 서비스를 제공하는 경우 이 옵션을 선택하여 특정 소스 스토리지 VM을 해당 클라이언트에만 할당된 특정 대상 스토리지 VM에 연결할 수 있습니다.
- * 외부 스토리지 VM과 연결 *: 소스 스토리지 VM과 대상 스토리지 VM의 유연한 외부 볼륨 간에 연결을 생성할 수 있습니다.

스토리지 **VM** 연결을 생성합니다

스토리지 가상 시스템 연결 생성 마법사를 사용하면 파트너 보호 애플리케이션에서 소스 스토리지 VM을 대상 스토리지 VM에 연결하여 SnapMirror 및 SnapVault 관계에 사용할 수 있습니다. 파트너 애플리케이션은 대상 볼륨의 초기 프로비저닝 시 이러한 연결을 사용하여 선택할 리소스를 결정합니다

- 필요한 것 *
- 연결하려는 스토리지 VM이 이미 있어야 합니다.
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

모든 소스 스토리지 VM 및 관계 유형에 대해 각 타겟 클러스터에서 하나의 대상 스토리지 VM만 선택할 수 있습니다.

삭제 및 생성 기능을 사용하여 연결을 변경하면 이후 프로비저닝 작업에만 영향을 줍니다. 기존 타겟 볼륨은 이동하지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 스토리지 VM 연결 * 을 클릭합니다.
2. 스토리지 VM 연결 * 페이지에서 * 생성 * 을 클릭합니다.

   스토리지 가상 머신 연결 생성 * 마법사가 시작됩니다.

3. 다음 소스 중 하나를 선택합니다.
   - * 모두 *

     운영 스토리지 VM 소스와 하나 이상의 대상 스토리지 VM 간의 연결을 생성하려는 경우 이 옵션을 선택합니다. 즉, 현재 보호가 필요한 모든 기존 스토리지 VM과 향후에 생성되는 모든 스토리지 VM이 지정된 대상 스토리지

VM에 연결됩니다. 예를 들어, 서로 다른 위치에 있는 여러 소스의 애플리케이션을 한 위치에 있는 하나 이상의 대상 스토리지 VM에 백업할 수 있습니다.

◦ * 단일 *

하나 이상의 대상 스토리지 VM에 연결된 특정 소스 스토리지 VM을 선택하려면 이 옵션을 선택합니다. 예를 들어, 데이터가 서로 분리되어 있어야 하는 여러 클라이언트에 스토리지 서비스를 제공하는 경우 이 옵션을 선택하여 특정 스토리지 VM 소스를 해당 클라이언트에만 할당된 특정 스토리지 VM 대상에 연결합니다.

◦ * 없음(외부) *

소스 스토리지 VM과 대상 스토리지 VM의 유연한 외부 볼륨 간에 연결을 생성하려는 경우 이 옵션을 선택합니다.

4. 생성할 보호 관계 유형 중 하나 또는 둘 모두를 선택합니다.
   ◦ * SnapMirror *
   ◦ * SnapVault *
5. 다음 * 을 클릭합니다.
6. 하나 이상의 스토리지 VM 보호 대상을 선택합니다.
7. 마침 * 을 클릭합니다.

스토리지 **VM** 연결을 삭제합니다

파트너 애플리케이션에 대한 스토리지 VM 연결을 삭제하여 소스 및 대상 스토리지 VM 간의 보조 프로비저닝 관계를 제거할 수 있습니다. 예를 들어, 대상 스토리지 VM이 가득 차서 새 스토리지 VM 보호 연결을 생성하려는 경우 이 작업을 수행할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

스토리지 VM 연결을 하나 이상 선택할 때까지 * Delete * 버튼이 비활성화됩니다. 삭제 및 생성 기능을 사용하여 연결을 변경하면 향후 프로비저닝 작업에만 영향을 미치며 기존 대상 볼륨은 이동하지 않습니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 스토리지 VM 연결 * 을 클릭합니다.
2. 스토리지 VM 연결을 하나 이상 선택합니다.

   삭제 * 버튼이 활성화됩니다.

3. 삭제 * 를 클릭합니다

   경고 대화 상자가 표시됩니다.

4. 계속하려면 * 예 * 를 클릭하십시오.

   선택한 스토리지 VM 연결이 목록에서 제거됩니다.

스토리지 서비스를 지원하기 위한 **SVM** 및 리소스 풀 요구사항

스토리지 서비스와 관련된 일부 SVM 연관 및 리소스 풀 요구사항을 관찰하면 파트너 애플리케이션이 더욱 잘 부합되도록 보장할 수 있습니다. 예를 들어, SVM을 연결하고 Unified Manager에서 리소스 풀을 생성하여 파트너 애플리케이션이 제공하는 스토리지 서비스의 보호 토폴로지를 지원할 수 있습니다.

일부 애플리케이션은 Unified Manager 서버와 파트너 관계를 맺고, 소스 볼륨과 2차 또는 3차 위치의 보호 볼륨 간에 SnapMirror 또는 SnapVault 백업 보호를 자동으로 구성 및 실행하는 서비스를 제공합니다. 이러한 보호 스토리지 서비스를 지원하려면 Unified Manager를 사용하여 필요한 SVM 연결 및 리소스 풀을 구성해야 합니다.

SnapMirror 소스 또는 SnapVault 운영 볼륨에서 대상 SnapMirror로 복제 또는 2차 또는 3차 위치에 있는 SnapVault 백업 볼륨으로 복제를 포함하여 스토리지 서비스 단일 홉 또는 다중 구간 보호를 지원하려면 다음 요구사항을 준수해야 합니다.

- SVM 연결은 SnapMirror 소스 또는 SnapVault 운영 볼륨을 포함하는 SVM과 2차 볼륨 또는 3차 볼륨이 상주하는 SVM 간에 구성되어야 합니다.
  - 예를 들어, 소스 볼륨 Vol_A가 SVM_1에 있고 SnapMirror 보조 타겟 볼륨 Vol_B가 SVM_2에 상주하는 보호 토폴로지를 지원하려면 3차 SnapVault 백업 볼륨 Vol_C는 SVM_3에 상주하며, Unified Manager 웹 UI를 사용하여 SVM_1과 SVM_2 사이에 SnapMirror 연결과 SVM_1과 SVM_3 사이의 SnapVault 백업 연결을 구성해야 합니다.

    이 예에서는 SVM_2와 SVM_3 간에 SnapMirror 연결 또는 SnapVault 백업 연결이 필요하지 않으며 사용되지 않습니다.

  - 소스 볼륨 Vol_A와 SnapMirror 대상 볼륨 Vol_B가 모두 SVM_1에 있는 보호 토폴로지를 지원하려면 SVM_1과 SVM_1 간에 SnapMirror 연결을 구성해야 합니다.
- 리소스 풀에는 관련 SVM에 사용 가능한 클러스터 애그리게이트 리소스가 포함되어야 합니다.

  Unified Manager 웹 UI를 통해 리소스 풀을 구성한 다음 파트너 애플리케이션을 통해 스토리지 서비스 2차 타겟 노드 및 3차 타겟 노드를 할당합니다.

어떤 작업인지

작업은 Unified Manager를 사용하여 모니터링할 수 있는 일련의 작업입니다. 작업 및 관련 작업을 보면 작업이 성공적으로 완료되었는지 확인할 수 있습니다.

SnapMirror 및 SnapVault 관계를 만들 때 관계 작업(중단, 편집, 중지, 제거, 재시작, 데이터 복원 작업을 수행할 때, 클러스터에 로그인할 때 다시 동기화 및 다시 동기화)를 수행합니다.

작업을 시작할 때 작업 페이지와 작업 세부 정보 페이지를 사용하여 관련 작업 작업의 진행 상황을 모니터링할 수 있습니다.

작업 모니터링

작업 페이지를 사용하여 작업 상태를 모니터링하고 스토리지 서비스 유형, 상태, 제출된 시간 및 완료된 시간과 같은 작업 속성을 보고 작업이 성공적으로 완료되었는지 여부를 확인할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 작업 * 을 클릭합니다.

   작업 페이지가 표시됩니다.

2. 상태* 열을 보고 현재 실행 중인 작업의 상태를 확인합니다.
3. 특정 작업에 대한 세부 정보를 보려면 작업 이름을 클릭하십시오.

   작업 세부 정보 페이지가 표시됩니다.

작업 세부 정보 보기

작업을 시작한 후 작업 세부 정보 페이지에서 작업 진행 상황을 추적하고 관련 작업에서 오류가 발생할 수 있는지 모니터링할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 작업 * 을 클릭합니다.
2. 작업 페이지의 * 이름 * 열에서 작업 이름을 클릭하여 작업과 연관된 작업 목록을 표시합니다.
3. 작업을 클릭하면 * 작업 세부 정보 * 창과 작업 목록 오른쪽의 * 작업 메시지 * 창에 추가 정보가 표시됩니다.

작업을 중단합니다

작업 페이지를 사용하여 작업을 완료하는 데 시간이 너무 오래 걸리거나, 오류가 너무 많이 발생하거나, 더 이상 필요하지 않은 경우 작업을 중단할 수 있습니다. 작업의 상태와 유형이 허용하는 경우에만 작업을 중단할 수 있습니다. 실행 중인 작업을 중단할 수 있습니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 작업 * 을 클릭합니다.
2. 작업 목록에서 하나의 작업을 선택한 다음 * Abort * (중단 *)를 클릭합니다.
3. 확인 프롬프트에서 * 예 * 를 클릭하여 선택한 작업을 중단합니다.

실패한 보호 작업을 다시 시도합니다

실패한 보호 작업을 수정하기 위한 조치를 취한 후 * Retry * 를 사용하여 작업을 다시 실행할 수

있습니다. 작업을 재시도하면 원래 작업 ID를 사용하여 새 작업이 생성됩니다.

- 필요한 것 *

애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

실패한 작업은 한 번에 하나만 다시 시도할 수 있습니다. 둘 이상의 작업을 선택하면 * 재시도 * 버튼이 비활성화됩니다. 보호 구성 및 보호 관계 작업 유형의 작업만 다시 시도할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 보호 * > * 작업 * 을 클릭합니다.
2. 작업 목록에서 실패한 보호 구성 또는 보호 관계 작업 유형 작업을 하나 선택합니다.

   Retry *(재시도 *) 버튼이 활성화됩니다.

3. 재시도 * 를 클릭합니다.

   작업이 다시 시작됩니다.

보호 관계 창 및 대화 상자에 대한 설명입니다

리소스 풀, SVM 협회 및 보호 작업과 같은 보호 관련 세부 정보를 보고 관리할 수 있습니다. 적절한 상태 임계값 페이지를 사용하여 애그리게이트, 볼륨 및 관계에 대한 글로벌 상태 임계값을 구성할 수 있습니다.

리소스 풀 페이지를 참조하십시오

리소스 풀 페이지에는 기존 리소스 풀과 해당 구성원이 표시되며, 이를 통해 용량 할당을 위해 리소스 풀을 생성, 모니터링 및 관리할 수 있습니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 생성 *

  자원 풀을 만드는 데 사용할 수 있는 자원 풀 생성 대화 상자를 시작합니다.

- * 편집 *

  생성한 리소스 풀의 이름과 설명을 편집할 수 있습니다.

- * 삭제 *

  하나 이상의 리소스 풀을 삭제할 수 있습니다.

리소스 풀 목록입니다

리소스 풀 목록에는 기존 리소스 풀의 속성이 표 형식으로 표시됩니다.

- * 리소스 풀 *

  리소스 풀의 이름을 표시합니다.

- * 설명 *

  에서는 리소스 풀을 설명합니다.

- * SnapLock 유형 *

  리소스 풀의 애그리게이트에서 사용 중인 SnapLock 유형을 표시합니다. SnapLock 유형에 유효한 값은 규정 준수, 엔터프라이즈 및 비 SnapLock입니다. 리소스 풀에는 SnapLock 유형이 하나인 애그리게이트만 포함될 수 있습니다.

- * 총 용량 *

  리소스 풀의 총 용량(MB, GB 등)을 표시합니다.

- * 사용된 용량 *

  리소스 풀에서 사용되는 공간 크기(MB, GB 등)를 표시합니다.

- * 가용 용량 *

  리소스 풀에서 사용할 수 있는 공간 크기(MB, GB 등)를 표시합니다.

- * % * 사용

  리소스 풀에서 사용된 공간의 비율을 표시합니다.

구성원 목록 명령 단추

구성원 목록 명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 추가 *

  리소스 풀에 구성원을 추가할 수 있습니다.

- * 삭제 *

  리소스 풀에서 하나 이상의 구성원을 삭제할 수 있습니다.

구성원 목록

구성원 목록에는 리소스 풀을 선택할 때 리소스 풀 구성원 및 해당 속성이 표 형식으로 표시됩니다.

- * 상태 *

  구성원 애그리게이트의 현재 상태를 표시합니다. 상태는 Critical(), 오류(), 경고() 또는 보통()를 클릭합니다.

- * 집계 이름 *

구성원 집계 이름을 표시합니다.

- * 시/도 *

  다음 중 하나의 집계 현재 상태를 표시합니다.

  - 오프라인

    읽기 또는 쓰기 액세스가 허용되지 않습니다.

  - 온라인

    이 애그리게이트에서 호스팅되는 볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

  - 제한

    제한된 작업(예: 패리티 재구성)은 허용되지만 데이터 액세스는 허용되지 않습니다.

  - 생성 중

    Aggregate가 생성 중입니다.

  - 제거 중

    애그리게이트는 폐기되고 있습니다.

  - 실패했습니다

    애그리게이트는 온라인 상태로 가져올 수 없습니다.

  - 고정

    애그리게이트는 (일시적으로) 요청을 처리하지 않습니다.

  - 일관성이 없습니다

    Aggregate가 손상된 것으로 표시되었습니다. 기술 지원 부서에 문의해야 합니다.

  - 다리미 제한

    진단 도구는 애그리게이트에서 실행할 수 없습니다.

  - 장착

    Aggregate가 마운트하는 중입니다.

  - 부분

    애그리게이트에 대해 하나 이상의 디스크를 찾았지만 둘 이상의 디스크가 누락되었습니다.

  - 정지 중

    애그리게이트를 정지하고 있습니다.

◦ 정지되었습니다

애그리게이트는 정지됩니다.

◦ 되돌렸습니다

Aggregate의 복원이 완료되었습니다.

◦ 마운트 해제되었습니다

애그리게이트가 마운트 해제되었습니다.

◦ 마운트 해제 중

애그리게이트는 오프라인 상태로 전환되고 있습니다.

◦ 알 수 없음

Aggregate가 검색되지만 Unified Manager 서버에서 애그리게이트 정보를 아직 검색하지 않습니다.

기본적으로 이 열은 숨겨져 있습니다.

- * 클러스터 *

  Aggregate가 속한 클러스터의 이름을 표시합니다.

- * 노드 *

  Aggregate가 상주하는 노드의 이름을 표시합니다.

- * 총 용량 *

  Aggregate의 총 용량(MB, GB 등)을 표시합니다.

- * 사용된 용량 *

  Aggregate에 사용되는 공간(MB, GB 등)을 표시합니다.

- * 가용 용량 *

  Aggregate에서 사용 가능한 공간 크기(MB, GB 등)를 표시합니다.

- * % * 사용

  Aggregate에 사용된 공간의 비율을 표시합니다.

- * 디스크 유형 *

  RAID 구성 유형을 표시합니다. RAID 구성 유형은 다음 중 하나일 수 있습니다.

  ◦ RAID0: 모든 RAID 그룹은 RAID0 유형입니다.
  ◦ RAID4: 모든 RAID 그룹은 RAID4 유형입니다.

◦ RAID-DP: 모든 RAID 그룹은 RAID-DP 유형입니다.

◦ RAID-TEC: 모든 RAID 그룹은 RAID-TEC 유형입니다.

◦ 혼합 RAID: Aggregate는 RAID 유형(RAID0, RAID4, RAID-DP 및 RAID-TEC)이 서로 다른 RAID 그룹을 포함합니다. 기본적으로 이 열은 숨겨져 있습니다.

리소스 풀 생성 대화 상자

리소스 풀 생성 대화 상자를 사용하여 새 리소스 풀의 이름과 설명을 지정하고 해당 리소스 풀에 애그리게이트를 추가하거나 해당 리소스 풀에서 애그리게이트를 삭제할 수 있습니다.

리소스 풀 이름입니다

텍스트 상자를 사용하면 다음 정보를 추가하여 리소스 풀을 만들 수 있습니다.

리소스 풀 이름을 지정할 수 있습니다.

설명

리소스 풀을 설명할 수 있습니다.

구성원

리소스 풀의 구성원을 표시합니다. 구성원을 추가 및 삭제할 수도 있습니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 추가 *

  특정 클러스터의 애그리게이트를 리소스 풀에 추가할 수 있도록 애그리게이트 대화 상자를 엽니다. 서로 다른 클러스터에서 애그리게이트를 추가할 수 있지만, 동일한 애그리게이트를 두 개 이상의 리소스 풀에 추가할 수 없습니다.

- * 제거 *

  선택한 애그리게이트를 리소스 풀에서 제거할 수 있습니다.

- * 생성 *

  리소스 풀을 생성합니다. 이 버튼은 자원 풀 이름 또는 설명 필드에 정보를 입력할 때까지 활성화되지 않습니다.

- * 취소 *

  변경 내용을 취소하고 자원 풀 만들기 대화 상자를 닫습니다.

리소스 풀 편집 대화 상자

리소스 풀 편집 대화 상자를 사용하여 기존 리소스 풀의 이름과 설명을 변경할 수 있습니다. 예를 들어 원래 이름과 설명이 부정확하거나 잘못된 경우 보다 정확하게 변경할 수 있습니다.

텍스트 상자

텍스트 상자를 사용하여 선택한 리소스 풀에 대해 다음 정보를 변경할 수 있습니다.

- * 리소스 풀 이름 *

  새 이름을 입력할 수 있습니다.

- * 설명 *

  새 설명을 입력할 수 있습니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 저장 *

  변경 사항을 리소스 풀 이름 및 설명에 저장합니다.

- * 취소 *

  변경 내용을 취소하고 자원 풀 편집 대화 상자를 닫습니다.

애그리게이트 대화 상자

애그리게이트 대화 상자를 사용하여 리소스 풀에 추가할 애그리게이트를 선택할 수 있습니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 추가 *

  선택한 애그리게이트를 리소스 풀에 추가합니다. 하나 이상의 Aggregate를 선택해야 Add 버튼을 사용할 수 있습니다.

- * 취소 *

  변경 사항을 취소하고 집계 대화 상자를 닫습니다.

애그리게이트 목록

애그리게이트 목록에는 모니터링되는 애그리게이트의 이름과 속성이 표 형식으로 표시됩니다.

- * 상태 *

  볼륨의 현재 상태를 표시합니다. 상태는 Critical( ), 오류( ), 경고( ) 또는 보통( )를 클릭합니다.

  상태 위로 포인터를 이동하여 볼륨에 대해 생성된 이벤트 또는 이벤트에 대한 자세한 정보를 볼 수 있습니다.

- * 집계 이름 *

  애그리게이트의 이름을 표시합니다.

- * 시/도 *

  다음 중 하나의 집계 현재 상태를 표시합니다.

  - 오프라인

    읽기 또는 쓰기 액세스가 허용되지 않습니다.

  - 제한

    제한된 작업(예: 패리티 재구성)은 허용되지만 데이터 액세스는 허용되지 않습니다.

  - 온라인

    이 애그리게이트에서 호스팅되는 볼륨에 대한 읽기 및 쓰기 액세스가 허용됩니다.

  - 생성 중

    Aggregate가 생성 중입니다.

  - 제거 중

    애그리게이트는 폐기되고 있습니다.

  - 실패했습니다

    애그리게이트는 온라인 상태로 가져올 수 없습니다.

  - 고정

    애그리게이트는 (일시적으로) 요청을 처리하지 않습니다.

  - 일관성이 없습니다

    Aggregate가 손상된 것으로 표시되었습니다. 기술 지원 부서에 문의해야 합니다.

  - 다리미 제한

    진단 도구는 애그리게이트에서 실행할 수 없습니다.

  - 장착

    Aggregate가 마운트하는 중입니다.

  - 부분

    애그리게이트에 대해 하나 이상의 디스크를 찾았지만 둘 이상의 디스크가 누락되었습니다.

  - 정지 중

애그리게이트를 정지하고 있습니다.

◦ 정지되었습니다

애그리게이트는 정지됩니다.

◦ 되돌렸습니다

Aggregate의 복원이 완료되었습니다.

◦ 마운트 해제되었습니다

애그리게이트는 오프라인 상태입니다.

◦ 마운트 해제 중

애그리게이트는 오프라인 상태로 전환되고 있습니다.

◦ 알 수 없음

Aggregate가 검색되지만 Unified Manager 서버에서 애그리게이트 정보를 아직 검색하지 않습니다.

- * 클러스터 *

  Aggregate가 상주하는 클러스터의 이름을 표시합니다.

- * 노드 *

  Aggregate가 포함된 스토리지 컨트롤러의 이름을 표시합니다.

- * 총 용량 *

  Aggregate의 총 데이터 크기(MB, GB 등)를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 확정 용량 *

  Aggregate의 모든 볼륨에 커밋된 총 공간(MB, GB 등)을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 사용된 용량 *

  Aggregate에 사용되는 공간(MB, GB 등)을 표시합니다.

- * 가용 용량 *

  Aggregate에서 데이터에 사용할 수 있는 공간 크기(MB, GB 등)를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 사용 가능 % *

  Aggregate에서 데이터에 사용 가능한 공간의 비율을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- * % * 사용

Aggregate의 데이터에 사용된 공간의 비율을 표시합니다.

- * RAID 유형 *

  선택한 볼륨의 RAID 유형을 표시합니다. RAID 유형은 RAID0, RAID4, RAID-DP, RAID-TEC 또는 혼합 RAID일 수 있습니다.

작업 페이지

작업 페이지에서는 현재 실행 중인 모든 파트너 애플리케이션 보호 작업과 완료된 작업에 대한 현재 상태 및 기타 정보를 볼 수 있습니다. 이 정보를 사용하여 아직 실행 중인 작업과 작업의 성공 또는 실패 여부를 확인할 수 있습니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 중단 *

  선택한 작업을 중단합니다. 이 옵션은 선택한 작업이 실행 중인 경우에만 사용할 수 있습니다.

- * 재시도 *

  보호 구성 또는 보호 관계 작업 유형의 실패한 작업을 다시 시작합니다. 실패한 작업은 한 번에 하나만 다시 시도할 수 있습니다. 실패한 작업이 두 개 이상 선택된 경우 * Retry *(재시도 *) 버튼이 비활성화됩니다. 실패한 스토리지 서비스 작업은 다시 시도할 수 없습니다.

- * 새로 고침 *

  작업 목록 및 관련 정보를 새로 고칩니다.

작업 목록

작업 목록은 진행 중인 작업 목록을 표 형식으로 표시합니다. 기본적으로 목록에는 지난 주 내에 생성된 작업만 표시됩니다. 열 정렬 및 필터링을 사용하여 표시할 작업을 사용자 지정할 수 있습니다.

- * 상태 *

  작업의 현재 상태를 표시합니다. 상태는 오류(❗) 또는 보통(✅)를 클릭합니다.

- * 작업 ID *

  작업의 식별 번호를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

  작업 식별 번호는 고유하며 작업을 시작할 때 서버에서 지정됩니다. 열 필터가 제공하는 텍스트 상자에 작업 ID 번호를 입력하여 특정 작업을 검색할 수 있습니다.

- * 이름 *

  작업 이름을 표시합니다.

- * 유형 *

  작업 유형을 표시합니다. 작업 유형은 다음과 같습니다.

  - * 클러스터 획득 *

    Workflow Automation 작업이 클러스터를 재검색하고 있습니다.

  - * 보호 구성 *

    보호 작업이 cron 일정, SnapMirror 정책 생성 등과 같은 Workflow Automation 워크플로우를 시작하고 있습니다.

  - * 보호 관계 작업 *

    보호 작업에서 SnapMirror 작업을 실행하고 있습니다.

  - * 보호 워크플로우 체인 *

    Workflow Automation 작업에서 여러 워크플로우가 실행되고 있습니다.

  - * 복원 *

    복원 작업이 실행 중입니다.

  - * 정리 *

    이 작업은 더 이상 복구를 위해 필요하지 않은 스토리지 서비스 구성원 아티팩트를 정리하는 중입니다.

  - * 준수 *

    이 작업은 스토리지 서비스 구성원이 규정을 준수하는지 확인하기 위해 스토리지 서비스 구성원의 구성을 확인하는 중입니다.

  - * 제거 *

    작업이 스토리지 서비스를 삭제하는 중입니다.

  - * 가져오기 *

    관리되지 않는 스토리지 객체를 기존 스토리지 서비스로 가져오는 중입니다.

  - * 수정 *

    작업이 기존 스토리지 서비스의 속성을 수정하고 있습니다.

  - * 구독 *

    스토리지 서비스에 가입하는 작업입니다.

  - * 구독 취소 *

    스토리지 서비스의 회원 가입을 취소하는 중입니다.

◦ * 업데이트 *

보호 업데이트 작업이 실행 중입니다.

◦ * WFA 구성 *

Workflow Automation 작업이 클러스터 자격 증명을 푸시하고 데이터베이스 캐시를 동기화하는 중입니다.

- * 시/도 *

작업의 실행 상태를 표시합니다. 상태 옵션은 다음과 같습니다.

◦ * 중단됨 *

작업이 중단되었습니다.

◦ * 중단 중 *

작업이 중단 중입니다.

◦ * 완료됨 *

작업이 완료되었습니다.

◦ * 러닝 *

작업이 실행 중입니다.

- * 제출 시간 *

작업이 제출된 시간을 표시합니다.

- * 기간 *

작업을 완료하는 데 걸린 시간을 표시합니다. 이 열은 기본적으로 표시됩니다.

- * 완료 시간 *

작업이 완료된 시간을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

작업 세부 정보 페이지

작업 세부 정보 페이지에서는 실행 중이거나 대기 중이거나 완료된 특정 보호 작업 작업에 대한 상태 및 기타 정보를 볼 수 있습니다. 이 정보를 사용하여 보호 작업 진행률을 모니터링하고 작업 오류를 해결할 수 있습니다.

작업 요약

작업 요약에는 다음 정보가 표시됩니다.

- 작업 ID입니다

- 유형
- 상태
- 제출된 시간
- 완료 시간
- 기간

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 새로 고침 *

  작업 목록과 각 작업과 연관된 속성을 새로 고칩니다.

- * 작업 보기 *

  작업 페이지로 돌아갑니다.

작업 작업 목록

작업 작업 목록은 특정 작업과 연관된 모든 작업과 각 작업과 관련된 속성을 테이블에 표시합니다.

- * 시작 시간 *

  작업이 시작된 날짜 및 시간을 표시합니다. 기본적으로 가장 최근 작업은 열 맨 위에 표시되고 이전 작업은 아래쪽에 표시됩니다.

- * 유형 *

  작업 유형을 표시합니다.

- * 시/도 *

  특정 작업의 상태:

  ◦ * 완료됨 *

    작업이 완료되었습니다.

  ◦ * 대기 중 *

    작업을 실행하려고 합니다.

  ◦ * 러닝 *

    작업이 실행 중입니다.

  ◦ * 대기 중 *

    작업이 제출되었으며 일부 관련 작업이 대기 및 실행 중입니다.

- * 상태 *

  작업 상태를 표시합니다.

  - * 오류(⚠) *

    작업이 실패했습니다.

  - * 보통(✅) *

    작업이 성공했습니다.

  - * 건너뜀(↷) *

    작업이 실패하여 후속 작업을 건너뜁니다.

- * 기간 *

  작업이 시작된 이후의 경과 시간을 표시합니다.

- * 완료 시간 *

  작업이 완료된 시간을 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 작업 ID *

  작업의 개별 작업을 식별하는 GUID를 표시합니다. 열을 정렬 및 필터링할 수 있습니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 종속성 순서 *

  첫 번째 작업에 0이 할당된 상태에서 그래프의 작업 시퀀스를 나타내는 정수를 표시합니다. 기본적으로 이 열은 숨겨져 있습니다.

- * 작업 세부 정보 창 *

  태스크 이름, 태스크 설명 및 태스크가 실패한 경우 실패의 원인을 포함하여 각 작업 태스크에 대한 추가 정보를 표시합니다.

- * 작업 메시지 창 *

  선택한 작업과 관련된 메시지를 표시합니다. 메시지에는 오류의 이유와 해결 방법이 포함될 수 있습니다. 일부 작업에는 작업 메시지가 표시되지 않습니다.

고급 보조 설정 대화 상자

고급 보조 설정 대화 상자를 사용하여 버전에 상관없이 유연하게 복제, 다중 복사본 백업 및 보조 볼륨에서 공간 관련 설정을 활성화할 수 있습니다. 현재 설정을 활성화 또는 비활성화하려는 경우 고급 보조 설정 대화 상자를 사용할 수 있습니다.

공간 관련 설정은 중복제거, 데이터 압축, 자동 확장, 공간 보장과 같이 저장되는 데이터의 양을 극대화합니다.

대화 상자에는 다음 필드가 포함되어 있습니다.

- * 버전에 상관없이 유연하게 복제 * 를 활성화합니다

  버전에 상관없이 유연하게 복제 가능한 SnapMirror를 지원합니다. 버전에 상관없이 유연하게 복제할 수 있어 소스 볼륨의 이전 버전인 ONTAP에서 타겟 볼륨을 실행하는 경우에도 소스 볼륨의 SnapMirror를 보호할 수 있습니다.

  - 백업을 활성화합니다

    버전에 상관없이 유연하게 복제할 수 있는 경우 SnapMirror 소스 데이터의 여러 스냅샷 복사본도 SnapMirror 대상에 전송 및 유지됩니다.

- * 중복 제거 사용 *

  SnapVault 관계에서 2차 볼륨의 중복제거를 지원하여 중복 데이터 블록을 제거하여 공간을 절약합니다. 절약 공간이 10% 이상, 데이터 덮어쓰기 속도가 빠른 경우에는 중복제거를 사용할 수 있습니다. 중복 제거는 가상화된 환경, 파일 공유 및 백업 데이터에 주로 사용됩니다. 이 설정은 기본적으로 비활성화되어 있습니다. 이 기능을 활성화하면 각 전송 후에 이 작업이 시작됩니다.

  - 압축을 설정합니다

    투명한 데이터 압축을 지원합니다. 공간 절약 효과가 10% 이상, 잠재적 오버헤드를 허용할 때, 그리고 비사용 시간 동안 압축을 완료할 수 있는 시스템 리소스가 충분할 때 압축을 사용할 수 있습니다. SnapVault 관계에서는 이 설정이 기본적으로 사용되지 않습니다. 압축은 중복제거를 선택한 경우에만 사용할 수 있습니다.

  - 인라인 압축

    데이터를 디스크에 쓰기 전에 데이터를 압축하여 공간을 즉시 절약할 수 있습니다. 피크 시간 동안 시스템의 활용률이 50%를 넘지 않고 시스템이 피크 시간 동안 새로운 쓰기와 추가 CPU를 수용할 수 있는 경우 인라인 압축을 사용할 수 있습니다. 이 설정은 ""압축 활성화""가 선택된 경우에만 사용할 수 있습니다.

- * Autogrow 사용 *

  연결된 Aggregate에서 사용 가능한 공간이 있는 경우, 사용 가능한 공간 비율이 지정된 임계값 미만이면 대상 볼륨을 자동으로 확장할 수 있습니다.

- * 최대 크기 *

  볼륨이 커질 수 있는 최대 비율을 설정합니다. 기본값은 소스 볼륨 크기보다 20% 더 큽니다. 현재 크기가 최대 자동 확장 비율보다 크거나 같은 경우에는 볼륨이 자동으로 확장되지 않습니다. 이 필드는 자동 확장 설정이 활성화된 경우에만 활성화됩니다.

- * 증분 크기 *

  소스 볼륨의 최대 비율에 도달하기 전에 볼륨이 자동으로 증가하는 비율을 지정합니다.

- * 공간 보장 *

  보조 볼륨에 충분한 공간이 할당되어 데이터 전송이 항상 성공하도록 합니다. 공간 보장 설정은 다음 중 하나일 수 있습니다.

  - 파일
  - 볼륨

◦ 없음 + 예를 들어 총 50GB의 파일을 포함하는 200GB 볼륨이 있을 수 있지만 이러한 파일은 10GB의 데이터만 저장합니다. 볼륨 보장은 소스의 컨텐츠에 관계없이 대상 볼륨에 200GB를 할당합니다. 파일 보증은 소스 파일에 충분한 공간이 확보되도록 50GB를 할당합니다. 이 시나리오에서 없음 을 선택하면 소스의 파일 데이터에 의해 사용되는 실제 공간에 대해 대상에 10GB만 할당됩니다.

공간 보장은 기본적으로 볼륨 으로 설정됩니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 적용 *

  보호 구성 대화 상자에서 * 적용 * 을 클릭하면 선택한 효율성 설정을 저장하고 적용합니다.

- * 취소 *

  선택 사항을 취소하고 고급 대상 설정 대화 상자를 닫습니다.

고급 대상 설정 대화 상자

고급 대상 설정 대화 상자를 사용하여 대상 볼륨에서 공간 보장 설정을 활성화할 수 있습니다. 소스에서 공간 보장이 비활성화되었지만 대상에서 사용하려면 고급 설정을 선택할 수 있습니다. SnapMirror 관계의 중복제거, 압축 및 자동 확장 설정은 소스 볼륨에서 상속되며 변경할 수 없습니다.

공간 보장

데이터가 항상 성공적으로 전송되도록 대상 볼륨에 충분한 공간이 할당되도록 합니다. 공간 보장 설정은 다음 중 하나일 수 있습니다.

- 파일
- 볼륨
- 없음

예를 들어 총 50GB의 파일을 포함하는 200GB 볼륨이 있을 수 있지만 이러한 파일은 10GB의 데이터만 저장할 수 있습니다. 볼륨 보장은 소스의 컨텐츠에 관계없이 대상 볼륨에 200GB를 할당합니다. 파일 보증은 50GB를 할당하여 대상의 소스 파일에 충분한 공간이 확보되도록 합니다. 이 시나리오에서 * 없음 * 을 선택하면 소스의 파일 데이터에 사용되는 실제 공간에 대해 대상에 10GB만 할당됩니다.

공간 보장은 기본적으로 볼륨 으로 설정됩니다.

복원 대화 상자

복원 대화 상자를 사용하여 특정 스냅샷 복사본에서 볼륨에 데이터를 복원할 수 있습니다.

에서 복원합니다

복원 위치 영역을 사용하여 데이터를 복원할 위치를 지정할 수 있습니다.

- * 볼륨 *

  데이터를 복원할 볼륨을 지정합니다. 기본적으로 복원 작업을 시작한 볼륨이 선택됩니다. 드롭다운 목록에서 복구 작업을 시작한 볼륨에 대한 보호 관계가 있는 모든 볼륨이 포함된 다른 볼륨을 선택할 수 있습니다.

- * 스냅샷 복사본 *

  데이터를 복원하는 데 사용할 스냅샷 복사본을 지정합니다. 기본적으로 가장 최근의 스냅샷 복사본이 선택됩니다. 드롭다운 목록에서 다른 스냅샷 복사본을 선택할 수도 있습니다. 선택한 볼륨에 따라 스냅샷 복사본 목록이 변경됩니다.

- * 최대 995개의 파일 및 디렉토리 목록 *

  기본적으로 최대 995개의 객체가 목록에 표시됩니다. 선택한 볼륨 내의 모든 개체를 보려면 이 확인란을 선택 취소할 수 있습니다. 항목 수가 매우 큰 경우 이 작업은 다소 시간이 걸릴 수 있습니다.

복원할 항목을 선택합니다

복원할 항목 선택 영역에서 전체 볼륨 또는 복원할 특정 파일 및 폴더를 선택할 수 있습니다. 최대 10개의 파일, 폴더 또는 두 가지 조합을 선택할 수 있습니다. 최대 항목 수를 선택하면 항목 선택 확인란이 비활성화됩니다.

- * 경로 필드 *

  복원하려는 데이터의 경로를 표시합니다. 복원할 폴더 및 파일을 탐색하거나 경로를 입력할 수 있습니다. 이 필드는 경로를 선택하거나 입력할 때까지 비어 있습니다. 를 클릭합니다 경로를 선택하면 디렉토리 구조에서 한 수준 위로 이동합니다.

- * 폴더 및 파일 목록 *

  입력한 경로의 내용을 표시합니다. 기본적으로 루트 폴더는 처음에 표시됩니다. 폴더 이름을 클릭하면 폴더의 내용이 표시됩니다.

다음과 같이 복원할 항목을 선택할 수 있습니다.

- 경로 필드에 지정된 특정 파일 이름의 경로를 입력하면 지정된 파일이 폴더 및 파일에 표시됩니다.
- 특정 파일을 지정하지 않고 경로를 입력하면 폴더의 내용이 폴더 및 파일 목록에 표시되며, 복원할 파일, 폴더 또는 이 둘을 최대 10개까지 선택할 수 있습니다.

  폴더에 995개 이상의 항목이 포함된 경우 표시할 항목이 너무 많음을 나타내는 메시지가 표시되고 작업을 계속하면 지정된 폴더의 모든 항목이 복원됩니다. 선택한 볼륨 내의 모든 오브젝트를 보려면 '"최대 995개의 파일 및 디렉터리 나열' 확인란을 선택 취소할 수 있습니다.

NTFS 파일 스트림은 복원할 수 없습니다.

에 복원합니다

복원 대상 영역을 사용하여 데이터를 복원할 위치를 지정할 수 있습니다.

- * Volume_Name * 의 원래 위치

선택한 데이터를 원래 백업된 소스의 디렉토리로 복원합니다.

- * 대체 위치 *

  선택한 데이터를 새 위치로 복원합니다.

  - 복원 경로

    선택한 데이터를 복원하기 위한 대체 경로를 지정합니다. 경로가 이미 있어야 합니다. 찾아보기 * 버튼을 사용하여 데이터를 복원할 위치로 이동하거나 cluster://svm/volume/path 형식을 사용하여 수동으로 경로를 입력할 수 있습니다.

  - 디렉터리 계층 구조 유지

    이 옵션을 선택하면 원본 파일이나 디렉터리의 구조가 유지됩니다. 예를 들어, 소스가 /A/B/C/MyFile.txt 이고 대상이 /X/Y/Z이면 Unified Manager는 대상에서 /X/Y/Z/A/B/C/myFile.txt라는 디렉토리 구조를 사용하여 데이터를 복원합니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 취소 *

  선택한 항목을 삭제하고 복원 대화 상자를 닫습니다.

- * 복원 *

  선택 사항을 적용하고 복원 프로세스를 시작합니다.

디렉터리 찾아보기 대화 상자

클러스터의 디렉토리에 데이터를 복원하려는 경우 디렉토리 찾아보기 대화 상자를 사용하고 원래 소스와 다른 SVM을 사용할 수 있습니다. 원본 소스 클러스터와 볼륨은 기본적으로 선택됩니다.

디렉토리 찾아보기 대화 상자에서 데이터를 복구할 클러스터, SVM, 볼륨 및 디렉토리 경로를 선택할 수 있습니다.

- * 클러스터 *

  에는 복구할 수 있는 사용 가능한 클러스터 대상이 나와 있습니다. 기본적으로 원본 소스 볼륨의 클러스터가 선택됩니다.

- * SVM 드롭다운 목록 *

  에는 선택한 클러스터에 사용 가능한 SVM이 나와 있습니다. 기본적으로 원래 소스 볼륨의 SVM이 선택됩니다.

- * 볼륨 *

  선택한 SVM에 있는 모든 읽기/쓰기 볼륨을 나열합니다. 이름 및 사용 가능한 공간으로 볼륨을 필터링할 수 있습니다. 공간이 가장 많은 볼륨은 먼저 내림차순으로 나열됩니다. 기본적으로 원본 소스 볼륨이 선택됩니다.

- * 파일 경로 텍스트 상자 *

  데이터를 복원할 파일 경로를 입력할 수 있습니다. 입력한 경로가 이미 있어야 합니다.

- * 이름 *

  선택한 볼륨에 사용 가능한 폴더의 이름을 표시합니다. 이름 목록에서 폴더를 클릭하면 하위 폴더가 표시됩니다(있는 경우). 폴더에 포함된 파일은 표시되지 않습니다. 를 클릭합니다 폴더를 선택하면 디렉토리 구조에서 한 수준 위로 이동합니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 디렉토리 선택 *

  선택 사항을 적용하고 디렉터리 찾아보기 대화 상자를 닫습니다. 선택한 디렉토리가 없으면 이 버튼이 비활성화됩니다.

- * 취소 *

  선택한 항목을 삭제하고 디렉터리 찾아보기 대화 상자를 닫습니다.

보호 구성 대화 상자

보호 구성 대화 상자를 사용하여 클러스터의 모든 읽기, 쓰기 및 데이터 보호 볼륨에 대해 SnapMirror 및 SnapVault 관계를 생성하여 소스 볼륨 또는 기본 볼륨의 데이터가 복제되도록 할 수 있습니다.

소스 탭

- * 토폴로지 뷰 *

  만들고 있는 관계를 시각적으로 표시합니다. 토폴로지의 소스는 기본적으로 강조 표시됩니다.

- * 소스 정보 *

  다음 정보를 포함하여 선택한 소스 볼륨에 대한 세부 정보를 표시합니다.

  - 소스 클러스터 이름입니다
  - 소스 SVM 이름
  - 누적 볼륨 총 크기입니다

    선택한 모든 소스 볼륨의 총 크기를 표시합니다.

  - 사용된 누적 볼륨 크기입니다

    선택한 모든 소스 볼륨의 사용된 누적 볼륨 크기를 표시합니다.

◦ 소스 볼륨

테이블에 다음 정보를 표시합니다.

▪ 소스 볼륨

선택한 소스 볼륨의 이름을 표시합니다.

▪ 유형

볼륨 유형을 표시합니다.

▪ SnapLock 유형

볼륨의 SnapLock 유형을 표시합니다. Compliance, Enterprise 및 Non-SnapLock 옵션이 있습니다.

▪ 스냅샷 복사본

기본 전송에 사용되는 스냅샷 복사본을 표시합니다. 소스 볼륨이 읽기/쓰기이면 스냅샷 복사본 열의 기본값에 새 스냅샷 복사본이 기본적으로 생성되고 기본 전송에 사용됩니다. 소스 볼륨이 데이터 보호 볼륨인 경우 스냅샷 복사본 열의 기본값 값은 새 스냅샷 복사본이 생성되지 않고 기존의 모든 스냅샷 복사본이 타겟으로 전송됨을 나타냅니다. 스냅샷 복사본 값을 클릭하면 기본 전송에 사용할 기존 스냅샷 복사본을 선택할 수 있는 스냅샷 복사본 목록이 표시됩니다. 소스 유형이 데이터 보호인 경우 다른 기본 스냅샷 복사본을 선택할 수 없습니다.

SnapMirror 탭

보호 관계를 위해 대상 클러스터, SVM(스토리지 가상 시스템), 애그리게이트를 지정할 수 있으며, SnapMirror 관계를 생성하면서 대상에 대한 명명 규칙을 지정할 수 있습니다. SnapMirror 정책 및 스케줄도 지정할 수 있습니다.

- * 토폴로지 뷰 *

  만들고 있는 관계를 시각적으로 표시합니다. 토폴로지에서 SnapMirror 대상 리소스가 기본적으로 강조 표시됩니다.

- * 목적지 정보 *

  보호 관계를 위한 대상 리소스를 선택할 수 있습니다.

  ◦ 고급 링크

  SnapMirror 관계를 작성할 때 고급 대상 설정 대화 상자를 시작합니다.

  ◦ 클러스터

  에는 보호 대상 호스트로 사용할 수 있는 클러스터가 나와 있습니다. 이 필드는 필수입니다.

  ◦ 스토리지 가상 시스템(SVM)

  에는 선택한 클러스터에서 사용할 수 있는 SVM이 나와 있습니다. SVM 목록이 채워지기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다.

  ◦ 집계

에는 선택한 SVM에서 사용 가능한 애그리게이트가 나와 있습니다. Aggregate 목록이 채워지기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다. 집계 목록에는 다음 정보가 표시됩니다.

- 순위

  여러 애그리게이트가 목적지의 모든 요구사항을 충족할 경우, 랭킹은 다음 조건에 따라 Aggregate가 나열된 우선순위를 나타냅니다.

  A. 장애 도메인 분리를 설정하려면 소스 볼륨 노드와 다른 노드에 있는 애그리게이트를 사용하는 것이 좋습니다.

  B. 볼륨의 수가 더 적은 노드의 aggregate는 클러스터의 노드 간에 로드 밸런싱을 지원하는 데 선호됩니다.

  C. 용량 밸런싱을 위해 다른 애그리게이트보다 여유 공간이 더 많은 애그리게이트가 선호됩니다. 1순위는 3가지 기준에 따라 가장 선호됨을 의미합니다.

- 애그리게이트 이름

  애그리게이트의 이름입니다

- 가용 용량
- Aggregate에서 데이터에 사용 가능한 공간입니다
- 리소스 풀

  Aggregate가 속한 리소스 풀의 이름입니다

◦ 명명 규칙

대상 볼륨에 적용되는 기본 명명 규칙을 지정합니다. 제공된 명명 규칙을 수락하거나 사용자 지정 명명 규칙을 만들 수 있습니다. 명명 규칙은 %C, %M, %V 및 %N과 같은 속성을 가질 수 있습니다. 여기서 %C는 클러스터 이름이고, %M은 SVM 이름이고, %V는 소스 볼륨이고, %N은 토폴로지 대상 노드 이름입니다.

입력한 이름이 올바르지 않으면 명명 규칙 필드가 빨간색으로 강조 표시됩니다. "미리 보기 이름" 링크를 클릭하면 입력한 명명 규칙의 미리 보기가 표시되며 텍스트 필드에 명명 규칙을 입력하면 미리 보기 텍스트가 동적으로 업데이트됩니다. 관계가 생성될 때 001에서 999 사이의 접미사가 대상 이름에 추가되고, 미리 보기 텍스트에 표시되는 nnn이 먼저 할당된 001, 할당된 002 등으로 대치됩니다.

- * 관계 설정 *

보호 관계에 사용되는 최대 전송 속도, SnapMirror 정책 및 스케줄을 지정할 수 있습니다.

◦ 최대 전송 속도

네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 최대 전송 속도를 사용하지 않도록 선택하는 경우 관계 간의 기본 전송은 무제한입니다.

◦ SnapMirror 정책

관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 기본값은 DPDefault 입니다.

◦ 정책을 생성합니다

새 SnapMirror 정책을 만들고 사용할 수 있는 SnapMirror 정책 만들기 대화 상자를 시작합니다.

◦ SnapMirror 일정 을 참조하십시오

관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 사용 가능한 스케줄에는 없음, 5분, 8시간, 일별, 시간별, 매주. 기본값은 없음 으로, 관계에 연결된 일정이 없음을 나타냅니다. 일정이 없는 관계는 스토리지 서비스에 속하지 않는 한 지연 상태 값이 없습니다.

◦ 일정 생성

새 SnapMirror 일정을 만들 수 있는 일정 만들기 대화 상자를 시작합니다.

SnapVault 탭

보호 관계를 위해 2차 클러스터, SVM 및 애그리게이트를 지정할 수 있을 뿐만 아니라, SnapVault 관계를 생성하면서 2차 볼륨의 명명 규칙을 지정할 수 있습니다. SnapVault 정책 및 스케줄을 지정할 수도 있습니다.

- * 토폴로지 뷰 *

  만들고 있는 관계를 시각적으로 표시합니다. 토폴로지의 SnapVault 보조 리소스가 기본적으로 강조 표시됩니다.

- * 보조 정보 *

  보호 관계에 사용할 보조 리소스를 선택할 수 있습니다.

  ◦ 고급 링크

  고급 보조 설정 대화 상자를 시작합니다.

  ◦ 클러스터

  에는 보조 보호 호스트로 사용할 수 있는 클러스터가 나와 있습니다. 이 필드는 필수입니다.

  ◦ 스토리지 가상 시스템(SVM)

  에는 선택한 클러스터에서 사용할 수 있는 SVM이 나와 있습니다. SVM 목록이 채워지기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다.

  ◦ 집계

  에는 선택한 SVM에서 사용 가능한 애그리게이트가 나와 있습니다. Aggregate 목록이 채워지기 전에 클러스터를 선택해야 합니다. 이 필드는 필수입니다. 집계 목록에는 다음 정보가 표시됩니다.

    ▪ 순위

    여러 애그리게이트가 목적지의 모든 요구사항을 충족할 경우, 랭킹은 다음 조건에 따라 Aggregate가 나열된 우선순위를 나타냅니다.

    A. 장애 도메인 분리를 설정하려면 기본 볼륨 노드와 다른 노드에 있는 애그리게이트를 사용하는 것이 좋습니다.
    B. 볼륨의 수가 더 적은 노드의 aggregate는 클러스터의 노드 간에 로드 밸런싱을 지원하는 데 선호됩니다.
    C. 용량 밸런싱을 위해 다른 애그리게이트보다 여유 공간이 더 많은 애그리게이트가 선호됩니다. 1순위는 3가지 기준에 따라 가장 선호됨을 의미합니다.

- 애그리게이트 이름

  애그리게이트의 이름입니다

- 가용 용량
- Aggregate에서 데이터에 사용 가능한 공간입니다
- 리소스 풀

  Aggregate가 속한 리소스 풀의 이름입니다

◦ 명명 규칙

보조 볼륨에 적용되는 기본 명명 규칙을 지정합니다. 제공된 명명 규칙을 수락하거나 사용자 지정 명명 규칙을 만들 수 있습니다. 명명 규칙은 %C, %M, %V 및 %N과 같은 속성을 가질 수 있습니다. 여기서 %C는 클러스터 이름이고, %M은 SVM 이름이고, %V는 소스 볼륨이고, %N은 토폴로지 보조 노드 이름입니다.

입력한 이름이 올바르지 않으면 명명 규칙 필드가 빨간색으로 강조 표시됩니다. "미리 보기 이름" 링크를 클릭하면 입력한 명명 규칙의 미리 보기가 표시되며 텍스트 필드에 명명 규칙을 입력하면 미리 보기 텍스트가 동적으로 업데이트됩니다. 잘못된 값을 입력하면 잘못된 정보가 미리 보기 영역에 빨간색 물음표로 표시됩니다. 관계를 만들 때 보조 이름에 001에서 999 사이의 접미사가 추가되어 미리 보기 텍스트에 표시되는 nnn을 001이 먼저 할당되고 002가 두 번째로 할당된 nnn으로 바꿉니다.

- * 관계 설정 *

보호 관계에 사용되는 최대 전송 속도, SnapVault 정책 및 SnapVault 스케줄을 지정할 수 있습니다.

◦ 최대 전송 속도

네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 최대 전송 속도를 사용하지 않도록 선택하는 경우 관계 간의 기본 전송은 무제한입니다.

◦ SnapVault 정책

관계에 대한 ONTAP SnapVault 정책을 지정합니다. 기본값은 XDPDefault 입니다.

◦ 정책을 생성합니다

새 SnapVault 정책을 만들고 사용할 수 있는 SnapVault 정책 만들기 대화 상자를 시작합니다.

◦ SnapVault 일정

관계의 ONTAP SnapVault 스케줄을 지정합니다. 사용 가능한 스케줄에는 없음, 5분, 8시간, 일별, 시간별, 매주. 기본값은 없음 으로, 관계에 연결된 일정이 없음을 나타냅니다. 일정이 없는 관계는 스토리지 서비스에 속하지 않는 한 지연 상태 값이 없습니다.

◦ 일정 생성

SnapVault 일정을 만들 수 있는 일정 만들기 대화 상자를 시작합니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 취소 *

  선택한 항목을 삭제하고 보호 구성 대화 상자를 닫습니다.

- * 적용 *

  선택한 항목을 적용하고 보호 프로세스를 시작합니다.

일정 생성 대화 상자

일정 생성 대화 상자에서는 SnapMirror 및 SnapVault 관계 전송에 대한 기본 또는 고급 보호 일정을 생성할 수 있습니다. 데이터 업데이트가 자주 발생하므로 데이터 전송 빈도를 높이기 위해 새 일정을 만들거나, 데이터가 자주 변경되지 않는 경우 일정을 덜 자주 만들 수 있습니다.

SnapMirror Synchronous 관계에 대한 일정을 구성할 수 없습니다.

- * 대상 클러스터 *

  보호 구성 대화 상자의 SnapVault 탭 또는 SnapMirror 탭에서 선택한 클러스터의 이름입니다.

- 별표 이름 *

  일정에 대해 제공한 이름입니다. 일정 이름은 A ~ Z 문자, a ~ z, 0 ~ 9 및 다음 특수 문자로 구성될 수 있습니다. @#$%{캐럿} & * () _ -. 일정 이름에는 다음 문자가 포함될 수 없습니다.<>

- * 기본 또는 고급 *

  사용할 스케줄 모드입니다.

  기본 모드는 다음과 같은 요소를 포함합니다.

  ◦ 반복합니다

    예약된 전송이 수행되는 빈도. 매시간, 매일, 매주 중에서 선택할 수 있습니다.

  ◦ 일

    매주 반복 을 선택하면 전송이 이루어지는 주의 일입니다.

  ◦ 시간

    Daily(매일) 또는 Weekly(매주) 를 선택하면 전송이 이루어지는 시간.

    고급 모드에는 다음 요소가 포함됩니다.

  ◦ 개월

    월을 나타내는 쉼표로 구분된 숫자 목록입니다. 유효한 값은 0에서 11 사이의 값이며 0은 1월을 나타내는 등의

값을 나타냅니다. 이 요소는 선택 사항입니다. 필드를 비워 두면 매월 전송이 수행됩니다.

◦ 일

월을 나타내는 쉼표로 구분된 숫자 목록입니다. 유효한 값은 1부터 31까지입니다. 이 요소는 선택 사항입니다. 필드를 비워 두면 해당 월의 매일 전송이 수행됩니다.

◦ 평일

요일을 나타내는 쉼표로 구분된 숫자 목록입니다. 유효한 값은 0에서 6 사이의 값이며 0은 일요일을 나타냅니다. 이 요소는 선택 사항입니다. 필드를 비워 두면 매일 전송이 수행됨을 의미합니다. 요일을 지정했지만 요일을 지정하지 않은 경우 매일 아니라 지정된 요일에만 전송이 수행됩니다.

◦ 시간

일 시간 수를 나타내는 쉼표로 구분된 숫자 목록입니다. 유효한 값은 0부터 23까지이며 0은 자정을 나타냅니다. 이 요소는 선택 사항입니다.

◦ 분

시간 단위의 분을 나타내는 쉼표로 구분된 숫자 목록입니다. 유효한 값은 0에서 59 사이입니다. 이 요소는 필수입니다.

SnapMirror 정책 생성 대화 상자

SnapMirror 정책 만들기 대화 상자에서는 SnapMirror 전송의 우선 순위를 설정하는 정책을 만들 수 있습니다. 정책을 사용하여 소스에서 타겟으로 전송하는 전송 효율성을 극대화할 수 있습니다.

- * 대상 클러스터 *

  보호 구성 대화 상자의 SnapMirror 탭에서 선택한 클러스터의 이름입니다.

- * 대상 SVM *

  보호 구성 대화 상자의 SnapMirror 탭에서 선택한 SVM의 이름입니다.

- * 정책 이름 *

  새 정책에 대해 제공한 이름입니다. 정책 이름은 A ~ Z 문자, a ~ z, 0 ~ 9, 마침표(.), 하이픈(-), 및 밑줄(_).

- * 전송 우선순위 *

  비동기 작업에 대해 전송이 실행되는 우선 순위입니다. 보통 또는 낮음을 선택할 수 있습니다. 낮은 전송 우선 순위를 지정하는 정책이 있는 정책보다 먼저 실행되는 일반 전송 우선 순위를 지정하는 정책과의 관계를 전송합니다.

- * 설명 *

  정책에 대한 설명을 추가할 수 있는 선택적 필드입니다.

- * 전송 재시작 *

  중단 작업 또는 네트워크 중단과 같은 장애 유형에 의해 전송이 중단될 때 수행할 재시작 작업을 나타냅니다. 다음 중

하나를 선택할 수 있습니다.

◦ 항상

전송을 다시 시작하기 전에 새 스냅샷 복사본이 생성되도록 지정한 다음, 새 스냅샷 복사본이 있는 경우 체크포인트에서 전송이 재시작되고 새로 생성된 스냅샷 복사본에서 증분 전송이 수행됩니다.

◦ 안 함

중단된 전송을 다시 시작하지 않도록 지정합니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 취소 *

  선택한 항목을 삭제하고 보호 구성 대화 상자를 닫습니다.

- * 적용 *

  선택 사항을 적용하고 보호 프로세스를 시작합니다.

SnapVault 정책 생성 대화 상자

SnapVault 정책 생성 대화 상자에서는 SnapVault 전송의 우선 순위를 설정하는 정책을 생성할 수 있습니다. 정책을 사용하여 운영 볼륨에서 2차 볼륨으로 전송하는 효율성을 극대화할 수 있습니다.

- * 대상 클러스터 *

  보호 구성 대화 상자의 SnapVault 탭에서 선택한 클러스터의 이름입니다.

- * 대상 SVM *

  보호 구성 대화 상자의 SnapVault 탭에서 선택한 SVM의 이름입니다.

- * 정책 이름 *

  새 정책에 대해 제공한 이름입니다. 정책 이름은 A ~ Z 문자, a ~ z, 0 ~ 9, 마침표(.), 하이픈(-), 및 밑줄(_).

- * 전송 우선순위 *

  전송이 실행되는 우선 순위입니다. 보통 또는 낮음을 선택할 수 있습니다. 낮은 전송 우선 순위를 지정하는 정책이 있는 정책보다 먼저 실행되는 일반 전송 우선 순위를 지정하는 정책과의 관계를 전송합니다. 기본 설정은 보통입니다.

- * 설명 *

  SnapVault 정책에 대해 최대 255자의 주석을 추가할 수 있는 선택적 필드입니다.

- * 액세스 시간 무시 *

  액세스 시간만 변경된 파일에 대해 증분 전송을 무시할지 여부를 지정합니다.

- * 복제 레이블 *

  테이블에 특정 복제 라벨이 정책에 포함된 ONTAP에서 선택한 스냅샷 복사본과 관련된 규칙이 나열되어 있습니다. 다음 정보 및 작업도 사용할 수 있습니다.

  - 명령 버튼

    명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

    - 추가

      스냅샷 복사본 레이블 및 보존 개수를 생성할 수 있습니다.

    - 보존 개수를 편집합니다

      기존 스냅샷 복사본 레이블의 보존 수를 변경할 수 있습니다. 보존 수는 1에서 251 사이의 숫자여야 합니다. 모든 규칙에 대한 모든 보존 수의 합계는 251을 초과할 수 없습니다.

    - 삭제

      기존 스냅샷 복사본 레이블을 삭제할 수 있습니다.

  - 스냅샷 복사본 레이블

    스냅샷 복사본 레이블을 표시합니다. 로컬 스냅샷 복사본 정책이 동일한 볼륨을 하나 이상 선택하면 정책의 각 레이블에 대한 항목이 표시됩니다. 둘 이상의 로컬 스냅샷 복사본 정책이 있는 볼륨을 여러 개 선택하면 모든 정책의 모든 레이블이 테이블에 표시됩니다

  - 스케줄

    각 스냅샷 복사본 레이블과 연결된 스케줄을 표시합니다. 레이블에 둘 이상의 일정이 연결되어 있는 경우 해당 레이블의 일정이 쉼표로 구분된 목록에 표시됩니다. 레이블이 같지만 스케줄이 다른 볼륨을 여러 개 선택한 경우 스케줄에는 ""다양한""이 표시되어 둘 이상의 스케줄이 선택한 볼륨과 연결되어 있음을 나타냅니다.

  - 대상 보존 수입니다

    지정된 레이블이 SnapVault 보조 이미지에 유지되는 스냅샷 복사본의 수를 표시합니다. 일정이 여러 개인 레이블의 보존 수에는 각 레이블 및 일정 쌍의 보존 수가 표시됩니다. 둘 이상의 로컬 스냅샷 복사본 정책이 있는 볼륨을 여러 개 선택하면 보존 카운트가 비어 있습니다.

관계 편집 대화 상자

기존 보호 관계를 편집하여 최대 전송 속도, 보호 정책 또는 보호 스케줄을 변경할 수 있습니다.

목적지 정보

- * 대상 클러스터 *

선택한 대상 클러스터의 이름입니다.

- * 대상 SVM *

  선택한 SVM의 이름입니다

- * 관계 설정 *

  보호 관계에 사용되는 최대 전송 속도, SnapMirror 정책 및 스케줄을 지정할 수 있습니다.

  - 최대 전송 속도

    네트워크를 통해 클러스터 간에 기본 데이터가 전송되는 최대 속도를 지정합니다. 이 옵션을 선택하면 네트워크 대역폭이 지정한 값으로 제한됩니다. 숫자 값을 입력한 다음 초당 킬로바이트(kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps) 또는 초당 테라바이트(Tbps)를 선택할 수 있습니다. 지정하는 최대 전송 속도는 1kbps 이상, 4Tbps 미만이어야 합니다. 최대 전송 속도를 사용하지 않도록 선택하는 경우 관계 간의 기본 전송은 무제한입니다. 운영 클러스터와 보조 클러스터가 동일한 경우 이 설정이 비활성화됩니다.

  - SnapMirror 정책

    관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 기본값은 DPDefault 입니다.

  - 정책을 생성합니다

    새 SnapMirror 정책을 만들고 사용할 수 있는 SnapMirror 정책 만들기 대화 상자를 시작합니다.

  - SnapMirror 일정 을 참조하십시오

    관계에 대한 ONTAP SnapMirror 정책을 지정합니다. 사용 가능한 스케줄에는 없음, 5분, 8시간, 일별, 시간별, 매주. 기본값은 없음 으로, 관계에 연결된 일정이 없음을 나타냅니다. 일정이 없는 관계는 스토리지 서비스에 속하지 않는 한 지연 상태 값이 없습니다.

  - 일정 생성

    새 SnapMirror 일정을 만들 수 있는 일정 만들기 대화 상자를 시작합니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 취소 *

  선택한 항목을 삭제하고 보호 구성 대화 상자를 닫습니다.

- * 제출 *

  선택 사항을 적용하고 관계 편집 대화 상자를 닫습니다.

초기화/업데이트 대화 상자

Initialize/Update 대화 상자를 사용하면 새 보호 관계에 대해 초기 계획을 처음 전송할 수도 있고, 이미 초기화된 상태에서 수동으로 예정되지 않은 증분 업데이트를 수행하려는 경우 관계를

업데이트할 수도 있습니다.

전송 옵션 탭

전송 옵션 탭에서는 전송의 초기화 우선 순위를 변경하고 전송 중에 사용되는 대역폭을 변경할 수 있습니다.

- * 전송 우선순위 *

  전송이 실행되는 우선 순위입니다. 보통 또는 낮음을 선택할 수 있습니다. 낮은 전송 우선 순위를 지정하는 정책보다 먼저 일반 전송 우선 순위를 지정하는 정책과의 관계. 기본적으로 보통이 선택되어 있습니다.

- * 최대 전송 속도 *

  네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 최대 전송 속도를 사용하지 않도록 선택하는 경우 관계 간의 기본 전송은 무제한입니다. 최대 전송 속도가 서로 다른 여러 관계를 선택한 경우 다음 최대 전송 속도 설정 중 하나를 지정할 수 있습니다.

  - 개별 관계를 설정하거나 편집하는 동안 지정된 값을 사용합니다

    이 옵션을 선택하면 초기화 및 업데이트 작업에서 각 관계의 생성 또는 편집 시 지정된 최대 전송 속도를 사용합니다. 이 필드는 전송 속도가 다른 여러 관계가 초기화되거나 업데이트되는 경우에만 사용할 수 있습니다.

  - 무제한

    관계 간 전송에 대한 대역폭 제한이 없음을 나타냅니다. 이 필드는 전송 속도가 다른 여러 관계가 초기화되거나 업데이트되는 경우에만 사용할 수 있습니다.

  - 대역폭 제한

    이 옵션을 선택하면 네트워크 대역폭이 지정한 값으로 제한됩니다. 숫자 값을 입력한 다음 초당 킬로바이트(kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps) 또는 초당 테라바이트(Tbps)를 선택할 수 있습니다. 지정하는 최대 전송 속도는 1kbps 이상, 4Tbps 미만이어야 합니다.

소스 **Snapshot** 복사본 탭

소스 스냅샷 복사본 탭에는 기본 전송에 사용되는 소스 스냅샷 복사본에 대한 다음 정보가 표시됩니다.

- * 소스 볼륨 *

  해당 소스 볼륨의 이름을 표시합니다.

- * 대상 볼륨 *

  선택한 대상 볼륨의 이름을 표시합니다.

- * 소스 유형 *

  볼륨 유형을 표시합니다. 유형은 읽기/쓰기 또는 데이터 보호 중 하나일 수 있습니다.

- * 스냅샷 복사본 *

  데이터 전송에 사용되는 스냅샷 복사본을 표시합니다. 스냅샷 복사본 값을 클릭하면 현재 사용 중인 보호 관계 유형과 수행 중인 작업에 따라 전송할 특정 스냅샷 복사본을 선택할 수 있는 소스 스냅샷 복사본 선택 대화 상자가

표시됩니다. 다른 스냅샷 복사본을 지정하는 옵션은 데이터 보호 유형 소스에 사용할 수 없습니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 취소 *

  선택 사항을 취소하고 초기화/업데이트 대화 상자를 닫습니다.

- * 제출 *

  선택 사항을 저장하고 초기화 또는 업데이트 작업을 시작합니다.

대화 상자를 다시 동기화합니다

재동기화 대화 상자를 사용하면 이전에 중단된 SnapMirror 또는 SnapVault 관계의 데이터를 재동기화한 다음 대상이 읽기/쓰기 볼륨으로 만들어진 후에 다시 동기화할 수 있습니다. 소스 볼륨에서 필요한 공통 스냅샷 복사본이 삭제되어 SnapMirror 또는 SnapVault 업데이트가 실패하는 경우에도 재동기화할 수 있습니다.

재동기화 옵션 탭

재동기화 옵션 탭에서는 재동기화하려는 보호 관계에 대한 전송 우선 순위 및 최대 전송 속도를 설정할 수 있습니다.

- * 전송 우선순위 *

  전송이 실행되는 우선 순위입니다. 보통 또는 낮음을 선택할 수 있습니다. 낮은 전송 우선 순위를 지정하는 정책이 있는 정책보다 먼저 일반 전송 우선 순위를 지정하는 정책과의 관계입니다.

- * 최대 전송 속도 *

  네트워크를 통해 클러스터 간에 데이터가 전송되는 최대 속도를 지정합니다. 이 옵션을 선택하면 네트워크 대역폭이 지정한 값으로 제한됩니다. 숫자 값을 입력한 다음 킬로바이트/초(kbps), 초당 메가바이트(Mbps), 초당 기가바이트(Gbps) 또는 Tbps를 선택할 수 있습니다. 최대 전송 속도를 사용하지 않도록 선택하는 경우 관계 간의 기본 전송은 무제한입니다.

소스 **Snapshot** 복사본 탭

소스 스냅샷 복사본 탭에는 기본 전송에 사용되는 소스 스냅샷 복사본에 대한 다음 정보가 표시됩니다.

- * 소스 볼륨 *

  해당 소스 볼륨의 이름을 표시합니다.

- * 대상 볼륨 *

  선택한 대상 볼륨의 이름을 표시합니다.

- * 소스 유형 *

읽기/쓰기 또는 데이터 보호와 같은 볼륨 유형을 표시합니다.

- * 스냅샷 복사본 *

  데이터 전송에 사용되는 스냅샷 복사본을 표시합니다. 스냅샷 복사본 값을 클릭하면 현재 사용 중인 보호 관계 유형과 수행 중인 작업에 따라 전송할 특정 스냅샷 복사본을 선택할 수 있는 소스 스냅샷 복사본 선택 대화 상자가 표시됩니다.

명령 버튼

- * 제출 *

  재동기화 프로세스를 시작하고 재동기화 대화 상자를 닫습니다.

- * 취소 *

  선택 사항을 취소하고 재동기화 대화 상자를 닫습니다.

소스 스냅샷 복사본 대화 상자를 선택합니다

소스 스냅샷 복사본 선택 대화 상자를 사용하여 보호 관계 간에 데이터를 전송할 특정 스냅샷 복사본을 선택하거나 기본 동작을 선택할 수 있습니다. 기본 동작은 관계를 초기화, 업데이트 또는 재동기화할지 여부 및 관계가 SnapMirror인지 SnapVault인지 여부에 따라 달라집니다.

기본값

SnapVault 및 SnapMirror 관계의 전송을 초기화, 업데이트 및 재동기화하는 데 사용할 스냅샷 복사본을 결정하는 기본 동작을 선택할 수 있습니다.

SnapVault 전송을 수행하는 경우 각 작업의 기본 동작은 다음과 같습니다.

작동	소스가 읽기/쓰기입니다 **SnapVault**	소스가 데이터 보호**(DP)**일 때의 기본 **SnapVault** 동작
초기화	새 스냅샷 복사본을 생성하고 전송합니다.	마지막으로 내보낸 스냅샷 복사본을 전송합니다.
업데이트	정책에 지정된 대로 레이블이 지정된 Snapshot 복사본만 전송합니다.	마지막으로 내보낸 스냅샷 복사본을 전송합니다.
재동기화	는 최신 공통 스냅샷 복사본 이후에 생성된 레이블이 지정된 모든 스냅샷 복사본을 전송합니다.	레이블이 지정된 최신 스냅샷 복사본을 전송합니다.

SnapMirror 전송을 수행하는 경우 각 작업의 기본 동작은 다음과 같습니다.

작동	기본 **SnapMirror** 동작입니다	**SnapMirror**와 **SnapMirror** 캐스케이드의 두 번째 홉이면 기본 **SnapMirror** 동작입니다
초기화	새 스냅샷 복사본을 생성하고 이 복사본과 새 스냅샷 복사본 이전에 생성된 모든 스냅샷 복사본을 전송합니다.	모든 스냅샷 복사본을 소스에서 전송
업데이트	새 스냅샷 복사본을 생성하고 이 복사본과 새 스냅샷 복사본 이전에 생성된 모든 스냅샷 복사본을 전송합니다.	모든 스냅샷 복사본을 전송합니다.
재동기화	새 스냅샷 복사본을 생성한 다음 소스에서 모든 스냅샷 복사본을 전송합니다.	2차 볼륨에서 3차 볼륨으로 모든 스냅샷 복사본을 전송하고, 최신 공통 스냅샷 복사본을 생성한 후 추가한 모든 데이터를 삭제합니다.

기존 스냅샷 복사본

해당 작업에 스냅샷 복사본을 선택할 수 있는 경우 목록에서 기존 스냅샷 복사본을 선택할 수 있습니다.

- * 스냅샷 복사본 *

  전송을 위해 선택할 수 있는 기존 스냅샷 복사본을 표시합니다.

- * 만든 날짜 *

  스냅샷 복사본이 생성된 날짜와 시간을 표시합니다. 스냅샷 복사본은 가장 최근 항목 부터 가장 최근 항목, 가장 최근 항목 목록 맨 위에 나열됩니다.

SnapVault 전송을 수행 중인 경우 소스에서 타겟으로 전송할 기존 스냅샷 복사본을 선택하려면 각 작업에 대한 동작은 다음과 같습니다.

작동	스냅샷 복사본을 지정할 때의 **SnapVault** 동작	계단식 배열 내 스냅샷 복사본을 지정할 때의 **SnapVault** 동작
초기화	지정된 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에 대해서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
업데이트	지정된 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에 대해서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
재동기화	선택한 스냅샷 복사본을 전송합니다.	데이터 보호 볼륨에 대해서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.

SnapMirror 전송을 수행 중인 경우 소스에서 타겟으로 전송할 기존 스냅샷 복사본을 선택하려면 각 작업에 대한 동작은 다음과 같습니다.

작동	스냅샷 복사본을 지정할 때의 **SnapMirror** 동작	계단식 배열 스냅샷 복사본을 지정할 때의 **SnapMirror** 동작
초기화	소스의 모든 스냅샷 복사본을 지정된 스냅샷 복사본으로 전송합니다.	데이터 보호 볼륨에 대해서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
업데이트	소스의 모든 스냅샷 복사본을 지정된 스냅샷 복사본으로 전송합니다.	데이터 보호 볼륨에 대해서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.
재동기화	소스에서 선택한 스냅샷 복사본으로 모든 스냅샷 복사본을 전송한 다음, 최신 공통 스냅샷 복사본을 생성한 후 추가한 데이터를 삭제합니다.	데이터 보호 볼륨에 대해서는 소스 스냅샷 복사본 선택이 지원되지 않습니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 제출 *

  선택 항목을 제출하고 소스 스냅샷 복사본 선택 대화 상자를 닫습니다.

- * 취소 *

  선택한 내용을 취소하고 소스 스냅샷 복사본 선택 대화 상자를 닫습니다.

역방향 재동기화 대화 상자

소스 볼륨이 비활성화되어 있고 대상이 읽기/쓰기 볼륨으로 설정되었기 때문에 보호 관계가 끊어진 경우, 역방향 재동기화를 통해 대상이 새 소스가 되고 소스가 새 대상이 될 수 있도록 관계의 방향을 바꿀 수 있습니다.

재해로 인해 보호 관계의 소스 볼륨이 비활성화되면 대상 볼륨을 사용하여 소스를 복구 또는 교체하고 소스를 업데이트하고 관계를 다시 설정하는 동안 데이터를 읽기/쓰기로 변환하여 데이터를 제공할 수 있습니다. 역재동기화 작업을 수행하면 공통 스냅샷 복사본의 데이터보다 최신 소스의 데이터가 삭제됩니다.

다시 동기화하기 전

역방향 재동기화 작업 전에 관계의 소스와 대상을 표시합니다.

- * 소스 볼륨 *

  역재동기화 작업 전의 소스 볼륨의 이름 및 위치입니다.

- * 대상 볼륨 *

역방향 재동기화 작업 전의 대상 볼륨의 이름 및 위치입니다.

역재동기화 후

예약 재동기화 작업 후 관계의 소스 및 대상을 표시합니다.

- * 소스 볼륨 *

  역재동기화 작업 후 소스 볼륨의 이름 및 위치입니다.

- * 대상 볼륨 *

  역방향 재동기화 작업 후 대상 볼륨의 이름 및 위치입니다.

명령 버튼

명령 단추를 사용하여 다음 작업을 수행할 수 있습니다.

- * 제출 *

  역방향 재동기화 프로세스를 시작합니다.

- * 취소 *

  역방향 재동기화 작업을 시작하지 않고 역방향 재동기화 대화 상자를 닫습니다.

관계**:** 모든 관계 보기

관계: 모든 관계 보기에는 스토리지 시스템의 보호 관계에 대한 정보가 표시됩니다.

기본적으로 관계 페이지에 액세스할 때 표시되는 보고서에는 볼륨 및 스토리지 VM 모두에 대한 최상위 보호 관계가 포함됩니다. 페이지 위쪽에 있는 컨트롤을 사용하면 특정 보기를 선택하고, 검색을 수행하여 특정 개체를 찾고, 필터를 만들어 적용하여 표시된 데이터 목록의 범위를 좁히고, 페이지에서 열을 추가/제거/재정렬하고, 페이지의 데이터를 .csv, .pdf, 또는 .xlsx 파일. 페이지를 사용자 지정한 후 결과를 사용자 정의 보기로 저장한 다음 이 데이터의 보고서를 정기적으로 생성 및 이메일로 전송할 수 있습니다. 기본적으로 * 관계 * 메뉴를 선택하면 데이터 센터에 있는 볼륨 및 스토리지 VM에 대한 보호 관계가 표시된 보고서에 포함됩니다. Filter * 옵션을 사용하면 볼륨 또는 스토리지 VM만 등 선택한 스토리지 시스템만 볼 수 있습니다. 동일한 보고서가 스토리지 페이지와 선택한 스토리지 엔티티에 대해서만 표시됩니다. 볼륨 또는 스토리지 VM 관계를 보려면 * 스토리지 * > * 볼륨 * > * 관계: 모든 관계 * 페이지에 액세스하거나 * 보호 * > * 관계 * > * 관계: 모든 관계 * 를 선택하고 * 필터 * 의 * 관계 객체 유형 * 옵션을 사용하여 볼륨 또는 스토리지 VM 데이터만 필터링합니다.

모든 보호 관계를 나열하는 관계 페이지에는 ONTAP 시스템 관리자에서 동일한 개체를 볼 수 있도록 하는 대상 클러스터에 대한 * 시스템 관리자 * 의 보기 링크가 있습니다.

- * 상태 *

  보호 관계의 현재 상태를 표시합니다.

  상태는 오류(), 경고() 또는 OK()를 클릭합니다.

- * 소스 스토리지 VM *

소스 SVM의 이름을 표시합니다. SVM 이름을 클릭하여 소스 SVM에 대한 자세한 정보를 확인할 수 있습니다.

SVM이 클러스터에 있지만 Unified Manager 인벤토리에 아직 추가되지 않았거나 클러스터의 마지막 업데이트 후 SVM이 생성된 경우 이 필드가 비어 있습니다. SVM이 있는지 확인하거나 클러스터에서 재검색을 수행하여 리소스 목록을 새로 고쳐야 합니다.

- * 출처 *

  선택한 항목에 따라 보호되는 소스 볼륨 또는 소스 스토리지 VM을 표시합니다. 볼륨 또는 스토리지 VM 이름을 클릭하여 소스 볼륨 또는 스토리지 VM에 대한 자세한 정보를 볼 수 있습니다.

  "Resource-key not discovered(리소스-키가 검색되지 않음)" 메시지가 표시되면 클러스터에 볼륨이 있지만 Unified Manager 인벤토리에 아직 추가되지 않았거나 클러스터의 마지막 새로 고침 후 볼륨이 생성되었음을 나타내는 것일 수 있습니다. 볼륨이 있는지 확인하거나 클러스터에서 재검색을 수행하여 리소스 목록을 새로 고쳐야 합니다.

- * 대상 스토리지 VM *

  대상 SVM의 이름을 표시합니다. SVM 이름을 클릭하여 대상 SVM에 대한 자세한 정보를 확인할 수 있습니다.

- * 목적지 *

  선택한 사항에 따라 대상 볼륨 또는 스토리지 VM의 이름을 표시합니다. 해당 오브젝트 이름을 클릭하여 대상 볼륨 또는 스토리지 VM에 대한 자세한 정보를 볼 수 있습니다.

- * 관계 객체 유형 *

  스토리지 VM, 볼륨 및 정합성 보장 그룹과 같이 관계에 사용되는 개체의 유형을 표시합니다. 정합성 보장 관계에 있는 개체의 경우 관계 소스와 대상에서 정합성 보장 그룹을 표시하고 이 그룹을 클릭하면 LUN 페이지로 이동하여 관계를 볼 수 있습니다.

- * 정책 *

  SnapMirror 관계에 대한 보호 정책의 이름을 표시합니다. 정책 이름을 클릭하면 다음 정보를 포함하여 해당 정책과 관련된 세부 정보를 볼 수 있습니다.

  - 전송 우선 순위

    비동기 작업에 대해 전송이 실행되는 우선 순위를 지정합니다. 전송 우선 순위는 보통 또는 낮음입니다. 우선 순위가 낮은 전송 전에 일반 우선 순위 전송이 예약됩니다. 기본값은 보통입니다.

  - 액세스 시간 무시

    SnapVault 관계에만 적용됩니다. 이 옵션은 액세스 시간이 변경된 파일을 증분 전송에서 무시할지 여부를 지정합니다. 값은 True 또는 False입니다. 기본값은 False입니다.

  - 관계가 동기화되지 않았을 때

    동기식 관계를 동기화할 수 없을 때 ONTAP가 수행하는 작업을 지정합니다. StrictSync 관계는 보조 볼륨과 동기화하지 못할 경우 운영 볼륨에 대한 액세스를 제한합니다. 동기화 관계는 보조 시스템과 동기화하지 못할 경우 기본 데이터에 대한 액세스를 제한하지 않습니다.

  - 시도 횟수 제한

SnapMirror 관계에 대해 각 수동 또는 예약된 전송을 시도할 최대 횟수를 지정합니다. 기본값은 8입니다.

- 설명

  선택한 정책에 대한 설명을 위한 텍스트 필드를 제공합니다.

- SnapMirror 레이블

  스냅샷 복사본 정책과 연결된 첫 번째 스케줄에 대한 SnapMirror 레이블을 지정합니다. SnapMirror 레이블은 SnapVault 하위 시스템에서 SnapVault 대상에 스냅샷 복사본을 백업할 때 사용됩니다.

- 보존 설정입니다

  백업 시간이나 수에 따라 백업 보관 기간을 지정합니다.

- 실제 Snapshot 복사본

  지정된 레이블과 일치하는 이 볼륨의 스냅샷 복사본 수를 지정합니다.

- Snapshot 복사본 유지

  정책에 대한 최대 제한에 도달하더라도 자동으로 삭제되지 않는 SnapVault 스냅샷 복사본의 수를 지정합니다. 값은 True 또는 False입니다. 기본값은 False입니다.

- 보존 경고 임계값

  최대 보존 제한에 거의 도달했음을 나타내기 위해 경고를 보내는 스냅샷 복사본 제한을 지정합니다.

- * 지연 기간 *

  미러의 데이터가 소스 뒤에 걸리는 시간을 표시합니다.

  지연 기간은 StrictSync 관계에 대해 0초와 같거나 같아야 합니다.

- * 지연 상태 *

  관리 관계에 대한 지연 상태와 해당 관계와 연결된 일정이 있는 관리되지 않는 관계에 대한 지연 상태를 표시합니다. 지연 상태는 다음과 같습니다.

  - 오류

    지연 기간이 지연 오류 임계값보다 크거나 같습니다.

  - 경고

    지연 기간이 지연 경고 임계값보다 크거나 같습니다.

  - 좋습니다

    지연 기간이 정상 한계 내에 있습니다.

  - 해당 없음

지연 상태는 일정을 구성할 수 없기 때문에 동기식 관계에 적용할 수 없습니다.

- * 마지막으로 성공한 업데이트 *

  마지막으로 성공한 SnapMirror 또는 SnapVault 작업의 시간을 표시합니다.

  마지막으로 성공한 업데이트는 동기 관계에 적용되지 않습니다.

- * 구성 관계 *

  선택한 객체에 볼륨이 있는지 여부를 표시합니다.

- * 관계 유형 *

  볼륨을 복제하는 데 사용되는 관계 유형을 표시합니다. 관계 유형은 다음과 같습니다.

  - 비동기식 미러
  - 비동기식 볼트
  - 비동기 MirrorVault
  - StrictSync를 선택합니다
  - 동기화

- * 전송 상태 *

  보호 관계에 대한 전송 상태를 표시합니다. 전송 상태는 다음 중 하나일 수 있습니다.

  - 중단 중

    SnapMirror 전송이 사용하도록 설정되어 있지만 체크포인트 제거가 포함된 전송 중단 작업이 진행 중입니다.

  - 확인 중입니다

    대상 볼륨에 진단 검사가 진행 중이며 전송이 진행 중입니다.

  - 마무리 중입니다

    SnapMirror 전송이 사용하도록 설정되었습니다. 이 볼륨은 현재 증분 SnapVault 전송을 위한 전송 후 단계에 있습니다.

  - 유휴

    전송이 활성화되고 진행 중인 전송이 없습니다.

  - In-Sync(동기화 중)

    동기 관계에 있는 두 볼륨의 데이터가 동기화됩니다.

  - 동기화 중단

    대상 볼륨의 데이터가 소스 볼륨과 동기화되지 않습니다.

- 준비 중

  SnapMirror 전송이 사용하도록 설정되었습니다. 볼륨은 현재 증분 SnapVault 전송을 위한 전송 전 단계에 있습니다.

- 대기열에 있습니다

  SnapMirror 전송이 사용하도록 설정되었습니다. 진행 중인 전송이 없습니다.

- 정지되었습니다

  SnapMirror 전송이 비활성화되었습니다. 진행 중인 전송이 없습니다.

- 정지 중

  SnapMirror 전송이 진행 중입니다. 추가 전송이 비활성화됩니다.

- 전송 중입니다

  SnapMirror 전송이 설정되고 전송 중입니다.

- 전환 중

  소스에서 대상 볼륨으로 데이터를 비동기적으로 전송하는 작업이 완료되고 동기식 작업으로 전환이 시작되었습니다.

- 대기 중

  SnapMirror 전송이 시작되었지만 연결된 일부 작업이 대기 중입니다.

- * 마지막 전송 기간 *

  마지막 데이터 전송을 완료하는 데 걸린 시간을 표시합니다.

  전송이 동시에 이루어져야 하므로 전송 기간은 StrictSync 관계에 적용되지 않습니다.

- * 마지막 전송 크기 *

  마지막 데이터 전송의 크기(바이트)를 표시합니다.

  전송 크기는 StrictSync 관계에 적용되지 않습니다.

- * 중개자 *

  중재자 상태를 표시합니다.

  - 해당 없음

    클러스터에서 SnapMirror 비즈니스 연속성을 지원하지 않는 경우

  - 구성되지 않았습니다

    구성되어 있지 않거나, 구성되어 있지만 대상 클러스터만 추가되고 소스 클러스터가 Unified Manager에

추가되지 않은 경우

◦ 중재자 IP 주소

구성되어 있고 소스 클러스터와 대상 클러스터가 Unified Manager에 모두 추가됩니다.

- * 시/도 *

  SnapMirror 또는 SnapVault 관계의 상태를 표시합니다. 상태는 Uninitialized, SnapMired 또는 Broken-Off 일 수 있습니다. 소스 볼륨을 선택하면 관계 상태가 적용되지 않고 표시되지 않습니다.

- * 관계 상태 *

  클러스터의 관계 상태 정보를 표시합니다.

- * 비정상적인 이유 *

  관계가 좋지 않은 상태에 있는 이유.

- * 전송 우선순위 *

  전송이 실행되는 우선 순위를 표시합니다. 전송 우선 순위는 보통 또는 낮음입니다. 우선 순위가 낮은 전송 전에 일반 우선 순위 전송이 예약됩니다.

  모든 전송이 동일한 우선 순위로 처리되기 때문에 전송 우선 순위는 동기 관계에 적용되지 않습니다.

- 별표 *

  관계에 할당된 보호 스케줄의 이름을 표시합니다.

  동기식 관계에는 일정이 적용되지 않습니다.

- * 버전에 상관없이 유연하게 복제 *

  백업 옵션과 함께 예, 예 또는 없음을 표시합니다.

- * 소스 클러스터 *

  SnapMirror 관계에 대한 소스 클러스터의 FQDN, 짧은 이름 또는 IP 주소를 표시합니다.

- * 소스 클러스터 FQDN *

  SnapMirror 관계에 대한 소스 클러스터의 이름을 표시합니다.

- * 소스 노드 *

  볼륨의 SnapMirror 관계에 대한 소스 노드 이름 링크 이름을 표시하고 객체가 스토리지 VM 또는 정합성 보장 그룹일 경우 SnapMirror 관계 노드 수 링크를 표시합니다.

사용자 지정 뷰에서 노드 이름 링크를 클릭하면 SM-BC 관계에 속하는 해당 정합성 보장 그룹의 볼륨이 있는 스토리지 객체에 대한 보호를 확인하고 확장할 수 있습니다.

노드 수 링크를 클릭하면 해당 관계와 연결된 각 노드가 있는 노드 페이지로 이동됩니다. 노드 수가 0이면 관계에 연결된

노드가 없으므로 값이 표시되지 않습니다.

- * 대상 노드 *

  볼륨의 SnapMirror 관계에 대한 대상 노드 이름 링크의 이름을 표시하고, 개체가 스토리지 VM 또는 일관성 그룹인 경우 SnapMirror 관계 노드 수 링크를 표시합니다.

  노드 수 링크를 클릭하면 해당 관계와 연결된 각 노드가 있는 노드 페이지로 이동됩니다. 노드 수가 0이면 관계에 연결된 노드가 없으므로 값이 표시되지 않습니다.

- * 대상 클러스터 *

  SnapMirror 관계에 대한 대상 클러스터의 이름을 표시합니다.

- * 대상 클러스터 FQDN *

  SnapMirror 관계에 대한 대상 클러스터의 FQDN, 짧은 이름 또는 IP 주소를 표시합니다.

- * 보호 대상 *

  다른 관계를 표시합니다. 이 열에서 클러스터 및 스토리지 가상 머신 순서에 대한 볼륨 및 정합성 보장 그룹 관계를 볼 수 있습니다. 여기에는 다음이 포함됩니다.

  - SnapMirror를 참조하십시오
  - 스토리지 VM DR
  - SnapMirror, 스토리지 VM DR
  - 정합성 보장 그룹
  - SnapMirror, 일관성 그룹:

- 관련 정보 *
- 관계:MetroCluster* 보기에 대한 자세한 내용은 을 참조하십시오 "MetroCluster 구성 모니터링".
- 관계: 지난 1개월 전송 상태* 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 최근 1개월 전송 상태 보기".
- 관계: 모든 관계 * 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 최근 1개월 전송 속도 보기".

관계**:** 최근 **1**개월 전송 상태 보기

관계: 지난 1개월 전송 상태 보기를 사용하면 비동기 관계의 볼륨 및 스토리지 VM에 대한 일정 기간 동안의 전송 추세를 분석할 수 있습니다. 이 페이지에는 전송이 성공 또는 실패인지 여부도 표시됩니다.

페이지 위쪽에 있는 컨트롤을 사용하면 특정 개체를 찾고, 필터를 만들고, 적용하여 표시된 데이터 목록의 범위를 좁히고, 페이지에서 열을 추가/제거/재정렬하고, 페이지의 데이터를 ".csv", ".pdf" 또는 ".xlsx" 파일로 내보낼 수 있습니다. 페이지를 사용자 지정한 후 결과를 사용자 정의 보기로 저장한 다음 이 데이터의 보고서를 정기적으로 생성 및 이메일로 전송할 수 있습니다. Filter * 옵션을 사용하면 볼륨 또는 스토리지 VM과 같이 선택한 스토리지 시스템만 볼 수 있습니다. 동일한 보고서가 스토리지 페이지와 선택한 스토리지 엔티티에 대해서만 표시됩니다. 예를 들어 볼륨 관계를 보려면 * 스토리지 * > * 스토리지 VM * > * 관계: 지난 1개월 전송 상태 * 메뉴 또는 * 보호 * > * 관계 * > * 관계: Last 1 Month Transfer Status * (지난 1개월 전송 상태 *) 메뉴에서 * Filter * (필터 *)를 사용하여 볼륨에 대한 데이터만 볼 수 있습니다.

- * 소스 볼륨 *

  소스 볼륨 이름을 표시합니다.

- * 대상 볼륨 *

  대상 볼륨 이름을 표시합니다.

- * 작업 유형 *

  볼륨 전송 유형을 표시합니다.

- * 작업 결과 *

  볼륨 전송 성공 여부를 표시합니다.

- * 전송 시작 시간 *

  볼륨 전송 시작 시간을 표시합니다.

- * 전송 종료 시간 *

  볼륨 전송 종료 시간을 표시합니다.

- * 전송 기간 *

  볼륨 전송을 완료하는 데 소요된 시간(시간)을 표시합니다.

- * 전송 크기 *

  전송된 볼륨의 크기(MB)를 표시합니다.

- * 소스 SVM *

  SVM(스토리지 가상 시스템) 이름을 표시합니다.

- * 소스 클러스터 *

  소스 클러스터 이름을 표시합니다.

- * 대상 SVM *

  대상 SVM 이름을 표시합니다.

- * 대상 클러스터 *

  대상 클러스터 이름을 표시합니다.

- 관련 정보 *
- 관계: 모든 관계 * 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 모든 관계 보기".
- 관계: MetroCluster * 보기에 대한 자세한 내용은 을 참조하십시오 "MetroCluster 구성 모니터링".

- 관계: 모든 관계 * 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 최근 1개월 전송 속도 보기".

관계**:** 최근 **1**개월 전송 속도 보기

Relationship:Last 1 Month Transfer Rate 보기를 사용하면 비동기 관계의 볼륨에 대해 매일 전송되는 데이터 볼륨의 양을 분석할 수 있습니다. 또한 이 페이지에서는 일일 전송 및 볼륨 및 스토리지 VM에 대한 전송 작업을 완료하는 데 필요한 시간에 대한 세부 정보를 제공합니다.

페이지 위쪽에 있는 컨트롤을 사용하면 검색을 수행하여 특정 개체를 찾고, 필터를 만들어 적용하여 표시된 데이터 목록의 범위를 좁히고, 페이지에서 열을 추가/제거/재정렬하고, 페이지의 데이터를 .csv, .pdf 또는 .xlsx 파일로 내보낼 수 있습니다. 페이지를 사용자 지정한 후 결과를 사용자 정의 보기로 저장한 다음 이 데이터의 보고서를 정기적으로 생성 및 이메일로 전송할 수 있습니다. 예를 들어, 볼륨 관계를 보려면 * 스토리지 * > * 볼륨 * > * 관계: 지난 1개월 전송율 * 메뉴에 액세스하거나 * 보호 * > * 관계 * > * 관계: 지난 1개월 전송율 * 메뉴에 액세스하고 * 필터 * 를 사용하여 볼륨에 대한 데이터만 볼 수 있습니다.

- * 총 전송 크기 *

  볼륨 전송의 총 크기를 GB 단위로 표시합니다.

- * 일 *

  볼륨 전송이 시작된 날짜를 표시합니다.

- * 종료 시간 *

  날짜와 함께 볼륨 전송 종료 시간을 표시합니다.

- 관련 정보 *
- 관계: MetroCluster * 보기에 대한 자세한 내용은 을 참조하십시오 "MetroCluster 구성 모니터링".
- 관계: 지난 1개월 전송 상태* 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 최근 1개월 전송 상태 보기".
- 관계: 모든 관계 * 보기에 대한 자세한 내용은 을 참조하십시오 "관계: 최근 1개월 전송 속도 보기"

사용자 정의 보고서를 생성합니다

Unified Manager 보고

Active IQ Unified Manager(이전의 OnCommand Unified Manager)은 ONTAP 스토리지 시스템에 대한 보고서를 확인, 사용자 지정, 다운로드 및 예약할 수 있는 기능을 제공합니다. 보고서는 스토리지 시스템 용량, 상태, 성능, 보안 및 보호 관계에 대한 세부 정보를 제공할 수 있습니다.

Active IQ Unified Manager 9.6에 도입된 새로운 Unified Manager 보고 및 예약 기능은 Unified Manager 버전 9.5에서 폐기된 이전 보고 엔진을 대체합니다.

보고 기능은 네트워크에 대한 다양한 뷰를 제공하므로 용량, 상태, 성능, 보안 및 보호 데이터에 대한 실행 가능한 인텔리전스를 제공합니다. 열 표시, 숨기기 및 다시 정렬, 데이터 필터링, 데이터 정렬, 결과를 검색합니다. 다시 사용할 사용자 지정 보기를 저장하고 보고서로 다운로드한 다음 전자 메일을 통해 배포할 반복 보고서로 일정을 지정할 수 있습니다.

Microsoft ® Excel 형식으로 보기를 다운로드하여 사용자 지정할 수 있습니다. 복잡한 정렬, 계층화된 필터, 피벗 테이블 및 차트와 같은 고급 Excel 기능을 사용할 수 있습니다. 결과 Excel 보고서에 만족하면 보고서를 예약 및 공유할 때마다 사용할 Excel 파일을 업로드할 수 있습니다.

사용자 인터페이스에서 보고서를 생성할 뿐만 아니라 다음 추가 방법을 사용하여 Unified Manager에서 상태, 보안 및 성능 데이터를 추출할 수 있습니다.

- ODBC(Open Database Connectivity) 및 ODBC 도구를 사용하여 데이터베이스에 직접 액세스하여 클러스터 정보를 확인할 수 있습니다
- Unified Manager REST API를 실행하여 검토할 정보를 반환합니다

이 Active IQ Unified Manager 릴리스에서 보고서에 다음과 같은 향상된 기능이 제공됩니다.

- 구성된 스케줄에 따라 보고서에 대한 이메일이 전송됩니다. 주문형 보고서를 생성할 때도 이메일을 받게 됩니다.
- 보고서의 파일 이름과 보고서 메타데이터는 보고서가 생성된 호스트 이름을 포함합니다. 파일 이름이 변경되더라도 이 기능 향상으로 인해 보고서가 생성된 호스트 이름을 확인할 수 있습니다.

보고서 생성을 위한 액세스 포인트

Unified Manager에서 클러스터에 대한 정보를 수집하여 UI, MySQL 데이터베이스 쿼리 및 REST API에서 보고서를 생성할 수 있습니다.

다음 섹션에서는 UI를 통해 Unified Manager 보고 및 스케줄링에 대해 설명합니다.

Unified Manager에서 제공하는 보고 기능에 액세스할 수 있는 세 가지 방법이 있습니다.

- UI의 인벤토리 페이지에서 직접 데이터 추출
- ODBC(Open Database Connectivity) 및 ODBC 도구를 사용하여 사용 가능한 모든 개체에 액세스합니다.
- Unified Manager REST API를 실행하여 검토할 정보를 반환합니다.

다음 섹션에서는 UI를 통해 Unified Manager 보고 및 스케줄링에 대해 설명합니다.

맞춤형 보고를 위해 액세스할 수 있는 **Unified Manager** 데이터베이스

Unified Manager는 MySQL 데이터베이스를 사용하여 모니터링 중인 클러스터의 데이터를 저장합니다. 데이터는 MySQL 데이터베이스의 다양한 스키마로 유지됩니다.

다음 데이터베이스의 모든 테이블 데이터를 사용할 수 있습니다.

데이터베이스	설명
netapp_model	ONTAP 컨트롤러의 개체에 대한 데이터입니다.
NetApp_모델_뷰	보고서 도구 사용에 적합한 ONTAP 컨트롤러의 개체에 대한 데이터입니다.
netapp_performance	클러스터별 성능 카운터
ocum	Unified Manager 애플리케이션 데이터와 UI 필터링, 정렬, 일부 파생 필드 계산 지원 정보
ocum_report 를 참조하십시오	인벤토리 구성 및 용량 관련 정보에 대한 데이터입니다.
ocum_report_bRT	보고서 도구 사용에 적합한 재고 구성 및 용량 관련 데이터 보기
OPM	성능 구성 설정 및 임계값 정보
스케일로토르	Unified Manager 애플리케이션 상태 및 성능 문제에 대한 데이터
vmware_model을 참조하십시오	NetApp 스토리지에 호스팅된 데이터 저장소의 VMware 오브젝트 데이터
vmware_model_view 를 참조하십시오	NetApp 스토리지에서 호스트되는 데이터 저장소의 VMware 오브젝트 데이터 보기, 보고서 툴 사용에 적합
vmware_성능	NetApp 스토리지에 호스팅된 데이터 저장소의 VMware 성능 카운터 데이터

보고서 스키마 역할을 가진 데이터베이스 사용자인 보고 사용자는 이러한 테이블의 데이터에 액세스할 수 있습니다. 이 사용자는 Unified Manager 데이터베이스에서 직접 보고 및 기타 데이터베이스 뷰에 대한 읽기 전용 액세스를 가집니다. 이 사용자는 사용자 데이터 또는 클러스터 자격 증명 정보가 포함된 테이블에 액세스할 수 있는 권한이 없습니다.

보고에 사용할 수 있는 **Unified Manager REST API**

REST API를 사용하여 Unified Manager에서 캡처한 상태, 용량, 성능 및 보안 정보를 확인하여

클러스터를 관리할 수 있습니다.

REST API는 Swagger 웹 페이지를 통해 표시됩니다. Swagger 웹 페이지에 액세스하여 Unified Manager REST API 설명서를 표시하고 API 호출을 수동으로 실행할 수 있습니다. Unified Manager 웹 UI의 메뉴 모음에서 * 도움말 * 버튼을 클릭한 다음 * API Documentation * 을 선택합니다. Unified Manager REST API에 대한 자세한 내용은 를 참조하십시오 "Active IQ Unified Manager REST API 시작하기".

REST API에 액세스하려면 운영자, 스토리지 관리자 또는 애플리케이션 관리자 역할이 있어야 합니다.

보고서 이해

보고서에는 스토리지, 네트워크, 서비스 품질 및 보호 관계에 대한 자세한 정보가 표시되어 잠재적 문제가 발생하기 전에 이를 파악하고 해결하는 데 도움이 됩니다.

보기를 사용자 지정할 때 나중에 사용할 수 있도록 고유한 이름으로 저장할 수 있습니다. 정기적으로 실행되도록 해당 보기를 기준으로 보고서를 예약하고 다른 사람과 공유할 수 있습니다. Excel에서 보기를 다운로드하여 고급 Excel 기능을 사용하여 사용자 지정한 다음 해당 파일을 Unified Manager에 다시 업로드할 수도 있습니다. 해당 보기를 사용하여 보고서를 예약하는 경우 업로드한 Excel 파일을 사용하여 공유할 수 있는 강력한 보고서를 만듭니다.

보고서 일정 페이지에서 예약된 모든 보고서를 관리할 수 있습니다.

보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

보고서를 CSV(쉼표로 구분된 값), Excel 또는 PDF 파일로 다운로드할 수 있습니다.

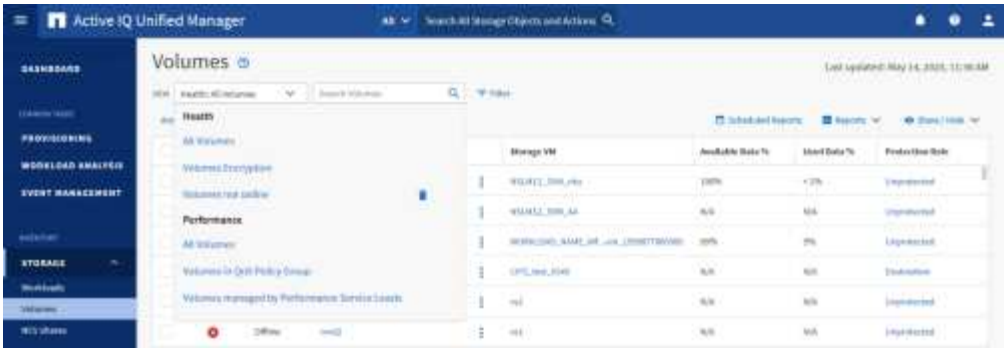
보기 및 보고서 관계 이해

보기 및 인벤토리 페이지는 다운로드하거나 예약할 때 보고서가 됩니다.

다시 사용할 보기 및 인벤토리 페이지를 사용자 지정하고 저장할 수 있습니다. Unified Manager에서 볼 수 있는 거의 모든 기능을 저장, 재사용, 사용자 지정, 예약 및 보고서로 공유할 수 있습니다.

보기 드롭다운에서 삭제 아이콘이 있는 항목은 사용자 또는 다른 사용자가 만든 기존 사용자 지정 보기입니다. 아이콘이 없는 항목은 Unified Manager와 함께 제공되는 기본 보기입니다. 기본 보기는 수정하거나 삭제할 수 없습니다.

- 목록에서 사용자 지정 보기를 삭제하면 해당 보기를 사용하는 모든 Excel 파일 또는 예약된 보고서도 삭제됩니다.
- 사용자 정의 보기를 변경하면 해당 보기를 사용하는 보고서에는 다음에 보고서를 생성하고 보고서 일정에 따라 이메일로 전송할 때 변경 사항이 반영됩니다. 보기를 변경할 때 보고서에 사용된 Excel 사용자 지정 관련 변경 내용이 제대로 적용되었는지 확인합니다. 필요한 경우 Excel 파일을 다운로드하여 필요한 내용을 변경한 다음 보기에 대한 새 Excel 사용자 지정으로 업로드하여 업데이트할 수 있습니다.



애플리케이션 관리자 또는 스토리지 관리자 역할을 가진 사용자만 삭제 아이콘을 보거나, 보기를 변경 또는 삭제하거나, 예약된 보고서를 변경 또는 삭제할 수 있습니다.

보고서 유형

이 표는 사용자 지정, 다운로드 및 예약할 수 있는 보고서로 사용할 수 있는 보기 및 인벤토리 페이지의 전체 목록을 제공합니다.

Active IQ Unified Manager 보고서

유형	스토리지 또는 네트워크 객체입니다
용량	클러스터 애그리게이트 볼륨 Qtree
상태	클러스터 노드 애그리게이트 스토리지 VM 볼륨 SMB/CIFS 공유 NFS 공유

유형	스토리지 또는 네트워크 객체입니다
성능	클러스터 노드 애그리게이트 스토리지 VM 볼륨 LUN을 클릭합니다 NVMe 네임스페이스 네트워크 인터페이스(LIF) 포트
서비스 품질	기존 QoS 정책 그룹 적응형 QoS 정책 그룹 성능 서비스 수준 정책 그룹
볼륨 보호 관계(볼륨 페이지에서 사용 가능)	모든 관계 최근 1개월 이전 상태 최근 1개월 전송 속도입니다
보안	스토리지 VM 클러스터

보고 제한 사항

새로운 Active IQ Unified Manager 보고 기능에는 몇 가지 제한 사항이 있습니다.

이전 버전의 **Unified Manager**의 기존 보고서

Unified Manager 9.5 이전 릴리즈에서는 생성 및 가져온 기존 보고서의 일정과 받는 사람(예: .rptdesign 파일)만 편집할 수 있습니다. Unified Manager 9.5 이전 버전에서 제공된 표준 보고서를 사용자 지정한 경우 이러한 사용자 지정 보고서는 새 보고 도구로 가져오지 않습니다.

rptdesign 파일에서 가져온 기존 보고서를 편집해야 하는 경우 다음 중 하나를 수행하고 가져온 보고서를 제거합니다.

- 새 보기를 만들고 해당 보기에서 보고서 예약(기본 설정)
- 보고서 위로 마우스를 이동하고 SQL을 복사한 다음 외부 도구를 사용하여 데이터를 가져옵니다

사용자 정의 없이 기본 보기를 보고서로 생성할 수 있습니다. 새로운 보고 솔루션을 사용하여 모든 사용자 지정 보고서를 다시 만들 수 있습니다.

일정 및 보고서 관계

저장된 각 보고서에 대해 받는 사람 조합을 사용하여 다양한 일정을 만들 수 있습니다. 그러나 여러 보고서에 대해 일정을 다시 사용할 수는 없습니다.

보고서 보호

적절한 권한이 있는 사용자는 보고서를 편집하거나 삭제할 수 있습니다. 다른 사용자가 저장된 보기 또는 일정을 제거하거나 변경하지 못하도록 하는 방법은 없습니다.

이벤트 보고서

이벤트 보기를 사용자 지정하고 결과 보고서를 CSV 형식으로 다운로드할 수 있지만 생성 및 배포를 위해 반복 이벤트 보고서를 예약할 수는 없습니다.

첨부 파일 보고

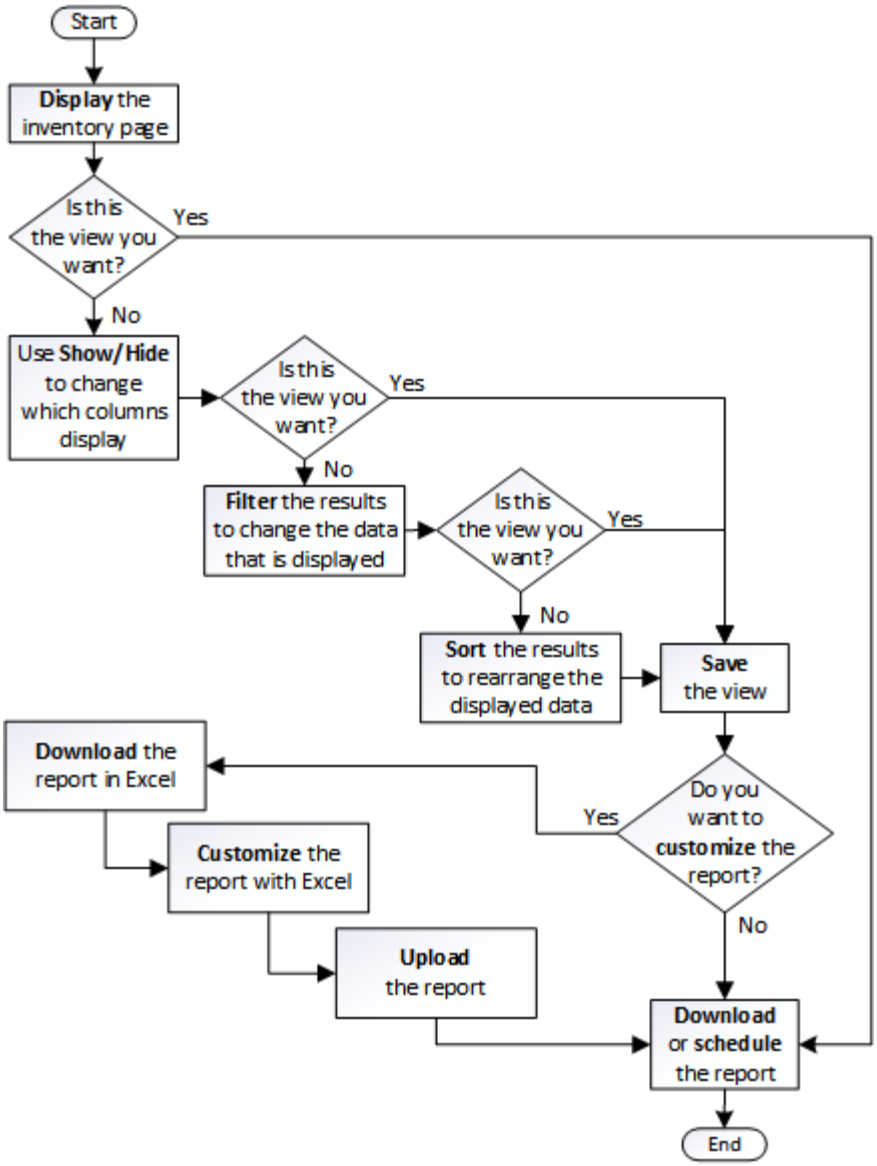
보고서는 이메일 본문에 보낼 수 없습니다. 대신 보고서는 PDF, Excel 또는 CSV 첨부 파일로만 전송됩니다.

보고서 작업

인벤토리 페이지 보기를 찾고 사용자 지정하여 공유 가능한 예약 보고서로 만드는 방법에 대해 알아봅니다.

보고서 워크플로

보고서 워크플로우를 설명하는 결정 트리 구조.



빠른 시작 보고

보기 탐색 및 보고서 예약을 경험할 수 있는 샘플 사용자 지정 보고서를 만듭니다. 이 빠른 시작 보고서에서는 상당히 많은 양의 비활성(콜드) 데이터가 있으므로 클라우드 계층으로 이동할 수 있는 볼륨 목록을 찾습니다. Performance:All Volumes 보기를 열고, 필터와 열을 사용하여 보기를 사용자 지정하고, 사용자 지정 보기를 보고서로 저장하고, 보고서를 일주일에 한 번 공유하도록 예약합니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- FabricPool 애그리게이트를 구성하고 해당 애그리게이트에 볼륨을 가지고 있어야 합니다.

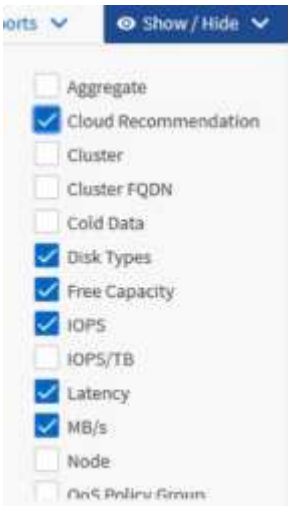
다음 단계를 수행하십시오.

- 기본 보기를 엽니다
- 데이터를 필터링하고 정렬하여 열을 사용자 지정합니다

- 뷰를 저장합니다
- 사용자 정의 보기에 대해 생성할 보고서를 예약합니다

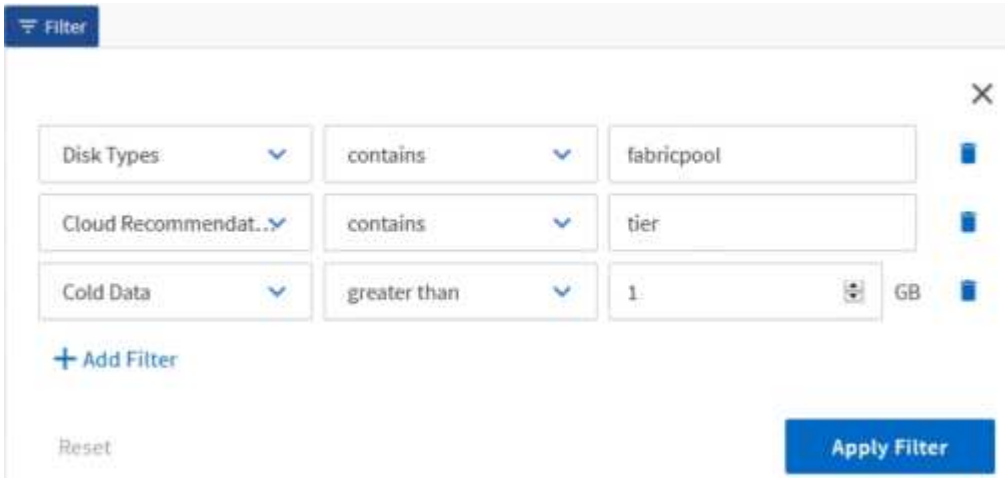
단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 성능 * > * 모든 볼륨 * 을 선택합니다.
3. Show/Hide * (표시/숨기기 *)를 클릭하여 보기에 "디스크 유형" 열이 나타나는지 확인합니다.



다른 열을 추가하거나 제거하여 보고서에 중요한 필드가 포함된 보기를 만듭니다.

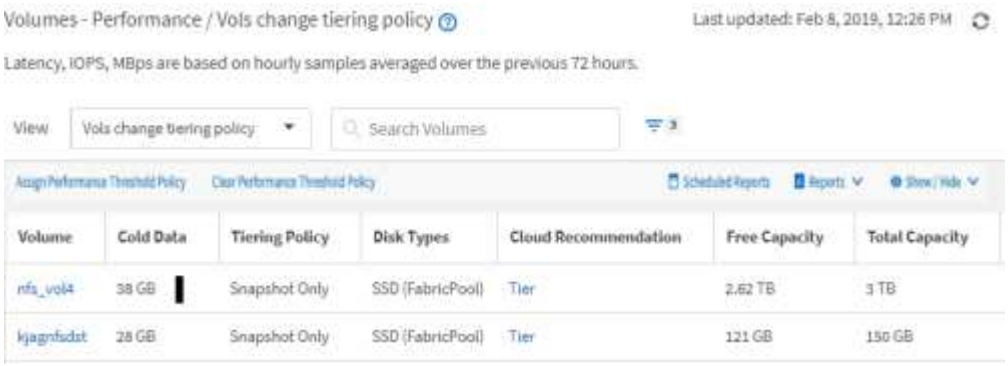
4. "클라우드 추천" 열 옆에 있는 "디스크 유형" 열을 끕니다.
5. 필터 아이콘을 클릭하여 다음 3개의 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 디스크 유형에 FabricPool가 포함되어 있습니다
   - 클라우드 권장에는 계층이 포함됩니다
   - 콜드 데이터가 10GB보다 큽니다



각 필터는 논리적 필터와 결합되므로 반환된 모든 볼륨이 모든 기준을 충족해야 합니다. 최대 5개의 필터를 추가할 수 있습니다.

6. 콜드 데이터 열 상단을 클릭하여 가장 차가운 데이터가 있는 볼륨이 보기의 맨 위에 표시되도록 결과를 정렬합니다.

7. 보기를 사용자 지정하면 보기 이름이 저장되지 않은 보기입니다. 보기의 이름을 ""Vols change Tiering policy""와 같이 보기에 표시되는 내용을 반영합니다. 완료되면 확인 표시를 클릭하거나 * Enter * 를 눌러 새 이름으로 보기를 저장합니다.



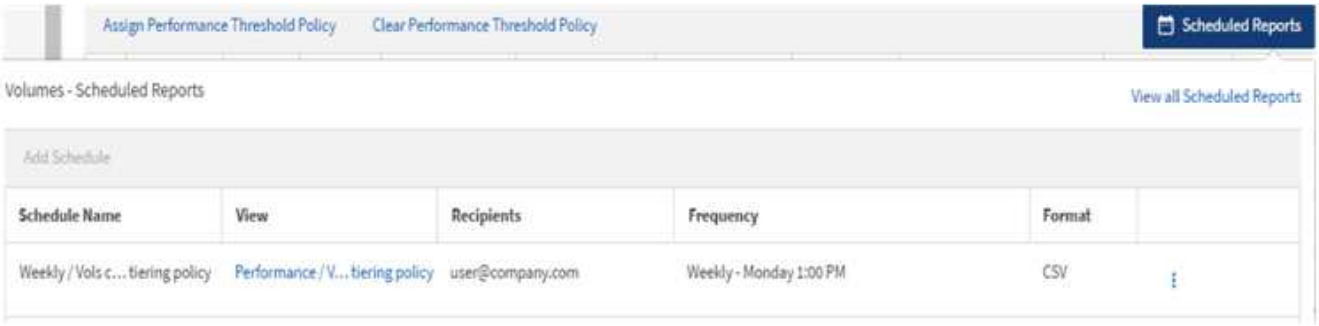
8. 예약 또는 공유하기 전에 보고서를 * CSV *, * Excel * 또는 * PDF * 파일로 다운로드하여 결과를 확인하십시오.

   Microsoft Excel(CSV 또는 Excel) 또는 Adobe Acrobat(PDF)과 같은 설치된 응용 프로그램으로 파일을 열거나 파일을 저장합니다.

   보기를 Excel 파일로 다운로드하여 복잡한 필터, 정렬, 피벗 테이블 또는 차트를 사용하여 보고서를 추가로 사용자 지정할 수 있습니다. Excel에서 파일을 연 후 고급 기능을 사용하여 보고서를 사용자 지정합니다. 만족하면 Excel 파일을 업로드합니다. 이 파일은 사용자 지정과 함께 보고서를 실행할 때 보기에 적용됩니다.

   Excel을 사용하여 보고서를 사용자 지정하는 방법에 대한 자세한 내용은 _Microsoft Excel 보고서 예제_를 참조하십시오.

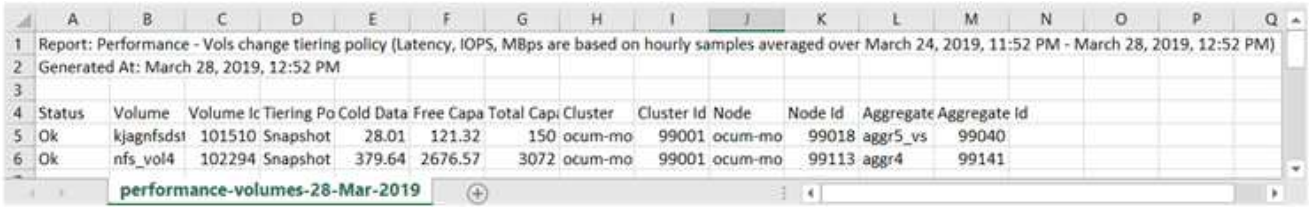
9. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다. 개체와 관련된 예약된 모든 보고서(이 경우 볼륨)가 목록에 나타납니다.



10. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
11. 보고서 이름을 입력하고 다른 보고서 필드를 작성한 다음 확인 표시(✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

    다음 샘플 보고서는 CSV 형식입니다.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1	Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:52 PM - March 28, 2019, 12:52 PM)																
2	Generated At: March 28, 2019, 12:52 PM																
3																	
4	Status	Volume	Volume Ic	Tiering Po	Cold Data	Free Capa	Total Capi	Cluster	Cluster Id	Node	Node Id	Aggregate	Aggregate Id				
5	Ok	kjagnfsdst	101510	Snapshot	28.01	121.32	150	ocum-mo	99001	ocum-mo	99018	aggr5_vs	99040				
6	Ok	nfs_vol4	102294	Snapshot	379.64	2676.57	3072	ocum-mo	99001	ocum-mo	99113	aggr4	99141				

performance-volumes-28-Mar-2019

다음 샘플 보고서는 PDF 형식입니다.

Report: Performance - Vols change tiering policy (Latency, IOPS, MBps are based on hourly samples averaged over March 24, 2019, 11:51 PM - March 28, 2019, 12:51 PM)
Generated At: March 28, 2019, 12:51 PM

Status	Volume	Tiering Policy	Cold Data (GB)	Free Capacity (GB)	Total Capacity (GB)	Cluster	Node	Aggregate
Ok		Snapshot Only	28.01	121.32	150			
Ok		Snapshot Only	379.64	2676.57	3072			

보고서에 표시된 결과에 따라 ONTAP System Manager 또는 ONTAP CLI를 사용하여 특정 볼륨에 대한 계층화 정책을 ""자동" 또는 ""모두""로 변경하여 더 많은 콜드 데이터를 클라우드 계층으로 오프로드할 수 있습니다.

예약된 보고서를 검색하는 중입니다

이름, 보기 이름, 개체 유형 또는 수신자별로 예약된 보고서를 검색할 수 있습니다.

1. 왼쪽 탐색 창에서 * Storage Management * > * Report Schedules * 를 클릭합니다.
2. 예약된 보고서 검색 * 텍스트 필드를 사용합니다.

보고서 검색 기준	시도...
스케줄 이름	보고서 일정 이름의 일부를 입력합니다.
뷰 이름	보고서 보기 이름의 일부를 입력합니다. 기본 보기 및 사용자 정의 보기가 보기 목록에 나타납니다.
받는 사람	이메일 주소의 일부를 입력합니다.
파일 형식	"PDF", "CSV" 또는 "XLSX"를 입력합니다.

3. 열 머리글을 클릭하여 일정 이름 또는 형식과 같이 해당 열을 기준으로 오름차순 또는 내림차순으로 보고서를 정렬할 수 있습니다.

보고서 사용자 정의

ONTAP 클러스터를 관리하는 데 필요한 모든 정보가 포함된 보고서를 만들 수 있도록 보기를 사용자 지정할 수 있는 여러 가지 방법이 있습니다.

기본 재고 페이지 또는 사용자 지정 보기로 시작한 다음 열을 추가 또는 제거하거나, 열 순서를 변경하거나, 데이터를 필터링하거나, 특정 열을 오름차순 또는 내림차순으로 정렬하여 사용자 지정합니다.

Unified Manager 9.8부터 Excel의 보기를 다운로드하여 고급 기능을 사용하여 사용자 지정할 수도 있습니다. 완료되면 사용자 지정 Excel 파일을 업로드합니다. 해당 보기를 사용하여 보고서를 예약하는 경우 사용자 지정된 Excel 파일을 사용하여 공유할 수 있는 강력한 보고서를 만듭니다.

Excel을 사용하여 보고서를 사용자 지정하는 방법에 대한 자세한 내용은 _Microsoft Excel 보고서 예제_를 참조하십시오.

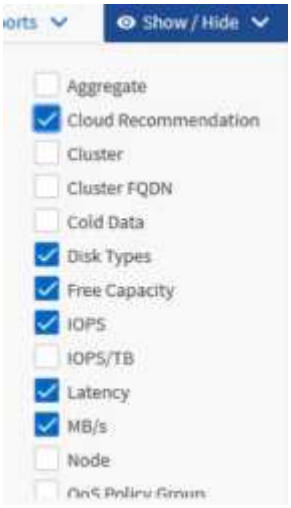
보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

열 사용자 지정

보고서에 사용할 열을 선택하려면 * 표시/숨기기 * 를 사용합니다. 재고 페이지의 열을 끌어서 다시 정렬합니다.

단계

1. 열을 추가하거나 제거하려면 * 표시/숨기기 * 를 클릭합니다.



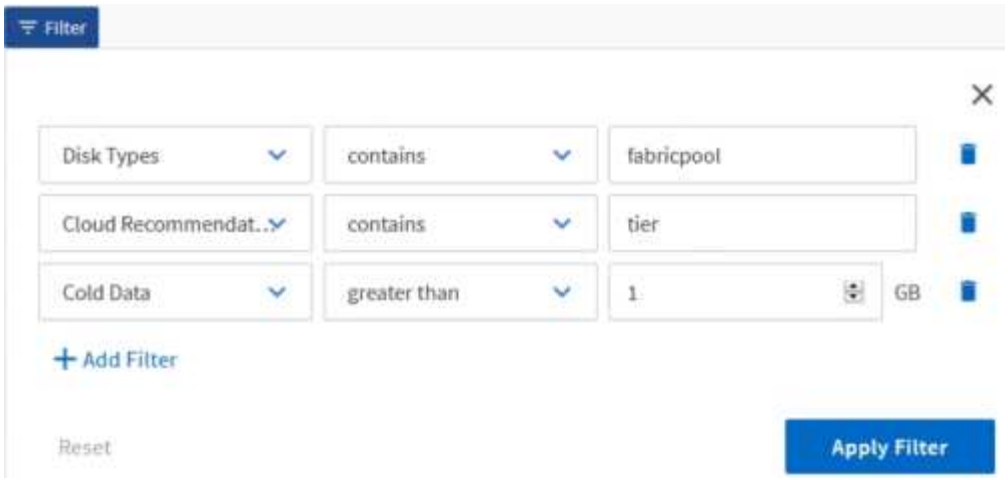
2. 재고 페이지에서 열을 끌어 보고서에서 원하는 순서대로 다시 정렬합니다.
3. 저장하지 않은 보기의 이름을 지정하여 변경 내용을 저장합니다.

데이터 필터링

데이터를 필터링하여 결과가 보고서 요구 사항과 일치하는지 확인합니다. 필터링을 사용하면 원하는 데이터만 표시할 수 있습니다.

단계

1. 필터 아이콘을 클릭하여 보려는 결과에 초점을 맞출 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.



2. 저장하지 않은 보기의 이름을 지정하여 변경 내용을 저장합니다.

데이터 정렬

결과를 정렬하려면 열을 클릭하고 오름차순 또는 내림차순을 지정합니다. 데이터 정렬은 보고서에 필요한 정보의 우선 순위를 지정합니다.

단계

1. 열 맨 위를 클릭하여 가장 중요한 정보가 보기 맨 위에 표시되도록 결과를 정렬합니다.
2. 저장하지 않은 보기의 이름을 지정하여 변경 내용을 저장합니다.

검색을 사용하여 보기를 구체화합니다

원하는 보기가 있으면 검색 필드를 사용하여 보고서에 포함할 결과에 초점을 맞춰 결과를 더 구체화할 수 있습니다.

단계

1. 보고서의 기반으로 사용할 사용자 지정 보기 또는 기본 보기를 엽니다.
2. 검색 필드에 입력하여 보기에 나열된 데이터를 구체화합니다. 표시된 열에 부분 데이터를 입력할 수 있습니다. 예를 들어 이름에 "US_East"가 포함된 노드를 검색하려면 전체 노드 목록을 구체화할 수 있습니다.

   검색 결과는 사용자 정의 보기에 저장되고 결과 예약된 보고서에 사용됩니다.

3. 저장하지 않은 보기의 이름을 지정하여 변경 내용을 저장합니다.

Excel을 사용하여 보고서를 사용자 지정합니다

보기를 저장한 후에는 Excel 통합 문서 형식(.xlsx)으로 다운로드할 수 있습니다. Excel 파일을 열 때 고급 Excel 기능을 사용하여 보고서를 사용자 지정할 수 있습니다.

- 필요한 것 *

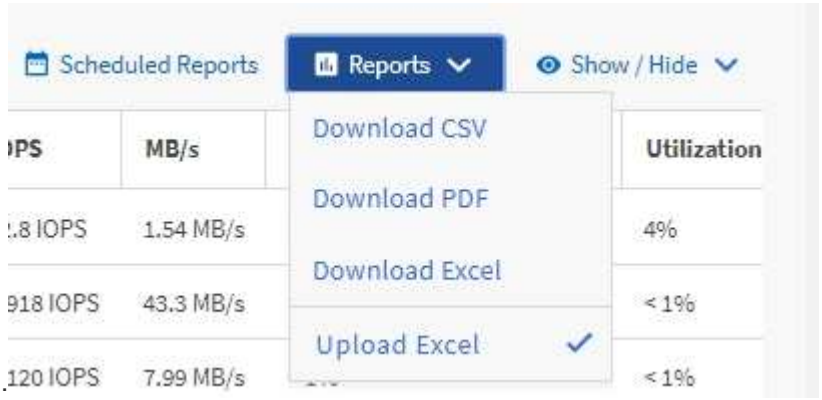
확장명이 .xlsx인 Excel 통합 문서 파일만 업로드할 수 있습니다.

예를 들어 보고서에 사용할 수 있는 일부 고급 Excel 기능은 다음과 같습니다.

- 다중 열 정렬
- 복잡한 필터링
- 피벗 테이블
- 차트

- 다운로드한 Excel 파일은 저장된 이름이 아니라 보기에 기본 파일 이름을 사용합니다.
  - 형식은 "<보기 영역>-<일>-<월>-<연도>-<시간>-<분>-<초>.xlsx"입니다
  - 예를 들어, 볼륨-온라인 아님 이라는 사용자 정의 저장 보기에는 해당 날짜 및 시간에 저장된 상태-볼륨-2020년 5월-2020년 5월-19-18-00.xlsx라는 파일 이름이 있습니다.
- Excel 파일에 시트를 추가할 수는 있지만 기존 시트는 변경할 수는 없습니다.
  - 기존 시트, 데이터 및 정보를 변경하지 마십시오. 대신 새로 만든 페이지에 데이터를 복사합니다.
  - 위의 규칙에 대한 한 가지 예외는 "데이터" 페이지에서 수식을 만들 수 있다는 것입니다. 데이터 페이지 수식을 사용하여 새 페이지에 차트를 만듭니다.
  - 새 시트 데이터 또는 정보의 이름을 지정하지 마십시오.

- 사용자 지정된 Excel 파일이 있는 경우 * Reports * > * Upload Excel * 메뉴 항목 옆에 확인 표시가 있습니다. Excel 파일을 다운로드하면 사용자 지정 버전이 사용됩니다



단계

1. 보고서의 기반으로 사용할 기본 보기, 사용자 정의 보기 또는 저장된 보기를 엽니다.
2. 보고서 * > * Excel 다운로드 * 를 선택합니다.
3. 파일을 저장합니다. 파일이 다운로드 폴더에 저장됩니다.
4. Excel에서 저장된 파일을 엽니다. 파일을 새 위치로 이동하지 마십시오. 또는 다른 위치에서 작업하는 경우 파일을 업로드하기 전에 원래 파일 이름을 사용하여 파일을 원래 위치에 다시 저장하십시오.
5. 복잡한 정렬, 계층화된 필터, 피벗 테이블 또는 차트와 같은 Excel 기능을 사용하여 파일을 사용자 지정합니다. 자세한 내용은 Microsoft ® Excel 문서를 참조하십시오.
6. Reports * > * Upload Excel * 을 선택하고 수정한 파일을 선택합니다. 가장 최근에 다운로드한 파일이 동일한 파일 위치에서 업로드됩니다.
7. 예약된 보고서 * 기능을 사용하여 테스트 보고서를 자신에게 보냅니다.

보고서를 다운로드하는 중입니다

보고서를 다운로드하여 로컬 또는 네트워크 드라이브에 CSV(쉼표로 구분된 값) 파일, Microsoft Excel(.xlsx) 파일 또는 PDF 파일로 저장할 수 있습니다. CSV 및 XLSX 파일은 Microsoft Excel과 같은 스프레드시트 응용 프로그램과 Adobe Acrobat과 같은 판독기로 열 수 있습니다.

단계

1. 보고서 * 버튼을 클릭하여 다음 중 하나로 보고서를 다운로드합니다.

을 선택합니다	대상...
CSV를 다운로드합니다	보고서를 CSV(쉼표로 구분된 값) 파일로 저장합니다.
PDF 다운로드	보고서를 .pdf 파일로 저장합니다.
Excel을 다운로드합니다	보고서를 Microsoft Excel(XLSX) 파일로 저장합니다.

보고서 예약

다시 사용하고 보고서로 공유할 보기가 있으면 Active IQ Unified Manager를 사용하여 일정을 예약할 수 있습니다. 예약된 보고서를 관리하고 각 보고서 일정에 대한 수신자와 배포 빈도를 변경할 수 있습니다.

Unified Manager에서 대부분의 보기 또는 인벤토리 페이지를 예약할 수 있습니다. 단, CSV 파일로 다운로드할 수 있는 보고서인 이벤트만 예외로, 재생성 및 공유를 위한 이벤트는 예약할 수 없습니다. 대시보드, 즐겨찾기 또는 구성 페이지도 다운로드하거나 예약할 수 없습니다.

Active IQ Unified Manager 9.8부터 Microsoft ® Excel 형식으로 보기를 다운로드하여 사용자 지정할 수 있습니다. 복잡한 정렬, 계층화된 필터, 피벗 테이블 및 차트와 같은 고급 Excel 기능을 사용할 수 있습니다. 결과 Excel 보고서에 만족하면 보고서를 예약 및 공유할 때마다 사용할 Excel 파일을 업로드할 수 있습니다.

기본 제공 보기 또는 사용자 지정 보기를 예약할 수 있습니다. CSV, PDF 또는 XSLX 중 어떤 파일 형식을 보낼 것인지 선택할 수 있습니다. 보고서를 처음 예약하는 경우 보고서를 다운로드하여 받는 사람이 볼 수 있는 보고서를 볼 수 있는 유일한 받는 사람으로 지정할 수 있습니다.

보고서 예약

정기 생성 및 배포를 예약할 보기 또는 Excel 파일이 있는 경우 보고서를 예약할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- 보고 엔진이 Unified Manager 서버의 수신자 목록에 전자 메일 첨부 파일로 보고서를 보낼 수 있도록 * 일반 * > * 알림 * 페이지에서 SMTP 서버 설정을 구성해야 합니다.
- 생성된 이메일과 함께 첨부 파일을 전송할 수 있도록 이메일 서버를 구성해야 합니다.

다음 단계를 사용하여 보기에 대해 생성할 보고서를 테스트하고 예약할 수 있습니다. 사용할 보기를 선택하거나 사용자

지정합니다. 다음 절차에서는 네트워크 인터페이스의 성능을 보여 주는 네트워크 보기를 사용하지만 원하는 보기를 사용할 수 있습니다.

단계

1. 보기를 엽니다. 이 예에서는 LIF 성능을 나타내는 기본 네트워크 보기를 사용합니다. 왼쪽 탐색 창에서 * 네트워크 > 네트워크 인터페이스 * 를 클릭합니다.
2. 기본 제공 Unified Manager 기능을 사용하여 필요에 따라 뷰를 사용자 지정합니다.
3. 보기를 사용자 지정한 후 * 보기 * 필드에 고유한 이름을 입력하고 확인 표시를 클릭하여 저장할 수 있습니다.

4. Microsoft ® Excel의 고급 기능을 사용하여 보고서를 사용자 지정할 수 있습니다. 자세한 내용은 을 참조하십시오 "Excel을 사용하여 보고서를 사용자 지정합니다".
5. 예약 또는 공유하기 전에 출력을 보려면:

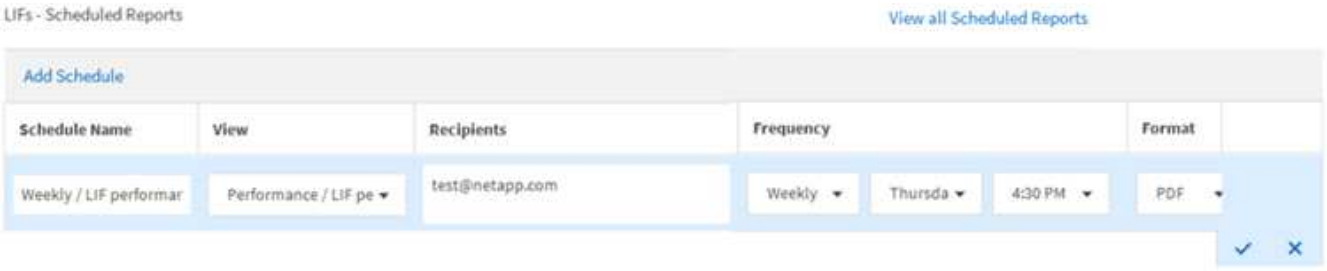
옵션을 선택합니다	설명
• Excel을 사용하여 보고서를 사용자 지정한 경우 *	다운로드한 기존 Excel 파일을 봅니다.
• Excel을 사용하여 보고서를 사용자 정의하지 않은 경우 *	보고서를 * CSV *, * PDF * 또는 * XLSX * 파일로 다운로드합니다.

   Microsoft Excel(CSV/XSLX) 또는 Adobe Acrobat(PDF)과 같은 설치된 응용 프로그램으로 파일을 엽니다.

6. 보고서에 만족하면 * Scheduled Reports * 를 클릭합니다.
7. 보고서 일정 페이지에서 * 일정 추가 * 를 클릭합니다.
8. 뷰 이름과 빈도의 조합인 기본 이름을 그대로 사용하거나 * 스케줄 이름 * 을 사용자 정의합니다.
9. 예약된 보고서를 처음으로 테스트하려면 자신을 * 받는 사람 * 으로만 추가하십시오. 만족하면 모든 보고서 수신자에 대한 이메일 주소를 추가합니다.
10. 보고서를 생성하고 수신자에게 보내는 빈도를 지정합니다. Daily *, * Weekly * 또는 * Monthly * 를 선택할 수 있습니다.
11. PDF *, * CSV * 또는 * XSLX * 형식으로 형식을 선택합니다.

    Excel을 사용하여 콘텐츠를 사용자 지정한 보고서의 경우 항상 * XSLX * 를 선택합니다.

12. 확인 표시(✓)를 클릭하여 보고서 일정을 저장합니다.



보고서가 즉시 테스트로 전송됩니다. 그런 다음 예약된 빈도를 사용하여 나열된 수신자에게 보고서를 생성하고 e-메일로 보냅니다.

가져온 **.rptdesign** 보고서 예약

이전 릴리즈의 Unified Manager에서 생성 및 가져온 기존 보고서를 예약할 수 있습니다.

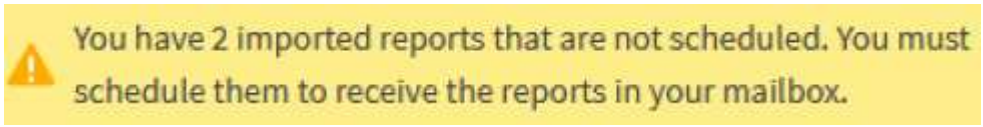
가져온 보고서를 예약하려면 다음이 필요합니다.

- 가져온 BIRT가 이전 Unified Manager 릴리즈에서 설계했던 .rptdesign 파일 보고서를 가져왔습니다
- Unified Manager 9.6 GA 이상으로 업그레이드할 경우 적용 가능합니다

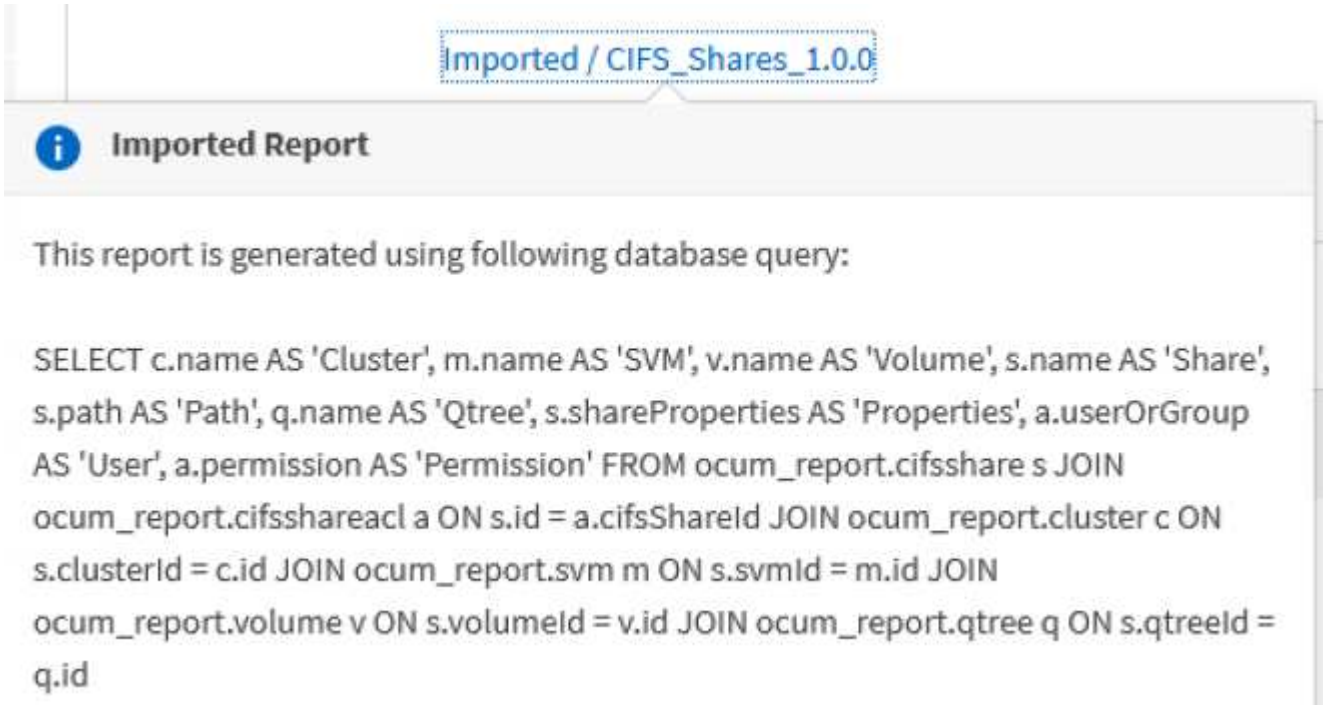
Unified Manager 9.6 GA 이상으로 업그레이드한 후 Report Schedules 페이지에 가져온 보고서가 나열됩니다. 이러한 보고서의 일정을 편집하여 받는 사람 전자 메일 주소, 빈도 및 형식(PDF 또는 CSV)을 지정할 수 있습니다. 그렇지 않으면 Unified Manager UI에서 보고서를 편집하거나 볼 수 없습니다.

단계

1. 보고서 일정 페이지를 엽니다. 보고서를 가져온 경우 메시지가 나타납니다.



2. 보기 * 이름을 클릭하여 보고서를 생성하는 데 사용 중인 SQL 쿼리를 표시합니다.



3. 자세히 아이콘을 클릭합니다 ⋮ , * 편집 * 을 클릭하고 보고서 일정 세부 정보를 정의한 다음 보고서를 저장합니다.

추가 아이콘에서 원하지 않는 보고서를 삭제할 수도 있습니다 ⋮ .

보고서 일정 관리

보고서 일정 페이지에서 보고서 일정을 관리할 수 있습니다. 기존 일정을 보거나 수정하거나 삭제할 수 있습니다.

- 필요한 것 *

> 보고서 일정 페이지에서 새 보고서를 예약할 수 없습니다. 객체 재고 페이지에서만 예약된 보고서를 추가할 수 있습니다.

- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * Storage Management * > * Report Schedules * 를 클릭합니다.
2. 보고서 일정 페이지에서 다음을 수행합니다.

원하는 작업	그러면...
기존 일정을 봅니다	스크롤 막대 및 페이지 컨트롤을 사용하여 기존 보고서 목록을 스크롤합니다.
기존 일정을 편집합니다	a. 자세히 아이콘을 클릭합니다 ⋮ 를 클릭합니다. b. 편집 * 을 클릭합니다. c. 필요한 사항을 변경합니다. d. 확인 표시를 클릭하여 변경 사항을 저장합니다.
기존 일정을 삭제합니다	a. 자세히 아이콘을 클릭합니다 ⋮ 를 클릭합니다. b. 삭제 * 를 클릭합니다. c. 결정을 확인합니다.

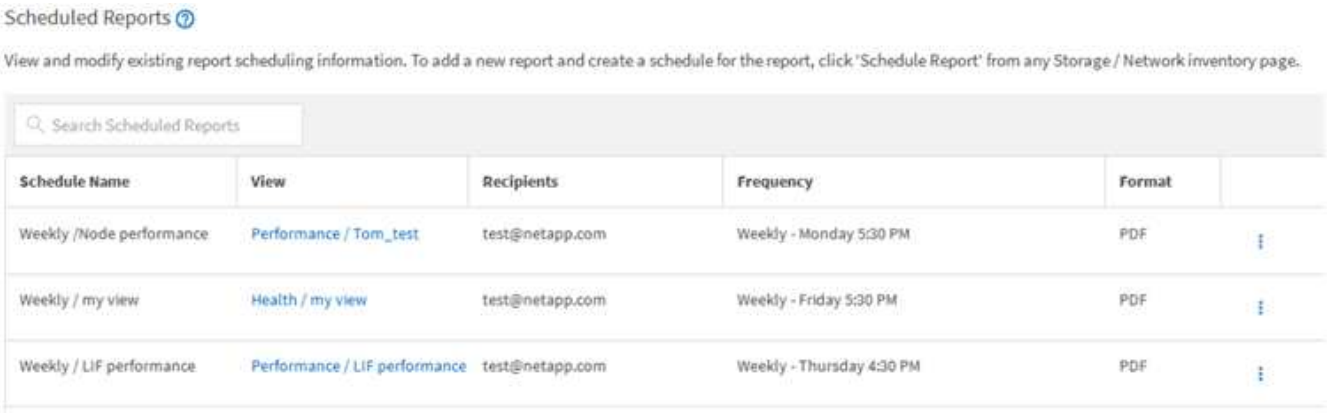
예약된 보고서 편집

보고서 일정을 예약한 후 보고서 일정 페이지에서 보고서를 편집할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * Storage Management * > * Report Schedules * 를 클릭합니다.



적절한 권한이 있는 경우 시스템에서 모든 보고서 및 해당 일정을 변경할 수 있습니다.

2. 자세히 아이콘을 클릭합니다 ⋮ 변경할 스케줄입니다.
3. 편집 * 을 클릭합니다.
4. 보고서 일정에 대해 별표 이름 *, * 수신자 * 목록, * 빈도 * 및 * 형식 * 을 변경할 수 있습니다.
5. 완료되면 확인 표시를 클릭하여 변경 사항을 저장합니다.

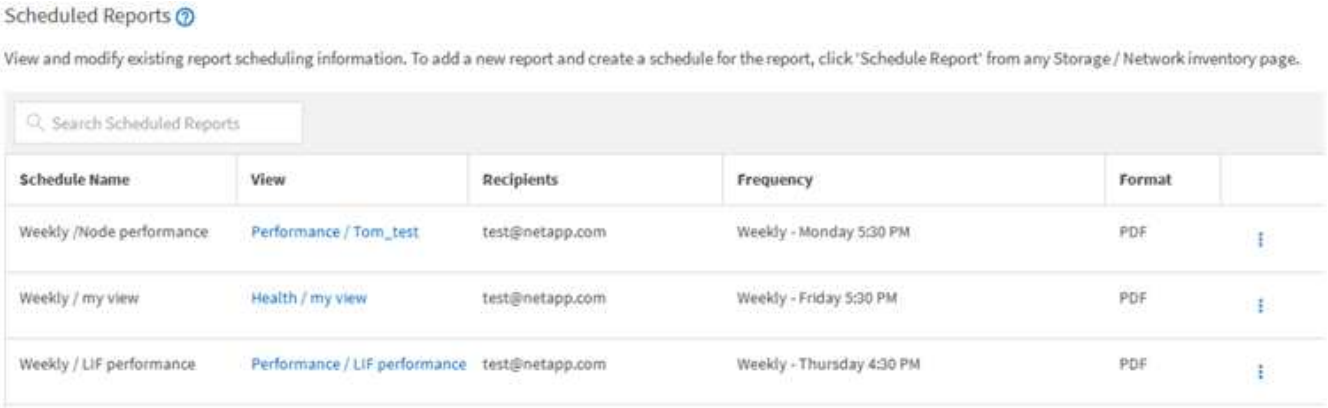
예약된 보고서를 삭제하는 중입니다

보고서가 예약된 후에는 보고서 일정 페이지에서 삭제할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

단계

1. 왼쪽 탐색 창에서 * Storage Management * > * Report Schedules * 를 클릭합니다.



적절한 권한이 있는 경우 시스템에서 모든 보고서 및 해당 일정을 제거할 수 있습니다.

2. 자세히 아이콘을 클릭합니다 ⋮ 제거할 스케줄의 경우.
3. 삭제 * 를 클릭합니다.
4. 결정을 확인합니다.

예약된 보고서가 목록에서 제거되고 설정된 일정에 따라 더 이상 생성 및 배포되지 않습니다.

재고 페이지에서 사용자 지정 보기를 삭제하면 해당 보기를 사용하는 사용자 지정 Excel 파일 또는 예약된 보고서도 삭제됩니다.

샘플 사용자 지정 보고서

이러한 샘플 사용자 지정 보고서는 문제가 발생하기 전에 잠재적 문제를 식별하고 잠재적 문제에 대응하는 데 일반적으로 사용됩니다.

이 섹션의 보고서 목록은 전체 내용이 아니며 시간이 지남에 따라 증가합니다. 문서 피드백을 제공하여 사용자 지정 보고서를 이 섹션에 추가하도록 제안할 수 있습니다.

보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

클러스터 스토리지 보고서 사용자 지정

이 섹션의 샘플 클러스터 스토리지 보고서는 스토리지 시스템 리소스를 모니터링하는 데 도움이 되도록 클러스터 용량에 대한 보고서를 생성하는 방법을 이해하는 데 도움이 되는 샘플입니다.

클러스터 모델별 용량을 볼 수 있는 보고서 생성

보고서를 생성하여 스토리지 시스템 모델을 기반으로 클러스터의 스토리지 용량 및 활용률을 분석할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 클러스터 모델별 용량을 표시하는 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 클러스터 * 를 선택합니다.
3. 보고서에 표시하지 않을 ""클러스터 FQDN"" 및 ""OS 버전""과 같은 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "총 물리적 용량", "모델/제품군", "클러스터" 열 근처의 세 개의 집계 열을 끕니다.
5. "Model/Family" 열 상단을 클릭하여 클러스터 유형별로 결과를 정렬합니다.
6. 보기의 표시 내용을 반영하는 특정 이름(예: ""클러스터 모델별 용량")으로 보기를 저장합니다.
7. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
8. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.
9. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 특정 클러스터에 용량을 추가하거나 이전 클러스터 모델을 업그레이드할 수 있습니다.

보고서를 생성하여 할당되지 않은 **LUN** 용량이 가장 많은 클러스터를 식별합니다

0.5TB를 초과하는 할당되지 않은 LUN 용량이 가장 많은 클러스터를 찾아 보고서를 생성하여 워크로드를 추가할 수 있는 위치를 파악할 수 있습니다.

- 필요한 사항 * * * 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 할당되지 않은 LUN 용량이 가장 많은 클러스터를 표시하는 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 클러스터 * 를 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "HA Pair" 열 근처의 "'할당되지 않은 LUN Capacity" 열을 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 할당되지 않은 LUN 용량이 0.5TB보다 큼
6. 할당되지 않은 LUN 용량 열의 맨 위를 클릭하여 할당되지 않은 LUN 용량을 가장 많이 기준으로 결과를 정렬합니다.
7. 뷰를 "'가장 할당되지 않은 LUN 용량'과 같이 보기의 표시 내용을 반영하는 특정 이름으로 저장하고 확인 표시(✓)를 클릭합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
10. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 클러스터의 할당되지 않은 LUN 용량을 사용할 수도 있습니다.

보고서를 생성하여 사용 가능한 용량이 가장 많은 **HA** 쌍을 표시합니다

보고서를 생성하여 새 볼륨 및 LUN을 프로비저닝할 때 가장 용량이 큰 고가용성(HA) 쌍을 찾을 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 새 볼륨 및 LUN 프로비저닝을 위해 사용 가능한 최대 용량별로 정렬된 HA 쌍을 표시하는 사용자 지정 보기를 생성한 다음, 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 클러스터 * 를 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 클러스터 * 를 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "HA Pair" 열 근처의 "Aggregate Unused Capacity" 열을 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 사용되지 않은 총 용량이 0.5TB를 초과하는 경우
6. "Aggregate Unused Capacity" 열의 상단을 클릭하여 미사용 총 용량을 기준으로 결과를 정렬합니다.
7. 보기의 표시 내용을 반영하는 특정 이름(예: ""최소 사용 집계 용량")으로 보기를 저장하고 확인 표시(를 클릭합니다)를 클릭합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
10. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시()를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 애그리게이트 용량을 기준으로 HA 쌍의 균형을 맞출 수 있습니다.

보고서를 생성하여 이전 버전의 **ONTAP**를 실행하는 노드를 봅니다

보고서를 생성하여 업그레이드해야 하는 노드를 확인할 수 있도록 모든 클러스터 노드에 설치된 ONTAP 소프트웨어 버전을 표시할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 수행하여 이전 버전의 ONTAP를 실행하는 노드를 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 노드 * 를 클릭합니다.
2. 보고서에 표시하지 않으려는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
3. 노드 칼럼 근처에 있는 OS Version 열을 끌어다 놓으십시오.
4. ""OS 버전"" 열 상단을 클릭하여 가장 오래된 버전의 ONTAP로 결과를 정렬합니다.
5. 보기의 표시 내용을 반영하는 특정 이름으로 보기를 저장합니다(예: ""ONTAP 버전별 노드").
6. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
7. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
8. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시()를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 이전 버전의 ONTAP를 실행하는 노드를 업그레이드할 수 있습니다.

애그리게이트 용량 보고서 사용자 지정

이러한 샘플 사용자 지정 보고서는 애그리게이트 스토리지 용량과 관련된 잠재적 문제를 식별하고 이에 대응하는 데 사용됩니다.

이 섹션의 보고서는 스토리지 시스템 리소스를 모니터링하는 데 도움이 되도록 집계 용량에 대한 보고서를 생성하는 방법을 이해하는 데 도움이 되는 샘플입니다.

보고서를 생성하여 전체 용량에 도달한 애그리게이트를 확인합니다

보고서를 생성하여 용량을 추가하거나 워크로드를 다른 애그리게이트로 이동할 수 있도록 전체 용량에 도달한 애그리게이트를 찾을 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 전체 용량에 도달한 애그리게이트를 표시하는 사용자 지정 보기를 생성한 다음, 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 애그리게이트 * 를 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 45일 이내에 최대 백업
5. "Days to Full" 열 상단을 클릭하여 전체 용량에 도달하기 위해 남은 일 수를 기준으로 결과를 정렬합니다.
6. "Days to full aggregate capacity(전체 집계 용량으로 저장)"와 같이 보기에 표시되는 내용을 반영하는 특정 이름으로 보기를 저장하고 확인 표시(를 클릭합니다✓)를 클릭합니다.
7. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
8. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.
9. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 기준으로 aggregate의 스토리지를 전체 용량에 도달하려고 할 수 있습니다. 또한 aggregate에서 공간이 부족해지는 데 더 많은 시간을 제공하는 이벤트를 수신할 수 있도록, 전체 용량 임계값에 도달할 때까지 일을 기본값 7일 이상으로 늘리고 싶을 수 있습니다.

80% 이상의 전체 애그리게이트를 볼 수 있는 보고서 생성

보고서를 생성하여 80% 이상의 꽉 찬 애그리게이트를 강조 표시할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 80% 이상의 꽉 찬 애그리게이트를 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 애그리게이트 * 를 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "'사용 가능한 데이터 %'"와 "'사용된 데이터 %'" 열을 "집계" 열 근처로 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 사용된 데이터 %가 80%보다 큽니다
6. "'Used Data%'" 열 상단을 클릭하여 결과를 용량 퍼센트로 정렬합니다.
7. 뷰를 ""집계 임박한 전체""와 같이 보기의 표시 내용을 반영하는 특정 이름으로 저장하고 확인 표시(를 클릭합니다 ✓)를 클릭합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
10. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 일부 데이터를 특정 애그리게이트에서 이동하려고 할 수 있습니다.

초과 커밋된 집계를 보기 위한 보고서 생성

보고서를 생성하여 스토리지 용량과 애그리게이트 사용을 분석하고 초과 커밋된 애그리게이트를 볼 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 초과 커밋된 임계값을 초과하는 애그리게이트를 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 애그리게이트 * 를 선택합니다.
3. 보고서에 표시하지 않으려는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "OverCommitted Capacity%" 열을 "Aggregate" 열 근처로 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.

◦ 초과 커밋된 용량 %가 100%보다 큽니다

6. "'OverCommitted Capacity%'" 열 상단을 클릭하여 결과를 용량 백분율 기준으로 정렬합니다.
7. 보기의 표시 내용을 반영하는 특정 이름(예: ""집계 오버커밋""으로 보기를 저장하고 확인 표시()를 클릭합니다)를 클릭합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
10. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시()를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 기준으로 aggregate에 용량을 추가하거나 특정 애그리게이트에서 일부 데이터를 이동하려고 할 수 있습니다.

볼륨 용량 보고서 사용자 지정

이러한 샘플 사용자 지정 보고서는 볼륨 용량 및 성능과 관련된 잠재적인 문제를 식별하고 이에 대응하는 데 사용됩니다.

보고서를 생성하여 스냅샷 자동 삭제 기능이 꺼진 전체 용량에 근접하는 볼륨을 식별합니다

스냅샷 자동 삭제 기능을 비활성화한 상태에서 전체 용량에 거의 도달한 볼륨 목록이 포함된 보고서를 생성할 수 있습니다. 이 결과를 통해 스냅샷 자동 삭제 기능을 구성할 볼륨을 식별할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 단계에 따라 필요한 열을 올바른 순서로 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 볼륨 * 을 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "스냅샷 자동 삭제" 및 "Days to Full" 열을 "Available Data Capacity" 열 근처에 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 두 개의 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
    ◦ 30일 이내에 최대 백업 완료
    ◦ 스냅샷 자동 삭제 기능이 비활성화되었습니다
6. 남은 일수가 가장 적은 볼륨이 목록의 맨 위에 표시되도록 * Days to Full * 열의 맨 위를 클릭합니다.
7. "Vols near capacity" 등의 특정 이름으로 뷰를 저장합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.

9. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 기준으로 볼륨에 대한 스냅샷 자동 삭제 기능을 사용하거나 사용 가능한 공간을 늘리는 방법을 찾을 수 있습니다.

씬 프로비저닝이 해제된 볼륨에서 사용하는 공간을 식별하는 보고서를 생성합니다

볼륨이 씬 프로비저닝되지 않은 경우 볼륨이 생성될 때 정의된 대로 디스크의 전체 공간을 차지합니다. 씬 프로비저닝을 사용하지 않는 볼륨을 식별하면 특정 볼륨에서 씬 프로비저닝을 사용할지 여부를 결정하는 데 도움이 됩니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

아래 단계에 따라 필요한 열을 올바른 순서로 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 용량 * > * 모든 볼륨 * 을 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "Used Data %"와 "Thin Provisioned" 열을 ""Available Data Capacity" 열 근처에 끌어다 놓으십시오.
5. 필터 아이콘을 클릭하고 다음 필터를 추가합니다. * Thin Provisioned * is * No * (씬 프로비저닝됨 * is * No *). 그런 다음 * Apply Filter * (필터 적용 *)를 클릭합니다.
6. ""Used Data%"" 열 상단을 클릭하여 목록 상단에 가장 높은 비율의 볼륨이 표시되도록 결과를 정렬합니다.
7. 뷰에 표시되는 내용을 반영하는 이름으로 뷰를 저장합니다(예: ""Vols no thin provisioning").
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.
10. 보고서 스케줄의 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시( )를 클릭합니다✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 특정 볼륨에서 씬 프로비저닝을 활성화할 수 있습니다.

보고서를 생성하여 데이터를 클라우드 계층으로 이동해야 하는 **FabricPool** 애그리게이트에서 볼륨을 식별합니다

현재 FabricPool 애그리게이트에 있는 볼륨 목록, 클라우드 권장 사항이 Tier인 볼륨 및 콜드 데이터가 많은 보고서를 생성할 수 있습니다. 이 보고서를 통해 특정 볼륨에 대한 계층화 정책을 ""자동"" 또는 ""모두""로 변경하여 더 많은 콜드(비활성) 데이터를 클라우드 계층으로 오프로드해야 할지 여부를 결정할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.
- FabricPool 애그리게이트를 구성하고 해당 애그리게이트에 볼륨을 가지고 있어야 합니다.

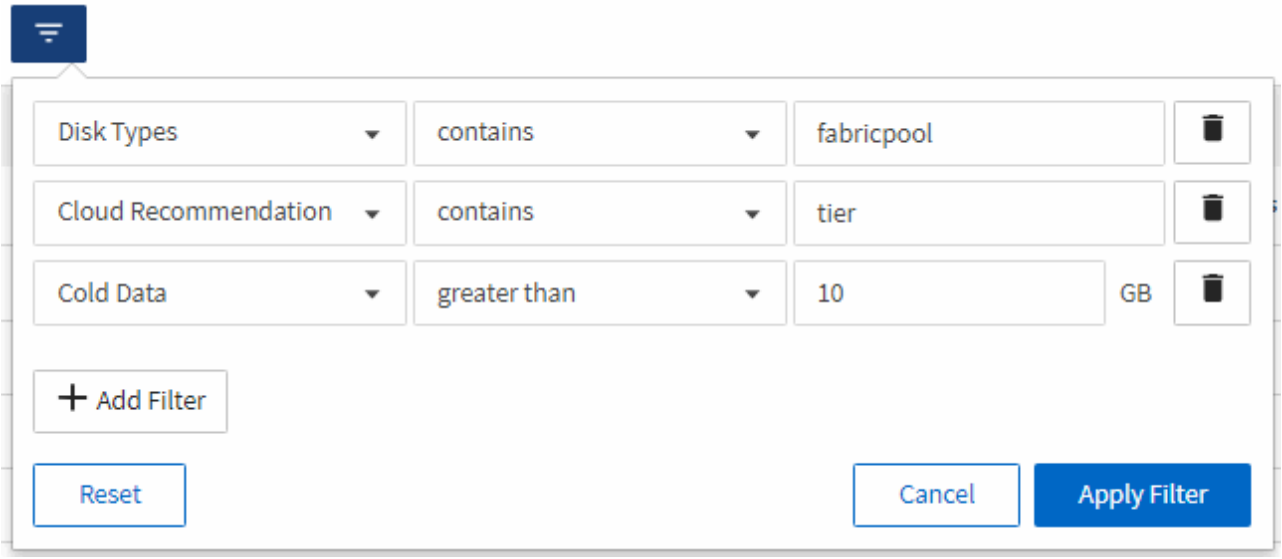
아래 단계에 따라 필요한 열을 올바른 순서로 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

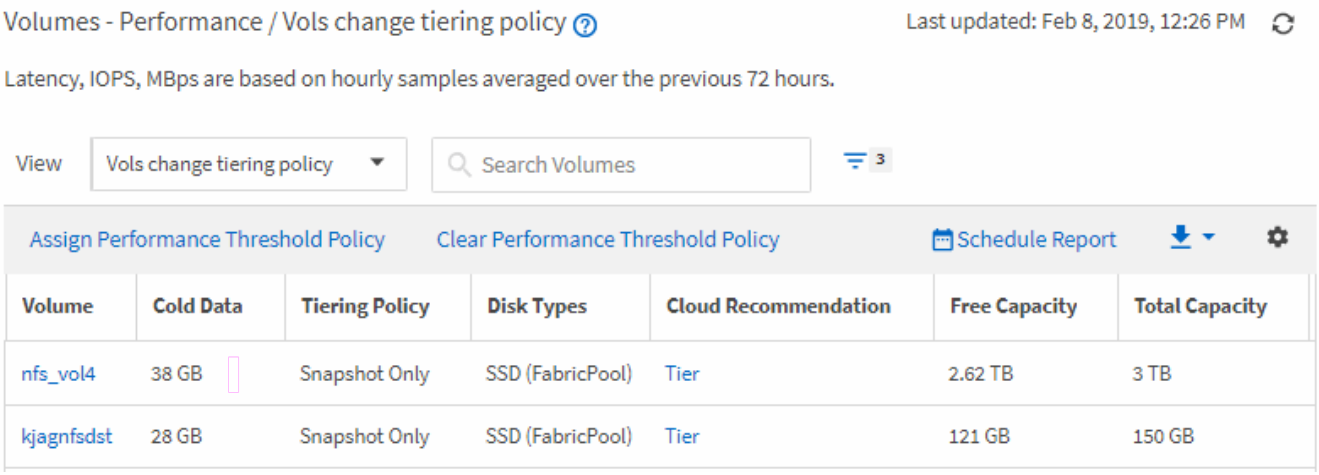
1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 성능 * > * 모든 볼륨 * 을 선택합니다.
3. 칼럼 선택기에서 "디스크 유형" 칼럼이 보기에 나타나는지 확인합니다.

   보고서에 중요한 보기를 만들려면 다른 열을 추가하거나 제거합니다.

4. "클라우드 권장 사항" 열 근처에 있는 "디스크 유형" 열을 끌어 놓습니다.
5. 필터 아이콘을 클릭하고 다음 3개의 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 디스크 유형에 FabricPool가 포함되어 있습니다
   - 클라우드 권장에는 계층이 포함됩니다
   - 콜드 데이터가 10GB보다 큽니다



6. 콜드 데이터 열의 맨 위를 클릭하여 가장 차가운 데이터가 있는 볼륨이 보기의 맨 위에 표시되도록 합니다.
7. 뷰에 표시되는 내용을 반영하는 이름으로 뷰를 저장합니다. 예를 들어 ""Vols change Tiering policy""를 사용할 수 있습니다.



8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
10. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 시스템 관리자 또는 ONTAP CLI를 사용하여 특정 볼륨에 대한 계층화 정책을 ""자동" 또는 ""모두""로 변경하여 더 많은 콜드 데이터를 클라우드 계층으로 오프로드할 수 있습니다.

Qtree 용량 보고서 사용자 지정

이러한 샘플 사용자 지정 보고서는 Qtree 용량과 관련된 잠재적인 문제를 식별하고 이에 대응하는 데 사용됩니다.

거의 가득 찬 **qtree**를 볼 수 있도록 보고서 생성

보고서를 작성하여 Qtree의 스토리지 용량 및 활용률을 분석하고 거의 가득 찬 qtree를 볼 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 거의 꽉 찬 qtree를 표시하는 사용자 지정 보기를 만든 다음 해당 뷰에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * Storage * > * qtree * 를 클릭합니다.
2. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
3. "qtrees used %" 열을 ""qtree" 열 근처로 끕니다.
4. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
    - 사용된 디스크 %가 75%보다 큽니다

5. "Disk Used %" 열의 상단을 클릭하여 결과를 용량 퍼센트로 정렬합니다.
6. 뷰를 ""qtree가 거의 가득 참""과 같이 보이는 뷰를 반영하는 특정 이름으로 저장하고 확인 표시(를 클릭합니다)를 클릭합니다.
7. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
8. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.
9. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시()를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 디스크 하드 및 소프트 제한값(설정된 경우)을 조정하거나 Qtree에서 데이터의 균형을 조정할 수 있습니다.

NFS 공유 보고서 사용자 지정

NFS 공유 보고서를 사용자 지정하여 스토리지 시스템의 볼륨에 대한 NFS 엑스포트 정책 및 규칙에 대한 정보를 분석할 수 있습니다. 예를 들어 보고서를 사용자 지정하여 액세스할 수 없는 마운트 경로가 있는 볼륨과 기본 엑스포트 정책으로 볼륨을 표시할 수 있습니다.

액세스할 수 없는 마운트 경로가 있는 볼륨을 보기 위한 보고서 생성

보고서를 생성하여 액세스할 수 없는 마운트 경로가 있는 볼륨을 찾을 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 액세스할 수 없는 마운트 경로가 있는 볼륨에 대한 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * NFS 공유 * 를 클릭합니다.
2. 보고서에 표시하지 않으려는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
3. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 마운트 경로 활성이 아니오로 표시됩니다
4. 보기에 표시되는 내용을 반영하는 특정 이름으로 뷰를 저장하고("액세스할 수 없는 마운트 경로가 있는 볼륨") 확인 표시를 클릭합니다()를 클릭합니다.
5. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
6. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
7. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시()를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 액세스할 수 없는 마운트 경로를 수정할 수 있습니다.

기본 엑스포트 정책을 사용하는 볼륨을 보기 위한 보고서 생성

보고서를 생성하여 기본 엑스포트 정책을 사용하는 볼륨을 찾을 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 수행하여 기본 엑스포트 정책을 사용하는 볼륨에 대한 사용자 지정 보기를 생성한 다음 해당 뷰에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * NFS 공유 * 를 클릭합니다.
2. 보고서에 표시하지 않으려는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
3. "볼륨" 열 근처에 있는 "내보내기 정책" 열을 끕니다.
4. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
    - 엑스포트 정책에 기본값이 포함되어 있습니다
5. 보기의 표시 내용을 반영하는 특정 이름으로 보기를 저장합니다. 예를 들어 ""기본 내보내기 정책이 있는 볼륨""과 같은 형식으로 저장하고 확인 표시("를 클릭합니다✓)를 클릭합니다.
6. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
7. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
8. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 사용자 지정 엑스포트 정책을 구성할 수 있습니다.

스토리지 **VM** 보고서 사용자 지정

스토리지 VM 보고서를 생성하여 볼륨 정보를 분석하고 전체 상태 및 스토리지 가용성을 볼 수 있습니다. 예를 들어, 보고서를 생성하여 SVM이 최대 볼륨 수에 도달하고 중지된 SVM을 분석할 수 있습니다.

보고서를 생성하여 최대 볼륨 제한에 도달한 스토리지 **VM**을 표시합니다

보고서를 생성하여 최대 볼륨 제한에 도달한 SVM을 찾을 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 최대 볼륨 제한에 도달한 스토리지 VM을 표시하는 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 스토리지 VM * 을 클릭합니다.

2. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
3. "스토리지 VM" 열 근처에 있는 "볼륨 수" 및 "최대 허용 볼륨" 열을 끕니다.
4. "허용되는 최대 볼륨" 열의 맨 위를 클릭하여 가장 많은 볼륨별로 결과를 정렬합니다.
5. "최대 볼륨에 도달한 VM"과 같이 보기에 표시되는 내용을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(를 클릭합니다)를 클릭합니다.
6. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
7. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.
8. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시()를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 스토리지 VM에 할당된 볼륨의 균형을 맞추거나 가능한 경우 ONTAP 시스템 관리자를 사용하여 허용되는 최대 볼륨을 변경할 수 있습니다.

중지된 스토리지 **VM**을 보기 위한 보고서 생성

보고서를 생성하여 중지된 모든 SVM의 목록을 표시할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 중지된 스토리지 VM을 표시하는 사용자 지정 보기를 생성한 다음 해당 보기에 대해 생성할 보고서를 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 스토리지 VM * 을 클릭합니다.
2. 보기 메뉴에서 * 상태 * > * 모든 스토리지 VM * 을 선택합니다.
3. 보고서에 표시하지 않으려는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "스토리지 VM" 열 근처에 있는 "상태" 열을 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 상태가 중지되었습니다
6. "위에 표시된 SVM"과 같이 뷰가 표시된 것을 반영하는 특정 이름으로 뷰를 저장하고 확인 표시(를 클릭합니다)를 클릭합니다.
7. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
8. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.
9. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시()를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 기준으로 SVM이 중지되는 이유를 조사하여 중지된 SVM을 다시 시작해야 하는지 여부를 확인할 수 있습니다.

볼륨 관계 보고서 사용자 지정

볼륨 관계 인벤토리 보고서를 사용하면 클러스터의 스토리지 인벤토리 세부 정보를 분석하고 볼륨에 필요한 보호 수준을 파악하며 장애 소스, 패턴 및 스케줄에 따라 볼륨 세부 정보를 필터링할 수 있습니다.

실패 원인을 기준으로 볼륨 관계를 그룹화하는 보고서 생성

관계가 상태가 양호하지 않은 이유로 볼륨을 그룹화하는 보고서를 생성할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 장애 소스별로 볼륨을 그룹화하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 모든 관계 * 를 선택합니다.
3. "관계 상태" 및 "비정상 이유" 열이 보기에 나타나는지 확인하려면 * 표시/숨기기 * 를 선택합니다.

   보고서에 중요한 보기를 만들려면 다른 열을 추가하거나 제거합니다.

4. '관계 상태'와 '비정상 이유' 열을 '상태' 열 근처에 끌어다 놓습니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 관계 상태가 좋지 않습니다
6. "비정상 이유" 열의 맨 위를 클릭하여 볼륨 관계를 실패 원인별로 그룹화합니다.
7. 보기를 "실패에 따른 볼륨 관계"와 같이 보기의 표시 내용을 반영하는 특정 이름으로 저장합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 각 유형의 실패에 대한 출처와 영향을 조사할 수 있습니다.

문제별로 볼륨 관계를 그룹화하는 보고서 생성

볼륨 관계를 문제별로 그룹화하는 보고서를 만들 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 수행하여 볼륨 관계를 문제별로 그룹화하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 모든 관계 * 를 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. '상태 불량 원인' 열을 '상태' 열 근처로 끕니다.
5. 문제별 부피를 그룹화하려면 ""비정상 이유"" 열의 상단을 클릭합니다.
6. "문제별 볼륨 관계"와 같이 보기에 표시되는 내용을 반영하는 특정 이름으로 보기를 저장합니다.
7. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
8. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 각 문제 유형의 출처와 영향을 조사할 수 있습니다.

특정 시간 간격으로 볼륨 전송 추세를 볼 수 있는 보고서 생성

특정 시간 간격으로 볼륨 전송 추세를 표시하는 보고서를 생성할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 특정 시간 간격으로 볼륨에 대한 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 최근 1개월 전송 상태 * 를 선택합니다.
3. 보고서에서 원하지 않는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. "Operational result(작업 결과)" 열 근처에 있는 전송 기간 열을 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 지난 7일 동안의 전송 종료 시간입니다
6. 시간 간격별로 체적을 정렬하려면 ""전송 기간"" 열의 상단을 클릭합니다.
7. 보기를 표시할 보기를 나타내는 특정 이름(예: ""지속 시간별 볼륨"")으로 저장합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 보고서 일정 이름을 입력하고 빈도를 * Weekly * 로 설정한 다음 다른 보고서 필드를 입력하고 확인 표시(를 클릭합니다✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 전송 시간 간격을 조사할 수 있습니다.

실패한 볼륨 또는 성공한 볼륨 전송을 보기 위한 보고서 생성

볼륨 전송 상태를 표시하는 보고서를 생성할 수 있습니다. 이 보고서에서 실패 및 성공한 볼륨 전송을 모두 볼 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 수행하여 실패한 전송과 성공한 전송을 표시하는 사용자 지정 보기를 만든 다음 해당 보기에 대해 보고서를 생성하도록 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 최근 1개월 전송 상태 * 를 선택합니다.
3. 보고서에 표시하지 않으려는 열을 제거하려면 * 표시/숨기기 * 를 선택합니다.
4. '상태' 열 근처의 '작업 결과' 열을 끕니다.
5. ""Operation result"" 열의 상단을 클릭하여 상태를 기준으로 볼륨을 정렬합니다.
6. 보기의 표시 내용을 반영하는 특정 이름으로 보기를 저장합니다(예: ""전송 상태별 볼륨"").
7. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
8. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 전송 상태를 조사할 수 있습니다.

전송 크기에 따라 볼륨 전송을 보는 보고서 생성

전송 크기에 따라 볼륨 전송을 보는 보고서를 생성할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 전송 크기를 기준으로 볼륨 전송에 대한 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 최근 1개월 전송율 * 을 선택합니다.
3. ""총 전송 크기"" 열의 상단을 클릭하여 크기별로 볼륨 전송을 정렬합니다.
4. 보기를 표시할 보기를 나타내는 특정 이름(예: ""전송 크기별 볼륨"")으로 저장합니다.
5. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
6. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 전송 크기별로 볼륨 관계를 조사할 수 있습니다.

일별 그룹별 볼륨 전송을 보기 위한 보고서 생성

보고서를 생성하여 매일 그룹화된 볼륨 전송을 볼 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 매일 그룹화된 볼륨 전송에 대한 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 관계 * > * 최근 1개월 전송율 * 을 선택합니다.
3. "Day" 열의 상단을 클릭하여 일일 볼륨 전송을 정렬합니다.
4. "일별 볼륨 전송"과 같이 보기에 표시되는 내용을 반영하는 특정 이름으로 보기를 저장합니다.
5. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
6. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 일일 볼륨 전송을 조사할 수 있습니다.

볼륨 성능 보고서 사용자 지정

이러한 샘플 사용자 지정 보고서는 볼륨 성능과 관련된 잠재적인 문제를 식별하고 이에 대응하는 데 사용됩니다.

FabricPool이 지원되지 않는 **aggregate**에서 많은 양의 콜드 데이터가 있는 볼륨을 보기 위한 보고서 생성

비 FabricPool 애그리게이트에 많은 양의 콜드 데이터가 포함된 볼륨을 표시하는 보고서를 생성할 수 있습니다. 이렇게 하면 FabricPool aggregate로 이동해야 하는 볼륨을 식별하는 데 도움이 될 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 비 FabricPool 지원 애그리게이트에서 많은 양의 콜드 데이터가 있는 볼륨에 대한 사용자 지정 보기를 생성한 다음 해당 보기에 대해 보고서를 생성하도록 일정을 예약할 수 있습니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보기 메뉴에서 * 성능 * > * 모든 볼륨 * 을 선택합니다.
3. Show/Hide * 를 선택하여 보기에 "Disk Type" 열이 나타나는지 확인합니다.

   보고서에 중요한 보기를 만들려면 다른 열을 추가하거나 제거합니다.

4. "콜드 데이터" 열 근처에 있는 "디스크 유형" 열을 끕니다.
5. 필터 아이콘을 클릭하고 다음 필터를 추가한 다음 * 필터 적용 * 을 클릭합니다.
   - 100GB 이상의 콜드 데이터
   - 디스크 유형에 SSD가 포함되어 있습니다
6. 디스크 유형 SSD(FabricPool)가 맨 아래에 오도록 디스크 유형별로 볼륨을 정렬하려면 "디스크 유형" 열의 맨 위를 클릭합니다.
7. 보기를 "FabricPool가 아닌 콜드 데이터 볼륨"과 같이 보기에 표시되는 내용을 반영하는 특정 이름으로 저장합니다.
8. 재고 페이지에서 * Scheduled Reports * 버튼을 클릭합니다.
9. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

   보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 기준으로 FabricPool 애그리게이트로 이동하기 적합한 볼륨을 찾을 수 있습니다.

Microsoft Excel 보고서 예제

이 예제 Microsoft Excel 보고서는 Excel 고급 기능을 사용하여 사용할 수 있는 보고 옵션을 소개하기 위한 것입니다.

Excel의 고급 기능을 사용하면 필요에 따라 다양한 보고서를 만들 수 있습니다. Excel 사용 방법에 대한 자세한 내용은 제품 설명서를 참조하십시오.

ⓘ 보고서를 관리하려면 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

집계 용량 테이블 및 차트를 보여 주는 보고서 생성

합계 및 묶은 세로 막대형 차트 형식을 사용하여 Excel 파일의 용량을 분석하는 보고서를 만들 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

상태를 열려면 다음 단계를 수행합니다. 모든 집계 보기, Excel에서 보기 다운로드, 사용 가능한 용량 차트 만들기, 사용자 지정된 Excel 파일 업로드 및 최종 보고서 예약

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.

2. 보고서 * > * Excel 다운로드 * 를 선택합니다.

   브라우저에 따라 * 확인 * 을 클릭하여 파일을 저장해야 할 수 있습니다.

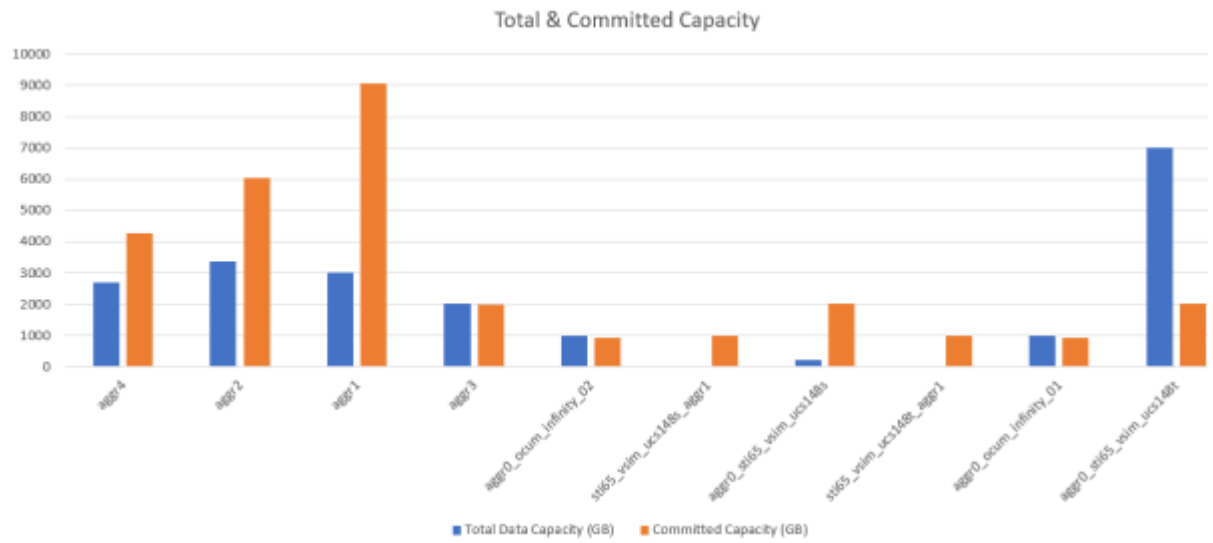
3. 필요한 경우 * 편집 사용 * 을 클릭합니다.
4. Excel에서 다운로드한 파일을 엽니다.
5. 새 시트(⊕) "데이터" 시트 뒤에 * 총 데이터 용량 * 이라는 이름을 지정합니다.
6. 새 Total Data Capacity 시트에 다음 열을 추가합니다.
   a. 총 데이터 용량(GB)
   b. 커밋된 용량(GB)
   c. 사용된 데이터 용량(GB)
   d. 사용 가능한 데이터 용량(GB)
7. 각 열의 첫 번째 행에 다음 수식을 입력하여 데이터 시트(data!)를 참조하고 캡처된 데이터의 올바른 열 및 행 지정자를 참조합니다(총 데이터 용량은 E 열의 데이터를 가져옵니다. 2 - 20행).
   a. =SUM(DATA!E$2:DATA!E$20)
   b. =SUM(DATA!F$2:DATA!F$50)
   c. =SUM(DATA!G$2:DATA!G$50)
   d. =SUM(DATA!H$2:DATA!H$50)

   수식은 현재 데이터를 기준으로 각 열의 합계를 구합니다.

Total Data Capacity (GB)	Committed Capacity (GB)	Used Data Capacity (GB)	Available Data Capacity (GB)
5380.31	6892.47	11764.27	3911.03

1. 데이터 시트에서 * Total Data Capacity(GB) * 및 * Committed Capacity(GB) * 열을 선택합니다.
2. 삽입 * 메뉴에서 * 추천 차트 * 를 선택하고 * 묶은 세로 막대형 * 차트를 선택합니다.
3. 차트를 마우스 오른쪽 버튼으로 클릭하고 차트 이동 * 을 선택하여 차트를 '총 데이터 용량' 시트로 이동합니다.
4. 차트를 선택할 때 사용할 수 있는 * Design * 및 * Format * 메뉴를 사용하여 차트의 모양을 사용자 지정할 수 있습니다.

5. 원하는 대로 파일을 변경 내용과 함께 저장합니다. 파일 이름 또는 위치를 변경하지 마십시오.

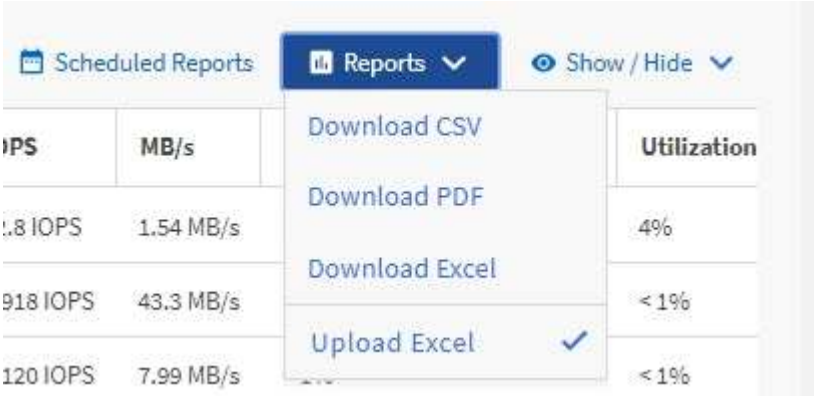


6. Unified Manager에서 * 보고서 * > * Excel 업로드 * 를 선택합니다.

   Excel 파일을 다운로드한 동일한 보기에 있는지 확인합니다.

7. 수정한 Excel 파일을 선택합니다.
8. 열기 * 를 클릭합니다.
9. 제출 * 을 클릭합니다.

   보고서 * > * Excel 업로드 * 메뉴 항목 옆에 확인 표시가 나타납니다.



10. 예약된 보고서 * 를 클릭합니다.
11. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.

    보고서의 * XLSX * 형식을 선택합니다.

12. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 바탕으로 네트워크 전체에서 사용 가능한 용량을 가장 효율적으로 사용하는 방법을 조사하고자 할 수 있습니다.

총 용량 대 사용 가능한 용량 차트를 보여 주는 보고서 생성

보고서를 생성하여 Excel 차트 형식으로 저장 총계와 확정 용량을 분석할 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

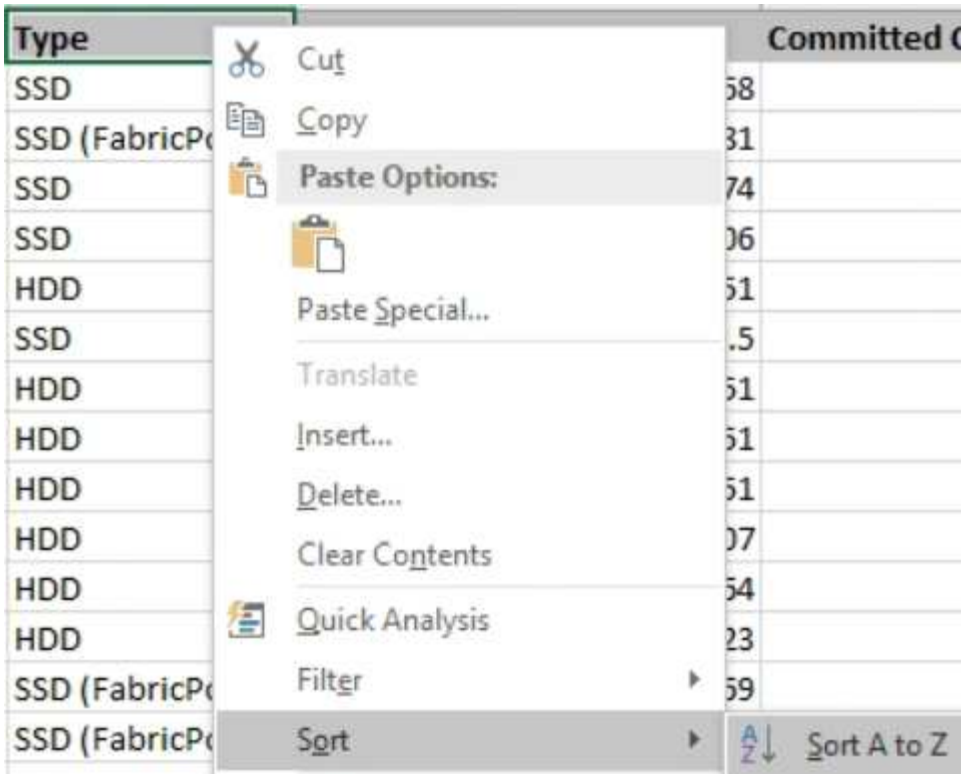
상태를 열려면 다음 단계를 수행합니다. 모든 집계 보기, Excel에서 보기 다운로드, 전체 및 커밋된 용량 차트 만들기, 사용자 지정된 Excel 파일 업로드 및 최종 보고서 예약

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. 보고서 * > * Excel 다운로드 * 를 선택합니다.

   브라우저에 따라 * 확인 * 을 클릭하여 파일을 저장해야 할 수 있습니다.

3. Excel에서 다운로드한 파일을 엽니다.
4. 필요한 경우 * 편집 사용 * 을 클릭합니다.
5. 데이터 시트에서 형식 열을 마우스 오른쪽 단추로 클릭하고 * 정렬 * > * A에서 Z * 정렬 * 을 선택합니다.

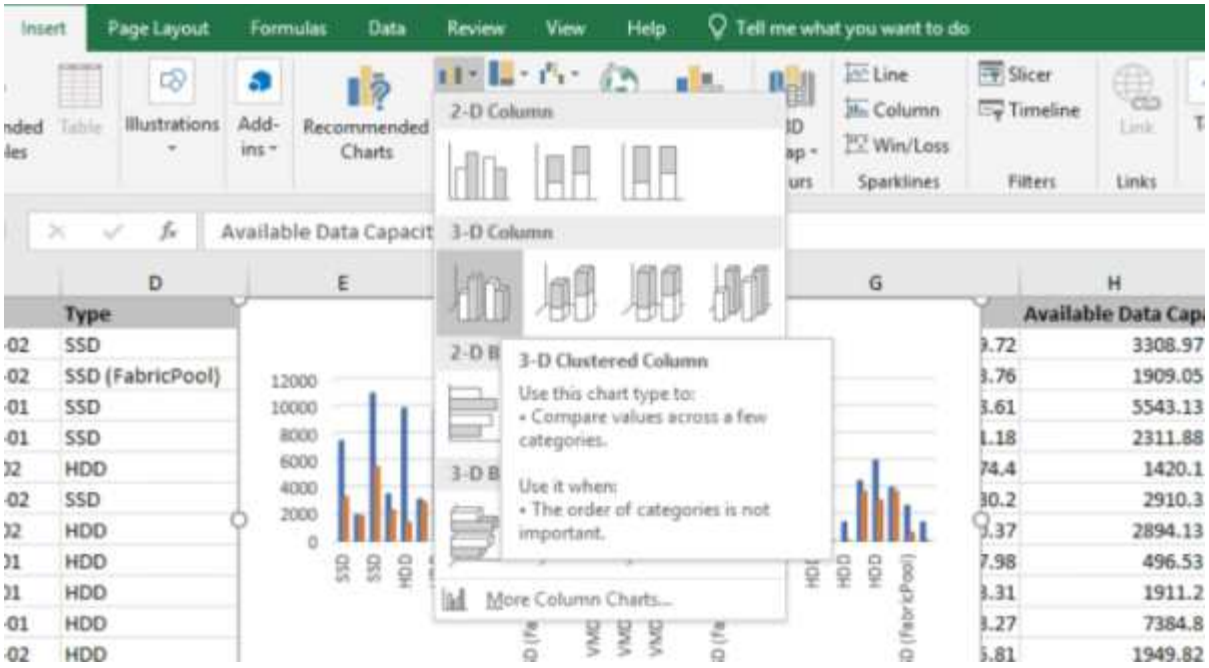


이렇게 하면 다음과 같은 스토리지 유형별로 데이터가 배열됩니다.

- HDD
- 하이브리드
- SSD를 지원합니다
- SSD(FabricPool)

6. Type, Total Data Capacity, Available Data Capacity 열을 선택합니다.
7. 삽입 * 메뉴에서 3차원 세로 막대형 차트를 선택합니다.

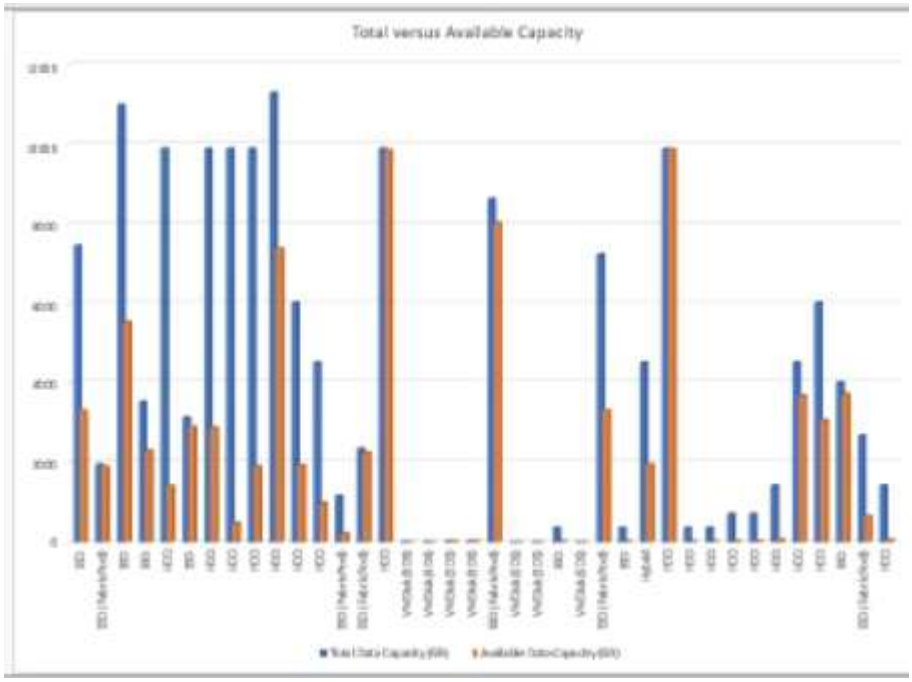
차트가 데이터 시트에 나타납니다.



8. 차트를 마우스 오른쪽 단추로 클릭하고 * 차트 이동 * 을 선택합니다.
9. 새 시트 * 를 선택하고 시트 이름을 * Total Storage Charts * 로 지정합니다.

   새 시트가 정보 및 데이터 시트 뒤에 나타나는지 확인합니다.

10. 차트 제목 이름 * 총 용량과 가용 용량 * 을 지정합니다.
11. 차트를 선택할 때 사용할 수 있는 * Design * 및 * Format * 메뉴를 사용하여 차트의 모양을 사용자 지정할 수 있습니다.
12. 원하는 대로 파일을 변경 내용과 함께 저장합니다. 파일 이름 또는 위치를 변경하지 마십시오.

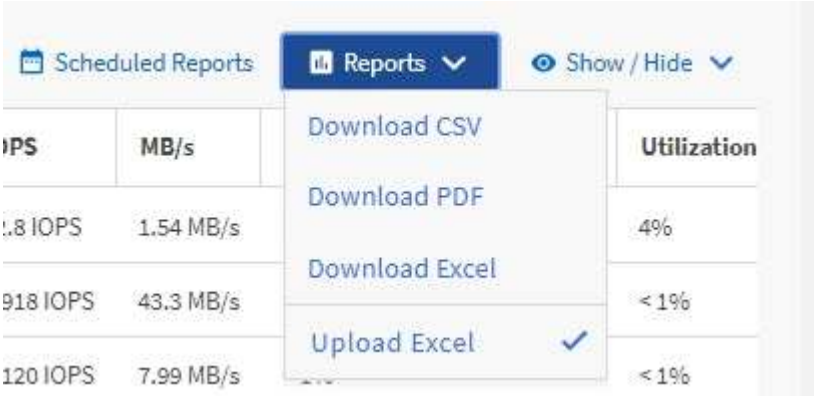


13. Unified Manager에서 * 보고서 * > * Excel 업로드 * 를 선택합니다.

Excel 파일을 다운로드한 동일한 보기에 있는지 확인합니다.

14. 수정한 Excel 파일을 선택합니다.
15. 열기 * 를 클릭합니다.
16. 제출 * 을 클릭합니다.

    보고서 * > * Excel 업로드 * 메뉴 항목 옆에 확인 표시가 나타납니다.



17. 예약된 보고서 * 를 클릭합니다.
18. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.

보고서의 * XLSX * 형식을 선택합니다.

19. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 기준으로 집계 부하의 균형을 맞출 수 있습니다.

보고서를 생성하여 사용 가능한 볼륨 용량 차트를 표시합니다

Excel 차트에서 사용 가능한 볼륨 용량을 분석하는 보고서를 만들 수 있습니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 Health(상태)를 엽니다. All Volumes(모든 볼륨) 보기를 열고, Excel에서 보기를 다운로드하고, 사용 가능한 용량 차트를 만들고, 사용자 지정된 Excel 파일을 업로드하고, 최종 보고서를 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 볼륨 * 을 클릭합니다.
2. 보고서 * > * Excel 다운로드 * 를 선택합니다.

브라우저에 따라 * 확인 * 을 클릭하여 파일을 저장해야 할 수 있습니다.

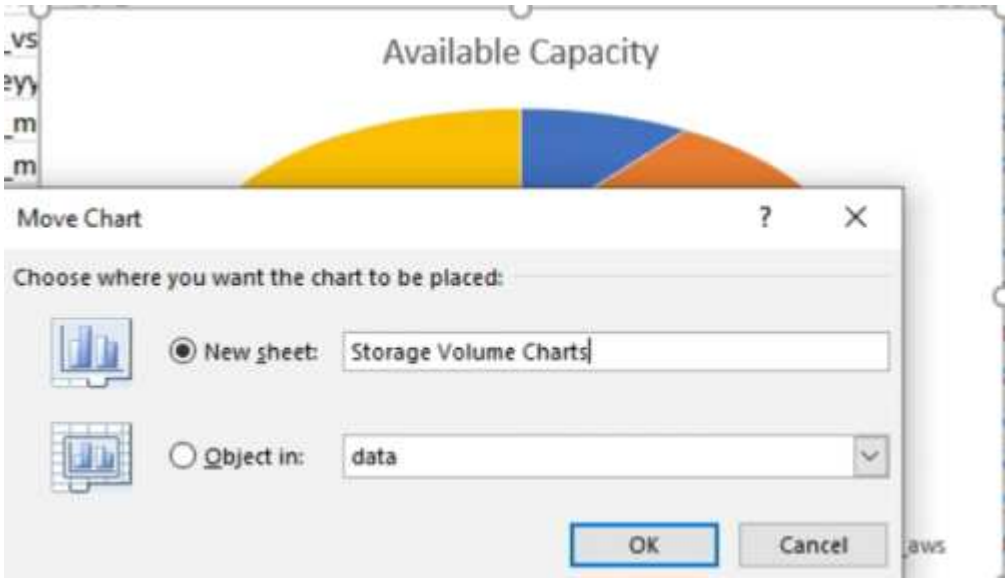
3. 필요한 경우 * 편집 사용 * 을 클릭합니다.
4. Excel에서 다운로드한 파일을 엽니다.
5. "데이터" 시트의 '볼륨' 및 '사용 가능한 데이터' % 열에서 사용할 데이터를 선택합니다.
6. Insert * (삽입 *) 메뉴에서 3-D piechart를 선택합니다

   이 차트는 사용 가능한 공간이 가장 큰 볼륨을 보여 줍니다. 차트가 데이터 시트에 나타납니다.

   네트워크 구성에 따라 전체 열 또는 너무 많은 데이터 행을 선택하면 원형 차트를 읽을 수 없게 될 수 있습니다. 이 샘플에서는 3차원 원형 차트를 사용하지만 모든 차트 종류를 사용할 수 있습니다. 캡처할 데이터를 가장 잘 표시하는 차트를 사용합니다.

7. 차트 제목 이름을 * Available Capacity * 로 지정합니다.
8. 차트를 마우스 오른쪽 단추로 클릭하고 * 차트 이동 * 을 선택합니다.
9. 새 시트 * 를 선택하고 시트 이름을 * 저장소 볼륨 차트 * 로 지정합니다.

   새 시트가 정보 및 데이터 시트 뒤에 나타나는지 확인합니다.

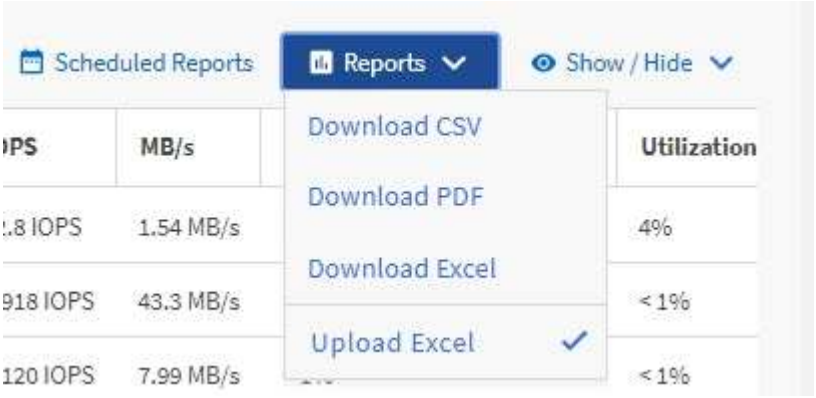


10. 차트를 선택할 때 사용할 수 있는 * Design * 및 * Format * 메뉴를 사용하여 차트의 모양을 사용자 지정할 수 있습니다.
11. 원하는 대로 파일을 변경 내용과 함께 저장합니다.
12. Unified Manager에서 * 보고서 * > * Excel 업로드 * 를 선택합니다.

    Excel 파일을 다운로드한 동일한 보기에 있는지 확인합니다.

13. 수정한 Excel 파일을 선택합니다.
14. 열기 * 를 클릭합니다.
15. 제출 * 을 클릭합니다.

    보고서 * > * Excel 업로드 * 메뉴 항목 옆에 확인 표시가 나타납니다.



16. 예약된 보고서 * 를 클릭합니다.
17. 새 보고서의 일정 특성을 정의할 수 있도록 별표 추가 * 를 클릭하여 * 보고서 일정 * 페이지에 새 행을 추가합니다.
18. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서의 * XLSX * 형식을 선택합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과에 따라 볼륨의 로드 밸런싱을 수행할 수 있습니다.

보고서를 생성하여 사용 가능한 IOPS가 가장 높은 애그리게이트를 확인합니다

이 보고서는 새 워크로드를 프로비저닝할 수 있는 애그리게이트 유형별로 가장 가용성이 높은 IOPS를 제공하는 애그리게이트를 보여줍니다.

- 필요한 것 *
- 애플리케이션 관리자 또는 스토리지 관리자 역할이 있어야 합니다.

다음 단계를 사용하여 Health(상태)를 엽니다. All Volumes(모든 볼륨) 보기를 열고, Excel에서 보기를 다운로드하고, 사용 가능한 용량 차트를 만들고, 사용자 지정된 Excel 파일을 업로드하고, 최종 보고서를 예약합니다.

단계

1. 왼쪽 탐색 창에서 * 스토리지 * > * 애그리게이트 * 를 클릭합니다.
2. View * 드롭다운에서 * Performance: All aggregate * 를 선택합니다.
3. Show/Hide * 를 선택하여 Available IOPS 열을 표시하고 Cluster FQDN, Inactive Data Reporting, Threshold Policy 열을 숨깁니다.
4. Type 열 옆에 Available IOPS와 Free Capacity 열을 끌어다 놓습니다.
5. 사용자 정의 보기의 이름을 지정하고 'Available IOPS per Aggregr.'를 저장합니다
6. 보고서 * > * Excel 다운로드 * 를 선택합니다.

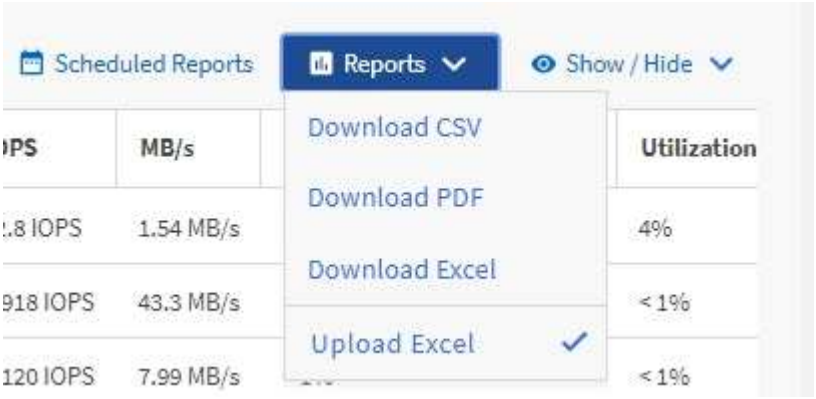
   브라우저에 따라 * 확인 * 을 클릭하여 파일을 저장해야 할 수 있습니다.

7. 필요한 경우 * 편집 사용 * 을 클릭합니다.
8. Excel에서 다운로드한 파일을 엽니다.
9. 데이터 시트에서 시트 왼쪽 위에 있는 작은 삼각형을 클릭하여 시트 전체를 선택합니다.
10. 데이터 * 리본 메뉴의 정렬 및 필터 영역에서 * 정렬 * 을 선택합니다
11. 다음 정렬 수준을 설정합니다.
    a. 정렬 기준 * 을 "사용 가능한 IOPS"(IOPS), * 정렬 기준 * 을 "셀 값"으로, * 순서 * 를 "가장 큰 값에서 가장 작은 값"으로 지정합니다
    b. 레벨 추가 * 를 클릭합니다.
    c. Sort by * 를 Type으로, * Sort on * 을 Cell Values로, * Order * 를 Z to A로 지정합니다
    d. 레벨 추가 * 를 클릭합니다.
    e. Sort by * 를 Free Capacity (GB), Sort on * 을 Cell Values 로, * Order * 를 Largest to Largest 로 지정합니다
    f. 확인 * 을 클릭합니다.
12. Excel 파일을 저장하고 닫습니다.
13. Unified Manager에서 * 보고서 * > * Excel 업로드 * 를 선택합니다.

    Excel 파일을 다운로드한 동일한 보기에 있는지 확인합니다.

14. 수정한 Excel 파일을 선택합니다(이 경우 'performance-aggregate-<date>.xlsx')
15. 열기 * 를 클릭합니다.
16. 제출 * 을 클릭합니다.

    보고서 * > * Excel 업로드 * 메뉴 항목 옆에 확인 표시가 나타납니다.



17. 예약된 보고서 * 를 클릭합니다.
18. 새 보고서의 일정 특성을 정의할 수 있도록 [일정 추가] * 를 클릭하여 [보고서 일정] 페이지에 새 행을 추가합니다.
19. 보고서 일정 이름을 입력하고 다른 보고서 필드를 입력한 다음 확인 표시(✓)를 클릭합니다.

    보고서의 * XLSX * 형식을 선택합니다.

    보고서가 즉시 테스트로 전송됩니다. 그런 다음 보고서가 생성되어 지정된 빈도를 사용하여 나열된 수신자에게 전자 메일로 전송됩니다.

보고서에 표시된 결과를 기준으로 사용 가능한 IOPS가 가장 높은 애그리게이트에 새로운 워크로드를 프로비저닝하고 싶어 할 수 있습니다.

REST API를 사용하여 스토리지 관리

Active IQ Unified Manager REST API 시작하기

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

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

이 콘텐츠의 대상

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

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

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

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

Active IQ Unified Manager API 액세스 및 범주

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

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

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

https://<hostname>/api+ 를 참조하십시오

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

온라인 **API** 설명서 페이지 액세스

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

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

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

범주

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

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

- * 데이터 센터 *

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

- * 관리 - 서버 *

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

- 스토리지 공급자 *

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

- * 관리 *

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

- * 게이트웨이 *

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

- 보안 *

  이 범주에는 Unified Manager 사용자 관리를 위한 API가 포함됩니다.

Active IQ Unified Manager에서 제공되는 REST 서비스

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

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

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

반환되는 최대 레코드 수는 1000개입니다.

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

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

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

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

모든 REST 작업에 대한 자세한 내용은 _Online API 설명서_를 참조하십시오.

Active IQ Unified Manager의 API 버전입니다

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

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

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

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

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

ONTAP의 스토리지 리소스

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

- 물리적 스토리지 리소스 *

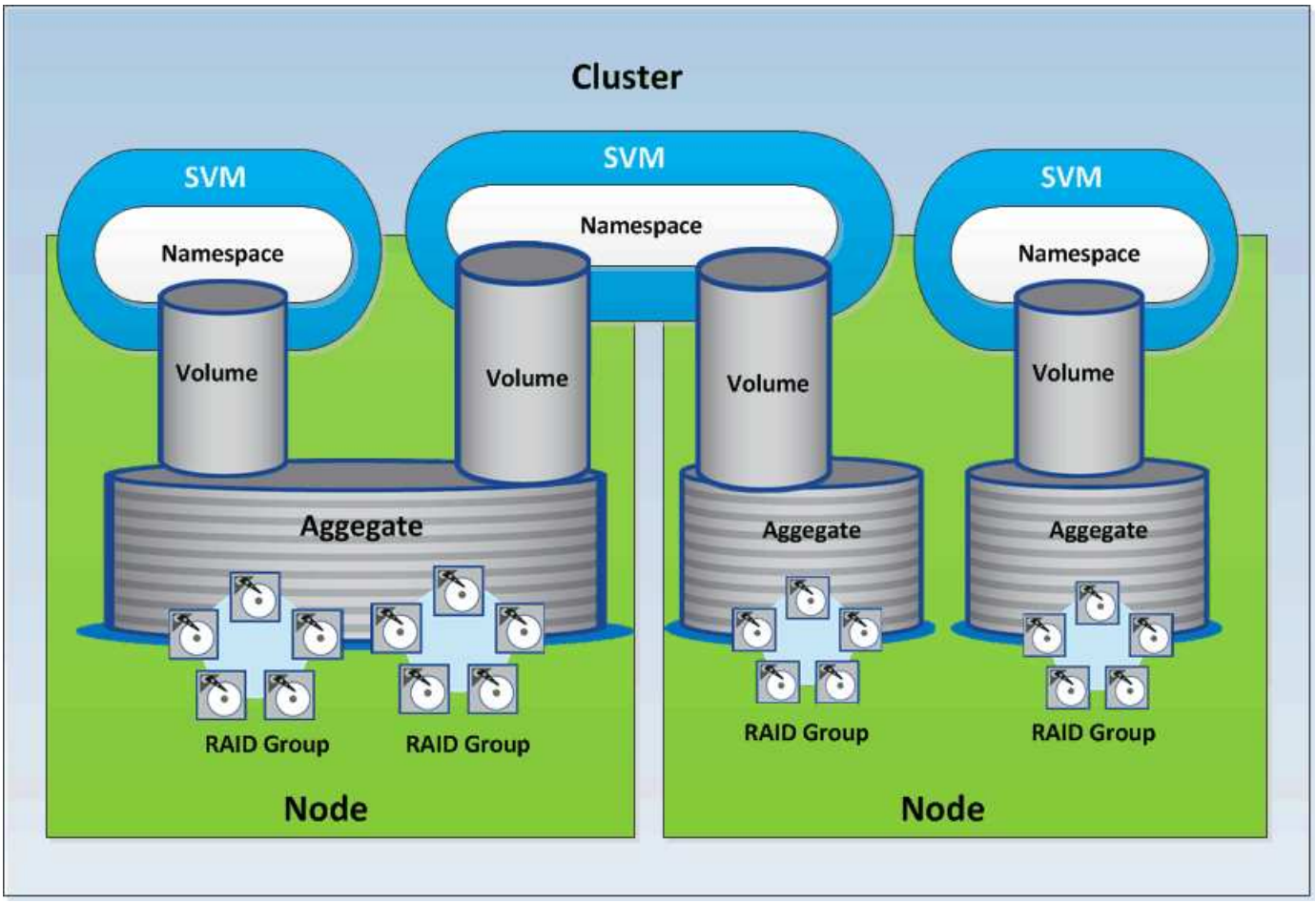
  ONTAP에서 제공하는 물리적 스토리지 객체를 나타냅니다. 물리적 스토리지 리소스에는 디스크, 클러스터, 스토리지 컨트롤러, 노드 및 애그리게이트가 포함됩니다.

- * 논리적 스토리지 리소스 *

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

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

다음 그림에서는 2노드 클러스터의 스토리지 리소스를 보여 줍니다.



Active IQ Unified Manager에서 REST API 액세스 및 인증

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

샘플 요청 및 응답:

- * 요청 *

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

- * 응답 *

```
{
  "records": [
    {
      "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster,uuid=4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
```

```
      "name": "fas8040-206-21",
      "uuid": "4c6bf721-2e3f-11e9-a3e2-00a0985badbb",
      "contact": null,
      "location": null,
      "version": {
        "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17 10:28:33
UTC 2019",
        "generation": 9,
        "major": 5,
        "minor": 0
      },
      "isSanOptimized": false,
      "management_ip": "10.226.207.25",
      "nodes": [
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb",
          "uuid": "12cf06cc-2e3a-11e9-b9b4-00a0985badbb",
          "name": "fas8040-206-21-01",
          "_links": {
            "self": {
              "href": "/api/datacenter/cluster/nodes/4c6bf721-2e3f-11e9-
a3e2-00a0985badbb:type=cluster_node,uuid=12cf06cc-2e3a-11e9-b9b4-
00a0985badbb"
            }
          },
          "location": null,
          "version": {
            "full": "NetApp Release Dayblazer__9.5.0: Thu Jan 17
10:28:33 UTC 2019",
            "generation": 9,
            "major": 5,
            "minor": 0
          },
          "model": "FAS8040",
          "uptime": 13924095,
          "serial_number": "701424000157"
        },
        {
          "key": "4c6bf721-2e3f-11e9-a3e2-
00a0985badbb:type=cluster_node,uuid=1ed606ed-2e3a-11e9-a270-
00a0985bb9b7",
          "uuid": "1ed606ed-2e3a-11e9-a270-00a0985bb9b7",
          "name": "fas8040-206-21-02",
          "_links": {
```

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

- '*IP address/hostname*'은(는) API 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다.
- 포트 443

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

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

인증

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

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

Active IQ Unified Manager에서 사용되는 HTTP 상태 코드입니다

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

다음 표에는 인증과 관련된 오류 코드가 정리되어 있습니다.

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

Active IQ Unified Manager용 API 사용을 위한 권장 사항

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

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

```
application/json
```

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

문제 해결을 위한 로그

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

다음 위치에서 로그를 검색하여 API 호출과 관련된 문제를 해결합니다.

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

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

작업 객체 비동기 프로세스

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

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

작업 개체를 사용하여 설명된 비동기 요청

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

API 요청과 관련된 작업 객체를 쿼리합니다

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

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

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

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

비동기 요청의 단계입니다

다음 고급 절차를 사용하여 비동기 API 호출을 완료할 수 있습니다.

1. 비동기 API 호출을 실행합니다.

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

Hello API 서버

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

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

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

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

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

샘플 코드를 컴파일하고 실행하려면 Java 컴파일러 1.8 이상을 사용해야 합니다.

```
import java.io.BufferedReader;
import java.io.InputStreamReader;
import java.net.URL;
import java.security.SecureRandom;
import java.security.cert.X509Certificate;
import javax.net.ssl.HostnameVerifier;
import javax.net.ssl.HttpsURLConnection;
import javax.net.ssl.SSLContext;
import javax.net.ssl.SSLSession;
import javax.net.ssl.TrustManager;
import javax.net.ssl.X509TrustManager;
```

```
import org.apache.commons.codec.binary.Base64;

public class HelloApiServer {

    private static String server;
    private static String user;
    private static String password;
    private static String response_format = "json";
    private static String server_url;
    private static String port = null;

    /*
     * * The main method which takes user inputs and performs the *
necessary steps
     * to invoke the REST URI and show the response
     */ public static void main(String[] args) {
        if (args.length < 2 || args.length > 3) {
            printUsage();
            System.exit(1);
        }
        setUserArguments(args);
        String serverBaseUrl = "https://" + server;
        if (null != port) {
            serverBaseUrl = serverBaseUrl + ":" + port;
        }
        server_url = serverBaseUrl + "/api/datacenter/svm/svms";
        try {
            HttpsURLConnection connection =
getAllTrustingHttpsUrlConnection();
            if (connection == null) {
                System.err.println("FATAL: Failed to create HTTPS
connection to URL: " + server_url);
                System.exit(1);
            }
            System.out.println("Invoking API: " + server_url);
            connection.setRequestMethod("GET");
            connection.setRequestProperty("Accept", "application/" +
response_format);
            String authString = getAuthorizationString();
            connection.setRequestProperty("Authorization", "Basic " +
authString);
            if (connection.getResponseCode() != 200) {
                System.err.println("API Invocation Failed : HTTP error
code : " + connection.getResponseCode() + " : "
                        + connection.getResponseMessage());
                System.exit(1);
```

```
            }
            BufferedReader br = new BufferedReader(new
InputStreamReader((connection.getInputStream())));
            String response;
            System.out.println("Response:");
            while ((response = br.readLine()) != null) {
                System.out.println(response);
            }
            connection.disconnect();
        } catch (Exception e) {
            e.printStackTrace();
        }
    }

    /* Print the usage of this sample code */ private static void
printUsage() {
        System.out.println("\nUsage:\n\tHelloApiServer <hostname> <user>
<password>\n");
        System.out.println("\nExamples:\n\tHelloApiServer localhost admin
mypassword");
        System.out.println("\tHelloApiServer 10.22.12.34:8320 admin
password");
        System.out.println("\tHelloApiServer 10.22.12.34 admin password
");
        System.out.println("\tHelloApiServer 10.22.12.34:8212 admin
password \n");
        System.out.println("\nNote:\n\t(1) When port number is not
provided, 443 is chosen by default.");
    }

    /* * Set the server, port, username and password * based on user
inputs. */ private static void setUserArguments(
            String[] args) {
        server = args[0];
        user = args[1];
        password = args[2];
        if (server.contains(":")) {
            String[] parts = server.split(":");
            server = parts[0];
            port = parts[1];
        }
    }

    /*
     * * Create a trust manager which accepts all certificates and * use
this trust
```

```
     * manager to initialize the SSL Context. * Create a
HttpsURLConnection for this
     * SSL Context and skip * server hostname verification during SSL
handshake. * *
     * Note: Trusting all certificates or skipping hostname verification *
is not
     * required for API Services to work. These are done here to * keep
this sample
     * REST Client code as simple as possible.
     */ private static HttpsURLConnection
getAllTrustingHttpsUrlConnection()    {        HttpsURLConnection conn =
null;        try {            /* Creating a trust manager that does not
validate certificate chains */            TrustManager[]
trustAllCertificatesManager = new                    TrustManager[]{new
X509TrustManager(){
     public X509Certificate[] getAcceptedIssuers(){return  null;}
     public void checkClientTrusted(X509Certificate[]
certs, String authType){}
     public void checkServerTrusted(X509Certificate[]
certs, String authType){}            }};            /* Initialize the
SSLContext with the all-trusting trust manager */
     SSLContext sslContext = SSLContext.getInstance("TLS");
sslContext.init(null, trustAllCertificatesManager, new
SecureRandom());
HttpsURLConnection.setDefaultSSLSocketFactory(sslContext.getSocketFactory(
));            URL url = new URL(server_url);            conn =
(HttpsURLConnection) url.openConnection();            /* Do not perform an
actual hostname verification during SSL Handshake.            Let all
hostname pass through as verified.*/
conn.setHostnameVerifier(new HostnameVerifier() {               public
boolean verify(String host, SSLSession                        session) {
return true;                }            });        } catch (Exception e)
{            e.printStackTrace();        }        return conn;    }

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

```
}
```

Unified Manager REST API

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

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

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

- 범주

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

- HTTP 동사(호출)

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

- 경로

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

API를 사용하여 데이터 센터의 스토리지 오브젝트 관리

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

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

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

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

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

데이터 센터의 스토리지 오브젝트를 위한 **API**

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

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

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

참고 사항:

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

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

데이터 센터의 네트워크 요소를 위한 **API**입니다

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

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

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

프록시 액세스를 통해 **ONTAP API** 액세스

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

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

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

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

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

API 게이트웨이 터널링 이해

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

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

> ONTAP API가 API 게이트웨이를 통해 성공적으로 실행되려면 API가 실행 중인 ONTAP 클러스터의 해당 버전에서 지원되어야 합니다. ONTAP 클러스터에서 지원되지 않는 API를 실행해도 결과가 반환되지 않습니다.

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

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

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

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

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

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

- 샘플 curl 명령 *

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

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

API 범위 설정

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

- 샘플 curl 명령 *

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

ONTAP REST API 사용에 대한 자세한 내용은 를 참조하십시오https://docs.netapp.com/us-en/ontap-automation/index.html["ONTAP REST API 자동화"]

API를 사용하여 관리 작업 수행

관리 범주의 API를 사용하여 백업 설정을 수정하고, 백업 파일 정보와 클러스터 인증서를 확인하고, ONTAP 클러스터를 Active IQ Unified Manager 데이터 소스로 관리할 수 있습니다.

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

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

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

API를 사용하여 사용자 관리

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

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

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

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

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

API를 사용하여 성능 메트릭 보기

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

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

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

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

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

메트릭	분석
노드나 클러스터의 세부 정보와 같이 개체의 기본 세부 정보가 검색됩니다.	특정 세부 정보가 검색되지 않습니다.
최소, 최대, 95번째 백분위수 및 특정 기간 동안의 평균 성능 값과 같은 누적 카운터는 읽기, 쓰기, 합계 및 기타 카운터 등의 단일 개체에 대해 검색됩니다.	동일한 형식의 모든 개체에 대해 집계된 단일 값이 표시됩니다.
시간 범위 및 예제 데이터는 데이터의 시간 범위인 다음 일정을 기반으로 합니다. 예: 1h, 12h, 1d, 2D, 3D, 15d, 1W, 1m, 2m, 3m, 6개월 범위가 3일(72시간)을 초과하는 경우 1시간 샘플이 수집되고, 그렇지 않은 경우 5분 샘플이 제공됩니다. 각 시간 범위의 기간은 다음과 같습니다. • 1시간: 5분 동안 샘플링한 최근 시간에 대한 메트릭입니다. • 12h: 5분 동안 샘플링한 최근 12시간 동안의 메트릭입니다. • 1D: 5분 동안 샘플링한 가장 최근 날짜의 메트릭 • 2D: 5분 동안 샘플링한 최근 2일간의 메트릭 • 3D: 5분 동안 가장 최근 3일간 샘플링한 메트릭스. • 15d: 1시간 동안 샘플링한 최근 15일간의 지표. • 1W: 1시간 동안 샘플링한 가장 최근 주에 대한 메트릭입니다. • 1m: 1시간 이상 샘플링한 가장 최근 달의 측정 지표입니다. • 2M: 1시간 동안 샘플링한 최근 2개월 동안의 메트릭 • 3M: 1시간 동안 샘플링한 최근 3개월 동안의 지표. • 6M: 1시간 동안 가장 최근 6개월 동안 샘플링한 수치. 사용 가능한 값: 1h, 12h, 1d, 2D, 3D, 15d, 1W, 1m, 2m, 3m, 6개월 기본값: 1h	72시간 이상. 이 샘플이 계산되는 기간은 ISO-8601 표준 형식으로 표시됩니다.

메트릭 **API**의 출력 샘플

예를 들어, '/datacenter/cluster/nodes/{key}/metrics' API는 노드에 대해 다음과 같은 세부 정보를 검색합니다.

요약 값의 95 백분위수는 해당 기간 동안 수집된 샘플의 95%가 95 백분위수로 지정된 값보다 작은 카운터 값을 가졌음을 나타냅니다.

```
{
```

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

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

분석 **API**의 출력 샘플

예를 들어, '/datacenter/cluster/nodes/analytics' API는 모든 노드에 대해 다음 값(다른 값 중)을 검색합니다.

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


사용 가능한 **API**의 목록입니다

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

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

HTTP 동사	경로	설명
"내려가세요	'/datacenter/cluster/clusters/{key}/metrics'	이 명령어는 cluster key의 input 매개변수로 지정한 cluster의 성능 데이터(샘플 및 요약)를 조회한다. 클러스터 키 및 UUID, 시간 범위, IOPS, 처리량, 샘플 수와 같은 정보가 반환됩니다.
"내려가세요	'/datacenter/cluster/cluster/analytics'	이 명령어는 데이터 센터의 모든 클러스터에 대한 고성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 집계된 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.
"내려가세요	'/datacenter/cluster/nodes/{key}/metrics'	노드 키의 input 매개 변수로 지정된 노드의 성능 데이터(샘플 및 요약)를 검색합니다. 노드 UUID, 시간 범위, IOPS 요약, 처리량, 지연 시간 및 성능, 수집된 샘플 수, 활용도와 같은 정보가 반환됩니다.
"내려가세요	'/datacenter/cluster/nodes/analytics'	이 명령어는 데이터 센터 내 모든 노드에 대해 높은 수준의 성능 지표를 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 노드 및 클러스터 키와 같은 정보와 집계된 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.
"내려가세요	'/datacenter/storage/aggregate/{key}/metrics'	이 명령어는 aggregate key의 input parameter로 지정된 aggregate에 대한 성능 데이터(sample, summary)를 조회한다. 시간 범위, IOPS 요약, 지연 시간, 처리량 및 성능 용량, 각 카운터에 대해 수집된 샘플 수, 사용된 비율 등의 정보가 반환됩니다.
"내려가세요	'/datacenter/storage/aggregate/analytics'	이 명령어는 데이터 센터의 모든 애그리게이트를 위한 높은 수준의 성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 집계 및 클러스터 키와 같은 정보와 집계 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.

HTTP 동사	경로	설명
"내려가세요	'/datacenter/storage/LUNs/{key}/metrics' '/datacenter/storage/volumes/{key}/metrics'	LUN 또는 볼륨 키의 입력 매개 변수로 지정한 LUN 또는 파일 공유(볼륨)의 성능 데이터(샘플 및 요약)를 검색합니다. 읽기, 쓰기 및 총 IOPS, 지연 시간, 처리량의 최소, 최대 및 평균에 대한 요약과 같은 정보 각 카운터에 대해 수집된 샘플의 수가 반환됩니다.
"내려가세요	'/datacenter/storage/LUNs/analytics' '/datacenter/storage/volumes/analytics'	이 명령어는 데이터 센터의 모든 LUN 또는 볼륨에 대해 높은 수준의 성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 스토리지 VM 및 클러스터 키와 같은 정보와 집계 IOPS, 처리량 및 수집 기간(시간)과 같은 값이 반환됩니다.
"내려가세요	'/datacenter/svm/sSVM/{key}/metrics'	스토리지 VM 키의 입력 매개 변수로 지정한 스토리지 VM의 성능 데이터(샘플 및 요약)를 검색합니다. nvmf, fcp, iscsi, NFS, 처리량 등 지원되는 각 프로토콜을 기반으로 한 IOPS 요약 지연 시간 및 수집된 샘플의 수가 반환됩니다.
"내려가세요	'/datacenter/svm/sSVM/analytics'	이 명령어는 데이터 센터에 있는 모든 스토리지 VM에 대한 높은 수준의 성능 메트릭을 조회한다. 필요한 기준에 따라 결과를 필터링할 수 있습니다. 스토리지 VM UUID, 집계된 IOPS, 지연 시간, 처리량 및 수집 기간(시간)과 같은 정보가 반환됩니다.
"내려가세요	'/datacenter/network/ethernet/ports/{key}/metrics'	이 명령어는 Port Key의 INPUT 파라미터로 지정된 특정 Ethernet Port에 대한 성능 메트릭을 조회한다. 지원되는 범위에서 간격(시간 범위)을 제공하면 API는 시간 동안 누적된 카운터(예: 최소값, 최대값 및 평균 성능 값)를 반환합니다.

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

HTTP 동사	경로	설명
"내려가세요	'/datacenter/network/ip/interface/{key}/metrics'	이 명령어는 interface key의 input parameter에 의해 지정된 네트워크 IP interface에 대한 성능 메트릭을 조회한다. 지원 범위에서 간격(시간 범위)이 제공된 경우 API는 샘플 수, 누적 카운터, 처리량 및 송수신 패킷 수와 같은 정보를 반환합니다.
"내려가세요	'/datacenter/network/ip/interfaces/analytics'	이 명령어는 데이터 센터 환경의 모든 네트워크 IP 인터페이스에 대한 높은 수준의 성능 지표를 조회한다. 클러스터 및 IP 인터페이스 키와 UUID, 처리량, IOPS, 지연 시간 등의 정보가 반환됩니다. 클러스터 및 IP 인터페이스 이름 및 UUID, IOPS, 지연 시간, 처리량 등과 같은 사용 가능한 매개 변수를 사용하여 결과를 필터링할 수 있습니다.

작업 및 시스템 세부 정보 보기

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

작업 보기

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

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

범주	HTTP 동사	경로	설명
관리 - 서버	가져오기	(/management-server/jobs)	모든 작업의 작업 세부 정보를 반환합니다. 정렬 순서가 없으면 마지막으로 제출한 작업 객체가 맨 위에 반환됩니다.

범주	HTTP 동사	경로	설명
관리 - 서버	가져오기	'/management-server/jobs/{key}' 해당 작업의 특정 세부 정보를 보려면 작업 오브젝트의 작업 키를 입력합니다.	특정 작업 오브젝트의 세부 정보를 반환합니다.

시스템 세부 정보 보기

'/management-server/system' API를 사용하여 Unified Manager 환경의 인스턴스별 세부 정보를 쿼리할 수 있습니다. API는 시스템에 설치된 Unified Manager 버전, UUID, 공급업체 이름, 호스트 OS, 이름 등과 같은 제품 및 서비스에 대한 정보를 반환합니다. Unified Manager 인스턴스에서 실행 중인 서비스에 대한 설명 및 상태

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

API를 사용하여 이벤트 및 경고 관리

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

이벤트 보기 및 수정

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

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

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

이벤트에 대한 자세한 내용은 를 참조하십시오 "이벤트 관리".

범주	**HTTP** 동사	경로	설명
관리 - 서버	가져오기	'/management-server/events'/management-server/events/{key}'	모두 가져오기 메서드를 실행할 때 응답 본문은 데이터 센터의 모든 이벤트에 대한 이벤트 세부 정보로 구성됩니다. 특정 키로 이벤트 세부 정보를 검색할 때 특정 이벤트의 세부 정보를 보고 리소스에 대한 다음 작업 집합을 실행할 수 있습니다. 응답 본문은 해당 이벤트의 세부 정보로 구성됩니다.
관리 - 서버	패치	'Management-server/events/{key}'	이 API를 실행하여 이벤트를 할당하거나 상태를 확인됨 또는 해결됨 으로 변경합니다. 또한 이 메서드를 사용하여 사용자나 다른 사용자에게 이벤트를 할당할 수도 있습니다. 동기식 작업입니다.

알림 관리

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

알림에 대한 자세한 내용은 을 참조하십시오 "알림 관리".

범주	**HTTP** 동사	경로	설명
관리 - 서버	가져오기	'/management-server/alerts"/management-server/alerts/{key}'	경고 키를 사용하여 사용자 환경 또는 특정 알림에 있는 기존 경고를 모두 쿼리합니다. 알림 설명, 작업, 알림을 보낼 e-메일 ID, 이벤트, 심각도 등 사용자 환경에서 생성된 알림에 대한 정보를 볼 수 있습니다.

범주	HTTP 동사	경로	설명
관리 - 서버	게시	'/management-server/alerts'	이 방법을 사용하면 특정 이벤트에 대한 알림을 추가할 수 있습니다. 경고 이름, 물리적 또는 논리적 리소스 또는 경고를 적용할 수 있는 이벤트, 경고가 설정되었는지 여부 및 SNMP 트랩을 발행하는지 여부를 추가해야 합니다. 알림 스크립트를 추가하는 경우 작업, 알림 이메일 ID, 스크립트 세부 정보 등과 같이 알림을 생성할 추가 세부 정보를 추가할 수 있습니다.
관리 - 서버	패치 및 삭제	'Management-server/events/{key}'	이러한 방법을 사용하여 특정 경고를 수정 및 삭제할 수 있습니다. 설명, 이름, 알림 설정 및 해제 등 다양한 속성을 수정할 수 있습니다. 알림이 더 이상 필요하지 않은 경우 알림을 삭제할 수 있습니다.

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

스크립트 관리

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

스크립트에 대한 자세한 내용은 을 참조하십시오 "스크립트 관리".

범주	HTTP 동사	경로	설명
관리 - 서버	가져오기	'/management-server/scripts'	이 API를 사용하여 사용자 환경의 모든 기존 스크립트를 쿼리합니다. 특정 스크립트만 보려면 표준 필터 및 작업별 순서를 사용합니다.

범주	HTTP 동사	경로	설명
관리 - 서버	게시	'/management-server/scripts'	이 API를 사용하여 스크립트에 대한 설명을 추가하고 경고와 관련된 스크립트 파일을 업로드합니다.

API를 사용하여 워크로드 관리

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

API를 사용하여 스토리지 워크로드 보기

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

스토리지 워크로드를 봅니다

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

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

스토리지 워크로드 요약 보기

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

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

API를 사용하여 액세스 엔드포인트 관리

SVM(Storage Virtual Machine), LUN 및 파일 공유를 프로비저닝하는 데 필요한 액세스 엔드포인트 또는 논리 인터페이스(LIF)를 생성해야 합니다. Active IQ Unified Manager

환경에서 SVM, LUN 또는 파일 공유에 대한 액세스 엔드포인트를 확인, 생성, 수정 및 삭제할 수 있습니다.

액세스 끝점을 봅니다

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

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

액세스 끝점을 추가합니다

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

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

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

액세스 끝점을 삭제합니다

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

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

액세스 끝점을 수정합니다

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

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

API를 사용하여 **Active Directory** 매핑 관리

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

Active Directory 매핑을 봅니다

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

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

Active Directory 매핑을 추가합니다

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

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

API를 사용하여 파일 공유 관리

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

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

파일 공유를 봅니다

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

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

파일 공유를 추가합니다

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

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

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

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

파일 공유를 삭제합니다

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

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

파일 공유를 수정합니다

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

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

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

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

API를 사용하여 **LUN** 관리

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

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

LUN을 봅니다

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

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

LUN을 추가합니다

다음 방법을 사용하여 SVM에 LUN을 추가할 수 있습니다.

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

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

LUN을 삭제합니다

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

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

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

LUN을 수정합니다

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

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

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

API를 사용하여 성능 서비스 수준 관리

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

성능 서비스 수준을 봅니다

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

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

성능 서비스 수준 추가

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

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

성능 서비스 수준을 삭제합니다

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

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

성능 서비스 수준을 수정합니다

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

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

성능 서비스 수준에 따라 집계 기능 보기

다음 방법을 사용하여 성능 서비스 수준에 따라 집계 기능을 쿼리할 수 있습니다. 이 API는 데이터 센터에서 사용할 수 있는 애그리게이트 목록을 반환하고 해당 애그리게이트에서 지원되는 성능 서비스 수준과 관련된 기능을 나타냅니다. 볼륨에서 워크로드를 프로비저닝하는 동안 특정 성능 서비스 수준을 지원하는 애그리게이트의 기능을 확인하고 해당 기능을 기준으로 워크로드를 프로비저닝할 수 있습니다. Aggregate를 지정하는 기능은 API를 사용하여 워크로드를 프로비저닝할 때만 사용할 수 있습니다. 이 기능은 Unified Manager 웹 UI에서 사용할 수 없습니다.

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

API를 사용하여 스토리지 효율성 정책 관리

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

다음 사항을 참고하십시오.

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

스토리지 효율성 정책을 봅니다

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

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

스토리지 효율성 정책을 추가합니다

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

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

스토리지 효율성 정책을 삭제합니다

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

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

스토리지 효율성 정책을 수정합니다

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

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

스토리지 관리를 위한 공통 **API** 워크플로우

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

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

워크플로에 사용되는 **API** 호출 이해

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

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

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

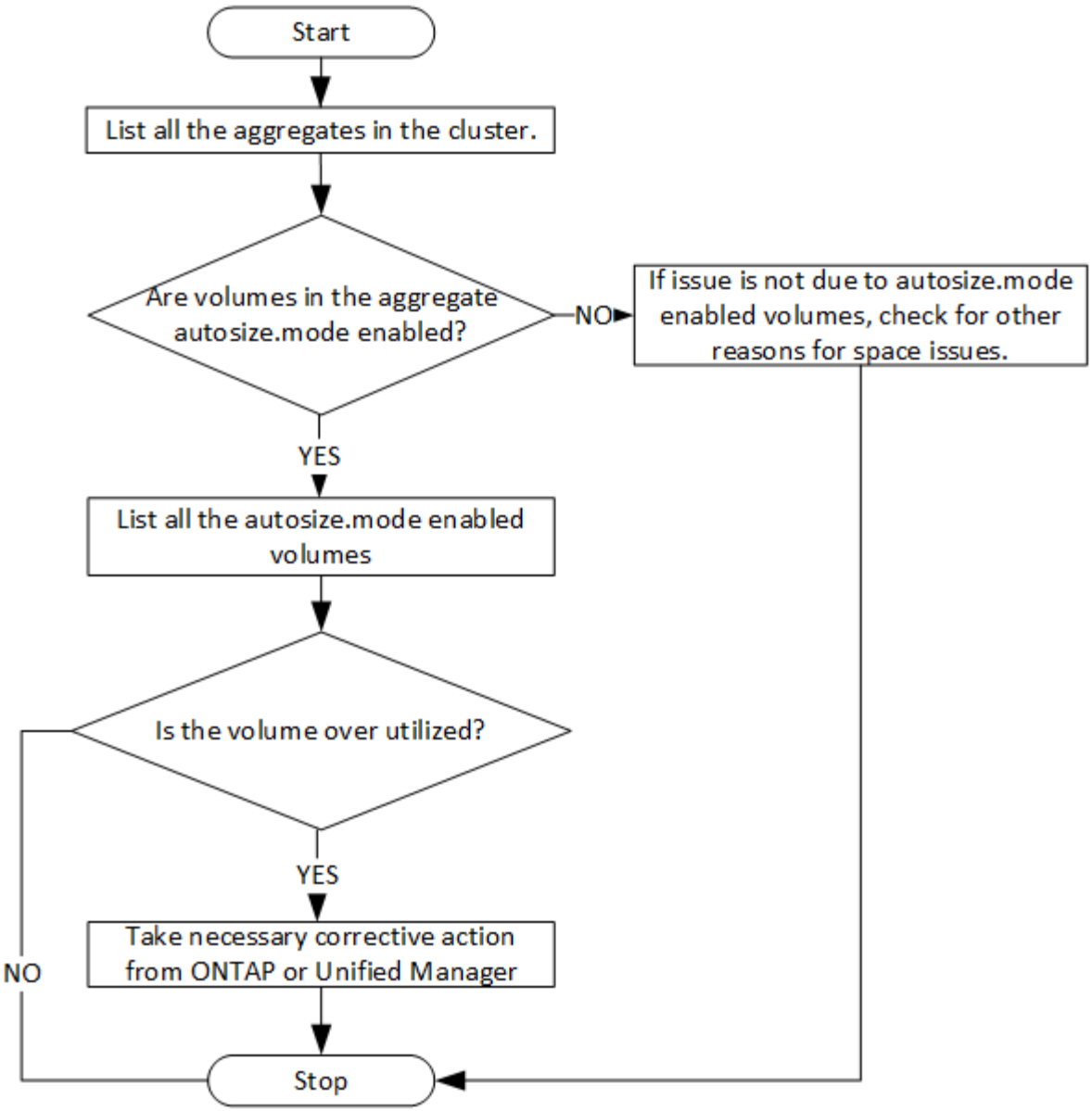
API를 사용하여 Aggregate의 공간 문제 확인

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

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

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

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



이 플로우에서는 클러스터가 ONTAP에서 이미 생성되어 Unified Manager에 추가되었다고 가정합니다.

1. 값을 모르는 경우 클러스터 키를 얻습니다.

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

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

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

3. 응답에서 애그리게이트의 공간 사용을 분석하고 공간 문제가 있는 애그리게이트를 결정합니다. 공간 문제가 있는 각 애그리게이트의 경우 동일한 JSON 출력에서 애그리게이트 키를 가져옵니다.

4. 각 집계 키를 사용하여 AutoSize.mode 매개 변수의 값이 있는 모든 볼륨을 'grow'로 필터링합니다

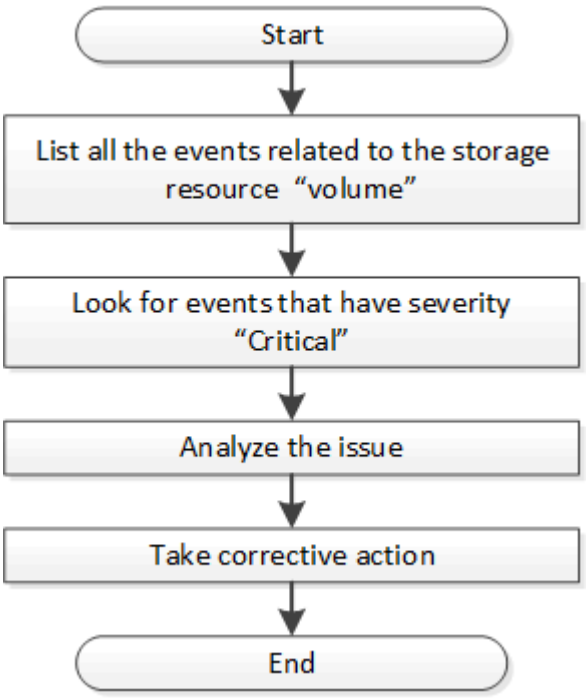
범주	**HTTP** 동사	경로
데이터 센터	가져오기	'/datacenter/storage/volumes'

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

이벤트 **API**를 사용하여 스토리지 개체의 문제 확인

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

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



개선 단계를 수행하기 전에 볼륨의 문제를 확인하려면 다음 단계를 수행하십시오.

단계

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

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

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

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

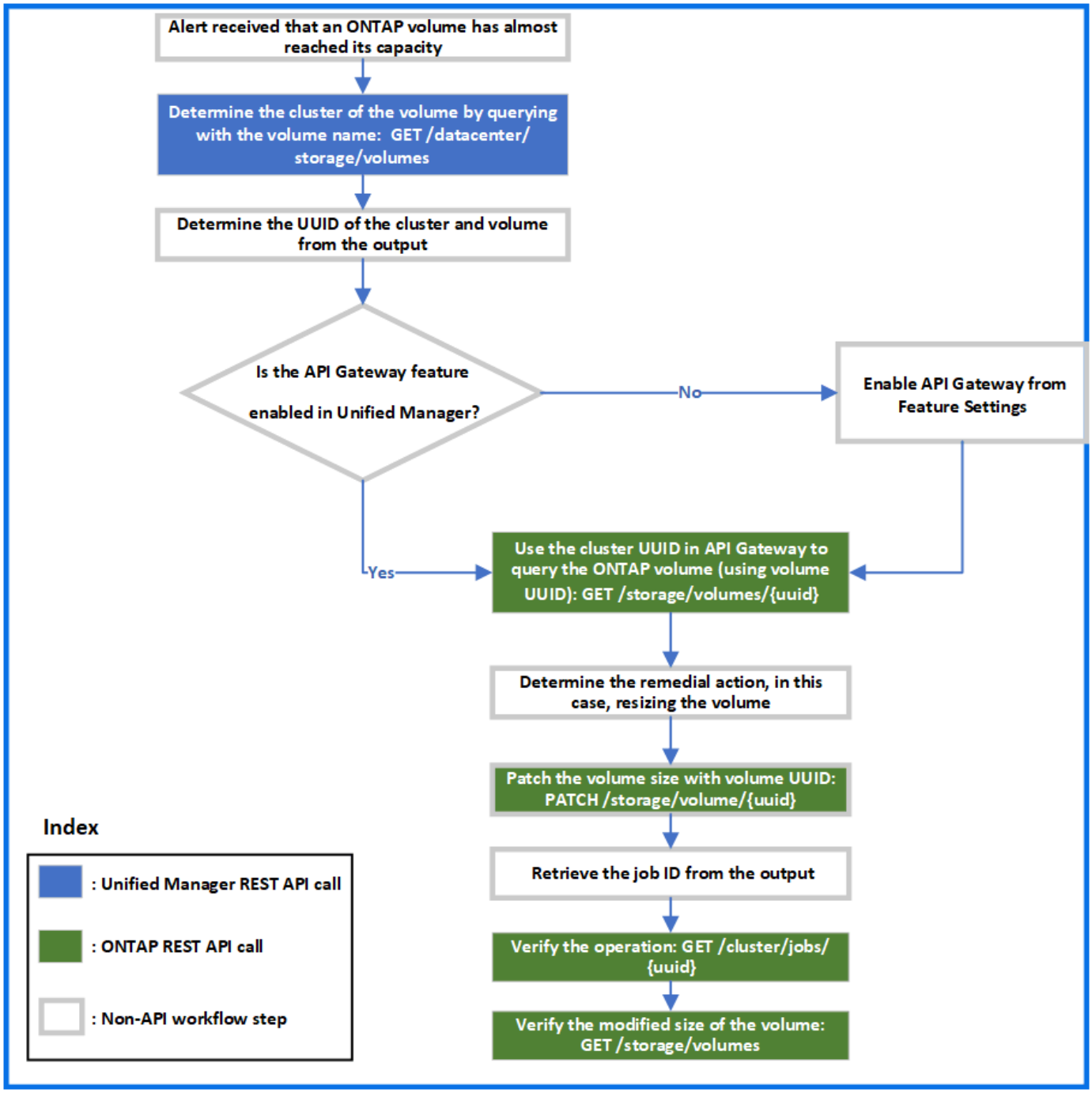
게이트웨이 API는 ONTAP API를 호출하여 ONTAP 스토리지 객체에 대한 정보를 쿼리하고 보고된 문제를 해결하기 위한 조치를 취하는 게이트웨이 역할을 합니다.

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

워크플로 단계를 실행하기 전에 다음 사항을 확인하십시오.

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

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



워크플로우에서 Unified Manager와 ONTAP REST API의 호출 포인트를 모두 지원합니다.

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

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

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

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

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

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

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

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

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

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

   ◦ 샘플 curl 명령 *

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

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

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

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

◦ 샘플 curl 명령 *

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

+
JSON 출력은 작업 UUID를 반환합니다.

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

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

반환되는 HTTP 코드는 ONTAP REST API HTTP 상태 코드와 동일합니다.

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

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

출력에는 120GB의 증가된 볼륨 크기가 표시됩니다.

워크로드 관리를 위한 **API** 워크플로우

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

다음 워크플로에 대해 설명합니다.

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

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

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

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

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

API를 사용하여 클러스터에서 **SVM** 확인

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

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

1. 클러스터에 SVM이 생성되었는지 확인합니다.

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

◦ 샘플 컬 *

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

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

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

클러스터 키를 가져옵니다.

◦ 샘플 컬 *

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

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

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

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

◦ 샘플 컬 *

SVM 객체 세부 정보를 입력 매개 변수로 입력합니다.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {},
\"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\",
\"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-
00a0986138f7\" } ],
\"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\":
\"string\",
\"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" },
\"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-
123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcp\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

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

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

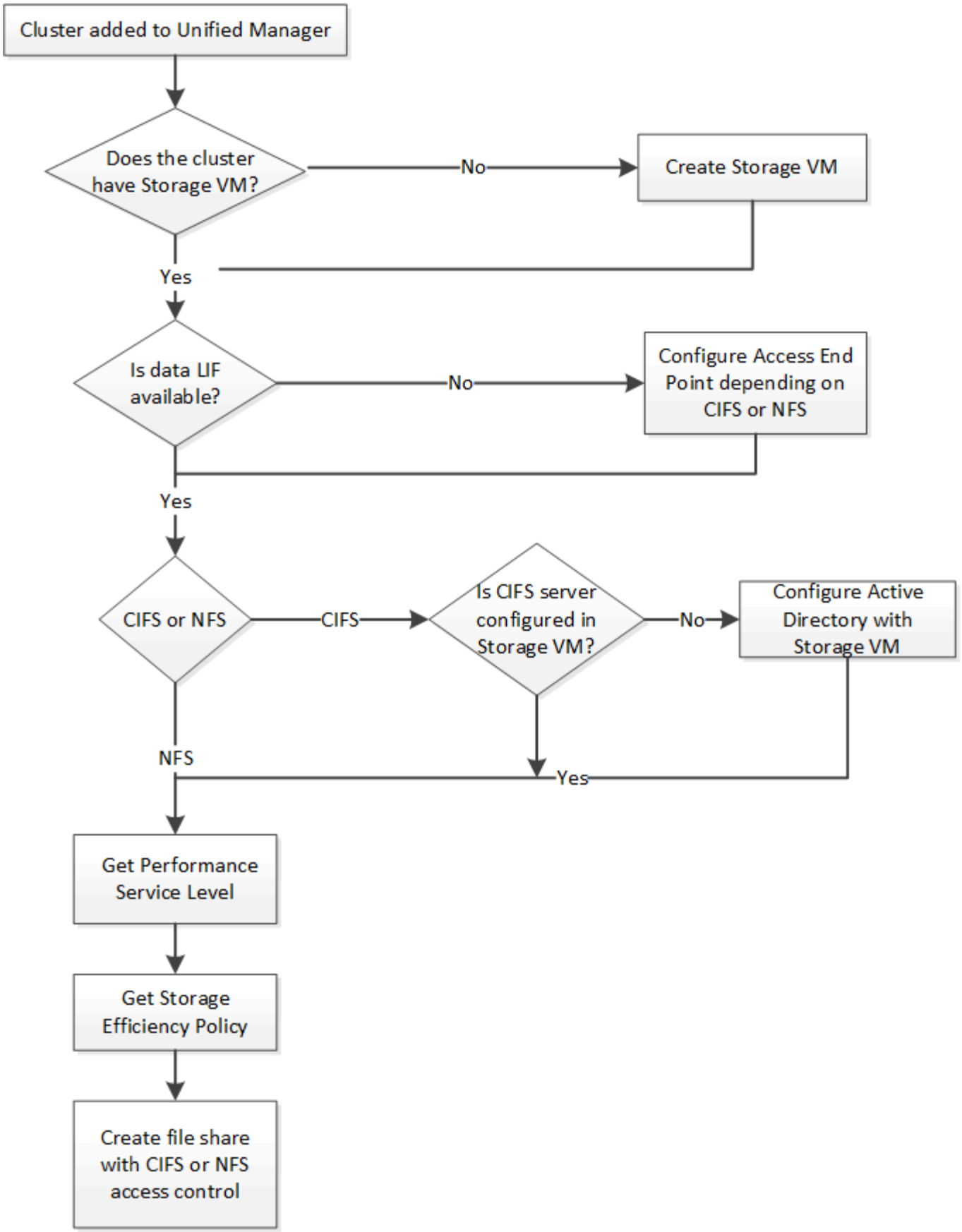
범주	**HTTP** 동사	경로
관리 - 서버	가져오기	'/management-server/jobs/{key}'

API를 사용하여 **CIFS** 및 **NFS** 파일 공유 프로비저닝

Active IQ Unified Manager의 일부로 제공되는 프로비저닝 API를 사용하여 SVM(스토리지 가상 머신)에서 CIFS 공유 및 NFS 파일 공유를 프로비저닝할 수 있습니다. 이 프로비저닝

워크플로에서는 파일 공유를 생성하기 전에 SVM의 키, 성능 서비스 수준 및 스토리지 효율성 정책을 검색하는 단계에 대해 자세히 설명합니다.

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


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

다음을 확인합니다.

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

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

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

◦ 샘플 컬 *

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

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

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

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

◦ 샘플 컬 *

생성하려는 액세스 끝점의 세부 정보를 입력 매개 변수로 입력해야 합니다.

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

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

3. 액세스 엔드포인트 확인:

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

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

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

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

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

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

- 샘플 컬 *

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

```
curl -X POST "https://<hostname>/api/storage-provider/active-
directories-mappings" -H "accept: application/json" -H "Content-Type:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
\"dns\": \"10.000.000.000\",
\"domain\": \"example.com\",
\"password\": \"string\",
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

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

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

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

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

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

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

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

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

      - 예제 값이 있는 curl 명령 *

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

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

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

- 예제 값이 있는 curl 명령 *

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

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

스토리지 효율성 정책은 파일 공유를 생성하는 선택적 매개 변수입니다.

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

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

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

응답이 끝나면 생성된 파일 공유의 키가 표시됩니다.

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

1. 반환된 키를 사용하여 다음 API를 실행하여 파일 공유가 생성되었는지 확인합니다.

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

◦ JSON 출력 샘플 *

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

```
{
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
    "name": "FileShare_377",
    "cluster": {
        "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
```

```
        "name": "AFFA300-206-68-70-72-74",
        "_links": {
            "self": {
                "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-
00a098dcc959"
            }
        }
    },
    "svm": {
        "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
        "name": "RRT_ritu_vs1",
        "_links": {
            "self": {
                "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-
8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-
00a098dcc959"
            }
        }
    },
    "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
    },
    "recommended_performance_service_level": {
        "key": null,
        "name": "Idle",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
```

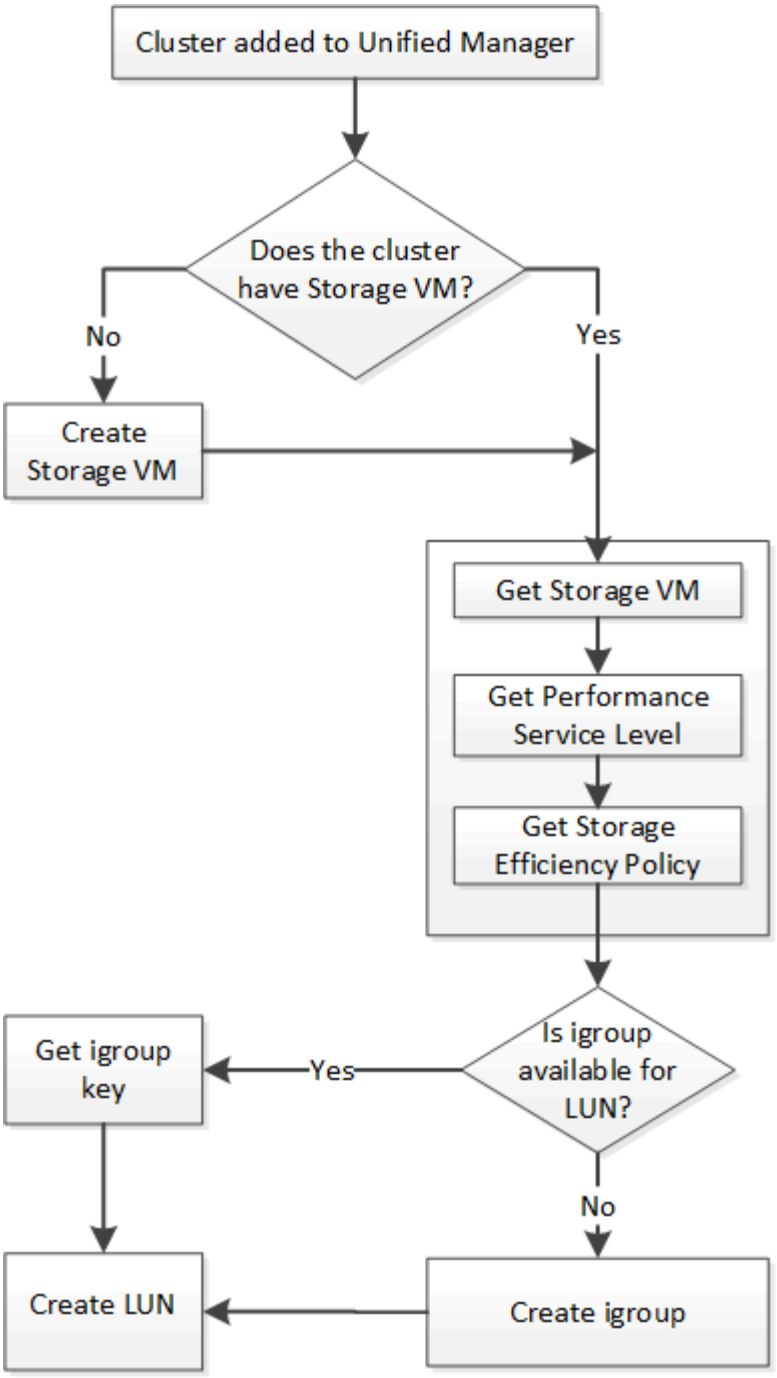
```
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key":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

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

API를 사용하여 **LUN** 프로비저닝

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

다음 다이어그램에서는 LUN 프로비저닝 워크플로우의 단계를 보여 줍니다.



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

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

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

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

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

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

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

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

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

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

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

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

6. LUN을 생성합니다.

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

LUN을 생성하려면 검색된 값을 필수 입력 매개 변수로 추가해야 합니다.

스토리지 효율성 정책은 LUN 생성을 위한 선택적 매개 변수입니다.

◦ 샘플 컬 *

입력 매개 변수로 생성할 LUN의 모든 세부 정보를 입력해야 합니다.

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

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

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

응답이 끝나면 생성된 LUN의 키가 표시됩니다.

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

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

◦ JSON 출력 샘플 *

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

== LUN 생성 또는 매핑에서 장애가 발생한 경우 문제 해결 단계

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

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with
the iSCSI or FCP protocol for Vserver <server_name>. Use the access-
endpoints API to create a LIF for the LUN.
```

이 문제를 해결하려면 다음 문제 해결 단계를 수행하십시오.

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

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

◦ 샘플 컬 *

입력 매개 변수로 만들려는 액세스 끝점의 세부 정보를 입력해야 합니다.

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

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

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

◦ JSON 출력 샘플 *

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

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

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

입력에서 LUN 매핑을 업데이트할 igroup 키를 LUN 키와 함께 지정합니다.

◦ 샘플 컬 *

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

4. LUN 키를 사용하여 쿼리하여 LUN 매핑을 확인합니다.

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

◦ JSON 출력 샘플 *

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

API를 사용하여 스토리지 워크로드 수정

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

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

워크플로우에서는 LUN 또는 파일 공유가 성능 서비스 수준으로 프로비저닝되었다고 가정합니다.

파일 공유를 수정하는 중입니다

파일 공유를 수정하는 동안 다음 매개 변수를 업데이트할 수 있습니다.

- 용량 또는 크기입니다.

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

ⓘ 단일 API를 실행하는 동안 매개 변수를 하나만 업데이트할 수 있습니다.

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

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

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

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

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

출력에서 파일 공유의 세부 정보를 봅니다.

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

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

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

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

4. 파일 공유에 성능 서비스 수준을 적용합니다.

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

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

◦ 샘플 컬 *

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

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

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

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

작업 객체의 ID로 쿼리하면 파일 공유가 성공적으로 업데이트되었는지 여부를 확인할 수 있습니다. 장애가 발생한 경우, 장애 해결 후 API를 다시 실행한다. 성공적으로 생성되면 파일 공유를 쿼리하여 수정된 객체를 확인합니다.

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

출력에서 파일 공유의 세부 정보를 봅니다.

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

LUN을 업데이트하는 중입니다

LUN을 업데이트하는 동안 다음 매개 변수를 수정할 수 있습니다.

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

단일 API를 실행하는 동안 매개 변수를 하나만 업데이트할 수 있습니다.

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

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

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

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

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

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

◦ JSON 출력 샘플 *

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

3. LUN에 할당할 성능 서비스 수준의 키를 얻습니다.

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

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

4. LUN에 성능 서비스 수준을 적용합니다.

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

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

◦ 샘플 컬 *

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

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

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

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

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

◦ JSON 출력 샘플 *

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

API를 사용하여 **CIFS**를 지원하여 **NFS** 파일 공유를 수정합니다

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

- 필요한 것 *

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

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

단계

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

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

◦ 샘플 컬 *

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

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

◦ JSON 출력 샘플 *

이 작업은 업데이트를 실행하는 작업의 작업 ID를 반환합니다.

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

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

◦ JSON 출력 샘플 *

```
"access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
```

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

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

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

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

"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/"

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/"

오픈 소스

이 제품에 사용된 타사 저작권 및 라이센스에 대한 정보입니다.

"Active IQ Unified Manager 9.14에 대한 고지 사항"

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄됨 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이센스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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