



OnCommand Insight 문서

OnCommand Insight

NetApp
April 01, 2024

목차

OnCommand Insight 문서	1
릴리즈 노트	2
릴리즈 노트	2
OnCommand Insight란 무엇입니까?	3
OnCommand Insight 개요	3
Insight 아키텍처	3
관리자, 관리자 및 계획자가 Insight를 사용하는 방법	5
Linux용 설치	6
설치 필수 구성 요소	6
Insight 설치 지침	13
Insight 업그레이드	24
OnCommand Insight를 제거하는 중입니다	31
Microsoft Windows용 설치	33
설치 필수 구성 요소	33
Insight 설치 지침	41
OnCommand Insight 업그레이드 중	54
소프트웨어 제거	78
구성 및 관리	80
Insight 설정	80
Insight Security 를 참조하십시오	169
스마트 카드 및 인증서 로그인 지원	182
스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성	194
스마트 카드 및 인증서 로그인을 위한 Cognos 구성(OnCommand Insight 7.3.5 ~ 7.3.9)	195
스마트 카드 및 인증서 로그인에 대한 Cognos 구성(OnCommand Insight 7.3.10 이상)	196
Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)	198
Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.10 이상)	200
SSL 인증서를 가져오는 중입니다	202
업무 엔티티 계층 구조	205
주석 정의	208
자산 쿼리 중	222
Insight 데이터 소스 관리	229
장치 해상도	330
Insight 유지 관리	348
환경을 모니터링합니다	370
데이터 웨어하우스 관리	398
OnCommand Insight 데이터 웨어하우스에 오신 것을 환영합니다	398
데이터 웨어하우스 시작	404
데이터 웨어하우스를 사용하여 수행할 수 있는 관리 작업입니다	425
보고	451

OnCommand Insight 보고를 시작합니다	451
간편한 보고	455
보고서 관리	463
사용자 정의 임시 보고서 작성	466
보고 데이터 모델	468
FAQ 를 참조하십시오	475
일반적인 질문	475
OnCommand Insight 라이선스	476
구성 및 지원 장치	478
확장성 및 사용 편의성	479
성능 문제 해결	480
환경 관리	481
Insight를 다른 톨과 통합	481
Data ONTAP 스토리지 IOPS	483
사용 방법 가이드	484
Insight 시작하기	484
사용자 지정 대시보드 만들기	497
성능 정책 생성 중	531
Fibre Channel BB 크레딧 0 오류 문제 해결	535
인프라 분석 중	540
썬 프로비저닝의 위험 최소화 소개	545
호스트 및 VM 파일 시스템 사용률 데이터 수집	551
차지백 데이터를 보고하도록 시스템을 구성합니다	555
입출력 밀도 보고서가 내부 데이터 볼륨만 설명하도록 합니다	561
통합 데이터 수집 중	563
애플리케이션 성능 문제 분석	572
AWS 청구 데이터 수집 및 보고	579
ServiceNow와 통합	583
법적 고지	590
저작권	590
상표	590
특허	590
개인 정보 보호 정책	590
주의	590

OnCommand Insight 문서

OnCommand Insight는 물리적 환경과 가상 환경의 네트워크, 스토리지 및 서버에서 도메인 간, 멀티벤더 리소스 관리 및 분석을 지원하는 단일 솔루션입니다. Insight를 사용하면 현재 인프라를 최적화할 수 있으므로 비즈니스 요구에 맞게 올바른 규모의 운영을 수행할 수 있습니다. 구입 항목 및 구입 시기를 결정하는 프로세스를 간소화합니다. 또한 클라우드 마이그레이션에 적합한 워크로드를 식별하여 하이브리드 클라우드로 전환하는 등의 복잡한 기술 마이그레이션 과정에서도 위험을 줄여줍니다. Insight를 사용하면 리소스를 회사의 전체 IT 서비스 제공망으로 통합하여 IT 인프라를 엔드 투 엔드 서비스로 관리할 수 있습니다.

릴리즈 노트

릴리즈 노트

OnCommand Insight 릴리스 정보는 문서 센터 외부에서 제공됩니다. NetApp Support 사이트 자격 증명을 사용하여 로그인하라는 메시지가 표시됩니다.

["릴리즈 노트.pdf"](#) (새 창에서 열림)

OnCommand Insight란 무엇입니까?

OnCommand Insight 개요

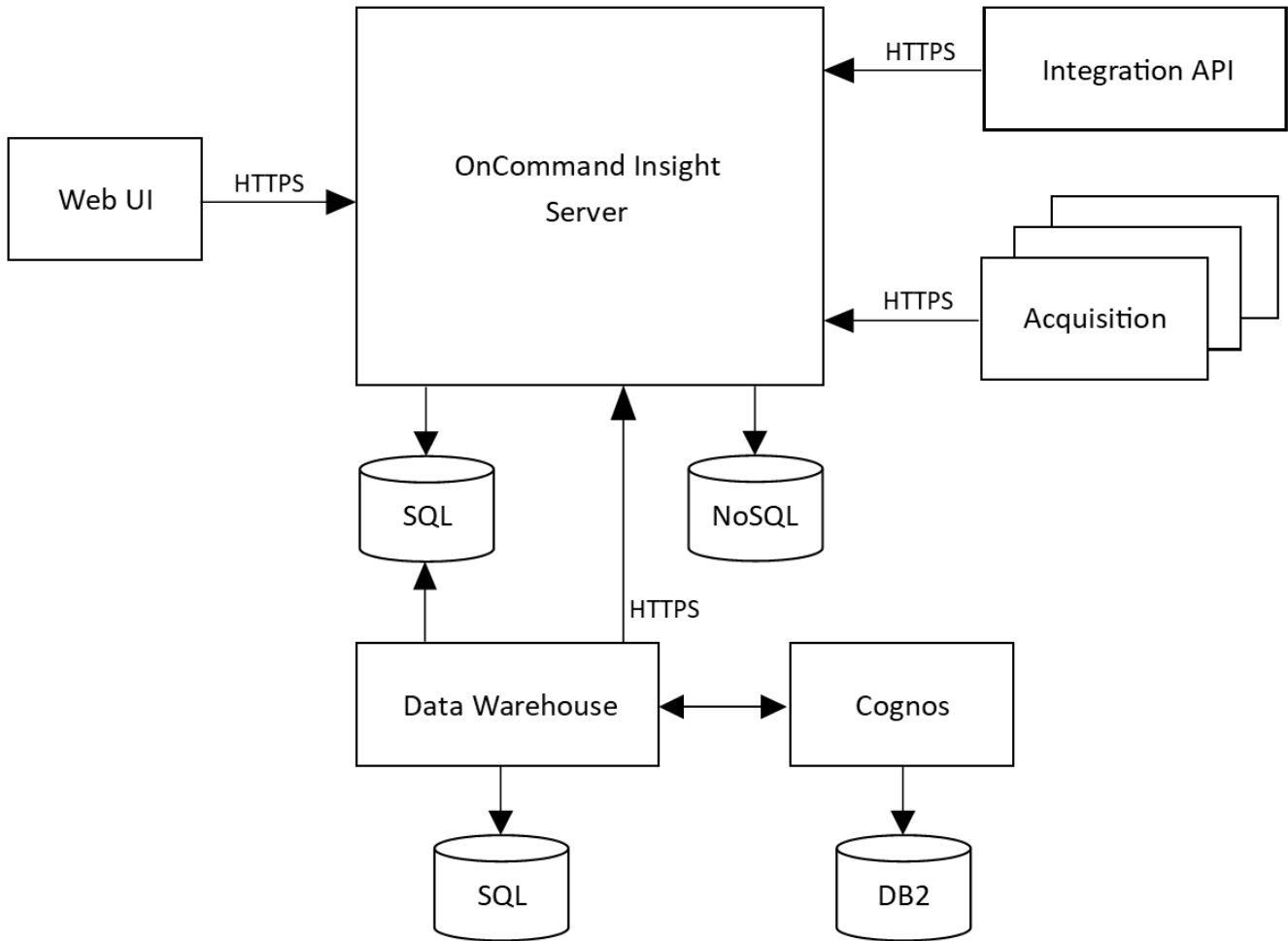
OnCommand Insight를 사용하면 복잡한 프라이빗 및 하이브리드 클라우드, 가상 IT 환경의 운영 관리를 간소화할 수 있습니다. Insight는 물리적 환경과 가상 환경의 네트워크, 스토리지 및 서버 전반에서 도메인 간, 멀티벤더 리소스 관리 및 분석을 지원하는 단일 솔루션입니다.

Insight를 사용하면 현재 인프라를 최적화할 수 있으므로 비즈니스 요구에 맞게 올바른 규모의 운영을 수행할 수 있습니다. 구입 항목 및 구입 시기를 결정하는 프로세스를 간소화합니다. 또한 클라우드 마이그레이션에 적합한 워크로드를 식별하여 하이브리드 클라우드로 전환하는 등의 복잡한 기술 마이그레이션 과정에서도 위험을 줄여줍니다. Insight를 사용하면 리소스를 회사의 전체 IT 서비스 제공망으로 통합하여 IT 인프라를 엔드 투 엔드 서비스로 관리할 수 있습니다.

Insight 아키텍처

OnCommand Insight의 일반적인 설치에는 웹 기반 UI에서 쉽게 액세스할 수 있는 보고서를 포함한 데이터 수집 및 데이터 웨어하우징이 포함됩니다. 보다 안전한 환경을 위해 원격 획득 장치를 통해 획득을 수행할 수 있습니다.

Insight 아키텍처의 주요 구성 요소는 다음 다이어그램에 나와 있습니다.



• * OnCommand Insight 서버 *

OnCommand Insight 서버에는 기본 데이터 저장소 및 분석 구성 요소가 포함되어 있습니다. 서버는 환경의 전체 토폴로지를 지속적으로 구축하고, 환경을 분석하고, 인시던트나 위반이 감지되면 알림을 생성합니다.

• * 취득 *

Insight 수집 엔진은 하나 이상의 수집 장치에 구축됩니다. 각 Insight 서버는 로컬 획득 장치를 포함하며 원격 획득 장치를 지원할 수 있습니다. 각 장치는 네트워크에서 실행 중인 서비스로서, 데이터 센터의 장치에서 데이터에 액세스하고 이를 통해 데이터를 수집합니다(_data sources_라고 함). 획득 장치에서 수집한 정보는 분석을 위해 서버로 전송됩니다.

수집 엔진은 모듈식으로 쉽게 패치할 수 있도록 설계되었습니다.

• * 통합 API *

API를 사용하면 외부 에이전트에서 데이터를 수집할 수 있습니다. 통합 데이터는 쿼리와 위젯을 사용하여 웹 UI에서 볼 수 있습니다. 대시보드에는 '기본' Insight 데이터와 통합 데이터가 포함될 수 있습니다. 이러한 대시보드의 데이터에 필터링, 롤업 및 그룹화를 적용할 수 있습니다.

• 웹 UI *

Insight용 HTML5 웹 기반 사용자 인터페이스를 통해 정책, 임계값 및 알림을 비롯한 데이터 소스와 모니터링

환경을 설정할 수 있습니다. 그런 다음 웹 UIAsset 대시보드 및 자산 페이지를 사용하여 잠재적인 문제를 파악하고 조사합니다. 다양한 위젯으로 사용자 지정 대시보드를 만들 수 있습니다. 각 위젯은 데이터를 표시, 분석 및 차트로 매우 유연하게 표시합니다.

- * 데이터 웨어하우스 *

OnCommand Insight 데이터 웨어하우스는 여러 Insight 서버의 데이터를 저장하고 쿼리 및 분석을 위한 공통의 다차원 데이터 모델로 데이터를 변환하는 중앙 집중식 저장소입니다.

OnCommand Insight 데이터 웨어하우스를 사용하면 지불 거절 보고서, 내역 데이터가 포함된 추세 보고서, 소비 분석 및 예측 보고서와 같은 사용자 정의 용량 및 성능 보고서를 생성할 수 있는 여러 데이터 마트로 구성된 공개 데이터베이스에 액세스할 수 있습니다.

데이터 웨어하우스는 하나 또는 여러 개의 Insight 설치를 위한 보고 데이터를 통합하고 준비합니다. 이 데이터에는 데이터 센터 인프라에 대한 장기 계획을 지원하기 위한 기록, 추세 분석, 인벤토리, 차지백, 표시 및 데이터 프레젠테이션이 포함됩니다.

- * Cognos *

Cognos는 미리 정의된 보고서를 보거나 사용자 지정 보고서를 만들 수 있는 IBM 비즈니스 인텔리전스 도구인 Insight의 보고 엔진입니다. Insight Reporting은 데이터 웨어하우스 데이터에서 보고서를 생성합니다.

관리자, 관리자 및 계획자가 Insight를 사용하는 방법

OnCommand Insight은 스토리지 관리자, 관리자 및 스토리지 설계자가 문제 해결과 분석을 수행하는 데 중요한 정보를 제공합니다.

숙련된 스토리지 관리자는 OnCommand Insight를 네트워크 스토리지 지식과 함께 사용하여 다음과 같은 일반적인 작업을 수행합니다.

- SAN 및 NAS 환경 관리
- SAN 엔지니어와 협력하여 네트워크 문제 해결
- 새로운 스토리지 기술을 평가, 테스트 및 환경에 통합합니다.
- 성능 문제, 경고, 정책 위반, 위반 및 취약점 해결

관리자와 네트워크 계획자는 OnCommand Insight를 사용하여 다음과 같은 비즈니스 작업을 수행합니다.

- 용량 계획
- 프로젝트 예산 및 일정 개발
- 프로젝트 계획을 평가하고 수정하여 변화하는 프로젝트 요구 사항을 충족시킵니다.
- 프로젝트 계획 및 비용 관리
- 하드웨어 및 소프트웨어 구매
- 용량 관리, 비용 청구, 적합한 사이징 및 서비스 수준 계약에 대한 비즈니스 보고서를 제공합니다.

Linux용 설치

설치 필수 구성 요소

OnCommand Insight를 설치하기 전에 현재 소프트웨어 버전을 다운로드하고 적절한 라이선스를 취득하며 환경을 설정해야 합니다.

OnCommand Insight를 설치하기 전에 다음 사항을 확인하십시오.

- 현재 버전의 다운로드한 설치 패키지에 있는 OnCommand Insight 소프트웨어 파일입니다
- 다운로드한 OnCommand Insight 버전을 작동하는 라이선스입니다
- 최소 하드웨어 및 소프트웨어 환경

현재 제품은 이전 버전의 OnCommand Insight 제품에서 사용되지 않은 추가 하드웨어 리소스(향상된 OnCommand Insight 제품 기능)를 사용할 수 있습니다.

- OnCommand Insight 서버, 데이터 웨어하우스 및 보고, 원격 획득 장치의 하드웨어 및 네트워크 구성을 포함하는 배포 계획.

배포 계획

성공적인 배포를 위해서는 OnCommand Insight를 설치하기 전에 특정 시스템 요소를 고려해야 합니다.

이 작업에 대해

Insight 배포를 계획할 때 다음과 같은 시스템 요소를 고려해야 합니다.

- Insight 아키텍처
- 모니터링할 네트워크 구성 요소
- Insight 설치 사전 요구 사항 및 서버 요구 사항
- Insight 웹 브라우저 요구사항

데이터 소스 지원 정보

구성 계획의 일환으로 Insight에서 사용자 환경의 장치를 모니터링할 수 있는지 확인해야 합니다. 이렇게 하려면 데이터 소스 지원 매트릭스에서 운영 체제, 특정 장치 및 프로토콜에 대한 자세한 내용을 확인할 수 있습니다. 일부 데이터 소스는 일부 운영 체제에서 사용하지 못할 수 있습니다.

데이터 소스 지원 매트릭스의 최신 버전 위치

OnCommand Insight 데이터 소스 지원 매트릭스는 각 서비스 팩 릴리스에 따라 업데이트됩니다. 문서의 최신 버전은 에서 찾을 수 있습니다 "[NetApp Support 사이트](#)". .

배포 계획의 일환으로 환경에 있는 장치에 대한 정보를 수집해야 합니다.

사용자 환경의 각 장치에 대한 다음 소프트웨어, 연결 및 정보가 필요합니다.

- OCI 서버에서 확인할 수 있는 IP 주소 또는 호스트 이름입니다
- 로그인 이름 및 암호
- 장치 액세스 유형(예: 컨트롤러 및 관리 스테이션)



대부분의 장치에 읽기 전용 액세스만으로도 충분하지만 일부 장치에는 관리자 권한이 필요합니다.

- 데이터 소스 포트 요구 사항에 따라 장치에 대한 포트 연결
- 스위치의 경우 SNMP 읽기 전용 커뮤니티 문자열(스위치에 대한 액세스를 제공하는 사용자 ID 또는 암호)
- 디바이스에 필요한 타사 소프트웨어(예: Solutions Enabler)
- 데이터 소스 사용 권한 및 요구 사항에 대한 자세한 내용은 웹 UI 도움말 또는 _OnCommand Insight 구성 및 관리 가이드_의 "공급업체별 데이터 소스 참조"를 참조하십시오.

OnCommand Insight에서 생성된 네트워크 트래픽입니다

OnCommand Insight가 생성하는 네트워크 트래픽, 네트워크를 통과하는 처리된 데이터의 양 및 OnCommand Insight가 디바이스에 배치하는 로드는 여러 요인에 따라 달라집니다.

트래픽, 데이터 및 로드는 다음 요소에 따라 환경에 따라 다릅니다.

- 원시 데이터
- 장치 구성
- OnCommand Insight의 구축 토폴로지
- 느린 디바이스를 발견하거나 대역폭을 처리할 수 있도록 여러 인벤토리 및 성능 데이터 소스 폴링 간격을 줄일 수 있습니다

OnCommand Insight에서 수집하는 원시 구성 데이터는 크게 다를 수 있습니다.

다음 예에서는 구성 데이터가 어떻게 변하는지, 그리고 여러 구성 요소의 트래픽, 데이터 및 로드가 어떤 영향을 받는지 보여 줍니다. 예를 들어 각각 1,000개의 디스크가 있는 두 개의 어레이가 있을 수 있습니다.

- 어레이 1: 크기가 모두 1TB인 SATA 디스크 1,000개가 있습니다. 1,000개의 디스크가 모두 하나의 스토리지 풀에 있고 1,000개의 LUN이 있으며, 모두 ESX 클러스터의 동일한 32개 노드에 표시(매핑 및 마스킹됨)됩니다.
- 어레이 2: 2TB 데이터 디스크 400개, 600GB FC 디스크 560개 및 SSD 40개가 있습니다. 스토리지 풀은 3개가 있지만 FC 디스크 320개가 기존 RAID 그룹에 사용됩니다. RAID 그룹에 포함된 LUN은 기존 마스킹 유형(symmaskdb)을 사용하는 반면, 씬 프로비저닝된 풀 기반 LUN은 최신 마스킹 유형(symaccess)을 사용합니다. 150개의 호스트에 600개의 LUN이 제공됩니다. 200개의 BCV(600개의 LUN 중 200개의 전체 블록 복제본 볼륨)가 있습니다. 다른 사이트의 스토리지에 있는 볼륨의 원격 복제본 볼륨인 R2 볼륨도 200개가 있습니다.

이러한 어레이에는 각각 1,000개의 디스크와 1,000개의 논리적 볼륨이 있습니다. 이러한 공간은 데이터 센터에서 소비하는 랙 공간의 크기와 물리적으로 동일하며 동일한 펌웨어를 실행하기도 하지만 두 번째 어레이는 첫 번째 어레이보다 구성에서 훨씬 복잡합니다.

MariaDB를 제거하는 중입니다

OnCommand Insight 또는 데이터 웨어하우스를 설치하기 전에 Insight 또는 데이터 웨어하우스 서버에서 MariaDB를 제거해야 합니다. 그렇지 않으면 설치를 계속할 수 없습니다. MySQL은 MariaDB와 호환되지 않습니다. MariaDB를 제거하지 않고 두 서버 중 하나에서 설치를 시도하면 설치가 종료되고 MariaDB를 제거하라는 오류 메시지가 표시됩니다.

시작하기 전에

sudo 권한이 있어야 합니다.

단계

1. Insight 서버에 로그인합니다.
2. MariaDB 구성 요소 목록 가져오기:

```
rpm -qa | grep mariadb
```

3. 서버에 설치된 각 MariaDB 구성 요소에 대해 다음을 입력합니다.

```
yum remove component_name
```

Insight Server 요구사항

전용 서버가 권장됩니다. 다른 애플리케이션이 설치된 서버에 Insight를 설치하지 마십시오. 제품 요구 사항이 충족되는 경우 물리적 서버와 가상 서버가 모두 지원됩니다.

OnCommand Insight 서버 소프트웨어를 설치하려면 sudo 권한이 있어야 합니다.

일부 Insight 구성 요소는 설치 중에 종속 패키지가 필요할 수 있습니다. Insight를 설치하기 전에 YUM 저장소에 액세스할 수 있는지 확인합니다.



OnCommand Insight 크기 조정에는 데이터 소스 유형 및 크기, 환경의 자산 수, 폴링 간격 등 다양한 종속 항목이 있습니다. 다음 사이징 예는 지침일 뿐이며 Insight가 테스트된 환경의 일부를 나타냅니다. 환경의 이러한 요인 또는 기타 요소를 변경하면 Insight의 사이징 요구 사항이 변경될 수 있습니다. 이러한 지침에는 최대 90일간의 성능 아카이브 데이터를 위한 디스크 공간이 포함되어 있습니다.


Insight를 설치 또는 업그레이드하기 전에 세일즈 엔지니어에게 자세한 사이징 지침을 문의하는 것이 좋습니다.

• 예: *

환경 요인:	테스트한 디스크 공간, CPU 및 메모리:
80개 스토리지 4,000개 볼륨	250GB 디스크 공간 8코어
4,000개의 VM	32GB RAM
4,000개의 스위치 포트	

160 스토리지 어레이 40,000개의 볼륨 8,000개의 VM 8,000개의 스위치 포트	1TB 디스크 공간 12개 코어 48GB RAM
---	-----------------------------------

• 요구 사항: *

구성 요소	필수 요소입니다
운영 체제	<p>다음 중 하나의 라이선스 버전을 실행하는 컴퓨터, 다른 응용 프로그램 수준 소프트웨어를 실행하지 않는 컴퓨터:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.8, 9.2 • CentOS 7.2, 7.5, 7.6, 7.7, 7.8, 7.9, CentOS 8 스트림, CentOS 9 스트림 • Oracle Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.8 <p>라이선스가 있는 버전은 설치에 필요한 종속 항목이 운영 체제에 의해 자동으로 해결되도록 합니다.</p> <p>Insight를 설치하기 전에 MariaDB를 제거해야 합니다.</p> <div>  <div> <p>MariaDB를 제거하면 Postfix Mail Transport Agent도 제거됩니다.</p> </div> </div> <p>전용 서버가 권장됩니다.</p>
가상 머신(VM)	이 구성 요소는 인스턴스에 대한 CPU 및 메모리 리소스가 예약되어 있는 경우 가상 환경에서 실행될 수 있습니다.
메모리 및 CPU	<p>24-256GB RAM</p> <p>8~32코어</p>

사용 가능한 디스크 공간입니다	<p>100GB - 3TB 설치 디스크 공간</p> <p>50GB - 1TB 성능 아카이브 디스크 공간</p> <p>예를 들어 500GB 환경에서는 다음과 같은 파티션 분할이 권장됩니다.</p> <ul style="list-style-type: none"> • /opt 디렉토리 — 50GB • /var/log 디렉토리 — 100GB • /var/lib 디렉토리 — 350GB <p>장착하는 것이 가장 좋습니다 /opt 및 /var 루트 파일 시스템과 별도의 디스크에 있습니다 (/)를 클릭합니다.</p> <p>Insight 설치 공간에는 SSD 디스크를 사용하는 것이 좋습니다.</p>
네트워크	<p>이더넷 연결 및 포트:</p> <ul style="list-style-type: none"> • FC 장치 및 원격 획득 장치를 포함하여 SAN의 모든 구성 요소에 대한 전용(정적) IP 주소 및 IP 연결을 통한 100Mbps 또는 1Gbps 이더넷 연결 • OnCommand Insight 서버 프로세스의 포트 요구 사항은 80, 443, 1090 ~ 1100, 3873, 8083입니다. 4444 ~ 4446, 5445, 5455, 4712 ~ 4714, 5500, 및 5501을 참조하십시오. • 획득 프로세스의 포트 요구 사항은 12123 및 5679입니다. • MySQL의 포트 요구 사항은 3306입니다. • Elasticsearch의 포트 요구 사항은 9200 및 9310입니다 <p>포트 443 및 3306은 존재하는 방화벽을 통해 외부 액세스를 필요로 합니다.</p>
권한	<p>OnCommand Insight 서버에 sudo 권한이 필요합니다.</p> <p>다음 폴더 중 하나가 심볼 링크인 경우 대상 디렉토리에 '755' 권한이 있는지 확인하십시오.</p> <ul style="list-style-type: none"> • /opt/NetApp을 참조하십시오 • /var/lib/netapp • /var/log/netapp
원격 연결	<p>WebEx 액세스를 위한 인터넷 연결 또는 설치 및 설치 후 지원을 위한 원격 데스크톱 연결</p>

접근성	HTTPS 액세스가 필요합니다.
HTTP 또는 HTTPS 서버	Apache HTTP 서버 또는 다른 HTTPS 서버는 OnCommand Insight 서버와 동일한 포트(443)에 대해 경쟁해서는 안 되며 자동으로 시작해서는 안 됩니다. 포트 443을 수신해야 하는 경우 다른 포트를 사용하도록 OnCommand Insight 서버를 구성해야 합니다.

데이터 웨어하우스 서버 요구 사항

데이터 웨어하우스 서버는 정해진 하드웨어 및 소프트웨어 요구 사항과 호환되는 컴퓨터에서 실행해야 합니다. Apache 웹 서버 또는 보고 소프트웨어가 이 시스템에 설치되어 있지 않은지 확인해야 합니다.



OnCommand Insight를 위한 사이징에는 운영 환경의 자산 수, 유지되는 기간별 데이터 양 등과 같은 다양한 종속 관계가 있습니다. 다음 데이터 웨어하우스 사이징 예는 지침일 뿐이며 Insight가 테스트된 일부 환경을 나타냅니다. 환경의 이러한 요인 또는 기타 요소를 변경하면 Insight의 사이징 요구 사항이 변경될 수 있습니다.

Insight를 설치 또는 업그레이드하기 전에 세일즈 엔지니어에게 자세한 사이징 지침을 문의하는 것이 좋습니다.

• 예: *

환경 요인:	테스트한 디스크 공간, CPU 및 메모리:
스토리지 18개가상 머신 3,400개	200GB 하드 디스크8 코어
4,500개의 스위치 포트	32GB RAM
110개의 스토리지 어레이11,500개의 VM을 제공합니다	300GB 하드 디스크8 코어
14,500개의 스위치 포트	48GB RAM

• 요구 사항: *

구성 요소	필수 요소입니다
운영 체제	<p>다음 중 하나의 라이선스 버전을 실행하는 컴퓨터, 다른 응용 프로그램 수준 소프트웨어를 실행하지 않는 컴퓨터:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.8, 9.2 • CentOS 7.2, 7.5, 7.6, 7.7, 7.8, 7.9, CentOS 8 스트림, CentOS 9 스트림 • Oracle Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.8

가상 머신(VM)	이 구성 요소는 인스턴스에 대한 CPU 및 메모리 리소스가 예약되어 있는 경우 가상 환경에서 실행될 수 있습니다.
CPU	8-40개의 CPU 코어
메모리	32GB - 2TB RAM
사용 가능한 디스크 공간	200GB - 512GB 디스크 공간에는 50GB 이상의 사용 가능한 디스크 공간이 있어야 합니다 /var/lib 파티션 및 /에서 25GB의 사용 가능한 디스크 공간 /opt 및 /var/log 파티션.
네트워크	<ul style="list-style-type: none"> • 100Mbps 또는 1Gbps 인터넷 연결 • 고정 IP 주소입니다 • OnCommand Insight DWH 서버 프로세스의 경우 포트 80, 443, 1098, 1099, 3873, 8083, 4444 ~ 4446 • MySQL의 경우 포트 3306입니다

원격 획득 장치 서버 요구 사항

방화벽 뒤, 원격 사이트, 사설 네트워크 또는 다른 네트워크 세그먼트에 있는 SAN 장치에서 정보를 가져오려면 RAU(원격 획득 장치)를 설치해야 합니다. RAU를 설치하기 전에 사용 환경이 RAU 운영 체제, CPU, 메모리 및 디스크 공간 요구 사항을 충족하는지 확인해야 합니다.

구성 요소	요구 사항
운영 체제	<p>다음 중 하나의 라이선스 버전을 실행하는 컴퓨터, 다른 응용 프로그램 수준 소프트웨어를 실행하지 않는 컴퓨터:</p> <ul style="list-style-type: none"> • Red Hat Enterprise Linux 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.8, 9.2 • CentOS 7.2, 7.5, 7.6, 7.7, 7.8, 7.9, CentOS 8 스트림, CentOS 9 스트림 • Oracle Enterprise Linux 7.5, 7.6, 7.7, 7.8, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5, 8.8 <p>전용 서버가 권장됩니다.</p>
CPU	CPU 코어 4개
메모리	16GB RAM
사용 가능한 디스크 공간입니다	40GB

네트워크	100Mbps/1Gbps 이더넷 연결, 정적 IP 주소, 모든 FC 디바이스에 대한 IP 연결 및 OnCommand Insight 서버에 대한 필수 포트(80 또는 443).
권한	RAU 서버에 대한 sudo 권한

OnCommand Insight에서 지원되는 브라우저

브라우저 기반 OnCommand Insightfob UI는 여러 브라우저에서 작동할 수 있습니다.

Insight는 다음 브라우저의 새로운 비 베타 릴리스를 지원합니다.

- Mozilla Firefox
- Google Chrome
- Microsoft Edge를 참조하십시오

OnCommand Insight에 적합한 브라우저 버전의 전체 목록은 를 참조하십시오 "[NetApp 상호 운용성 매트릭스 툴](#)".

Insight 설치 지침

설치 시 여러 OnCommand Insight 구성 요소, Insight Server 및 데이터 웨어하우스를 설치해야 합니다.

설치에는 다음과 같은 주요 작업이 포함됩니다.

- OnCommand Insight 설치 프로그램을 다운로드하는 중입니다
- OnCommand Insight 서버 설치 중
- 라이선스 설치 중
- 선택적으로 DWH 및 Reporting 설치(별도의 컴퓨터 또는 가상 시스템에 설치해야 합니다. 보고에는 Microsoft Windows가 필요합니다.)
- 선택적으로 방화벽 뒤에 있는 장치 리소스에서 정보를 가져오는 RAU(원격 획득 장치)를 원격 사이트에 설치하거나 개인 네트워크에 설치합니다

설치 후 환경에 대한 정보를 얻도록 Insight를 구성해야 합니다. 필요한 작업은 _OnCommand Insight 구성 및 관리 가이드_에 설명되어 있습니다.

OnCommand Insight 설치 프로그램을 다운로드하는 중입니다

NetApp Support 사이트에서 OnCommand Insight 설치 프로그램을 다운로드할 수 있습니다.

시작하기 전에

에서 NetApp Support 사이트에 로그인해야 합니다 "mysupport.netapp.com".

또한 설치를 열 수 있는 압축 해제 유틸리티가 있어야 합니다 .ZIP 파일.

단계

1. OnCommand Insight를 설치할 서버에 로그인합니다.
2. NetApp Support 사이트에서 설치 파일을 다운로드합니다.

OnCommand Insight 서버 설치

OnCommand Insight 서버는 명령줄을 사용하여 설치됩니다.

시작하기 전에

설치 필수 구성 요소를 모두 완료해야 합니다.

단계

1. sudo 권한이 있는 계정을 사용하여 Insight 서버에 로그인합니다.
2. 설치 파일이 있는 서버의 디렉터리로 이동하여 다음 명령을 입력합니다.

```
unzip oci-<version>-linux-x86_64.zip
```

설치 파일의 버전 번호를 확인하십시오. 버전 번호가 명령에 표시된 번호와 다를 수 있습니다.

3. 예 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 `oci-install.sh`:

```
sudo ./oci-<version>-linux-x86_64/oci-install.sh --help
```

4. 설치 스크립트를 실행합니다.

```
sudo ./oci-<version>-linux-x86_64/oci-install.sh
```

5. 사용권 계약을 읽고 동의하며 화면의 지시를 따릅니다.
6. Insight 소비 라이선스 모델을 사용하는 경우 사용 정보를 NetApp에 전송할 수 있어야 합니다. 를 입력합니다 y 메시지가 표시됩니다.

결과

모든 메시지에 응답하면 설치가 시작되고 설치된 응용 프로그램에 따라 약 10분 정도 소요됩니다.

OnCommand Insight 데이터 웨어하우스 설치 중

설치는 자체 완비되었으며 DWH(OnCommand Insight Data Warehouse)를 실행하고 운영하는 데 필요한 요소를 포함합니다.

시작하기 전에

설치 필수 구성 요소를 모두 완료해야 합니다.

이 작업에 대해

데이터 웨어하우스에는 Cognos 보고 기능이 있습니다. Linux 서버에 Insight를 설치하는 경우에는 Windows 서버에 데이터 웨어하우스를 설치하는 경우에만 이러한 기능을 사용할 수 있습니다. Windows에 데이터 웨어하우스 설치 및 Cognos 보고 기능에 대한 자세한 내용은 Microsoft Windows_용 _OnCommand Insight 설치 안내서 를 참조하십시오.

단계

1. sudo 권한이 있는 계정을 사용하여 데이터 웨어하우스 서버에 로그인합니다.
2. 설치 파일이 있는 서버의 디렉터리로 이동하여 다음 명령을 입력합니다.

```
unzip oci-dwh-<version>-linux-x86_64.zip
```

설치 파일의 버전 번호를 확인하십시오. 버전 번호가 명령에 표시된 번호와 다를 수 있습니다.

3. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 oci-install.sh 설치를 시작하기 전에:

```
sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help
```

4. 설치 스크립트를 실행합니다.

```
sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh
```

5. 사용권 계약을 읽고 동의하며 화면의 지시를 따릅니다.

결과

모든 메시지에 응답하면 설치가 시작되고 설치된 응용 프로그램에 따라 약 10분 정도 소요됩니다.

원격 획득 장치 설치

OnCommand Insight 환경에 하나 이상의 원격 획득 장치(RU)를 설치할 수 있습니다. 획득 장치는 데이터 센터의 여러 장치에서 데이터에 액세스하고(data_sources _ 라는 모듈 사용) 데이터를 수집하는 네트워크에서 실행됩니다.

시작하기 전에

설치 필수 구성 요소를 모두 완료해야 합니다.

변경 정보를 서버로 전달하려면 RAU 서버와 OnCommand Insight 서버 간에 하나 이상의 포트가 열려 있고 사용 가능해야 합니다. 확실하지 않은 경우 RAU 컴퓨터에서 웹 브라우저를 열고 OnCommand Insight 서버로 전달하여 유효성을 검사합니다.

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

획득 포트는 기본적으로 443으로 설정되지만 서버 설치 중에 변경되었을 수 있습니다. 연결에 성공하면 OnCommand Insight 응답 페이지가 표시되어 RAU와 OnCommand Insight 서버 간에 사용 가능한 포트가 열려 있음을 나타냅니다.

네트워크 주소 변환 또는 포트 주소 변환(NAT/PAT:i.e, IP 주소 변환)을 사용하는 환경의 경우 Insight는 NAT와 장치 사이에 RAU만 삽입할 수 있습니다.

- 지원: OnCommand Insight->NAT->RAU->장치
- 지원되지 않음: OnCommand Insight->RAU->NAT->장치

단계

1. sudo 권한이 있는 계정을 사용하여 RAU 서버에 로그인합니다.
2. 설치 파일이 있는 서버의 디렉터리로 이동하여 다음 명령을 입력합니다.

```
unzip oci-rau-<version>-linux-x86_64.zip
```

3. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 oci-install.sh:

```
sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
```

4. 설치 스크립트를 실행합니다.

```
sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
```

5. 사용권 계약을 읽고 동의한 다음 화면의 지시를 따릅니다.

모든 메시지에 응답하면 설치가 시작되고 설치된 응용 프로그램에 따라 약 10분 정도 소요됩니다.

원격 획득 장치 설치를 검증합니다

원격 획득 장치가 올바르게 설치되었는지 확인하려면 서버에 연결된 원격 획득 장치의 상태를 볼 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 획득 단위 * 를 클릭합니다.
3. 새 원격 획득 장치가 올바르게 등록되었고 연결 상태인지 확인합니다.

연결 상태가 아닌 경우 서비스를 다시 시작해 보십시오. 원격 수집 장치 시스템에 로그인하고 다음 명령을 실행합니다.

```
oci-service.sh restart acquisition
```

그래도 연결되지 않으면 기술 지원 부서에 문의하십시오.

설치 확인

설치를 완료한 후 설치 디렉토리는 에 있습니다 /opt/netapp/oci. 지원되는 브라우저에서 Insight를 열어 설치를 확인할 수 있습니다. Insight 로그 파일을 확인할 수도 있습니다.

Insight를 처음 열면 라이선스 설정 페이지가 열립니다. 라이선스 정보를 입력한 후에는 데이터 소스를 설정해야 합니다. 데이터 소스 정의 입력 및 Insight 사용자 및 알림 설정에 대한 자세한 내용은 [_OnCommand Insight 구성 및 관리 가이드_](#)를 참조하십시오.

설치 문제가 발생한 경우 기술 지원 부서에 문의하여 요청한 정보를 제공하십시오.

새 **Insight** 구성 요소가 설치되었는지 확인합니다

설치 후 서버에 새 구성 요소가 있는지 확인해야 합니다.

단계

1. 로그인한 서버에서 현재 작동 중인 서비스 목록을 표시하려면 다음을 입력합니다.

```
sudo oci-service.sh status all
```

2. 로그인한 서버에 따라 목록에서 다음 Insight 서비스를 확인하고 해당 서비스가 ""실행 중"" 상태인지 확인합니다.

- Insight 서버: Wildfly, acquisition, mysql, elasticsearch
- 데이터 웨어하우스 서버: Wildfly, MySQL
- 원격 획득 서버: 획득

결과

이러한 구성 요소가 목록에 없으면 기술 지원 부서에 문의하십시오.

Insight 로그

Insight는 조사 및 문제 해결에 도움이 되는 많은 로그 파일을 제공합니다. 사용 가능한 로그가 로그 디렉토리에 나열됩니다. BareTail과 같은 로그 모니터링 도구를 사용하여 모든 로그를 한 번에 표시할 수 있습니다.

로그 파일은 에 있습니다 `/var/log/netapp/oci/wildfly/` 디렉토리. 획득 로그는 에 있습니다 `/var/log/netapp/oci/acq` 디렉토리. 데이터 파일은 에 있습니다 `/var/lib/netapp/oci`.

웹 UI 액세스

OnCommand Insight를 설치한 후에는 라이선스를 설치한 다음 환경을 모니터링할 Insight를 설정해야 합니다. 웹 브라우저를 사용하여 Insight 웹 UI에 액세스하면 됩니다.

단계

1. 다음 중 하나를 수행합니다.

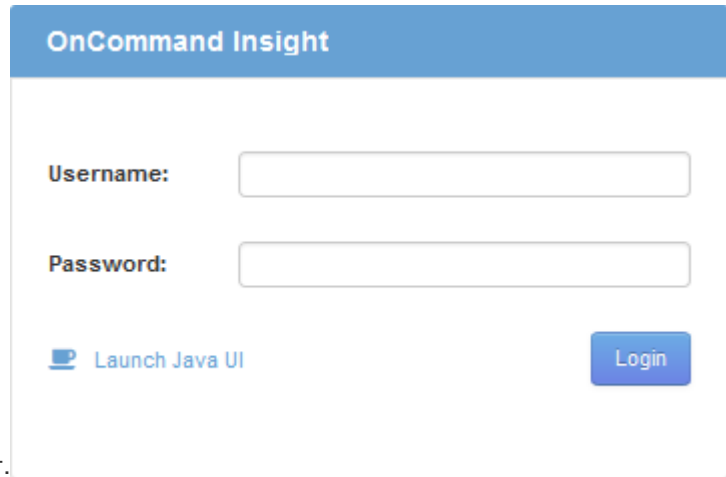
- Insight 서버에 대한 Insight를 엽니다.

```
https://fqdn
```

- 다른 위치에서 Insight 열기:

https://fqdn:port

포트 번호는 Insight 서버를 설치할 때 구성된 443 또는 다른 포트입니다. URL에서 포트 번호를 지정하지 않으면 포트 번호는 443으로 기본 설정됩니다.

The image shows the OnCommand Insight login page. It has a blue header with the text "OnCommand Insight". Below the header, there are two input fields: "Username:" and "Password:". To the right of the "Password:" field is a blue button labeled "Login". Below the input fields, there is a link that says "Launch Java UI" with a small icon of a Java logo.

OnCommand Insight 대화 상자가 표시됩니다.

2. 사용자 이름과 암호를 입력하고 * 로그인 * 을 클릭합니다.

라이센스가 설치된 경우 데이터 소스 설정 페이지가 표시됩니다.



30분 동안 비활성 상태인 Insight 브라우저 세션이 시간 초과되고 시스템에서 자동으로 로그아웃됩니다. 보안 강화를 위해 Insight에서 로그아웃한 후 브라우저를 닫는 것이 좋습니다.

Insight 라이선스 설치

NetApp의 Insight 라이선스 키가 포함된 라이선스 파일을 받으면 설정 기능을 사용하여 모든 라이선스를 동시에 설치할 수 있습니다.

이 작업에 대해

Insight 라이선스 키는 에 저장됩니다 .txt 또는 .lic 파일.

단계

1. 텍스트 편집기에서 라이선스 파일을 열고 텍스트를 복사합니다.
2. 브라우저에서 Insight를 엽니다.
3. Insight 도구 모음에서 * Admin * 을 클릭합니다.
4. 설정 * 을 클릭합니다.
5. Licenses * 탭을 클릭합니다.
6. Update License * 를 클릭합니다.
7. 라이선스 키 텍스트를 * 라이선스 * 텍스트 상자에 복사합니다.
8. 업데이트(가장 일반적인) * 작업을 선택합니다.
9. 저장 * 을 클릭합니다.

10. Insight 소비 라이선스 모델을 사용하는 경우 * Send usage information * 섹션에서 * Enable susage information to NetApp * 확인란을 선택해야 합니다. 프록시는 환경에 맞게 적절히 구성 및 설정되어 있어야 합니다.

작업을 마친 후

라이선스를 설치한 후 다음 구성 작업을 수행할 수 있습니다.

- 데이터 소스를 구성합니다.
- OnCommand Insight 사용자 계정을 생성합니다.

OnCommand Insight 라이선스

OnCommand Insight는 Insight 서버에서 특정 기능을 활성화하는 라이선스로 작동합니다.

- * 발견 *

Discover는 재고를 지원하는 기본 Insight 라이선스입니다. OnCommand Insight를 사용하려면 Discover 라이선스가 있어야 하며 Discover 라이선스가 최소한 하나의 보증, 수행 또는 계획 라이선스와 페어링되어야 합니다.

- * 보증 *

보증 라이선스는 글로벌 및 SAN 경로 정책, 위반 관리를 비롯한 보증 기능을 지원합니다. 라이선스 보증으로 취약점을 보고 관리할 수도 있습니다.

- * 성능 *

Perform 라이선스는 자산 페이지, 대시보드 위젯, 쿼리 등의 성능 모니터링을 지원할 뿐 아니라 성능 정책 및 위반 사항을 관리합니다.

- * 계획 *

플랜 라이선스는 리소스 사용 및 할당을 비롯한 계획 기능을 지원합니다.

- * 호스트 활용률 팩 *

Host Utilization 라이선스는 호스트 및 가상 머신의 파일 시스템 활용도를 지원합니다.

- * 보고서 작성 *

보고서 작성 라이선스는 보고를 위한 추가 작성자를 지원합니다. 이 라이선스에는 플랜 라이선스가 필요합니다.

OnCommand Insight 모듈은 연간 기간 또는 영구 라이선스됩니다.

- 검색, 보증, 계획, 모듈 수행을 위해 테라바이트별로 모니터링되는 용량을 기준으로 합니다
- 호스트 활용도 팩의 호스트 수 기준
- 보고서 작성을 위해 필요한 Cognos 전문가 집필자 수 기준

라이선스 키는 각 고객에 대해 생성되는 고유한 문자열 집합입니다. OnCommand Insight 담당자에게 라이선스 키를 받을 수 있습니다.

설치된 라이선스는 소프트웨어에서 사용할 수 있는 다음 옵션을 제어합니다.

- * 발견 *

재고 확보 및 관리(기초)

변경 사항을 모니터링하고 인벤토리 정책을 관리합니다

- * 보증 *

SAN 경로 정책 및 위반 사항을 확인하고 관리합니다

취약점을 보고 관리합니다

작업 및 마이그레이션 보기 및 관리

- * 계획 *

요청을 보고 관리합니다

보류 중인 작업을 보고 관리합니다

예약 위반 사항을 보고 관리합니다

포트 균형 위반을 보고 관리합니다

- * 성능 *

대시보드 위젯, 자산 페이지 및 쿼리의 데이터를 비롯한 성능 데이터를 모니터링합니다

성능 정책 및 위반 사항을 확인하고 관리합니다

다음 표에서는 admin 사용자 및 admin이 아닌 사용자에게 대한 Perform 라이선스와 함께 사용할 수 있는 기능에 대한 세부 정보를 제공합니다.

기능(관리자)	Perform 라이선스 사용	Perform 라이선스 없음
응용 프로그램	예	성능 데이터 또는 차트가 없습니다
가상 머신	예	성능 데이터 또는 차트가 없습니다
하이퍼바이저	예	성능 데이터 또는 차트가 없습니다
호스트	예	성능 데이터 또는 차트가 없습니다
데이터 저장소	예	성능 데이터 또는 차트가 없습니다
VMDK입니다	예	성능 데이터 또는 차트가 없습니다

내부 볼륨	예	성능 데이터 또는 차트가 없습니다
볼륨	예	성능 데이터 또는 차트가 없습니다
스토리지 풀	예	성능 데이터 또는 차트가 없습니다
디스크	예	성능 데이터 또는 차트가 없습니다
스토리지	예	성능 데이터 또는 차트가 없습니다
스토리지 노드	예	성능 데이터 또는 차트가 없습니다
패브릭	예	성능 데이터 또는 차트가 없습니다
스위치 포트	예	성능 데이터 또는 차트 없음, "포트 오류"는 "해당 없음"으로 표시됨
스토리지 포트입니다	예	예
NPV 포트입니다	예	성능 데이터 또는 차트가 없습니다
스위치	예	성능 데이터 또는 차트가 없습니다
NPV 전환	예	성능 데이터 또는 차트가 없습니다
Qtree	예	성능 데이터 또는 차트가 없습니다
할당량	예	성능 데이터 또는 차트가 없습니다
경로	예	성능 데이터 또는 차트가 없습니다
Zone(영역)	예	성능 데이터 또는 차트가 없습니다
Zone 멤버	예	성능 데이터 또는 차트가 없습니다
일반 장치	예	성능 데이터 또는 차트가 없습니다
테이프	예	성능 데이터 또는 차트가 없습니다
마스킹	예	성능 데이터 또는 차트가 없습니다
iSCSI 세션	예	성능 데이터 또는 차트가 없습니다

ICSI 네트워크 포털	예	성능 데이터 또는 차트가 없습니다
검색	예	예
관리자	예	예
대시보드	예	예
위젯	예	부분적으로 사용 가능(자산, 쿼리 및 관리 위젯만 사용 가능)
위반 대시보드	예	숨김
자산 대시보드	예	부분적으로 사용 가능(스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)
성능 정책 관리	예	숨김
주석 관리	예	예
주석 규칙을 관리합니다	예	예
애플리케이션 관리	예	예
쿼리	예	예
업무 엔티티를 관리합니다	예	예

피처	사용자 - Perform 라이센스가 있는 경우	게스트 - Perform 라이센스 포함	사용자 - Perform 라이센스가 없습니다	게스트 - Perform 라이센스 없음
자산 대시보드	예	예	부분적으로 사용 가능 (스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)	부분적으로 사용 가능 (스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)
맞춤형 대시보드	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)
성능 정책 관리	예	숨김	숨김	숨김
주석 관리	예	숨김	예	숨김

애플리케이션 관리	예	숨김	예	숨김
업무 엔티티를 관리합니다	예	숨김	예	숨김
쿼리	예	보기 및 편집만(저장 옵션 없음)	예	보기 및 편집만(저장 옵션 없음)

설치 문제 해결

OnCommand Insight 설치 는 일반적으로 설치 마법사를 통해 관리됩니다. 그러나 업그레이드 도중 문제가 발생하거나 컴퓨터 환경으로 인해 충돌이 발생할 수 있습니다.

또한 소프트웨어 설치에 필요한 모든 OnCommand Insight 라이선스를 설치해야 합니다.

라이선스가 없습니다

OnCommand Insight 기능마다 다른 라이선스가 필요합니다. OnCommand Insight에 표시되는 내용은 설치된 라이선스에 의해 제어됩니다. 각 라이선스로 제어되는 기능에 대한 자세한 내용은 OnCommand Insight 라이선스 섹션을 참조하십시오.

각 라이선스로 제어되는 기능에 대한 자세한 내용은 OnCommand Insight 라이선스 섹션을 참조하십시오.

온라인 기술 지원 요청 제출

Insight 설치에 문제가 있는 경우 등록된 지원 고객으로서 온라인 기술 지원 요청을 제출할 수 있습니다.

시작하기 전에

회사 이메일 주소를 사용하여 온라인 지원 서비스를 받으려면 지원 고객으로 등록해야 합니다. 등록은 지원 사이트를 통해 수행됩니다 .

이 작업에 대해

설치 문제 해결에 대한 고객 지원을 지원하려면 다음 항목을 포함하여 가능한 많은 정보를 수집해야 합니다.

- Insight 일련 번호
- 문제에 대한 설명입니다
- 모든 Insight 로그 파일
- 오류 메시지의 화면 캡처

단계

1. 을 생성합니다 .zip 문제 해결 패키지를 만들기 위해 수집한 정보 파일
2. 에서 지원 사이트에 로그인합니다 "mysupport.netapp.com" 을 클릭하고 * 기술 지원 * 을 선택합니다.

3. 케이스 열기 * 를 클릭합니다.
4. 데이터 패키지에 대한 지침을 따르십시오.

작업을 마친 후

기술 지원 페이지의 * 케이스 상태 확인 * 을 사용하여 요청을 추적할 수 있습니다.

Insight 업그레이드

새 버전의 OnCommand Insight를 사용할 수 있는 경우 새 기능 및 문제 해결 방법을 활용하기 위해 업그레이드할 수 있습니다. Insight 서버 및 DWH(데이터 웨어하우스)는 별도로 업그레이드해야 합니다.



업그레이드 프로세스 중에 전체 설치 폴더를 덮어쓰므로 Insight 설치 디렉토리에 자동 또는 수동 백업을 저장하면 안 됩니다. 이러한 디렉토리에 백업 파일을 저장한 경우 업그레이드 또는 제거 프로세스를 수행하기 전에 백업을 다른 위치로 이동해야 합니다.

Insight의 최신 버전은 디스크 공간, 메모리 및 CPU 요구 사항이 더 큼니다. Insight 최신 버전으로 업그레이드하기 전에 설치 요구 사항을 검토하십시오. Insight를 설치 또는 업그레이드하기 전에 세일즈 엔지니어에게 자세한 사이징 지침을 문의하는 것이 좋습니다.

Insight 소프트웨어를 업그레이드하기 전에 보안 백업 및 데이터베이스 백업을 수행하는 것이 좋습니다.

Insight를 버전 7.3.12 이상으로 업그레이드 - Linux

OnCommand Insight 7.3.10-7.3.11에서 버전 7.3.12 이상으로 업그레이드하기 전에 OCI 데이터 마이그레이션 툴을 실행해야 합니다.

배경

OnCommand Insight 버전 7.3.12 이상은 이전 버전과 호환되지 않을 수 있는 기본 소프트웨어를 사용합니다. Insight 버전 7.3.12 이상에는 업그레이드를 지원하는 * 데이터 마이그레이션 도구 * 가 포함되어 있습니다.



OnCommand Insight 버전 7.3.9 및 이전 버전은 더 이상 지원되지 않습니다. 이러한 버전 중 하나를 실행 중인 경우 7.3.12 이상으로 업그레이드하기 전에 Insight 버전 7.3.10 이상으로 _업그레이드해야 합니다(7.3.11 권장).

데이터 마이그레이션 툴은 어떤 기능을 합니까?

마이그레이션 도구는 초기 호환성 검사를 수행한 다음 세 가지 업그레이드 경로 중 하나를 따릅니다. 선택한 경로는 현재 버전의 데이터 호환성을 기반으로 합니다.



업그레이드하기 전에 데이터 마이그레이션 도구를 실행하고 권장 단계를 수행해야 합니다.

시작하기 전에

- 데이터 마이그레이션 툴을 실행하기 전에 OnCommand Insight 시스템을 백업하는 것이 좋습니다.

- 서버의 Elasticsearch 서비스가 실행 중이어야 합니다.
- Insight를 업그레이드하기 전에 데이터베이스 및 성능 아카이브를 위해 Data Migration Tool_many_be를 실행해야 합니다.

데이터 마이그레이션 툴 실행

1. 최신 버전의 데이터 마이그레이션 도구(예: *SANScreenDataMigrationTool-x86-7.3.12-97.zip*)를 Insight 서버와 해당 Insight 설치 프로그램 파일로 다운로드합니다. 작업 폴더에 압축을 풉니다. 다운로드는 [에서 찾을 수 있습니다](#) "NetApp Support 사이트".
2. 명령 창을 열고 작업 폴더로 이동합니다.
 - Bash 셸을 사용하는 것이 좋습니다.
3. 다음 명령을 사용하여 데이터 마이그레이션 툴을 실행합니다.
 - `_SUDO./SANScreenDataMigrationTool.sh' _`
4. 필요에 따라 지침을 따릅니다. 다음은 예제입니다.

```
sudo ./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
    the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

데이터 마이그레이션 도구는 시스템에 사용되지 않는 인덱스가 있는지 확인하고 있는지 보고합니다. 없을 경우 도구가 종료됩니다.

SANscreen 서버 서비스가 실행되는 동안 일부 인덱스가 마이그레이션될 수 있습니다. 다른 서버는 서버가 중지된 경우에만 마이그레이션될 수 있습니다. 마이그레이션할 수 있는 인덱스가 없는 경우 이 도구는 종료됩니다. 그렇지 않으면 메시지가 나타나면 지침을 따릅니다.

데이터 마이그레이션 도구가 완료되면 사용되지 않는 인덱스가 있는지 다시 확인합니다. 모든 인덱스가 마이그레이션된 경우 OnCommand Insight 7.3.12로의 업그레이드가 지원된다는 메시지가 표시됩니다. 이제 Insight 업그레이드를 진행할 수 있습니다.

```

sudo ./SansscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-132

OCI 7.3.10.8.139 is installed
Elasticsearch REST port = 9200

Checking for obsolete (version 5) indexes...
Found 76 obsolete OCI indexes. Of these,
76 indexes may be migrated with OCI server running

SANscreen Server service is running

Proceed with online migration of 76 indexes (y or [n])? y
If you supply performance archive location, entries for any dates with
migrated
indexes will be replaced. Each original entry will be renamed and you may
delete
it after migration is completed.
When prompted enter the archive location including the site-name
directory.

Enter the location of the performance archive or blank if none:
Performance archive entries will not be updated

Running the migration application with options -u http://localhost:9200
--online -sa -

Preparing to migrate oci-timeseries-disk-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-internalvolume-2021-03-22: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate oci-timeseries-port-2021-03-22: copied; backup;
delete old; restore new; cleanup; done.
...
Preparing to migrate oci-timeseries-disk-2021-03-27: copied; backup;
delete old; restore new; cleanup; done.
Execution time 0:08:17
Checking for obsolete (version 5) indexes...

No obsolete indexes found. Upgrade and Inline Upgrade to 7.3.12+ are
supported

```

SANscreen 서비스를 중지하라는 메시지가 표시되면 Insight를 업그레이드하기 전에 다시 시작합니다.

검증 실패

인덱스 유효성 검사에 실패하는 경우 마이그레이션 도구는 종료하기 전에 문제를 알려 줍니다.

- OnCommand Insight가 없습니다: *

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

- 잘못된 Insight 버전: *

```
./SanscreenDataMigrationTool.sh

NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

- Elasticsearch 서비스가 실행되고 있지 않습니다: *

```
./SanscreenDataMigrationTool.sh
NetApp SANScreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

명령줄 옵션

데이터 마이그레이션 툴에는 작업에 영향을 주는 몇 가지 선택적 매개 변수가 포함되어 있습니다.

옵션(Linux)	기능
	--조용히
모든 프롬프트를 표시하지 않습니다	-A
--아카이브	<p>지정된 경우 인덱스가 마이그레이션되는 모든 날짜의 기존 아카이브 항목이 교체됩니다. 경로는 아카이브 항목 zip 파일이 포함된 디렉토리를 가리켜야 합니다.</p> <p>업데이트할 성능 아카이브가 없음을 나타내기 위해 '-'의 인수를 지정할 수 있습니다.</p> <p>이 인수가 있으면 아카이브 위치에 대한 프롬프트가 표시되지 않습니다.</p>
	— 확인
이 경우 인덱스 카운트를 보고한 후 스크립트가 즉시 종료됩니다.	-d
--dryrun	마이그레이션 실행 파일이 있는 경우 데이터 마이그레이션 및 아카이브 항목 업데이트를 위해 수행할 작업은 보고하지만 작업을 수행하지 않습니다.
-p	--포트
<p>제공된 값이 있는 경우 Elasticsearch의 REST 포트로 사용합니다. 없는 경우 가능한 경우 설치에서 값을 구합니다. 그렇지 않으면 기본값 9200을 사용합니다.</p> <div>  <p>일부 Linux OnCommand Insight 설치의 경우 기본 9200 포트에서 Elasticsearch REST 포트가 실행되지 않을 수 있습니다. 이 경우 --port 옵션을 사용하여 값을 제공합니다</p> </div>	-h
- 도움말	사용 정보를 표시합니다

문제 해결

아카이브 항목이 업데이트된 경우 업데이트된 아카이브의 소유권 및 권한이 올바른지 _해야 합니다. 이 경우 * ocisys ocisys 644 * 이어야 합니다. 그렇지 않은 경우 성능 아카이브 폴더로 이동하여 다음 명령을 실행합니다.

```
chown ocisys *
chgrp ocisys *
chmod 644 *
```

Insight Server 소프트웨어 업그레이드 중

서버에 로그인한 후 OnCommand Insight 서버 업데이트를 확인할 수 있습니다.

단계

1. Insight 도구 모음에서 * 도움말 * 아이콘을 클릭합니다.
2. 업데이트 확인 * 을 선택합니다.
3. 의 경우 * 확인 * 을 클릭합니다 Version is up to date 메시지가 표시됩니다.
4. 최신 버전이 감지되면 메시지 상자에서 * download here * 링크를 클릭합니다.
5. 다운로드 * 페이지에서 * 다운로드 * 를 클릭합니다. 다운로드 디렉터리 위치를 확인합니다.

NetApp Support 사이트에서 최신 버전을 다운로드할 수도 있습니다.

6. sudo 권한이 있는 계정을 사용하여 Insight 서버에 로그인합니다.
7. 다운로드 디렉터리로 이동하여 다음 명령을 입력합니다.

```
unzip oci-<version>-linux-x86_64.zip
```

설치 파일의 버전 번호가 올바른지 확인합니다.

8. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 oci-install.sh :

```
sudo ./oci-<version>-linux-x86_64/oci-install.sh --help
```

9. 설치 스크립트를 실행합니다.

```
sudo ./oci-<version>-linux-x86_64/oci-install.sh
```

10. 사용권 계약에 동의하고 화면의 지시를 따릅니다.

데이터 웨어하우스 소프트웨어 업그레이드 중

Insight 서버 소프트웨어를 업그레이드한 후에는 데이터 웨어하우스 소프트웨어를 업그레이드해야 합니다.

단계

1. sudo 권한이 있는 계정을 사용하여 DWH(데이터 웨어하우스) 서버에 로그인합니다.
2. NetApp Support 사이트에서 Insight DWH 소프트웨어를 다운로드합니다.
3. 다운로드 디렉터리로 이동하여 다음 명령을 입력합니다.

```
unzip oci-dwh-<version>-linux-x86_64.zip
```

설치 파일의 버전 번호가 올바른지 확인합니다.

4. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 oci-install.sh :


```
sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh --help
```

5. 설치 스크립트를 실행합니다.

```
sudo ./oci-dwh-<version>-linux-x86_64/oci-install.sh
```

6. 사용권 계약에 동의하고 화면의 지시를 따릅니다.

원격 획득 장치 소프트웨어 업그레이드

Insight 서버 소프트웨어를 업그레이드한 후에는 원격 구입 소프트웨어를 업그레이드해야 합니다.

단계

1. sudo 권한이 있는 계정을 사용하여 RAU(원격 획득 장치) 서버에 로그인합니다.
2. NetApp Support 사이트에서 Insight RAU 소프트웨어를 다운로드합니다.
3. 다운로드 디렉터리로 이동하여 다음 명령을 입력합니다.

```
unzip oci-rau-<version>-linux-x86_64.zip
```

설치 파일의 버전 번호가 올바른지 확인합니다.

4. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 `oci-install.sh`:

```
sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh --help
```

5. 설치 스크립트를 실행합니다.

```
sudo ./oci-rau-<version>-linux-x86_64/oci-install.sh
```

6. 사용권 계약에 동의하고 화면의 지시를 따릅니다.

Windows에서 Linux로 마이그레이션

기존 Windows를 설치한 경우 Linux에서 Insight를 사용하려면 마이그레이션을 수행해야 합니다. Insight 서버와 데이터 웨어하우스 구성 요소 모두에서 이 절차를 수행해야 합니다.

단계

1. 서버에 현재 Insight 설치를 백업합니다.

OCI 데이터베이스를 백업하는 방법에 대한 자세한 내용은 `_OnCommand Insight 구성 및 관리 가이드_`를 참조하십시오.

2. Linux용 Insight를 설치합니다.
3. 이전 버전의 데이터베이스를 복원합니다.

OCI 데이터베이스를 복원하는 방법에 대한 자세한 내용은 `_OnCommand Insight 구성 및 관리 가이드_`를

참조하십시오.

4. 이전 버전의 Insight for Windows를 제거합니다.

OnCommand Insight를 제거하는 중입니다

필요한 경우 OnCommand Insight 구성 요소를 제거할 수 있습니다. OnCommand Insight 구성 요소는 별도로 제거해야 합니다.

각 구성 요소는 별도로 제거됩니다.

OnCommand Insight 서버 제거

필요한 경우 OnCommand Insight 서버를 제거할 수 있습니다.

시작하기 전에

모범 사례: Insight를 제거하기 전에 OnCommand Insight 데이터베이스를 백업하십시오.

단계

1. sudo 권한이 있는 계정을 사용하여 OnCommand Insight 서버에 로그인합니다.
2. 모든 OnCommand Insight 창이 닫혔는지 확인합니다.
3. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 `oci-uninstall.sh` 다음 명령을 입력합니다.

```
sudo /usr/bin/oci-uninstall.sh --help
```

일반적인 설치 제거를 수행해도 Insight 라이선스나 일일 백업은 제거되지 않습니다. 전체 설치를 제거하려면 `oci-uninstall.sh` 명령을 사용합니다 `--purge` 와 함께 하는 `oci-install.sh` 명령.

4. 다음 명령을 입력합니다.

```
sudo /usr/bin/oci-uninstall.sh
```

데이터 웨어하우스 제거 중

필요한 경우 데이터 웨어하우스를 제거할 수 있습니다.

시작하기 전에

DWH(OnCommand Insight Data Warehouse) 데이터베이스의 현재 버전을 백업합니다.

이 작업에 대해

OnCommand Insight 데이터 웨어하우스를 제거하면 이전에 수집한 모든 데이터가 영구적으로 삭제됩니다.

단계

1. sudo 권한이 있는 계정을 사용하여 데이터 웨어하우스 서버에 로그인합니다.
2. 모든 OnCommand Insight 창이 닫혔는지 확인합니다.
3. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 `uninstall.sh` 다음 명령을 입력합니다. `sudo /usr/bin/oci-uninstall.sh --help`
4. 다음 명령을 입력합니다. `sudo /usr/bin/oci-uninstall.sh`

원격 획득 장치 제거

원격 획득 장치가 더 이상 필요하지 않으면 제거할 수 있습니다.

단계

1. sudo 권한이 있는 계정을 사용하여 원격 획득 장치 서버에 로그인합니다.
2. 모든 OnCommand Insight 창이 닫혔는지 확인합니다.
3. 에 대한 구문, 명령 인수 및 매개 변수 사용을 볼 수 있습니다 `uninstall.sh` 다음 명령을 입력합니다. `sudo /usr/bin/oci-uninstall.sh --help`
4. 다음 명령을 입력합니다. `sudo /usr/bin/oci-uninstall.sh`

제거 스크립트가 실행됩니다. 화면의 지시를 따릅니다.

Microsoft Windows용 설치

설치 필수 구성 요소

OnCommand Insight를 설치하기 전에 현재 소프트웨어 버전을 다운로드하고 적절한 라이선스를 취득하며 환경을 설정해야 합니다.

OnCommand Insight를 설치하기 전에 다음 사항을 확인하십시오.

- 현재 버전의 다운로드한 설치 패키지에 있는 OnCommand Insight 소프트웨어 파일입니다
- 다운로드한 OnCommand Insight 버전을 작동하는 라이선스입니다
- 최소 하드웨어 및 소프트웨어 환경

현재 제품은 이전 버전의 OnCommand Insight 제품에서 사용되지 않은 추가 하드웨어 리소스(향상된 OnCommand Insight 제품 기능)를 사용할 수 있습니다.

- OnCommand Insight 서버, 데이터 웨어하우스 및 보고, 원격 획득 장치의 하드웨어 및 네트워크 구성을 포함하는 배포 계획.
- 바이러스 검사 소프트웨어를 비활성화했습니다

OnCommand Insight를 설치하는 동안 모든 바이러스 스캐너를 완전히 비활성화해야 합니다. 설치 후 Insight 구성 요소(설치, 백업 및 Archiver 경로)에서 사용하는 경로는 전체 경로를 제외하고 바이러스 검사에서 제외되어야 합니다 sansscreen 스캔 디렉터리.

또한 설치 후 바이러스 백신 검사에서 IBM/DB2 폴더(예: C:\Program Files\IBM\DB2)를 제외해야 합니다.

업그레이드 또는 새 하드웨어로 전체 설치를 수행하는 경우 기존 시스템에 기본값이 아닌 보안 구성이 포함되어 있는 경우 설치를 수행하기 전에 보안 구성을 백업해야 합니다. 설치가 완료되면 서버(로컬 획득 장치 포함) 또는 데이터 웨어하우스 데이터베이스를 복원하기 전에 보안 구성을 복원해야 합니다. DWH 데이터베이스를 복원하기 전에 모든 Insight 서버에 보안 구성을 복원해야 합니다.



현재 위치 업그레이드의 경우(Insight Server에서만 사용 가능) 보안 구성이 올바르게 처리되므로 복원할 필요가 없습니다.

를 사용합니다 securityadmin 구성 백업을 생성하고 저장된 구성을 복원하는 도구입니다. 자세한 내용을 보려면 을 검색합니다 securityadmin OnCommand Insight 문서 센터에서:

<http://docs.netapp.com/oci-73/index.jsp>

배포 계획

성공적인 배포를 위해서는 OnCommand Insight를 설치하기 전에 특정 시스템 요소를 고려해야 합니다.

이 작업에 대해

Insight 배포를 계획할 때 다음과 같은 시스템 요소를 고려해야 합니다.

- Insight 아키텍처
- 모니터링할 네트워크 구성 요소
- Insight 설치 사전 요구 사항 및 서버 요구 사항
- Insight 웹 브라우저 요구사항

데이터 소스 지원 정보

구성 계획의 일환으로 Insight에서 사용자 환경의 장치를 모니터링할 수 있는지 확인해야 합니다. 이렇게 하려면 데이터 소스 지원 매트릭스에서 운영 체제, 특정 장치 및 프로토콜에 대한 자세한 내용을 확인할 수 있습니다. 일부 데이터 소스는 일부 운영 체제에서 사용하지 못할 수 있습니다.

데이터 소스 지원 매트릭스의 최신 버전 위치

OnCommand Insight 데이터 소스 지원 매트릭스는 각 서비스 팩 릴리스에 따라 업데이트됩니다. 문서의 최신 버전은 [여기](#)에서 찾을 수 있습니다 "[NetApp Support 사이트](#)". .

장치 식별 및 데이터 소스 계획

배포 계획의 일환으로 환경에 있는 장치에 대한 정보를 수집해야 합니다.

사용자 환경의 각 장치에 대한 다음 소프트웨어, 연결 및 정보가 필요합니다.

- OCI 서버에서 확인할 수 있는 IP 주소 또는 호스트 이름입니다
- 로그인 이름 및 암호
- 장치 액세스 유형(예: 컨트롤러 및 관리 스테이션)



대부분의 장치에 읽기 전용 액세스만으로도 충분하지만 일부 장치에는 관리자 권한이 필요합니다.

- 데이터 소스 포트 요구 사항에 따라 장치에 대한 포트 연결
- 스위치의 경우 SNMP 읽기 전용 커뮤니티 문자열(스위치에 대한 액세스를 제공하는 사용자 ID 또는 암호)
- 디바이스에 필요한 타사 소프트웨어(예: Solutions Enabler)
- 데이터 소스 사용 권한 및 요구 사항에 대한 자세한 내용은 웹 UI 도움말 또는 _OnCommand Insight 구성 및 관리 가이드_의 "공급업체별 데이터 소스 참조"를 참조하십시오.

OnCommand Insight에서 생성된 네트워크 트래픽입니다

OnCommand Insight가 생성하는 네트워크 트래픽, 네트워크를 통과하는 처리된 데이터의 양 및 OnCommand Insight가 디바이스에 배치하는 로드는 여러 요인에 따라 달라집니다.

트래픽, 데이터 및 로드는 다음 요소에 따라 환경에 따라 다릅니다.

- 원시 데이터
- 장치 구성
- OnCommand Insight의 구축 토폴로지

- 느린 디바이스를 발견하거나 대역폭을 처리할 수 있도록 여러 인벤토리 및 성능 데이터 소스 폴링 간격을 줄일 수 있습니다

OnCommand Insight에서 수집하는 원시 구성 데이터는 크게 다를 수 있습니다.

다음 예에서는 구성 데이터가 어떻게 변하는지, 그리고 여러 구성 요소의 트래픽, 데이터 및 로드가 어떤 영향을 받는지 보여 줍니다. 예를 들어 각각 1,000개의 디스크가 있는 두 개의 어레이가 있을 수 있습니다.

- 어레이 1: 크기가 모두 1TB인 SATA 디스크 1,000개가 있습니다. 1,000개의 디스크가 모두 하나의 스토리지 풀에 있고 1,000개의 LUN이 있으며, 모두 ESX 클러스터의 동일한 32개 노드에 표시(매핑 및 마스킹됨)됩니다.
- 어레이 2: 2TB 데이터 디스크 400개, 600GB FC 디스크 560개 및 SSD 40개가 있습니다. 스토리지 풀은 3개가 있지만 FC 디스크 320개가 기존 RAID 그룹에 사용됩니다. RAID 그룹에 포함된 LUN은 기존 마스킹 유형(symmaskdb)을 사용하는 반면, 씬 프로비저닝된 풀 기반 LUN은 최신 마스킹 유형(symaccess)을 사용합니다. 150개의 호스트에 600개의 LUN이 제공됩니다. 200개의 BCV(600개의 LUN 중 200개의 전체 블록 복제본 볼륨)가 있습니다. 다른 사이트의 스토리지에 있는 볼륨의 원격 복제본 볼륨인 R2 볼륨도 200개가 있습니다.

이러한 어레이에는 각각 1,000개의 디스크와 1,000개의 논리적 볼륨이 있습니다. 이러한 공간은 데이터 센터에서 소비하는 랙 공간의 크기와 물리적으로 동일하며 동일한 펌웨어를 실행하기도 하지만 두 번째 어레이는 첫 번째 어레이보다 구성에서 훨씬 복잡합니다.

바이러스 검사 소프트웨어 비활성화

시스템에서 바이러스 백신 소프트웨어가 활성 상태인 경우 OnCommand Insight 설치가 실패합니다. 설치하기 전에 바이러스 검사 소프트웨어를 비활성화하여 이 문제를 방지할 수 있습니다.

활성 바이러스 검사 소프트웨어로 인한 설치 실패를 방지하려면 각 OnCommand Insight 구성 요소를 설치하는 동안 모든 바이러스 스캐너를 완전히 비활성화해야 합니다. 설치 후에는 Insight 구성 요소(설치, 백업 및 Archiver 경로)에서 사용하는 경로를 바이러스 검사에서 제외해야 합니다.

또한 설치 후 바이러스 백신 검사에서 IBM/DB2 폴더(예: C:\Program Files\IBM\DB2)를 제외해야 합니다.

Insight Server 요구사항

전용 서버가 권장됩니다. 다른 애플리케이션이 설치된 서버에 Insight를 설치하지 마십시오. 제품 요구 사항이 충족되는 경우 물리적 서버와 가상 서버가 모두 지원됩니다.

OnCommand Insight 서버 소프트웨어를 설치하려면 로컬 관리자 권한이 있어야 합니다.



OnCommand Insight 크기 조정에는 데이터 소스 유형 및 크기, 환경의 자산 수, 폴링 간격 등 다양한 종속 항목이 있습니다. 다음 사이징 예는 지침일 뿐이며 Insight가 테스트된 환경의 일부를 나타냅니다. 환경의 이러한 요인 또는 기타 요소를 변경하면 Insight의 사이징 요구 사항이 변경될 수 있습니다. 이러한 지침에는 최대 90일간의 성능 아카이브 데이터를 위한 디스크 공간이 포함되어 있습니다.

Insight를 설치 또는 업그레이드하기 전에 세일즈 엔지니어에게 자세한 사이징 지침을 문의하는 것이 좋습니다.

- 예: *

환경 요인:	테스트한 디스크 공간, CPU 및 메모리:
--------	-------------------------

80개 스토리지 4,000개 볼륨 4,000개의 VM 4,000개의 스위치 포트	250GB 디스크 공간 8코어 32GB RAM
160 스토리지 어레이 40,000개의 볼륨 8,000개의 VM 8,000개의 스위치 포트	1TB 디스크 공간 12개 코어 48GB RAM

• 요구 사항: *

구성 요소	필수 요소입니다
운영 체제	<p>최신 서비스 팩이 설치된 64비트 Microsoft Windows Server 2016, 2019 또는 2022를 실행하는 컴퓨터.</p> <p>Windows Server 2012에 도입된 복구 파일 시스템(ReFS)은 OnCommand Insight와 호환되지 않습니다. OnCommand Insight의 Windows 설치 NTFS 파일 시스템에서만 지원됩니다.</p> <p>전용 서버가 권장됩니다.</p>
가상 머신(VM)	이 구성 요소는 인스턴스에 대한 CPU 및 메모리 리소스가 예약되어 있는 경우 가상 환경에서 실행될 수 있습니다.
메모리 및 CPU	<p>24-256GB RAM</p> <p>8~32코어</p> <p>페이징 파일 크기를 "Windows 관리"로 설정하는 것이 좋습니다. 크기가 작은 페이징 파일은 Insight 성능 데이터의 성공적인 저장을 방해할 수 있습니다.</p>
사용 가능한 디스크 공간입니다	<p>100GB - 3TB 설치 디스크 공간</p> <p>50GB - 1TB 성능 아카이브 디스크 공간</p> <p>Insight 설치 공간에는 SSD 디스크를 사용하는 것이 좋습니다.</p>

네트워크	<p>이더넷 연결 및 포트:</p> <ul style="list-style-type: none"> • FC 장치 및 원격 획득 장치를 포함하여 SAN의 모든 구성 요소에 대한 전용(정적) IP 주소 및 IP 연결을 통한 100Mbps 또는 1Gbps 이더넷 연결 • OnCommand Insight 서버 프로세스의 포트 요구 사항은 80, 443, 1090 ~ 1100, 3873, 8083입니다. 4444 ~ 4446, 5445, 5455, 4712 ~ 4714, 5500, 및 5501을 참조하십시오. • 획득 프로세스의 포트 요구 사항은 12123 및 5679입니다. • MySQL의 포트 요구 사항은 3306입니다. • Elasticsearch의 포트 요구 사항은 9200 및 9310입니다 • Win2008/2012의 동적 포트 요구 사항은 49152 ~ 65535입니다 <p>포트 443 및 3306은 존재하는 방화벽을 통해 외부 액세스를 필요로 합니다.</p>
권한	<p>OnCommand Insight 서버에 로컬 관리자 권한이 필요합니다.</p> <p>다음 폴더 중 하나가 심볼 링크인 경우 대상 디렉토리에 '755' 권한이 있는지 확인하십시오.</p> <ul style="list-style-type: none"> • /opt/NetApp을 참조하십시오 • /var/lib/netapp • /var/log/netapp
원격 연결	WebEx 액세스를 위한 인터넷 연결 또는 설치 및 설치 후 지원을 위한 원격 데스크톱 연결
접근성	HTTPS 액세스가 필요합니다.
바이러스 검사	<p>이 OnCommand Insight 구성 요소를 설치하는 동안 모든 바이러스 스캐너를 완전히 비활성화해야 합니다. 설치 후에는 Insight 구성 요소(설치, 백업 및 Archiver 경로)에서 사용하는 경로를 바이러스 검사에서 제외해야 합니다.</p> <p>또한 설치 후 바이러스 백신 검사에서 IBM/DB2 폴더(예: C:\Program Files\IBM\DB2)를 제외해야 합니다.</p>

HTTP 또는 HTTPS 서버	Microsoft IIS(인터넷 정보 서비스) 또는 다른 HTTPS 서버는 OnCommand Insight 서버와 동일한 포트(443)에 대해 경쟁해서는 안 되며 자동으로 시작해서는 안 됩니다. 포트 443을 수신해야 하는 경우 다른 포트를 사용하도록 OnCommand Insight 서버를 구성해야 합니다.
------------------	--

데이터 웨어하우스 및 보고 서버 요구 사항

이미 설정된 하드웨어 및 소프트웨어 요구 사항과 호환되는 컴퓨터에서 데이터 웨어하우스 및 보고 서버를 실행해야 Apache 웹 서버 또는 보고 소프트웨어가 이 컴퓨터에 설치되어 있지 않습니다.



OnCommand Insight를 위한 사이징에는 운영 환경의 자산 수, 유지되는 기간별 데이터 양 등과 같은 다양한 종속 관계가 있습니다. 다음 데이터 웨어하우스 사이징 예는 지침일 뿐이며 Insight가 테스트된 일부 환경을 나타냅니다. 환경의 이러한 요인 또는 기타 요소를 변경하면 Insight의 사이징 요구 사항이 변경될 수 있습니다.

Insight를 설치 또는 업그레이드하기 전에 세일즈 엔지니어에게 자세한 사이징 지침을 문의하는 것이 좋습니다.

• 예: *

환경 요인:	테스트한 디스크 공간, CPU 및 메모리:
스토리지 18개 이상 머신 3,400개	200GB 하드 디스크 8 코어
4,500개의 스위치 포트	32GB RAM
110개의 스토리지 어레이 11,500개의 VM을 제공합니다	300GB 하드 디스크 8 코어
14,500개의 스위치 포트	48GB RAM

• 요구 사항: *

구성 요소	필수 요소입니다
운영 체제	최신 서비스 팩이 설치된 64비트 Microsoft Windows Server 2016, 2019 또는 2022를 실행하는 컴퓨터.
가상 머신(VM)	이 구성 요소는 인스턴스에 대한 CPU 및 메모리 리소스가 예약되어 있는 경우 가상 환경에서 실행될 수 있습니다.
CPU	8-40개의 CPU 코어

메모리	32GB - 2TB RAM 모범 사례: 페이징 파일 크기를 ""Windows 관리"로 설정하는 것이 좋습니다. 크기가 작은 페이징 파일은 Insight 성능 데이터의 성공적인 저장을 방해할 수 있습니다.
사용 가능한 디스크 공간입니다	<p>200GB - 2TB 디스크 공간 설치 시 C: 드라이브에 최소 20GB의 여유 공간이 필요합니다.</p> <div>  <p>Windows에서 Insight Data Warehouse with Reporting을 사용하려면 설치 드라이브에 8dot3 이름 생성 지원을 활성화해야 합니다. 일반적으로 C: 드라이브에는 이 기능이 기본적으로 활성화되어 있습니다. 다음 명령을 실행하여 타겟 설치 드라이브에서 8dot3 이름 생성이 활성화되었는지 확인할 수 있습니다(D: 타겟 설치 드라이브로 대체).</p> </div> <p>Fsutil 8dot3name 쿼리 D:</p> <p>8dot3 이름 생성을 활성화하려면 다음 명령을 실행합니다(D: 대상 설치 드라이브로 대체).</p> <p>fsutil 8dot3name 집합 D:0</p>
네트워크	<ul style="list-style-type: none"> • 100Mbps 또는 1Gbps 이더넷 연결 • 고정 IP 주소입니다 • Windows에 Reporting이 있는 데이터 웨어하우스를 설치하기 전에 포트 50000을 사용할 수 있어야 합니다 • OnCommand Insight DWH 서버 프로세스의 경우 포트 80, 443, 1098, 1099, 3873, 8083, 4444 ~ 4446 • 보고 엔진용 포트 1527, 9362, 9300 및 9399 • MySQL의 경우 포트 3306입니다 • 을 수행하여 DNS가 제대로 작동하는지 확인합니다 nslookup 호스트 반대입니다
바이러스 검사	이 OnCommand Insight 구성 요소를 설치하는 동안 모든 바이러스 스캐너를 완전히 비활성화해야 합니다. 설치 후에는 Insight 구성 요소(설치, 백업 및 Archiver 경로)와 모든 DWH 구성 요소 설치 경로(SANscreen, DB2 및 백업 경로)에 사용되는 경로를 바이러스 검사에서 제외해야 합니다.

Visual Studio를 참조하십시오	Visual Studio 2019 " 재배포판 " Windows에 Reporting을 사용하여 데이터 웨어하우스를 설치하기 전에 설치해야 합니다.
-----------------------	---

원격 획득 장치 서버 요구 사항

방화벽 뒤, 원격 사이트, 사설 네트워크 또는 다른 네트워크 세그먼트에 있는 SAN 장치에서 정보를 가져오려면 RAU(원격 획득 장치)를 설치해야 합니다. RAU를 설치하기 전에 사용 환경이 RAU 운영 체제, CPU, 메모리 및 디스크 공간 요구 사항을 충족하는지 확인해야 합니다.

구성 요소	요구 사항
운영 체제	최신 서비스 팩이 설치된 64비트 Microsoft Windows Server 2016, 2019 또는 2022를 실행하는 컴퓨터.
CPU	CPU 코어 4개
메모리	16GB RAM
사용 가능한 디스크 공간입니다	40GB
네트워크	100Mbps/1Gbps 이더넷 연결, 정적 IP 주소, 모든 FC 디바이스에 대한 IP 연결 및 OnCommand Insight 서버에 대한 필수 포트(80 또는 443).
권한	RAU 서버에 대한 로컬 관리자 권한
바이러스 검사	이 OnCommand Insight 구성 요소를 설치하는 동안 모든 바이러스 스캐너를 완전히 비활성화해야 합니다. 설치 후 Insight 구성 요소에서 사용하는 경로는 바이러스 검사에서 제외되어야 합니다. 또한 설치 후 바이러스 백신 검사에서 IBM/DB2 폴더(예: C:\Program Files\IBM\DB2)를 제외해야 합니다.

OnCommand Insight에서 지원되는 브라우저

브라우저 기반 OnCommand Insightfob UI는 여러 브라우저에서 작동할 수 있습니다.

Insight는 다음 브라우저의 새로운 비 베타 릴리스를 지원합니다.

- Mozilla Firefox
- Google Chrome
- Microsoft Edge를 참조하십시오

OnCommand Insight에 적합한 브라우저 버전의 전체 목록은 를 참조하십시오 "[NetApp 상호 운용성 매트릭스 툴](#)".

Insight 설치 지침

설치 시 Insight Server, 데이터 웨어하우스 및 보고를 포함한 여러 OnCommand Insight 구성 요소를 설치해야 합니다.

설치에는 다음과 같은 주요 작업이 포함됩니다.

- OnCommand Insight 설치 프로그램을 다운로드하는 중입니다
- OnCommand Insight 서버 설치 중
- 라이선스 설치 중
- 필요한 경우 DWH 및 Reporting 설치(별도의 컴퓨터 또는 가상 시스템에 설치해야 함)
- 선택적으로 방화벽 뒤에 있는 장치 리소스에서 정보를 가져오는 RAU(원격 획득 장치)를 원격 사이트에 설치하거나 개인 네트워크에 설치합니다
- 업그레이드의 경우 OnCommand Insight 보고서를 업그레이드합니다.

설치 후 환경에 대한 정보를 얻도록 Insight를 구성해야 합니다. 필요한 작업은 _OnCommand Insight 구성 및 관리 가이드_에 설명되어 있습니다.

OnCommand Insight 설치 프로그램을 다운로드하는 중입니다

NetApp Support 사이트에서 OnCommand Insight 설치 프로그램을 다운로드할 수 있습니다.

시작하기 전에

에서 NetApp Support 사이트에 로그인해야 합니다 "mysupport.netapp.com".

단계

1. OnCommand Insight를 설치할 서버에 로그인합니다.
2. NetApp Support 사이트에서 설치 파일을 다운로드합니다.

OnCommand Insight 서버 설치


OnCommand Insight 설치 마법사를 사용하여 OnCommand Insight 서버를 쉽게 설치할 수 있습니다.

시작하기 전에

설치 필수 구성 요소를 모두 완료해야 합니다.

단계

1. 관리자 권한이 있는 계정을 사용하여 Insight 서버에 로그인합니다.
2. Windows 탐색기를 열고 설치 파일이 있는 디렉터리로 이동합니다.
3. 를 두 번 클릭합니다 .MSI 파일을 다운로드했습니다.
4. 계속하려면 * 다음 * 을 클릭합니다.

5. 사용권 계약을 읽고 사용권 계약 * 확인란의 조건에 동의합니다 * 를 선택한 후 * 다음 * 을 클릭합니다.
 6. 고객 정보 * 창에 고객 이름과 사이트 이름을 입력하고 * 다음 * 을 클릭합니다.
 - 모범 사례: * 고객 이름을 사이트 접두사로 사용합니다(예: NetApp).
 7. 고객 정보: NetApp ASUP * 구성 창에서 다음을 수행합니다.
 - a. 다음 옵션 중 하나를 선택하여 ASUP에 업로드할 데이터가 포함된 데이터베이스를 선택합니다.
 - * 데이터베이스 백업 없음 *: 백업이 ASUP로 전송되지 않습니다.
 - * 성능 데이터 없이 백업 *: 백업이 수행되어 ASUP로 전송되지만 성능 데이터는 포함되지 않습니다.
 - * 성능 데이터를 사용한 백업 : 성능 데이터가 포함된 백업이 만들어지지만 이로 인해 엄청난 문제가 발생할 수 있습니다 .gz 파일.
-  ASUP는 HTTPS 프로토콜을 사용하여 제공됩니다.
- +
- a. 로그 * 에서 데이터 소스 기록을 포함하는 로그, 기본 로그 또는 확장 로그를 사용하지 않도록 선택합니다.
 - b. 다음 * 을 클릭합니다.
8. Insight 소비 라이선스 모델을 사용하는 경우 * Send usage information * 섹션에서 * Enable susage information to NetApp * 확인란을 선택해야 합니다.
9. 다음 * 을 클릭합니다
10. 서버 구성* 창에서 OnCommand Insight 서버를 구성하기 위한 적절한 구성 매개 변수를 선택하거나 설정합니다.

옵션을 선택합니다	설명
포털 포트(HTTP)	관리 작업을 수행하기 위한 포털을 포함하여 사용자 웹 서비스를 지원하기 위해 OnCommand Insight 서버에서 사용하는 포트입니다. 기본값(80)을 사용합니다. 그러나 기본 포트가 사용 중이면 다른 포트로 변경합니다.
포털 포트(HTTPS)	보안 채널을 통해 SAN 변경 정보를 OnCommand Insight 서버로 전송하기 위해 원격 획득 장치에서 사용하는 포트입니다. 기본값(443)을 사용합니다. 그러나 기본 포트가 사용 중이면 다른 포트로 변경합니다. RA를 구성할 때 동일한 포트 번호를 지정합니다.
내부 데이터베이스 포트(SQL)	OnCommand Insight 서버가 실행 중인 PC에서 데이터베이스에 대한 액세스 지점 역할을 하기 위해 내부적으로 사용하는 포트입니다. 기본값(3306)을 사용합니다. 그러나 기본 포트가 사용 중이면 다른 포트로 변경하십시오.

11. 다음 * 을 클릭합니다.
12. 계속하려면 * 설치 * 를 클릭하십시오.



OnCommand Insight 7.3.10 이상에서는 적절한 DWH/Reporting 설치를 위해 스크립트를 실행해야 합니다. MSI 설치 실행 파일을 실행하지 마십시오.

4. DB2 도메인을 입력하거나 로컬 도메인에 대해 Enter 키를 누릅니다.
5. DB2 사용자 이름을 입력합니다. 사용자 이름 제한에 대해서는 위 항목을 참조하십시오.
6. DB2 사용자의 암호를 입력합니다. 메시지가 나타나면 암호를 다시 입력합니다.
7. DB2 구성 요소의 설치 경로를 입력하거나 기본값으로 Enter 키를 누릅니다.
8. 입력한 정보가 표시됩니다. 모든 설정을 주의 깊게 확인하십시오. Enter 키를 눌러 설치를 시작합니다.
9. 메시지가 표시되면 Windows에서 DB2 설치를 계속 진행하도록 허용합니다.
10. DB2 설치 후 DWH 설치 마법사가 실행됩니다. 지침에 따라 DWH with Reporting을 설치합니다.

보고 설치를 완료하는 데 최대 1시간이 소요될 수 있습니다.

IBM Cognos 설명서 찾기

보고 포털 소프트웨어를 시작 및 중지하는 방법과 같은 기본 정보는 제품과 함께 설치된 IBM Cognos 설명서를 참조하십시오. 웹 브라우저를 통해 해당 소프트웨어 제품에 대한 IBM 웹 사이트의 Query Studio, Report Studio, Business Insight 또는 Business Insight Advanced와 같은 IBM Cognos 보고 제품에 대한 정보를 검색할 수 있습니다.

단계

1. OnCommand Insight와 함께 설치된 IBM Cognos 설명서를 찾으려면 이 디렉터리로 이동합니다.

```
<install_dir>\cognos\c10_64\webcontent\documentation\help_docs.html
```

2. OnCommand Insight 보고 포털에서 사용되는 개별 IBM Cognos 창을 설명하는 항목을 표시할 수도 있습니다. 창 도구 모음에서 *? * 아이콘을 클릭합니다.

데이터 웨어하우스 및 보고 설치 확인

OnCommand Insight 데이터 웨어하우스를 성공적으로 설치한 후에는 모든 DWH 및 보고 서비스를 Microsoft Windows 서비스에서 사용할 수 있는지 확인해야 합니다.

단계

1. Windows 시작 메뉴에서 제어판 [시스템 및 보안 > 관리 도구 > 서비스] 메뉴를 선택합니다.
2. 서비스 목록에 다음 항목이 나타나는지 확인합니다.

이름/상태	설명
• SANscreen 서버/실행 *	OnCommand Insight DWH 서버
• MySQL/Running *	OnCommand Insight SQL 데이터베이스

• IBM Cognos/Running *	IBM Cognos 콘텐츠 데이터베이스
• DB2-DB2COPY1-DB2-0/실행 중 *	DB2 데이터베이스 관리
• DB2 Governor(DB2COPY1)/Not Running *	DB2 데이터베이스에 연결된 애플리케이션에 대한 통계를 수집합니다.
• DB2 라이선스 서버(DB2COPY1)/실행 안 됨 *	DB2 라이선스 규정 준수 모니터링
• DB2 관리 서비스(DB2COPY1)/실행 중 *	DB2 레지스트리 항목이 이전 DB2 사본 버전과 호환되도록 관리합니다.
• DB2 원격 명령 서버(DB2COPY1)/실행 중 *	원격 DB2 명령 실행을 지원합니다.
• Windows용 IBM Secure Shell 서버/실행 안 함 *	Windows용 IBM Secure Shell Server

원격 획득 장치(RAU) 설치

OnCommand Insight 환경에 하나 이상의 RA를 설치합니다.

시작하기 전에

설치 필수 구성 요소를 모두 완료해야 합니다.

변경 정보를 서버로 전달하려면 RAU 서버와 OnCommand Insight 서버 간에 하나 이상의 포트를 열고 사용할 수 있어야 합니다. 확실하지 않은 경우 RAU 컴퓨터에서 웹 브라우저를 열고 OnCommand Insight 서버로 전달하여 유효성을 검사합니다.

```
https://< OnCommand Insight Server hostname >:< acquisition_port >
```

획득 포트는 기본적으로 443으로 설정되지만 서버 설치 중에 변경되었을 수 있습니다. 연결에 성공하면 RAU와 OnCommand Insight 서버 간에 사용 가능한 포트가 열려 있음을 나타내는 OnCommand Insight 응답 페이지가 나타납니다.

단계

1. 관리자 권한이 있는 계정을 사용하여 RAU 서버에 로그인합니다.
2. Windows 탐색기를 열고 RAU 설치 파일이 있는 디렉터리로 이동합니다.
3. 두 번 클릭합니다 .MSI 파일을 클릭하여 설치를 시작합니다.
4. 라이선스 계약을 표시하는 창으로 계속 진행하려면 * 다음 * 을 클릭합니다. 이 내용을 읽고 사용권 계약 내용에 동의한 후 * 다음 * 을 클릭합니다.
5. 로컬 하드 드라이브에 RAU를 설치하거나 로컬 하드 드라이브에 전체 기능을 설치하려면 선택합니다. 디스크 사용 링크를 확인하여 공간이 충분한지 확인할 수 있습니다. 116MB가 필요합니다. 다음 * 을 클릭합니다.

6. 구성 창에서 사이트에 특정한 다음 매개 변수를 설정합니다.

- * OnCommand Insight * * * 서버 이름 또는 주소 * - OnCommand Insight 서버를 식별하기 위한 호스트 이름 또는 IP 주소입니다. RAU는 이 이름/IP를 사용하여 서버와의 통신 링크를 엽니다. 호스트 이름을 지정하는 경우 DNS를 통해 호스트 이름을 확인할 수 있는지 확인합니다.
- * 획득 장치 이름 * - RAU를 식별하는 고유한 이름입니다.
- * OnCommand Insight 보안 원격 획득 포트(HTTPS) * - 환경 변경 정보를 OnCommand Insight 서버로 전송하기 위해 원격 획득 장치에서 사용하는 포트입니다. 이 설정은 OnCommand Insight 서버를 설치할 때 입력한 값과 일치해야 하며 모든 RA에서 동일해야 합니다.

7. 선택 사항을 검토합니다. 뒤로 돌아가 변경하려면 * 뒤로 * 를 클릭합니다. 다음 * 을 클릭합니다.

8. 설치를 시작하려면 * 설치 * 를 클릭합니다.

설치가 완료될 때까지 기다립니다. 이 작업은 약 5-10분 정도 걸립니다.

작업을 마친 후

설치가 완료되면 최종 창이 나타납니다. 원격 촬영 서비스 시작 * 상자를 클릭하여 RAU를 시작하고 * 마침 * 을 클릭하여 이 작업을 종료합니다.

원격 획득 장치 서비스 확인

RAU(원격 획득 장치)를 성공적으로 설치한 후에는 Microsoft Windows 서비스 환경에서 OnCommand Insight RAU 서비스를 사용할 수 있어야 합니다.

단계

1. RAU가 Windows 서비스에 추가되었는지 확인하려면 Windows 시작 메뉴를 열고 * 제어판 * > * 관리 도구 * > * 서비스 * 를 선택합니다.
2. 목록에서 * OnCommand Insight Acq-OnCommand Insight의 원격 획득 장치(RAU) * 를 찾습니다.

원격 획득 장치 설치를 검증합니다

원격 획득 장치가 올바르게 설치되었는지 확인하려면 서버에 연결된 원격 획득 장치의 상태를 볼 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 획득 단위 * 를 클릭합니다.
3. 새 원격 획득 장치가 올바르게 등록되었고 연결 상태인지 확인합니다.

그렇지 않으면 기술 지원 부서에 문의해야 합니다.

설치 확인

지원되는 브라우저에서 Insight를 열어 설치를 확인할 수 있습니다. Insight 로그 파일을 확인할 수도 있습니다.

Insight를 처음 열면 라이선스 설정 페이지가 열립니다. 라이선스 정보를 입력한 후에는 데이터 소스를 설정해야 합니다. 데이터 소스 정의 입력 및 Insight 사용자 및 알림 설정에 대한 자세한 내용은 [_OnCommand Insight 구성 및 관리 가이드_](#)를 참조하십시오.

설치 문제가 발생한 경우 기술 지원 부서에 문의하여 요청한 정보를 제공하십시오.

새로운 **Insight** 서비스 확인

성공적으로 설치한 후 Insight 구성 요소에 대한 서비스가 서버에서 작동하고 있는지 확인해야 합니다.

단계

1. 현재 작동 중인 서비스 목록을 표시하려면:

- a. 시작 * 단추를 클릭합니다.
- b. Run * 을 클릭합니다.
- c. 다음을 입력합니다.

```
cmd
```

- d. Enter 키를 누릅니다.
- e. 명령 프롬프트 * 창에 다음을 입력합니다.

```
net start
```

2. 목록에서 다음 Insight 서비스를 확인하십시오.

- * SANscreen 서버 *
- * SANscreen Acq * (획득 프로세스)
- * MySQL * (Insight SQL 데이터베이스)
- * Elasticsearch * (Insight 데이터를 위한 데이터 저장소) 이러한 서비스가 목록에 표시되지 않으면 기술 지원 부서에 문의하십시오.

Insight 로그

Insight는 조사 및 문제 해결에 도움이 되는 많은 로그 파일을 제공합니다. 사용 가능한 로그가 로그 디렉토리에 나열됩니다. BareTail과 같은 로그 모니터링 도구를 사용하여 모든 로그를 한 번에 표시할 수 있습니다.

로그 파일은 에 있습니다 <install directory>\SANscreen\wildfly\standalone\log 디렉토리. 획득 로그는 에 있습니다 <install directory>\SANscreen\Acq\Log 디렉토리.

웹 **UI** 액세스

OnCommand Insight를 설치한 후에는 라이선스를 설치한 다음 환경을 모니터링할 Insight를 설정해야 합니다. 웹 브라우저를 사용하여 Insight 웹 UI에 액세스하면 됩니다.

단계

1. 다음 중 하나를 수행합니다.

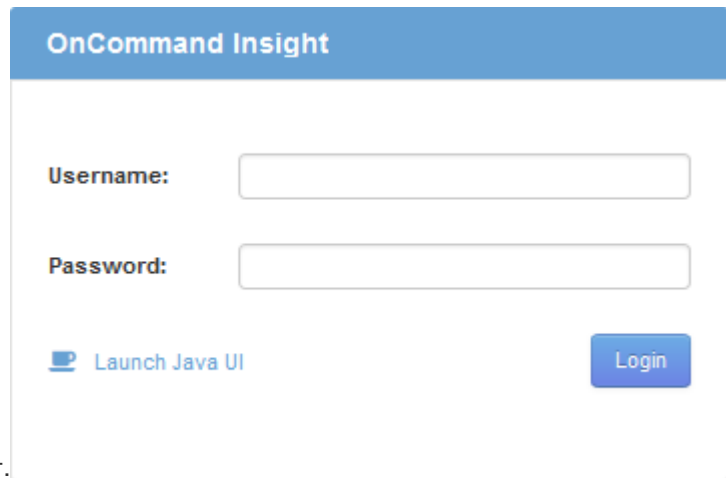
- Insight 서버에 대한 Insight를 엽니다.

`https://fqdn`

- 다른 위치에서 Insight 열기:

`https://fqdn:port`

포트 번호는 Insight 서버를 설치할 때 구성된 443 또는 다른 포트입니다. URL에서 포트 번호를 지정하지 않으면 포트 번호는 443으로 기본 설정됩니다.

The image shows the OnCommand Insight login page. It has a blue header with the text "OnCommand Insight". Below the header, there are two input fields: "Username:" and "Password:". Below the "Password:" field, there is a link that says "Launch Java UI" with a small icon of a Java logo. To the right of the "Launch Java UI" link is a blue button with the text "Login".

OnCommand Insight 대화 상자가 표시됩니다.

2. 사용자 이름과 암호를 입력하고 * 로그인 * 을 클릭합니다.

라이센스가 설치된 경우 데이터 소스 설정 페이지가 표시됩니다.



30분 동안 비활성 상태인 Insight 브라우저 세션이 시간 초과되고 시스템에서 자동으로 로그아웃됩니다. 보안 강화를 위해 Insight에서 로그아웃한 후 브라우저를 닫는 것이 좋습니다.

Insight 라이선스 설치

NetApp의 Insight 라이선스 키가 포함된 라이선스 파일을 받으면 설정 기능을 사용하여 모든 라이선스를 동시에 설치할 수 있습니다.

이 작업에 대해

Insight 라이선스 키는 에 저장됩니다 .txt 또는 .lic 파일.

단계

1. 텍스트 편집기에서 라이선스 파일을 열고 텍스트를 복사합니다.
2. 브라우저에서 Insight를 엽니다.
3. Insight 도구 모음에서 * Admin * 을 클릭합니다.

4. 설정 * 을 클릭합니다.
5. Licenses * 탭을 클릭합니다.
6. Update License * 를 클릭합니다.
7. 라이선스 키 텍스트를 * 라이선스 * 텍스트 상자에 복사합니다.
8. 업데이트(가장 일반적인) * 작업을 선택합니다.
9. 저장 * 을 클릭합니다.
10. Insight 소비 라이선스 모델을 사용하는 경우 * Send usage information * 섹션에서 * Enable susage information to NetApp * 확인란을 선택해야 합니다. 프록시는 환경에 맞게 적절히 구성 및 설정되어 있어야 합니다.

작업을 마친 후

라이선스를 설치한 후 다음 구성 작업을 수행할 수 있습니다.

- 데이터 소스를 구성합니다.
- OnCommand Insight 사용자 계정을 생성합니다.

OnCommand Insight 라이선스

OnCommand Insight는 Insight 서버에서 특정 기능을 활성화하는 라이선스로 작동합니다.

• * 발견 *

Discover는 재고를 지원하는 기본 Insight 라이선스입니다. OnCommand Insight를 사용하려면 Discover 라이선스가 있어야 하며 Discover 라이선스가 최소한 하나의 보증, 수행 또는 계획 라이선스와 페어링되어야 합니다.

• * 보증 *

보증 라이선스는 글로벌 및 SAN 경로 정책, 위반 관리를 비롯한 보증 기능을 지원합니다. 라이선스 보증으로 취약점을 보고 관리할 수도 있습니다.

• * 성능 *

Perform 라이선스는 자산 페이지, 대시보드 위젯, 쿼리 등의 성능 모니터링을 지원할 뿐 아니라 성능 정책 및 위반 사항을 관리합니다.

• * 계획 *

플랜 라이선스는 리소스 사용 및 할당을 비롯한 계획 기능을 지원합니다.

• * 호스트 활용률 팩 *

Host Utilization 라이선스는 호스트 및 가상 머신의 파일 시스템 활용도를 지원합니다.

• * 보고서 작성 *

보고서 작성 라이선스는 보고를 위한 추가 작성자를 지원합니다. 이 라이선스에는 플랜 라이선스가 필요합니다.

OnCommand Insight 모듈은 연간 기간 또는 영구 라이선스됩니다.

- 검색, 보증, 계획, 모듈 수행을 위해 테라바이트별로 모니터링되는 용량을 기준으로 합니다
- 호스트 활용도 팩의 호스트 수 기준
- 보고서 작성을 위해 필요한 Cognos 전문가 집필자 수 기준

라이선스 키는 각 고객에 대해 생성되는 고유한 문자열 집합입니다. OnCommand Insight 담당자에게 라이선스 키를 받을 수 있습니다.

설치된 라이선스는 소프트웨어에서 사용할 수 있는 다음 옵션을 제어합니다.

• * 발견 *

재고 확보 및 관리(기초)

변경 사항을 모니터링하고 인벤토리 정책을 관리합니다

• * 보증 *

SAN 경로 정책 및 위반 사항을 확인하고 관리합니다

취약점을 보고 관리합니다

작업 및 마이그레이션 보기 및 관리

• * 계획 *

요청을 보고 관리합니다

보류 중인 작업을 보고 관리합니다

예약 위반 사항을 보고 관리합니다

포트 균형 위반을 보고 관리합니다

• * 성능 *

대시보드 위젯, 자산 페이지 및 쿼리의 데이터를 비롯한 성능 데이터를 모니터링합니다

성능 정책 및 위반 사항을 확인하고 관리합니다

다음 표에서는 admin 사용자 및 admin이 아닌 사용자에게 대한 Perform 라이선스와 함께 사용할 수 있는 기능에 대한 세부 정보를 제공합니다.

기능(관리자)	Perform 라이선스 사용	Perform 라이선스 없음
응용 프로그램	예	성능 데이터 또는 차트가 없습니다
가상 머신	예	성능 데이터 또는 차트가 없습니다

하이퍼바이저	예	성능 데이터 또는 차트가 없습니다
호스트	예	성능 데이터 또는 차트가 없습니다
데이터 저장소	예	성능 데이터 또는 차트가 없습니다
VMDK입니다	예	성능 데이터 또는 차트가 없습니다
내부 볼륨	예	성능 데이터 또는 차트가 없습니다
볼륨	예	성능 데이터 또는 차트가 없습니다
스토리지 풀	예	성능 데이터 또는 차트가 없습니다
디스크	예	성능 데이터 또는 차트가 없습니다
스토리지	예	성능 데이터 또는 차트가 없습니다
스토리지 노드	예	성능 데이터 또는 차트가 없습니다
패브릭	예	성능 데이터 또는 차트가 없습니다
스위치 포트	예	성능 데이터 또는 차트 없음, "포트 오류"는 "해당 없음"으로 표시됨
스토리지 포트입니다	예	예
NPV 포트입니다	예	성능 데이터 또는 차트가 없습니다
스위치	예	성능 데이터 또는 차트가 없습니다
NPV 전환	예	성능 데이터 또는 차트가 없습니다
Qtree	예	성능 데이터 또는 차트가 없습니다
할당량	예	성능 데이터 또는 차트가 없습니다
경로	예	성능 데이터 또는 차트가 없습니다
Zone(영역)	예	성능 데이터 또는 차트가 없습니다
Zone 멤버	예	성능 데이터 또는 차트가 없습니다

일반 장치	예	성능 데이터 또는 차트가 없습니다
테이프	예	성능 데이터 또는 차트가 없습니다
마스킹	예	성능 데이터 또는 차트가 없습니다
iSCSI 세션	예	성능 데이터 또는 차트가 없습니다
ICSI 네트워크 포털	예	성능 데이터 또는 차트가 없습니다
검색	예	예
관리자	예	예
대시보드	예	예
위젯	예	부분적으로 사용 가능(자산, 쿼리 및 관리 위젯만 사용 가능)
위반 대시보드	예	숨김
자산 대시보드	예	부분적으로 사용 가능(스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)
성능 정책 관리	예	숨김
주석 관리	예	예
주석 규칙을 관리합니다	예	예
애플리케이션 관리	예	예
쿼리	예	예
업무 엔티티를 관리합니다	예	예

피처	사용자 - Perform 라이센스가 있는 경우	게스트 - Perform 라이센스 포함	사용자 - Perform 라이센스가 없습니다	게스트 - Perform 라이센스 없음
자산 대시보드	예	예	부분적으로 사용 가능 (스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)	부분적으로 사용 가능 (스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)

맞춤형 대시보드	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)
성능 정책 관리	예	숨김	숨김	숨김
주석 관리	예	숨김	예	숨김
애플리케이션 관리	예	숨김	예	숨김
업무 엔티티를 관리합니다	예	숨김	예	숨김
쿼리	예	보기 및 편집만(저장 옵션 없음)	예	보기 및 편집만(저장 옵션 없음)

설치 문제 해결

OnCommand Insight 설치하는 일반적으로 설치 마법사를 통해 관리됩니다. 그러나 업그레이드 도중 문제가 발생하거나 컴퓨터 환경으로 인해 충돌이 발생할 수 있습니다.

또한 소프트웨어 설치에 필요한 모든 OnCommand Insight 라이선스를 설치해야 합니다.

라이선스가 없습니다

OnCommand Insight 기능마다 다른 라이선스가 필요합니다. OnCommand Insight에 표시되는 내용은 설치된 라이선스에 의해 제어됩니다. 각 라이선스로 제어되는 기능에 대한 자세한 내용은 OnCommand Insight 라이선스 섹션을 참조하십시오.

각 라이선스로 제어되는 기능에 대한 자세한 내용은 OnCommand Insight 라이선스 섹션을 참조하십시오.

온라인 기술 지원 요청 제출

Insight 설치에 문제가 있는 경우 등록된 지원 고객으로서 온라인 기술 지원 요청을 제출할 수 있습니다.

시작하기 전에

회사 이메일 주소를 사용하여 온라인 지원 서비스를 받으려면 지원 고객으로 등록해야 합니다. 등록은 지원 사이트를 통해 수행됩니다 .

이 작업에 대해

설치 문제 해결에 대한 고객 지원을 지원하려면 다음 항목을 포함하여 가능한 많은 정보를 수집해야 합니다.

- Insight 일련 번호

- 문제에 대한 설명입니다
- 모든 Insight 로그 파일
- 오류 메시지의 화면 캡처

단계

1. 을 생성합니다 .zip 문제 해결 패키지를 만들기 위해 수집한 정보 파일
2. 에서 지원 사이트에 로그인합니다 "mysupport.netapp.com" 을 클릭하고 * 기술 지원 * 을 선택합니다.
3. 케이스 열기 * 를 클릭합니다.
4. 데이터 패키지에 대한 지침을 따르십시오.

작업을 마친 후

기술 지원 페이지의 * 케이스 상태 확인 * 을 사용하여 요청을 추적할 수 있습니다.

OnCommand Insight 업그레이드 중

일반적으로 업그레이드는 모든 Insight 서버(Insight Server, Data Warehouse Server, Remote Acquisition Unit)에서 수행되어야 합니다. OnCommand Insight의 새 릴리스에 대한 업그레이드 요구 사항은 항상 릴리스 노트를 참조하십시오.

다리 명시하지 않는 한, 요구 사항 및 절차는 Insight 7.x에서 Insight의 현재 버전으로 업그레이드하는 데 적용됩니다. 7.0 이전 버전에서 업그레이드하는 경우 계정 담당자에게 문의하십시오.

Insight를 버전 7.3.12 이상으로 업그레이드 - Windows

OnCommand Insight 7.3.10-7.3.11에서 버전 7.3.12 이상으로 업그레이드하기 전에 OCI 데이터 마이그레이션 툴을 실행해야 합니다.

배경

OnCommand Insight 버전 7.3.12 이상은 이전 버전과 호환되지 않을 수 있는 기본 소프트웨어를 사용합니다. Insight 버전 7.3.12 이상에는 업그레이드를 지원하는 * 데이터 마이그레이션 도구 * 가 포함되어 있습니다.



OnCommand Insight 버전 7.3.9 및 이전 버전은 더 이상 지원되지 않습니다. 이러한 버전 중 하나를 실행 중인 경우 7.3.12 이상으로 업그레이드하기 전에 Insight 버전 7.3.10 이상으로 _업그레이드해야 합니다(7.3.11 권장).

데이터 마이그레이션 툴은 어떤 기능을 합니까?

마이그레이션 도구는 초기 호환성 검사를 수행한 다음 세 가지 업그레이드 경로 중 하나를 따릅니다. 선택한 경로는 현재 버전의 데이터 호환성을 기반으로 합니다.



업그레이드하기 전에 데이터 마이그레이션 도구를 실행하고 권장 단계를 수행해야 합니다.

시작하기 전에

- 데이터 마이그레이션 툴을 실행하기 전에 OnCommand Insight 시스템을 백업하는 것이 좋습니다.
- 서버의 Elasticsearch 서비스가 실행 중이어야 합니다.
- Insight를 업그레이드하기 전에 데이터베이스 및 성능 아카이브를 위해 Data Migration Tool_many_be를 실행해야 합니다.

데이터 마이그레이션 툴 실행

1. 최신 버전의 데이터 마이그레이션 도구(예: *SANScreenDataMigrationTool-x86-7.3.12-97.zip*)를 Insight 서버와 해당 Insight 설치 프로그램 파일로 다운로드합니다. 작업 폴더에 압축을 풉니다. 다운로드는 [에서 찾을 수 있습니다](#) "NetApp Support 사이트".
2. 명령 창을 열고 작업 폴더로 이동합니다.
 - Powershell을 관리자로 엽니다.
3. 다음 명령을 사용하여 데이터 마이그레이션 툴을 실행합니다.
 - `_.\SANScreenDataMigrationTool.PS1' _`
4. 필요에 따라 지침을 따릅니다. 다음은 예제입니다.

```
.\SANScreenDataMigrationTool.ps1

NetApp SANScreen Data Migration Tool 7.3.12-121

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory: C:\Program Files\SANscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 54 obsolete indexes. Of these,
    54 indexes may be migrated with OCI server running,
    the most recent of which is for 2021-05-13

Verifying migration component is present...
SANscreen Server service is Running

Proceed with online migration of 54 indexes (y or [n])?:
```

데이터 마이그레이션 도구는 시스템에 사용되지 않는 인덱스가 있는지 확인하고 있는지 보고합니다. 없을 경우 도구가 종료됩니다.

SANscreen 서버 서비스가 실행되는 동안 일부 인덱스가 마이그레이션될 수 있습니다. 다른 서버는 서버가 중지된 경우에만 마이그레이션될 수 있습니다. 마이그레이션할 수 있는 인덱스가 없는 경우 이 도구는 종료됩니다. 그렇지 않으면 메시지가 나타나면 지침을 따릅니다.

데이터 마이그레이션 도구가 완료되면 사용되지 않는 인덱스가 있는지 다시 확인합니다. 모든 인덱스가 마이그레이션된 경우 OnCommand Insight 7.3.12로의 업그레이드가 지원된다는 메시지가 표시됩니다. 이제 Insight 업그레이드를 진행할 수 있습니다.

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-127

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.10 (139) is installed

Getting installation parameters...
Installation Directory: D:\SANSscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
Elasticsearch service is up

Checking for obsolete (version 5) indexes...
Found 5 obsolete indexes. Of these,
    5 indexes need to be migrated with OCI server stopped

Verifying migration component is present...
SANSscreen Server service is Stopped

Proceed with offline migration of 5 indexes (y or [n])?: y
Preparing to perform migration...
Preparing to migrate ociint-inventory-snmp_win2012_host: copied; backup;
delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_interface: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_load_average: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_storage: copied;
backup; delete old; restore new; cleanup; done.
Preparing to migrate ociint-inventory-snmp_win2012_tcp_connection: copied;
backup; delete old; restore new; cleanup; done.
Execution time 0:00:15

Checking for obsolete (version 5) indexes...
No obsolete indexes found. Upgrade to 7.3.12+ is supported.

C:\Users\root\Desktop\SANSscreenDataMigrationTool-x64-7.3.12-127>
```

SANSscreen 서비스를 중지하라는 메시지가 표시되면 Insight를 업그레이드하기 전에 다시 시작합니다.

검증 실패

인덱스 유효성 검사에 실패하는 경우 마이그레이션 도구는 종료하기 전에 문제를 알려 줍니다.

- OnCommand Insight가 없습니다: *

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool V1.0

Checking OnCommand Insight Installation...
ERROR: OnCommand Insight is not installed
```

- 잘못된 Insight 버전: *

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.4 (126) is installed
ERROR: The OCI Data Migration Tool is intended to be run against OCI 7.3.5
- 7.3.11
```

- Elasticsearch 서비스가 실행되고 있지 않습니다: *

```
.\SANSscreenDataMigrationTool.ps1

NetApp SANSscreen Data Migration Tool 7.3.12-105

Checking OnCommand Insight Installation...
OnCommand Insight 7.3.11 (126) is installed

Getting installation parameters...
Installation Directory: C:\Program Files\SANSscreen\
Elasticsearch Rest Port: 9200

Checking Elasticsearch service...
ERROR: The Elasticsearch service is not running

Please start the service and wait for initialization to complete
Then rerun OCI Data Migration Tool
```

명령줄 옵션

데이터 마이그레이션 툴에는 작업에 영향을 주는 몇 가지 선택적 매개 변수가 포함되어 있습니다.

옵션(Windows)	기능
-s	모든 프롬프트를 표시하지 않습니다
-perf_archive 를 입력합니다	<p>지정된 경우 인덱스가 마이그레이션되는 모든 날짜의 기존 아카이브 항목이 교체됩니다. 경로는 아카이브 항목 zip 파일이 포함된 디렉토리를 가리켜야 합니다.</p> <p>업데이트할 성능 아카이브가 없음을 나타내기 위해 '-'의 인수를 지정할 수 있습니다.</p> <p>이 인수가 있으면 아카이브 위치에 대한 프롬프트가 표시되지 않습니다.</p>
확인하십시오	이 경우 인덱스 카운트를 보고한 후 스크립트가 즉시 종료됩니다.
-드라이런	마이그레이션 실행 파일이 있는 경우 데이터 마이그레이션 및 아카이브 항목 업데이트를 위해 수행할 작업은 보고하지만 작업을 수행하지 않습니다.

OnCommand Insight 업그레이드 프로세스 개요

Insight 업그레이드를 시작하기 전에 업그레이드 프로세스를 이해하는 것이 중요합니다. 대부분의 Insight 버전에서 업그레이드 프로세스는 동일합니다.

Insight의 업그레이드 프로세스에는 다음과 같은 상위 작업이 포함됩니다.

- 설치 패키지를 다운로드합니다
- 데이터 웨어하우스 데이터베이스 백업

데이터 보고 오류가 발생하지 않도록 하려면 Insight 데이터베이스를 백업하기 전에 데이터 웨어하우스 데이터베이스를 백업해야 합니다.

- Insight 데이터베이스 백업

데이터 이동 없이 업그레이드를 수행하면 Insight 데이터베이스가 자동으로 백업됩니다. 업그레이드하기 전에 데이터베이스를 백업하고 Insight 서버 이외의 위치에 백업을 배치하는 것이 좋습니다. Insight는 업그레이드 프로세스 중에 새 데이터를 수집하지 않습니다. 수집되지 않은 데이터의 양을 최소화하려면 계획된 업그레이드 시간 중 1시간 또는 2시간 이내에 데이터베이스 백업을 시작해야 합니다.

- 기본 구성에서 구성이 변경된 경우 데이터 웨어하우스 및 원격 획득 장치 보안 구성을 백업합니다.

업그레이드가 완료된 후 데이터 웨어하우스 데이터베이스를 시스템으로 복원하기 전에 기본값이 아닌 보안 구성을 데이터 웨어하우스 및 RAU 서버로 복원해야 합니다.

- 사용자 지정 데이터 웨어하우스 보고서 백업

데이터 웨어하우스 데이터베이스를 백업하는 경우 사용자 정의 보고서가 포함됩니다. 백업 파일은 데이터 웨어하우스 서버에 생성됩니다. 사용자 정의 보고서를 데이터 웨어하우스 서버가 아닌 다른 위치에 백업하는 것이

종습니다.

- 데이터 웨어하우스 및 원격 획득 장치 소프트웨어 제거(해당하는 경우)

Insight 서버에는 현재 위치 업그레이드가 있으므로 소프트웨어를 제거할 필요가 없습니다. 현재 위치 업그레이드는 데이터베이스를 백업하고 소프트웨어를 제거한 다음 새 버전을 설치한 다음 데이터베이스를 복원합니다.

- Insight 서버, 데이터 웨어하우스 및 원격 획득 장치에서 소프트웨어 업그레이드

이전에 적용한 모든 사용권은 레지스트리에 남아 있으므로 이 사용권을 다시 적용할 필요가 없습니다.

- 업그레이드 후 작업 완료

OnCommand Insight 업그레이드 체크리스트

제공된 체크리스트를 사용하여 업그레이드를 준비하는 동안 진행 상황을 기록할 수 있습니다. 이러한 작업은 업그레이드 실패 위험을 완화하고 복구 및 복원 작업을 신속하게 수행하는 데 도움이 됩니다.

업그레이드 준비 체크리스트(필수)

조건	완료?
모든 Insight 서버에서 업그레이드 프로세스를 수행하는 데 필요한 Windows 로컬 관리자 권한이 있는지 확인합니다.	
Insight, Data Warehouse 또는 Remote Acquisition Unit 서버가 32비트 플랫폼에 상주하는 경우 서버를 64비트 플랫폼으로 업그레이드해야 합니다. Insight 7.x는 64비트 플랫폼에서만 업그레이드할 수 있습니다.	
사용자 환경의 모든 서버에서 바이러스 백신 소프트웨어를 수정하거나 비활성화하는 데 필요한 권한이 있는지 확인합니다. 활성 바이러스 검사 소프트웨어로 인한 업그레이드 실패를 방지하려면 Insight 설치 디렉터리를 제외해야 합니다 (disk drive:\install directory\sanscreen 업그레이드 중 바이러스 백신 검사에 액세스할 수 있습니다. 모든 구성 요소를 업그레이드한 후 바이러스 백신 소프트웨어를 안전하게 다시 활성화할 수 있습니다. 그러나 Insight 설치 디렉터리의 모든 내용을 제외하도록 검사를 구성해야 합니다. 또한 설치 후 바이러스 백신 검사에서 IBM/DB2 폴더(예: C:\Program Files\IBM\DB2)를 제외해야 합니다.	

업그레이드 준비 체크리스트(모범 사례)

조건	완료?
----	-----

업그레이드 시기를 계획하십시오. 대부분의 업그레이드는 최소 4~8시간이 소요되고, 대기업은 더 오래 걸립니다. 업그레이드 시간은 사용 가능한 리소스(아키텍처, CPU 및 메모리), 데이터베이스 크기 및 환경에서 모니터링되는 개체의 수에 따라 달라질 수 있습니다.	
업그레이드 계획에 대해 계정 담당자에게 문의하고 설치한 Insight 버전과 업그레이드하려는 버전을 제공하십시오.	
Insight, 데이터 웨어하우스 및 원격 획득 장치에 할당된 현재 리소스가 권장 사양을 충족하는지 확인합니다. 모든 서버에 대한 권장 사이징 지침을 참조하거나 계정 담당자에게 문의하여 사이징 지침을 논의할 수 있습니다.	
데이터베이스 백업 및 복원 프로세스에 충분한 디스크 공간이 있는지 확인합니다. 백업 및 복원 프로세스에는 Insight 및 데이터 웨어하우스 서버의 백업 파일에 사용되는 디스크 공간의 약 5배가 필요합니다. 예를 들어 50GB 백업에는 250GB에서 300GB의 사용 가능한 디스크 공간이 필요합니다.	
Insight 및 Data Warehouse 데이터베이스를 백업할 때 Firefox ® 또는 Chrome ™ 브라우저에 액세스할 수 있는지 확인합니다. 4GB보다 큰 파일을 업로드 및 다운로드할 때 문제가 발생하기 때문에 Internet Explorer는 권장되지 않습니다.	
를 삭제합니다 .tmp 다음 위치에서 찾을 수 있는 Insight 서버의 파일: <install directory>\SANscreen\wildfly\standalone\tmp.	
Insight 클라이언트에서 중복 데이터 소스 및 사용 중지된 데이터 소스를 제거합니다. 사용 중단되거나 중복된 데이터 원본을 제거하면 업그레이드를 수행하는 데 필요한 시간이 줄어들고 데이터 손상 가능성이 줄어듭니다.	
Insight와 함께 제공된 기본 보고서를 수정한 경우 보고서를 다른 이름으로 저장한 다음 고객 보고서 폴더에 저장하여 시스템을 업그레이드 또는 복원할 때 수정된 보고서를 잃지 않도록 해야 합니다.	

<p>사용자나 전문 서비스에서 만든 사용자 지정 또는 수정된 데이터 웨어하우스 보고서가 있는 경우 이를 XML로 내보낸 다음 고객 보고서 폴더로 이동하여 백업을 만듭니다. 백업이 데이터 웨어하우스 서버에 있지 않은지 확인합니다. 보고서를 권장 폴더로 이동하지 않으면 업그레이드 프로세스에서 이러한 보고서가 백업되지 않을 수 있습니다. 이전 버전의 Insight에서 해당 폴더에서 보고서를 찾지 못하면 사용자 지정 보고서와 수정된 보고서가 손실될 수 있습니다.</p>	
<p>IBM Cognos 구성 유틸리티의 모든 설정을 기록합니다. 이러한 설정은 데이터 웨어하우스 백업에 포함되지 않으므로 업그레이드 후에 다시 구성해야 합니다. 이 유틸리티는 에 있습니다 <code>disk drive:\install directory\SANscreen\cognos\c10_64\bin64</code> 데이터 웨어하우스 서버의 디렉터리이며 을 사용하여 실행합니다 <code>cogconfigw</code> 명령. 또는 Cognos의 전체 백업을 수행한 다음 모든 설정을 가져올 수 있습니다. 자세한 내용은 IBM Cognos 설명서를 참조하십시오.</p>	

업그레이드 준비 체크리스트(해당하는 경우)

조건	완료?
<p>브라우저 보안 경고로 인해 Insight 설치가 생성한 자체 서명된 인증서를 내부 인증 기관이 서명한 인증서로 대체한 경우 다음 위치에 있는 키 저장소 파일을 백업합니다. <code>disk drive:\install directory\SANscreen\wildfly\standalone\configuration</code> 업그레이드 후 복원합니다. 이렇게 하면 Insight에서 만든 자체 서명된 인증서가 서명된 인증서와 교체됩니다.</p>	
<p>사용자 환경에서 수정된 데이터 소스가 있고 업그레이드하는 Insight 버전에서 이러한 수정 사항이 사용 가능한지 확실하지 않은 경우 다음 디렉토리의 복사본을 만듭니다. 이 디렉토리는 복구 문제가 있을 경우 문제를 해결하는 데 도움이 됩니다. <code>disk drive:\install directory\SANscreen\wildfly\standalone\deployments\datasources.war</code>.</p>	
<p>를 사용하여 모든 사용자 지정 데이터베이스 테이블 및 뷰를 백업합니다 <code>mysqldump</code> 명령줄 도구. 사용자 지정 데이터베이스 테이블을 복원하려면 권한이 있는 데이터베이스 액세스가 필요합니다. 이러한 테이블 복원에 대한 자세한 내용은 기술 지원 부서에 문의하십시오.</p>	

Insight 데이터 소스, 백업 또는 기타 필수 데이터에 필요한 사용자 지정 통합 스크립트, 타사 구성 요소가 에 저장되지 않도록 합니다 disk drive:\install directory\sanscreen 업그레이드 프로세스에서 이 디렉토리의 내용이 삭제되므로 디렉토리입니다. 이러한 항목을 에서 이동시키십시오 \sanscreen 다른 위치에 디렉토리를 지정합니다. 예를 들어 환경에 사용자 지정 통합 스크립트가 포함되어 있는 경우 다음 파일을 이 아닌 다른 디렉터리에 복사해야 합니다 \sanscreen 디렉터리:

```
\install_dir\SANscreen\wildfly\standalone\deployments\datasources.war\new_disk_models.txt.
```

OnCommand Insight 설치 패키지를 다운로드합니다

업그레이드하기 전에 Insight, Data Warehouse 및 Remote Acquisition Unit(해당되는 경우)에 대한 설치 패키지를 다운로드해야 합니다. 패키지 다운로드 시간 (.msi 파일)은 사용 가능한 대역폭에 따라 다릅니다.

이 작업에 대해

Insight WebUI를 사용하거나 에서 해당 OnCommand Insight 링크로 이동하여 설치 패키지를 다운로드할 수 있습니다 <http://support.netapp.com/NOW/cgi-bin/software>.

Insight 서버 내에서 설치 패키지를 다운로드하려면 다음을 수행합니다.

단계

1. 웹 브라우저를 열고 다음 중 하나를 입력하여 Insight 웹 UI를 엽니다.

- Insight 서버: `https://localhost`
- 모든 위치: `https://IP Address:port or fqdn:port`

포트 번호는 443 또는 Insight 서버를 설치할 때 구성된 포트입니다. URL에 포트 번호를 지정하지 않으면 포트 번호는 443으로 기본 설정됩니다.

2. Insight에 로그인합니다.

3. 도움말 아이콘을 클릭하고 * 업데이트 확인 * 을 선택합니다.

4. 최신 버전이 감지되면 메시지 상자의 지침을 따르십시오.

최신 버전의 InsightDescription 페이지로 이동합니다.

5. 설명 * 페이지에서 * 계속 * 을 클릭합니다.

6. 최종 사용자 사용권 계약(EULA)이 표시되면 * 동의 * 를 클릭합니다.

7. 각 구성 요소(Insight 서버, 데이터 웨어하우스, 원격 획득 장치) 등에 대한 설치 패키지 링크를 클릭하고 * 다른 이름으로 저장 * 을 클릭하여 설치 패키지를 저장합니다.

업그레이드하기 전에 데이터 웨어하우스 및 원격 획득 장치 설치 패키지를 해당 서버에 로컬인 디스크에 복사해야 합니다.

8. checksum * 을 클릭하고 각 설치 패키지와 관련된 숫자 값을 기록합니다.
9. 설치 패키지를 다운로드한 후 오류 없이 설치가 완료되었는지 확인합니다.

파일 전송이 완료되지 않으면 업그레이드 프로세스에 문제가 발생할 수 있습니다.

설치 패키지에 대한 MD5 해시 값을 생성하려면 Microsoft와 같은 타사 유틸리티를 사용하십시오 "[파일 Checksum Integrity Verifier](#)" 유틸리티.

데이터베이스 백업

업그레이드하기 전에 데이터 웨어하우스와 OnCommand Insight 데이터베이스를 모두 백업해야 합니다. 업그레이드를 하려면 나중에 업그레이드 프로세스에서 데이터베이스를 복원할 수 있도록 데이터 웨어하우스 데이터베이스를 백업해야 합니다. Insight의 현재 위치 업그레이드를 통해 데이터베이스를 백업할 수 있지만, 업그레이드 전에 데이터베이스를 백업하는 것이 좋습니다.

데이터가 잘못 보고되지 않도록 하려면 Insight 데이터베이스를 백업하기 전에 데이터 웨어하우스 데이터베이스를 백업해야 합니다. 또한 테스트 환경이 있는 경우 업그레이드를 계속하기 전에 백업을 복원할 수 있는지 확인하는 것이 좋습니다.

데이터 웨어하우스 데이터베이스 백업

Cognos 백업도 포함된 데이터 웨어하우스 데이터베이스를 파일에 백업하고 나중에 데이터 웨어하우스 포털을 사용하여 복원할 수 있습니다. 이러한 백업을 사용하면 다른 데이터 웨어하우스 서버로 마이그레이션하거나 새 데이터 웨어하우스 버전으로 업그레이드할 수 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://fqdn/dwh>.
2. 왼쪽의 탐색 창에서 * 백업/복원 * 을 선택합니다.
3. 백업 * 을 클릭하고 백업 구성을 선택합니다.
 - a. 성능 데이터 마트를 제외한 모든 데이터 마트
 - b. 모든 데이터 마트

이 작업은 30분 이상 소요될 수 있습니다.

+ 데이터 웨어하우스는 백업 파일을 만들고 그 이름을 표시합니다.

4. 백업 파일을 마우스 오른쪽 단추로 클릭하고 원하는 위치에 저장합니다.

파일 이름을 변경하지 않으려는 경우에는 데이터 웨어하우스 설치 경로 외부에 파일을 저장해야 합니다.

데이터 웨어하우스 백업 파일에는 DWH 인스턴스의 MySQL, 사용자 정의 스키마(MySQL DB) 및 테이블, LDAP 구성, Cognos를 MySQL 데이터베이스에 연결하는 데이터 소스(Insight 서버를 데이터를 얻기 위해 장치에

연결하는 데이터 소스 아님)가 포함됩니다. 보고서를 가져오거나 내보낸 작업, 보안 역할, 그룹 및 네임스페이스 보고, 사용자 계정 수정된 보고 포털 보고서 및 내 폴더 디렉토리에서도 저장된 위치에 관계없이 모든 사용자 정의 보고서 SMTP 서버 설정 및 Cognos 사용자 지정 메모리 설정과 같은 Cognos 시스템 구성 매개 변수는 백업되지 않습니다.

사용자 지정 테이블이 백업되는 기본 스키마는 다음과 같습니다.

dWh _ 용량
dWh_capacity_staging
dWh _ 치수
dWh_fs_util
dWh_재고
dWh_inventory_staging
dWh_inventory_transient
dWh _ 관리
더 뛰어난 성능
dWh_performance_staging
dWh_ports
dWh 보고서
dWh_sa_staging

사용자 지정 테이블이 백업에서 제외되는 스키마는 다음과 같습니다.

information_schema를 참조하십시오
획득
CLOUD_MODEL
host_data를 선택합니다

InnoDB
인벤토리
Inventory_private을 선택합니다
Inventory_Time(재고 시간)
로그
관리
MySQL
NAS
성능
performance_schema를 나타냅니다
Performance_views(성능 보기)
SANscreen
스크럽
서비스 보장
테스트
tmp(tmp)
워크벤치

수동으로 시작된 모든 백업에서 는 입니다 .zip 다음 파일이 포함된 파일이 생성됩니다.

- 일일 백업입니다 .zip Cognos 보고서 정의가 포함된 파일
- 가 백업을 보고합니다 .zip 내 폴더 디렉토리의 보고서를 포함하여 Cognos의 모든 보고서가 들어 있는 파일입니다
- 데이터 웨어하우스 데이터베이스 백업 파일 Cognos는 언제든지 수행할 수 있는 수동 백업 외에도 매일 실행되는 백업(라는 파일에 매일 자동으로 생성됨)을 생성합니다 DailyBackup.zip)에 보고서 정의가 포함되어 있습니다. 일일 백업에는 제품과 함께 제공되는 최상위 폴더와 패키지가 포함됩니다. 내 폴더 디렉토리 및 제품의 최상위 폴더 외부에서 생성한 디렉토리는 Cognos 백업에 포함되지 않습니다.



Insight에서 파일 이름을 로 지정하는 방식 때문입니다. .zip 파일, 일부 압축 해제 프로그램은 파일을 열 때 파일이 비어 있음을 표시합니다. 를 누릅니다. .zip 파일의 크기가 0보다 크고 로 끝나지는 않습니다. .bad 내선 번호 .zip 파일이 유효합니다. 7-Zip 또는 WinZip® 과 같은 다른 압축 해제 프로그램으로 파일을 열 수 있습니다.

OnCommand Insight 데이터베이스를 백업하는 중입니다

업그레이드 후 문제가 발생할 경우 Insight 데이터베이스를 백업하여 최근 백업이 있는지 확인합니다. 백업 및 복원 단계에서는 성능 데이터가 수집되지 않으므로 가능한 한 업그레이드 시간에 가깝게 백업이 수행됩니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Admin * > * Troubleshooting * 을 클릭합니다.
3. 문제 해결 * 페이지에서 * 백업 * 을 클릭합니다.

데이터베이스 백업 시간은 사용 가능한 리소스(아키텍처, CPU 및 메모리), 데이터베이스 크기 및 환경에서 모니터링되는 개체의 수에 따라 달라질 수 있습니다.

백업이 완료되면 파일을 다운로드할지 묻는 메시지가 표시됩니다.

4. 백업 파일을 다운로드합니다.

보안 구성 백업

Insight 구성 요소에서 기본값이 아닌 보안 구성을 사용하는 경우 새 소프트웨어를 설치한 후 보안 구성을 백업한 다음 모든 구성 요소에 대한 구성을 복원해야 합니다. 데이터 웨어하우스 데이터베이스 백업을 복원하기 전에 보안 구성을 복원해야 합니다.


이 작업에 대해

를 사용합니다 securityadmin 구성 백업을 생성하고 저장된 구성을 복원하는 도구입니다. 자세한 내용을 보려면 을 검색합니다 securityadmin OnCommand Insight 문서 센터에서: <http://docs.netapp.com/oci-73/index.jsp>

사용자 지정 데이터 웨어하우스 보고서 백업

사용자 정의 보고서를 작성했고 이 없는 경우 .xml 해당 파일의 원본을 만든 다음 업그레이드하기 전에 이 보고서를 백업해야 합니다. 그런 다음 데이터 웨어하우스 서버 이외의 서버로 복사해야 합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://fqdn/dwh>.
2. 데이터 웨어하우스 도구 모음에서 를 클릭합니다  를 눌러 보고 포털을 열고 로그인합니다.
3. 파일 * > * 열기 * 를 선택합니다.

4. 보고서가 있는 폴더를 선택하고 보고서를 선택한 다음 * 열기 * 를 클릭합니다.
5. 도구 * > * 클립보드로 보고서 복사 * 를 선택합니다.
6. 텍스트 편집기를 열고 보고서 내용을 붙여 넣은 다음 파일을 다른 이름으로 저장합니다 report_name.txt, 위치 report _name 보고서 이름입니다.
7. 데이터 웨어하우스 서버 이외의 서버에 보고서를 저장합니다.

소프트웨어 업그레이드 수행

모든 필수 작업을 완료한 후에는 각 서버에서 해당 설치 패키지를 다운로드하여 실행하여 모든 Insight 구성 요소를 새 릴리스로 업그레이드할 수 있습니다.

Insight 업그레이드

모든 필수 작업을 완료한 후 Insight 서버에 로그인하여 설치 패키지를 실행하여 업그레이드를 완료합니다. 업그레이드 프로세스는 기존 소프트웨어를 제거하고 새 소프트웨어를 설치한 다음 서버를 재부팅합니다.

시작하기 전에

Insight 설치 패키지는 서버에 있어야 합니다.

단계

1. Windows 로컬 관리자 권한이 있는 계정을 사용하여 Insight 서버에 로그인합니다.
2. Insight 설치 패키지를 찾습니다 (SANscreenServer-x64-version_number-build_number.msi)
Windows 탐색기를 사용하여 두 번 클릭합니다.

OnCommand InsightSetup 마법사가 표시됩니다.

3. 생성된 모든 오류가 보기에서 숨겨지지 않도록 화면 중앙에서 * Setup * 마법사 창 밖으로 진행률 창을 이동합니다.
4. 설정 마법사의 지시를 따릅니다.

모든 기본값을 그대로 두는 것이 가장 좋습니다.

작업을 마친 후

업그레이드가 성공했는지 또는 오류가 생성되었는지 확인하려면 다음 위치에서 업그레이드 로그를 확인하십시오.
<install directory>\SANscreen\wildfly\standalone\log.

데이터 웨어하우스 업그레이드 중

모든 필수 작업을 완료한 후 데이터 웨어하우스 서버에 로그인하여 설치 패키지를 실행하여 업그레이드를 완료할 수 있습니다.

이 작업에 대해

DWH(데이터 웨어하우스)에서는 인라인 업그레이드를 지원하지 않습니다. DWH 소프트웨어의 새 버전으로

업그레이드하려면 다음 단계를 수행하십시오.

DWH를 업그레이드하면 _SecurityAdmin_tool 볼트 백업이 포함된 폴더가 삭제됩니다. DWH를 업그레이드하기 전에 볼트를 백업하는 것이 좋습니다. 참조의 경우 기본 볼트 폴더는 다음과 같습니다.



- 볼트 폴더 (사용 중인 볼트)
):%SANSSCREEN_HOME%\wildfly\standalone\configuration\vault
- 볼트 백업: %SANSSCREEN_HOME%\backup\vault

을 참조하십시오 "데이터 웨어하우스의 보안 관리" 를 참조하십시오.

단계

1. Windows 로컬 관리자 권한이 있는 계정을 사용하여 DWH 서버에 로그인합니다.
2. DWH 포털 인터페이스를 사용하여 DWH DB 및 보고서를 백업합니다.
3. 서버가 기본값이 아닌 보안 구성을 사용하는 경우 보안 구성을 백업합니다.
4. 서버에서 DWH 소프트웨어를 제거합니다.
5. 메모리를 구성 요소 제거하기 위해 서버를 재부팅합니다.
6. 새 버전의 DWH를 서버에 설치합니다.

설치 시간은 약 2시간입니다. 모든 기본값을 그대로 두는 것이 가장 좋습니다.

7. 기본이 아닌 보안 구성을 DWH 서버로 복원합니다.
8. DWH 데이터베이스를 서버로 복원합니다.

작업을 마친 후

업그레이드 후 데이터 웨어하우스 데이터베이스를 복원해야 합니다. 이 데이터베이스는 업그레이드보다 오래 또는 오래 걸릴 수 있습니다.



OnCommand Insight 업그레이드 중에 고객이 다른 Insight 서버로 전환하는 경우가 드물지 않게 있습니다. Insight 서버를 변경한 경우 데이터 웨어하우스 데이터베이스를 복원하면 기존 커넥터가 이전 서버 IP 주소 또는 호스트 이름을 가리킵니다. 오류가 발생하지 않도록 커넥터를 삭제하고 새 커넥터를 작성하는 것이 가장 좋습니다.

데이터 웨어하우스 업그레이드 중에 사용자 정의 Cognos 설정 유지

기본 SMTP 전자 메일 설정이 아닌 사용자 지정 Cognos 설정은 데이터 웨어하우스 업그레이드의 일부로 자동으로 백업되지 않습니다. 업그레이드 후 사용자 지정 설정을 수동으로 문서화한 다음 복원해야 합니다.

데이터 웨어하우스를 업그레이드하기 전에 보존하려는 사용자 지정 Cognos 설정이 포함된 체크리스트를 준비하고 시스템을 업그레이드하기 전에 목록을 검토하십시오. 업그레이드가 완료된 후 값을 수동으로 복원하여 원래 구성의 설정으로 되돌릴 수 있습니다.

보안 구성 백업

Insight 환경에서 기본이 아닌 보안 구성을 사용하는 경우 새 소프트웨어를 설치한 후 보안 구성을 백업한 다음 보안 구성을 복원해야 합니다. 데이터 웨어하우스 데이터베이스 백업을 복원하기 전에 보안 구성을 복원해야 합니다.

이 작업에 대해

를 사용합니다 securityadmin 구성 백업을 생성하고 저장된 구성을 복원하는 도구입니다. 자세한 내용을 보려면 을 검색합니다 securityadmin OnCommand Insight 문서 센터에서: <http://docs.netapp.com/oci-73/index.jsp>

원격 획득 장치 서버 업그레이드

모든 필수 작업을 완료한 후 원격 획득 장치 서버에 로그인하여 설치 패키지를 실행하여 업그레이드를 완료할 수 있습니다. 사용자 환경의 모든 원격 획득 서버에서 이 작업을 수행해야 합니다.

시작하기 전에

- OnCommand Insight를 업그레이드해야 합니다.
- OnCommand Insight 설치 패키지는 서버에 있어야 합니다.

단계

1. Windows 로컬 관리자 권한이 있는 계정을 사용하여 원격 획득 장치 서버에 로그인합니다.
2. Insight 설치 패키지를 찾습니다 (RAU-x64-version_number-build_number.msi) Windows 탐색기를 사용하여 두 번 클릭합니다.

OnCommand Insight 설치 마법사가 표시됩니다.

3. 생성된 모든 오류가 보기에서 숨겨지지 않도록 설치 마법사 진행률 창을 화면 중앙에서 멀리 이동하고 설치 마법사 창에서 멀리 이동합니다.
4. 설치 마법사의 지시를 따릅니다.

모든 기본값을 그대로 두는 것이 가장 좋습니다.

작업을 마친 후

- 업그레이드가 성공했는지 또는 오류가 생성되었는지 확인하려면 다음 위치에서 업그레이드 로그를 확인하십시오.
<install directory>\SANscreen\bin\log.

- 를 사용합니다 securityadmin 저장된 보안을 복원하는 도구입니다

구성. 자세한 내용은 OnCommand Insight에서 SecurityAdmin을 검색하십시오

문서 센터: <http://docs.netapp.com/oci-73/index.jsp>

- 브라우저의 캐시 및 기록을 지워 서버에서 최신 데이터를 수신하고 있는지 확인합니다.

업그레이드 후 작업 완료

최신 버전의 Insight로 업그레이드한 후에는 추가 작업을 완료해야 합니다.

데이터 소스 패치를 설치하는 중입니다

해당되는 경우 데이터 원본에 사용할 수 있는 최신 패치를 설치하여 최신 기능과 향상된 기능을 활용해야 합니다. 데이터 원본 패치를 업로드한 후에는 같은 형식의 모든 데이터 원본에 설치할 수 있습니다.

시작하기 전에

기술 지원에 연락하여 을(를) 받아야 합니다. .zip 업그레이드할 버전과 업그레이드할 버전을 제공하여 최신 데이터 소스 패치를 포함하는 파일입니다.

단계

1. Insight 서버에 패치 파일을 저장합니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 패치 * 를 클릭합니다.
4. 작업 버튼에서 * 패치 적용 * 을 선택합니다.
5. 데이터 원본 패치 적용 * 대화 상자에서 * 찾아보기 * 를 클릭하여 업로드된 패치 파일을 찾습니다.
6. 패치 이름 *, * 설명 * 및 * 영향받는 데이터 소스 유형 * 을 검토하십시오.
7. 선택한 패치가 올바르면 * 패치 적용 * 을 클릭합니다.

동일한 유형의 모든 데이터 소스가 이 패치로 업데이트됩니다. Insight는 데이터 소스를 추가할 때 자동으로 획득을 다시 시작하도록 합니다. 검색에는 노드나 인터페이스의 추가 또는 삭제를 포함하여 네트워크 토폴로지의 변경 사항이 감지됩니다.

8. 검색 프로세스를 수동으로 강제로 처리하려면 * 데이터 소스 * 를 클릭하고 데이터 소스 옆에 있는 * 다시 폴링 * 을 클릭하여 데이터를 즉시 수집하도록 합니다.

데이터 소스가 이미 획득 프로세스에 있는 경우 Insight는 폴링 요청을 다시 무시합니다.

OnCommand Insight를 업그레이드한 후 인증서 교체

업그레이드 후 OnCommand Insight 웹 UI를 열면 인증 경고가 표시됩니다. 업그레이드 후 유효한 자체 서명된 인증서를 사용할 수 없기 때문에 경고 메시지가 표시됩니다. 나중에 경고 메시지가 표시되지 않도록 하려면 유효한 자체 서명된 인증서를 설치하여 원래 인증서를 대체할 수 있습니다.

시작하기 전에

시스템은 최소 암호화 비트 수준(1024비트)을 충족해야 합니다.

이 작업에 대해

인증 경고는 시스템 사용성에 영향을 주지 않습니다. 메시지 프롬프트에서 위험을 이해하고 있음을 표시한 다음 Insight를 계속 사용할 수 있습니다.

단계

1. 키 저장소의 내용을 나열합니다. `C:\Program Files\SANscreen\java64\bin>keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

암호를 묻는 메시지가 나타나면 를 입력합니다 `changeit`.

키 저장소에 인증서가 하나 이상 있어야 합니다. `ssl certificate`.

2. 를 삭제합니다 `ssl certificate: keytool -delete -alias ssl certificate -keystore c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore`

3. 새 키 생성: `keytool -genkey -alias OCI.hostname.com -keyalg RSA -keysize 2048 -keystore "c:\ProgramFiles\SANscreen\wildfly\standalone\configuration\server.keystore"`

a. 성과 이름을 묻는 메시지가 나타나면 사용하려는 FQDN(정규화된 도메인 이름)을 입력합니다.

b. 조직 및 조직 구조에 대한 다음 정보를 제공합니다.

- 국가: 해당 국가의 두 글자 ISO 약어(예: US)
- 시/도: 조직의 본사 소재지가 위치한 시/도의 이름(예: 매사추세츠주)
- 지역: 조직의 본사 소재지(예: Waltham)의 이름입니다.
- 조직 이름: 도메인 이름을 소유한 조직의 이름(예: NetApp)
- 조직 단위 이름: 인증서를 사용할 부서 또는 그룹의 이름(예: 지원)
- 도메인 이름/일반 이름: 서버의 DNS 조회에 사용되는 FQDN(예: `www.example.com`) 시스템이 다음과 유사한 정보로 응답합니다. `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`

c. 를 입력합니다 `Yes` CN(Common Name)이 FQDN과 같은 경우

d. 키 암호를 묻는 메시지가 나타나면 암호를 입력하거나 Enter 키를 눌러 기존 키 저장소 암호를 사용합니다.

4. 인증서 요청 파일 생성: `keytool -certreq -alias localhost -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

를 클릭합니다 `c:\localhost.csr` file 은 새로 생성된 인증서 요청 파일입니다.

5. 를 제출합니다 `c:\localhost.csr` 승인을 위해 인증 기관(CA)에 파일을 첨부합니다.

인증서 요청 파일이 승인되면 에서 인증서를 반환하도록 합니다. `.der` 형식. 파일이 로 반환될 수도 있고 반환되지 않을 수도 있습니다. `.der` 파일. 기본 파일 형식은 입니다. `.cer` Microsoft CA 서비스의 경우.

6. 승인된 인증서 가져오기: `keytool -importcert -alias localhost -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

- a. 암호를 묻는 메시지가 나타나면 키 저장소 암호를 입력합니다.

다음과 같은 메시지가 표시됩니다. Certificate reply was installed in keystore

7. SANscreen 서버 서비스를 다시 시작합니다.

결과

웹 브라우저가 더 이상 인증서 경고를 보고하지 않습니다.

Cognos 메모리 증가

데이터 웨어하우스 데이터베이스를 복원하기 전에 Cognos에 대한 Java 할당을 768MB에서 2048MB로 늘려 보고서 생성 시간을 줄여야 합니다.


단계

1. 데이터 웨어하우스 서버에서 관리자 권한으로 명령 프롬프트 창을 엽니다.
2. 로 이동합니다 disk drive:\install directory\SANscreen\cognos\c10_64\bin64 디렉토리.
3. 다음 명령을 입력합니다. cogconfigw



IBM Cognos 구성 창이 표시됩니다.



IBM Cognos 구성 바로 가기 응용 프로그램은 를 가리킵니다 disk drive:\Program Files\SANscreen\cognos\c10_64\bin64\cognosconfigw.bat. 프로그램 파일(공간 없음) 디렉터리 대신 기본값인 프로그램 파일(간격) 디렉터리에 Insight가 설치되어 있는 경우 를 사용합니다 .bat 파일이 작동하지 않습니다. 이 경우 응용 프로그램 바로 가기를 마우스 오른쪽 단추로 클릭하고 변경합니다 cognosconfigw.bat 를 선택합니다 cognosconfig.exe 바로 가기를 수정합니다.

4. 왼쪽의 탐색 창에서 * 환경 * 을 확장하고 * IBM Cognos 서비스 * 를 확장한 다음 * IBM Cognos * 를 클릭합니다.
5. Tomcat의 최대 메모리(MB) * 를 선택하고 768 MB에서 2048 MB로 변경합니다.
6. IBM Cognos 구성 도구 모음에서 를 클릭합니다  (저장).

Cognos가 수행 중인 작업을 알려주는 정보 메시지가 표시됩니다.

7. 닫기 * 를 클릭합니다.
8. IBM Cognos 구성 도구 모음에서 를 클릭합니다  (중지).
9. IBM Cognos 구성 도구 모음에서 를 클릭합니다  (시작).

데이터 웨어하우스 데이터베이스 복원

데이터 웨어하우스 데이터베이스를 백업할 때 데이터 웨어하우스는 을 작성합니다 .zip 나중에 동일한 데이터베이스를 복원하는 데 사용할 수 있는 파일입니다.

이 작업에 대해

데이터 웨어하우스 데이터베이스를 복원할 때 백업에서 사용자 계정 정보도 복원할 수 있습니다. 사용자 관리 테이블은 데이터 웨어하우스 보고서 엔진이 데이터 웨어하우스 전용 설치에서 사용됩니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://fqdn/dwh>.
2. 왼쪽의 탐색 창에서 * 백업/복원 * 을 클릭합니다.
3. Restore Database and Reports * 섹션에서 * Browse * 를 클릭하고 를 찾습니다 .zip 데이터 웨어하우스 백업을 보관하는 파일입니다.
4. 다음 옵션을 모두 선택한 상태로 두는 것이 좋습니다.

- * 데이터베이스 복원 *

데이터 웨어하우스 설정, 데이터 매트, 연결 및 사용자 계정 정보가 포함됩니다.

- * 보고서 복원 *

사용자 지정 보고서, 미리 디자인된 보고서, 사용자가 만든 미리 디자인된 보고서의 변경 내용 및 보고 연결에서 수행한 보고 설정이 포함됩니다.

5. 복원 * 을 클릭합니다.

복원 상태를 벗어나지 마십시오. 이렇게 하면 복구 상태가 더 이상 표시되지 않으며 복원 작업이 완료되면 아무런 표시가 나타나지 않습니다.

6. 업그레이드 프로세스를 확인하려면 를 참조하십시오 `dwh_upgrade.log` 다음 위치에 있는 파일: `<install directory>\SANSscreen\wildfly\standalone\log`.

복원 프로세스가 완료되면 * Restore * 버튼 바로 아래에 메시지가 나타납니다. 복원 프로세스가 성공적으로 완료되면 성공 메시지가 표시됩니다. 복원 프로세스가 실패하면 이 메시지는 실패의 원인이 된 특정 예외를 나타냅니다. 이 경우 기술 지원 부서에 연락하여 지원을 요청하십시오 `dwh_upgrade.log` 파일. 예외가 발생하고 복원 작업이 실패하면 원래 데이터베이스가 자동으로 재설정됩니다.




""COGnos 콘텐츠 저장소 업그레이드 실패" 메시지와 함께 복구 작업이 실패하면 데이터 웨어하우스 데이터베이스를 보고서 없이 복원하고(데이터베이스만 해당) XML 보고서 백업을 사용하여 보고서를 가져옵니다.

사용자 지정 데이터 웨어하우스 보고서 복원

해당하는 경우 업그레이드 전에 백업한 사용자 지정 보고서를 수동으로 복원할 수 있지만 손상된 경우 보고서를 분실했을 경우에만 복원할 수 있습니다.

단계

1. 텍스트 편집기로 보고서를 연 다음 해당 내용을 선택하여 복사합니다.
2. 에서 보고 포털에 로그인합니다 <https://fqdn/reporting>.
3. 데이터 웨어하우스 도구 모음에서 를 클릭합니다  Insight Reporting 포털을 엽니다.

4. 시작 메뉴에서 * Report Studio * 를 선택합니다.

5. 패키지를 선택합니다.

Report Studio가 표시됩니다.

6. Create new * 를 클릭합니다.

7. 목록 * 을 선택합니다.

8. 도구 메뉴에서 * 클립보드에서 보고서 열기 * 를 선택합니다.

클립보드에서 보고서 열기 * 대화 상자가 표시됩니다.

9. 파일 메뉴에서 * 다른 이름으로 저장 * 을 선택하고 보고서를 사용자 정의 보고서 폴더에 저장합니다.

10. 보고서를 열어서 가져왔는지 확인합니다.

각 보고서에 대해 이 작업을 반복합니다.




보고서를 로드할 때 ""표현식 구문 분석 오류""가 나타날 수 있습니다. 즉, 쿼리에 존재하지 않는 하나 이상의 개체에 대한 참조가 포함되어 있습니다. 즉, 소스 창에서 보고서를 검증하는 데 사용할 패키지가 선택되지 않았음을 의미합니다. 이 경우 소스 창에서 데이터 마트 차원을 마우스 오른쪽 단추로 클릭하고 보고서 패키지를 선택합니다. 그런 다음 보고서와 연결된 패키지를 선택하여(예: 인벤토리 보고서인 경우 인벤토리 패키지, 성능 보고서인 경우 성능 패키지 중 하나) Report Studio에서 유효성을 검사한 다음 저장할 수 있습니다.

데이터 웨어하우스에 기간별 데이터가 있는지 검증


사용자 지정 보고서를 복원한 후에는 사용자 지정 보고서를 확인하여 데이터 웨어하우스에서 기간별 데이터를 수집하고 있는지 확인해야 합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://fqdn/dwh>.

2. 데이터 웨어하우스 도구 모음에서 를 클릭합니다  Insight Reporting 포털을 열고 로그인합니다.

3. 사용자 지정 보고서(예: 사용자 지정 보고서)가 들어 있는 폴더를 엽니다.

4. 을 클릭합니다  이 보고서의 출력 형식 옵션을 엽니다.

5. 원하는 옵션을 선택하고 * Run * 을 클릭하여 스토리지, 컴퓨팅 및 스위치 내역 데이터가 채워졌는지 확인합니다.

성능 아카이브 복원 중

성능 아카이빙을 수행하는 시스템의 경우 업그레이드 프로세스에서는 7일간의 아카이브 데이터만 복원합니다. 업그레이드가 완료된 후 나머지 아카이브 데이터를 복구할 수 있습니다.

이 작업에 대해

성능 아카이브를 복원하려면 다음 단계를 수행하십시오.

단계

1. 도구 모음에서 * Admin * > * Troubleshooting * 을 클릭합니다
2. 복원 섹션의 * 성능 아카이브 로드 * 에서 * 로드 * 를 클릭합니다.

아카이브 로딩은 백그라운드에서 처리됩니다. 매일 아카이빙된 성능 데이터가 Insight에 채워지면 전체 아카이브를 로드하는 데 시간이 오래 걸릴 수 있습니다. 아카이브 로드 상태가 이 페이지의 아카이브 섹션에 표시됩니다.

커넥터를 테스트합니다

업그레이드 후 커넥터를 테스트하여 OnCommand Insight 데이터 웨어하우스에서 OnCommand Insight 서버로 연결되었는지 확인합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://fqdn/dwh>.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.
3. 첫 번째 커넥터를 선택합니다.

커넥터 편집 페이지가 표시됩니다.

4. Test * 를 클릭합니다.
5. 테스트가 성공적으로 완료되면 * Close * 를 클릭합니다. 실패하면 * Name * 필드에 Insight 서버의 이름과 * Host * 필드에 해당 IP 주소를 입력하고 * Test * 를 클릭합니다.
6. 데이터 웨어하우스와 Insight 서버가 성공적으로 연결되면 * 저장 * 을 클릭합니다.

성공하지 못하면 연결 구성을 확인하고 Insight 서버에 문제가 없는지 확인합니다.

7. Test * 를 클릭합니다.

데이터 웨어하우스가 연결을 테스트합니다.

추출, 변환 및 로드 일정 계획 확인

업그레이드 후에는 ETL(Extract, Transform, Load) 프로세스에서 OnCommand Insight 데이터베이스에서 데이터를 검색하고 데이터를 변환하며 데이터 마트에 저장해야 합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://fqdn/dwh>.
2. 왼쪽의 탐색 창에서 * Schedule * 을 클릭합니다.
3. 일정 편집 * 을 클릭합니다.
4. Type * 목록에서 * Daily * 또는 * Weekly * 를 선택합니다.

하루에 한 번 ETL을 실행하도록 예약하는 것이 좋습니다.

5. 선택한 시간이 작업을 실행할 시간인지 확인합니다.

이렇게 하면 빌드 작업이 자동으로 실행됩니다.

6. 저장 * 을 클릭합니다.

디스크 모델을 업데이트하는 중입니다

업그레이드 후에는 업데이트된 디스크 모델이 있어야 합니다. 그러나 어떤 이유로 Insight에서 새 디스크 모델을 검색하지 못한 경우 수동으로 업데이트할 수 있습니다.

시작하기 전에

기술 지원 에서 을(를) 받아야 합니다 .zip 최신 데이터 소스 패치가 포함된 파일입니다.

단계

1. SANscreen Acq 서비스를 중지합니다.
2. 다음 디렉토리로 이동합니다. <install directory>\SANscreen\wildfly\standalone\deployments\datasources.war.
3. 전류를 이동합니다 diskmodels.jar 파일을 다른 위치에 저장합니다.
4. 새 을 복사합니다 diskmodels.jar 에 파일을 넣습니다 datasources.war 디렉토리.
5. SANscreen Acq 서비스를 시작합니다.

비즈니스 인텔리전스 툴이 실행 중인지 확인

해당되는 경우, 업그레이드 후 비즈니스 인텔리전스 도구가 실행 중인지, 그리고 데이터를 검색하는지 확인해야 합니다.

BMC Atrium 및 ServiceNow와 같은 비즈니스 인텔리전스 도구가 실행되고 있고 데이터를 검색할 수 있는지 확인합니다. 여기에는 REST를 활용하는 BMC 커넥터와 솔루션이 포함됩니다.

업그레이드 문제 해결

OnCommand Insight 업그레이드 후 문제가 발생할 경우 몇 가지 가능한 문제와 관련된 문제 해결 정보를 검토하는 것이 좋습니다.

Windows 시작 메뉴에서 **Cognos**를 시작할 수 없습니다

앞에 공백이 있습니다 \SANscreen\cognos 경로 이름에 문제가 있습니다. 자세한 내용은 NetApp 고객 성공 커뮤니티에서 다음 내용을 참조하십시오. <https://forums.netapp.com/thread/62721>.

""유효하지 않은 Win32 응용 프로그램"" 오류 메시지

이것은 Microsoft Windows의 문제입니다. 이 문제를 해결하려면 레지스트리의 이미지 경로 주위에 따옴표를 입력해야 합니다. 자세한 내용은 다음 설명서를 참조하십시오. <https://support.microsoft.com/en-us/kb/812486/en-us>.

주석이 없습니다

데이터 웨어하우스 ETL 작업이 Insight 인스턴스의 주석을 쿼리하면 경우에 따라 빈 응답(0 결과)이 오류로 수신되기도

합니다. 이 오류는 데이터 웨어하우스의 ""현재" 및 ""존재하지 않음"" 상태 사이에서 특정 개체가 앞뒤로 이동하는 주석을 만듭니다. 자세한 내용은 다음을 참조하십시오. <https://forums.netapp.com/docs/DOC-44167>

보고서에 표시되는 값의 차이

7.0 이전에는 보고서가 정수 기반이었습니다. 이 값은 이제 10진수이므로 업그레이드한 후 값이 표시되는 방식이 증가하거나 감소하는 것을 확인할 수 있습니다.

데이터가 보고서에 표시되지 않습니다

7.0.1에서는 여러 모델 이름이 변경되었습니다(예: Symmetrix가 Symmetrix VMAX로 변경됨). 따라서 보고서에 'Symmetrix metrix' 필터가 포함되어 있으면 보고서를 실행할 때 데이터가 표시되지 않습니다. 보고서를 변경하려면 Report Studio에서 쿼리 탐색기 로 보고서를 열고 모델 이름을 검색하고 새 모델 이름으로 바꾸고 보고서를 저장해야 합니다.

소프트웨어 제거

새 버전을 설치하려면 데이터 웨어하우스 및 원격 획득 소프트웨어의 이전 버전을 제거해야 합니다. 이러한 구성 요소를 업그레이드하기 전에 이 작업을 수행해야 합니다. Insight 서버의 소프트웨어는 데이터 이동 없이 업그레이드하는 동안 제거됩니다.

OnCommand Insight 서버 제거

필요한 경우 OnCommand Insight 서버를 제거할 수 있습니다.

시작하기 전에

모범 사례: Insight를 제거하기 전에 OnCommand Insight 데이터베이스를 백업하십시오.

단계

1. 관리자 권한이 있는 계정을 사용하여 OnCommand Insight 서버에 로그인합니다.
2. 서버의 모든 Insight 창을 닫았는지 확인합니다.
3. 제어판에서 프로그램 제거 * 기능을 열고 제거할 OnCommand Insight 응용 프로그램을 선택합니다.
4. 제거 * 를 클릭하고 화면의 지시를 따릅니다.

데이터 웨어하우스 소프트웨어 제거

업그레이드하기 전에 데이터 웨어하우스 소프트웨어를 제거해야 합니다.

시작하기 전에

보관하려는 보고서를 변경한 경우 데이터 웨어하우스를 제거하기 전에 백업을 생성하는 것이 중요합니다. Data Warehouse를 제거하면 이전에 수집된 모든 데이터가 영구적으로 삭제되며 새로 생성되거나 편집된 보고서를 비롯한 모든 보고서가 제거됩니다.

단계

1. 데이터 웨어하우스 서버에 로그인합니다.
2. 서버의 모든 Insight 창을 닫았는지 확인합니다.
3. 제어판을 사용하여 제거하려면:
 - a. 제어판에서 프로그램 제거 * 를 열고 제거할 OnCommand Insight 응용 프로그램을 선택합니다. 제거 * 를 클릭하고 화면의 지시를 따릅니다.
 - b. 제거할 IBM DB2 애플리케이션을 선택합니다. 제거 * 를 클릭하고 화면의 지시를 따릅니다.
 - c. DB2 설치 폴더(예: *C:\Program Files\IBM\DB2*)를 삭제하여 DB2 데이터베이스를 완전히 제거합니다.
4. 제공된 스크립트를 사용하여 제거하려면 다음을 수행하십시오.
 - a. <download location>\OCI_dWh_uninstall_폴더로 이동하고 _INSTALL_OCI_dWh.bat_script를 실행합니다.
5. 서버를 재부팅합니다.

원격 획득 장치 소프트웨어 제거

새 버전으로 업그레이드하려면 기존 버전의 원격 획득 장치 소프트웨어를 제거해야 합니다. 사용자 환경의 모든 원격 획득 장치 서버에서 이 작업을 수행해야 합니다.

단계

1. 원격 획득 장치 서버에 로그인합니다.
2. 서버의 모든 OnCommand Insight 창이 닫혀 있는지 확인합니다.
3. 제어판에서 * 프로그램 제거 * 기능을 열고 제거할 OnCommand Insight 원격 획득 장치 프로그램을 선택합니다.
4. 제거 * 를 클릭하고 화면의 지시를 따릅니다.

구성 및 관리

Insight 설정

Insight를 설정하려면 Insight 라이선스를 활성화하고, 데이터 소스를 설정하고, 사용자와 알림을 정의하고, 백업을 설정하고, 필요한 고급 구성 단계를 수행해야 합니다.

OnCommand Insight 시스템을 설치한 후 다음 설치 작업을 수행해야 합니다.

- Insight 라이선스를 설치합니다.
- Insight에서 데이터 소스 설정
- 사용자 계정을 설정합니다.
- 이메일을 구성합니다.
- 필요한 경우 SNMP, e-메일 또는 syslog 알림을 정의합니다.
- Insight 데이터베이스의 주별 자동 백업을 설정합니다.
- 주석 및 임계값 정의를 포함하여 필요한 고급 구성 단계를 수행합니다.

웹 UI 액세스

OnCommand Insight를 설치한 후에는 라이선스를 설치한 다음 환경을 모니터링할 Insight를 설정해야 합니다. 웹 브라우저를 사용하여 Insight 웹 UI에 액세스하면 됩니다.

단계

1. 다음 중 하나를 수행합니다.

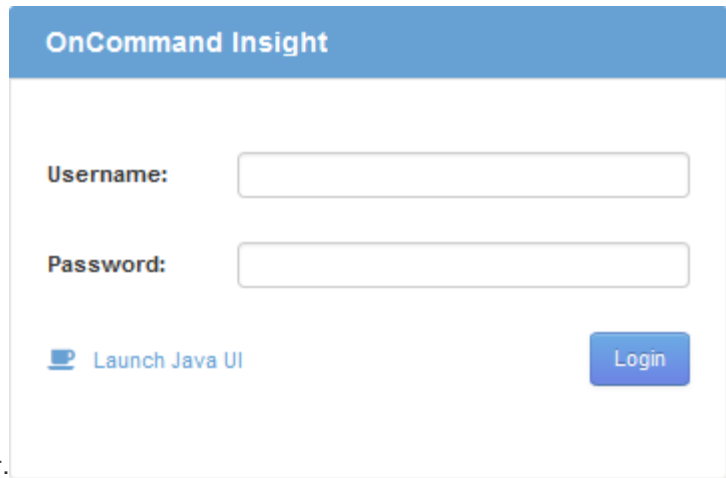
- Insight 서버에 대한 Insight를 엽니다.

`https://fqdn`

- 다른 위치에서 Insight 열기:

`https://fqdn:port`

포트 번호는 Insight 서버를 설치할 때 구성된 443 또는 다른 포트입니다. URL에서 포트 번호를 지정하지 않으면 포트 번호는 443으로 기본 설정됩니다.



The image shows the OnCommand Insight login page. It has a blue header with the text 'OnCommand Insight'. Below the header, there are two input fields: 'Username:' and 'Password:'. To the right of the 'Password:' field is a blue button labeled 'Login'. Below the input fields, there is a link that says 'Launch Java UI' with a small icon of a laptop.

OnCommand Insight 대화 상자가 표시됩니다.

2. 사용자 이름과 암호를 입력하고 * 로그인 * 을 클릭합니다.

라이센스가 설치된 경우 데이터 소스 설정 페이지가 표시됩니다.



30분 동안 비활성 상태인 Insight 브라우저 세션이 시간 초과되고 시스템에서 자동으로 로그아웃됩니다. 보안 강화를 위해 Insight에서 로그아웃한 후 브라우저를 닫는 것이 좋습니다.

Insight 라이선스 설치

NetApp의 Insight 라이선스 키가 포함된 라이선스 파일을 받으면 설정 기능을 사용하여 모든 라이선스를 동시에 설치할 수 있습니다.

이 작업에 대해

Insight 라이선스 키는 에 저장됩니다 .txt 또는 .lcn 파일.

단계

1. 텍스트 편집기에서 라이선스 파일을 열고 텍스트를 복사합니다.
2. 브라우저에서 Insight를 엽니다.
3. Insight 도구 모음에서 * Admin * 을 클릭합니다.
4. 설정 * 을 클릭합니다.
5. Licenses * 탭을 클릭합니다.
6. Update License * 를 클릭합니다.
7. 라이선스 키 텍스트를 * 라이선스 * 텍스트 상자에 복사합니다.
8. 업데이트(가장 일반적인) * 작업을 선택합니다.
9. 저장 * 을 클릭합니다.
10. Insight 소비 라이선스 모델을 사용하는 경우 * Send usage information * 섹션에서 * Enable susage information to NetApp * 확인란을 선택해야 합니다. 프로키는 환경에 맞게 적절히 구성 및 설정되어 있어야 합니다.

작업을 마친 후

라이센스를 설치한 후 다음 구성 작업을 수행할 수 있습니다.

- 데이터 소스를 구성합니다.
- OnCommand Insight 사용자 계정을 생성합니다.

OnCommand Insight 라이선스

OnCommand Insight는 Insight 서버에서 특정 기능을 활성화하는 라이선스로 작동합니다.

• * 발견 *

Discover는 재고를 지원하는 기본 Insight 라이선스입니다. OnCommand Insight를 사용하려면 Discover 라이선스가 있어야 하며 Discover 라이선스가 최소한 하나의 보증, 수행 또는 계획 라이선스와 페어링되어야 합니다.

• * 보증 *

보증 라이선스는 글로벌 및 SAN 경로 정책, 위반 관리를 비롯한 보증 기능을 지원합니다. 라이선스 보증으로 취약점을 보고 관리할 수도 있습니다.

• * 성능 *

Perform 라이선스는 자산 페이지, 대시보드 위젯, 쿼리 등의 성능 모니터링을 지원할 뿐 아니라 성능 정책 및 위반 사항을 관리합니다.

• * 계획 *

플랜 라이선스는 리소스 사용 및 할당을 비롯한 계획 기능을 지원합니다.

• * 호스트 활용률 팩 *

Host Utilization 라이선스는 호스트 및 가상 머신의 파일 시스템 활용도를 지원합니다.

• * 보고서 작성 *

보고서 작성 라이선스는 보고를 위한 추가 작성자를 지원합니다. 이 라이선스에는 플랜 라이선스가 필요합니다.

OnCommand Insight 모듈은 연간 기간 또는 영구 라이선스됩니다.

- 검색, 보증, 계획, 모듈 수행을 위해 테라바이트별로 모니터링되는 용량을 기준으로 합니다
- 호스트 활용도 팩의 호스트 수 기준
- 보고서 작성을 위해 필요한 Cognos 전문가 집필자 수 기준

라이선스 키는 각 고객에 대해 생성되는 고유한 문자열 집합입니다. OnCommand Insight 담당자에게 라이선스 키를 받을 수 있습니다.

설치된 라이선스는 소프트웨어에서 사용할 수 있는 다음 옵션을 제어합니다.

• * 발견 *

재고 확보 및 관리(기초)

변경 사항을 모니터링하고 인벤토리 정책을 관리합니다

• * 보증 *

SAN 경로 정책 및 위반 사항을 확인하고 관리합니다

취약점을 보고 관리합니다

작업 및 마이그레이션 보기 및 관리

• * 계획 *

요청을 보고 관리합니다

보류 중인 작업을 보고 관리합니다

예약 위반 사항을 보고 관리합니다

포트 균형 위반을 보고 관리합니다

• * 성능 *

대시보드 위젯, 자산 페이지 및 쿼리의 데이터를 비롯한 성능 데이터를 모니터링합니다

성능 정책 및 위반 사항을 확인하고 관리합니다

다음 표에서는 admin 사용자 및 admin이 아닌 사용자에게 대한 Perform 라이선스와 함께 사용할 수 있는 기능에 대한 세부 정보를 제공합니다.

기능(관리자)	Perform 라이선스 사용	Perform 라이선스 없음
응용 프로그램	예	성능 데이터 또는 차트가 없습니다
가상 머신	예	성능 데이터 또는 차트가 없습니다
하이퍼바이저	예	성능 데이터 또는 차트가 없습니다
호스트	예	성능 데이터 또는 차트가 없습니다
데이터 저장소	예	성능 데이터 또는 차트가 없습니다
VMDK입니다	예	성능 데이터 또는 차트가 없습니다
내부 볼륨	예	성능 데이터 또는 차트가 없습니다
볼륨	예	성능 데이터 또는 차트가 없습니다

스토리지 풀	예	성능 데이터 또는 차트가 없습니다
디스크	예	성능 데이터 또는 차트가 없습니다
스토리지	예	성능 데이터 또는 차트가 없습니다
스토리지 노드	예	성능 데이터 또는 차트가 없습니다
패브릭	예	성능 데이터 또는 차트가 없습니다
스위치 포트	예	성능 데이터 또는 차트 없음, "포트 오류"는 "해당 없음"으로 표시됨
스토리지 포트입니다	예	예
NPV 포트입니다	예	성능 데이터 또는 차트가 없습니다
스위치	예	성능 데이터 또는 차트가 없습니다
NPV 전환	예	성능 데이터 또는 차트가 없습니다
Qtree	예	성능 데이터 또는 차트가 없습니다
할당량	예	성능 데이터 또는 차트가 없습니다
경로	예	성능 데이터 또는 차트가 없습니다
Zone(영역)	예	성능 데이터 또는 차트가 없습니다
Zone 멤버	예	성능 데이터 또는 차트가 없습니다
일반 장치	예	성능 데이터 또는 차트가 없습니다
테이프	예	성능 데이터 또는 차트가 없습니다
마스킹	예	성능 데이터 또는 차트가 없습니다
iSCSI 세션	예	성능 데이터 또는 차트가 없습니다
ICSI 네트워크 포털	예	성능 데이터 또는 차트가 없습니다
검색	예	예

관리자	예	예
대시보드	예	예
위젯	예	부분적으로 사용 가능(자산, 쿼리 및 관리 위젯만 사용 가능)
위반 대시보드	예	숨김
자산 대시보드	예	부분적으로 사용 가능(스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)
성능 정책 관리	예	숨김
주석 관리	예	예
주석 규칙을 관리합니다	예	예
애플리케이션 관리	예	예
쿼리	예	예
업무 엔티티를 관리합니다	예	예

피쳐	사용자 - Perform 라이선스가 있는 경우	게스트 - Perform 라이선스 포함	사용자 - Perform 라이선스가 없습니다	게스트 - Perform 라이선스 없음
자산 대시보드	예	예	부분적으로 사용 가능 (스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)	부분적으로 사용 가능 (스토리지 IOPS 및 VM IOPS 위젯이 숨겨짐)
맞춤형 대시보드	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)	보기 전용(만들기, 편집 또는 저장 옵션 없음)
성능 정책 관리	예	숨김	숨김	숨김
주석 관리	예	숨김	예	숨김
애플리케이션 관리	예	숨김	예	숨김
업무 엔티티를 관리합니다	예	숨김	예	숨김

쿼리	예	보기 및 편집만(저장 옵션 없음)	예	보기 및 편집만(저장 옵션 없음)
----	---	--------------------	---	--------------------

사용자 계정 설정 및 관리

사용자 계정, 사용자 인증 및 사용자 인증은 Microsoft Active Directory(버전 2 또는 3) LDAP(Lightweight Directory Access Protocol) 서버 또는 내부 OnCommand Insight 사용자 데이터베이스의 두 가지 방법 중 하나로 정의 및 관리할 수 있습니다. 각 사용자에게 대해 다른 사용자 계정을 만들면 액세스 권한, 개인 기본 설정 및 책임을 제어할 수 있습니다. 이 작업에 대한 관리자 권한이 있는 계정을 사용합니다.

시작하기 전에

다음 작업을 완료해야 합니다.

- OnCommand Insight 라이선스를 설치합니다.
- 각 사용자에게 대해 고유한 사용자 이름을 할당합니다.
- 사용할 암호를 결정합니다.
- 올바른 사용자 역할을 할당합니다.



관리자가 비 관리자/표준 사용자의 대화형 로그인을 방지하도록 호스트 운영 체제를 구성하는 것이 보안 모범 사례입니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 탭을 선택합니다.
5. 새 사용자를 생성하려면 * Actions * 버튼을 클릭하고 * Add user * 를 선택합니다.
이름 *, * 암호 *, * 이메일 * 주소를 입력하고 관리자, 사용자 또는 게스트로 * 역할 * 사용자 중 하나를 선택합니다.
6. 사용자 정보를 변경하려면 목록에서 사용자를 선택하고 사용자 설명 오른쪽에 있는 * 사용자 계정 편집 * 기호를 클릭합니다.
7. OnCommand Insight 시스템에서 사용자를 제거하려면 목록에서 사용자를 선택하고 사용자 설명 오른쪽에 있는 * 사용자 계정 삭제 * 를 클릭합니다.

결과

사용자가 OnCommand Insight에 로그인하면 LDAP가 활성화된 경우 서버에서 먼저 LDAP를 통해 인증을 시도합니다. OnCommand Insight가 LDAP 서버에서 사용자를 찾을 수 없는 경우 로컬 Insight 데이터베이스에서 검색합니다.

Insight 사용자 역할

각 사용자 계정에는 세 가지 가능한 권한 수준 중 하나가 할당됩니다.

- 게스트는 Insight에 로그인하고 다양한 페이지를 볼 수 있도록 허용합니다.
- 사용자는 모든 게스트 수준 권한을 허용하며 정책 정의 및 일반 장치 식별과 같은 Insight 작업에 액세스할 수 있습니다. 사용자 계정 유형에서는 데이터 원본 작업을 수행하거나 사용자 계정이 아닌 다른 사용자 계정을 추가 또는 편집할 수 없습니다.
- 관리자는 새 사용자 추가 및 데이터 원본 관리를 포함하여 모든 작업을 수행할 수 있도록 허용합니다.
- 모범 사례: * 사용자 또는 게스트에 대한 대부분의 계정을 만들어 관리자 권한이 있는 사용자의 수를 제한합니다.

LDAP에 대한 Insight 구성

OnCommand Insight는 회사 LDAP 도메인에서 구성되므로 LDAP(Lightweight Directory Access Protocol) 설정으로 구성해야 합니다.

LDAP 또는 보안 LDAP(LDAPS)와 함께 사용하도록 Insight를 구성하기 전에 회사 환경의 Active Directory 구성을 기록해 두십시오. Insight 설정은 조직의 LDAP 도메인 구성에 있는 설정과 일치해야 합니다. LDAP와 함께 사용하도록 Insight를 구성하기 전에 아래 개념을 검토하고 LDAP 도메인 관리자에게 해당 환경에서 사용할 수 있는 적절한 속성을 확인하십시오.

모든 보안 Active Directory(예: LDAPS) 사용자의 경우 인증서에 정의된 대로 AD 서버 이름을 정확히 사용해야 합니다. 보안 AD 로그인에 IP 주소를 사용할 수 없습니다.



OnCommand Insight는 Microsoft Active Directory 서버 또는 Azure AD를 통해 LDAP 및 LDAPS를 지원합니다. 추가 LDAP 구현은 작동할 수 있지만 Insight에서 검증되지 않았습니다. 이 가이드의 절차에서는 Microsoft Active Directory 버전 2 또는 3 LDAP(Lightweight Directory Access Protocol)를 사용하고 있다고 가정합니다.

- 사용자 기본 이름 속성: *

LDAP 사용자 기본 이름 속성(userPrincipalName)은 Insight에서 사용자 이름 속성으로 사용하는 속성입니다. 사용자 주체 이름은 AD(Active Directory) 포리스트에서 전역적으로 고유하도록 보장되지만 많은 대규모 조직에서 사용자의 주 이름이 즉시 분명하지 않거나 알려지지 않을 수 있습니다. 조직에서 기본 사용자 이름에 사용자 기본 이름 속성 대신 을 사용할 수 있습니다.

다음은 User Principal Name 속성 필드에 대한 몇 가지 대체 값입니다.

- * sAMAccountName *

이 사용자 속성은 기존 Windows 2000 NT 이전 사용자 이름입니다. 대부분의 사용자가 개인 Windows 시스템에 로그인하는 데 익숙합니다. 이는 AD 포리스트 전체에서 전체적으로 고유한 것으로 보장되지는 않습니다.



sAMAccountName은 User Principal Name 속성에 대해 대/소문자를 구분합니다.

- 메일 *

MS Exchange가 있는 AD 환경에서는 이 속성이 최종 사용자의 기본 이메일 주소입니다. 이는 해당 userPrincipalName 특성과 달리 AD 포리스트 전체에서 전역적으로 고유해야 하며 최종 사용자에게 익숙한 것이어야 합니다. 대부분의 비 MS Exchange 환경에는 메일 특성이 없습니다.

• * 조회 *

LDAP 호출은 요청된 개체의 복사본이 없거나 더 정확하게는 클라이언트 응용 프로그램에 대한 도메인 컨트롤러의 표시 방식입니다. 실제로 존재하는 경우 해당 개체가 될 디렉터리 트리의 섹션을 보유하지 않고 클라이언트에 개체를 보관할 수 있는 위치를 제공합니다. 클라이언트는 도메인 컨트롤러에 대한 DNS 검색 기준으로 조회를 사용합니다. 가장 이상적인 방법은 항상 개체를 포함하는 도메인 컨트롤러를 참조하는 것입니다. 그러나 참조된 도메인 컨트롤러가 다른 조회를 생성할 수는 있지만 일반적으로 개체가 존재하지 않는다는 사실을 발견하고 클라이언트에 알리는 데 시간이 오래 걸리지는 않습니다.



sAMAccountName은 일반적으로 User Principal Name 보다 선호됩니다. sAMAccountName은 도메인에서 고유하지만(도메인 포리스트에서는 고유하지 않을 수 있음) 일반적으로 로그인에 사용하는 문자열 도메인 사용자입니다(예: *NetApp\username*). 고유 이름은 포리스트의 고유 이름이지만 일반적으로 사용자가 알 수 없습니다.



동일한 도메인의 Windows 시스템 부분에서 항상 명령 프롬프트를 열고 set 을 입력하여 적절한 도메인 이름(USERDOMAIN=)을 찾을 수 있습니다. 그러면 OCI 로그인 이름이 가 됩니다
USERDOMAIN\sAMAccountName.

도메인 이름 * mydomain.x.y.z.com * 에 를 사용합니다 DC=x, DC=y, DC=z, DC=com Insight의 Domain 필드

• 포트 *:

LDAP의 기본 포트는 389이고 LDAPS의 기본 포트는 636입니다

LDAPS의 일반 URL: ldaps://<ldap_server_host_name>:636

로그 위치: \\<install_directory>\SANSscreen\wildfly\standalone\log\ldap.log

기본적으로 Insight는 다음 필드에 표시된 값을 예상합니다. Active Directory 환경에서 이러한 변경 사항이 발생할 경우 Insight LDAP 구성에서 변경해야 합니다.

역할 속성
멤버
메일 속성입니다
메일
고유 이름 특성입니다
DistinguishedName입니다
불합격
를 따릅니다

그룹: *

OnCommand Insight 및 DWH 서버에서 서로 다른 액세스 역할을 가진 사용자를 인증하려면 Active Directory에서 그룹을 만들고 OnCommand Insight 및 DWH 서버에 해당 그룹 이름을 입력해야 합니다. 아래 그룹 이름은 예제일 뿐이며 Insight에서 LDAP에 대해 구성하는 이름은 Active Directory 환경에 대해 설정된 이름과 일치해야 합니다.

Insight Group	예
Insight 서버 관리자 그룹	insight.server.admins
Insight administrators 그룹	Insight.admins입니다
Insight 사용자 그룹	insight.users
Insight Guest 그룹	Insight.게스트
보고 관리자 그룹	Insight.report.admins입니다
보고 전문가 저자 그룹	insight.report.proauthors
보고 작성자 그룹	insight.report.business.authors
보고 소비자 그룹	Insight.report.business.consumer 를 참조하십시오
보고 받는 사람 그룹	Insight.report.수신자

LDAP를 사용하여 사용자 정의 구성

LDAP 서버에서 사용자 인증 및 승인을 위해 OnCommand Insight(OCI)를 구성하려면 OnCommand Insight 서버 관리자로 LDAP 서버에 정의되어 있어야 합니다.

시작하기 전에

LDAP 도메인에서 Insight에 대해 구성된 사용자 및 그룹 속성을 알아야 합니다.

모든 보안 Active Directory(예: LDAPS) 사용자의 경우 인증서에 정의된 대로 AD 서버 이름을 정확히 사용해야 합니다. 보안 AD 로그인에 IP 주소를 사용할 수 없습니다.

이 작업에 대해

OnCommand Insight는 Microsoft Active Directory 서버를 통해 LDAP 및 LDAPS를 지원합니다. 추가 LDAP 구현은 작동할 수 있지만 Insight에서 검증되지 않았습니다. 이 절차에서는 Microsoft Active Directory 버전 2 또는 3 LDAP(Lightweight Directory Access Protocol)를 사용하고 있다고 가정합니다.

LDAP 사용자는 * Admin * > menu:Setup [Users](설정 [사용자]) 목록에 로컬로 정의된 사용자와 함께 표시됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 설정 * 을 클릭합니다.
3. 사용자 * 탭을 클릭합니다.
4. 여기에 표시된 것처럼 LDAP 섹션으로 스크롤합니다.

LDAP

LDAP integration enables authentication of users via LDAP (or ActiveDirectory). This is done by assigning these users to LDAP groups. The groups are used to identify the user permissions.

☒ Enable LDAP

Please provide credentials for a user authorized for directory lookup queries.

LDAP servers:

User:

Password:

[Show more](#) ▼

5. LDAP 사용자 인증 및 권한 부여를 허용하려면 * LDAP 활성화 * 를 클릭합니다.
6. 다음 필드에 내용을 입력합니다.

- LDAP servers: Insight는 쉼표로 구분된 LDAP URL 목록을 허용합니다. Insight는 LDAP 프로토콜의 유효성을 검사하지 않고 제공된 URL에 연결을 시도합니다.



LDAP 인증서를 가져오려면 * Certificates * 를 클릭하고 인증서 파일을 자동으로 가져오거나 수동으로 찾습니다.

LDAP 서버를 식별하는 데 사용되는 IP 주소 또는 DNS 이름은 일반적으로 다음 형식으로 입력됩니다.

```
ldap://<ldap-server-address>:port
```

또는 기본 포트를 사용하는 경우:

```
ldap://<ldap-server-address>
```

+

이 필드에 여러 LDAP 서버를 입력할 때 각 항목에 올바른 포트 번호가 사용되는지 확인하십시오.

- User name: LDAP 서버에서 디렉터리 조회 쿼리에 대해 승인된 사용자의 자격 증명을 입력합니다.
- Password: 위 사용자의 암호를 입력합니다. LDAP 서버에서 이 암호를 확인하려면 * Validate * 를

클릭합니다.

7. 이 LDAP 사용자를 보다 정확하게 정의하려면 * 더 보기 * 를 클릭하고 나열된 속성의 필드를 채웁니다.

이러한 설정은 LDAP 도메인에 구성된 속성과 일치해야 합니다. 이러한 필드에 입력할 값이 확실하지 않으면 Active Directory 관리자에게 문의하십시오.

◦ * Admins 그룹 *

Insight Administrator 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.admins`.

◦ * 사용자 그룹 *

Insight 사용자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.users`.

◦ * 손님 그룹 *

Insight 게스트 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.guests`.

◦ * 서버 관리자 그룹 *

Insight Server 관리자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.server.admins`.

◦ * 시간 초과 *

시간 초과 전에 LDAP 서버의 응답을 기다리는 시간(밀리초)입니다. 기본값은 2,000이며, 모든 경우에 적절하며 수정할 수 없습니다.

◦ * 도메인 *

OnCommand Insight가 LDAP 사용자를 찾기 시작해야 하는 LDAP 노드입니다. 일반적으로 조직의 최상위 도메인입니다. 예를 들면 다음과 같습니다.

```
DC=<enterprise>,DC=com
```

◦ * 사용자 기본 이름 속성 *

LDAP 서버의 각 사용자를 식별하는 속성입니다. 기본값은 `userPrincipalName`입니다. 이는 세계적으로 고유한 기능입니다. OnCommand Insight는 이 특성의 내용과 위에서 제공한 사용자 이름을 일치시킵니다.

◦ * 역할 속성 *

지정된 그룹 내에서 사용자의 맞춤을 식별하는 LDAP 속성입니다. 기본값은 `memberOf`.

◦ * 메일 속성 *

사용자의 이메일 주소를 식별하는 LDAP 속성입니다. 기본값은 `mail`. 이 기능은 OnCommand Insight에서 제공하는 보고서를 구독하려는 경우에 유용합니다. Insight는 각 사용자가 처음 로그인할 때 사용자의 이메일 주소를 선택하며, 그 후에는 이를 찾아보지 않습니다.



LDAP 서버에서 사용자의 이메일 주소가 변경되면 Insight에서 업데이트해야 합니다.

◦ * 고유 이름 특성 *

사용자의 고유 이름을 식별하는 LDAP 속성입니다. 기본값은 `distinguishedName`.

8. 저장 * 을 클릭합니다.

사용자 암호 변경

관리자 권한이 있는 사용자는 로컬 서버에 정의된 OnCommand Insight 사용자 계정의 암호를 변경할 수 있습니다.

시작하기 전에

다음 항목을 완료해야 합니다.

- 수정하려는 사용자 계정에 로그인하는 모든 사용자에게 알림.
- 이 변경 후 사용할 새 암호입니다.

이 작업에 대해

이 방법을 사용할 때는 LDAP를 통해 유효성이 검증된 사용자의 암호를 변경할 수 없습니다.

단계

1. 관리자 권한으로 로그인합니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 * 탭을 클릭합니다.
5. 수정할 사용자 계정이 표시된 행을 찾습니다.
6. 사용자 정보 오른쪽에서 * 사용자 계정 편집 * 을 클릭합니다.
7. 새 * 암호 * 를 입력한 다음 확인 필드에 다시 입력합니다.
8. 저장 * 을 클릭합니다.

사용자 정의 편집

관리자 권한이 있는 사용자는 사용자 계정을 편집하여 OnCommand Insight 또는 DWH 및 보고 기능의 이메일 주소 또는 역할을 변경할 수 있습니다.

시작하기 전에

변경해야 하는 사용자 계정 유형(OnCommand Insight, DWH 또는 조합)을 확인합니다.

이 작업에 대해

LDAP 사용자의 경우 이 방법을 사용해서만 이메일 주소를 수정할 수 있습니다.

단계

1. 관리자 권한으로 로그인합니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 * 탭을 클릭합니다.
5. 수정할 사용자 계정이 표시된 행을 찾습니다.
6. 사용자 정보 오른쪽에서 * 사용자 계정 편집 * 아이콘을 클릭합니다.
7. 필요한 사항을 변경합니다.
8. 저장 * 을 클릭합니다.

사용자 계정을 삭제하는 중입니다

관리자 권한이 있는 사용자는 사용자 계정을 더 이상 사용하지 않을 때(로컬 사용자 정의용) 삭제하거나 사용자가 다음에 로그인할 때(LDAP 사용자의 경우) OnCommand Insight에서 사용자 정보를 다시 검색하도록 할 수 있습니다.

단계

1. 관리자 권한으로 OnCommand Insight에 로그인합니다.
2. Insight 도구 모음에서 * Admin * 을 클릭합니다.
3. 설정 * 을 클릭합니다.
4. 사용자 * 탭을 클릭합니다.
5. 삭제할 사용자 계정을 표시하는 행을 찾습니다.
6. 사용자 정보 오른쪽에서 * 사용자 계정 삭제 * " * x * " 아이콘을 클릭합니다.
7. 저장 * 을 클릭합니다.

로그인 경고 메시지 설정

OnCommand Insight를 사용하면 관리자가 사용자가 로그인할 때 표시되는 사용자 지정 텍스트 메시지를 설정할 수 있습니다.

단계

1. OnCommand Insight 서버에서 메시지를 설정하려면 다음을 수행하십시오.
 - a. 관리 [문제 해결 > 고급 문제 해결 > 고급 설정] 메뉴로 이동합니다.
 - b. 텍스트 영역에 로그인 메시지를 입력합니다.
 - c. 클라이언트 디스플레이 로그인 경고 메시지 * 확인란을 클릭합니다.

d. 저장 * 을 클릭합니다.

모든 사용자에게 대해 로그인할 때 메시지가 표시됩니다.

2. DWH(Data Warehouse) 및 Cognos(Reporting)에서 메시지를 설정하려면

a. 시스템 정보 * 로 이동하여 * 로그인 경고 * 탭을 클릭합니다.

b. 텍스트 영역에 로그인 메시지를 입력합니다.

c. 저장 * 을 클릭합니다.

이 메시지는 모든 사용자의 DWH 및 Cognos 보고 로그인에 표시됩니다.

Insight Security 를 참조하십시오

OnCommand Insight 7.3.1에서는 향상된 보안으로 Insight 환경을 운영할 수 있는 보안 기능이 도입되었습니다. 암호화, 암호 해싱의 개선, 암호를 암호화하고 해독하는 내부 사용자 암호 및 키 쌍 변경 기능이 포함되어 있습니다. Insight 환경의 모든 서버에서 이러한 기능을 관리할 수 있습니다.

Insight의 기본 설치에는 사용자 환경의 모든 사이트에서 동일한 키와 동일한 기본 암호를 공유하는 보안 구성이 포함됩니다. 중요 데이터를 보호하려면 설치 또는 업그레이드 후에 기본 키와 취득 사용자 암호를 변경하는 것이 좋습니다.

데이터 소스 암호화된 암호는 Insight Server 데이터베이스에 저장됩니다. 서버에 공개 키가 있으며 사용자가 WebUI 데이터 소스 구성 페이지에 암호를 입력할 때 암호를 암호화합니다. 서버에 Server 데이터베이스에 저장된 데이터 소스 암호를 해독하는 데 필요한 개인 키가 없습니다. 획득 장치(Lau, RAU)만 데이터 소스 암호를 해독하는 데 필요한 데이터 소스 개인 키를 가지고 있습니다.

서버 키를 다시 입력합니다

기본 키를 사용하면 환경에 보안 취약점이 발생합니다. 기본적으로 데이터 소스 암호는 Insight 데이터베이스에 암호화됩니다. 모든 Insight 설치에 공통적으로 사용되는 키를 사용하여 암호화됩니다. 기본 구성에서 NetApp에 전송된 Insight 데이터베이스에는 이론적으로 NetApp에 의해 암호 해독될 수 있는 암호가 포함되어 있습니다.

획득 사용자 암호 변경

기본 '획득' 사용자 암호를 사용하면 환경에 보안 취약점이 발생합니다. 모든 획득 장치는 ""획득" 사용자를 사용하여 서버와 통신합니다. 기본 암호가 있는 RA는 이론적으로 기본 암호를 사용하여 모든 Insight 서버에 연결할 수 있습니다.

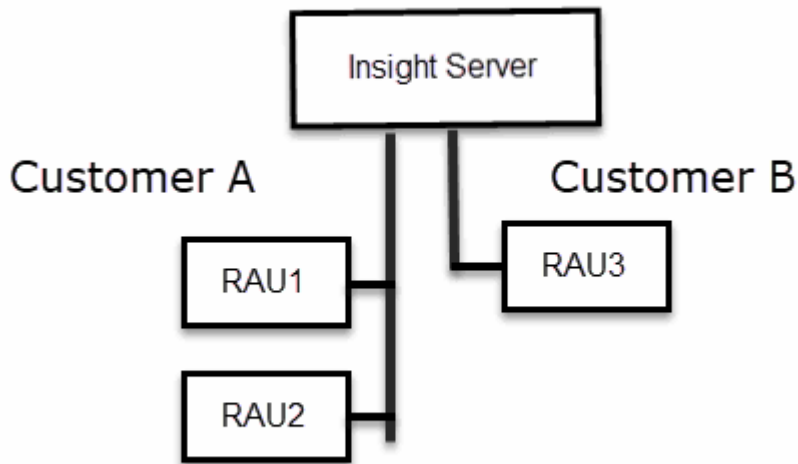
업그레이드 및 설치 고려 사항

Insight 시스템에 기본 보안 구성이 아닌 구성(암호 키를 다시 입력하거나 변경한 경우)이 포함된 경우 보안 구성을 백업해야 합니다. 새 소프트웨어를 설치하거나 소프트웨어를 업그레이드하는 경우 시스템을 기본 보안 구성으로 되돌립니다. 시스템이 기본 구성으로 복원되면 시스템이 올바르게 작동하려면 기본이 아닌 구성을 복원해야 합니다.

복잡한 서비스 공급자 환경에서 키 관리

서비스 공급자는 데이터를 수집하는 여러 OnCommand Insight 고객을 호스팅할 수 있습니다. 이 키는 Insight 서버의 여러 고객이 무단으로 고객 데이터에 액세스하지 못하도록 보호합니다. 각 고객의 데이터는 특정 키 쌍으로 보호됩니다.

이 Insight 구현은 다음 그림과 같이 구성할 수 있습니다.



이 구성에서는 각 고객에 대해 개별 키를 생성해야 합니다. 고객 A는 두 RA 모두에 대해 동일한 키를 필요로 합니다. 고객 B에는 단일 키 세트가 필요합니다.

고객 A의 암호화 키를 변경하는 단계:

1. RAU1을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.
5. RAU2를 호스팅하는 서버에 원격 로그인을 수행합니다.
6. 보안 구성의 백업 zip 파일을 RAU2에 복사합니다.
7. 보안 관리 도구를 시작합니다.
8. 보안 백업을 RAU1에서 현재 서버로 복원합니다.

고객 B의 암호화 키를 변경하는 단계:

1. RAU3을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.

Insight 서버의 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 Insight 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 암호 변경, 새 키 생성, 사용자가 만든 보안 구성 저장 및 복원, 기본

설정으로 구성 복원 등이 포함됩니다.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

단계

1. Insight 서버에 원격 로그인을 수행합니다.

2. 대화형 모드에서 보안 관리 도구를 시작합니다.

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
- Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명에 있는 계정의 사용자 이름과 암호를 입력합니다.

4. 서버 * 를 선택합니다.

다음 서버 구성 옵션을 사용할 수 있습니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 서버 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

프록시 사용자 암호, SMTP 사용자 암호, LDAP 사용자 암호 등을 암호화 또는 해독하는 데 사용되는 서버 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

Insight에서 사용하는 내부 계정의 암호를 변경합니다. 다음 옵션이 표시됩니다.

- _내부
- 획득
- Cognos_admin
- DWh _ 내부
- 호스트
- 인벤토리
- 루트



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

• * 기본값으로 재설정 *

키와 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

• * 종료 *

를 종료합니다 securityadmin 도구.

a. 변경할 옵션을 선택하고 화면의 지시를 따릅니다.

로컬 획득 장치의 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 로컬 획득 사용자(Lau)의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 키 및 암호 관리, 사용자가 만들고 복원한 보안 구성을 기본 설정으로 저장 및 복원하는 작업이 포함됩니다.

시작하기 전에

이(가) 있어야 합니다 admin 보안 구성 작업을 수행할 수 있는 권한.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

단계

1. Insight 서버에 원격 로그인을 수행합니다.

2. 대화형 모드에서 보안 관리 도구를 시작합니다.

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
- Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.
4. Local Acquisition Unit(로컬 획득 장치) * 을 선택하여 Local Acquisition Unit(로컬 획득 장치) 보안 구성을 재구성합니다.

다음 옵션이 표시됩니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원을 사용하여 여러 서버의 패스워드와 키를 동기화할 수 있습니다. 예를 들어: - Lau에서 암호화 키 변경 - 볼트 백업 작성 - 각 RA에 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

장치 암호를 암호화 또는 해독하는 데 사용되는 AU 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

'촬영' 사용자 계정의 암호를 변경합니다.



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 기본값으로 재설정 *

획득 사용자 암호 및 획득 사용자 암호화 키를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

5. 구성할 옵션을 선택하고 화면의 지시를 따릅니다.

RAU에 대한 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 RA의 보안 옵션을 관리할 수 있습니다. 볼트 구성을 백업 또는 복원하거나 암호화 키를 변경하거나 획득 장치의 암호를 업데이트해야 할 수 있습니다.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

Lau, RAU에 대한 보안 구성을 업데이트하는 한 가지 시나리오는 해당 사용자의 암호가 서버에서 변경된 경우 'acquisition' 사용자 암호를 업데이트하는 것입니다. 모든 RA와 Lau는 서버 '획득' 사용자의 암호와 동일한 암호를 사용하여 서버와 통신합니다.

'acquisition' 사용자는 Insight 서버에만 있습니다. RAU 또는 Lau는 서버에 연결할 때 해당 사용자로 로그인합니다.

RAU에서 보안 옵션을 관리하려면 다음 단계를 따르십시오.

단계

1. RAU를 실행 중인 서버에 원격 로그인을 수행한다
2. 대화형 모드에서 보안 관리 도구를 시작합니다.

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
- Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

RAU에 대한 메뉴가 표시됩니다.

- * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

- * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

단말기 암호를 암호화 또는 해독하는 데 사용되는 RAU 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

'촬영' 사용자 계정의 암호를 변경합니다.



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 기본값으로 재설정 *

암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

데이터 웨어하우스의 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 데이터 웨어하우스 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 DWH 서버의 내부 사용자에 대한 내부 암호 업데이트, 보안 구성 백업 생성 또는 기본 설정으로 구성 복원이 포함됩니다.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

단계

1. 데이터 웨어하우스 서버에 원격 로그인을 수행합니다.
2. 대화형 모드에서 보안 관리 도구를 시작합니다.

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
- Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

데이터 웨어하우스에 대한 보안 관리 메뉴가 표시됩니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다
를 누릅니다

◦ * 암호화 키 변경 *

커넥터 암호 및 SMTP 암호와 같은 암호를 암호화 또는 해독하는 데 사용되는 DWH 암호화 키를 변경합니다.

◦ * 암호 업데이트 *

특정 사용자 계정의 암호를 변경합니다.

- _내부
- 획득
- Cognos_admin
- 드Wh
- DWh _ 내부
- Dwhuser(사용자)
- 호스트
- 인벤토리
- 루트



dwhuser, hosts, inventory 또는 root 암호를 변경하면 SHA-256 암호 해싱을 사용할 수 있습니다. 이 옵션을 사용하려면 계정에 액세스하는 모든 클라이언트가 SSL 연결을 사용해야 합니다.

+

◦ * 기본값으로 재설정 *

암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

OnCommand Insight 내부 사용자 암호 변경

보안 정책에 따라 OnCommand Insight 환경의 암호를 변경해야 할 수 있습니다. 한 서버의 암호 중 일부는 환경의 다른 서버에 있으므로 두 서버의 암호를 변경해야 합니다. 예를 들어, Insight Server에서 ""인벤토리"" 사용자 암호를 변경할 경우 해당 Insight Server에 대해 구성된 데이터 웨어하우스 서버 Connector의 ""인벤토리"" 사용자 암호와 일치해야 합니다.

시작하기 전에



암호를 변경하기 전에 사용자 계정의 종속성을 이해해야 합니다. 필요한 모든 서버에서 암호를 업데이트하지 못하면 Insight 구성 요소 간의 통신 장애가 발생합니다.

이 작업에 대해

다음 표에는 Insight Server의 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Insight Server 암호	필수 변경 사항
_내부	
획득	Lau, RAU
DWh _ 내부	데이터 웨어하우스
호스트	
인벤토리	데이터 웨어하우스
루트	

다음 표에는 데이터 웨어하우스에 대한 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

데이터 웨어하우스 암호	필수 변경 사항
Cognos_admin	
드Wh	
dWh_INTERNAL(서버 커넥터 구성 UI를 사용하여 변경)	Insight 서버
Dwhuser(사용자)	

호스트	
인벤토리(서버 커넥터 구성 UI를 사용하여 변경됨)	Insight 서버
루트	

- DWH 서버 연결 구성 UI * 에서 암호 변경

다음 표에는 Lau의 사용자 암호와 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Lau 암호	필수 변경 사항
획득	Insight 서버, RAU

서버 연결 구성 UI를 사용하여 "inventory" 및 "dWh_internal" 암호 변경

데이터 웨어하우스 UI를 사용하는 Insight 서버의 암호와 일치하도록 ""인벤토리" 또는 ""DIH_INTERNAL"" 암호를 변경해야 하는 경우

시작하기 전에

이 작업을 수행하려면 관리자로 로그인해야 합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh> 여기서 hostname 은 OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

커넥터 편집 * 화면이 표시됩니다.

Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="••••••••"/>
Advanced ▼	
<input type="button" value="Save"/>	<input type="button" value="Cancel"/> <input type="button" value="Test"/> <input type="button" value="Remove"/>

3. Database password * 필드에 새 ""Inventory"" 암호를 입력합니다.
4. 저장 * 을 클릭합니다
5. "dWh_INTERNAL" 암호를 변경하려면 * 고급 * 을 클릭합니다

커넥터 고급 편집 화면이 표시됩니다.

Edit Connector

ID:	1
Encryption:	Enabled
Name:	Oci-stg06-s12r2.nane.netapp.com
Host:	Oci-stg06-s12r2.nane.netapp.com
Database user name:	inventory
Database password:
Server user name:	dwh_internal
Server password:
HTTPS port:	443
TCP port:	3306

Basic ^

Save Cancel Test Remove

6. 서버 암호 * 필드에 새 암호를 입력합니다.

7. 저장 을 클릭합니다.

ODBC 관리 도구를 사용하여 **dWh** 암호를 변경합니다

Insight 서버에서 dWh 사용자의 암호를 변경하면 데이터 웨어하우스 서버에서도 암호를 변경해야 합니다. ODBC 데이터 원본 관리자 도구를 사용하여 데이터 웨어하우스의 암호를 변경할 수 있습니다.

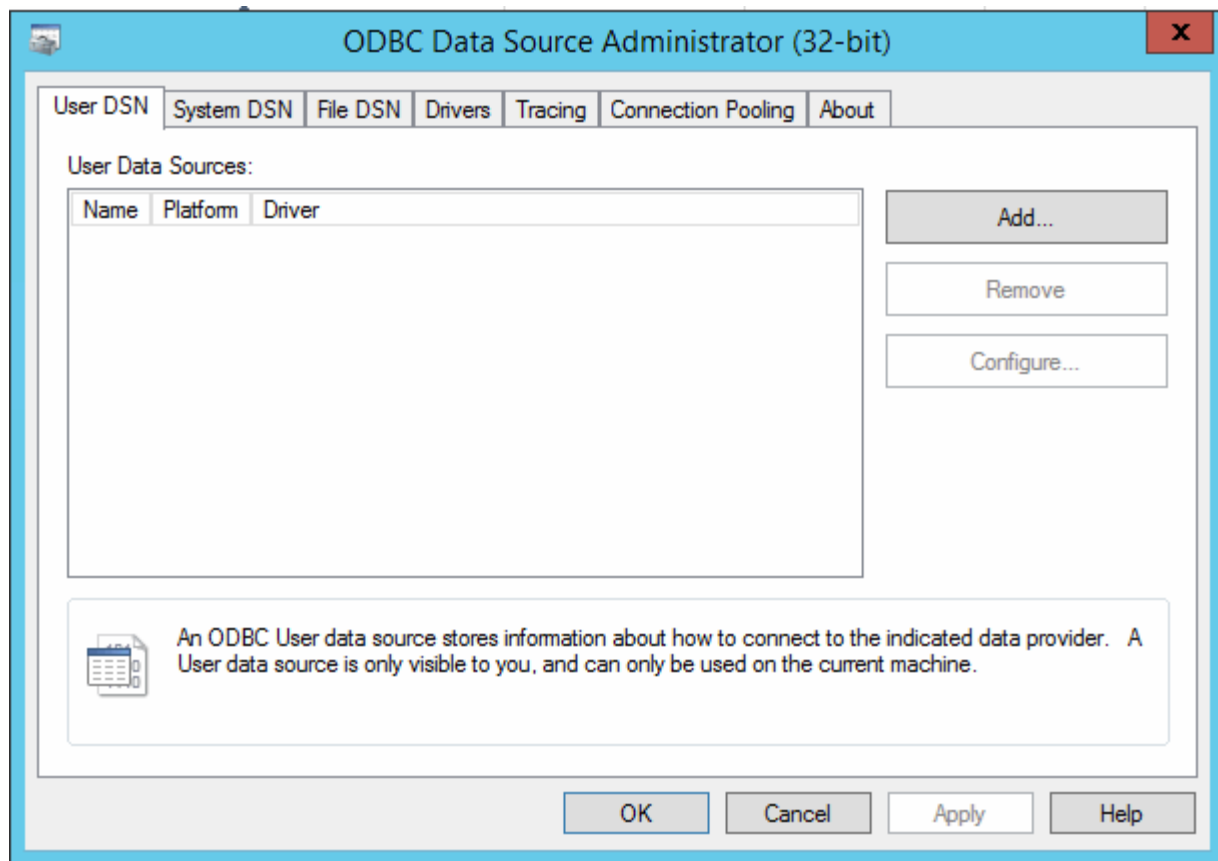
시작하기 전에

관리자 권한이 있는 계정을 사용하여 데이터 웨어하우스 서버에 원격으로 로그인해야 합니다.

단계

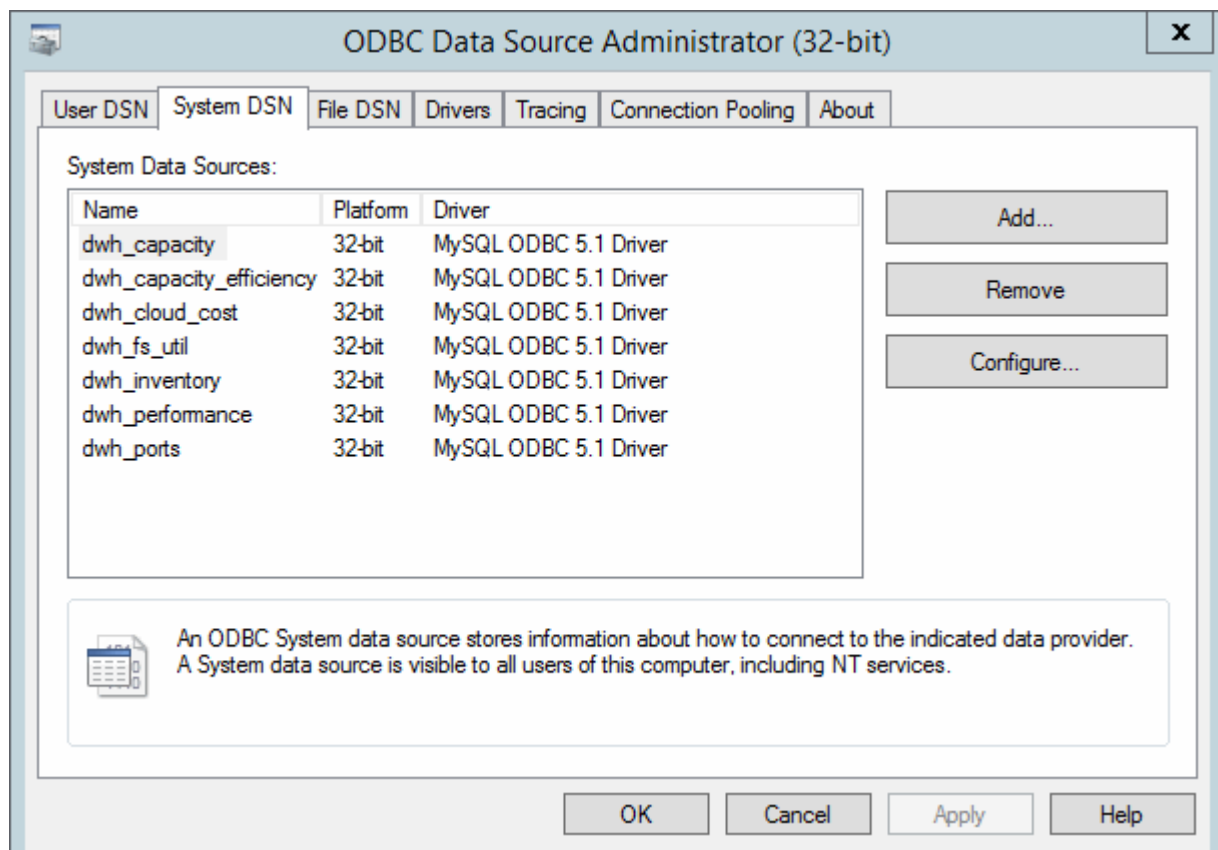
1. 해당 데이터 웨어하우스를 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 에서 ODBC 관리 도구에 액세스합니다 C:\Windows\SysWOW64\odbcad32.exe

ODBC 데이터 원본 관리자 화면이 표시됩니다.



3. 시스템 DSN*을 클릭합니다

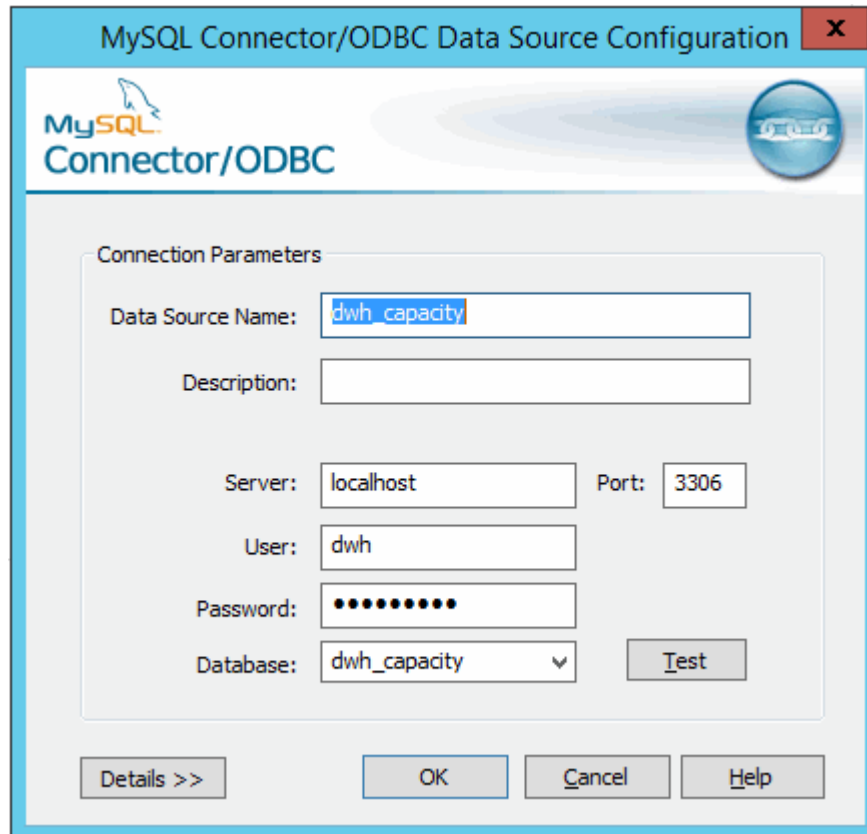
시스템 데이터 소스가 표시됩니다.



4. 목록에서 OnCommand Insight 데이터 원본을 선택합니다.

5. 구성 * 을 클릭합니다

데이터 소스 구성 화면이 표시됩니다.



The image shows the 'MySQL Connector/ODBC Data Source Configuration' dialog box. The title bar is blue with the MySQL logo and the text 'MySQL Connector/ODBC'. The main area is titled 'Connection Parameters' and contains several input fields: 'Data Source Name' (containing 'dwh_capacity'), 'Description' (empty), 'Server' (containing 'localhost'), 'Port' (containing '3306'), 'User' (containing 'dwh'), 'Password' (masked with dots), and 'Database' (a dropdown menu showing 'dwh_capacity'). There is a 'Test' button next to the Database dropdown. At the bottom, there are buttons for 'Details >>', 'OK', 'Cancel', and 'Help'.

6. 암호 * 필드에 새 암호를 입력합니다.

스마트 카드 및 인증서 로그인 지원

OnCommand Insight는 CAC(스마트 카드) 및 인증서를 사용하여 Insight 서버에 로그인하는 사용자를 인증할 수 있습니다. 이러한 기능을 사용하려면 시스템을 구성해야 합니다.

CAC 및 인증서를 지원하도록 시스템을 구성한 후 OnCommand Insight의 새 세션을 탐색하면 브라우저에 기본 대화 상자가 표시되어 사용자가 선택할 수 있는 개인 인증서 목록을 제공합니다. 이러한 인증서는 OnCommand Insight 서버에서 신뢰할 수 있는 CA에서 발급한 개인 인증서 집합을 기반으로 필터링됩니다. 대부분의 경우 단일 선택 옵션이 있습니다. 기본적으로 Internet Explorer는 하나만 선택할 경우 이 대화 상자를 건너뛵니다.



CAC 사용자의 경우 스마트 카드에는 신뢰할 수 있는 CA와 일치할 수 있는 인증서가 여러 개 있습니다. 에 대한 CAC 인증서입니다 identification 사용해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

스마트 카드 및 인증서 로그인을 위한 호스트 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하려면 OnCommand Insight 호스트 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 User principal account name 속성은 사용자 ID가 포함된 LDAP 필드와 일치해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. 를 사용합니다 regedit 에서 레지스트리 값을 수정하는 유틸리티입니다
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java:
 - a. jvm_option을 변경합니다 DclientAuth=false 를 선택합니다 DclientAuth=true.
2. 키 저장소 파일을 백업합니다. C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
3. 를 지정하는 명령 프롬프트를 엽니다 Run as administrator
4. 자체 생성된 인증서 삭제: C:\Program Files\SANscreen\java64\bin\keytool.exe -delete

```
-alias "ssl certificate" -keystore C:\Program  
Files\SANscreen\wildfly\standalone\configuration\server.keystore
```

5. 새 인증서 생성: C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"
6. 인증서 서명 요청(CSR) 생성: C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"
7. 6단계에서 CSR이 반환된 후 인증서를 가져온 다음 Base-64 형식으로 인증서를 내보내고 에 넣습니다 "C:\temp" named servername.cer.
8. 키 저장소에서 인증서를 추출합니다. C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12
9. P12 파일에서 개인 키를 추출합니다. openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"
10. 7단계에서 내보낸 Base-64 인증서를 개인 키와 병합합니다. openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"
11. 병합된 인증서를 키 저장소로 가져옵니다. C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"
12. 루트 인증서 가져오기: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"
13. 루트 인증서를 서버로 가져옵니다. trustore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"
14. 중간 인증서 가져오기: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"

모든 중간 인증서에 대해 이 단계를 반복합니다.

15. 이 예제와 일치하도록 LDAP에 도메인을 지정합니다.
16. 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 지원하도록 클라이언트 구성

클라이언트 시스템은 스마트 카드 사용 및 인증서 로그인을 지원하기 위해 미들웨어와 브라우저 수정이 필요합니다. 이미 스마트 카드를 사용하고 있는 고객은 클라이언트 시스템을 추가로 수정할 필요가 없습니다.

시작하기 전에



최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

다음은 일반적인 클라이언트 구성 요구 사항입니다.

- ActivClient와 같은 스마트 카드 미들웨어 설치(참조
- IE 브라우저 수정(참조
- Firefox 브라우저 수정(참조

Linux 서버에 대한 CAC 활성화

Linux OnCommand Insight 서버에서 CAC를 활성화하려면 몇 가지 수정이 필요합니다.

단계

1. 로 이동합니다 `/opt/netapp/oci/conf/`
2. 편집 `wildfly.properties` 의 값을 변경합니다 `CLIENT_AUTH_ENABLED "참"`으로
3. 아래에 있는 "루트 인증서"를 가져옵니다
`/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 서버를 다시 시작합니다

스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 User principal account name 속성은 사용자의 정부 ID 번호가 포함된 LDAP 필드와 일치해야 합니다.

정부에서 발급한 CAC에 저장된 일반 이름(CN)은 일반적으로 다음과 같은 형식입니다. first.last.ID. 와 같은 일부 LDAP 필드의 경우 sAMAccountName, 이 형식은 너무 깁니다. 이러한 필드의 경우 OnCommand Insight는 cns에서 ID 번호만 추출합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"



단계

1. regedit를 사용하여 의 레지스트리 값을 수정합니다

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software  
Foundation\Procrun2.0\SANscreen Server\Parameters\Java
```

- a. jvm_option을 변경합니다 -DclientAuth=false 를 선택합니다 -DclientAuth=true.

Linux의 경우 를 수정합니다 clientAuth 매개 변수 in /opt/netapp/oci/scripts/wildfly.server

2. CA(인증 기관)를 데이터 웨어하우스 trustore에 추가합니다.

- a. 명령 창에서 로 이동합니다 ..\SANscreen\wildfly\standalone\configuration.

- b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: C:\Program
Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore
-storepass changeit

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 필요한 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일. 데이터 웨어하우스 신뢰할 수 있는 CA와
함께 고객의 CA를 포함하려면 을 참조하십시오

..\SANscreen\wildfly\standalone\configuration 를 사용합니다 keytool 가져오기 명령:

```
C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore  
server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts
```

my_alias는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

3. OnCommand Insight 서버에서 를 클릭합니다 wildfly/standalone/configuration/standalone-full.xml 에서 verify-client를 "requested"로 업데이트하여 파일을 수정해야 합니다 /subsystem=undertow/server=default-server/https-listener=default-httpsCAC 활성화 Insight 서버에 로그인하고 적절한 명령을 실행합니다.

OS	스크립트
Windows	<install dir>\SANscreen\Wildfly\bin\enableCACforRemoteEJB.bat 을 참조하십시오
리눅스	/opt/netapp/OCI/Wildfly/bin/enableCACforRemoteEJB.sh 을 참조하십시오

스크립트를 실행한 후 다음 단계로 진행하기 전에 Wildfly 서버의 재로드가 완료될 때까지 기다립니다.

4. OnCommand Insight 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 위한 **Cognos** 구성(OnCommand Insight 7.3.5 ~ 7.3.9)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.
 - a. 명령 창에서 로 이동합니다 ..\SANscreen\cognos\analytics\configuration\certs\
 - b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: ..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다
`..\SANscreen\cognos\analytics\configuration\certs\.`
- e. 를 사용합니다 keytool 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

- f. 암호를 묻는 메시지가 나타나면 를 입력합니다 NoPassWordSet.

- g. 답변 yes 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 를 실행합니다 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. CAC 모드를 해제하려면 를 실행한다 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

스마트 카드 및 인증서 로그인에 대한 **Cognos 구성(OnCommand Insight 7.3.10 이상)**

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.

- a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
- b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다
`..\SANscreen\cognos\analytics\configuration\certs\.`
- e. 를 사용합니다 keytool 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

- f. 암호를 묻는 메시지가 나타나면 를 입력합니다 NoPassWordSet.
- g. 답변 yes 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 다음을 수행합니다.

- a. 다음 단계에 따라 CAC 로그아웃 페이지를 구성합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
 - (7.3.10 및 7.3.11에만 해당) 관리->구성->시스템->보안을 클릭합니다
 - (7.3.10 및 7.3.11에만 해당) 로그아웃 리디렉션 URL에 대해 cacLogout.html 을 입력합니다.\ → 적용
 - 브라우저를 닫습니다.
- b. 실행 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
- c. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

3. CAC 모드를 해제하려면 다음을 수행합니다.

- a. 실행 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
- b. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.
- c. (7.3.10 및 7.3.11에만 해당) 다음 단계에 따라 CAC 로그아웃 페이지를 구성 해제합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
 - 관리\ → 구성\ → 시스템\ → 보안을 클릭합니다
 - 로그아웃 리디렉션 URL \ → 적용에 대해 cacLogout.html 를 입력합니다
 - 브라우저를 닫습니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. 의 백업을 생성합니다 ..\SANSscreen\cognos\analytics\configuration\cogstartup.xml.
2. 아래의 ""certs"" 및 ""csk"" 폴더의 백업을 만듭니다 ..\SANSscreen\cognos\analytics\configuration.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
 - a. CD "\\Program Files\sansscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr
4. 를 엽니다 c:\temp\encryptRequest.csr 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. SSL 인증서를 얻으려면 encryptRequest.csr을 CA(인증 기관)에 보냅니다.

"san:dns=FQDN(예: hostname.netapp.com)" SubjectAltName을 추가하려면 추가 속성)을 추가해야 합니다.
Google Chrome 버전 58 이상에서 SubjectAltName이 인증서에서 누락되면 불만을 표시합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다
FQDN.p7b 파일이 다운로드됩니다
7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
 - a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
 - b. 왼쪽 창에서 ""인증서""를 찾습니다.
 - c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
 - d. Base64 출력을 선택합니다.
 - e. 루트 인증서로 식별하는 파일 이름을 입력합니다.

- f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a-8C단계를 반복합니다.
- g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
 - a. 메모장에서 intermediate.cer를 열고 내용을 복사합니다.
 - b. 메모장에서 root.cer를 열고 9a의 콘텐츠를 저장합니다.
 - c. 파일을 CA.CER로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
 - a. `cd ""Program Files\SANscreen\cognos\analytics\bin"`
 - b. `ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\CA.cer`

그러면 CA.cer가 루트 인증 기관으로 설정됩니다.
 - c. `ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer`

이렇게 하면 Cognos.cer 가 CA.cer 에 의해 서명된 암호화 인증서로 설정됩니다.
11. IBM Cognos 구성을 엽니다.
 - a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다
 - b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
 - c. 구성을 저장합니다.
 - d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
 - a. `"D:\Program Files\SANscreen\Java\bin\keytool.exe" -exportcert -file "" c:\temp\cognos.crt" -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12-storepass NoPassSet-alias 암호화`
13. 관리 CMD 프롬프트 창을 사용하여 "c:\temp\cognos.crt"를 dWh trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
 - a. `"D:\Program Files\SANscreen\Java\bin\keytool.exe" - importcert -file ""c:\temp\cognos.crt" - keystore "D:\Program Files\SANscreen\standalone\configuration\server.trustore" - storepass changeit -alias cognosert`
14. SANscreen 서비스를 다시 시작합니다.
15. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.10 이상)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. IBM Cognos 구성 도구를 사용하여 Cognos를 중지합니다. Cognos를 닫습니다.
2. 의 백업을 생성합니다 ..\SANSscreen\cognos\analytics\configuration 및 ..\SANSscreen\cognos\analytics\temp\cam\freshness 폴더.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
 - a. CD "\Program Files\sansscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress". 참고: 여기서 -H와 -I는 DNS 및 ipaddress와 같은 subjectAltNames를 추가합니다.
4. 를 엽니다 c:\temp\encryptRequest.csr 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. encryptRequest.csr 콘텐츠를 입력하고 CA 서명 포털을 사용하여 인증서를 생성합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

FQDN.p7b 파일이 다운로드됩니다
7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
 - a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
 - b. 왼쪽 창에서 ""인증서""를 찾습니다.
 - c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
 - d. Base64 출력을 선택합니다.
 - e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
 - f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a ~ 8e 단계를 반복합니다.

- g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
 - a. 메모장에서 root.cer를 열고 내용을 복사합니다.
 - b. 메모장을 사용하여 intermediate.cer를 열고 9a(중간 우선 및 루트 다음)의 콘텐츠를 추가합니다.
 - c. 파일을 chain.cer로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
 - a. cd ""Program Files\SANscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\root.cer
 - c. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\intermediate.cer
 - d. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. IBM Cognos 구성을 엽니다.
 - a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다
 - b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
 - c. 구성을 저장합니다.
 - d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
 - a. CD "C:\Program Files\SANscreen"
 - b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore-storetype pkcs12-storepass NoPassWordSet-alias encryption
13. 에서 DWH 서버 트루스토어를 백업합니다.


```
..\SANscreen\wildfly\standalone\configuration\server.trustore
```
14. 관리 CMD 프롬프트 창을 사용하여 "c:\temp\cognos.crt"를 DWH trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
 - a. CD "C:\Program Files\SANscreen"
 - b. java\bin\keytool.exe - importcert -file c:\temp\cognos.crt -keystore wandiderfly\standalone\configuration\server.trutstore -storephass changeit -alias coclnos3rdca
15. SANscreen 서비스를 다시 시작합니다.
16. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.
17. 's' 인증서만 변경되고 기본 Cognos 인증서는 변경되지 않은 경우에도 다음 단계를 수행해야 합니다. 그렇지 않으면 Cognos가 새 SANscreen 인증서에 대해 불만을 제기하거나 DWH 백업을 생성할 수 없습니다.
 - a. cd "%SANSSCREEN_HOME%cognos\analytics\bin\"
 - b. "%SANSSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sansscreen.cer" -keystore "%SANSSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"
 - c. ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.cer"

일반적으로 이러한 단계는 에 설명된 Cognos 인증서 가져오기 프로세스의 일부로 수행됩니다 "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 User principal account name 속성은 사용자의 정부 ID 번호가 포함된 LDAP 필드와 일치해야 합니다.

정부에서 발급한 CAC에 저장된 일반 이름(CN)은 일반적으로 다음과 같은 형식입니다. first.last.ID. 와 같은 일부 LDAP 필드의 경우 sAMAccountName, 이 형식은 너무 길다. 이러한 필드의 경우 OnCommand Insight는 cns에서 ID 번호만 추출합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. regedit를 사용하여 의 레지스트리 값을 수정합니다

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java

- a. jvm_option을 변경합니다 -DclientAuth=false 를 선택합니다 -DclientAuth=true.

Linux의 경우 를 수정합니다 clientAuth 매개 변수 in /opt/netapp/oci/scripts/wildfly.server

2. CA(인증 기관)를 데이터 웨어하우스 trustore에 추가합니다.

- a. 명령 창에서 로 이동합니다 ..\SANscreen\wildfly\standalone\configuration.
- b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 필요한 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일. 데이터 웨어하우스 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 을 참조하십시오

..\SANscreen\wildfly\standalone\configuration 를 사용합니다 keytool 가져오기 명령:
C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore
server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts

my_alias는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

3. OnCommand Insight 서버에서 를 클릭합니다 wildfly/standalone/configuration/standalone-full.xml 에서 verify-client를 "requested"로 업데이트하여 파일을 수정해야 합니다
/subsystem=undertow/server=default-server/https-listener=default-httpsCAC 활성화
Insight 서버에 로그인하고 적절한 명령을 실행합니다.

OS	스크립트
Windows	<install dir>\SANscreen\Wildfly\bin\enableCACforRemoteEJB.bat 을 참조하십시오
리눅스	/opt/netapp/OCI/Wildfly/bin/enableCACforRemoteEJB.sh 을 참조하십시오

스크립트를 실행한 후 다음 단계로 진행하기 전에 Wildfly 서버의 재로드가 완료될 때까지 기다립니다.

4. OnCommand Insight 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 위한 **Cognos** 구성(OnCommand Insight 7.3.5 ~ 7.3.9)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Truststore에 CA(인증 기관)를 추가합니다.

- 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
- 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.
- 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다 `keytool -list` 작동.

- 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.
- 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 를 실행합니다 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. CAC 모드를 해제하려면 를 실행한다 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

스마트 카드 및 인증서 로그인에 대한 **Cognos** 구성(OnCommand Insight 7.3.10 이상)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.

- a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
- b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.
- e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다 `keytool -list` 작동.

- f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.
- g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 다음을 수행합니다.

- a. 다음 단계에 따라 CAC 로그아웃 페이지를 구성합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: `cognos_admin`)에 속해야 함)
 - (7.3.10 및 7.3.11에만 해당) 관리->구성->시스템->보안을 클릭합니다
 - (7.3.10 및 7.3.11에만 해당) 로그아웃 리디렉션 URL에 대해 `cacLogout.html` 을 입력합니다.\ → 적용
 - 브라우저를 닫습니다.
- b. 실행 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
- c. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

3. CAC 모드를 해제하려면 다음을 수행합니다.

- a. 실행 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
- b. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.
- c. (7.3.10 및 7.3.11에만 해당) 다음 단계에 따라 CAC 로그아웃 페이지를 구성 해제합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: `cognos_admin`)에 속해야 함)
 - 관리\ → 구성\ → 시스템\ → 보안을 클릭합니다
 - 로그아웃 리디렉션 URL \ → 적용에 대해 `cacLogout.html` 를 입력합니다
 - 브라우저를 닫습니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. 의 백업을 생성합니다 ..\SANSscreen\cognos\analytics\configuration\cogstartup.xml.
2. 아래의 ""certs"" 및 ""csk"" 폴더의 백업을 만듭니다 ..\SANSscreen\cognos\analytics\configuration.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
 - a. CD "\Program Files\sansscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr
4. 를 엽니다 c:\temp\encryptRequest.csr 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. SSL 인증서를 얻으려면 encryptRequest.csr을 CA(인증 기관)에 보냅니다.

"san:dns=FQDN(예: hostname.netapp.com)" SubjectAltName을 추가하려면 추가 속성)을 추가해야 합니다.
Google Chrome 버전 58 이상에서 SubjectAltName이 인증서에서 누락되면 불만을 표시합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다
FQDN.p7b 파일이 다운로드됩니다
7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.

8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
 - a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
 - b. 왼쪽 창에서 ""인증서""를 찾습니다.
 - c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
 - d. Base64 출력을 선택합니다.
 - e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
 - f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a-8C단계를 반복합니다.
 - g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
 - a. 메모장에서 intermediate.cer를 열고 내용을 복사합니다.
 - b. 메모장에서 root.cer를 열고 9a의 콘텐츠를 저장합니다.
 - c. 파일을 CA.CER로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
 - a. cd ""Program Files\SANscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\CA.cer

그러면 CA.cer가 루트 인증 기관으로 설정됩니다.

 - c. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer

이렇게 하면 Cognos.cer 가 CA.cer 에 의해 서명된 암호화 인증서로 설정됩니다.
11. IBM Cognos 구성을 엽니다.
 - a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다
 - b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
 - c. 구성을 저장합니다.
 - d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
 - a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" -exportcert -file "" c:\temp\cognos.crt" -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12-storepass NoPassSet-alias 암호화
13. 관리 CMD 프롬프트 창을 사용하여 ""c:\temp\cognos.crt""를 dWh trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
 - a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" - importcert -file ""c:\temp\cognos.crt" - keystore "D:\Program Files\SANscreen\standalone\configuration\server.trustore" - storepass changeit -alias cognosert
14. SANscreen 서비스를 다시 시작합니다.
15. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.10 이상)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. IBM Cognos 구성 도구를 사용하여 Cognos를 중지합니다. Cognos를 닫습니다.
2. 의 백업을 생성합니다 `..\SANSscreen\cognos\analytics\configuration` 및 `..\SANSscreen\cognos\analytics\temp\cam\freshness` 폴더.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
 - a. `CD "\Program Files\sansscreen\cognos\analytics\bin"`
 - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress"`. 참고: 여기서 -H와 -I는 DNS 및 ipaddress와 같은 `subjectAltNames`를 추가합니다.
4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. `encryptRequest.csr` 콘텐츠를 입력하고 CA 서명 포털을 사용하여 인증서를 생성합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

`FQDN.p7b` 파일이 다운로드됩니다
7. CA에서 `.p7b` 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. `ThirdPartyCertificateTool.bat` 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.

- a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
 - b. 왼쪽 창에서 ""인증서""를 찾습니다.
 - c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
 - d. Base64 출력을 선택합니다.
 - e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
 - f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a ~ 8e 단계를 반복합니다.
 - g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
- a. 메모장에서 root.cer를 열고 내용을 복사합니다.
 - b. 메모장을 사용하여 intermediate.cer를 열고 9a(중간 우선 및 루트 다음)의 콘텐츠를 추가합니다.
 - c. 파일을 chain.cer로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
- a. cd ""Program Files\SANscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\root.cer
 - c. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\intermediate.cer
 - d. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. IBM Cognos 구성을 엽니다.
- a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다
 - b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
 - c. 구성을 저장합니다.
 - d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
- a. CD "C:\Program Files\SANscreen"
 - b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore-storetype pkcs12-storepass NoPassWordSet-alias encryption
13. 에서 DWH 서버 트루스토어를 백업합니다. .\SANscreen\wildfly\standalone\configuration\server.trustore
14. 관리 CMD 프롬프트 창을 사용하여 "c:\temp\cognos.crt"를 DWH trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
- a. CD "C:\Program Files\SANscreen"
 - b. java\bin\keytool.exe - importcert -file c:\temp\cognos.crt -keystore wandiderfly\standalone\configuration\server.trutstore -storephass changeit -alias coclnos3rdca
15. SANscreen 서비스를 다시 시작합니다.
16. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.
17. 's' 인증서만 변경되고 기본 Cognos 인증서는 변경되지 않은 경우에도 다음 단계를 수행해야 합니다. 그렇지 않으면

Cognos가 새 SANscreen 인증서에 대해 불만을 제기하거나 DWH 백업을 생성할 수 없습니다.

- a. `cd "%SANSCREEN_HOME%cognos\analytics\bin\"`
- b. `"%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
- c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"`

일반적으로 이러한 단계는 에 설명된 Cognos 인증서 가져오기 프로세스의 일부로 수행됩니다 "[Cognos CA\(인증 기관\) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법](#)"

SSL 인증서를 가져오는 중입니다

SSL 인증서를 추가하여 OnCommand Insight 환경의 보안을 강화하기 위한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

시스템이 최소 필수 비트 수준(1024비트)을 충족하는지 확인해야 합니다.

이 작업에 대해



이 절차를 수행하기 전에 기존 를 백업해야 합니다 server.keystore 파일 및 백업 이름을 지정합니다 server.keystore.old. 의 손상 또는 손상 server.keystore Insight 서버를 다시 시작한 후 Insight 서버가 작동하지 않을 수 있습니다. 백업을 생성하는 경우 문제가 발생할 경우 이전 파일로 되돌릴 수 있습니다.

단계

1. 원본 키 저장소 파일의 복사본을 만듭니다. `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old"`
2. 키 저장소의 내용을 나열합니다. `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
 - a. 암호를 묻는 메시지가 나타나면 를 입력합니다 changeit.키 저장소의 내용이 표시됩니다. 키 저장소에 인증서가 하나 이상 있어야 합니다. "ssl certificate".
3. 를 삭제합니다 "ssl certificate": `keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. 새 키 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
 - a. 성과 이름을 묻는 메시지가 나타나면 사용하려는 FQDN(정규화된 도메인 이름)을 입력합니다.
 - b. 조직 및 조직 구조에 대한 다음 정보를 제공합니다.

- 국가: 해당 국가의 두 글자 ISO 약어(예: US)
- 시/도: 조직의 본사 소재지가 위치한 시/도의 이름(예: 매사추세츠주)
- 지역: 조직의 본사 소재지(예: Waltham)의 이름입니다.
- 조직 이름: 도메인 이름을 소유한 조직의 이름(예: NetApp)
- 조직 단위 이름: 인증서를 사용할 부서 또는 그룹의 이름(예: 지원)
- 도메인 이름/일반 이름: 서버의 DNS 조회에 사용되는 FQDN(예: www.example.com) 시스템이 다음과 유사한 정보로 응답합니다. Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?

c. 를 입력합니다 Yes CN(Common Name)이 FQDN과 같은 경우

d. 키 암호를 묻는 메시지가 나타나면 암호를 입력하거나 Enter 키를 눌러 기존 키 저장소 암호를 사용합니다.

5. 인증서 요청 파일 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

를 클릭합니다 c:\localhost.csr file 은 새로 생성된 인증서 요청 파일입니다.

6. 를 제출합니다 c:\localhost.csr 승인을 위해 CA(인증 기관)에 파일을 저장합니다.

인증서 요청 파일이 승인되면 에서 인증서를 반환하도록 합니다 .der 형식. 파일이 로 반환될 수도 있고 반환되지 않을 수도 있습니다 .der 파일. 기본 파일 형식은 입니다 .cer Microsoft CA 서비스의 경우.

대부분의 조직의 CA는 루트 CA를 포함하여 신뢰할 수 있는 모델 체인을 사용합니다. 이 모델은 대개 오프라인 상태입니다. 이 인증서는 중간 CA라고 하는 몇 개의 하위 CA에 대해서만 인증서에 서명했습니다.

전체 신뢰 체인에 대한 공개 키(인증서)를 얻어야 합니다. 즉, OnCommand Insight 서버의 인증서에 서명한 CA의 인증서와 조직 루트 CA에 등록하는 CA 간의 모든 인증서를 얻어야 합니다.

일부 조직에서는 서명 요청을 제출할 때 다음 중 하나를 받을 수 있습니다.

- 서명된 인증서와 신뢰 체인에서 모든 공개 인증서가 들어 있는 PKCS12 파일입니다
- A .zip 개별 파일(서명된 인증서 포함)과 신뢰 체인에서 모든 공용 인증서를 포함하는 파일입니다
- 서명된 인증서만

공용 인증서를 얻어야 합니다.

7. server.keystore에 대해 승인된 인증서를 가져옵니다. `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`

a. 메시지가 표시되면 키 저장소 암호를 입력합니다.

다음 메시지가 표시됩니다. Certificate reply was installed in keystore

8. 서버에 대해 승인된 인증서를 가져옵니다. trustore: `C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com`

```
-file c:\localhost2.DER -keystore "c:\Program  
Files\SANscreen\wildfly\standalone\configuration\server.trustore"
```

a. 메시지가 표시되면 Trustore 암호를 입력합니다.

다음 메시지가 표시됩니다. Certificate reply was installed in trustore

9. 를 편집합니다 SANscreen\wildfly\standalone\configuration\standalone-full.xml 파일:

다음 별칭 문자열을 대체합니다. alias="cbc-oci-02.muccbc.hq.netapp.com". 예를 들면 다음과 같습니다.

```
<keystore path="server.keystore" relative-to="jboss.server.config.dir"  
keystore-password="{VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-  
02.muccbc.hq.netapp.com" key-  
password="{VAULT::HttpsRealm::key_password::1}"/>
```

10. SANscreen 서버 서비스를 다시 시작합니다.

Insight가 실행되면 자물쇠 아이콘을 클릭하여 시스템에 설치된 인증서를 볼 수 있습니다.

"발급자" 정보와 일치하는 "발급 대상" 정보가 포함된 인증서가 표시되는 경우 자체 서명된 인증서가 설치되어 있는 것입니다. Insight 설치 관리자가 생성한 자체 서명 인증서의 만료 기간은 100년입니다.

NetApp은 이 절차로 디지털 인증서 경고가 제거된다고 보장할 수 없습니다. NetApp은 최종 사용자 워크스테이션의 구성 방법을 제어할 수 없습니다. 다음과 같은 시나리오를 고려해 보십시오.

- Microsoft Internet Explorer와 Google Chrome 모두 Windows에서 Microsoft의 기본 인증서 기능을 사용합니다.

즉, Active Directory 관리자가 조직의 CA 인증서를 최종 사용자의 인증서 트루스토어로 푸시하면 OnCommand Insight 자체 서명된 인증서가 내부 CA 인프라에서 서명한 인증서로 교체되면 이러한 브라우저의 사용자에게 인증서 경고가 사라집니다.

- Java 및 Mozilla Firefox에는 자체 인증서 저장소가 있습니다.

시스템 관리자가 CA 인증서를 이러한 응용 프로그램의 신뢰할 수 있는 인증서 저장소에 자동으로 수집하지 않는 경우 자체 서명된 인증서가 교체되더라도 신뢰할 수 없는 인증서로 인해 Firefox 브라우저를 사용하면 인증서 경고가 계속 생성될 수 있습니다. 조직의 인증서 체인을 Trustore에 설치하는 것도 추가 요구 사항입니다.

Insight 데이터베이스의 주별 백업 설정

Insight 데이터베이스의 데이터를 보호하기 위해 매주 자동으로 백업을 설정할 수도 있습니다. 이러한 자동 백업은 지정된 백업 디렉토리의 파일을 덮어씁니다.

이 작업에 대해

- 모범 사례 *: OCI 데이터베이스의 주간 백업을 설정할 때는 서버에 오류가 발생할 경우 Insight에서 사용하는 것과 다른 서버에 백업을 저장해야 합니다. 매주 백업마다 디렉토리의 파일을 덮어쓰므로 수동 백업을 주별 백업 디렉토리에 저장하지 마십시오.

백업 파일에는 다음이 포함됩니다.

- 재고 데이터
- 최대 7일간의 성능 데이터

단계

1. Insight 도구 모음에서 * Admin * > * Setup * 을 클릭합니다.
2. 백업 및 아카이브 * 탭을 클릭합니다.
3. Weekly Backup 섹션에서 * Enable weekly backup * 을 선택합니다.
4. 백업 위치 * 의 경로를 입력합니다. 로컬 Insight 서버의 또는 Insight 서버에서 액세스할 수 있는 원격 서버에 있을 수 있습니다.



백업 위치 설정은 백업 자체에 포함되어 있으므로 다른 시스템에서 백업을 복원할 경우 새 시스템에서 백업 폴더 위치가 잘못되었을 수 있습니다. 백업을 복원한 후 백업 위치 설정을 다시 확인합니다.

5. 마지막 2개 또는 마지막 5개 백업을 유지하려면 * Cleanup * 옵션을 선택합니다.
6. 저장 * 을 클릭합니다.

결과

Admin * > * Troubleshooting * 으로 이동하여 필요 시 백업을 생성할 수도 있습니다.

백업에 포함된 항목

매주 및 필요 시 백업을 문제 해결 또는 마이그레이션에 사용할 수 있습니다.

주별 또는 주문형 백업에는 다음이 포함됩니다.

- 재고 데이터
- 성능 데이터(백업에 포함하도록 선택한 경우)
- 데이터 원본 및 데이터 원본 설정
- 통합 팩
- 원격 획득 장치
- ASUP/프록시 설정
- 위치 설정 백업
- 보관 위치 설정
- 알림 설정
- 사용자
- 성능 정책
- 업무 엔티티 및 애플리케이션

- 장치 해상도 규칙 및 설정
- 대시보드 및 위젯
- 맞춤형 자산 페이지 대시보드 및 위젯
- 쿼리
- 주식 및 주식 규칙

주별 백업에는 다음이 포함되지 않습니다.

- 보안 도구 설정/볼트 정보(별도의 CLI 프로세스를 통해 백업)
- 로그(요청 시 .zip 파일에 저장 가능)
- 성능 데이터(백업에 포함하도록 선택하지 않은 경우)
- 추가 수익 실적을



백업에 성능 데이터를 포함하도록 선택하면 최근 7일 동안의 데이터가 백업됩니다. 해당 기능이 활성화된 경우 나머지 데이터는 아카이브에 포함됩니다.

성능 데이터 아카이빙

OnCommand Insight 7.3에는 성능 데이터를 매일 아카이빙하는 기능이 도입되었습니다. 이 기능은 구성 및 제한된 성능 데이터 백업을 보완합니다.

OnCommand Insight은 최대 90일 동안의 성능 및 위반 데이터를 보존합니다. 그러나 해당 데이터의 백업을 생성할 때는 가장 최근의 정보만 백업에 포함됩니다. 아카이빙을 통해 나머지 성능 데이터를 저장하고 필요에 따라 로드할 수 있습니다.

아카이브 위치가 구성되고 아카이빙이 활성화되면 Insight에서 모든 객체에 대한 전일 성능 데이터를 아카이브 위치에 아카이브합니다. 각 날짜의 아카이브는 별도의 파일에 있는 보관 폴더에 보관됩니다. 보관은 백그라운드에서 수행되며 Insight가 실행되는 동안에는 계속됩니다.

최근 90일 동안의 아카이브가 보존되며, 90일이 지난 아카이브 파일은 새 아카이브가 생성됨에 따라 삭제됩니다.

성능 아카이브 지원

성능 데이터 아카이빙을 활성화하려면 다음 단계를 수행하십시오.

단계

1. 도구 모음에서 * Admin * > * Setup * 을 클릭합니다.
2. Backup & Archive * 탭을 선택합니다.
3. 성능 아카이브 섹션에서 성능 아카이브 활성화 가 선택되어 있는지 확인합니다.
4. 올바른 아카이브 위치를 지정하십시오.

Insight 설치 폴더 아래에 폴더를 지정할 수 없습니다.

모범 사례: Insight 백업 위치와 동일한 보관 폴더를 지정하지 마십시오.

5. 저장 * 을 클릭합니다.

아카이브 프로세스는 백그라운드에서 처리되며 다른 Insight 활동을 방해하지 않습니다.

성능 아카이브 로드 중

성능 데이터 아카이브를 로드하려면 다음 단계를 수행하십시오.

시작하기 전에

성능 데이터 아카이브를 로드하기 전에 유효한 주별 또는 수동 백업을 복원해야 합니다.

단계

1. 도구 모음에서 * Admin * > * Troubleshooting * 을 클릭합니다.
2. 복원 섹션의 * 성능 아카이브 로드 * 에서 * 로드 * 를 클릭합니다.



아카이브 로딩은 백그라운드에서 처리됩니다. 매일 아카이빙된 성능 데이터가 Insight에 채워지면 전체 아카이브를 로드하는 데 시간이 오래 걸릴 수 있습니다. 아카이브 로드 상태가 이 페이지의 아카이브 섹션에 표시됩니다.

전자 메일 구성

OnCommand Insight Server에서 이메일을 통해 보고서 및 구독자 정보를 제공하고, 문제 해결을 위한 지원 정보를 NetApp 기술 지원 팀에 전송할 수 있도록 이메일 시스템에 액세스하도록 OnCommand Insight를 구성해야 합니다.

e-메일 구성 사전 요구 사항

이메일 시스템에 액세스하도록 OnCommand Insight를 구성하려면 먼저 호스트 이름 또는 IP 주소를 검색하여 (SMTP 또는 Exchange) 메일 서버를 식별하고 OnCommand Insight 보고서에 대한 이메일 계정을 할당해야 합니다.

이메일 관리자에게 문의하여 OnCommand Insight에 대한 이메일 계정을 만드십시오. 다음 정보가 필요합니다.

- 조직에서 사용하는 (SMTP 또는 Exchange) 메일 서버를 식별하기 위한 호스트 이름 또는 IP 주소입니다. 이 정보는 전자 메일을 읽는 데 사용하는 응용 프로그램을 통해 찾을 수 있습니다. 예를 들어 Microsoft Outlook에서 계정 구성을 확인하여 서버의 이름을 찾을 수 있습니다. 도구 - 전자 메일 계정 - 기존 전자 메일 계정을 보거나 변경할 수 있습니다.
- OnCommand Insight에서 정기 보고서를 보내는 데 사용할 전자 메일 계정의 이름입니다. 계정은 조직에서 유효한 이메일 주소여야 합니다. (대부분의 메일 시스템은 유효한 사용자로부터 메시지를 보내지 않는 한 메시지를 보내지 않습니다.) 전자 메일 서버에서 메일을 보내기 위해 사용자 이름과 암호가 필요한 경우 시스템 관리자에게 문의하십시오.

Insight에 대한 이메일 구성

사용자가 자신의 이메일 계정으로 Insight 보고서를 받으려면 이 기능을 사용하도록 이메일 서버를 구성해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Notifications * 를 선택합니다.
2. 페이지의 * 이메일 * 섹션으로 스크롤합니다.
3. 서버 * 상자에 조직의 SMTP 서버 이름을 입력합니다. 이 이름은 호스트 이름 또는 IP 주소 (_nnn.nnn.nnn_format)를 사용하여 식별됩니다.

호스트 이름을 지정하는 경우 DNS를 통해 이름을 확인할 수 있는지 확인합니다.

4. 사용자 이름 * 상자에 사용자 이름을 입력합니다.
5. 암호 * 상자에 전자 메일 서버에 액세스하기 위한 암호를 입력합니다. 이 암호는 SMTP 서버가 암호로 보호되는 경우에만 필요합니다. 이 암호는 전자 메일을 읽을 수 있는 응용 프로그램에 로그인하는 데 사용하는 암호와 동일합니다. 암호가 필요한 경우 확인을 위해 두 번째 암호를 입력해야 합니다.
6. 보낸 사람 e-메일 * 상자에 모든 OnCommand Insight 보고서의 보낸 사람으로 식별되는 보낸 사람 e-메일 계정을 입력합니다.

이 계정은 조직 내의 유효한 전자 메일 계정이어야 합니다.

7. 전자 메일 서명 * 상자에 보낼 모든 전자 메일에 삽입할 텍스트를 입력합니다.
8. 받는 사람 상자에서 을 클릭합니다 +이메일 주소를 입력하고 * 확인 * 을 클릭합니다.

이메일 주소를 편집하려면 주소를 선택하고 을 클릭합니다 ✎. 이메일 주소를 삭제하려면 주소를 선택하고 을 클릭합니다 ✕.

9. 지정된 수신자에게 테스트 이메일을 보내려면 을 클릭합니다 ✓.
10. 저장 * 을 클릭합니다.

SNMP 알림을 구성합니다

OnCommand Insight는 구성 및 글로벌 경로 정책 변경 및 위반에 대한 SNMP 알림을 지원합니다. 예를 들어, 데이터 소스 임계값이 초과되면 SNMP 알림이 전송됩니다.

시작하기 전에

다음을 완료해야 합니다.

- 각 이벤트 유형에 대한 트랩을 통합하는 서버의 IP 주소를 식별합니다.
이 정보를 얻으려면 시스템 관리자에게 문의해야 할 수도 있습니다.
- 지정된 시스템에서 각 이벤트 유형에 대해 SNMP 트랩을 가져오는 데 사용되는 포트 번호를 식별합니다.
SNMP 트랩의 기본 포트는 162입니다.
- 사이트에서 MIB 컴파일.

독점 MIB는 OnCommand Insight 트랩을 지원하는 설치 소프트웨어와 함께 제공됩니다. NetApp MIB는 모든 표준 SNMP 관리 소프트웨어와 호환되며 Insight 서버에서 찾을 수 있습니다 <install dir>\SANscreen\MIBS\sanscreen.mib.

단계

1. 관리자 * 를 클릭하고 * 알림 * 을 선택합니다.
2. 페이지의 * SNMP * 섹션으로 스크롤합니다.
3. Actions * 를 클릭하고 * Add trap source * 를 선택합니다.
4. SNMP 트랩 수신자 추가 * 대화 상자에 다음 값을 입력합니다.
 - * IP *

OnCommand Insight가 SNMP 트랩 메시지를 보내는 IP 주소입니다.

- * 포트 *

OnCommand Insight가 SNMP 트랩 메시지를 보내는 포트 번호입니다.

- * 커뮤니티 문자열 *

SNMP 트랩 메시지에 ""public""을 사용합니다.

5. 저장 * 을 클릭합니다.

syslog 기능을 활성화합니다

OnCommand Insight 위반 및 성능 경고 로그와 감사 메시지를 위한 위치를 식별하고 로깅 프로세스를 활성화할 수 있습니다.

시작하기 전에

- 시스템 로그를 저장할 서버의 IP 주소가 있어야 합니다.
- local1 또는 user와 같이 메시지를 로깅하는 프로그램 유형에 해당하는 기능 수준을 알아야 합니다.

이 작업에 대해

syslog에는 다음과 같은 유형의 정보가 포함되어 있습니다.

- 위반 메시지
- 성능 경고
- 필요에 따라 감사 로그 메시지를 선택합니다

syslog에 사용되는 단위는 다음과 같습니다.

- 사용률 메트릭: 백분율
- 트래픽 메트릭: MB
- 트래픽 속도: MB/s

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Notifications * 를 선택합니다.

2. 페이지의 * Syslog * 섹션으로 스크롤합니다.
3. syslog * 활성화 확인란을 선택합니다.
4. 원하는 경우 * Send audit * (감사 보내기 *) 확인란을 선택합니다. 새 감사 로그 메시지는 감사 페이지에 표시될 뿐만 아니라 syslog에 전송됩니다. 이미 존재하는 감사 로그 메시지는 syslog에 전송되지 않으며 새로 생성된 로그 메시지만 전송됩니다.
5. 서버 * 필드에 로그 서버의 IP 주소를 입력합니다.

서버 IP(예: server:port)의 끝에서 콜론 다음에 사용자 지정 포트를 추가하여 사용자 지정 포트를 지정할 수 있습니다. 포트가 지정되지 않은 경우 기본 syslog 포트 514가 사용됩니다.

6. Facility * 필드에서 메시지를 로깅하는 프로그램 유형에 해당하는 시설 수준을 선택합니다.
7. 저장 * 을 클릭합니다.

Insight syslog 콘텐츠

서버에서 syslog를 활성화하여 활용률 및 트래픽 데이터를 포함한 Insight 위반 및 성능 경고 메시지를 수집할 수 있습니다.

메시지 유형

Insight syslog에는 세 가지 유형의 메시지가 나열됩니다.

- SAN 경로 위반
- 일반 위반
- 성능 경고

데이터가 제공됩니다

위반 설명에는 관련 요소, 이벤트 시간, 위반의 상대적 심각도 또는 우선 순위가 포함됩니다.

성능 알림에는 다음 데이터가 포함됩니다.

- 활용률
- 트래픽 유형
- 트래픽 속도(MB

성능을 구성하고 위반 알림을 확인합니다

OnCommand Insight는 성능 관련 알림을 지원하고 위반을 보장합니다. 기본적으로 Insight는 이러한 위반에 대한 알림을 보내지 않습니다. Insight에서 이메일을 보내거나, syslog 메시지를 syslog 서버로 보내거나, 위반이 발생할 경우 SNMP 알림을 보내도록 구성해야 합니다.

시작하기 전에

위반에 대한 e-메일, syslog 및 SNMP 전송 방법을 구성해야 합니다.

단계

1. 관리자 * > * 알림 * 을 클릭합니다.
2. 이벤트 * 를 클릭합니다.
3. 성능 위반 이벤트 * 또는 * 위반 이벤트 보증 * 섹션에서 원하는 알림 방법(* 이메일 , * Syslog * 또는 * SNMP *) 목록을 클릭하고 위반의 심각도 수준(경고 이상 * 또는 * 긴급 *)을 선택합니다.
4. 저장 * 을 클릭합니다.

시스템 수준 이벤트 알림 구성

OnCommand Insight는 획득 장치 장애 또는 데이터 소스 오류와 같은 시스템 수준 이벤트에 대한 알림을 지원합니다. 알림을 수신하려면 이러한 이벤트 중 하나 이상이 발생할 때 Insight에서 이메일을 보내도록 구성해야 합니다.

시작하기 전에

관리 * > * 알림 * > * 전송 방법 * 에서 알림을 수신할 이메일 수신자를 구성해야 합니다.

단계

1. 관리자 * > * 알림 * 을 클릭합니다.
2. 이벤트 * 를 클릭합니다.
3. 시스템 경고 이벤트 * 이메일 섹션에서 알림에 대한 심각도 수준(* 경고 이상 * 또는 * 긴급 *)을 선택하거나 시스템 수준 이벤트 알림을 수신하지 않으려면 * 보내지 않음 * 을 선택합니다.
4. 저장 * 을 클릭합니다.
5. Admin * > * System Alerts * 를 클릭하여 알림을 직접 구성합니다.
6. 새 경고를 추가하려면 * + 추가 * 를 클릭하고 알림에 고유한 * 이름 * 을 지정합니다. 오른쪽 아이콘을 클릭하여 기존 경고를 * 편집 * 할 수도 있습니다.
7. 경고할 * 이벤트 유형 * 을 선택합니다(예: _ 획득 장치 실패 _).
8. 선택한 시간 간격 동안 선택한 유형의 중복 이벤트에 대한 알림을 표시하지 않으려면 * Snooze * 간격을 선택합니다. never_를 선택하면 이벤트가 더 이상 발생하지 않을 때까지 1분에 한 번씩 반복 알림이 수신됩니다.
9. 이벤트 알림에 대해 * 심각도 * (경고 또는 위험)를 선택합니다.
10. 이메일 알림은 기본적으로 글로벌 이메일 수신자 목록으로 전송됩니다. 또는 제공된 링크를 클릭하여 글로벌 목록을 재정의하고 특정 수신자에게 알림을 보낼 수 있습니다.
11. 저장을 클릭하여 경고를 추가합니다.

ASUP 처리 구성

모든 NetApp 제품은 자동화된 기능을 갖추고 있어 고객에게 최상의 지원을 제공합니다. 자동화된 지원(ASUP)은 사전 정의된 특정 정보를 고객 지원 팀에 주기적으로 전송합니다. NetApp에 전달할 정보와 전송 빈도를 제어할 수 있습니다.

시작하기 전에

데이터를 전송하기 전에 데이터를 전달하도록 OnCommand Insight를 구성해야 합니다.

이 작업에 대해

ASUP 데이터는 HTTPS 프로토콜을 사용하여 전달됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 설정 * 을 클릭합니다.
3. ASUP & Proxy * 탭을 클릭합니다.
4. ASUP * 섹션에서 * ASUP * 활성화 를 선택하여 ASUP 시설을 활성화하십시오.
5. 회사 정보를 변경하려면 다음 필드를 업데이트합니다.
 - * 회사 이름 *
 - * 사이트 이름 *
 - * 전송할 항목 *: 로그, 구성 데이터, 성능 데이터
6. 지정한 연결이 작동하는지 확인하려면 * 연결 테스트 * 를 클릭합니다.
7. 저장 * 을 클릭합니다.
8. Proxy* 섹션에서 * 프록시 * 활성화 여부를 선택하고 프록시 * 호스트 *, * 포트 * 및 * 사용자 * 정보를 지정합니다.
9. 지정한 프록시가 작동하는지 확인하려면 * 연결 테스트 * 를 클릭합니다.
10. 저장 * 을 클릭합니다.

AutoSupport(ASUP) 패키지에 포함된 내용

AutoSupport 패키지에는 데이터베이스 백업과 확장 정보가 들어 있습니다.

AutoSupport 패키지에는 다음이 포함됩니다.

- 재고 데이터
- 성능 데이터(ASUP에 포함할 경우)
- 데이터 원본 및 데이터 원본 설정
- 통합 팩
- 원격 획득 장치
- ASUP/프록시 설정
- 위치 설정 백업
- 보관 위치 설정
- 알림 설정
- 사용자

- 성능 정책
- 업무 엔티티 및 애플리케이션
- 장치 해상도 규칙 및 설정
- 대시보드 및 위젯
- 맞춤형 자산 페이지 대시보드 및 위젯
- 쿼리
- 주석 및 주석 규칙
- 로그
- 추가 수익 실적을
- 획득/데이터 소스 상태
- MySQL 상태
- 시스템 정보

AutoSupport 패키지에는 다음이 포함되지 않습니다.

- 보안 도구 설정/볼트 정보(별도의 CLI 프로세스를 통해 백업)
- 성능 데이터(ASUP에 포함할 것을 선택하지 않은 경우)



ASUP에 성능 데이터를 포함하려는 경우 가장 최근의 7일 데이터가 포함됩니다. 해당 기능이 활성화된 경우 나머지 데이터는 아카이브에 포함됩니다. 아카이브 데이터는 ASUP에 포함되지 않습니다.

응용 프로그램 정의

사용자 환경에서 실행 중인 특정 애플리케이션과 관련된 데이터를 추적하려면 해당 애플리케이션을 정의해야 합니다.

시작하기 전에

애플리케이션을 업무 엔티티에 연결하려면 이미 업무 엔티티를 생성해야 합니다.

이 작업에 대해

호스트, 가상 머신, 볼륨, 내부 볼륨, qtree, 공유 및 하이퍼바이저.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 응용 프로그램 * 을 선택합니다.

응용 프로그램을 정의한 후 응용 프로그램 페이지에는 응용 프로그램의 이름, 우선 순위 및 응용 프로그램과 연결된 업무 엔티티가 표시됩니다(해당하는 경우).

3. 추가 * 를 클릭합니다.

응용 프로그램 추가 대화 상자가 표시됩니다.

- 이름 * 상자에 응용 프로그램의 고유한 이름을 입력합니다.
- Priority * 를 클릭하고 해당 환경의 애플리케이션에 대한 우선 순위(중요, 높음, 중간 또는 낮음)를 선택합니다.
- 이 응용 프로그램을 업무 엔티티와 함께 사용하려면 * 업무 엔티티 * 를 클릭하고 목록에서 엔티티를 선택합니다.
- * 선택 사항 *: 볼륨 공유를 사용하지 않는 경우 * 볼륨 공유 확인 * 상자를 클릭하여 지웁니다.

이 작업을 수행하려면 보증 라이선스가 필요합니다. 각 호스트가 클러스터의 동일한 볼륨에 액세스할 수 있도록 하려면 이 옵션을 설정합니다. 예를 들어, high-availability 클러스터의 호스트는 장애 조치를 위해 동일한 볼륨에 마스킹되어야 하는 경우가 많지만, 관련 없는 애플리케이션의 호스트는 일반적으로 동일한 물리적 볼륨에 액세스할 필요가 없습니다. 또한 규정 정책에 따라 보안상의 이유로 관련 없는 응용 프로그램이 동일한 물리적 볼륨에 액세스하는 것을 명시적으로 허용하지 않을 수 있습니다.

- 저장 * 을 클릭합니다.

응용 프로그램이 응용 프로그램 페이지에 나타납니다. 애플리케이션 이름을 클릭하면 Insight에서 애플리케이션의 자산 페이지를 표시합니다.



작업을 마친 후

애플리케이션을 정의한 후 호스트, 가상 머신, 볼륨, 내부 볼륨 또는 하이퍼바이저의 자산 페이지로 이동하여 애플리케이션을 자산에 할당할 수 있습니다.

자산에 애플리케이션 할당

비즈니스 엔티티를 사용하거나 사용하지 않고 애플리케이션을 정의한 후 해당 애플리케이션을 자산과 연결할 수 있습니다.

단계


- OnCommand Insight 웹 UI에 로그인합니다.
- 다음 중 하나를 수행하여 애플리케이션을 적용할 자산(호스트, 가상 머신, 볼륨 또는 내부 볼륨)을 찾습니다.
 - Dashboard * 를 클릭하고 * Assets Dashboard * 를 선택한 다음 자산을 클릭합니다.
 - 을 클릭합니다  도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
- 자산 페이지의 * 사용자 데이터 * 섹션에서 현재 자산에 할당된 애플리케이션 이름(할당된 애플리케이션이 없을 경우 * 없음 * 이 대신 표시됨)에 커서를 놓고 클릭합니다  (응용 프로그램 편집).

선택한 자산에 대해 사용 가능한 애플리케이션 목록입니다. 현재 자산과 연결된 응용 프로그램 앞에는 확인 표시가 나타납니다.

- 검색 상자에 입력하여 응용 프로그램 이름을 필터링하거나 목록을 아래로 스크롤할 수 있습니다.
- 자산과 연결할 애플리케이션을 선택합니다.

여러 애플리케이션을 호스트, 가상 시스템 및 내부 볼륨에 할당할 수 있지만 하나의 애플리케이션만 볼륨에 할당할 수 있습니다.

-


을 클릭합니다  선택한 애플리케이션 또는 애플리케이션을 자산에 할당합니다.

응용 프로그램 이름은 사용자 데이터 섹션에 나타납니다. 응용 프로그램이 업무 엔티티와 연결되어 있으면 이 섹션에도 업무 엔티티의 이름이 표시됩니다.

응용 프로그램 편집

애플리케이션의 우선 순위, 애플리케이션과 연계된 업무 엔티티 또는 볼륨 공유 상태를 변경할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 응용 프로그램 * 을 선택합니다.
3. 편집하려는 응용 프로그램 위에 커서를 놓고 클릭합니다 .

응용 프로그램 편집 대화 상자가 표시됩니다.

4. 다음 중 하나를 수행합니다.
 - Priority * 를 클릭하고 다른 우선 순위를 선택합니다.



응용 프로그램의 이름은 변경할 수 없습니다.

- [업무 엔티티]를 클릭하고 응용 프로그램을 연결할 다른 업무 엔티티를 선택하거나 [없음]을 선택하여 응용 프로그램과 업무 엔티티의 연결을 제거합니다.
- 클릭하여 지우거나 * 볼륨 공유 확인 * 을 선택합니다.




이 옵션은 보증 라이선스가 있는 경우에만 사용할 수 있습니다.

5. 저장 * 을 클릭합니다.

응용 프로그램을 삭제하는 중입니다

사용자 환경에서 더 이상 필요하지 않은 응용 프로그램을 삭제할 수 있습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 응용 프로그램 * 을 선택합니다.
3. 삭제할 응용 프로그램 위에 커서를 놓고 클릭합니다 .

응용 프로그램을 삭제할 것인지 묻는 확인 대화 상자가 표시됩니다.

4. 확인 * 을 클릭합니다.

업무 엔티티 계층 구조

환경 데이터를 더 세밀한 수준에서 추적 및 보고할 비즈니스 엔티티를 정의할 수 있습니다.

OnCommand Insight에서 비즈니스 엔티티 계층에는 다음 수준이 포함되어 있습니다.

- * 테넌트 * 는 서비스 공급자가 주로 리소스를 NetApp과 같은 고객과 연결하는 데 사용됩니다.
- * LOB(Line of Business) * 는 회사 내 사업 부문 또는 제품 라인입니다(예: 데이터 스토리지).
- * 사업부 * 는 법률 또는 마케팅과 같은 전통적인 사업부를 나타냅니다.
- * Project * 는 종종 용량 비용 청구를 원하는 사업부 내의 특정 프로젝트를 식별하는 데 사용됩니다. 예를 들어 "특허"는 법률 부서의 프로젝트 이름일 수 있으며 "판매 이벤트"는 마케팅 부서의 프로젝트 이름일 수 있습니다. 수준 이름에는 공백이 포함될 수 있습니다.

회사 계층 구조의 디자인에 있는 모든 수준을 사용할 필요는 없습니다.

비즈니스 엔티티 계층 구조 디자인

OnCommand Insight 데이터베이스의 고정 구조가 되기 때문에 회사 구조의 요소와 비즈니스 엔티티에 표시해야 할 요소를 이해해야 합니다. 다음 정보를 사용하여 업무 엔티티를 설정할 수 있습니다. 이러한 범주의 데이터를 수집하기 위해 모든 계층 레벨을 사용할 필요는 없습니다.

단계

1. 각 업무 엔티티 계층 수준을 검토하여 해당 수준이 회사의 업무 엔티티 계층 구조에 포함되어야 하는지 확인합니다.
 - 회사가 ISP인 경우 * Tenant * 레벨이 필요하며, 고객의 자원 사용량을 추적하고자 하는 경우.
 - * 여러 제품 라인의 데이터를 추적해야 하는 경우 계층 구조에 LOB(Line of Business) * 가 필요합니다.
 - 서로 다른 부서의 데이터를 추적해야 하는 경우 * 사업부 * 가 필요합니다. 이러한 계층 수준은 한 부서가 다른 부서에서 사용하지 않는 리소스를 분리하는 데 유용합니다.
 - * Project * 레벨은 부서 내 특수 작업에 사용할 수 있습니다. 이 데이터는 회사 또는 부서의 다른 프로젝트와 비교하여 개별 프로젝트의 기술 요구 사항을 정확히 파악하고 정의하며 모니터링하는 데 유용할 수 있습니다.
2. 각 업무 엔티티를 보여 주는 차트를 만들고 엔티티 내의 모든 수준 이름을 표시합니다.
3. 계층 구조의 이름을 확인하여 OnCommand Insight 보기 및 보고서에 대한 설명이 있는지 확인합니다.
4. 각 업무 엔티티와 관련된 모든 애플리케이션을 식별합니다.

비즈니스 엔티티 생성

회사의 비즈니스 엔티티 계층 구조를 디자인한 후 응용 프로그램을 설정한 다음 비즈니스 엔티티를 응용 프로그램과 연결할 수 있습니다. 이 프로세스는 OnCommand Insight 데이터베이스에 업무 엔티티 구조를 만듭니다.

이 작업에 대해

응용 프로그램을 비즈니스 엔티티와 연결하는 것은 선택 사항이지만 이는 최선의 방법입니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 업무 엔티티 * 를 선택합니다.

사업체 페이지가 표시됩니다.

3. 을 클릭합니다  새 요소 작성을 시작합니다.

[업무 엔티티 추가] * 대화 상자가 표시됩니다.

4. 각 엔티티 수준(테넌트, 사업부, 사업부 및 프로젝트)에 대해 다음 중 하나를 수행할 수 있습니다.
 - 요소 수준 목록을 클릭하고 값을 선택합니다.
 - 새 값을 입력하고 Enter 키를 누릅니다.
 - 업무 엔티티에 엔티티 수준을 사용하지 않으려면 엔티티 수준 값을 N/A로 둡니다.
5. 저장 * 을 클릭합니다.

자산에 업무 엔티티 할당

자산에 업무 엔티티를 할당할 수 있습니다(호스트, 포트, 스토리지, 스위치, 가상 시스템, 비즈니스 엔티티를 애플리케이션에 연결하지 않고 qtree, 공유, 볼륨 또는 내부 볼륨). 그러나 해당 자산이 비즈니스 엔티티와 관련된 애플리케이션에 연결되어 있는 경우 비즈니스 엔티티가 자산에 자동으로 할당됩니다.



시작하기 전에

이미 업무 엔티티를 생성해야 합니다.

이 작업에 대해

자산에 직접 비즈니스 엔티티를 할당할 수 있지만 자산에 애플리케이션을 할당한 다음 자산에 비즈니스 엔티티를 할당하는 것이 좋습니다.


단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 업무 엔티티를 적용할 자산을 찾습니다.
 - 자산 대시보드에서 자산을 클릭합니다.
 - 을 클릭합니다  도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
3. 자산 페이지의 * 사용자 데이터 * 섹션에서 * 비즈니스 엔티티 * 옆에 * 없음 * 으로 커서를 이동한 다음 를 클릭합니다  .

사용 가능한 업무 엔티티 목록이 표시됩니다.

4. 검색 * 상자에 특정 엔티티의 목록을 필터링하거나 목록을 아래로 스크롤하거나 목록에서 비즈니스 엔티티를 선택합니다.

선택한 업무 엔티티가 애플리케이션에 연결되어 있으면 애플리케이션 이름이 표시됩니다. 이 경우 사업주명 옆에 "파생된"이라는 단어가 나타납니다. 연결된 응용 프로그램이 아닌 자산에 대해서만 엔티티를 유지하려면 응용 프로그램의 할당을 수동으로 재정의할 수 있습니다.

5. 업무 엔티티로부터 파생된 응용 프로그램을 재정의하려면 응용 프로그램 이름 위에 커서를 놓고 를 클릭합니다
 다른 업무 엔티티를 선택하고 목록에서 다른 애플리케이션을 선택합니다.


여러 자산에 비즈니스 엔티티를 할당하거나 제거합니다

수동으로 할당하거나 제거할 필요 없이 쿼리를 사용하여 여러 자산에 비즈니스 엔티티를 할당하거나 제거할 수 있습니다.


시작하기 전에

원하는 자산에 추가할 비즈니스 엔티티를 이미 만들어야 합니다.


단계

1. 새 쿼리를 만들거나 기존 쿼리를 엽니다.
2. 필요한 경우 비즈니스 엔티티를 추가할 자산을 필터링합니다.
3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다  모두 * 를 선택합니다.

작업 * 버튼이 표시됩니다.

4. 선택한 자산에 업무 엔티티를 추가하려면 을 클릭합니다 . 선택한 자산 유형에 업무 엔티티가 할당되어 있을 수 있는 경우, [업무 엔티티 추가]에 대한 메뉴 선택이 표시됩니다. 이 옵션을 선택합니다.
5. 목록에서 원하는 업무 엔티티를 선택하고 * 저장 * 을 클릭합니다.

지정한 새 업무 엔티티는 이미 자산에 할당된 모든 업무 엔티티보다 우선합니다. 자산에 애플리케이션을 할당하면 동일한 방식으로 할당된 비즈니스 엔티티도 무시됩니다. 비즈니스 엔티티를 자산으로 할당하면 해당 자산에 할당된 모든 애플리케이션도 재정의될 수 있습니다.

6. 자산에 할당된 업무 엔티티를 제거하려면 를 클릭합니다  을 클릭하고 * 업무 엔티티 제거 * 를 선택합니다.
7. 목록에서 원하는 업무 엔티티를 선택하고 * 삭제 * 를 클릭합니다.

주석 정의

회사 요구사항에 맞게 데이터를 추적하도록 OnCommand Insight을 사용자 지정할 때 자산의 수명 종료, 데이터 센터, 건물 위치, 스토리지 계층 또는 볼륨 등 데이터를 완벽하게 파악하는 데 필요한 특수 주석을 정의할 수 있습니다. 내부 볼륨 서비스 레벨을 지원합니다.

단계

1. 환경 데이터를 연결해야 하는 업계 용어를 나열하십시오.
2. 비즈니스 엔티티를 사용하여 아직 추적되지 않은 환경 데이터를 연결해야 하는 기업 용어를 나열하십시오.
3. 사용할 수 있는 기본 주석 유형을 식별합니다.

4. 만들어야 하는 사용자 지정 주석을 식별합니다.

주석을 사용하여 환경을 모니터링합니다

회사 요구 사항에 맞는 데이터를 추적하도록 OnCommand Insight를 사용자 지정할 때 `_annotations`라는 특수 메모를 정의하여 자산에 할당할 수 있습니다. 예를 들어, 자산의 수명 종료, 데이터 센터, 건물 위치, 스토리지 계층 또는 볼륨 서비스 수준과 같은 정보에 주석을 달 수 있습니다.

주석을 사용하여 환경을 모니터링하는 데 유용한 작업은 다음과 같습니다.

- 모든 주석 유형에 대한 정의를 만들거나 편집합니다.
- 자산 페이지를 표시하고 각 자산을 하나 이상의 주석과 연결합니다.

예를 들어, 자산이 임대되고 2개월 이내에 임대가 만료되는 경우 자산에 수명 종료 주석을 적용할 수 있습니다. 이렇게 하면 다른 사용자가 해당 자산을 장기간 사용하지 못하게 할 수 있습니다.

- 같은 유형의 여러 자산에 주석을 자동으로 적용하는 규칙을 작성합니다.
- 주석 가져오기 유틸리티를 사용하여 주석을 가져옵니다.
- 주석을 기준으로 자산을 필터링합니다.
- 주석을 기반으로 보고서의 데이터를 그룹화하고 해당 보고서를 생성합니다.

보고서에 대한 자세한 내용은 `_OnCommand Insight 보고 가이드`를 참조하십시오.

주석 유형 관리

OnCommand Insight는 자산 수명 주기(생일 또는 수명 종료), 건물 또는 데이터 센터 위치, 계층 등 보고서에 표시되도록 사용자 지정할 수 있는 몇 가지 기본 주석 유형을 제공합니다. 기본 주석 유형의 값을 정의하거나 사용자 정의 주석 유형을 직접 만들 수 있습니다. 나중에 이러한 값을 편집할 수 있습니다.

기본 주석 유형

OnCommandInsight는 몇 가지 기본 주석 유형을 제공합니다. 이러한 주석은 데이터를 필터링하거나 그룹화하고 데이터 보고를 필터링하는 데 사용할 수 있습니다.

다음과 같은 기본 주석 유형과 자산을 연결할 수 있습니다.

- 생일, 일몰 또는 수명 종료 등의 자산 수명 주기
- 데이터 센터, 건물 또는 바닥과 같은 장치에 대한 위치 정보
- 품질(계층), 연결된 장치(스위치 수준) 또는 서비스 수준별 자산 분류
- 핫(높은 활용도) 등의 상태

다음 표에는 기본 주석 유형이 나열되어 있습니다. 이러한 주석 이름을 필요에 맞게 편집할 수 있습니다.

주석 유형	설명	유형
-------	----	----

별칭	리소스에 대한 사용자 친화적인 이름입니다.	텍스트
생일	장치가 온라인 상태가 되거나 온라인으로 전환되는 날짜입니다.	날짜
건물	호스트, 스토리지, 스위치 및 테이프 리소스의 물리적 위치	목록
도시	호스트, 스토리지, 스위치 및 테이프 리소스의 지방자치당국 위치	목록
컴퓨팅 리소스 그룹	Host 및 VM Filesystems 데이터 소스에서 사용하는 그룹 할당입니다.	목록
대륙	호스트, 스토리지, 스위치 및 테이프 리소스의 지리적 위치	목록
국가	호스트, 스토리지, 스위치 및 테이프 리소스의 국가별 위치	목록
데이터 센터	리소스의 물리적 위치이며 호스트, 스토리지 시스템, 스위치 및 테이프에서 사용할 수 있습니다.	목록
직접 연결	스토리지 리소스가 호스트에 직접 접속되어 있으면 (예 또는 아니요)를 나타냅니다.	부울
수명 종료	예를 들어 임대가 만료되었거나 하드웨어가 폐기되는 경우 장치가 오프라인 상태가 되는 날짜입니다.	날짜
패브릭 별칭	Fabric의 사용자 친화적인 이름입니다.	텍스트
바닥	건물 바닥에 있는 장치의 위치. 호스트, 스토리지 시스템, 스위치 및 테이프에 대해 설정할 수 있습니다.	목록
하트	이미 사용량이 많은 디바이스를 정기적으로 또는 용량 임계값으로 사용 중입니다.	부울
참고	자원에 연결할 메모입니다.	텍스트

랙	리소스가 상주하는 랙입니다.	텍스트
있습니다	호스트, 스토리지, 스위치 및 테이프 리소스의 건물 또는 기타 위치 내의 공간입니다.	목록
산	네트워크의 논리 파티션입니다. 호스트, 스토리지 시스템, 테이프, 스위치 및 애플리케이션에서 사용할 수 있습니다.	목록
서비스 수준	리소스에 할당할 수 있는 지원되는 서비스 수준 집합입니다. 내부 볼륨, qtree, 볼륨에 대한 정렬 옵션 목록을 제공합니다. 서비스 수준을 편집하여 다양한 수준에 대한 성능 정책을 설정합니다.	목록
시/도	리소스가 있는 시/군/구 또는 시/군/구	목록
일몰	해당 디바이스에 새 할당을 수행할 수 없는 임계값을 설정합니다. 계획된 마이그레이션 및 기타 보류 중인 네트워크 변경에 유용합니다.	날짜
스위치 레벨	에는 스위치에 대한 범주를 설정하기 위한 미리 정의된 옵션이 포함되어 있습니다. 일반적으로 이러한 지정은 필요한 경우 편집할 수 있지만 장치의 수명 기간 동안 유지됩니다. 스위치에만 사용할 수 있습니다.	목록
계층	는 사용자 환경 내에서 서로 다른 서비스 수준을 정의하는 데 사용할 수 있습니다. 계층은 필요한 속도(예: 금 또는 은)와 같은 수준의 유형을 정의할 수 있습니다. 이 기능은 내부 볼륨, Qtree, 스토리지 어레이, 스토리지 풀 및 볼륨에서만 사용할 수 있습니다.	목록
위반 심각도입니다	중요도가 가장 높은 계층부터 가장 낮은 계층까지 위반 등급(예: 중요)의 순위를 지정합니다(예: 호스트 포트 누락 또는 이중화 누락).	목록



별칭, 데이터 센터, 핫, 서비스 레벨, 일몰, 스위치 수준, 서비스 수준, 계층 및 위반 심각성 은 시스템 수준 주석으로, 삭제하거나 이름을 바꿀 수 없습니다. 할당된 값만 변경할 수 있습니다.

주석 지정 방법

주석 규칙을 사용하여 수동으로 또는 자동으로 주석을 지정할 수 있습니다. 또한 OnCommand Insight는 자산 취득 및 상속에 대한 일부 주석을 자동으로 할당합니다. 자산에 할당한 주석은 자산 페이지의 사용자 데이터 섹션에 표시됩니다.

주석은 다음과 같은 방법으로 지정됩니다.

- 주석을 자산에 수동으로 지정할 수 있습니다.

주석을 자산에 직접 지정하면 주석이 자산 페이지에 일반 텍스트로 표시됩니다. 수동으로 할당된 주석은 항상 주석 규칙에 의해 상속되거나 할당된 주석보다 우선합니다.

- 동일한 유형의 자산에 주석을 자동으로 할당하는 주석 규칙을 생성할 수 있습니다.

주석이 규칙별로 할당된 경우 Insight는 자산 페이지의 주석 이름 옆에 규칙 이름을 표시합니다.

- Insight는 계층 레벨을 스토리지 계층 모델과 자동으로 연결하여 자산 구입 시 리소스에 스토리지 주석을 신속하게 할당할 수 있습니다.

특정 스토리지 리소스는 사전 정의된 계층(계층 1 및 계층 2)과 자동으로 연결됩니다. 예를 들어 Symmetrix 스토리지 계층은 Symmetrix 및 VMAX 제품군을 기반으로 하며 계층 1과 연결됩니다. 계층 요구 사항에 맞게 기본값을 변경할 수 있습니다. 주석을 Insight(예: 계층)에 할당하면 자산 페이지의 주석 이름 위에 커서를 놓으면 "시스템 정의"가 표시됩니다.

- 일부 리소스(자산의 하위 항목)는 자산(상위)에서 사전 정의된 계층 주석을 파생시킬 수 있습니다.

예를 들어, 주석을 스토리지에 할당할 경우 계층 주석은 모든 스토리지 풀, 내부 볼륨, 볼륨, Qtree 및 스토리지에 속한 공유에 의해 파생됩니다. 스토리지의 내부 볼륨에 다른 주석이 적용되는 경우 주석은 이후에 모든 볼륨, qtree 및 공유에 의해 파생됩니다. 자산 페이지의 주석 이름 옆에 "Deribed"가 나타납니다.


주석과 비용 연관

비용 관련 보고서를 실행하기 전에 비용을 서비스 수준, 스위치 수준 및 계층 시스템 수준 주석과 연계해야 합니다. 그러면 운영 및 복제 용량의 실제 사용량을 기준으로 스토리지 사용자에게 비용 청구를 수행할 수 있습니다. 예를 들어, 계층 레벨의 경우 골드 및 실버 등급 값을 가지고 실버 계층보다 더 높은 비용을 골드 계층에 할당할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 관리를 클릭하고 * 주석 * 을 선택합니다.


주석 페이지가 표시됩니다.

3. 서비스 수준, 스위치 수준 또는 계층 주석 위에 커서를 놓고 를 클릭합니다 .

Edit Annotation(주석 편집) 대화 상자가 표시됩니다.

4. 비용 * 필드에 기존 수준의 값을 입력합니다.

계층 및 서비스 수준 주식에는 각각 자동 계층 및 오브젝트 스토리지 값이 있으며, 이 값은 제거할 수 없습니다.

5. 을 클릭합니다  를 눌러 수준을 추가합니다.
6. 작업을 마치면 * 저장 * 을 클릭합니다.

사용자 정의 주식 작성

주식을 사용하여 비즈니스 요구에 맞는 맞춤형 비즈니스 관련 데이터를 자산에 추가할 수 있습니다. OnCommand Insight에서 기본 주식 집합을 제공하는 경우 다른 방법으로 데이터를 볼 수 있습니다. 사용자 지정 주식의 데이터는 스위치 제조업체, 포트 수 및 성능 통계와 같이 이미 수집된 장치 데이터를 보완합니다. 주식을 사용하여 추가하는 데이터는 Insight에서 검색되지 않습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주식 * 을 선택합니다.

주식 페이지에는 주식 목록이 표시됩니다.

3. 을 클릭합니다 .

주식 추가 * 대화 상자가 표시됩니다.

4. 이름 * 및 * 설명 * 필드에 이름과 설명을 입력합니다.

이 필드에는 최대 255자까지 입력할 수 있습니다.



점 ""으로 시작하거나 끝나는 주식 이름. 지원되지 않습니다.

5. Type * 을 클릭한 다음 이 주식에 허용되는 데이터 유형을 나타내는 다음 옵션 중 하나를 선택합니다.

- 부울

그러면 예 및 아니요 선택 항목이 있는 드롭다운 목록이 만들어집니다 예를 들어 "Direct Attached" 주식은 Boolean입니다.

- 날짜

이렇게 하면 날짜가 들어 있는 필드가 만들어집니다. 예를 들어, 주식이 날짜가 될 경우 이를 선택합니다.

- 목록

이렇게 하면 다음 중 하나가 생성될 수 있습니다.

- 드롭다운 고정 목록

다른 사용자가 장치에 이 주식 유형을 할당하는 경우 목록에 값을 더 추가할 수 없습니다.

- 드롭다운 유연한 목록

이 목록을 만들 때 * Add new values on the fly * 옵션을 선택하면 다른 사용자가 장치에 이 주식 유형을 할당할 때 목록에 더 많은 값을 추가할 수 있습니다.

- 번호

이렇게 하면 주석을 지정하는 사용자가 숫자를 입력할 수 있는 필드가 생성됩니다. 예를 들어, 주식 유형이 ""바닥""인 경우 사용자는 ""숫자""의 값 유형을 선택하고 바닥 번호를 입력할 수 있습니다.

- 텍스트

그러면 자유 형식 텍스트를 허용하는 필드가 만들어집니다. 예를 들어, 주식 유형으로 ""Language""를 입력하고 값 유형으로 ""Text""를 선택한 다음 언어를 값으로 입력할 수 있습니다.



유형을 설정하고 변경 사항을 저장한 후에는 주식 유형을 변경할 수 없습니다. 유형을 변경해야 하는 경우 주석을 삭제하고 새 주석을 만들어야 합니다.

6. 주식 유형으로 목록 을 선택한 경우 다음을 수행합니다.

- a. 자산 페이지에서 주식에 더 많은 값을 추가할 수 있는 기능을 원하는 경우 * 즉시 새 값 추가 * 를 선택하여 유연한 목록을 만듭니다.

예를 들어 자산 페이지에 있고 자산에는 Detroit, Tampa 및 Boston 값이 있는 City 주석이 있다고 가정해 보겠습니다. 빠른 실행 시 새 값 추가 * 옵션을 선택한 경우 주식 페이지로 이동하여 추가할 필요 없이 자산 페이지에서 샌프란시스코 및 시카고와 같은 도시에 직접 추가 값을 추가할 수 있습니다. 이 옵션을 선택하지 않으면 주석을 적용할 때 새 주식 값을 추가할 수 없습니다. 그러면 고정 목록이 생성됩니다.

- b. 값 * 및 * 설명 * 필드에 값과 이름을 입력합니다.

- c. 을 클릭합니다  를 눌러 추가 값을 추가합니다.

- d. 을 클릭합니다  를 눌러 값을 제거합니다.

7. 저장 * 을 클릭합니다.

주석이 주식 페이지의 목록에 나타납니다.

- 관련 정보 *

"사용자 데이터 가져오기 및 내보내기"


자산에 주식 수동 할당

자산에 주석을 지정하면 비즈니스와 관련된 방식으로 자산을 정렬, 그룹화 및 보고할 수 있습니다. 주식 규칙을 사용하여 특정 유형의 자산에 주석을 자동으로 할당할 수 있지만 자산 페이지를 사용하여 개별 자산에 주석을 할당할 수 있습니다.


시작하기 전에

지정할 주석을 만들어야 합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 주석을 적용할 자산을 찾습니다.
 - 자산 대시보드에서 자산을 클릭합니다.
 - 을 클릭합니다  도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산의 유형 또는 이름을 입력한 다음 표시되는 목록에서 자산을 선택합니다.


자산 페이지가 표시됩니다.

3. 자산 페이지의 * 사용자 데이터 * 섹션에서 를 클릭합니다 .

주석 추가 대화 상자가 표시됩니다.

4. Annotation(주석) * 을 클릭하고 목록에서 주석을 선택합니다.
5. 값 * 을 클릭하고 선택한 주석 유형에 따라 다음 중 하나를 수행합니다.
 - 주석 유형이 목록, 날짜 또는 부울인 경우 목록에서 값을 선택합니다.
 - 주석 유형이 텍스트인 경우 값을 입력합니다.

6. 저장 * 을 클릭합니다.

7. 주석을 지정한 후 주석 값을 변경하려면 을 클릭합니다  다른 값을 선택합니다.

주석이 * 주석 지정 시 동적으로 값 추가 * 옵션을 선택한 목록 유형인 경우 기존 값을 선택하는 것 외에도 새 값을 추가하도록 입력할 수 있습니다.


주석 수정

주석의 이름, 설명 또는 값을 변경하거나 더 이상 사용하지 않을 주석을 삭제할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

주석 페이지가 표시됩니다.

3. 편집할 주석 위에 커서를 놓고 클릭합니다 .

Edit Annotation(주석 편집) * 대화 상자가 표시됩니다.


4. 주석을 다음과 같이 수정할 수 있습니다.


- a. 이름, 설명 또는 둘 모두를 변경합니다.

그러나 이름과 설명 모두에 최대 255자를 입력할 수 있으며 주석 유형은 변경할 수 없습니다. 또한 시스템 수준 주석의 경우 이름이나 설명을 변경할 수 없지만, 주석이 목록 유형인 경우 값을 추가하거나 제거할 수 있습니다.



사용자 지정 주석이 데이터 웨어하우스에 게시되고 이름을 바꾸면 내역 데이터가 손실됩니다.

a. 목록 유형의 주석에 다른 값을 추가하려면  을 클릭합니다.

b. 목록 유형의 주석에서 값을 제거하려면  를 클릭합니다.

주석 값이 주석 규칙, 쿼리 또는 성능 정책에 포함된 주석과 관련된 경우 주석 값을 삭제할 수 없습니다.

5. 작업을 마치면 * 저장 * 을 클릭합니다.

작업을 마친 후

데이터 웨어하우스에서 주석을 사용하려는 경우 데이터 웨어하우스에서 주석을 강제로 업데이트해야 합니다. OnCommand Insight 데이터 웨어하우스 관리 가이드 _ 를 참조하십시오.

주석 삭제

더 이상 사용하지 않을 주석을 삭제할 수 있습니다. 시스템 수준 주석 또는 주석 규칙, 쿼리 또는 성능 정책에 사용되는 주석은 삭제할 수 없습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.

2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

주석 페이지가 표시됩니다.

3. 삭제할 주석 위에 커서를 놓고  를 클릭합니다.

확인 대화 상자가 표시됩니다.

4. 확인 * 을 클릭합니다.

주석 규칙을 사용하여 자산에 주석 지정

사용자가 정의한 기준에 따라 자산에 주석을 자동으로 할당하려면 주석 규칙을 구성합니다. OnCommand Insight는 이러한 규칙에 따라 자산에 주석을 할당합니다. 또한 Insight에서는 두 가지 기본 주석 규칙을 제공합니다. 이 규칙은 필요에 맞게 수정하거나 사용하지 않으려는 경우 제거할 수 있습니다.

기본 스토리지 주석 규칙

스토리지 주석을 리소스에 빠르게 할당할 수 있도록 OnCommand Insight에는 21개의 기본 주석 규칙이 포함되어 있으며, 이 규칙은 계층 레벨을 스토리지 계층 모델과 연결합니다. 모든 스토리지 리소스는 귀사 환경에서 자산을 획득할 때 계층에 자동으로 연결됩니다.

기본 주석 규칙은 다음과 같은 방법으로 계층 주석을 적용합니다.

- 계층 1, 스토리지 품질 계층

Tier 1 주석은 EMC(Symmetrix), HDS(HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM(DS8000), NetApp(FAS6000 또는 FAS6200), Violin(Memory).

- 계층 2, 스토리지 품질 계층

Tier 2 주석은 HP(3PAR StoreServ 또는 EVA), EMC(CLARiiON), HDS(AMS 또는 D800), IBM(XIV), NetApp(FAS3000, FAS3100 및 FAS3200) 등의 공급업체 및 지정된 제품군에 적용됩니다.

이러한 규칙의 기본 설정을 계층 요구 사항에 맞게 편집하거나 필요하지 않은 경우 제거할 수 있습니다.

주석 규칙 작성

개별 자산에 주석을 수동으로 적용하는 대신 주석 규칙을 사용하여 여러 자산에 주석을 자동으로 적용할 수 있습니다. Insight에서 주석 규칙을 평가할 때 개별 자산 페이지에 수동으로 설정된 주석이 규칙 기반 주석보다 우선합니다.

시작하기 전에

주석 규칙에 대한 쿼리를 만들어야 합니다.

이 작업에 대해

규칙을 만드는 동안 주석 유형을 편집할 수 있지만, 미리 유형을 정의해야 합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 을 클릭합니다  Add .

규칙 추가 대화 상자가 표시됩니다.

4. 다음을 수행합니다.
 - a. 이름 * 상자에 규칙을 설명하는 고유한 이름을 입력합니다.

이 이름은 주석 규칙 페이지에 표시됩니다.
 - b. Query * 를 클릭하고 OnCommand Insight가 에셋에 주석을 적용하는 데 사용해야 하는 쿼리를 선택합니다.
 - c. Annotation(주석) * 을 클릭하고 적용할 주석을 선택합니다.
 - d. 값 * 을 클릭하고 주석 값을 선택합니다.

예를 들어 주석으로 생일 을 선택한 경우 값의 날짜를 지정합니다.

5. 저장 * 을 클릭합니다.
6. 모든 규칙을 즉시 실행하려면 * 모든 규칙 실행 * 을 클릭합니다. 그렇지 않으면 규칙들이 정기적으로 예약된 간격으로 실행됩니다.

주석 규칙 우선 순위 설정

기본적으로 OnCommand Insight에서는 주석 규칙을 순차적으로 평가합니다. 그러나 Insight에서 특정 순서로 규칙을 평가하려면 OnCommand Insight에서 주석 규칙을 평가하는 순서를 구성할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 주석 규칙 위에 커서를 놓습니다.

우선 순위 화살표가 규칙의 오른쪽에 나타납니다.

4. 목록에서 규칙을 위 또는 아래로 이동하려면 위쪽 화살표 또는 아래쪽 화살표를 클릭합니다.

기본적으로 새 규칙은 규칙 목록에 순차적으로 추가됩니다. Insight에서 주석 규칙을 평가할 때 개별 자산 페이지에 수동으로 설정된 주석이 규칙 기반 주석보다 우선합니다.

주석 규칙 수정

주석 규칙을 수정하여 규칙 이름, 주석, 주석 값 또는 규칙과 연결된 쿼리를 변경할 수 있습니다.

단계


1. OnCommand Insightfob UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 수정할 규칙을 찾습니다.

- 주석 규칙 페이지에서 필터 상자에 값을 입력하여 주석 규칙을 필터링할 수 있습니다.
- 페이지에 맞는 규칙보다 더 많은 규칙이 있는 경우 페이지 번호를 클릭하여 페이지별로 주석 규칙을 찾아봅니다.

4. 다음 중 하나를 수행하여 * 규칙 편집 * 대화 상자를 표시합니다.

- 주석 규칙 페이지에 있는 경우 주석 규칙 위에 커서를 놓고  을 클릭합니다.
- 자산 페이지에 있는 경우 규칙과 연결된 주석 위에 커서를 놓고 규칙 이름이 표시되면 커서를 규칙 이름 위에 놓은 다음 규칙 이름을 클릭합니다.

5. 필요한 내용을 변경하고 * Save * 를 클릭합니다.


주석 규칙 삭제

규칙이 더 이상 네트워크의 개체를 모니터링할 필요가 없는 경우 주석 규칙을 삭제할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 규칙 * 을 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 삭제할 규칙을 찾습니다.
 - 주석 규칙 페이지에서 필터 상자에 값을 입력하여 주석 규칙을 필터링할 수 있습니다.
 - 한 페이지에 맞는 규칙보다 더 많은 규칙이 있는 경우 페이지 번호를 클릭하여 페이지별로 주석 규칙을 찾아봅니다.
4. 삭제할 규칙 위에 커서를 놓은 다음 을 클릭합니다 .

규칙을 삭제할 것인지 묻는 확인 메시지가 표시됩니다.

5. 확인 * 을 클릭합니다.

주석 값 불러오기

CSV 파일에서 SAN 객체(예: 스토리지, 호스트, 가상 머신)에 대한 주석을 유지하는 경우 해당 정보를 OnCommand Insight로 가져올 수 있습니다. 응용 프로그램, 사업체 또는 계층 및 건물 등의 주석을 가져올 수 있습니다.

이 작업에 대해

다음 규칙이 적용됩니다.

- 주석 값이 비어 있으면 해당 주석이 개체에서 제거됩니다.
- 볼륨 또는 내부 볼륨에 주석을 달 때 개체 이름은 대시 및 화살표(->) 구분 기호를 사용하여 스토리지 이름과 볼륨 이름의 조합입니다.

```
<storage_name>-><volume_name>
```

- 스토리지, 스위치 또는 포트에 주석이 추가된 경우 응용 프로그램 열은 무시됩니다.
- Tenant, Line_of_Business, Business_Unit 및 Project 열은 업무 엔티티를 만듭니다.

모든 값은 비워 둘 수 있습니다. 응용 프로그램이 이미 입력 값과 다른 업무 엔티티와 연결되어 있는 경우 응용 프로그램은 새 업무 엔티티에 할당됩니다.

가져오기 유틸리티에서 지원되는 개체 유형 및 키는 다음과 같습니다.

유형	키
호스트	id-><id> 또는 <Name> 또는 <IP>

VM	id-><id> 또는 <Name>
스토리지 풀	id-><id> 또는 '<Storage_name>'를 클릭합니다<Storage_Pool_name>
내부 볼륨	id-><id> 또는 '<Storage_name>'를 클릭합니다<Internal_volume_name>
볼륨	id-><id> 또는 '<Storage_name>'를 클릭합니다<Volume_name>
스토리지	id-><id> 또는 <Name> 또는 <IP>
스위치	id-><id> 또는 <Name> 또는 <IP>
포트	id-><id> 또는 <WWN>
공유	id-><id> 또는 <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree> 기본 qtree가 있는 경우 선택 사항입니다.
qtree입니다	id-><id> 또는 <Storage Name>-><Internal Volume Name>-><Qtree Name>

CSV 파일은 다음 형식을 사용해야 합니다.

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

단계

1. Insight 웹 UI에 로그인합니다.

2. Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.

문제 해결 페이지가 표시됩니다.

3. 페이지의 * 기타 작업 섹션 * 에서 * OnCommand Insight 포털 * 링크를 클릭합니다.

4. Insight Connect API * 를 클릭합니다.

5. 포털에 로그인합니다.

6. 주석 가져오기 유틸리티 * 를 클릭합니다.

7. 를 저장합니다 .zip 파일을 압축 해제하고 를 읽습니다 readme.txt 추가 정보 및 샘플을 위한 파일.

8. CSV 파일을 와 동일한 폴더에 저장합니다 .zip 파일.

9. 명령줄 창에서 다음을 입력합니다.

```
java -jar rest-import-utility.jar [-username] [-password]
[-server name or IP address] [-batch size] [-ccase
sensitive:true/false]
[-lextra logging:true/false] csv filename
```

추가 로깅을 사용하는 -l 옵션과 대/소문자 구분을 사용하는 -c 옵션은 기본적으로 false로 설정됩니다. 따라서 피처를 사용하려는 경우에만 지정해야 합니다.



옵션과 해당 값 사이에는 공백이 없습니다.



다음 키워드는 예약되며 사용자가 주석 이름으로 지정할 수 없습니다. - Application - Application_Priority - Tenant - Line_of_Business - Business_Unit - 예약된 키워드 중 하나를 사용하여 주석 유형을 가져오려고 하면 프로젝트 오류가 생성됩니다. 이러한 키워드를 사용하여 주석 이름을 만든 경우, 불러오기 유틸리티 도구가 올바르게 작동할 수 있도록 주석을 수정해야 합니다.



주석 가져오기 유틸리티를 사용하려면 Java 8 또는 Java 11이 필요합니다. 가져오기 유틸리티를 실행하기 전에 이 중 하나가 설치되어 있는지 확인하십시오. 최신 OpenJDK 11을 사용하는 것이 좋습니다.

쿼리를 사용하여 여러 자산에 주석 할당

자산 그룹에 주석을 할당하면 쿼리 또는 대시보드에서 관련 자산을 보다 쉽게 식별하거나 사용할 수 있습니다.

시작하기 전에

자산에 지정하려는 주석이 이미 생성되어 있어야 합니다.

이 작업에 대해

쿼리를 사용하여 여러 자산에 주석을 할당하는 작업을 단순화할 수 있습니다. 예를 들어 특정 데이터 센터 위치의 모든

어레이에 사용자 지정 주소 주석을 할당하려는 경우

단계

1. 새 쿼리를 만들어 주석을 할당할 자산을 식별합니다. 쿼리 * > * + 새 쿼리 * 를 클릭합니다.
2. Search for... * 드롭다운에서 * Storage * 를 선택합니다. 표시된 저장소 목록을 더 좁히도록 필터를 설정할 수 있습니다.
3. 표시된 저장소 목록에서 저장소 이름 옆의 확인란을 클릭하여 하나 이상의 저장소 를 선택합니다. 목록 상단의 기본 확인란을 클릭하여 표시된 모든 저장소를 선택할 수도 있습니다.
4. 원하는 저장소를 모두 선택한 경우 * Actions * > * Edit Annotation * 을 클릭합니다.

주석 추가 대화 상자가 표시됩니다.

5. 저장소에 할당할 * 주석 * 및 * 값 * 을 선택하고 * 저장 * 을 클릭합니다.

해당 주석의 열을 표시하는 경우 선택한 모든 저장소에 표시됩니다.

6. 이제 주석을 사용하여 위젯 또는 쿼리의 저장소를 필터링할 수 있습니다. 위젯에서 다음을 수행할 수 있습니다.
 - a. 대시보드를 만들거나 기존 대시보드를 엽니다. 변수 * 를 추가하고 위의 저장소에 설정한 주석을 선택합니다. 변수가 대시보드에 추가됩니다.
 - b. 방금 추가한 변수 필드에서 * any * 를 클릭하고 필터링할 적절한 값을 입력합니다. 체크 표시를 클릭하여 변수 값을 저장합니다.
 - c. 위젯을 추가합니다. 위젯의 쿼리에서 필터 기준 + 단추를 클릭하고 목록에서 적절한 주석을 선택합니다.
 - d. 아무 * 나 * 를 클릭하고 위에서 추가한 주석 변수를 선택합니다. 작성한 변수는 ""\$로 시작하고 드롭다운에 표시됩니다.
 - e. 원하는 다른 필터 또는 필드를 설정한 다음 위젯이 원하는 대로 사용자 지정되면 * 저장 * 을 클릭합니다.

대시보드의 위젯에는 주석을 할당한 저장소에 대한 데이터만 표시됩니다.

자산 쿼리 중

쿼리를 사용하면 사용자 선택 기준(주석 및 성능 메트릭)에 따라 사용자 환경의 자산을 세분화된 수준으로 검색하여 네트워크를 모니터링하고 문제를 해결할 수 있습니다. 또한 자산에 주석을 자동으로 할당하는 주석 규칙에는 쿼리가 필요합니다.

쿼리 및 대시보드에 사용되는 자산

Insight 쿼리 및 대시보드 위젯은 다양한 자산 유형과 함께 사용할 수 있습니다

쿼리, 대시보드 위젯 및 사용자 지정 자산 페이지에서 다음 자산 유형을 사용할 수 있습니다. 필터, 식 및 표시에 사용할 수 있는 필드와 카운터는 자산 유형에 따라 달라집니다. 일부 자산은 일부 위젯 유형에 사용할 수 없습니다.

- 응용 프로그램
- 데이터 저장소
- 디스크

- 패브릭
- 일반 장치
- 호스트
- 내부 볼륨
- iSCSI 세션
- iSCSI 네트워크 포털
- 경로
- 포트
- qtree입니다
- 할당량
- 공유
- 스토리지
- 스토리지 노드
- 스토리지 풀
- 스위치
- 테이프
- VMDK입니다
- 가상 머신
- 볼륨
- Zone(영역)
- 존 구성원

쿼리 만들기

환경 내의 자산을 세분화된 수준으로 검색할 수 있도록 쿼리를 만들 수 있습니다. 쿼리를 사용하면 필터를 추가한 다음 결과를 정렬하여 하나의 뷰에서 인벤토리 및 성능 데이터를 볼 수 있으므로 데이터를 분류할 수 있습니다.

이 작업에 대해

예를 들어, 볼륨에 대한 쿼리를 생성하고, 선택한 볼륨과 연결된 특정 저장소를 찾기 위한 필터를 추가하고, 필터를 추가하여 선택한 저장소의 계층 1과 같은 특정 주석을 찾을 수 있습니다. 마지막으로 IOPS-Read(IO/s)가 25보다 큰 모든 스토리지를 찾기 위해 다른 필터를 추가합니다. 결과가 표시되면 쿼리와 관련된 정보 열을 오름차순 또는 내림차순으로 정렬할 수 있습니다.

자산을 취득하거나 주석 또는 응용 프로그램 할당을 만드는 새 데이터 원본이 추가되면 쿼리를 인덱싱한 후 정기적으로 예약된 간격으로 이러한 자산, 주석 또는 응용 프로그램을 쿼리할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.

2. 쿼리 * 를 클릭하고 * + 새 쿼리 * 를 선택합니다.

3. 자원 유형 선택 * 을 클릭하고 자산 유형을 선택합니다.

쿼리에 대해 자원을 선택하면 여러 기본 열이 자동으로 표시됩니다. 이러한 열을 제거하거나 언제든지 새 열을 추가할 수 있습니다.

4. 이름 * 텍스트 상자에 자산 이름을 입력하거나 자산 이름을 기준으로 필터링할 텍스트 부분을 입력합니다.

다음 중 하나만 사용하거나 조합하여 새 쿼리 페이지의 텍스트 상자에서 검색을 구체화할 수 있습니다.


- 별표를 사용하면 모든 항목을 검색할 수 있습니다. 예를 들면, 다음과 같습니다. vol*rhel ""vol""로 시작하고 ""rhel""으로 끝나는 모든 리소스를 표시합니다.
- 물음표를 사용하면 특정 수의 문자를 검색할 수 있습니다. 예를 들면, 다음과 같습니다. BOS-PRD??-S12 BOS-PRD12-S12, BOS-PRD13-S12 등을 표시합니다.
- 또는 연산자를 사용하여 여러 요소를 지정할 수 있습니다. 예를 들면, 다음과 같습니다. FAS2240 OR CX600 OR FAS3270 여러 스토리지 모델을 찾습니다.
- NOT 연산자를 사용하면 검색 결과에서 텍스트를 제외할 수 있습니다. 예를 들면, 다음과 같습니다. NOT EMC* "EMC"로 시작하지 않는 모든 항목을 찾습니다. 을 사용할 수 있습니다 NOT * 값이 없는 필드를 표시합니다.

5. 을 클릭합니다  를 눌러 자산을 표시합니다.

6. 조건을 추가하려면 을 클릭합니다  다음 중 하나를 수행합니다.

- 특정 기준을 검색하여 입력한 다음 선택합니다.
- 목록을 아래로 스크롤하여 기준을 선택합니다.
- IOPS-읽기(IO/s)와 같은 성능 메트릭을 선택한 경우 값 범위를 입력합니다. Insight에서 제공하는 기본 주석은 로 표시됩니다 🗨️ 즉, 이름이 중복된 주석이 있을 수 있습니다.

조건 및 목록의 쿼리 결과에 대한 열이 쿼리 결과 목록에 추가됩니다.

7. 필요에 따라 를 클릭할 수도 있습니다  쿼리 결과에서 주석 또는 성능 메트릭을 제거합니다.

예를 들어 쿼리에 데이터 저장소의 최대 지연 시간 및 최대 처리량이 표시되고 쿼리 결과 목록에 최대 지연 시간만을 표시하려면 이 단추를 클릭하고 * Throughput - Max * 확인란의 선택을 취소합니다. Throughput-Max(MB/s) 열이 쿼리 결과 목록에서 제거됩니다.



쿼리 결과 테이블에 표시되는 열 수에 따라 추가된 열을 추가로 볼 수 없을 수도 있습니다. 원하는 열이 표시될 때까지 하나 이상의 열을 제거할 수 있습니다.

8. 저장 * 을 클릭하고 쿼리 이름을 입력한 다음 * 저장 * 을 다시 클릭합니다.

관리자 역할이 있는 계정이 있는 경우 사용자 지정 대시보드를 만들 수 있습니다. 사용자 지정 대시보드는 위젯 라이브러리의 모든 위젯으로 구성될 수 있으며, 이 중 일부는 사용자 지정 대시보드에서 쿼리 결과를 나타낼 수 있습니다. 사용자 지정 대시보드에 대한 자세한 내용은 _OnCommand Insight 시작 가이드_를 참조하십시오.

- 관련 정보 *

["사용자 데이터 가져오기 및 내보내기"](#)

쿼리 보기

쿼리를 보고 자산을 모니터링하고 쿼리에 자산과 관련된 데이터가 표시되는 방식을 변경할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.
3. 다음 중 하나를 실행하여 쿼리가 표시되는 방식을 변경할 수 있습니다.
 - 필터 * 상자에 텍스트를 입력하여 특정 쿼리를 표시할 수 있습니다.
 - 열 머리글의 화살표를 클릭하여 쿼리 테이블의 열 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다.
 - 열 크기를 조정하려면 파란색 막대가 나타날 때까지 열 머리글 위로 마우스를 가져갑니다. 마우스를 막대 위에 놓고 오른쪽이나 왼쪽으로 끕니다.
 - 열을 이동하려면 열 머리글을 클릭하고 오른쪽 또는 왼쪽으로 끕니다.
 - 쿼리 결과를 스크롤할 때 Insight에서 자동으로 데이터 원본을 폴링하므로 결과가 변경될 수 있습니다. 이로 인해 일부 항목이 누락되거나 정렬 방식에 따라 일부 항목이 순서대로 표시되지 않을 수 있습니다.


쿼리 결과를 **.csv** 파일로 내보내는 중입니다

쿼리 결과를 **.csv** 파일로 내보내 데이터를 다른 응용 프로그램으로 가져올 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

3. 쿼리를 클릭합니다.
4. 을 클릭합니다  쿼리 결과를 로 내보냅니다. CSV 파일.
5. 다음 중 하나를 수행합니다.

- Open with * 를 클릭한 다음 * OK * 를 클릭하여 Microsoft Excel로 파일을 열고 파일을 특정 위치에 저장합니다.
- 파일 저장 * 을 클릭한 다음 * 확인 * 을 클릭하여 파일을 다운로드 폴더에 저장합니다. 표시된 열의 속성만 내보내집니다. 표시되는 일부 열, 특히 복잡한 중첩 관계의 일부인 열은 내보내지지 않습니다.



자산 이름에 심표가 나타나면 자산 이름과 올바른 .csv 형식을 유지하면서 내보내기가 따옴표로 이름을 묶습니다.

+ 쿼리 결과를 내보낼 때 결과 테이블의 * 모든 * 행이 화면에서 선택 또는 표시된 행이 아닌 최대 10,000개 행까지 내보내진다는 점에 유의하십시오.

를 누릅니다

Excel에서 내보낸 .csv 파일을 열 때 NN:NN(두 자리 뒤에 콜론이 두 자리 더 오는 경우) 형식의 개체 이름이나 기타 필드가 있으면 Excel에서 해당 이름을 텍스트 형식 대신 시간 형식으로 해석하는 경우가 있습니다. 이로 인해 Excel에서 해당 열에 잘못된 값이 표시될 수 있습니다. 예를 들어 "81:45"라는 이름의 개체는 Excel에서 "81:45:00"으로 표시됩니다. 이 문제를 해결하려면 다음 단계를 사용하여 .csv를 Excel로 가져옵니다.

를 누릅니다



- Open a new sheet in Excel.
 - On the "Data" tab, choose "From Text".
 - Locate the desired .CSV file and click "Import".
 - In the Import wizard, choose "Delimited" and click Next.
 - Choose "Comma" for the delimiter and click Next.
 - Select the desired columns and choose "Text" for the column data format.
 - Click Finish.
- Your objects should show in Excel in the proper format.

를 누릅니다



쿼리 수정

쿼리 중인 자산에 대한 검색 기준을 변경하려는 경우 쿼리와 연결된 조건을 변경할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

3. 쿼리 이름을 클릭합니다.
4. 쿼리에서 조건을 제거하려면 을 클릭합니다 .
5. 쿼리에 조건을 추가하려면 을 클릭합니다  을 클릭하고 목록에서 조건을 선택합니다.
6. 다음 중 하나를 수행합니다.
 - 저장 * 을 클릭하여 처음에 사용된 이름으로 쿼리를 저장합니다.
 - 다른 이름으로 저장을 클릭하여 쿼리를 다른 이름으로 저장합니다.
 - 처음에 사용한 쿼리 이름을 변경하려면 * 이름 바꾸기 * 를 클릭합니다.
 - 쿼리 이름을 처음 사용한 이름으로 다시 변경하려면 * 되돌리기 * 를 클릭합니다.

쿼리를 삭제하는 중입니다


더 이상 자산에 대한 유용한 정보를 수집하지 않을 경우 쿼리를 삭제할 수 있습니다. 쿼리가 주식

규칙에 사용되는 경우 삭제할 수 없습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

3. 삭제할 쿼리 위에 커서를 놓고 클릭합니다 .

쿼리를 삭제할 것인지 묻는 확인 메시지가 표시됩니다.

4. 확인 * 을 클릭합니다.

자산에 여러 애플리케이션을 할당하거나 자산에서 여러 애플리케이션을 제거합니다

수동으로 할당하거나 제거할 필요 없이 쿼리를 사용하여 여러 응용 프로그램을 자산에 할당하거나 자산에서 제거할 수 있습니다.

시작하기 전에

편집할 모든 자산을 찾는 쿼리를 이미 만들어야 합니다.


단계

1. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.


쿼리 페이지가 표시됩니다.

2. 자산을 찾는 쿼리의 이름을 클릭합니다.

쿼리와 연결된 자산 목록이 표시됩니다.

3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다  | 모두 * 를 선택합니다.


작업 * 버튼이 표시됩니다.

4. 선택한 자산에 애플리케이션을 추가하려면 을 클릭합니다  을 클릭하고 * 응용 프로그램 편집 * 을 선택합니다.

- a. 응용 프로그램 * 을 클릭하고 하나 이상의 응용 프로그램을 선택합니다.

호스트, 내부 볼륨 및 가상 머신에 대해 여러 애플리케이션을 선택할 수 있지만, 볼륨에 대해 하나의 애플리케이션만 선택할 수 있습니다.

- b. 저장 * 을 클릭합니다.

5. 자산에 할당된 애플리케이션을 제거하려면 를 클릭합니다  을 클릭하고 * 응용 프로그램 제거 * 를 선택합니다.

- a. 제거할 응용 프로그램을 선택합니다.

b. 삭제 * 를 클릭합니다.

할당한 모든 새 응용 프로그램은 다른 자산에서 파생된 자산의 모든 응용 프로그램을 재정의합니다. 예를 들어, 볼륨은 호스트에서 애플리케이션을 상속하고 새 애플리케이션이 볼륨에 할당되면 새 애플리케이션이 파생된 애플리케이션보다 우선합니다.

자산에서 여러 주식 편집 또는 제거

수동으로 편집하거나 제거할 필요 없이 쿼리를 사용하여 자산에 대한 여러 주식을 편집하거나 자산에서 여러 주식을 제거할 수 있습니다.

시작하기 전에

편집하려는 모든 자산을 찾는 쿼리를 이미 만들어야 합니다.

단계

1. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

2. 자산을 찾는 쿼리의 이름을 클릭합니다.

쿼리와 연결된 자산 목록이 표시됩니다.

3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다 ☐ ▼ 모두 * 를 선택합니다.

작업 * 버튼이 표시됩니다.

4. 자산에 주식을 추가하거나 자산에 할당된 주식 값을 편집하려면 을 클릭합니다 **Actions ▼** 을 클릭하고 * 주식 편집 * 을 선택합니다.

a. Annotation(주식) * 을 클릭하고 값을 변경할 주식을 선택하거나 새 주식을 선택하여 모든 자산에 할당합니다.

b. 값 * 을 클릭하고 주식 값을 선택합니다.

c. 저장 * 을 클릭합니다.

5. 자산에 할당된 주식을 제거하려면 를 클릭합니다 **Actions ▼** 을 클릭하고 * 주식 제거 * 를 선택합니다.

a. Annotation(주식) * 을 클릭하고 자산에서 제거할 주식을 선택합니다.

b. 삭제 * 를 클릭합니다.

테이블 값 복사 중

테이블의 값을 복사하여 검색 상자 또는 다른 응용 프로그램에서 사용할 수 있습니다.

이 작업에 대해

테이블 또는 쿼리 결과에서 값을 복사하는 데 사용할 수 있는 두 가지 방법이 있습니다.

단계

1. 방법 1: 마우스로 원하는 텍스트를 강조 표시하고 복사한 다음 검색 필드 또는 다른 응용 프로그램에 붙여 넣습니다.
2. 방법 2: 길이가 테이블 열 너비를 초과하는 단일 값 필드의 경우 줄임표(...)로 표시되며 필드 위로 마우스를 가져가서 클립보드 아이콘을 클릭합니다. 검색 필드 또는 기타 응용 프로그램에서 사용할 수 있도록 값이 클립보드에 복사됩니다.

자산에 대한 링크인 값만 복사할 수 있습니다. 단일 값(예: 비목록)이 포함된 필드에만 복사 아이콘이 있습니다.

성능 정책 관리

OnCommand Insight를 사용하면 성능 정책을 생성하여 네트워크를 모니터링하여 다양한 임계값을 설정할 수 있으며, 임계값을 초과할 경우 경고를 발생시킬 수 있습니다. 성능 정책을 사용하면 임계치 위반을 즉시 탐지하고, 그 영향을 식별하고, 문제의 영향과 근본 원인을 빠르고 효과적으로 수정할 수 있는 방식으로 분석할 수 있습니다.

성능 정책을 사용하면 모든 오브젝트(데이터 저장소, 디스크, 하이퍼바이저, 내부 볼륨, 포트, 스토리지, 스토리지 노드, 스토리지 풀, VMDK, 가상 머신, 성능 카운터(예: 총 IOPS)를 포함하는 볼륨 임계값 위반이 발생하는 경우 Insight는 빨간색 실선 원, 이메일 경고(구성된 경우), 위반 대시보드 또는 위반을 보고하는 사용자 지정 대시보드를 표시하여 관련 자산 페이지에서 이를 감지하여 보고합니다.

Insight에서는 일부 기본 성능 정책을 제공합니다. 이러한 성능 정책은 사용자 환경에 적용할 수 없는 경우 수정하거나 삭제할 수 있으며 다음과 같은 개체에 대해 사용할 수 있습니다.

- 하이퍼바이저

ESX 스와핑 및 ESX 사용률 정책이 있습니다.

- 내부 볼륨 및 볼륨

각 리소스에 대해 두 가지 지연 정책이 있으며, 하나는 계층 1에 대해 주석이 추가되고 다른 하나는 계층 2에 대해 주석이 달립니다.

- 포트

BB 크레딧 0에 대한 정책이 있습니다.

- 스토리지 노드

노드 활용률에 대한 정책이 있습니다.

- 가상 머신

VM 스와핑과 ESX CPU 및 메모리 정책이 있습니다.

- 볼륨

계층별 지연 시간 및 볼륨 정책 정렬 불량에 있습니다.

성능 정책 생성 중

성능 정책을 생성하여 네트워크 리소스와 관련된 문제를 알리기 위해 알림을 트리거하는 임계값을 설정합니다. 예를 들어, 스토리지 풀의 총 활용률이 60%를 초과할 경우 알림을 보낼 성능 정책을 생성할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 엽니다.
2. Manage * > * Performance Policies * 를 선택합니다.

성능 정책 페이지가 표시됩니다

The screenshot shows the 'Performance Policies' page in the OnCommand Insight interface. It features a navigation bar with 'Dashboards', 'Queries', 'Manage', and 'Admin' tabs. Below the navigation bar, there's a section for 'Performance Policies' with an 'Add new policy' button. The page displays three tables of policies:

- Database policies:** Contains two policies: 'Latency' and 'Database_0'. Both have a 'Warning' severity and a 'First occurrence' time window. The 'Latency' policy has a threshold of 'Latency - Total > 200 ms'. The 'Database_0' policy has a threshold of 'IOPS - Total > 0 IOPS or Latency - Total > 0 ms'.
- Network policies:** Contains two policies: 'Almos Service Level' and 'Global'. Both have a 'Critical' severity and a 'First occurrence' time window. The 'Almos Service Level' policy has a threshold of 'Latency - Total > 100 ms or IOPS - Total > 100 IOPS or Throughput - Total > 200 MB/s'. The 'Global' policy has a threshold of 'Latency - Total > 200 ms or IOPS - Total > 1 IOPS or Throughput - Total > 300 MB/s'.
- Storage policies:** Contains two policies: 'Storage_Storage' and 'Storage_0'. Both have a 'Warning' severity and a 'First occurrence' time window. The 'Storage_Storage' policy has a threshold of 'IOPS - Read > 10 IOPS'. The 'Storage_0' policy has a threshold of 'Throughput - Total > 0 MB/s or IOPS - Total > 0 IOPS'.

정책은 객체별로 구성되며 해당 객체의 목록에 나타나는 순서대로 평가됩니다.

3. 새 정책 추가 * 를 클릭합니다.

정책 추가 대화 상자가 표시됩니다.

4. Policy name * 필드에 정책 이름을 입력합니다.

개체의 다른 모든 정책 이름과 다른 이름을 사용해야 합니다. 예를 들어, 내부 볼륨에 대해 "지연 시간"이라는 두 가지 정책을 사용할 수는 없지만, 내부 볼륨에 대해 "지연 시간" 정책과 다른 볼륨에 대해 "지연 시간" 정책을 사용할 수 있습니다. 가장 좋은 방법은 개체 유형에 관계없이 모든 정책에 대해 항상 고유한 이름을 사용하는 것입니다.

5. Type * 의 개체에 적용 목록에서 정책이 적용되는 개체 유형을 선택합니다.
6. With annotation * (주석 포함 *) 목록에서 주석 유형을 선택하고, 해당되는 경우 * Value * (값 *) 상자에 주석 값을 입력하여 이 특정 주석 세트가 있는 개체에만 정책을 적용합니다.
7. 객체 유형으로 * Port * 를 선택한 경우 * Connected to * 목록에서 포트가 연결된 대상을 선택합니다.
8. [다음 창 뒤에 적용]목록에서 임계값 위반을 나타내기 위해 경고를 표시할 시기를 선택합니다.

첫 번째 발생 옵션은 첫 번째 데이터 샘플에서 임계값이 초과되면 알림을 트리거합니다. 다른 모든 옵션은 임계값을 한 번 넘어섰을 때 경고를 발생시키고 지정된 시간 이상 연속적으로 교차하는 경우에 발생합니다.

9. with severity * 목록에서 위반 심각도를 선택합니다.

10. 기본적으로 정책 위반에 대한 전자 메일 알림이 글로벌 전자 메일 목록의 받는 사람에게 전송됩니다. 특정 정책에 대한 알림이 특정 수신자에게 전송되도록 이러한 설정을 재정의할 수 있습니다.

- 링크를 클릭하여 받는 사람 목록을 연 다음 * + * 버튼을 클릭하여 받는 사람을 추가합니다. 해당 정책에 대한 위반 알림은 목록의 모든 수신자에게 전송됩니다.

11. 다음 중 하나라도 참인 경우 * 알림 생성 섹션에서 * 임의 * 링크를 클릭하여 알림 트리거 방법을 제어합니다.

- * 모두 *

이 설정은 정책과 관련된 임계값 중 하나라도 넘을 경우 알림을 생성하는 기본 설정입니다.

- * 모두 *

이 설정은 정책에 대한 모든 임계값을 초과할 때 알림을 생성합니다. All * 을 선택하면 성능 정책에 대해 생성한 첫 번째 임계값을 기본 규칙이라고 합니다. 기본 규칙 임계값이 성능 정책에 대해 가장 우려되는 위반인지 확인해야 합니다.

12. Create alert if * 섹션에서 성능 카운터와 연산자를 선택한 다음 값을 입력하여 임계값을 생성합니다.

13. 임계값을 더 추가하려면 * Add threshold * (임계값 추가)를 클릭합니다.

14. 임계값을 제거하려면 휴지통 아이콘을 클릭합니다.

15. 경고 발생 시 정책 처리를 중지하려면 * 알림이 생성되면 추가 정책 처리 중지 * 확인란을 선택합니다.

예를 들어, 데이터 저장소에 대한 정책이 4개 있고 경고가 발생할 때 처리를 중지하도록 두 번째 정책이 구성된 경우 두 번째 정책 위반이 활성화되어 있는 동안에는 세 번째 정책과 네 번째 정책이 처리되지 않습니다.

16. 저장 * 을 클릭합니다.

성능 정책 페이지가 표시되고 성능 정책이 개체 유형에 대한 정책 목록에 표시됩니다.

성능 정책 평가 우선 순위

성능 정책 페이지는 정책을 개체 유형별로 그룹화하고 Insight는 개체의 성능 정책 목록에 나타나는 순서대로 정책을 평가합니다. Insight에서 정책을 평가하는 순서를 변경하여 네트워크에서 가장 중요한 정보를 표시할 수 있습니다.

Insight는 성능 데이터 샘플을 해당 개체에 대해 시스템으로 가져올 때 개체에 적용할 수 있는 모든 정책을 순차적으로 평가합니다. 하지만 주석에 따라 일부 정책은 하나의 개체 그룹에 적용되지 않습니다. 예를 들어 내부 볼륨에 다음 정책이 있다고 가정합니다.

- 정책 1(Insight 제공 기본 정책)
- 정책 2('서비스 수준=실버' 주석 및 경고가 생성되면 추가 정책 처리 중지 * 옵션 포함)
- 정책 3("서비스 수준 = 골드" 주석 사용)
- 정책 4

Gold 주석이 있는 내부 볼륨 계층의 경우 Insight는 정책 1을 평가하고 정책 2를 무시한 다음 정책 3과 정책 4를 평가합니다. 주석이 없는 계층의 경우 Insight는 정책 순서에 따라 평가하므로 Insight는 정책 1과 정책 4만 평가합니다. Silver 주석이 있는 내부 볼륨 계층의 경우 Insight는 정책 1과 정책 2를 평가합니다. 그러나 정책의 임계값이 한 번 초과되어 정책에 지정된 시간 동안 연속적으로 교차하는 경우에 경고가 트리거되면 Insight는 개체의 현재 카운터를 평가하는 동안 목록의 다른 정책을 더 이상 평가하지 않습니다. Insight에서 객체에 대한 다음 성능 샘플 세트를 캡처하면 해당 객체에 대한 성능 정책을 필터 및 순서별로 다시 평가하기 시작합니다.

성능 정책의 우선 순위 변경

기본적으로 Insight는 오브젝트의 정책을 순차적으로 평가합니다. Insight에서 성능 정책을 평가하는 순서를 구성할 수 있습니다. 예를 들어, 골드 계층 스토리지에 대한 위반이 발생할 경우 해당 정책을 먼저 목록에 배치하고 동일한 스토리지 자산에 대한 일반적인 위반을 더 이상 보지 않도록 할 수 있습니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Manage * (관리 *) 메뉴에서 * Performance Policies * (성능 정책 *)를 선택합니다.

성능 정책 페이지가 표시됩니다.

3. 개체 유형의 성능 정책 목록에서 정책 이름 위에 커서를 놓습니다.

정책 오른쪽에 우선순위 화살표가 나타납니다.

4. 목록에서 정책을 위로 이동하려면 위쪽 화살표를 클릭하고 목록에서 정책을 아래로 이동하려면 아래쪽 화살표를 클릭합니다.

기본적으로 새 정책은 개체의 정책 목록에 순차적으로 추가됩니다.


성능 정책 편집

기존 및 기본 성능 정책을 편집하여 Insight에서 사용자 네트워크의 관심 조건을 모니터링하는 방법을 변경할 수 있습니다. 예를 들어 정책의 임계값을 변경할 수 있습니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Manage * (관리 *) 메뉴에서 * Performance Policies * (성능 정책 *)를 선택합니다.

성능 정책 페이지가 표시됩니다.

3. 개체의 성능 정책 목록에서 정책 이름 위에 커서를 놓습니다.
4. 을 클릭합니다 .

정책 편집 대화 상자가 표시됩니다.

5. 필요한 사항을 변경합니다.

정책 이름 이외의 다른 옵션을 변경하면 Insight에서 해당 정책에 대한 모든 기존 위반 사항을 삭제합니다.

6. 저장 * 을 클릭합니다


성능 정책을 삭제하는 중입니다

네트워크의 객체를 모니터링하는 데 더 이상 적용되지 않을 경우 성능 정책을 삭제할 수 있습니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Manage * (관리 *) 메뉴에서 * Performance Policies * (성능 정책 *)를 선택합니다.

성능 정책 페이지가 표시됩니다.

3. 개체의 성능 정책 목록에 있는 정책 이름 위에 커서를 놓습니다.
4. 을 클릭합니다 .

정책을 삭제할 것인지 묻는 메시지가 나타납니다.

5. 확인 * 을 클릭합니다.

사용자 데이터 가져오기 및 내보내기

가져오기 및 내보내기 기능을 사용하여 주식, 주식 규칙, 쿼리, 성능 정책 및 사용자 지정 대시보드를 하나의 파일로 내보낼 수 있습니다. 그런 다음 이 파일을 다른 OnCommand Insight 서버로 가져올 수 있습니다.

내보내기 및 가져오기 기능은 동일한 버전의 OnCommand Insight를 실행하는 서버 간에만 지원됩니다.

사용자 데이터를 내보내거나 가져오려면 * Admin * 을 클릭하고 * Setup * 을 선택한 다음 * Import/Export user data * 탭을 선택합니다.

가져오는 개체와 개체 형식에 따라 가져오기 작업 중에 데이터가 추가, 병합 또는 교체됩니다.

• 주식 유형

- 대상 시스템에 동일한 이름의 주식이 없는 경우 주식을 추가합니다.
- 주식 유형이 목록이고 이름이 같은 주식이 대상 시스템에 있는 경우 주식을 병합합니다.
- 주식 유형이 목록 이외의 주식 유형이고 대상 시스템에 동일한 이름의 주식이 있는 경우 주식을 대체합니다.



이름이 같지만 유형이 다른 주식이 대상 시스템에 있는 경우 가져오기에 실패합니다. 개체가 실패한 주식에 따라 달라지는 경우 이러한 개체는 부정확하거나 원치 않는 정보를 표시할 수 있습니다. 가져오기 작업이 완료된 후에는 모든 주식 종속성을 확인해야 합니다.

• 주식 규칙

- 대상 시스템에 같은 이름의 주식 규칙이 없으면 주식 규칙을 추가합니다.
- 주식 규칙이 대상 시스템에 동일한 이름의 규칙이 있는 경우 주식 규칙을 바꿉니다.



주석 규칙은 쿼리와 주석 모두에 따라 달라집니다. 가져오기 작업이 완료된 후 모든 주석 규칙이 정확한지 확인해야 합니다.

• 정책

- 대상 시스템에 동일한 이름의 정책이 없는 경우 정책을 추가합니다.
- 대상 시스템에 동일한 이름의 정책이 있는 경우 정책을 교체합니다.



가져오기 작업이 완료된 후 정책이 순서를 벗어났을 수 있습니다. 가져온 후에는 정책 순서를 확인해야 합니다. 주석이 잘못된 경우 주석에 종속된 정책이 실패할 수 있습니다. 가져온 후에는 모든 주석 종속성을 확인해야 합니다.

를 누릅니다

• 쿼리

- 대상 시스템에 동일한 이름의 쿼리가 없는 경우 쿼리를 추가합니다.
- 쿼리의 리소스 유형이 다른 경우에도 대상 시스템에 동일한 이름의 쿼리가 있는 경우 쿼리를 바꿉니다.



쿼리의 리소스 유형이 다른 경우 가져오기 후 해당 쿼리를 사용하는 대시보드 위젯에 원치 않는 결과 또는 잘못된 결과가 표시될 수 있습니다. 가져오기 후 모든 쿼리 기반 위젯의 정확성을 확인해야 합니다. 주석이 잘못된 경우 주석에 종속된 쿼리가 실패할 수 있습니다. 가져온 후에는 모든 주석 종속성을 확인해야 합니다.

를 누릅니다

• 대시보드

- 타겟 시스템에 동일한 이름의 대시보드가 없는 경우 대시보드를 추가합니다.
- 쿼리의 리소스 유형이 다른 경우에도 대상 시스템에 동일한 이름의 대시보드가 있는 경우 대시보드를 대체합니다.



가져오기 후 대시보드의 모든 쿼리 기반 위젯이 정확한지 확인해야 합니다. 소스 서버에 동일한 이름의 대시보드가 여러 개 있는 경우 모두 내보내집니다. 그러나 첫 번째 서버만 대상 서버로 가져옵니다. 가져오는 동안 오류를 방지하려면 대시보드를 내보내기 전에 고유한 이름을 지정해야 합니다.

를 누릅니다

Insight Security 를 참조하십시오

OnCommand Insight 7.3.1에서는 향상된 보안으로 Insight 환경을 운영할 수 있는 보안 기능이 도입되었습니다. 암호화, 암호 해싱의 개선, 암호를 암호화하고 해독하는 내부 사용자 암호 및 키 쌍 변경 기능이 포함되어 있습니다. Insight 환경의 모든 서버에서 이러한 기능을 관리할 수 있습니다.

Insight의 기본 설치에는 사용자 환경의 모든 사이트에서 동일한 키와 동일한 기본 암호를 공유하는 보안 구성이 포함됩니다. 중요 데이터를 보호하려면 설치 또는 업그레이드 후에 기본 키와 취득 사용자 암호를 변경하는 것이

좋습니다.

데이터 소스 암호화된 암호는 Insight Server 데이터베이스에 저장됩니다. 서버에 공개 키가 있으며 사용자가 WebUI 데이터 소스 구성 페이지에 암호를 입력할 때 암호를 암호화합니다. 서버에 Server 데이터베이스에 저장된 데이터 소스 암호를 해독하는 데 필요한 개인 키가 없습니다. 획득 장치(Lau, RAU)만 데이터 소스 암호를 해독하는 데 필요한 데이터 소스 개인 키를 가지고 있습니다.

서버 키를 다시 입력합니다

기본 키를 사용하면 환경에 보안 취약점이 발생합니다. 기본적으로 데이터 소스 암호는 Insight 데이터베이스에 암호화됩니다. 모든 Insight 설치에 공통적으로 사용되는 키를 사용하여 암호화됩니다. 기본 구성에서 NetApp에 전송된 Insight 데이터베이스에는 이론적으로 NetApp에 의해 암호 해독될 수 있는 암호가 포함되어 있습니다.

획득 사용자 암호 변경

기본 '획득' 사용자 암호를 사용하면 환경에 보안 취약점이 발생합니다. 모든 획득 장치는 ""획득" 사용자를 사용하여 서버와 통신합니다. 기본 암호가 있는 RA는 이론적으로 기본 암호를 사용하여 모든 Insight 서버에 연결할 수 있습니다.

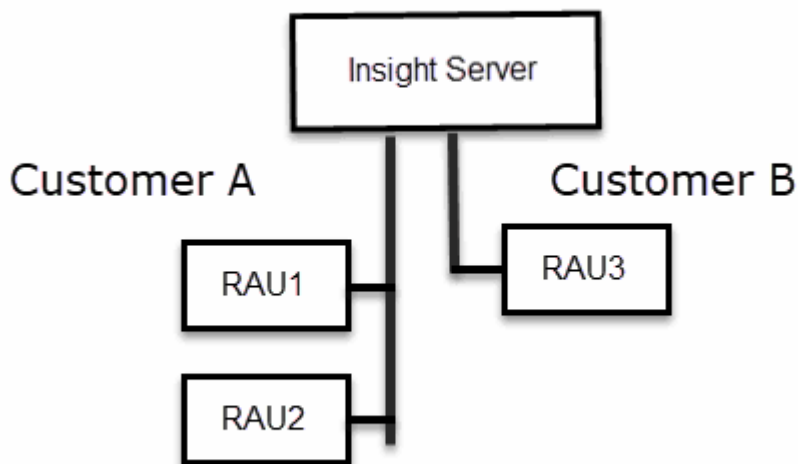
업그레이드 및 설치 고려 사항

Insight 시스템에 기본 보안 구성이 아닌 구성(암호 키를 다시 입력하거나 변경한 경우)이 포함된 경우 보안 구성을 백업해야 합니다. 새 소프트웨어를 설치하거나 소프트웨어를 업그레이드하는 경우 시스템을 기본 보안 구성으로 되돌립니다. 시스템이 기본 구성으로 복원되면 시스템이 올바르게 작동하려면 기본이 아닌 구성을 복원해야 합니다.

복잡한 서비스 공급자 환경에서 키 관리

서비스 공급자는 데이터를 수집하는 여러 OnCommand Insight 고객을 호스팅할 수 있습니다. 이 키는 Insight 서버의 여러 고객이 무단으로 고객 데이터에 액세스하지 못하도록 보호합니다. 각 고객의 데이터는 특정 키 쌍으로 보호됩니다.

이 Insight 구현은 다음 그림과 같이 구성할 수 있습니다.



이 구성에서는 각 고객에 대해 개별 키를 생성해야 합니다. 고객 A는 두 RA 모두에 대해 동일한 키를 필요로 합니다.

고객 B에는 단일 키 세트가 필요합니다.

고객 A의 암호화 키를 변경하는 단계:

1. RAU1을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.
5. RAU2를 호스팅하는 서버에 원격 로그인을 수행합니다.
6. 보안 구성의 백업 zip 파일을 RAU2에 복사합니다.
7. 보안 관리 도구를 시작합니다.
8. 보안 백업을 RAU1에서 현재 서버로 복원합니다.

고객 B의 암호화 키를 변경하는 단계:

1. RAU3을 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 보안 관리 도구를 시작합니다.
3. 기본 키를 대체하려면 암호화 키 변경 을 선택합니다.
4. 백업 을 선택하여 보안 구성의 백업 zip 파일을 생성합니다.

Insight 서버의 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 Insight 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 암호 변경, 새 키 생성, 사용자가 만든 보안 구성 저장 및 복원, 기본 설정으로 구성 복원 등이 포함됩니다.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

단계

1. Insight 서버에 원격 로그인을 수행합니다.
2. 대화형 모드에서 보안 관리 도구를 시작합니다.
 - 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
 - Linux - /bin/oci-securityadmin.sh -i시스템에서 로그인 자격 증명을 요청합니다.
3. "Admin" 자격 증명에 있는 계정의 사용자 이름과 암호를 입력합니다.

4. 서버 * 를 선택합니다.

다음 서버 구성 옵션을 사용할 수 있습니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 서버 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

프록시 사용자 암호, SMTP 사용자 암호, LDAP 사용자 암호 등을 암호화 또는 해독하는 데 사용되는 서버 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

Insight에서 사용하는 내부 계정의 암호를 변경합니다. 다음 옵션이 표시됩니다.

- _내부
- 획득
- Cognos_admin
- DWh _ 내부
- 호스트
- 인벤토리
- 루트



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

• * 기본값으로 재설정 *

키와 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

• * 종료 *

를 종료합니다 securityadmin 도구.

- a. 변경할 옵션을 선택하고 화면의 지시를 따릅니다.

로컬 획득 장치의 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 로컬 획득 사용자(Lau)의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 키 및 암호 관리, 사용자가 만들고 복원한 보안 구성을 기본 설정으로 저장 및 복원하는 작업이 포함됩니다.

시작하기 전에

이(가) 있어야 합니다 admin 보안 구성 작업을 수행할 수 있는 권한.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

단계

1. Insight 서버에 원격 로그인을 수행합니다.

2. 대화형 모드에서 보안 관리 도구를 시작합니다.

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
- Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

4. Local Acquisition Unit(로컬 획득 장치) * 을 선택하여 Local Acquisition Unit(로컬 획득 장치) 보안 구성을 재구성합니다.

다음 옵션이 표시됩니다.

- * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

- * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원을 사용하여 여러 서버의 패스워드와 키를 동기화할 수 있습니다. 예를 들어: - Lau에서 암호화 키 변경 - 볼트 백업 작성 - 각 RA에 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

장치 암호를 암호화 또는 해독하는 데 사용되는 AU 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

'촬영' 사용자 계정의 암호를 변경합니다.



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 기본값으로 재설정 *

획득 사용자 암호 및 획득 사용자 암호화 키를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

5. 구성할 옵션을 선택하고 화면의 지시를 따릅니다.

RAU에 대한 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 RA의 보안 옵션을 관리할 수 있습니다. 볼트 구성을 백업 또는 복원하거나 암호화 키를 변경하거나 획득 장치의 암호를 업데이트해야 할 수 있습니다.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

Lau, RAU에 대한 보안 구성을 업데이트하는 한 가지 시나리오는 해당 사용자의 암호가 서버에서 변경된 경우 'acquisition' 사용자 암호를 업데이트하는 것입니다. 모든 RA와 Lau는 서버 '획득' 사용자의 암호와 동일한 암호를 사용하여 서버와 통신합니다.

'acquisition' 사용자는 Insight 서버에만 있습니다. RAU 또는 Lau는 서버에 연결할 때 해당 사용자로 로그인합니다.

RAU에서 보안 옵션을 관리하려면 다음 단계를 따르십시오.

단계

1. RAU를 실행 중인 서버에 원격 로그인을 수행한다
2. 대화형 모드에서 보안 관리 도구를 시작합니다.

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
- Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명이 있는 계정의 사용자 이름과 암호를 입력합니다.

RAU에 대한 메뉴가 표시됩니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 다음 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

◦ * 암호화 키 변경 *

단말기 암호를 암호화 또는 해독하는 데 사용되는 RAU 암호화 키를 변경합니다.



암호화 키를 변경할 때는 업그레이드 또는 설치 후 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 암호 업데이트 *

'촬영' 사용자 계정의 암호를 변경합니다.



암호를 변경할 때 일부 계정을 동기화해야 합니다. 예를 들어, 서버에서 'acquisition' 사용자의 암호를 변경하는 경우 Lau, RAU 및 DWH에서 'acquisition' 사용자의 암호를 변경하여 일치시켜야 합니다. 또한 암호를 변경할 때는 업그레이드 또는 설치 후에 복원할 수 있도록 새 보안 구성을 백업해야 합니다.

◦ * 기본값으로 재설정 *

암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

데이터 웨어하우스의 보안 관리

를 클릭합니다 securityadmin 도구를 사용하면 데이터 웨어하우스 서버의 보안 옵션을 관리할 수 있습니다. 보안 관리에는 DWH 서버의 내부 사용자에게 대한 내부 암호 업데이트, 보안 구성 백업 생성 또는 기본 설정으로 구성 복원이 포함됩니다.

이 작업에 대해

를 사용합니다 securityadmin 보안 관리 도구:

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat
- Linux - /bin/oci-securityadmin.sh

단계

1. 데이터 웨어하우스 서버에 원격 로그인을 수행합니다.
2. 대화형 모드에서 보안 관리 도구를 시작합니다.

- 윈도우 - C:\Program Files\SANscreen\securityadmin\bin\securityadmin.bat -i
- Linux - /bin/oci-securityadmin.sh -i

시스템에서 로그인 자격 증명을 요청합니다.

3. "Admin" 자격 증명에 있는 계정의 사용자 이름과 암호를 입력합니다.

데이터 웨어하우스에 대한 보안 관리 메뉴가 표시됩니다.

◦ * 백업 *

모든 암호 및 키가 포함된 볼트의 백업 zip 파일을 작성하고 사용자가 지정한 위치 또는 기본 위치에 파일을 배치합니다.

- 윈도우 - C:\Program Files\SANscreen\backup\vault
- Linux - /var/log/netapp/oci/backup/vault

◦ * 복원 *

작성된 볼트의 zip 백업을 복원합니다. 복원되면 모든 암호와 키는 백업 생성 시 기존 값으로 되돌려집니다.



복원은 여러 서버의 암호와 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 - 한 서버의 암호화 키 변경 - 볼트 백업 작성 - 두 번째 서버로 볼트 백업을 복원합니다

를 누릅니다

◦ * 암호화 키 변경 *

커넥터 암호 및 SMTP 암호와 같은 암호를 암호화 또는 해독하는 데 사용되는 DWH 암호화 키를 변경합니다.

◦ * 암호 업데이트 *

특정 사용자 계정의 암호를 변경합니다.

- _내부
- 획득
- Cognos_admin
- 드Wh
- DWh _ 내부
- Dwhuser(사용자)
- 호스트
- 인벤토리
- 루트



dwhuser, hosts, inventory 또는 root 암호를 변경하면 SHA-256 암호 해싱을 사용할 수 있습니다. 이 옵션을 사용하려면 계정에 액세스하는 모든 클라이언트가 SSL 연결을 사용해야 합니다.

+

◦ * 기본값으로 재설정 *

암호화 키 및 암호를 기본값으로 재설정합니다. 기본값은 설치 중에 제공되는 값입니다.

◦ * 종료 *

를 종료합니다 securityadmin 도구.

OnCommand Insight 내부 사용자 암호 변경

보안 정책에 따라 OnCommand Insight 환경의 암호를 변경해야 할 수 있습니다. 한 서버의 암호 중 일부는 환경의 다른 서버에 있으므로 두 서버의 암호를 변경해야 합니다. 예를 들어, Insight Server에서 ""인벤토리"" 사용자 암호를 변경할 경우 해당 Insight Server에 대해 구성된 데이터 웨어하우스 서버 Connector의 ""인벤토리"" 사용자 암호와 일치해야 합니다.

시작하기 전에



암호를 변경하기 전에 사용자 계정의 종속성을 이해해야 합니다. 필요한 모든 서버에서 암호를 업데이트하지 못하면 Insight 구성 요소 간의 통신 장애가 발생합니다.

이 작업에 대해

다음 표에는 Insight Server의 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Insight Server 암호	필수 변경 사항
_내부	
획득	Lau, RAU
DWh _ 내부	데이터 웨어하우스
호스트	
인벤토리	데이터 웨어하우스
루트	

다음 표에는 데이터 웨어하우스에 대한 내부 사용자 암호가 나열되어 있으며 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

데이터 웨어하우스 암호	필수 변경 사항
Cognos_admin	
드Wh	
dWh_INTERNAL(서버 커넥터 구성 UI를 사용하여 변경)	Insight 서버
Dwhuser(사용자)	
호스트	
인벤토리(서버 커넥터 구성 UI를 사용하여 변경됨)	Insight 서버
루트	

- DWH 서버 연결 구성 UI * 에서 암호 변경

다음 표에는 Lau의 사용자 암호와 새 암호와 일치해야 하는 종속 암호가 있는 Insight 구성 요소가 나열되어 있습니다.

Lau 암호	필수 변경 사항
획득	Insight 서버, RAU

서버 연결 구성 UI를 사용하여 **"inventory"** 및 **"dWh_internal"** 암호 변경

데이터 웨어하우스 UI를 사용하는 Insight 서버의 암호와 일치하도록 **"인벤토리"** 또는 **"DIH_INTERNAL"** 암호를 변경해야 하는 경우

시작하기 전에

이 작업을 수행하려면 관리자로 로그인해야 합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh> 여기서 hostname 은 OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

커넥터 편집 * 화면이 표시됩니다.

Edit Connector

ID:	<input type="text" value="1"/>
Encryption:	<input type="text" value="Enabled"/>
Name:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Host:	<input type="text" value="Oci-stg06-s12r2.nane.netapp.com"/>
Database user name:	<input type="text" value="inventory"/>
Database password:	<input type="password" value="....."/>

Advanced ▾

3. Database password * 필드에 새 ""Inventory"" 암호를 입력합니다.
4. 저장 * 을 클릭합니다
5. "dWh_INTERNAL" 암호를 변경하려면 * 고급 * 을 클릭합니다

커넥터 고급 편집 화면이 표시됩니다.

Edit Connector

ID:	1
Encryption:	Enabled
Name:	Oci-stg06-s12r2.nane.netapp.com
Host:	Oci-stg06-s12r2.nane.netapp.com
Database user name:	inventory
Database password:	••••••••
Server user name:	dwh_internal
Server password:	••••••••••••
HTTPS port:	443
TCP port:	3306

Basic ^

Save Cancel Test Remove

6. 서버 암호 * 필드에 새 암호를 입력합니다.

7. 저장 을 클릭합니다.

ODBC 관리 도구를 사용하여 **dWh** 암호를 변경합니다

Insight 서버에서 dWh 사용자의 암호를 변경하면 데이터 웨어하우스 서버에서도 암호를 변경해야 합니다. ODBC 데이터 원본 관리자 도구를 사용하여 데이터 웨어하우스의 암호를 변경할 수 있습니다.

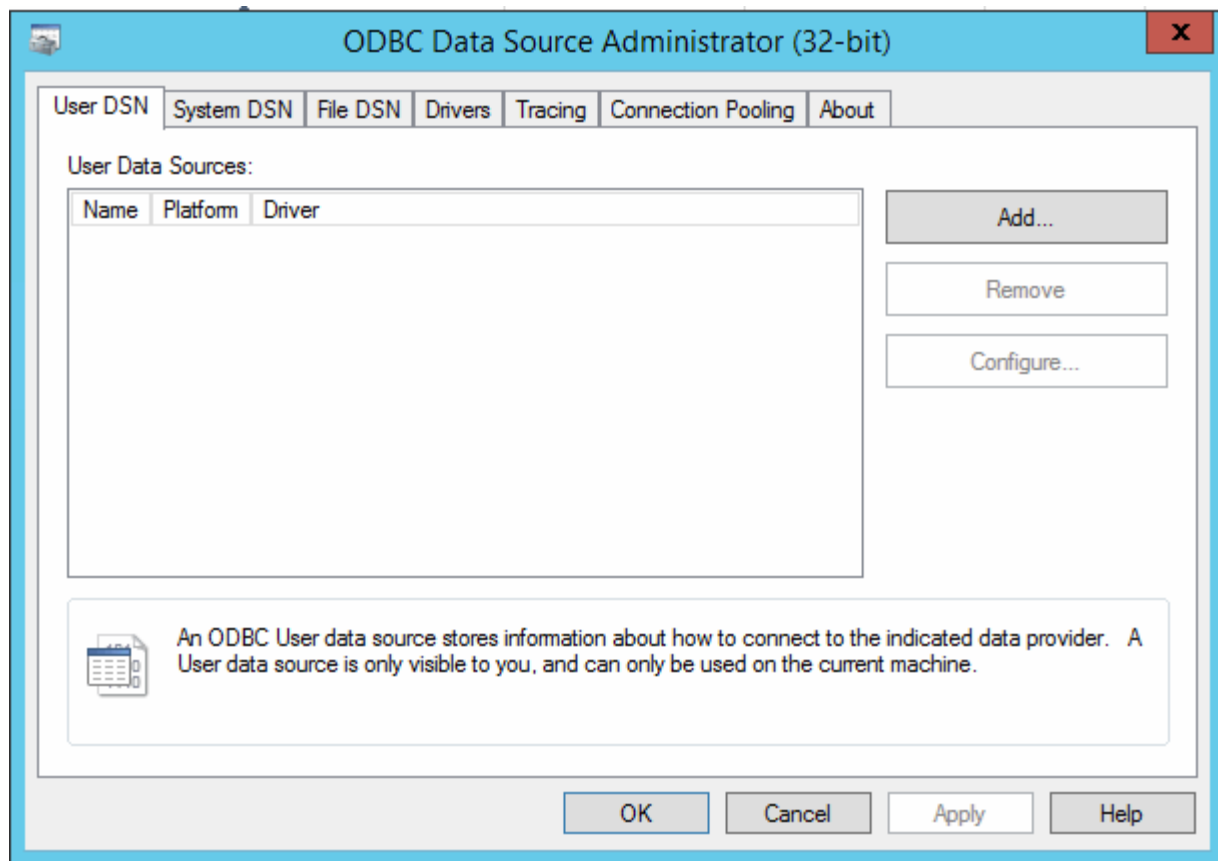
시작하기 전에

관리자 권한이 있는 계정을 사용하여 데이터 웨어하우스 서버에 원격으로 로그인해야 합니다.

단계

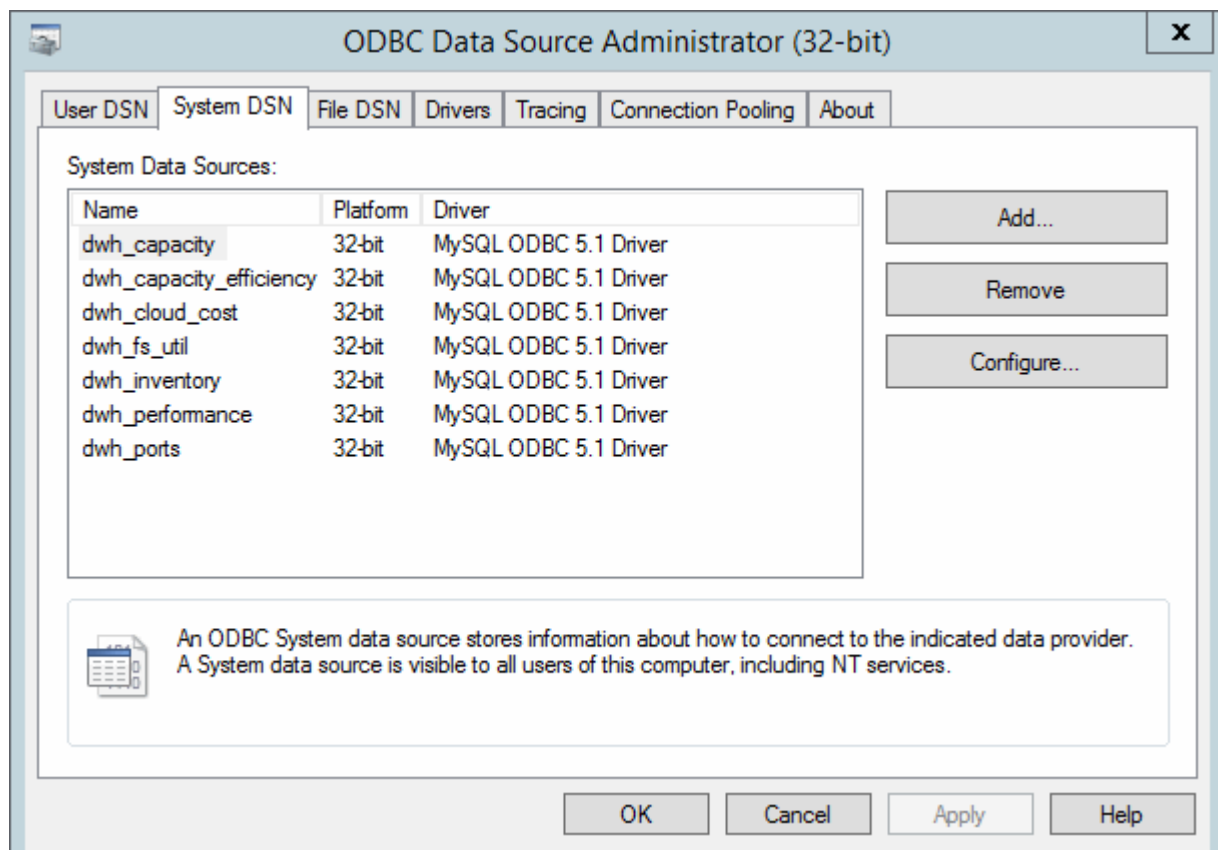
1. 해당 데이터 웨어하우스를 호스팅하는 서버에 원격 로그인을 수행합니다.
2. 에서 ODBC 관리 도구에 액세스합니다 C:\Windows\SysWOW64\odbcad32.exe

ODBC 데이터 원본 관리자 화면이 표시됩니다.



3. 시스템 DSN*을 클릭합니다

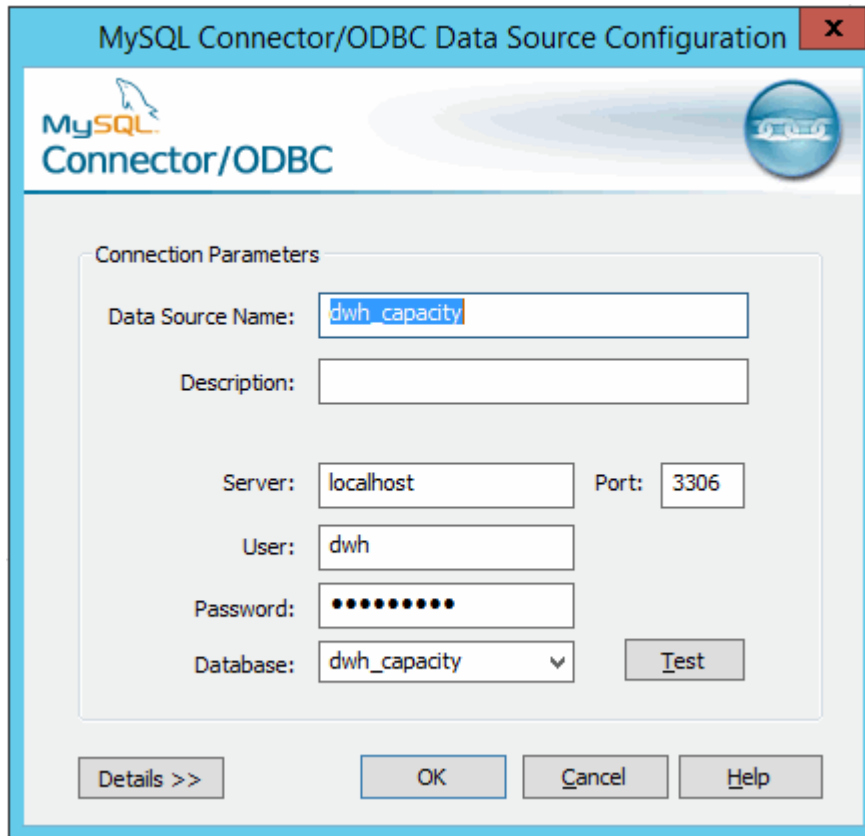
시스템 데이터 소스가 표시됩니다.



4. 목록에서 OnCommand Insight 데이터 원본을 선택합니다.

5. 구성 * 을 클릭합니다

데이터 소스 구성 화면이 표시됩니다.



6. 암호 * 필드에 새 암호를 입력합니다.

스마트 카드 및 인증서 로그인 지원

OnCommand Insight는 CAC(스마트 카드) 및 인증서를 사용하여 Insight 서버에 로그인하는 사용자를 인증할 수 있습니다. 이러한 기능을 사용하려면 시스템을 구성해야 합니다.

CAC 및 인증서를 지원하도록 시스템을 구성한 후 OnCommand Insight의 새 세션을 탐색하면 브라우저에 기본 대화 상자가 표시되어 사용자가 선택할 수 있는 개인 인증서 목록을 제공합니다. 이러한 인증서는 OnCommand Insight 서버에서 신뢰할 수 있는 CA에서 발급한 개인 인증서 집합을 기반으로 필터링됩니다. 대부분의 경우 단일 선택 옵션이 있습니다. 기본적으로 Internet Explorer는 하나만 선택할 경우 이 대화 상자를 건너뛸니다.



CAC 사용자의 경우 스마트 카드에는 신뢰할 수 있는 CA와 일치할 수 있는 인증서가 여러 개 있습니다. 이 인증서들은 identification 사용해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

스마트 카드 및 인증서 로그인을 위한 호스트 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하려면 OnCommand Insight 호스트 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 User principal account name 속성은 사용자 ID가 포함된 LDAP 필드와 일치해야 합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. 를 사용합니다 regedit 에서 레지스트리 값을 수정하는 유틸리티입니다
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java:
 - a. jvm_option을 변경합니다 DclientAuth=false 를 선택합니다 DclientAuth=true.
2. 키 저장소 파일을 백업합니다. C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
3. 를 지정하는 명령 프롬프트를 엽니다 Run as administrator

4. 자체 생성된 인증서 삭제: C:\Program Files\SANscreen\java64\bin\keytool.exe -delete -alias "ssl certificate" -keystore C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore
5. 새 인증서 생성: C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "alias_name" -keyalg RSA -sigalg SHA1withRSA -keysize 2048 -validity 365 -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -dname "CN=commonName,OU=orgUnit,O=orgName,L=localityNameI,S=stateName,C=countryName"
6. 인증서 서명 요청(CSR) 생성: C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -sigalg SHA1withRSA -alias "alias_name" -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file C:\temp\server.csr"
7. 6단계에서 CSR이 반환된 후 인증서를 가져온 다음 Base-64 형식으로 인증서를 내보내고 에 넣습니다 "C:\temp" named servername.cer.
8. 키 저장소에서 인증서를 추출합니다. C:\Program Files\SANscreen\java64\bin\keytool.exe -v -importkeystore -srckeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srcalias "alias_name" -destkeystore "C:\temp\file.p12" -deststoretype PKCS12
9. P12 파일에서 개인 키를 추출합니다. openssl pkcs12 -in "C:\temp\file.p12" -out "C:\temp\servername.private.pem"
10. 7단계에서 내보낸 Base-64 인증서를 개인 키와 병합합니다. openssl pkcs12 -export -in "<folder>\<certificate>.cer" -inkey "C:\temp\servername.private.pem" -out "C:\temp\servername.new.p12" -name "servername.abc.123.yyy.zzz"
11. 병합된 인증서를 키 저장소로 가져옵니다. C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -destkeystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -srckeystore "C:\temp\servername.new.p12" -srcstoretype PKCS12 -alias "alias_name"
12. 루트 인증서 가져오기: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file "C:\<root_certificate>.cer" -trustcacerts -alias "alias_name"
13. 루트 인증서를 서버로 가져옵니다. trustore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<email_certificate>.cer" -trustcacerts -alias "alias_name"
14. 중간 인증서 가져오기: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore "C:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore" -file "C:\<intermediate_certificate>.cer" -trustcacerts -alias "alias_name"

모든 중간 인증서에 대해 이 단계를 반복합니다.

15. 이 예제와 일치하도록 LDAP에 도메인을 지정합니다.

16. 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 지원하도록 클라이언트 구성

클라이언트 시스템은 스마트 카드 사용 및 인증서 로그인을 지원하기 위해 미들웨어와 브라우저 수정이 필요합니다. 이미 스마트 카드를 사용하고 있는 고객은 클라이언트 시스템을 추가로 수정할 필요가 없습니다.

시작하기 전에

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

다음은 일반적인 클라이언트 구성 요구 사항입니다.

- ActivClient와 같은 스마트 카드 미들웨어 설치(참조)
- IE 브라우저 수정(참조)
- Firefox 브라우저 수정(참조)

Linux 서버에 대한 CAC 활성화

Linux OnCommand Insight 서버에서 CAC를 활성화하려면 몇 가지 수정이 필요합니다.

단계

1. 로 이동합니다 `/opt/netapp/oci/conf/`
2. 편집 `wildfly.properties` 의 값을 변경합니다 `CLIENT_AUTH_ENABLED "참"`으로
3. 아래에 있는 "루트 인증서"를 가져옵니다
`/opt/netapp/oci/wildfly/standalone/configuration/server.keystore`
4. 서버를 다시 시작합니다

스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 User principal account name 속성은 사용자의 정부 ID 번호가 포함된 LDAP 필드와 일치해야 합니다.

정부에서 발급한 CAC에 저장된 일반 이름(CN)은 일반적으로 다음과 같은 형식입니다. first.last.ID. 와 같은 일부 LDAP 필드의 경우 sAMAccountName, 이 형식은 너무 깁니다. 이러한 필드의 경우 OnCommand Insight는 cns에서 ID 번호만 추출합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"



단계

1. regedit를 사용하여 의 레지스트리 값을 수정합니다

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software  
Foundation\Procrun2.0\SANscreen Server\Parameters\Java
```

- a. jvm_option을 변경합니다 -DclientAuth=false 를 선택합니다 -DclientAuth=true.

Linux의 경우 를 수정합니다 clientAuth 매개 변수 in /opt/netapp/oci/scripts/wildfly.server

2. CA(인증 기관)를 데이터 웨어하우스 trustore에 추가합니다.

- a. 명령 창에서 로 이동합니다 ..\SANscreen\wildfly\standalone\configuration.

- b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: C:\Program
Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore
-storepass changeit

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 필요한 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일. 데이터 웨어하우스 신뢰할 수 있는 CA와
함께 고객의 CA를 포함하려면 을 참조하십시오

..\SANscreen\wildfly\standalone\configuration 를 사용합니다 keytool 가져오기 명령:
C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore
server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts

my_alias는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

3. OnCommand Insight 서버에서 를 클릭합니다 wildfly/standalone/configuration/standalone-full.xml 에서 verify-client를 "requested"로 업데이트하여 파일을 수정해야 합니다
/subsystem=undertow/server=default-server/https-listener=default-httpsCAC 활성화
Insight 서버에 로그인하고 적절한 명령을 실행합니다.

OS	스크립트
Windows	<install dir>\SANscreen\Wildfly\bin\enableCACforRemoteEJB.bat 을 참조하십시오
리눅스	/opt/netapp/OCI/Wildfly/bin/enableCACforRemoteEJB.sh 을 참조하십시오

스크립트를 실행한 후 다음 단계로 진행하기 전에 Wildfly 서버의 재로드가 완료될 때까지 기다립니다.

4. OnCommand Insight 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 위한 Cognos 구성(OnCommand Insight 7.3.5 ~ 7.3.9)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.
 - a. 명령 창에서 로 이동합니다 ..\SANscreen\cognos\analytics\configuration\certs\
 - b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: ..\..\jre\bin\keytool.exe
-list -keystore CAMKeystore.jks -storepass NoPasswordSet

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다
`..\SANscreen\cognos\analytics\configuration\certs\.`
- e. 를 사용합니다 keytool 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

- f. 암호를 묻는 메시지가 나타나면 를 입력합니다 NoPassWordSet.
- g. 답변 yes 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 를 실행합니다 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. CAC 모드를 해제하려면 를 실행한다 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

스마트 카드 및 인증서 로그인에 대한 **Cognos** 구성(OnCommand Insight 7.3.10 이상)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnComand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Trustore에 CA(인증 기관)를 추가합니다.

- a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
- b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다
`..\SANscreen\cognos\analytics\configuration\certs\.`
- e. 를 사용합니다 keytool 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

- f. 암호를 묻는 메시지가 나타나면 를 입력합니다 NoPassWordSet.
- g. 답변 yes 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 다음을 수행합니다.

- a. 다음 단계에 따라 CAC 로그아웃 페이지를 구성합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
 - (7.3.10 및 7.3.11에만 해당) 관리->구성->시스템->보안을 클릭합니다
 - (7.3.10 및 7.3.11에만 해당) 로그아웃 리디렉션 URL에 대해 cacLogout.html 을 입력합니다.\ → 적용
 - 브라우저를 닫습니다.
- b. 실행 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
- c. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.

3. CAC 모드를 해제하려면 다음을 수행합니다.

- a. 실행 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
- b. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.
- c. (7.3.10 및 7.3.11에만 해당) 다음 단계에 따라 CAC 로그아웃 페이지를 구성 해제합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
 - 관리\ → 구성\ → 시스템\ → 보안을 클릭합니다
 - 로그아웃 리디렉션 URL \ → 적용에 대해 cacLogout.html 를 입력합니다
 - 브라우저를 닫습니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. 의 백업을 생성합니다 `..\SANSscreen\cognos\analytics\configuration\cogstartup.xml`.
2. 아래의 `""certs""` 및 `""csk""` 폴더의 백업을 만듭니다 `..\SANSscreen\cognos\analytics\configuration`.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
 - a. `CD "\Program Files\sansscreen\cognos\analytics\bin"`
 - b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`
4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. SSL 인증서를 얻으려면 `encryptRequest.csr`을 CA(인증 기관)에 보냅니다.

"san:dns=FQDN(예: hostname.netapp.com)" SubjectAltName을 추가하려면 추가 속성)을 추가해야 합니다. Google Chrome 버전 58 이상에서 SubjectAltName이 인증서에서 누락되면 불만을 표시합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

FQDN.p7b 파일이 다운로드됩니다
7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
 - a. `""Crypto Shell Extensions""`에서 .p7b 인증서를 엽니다.
 - b. 왼쪽 창에서 `""인증서""`를 찾습니다.
 - c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
 - d. Base64 출력을 선택합니다.
 - e. 루트 인증서로 식별하는 파일 이름을 입력합니다.

- f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a-8C단계를 반복합니다.
- g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
 - a. 메모장에서 intermediate.cer를 열고 내용을 복사합니다.
 - b. 메모장에서 root.cer를 열고 9a의 콘텐츠를 저장합니다.
 - c. 파일을 CA.CER로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
 - a. `cd ""Program Files\SANscreen\cognos\analytics\bin"`
 - b. `ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\CA.cer`

그러면 CA.cer가 루트 인증 기관으로 설정됩니다.
 - c. `ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer`

이렇게 하면 Cognos.cer 가 CA.cer 에 의해 서명된 암호화 인증서로 설정됩니다.
11. IBM Cognos 구성을 엽니다.
 - a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다
 - b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
 - c. 구성을 저장합니다.
 - d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
 - a. `"D:\Program Files\SANscreen\Java\bin\keytool.exe" -exportcert -file "" c:\temp\cognos.crt" -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12-storepass NoPassSet-alias 암호화`
13. 관리 CMD 프롬프트 창을 사용하여 "c:\temp\cognos.crt"를 dWh trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
 - a. `"D:\Program Files\SANscreen\Java\bin\keytool.exe" - importcert -file ""c:\temp\cognos.crt" - keystore "D:\Program Files\SANscreen\standalone\configuration\server.trustore" - storepass changeit -alias cognosert`
14. SANscreen 서비스를 다시 시작합니다.
15. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.10 이상)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. IBM Cognos 구성 도구를 사용하여 Cognos를 중지합니다. Cognos를 닫습니다.
2. 의 백업을 생성합니다 ..\SANSscreen\cognos\analytics\configuration 및 ..\SANSscreen\cognos\analytics\temp\cam\freshness 폴더.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
 - a. CD "\Program Files\sansscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress". 참고: 여기서 -H와 -I는 DNS 및 ipaddress와 같은 subjectAltNames를 추가합니다.
4. 를 엽니다 c:\temp\encryptRequest.csr 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. encryptRequest.csr 콘텐츠를 입력하고 CA 서명 포털을 사용하여 인증서를 생성합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

FQDN.p7b 파일이 다운로드됩니다
7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
 - a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
 - b. 왼쪽 창에서 ""인증서""를 찾습니다.
 - c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
 - d. Base64 출력을 선택합니다.
 - e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
 - f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a ~ 8e 단계를 반복합니다.

- g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
 - a. 메모장에서 root.cer를 열고 내용을 복사합니다.
 - b. 메모장을 사용하여 intermediate.cer를 열고 9a(중간 우선 및 루트 다음)의 콘텐츠를 추가합니다.
 - c. 파일을 chain.cer로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
 - a. `cd ""Program Files\SANscreen\cognos\analytics\bin"`
 - b. `ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\root.cer`
 - c. `ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\intermediate.cer`
 - d. `ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer`
11. IBM Cognos 구성을 엽니다.
 - a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다
 - b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
 - c. 구성을 저장합니다.
 - d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
 - a. `CD "C:\Program Files\SANscreen"`
 - b. `java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore-storetype pkcs12-storepass NoPassWordSet-alias encryption`
13. 에서 DWH 서버 트루스토어를 백업합니다..`\SANscreen\wildfly\standalone\configuration\server.trustore`
14. 관리 CMD 프롬프트 창을 사용하여 "`c:\temp\cognos.crt`"를 DWH trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
 - a. `CD "C:\Program Files\SANscreen"`
 - b. `java\bin\keytool.exe - importcert -file c:\temp\cognos.crt -keystore wandiderfly\standalone\configuration\server.trutstore -storephass changeit -alias coclnos3rdca`
15. SANscreen 서비스를 다시 시작합니다.
16. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.
17. 's' 인증서'만 변경되고 기본 Cognos 인증서는 변경되지 않은 경우에도 다음 단계를 수행해야 합니다. 그렇지 않으면 Cognos가 새 SANscreen 인증서에 대해 불만을 제기하거나 DWH 백업을 생성할 수 없습니다.
 - a. `cd "%SANSSCREEN_HOME%cognos\analytics\bin\"`
 - b. `"%SANSSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sansscreen.cer" -keystore "%SANSSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"`
 - c. `ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sansscreen.cer"`

일반적으로 이러한 단계는 에 설명된 Cognos 인증서 가져오기 프로세스의 일부로 수행됩니다 "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

스마트 카드 및 인증서 로그인을 위한 데이터 웨어하우스 구성

스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

- 시스템에서 LDAP를 활성화해야 합니다.
- LDAP입니다 User principal account name 속성은 사용자의 정부 ID 번호가 포함된 LDAP 필드와 일치해야 합니다.

정부에서 발급한 CAC에 저장된 일반 이름(CN)은 일반적으로 다음과 같은 형식입니다. first.last.ID. 와 같은 일부 LDAP 필드의 경우 sAMAccountName, 이 형식은 너무 길다. 이러한 필드의 경우 OnCommand Insight는 cns에서 ID 번호만 추출합니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. regedit를 사용하여 의 레지스트리 값을 수정합니다

```
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun2.0\SANscreen Server\Parameters\Java
```

- a. jvm_option을 변경합니다 -DclientAuth=false 를 선택합니다 -DclientAuth=true.

Linux의 경우 를 수정합니다 clientAuth 매개 변수 in /opt/netapp/oci/scripts/wildfly.server

2. CA(인증 기관)를 데이터 웨어하우스 trustore에 추가합니다.

- a. 명령 창에서 로 이동합니다 ..\SANscreen\wildfly\standalone\configuration.
- b. 를 사용합니다 keytool 신뢰할 수 있는 CA를 나열하는 유틸리티: C:\Program Files\SANscreen\java64\bin\keytool.exe -list -keystore server.trustore -storepass changeit

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 필요한 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일. 데이터 웨어하우스 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 을 참조하십시오

..\SANscreen\wildfly\standalone\configuration 를 사용합니다 keytool 가져오기 명령:
C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -keystore
server.trustore -alias my_alias -file 'path/to/my.pem' -v -trustcacerts

my_alias는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다keytool -list 작동.

3. OnCommand Insight 서버에서 를 클릭합니다 wildfly/standalone/configuration/standalone-full.xml 에서 verify-client를 "requested"로 업데이트하여 파일을 수정해야 합니다
/subsystem=undertow/server=default-server/https-listener=default-httpsCAC 활성화
Insight 서버에 로그인하고 적절한 명령을 실행합니다.

OS	스크립트
Windows	<install dir>\SANscreen\Wildfly\bin\enableCACforRemoteEJB.bat 을 참조하십시오
리눅스	/opt/netapp/OCI/Wildfly/bin/enableCACforRemoteEJB.sh 을 참조하십시오

스크립트를 실행한 후 다음 단계로 진행하기 전에 Wildfly 서버의 재로드가 완료될 때까지 기다립니다.

4. OnCommand Insight 서버를 다시 시작합니다.

스마트 카드 및 인증서 로그인을 위한 Cognos 구성(OnCommand Insight 7.3.5 ~ 7.3.9)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Truststore에 CA(인증 기관)를 추가합니다.

- a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
- b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.
- e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다 `keytool -list` 작동.

- f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.
- g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 를 실행합니다 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`

3. CAC 모드를 해제하려면 를 실행한다 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`

스마트 카드 및 인증서 로그인에 대한 Cognos 구성(OnCommand Insight 7.3.10 이상)

Cognos 서버에 대한 스마트 카드(CAC) 및 인증서 로그인을 지원하도록 OnCommand Insight 데이터 웨어하우스 구성을 수정해야 합니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.



최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).

- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

단계

1. Cognos Truststore에 CA(인증 기관)를 추가합니다.

- a. 명령 창에서 로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`
- b. 를 사용합니다 `keytool` 신뢰할 수 있는 CA를 나열하는 유틸리티: `..\..\ibm-jre\jre\bin\keytool.exe -list -keystore CAMKeystore.jks -storepass NoPassWordSet`

각 줄의 첫 번째 단어는 CA 별칭을 나타냅니다.

- c. 적합한 파일이 없는 경우 CA 인증서 파일(일반적으로 A)을 제공합니다 .pem 파일.
- d. OnCommand Insight의 신뢰할 수 있는 CA와 함께 고객의 CA를 포함하려면 으로 이동합니다 `..\SANscreen\cognos\analytics\configuration\certs\`.
- e. 를 사용합니다 `keytool` 을(를) 가져오는 유틸리티입니다 .pem 파일: `..\..\ibm-jre\jre\bin\keytool.exe -importcert -keystore CAMKeystore.jks -alias my_alias -file 'path/to/my.pem' -v -trustcacerts`

`my_alias` 는 일반적으로 에서 CA를 쉽게 식별하는 별칭입니다 `keytool -list` 작동.

- f. 암호를 묻는 메시지가 나타나면 를 입력합니다 `NoPassWordSet`.
- g. 답변 `yes` 인증서를 신뢰할 수 있는 것인지 묻는 메시지가 표시됩니다.

2. CAC 모드를 활성화하려면 다음을 수행합니다.

- a. 다음 단계에 따라 CAC 로그아웃 페이지를 구성합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: `cognos_admin`)에 속해야 함)
 - (7.3.10 및 7.3.11에만 해당) 관리->구성->시스템->보안을 클릭합니다
 - (7.3.10 및 7.3.11에만 해당) 로그아웃 리디렉션 URL에 대해 `cacLogout.html` 을 입력합니다.\ → 적용
 - 브라우저를 닫습니다.

- b. 실행 `..\SANscreen\bin\cognos_cac\enableCognosCAC.bat`
 - c. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.
3. CAC 모드를 해제하려면 다음을 수행합니다.
- a. 실행 `..\SANscreen\bin\cognos_cac\disableCognosCAC.bat`
 - b. IBM Cognos 서비스를 시작합니다. Cognos 서비스가 시작될 때까지 기다립니다.
 - c. (7.3.10 및 7.3.11에만 해당) 다음 단계에 따라 CAC 로그아웃 페이지를 구성 해제합니다.
 - Cognos 포털 로그인(사용자는 시스템 관리자 그룹(예: cognos_admin)에 속해야 함)
 - 관리\ → 구성\ → 시스템\ → 보안을 클릭합니다
 - 로그아웃 리디렉션 URL\ → 적용에 대해 cacLogout.html 를 입력합니다
 - 브라우저를 닫습니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.5 ~ 7.3.9)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.5 ~ 7.3.9를 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. 의 백업을 생성합니다 `..\SANScreen\cognos\analytics\configuration\cogstartup.xml`.
2. 아래의 `""certs""` 및 `""csk""` 폴더의 백업을 만듭니다 `..\SANScreen\cognos\analytics\configuration`.

3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.

a. `CD "\\Program Files\sansscreen\cognos\analytics\bin"`

b. `ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -d "CN=FQDN,O=orgname,C=US" -r c:\temp\encryptRequest.csr`

4. 를 엽니다 `c:\temp\encryptRequest.csr` 생성된 콘텐츠를 파일로 만들어 복사합니다.

5. SSL 인증서를 얻으려면 `encryptRequest.csr`을 CA(인증 기관)에 보냅니다.

"san:dns=FQDN(예: hostname.netapp.com)" SubjectAltName을 추가하려면 추가 속성)을 추가해야 합니다. Google Chrome 버전 58 이상에서 SubjectAltName이 인증서에서 누락되면 불만을 표시합니다.

6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다

FQDN.p7b 파일이 다운로드됩니다

7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.

8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.

a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.

b. 왼쪽 창에서 ""인증서""를 찾습니다.

c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.

d. Base64 출력을 선택합니다.

e. 루트 인증서로 식별하는 파일 이름을 입력합니다.

f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a-8C단계를 반복합니다.

g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.

9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.

a. 메모장에서 intermediate.cer를 열고 내용을 복사합니다.

b. 메모장에서 root.cer를 열고 9a의 콘텐츠를 저장합니다.

c. 파일을 CA.CER로 저장합니다.

10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.

a. `cd ""Program Files\SANscreen\cognos\analytics\bin"`

b. `ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\CA.cer`

그러면 CA.cer가 루트 인증 기관으로 설정됩니다.

c. `ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\CA.cer`

이렇게 하면 Cognos.cer 가 CA.cer 에 의해 서명된 암호화 인증서로 설정됩니다.

11. IBM Cognos 구성을 엽니다.

a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다

b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.

- c. 구성을 저장합니다.
 - d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
- a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" -exportcert -file "" c:\temp\cognos.crt" -keystore "D:\Program Files\SANscreen\cognos\analytics\configuration\certs\CAMKeystore" -storetype PKCS12-storepass NoPassSet-alias 암호화
13. 관리 CMD 프롬프트 창을 사용하여 "c:\temp\cognos.crt"를 dWh trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
- a. "D:\Program Files\SANscreen\Java\bin\keytool.exe" - importcert -file ""c:\temp\cognos.crt" - keystore "D:\Program Files\SANscreen\standalone\configuration\server.trustore" - storepass changeit -alias cognosert
14. SANscreen 서비스를 다시 시작합니다.
15. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.

Cognos 및 DWH에 대해 CA 서명 SSL 인증서 가져오기(Insight 7.3.10 이상)

SSL 인증서를 추가하여 데이터 웨어하우스 및 Cognos 환경에 대한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

이 절차는 OnCommand Insight 7.3.10 이상을 실행하는 시스템에 적용됩니다.

최신 CAC 및 인증서 지침은 다음 기술 자료 문서를 참조하십시오(Support login required).



- "OnCommand Insight에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "OnCommand Insight 데이터 웨어하우스에 대한 CAC(Common Access Card) 인증을 구성하는 방법"
- "CA(인증 기관) 서명 인증서를 만들어 OnCommand Insight 및 OnCommand Insight 데이터 웨어하우스 7.3.x로 가져오는 방법"
- "Windows 호스트에 설치된 OnCommand Insight 7.3.X 내에서 자체 서명된 인증서를 만드는 방법"
- "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

이 작업에 대해

이 절차를 수행하려면 관리자 권한이 있어야 합니다.

단계

1. IBM Cognos 구성 도구를 사용하여 Cognos를 중지합니다. Cognos를 닫습니다.

2. 의 백업을 생성합니다 ..\SANSscreen\cognos\analytics\configuration 및 ..\SANSscreen\cognos\analytics\temp\cam\freshness 폴더.
3. Cognos에서 인증서 암호화 요청을 생성합니다. 관리자 CMD 창에서 다음을 실행합니다.
 - a. CD "\Program Files\sansscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat -java:local -c -e -p NoPassWordSet -a RSA -r c:\temp\encryptRequest.csr -d "CN=server.domain.com,O=NETAPP,C=US" -H "server.domain.com" -I "ipaddress". 참고: 여기서 -H와 -I는 DNS 및 ipaddress와 같은 subjectAltNames를 추가합니다.
4. 를 엽니다 c:\temp\encryptRequest.csr 생성된 콘텐츠를 파일로 만들어 복사합니다.
5. encryptRequest.csr 콘텐츠를 입력하고 CA 서명 포털을 사용하여 인증서를 생성합니다.
6. PKCS7 형식을 사용하여 루트 인증서를 포함시켜 체인 인증서를 다운로드합니다
FQDN.p7b 파일이 다운로드됩니다
7. CA에서 .p7b 형식의 인증서를 가져옵니다. Cognos Webserver의 인증서로 표시하는 이름을 사용합니다.
8. ThirdPartyCertificateTool.bat 에서 전체 체인을 가져오지 못하므로 모든 인증서를 내보내려면 여러 단계가 필요합니다. 다음과 같이 체인을 개별적으로 내보내서 분할합니다.
 - a. ""Crypto Shell Extensions""에서 .p7b 인증서를 엽니다.
 - b. 왼쪽 창에서 ""인증서""를 찾습니다.
 - c. 루트 CA > 모든 작업 > 내보내기를 마우스 오른쪽 버튼으로 클릭합니다.
 - d. Base64 출력을 선택합니다.
 - e. 루트 인증서로 식별하는 파일 이름을 입력합니다.
 - f. 모든 인증서를 .cer 파일로 별도로 내보내려면 8a ~ 8e 단계를 반복합니다.
 - g. 파일 이름을 mediateX.cer 및 cognos.cer 로 지정합니다.
9. CA 인증서가 하나만 있는 경우 이 단계를 무시하거나, 그렇지 않으면 root.cer와 mediateX.cer를 모두 하나의 파일로 병합합니다.
 - a. 메모장에서 root.cer를 열고 내용을 복사합니다.
 - b. 메모장을 사용하여 intermediate.cer를 열고 9a(중간 우선 및 루트 다음)의 콘텐츠를 추가합니다.
 - c. 파일을 chain.cer로 저장합니다.
10. 관리자 CMD 프롬프트를 사용하여 Cognos 키 저장소로 인증서를 가져옵니다.
 - a. cd ""Program Files\SANSscreen\cognos\analytics\bin"
 - b. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\root.cer
 - c. ThirdPartyCertificateTool.bat - java:local -i -T -r c:\temp\intermediate.cer
 - d. ThirdPartyCertificateTool.bat - java:local -i -e -r c:\temp\cognos.cer -t c:\temp\chain.cer
11. IBM Cognos 구성을 엽니다.
 - a. 로컬 구성 → 보안 → 암호화 → Cognos 를 선택합니다
 - b. "Use third party CA?"를 변경합니다. 를 True로 설정합니다.
 - c. 구성을 저장합니다.

- d. Cognos를 다시 시작합니다
12. 관리 CMD 프롬프트를 사용하여 최신 Cognos 인증서를 cognos.crt로 내보냅니다.
 - a. CD "C:\Program Files\SANscreen"
 - b. java\bin\keytool.exe -exportcert -file c:\temp\cognos.crt -keystore cognos\analytics\configuration\certs\CAMKeystore-storetype pkcs12-storepass NoPassWordSet-alias encryption
13. 에서 DWH 서버 트루스토어를 백업합니다. .\SANscreen\wildfly\standalone\configuration\server.trustore
14. 관리 CMD 프롬프트 창을 사용하여 "c:\temp\cognos.crt"를 DWH trustore로 가져와서 Cognos와 DWH 간에 SSL 통신을 설정합니다.
 - a. CD "C:\Program Files\SANscreen"
 - b. java\bin\keytool.exe - importcert -file c:\temp\cognos.crt -keystore wandiderfly\standalone\configuration\server.trustore -storephass changeit -alias coclnos3rdca
15. SANscreen 서비스를 다시 시작합니다.
16. DWH 백업을 수행하여 DWH가 Cognos와 통신하는지 확인합니다.
17. 's' 인증서만 변경되고 기본 Cognos 인증서는 변경되지 않은 경우에도 다음 단계를 수행해야 합니다. 그렇지 않으면 Cognos가 새 SANscreen 인증서에 대해 불만을 제기하거나 DWH 백업을 생성할 수 없습니다.
 - a. cd "%SANSCREEN_HOME%cognos\analytics\bin\"
 - b. "%SANSCREEN_HOME%java64\bin\keytool.exe" -exportcert -file "c:\temp\sanscreen.cer" -keystore "%SANSCREEN_HOME%wildfly\standalone\configuration\server.keystore" -storepass changeit -alias "ssl certificate"
 - c. ThirdPartyCertificateTool.bat -java:local -i -T -r "c:\temp\sanscreen.cer"

일반적으로 이러한 단계는 에 설명된 Cognos 인증서 가져오기 프로세스의 일부로 수행됩니다 "Cognos CA(인증 기관) 서명 인증서를 OnCommand Datawarehouse 7.3.3 이상으로 가져오는 방법"

SSL 인증서를 가져오는 중입니다

SSL 인증서를 추가하여 OnCommand Insight 환경의 보안을 강화하기 위한 향상된 인증 및 암호화를 활성화할 수 있습니다.

시작하기 전에

시스템이 최소 필수 비트 수준(1024비트)을 충족하는지 확인해야 합니다.

이 작업에 대해



이 절차를 수행하기 전에 기존 를 백업해야 합니다 server.keystore 파일 및 백업 이름을 지정합니다 server.keystore.old. 의 손상 또는 손상 server.keystore Insight 서버를 다시 시작한 후 Insight 서버가 작동하지 않을 수 있습니다. 백업을 생성하는 경우 문제가 발생할 경우 이전 파일로 되돌릴 수 있습니다.

단계

1. 원본 키 저장소 파일의 복사본을 만듭니다. `cp c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore.old"`
2. 키 저장소의 내용을 나열합니다. `C:\Program Files\SANscreen\java64\bin\keytool.exe -list -v -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
 - a. 암호를 묻는 메시지가 나타나면 를 입력합니다 `changeit`.

키 저장소의 내용이 표시됩니다. 키 저장소에 인증서가 하나 이상 있어야 합니다. "ssl certificate".
3. 를 삭제합니다 `"ssl certificate":keytool -delete -alias "ssl certificate" -keystore c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore`
4. 새 키 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -genkey -alias "ssl certificate" -keyalg RSA -keysize 2048 -validity 365 -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"`
 - a. 성과 이름을 묻는 메시지가 나타나면 사용하려는 FQDN(정규화된 도메인 이름)을 입력합니다.
 - b. 조직 및 조직 구조에 대한 다음 정보를 제공합니다.
 - 국가: 해당 국가의 두 글자 ISO 약어(예: US)
 - 시/도: 조직의 본사 소재지가 위치한 시/도의 이름(예: 매사추세츠주)
 - 지역: 조직의 본사 소재지(예: Waltham)의 이름입니다.
 - 조직 이름: 도메인 이름을 소유한 조직의 이름(예: NetApp)
 - 조직 단위 이름: 인증서를 사용할 부서 또는 그룹의 이름(예: 지원)
 - 도메인 이름/일반 이름: 서버의 DNS 조회에 사용되는 FQDN(예: `www.example.com`) 시스템이 다음과 유사한 정보로 응답합니다. `Is CN=www.example.com, OU=support, O=NetApp, L=Waltham, ST=MA, C=US correct?`
 - c. 를 입력합니다 `Yes` CN(Common Name)이 FQDN과 같은 경우
 - d. 키 암호를 묻는 메시지가 나타나면 암호를 입력하거나 Enter 키를 눌러 기존 키 저장소 암호를 사용합니다.
5. 인증서 요청 파일 생성: `C:\Program Files\SANscreen\java64\bin\keytool.exe -certreq -alias "ssl certificate" -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore" -file c:\localhost.csr`

를 클릭합니다 `c:\localhost.csr` file 은 새로 생성된 인증서 요청 파일입니다.
6. 를 제출합니다 `c:\localhost.csr` 승인을 위해 CA(인증 기관)에 파일을 저장합니다.

인증서 요청 파일이 승인되면 에서 인증서를 반환하도록 합니다 .der 형식. 파일이 로 반환될 수도 있고 반환되지 않을 수도 있습니다 .der 파일. 기본 파일 형식은 입니다 .cer Microsoft CA 서비스의 경우.

대부분의 조직의 CA는 루트 CA를 포함하여 신뢰할 수 있는 모델 체인을 사용합니다. 이 모델은 대개 오프라인 상태입니다. 이 인증서는 중간 CA라고 하는 몇 개의 하위 CA에 대해서만 인증서에 서명했습니다.

전체 신뢰 체인에 대한 공개 키(인증서)를 얻어야 합니다. 즉, OnCommand Insight 서버의 인증서에 서명한 CA의 인증서와 조직 루트 CA에 등록하는 CA 간의 모든 인증서를 얻어야 합니다.

일부 조직에서는 서명 요청을 제출할 때 다음 중 하나를 받을 수 있습니다.

- 서명된 인증서와 신뢰 체인에서 모든 공개 인증서가 들어 있는 PKCS12 파일입니다
- A.zip 개별 파일(서명된 인증서 포함)과 신뢰 체인에서 모든 공용 인증서를 포함하는 파일입니다
- 서명된 인증서만

공용 인증서를 얻어야 합니다.

7. server.keystore에 대해 승인된 인증서를 가져옵니다. C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.keystore"

- a. 메시지가 표시되면 키 저장소 암호를 입력합니다.

다음 메시지가 표시됩니다. Certificate reply was installed in keystore

8. 서버에 대해 승인된 인증서를 가져옵니다. trustore: C:\Program Files\SANscreen\java64\bin\keytool.exe -importcert -alias OCI.hostname.com -file c:\localhost2.DER -keystore "c:\Program Files\SANscreen\wildfly\standalone\configuration\server.trustore"

- a. 메시지가 표시되면 Trustore 암호를 입력합니다.

다음 메시지가 표시됩니다. Certificate reply was installed in trustore

9. 를 편집합니다 SANscreen\wildfly\standalone\configuration\standalone-full.xml 파일:

다음 별칭 문자열을 대체합니다. alias="cbc-oci-02.muccbc.hq.netapp.com". 예를 들면 다음과 같습니다.

```
<keystore path="server.keystore" relative-to="jboss.server.config.dir"
keystore-password="${VAULT::HttpsRealm::keystore_password::1}" alias="cbc-oci-
02.muccbc.hq.netapp.com" key-
password="${VAULT::HttpsRealm::key_password::1}"/>
```

10. SANscreen 서버 서비스를 다시 시작합니다.

Insight가 실행되면 자물쇠 아이콘을 클릭하여 시스템에 설치된 인증서를 볼 수 있습니다.

"발급자" 정보와 일치하는 "발급 대상" 정보가 포함된 인증서가 표시되는 경우 자체 서명된 인증서가 설치되어 있는 것입니다. Insight 설치 관리자가 생성한 자체 서명 인증서의 만료 기간은 100년입니다.

NetApp은 이 절차로 디지털 인증서 경고가 제거된다고 보장할 수 없습니다. NetApp은 최종 사용자 워크스테이션의 구성 방법을 제어할 수 없습니다. 다음과 같은 시나리오를 고려해 보십시오.

- Microsoft Internet Explorer와 Google Chrome 모두 Windows에서 Microsoft의 기본 인증서 기능을 사용합니다.

즉, Active Directory 관리자가 조직의 CA 인증서를 최종 사용자의 인증서 트루스토어로 푸시하면 OnCommand Insight 자체 서명된 인증서가 내부 CA 인프라에서 서명한 인증서로 교체되면 이러한 브라우저의 사용자에게 인증서 경고가 사라집니다.

- Java 및 Mozilla Firefox에는 자체 인증서 저장소가 있습니다.

시스템 관리자가 CA 인증서를 이러한 응용 프로그램의 신뢰할 수 있는 인증서 저장소에 자동으로 수집하지 않는 경우 자체 서명된 인증서가 교체되더라도 신뢰할 수 없는 인증서로 인해 Firefox 브라우저를 사용하면 인증서 경고가 계속 생성될 수 있습니다. 조직의 인증서 체인을 Trustore에 설치하는 것도 추가 요구 사항입니다.

업무 엔티티 계층 구조

환경 데이터를 더 세밀한 수준에서 추적 및 보고할 비즈니스 엔티티를 정의할 수 있습니다.

OnCommand Insight에서 비즈니스 엔티티 계층에는 다음 수준이 포함되어 있습니다.

- * 테넌트 * 는 서비스 공급자가 주로 리소스를 NetApp과 같은 고객과 연결하는 데 사용됩니다.
- * LOB(Line of Business) * 는 회사 내 사업 부문 또는 제품 라인입니다(예: 데이터 스토리지).
- * 사업부 * 는 법률 또는 마케팅과 같은 전통적인 사업부를 나타냅니다.
- * Project * 는 종종 용량 비용 청구를 원하는 사업부 내의 특정 프로젝트를 식별하는 데 사용됩니다. 예를 들어 "특허"는 법률 부서의 프로젝트 이름일 수 있으며 "판매 이벤트"는 마케팅 부서의 프로젝트 이름일 수 있습니다. 수준 이름에는 공백이 포함될 수 있습니다.

회사 계층 구조의 디자인에 있는 모든 수준을 사용할 필요는 없습니다.

비즈니스 엔티티 계층 구조 디자인

OnCommand Insight 데이터베이스의 고정 구조가 되기 때문에 회사 구조의 요소와 비즈니스 엔티티에 표시해야 할 요소를 이해해야 합니다. 다음 정보를 사용하여 업무 엔티티를 설정할 수 있습니다. 이러한 범주의 데이터를 수집하기 위해 모든 계층 레벨을 사용할 필요는 없습니다.

단계

1. 각 업무 엔티티 계층 수준을 검토하여 해당 수준이 회사의 업무 엔티티 계층 구조에 포함되어야 하는지 확인합니다.
 - 회사가 ISP인 경우 * Tenant * 레벨이 필요하며, 고객의 자원 사용량을 추적하고자 하는 경우.
 - * 여러 제품 라인의 데이터를 추적해야 하는 경우 계층 구조에 LOB(Line of Business) * 가 필요합니다.
 - 서로 다른 부서의 데이터를 추적해야 하는 경우 * 사업부 * 가 필요합니다. 이러한 계층 수준은 한 부서가 다른 부서에서 사용하지 않는 리소스를 분리하는 데 유용합니다.
 - * Project * 레벨은 부서 내 특수 작업에 사용할 수 있습니다. 이 데이터는 회사 또는 부서의 다른 프로젝트와 비교하여 개별 프로젝트의 기술 요구 사항을 정확히 파악하고 정의하며 모니터링하는 데 유용할 수 있습니다.
2. 각 업무 엔티티를 보여 주는 차트를 만들고 엔티티 내의 모든 수준 이름을 표시합니다.
3. 계층 구조의 이름을 확인하여 OnCommand Insight 보기 및 보고서에 대한 설명이 있는지 확인합니다.
4. 각 업무 엔티티와 관련된 모든 애플리케이션을 식별합니다.

비즈니스 엔티티 생성

회사의 비즈니스 엔티티 계층 구조를 디자인한 후 응용 프로그램을 설정한 다음 비즈니스 엔티티를 응용 프로그램과 연결할 수 있습니다. 이 프로세스는 OnCommand Insight 데이터베이스에 업무 엔티티 구조를 만듭니다.

이 작업에 대해

응용 프로그램을 비즈니스 엔티티와 연결하는 것은 선택 사항이지만 이는 최선의 방법입니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 업무 엔티티 * 를 선택합니다.

사업체 페이지가 표시됩니다.

3. 을 클릭합니다  새 요소 작성을 시작합니다.

[업무 엔티티 추가] * 대화 상자가 표시됩니다.

4. 각 엔티티 수준(테넌트, 사업부, 사업부 및 프로젝트)에 대해 다음 중 하나를 수행할 수 있습니다.
 - 요소 수준 목록을 클릭하고 값을 선택합니다.
 - 새 값을 입력하고 Enter 키를 누릅니다.
 - 업무 엔티티에 엔티티 수준을 사용하지 않으려면 엔티티 수준 값을 N/A로 둡니다.
5. 저장 * 을 클릭합니다.

자산에 업무 엔티티 할당

자산에 업무 엔티티를 할당할 수 있습니다(호스트, 포트, 스토리지, 스위치, 가상 시스템, 비즈니스 엔티티를 애플리케이션에 연결하지 않고 qtree, 공유, 볼륨 또는 내부 볼륨). 그러나 해당 자산이 비즈니스 엔티티와 관련된 애플리케이션에 연결되어 있는 경우 비즈니스 엔티티가 자산에 자동으로 할당됩니다.

시작하기 전에

이미 업무 엔티티를 생성해야 합니다.


이 작업에 대해


자산에 직접 비즈니스 엔티티를 할당할 수 있지만 자산에 애플리케이션을 할당한 다음 자산에 비즈니스 엔티티를 할당하는 것이 좋습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 업무 엔티티를 적용할 자산을 찾습니다.

◦ 자산 대시보드에서 자산을 클릭합니다.


◦ 을 클릭합니다  도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.

3. 자산 페이지의 * 사용자 데이터 * 섹션에서 * 비즈니스 엔티티 * 옆에 * 없음 * 으로 커서를 이동한 다음 를 클릭합니다 .

사용 가능한 업무 엔티티 목록이 표시됩니다.

4. 검색 * 상자에 특정 엔티티의 목록을 필터링하거나 목록을 아래로 스크롤하거나 목록에서 비즈니스 엔티티를 선택합니다.

선택한 업무 엔티티가 애플리케이션에 연결되어 있으면 애플리케이션 이름이 표시됩니다. 이 경우 사업주명 옆에 "파생된"이라는 단어가 나타납니다. 연결된 응용 프로그램이 아닌 자산에 대해서만 엔티티를 유지하려면 응용 프로그램의 할당을 수동으로 재정의할 수 있습니다.

5. 업무 엔티티로부터 파생된 응용 프로그램을 재정의하려면 응용 프로그램 이름 위에 커서를 놓고 를 클릭합니다  다른 업무 엔티티를 선택하고 목록에서 다른 애플리케이션을 선택합니다.


여러 자산에 비즈니스 엔티티를 할당하거나 제거합니다

수동으로 할당하거나 제거할 필요 없이 쿼리를 사용하여 여러 자산에 비즈니스 엔티티를 할당하거나 제거할 수 있습니다.


시작하기 전에

원하는 자산에 추가할 비즈니스 엔티티를 이미 만들어야 합니다.


단계

1. 새 쿼리를 만들거나 기존 쿼리를 엽니다.
2. 필요한 경우 비즈니스 엔티티를 추가할 자산을 필터링합니다.
3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다  모두 * 를 선택합니다.

작업 * 버튼이 표시됩니다.

4. 선택한 자산에 업무 엔티티를 추가하려면 을 클릭합니다 . 선택한 자산 유형에 업무 엔티티가 할당되어 있을 수 있는 경우, [업무 엔티티 추가]에 대한 메뉴 선택이 표시됩니다. 이 옵션을 선택합니다.
5. 목록에서 원하는 업무 엔티티를 선택하고 * 저장 * 을 클릭합니다.

지정한 새 업무 엔티티는 이미 자산에 할당된 모든 업무 엔티티보다 우선합니다. 자산에 애플리케이션을 할당하면 동일한 방식으로 할당된 비즈니스 엔티티도 무시됩니다. 비즈니스 엔티티를 자산으로 할당하면 해당 자산에 할당된 모든 애플리케이션도 재정의될 수 있습니다.

6. 자산에 할당된 업무 엔티티를 제거하려면 를 클릭합니다  을 클릭하고 * 업무 엔티티 제거 * 를 선택합니다.
7. 목록에서 원하는 업무 엔티티를 선택하고 * 삭제 * 를 클릭합니다.

주석 정의

회사 요구사항에 맞게 데이터를 추적하도록 OnCommand Insight을 사용자 지정할 때 자산의 수명 종료, 데이터 센터, 건물 위치, 스토리지 계층 또는 볼륨 등 데이터를 완벽하게 파악하는 데 필요한 특수 주석을 정의할 수 있습니다. 내부 볼륨 서비스 레벨을 지원합니다.

단계

1. 환경 데이터를 연결해야 하는 업계 용어를 나열하십시오.
2. 비즈니스 엔티티를 사용하여 아직 추적되지 않은 환경 데이터를 연결해야 하는 기업 용어를 나열하십시오.
3. 사용할 수 있는 기본 주석 유형을 식별합니다.
4. 만들어야 하는 사용자 지정 주석을 식별합니다.

주석을 사용하여 환경을 모니터링합니다

회사 요구 사항에 맞는 데이터를 추적하도록 OnCommand Insight를 사용자 지정할 때 `_annotations_`라는 특수 메모를 정의하여 자산에 할당할 수 있습니다. 예를 들어, 자산의 수명 종료, 데이터 센터, 건물 위치, 스토리지 계층 또는 볼륨 서비스 수준과 같은 정보에 주석을 달 수 있습니다.

주석을 사용하여 환경을 모니터링하는 데 유용한 작업은 다음과 같습니다.

- 모든 주석 유형에 대한 정의를 만들거나 편집합니다.
- 자산 페이지를 표시하고 각 자산을 하나 이상의 주석과 연결합니다.

예를 들어, 자산이 임대되고 2개월 이내에 임대가 만료되는 경우 자산에 수명 종료 주석을 적용할 수 있습니다. 이렇게 하면 다른 사용자가 해당 자산을 장기간 사용하지 못하게 할 수 있습니다.

- 같은 유형의 여러 자산에 주석을 자동으로 적용하는 규칙을 작성합니다.
- 주석 가져오기 유틸리티를 사용하여 주석을 가져옵니다.
- 주석을 기준으로 자산을 필터링합니다.
- 주석을 기반으로 보고서의 데이터를 그룹화하고 해당 보고서를 생성합니다.

보고서에 대한 자세한 내용은 `_OnCommand Insight 보고 가이드_`를 참조하십시오.

주석 유형 관리

OnCommand Insight는 자산 수명 주기(생일 또는 수명 종료), 건물 또는 데이터 센터 위치, 계층 등 보고서에 표시되도록 사용자 지정할 수 있는 몇 가지 기본 주석 유형을 제공합니다. 기본 주석 유형의 값을 정의하거나 사용자 정의 주석 유형을 직접 만들 수 있습니다. 나중에 이러한 값을 편집할 수 있습니다.

OnCommandInsight는 몇 가지 기본 주석 유형을 제공합니다. 이러한 주석은 데이터를 필터링하거나 그룹화하고 데이터 보고를 필터링하는 데 사용할 수 있습니다.

다음과 같은 기본 주석 유형과 자산을 연결할 수 있습니다.

- 생일, 일몰 또는 수명 종료 등의 자산 수명 주기
- 데이터 센터, 건물 또는 바닥과 같은 장치에 대한 위치 정보
- 품질(계층), 연결된 장치(스위치 수준) 또는 서비스 수준별 자산 분류
- 핫(높은 활용도) 등의 상태

다음 표에는 기본 주석 유형이 나열되어 있습니다. 이러한 주석 이름을 필요에 맞게 편집할 수 있습니다.

주석 유형	설명	유형
별칭	리소스에 대한 사용자 친화적인 이름입니다.	텍스트
생일	장치가 온라인 상태가 되거나 온라인으로 전환되는 날짜입니다.	날짜
건물	호스트, 스토리지, 스위치 및 테이프 리소스의 물리적 위치	목록
도시	호스트, 스토리지, 스위치 및 테이프 리소스의 지방자치당국 위치	목록
컴퓨팅 리소스 그룹	Host 및 VM Filesystems 데이터 소스에서 사용하는 그룹 할당입니다.	목록
대륙	호스트, 스토리지, 스위치 및 테이프 리소스의 지리적 위치	목록
국가	호스트, 스토리지, 스위치 및 테이프 리소스의 국가별 위치	목록
데이터 센터	리소스의 물리적 위치이며 호스트, 스토리지 시스템, 스위치 및 테이프에서 사용할 수 있습니다.	목록
직접 연결	스토리지 리소스가 호스트에 직접 접속되어 있으면 (예 또는 아니요)를 나타냅니다.	부울

수명 종료	예를 들어 임대가 만료되었거나 하드웨어가 폐기되는 경우 장치가 오프라인 상태가 되는 날짜입니다.	날짜
패브릭 별칭	Fabric의 사용자 친화적인 이름입니다.	텍스트
바닥	건물 바닥에 있는 장치의 위치. 호스트, 스토리지 시스템, 스위치 및 테이프에 대해 설정할 수 있습니다.	목록
핫	이미 사용량이 많은 디바이스를 정기적으로 또는 용량 임계값으로 사용 중입니다.	부울
참고	자원에 연결할 메모입니다.	텍스트
랙	리소스가 상주하는 랙입니다.	텍스트
있습니다	호스트, 스토리지, 스위치 및 테이프 리소스의 건물 또는 기타 위치 내의 공간입니다.	목록
산	네트워크의 논리 파티션입니다. 호스트, 스토리지 시스템, 테이프, 스위치 및 애플리케이션에서 사용할 수 있습니다.	목록
서비스 수준	리소스에 할당할 수 있는 지원되는 서비스 수준 집합입니다. 내부 볼륨, qtree, 볼륨에 대한 정렬 옵션 목록을 제공합니다. 서비스 수준을 편집하여 다양한 수준에 대한 성능 정책을 설정합니다.	목록
시/도	리소스가 있는 시/군/구 또는 시/군/구	목록
일몰	해당 디바이스에 새 할당을 수행할 수 없는 임계값을 설정합니다. 계획된 마이그레이션 및 기타 보류 중인 네트워크 변경에 유용합니다.	날짜

스위치 레벨	에는 스위치에 대한 범주를 설정하기 위한 미리 정의된 옵션이 포함되어 있습니다. 일반적으로 이러한 지정은 필요한 경우 편집할 수 있지만 장치의 수명 기간 동안 유지됩니다. 스위치에만 사용할 수 있습니다.	목록
계층	는 사용자 환경 내에서 서로 다른 서비스 수준을 정의하는 데 사용할 수 있습니다. 계층은 필요한 속도(예: 금 또는 은)와 같은 수준의 유형을 정의할 수 있습니다. 이 기능은 내부 볼륨, Qtree, 스토리지 어레이, 스토리지 풀 및 볼륨에서만 사용할 수 있습니다.	목록
위반 심각도입니다	중요도가 가장 높은 계층부터 가장 낮은 계층까지 위반 등급(예: 중요)의 순위를 지정합니다(예: 호스트 포트 누락 또는 이중화 누락).	목록



별칭, 데이터 센터, 핫, 서비스 레벨, 일물, 스위치 수준, 서비스 수준, 계층 및 위반 심각성 은 시스템 수준 주석으로, 삭제하거나 이름을 바꿀 수 없습니다. 할당된 값만 변경할 수 있습니다.

주석 지정 방법

주석 규칙을 사용하여 수동으로 또는 자동으로 주석을 지정할 수 있습니다. 또한 OnCommand Insight는 자산 취득 및 상속에 대한 일부 주석을 자동으로 할당합니다. 자산에 할당한 주석은 자산 페이지의 사용자 데이터 섹션에 표시됩니다.

주석은 다음과 같은 방법으로 지정됩니다.

- 주석을 자산에 수동으로 지정할 수 있습니다.

주석을 자산에 직접 지정하면 주석이 자산 페이지에 일반 텍스트로 표시됩니다. 수동으로 할당된 주석은 항상 주석 규칙에 의해 상속되거나 할당된 주석보다 우선합니다.

- 동일한 유형의 자산에 주석을 자동으로 할당하는 주석 규칙을 생성할 수 있습니다.

주석이 규칙별로 할당된 경우 Insight는 자산 페이지의 주석 이름 옆에 규칙 이름을 표시합니다.

- Insight는 계층 레벨을 스토리지 계층 모델과 자동으로 연결하여 자산 구입 시 리소스에 스토리지 주석을 신속하게 할당할 수 있습니다.

특정 스토리지 리소스는 사전 정의된 계층(계층 1 및 계층 2)과 자동으로 연결됩니다. 예를 들어 Symmetrix 스토리지 계층은 Symmetrix 및 VMAX 제품군을 기반으로 하며 계층 1과 연결됩니다. 계층 요구 사항에 맞게 기본값을 변경할 수 있습니다. 주석을 Insight(예: 계층)에 할당하면 자산 페이지의 주석 이름 위에 커서를 놓으면 "시스템 정의"가 표시됩니다.

- 일부 리소스(자산의 하위 항목)는 자산(상위)에서 사전 정의된 계층 주석을 파생시킬 수 있습니다.

예를 들어, 주석을 스토리지에 할당할 경우 계층 주석은 모든 스토리지 풀, 내부 볼륨, 볼륨, Qtree 및 스토리지에 속한 공유에 의해 파생됩니다. 스토리지의 내부 볼륨에 다른 주석이 적용되는 경우 주석은 이후에 모든 볼륨, qtree 및 공유에 의해 파생됩니다. 자산 페이지의 주석 이름 옆에 "Deribed"가 나타납니다.


주석과 비용 연관

비용 관련 보고서를 실행하기 전에 비용을 서비스 수준, 스위치 수준 및 계층 시스템 수준 주석과 연계해야 합니다. 그러면 운영 및 복제 용량의 실제 사용량을 기준으로 스토리지 사용자에게 비용 청구가 수행될 수 있습니다. 예를 들어, 계층 레벨의 경우 골드 및 실버 등급 값을 가지고 실버 계층보다 더 높은 비용을 골드 계층에 할당할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 관리를 클릭하고 * 주석 * 을 선택합니다.


주석 페이지가 표시됩니다.

3. 서비스 수준, 스위치 수준 또는 계층 주석 위에 커서를 놓고 를 클릭합니다 .

Edit Annotation(주석 편집) 대화 상자가 표시됩니다.

4. 비용 * 필드에 기존 수준의 값을 입력합니다.

계층 및 서비스 수준 주석에는 각각 자동 계층 및 오브젝트 스토리지 값이 있으며, 이 값은 제거할 수 없습니다.

5. 을 클릭합니다  를 눌러 수준을 추가합니다.
6. 작업을 마치면 * 저장 * 을 클릭합니다.

사용자 정의 주석 작성

주석을 사용하여 비즈니스 요구에 맞는 맞춤형 비즈니스 관련 데이터를 자산에 추가할 수 있습니다. OnCommand Insight에서 기본 주석 집합을 제공하는 경우 다른 방법으로 데이터를 볼 수 있습니다. 사용자 지정 주석의 데이터는 스위치 제조업체, 포트 수 및 성능 통계와 같이 이미 수집된 장치 데이터를 보완합니다. 주석을 사용하여 추가하는 데이터는 Insight에서 검색되지 않습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

주석 페이지에는 주석 목록이 표시됩니다.

3. 을 클릭합니다 .

주석 추가 * 대화 상자가 표시됩니다.

4. 이름 * 및 * 설명 * 필드에 이름과 설명을 입력합니다.

이 필드에는 최대 255자까지 입력할 수 있습니다.



점 ""으로 시작하거나 끝나는 주식 이름. 지원되지 않습니다.

5. Type * 을 클릭한 다음 이 주식에 허용되는 데이터 유형을 나타내는 다음 옵션 중 하나를 선택합니다.

◦ 부울

그러면 예 및 아니요 선택 항목이 있는 드롭다운 목록이 만들어집니다 예를 들어 "Direct Attached" 주식은 Boolean입니다.

◦ 날짜

이렇게 하면 날짜가 들어 있는 필드가 만들어집니다. 예를 들어, 주식이 날짜가 될 경우 이를 선택합니다.

◦ 목록

이렇게 하면 다음 중 하나가 생성될 수 있습니다.

▪ 드롭다운 고정 목록

다른 사용자가 장치에 이 주식 유형을 할당하는 경우 목록에 값을 더 추가할 수 없습니다.

▪ 드롭다운 유연한 목록

이 목록을 만들 때 * Add new values on the fly * 옵션을 선택하면 다른 사용자가 장치에 이 주식 유형을 할당할 때 목록에 더 많은 값을 추가할 수 있습니다.

◦ 번호

이렇게 하면 주식을 지정하는 사용자가 숫자를 입력할 수 있는 필드가 생성됩니다. 예를 들어, 주식 유형이 ""바닥""인 경우 사용자는 ""숫자""의 값 유형을 선택하고 바닥 번호를 입력할 수 있습니다.

◦ 텍스트

그러면 자유 형식 텍스트를 허용하는 필드가 만들어집니다. 예를 들어, 주식 유형으로 ""Language""를 입력하고 값 유형으로 ""Text""를 선택한 다음 언어를 값으로 입력할 수 있습니다.



유형을 설정하고 변경 사항을 저장한 후에는 주식 유형을 변경할 수 없습니다. 유형을 변경해야 하는 경우 주식을 삭제하고 새 주식을 만들어야 합니다.

6. 주식 유형으로 목록 을 선택한 경우 다음을 수행합니다.

- a. 자산 페이지에서 주식에 더 많은 값을 추가할 수 있는 기능을 원하는 경우 * 즉시 새 값 추가 * 를 선택하여 유연한 목록을 만듭니다.

예를 들어 자산 페이지에 있고 자산에는 Detroit, Tampa 및 Boston 값이 있는 City 주식이 있다고 가정해 보겠습니다. 빠른 실행 시 새 값 추가 * 옵션을 선택한 경우 주식 페이지로 이동하여 추가할 필요 없이 자산 페이지에서 샌프란시스코 및 시카고와 같은 도시에 직접 추가 값을 추가할 수 있습니다. 이 옵션을 선택하지 않으면 주식을 적용할 때 새 주식 값을 추가할 수 없습니다. 그러면 고정 목록이 생성됩니다.

b. 값 * 및 * 설명 * 필드에 값과 이름을 입력합니다.

c. 을 클릭합니다  를 눌러 추가 값을 추가합니다.

d. 을 클릭합니다  를 눌러 값을 제거합니다.

7. 저장 * 을 클릭합니다.

주석이 주식 페이지의 목록에 나타납니다.

◦ 관련 정보 *

"사용자 데이터 가져오기 및 내보내기"

자산에 주식 수동 할당

자산에 주식을 지정하면 비즈니스와 관련된 방식으로 자산을 정렬, 그룹화 및 보고할 수 있습니다. 주식 규칙을 사용하여 특정 유형의 자산에 주식을 자동으로 할당할 수 있지만 자산 페이지를 사용하여 개별 자산에 주식을 할당할 수 있습니다.

시작하기 전에


지정할 주식을 만들어야 합니다.

단계


1. OnCommand Insight 웹 UI에 로그인합니다.

2. 다음 중 하나를 수행하여 주식을 적용할 자산을 찾습니다.

◦ 자산 대시보드에서 자산을 클릭합니다.

◦ 을 클릭합니다  도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산의 유형 또는 이름을 입력한 다음 표시되는 목록에서 자산을 선택합니다.

자산 페이지가 표시됩니다.

3. 자산 페이지의 * 사용자 데이터 * 섹션에서 을 클릭합니다 .

주식 추가 대화 상자가 표시됩니다.


4. Annotation(주식) * 을 클릭하고 목록에서 주식을 선택합니다.

5. 값 * 을 클릭하고 선택한 주식 유형에 따라 다음 중 하나를 수행합니다.

◦ 주식 유형이 목록, 날짜 또는 부울인 경우 목록에서 값을 선택합니다.

◦ 주식 유형이 텍스트인 경우 값을 입력합니다.

6. 저장 * 을 클릭합니다.

7. 주식을 지정한 후 주식 값을 변경하려면 을 클릭합니다  다른 값을 선택합니다.

주석이 * 주식 지정 시 동적으로 값 추가 * 옵션을 선택한 목록 유형인 경우 기존 값을 선택하는 것 외에도 새 값을 추가하도록 입력할 수 있습니다.

주석 수정


주석의 이름, 설명 또는 값을 변경하거나 더 이상 사용하지 않을 주석을 삭제할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.

2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

주석 페이지가 표시됩니다.

3. 편집할 주석 위에 커서를 놓고 클릭합니다 .

Edit Annotation(주석 편집) * 대화 상자가 표시됩니다.


4. 주석을 다음과 같이 수정할 수 있습니다.


a. 이름, 설명 또는 둘 모두를 변경합니다.

그러나 이름과 설명 모두에 최대 255자를 입력할 수 있으며 주석 유형은 변경할 수 없습니다. 또한 시스템 수준 주석의 경우 이름이나 설명을 변경할 수 없지만, 주석이 목록 유형인 경우 값을 추가하거나 제거할 수 있습니다.



사용자 지정 주석이 데이터 웨어하우스에 게시되고 이름을 바꾸면 내역 데이터가 손실됩니다.

a. 목록 유형의 주석에 다른 값을 추가하려면  을 클릭합니다.

b. 목록 유형의 주석에서 값을 제거하려면  를 클릭합니다.

주석 값이 주석 규칙, 쿼리 또는 성능 정책에 포함된 주석과 관련된 경우 주석 값을 삭제할 수 없습니다.

5. 작업을 마치면 * 저장 * 을 클릭합니다.

작업을 마친 후

데이터 웨어하우스에서 주석을 사용하려는 경우 데이터 웨어하우스에서 주석을 강제로 업데이트해야 합니다. OnCommand Insight 데이터 웨어하우스 관리 가이드 _ 를 참조하십시오.

주석 삭제


더 이상 사용하지 않을 주석을 삭제할 수 있습니다. 시스템 수준 주석 또는 주석 규칙, 쿼리 또는 성능 정책에 사용되는 주석은 삭제할 수 없습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.

2. 관리 * 를 클릭하고 * 주석 * 을 선택합니다.

주석 페이지가 표시됩니다.

3. 삭제할 주석 위에 커서를 놓고  를 클릭합니다.

확인 대화 상자가 표시됩니다.

4. 확인 * 을 클릭합니다.

주석 규칙을 사용하여 자산에 주석 지정

사용자가 정의한 기준에 따라 자산에 주석을 자동으로 할당하려면 주석 규칙을 구성합니다. OnCommand Insight는 이러한 규칙에 따라 자산에 주석을 할당합니다. 또한 Insight에서는 두 가지 기본 주석 규칙을 제공합니다. 이 규칙은 필요에 맞게 수정하거나 사용하지 않으려는 경우 제거할 수 있습니다.

기본 스토리지 주석 규칙

스토리지 주석을 리소스에 빠르게 할당할 수 있도록 OnCommand Insight에는 21개의 기본 주석 규칙이 포함되어 있으며, 이 규칙은 계층 레벨을 스토리지 계층 모델과 연결합니다. 모든 스토리지 리소스는 귀사 환경에서 자산을 획득할 때 계층에 자동으로 연결됩니다.

기본 주석 규칙은 다음과 같은 방법으로 계층 주석을 적용합니다.

- 계층 1, 스토리지 품질 계층

Tier 1 주석은 EMC(Symmetrix), HDS(HDS9500V, HDS9900, HDS9900V, R600, R700, USP r, USP V), IBM(DS8000), NetApp(FAS6000 또는 FAS6200), Violin(Memory).

- 계층 2, 스토리지 품질 계층

Tier 2 주석은 HP(3PAR StoreServ 또는 EVA), EMC(CLARiiON), HDS(AMS 또는 D800), IBM(XIV), NetApp(FAS3000, FAS3100 및 FAS3200) 등의 공급업체 및 지정된 제품군에 적용됩니다.

이러한 규칙의 기본 설정을 계층 요구 사항에 맞게 편집하거나 필요하지 않은 경우 제거할 수 있습니다.

주석 규칙 작성

개별 자산에 주석을 수동으로 적용하는 대신 주석 규칙을 사용하여 여러 자산에 주석을 자동으로 적용할 수 있습니다. Insight에서 주석 규칙을 평가할 때 개별 자산 페이지에 수동으로 설정된 주석이 규칙 기반 주석보다 우선합니다.

시작하기 전에

주석 규칙에 대한 쿼리를 만들어야 합니다.

이 작업에 대해

규칙을 만드는 동안 주석 유형을 편집할 수 있지만, 미리 유형을 정의해야 합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 을 클릭합니다 .

규칙 추가 대화 상자가 표시됩니다.

4. 다음을 수행합니다.

- a. 이름 * 상자에 규칙을 설명하는 고유한 이름을 입력합니다.

이 이름은 주석 규칙 페이지에 표시됩니다.

- b. Query * 를 클릭하고 OnCommand Insight가 에셋에 주석을 적용하는 데 사용해야 하는 쿼리를 선택합니다.

- c. Annotation(주석) * 을 클릭하고 적용할 주석을 선택합니다.

- d. 값 * 을 클릭하고 주석 값을 선택합니다.

예를 들어 주석으로 생일 을 선택한 경우 값의 날짜를 지정합니다.

5. 저장 * 을 클릭합니다.

6. 모든 규칙을 즉시 실행하려면 * 모든 규칙 실행 * 을 클릭합니다. 그렇지 않으면 규칙들이 정기적으로 예약된 간격으로 실행됩니다.

주석 규칙 우선 순위 설정

기본적으로 OnCommand Insight에서는 주석 규칙을 순차적으로 평가합니다. 그러나 Insight에서 특정 순서로 규칙을 평가하려면 OnCommand Insight에서 주석 규칙을 평가하는 순서를 구성할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 주석 규칙 위에 커서를 놓습니다.

우선 순위 화살표가 규칙의 오른쪽에 나타납니다.

4. 목록에서 규칙을 위 또는 아래로 이동하려면 위쪽 화살표 또는 아래쪽 화살표를 클릭합니다.

기본적으로 새 규칙은 규칙 목록에 순차적으로 추가됩니다. Insight에서 주석 규칙을 평가할 때 개별 자산 페이지에 수동으로 설정된 주석이 규칙 기반 주석보다 우선합니다.


주석 규칙 수정

주석 규칙을 수정하여 규칙 이름, 주석, 주석 값 또는 규칙과 연결된 쿼리를 변경할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. Manage * 를 클릭하고 * Annotation rules * 를 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 수정할 규칙을 찾습니다.
 - 주석 규칙 페이지에서 필터 상자에 값을 입력하여 주석 규칙을 필터링할 수 있습니다.
 - 페이지에 맞는 규칙보다 더 많은 규칙이 있는 경우 페이지 번호를 클릭하여 페이지별로 주석 규칙을 찾아봅니다.
4. 다음 중 하나를 수행하여 * 규칙 편집 * 대화 상자를 표시합니다.
 - 주석 규칙 페이지에 있는 경우 주석 규칙 위에 커서를 놓고  을 클릭합니다.
 - 자산 페이지에 있는 경우 규칙과 연결된 주석 위에 커서를 놓고 규칙 이름이 표시되면 커서를 규칙 이름 위에 놓은 다음 규칙 이름을 클릭합니다.
5. 필요한 내용을 변경하고 * Save * 를 클릭합니다.


주석 규칙 삭제

규칙이 더 이상 네트워크의 개체를 모니터링할 필요가 없는 경우 주석 규칙을 삭제할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. 관리 * 를 클릭하고 * 주석 규칙 * 을 선택합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

3. 삭제할 규칙을 찾습니다.
 - 주석 규칙 페이지에서 필터 상자에 값을 입력하여 주석 규칙을 필터링할 수 있습니다.
 - 한 페이지에 맞는 규칙보다 더 많은 규칙이 있는 경우 페이지 번호를 클릭하여 페이지별로 주석 규칙을 찾아봅니다.
4. 삭제할 규칙 위에 커서를 놓은 다음  을 클릭합니다.

규칙을 삭제할 것인지 묻는 확인 메시지가 표시됩니다.

5. 확인 * 을 클릭합니다.

주석 값 불러오기

CSV 파일에서 SAN 객체(예: 스토리지, 호스트, 가상 머신)에 대한 주석을 유지하는 경우 해당 정보를 OnCommand Insight로 가져올 수 있습니다. 응용 프로그램, 사업체 또는 계층 및 건물 등의 주석을 가져올 수 있습니다.

이 작업에 대해

다음 규칙이 적용됩니다.

- 주석 값이 비어 있으면 해당 주석이 개체에서 제거됩니다.
- 볼륨 또는 내부 볼륨에 주석을 달 때 개체 이름은 대시 및 화살표(->) 구분 기호를 사용하여 스토리지 이름과 볼륨 이름의 조합입니다.

```
<storage_name>-><volume_name>
```

- 스토리지, 스위치 또는 포트에 주석이 추가된 경우 응용 프로그램 열은 무시됩니다.
- Tenant, Line_of_Business, Business_Unit 및 Project 열은 업무 엔티티를 만듭니다.

모든 값은 비워 둘 수 있습니다. 응용 프로그램이 이미 입력 값과 다른 업무 엔티티와 연결되어 있는 경우 응용 프로그램은 새 업무 엔티티에 할당됩니다.

가져오기 유틸리티에서 지원되는 개체 유형 및 키는 다음과 같습니다.

유형	키
호스트	id-><id> 또는 <Name> 또는 <IP>
VM	id-><id> 또는 <Name>
스토리지 풀	id-><id> 또는 `<Storage_name>`를 클릭합니다<Storage_Pool_name>
내부 볼륨	id-><id> 또는 `<Storage_name>`를 클릭합니다<Internal_volume_name>
볼륨	id-><id> 또는 `<Storage_name>`를 클릭합니다<Volume_name>
스토리지	id-><id> 또는 <Name> 또는 <IP>
스위치	id-><id> 또는 <Name> 또는 <IP>
포트	id-><id> 또는 <WWN>
공유	id-><id> 또는 <Storage Name>-><Internal Volume Name>-><Share Name>-><Protocol> <Qtree> 기본 qtree가 있는 경우 선택 사항입니다.

qtree입니다	id-><id> 또는 <Storage Name>-><Internal Volume Name>-><Qtree Name>
----------	--

CSV 파일은 다음 형식을 사용해야 합니다.

```
, , <Annotation Type> [, <Annotation Type> ...]
[, Application] [, Tenant] [, Line_Of_Business] [,
Business_Unit] [, Project]

<Object Type Value 1>, <Object Key 1>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]

...

<Object Type Value N>, <Object Key N>, <Annotation Value> [,
<Annotation Value> ...] [, <Application>] [, <Tenant>] [,
<Line_Of_Business>] [, <Business_Unit>] [, <Project>]
```

단계

1. Insight 웹 UI에 로그인합니다.
2. Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
문제 해결 페이지가 표시됩니다.
3. 페이지의 * 기타 작업 섹션 * 에서 * OnCommand Insight 포털 * 링크를 클릭합니다.
4. Insight Connect API * 를 클릭합니다.
5. 포털에 로그인합니다.
6. 주석 가져오기 유틸리티 * 를 클릭합니다.
7. 를 저장합니다 .zip 파일을 압축 해제하고 를 읽습니다 readme.txt 추가 정보 및 샘플을 위한 파일.
8. CSV 파일을 와 동일한 폴더에 저장합니다 .zip 파일.
9. 명령줄 창에서 다음을 입력합니다.

```
java -jar rest-import-utility.jar [-username] [-password]
[-aserver name or IP address] [-batch size] [-ccase
sensitive:true/false]
[-lextra logging:true/false] csv filename
```

추가 로깅을 사용하는 -l 옵션과 대/소문자 구분을 사용하는 -c 옵션은 기본적으로 false로 설정됩니다. 따라서 피처를 사용하려는 경우에만 지정해야 합니다.



옵션과 해당 값 사이에는 공백이 없습니다.



다음 키워드는 예약되며 사용자가 주석 이름으로 지정할 수 없습니다. - Application - Application_Priority - Tenant - Line_of_Business - Business_Unit - 예약된 키워드 중 하나를 사용하여 주석 유형을 가져오려고 하면 프로젝트 오류가 생성됩니다. 이러한 키워드를 사용하여 주석 이름을 만든 경우, 불러오기 유틸리티 도구가 올바르게 작동할 수 있도록 주석을 수정해야 합니다.



주석 가져오기 유틸리티를 사용하려면 Java 8 또는 Java 11이 필요합니다. 가져오기 유틸리티를 실행하기 전에 이 중 하나가 설치되어 있는지 확인하십시오. 최신 OpenJDK 11을 사용하는 것이 좋습니다.

쿼리를 사용하여 여러 자산에 주석 할당

자산 그룹에 주석을 할당하면 쿼리 또는 대시보드에서 관련 자산을 보다 쉽게 식별하거나 사용할 수 있습니다.

시작하기 전에

자산에 지정하려는 주석이 이미 생성되어 있어야 합니다.

이 작업에 대해

쿼리를 사용하여 여러 자산에 주석을 할당하는 작업을 단순화할 수 있습니다. 예를 들어 특정 데이터 센터 위치의 모든 어레이에 사용자 지정 주소 주석을 할당하려는 경우

단계

1. 새 쿼리를 만들어 주석을 할당할 자산을 식별합니다. 쿼리 * > * + 새 쿼리 * 를 클릭합니다.
2. Search for... * 드롭다운에서 * Storage * 를 선택합니다. 표시된 저장소 목록을 더 좁히도록 필터를 설정할 수 있습니다.
3. 표시된 저장소 목록에서 저장소 이름 옆의 확인란을 클릭하여 하나 이상의 저장소 를 선택합니다. 목록 상단의 기본 확인란을 클릭하여 표시된 모든 저장소를 선택할 수도 있습니다.
4. 원하는 저장소를 모두 선택한 경우 * Actions * > * Edit Annotation * 을 클릭합니다.

주석 추가 대화 상자가 표시됩니다.

5. 저장소에 할당할 * 주석 * 및 * 값 * 을 선택하고 * 저장 * 을 클릭합니다.

해당 주석의 열을 표시하는 경우 선택한 모든 저장소에 표시됩니다.

6. 이제 주석을 사용하여 위젯 또는 쿼리의 저장소를 필터링할 수 있습니다. 위젯에서 다음을 수행할 수 있습니다.
 - a. 대시보드를 만들거나 기존 대시보드를 엽니다. 변수 * 를 추가하고 위의 저장소에 설정한 주석을 선택합니다. 변수가 대시보드에 추가됩니다.
 - b. 방금 추가한 변수 필드에서 * any * 를 클릭하고 필터링할 적절한 값을 입력합니다. 체크 표시를 클릭하여 변수 값을 저장합니다.

- c. 위젯을 추가합니다. 위젯의 쿼리에서 필터 기준 + 단추를 클릭하고 목록에서 적절한 주석을 선택합니다.
 - d. 아무 * 나 * 를 클릭하고 위에서 추가한 주석 변수를 선택합니다. 작성한 변수는 ""\$로 시작하고 드롭다운에 표시됩니다.
 - e. 원하는 다른 필터 또는 필드를 설정한 다음 위젯이 원하는 대로 사용자 지정되면 * 저장 * 을 클릭합니다.
- 대시보드의 위젯에는 주석을 할당한 저장소에 대한 데이터만 표시됩니다.

자산 쿼리 중

쿼리를 사용하면 사용자 선택 기준(주석 및 성능 메트릭)에 따라 사용자 환경의 자산을 세분화된 수준으로 검색하여 네트워크를 모니터링하고 문제를 해결할 수 있습니다. 또한 자산에 주석을 자동으로 할당하는 주석 규칙에는 쿼리가 필요합니다.

쿼리 및 대시보드에 사용되는 자산

Insight 쿼리 및 대시보드 위젯은 다양한 자산 유형과 함께 사용할 수 있습니다

쿼리, 대시보드 위젯 및 사용자 지정 자산 페이지에서 다음 자산 유형을 사용할 수 있습니다. 필터, 식 및 표시에 사용할 수 있는 필드와 카운터는 자산 유형에 따라 달라집니다. 일부 자산은 일부 위젯 유형에 사용할 수 없습니다.

- 응용 프로그램
- 데이터 저장소
- 디스크
- 패브릭
- 일반 장치
- 호스트
- 내부 볼륨
- iSCSI 세션
- iSCSI 네트워크 포털
- 경로
- 포트
- qtree입니다
- 할당량
- 공유
- 스토리지
- 스토리지 노드
- 스토리지 풀
- 스위치
- 테이프

- VMDK입니다
- 가상 머신
- 볼륨
- Zone(영역)
- 존 구성원

쿼리 만들기

환경 내의 자산을 세분화된 수준으로 검색할 수 있도록 쿼리를 만들 수 있습니다. 쿼리를 사용하면 필터를 추가한 다음 결과를 정렬하여 하나의 뷰에서 인벤토리 및 성능 데이터를 볼 수 있으므로 데이터를 분류할 수 있습니다.

이 작업에 대해

예를 들어, 볼륨에 대한 쿼리를 생성하고, 선택한 볼륨과 연결된 특정 저장소를 찾기 위한 필터를 추가하고, 필터를 추가하여 선택한 저장소의 계층 1과 같은 특정 주석을 찾을 수 있습니다. 마지막으로 IOPS-Read(IO/s)가 25보다 큰 모든 스토리지를 찾기 위해 다른 필터를 추가합니다. 결과가 표시되면 쿼리와 관련된 정보 열을 오름차순 또는 내림차순으로 정렬할 수 있습니다.

자산을 취득하거나 주석 또는 응용 프로그램 할당을 만드는 새 데이터 원본이 추가되면 쿼리를 인덱싱한 후 정기적으로 예약된 간격으로 이러한 자산, 주석 또는 응용 프로그램을 쿼리할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * + 새 쿼리 * 를 선택합니다.
3. 자원 유형 선택 * 을 클릭하고 자산 유형을 선택합니다.

쿼리에 대해 자원을 선택하면 여러 기본 열이 자동으로 표시됩니다. 이러한 열을 제거하거나 언제든지 새 열을 추가할 수 있습니다.


4. 이름 * 텍스트 상자에 자산 이름을 입력하거나 자산 이름을 기준으로 필터링할 텍스트 부분을 입력합니다.

다음 중 하나만 사용하거나 조합하여 새 쿼리 페이지의 텍스트 상자에서 검색을 구체화할 수 있습니다.

- 별표를 사용하면 모든 항목을 검색할 수 있습니다. 예를 들면, 다음과 같습니다. vol*rhel ""vol""로 시작하고 ""rhel""으로 끝나는 모든 리소스를 표시합니다.
- 물음표를 사용하면 특정 수의 문자를 검색할 수 있습니다. 예를 들면, 다음과 같습니다. BOS-PRD??-S12 BOS-PRD12-S12, BOS-PRD13-S12 등을 표시합니다.
- 또는 연산자를 사용하여 여러 요소를 지정할 수 있습니다. 예를 들면, 다음과 같습니다. FAS2240 OR CX600 OR FAS3270 여러 스토리지 모델을 찾습니다.
- NOT 연산자를 사용하면 검색 결과에서 텍스트를 제외할 수 있습니다. 예를 들면, 다음과 같습니다. NOT EMC* "EMC"로 시작하지 않는 모든 항목을 찾습니다. 을 사용할 수 있습니다 NOT * 값이 없는 필드를 표시합니다.

5. 을 클릭합니다  를 눌러 자산을 표시합니다.
- 6.

조건을 추가하려면  을 클릭합니다 다음 중 하나를 수행합니다.

- 특정 기준을 검색하여 입력한 다음 선택합니다.
- 목록을 아래로 스크롤하여 기준을 선택합니다.
- IOPS-읽기(IO/s)와 같은 성능 메트릭을 선택한 경우 값 범위를 입력합니다. Insight에서 제공하는 기본 주석은  로 표시됩니다 즉, 이름이 중복된 주석이 있을 수 있습니다.

조건 및 목록의 쿼리 결과에 대한 열이 쿼리 결과 목록에 추가됩니다.

7. 필요에 따라  를 클릭할 수도 있습니다 쿼리 결과에서 주석 또는 성능 메트릭을 제거합니다.

예를 들어 쿼리에 데이터 저장소의 최대 지연 시간 및 최대 처리량이 표시되고 쿼리 결과 목록에 최대 지연 시간만을 표시하려면 이 단추를 클릭하고 * Throughput - Max * 확인란의 선택을 취소합니다. Throughput-Max(MB/s) 열이 쿼리 결과 목록에서 제거됩니다.



쿼리 결과 테이블에 표시되는 열 수에 따라 추가된 열을 추가로 볼 수 없을 수도 있습니다. 원하는 열이 표시될 때까지 하나 이상의 열을 제거할 수 있습니다.

8. 저장 * 을 클릭하고 쿼리 이름을 입력한 다음 * 저장 * 을 다시 클릭합니다.

관리자 역할이 있는 계정이 있는 경우 사용자 지정 대시보드를 만들 수 있습니다. 사용자 지정 대시보드는 위젯 라이브러리의 모든 위젯으로 구성될 수 있으며, 이 중 일부는 사용자 지정 대시보드에서 쿼리 결과를 나타낼 수 있습니다. 사용자 지정 대시보드에 대한 자세한 내용은 [_OnCommand Insight 시작 가이드_](#)를 참조하십시오.

- 관련 정보 *

"사용자 데이터 가져오기 및 내보내기"

쿼리 보기

쿼리를 보고 자산을 모니터링하고 쿼리에 자산과 관련된 데이터가 표시되는 방식을 변경할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.
3. 다음 중 하나를 실행하여 쿼리가 표시되는 방식을 변경할 수 있습니다.
 - 필터 * 상자에 텍스트를 입력하여 특정 쿼리를 표시할 수 있습니다.
 - 열 머리글의 화살표를 클릭하여 쿼리 테이블의 열 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다.
 - 열 크기를 조정하려면 파란색 막대가 나타날 때까지 열 머리글 위로 마우스를 가져갑니다. 마우스를 막대 위에 놓고 오른쪽이나 왼쪽으로 끕니다.
 - 열을 이동하려면 열 머리글을 클릭하고 오른쪽 또는 왼쪽으로 끕니다.
 - 쿼리 결과를 스크롤할 때 Insight에서 자동으로 데이터 원본을 폴링하므로 결과가 변경될 수 있습니다. 이로 인해 일부 항목이 누락되거나 정렬 방식에 따라 일부 항목이 순서대로 표시되지 않을 수 있습니다.


쿼리 결과를 **.csv** 파일로 내보내는 중입니다

쿼리 결과를 .csv 파일로 내보내 데이터를 다른 응용 프로그램으로 가져올 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

3. 쿼리를 클릭합니다.
4. 을 클릭합니다  쿼리 결과를 로 내보냅니다 .CSV 파일.
5. 다음 중 하나를 수행합니다.

- Open with * 를 클릭한 다음 * OK * 를 클릭하여 Microsoft Excel로 파일을 열고 파일을 특정 위치에 저장합니다.
- 파일 저장 * 을 클릭한 다음 * 확인 * 을 클릭하여 파일을 다운로드 폴더에 저장합니다. 표시된 열의 속성만 내보내집니다. 표시되는 일부 열, 특히 복잡한 중첩 관계의 일부인 열은 내보내지지 않습니다.



자산 이름에 쉼표가 나타나면 자산 이름과 올바른 .csv 형식을 유지하면서 내보내기가 따옴표로 이름을 묶습니다.

+ 쿼리 결과를 내보낼 때 결과 테이블의 * 모든 * 행이 화면에서 선택 또는 표시된 행이 아닌 최대 10,000개 행까지 내보내진다는 점에 유의하십시오.

를 누릅니다

Excel에서 내보낸 .csv 파일을 열 때 NN:NN(두 자리 뒤에 콜론이 두 자리 더 오는 경우) 형식의 개체 이름이나 기타 필드가 있으면 Excel에서 해당 이름을 텍스트 형식 대신 시간 형식으로 해석하는 경우가 있습니다. 이로 인해 Excel에서 해당 열에 잘못된 값이 표시될 수 있습니다. 예를 들어 "81:45"라는 이름의 개체는 Excel에서 "81:45:00"으로 표시됩니다. 이 문제를 해결하려면 다음 단계를 사용하여 .csv를 Excel로 가져옵니다.

를 누릅니다



- Open a new sheet in Excel.
 - On the "Data" tab, choose "From Text".
 - Locate the desired .CSV file and click "Import".
 - In the Import wizard, choose "Delimited" and click Next.
 - Choose "Comma" for the delimiter and click Next.
 - Select the desired columns and choose "Text" for the column data format.
 - Click Finish.
- Your objects should show in Excel in the proper format.

를 누릅니다



쿼리 수정

쿼리 중인 자산에 대한 검색 기준을 변경하려는 경우 쿼리와 연결된 조건을 변경할 수 있습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

3. 쿼리 이름을 클릭합니다.
4. 쿼리에서 조건을 제거하려면 을 클릭합니다 .
5. 쿼리에 조건을 추가하려면 을 클릭합니다  을 클릭하고 목록에서 조건을 선택합니다.
6. 다음 중 하나를 수행합니다.
 - 저장 * 을 클릭하여 처음에 사용된 이름으로 쿼리를 저장합니다.
 - 다른 이름으로 저장을 클릭하여 쿼리를 다른 이름으로 저장합니다.
 - 처음에 사용한 쿼리 이름을 변경하려면 * 이름 바꾸기 * 를 클릭합니다.
 - 쿼리 이름을 처음 사용한 이름으로 다시 변경하려면 * 되돌리기 * 를 클릭합니다.


쿼리를 삭제하는 중입니다

더 이상 자산에 대한 유용한 정보를 수집하지 않을 경우 쿼리를 삭제할 수 있습니다. 쿼리가 주식 규칙에 사용되는 경우 삭제할 수 없습니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

3. 삭제할 쿼리 위에 커서를 놓고 클릭합니다 .

쿼리를 삭제할 것인지 묻는 확인 메시지가 표시됩니다.

4. 확인 * 을 클릭합니다.

자산에 여러 애플리케이션을 할당하거나 자산에서 여러 애플리케이션을 제거합니다

수동으로 할당하거나 제거할 필요 없이 쿼리를 사용하여 여러 응용 프로그램을 자산에 할당하거나 자산에서 제거할 수 있습니다.

시작하기 전에

편집할 모든 자산을 찾는 쿼리를 이미 만들어야 합니다.

단계

1. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.


쿼리 페이지가 표시됩니다.

2. 자산을 찾는 쿼리의 이름을 클릭합니다.

쿼리와 연결된 자산 목록이 표시됩니다.

3. 목록에서 원하는 자산을 선택하거나 를 클릭합니다  ▼ 모두 * 를 선택합니다.

작업 * 버튼이 표시됩니다.

4. 선택한 자산에 애플리케이션을 추가하려면 을 클릭합니다  을 클릭하고 * 응용 프로그램 편집 * 을 선택합니다.

- a. 응용 프로그램 * 을 클릭하고 하나 이상의 응용 프로그램을 선택합니다.

호스트, 내부 볼륨 및 가상 머신에 대해 여러 애플리케이션을 선택할 수 있지만, 볼륨에 대해 하나의 애플리케이션만 선택할 수 있습니다.

- b. 저장 * 을 클릭합니다.

5. 자산에 할당된 애플리케이션을 제거하려면 **를** 클릭합니다 **Actions ▼** 을 클릭하고 * 응용 프로그램 제거 * 를 선택합니다.

- a. 제거할 응용 프로그램을 선택합니다.
- b. 삭제 * 를 클릭합니다.

할당한 모든 새 응용 프로그램은 다른 자산에서 파생된 자산의 모든 응용 프로그램을 재정의합니다. 예를 들어, 볼륨은 호스트에서 애플리케이션을 상속하고 새 애플리케이션이 볼륨에 할당되면 새 애플리케이션이 파생된 애플리케이션보다 우선합니다.

자산에서 여러 주식 편집 또는 제거

수동으로 편집하거나 제거할 필요 없이 쿼리를 사용하여 자산에 대한 여러 주식을 편집하거나 자산에서 여러 주식을 제거할 수 있습니다.

시작하기 전에

편집하려는 모든 자산을 찾는 쿼리를 이미 만들어야 합니다.

단계

1. 쿼리 * 를 클릭하고 * 모든 쿼리 표시 * 를 선택합니다.

쿼리 페이지가 표시됩니다.

2. 자산을 찾는 쿼리의 이름을 클릭합니다.

쿼리와 연결된 자산 목록이 표시됩니다.

3. 목록에서 원하는 자산을 선택하거나 **를** 클릭합니다 **□ ▼** | 모두 * 를 선택합니다.

작업 * 버튼이 표시됩니다.

4. 자산에 주식을 추가하거나 자산에 할당된 주식 값을 편집하려면 **을** 클릭합니다 **Actions ▼** 을 클릭하고 * 주식 편집 * 을 선택합니다.

- a. Annotation(주식) * 을 클릭하고 값을 변경할 주식을 선택하거나 새 주식을 선택하여 모든 자산에 할당합니다.
- b. 값 * 을 클릭하고 주식 값을 선택합니다.
- c. 저장 * 을 클릭합니다.

5. 자산에 할당된 주식을 제거하려면 **를** 클릭합니다 **Actions ▼** 을 클릭하고 * 주식 제거 * 를 선택합니다.

- a. Annotation(주식) * 을 클릭하고 자산에서 제거할 주식을 선택합니다.
- b. 삭제 * 를 클릭합니다.

테이블 값 복사 중

테이블의 값을 복사하여 검색 상자 또는 다른 응용 프로그램에서 사용할 수 있습니다.

이 작업에 대해

테이블 또는 쿼리 결과에서 값을 복사하는 데 사용할 수 있는 두 가지 방법이 있습니다.

단계

1. 방법 1: 마우스로 원하는 텍스트를 강조 표시하고 복사한 다음 검색 필드 또는 다른 응용 프로그램에 붙여 넣습니다.
2. 방법 2: 길이가 테이블 열 너비를 초과하는 단일 값 필드의 경우 줄임표(...)로 표시되며 필드 위로 마우스를 가져가서 클립보드 아이콘을 클릭합니다. 검색 필드 또는 기타 응용 프로그램에서 사용할 수 있도록 값이 클립보드에 복사됩니다.

자산에 대한 링크인 값만 복사할 수 있습니다. 단일 값(예: 비목록)이 포함된 필드에만 복사 아이콘이 있습니다.

Insight 데이터 소스 관리

데이터 소스는 OnCommand Insight 환경을 유지 관리하는 데 사용되는 가장 중요한 구성 요소입니다. 이러한 정보가 Insight의 주요 정보원이므로 실행 중인 상태에서 데이터 소스를 유지하는 것이 중요합니다.

데이터 소스를 선택하여 상태와 관련된 이벤트를 확인하고 문제가 발생했을 수 있는 변경 사항을 확인하여 네트워크의 데이터 소스를 모니터링할 수 있습니다.

개별 데이터 소스를 검사하는 것 외에도 다음과 같은 작업을 수행할 수 있습니다.

- 데이터 소스를 복제하여 Insight에서 유사한 여러 데이터 소스를 생성합니다
- 데이터 원본 정보를 편집합니다
- 자격 증명을 변경합니다
- 폴링 제어
- 데이터 원본을 삭제합니다
- 데이터 소스 패치를 설치합니다
- 패치에서 새 데이터 원본을 설치합니다
- NetApp 고객 지원을 위한 오류 보고서 준비

Insight에서 데이터 소스 설정

데이터 소스는 Insight 환경을 유지하려고 할 때 가장 중요한 구성 요소입니다. 데이터 소스는 분석 및 검증에 사용되는 네트워크 정보를 검색합니다. Insight 내에서 데이터 소스를 구성하여 네트워크 내에서 모니터링할 수 있어야 합니다.

각 데이터 소스에 대해 데이터 소스를 정의하는 특정 요구 사항은 해당 디바이스의 공급업체 및 모델에 따라 다릅니다. 데이터 소스를 추가하기 전에 모든 장치에 대한 네트워크 주소, 계정 정보 및 암호가 필요하며, 이러한 추가 세부 정보는 다음과 같습니다.

- 스위치
- 장치 관리 스테이션

- IP 접속이 가능한 스토리지 시스템
- 스토리지 관리 스테이션
- IP 연결이 없는 스토리지 디바이스에 대해 관리 소프트웨어를 실행하는 호스트 서버입니다

데이터 소스 정의에 대한 자세한 내용은 이 섹션의 "공급업체별 데이터 소스 참조" 정보를 참조하십시오.

데이터 소스 지원 정보

구성 계획의 일환으로 Insight에서 사용자 환경의 장치를 모니터링할 수 있는지 확인해야 합니다. 이렇게 하려면 데이터 소스 지원 매트릭스에서 운영 체제, 특정 장치 및 프로토콜에 대한 자세한 내용을 확인할 수 있습니다. 일부 데이터 소스는 일부 운영 체제에서 사용하지 못할 수 있습니다.

데이터 소스 지원 매트릭스의 최신 버전 위치

OnCommand Insight 데이터 소스 지원 매트릭스는 각 서비스 팩 릴리스에 따라 업데이트됩니다. 문서의 최신 버전은 에서 찾을 수 있습니다 ["NetApp Support 사이트"](#). .

데이터 소스 추가

데이터 원본 추가 대화 상자를 사용하여 데이터 원본을 빠르게 추가할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 열고 관리자 권한이 있는 사용자로 로그인합니다.
2. Admin * 을 선택하고 * Data Sources * 를 선택합니다.
3. 추가 * 버튼을 클릭합니다.

데이터 소스 추가 마법사가 열립니다.

4. 설정 * 섹션에서 다음 정보를 입력합니다.

필드에 입력합니다	설명
이름	이 데이터 원본의 고유한 네트워크 이름을 입력합니다. 참고: 데이터 소스 이름에는 문자, 숫자 및 밑줄(_) 문자만 사용할 수 있습니다.
공급업체	드롭다운에서 데이터 소스의 공급업체를 선택합니다.
모델	드롭다운에서 데이터 원본의 모델을 선택합니다.
실행 위치	로컬 을 선택하거나 환경에 RAU가 구성되어 있는 경우 원격 획득 장치를 선택할 수 있습니다.

수집 대상	대부분의 데이터 원본의 경우 이러한 옵션은 인벤토리 및 성능입니다. 재고는 항상 기본적으로 선택되며 선택 취소할 수 없습니다. 일부 데이터 원본의 경우 옵션이 다를 수 있습니다. 선택한 컬렉션 옵션은 구성 및 고급 구성 섹션에서 사용 가능한 필드를 변경합니다.
-------	---

5. Configuration* 링크를 클릭하고 선택한 데이터 수집 유형을 사용하여 데이터 원본에 필요한 기본 설정 정보를 입력합니다.
6. 이러한 유형의 데이터 소스를 네트워크에 설정하기 위해 일반적으로 더 자세한 정보가 필요한 경우 * 고급 구성 * 링크를 클릭하여 추가 정보를 입력합니다.
7. 특정 데이터 소스에 필요하거나 사용할 수 있는 구성 또는 고급 구성 정보에 대한 자세한 내용은 를 참조하십시오 ["공급업체별 데이터 소스 참조"](#).
8. 데이터 소스가 올바르게 구성되었는지 확인하려면 * Test *(테스트 *) 링크를 클릭합니다.
9. 저장 * 을 클릭합니다.

스프레드시트에서 데이터 원본을 가져옵니다

스프레드시트에서 여러 데이터 원본을 OnCommand Insight로 가져올 수 있습니다. 이 기능은 검색 장치를 스프레드시트에 이미 유지 관리하는 경우에 유용할 수 있습니다. 이 프로세스는 새 데이터 원본을 추가하지만 기존 데이터 원본을 업데이트하는 데 사용할 수는 없습니다.

이 작업에 대해

OnCommand Insight에는 데이터 원본을 만드는 데 도움이 되는 스프레드시트가 포함되어 있습니다. 이 스프레드시트에는 다음과 같은 속성이 있습니다.

- 스프레드시트는 Microsoft Excel 2003 이상에서 사용할 수 있습니다.
- 각 탭에는 데이터 소스 유형(예: Brocade SSH/CLI)이 하나씩 있습니다.
- 각 행은 만들 새 데이터 소스의 인스턴스를 나타냅니다.

스프레드시트에는 OnCommand Insight에서 새 데이터 원본을 만드는 매크로가 포함되어 있습니다.

단계

1. 에서 스프레드시트를 찾습니다
`<install_directory>/SANscreen/acq/bin/acqcli/SiteSurvey_DataSourceImporter_w_Macro.zip.`
2. 스프레드시트에서 색이 있는 셀에 데이터 원본 정보를 입력합니다.
3. 빈 행을 삭제합니다.
4. 스프레드시트에서 을 실행합니다 CreateDataSources 데이터 원본을 만드는 매크로
5. 자격 증명을 묻는 메시지가 나타나면 OnCommand Insight 서버 관리 사용자 이름과 암호를 입력합니다.

 결과는 획득 로그에 기록됩니다.
6. 현재 매크로를 실행 중인 컴퓨터에 OnCommand Insight가 설치되어 있는지 묻는 메시지가 나타납니다.

다음 중 하나를 선택합니다.

- 아니요: OnCommand Insight 시스템에서 실행해야 하는 배치 파일을 만들 경우 "아니요"를 선택합니다. 설치 디렉토리에서 이 배치 파일을 실행합니다.
- 예: OnCommand Insight가 이미 설치되어 있고 데이터 소스 정보를 생성하는 데 추가 단계가 필요하지 않은 경우 "예"를 선택합니다.

7. 데이터 소스가 추가되었는지 확인하려면 브라우저에서 Insight를 엽니다.
8. Insight 도구 모음에서 * Admin * 을 클릭합니다.
9. 가져온 데이터 원본에 대한 데이터 원본 목록을 확인합니다.

패치를 사용하여 새 데이터 원본을 추가합니다

새 데이터 소스는 패치 프로세스를 사용하여 시스템에 로드할 수 있는 패치 파일로 릴리스됩니다. 이 프로세스를 통해 예약된 OnCommand Insight 릴리스 간에 새 데이터 소스를 사용할 수 있습니다.

시작하기 전에

설치할 패치 파일을 업로드해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 선택합니다.
3. Actions * > * Install service pack or patch * 를 선택합니다.
4. 서비스 팩 또는 패치* 설치 대화 상자에서 * 찾아보기 * 를 클릭하여 업로드한 패치 파일을 찾아 선택합니다.
5. 패치 요약 * 대화 상자에서 * 다음 * 을 클릭합니다.
6. 추가 정보 * 를 검토하고 계속하려면 * 다음 * 을 클릭합니다.
7. 설치 * 대화 상자에서 * 마침 * 을 클릭합니다.

데이터 소스 클론 생성

클론 기능을 사용하면 다른 데이터 소스와 동일한 자격 증명 및 속성을 가진 데이터 소스를 빠르게 추가할 수 있습니다. 클론 생성 기능을 사용하면 동일한 디바이스 유형의 여러 인스턴스를 쉽게 구성할 수 있습니다.

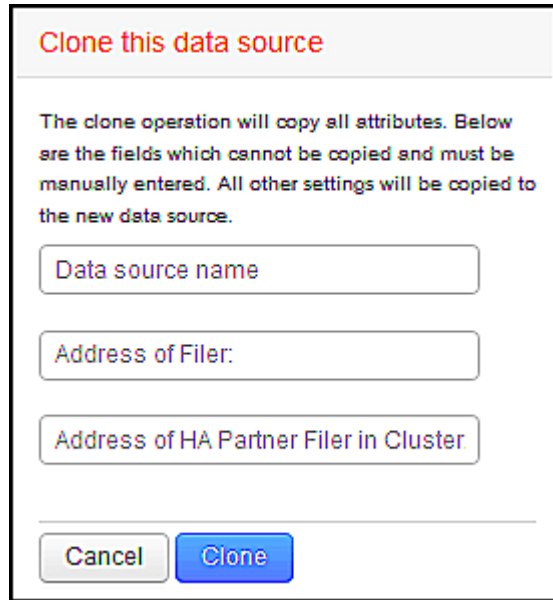
단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

데이터 소스 목록이 열립니다.

2. 새 데이터 원본에 사용할 설정 정보가 있는 데이터 원본을 강조 표시합니다.
3. 강조 표시된 데이터 소스의 오른쪽에 있는 * Clone * 아이콘을 클릭합니다.

이 데이터 소스 클론 복제 대화 상자에는 NetApp 데이터 소스에 대해 다음 예와 같이 선택한 데이터 소스에 대해 제공해야 하는 정보가 표시됩니다.

A screenshot of a 'Clone this data source' dialog box. The title bar is red with the text 'Clone this data source' in white. Below the title bar, there is a paragraph of text: 'The clone operation will copy all attributes. Below are the fields which cannot be copied and must be manually entered. All other settings will be copied to the new data source.' Below this text are three input fields: 'Data source name', 'Address of Filer:', and 'Address of HA Partner Filer in Cluster'. At the bottom of the dialog box are two buttons: 'Cancel' and 'Clone'.

4. 필드에 필수 정보를 입력합니다. 이러한 세부 정보는 기존 데이터 원본에서 복사할 수 없습니다.
5. 클론 * 을 클릭합니다.

결과

클론 작업은 다른 모든 속성 및 설정을 복제하여 새 데이터 소스를 생성합니다.

데이터 소스 구성을 테스트하는 중입니다

데이터 소스를 추가할 때 해당 데이터 소스를 저장하거나 업데이트하기 전에 장치와 통신하도록 구성이 올바른지 확인할 수 있습니다.

데이터 소스 마법사에서 * Test * 버튼을 클릭하면 지정된 장치와의 통신이 선택됩니다. 테스트에서 다음 결과 중 하나가 생성됩니다.

- Passed(통과): 데이터 소스가 올바르게 구성되었습니다.
- 경고: 처리 중 시간 초과나 획득 실행 중이 아닌 경우 테스트가 완료되지 않았습니다.
- 실패: 구성된 데이터 소스가 지정된 장치와 통신할 수 없습니다. 구성 설정을 확인하고 다시 테스트하십시오.

공급업체별 데이터 소스 참조

구성 세부 정보는 추가되는 데이터 소스의 공급업체 및 모델에 따라 달라집니다.

공급업체의 데이터 원본에 특별한 요구 사항 및 특정 명령과 같은 고급 Insight 구성 지침이 필요한 경우 이 정보가 이 섹션에 포함됩니다.

3PAR InServ 데이터 소스

OnCommand Insight는 3PAR InServ(펌웨어 2.2.2+, SSH) 데이터 소스를 사용하여 HP

3PAR StoreServ 스토리지 어레이의 인벤토리를 검색합니다.

용어

OnCommand Insight는 3PAR InServ 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
물리 디스크	디스크
스토리지 시스템	스토리지
컨트롤러 노드	스토리지 노드
공동 프로비저닝 그룹	스토리지 풀
가상 볼륨	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- InServ 클러스터의 IP 주소 또는 FQDN입니다
- 인벤토리의 경우 InServ 서버에 대한 읽기 전용 사용자 이름 및 암호입니다.
- 성능을 위해 InServ 서버에 대한 읽기-쓰기 사용자 이름 및 암호.
- 포트 요구 사항: 22(인벤토리 수집), 5988 또는 5989(성능 수집) [참고: 3PAR 성능은 InServ OS 3.x+에서 지원됩니다.]
- 성능 수집을 위해 SSH를 통해 3PAR 스토리지에 로그인하여 SMI-S가 활성화되었는지 확인합니다.

구성

필드에 입력합니다	설명
클러스터 IP	InServ 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	InServ 서버의 사용자 이름입니다
암호	InServ 서버에 사용되는 암호입니다
SMI-S 호스트 IP입니다	SMI-S Provider 호스트의 IP 주소입니다

SMI-S 사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
SMI-S 암호	SMI-S Provider 호스트에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
장치 제외	제외할 장치 IP의 심표로 구분된 목록입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 60초)
SSH 재시도 횟수	SSH 재시도 횟수입니다
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 20초)
SMI-S 포트	SMI-S Provider 호스트에서 사용하는 포트입니다
프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다
SMI-S 네임스페이스	SMI-S 네임스페이스
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SMI-S 연결 재시도 횟수	SMI-S 연결 재시도 횟수입니다

Amazon AWS EC2 데이터 소스

OnCommand Insight은 이 데이터 소스를 사용하여 Amazon AWS EC2의 인벤토리 및 성능을 검색합니다.

전제 조건:

Amazon EC2 장치에서 데이터를 수집하려면 다음 정보가 있어야 합니다.

- IAM 액세스 키 ID가 있어야 합니다
- Amazon EC2 클라우드 계정에 대한 비밀 액세스 키가 있어야 합니다
- "조직 목록" 권한이 있어야 합니다
- 포트 433 HTTPS
- EC2 인스턴스는 가상 머신 또는 (비교적 자연스럽게) 호스트로 보고할 수 있습니다. EBS 볼륨은 VM에서 사용하는 가상 디스크와 가상 디스크의 용량을 제공하는 데이터 저장소로 보고될 수 있습니다.

액세스 키는 액세스 키 ID(예: AKIAIOSFODN7EXAMPLE)와 비밀 액세스 키(예: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY)로 구성됩니다. 액세스 키를 사용하여 Amazon EC2 SDK, REST 또는 쿼리 API 작업을 사용하는 경우 EC@에 만드는 프로그래밍 방식 요청에 서명할 수 있습니다. 이러한 키는 아마존에서 귀하의 계약과 함께 제공됩니다.

이 데이터 소스를 구성하는 방법

Amazon AWS EC2 데이터 소스를 구성하려면 AWS 계정에 대한 AWS IAM 액세스 키 ID와 비밀 액세스 키가 필요합니다.

아래 표에 따라 데이터 원본 필드를 채웁니다.

구성:

필드에 입력합니다	설명
AWS 지역	AWS 지역을 선택하십시오
IAM 역할	AWS의 AU에서 획득한 경우에만 사용합니다. IAM 역할에 대한 자세한 내용은 아래를 참조하십시오.
AWS IAM 액세스 키 ID	AWS IAM 액세스 키 ID를 입력합니다. IAM Role을 사용하지 않는 경우 필수입니다.
AWS IAM 비밀 액세스 키	AWS IAM 비밀 액세스 키를 입력합니다. IAM Role을 사용하지 않는 경우 필수입니다.
저는 AWS가 API 요청에 대해 청구하는 것을 알고 있습니다	이 확인란을 선택하여 AWS에서 Insight 폴링으로 인한 API 요청 비용을 청구하는지 확인하십시오

고급 구성:

필드에 입력합니다	설명
추가 지역 포함	폴링에 포함할 추가 영역을 지정합니다.
교차 계정 역할	서로 다른 AWS 계정의 리소스에 액세스하는 역할입니다.
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
HTTP 연결 및 소켓 시간 제한(초)	HTTP 연결 시간 초과(기본값 300초)
AWS 태그 포함	Insight 주식에서 AWS 태그에 대한 지원을 활성화하려면 이 확인란을 선택합니다
성능 폴링 간격(초)	성능 폴링 간격(기본값: 1800초)

AWS 태그를 Insight 주석에 매핑

AWS EC2 데이터 원본에는 AWS에 구성된 태그로 Insight 주석을 채울 수 있는 옵션이 포함되어 있습니다. 주석 이름은 AWS 태그와 정확히 일치해야 합니다. Insight는 항상 같은 이름의 텍스트 유형 주석을 채우고 다른 유형의 주석(숫자, 부울 등)을 채우기 위한 "최선의 시도"를 만듭니다. 주석이 다른 유형이고 데이터 소스가 주석을 채우지 못할 경우 주석을 제거하고 텍스트 유형으로 다시 생성해야 할 수 있습니다.

AWS는 대/소문자를 구분하며 Insight는 대/소문자를 구분합니다. 따라서 Insight에서 "소유자"라는 주석을 만들고 AWS에서 "소유자", "소유자", "소유자", "소유자"라는 태그를 만들면 "소유자"의 모든 AWS 변형이 Insight의 "소유자" 주석에 매핑됩니다.

관련 정보:

"IAM 사용자를 위한 액세스 키 관리"

추가 지역 포함

AWS Data Collector * 고급 구성 * 섹션에서 추가 영역을 포함하도록 * 추가 영역 포함 * 필드를 쉼표 또는 세미콜론으로 구분하여 설정할 수 있습니다. 기본적으로 이 필드는 모든 미국 AWS 지역에서 수집하는 *_us-. * _* 로 설정됩니다. on_all_regions를 수집하려면 이 필드를 *_.*_* 로 설정합니다.

추가 영역 포함 * 필드가 비어 있으면 * 구성 * 섹션에 지정된 * AWS 지역 * 필드에 지정된 자산에 대한 데이터 수집기가 수집됩니다.

* AWS 하위 계정에서 수집 *

Insight는 단일 AWS 데이터 수집기 내에서 AWS의 하위 계정 수집을 지원합니다. 이 컬렉션에 대한 구성은 AWS 환경에서 수행됩니다.

- 운영 계정 ID가 하위 계정에서 EC2 세부 정보에 액세스할 수 있도록 각 하위 계정에 AWS 역할을 구성해야 합니다.
- 각 하위 계정에는 동일한 문자열로 구성된 역할 이름이 있어야 합니다
- 이 역할 이름 문자열을 * 교차 계정 역할 * 필드의 Insight AWS Data Collector * 고급 구성 * 섹션에 입력합니다.

모범 사례: AWS 사전 정의된 AmazonEC2ReadOnlyAccess 정책을 ECS 기본 계정에 할당하는 것이 좋습니다. 또한 데이터 소스에서 구성된 사용자는 AWS를 쿼리하기 위해 미리 정의된 *AWSOrganizationReadOnlyAccess* 정책이 할당되어 있어야 합니다.

Insight를 AWS 하위 계정에서 수집할 수 있도록 환경을 구성하는 방법은 다음을 참조하십시오.

"자습서: IAM 역할을 사용하여 AWS 계정 전체에서 대리인 액세스"

"AWS 설정: 사용자가 소유한 다른 AWS 계정에서 IAM 사용자에게 대한 액세스 제공"

"IAM 사용자에게 대한 권한을 위임하기 위한 역할 생성"

IAM 역할

IAM Role_security를 사용할 때는 생성하거나 지정하는 역할에 리소스에 액세스하는 데 필요한 적절한 권한이 있는지 확인해야 합니다.

예를 들어, 이름이 _InstanceE2ReadOnly_인 IAM 역할을 생성하는 경우 이 IAM 역할에 대한 모든 EC2 리소스에 EC2 읽기 전용 목록 액세스 권한을 부여하도록 정책을 설정해야 합니다. 또한 이 역할이 계정 간에 역할을 수행할 수

있도록 STS(보안 토큰 서비스) 액세스를 부여해야 합니다.

IAM 역할을 생성한 후 새 EC2 인스턴스 또는 기존 EC2 인스턴스를 생성할 때 연결할 수 있습니다.

IAM role_InstanceE2ReadOnly_를 EC2 인스턴스에 연결하면 IAM 역할 이름으로 인스턴스 메타데이터를 통해 임시 자격 증명을 검색하고 이 EC2 인스턴스에서 실행되는 모든 애플리케이션에서 이 자격 증명을 사용하여 AWS 리소스에 액세스할 수 있습니다.



IAM 역할은 획득 장치가 AWS 인스턴스에서 실행 중인 경우에만 사용할 수 있습니다.

Brocade Enterprise Fabric Connectivity Manager 데이터 소스

OnCommand Insight는 Brocade EFCM(Enterprise Fabric Connectivity Manager) 데이터 소스를 사용하여 Brocade EFCM 스위치의 인벤토리를 검색합니다. Insight는 EFCM 버전 9.5, 9.6 및 9.7을 지원합니다.

요구 사항



이 데이터 수집기는 OnCommand Insight 7.3.11부터 사용할 수 없습니다.

- EFCM 서버의 네트워크 주소 또는 정규화된 도메인 이름입니다
- EFCM 버전은 9.5, 9.6 또는 9.7이어야 합니다
- EFCM 서버의 IP 주소입니다
- EFCM 서버에 대한 읽기 전용 사용자 이름 및 암호입니다
- 포트 51512를 통해 읽기 전용 사용자 이름과 암호를 사용하여 Insight 서버에서 텔넷을 통해 Connectrix 스위치에 대한 액세스를 검증했습니다

구성

* 필드 *	* 설명 *
EFC 서버	EFC 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	스위치의 사용자 이름입니다
암호	스위치에 사용되는 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
패브릭 이름	EFCM 데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.

통신 포트	스위치와 통신하는 데 사용되는 포트입니다
트래핑을 활성화합니다	장치에서 SNMP 트랩을 수신할 때 획득을 활성화하려면 선택합니다. 트래핑 활성화를 선택한 경우 SNMP도 활성화해야 합니다.
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 15초)
비활성 Zoneset	활성 영역 세트에서 획득을 수행할 뿐만 아니라 획득을 수행할 비활성 Zoneset의 심표로 구분된 목록입니다
사용할 NIC입니다	SAN 디바이스에서 보고할 때 RAU에서 사용해야 하는 네트워크 인터페이스를 지정합니다
장치 제외	폴링에서 포함하거나 제외할 단위 이름의 심표로 구분된 목록입니다
EFCM 스위치 별칭을 Insight 스위치 이름으로 사용합니다	EFCM 스위치 별칭을 Insight 스위치 이름으로 사용하려면 선택합니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Brocade FC 스위치 데이터 소스

OnCommand Insight는 Brocade FC 스위치(SSH) 데이터 소스를 사용하여 계수 운영 체제(FOS) 펌웨어 4.2 이상을 실행하는 Brocade 또는 재브랜딩 스위치 디바이스의 인벤토리를 검색합니다. FC 스위치와 액세스 게이트웨이 모드의 디바이스가 모두 지원됩니다.

용어

OnCommand Insight는 Brocade FC 스위치 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
스위치	스위치
포트	포트
가상 패브릭, 물리적 패브릭	패브릭
Zone(영역)	Zone(영역)

논리 스위치	논리 스위치
LSAN 구역	IVR 영역



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 획득 장치(로컬 또는 원격)는 Brocade 스위치의 TCP 포트 22에 대한 연결을 시작하여 인벤토리 데이터를 수집합니다. 또한 AU는 성능 데이터 수집을 위해 UDP 포트 161에 대한 연결을 시작합니다.
- Fabric의 모든 스위치에 대한 IP 연결이 있어야 합니다. Fabric에서 모든 스위치 검색 확인란을 선택하면 OCI가 Fabric의 모든 스위치를 식별하지만, 추가 스위치를 검색하려면 해당 스위치에 대한 IP 연결이 필요합니다.
- Fabric의 모든 스위치에서 동일한 계정이 전 세계적으로 필요합니다. PuTTY(오픈 소스 터미널 에뮬레이터)를 사용하여 액세스를 확인할 수 있습니다.
- Perform 라이선스가 설치된 경우 SNMP 성능 폴링을 위해 Fabric의 모든 스위치에 대해 포트 161과 162가 열려 있어야 합니다.
- SNMP 읽기 전용 커뮤니티 문자열

구성

필드에 입력합니다	설명
스위치 IP	스위치의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	스위치의 사용자 이름입니다
암호	스위치에 사용되는 암호입니다
SNMP 버전	SNMP 버전입니다
SNMP 커뮤니티 문자열	스위치에 액세스하는 데 사용되는 SNMP 읽기 전용 커뮤니티 문자열입니다
SNMP 사용자 이름입니다	SNMP 버전 프로토콜 사용자 이름(SNMP v3에만 적용)
SNMP 암호	SNMP 버전 프로토콜 암호(SNMP v3에만 적용)

고급 구성

필드에 입력합니다	설명
패브릭 이름	데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.

장치 제외	폴링에서 제외할 장치 ID의 쉼표로 구분된 목록입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
시간 초과(초)	연결 시간 초과(기본값 30초)
배너 대기 제한 시간(초)	SSH 배너 대기 시간 초과(기본값 5초)
관리자 도메인이 활성화되었습니다	관리자 도메인을 사용하는 경우 선택합니다
MPR 데이터 검색	다중 프로토콜 라우터(MPR)에서 라우팅 데이터를 가져오려면 선택합니다.
트래핑을 활성화합니다	장치에서 SNMP 트랩을 수신할 때 획득을 활성화하려면 선택합니다. 트래핑 활성화를 선택한 경우 SNMP도 활성화해야 합니다.
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
패브릭의 모든 스위치를 살펴보십시오	Fabric의 모든 스위치를 검색하려면 선택합니다
HBA와 을 선택합니다 영역 별칭	HBA 또는 영역 별칭을 사용할지 여부를 선택합니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMP v3만 해당)
SNMP 개인 정보 보호 프로토콜	SNMP 개인 정보 보호 프로토콜(SNMP v3만 해당)
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호(SNMP v3만 해당)
SNMP 재시도	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)

Brocade Sphereon/Intrepid 스위치 데이터 소스

OnCommand Insight는 Brocade Sphereon/Intrepid 스위치(SNMP) 데이터 소스를 사용하여 Brocade Sphereon 또는 Intrepid 스위치의 인벤토리를 검색합니다.

요구 사항



이 데이터 수집기는 OnCommand Insight 7.3.11부터 사용할 수 없습니다.

- Fabric의 모든 스위치에 대한 IP 연결이 있어야 합니다. Fabric에서 모든 스위치 검색 확인란을 선택하면 OCI가 Fabric의 모든 스위치를 식별하지만, 추가 스위치를 검색하려면 해당 스위치에 대한 IP 연결이 필요합니다.
- SNMP V1 또는 SNMP V2를 사용하는 경우 읽기 전용 커뮤니티 문자열입니다.
- 조닝 정보를 얻기 위해 스위치에 대한 HTTP 액세스.
- 를 실행하여 액세스 검증을 수행합니다 `snmpwalk` 스위치에 대한 유틸리티(참조 `<install_path>\bin\`).

구성

* 필드 *	* 설명 *
Sphereon 스위치	스위치의 IP 주소 또는 정규화된 도메인 이름입니다
SNMP 버전	SNMP 버전입니다
SNMP 커뮤니티	스위치에 액세스하는 데 사용되는 SNMP 읽기 전용 커뮤니티 문자열입니다
사용자 이름	스위치에 대한 SMI-S 사용자 이름(SNMP v3만 해당)
암호	스위치에 대한 SMI-S 암호(SNMP v3만 해당)

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 프로토콜	SNMP 개인 정보 보호 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호입니다
SNMP 재시도 횟수	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)
패브릭 이름	데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.
트래핑을 활성화합니다	장치에서 SNMP 트랩을 수신할 때 획득을 활성화하려면 선택합니다. 트래핑 활성화를 선택한 경우 SNMP도 활성화해야 합니다.

Ttrap(Ttrap) 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Cisco FC 스위치 펌웨어(SNMP) 데이터 소스

OnCommand Insight는 Cisco FC 스위치 펌웨어 2.0+(SNMP) 데이터 소스를 사용하여 Cisco MDS 파이버 채널 스위치에 대한 인벤토리 및 FC 서비스가 사용되는 다양한 Cisco Nexus FCoE 스위치를 검색합니다. 또한 이 데이터 소스를 통해 NPV 모드에서 실행되는 여러 Cisco 장치 모델을 발견할 수 있습니다.

용어

OnCommand Insight는 Cisco FC 스위치 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
스위치	스위치
포트	포트
vSAN을 선택합니다	패브릭
Zone(영역)	Zone(영역)
논리 스위치	논리 스위치
이름 서버 항목	이름 서버 항목
IVR(Inter-VSAN Routing) 존	IVR 영역



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 패브릭 또는 개별 스위치에 있는 스위치 중 하나의 IP 주소입니다
- 새시 검색, 패브릭 검색 지원
- SNMP V2를 사용하는 경우 읽기 전용 커뮤니티 문자열입니다
- 포트 161은 장치에 액세스하는 데 사용됩니다
- 를 사용하여 유효성 검사에 액세스합니다 snmpwalk 스위치에 대한 유틸리티(참조 <install_path>\bin\)

구성

필드에 입력합니다	설명
Cisco 스위치 IP	스위치의 IP 주소 또는 정규화된 도메인 이름입니다
SNMP 버전	성능 획득을 위해서는 SNMP 버전 v2 이상이 필요합니다
SNMP 커뮤니티 문자열	스위치에 액세스하는 데 사용되는 SNMP 읽기 전용 커뮤니티 문자열(SNMP v3에는 적용되지 않음)
사용자 이름	스위치의 사용자 이름(SNMP v3만 해당)
암호	스위치에 사용된 암호(SNMPv3만 해당)

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 프로토콜	SNMP 개인 정보 보호 프로토콜(SNMPv3만 해당)
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호입니다
SNMP 재시도	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)
트래핑을 활성화합니다	트래핑을 활성화하려면 선택합니다. 트래핑을 사용하는 경우 SNMP 알림도 활성화해야 합니다.
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
모든 패브릭 스위치를 살펴보십시오	Fabric의 모든 스위치를 검색하려면 선택합니다
장치 제외	폴링에서 제외할 장치 IP의 심표로 구분된 목록입니다
장치 포함	폴링에 포함할 장치 IP의 심표로 구분된 목록입니다
장치 유형을 확인하십시오	자신을 Cisco 장치로 명시적으로 광고하는 장치만 수락하려면 선택합니다

기본 별칭 유형	<p>별칭 해상도에 대한 첫 번째 기본 설정을 제공합니다. 다음 중에서 선택합니다.</p> <ul style="list-style-type: none"> • * 장치 별칭 * <p>이 이름은 필요에 따라 모든 구성 명령에 사용할 수 있는 포트 WWN(pwwn)에 대한 사용자 친화적인 이름입니다. Cisco MDS 9000 제품군의 모든 스위치는 분산 장치 별칭(장치 별칭)을 지원합니다.</p> <ul style="list-style-type: none"> • * 없음 * <p>별칭을 보고하지 않습니다</p> <ul style="list-style-type: none"> • * 포트 설명 * <p>포트 목록에서 포트를 식별하는 데 도움이 되는 설명입니다</p> <ul style="list-style-type: none"> • * 영역 별칭(모두) * <p>조닝 구성에만 사용할 수 있는 포트에 대한 알기 쉬운 이름입니다</p> <ul style="list-style-type: none"> • * 영역 별칭(활성 전용) * <p>활성 구성에만 사용할 수 있는 포트에 대한 사용자 친화적인 이름입니다. 이것이 기본값입니다.</p>
보조 별칭 유형	별칭 해상도에 대한 두 번째 기본 설정을 제공합니다
제3 별칭 유형	별칭 해상도에 대한 세 번째 기본 설정을 제공합니다
SANTap 프록시 모드 지원을 설정합니다	Cisco 스위치가 프록시 모드에서 SANTap을 사용하고 있는지 여부를 선택합니다. EMC RecoverPoint를 사용하는 경우 SANTap을 사용할 수 있습니다.
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

EMC Celerra 데이터 소스

Celerra(SSH) 데이터 소스는 Celerra 스토리지에서 인벤토리 정보를 수집합니다. 구성의 경우 이 데이터 원본에는 스토리지 프로세서의 IP 주소와 _read-only_user 이름 및 암호가 필요합니다.

용어

OnCommand Insight는 EMC Celerra 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음

용어를 옆두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
Celerra Network Server입니다	스토리지
Celerra 메타 볼륨/Celerra 스토리지 풀	스토리지 풀
파일 시스템	내부 볼륨
Data Mover입니다	컨트롤러
Data Mover에 마운트된 파일 시스템입니다	파일 공유
CIFS 및 NFS 익스포트	공유
디스크 볼륨	백엔드 LUN



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지 프로세서의 IP 주소입니다
- 읽기 전용 사용자 이름 및 암호
- SSH 포트 22

구성

필드에 입력합니다	설명
Celerra의 주소입니다	Celerra 디바이스의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Celerra 디바이스에 로그인하는 데 사용되는 이름입니다
암호	Celerra 디바이스에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)

재시도 횟수	인벤토리 재시도 횟수입니다
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 20초)

EMC CLARiX(NaviCLI) 데이터 소스

이 데이터 소스를 구성하기 전에 EMC Navisphere CLI가 타겟 디바이스 및 Insight 서버에 설치되어 있는지 확인합니다. Navisphere CLI 버전은 컨트롤러의 펌웨어 버전과 일치해야 합니다. 성능 데이터 수집을 위해 통계 로깅을 설정해야 합니다.

Navisphere 명령줄 인터페이스 구문입니다

```
naviseccli.exe -h <IP address> -user <user> -password <password> -scope
<scope, use 0 for global scope> -port <use 443 by default> command
```

용어

OnCommand Insight는 EMC CLARiX 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
스토리지 프로세서	스토리지 노드
썸 풀, RAID 그룹	스토리지 풀
LUN을 클릭합니다	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 각 CLARiX 스토리지 프로세서의 IP 주소입니다
- CLARiX 스토리지에 대한 읽기 전용 Navisphere 사용자 이름 및 암호입니다
- NaviCLI는 Insight 서버/RAU에 설치해야 합니다
- 액세스 검증: 위의 사용자 이름과 암호를 사용하여 Insight 서버에서 각 어레이로 NaviCLI를 실행합니다.
- NaviCLI 버전은 스토리지의 최신 FLARE 코드와 일치해야 합니다

- 성능을 위해서는 통계 로깅을 설정해야 합니다.
- 포트 요구 사항: 80, 443

구성

필드에 입력합니다	설명
CLARiX 스토리지	CLARiX 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	CLARiX 스토리지 디바이스에 로그인하는 데 사용되는 이름입니다.
암호	CLARiX 스토리지 디바이스에 로그인하는 데 사용되는 암호입니다.
NaviCLI.exe 경로 또는 naviseccli.exe 경로에 대한 CLI 경로	에 대한 전체 경로입니다 navicli.exe 또는 naviseccli.exe 실행 파일

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
보안 클라이언트 사용(naviseccli)	보안 클라이언트(navseccli)를 사용하려면 선택합니다.
범위	보안 클라이언트 범위 기본값은 Global 입니다.
CLARiX CLI 포트입니다	CLARiX CLI에 사용되는 포트입니다
재고 외부 프로세스 시간 초과(초)	외부 프로세스 시간 초과(기본값 1800초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
성능 외부 프로세스 시간 초과(초)	외부 프로세스 시간 초과(기본값 1800초)

EMC Data Domain 데이터 소스

이 데이터 소스는 EMC Data Domain 데이터 중복 제거 스토리지 시스템에서 스토리지 및 구성 정보를 수집합니다. 데이터 소스를 추가하려면 특정 구성 지침 및 명령을 사용하고 데이터 소스 요구 사항 및 사용 권장 사항을 알고 있어야 합니다.

용어

OnCommand Insight는 EMC Data Domain 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
포트	포트
파일 시스템	내부 볼륨
MTree입니다	qtree를 입력합니다
할당량	할당량
NFS 및 CIFS 공유	파일 공유



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Data Domain 디바이스의 IP 주소입니다
- Data Domain 스토리지에 대한 읽기 전용 사용자 이름 및 암호
- SSH 포트 22

구성

필드에 입력합니다	설명
IP 주소입니다	Data Domain 스토리지 시스템의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름입니다	Data Domain 스토리지 시스템의 사용자 이름입니다
암호	Data Domain 스토리지 시스템의 암호입니다

고급 구성

필드에 입력합니다	설명
-----------	----

재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 180초)
SSH 포트	SSH 서비스 포트입니다

EMC ECC StorageScope 데이터 소스

EMC ECC StorageScope 디바이스에는 5.x, 6.0 및 6.1의 세 가지 데이터 소스가 있습니다.

구성



이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

* 필드 *	* 설명 *
ECC 서버	ECC 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	ECC 서버의 사용자 이름입니다
암호	암호 r ECC 서버

고급 구성

* 필드 *	* 설명 *
ECC 포트	ECC 서버에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
데이터베이스에 연결할 프로토콜입니다	데이터베이스에 연결하는 데 사용되는 프로토콜입니다
파일 시스템 정보를 쿼리합니다	WWN 별칭 및 파일 시스템에 대한 세부 정보를 검색하려면 선택합니다.

Dell EMC ECS 데이터 소스

이 데이터 수집기는 EMC ECS 스토리지 시스템에서 인벤토리 및 성능 데이터를 가져옵니다. 구성을 위해 데이터 수집기는 ECS 서버의 IP 주소와 관리 수준 도메인 계정이 필요합니다.

용어

OnCommand Insight는 EMC ECS 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
Cluser(사용자)	스토리지
테넌트	스토리지 풀
버킷	내부 볼륨
디스크	디스크



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- ECS Management Console의 IP 주소입니다
- ECS 시스템의 관리 수준 도메인 계정입니다
- 포트 443(HTTPS). ECS 시스템에서 TCP 포트 443에 대한 아웃바운드 연결이 필요합니다.
- 성능을 위해 ssh/scp 액세스를 위한 읽기 전용 사용자 이름과 암호를 사용합니다.
- 성능을 위해서는 포트 22가 필요합니다.

구성

필드에 입력합니다	설명
ECS 호스트	ECS 시스템의 IP 주소 또는 정규화된 도메인 이름입니다
ECS 호스트 포트	ECS 호스트와 통신하는 데 사용되는 포트입니다
ECS 공급업체 ID입니다	ECS의 공급업체 ID입니다
암호	ECS에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 360분입니다.

EMC Isilon 데이터 소스

Isilon SSH 데이터 소스는 EMC Isilon 스케일 아웃 NAS 스토리지에서 인벤토리 및 성능을 수집합니다.

용어

OnCommand Insight는 EMC Isilon 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
파일 시스템	내부 볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Isilon 스토리지에 대한 관리자 권한
- 을 사용하여 액세스를 검증했습니다 telnet 포트 22로 이동합니다

구성

필드에 입력합니다	설명
IP 주소입니다	Isilon 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름입니다	Isilon 클러스터의 사용자 이름입니다
암호	Isilon 클러스터의 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SSH 프로세스 대기 시간이 초과되었습니다	SSH 프로세스 시간 초과(기본값 60초)
SSH 포트	SSH 서비스 포트입니다

CLI 명령 실행 중

OnCommand Insight 버전 7.3.11 및 서비스 팩 9부터는 EMC Isilon 데이터 소스에 향상된 기능이 포함되어 Insight에서 더 많은 CLI 명령을 실행할 수 있습니다. 데이터 소스 내에서 루트 이외의 사용자를 사용하는 경우 해당 사용자 계정에 SSH를 통해 특정 CLI 명령을 실행할 수 있는 기능을 부여하기 위해 "sudoers" 파일을 구성했을 수 있습니다.

Insight에서 EMC의 "Access Zones" 기능을 이해하기 위해 이제 Insight에서 다음과 같은 새로운 CLI 명령을 추가로 실행합니다.

- `sudo isi zone zones list --format json -verbose`
- `sudo isi zone zones list`

Insight는 이러한 명령의 출력을 구문 분석하고 더 많은 기존 명령 인스턴스를 실행하여 기본 액세스 존이 아닌 영역에 있는 qtree, 할당량 및 NAS 공유/내보내기와 같은 개체의 논리적 구성을 가져옵니다. Insight Now는 이 기능 향상의 결과로 기본값이 아닌 액세스 존에 대한 개체를 보고합니다. Insight가 기존 명령(다른 옵션 사용)을 실행하여 해당 데이터를 가져올 때 해당 명령이 작동하려면 sudoers 파일을 변경할 필요가 없습니다. 이는 변경 사항이 필요하다는 위의 새 명령이 도입된 경우에만 해당됩니다.

Insight 서비스 계정이 이 Insight 릴리즈로 업그레이드하기 전에 해당 명령을 실행할 수 있도록 sudoers 파일을 업데이트하십시오. 그렇지 않으면 Isilon 데이터 소스가 실패합니다.

"파일 시스템" 통계

OnCommand Insight 7.3.12부터 EMC Isilon 데이터 수집기는 EMC Isilon의 노드 객체에 대한 "파일 시스템" 통계를 도입했습니다. OnCommand Insight에서 보고하는 기존 노드 통계는 "디스크" 기반 i.e, 스토리지 노드의 IOPS 및 처리량에 대해 이 노드의 디스크는 Aggregate에서 어떤 작업을 합니까? 그러나 읽기 작업이 메모리에 캐시되거나 압축이 사용 중인 워크로드의 경우 파일 시스템 워크로드가 실제로 디스크에 적중하는 것보다 훨씬 높을 수 있습니다. 5:1을 압축하는 데이터 세트에서는 "파일 시스템 읽기 처리량" 값이 스토리지 노드의 읽기 처리량보다 5배 높을 수 있습니다. 후자는 디스크에서 읽기를 측정하므로 노드가 데이터를 압축 해제하고 클라이언트의 읽기 요청을 처리할 때 5배 확장됩니다.

Dell EMC PowerStore 데이터 소스

Dell EMC PowerStore 데이터 수집기는 Dell EMC PowerStore 스토리지에서 인벤토리 정보를 수집합니다. 구성을 위해 데이터 수집기는 스토리지 프로세서의 IP 주소와 읽기 전용 사용자 이름 및 암호를 필요로 합니다.

용어

OnCommand Insight는 EMC Data Domain 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
호스트	호스트
host_volume_mapping을 선택합니다	host_volume_mapping을 선택합니다

하드웨어("extra_details" 객체 아래에 드라이브가 있음): 드라이브	디스크
어플라이언스	스토리지 풀
클러스터	스토리지
노드	스토리지노드
fc_port 를 선택합니다	포트
볼륨	볼륨
내부 볼륨	파일 시스템
파일 시스템	내부 볼륨
MTree입니다	qtree를 입력합니다
할당량	할당량
NFS 및 CIFS 공유	파일 공유



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지 프로세서의 IP 주소 또는 정규화된 도메인 이름입니다
- 읽기 전용 사용자 이름 및 암호

상위 일련 번호가 설명되었습니다

일반적으로 Insight는 스토리지 어레이의 일련 번호 또는 개별 스토리지 노드의 일련 번호를 보고할 수 있습니다. 그러나 일부 스토리지 어레이 아키텍처는 이 문제에 완전히 부합되지 않습니다. PowerStore 클러스터는 1-4개의 어플라이언스로 구성될 수 있으며 각 어플라이언스에는 2개의 노드가 있습니다. 어플라이언스 자체에 일련 번호가 있는 경우 해당 일련 번호는 클러스터나 노드의 일련 번호가 아닙니다.

개별 노드가 대형 클러스터의 일부인 중간 어플라이언스/엔클로저 내에 있는 경우 스토리지 노드 개체의 "상위 일련 번호" 속성은 Dell/EMC PowerStore 어레이에 맞게 적절하게 채워집니다.

구성

필드에 입력합니다	설명
-----------	----

PowerStore 게이트웨이	PowerStore 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	PowerStore의 사용자 이름입니다
암호	PowerStore에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
HTTPS 포트	기본값은 443입니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.

OnCommand Insight의 PowerStore 성능 수집을 통해 PowerStore의 5분 단위 소스 데이터를 사용할 수 있습니다. 따라서 Insight는 5분마다 해당 데이터를 폴링하여 구성할 수 없습니다.

EMC RecoverPoint 데이터 소스

EMC RecoverPoint 데이터 소스는 EMC RecoverPoint 스토리지에서 인벤토리 정보를 수집합니다. 구성의 경우 데이터 소스에 스토리지 프로세서의 IP 주소와 `_read-only_user` 이름 및 암호가 필요합니다.

EMC RecoverPoint 데이터 소스는 RecoverPoint가 다른 스토리지 시스템 간에 조정하는 볼륨 간 복제 관계를 수집합니다. OnCommand Insight는 각 RecoverPoint 클러스터의 스토리지 시스템을 보여 주며 해당 클러스터의 노드 및 스토리지 포트에 대한 인벤토리 데이터를 수집합니다. 스토리지 풀 또는 볼륨 데이터가 수집되지 않습니다.

요구 사항

- 스토리지 프로세서의 IP 주소 또는 정규화된 도메인 이름입니다
- 읽기 전용 사용자 이름 및 암호
- 포트 443을 통한 REST API 액세스
- PuTTY를 통한 SSH 액세스

구성

필드에 입력합니다	설명
RecoverPoint의 주소입니다	RecoverPoint 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	RecoverPoint 클러스터의 사용자 이름입니다
암호	RecoverPoint 클러스터의 암호입니다

필드에 입력합니다	설명
TCP 포트	RecoverPoint 클러스터에 접속하는 데 사용되는 TCP 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
제외된 클러스터	폴링 시 제외할 클러스터 ID 또는 이름의 심표로 구분된 목록입니다

SMI-S 성능 데이터 소스를 지원하는 EMC Solutions Enabler

OnCommand Insight는 Solutions Enabler를 사용하여 Symmetrix 스토리지 시스템을 검색합니다. `symcli` 사용자 환경에서 기존 Solutions Enabler 서버와 함께 사용되는 명령입니다. 기존 Solutions Enabler 서버는 게이트키퍼 볼륨에 대한 액세스를 통해 Symmetrix 스토리지에 접속할 수 있습니다. 이 장치에 액세스하려면 관리자 권한이 필요합니다.

용어

OnCommand Insight는 EMC Solutions Enabler 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
디스크 그룹	디스크 그룹
스토리지	스토리지
책임자	스토리지 노드
디바이스 풀, SRP(Storage Resource Pool)	스토리지 풀
디바이스, TDEV	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

이 데이터 소스를 구성하기 전에 OnCommand Insight 서버가 기존 Solutions Enabler 서버의 포트 2707에 대한 TCP 연결을 가지고 있는지 확인해야 합니다. OnCommand Insight는 해당 서버의 "sycfg list" 출력에 표시된 것처럼 이 서버에 대한 "Local" Symmetrix 스토리지를 모두 검색합니다.

- SMI-S Provider 애플리케이션이 포함된 EMC Solutions Enabler(CLI)가 설치되어 있어야 하며 버전이 Solutions Enabler Server에서 실행 중인 버전과 동일하거나 그 이전이어야 합니다.
- 올바르게 구성되었습니다 {installdir}\EMC\SYMAPI\config\netcnfg 파일이 필요합니다. 이 파일은 Solutions Enabler 서버의 서비스 이름 및 액세스 방법(Secure/NOSECURE/Any)을 정의합니다.
- 스토리지 노드 레벨에서 읽기/쓰기 지연 시간이 필요한 경우 SMI-S Provider는 Unisphere for VMAX 애플리케이션의 실행 중인 인스턴스와 통신해야 합니다.
- SE(Solutions Enabler) 서버에 대한 관리자 권한
- SE 소프트웨어의 읽기 전용 사용자 이름 및 암호
- Solutions Enabler Server 6.5X 요구 사항:
 - SMIS-S v1.2용 SMI-S Provider 3.3.1 설치
 - 설치 후 를 실행합니다 \Program Files\EMC\SYMCLI\bin>stordaemon start storsrvd
- Unisphere for VMAX 애플리케이션은 SMI-S Provider 설치를 통해 관리되는 Symmetrix VMAX 스토리지 시스템에 대한 통계를 실행 및 수집해야 합니다
- 액세스 검증: SMI-S Provider가 실행 중인지 확인합니다. telnet <se_server> 5988

구성



SMI-S 사용자 인증을 사용하지 않으면 OnCommand Insight 데이터 소스의 기본값이 무시됩니다.

Symmetrix 스토리지에 symauth를 설정하면 OnCommand Insight에서 해당 스토리지를 검색하는 기능이 억제될 수 있습니다. OnCommand Insight 취득은 Solutions Enabler 서버와 통신하는 OnCommand Insight/원격 획득 장치 서버에서 시스템 사용자로 실행됩니다. hostname\system에 symauth 권한이 없으면 OnCommand Insight에서 스토리지를 검색하지 못합니다.

EMC Solutions Enabler Symmetrix CLI 데이터 소스에는 씬 프로비저닝 및 SRDF(Symmetrix Remote Data Facility)에 대한 디바이스 구성이 지원됩니다.

Fibre Channel 및 스위치 성능 패키지에 대한 정의가 제공됩니다.

필드에 입력합니다	설명
서비스 이름	netcnfg 파일에 지정된 서비스 이름입니다
CLI의 전체 경로입니다	Symmetrix CLI의 전체 경로입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다

재고 제외 장치	포함하거나 제외할 장치 ID의 심표로 구분된 목록입니다
연결 캐싱	<p>연결 캐싱 방법 선택:</p> <ul style="list-style-type: none"> 로컬은 검색하려는 Symmetrix 스토리지에 Fibre Channel 접속이 가능하고 게이트키퍼 볼륨에 액세스할 수 있는 Solutions Enabler 서버에서 OnCommand Insight 획득 서비스가 실행되고 있음을 의미합니다. 이 문제는 일부 RAU(Remote Acquisition Unit) 구성에서 확인할 수 있습니다. remote_cached가 기본값입니다. 대부분의 경우 이 기능을 사용해야 합니다. 이 경우 NETCNFG 파일 설정을 사용하여 IP를 사용하여 Solutions Enabler 서버에 접속합니다. 이 서버는 검색할 Symmetrix 스토리지에 Fibre Channel 접속이 있어야 하며 게이트키퍼 볼륨에 액세스할 수 있어야 합니다. remote_cached 옵션으로 인해 CLI 명령이 실패하는 경우 원격 옵션을 사용합니다. 구입 프로세스가 느려집니다(극단적인 경우 몇 시간 또는 며칠이 걸릴 수 있음). NETCNFG 파일 설정은 검색 중인 Symmetrix 스토리지에 Fibre Channel 접속이 설정된 Solutions Enabler 서버에 대한 IP 접속에 계속 사용됩니다. <div>  <p>이 설정은 "symcfg list" 출력에 의해 원격 스토리지로 나열된 스토리지에 대한 OnCommand Insight 동작을 변경하지 않습니다. OnCommand Insight는 이 명령으로 로컬로 표시된 장치에서만 데이터를 수집합니다.</p> </div>
CLI 시간 제한(초)	CLI 프로세스 시간 초과(기본값: 7200초)
SMI-S 호스트 IP입니다	SMI-S Provider 호스트의 IP 주소입니다
SMI-S 포트	SMI-S Provider 호스트에서 사용하는 포트입니다
프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다
SMI-S 네임스페이스	SMI-S 공급자가 사용하도록 구성된 상호 운용성 네임스페이스입니다
SMI-S 사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
SMI-S 암호	SMI-S Provider 호스트의 사용자 이름입니다

성능 폴링 간격(초)	성능 폴링 간격(기본값 1000초)
성능 필터 유형	성능 데이터를 수집할 때 아래 스토리지 목록을 포함할지 제외할지 여부를 지정합니다
성능 필터 장치 목록	포함하거나 제외할 장치 ID의 쉼표로 구분된 목록입니다
RPO 폴링 간격(초)	RPO 폴링 간격(기본값 300초)

EMC VNX 데이터 소스

구성의 경우 EMC VNX(SSH) 데이터 소스에는 Control Station의 IP 주소와 _read-only_username 및 암호가 필요합니다.

구성

필드에 입력합니다	설명
VNX IP	VNX Control Station의 IP 주소 또는 정규화된 도메인 이름입니다
VNX 사용자 이름입니다	VNX Control Station의 사용자 이름입니다
VNX 암호	VNX Control Station의 암호입니다

요구 사항

- Control Station의 IP 주소입니다
- 읽기 전용 사용자 이름 및 암호.
- 액세스 검증: PuTTY를 통해 SSH 액세스를 검증합니다.

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
VNX SSH 프로세스 대기 시간 초과(초)	VNX SSH 프로세스 시간 초과(기본값 600초)
Celerra 명령 재시도 횟수입니다	Celerra 명령 재시도 횟수입니다
인벤토리에 대한 CLARiX 외부 프로세스 시간 초과(초)	인벤토리에 대한 CLARiX 외부 프로세스 시간 초과(기본값 1800초)

성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
CLARiX 외부 프로세스 성능 제한 시간(초)	성능을 위한 CLARiX 외부 프로세스 시간 초과(기본값 1800초)

EMC VNXe 데이터 소스

EMC VNXe 데이터 소스는 EMC VNXe 및 Unity 유니파이드 스토리지 시스템에 대한 인벤토리 지원을 제공합니다.

이 데이터 소스는 CLI 기반이며 VNXe 데이터 소스가 상주하는 수집 유닛에 Unisphere for VNXe CLI(uemcli.exe)를 설치해야 합니다. uemcli.exe 전송 프로토콜로 HTTPS를 사용하므로 획득 장치에서 VNXe/Unity 어레이에 대한 HTTPS 연결을 시작할 수 있어야 합니다. 데이터 소스에서 사용할 수 있는 읽기 전용 사용자가 적어도 있어야 합니다.

용어

OnCommand Insight는 EMC VNXe 데이터 소스에서 다음과 같은 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
프로세서	스토리지 노드
스토리지 풀	스토리지 풀
일반 iSCSI 블록 정보, VMware VMFS	볼륨
공유 폴더	내부 볼륨
CIFS 공유, NFS 공유, VMware NFS 데이터 저장소에서 공유	공유
복제 원격 시스템	동기화
iSCSI 노드	iSCSI 타겟 노드
iSCSI 초기자	iSCSI 대상 초기자



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하고 사용하기 위한 요구 사항입니다.

- VNXe 데이터 수집기는 CLI를 기반으로 합니다. VNXe 데이터 수집기가 있는 획득 유닛에 Unisphere for VNXe CLI(uemcli.exe)를 설치해야 합니다.
- uemcli.exe 전송 프로토콜로 HTTPS를 사용하므로 획득 장치에서 VNXe에 대한 HTTPS 연결을 시작할 수 있어야 합니다.
- 데이터 소스에서 사용할 수 있는 읽기 전용 사용자가 적어도 있어야 합니다.
- 관리 솔루션 Enabler 서버의 IP 주소입니다.
- 포트 443의 HTTPS가 필요합니다
- EMC VNXe 데이터 수집기는 인벤토리에 대한 NAS 및 iSCSI 지원을 제공합니다. Fibre Channel 볼륨은 검색되지만 Insight는 FC 매핑, 마스킹 또는 스토리지 포트에 대해서는 보고하지 않습니다.

구성

필드에 입력합니다	설명
VNXe 스토리지	VNXe 디바이스의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	VNXe 디바이스의 사용자 이름입니다
암호	VNXe 디바이스의 암호입니다
uemcli 실행 파일의 전체 경로입니다	에 대한 전체 경로입니다 uemcli.exe 실행 파일

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
VNXe CLI 포트	VNXe CLI에 사용되는 포트입니다
재고 외부 프로세스 시간 초과(초)	외부 프로세스 시간 초과(기본값 1800초)

EMC VPLEX 데이터 소스

구성의 경우 이 데이터 소스에 VPLEX 서버의 IP 주소와 관리 레벨 도메인 계정이 필요합니다.

용어

OnCommand Insight는 EMC VPLEX 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
클러스터	스토리지
엔진	스토리지 노드
장치, 시스템 확장	백엔드 스토리지 풀입니다
가상 볼륨	볼륨
프런트엔드 포트, 백엔드 포트	포트
분산 장치	저장소 동기화
스토리지 보기	볼륨 맵, 볼륨 마스크
스토리지 볼륨	백엔드 LUN
ITL	백엔드 경로



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- VPLEX 서버의 IP 주소입니다
- VPLEX 서버의 관리 레벨 도메인 계정입니다
- 포트 443(HTTPS). VPLEX 관리 스테이션의 TCP 포트 443에 대한 아웃바운드 연결이 필요합니다.
- 성능을 위해 ssh/scp 액세스를 위한 읽기 전용 사용자 이름과 암호를 사용합니다.
- 성능을 위해서는 포트 22가 필요합니다.
- 액세스 확인: 을 사용하여 확인합니다 telnet 포트 443으로 이동합니다. 기본 포트 이외의 포트에 대해 브라우저를 사용할 수 있습니다

구성

필드에 입력합니다	설명
VPLEX Management Console의 IP 주소입니다	VPLEX Management Console의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	VPLEX CLI의 사용자 이름입니다
암호	VPLEX CLI에 사용되는 암호입니다

VPLEX Management Console의 성능 원격 IP 주소입니다	VPLEX Management Console의 성능 원격 IP 주소입니다
성능 원격 사용자 이름입니다	VPLEX Management Console의 Performance Remote 사용자 이름입니다
성능 원격 암호	VPLEX Management Console의 성능 원격 암호

고급 구성

필드에 입력합니다	설명
통신 포트	VPLEX CLI에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
재시도 횟수	인벤토리 재시도 횟수입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 600초)
성능 SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 20초)
재시도 횟수	성능 재시도 횟수입니다

EMC XtremIO 데이터 소스

EMC XtremIO(HTTP) 데이터 소스를 구성하려면 XtremIO 관리 서버(XMS) 호스트 주소와 관리자 권한이 있는 계정이 있어야 합니다.

용어

OnCommand Insight는 EMC XtremIO 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크(SSD)	디스크
클러스터	스토리지

컨트롤러	스토리지 노드
볼륨	볼륨
LUN 매핑	볼륨 맵
초기자, 대상	볼륨 마스크



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 각 XtremIO 관리 서버의 IP 주소
- 관리자 권한이 있는 계정입니다
- 포트 443(HTTPS)에 대한 액세스

구성

필드에 입력합니다	설명
XMS 호스트	XtremIO 관리 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름입니다	XtremIO 관리 서버의 사용자 이름입니다
암호	XtremIO 관리 서버의 암호입니다

고급 구성

필드에 입력합니다	설명
TCP 포트	XTremIO 관리 서버에 연결하는 데 사용되는 TCP 포트 (기본값 443)
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Fujitsu ETERNUS 데이터 소스

Fujitsu ETERNUS 데이터 원본에는 스토리지의 IP 주소가 필요합니다. 심표로 구분할 수

없습니다.

용어

OnCommand Insight는 Fujitsu ETERNUS 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지	스토리지
씬 풀, 유연한 계층 풀, RAID 그룹	스토리지 풀
표준 볼륨, 스냅 데이터 볼륨(SDV), 스냅 데이터 풀 볼륨(SDPV), 씬 프로비저닝 볼륨(TPV)	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- ETERNUS 저장소의 IP 주소로, 심표로 구분될 수 없습니다
- SSH 관리 수준 사용자 이름 및 암호
- 포트 22
- 페이지 스크롤이 비활성화되어 있는지 확인합니다. (clienv -show -more -scroll disable)

구성

필드에 입력합니다	설명
ETERNUS 스토리지의 IP 주소입니다	ETERNUS 스토리지의 IP 주소입니다
사용자 이름	ETERNUS 스토리지에 대한 사용자 이름입니다
암호	휴기에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 풀링 간격(분)	재고 조사 간격(기본값 20분)
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)

Hitachi Content Platform(HCP) 데이터 소스

이 데이터 수집기는 HCP 관리 API를 사용하는 HCP(Hitachi Content Platform)를 지원합니다.

용어

OnCommand Insight는 HCP 데이터 소스에서 다음 재고 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
HCP 클러스터	스토리지
테넌트	스토리지 풀
네임스페이스	내부 볼륨
노드	노드



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- HCP 서버의 IP 주소입니다
- HCP 소프트웨어 및 피어 권한에 대한 읽기 전용 사용자 이름 및 암호입니다

구성

* 필드 *	* 설명 *
HCP 호스트	HCP 호스트의 IP 주소 또는 정규화된 도메인 이름입니다
HCP 포트	기본값은 9090입니다
HCP 사용자 ID입니다	HCP 호스트의 사용자 이름입니다

HCP 암호	HCP 호스트에 사용되는 암호입니다
HCP 인증 유형	HCP_LOCAL 또는 ACTIVE_DIRECTORY 를 선택합니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 900초)

HDS HiCommand Device Manager 데이터 소스

HDS HiCommand 및 HiCommand Lite 데이터 소스는 HiCommand Device Manager 서버를 지원합니다. OnCommand Insight는 표준 HiCommand API를 사용하여 HiCommand Device Manager 서버와 통신합니다.

용어

OnCommand Insight는 HDS HiCommand 및 HiCommand Lite 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
개발	디스크
저널 풀	디스크 그룹
스토리지	스토리지
포트 컨트롤러	스토리지 노드
스토리지 그룹, DP 풀	스토리지 풀
논리 유닛, LDEV	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- HiCommand Device Manager 서버의 IP 주소입니다

- HiCommand Device Manager 소프트웨어 및 피어 권한에 대한 읽기 전용 사용자 이름 및 암호입니다
- 포트 요구 사항: 2001(http) 또는 2443(https)
- 액세스 확인:
 - 피어 사용자 이름 및 암호를 사용하여 HiCommand Device Manager 소프트웨어에 로그인합니다.
 - HiCommand Device Manager API에 대한 액세스 확인: telnet <HiCommand Device_Manager_server_ip> 2001

성능 요구사항

- HDS USP, USP V 및 VSP 성능
 - 성능 모니터에 라이선스가 있어야 합니다.
 - 모니터링 스위치를 활성화해야 합니다.
 - 내보내기 도구 (Export.exe)을 OnCommand Insight 서버에 복사해야 합니다.
 - 내보내기 도구 버전은 대상 스토리지의 마이크로코드 버전과 일치해야 합니다.
- HDS AMS 성능
 - 성능 모니터의 라이선스를 받아야 합니다.
 - SNM2(Storage Navigator Modular 2) CLI 유틸리티를 OnCommand Insight 서버에 설치해야 합니다.
 - 다음 명령을 사용하여 OnCommand Insight에서 성능을 획득해야 하는 모든 AMS, WMS, SMS 저장소 어레이를 등록해야 합니다.
 - 등록한 모든 스토리지가 다음 명령의 출력에 나열되어 있는지 확인해야 합니다. auunitref.exe.

구성

* 필드 *	* 설명 *
HiCommand 서버	HiCommand Device Manager 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	HiCommand Device Manager 서버의 사용자 이름입니다.
암호	HiCommand Device Manager 서버에 사용되는 암호입니다.

디바이스 - VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지	<p>VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지를 위한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다.</p> <ul style="list-style-type: none"> • 스토리지의 IP: 스토리지의 IP 주소입니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다 • Export Utility Jar Files(유틸리티 JAR 파일 내보내기): Export Utility(내보내기 유틸리티)가 포함된 폴더입니다 .jar 파일
SNM2Devices - WMS/SMS/AMS 저장소	<p>WMS/SMS/AMS 저장소에 대한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다.</p> <ul style="list-style-type: none"> • 스토리지의 IP: 스토리지의 IP 주소입니다 • Storage Navigator CLI 경로: SNM2 CLI 경로 • 계정 인증 유효: 유효한 계정 인증을 선택하려면 선택합니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다
성능 조정 관리자 를 선택합니다	성능 튜닝 관리자를 선택하고 다른 성능 옵션을 재정의합니다
튜닝 관리자 호스트	튜닝 관리자의 IP 주소 또는 정규화된 도메인 이름입니다
Tuning Manager 포트	Tuning Manager에 사용되는 포트입니다
튜닝 관리자 사용자 이름	Tuning Manager의 사용자 이름입니다
조정 관리자 암호	Tuning Manager 암호



HDS USP, USP V 및 VSP에서 모든 디스크는 둘 이상의 스토리지 그룹에 속할 수 있습니다.

고급 구성

필드에 입력합니다	설명
HiCommand 서버 포트	HiCommand 장치 관리자에 사용되는 포트입니다
HTTPS가 활성화되었습니다	HTTPS를 활성화하려면 선택합니다
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)

목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다
장치 제외 또는 포함	포함하거나 제외할 장치 ID 또는 배열 이름의 심표로 구분된 목록입니다
호스트 관리자를 쿼리합니다	호스트 관리자를 쿼리하려면 선택합니다
HTTP 시간 제한(초)	HTTP 연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
내보내기 제한 시간(초)	내보내기 유틸리티 시간 초과(기본값 300초)

Hitachi Ops Center 데이터 수집기

이 데이터 수집기는 Hitachi Ops Center의 통합 애플리케이션 제품군을 사용하여 여러 스토리지 디바이스의 인벤토리 및 성능 데이터에 액세스합니다. 인벤토리 및 용량 검색을 위해 Ops Center 설치에는 "공동 서비스" 및 "관리자" 구성 요소가 모두 포함되어야 합니다. 성능 수집을 위해 "Analyzer"를 추가로 구축해야 합니다.

용어

OnCommand Insight는 이 데이터 수집기에서 다음 인벤토리 정보를 가져옵니다. 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	OnCommand Insight 용어입니다
스토리지 시스템	스토리지
볼륨	볼륨
패리티 그룹	스토리지 풀(RAID), 디스크 그룹
디스크	디스크
스토리지 풀	스토리지 풀(썸, 스냅)
외부 패리티 그룹	스토리지 풀(백엔드), 디스크 그룹
포트	스토리지 노드 → 컨트롤러 노드 → 포트
호스트 그룹	볼륨 매핑 및 마스킹
볼륨 쌍	저장소 동기화

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

재고 데이터를 수집하려면 다음이 있어야 합니다.

- "공통 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 호스트 이름입니다
- Ops Center 구성 요소를 호스팅하는 모든 서버에 있는 루트/sysadmin 사용자 계정 및 암호입니다. HDS는 Ops Center 10.8 이상이 될 때까지 LDAP/SSO 사용자의 REST API 지원을 구현하지 않았습니다

성능 요구사항

성능 데이터를 수집하려면 다음 요구사항을 충족해야 합니다.

- HDS Ops Center "Analyzer" 모듈을 설치해야 합니다
- 스토리지 어레이가 운영 센터 "Analyzer" 모듈에 제공되어야 합니다

구성

필드에 입력합니다	설명
Hitachi Ops Center IP 주소입니다	"공통 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Ops Center 서버의 사용자 이름입니다.
암호	Ops Center 서버에 사용되는 암호입니다.

고급 구성

필드에 입력합니다	설명
연결 유형	기본값은 HTTPS(포트 443)입니다
TCP 포트를 재정의합니다	기본값이 아닌 경우 사용할 포트를 지정합니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40입니다.
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다.
장치 목록을 필터링합니다	포함하거나 제외할 장치 일련 번호의 심표로 구분된 목록입니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.

HDS 스토리지

HDS 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트나 참조에 적용되는 용어입니다.

HDS 스토리지 용어

다음 용어는 HDS 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 이름 — GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 ""이름" 속성에서 직접 가져옵니다
- 모델 - GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 ""arrayType"" 특성에서 직접 제공됩니다

- 공급업체 — HDS
- Family - GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 ""arrayFamily" 속성에서 직접 제공됩니다
- IP — 어레이의 모든 IP 주소 목록이 아니라 어레이의 관리 IP 주소입니다
- Raw Capacity — 디스크 역할에 관계없이 이 시스템에 있는 모든 디스크의 총 용량 합계를 나타내는 Base2 값입니다.

HDS 스토리지 풀

HDS 스토리지 풀 자산 랜딩 페이지에서 찾을 수 있는 오브젝트나 참조에 적용되는 용어입니다.

HDS 스토리지 풀 용어

다음 용어는 HDS 스토리지 풀 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 유형: 여기에 있는 값은 다음 중 하나입니다.
 - 예약됨 — 이 풀이 데이터 볼륨(예: 저널링, 스냅샷)이 아닌 다른 용도로 사용되는 경우
 - 씬 프로비저닝 — HDP 풀인 경우
 - RAID 그룹 — 다음과 같은 몇 가지 이유로 이러한 항목이 표시되지 않을 수 있습니다.

OCI는 용량을 모든 비용에 두 배로 늘리는 것을 피하기 위해 강력한 입지를 가지고 있습니다. HDS에서는 일반적으로 디스크에서 RAID 그룹을 구축하고, 해당 RAID 그룹에 풀 볼륨을 생성하고, 해당 풀 볼륨에서 풀 (대개 HDP이지만 특수한 용도로 사용될 수 있음)을 구성해야 합니다. OCI가 기본 RAID 그룹과 풀을 모두 보고한 경우 원시 용량의 합이 디스크 합보다 엄청나게 큼니다.

대신, OCI의 HDS HiCommand 데이터 수집기는 풀 볼륨의 용량에 따라 RAID 그룹의 크기를 임의로 축소합니다. 결과적으로 OCI가 RAID 그룹을 보고하지 않을 수 있습니다. 또한 결과 RAID 그룹은 OCI WebUI에서 표시되지 않지만 DWH(OCI 데이터 웨어하우스)로 흐르게 되는 방식으로 플래그가 지정됩니다. 이러한 의사 결정의 목적은 대부분의 사용자가 신경 쓰지 않는 것들에 대한 UI 혼란을 피하는 것입니다. HDS 어레이에 50MB의 여유 공간이 있는 RAID 그룹이 있는 경우, 의미 있는 결과를 얻기 위해 이 여유 공간을 사용할 수 없을 것입니다.

- HDS 풀은 특정 노드에 연결되지 않으므로 노드 N/A입니다
- 이중화 - 풀의 RAID 레벨입니다. 여러 RAID 유형으로 구성된 HDP 풀의 값이 여러 개일 수 있습니다
- 용량 % - 풀의 사용된 GB 및 총 논리적 GB 크기와 함께 데이터 사용에 사용된 풀의 비율
- 과도하게 커밋된 용량 - 이 풀의 논리적 용량이 풀의 논리적 용량을 이 비율로 초과하는 논리적 볼륨의 합계로 이 비율에 의해 초과 할당되고 있습니다.
- 스냅샷 - 이 풀의 스냅샷 사용을 위해 예약된 용량을 표시합니다

HDS 스토리지 노드

HDS 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트나 참조에 적용되는 용어입니다.

HDS 스토리지 노드 용어

다음 용어는 HDS 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 이름 - 모듈식 어레이에 있는 프런트엔드 디렉터(FED) 또는 채널 어댑터의 이름 또는 모듈식 어레이에서 컨트롤러의 이름입니다. 주어진 HDS 어레이에는 2개 이상의 스토리지 노드가 있습니다
- 볼륨 — 볼륨 테이블에는 이 스토리지 노드가 소유한 포트에 매핑된 모든 볼륨이 표시됩니다

Hitachi Ops Center 데이터 수집기

이 데이터 수집기는 Hitachi Ops Center의 통합 애플리케이션 제품군을 사용하여 여러 스토리지 디바이스의 인벤토리 및 성능 데이터에 액세스합니다. 인벤토리 및 용량 검색을 위해 Ops Center 설치에는 "공통 서비스" 및 "관리자" 구성 요소가 모두 포함되어야 합니다. 성능 수집을 위해 "Analyzer"를 추가로 구축해야 합니다.

용어

OnCommand Insight는 이 데이터 수집기에서 다음 인벤토리 정보를 가져옵니다. 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	OnCommand Insight 용어입니다
스토리지 시스템	스토리지
볼륨	볼륨
패리티 그룹	스토리지 풀(RAID), 디스크 그룹
디스크	디스크
스토리지 풀	스토리지 풀(썸, 스냅)
외부 패리티 그룹	스토리지 풀(백엔드), 디스크 그룹
포트	스토리지 노드 → 컨트롤러 노드 → 포트
호스트 그룹	볼륨 매핑 및 마스킹
볼륨 쌍	저장소 동기화

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

재고 데이터를 수집하려면 다음이 있어야 합니다.

- "공통 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 호스트 이름입니다
- Ops Center 구성 요소를 호스팅하는 모든 서버에 있는 루트/sysadmin 사용자 계정 및 암호입니다. HDS는 Ops Center 10.8 이상이 될 때까지 LDAP/SSO 사용자의 REST API 지원을 구현하지 않았습니다

성능 요구사항

성능 데이터를 수집하려면 다음 요구사항을 충족해야 합니다.

- HDS Ops Center "Analyzer" 모듈을 설치해야 합니다
- 스토리지 어레이가 운영 센터 "Analyzer" 모듈에 제공되어야 합니다

구성

필드에 입력합니다	설명
Hitachi Ops Center IP 주소입니다	"공동 서비스" 구성 요소를 호스팅하는 Ops Center 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Ops Center 서버의 사용자 이름입니다.
암호	Ops Center 서버에 사용되는 암호입니다.

고급 구성

필드에 입력합니다	설명
연결 유형	기본값은 HTTPS(포트 443)입니다
TCP 포트를 재정의합니다	기본값이 아닌 경우 사용할 포트를 지정합니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40입니다.
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다.
장치 목록을 필터링합니다	포함하거나 제외할 장치 일련 번호의 심표로 구분된 목록입니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.

HDS NAS(HNAS) 데이터 소스

HDS NAS(HNAS) 데이터 소스는 HDS NAS 클러스터의 검색을 지원하는 인벤토리 및 구성 데이터 소스입니다. Insight는 NFS 및 CIFS 공유, 파일 시스템(Insight 내부 볼륨) 및 확장(Insight 스토리지 풀)을 검색할 수 있도록 지원합니다.

이 데이터 소스는 SSH 기반이므로 HNAS 자체의 TCP 22 또는 클러스터가 연결된 시스템 관리 장치(SMU)에 대해 SSH 세션을 시작할 수 있어야 합니다.

용어

OnCommand Insight는 HNAS 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
계층	디스크 그룹
클러스터	스토리지

노드	스토리지 노드
스팬	스토리지 풀
파일 시스템	내부 볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하고 사용하기 위한 요구 사항입니다.

- 장치 IP 주소입니다
- 포트 22, SSH 프로토콜
- 사용자 이름 및 암호 권한 수준: 감독자
- 참고: 이 데이터 수집기는 SSH 기반이므로 HNAS 자체의 TCP 22 또는 클러스터가 연결된 시스템 관리 장치(SMU)에 대해 SSH 세션을 시작할 수 있어야 합니다.



이 데이터 수집기는 SSH 기반이므로 HNAS 자체의 TCP 22 또는 클러스터가 연결된 시스템 관리 장치(SMU)에 대해 SSH 세션을 시작할 수 있어야 합니다.

구성

필드에 입력합니다	설명
HNAS 호스트	HNAS 관리 호스트의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	HNAS CLI의 사용자 이름입니다
암호	HNAS CLI에 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
SSH 배너 대기 시간 제한(초)	SSH 배너 대기 시간 초과(기본값 15초)
SSH 명령 시간 초과(초)	SSH 명령 시간 초과(기본값 30초)

HP CommandView AE 데이터 소스

HP CommandView Advanced Edition(AE) 및 CommandView AE CLI/SMI(AE Lite) 데이터 소스는 CommandView(HiCommand) 장치 관리자 서버라고도 함)의 인벤토리 및 성능을 지원합니다.

용어

OnCommand Insight는 HP CommandView AE 및 AE Lite 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
개발	디스크
저널 풀	디스크 그룹
스토리지	스토리지
포트 컨트롤러	스토리지 노드
스토리지 그룹, DP 풀	스토리지 풀
논리 유닛, LDEV	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- HiCommand Device Manager 서버의 IP 주소입니다
- CommandView AE 소프트웨어 및 피어 권한에 대한 읽기 전용 사용자 이름 및 암호
- 장치 관리자의 CommandView AE Lite 버전에는 CLI 라이선스만 있습니다
- 포트 요구 사항: 2001

성능 요구사항

- HDS USP, USP V 및 VSP 성능
 - 성능 모니터에 라이선스가 있어야 합니다.
 - 모니터링 스위치를 활성화해야 합니다.
 - 내보내기 도구 (Export.exe)을 OnCommand Insight 서버에 복사해야 합니다.
 - 내보내기 도구 버전은 대상 스토리지의 마이크로코드 버전과 일치해야 합니다.
- HDS AMS 성능

- 성능 모니터의 라이선스를 받아야 합니다.
- SNM2(Storage Navigator Modular 2) CLI 유틸리티를 OnCommand Insight 서버에 설치해야 합니다.
- 다음 명령을 사용하여 OnCommand Insight에서 성능을 획득해야 하는 모든 AMS, WMS, SMS 저장소 어레이를 등록해야 합니다.
- 등록한 모든 스토리지가 다음 명령의 출력에 나열되어 있는지 확인해야 합니다. `auunitref.exe`.

구성

* 필드 *	* 설명 *
HiCommand 서버	HiCommand Device Manager 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	HiCommand Device Manager 서버의 사용자 이름입니다.
암호	HiCommand Device Manager 서버에 사용되는 암호입니다.
장치 - USP, USP V, VSP/R600 보관	<p>VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지를 위한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다.</p> <ul style="list-style-type: none"> • 스토리지의 IP: 스토리지의 IP 주소입니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다 • Export Utility Jar Files(유틸리티 JAR 파일 내보내기): Export Utility(내보내기 유틸리티)가 포함된 폴더입니다 .jar 파일
SNM2Devices - WMS/SMS/AMS 저장소	<p>WMS/SMS/AMS 저장소에 대한 장치 목록입니다. 각 스토리지에는 다음이 필요합니다.</p> <ul style="list-style-type: none"> • 스토리지의 IP: 스토리지의 IP 주소입니다 • Storage Navigator CLI 경로: SNM2 CLI 경로 • 계정 인증 유효: 유효한 계정 인증을 선택하려면 선택합니다 • User Name: 스토리지의 사용자 이름입니다 • 암호: 스토리지의 암호입니다
성능 조정 관리자 를 선택합니다	성능 튜닝 관리자를 선택하고 다른 성능 옵션을 재정의합니다
튜닝 관리자 호스트	튜닝 관리자의 IP 주소 또는 정규화된 도메인 이름입니다

Tuning Manager 포트	Tuning Manager에 사용되는 포트입니다
튜닝 관리자 사용자 이름	Tuning Manager의 사용자 이름입니다
조정 관리자 암호	Tuning Manager 암호



HDS USP, USP V 및 VSP에서 모든 디스크는 둘 이상의 스토리지 그룹에 속할 수 있습니다.

고급 구성

필드에 입력합니다	설명
HiCommand 서버 포트	HiCommand 장치 관리자에 사용되는 포트입니다
HTTPS가 활성화되었습니다	HTTPS를 활성화하려면 선택합니다
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다
장치 제외 또는 포함	포함하거나 제외할 장치 ID 또는 배열 이름의 심표로 구분된 목록입니다
호스트 관리자를 쿼리합니다	호스트 관리자를 쿼리하려면 선택합니다
HTTP 시간 제한(초)	HTTP 연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
내보내기 제한 시간(초)	내보내기 유틸리티 시간 초과(기본값 300초)

HP EVA 스토리지 데이터 소스

구성을 위해 EVA 스토리지(SSSU) 데이터 원본에는 명령 보기(CV) 서버의 IP 주소와 CV 소프트웨어에 대한 `_read-only_username` 및 암호가 필요합니다. 사용자는 CV 소프트웨어에서 정의해야 합니다.

용어

OnCommand Insight는 HP EVA 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
디스크 그룹	디스크 그룹(모델링되지 않음)
스토리지 셀	스토리지
가상 디스크	스토리지 풀
가상 디스크	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- CV 서버의 IP 주소입니다
- CV 소프트웨어에 대한 읽기 전용 사용자 이름 및 암호 사용자는 CV 소프트웨어에서 정의해야 합니다.
- OnCommand Insight 서버/RAU에 설치된 타사 소프트웨어: `sssu.exe`. 를 클릭합니다 `sssu.exe` 버전은 CV 버전과 일치해야 합니다.
- 액세스 검증: 실행 `sssu.exe` 사용자 이름 및 암호를 사용하는 명령입니다.

성능 요구사항

HP StorageWorks 명령 보기 EVA 소프트웨어 제품군을 OnCommand Insight 서버에 설치해야 합니다. 또는 EVA 서버에 RAU(원격 획득 장치)를 설치할 수 있습니다.

1. OnCommand Insight 서버에 HP StorageWorks 명령 보기 EVA 소프트웨어 제품군을 설치하거나 명령 보기 EVA 서버에 원격 획득 장치를 설치합니다.
2. 를 찾습니다 `evaperf.exe` 명령. 예를 들면, 다음과 같습니다. `c:\Program Files\Hewlett-Packard\EVA Performance Monitor\`
3. Command View 서버의 IP를 사용하여 다음 단계를 수행하십시오.
 - a. 860이 기본 포트인 경우 이 명령을 실행합니다 `Evaperf.exe server <Command View Server IP> 860 <username>`
 - b. 암호 프롬프트에 Command View 서버 암호를 입력합니다.

이렇게 하면 명령줄 프롬프트가 반환되고 다른 것은 반환되지 않습니다.

4. 를 실행하여 설정을 확인합니다 `evaperf.exe ls`.

Command View 서버에서 관리하는 어레이 또는 컨트롤러 목록이 표시됩니다. 각 라인은 EVA 어레이에서 컨트롤러를 표시합니다.

구성

* 필드 *	* 설명 *
CommandView 서버	EVA Storage Manager의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Command View Manager의 사용자 이름입니다. 이름은 Command View에서 정의해야 합니다.
암호	Command View Manager에 사용되는 암호입니다.
성능 사용자 이름입니다	성능을 위해 Command View Manager의 사용자 이름입니다. 이름은 Command View에서 정의해야 합니다.
성능 암호	성능을 위해 Command View Manager에 사용되는 암호입니다.

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
CLI 홈	CLI 홈 디렉토리의 전체 경로 이름 <code>sssu.exe</code> 있습니다
재고 제외 장치	심표로 구분된 포함할 장치 이름 목록입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
Performance CLI Home을 참조하십시오	어레이 성능의 경우 <code>sssu.exe</code> 있는 CLI 홈 디렉토리의 전체 경로 이름입니다. 액세스를 확인하려면 <code>sssu.exe</code> 실행합니다
명령 시간 초과(초)	<code>evaperf</code> 명령 대기 시간 초과(기본값 600초)
성능 제외 장치	성능 데이터 수집에서 제외할 장치 이름의 심표로 구분된 목록입니다

HPE Nimble 데이터 소스

HPE Nimble 데이터 수집기는 HPE Nimble 스토리지 어레이에 대한 인벤토리 및 성능 데이터를 지원합니다.

용어

OnCommand Insight는 HPE Nimble 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
스토리지	스토리지
디스크	디스크
수영장	스토리지 풀
볼륨	볼륨
이니시에이터	스토리지 호스트 별칭입니다
컨트롤러	스토리지 노드
Fibre Channel 인터페이스	컨트롤러



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지를 설치하고 구성해야 하며 FQDN(정규화된 도메인 이름) 또는 스토리지 관리 IP 주소를 통해 클라이언트에서 연결할 수 있어야 합니다.
- 스토리지에서 NimbleOS 2.3.x 이상을 실행해야 합니다.
- 어레이에 대한 유효한 사용자 이름과 암호가 있어야 합니다.
- 포트 5392가 어레이에서 열려 있어야 합니다.

구성

* 필드 *	* 설명 *
스토리지 관리 IP 주소입니다	FQDN(정규화된 도메인 이름) 또는 스토리지 관리 IP 주소입니다.
사용자 이름	Nimble 스토리지의 사용자 이름입니다
암호	Nimble 스토리지의 암호입니다

고급 구성

* 필드 *	* 설명 *
포트	Nimble REST API에서 사용하는 포트입니다. 기본값은 5392입니다.
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)

참고: 기본 성능 폴링 간격은 300초이며 변경할 수 없습니다. Nimble에서 지원하는 유일한 간격입니다.

Huawei OceanStor 데이터 소스

OnCommand Insight는 Huawei OceanStor(REST/HTTPS) 데이터 소스를 사용하여 Huawei OceanStor 스토리지의 인벤토리를 검색합니다.

용어

OnCommand Insight는 Huawei OceanStor로부터 다음과 같은 인벤토리 및 성능 정보를 수집합니다. OnCommand Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	OnCommand Insight 용어입니다
스토리지 풀	스토리지 풀
파일 시스템	내부 볼륨
컨트롤러	스토리지 노드
FC 포트(매핑)	볼륨 맵
호스트 FC 이니시에이터(매핑)	볼륨 마스크
NFS/CIFS 공유입니다	공유
공유	iSCSI 타겟 노드
iSCSI 링크 초기자	iSCSI 이니시에이터 노드입니다
디스크	디스크
LUN을 클릭합니다	볼륨

요구 사항

다음은 이 데이터 수집기를 구성하고 사용하기 위한 요구 사항입니다.

- 장치 IP
- OceanStor 장치 관리자에 액세스하기 위한 자격 증명
- 포트 8088을 사용할 수 있어야 합니다

구성

필드에 입력합니다	설명
OceanStor 호스트 IP 주소입니다	OceanStor Device Manager의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	OceanStor Device Manager에 로그인하는 데 사용되는 이름입니다
암호	OceanStor Device Manager에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
TCP 포트	OceanStor Device Manager에 연결하는 데 사용되는 TCP 포트(기본값 8088)
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)

IBM Cleversafe 데이터 소스

이 데이터 소스는 IBM Cleversafe에 대한 인벤토리 및 성능 데이터를 수집합니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- 관리자 IP 주소 또는 호스트 이름
- 동일한 사용자 이름과 암호
- 포트 9440

구성

필드에 입력합니다	설명
-----------	----

Cleversafe 관리자 호스트 이름 또는 IP 주소	클레버세이프 장치의 호스트 IP 주소입니다
사용자 이름	Cleversafe에 로그인하는 데 사용되는 이름입니다
암호	Cleversafe에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다
HTTP 연결 시간 초과)	기본값은 60초입니다

IBM DS 데이터 소스

IBM DS(CLI) 데이터 소스는 DS6xxx 및 DS8xxx 디바이스만 지원합니다. DS3xxx, DS4xxx 및 DS5xxx 장치는 NetApp E-Series 데이터 소스에서 지원됩니다. 지원되는 모델 및 펌웨어 버전은 Insight 데이터 소스 지원 매트릭스를 참조하십시오.

용어

OnCommand Insight는 IBM DS 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크 드라이브 모듈	디스크
스토리지 이미지	스토리지
익스텐트 풀	스토리지 풀
고정 블록 볼륨	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 각 DS 배열의 IP 주소입니다
- 스토리지 표시 이름은 선택 사항이며 외관만 가능합니다
- 각 DS 어레이에 대한 읽기 전용 사용자 이름 및 암호

- Insight 서버에 설치된 타사 소프트웨어: IBM dscli
- 액세스 검증: 실행 dscli 사용자 이름 및 암호를 사용하는 명령입니다
- 포트 요구 사항: 80, 443 및 1750

구성

필드에 입력합니다	설명
DS 스토리지	DS Storage Host의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	DS CLI에 사용되는 이름입니다
암호	DS CLI에 사용되는 암호입니다
실행 파일 dscli.exe 경로	에 대한 전체 경로입니다 dscli.exe유틸리티.

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
스토리지 표시 이름	IBM DS 스토리지 어레이의 이름입니다
재고 제외 장치	인벤토리 수집에서 제외할 장치 일련 번호의 쉼표로 구분된 목록입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
성능 필터 유형	Include(포함): 목록의 장치에서만 수집된 데이터입니다. 제외: 이러한 장치에서 데이터가 수집되지 않습니다
성능 필터 장치 목록	성능 컬렉션에서 포함하거나 제외할 장치 ID의 쉼표로 구분된 목록입니다

IBM PowerVM 데이터 소스

IBM PowerVM(SSH) 데이터 소스는 HMC(하드웨어 관리 콘솔)에서 관리하는 IBM POWER 하드웨어 인스턴스에서 실행되는 가상 파티션에 대한 정보를 수집합니다. 구성의 경우 이 데이터 원본에서는 SSH를 통해 HMC에 로그인하기 위한 사용자 이름과 HMC 구성에 대한 보기 수준 권한이 필요합니다.

용어

OnCommand Insight는 IBM PowerVM 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
hdisk	가상 디스크
관리 대상 시스템	호스트
LPAR, VIO 서버	가상 머신
볼륨 그룹	데이터 저장소
물리적 볼륨	LUN을 클릭합니다



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- HMC(Hardware Management Console)의 IP 주소
- SSH를 통해 HMC에 대한 액세스를 제공하는 사용자 이름 및 암호
- 포트 요구 사항 SSH-22
- 모든 관리 시스템 및 논리 파티션 보안 도메인에 대한 권한을 봅니다

또한 HMC 구성에 대한 보기 권한과 HMC 콘솔 보안 그룹화를 위한 VPD 정보를 수집할 수 있는 기능도 있어야 합니다. 또한 사용자는 논리 파티션 보안 그룹화를 통해 가상 IO 서버 명령 액세스를 허용해야 합니다. 작업자의 역할에서 시작하여 모든 역할을 제거하는 것이 가장 좋습니다. HMC의 읽기 전용 사용자는 AIX 호스트에서 프록시 명령을 실행할 권한이 없습니다.

- IBM 모범 사례는 두 개 이상의 HMCS를 통해 디바이스를 모니터링하는 것입니다. 이렇게 하면 OnCommand Insight에서 중복된 디바이스를 보고할 수 있으므로 이 데이터 수집기의 고급 구성에 있는 "장치 제외" 목록에 중복 디바이스를 추가하는 것이 좋습니다.

구성

* 필드 *	* 설명 *
HMC(Hardware Management Console) 주소입니다	PowerVM 하드웨어 관리 콘솔의 IP 주소 또는 정규화된 도메인 이름입니다
HMC 사용자	하드웨어 관리 콘솔의 사용자 이름입니다
암호	하드웨어 관리 콘솔에 사용되는 암호입니다

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
SSH 포트	SSH에서 PowerVM에 사용되는 포트입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 600초)
재시도 횟수	인벤토리 재시도 횟수입니다
장치 제외	제외할 장치 ID 또는 표시 이름의 쉼표로 구분된 목록입니다

IBM SVC 데이터 소스

IBM SVC 데이터 소스는 SSH를 사용하여 인벤토리 및 성능 데이터를 수집하여 SVC 운영 체제를 실행하는 다양한 디바이스를 지원합니다. 지원되는 디바이스 목록에는 SVC, V7000, V5000 및 V3700과 같은 모델이 포함됩니다. 지원되는 모델 및 펌웨어 버전은 Insight 데이터 소스 지원 매트릭스를 참조하십시오.

용어

OnCommand Insight는 IBM SVC 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
Mdisk 그룹	스토리지 풀
vDisk를 선택합니다	볼륨
Mdisk	백엔드 LUN



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

재고 요건

- 각 SVC 클러스터의 IP 주소입니다
- 포트 22를 사용할 수 있습니다
- Insight에서 생성하거나 이미 SVC에서 사용 중인 키 쌍을 재사용하는 공개 키 및 개인 키 쌍

기존 키 쌍을 재사용하는 경우 Putty 형식에서 OpenSSH 형식으로 변환해야 합니다.

- SVC 클러스터에 설치된 공개 키
- 개인 키는 데이터 소스에서 식별되어야 합니다
- 액세스 검증: 열기 `ssh` 개인 키를 사용하여 SVC 클러스터에 대한 세션입니다



타사 소프트웨어를 설치할 필요가 없습니다.

성능 요구사항

- SVC 콘솔은 모든 SVC 클러스터에 필수이며 SVC 검색 기반 패키지에 필요합니다.
- 관리 액세스 수준은 클러스터 노드에서 구성 노드로 성능 데이터 파일을 복사하는 경우에만 필요합니다.



SVC Foundation Discovery Package에 이 액세스 수준이 필요하지 않으므로 SVC Foundation 사용자가 정상적으로 작동하지 않을 수 있습니다.

- 포트 22가 필요합니다
- 이 사용자에게 대해 개인 및 공용 SSH 키를 생성하고 개인 키를 저장하여 획득 장치에서 액세스할 수 있도록 해야 합니다. SVC Foundation 사용자에게 적절한 권한이 있는 경우 동일한 사용자 및 키가 작동합니다. 인벤토리 및 성능 데이터에 동일한 SSH 키를 사용할 수 있습니다.
- SSH를 통해 SVC 클러스터에 접속하고 다음을 실행하여 데이터 수집을 활성화합니다. `svctask startstats -interval 1`



또는 SVC 관리 사용자 인터페이스를 사용하여 데이터 수집을 사용하도록 설정합니다.

상위 일련 번호가 설명되었습니다

일반적으로 Insight는 스토리지 어레이의 일련 번호 또는 개별 스토리지 노드의 일련 번호를 보고할 수 있습니다. 그러나 일부 스토리지 어레이 아키텍처는 이 문제에 완전히 부합되지 않습니다. SVC 클러스터는 1-4개의 어플라이언스로 구성될 수 있으며, 각 어플라이언스에는 2개의 노드가 있습니다. 어플라이언스 자체에 일련 번호가 있는 경우 해당 일련 번호는 클러스터나 노드의 일련 번호가 아닙니다.

개별 노드가 대규모 클러스터의 일부인 중간 어플라이언스/엔클로저 내에 있는 경우 스토리지 노드 객체의 "상위 일련 번호" 속성이 IBM SVC 스토리지에 맞게 채워집니다.

구성

* 필드 *	* 설명 *
--------	--------

클러스터 IP입니다	SVC 스토리지에 대한 정규화된 도메인 이름의 IP 주소입니다
자격 증명 유형을 지정하려면 '암호' 또는 'OpenSSH 키 파일'을 선택하십시오	SSH를 통해 장치에 연결하는 데 사용되는 자격 증명 유형입니다
재고 사용자 이름입니다	SVC CLI의 사용자 이름입니다
재고 암호	SVC CLI의 암호입니다
재고 개인 키에 대한 전체 경로	인벤토리 개인 키 파일의 전체 경로입니다
성능 사용자 이름입니다	성능 수집을 위한 SVC CLI의 사용자 이름입니다
성능 암호	성능 수집을 위한 SVC CLI의 암호입니다
성능 개인 키로 가는 전체 경로	성능 개인 키 파일의 전체 경로입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
장치 제외	인벤토리 수집에서 제외할 장치 ID의 심표로 구분된 목록입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 200초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
성능 제외 장치	성능 컬렉션에서 제외할 장치 ID의 심표로 구분된 목록입니다
성능 SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 200초)
덤프된 통계 파일 정리	덤프된 통계 파일을 정리하려면 선택합니다

IBM Tivoli Monitoring 데이터 소스

이 데이터 소스는 파일 시스템 사용에만 사용됩니다. Tivoli Monitoring Data Warehouse라고도 하는 Tivoli Monitoring Database와 직접 통신합니다. Oracle 및 DB2 데이터베이스가 지원됩니다.



이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

지정된 SID로 인해 연결 시도 시 "ORA-12154"가 포함된 오류 메시지가 나타나는 경우 Oracle DB 네트워크 서비스 구성을 다시 확인하십시오. 액세스 구성에서 정규화된 호스트 이름(예: "names.default_domain")을 지정하는 경우 SID 필드에 정규화된 서비스 이름을 삽입하십시오. 간단한 예로 SID에 대한 연결을 들 수 있습니다 testdb 가 실패하고 Oracle 구성이 의 도메인을 지정합니다 company.com. 연결을 시도하기 위해 기본 SID 대신 다음 문자열을 사용할 수 있습니다. testdb.company.com.

구성

필드에 입력합니다	설명
Tivoli 모니터링 데이터베이스 IP	Tivoli Monitoring 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Tivoli Monitoring 서버의 사용자 이름입니다
암호	Tivoli 모니터링 서버의 암호입니다

고급 구성

필드에 입력합니다	설명
Tivoli 모니터링 데이터베이스 포트	Tivoli 모니터링 데이터베이스에 사용되는 포트입니다
Oracle SID 또는 DB2 데이터베이스 이름입니다	Oracle 리스너 서비스 ID 또는 DB2 데이터베이스 이름입니다
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
사용할 데이터베이스 드라이버	사용할 데이터베이스 드라이버를 선택합니다
데이터베이스에 연결하는 데 사용되는 프로토콜입니다	데이터베이스에 연결하는 데 사용되는 프로토콜입니다
데이터베이스 스키마	데이터베이스 스키마를 입력합니다

IBM TotalStorage DS4000 데이터 소스

이 데이터 소스는 인벤토리 및 성능 정보를 수집합니다. 두 가지 구성(펌웨어 6.x 및 7.x+)이 있으며 두 구성 모두 동일한 값을 갖습니다. API는 볼륨 데이터 통계를 수집합니다.

구성

* 필드 *	* 설명 *
--------	--------

심표로 구분된 Array SANtricity 컨트롤러 IP 목록입니다	심표로 구분된 컨트롤러의 IP 주소 또는 정규화된 도메인 이름입니다
--	---------------------------------------

요구 사항

- 각 DS5 또는 FAStT 스토리지의 IP 주소입니다
- 액세스 검증: 각 어레이에서 두 컨트롤러의 IP 주소를 Ping(핑)합니다.

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
성능 폴링 간격(최대 3600초)	성능 폴링 간격(기본값 300초)

IBM XIV 데이터 소스

IBM XIV(CLI) 데이터 소스 인벤토리는 XIV 명령줄 인터페이스를 사용하여 수행됩니다. XIV 성능은 포트 5989에서 SMI-S 공급자를 실행하는 XIV 스토리지에 대한 SMI-S 호출을 통해 구현됩니다.

용어

OnCommand Insight는 IBM XIV 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크
스토리지 시스템	스토리지
스토리지 풀	스토리지 풀
볼륨	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 포트 요구 사항: TCP 포트 7778
- XIV 관리 인터페이스의 IP 주소입니다

- 읽기 전용 사용자 이름 및 암호
- XIV CLI는 Insight 서버 또는 RAU에 설치해야 합니다
- 액세스 검증: 사용자 이름과 암호를 사용하여 Insight 서버에서 XIV 사용자 인터페이스에 로그인합니다.

구성

* 필드 *	* 설명 *
IP 주소	XIV 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	XIV 스토리지의 사용자 이름입니다
암호	XIV 스토리지의 암호입니다
XIV CLI 디렉토리의 전체 경로입니다	XIV CLI 디렉토리의 전체 경로입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 40분)
CLI 프로세스 대기 시간 초과(ms)	CLI 프로세스 시간 초과(기본 7200000ms)
SMI-S 호스트 IP입니다	SMI-S Provider 호스트의 IP 주소입니다
SMI-S 포트	SMI-S Provider 호스트에서 사용하는 포트입니다
SMI-S 프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다
SMI-S 네임스페이스	SMI-S 네임스페이스
사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
암호	SMI-S Provider 호스트의 암호입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
SMI-S 연결 재시도 횟수	SMI-S 연결 재시도 횟수입니다

Infinidat .NET 데이터 소스

Infinidat .NET(HTTP) 데이터 소스는 Infinidat Microsoft .NET Framework 스토리지로부터 정보를 수집하는 데 사용됩니다. 따라서, 귀하는 반드시 서비스 플랫폼 관리 노드에 대한 액세스

권한이 있어야 합니다.

용어

OnCommand Insight는 다음과 같은 인벤토리 정보를 데이터 소스에서 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
상자	스토리지
노드	스토리지 노드
수영장	스토리지 풀
볼륨	볼륨
FC 포트	포트
파일 시스템	내부 볼륨
파일 시스템	파일 공유
파일 시스템 내보내기	공유



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

구성

필드에 입력합니다	설명
서비스 박스 호스트	IP 주소 또는 Management Node의 정규화된 도메인 이름입니다
사용자 이름	작업 영역 관리 노드에 대한 사용자 이름입니다
암호	작업 영역 관리 노드에 대한 암호입니다

고급 구성

필드에 입력합니다	설명
-----------	----

TCP 포트	TCP 포트 - Microsoft Windows Server에 연결하는 데 사용됩니다(기본 443).
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
연결 시간 초과	연결 시간 초과(기본값 60초)

Microsoft Azure 컴퓨팅 데이터 소스

OnCommand Insights는 Azure 컴퓨팅 데이터 수집기를 사용하여 Azure 컴퓨팅 인스턴스에서 인벤토리 및 성능 데이터를 가져옵니다.

요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 포트 요구 사항: 443 HTTPS
- Azure 관리 REST IP(management.azure.com)
- Azure 서비스 주 응용 프로그램(클라이언트) ID(사용자 계정)
- Azure Service Principal Authentication 키(사용자 암호)

Insight 검색을 위해 Azure 계정을 설정해야 합니다. 계정이 올바르게 구성되고 Azure에 애플리케이션을 등록하면 Insight에서 Azure 인스턴스를 검색하는 데 필요한 자격 증명이 제공됩니다. 다음 링크에서는 검색을 위해 계정을 설정하는 방법에 대해 설명합니다. <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

구성

아래 표에 따라 데이터 원본 필드에 데이터를 입력합니다.

필드에 입력합니다	설명
Azure 서비스 주 응용 프로그램(클라이언트) ID(리더 역할 필요)	Azure에 로그인 ID를 입력합니다. 리더 역할 액세스가 필요합니다.
Azure 테넌트 ID입니다	Microsoft 테넌트 ID입니다
Azure 서비스 주 인증 키	로그인 인증 키
API 요청에 대한 Microsoft의 청구서를 알고 있습니다	Insight 폴링을 통해 API 요청이 접수된다는 사실을 알고 있는지 확인하려면 이 확인란을 선택하십시오.

고급 구성

아래 표에 따라 데이터 원본 필드에 데이터를 입력합니다.

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60입니다
태그별로 VM 필터링에 적용하려면 '제외' 또는 '포함'을 선택합니다	데이터를 수집할 때 태그별로 VM을 포함할지 제외할지 여부를 지정합니다. "포함"을 선택하면 태그 키 필드를 비워둘 수 없습니다.
태그 키 및 VM을 필터링할 값	VM의 키 및 태그 값과 일치하는 키 및 값을 필터링하여 포함/제외할 VM(및 관련 디스크)을 선택하려면 * + 필터 태그 * 를 클릭합니다. 태그 키는 필수이며 태그 값은 선택 사항입니다. 태그 값이 비어 있으면 태그 키와 일치하는 한 VM이 필터링됩니다.
성능 폴링 간격(초)	

Azure NetApp Files 데이터 소스

이 데이터 소스는 ANF(Azure NetApp Files)에 대한 인벤토리 및 성능 데이터를 가져옵니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- 포트 요구 사항: 443 HTTPS
- Azure 관리 REST IP(management.azure.com)
- Azure 서비스 주 응용 프로그램(클라이언트) ID(사용자 계정)
- Azure Service Principal 인증 키(사용자 암호)
- Cloud Insights 검색을 위해 Azure 계정을 설정해야 합니다.

계정이 올바르게 구성되고 Azure에 애플리케이션을 등록하면 Cloud Insights로 Azure 인스턴스를 검색하는 데 필요한 자격 증명이 제공됩니다. 다음 링크에서는 검색을 위해 계정을 설정하는 방법에 대해 설명합니다.

<https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

구성

필드에 입력합니다	설명
Azure 서비스 주 응용 프로그램(클라이언트) ID입니다	Azure에 로그인 ID를 입력합니다
Azure 테넌트 ID입니다	Azure 테넌트 ID입니다
Azure 서비스 주 인증 키	로그인 인증 키

API 요청에 대한 Microsoft의 청구서를 알고 있습니다	Insight 폴링을 통해 API 요청이 접수된다는 사실을 알고 있는지 확인하려면 이 확인란을 선택하십시오.
------------------------------------	--

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다

Microsoft Hyper-V 데이터 소스

구성의 경우 Microsoft Hyper-V 데이터 원본에는 물리적 호스트(하이퍼바이저)의 IP 주소 또는 확인 가능한 DNS 이름이 필요합니다. 이 데이터 소스는 Powershell(이전에 사용한 WMI)을 사용합니다.

용어

OnCommand Insight는 Hyper-V 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
가상 하드 디스크	가상 디스크
호스트	호스트
가상 머신	가상 머신
CSV(Cluster Shared Volumes), 파티션 볼륨	데이터 저장소
인터넷 SCSI 장치, 다중 경로 SCSI LUN	LUN을 클릭합니다
Fibre Channel 포트	포트



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Hyper-V를 사용하려면 데이터 수집 및 원격 액세스/관리를 위해 포트 5985를 열어야 합니다.
- 클러스터링 그룹 노드의 IP 주소입니다
- 하이퍼바이저의 로컬 관리자 사용자 및 암호
- 관리 수준 사용자 계정

- 포트 요구 사항: Windows 2003 및 이전 버전의 경우 포트 135 및 동적 TCP 포트 1024-65535와 Windows 2008의 경우 49152-65535가 할당됩니다.
- 데이터 수집기가 IP 주소만 가리키는 경우에도 DNS 확인이 성공해야 합니다.
- 각 Hyper-V 하이퍼바이저에는 모든 호스트의 모든 VM에 대해 "리소스 계측"이 켜져 있어야 합니다. 따라서 각 하이퍼바이저마다 각 게스트에서 Cloud Insights에 사용할 수 있는 데이터가 더 많아집니다. 이 옵션을 설정하지 않으면 각 게스트에 대해 더 적은 성능 메트릭이 획득됩니다. 리소스 측정에 대한 자세한 내용은 Microsoft 설명서를 참조하십시오.

"Hyper-V 리소스 측정 개요"

"활성화 - VMResourceMetering"

구성

* 필드 *	* 설명 *
물리적 호스트 IP 주소입니다	물리적 호스트(하이퍼바이저)의 IP 주소 또는 정규화된 도메인 이름
사용자 이름	관리자 사용자 이름은 하이퍼바이저를 수행합니다
암호	하이퍼바이저의 암호입니다
NT 도메인	클러스터의 노드에서 사용하는 DNS 이름입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(ms)	연결 시간 초과(기본값 60000ms)

NetApp clustered Data ONTAP 데이터 소스

이 데이터 소스는 clustered Data ONTAP을 사용하는 스토리지 시스템에 사용해야 하며 읽기 전용 API 호출에 사용되는 관리자 계정이 필요합니다.

용어

OnCommand Insight는 clustered Data ONTAP 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
------------	---------------

디스크	디스크
RAID 그룹	디스크 그룹
클러스터	스토리지
노드	스토리지 노드
집계	스토리지 풀
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 읽기 전용 API 호출에 사용되는 관리자 계정입니다
- 타겟 IP는 클러스터 관리 LIF입니다
- NetApp 클러스터에 로그인할 수 있는 사용자 이름(읽기 전용 역할 이름을 ontapi 애플리케이션에 기본 SVM으로 지정) 및 암호
- 포트 요구 사항: 80 또는 443
- 라이선스 요구사항: 검색에 필요한 FCP 라이선스 및 매핑/마스킹된 볼륨

구성

* 필드 *	* 설명 *
NetApp 관리 IP	NetApp 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	NetApp 클러스터의 사용자 이름입니다
암호	NetApp 클러스터의 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)

성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)
-------------	--------------------

Clustered Data ONTAP 스토리지

NetApp clustered Data ONTAP 스토리지 자산 랜딩 페이지에서 오브젝트 또는 레퍼런스에 적용되는 용어입니다.

Clustered Data ONTAP 스토리지 용어

다음 용어는 NetApp clustered Data ONTAP 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 모델 — 이 클러스터 내에서 고유한 개별 노드 모델 이름을 심표로 구분한 목록입니다. 클러스터의 모든 노드가 동일한 모델 유형인 경우 하나의 모델 이름만 표시됩니다.
- 공급업체 — 새 데이터 원본을 구성하는 경우 동일한 공급업체 이름입니다.
- 일련 번호 — 스토리지 일련 번호입니다. NetApp clustered Data ONTAP과 같은 클러스터 아키텍처 스토리지 시스템에서는 이 일련 번호가 개별 "스토리지 노드" 일련 번호보다 덜 유용할 수 있습니다.
- IP — 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다.
- 마이크로코드 버전 — 펌웨어.
- Raw Capacity - - 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2개의 합계입니다.
- 지연 시간 — 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. 이상적으로는 OCI가 이 가치를 직접 소싱하지만 이 아닌 경우가 많습니다. 이러한 업적을 제공하는 스토리지 대신, OCI는 일반적으로 개별 내부 볼륨 "" 통계에서 파생된 IOP 가중 계산을 수행합니다.
- Throughput - 내부 볼륨에서 집계된 것입니다.
- 관리 — 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Insight 데이터 소스에 의해 프로그래밍 방식으로 만들어집니다.

Clustered Data ONTAP 스토리지 풀

NetApp clustered Data ONTAP 스토리지 풀 자산 랜딩 페이지에서 오브젝트 또는 레퍼런스에 적용되는 용어입니다.

Clustered Data ONTAP 스토리지 풀 용어

다음 용어는 NetApp clustered Data ONTAP 스토리지 풀 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 풀이 상주하는 스토리지 배열입니다. 필수입니다.
- 형식 — 가능성 목록 목록의 설명 값입니다. 가장 흔히 "집계" 또는 "RAID 그룹"이 됩니다.
- 노드 — 이 스토리지 시스템의 아키텍처가 특정 스토리지 노드에 속해 있는 경우 이 스토리지 시스템의 이름은 해당 랜딩 페이지의 하이퍼링크로 표시됩니다.
- Flash Pool 사용 — 예/아니요 가치 — 이 SATA/SAS 기반 풀에 캐싱 가속화에 SSD가 사용됩니까?
- 중복 — RAID 레벨 또는 보호 체계입니다. RAID_DP는 이중 패리티이고, RAID_TP는 삼중 패리티입니다.

- 용량 — 이 값은 사용된 논리적 용량, 가용 용량 및 총 논리적 용량 및 이 용량 전체에서 사용된 비율입니다.
- 과도하게 커밋된 용량 — 효율성 기술을 사용하여 스토리지 풀의 논리적 용량보다 큰 볼륨 또는 내부 볼륨 용량의 합계를 할당한 경우 여기에 있는 백분율 값은 0%보다 큼니다.
- 스냅샷 — 사용 중인 스냅샷 용량 및 총 용량. 스토리지 풀 아키텍처가 용량의 일부를 스냅샷용 영역으로 세그먼트하는 경우 MetroCluster 구성의 ONTAP은 이 문제를 나타낼 가능성이 높지만, 다른 ONTAP 구성은 더 적습니다.
- Utilization — 이 스토리지 풀에 용량을 제공하는 모든 디스크의 사용 중 가장 높은 비율을 나타내는 백분율입니다. 디스크 사용률이 반드시 스토리지 성능과 강력한 상관 관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 재구성, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지 "" 복제 구현으로 인해 내부 볼륨 또는 볼륨 작업 부하로 표시되지 않는 동안 디스크 사용률이 발생할 수 있습니다.
- IOPS — 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다.
- Throughput - - 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다.

Clustered Data ONTAP 스토리지 노드

NetApp clustered Data ONTAP 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

Clustered Data ONTAP 스토리지 노드 용어

다음 용어는 NetApp clustered Data ONTAP 스토리지 풀 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 노드가 속하는 스토리지 시스템입니다. 필수입니다.
- HA 파트너 — 노드가 1개 노드로 페일오버되고 다른 1개 노드만 장애 조치되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다.
- State — 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다.
- 모델 — 노드의 모델 이름입니다.
- Version — 디바이스의 버전 이름입니다.
- 일련 번호 — 노드 일련 번호입니다.
- 메모리 — 베이스 2 메모리(있는 경우)
- 활용률 — ONTAP에서 이것은 독점 알고리즘의 컨트롤러 스트레스 인덱스입니다. 성능 폴링이 발생할 때마다 WAFL 디스크 경합 또는 평균 CPU 사용률의 증가인 0에서 100% 사이의 숫자가 보고됩니다. 값이 50%를 초과하는 경우 이는 낮은 크기 조정을 나타내는 것입니다. 컨트롤러/노드가 충분히 크지 않거나 회전 디스크가 부족하여 쓰기 워크로드를 흡수할 수 없습니다.
- IOPS — 노드 개체에 대해 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 지연 시간 — 노드 개체에 대해 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 처리량 — 노드 개체에서 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 프로세서 — CPU 수입니다.

Unified Manager 데이터 소스를 위한 NetApp clustered Data ONTAP

이 데이터 소스는 UM(Unified Manager) 6.0+ 데이터베이스에서 ONTAP 8.1.x 데이터를 수집합니다. Insight는 이 데이터 소스를 사용하여 UM에서 구성 및 채워진 모든 클러스터를 검색합니다. 효율성을 위해 Insight는 클러스터 자체의 ZAPI를 호출하지 않습니다. 이 데이터 원본에서는 성능이 지원되지 않습니다.

구성



이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

* 필드 *	* 설명 *
Unified Manager IP를 참조하십시오	Unified Manager의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Unified Manager의 사용자 이름입니다
암호	Unified Manager의 암호입니다
포트	Unified Manager와의 통신에 사용되는 포트(기본값 3306)

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
클러스터 제외	제외할 클러스터 IP의 심표로 구분된 목록입니다

7-Mode 데이터 소스에서 작동하는 NetApp Data ONTAP

7-Mode에서 작동하는 Data ONTAP 소프트웨어를 사용하는 스토리지 시스템의 경우, 용량 번호를 얻기 위해 CLI를 사용하는 ONTAPI 데이터 소스를 사용해야 합니다.

용어

OnCommand Insight는 NetApp Data ONTAP 7-Mode 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크	디스크

RAID 그룹	디스크 그룹
파일러	스토리지
파일러	스토리지 노드
집계	스토리지 풀
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- FAS 스토리지 컨트롤러 및 파트너의 IP 주소입니다
- 포트 443
- 컨트롤러 및 파트너의 사용자 이름 및 암호
- 7-Mode에서 다음 역할 기능을 지원하는 컨트롤러 및 파트너 컨트롤러에 대한 사용자 지정 관리자 레벨 사용자 이름 및 암호:
 - "API- *": OnCommand Insight에서 모든 NetApp 스토리지 API 명령을 실행할 수 있도록 허용합니다.
 - "login-http-admin": OnCommand Insight이 HTTP를 통해 NetApp 스토리지에 연결할 수 있도록 허용하려면 이 옵션을 사용하십시오.
 - "security-api-vFiler": OnCommand Insight가 NetApp 스토리지 API 명령을 실행하여 vFiler 유닛 정보를 검색할 수 있도록 합니다.
 - "CLI-options": 스토리지 시스템 옵션을 읽으려면 이 옵션을 사용합니다.
 - "CLI-LUN": LUN 관리를 위한 다음 명령에 액세스합니다. 지정된 LUN 또는 LUN 클래스의 상태(LUN 경로, 크기, 온라인/오프라인 상태 및 공유 상태)를 표시합니다.
 - "CLI-df": 사용 가능한 디스크 공간을 표시하려면 이 옵션을 사용합니다.
 - "CLI-ifconfig": 인터페이스 및 IP 주소를 표시하려면 이 옵션을 사용합니다.

구성

* 필드 *	* 설명 *
파일러 주소	NetApp Filer의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	NetApp Filer의 사용자 이름입니다
암호	NetApp Filer 암호

클러스터에 있는 HA 파트너 파일러의 주소입니다	HA 파트너 파일러의 IP 주소 또는 정규화된 도메인 이름입니다
클러스터에 있는 HA 파트너 파일러의 사용자 이름입니다	NetApp HA 파트너 파일러의 사용자 이름입니다
클러스터에 있는 HA 파트너 파일러의 암호	NetApp HA 파트너 파일러의 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 유형	연결 유형을 선택합니다
연결 포트	NetApp API에 사용되는 포트입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

스토리지 시스템 접속입니다

이 데이터 원본에 대한 기본 관리 사용자를 사용하는 대신 NetApp 스토리지 시스템에서 직접 관리 권한을 가진 사용자를 구성하여 데이터 원본이 NetApp 스토리지 시스템에서 데이터를 가져올 수 있도록 할 수 있습니다.

NetApp 스토리지 시스템에 연결하려면 스토리지 시스템이 있는 기본 pfiler를 획득할 때 지정된 사용자가 다음 조건을 충족해야 합니다.

- 사용자는 vfiler0(루트 파일러/pfiler)에 있어야 합니다.

스토리지 시스템은 기본 pfiler를 획득할 때 획득됩니다.

- 다음 명령은 사용자 역할 기능을 정의합니다.
 - "API- *": OnCommand Insight에서 모든 NetApp 스토리지 API 명령을 실행할 수 있도록 허용합니다. ZAPI를 사용하려면 이 명령이 필요합니다.
 - "login-http-admin": OnCommand Insight이 HTTP를 통해 NetApp 스토리지에 연결할 수 있도록 허용하려면 이 옵션을 사용하십시오. ZAPI를 사용하려면 이 명령이 필요합니다.
 - "security-api-vFiler": OnCommand Insight가 NetApp 스토리지 API 명령을 실행하여 vFiler 유닛 정보를 검색할 수 있도록 합니다.
 - "CLI-options": "options" 명령에 대해 사용되며 파트너 IP 및 활성화된 라이선스에 사용됩니다.
 - "CLI-LUN": LUN 관리를 위해 다음 명령을 사용합니다. 지정된 LUN 또는 LUN 클래스의 상태(LUN 경로, 크기, 온라인/오프라인 상태 및 공유 상태)를 표시합니다.
 - "CLI-df": "df-s", "df-r", "df-a-r" 명령의 경우 및 사용 가능한 공간을 표시하는 데 사용됩니다.
 - "CLI-ifconfig": "ifconfig -a" 명령용이며 파일러 IP 주소를 가져오는 데 사용됩니다.
 - "CLI-rdfile": "rdfile /etc/netgroup" 명령에 대해, 넷그룹을 가져오는 데 사용됩니다.

- "CLI-date": "date" 명령을 기준으로, 스냅샷 복사본을 얻기 위한 전체 날짜를 얻는 데 사용됩니다.
- "CLI-snap": "snap list" 명령에 사용되며 스냅샷 복사본을 가져오는 데 사용됩니다.

CLI-date 또는 CLI-snap 권한이 제공되지 않는 경우, 획득이 완료될 수 있지만 스냅샷 복사본은 보고되지 않습니다.

7-Mode 데이터 소스를 성공적으로 획득하고 스토리지 시스템에 경고가 표시되지 않도록 하려면 다음 명령 문자열 중 하나를 사용하여 사용자 역할을 정의해야 합니다. 여기에 나열된 두 번째 문자열은 첫 번째 문자열의 간소화된 버전입니다.

```
login-http-admin,api-*,security-api-vfile,cli-rdfile,cli-options,cli-  
df,cli-lun,cli-ifconfig,cli-date,cli-snap,  
or  
login-http-admin,api-*,security-api-vfile,cli-*
```

NetApp E-Series 데이터 소스

NetApp E-Series 데이터 소스에서 인벤토리 및 성능 정보를 수집합니다. 두 가지 구성(펌웨어 6.x 및 펌웨어 7.x+)이 있으며 두 구성 모두 동일한 값을 갖습니다.

용어

OnCommand Insight는 NetApp E-Series 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
볼륨 그룹	디스크 그룹
스토리지	스토리지
컨트롤러	스토리지 노드
볼륨 그룹	스토리지 풀
볼륨	볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 어레이에 있는 각 컨트롤러의 IP 주소입니다

- 포트 요구 사항 2463

구성

* 필드 *	* 설명 *
임의로 구분된 Array SANtricity 컨트롤러 IP 목록입니다	스토리지 컨트롤러의 IP 주소 및/또는 정규화된 도메인 이름입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 30분)
성능 폴링 간격(최대 3600초)	성능 폴링 간격(기본값 300초)

E-Series 스토리지

NetApp E-Series 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

E-Series 스토리지 용어

다음 용어는 NetApp E-Series 스토리지 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조 자료에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 모델 — 장치의 모델 이름입니다.
- 공급업체 — 새 데이터 원본을 구성하는 경우 동일한 공급업체 이름입니다.
- 일련 번호 — 스토리지 일련 번호입니다. NetApp clustered Data ONTAP과 같은 클러스터 아키텍처 스토리지 시스템에서는 이 일련 번호가 개별 "스토리지 노드" 일련 번호보다 덜 유용할 수 있습니다.
- IP — 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다.
- 마이크로코드 버전 — 펌웨어.
- Raw Capacity - - 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2개의 합계입니다.
- 지연 시간 — 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. Insight는 스토리지의 볼륨에서 파생된 IOPS 가중 평균을 계산합니다.
- Throughput — 스토리지의 총 호스트 처리량입니다. Insight는 이 값을 도출하기 위해 볼륨 "의 처리량을 합산합니다.
- 관리 — 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Insight 데이터 소스에 의해 프로그래밍 방식으로 만들어집니다.

E-Series 스토리지 풀

NetApp E-Series 스토리지 풀 자산 랜딩 페이지에서 확인할 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

E-Series 스토리지 풀 용어

다음 용어는 NetApp E-Series 스토리지 풀 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조 자료에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 풀이 상주하는 스토리지 배열입니다. 필수입니다.
- 형식 — 가능성 목록 목록의 설명 값입니다. 가장 일반적인 것은 "썸 프로비저닝" 또는 "RAID 그룹"입니다.
- 노드 — 이 스토리지 시스템의 아키텍처가 특정 스토리지 노드에 속해 있는 경우 이 스토리지 시스템의 이름은 해당 랜딩 페이지의 하이퍼링크로 표시됩니다.
- Flash Pool 사용 — 예/아니요 값
- 중복 — RAID 레벨 또는 보호 체계입니다. DDP 풀에 대한 E-Series의 보고서 "RAID 7".
- 용량 — 이 값은 사용된 논리적 용량, 가용 용량 및 총 논리적 용량 및 이 용량 전체에서 사용된 비율입니다. 이러한 값에는 E-Series의 "보존" 용량이 모두 포함되어 있어 E-Series의 사용자 인터페이스에서 표시할 수 있는 용량보다 숫자 및 백분율이 높습니다.
- 과도하게 커밋된 용량 — 효율성 기술을 사용하여 스토리지 풀의 논리적 용량보다 큰 총 볼륨 용량을 할당한 경우 여기에 있는 백분율 값은 0%보다 큼니다.
- 스냅샷 — 사용 중인 스냅샷 용량 및 총 용량. 스토리지 풀 아키텍처가 용량의 일부를 스냅샷용 영역으로 세그먼트하는 경우
- Utilization — 이 스토리지 풀에 용량을 제공하는 디스크 사용량이 가장 높은 비율을 나타내는 백분율입니다. 디스크 사용률이 반드시 스토리지 성능과 강력한 상관관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 리빌드, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지 "" 복제 구현으로 인해 볼륨 작업 부하로 표시되지 않는 동안 디스크 사용률이 발생할 수 있습니다.
- IOPS — 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다.
- Throughput - - 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다.

E-Series 스토리지 노드

NetApp E-Series 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용되는 용어입니다.

E-Series 스토리지 노드 용어

다음 용어는 NetApp E-Series 스토리지 풀 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조 자료에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 스토리지 — 이 노드가 속하는 스토리지 시스템입니다. 필수입니다.
- HA 파트너 — 노드가 1개 노드로 페일오버되고 다른 1개 노드만 장애 조치되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다.
- State — 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다.
- 모델 — 노드의 모델 이름입니다.
- Version — 디바이스의 버전 이름입니다.
- 일련 번호 — 노드 일련 번호입니다.
- 메모리 — 베이스 2 메모리(있는 경우)

- Utilization — 현재 NetApp E-Series에서 사용할 수 없습니다.
- IOPS — 이 노드에만 속하는 볼륨의 모든 IOP를 합산하여 계산됩니다.
- 지연 시간 — 이 컨트롤러의 일반적인 호스트 지연 시간 또는 응답 시간을 나타내는 숫자입니다. Insights는 이 노드에만 속하는 볼륨에서 IOPS 가중 평균을 계산합니다.
- 처리량 — 이 컨트롤러의 호스트 기반 처리량을 나타내는 숫자입니다. 이 노드에만 속하는 볼륨에 대한 모든 처리량을 합산하여 계산됩니다.
- 프로세서 — CPU 수입니다.

NetApp 호스트 및 VM 파일 시스템 데이터 소스

NetApp 호스트 및 VM 파일 시스템 데이터 소스를 사용하여 모든 Microsoft Windows 호스트 및 VM(가상 머신) 파일 시스템과 지원되는 모든 Linux VM(가상 매핑된 것에만 해당)에 대한 파일 시스템 세부 정보 및 스토리지 리소스 매핑을 검색할 수 있습니다. 구성된 CRG(Compute Resource Group)로 주석이 추가된 Insight 서버의 기존

일반 요구 사항

- 이 기능은 별도로 구입해야 합니다.

도움이 필요하면 Insight 담당자에게 문의하십시오.

- Insight Support Matrix를 확인하여 호스트 또는 가상 머신 운영 체제가 지원되는지 확인해야 합니다.

파일 시스템에서 스토리지 리소스로의 링크가 생성되었는지 확인하려면 관련 스토리지 또는 가상화 공급업체 유형 및 버전이 필요한 볼륨 또는 가상 디스크 식별 데이터를 보고하는지 확인하십시오.

Microsoft Windows 요구 사항

- 이 데이터 소스는 WMI(Window Management Instrumentation) 데이터 구조를 사용하여 데이터를 검색합니다.

이 서비스는 원격으로 작동하고 사용 가능해야 합니다. 특히, 포트 135에 액세스할 수 있어야 하며 방화벽 뒤에 있는 경우 열어야 합니다.

- Windows 도메인 사용자는 WMI 구조에 액세스할 수 있는 적절한 권한이 있어야 합니다.
- 관리자 권한이 필요합니다.
- Windows 2003 및 이전 버전에서 1024-65535로 할당된 동적 TCP 포트
- Windows 2008의 경우 포트 49152 - 65535



일반적으로 Insight, AU 및 이 데이터 소스 간에 방화벽을 사용하려고 할 때 Microsoft 팀에 문의하여 필요한 포트를 확인해야 합니다.

Linux 요구 사항

- 이 데이터 소스는 SSH(Secure Shell) 연결을 사용하여 Linux VM에서 명령을 실행합니다.

SSH 서비스가 운영되어야 하며 원격으로 이용할 수 있어야 합니다. 특히, 포트 22에 액세스할 수 있어야 하며 방화벽 뒤에 있는 경우 열어야 합니다.

- SSH 사용자는 sudo 권한이 있어야 Linux VM에서 읽기 전용 명령을 실행할 수 있습니다.

동일한 암호를 사용하여 SSH에 로그인하고 sudo 암호 챌린지에 응답해야 합니다.

사용 권장 사항

- 동일한 Compute Resource Group 주석을 사용하여 공통 운영 체제 자격 증명이 있는 호스트 및 가상 시스템 그룹에 주석을 추가해야 합니다.

각 그룹에는 이러한 호스트 및 가상 시스템에서 파일 시스템 세부 정보를 검색하는 이 데이터 소스의 인스턴스가 있습니다.

- 성공률이 낮은 이 데이터 소스의 인스턴스가 있는 경우(예: OnCommand Insight가 그룹에 있는 1000개의 호스트 및 가상 머신 중 50개에 대한 파일 시스템 세부 정보를 검색하는 경우), 검색이 성공한 호스트와 가상 머신을 별도의 컴퓨팅 리소스 그룹으로 이동해야 합니다.

구성

필드에 입력합니다	설명
사용자 이름	운영 체제 사용자 Windows 운영 체제 사용자의 파일 시스템 데이터를 검색할 수 있는 적절한 권한이 있어야 합니다. 여기에는 도메인 접두사가 포함되어야 합니다.
암호	운영 체제 사용자의 암호입니다
컴퓨팅 리소스 그룹	데이터 소스에 대한 호스트 및 가상 머신에 플래그를 지정하는 데 사용되는 주석 값은 파일 시스템을 검색합니다. 빈 값은 데이터 소스가 현재 Compute Resource Group(계산 리소스 그룹)으로 주석이 추가되지 않은 모든 호스트 및 가상 시스템에 대한 파일 시스템을 검색함을 나타냅니다.

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값 360분)

NetApp SolidFire 데이터 소스

NetApp SolidFire 데이터 소스는 인벤토리 및 성능 수집을 위해 iSCSI와 파이버 채널 SolidFire 구성을 모두 지원합니다.

SolidFire 데이터 소스는 SolidFire REST API를 사용합니다. 데이터 소스가 상주하는 획득 장치에서는 SolidFire 클러스터 관리 IP 주소의 TCP 포트 443에 대한 HTTPS 연결을 시작할 수 있어야 합니다. 데이터 원본에는 SolidFire 클러스터에서 REST API 쿼리를 수행할 수 있는 자격 증명이 필요합니다.

용어

OnCommand Insight는 NetApp SolidFire 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
볼륨	볼륨
Fibre Channel 포트	포트
볼륨 액세스 그룹, LUN 할당	볼륨 맵
iSCSI 세션	볼륨 마스크



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- 관리 가상 IP 주소
- 포트 443

구성

필드에 입력합니다	설명
관리 가상 IP 주소(MVIP)	SolidFire 클러스터의 관리 가상 IP 주소입니다
사용자 이름	SolidFire 클러스터에 로그인하는 데 사용되는 이름입니다
암호	SolidFire 클러스터에 로그인하는 데 사용되는 암호입니다

고급 구성

필드에 입력합니다	설명
-----------	----

재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
TCP 포트	SolidFire 서버에 연결하는 데 사용되는 TCP 포트(기본값 443)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

문제 해결

SolidFire에서 오류를 보고하면 다음과 같이 OnCommand Insight에 표시됩니다.

```
An error message was received from a SolidFire device while trying to retrieve data. The call was <method> (<parameterString> ). The error message from the device was (check the device manual): <message>
```

여기서,

- 메소드>는 GET 또는 PUT와 같은 HTTP 메소드입니다.
- parameterString>은 REST 호출에 포함된 심표로 구분된 매개 변수 목록입니다.
- message>는 오류 메시지로 반환된 장치와 상관없이 표시됩니다.

NetApp StorageGRID 데이터 소스

이 데이터 소스는 StorageGRID에 대한 인벤토리 및 성능 데이터를 수집합니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- StorageGRID 호스트 IP 주소입니다
- 메트릭 쿼리 및 테넌트 액세스 역할이 할당된 사용자의 사용자 이름 및 암호입니다
- 포트 443

구성

필드에 입력합니다	설명
StorageGRID 호스트 IP 주소(MVIP)	StorageGRID의 호스트 IP 주소입니다
사용자 이름	StorageGRID에 로그인하는 데 사용되는 이름입니다
암호	StorageGRID에 로그인하는 데 사용되는 암호입니다

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 900초)

OpenStack 데이터 소스

OpenStack(REST API/KVM) 데이터 소스에서 OpenStack 하드웨어 인스턴스에 대한 정보를 수집합니다. 이 데이터 소스는 모든 OpenStack 인스턴스에 대한 인벤토리 데이터를 수집하고 선택적으로 VM 성능 데이터를 수집합니다.

요구 사항

다음은 OpenStack 데이터 소스를 구성하기 위한 요구사항입니다.

- OpenStack 컨트롤러의 IP 주소입니다
- OpenStack 관리자 역할 자격 증명 및 Linux KVM 하이퍼바이저에 대한 sudo 액세스를 권장합니다.



admin 계정 또는 admin에 상응하는 권한을 사용하지 않는 경우에도 데이터 소스에서 데이터를 획득할 수 있습니다. admin 역할이 아닌 사용자가 API를 호출할 수 있도록 정책 구성 파일(예: `etc/nova/policy.json`)을 수정해야 합니다.

- "OS_컴퓨팅_API:OS-가용성-영역:세부 정보:"
- "OS_컴퓨팅_API:OS-하이퍼바이저:"
- OS_컴퓨팅_API:서버:세부 정보:get_all_tenant":""
- 성능 수집을 위해 OpenStack Ceilometer 모듈을 설치하고 구성해야 합니다. Ceilometer 구성은 를 편집하여 수행할 수 있습니다 `nova.conf` 각 하이퍼바이저에 대해 파일을 생성한 다음 각 하이퍼바이저에서 Nova 컴퓨팅 서비스를 다시 시작합니다. 옵션 이름이 OpenStack의 다양한 릴리즈에서 변경되었습니다.
 - 아이스하우스
 - 준오
 - 킬로
 - 리버티
 - 미타카
 - 뉴턴
 - 옥타
- CPU 통계의 경우 컴퓨팅 노드의 `/etc/nova/nova.conf`에서 "compute_monitor=ComputeDriverCPUMonitor"를 켜야 합니다.
- 포트 요구 사항:
 - http의 경우 5000, Keystone 서비스의 경우 13000

- 22 KVM SSH의 경우
- Nova 컴퓨팅 서비스: 8774
- 8776을 참조하십시오
- Ceilometer 성능 서비스용 8777
- Glance 이미지 서비스를 위한 9292



포트는 특정 서비스에 바인딩되며, 대규모 환경의 컨트롤러 또는 다른 호스트에서 서비스가 실행될 수 있습니다.

구성

* 필드 *	* 설명 *
OpenStack 컨트롤러 IP 주소입니다	OpenStack 컨트롤러의 IP 주소 또는 정규화된 도메인 이름입니다
OpenStack 관리자	OpenStack 관리자의 사용자 이름입니다
OpenStack 암호	OpenStack Admin에 사용되는 암호입니다
OpenStack 관리자 테넌트	OpenStack 관리자 테넌트
KVM Sudo 사용자	KVM Sudo 사용자 이름입니다
자격 증명 유형을 지정하려면 '암호' 또는 'OpenSSH 키 파일'을 선택하십시오	SSH를 통해 장치에 연결하는 데 사용되는 자격 증명 유형입니다
재고 개인 키에 대한 전체 경로	재고 개인 키에 대한 전체 경로
KVM Sudo 암호	KVM Sudo 암호

고급 구성

* 필드 *	* 설명 *
SSH를 통해 하이퍼바이저 인벤토리 검색을 설정합니다	SSH를 통해 하이퍼바이저 인벤토리 검색을 설정하려면 이 확인란을 선택합니다
OpenStack 관리 URL 포트입니다	OpenStack 관리 URL 포트입니다
HTTPS를 사용합니다	보안 HTTP를 사용하려면 선택합니다
HTTP 연결 시간 초과(초)	HTTP 연결 시간 초과(기본값 300초)

SSH 포트	SSH에 사용되는 포트입니다
SSH 프로세스 대기 시간 초과(초)	SSH 프로세스 시간 초과(기본값 30초)
SSH 프로세스 재시도	인벤토리 재시도 횟수입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)

Oracle ZFS 데이터 소스

Oracle ZFS 데이터 소스는 인벤토리 및 성능 수집을 지원합니다.

용어

OnCommand Insight는 이 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
디스크(SDD)	디스크
클러스터	스토리지
컨트롤러	스토리지 노드
LUN을 클릭합니다	볼륨
LUN 매핑	볼륨 맵
초기자, 대상	볼륨 마스크
공유	내부 볼륨



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

다음은 이 데이터 소스를 구성하기 위한 요구 사항입니다.

- ZFS Controller-1 및 ZFS Controller-2의 호스트 이름
- 관리자 사용자 이름 및 자격 증명
- 포트 요구 사항: 215 HTTP/HTTPS

구성

ZFS Controller-1 호스트 이름	스토리지 컨트롤러 1의 호스트 이름입니다
ZFS Controller-2 호스트 이름	스토리지 컨트롤러의 호스트 이름 2
사용자 이름입니다	스토리지 시스템 관리자 사용자 계정의 사용자 이름입니다
암호	관리자 사용자 계정의 암호입니다

고급 구성

필드에 입력합니다	설명
TCP 포트	ZFS에 연결하는 데 사용되는 TCP 포트(기본값 215)
연결 유형	HTTP 또는 HTTPS
인벤토리 폴링 간격입니다	인벤토리 폴링 간격(기본값: 60분)
연결 시간 초과	기본값은 60초입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

문제:	다음을 시도해 보십시오.
"잘못된 로그인 자격 증명"	ZFS 사용자 계정 및 암호를 확인합니다
"구성 오류" 및 "reST 서비스가 비활성화되었습니다" 오류 메시지	이 장치에서 REST 서비스가 활성화되어 있는지 확인합니다.

"구성 오류" 및 "명령에 대한 권한이 없는 사용자" 오류 메시지	<p>특정 역할(예: 'advanced_analytics')이 구성된 사용자 <userName>에 포함되지 않을 수 있습니다. 가능한 해결 방법:</p> <ul style="list-style-type: none"> 읽기 전용 역할을 사용하여 \${user} 사용자의 분석 (통계) 범위를 수정하십시오. - 구성 → 사용자 화면에서 마우스를 역할 위에 놓고 두 번 클릭하여 편집할 수 있습니다 범위 드롭다운 메뉴에서 "분석"을 선택합니다. 가능한 속성 목록이 나타납니다. 맨 위 확인란을 클릭하면 세 가지 속성이 모두 선택됩니다. - 오른쪽에 있는 추가 단추를 클릭합니다. 팝업 창의 오른쪽 위에 있는 적용 단추를 클릭합니다. 팝업 창이 닫힙니다.
--------------------------------------	--

Pure Storage FlashArray 데이터 소스

Pure Storage FlashArray(HTTP) 데이터 소스는 Pure Storage Flash Array로부터 정보를 수집하는 데 사용됩니다. Insight는 인벤토리 및 성능 수집을 모두 지원합니다.

용어

OnCommand Insight는 Pure Storage FlashArray 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
드라이브(SSD)	디스크
스토리지	스토리지
컨트롤러	스토리지 노드
볼륨	볼륨
포트	포트
LUN 맵(호스트, 호스트 그룹, 타겟 포트)	볼륨 맵, 볼륨 마스크



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지 시스템 IP 주소입니다

- Pure 스토리지 시스템의 관리자 계정에 대한 사용자 이름 및 암호입니다.
- 포트 요구 사항: HTTP/HTTPS 80/443

구성

* 필드 *	* 설명 *
FlashArray 호스트	FlashArray Management Server의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	FlashArray 관리 서버의 사용자 이름입니다
암호	FlashArray Management Server의 암호입니다

고급 구성

* 필드 *	* 설명 *
연결 유형	관리 서버
TCP 포트	FlashArray 서버에 연결하는 데 사용되는 TCP 포트 (기본값 443)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
재고 폴링 간격(분)	재고 조사 간격(기본값: 60분)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

QLogic FC 스위치 데이터 소스

구성의 경우, QLogic FC 스위치(SNMP) 데이터 소스에는 IP 주소로 지정된 FC 스위치 장치의 네트워크 주소와 장치에 액세스하는 데 사용되는 SNMP_READ-OVERY_COLANCE 문자열이 필요합니다.

구성

* 필드 *	* 설명 *
SANsurfer 스위치	SANsurfer 스위치의 IP 주소 또는 정규화된 도메인 이름입니다
SNMP 버전입니다	SNMP 버전입니다
SNMP 커뮤니티	SNMP 커뮤니티 문자열

사용자 이름	SANsurfer 스위치의 사용자 이름입니다
암호	SANsurfer 스위치의 암호입니다

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 15분)
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMPv3만 해당)
SNMP 재시도	SNMP 재시도 횟수입니다
SNMP 시간 초과(ms)	SNMP 시간 초과(기본값 5,000ms)
트래핑을 활성화합니다	트래핑을 활성화하려면 선택합니다
트랩 사이의 최소 시간(초)	트랩에 의해 트리거된 획득 시도 사이의 최소 시간(기본값 10초)
패브릭 이름	데이터 소스에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

Red Hat(RHEV) 데이터 소스

Red Hat Enterprise Virtualization(REST) 데이터 소스는 HTTPS를 통해 RHEV 인스턴스에 대한 정보를 수집합니다.

요구 사항

- REST API를 통해 포트 443을 통해 RHEV 서버의 IP 주소입니다
- 읽기 전용 사용자 이름 및 암호
- RHEV 버전 3.0+

구성

필드에 입력합니다	설명
RHEV 서버 IP 주소입니다	RHEV 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	RHEV 서버의 사용자 이름입니다

암호	RHEV 서버에 사용되는 암호입니다
----	---------------------

고급 구성

필드에 입력합니다	설명
HTTPS 통신 포트	RHEV에 대한 HTTPS 통신에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)

Violin Flash Memory Array 데이터 소스

Violin 6000 시리즈 Flash Memory Array(HTTP) 데이터 소스는 Violin 6000 시리즈 플래시 메모리 어레이에서 분석 및 검증을 위해 네트워크 정보를 수집합니다.

용어



이 데이터 수집기는 OnCommand Insight 7.3.11부터 더 이상 사용할 수 없습니다.

OnCommand Insight는 Violin 6000 시리즈 플래시 메모리 어레이 데이터 소스에서 다음 인벤토리 정보를 수집합니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
Violin 지능형 메모리 모듈(VIMM)	디스크
컨테이너	스토리지
메모리 게이트웨이	스토리지 노드
LUN을 클릭합니다	볼륨
이니시에이터, 이니시에이터 그룹, 타겟	볼륨 맵, 볼륨 마스크



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- 스토리지에 대한 읽기 전용 사용자 이름과 암호가 필요합니다.
- 스토리지 IP 주소를 사용하여 웹 브라우저에서 액세스를 검증합니다.

구성

필드에 입력합니다	설명
Violin Memory Array 주 게이트웨이의 IP 주소 또는 FQDN	Violin Memory Array Main Gateway의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Violin Memory Array 주 게이트웨이의 사용자 이름입니다
암호	Violin Memory Array 주 게이트웨이의 암호입니다

고급 구성

필드에 입력합니다	설명
통신 포트	Violin Array와의 통신에 사용되는 포트입니다
HTTPS가 활성화되었습니다	HTTPS를 사용하려면 선택합니다
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(초)	연결 시간 초과(기본값 60초)
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

VMware vSphere 데이터 소스

VMware vSphere(Web Services) 데이터 소스는 ESX 호스트 정보를 수집하고 Virtual Center 내의 모든 객체에 대해 _read-only_ 권한을 필요로 합니다.

용어

OnCommand Insight는 VMware vSphere 데이터 소스에서 다음 인벤토리 정보를 가져옵니다. Insight에서 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Insight 용어입니다
가상 디스크	디스크
호스트	호스트
가상 머신	가상 머신
데이터 저장소	데이터 저장소

LUN을 클릭합니다	LUN을 클릭합니다
Fibre Channel 포트	포트



이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

- Virtual Center 서버의 IP 주소입니다
- Virtual Center의 읽기 전용 사용자 이름 및 암호
- Virtual Center 내의 모든 객체에 대한 읽기 전용 권한
- Virtual Center 서버에서 SDK 액세스
- 포트 요구 사항: http-80 https-443
- 사용자 이름 및 암호를 사용하여 Virtual Center Client에 로그인하고 를 입력하여 SDK가 활성화되었는지 확인하여 액세스를 검증합니다 telnet <vc_ip> 443.

구성

* 필드 *
* 설명 *
가상 센터 주소
IP_(nnn.nnn.nnn.nnn_format) 주소 또는 DNS를 통해 확인할 수 있는 호스트 이름으로 지정된 Virtual Center 또는 vSphere 서버의 네트워크 주소입니다.
사용자 이름
VMware 서버의 사용자 이름입니다.
암호
VMware 서버의 암호입니다.

고급 구성

* 필드 *	* 설명 *
재고 폴링 간격(분)	재고 조사 간격(기본값 20분)
연결 시간 초과(ms)	연결 시간 초과(기본값 60000ms)

VM 필터링 기준	VM 필터링 방법을 선택합니다
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 VM 목록을 포함할지 제외할지 여부를 지정합니다
필터링할 VM 목록(값에 심표를 사용하는 경우 심표로 구분 또는 세미콜론으로 구분)	폴링을 포함하거나 폴링에서 제외할 VM 목록을 심표로 구분하거나 세미콜론으로 구분합니다
vCenter에 대한 요청 재시도 횟수입니다	vCenter 요청 재시도 횟수입니다
통신 포트	VMware 서버에 사용되는 포트입니다
성능 폴링 간격(초)	성능 폴링 간격(기본값 300초)

데이터 소스 자격 증명을 변경하는 중입니다

같은 유형의 여러 데이터 소스가 사용자 이름과 암호를 공유하는 경우 그룹의 모든 장치에 대한 암호를 동시에 변경할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

데이터 소스 * 목록이 열립니다.

2. Actions * 버튼을 클릭하고 * Change credentials * 옵션을 선택합니다.

3. 자격 증명 관리 대화 상자의 목록에서 데이터 소스 그룹 중 하나를 선택합니다.

용지 한 장에 있는 펜인 편집 아이콘이 오른쪽으로 활성화됩니다.

Credentials Management

Below is a list of groups of data sources with the same credentials. You can change the credentials of the entire group in a single action by pressing the edit button next to the desired group.

Data source type	Package	User/Community	Used by	
FC Switch Firmware 2.0+ (SNMP)	foundation	UHTSAN	elr1scvblkodd01 and 1 others	
FC Switch Firmware 4.2+ (SSH)	foundation	ssacct	ELR5_EvenFabric and 1 others	
FC Switch Firmware 4.2+ (SSH)	performance	UHTSAN	ELR5_EvenFabric	
HiCommand Device Manager	foundation	sanscm	ELR5_APSWP1008_HCS7 and 1 others	
Solutions Enabler (CLI) with Performance (SMT-S)	storageperformance	admin	ELR1_Vblock EMC	

Showing 1 to 5 of 5 entries

4. 편집 * 을 클릭합니다.

5. 새 암호를 입력하고 확인합니다.

데이터 수집 문제를 일으키는 변경 사항

OnCommand Insight에서 데이터 수집 문제가 발생하는 경우 환경 변화가 원인일 수 있습니다. 일반적인 유지 관리 규칙으로서 Insight에서도 환경의 모든 변경 사항을 고려해야 합니다.

이 검사 목록을 사용하여 문제를 일으킬 수 있는 네트워크 변경 사항을 확인할 수 있습니다.

- 암호를 변경했습니까? Insight에서 암호가 변경되었습니까?
- 네트워크에서 장치를 제거했습니까? 또한 장치가 다시 검색되고 다시 도입되지 않도록 OnCommand Insight에서 장치를 제거해야 합니다.
- 인프라 소프트웨어(예: HP CommandView EVA 또는 EMC Solutions Enabler)를 업그레이드했습니까?

획득 장치에 적절한 버전의 클라이언트 도구가 설치되어 있는지 확인합니다. 데이터 소스 장애가 지속될 경우 기술 지원 부서에 문의하여 지원을 요청하고 데이터 소스 패치를 적용해야 합니다.

- 모든 OnCommand Insight 획득 장치에서 동일한 OnCommand Insight 버전을 사용하고 있습니까? 원격 획득 장치 및 로컬 획득 장치가 서로 다른 OnCommand Insight 버전을 실행 중인 경우 모든 장치에 동일한 버전을 설치하여 데이터 수집 문제를 해결하십시오.

모든 획득 장치에 새 버전의 OnCommand Insight를 설치해야 하는 경우 지원 사이트로 이동하여 올바른 버전을 다운로드하십시오.

- 도메인 이름을 변경하거나 새 도메인을 추가했습니까? 장치 해상도(이전의 자동 해상도) 방법을 업데이트해야 합니다.

하나의 데이터 소스를 자세히 조사 중입니다

데이터 원본에 오류가 있거나 속도가 느려지면 해당 데이터 원본에 대한 자세한 정보 요약 검토하여 문제의 원인을 확인할 수 있습니다. 주의를 기울여야 하는 조건이 있는 데이터 소스는 빨간색 원으로 표시됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

데이터 소스 * 목록이 열립니다. 잠재적인 문제가 있는 나열된 모든 데이터 원본은 빨간색 원으로 표시됩니다. 가장 심각한 문제는 목록의 맨 위에 있습니다.

2. 문제를 일으키는 데이터 소스를 선택합니다.
3. 데이터 원본 이름 링크를 클릭합니다.
4. 데이터 원본 요약 페이지에서 다음 섹션의 정보를 확인합니다.

- * 이벤트 일정 *

데이터 소스 목록에 표시된 현재 상태와 연결된 이벤트를 나열합니다. 이 요약의 이벤트는 장치별로 표시됩니다. 오류는 빨간색으로 표시됩니다. 타임라인 항목 위에 마우스 포인터를 놓으면 추가 정보를 표시할 수 있습니다.

- * 이 데이터 소스에서 보고한 장치 *

디바이스 유형, 해당 IP 주소 및 각 디바이스에 대한 자세한 정보에 대한 링크를 표시합니다.

- * 이 데이터 소스에서 보고된 변경 사항(지난 3주) *

추가 또는 제거되었거나 구성이 변경된 모든 장치를 나열합니다.

5. 데이터 원본 정보를 검토한 후 페이지 맨 위에 있는 단추를 사용하여 다음 작업 중 하나를 수행할 수 있습니다.

- * 편집 * 문제를 해결하기 위한 데이터 원본에 대한 설명입니다.
- * 다시 폴링 * 문제가 지속적이었거나 간헐적으로 발생하는지 여부를 폴링하도록 강제합니다.
- * 3, 7 또는 30일 동안 데이터 소스 폴링을 연기하여 문제를 조사하고 경고 메시지를 중지할 시간을 제공합니다.
- * 데이터 원본에 패치 * 를 설치하여 문제를 해결합니다.
- 기술 지원을 위해 * 오류 보고서 * 를 준비합니다.
- * Insight 모니터링 환경에서 데이터 소스를 * 삭제 * 합니다.

실패한 데이터 소스 조사

데이터 소스에 " * Inventory failed! * " 또는 " * Performance failed! * " 메시지가 있고 High 또는 Medium Impact가 있는 경우 연결된 정보가 있는 데이터 소스 요약 페이지를 사용하여 이 문제를 조사해야 합니다.

단계

1. 데이터 원본의 연결된 * 이름 * 을 클릭하여 요약 페이지를 엽니다.
2. 요약 페이지에서 * Comments * 영역을 확인하여 이 고장을 조사할 수 있는 다른 엔지니어가 남긴 메모를 읽습니다.
3. 성능 메시지를 기록합니다.
4. 이 데이터 원본에 적용되는 패치가 있는 경우 링크를 클릭하여 * 패치 페이지 * 를 확인하여 문제가 발생했는지 확인합니다.
5. 마우스 포인터를 * 이벤트 타임라인 * 그래프 세그먼트 위로 이동하여 추가 정보를 표시합니다.
6. 장치에 대한 오류 메시지를 선택하고 이벤트 타임라인 아래에 표시된 * 오류 세부 정보 * 아이콘을 클릭하면 메시지 오른쪽에 표시됩니다.

오류 세부 정보에는 오류 메시지 텍스트, 가능한 원인, 사용 중인 정보 및 문제 해결을 위해 시도할 수 있는 권장 사항이 포함됩니다.

7. 이 데이터 소스 영역에서 보고한 장치 영역에서 목록을 필터링하여 관심 있는 장치만 표시할 수 있으며, 장치의 연결된 * 이름 * 을 클릭하여 해당 장치의 _asset 페이지_를 표시할 수 있습니다.
8. 이전에 표시된 페이지로 돌아가려면 다음 방법 중 하나를 사용합니다.
 - 브라우저의 뒤로 화살표를 클릭합니다.
 - 뒤로 화살표를 마우스 오른쪽 단추로 클릭하여 페이지 목록을 표시하고 원하는 페이지를 선택합니다.
9. 다른 자원에 대한 자세한 정보를 표시하려면 연결된 다른 이름을 클릭합니다.
10. 데이터 원본 요약 페이지로 돌아가면 페이지 하단의 * 변경 * 영역을 확인하여 최근 변경으로 인해 문제가 발생했는지 확인합니다.

데이터 소스 폴링을 제어합니다

데이터 원본을 변경한 후 변경 내용을 확인하기 위해 즉시 폴링하거나 문제 해결 중에 데이터 원본의 데이터 수집을 1, 3 또는 5일 동안 연기할 수 있습니다.

단계

1. Admin * 을 클릭하고 데이터 소스 목록 보기로 이동합니다
2. 폴링을 제어할 데이터 소스를 선택합니다.
3. 데이터 원본 이름 링크를 클릭합니다.
4. 데이터 원본 요약 페이지에서 정보를 확인하고 다음 두 폴링 옵션 중 하나를 클릭합니다.
 - * 다시 폴링* 데이터 소스가 데이터를 즉시 수집하도록 강제합니다.
 - *연기* 를 선택하고 폴링 지연 기간을 3일, 7일 또는 30일로 선택합니다.

작업을 마친 후

데이터 소스에서 데이터 수집을 연기하고 컬렉션을 다시 시작하려면 요약 페이지에서 * Resume * 을 클릭합니다.

데이터 원본 정보 편집

데이터 소스 설정 정보를 빠르게 편집할 수 있습니다.

단계

1. Admin * 을 클릭하고 데이터 소스 목록 보기로 이동합니다
2. 편집할 데이터 원본을 찾습니다.
3. 다음 방법 중 하나를 사용하여 변경을 시작합니다.
 - 선택한 데이터 원본의 오른쪽에 있는 * 데이터 원본 편집 * 을 클릭합니다.
 - 선택한 데이터 원본의 연결된 이름을 클릭하고 * 편집 * 을 클릭합니다. 두 방법 중 하나를 선택하면 데이터 원본 편집 대화 상자가 열립니다.
4. 원하는 대로 변경하고 * Save * (저장 *)를 클릭합니다.

여러 데이터 원본에 대한 정보 편집

동일한 공급업체 및 모델의 여러 데이터 원본에 대한 대부분의 정보를 한 번에 편집할 수 있습니다. 예를 들어 이러한 데이터 원본이 사용자 이름과 암호를 공유하는 경우 한 곳에서 암호를 변경하여 선택한 모든 데이터 원본의 암호를 업데이트할 수 있습니다.

이 작업에 대해

선택한 데이터 원본에 대해 편집할 수 없는 옵션은 흐리게 표시되거나 데이터 원본 편집 대화 상자에 표시되지 않습니다. 또한 옵션이 * Mixed * 값을 표시할 때 옵션의 값이 선택한 데이터 소스 간에 다르다는 것을 나타냅니다. 예를 들어 선택한 두 데이터 원본에 대한 * Timeout(sec) * 옵션이 * Mixed * 인 경우 한 데이터 원본의 시간 초과 값은 60이고 다른 데이터 원본의 값은 90일 수 있습니다. 따라서 이 값을 120으로 변경하고 데이터 원본에 대한 변경 내용을 저장하면 두 데이터 원본에 대한 시간 초과 설정이 120이 됩니다.

단계

1. Admin * 을 클릭하고 데이터 소스 목록 보기로 이동합니다
2. 수정할 데이터 원본을 선택합니다. 선택한 데이터 소스는 동일한 공급업체, 모델 및 획득 단위에 속해야 합니다.
3. Actions * 버튼을 클릭하고 * Edit * 옵션을 선택합니다.
4. 편집 대화 상자에서 필요에 따라 * 설정 * 을 변경합니다.
5. 데이터 원본에 대한 기본 옵션을 변경하려면 * 구성 * 링크를 클릭합니다.
6. 데이터 원본에 대한 고급 옵션을 변경하려면 * 고급 구성 * 링크를 클릭합니다.
7. 저장 * 을 클릭합니다.

주석에 데이터 원본 태그 매핑

데이터 소스가 태그 데이터를 폴링하도록 구성된 경우 Insight는 태그와 같은 이름의 기존 Insight 주석에 대한 주석 값을 자동으로 설정합니다.

데이터 소스에서 태그를 사용하기 전에 Insight 주석이 있으면 데이터 소스 태그 데이터가 Insight 주석에 자동으로

추가됩니다.

태그가 활성화된 후 주석을 만들 때 데이터 소스의 초기 폴링은 주석을 자동으로 업데이트하지 않습니다. Insight 주석을 교체하거나 채우는 데 걸리는 시간이 지연됩니다. 지연을 방지하려면 데이터 소스를 연기했다가 다시 시작하면 태그가 주석으로 업데이트되도록 할 수 있습니다.

데이터 원본을 삭제하는 중입니다

환경에서 데이터 소스를 제거한 경우에는 OnCommand Insight 모니터링 환경에서도 삭제해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.

데이터 소스 목록이 열립니다.

2. 삭제할 데이터 원본을 선택합니다.
3. 연결된 데이터 원본 이름을 클릭합니다.
4. 요약 페이지에서 선택한 데이터 원본에 대한 정보를 확인하여 삭제할 데이터 원본인지 확인합니다.
5. 삭제 * 를 클릭합니다.
6. 확인 * 을 클릭하여 작업을 확인합니다.

어떤 데이터 소스 패치가 있는지 확인합니다

데이터 소스 패치는 기존 패치의 문제를 해결하고 새 데이터 소스 유형(공급업체 및 모델)을 쉽게 추가할 수 있습니다. 네트워크의 각 데이터 소스 유형에 대해 데이터 소스 패치를 업로드할 수 있습니다. 패치 프로세스를 설치, 테스트 및 관리할 수도 있습니다. 그러나 한 번에 하나의 패치만 데이터 소스 유형에 대해 활성화될 수 있습니다.

각 패치에 대해 다음 작업을 수행할 수 있습니다.

- 패치를 수신하는 각 데이터 소스의 비교 전과 후를 확인합니다.
- 의견을 작성하여 결정을 설명하거나 연구를 요약합니다.
- 패치에 잘 응답하지 않는 데이터 소스를 변경합니다.
- Insight 서버에 커밋할 패치를 승인합니다.
- 의도한 대로 작동하지 않는 패치를 롤백합니다.
- 결함이 있는 패치를 다른 패치로 교체합니다.

데이터 소스 패치를 적용하는 중입니다

데이터 소스 패치를 주기적으로 사용할 수 있으며 기존 데이터 소스의 문제를 해결하거나 새 공급업체의 데이터 소스를 추가하거나 공급업체의 새 모델을 추가할 수 있습니다.

시작하기 전에

을(를) 받아야 합니다. .zip 최신 데이터 소스가 포함된 파일입니다. .patch 기술 지원 부서의 파일.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 작업 버튼에서 * 패치 적용 * 을 선택합니다.
4. 데이터 원본 패치 적용 * 대화 상자에서 * 찾아보기 * 를 클릭하여 을 찾습니다. .patch 파일.
5. 패치 이름 *, * 설명 * 및 * 영향받는 데이터 소스 유형 * 을 검사합니다.
6. 선택한 패치가 올바르면 * 패치 적용 * 을 클릭합니다.

데이터 원본 관련 문제를 해결하는 패치를 적용하는 경우 동일한 유형의 모든 데이터 원본이 패치로 업데이트되므로 패치를 승인해야 합니다. 구성된 데이터 원본에 영향을 주지 않는 패치는 자동으로 승인됩니다.

작업을 마친 후

새 공급업체나 새 모델에 대한 데이터 원본을 추가하는 패치를 적용하는 경우 패치를 적용한 후 데이터 원본을 추가해야 합니다.

하나의 데이터 소스에 패치 설치

데이터 원본 패치를 업로드한 후에는 같은 형식의 모든 데이터 원본에 설치할 수 있습니다.

시작하기 전에

한 유형의 데이터 원본에 설치할 패치 파일을 업로드해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 작업 버튼에서 * 패치 적용 * 을 선택합니다.
4. 데이터 원본 패치 적용 * 대화 상자에서 * 찾아보기 * 를 클릭하여 업로드된 패치 파일을 찾습니다.
5. 패치 이름 *, * 설명 * 및 * 영향받는 데이터 소스 유형 * 을 확인하십시오.
6. 선택한 패치가 올바르면 * 패치 적용 * 을 클릭합니다.

동일한 유형의 모든 데이터 소스가 이 패치로 업데이트됩니다.

패치 관리

네트워크에 적용되는 모든 데이터 소스 패치의 현재 상태를 검토할 수 있습니다. 패치에 대한 작업을 수행하려면 현재 검토 중인 패치에서 연결된 이름을 클릭하면 됩니다.

시작하기 전에

이미 업로드된 패치를 하나 이상 설치해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.

설치된 패치가 없는 경우 현재 검토 중인 패치 테이블이 비어 있습니다.

3. 현재 검토 중인 * 패치 * 에서 현재 적용 중인 데이터 소스 패치의 상태를 확인합니다.
4. 특정 패치와 관련된 세부 정보를 검사하려면 패치의 연결된 이름을 클릭합니다.
5. 선택한 패치에 대해 다음 옵션을 클릭하여 패치에 대한 다음 작업을 수행할 수 있습니다.
 - * Approve patch * 는 데이터 소스에 패치를 적용합니다.
 - * 롤백 * 은 패치를 제거합니다.
 - * 패치 바꾸기 * 를 사용하면 해당 데이터 원본에 대해 다른 패치를 선택할 수 있습니다.

데이터 소스 패치 커밋

패치 요약의 정보를 사용하여 패치가 예상대로 작동하는지 확인한 다음 패치를 네트워크에 커밋합니다.

시작하기 전에

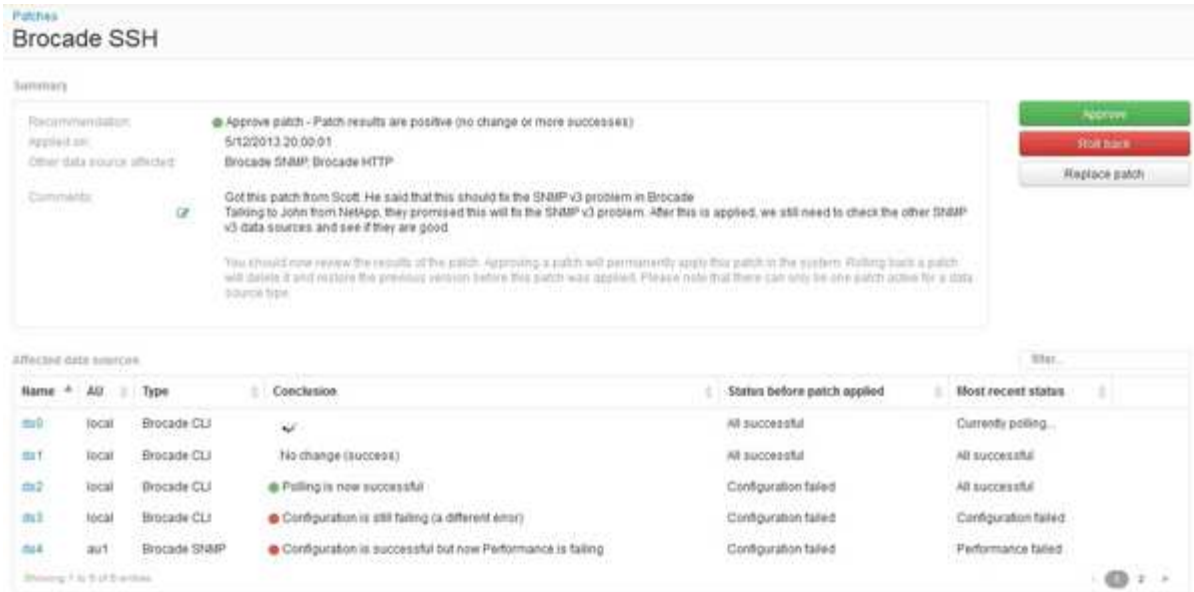
패치를 설치했으며 패치가 성공적인지 확인해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.

설치된 패치가 없으면 현재 검토 중인 패치가 비어 있습니다.

3. 현재 검토 중인 * 패치 * 에서 현재 적용 중인 데이터 소스 패치의 상태를 확인합니다.
4. 특정 패치와 관련된 세부 정보를 검사하려면 패치의 연결된 이름을 클릭합니다.
5. 이 예제에 표시된 패치 요약 정보에서 * 권장 * 및 * 설명 * 을 확인하여 패치의 진행 상황을 평가합니다.



6. 영향을 받는 * 데이터 소스 * 표를 확인하여 패치 전후에 영향을 받는 각 데이터 소스의 상태를 확인하십시오.

패치하는 데이터 원본 중 하나에 문제가 있는 경우 영향을 받는 데이터 원본 테이블에서 연결된 이름을 클릭합니다.

7. 해당 유형의 데이터 원본에 패치를 적용해야 한다고 판단하면 * Approve * (승인 *)를 클릭합니다.

데이터 소스가 변경되고 현재 검토 중인 패치에서 패치가 제거됩니다.

데이터 소스 패치를 롤백하는 중입니다

데이터 소스 패치가 예상한 방식으로 작동하지 않으면 롤백할 수 있습니다. 패치를 롤백하면 패치가 삭제되고 이 패치가 적용되기 전의 이전 버전이 복원됩니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 현재 검토 중인 패치 * 에서 실패한 것으로 보이는 패치의 연결된 이름을 클릭합니다.
4. 데이터 원본의 패치 페이지에서 다음 정보를 확인합니다.
 - * 요약 * 은 패치가 적용된 시기, 영향을 받는 데이터 원본, 사용자 또는 팀의 다른 구성원으로부터 받은 패치에 대한 설명을 나타냅니다.
 - 영향을 받는 데이터 소스 * 는 패치되는 모든 데이터 소스를 나열하며 패치 이전 및 이후 상태의 비교를 포함합니다.
5. 패치를 성공적으로 처리하지 않는 데이터 원본에 대한 세부 정보를 표시하려면 연결된 * 이름 * 을 클릭합니다.
 - a. 요약 정보를 확인합니다.
 - b. 이벤트 타임라인 * 을 확인하여 이 데이터 소스에 영향을 줄 수 있는 구성 또는 성능 데이터를 확인하십시오.
6. 패치가 제대로 실행되지 않을 것이라고 판단될 경우 브라우저의 뒤로 화살표를 클릭하여 패치 요약 페이지로 돌아갑니다.

7. 롤백 * 을 클릭하여 해당 패치를 제거합니다.

다른 패치가 성공적임을 알고 있는 경우 * 패치 바꾸기 * 를 클릭하고 새 패치를 업로드하십시오.

장치 해상도

OnCommand Insight를 사용하여 모니터링하려는 모든 장치를 검색해야 합니다. 환경의 성능과 인벤토리를 정확하게 추적하려면 검색이 필요합니다. 일반적으로 사용자 환경의 대부분의 장치는 자동 장치 해상도를 통해 검색됩니다.



업그레이드를 수행하는 중에 업그레이드 중인 시스템에 비활성 자동 해결 규칙이 있는 경우 업그레이드 중에 이러한 규칙이 삭제됩니다. 비활성 자동 해결 규칙을 유지하려면 업그레이드를 수행하기 전에 규칙을 활성화(확인란 선택)합니다.

데이터 소스를 설치 및 구성한 후에는 스위치, 스토리지 어레이 및 하이퍼바이저와 VM의 가상 인프라를 비롯한 환경의 장치가 식별됩니다. 그러나 이 경우 일반적으로 사용자 환경의 디바이스 중 100%는 식별되지 않습니다.

데이터 소스 유형 디바이스를 구성한 후에는 디바이스 해결 규칙을 활용하여 사용자 환경에서 나머지 알 수 없는 디바이스를 식별하는 것이 가장 좋습니다. 장치 해상도를 통해 알 수 없는 장치를 다음 장치 유형으로 해결할 수 있습니다.

- 물리적 호스트
- 지원합니다
- 테이프
- 스위치

디바이스 확인 후 ""알 수 없음""으로 남아 있는 디바이스는 쿼리와 대시보드에도 표시할 수 있는 일반 디바이스로 간주됩니다.

차례로 생성된 규칙은 사용자 환경에 추가되는 것과 유사한 특성을 가진 새 디바이스를 자동으로 식별합니다. 경우에 따라 장치 해상도를 통해 Insight 내에서 검색되지 않은 장치에 대한 장치 해결 규칙을 우회하여 수동으로 식별할 수도 있습니다.

기기 식별이 완료되지 않으면 다음과 같은 문제가 발생할 수 있습니다.

- 불완전한 경로
- 알 수 없는 다중 경로 연결
- 애플리케이션을 그룹화할 수 없습니다
- 토폴로지 뷰가 부정확합니다
- 데이터 웨어하우스 및 보고의 부정확한 데이터

장치 해상도 기능(* 관리*>* 장치 해상도*)에는 다음 탭이 포함되어 있으며 각 탭은 장치 해상도 계획 및 결과 보기에 역할을 합니다.

- "FC Identify"(FC 식별)에는 자동 디바이스 확인을 통해 해결되지 않은 Fibre Channel 디바이스의 WWN 및 포트 정보가 포함됩니다. 이 탭은 식별된 디바이스의 비율도 식별합니다.

- "IP Identify"(IP 식별)에는 자동 디바이스 확인을 통해 식별되지 않은 CIFS 공유 및 NFS 공유에 액세스하는 디바이스 목록이 포함되어 있습니다. 이 탭은 식별된 디바이스의 비율도 식별합니다.
- "자동 해상도 규칙"에는 Fibre Channel 디바이스 해상도를 수행할 때 실행되는 규칙 목록이 포함되어 있습니다. 식별되지 않은 Fibre Channel 디바이스를 확인하기 위해 생성하는 규칙입니다.
- ""기본 설정""은 환경에 맞게 장치 해상도를 사용자 정의하는 데 사용하는 구성 옵션을 제공합니다.

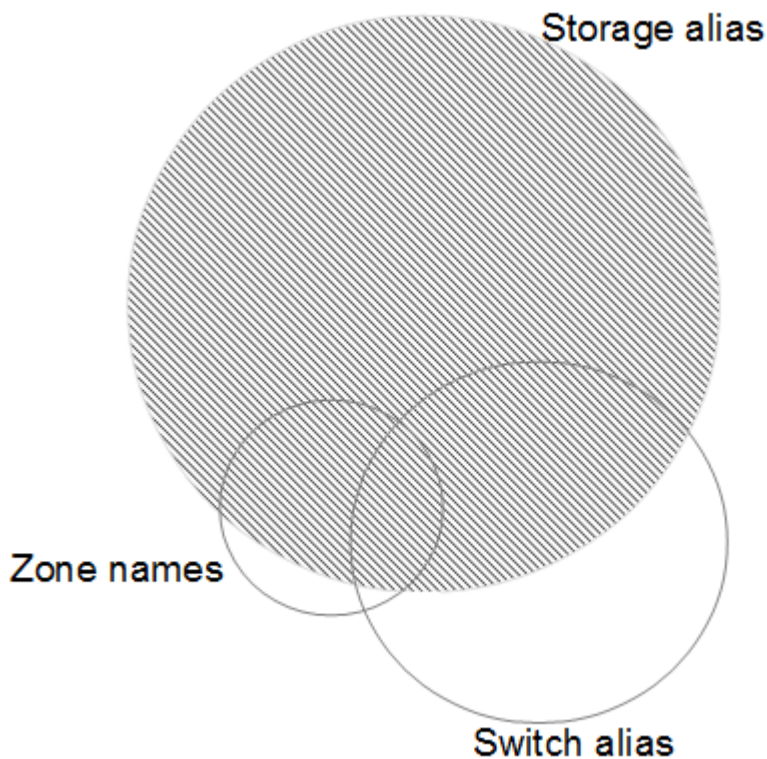
시작하기 전에

디바이스 식별 규칙을 정의하기 전에 환경 구성 방법을 알아야 합니다. 환경에 대해 더 많이 알수록 장치를 더 쉽게 식별할 수 있습니다.

정확한 규칙을 만들려면 다음과 유사한 질문에 대답해야 합니다.

- 귀사의 환경에 존 또는 호스트에 대한 명명 표준이 있습니까? 이 중 몇 퍼센트가 정확합니까?
- 귀사의 환경에서 스위치 별칭 또는 스토리지 별칭이 사용되고 있으며 이 별칭이 호스트 이름과 일치합니까?
- 사용 중인 환경에서 SRM 툴을 사용하고 있으며 이를 사용하여 호스트 이름을 식별할 수 있습니까? SRM은 어떤 서비스를 제공합니까?
- 사용자 환경에서 명명 체계가 얼마나 자주 변경됩니까?
- 서로 다른 이름 지정 체계를 도입한 인수 또는 합병이 있었습니까?

환경을 분석한 후에는 신뢰할 수 있는 명명 기준이 무엇인지 파악할 수 있어야 합니다. 수집한 정보는 다음과 유사한 그림으로 표시될 수 있습니다.

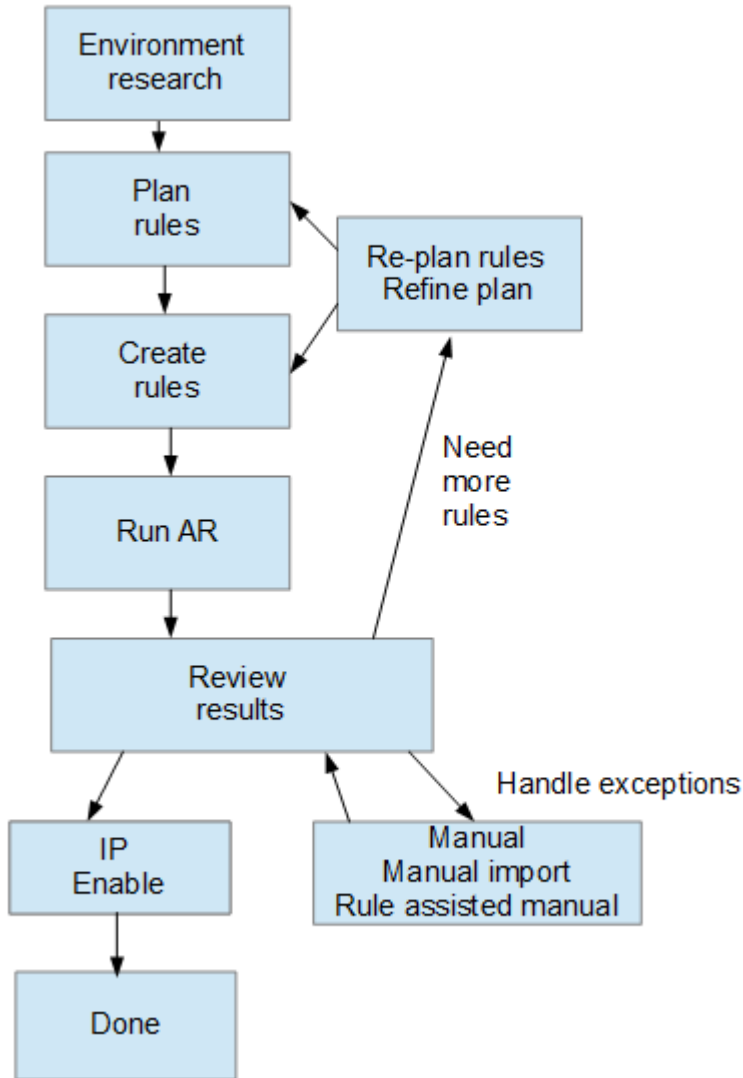


이 예에서는 가장 많은 수의 디바이스가 스토리지 별칭으로 안정적으로 표시됩니다. 스토리지 별칭을 사용하여 호스트를 식별하는 규칙을 먼저 작성하고, 스위치 별칭을 사용하는 규칙을 다음에 작성해야 하며, 마지막으로 생성된 규칙은 존 별칭을 사용해야 합니다. 영역 별칭과 스위치 별칭의 사용이 겹치기 때문에 일부 스토리지 별칭 규칙은 추가 디바이스를

식별할 수 있으므로 영역 별칭과 스위치 별칭에 필요한 규칙이 줄어듭니다.

사용자 환경에서 장치를 정의하는 단계입니다

일반적으로 다음과 유사한 워크플로를 사용하여 사용자 환경에서 장치를 식별합니다. 식별은 반복적인 프로세스이며 규칙을 계획하고 구체화하는 여러 단계가 필요할 수 있습니다.



사용자 환경에 알 수 없는 장치("알 수 없음" 또는 일반 장치)가 있고 이후에 폴링 시 이러한 장치를 식별하는 데이터 소스를 구성하면 더 이상 일반 장치로 표시되거나 계산되지 않습니다.

환경에 대한 장치 해결 규칙 계획

규칙을 사용하여 사용자 환경에서 장치를 식별하는 것은 일반적으로 환경을 철저히 분석하고 가능한 많은 장치를 식별하기 위해 여러 규칙을 만들어야 하는 반복적인 프로세스입니다. 가장 좋은 시나리오는 환경에 있는 장치의 100%를 식별하기 위한 목표를 설정하는 것입니다.

규칙의 가장 효율적인 순서는 가장 제한적인 규칙을 먼저 배치하여 대부분의 항목이 패턴 일치되지 않도록 하고, 프로세스는 덜 제한적인 규칙으로 진행되도록 하는 것입니다. 이를 통해 Insight는 각 항목에 더 많은 패턴을 적용하여 패턴 일치 및 양성 호스트 식별 가능성을 높일 수 있습니다.

규칙을 만들 때 목표는 가능한 최대 수의 식별되지 않은 장치를 처리하는 규칙을 만드는 것입니다. 예를 들어, 다음과 같은 적용 범위 패턴을 따르는 규칙을 만들면 적용 범위 비율이 낮은 30개의 규칙을 만드는 것이 훨씬 효율적입니다.

규칙	적용 범위의 백분율입니다
규칙 1	60%
규칙 2	25%
규칙 3	8%
규칙 4	4%
규칙 5	1%

장치 해상도 규칙을 만드는 중입니다

디바이스 확인 규칙을 생성하여 현재 OnCommand Insight에서 자동으로 식별되지 않는 호스트, 스토리지 및 테이프를 식별합니다. 생성하는 규칙은 현재 환경에 있는 디바이스를 식별하고 유사한 디바이스를 환경에 추가할 때 식별합니다.

이 작업에 대해

규칙을 만들 때는 먼저 규칙이 실행되는 정보의 소스, 정보를 추출하는 데 사용되는 메서드 및 DNS 조회가 규칙의 결과에 적용되는지 여부를 확인합니다.

장치를 식별하는 데 사용되는 소스입니다
<ul style="list-style-type: none"> • 호스트에 대한 SRM 별칭입니다 • 포함된 호스트 또는 테이프 이름을 포함하는 스토리지 별칭입니다 • 포함된 호스트 또는 테이프 이름이 포함된 스위치 별칭입니다 • 포함된 호스트 이름이 포함된 영역 이름입니다
소스에서 디바이스 이름을 추출하는 데 사용되는 방법입니다
<ul style="list-style-type: none"> • 있는 그대로(SRM에서 이름 추출) • 구분 기호 • 정규식입니다
DNS 조회
DNS를 사용하여 호스트 이름을 확인할지 여부를 지정합니다.

자동 해결 규칙 탭에서 규칙을 만듭니다. 다음 단계에서는 규칙 생성 프로세스를 설명합니다.

단계

1. Manage * > * Device resolution * 을 클릭합니다
2. 자동 해상도 규칙 * 탭에서 * + 추가 * 를 클릭합니다

새 규칙 화면이 표시됩니다.



새 규칙 화면에는 정규식을 만들기 위한 도움말과 예제를 제공하는 *? * 아이콘이 포함되어 있습니다.

3. Type * 목록에서 식별하려는 장치를 선택합니다.

호스트 또는 테이프 를 선택할 수 있습니다.

4. 소스 * 목록에서 호스트를 식별하는 데 사용할 소스를 선택합니다.

선택한 소스에 따라 Insight에 다음 응답이 표시됩니다.

- 영역은 Insight에서 식별해야 하는 영역 및 WWN을 나열합니다.
- SRM에는 Insight로 식별해야 하는 식별되지 않은 별칭이 나열됩니다
- 스토리지 별칭에는 Insight에서 식별해야 하는 스토리지 별칭과 WWN이 나열됩니다
- 스위치 별칭에는 Insight에서 식별해야 하는 스위치 별칭이 나열됩니다

5. Method* 목록에서 호스트를 식별하기 위해 사용할 방법을 선택합니다.

출처	방법
SRM	"있는 그대로", "기한도자", "정규식"
스토리지 별칭입니다	"기한도자" 또는 "정규식"
별칭 전환	"기한도자" 또는 "정규식"
존	"기한도자" 또는 "정규식"

- "기한자"를 사용하는 규칙에는 구분 기호 및 호스트 이름의 최소 길이가 필요합니다.

호스트 이름의 최소 길이는 Insight에서 호스트를 식별하는 데 사용해야 하는 문자 수입입니다. Insight는 길이가 길거나 긴 호스트 이름에 대해서만 DNS 조회를 수행합니다.


Delimiters를 사용하는 규칙의 경우 입력 문자열은 구분 기호로 토큰화되며 인접한 토큰을 여러 개 조합하여 호스트 이름 후보 목록이 만들어집니다. 그런 다음 목록이 가장 큰 것부터 가장 작은 순서로 정렬됩니다. 예를 들어 vipsnq03_hba3_emcp3_12ep0의 경우 다음과 같은 결과가 나타납니다.

- vipsnq03_hba3_emcp3_12ep0을 입력합니다
- vipsnq03_hba3_emcp3

- hba3 emc3_12ep0
- vipsnq03_hba3
- emc3_12ep0을 참조하십시오
- hba3_emc3
- vipsnq03
- 12ep0
- emc3
- hba3

◦ 정규식을 사용하는 규칙에는 정규식과 형식, 케이스 민감도를 선택해야 합니다.

6.

을 클릭합니다  모든 규칙을 실행하거나, 버튼을 눌러 만든 규칙(및 AR의 마지막 전체 실행 이후 생성된 기타 규칙)을 실행합니다.

결과

규칙 실행 결과는 FC 식별 탭에 표시됩니다.

자동 장치 해상도 업데이트를 시작합니다

장치 해상도 업데이트는 마지막 전체 자동 장치 해상도 실행 이후 추가된 수동 변경 사항을 커밋합니다. 업데이트를 실행하면 장치 해상도 구성에 대한 새 수동 항목만 커밋하고 실행할 수 있습니다. 전체 장치 해상도 실행이 수행되지 않습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. 장치 해상도 * 화면에서 * AR 실행 * 버튼의 아래쪽 화살표를 클릭합니다.
4. 업데이트를 시작하려면 * 업데이트 * 를 클릭합니다.

규칙 지원 수동 식별

이 기능은 알 수 없는 호스트, 스토리지 및 테이프 디바이스 또는 그룹 문제를 해결하기 위해 특정 규칙 또는 규칙 목록(일회성 순서 재조정 포함 또는 제외)을 실행하려는 특수한 경우에 사용됩니다.

시작하기 전에

식별되지 않은 다수의 장치가 있고 다른 장치를 성공적으로 식별하는 여러 규칙이 있습니다.

이 작업에 대해



소스에 호스트 또는 장치 이름의 일부만 포함되어 있는 경우 정규식 규칙을 사용하여 서식을 지정하여 누락된 텍스트를 추가합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. Manage * > * Device resolution * 을 클릭합니다
3. FC 식별 * 탭을 클릭합니다.

시스템에서 식별된 장치 및 식별되지 않은 장치를 표시합니다.

4. 식별되지 않은 여러 장치를 선택합니다.
5. Identify * > * Set host resolution * 또는 * > Set tape resolution * 을 클릭합니다

성공적으로 식별된 장치의 모든 규칙 목록이 포함된 식별 화면이 표시됩니다.

6. 규칙 순서를 필요에 맞는 순서로 변경합니다.

규칙 순서는 식별 화면에서 변경되지만 전역적으로 변경되지는 않습니다.

7. 필요에 맞는 방법을 선택하십시오.

OnCommand Insight는 메시드가 나타나는 순서대로 호스트 확인 프로세스를 실행하며, 맨 위에 있는 방법부터 시작합니다.

적용되는 규칙이 있으면 규칙 이름이 규칙 열에 표시되고 수동으로 식별됩니다.

파이버 채널 장치 해상도

FC 식별 화면에는 호스트가 자동 디바이스 확인 방법으로 식별되지 않은 Fibre Channel 디바이스의 WWN 및 WWPN이 표시됩니다. 또한 화면에는 수동 장치 해상도에 의해 해결된 모든 장치가 표시됩니다.

수동 해상도에 의해 해결된 장치에는 ""OK"" 상태가 포함되어 있으며 장치를 식별하는 데 사용되는 규칙을 식별합니다. 누락된 장치는 ""알 수 없음"" 상태입니다. 장치 식별의 총 범위는 이 페이지에 나와 있습니다.

+ Add

Total coverage
30% (3/10)

	WWN	Port WWN	IP	Name	Type	Status	Rule
<input type="checkbox"/>	30:E0:00:00:00:00:00	10:B0:00:00:00:00:28:20	1.1.1.1	ResolvedHost1	Host	OK	Hosts by zone
<input type="checkbox"/>	30:E0:00:00:00:00:00:02	10:B0:00:00:00:00:28:22	2.2.2.2	ResolvedHost2	Host	OK	Rule deleted
<input type="checkbox"/>	30:E0:00:00:00:00:00:03	10:B0:00:00:00:00:28:23			Unknown	Unidentified	
<input type="checkbox"/>	30:E0:00:00:00:00:00:04	10:B0:00:00:00:00:28:24			Unknown	Unidentified	
<input type="checkbox"/>	30:E0:00:00:00:00:00:05	10:B0:00:00:00:00:28:25			Unknown	Unidentified	

Showing 1 to 5 of 10 entries

FC 식별 화면의 왼쪽에서 여러 디바이스를 선택하여 대량 작업을 수행합니다. 장치 위로 마우스를 가져간 다음 목록의 맨 오른쪽에 있는 식별 또는 식별 안 함 단추를 선택하여 단일 장치에서 작업을 수행할 수 있습니다.

Total coverage(전체 범위) 링크는 사용자의 구성에 대해 "식별된 장치 수/사용 가능한 장치 수" 목록을 표시합니다.

- SRM 별칭

- 스토리지 별칭입니다
- 별칭 전환
- 존
- 사용자 정의

Fibre Channel 디바이스를 수동으로 추가합니다

디바이스 해상도 FC 식별 탭에서 사용할 수 있는 수동 추가 기능을 사용하여 Fibre Channel 디바이스를 OnCommand Insight에 수동으로 추가할 수 있습니다. 이 프로세스는 향후 발견될 것으로 예상되는 장치를 사전 식별하는 데 사용될 수 있습니다.

시작하기 전에

시스템에 디바이스 ID를 추가하려면 WWN 또는 IP 주소와 디바이스 이름을 알아야 합니다.

이 작업에 대해

호스트, 스토리지, 테이프 또는 알 수 없는 Fibre Channel 디바이스를 수동으로 추가할 수 있습니다.

단계

1. Insight 웹 UI에 로그인합니다
2. Manage * > * Device resolution * 을 클릭합니다
3. FC 식별 * 탭을 클릭합니다.
4. 추가 버튼을 클릭합니다.

장치 추가 대화 상자가 표시됩니다

5. WWN 또는 IP 주소, 디바이스 이름을 입력하고 디바이스 유형을 선택합니다.

결과

입력한 디바이스가 FC 식별 탭의 디바이스 목록에 추가됩니다. '규칙'은 '수동'으로 식별됩니다.

CSV 파일에서 **Fibre Channel** 디바이스 ID 가져오기

CSV 파일의 디바이스 목록을 사용하여 Fibre Channel 디바이스 ID를 OnCommand Insight 디바이스 해상도 기능으로 수동으로 가져올 수 있습니다.

시작하기 전에

장치 식별 정보를 장치 해상도 기능으로 직접 가져오려면 올바른 형식의 CSV 파일이 있어야 합니다. Fibre Channel 디바이스용 CSV 파일에는 다음 정보가 필요합니다.

WWN입니다

IP
이름
유형



모범 사례로서 먼저 FC 식별 정보를 CSV 파일로 내보내고 해당 파일에서 원하는 대로 변경한 다음 파일을 다시 FC Identify로 가져오는 것이 좋습니다. 이렇게 하면 예상 열이 올바른 순서로 표시됩니다.

FC 식별 정보를 가져오려면

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. FC 식별 * 탭을 선택합니다.
4. 식별 * > * 파일에서 식별 * 을 클릭합니다

- a. 가져올 CSV 파일이 포함된 폴더로 이동하고 원하는 파일을 선택합니다.

입력한 디바이스는 FC Identify 탭의 디바이스 목록에 추가됩니다. 규칙(Rule)은 'Manual'(수동)으로 식별됩니다.

Fibre Channel 디바이스 식별 정보를 CSV 파일로 내보내는 중입니다

OnCommand Insight 디바이스 확인 기능을 사용하여 기존 Fibre Channel 디바이스 식별 정보를 CSV 파일로 내보낼 수 있습니다. 장치 ID를 수정하여 Insight로 다시 가져온 다음 내보낸 ID와 원래 일치하는 장치를 식별하는 데 이 ID를 사용할 수 있도록 장치 ID를 내보낼 수 있습니다.


이 작업에 대해

이 시나리오에는 CSV 파일에서 쉽게 편집한 후 시스템으로 다시 가져올 수 있는 유사한 속성이 장치에 있을 때 사용할 수 있습니다.

Fibre Channel 디바이스 ID를 CSV 파일로 내보낼 때 파일은 다음 정보를 표시된 순서대로 포함합니다.

WWN입니다
IP
이름
유형

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. FC 식별 * 탭을 선택합니다.
4. ID를 내보낼 Fibre Channel 디바이스를 선택합니다.
5. 내보내기를 클릭합니다  아이콘을 클릭합니다.
6. CSV 파일을 열거나 파일을 저장할 것인지 선택합니다.

IP 장치 해상도

IP 식별 화면에는 자동 디바이스 확인 또는 수동 디바이스 확인으로 식별된 iSCSI 및 CIFS 또는 NFS 공유가 표시됩니다. 식별되지 않은 장치도 표시됩니다. 화면에는 장치의 IP 주소, 이름, 상태, iSCSI 노드 및 공유 이름이 포함됩니다. 성공적으로 식별된 디바이스의 비율도 표시됩니다.

+ Add

Total coverage
20% (2/10)

IP identify (10)

Identify Unidentify filter...

Address IP Name Status iSCSI node Share name

☐

1.1.1.11.1.1.1LA3-CNS-SQL-06AOK

iqn.1991-05.com.microsoft:la3-cns-sql-06b.cns.comcastnets.com

/vol/ServerLogs_STG/

☐

0.0.0.0/0

iqn.1991-05.com.microsoft:jec20643597717.tfayd.com

/vol/wc_sc_libraries_prod/libraries_qtree/

☐

10.56.100.18

iqn.1991-05.com.microsoft:jec20643597717.tfayd.com

/vol/wc_sc_libraries_prod/libraries_qtree/

☐

10.56.100.19

iqn.1991-05.com.microsoft:jec20643597717.tfayd.com

/vol/wc_sc_libraries_prod/libraries_qtree/

☐

100.54.18.100100.54.18.100ushapl00096ibOK

iqn.1991-05.com.microsoft:jec20643597717.tfayd.com

/vol/wc_sc_libraries_prod/libraries_qtree/

Showing 1 to 5 of 10 entries

< 1 2 >

수동으로 IP 장치 추가

IP 식별 화면에서 사용할 수 있는 수동 추가 기능을 사용하여 IP 장치를 OnCommand Insight에 수동으로 추가할 수 있습니다.

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device resolution * 을 클릭합니다
3. IP 식별 * 탭을 클릭합니다.
4. 추가 버튼을 클릭합니다.

장치 추가 대화 상자가 표시됩니다

5. 주소, IP 주소 및 고유한 장치 이름을 입력합니다.

결과

입력한 장치가 IP 식별 탭의 장치 목록에 추가됩니다.

CSV 파일에서 IP 장치 ID 가져오기

CSV 파일에서 장치 식별 목록을 사용하여 IP 장치 식별 정보를 장치 해상도 기능으로 수동으로 가져올 수 있습니다.

시작하기 전에

장치 식별 정보를 가져오려면 올바른 형식의 CSV 파일이 있어야 합니다. IP 장치용 CSV 파일에는 다음 정보가 필요합니다.

주소
IP
이름



모범 사례로서 먼저 IP 식별 정보를 CSV 파일로 내보내고 해당 파일에서 원하는 대로 변경한 다음 파일을 다시 IP Identify로 가져오는 것이 좋습니다. 이렇게 하면 예상 열이 올바른 순서로 표시됩니다.

IP 식별 정보를 가져오려면

단계

1. Insight 웹 UI에 로그인합니다.
 2. Manage * > * Device Resolution * 을 클릭합니다
 3. IP 식별 * 탭을 선택합니다.
 4. 식별 * > * 파일에서 식별 * 을 클릭합니다.
 - a. 가져올 CSV 파일이 포함된 폴더로 이동하고 원하는 파일을 선택합니다.
- 입력한 장치는 IP 식별 탭의 장치 목록에 추가됩니다.

CSV 파일로 IP 장치 ID를 내보내는 중입니다

장치 해상도 기능을 사용하여 Insight에서 기존 IP 장치 ID를 내보낼 수 있습니다. 장치 ID를 수정한 다음 다시 Insight로 가져와 내보낸 ID와 유사한 장치를 식별하는 데 사용할 수 있도록 장치 ID를 내보낼 수 있습니다.


이 작업에 대해

IP 장치 ID를 CSV 파일로 내보낼 때 파일은 다음 정보를 표시된 순서대로 포함합니다.

주소
IP

이름

단계

1. Insight 웹 UI에 로그인합니다.
2. Manage * > * Device Resolution * 을 클릭합니다
3. IP 식별 * 탭을 선택합니다.
4. ID를 내보내려는 IP 장치 또는 장치를 선택합니다.
5. 내보내기를 클릭합니다  아이콘을 클릭합니다.
6. CSV 파일을 열거나 파일을 저장할 것인지 선택합니다.

기본 설정 탭에서 옵션 설정

장치 해상도 기본 설정 탭에서는 자동 해결 일정을 생성하고, 식별에서 포함하거나 제외할 스토리지 및 테이프 벤더 를 지정하고, DNS 조회 옵션을 설정할 수 있습니다.

자동 해결 일정

자동 해상도 스케줄은 자동 장치 해상도 실행 시기를 지정할 수 있습니다.

옵션을 선택합니다	설명
모든	일, 시간 또는 분 간격으로 자동 장치 해상도를 실행하려면 이 옵션을 사용합니다.
매일	이 옵션을 사용하여 매일 특정 시간에 자동 장치 해상도를 실행할 수 있습니다.
수동	이 옵션은 자동 장치 해상도만 수동으로 실행할 때 사용합니다.
모든 환경은 변동합니다	이 옵션을 사용하면 환경에 변화가 있을 때마다 자동 장치 해상도를 실행할 수 있습니다.

수동으로 지정하면 야간 자동 장치 해결이 비활성화됩니다.

DNS 처리 옵션

DNS 처리 옵션을 사용하여 다음 기능을 선택할 수 있습니다.

- DNS 조회 결과 처리가 활성화되면 DNS 이름 목록을 추가하여 확인된 장치에 추가할 수 있습니다.
- DNS 조회를 사용하여 NFS 공유에 액세스하는 iSCSI 초기자 및 호스트에 대해 자동 호스트 확인을 설정하려면 ""IP 자동 해상도:""를 선택할 수 있습니다. 이 옵션을 지정하지 않으면 FC 기반 해상도만 수행됩니다.
- 호스트 이름에 밑줄을 허용하고 결과에 표준 포트 별칭 대신 "연결됨" 별칭을 사용하도록 선택할 수 있습니다.

특정 스토리지 및 테이프 공급업체 포함 또는 제외

자동 해결을 위해 특정 스토리지 및 테이프 공급업체를 포함하거나 제외할 수 있습니다. 예를 들어 특정 호스트가 기존 호스트가 되어 새 환경에서 제외되어야 한다는 것을 알고 있는 경우 특정 공급업체를 제외할 수 있습니다. 이전에 제외했지만 더 이상 제외하지 않으려는 공급업체를 다시 추가할 수도 있습니다.



테이프에 대한 디바이스 확인 규칙은 해당 WWN의 공급업체가 공급업체 기본 설정에서 * 테이프 전용 * 으로 설정된 WWN에만 적용됩니다.

정규식 예

정규식을 소스 명명 전략으로 선택한 경우 정규식 예제를 OnCommand Insight 자동 확인 메서드에서 사용하는 자체 식에 대한 가이드로 사용할 수 있습니다.

정규식 서식 지정

OnCommand Insight 자동 확인을 위한 정규식을 만들 때 이라는 필드에 값을 입력하여 출력 형식을 구성할 수 있습니다 FORMAT.

기본 설정은 입니다 \1\ 즉, 정규식과 일치하는 영역 이름이 정규식에 의해 만들어진 첫 번째 변수의 내용으로 대체됩니다. 정규식에서 변수 값은 괄호를 사용하여 만들어집니다. 괄호를 여러 개 사용하면 변수가 왼쪽에서 오른쪽으로 숫자로 참조됩니다. 변수는 출력 형식으로 어떤 순서로든 사용할 수 있습니다. 상수 텍스트는 에 추가하여 출력에도 삽입할 수 있습니다 FORMAT 필드에 입력합니다.

예를 들어 이 영역 명명 규칙에 다음과 같은 영역 이름이 있을 수 있습니다.

```
[Zone number]_[data center]_[hostname]_[device type]_[interface number]
```

- S123_Miami_hostname1_filer_FC1
- S14_Tampa_hostname2_switch_FC4
- S3991_Boston_hostname3_windows2K_FC0
- S44_Raleigh_hostname4_Solaris_FC1

출력을 다음 형식으로 지정할 수 있습니다.

```
[hostname]-[data center]-[device type]
```

이렇게 하려면 변수에 호스트 이름, 데이터 센터 및 장치 유형 필드를 캡처하여 출력에 사용해야 합니다. 다음과 같은 정규식을 사용하면 됩니다.

```
.*?_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_([a-zA-Z0-9]+)_.*
```

괄호는 세 개이므로 변수가 됩니다 \1, \2 및 \3 자동으로 채워집니다.

그런 다음 다음 다음 다음 다음 형식을 사용하여 원하는 형식으로 출력을 받을 수 있습니다.

```
\2-\1-\3
```

출력은 다음과 같습니다.

```
hostname1-Miami-filer
hostname2-Tampa-switch
hostname3-Boston-windows2K
hostname4-Raleigh-solaris
```

변수 사이의 하이픈은 서식이 지정된 출력에 삽입된 상수 텍스트의 예를 제공합니다.

영역 이름을 보여 주는 예제 1

이 예제에서는 정규식을 사용하여 영역 이름에서 호스트 이름을 추출합니다. 다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- S0032_myComputer1Name - HBA0
- S0434_myComputer1Name - HBA1
- S0432_myComputer1Name - HBA3

호스트 이름을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
S[0-9]+_([a-zA-Z0-9]*)[_-]HBA[0-9]
```

결과는 S로 시작하는 모든 영역과 일치하며 그 뒤에 숫자 조합, 밑줄, 영숫자 호스트 이름(myComputer1Name), 밑줄 또는 하이픈, 대문자 HBA 및 단일 숫자(0-9)가 옵니다. 호스트 이름만 *1 * 변수에 저장됩니다.

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- "S"는 영역 이름을 나타내고 식을 시작합니다. 이것은 영역 이름의 시작 부분에 있는 "S"만 일치합니다.
- 괄호 안의 문자 [0-9]는 "S" 뒤에 오는 문자가 0에서 9 사이의 숫자여야 함을 나타냅니다.
- 기호(+)는 이전 대괄호 안의 정보가 한 번 이상 존재해야 함을 나타냅니다.
- 밑줄(_)은 S 다음에 오는 숫자는 영역 이름에 밑줄만 사용해야 함을 의미합니다. 이 예제에서 영역 명명 규칙은 밑줄을 사용하여 호스트 이름과 영역 이름을 구분합니다.
- 필요한 밑줄 뒤에 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 괄호 문자 [A-Za-Z0-9]는 일치하는 문자가 대/소문자를 불문하고 모든 문자와 숫자임을 나타냅니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- 괄호 문자 [_-](밑줄 및 대시)는 영숫자 패턴 뒤에 밑줄이나 대시를 사용해야 함을 나타냅니다.
- 정규식의 문자 HBA는 영역 이름에 이 정확한 문자 시퀀스가 발생해야 함을 나타냅니다.
- 괄호 안의 마지막 문자 세트 [0-9]는 0에서 9 사이의 한 자리 숫자와 일치합니다.

예 2

이 예에서는 첫 번째 밑줄 "_"까지 건너뛰고, 그 다음 E와 모든 것을 두 번째 "_"까지 일치시킨 다음 그 이후의 모든 내용을 건너뛰니다.

- 영역: * Z_E2FHDBS01_E1NETAPP
- 호스트 이름: * E2FHDBS01
- 등록: * .? (E.?) .*?

예 3

정규식(아래)의 마지막 섹션 주위의 괄호 "()"는 호스트 이름인 부분을 식별합니다. VSAN3을 호스트 이름으로 사용하려는 경우 _([A-Za-Z0-9]).* 입니다

- 영역: * A_VSAN3_SR48KENT_A_CX2578_SPA0
- 호스트 이름: * SR48KENT
- 등록: * _[a-zA-Z0-9]+_([a-zA-Z0-9]).*

예제 4에서는 보다 복잡한 명명 패턴을 보여 줍니다

다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- myComputerName123-HBA1_Symm1_FA3
- myComputerName123-HBA2_Symm1_FA5
- myComputerName123-HBA3_Symm1_FA7

이러한 항목을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
([a-zA-Z0-9]*)_.*
```

를 클릭합니다 \1 변수에는 만 포함됩니다 myComputerName123 이 식을 사용하여 계산한 후

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 괄호 문자 [A-Za-Z0-9]는 모든 문자(대/소문자 구분 없음) 또는 숫자가 일치함을 의미합니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- 정규식의 _ (밑줄) 문자는 영역 이름에 앞의 대괄호와 일치하는 영숫자 문자열 바로 뒤에 밑줄이 있어야 함을 의미합니다.
- 를 클릭합니다. (마침표)는 임의의 문자(와일드카드)와 일치합니다.
- 별표(*)는 이전 기간 와일드카드가 0번 이상 발생할 수 있음을 나타냅니다.

즉, 조합을 나타냅니다. * 모든 문자를 임의의 횟수만큼 나타냅니다.

예제 5 패턴 없이 영역 이름을 표시합니다

다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- myComputerName_HBA1_Symm1_FA1
- myComputerName123_HBA1_Symm1_FA1

이러한 항목을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
(.*?)_.*
```

1 변수는 첫 번째 영역 이름 예제에서 *myComputerName* 또는 *myComputerName123*(두 번째 영역 이름 예제의 경우)를 포함합니다. 따라서 이 정규식은 첫 번째 밑줄 이전의 모든 것과 일치합니다.

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 마침표 별표(.*)는 임의의 문자(횟수)와 일치합니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- ? Character는 greedy가 아닌 문자와 일치하는 항목을 만듭니다. 이렇게 하면 마지막 밑줄이 아니라 첫 번째 밑줄에서의 일치가 중지됩니다.
- 문자 _.* 는 발견된 첫 번째 밑줄과 그 뒤에 나오는 모든 문자와 일치합니다.

예제 6 컴퓨터 이름을 패턴으로 표시합니다

다음 영역 이름과 유사한 항목이 있는 경우 정규식을 만들 수 있습니다.

- storage1_Switch1_myComputerName123A_A1_FC1
- storage2_Switch2_myComputerName123B_A2_FC2 를 참조하십시오
- storage3_Switch3_myComputerName123T_A3_FC3

이러한 항목을 캡처하는 데 사용할 수 있는 정규식은 다음과 같습니다.

```
.*?_.*?_([a-zA-Z0-9]*[ABT])_.*
```

영역 명명 규칙에 더 많은 패턴이 있으므로 위의 식을 사용하여 A, AB 또는 AT로 끝나는 호스트 이름(예: myComputerName)의 모든 인스턴스(예: \1 변수에 해당 호스트 이름을 지정)와 일치시킬 수 있습니다.

정규식은 다음과 같이 해당 구성 요소로 나눌 수 있습니다.

- 마침표 별표(.*)는 임의의 문자(횟수)와 일치합니다.
- ? Character는 greedy가 아닌 문자와 일치하는 항목을 만듭니다. 이렇게 하면 마지막 밑줄이 아니라 첫 번째 밑줄에서의 일치가 중지됩니다.
- 밑줄 문자는 영역 이름의 첫 번째 밑줄과 일치합니다.

- 따라서 첫 번째. *_ 조합은 첫 번째 영역 이름 예제에서 *storage1_* 문자와 일치합니다.
- 두 번째. *_ 조합은 첫 번째 과 같이 동작하지만 첫 번째 영역 이름 예제에서 *_Switch1__*과 일치합니다.
- 괄호는 안에 포함된 패턴이 \1 변수에 저장됨을 나타냅니다.
- 괄호 문자 [A-zA-Z0-9]는 모든 문자(대/소문자 구분 없음) 또는 숫자가 일치함을 의미합니다.
- 괄호 뒤에 있는 * (별표)는 괄호 안의 문자가 0번 이상 발생했음을 나타냅니다.
- 정규식 [ABT]의 괄호 문자는 영역 이름의 단일 문자와 일치해야 하며 A, B 또는 T여야 합니다
- 괄호 뒤에 있는 _ (밑줄)은 [ABT] 문자 일치 뒤에 밑줄을 추가해야 함을 나타냅니다.
- 마침표 별표(. *)는 임의의 문자(횟수)와 일치합니다.

따라서 이 결과로 \1 변수에 다음과 같은 영숫자 문자열이 포함됩니다.

- 앞에 몇 개의 영숫자 문자와 두 개의 밑줄이 있습니다
- 뒤에 밑줄과 영숫자 문자를 차례로 사용했습니다.
- 세 번째 밑줄 앞에 A, B 또는 T의 마지막 문자가 있습니다.

예 7

- 영역: `*myComputerName123_HBA1_Symm1_FA1`
- 호스트 이름: `*myComputerName123`
- 등록: `*([a-zA-Z0-9]+)_.*`

예 8

이 예제에서는 First _ 앞에 있는 모든 항목을 찾습니다.

- 영역: `*MyComputerName_HBA1_Symm1_FA1`

`MyComputerName123_HBA1_Symm1_FA1`

- 호스트 이름: `*MyComputerName`
- 등록: `*(.?)*_.`

예 9

이 예제에서는 1_ 이후의 모든 것과 두 번째 _ 까지의 모든 것을 찾습니다.

- 영역: `*z_MyComputerName_StorageName`
- 호스트 이름: `*MyComputerName`
- 등록: `*.?(.?) .*?`

예 10

이 예제에서는 영역 예제에서 "MyComputerName123"을 추출합니다.

- 영역: *Storage1_Switch1_MyComputerName123A_A1_FC1

Storage2_Switch2_MyComputerName123B_A2_FC2

Storage3_Switch3_MyComputerName123T_A3_FC3

- 호스트 이름: *MyComputerName123
- 등록: * .? .? ([a-zA-Z0-9]+) [ABT] _ .

예 11

- 영역: *Storage1_Switch1_MyComputerName123A_A1_FC1
- 호스트 이름: *MyComputerName123A
- 등록: * .? .? ([a-zA-Z0-9]+) . *?

예 12

^(circumflex 또는 caret) * 대괄호 안에 * * 는 식을 부정합니다. 예를 들어 [{캐럿} FF]는 대문자 또는 소문자 F를 제외한 모든 것을 의미하고 [{캐럿} a-z]는 소문자 a ~ z를 제외한 모든 것을 의미합니다. 위의 경우 _ 를 제외한 모든 것을 의미합니다. format 문은 출력 호스트 이름에 "-"를 추가합니다.

- 영역: *mhs_apps44_d_A_10a0_0429
- 호스트 이름: *mhs-apps44-d
- 등록: * ([^_])_([AB]) . *+OnCommand Insight 형식:

([^_])_() . *OnCommand Insight 형식:

예 13

이 예제에서 저장소 별칭은 "\"로 구분되며 표현식은 "\"를 사용하여 문자열에 실제로 "\"가 사용되고 있으며 해당 별칭이 표현식 자체의 일부가 아닌 것을 정의해야 합니다.

- 스토리지 별칭: * \Hosts\E2DOC01C1\E2DOC01N1
- 호스트 이름: *E2DOC01N1
- 등록: * \\ .? \\ .? \\ (. *?)

예 14

이 예에서는 영역 예에서 "PD-RV-W-AD-2"를 추출합니다.

- 영역: *PD_D-PD-RV-W-AD-2_01
- 호스트 이름: *PD-RV-W-AD-2
- 등록: * [^~] - (. - \d+) . +

예 15

이 경우 형식 설정은 호스트 이름에 "US-BV-"를 추가합니다.

- 영역: * SRV_USBVM11_F1
- 호스트 이름: * US-BV-M11
- 등록: * SRV_USBV([A-Za-z0-9]+)_F[12]
- 형식: * US-BV-\1

Insight 유지 관리

Insight를 처음 사용하는 경우 새로운 시스템을 설치했거나 시스템이 일정 시간 운영 중인지에 관계없이 Insight와 네트워크의 원활한 운영을 유지하기 위한 조치를 취해야 합니다. 주요 유지 관리 개념은 일반적으로 네트워크 변경 사항을 Insight에 수용해야 한다는 것입니다.

가장 일반적인 유지보수 작업은 다음과 같습니다.

- Insight 백업 유지 관리
- 만료된 Insight 라이선스를 업데이트하는 중입니다
- 데이터 소스 패치 조정
- 모든 획득 장치에서 Insight 버전을 업데이트합니다
- Insight에서 제거된 데이터 원본 삭제

Insight 관리

OnCommand Insight은 환경을 모니터링하여 위기 상황이 보고되기 전에 잠재적 문제를 조사할 수 있도록 합니다. 자산 대시보드는 요약 원형 차트, IOPS용 열 맵, 사용률이 가장 높은 10개의 스토리지 풀에 대한 대화형 차트를 제공합니다.

단계

1. Insight **Assets Dashboard** 를 열고 커서를 원형 차트 위로 이동하여 다음 세 가지 차트의 자산 분포를 검토합니다.
 - 공급업체별 용량 에는 각 공급업체의 총 스토리지 물리적 용량이 표시됩니다.
 - 계층별 용량은 각 스토리지 계층에 대해 사용 가능한 총 용량을 보여 줍니다.
 - 스위치 포트 원형 차트는 포트 제조업체를 표시하고 사용된 포트 비율을 표시합니다.
2. 환경 관련 정보 * 를 보고 사용 중인 환경의 용량, 용량 효율성, 사용된 FC 리소스 및 가상 인프라 통계에 대한 정보를 확인하십시오.
3. 스토리지 풀의 사용된 용량과 사용되지 않는 용량을 보려면 * 상위 10개 사용 풀 * 차트의 스토리지 풀 바 위에 커서를 놓습니다.
4. 스토리지 IOP * 히트맵에서 큰 텍스트(자산에 문제가 있음을 나타냄)로 표시되는 자산 이름을 클릭하여 해당 자산의 현재 상태를 요약하는 페이지를 표시합니다.

5. 자산 대시보드 * 의 오른쪽 아래 모서리에 있는 * 가상 머신 IOPS * 히트맵에서 큰 텍스트(자산에 문제가 있음을 나타냄)로 표시되는 자산 이름을 클릭하여 자산의 현재 상태를 요약하는 페이지를 표시합니다.
6. Insight 도구 모음에서 * Admin * 을 클릭합니다.
7. 빨간색 원으로 표시된 영역을 확인합니다.

OnCommand Insightfob UI에서는 잠재적인 문제가 빨간색 원으로 표시됩니다.

8. 데이터 소스 * 를 클릭하여 모니터링된 모든 데이터 소스 목록을 검사합니다.

빨간색 원으로 고정된 메시지가 포함된 * Status * 열이 있는 데이터 소스를 검사하고, * Impact * 가 High 또는 Medium 으로 나열됩니다. 이러한 항목은 테이블 상단에 있습니다. 이러한 데이터 소스의 문제는 해결해야 하는 네트워크의 중요한 부분에 영향을 미칩니다.

9. Insight를 실행하는 각 IP 주소의 상태를 확인하고 필요한 경우 획득 장치를 다시 시작하려면 * Acquisition Units * (획득 단위)를 클릭합니다
10. Insight 서버의 상위 인스턴스 모니터링을 보려면 * 상태 * 를 클릭하십시오.

OnCommand Insight 시스템 상태 모니터링

Insight 시스템 구성 요소의 현재 상태를 주기적으로 확인하여 각 구성 요소의 상태를 표시하고 문제가 있을 경우 알려줍니다.

단계

1. Insight트위브 UI에 로그인합니다.
2. Admin * 을 클릭하고 * Health * 를 선택합니다.

상태 페이지가 표시됩니다.

3. 빨간색 원 앞에 있는 * Details * 열의 주의 상태에 특히 주의를 기울인 구성 요소의 현재 상태에 대한 요약을 봅니다. 이 열은 즉각적인 주의가 필요한 문제를 나타냅니다.

상태 페이지에는 시스템 구성에 따라 다음과 같은 Insight 구성 요소 중 일부 또는 전체에 대한 정보가 표시됩니다.

구성 요소	테스트	세부 정보	표시됩니다
획득	재고 데이터 처리	로컬 획득 장치의 상태입니다	동시 폴링 데이터 소스의 수가 실행 풀 최대값의 75% 미만일 경우 ""OK""(기본값: 30). 사용이 75%를 초과하는 경우 "Acquisition is busy(획득 사용 중)", 폴링 간격을 늘리거나 원격 획득 장치를 더 추가하는 것이 좋습니다.

DWH	백업	데이터 웨어하우스 예약 백업의 상태입니다	DWH 예약 백업이 활성화된 경우 "OK(확인)" 및 마지막으로 성공한 DWH 백업 시간 그렇지 않으면 발견된 오류에 대한 정보가 표시됩니다.
DWH	ETL	데이터 웨어하우스 ETL의 상태입니다	"OK"와 마지막 성공한 DWH 빌드 시간(오류 없음). 그렇지 않으면 발견된 오류에 대한 정보가 표시됩니다.
서버	ASUP	ASUP 상태	<p>""ASUP 활성화"" 및 가능한 경우 마지막으로 성공한 전화집 시간.</p> <p>"ASUP Failed"(ASUP 실패) - phonehome이 활성화되어 있지만 문제가 발생한 경우</p> <p>백업 디렉토리가 유효하지 않은 경우 + "잘못된 백업 위치"</p> <p>+ 마지막으로 성공한 전화 시간과 마지막으로 실패한 시도(있는 경우)를 표시합니다.</p> <p>폰홈이 비활성화된 경우 + ""ASUP 비활성화".</p>
서버	자동 해상도	자동 장치 해상도 상태입니다	<p>오류가 없으면 OK를 누릅니다. 확인 오류로 인해 해결 과정이 진행되지 않으면 자동 해결이 차단됩니다.</p> <p>일반 디바이스의 75% 미만이 식별될 수 있는 경우 + ""낮은 성공률""</p>

서버	Elasticsearch(Elasticsearch)	탄력적인 검색 데이터 저장소의 상태입니다	<p>오류가 없으면 OK를 누릅니다. "서비스를 사용할 수 없습니다."라는 메시지가 표시됩니다.</p> <p>둘 이상의 노드가 감지되면 + "클러스터 모드 감지됨"</p> <p>사용된 힙 공간이 85%를 초과하는 경우 + "높은 메모리 사용률"</p> <p>"상태: 빨간색"은 탄성 검색에서 보고된 오류를 나타냅니다. 오류에 대한 정보를 표시하고 고객 지원 센터에 문의할 것을 권장합니다.</p>
서버	CPU	Insight CPU 사용량	CPU 부하가 65% 미만이면 "OK" 시스템 CPU 부하가 높습니다. CPU 부하를 줄입니다. CPU 로드가 65%보다 큰 경우
서버	디스크 공간	디스크 공간의 상태입니다	디스크 여유 공간, Insight에서 사용 중인 디스크 공간 및 Insight용으로 예약된 권장 디스크 공간 디스크 사용률이 80%를 초과할 경우 ""디스크 공간 부족"".
서버	이벤트 버스	EventBus의 상태입니다	EventBus는 비어 있습니다. EventBus 대기열이 비어 있으면 EventBus 대기열 상태를 표시합니다.
서버	재고 데이터 처리	Insight 서버의 인벤토리 데이터 처리 기능 상태입니다	Insight 서버가 사용 중이 아니면 "OK"입니다. 서버가 마지막 시간의 75% 이상 사용 중이면 서버가 사용 중입니다. 예서는 데이터 소스를 더 추가하지 않을 것을 권장하며 환경을 여러 서버로 분할할 것을 권장합니다.

서버	MySQL	MySQL 데이터베이스의 상태입니다	<p>문제가 발견되지 않으면 OK. "데이터베이스에 성능 문제가 있습니다. 일부 쿼리는 느린 쿼리 수가 5%를 초과할 경우 "(을) 실행하는 데 너무 오래 걸립니다.</p> <p>데이터베이스 로그 파일은 지난 한 시간 동안 <size>보다 더 많이 성장했습니다. 오류 로그가 20KB를 초과할 경우 MySQL 로그 파일 ""을 확인하십시오.</p>
서버	성능 아카이브	성능 아카이브의 상태입니다	<p>"Performance archive is enabled" 또는 "Performance archive is not enabled".</p>
서버	물리적 메모리	물리적 메모리의 상태입니다	<p>메모리 사용량이 85% 미만일 경우 "OK". "메모리 사용량이 높습니다. 시스템 안정성을 위해 전체 메모리 공간을 줄일 수 있습니다."</p>
서버	서비스 팩	서비스 팩 가용성	<p>Insight에서 서비스 팩을 사용할 수 있는지 여부를 표시합니다. 서비스 팩을 사용할 수 있는 경우 에 지침이 표시됩니다.</p>
서버	사용 정보	사용 정보 전송 상태	<p>NetApp에 사용 정보 전송이 설정되었는지 여부를 표시합니다. 는 사용하지 않는 경우 활성화할 것을 권장합니다. 마지막으로 시도했거나 마지막으로 성공한 전송 시간을 표시합니다.</p> <p>+ 발생한 문제에 대한 정보를 표시합니다.</p>

서버	위반	미결 위반 상태	<p>개방형 위반 건수가 위반 건수의 75% 미만이면 OK. "허용되는 최대 공개 위반 수는 <number>"입니다. 위반 허용 횟수가 위반 제한의 75%를 초과하는 경우. 에서는 성능 정책 구성을 검토할 것을 권장합니다.</p> <p>위반 건수가 위반 한도인 경우 위반 관리자가 차단됩니다.</p> <p>+위반 관리자는 새로운 위반 사항을 작성할 수 없으며 성능 정책 구성을 검토할 것을 권장합니다.</p>
서버	주간 백업	주별 백업의 상태입니다	<p>주 단위 백업이 활성화된 경우 "OK(확인)", 그렇지 않으면 "Weekly backup is not enabled(주간 백업이 활성화되지 않음)"가 표시됩니다.</p>

비활성 장치를 삭제하는 중입니다

비활성 상태인 장치를 삭제하면 데이터를 보다 깨끗하게 유지하고 탐색하기 쉽습니다.

이 작업에 대해

Insight에서 비활성 장치를 삭제하려면 다음을 수행합니다.

단계

1. 새 쿼리를 만들거나 기존 쿼리를 엽니다.
2. *generic device*, *host*, *storage*, *switch* 또는 *_tape_asset* 유형을 선택합니다.
3. 필터 추가 * 가 활성 * 이고 필터를 * 아니요 * 로 설정합니다.

결과 테이블에는 활성 상태가 아닌 자산만 표시됩니다.

4. 삭제할 장치를 선택합니다.
5. Actions * 버튼을 클릭하고 * Delete Inactive Devices * 를 선택합니다.

비활성 장치는 삭제되고 더 이상 Insight에 표시되지 않습니다.

시스템 및 사용자 작업 감사

예기치 않은 변경 내용을 찾으려면 OnCommand Insight 시스템 및 해당 사용자 작업의 감사 추적을 볼 수 있습니다. 감사 로그 메시지는 감사 페이지에 표시될 뿐만 아니라 syslog에 선택적으로 보낼 수 있습니다.

이 작업에 대해

Insight는 다음을 비롯하여 스토리지 네트워크 또는 스토리지 관리에 영향을 미치는 모든 사용자 활동에 대한 감사 항목을 생성합니다.

- 로그인 중입니다
- 경로를 승인 또는 승인 해제하는 중입니다
- 승인된 경로 업데이트 중
- 글로벌 정책 또는 임계값 설정
- 데이터 소스 추가 또는 제거
- 데이터 소스 시작 또는 중지
- 데이터 소스 속성을 업데이트하는 중입니다
- 작업 추가, 편집 또는 삭제
- 응용 프로그램 그룹을 제거하는 중입니다
- 장치 ID 식별 또는 변경
- 사용자를 생성합니다
- 사용자를 삭제합니다
- 사용자 역할 변경
- 사용자 수정(Guest à Admin)
- 사용자 로그아웃(강제 로그아웃 또는 수동 로그아웃)
- 획득 장치 삭제
- 라이선스 업데이트
- 백업 설정 중
- 백업을 사용하지 않도록 설정합니다
- ASUP 활성화(동일한 페이지에서 프록시 활성화 가 감사 로그에 보고됨)
- ASUP 비활성화(동일한 페이지에서 프록시 비활성화가 감사 로그에 보고됨)
- 보안 - 키를 다시 누르고 시스템 암호를 변경합니다.
- 자산의 주식 제거/추가
- CAC 사용자 로그인/로그오프
- CAC 사용자 세션 시간 초과

단계

1. 브라우저에서 Insight를 엽니다.
2. Admin * 을 클릭하고 * Audit * 을 선택합니다.

감사 페이지에는 표에 감사 항목이 표시됩니다.

3. 테이블에서 다음 세부 정보를 볼 수 있습니다.

- 시간 *

변경 날짜 및 시간입니다

- * 사용자 *

감사 항목과 연결된 사용자의 이름입니다

- * 역할 *

게스트, 사용자 또는 관리자인 사용자 계정의 역할

- * IP *

감사 항목과 연결된 IP 주소입니다

- * 작업 *

감사 항목의 작업 유형입니다

- * 세부 정보 *

감사 항목의 세부 정보입니다

데이터 소스 또는 애플리케이션과 같이 리소스에 영향을 미치는 사용자 활동이 있는 경우 세부 정보에는 리소스의 랜딩 페이지에 대한 링크가 포함됩니다.



데이터 소스가 삭제되면 데이터 소스와 관련된 사용자 활동 세부 정보에 더 이상 데이터 소스의 랜딩 페이지에 대한 링크가 포함되지 않습니다.

4. 특정 기간(1시간, 3시간, 24시간, 3일, 7일)을 선택하여 감사 항목을 표시할 수 있습니다. Insight에서 선택한 기간 동안 최대 1000건의 위반 사례를 보여줍니다.

한 페이지에 맞는 것보다 많은 데이터가 있는 경우 표 아래의 페이지 번호를 클릭하여 페이지별로 데이터를 탐색할 수 있습니다.

5. 테이블의 열 정렬 순서를 열 머리글의 화살표를 클릭하여 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경하고 기본 정렬 순서로 돌아가려면 다른 열 머리글을 클릭합니다.

기본적으로 테이블에는 항목이 내림차순으로 표시됩니다.

6. 필터 * 상자를 사용하여 표에 원하는 항목만 표시할 수 있습니다.

사용자가 감사 항목만 표시합니다 `izzyk``를 입력합니다 ``izzyk` 필터 * 상자에 입력합니다.



네트워크 위반 모니터링

Insight에서 성능 정책에 설정된 임계값으로 인해 위반을 생성하는 경우 위반 대시보드를 사용하여 해당 위반 사항을 볼 수 있습니다. 대시보드에는 네트워크에서 발생하는 모든 위반 사항이 나열되며 이를 통해 문제를 찾아 해결할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 엽니다.
2. Insight 도구 모음에서 * 대시보드 * 를 클릭하고 * 위반 대시보드 * 를 선택합니다.



위반 대시보드가 표시됩니다.

3. Policies * 파이 차트에서는 다음과 같은 방법으로 * 위반 항목을 사용할 수 있습니다.
 - 특정 정책 또는 메트릭에 대해 발생한 총 위반의 비율을 표시하기 위해 차트의 임의 슬라이스 위에 커서를 배치할 수 있습니다.
 - 차트의 한 조각을 "확대"하려면 차트 조각을 클릭하면 나머지 차트에서 멀리 이동하여 해당 슬라이스를 더 강조하고 연구할 수 있습니다.
 - 를 클릭할 수 있습니다.  아이콘을 클릭하여 원형 차트를 전체 화면 모드로 표시하고 을 클릭합니다.  다시 한 번 클릭하여 원형 차트를 최소화합니다. 파이 차트는 최대 5개의 조각을 포함할 수 있으므로 위반을 생성하는 6개의 정책이 있는 경우 Insight는 5번째 슬라이스와 6번째 슬라이스를 ""기타" 슬라이스로 결합합니다. Insight는 가장 많은 위반 사항을 첫 번째 슬라이스에 할당하고 두 번째 슬라이스에 가장 많은 위반 사항을 할당합니다.



4. 다음과 같은 방법으로 * 위반 이력 * 차트를 사용할 수 있습니다.


- 차트 위에 커서를 놓으면 특정 시간에 발생한 총 위반 수와 지정된 각 메트릭에 대해 발생한 총 위반 횟수를 표시할 수 있습니다.
- 범례 레이블을 클릭하여 범례와 관련된 데이터를 차트에서 제거할 수 있습니다.

범례를 클릭하여 데이터를 다시 표시합니다.

- 를 클릭할 수 있습니다.  아이콘을 클릭하여 차트를 전체 화면 모드로 표시하고 을 클릭합니다.  다시 한 번 클릭하여 원형 차트를 최소화합니다.

5. 다음과 같은 방법으로 * 위반 표 * 를 사용할 수 있습니다.

- 를 클릭할 수 있습니다.  아이콘을 클릭하여 전체 화면 모드로 테이블을 표시하고 을 클릭합니다.  다시 한 번 클릭하여 원형 차트를 최소화합니다.


창 크기가 너무 작은 경우 위반 테이블에는 세 개의 열만 표시되지만 을 클릭하면 표시됩니다. , 추가 열(최대 7개)이 표시됩니다.

- 특정 기간(* 1h *, * 3h *, * 24h *, * 3D *, * 7d *, 및 * 30d *), Insight에서 선택한 기간 동안 최대 1000건의 위반 사례를 보여줍니다.
- 필터 * 상자를 사용하여 원하는 위반만 표시할 수 있습니다.
- 열 머리글의 화살표를 클릭하여 테이블의 열 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다. 기본 정렬 순서로 돌아가려면 다른 열 머리글을 클릭합니다.

기본적으로 테이블에는 위반사항이 내림차순으로 표시됩니다.

- ID 열에서 위반을 클릭하여 위반 기간 동안 자산 페이지를 표시할 수 있습니다.
- 설명 열에서 리소스 링크(예: 스토리지 풀 및 스토리지 볼륨)를 클릭하여 해당 리소스와 연결된 자산 페이지를 표시할 수 있습니다.
- 정책 열에서 성능 정책 링크를 클릭하여 정책 편집 대화 상자를 표시할 수 있습니다.

너무 많거나 너무 많은 위반이 발생하는 경우 정책의 임계값을 조정할 수 있습니다.

- 한 페이지에 맞는 것보다 많은 데이터가 있는 경우 페이지 번호를 클릭하여 페이지별로 데이터를 탐색할 수 있습니다.
- 를 클릭할 수 있습니다  을 클릭하여 위반 사항을 취소합니다.

획득 장치 상태

Acquisition Unit(획득 장치) 화면에서는 상태 및 현재 오류를 포함하여 모든 획득 장치를 볼 수 있습니다.

서버에 연결된 Insight 획득 장치의 상태가 * Admin * > * Acquisition Units * (획득 단위) 표에 표시됩니다. 이 표에는 각 획득 장치에 대한 다음 정보가 표시됩니다.

- * 이름 *
- * IP *
- * Status * 는 획득 장치의 작동 상태입니다.
- **Last** 보고에 보고됨 획득 장치에 연결된 데이터 소스가 마지막으로 보고된 시간을 표시합니다.
- * 참고 * AU와 관련된 사용자 입력 메모를 표시합니다.

목록의 획득 장치에 문제가 있는 경우 Status(상태) 필드에 문제에 대한 간략한 정보가 포함된 빨간색 원이 표시됩니다. 획득 장치 문제는 데이터 수집에 영향을 줄 수 있으므로 조사해야 합니다.

획득 장치를 다시 시작하려면 장치 위로 마우스를 가져가 나타나는 *Restart Acquisition Unit*(획득 장치 재시작) 버튼을 클릭합니다.

텍스트 메모를 추가하려면 획득 장치 위로 마우스를 가져가 나타나는 *Add Note* 단추를 클릭합니다. 가장 최근에 입력한 메모만 표시됩니다.

Insight 데이터베이스를 복원하는 중입니다

검증된 백업 파일에서 Insight 데이터베이스를 복원하려면 문제 해결 옵션을 사용합니다. 이 작업은 현재 OnCommand Insight 데이터를 완전히 대체합니다.

시작하기 전에

- 모범 사례:** OnCommand Insight 데이터베이스를 복원하기 전에 수동 백업 프로세스를 사용하여 현재 데이터베이스의 복사본을 만듭니다. 복원하려는 백업 파일 확인 복원하려는 파일이 포함된 백업이 성공했는지 확인합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 문제 해결 * 을 클릭합니다.

Send / Collect data

Action	Description
<button>Back up</button>	Back up the database (configuration and performance) into a ZIP file.
<button>Bundle logs</button>	Collect all log files (including acquisition recordings) and bundle them into a ZIP file. Can be used to send data back to NetApp support when troubleshooting an issue with the software.
<button>Send ASUP now</button>	Forces an ad-hoc ASUP report. Can be used to allow NetApp support to get the latest support data when troubleshooting an issue with the software.

Restore a database

Select backup ▾ No file selected Restore

Warning: Your current database will be discarded!

Other tasks

Couldn't find what you are looking for? Connect to the old [OnCommand Insight Portal](#).
Need to send anonymous data back? Open the [scrub utilities](#).

3. 데이터베이스 복원 섹션의 * 백업 선택 * 메뉴에서 복원할 백업 파일을 선택합니다.
4. 복원 * 을 클릭합니다.
5. 모든 데이터가 교체된다는 경고가 나타나면 * OK * 를 클릭합니다

복원 작업의 상태가 복원 페이지에 표시됩니다.

만료된 라이선스를 업데이트하는 중입니다

하나 이상의 Insight 라이선스가 만료된 경우 원래 라이선스를 설치할 때와 동일한 절차를 사용하여 라이선스를 빠르게 업데이트할 수 있습니다.

단계

1. 메모장 같은 텍스트 편집기에서 NetApp Support에서 받은 새 라이선스 파일을 열고 라이선스 키 텍스트를 Windows 클립보드로 복사합니다.
2. 브라우저에서 OnCommand Insight를 엽니다.
3. 도구 모음에서 * Admin * 을 클릭합니다.
4. 설정 * 을 클릭합니다.
5. Licenses * 탭을 클릭합니다.
6. Update License * 를 클릭합니다.
7. 라이선스 키 텍스트를 * 라이선스 * 텍스트 상자에 복사합니다.
8. 업데이트(가장 일반적인) * 작업을 선택합니다.

이 작업을 수행하면 현재 활성화된 모든 Insight 라이선스에 새 라이선스가 추가됩니다.

9. 저장 * 을 클릭합니다.
10. Insight 소비 라이선싱 모델을 사용하는 경우 사용 섹션에서 * 사용 정보를 NetApp * 으로 전송 가능 확인란을 선택해야 합니다. 프록시는 환경에 맞게 적절히 구성 및 설정되어 있어야 합니다.

라이선스가 더 이상 규정을 준수하지 않습니다

Insight Licenses 페이지에서 "Not Compliant" 메시지가 표시되면 Insight에서 회사의 라이선스된 것보다 테라바이트를 더 많이 관리하고 있는 것입니다.

"규정을 준수하지 않음" 메시지는 회사가 현재 Insight에서 관리하는 것보다 TB를 적게 지불했다는 의미입니다. 관리 테라바이트 및 라이선스 용량(TB)의 차이가 규정 미준수 메시지 옆에 표시됩니다.

Insight 시스템의 작동은 영향을 받지 않지만, NetApp 담당자에게 문의하여 라이선스 범위를 늘리고 적절한 라이선스를 업데이트해야 합니다.

이전 **Insight** 버전의 라이선스 대체

이전 버전과 호환되지 않는 새 Insight 버전을 구입한 경우 이전 라이선스를 새 라이선스로 교체해야 합니다.

새 라이선스를 설치할 때 라이선스 키 텍스트를 저장하기 전에 * 바꾸기 * 작업을 선택해야 합니다.

서비스 팩을 적용하는 중입니다

서비스 팩을 주기적으로 사용할 수 있으며, OnCommand Insight의 수정 및 개선 사항을 활용할 수 있도록 서비스 팩을 적용할 수 있습니다.

시작하기 전에

- 서비스 팩 파일을 다운로드해야 합니다(예: 7.2service_pack_1.patch)를 참조하십시오.
- 모든 패치를 승인해야 합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 패치 * 를 클릭합니다.
3. 작업 버튼에서 * 패치 적용 * 을 선택합니다.
4. 데이터 소스 패치 적용 * 대화 상자에서 * 찾아보기 * 를 클릭하여 서비스 팩 파일을 찾습니다.
5. 패치 이름 *, * 설명 *, * 영향 받는 데이터 소스 유형 * 을 검사하여 데이터 소스가 영향을 받는지 여부를 확인하고, 서비스 팩에 포함된 개선 사항을 설명하는 * 세부 정보 * 를 확인합니다.
6. 선택한 서비스 팩이 올바르면 * 패치 적용 * 을 클릭합니다.

서비스 팩은 자동으로 승인되므로 추가 조치가 필요하지 않습니다.

특수 문제 해결 보고서 준비

Insight는 소프트웨어 설치 후 설정한 ASUP 시스템을 통해 NetApp 고객 지원 팀에 정보를 자동으로 전송합니다. 그러나 문제 해결 보고서를 만들고 지원 팀에 특정 문제에 대한 케이스를 개설할 수 있습니다.

Insight의 툴을 사용하여 수동 Insight 백업을 수행하고 로그를 번들로 묶어 NetApp 고객 지원 센터로 보낼 수 있습니다.

OnCommand Insight 데이터베이스를 수동으로 백업합니다

OnCommand Insight 데이터베이스에 대해 주별 백업을 사용하도록 설정한 경우 필요한 경우 데이터베이스를 복구하는 데 사용할 수 있는 복사본을 자동으로 생성합니다. 복원 작업 전에 백업을 생성하거나 NetApp 기술 지원 부서에 지원을 요청해야 하는 경우 백업을 생성할 수 있습니다. .zip 파일을 수동으로 선택합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 문제 해결 * 을 클릭합니다.
3. 데이터 보내기/수집 섹션에서 * 백업 * 을 클릭합니다.
4. 파일 저장 * 을 클릭합니다.
5. 확인 * 을 클릭합니다.

지원을 위한 로그 번들링

Insight 소프트웨어의 문제를 해결할 때 "gz" 형식을 사용하여 NetApp 고객 지원 본부에 전송되는 로그 및 수집 기록의 zip 파일을 신속하게 생성할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 문제 해결 * 을 클릭합니다.
3. 데이터 보내기/수집 섹션에서 * 번들 로그 * 를 클릭합니다.
4. 파일 저장 * 을 클릭합니다.
5. 확인 * 을 클릭합니다.

NetApp Support에 정보 전송

NetApp ASUP(자동화된 지원) 기능은 문제 해결 정보를 NetApp 고객 지원 팀에 직접 전송합니다. 특수 보고서를 강제로 전송할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭합니다.
2. 설정 * 을 클릭합니다.

3. Backup/ASUP * 탭을 클릭합니다.

4. 데이터 보내기/수집 영역에서 * ASUP 지금 전송 * 을 클릭하여 로그, 기록 및 백업을 NetApp 지원에 제출합니다.

Send / Collect data

Action	Description
<button>Back up</button>	Back up the database (configuration and performance) into a ZIP file.
<button>Bundle logs</button>	Collect all log files (including acquisition recordings) and bundle them into a ZIP file. Can be used to send data back to NetApp support when troubleshooting an issue with the software.
<button>Send ASUP now</button>	Forces an ad-hoc ASUP report. Can be used to allow NetApp support to get the latest support data when troubleshooting an issue with the software.

Restore a database

Select backup ▾ No file selected Restore

Warning: Your current database will be discarded!

Other tasks

Couldn't find what you are looking for? Connect to the old [OnCommand Insight Portal](#).
Need to send anonymous data back? Open the [scrub utilities](#).

전송을 지원하기 위해 데이터를 스크러빙합니다

보안 환경을 갖춘 고객은 NetApp 고객 서비스와 통신하여 데이터베이스 정보를 그대로 유지하면서 발생하는 문제를 해결해야 합니다. OnCommand Insight 스크럽 유틸리티를 사용하면 키워드 및 패턴의 포괄적인 사전 설정을 설정하여 중요한 데이터를 "정리"하고 스크러빙된 파일을 고객 지원 센터로 보낼 수 있습니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 스크럽 유틸리티 * 링크를 클릭합니다.

사전, 스크럽 데이터 및 빌드 사전의 조회, 사용자 지정 키워드, 정규식 등 여러 가지 스크럽 섹션이 있습니다.

.

+

.. 사전의 조회 섹션에서 대체 값을 표시할 코드를 입력하거나 값을 입력하여 해당 값을 대체하는 코드를 표시합니다.
참고: 조회를 수행하기 전에 지원 데이터에서 스크럽할 값을 식별하기 위해 사전을 * 구축 * 해야 합니다.

1. 지원 데이터에서 스크럽할 키워드를 직접 추가하려면 * 사용자 정의 키워드 * 섹션에서 메뉴 [사용자 정의 키워드 추가]를 클릭합니다. 키워드를 입력하고 * 저장 * 을 클릭합니다. 키워드가 사전에 추가됩니다.
2. 패턴(regex) * 을 확장합니다. 새 패턴을 입력하기 위한 대화 상자를 표시하려면 * 추가 * 를 클릭합니다.
3. 정규식을 사용하여 스크럽할 단어나 구를 식별하려면 * 정규식 * 섹션에 패턴이나 패턴을 입력합니다. 메뉴 클릭: 작업 [정규식 추가], 패턴의 이름 및 필드에 정규식을 입력하고 * 저장 * 을 클릭합니다. 사전에 정보가 추가되었습니다.



패턴은 정규식 캡처 그룹을 식별하기 위해 둥근 괄호로 묶어야 합니다.

4. 빌드 사전** 섹션에서 * 빌드 * 를 클릭하여 OnCommand Insight 데이터베이스에서 중요한 것으로 식별되는 모든 단어의 사전 컴파일을 시작합니다.

완료되면 개정된 사전을 사용할 수 있음을 알리는 메시지가 표시됩니다. 데이터베이스 설명에는 사전에 있는 키워드 수를 나타내는 줄이 포함됩니다. 사전에 있는 키워드의 정확성을 확인하십시오. 문제를 찾고 사전을 다시 빌드하려면 데이터베이스 블록에서 * 재설정 * 을 클릭하여 OnCommand Insight 데이터베이스에서 수집한 모든 키워드를 사전에서 제거합니다. 메시지가 표시되면 다른 키워드는 삭제되지 않습니다. 스크립 유틸리티로 돌아가서 사용자 지정 키워드를 다시 입력합니다.
5. 스크립 사전을 만든 후 이를 사용하여 로그, XML 또는 기타 텍스트 파일을 스크립하여 데이터를 익명으로 만들 수 있습니다.
6. 로그, XML 또는 기타 텍스트 파일을 스크립하려면 * 스크립 데이터 * 섹션에서 찾아보기를 클릭하여 파일을 찾은 다음 * 스크립 파일 * 을 클릭합니다.

고급 문제 해결

OnCommand Insight 구성을 완료하려면 고급 문제 해결 도구를 사용해야 합니다. 이러한 도구는 브라우저에서 실행되며 * Admin * > * Troubleshooting * 페이지에서 열립니다.

브라우저에서 고급 문제 해결 도구를 열려면 페이지 하단의 * 고급 문제 해결 * 링크를 클릭하십시오.

고급 문제 해결 도구를 사용하면 다양한 보고서, 시스템 정보, 설치된 패키지 및 로그를 볼 수 있을 뿐만 아니라 서버 또는 획득 장치 재시작, DWH 주석 업데이트, 주석 가져오기 등의 다양한 작업을 수행할 수 있습니다.

사용 가능한 모든 옵션은 고급 문제 해결 페이지를 참조하십시오.

동적 데이터를 무시할 시간 구성

OnCommand Insight에서 사용된 용량과 같은 동적 데이터 업데이트를 무시하는 시간을 구성할 수 있습니다. 기본 6시간이 사용되고 구성이 변경되지 않으면 기본 시간 이후까지 보고서가 동적 데이터로 업데이트되지 않습니다. 이 옵션은 동적 데이터만 변경될 때 업데이트를 지연하므로 성능이 향상됩니다.

이 작업에 대해

이 옵션에 값이 설정되어 있으면 OnCommand Insight는 다음 규칙에 따라 동적 데이터를 업데이트합니다.

- 구성을 변경하지 않고 용량 데이터가 변경되면 데이터가 업데이트되지 않습니다.
- 구성 변경 이외의 동적 데이터는 이 옵션에 지정된 시간 제한 이후에만 업데이트됩니다.
- 구성이 변경되면 구성 및 동적 데이터가 업데이트됩니다.

이 옵션의 영향을 받는 동적 데이터에는 다음이 포함됩니다.

- 용량 위반 데이터
- 파일 시스템에 할당된 용량 및 사용된 용량
- 하이퍼바이저
 - 가상 디스크 사용된 용량

- 가상 머신 사용 용량
- 내부 볼륨
 - 데이터 할당 용량
 - 사용된 데이터 용량
 - 중복제거 절약
 - 마지막으로 알려진 액세스 시간입니다
 - 마지막 스냅샷 시간입니다
 - 기타 사용된 용량
 - 스냅샷 수
 - 사용된 스냅샷 용량
 - 사용된 총 용량입니다
- iSCSI 세션 초기자 IP, 대상 세션 ID 및 초기자 세션 ID
- 사용된 용량 qtree 할당량
- 사용된 할당량 파일 및 사용된 용량
- 스토리지 효율성 기술, 이득/손실 및 잠재적 이득/손실
- 스토리지 풀
 - 사용된 데이터 용량
 - 중복제거 절약
 - 기타 사용된 용량
 - 사용된 스냅샷 용량
 - 사용된 총 용량입니다
- 볼륨
 - 중복제거 절약
 - 마지막으로 알려진 액세스 시간입니다
 - 사용된 용량

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 설정 * 탭을 클릭하고 획득 동적 속성 섹션에서 OnCommand Insight가 획득 동적 속성의 동적 데이터를 무시해야 하는 시간을 입력합니다.
4. 저장 * 을 클릭합니다.
5. (선택 사항) 획득 장치를 다시 시작하려면 * Restart Acquisition Unit(획득 장치 재시작) * 링크를 클릭합니다.

로컬 획득 장치를 다시 명시하면 모든 OnCommand Insight 데이터 소스 뷰가 다시 로드됩니다. 이 변경 사항은 다음 폴링 중에 적용되므로 획득 장치를 다시 시작할 필요가 없습니다.

고객 지원을 위한 로그를 생성하는 중입니다

고객 지원 본부에서 요청하는 경우 문제 해결을 위해 서버, 획득 또는 원격 로그를 생성합니다.

이 작업에 대해

NetApp 고객 지원을 요청하는 경우 이 옵션을 사용하여 로그를 생성합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 을 클릭합니다.
3. 고급 메뉴의 다음 페이지에서 * 문제 해결 * 링크를 클릭합니다.
4. 로그 * 탭을 클릭하고 다운로드할 로그 파일을 선택합니다.

로그를 열거나 로그를 로컬로 저장할 수 있는 대화 상자가 열립니다.

시스템 정보를 표시합니다

OnCommand Insight 서버가 배포된 시스템에 대한 Microsoft Windows IP 구성 정보를 표시할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 문제 해결 페이지에서 * 보고서 * 탭을 클릭합니다.
4. 시스템 정보 * 를 클릭합니다.

Windows IP 구성에는 호스트 이름, DNS, IP 주소, 서브넷 마스크, OS 정보 등의 정보가 포함됩니다. 메모리, 부팅 장치 및 연결 이름입니다.

설치된 **OnCommand Insight** 구성 요소 나열

설치된 OnCommand Insight 구성 요소의 목록을 표시할 수 있습니다. 그 중에는 인벤토리, 용량, 치수, 및 데이터 웨어하우스 뷰 고객 지원 팀에서 이 정보를 요청하거나 설치된 소프트웨어 버전과 설치 시기를 확인할 수 있습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 문제 해결 페이지에서 * 보고서 * 탭을 클릭합니다.
4. 설치된 소프트웨어 패키지 * 를 클릭합니다.

OnCommand Insight 데이터베이스의 개체 수를 확인하려면 배율 계산 기능을 사용합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 문제 해결 페이지에서 * 보고서 * 탭을 클릭합니다.
4. 계산된 배율 * 을 클릭합니다.

OnCommand Insight 서버를 다시 시작합니다

OnCommand Insight 서버를 다시 시작하면 페이지를 새로 고치고 OnCommand Insight 포털에 다시 로그인합니다.

이 작업에 대해



이 두 옵션은 모두 NetApp 고객 지원 본부의 요청에 따라 사용해야 합니다. 다시 시작하기 전에 확인 메시지가 없습니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 고급 메뉴의 다음 페이지에서 * 작업 * 탭을 클릭합니다.
4. 서버 재시작 * 을 클릭합니다.

마이그레이션 옵션을 사용하여 **MySQL** 데이터를 이동하는 중입니다

MySQL DATA 디렉토리를 다른 디렉터리로 마이그레이션 을 사용할 수 있습니다. 현재 데이터 디렉토리를 유지할 수 있습니다. 문제 해결 메뉴에서 마이그레이션 옵션을 사용하거나 명령줄을 사용할 수 있습니다. 이 절차에서는 * Troubleshooting * > * Migrate MySQL data * 옵션을 사용하는 방법에 대해 설명합니다.

이 작업에 대해

현재 데이터 디렉토리를 유지하는 경우 해당 디렉터리가 백업으로 유지되고 이름이 변경됩니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 고급 문제 해결 * 을 클릭합니다.
3. Actions * 탭을 선택합니다
4. Migrate MySQL Data * 를 선택합니다.

5. 데이터를 마이그레이션할 경로를 입력합니다.
6. 기존 데이터 디렉토리를 유지하려면 * 기존 데이터 디렉토리 유지 * 를 선택합니다
7. 마이그레이션 * 을 클릭합니다.

명령줄을 사용하여 **MySQL** 데이터를 이동하는 중입니다

MySQL DATA 디렉토리를 다른 디렉터리로 마이그레이션 을 사용할 수 있습니다. 현재 데이터 디렉토리를 유지할 수 있습니다. 문제 해결 메뉴에서 마이그레이션 옵션을 사용하거나 명령줄을 사용할 수 있습니다. 이 절차에서는 명령줄을 사용하는 방법에 대해 설명합니다.

이 작업에 대해

현재 데이터 디렉토리를 유지하는 경우 해당 디렉터리가 백업으로 유지되고 이름이 변경됩니다.

Migrate MySQL Data 유틸리티를 사용하거나 을 사용할 수 있습니다 `java -jar mysqldatamigrator.jar` 의 OnCommand Insight 경로에 있는 옵션 `\bin\mysqldatamigrator` 다음 매개변수를 사용해야 하는 경우:

- 필수 매개변수

- * -경로 *

데이터 폴더가 복사될 새 데이터 경로입니다.

- 선택적 매개 변수입니다

- * - myCnf <my .cnf file> *

CNF 파일의 경로입니다. 기본값은 입니다 `<install path>\mysql\my.cnf`. 기본 MySQL이 아닌 MySQL이 사용되는 경우에만 이 플래그를 사용하십시오.

- * -doBackup *

이 플래그를 설정하면 현재 데이터 폴더의 이름이 바뀌지만 삭제되지는 않습니다.

단계

1. 명령줄 톨은 여기에서 액세스할 수 있습니다. `<installation path> bin\mysqldatamigrator\mysqldatamigrator.jar`

사용 예

```
java -jar mysqldatamigrator.jar -path "C:\<new path>" -doBackup
```

주석 업데이트 적용

주석을 변경한 후 즉시 보고서에 사용하려면 힘 주석 옵션 중 하나를 사용합니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 작업 * 탭을 클릭합니다.
4. 다음 옵션 중 하나를 선택합니다.
 - * DWH 주석 * 을 업데이트하여 보고서에 데이터 웨어하우스의 주석 업데이트를 사용하도록 합니다.
 - * DWH 주석 업데이트(삭제됨) * 데이터 웨어하우스의 주석 업데이트(삭제된 개체 포함)를 보고서에 사용하도록 강제합니다.

서버 리소스의 상태 확인

이 옵션은 서버 메모리, 디스크 공간, OS, CPU 및 OnCommand Insight 데이터베이스 정보(InnoDB 데이터 크기 포함)와 데이터베이스가 상주하는 디스크 여유 공간 등의 OnCommand Insight 서버 정보를 표시합니다.

단계

1. Insight 도구 모음에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * OnCommand Insight 포털 * 링크를 클릭합니다.
3. 고급 메뉴의 다음 페이지에서 * 문제 해결 * 링크를 클릭합니다.
4. 서버 리소스 상태 * 를 클릭합니다.
 - 고급 OnCommand Insight 사용자의 경우: * 관리자는 일부 SQL 테스트를 실행하여 정보 요약 끝에 있는 버튼을 통해 데이터베이스와 서버의 응답 시간을 확인할 수 있습니다. 이 옵션은 서버 리소스가 부족할 경우 경고를 표시합니다.

고스트 데이터 소스 찾기

장치를 제거했지만 장치 데이터가 남아 있는 경우 고스트 데이터 원본을 찾아서 제거할 수 있습니다.

단계

1. 웹 UI에서 * Admin * 을 클릭하고 * Troubleshooting * 을 선택합니다.
2. 다른 작업 영역의 페이지 하단에서 * 고급 문제 해결 * 링크를 클릭합니다.
3. 보고서 * 탭에서 * 고스트 데이터 소스 * 링크를 클릭합니다.

OnCommand Insight는 장치 정보가 포함된 독창자 목록을 생성합니다.

누락된 디스크 모델을 추가하는 중입니다

알 수 없는 디스크 모델로 인해 획득에 실패한 경우 누락된 디스크 모델을 에 추가할 수 있습니다
new_disk_models.txt 촬영 후 다시 실행합니다.

이 작업에 대해

OnCommand Insight 획득을 통해 스토리지 디바이스를 폴링하는 과정에서 스토리지 디바이스의 디스크 모델이 읽힙니다. 공급업체가 Insight에서 알지 못하는 새로운 디스크 모델을 어레이에 추가하거나, Insight가 찾는 모델 번호와 스토리지 장치에서 반환된 모델 번호가 일치하지 않으면 해당 데이터 소스를 획득하지 못하고 오류가 발생합니다. 이러한 오류를 방지하려면 Insight에 알려진 디스크 모델 정보를 업데이트해야 합니다. 업데이트, 패치 및 유지 관리 릴리즈를 통해 새로운 디스크 모델이 Insight에 추가됩니다. 그러나 패치나 업데이트를 기다리는 대신 이 정보를 수동으로 업데이트할 수 있습니다.

OnCommand Insight는 5분마다 디스크 모델 파일을 읽기 때문에 입력한 새 데이터 모델 정보가 자동으로 업데이트됩니다. 변경 사항을 적용하기 위해 서버를 다시 시작할 필요는 없지만 서버 및 원격 획득 장치(RA)를 다시 시작하여 다음 업데이트 전에 변경 사항을 적용할 수 있습니다.

디스크 모델 업데이트가 에 추가됩니다 `new_disk_models.txt` 에 있는 파일 `<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` 디렉토리. 를 업데이트하기 전에 새 디스크 모델을 설명하는 데 필요한 정보를 파악합니다 `new_disk_models.txt` 파일. 파일의 정보가 부정확하면 잘못된 시스템 데이터가 생성되고 획득 실패를 초래할 수 있습니다.

Insight 디스크 모델을 수동으로 업데이트하려면 다음 지침을 따르십시오.

단계

1. 디스크 모델에 대한 적절한 정보를 찾습니다.
2. 텍스트 편집기를 사용하여 를 엽니다 `new_disk_models.txt` 파일.
3. 새 데이터 원본에 필요한 정보를 추가합니다.
4. 에 파일을 저장합니다
`<SANScreenInstallDir>\wildfly\standalone\deployments\datasources.war` 서버의 디렉터리입니다.
5. 를 백업합니다 `new_disk_models.txt` 파일을 안전한 위치에 보관합니다. 이후의 OnCommand Insight 업그레이드 중에 이 파일을 덮어씁니다. 디스크 모델 정보가 업그레이드된 파일에 없는 경우 다시 입력해야 합니다.

새 디스크 모델에 필요한 정보 찾기

디스크 모델 정보를 찾으려면 공급업체 및 모델 번호를 확인하고 인터넷 검색을 실행합니다.

이 작업에 대해

디스크 모델 정보는 인터넷 검색을 실행하는 것처럼 간단하게 찾을 수 있습니다. 검색하기 전에 공급업체 이름과 디스크 모델 번호를 기록해 두십시오.

단계

1. 공급업체의 데이터 시트 및/또는 드라이브 설치 설명서를 찾으려면 공급업체, 모델 및 문서 유형 ""PDF"에 대한 고급 인터넷 검색을 사용하는 것이 좋습니다. 이러한 데이터 시트는 일반적으로 공급업체 디스크 정보의 가장 좋은 소스입니다.
2. 공급업체 사양이 전체 모델 번호를 기반으로 필요한 모든 정보를 제공하는 것은 아닙니다. 공급업체 사이트에서 모델 번호 문자열의 여러 부분을 검색하여 모든 정보를 찾는 것이 유용합니다.
3. 디스크 공급업체 이름, 전체 모델 번호, 디스크 크기 및 속도 및 인터페이스 유형을 찾습니다. OnCommand Insight에서 새 디스크 모델을 정의하려면 다음 표를 참조하십시오.

이 필드의 경우:	다음 중 무엇입니까?	입력 내용:
모델 번호(aka Key)	필수 요소입니다	
공급업체	필수 요소입니다	
디스크 속도(RPM)	필수 요소입니다	
크기(GB)	필수 요소입니다	
인터페이스 유형(하나 선택)	필수 요소입니다	ATA, SATA, SATA2, SATA3, FC, SAS, FATA, SSD, 기타
탐색 시간(ms)	선택 사항	
최대 전송 속도(MB/sec)입니다	선택 사항	
인터페이스 전송 속도 (MB/sec)입니다	선택 사항	
공급업체/모델 정보 링크	선택 사항이지만 권장됩니다	

4. 에 해당 정보를 입력합니다 `new_disk_models.txt` 파일. 을 참조하십시오 ["new_disk_models.txt 파일의 내용입니다"](#) 형식, 순서 및 예제를 보려면

new_disk_models.txt 파일의 내용입니다

를 클릭합니다 `new_disk_models.txt` 파일에 필수 및 옵션 필드가 있습니다. 필드는 쉼표로 구분되므로 필드에 쉼표 _ 를 사용하지 마십시오.

검색 시간, 전송 속도 및 Additional_info를 제외한 모든 필드는 필수입니다. 가능한 경우, SUPPLICATION_info 필드에 공급업체/모델 웹 사이트 링크를 포함합니다.

텍스트 편집기를 사용하여 추가하려는 각 새 디스크 모델에 대해 다음 정보를 쉼표로 구분하여 이 순서로 입력하십시오.

1. * 키 *: 모델 번호 사용(필수)
2. * 벤더 *: 이름(필수)
3. * 모델 번호 *: 전체 번호(일반적으로 "키"와 동일한 값)(필수)
4. 디스크의 * rpm *: 예: 10000 또는 15000(필수)
5. * 크기 *: 용량(GB)(필수)
6. * 인터페이스 유형 *: ATA, SATA, FC, SAS, FATA, SSD, 기타(필수)
7. * 탐색 시간 *: ms(선택 사항)
8. * 잠재적 전송 속도 *: 잠재적인 전송 속도(MB/sec) 디스크 자체의 최대 전송 속도입니다. (선택 사항)

9. * 인터페이스 전송 속도 *: 호스트 간 전송 속도(MB/sec)(선택 사항)

10. * 추가 정보 *: 캡처하려는 추가 정보입니다. 가장 좋은 방법은 사양을 찾은 공급업체 페이지 링크를 참조(선택 사항)하는 것입니다.

비어 있는 옵션 필드의 경우 심표를 포함해야 합니다.

예제(각 줄은 공백 없이 한 줄에 하나씩):

ST373405,Seagate,ST373405,10000,73,FC,5.3,64,160,[http://www.seagate.com/staticfiles/support/disc/manuals/enterprise/cheetah/73\(LP\)/100109943e.pdf](http://www.seagate.com/staticfiles/support/disc/manuals/enterprise/cheetah/73(LP)/100109943e.pdf)

SLR5B-M400SS,HITACHI,SLR5B-M400SS,1000000,400,SSD,,,,,

X477_THARX04TA07,TOSHIBA,X477_THARX04TA07,7200,4000,SATA,9.5,,, <https://storage.toshiba.eu/export/sites/toshiba-sdd/media/products/datasheets/MG03ACAxxxY.pdf>

환경을 모니터링합니다

Insight를 사용하면 환경의 문제를 예방하고 잠재적인 문제를 신속하게 해결할 수 있습니다.

자산 페이지 데이터

자산 페이지에서는 성능 문제 해결 데이터를 제공하고 기본 자산(예: 가상 머신 또는 볼륨)과 기본 자산(예: 스토리지 풀, 스토리지 노드, 연결된 스위치 포트)에 대한 요약 정보를 제공하며 추가 정보에 대한 링크를 제공합니다.

OnCommand Insight 7.3.1부터 모든 자산 페이지에는 * 주 * 페이지와 * 추가 데이터 * 페이지가 있습니다. 기본 페이지에는 자산에 대한 요약과 차트, 토폴로지 및 기타 정보에 대한 여러 섹션이 있습니다. Additional data * 페이지에서 현재 자산 유형에 대해 사용자 지정 가능한 대시보드 페이지를 구성할 수 있습니다.

자산 페이지 기본 탭의 선이나 메시지 옆에 있는 빨간색 원은 모니터링되는 환경에서 발생할 수 있는 문제를 나타냅니다.

자산 페이지 유형

자산 페이지는 자산의 현재 상태를 요약하고 자산 및 관련 자산에 대한 추가 정보에 대한 링크를 포함합니다.

OnCommand Insight는 다음 자산에 대한 자산 페이지를 제공합니다.

- 가상 머신
- 볼륨
- 내부 볼륨
- 물리적 호스트
- 스토리지 풀
- 스토리지
- 데이터 저장소

- 하이퍼바이저
- 응용 프로그램
- 스토리지 노드
- qtree입니다
- 디스크
- VMDK입니다
- 포트
- 스위치
- 패브릭
- 오브젝트 스토리지(예: Atmos, Centera, Amazon S3)
- Zone(영역)

매핑 및 마스킹 정보는 영역, 볼륨, VM 및 호스트/하이퍼바이저 자산 페이지의 표에서 볼 수 있습니다.



요약 정보는 오브젝트 스토리지 자산에서 사용할 수 있지만 데이터 소스 세부 정보 페이지에서만 이 정보에 액세스할 수 있습니다.

특정 자산을 위한 환경 검색

검색 기능을 사용하여 특정 자산에 대한 정보를 찾을 수 있습니다. 예를 들어, 시스템 사용자가 특정 서버에 대한 불만을 가지고 스토리지 관리자에게 연락할 경우 관리자는 서버 이름을 검색하고 상태를 요약하고 추가 연결 정보를 제공하는 자산 페이지를 표시할 수 있습니다.

단계

1. OnCommand Insightfob UI를 엽니다.

2. 도구 모음에서 를 클릭합니다 .

자산 검색 * 상자가 표시됩니다.

3. 자산 이름 또는 이름의 일부를 입력합니다.

4. 검색 결과에서 원하는 리소스를 선택합니다.

해당 자원의 자산 페이지가 표시됩니다.

고급 검색 기술

모니터링되는 환경에서 데이터 또는 개체를 검색하는 데 여러 검색 기술을 사용할 수 있습니다.

와일드카드 검색

문자를 사용하여 여러 문자 와일드카드 검색을 수행할 수 있습니다. 예를 들어, `_applic*n_`은(는) 응용 프로그램을 반환합니다.

검색에 사용되는 구

구문은 큰따옴표로 둘러싸인 단어 그룹입니다(예: "Paw VNX LUN 5"). 큰따옴표를 사용하여 이름이나 속성에 공백이 포함된 문서를 검색할 수 있습니다.

부울 연산자

부울 연산자를 사용하면 여러 용어를 결합하여 보다 복잡한 쿼리를 만들 수 있습니다.

• * 또는 *

- 또는 연산자는 기본 결합 연산자입니다.

두 용어 사이에 부울 연산자가 없으면 OR 연산자가 사용됩니다.

- OR 연산자는 두 용어를 연결하고 문서에 일치하는 용어가 있는 경우 일치하는 문서를 찾습니다.

예를 들어, "스토리지 또는 NetApp"은 "스토리지" 또는 "NetApp"이 포함된 문서를 검색합니다.

- 대부분의 조건과 일치하는 문서에 높은 점수가 부여됩니다.

• 및 *

AND 연산자를 사용하여 두 검색어가 모두 하나의 문서에 있는 문서를 찾을 수 있습니다. 예를 들어, ""오로라"와 "NetApp""이 모두 포함된 문서를 검색합니다.

단어 및 대신 && 기호를 사용할 수 있습니다.

• * NOT *

NOT 연산자를 사용하면 NOT가 포함된 모든 문서가 검색 결과에서 제외됩니다. 예를 들어, "NetApp이 아닌 스토리지"는 "NetApp"이 아닌 "스토리지"만 포함된 문서를 검색합니다.

기호를 사용할 수 있습니다! 대신 'NOT'이라는 단어를 사용하십시오.

접두사 및 접미사 검색

- 검색 문자열을 입력하기 시작하면 검색 엔진은 가장 일치하는 항목을 찾기 위해 접두사 및 접미사 검색을 수행합니다.
- 정확히 일치하는 항목이 접두사 또는 접미사 일치보다 높은 점수를 받습니다. 점수는 실제 검색 결과와 검색 용어의 거리를 기준으로 계산됩니다. 예를 들어, ""오로라", ""오로라 1", ""오로라 11""의 세 가지 창고를 사용할 수 있습니다. 아우르(Aur)를 검색하면 3곳의 모든 업소를 찾을 수 있습니다. 그러나 검색결과 검색어와 검색문자열 사이의 거리가 가장 가깝기 때문에 검색 결과가 가장 높은 점수를 받게 됩니다.
- 또한 검색 엔진은 검색어를 역순으로 검색하여 접미사 검색을 수행할 수 있습니다. 예를 들어 검색 상자에 ""345""를 입력하면 검색 엔진이 ""345""를 검색합니다.
- 검색은 대/소문자를 구분하지 않습니다.

인덱싱된 용어를 사용하여 검색합니다

인덱싱된 용어 중 더 많은 조건과 일치하는 검색을 수행하면 더 높은 점수를 얻을 수 있습니다.

검색 문자열은 스페이스를 기준으로 별도의 검색어로 분할됩니다. 예를 들어 검색 문자열 "Storage aurora NetApp"은

"Storage", "aurora", "NetApp" 등의 세 가지 키워드로 구분됩니다. 검색은 세 가지 용어를 모두 사용하여 수행됩니다. 이 용어 중 대부분과 일치하는 문서의 점수가 가장 높습니다. 더 많은 정보를 제공할수록 검색 결과가 더 좋습니다. 예를 들어 이름 및 모드로 스토리지를 검색할 수 있습니다.

UI는 범주 별로 검색 결과를 표시하며 범주 당 상위 3개 결과를 표시합니다. 원하는 문서를 찾지 못한 경우 검색 문자열에 더 많은 용어를 포함해서 검색 결과를 개선할 수 있습니다.

다음 표에서는 검색 문자열에 추가할 수 있는 인덱싱된 용어 목록을 제공합니다.

범주	인덱싱된 용어
스토리지	<ul style="list-style-type: none"> • "스토리지" • 이름 • 공급업체 • 모델
스토리지 풀	<ul style="list-style-type: none"> • "초라풀" • 이름 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델 • 연결된 모든 내부 볼륨의 이름입니다 • 연결된 모든 디스크의 이름입니다
내부 볼륨	<ul style="list-style-type: none"> • "인턴 볼륨" • 이름 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델 • 스토리지 풀의 이름입니다 • 연결된 모든 공유의 이름입니다 • 모든 관련 애플리케이션 및 업무 엔티티의 이름

볼륨	<ul style="list-style-type: none"> • "볼륨" • 이름 • 라벨 • 모든 내부 볼륨의 이름입니다 • 스토리지 풀의 이름입니다 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델
스토리지 노드	<ul style="list-style-type: none"> • "거어코드" • 이름 • 스토리지의 이름입니다 • 스토리지의 IP 주소입니다 • 스토리지의 일련 번호입니다 • 스토리지 공급업체 • 스토리지 모델
호스트	<ul style="list-style-type: none"> • "호스트" • 이름 • IP 주소 • 모든 관련 애플리케이션 및 업무 엔티티의 이름
데이터 저장소	<ul style="list-style-type: none"> • "다타스토어" • 이름 • 가상 센터 IP • 모든 볼륨의 이름입니다 • 모든 내부 볼륨의 이름입니다

가상 머신	<ul style="list-style-type: none"> • "가상시스템" • 이름 • DNS 이름입니다 • IP 주소 • 호스트의 이름입니다 • 호스트의 IP 주소입니다 • 모든 데이터 저장소의 이름입니다 • 모든 관련 애플리케이션 및 업무 엔티티의 이름
스위치(일반 및 NPV)	<ul style="list-style-type: none"> • 마녀 • IP 주소입니다 • WWN입니다 • 이름 • 일련 번호입니다 • 모델 • 도메인 ID입니다 • 패브릭의 이름입니다 • 패브릭의 WWN입니다
응용 프로그램	<ul style="list-style-type: none"> • "응용 프로그램" • 이름 • 테넌트 • LOB가 포함됩니다 • 부서 • 프로젝트
테이프	<ul style="list-style-type: none"> • "테이프" • IP 주소입니다 • 이름 • 일련 번호입니다 • 공급업체
포트	<ul style="list-style-type: none"> • "포트" • WWN입니다 • 이름

패브릭	<ul style="list-style-type: none"> • "fabric" • WWN입니다 • 이름
-----	--



표시된 데이터의 시간 범위를 변경합니다

기본적으로 자산 페이지에는 지난 24시간 동안의 데이터가 표시되지만 표시되는 데이터 세그먼트는 다른 고정 시간 또는 사용자 지정 시간 범위를 선택하여 변경하거나 더 적은 데이터 또는 더 많은 데이터를 볼 수 있습니다.


이 작업에 대해

자산 유형에 관계없이 모든 자산 페이지에 있는 옵션을 사용하여 표시된 데이터의 시간 세그먼트를 변경할 수 있습니다.

단계

1. OnCommand Insightfob UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서  를 클릭합니다  을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 페이지의 왼쪽 상단 모서리에서 다음 시간 아이콘 중 하나를 클릭하여 표시되는 데이터의 세그먼트를 변경합니다.
 - 3시간 *
최근 3시간의 데이터를 표시합니다.
 - * 24시간 *
최근 24시간 동안의 데이터를 표시합니다.
 - * 3D *
마지막 3일간의 데이터를 표시합니다.
 - * 7d *
최근 7일 동안의 데이터를 표시합니다.
 - * 30d *
최근 30일 동안의 데이터를 표시합니다.
 - * 사용자 정의 *

사용자 지정 시간 범위를 선택할 수 있는 대화 상자를 표시합니다. 한 번에 최대 31일의 데이터를 표시할 수 있습니다.

4. 사용자 정의 * 를 선택한 경우 다음을 수행합니다.
 - a. 날짜 필드를 클릭하고 시작 날짜의 월, 일 및 연도를 선택합니다.
 - b. 시간 목록을 클릭하고 시작 시간을 선택합니다.
 - c. 끝 데이터와 시간에 대해 a와 b 단계를 모두 반복합니다.
 - d.  을 클릭합니다.

데이터 소스 획득 상태를 확인하는 중입니다



데이터 소스가 Insight의 주요 정보원이기 때문에 데이터 소스가 실행 상태를 유지하도록 하는 것이 중요합니다.

직접 획득한 모든 자산에 대해 모든 자산 페이지에서 데이터 소스 획득 상태를 볼 수 있습니다. 다음 획득 시나리오 중 하나가 발생할 수 있으며, 이 경우 자산 페이지의 오른쪽 상단 모서리에 상태가 표시됩니다.

- 데이터 소스에서 성공적으로 획득되었습니다

상태 ""를 표시합니다 xxxx`", where `xxxx 자산 데이터 소스의 가장 최근 획득 시간을 나타냅니다.

- 획득 오류가 있습니다.

상태 ""를 표시합니다 xxxx`", where `xxxx 에서 자산에 있는 하나 이상의 데이터 소스의 가장 최근 획득 시간을 나타냅니다.  를 클릭합니다  창에서 자산에 대한 각 데이터 소스, 데이터 소스의 상태 및 마지막으로 데이터를 획득한 시간을 표시합니다. 데이터 원본을 클릭하면 데이터 원본의 세부 정보 페이지가 표시됩니다.

자산을 직접 획득하지 않으면 상태가 표시되지 않습니다.

자산 페이지 섹션

자산 페이지에는 자산과 관련된 정보가 포함된 여러 섹션이 표시됩니다. 표시되는 섹션은 자산의 유형에 따라 다릅니다.

요약

자산 페이지의 요약 섹션에는 특정 자산에 대한 정보가 요약되어 표시되며, 자산과 관련된 문제가 빨간색 원으로 표시되며 관련 자산 및 자산에 할당된 성능 정책에 대한 추가 정보로 연결되는 하이퍼링크가 표시됩니다.

다음 예에서는 가상 머신에 대한 자산 페이지의 요약 섹션에서 사용할 수 있는 일부 정보 유형을 보여 줍니다. 빨간색 원이 있는 항목은 모니터링되는 환경에서 발생할 수 있는 문제를 나타냅니다.


Summary

Power state:	On
Guest state:	Running
Datastore:	DS_SP1_1
CPU:	41.05%
Memory:	● 51% (1,047 / 2,048 MB)
Capacity:	10% (19.5 / 195.3 GB)
Latency:	1.93 ms (6.00 ms max)
IOPS:	1,317.33 IO/s (4,964.00 IO/s max)
Throughput:	38.79 MB/s (142.00 MB/s max)
DNS name:	VM_Cs_travBookcomp.com
IP:	10.97.133.23
OS:	Microsoft Windows Server 2008 R2(64-bit)
Processors:	4
FC Fabrics Connected:	1
Performance Policies:	VM Latency-Critical VM Latency-Warning Comp Corp.Customer Support SLA latency ● Exchange SL0

요약 섹션을 사용합니다

요약 섹션을 보고 자산에 대한 일반 정보를 볼 수 있습니다. 특히 메트릭 또는 성능 정책 옆에 빨간색 원을 표시하여 OnCommand Insight가 나타내는 메트릭(예: 메모리, 용량, 지연 시간)이나 성능 정책이 문제가 되는지 확인하는 것이 좋습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서 를 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 *를 클릭하고 * 자산 대시보드 *를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.



요약 섹션에 표시되는 정보는 보고 있는 자산 페이지 유형에 따라 다릅니다.

3. 자산 링크를 클릭하여 자산 페이지를 볼 수 있습니다.

예를 들어, 스토리지 노드를 보고 있는 경우 링크를 클릭하여 연결된 스토리지의 자산 페이지를 보거나 HA 파트너의 자산 페이지를 볼 수 있습니다.

4. 자산과 연결된 메트릭을 볼 수 있습니다.

메트릭 옆에 있는 빨간색 원은 잠재적인 문제를 진단하고 해결해야 할 수 있음을 나타냅니다.



일부 스토리지 자산에서는 볼륨 용량이 100% 이상 표시될 수 있습니다. 이는 자산에서 보고하는 사용된 용량 데이터의 일부인 볼륨의 용량과 관련된 메타데이터 때문입니다.

5. 해당되는 경우 성능 정책 링크를 클릭하여 자산과 관련된 성능 정책 또는 정책을 볼 수 있습니다.

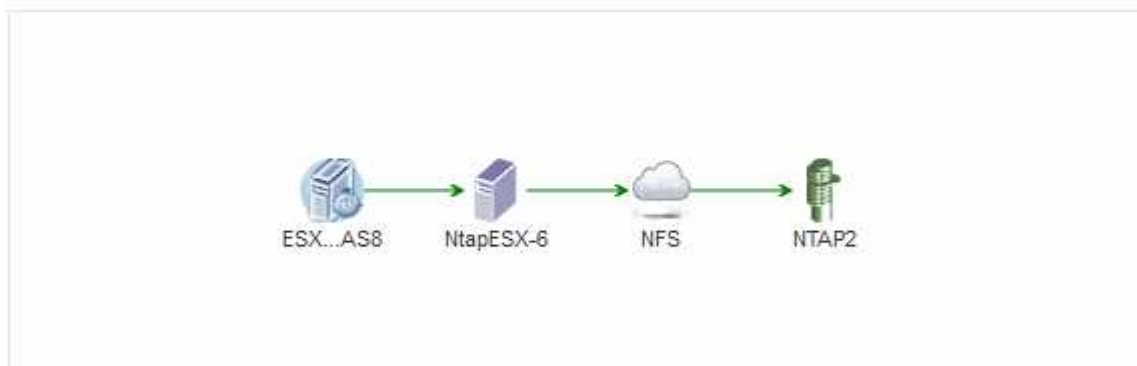
성능 정책 옆에 빨간색 원이 나타나면 자산이 성능 정책의 정의된 임계값을 초과했음을 나타냅니다. 문제를 더 자세히 진단하려면 성능 정책을 검토해야 합니다.

토폴로지

자산에 해당되는 경우 토폴로지 섹션을 통해 기본 자산이 관련 자산에 어떻게 연결되어 있는지 확인할 수 있습니다.

다음은 가상 머신 자산 페이지의 토폴로지 섹션에 표시될 수 있는 항목의 예입니다.

Topology



자산의 토폴로지가 섹션에 들어갈 수 있는 것보다 크면 * 토폴로지 * 하이퍼링크를 보기 위한 * 클릭 링크가 대신 표시됩니다.

Topology 섹션 사용

Topology(토폴로지) 섹션에서는 네트워크의 자산이 서로 어떻게 연결되어 있는지 확인하고 관련 자산에 대한 정보를 표시할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서 를 클릭합니다 을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다. 자산 페이지의 오른쪽 상단 모서리에 있는 토폴로지 섹션을 찾을 수 있습니다.




자산의 토폴로지가 섹션에 들어갈 수 있는 것보다 큰 경우 * 클릭 링크를 클릭하여 토폴로지 * 하이퍼링크를 확인하십시오.

3. 기본 자산의 관련 자산에 대한 자세한 정보를 보려면 토폴로지의 관련 자산 위에 커서를 놓고 해당 이름을 클릭하면 자산 페이지가 표시됩니다.

자산 페이지의 사용자 데이터 섹션이 표시되고 응용 프로그램, 사업체 및 주식과 같은 사용자 정의 데이터를 변경할 수 있습니다.

다음은 애플리케이션, 사업체 및 주식이 자산에 할당될 때 가상 시스템 자산 페이지의 사용자 데이터 섹션에 표시될 수 있는 항목의 예입니다.





User Data

Application(s):	Concur
Business Entities:	Hybridsoft Corporation.Sales.Wes...
Birthday:	01/30/2016  
 Add	


사용자 데이터 섹션을 사용하여 응용 프로그램을 할당하거나 수정합니다

사용자 환경에서 실행 중인 애플리케이션을 특정 자산(호스트, 가상 머신, 볼륨, 내부 볼륨 및 하이퍼바이저)에 할당할 수 있습니다. 사용자 데이터 섹션을 사용하면 자산에 할당된 애플리케이션을 변경하거나 애플리케이션 또는 추가 애플리케이션을 자산에 할당할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서  을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 다음을 수행할 수 있습니다.
 - 응용 프로그램의 자산 페이지를 보려면 응용 프로그램 이름을 클릭합니다.
 - 할당된 응용 프로그램을 변경하거나 응용 프로그램 또는 추가 응용 프로그램을 할당하려면 응용 프로그램 이름 위에 커서를 놓고 응용 프로그램이 할당된 경우 * 없음 * 위에 커서를 놓습니다. 할당된 응용 프로그램이 없는 경우  을 클릭합니다  을 입력하여 응용 프로그램을 검색하거나 목록에서 하나를 선택한 다음  을 클릭합니다.

업무 엔티티와 연결된 애플리케이션을 선택하면 업무 엔티티가 자동으로 자산에 할당됩니다. 이 경우 사업체 이름 위에 커서를 놓으면 _Derived_ 라는 단어가 표시됩니다. 연결된 응용 프로그램이 아닌 자산에 대해서만 엔티티를 유지하려면 응용 프로그램의 할당을 수동으로 재정의할 수 있습니다.







 - 응용 프로그램을 제거하려면  를 클릭합니다.

사용자 데이터 섹션을 사용하여 업무 엔티티를 할당하거나 수정합니다

환경 데이터를 더 세밀한 수준에서 추적 및 보고할 비즈니스 엔티티를 정의할 수 있습니다. 자산

페이지의 사용자 데이터 섹션을 사용하면 자산에 할당된 업무 엔티티를 변경하거나 자산에서 업무 엔티티를 제거할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서  를 클릭합니다  을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 다음을 수행할 수 있습니다.
 - 지정된 엔티티를 변경하거나 엔티티를 할당하려면  을 클릭합니다  목록에서 요소를 선택합니다.
 - 업무 엔티티를 제거하려면  을 클릭합니다 .







자산에 할당된 애플리케이션에서 파생된 엔티티는 제거할 수 없습니다.

User Data(사용자 데이터) 섹션을 사용하여 주석을 할당하거나 수정합니다

회사 요구 사항에 맞는 데이터를 추적하도록 OnCommand Insight를 사용자 지정할 때 `_annotations_` 라는 특수 메모를 정의하여 자산에 할당할 수 있습니다. 자산 페이지의 사용자 데이터 섹션에는 자산에 할당된 주석이 표시되며 해당 자산에 할당된 주석을 변경할 수도 있습니다.



단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서  를 클릭합니다  을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.
3. 자산 페이지의 * 사용자 데이터 * 섹션에서  를 클릭합니다 .

주석 추가 대화 상자가 표시됩니다.

4. Annotation(주석) * 을 클릭하고 목록에서 주석을 선택합니다.
5. 값 * 을 클릭하고 선택한 주석 유형에 따라 다음 중 하나를 수행합니다.
 - 주석 유형이 목록, 날짜 또는 부울인 경우 목록에서 값을 선택합니다.
 - 주석 유형이 텍스트인 경우 값을 입력합니다.
6. 저장 * 을 클릭합니다.

주석이 자산에 할당됩니다. 나중에 쿼리를 사용하여 주석을 기준으로 자산을 필터링할 수 있습니다.

7. 주석을 지정한 후 주석 값을 변경하려면  을 클릭합니다  다른 값을 선택합니다.

주석이 * 주석 지정 시 동적으로 값 추가 * 옵션을 선택한 목록 유형인 경우 기존 값을 선택하는 것 외에도 새 값을 추가하도록 입력할 수 있습니다.

전문가 뷰

자산 페이지의 전문가 보기 섹션에서는 선택한 기간(3시간, 24시간, 3일, 7일, 또는 사용자 지정 기간)을 성능 차트 및 관련 자산에 입력합니다.

다음은 볼륨 자산 페이지의 전문가 보기 섹션의 예입니다.



선택한 기간의 성능 차트에서 확인할 메트릭을 선택할 수 있습니다.

자원 섹션에는 기본 자산의 이름과 성능 차트의 기본 자산을 나타내는 색상이 표시됩니다. 상호 연결된 최상위 섹션에 성능 차트에서 보려는 자산이 없는 경우 추가 리소스 섹션의 * 자산 검색 * 상자를 사용하여 자산을 찾고 성능 차트에 추가할 수 있습니다. 자원을 추가하면 추가 자원 섹션에 나타납니다.

또한 리소스 섹션에 표시된 대로 다음 범주의 기본 자산과 관련된 자산이 있을 수 있습니다.

- 상호 연관성

에는 기본 자산에 대한 하나 이상의 성능 메트릭과 높은 상관 관계(백분율)가 있는 자산이 나와 있습니다.

- 최고 기여자

기본 자산에 기여하는 자산(백분율)을 표시합니다.

- 탐욕심

에는 호스트, 네트워크 및 스토리지와 같은 동일한 리소스를 공유하여 자산에서 시스템 리소스를 빼앗는 자산이 나와 있습니다.

- 성능 저하

이 자산으로 인해 시스템 리소스가 고갈된 자산을 표시합니다.

자산 페이지의 전문가 보기 섹션에는 자산에 대해 선택한 기간에 따라 몇 가지 메트릭이 표시됩니다. 각 메트릭은 자체 성능 차트에 표시됩니다. 보려는 데이터에 따라 차트에서 메트릭 및 관련 자산을 추가하거나 제거할 수 있습니다.

미터	설명
BB 크레딧 제로 Rx, Tx	샘플링 기간 동안 수신/전송 버퍼 대 버퍼 크레딧 수가 0으로 전환된 횟수입니다. 이 메트릭은 제공할 크레딧이 없기 때문에 연결된 포트의 전송을 중지해야 하는 횟수를 나타냅니다.
BB 크레딧 없음 기간 Tx	샘플링 간격 동안 전송 BB 크레딧이 0인 시간(밀리초)입니다.
캐시 적중률(총, 읽기, 쓰기) %	캐시 적중으로 인한 요청의 비율입니다. 적중 횟수와 볼륨 액세스 횟수가 많을수록 성능이 향상됩니다. 캐시 적중 정보를 수집하지 않는 스토리지 시스템의 경우 이 열이 비어 있습니다.
캐시 활용률(총) %	캐시 적중으로 인한 캐시 요청의 총 비율입니다
클래스 3이 삭제됩니다	Fibre Channel Class 3 데이터 전송 폐기 횟수
CPU 사용률(총) %	사용 가능한 총 CPU(모든 가상 CPU)의 백분율로 사용 중인 CPU 리소스의 양입니다.
CRC 오류입니다	샘플링 기간 동안 포트에서 감지된 잘못된 CRC(Cyclic Redundancy Check)의 프레임 수입니다
프레임 속도	초당 프레임 수(FPS)로 프레임 속도 전송
프레임 크기 평균(Rx, Tx)	프레임 크기에 대한 트래픽 비율입니다. 이 메트릭을 통해 Fabric에 오버헤드 프레임이 있는지 여부를 확인할 수 있습니다.
프레임 크기가 너무 길다	너무 긴 Fibre Channel 데이터 전송 프레임 수입니다.
프레임 크기가 너무 짧습니다	너무 짧은 Fibre Channel 데이터 전송 프레임 수입니다.
I/O 밀도(Total, Read, Write)	볼륨, 내부 볼륨 또는 스토리지 요소에 대한 IOPS를 사용된 용량(데이터 소스의 최신 인벤토리 풀에서 얻은 값)으로 나눈 값입니다. TB당 초당 I/O 작업 수로 측정


IOPS(총, 읽기, 쓰기)	I/O 채널을 통해 전달되는 읽기/쓰기 I/O 서비스 요청 수 또는 시간 단위당 해당 채널의 일부(초당 I/O로 측정)
IP 처리량(총, 읽기, 쓰기)	<p>총계: 초당 메가바이트 단위의 IP 데이터가 전송 및 수신된 총 속도입니다. 읽기: IP 처리량(수신): IP 데이터가 수신된 평균 속도(MB/초)입니다.</p> <p>쓰기: IP 처리량(전송): IP 데이터가 전송된 평균 속도(MB/초)입니다.</p>
지연 시간(총, 읽기, 쓰기)	<p>지연 시간(R&W): 고정된 시간 내에 데이터를 가상 시스템에 읽거나 쓰는 비율. 이 값은 초당 메가바이트로 측정됩니다.</p> <p>지연 시간: 데이터 저장소의 가상 머신에서 평균 응답 시간입니다.</p> <p>최고 지연 시간: 데이터 저장소의 가상 머신에서 응답 시간이 가장 긴 경우</p>
링크 실패	샘플링 기간 동안 포트에서 감지된 링크 장애 수입니다.
Link Reset Rx, Tx(링크 재설정 Rx, Tx)	샘플링 기간 동안 수신 또는 전송 링크 재설정 횟수 이 메트릭은 이 포트에 연결된 포트에서 실행된 링크 재설정의 수를 나타냅니다.
메모리 사용률(총) %	호스트에서 사용하는 메모리의 임계값입니다.
부분 R/W(총) %	<p>읽기/쓰기 작업이 RAID 5, RAID 1/0 또는 RAID 0 LUN의 디스크 모듈에서 스트라이프 경계를 교차하는 총 횟수입니다. 일반적으로 스트라이프 크로싱은 각 LUN에 추가 I/O가 필요하기 때문에 유용하지 않습니다 비율이 낮다면 효율적인 스트라이프 요소 크기를 나타내며 볼륨(또는 NetApp LUN)이 잘못 정렬되었음을 나타냅니다.</p> <p>CLARiX의 경우 이 값은 총 IOPS 수로 나눈 스트라이프 크로싱 수입니다.</p>
포트 오류	샘플링 기간/지정된 기간 동안의 포트 오류 보고.
신호 손실 카운트	신호 손실 오류 수입니다. 신호 손실 오류가 발생하면 전기 연결이 없고 물리적 문제가 있는 것입니다.
스왑 속도(총 속도, 속도, 아웃 속도)	샘플링 기간 동안 메모리를 디스크에서 활성 메모리로 스왑하거나, 스왑 아웃하거나, 둘 다 활성 메모리로 스왑하는 속도입니다. 이 카운터는 가상 머신에 적용됩니다.

동기화 손실 카운트	동기화 손실 오류 수입니다. 동기화 손실 오류가 발생하면 하드웨어가 트래픽을 감지하거나 해당 트래픽을 잠글 수 없습니다. 모든 장비가 동일한 데이터 속도를 사용하지 않거나, 광학 또는 물리적 연결의 품질이 저하될 수 있습니다. 이러한 각 오류 후에 포트가 재동기화되어야 하며, 이는 시스템 성능에 영향을 줍니다. KB/초 단위로 측정됩니다
처리량(총, 읽기, 쓰기)	입출력 서비스 요청에 대한 응답으로 데이터가 전송, 수신 또는 모두 고정된 시간(MB/sec 단위로 측정)으로 전송되는 속도입니다.
시간 초과 폐기 프레임 - Tx	시간 초과로 인해 폐기된 전송 프레임 수입니다.
트래픽 속도(합계, 읽기, 쓰기)	샘플링 기간 동안 전송, 수신 또는 두 가지 모두 수신된 트래픽(초당 메비바이트)입니다.
트래픽 사용률(총, 읽기, 쓰기)	샘플링 기간 동안 수신/전송/총 수신/전송/총 용량의 비율입니다.
사용률(총, 읽기, 쓰기) %	전송(Tx) 및 수신(Rx)에 사용되는 가용 대역폭의 비율입니다.
쓰기 보류(총)	보류 중인 쓰기 입출력 서비스 요청 수입니다.

전문가 보기 섹션을 사용합니다

전문가 보기 섹션에서는 선택한 기간 동안 원하는 수의 해당 메트릭을 기준으로 자산에 대한 성능 차트를 보고, 서로 다른 기간 동안 자산 및 관련 자산 성과를 비교 및 대조할 수 있도록 관련 자산을 추가할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서 **를** 클릭합니다  을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 * **를** 클릭하고 * 자산 대시보드 * **를** 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다. 기본적으로 성능 차트는 자산 페이지에 대해 선택한 기간에 대해 두 가지 메트릭을 보여 줍니다. 예를 들어, 스토리지의 경우 성능 차트에는 기본적으로 지연 시간과 총 IOPS가 표시됩니다. 자원 섹션에는 자원 이름과 자산을 검색할 수 있는 추가 자원 섹션이 표시됩니다. 자산에 따라 Top Correlated, Top Contributor, greedy 및 Degraded 섹션에도 자산이 표시될 수 있습니다.
3. 표시할 메트릭 선택 * **을** 클릭하고 메트릭을 선택하여 메트릭에 대한 성능 차트를 추가할 수 있습니다.

선택한 메트릭에 대한 성능 차트가 추가됩니다. 선택한 기간의 데이터가 차트에 표시됩니다. 자산 페이지의 왼쪽 상단 모서리에 있는 다른 기간을 클릭하여 기간을 변경할 수 있습니다.

단계를 다시 수행하고 클릭하여 메트릭을 지울 수 있습니다. 메트릭에 대한 성능 차트가 제거됩니다.

4. 커서를 차트 위에 놓고 자산에 따라 다음 중 하나를 클릭하여 표시되는 메트릭 데이터를 변경할 수 있습니다.

- * 읽기 * 또는 * 쓰기 *
- **Tx** 또는 * Rx * * Total * 이 기본값입니다.

5. 선택한 기간 동안 메트릭 값이 어떻게 변경되는지 확인하려면 차트의 데이터 요소 위로 커서를 끌어다 놓습니다.


6. Resources * 섹션에서 다음 중 하나를 수행하여 해당되는 경우 성능 차트에 관련 자산을 추가할 수 있습니다.

- Top Correlated, Top 컨트리뷰터, greedy 또는 Degraded 섹션에서 관련 자산을 선택하여 해당 자산의 데이터를 선택한 각 메트릭의 성능 차트에 추가할 수 있습니다. 자산에는 최소 15%의 상관 관계 또는 기여도가 표시되어야 합니다.

자산을 선택하면 자산 옆에 색상 블록이 표시되어 차트의 데이터 요소 색상을 나타냅니다.

- 표시된 자산의 경우 자산 이름을 클릭하여 해당 자산 페이지를 표시하거나, 자산이 상호 연관되거나 기본 자산에 기여하는 비율을 클릭하여 기본 자산에 대한 자산 관계에 대한 추가 정보를 볼 수 있습니다.

예를 들어 상호 연결된 최상위 자산 옆에 있는 연결된 백분율을 클릭하면 해당 자산의 상관 관계 유형과 기본 자산을 비교한 정보 메시지가 표시됩니다.

- 비교 목적으로 성능 차트에 표시할 자산이 상관관계 섹션에 없는 경우 추가 리소스 섹션의 * 자산 검색 * 상자를 사용하여 다른 자산을 찾을 수 있습니다. 자산을 선택하면 추가 자원 섹션에 표시됩니다. 자산에 대한 정보를 더 이상 볼 수 없게 하려면 를 클릭합니다 .

관련 자산

해당하는 경우 자산 페이지에 관련 자산 섹션이 표시됩니다. 예를 들어, 볼륨 자산 페이지에는 스토리지 풀, 연결된 스위치 포트, 컴퓨팅 리소스 등의 자산에 대한 정보가 표시될 수 있습니다. 각 섹션은 해당 범주의 관련 자산 중 하나를 나열하고 각 자산 페이지에 대한 링크와 자산과 관련된 몇 가지 성능 통계를 나열하는 표로 구성됩니다.


관련 자산 섹션을 사용합니다

Related Assets(관련 자산) 섹션에서 기본 자산과 관련된 자산을 볼 수 있습니다. 각 관련 자산이 해당 자산에 대한 관련 통계와 함께 표에 표시됩니다. 자산 정보를 내보내거나 전문가 보기 성능 차트에서 자산 통계를 보거나 관련 자산에 대한 통계만 표시하는 차트를 표시할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.

2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.

- Insight 도구 모음에서 를 클릭합니다  을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
- 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다.

3. 테이블에 에셋이 표시되는 방식을 제어하려면 다음을 수행합니다.

- 자산 페이지를 표시하려면 자산 이름을 클릭합니다.

- 특정 자산만 표시하려면 * filter * 상자를 사용합니다.
- 테이블에 5개 이상의 자산이 있는 경우 페이지별로 자산을 찾아보려면 페이지 번호를 클릭합니다.
- 열 머리글의 화살표를 클릭하여 표에서 열의 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경합니다.
- 관련 자산 위에 커서를 놓고 을 클릭하여 전문가 보기 섹션의 성과 차트에 관련 자산을 추가합니다 📊.

4. 표에 표시된 정보를 로 내보냅니다 .CSV 파일:

- 을 클릭합니다 📄 .
- Open with * 를 클릭한 다음 * OK * 를 클릭하여 Microsoft Excel에서 파일을 열고 파일을 특정 위치에 저장하거나 * Save file * 을 클릭하고 * OK * 를 클릭하여 파일을 Downloads 폴더에 저장합니다.

표시를 위해 현재 선택된 컬럼의 모든 오브젝트 속성이 파일로 내보내집니다. 표시된 열의 속성만 내보내집니다. 표의 처음 10,000개 행만 내보내집니다.

5. 테이블 아래의 차트에 관련 자산 정보를 표시하려면 을 클릭합니다 📊 다음 중 하나를 수행합니다.

- 표시되는 메트릭 데이터를 변경하려면 * Read * , * Write * 또는 * Total * 을 클릭합니다. 기본값은 * Total * 입니다.
- 을 클릭합니다 🛠️ 다른 메트릭을 선택합니다.
- 을 클릭합니다 📊 차트 종류를 변경하려면 다음을 수행합니다. 기본값은 * 꺾은선형 차트 * 입니다.
- 차트의 데이터 요소 위로 커서를 이동하면 각 관련 자산에 대해 선택한 기간 동안 메트릭 값이 어떻게 변경되는지 확인할 수 있습니다.
- 차트 범례에서 관련 자산을 클릭하여 차트에 추가하거나 차트에서 제거합니다.
- 관련 자산 표에서 페이지 번호를 클릭하면 차트의 다른 관련 자산을 볼 수 있습니다.
- 을 클릭합니다 ✕ 를 눌러 차트를 닫습니다.

위반

자산 페이지의 위반 섹션을 사용하여 자산에 할당된 성능 정책의 결과로 사용자 환경에서 발생한 위반 사항을 확인할 수 있습니다. 성능 정책은 네트워크 임계값을 모니터링하고, 임계값 위반을 즉시 감지하고, 영향을 식별하고, 문제의 영향과 근본 원인을 빠르고 효과적으로 수정할 수 있는 방식으로 분석할 수 있도록 합니다.

다음 예제는 하이퍼바이저의 자산 페이지에 표시되는 보라색 섹션을 보여 줍니다.


Time	Description
06/05/2015 5:00:00 pm	Port balance index of 74 on esx1 exceeds the threshold of 50
06/12/2015 8:59:54 am	2 violations for esx2 with 'Swap out rate' > 3
06/12/2015 12:04:54 pm	esx1 violation with 'Swap out rate' > 3.00 KB/s (value of 86.85 KB/s)
06/12/2015 12:29:54 pm	esx1 violation with 'Swap in rate' > 3.00 KB/s (value of 59.90 KB/s)
06/12/2015 1:04:54 pm	7 violations for ds-30 with 'Latency - Total' > 50

Showing 1 to 5 of 32 entries


위반 섹션을 사용하십시오

위반 섹션에서는 자산에 할당된 성능 정책의 결과로 네트워크에서 발생하는 모든 위반 사항을 보고 관리할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
 - Insight 도구 모음에서 를 클릭합니다  을 클릭하고 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
 - 대시보드 * 를 클릭하고 * 자산 대시보드 * 를 선택한 다음 자산 이름을 찾아 클릭합니다. 자산 페이지가 표시됩니다. 위반 섹션에는 위반이 발생한 시간 및 발생한 임계값에 대한 설명과 함께 위반이 발생한 자산에 대한 하이퍼링크가 표시됩니다(예: "'자연 시간이 있는 2개의 위반 FIR DS-30, 총 > 50'").
3. 다음과 같은 옵션 작업을 수행할 수 있습니다.
 - 특정 위반만 표시하려면 * filter * 상자를 사용합니다.
 - 표에 위반사항이 5개 이상 있는 경우 페이지 번호를 클릭하여 위반사항을 페이지별로 탐색합니다.
 - 열 머리글의 화살표를 클릭하여 표에서 열의 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경합니다.
 - 설명에서 자산 이름을 클릭하여 자산 페이지를 표시합니다. 빨간색 원은 추가 조사가 필요한 문제를 나타냅니다.

정책 편집 대화 상자가 표시된 성능 정책을 클릭하여 성능 정책을 검토하고 필요한 경우 정책을 변경할 수 있습니다.

 - 을 클릭합니다  문제가 더 이상 문제의 원인이 아닌 것으로 판단될 경우 목록에서 위반 사항을 제거합니다.

사용자 지정 가능한 자산 페이지

추가 데이터는 각 자산 페이지의 사용자 지정 가능한 위젯에 표시될 수 있습니다. 자산에 대한 페이지를 사용자 지정하면 해당 유형의 모든 자산에 대한 사용자 지정이 페이지에 적용됩니다.

다음 작업을 수행하여 자산 페이지 위젯을 사용자 지정합니다.

1. 페이지에 위젯을 추가합니다
2. 원하는 데이터를 표시할 위젯에 대한 쿼리 또는 표현식을 생성합니다
3. 원하는 경우 필터를 선택합니다
4. 롤업 또는 그룹화 방법을 선택합니다
5. 위젯을 저장합니다
6. 원하는 모든 위젯에 대해 반복합니다
7. 자산 페이지를 저장합니다

위젯에서 표시된 데이터를 더욱 구체화하는 데 사용할 수 있는 변수를 사용자 지정 자산 페이지에 추가할 수도 있습니다. 각 자산 유형은 일반 변수 외에도 "\$this" 변수 세트를 사용하여 현재 자산과 직접 관련된 리소스를 빠르게 식별할 수 있습니다. 예를 들어, 현재 가상 머신을 호스팅하는 동일한 하이퍼바이저에 의해 호스팅되는 모든 가상 머신을 확인할 수 있습니다.

이 사용자 지정 자산 페이지는 각 사용자뿐 아니라 각 자산 유형에 대해 고유합니다. 예를 들어 사용자 A가 가상 머신에 대한 사용자 지정 자산 페이지를 생성하는 경우 해당 사용자에게 대한 모든 가상 머신 자산 페이지에 대해 해당 사용자 지정 페이지가 표시됩니다.

사용자는 자신이 만든 사용자 지정 자산 페이지만 보고, 편집하거나 삭제할 수 있습니다.

사용자 지정 자산 페이지는 Insight의 내보내기/가져오기 기능에 포함되지 않습니다.

"\$이" 변수 이해

자산의 "추가 데이터" 사용자 지정 페이지에 있는 특수 변수를 사용하면 현재 자산과 직접 관련된 추가 정보를 쉽게 표시할 수 있습니다.

이 작업에 대해

자산의 사용자 지정 가능한 랜딩 페이지의 위젯에 "\$This" 변수를 사용하려면 다음 단계를 따르십시오. 이 예에서는 테이블 위젯을 추가합니다.



"\$This" 변수는 자산의 사용자 지정 가능한 랜딩 페이지에만 유효합니다. 다른 Insight 대시보드에는 사용할 수 없습니다. 사용 가능한 "\$This" 변수는 자산 유형에 따라 다릅니다.

단계

1. 선택한 자산에 대한 자산 페이지로 이동합니다. 이 예에서는 가상 머신(VM) 자산 페이지를 선택하겠습니다. VM을 쿼리하거나 검색하고 링크를 클릭하여 해당 VM의 자산 페이지로 이동합니다.

VM의 자산 페이지가 열립니다.

2. 해당 자산의 사용자 지정 가능한 랜딩 페이지로 이동하려면 * Change view: * > * Additional Virtual Machine data * 드롭다운을 클릭합니다.
3. Widget * 버튼을 클릭하고 * Table widget * 을 선택합니다.

편집을 위해 테이블 위젯이 열립니다. 기본적으로 모든 스토리지가 테이블에 표시됩니다.

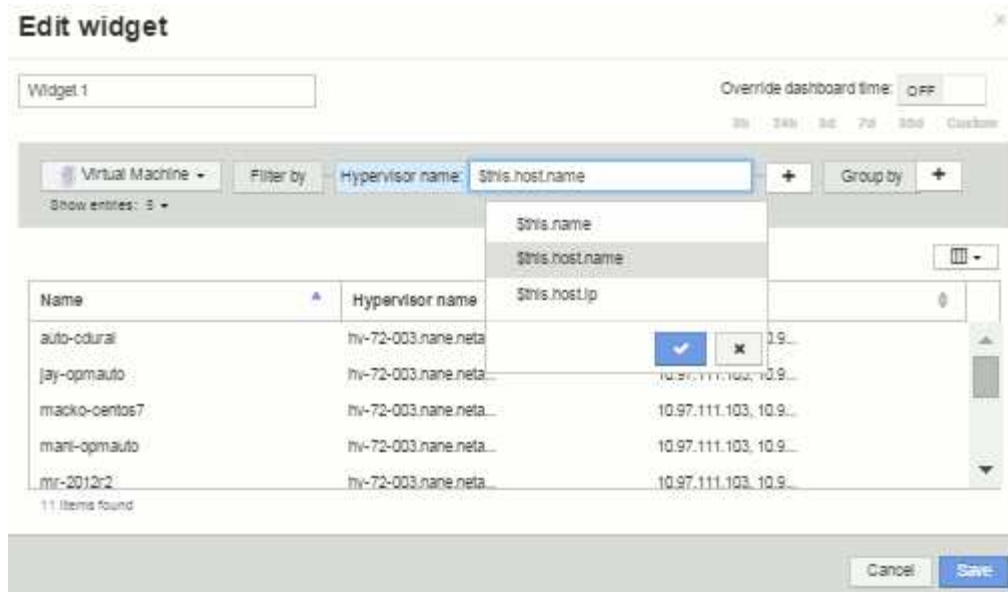
4. 모든 가상 시스템을 표시하려고 합니다. 자산 선택기를 클릭하고 * 스토리지 * 를 * 가상 머신 * 으로 변경합니다.

이제 모든 가상 머신이 테이블에 표시됩니다.

5. 열 선택기 * 버튼을 클릭합니다  하이퍼바이저 이름 * 필드를 테이블에 추가합니다.

하이퍼바이저 이름이 표에 각 VM에 대해 표시됩니다.

6. 우리는 현재 VM을 호스팅하는 하이퍼바이저만 신경 쓸 뿐입니다. 필터 기준* 필드의 + 버튼을 클릭하고 * 하이퍼바이저 이름 * 을 선택합니다.
7. 아무 * 나 * 를 클릭하고 * \$this.host.name * 변수를 선택합니다. 확인 버튼을 클릭하여 필터를 저장합니다.



8. 이제 이 표에는 현재 VM의 하이퍼바이저에 의해 호스팅되는 모든 VM이 표시됩니다. 저장 * 을 클릭합니다.

결과

이 가상 머신 자산 페이지에 대해 생성한 테이블이 표시되는 모든 VM 자산 페이지에 대해 표시됩니다. 위젯에서 * \$this.host.name * 변수를 사용하면 현재 자산의 하이퍼바이저가 소유한 VM만 테이블에 표시됩니다.

네트워크 리소스 밸런싱

밸런싱 문제를 해결하려면 자산 페이지를 사용하여 문제를 찾고 사용량이 적은 고용량 볼륨을 식별합니다.

단계

1. 브라우저에서 자산 대시보드를 엽니다.
2. 가상 머신 IOPS 히트 맵에서 매우 큰 인쇄물에 VM 이름이 표시되므로 종종 문제를 보고할 수 있습니다.
3. VM 이름을 클릭하여 자산 페이지를 표시합니다.
4. 요약에서 오류 메시지를 확인합니다.
5. 성능 차트 및 특히 상호 연결된 최상위 리소스를 확인하여 경합 중인 볼륨을 찾습니다.
6. 성능 차트에 볼륨을 추가하여 활동 패턴을 비교하고 문제와 관련된 다른 리소스의 자산 페이지를 더 많이 표시합니다.
7. 자산 페이지 맨 아래로 스크롤하여 VM과 관련된 모든 리소스 목록을 확인합니다. 고용량 vmdks를 실행합니다. 이로 인해 경합이 발생할 수 있습니다.
8. 균형 조정 문제를 해결하려면 과도하게 사용되는 리소스로부터 로드를 받거나 사용량이 많은 리소스에서 덜 까다로운 애플리케이션을 제거하기 위해 활용도가 낮은 리소스를 파악합니다.

네트워크 성능 검사

스토리지 환경의 성능을 검사하고 활용률이 저조하거나 활용도가 높은 리소스를 식별하고 문제가 발생하기 전에 위험을 식별할 수 있습니다.

Insight는 수집된 스토리지 데이터를 통해 밝혀진 성능 및 가용성 문제를 해결합니다.

Insight를 사용하여 다음과 같은 성능 관리 작업을 수행할 수 있습니다.

- 환경 전체의 성능 모니터링
- 다른 장치의 성능에 영향을 미치는 리소스를 파악합니다

포트의 중요성

DWH(Insight Server and Data Warehouse) 서버는 안정적으로 작동하려면 많은 TCP 포트를 사용할 수 있어야 합니다. 이러한 포트 중 일부는 localhost 어댑터(127.0.0.1)에 바인딩된 프로세스에만 활용되지만 핵심 서비스가 안정적으로 작동하려면 여전히 필요합니다. 필요한 포트 수는 네트워크에서 사용되는 포트의 상위 집합입니다.

Insight 서버 포트

Insight Server에는 소프트웨어 방화벽이 설치되어 있을 수 있습니다. 열어야 할 "구멍"은 아래와 같습니다.

- 인바운드 HTTPS 443 * - TCP 443에서 Insight WebUI를 실행 중인 경우 다음 소비자 중 일부 및 모두를 허용하도록 해당 룰 노출해야 합니다.
- WebUI의 Insight 사용자
- Insight 서버에 연결하려는 원격 획득 장치
- 이 Insight 서버에 대한 커넥터가 있는 OCI DWH 서버
- Insight REST API와의 프로그래밍 상호 작용

Insight 서버 호스트 레벨 방화벽 구축을 원하는 모든 사람에게 NetApp은 모든 기업 네트워크 IP 블록에 HTTPS 액세스를 허용하도록 권장합니다.

- 인바운드 MySQL(TCP 3306) *. 이 포트는 커넥터가 있는 Insight DWH 서버에만 노출되어야 합니다

Insight에는 수십 개의 데이터 수집기가 있지만 모두 폴링 기반 Insight로 인해 획득 장치(AUS)가 다양한 장치에 대한 아웃바운드 통신을 시작합니다. 호스트 기반 방화벽이 방화벽을 통해 반환 트래픽을 허용할 수 있도록 "상태 저장"되어 있는 한 Insight Server의 호스트 기반 방화벽은 데이터 획득에 영향을 주지 않습니다.

데이터 웨어하우스 포트

Insight DWH 서버의 경우:

- 인바운드 HTTPS 443 * - TCP 443에서 Insight WebUI를 실행 중인 경우 다음 소비자를 허용하도록 해당 룰 노출해야 합니다.
- DWH 관리 포털의 Insight 관리 사용자
- 인바운드 HTTPS(TCP 9300) * - Cognos 보고 인터페이스입니다. 사용자가 Cognos 보고 인터페이스와 상호 작용할 경우 이 정보는 원격으로 노출되어야 합니다.

DWH를 노출할 필요가 없는 환경을 상상할 수 있습니다. 보고서 작성자는 DWH 서버에 RDP 연결을 만들고 보고서를 작성 및 예약하는 동시에 모든 보고서가 SMTP를 통해 전송되거나 원격 파일 시스템에 기록되도록 예약할 수 있습니다.

- 인바운드 MySQL(TCP 3306) *. 이 포트는 조직이 DWH 데이터와 MySQL 기반 통합을 수행하는 경우에만 노출되어야 합니다. - CMDB, 차지백 시스템 등과 같은 다른 애플리케이션에 대한 인제스트하기 위해 다양한 DWH 데이터 마트에서 데이터를 추출하는 경우

느린 PC 성능 분석

네트워크 사용자의 컴퓨터가 느리게 실행된다고 불평하는 전화를 받는 경우 호스트 성능을 분석하고 영향을 받는 리소스를 확인해야 합니다.

시작하기 전에

이 예제에서 호출자는 호스트 이름을 지정합니다.

단계

1. 브라우저에서 Insight를 엽니다.
2. Search assets * 상자에 호스트 이름을 입력하고 검색 결과에서 호스트 이름을 클릭합니다.

리소스의 _asset 페이지_가 열립니다.

3. 호스트의 자산 페이지에서 페이지 중앙의 성능 차트를 확인합니다. 일반적으로 사전 선택된 지연 시간 및 IOPS 외에 다른 유형의 데이터를 표시할 수 있습니다. 장치 유형에 따라 처리량, 메모리, CPU 또는 IP 처리량 등 다른 유형의 데이터에 대한 확인란을 클릭합니다.
4. 차트에 점에 대한 설명을 표시하려면 마우스 포인터를 해당 점 위에 놓습니다.
5. 또한 페이지 맨 위에 있는 선택 항목의 시간 범위를 3시간~7일 또는 사용 가능한 모든 데이터로 변경할 수도 있습니다.
6. 상호 연결된 상위 리소스 * 의 목록을 검토하여 기본 리소스와 패턴이 동일한 다른 리소스가 있는지 확인합니다.

목록의 첫 번째 자원은 항상 기본 자원입니다.

- a. 연결된 리소스 옆의 연결된 백분율을 클릭하여 연결된 활동 패턴이 기본 리소스 및 다른 리소스의 IOPS 또는 CPU에 있는지 확인합니다.
 - b. 연결된 리소스의 확인란을 클릭하여 해당 데이터를 성능 차트에 추가합니다.
 - c. 연결된 리소스의 연결된 이름을 클릭하여 자산 페이지를 표시합니다.
7. 이 예에서 볼 수 있듯이 VM의 경우 * 상호 연결된 최상위 리소스 * 에서 스토리지 풀을 찾고 스토리지 풀 이름을 클릭합니다.

관련 리소스 분석 중

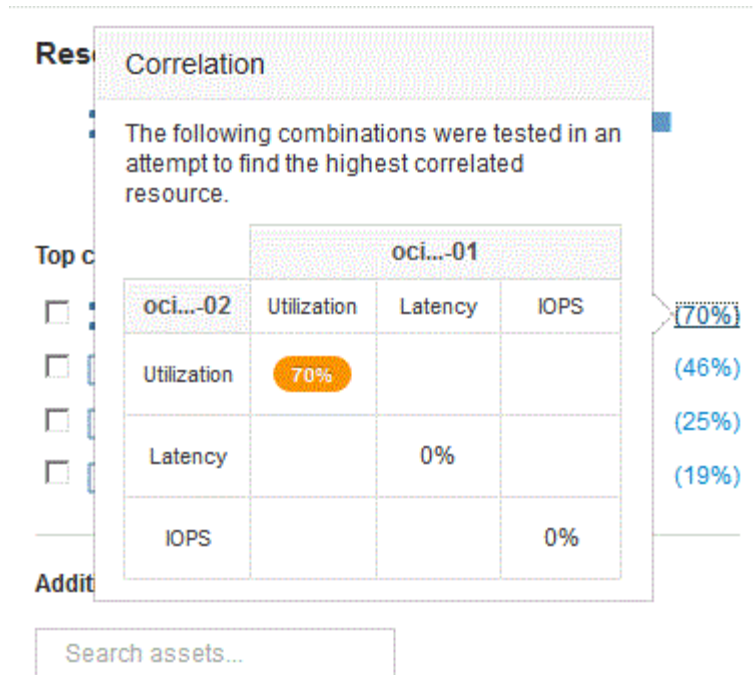
성능 문제를 조사하고 장치에 대한 _asset 페이지_를 여는 경우 상호 연결된 최상위 리소스 목록을 사용하여 성능 차트에 표시되는 데이터를 구체화해야 합니다. 백분율이 높은 자원은 기본 자원과 활동이 유사함을 나타냅니다.

이 작업에 대해

성능 문제를 조사 중이며 장치의 자산 페이지를 열었습니다.

단계

1. Top Correlated resources * 목록에서 첫 번째 리소스는 기본 리소스입니다. 목록의 상관 자원은 첫 번째 장치에 대한 상관 활동의 비율에 따라 순위가 매겨집니다. 연결된 상관 비율을 클릭하여 세부 정보를 봅니다. 이 예에서 70%의 상관관계는 사용률이므로 기본 리소스와 상호 연결된 리소스 모두 동일한 수준의 사용률을 가지고 있습니다.



- 성능 차트에 연결된 리소스를 추가하려면 추가하려는 리소스의 * 상호 연결된 최상위 리소스 * 목록에서 확인란을 선택합니다. 기본적으로 각 자원에는 사용 가능한 전체 데이터가 제공되지만 확인란의 메뉴에서 읽기 또는 쓰기 데이터만 선택할 수 있습니다.

차트의 각 리소스는 서로 다른 색을 사용하여 각 리소스의 성능 측정값을 비교할 수 있습니다. 선택한 측정 메트릭에는 적절한 유형의 데이터만 플롯됩니다. 예를 들어 CPU 데이터에는 읽기 또는 쓰기 메트릭이 없으므로 총 데이터만 사용할 수 있습니다.

- 연결된 리소스의 연결된 이름을 클릭하여 자산 페이지를 표시합니다.
- 분석에 고려되어야 한다고 생각하는 상호 연결된 최상위 리소스에 나열된 리소스가 표시되지 않으면 * 자산 검색 * 상자를 사용하여 해당 리소스를 찾을 수 있습니다.

파이버 채널 환경 모니터링

OnCommand Insight의 파이버 채널 자산 페이지를 사용하여 환경 내의 패브릭의 성능 및 인벤토리를 모니터링하고 문제를 일으킬 수 있는 변경 사항을 인지할 수 있습니다.

파이버 채널 자산 페이지

Insight의 자산 페이지에서는 리소스, 토폴로지(장치 및 연결), 성능 차트 및 관련 리소스 표에 대한 요약 정보를 제공합니다. 패브릭, 스위치 및 포트 자산 페이지를 사용하여 파이버 채널 환경을 모니터링할 수 있습니다. Fibre Channel 문제를 해결할 때 특히 유용하며, 각 포트 자산에 대한 성능 도표는 선택한 최상위 기여 포트의 트래픽을 보여 줍니다. 또한 Insight에서 각 메트릭에 대한 별도의 성능 차트를 표시하면서 이 차트에 버퍼링까지 크레딧 메트릭과 포트 오류를 표시할 수도 있습니다.

포트 메트릭에 대한 성능 정책

Insight를 사용하면 성능 정책을 생성하여 네트워크를 모니터링하여 다양한 임계값을 파악하고 이러한 임계값을 초과할 때 경고를 표시할 수 있습니다. 사용 가능한 포트 메트릭을 기준으로 포트에 대한 성능 정책을 생성할 수 있습니다. 임계값 위반이 발생하면 Insight는 빨간색 실선 원을 표시하고, 이메일 알림을 구성하고, 위반 대시보드 또는 위반을 보고하는 사용자 지정 대시보드를 통해 관련 자산 페이지에서 이를 감지하여 보고합니다.

TTL(Time-to-Live) 및 다운샘플링 데이터

OnCommand Insight 7.3부터는 데이터 보존 또는 TTL(Time-to-Live)이 7일에서 90일로 증가했습니다. 즉, 차트 및 테이블에 대해 훨씬 더 많은 데이터가 처리되고 수만 개의 데이터 포인트(datapoint)가 발생할 가능성이 있기 때문에 데이터가 표시되기 전에 다운샘플링됩니다.

다운샘플링은 차트에서 데이터의 통계적 근사치를 제공하여 수집된 데이터의 정확한 뷰를 유지하면서 모든 데이터 요소를 표시할 필요 없이 데이터를 효율적으로 개괄적으로 보여 줍니다.

다운샘플링이 필요한 이유는 무엇입니까?

Insight 7.3은 데이터의 TTL(Time-to-Live)을 90일로 늘립니다. 즉, 차트 및 그래프에 표시할 데이터를 준비하는 데 필요한 처리 양이 증가합니다. 차트를 빠르고 효율적으로 표시할 수 있도록 해당 차트의 모든 데이터 요소를 처리할 필요 없이 차트의 전체 모양을 유지하는 방식으로 데이터가 다운샘플링됩니다.



다운샘플링 중에는 실제 데이터가 손실되지 않습니다. 아래 그림에 표시된 단계를 따르면 다운샘플링된 데이터 대신 차트의 실제 데이터를 볼 수 있습니다.

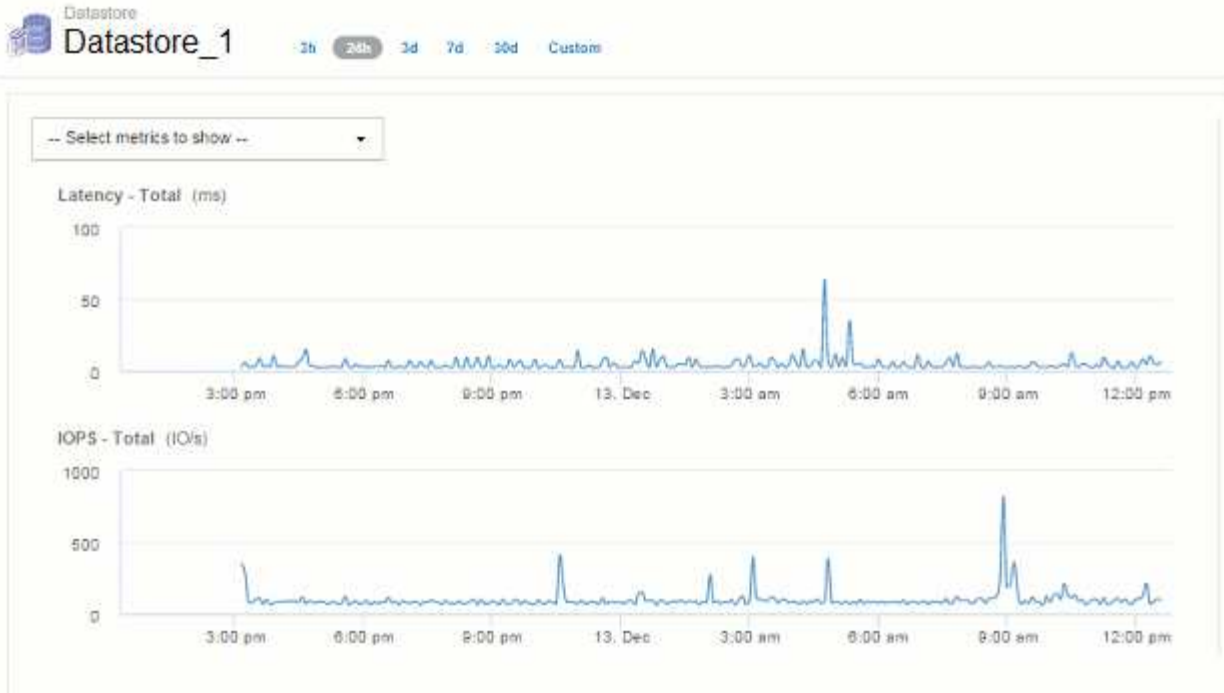
다운샘플링의 작동 방식

데이터는 다음 조건에서 다운샘플링됩니다.

- 선택한 시간 범위에 7일 이하의 데이터가 포함된 경우 다운샘플링이 발생하지 않습니다. 차트는 실제 데이터를 표시합니다.
- 선택한 시간 범위에 7일 이상의 데이터가 포함되어 있지만 데이터 요소가 1,000개 미만인 경우 다운샘플링이 발생하지 않습니다. 차트는 실제 데이터를 표시합니다.
- 선택한 시간 범위에 7일 이상의 데이터와 1,000개 이상의 데이터 요소가 포함된 경우 데이터가 다운샘플링됩니다. 차트는 근사화된 데이터를 표시합니다.

다음 예에서는 다운샘플링이 실제 작동 중인 것을 보여 줍니다. 첫 번째 그림에서는 데이터 저장소 자산 페이지의 시간 선택기에서 * 24h * 를 선택하여 24시간 동안 데이터 저장소 자산 페이지에 지연 시간 및 IOPS 차트를 보여 줍니다. 또한 * Custom * 을 선택하고 동일한 24시간 기간으로 시간 범위를 설정하여 동일한 데이터를 볼 수도 있습니다.

7일 미만의 시간 범위를 선택하고 차트에 사용할 데이터 요소가 1,000개 미만인 경우 표시되는 데이터는 실제 데이터입니다. 다운샘플링이 발생하지 않습니다.



그러나 자산 페이지 시간 선택기에서 * 30d * 를 선택하여 데이터를 보는 경우 또는 7일 이상의 사용자 지정 시간 범위를 설정하여(또는 Insight가 선택한 기간 동안 1,000개 이상의 데이터 샘플을 수집한 경우) 데이터가 표시되기 전에 다운샘플링됩니다. 다운샘플링된 차트를 확대하면 디스플레이에 근사화된 데이터가 계속 표시됩니다.



다운샘플링된 차트를 확대할 때 확대/축소는 디지털 확대/축소입니다. 디스플레이에 근사치 데이터가 계속 표시됩니다.

다음 그림에서 시간 범위가 처음 30d로 설정된 것을 볼 수 있으며, 그런 다음 차트를 확대하여 위와 동일한 24시간 기간을 표시할 수 있습니다.



다운샘플링된 차트는 위의 "실제" 차트와 동일한 24시간 기간을 보여 주므로 동일한 일반 셰이프를 따라 선이

표시되므로 성능 데이터에서 흥미로운 최고점 또는 최저점을 빠르게 찾을 수 있습니다.



다운샘플링을 위해 데이터가 근사화되기 때문에 다운샘플과 비교할 때 차트 선이 약간 꺼질 수 있습니다. 실제 데이터를 사용하여 그래프를 더 잘 정렬할 수 있습니다. 그러나 차이는 크지 않으며 표시되는 데이터의 전체 정확도에는 영향을 미치지 않습니다.

다운샘플링된 차트에 대한 위반

다운샘플링된 차트를 볼 때는 위반 사항이 표시되지 않는다는 점에 유의하십시오. 위반 사항을 보려면 다음 두 가지 중 하나를 수행합니다.

- 자산 페이지 시간 선택기에서 사용자 정의를 선택하고 7일 미만의 시간 범위를 입력하여 해당 시간 범위의 실제 데이터를 봅니다. 각 빨간색 점 위로 마우스를 가져갑니다. 도구 설명에 발생한 위반이 표시됩니다.
- 시간 범위를 기록하고 위반 대시보드에서 위반 사항을 찾습니다.

재고 기록 정리

Insight는 버전 7.3.2부터 90일 동안 인벤토리(기반) 변경 기록을 유지합니다. 이전 버전의 Insight에서는 설치 시점의 모든 재고 변경 내역이 유지됩니다. 이전 버전의 Insight에서 업그레이드한 후 오래된 재고 기록은 로 정리된 후 90일 동안 유지됩니다.

최신 버전의 OnCommand Insight로 업그레이드한 후 가장 최근 90일 동안 기록이 정리됩니다. Insight는 가장 오래된 것부터 시작하여 90일 분량의 역사가 남아 있을 때까지 하루에 한 번 30일 단위로 역사를 정리합니다. 그런 다음, 매일 역사를 정리하여 90일 동안의 재고 변경 내역을 유지합니다.

VM의 NAS 경로입니다

OnCommand Insight 7.3은 가상 머신에서 스토리지 공유에 대한 NAS 경로를 지원합니다. 이러한 경로는 호스트에서 스토리지 공유에 대한 NAS 경로와 유사합니다. VM의 IP 주소가 공유에 액세스할 수 있으면 NAS 경로가 생성됩니다.

가상 머신의 NAS 경로는 내부 볼륨 랜딩 페이지에 표시됩니다. 이 페이지에는 VM이 액세스할 수 있는 내부 볼륨을 식별하는 게스트 마운트 스토리지 리소스 위젯이 포함되어 있습니다.

- NAS 경로는 가상 머신이 백엔드 공유에 액세스할 수 있을 때 생성됩니다. 가상 머신이 공유에 액세스하는지 여부에 대한 확인은 없습니다.
- 상관 관계 계산은 지연 시간과 IOPS를 기반으로 하며 VM에 백엔드 스토리지에 대한 NAS 경로가 있는 경우는 포함되지 않습니다.
- 사용자는 이니시에이터 IP 주소로 공유를 쿼리할 수 있지만, 경로로 쿼리하는 것은 지원되지 않습니다.

이제 내부 볼륨의 컴퓨팅 리소스 표에 NAS 경로가 있는 VM도 표시됩니다. 각 VM, CPU 및 메모리에 대해 사용률 및 성능 데이터가 제공됩니다.

데이터 웨어하우스에 미치는 영향

OnCommand Insight 7.3으로 업그레이드한 후 표시되는 데이터 웨어하우스의 변경 사항은 다음과 같습니다.

- dWh_inventory.nas_logical 테이블이 Inventory Data Mart에서 제거되고 보기로 교체됩니다.

NFS 경로 테이블이 포함된 Insight 7.2.x 보고서는 그대로 유지됩니다.

- dWh_inventory.nas_cr_logical 테이블이 Inventory Data Mart에 추가되고 다음 항목이 포함됩니다.
 - 컴퓨팅 리소스
 - 내부 볼륨
 - 스토리지
 - NAS 공유

시간 시리즈로서의 용량

OnCommand Insight 7.3.1에서는 용량 정보가 시간 시리즈 데이터로 보고되고 차트로 작성됩니다.

이전에는 데이터 소스에서 가져온 용량 정보가 "시점" 데이터(PIT)로만 제공되기 때문에 차트에서 시계열 데이터로 사용할 수 없었습니다. 이제 자산의 용량 값을 다음과 같은 방법으로 시계열 데이터로 사용할 수 있습니다.

- 표, 위젯, 전문가 뷰 및 시계열 데이터가 표시되는 모든 위치에 그래프로 표시됩니다
- 기존 의미를 사용하는 위반의 성능 임계값에 적용됩니다
- 필요한 경우 다른 성능 카운터와 함께 식에 사용됩니다

이전 버전의 Insight에서 업그레이드하는 경우 쿼리 또는 사용자 지정 대시보드의 필터에 사용된 이전 PIT 용량 값이 시계열 용량 데이터로 대체됩니다. 따라서 이전 Insight 버전의 동급 데이터와 비교할 때 용량 데이터가 보고되거나 필터링되는 방식이 약간 변경될 수 있습니다.

데이터 웨어하우스 관리

OnCommand Insight 데이터 웨어하우스에 오신 것을 환영합니다

OnCommand Insight 데이터 웨어하우스는 여러 OnCommand Insight 서버의 데이터를 저장하고 쿼리 및 분석을 위한 공통의 다차원 데이터 모델로 데이터를 변환하는 중앙 집중식 저장소입니다.

OnCommand Insight 데이터 웨어하우스를 사용하면 지불 거절 보고서, 내역 데이터가 포함된 추세 보고서, 소비 분석 및 예측 보고서와 같은 사용자 정의 용량 및 성능 보고서를 생성할 수 있는 여러 데이터 마트로 구성된 공개 데이터베이스에 액세스할 수 있습니다.

데이터 웨어하우스 기능

OnCommand Insight 데이터 웨어하우스는 여러 데이터 마트로 구성된 독립 데이터베이스입니다.

데이터 웨어하우스에는 다음과 같은 기능이 있습니다.

- 현재 및 기간별 구성 및 인벤토리 데이터를 통해 예측 및 계획에 유용한 추세 보고서를 생성할 수 있습니다
- 여러 다차원 내역 데이터 마트와 추가 현재 전용 인벤토리 데이터 마트가 있습니다
- 미리 정의된 쿼리 또는 사용자 정의 쿼리에 최적화된 데이터베이스입니다
- 타사 보고 및 비즈니스 인텔리전스 엔진과의 통합을 위한 플랫폼:
 - 구성 관리 데이터베이스
 - 재무 회계 시스템
 - 자산 관리 시스템

데이터 웨어하우스 구성 요소

데이터 웨어하우스에는 여러 구성 요소가 포함되어 있습니다.

- 데이터 웨어하우스 포털
- OnCommand Insight 보고 포털
- 보고서 작성 도구

데이터 웨어하우스 포털을 사용하여 수행할 수 있는 작업

데이터 웨어하우스 포털은 옵션을 구성하고 데이터를 검색하기 위한 고정 일정을 설정하는 데 사용하는 웹 기반 사용자 인터페이스입니다. 데이터 웨어하우스 포털에서 OnCommand Insight 보고 포털에 액세스할 수도 있습니다.

데이터 웨어하우스 포털을 사용하여 다음을 수행할 수 있습니다.

- OnCommand Insight 보고 포털에 액세스하여 미리 디자인된 보고서를 보거나 보고서 작성 도구를 사용하여

사용자 지정 보고서를 만들 수 있습니다.

- 여러 OnCommand Insight 데이터베이스 통합
- OnCommand Insight 서버에 대한 연결을 관리합니다.
- 실행 중인 현재 작업 또는 쿼리의 상태를 확인합니다.
- 데이터 웨어하우스 빌드 예약
- 사이트 이름을 편집합니다.
- 모듈 버전, 사이트 및 라이선스와 같은 특정 정보를 포함한 데이터 웨어하우스 버전 및 업그레이드 기록을 봅니다.
- 주식 불러오기.
- 기록에서 빌드를 구성합니다.
- 데이터 웨어하우스 설명서 및 데이터베이스 스키마를 봅니다.
- 데이터 웨어하우스 데이터베이스를 재설정합니다.
- 데이터 웨어하우스 데이터베이스를 백업 및 복원합니다.
- 데이터 웨어하우스 문제를 해결합니다.
- 사용자 계정을 관리합니다.

데이터 웨어하우스 소프트웨어 구성 요소

OnCommand Insight 데이터 웨어하우스에는 여러 소프트웨어 구성 요소가 포함되어 있습니다.

- MySQL 데이터베이스

Data Mart 테이블의 백엔드 저장소입니다

- IBM Cognos

OnCommand Insight의 보고 엔진입니다

- Apache Derby 데이터베이스

Cognos 구성 및 콘텐츠를 저장하는 데 사용됩니다

- 와일드플라이

OnCommand Insight 구성 요소를 호스팅하는 Java Enterprise 애플리케이션 서버입니다

데이터 웨어하우스 프로세스

데이터 웨어하우스는 다양한 유형의 프로세스를 수행합니다.

- ETL 프로세스 *

ETL(Extract Transform and Load) 프로세스는 여러 OnCommand Insight 데이터베이스에서 데이터를 검색하고, 데이터를 변환하여 데이터 마트에 저장합니다. 데이터 웨어하우스 구축 프로세스는 ETL 프로세스입니다.

• * 작업 *

데이터 웨어하우스는 인벤토리, 차원, 용량, 포트 용량, VM 용량 등의 작업을 수행하고 보고합니다. 파일 시스템 활용률, 성능, 용량 효율성, 라이선스, 내역 구축, 동적 주석, 커넥터 제거, 건너뛴 빌드, ASUP 옵션 및 유지보수 작업.

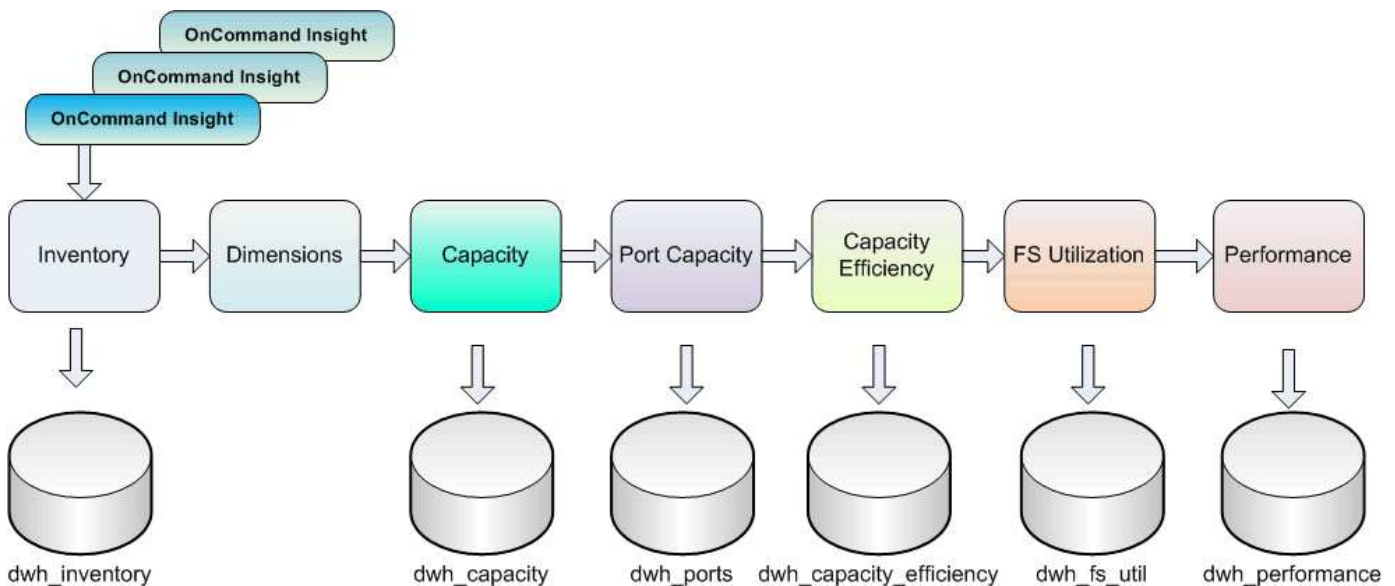
• * 통합 프로세스 *

데이터 웨어하우스는 여러 OnCommand Insight 서버를 동일한 데이터 웨어하우스 데이터베이스로 통합할 수 있도록 지원합니다. 여러 구성에서 동일한 개체가 여러 커넥터에서 보고될 수 있습니다(즉, 동일한 스위치가 두 개의 OnCommand Insight 인스턴스에 있을 수 있음). 이 경우 데이터 웨어하우스는 여러 오브젝트를 하나로 통합합니다(기본 커넥터가 선택되고 개체의 데이터는 해당 커넥터에서만 가져와짐).

데이터 웨어하우스가 데이터를 추출하는 방법

ETL(Extract, Transform, Load) 프로세스는 여러 OnCommand Insight 데이터베이스에서 데이터를 검색하고 데이터를 변환하여 데이터 마트에 저장합니다.

OnCommand Insight 커넥터는 여러 OnCommand Insight MySQL 데이터베이스에서 데이터를 추출하고 다음 다이어그램에 표시된 대로 다양한 데이터 마트에 데이터를 게시하기 위해 일련의 배치 작업을 호출합니다.



ETL 프로세스는 다음과 같은 개별 프로세스를 포함합니다.

• 압축 풀기 *

이 프로세스는 여러 OnCommand Insight 데이터베이스의 데이터를 가져와 변환하여 데이터 마트에 저장합니다. 이 프로세스는 각 OnCommand Insight 인스턴스에 대해 동시에 수행됩니다. 데이터 정리 및 데이터 중복 제거가 수행되도록 하려면 ETL 프로세스를 여러 개의 예약된 ETL 작업으로 분할할 수 없습니다.

• * 변환 *

이 프로세스는 비즈니스 로직 규칙 또는 함수를 적용하여 OnCommand Insight 데이터베이스에서 데이터를 추출합니다.

• * 로드 *

이 프로세스는 변환된 데이터를 공용 데이터 마트로 로드합니다.

ETL 빈도 및 날짜 데이터

압축 풀기, 변환 및 로드(ETL) 프로세스를 하루에 한 번 이상 실행해야 합니다. 그러나 필요한 경우 ETL을 여러 번 실행하도록 선택할 수 있습니다.

기본적으로 Cognos 보고 엔진은 모든 용량 및 성능 팩트를 추가 기능으로 처리합니다. 따라서 적절한 시간 필터 없이 하루에 ETL 프로세스를 여러 번 실행하면 용량 데이터가 두 배로 계산될 위험이 있습니다.

날짜 차원에 있는 두 날짜 데이터 요소는 일별 ETL 프로세스와 관련됩니다. 여러 데이터 모델에서 사용되는 Date 차원은 ETL의 영향을 받는 다음과 같은 데이터 요소를 포함합니다.

• * 일 대표 * 입니다

"IS Day Representative" 데이터 요소는 지정된 날짜 동안 첫 번째 ETL 프로세스가 실행되는 동안 1(TRUE)의 값으로 설정됩니다. 첫 번째 ETL 프로세스가 오전 1시에 실행되면 오전 1시에 로드된 모든 데이터에 대해 Day Representative가 1로 설정됩니다 ETL 프로세스. 두 번째 ETL이 나중에 예약된 경우(예: 오후 1:00), IS Day Representative는 해당 ETL 프로세스 중에 로드된 데이터에 대해 0(false)으로 설정됩니다.

• * 는 최신 * 입니다

"is latest" 멤버는 각 ETL 프로세스가 완료된 후 1(TRUE)의 값으로 설정됩니다. 첫 번째 ETL 프로세스가 오전 1:00에 실행되면 오전 1:00에 로드된 모든 데이터에 대해 가 최신인 가 1로 설정됩니다 ETL 프로세스. 나중에 다른 ETL 프로세스가 예약되면(예: 오후 1:00), 는 오후 1:00 동안 로드된 데이터에 대해 1로 설정됩니다 ETL 프로세스. ETL 프로세스는 오전 1시도 설정합니다 ETL 로드가 0에 가장 최근 항목입니다(FALSE).

과거 데이터가 데이터 웨어하우스에 보관되는 방식

데이터 웨어하우스는 일정에 따라 데이터를 유지 관리합니다. 데이터가 오래되면 데이터 레코드 보존이 줄어듭니다.

데이터 웨어하우스는 다음 표와 같이 데이터 마트와 데이터 세분화를 기반으로 기간별 데이터를 보유합니다.

데이터 마트	측정 대상	세분화	보존 기간
성능 마트	볼륨 및 내부 볼륨	매시간	14일
성능 마트	볼륨 및 내부 볼륨	매일	13개월
성능 마트	응용 프로그램	매시간	13개월
성능 마트	호스트	매시간	13개월
성능 마트	포트의 스위치 성능	매시간	5주

성능 마트	호스트, 스토리지 및 테이프의 스위치 성능	매시간	13개월
성능 마트	스토리지 노드	매시간	14일
성능 마트	스토리지 노드	매일	13개월
성능 마트	VM 성능	매시간	14일
성능 마트	VM 성능	매일	13개월
성능 마트	하이퍼바이저 성능	매시간	14일
성능 마트	하이퍼바이저 성능	매일	13개월
성능 마트	VMDK 성능	매시간	14일
성능 마트	VMDK 성능	매일	13개월
성능 마트	디스크 성능	매시간	14일
성능 마트	디스크 성능	매일	13개월
용량 마트	모두(개별 볼륨 제외)	매일	13개월
용량 마트	모두(개별 볼륨 제외)	월간 담당자	14개월 이상
재고 마트	개별 볼륨	현재 상태	1일(또는 다음 ETL이 될 때까지)

13개월 후(구성 가능) 데이터 웨어하우스는 다음 팩트 테이블에서 용량, 성능 및 리소스 데이터에 대해 하루 한 개의 레코드 대신 매월 한 개의 레코드만 보유합니다.

- 차지백 팩트 테이블(dwh_capacity.chargeback_fact)
- 파일 시스템 사용률 팩트 테이블(dWh_fs_util.fs_util_fact)
- 호스트 팩트 테이블(dWh_sa.sa_host_fact)
- 내부 볼륨 용량 팩트 테이블(dwh_capacity.internal_volume_capacity_fact)
- 포트 팩트 테이블(dWh_ports.ports_fact)
- qtree 용량 팩트 테이블(dWh_capacity.qtree_capacity_fact)
- 스토리지 및 스토리지 풀 용량 팩트 테이블(dWh_capacity.storage_and_storage_pool_capacity_fact)
- 볼륨 용량 팩트 테이블(dWh_capacity.vm_capacity_fact)

- 스토리지 노드 시간별 성능(storage_node_hourly_performance_fact) 및 스토리지 노드 일별 성능(storage_node_daily_performance_fact) 팩트 테이블

데이터 보존, ETL 및 기간

OnCommand Insight 데이터 웨어하우스는 ETL(Extract, Transform, Load) 프로세스에서 얻은 데이터를 데이터의 다양한 데이터 마트와 시간 세분화에 따라 다른 기간 동안 보존합니다.

볼륨 및 내부 볼륨에 대한 성능 및 시간 단위 세분화

OnCommand Insight 데이터 웨어하우스는 14일 동안 하루 중 각 시간(24개 데이터 포인트)에 대한 시간별 평균, 시간별 최대값 및 액세스 비트를 기록합니다. 액세스 비트는 매시간 간격 동안 볼륨에 액세스하지 않을 경우 true 이고, 볼륨이 액세스되지 않으면 false 입니다. 이전 날짜의 모든 24개 데이터 포인트는 해당 날짜의 첫 번째 ETL 프로세스 중에 얻어집니다.

시간별 데이터 지점을 수집하기 위해 시간당 하나의 ETL 프로세스를 실행할 필요가 없습니다. 하루 동안 추가 ETL 프로세스를 실행해도 OnCommand Insight 서버에서 성능 정보를 얻을 수 없습니다.

볼륨 및 내부 볼륨에 대한 성능 마트와 일일 세분화를 설명합니다

ETL을 처리할 때마다 데이터 웨어하우스 내에서 전날의 일별 평균이 계산되고 채워집니다. 일일 평균은 전날의 24개 데이터 요소에 대한 요약입니다. 성능 데이터 마트는 13개월 동안 볼륨 및 내부 볼륨에 대한 일일 요약을 보존합니다.

용량 마트 및 매일 단위

용량 마트는 13개월 동안 매일 다양한 용량 팩트에 대한 일일 측정을 제공합니다. 데이터 웨어하우스의 용량 팩트는 ETL 이전에 장치에 대한 마지막 데이터 소스 취득의 최신 상태입니다.

용량 마트 및 월별 세분성

데이터 웨어하우스는 13개월 동안 일일 용량 데이터를 보존합니다. 13개월 임계값에 도달하면 용량 데이터가 월별 기준으로 요약됩니다. 월별 데이터는 월별 대표 날짜인 날짜에 반영된 값을 기준으로 합니다.

다음 표는 월별 요약에 포함되는 월별 데이터를 보여줍니다.

날짜	은(는) 월 대표 값입니다	할당된 용량입니다
1월 1일	1(참)	50TB
1월 2일	0(거짓)	52TB
...
1월 31일	0(거짓)	65TB
2월 1일	1(참)	65TB

이 표에 따르면 월별 보고서에는 1월에 할당된 50TB와 2월에 할당된 65TB가 표시됩니다. 1월의 다른 모든 용량 값은 월별 요약에 포함되지 않습니다.

재고 데이터 마트는 기록이 아닙니다. ETL 프로세스가 실행될 때마다 Inventory Mart가 삭제되고 재구축됩니다. 따라서 재고 마트에서 생성된 모든 보고서는 과거 재고 구성을 반영하지 않습니다.

데이터 웨어하우스 시작

OnCommand Insight 데이터 웨어하우스를 사용하면 데이터를 포함하는 보고서를 생성하기 전에 필요한 옵션을 구성할 수 있습니다. 데이터 웨어하우스에는 많은 기능이 포함되어 있지만 시작하기 위해서는 몇 가지 기능만 사용해야 합니다. 데이터 웨어하우스를 설정하려면 데이터 웨어하우스 포털의 옵션을 사용합니다.

이 작업에 대해

OnCommand Insight 데이터 웨어하우스를 설정하려면 스토리지 관리자가 다음 절차를 완료해야 합니다.

- 데이터 웨어하우스 포털에 액세스
- OnCommand Insight 서버에 데이터 웨어하우스 연결
- 기록에서 데이터베이스 작성
- 백업 및 복원 프로세스 설정

또한 스토리지 관리자는 다음 절차를 완료할 수 있습니다.

- 명령줄 인터페이스를 사용하여 MySQL 액세스
- 일별 빌드 예약
- 보고에서 다중 임차 설정
- 설치 문제 해결
 - 내 주석이 표시되지 않는 이유는 무엇입니까?
 - 실패한 기간별 빌드 포인트에 대해 어떻게 해야 합니까?

Data Warehouse Portal을 처음 사용하는 경우 작업 페이지에 정보를 표시하려면 먼저 데이터 웨어하우스를 설정해야 합니다. 또한 데이터 웨어하우스 데이터베이스를 재설정 후 이 설정 프로세스를 반복해야 합니다.

데이터 웨어하우스 포털에 액세스

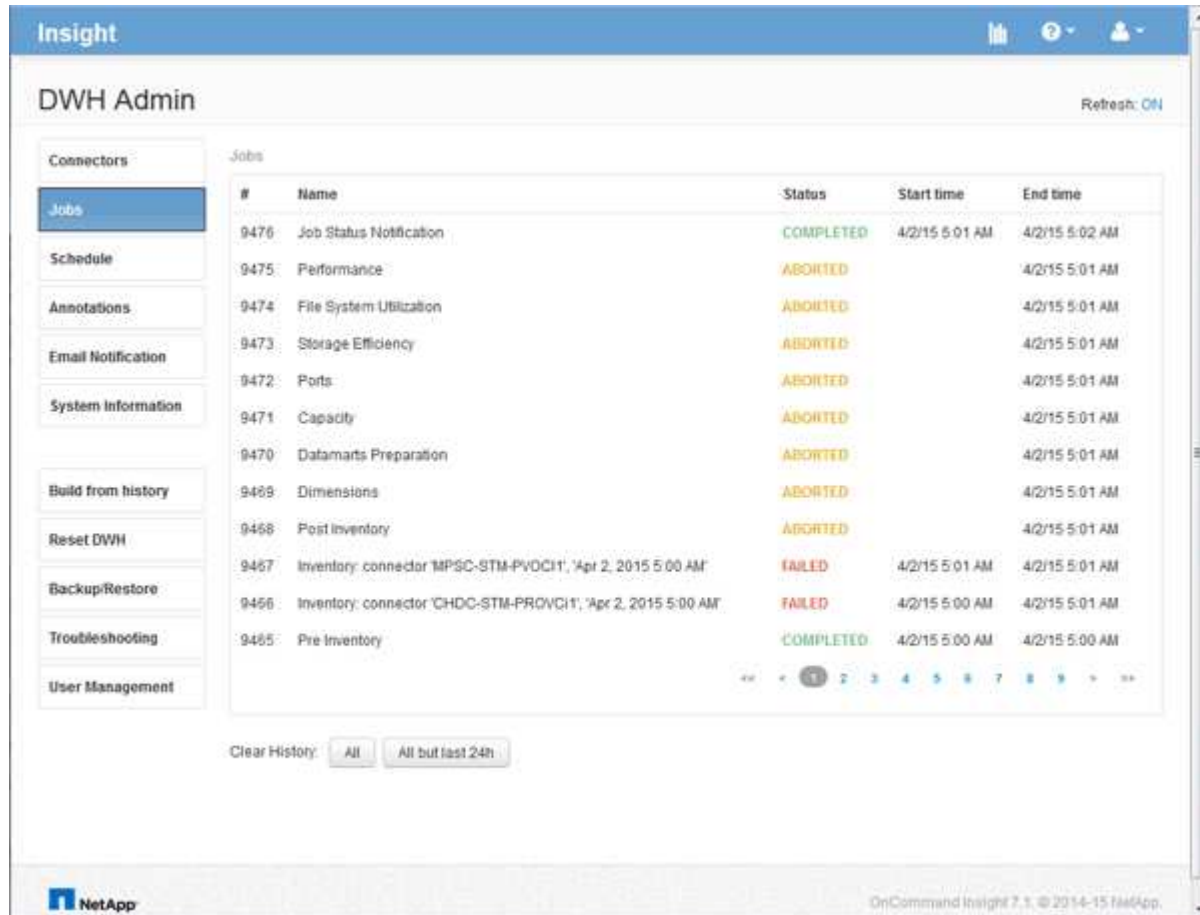
OnCommand Insight 데이터 웨어하우스 포털은 커넥터 정보 업데이트, 작업 대기열 보기, 일별 빌드 예약, 주식 선택, 이메일 알림 설정, 시스템 정보 보기, 데이터베이스 구축, 데이터 웨어하우스 재설정, 데이터베이스 백업 및 복원, 문제 해결, 데이터 웨어하우스 및 보고 포털 사용자 계정을 관리하고 문서 및 스키마 다이어그램에 액세스합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 사용자 이름과 암호를 입력합니다.

3. 로그인 * 을 클릭합니다.

데이터 웨어하우스 포털이 열립니다.



데이터 웨어하우스 및 보고 사용자 계정 관리

OnCommand Insight 보고 도구에 대한 사용자 계정, 사용자 인증 및 사용자 인증은 DWH(데이터 웨어하우스)에서 정의 및 관리됩니다. 이러한 구성을 기반으로 사용자와 관리자는 사용 가능한 OnCommand Insight 보고서의 일부 또는 전체에 액세스할 수 있습니다.

데이터 웨어하우스에서 사용자 관리에 액세스하려면 시스템 관리자 권한이 있는 계정이 필요합니다. 여기에는 다음이 포함됩니다.


- 데이터 웨어하우스를 위한 완벽한 관리 기능
- 모든 사용자 계정의 구성 및 유지 관리
- 데이터베이스에 대한 읽기 액세스
- ETL에서 커넥터를 설정하고, 데이터 웨어하우스 작업을 예약하고, 데이터베이스를 재설정하고, 역할을 할당하거나 변경하고, 사용자 계정을 추가 및 제거하는 기능

데이터 웨어하우스 및 보고 포털 액세스

데이터 웨어하우스 포털은 관리 옵션에 대한 액세스를 제공합니다. 데이터 웨어하우스 포털에서

보고 포털에 액세스할 수도 있습니다.

단계

1. Data Warehouse 포털에 관리자로 로그인합니다 `https://hostname/dwh`, 위치 `hostname` OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 데이터 웨어하우스 도구 모음에서  보고 포털을 엽니다.

사용자 역할을 보고합니다

각 사용자 계정에는 권한 집합이 있는 역할이 할당됩니다. 사용자 수는 각 역할에 연결된 보고 라이선스 수에 따라 제한됩니다.

각 역할은 다음 작업을 수행할 수 있습니다.

• * 수신자 *

OnCommand Insight 보고 포털 보고서를 보고 언어 및 표준 시간대와 같은 개인 기본 설정을 설정합니다.



받는 사람은 보고서를 만들거나, 보고서를 실행하거나, 보고서를 예약하거나, 보고서를 내보내거나, 관리 작업을 수행할 수 없습니다.

• * 기업 소비자 *

보고서를 실행하고 모든 사용자 옵션을 수행합니다.

• * 비즈니스 저자 *

예약된 보고서를 보고, 대화형으로 보고서를 실행하고, 스토리를 만들고, 모든 비즈니스 소비자 옵션을 수행합니다.

• * 프로 작가 *

모든 Business Author 옵션을 수행할 뿐 아니라 보고서를 만들고 패키지 및 데이터 모듈을 만듭니다.

• * 관리자 *

보고서 정의 가져오기 및 내보내기, 보고서 구성, 데이터 소스 구성, 보고 작업 종료 및 재시작 등의 보고 관리 작업을 수행합니다.

다음 표에는 각 역할에 허용되는 권한 및 최대 사용자 수가 나와 있습니다.

피처	받는 사람	비즈니스 소비자	비즈니스 저자	프로 작가	관리자
팀 콘텐츠 탭에서 보고서를 봅니다	예	예	예	예	예
보고서를 실행합니다	아니요	예	예	예	예

보고서 예약	아니요	예	예	예	예
외부 파일을 업로드합니다	아니요	아니요	예	예	아니요
스토리 만들기	아니요	아니요	예	예	아니요
보고서 작성	아니요	아니요	예	예	아니요
패키지 및 데이터 모듈을 생성합니다	아니요	아니요	아니요	예	아니요
관리 작업을 수행합니다	아니요	아니요	아니요	아니요	예
사용자 수	OnCommand Insight 사용자 수입니다	20	2	1	1

새 데이터 웨어하우스 및 보고 사용자를 추가할 때 역할의 제한을 초과하면 해당 사용자는 "비활성화"로 추가되며, 새 사용자 멤버십을 부여하려면 해당 역할을 가진 다른 사용자를 비활성화 또는 제거해야 합니다.



보고서 작성 기능을 사용하려면 Insight Plan 라이선스가 필요합니다. ARAP(Additional Report Authoring Package)를 구매하여 비즈니스 작성자 및 Pro Author 사용자를 추가할 수 있습니다. 도움이 필요하면 OnCommand Insight 담당자에게 문의하십시오.

이러한 보고 사용자 역할은 직접 데이터베이스 액세스에 영향을 주지 않습니다. 이러한 보고 사용자 역할은 데이터 마트를 사용하여 SQL 쿼리를 만드는 기능에 영향을 주지 않습니다.

보고 사용자 추가

보고 포털에 액세스해야 하는 각 사용자에게 대해 새 사용자 계정을 추가해야 합니다. 각 사용자에게 대해 다른 사용자 계정을 만들면 액세스 권한, 개인 기본 설정 및 책임을 제어할 수 있습니다.

시작하기 전에

보고 사용자를 추가하기 전에 고유한 사용자 이름을 할당하고, 사용할 암호를 결정하고, 올바른 사용자 역할 또는 역할을 확인해야 합니다. 이러한 역할은 보고 포털에 전문화되어 있습니다.

단계

1. Data Warehouse Portal()에 관리자로 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 사용자 관리 * 를 클릭합니다.
3. 사용자 관리 * 창에서 * 새 사용자 추가 * 를 클릭합니다.
4. 새 보고 사용자에게 대해 다음 정보를 입력합니다.

◦ * 사용자 이름 *

계정에 대한 사용자 이름(영숫자, a-z, A-Z 및 0-9 포함)

◦ * 이메일 주소 *

사용자 계정과 연결된 이메일 주소이며 사용자가 보고서를 구독하는 경우 필요합니다

◦ * 암호 *

사용자가 일반적으로 선택하고 인터페이스에서 확인할 수 있는 이 사용자 계정으로 OnCommand Insight에 로그인하기 위한 암호입니다

◦ * Insight 역할 *

적절한 권한이 있는 사용자가 사용할 수 있는 역할



OnCommand Insight 역할의 옵션은 OnCommand Insight가 보고 기능과 동일한 시스템에 설치되어 있는 경우에만 표시되며, 이는 일반적인 옵션은 아닙니다.

◦ * 보고 역할 *

이 사용자 계정에 대한 보고 역할(예: Pro Author)



관리자 역할은 고유합니다. 이 역할은 모든 사용자에게 추가할 수 있습니다.

5. 추가 * 를 클릭합니다.

사용자 계정 관리

데이터 웨어하우스 포털에서 사용자 계정, 사용자 인증 및 사용자 인증을 구성할 수 있습니다. 각 사용자 계정에는 다음 권한 수준 중 하나를 가진 역할이 할당됩니다. 사용자 수는 각 역할에 연결된 보고 라이선스 수에 따라 제한됩니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 사용자 관리 * 를 클릭합니다.

Name	OnCommand Insight roles			Reporting roles					E-mail				
	Guest	User	Administrator	Recipient	Business Consumer	Business Author	Pro Author	Administrator					
guest	X									Edit	Delete	Change password	Deactivate
user	X	X								Edit	Delete	Change password	Deactivate
admin	X	X	X				X	X		Edit		Change password	
oadmin	X	X	X							Edit		Change password	Deactivate

LDAP Configuration Add New User Change DWH User password

The following table shows the privileges for each reporting role:

Feature	Recipient	Business Consumer	Business Author	Pro Author	Administrator
View reports (in Public Folder tab, My Folders)	Yes	Yes	Yes	Yes	Yes
Run reports	No	Yes	Yes	Yes	Yes
Schedule Reports	No	Yes	Yes	Yes	Yes
Create reports in Query Studio	No	No	Yes	Yes	No
Create reports in Workspace (Standard)	No	Yes	Yes	Yes	No
Create reports in Workspace (Advanced)	No	No	Yes	Yes	No
Create reports in Report Studio	No	No	No	Yes	No
Perform administrative tasks	No	No	No	No	Yes

3. 다음 중 하나를 수행합니다.

- 기존 사용자를 편집하려면 사용자의 행을 선택하고 * 편집 * 을 클릭합니다.
- 사용자 암호를 변경하려면 사용자의 행을 선택하고 * 암호 변경 * 을 클릭합니다.
- 사용자를 삭제하려면 해당 사용자의 행을 선택하고 * Delete * (삭제 *)를 클릭합니다

4. 사용자를 활성화 또는 비활성화하려면 사용자의 행을 선택하고 * 활성화 * 또는 * 비활성화 * 를 클릭합니다.

보고를 위해 LDAP 구성

관리자는 데이터 웨어하우스 포털에서 데이터 웨어하우스 및 보고에 대한 LDAP 사용을 구성할 수 있습니다.

시작하기 전에

이 작업을 수행하려면 Insight에 관리자로 로그인해야 합니다.

모든 보안 Active Directory(예: LDAPS) 사용자의 경우 인증서에 정의된 대로 AD 서버 이름을 정확히 사용해야 합니다. 보안 AD 로그인에 IP 주소를 사용할 수 없습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname` OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 사용자 관리 * 를 클릭합니다.
3. LDAP 구성 * 을 클릭합니다.
4. LDAP 사용자 인증 및 인증 프로세스를 시작하려면 * LDAP 활성화 * 를 선택합니다.
5. LDAP를 구성하는 데 필요한 모든 변경 작업을 수행합니다.

대부분의 필드에는 기본값이 포함되어 있습니다. 기본 설정은 Active Directory에 유효합니다.

- * 사용자 기본 이름 속성 *

LDAP 서버의 각 사용자를 식별하는 속성입니다. 기본값은 입니다 `userPrincipalName` 이는 세계적으로 고유한 기능입니다. OnCommand Insight는 이 특성의 내용과 위에서 제공한 사용자 이름을 일치시킵니다.

◦ * 역할 속성 *

지정된 그룹 내에서 사용자의 맞춤을 식별하는 LDAP 속성입니다. 기본값은 입니다 `memberOf`.

◦ * 메일 속성 *

사용자의 이메일 주소를 식별하는 LDAP 속성입니다. 기본값은 입니다 `mail`. 이 기능은 OnCommand Insight에서 제공하는 보고서를 구독하려는 경우에 유용합니다. Insight는 각 사용자가 처음 로그인할 때 사용자의 이메일 주소를 선택하며, 그 후에는 이를 찾아보지 않습니다.



LDAP 서버에서 사용자의 이메일 주소가 변경되면 Insight에서 업데이트해야 합니다.

◦ * 고유 이름 특성 *

사용자의 고유 이름을 식별하는 LDAP 속성입니다. 기본값은 입니다 `distinguishedName`.

◦ * 참조 *

엔터프라이즈에 여러 도메인이 있는 경우 다른 도메인에 대한 경로를 따르는지 여부를 나타냅니다. 항상 기본값을 사용해야 합니다 `follow` 설정.

◦ * 시간 초과 *

시간 초과 전에 LDAP 서버의 응답을 기다리는 시간(밀리초)입니다. 기본값은 2,000이며, 모든 경우에 적절하며 수정할 수 없습니다.

◦ LDAP 서버 *

LDAP 서버를 식별하기 위한 IP 주소 또는 DNS 이름입니다. 특정 포트를 식별하기 위해 `ldap-server-address` LDAP 서버의 이름이며 다음 형식을 사용할 수 있습니다.

```
ldap://ldap-server-address:port
```

기본 포트를 사용하려면 다음 형식을 사용할 수 있습니다.

```
ldap://ldap-server-address
```



When entering multiple LDAP servers in this field, separate entries with a comma, and ensure that the correct port number is used in each entry.

+ LDAP 인증서를 가져오려면 * 인증서 가져오기 * 를 클릭하고 인증서 파일을 자동으로 가져오거나 수동으로 찾습니다.

- * 도메인 *

OnCommand Insight가 LDAP 사용자를 찾기 시작해야 하는 LDAP 노드입니다. 일반적으로 조직의 최상위 도메인입니다. 예를 들면 다음과 같습니다.

```
DC=<enterprise>,DC=com
```

- * Insight 서버 관리자 그룹 *

Insight Server 관리자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.server.admins`.

- * Insight 관리자 그룹 *

Insight Administrator 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.admins`.

- * Insight 사용자 그룹 *

Insight 사용자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.users`.

- * Insight 게스트 그룹 *

Insight 게스트 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.guests`.

- * 보고 관리자 그룹 *

Insight Reporting 관리자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.report.admins`.

- * 보고 전문가 그룹 *

Insight Reporting Pro 작성자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.report.proauthors`.

- * 보고 비즈니스 저자 그룹 *

Insight Reporting 비즈니스 작성자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.report.business.authors`.

- * 비즈니스 소비자 그룹 보고 *

Insight Reporting 비즈니스 소비자 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.report.business.consumers`.

- * 보고 수신자 그룹 *

Insight Reporting 받는 사람 권한이 있는 사용자를 위한 LDAP 그룹입니다. 기본값은 `insight.report.recipients`.

6. 변경한 경우 * 디렉터리 조회 사용자 * 및 * 디렉터리 조회 사용자 암호 * 필드에 값을 입력합니다.

이러한 필드에 수정된 값을 입력하지 않으면 변경 내용이 저장되지 않습니다.

7. 디렉터리 조회 사용자 암호 확인 * 필드에 디렉터리 조회 사용자 암호를 다시 입력하고 * 암호 확인 * 을 클릭하여 서버에서 암호를 확인합니다.
8. Update * 를 클릭하여 변경 사항을 저장합니다. 변경 사항을 제거하려면 * 취소 * 를 클릭합니다.

OnCommand Insight 서버에 데이터 웨어하우스 연결

커넥터는 OnCommand Insight 데이터 웨어하우스에서 OnCommand Insight 서버로의 연결을 설정합니다. 데이터 웨어하우스를 하나 이상의 OnCommand Insight 서버에 연결할 수 있습니다. OnCommand Insight 데이터베이스에 대한 연결을 추가하거나 데이터베이스에서 연결을 제거할 수 있습니다.

이 작업에 대해

데이터 웨어하우스는 커넥터 이름과 함께 사용되는 커넥터에 글로벌 고유 ID를 할당합니다. 커넥터를 추가한 후 데이터 웨어하우스는 OnCommand Insight 데이터베이스에서 OnCommand Insight 사이트 이름 및 버전을 쿼리합니다.

SSL을 사용하거나 사용하지 않고 데이터 원본에 연결하도록 선택할 수 있습니다. 보안 데이터 소스를 선택하면 OnCommand Insight 원격 데이터베이스와 통신할 때 연결이 SSL을 사용하게 됩니다.

데이터 웨어하우스는 여러 OnCommand Insight 설치에서 통합된 데이터 뷰를 제공할 수 있습니다. 이 통합 데이터베이스는 다음 정보를 제공합니다.

- 전역적으로 고유한 식별자

각 개체에는 충돌하는 ID를 방지하고 중복 검색을 사용하기 위해 개별 사이트에서 사용하는 ID와 독립적인 전역 고유 ID가 할당됩니다. 이러한 ID는 모든 데이터 마트 간에 공유됩니다. 이 ID는 Inventory Data Mart 테이블의 Comment 열에 있는 GUID(Globally Unique ID)입니다.

- 중복이 없습니다

여러 OnCommand Insight 데이터베이스에 있는 엔터티는 통합 데이터베이스에 한 번만 등록됩니다.

- 현재 레코드

통합된 데이터베이스(Inventory Data Mart)의 데이터는 항상 가장 최신 상태로 유지됩니다.

연결을 추가하거나 편집할 때 연결을 테스트할 수도 있습니다. 테스트는 다음을 수행합니다.

- 호스트 IP 주소, 사용자 이름 및 암호를 확인하고 연결을 설정할 수 있는지 확인합니다.

잘못된 연결이 빨간색으로 표시됩니다.

- OnCommand Insight 버전을 데이터 웨어하우스 버전과 비교합니다.

버전이 호환되지 않으면 오류 메시지가 나타납니다.

- OnCommand Insight 데이터베이스가 마지막 데이터 웨어하우스 처리에 표시된 다른 데이터베이스로 변경 또는 복원되지 않았는지 확인합니다. 변경 사항이 있으면 오류 메시지가 나타납니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 커넥터 * 를 클릭합니다.

커넥터 테이블은 처음에 공백으로 나타나고 커넥터를 추가한 후 커넥터 정보를 표시합니다.

3. 새 커넥터를 추가하려면 * 새로 만들기 * 를 클릭합니다.
4. 다음을 입력합니다.

- * 암호화 *

SSL 암호화를 사용하여 데이터 웨어하우스 요청을 하려면 `Enabled` 를 선택합니다.

- * 이름 *

커넥터 뷰에서 커넥터를 식별하는 커넥터 이름입니다.

- * 호스트 *

호스트 IP 주소입니다

- * 사용자 이름 *

"재고"



이 사용자 이름 및 암호를 사용하여 원격 OnCommand Insight 데이터베이스에 로그인하고 데이터에 대한 쿼리를 수행할 수 있습니다.

- * 암호 *

"SANscreen"

5. 호스트에 대한 TCP 연결에 사용할 포트를 지정하려면 * 고급 * 을 클릭하고 TCP 포트 번호를 입력합니다.
6. 호스트에 대한 HTTPS 연결에 사용할 포트(기본 포트 제외)를 지정하려면 * 고급 * 을 클릭하고 포트 번호를 입력합니다.
7. Test * 를 클릭합니다.

데이터 웨어하우스가 연결을 테스트합니다.

8. 저장 * 을 클릭합니다.

여러 설치에 대해 여러 연결을 입력하면 데이터 웨어하우스는 데이터를 추출할 각 데이터베이스마다 하나씩 독립 빌드 프로세스를 호출합니다. 이러한 각 빌드 프로세스는 OnCommand Insight 데이터베이스에서 데이터를 추출하여 통합된 데이터베이스에 로드합니다.

데이터 웨어하우스 데이터베이스는 기록 개요에서 빌드됩니다

OnCommand Insight 서버의 기록 데이터를 사용하여 데이터 웨어하우스 데이터베이스를 구축할 수 있습니다. 데이터 웨어하우스는 OnCommand Insight 서버에서 데이터를 추출하고 기록 일정에 따라 데이터 웨어하우스 데이터 마트를 작성합니다.

이 옵션에는 특수 라이선스가 필요하지 않으며, 재고 데이터가 빌드에 포함됩니다. 그러나 용량 정보를 작성하려면 OnCommand Insight Plan 및 OnCommand Insight Perform 라이선스가 필요합니다.

기록 또는 현재 빌드가 이미 수행된 경우 마지막 작업 이전 날짜에 빌드를 수행할 수 없습니다. 즉, 현재 빌드를 수행하는 경우 기록에서 빌드할 수 없습니다. 보다 구체적으로, 2012년 1월 1일에 종료된 기록에서 빌드를 수행한 경우 2011년부터는 빌드를 수행할 수 없습니다.

기록 빌드에 실패한 ETL 프로세스가 하루 또는 2개 포함되어 있지 않으면 며칠 동안 기록을 작성하려고 하지 마십시오. 기록 데이터는 더 긴 기간이며 하루 또는 이틀 동안 추세를 크게 변경하지 않습니다. 기록에서 재생성하려면 전체 기록을 재생성합니다.

기록에서 작성 보기에는 모든 커넥터의 모든 빌드 작업이 표시됩니다. 예를 들어, 보기에는 모든 커넥터의 인벤토리 작업, 모든 빌드 실행에 대한 포트 용량 작업 및 주석 작업이 표시될 수 있습니다.

기록에서 빌드를 구성하기 전에 다음 작업이 수행되어야 합니다.

- 커넥터를 구성해야 합니다.
- 주석은 OnCommand Insight에 입력해야 하며 이전 OnCommand Insight 포털에서 * DWH용 주석 강제 업데이트 옵션 * 을 사용하여 수동으로 업데이트할 수 있습니다. 그렇지 않으면 15분 후에 자동으로 업데이트됩니다.

기록에서 데이터 웨어하우스 데이터베이스를 구축하는 작업 추가

OnCommand Insight 서버에 보관된 기록 데이터를 사용하여 데이터 웨어하우스 데이터베이스를 구축할 수 있으며, 이 데이터를 사용하여 예상 보고서를 실행할 수 있습니다.

시작하기 전에

OnCommand Insight 서버에 업데이트된 주석이 있어야 하고 데이터 웨어하우스에 대한 주석 정보를 강제로 업데이트해야 합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 기록에서 작성 * 을 클릭합니다.

Build From History

Target time	Start running	Status
3/13/15 12:00 AM	3/25/15 9:28 AM	COMPLETED
3/14/15 12:00 AM	3/25/15 9:34 AM	COMPLETED
3/15/15 12:00 AM	3/25/15 9:39 AM	COMPLETED
3/16/15 12:00 AM	3/25/15 9:45 AM	COMPLETED
3/17/15 12:00 AM	3/25/15 9:51 AM	COMPLETED
3/18/15 12:00 AM	3/25/15 9:57 AM	COMPLETED
3/19/15 12:00 AM	3/25/15 10:03 AM	COMPLETED
3/20/15 12:00 AM	3/25/15 10:09 AM	COMPLETED
3/21/15 12:00 AM	3/25/15 10:16 AM	COMPLETED
3/22/15 12:00 AM	3/25/15 10:23 AM	COMPLETED
3/23/15 12:00 AM	3/25/15 10:30 AM	COMPLETED
3/24/15 12:00 AM	3/25/15 10:38 AM	COMPLETED
3/25/15 12:00 AM	3/25/15 10:44 AM	COMPLETED

Cancel Pending Jobs

Configure

Run

Skip history build failures: ☒

3. 구성 * 을 클릭합니다.

Configure Build From History

Start time:	11	February
	2015	...
End time:	02	April
	2015	...
Interval:	<input checked="" type="radio"/> Daily <input type="radio"/> Weekly <input type="radio"/> Monthly <input type="radio"/> Quarterly	
Hour:	12:00 AM	
<input type="button" value="Save"/> <input type="button" value="Reset"/> <input type="button" value="Cancel"/>		

4. 시작 및 종료 시간을 입력합니다.

이러한 날짜를 선택할 수 있는 달력을 표시하려면 월 이름 옆의 아래쪽 화살표를 클릭합니다.

시간 형식은 데이터 웨어하우스 서버의 로캘에 따라 달라집니다.

시작 및 종료 시간은 데이터 웨어하우스 포털 커넥터 옵션에 설정된 대로 데이터 웨어하우스가 연결된 모든 OnCommand Insight 서버에 포함된 기록 범위 내에 있어야 합니다. 기본 시작 및 종료 시간은 최대 유효 기간을 반영합니다. 데이터 웨어하우스 빌드 작업은 사용자가 지정한 시간에 자동으로 실행됩니다.



4년간 매일 하는 등 비현실적인 스케줄을 구성하면 1460회의 제작 주기가 완료되기까지 10일이 걸릴 수 있습니다.

5. 간격을 선택합니다.

월 단위 또는 주 단위 간격을 선택하면 일 필드가 나타납니다. 매월 을 선택한 경우, 일 은 날짜입니다. 주단위 를 선택한 경우 요일은 일요일부터 토요일입니다.

6. 빌드가 진행되는 시간을 선택합니다.

7. 선택적으로 옵션을 기본 설정으로 되돌리려면 * Reset * (재설정 *)을 클릭합니다.

8. 저장 * 을 클릭합니다.

9. 기록에서 작성 * 페이지에서 자동 일정 빌드 이외의 빌드를 수행하려면 * 실행 * 을 클릭합니다.

목표 시간 옆에는 이 항목이 작성된 시간이 표시됩니다. 상태 옆에는 빌드가 완료되었는지 또는 실패했는지 여부가 표시됩니다.

기록 작업에서 빌드를 취소합니다

모든 계획된 작업을 취소할 수 있습니다. 작업 상태는 ""중단됨""이 됩니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 기록에서 작성 * 을 클릭합니다.
3. 취소 * 를 클릭합니다.

데이터 웨어하우스 데이터베이스 백업

Cognos 백업도 포함된 데이터 웨어하우스 데이터베이스를 파일에 백업하고 나중에 데이터 웨어하우스 포털을 사용하여 복원할 수 있습니다. 이러한 백업을 사용하면 다른 데이터 웨어하우스 서버로 마이그레이션하거나 새 데이터 웨어하우스 버전으로 업그레이드할 수 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://fqdn/dwh>.
2. 왼쪽의 탐색 창에서 * 백업/복원 * 을 선택합니다.
3. 백업 * 을 클릭하고 백업 구성을 선택합니다.

- a. 성능 데이터 마트를 제외한 모든 데이터 마트
- b. 모든 데이터 마트

이 작업은 30분 이상 소요될 수 있습니다.

+ 데이터 웨어하우스는 백업 파일을 만들고 그 이름을 표시합니다.

4. 백업 파일을 마우스 오른쪽 단추로 클릭하고 원하는 위치에 저장합니다.

파일 이름을 변경하지 않으려는 경우에는 데이터 웨어하우스 설치 경로 외부에 파일을 저장해야 합니다.

데이터 웨어하우스 백업 파일에는 DWH 인스턴스의 MySQL, 사용자 정의 스키마(MySQL DB) 및 테이블, LDAP 구성, Cognos를 MySQL 데이터베이스에 연결하는 데이터 소스(Insight 서버를 데이터를 얻기 위해 장치에 연결하는 데이터 소스 아님)가 포함됩니다. 보고서를 가져오거나 내보낸 작업, 보안 역할, 그룹 및 네임스페이스 보고, 사용자 계정 수정된 보고 포털 보고서 및 내 폴더 디렉토리에서도 저장된 위치에 관계없이 모든 사용자 정의 보고서 SMTP 서버 설정 및 Cognos 사용자 지정 메모리 설정과 같은 Cognos 시스템 구성 매개 변수는 백업되지 않습니다.

사용자 지정 테이블이 백업되는 기본 스키마는 다음과 같습니다.

dWh _ 용량
dWh_capacity_staging
dWh _ 치수
dWh_fs_util
dWh_재고
dWh_inventory_staging
dWh_inventory_transient
dWh _ 관리
더 뛰어난 성능
dWh_performance_staging
dWh_ports
dWh 보고서
dWh_sa_staging

사용자 지정 테이블이 백업에서 제외되는 스키마는 다음과 같습니다.

information_schema를 참조하십시오
획득

CLOUD_MODEL
host_data를 선택합니다
InnoDB
인벤토리
Inventory_private을 선택합니다
Inventory_Time(재고 시간)
로그
관리
MySQL
NAS
성능
performance_schema를 나타냅니다
Performance_views(성능 보기)
SANscreen
스크립
서비스 보장
테스트
tmp(tmp)
워크벤치

수동으로 시작된 모든 백업에서 는 입니다 .zip 다음 파일이 포함된 파일이 생성됩니다.

- 일일 백업입니다 .zip Cognos 보고서 정의가 포함된 파일
- 가 백업을 보고합니다 .zip 내 폴더 디렉토리의 보고서를 포함하여 Cognos의 모든 보고서가 들어 있는 파일입니다

- 데이터 웨어하우스 데이터베이스 백업 파일 Cognos는 언제든지 수행할 수 있는 수동 백업 외에도 매일 실행되는 백업(라는 파일에 매일 자동으로 생성됨)을 생성합니다 DailyBackup.zip)에 보고서 정의가 포함되어 있습니다. 일일 백업에는 제품과 함께 제공되는 최상위 폴더와 패키지가 포함됩니다. 내 폴더 디렉토리 및 제품의 최상위 폴더 외부에서 생성한 디렉토리는 Cognos 백업에 포함되지 않습니다.



Insight에서 파일 이름을 로 지정하는 방식 때문입니다 .zip 파일, 일부 압축 해제 프로그램은 파일을 열 때 파일이 비어 있음을 표시합니다. 를 누릅니다 .zip 파일의 크기가 0보다 크고 로 끝나지는 않습니다 .bad 내선 번호 .zip 파일이 유효합니다. 7-Zip 또는 WinZip® 과 같은 다른 압축 해제 프로그램으로 파일을 열 수 있습니다.

사용자 정의 보고서 및 보고서 아티팩트 백업

7.0 이전의 Insight 버전에서 사용자 지정 보고서를 만든 경우 최신 Insight 버전으로 업그레이드하려면 업그레이드 설치 전에 보고서와 보고서 아티팩트를 백업하고 업그레이드 설치 후에 복원해야 합니다. 또한 보고서 아티팩트를 저장하는 데 사용하는 폴더에도 주의를 기울여야 합니다.

이 작업에 대해

미리 디자인된 보고서를 변경한 경우 해당 보고서의 복사본을 별도의 폴더에 만듭니다. 이렇게 하면 미리 디자인된 아티팩트를 업데이트할 때 변경 내용을 덮어쓰지 않습니다.

내 폴더 영역에 보고서가 있는 경우 보고서가 손실되지 않도록 사용자 지정 보고서 폴더에 복사해야 합니다.

데이터 웨어하우스 데이터베이스 복원

을 사용하여 데이터 웨어하우스 데이터베이스를 복원할 수 있습니다 .zip 데이터 웨어하우스 데이터베이스를 백업할 때 생성된 파일입니다.

이 작업에 대해

데이터 웨어하우스 데이터베이스를 복원할 때 백업에서 사용자 계정 정보를 복원할 수도 있습니다. 사용자 관리 테이블은 데이터 웨어하우스 보고서 엔진이 데이터 웨어하우스 전용 설치에서 사용됩니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 백업/복원 * 을 클릭합니다.
3. 데이터베이스 및 보고서 복원 * 섹션에서 * 찾아보기 * 를 클릭하고 을 찾습니다 .zip 데이터 웨어하우스 백업을 포함하는 파일입니다.
4. 보고서 또는 사용자 계정 데이터를 복원하려면 다음 확인란 중 하나 또는 둘 다를 선택합니다.

- * 데이터베이스 복원 *

데이터 웨어하우스 설정, 데이터 마트, 연결 및 사용자 계정 정보가 포함됩니다.

- * 보고서 복원 *

사용자 지정 보고서, 미리 디자인된 보고서, 미리 디자인된 보고서의 변경 내용, 보고 포털에서 만든 보고 설정 등이 포함됩니다.



데이터베이스 백업에 이름에 슬래시(/) 또는 여는 대괄호([)가 있는 사용자 지정 보고서(예: US IT Center Switch Port Boston/July)가 포함되어 있는 경우 복원 작업에서는 보고서의 이름을 바꾸고 슬래시 또는 여는 대괄호를 밑줄로 바꿉니다(예: 미국 IT 센터 스위치 포트 Boston_July).

5. 복원 * 을 클릭합니다.

복원 프로세스가 완료되면 복원 단추 아래에 메시지가 표시됩니다. 복원 프로세스가 성공적으로 완료되면 성공 메시지가 표시됩니다. 복원 프로세스가 실패하면 이 메시지는 오류를 발생시킨 특정 예외를 보고합니다. 예외가 발생하고 복원 프로세스가 실패하면 원래 데이터베이스가 자동으로 재설정됩니다.

보고에서 다중 임차 설정

OnCommand Insight 데이터 웨어하우스는 사용자를 하나 이상의 비즈니스 엔티티에 연결할 수 있도록 하여 보고에서 다중 임차(종종 "몰티 테넌시" 또는 "몰티테넌시"로 단축)를 수용합니다. 이 기능을 사용하면 관리자는 사용자 속성 또는 사용자 가입에 따라 데이터나 보고서를 분리할 수 있습니다.

업무 엔티티는 다음 값을 사용하여 용량 차지백 목적으로 계층을 사용합니다.

- 테넌트: 기본적으로 서비스 공급자가 리소스를 고객과 연결하는 데 사용합니다. 예를 들어 NetApp이 있습니다.
- 사업 부문(LOB): 회사 내 사업 부문(예: "하드웨어" 또는 "소프트웨어").
- 사업부: "영업" 또는 "마케팅"과 같은 기존 사업부입니다.
- Project(프로젝트): 용량 비용 청구를 할당할 수 있는 프로젝트입니다.

다중 임차를 구성하는 프로세스에는 다음과 같은 주요 단계가 포함됩니다.

- 데이터 웨어하우스 사용자 계정을 구성합니다.
- 보고 포털에서 그룹을 만듭니다.
- 비즈니스 엔티티를 나타내는 하나 이상의 그룹에 사용자를 할당합니다.
- 사용자를 하나 이상의 업무 엔티티에 할당합니다. 예를 들어, "NetApp"과 관련된 사용자는 테넌트로 ""NetApp""을 보유한 모든 비즈니스 엔티티에 액세스할 수 있습니다.
- 사용자가 볼 수 있는 보고서만 볼 수 있는지 테스트합니다.

다음은 사용자가 보고 데이터에 액세스하는 방법을 요약한 내용입니다.

- 그룹에 할당되지 않은 사용자는 모든 데이터에 액세스할 수 있습니다.
- 그룹에 할당된 사용자는 업무 엔티티가 없는 레코드에 액세스할 수 없습니다.

예를 들어 다음 부서가 있을 수 있으며 이러한 부서 내의 사용자에 대한 보고서를 분리해야 할 수 있습니다.

사용자	엔지니어링	지원	재무	법적 고지
-----	-------	----	----	-------

사용자1	X	X		
사용자2			X	X
사용자3		X		

사용자 계정을 구성하는 중입니다

사용자 계정을 구성하려면 몇 가지 단계를 완료해야 합니다.


단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 사용자 관리 * 를 클릭합니다.
3. 각 사용자 계정을 구성합니다.

비즈니스 엔티티에 사용자 할당

사용자를 업무 엔티티에 할당하려면 일련의 단계를 완료해야 합니다. 데이터 웨어하우스는 사용자를 하나 이상의 비즈니스 엔티티에 연결할 수 있도록 하여 보고서에서 다중 임차(종종 "멀티 테넌시" 또는 "멀티테넌시"로 단축)를 수용합니다. 이를 통해 관리자는 사용자 속성 또는 사용자 가입에 따라 데이터 또는 보고서를 분리할 수 있습니다.

단계

1. 에서 Data Warehouse Portal에 관리자로 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 데이터 웨어하우스 도구 모음에서  보고 포털을 엽니다.
3. 사용자 이름과 암호를 입력하고 * 로그인 * 을 클릭합니다.
4. 시작 메뉴에서 * IBM Cognos Administration * 을 선택합니다.
5. 보안 * 탭을 클릭합니다.
6. 디렉터리에서 * Cognos * 를 선택합니다.
7. "BES"라는 Cognos 폴더에 비즈니스 엔티티에 대한 새 하위 폴더를 만듭니다.
8. BES 폴더를 엽니다.
9. 다른 권한 수준에 해당하는 그룹을 추가하려면 * 새 그룹 * 아이콘을 클릭합니다.

이러한 사용 권한 수준은 업무 엔티티의 전체 이름(예: NetApp.N/A) 또는 접두사(예: NetApp.N/A Finance)일 수 있습니다. 이 두 형식 중 하나를 사용하면 사업체 내의 모든 프로젝트에 액세스할 수 있습니다(NetApp.N/A. Finance).

새 그룹 마법사가 표시됩니다.

10. 마법사의 페이지를 완료합니다.

11. 업무 엔티티를 선택하고 * 자세히 * 를 클릭합니다.
12. 구성원 설정 * 을 클릭합니다.
13. 추가 * 를 클릭합니다.
14. SANscreen 디렉터리를 선택합니다.
15. 사용자 목록에서 업무 엔티티에 포함할 각 사용자를 선택하고 선택한 항목 상자에 사용자를 추가합니다.
16. 확인 * 을 클릭합니다.
17. 각 업무 엔티티 그룹에 구성원을 추가하는 과정을 반복합니다.

설치 문제 해결

주석, 빌드 및 보고서를 설치하는 동안 발생할 수 있는 몇 가지 일반적인 문제가 있습니다. 설명된 단계에 따라 이러한 문제를 해결할 수 있습니다.

주석을 볼 수 없는 이유

데이터 웨어하우스에서 주석을 볼 수 없는 경우 주석을 강제로 업데이트한 다음 데이터 웨어하우스 빌드를 시작해야 할 수 있습니다.

누락된 주석은 데이터를 데이터 웨어하우스로 가져오는 방식에 영향을 주며 보고서에 표시됩니다. 예를 들어 ""계층" 주석을 사용할 수 없는 경우 데이터 웨어하우스 보고서에서 스토리지 시스템을 계층별로 그룹화할 수 없습니다.

데이터 웨어하우스에 대한 주석 업데이트 강제 적용

OnCommand Insight에서 데이터 웨어하우스로 주석 업데이트를 시작할 수 있습니다.

이 작업에 대해

다음 두 옵션 중 하나를 사용하여 주석을 업데이트할 수 있습니다.

- 삭제된 객체 포함: 제거된 호스트, 스토리지 시스템 또는 스위치와 같이 더 이상 존재하지 않는 디바이스에 대한 데이터가 포함됩니다. 이 기능은 기록 데이터 요소를 사용하여 데이터 웨어하우스 데이터를 작성하려는 경우에 필요합니다.
- 삭제된 개체 제외: 삭제된 개체를 제외하려면 이 옵션을 선택합니다.

단계

1. OnCommand Insight 포털에 관리자로 로그인합니다 `https://hostname`, 위치 `hostname` OnCommand Insight가 설치된 시스템의 이름입니다.
2. Admin * > * Troubleshooting * 을 클릭합니다. 페이지 하단에서 * 고급 문제 해결 * 을 클릭합니다.
3. Actions * 탭에서 * Update DWH Annotations (include deleted) * 를 클릭합니다.

수동 데이터 웨어하우스 빌드 생성

OnCommand Insight에서 주석 업데이트(임시 데이터 실행)를 강제 적용한 후 데이터 웨어하우스 빌드를 시작해야 합니다. 다음 예약된 빌드가 나올 때까지 기다리거나 지금 빌드를

시작할 수 있습니다.

단계

1. Data Warehouse Portal()에 관리자로 로그인합니다 `https://hostname/dwh`, 위치 `hostname` OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * Schedule * 을 클릭합니다.
3. 지금 구축 * 을 클릭합니다.

사용자 정의 주석을 데이터 웨어하우스로 불러오기

OnCommand Insight에서 주석 업데이트를 적용한 후 데이터 웨어하우스에서 원하는 주석을 선택하고 데이터 웨어하우스 빌드를 시작해야 합니다. 다음 예약된 빌드가 나올 때까지 기다리거나 지금 빌드를 시작할 수 있습니다.

단계

1. Data Warehouse Portal()에 관리자로 로그인합니다 `https://hostname/dwh`, 위치 `hostname` OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * Annotations * 를 클릭합니다.

Annotations

Annotation	Column Name	Target Object	Published
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	
Data_Center	dataCenter	Host	✓
Data_Center	dataCenter	Storage	✓
Data_Center	dataCenter	Switch	✓
Note	Note	Switch	
Switch_Level	switchLevel	Switch	✓
Tier	Tier	Internal Volume	
Tier	Tier	Qtree	
Tier	Tier	Storage	
Tier	Tier	Storage Pool	
Tier	Tier	Volume	

Edit

이 목록에는 모든 주석 유형에 대한 행과 주석을 지정할 수 있는 대상 객체가 표시됩니다. Published(게시됨) 열의 체크 표시는 특정 대상 개체에 대해 주석이 이미 선택되었으며 Data Warehouse(데이터 웨어하우스) 데이터 마트를 통해 이미 사용 가능함을 나타냅니다.

3. OnCommand Insight에서 주석을 가져오는 방법을 편집하려면 * 편집 * 을 클릭합니다.

Annotation	Column Name	Target Object	Published All / None	Init With Current All / None
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	<input type="checkbox"/>	<input type="checkbox"/>
Data_Center	dataCenter	Host	<input type="checkbox"/>	<input type="checkbox"/>
Data_Center	dataCenter	Storage	<input type="checkbox"/>	<input type="checkbox"/>
Data_Center	dataCenter	Switch	<input type="checkbox"/>	<input type="checkbox"/>
Note	Note	Switch	<input type="checkbox"/>	<input type="checkbox"/>
Switch_Level	switchLevel	Switch	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Internal Volume	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Qtree	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Storage	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Storage Pool	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Volume	<input type="checkbox"/>	<input type="checkbox"/>

Save Cancel

4. 주식 프로세스를 편집하려면 다음을 수행합니다.

- OnCommand Insight에서 가져온 주석을 데이터 웨어하우스 데이터베이스에 추가하려면 * Published * 를 선택합니다. 모든 개체의 모든 주석을 선택하려면 * All * (모두 *)을 클릭합니다. 모든 옵션을 선택하지 않으려면 * 없음 * 을 클릭합니다.



특정 객체의 재고 테이블 및 관련 데이터 마트에서 주식 열을 제거하려면 이 옵션을 선택 취소합니다. 사용자 정의 보고서가 주식 데이터를 사용하는 경우 보고서가 성공적으로 실행되지 않습니다.

- 데이터 웨어하우스 차원 테이블의 기록 데이터를 현재 주식 값으로 초기화하려면 * Init with Current * 를 선택합니다. 모든 개체의 모든 주석을 선택하려면 * All * (모두 *)을 클릭합니다. 모든 옵션을 선택하지 않으려면 * 없음 * 을 클릭합니다. 주석을 게시한 후에는 이 확인란을 사용할 수 없으며 게시되지 않은 주석에는 확인란을 사용할 수 있습니다. 예를 들어, 호스트에 주식 유형 ""바닥""이 주식으로 추가되고 호스트 차원 테이블에 해당 호스트에 대한 행 3개가 있는 경우 * 현재 * 와 함께 초기화 를 선택하면 호스트 차원 테이블의 "바닥" 열에 있는 값 ""1""이 연결됩니다. 현재 * 포함 초기화 * 를 선택하지 않으면 해당 호스트의 최신 행만 바닥 열에 ""1"" 값을 갖게 됩니다.

5. 저장 * 을 클릭합니다.

주석을 제거할 경우 데이터 구조 또는 데이터 손실이 변경된다는 경고 메시지가 나타납니다.

6. 계속하려면 * 예 * 를 클릭합니다.

데이터 웨어하우스는 요청된 변경 사항을 적용하는 비동기 주식 작업을 시작합니다. 작업 페이지에서 작업을 볼 수 있습니다. 데이터 웨어하우스 데이터베이스 스키마의 변경 사항도 볼 수 있습니다.

실패한 기간별 빌드 포인트에 대한 조치

히스토리 빌드 실패 건너뛰기 * 옵션을 사용하면 실패한 빌드를 생략하고 기록에서 빌드할 수 있습니다.

이렇게 하면 기록에서 빌드가 계속됩니다. 빌드에 실패하고 이 옵션이 활성화된 경우 데이터 웨어하우스는 빌드를 계속

수행하고 실패한 빌드는 무시합니다. 이러한 경우 건너뛴 빌드에 대한 기간별 데이터에 데이터 포인트가 없습니다. 이 옵션을 활성화하지 않고 빌드에 실패하면 이후의 모든 작업이 중단됩니다.

데이터 웨어하우스를 사용하여 수행할 수 있는 관리 작업입니다

OnCommand Insight 데이터 웨어하우스는 사용자가 OnCommand Insight 데이터 웨어하우스에서 데이터를 구성 및 문제 해결하고 OnCommand Insight에서 데이터를 검색할 일정을 설정할 수 있는 웹 기반 사용자 인터페이스입니다.

데이터 웨어하우스 포털을 사용하여 다음과 같은 관리 작업을 수행할 수 있습니다.

- 실행 중인 현재 작업 또는 쿼리의 상태를 확인합니다
- 주석 관리
- 이메일 알림을 구성합니다
- 사용자 정의 보고서 액세스 및 작성
- 데이터 웨어하우스 문서 및 데이터베이스 스키마를 검토합니다
- 사이트 이름을 편집합니다
- 데이터 웨어하우스 버전 및 업그레이드 기록 파악
- 기록에서 데이터 웨어하우스 데이터를 작성합니다
- 데이터 웨어하우스 데이터베이스를 재설정합니다
- 데이터 웨어하우스 데이터베이스를 백업 및 복원합니다
- 데이터 웨어하우스 문제를 해결하고 OnCommand Insight 로그를 확인합니다
- 사용자 계정을 관리합니다

작업 관리

현재 작업 목록과 해당 상태를 볼 수 있습니다. 빌드 주기의 첫 번째 작업은 굵은 글꼴로 표시됩니다. 데이터 웨어하우스가 각 커넥터 및 각 데이터 마트에 대해 수행하는 빌드는 작업으로 간주됩니다.

이 작업에 대해

예약했거나 시작한 보류 중인 작업을 취소할 수 있습니다. 이전에 실행된 작업의 기록을 지울 수도 있습니다. 보류 중, 실행 중이 아니거나 중단 중인 작업의 기록을 지울 수 있습니다. 지난 24시간을 제외한 모든 기록 또는 모든 기록을 지우면 마지막 날의 항목을 제외한 모든 기록을 제거할 수 있습니다.

라이선스, 재고 전, 재고, 재고 후, 재고, 치수, 데이터 마트 준비, 용량, 포트, 스토리지 효율성, 파일 시스템 활용률, 성능, 작업 상태 알림, 기록 빌드, 동적 주석, 커넥터 제거, 빌드, Phone Home 및 유지 관리를 건너뛰었습니다.

유지 관리 작업은 매주 실행되며 MySQL 도구를 사용하여 데이터베이스를 최적화합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand

Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.

2. 왼쪽의 탐색 창에서 * Jobs * 를 클릭합니다.

#	Name	Status	Start time	End time
1551	Job Status Notification	COMPLETED	4/9/15 2:12 AM	4/9/15 2:12 AM
1550	Performance	COMPLETED	4/9/15 2:11 AM	4/9/15 2:12 AM
1549	File System Utilization	COMPLETED	4/9/15 2:11 AM	4/9/15 2:11 AM
1548	Storage Efficiency	COMPLETED	4/9/15 2:11 AM	4/9/15 2:11 AM
1547	Ports	COMPLETED	4/9/15 2:11 AM	4/9/15 2:11 AM
1546	Capacity	COMPLETED	4/9/15 2:11 AM	4/9/15 2:11 AM
1545	Datamarts Preparation	COMPLETED	4/9/15 2:10 AM	4/9/15 2:11 AM
1544	Dimensions	COMPLETED	4/9/15 2:10 AM	4/9/15 2:10 AM
1543	Post Inventory	COMPLETED	4/9/15 2:10 AM	4/9/15 2:10 AM
1542	Inventory: connector 'oci-stg01-s08', 'Apr 9, 2015 2:00 AM'	COMPLETED	4/9/15 2:06 AM	4/9/15 2:10 AM
1541	Inventory: connector 'oci-stg06-s08', 'Apr 9, 2015 2:00 AM'	COMPLETED	4/9/15 2:04 AM	4/9/15 2:06 AM
1540	Inventory: connector 'oci-stg03-s08', 'Apr 9, 2015 2:00 AM'	COMPLETED	4/9/15 2:04 AM	4/9/15 2:04 AM

보류 중 상태가 나타나면 취소 링크가 나타납니다.

3. 보류 중인 작업을 취소하려면 * CANCEL * (취소 *)을 클릭합니다.

4. 작업 기록을 제거하려면 * 모두 * 또는 * 마지막 24시간을 제외한 모두 * 를 클릭합니다.

데이터 웨어하우스 상태 모니터링

DWH(데이터 웨어하우스)에는 DWH 상태에 대한 정보를 표시하는 상태 모니터가 포함되어 있습니다. 경고 메시지는 DWH의 * 커넥터 * 및 * 작업 * 페이지에 표시되며, 연결된 Insight 서버로 전송되어 * 관리 * > * 상태 * 페이지에 표시됩니다.

DWH는 10분마다 지표를 수집하고 다음과 같은 조건에서 알람을 표시합니다.

- Insight 서버 연결이 끊어졌습니다
- 디스크 사용률이 90%를 넘습니다
- 보고(Cognos) 서비스가 다운되었습니다
- 쿼리는 어떤 테이블에도 오랜 시간 동안 잠금을 유지합니다
- 유지보수 작업이 비활성화되었습니다
- 자동 백업이 비활성화되었습니다
- 보안 위험: 기본 암호화 키가 감지되었습니다

데이터 웨어하우스의 상태 모니터 경고는 최대 30일 동안 억제할 수 있습니다.

이메일 알림이 활성화되면 이러한 이벤트도 이메일로 보고됩니다. 이메일에 첨부 파일이 포함되어 있지 않습니다.

이러한 이벤트는 에 기록됩니다 `dwh_troubleshoot.log` 다음 위치에 있는 파일:

- 창: `<install dir>\SANscreen\Wildfly\Standalone\Logs`
- Linux: `/var/log/netapp/oci/wildfly/`

일별 빌드 예약

언제든지 Build Now 컨트롤을 사용하여 데이터 웨어하우스를 수동으로 작성할 수 있지만, 데이터 웨어하우스 데이터베이스를 구축할 시기와 빈도를 정의하여 자동 빌드를 예약하는 것이 가장 좋습니다. 데이터 웨어하우스는 각 커넥터 및 각 데이터 마트에 대해 빌드 작업을 수행합니다. 데이터 웨어하우스는 라이선스 및 인벤토리에 대해 각 커넥터에 대해 빌드 작업을 수행하고 다른 모든 빌드 작업(예: 용량)은 통합 데이터베이스에서 수행됩니다.

이 작업에 대해

데이터 웨어하우스가 구축될 때마다 모든 커넥터에 대해 인벤토리 작업을 수행합니다. 인벤토리 작업이 완료되면 데이터 웨어하우스는 차원, 용량 및 나머지 데이터 마트에 대한 작업을 수행합니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 일정 편집 * 을 클릭합니다.

Automatic Schedule

Enabled:	<input type="text" value="yes"/>	<input type="button" value="Edit schedule"/>
Schedule:	<input type="text" value="Daily at 2:00 AM,7:00 PM"/>	
Next run:	<input type="text" value="4/2/15 7:00 PM"/>	

3. 일정 작성 * 대화 상자에서 * 편집 * 을 클릭하여 새 일정을 추가합니다.

Type:

Enabled: ☒

Run at:

<input type="checkbox"/> 12:00 AM	<input type="checkbox"/> 1:00 AM	<input checked="" type="checkbox"/> 2:00 AM	<input type="checkbox"/> 3:00 AM	<input type="checkbox"/> 4:00 AM	<input type="checkbox"/> 5:00 AM	<input type="checkbox"/> 6:00 AM	<input type="checkbox"/> 7:00 AM	<input type="checkbox"/> 8:00 AM	<input type="checkbox"/> 9:00 AM	<input type="checkbox"/> 10:00 AM	<input type="checkbox"/> 11:00 AM
<input type="checkbox"/> 12:00 PM	<input type="checkbox"/> 1:00 PM	<input type="checkbox"/> 2:00 PM	<input type="checkbox"/> 3:00 PM	<input type="checkbox"/> 4:00 PM	<input type="checkbox"/> 5:00 PM	<input type="checkbox"/> 6:00 PM	<input checked="" type="checkbox"/> 7:00 PM	<input type="checkbox"/> 8:00 PM	<input type="checkbox"/> 9:00 PM	<input type="checkbox"/> 10:00 PM	<input type="checkbox"/> 11:00 PM

- 빈도 - 매주 를 선택합니다.
- 작업을 실행할 각 날짜의 시간을 선택합니다.
- 빌드를 실행하지 않으려는 날짜에 대해 N/A를 선택합니다.
- 일정을 활성화하려면 * Enabled * 를 선택합니다.



이 옵션을 선택하지 않으면 일정 빌드가 발생하지 않습니다.

- 저장 * 을 클릭합니다.
- 자동 예약 빌드 외부에서 데이터 웨어하우스를 빌드하려면 * 지금 빌드 * 를 클릭합니다.

주별 스케줄 구성

언제든지 Build Now 컨트롤을 사용하여 데이터 웨어하우스를 수동으로 작성할 수 있지만, 데이터 웨어하우스 데이터베이스를 구축할 시기와 빈도를 정의하여 자동 빌드를 예약하는 것이 가장 좋습니다. 데이터 웨어하우스는 각 커넥터 및 각 데이터 마트에 대해 빌드 작업을 수행합니다. 데이터 웨어하우스는 라이선스 및 인벤토리에 대해 각 커넥터에 대해 빌드 작업을 수행하고 다른 모든 빌드 작업(예: 용량)은 통합 데이터베이스에서 수행됩니다. 주별 일정을 사용하면 해당 요일에 대한 빌드를 실행할 시간을 지정할 수 있습니다.

단계

- 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
- 왼쪽의 탐색 창에서 * 일정 편집 * 을 클릭합니다.
- 빈도 - 매주 를 선택합니다.
- 작업을 실행할 각 날짜의 시간을 선택합니다.
- 빌드를 실행하지 않으려는 날짜에 대해 N/A를 선택합니다.
- 일정을 활성화하려면 * Enabled * 를 선택합니다.



이 옵션을 선택하지 않으면 일정 빌드가 발생하지 않습니다.

7. 저장 * 을 클릭합니다.

8. 자동 예약 빌드 외부에서 데이터 웨어하우스를 빌드하려면 * 지금 빌드 * 를 클릭합니다.

일일 백업 예약

언제든지 백업/복원 컨트롤을 사용하여 데이터 웨어하우스를 수동으로 백업할 수 있지만 데이터 웨어하우스 데이터베이스 및 Cognos 콘텐츠 저장소를 백업할 시기와 빈도를 정의하여 자동 백업을 예약하는 것이 좋습니다. 백업은 데이터 손실로부터 보호하므로 필요한 경우 데이터 웨어하우스 데이터베이스를 복원할 수 있습니다. 또한 새 데이터 웨어하우스 서버로 마이그레이션하거나 새 데이터 웨어하우스 버전으로 업그레이드할 때 백업을 사용합니다.

이 작업에 대해

데이터 웨어하우스 서버가 사용 중이 아닌 시간에 백업을 예약하면 백업 성능이 향상되고 사용자에게 미치는 영향이 줄어듭니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * Schedule * 을 클릭합니다.
3. 백업 일정 * 대화 상자에서 * 편집 * 을 클릭하여 새 일정을 추가합니다.

Backup Enabled: ☐

Backup Location:

Select Backup Configuration:

Run every:

<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday

Run at hour:

Cleanup:

4. 예약된 백업을 활성화하려면 * Backup Enabled * 를 선택합니다.
5. 백업 파일을 저장할 위치를 지정합니다.
6. 백업할 데이터를 지정합니다.
7. 백업을 수행할 요일을 지정합니다.
8. 백업을 시작할 시간을 지정합니다.
9. 유지할 과거 백업 복사본 수를 지정합니다.

10. 저장 * 을 클릭합니다.

데이터 웨어하우스에서 사용자 정의 스크립트 실행

데이터 웨어하우스를 통해 고객은 데이터 웨어하우스에서 맞춤형 데이터를 준비하는 사용자 정의 스크립트를 실행할 수 있는 작업을 생성할 수 있습니다.

시작하기 전에

데이터 웨어하우스 업그레이드 중에 사용자 정의 스크립트가 삭제되지 않도록 하려면 SANscreen 디렉토리에 스크립트를 저장하지 않아야 합니다.

이 작업에 대해

작업은 하나의 스크립트만 지정할 수 있습니다. 하나의 스크립트에서 여러 스크립트와 명령을 실행할 수 있습니다.

단계

1. 데이터 웨어하우스에서 * DWH Admin * > * Schedule * 을 선택합니다.
2. 스크립트 사용 * 확인란을 선택합니다.
3. 스크립트 이름의 절대 경로를 * 스크립트 위치 * 텍스트 상자에 입력합니다.
4. 저장 * 을 클릭합니다.

결과

데이터 웨어하우스 작업 엔진은 ""사용자 정의 스크립트"" 작업을 실행하도록 작업을 예약합니다. ETL을 실행한 후 다른 충돌하는 백그라운드 프로세스를 방지하도록 작업이 예약됩니다. 이 작업은 "역사적 Build from history" 연산으로 실행되지 않습니다.

주석을 사용하여 수행할 수 있는 작업

주석은 사용자 환경의 개체와 관련된 정보를 정의한 다음 주석을 기반으로 개체를 추적할 수 있는 방법을 제공합니다. 예를 들어 사용자 환경의 디바이스에 건물 또는 층 번호 주석을 추가한 다음 데이터 센터의 1층에 있는 모든 디바이스를 반환하는 쿼리를 만들 수 있습니다.

또한 특정 데이터 센터 또는 사업체 에 있는 모든 장치를 살펴보고 최상위 계층 1 스토리지를 사용 중인 업무 엔티티를 결정할 수 있습니다. 이렇게 하려면 OnCommand Insight 웹 UI를 사용하여 데이터 센터, 사업체 또는 계층 주석을 장치에 할당합니다. 그런 다음 OnCommand Insight에서 선택한 사용자 정의 주석을 데이터 웨어하우스로 가져올 수 있습니다. 개체에 할당된 주석 값이 사용자 정의 보고서에 표시되도록 하려면 이 작업을 수행합니다.

데이터 웨어하우스에 적용할 사용자 정의 주석을 지정할 수 있습니다. 주석은 인벤토리의 객체 테이블과 데이터 마트의 관련 차원 테이블에 추가 열로 추가됩니다. OnCommand Insight 사용자 인터페이스를 사용하여 리소스의 주석을 업데이트하고 다음 데이터 웨어하우스 빌드를 시작하거나 기다릴 때 다음 표에 결과가 표시됩니다.

- dWh_inventory.annotation_value 를 입력합니다
- dWh_inventory.object_to_annotation

OnCommand Insight에 입력된 주석이 데이터 웨어하우스에 포함되는지 확인하려면 다음과 같은 주요 프로세스가 필요합니다.

- 주석을 데이터 웨어하우스로 가져오기 전에 OnCommand Insight에서 준비되었는지 확인해야 합니다.

이렇게 하려면 * Troubleshooting * > * Force Update of Annotations for Data Warehouse * 옵션을 수동으로 실행하거나 예약된 다음 임시 데이터 실행 프로세스가 실행될 때까지 기다립니다. 주석을 강제로 업데이트할 때 OnCommand Insight 서버가 임시 데이터(예: 주석 값)를 계산하고 데이터베이스 테이블에 배치하도록 하여 데이터 웨어하우스 ETL 프로세스에서 데이터를 읽을 수 있도록 합니다. 주석 데이터는 15분마다 자동으로 업데이트되지만, 더 자주 강제로 업데이트할 수 있습니다.

- 그런 다음 데이터 웨어하우스 주석 옵션을 사용하여 주석을 데이터 웨어하우스로 가져옵니다.
- OnCommand Insight 보고 포털 보고서 작성 도구를 사용하여 작성한 보고서에 주석을 포함하려면 OnCommand Insight 보고 메타데이터 모델을 업데이트해야 합니다.

데이터 웨어하우스를 업그레이드하면 데이터베이스 복원 프로세스 중에 주석 작업이 자동으로 실행됩니다. WildFly가 시작되면 주석 작업도 자동으로 실행됩니다.



WildFly는 OnCommand Insight Java 코드가 실행되고 OnCommand Insight 서버 및 데이터 웨어하우스 모두에 필요한 응용 프로그램 서버입니다.

OnCommand Insight에서 주석 준비 중

주석을 OnCommand Insight에서 준비해야 데이터 웨어하우스로 가져올 수 있습니다.

단계

1. OnCommand Insight 포털에 관리자로 로그인합니다 <https://hostname>, 위치 hostname OnCommand Insight가 설치된 시스템의 이름입니다.
2. Admin * > * Troubleshooting * 을 클릭합니다. 페이지 하단에서 * 고급 문제 해결 * 을 클릭합니다.
3. Actions * 탭에서 * Update DWH Annotations (include deleted) * 를 클릭합니다.

사용자 정의 주석을 데이터 웨어하우스로 불러오기

OnCommand Insight에서 주석 업데이트를 적용한 후 데이터 웨어하우스에서 원하는 주석을 선택하고 데이터 웨어하우스 빌드를 시작해야 합니다. 다음 예약된 빌드가 나올 때까지 기다리거나 지금 빌드를 시작할 수 있습니다.

단계

1. Data Warehouse Portal()에 관리자로 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * Annotations * 를 클릭합니다.

Annotations

Annotation	Column Name	Target Object	Published
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	
Data_Center	dataCenter	Host	✓
Data_Center	dataCenter	Storage	✓
Data_Center	dataCenter	Switch	✓
Note	Note	Switch	
Switch_Level	switchLevel	Switch	✓
Tier	Tier	Internal Volume	
Tier	Tier	Qtree	
Tier	Tier	Storage	
Tier	Tier	Storage Pool	
Tier	Tier	Volume	

Edit

이 목록에는 모든 주석 유형에 대한 행과 주석을 지정할 수 있는 대상 객체가 표시됩니다. Published(게시됨) 열의 체크 표시는 특정 대상 개체에 대해 주석이 이미 선택되었으며 Data Warehouse(데이터 웨어하우스) 데이터 마트를 통해 이미 사용 가능함을 나타냅니다.

3. OnCommand Insight에서 주석을 가져오는 방법을 편집하려면 * 편집 * 을 클릭합니다.

Edit Annotations

Annotation	Column Name	Target Object	Published All / None	Init With Current All / None
Compute_Resource_Group	Compute_Resource_Group	Virtual Machine	<input type="checkbox"/>	<input type="checkbox"/>
Data_Center	dataCenter	Host	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data_Center	dataCenter	Storage	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Data_Center	dataCenter	Switch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Note	Note	Switch	<input type="checkbox"/>	<input type="checkbox"/>
Switch_Level	switchLevel	Switch	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Internal Volume	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Qtree	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Storage	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Storage Pool	<input type="checkbox"/>	<input type="checkbox"/>
Tier	Tier	Volume	<input type="checkbox"/>	<input type="checkbox"/>

Save Cancel

4. 주석 프로세스를 편집하려면 다음을 수행합니다.

- OnCommand Insight에서 가져온 주석을 데이터 웨어하우스 데이터베이스에 추가하려면 * Published * 를 선택합니다. 모든 개체의 모든 주석을 선택하려면 * All * (모두 *)을 클릭합니다. 모든 옵션을 선택하지 않으려면 * 없음 * 을 클릭합니다.



특정 객체의 재고 테이블 및 관련 데이터 마트에서 주석 열을 제거하려면 이 옵션을 선택 취소합니다. 사용자 정의 보고서가 주석 데이터를 사용하는 경우 보고서가 성공적으로 실행되지 않습니다.

- 데이터 웨어하우스 차원 테이블의 기록 데이터를 현재 주석 값으로 초기화하려면 * Init with Current * 를

선택합니다. 모든 개체의 모든 주석을 선택하려면 * All * (모두 *)을 클릭합니다. 모든 옵션을 선택하지 않으려면 * 없음 * 을 클릭합니다. 주석을 게시한 후에는 이 확인란을 사용할 수 없으며 게시되지 않은 주석에는 확인란을 사용할 수 있습니다. 예를 들어, 호스트에 주석 유형 ""바닥""이 주석으로 추가되고 호스트_차원 테이블에 해당 호스트에 대한 행 3개가 있는 경우 * 현재 * 와 함께 초기화 를 선택하면 호스트_차원 테이블의 "바닥" 열에 있는 값 ""1""이 연결됩니다. 현재 * 포함 초기화 * 를 선택하지 않으면 해당 호스트의 최신 행만 바닥 열에 ""1"" 값을 갖게 됩니다.

5. 저장 * 을 클릭합니다.

주석을 제거할 경우 데이터 구조 또는 데이터 손실이 변경된다는 경고 메시지가 나타납니다.

6. 계속하려면 * 예 * 를 클릭합니다.

데이터 웨어하우스는 요청된 변경 사항을 적용하는 비동기 주석 작업을 시작합니다. 작업 페이지에서 작업을 볼 수 있습니다. 데이터 웨어하우스 데이터베이스 스키마의 변경 사항도 볼 수 있습니다.

작업 목록에서 주석 작업 보기

작업 목록에서 주석 작업을 보고 주석 변경 사항을 데이터 웨어하우스 데이터 마트에 적용할 수 있습니다.

단계

1. Data Warehouse Portal()에 관리자로 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * Jobs * 를 클릭합니다.

데이터베이스 스키마의 주석 변경 표시

데이터베이스 스키마는 특정 테이블의 변경 사항을 반영합니다.


이 작업에 대해

예를 들어 스토리지 배열에 주석을 추가하는 경우 인벤토리 또는 기타 데이터 마트의 스토리지 또는 스위치 테이블에 주석이 표시됩니다.

OnCommand Insight 사용자 인터페이스를 사용하여 리소스의 주석을 업데이트하고 다음 데이터 웨어하우스 빌드를 시작하거나 기다릴 경우 재고(dWh_inventory)의 해당 객체와 해당 차원 테이블에서도 새 열이 추가되거나 제거됩니다 (해당 데이터 마트에서). 결과는 다음 표에 나와 있습니다.

- dWh_inventory.annotation_value 를 입력합니다
- dWh_inventory.object_to_annotation

단계

1. 을 클릭합니다  데이터 웨어하우스 도구 모음에서 * 문서 * 를 선택합니다.
2. 데이터베이스 스키마 * 를 선택합니다.
3. 왼쪽의 * 데이터베이스 스키마 * 창에서 * DWH_INVENTORY * 섹션으로 스크롤하여 * SWITCH * 를 클릭합니다.

Database Schema

Databases

storage_port

storage_to_applica

switch

switch_port

switch_port_to_ap

switch_to_applicati

tape

tape_controller

tape_port

tier

violation

virtual_switch

virtual_to_backend

vm_to_application

volume

volume_in_storage

dwh_inventory.switch

Column	Type	Nullable	Description
id	int(11)	false	GUID of the switch.
fabricId	int(11)	true	GUID of the fabric on which this switch is configured to operate. References: <ul style="list-style-type: none">id in dwh_inventory.fabric
identifier	varchar (255)	false	Identifier of the device.
wwn	varchar (255)	false	WWN of the switch.
ip	varchar (255)	false	IP address of the switch.
Name	varchar (255)	false	Name of the switch.
Manufacturer	varchar (255)	true	Manufacturer of the switch
Model	varchar (255)	true	Manufacturer's model of the switch.
Firmware	varchar (255)	true	Firmware version running on the switch.

4. dWh_inventory.switch * 테이블에는 변경 사항이 반영됩니다.

Database Schema

Databases

host_group_dimen

internal_volume_c

internal_volume_d

qtree_capacity_fac

qtree_dimension

service_level_dime

storage_dimension

storage_pool_dime

tier_dimension

vm_capacity_fact

vm_dimension

volume_fact_curre

dwh_capacity.storage_dimension

Column	Type	Nullable	Description
tk	int(11)	false	TK of this storage array row.
name	varchar (255)	false	Name of the storage array.
identifier	varchar (255)	false	Identifier of the device.
ip	varchar (255)	false	IP address of the storage array.
model	varchar (255)	true	Manufacturer's model of the storage array.
manufacturer	varchar (255)	true	Manufacturer of the storage array.
serialNumber	varchar (255)	true	Serial number for the storage array.
microcodeVersion	varchar (255)	true	Version of the firmware running on the storage array.
family	varchar (255)	true	Family name of the storage array (e.g. Clariion, Symmetrix etc).
id	int(11)	true	GUID of the storage array in dwh_inventory.storage.

DataCenter 주석 열이 storage_dimensions 테이블에 나타납니다.

이메일 알림 설정

데이터 웨어하우스 작업이 성공적으로 완료되지 않은 경우 데이터 웨어하우스에서 특정 이메일 주소로 이메일을 보내도록 할 수 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname` OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 이메일 알림 * 을 클릭합니다.
3. 다음을 입력합니다.

- SMTP 서버 주소입니다

조직의 SMTP 서버 역할을 하는 서버를 지정합니다. 이 서버는 `nnn.nnn.nnn.nnn` 형식을 사용하여 호스트 이름 또는 IP 주소를 사용하여 식별됩니다. 호스트 이름을 지정하는 경우 DNS에서 해당 이름을 확인할 수 있는지 확인합니다.

- SMTP 서버 사용자 이름 및 암호

전자 메일 서버에 액세스할 사용자 이름을 지정하며 SMTP 서버에 사용자가 서버에 로그인해야 하는 경우에만 필요합니다. 응용 프로그램에 로그인하고 전자 메일에 액세스하는 데 사용하는 것과 동일한 사용자 이름입니다.

- 알림이 활성화되었습니다

- 예 * 알림을 활성화하고 * 아니요 * 알림을 비활성화합니다.

- 보낸 사람의 이메일

알림을 보내는 데 사용되는 이메일 주소를 지정합니다. 조직의 유효한 이메일 주소여야 합니다.

- 받는 사람의 이메일

항상 전자 메일을 받을 사람의 전자 메일 주소 또는 주소를 지정합니다. 주소가 여러 개인 경우 쉼표로 구분하십시오.

- 이메일 제목

알림의 제목을 지정합니다.


- 이메일 서명

전자 메일 하단에 표시되는 정보(예: 부서 이름)를 지정합니다.

보고 포털에 액세스

데이터 웨어하우스 포털에서 보고 포털에 액세스하여 Workspace Advanced 및 Report Studio와 같은 보고서 작성 도구를 사용하여 사용자 지정 보고서를 만들 수 있습니다.

단계

1. 데이터 웨어하우스 도구 모음에서  Insight Reporting Portal을 엽니다.
2. 사용자 이름과 암호를 입력하고 * 로그인 * 을 클릭합니다.

데이터 웨어하우스 데이터베이스 스키마 문서 보기

데이터 웨어하우스 데이터베이스 스키마 정보를 검토할 수 있습니다.


단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 데이터 웨어하우스 도구 모음에서  스키마 * 를 선택합니다.

데이터 웨어하우스 데이터베이스 스키마 보기

데이터베이스 스키마를 보고 다른 API에서 데이터를 사용하는 방법을 이해하거나 SQL 쿼리를 개발할 수 있습니다. 스키마 옵션은 스키마의 모든 데이터베이스, 테이블 및 열을 나열합니다. 테이블 관계를 보여 주는 데이터베이스 스키마 다이어그램을 검토할 수도 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2.  을 클릭합니다. 데이터 웨어하우스 도구 모음에서 * 문서 * 를 선택합니다.
3. 데이터베이스 스키마 * 를 선택합니다.
4. 예를 들어, * Databases * 창에서 * DWH_inventory * 를 클릭합니다.
5. 모든 테이블 * 창에서 * DWH_INVENTORY * 섹션으로 스크롤하여 * annotation_Value * 테이블을 클릭합니다.

Databases DWH_CAPACITY DWH_CAPACITY_EFFICIENCY DWH_FS_UTIL DWH_INVENTORY DWH_PERFORMANCE DWH_PORTS	dataSourceUserName	role	type	message description for the data source status
	additionalDataSourceMessage	varchar(255)	true	Additional status message for the data source.

dwh_inventory.annotation_value			
Column	Type	Nullable	Description
id	int(11)	false	GUID for the annotation.
annotationType	varchar(255)	false	System or user defined type such as Tier, Data center, etc.
valueIdentifier	varchar(255)	false	Value of the annotation.
valueType	enum('BOOLEAN', 'DATE', 'ENUM', 'FLEXIBLE_ENUM', 'NUMBER', 'ORDERED_ENUM', 'TEXT')	false	The data type for annotation value.
valueDate	datetime	true	Value of the annotation (Date format).
sequence	int(11)	true	Sequence number determining the order of enumeration values. This is used primarily for display purposes.
costCost	double	true	Optional cost associated with the annotation. Applicable for Tier annotation.

dwh_inventory.application			
Column	Type	Nullable	Description
id	int(11)	false	GUID for the application.
businessEntityId	int(11)	true	GUID of the business entity References: • id in dwh_inventory.business_entity
name	varchar(255)	false	Name of the application.

dWh_inventory.annotation 테이블이 나타납니다.

시스템 정보 보기

시스템, 모듈, 라이선스 및 데이터 웨어하우스 업그레이드 정보를 볼 수 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 시스템 정보 * 를 클릭합니다.
3. System* 탭에서 시스템 정보를 검토하고 필요한 경우 사이트 이름을 편집합니다.
 - a. Edit Site Name * 을 클릭합니다
 - b. 새 사이트 이름을 입력하고 * 저장 * 을 클릭합니다.
4. 응용 프로그램 정보(응용 프로그램 이름, 모듈, 버전 및 설치 날짜)를 보려면 * 응용 프로그램 정보 * 탭을 클릭합니다.
5. 라이선스 정보(프로토콜, 코드, 만료 날짜 및 수량)를 보려면 * Licenses * 탭을 클릭합니다.
6. 응용 프로그램 업그레이드 정보(응용 프로그램 이름, 시작 날짜, 종료 날짜, 시간, 사용자, 및 파일 크기)를 클릭하고 * 업그레이드 기록 * 을 클릭합니다.

고급 옵션

데이터 웨어하우스에는 다양한 고급 옵션이 포함되어 있습니다.

실패한 빌드를 건너뛰니다

처음 빌드한 후 경우에 따라 빌드 실패 문제가 발생할 수 있습니다. 빌드 실패 후 모든 작업이

성공적으로 완료되도록 하려면 * 기록 빌드 실패 건너뛰기 * 옵션을 활성화합니다.

이 작업에 대해

빌드가 실패하고 * 기록 빌드 실패 건너뛰기 * 옵션이 활성화된 경우 데이터 웨어하우스는 빌드를 계속 수행하고 실패한 빌드는 무시합니다. 이 경우 건너뛴 빌드에 대한 기간별 데이터에 데이터 포인트가 없습니다.

빌드에 성공하지 못한 경우에만 이 옵션을 사용합니다.

기록에서 빌드에 실패하고 * 기록 빌드 실패 건너뛰기 * 확인란을 선택하지 않으면 이후의 모든 작업이 중단됩니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 기록에서 작성 * 을 클릭합니다.

Build From History

Target time	Start running	Status
3/13/15 12:00 AM	3/25/15 9:28 AM	COMPLETED
3/14/15 12:00 AM	3/25/15 9:34 AM	COMPLETED
3/15/15 12:00 AM	3/25/15 9:39 AM	COMPLETED
3/16/15 12:00 AM	3/25/15 9:45 AM	COMPLETED
3/17/15 12:00 AM	3/25/15 9:51 AM	COMPLETED
3/18/15 12:00 AM	3/25/15 9:57 AM	COMPLETED
3/19/15 12:00 AM	3/25/15 10:03 AM	COMPLETED
3/20/15 12:00 AM	3/25/15 10:09 AM	COMPLETED
3/21/15 12:00 AM	3/25/15 10:16 AM	COMPLETED
3/22/15 12:00 AM	3/25/15 10:23 AM	COMPLETED
3/23/15 12:00 AM	3/25/15 10:30 AM	COMPLETED
3/24/15 12:00 AM	3/25/15 10:38 AM	COMPLETED
3/25/15 12:00 AM	3/25/15 10:44 AM	COMPLETED

<< < 1 2 3 > >>

Cancel Pending Jobs Configure Run

Skip history build failures: ☒

3. 구성 * 을 클릭합니다.
4. 빌드를 구성합니다.
5. 저장 * 을 클릭합니다.
6. 실패한 빌드를 건너뛰려면 * Skip history build failures * 를 선택합니다.

이 확인란은 * Run * 버튼이 활성화된 경우에만 표시됩니다.

7. 자동 예약된 빌드 외부에서 빌드를 수행하려면 * 실행 * 을 클릭합니다.

데이터 웨어하우스 데이터베이스 또는 보고 서버 재설정

데이터 웨어하우스 데이터 마트의 내용을 삭제하고 구성된 모든 커넥터를 삭제할 수 있습니다. 설치 또는 업그레이드가 성공적으로 완료되지 않고 데이터 웨어하우스 데이터베이스를 중간 상태로 둔 경우 이 작업을 수행할 수 있습니다. 재고 데이터 모델 또는 Cognos 보고 데이터 모델만 삭제할 수도 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * DWH 데이터베이스 재설정 * 을 클릭합니다.
3. 다음 옵션 중 하나를 클릭합니다.

- * DWH 데이터베이스 재설정 *

이렇게 하면 모든 데이터 웨어하우스 데이터 마트의 내용과 구성된 모든 커넥터가 삭제되고 사용자 정의 구성 없이 데이터 웨어하우스가 기본 설치 상태로 전환됩니다. 예를 들어 연결된 서버를 변경했지만 실수로 다른 데이터 웨어하우스 데이터베이스를 서버에 복원하여 기본 설치 상태로 돌아가야 하는 경우 이 옵션을 선택할 수 있습니다. 이 경우 보고서가 삭제되지 않습니다. (보고서는 Cognos 콘텐츠 저장소에 저장됩니다.)

- * 재고만 재설정 *

그러면 재고 데이터 모델의 내용만 삭제됩니다. 기록 데이터는 삭제되지 않습니다.

- * 보고 콘텐츠 재설정 *

이렇게 하면 보고 서버의 내용이 재설정됩니다. 이렇게 하면 사용자 정의 보고서가 삭제됩니다. 이 옵션을 선택하기 전에 보고서를 백업하십시오.

경고 메시지가 표시됩니다.

4. 계속하려면 * 예 * 를 클릭합니다.

6.3 이전 버전의 보고서 복원 및 업그레이드

6.3 이전 Insight 버전을 업그레이드하는 경우 보고 아티팩트를 수동으로 복원해야 합니다.

시작하기 전에

"DWH(데이터 웨어하우스 업그레이드)" 및 "사용자 정의 보고서 및 보고 아티팩트 백업" 항목의 지침을 따릅니다.

단계

1. 버전 6.3 이전 버전에서 보고 아티팩트를 복원하려면 에서 만들고 저장한 backup.zip 파일 내보내기 를 복사합니다 <install>\cognos\c10_64\deployment 디렉토리.
2. 브라우저를 열고 로 이동합니다 <http://<server>:<port>/reporting> 설치 중에 사용한 서버 및 포트의 경우.

3. 사용자 이름과 암호를 입력하고 * 로그인 * 을 클릭합니다.
4. 시작 * 메뉴에서 * Insight Reporting Administration * 을 선택합니다.
5. Configuration * 탭을 클릭합니다.

데이터 모델의 변경으로 인해 이전 패키지의 보고서가 실행되지 않을 수 있으므로 업그레이드해야 합니다.

6. 콘텐츠 관리 * 를 클릭합니다.
7. 새 가져오기 * 버튼을 클릭합니다.
8. 배포 디렉토리에 복사한 아카이브를 확인합니다(예: backup6.0.zip)를 선택하고 * 다음 * 을 클릭합니다.
9. 보관 파일을 보호하기 위해 비밀번호를 입력한 경우 비밀번호를 입력하고 * OK * (확인 *)를 클릭합니다.
10. 이름을 변경합니다 Export... 를 선택합니다 Import Backup 를 클릭하고 * 다음 * 을 클릭합니다.
11. 각 패키지 이름 옆에 있는 연필 아이콘을 클릭하고 필요한 경우 새 대상 이름을 입력합니다. 예를 들어, 을 추가합니다 _original 기존 이름에 접미사 사용. 그런 다음 * 확인 * 을 클릭합니다.
12. 모든 패키지의 대상 패키지 이름을 변경한 후 모든 파란색 폴더를 선택하고 * 다음 * 을 클릭하여 계속합니다.
13. 모든 기본값을 적용합니다.
14. 마침 * 을 클릭한 다음 * 실행 * 을 선택합니다.
15. 이 가져오기의 세부 정보를 확인하고 * OK * 를 클릭합니다.
16. 가져오기 상태를 보려면 * Refresh * (새로 고침 *)를 클릭합니다.
17. 가져오기가 완료되면 * 닫기 * 를 클릭합니다.

결과

두 개의 패키지 세트가 공용 폴더 탭에 나타납니다. 예를 들어, 가 있는 가 있습니다 7.0 접미사(새 버전의 경우) 및 가 포함된 접미사 _original (또는 백업/복원 절차 중에 입력한 내용) 접미사에 이전 보고서가 포함되어 있습니다. 데이터 모델의 변경으로 인해 이전 패키지의 보고서가 실행되지 않을 수 있으므로 업그레이드해야 합니다. 이제 포털 탭이 포털 페이지의 현재 버전을 가리킵니다.

명령줄 인터페이스를 사용하여 MySQL 액세스

보고서 작성 도구를 통해 데이터 웨어하우스 데이터 요소에 액세스하는 것 외에도 MySQL 사용자로 연결하여 데이터 웨어하우스 데이터 요소에 직접 액세스할 수 있습니다. MySQL 사용자로 연결하여 응용 프로그램의 데이터 요소를 사용할 수 있습니다.

이 작업에 대해

다양한 방법으로 연결할 수 있습니다. 다음 단계에서는 한 가지 방법을 보여 줍니다.

MySQL에 액세스할 때 데이터 웨어하우스가 설치된 시스템의 MySQL 데이터베이스에 연결합니다. MySQL 포트는 기본적으로 3306이지만 설치 중에 변경할 수 있습니다. 사용자 이름 및 암호는 dwhuser/netap123 입니다.

단계

1. 데이터 웨어하우스가 설치된 컴퓨터에서 명령줄 창을 엽니다.
2. OnCommand Insight 디렉토리에서 MySQL 디렉토리에 액세스합니다.

3. 다음 사용자 이름 및 암호를 입력합니다. `mysql -udwhuser -pnetapp123`

데이터 웨어하우스가 설치된 위치에 따라 다음이 표시됩니다.

```
c:\Program Files\SANscreen\mysql\bin> mysql -udwhuser -pnetapp123
```

```
Welcome to the MySQL monitor. Commands end with ; or \g.  
Your MySQL connection id is 882  
Server version: 5.1.28-rc-community MySQL Community Server (GPL)
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the buffer.
```

4. 데이터 웨어하우스 데이터베이스 표시: `show databases;`

다음과 같은 메시지가 표시됩니다.

```
mysql> show databases;  
+-----+  
| Database |  
+-----+  
| information_schema |  
| dwh_capacity |  
| dwh_capacity_efficiency |  
| dwh_fs_util |  
| dwh_inventory |  
| dwh_performance |  
| dwh_ports |  
+-----+
```

데이터 웨어하우스 문제 해결

데이터 웨어하우스 문제 해결과 관련된 다양한 작업을 수행할 수 있습니다.

- OnCommand Insight ASUP를 사용하십시오.
- OnCommand Insight 로그를 봅니다.
- 업그레이드 및 업무 엔티티와 관련된 문제를 해결합니다.
- 여러 OnCommand Insight 서버의 통합과 관련된 문제를 해결합니다.

여러 OnCommand Insight 서버를 동일한 데이터 웨어하우스 데이터베이스에 통합할 수 있습니다. 여러 구성에서 여러 커넥터에서 동일한 개체를 보고할 수 있습니다(즉, 두 OnCommand Insight 인스턴스에 동일한 스위치가 있음). 이러한 경우 데이터 웨어하우스는 여러 오브젝트를 하나로 통합합니다(기본 커넥터가 선택되고 개체의 데이터는 해당

커넥터에서만 가져옵니다).

스토리지 관리자는 문제 해결 페이지를 사용하여 통합 문제와 관련된 문제를 해결할 수 있습니다.

ASUP로 문제를 해결합니다

문제 해결에 도움이 필요하면 ASUP 로그를 기술 지원 팀에 보낼 수 있습니다. 데이터 웨어하우스에 대한 ASUP는 자동으로 실행되도록 구성됩니다. 데이터 웨어하우스 포털에서 자동 전송 프로세스를 비활성화하거나 데이터 웨어하우스 데이터베이스의 백업을 포함할지 아니면 ASUP로 전송을 시작할지 선택할 수 있습니다.

로그의 정보는 HTTPS 프로토콜을 사용하여 기술 지원 부서로 전달됩니다. Insight Server에서 먼저 구성하지 않으면 ASUP를 사용하여 데이터가 전달되지 않습니다.

데이터 웨어하우스는 로그를 데이터 웨어하우스 포털 커넥터 페이지에 나열된 첫 번째 커넥터인 OnCommand Insight 서버로 보냅니다. 자동 프로세스는 다음 파일을 전송합니다.

- 데이터 웨어하우스 로그 - 다음 포함:
 - boot.log (백업 포함)
 - dwh.log (dWh.log와 같은 백업 포함1)
 - dhw_troubleshoot.log
 - dwh_upgrade.log (백업 포함)
 - WildFly.log (백업 포함)
 - ldap.log (백업 포함)
 - 데이터 웨어하우스 관리 데이터베이스의 SQL 덤프
 - MySQL: my.cnf, .err 및 slow query logs
 - Full innodb 상태

- 다음 항목이 포함된 Cognos 로그:

- cognos-logs.zip

의 Cognos 로그 파일이 들어 있습니다 <install>\cognos\c10_64\logs 디렉토리. 또한 Cognos에서 생성된 로그와 OnCommand Insight 보고 로그인 및 로그아웃 사용자의 모든 로깅이 포함된 OnCommand InsightAP.log 파일도 포함합니다.

- DailyBackup.zip

공용 폴더에 있는 보고 아티팩트의 백업이 포함되어 있습니다. 내 폴더의 내용은 여기에 포함되지 않습니다.

- Cognos versionsite name_content_store.zip

Cognos 콘텐츠 저장소의 전체 백업이 포함되어 있습니다.

문제 해결 보고서를 수동으로 생성할 수 있습니다. Troubleshooting Report.zip 파일에는 다음과 같은 데이터 웨어하우스 정보가 포함되어 있습니다.

- boot.log (백업 포함)

- dwh.log (dWh.log와 같은 백업 포함1)
- dwh_upgrade.log (백업 포함)
- wildfly.log (백업 포함)
- ldap.log (백업 포함)
- c:\Program Files\SANscreen\Wildfly\standalone\log\dWh\에서 파일을 덤프합니다
- 데이터 웨어하우스 관리 데이터베이스의 SQL 덤프
- MySQL: my.cnf, .err 및 slow query logs
- Full innodb 상태



ASUP 톨은 OnCommand Insight 데이터베이스의 백업을 기술 지원으로 자동으로 전송하지 않습니다.

자동 **ASUP** 전송 비활성화

모든 NetApp 제품에는 자동화된 기능을 제공하여 고객 환경에서 발생하는 문제를 해결하는 데 가장 적합한 지원을 제공합니다. ASUP는 사전 정의된 특정 정보를 고객 지원에 주기적으로 전송합니다. 기본적으로 ASUP는 데이터 웨어하우스에 대해 활성화되어 있지만, 더 이상 정보를 전송하지 않으려는 경우 비활성화할 수 있습니다.

단계

1. 왼쪽의 탐색 창에서 * 문제 해결 * 을 클릭합니다.
2. ASUP에서 일별 보고서를 전송하지 않으려면 * 비활성화 * 를 클릭합니다.

ASUP가 비활성화되었다는 메시지가 표시됩니다.

데이터 웨어하우스 데이터베이스의 백업 포함

기본적으로 ASUP에서는 문제 해결에 도움이 되도록 데이터 웨어하우스 로그 파일만 기술 지원 부서에 보냅니다. 그러나 데이터 웨어하우스 데이터베이스의 백업을 포함하고 보낼 데이터 유형을 선택할 수도 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 문제 해결 * 을 클릭합니다.
3. 데이터 웨어하우스 데이터베이스의 백업을 ASUP에 포함하도록 지정하려면 * Include DWH Database Backup *(DWH 데이터베이스 백업 포함 *) 목록을 클릭하고 백업에 포함되어야 하는 데이터 유형에 대해 다음 옵션 중 하나를 선택합니다.
 - 모두(성능 포함)
 - 성능을 제외한 모든 시장
 - 재고만

4. Update * 를 클릭합니다.

ASUP에 Insight 로그 전송

문제 해결에 도움이 필요하다면 ASUP 로그를 기술 지원 팀에 보낼 수 있습니다. 데이터 웨어하우스에 대한 ASUP는 자동으로 실행되도록 구성됩니다. 데이터 웨어하우스 포털에서 자동 전송 프로세스를 비활성화하거나 데이터 웨어하우스 데이터베이스의 백업을 포함할지 아니면 ASUP로 전송을 시작할지 선택할 수 있습니다. ASUP 보고서를 요청하면 보고서 요청이 데이터 웨어하우스 포털 작업 페이지에 작업으로 나타납니다.

이 작업에 대해

작업은 다른 작업의 처리와 유사한 작업 대기열에 의해 관리됩니다. ASUP 작업이 이미 보류 또는 실행 중인 상태인 경우 작업 대기열에 보류 중이거나 실행 중인 요청이 포함되어 있어 작업 요청에 ASUP 보고서 요청을 추가할 수 없음을 나타내는 오류 메시지가 나타납니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 문제 해결 * 을 클릭합니다.
3. 문제 해결 * 페이지의 * OnCommand Insight ASUP * 섹션에서 * DWH 문제 해결 보고서 다운로드 * 를 클릭하여 문제 해결 보고서를 검색합니다.
4. 데이터 웨어하우스 포털 * 커넥터 * 페이지의 첫 번째 커넥터로 나열된 OnCommand Insight 서버로 보고서를 보내려면 * 지금 보내기 * 를 클릭합니다.

OnCommand Insight 로그 보기

OnCommand Insight에서 다양한 데이터 웨어하우스 및 Cognos 로그를 볼 수 있습니다.

이 작업에 대해

Cognos 및 데이터 웨어하우스 로그 파일에서 문제 해결 및 상태 정보를 확인할 수 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 문제 해결 * 을 클릭합니다.
3. 로그 * 섹션에서 * 로그 파일 * 을 클릭합니다.

다음 로그 파일이 표시됩니다.

dwh.log

데이터 웨어하우스 작업의 상태를 나열합니다

wildfly.log
WildFly 응용 프로그램 서버에 대한 자세한 내용은 에 나와 있습니다
dWh_업그레이드 로그
데이터 웨어하우스의 업그레이드에 대한 내용은 에 나와 있습니다
ldap.log
LDAP 인증과 관련된 메시지를 기록합니다
dwh_troubleshoot.log
DWH 문제 해결에 도움이 되는 메시지를 기록합니다
sansscreenap.log
서버 연결, Cognos 리포지토리에 대한 인증 및 액세스, 기타 프로세스에 대한 정보를 제공합니다
cognosserver.log
Cognos 로그

4. 보려는 로그 파일의 이름을 클릭합니다.

여러 서버 새시 통합 문제

호스트 및 어댑터, SAN 스위치 및 스토리지 배열에 대해 보고하는 커넥터를 볼 수 있습니다. 개체에 대해 보고하는 다양한 커넥터를 확인하고 개체에 대해 선택한 커넥터인 기본 커넥터를 식별할 수도 있습니다.

호스트 및 어댑터 통합 문제 보기

호스트 및 관련 어댑터에 대해 보고된 데이터는 Inventory Data Mart에서 파생됩니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 문제 해결 * 을 클릭합니다.
3. 새시 통합 * 섹션에서 * 호스트 및 어댑터 * 를 클릭합니다.



이 예에 표시된 구성은 올바른 구성이 아닙니다. localhost의 보안 및 사용 가능한 커넥터는 Insight 서버와 DWH가 모두 동일한 서버에 설치된다는 것을 의미합니다. 이 예제의 목적은 통합 테이블을 숙지하는 것입니다.

Hosts and Adapters Consolidation

Host GUID	Host Name	Host IP	Adapter GUID	Adapter WWN	Principal Connector	Available Connectors	Insight ID	Insight Change Time
288	Agassi	192.1.168.71			localhost (1)	localhost (1)	9927	11/18/10 1:36 PM
			576	40:A0:00:00:00:00:84	localhost (1)	localhost (1)	9928	11/18/10 1:36 PM
			577	40:A0:00:00:00:00:85	localhost (1)	localhost (1)	9930	11/18/10 1:36 PM
305	AI_Host1	192.1.168.88			localhost (1)	localhost (1)	12254	11/18/10 1:38 PM
			597	40:A0:00:00:00:00:01:05	localhost (1)	localhost (1)	12255	11/18/10 1:38 PM
306	AI_Host2	192.1.168.89			localhost (1)	localhost (1)	12257	11/18/10 1:38 PM
			598	40:A0:00:00:00:00:01:06	localhost (1)	localhost (1)	12258	11/18/10 1:38 PM
307	AI_Host3	192.1.168.90			localhost (1)	localhost (1)	12260	11/18/10 1:38 PM

모든 호스트 및 어댑터의 경우 각 커넥터에 대해 보고하는 행과 호스트 및 어댑터가 사용되는 기본 커넥터가 있습니다. 호스트 및 어댑터만 해당, 한 커넥터에서 보고하는 호스트에는 다른 커넥터가 보고하는 어댑터가 있을 수 있습니다.

각 커넥터의 호스트/어댑터의 OnCommand Insight 변경 시간도 볼 수 있습니다. 이 매개 변수를 사용하면 호스트/어댑터의 OnCommand Insight에서 업데이트가 발생한 시기와 다른 OnCommand Insight 서버에서 동일한 호스트/어댑터가 업데이트된 시기를 확인할 수 있습니다.

- 필요한 경우 텍스트 부분을 입력하고 * Filter * 를 클릭하여 이 보기의 데이터를 필터링합니다. 필터를 지우려면 * Filter * (필터) 상자의 텍스트를 삭제하고 * Filter * (필터)를 클릭합니다. 호스트 이름, 호스트 IP, 어댑터 WWN 또는 OnCommand Insight 객체 ID를 기준으로 필터링할 수 있습니다.

필터는 대소문자를 구분합니다.

- 다음 데이터를 검토합니다.

- 호스트 GUID *

이 유형의 통합 장치(호스트)에 대한 글로벌 고유 식별자

- * 호스트 이름 *

데이터 웨어하우스에 표시되는 통합 호스트의 이름입니다

- * 호스트 IP *

통합 호스트의 IP 주소입니다

- * 어댑터 GUID *

호스트 어댑터의 글로벌 고유 식별자입니다

- * 어댑터 WWN *

호스트 어댑터의 WWN입니다

- * 주 커넥터 *

데이터의 실제 소스인 OnCommand Insight 커넥터의 이름입니다

- * 사용 가능한 커넥터 *

통합 호스트/어댑터가 상주하는 모든 OnCommand Insight 커넥터

- * Insight ID *

관련 보고 커넥터용 통합 호스트/어댑터의 OnCommand Insight ID입니다

- * Insight 변경 시간 *

호스트/어댑터의 OnCommand Insight에서 업데이트가 발생한 경우 및 다른 OnCommand Insight 서버에서 동일한 호스트/어댑터가 업데이트된 경우

6. 커넥터에 대한 자세한 내용을 보려면 커넥터를 클릭하십시오.

커넥터에 대한 다음 정보를 볼 수 있습니다.

- 호스트 이름입니다
- 해당 커넥터에서 데이터 웨어하우스 작업을 마지막으로 실행한 시간입니다
- 해당 커넥터로부터 마지막으로 변경 사항을 수신한 시간입니다
- 해당 커넥터가 가리키는 OnCommand Insight 서버의 버전입니다

스토리지 시스템 통합 문제 보기

스토리지 어레이에 대해 보고된 데이터는 Inventory Data Mart에서 파생됩니다. 모든 스토리지 어레이에는 각 어레이가 사용되는 기본 커넥터뿐만 아니라 각 커넥터에 대해 보고하는 행이 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 문제 해결 * 을 클릭합니다.
3. 새시 통합 * 섹션에서 * SAN 스토리지 어레이 * 를 클릭합니다.
4. 필요에 따라 이 보기에서 데이터를 필터링하려면 필터 상자에 텍스트 부분을 입력하고 * 필터 * 를 클릭합니다. 필터를 지우려면 필터 상자의 텍스트를 삭제하고 * 필터 * 를 클릭합니다. 스토리지 이름, 스토리지 IP, 공급업체 모델 또는 OnCommand Insight 객체 ID를 기준으로 필터링할 수 있습니다.

필터는 대소문자를 구분합니다.

5. 다음 데이터를 검토합니다.

◦ GUID *

이 유형의 통합 디바이스(스토리지 어레이)에 대한 글로벌 고유 식별자

◦ * 이름 *

데이터 웨어하우스에 표시되는 통합 스토리지 배열의 이름입니다

◦ * IP *

통합 스토리지 시스템의 IP 주소입니다

◦ * 공급업체 및 모델 *

통합 스토리지 어레이를 판매하는 공급업체 이름 및 제조업체의 모델 번호입니다

◦ * 주 커넥터 *

데이터의 실제 소스인 OnCommand Insight 커넥터의 이름입니다

◦ * 사용 가능한 커넥터 *

통합 스토리지 배열이 있는 모든 OnCommand Insight 커넥터

◦ * Insight ID *

주 커넥터가 상주하는 OnCommand Insight 새시의 통합 스토리지 배열의 ID입니다

◦ * Insight 변경 시간 *

스토리지 배열에 대한 OnCommand Insight에서 업데이트가 발생한 경우 및 다른 OnCommand Insight 서버에서 동일한 스토리지 배열이 업데이트된 경우

스위치 통합 문제 보기

스위치에 대해 보고된 데이터는 Inventory Data Mart에서 파생됩니다. 모든 스위치에 대해 각 커넥터를 보고하는 행과 각 스위치를 사용하는 기본 커넥터가 있습니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 `https://hostname/dwh`, 위치 `hostname OnCommand Insight` 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 문제 해결 을 클릭합니다.
3. 새시 통합 * 섹션에서 * SAN 스위치 * 를 클릭합니다.
4. 필요한 경우 텍스트 부분을 입력하고 * Filter * 를 클릭하여 이 보기의 데이터를 필터링합니다. 필터를 지우려면 필터 상자의 선택을 취소하고 * 필터 * 를 클릭합니다. 스위치 이름, 스위치 IP, 공급업체 모델 또는 OnCommand Insight 객체 ID를 기준으로 필터링할 수 있습니다.

필터는 대소문자를 구분합니다.

5. 다음 데이터를 검토합니다.

- GUID *

이 유형의 통합 디바이스(스토리지 어레이)에 대한 글로벌 고유 식별자

- * 이름 *

데이터 웨어하우스에 표시되는 통합 스토리지 배열의 이름입니다

- * IP *

통합 스토리지 시스템의 IP 주소입니다

- * 공급업체 및 모델 *

통합 스토리지 어레이를 판매하는 공급업체 이름 및 제조업체의 모델 번호입니다

- WWN *

통합 스위치의 WWN입니다

- * 주 커넥터 *

데이터의 실제 소스인 OnCommand Insight 커넥터의 이름입니다

- * 사용 가능한 커넥터 *

통합 스토리지 배열이 있는 모든 OnCommand Insight 커넥터

- * Insight ID *

주 커넥터가 상주하는 OnCommand Insight 새시의 통합 스토리지 배열의 ID입니다

- * Insight 변경 시간 *

스토리지 배열에 대한 OnCommand Insight에서 업데이트가 발생한 경우 및 다른 OnCommand Insight 서버에서 동일한 스토리지 배열이 업데이트된 경우

데이터 웨어하우스 문제 해결 보기의 주석 통합 보기에는 사용 가능한 모든 주석 유형과 적용할 수 있는 개체 유형이 포함된 표가 표시됩니다.

이 작업에 대해

주석 값의 통합은 주석 유형 값을 기반으로 합니다. 스토리지 배열은 각각 다른 커넥터에서 오는 두 개의 서로 다른 계층 값을 가질 수 있습니다. 따라서 한 커넥터에 gold라는 이름으로 정의된 계층이 있고 두 번째 커넥터에 goldy라는 이름으로 계층이 정의되어 있는 경우 이 정보는 데이터 웨어하우스에 두 개의 개별 계층으로 표시됩니다.

일부 주석 유형에서는 동일한 개체에 여러 주석 값을 할당할 수 있으므로 데이터 웨어하우스는 개체(예: ""호스트"")에 여러 개의 주석 값을 할당할 수 있습니다(예: ""데이터 센터 1"" 및 ""데이터 센터 2""를 같은 호스트에 할당할 수 있음).

볼륨의 계층 주석은 일반 주석 테이블과 약간 다르게 작동합니다. 환경에 매우 많은 양의 볼륨이 있을 수 있으며 데이터 웨어하우스에 모든 볼륨을 표시하면 정보의 사용성에 영향을 줄 수 있습니다. 따라서 Annotations Consolidation(주석 통합) 보기에는 여러 계층 값이 할당된 볼륨과 이러한 각 볼륨이 포함된 스토리지만 표시됩니다.

단계

1. 에서 데이터 웨어하우스 포털에 로그인합니다 <https://hostname/dwh>, 위치 hostname OnCommand Insight 데이터 웨어하우스가 설치된 시스템의 이름입니다.
2. 왼쪽의 탐색 창에서 * 문제 해결 * 을 클릭합니다.
3. 주석 통합 * 섹션의 개체 행에서 * 표시 * 를 클릭합니다.

다음은 Data_Center에 대한 주석의 예입니다.

Troubleshooting Annotations Consolidation

Annotation Type: Data_Center

Object Type: Host

Host GUID	Host Name	Host Natural Key	Data_Center Value	Connector
305	AI_Host1	192.1.168.88	New York	localhost (1)
306	AI_Host2	192.1.168.89	New York	localhost (1)
307	AI_Host3	192.1.168.90	New York	localhost (1)

보고

OnCommand Insight 보고를 시작합니다

OnCommand Insight 보고 기능은 미리 정의된 보고서를 보거나 사용자 지정 보고서를 만들 수 있는 비즈니스 인텔리전스 도구입니다. OnCommand Insight 보고는 DWH(데이터 웨어하우스) 데이터에서 보고서를 생성합니다.

OnCommand Insight 보고를 사용하면 다음 작업을 수행할 수 있습니다.

- 미리 정의된 보고서를 실행합니다
- 사용자 지정 보고서를 만듭니다
- 보고서 형식 및 전달 방법을 사용자 지정합니다
- 보고서가 자동으로 실행되도록 예약합니다
- 이메일 보고서
- 색상을 사용하여 데이터의 임계값을 표시합니다

미리 정의된 보고서는 표준 OnCommand Insight 보고서입니다. 이 가이드에서는 모든 제품 라이선스와 함께 사용할 수 있는 미리 정의된 보고서에 대해 설명합니다.

OnCommand Insight 보고 포털 액세스

웹 브라우저, 데이터 웨어하우스 또는 Insight 서버에서 직접 OnCommand Insight 보고 포털에 액세스할 수 있습니다. 보고 포털을 사용하여 미리 정의된 보고서에 액세스하거나 데이터 웨어하우스 데이터를 사용하여 고유한 보고서를 만들 수 있습니다.

웹 브라우저에서 보고 포털에 액세스합니다

단계

1. 웹 브라우저를 엽니다.
2. 다음 URL을 입력합니다. `https://server-name:9300/bi`


9300은 설치 중에 지정된 기본 포트를 나타냅니다. 다른 포트를 지정한 경우 포트를 변경해야 합니다.

3. 사용자 이름과 암호를 입력한 다음 * 확인 * 을 클릭합니다.

Insight 서버에서 보고 포털에 액세스

단계

1. 웹 브라우저를 엽니다.
2. Insight 서버에 액세스하려면 다음 URL을 입력하십시오. `https://server-name`
3. 사용자 이름과 암호를 입력한 다음 * 확인 * 을 클릭합니다.

4. Insight 도구 모음에서 를 클릭합니다 .

5. 나타나는 로그인 페이지에서 사용자 이름과 암호를 입력한 다음 * 확인 * 을 클릭합니다.


데이터 웨어하우스에서 보고 포털에 액세스

단계

1. 웹 브라우저를 엽니다.

2. 데이터 웨어하우스에 액세스하려면 다음 URL을 입력하십시오. `https://server-name/dwh`

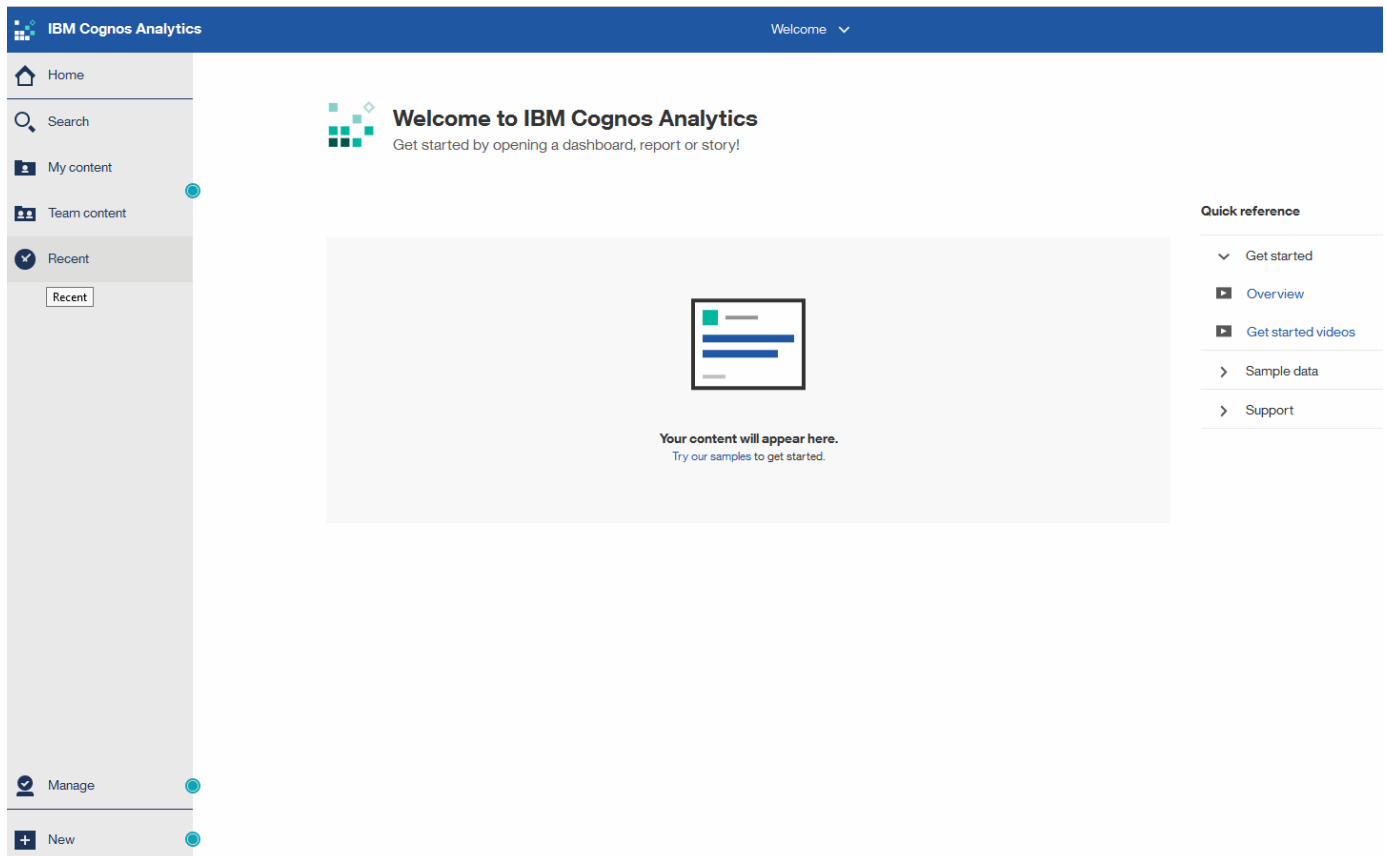
3. 사용자 이름과 암호를 입력한 다음 * 확인 * 을 클릭합니다.

4. 데이터 웨어하우스 도구 모음에서 를 클릭합니다 .

5. 나타나는 로그인 페이지에서 사용자 이름과 암호를 입력한 다음 * 확인 * 을 클릭합니다.

결과

IBM Cognos Analytics 시작 페이지가 표시됩니다. 이 페이지는 OnCommand Insight 보고 포털의 기본 랜딩 페이지입니다.



설치된 라이선스로 인한 변형

OnCommand Insight 보고서의 데이터는 사용자가 구매한 OnCommand Insight 라이선스를 기반으로 합니다. 예를 들어, Plan 라이선스가 없으면 인벤토리 데이터마트에 용량 및 성능을 위한 시점 데이터(오늘)를 얻지만 디바이스의 용량 또는 성능 데이터를 추세 분석(특정 기간 동안 보고)할 수는 없습니다.

플랜 라이선스가 없으면 새 보고서를 만들거나 기존 보고서를 편집할 수 없습니다. OnCommand Insight 시스템에서 사용할 수 있는 보고서와 문서의 그림이 다를 수 있습니다. 이러한 차이는 시스템에 설치된 라이선스와 일러스트레이션을 만드는 데 사용되는 시스템의 라이선스 간의 차이로 인해 발생합니다.

라이선스에 대한 자세한 내용은 OnCommand Insight 설치 가이드를 참조하십시오.

사용자 역할을 보고합니다

각 사용자 계정에는 권한 집합이 있는 역할이 할당됩니다. 사용자 수는 각 역할에 연결된 보고 라이선스 수에 따라 제한됩니다.

각 역할은 다음 작업을 수행할 수 있습니다.

- * 수신자 *

OnCommand Insight 보고 포털 보고서를 보고 언어 및 표준 시간대와 같은 개인 기본 설정을 설정합니다.



받는 사람은 보고서를 만들거나, 보고서를 실행하거나, 보고서를 예약하거나, 보고서를 내보내거나, 관리 작업을 수행할 수 없습니다.

- * 기업 소비자 *

보고서를 실행하고 모든 사용자 옵션을 수행합니다.

- * 비즈니스 저자 *

예약된 보고서를 보고, 대화형으로 보고서를 실행하고, 스토리를 만들고, 모든 비즈니스 소비자 옵션을 수행합니다.

- * 프로 작가 *

모든 Business Author 옵션을 수행할 뿐 아니라 보고서를 만들고 패키지 및 데이터 모듈을 만듭니다.

- * 관리자 *

보고서 정의 가져오기 및 내보내기, 보고서 구성, 데이터 소스 구성, 보고 작업 종료 및 재시작 등의 보고 관리 작업을 수행합니다.

다음 표에는 각 역할에 허용되는 권한 및 최대 사용자 수가 나와 있습니다.

피처	받는 사람	비즈니스 소비자	비즈니스 저자	프로 작가	관리자
팀 콘텐츠 탭에서 보고서를 봅니다	예	예	예	예	예
보고서를 실행합니다	아니요	예	예	예	예
보고서 예약	아니요	예	예	예	예

외부 파일을 업로드합니다	아니요	아니요	예	예	아니요
스토리 만들기	아니요	아니요	예	예	아니요
보고서 작성	아니요	아니요	아니요	예	아니요
패키지 및 데이터 모듈을 생성합니다	아니요	아니요	아니요	예	아니요
관리 작업을 수행합니다	아니요	아니요	아니요	아니요	예
사용자 수	OnCommand Insight 사용자 수입니다	20	2	1	1

새 데이터 웨어하우스 및 보고 사용자를 추가할 때 역할의 제한을 초과하면 해당 사용자는 "비활성화"로 추가되며, 새 사용자 멤버십을 부여하려면 해당 역할을 가진 다른 사용자를 비활성화 또는 제거해야 합니다.



보고서 작성 기능을 사용하려면 Insight Plan 라이선스가 필요합니다. ARAP(Additional Report Authoring Package)를 구매하여 비즈니스 작성자 및 Pro Author 사용자를 추가할 수 있습니다. 도움이 필요하면 OnCommand Insight 담당자에게 문의하십시오.

이러한 보고 사용자 역할은 직접 데이터베이스 액세스에 영향을 주지 않습니다. 이러한 보고 사용자 역할은 데이터 마트를 사용하여 SQL 쿼리를 만드는 기능에 영향을 주지 않습니다.

보안 헤더 사용

HTTP 헤더는 Cognos Analytics 웹 애플리케이션의 전반적인 보안을 강화하도록 구성할 수 있습니다.

응답 헤더를 추가하려면

- Cognos Analytics UI에 로그인하고 * 관리 \ → 구성 \ → 시스템 \ → 고급 설정 * 으로 이동합니다
- 다음 키/값을 추가하고 적용합니다.
 - 키: BIHeaderFilter.responseHeaders
 - 값: [{"name": "X-FRAME-OPTIONS", "value": "SAMEORIGIN"}, {"name": "X-XSS-Protection", "value": "1"}, {"name": "X-Content-Type-Options", "value": "nosniff"}]
- 브라우저를 새로 고쳐 머리글을 활성화합니다.

간편한 보고

OnCommand Insight 보고 포털에서 미리 정의된 보고서를 생성하고, 다른 사용자에게 이메일로 보내고, 수정할 수도 있습니다. 여러 보고서를 통해 장치, 사업체 또는 계층별로 필터링할 수 있습니다. 보고 도구는 IBM Cognos를 기반으로 하며 다양한 데이터 표시 옵션을 제공합니다.

- OnCommand Insight의 사전 정의 보고서에는 인벤토리, 스토리지 용량, 비용 청구, 성능, 스토리지 효율성, 클라우드 비용 데이터입니다. 이러한 사전 정의된 보고서를 수정하고 수정 사항을 저장할 수 있습니다.

사용 가능한 보고서 데이터는 다음을 비롯한 여러 가지 사항에 의해 제어됩니다.

- 역할에 따라 정의된 OnCommand Insight 보고 포털에 로그인합니다.
- 보고서에 대한 데이터를 저장하는 OnCommand InsightData Warehouse의 설정입니다.

HTML, PDF, CSV, XML 등 다양한 형식의 보고서를 생성할 수 있습니다. Excel을 클릭합니다.

OnCommand Insight는 사용자를 사업부와 연결할 수 있도록 하여 보고에서 다중 임차를 수용합니다. 이 기능을 사용하면 관리자는 사용자 또는 소속 관계 특성에 따라 데이터나 보고서를 분리할 수 있습니다.



Cognos 버전 11.1.2 이상에서는 보고 URL이 "안정성"으로 간주되지 않으며 변경될 수 있습니다. 보고 URL을 북마크한 경우 이러한 북마크가 나중에 실패할 수 있습니다. 자세한 내용은 다음 웹 사이트를 참조하십시오. <http://queryvision.com/ibm-analytics-11-x-urls-they-are-a-changing/>



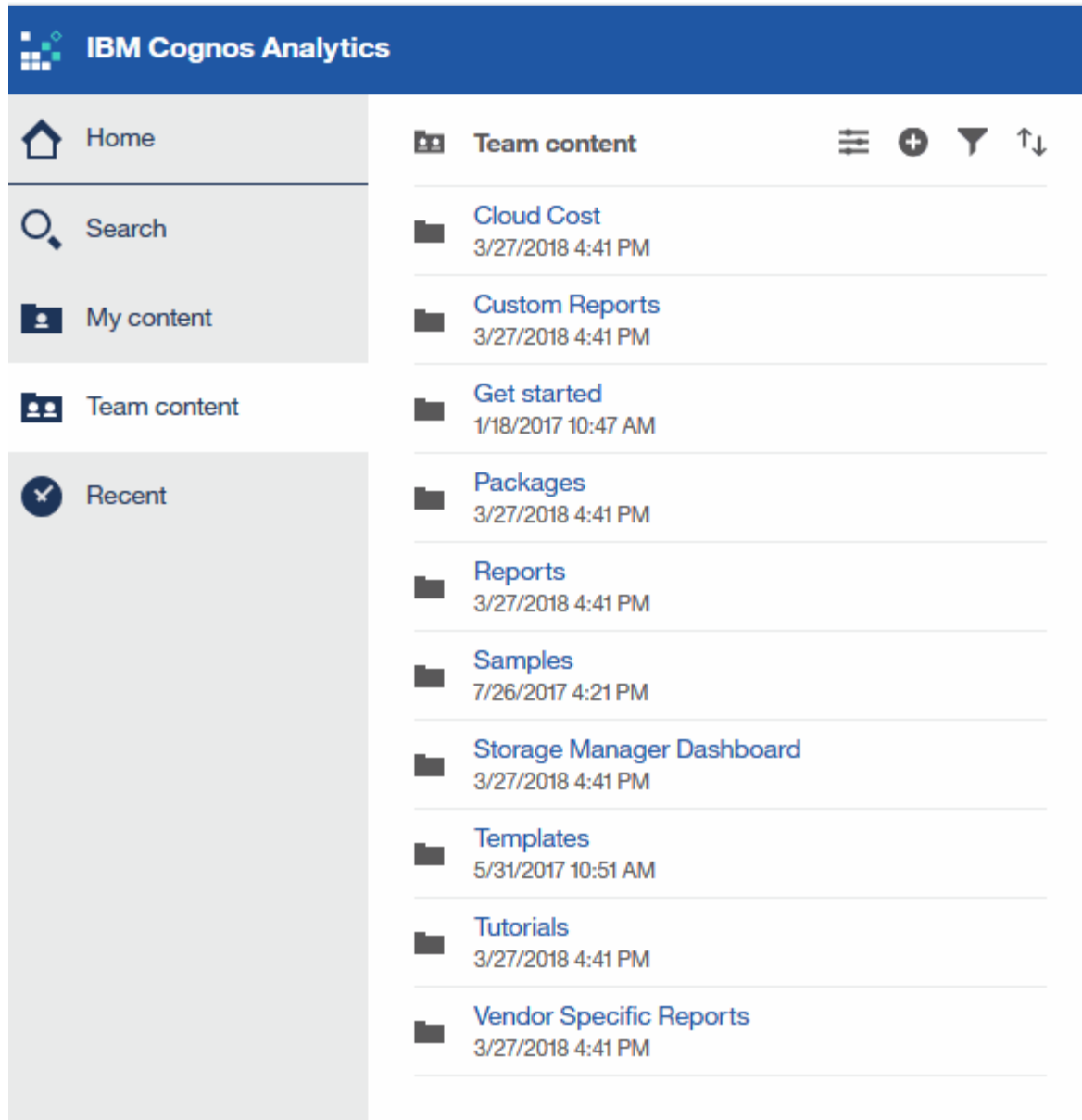
OnCommand Insight는 새로운 데이터 모듈 기능을 사용하지 않는 한 IBM Cognos의 패키지를 사용하여 만든 대시보드를 지원하지 않습니다.

미리 정의된 **OnCommand Insight** 보고서로 이동합니다

보고 포털을 열면 팀 콘텐츠 폴더가 OnCommand Insight 보고서에서 필요한 정보 유형을 선택하는 시작점입니다.

단계

1. 왼쪽 탐색 창에서 * 팀 콘텐츠 * 를 클릭하고 사용할 정보 범주를 선택합니다.



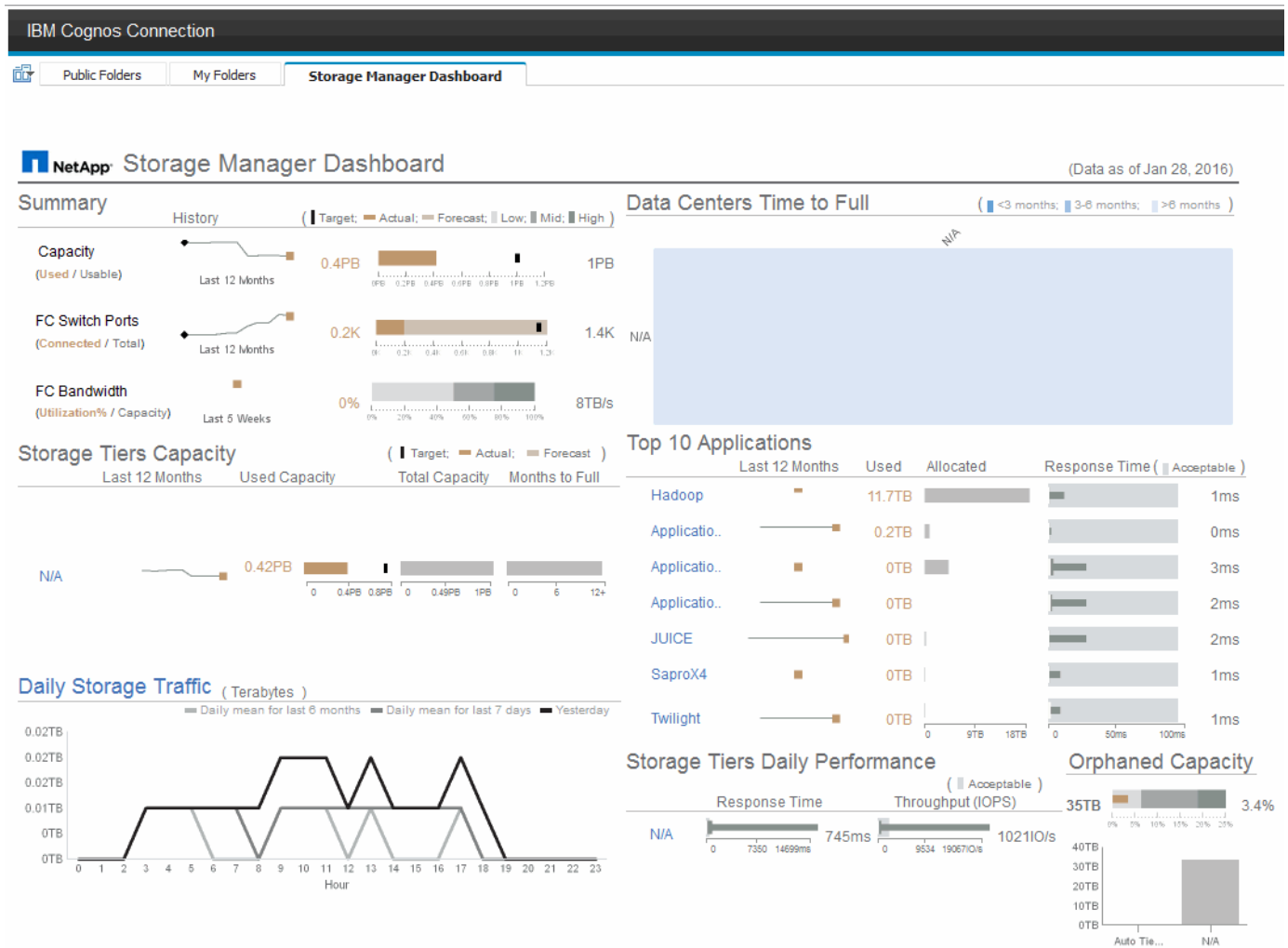
2. 보고서 * 를 클릭하여 미리 정의된 보고서에 액세스합니다.
3. 보고서 작성 방법을 알아보려면 * 시작하기 *, * 샘플 * 또는 * 자습서 * 를 클릭하십시오.

Storage Manager 대시보드를 통해 수행할 수 있는 작업

스토리지 서비스를 매일 관리하는 데 Storage Manager 대시보드를 사용할 수 있습니다.

Storage Manager 대시보드에서는 시간에 따른 리소스 사용을 허용 가능한 범위 및 이전 활동 일수와 비교하고 대조할 수 있는 중앙 집중식 시각화를 제공합니다. 스토리지 서비스의 핵심 성능 메트릭만 표시되어 있으므로 데이터 센터 유지보수 방법을 결정할 수 있습니다.

대시보드에는 스토리지 환경의 특정 측면에 대한 컨텍스트 정보가 포함된 7개의 구성 요소가 포함되어 있습니다. 스토리지 서비스의 측면에 대해 드릴다운하여 가장 관심 있는 섹션에 대한 심층 분석을 수행할 수 있습니다.



이 구성 요소는 사용된 스토리지 용량과 사용 가능한 스토리지 용량, 총 스위치 포트 수 및 연결된 스위치 포트 수, 총 연결 스위치 포트 사용률 대 총 대역폭 및 시간 경과에 따른 각 추세를 보여줍니다. 낮음, 중간 및 높은 범위와 비교하여 실제 사용률을 볼 수 있으므로 목표를 기준으로 Insight 투사 및 원하는 실제 사용량 간에 비교 및 대조할 수 있습니다. 용량 및 스위치 포트의 경우 이 타겟을 구성할 수 있습니다. 예측은 현재 성장률 및 설정한 날짜를 추정하여 계산됩니다. 향후 사용 예상 일자를 기준으로 예측된 사용된 용량이 목표를 초과하면 용량 옆에 경고(빨간색 원 표시)가 나타납니다.

스토리지 계층 용량

이 구성 요소는 사용된 계층 용량과 계층에 할당된 용량을 비교하여 보여 줍니다. 즉, 사용된 용량이 12개월 동안 증가 또는 감소하는 방식과 전체 용량에 남은 기간이 몇 개월인지 나타냅니다. 용량 사용량은 실제 사용량에 대한 값, Insight에서 제공하는 사용량 예측 및 구성할 수 있는 용량 목표와 함께 표시됩니다. 향후 사용 예상 날짜를 기준으로 예측된 사용된 용량이 목표 용량을 초과하면 계층 옆에 경고(빨간색 원 표시)가 표시됩니다.

임의의 계층을 클릭하여 스토리지 풀 용량 및 성능 세부 정보 보고서를 표시할 수 있습니다. 이 보고서에는 선택한 계층의 모든 풀에 대한 사용 가능한 용량과 사용 중인 용량 비교, 전체 일 수, 성능(IOPS 및 응답 시간) 세부 정보가 표시됩니다. 이 보고서에서 스토리지 또는 스토리지 풀 이름을 클릭하여 해당 리소스의 현재 상태를 요약하는 자산 페이지를 표시할 수도 있습니다.

일일 스토리지 트래픽

이 구성 요소는 이전 6개월 동안의 환경 성능, 큰 성장, 변화 또는 잠재적 문제가 있는지 여부를 보여 줍니다. 또한 이전 7일 동안의 평균 트래픽과 이전 날짜의 트래픽을 비교하여 보여 줍니다. 순환(이전 7일) 및 계절별 변동(이전 6개월)을

모두 강조하는 정보를 제공하므로 인프라가 수행 중인 방식을 시각화할 수 있습니다.

제목(* Daily Storage Traffic*)을 클릭하여 스토리지 트래픽 세부 정보 보고서를 표시할 수 있습니다. 이 보고서는 각 스토리지 시스템에 대한 이전 날짜의 시간별 스토리지 트래픽 히트맵을 보여 줍니다. 이 보고서에서 스토리지 이름을 클릭하면 해당 리소스의 현재 상태를 요약하는 자산 페이지가 표시됩니다.

Data Center Time to Full(데이터 센터 전체 시간)

이 구성 요소는 Insight의 예측 성장률을 기준으로 각 스토리지 계층의 각 데이터 센터에 남아 있는 용량과 모든 데이터 센터를 비교하여 보여줍니다. 계층 용량 수준은 파란색으로 표시됩니다. 색이 어두울수록 해당 위치의 계층이 가득 차기 전에 남은 시간이 줄어듭니다.

계층의 섹션을 클릭하여 스토리지 풀 전체 세부 정보에 대한 일 수 보고서를 표시할 수 있습니다. 이 보고서는 선택한 계층 및 데이터 센터의 모든 풀에 대해 전체 용량, 사용 가능한 용량 및 전체 일 수를 보여 줍니다. 이 보고서에서 스토리지 또는 스토리지 풀 이름을 클릭하면 해당 리소스의 현재 상태를 요약하는 자산 페이지가 표시됩니다.

상위 10개 애플리케이션

이 구성 요소는 사용된 용량을 기준으로 상위 10개 애플리케이션을 보여 줍니다. 계층의 데이터 구성 방식에 관계없이 이 영역에는 현재 사용된 용량과 인프라스트럭처의 공유가 표시됩니다. 지난 7일간 사용자 경험 범위를 시각화하여 소비자가 허용 가능한(또는 더 중요한 것은 수용 불가) 응답 시간을 경험하는지 확인할 수 있습니다.

또한 이 영역에는 애플리케이션이 성능 서비스 수준 목표(SLO)를 충족하는지 여부를 나타내는 트렌드가 표시됩니다. 이전 주의 최소 응답 시간, 첫 번째 사분위, 세 번째 사분위 및 최대 응답 시간을 볼 수 있으며, 구성할 수 있는 허용되는 SLO에 대한 중간값이 표시됩니다. 모든 애플리케이션의 중간 응답 시간이 허용 가능한 SLO 범위를 벗어나면 애플리케이션 옆에 경고(빨간색 원 커짐)가 표시됩니다. 응용 프로그램을 클릭하여 해당 자원의 현재 상태를 요약하는 자산 페이지를 표시할 수 있습니다.

스토리지 계층 일별 성능

이 구성 요소는 이전 7일 동안의 응답 시간 및 IOPS에 대한 계층의 성능을 요약한 것입니다. 이 성능은 구성할 수 있는 SLO와 비교되며, 이를 통해 계층을 통합하거나, 해당 계층에서 제공되는 워크로드를 재정렬하거나, 특정 계층의 문제를 식별할 수 있습니다. 중간 응답 시간 또는 중간 IOPS가 허용 가능한 SLO 범위를 벗어나면 계층 옆에 경고(빨간색 원 유지)가 표시됩니다.

계층 이름을 클릭하여 스토리지 풀 용량 및 성능 세부 정보 보고서를 표시할 수 있습니다. 이 보고서에는 선택한 계층의 모든 풀에 대한 사용 가능한 용량과 사용 중인 용량, 전체 일 수, 성능(IOPS 및 응답 시간) 세부 정보가 표시됩니다. 이 보고서에서 스토리지 또는 스토리지 풀을 클릭하면 해당 리소스의 현재 상태를 요약하는 자산 페이지가 표시됩니다.

고립된 용량

이 구성 요소는 계층별로 분리된 총 용량과 분리된 용량을 비교하여 총 가용 용량에 대한 허용 범위를 비교하여 분리된 실제 용량을 보여줍니다. 고립된 용량은 구성과 성능에 의해 정의됩니다. _CONFIGURATION_에 의해 고립된 스토리지는 호스트에 스토리지가 할당된 상황을 설명합니다. 그러나 구성이 제대로 수행되지 않아 호스트가 스토리지를 액세스할 수 없습니다. _성능이 고립되면_은(는) 호스트가 액세스할 수 있도록 스토리지가 올바르게 구성된 상태입니다. 하지만 스토리지 트래픽이 없습니다.

가로 누적 막대는 허용 가능한 범위를 표시합니다. 회색이 어두울수록 상황은 더 수용할 수 없습니다. 실제 상황은 분리된 실제 용량을 보여 주는 좁은 청동 막대로 표시됩니다.

계층을 클릭하여 선택한 계층의 구성 및 성능에 의해 분리된 것으로 식별된 모든 볼륨을 표시하는 분리된 스토리지 세부 정보 보고서를 표시할 수 있습니다. 이 보고서에서 스토리지, 스토리지 풀 또는 볼륨을 클릭하면 해당 리소스의 현재 상태를 요약하는 자산 페이지가 표시됩니다.

사전 정의된 보고서를 사용하여 일반적인 질문에 답합니다

OnCommand Insight에는 수많은 일반 보고 요구사항을 해결하는 사전 정의된 보고서가 포함되어 있으며, 이를 통해 이해 관계자가 스토리지 인프라에 대해 정확한 정보를 기반으로 의사결정을 내리는 데 필요한 중요한 통찰력을 얻을 수 있습니다.

다음 미리 정의된 보고서는 * 팀 콘텐츠 * > * 보고서 * 또는 * 팀 콘텐츠 * > * 공급업체별 보고서 * 에서 사용할 수 있습니다.

NetApp Storage Automation Store에서 최신 버전의 보고서를 확인할 수 있습니다. Automation Store에서 보고서를 정기적으로 확인해야 합니다.

- * AWS 클라우드 비용 데이터 *

클라우드 비용 보고서는 모든 자산에 대한 통합 뷰를 제공하므로 사용자는 운영 환경에서 동적으로 확장하면서 클라우드 기반뿐 아니라 온프레미스 서비스의 사용량과 비용을 추적, 분석, 최적화할 수 있습니다.

이 보고서는 인프라-비용 상관 관계를 제공하며, 명확하고 실용적인 보고를 통해 집중적인 용량 계획 및 폐기물 감지를 통해 적절한 사이징을 보장합니다.

- * 애플리케이션 서비스 수준 용량 및 성능 *

애플리케이션 서비스 수준 용량 및 성능 보고서는 애플리케이션에 대한 개괄적인 개요를 제공합니다. 이 정보는 용량 계획 또는 마이그레이션 계획에 사용할 수 있습니다.

- * 지불 거절 *

Chargeback 보고서는 호스트, 애플리케이션 및 비즈니스 엔터티별 스토리지 용량 차지백 및 책임 정보, 현재 데이터와 기간별 데이터를 모두 포함합니다.

이중 카운트를 방지하려면 ESX Server를 포함하지 말고 VM만 모니터링하십시오.

이 보고서의 최신 버전은 NetApp 스토리지 자동화 스토어 에서 제공됩니다.

- * 데이터 소스 *

데이터 원본 보고서에는 사이트에 설치된 모든 데이터 원본, 데이터 원본 상태(성공/실패) 및 상태 메시지가 표시됩니다. 이 보고서는 데이터 소스 문제 해결을 시작하는 위치에 대한 정보를 제공합니다. 실패한 데이터 소스는 Insight 보고의 정확성과 제품의 일반적인 사용성에 영향을 미칩니다.

- ESX와 VM 성능 비교 *

ESX와 VM 성능 비교 보고서는 ESX 서버와 VM을 비교하여 ESX 서버와 VM의 평균 및 최대 IOPS, 처리량, 지연 시간 및 사용률을 보여 줍니다. 이중 카운트를 방지하려면 ESX Server를 제외하고 VM만 포함합니다.

이 보고서의 최신 버전은 NetApp 스토리지 자동화 스토어 에서 제공됩니다.

- * 패브릭 요약 *

패브릭 요약 보고서는 포트 수, 펌웨어 버전 및 라이선스 상태를 포함한 스위치 및 스위치 정보를 식별합니다. 이 보고서에는 NPV 스위치 포트가 포함되어 있지 않습니다.

- * 호스트 HBA *

호스트 HBA 보고서는 환경의 호스트에 대한 개요를 제공하고 HBA의 공급업체, 모델 및 펌웨어 버전과 연결된 스위치의 펌웨어 레벨을 제공합니다. 이 보고서는 스위치 또는 HBA에 대한 펌웨어 업그레이드를 계획할 때 펌웨어 호환성을 분석하는 데 사용할 수 있습니다.

- * 호스트 서비스 수준 용량 및 성능 *

호스트 서비스 수준 용량 및 성능 보고서는 블록 전용 애플리케이션의 호스트별 스토리지 활용도에 대한 개요를 제공합니다.

- * 호스트 요약 *

Host Summary 보고서는 선택한 각 호스트의 스토리지 활용도에 대한 개요와 Fibre Channel 및 iSCSI 호스트에 대한 정보를 제공합니다. 보고서를 통해 포트 및 경로, Fibre Channel 및 iSCSI 용량, 위반 횟수를 비교할 수 있습니다.

- * 라이선스 세부 정보 *

라이선스 세부 정보 보고서에는 활성 라이선스가 있는 모든 사이트에서 사용 허가를 받은 정규 리소스 양이 표시됩니다. 또한 활성 라이선스가 있는 모든 사이트에 대한 실제 수량 합서도 표시됩니다. 합에는 여러 서버가 관리하는 스토리지 어레이의 중첩이 포함될 수 있습니다.

- * 매핑되었지만 마스킹되지 않은 볼륨 *

매핑되었지만 마스킹되지 않은 볼륨 보고서에는 특정 호스트에서 사용하도록 LUN(Logical Unit Number)이 매핑되었지만 해당 호스트에 마스킹되지 않은 볼륨이 나열됩니다. 일부 경우에는 마스킹되지 않은 사용 중지된 LUN이 될 수 있습니다. 마스킹되지 않은 볼륨은 모든 호스트에서 액세스할 수 있으므로 데이터 손상에 취약합니다.

- * NetApp 용량 및 성능 *

NetApp 용량 및 성능 보고서는 NetApp 용량에 대한 추세 및 성능 데이터와 함께 할당, 활용 및 커밋된 용량에 대한 글로벌 데이터를 제공합니다.

- OCI 스코어카드 *

OCI 스코어카드 보고서는 OnCommand Insight에서 검색된 모든 자산에 대한 요약 및 일반 상태를 제공합니다. 상태는 녹색, 노란색 및 빨간색 플래그로 표시됩니다.

- 녹색은 정상 상태를 나타냅니다
- 노란색은 환경에 잠재적인 문제가 있음을 나타냅니다
- 빨간색은 주의를 기울여야 하는 문제를 나타냅니다. 보고서의 모든 필드는 보고서와 함께 제공되는 데이터 사전에 설명되어 있습니다.

- * 스토리지 요약 *

스토리지 요약 보고서는 원시, 할당, 스토리지 풀 및 볼륨에 대한 사용 및 미사용 용량 데이터의 전체 요약을 제공합니다. 이 보고서는 검색된 모든 스토리지에 대한 개요를 제공합니다.

이 보고서의 최신 버전은 NetApp 스토리지 자동화 스토어 에서 제공됩니다.

- * VM 용량 및 성능 *

에는 가상 머신(VM) 환경 및 용량 사용량이 나와 있습니다. VM의 전원이 꺼진 경우와 같은 일부 데이터를 보려면 VM 도구를 활성화해야 합니다.

- * VM 경로 *

VM 경로 보고서는 가상 머신이 실행 중인 호스트, 액세스 중인 공유 볼륨, 활성 액세스 경로 및 용량 할당 및 사용량에 대한 데이터 저장소 용량 데이터 및 성능 메트릭을 제공합니다.

- * 씬 풀별 HDS 용량 *

HDS Capacity by Thin Pool 보고서는 씬 프로비저닝된 스토리지 풀에서 사용 가능한 용량을 보여 줍니다.

- * NetApp 애그리게이트 용량 *

NetApp Capacity by Aggregate 보고서는 애그리게이트의 총 물리적 공간, 총 공간, 사용된 공간, 사용 가능한 공간 및 커밋된 공간을 보여줍니다.

- * 일반 스토리지별 Symmetrix 용량 *

Symmetrix Capacity by Thick Array 보고서는 물리적 용량, 가용 용량, 사용 가능한 용량, 매핑된 용량, 마스킹된 용량, 총 사용 가능 용량입니다.

- * 씬 풀별 Symmetrix 용량 *

Symmetrix Capacity by Thin Pool 보고서는 물리적 용량, 가용 용량, 사용된 용량, 사용 가능한 용량, 사용된 비율을 보여 줍니다. 서비스 용량 및 구독 요금입니다.

- * 스토리지별 XIV 용량 *

XIV Capacity by Array 보고서는 스토리지에 사용된 용량과 사용되지 않은 용량을 보여 줍니다.

- * 풀별 XIV 용량 *

XIV Capacity by Pool 보고서는 스토리지 풀에 사용된 용량과 사용되지 않은 용량을 보여 줍니다.


Cognos 11을 사용하여 보고서 만들기

Cognos 11을 사용하여 보고서를 만드는 것은 이전 버전의 Cognos와 다릅니다. 이 절차를 사용하여 미리 정의된 OnCommand Insight 보고서를 사용하여 보고서를 만들 수 있습니다.

이 작업에 대해


다음 단계를 수행하여 여러 데이터 센터에 있는 스토리지 및 스토리지 풀의 물리적 용량에 대한 간단한 보고서를 생성할 수 있습니다.

단계

1. 도구 모음에서  를 클릭합니다
2. 보고서 * 를 클릭합니다
3. 템플릿 * > * 공백 * 을 클릭합니다

4. 테마 * > * 쿨 블루 * > * 확인 * 을 클릭합니다


소스 및 데이터 탭이 표시됩니다

5. 소스 * > * 를 클릭합니다 

6. 파일 열기 대화 상자에서 * 팀 콘텐츠 * > * 패키지 * 를 클릭합니다

사용 가능한 패키지 목록이 표시됩니다.

7. 스토리지 및 스토리지 풀 용량 * > * 열기 * 를 클릭합니다

8. 을 클릭합니다 

보고서에 사용할 수 있는 스타일이 표시됩니다.

9. 목록 * 을 클릭합니다

목록 및 쿼리에 적절한 이름을 추가합니다

10. 확인 * 을 클릭합니다

11. 물리적 용량 * 을 확장합니다

12. 가장 낮은 수준의 * 데이터 센터 * 로 확장합니다

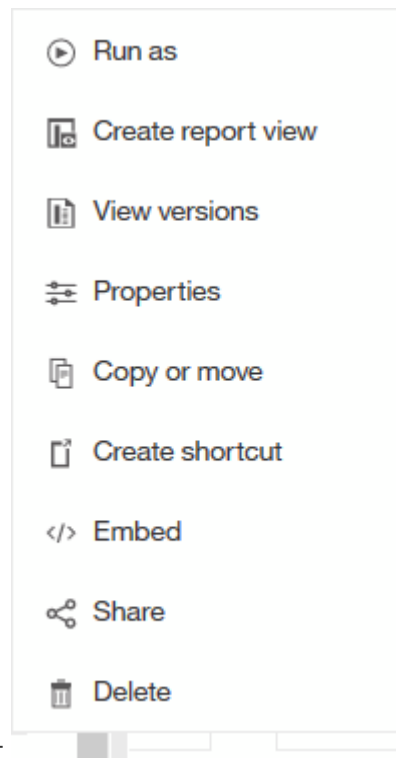
13. 끌기  Data Center 보고 미각을 표시합니다.

14. 용량(MB) * 을 확장합니다

15. 용량(MB) * 을 보고 입천장에 끌어다 놓습니다.

16. Used Capacity(MB) * 를 Reporting palate(보고 구개)로 끌어다 놓습니다.

17.















를 클릭하여 보고서를 실행합니다

출력 유형을 선택합니다.

결과

다음과 유사한 보고서가 생성됩니다.

	Data Center	Capacity (MB)	Used Capacity (MB)
	Asia	122,070,096.00	45,708,105.00
	BLR	100,709,506.00	54,982,204.00
	Boulder	22,883,450.00	12,011,075.00
	DC01	1,707,024,715.00	1,407,609,686.00
	DC02	732,370,688.00	732,370,688.00
	DC03	314,598,162.00	65,448,975.00
	DC04	573,573,884.00	282,645,615.00
	DC05	89,245,458.00	62,145,011.00
	DC06	19,455,433,799.00	11,283,487,744.00
	DC08	100,709,506.00	44,950,171.00
	DC10	112,916,718.00	43,346,818.00
	DC14	23,565,735,054.00	17,357,431,924.00
	DC56	137,549,084.00	10,657,793.00
	Europe	743,942,208.00	240,369,325.00
	HIO	9,823,036,853.00	4,216,750,338.00
	London	0.00	0.00
	N/A	9,049,939,023.00	5,887,911,992.00
	RTP	12,386,326,262.00	5,638,948,477.00
	SAC	9,269,642,330.00	6,197,549,437.00
	 Top  Page up  Page down  Bottom		

보고서 관리

각 보고서에 대해 작업 열에서 * 자세히 * 링크를 선택하고 보고서 속성 설정, 보고서 예약, 보고서 이메일 전송 등의 모든 보고서 작업에 액세스할 수 있습니다. 관리자는 다른 사용자보다 더 많은 관리 옵션을 사용할 수 있습니다.

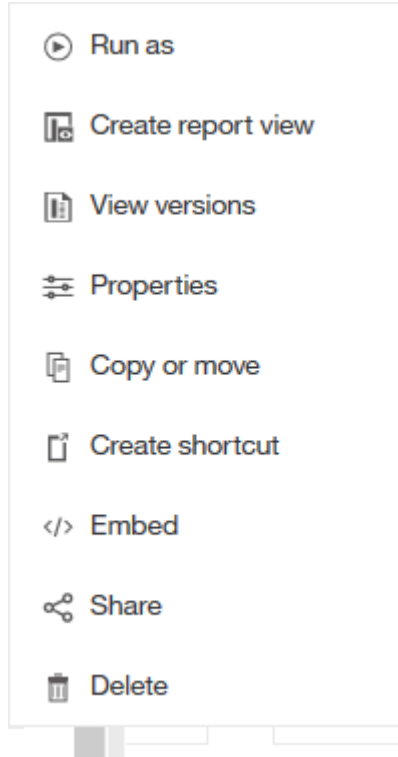
관리자는 OnCommand Insight 역할에 따라 다른 보고서 사용자에게 대한 권한을 설정할 수 있습니다.

보고서의 출력 형식 및 배달 사용자 지정

보고서의 형식 및 전달 방법을 사용자 지정할 수 있습니다.

단계

1. OnCommand Insight 보고 포털을 열고 사용자 정의할 보고서를 선택하고 * [...] * 를 클릭합니다.



2. Properties * > * Schedule * 을 클릭합니다

[< Back](#)
Create schedule

Period

Start

2018-04-06

1:49 PM

End

2018-07-06

1:49 PM

☐ No end date

Run every

1

week(s)

On day(s)

M

T

W

T

F

S

S

☐ Daily time interval

Options

Format

HTML

>

Delivery

Save

>

Prompts

Set values

>

Languages

English (United States)

>

3. 다음 옵션을 설정할 수 있습니다.

- * 보고서를 실행하려는 경우 별표 * 를 사용합니다.
- * 보고서 출력 형식 *.
- * Delivery * 보고서를 인쇄, 저장 또는 이메일로 전송합니다.
- * 언어 * 보고서가 제공되는 언어를 정의합니다.

4. 선택한 항목을 사용하여 보고서를 생성하려면 * Create * 를 클릭합니다.

보고서를 클립보드로 복사합니다

이 프로세스를 사용하여 보고서를 클립보드로 복사합니다.

단계

1. Cognos 11 보고 포털 열기: <https://server-name:9300/bi/>

2. 도구 모음에서  를 클릭합니다
3. 보고서 * 를 클릭합니다
4. 페이지 * 아이콘을 클릭합니다 
- 보고서 * 아이콘  Report 가 표시됩니다
5. Report * 아이콘을 마우스 왼쪽 버튼으로 클릭합니다
- 보고서 옵션이 표시됩니다.
6. 클립보드로 보고서 복사 * 를 클릭합니다.



클립보드에서 보고서(XML)를 엽니다

이전에 클립보드에 복사한 보고서 설정을 열 수 있습니다.

이 작업에 대해

새 보고서를 만들거나 기존 보고서를 열어 보고 사용자 인터페이스를 입력합니다

단계

1. Cognos 11 보고 포털 열기: <https://server-name:9300/bi/>
2. 도구 모음에서  를 클릭합니다
3. 보고서 * 를 클릭합니다
4. 페이지 * 아이콘을 클릭합니다 
- 보고서 * 아이콘  Report 가 표시됩니다
5. Report * 아이콘을 마우스 왼쪽 버튼으로 클릭합니다
- 보고서 옵션이 표시됩니다.
6. 클립보드에서 보고서 열기 * 를 클릭합니다.

사용자 정의 임시 보고서 작성

보고서 작성 도구를 사용하여 사용자 정의 보고서를 만들 수 있습니다. 보고서를 만든 후에는 보고서를 저장하고 정기적으로 실행할 수 있습니다. 보고서 결과는 사용자 자신 및 다른 사람에게 이메일로 자동 전송될 수 있습니다.

이 섹션의 예제는 OnCommand Insight 데이터 모델에 사용할 수 있는 다음 프로세스를 보여 줍니다.

- 보고서로 답할 질문 식별

- 결과를 지원하는 데 필요한 데이터 결정
- 보고서의 데이터 요소 선택

보고서를 디자인하기 전에 수행해야 할 작업

사용자 지정 보고서를 디자인하기 전에 몇 가지 필수 작업을 완료해야 합니다. 이 작업을 완료하지 않으면 보고서가 부정확하거나 불완전할 수 있습니다.

예를 들어, 디바이스 식별 프로세스를 완료하지 않으면 용량 보고서가 정확하지 않게 됩니다. 또는 주식 설정(예: 계층, 사업부 및 데이터 센터)을 완료하지 않으면 사용자 지정 보고서가 도메인 전체의 데이터를 정확하게 보고하지 않을 수 있으며 일부 데이터 요소에 대해 "N/A"가 표시될 수 있습니다.

보고서를 디자인하기 전에 다음 작업을 완료합니다.

- 모든 데이터 소스를 구성합니다. 자세한 내용은 `_OnCommand Insight` 구성 및 관리 가이드를 참조하십시오.
- 사용자 환경의 장치 및 리소스에 대한 주식(예: 계층, 데이터 센터 및 부서)을 입력합니다. OnCommand Insight 데이터 웨어하우스는 기록 정보를 수집하므로 보고서를 생성하기 전에 주석을 안정적으로 확보하는 것이 좋습니다.
- ETL(Extract, Transform, Load) 프로세스에서 OnCommand Insight 서버의 데이터를 허용하도록 OnCommand Insight 데이터 웨어하우스를 구성합니다.

보고서 작성 프로세스

임시 보고서를 만드는 프로세스에는 여러 작업이 포함됩니다.

- 보고서 결과를 계획합니다.
- 결과를 지원하는 데이터를 식별합니다.
- 데이터가 포함된 데이터 모델(예: 차지백 데이터 모델, 재고 데이터 모델 등)을 선택합니다.
- 보고서의 데이터 요소를 선택합니다.
- 보고서 결과의 서식 지정, 정렬 및 필터링 옵션을 선택할 수 있습니다.

사용자 지정 보고서의 결과를 계획하는 방법

보고서 디자인 도구를 열기 전에 보고서에서 원하는 결과를 계획할 수 있습니다. 보고서 작성 도구를 사용하면 보고서를 쉽게 만들 수 있으며 많은 계획을 세울 필요가 없을 수도 있습니다. 그러나 보고서 요청자로부터 보고서 요구 사항에 대한 설명을 받는 것이 좋습니다.

- 답변하려는 정확한 질문을 식별합니다. 예를 들면 다음과 같습니다.
 - 남은 용량은 얼마나 됩니까?
 - 사업부당 차지백 비용은 얼마입니까?
 - 비즈니스 유닛이 적절한 스토리지 계층에 맞춰 정렬되도록 하는 계층별 용량은 얼마입니까?
 - 전력 및 냉각 요구 사항을 어떻게 예측할 수 있습니까? (리소스에 주석을 추가하여 사용자 지정된 메타데이터를 추가합니다.)
- 답변을 지원하는 데 필요한 데이터 요소를 식별합니다.

- 답안에 표시할 데이터 간의 관계를 식별합니다. "용량과 관련된 포트를 보고 싶습니다."와 같은 비논리적 관계를 질문에 포함하지 마십시오.
- 데이터에 필요한 계산을 식별합니다.
- 결과를 제한하는 데 필요한 필터링 유형을 결정합니다.
- 현재 또는 과거 데이터를 사용해야 하는지 확인합니다.
- 보고서에 대한 액세스 권한을 설정하여 데이터를 특정 대상에게 제한해야 하는지 확인합니다.
- 보고서를 배포하는 방법을 식별합니다. 예를 들어, 설정된 일정에 따라 전자 메일로 보내거나 팀 콘텐츠 폴더 영역에 포함되어 있어야 합니까?
- 보고서를 유지 관리할 사람을 결정합니다. 이는 설계의 복잡성에 영향을 줄 수 있습니다.
- 보고서 모형을 만듭니다.

보고서 디자인 팁

보고서를 디자인할 때 몇 가지 팁이 도움이 될 수 있습니다.

- 현재 데이터 또는 기간별 데이터를 사용해야 하는지 여부를 결정합니다.
- 대부분의 보고서는 데이터 웨어하우스에서 사용할 수 있는 최신 데이터만 보고하면 됩니다.
- 데이터 웨어하우스는 용량 및 성능에 대한 기간별 정보를 제공하지만 인벤토리에 대해서는 제공하지 않습니다.
 - 모든 사람이 모든 데이터를 볼 수 있지만 특정 대상에만 데이터를 제한해야 할 수 있습니다.

서로 다른 사용자에 대한 정보를 분할하려면 보고서를 만들고 이에 대한 액세스 권한을 설정할 수 있습니다.

보고 데이터 모델

기업은 OnCommand Insight 데이터 웨어하우스에 검색 및 저장된 데이터를 활용할 수 있습니다. OnCommand Insight 데이터 웨어하우스는 여러 정보 소스의 데이터를 저장하고 효율적인 쿼리 및 분석을 위해 공통 다차원 데이터 모델로 변환하는 중앙 집중식 저장소입니다.

이 저장소에서 다음과 같은 질문에 대답하는 비용 청구, 소비 분석 및 예측 보고서와 같은 사용자 지정 보고서를 생성할 수 있습니다.

- 보유하고 있는 재고는 무엇입니까?
- 내 재고는 어디에 있습니까?
- 누가 우리의 자산을 사용하고 있습니까?
- 비즈니스 유닛에 할당된 스토리지에 대한 비용청구는 무엇입니까?
- 스위치 포트에 얼마나 많은 여유 공간이 있습니까?
- 추가 스토리지 용량을 구입할 때까지 얼마나 걸립니까?
- 사업부가 적절한 스토리지 계층에 맞게 조정됩니까?
- 월, 분기 또는 연도별로 스토리지 할당이 어떻게 변경됩니까?

OnCommand Insight 보고와 함께 제공되는 데이터 모델을 사용하면 보고서 작성 도구를 사용하여 보고서를 디자인하고 예약할 수 있습니다.

데이터 모델 개요

OnCommand Insight는 보고서 개발에 사용할 수 있는 여러 가지 데이터 모델을 제공합니다. 각 데이터 모델은 데이터를 요약하는 집계로서, 쿼리하고 검색할 수 있습니다. 예를 들어 용량 계획에 대한 보고서에서는 용량 데이터 모델을 사용합니다.

OnCommand Insight 엔터프라이즈 보고 데이터 모델은 데이터 요소 간의 데이터 요소와 상호 관계를 제공하여 데이터를 비즈니스 뷰로 볼 수 있도록 합니다. 데이터 요소와 관계를 사용하면 NetApp에서 권장하는 IBM Cognos Analytics 보고서 생성 도구를 사용하여 보고서를 만들 수 있습니다.

또한 OnCommand Insight는 자체 SQL 쿼리를 개발하는 데 사용할 수 있는 데이터 마트를 제공합니다. 이러한 SQL 쿼리 데이터 마트와 보고에 사용되는 데이터 모델 간에는 차이가 있습니다. 개별 OnCommand Insight 보고 데이터 모델은 데이터 마트에 제공된 기본 OnCommand Insight 데이터베이스 스키마를 사용합니다. 그러나 데이터 모델은 테이블의 추가 테이블과 때로는 새 요소를 사용합니다. 예를 들어 데이터 모델에는 데이터베이스 스키마 및 데이터 마트의 용량 팩트 테이블을 기반으로 하는 스토리지 용량 데이터 모델에 월별 용량 팩트 테이블이 포함됩니다. 데이터 모델은 데이터베이스 스키마 테이블의 값을 필터링하여 월 정보만 표시합니다.

데이터 마트에 사용되는 데이터베이스 스키마와 데이터 모델 간의 차이에 대한 또 다른 예는 위반 테이블과 위반 유형 열에 있습니다. 데이터 모델은 OnCommand Insight 웹 UI에 표시되는 텍스트와 일치하도록 데이터베이스의 프로그래밍 방식의 명명된 값을 변환합니다.

OnCommand Insight 데이터 모델

OnCommand Insight에는 미리 정의된 보고서를 선택하거나 사용자 지정 보고서를 만들 수 있는 여러 데이터 모델이 포함되어 있습니다.

각 데이터 모델에는 간단한 데이터 마트와 고급 데이터 마트가 포함되어 있습니다.

- Simple Data Mart는 가장 일반적으로 사용되는 데이터 요소에 빠르게 액세스할 수 있도록 하며 데이터 웨어하우스 데이터의 마지막 스냅샷만 포함하고 기록 데이터는 포함하지 않습니다.
- Advanced Data Mart는 Simple Data Mart에서 사용할 수 있는 모든 값과 세부 정보를 제공하며 기록 데이터 값에 대한 액세스를 포함합니다.
- * 용량 데이터 모델 *

스토리지 용량, 파일 시스템 활용률, 내부 볼륨 용량, 포트 용량, qtree 용량, 가상 머신(VM) 용량을 제공합니다. 용량 데이터 모델은 여러 용량 데이터 모델의 컨테이너입니다. 이 데이터 모델을 사용하여 다양한 유형의 질문에 대한 답변을 작성할 수 있습니다.

◦ * 스토리지 및 스토리지 풀 용량 데이터 모델 *

스토리지 및 스토리지 풀을 비롯하여 스토리지 용량 리소스 계획에 대한 질문에 답변하고 물리적 및 가상 스토리지 풀 데이터를 모두 포함할 수 있습니다. 이 간단한 데이터 모델을 통해 설치 현장의 용량 및 시간에 따른 계층 및 데이터 센터별 스토리지 풀의 용량 사용과 관련된 질문에 답할 수 있습니다.

용량 보고를 처음 사용하는 경우, 이 데이터 모델은 단순한 타겟 데이터 모델이기 때문에 먼저 시작해야 합니다. 이 데이터 모델을 사용하여 다음과 유사한 질문에 답할 수 있습니다.

- 물리적 스토리지의 용량 임계값 80%에 도달할 것으로 예상되는 날짜는 언제입니까?

- 특정 계층의 스토리지에 있는 물리적 스토리지 용량은 얼마입니까?
- 데이터 센터뿐 아니라 제조업체 및 제품군별 스토리지 용량은 얼마나 됩니까?
- 모든 계층의 스토리지 사용률 추세는 무엇입니까?
- 사용률이 가장 높은 상위 10개 스토리지 시스템은 무엇입니까?
- 스토리지 풀의 스토리지 활용률 동향은 무엇입니까?
- 이미 할당된 용량은 어느 정도입니까?
- 할당에 사용할 수 있는 용량은 무엇입니까?

◦ * 파일 시스템 활용률 데이터 모델 *

파일 시스템 활용도에 대한 질문에 답할 수 있습니다. 이 데이터 모델을 사용하면 파일 시스템 레벨에서 호스트의 용량 활용도를 파악할 수 있습니다. 관리자는 파일 시스템당 할당 및 사용 용량을 확인하고, 파일 시스템 유형을 결정하고, 파일 시스템 유형별로 추세 통계를 식별할 수 있습니다. 이 데이터 모델을 사용하여 다음 질문에 답할 수 있습니다.

- 파일 시스템의 크기는 얼마입니까?
- 데이터는 어디에 보관되며 로컬 또는 SAN과 같은 액세스 방법은 무엇입니까?
- 파일 시스템 용량에 대한 기간별 동향은 무엇입니까? 그런 다음, 이를 토대로 향후 요구 사항에 대해 무엇을 예상할 수 있습니까?

◦ * 내부 볼륨 용량 데이터 모델 *

시간이 지남에 따라 내부 볼륨 사용 용량, 할당된 용량 및 용량 사용량에 대한 질문에 답할 수 있습니다.

- 활용률이 사전 정의된 임계값보다 높은 내부 볼륨은 무엇입니까?
- 추세에 따라 용량이 부족해질 위험이 있는 내부 볼륨은 무엇입니까?
- 내부 볼륨에서 할당된 용량과 사용된 용량은 어떻게 됩니까?

◦ * 포트 용량 데이터 모델 *

스위치 포트 연결, 포트 상태 및 포트 속도에 대한 질문에 시간 경과에 따른 답변을 얻을 수 있습니다. 새 스위치 구매를 계획하는 데 도움이 되도록 다음과 같은 질문에 답할 수 있습니다.

- 데이터 센터, 스위치 공급업체 및 포트 속도에 따라 리소스(포트) 가용성을 예측하는 포트 소비 예측을 어떻게 작성할 수 있습니까?
- 용량이 부족해 데이터 속도, 데이터 센터, 공급업체, 호스트 및 스토리지 포트 수를 제공하는 포트는 무엇입니까?
- 시간에 따른 스위치 포트 용량 동향은 무엇입니까?
- 포트 속도는 어떻게 됩니까?
- 어떤 유형의 포트 용량이 필요하며 특정 포트 유형 또는 공급업체에서 부족하게 될 조직은 무엇입니까?
- 해당 용량을 구매하여 사용할 수 있는 최적의 시간은 언제입니까?

◦ * Qtree 용량 데이터 모델 *

시간이 지남에 따라 사용된 용량과 할당된 용량 등의 데이터를 사용하여 qtree 사용률을 추세를 파악할 수 있습니다. 사업체, 응용 프로그램, 계층 및 서비스 수준과 같이 다양한 차원에서 정보를 볼 수 있습니다. 이 데이터 모델을 사용하여 다음 질문에 답할 수 있습니다.

- Qtree에서 사용되는 용량과 애플리케이션 또는 비즈니스 엔터티별 설정된 제한 용량은 얼마나 됩니까?
- 용량 계획을 위해 사용되는 용량과 가용 용량의 동향은 무엇입니까?
- 어떤 비즈니스 엔터티가 용량을 가장 많이 사용하고 있습니까?
- 어떤 애플리케이션이 가장 많은 용량을 소비하고 있습니까?

◦ * VM 용량 데이터 모델 *

가상 환경 및 용량 사용을 보고할 수 있습니다. 이 데이터 모델을 사용하면 VM 및 데이터 저장소에 대한 시간 경과에 따른 용량 사용량 변화를 보고할 수 있습니다. 또한 데이터 모델은 썸 프로비저닝 및 가상 머신 차지백 데이터를 제공합니다.

- VM 및 데이터 저장소에 프로비저닝된 용량을 기준으로 용량 비용 청구를 어떻게 결정할 수 있습니까?
- VM에서 사용되지 않는 용량과 사용되지 않는 부분, 분리된 용량 또는 기타 공간 중 어느 것이 있습니까?
- 소비 동향을 기반으로 무엇을 구입해야 합니까?
- 스토리지 썸 프로비저닝 및 중복제거 기술을 사용하여 얻을 수 있는 스토리지 효율성 절감액은 무엇입니까? VM 용량 데이터 모델의 용량은 VMDK(가상 디스크)에서 가져옵니다. 즉, VM 용량 데이터 모델을 사용하는 VM의 프로비저닝된 크기가 해당 가상 디스크의 크기입니다. 이 용량은 OnCommand Insight의 가상 머신 보기에 있는 프로비저닝된 용량과 다르며, 이 보기에는 VM 자체의 프로비저닝된 크기가 표시됩니다.

◦ * 볼륨 용량 데이터 모델 *

사용자 환경에서 볼륨의 모든 측면을 분석하고 공급업체, 모델, 계층, 서비스 수준 및 데이터 센터별로 데이터를 구성할 수 있습니다. 분리된 볼륨, 미사용 볼륨 및 보호 볼륨(복제에 사용됨)과 관련된 용량을 볼 수 있습니다. 또한 다양한 볼륨 기술(iSCSI 또는 FC)을 확인하고 스토리지 가상화 문제에 대해 가상 볼륨을 비가상 볼륨과 비교할 수 있습니다. 이 데이터 모델을 사용하여 다음과 유사한 질문에 답할 수 있습니다.

- 활용률이 사전 정의된 임계값보다 높은 볼륨은 무엇입니까?
- 데이터 센터에서 거의 사용되지 않는 볼륨 용량에 대한 추세가 어떻게 됩니까?
- 가상화 또는 썸 프로비저닝된 데이터 센터 용량은 어느 정도입니까?
- 복제용으로 예약해야 하는 데이터 센터 용량은 얼마나 됩니까?

• * Chargeback 데이터 모델 *

스토리지 리소스(볼륨, 내부 볼륨 및 Qtree)에서 사용된 용량 및 할당된 용량에 대한 질문에 답변할 수 있습니다. 이 데이터 모델은 호스트, 애플리케이션 및 업무 엔티티별로 스토리지 용량 차지백 및 책임 정보 정보를 제공하며 현재 데이터와 기간별 데이터를 모두 포함합니다. 보고서 데이터는 서비스 수준 및 스토리지 계층별로 분류할 수 있습니다.

이 데이터 모델을 사용하여 업무 엔티티가 사용하는 용량을 찾아서 비용청구 보고서를 생성할 수 있습니다. 이 데이터 모델을 사용하면 여러 프로토콜(NAS, SAN, FC 및 iSCSI 포함)에 대한 통합 보고를 생성할 수 있습니다.

◦ 내부 볼륨이 없는 스토리지의 경우 차지백 보고서는 볼륨별 차지백을 표시합니다.

◦ 내부 볼륨이 있는 스토리지의 경우:

- 업무 엔티티가 볼륨에 할당된 경우 비용 청구 보고서는 볼륨별 비용 청구를 표시합니다.
- 비즈니스 엔터티가 볼륨에 할당되지 않고 qtree에 할당된 경우, 차지백 보고서는 qtree에 따른 차지백을 표시합니다.
- 비즈니스 엔터티가 볼륨에 할당되지 않고 Qtree에 할당되지 않은 경우, 비용청구 보고서는 내부 볼륨을

표시합니다.

- 각 내부 볼륨별로 볼륨, qtree 또는 내부 볼륨별로 차지백을 표시할지 여부를 결정하므로 동일한 스토리지 풀에 있는 서로 다른 내부 볼륨에서 차지백을 서로 다른 레벨로 표시할 수 있습니다. 용량 팩트는 기본 시간 간격 후에 삭제됩니다. 자세한 내용은 데이터 웨어하우스 프로세스를 참조하십시오.

Chargeback 데이터 모델을 사용하는 보고서에는 Storage Capacity 데이터 모델을 사용하는 보고서와 다른 값이 표시될 수 있습니다.

- NetApp 스토리지 시스템이 아닌 스토리지 어레이의 경우 두 데이터 모델의 데이터는 동일합니다.
- NetApp 및 Celerra 스토리지 시스템의 경우 Chargeback 데이터 모델은 단일 계층(볼륨, 내부 볼륨 또는 qtree)을 사용하여 요금을 내지만 Storage Capacity 데이터 모델은 여러 계층(볼륨 및 내부 볼륨)을 사용하여 요금을 기준으로 합니다.

• * 재고 데이터 모델 *

호스트, 스토리지 시스템, 스위치, 디스크, 테이프, 디스크 및 기타 리소스 등 인벤토리 리소스에 대한 Qtree, 할당량, 가상 머신 및 서버, 일반 디바이스 인벤토리 데이터 모델에는 복제, FC 경로, iSCSI 경로, NFS 경로 및 위반 사항에 대한 정보를 볼 수 있는 여러 하위 마트가 포함되어 있습니다. 재고 데이터 모델에는 내역 데이터가 포함되어 있지 않습니다. 이 데이터 마트로 대답할 수 있는 질문은 다음과 같습니다.

- 보유하고 있는 자산은 무엇이며 어디에 있습니까?
- 누가 자산을 사용하고 있습니까?
- 어떤 유형의 장치가 있고 이러한 장치의 구성 요소는 무엇입니까?
- OS당 호스트 수와 해당 호스트에 몇 개의 포트가 있습니까?
- 각 데이터 센터에 공급업체당 어떤 스토리지 어레이가 있습니까?
- 각 데이터 센터에 공급업체 당 몇 개의 스위치가 있습니까?
- 라이선스가 부여되지 않은 포트 수는 몇 개입니까?
- 어떤 공급업체 테이프를 사용하고 있으며 각 테이프에는 몇 개의 포트가 있습니까?
- 보고서 작업을 시작하기 전에 모든 일반 장치가 식별되었습니까?
- 호스트와 스토리지 볼륨 또는 테이프 사이의 경로는 무엇입니까?
- 일반 디바이스와 스토리지 볼륨 또는 테이프 간의 경로는 무엇입니까?
- 데이터 센터당 각 유형 위반은 몇 개입니까?
- 복제된 각 볼륨에 대해 소스 볼륨과 타겟 볼륨은 무엇입니까?
- Fibre Channel 호스트 HBA와 스위치 간에 펌웨어 비호환성 또는 포트 속도가 일치하지 있습니까?

• * 성능 데이터 모델 *

볼륨, 애플리케이션 볼륨, 내부 볼륨, 스위치, 애플리케이션 및 성능에 대한 질문에 VM, VMDK, ESX 대 VM, 호스트 및 애플리케이션 노드 이 데이터 모델을 사용하면 다음과 같은 여러 유형의 성과 관리 질문에 대한 답변을 제공하는 보고서를 작성할 수 있습니다.

- 특정 기간 동안 사용 또는 액세스하지 않은 볼륨 또는 내부 볼륨은 무엇입니까?
- 애플리케이션에 대한 스토리지의 구성 오류를 찾아낼 수 있습니까(미사용)?
- 애플리케이션의 전반적인 액세스 동작 패턴은 무엇이었습니까?
- 특정 애플리케이션에 대해 계층형 볼륨이 적절하게 할당됩니까?

- 애플리케이션 성능에 영향을 주지 않고 현재 실행 중인 애플리케이션에 더 저렴한 스토리지를 사용할 수 있습니까?
- 현재 구성된 스토리지에 더 많은 액세스를 생성하는 애플리케이션은 무엇입니까? 스위치 성능 표를 사용할 때 다음 정보를 얻을 수 있습니다.
- 연결된 포트를 통한 호스트 트래픽의 균형이 조정됩니까?
- 많은 오류가 발생하는 스위치 또는 포트는 무엇입니까?
- 포트 성능에 따라 가장 많이 사용되는 스위치는 무엇입니까?
- 포트 성능에 따라 활용도가 낮은 스위치는 무엇입니까?
- 포트 성능을 기반으로 하는 호스트 추세 처리량은 얼마입니까?
- 지정된 호스트, 스토리지 시스템, 테이프 또는 스위치 하나에 대한 마지막 X일 동안의 성능 사용률은 어떻습니까?
- 특정 스위치에서 트래픽을 생성하는 장치(예: 활용도가 높은 스위치를 사용하는 장치)는 무엇입니까?
- 우리 환경에서 특정 사업부의 처리량은 어떻습니까? 디스크 성능 테이블을 사용할 때 다음 정보를 얻을 수 있습니다.
- 디스크 성능 데이터를 기반으로 지정된 스토리지 풀의 처리량은 얼마입니까?
- 가장 많이 사용되는 스토리지 풀은 무엇입니까?
- 특정 스토리지의 평균 디스크 사용률은 어떻습니까?
- 디스크 성능 데이터를 기반으로 스토리지 시스템 또는 스토리지 풀을 사용하는 추세가 어떻게 됩니까?
- 특정 스토리지 풀에 대한 디스크 사용 동향은 무엇입니까? VM 및 VMDK 성능 표를 사용하는 경우 다음 정보를 얻을 수 있습니다.
- 가상 환경이 최적의 성능을 발휘하고 있습니까?
- 가장 높은 워크로드를 보고하는 VMDK는 무엇입니까?
- 다른 데이터 저장소에 매핑된 VMD에서 보고된 성능을 사용하여 재계산에 대한 결정을 내리는 방법 성능 데이터 모델에는 계층의 적절성, 애플리케이션의 스토리지 구성 오류, 볼륨 및 내부 볼륨의 마지막 액세스 시간을 결정하는 데 도움이 되는 정보가 포함되어 있습니다. 이 데이터 모델은 응답 시간, IOPS, 처리량, 보류 중인 쓰기 수 및 액세스 상태와 같은 데이터를 제공합니다.

• * 스토리지 효율성 데이터 모델 *

시간의 경과에 따른 스토리지 효율성 점수 및 잠재 가치를 추적할 수 있습니다. 이 데이터 모델은 프로비저닝된 용량뿐만 아니라 사용 또는 사용된 용량(물리적 측정)의 측정치도 저장합니다. 예를 들어, 씬 프로비저닝이 설정된 경우 OnCommand Insight는 디바이스에서 얼마나 많은 용량을 가져가는지를 나타냅니다. 또한 이 모델을 사용하여 중복제거가 활성화되어 있는 경우의 효율성을 확인할 수 있습니다. Storage Efficiency Data Mart:

- 씬 프로비저닝 및 중복제거 기술 구현 시 NetApp의 스토리지 효율성이 어떻게 절감됩니까?
- 데이터 센터 전체에서 스토리지 비용이 얼마나 절감됩니까?
- 과거 용량 추세를 기준으로 추가 스토리지를 언제 구입해야 합니까?
- 씬 프로비저닝 및 중복 제거와 같은 기술을 사용할 경우 얻게 되는 용량 이득은 무엇입니까?
- 스토리지 용량과 관련하여 현재 제가 위험에 노출되어 있습니까?

각 데이터 모델에는 팩트 테이블과 차원 테이블이 모두 포함됩니다.

- 팩트 테이블: 수량, 원시 용량 및 가용 용량과 같이 측정된 데이터를 포함합니다. 테이블에 대한 외래 키를 포함합니다.
- 차원 테이블: 데이터 센터 및 사업부 등의 팩트에 대한 설명 정보를 포함합니다. 차원은 데이터를 범주화하는 계층 구조로 구성되는 구조입니다. 차원 특성은 차원 값을 설명하는 데 도움이 됩니다.

보고서에서 열로 표시되는 여러 차원 속성 또는 여러 차원 속성을 사용하면 데이터 모델에 설명된 각 차원의 데이터에 액세스하는 보고서를 작성할 수 있습니다.

보고서 작성에 사용된 모든 데이터 요소에 대한 설명은 데이터 용어집을 참조하십시오.

데이터 모델 요소에 사용된 색상

데이터 모델 요소의 색상은 서로 다른 표시를 가집니다.

- 노란색 자산: 측정값을 나타냅니다.
- 노란색이 아닌 자산: 속성을 나타냅니다. 이러한 값은 집계되지 않습니다.

하나의 보고서에서 여러 데이터 모델 사용

일반적으로 보고서당 하나의 데이터 모델을 사용합니다. 그러나 여러 데이터 모델의 데이터를 결합하는 보고서를 작성할 수 있습니다.

여러 데이터 모델의 데이터를 결합하는 보고서를 작성하려면 기반으로 사용할 데이터 모델 중 하나를 선택한 다음 SQL 쿼리를 작성하여 추가 데이터 마트에서 데이터에 액세스합니다. SQL 조인 기능을 사용하여 다른 쿼리의 데이터를 보고서 쓰기에 사용할 수 있는 단일 쿼리로 결합할 수 있습니다.

예를 들어, 각 스토리지 배열의 현재 용량을 원하는 경우 배열에 사용자 지정 주석을 캡처하려는 경우를 가정해 봅니다. 스토리지 용량 데이터 모델을 사용하여 보고서를 생성할 수 있습니다. 현재 용량 및 차원 테이블의 요소를 사용하고 별도의 SQL 쿼리를 추가하여 인벤토리 데이터 모델의 주석 정보에 액세스할 수 있습니다. 마지막으로 저장소 이름 및 연결 조건을 사용하여 재고 저장소 데이터를 저장소 차원 테이블에 연결하여 데이터를 결합할 수 있습니다.

FAQ 를 참조하십시오

일반적인 질문

이 FAQ는 OnCommand Insight에 대한 일반적인 질문과 답변을 제공합니다.

OCI(OnCommand Insight)가 언제 출시되었습니까?

OCI는 10년 이상 능동적 개발을 통해 업계에서 가장 완성도가 높은 인프라 모니터링 제품 중 하나입니다. 이전에는 Onaro 또는 SANscreen로 알려진 SANscreen 이름은 OnCommand 포트폴리오 제품군에 참여할 때 변경되었으며 현재 OnCommand Insight 또는 보다 일반적인 Insight 또는 OCI로 불립니다.

현재 환경에 OCI를 배포하는 데 시간이 얼마나 걸립니까?

OCI는 단순히 소프트웨어를 다운로드하는 것입니다. 소프트웨어는 2개의 전용 가상 서버 또는 물리적 서버에 설치됩니다. 일반적인 설치에는 2시간 이내에 수행할 수 있으며 인벤토리, 용량 및 성능 데이터는 거의 즉시 제공됩니다. 추가적인 성능 및 모범 사례 정책, 사용자 주석 및 비용 인식 설정은 추가적인 계획 논의를 필요로 합니다.

OCI에 에이전트, 수집기 또는 프로브가 필요합니까?

OCI는 100% 에이전트가 없기 때문에 에이전트, 탭 또는 프로브를 사용할 필요가 없습니다. 모든 장치 검색은 읽기 전용이며 대역외 및 IP를 통해 수행됩니다.

OCI는 어떻게 장치를 검색하고 연결합니까?

OCI는 에이전트나 프로브 없이 데이터 센터 환경에 이미 존재하는 기본 API 및 프로토콜을 활용합니다. SSH, HTTP, SMIS 및 CLI는 몇 가지 예에 불과합니다. 디바이스 요소 관리자가 이미 존재하는 경우(예: EMC의 Unisphere), OCI는 요소 관리자와 통신하여 기존 환경 데이터를 캡처합니다. 대부분의 장치 검색 시 IP 주소와 읽기 전용 사용자 이름 및 암호만 필요합니다. 이러한 디바이스 발견은 OCI의 VMware 데이터 소스와 같이 "일대다"일 수 있습니다. VMware vCenter를 검색하면 하나의 IP 주소 및 자격 증명을 통해 모든 ESXi 호스트와 관련 VM을 검색할 수 있습니다.

OCI에 프로페셔널 서비스가 필요합니까? 그러한 서비스를 이용할 수 있습니까? 그리고 어떤 서비스를 제공합니까?

중간 규모의 환경에서는 배포, 구성 및 통합뿐만 아니라 다양한 사용자 지정 보고 및 데이터 유효성 검사 기능을 위한 프로페셔널 서비스를 권장합니다. OCI 팀 및 어카운트 계약 관리자와의 짧은 논의를 통해 귀사에 가장 큰 도움이 될 서비스를 파악할 수 있습니다.

새로운 기능 및 개선을 위해 OCI 릴리스를 얼마나 자주 업데이트합니까?

여러 버전의 OCI에 대한 제품 업데이트 및 서비스 팩을 사용할 수 있습니다. 주요 릴리스 또는 부 릴리스는 일반적으로 몇 개월마다 제공되며, 새 장치 지원 및 펌웨어를 더 자주 릴리스하는 서비스 팩을 포함합니다. 두 가지 모두 support.netapp.com 다운로드 사이트에서 다운로드할 수 있습니다. 제조업체로부터 더 자주 나오는 새로운 디스크 모델과 같은 특정 업데이트는 자동으로 OCI 소프트웨어로 푸시됩니다. 또한 개발 수정 또는 업데이트 직후 사이트에서 OCI 데이터 소스 장치 수집에 패치를 적용할 수 있습니다.

OCI 관리 팀에서 새 데이터 소스 요청에 대해 우선순위를 어떻게 지정합니까?

OCI의 제품 관리 팀은 모든 고객 개선 사항 및 상호 운용성 기능 요청(IFR)을 적극적으로 추적합니다. 각 요청은 실현 가능성에 대해 자세히 평가되고 고객 수요 및 전반적인 전략적 비즈니스 영향에 따라 우선 순위가 지정됩니다. 요청이 수락되면 노력 수준 및 향후 개발 일정을 기준으로 요청 크기가 조정됩니다. OCI 개발 프로세스의 민첩한 특성을 통해 정기적으로 예정된 릴리스 주기 외에 새로운 데이터 소스를 사용할 수 있습니다. NetApp 어카운트 담당자는 고객 문의 및 귀사를 대신하여 새로운 요청을 제출할 수 있도록 지원할 수 있습니다. OCI를 업그레이드할 필요 없이 데이터 소스에 패치를 적용할 수 있습니다.

우리 회사는 리눅스에서 완벽하게 운영된다. OCI는 Linux에서 작동합니까?

예. OCI는 Linux와 Windows의 다양한 기능을 지원합니다. COGNOS(데이터 웨어하우스와 함께 OCI에 사용되는 IBM의 보고 도구)는 Windows에서만 지원되므로 보고에 OCI를 사용하는 경우 Windows 서버에서 보고 도구를 실행해야 합니다. OCI 설치 가이드에는 각 OCI 구성 요소에 대한 서버 요구 사항과 지원되는 운영 체제가 나와 있습니다.

OCI는 인터넷에 연결되지 않은 보안 환경에 적합합니까?

예, OCI는 상위 10개 Fortune 500대 기업에서 사용되고 있으며 오늘날 전 세계 최고의 은행, 의료, 연구 및 정부 기관을 통해 사용되고 있습니다. OCI는 미국 군사용 CAC(Common Access Card)를 지원하며 지리적으로 분산되어 있거나 방화벽으로 둘러싸인 환경을 위한 솔루션을 제공합니다.

OCUM(OnCommand Unified Manager)이 cDOT용 관리 솔루션이라는 말을 계속 듣게 됩니다. 제가 OCI를 사용해야 하는 이유를 이해하는 데 도움을 줄 수 있습니까?

OnCommand Unified Manager는 스토리지 어레이 "장치 관리" 계층에서 운영되며 cDOT(clustered Data ONTAP) 어레이 및 클러스터 인터랙트에 대한 심층 인시던트 및 이벤트 기반 분석을 제공합니다. OCI 7-Mode, clustered Data ONTAP 및 기타 타사 어레이로 구성된 사내 및 전 세계에 분산된 환경에 대한 종합적인 뷰를 제공합니다. VM에서 스펠들에 이르는 엔드 투 엔드 가시성을 통해 용량, 성능 및 비용 모델링에 대한 기간별 추세 파악과 예측을 수행할 수 있으므로 데이터 센터 관리에 대한 사전 예방적 서비스 품질 접근 방식을 적용할 수 있습니다.

Automation Storefront에 언급된 OnCommand Insight 보조 ETL은 무엇입니까?

일부 OnCommand Insight 자동화 Storefront 보고서 다운로드에서 참조되는 "보조 ETL" 요구 사항은 캡처된 데이터의 추가 ETL(Extract, Transform, Load)을 호출하는 데 사용되는 개발된 전문 서비스 구현을 나타냅니다. 이 구현은 OnCommand Insight 데이터 웨어하우스로 모을 수 있습니다.

보조 ETL 프로세스의 주요 목적은 "배치" 데이터를 프리페치하여 복잡한 보고서를 더 빠르게 생성하거나 매일 실행되도록 예약하는 것입니다.

이 보조 ETL은 OnCommand Insight 데이터 웨어하우스 관리 가이드에 자세히 설명되어 있는 권장 "하루에 한 번" ETL에 추가됩니다.

NetApp 프로페셔널 서비스는 기존 OnCommand Insight 보고서 스케줄, 자동화된 백업, 확장성 또는 기타 시스템 성능 활동에 영향을 미치지 않도록 보조 ETL 스크립팅을 구성할 수 있습니다. ETL 스크립팅 또는 데이터 검증 요구사항에 대한 자세한 내용은 NetApp 영업 담당자에게 연락하여 NetApp의 전문 서비스가 어떤 도움을 줄 수 있는지 논의하십시오.

OnCommand Insight 라이선스

OnCommand Insight 라이선스에 대한 일반적인 질문에 대한 답변입니다.

OCI 라이선싱 개요

OCI는 용량별로 라이선스가 부여됩니다. 고객은 사용하려는 각 모듈에 대해 라이선스를 구입해야 합니다.

- Discover * 는 보증, 수행 및 계획을 위한 필수 조건이며 단독으로 제공되지 않습니다. 검색 라이선스가 TB의 관리 용량으로 제공됩니다.
- Assure * 는 관리형 용량을 TB 단위로 라이선싱합니다(FC, NAS, iSCSI, FCoE 등의 모든 스토리지 인프라에 대한 단일 비용 청구 단위).
- Perform * 은 TB의 관리 용량으로 라이선스가 부여됩니다.
- 계획 * 은 TB의 관리 용량으로 라이선스가 부여됩니다.

"매노화된 용량"은 포맷하기 전에 물리 디스크, 가상 디스크 및 테이프의 원시 용량으로 정의됩니다. 이는 Insight가 사내 및 클라우드에서 모두 검색한 모든 스토리지에 적용할 수 있습니다.

대부분의 데이터 소스는 디스크 물리적 용량 2를 기준으로 합니다. 스페어 디스크, 할당되지 않은 디스크 또는 RAID 디스크와 같은 디스크 역할은 고려하지 않습니다.

두 가지 유형의 Insight 라이선스를 사용할 수 있습니다. * 영구 * 및 * 가입 *.

- 영구 라이선스 * 를 사용하면 해당 라이선스 약관에 따라 얻은 소프트웨어의 특정 버전/릴리스를 무기한 사용할 수 있습니다. SSP(소프트웨어 지원 계획)를 구입한 경우 NetApp은 지원 서비스 약관에 따라 업데이트가 제공되는 경우 NetApp Support 사이트를 통해 상용 소프트웨어 업데이트에 대한 액세스를 제공합니다. NetApp 기술 지원 센터에서 제공하는 특별 패치에 액세스할 수도 있습니다.
- 가입 * 은 다음과 같은 권한을 부여하는 소프트웨어의 고정 기간 라이선스입니다.
- 해당 라이선스 약관에 따라 제한된 기간(가장 일반적으로 12개월) 동안만 소프트웨어를 사내에 사용합니다
- 해당 기간 동안 소프트웨어 지원(이전 SSP)을 받습니다
- 유효한 동안 정식 사용자는 최신 상용 버전, 릴리스 또는 업데이트를 사용할 수 있으며 소프트웨어에 대한 지원을 받을 수 있습니다

각 고정 기간(가장 일반적으로 12개월)이 끝나면 추가 고정 기간(가장 일반적으로 12개월)에 대해 라이선스를 갱신할 수 있습니다. 라이선스를 갱신하지 않을 경우 라이선스를 부여받은 회사는 더 이상 소프트웨어를 사용할 권리를 보유하지 않으며 SSP의 혜택을 받을 수 없으며 정식 사용자는 소프트웨어의 모든 사본을 파기해야 합니다.

OCI 라이선스 모듈에 대해 자세히 알아보십시오

OCI는 현재의 데이터 센터 환경 요구사항을 충족하는 4개의 핵심 라이선스 모듈을 가지고 있습니다. 이러한 모듈은 * 검색, 수행, 보증 및 계획 * 입니다. Discover는 기본 모듈이며 다른 모든 모듈 구매에 필요합니다.

Discover * 모듈을 사용하면 OCI가 데이터 센터에서 자산을 찾고 장치 서비스 경로를 동적으로 매핑할 수 있습니다. 용량, 공급업체 정보, 모델, 펌웨어 및 일련 번호와 같은 정보가 제공됩니다.

- Perform * 은 OCI의 성능 수집 모듈입니다. IOPS, 처리량, 지연 시간, CPU 및 메모리 정보를 캡처하고 다른 분석을 제공합니다.
- 보증 * 은 파이버 채널 환경 및 효율성 기술을 지향합니다. 이 솔루션은 파이버 채널 및 iSCSI 환경의 위험을 식별하고 관리하는 데 도움이 됩니다. 또한 마스킹, 매핑 및 조닝 서비스 경로 항목에 대한 식별, 매핑 및 경고, Fabric 이중화, 스위치 홉, 팬아웃 비율 및 씬 프로비저닝과 같은 효율성 Best Practice 정책에 대한 정보를 제공합니다.
- Plan * 은 하이브리드 사내 및 전 세계에 분산된 데이터 센터 환경에서 컴퓨팅, 패브릭 및 다양한 유형의

스토리지(cDOT, 7-Mode, 타사) 전반의 추세를 식별하고 예측하는 기능을 제공합니다. 보존 시간이 길어집니다. 데이터 웨어하우스는 보고서를 작성할 수 있는 기본 제공 인텔리전스로 구성되어 있으며 엔터프라이즈 공유 스토리지 환경에서 메트릭의 이중 카운트를 방지합니다. 제품화된 보고서의 보안을 만들고 예약할 수 있으며 통합 보고서 작성 도구를 사용하여 자신만의 보고서를 만들 수도 있습니다.

구성 및 지원 장치

이 FAQ는 OnCommand Insight 구성 및 지원되는 장치에 대한 일반적인 질문에 대한 답변을 제공합니다.

OCI가 환경을 변경합니까?

아니요 OCI는 사용자 환경에 대한 정보를 수집하는 읽기 전용 툴입니다. OCI는 자산 또는 구성을 변경하지 않습니다.

내 장치에 OCI가 필요한 권한 수준 액세스는 무엇입니까?

장치가 지원하는 대부분의 경우 읽기 전용 액세스만 있으면 됩니다. 읽기 전용 액세스를 허용하지 않으므로 적절한 상승된 권한이 필요한 솔루션이 있습니다.

OCI에서 정보를 얼마나 자주 수집합니까?

OCI는 일반적으로 5분마다 성능 데이터를 수집하고 논리 및 물리적 구조를 30분마다 검색합니다. OCI는 제안된 모범 사례와 확장성에 따라 기본 폴링 간격을 설정하지만 사용자가 이러한 간격을 완전히 제어할 수는 있습니다.

내 환경에 OCI가 어떤 영향을 미칩니까?

OCI의 에이전트리스, 대역 외 및 패시브 IP 통신은 설정, 유지 관리 및 데이터 센터 에코시스템에 대한 영향을 최소화합니다. OCI의 성과 개발 팀은 성능 모니터링 활동에서 데이터 센터의 성능에 미치는 영향을 최소화하기 위해 훌륭한 조치를 취합니다. 일반적인 운영 환경에서는 영향이 거의 없는 것으로 간주되며, 사용률이 높거나 성능이 떨어지는 기술 플랫폼에서는 완화하거나 강화될 수 있습니다. 자세한 내용은 OnCommand Insight 설치 가이드를 참조하십시오.

OCI에 모든 호스트/VM을 나열하려면 어떻게 해야 합니까?

OCI의 위젯 및 쿼리 리스팅 보완 기능을 사용하여 데이터 센터 자산에 대한 인벤토리 스타일 목록을 제공할 수 있습니다. 스피들 아래에 있는 가상 머신 목록과 그 사이에 있는 다양한 구문을 쿼리, 위젯, 대시보드, 데이터 웨어하우스 보고 등에 사용할 수 있으며 RESTful API를 통해 액세스할 수 있습니다.

OCI는 관련된 비 하이퍼바이저 호스트(예: 물리적 서버)에 대해 동일한 유형의 지원을 제공합니까?

VMware와 같은 하이퍼바이저에서는 ESXi 호스트 및 관련 VM(가상 머신)에 대한 자세한 정보를 제공합니다. 물리적 서버의 경우 OCI는 호스트 HBA까지 메트릭을 수집합니다. OCI는 특허 출원 중인 기술을 사용하여 물리적 서버를 검색하는 고유한 방법을 사용합니다. 스토리지 및/또는 스위치가 검색되면 물리적 서버의 호스트 이름이 Fabric 별칭 정보에 포함됩니다. OCI는 이러한 호스트 이름을 선택하고 DNS에 일치시킬 수 있으며 호스트를 OCI에 자동으로 가져오게 됩니다. 이 기술은 수동 입력 업데이트 및 도구 재고 유지 관리의 필요성을 크게 최소화합니다.

OCI는 이기종 환경에서 동일한 장치 메트릭 깊이(패리티)를 제공합니까?

타사 플랫폼 및 공급업체 기술 전반에 걸쳐 표준화, 공통성 및 명명도의 정도가 다양합니다. OCI는 용량 및 성능 정보를 일관된 프레임워크로 정규화하려고 합니다. IOPS, 지연 시간, 물리적 용량 등의 일부 용량 및 성능 메트릭이 디바이스의 카운터로부터 기본적으로 제공됩니다. 카운터가 제공되지 않을 경우, OCI는 값을 요약할 수 있습니다(예: 기본 볼륨의 IOP 또는 용량을 합산하여). 두 값을 모두 사용할 수 없는 경우, OCI는 다양한 계산 알고리즘을 통해 메트릭 값을 도출하려고 시도합니다. OCI는 현재 OCI에서 수집하지 않은 추가 메트릭을 통합할 수 있는 범용 SNMP 통합 기능을 제공합니다.

OCI는 파이버 채널 스위치를 지원합니까?

예. OCI는 스토리지 자산에서 데이터를 수집하는 것 외에도 사용자 환경의 Cisco, Brocade 및 QLogic 스위치에서 인벤토리 및 성능 데이터를 가져옵니다.

전체 인프라의 토폴로지 뷰를 사용할 수 있습니까? OCI에 ""엔드-투-엔드 가시성""이 표시됩니까?

예. OCI는 논리적 및 물리적 구조를 동적으로 검색 및 매핑하여 컴퓨팅, 패브릭, 가상라이저 및 백엔드 스토리지의 대화형 엔드 투 엔드 토폴로지 뷰를 제공합니다. 토폴로지 아이콘을 사용하면 영향을 받는 리소스를 빠르게 탐색할 수 있으며 공유 스토리지 환경에서 워크로드 및 위반 사항을 쉽게 식별할 수 있습니다.

확장성 및 사용 편의성

이 FAQ는 OnCommand Insight 확장과 사용 편의성에 대한 일반적인 질문에 답합니다.

OCI는 어떻게 확장됩니까?

OCI는 상호 운용성과 최소한의 설치 공간으로 얻을 수 있는 자산 수를 기준으로 한 리더입니다. 핵심 요소로서 OCI는 2개의 가상 또는 물리적 서버가 필요합니다. 하나는 모든 데이터 센터 자산을 검색하는 운영 서버용이고, 다른 하나는 장기 내역 보고를 위해 통합된 데이터 웨어하우스에 적합합니다. OCI의 기업 범위에서는 단일 서버 인스턴스에서 수백 개의 어레이, 수만 개의 가상 머신, 100,000개의 파이버 채널 경로 및 10,000개 이상의 파이버 채널 포트를 모두 지원합니다.

OCI 애플리케이션을 관리하는 데 필요한 사람은 몇 명입니까?

OCI는 한 명의 담당자가 관리할 수 있습니다. 하지만 OCI에는 보고, 문제 해결 또는 분석 요구 사항이 각각 다른 역할을 가진 비즈니스 환경 내의 여러 사용자가 사용할 수 있는 기능이 있습니다. 구성 문제를 표시하는 상태 및 알림 메뉴에서 Fabric에 연결된 물리적 호스트의 자동 검색에 이르기까지 톨 유지 보수를 최소화하기 위해 모든 노력을 기울였습니다. 유연한 주석을 통해 모든 유형의 사용자에게 대한 에코시스템 데이터에 비즈니스 컨텍스트를 제공할 수 있습니다. 스토리지, 패브릭 및 가상화 관리자부터 용량 플래너, 비즈니스 분석가 및 경영진에 이르기까지, OCI는 비즈니스 사일로와 기술 전반에 걸쳐 단일 창에서 정보를 공유할 수 있도록 합니다.

OCI는 맞춤형 보고를 지원합니까?

예. OCI는 IBM Cognos 비즈니스 인텔리전스 툴을 통해 보고 기능을 제공하므로, OCI의 데이터 웨어하우스에 수집된 데이터로부터 완전한 맞춤형 보고서를 생성할 수 있습니다.

사용자 지정 보고서를 얼마나 쉽게 만들 수 있습니까?

OCI 보고 기능은 초보자 및 고급 사용자 모두에게 제공됩니다. OCI는 "Dag and Drop" 보고서 작성 및 고급 사용자 또는 전문 서비스 계약을 위한 SQL 쿼리 기반 보고 등 다양한 보고서 작성 기능을 제공합니다. OCI에 내장된 비즈니스 인텔리전스 솔루션(IBM Cognos)은 용량 두 배 증가 같은 일반적인 실수를 방지합니다. 즉시 사용 가능한 보고서, 위젯, 쿼리 및 대시보드를 보완하여 모든 보고 요구 사항에 맞는 서비스를 제공합니다.

또한 고객은 OCI 커뮤니티 스토어에서 제공되는 다운로드 가능한 보고 템플릿을 찾을 수 있습니다.

OCI는 "신호등" 단순성으로 성능 및 가용성을 보여줄 수 있습니까?

예. OCI 데이터 웨어하우스 및 보고 기능을 사용하면 색상 개선 사항(예: 빨강/노랑/녹색 ""조건부 스타일"" 값)이 있는 보고서를 작성할 수 있습니다. 최종 사용자와 전문 서비스 모두 보고서에 컬러 글꼴 또는 배경 생성 기능을 구현할 수 있습니다. OCIS 위젯 라이브러리를 사용하면 비즈니스 관련 성능 메트릭을 대시보드에 표시할 수 있습니다.

성능 문제 해결

이 FAQ는 OnCommand Insight 성능 문제 해결과 관련된 일반적인 질문에 답합니다.

내 환경에서 모든 **greedy** 리소스 목록을 생성하려면 어떻게 해야 합니까?

OCI의 상관관계 분석을 사용하면 지정된 서비스 경로에 대해 과다 사용 및 성능 저하 리소스를 식별할 수 있습니다. 상관 관계 피처의 생성된 분석은 각 개체를 보는 동안 실시간으로 수행됩니다. 제공된 분석을 통해 성능 문제를 해결하고 근본 원인을 파악하는 데 필요한 시간을 크게 줄일 수 있습니다. 정의된 성능 정책에 대해 생성된 위반 사항을 탐색하는 것은 과다 사용 또는 성능 저하 리소스를 검색하는 한 가지 진입 지점입니다. 위젯과 대시보드 모두 최신 쿼리 기능을 사용하여 예상 IOPS(과다 사용), 활용률 또는 지연 시간이 높은 리소스를 필터링, 정렬 및 시각화할 수 있습니다.

OCI는 성능 문제를 진단할 수 있는 장소를 제공할 수 있습니까?

예. OCI의 성능 문제 해결은 여러 가지 방법으로 접근할 수 있습니다. OCI에는 다양한 경고 방법이 있습니다. SNMP, Syslog 및 e-메일 알림이 일반적으로 사용됩니다. e-메일 알림을 통해 사용자는 OCI 내에서 영향을 받는 리소스를 빠르게 클릭하여 시작할 수 있습니다. 전역 검색 창을 사용하면 관리자가 자원 이름을 입력하기만 하면 상황 분석을 시작할 수 있습니다.

OCI의 위반 대시보드를 사용하면 이벤트 수, 기간 및 시간을 기준으로 작업의 우선순위를 지정할 수 있습니다. 다양한 알림 유형의 예로는 지연 시간, IOPS, 활용률, 심각도, 사업부 또는 관련 애플리케이션 등이 있습니다.

관리자는 OCI의 상관관계 분석을 통해 영향을 받는 리소스와 연결된 객체를 비교하고 IOPS, 지연 시간, 활용률, CPU 및 BB 크레딧에 대한 영향을 파악할 수 있습니다.

OCI의 쿼리 기술 및 위젯 대시보드를 사용하면 데이터 센터 내의 문제 영역을 대상으로 하는 체계화된 보기에서 구체적인 내용을 파악할 수 있습니다.

OCI가 7-Mode에서 cDOT로의 마이그레이션을 지원할 수 있습니까?

예, OCI는 기존 워크로드 수요 및 마이그레이션 후 검증에 대한 중요한 이해를 제공합니다. 오늘날 데이터 센터를 현대화하는 OCI의 역할은 변경 관리 시뮬레이션, 마이그레이션 전 최적화 계획 및 적합한 서비스 계층을 정의하는 데 있습니다. OCI는 단 몇 번의 클릭으로 멀티 벤더 환경에서 수천 개의 NFS 공유와 파이버 채널 경로에 걸쳐 비즈니스 영향을 손쉽게 수집 및 상호 연관시킵니다. OCI에서 마이그레이션에서 기술 업데이트까지, 안정적이고 적절한 규모의 마이그레이션을 지원하고 계획되지 않은 서비스 중단을 완화할 수 있는 경로를 제공합니다.

OCI 성능 모니터링은 "실시간"에 어떤 영향을 줍니까?

OCI는 사내 및 하이브리드 클라우드 데이터 센터 관리 모두에서 * 거의 실시간 * 으로 간주됩니다. 데이터 소스 폴링은 더 자주 발생하도록 구성할 수 있지만 대부분의 사용자는 5분 미만의 대부분의 디바이스에 대해 성능 수집 간격을 설정하여 분석 기능을 크게 활용할 수 없습니다. 더 자주 수집하면 관리 중인 개체와 수행된 분석에 불필요한 부담이 될 수 있습니다. 물론 보다 세분화된 수집이 필요한 상황이 있을 수 있으며, 다행히도 OCI는 구성 가능한 장치 인벤토리 및 특정 데이터 센터 환경 요구 사항에 맞는 성능 폴링 간격을 비롯한 완벽한 유연성을 제공합니다.

"합계"가 "읽기" 및 "쓰기"와 다른 이유는 무엇입니까?

경우에 따라 카운터의 `_Total_` 이 해당 카운터의 `_reads_plus_Writes_` 의 합계와 같지 않을 수 있습니다. 이 문제가 발생할 수 있는 경우는 몇 가지가 있습니다.

- **IOPS ***: 스토리지 어레이 또는 기타 자산은 읽기 및 쓰기 외에도 워크로드 데이터 흐름과 관련이 없는 내부 작업을 처리합니다. 이러한 작업을 "시스템", "메타데이터" 또는 "기타" 작업이라고도 하며 스냅샷, 중복 제거 또는 공간 재할당 등의 내부 프로세스에 기인합니다. 이 경우 지정된 자산에 대한 시스템 작업의 양을 찾으려면 `_Total_IOPS`에서 `_Read_and_Write_IOPS`의 합계를 빼십시오. 읽기 및 쓰기 IOPS의 합계는 데이터 흐름과 직접 관련된 총 IOPS입니다.
- **지연 시간 ***: 총 응답 시간이 시간 가중 평균이므로 작업에 대한 총 응답 시간(지연 시간)은 쓰기 응답 시간 `_` 미만으로 보고될 수 있습니다. I/O 워크로드는 종종 쓰기 작업보다 더 많은 읽기 작업으로 구성되며 쓰기 작업은 일반적으로 더 큰 지연 시간을 관찰합니다. 예를 들어, 평균 지연 시간이 5ms인 10개의 읽기 작업과 평균 지연 시간이 10ms인 5개의 쓰기 작업을 수행한 경우 총 가중치 평균 지연 시간은 읽기 지연 시간의 읽기 횟수를 기준으로 계산되며 또한 쓰기 횟수에는 평균 쓰기 지연 시간이 곱되고 총 I/O 작업 수로 나누어집니다(예: $(10 * 5 + 5 * 10) / (10 + 5) = 6.33\text{ms}$).

OCIOCI와 OCUM에서 초과된 공간에 대해 서로 다른 값을 표시하는 이유는 무엇입니까?

OCUM(OnCommand Unified Manager) 개념을 통해 "프로비저닝된" 공간에 FlexVol(OnCommand Insight 내부 볼륨)이 증가할 수 있는 자동 확장 제한이 있을 수 있습니다. OCI "용량"에 자동 확장 제한이 반영되지 않습니다. 따라서 자동 확장 FlexVol이 있는 환경에서 OCUM 프로비저닝 용량은 OCI 스토리지 레벨 "오버 커밋 용량"을 초과할 수 있습니다. 델타는 FlexVol 용량과 자동 용량 간의 차이가 됩니다.

환경 관리

이 FAQ는 OnCommand Insight 환경 관리에 대한 일반적인 질문에 답합니다.

특정 사용자에게 **OCI**에 대한 액세스 권한을 제공하면서 특정 리소스(예: **SVM** 및 관련 볼륨, **VM**, 서버)가 있습니까?

OCI는 역할 기반 액세스를 제공합니다. 예를 들어, 보고서에 대한 액세스는 OCI의 데이터 웨어하우스 보고를 통해 제어됩니다. 보고서를 예약하거나 PDF, HTML 또는 CSV로 e-메일로 보내거나, 파일 공유 또는 사용자가 보기 전에 인증을 받아야 하는 URL로 보낼 수 있습니다. 사용자 기반 액세스는 Admins, Users 및 Guest 형식으로 부여됩니다. Active Directory/LDAP 지원도 사용할 수 있습니다.

Insight를 다른 툴과 통합

이 FAQ에서는 OnCommand Insight와 다른 툴의 통합에 대한 일반적인 질문에 답합니다.

OCI를 다른 톨과 통합할 수 있습니까? 사용 가능한 통합 포인트는 무엇입니까?

예. OCI는 타사 오케스트레이션, 비즈니스 관리, 변경 제어 및 티켓 시스템과 사용자 정의 CMDB 통합을 지원하는 확장 가능한 개방형 솔루션입니다. OCI에서 완전히 게시된 RESTful API와 개방형 MySQL 데이터베이스 기본 통합 지점을 사용하면 데이터를 간단하고 효과적으로 이동할 수 있으며 사용자가 데이터에 원활하게 액세스할 수 있습니다.

Insight의 Swagger 기반 API 설명서는 * (?) 아래 제품에 있습니다. 도움말 > REST API 설명서 *.

Insight BMC Connector란 무엇입니까?

BMC용 OnCommand Insight 커넥터는 DWH(OnCommand Insight 데이터 웨어하우스)와 CMDB(BMC Atrium 구성 관리 데이터베이스)를 통합합니다. Insight Connector for BMC는 네트워크 스토리지 시스템(예: 스토리지 장치, 호스트 스토리지 서비스, VS 스토리지 서비스 및 VM 스토리지 서비스)과 장치(호스트, 스토리지 스위치, 및 테이프)를 BMC CMDB에 구성 항목 및 관계로 가져옵니다. BMC용 OnCommand Insight 커넥터에 대한 자세한 내용은 NetApp Support 사이트에서 확인할 수 있습니다.

OCI가 SCOM 또는 VROL과 작동합니까?

예. OCI는 많은 비즈니스 관리 솔루션을 보완하며 데이터 센터의 스토리지, 컴퓨팅, 하이퍼바이저 및 패브릭 정보에 대한 신뢰할 수 있는 소스로 간주됩니다. OCI 고객은 OCI의 RESTful API 및 확장형 MySQL 데이터베이스를 활용하여 BMC의 Remedy, ServiceNow, SCOM, Vrops, Splunk와 같은 수많은 애플리케이션을 개선하고 몇 가지 이름을 말하십시오. OCI는 거의 모든 기록 소스에서 정보를 가져오거나 캡처된 환경 메트릭을 인기 있는 타사 모니터링, 발견, CMDB 청구 및 오케스트레이션 시스템에 전송하여 통합을 확장합니다.

OCI를 이미 사용하고 있거나 사용을 고려 중인 클라우드 서비스와 함께 사용할 수 있습니까?

예. 기존 사내 환경과 민첩한 하이브리드 클라우드 환경을 모두 관리하는 OCI는 비즈니스 서비스 요구사항에 가장 적합한 비용 효율적인 플랫폼을 결정할 때 가시성을 제공합니다. OCI는 마이그레이션 전/후 분석에 활용될 수 있으며, 클라우드에 적합한 워크로드를 식별하는 데 도움이 됩니다. 적절한 클라우드 서비스를 선택하려면 기간별 용량 추세, 성능 및 비용이 모두 필요합니다. OCI의 I/O 밀도와 기타 메트릭을 활용하는 서비스 설계 워크숍은 환경을 최적화했는지와 클라우드가 적합했는지와 같은 질문에 답변하는 데에도 도움이 됩니다. OCI는 NetApp 프라이빗 스토리지, Cloud ONTAP, Amazon S3, OpenStack KVM을 지원하여 범위를 지속적으로 확장하고 있습니다. OCI는 NetApp 클라우드 관리 캠페인에서 중요한 역할을 계속 수행하며, 특히 용량 계획, 성능, 서비스 품질 및 지불 거절에 대한 가시성이 중요한 영역에서 더욱 그러합니다.

OCI 인시던트 관리 솔루션에서 인시던트를 열 수 있습니까?

예. OCI 위반 이벤트는 SNMP를 통해 트랩 또는 Syslog를 통해 서버로, 그리고 일부는 RESTful API를 통해 트리거되어 전송될 수 있습니다. 제공된 이벤트에 포함된 세부 정보는 여러 타사 사고 관리 및 발견 솔루션에서 해석할 수 있습니다.

부서 또는 부서에 리소스를 할당할 수 있습니까?

예. OCI는 주석이라는 메타데이터 태그 지정 방법을 통합합니다. 사업부, 사업부, 사업 부문, 테넌트 및 프로젝트를 데이터 센터 리소스에 할당하여 자산, 용량 계획, 문제 해결 및 보고에 관한 보다 풍부한 비즈니스 컨텍스트를 제공할 수 있습니다.

OCI는 WFA(Work Flow Automator)와 작동합니까?

OCI와 타사 CMDB, 청구 및 오케스트레이션 기술의 통합 기능은 성공을 위한 핵심 가치이며 WFA도 예외는 아닙니다. NetApp의 프로페셔널 서비스는 현재 WFA 워크플로우 및 OCI와 수많은 성공적인 통합을 수행했습니다. NetApp

Automation Storefront에서 OCI용 WFA 커넥터를 다운로드할 수 있습니다.

성능 데이터에 대한 **OCI** 보존 시간은 얼마입니까?

OCI 서버는 실시간에 가까운 90일 동안의 성능과 현재(시점) 인벤토리(논리적 및 물리적 구조)를 보유합니다.

OCI 성능 폴링 간격은 사용자가 구성할 수 있습니다. 일반적으로 대부분의 공급업체는 스토리지 성능을 5분마다 구성합니다. 성능/인벤토리 데이터는 장기 기록 및 예측 보고를 위해 DWH(OCI 데이터 웨어하우스)로 매일 전송됩니다. DWH는 이 데이터를 요약된 데이터(시간별, 일별, 월별 롤업 데이터)로 변환합니다. 스토리지/컴퓨팅/패브릭 구성/매핑에 대해 모니터링되는 환경 기록과 같이 ""변경""을 추적하는 우리의 능력은 오늘 정의된 제한이 없습니다.

데이터 웨어하우스는 데이터 마트 및 데이터 세분화를 기반으로 기간별 데이터를 보유합니다.

성과 계획 보고서가 있습니까?

예, OCI와 함께 제공된 여러 보고서가 있으며 사용 사례를 기반으로 당사의 프로페셔널 서비스 카탈로그에 여러 보고서가 있습니다. 또한 데이터 웨어하우스 모듈에는 사용자가 자신의 보고서를 만들 수 있는 Cognos 보고서 작성 도구 제품군이 함께 제공됩니다. 또한 NetApp Automation Storefront에서 제공되는 다양한 커뮤니티 생성 보고 템플릿 및 기타 다운로드도 제공됩니다.

Data ONTAP 스토리지 IOPS

이 FAQ는 Data ONTAP 스토리지 시스템에서 IOPS 수치가 도출되는 방식에 대한 일반적인 질문에 답변합니다.

스토리지 **IOPS**가 **Data ONTAP** 스토리지 시스템에서 파생되는 방법

- 스토리지 어레이 레벨 IOPS는 내부 볼륨 IOPS에서 집계됩니다
- 스토리지 노드 레벨 IOPS에는 메타 데이터 OPS가 포함됩니다
- 스토리지 풀 레벨 IOPS는 메타 데이터 OPS를 제외하며 디스크만 측정합니다
- 내부 볼륨 레벨 IOPS에는 읽기 + 쓰기 OPS(작업) + 기타 OPS가 포함됩니다

질문 - 애그리게이트 **IOPS**가 노드 **IOPS**보다 높을 수 있는 경우도 있습니다.

cDOT 8.3.1 이전 노드 IOPS는 프로토콜 IOPS로 구성됩니다. 향상된 주요 기능을 확인하십시오. 이후 이들은 시스템 구성 요소별 메트릭으로 구성됩니다. 여기에는 데이터에 대한 '전용' 요청, 프런트 도어를 통한 요청, snapmirror, 중복 제거 등의 백엔드 작업은 포함되지 않습니다. 반면에 이러한 작업은 디스크 IOPS를 생성하므로 Aggregate IOPS가 발생합니다. 따라서 집계 IOPS가 노드 IOPS보다 높을 수 있습니다.

질문 - 메타 데이터 또는 기타 **OPS**는 어떻게 계산합니까

기타 OPS = 합계 - (읽기 + 쓰기)

사용 방법 가이드

Insight 시작하기

OnCommand Insight가 설치되고 적절하게 라이선스가 부여된 후에는 중요한 데이터를 보여주기 위해 환경 준비를 시작하는 데 필요한 여러 가지 작업이 있습니다.

일반적인 환경에서 수행되는 작업 중 일부는 다음과 같습니다.

1. * 쿼리 및 보고를 위해 준비할 수 있도록 자산에 주석을 작성합니다 *. 유용한 초기 주석에는 일반적으로 데이터 센터, 계층 및 서비스 수준이 포함됩니다.
2. 쿼리 만들기 중요한 데이터를 표시하고 문제 해결에 도움을 줍니다
3. * 자산에 응용 프로그램 * 및 * 비즈니스 엔터티 * 할당
4. 해당 정책에 대한 위반은 * 성능 정책 생성 * 및 * 알림 * 을 통해 확인할 수 있습니다
5. * 사용자 정의 대시보드 생성 * - 필요 또는 사용자 역할에 따라 데이터를 강조 표시합니다

알림 설정

e-메일, SNMP 또는 Syslog를 통해 성능 정책, 글로벌 경로 또는 용량 위반 등의 트리거 이벤트에 대한 알림을 보내도록 Insight를 구성할 수 있습니다. 또한 데이터 소스 오류 또는 획득 장치 오류와 같은 시스템 수준 이벤트에 대한 이메일 알림을 보내도록 Insight를 구성할 수도 있습니다.

다음은 기본 지침입니다. 알림에 대한 자세한 내용은 구성 및 관리 > Insight 구성 및 관리 > Insight 설정 을 참조하십시오.

알림을 위한 이메일 설정

Insight는 성능 정책 위반과 같은 트리거 이벤트에 대한 이메일 알림을 보낼 수 있습니다.

이 작업에 대해

이메일 알림을 구성하려면 다음 기본 단계를 따르십시오.

단계

1. 관리자 * > * 알림 * 을 클릭하고 * 이메일 * 섹션으로 이동합니다.
2. 서버 * 상자에 SMTP 서버의 이름을 입력합니다. 정규화된 도메인 이름 또는 IP 주소를 입력할 수 있습니다.
3. SMTP 사용자 이름 및 (SMTP 서버에 필요한 경우) 암호를 입력합니다.
4. 보낸 사람 e-메일 * 상자에 알림에 보낸 사람으로 식별될 보낸 사람 e-메일 계정을 입력합니다.

이 계정은 조직 내의 유효한 전자 메일 계정이어야 합니다.

5. 전자 메일 서명 * 상자에 보낼 모든 전자 메일에 삽입할 텍스트를 입력합니다.
6. 받는 사람* 상자에서 를 클릭합니다 ➕이메일 주소를 입력하려면 * 확인 * 을 클릭합니다.

7. 저장 * 을 클릭합니다.

이메일 주소를 편집 또는 제거하거나 테스트 이메일을 보내려면 주소를 선택하고 나타나는 해당 버튼을 클릭합니다.

Insight를 구성하여 특정 개인 또는 그룹에 지정된 성능 정책 위반에 대한 이메일 알림을 보낼 수 있습니다. 예를 들어, 클라우드 자산 위반을 한 그룹에 전송하고 물리적 호스트 이벤트를 다른 그룹에 전송할 수 있습니다. 개별 정책 알림을 구성하려면 * 관리 * > * 성능 정책 * 으로 이동합니다.

로깅할 Syslog 설정

Insight는 용량 또는 경로 위반과 성능 경고를 위해 syslog 이벤트를 전송할 수 있습니다.

이 작업에 대해

Insight에서 syslog 알림을 구성하려면 다음 기본 단계를 따르십시오.

단계

1. Admin * > * Notifications * 를 클릭하고 * Syslog * 섹션으로 이동합니다.
2. Syslog 활성화 * 확인란을 선택합니다.
3. 서버 * 필드에 로그 서버의 IP 주소를 입력합니다.
4. Facility * 필드에서 메시지를 로깅하는 프로그램 유형에 해당하는 시설 수준을 선택합니다.
5. 저장 * 을 클릭합니다.

알림에 대한 SNMP 설정

Insight는 위반 또는 데이터 소스 임계값이 초과된 경우 트리거 이벤트에 대해 SNMP 알림을 보낼 수 있습니다.

이 작업에 대해

Insight에서 SNMP를 구성하려면 다음 기본 단계를 따르십시오.

단계

1. Admin * > * Notifications * 를 클릭하고 * SNMP * 섹션으로 이동합니다.
2. Actions * 를 클릭하고 * Add trap source * 를 선택합니다.
3. SNMP 트랩 수신자 추가 * 대화 상자에 SNMP 트랩 메시지를 보낼 * IP * 주소 및 * 포트 * 를 입력합니다. Community String*의 경우 SNMP 트랩 메시지에 ""public""을 사용합니다.
4. 저장 * 을 클릭합니다.

자산 준비:주석 달기

주석을 사용하면 특정 태그 또는 레이블을 선택한 자산에 연결할 수 있으므로 해당 자산을 관리하고 보고하는 데 도움이 됩니다.

이 가이드에서는 쿼리, 필터링, 경고 알림 및 보고에 사용할 수 있는 사용자 환경에 대한 주석을 만들고 사용자 지정하는 방법을 설명합니다.

주석은 사용자 환경의 특정 자산과 관련된 메모 또는 태그입니다. OnCommand Insight에서는 필요에 따라 자산에 대해 구성할 수 있는 여러 주석을 제공하거나 비즈니스 요구 사항에 따라 사용자 정의 주석을 만들 수 있습니다.

다음 예는 일반적으로 새로운 고객 환경에서 먼저 구성되며 추가 작업의 기준으로 사용됩니다. 사용자 고유의 주석 요구 사항은 다를 수 있지만 여기에 설명된 단계를 참조하여 원하는 자산에 필요한 주석을 구성할 수 있습니다.

이 가이드는 다음과 같은 가정을 기반으로 합니다.

- OnCommand Insight 서버가 설치되어 있고 적절한 라이선스가 있습니다.
- 사용 가능한 모든 옵션이 아닌 모범 사례를 살펴보고자 합니다.
- 이러한 내용은 예제일 뿐이며 특정 요구 사항이 다를 수 있다는 점을 이해합니다.

이 안내서에서는 기존 주석을 수정하고 사용자 정의 주석을 만드는 과정을 안내합니다

이 예제 환경에서는 데이터 센터, 계층, 서비스 수준 및 환경에 따라 자산을 나열할 수 있기를 원합니다.

데이터 센터 주석 구성

데이터 센터 주석은 일반적으로 스토리지 배열, 스위치 또는 물리적 호스트 자산을 데이터 센터 위치와 연결하는 데 사용됩니다. 데이터 센터 주석을 사용자 환경의 다른 자산과 연결할 수도 있습니다.

단계:

- 관리 권한이 있는 사용자로 Insight에 로그인합니다.
- Manage * > * Annotations * 를 선택합니다.
- 데이터 센터 * 주석을 선택하고 * 편집 * 아이콘을 클릭합니다.
- 추가 * 를 클릭하고 첫 번째 데이터 센터의 이름과 설명을 주석 목록에 추가합니다.
- 다른 데이터 센터에서도 마찬가지입니다.
- 완료되면 * Save * 를 클릭합니다.

데이터 센터 주석 예:

이름	설명
DC1_SVL	서니베일 건물 1
DC2_SVLb3	SVL Bldg3 KOR
DC3_NY	뉴욕

DC4_런던	런던
...	

Insight에는 사용자가 필요에 맞게 값을 정의하거나 수정할 수 있는 몇 가지 즉시 사용 가능한 주식 유형이 포함되어 있습니다. 이러한 기본 주식 유형은 항상 Insight 웹 UI 및 보고에 사용할 수 있습니다. 새로 생성된 사용자 지정 주식은 Insight 웹 UI에서 볼 수 있지만 보고에 사용할 수 있도록 추가 조치가 필요합니다. 보고서에 사용자 정의 주석을 포함시키는 방법에 대한 자세한 내용은 를 참조하십시오. NetApp 고객 지원 담당자에게 문의하십시오.



일부 사용자는 데이터 센터 주식과 반대로 국가 주석을 사용하여 자산 위치를 설정할 수 있습니다. 그러나 국가 주석은 Insight 데이터 웨어하우스에서 사용자 지정 주식 유형으로 간주되므로 데이터 센터와 동일한 세분화 수준에서 보고 시 표시되지 않을 수 있습니다.

계층 주석을 구성합니다

계층 주석은 비용 회계에 사용할 수 있도록 자산을 각 계층에 연결하는 데 사용됩니다. Insight에는 여러 기본 계층 주석이 함께 제공됩니다. 계층화 명명 규칙에 따라 주석을 수정하거나 필요에 따라 고유한 계층을 생성할 수 있습니다.

계층 주석을 설정할 때 다음 사항을 염두에 두십시오.

- 기가바이트당 비용은
- 계층 1, 2, 3은 디스크 유형에 따라 스토리지 어레이 레벨에서 구성된 기본 계층입니다. 그러나 대부분의 고객은 어레이 내에서 또는 동일한 유형의 어레이 전체에서 여러 디스크 유형을 갖게 됩니다.
- 모범 사례는 디스크 유형 및/또는 디스크 속도를 기준으로 계층 주석을 작성하는 것입니다. 이는 일반적인 계층 방법론이며, 사용자의 요구 사항은 다를 수 있습니다.

단계:

- Tier * 주석을 선택하고 * Edit * 아이콘을 클릭합니다.
- 원하는 경우 * + Add * (추가 *)를 클릭하고 첫 번째 계층의 이름과 설명을 주식 목록에 추가합니다.
- 다른 계층에 대해서도 같은 작업을 수행합니다.
- 완료되면 * Save * 를 클릭합니다.

계층 주식 예:

이름	설명	Gb당 비용
자동 계층	자동 스토리지 계층화 계층	0.5
계층 1 SSD	All-Flash 어레이	0.5
계층 2 SAS	SAS를 참조하십시오	0.25
계층 3 SATA	SATA를 클릭합니다	0.1

...		
-----	--	--

서비스 수준 주석을 구성합니다

Service Level(서비스 수준) 주석은 자산을 해당 서비스 수준과 연결하는 데 사용됩니다.

서비스 수준 주석은 일반적으로 자동 계층화를 사용하는 고객 환경에서만 설정됩니다. Insight 데이터 웨어하우스에서는 계층이 선호됩니다. 그러나 프로비저닝된 비용과 이 비용을 자세히 설명하려면 서비스 수준을 사용하는 것이 가장 좋습니다 고객 비용. 데이터 웨어하우스에 둘 다 있는 경우 서비스 수준이 계층을 대체합니다.

단계:

- 서비스 수준 * 주석을 선택하고 * 편집 * 아이콘을 클릭합니다.
- 추가 * 를 클릭하고 첫 번째 서비스 수준의 이름 및 설명을 주석 목록에 추가합니다.
- 다른 서비스 수준에도 같은 작업을 수행하십시오.
- 완료되면 * Save * 를 클릭합니다.

서비스 수준 주석 예:

이름	설명	Gb당 비용
서비스 수준 1	FC 또는 SAS, 로컬 및 원격 미러와 테이프가 있는 FAS 컨트롤러	0.93
서비스 수준 2	FC 또는 SAS, 로컬 및 원격 미러를 포함하는 FAS 컨트롤러	0.85
서비스 수준 3	SATA 및 로컬 미러가 있는 FAS 컨트롤러	0.48
...		

사용자 정의 환경 주석을 구성합니다

환경 주석은 자산을 각각의 환경 위치와 연계하거나 사용하기 위한 사용자 정의 주석입니다(예: Lab, R&D, Production, 등 환경 주석을 생성하여 이러한 자산에 설정하면 생산 자산과 별도로 실험실 자산을 쉽게 검색, 필터링 및 보고할 수 있습니다.

단계:

- Manage * > * Annotations * 를 선택합니다.
- 페이지 맨 위에 있는 * + 추가 * 버튼을 클릭합니다.
- 이름 * 에 " * 환경 * "을 입력합니다.
- 설명 * 에 " * 자산 환경 유형 * "을 입력합니다.
- Type * 에서 * List * 를 선택합니다. 목록을 만들 수 있는 새 필드가 표시됩니다.

- 지금은 * 즉시 새 자산 추가 * 를 선택하지 않은 상태로 둡니다. 새 환경을 자산에 연결할 때 선택 목록에 추가할 수 있도록 하려면 이 옵션을 선택합니다.
- 첫 번째 환경의 이름과 설명을 입력합니다.
- 다른 환경에 대해서도 * + 추가 * 를 클릭하고 동일한 작업을 수행합니다.
- 완료되면 * Save * 를 클릭합니다.

예제 환경 주식:

이름	설명
랩	랩
개발	개발
운영	운영
...	

자산 찾기:질의

강력한 쿼리를 사용하여 환경에서 자산을 쉽게 찾고 표시할 수 있습니다.

쿼리를 사용하여 자산에 주석을 달니다


이제 초기 주석을 만들었으므로 이러한 주석을 특정 자산과 연결하는 방법을 살펴보겠습니다.

다음 예에서는 이러한 주석을 특정 자산에 적용합니다. 예를 들어 특정 데이터 센터에 있는 모든 스토리지 배열을 나열하는 쿼리를 생성하고 적절한 주석을 사용하여 스토리지 배열을 표시할 수 있습니다. 그런 다음 특정 계층 및 서비스 수준에 속한 자산에 대해서도 동일한 작업을 수행합니다.

데이터 센터 쿼리 및 주석 달기

쿼리를 사용하여 주석을 사용자 환경의 적절한 자산과 연결할 수 있습니다. 이 예제에서는 데이터 센터 주석을 선택한 자산과 연결합니다.

Insight는 데이터 소스를 수집하는 동안 다른 여러 정보 중에서 발견한 각 자산의 이름을 수집합니다. 이 예에서는 Sunnyvale에 상주하는 스토리지에 대해 "SVL_NN_<label>"와 같이 모든 스토리지 어레이가 상주하는 데이터 센터에 따라 이름이 지정되었다고 가정합니다. Insight 쿼리를 사용하면 이러한 자산에 간단하게 주석을 달 수 있습니다.

- 관리 권한이 있는 사용자로 Insight에 로그인합니다
- 쿼리 * > * + 새 쿼리 * 를 선택합니다
- Search for... * 필드를 선택하고 * Storage * 를 선택합니다. 모든 스토리지 배열 목록이 표시됩니다.
- 이름 * 필터 필드에 "VL"을 입력하고  을 클릭합니다 단추를 누릅니다(또는 Enter 키를 누릅니다). 이제 쿼리 결과 목록이 업데이트되어 문자열 "s VL"이 포함된 배열만 표시됩니다.
- 필터링할 때 다음 문자를 단독으로 사용하거나 결합하여 쿼리 페이지의 텍스트 상자에서 검색을 구체화할 수

있습니다.

- 별표를 사용하면 모든 항목을 검색할 수 있습니다. 예를 들어 "'vol * rhel'은 "'vol'로 시작하고 "'rhel'으로 끝나는 에셋을 표시합니다.
- 물음표를 사용하면 특정 수의 문자를 검색할 수 있습니다. 예를 들어, "SVL-PRD??-S12"에 대한 필터링은 SVL-PRD12-S12, SVL-PRD13-S12 등을 표시합니다.
- 또는 연산자를 사용하여 여러 요소를 지정할 수 있습니다. 예를 들어 "'FAS2240 또는 CX600 또는 FAS3270'"은 여러 스토리지 모델을 찾습니다.
- 이 데이터 센터에 연결할 스토리지 어레이를 선택합니다. 원하는 배열을 모두 선택한 후 * Actions(동작) * 버튼을 클릭하고 * Edit annotation(주석 편집) * 을 선택합니다.
- 주석 추가 * 대화 상자에서 * 데이터 센터 * 주석을 선택합니다.
- 원하는 * 값 * 을 선택합니다(예: "DC1_SVL").
- 저장 * 을 클릭합니다.
- 데이터 센터 열이 쿼리 결과 페이지에 표시되지 않으면 * 열 * 버튼을 아래로 내리고 * 데이터 센터 * 를 선택하여 해당 열을 선택합니다.
- 원하는 경우 쿼리 페이지의 오른쪽 위 모서리에 있는 * 저장 * 단추를 클릭하고 고유하고 명시적인 이름을 지정하여 나중에 사용할 수 있도록 쿼리를 저장할 수 있습니다. 예를 들어 "'스토리지 어레이 - SVL 데이터 센터'"를 입력합니다.

'stl' 주석을 다른 자산과 연결하려면 새 쿼리를 만들고 원하는 각 자산 유형에 대해 다음 단계를 수행합니다.

각 데이터 센터의 자산에 대해 이 단계를 반복합니다.

계층 쿼리 및 주석 달기


쿼리를 사용하여 주석을 사용자 환경의 적절한 자산과 연결할 수 있습니다. 여기서는 해당 계층을 적절한 자산과 연결합니다.

이전 버전에서는 계층에 대한 주석을 설정했습니다. 이 예에서는 스토리지 풀에 계층을 연결하고 계층 주석이 다음과 같이 구성되어 있다고 가정합니다.

값	설명	Gb당 비용
계층 1 SSD	All-Flash 어레이	0.5
계층 2 SAS	SAS를 참조하십시오	0.25
계층 3 SATA	SATA를 클릭합니다	0.1

사용자 환경에서 모든 SSD 디스크를 검색하고 "'계층 1 SSD" 주석을 해당 SSD에 연결합니다.

- 관리 권한이 있는 사용자로 Insight에 로그인합니다
- 쿼리 * > * + 새 쿼리 * 를 선택합니다
- Search for... * 필드를 선택하고 * Storage Pool * 을 선택합니다. 모든 스토리지 풀 목록이 표시됩니다.
- 현재 * 이름 * 필드가 도움이 되지 않을 수 있으므로 다른 필드를 사용하겠습니다. More* 드롭다운을 클릭하고 "'가장

적은 성능 디스크 유형'을 선택합니다. 이 필드에는 관심이 있는 디스크 유형이 나열됩니다. 필드에 'SSD'를 입력하고  를 클릭합니다. 단추를 클릭합니다. 쿼리 결과 목록에는 SSD 스토리지 풀만 표시됩니다.

- 자세히 필터링하려면 * 자세히 * 드롭다운을 클릭하고 추가 필드를 선택합니다.
- 이 계층에 연결할 스토리지 풀을 선택합니다. 원하는 모든 스토리지 풀이 선택되면 * Actions * 버튼을 클릭하고 * Edit annotation * 을 선택합니다.
- 주식 추가 * 대화 상자에서 * 계층 * 주석을 선택합니다.
- 목록에서 원하는 * 값 * 을 선택합니다. 이 예에서는 ""계층 1 SSD""를 선택합니다.
- 저장 * 을 클릭합니다.
- 쿼리 결과 페이지에 계층 열이 표시되지 않으면 * 열 * 버튼을 내리고 * 계층 * 을 선택하여 해당 열을 선택합니다. 이제 자산과 관련된 적절한 주석을 볼 수 있습니다.
- 쿼리 페이지의 오른쪽 위 모서리에 있는 * 저장 * 단추를 클릭하고 고유한 이름을 지정하여 쿼리를 저장합니다. 예를 들어, "Storage Pools - Tier 1 SSD".

""계층 1 SSD" 주석을 다른 자산과 연결하려면 새 쿼리를 만들고 원하는 자산 유형에 대해 다음 단계를 수행합니다.

나머지 각 계층의 자산에 대해 이 단계를 반복합니다.

서비스 수준 및 환경 주석

학습한 단계와 개념을 사용하여 적절한 자산에 서비스 수준 및 환경 주석을 추가합니다.

사용자 환경의 적절한 자산에 서비스 수준 및 환경 주석을 추가하려면 위에 설명된 단계를 따라 원하는 자산 및 적절한 서비스 수준 또는 환경 주석을 선택합니다. 동일한 자산에 여러 개의 주석을 연결할 수 있으며, 실제로 이 방법을 사용하면 Insight를 통해 환경을 보다 유연하게 관리할 수 있습니다.

이제 자산에 주석을 다는 쿼리를 만들었으므로 다음과 같은 다양한 방법으로 주석을 사용할 수 있습니다.

- 원하는 자산에 이벤트가 발생할 경우 이를 알리는 성능 정책입니다
- 활동을 모니터링하기 위한 맞춤형 대시보드 및 위젯
- 보고

기업 구조: 업무 엔티티 및 애플리케이션 설정

회사 구조의 요소를 이해하면 자산 사용을 추적하고 비용을 보고하는 데 도움이 됩니다.

회사의 업무 엔티티를 구성합니다

회사 구조의 비즈니스 요소를 이해하면 자산 사용을 추적하고 비용을 보고하는 데 도움이 됩니다. 여기에서 회사 업무 엔티티를 구성합니다.

이 작업에 대해

OnCommand Insight를 사용하면 최대 4개의 세분화 수준을 포함하는 계층 구조에서 비즈니스 엔티티를 정의할 수 있습니다.

- * 테넌트 *

주로 서비스 공급자가 리소스를 고객과 연결하는 데 사용합니다. 회사가 ISP인 경우 고객의 리소스 사용량을 추적하려는 경우 테넌트 레벨이 필요합니다.

• * 제품군(LOB) *

회사 내 사업 부문 또는 제품 라인(예: 데이터 스토리지) 여러 제품 라인에 대한 데이터를 추적해야 하는 경우 계층 구조에서 LOB가 필요합니다.

• * 사업부 *

법률 또는 마케팅과 같은 기존 사업 단위를 나타냅니다. 서로 다른 부서의 데이터를 추적해야 하는 경우 업무 단위가 필요합니다. 이러한 계층 수준은 한 부서가 다른 부서에서 사용하지 않는 리소스를 분리하는 데 유용합니다.

• * 프로젝트 *

용량 비용 청구를 원하는 사업부 내의 특정 프로젝트를 식별하는 데 주로 사용됩니다. 예를 들어, "특허"는 법무 부서의 프로젝트 이름일 수 있으며 "영업 이벤트"는 마케팅 부서의 프로젝트 이름일 수 있습니다. 수준 이름에는 공백이 포함될 수 있습니다.

업무 엔티티 계층 구조의 예는 다음과 같습니다.



모범 사례: 계층 구조에서 전체 업무 엔티티가 하나씩 표시된 각 행이 포함된 테이블을 만듭니다.

테넌트	사업 부문	사업부	프로젝트
NetApp Inc.의 경우	데이터 스토리지	법적 고지	특허
NetApp Inc.의 경우	데이터 스토리지	마케팅	영업 이벤트
해당 없음	해당 없음	안전 및 보안	해당 없음
...			



회사 계층 구조의 디자인에 있는 모든 수준을 사용할 필요는 없습니다. 사용하지 않는 수준에 대해 "N/A"를 선택할 수 있습니다.

Insight에서 사업체 계층을 만들려면 다음을 실행합니다.

단계

1. 관리 권한이 있는 사용자로 Insight에 로그인합니다.
2. Manage * > * Business Entities * 를 선택합니다.
3. 추가 * 버튼을 클릭합니다
4. Tenant * 상자를 클릭하고 테넌트 이름을 입력합니다.

환경에 대한 테넌트를 이미 입력한 경우 선택할 수 있는 기존 테넌트 목록이 나타납니다. 또한 테넌트가 이 업무 엔티티에 적용되지 않는 경우 N/A를 선택할 수 있습니다.

5. 비즈니스 라인 *, * 사업 부문 * 및 * 프로젝트 * 에 대해 반복합니다.
6. 저장 * 을 클릭합니다

작업을 마친 후

모범 사례:

- 테이블의 비즈니스 계층을 매핑하고 계층 구조의 이름이 Insight 보기 및 보고서에 설명되어 있는지 확인합니다.
- 응용 프로그램을 만들기 전에 Insight에서 비즈니스 엔티티를 만듭니다.
- 각 업무 엔티티와 연관될 모든 애플리케이션을 식별하고 나열합니다.

회사의 애플리케이션을 구성하는 중입니다

회사 환경에서 사용되는 애플리케이션을 이해하면 자산 사용량을 추적하고 비용을 보고하는 데 도움이 됩니다. 여기서는 회사의 애플리케이션을 구성하고 적절한 자산과 연결합니다.

이 작업에 대해

회사의 업무 엔티티 구성 섹션에서 일부 업무 엔티티를 만들고 각 업무 엔티티에 연결된 모든 애플리케이션을 나열하도록 권장합니다. OnCommand Insight를 사용하면 사용 또는 비용 보고와 같은 관련 애플리케이션과 관련된 데이터를 추적할 수 있습니다.

사용자 환경에서 실행 중인 애플리케이션과 관련된 데이터를 추적하려면 먼저 해당 애플리케이션을 정의하고 적절한 자산과 연결해야 합니다. 호스트, 가상 머신, 볼륨, 내부 볼륨, qtree, 공유 및 하이퍼바이저.

이 연습에서는 마케팅 팀이 Exchange 전자 메일에 사용하는 가상 시스템의 사용을 추적하려고 합니다. 비즈니스 엔티티를 정의하는 동안 작성한 다음 테이블을 기억하실 것입니다. 이 워크시트에 각 업무 엔티티가 사용하는 애플리케이션을 나열하는 열을 추가해 보겠습니다. (이 표는 워크시트 예일 뿐입니다. Insight의 비즈니스 엔터티 테이블에는 "애플리케이션" 열이 표시되지 않습니다.)

테넌트	사업 부문	사업부	프로젝트	응용 프로그램
-----	-------	-----	------	---------

넷업	데이터 스토리지	법적 고지	특허	Oracle Identity Manager, Oracle On Demand, Patentg마법사
넷업	데이터 스토리지	마케팅	영업 이벤트	Exchange, Oracle Shared database, Blastoff Event Planner
해당 없음	해당 없음	안전 및 보안	해당 없음	해당 없음
...				

- Insight에서 애플리케이션 생성: *

단계

1. 관리 권한이 있는 사용자로 Insight에 로그인합니다.
2. Manage * > * Applications * 를 선택합니다
3. 추가 * 버튼을 클릭합니다
4. 애플리케이션의 이름을 입력합니다(예: ""Exchange"" 입력).
5. 응용 프로그램의 우선 순위를 선택합니다
6. 응용 프로그램을 업무 엔티티에 연결하려면 * 업무 엔티티 * 드롭다운에서 하나를 선택합니다. 그렇지 않으면 이를 "없음"으로 남겨둘 수 있습니다.
7. 각 호스트가 클러스터의 동일한 볼륨에 액세스할 수 있도록 하려면 * 볼륨 공유 확인 * 상자가 선택되어 있는지 확인합니다. 예를 들어, high-availability 클러스터의 호스트는 장애 조치를 위해 동일한 볼륨에 마스킹되어야 하는 경우가 많지만, 관련 없는 애플리케이션의 호스트는 일반적으로 동일한 물리적 볼륨에 액세스할 필요가 없습니다. 또한 규정 정책에 따라 보안상의 이유로 관련 없는 응용 프로그램이 동일한 물리적 볼륨에 액세스하는 것을 명시적으로 허용하지 않을 수 있습니다. 볼륨 공유를 사용하지 않는 경우 * 볼륨 공유 확인 * 상자의 선택을 취소합니다. 이 작업을 수행하려면 보증 라이선스가 필요합니다.
8. 저장 을 클릭합니다.
9. 사용자 환경의 다른 모든 애플리케이션에 대해 이 과정을 반복합니다.

작업을 마친 후

마케팅 팀에서 Exchange 애플리케이션을 사용하고 있음을 알 수 있습니다. Exchange의 가상 시스템 활용률을 보고 스토리지 추가 시기를 예측하고자 합니다. Exchange 애플리케이션을 모든 마케팅 VM과 연결하겠습니다. 이 작업을 수행하는 가장 쉬운 방법은 쿼리를 사용하는 것입니다.

다음 단계에 따라 각 응용 프로그램을 해당 자산과 연결할 수 있습니다.

- 응용 프로그램을 자산에 연결: *

이제 애플리케이션을 만들고 원하는 비즈니스 엔티티에 연결했으므로 이제 해당 애플리케이션을 사용자 환경의 자산과 연결할 수 있습니다. 이 예에서는 Exchange 애플리케이션을 회사의 여러 가상 머신에 연결합니다. 가장 쉬운 방법은 쿼리입니다.

1. 쿼리 * > * + 새 쿼리 * 를 선택합니다.
2. 리소스 유형 선택 * 드롭다운에서 _Virtual Machine_을 선택합니다
3. 마케팅 팀에서 자산 이름을 ""mktg" 문자열로 지정합니다. 이름 필터 상자에 ""mktg"(따옴표 제외)를 입력하고 적용 (확인 표시) 단추를 클릭합니다.
4. ""mktg" 문자열이 있는 모든 VM의 목록이 표시됩니다.
5. 필요한 경우 * More * (자세히 *) 드롭다운을 클릭하고 추가 필터를 추가합니다.
6. 원하는 각 VM 이름 옆의 확인란을 클릭하여 Exchange에 사용되는 VM을 선택하거나 열 상단의 확인란을 클릭하여 모든 VM을 선택합니다.
7. 원하는 VM을 선택한 후 * Actions * 버튼을 클릭하고 * Add Application * 을 선택합니다.
8. 응용 프로그램 할당 대화 상자에서 * 응용 프로그램 * 드롭다운을 클릭하고 ""교환""을 선택합니다.
9. 저장 * 을 클릭합니다.
10. 필요에 따라 Exchange 애플리케이션을 다른 자산(호스트, 볼륨 등)과 연결하려면 이 과정을 반복합니다.

알림을 위한 성능 정책 생성

성능 정책을 사용하면 특정 조건이 충족되면 경고를 모니터링하고 보낼 수 있습니다.

이 작업에 대해

이제 자산에 대한 주석을 작성했으므로 Sunnyvale(DC1_SVL) 데이터 센터의 모든 스토리지 어레이에서 지연 시간이 2ms보다 높을 때 경고하는 데 사용할 수 있는 성능 정책을 만들어 보겠습니다. 이러한 상황이 발생하면 선택한 수신자에게 이메일을 보냅니다.

단계

1. 관리 * > * 성능 정책 * 을 선택합니다.

성능 정책 페이지가 열립니다. 여러 가지 기본 정책이 이미 설정되어 있으므로 필요에 따라 수정할 수 있습니다. 그러나 새 정책을 만들 것입니다.

2. 추가 * 버튼을 클릭합니다.

Add Policy * (정책 추가 *) 대화 상자가 열립니다.

3. Policy name * 필드에 ""VL Data Center Latency policy"를 입력합니다.

개체의 다른 모든 정책 이름과 다른 이름을 사용해야 합니다. 예를 들어, 내부 볼륨에 대해 "지연 시간"이라는 두 개의 정책을 사용할 수는 없지만, 내부 볼륨에 대한 "지연 시간" 정책과 다른 볼륨에 대한 "지연 시간" 정책을 사용할 수는 있습니다. 가장 좋은 방법은 개체 유형에 관계없이 모든 정책에 대해 항상 고유한 이름을 사용하는 것입니다.

4. 유형 * 의 개체에 적용 에서 * 스토리지 * 를 선택합니다.
5. with annotation * 필드에서 * Data Center * 가 "dc1_SVL"인 경우(또는 여기서 원하는 데이터 센터의 이름을 선택하십시오).
6. 첫 번째 발생 항목 * 의 창 뒤에 적용합니다.

첫 번째 발생 옵션은 첫 번째 데이터 샘플에서 임계값이 초과되면 알림을 트리거합니다. 다른 모든 옵션은 임계값을

한 번 넘어섰을 때 경고를 발생시키고 지정된 시간 이상 연속적으로 교차하는 경우에 발생합니다.

7. with severity * 목록에서 * Warning * 을 선택합니다.
8. Email recipient * 에서 글로벌 수신자 목록을 무시하려면 클릭합니다. 처음 원하는 알림 수신인의 이메일 주소를 추가하려면 + 을 클릭하고 * 확인 * 을 클릭합니다. 원하는 추가 이메일 수신자에 대해 반복합니다.
9. 다음 중 * 가 참인 경우 기본 선택 항목을 Create alert 로 둡니다. 설정된 임계값 중 하나가 충족되면 경고가 전송됩니다. 또한 설정된 모든 * 임계값이 충족되는 경우에만 알림을 보내도록 선택할 수 있습니다.
10. 첫 번째 임계값을 설정하려면 드롭다운에서 * Latency - Total * 을 선택하고 2ms를 초과하도록 설정합니다.
11. 필요한 경우 * Add threshold * (임계값 추가) 버튼을 클릭하여 알림에 추가 임계값을 추가합니다. 정책이 원하는 방식으로 사용자 지정되면 * 저장 * 을 클릭합니다.
12. 알림이 생성된 경우 * 추가 정책 처리 중지 * 를 선택할 수도 있습니다. 이 정책 조건이 충족되면 추가 정책 경고가 중지됩니다.
13. 비즈니스 요구에 따라 다른 조건에 따라 다른 받는 사람에 대한 알림을 설정하여 원하는 만큼 새 정책을 추가할 수 있습니다. 특정 수신자 없이 구성된 모든 정책은 * Admin * > * Notifications * 페이지에 설정된 글로벌 수신자 목록으로 경고를 보냅니다

작업을 마친 후

새 정책이 저장되면 각 정책이 자동으로 활성화되고 정책 조건이 충족되면 수신자는 알림을 받기 시작합니다(A_Violation_). 대시보드 * > * 위반 대시보드 * 에서 이러한 위반 사항을 모니터링할 수도 있습니다.

대시보드를 사용하여 데이터 강조 표시

이제 자산에 대한 주석이 추가되고 위반을 경고하기 위한 성능 정책이 구성되었으므로 대시보드를 생성하여 목표할 특정 데이터를 강조할 수 있습니다.

이 작업에 대해

이 예에서는 VM 성능 데이터를 강조 표시하는 단일 위젯이 포함된 대시보드를 생성하여 대시보드 생성을 개괄적으로 보여 줍니다. 단일 대시보드에 필요한 만큼의 위젯을 추가할 수 있으며 필요한 만큼 대시보드를 만들 수 있습니다. 위젯의 크기를 조정하고 원하는 대로 이동할 수 있습니다.

대시보드 및 위젯에 대한 자세한 내용은 OnCommand Insight 문서 전체에서 찾을 수 있습니다.

단계

1. 관리 권한이 있는 사용자로 Insight에 로그인합니다.
2. 대시보드 * 메뉴에서 * + 새 대시보드 * 를 선택합니다.



새 대시보드 페이지가 열립니다.

3. 모범 사례: 대시보드를 만드는 즉시 이름을 설정하고 저장합니다. 저장 * 버튼을 클릭하고 * 이름 * 필드에 대시보드의 고유 이름을 입력합니다. 예: ""VM 성능 대시보드"". 저장 * 을 클릭합니다.
4. 필요한 경우 * 편집 * 스위치를 ""켜짐""으로 밀어 편집 모드를 활성화합니다. 이렇게 하면 대시보드에 위젯을 추가할 수 있습니다.
5. 대시보드에 새 표 위젯을 추가하려면 * + 위젯 * 버튼을 클릭하고 * 표 * 를 선택합니다.

위젯 편집 대화 상자가 열립니다.

- 이름 필드에서 ""Widget 1"을 삭제하고 ""가상 시스템 성능 테이블"을 입력합니다.
- 자산 유형 드롭다운을 클릭하고 * Storage * 를 * Virtual Machine * 으로 변경합니다.

테이블 데이터가 변경되어 사용자 환경의 모든 가상 시스템이 표시됩니다.

- 표에 열을 추가하려면 * 열 * 을 클릭합니다  단추를 클릭하고 원하는 열을 선택합니다(예: *Data Center*, *Storage name* 및 *Tier*). 이러한 열을 기준으로 테이블을 정렬할 수 있습니다.
- 필요에 따라 필터를 설정하여 이 대시보드에 중요한 데이터를 강조 표시할 수 있습니다. 예를 들어 ""계층 1 - SSD" 주석이 있는 가상 머신만 표시하도록 선택할 수 있습니다. 필터 기준 * 옆에 있는 "+" 버튼을 클릭하고 *Tier*를 선택합니다. 아무거나 * 를 클릭하고 ""계층 1-SSD"를 입력합니다. 를 클릭합니다  버튼을 눌러 필터를 저장합니다.

이제 이 테이블에는 "SSD" 계층에 있는 가상 컴퓨터만 표시됩니다.

- Group By *(그룹화 기준) 옆의 "+" 버튼을 클릭하고 데이터 센터와 같이 그룹화할 필드를 선택하여 결과를 그룹화할 수 있습니다. 그룹화는 테이블에 자동으로 적용됩니다.
- 위젯을 원하는 대로 사용자 정의했으면 * Save * (저장 *) 버튼을 클릭합니다.

테이블 위젯이 대시보드에 저장됩니다.

- 오른쪽 아래 모서리를 끌어 대시보드에서 위젯의 크기를 조정할 수 있습니다.
- 위젯을 더 추가하려면 * + 위젯 * 버튼을 클릭합니다. 각 위젯은 저장될 때 대시보드에 추가됩니다.
- 원하는 모든 변경 사항을 적용했으면 * Save * 를 클릭하여 대시보드를 저장하십시오.
- 다른 데이터를 강조 표시하기 위해 추가 대시보드를 만들 수 있습니다.

사용자 지정 대시보드 만들기

OnCommand Insight 7.3에는 향상된 맞춤형 대시보드 기능이 포함되어 있어 사용자에게 중요한 데이터를 한눈에 파악할 수 있으며, 데이터를 한눈에 파악할 수 있습니다.

OnCommand Insight를 사용하면 다양한 위젯이 포함된 사용자 지정 대시보드를 생성할 수 있으므로 IT 플랫폼 전반에 걸쳐 운영 뷰 인프라 데이터를 유연하게 생성할 수 있습니다. 각 대시보드는 데이터를 표시하고 차트에 작성할 때 매우 유연하게 사용할 수 있습니다. 이 사용 방법에서는 VM 성능을 강조하는 예제 대시보드를 만듭니다.

이 사용 방법은 예제로만 사용해야 하며 가능한 모든 시나리오를 포괄하지는 않습니다. 이 문서의 개념 및 단계를 사용하여 고유한 사용자 지정 대시보드를 만들어 특정 요구 사항에 맞는 데이터를 강조할 수 있습니다.

• 개요 *

다음 방법 중 하나를 사용하여 사용자 지정 대시보드를 만들 수 있습니다.

- * 대시보드 * > * + 새 대시보드 *
- 대시보드 * > * 모든 대시보드 표시 * 를 선택하고 * + 추가 * 를 클릭합니다

New Dashboard 화면에는 다음과 같은 몇 가지 컨트롤이 있습니다.

- * 시간 선택기 *: 사용자 지정 날짜 범위 선택기를 사용하여 3시간에서 90일까지 일정 범위의 대시보드 데이터를 볼 수 있습니다. 개별 위젯에서 이 전역 시간 범위를 재정의할 수 있습니다.
- [편집] * 버튼: ""켜기""를 선택하면 [편집] 모드가 활성화되므로 대시보드를 변경할 수 있습니다. 새 대시보드는 기본적으로 편집 모드로 열립니다.
- * 저장 * 버튼: 대시보드를 저장, 이름 변경 또는 삭제할 수 있습니다.
- * 변수 * 버튼: 대시보드에 변수를 추가할 수 있습니다. 변수를 변경하면 모든 위젯이 한 번에 업데이트됩니다. 변수에 대한 자세한 내용은 [참조하십시오 "사용자 지정 대시보드 개념"](#)
- * Widget * 버튼: 대시보드에 표, 차트 또는 기타 위젯을 원하는 수만큼 추가할 수 있습니다.

위젯의 크기를 조정하고 대시보드 내의 다른 위치로 재배치하여 현재 필요에 따라 데이터를 가장 잘 볼 수 있습니다.

- 위젯 유형 *

다음 위젯 유형 중에서 선택할 수 있습니다.

- 표 * 위젯: 선택한 필터 및 열에 따라 데이터를 표시하는 테이블 테이블 데이터를 축소 및 확장할 수 있는 그룹으로 결합할 수 있습니다.
- 선, 자유곡선, 영역, 누적 영역 * 차트: 시간 경과에 따라 성능 및 기타 데이터를 표시할 수 있는 시계열 차트 위젯입니다.
- 단일 값 * 위젯: 카운터로부터 직접 유도하거나 쿼리 또는 표현식을 사용하여 계산할 수 있는 단일 값을 표시할 수 있는 위젯. 예를 들어, 환경의 모든 스토리지에 대한 총 IOPS의 합계를 대시보드 상단에 단일 값으로 표시할 수 있습니다.
- 막대 * 차트: 상위 또는 하위 5, 10, 20 또는 50 값을 표시하는 차트.
- 상자 플롯 * 차트: 단일 차트에서 데이터의 최소, 최대, 중간값 및 하위 사분점과 상위 사분위 사이의 범위에 대한 플롯.
- 산란 플롯 * 차트: IOPS 및 지연 시간과 같은 점으로 관련 데이터를 플롯합니다. 이 예에서는 짧은 지연 시간과 낮은 IOPS의 자산을 빠르게 봅니다.

또한 선택할 수 있는 여러 개의 레거시 위젯이 있습니다. 이러한 위젯을 보려면 * 위젯 * 드롭다운에서 더 보기...를 선택합니다.

사용자 지정 대시보드 개념

사용자 지정 대시보드 및 위젯을 통해 데이터가 표시되는 방식을 유연하게 지정할 수 있습니다. 다음은 사용자 지정 대시보드를 최대한 활용하는 데 도움이 되는 몇 가지 개념입니다. 각 개념은 다음 섹션에서 자세히 설명합니다.

- 변수 *

변수를 사용하면 대시보드의 일부 또는 모든 위젯에 표시된 데이터를 한 번에 변경할 수 있습니다. 각 위젯이 공통 변수를 사용하도록 설정하면 한 곳에서 변경한 경우 각 위젯에 표시된 데이터가 자동으로 업데이트됩니다.

- 여러 쿼리 및/또는 식 *

각 시계열 위젯(꺾은선형, 스플라인, 영역형 또는 누적 영역형 차트)에는 최대 5개의 쿼리 및/또는 식을 사용하여 표시할 데이터를 결정할 수 있으므로 단일 차트에서 서로 다른 데이터 집합을 비교할 수 있습니다. 예를 들어, 스토리지 및 VM의 IOPS를 보여 주는 선형 차트 또는 모든 스토리지 풀의 처리량과 지연 시간을 비교한 단일 차트를 사용할 수 있습니다.

- 롤업 및 그룹화 *

각 위젯에 표시된 데이터는 수집된 데이터 포인트에서 취합됩니다. 다음 방법 중 하나로 이 데이터를 롤업하도록 선택할 수 있습니다.

- Avg: 데이터를 기본 데이터의 평균으로 롤업합니다
- Max(최대): 데이터를 기본 데이터의 최대값으로 롤업합니다
- MIN(최소): 데이터를 최소 내부 데이터로 롤업합니다
- Sum(합계): 데이터를 원본 데이터의 합계로 롤업합니다

기본적으로 모든 원본 데이터는 차트 또는 테이블의 단일 항목(모두)으로 롤업됩니다. 데이터 센터 또는 계층과 같은 특정 속성에 대한 데이터를 롤업하여 기본 데이터를 원하는 그룹으로 분산하도록 선택할 수 있습니다. 위젯에는 선택한 속성에 대한 데이터만 표시됩니다.

선택한 특성에 따라 테이블 위젯에서 데이터를 그룹화할 수 있습니다. 예를 들어 데이터 센터별로 테이블을 그룹화하도록 선택할 수 있습니다. 그룹은 가능한 한 확장 또는 축소할 수 있습니다. 위젯에서 설정한 롤업 방법(평균, 최대, 최소 또는 합계)에 따라 테이블의 성능 데이터가 그룹 헤더에서 롤업됩니다.

표 위젯은 모든 열을 기준으로 정렬할 수 있으며 필요에 따라 열을 이동하거나 크기를 조정할 수 있습니다.

- 위/아래 *

이 옵션을 사용하여 차트 위젯에서 결과 집합을 제한하거나 위젯에 상위 N개의 결과를 표시할지 또는 하위 N개의 결과를 표시할지 여부를 선택할 수 있습니다. 데이터가 롤업되지 않거나 특정 특성에 의해 롤업되는 경우 이 옵션을 선택할 수 있습니다.

- 대시보드 시간 재정의 *

기본적으로 대시보드에 추가하는 대부분의 위젯은 대시보드의 시간 범위 설정(3시간, 24시간, 3D, 7d, 30d 또는 사용자 지정 범위)에 따라 데이터를 표시합니다. 그러나 개별 위젯에서 이 시간 설정을 재정의하여 대시보드의 시간 설정에 관계없이 특정 시간 컨텍스트에 데이터를 표시하도록 할 수 있습니다.

이러한 개념은 다음 섹션에서 자세히 설명합니다.

대시보드 변수

대시보드 변수를 사용하면 대시보드의 여러 위젯에서 데이터를 빠르고 쉽게 필터링할 수 있습니다.

시작하기 전에

이 예에서는 여러 스토리지 자산에 대해 * City * 주식(City 속성이라고도 함)을 설정해야 합니다.

최상의 결과를 얻으려면 여러 도시에 여러 도시를 설정하십시오.

이 작업에 대해

변수를 사용하면 사용자 지정 대시보드의 일부 또는 모든 위젯에 표시되는 데이터를 빠르고 간단하게 필터링할 수 있습니다. 다음 단계에서는 변수를 사용하는 위젯을 만들고 대시보드에서 사용하는 방법을 보여 줍니다.


단계

1. 관리 권한이 있는 사용자로 Insight에 로그인합니다
2. 대시보드 * > * + 새 대시보드 * 를 클릭합니다.
3. 위젯을 추가하기 전에 대시보드 데이터를 필터링하는 데 사용할 변수를 정의하려고 합니다. 변수 * 버튼을 클릭합니다.

속성 목록이 표시됩니다.

4. 도시를 기준으로 필터링하도록 대시보드를 설정하려고 합니다. 목록에서 * City * 속성을 선택합니다.

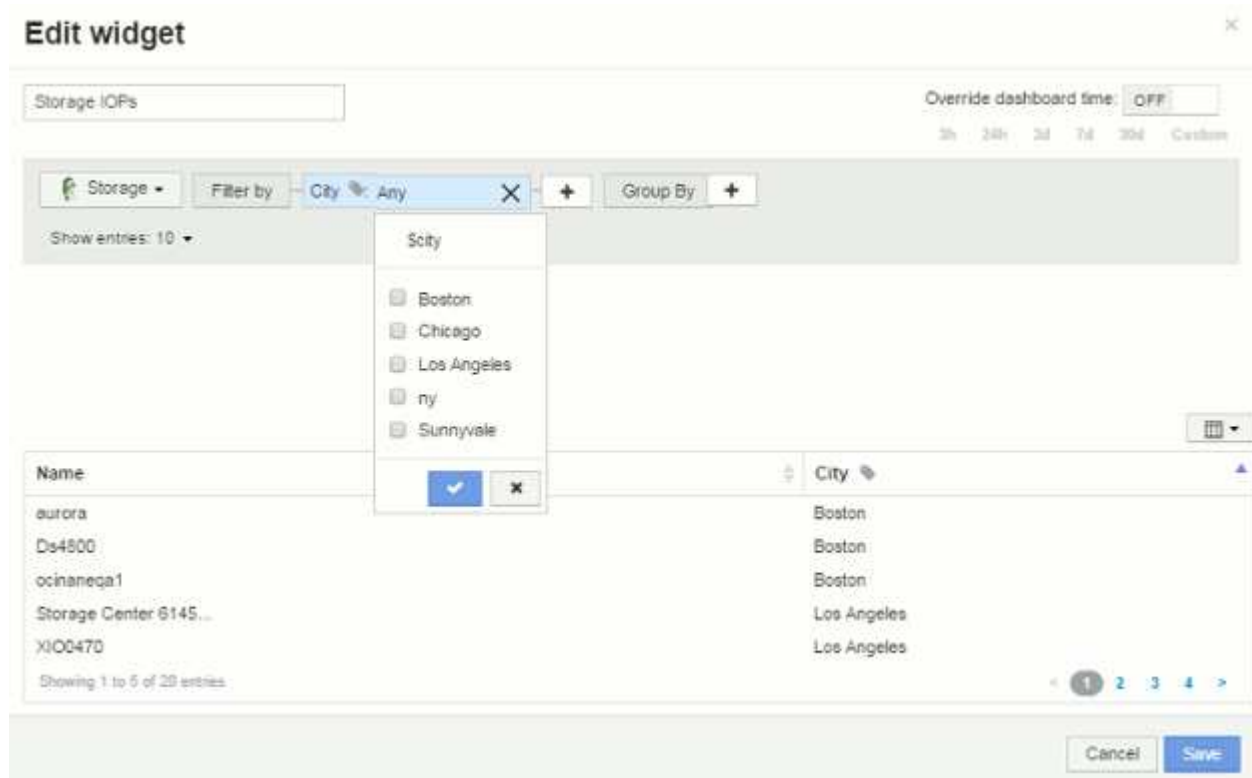
\$CITY 변수 필드가 생성되어 대시보드에 추가됩니다.

5. 다음으로 이 변수를 사용하려면 위젯에 알려야 합니다. 이를 설명하는 가장 간단한 방법은 도시 열을 보여 주는 테이블 위젯을 추가하는 것입니다. Widget * 버튼을 클릭하고 * Table * 위젯을 선택하십시오.
6. 먼저 열 선택에서 도시 필드를 선택하여 테이블에 추가합니다  단추를 클릭합니다.

구/군/시는 목록 유형 특성이므로 이전에 정의된 선택 항목의 목록이 포함됩니다. 텍스트, 부울 또는 날짜 유형 속성을 선택할 수도 있습니다.

7. 다음으로 * Filter by+ * 버튼을 클릭하고 * City * 를 선택합니다.
8. 임의 * 를 클릭하여 구/군/시에 대해 가능한 필터 선택 항목을 봅니다. 이 목록에는 이전에 사용 가능한 선택 항목 외에 ""\$city""가 포함되어 있습니다. 이 대시보드 변수를 사용하려면 ""\$city""를 선택하십시오.

""\$city" 선택 옵션은 이전에 기본 대시보드 페이지에 정의된 경우에만 여기에 표시됩니다. 변수가 이전에 정의되지 않은 경우 필터에 대한 기존 선택 항목만 표시됩니다. 선택한 속성 유형에 적용 가능한 변수만 해당 필터에 대한 드롭다운에 표시됩니다.



9. * 위젯을 * 저장 * 합니다.

10. 대시보드 페이지에서 \$CITY 변수 옆의 * Any * 를 클릭하고 보려는 도시를 선택합니다.

선택한 도시만 표시하도록 표 위젯이 업데이트됩니다. 원하는 대로 \$CITY 변수의 값을 변경할 수 있으며, \$CITY 변수를 사용하도록 설정된 대시보드의 모든 위젯이 자동으로 새로 고쳐지고 선택한 값에 대한 데이터만 표시됩니다.

11. 대시보드를 원하는 대로 구성했으면 * 저장 * 하십시오.

대시보드 변수에 대한 자세한 정보

대시보드 변수는 여러 가지 형식으로 제공되며 서로 다른 필드에서 사용할 수 있으며 명명 규칙을 따라야 합니다. 이러한 개념은 여기에 설명되어 있습니다.

변수 유형

변수는 다음 형식 중 하나일 수 있습니다.

- 텍스트 *: 영숫자 문자열입니다. 기본 변수 유형입니다.
- 숫자 *: 숫자 또는 숫자 범위.
- 부울 *: True/False, Yes/No, 0/1 등의 값을 가진 필드에 사용합니다 부울 변수의 선택 항목은 Yes, No, None, _Any_입니다.
- 날짜 *: 날짜 또는 날짜 범위입니다.

"일반" 변수

변수 * 버튼을 클릭하고 위에 나열된 유형 중 하나를 선택하여 일반 또는 범용 변수를 설정할 수 있습니다. 이러한 유형은 항상 드롭다운 목록의 맨 위에 표시됩니다. 변수에 ""\$var1" 등의 기본 이름이 지정되고 특정 주석이나 속성에 연결되지 않습니다.

제네릭 변수를 구성하면 위젯에서 해당 변수를 사용하여 해당 형식의 *any_* 필드를 필터링할 수 있습니다. 예를 들어, *_Name*, *Alias* 및 *Vendor*(모든 텍스트 유형 속성)를 표시하는 테이블 위젯이 있고 ""\$var1""가 텍스트 유형 변수인 경우 위젯에서 각 필드에 대해 필터를 설정하여 \$var1 변수를 사용할 수 있습니다. 다른 위젯에서 해당 필드나 텍스트 필드에 \$var1을 사용하도록 설정할 수 있습니다.

대시보드 페이지에서 \$var1을 값(예: ""NetApp"")으로 설정하면 해당 변수를 사용하도록 설정된 *_ALL_Widget*의 해당 필드 중 *_ALL_*이 필터링됩니다. 이렇게 하면 여러 위젯을 한 번에 업데이트하여 원하는 대시보드 데이터를 강조 표시할 수 있습니다.

제네릭 변수는 해당 형식의 모든 필드에 사용될 수 있으므로 해당 기능을 변경하지 않고 제네릭 변수의 이름을 변경할 수 있습니다.



모든 변수는 특정 특성에 대해 생성한 변수까지도 "일반" 변수로 취급됩니다. 해당 형식의 특성이나 주석에 대해 필터를 설정할 때 형식의 구성된 모든 변수가 표시되기 때문입니다. 그러나 위의 *_Name/Alias/Vendor_Example* 과 같이 여러 필드에 걸쳐 값을 필터링하는 데 사용할 일반 변수를 만드는 것이 가장 좋습니다.

변수 이름 지정

변수 이름:

- 항상 "\$" 접두사로 붙여야 합니다. 변수를 설정하면 자동으로 추가됩니다.
- 특수 문자는 포함할 수 없습니다. 문자 A-z 및 숫자 0-9 만 허용됩니다.
- "\$" 기호를 포함하여 20자를 초과할 수 없습니다.
- 대소문자를 구분하지 않습니다. \$CityName 및 \$cityname은 동일한 변수입니다.
- 기존 변수 이름과 같을 수 없습니다.
- "\$" 기호만이 될 수 없습니다.

변수를 사용하는 위젯

변수는 다음 위젯과 함께 사용할 수 있습니다.

- 영역 차트
- 가로 막대형 차트
- 상자 플롯 차트
- 꺾은선형 차트
- 산포도 차트
- 단일 값 위젯
- 스플라인 차트
- 누적 영역형 차트
- 테이블 위젯

위젯 범례 표시

대시보드의 위젯은 범례와 함께 또는 범례 없이 표시할 수 있습니다.

위젯의 범례는 다음 두 가지 방법 중 하나를 사용하여 대시보드에서 켜거나 끌 수 있습니다.

1. 위젯 자체를 만들거나 편집할 때 범례 확인란을 선택하고 위젯을 저장합니다.
2. 대시보드를 편집 모드로 설정한 상태에서 위젯의 옵션 버튼을 클릭하고 메뉴에서 범례 확인란을 선택합니다.

위젯에 표시된 데이터를 편집하고 변경하면 해당 위젯의 범례가 동적으로 업데이트됩니다.

범례가 표시될 때 범례가 나타내는 자산의 랜딩 페이지를 탐색할 수 있으면 범례가 해당 자산 페이지에 대한 링크로 표시됩니다.

대시보드 위젯 쿼리 및 필터

대시보드 위젯의 쿼리는 데이터 표시를 관리하는 강력한 도구입니다. 다음은 위젯 쿼리에 대해 주의해야 할 몇 가지 사항입니다.

일부 위젯에는 최대 5개의 쿼리가 있을 수 있습니다. 각 쿼리는 위젯에 고유한 선 또는 그래프 세트를 플롯합니다. 한 쿼리에 롤업, 그룹화, 상위/하위 결과 등을 설정해도 위젯에 대한 다른 쿼리에는 영향을 주지 않습니다.

아이 아이콘을 클릭하여 쿼리를 일시적으로 숨길 수 있습니다. 쿼리를 숨기거나 표시하면 위젯이 자동으로

업데이트됩니다. 이렇게 하면 위젯을 구축할 때 개별 쿼리에 대해 표시된 데이터를 확인할 수 있습니다.

다음 위젯 유형에는 여러 개의 쿼리가 있을 수 있습니다.

- 영역형 차트
- 누적 영역형 차트
- 꺾은선형 차트
- 스플라인 차트
- 단일 값 위젯

나머지 위젯 유형에는 하나의 쿼리만 있을 수 있습니다.

- 표
- 가로 막대형 차트
- 상자 플롯
- 산포도

대시보드 쿼리에서 필터링

다음 중 하나를 사용하여 필터링하여 쿼리의 * 텍스트 필드 * 에서 검색을 구체화할 수 있습니다.

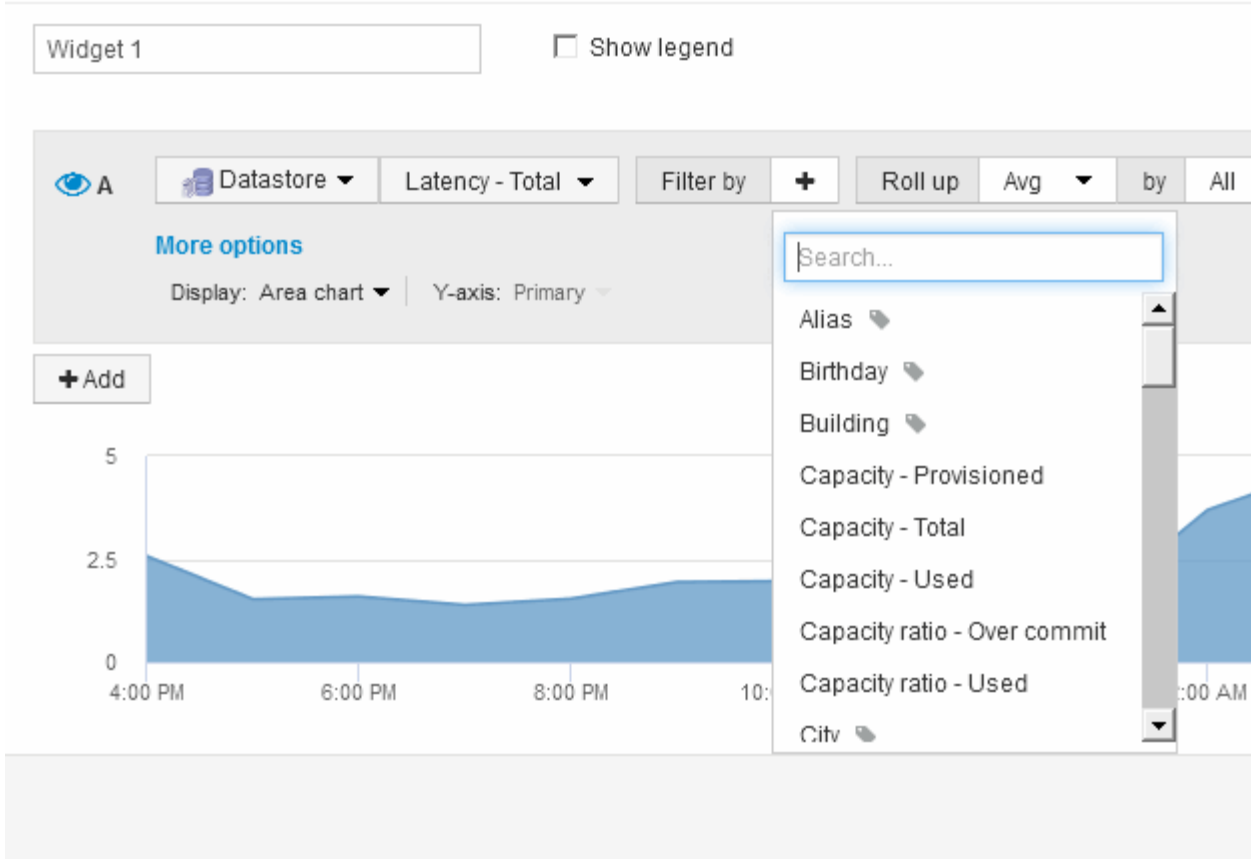
- 별표를 사용하면 모든 항목을 검색할 수 있습니다. 예를 들면, 다음과 같습니다. `vol*rhel ""vol""`로 시작하고 `""rhel""`으로 끝나는 모든 리소스를 표시합니다.
- 물음표를 사용하면 특정 수의 문자를 검색할 수 있습니다. 예를 들면, 다음과 같습니다. `BOS-PRD??-S12 BOS-PRD12-S12, BOS-PRD13-S12` 등을 표시합니다.
- 또는 연산자를 사용하여 여러 요소를 지정할 수 있습니다. 예를 들면, 다음과 같습니다. `FAS2240 OR CX600 OR FAS3270` 여러 스토리지 모델을 찾습니다.
- NOT 연산자를 사용하면 검색 결과에서 텍스트를 제외할 수 있습니다. 예를 들면, 다음과 같습니다. `NOT EMC* "EMC"`로 시작하지 않는 모든 항목을 찾습니다. 을 사용할 수 있습니다 `NOT * null` 값을 포함하는 필드를 표시합니다.

필터 문자열을 큰따옴표로 묶으면 Insight는 첫 번째 견적과 마지막 견적 사이의 모든 항목을 정확히 일치하는 것으로 간주합니다. 따옴표 안에 있는 모든 특수 문자나 연산자는 리터럴로 처리됩니다. 예를 들어, `"" * ""`를 필터링하면 리터럴 별표로 된 결과가 반환되고, 이 경우 별표는 와일드카드로 처리되지 않습니다. 연산자 및, 또는 및 는 큰따옴표로 묶으면 리터럴 문자열로 처리됩니다.

쿼리 및 필터에 의해 반환된 개체를 식별합니다

쿼리 및 필터에 의해 반환된 개체는 다음 그림에 표시된 개체와 비슷합니다. '태그'가 할당된 개체는 주석이고, 태그가 없는 개체는 성능 카운터 또는 개체 특성입니다.

Edit widget



롤업 및 집선

대시보드 위젯에 표시되는 데이터는 수집된 데이터 지점에서 취합되므로 대시보드에서 유연성과 오목성이 확보됩니다.

각 위젯에 표시되는 데이터는 획득 중에 수집된 기본 데이터 지점에서 롤업됩니다. 예를 들어, 시간에 따른 스토리지 IOPS를 보여 주는 선형 차트 위젯이 있는 경우 각 데이터 센터에 대해 별도의 줄을 표시하여 빠르게 비교할 수 있습니다. 다음 방법 중 하나로 이 데이터를 롤업하도록 선택할 수 있습니다.

- * Avg *: 각 행을 기본 데이터의 `_average_`로 표시합니다.
- * Max *: 각 행을 내부 데이터의 `_maximum_`으로 표시합니다.
- * Min *: 각 행을 내부 데이터의 `_minimum_`으로 표시합니다.
- * Sum *: 각 행을 원본 데이터의 `_sum_`으로 표시합니다.

이렇게 하려면 먼저 위젯의 쿼리에서 자산 유형(예: *Storage*) 및 메트릭(예: *IOPS-Total*)을 선택합니다. Roll Up * 의 경우 롤업 방법(예: *Avg*)을 선택하고 데이터를 롤업할 특성 또는 주석을 선택합니다(예: *Data Center*). 위젯이 자동으로 업데이트되고 각 데이터 센터에 대한 줄이 표시됩니다.

기본 데이터의 `_ALL_`을 차트 또는 테이블로 롤업하도록 선택할 수도 있습니다. 이 경우 위젯의 각 쿼리에 대해 하나의 줄이 표시됩니다. 이 라인은 모든 기본 자산에 대해 선택한 메트릭의 평균, 최소, 최대 또는 합계를 표시합니다.

쿼리에 대한 필터를 설정한 경우 롤업되는 데이터는 필터링된 데이터를 기반으로 합니다.

모든 필드(예: *Model*)별로 위젯을 롤업하도록 선택한 경우에도 해당 필드에 대한 데이터를 차트나 테이블에 올바르게 표시하려면 해당 필드를 * Filter by * 로 지정해야 합니다.

- 데이터 집계: * 데이터 포인트를 분, 시간 또는 일 단위로 집계하여 해당 데이터가 속성(선택한 경우)에 의해 롤업되기 전에 시계열 차트(선, 영역 등)를 추가로 정렬할 수 있습니다. 평균, 최대, 최소 또는 합계에 따라 또는 선택한 간격 동안 수집된 마지막 데이터 요소에 따라 데이터 요소를 집계하도록 선택할 수 있습니다. 집계 방법을 선택하려면 위젯의 쿼리 섹션에서 * 추가 옵션 * 을 클릭합니다.

최소 허용 간격은 10분입니다. 긴 시간 범위와 결합하여 작은 간격을 사용하면 "집계 간격 때문에 데이터 요소가 너무 많습니다."가 발생할 수 있습니다. 경고. 간격이 작고 대시보드 기간을 7일로 늘릴 경우 이 내용이 표시될 수 있습니다. 이 경우 더 작은 기간을 선택할 때까지 Insight는 집계 간격을 1시간으로 일시적으로 늘립니다.

막대 차트 위젯과 단일 값 위젯에서 데이터를 집계할 수도 있습니다.

대부분의 자산 카운터는 기본적으로 *Avg_*로 집계됩니다. 일부 카운터는 기본적으로 *_Max*, *Min* 또는 *_Sum_*으로 집계됩니다. 예를 들어 포트 오류는 기본적으로 *_Sum_*으로 집계되며, 여기서 스토리지 IOPS는 *_Avg_*로 집계됩니다.

대시보드 위젯에 위/아래 결과 표시

사용자 지정 대시보드의 차트 위젯에서 롤업된 데이터에 대한 상위 또는 하위 결과를 표시하고 표시되는 결과 수를 선택할 수 있습니다. 표 위젯에서 표시되는 행 수를 선택하고 열을 기준으로 정렬할 수 있습니다.

차트 위젯 위/아래

차트 위젯에서 특정 속성으로 데이터를 롤업하도록 선택하면 상위 N 또는 하위 N 결과를 볼 수 있습니다. ALL_ATTURES로 롤업을 선택하면 위 또는 아래 결과를 선택할 수 없습니다.

쿼리의 * 표시 * 필드에서 * 상위 * 또는 * 하위 * 를 선택하고 제공된 목록에서 값을 선택하여 표시할 결과를 선택할 수 있습니다.

테이블 위젯에 항목이 표시됩니다

표 위젯에서 표 결과에 표시되는 결과 수를 선택할 수 있습니다. 5, 10, 20 또는 50개의 결과 중에서 선택할 수 있습니다. 필요 시 열을 기준으로 오름차순 또는 내림차순으로 정렬할 수 있으므로 위 또는 아래 결과를 선택할 수 있는 옵션이 제공되지 않습니다.

쿼리의 * 항목 표시 * 필드에서 값을 선택하여 대시보드의 테이블에 표시할 결과 수를 선택할 수 있습니다.

더 많은 결과를 표시하도록 선택하면 위젯을 대시보드에 저장할 때 위젯이 더 크게 표시됩니다. 표시된 행 수보다 작은 위젯 크기를 조정할 수 없습니다.

표 위젯에서 그룹화

테이블 위젯의 데이터는 사용 가능한 속성별로 그룹화되어 데이터의 개요를 볼 수 있고 더 자세한 정보를 위해 드릴다운할 수 있습니다. 테이블의 메트릭은 축소된 각 행에서 쉽게 볼 수 있도록 롤업됩니다.

표 위젯을 사용하면 설정한 특성에 따라 데이터를 그룹화할 수 있습니다. 예를 들어, 해당 스토리지가 있는 데이터 센터별로 그룹화된 총 스토리지 IOPS를 표에 표시할 수 있습니다. 또는 가상 머신을 호스팅하는 하이퍼바이저에 따라 그룹화된 가상 머신 테이블을 표시할 수도 있습니다. 목록에서 각 그룹을 확장하여 해당 그룹의 자산을 볼 수 있습니다.

그룹화는 * 표 * 위젯 유형에서만 사용할 수 있습니다.

성능 데이터 롤업

테이블 위젯에 성능 데이터 열(예: *IOPS - Total*)을 포함하는 경우 데이터를 그룹화하도록 선택하면 해당 열에 대해 롤업 방법을 선택할 수 있습니다. 기본 롤업 방법은 그룹 행에 있는 내부 데이터의 *average_*를 표시하는 것입니다. 또한 데이터의 *_sum*, *minimum* 또는 *_maximum_*을 표시하도록 선택할 수 있습니다.


그룹화 예제(롤업 설명 포함)

표 위젯을 사용하면 데이터를 그룹화하여 보다 쉽게 표시할 수 있습니다.

이 작업에 대해

이 예에서는 데이터 센터별로 그룹화된 모든 VM을 보여 주는 테이블 위젯을 생성합니다.

단계

1. 대시보드를 만들거나 열고 * Table * 위젯을 추가합니다.
2. 이 위젯의 자산 유형으로 * 가상 머신 * 을 선택합니다.
3. 열 선택기를 클릭합니다  하이퍼바이저 이름 _ 및 _ IOPS - 합계 _ 를 선택합니다.

이제 이러한 열이 표에 표시됩니다.

4. IOPS가 없는 VM은 무시하고 총 IOPS가 1보다 큰 VM만 포함해보겠습니다. 필터 기준 + * 버튼을 클릭하고 * IOPS - 합계 * 를 선택합니다. 임의의 * 를 클릭하고 * 보낸 사람 * 필드에 1을 입력합니다. 받는 사람 * 필드는 비워둡니다. 확인 버튼을 클릭하여 필터를 적용합니다.

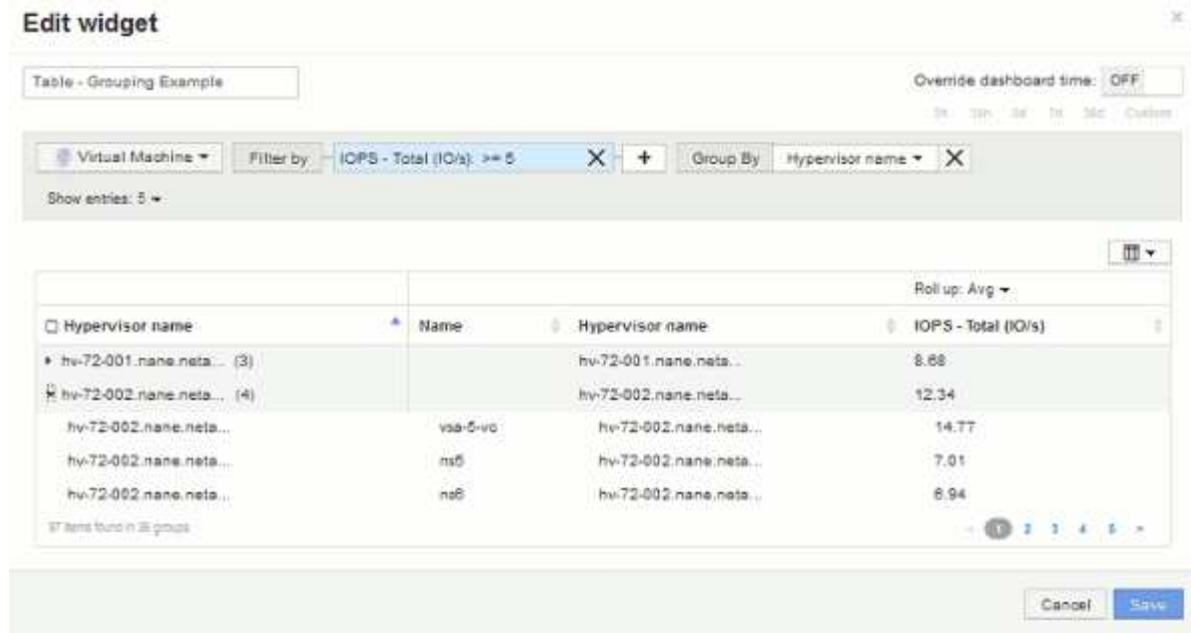
이제 표에는 총 IOPS가 1보다 크거나 같은 모든 VM이 표시됩니다. 테이블에 그룹이 없습니다. 모든 VM이 표시됩니다.

5. Group By + * 버튼을 클릭하십시오.

기본적으로 모든 * 가 그룹화 방법으로 선택되기 때문에 모든 VM은 ""모두""라는 단일 그룹으로 이동됩니다.

6. IOPS - Total_column 위에 * Roll Up * 옵션이 추가되었습니다. 기본 롤업 방법은 _ Avg _ 입니다. 즉, 그룹에 표시된 숫자는 그룹 내의 각 VM에 대해 보고된 총 IOPS의 평균입니다. 이 열을 *Avg*, *Sum*, *Min* 또는 *_Max_*로 롤업하도록 선택할 수 있습니다. 성능 메트릭이 포함된 각 열을 개별적으로 롤업할 수 있습니다.
7. 모두 * 를 클릭하고 * 하이퍼바이저 이름 * 을 선택합니다.

이제 VM 목록이 하이퍼바이저별로 그룹화됩니다. 각 하이퍼바이저를 확장하여 해당 하이퍼바이저에서 호스팅되는 VM을 볼 수 있습니다.



8. 저장 * 을 클릭하여 테이블을 대시보드에 저장합니다. 위젯 크기를 조정할 수 있습니다.

9. 대시보드를 저장하려면 * 저장 * 을 클릭합니다.

개별 위젯에 대한 대시보드 시간 재정의

개별 위젯에서 기본 대시보드 시간 프레임 설정을 재정의할 수 있습니다. 이러한 위젯은 대시보드 타임프레임이 아닌 설정된 기간을 기준으로 데이터를 표시합니다.

대시보드 시간을 무시하고 위젯이 자체 시간 프레임을 사용하도록 하려면 위젯의 편집 모드에서 * 대시보드 시간 재정의 * 를 * 켜짐 * 으로 설정하고 위젯의 시간 프레임을 선택합니다. * 위젯을 대시보드에 * 저장 * 합니다.

위젯은 대시보드 자체에서 선택한 기간에 관계없이 시간 프레임 세트에 따라 해당 데이터를 표시합니다.

한 위젯에 대해 설정한 기간은 대시보드의 다른 위젯에 영향을 주지 않습니다.

기본 및 보조 축에 대해 설명합니다

보조 축을 사용하면 서로 다른 측정 단위를 사용하는 두 개의 서로 다른 값 집합의 데이터를 쉽게 볼 수 있습니다.

이 작업에 대해

메트릭마다 차트에서 보고하는 데이터에 대해 서로 다른 측정 단위를 사용합니다. 예를 들어, IOPS를 볼 때 측정 단위는 초당 I/O 작업 수(IO/s)이고 지연 시간은 순전히 시간 단위(밀리초, 마이크로초, 초 등)입니다. 단일 집합에 Y축 값을 사용하여 두 메트릭을 모두 차트에 작성할 경우 지연 시간 번호(일반적으로 몇 밀리초)는 IOPS(일반적으로 수천 단위로 번호 지정)를 사용하여 동일한 배율로 차트로 작성되고 지연 시간 선은 해당 배율로 손실됩니다.

그러나 기본(왼쪽) Y축에 하나의 측정 단위를 설정하고 보조(오른쪽) Y축에 다른 측정 단위를 설정하여 하나의 의미 있는 그래프에 두 데이터 집합을 모두 표시할 수 있습니다. 각 메트릭은 자체 척도에 따라 차트로 작성됩니다.

단계

1. 대시보드를 만들거나 엽니다. 꺾은선형 차트 *, * 스플라인 차트 *, * 영역형 차트 * 또는 * 누적 영역형 차트 * 위젯을 대시보드에 추가합니다.
2. 자산 유형(예: * 스토리지 *)을 선택하고 첫 번째 메트릭으로 * IOPS - 합계 * 를 선택합니다. 원하는 필터를 설정하고 원하는 경우 롤업 방법을 선택합니다.

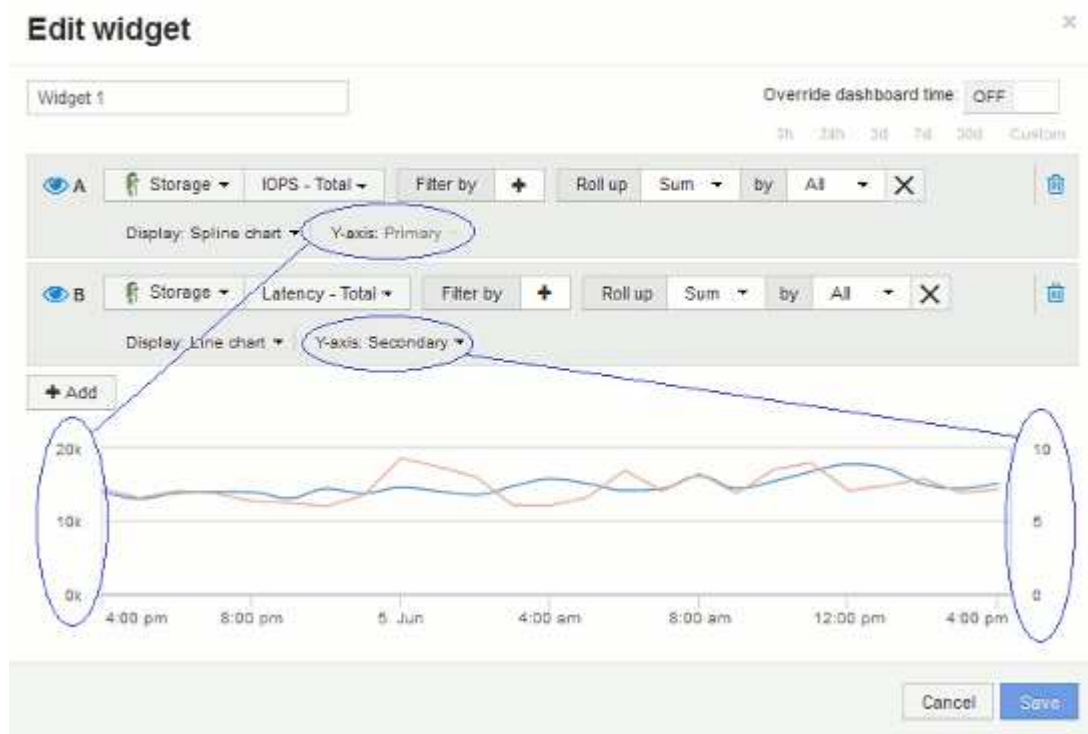
IOPS 선이 차트에 표시되고, 눈금은 왼쪽에 표시됩니다.

3. 차트에 두 번째 줄을 추가하려면 * + 추가 * 를 클릭합니다. 이 행의 경우 메트릭에 대해 * Latency - Total * 을 선택합니다.

차트 아래쪽에 선이 평평하게 표시됩니다. IOPS 라인과 동일한 규모로 그리기 때문입니다.

4. 지연 시간 쿼리에서 * Y축: 보조 * 를 선택합니다.

이제 지연 시간 선이 차트 오른쪽에 표시되는 자체 배율로 그려집니다.



대시보드 위젯의 식

시계열 위젯의 식을 사용하면 선택한 메트릭으로 계산을 기반으로 데이터를 표시할 수 있습니다.

대시보드에서 임의의 시간 계열 위젯(선, 스플라인, 영역, 스택 영역)을 사용하면 선택한 메트릭에서 식을 작성하고 이러한 식의 결과를 단일 그래프에 표시할 수 있습니다. 다음 예제에서는 식을 사용하여 특정 문제를 해결합니다. 첫 번째 예에서는 환경의 모든 스토리지 자산에 대해 총 IOPS의 백분율로 읽기 IOPS를 표시하려고 합니다. 두 번째 예에서는 사용자 환경에서 발생하는 "시스템" 또는 "오버헤드" IOPS, 즉 데이터를 읽거나 쓰지 않는 IOPS에 대한 가시성을 제공합니다.

식을 사용하면 함께 비율과 같은 대체 방법으로 메트릭을 볼 수 있습니다.

이 작업에 대해

이 예에서는 총 IOPS의 백분율로 읽기 IOPS를 표시하려고 합니다. 이 수식을 다음과 같은 수식으로 생각할 수 있습니다.

$$\bullet \text{ 읽기 백분율} = (\text{읽기 IOPS} / \text{총 IOPS}) \times 100$$

이 데이터는 대시보드의 선 그래프에 표시할 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

단계

1. 새 대시보드를 만들거나 * 편집 모드 * 로 기존 대시보드를 엽니다.
2. 대시보드에 위젯을 추가합니다. 영역표 * 를 선택합니다.

위젯이 편집 모드로 열립니다. 기본적으로 * 스토리지 * 자산에 대한 * IOPS - 합계 * 가 표시된 쿼리가 표시됩니다. 원하는 경우 다른 자산 유형을 선택합니다.

3. Expression * 으로 변환 단추를 클릭합니다.

현재 쿼리가 식 모드로 변환됩니다. 표현식 모드에서는 자산 유형을 변경할 수 없습니다. 표현식 모드에 있는 동안 버튼이 * Query * 로 바뀝니다. 언제든지 쿼리 모드로 다시 전환하려면 이 옵션을 클릭합니다. 모드 간을 전환하면 필드가 기본값으로 재설정됩니다.

지금은 * Expression * 모드를 사용할 수 있습니다.

4. IOPS-Total * 메트릭은 이제 알파벳 변수 필드 ""A""에 있습니다. ""b"" 변수 필드에서 * 선택 * 을 클릭하고 * IOPS - 읽기 * 를 선택합니다.

변수 필드 뒤에 있는+ 버튼을 클릭하여 식에 대해 최대 5개의 알파벳 변수를 추가할 수 있습니다. 읽기 백분율 예에서는 총 IOPS("""a") 및 읽기 IOPS("""b")만 필요합니다.

5. 식 * 필드에서 각 변수에 해당하는 문자를 사용하여 식을 작성합니다. 우리는 $_ \text{읽기 백분율} = (\text{읽기 IOPS} / \text{총 IOPS}) \times 100$ _ 을(를) 알고 있으므로 이 식을 다음과 같이 씁니다. $(b / a) * 100$
6. Label * 필드는 표현식을 식별합니다. 레이블을 ""읽기 백분율" 또는 사용자에게 똑같이 의미 있는 것으로 변경합니다.
7. 단위 * 필드를 ""%" 또는 ""%"로 변경합니다.

선택한 스토리지 디바이스에 대한 IOPS 읽기 백분율이 차트에 표시됩니다. 원하는 경우 필터를 설정하거나 다른 롤업 방법을 선택할 수 있습니다. Rollup 방법으로 * Sum * 을 선택하면 모든 백분율 값이 함께 추가되므로 100%보다 높아질 수 있습니다.

8. 차트를 대시보드에 저장하려면 * 저장 * 을 클릭합니다.

또한 * 선형 차트 *, * 스플라인 차트 * 또는 * 누적 영역형 차트 * 위젯에서 식을 사용할 수도 있습니다.

식 예: "System" I/O

식은 다른 메트릭에서 계산할 수 있는 차트 데이터를 자유롭게 제공합니다.

이 작업에 대해

예 2: OnCommand Insight는 데이터 소스에서 여러 메트릭을 획득합니다. 그 중에는 읽기, 쓰기 및 총 IOPS가 있습니다. 그러나 취득에서 보고된 총 IOPS 수에 "시스템" IOPS가 포함되는 경우가 있습니다. 이는 데이터 읽기 또는 쓰기의 직접적인 부분이 아닌 IO 작업입니다. 또한 이 시스템 I/O는 적절한 시스템 작동에 필요하지만 데이터 작업과 직접 관련이 없는 "오버헤드" I/O로 생각할 수 있습니다.

이러한 시스템 I/O를 표시하기 위해 획득에서 보고된 총 IOPS에서 읽기 및 쓰기 IOPS를 뺄 수 있습니다. 수식은 다음과 같습니다.

- 시스템 IOPS = 총 IOPS - (읽기 IOPS + 쓰기 IOPS)

그런 다음 이 데이터를 대시보드의 선 그래프로 표시할 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

단계

1. 새 대시보드를 만들거나 * 편집 모드 * 로 기존 대시보드를 엽니다.
2. 대시보드에 위젯을 추가합니다. 꺾은선형 차트 * 를 선택합니다.

위젯이 편집 모드로 열립니다. 기본적으로 * 스토리지 * 자산에 대한 * IOPS - 합계 * 가 표시된 쿼리가 표시됩니다. 원하는 경우 다른 자산 유형을 선택합니다.

3. 쿼리 복사본을 만들려면 단추를 클릭합니다.

쿼리의 복제본이 원본 아래에 추가됩니다.

4. 두 번째 쿼리에서 * 표현식으로 변환 * 단추를 클릭합니다.

현재 쿼리가 식 모드로 변환됩니다. 언제든지 쿼리 모드로 다시 전환하려면 * 쿼리에서 되돌리기 * 를 클릭합니다. 모드 간을 전환하면 필드가 기본값으로 재설정됩니다.

지금은 * Expression * 모드를 사용할 수 있습니다.

5. IOPS-Total * 메트릭은 이제 알파벳 변수 필드 ""A""에 있습니다. IOPS - 합계 * 를 클릭하고 * IOPS - 읽기 * 로 변경합니다. .
6. ""b"" 변수 필드에서 * 선택 * 을 클릭하고 * IOPS-쓰기 * 를 선택합니다.
7. 식 * 필드에서 각 변수에 해당하는 문자를 사용하여 식을 작성합니다. 간단히 다음과 같이 표현해 보겠습니다. a + b. Display* 섹션에서 이 표현식에 대한 **Area chart**를 선택합니다.
8. Label * 필드는 표현식을 식별합니다. 레이블을 "시스템 IOPS"로 변경하거나 사용자에게 똑같이 의미 있는 레이블을 변경합니다.

이 차트에는 총 IOPS가 선형 차트로 표시되며, 아래에 읽기 및 쓰기 IOPS의 조합이 나와 있는 영역 차트가 표시됩니다. 이 두 가지 간의 공백은 데이터 읽기 또는 쓰기 작업과 직접 관련이 없는 IOPS를 나타냅니다.

9. 차트를 대시보드에 저장하려면 * 저장 * 을 클릭합니다.

사용자 지정 대시보드: 가상 머신 성능

OnCommand Insight의 맞춤형 대시보드와 위젯은 재고 및 성능 동향을 파악하는 데 도움이 됩니다.

이 작업에 대해

오늘날 IT 운영에는 많은 과제가 있습니다. 관리자는 더 적은 리소스로 더 많은 작업을 수행해야 하며, 동적 데이터 센터를 완벽하게 파악할 수 있어야 합니다. 이 예에서는 사용자 환경의 가상 머신 성능에 대한 운영 통찰력을 제공하는 위젯이 포함된 사용자 지정 대시보드를 만드는 방법을 보여 줍니다. 이 예제를 따르고 특정 요구 사항을 충족하기 위한 위젯을 생성하면 프런트엔드 가상 머신(VM) 성능과 비교하여 백엔드 스토리지 성능을 시각적으로 표시하거나, VM 지연 시간과 I/O 요구 사항을 확인할 수 있습니다.

맞춤형 대시보드를 통해 작업의 우선 순위를 지정하고 리소스 가용성을 파악할 수 있습니다. bb 및 워크로드 흐름에 대응하고 새로운 문제를 감지하고 해결하는 시간을 최소화할 수 있습니다. 맞춤형 대시보드를 통해 비즈니스 κρίITICAL 인프라에 대한 우선 순위 뷰를 유연하게 생성할 수 있으며, 여러 공급업체 기술에서 성능 가용성을 파악하는 데 유용합니다.

여기에서는 다음을 포함하는 Virtual Machine Performance 대시보드를 생성합니다.

- VM 이름 및 성능 데이터가 나열된 표
- VM 지연 시간과 스토리지 지연 시간을 비교한 차트
- VM의 읽기, 쓰기 및 총 IOPS를 보여 주는 차트
- VM의 최대 처리량을 보여 주는 차트입니다

이는 기본적인 예에 불과합니다. 운영 모범 사례를 목표로 선택한 성능 데이터를 강조하고 비교하기 위해 대시보드를 사용자 지정할 수 있습니다.

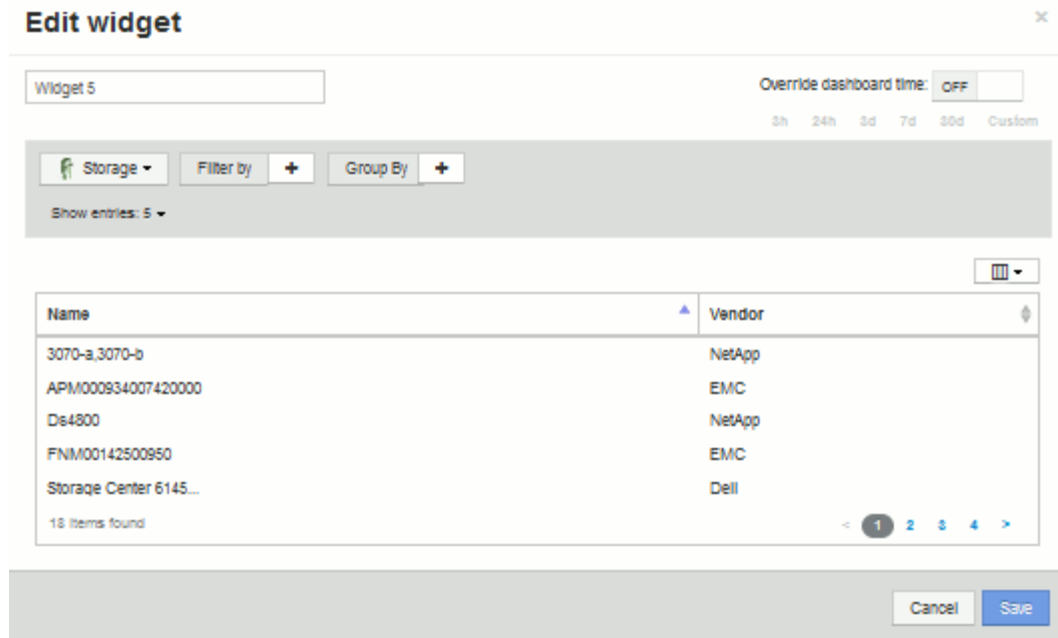
단계

1. 관리 권한이 있는 사용자로 Insight에 로그인합니다.
2. 대시보드 * 메뉴에서 * + 새 대시보드 * 를 선택합니다.

새 대시보드 페이지가 열립니다.


3. 대시보드의 이름을 의미 있는 이름으로 지정하겠습니다. 저장 * 을 클릭합니다. 이름 * 필드에 대시보드의 고유 이름 (예: ""응용 프로그램별 VM 성능"")을 입력합니다.
4. 대시보드를 새 이름으로 저장하려면 * 저장 * 을 클릭합니다.
5. 이제 위젯을 추가해 보겠습니다. 필요한 경우 * 편집 * 스위치를 ""켜짐""으로 밀어 편집 모드를 활성화합니다.
6. Widget * 버튼을 클릭하고 * Table widget * 을 선택하여 대시보드에 새 테이블 위젯을 추가합니다.

위젯 편집 대화 상자가 열립니다. 기본 이름은 ""Widget 1""이며, 표시된 기본 데이터는 사용자 환경의 모든 스토리지에 대한 것입니다.




7. 이 위젯을 사용자 지정할 수 있습니다. 이름 필드에서 ""Widget 1"을 삭제하고 ""가상 시스템 성능 테이블"을 입력합니다.
8. 자산 유형 드롭다운을 클릭하고 * Storage * 를 * Virtual Machine * 으로 변경합니다.

테이블 데이터가 변경되어 사용자 환경의 모든 가상 시스템이 표시됩니다. NOW의 경우 테이블에는 VM 이름만 표시됩니다. 표에 몇 개의 열을 추가해 보겠습니다.

9. 열 * 을 클릭합니다  버튼을 클릭하고 *Data Center*, 스토리지 이름 및 _IOPS - 합계_를 선택합니다. 검색에 이름을 입력하여 원하는 필드를 빠르게 표시할 수도 있습니다.

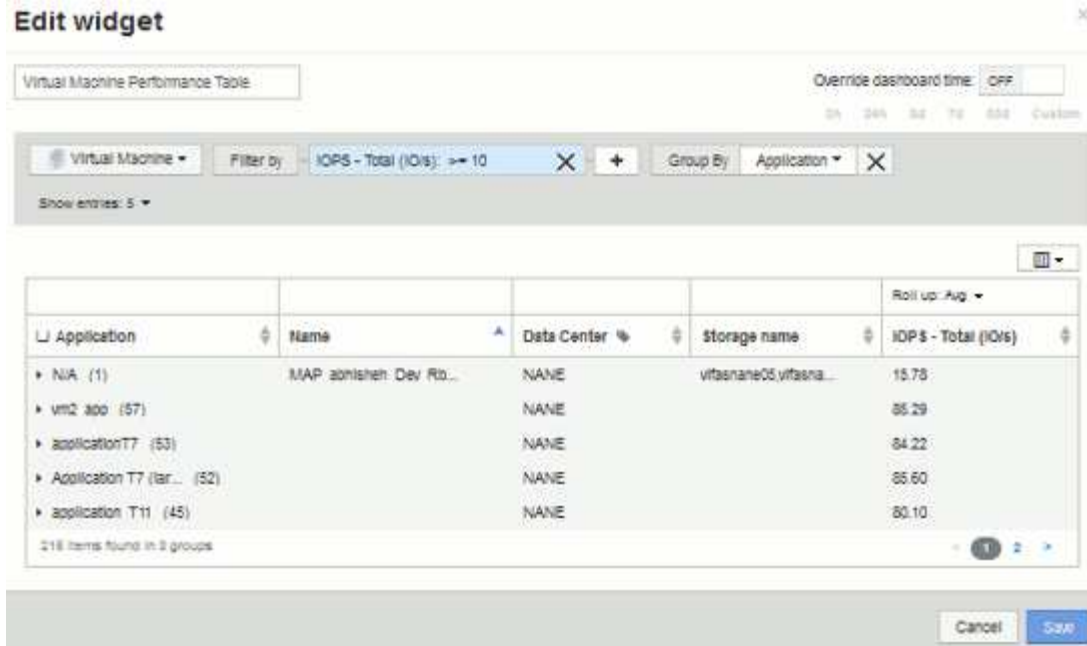
이제 이러한 열이 표에 표시됩니다. 이러한 열을 기준으로 테이블을 정렬할 수 있습니다. 열은 위젯에 추가된 순서대로 표시됩니다.

10. 이 실습에서는 사용 중이 아닌 VM을 제외하므로 총 IOPS가 10개 미만인 VM을 필터링하겠습니다. Filter by * 옆에 있는 "+" 버튼을 클릭하고 *IOPS - Total (IO/s)* 을(를) 선택합니다. 아무 * 나 * 를 클릭하고 * 보내는 사람 * 필드에 ""10""을 입력합니다. 받는 사람 * 필드는 비워 둡니다. 를 클릭합니다  버튼을 눌러 필터를 저장합니다.

이제 표에는 총 IOPS가 10개 이상인 VM만 표시됩니다.

11. 결과를 그룹화하여 테이블을 더 축소할 수 있습니다. Group By *(그룹화 기준) 옆의 "+" 버튼을 클릭하고 Application(애플리케이션) 또는 Cluster(클러스터) 등 그룹화할 필드를 선택합니다. 그룹화는 자동으로 적용됩니다.

이제 설정에 따라 표 행이 그룹화됩니다. 필요에 따라 그룹을 확장하고 축소할 수 있습니다. 그룹화된 행은 각 열에 대해 겹쳐서 표시된 데이터를 표시합니다. 일부 열을 사용하면 해당 열의 롤업 방법을 선택할 수 있습니다.



12. 표 위젯을 원하는 대로 사용자 정의했으면 * Save * (저장 *) 버튼을 클릭합니다.

테이블 위젯이 대시보드에 저장됩니다.

13. 오른쪽 아래 모서리를 끌어 대시보드에서 위젯의 크기를 조정할 수 있습니다. 위젯을 더 넓게 만들어 모든 열을 명확하게 표시합니다. Save * 를 클릭하여 현재 대시보드를 저장합니다.

14. 다음으로 몇 가지 차트를 추가하여 VM 성능을 보여 드리겠습니다. VM 지연 시간과 스토리지 지연 시간을 비교한 선형 차트를 만들어 보겠습니다.

15. 필요한 경우 * 편집 * 스위치를 ""켜짐""으로 밀어 편집 모드를 활성화합니다.

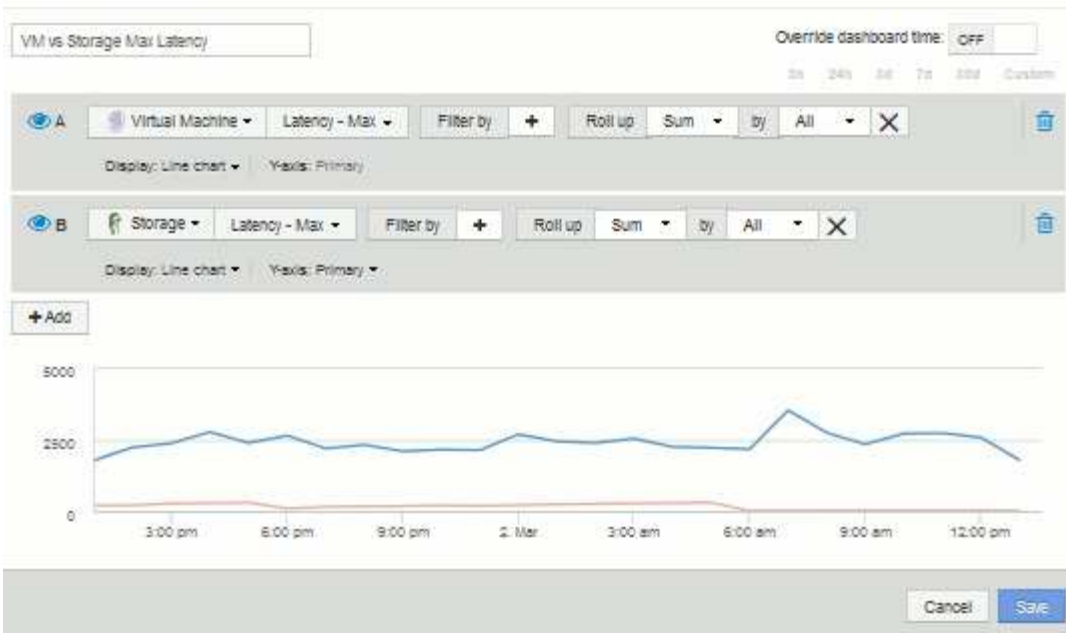
16. Widget * 버튼을 클릭하고 * Line Chart * 를 선택하여 대시보드에 새 선형 차트 위젯을 추가합니다.

위젯 편집 대화 상자가 열립니다. Name * 필드를 클릭하고 이 위젯 이름을 ""VM vs Storage Max Latency""로 지정합니다.

17. Virtual Machine * 을 선택하고 * Latency-Max * 를 선택합니다. 원하는 필터를 설정하거나 * Filter by * 를 비워 둡니다. Roll Up * 의 경우 "모두"로 "Sum"을 선택합니다. 이 데이터를 꺾은선형 차트로 표시하고 Y-축을 * 기본 * 으로 둡니다.

18. 두 번째 데이터 라인을 추가하려면 * + 추가 * 버튼을 클릭합니다. 이 행에 대해 * 스토리지 * 및 * 지연 시간 - 최대 * 를 선택합니다. 원하는 필터를 설정하거나 * Filter by * 를 비워 둡니다. Roll Up * 의 경우 "모두"로 "Sum"을 선택합니다. 이 데이터를 꺾은선형 차트로 표시하고 Y-축을 * 기본 * 으로 둡니다.

Edit widget



19. 이 위젯을 대시보드에 추가하려면 * 저장 * 을 클릭합니다.

20. 다음으로 단일 차트에서 VM 읽기, 쓰기 및 총 IOPS를 보여 주는 차트를 추가합니다.

21. Widget * 버튼을 클릭하고 * Area Chart * 를 선택하여 대시보드에 새 영역 차트 위젯을 추가합니다.

위젯 편집 대화 상자가 열립니다. 이름 * 필드를 클릭하고 이 위젯 이름을 ""VM IOPS""로 지정합니다.

22. Virtual Machine * 을 선택하고 * IOPS - Total * 을 선택합니다. 원하는 필터를 설정하거나 * Filter by * 를 비웁니다. Roll Up * 의 경우 "모두"로 "Sum"을 선택합니다. 이 데이터를 면적 도표 로 표시하고 Y축을 * 기본 * 으로 둡니다.

23. 추가 버튼을 클릭하여 두 번째 데이터 라인을 추가합니다. 이 행에 대해 * Virtual Machine * 을 선택하고 * IOPS - 읽기 * 를 선택합니다. Y축을 * 기본 * 으로 놉니다.

24. 추가 단추를 클릭하여 세 번째 데이터 행을 추가합니다. 이 행에 대해 * Virtual Machine * 을 선택하고 * IOPS-Write * 를 선택합니다. Y축을 * 기본 * 으로 놉니다.

Edit widget



25. 이 위젯을 대시보드에 추가하려면 * 저장 * 을 클릭합니다.

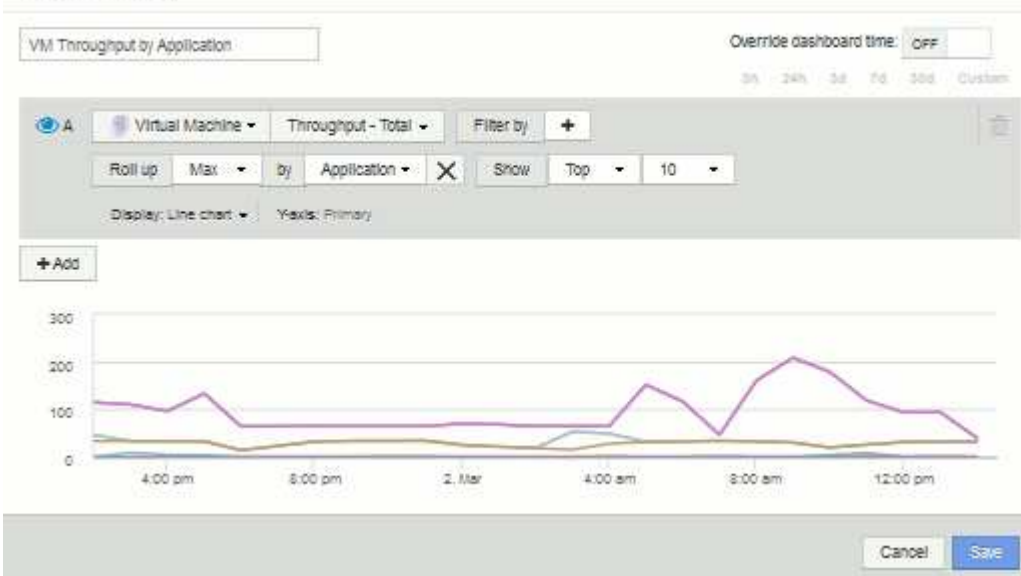
26. 다음으로 VM과 연결된 각 애플리케이션의 VM 처리량을 보여 주는 차트를 추가합니다. 이에 대해 롤업 기능을 사용할 것입니다.

27. Widget * 버튼을 클릭하고 * Line Chart * 를 선택하여 대시보드에 새 선형 차트 위젯을 추가합니다.

위젯 편집 대화 상자가 열립니다. 이름 * 필드를 클릭하고 이 위젯 이름을 ""애플리케이션별 VM 처리량""으로 지정합니다.

28. Virtual Machine * 을 선택하고 * Throughput - Total * 을 선택합니다. 원하는 필터를 설정하거나 * Filter by * 를 비워 둡니다. Roll Up * 의 경우 "Max"를 선택하고 "Application" 또는 "Name"을 선택합니다. 상위 10개 * 응용 프로그램을 표시합니다. 이 데이터를 꺾은선형 차트로 표시하고 Y-축을 * 기본 * 으로 둡니다.

Edit widget



29. 이 위젯을 대시보드에 추가하려면 * 저장 * 을 클릭합니다.

30. 위젯 상단의 아무 곳이나 마우스 버튼을 누른 채 새 위치로 드래그하여 위젯을 이동할 수 있습니다. 오른쪽 아래 모서리를 끌어 위젯 크기를 조정할 수 있습니다. 변경한 후에는 대시보드를 * 저장 * 해야 합니다.

최종 VM 성능 대시보드는 다음과 같습니다.



변수가 있는 스토리지 노드 활용률 대시보드 예

스토리지, 스토리지 풀, 노드, 계층, 사용률 및 지연 시간에 대한 변수가 있는 Storage Analysis에 대한 사용자 지정 대시보드를 생성합니다.

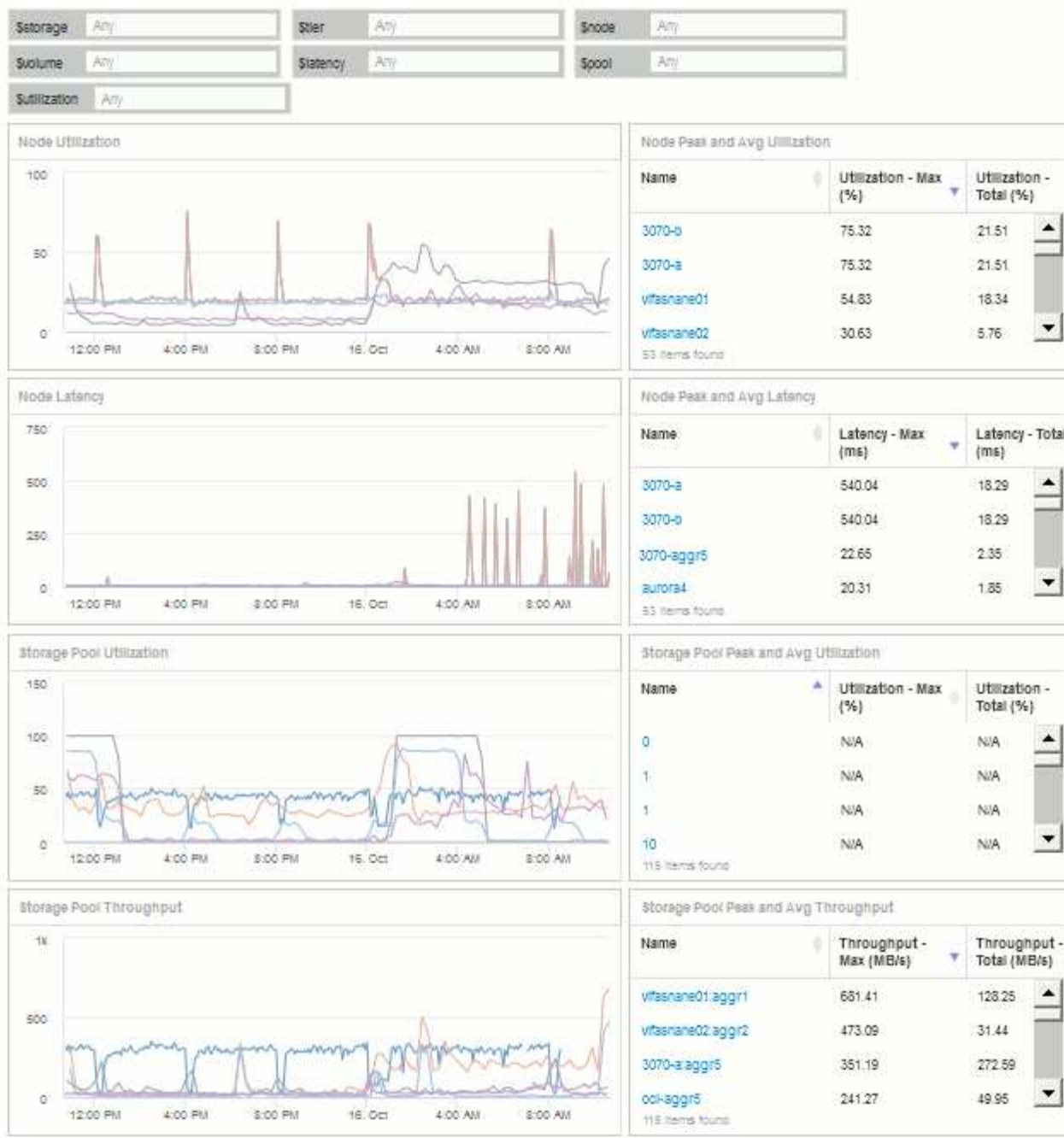
시작하기 전에

Insight의 대시보드에 익숙해지는 것이 좋지만 반드시 필요한 것은 아닙니다.

이 작업에 대해

다음 절차에서는 스토리지, 스토리지 풀, 노드, 계층, 사용률 및 지연 시간에 대한 변수를 사용하는 사용자 지정 스토리지 분석 개요 대시보드를 생성합니다. 아래 예제의 변수는 대시보드에서 사용할 수 있는 하나 이상의 위젯에서 표시된 자산 또는 메트릭을 필터링하는 데 사용됩니다. 이러한 변수를 필터로 사용하는 위젯은 대시보드의 변수 필드에 입력된 값에 따라 온디맨드 필터링 콘텐츠로 업데이트되므로 여러 차트와 그래프를 빠르게 필터링하여 특정 관심 영역으로 드릴다운할 수 있습니다.

이 예제의 단계를 따르면 다음과 같은 대시보드를 만들 수 있습니다. 이러한 위젯을 변경하거나 추가 위젯을 원하는 수만큼 추가하여 선택한 데이터를 강조 표시할 수 있습니다.



단계

1. 새 대시보드를 만들고 이름을 ""분석: 스토리지 개요"" 또는 동일한 설명이 포함된 것으로 지정합니다.
2. 변수 * 드롭다운을 클릭하고 * 텍스트 * 변수 유형을 선택합니다. 기본적으로 변수 이름은 `$var1`입니다. 이름을 편집하려면 `_ $var1`을(를) 클릭하고, 변수를 `_ $storage`로 변경한 다음 체크 표시를 클릭하여 변수를 저장합니다. 이 과정을 반복하여 `_ $node`, `$pool` 및 `_ $volume`에 대한 텍스트 변수를 생성합니다.
3. 위의 프로세스를 반복하여 `$Utilization_and$latency`라는 * Number * 유형 변수를 만듭니다.
4. Variable * (변수 *) 드롭다운을 클릭하고 `_ Tier_annotation`을 검색합니다. 이를 선택하여 `_ $tier`라는 변수를 만듭니다.

언제든지 변수를 추가할 수 있지만 변수를 미리 만들면 모든 위젯에서 변수를 만들 때 사용할 수 있습니다.

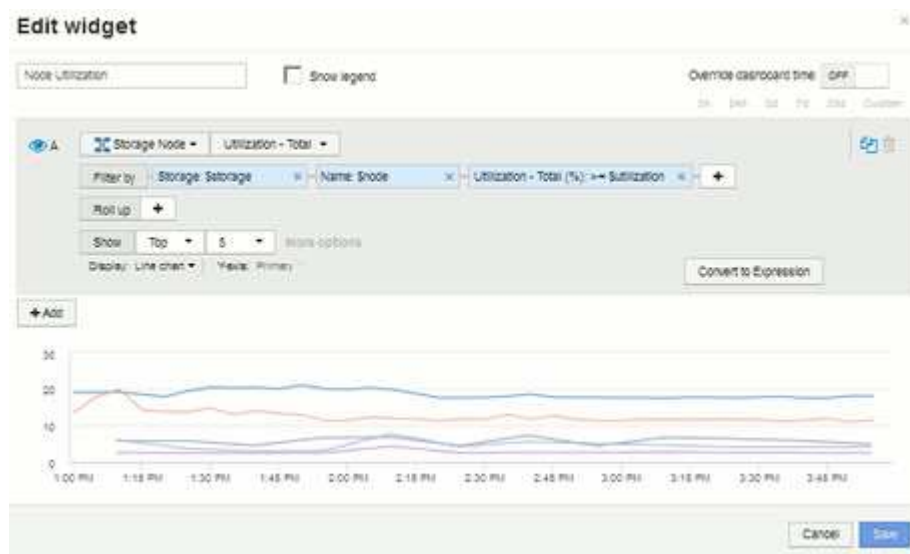
- Widget* 드롭다운을 클릭하고 꺾은선형 차트 또는 * 영역형 차트 * 위젯을 선택하여 위젯을 추가합니다. 위젯 이름을 "Node Utilization" 로 지정합니다. 스토리지 * 자산 유형을 클릭하고 * 스토리지 노드 * 로 변경합니다. 차트 데이터에 대해 * Utilization - Total * 을 선택합니다.
- 필터 기준 + * 버튼을 클릭하여 필터를 추가합니다. Storage * 를 검색하여 선택한 다음 * Any * 를 클릭하고 `$_storage_variable` 를 선택합니다.
- * 이름*에 대한 다른 필터를 추가하려면 + 단추를 클릭합니다. 변수를 `$_node_`로 설정합니다.

주석 이름 필터에 다른 변수를 지정할 수 있습니다. 위젯의 개체에 따라 가장 낮은 수준에서 이름/변수 쌍을 사용합니다. 예를 들면 다음과 같습니다.

- 노드 중심 위젯의 * 이름 * 필터에 `$_node_variable` 를 할당할 수 있습니다.
- 풀 중심 위젯에 대해 `$_pool_variable` 을 * Name * 필터에 할당할 수 있습니다.

- 사용률 - 합계(%)*에 대한 다른 필터를 추가하려면 + 버튼을 클릭합니다. 변수를 `_>=$Utilization_`로 설정합니다.
- 롤업 필드 뒤에 있는 * X * 를 클릭하여 필드를 축소합니다.
- 상위 5개 표시 * 를 선택하고 * 저장 * 을 클릭하여 위젯을 저장하고 대시보드로 돌아갑니다.

위젯은 다음과 같이 표시되어야 합니다.



- 대시보드에 다른 꺾은선형 또는 영역형 차트 위젯을 추가합니다. 자산 유형으로 * 스토리지 노드 * 를 선택하고 차트에 사용할 메트릭으로 * 지연 시간 - 합계 * 를 선택합니다.
- 필터 기준 + * 버튼을 클릭하여 * 스토리지:\$storage * 및 * Name:\$node * 에 대한 필터를 추가합니다.
- 지연 시간 - 합계 * 에 대한 필터를 추가하고 * \$ 지연 시간 * 변수를 선택합니다.
- 위젯 이름을 "Node Latency"로 지정하고 저장합니다.
- 최대 또는 평균 노드 사용률과 같이 생성한 차트에 대한 세부 정보를 표시하는 지원 테이블을 추가할 수 있습니다. 대시보드에 * 표 위젯 * 을 추가하고 자산 유형으로 * 스토리지 노드 * 를 선택하고 * 스토리지: \$storage *, * 이름: \$node * 및 * Utilization - Total: \$Utilization * 에 대한 필터를 생성합니다.
- Utilization - Max *, * Utilization - Total * 또는 기타 원하는 열에 대해 테이블에 열을 추가합니다.
- 위젯 이름을 "Node Peak and Avg Utilization"으로 지정하고 저장합니다.

Node Peak and Avg Utilization

Override dashboard time:

OFF

3h

24h

3d

7d

30d

Custom

Storage Node

Filter by

Storage: \$storage

Name: \$node

Utilization - Total (%): >= \$utilization

+

Group by

+

Name

Utilization - Max (%)

Utilization - Total (%)

3070-a	76.79	21.57
3070-b	76.79	21.57
vifasane01	54.83	18.55
vifasane02	32.50	6.06
aurora3	29.27	12.88

53 items found

Cancel

Save

- 이 단계를 반복하여 노드 지연 시간에 대한 테이블을 만듭니다. 이때 노드 지연 시간은 * Latency-Max *, * Latency-Total * 또는 기타 열을 원하는 대로 표시합니다.
- 대시보드를 둥글게 만들려면 다음 중 일부 또는 전체에 대해 차트 및 표 위젯을 더 추가할 수 있습니다.

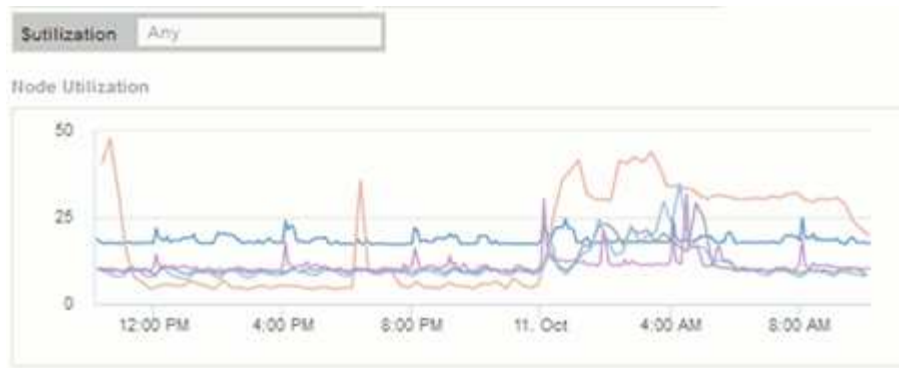
차트	표
스토리지 풀 활용률입니다	스토리지 풀 최대 및 평균 사용률
스토리지 풀 처리량입니다	스토리지 풀 최대 및 평균 처리량
볼륨 지연 시간	볼륨 최대 및 평균 지연 시간
볼륨 IOPS	볼륨 최대 및 평균 IOPS

- 대시보드에서 원하는 위치에 상관없이 위젯을 이동하고 크기를 조정할 수 있습니다. 완료되면 대시보드를 * 저장 * 합니다.
- 마지막 대시보드는 다음과 같습니다.



2. 변수를 사용하여 대시보드의 특정 자산에 집중할 수 있습니다. 변수 필드에 값을 입력하면 위젯이 자동으로 업데이트되어 해당 변수를 반영합니다. 예를 들어, \$Utilization 변수 필드에 "15"를 입력하면 해당 변수 업데이트를 사용하는 위젯이 전체 사용률이 15% 이상인 자산만 표시합니다.

모든 노드 중 상위 5개를 보여 주는 노드 활용률 위젯:



사용률이 15% 이상인 노드를 보여 주는 노드 활용률 위젯:



3. 위젯을 생성할 때는 다음 사항에 유의하십시오.

- \$tier 변수는 * Tier * 주석이 달린 리소스에만 영향을 줍니다.
- 위젯이 지정된 변수를 허용하도록 설계되었는지에 따라 일부 필터가 모든 위젯에 영향을 미치지 않습니다.
- 숫자 변수는 지정된 값 ""보다 크거나 같음""으로 적용됩니다. 변수가 위젯이 실행 중인 자산에 대해 유효한 경우 모든 변수를 스토리지 계층 구조의 모든 레벨에 있는 위젯의 필터로 사용할 수 있습니다. 노드 레벨에서 스토리지 풀로 볼륨 위젯으로 이동하는 경우 필터로 할당하기 위해 더 많은 변수가 존재합니다. 예를 들어, 스토리지 노드 레벨 위젯에서 *Storage* 및 *Name* 변수를 필터로 할당할 수 있습니다. 스토리지 풀 레벨에서 *Storage*, *Nodes*, *Storage Pools* 및 *_Name_*을 모두 사용할 수 있습니다. 변수를 적절하게 할당하고 스택의 가장 낮은 수준에서 \$NAME 변수를 사용합니다. 이렇게 하면 \$NAME 변수가 위젯이 실행 중인 자산의 실제 이름을 기준으로 필터링할 수 있습니다.

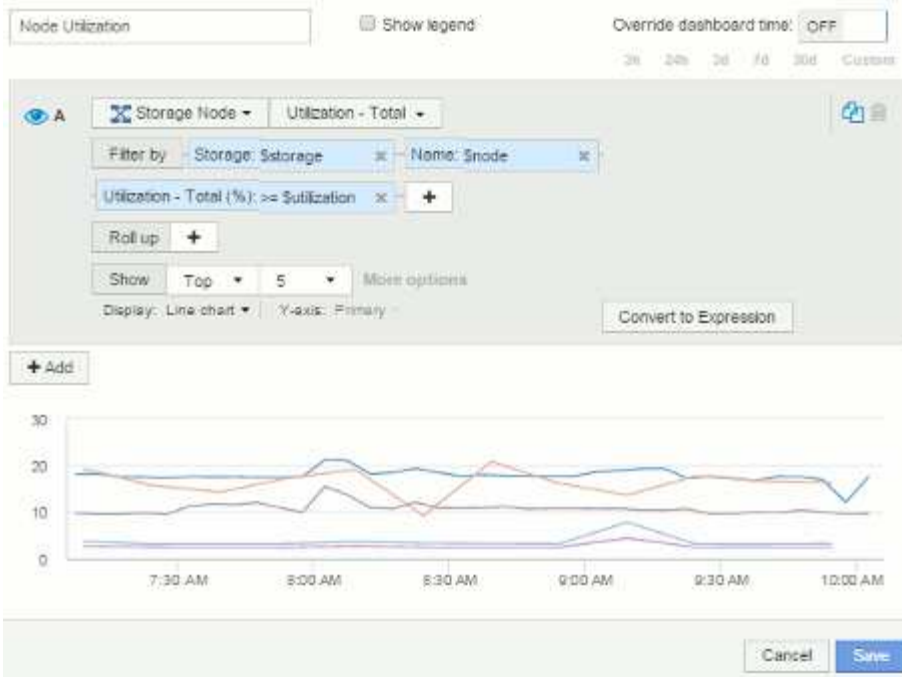
노드 대시보드 위젯 설정의 예

변수 예시가 있는 노드 대시보드의 위젯 설정

다음은 스토리지 노드 대시보드 예에 있는 각 위젯에 대한 설정입니다.

노드 활용률:

Edit widget



Edit widget

Node Peak and Avg Utilization Override dashboard time: OFF

3h 24h 3d 7d 30d Custom

Storage Node

Filter by: **Storage: \$storage** **Name: \$node** **Utilization - Total (%): >= \$utilization**

Group by: **+**

Name	Utilization - Max (%)	Utilization - Total (%)
3070-a	76.79	21.57
3070-b	76.79	21.57
vifasane01	54.83	18.55
vifasane02	32.50	6.06
aurora3	29.27	12.88

53 items found

Cancel Save

노드 지연 시간:

Edit widget

Node Latency

Show legend

Override dashboard time: OFF

3h24h3d7d30dCustom

Storage Node

Latency - Total

Filter by

Storage: \$storage

Name: \$node

Latency - Total (ms) >= \$latency

Roll up

Show

Top

5


More options

Display: Line chart

Y-axis: Primary

Convert to Expression

+ Add



Cancel

Save

Edit widget

Node Peak and Avg Latency

Override dashboard time: OFF

3h3m3d7d30dCustom

Storage Node

Filter by

Storage: \$storage

Name: \$node

Latency - Total (ms) >= \$latency

Group by

Name

Latency - Max (ms)

Latency - Total (ms)

vfasname04

9.05

7.70

vfasname05

2.25

0.41

vfasname02

1.62

0.90

vfasname01

1.42

1.03

vfasname06

0.97

0.64

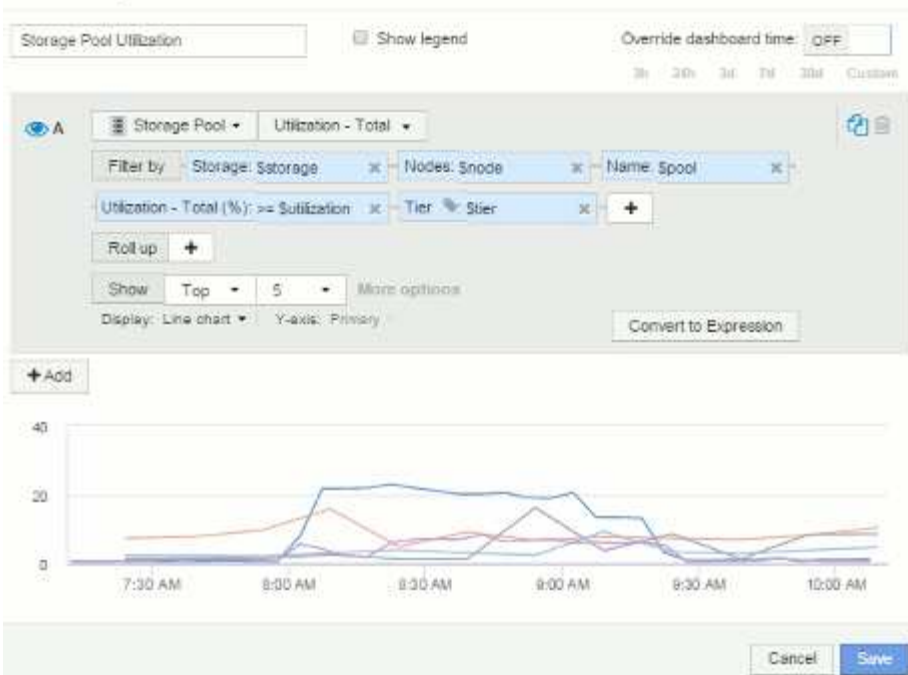
8 items found

Cancel

Save

스토리지 풀 사용률:

Edit widget



Edit widget

Storage Pool Peak and Avg Utilization

Override dashboard time:

3h 24h 3d 7d 30d Custom

Storage Pool

Filter by: Storage: \$storage x Nodes: \$node x Name: \$pool x

Utilization - Total (%) >= Utilization x Tier: \$tier x +

Group by: +

Utilization - Max (%) Utilization - Total (%)

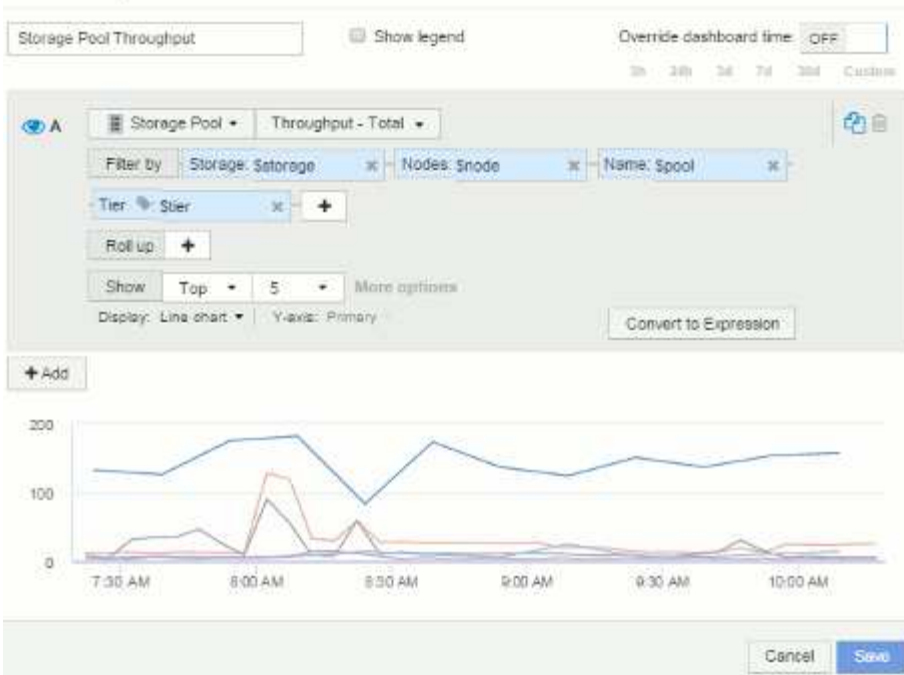
Name	Utilization - Max (%)	Utilization - Total (%)
vfasname01:aggr1	15.85	8.52
vfasname01:vfasna...	16.19	4.71
vfasname02:aggr2	9.28	3.65
vfasname02:vfasna...	4.96	1.63
vfasname03:aggr3	1.04	0.68

14 items found

Cancel Save

스토리지 풀 처리량:

Edit widget



Edit widget

Storage Pool Peak and Avg Throughput

Override dashboard time: OFF

3h 24h 3d 7d 30d Custom

Storage Pool

Filter by: Storage: \$storage x Nodes: \$node x Name: \$pool x

Tier: \$tier x +

Group by: +

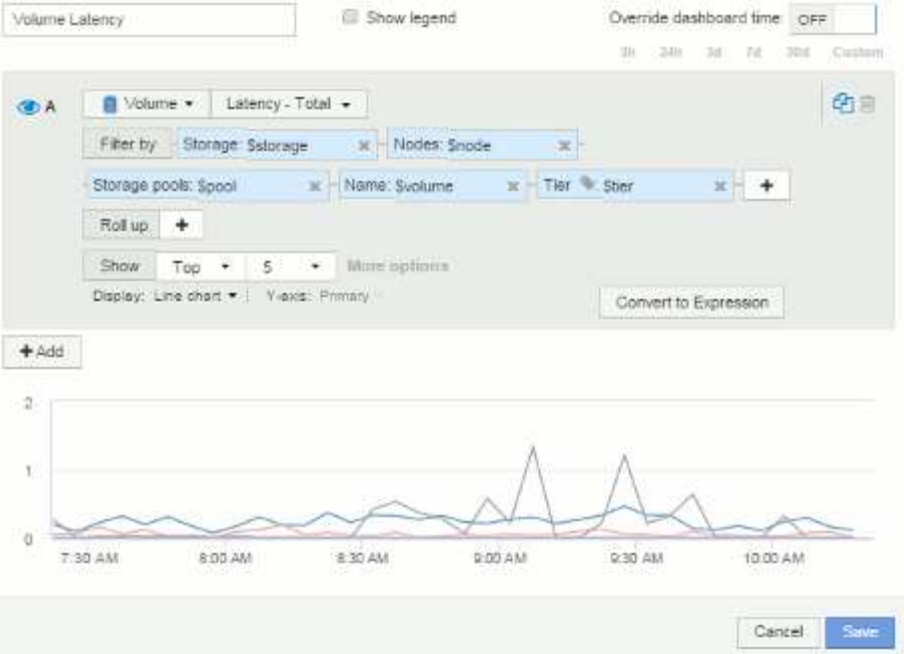
Name	Throughput - Max (MB/s)	Throughput - Total (MB/s)
vfasname01:aggr1	181.17	143.62
vfasname06:aggr1	127.19	26.75
vfasname05:aggr1	89.83	18.20
vfasname02:aggr2	24.57	9.70
vfasname05:aggr_opm1	14.61	4.75

14 items found

Cancel Save

블룸 지연 시간:

Edit widget



Edit widget

Volume Peak and Avg Latency

Override dashboard time: OFF

3h 24h 3d 7d 30d Custom

Volume

Filter by: Storage: \$storage Nodes: \$node Storage pools: \$pool

Name: \$volume Latency - Total (ms) >= Latency Tier: \$tier

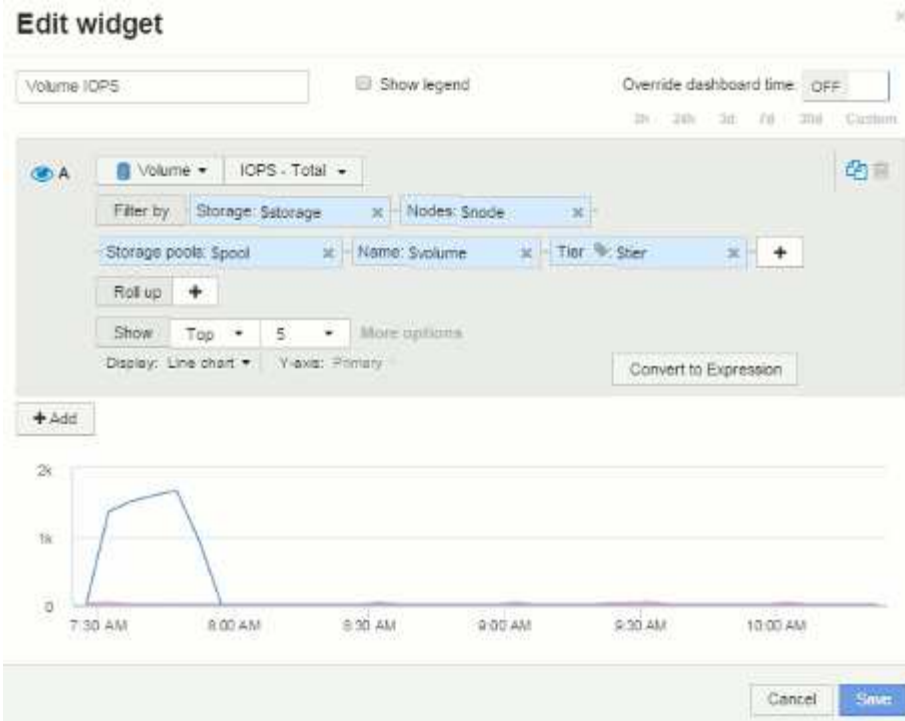
Group by: +

Name	Latency - Max (ms)	Latency - Total (ms)
vfasname05/vol/bo...	0.00	0.00
vfasname05/vol/bo...	0.19	0.06
vfasname05/vol/bo...	0.00	0.00
vfasname05/vol/bo...	0.00	0.00
vfasname05/vol/bo...	0.00	0.00

51 items found

Cancel Save

블룸 IOPS:



Edit widget

Volume Peak and Avg IOPS Override dashboard time: OFF

3h 24h 3d 7d 30d Custom

Configuration:

- Volume: Volume
- Filter by: Storage: Sstorage, Nodes: Snode, Storage pools: Spool, Name: Svolume, Tier: Stier
- Group by: +

Table Data:

Name	IOPS - Max (IO/s)	IOPS - Total (IO/s)
vfasname05/vol/vl...	1,089.31	198.97
vfasname05/vol/vl...	50.03	19.18
vfasname05/vol/bo...	1.51	1.11
vfasname05/vol/bo...	0.00	0.00
vfasname06/vol/bo...	0.00	0.00

31 items found

Buttons: Cancel, Save


대시보드 및 위젯에 대한 모범 사례

대시보드와 위젯의 강력한 기능을 최대한 활용할 수 있도록 도와주는 팁과 요령.

모범 사례: 올바른 메트릭 찾기

OnCommand Insight는 때때로 데이터 소스에서 데이터 소스까지 다른 이름을 사용하여 카운터 및 메트릭을 획득합니다.

대시보드 위젯에 대한 적절한 메트릭이나 카운터를 검색할 때 원하는 메트릭이 생각하려는 메트릭과 다른 이름으로 표시될 수 있다는 점에 유의하십시오. OnCommand Insight의 드롭다운 목록은 대개 사전순 목록이지만, 경우에 따라 필요할 것으로 생각되는 목록에 용어가 나타나지 않을 수 있습니다. 예를 들어 "물리적 용량" 및 "사용된 용량"과 같은 용어는 대부분의 목록에 함께 나타나지 않습니다.

모범 사례: * 필터 기준 * 과 같은 필드 또는 열 선택기와 같은 위치에 검색 기능을 사용하십시오  원하는 것을 찾을 수 있습니다. 예를 들어 "CAP"를 검색하면 발생 위치에 관계없이 이름에 "capacity"가 있는 모든 메트릭이 표시됩니다. 그런 다음 해당 간단한 목록에서 원하는 메트릭을 쉽게 선택할 수 있습니다.

메트릭을 검색할 때 다음과 같은 몇 가지 대체 문구를 사용할 수 있습니다.

찾을 내용:	다음을 검색해 보십시오.
CPU	프로세서
용량	사용된 용량 물리적 용량입니다 용량을 프로비저닝합니다 스토리지 풀 용량입니다 <other asset type> 용량 쓰인 용량
디스크 속도	최저 디스크 속도디스크 유형을 수행하는 중입니다
호스트	하이퍼visorHosts 를 선택합니다
하이퍼바이저	하이퍼바이저 호스트
마이크로코드	펌웨어
이름	AliasHypervisor 이름입니다 스토리지 이름입니다 <other asset type> 이름입니다 간단한 이름 리소스 이름입니다 패브릭 별칭

읽기/쓰기	부분 R/WPending 쓰기 IOPS - 쓰기 쓰인 용량 지연 시간 - 읽기 캐시 활용률 - 읽기
가상 머신	VMI 가상

이것은 포괄적인 목록이 아닙니다. 다음은 가능한 검색어의 예일 뿐입니다.

모범 사례: 적합한 자산 찾기

위젯 필터 및 검색에서 참조할 수 있는 Insight 자산은 자산 유형에 따라 다릅니다.

대시보드에서 위젯을 구성하는 자산 유형에 따라 열을 필터링하거나 추가할 수 있는 다른 자산 유형 카운터가 결정됩니다. 위젯을 구축할 때는 다음 사항에 유의하십시오.

이 자산 유형/카운터:	다음 자산에서 필터링할 수 있습니다.
가상 머신	VMDK입니다
데이터 저장소	내부 VolumeVMDK 가상 머신 볼륨
하이퍼바이저	가상 머신
하이퍼바이저입니다	호스트
호스트	내부 볼륨
클러스터	호스트 가상 시스템
패브릭	포트

이것은 포괄적인 목록이 아닙니다.

모범 사례: 목록에 나타나지 않는 특정 자산 유형을 필터링하는 경우 대체 자산 유형에 대한 쿼리를 작성합니다.

산점도 예: 축 이해

산점도 위젯의 카운터 순서를 변경하면 데이터가 표시되는 축이 변경됩니다.

이 작업에 대해

이 예에서는 낮은 IOPS에 비해 지연 시간이 긴 성능 미달 VM을 볼 수 있는 산란 플롯을 작성합니다.

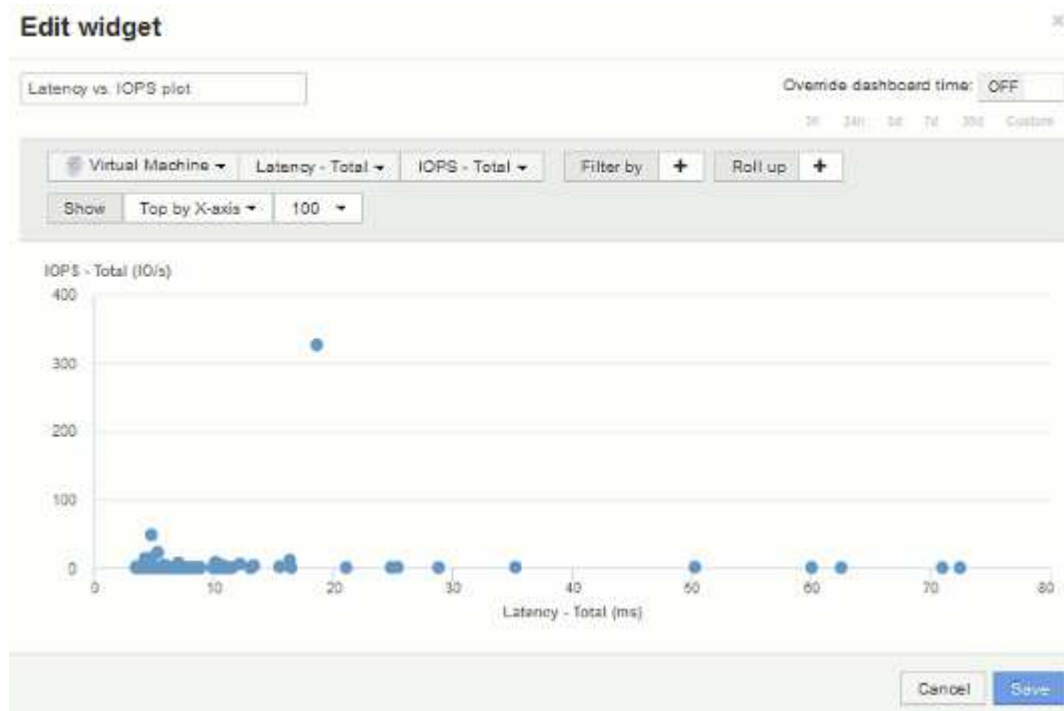
단계

1. 편집 모드에서 대시보드를 만들거나 열고 * Scatter Plot Chart * 위젯을 추가합니다.
2. 자산 유형을 선택합니다(예: * Virtual Machine *).
3. 플롯할 첫 번째 카운터를 선택합니다. 이 예에서는 * Latency - Total * 을 선택합니다.

_Latency - Total_은 차트의 X축을 따라 차트로 작성됩니다.

4. 플롯할 두 번째 카운터를 선택합니다. 이 예에서는 * IOPS - Total * 을 선택합니다.

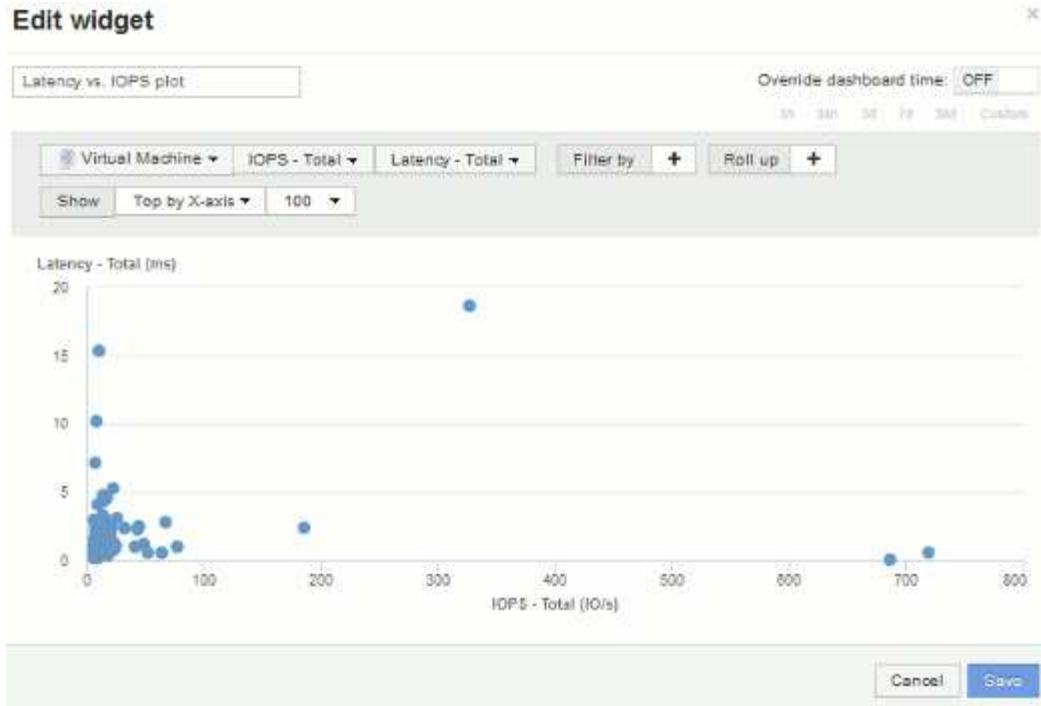
_IOPS - Total_은 차트의 Y축을 따라 차트로 작성됩니다. 지연 시간이 긴 VM은 차트 오른쪽에 표시됩니다. 상위 100개 지연 시간이 가장 긴 VM만 표시됩니다. * X축 기준 상위 * 설정이 최신이기 때문입니다.



5. 이제 첫 번째 카운터를 * IOPS - Total * 으로 설정하고 두 번째 카운터를 * Latency - Total * 로 설정하여 카운터 순서를 거꾸로 바꿉니다.

_latency-Total_은 이제 차트의 Y축을 따라 차트로 작성되고 X축을 따라 *IOPS-Total*이 작성됩니다. IOPS가 높은 VM이 이제 차트 오른쪽에 표시됩니다.

X-Axis * 설정으로 * Top을 변경하지 않았기 때문에 위젯은 현재 X축을 따라 플롯된 것이므로 상위 100개의 가장 높은 IOPS VM을 표시합니다.



6. 차트에 X축 기준 N 상단, Y축 기준 N 상단, X축 기준 N 하단 또는 Y축 기준 N 하단 을 표시하도록 선택할 수 있습니다. 마지막 예에서는 가장 높은_총 IOPS_를 가진 상위 100개 VM을 표시합니다. Y축을 기준으로 위로 변경하면 차트에 _total latency_가 가장 높은 상위 100개 VM이 다시 표시됩니다.

산점도 차트에서 지점을 클릭하여 해당 리소스의 자산 페이지를 열 수 있습니다.

성능 정책 생성 중

성능 정책을 생성하여 네트워크 리소스와 관련된 문제를 알리기 위해 알림을 트리거하는 임계값을 설정합니다. 예를 들어, 스토리지 풀의 총 활용률이 60%를 초과할 경우 알림을 보낼 성능 정책을 생성할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 엽니다.
2. Manage * > * Performance Policies * 를 선택합니다.

성능 정책 페이지가 표시됩니다

Performance Policies

[Add new policy](#)

Database policies

Policy Name	Severity	Annotations	Time Window	Thresholds
Latency	Warning		First occurrence	'Latency - Total' > 200 ms
Databases_0	Warning		First occurrence	'IOPS - Total' > 0 I/Os or 'Latency - Total' > 0 ms

Showing 1 to 2 of 2 entries

Internal volume policies

Policy Name	Severity	Annotations	Time Window	Thresholds
Atmos Service Level	Critical	Service_Level = Atmos	First occurrence	'Latency - Total' > 100 ms or 'IOPS - Total' > 100 I/Os or 'Throughput - Total' > 200 MB/s
Global	Critical		First occurrence	'Latency - Total' > 200 ms or 'IOPS - Total' > 1 I/Os or 'Throughput - Total' > 300 MB/s

Showing 1 to 2 of 2 entries

Storage policies

Policy Name	Severity	Annotations	Time Window	Thresholds
Storage_Storage	Warning		First occurrence	'IOPS - Read' > 10 I/Os
Storage_0	Warning		First occurrence	'Throughput - Total' > 0 MB/s or 'IOPS - Total' > 0 I/Os

Showing 1 to 2 of 2 entries

정책은 객체별로 구성되며 해당 객체의 목록에 나타나는 순서대로 평가됩니다.

3. 새 정책 추가 * 를 클릭합니다.

정책 추가 대화 상자가 표시됩니다.

4. Policy name * 필드에 정책 이름을 입력합니다.

개체의 다른 모든 정책 이름과 다른 이름을 사용해야 합니다. 예를 들어, 내부 볼륨에 대해 "지연 시간"이라는 두 가지 정책을 사용할 수는 없지만, 내부 볼륨에 대해 "지연 시간" 정책과 다른 볼륨에 대해 "지연 시간" 정책을 사용할 수 있습니다. 가장 좋은 방법은 개체 유형에 관계없이 모든 정책에 대해 항상 고유한 이름을 사용하는 것입니다.

5. Type * 의 개체에 적용 목록에서 정책이 적용되는 개체 유형을 선택합니다.

6. With annotation * (주석 포함 *) 목록에서 주석 유형을 선택하고, 해당되는 경우 * Value * (값 *) 상자에 주석 값을 입력하여 이 특정 주석 세트가 있는 개체에만 정책을 적용합니다.

7. 객체 유형으로 * Port * 를 선택한 경우 * Connected to * 목록에서 포트가 연결된 대상을 선택합니다.

8. [다음 창 뒤에 적용]목록에서 임계값 위반을 나타내기 위해 경고를 표시할 시기를 선택합니다.

첫 번째 발생 옵션은 첫 번째 데이터 샘플에서 임계값이 초과되면 알림을 트리거합니다. 다른 모든 옵션은 임계값을 한 번 넘어섰을 때 경고를 발생시키고 지정된 시간 이상 연속적으로 교차하는 경우에 발생합니다.

9. with severity * 목록에서 위반 심각도를 선택합니다.

10. 기본적으로 정책 위반에 대한 전자 메일 알림이 글로벌 전자 메일 목록의 받는 사람에게 전송됩니다. 특정 정책에 대한 알림이 특정 수신자에게 전송되도록 이러한 설정을 재정의할 수 있습니다.

- 링크를 클릭하여 받는 사람 목록을 연 다음 * + * 버튼을 클릭하여 받는 사람을 추가합니다. 해당 정책에 대한 위반 알림은 목록의 모든 수신자에게 전송됩니다.

11. 다음 중 하나라도 참인 경우 * 알림 생성 섹션에서 * 임의 * 링크를 클릭하여 알림 트리거 방법을 제어합니다.

- * 모두 *

이 설정은 정책과 관련된 임계값 중 하나라도 넘을 경우 알림을 생성하는 기본 설정입니다.

◦ * 모두 *

이 설정은 정책에 대한 모든 임계값을 초과할 때 알림을 생성합니다. All * 을 선택하면 성능 정책에 대해 생성한 첫 번째 임계값을 기본 규칙이라고 합니다. 기본 규칙 임계값이 성능 정책에 대해 가장 우려되는 위반인지 확인해야 합니다.

12. Create alert if * 섹션에서 성능 카운터와 연산자를 선택한 다음 값을 입력하여 임계값을 생성합니다.

13. 임계값을 더 추가하려면 * Add threshold * (임계값 추가)를 클릭합니다.

14. 임계값을 제거하려면 휴지통 아이콘을 클릭합니다.

15. 경고 발생 시 정책 처리를 중지하려면 * 알림이 생성되면 추가 정책 처리 중지 * 확인란을 선택합니다.

예를 들어, 데이터 저장소에 대한 정책이 4개 있고 경고가 발생할 때 처리를 중지하도록 두 번째 정책이 구성된 경우 두 번째 정책 위반이 활성화되어 있는 동안에는 세 번째 정책과 네 번째 정책이 처리되지 않습니다.

16. 저장 * 을 클릭합니다.

성능 정책 페이지가 표시되고 성능 정책이 개체 유형에 대한 정책 목록에 표시됩니다.

성능을 구성하고 위반 알림을 확인합니다

OnCommand Insight는 성능 관련 알림을 지원하고 위반을 보장합니다. 기본적으로 Insight는 이러한 위반에 대한 알림을 보내지 않습니다. Insight에서 이메일을 보내거나, syslog 메시지를 syslog 서버로 보내거나, 위반이 발생할 경우 SNMP 알림을 보내도록 구성해야 합니다.

시작하기 전에

위반에 대한 e-메일, syslog 및 SNMP 전송 방법을 구성해야 합니다.

단계

1. 관리자 * > * 알림 * 을 클릭합니다.

2. 이벤트 * 를 클릭합니다.

3. 성능 위반 이벤트 * 또는 * 위반 이벤트 보증 * 섹션에서 원하는 알림 방법(* 이메일 , * Syslog * 또는 * SNMP *) 목록을 클릭하고 위반의 심각도 수준(경고 이상 * 또는 * 긴급 *)을 선택합니다.

4. 저장 * 을 클릭합니다.

네트워크 위반 모니터링

Insight에서 성능 정책에 설정된 임계값으로 인해 위반을 생성하는 경우 위반 대시보드를 사용하여 해당 위반 사항을 볼 수 있습니다. 대시보드에는 네트워크에서 발생하는 모든 위반 사항이 나열되며 이를 통해 문제를 찾아 해결할 수 있습니다.

단계

1. 브라우저에서 OnCommand Insight를 엽니다.
2. Insight 도구 모음에서 * 대시보드 * 를 클릭하고 * 위반 대시보드 * 를 선택합니다.

위반 대시보드가 표시됩니다.

3. Policies * 파이 차트에서는 다음과 같은 방법으로 * 위반 항목을 사용할 수 있습니다.
 - 특정 정책 또는 메트릭에 대해 발생한 총 위반의 비율을 표시하기 위해 차트의 임의 슬라이스 위에 커서를 배치할 수 있습니다.
 - 차트의 한 조각을 "확대"하려면 차트 조각을 클릭하면 나머지 차트에서 멀리 이동하여 해당 슬라이스를 더 강조하고 연구할 수 있습니다.
 - 를 클릭할 수 있습니다. 아이콘을 클릭하여 원형 차트를 전체 화면 모드로 표시하고 을 클릭합니다. 다시 한 번 클릭하여 원형 차트를 최소화합니다. 파이 차트는 최대 5개의 조각을 포함할 수 있으므로 위반을 생성하는 6개의 정책이 있는 경우 Insight는 5번째 슬라이스와 6번째 슬라이스를 ""기타" 슬라이스로 결합합니다. Insight는 가장 많은 위반 사항을 첫 번째 슬라이스에 할당하고 두 번째 슬라이스에 가장 많은 위반 사항을 할당합니다.

4. 다음과 같은 방법으로 * 위반 이력 * 차트를 사용할 수 있습니다.

- 차트 위에 커서를 놓으면 특정 시간에 발생한 총 위반 수와 지정된 각 메트릭에 대해 발생한 총 위반 횟수를 표시할 수 있습니다.
- 범례 레이블을 클릭하여 범례와 관련된 데이터를 차트에서 제거할 수 있습니다.

범례를 클릭하여 데이터를 다시 표시합니다.

- 를 클릭할 수 있습니다. 아이콘을 클릭하여 차트를 전체 화면 모드로 표시하고 을 클릭합니다. 다시 한 번 클릭하여 원형 차트를 최소화합니다.

5. 다음과 같은 방법으로 * 위반 표 * 를 사용할 수 있습니다.

- 를 클릭할 수 있습니다. 아이콘을 클릭하여 전체 화면 모드로 테이블을 표시하고 을 클릭합니다. 다시 한 번 클릭하여 원형 차트를 최소화합니다.

창 크기가 너무 작은 경우 위반 테이블에는 세 개의 열만 표시되지만 을 클릭하면 표시됩니다, 추가 열(최대 7개)이 표시됩니다.

- 특정 기간(* 1h *, * 3h *, * 24h *, * 3D *, * 7d *, 및 * 30d *), Insight에서 선택한 기간 동안 최대 1000건의 위반 사례를 보여줍니다.
- 필터 * 상자를 사용하여 원하는 위반만 표시할 수 있습니다.
- 열 머리글의 화살표를 클릭하여 테이블의 열 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다. 기본 정렬 순서로 돌아가려면 다른 열 머리글을 클릭합니다.

기본적으로 테이블에는 위반사항이 내림차순으로 표시됩니다.

- ID 열에서 위반을 클릭하여 위반 기간 동안 자산 페이지를 표시할 수 있습니다.
- 설명 열에서 리소스 링크(예: 스토리지 풀 및 스토리지 볼륨)를 클릭하여 해당 리소스와 연결된 자산 페이지를 표시할 수 있습니다.
- 정책 열에서 성능 정책 링크를 클릭하여 정책 편집 대화 상자를 표시할 수 있습니다.

너무 많거나 너무 많은 위반이 발생하는 경우 정책의 임계값을 조정할 수 있습니다.

- 한 페이지에 맞는 것보다 많은 데이터가 있는 경우 페이지 번호를 클릭하여 페이지별로 데이터를 탐색할 수 있습니다.
- 를 클릭할 수 있습니다 ✕ 을 클릭하여 위반 사항을 취소합니다.

Fibre Channel BB 크레딧 0 오류 문제 해결

파이버 채널은 BB 크레딧(Buffer-to-Buffer 크레딧)을 사용하여 전송 흐름을 제어합니다. 포트에서 프레임이 전송되면 크레딧 값이 감소하고 포트에서 응답을 받으면 크레딧 값이 보충됩니다. 포트의 BB 크레딧을 보충하지 않으면 전송 흐름에 영향을 줄 수 있습니다. 포트가 순서대로 조립되어 전달될 때까지 프레임을 임시로 저장하려면 메모리 또는 버퍼가 필요합니다. 버퍼 수는 포트가 저장할 수 있는 프레임 수이며 버퍼 크레딧이라고 합니다.

지정된 포트 접근 0에 대해 사용 가능한 크레딧으로, 0에 도달하면 포트에서 전송 수신을 중지하고 BB 크레딧을 보충할 때까지 다시 시작하지 않는다는 경고가 표시됩니다.

Insight 성능 정책을 사용하면 다음 포트 메트릭에 대한 임계값을 설정할 수 있습니다.

BB 크레딧 제로 Rx
샘플링 기간 동안 수신 버퍼 대 버퍼 크레딧 수가 0으로 전환된 횟수입니다
BB 크레딧 0 - Tx
샘플링 기간 동안 전송 버퍼 대 버퍼 크레딧 수가 0으로 전환된 횟수입니다
BB 크레딧 없음 - 합계
연결된 포트가 제공할 수 있는 크레딧이 없기 때문에 이 포트가 전송을 중지해야 하는 횟수입니다
BB 크레딧 없음 기간 - Tx
샘플링 간격 동안 Tx BB 크레딧이 0인 시간(밀리초)입니다

BB 크레딧 오류는 다음과 같은 경우에 발생할 수 있습니다.

- 지정된 구축 환경에서 FC 프레임의 비율이 최대 크기보다 훨씬 작을 경우 더 많은 BB 크레딧이 필요할 수 있습니다.
- 스토리지 노드와 같이 포트에 연결된 장치 또는 포트에 영향을 줄 수 있는 환경의 워크로드 변경

패브릭, 스위치 및 포트 자산 페이지를 사용하여 파이버 채널 환경을 모니터링할 수 있습니다. 포트 자산 페이지는 리소스, 해당 토폴로지(장치 및 연결), 성능 차트 및 관련 리소스 표에 대한 요약 정보를 제공합니다. Fibre Channel 문제를 해결할 때 각 포트 자산에 대한 성능 차트는 선택한 최상위 기여 포트의 트래픽을 보여 주기 때문에 유용합니다. 또한 포트 자산 페이지에는 버퍼 대 버퍼 크레딧 메트릭과 포트 오류가 이 차트에 표시되며 Insight는 각 메트릭에 대한 별도의 성능 차트를 표시합니다.

포트에 대한 성능 정책 및 임계값 생성

포트에 연결된 메트릭에 대한 임계값을 사용하여 성능 정책을 생성할 수 있습니다. 기본적으로 성능 정책은 지정된 유형의 모든 디바이스를 생성할 때 적용됩니다. 성능 정책에 특정 장치 또는 장치 집합만 포함하도록 주석을 만들 수 있습니다. 이 절차에서는 간단한 방법으로 주석을 사용하지 않습니다.

시작하기 전에

이 성능 정책과 함께 주석을 사용하려면 성능 정책을 만들기 전에 주석을 만들어야 합니다.

단계

1. Insight 도구 모음에서 * 관리 * > * 성능 정책 * 을 클릭합니다

기존 정책이 표시됩니다. 스위치 포트에 대한 정책이 있는 경우 기존 정책을 편집하여 새 정책 및 임계값을 추가할 수 있습니다.

2. 기존 포트 정책을 편집하거나 새 포트 정책을 생성합니다

- 기존 정책의 맨 오른쪽에 있는 연필 아이콘을 클릭합니다. "" 및 ""e"" 단계에서 설명한 임계값을 추가합니다.
- 새 정책을 추가하려면 * + 추가 * 를 클릭합니다
 - i. "정책 이름" 추가: 저속 방전 장치
 - ii. 포트를 개체 유형으로 선택합니다
 - iii. 의 ""다음 창 적용""에 대한 첫 번째 항목을 입력합니다
 - iv. 임계값: BB 크레딧 제로 - Rx > 1,000,000을 입력합니다
 - v. 임계값: BB 크레딧 제로 - Tx > 1,000,000을 입력합니다
 - vi. '경고가 생성되면 추가 정책 처리 중'을 클릭합니다.
 - vii. "저장"을 클릭합니다.

생성하는 정책은 24시간 동안 설정한 임계값을 모니터링합니다. 임계값을 초과하면 위반이 보고됩니다.

3. 대시보드 * > * 위반 대시보드 * 를 클릭합니다

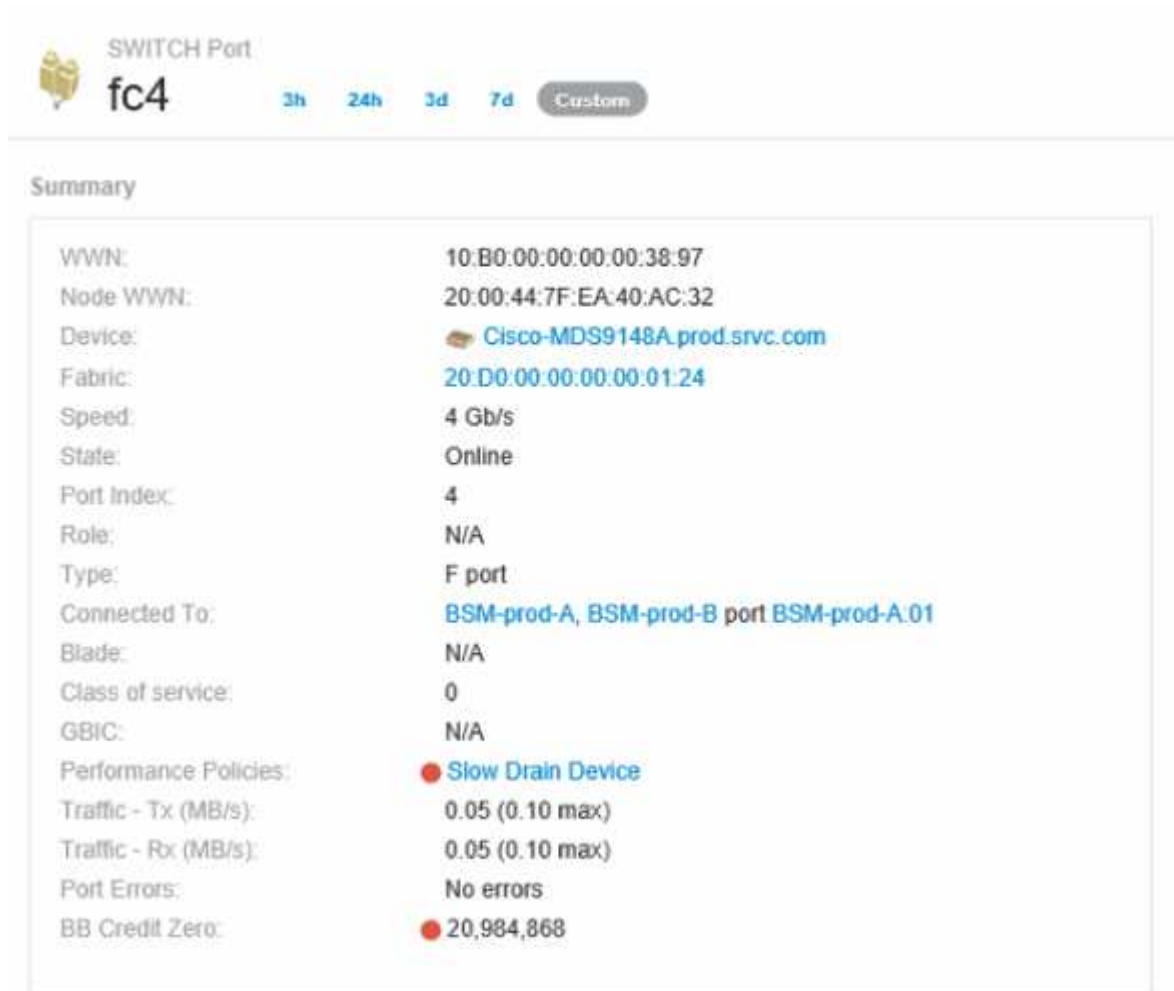
시스템에서 발생한 모든 위반 사항이 표시됩니다. '저배액기' 위반 사항을 보기 위해 위반 사항을 검색하거나 정렬합니다. 위반 대시보드에는 성능 정책에 설정된 임계값을 초과하는 BB Credit 0 오류가 발생한 모든 포트가 표시됩니다. 위반 대시보드에서 식별된 각 스위치 포트는 포트 랜딩 페이지에 대한 강조 표시된 링크입니다.

4. 강조 표시된 포트 링크를 클릭하여 포트 랜딩 페이지를 표시합니다.

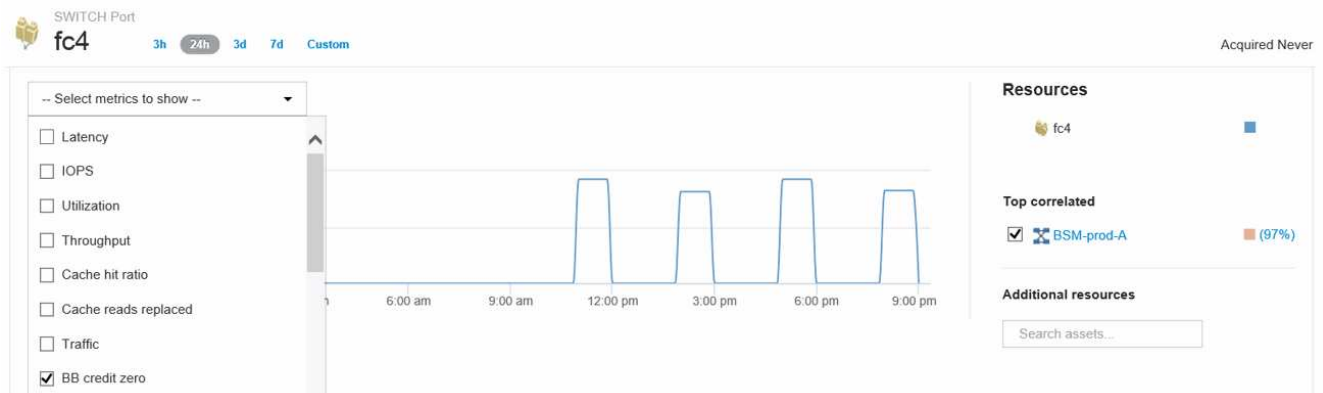
포트 랜딩 페이지가 표시되며 BB Credit 0 문제 해결에 유용한 정보가 포함되어 있습니다.

- 포트가 연결된 장치
- Fibre Channel 스위치 포트인 위반을 보고하는 포트의 ID입니다.
- 포트의 속도입니다
- 연결된 노드 및 포트

이름입니다



5. 아래로 스크롤하여 포트 메트릭을 확인합니다. 표시할 메트릭 선택 * > * BB 크레딧 없음 * 을 클릭하여 BB 크레딧 그래프를 표시합니다.



6. Top Correlated * 를 클릭합니다

상호 연결된 최상위 리소스 분석에서는 포트가 성능과 가장 상호 연결된 리소스로 서비스 중인 연결된 컨트롤러 노드를 보여줍니다. 이 단계에서는 포트 활동의 IOPS 메트릭을 전체 노드 작업과 비교합니다. 디스플레이에 Tx 및 Rx BB Credit Zero 메트릭과 컨트롤러 노드의 IOPS가 표시됩니다. 디스플레이에 다음이 표시됩니다.

- 컨트롤러 IO는 포트 트래픽과 높은 상관관계가 있습니다

- 포트가 IO를 서버로 전송할 때 성능 정책을 위반합니다.
- 포트 성능 위반이 스토리지 컨트롤러의 높은 IOPS 로드와 함께 발생하는 경우 스토리지 노드의 워크로드 때문에 위반이 발생할 수 있습니다



7. 포트 랜딩 페이지로 돌아가서 스토리지 컨트롤러 노드의 랜딩 페이지에 액세스하여 워크로드 메트릭을 분석할 수 있습니다.

노드는 사용을 위반 사항을 표시하고 메트릭은 버퍼 대 버퍼 제로 크레딧 상태와 관련된 높은 "캐시 읽기 대체됨"을 표시합니다.



Storage Node

BSM-prod-A

3h

24h

3d

7d

Custom

Storage: BSM-prod-A, BSM-prod-B
HA partner: BSM-prod-B
State: N/A
Model: FAS6070
Version: 8.0.5 7-Mode
Serial number: 700001181351
Memory: 98,304 MB
Utilization: 21.26% (94.56% max)
IOPS: 232.73 IO/s (1,153.00 IO/s max)
Latency: 7.07 ms (15.00 ms max)
Throughput: 22.44 MB/s (106.00 MB/s max)
Processors: 12
Performance Policies: Node Utilization
Node Read Latency

8. 노드 랜딩 페이지에서 상관 관계 리소스 목록에서 포트를 선택하여 BB 크레딧 0을 비교하고 메트릭 메뉴에서 노드에 대한 캐시 사용률 데이터를 포함한 활용 데이터를 선택할 수 있습니다.



이 데이터를 통해 캐시 적중률이 다른 메트릭과 반비례한다는 것을 알 수 있습니다. 캐시에서 서버 로드에는 응답하는

대신 스토리지 노드에 높은 캐시 읽기가 교체됩니다. 캐시보다는 디스크에서 대부분의 데이터를 검색해야 할 경우 포트가 서버로 데이터를 전송하는 데 지연이 발생할 수 있습니다. 성능 문제의 원인은 입출력 동작 시 워크로드가 생성되고 노드 캐시 및 해당 구성이 원인일 수 있습니다. 노드의 캐시 크기를 늘리거나 캐싱 알고리즘의 동작을 변경하여 문제를 해결할 수 있습니다.

인프라 분석 중

이 항목의 절차는 사용자 환경의 인프라 부분을 분석하는 데 사용할 수 있는 절차입니다. 이 연습에서 수집하는 단계, 보기 및 데이터는 가상 컴퓨팅 개체를 예로 사용합니다. 사용자 환경의 다른 자산에 대한 분석은 각 특정 자산에 대한 관련 카운터를 사용하여 유사한 단계를 따릅니다. 이 연습의 목적은 Insight에서 제공하는 다양한 옵션을 숙지하여 데이터 센터 자산의 특성을 모니터링하고 이해하는 것입니다.

이 작업에 대해

인프라의 상태를 분석하기 위해 수행할 수 있는 몇 가지 작업은 다음과 같습니다.

- 시간에 따른 개체의 동작을 관찰합니다
- 객체의 메트릭을 상위 10개 유사 객체의 메트릭과 비교합니다
- 개체의 숫자를 비교합니다
- 상위 10개 객체를 평균과 비교합니다
- 메트릭 A와 B를 비교합니다 - 범주 및 이상을 표시하는 많은 개체의 경우
- 개체 범위를 다른 개체와 비교합니다
- 표현식을 사용하여 웹 UI에서 사용할 수 없는 메트릭을 표시합니다

수행하는 각 분석에 대한 위젯을 사용하여 대시보드에서 인프라스트럭처의 모든 객체 뷰를 생성할 수 있습니다. 대시보드를 저장하면 인프라의 현재 데이터에 빠르게 액세스할 수 있습니다.

시간이 지남에 따라 개체의 동작을 관찰합니다

단일 개체의 동작을 관찰하여 개체가 예상 작동 수준 내에서 작동하는지 확인할 수 있습니다.

단계

1. 쿼리를 사용하여 분석 대상이 될 VM을 식별합니다. * 쿼리 * > * + 새 쿼리 * > * 가상 머신 * > * "이름" *

이름 필드를 비워 두면 모든 VM이 반환됩니다. 이 실습에서 사용할 VM을 선택합니다. VM 목록을 스크롤하여 선택할 수 있습니다.

2. 수집할 정보에 대한 새 대시보드를 생성합니다. 도구 모음에서 * 대시보드 * > * + 새 대시보드 * 를 클릭합니다.
3. 새 대시보드에서 * 변수 * > * 텍스트 * 를 선택합니다.

a. 쿼리에서 VM 이름을 로 추가합니다 \$var1 값.

b. 확인란을 클릭합니다.

변수는 분석할 여러 개체 집합 간에 쉽게 스와핑하는 데 사용됩니다. 분석의 다른 단계에서 이 변수를 처음에 선택한

단일 VM에 대한 추가 분석에 다시 사용할 수 있습니다. 여러 개체를 식별할 때 변수가 더 유용합니다.

4. 새 대시보드에 선형 차트 위젯을 추가합니다. * Widget * > * Line Chart *.

a. 기본 자산 유형을 가상 시스템으로 변경합니다. * 가상 머신 * > * 지연 시간 - 합계 * 를 클릭합니다.

b. 필터 기준 * > * 이름 * > * \$var1 * 을 클릭합니다.

c. 대시보드에서 기간을 변경합니다. * 대시보드 시간 재정의 * > * 컴 * > * 7일 *.

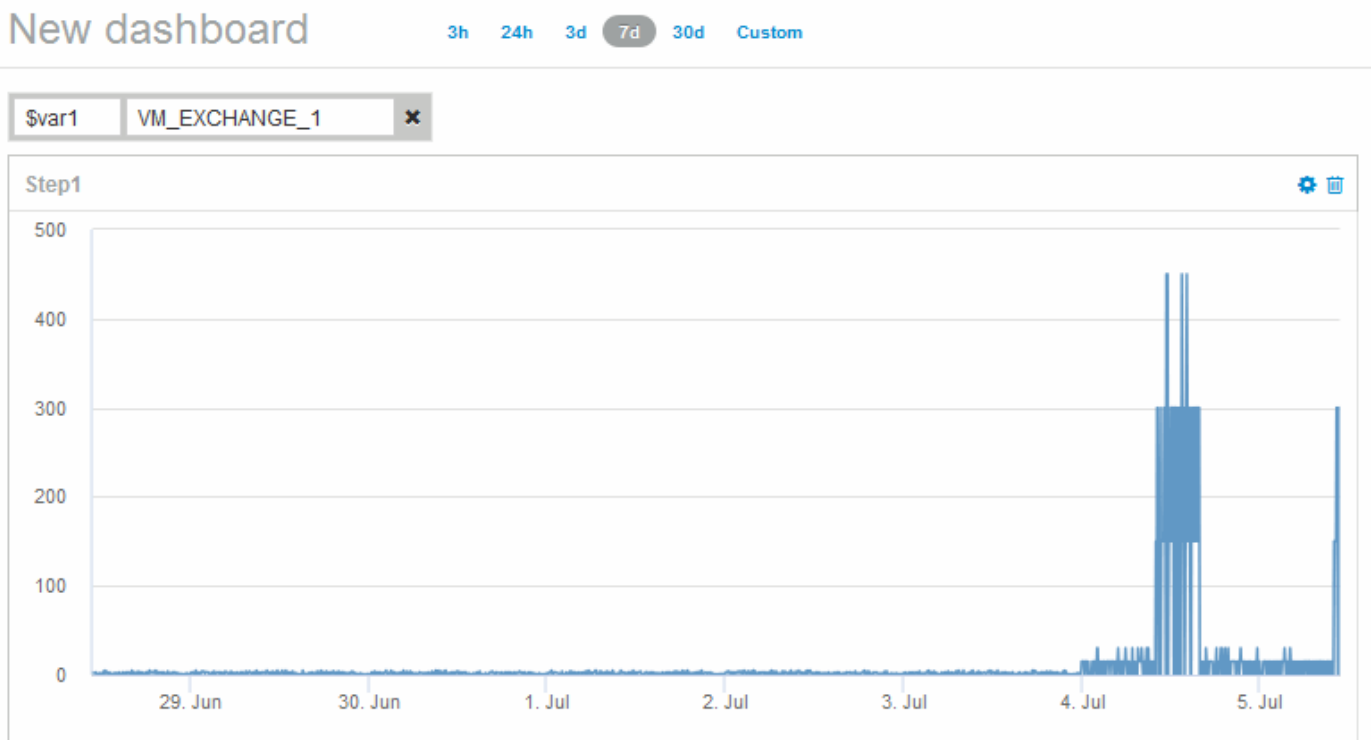
사전 설정 선택 항목을 사용하거나 사용자 지정 시간 범위를 지정하여 디스플레이 기간을 변경할 수 있습니다.

+ 지정한 기간 동안 VM의 * IOPS - 합계 * 가 대시보드에 표시됩니다.

5. 위젯에 이름을 지정하고 위젯을 저장합니다.

결과

위젯에는 다음과 유사한 데이터가 포함되어야 합니다.



VM은 표시된 7일 동안 짧은 시간 동안 비정상적으로 높은 대기 시간을 표시합니다.

오브젝트 및 비슷한 모든 오브젝트의 평균 지연 시간과 상위 **10개** 지연 시간을 비교합니다

VM을 총 10개의 지연 시간 중 가장 짧은 지연 시간과 총 평균 지연 시간을 비교하여 평균 범위를 벗어나는 지연 시간을 확인할 수 있습니다. 이 정보는 VM에서 워크로드의 균형을 조정하는 결정에 도움이 될 수 있습니다.

단계

1. 누적 영역형 차트가 있는 위젯을 새 대시보드에 추가합니다. * Widget * > * Stacked Area Chart *

- a. 기본 디바이스를 가상 머신으로 변경합니다. * Storage * > * Virtual Machine * > * Latency Total * 을 클릭합니다

위젯은 모든 VM에 대한 총 지연 시간을 24시간 동안 누적 영역형 차트로 표시합니다.

- b. 이 위젯에서 모든 VM에 대한 지연 시간 합계: * Widget * > * Line Chart * 를 표시하는 두 번째 디스플레이를 만듭니다

- c. 기본 디바이스를 가상 머신으로 변경합니다. * Virtual Machine * > * Latency-total * 을 클릭합니다

위젯은 선형 차트를 사용하여 기본 24시간 기간의 지연 시간 합계를 표시합니다.

- d. Roll Up * 표시줄에서 * X * 를 클릭하고 * Show * > * Top * > * 10 * 을 선택합니다

총 지연 시간을 기준으로 상위 10개의 VM이 표시됩니다.

2. 모든 VM의 총 평균 지연 시간을 상위 10 IOPS와 비교하려면 다음 단계를 사용하십시오.

- a. 추가 * 를 클릭합니다

- b. 기본 디바이스를 가상 머신으로 변경합니다. * 스토리지 * > * 가상 머신 * > * IOPS 합계 * 를 클릭합니다

- c. Roll Up * 표시줄에서 * X * 를 클릭하고 * Show * > * Top * > * 10 * 을 선택합니다

시스템은 지연 시간이 긴 10개의 오브젝트를 표시하며 선형 차트에 평균 지연 시간을 표시합니다.

이미지:::/media/analytics-top10-avg.gif[]

+평균 지연 시간은 1.6ms이고 상위 10개 VM의 지연 시간은 200ms입니다.

한 개체의 총 지연 시간을 상위 **10**개 개체의 총 지연 시간과 비교합니다

다음 단계에서는 단일 VM의 총 지연 시간을 전체 가상 인프라의 총 10대 지연 시간을 보고하는 VM과 비교합니다.

단계

1. 꺾은선형 차트가 포함된 위젯을 새 대시보드(* Widget*>* Line Chart*)에 추가합니다

- a. 기본 디바이스를 가상 머신으로 변경합니다. * Storage * > * Virtual Machine * > * Latency-total * 을 클릭합니다

위젯은 모든 VM에 대한 총 지연 시간을 영역 차트에 기본 24시간으로 표시합니다.

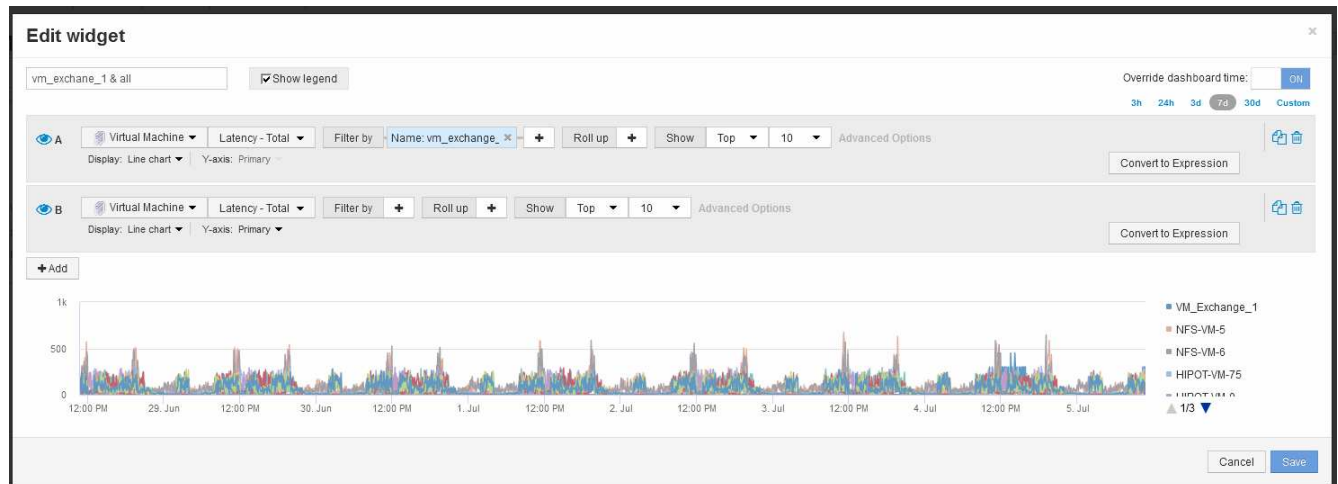
- b. 이 위젯에서 모든 VM에 대한 지연 시간 합계: * Widget * > * Line Chart * 를 표시하는 두 번째 디스플레이를 만듭니다

- c. 기본 디바이스를 가상 머신으로 변경합니다. * 스토리지 * > * 가상 머신 * > * 지연 시간 - 합계 * 를 클릭합니다

위젯은 선형 차트를 사용하여 기본 24시간 기간의 총 지연 시간을 표시합니다.

d. Roll Up * 표시줄에서 * X * 를 클릭하고 * Show * > * Top * > * 10 * 을 선택합니다

시스템은 지연 시간 - 총계를 기준으로 상위 10개의 VM을 표시합니다.



2. 비교할 VM을 상위 10개 VM에 추가합니다.

a. 추가 * 를 클릭합니다

b. 기본 디바이스를 가상 머신으로 변경합니다. * Storage * > * Virtual Machine * > * Latency Total * 을 클릭합니다

c. 필터 기준 * > * 이름 * > * \$var1 * 을 클릭합니다

3. 범례 표시 * 를 클릭합니다

결과

범례는 분석 중인 각 VM을 식별합니다. VM_Exchange_1을 쉽게 식별하고 해당 환경에서 상위 10개의 VM과 유사한 지연 시간이 발생하는지 확인할 수 있습니다.

메트릭-A를 메트릭-B와 비교하여 범주 및 이상을 표시합니다

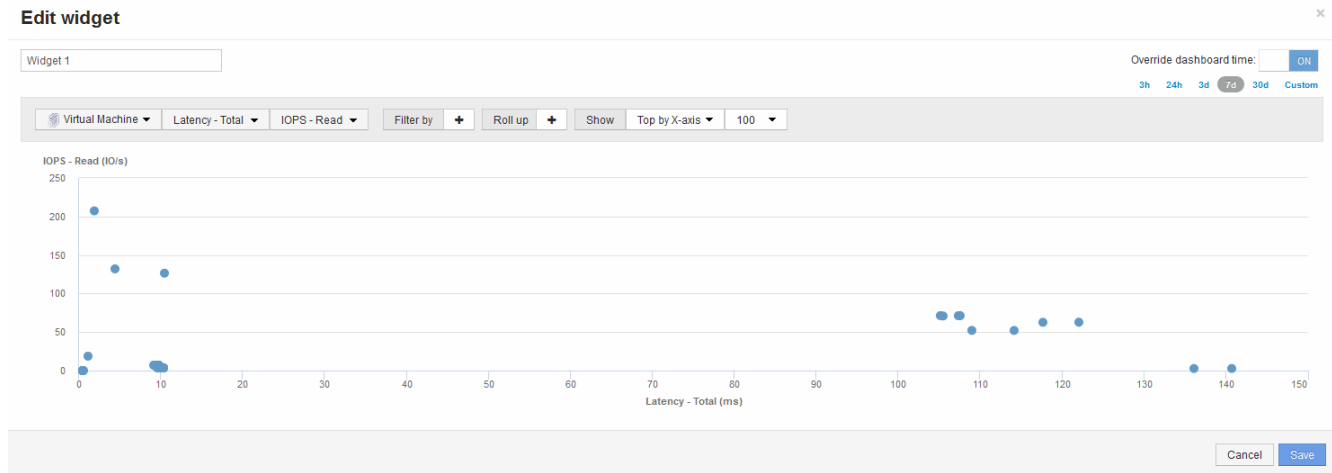
산포도를 사용하여 각 개체에 대해 두 개의 데이터 집합을 표시할 수 있습니다. 예를 들어, 각 개체에 대해 표시할 IOPS 읽기 및 지연 시간 합계를 지정할 수 있습니다. 이 차트를 사용하여 IOPS와 지연 시간의 조합을 기반으로 문제가 있다고 생각하는 객체를 식별할 수 있습니다.

단계

1. 분산형 플롯 차트가 있는 위젯을 새 대시보드에 추가합니다. * Widget * > * Scatter Plot Chart *

2. 기본 디바이스를 가상 머신으로 변경합니다. * 스토리지 * > * 가상 머신 * > * 지연 시간 합계 * > * IOPS 읽기 * 를 클릭합니다

다음과 유사한 분산형 플롯이 표시됩니다.



식을 사용하여 대체 메트릭을 식별합니다

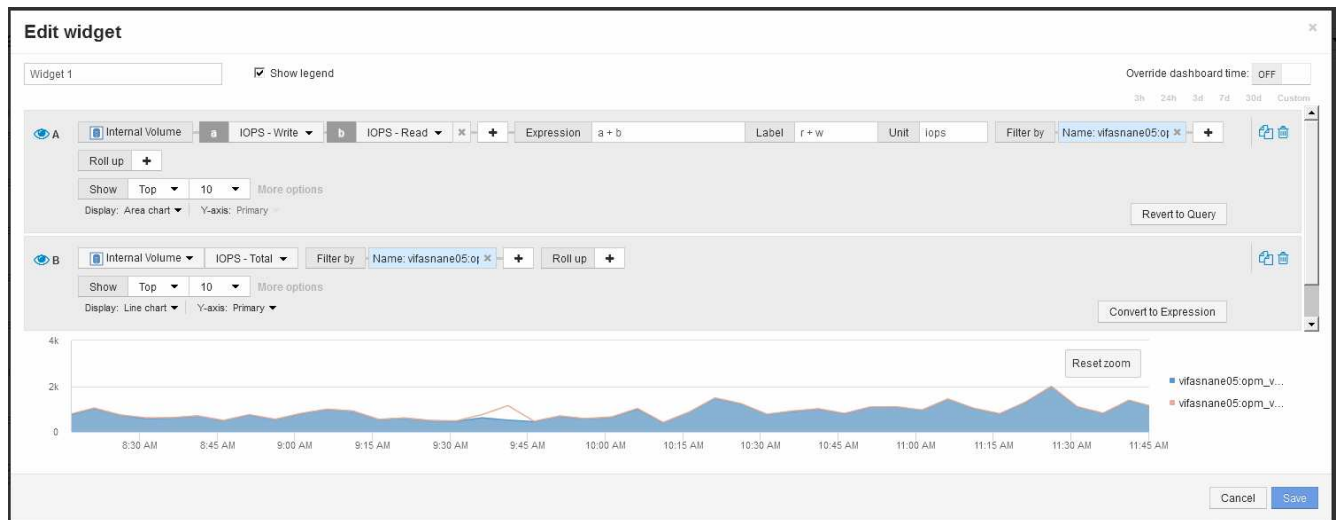
표현식을 사용하여 생성된 시스템 오버헤드 IOPS와 같이 웹 UI에서 제공하지 않은 메트릭을 볼 수 있습니다.

이 작업에 대해

식을 사용하여 내부 볼륨의 오버헤드 작업과 같이 읽기 또는 쓰기가 아닌 작업에서 생성된 총 IOPS를 표시할 수 있습니다.

단계

1. 대시보드에 위젯을 추가합니다. 영역표 * 를 선택합니다.
2. 기본 장치를 내부 볼륨으로 변경합니다. * 저장소 * > * 내부 볼륨 * > * IOPS 쓰기 * 를 클릭합니다
3. Expression * 으로 변환 단추를 클릭합니다.
4. 이제 * IOPS-Write * 메트릭은 알파벳 변수 필드 "" * A * ""에 있습니다.
5. "" * b * "" 변수 필드에서 * 선택 * 을 클릭하고 * IOPS-읽기 * 를 선택합니다.
6. 표현식 * 필드에 * a+b * 를 입력합니다. Display* 섹션에서 표현식에 대한 **Area chart**를 선택합니다.
7. 필터 기준 * 필드에 분석 중인 내부 볼륨의 이름을 입력합니다.
8. Label * 필드는 표현식을 식별합니다. 레이블을 ""R+W IOPS""와 같이 의미 있는 것으로 변경합니다.
9. 위젯에 총 IOPS를 위한 줄을 추가하려면 +추가를 클릭합니다.
10. 기본 디바이스를 내부 볼륨으로 변경합니다. * Storage * > * Internal volume * > * IOPS Total * 을 클릭합니다
11. 필터 기준 * 필드에 분석 중인 내부 볼륨의 이름을 입력합니다.



이 차트는 총 IOPS를 선으로 표시하며, 차트는 읽기 및 쓰기 IOPS의 조합을 파란색으로 표시합니다. 9:30과 9:45 사이의 간극은 비 읽기 및 비 쓰기 입출력(오버헤드) 작업을 나타냅니다.

썬 프로비저닝의 위험 최소화 소개

오늘날의 하이브리드 IT 데이터 센터에서 관리자는 썬 프로비저닝과 같은 용량 효율성 기술을 활용하여 할당을 제어하고 한때 사용할 수 없게 된 용량을 활용함으로써 물리적 한계를 넘어 리소스 활용률을 높여야 하는 부담을 안고 있습니다.

OnCommand Insight는 IT 서비스 스택 내의 여러 썬 프로비저닝 계층에 걸쳐 지금까지 거의 실시간으로 용량 사용량 및 활용도에 대한 세부 정보를 제공합니다. 초과 할당 위험을 적절하게 관리하지 못하면 비즈니스에 대한 다운타임이 시기적절하게 실행되지 않을 수 있습니다.

스토리지 풀 모니터링

각 스토리지 풀 랜딩 페이지는 초과 할당 비율을 제공하고, 상호 연결된 리소스, LUN 및 디스크 사용률을 식별하며, 스토리지 풀에서 발생한 정책 위반 및 위반을 식별합니다.

스토리지 풀 랜딩 페이지를 사용하여 가상 인프라를 지원하는 물리적 자산과 관련된 잠재적인 문제를 식별합니다. 30일 동안의 용량 및 용량 추세를 추적하거나 사용자 지정 기간을 사용할 수 있습니다. 스토리지 풀의 상태를 모니터링하려면 다음 섹션의 데이터를 확인하십시오.

* 요약 *

이 섹션을 통해 다음 사항을 이해할 수 있습니다.

- 물리적 용량 및 초과 커밋된 용량을 비롯한 스토리지 풀 용량 정보
- 초과 할당 여부와 초과 할당 정도.
- 발생한 모든 정책 위반.

* 스토리지 리소스 및 디스크 섹션 *

스토리지 리소스 섹션에 LUN 사용률이 표시됩니다.

디스크 섹션에는 스토리지 풀을 구성하는 개별 디스크가 표시됩니다.

- * 리소스 *

이 섹션을 사용하여 LUN에 대한 VMDK 상관 관계를 이해하고 스토리지-VM 애플리케이션 경로를 파악할 수 있습니다.

- * 위반 섹션 *

위반 섹션에서는 스토리지 풀에 대해 설정된 성능 정책에 대한 위반 사항을 식별합니다.

데이터 저장소 모니터링

데이터 저장소 랜딩 페이지에서는 초과 할당 비율, LUN 및 디스크 사용률, 상호 연결된 리소스를 식별하고 데이터 저장소에서 발생한 정책 위반과 관련 사항을 보여 줍니다.

이 랜딩 페이지를 사용하여 가상 인프라 문제를 식별합니다. 용량 및 용량 비율 추세를 추적하여 용량 변화를 예측할 수 있습니다.

- * 요약 *

이 섹션을 통해 다음 사항을 이해할 수 있습니다.

- 물리적 용량 및 초과 커밋된 용량을 비롯한 데이터 저장소 용량 정보
- 초과 커밋된 용량의 비율입니다.
- 지연 시간, IOPS, 처리량을 위한 메트릭

- * VMDK *

VMDK 섹션에는 가상 디스크 용량 및 성능이 표시됩니다.

- * 스토리지 리소스 *

이 섹션에는 사용된 용량과 데이터 저장소와 연결된 내부 볼륨의 성능 메트릭이 표시됩니다.

- * 리소스 *

이 섹션을 사용하여 LUN의 VMDK 상관 관계를 이해하고 스토리지-VM 애플리케이션 경로를 파악할 수 있습니다.

- * 위반 섹션 *

위반 섹션에서는 데이터 저장소에 대해 설정된 성능 정책에 대한 위반 사항을 식별합니다.

대시보드를 생성하여 씬 프로비저닝 환경을 모니터링합니다

OnCommand Insight의 유연한 대시보드 위젯 설계 및 표시 차트 옵션을 사용하면 용량 사용 및 활용률에 대한 심층 분석, 씬 프로비저닝된 데이터 센터 인프라의 위험을 최소화할 수 있는 전략적 정보를 얻을 수 있습니다.

모니터링할 데이터 저장소 및 스토리지 풀 정보에 대한 액세스를 제공하는 대시보드를 생성할 수 있습니다.

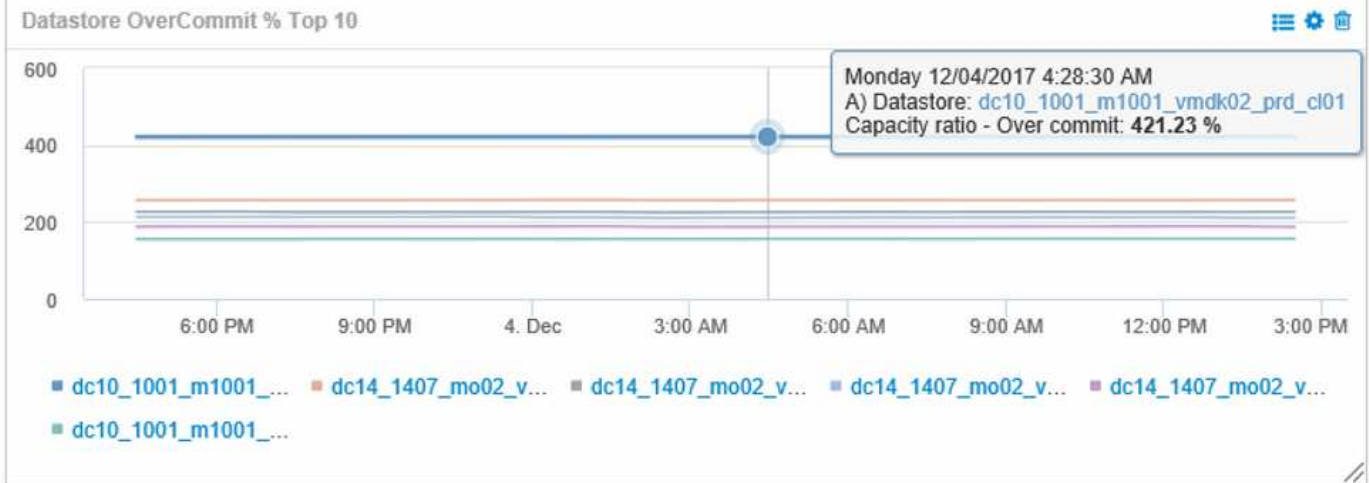
대시보드를 사용하여 데이터 저장소 정보에 액세스합니다

가상 인프라에서 모니터링하려는 데이터에 빠르게 액세스할 수 있는 대시보드를 생성할 수 있습니다. 대시보드에는 초과 커밋된 % 및 데이터 저장소의 용량 데이터를 보여 주는 위젯을 기반으로 상위 10개 데이터 저장소를 식별하기 위해 다음과 유사한 위젯이 포함될 수 있습니다. 대시보드는 150% 이상 초과 커밋된 데이터 저장소와 80% 이상의 사용된 용량을 초과한 데이터 저장소를 강조하기 위해 변수를 사용합니다.

New dashboard

3h 24h 3d 7d 30d Custom

\$OverCommit... 150 x \$UsedCapRatio 80 x



Overcommit Subscription %

Name	Capacity - Total (GB)	Capacity - Used (GB)	Capacity - Provisioned (GB)	Capacity ratio - Over commit (%)	Capacity ratio - Used (%)
dc14_1407_...1_prd_cl03	5,008.00	4,091.04	12,876.38	257.12	81.69
dc14_1407_...2_prd_cl03	6,936.69	5,872.31	14,633.80	210.96	84.66
dc14_1407_...3_prd_cl03	9,437.03	7,951.36	17,639.86	186.92	84.26
dc14_1407_...4_prd_cl03	7,911.09	6,627.00	17,891.24	226.15	83.77

4 items found

빈 프로비저닝된 환경을 모니터링하는 데 사용할 수 있는 추가 위젯에는 다음 정보 중 일부가 포함될 수 있습니다.

- VMDK 용량은 데이터 저장소와 상호 관련되었습니다
- VM 용량
- 사용된 데이터 저장소 용량 추세

대시보드를 사용하여 스토리지 풀 정보를 액세스합니다

대시보드에는 다음과 유사한 위젯이 포함될 수 있으며, 사용된 물리적 스토리지 용량의 양을 식별하거나, 스토리지 풀의 초과 할당 용량을 식별할 수 있습니다.



성능 정책을 사용하여 씬 프로비저닝의 위험 감소

가상 인프라스트럭처의 임계값이 위반될 경우 알림을 발생시키기 위해 성능 정책을 만들어야 합니다. 알림을 통해 운영 중단 또는 중단을 일으킬 수 있는 환경 변화에 미리 대응할 수 있습니다.

가상 인프라스트럭처를 모니터링하는 데 도움이 되는 정책은 다음과 같습니다.

• * 데이터 저장소 *

데이터 저장소에서 다음 정책을 사용할 수 있습니다.

- 용량 비율 - Overcommit
- 용량 비율 - 사용됨
- 용량 - 사용됨
- 용량 - 합계

• * 스토리지 풀 *

다음 정책은 씬 프로비저닝 환경에서 스토리지 관련 용량 중단으로부터 보호할 수 있습니다.

- 용량이 프로비저닝되었습니다
- 사용된 용량
- 용량 비율 - Overcommit
- 용량 비율 - 사용됨

이러한 정책을 확장하여 다음과 같은 가상 인프라스트럭처의 용량을 모니터링할 수 있습니다.

- 내부 볼륨
- LUN을 클릭합니다
- 디스크
- VMDK입니다
- VM

주석을 사용하여 정책을 구성할 수 있습니다. 응용 프로그램을 지원하는 특정 자산에 동일한 주석을 할당합니다. 예를 들어, 실행 프로비저닝된 애플리케이션의 데이터 저장소 및 스토리지 풀에 주석을 할당할 수 있습니다. 운영 환경에 대한 Production, 개발 환경에 대한 Development 등의 주석이 있을 수 있습니다. 자산이 지원하는 애플리케이션의 유형에 따라 경고의 임계값과 중요도를 변경할 수 있습니다. 예를 들어 운영 애플리케이션의 데이터 저장소에 대한 임계값을 위반할 경우 `_critical warning_`이 발생할 수 있지만 개발 환경에 대한 동일한 위반은 `_warning_`만 발생시킬 수 있습니다. 정의된 정책 내에 주석을 통합하면 중요하지 않은 자산에 대한 원치 않는 경고 소음을 더욱 줄일 수 있습니다.

스토리지 풀에 대한 성능 정책 생성

스토리지 풀 자산에 대한 임계값이 초과되었을 때 알림을 트리거하는 성능 정책을 생성할 수 있습니다.

시작하기 전에

이 절차에서는 스토리지 풀을 실행 프로비저닝했다고 가정합니다.

이 작업에 대해

운영 중단을 일으킬 수 있는 스토리지 풀의 변경 사항을 모니터링하고 보고하는 정책을 생성하려고 합니다. 실행 프로비저닝된 물리적 스토리지 풀의 경우 물리적 용량을 모니터링하고 Overcommit Ratio를 모니터링하려고 합니다.

단계

1. 브라우저에서 OnCommand Insight를 엽니다.
2. Manage > * Performance Policies * 를 선택합니다

성능 정책 페이지가 표시됩니다. 정책은 객체별로 구성되며 목록에 나타나는 순서대로 평가됩니다. 알림이 활성화된 경우(* Admin>* Notifications*) 성능 정책이 위반될 때 Insight에서 이메일을 보내도록 구성할 수 있습니다.

3. 새 정책을 만들려면 **+Add**를 클릭합니다.
4. 정책 이름 * 에 스토리지 풀의 정책 이름을 입력합니다.
5. Apply to objects of type * 에서 Storage Pool 을 선택합니다.
6. 다음 시간 뒤에 적용 * 에서 첫 번째 발생 항목을 입력합니다.
7. 심각도 * 로 * 에 Critical 을 입력합니다
8. 임계값이 위반될 때 알림을 받을 e-메일 수신자를 구성합니다.

기본적으로 정책 위반에 대한 전자 메일 알림은 전역 전자 메일 목록의 받는 사람에게 전송됩니다. 특정 정책에 대한 알림이 특정 수신자에게 전송되도록 이러한 설정을 재정의할 수 있습니다.

링크를 클릭하여 받는 사람 목록을 연 다음 + 단추를 클릭하여 받는 사람을 추가합니다. 이 정책에 대한 위반 알림은 목록의 모든 수신자에게 전송됩니다.

9. 다음 중 하나라도 해당되는 경우 * Create alert에서 * Capacity ratio-used > 85%를 입력합니다

결과

이 구성은 스토리지 풀의 물리적 용량의 85% 이상이 사용될 때 시스템에서 심각한 경고 메시지를 보냅니다. 물리적 메모리의 100%를 사용하면 응용 프로그램 오류가 발생합니다.

추가 스토리지 풀 정책을 생성합니다

이 작업에 대해

사용된 스토리지 풀 용량이 75%를 초과할 경우 경고 메시지를 표시하는 추가 "사용된 용량 비율" 정책을 생성합니다. 알림이 활성화된 경우(* Admin*>* Notifications*) 성능 정책이 위반될 때 Insight에서 이메일을 보내도록 구성할 수 있습니다.

데이터 저장소에 대한 성능 정책 생성

모니터링 중인 스토리지 풀과 관련된 데이터 저장소와 연결된 메트릭에 대한 임계값을 사용하여 성능 정책을 생성할 수 있습니다. 기본적으로 성능 정책은 지정된 유형의 모든 디바이스를 생성할 때 적용됩니다. 성능 정책에 특정 장치 또는 장치 집합만 포함하도록 주석을 만들 수 있습니다.

시작하기 전에

성능 정책에서 주석을 사용하는 경우 정책을 생성하기 전에 주석이 존재해야 합니다.

이 작업에 대해

모니터링 중인 하나 이상의 데이터 저장소가 사용자가 설정한 임계값을 초과할 때 알림을 제공하는 성능 정책을 생성합니다. 사용자의 요구에 맞는 글로벌 정책이 시스템에 이미 포함되어 있거나, 데이터 저장소에 주석을 달 경우 주석을 사용하는 정책도 작동할 수 있습니다.

단계

1. Insight(인사이트) 도구 모음에서 * Manage(관리) * > * Performance Policies(성능 정책) * 를 선택합니다

성능 정책 페이지가 표시됩니다. 기존 성능 정책을 검토하여 모니터링할 임계값에 대한 메트릭을 처리하는 기존 정책을 식별합니다.

2. 새 정책을 추가하려면 * + 추가 * 를 클릭합니다

3. "정책 이름" 추가

개체의 다른 모든 정책 이름과 다른 이름을 사용해야 합니다. 예를 들어, 내부 볼륨에 대해 "지연 시간"이라는 두 개의 정책을 사용할 수는 없지만, 내부 볼륨에 대한 "지연 시간" 정책과 데이터 저장소에 대한 또 다른 "지연 시간" 정책을 가질 수는 있습니다. 가장 좋은 방법은 개체 유형에 관계없이 모든 정책에 대해 항상 고유한 이름을 사용하는 것입니다.

4. Object Type으로 "Datastore"를 선택합니다

5. "첫 번째 항목"을 클릭합니다.

첫 번째 발생 옵션은 첫 번째 데이터 샘플에서 임계값이 초과되면 알림을 트리거합니다. 다른 모든 옵션은 임계값을 한 번 넘어섰을 때 경고를 발생시키고 지정된 시간 이상 연속적으로 교차하는 경우에 발생합니다.

6. "경고"를 클릭합니다.

7. "'알림 생성'으로 * Capacity ratio-over commit * 을 선택하고 값을 * > 150 * 로 설정합니다

용량 합계** 및 * 사용된 용량 * 과 같은 용량 관련 경고를 추가로 생성할 수 있습니다.

호스트 및 VM 파일 시스템 사용률 데이터 수집

호스트 및 VM 파일 시스템 데이터 소스와 호스트 활용도 라이선스를 함께 사용하면 알려진 호스트 및 VM의 파일 시스템 레벨에서 보고 및 차지백을 수행할 수 있습니다.

OnCommand Insight는 스토리지 디바이스에서 데이터를 취합하며, 이 중 대부분은 볼륨을 블록 디바이스로 보고합니다. Insight는 이를 통해 파일 시스템 레벨이 아닌 스토리지 레벨의 활용도에 대해 보고할 수 있습니다. 스토리지 어레이는 일반적으로 어떤 블록이 기록되었지만 어떤 블록이 해제되었는지 알지 못합니다.

클라이언트 호스트 및 VM에서 파일 시스템 구현(NTFS, ext *...) 블록 장치 위에 있습니다. 대부분의 파일 시스템은 디렉토리 및 파일 메타데이터를 포함하는 목차를 보관합니다. 파일이 삭제되면 해당 항목이 목차에서 제거됩니다. 이러한 파일이 사용하는 블록은 이제 파일 시스템에서 재사용할 수 있지만 스토리지 시스템은 이를 알지 못합니다. Insight에서 파일 시스템 사용량을 보고하려면 정확한 차지백을 위해 클라이언트 호스트 또는 VM 관점에서 데이터를 수집해야 합니다.

Insight를 사용하면 * 호스트 활용률 * 라이선스와 함께 * NetApp 호스트 및 VM 파일 시스템 * 데이터 소스를 통해 이러한 수준의 파일 시스템 활용률 데이터 수집을 수행할 수 있습니다. VM에는 적절한 * Compute Resource Group * 이름을 주석으로 추가해야 하며, 관련 스토리지 어레이에는 정확한 비용 보고를 위해 적절한 비용으로 적절한 * Tier * 주석을 추가해야 합니다.



Host Utilization 라이선스는 다른 Insight 라이선스와 달리 용량 기반과는 달리 리소스 기반입니다.

파일 시스템 수집에 대한 **Insight**를 구성합니다

파일 시스템 사용률 데이터 수집에 대한 Insight를 구성하려면 Host Utilization Pack 라이선스를 설치하고 NetApp Host and VM File Systems 데이터 소스를 구성해야 합니다.

시작하기 전에

아직 Host Utilization Pack 라이선스를 설치하지 않은 경우 Admin * > * Setup * 페이지의 * Licenses * 탭에서 라이선스를 확인할 수 있습니다.

호스트 및 VM 파일 시스템 데이터 원본은 현재 Insight에서 수집 또는 검색되고 있는 알려진 * 컴퓨팅 리소스 * (호스트 및 VM)에 대한 파일 시스템 사용률 및 파일 시스템 메타데이터만 보고합니다.

- 가상 시스템은 Hyper-V 및 VMware와 같은 하이퍼바이저 데이터 소스에 의해 수집됩니다.
- 호스트는 장치 확인을 통해 검색됩니다.

적절한 스토리지 리소스에 적절한 계층 주석이 있어야 합니다.

다음과 같은 연결된 블록 스토리지 디바이스가 지원됩니다.

- NetApp clustered Data ONTAP(cDOT)
- NetApp 7-Mode에서 직접 지원합니다
- CLARiX
- Windows: FC, iSCSI용 VMware 가상 디스크(VMDK)입니다
- Linux: VMware VMDK(iSCSI 및 FC 지원 안 됨)

Compute Resource Group * 은 공통 관리 자격 증명을 공유하는 호스트 및/또는 가상 시스템을 그룹화할 수 있는 주석입니다.

단계

1. 먼저 * Compute Resource Group * 에 포함될 호스트 및/또는 가상 시스템에 주석을 답니다. 쿼리 * > * + 새 쿼리 * 로 이동하여 _Virtual Machine_assets를 검색합니다.

Host_assets에 대해 이 단계를 반복해야 합니다.

2. 테이블 오른쪽의 열 선택기를 클릭하고 * Compute Resource Group * 열을 선택하여 쿼리 결과 테이블에 표시합니다.
3. 원하는 컴퓨팅 리소스 그룹에 추가할 가상 머신을 선택합니다. 필터를 사용하여 특정 자산을 검색할 수 있습니다.
4. Actions * 버튼을 클릭하고 * Edit annotation * 을 선택합니다.
5. Compute Resource Group_annotation을 선택한 후 _Value_field에서 원하는 자원 그룹 이름을 선택합니다.

선택한 VM에 리소스 그룹 주석이 추가됩니다. 리소스 그룹 이름은 나중에 호스트 및 VM 파일 시스템 데이터 소스에서 구성할 이름과 일치해야 합니다.

6. 컴퓨팅 리소스 그룹의 호스트 및 VM 파일 시스템 데이터 소스를 구성하려면 * Admin * > * Data Sources * 를 클릭하고 * Add * the_NetApp Host and VM File Systems_data source 를 클릭합니다.

Settings

*Name

Vendor

Model

Where to run

What to collect

Configuration

Advanced configuration

Test

Cancel Save

- 구성* 섹션에서 파일 시스템 데이터를 검색할 수 있는 적절한 권한이 있는 운영 체제 사용자의 * 사용자 이름 * 및 * 암호 * 를 입력합니다. Windows 운영 체제 사용자의 경우 Windows 환경에서 도메인 접두사를 사용해야 합니다.

Linux에 설치된 AU(Insight Acquisition Unit)는 Linux 컴퓨팅 리소스에 대해 보고할 수 있고, Windows에 설치된 AU는 Linux 또는 Windows 컴퓨팅 리소스에 대해 말할 수 있습니다.

- 파일 시스템 사용률 데이터를 수집할 자산에 대한 * 컴퓨팅 리소스 그룹 * 의 이름을 입력합니다. 이 이름은 위의 자산에 주석을 다는 데 사용한 리소스 그룹 이름과 일치해야 합니다.

Compute Resource Group 필드를 비워 두면 데이터 소스에서 Compute Resource Group 주석이 없는 호스트 또는 VM에 대한 데이터를 수집합니다.

- 고급 구성** 섹션에서 이 데이터 소스에 대해 원하는 폴링 간격을 입력합니다. 일반적으로 6시간의 기본값은 적당합니다.
- 데이터 소스 연결을 저장하기 전에 * 테스트 * 하는 것이 좋습니다. 연결 결과가 성공하면 그룹에 포함된 컴퓨팅 리소스 타겟의 수도 표시됩니다.
- 저장 * 을 클릭합니다. 호스트 및 VM 파일 시스템 데이터 소스가 다음 폴에서 데이터 수집을 시작합니다.
- 파일 시스템 데이터가 수집되면 호스트 또는 VM의 자산 페이지의 파일 시스템 위젯에서 해당 데이터를 볼 수 있습니다.

File Systems

Name	Capacity (Used / Total GB)	Type	Storage Resource
/	9.15% (11.0 / 120.0)	xfs	vifasnane:...vm_oci_
/boot	23.79% (0.1 / 0.5)	xfs	vifasnane:...vm_oci_
/dev/dm-1	7.8	swap	vifasnane:...vm_oci_

Showing 1 to 3 of 3 entries

13. 가질 각 컴퓨팅 리소스 그룹에 대해 이 단계를 반복합니다. 각 컴퓨팅 리소스 그룹은 자체 호스트 및 VM 파일 시스템 데이터 소스와 연결되어야 합니다.

파일 시스템 정보는 사용자 환경의 기존 VMware 또는 Hyper-V 데이터 소스에 의해 이미 획득되고 있는 호스트 및 VM에 대해 수집됩니다.

파일 시스템 차지백 및 보고

파일 시스템에 대한 차지백은 항상 스토리지의 관점에서 수행됩니다. 특정 컴퓨팅 리소스 그룹에 대해 주석이 추가된 가상 머신과 연결된 스토리지 스토리지가 해당 리소스 그룹에 대한 차지백 보고서에 포함됩니다.

시작하기 전에

파일 시스템 사용률 차지백에 포함하려는 모든 가상 머신에는 적절한 컴퓨팅 리소스 그룹 이름을 주석으로 추가해야 합니다. 이러한 가상 머신과 연결된 스토리지 어레이에는 적절한 계층 주석이 주석으로 첨부되어야 합니다. 데이터 웨어하우스에 대한 ETL은 이러한 주석이 추가된 후에 발생해야 합니다.

단계

1. 일반적으로 보고 서버에 대한 브라우저를 엽니다 <https://<host or IP>:9300/p2pd`http://<host or IP>:9300/bi> (7.3.3 or later) 로그인한 다음
2. File System Utilization * 패키지를 선택하고 새 보고서를 생성합니다.



3. 데이터 마트에서 항목을 끌어다 놓아 보고서를 작성합니다.

아래 예는 매우 간단한 보고서입니다. 특정 비즈니스 요구 사항에 따라 복잡한 보고서를 작성할 수 있습니다.

Name	Type	Allocated Capacity GB	Used Capacity GB	Tier Name	Cost	Storage Name
/	xfs	119.96	9.96	N/A		vifasnane05,vifasnane06
/	xfs	5,492.53	799.63	Tier 1	100	vifasnane
/boot	xfs	0.48	0.17	N/A		vifasnane05,vifasnane06
/boot	xfs	8.72	2.41	Tier 1	100	vifasnane
/dev/dm-1	swap	7.81	0.00	N/A		vifasnane05,vifasnane06
/dev/dm-1	swap	140.61	0.78	Tier 1	100	vifasnane
C:\	NTFS	948.27	331.98	Tier 1	100	vifasnane
PHYSICALDRIVE0: System Reserved	NTFS	1.70	1.41	Tier 1	100	vifasnane

차지백 데이터를 보고하도록 시스템을 구성합니다

차지백 보고서는 호스트, 애플리케이션 및 비즈니스 엔티티별로 스토리지 용량 차지백 및 책임 정보를 제공하며 현재 데이터와 기간별 데이터를 모두 포함합니다.

이 가이드에서는 서비스 수준 비용 및 스토리지 사용 비용에 대한 책임을 제공하는 차지백 보고서를 생성하도록 Insight를 구성하는 방법에 대해 설명합니다. 이 가이드의 목적은 간단한 차지백 보고서를 생성하는 데 필요한 단계를 제공하고 Insight 사용자가 고유한 환경에서 차지백을 구성할 때 사용할 수 있는 옵션을 숙지하는 것입니다.

예제 보고서는 각 응용 프로그램에 대해 프로비저닝된 리소스와 리소스 비용을 식별합니다. Insight에서 다음 데이터를 정의하여 보고서 출력을 생성합니다

- 제공합니다
- 각 스토리지 계층과 연관된 비용
- 프로비저닝된 스토리지 용량
- 서비스 레벨
- 서비스 수준별 비용

다음 섹션에서는 Insight Reporting에서 액세스할 수 있도록 이 데이터를 구성하는 데 필요한 단계를 설명합니다.

차지백과 함께 사용할 주식 정의

회사 요구 사항에 맞는 데이터를 추적하도록 OnCommand Insight를 사용자 지정할 때 데이터의 전체 그림을 제공하는 데 필요한 특수 주석을 정의할 수 있습니다. 예를 들어 주석을 통해 자산의 수명 종료, 자산이 상주하는 데이터 센터 또는 스토리지의 GB당 비용을 정의하는 스토리지 계층을 정의할 수 있습니다.


이 작업에 대해

이 가이드의 차지백 보고서 예는 서비스 수준과 계층 수준에 대한 데이터를 제공합니다. 각 서비스 수준 및 계층 수준에 대한 주석을 작성한 다음 서비스 수준 및 계층 수준에 대한 비용을 정의해야 합니다.

단계

1. Insight 웹 UI에 로그인합니다
2. 관리 * > * 주식 * 을 클릭합니다

주식 페이지가 표시됩니다.

3. 서비스 수준 또는 계층 주식 위에 커서를 놓고 를 클릭합니다 .

Edit Annotation(주식 편집) 대화 상자가 표시됩니다.

4. 새 계층 및 비용을 추가하려면 * 추가 * 를 클릭합니다.

보고서 예에서 계층 및 서비스 수준 이름은 골드, 실버 및 브론즈라는 귀금속 비유를 사용합니다. 조직에서 선택한 이름 지정 규칙(예: 계층 1, 수준 2, 최상)을 사용할 수 있습니다.

5. Gold-Fast, Gold, Silver 및 Bronze 계층에 대한 값과 각 계층과 관련된 비용을 입력합니다.

입력한 값은 애플리케이션에서 사용하는 스토리지의 GB당 비용을 정의합니다. 서비스 수준 비용은 서비스 제공 비용이거나 소비자에게 서비스를 제공하는 실제 가격일 수 있습니다. 이러한 비용은 Chargeback 보고서에 보고됩니다.

6. 작업을 마치면 * 저장 * 을 클릭합니다.

차지백과 함께 사용할 애플리케이션 정의

사용자 환경에서 실행 중인 특정 애플리케이션과 관련된 비용 데이터를 추적하려면 먼저 애플리케이션을 정의해야 합니다.

시작하기 전에

애플리케이션을 업무 엔티티에 연결하려면 이미 업무 엔티티를 생성해야 합니다.



이 예제에서는 어떠한 응용 프로그램도 비즈니스 엔티티와 연결하지 않습니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. Manage * > * Application * 을 클릭합니다

응용 프로그램을 정의한 후 응용 프로그램 페이지에는 응용 프로그램의 이름, 우선 순위 및 응용 프로그램과 연결된 업무 엔티티가 표시됩니다(해당하는 경우).

3. 추가 를 클릭합니다

응용 프로그램 추가 대화 상자가 표시됩니다.

4. 이름 상자에 응용 프로그램의 고유한 이름을 입력합니다. 보고서에 표시된 응용 프로그램(아프리카 투어, APAC 상용 판매 등)을 입력합니다.
5. Priority * 를 클릭하고 해당 환경의 애플리케이션에 대한 우선 순위(중요, 높음, 중간 또는 낮음)를 선택합니다.

6. 비즈니스 엔티티와 함께 이 응용 프로그램을 사용하려면 * 사업체 * 를 클릭하고 목록에서 엔티티를 선택합니다.
7. 볼륨 공유를 사용하지 않습니다. * 볼륨 공유 확인 상자를 클릭하여 지웁니다.
8. 저장 * 을 클릭합니다.

응용 프로그램이 응용 프로그램 페이지에 나타납니다. 애플리케이션 이름을 클릭하면 Insight에서 애플리케이션의 자산 페이지를 표시합니다. 애플리케이션을 정의한 후 호스트, 가상 머신, 볼륨, 내부 볼륨 또는 하이퍼바이저의 자산 페이지로 이동하여 애플리케이션을 자산에 할당할 수 있습니다.

자산에 애플리케이션 할당

응용 프로그램을 정의한 후에는 응용 프로그램을 특정 자산과 연결해야 합니다. 간단한 Ad Hoc 방법을 사용하여 응용 프로그램을 자산에 적용할 수 있습니다. 응용 프로그램을 대량으로 적용하려는 사용자는 쿼리 방법을 사용하여 응용 프로그램에 할당할 자산을 식별해야 합니다.

임시 방법을 사용하여 자산에 응용 프로그램 할당

애플리케이션에서 사용하는 자산의 리소스를 식별할 수 있도록 자산에 애플리케이션을 할당합니다. 자산에 비용이 할당된 경우 애플리케이션에서 발생한 비용을 식별할 수 있고 리소스가 크기별로 측정되는 경우 리소스를 보충해야 하는지 여부를 결정할 수 있습니다.


이 작업에 대해

다음 방법을 사용하여 응용 프로그램을 자산에 할당합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. 다음 중 하나를 수행하여 애플리케이션을 적용할 자산(호스트, 가상 머신, 볼륨 또는 내부 볼륨)을 찾습니다.


옵션을 선택합니다	설명
자산 목록으로 이동합니다	대시보드 * > * 자산 대시보드 * 를 클릭하고 자산을 선택합니다.
자산을 검색합니다	을 클릭합니다  도구 모음에서 * 자산 검색 * 상자를 표시하려면 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.

3. 자산 페이지의 * 사용자 데이터 * 섹션에서 현재 자산에 할당된 애플리케이션 이름(할당된 애플리케이션이 없는 경우 * 없음 * 이 표시됨)에 커서를 놓고 클릭합니다  (응용 프로그램 편집).

선택한 자산에 대해 사용 가능한 애플리케이션 목록이 표시됩니다. 현재 자산과 연결된 응용 프로그램 앞에는 확인 표시가 나타납니다.

4. 검색 상자에 입력하여 응용 프로그램 이름을 필터링하거나 목록을 아래로 스크롤할 수 있습니다.
5. 자산과 연결할 애플리케이션을 선택합니다.

여러 애플리케이션을 호스트, 가상 시스템 및 내부 볼륨에 할당할 수 있지만 하나의 애플리케이션만 볼륨에 할당할 수 있습니다.

6.  을 클릭합니다 선택한 애플리케이션 또는 애플리케이션을 자산에 할당합니다.

응용 프로그램 이름은 사용자 데이터 섹션에 나타납니다. 응용 프로그램이 업무 엔티티와 연결되어 있으면 이 섹션에도 업무 엔티티의 이름이 표시됩니다.

쿼리를 사용하여 자산에 응용 프로그램 할당

애플리케이션에서 사용하는 자산의 리소스를 식별할 수 있도록 자산에 애플리케이션을 할당합니다. 자산에 비용이 할당된 경우 애플리케이션에서 발생한 비용을 식별할 수 있고 리소스가 크기별로 측정되는 경우 리소스를 보충해야 하는지 여부를 결정할 수 있습니다.


이 작업에 대해

쿼리를 사용하여 애플리케이션에 여러 자산을 할당하는 작업을 단순화할 수 있습니다.

단계


1. 새 쿼리를 만들어 응용 프로그램을 할당할 자산을 식별합니다. 예를 들어 지리적 위치와 관련된 특정 이름의 호스트에 할당하려면 * 쿼리 * > * + 새 쿼리 * 를 클릭합니다
2. 호스트 * 를 클릭합니다
3. 이름 * 필드에 를 입력합니다 Chicago

시스템에 가 있는 모든 호스트가 표시됩니다 Chicago 이름을 입력할 수 있습니다.

 Host

Name

chicago



More ▾

Query results

<input type="checkbox"/> ▾	Name ▲	IP ▲	Application
<input type="checkbox"/>	Chicago-Host1	10.11.12.21	Sydney Airline Sales
<input type="checkbox"/>	Chicago-Host2	10.11.12.32	Sydney Airline Sales
<input type="checkbox"/>	Chicago-NAS	10.11.12.10	Sydney Airline Sales

Showing 1 to 3 of 3 entries

4. 쿼리에서 식별된 호스트 중 하나 이상을 선택합니다.
5. Actions * > * Add Application * 을 클릭합니다

Assign Application



Application

None

☐ African Tours
 ☐ APAC Commercial Sales
 ☐ APAC Cruises
 ☐ BSM System
 ☐ Carboard Collection Centers
 ☐ Caribbean
 ☐ Commercial Applications
 ☐ Commercial Environments
 ☐ Concur
 ☐ Consumer Feedback

Application

Sydney Airline Sales

Sydney Airline Sales

Sydney Airline Sales

IOPS - Total (IO/s)

N/A

N/A

N/A

응용 프로그램 할당 대화 상자가 표시됩니다.

6. 호스트에 할당할 애플리케이션을 선택하고 를 클릭합니다
7. 저장 * 을 클릭합니다

응용 프로그램 이름이 사용자 데이터 섹션에 나타납니다.

단순 차지백 보고서 생성

비용 청구 보고서를 통해 관리자와 관리자는 애플리케이션, 사업체, 서비스 수준 및 계층별로 용량 사용을 평가할 수 있습니다. 비용 청구 보고서에는 용량 책임, 용량 책임 기록 및 추세 데이터가 포함됩니다. 이러한 보고서의 데이터는 OnCommand Insight 데이터 웨어하우스에서 구축 및 예약됩니다.

시작하기 전에

샘플 보고서를 생성하려면 스토리지 계층에 대한 비용을 보고하도록 시스템을 구성해야 합니다. 다음 작업을 완료해야 합니다.

- 계층에 대한 주석을 정의합니다.

- 주석에 비용을 지정합니다.
- 데이터를 추적할 응용 프로그램을 정의합니다.
- 자산에 응용 프로그램을 할당합니다.

이 작업에 대해

이 예제에서는 Cognos Workspace 고급 보고 도구를 사용하여 Chargeback 보고서를 만듭니다. 작업 영역 고급을 사용하면 데이터 요소를 보고서 팔레트로 끌어 놓아 보고서를 만들 수 있습니다.

단계

1. OnCommand Insight 웹 UI에서 보고 아이콘을 클릭합니다.
2. 보고 포털에 로그인합니다.
3. IBM Cognos Connection 도구 모음에서 * 시작 * > * Cognos Worksapce Advanced * 를 클릭합니다

Workspace 고급 패키지 화면이 열립니다.

4. Packages * > * Chargeback * 을 클릭합니다

IBM Workspace Advantace 화면이 표시됩니다.

5. 새로 만들기 * 를 클릭합니다
6. 새 * 보고서 대화 상자에서 * 목록 * 을 클릭하여 목록 보고서를 지정합니다.

보고서 팔레트가 표시되고 차지백 "단순 데이터 마트"와 "고급 데이터 마트"가 소스 제목 아래에 표시됩니다.

7. 각 데이터 마트 옆에 있는 화살표를 클릭하여 확장합니다.

데이터 마트의 전체 내용이 표시됩니다.

8. '단순 데이터 마트'에서 '응용 프로그램'을 보고서 팔레트의 맨 왼쪽 열로 끌어다 놓습니다.

항목을 팔레트로 드래그하면 열이 축소되고 강조 표시됩니다. 응용 프로그램 데이터를 강조 표시된 열에 놓으면 모든 응용 프로그램이 열에 올바르게 나열됩니다.

9. '단순 데이터 마트'에서 '계층'을 보고서 팔레트의 다음 열로 끌어다 놓습니다.

각 응용 프로그램과 연결된 저장소 계층이 팔레트에 추가됩니다.

10. '단순 데이터 마트'에서 '계층 비용'을 보고서 팔레트의 다음 열로 끌어다 놓습니다.
11. '단순 데이터 마트'에서 '프로비저닝된 용량'을 보고서 팔레트의 다음 열로 끌어다 놓습니다.
12. Ctrl * 키를 누른 상태에서 팔레트에서 ""계층 비용" 및 ""프로비저닝된 용량" 열을 선택합니다.
13. 선택한 열 중 하나에서 마우스 오른쪽 버튼을 클릭합니다.
14. Calculate * > * Tier Cost * Provisioned Capacity DB * 를 클릭합니다

팔레트에 "계층 비용 * 프로비저닝 용량 GB"라는 제목의 새 열이 추가됩니다.

15. Tier Cost * Provision Capacity GB * 열을 마우스 오른쪽 버튼으로 클릭합니다.

16. 스타일 * > * 데이터 형식 * 을 클릭합니다

17. 형식 유형 * > * 통화 * 를 클릭합니다

18. 확인 * 을 클릭합니다

이제 열 데이터의 형식이 미국 통화로 지정됩니다.

19. ""계층 비용 * 용량 할당 GB""를 마우스 오른쪽 버튼으로 클릭하고 * 데이터 항목 레이블 편집 * 을 선택합니다

20. 이름 필드를 ""프로비저닝된 용량 비용""으로 대체

21. 보고서를 실행하려면 * Run * > * Run report-html * 을 클릭합니다

다음과 유사한 보고서가 표시됩니다.

Application	Service Level	Service Level Cost	Tier	Tier Cost	Provisioned Capacity GB	Provisioned Capacity Cost
APAC Commercial Sales	Gold-Fast	12	Gold-Fast	12	674.04	\$8,088.42
APAC Commercial Sales	Silver	10	Silver	7	1,903.83	\$13,326.82
APAC Cruises	Gold-Fast	12	Gold-Fast	12	730.20	\$8,762.44
African Tours	Gold	12	Gold	10	4,856.12	\$48,561.16
African Tours	Silver	10	Silver	7	1,480.85	\$10,365.93
CRM	Bronze	3	Bronze	3	5,689.08	\$17,067.23
Caribbean	Gold	12	Gold	10	4,590.41	\$45,904.08
Commercial Applications	Bronze	3	Bronze	3	14,312.88	\$42,938.64
Commercial Applications	Gold-Fast	12	Gold-Fast	12	40,308.42	\$483,701.05
Commercial Environments	Bronze	3	Bronze	3	16,812.27	\$50,436.81
Commercial Environments	Gold	12	Gold	10	9,313.51	\$93,135.13
Commercial Environments	Silver	10	Silver	7	1,480.79	\$10,365.54
Concur	Gold	12	Gold	10	247.39	\$2,473.91
Concur	Gold-Fast	12	Gold-Fast	12	575.17	\$6,902.09
Consumer Feedback	Gold	12	Gold	10	1,335.89	\$13,358.94

입출력 밀도 보고서가 내부 데이터 볼륨만 설명하도록 합니다

NetApp 스토리지 시스템에서 루트 애그리게이트에 루트 볼륨이 포함되어 있습니다. 루트 볼륨에는 스토리지 시스템을 관리 및 제어하기 위한 특수 디렉토리와 구성 파일이 포함되어 있습니다. 관리 및 제어 작업으로 인해 루트 애그리게이트에 다수의 작업이 생성될 수 있습니다. IO 밀도가 가장 높은 상위 10개 내부 볼륨에 대해 Insight 시스템을 쿼리할 때, 상위 10개 내부 볼륨의 멤버로 NetApp 루트 애그리게이트를 포함할 수 있습니다.

환경을 모니터링할 때 높은 I/O 밀도를 생성하는 내부 데이터 볼륨을 확인하는 것이 더 중요합니다. 데이터 볼륨만 정확하게 식별하려면 NetApp 내부 볼륨을 I/O 밀도를 모니터링하는 데 사용하는 쿼리와 격리해야 합니다.

이 가이드에서는 NetApp 루트 애그리게이트를 쉽게 식별하고, 내부 볼륨 쿼리 결과에서 해당 애그리게이트를 파악하고, 새 NetApp 루트 애그리게이트를 시스템에 추가할 때 제외하는 규칙을 생성하는 방법에 대해 설명합니다. 다음 Insight 기능을 사용하여 I/O 밀도 보고서가 내부 데이터 볼륨에서 파생되도록 할 수 있습니다.

- Insight에서 모니터링하는 모든 NetApp 루트 애그리게이트를 식별할 수 있도록 쿼리가 생성됩니다.
- 각 NetApp 루트 애그리게이트에 하나의 주석이 할당됩니다.

- NetApp 애그리게이트를 제외하기 위해 주식 규칙이 생성됩니다

사용자 환경에서 **NetApp** 루트 애그리게이트를 식별하는 쿼리를 생성합니다

쿼리는 사용자가 선택한 기준에 따라 세분화된 수준으로 검색을 제공합니다. 쿼리를 사용하여 NetApp 루트 애그리게이트가 포함된 환경에서 내부 볼륨을 검색할 수 있습니다.

단계

1. OnCommand Insight 웹 UI에서 쿼리를 생성하여 * 쿼리 * > * 새 쿼리 * > * 리소스 유형 * 을 환경에서 NetApp 루트 애그리게이트를 식별합니다
2. 스토리지 풀 * 을 클릭합니다
3. 루트 애그리게이트의 이름을 입력합니다

이 예제에서는 이름에 ""aggr0""을 사용합니다. Aggregate를 생성할 때 이름의 다음 요구 사항만을 따라야 합니다.

- 문자 또는 밑줄(_)으로 시작해야 합니다.
- 문자, 숫자 및 밑줄만 포함할 수 있습니다.
- 250자 이하일 수 있습니다. 대부분의 경우 Aggregate는 aggr0, aggr_0 또는 이와 유사한 이름을 사용합니다. 사용자 환경에서 모든 NetApp 루트 애그리게이트를 식별하려면 반복적인 프로세스가 필요할 수 있습니다.

4. 저장 * 을 클릭하고 새 쿼리의 이름을 입력합니다.

앞에서 설명한 대로 이 프로세스는 반복 프로세스이며 모든 NetApp 루트 애그리게이트를 확인하기 위해 여러 쿼리가 필요합니다.

쿼리에서 반환된 루트 볼륨에 대한 주석을 생성합니다

주석은 자산에 할당하는 특수 노트로서 주석을 기준으로 자산을 필터링할 수 있습니다. 생성하는 주석은 사용자 환경에서 NetApp 루트 애그리게이트를 파악하고 이러한 애그리게이트가 특정 보고서에 포함되지 않도록 하는 데 사용됩니다.

시작하기 전에

"높은 I/O 밀도" 보고서에서 제외할 루트 애그리게이트를 모두 식별해야 합니다.

단계

1. 쿼리로 식별된 모든 NetApp 루트 애그리게이트를 연결하는 주석을 생성합니다. * Manage * > * Annotations *
2. 추가 * 를 클릭합니다
 - a. 주석의 이름을 * RootAggregr * 로 입력합니다
 - b. 주석에 대한 설명을 입력합니다. * "높은 I/O 밀도" 보고서에서 루트 애그리게이트 제거 *
 - c. 주석 유형 * 부울 * 을 입력합니다
3. 저장 * 을 클릭합니다

I/O 밀도 보고서에서 특정 애그리게이트를 제외하도록 주식 규칙을 생성합니다

개별 자산에 주석을 수동으로 적용하는 대신 주식 규칙을 사용하여 여러 자산에 주석을 자동으로 적용할 수 있습니다. 주식 규칙은 사용자가 만든 쿼리를 기반으로 하며 시스템에서 실행할 때 기존 자산 집합에 새 자산을 추가합니다. 이러한 자산 세트를 보고서에서 제외하면 새 자산도 자동으로 제외됩니다.

시작하기 전에

사용자 환경에서 식별한 NetApp 루트 애그리게이트를 식별하는 쿼리를 작성하여 저장해야 합니다.

단계

1. OnCommand Insight 웹 UI에 로그인합니다.
2. Manage * (관리 *) > * Annotation rules * (주식 규칙 *)를 클릭합니다
3. 추가 * 를 클릭합니다

규칙 추가 대화 상자가 표시됩니다.

4. 다음을 수행합니다.
 - a. 이름 상자에 `""RootAggrExclude""` 규칙을 설명하는 고유한 이름을 입력합니다.
 - b. Query를 클릭하고 Insight가 주식 규칙을 적용할 때 사용해야 할 Query를 선택합니다. `""Aggregate0""`
 - c. 주석을 클릭하고 `""Root agg exclude""`(루트 agg 제외)를 선택합니다.
 - d. 값을 클릭하고 True 를 입력합니다

통합 데이터 수집 중

통합 데이터를 OnCommand Insight 시스템으로 가져올 수 있습니다. 성능 데이터를 수집하는 데몬으로 실행되는 오픈 소스 소프트웨어인 Collectd를 사용하거나 일반 SNMP 데이터를 수집할 수 있는 통합 SNMP 데이터 소스를 사용하여 데이터를 가져올 수 있습니다.

통합 데이터를 위한 데이터 흐름

다음은 OnCommand Insight 서버에 제공할 수 있는 총 통합 데이터 양에 적용됩니다.

- 100개의 통화가 대기됩니다.
클라이언트가 대기열에서 1분 이상 대기하면 시간 초과 오류가 발생합니다.
- 통합 데이터에 권장되는 수집 속도는 클라이언트당 분당 1회입니다.
- 허용되는 통합 객체 유형은 300개로 제한됩니다.

Collectd 소프트웨어 및 설명서 액세스

NetApp의 GitHub 사이트에서 collectd에 대한 출력 작성기 플러그인 소프트웨어 및 문서에 액세스할 수 있습니다.
https://github.com/NetApp/OCI_collectd

통합 데이터의 백업 및 복원

통합 데이터의 백업 및 복구는 OnCommand Insight 성능 데이터 백업 및 복원 정책을 기반으로 모델링됩니다. 성능 데이터를 위해 백업을 구성하면 통합 데이터도 백업에 포함됩니다. 성능 백업과 마찬가지로 최근 7일간의 통합 데이터가 백업에 포함됩니다. 백업에 있는 모든 통합 데이터는 복원 작업에서 복원됩니다.

추가 수익 실적을

통합 데이터를 보고하려면 Perform 라이선스가 필요합니다. Perform 라이선스가 없는 경우 "Perform license required to report integration data(통합 데이터를 보고하는 데 필요한 라이선스 수행)" 메시지와 함께 오류가 발생합니다.

SNMP 통합 데이터를 수집하는 중입니다

통합 SNMP 데이터 소스를 사용하면 OnCommand Insight에서 일반 SNMP 데이터를 수집할 수 있습니다.

통합 팩

SNMP Integration 데이터 소스는 ""통합 팩""을 사용하여 수집되는 통합 값과 이러한 값을 제공하는 SNMP 개체를 정의합니다.

통합 팩은 다음으로 구성됩니다.

- 특정 장치 유형(스위치, 라우터 등)의 SNMP 개체 측면에서 통합 페이로드 콘텐츠를 정의하는 JSON 구성 파일(integration.json)입니다.
- 통합 팩이 의존하는 MIB 파일 목록입니다.

통합 팩은 여러 데이터 유형을 정의할 수 있습니다. 예를 들어 RHEL 호스트를 통합할 때 가동 시간, 사용자 수, 실행 중인 프로세스 수와 같은 일반 시스템 정보에 대해 데이터 유형을 정의할 수 있으며, 메모리 및 파일 시스템 사용 데이터에 대해 두 번째 데이터 유형을 정의할 수 있습니다. 일반적으로 각 데이터 형식은 ""플랫""이어야 하며 중첩된 데이터를 포함할 수 없습니다.

단일 통합 팩에서 24개 이상의 데이터 유형을 정의해서는 안 됩니다. Insight는 수집되는 통합 데이터의 양을 제한합니다. 1분 동안 24개 이상의 보고서를 수집하려고 시도하면 속도 오류가 발생합니다.

통합 유형의 이름은 다음 규칙을 준수해야 합니다.

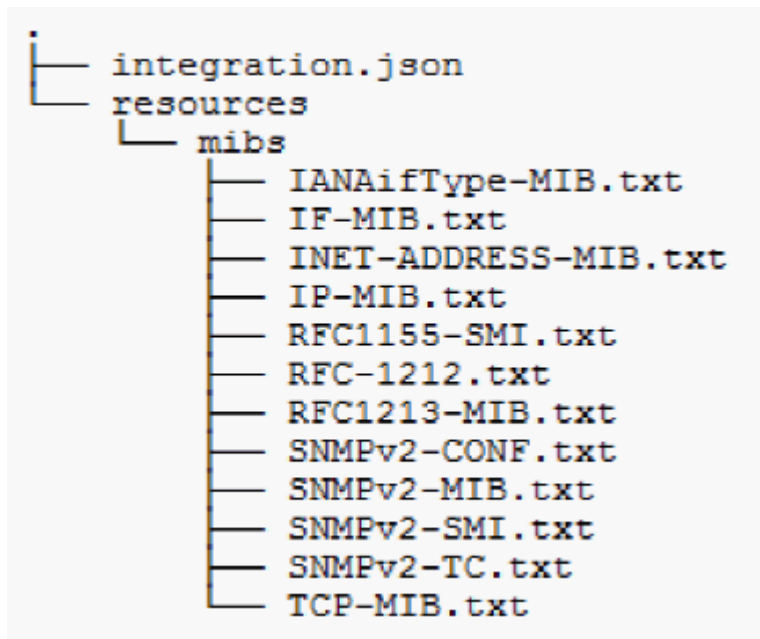
- 이름은 _, - 또는, + 문자로 시작할 수 없습니다
- 이름에는 #, \, /, *, ?, ", <, >, |, ' ,
- UTF-8로 인코딩된 바이트 수가 100개를 초과할 수 없습니다
- 이름을 지정할 수 없습니다. 또는...

통합 파일 형식

통합 팩은 SNMP 개체 측면에서 통합 페이로드 콘텐츠를 정의하는 JSON 구성 파일(integration.json)이 포함된 ZIP 파일입니다. 또한 모든 MIB 파일과 해당 MIB 종속성이 포함된 MIBS 폴더도 포함되어 있습니다.

를 클릭합니다 integration.json 파일은 ZIP 파일의 최상위 수준에 있어야 하며 MIB 파일은 ZIP 내의 "resources/mibs" 하위 디렉토리에 있어야 합니다. 필요한 경우 ZIP 파일에는 "readme.txt"와 같은 파일도 포함될 수

있습니다. 통합 ZIP 구조의 예는 다음과 같습니다.



SNMP 통합 팩을 가져오는 중입니다

웹 UI를 사용하여 SNMP 통합 팩을 OnCommand Insight로 가져옵니다. 통합 팩은 에 정의된 "통합 팩 이름" 값으로 식별됩니다 integration.json ZIP 파일에 포함된 구성 파일입니다.

시작하기 전에

OnCommand Insight 서버로 가져올 통합 팩이 포함된 올바른 형식의 ZIP 파일을 만들어야 합니다.

이 작업에 대해

다음 단계를 사용하여 SNMP 통합 팩을 Insight 서버로 가져옵니다.

단계

1. Admin * > * Setup * > * SNMP Integration * 을 클릭합니다

SNMP 패키지 가져오기 화면이 표시됩니다.

Import SNMP package

📁 Select file No file selected ⬇ Import

Warning: This will overwrite any conflicting package from existing database.

2. SNMP 패키지가 포함된 로컬 파일을 선택하려면 * 파일 선택 * 을 클릭합니다.

선택한 파일이 파일 상자에 표시됩니다.



같은 이름의 기존 통합 팩을 덮어씁니다.

3. 가져오기 * 를 클릭합니다

파일을 Insight 서버로 가져옵니다.

SNMP 통합 데이터 소스 생성

통합 SNMP 데이터 소스는 Brocade 및 Cisco용 OnCommand Insight 데이터 소스에 포함된 다른 SNMP 기반 데이터 소스와 유사한 공통 SNMP 구성 속성을 제공합니다.

시작하기 전에

Integration SNMP 데이터 소스를 성공적으로 사용하여 수집하려면 다음 조건이 참이어야 합니다.

- 이 SNMP 데이터 소스에 사용할 통합 팩을 이미 가져와야 합니다.
- 모든 타겟 디바이스는 동일한 자격 증명을 공유합니다.
- 모든 타겟 디바이스는 구성된 통합 팩이 참조하는 SNMP 객체를 구현합니다.

이 작업에 대해

SNMP Integration 데이터 소스를 생성하려면 데이터 소스 생성 마법사에서 공급업체 "통합"과 모델 "SNMP"를 선택합니다.

단계

1. OnCommand Insight 웹 UI에서 * 관리자 * > * 데이터 소스 * 를 클릭합니다
2. 추가 * 를 클릭합니다
3. 데이터 원본의 이름을 입력합니다
4. 공급 업체의 경우 * 통합 * 을 선택합니다
5. 모델 에서 * SNMP * 를 선택합니다

Add data source

Settings

*Name

Vendor

Integration

Model

SNMP

Where to run

local

What to collect

☒ Integration (BETA)

Configure

Configuration

Advanced configuration

Test

Cancel

Save

6. 수집 대상 에 대해서는 * 통합 * 을 확인하십시오

이 데이터 원본의 유일한 패키지이며 기본적으로 선택되어 있습니다.

7. 구성 * 을 클릭합니다

8. SNMP 데이터를 수집할 시스템의 IP 주소를 입력합니다

9. 가져온 SNMP 통합 팩을 선택합니다

10. 통합 폴링 간격을 설정합니다

11. SNMP 버전을 선택합니다

12. SNMP 커뮤니티 문자열을 입력합니다

SNMP V1 및 V2의 경우

13. 데이터를 수집할 시스템의 사용자 이름과 암호를 추가합니다.

SNMP V3의 경우

14. 고급 구성 * 을 클릭합니다

고급 구성 기본 설정이 표시됩니다. 필요한 설정을 변경합니다.

integration.json 파일 정보

integration.json 파일은 페이로드를 식별합니다.

다음 그림에서는 간단한 통합 .json 파일의 컬러 코딩 표현을 제공합니다. 첨부 테이블은 파일에 있는 오브젝트의 기능을 식별합니다.

```
{
  "integrationPackName": "WindowsSnmp",
  "description": "Generic integration for mibs supported by the default
SNMP Agent for Windows 2012, including HOST-RESOURCES",
  "acquisitionType": "SNMP",
  "integrationTypes": [
    {
      "integrationType": "snmp_win2012_host",
      "name": {
        "mibModuleName": "RFC1213-MIB",
        "objectName": "sysName"
      },
      "identifiers": {
        "hostname": {
          "mibModuleName": "RFC1213-MIB",
        }
      },
      "attributes": {
        "description": {
          "mibModuleName": "RFC1213-MIB",
          "objectName": "sysDescr"
        },
        "snmp_sys_obj_id": {
          "mibModuleName": "RFC1213-MIB",
          "objectName": "sysObjectID"
        }
      },
      "dataPoints": {
        "uptime": {
          "num": {
            "mibModuleName": "RFC1213-MIB",
            "objectName": "sysUpTime"
          }
        }
      }
    }
  ]
}
```

Blue	Reserved
Red	User customizable strings and IDs
Green	MIB names
Purple	MIB object
Black	JSON structure

integration.json 파일 정보

각 필드에는 다음과 같은 특성이 있습니다.

- "식별자" 섹션은 Insight에서 새 "개체"를 만들기 위해 고유한 복합 키를 형성합니다
- "속성"은 객체에 대한 메타 데이터를 지원합니다.

이 두 경우 모두 해당 개체에 대한 최신 보고서 값(식별자로 식별)만 보존됩니다.

- "데이터 요소"는 시계열 데이터이며 숫자 값이어야 합니다. Insight는 여기에 보고된 각 값과 모든 값을 기본적으로 90일 동안 유지하고 타임 시리즈를 식별된 개체에 연결합니다.

수치 표현식

기본적으로 모든 값 식은 통합 페이로드에서 문자열로 보고됩니다. "식별자" 및 "특성"은 문자열 값만 정의할 수 있습니다. "datapoints"는 문자열 또는 숫자 값을 정의할 수 있습니다. 숫자 값은 다음 한정자 키 중 하나를 사용하여 정의됩니다.

- Num - 카운터가 마지막으로 초기화된 이후 수신된 총 바이트 수입니다
- Delta - 폴링 간격 동안 수신된 바이트 수입니다
- 속도 - 폴링 간격 동안의 평균 수신 속도(바이트/초)입니다

폴링 간격 동안 초당 메가바이트의 평균 수신 속도는 속도 및 수학 연산의 조합을 사용하여 수행할 수 있습니다

수학 연산

를 클릭합니다 integration.json 파일에서 지원되는 수학 연산은 더하기, 빼기, 곱하기, 나누기 입니다. 다음 예제에서는 JSON 파일의 곱하기, 나누기 및 합계 작업을 보여 줍니다.

```

"network_utilization":
{
  "mult": [
    {
      "div": [
        {
          "sum": [
            "rate": {
              "mibModuleName": "IF-MIB",
              "objectName": "ifHCOutOctets",
              "comment": "bytes per second out"
            },
            "rate": {
              "mibModuleName": "IF-MIB",
              "objectName": "ifHCInOctets",
              "comment": "bytes per second in"
            }
          ]
        },
        {
          "num": {
            "mibModuleName": "IF-MIB",
            "objectName": "ifSpeed",
            "comment": "1,000,000 bits per second"
          }
        }
      ],
      "const": 0.0008,
      "comment": "normalize to ratio of bits and convert to percent:
8 * 100 / 1,000,000 = 0.0008"
    }
  ]
}

```

키워드

통합 팩 키워드 string은 일반적으로 16진수 형식으로 렌더링되어 ASCII 문자로 렌더링되는 옥텟 문자열이나 옥텟 문자열에서 파생된 독점 형식을 강제로 사용하도록 구현됩니다.

옥텟 문자열에는 대개 바이너리 데이터가 포함됩니다(예: MAC 주소 및 WWN:

```

"interface_mac": {
  "mibModuleName": "IF-MIB",
  "objectName": "ifPhysAddress"
}

```

ifPhysAddress 는 물리주소 유형으로, 옥텟 문자열일 뿐입니다:

```

PhysAddress ::= TEXTUAL-CONVENTION
    DISPLAY-HINT "1x:"
    STATUS      current
    DESCRIPTION
        "Represents media- or physical-level
addresses."
    SYNTAX      OCTET STRING

```

ifPhysAddress 가 기본적으로 16진수로 렌더링되면 결과는 다음과 같습니다.

```
"interface_mac": "00:50:56:A2:07:E7"
```

그러나 ASCII로 해석하려는 옥텟 문자열에서 파생된 옥텟 문자열 또는 독점 유형이 있는 경우 "string" 키워드를 사용할 수 있습니다.

```

"string_test_1": {
    "string": {
        "mibModuleName":      "IF-MIB",
        "objectName":         "ifPhysAddress"
    }
},

"string_test_2": {
    "string": [
        {
            "mibModuleName":      "IF-MIB",
            "objectName":         "ifPhysAddress"
        },
        {
            "const": "JSD"
        },
        {
            "mibModuleName":      "IF-MIB",
            "objectName":         "ifPhysAddress"
        }
    ]
}

```

키워드는 기존 문자열 연결 규칙을 따르며 다음 예제에서 용어 사이에 공백을 하나만 삽입합니다.

```

"string_test_1": "PV☞☞",
"string_test_2": "PV☞☞ JSD PV☞☞"

```

"string" 키워드는 단일 용어 또는 용어 목록에 작동하지만 중첩된 식에는 적용되지 않습니다. 중첩 식은 dataPoint 표현식에만 지원됩니다. dataPoint 식에서 "string" 식을 사용하려고 하면 다음과 유사한 오류가 발생합니다.

```
_java.lang.IllegalArgumentException: 통합 팩 'GenericSwitch32' 인덱스 'snmp_generic_interface_32' 섹션  
'ataPoints' 키 'tring_test_3'은 지원되지 않는 JSON 수치 표현식 '{"string":{"mibModuleName":"if-MIB",  
"ifjectName"}}' _
```

DisplayString, SnmpAdminString 등의 일부 파생 옥텟 문자열 형식은 "string" 키워드보다 하드 코딩된 우선 순위를 가집니다. 이는 특히 SnmpAdminString이 UTF-8로 인코딩되어 올바르게 처리하려고 하는 반면 "string" 키워드는 문자당 1바이트 ASCII 코드 포인트를 사용하는 snmp_Framework에서 반환하는 기본 문자열 표현을 강제로 사용하기 때문입니다.

애플리케이션 성능 문제 분석

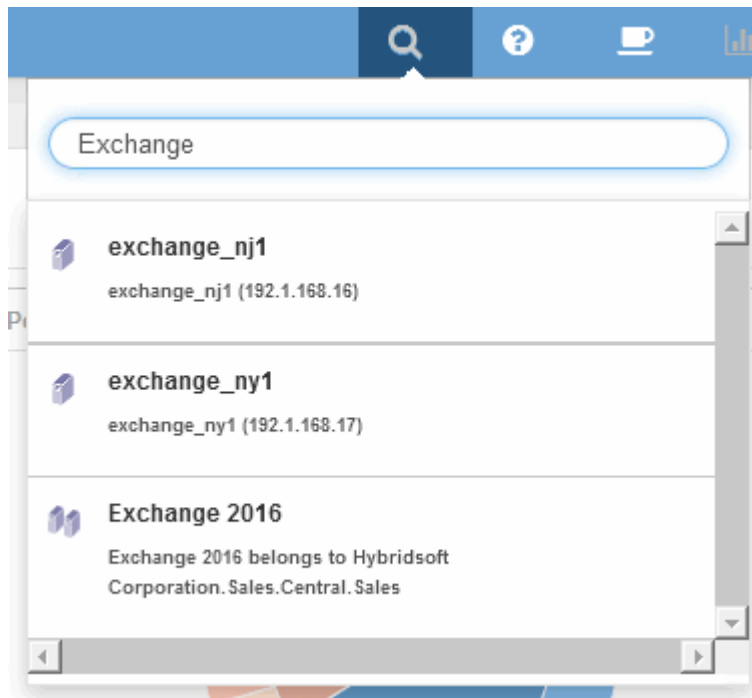
이 문서에서는 사용자 또는 관리자에게 영향을 주는 응용 프로그램의 성능 문제 보고서를 해결하기 위해 수행할 수 있는 단계에 대해 설명합니다. 예를 들어, 사용자는 Exchange 애플리케이션이 하루 종일 느려지는 것을 호소합니다.

이 작업에 대해

OnCommand Insight에서 응용 프로그램은 구성된 엔터티입니다. 이를 및 업무 엔티티를 애플리케이션에 할당하고 컴퓨팅 및 스토리지 리소스를 애플리케이션에 할당합니다. 이를 통해 인프라 상태를 보다 효과적으로 엔드 투 엔드 방식으로 확인하고 인프라 자산 관리를 보다 선제적인 방식으로 관리할 수 있습니다.

단계

1. 문제 조사를 시작하려면 Insight 도구 모음을 사용하여 Exchange 애플리케이션에 대한 전체 검색을 수행합니다.



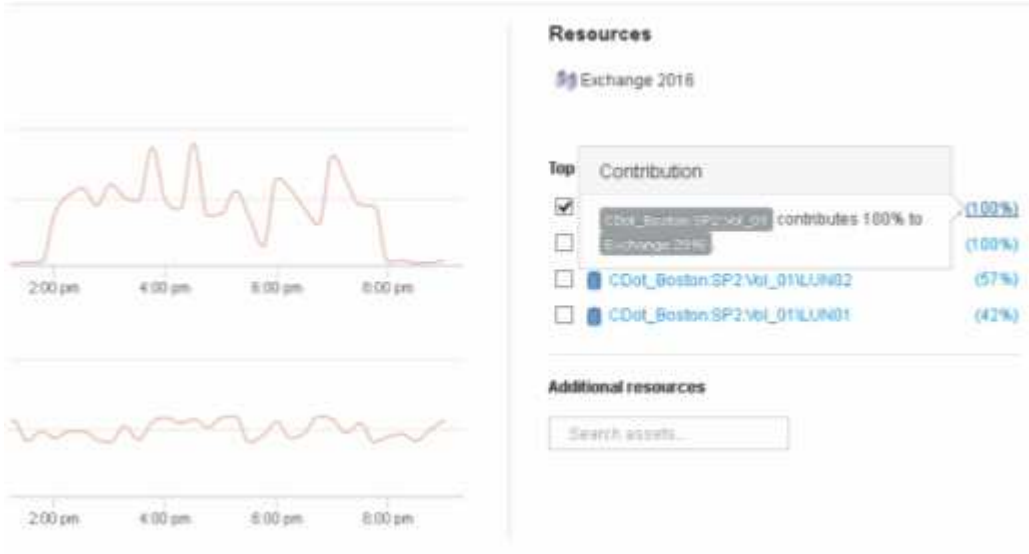
검색을 수행할 때 개체 이름 앞에 개체 설명자를 추가하여 검색 결과를 구체화할 수 있습니다.

2. 검색 결과에서 "Exchange 2016"을 선택하면 애플리케이션 랜딩 페이지가 표시됩니다.



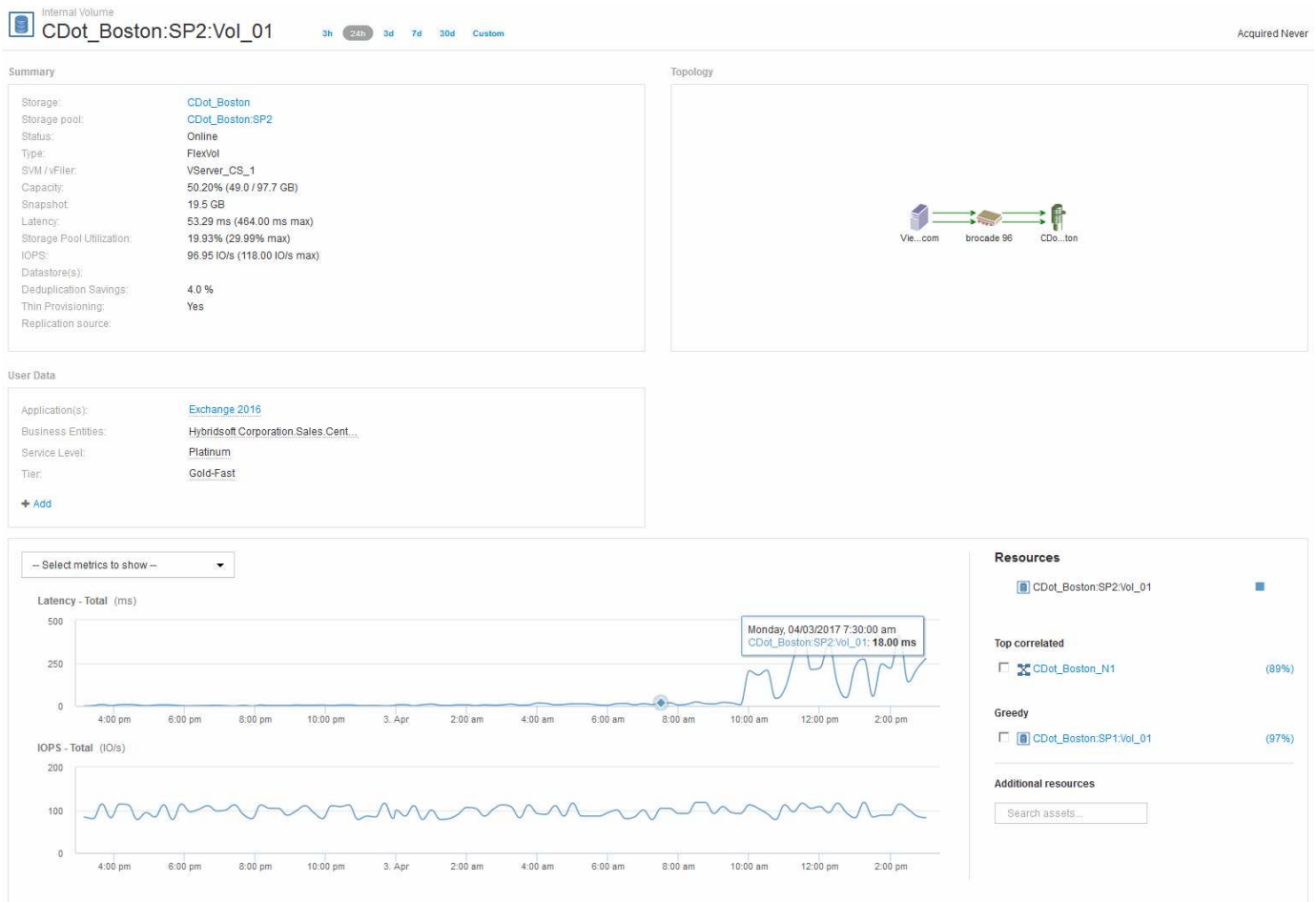
애플리케이션 랜딩 페이지에서 다음 정보를 확인할 수 있습니다.

- 선택한 24시간 간격 동안 지연 시간 그래프 오른쪽에 지연 시간 증가가 표시됩니다.
- 지연 시간이 증가하는 동안에는 IOPS 레벨이 크게 변경되지 않습니다. 지연 시간이 증가하는 것은 애플리케이션 사용량이 증가했기 때문인 것 같습니다. 실제로 지연 시간의 급증에 대해 고려될 수 있는 스토리지에 대한 높은 IOPS 수요가 있는 것은 아닙니다. 지연 시간의 증가는 외부 요인으로 인해 발생할 수 있습니다.
- 최상위 기여 요소 섹션의 차트 오른쪽에서 선택한 내부 볼륨(cDOT_Boston:SP2:Vol_01)에 대해 100%를 클릭합니다. 이 리소스가 Exchange 2016 애플리케이션에 100% 기여하고 있음을 시스템에서 보여줍니다.



- 이 내부 볼륨(cDOT_Boston:SP2:Vol_01)에 대한 탐색 링크를 클릭하여 내부 볼륨 랜딩 페이지에 액세스합니다. 내부 볼륨에 대한 분석에서는 지연 시간 급증과 관련된 정보를 제공할 수 있습니다.

내부 볼륨 검사



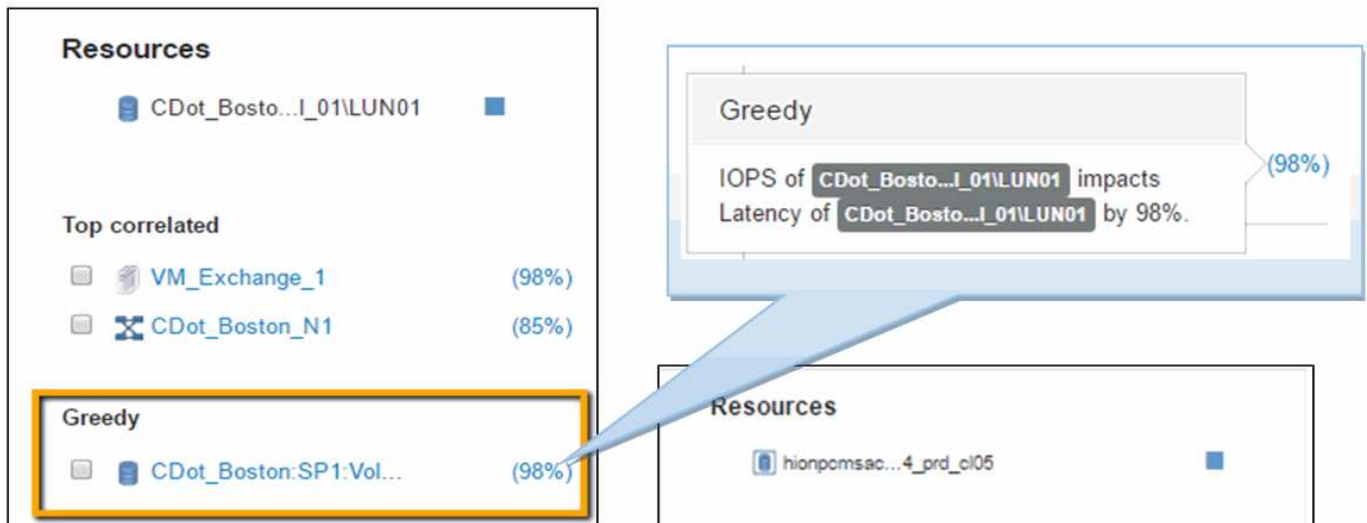
내부 볼륨 랜딩 페이지에는 다음이 표시됩니다.

- 내부 볼륨의 성능 차트는 지연 시간 및 IOPS 측면에서 이전에 볼 수 있었던 애플리케이션 성능 차트와 일치합니다.
- 관련 자산이 표시되는 Resources 섹션에서 "greedy" 리소스가 식별됩니다(CDOT_Boston:SP1:Vol_01).

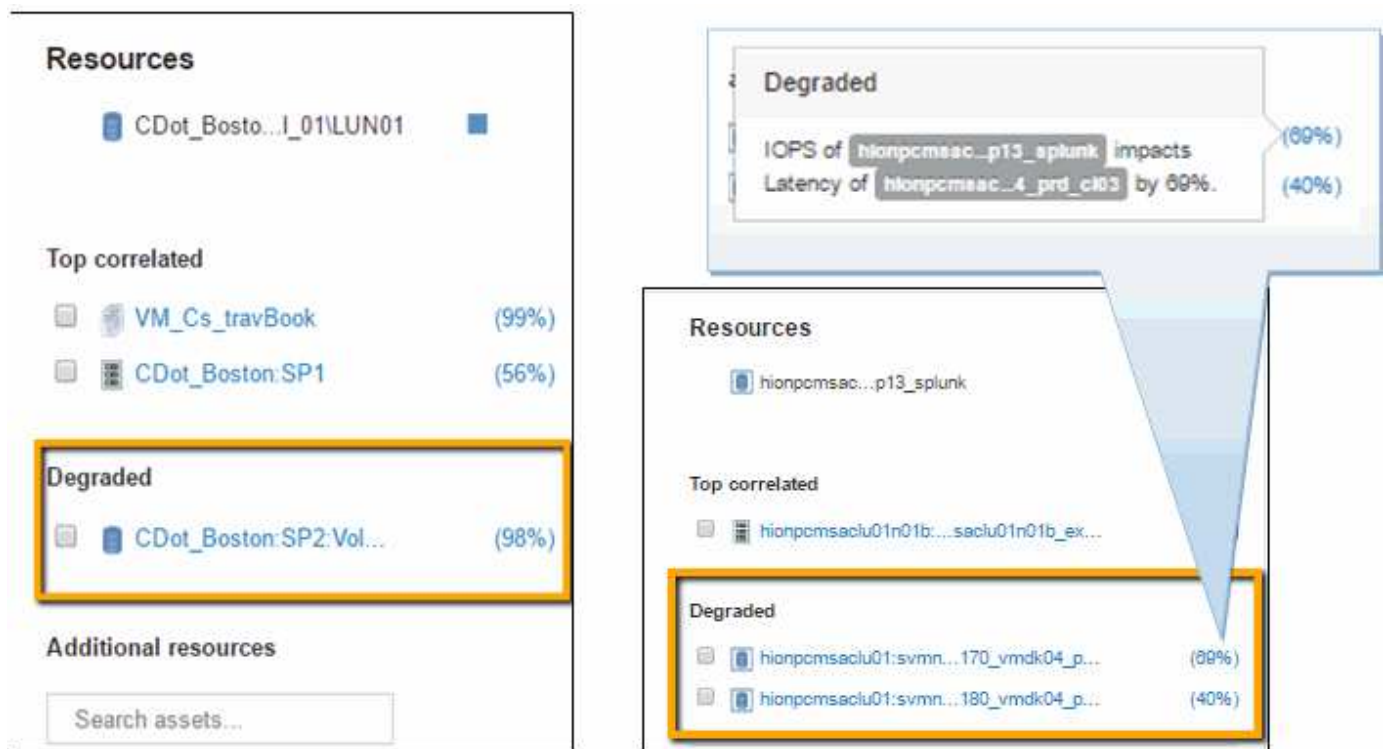
과다 사용 리소스는 통찰력 상관 관계 분석으로 식별됩니다. 욕심/성능 저하 리소스는 동일한 공유 리소스를 활용하는 "피어"입니다. greedy 리소스에는 성능이 저하된 리소스의 IOPS 또는 지연 시간에 부정적인 영향을 주는 IOPS 또는 사용률이 있습니다.

가상 머신, 볼륨 및 내부 볼륨 랜딩 페이지에서 과다 사용 및 성능 저하 리소스를 확인할 수 있습니다. 각 랜딩 페이지에는 최대 2개의 greedy 리소스가 표시됩니다.

상관 순위(%)를 선택하면 greedy 리소스 분석 결과가 제공됩니다. 예를 들어, greedy percentage 값을 클릭하면 다음 예에 표시된 것과 유사하게 Degraded 자산의 작업에 영향을 주는 작업이 식별됩니다.



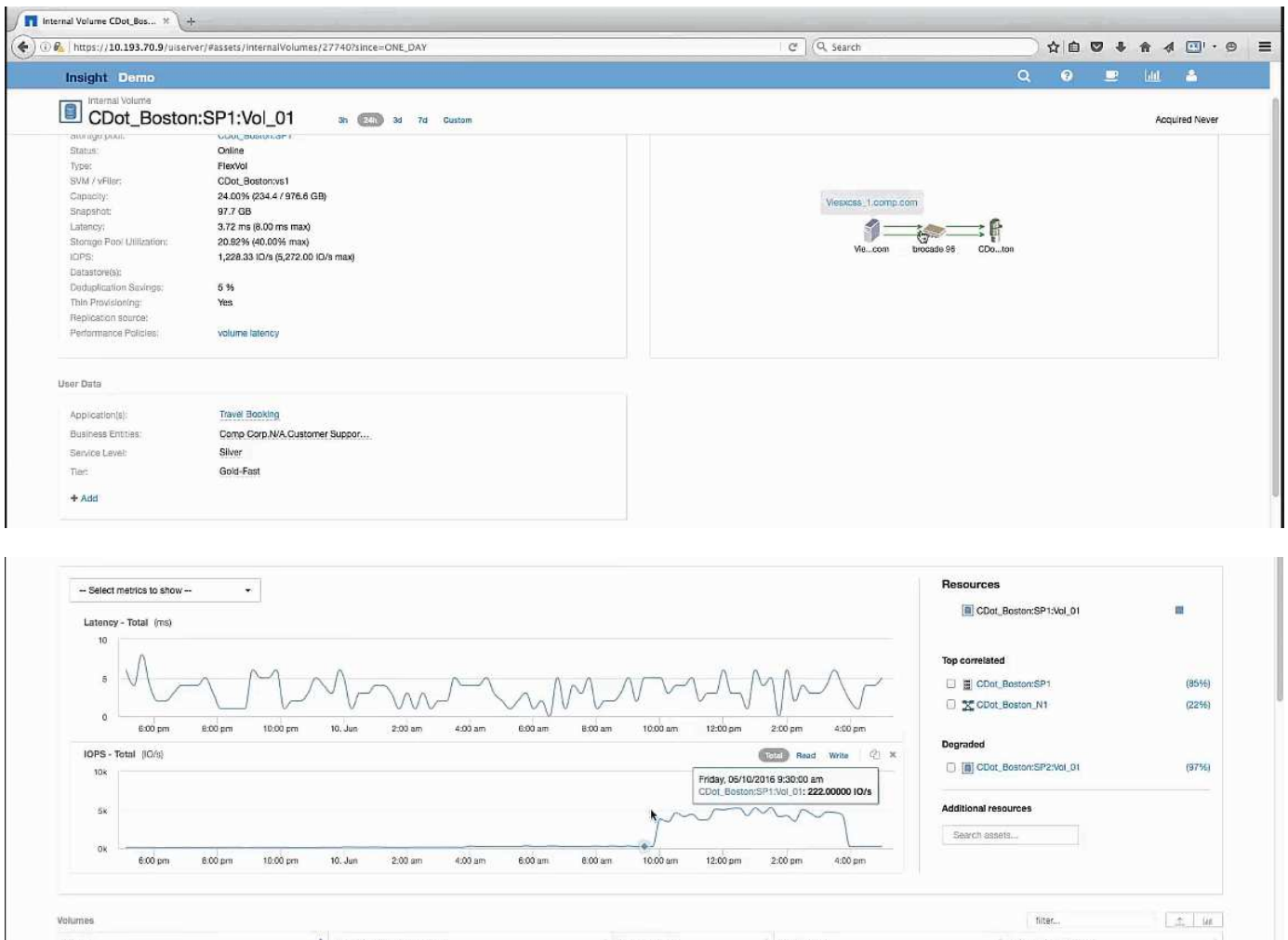
성능이 저하된 리소스가 식별되면 성능 저하(%) 점수를 선택하여 성능이 저하된 리소스에 영향을 미치는 작업 및 리소스를 식별할 수 있습니다.



greedy 리소스 검사

greedy 리소스로 식별된 내부 볼륨을 클릭하면 볼륨 cDOT_Boston:SP1:Vol_01의 랜딩 페이지가 열립니다.

요약에서 이 내부 볼륨은 다른 애플리케이션(여행 예약)을 위한 리소스이며, 다른 스토리지 풀에 포함되어 있지만 Exchange 2016(cDOT_Boston_N1)의 내부 볼륨과 동일한 노드에 있습니다.



랜딩 페이지에는 다음이 표시됩니다.

- 여행 예약 신청과 관련된 내부 볼륨입니다.
- 상호 연결된 리소스에서 새 스토리지 풀이 식별됩니다.
- 검사 중인 원래 내부 볼륨(cDOT_Boston:SP2:Vol_01)은 "Degraded"로 식별됩니다.
- 성능 그래프에서 애플리케이션의 지연 시간 급증은 안정적인 지연 시간 프로필을 기반으로 하며, Exchange 애플리케이션의 지연 시간 급증과 동시에 대충 IOPS 스파이크가 발생합니다.

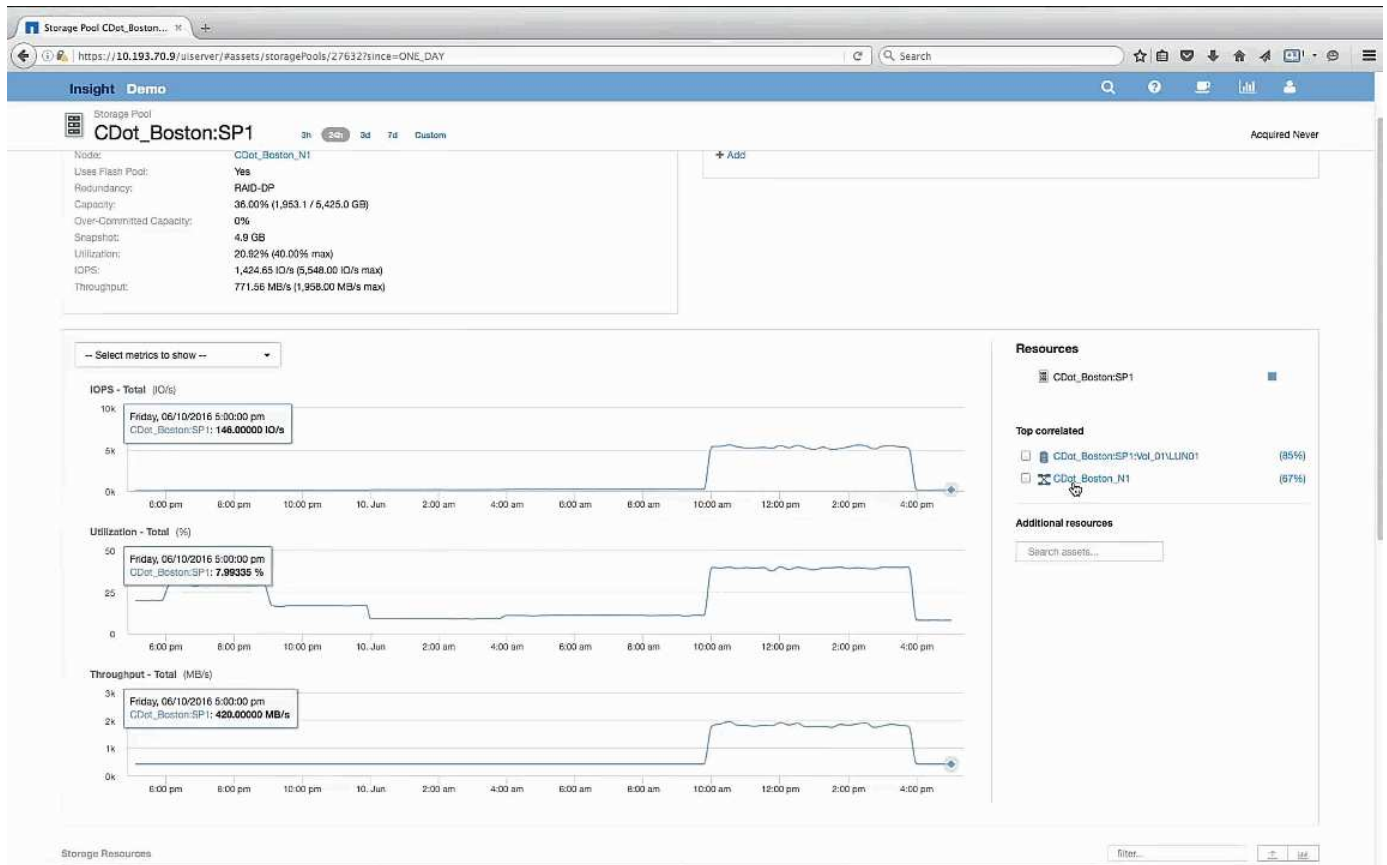
이는 Exchange 애플리케이션의 지연 시간 급증이 이 볼륨의 IOPS 급증으로 인한 것일 수 있음을 나타낼 수 있습니다.

리소스 섹션의 차트 오른쪽에는 Exchange 2016 내부 볼륨(cDOT_Boston:SP2:Vol_01)인 상관 관계 저하된 리소스가 표시됩니다. 성능 그래프에 저하된 내부 볼륨을 포함하려면 확인란을 클릭합니다. 두 성능 그래프를 정렬하면 지연 시간과 IOPS 급증이 거의 동시에 발생하는 것을 알 수 있습니다. 이는 여행 예약 애플리케이션에 대한 이해를 높이는 데 도움이 됩니다. 애플리케이션에 이와 같은 장시간 IOPS 스파이크가 발생하는 이유를 파악해야 합니다.

Travel Booking 애플리케이션과 연결된 스토리지 풀을 검사하면 애플리케이션에 IOPS 스파이크가 발생하는 이유를 파악할 수 있습니다. 스토리지 풀 랜딩 페이지를 보려면 cDOT_Boston:SP1을 클릭하십시오.

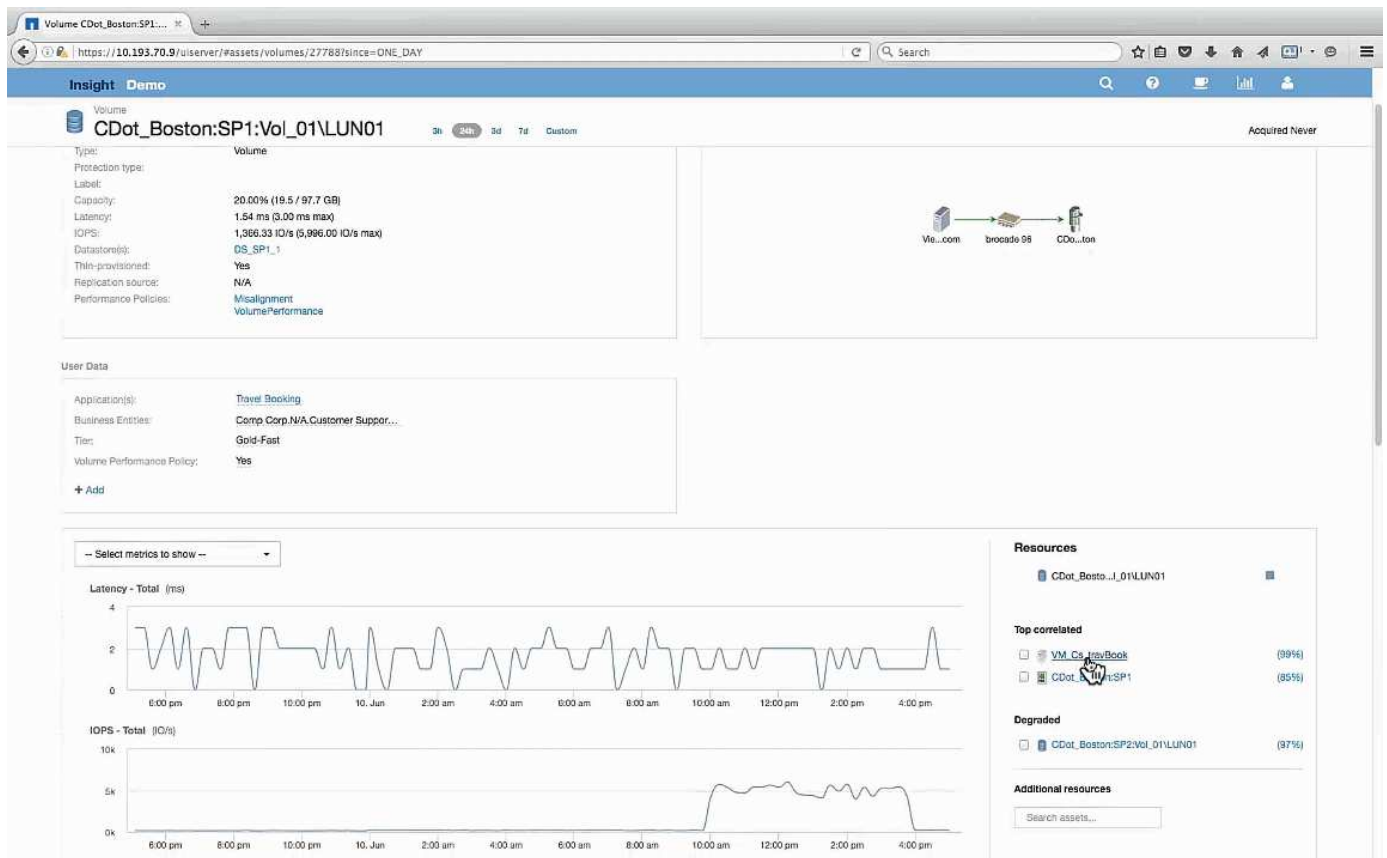
스토리지 풀을 검토합니다

스토리지 풀 랜딩 페이지를 살펴보면 상호 연결된 자산에서 볼 수 있는 것과 동일한 IOPS 급증이 나타납니다. 리소스 섹션에서 이 스토리지 풀 랜딩 페이지가 여행 애플리케이션의 볼륨에 링크되어 있음을 확인할 수 있습니다. 볼륨을 클릭하여 볼륨 랜딩 페이지를 엽니다.



볼륨을 검사하는 중입니다

볼륨 랜딩 페이지에는 상호 연결된 자산에서 볼 수 있는 것과 동일한 친숙한 IOPS 급증 문제가 표시됩니다.



리소스 섹션에서 여행 예약 애플리케이션의 VM이 식별됩니다. VM 랜딩 페이지를 보려면 VM 링크를 클릭하십시오.

VM 검사

VM 랜딩 페이지에서 CPU 사용률 및 메모리 사용률을 표시하고 포함할 추가 메트릭을 선택합니다. CPU 및 메모리 활용도에 대한 그래프는 모두 거의 100%의 용량으로 작동하고 있음을 보여줍니다. 이는 Exchange Server의 문제가 스토리지 문제가 아니라 VM CPU 및 메모리 사용률이 높고 I/O를 디스크로 스왑하는 결과라는 것을 의미합니다.



이 문제를 해결하려면 유사한 리소스를 추가로 찾을 수 있습니다. 추가 리소스 입력 대화 상자에 ""노드""를 입력하여 Exchange VM과 유사한 자산에 대한 메트릭을 표시합니다. 이 비교는 변경이 필요할 경우 워크로드를 호스팅하는 데 더 적합한 노드를 파악하는 데 도움이 될 수 있습니다.



AWS 청구 데이터 수집 및 보고

Amazon AWS Cloud Cost 데이터 소스는 Amazon에서 생성된 청구 데이터를 통합 데이터로 Insight로 가져와, 데이터 웨어하우스에 보고 기능을 제공합니다.

Insight에서 클라우드 청구 데이터를 사용할 수 있도록 하는 3가지 요소:

AWS 계정 정보를 확인하는 중입니다.

Insight에서 AWS Cloud Cost 데이터 소스를 구성하여 데이터를 수집합니다.

보고서에서 사용할 ETL을 통해 데이터 웨어하우스로 데이터 전송

Insight 데이터 수집을 위한 AWS 준비

Insight에서 클라우드 비용 데이터를 수집할 수 있도록 AWS 계정을 올바르게 구성해야 합니다.

이 작업에 대해

다음 단계는 AWS 계정을 통해 수행됩니다. 자세한 내용은 아마존 문서를 참조하십시오.

["http://docs.aws.amazon.com"](http://docs.aws.amazon.com). AWS 클라우드 계정 설정에 대해 잘 모르는 경우 클라우드 공급자에게 지원을 문의하십시오.



이러한 단계는 예의상 제공된 것으로, 발행 시점을 기준으로 정확합니다. NetApp은 이러한 단계의 정확성을 보증하지 않습니다. AWS 계정 구성에 대한 정보나 지원은 클라우드 공급자 또는 AWS 계정 보유자에게 문의하십시오.

모범 사례: Insight는 청구 보고서가 업로드되는 S3 버킷을 소유한 동일한 계정에서 기본 IAM 사용자를 생성하고 이 사용자를 사용하여 AWS 청구 데이터를 구성 및 수집할 것을 권장합니다.

Insight에서 데이터를 수집할 수 있도록 AWS 계정을 구성하려면 다음 단계를 수행하십시오.

단계

1. AWS 계정에 IAM(Identity Access Management) 사용자로 로그인합니다. 적절한 수집을 위해 그룹 IAM 계정이 아닌 기본 IAM 계정에 로그인합니다.
2. Amazon S3 * 로 이동하여 버킷을 생성합니다. 고유한 버킷 이름을 입력하고 올바른 지역을 확인하십시오.
3. 아마존 비용 및 사용량 보고서를 봅니다. 을 참조하십시오 <https://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/billing-reports-gettingstarted-turnonreports.html> 를 참조하십시오.
 - a. AWS 청구 및 비용 관리 대시보드로 이동하여 * Reports * 를 선택합니다.
 - b. 보고서 작성 * 을 클릭하고 보고서 이름 을 입력합니다. 시간 단위 * 의 경우 매일 을 선택합니다. 리소스 ID * 를 포함하려면 확인란을 선택하고 * 다음 * 을 클릭합니다.
 - c. 배달 옵션 선택 페이지에서 * 샘플 정책 * 링크를 클릭합니다. 상자에 있는 샘플 정책 텍스트를 클립보드로 복사합니다. 닫기 * 를 클릭합니다.
 - d. 생성된 S3 버킷으로 돌아가 * Permissions * 탭을 클릭하고 * Bucket Policy * 버튼을 선택합니다.
 - e. 샘플 정책의 텍스트를 붙여 넣고 바꿉니다 <bucketname> 다음을 포함하는 각 줄에 실제 버킷 이름 포함: "Resource": "arn:aws:s3::: <bucketname>". * 정책을 저장 * 합니다.
 - f. 보고서 작성 화면으로 돌아가서 S3 버킷을 입력하고 * 확인 * 버튼을 클릭합니다. 다음 * 을 클릭합니다.
 - g. 정보를 확인하고 * 검토 및 완료 * 를 클릭합니다.
4. Insight에서 AWS에서 데이터를 수집하려면 사용 권한을 부여해야 합니다. 다음 링크에서는 * 모든 버킷 나열 * (4.1단계) 및 폴더의 객체에 대한 권한을 설정하는 방법에 대한 자세한 정보를 제공합니다(5.2단계).

<https://docs.aws.amazon.com/AmazonS3/latest/dev/walkthrough1.html>.

5. IAM 콘솔에서 * Policies * 로 이동하고 * Create policy * 를 클릭합니다.
6. Policy Name * 필드에 이름을 입력하고 하단의 * Create policy * 를 클릭합니다.
7. IAM 콘솔에서 사용자를 선택한 다음 화면 하단의 * Add Inline Policy * 를 선택합니다.
8. 서비스 선택 * 을 클릭하고 S3을 선택합니다.
9. JSON * 탭으로 이동합니다. JSON 샘플 텍스트를 AWS 연습의 5.1.2.g 단계에서 JSON 상자로 복사합니다.
10. JSON의 _companybucket_and_Development_fields를 S3 정보로 바꾸십시오.
11. 정책 설정을 검토하려면 * 정책 검토 * 를 클릭합니다.

AWS Cloud Cost 데이터 소스 구성

모든 Insight 데이터 원본과 마찬가지로 AWS Cloud Cost 데이터 소스를 구성합니다.

시작하기 전에

Insight 데이터를 수집할 수 있도록 Amazon AWS 계정이 이미 설정 및 준비되어 있어야 하며, 다음 정보를 준비해 두어야 합니다.

- 보고서 이름
- S3 버킷 이름
- S3 버킷이 상주하는 AWS 지역
- 보고서 경로 접두어

이 작업에 대해

AWS 계정이 준비되고 적절한 사용 권한이 설정되면 청구 보고서 데이터를 수집하도록 OnCommand Insight를 구성할 수 있습니다.



청구 데이터를 검색할 각 청구 가능한 사용자/계정에 대해 별도의 AWS Cloud Cost 데이터 소스를 추가해야 합니다.

단계

1. 관리자로 OnCommand Insight에 로그인합니다.
2. Admin * > * Data Sources * 를 클릭하여 Insight Data Source 페이지를 엽니다.
3. 새 데이터 원본을 추가하려면 * + 추가 * 를 클릭합니다. Amazon * 을 선택하고 * AWS 클라우드 비용 * 을 선택합니다.
4. Configuration * 섹션에서 *Report name*, *S3 Bucket_name*, *_S3 Region*(S3 버킷이 있는 지역이어야 함), *Report path prefix*, *AWS IAM Access Key ID* 및 *_AWS IAM Secret Access Key _* 를 입력합니다. 확실하지 않은 경우 클라우드 공급자 또는 AWS 계정 보유자에게 문의하십시오.
5. 이 확인란을 클릭하여 AWS에서 Insight 데이터 소스에서 발생하는 API 요청 및 데이터 전송에 대해 요금을 청구하는지 확인합니다.
6. 고급 구성 * 에서 HTTP 연결 및 소켓 시간 초과를 입력합니다. 기본값은 300초입니다.

7. 저장 * 을 클릭합니다.

Insight에서 AWS Cloud Cost 데이터 처리

Insight는 이전 달에 한 번 AWS 청구 보고서에서 데이터를 수집하고, 해당 월의 최종 클라우드 비용을 반영합니다.

AWS Cloud Cost 데이터 소스를 설정한 후 S3로 생성된 청구 보고서가 이미 있는 경우 첫 번째 데이터 소스 폴링 직후 최대 3개월의 이전 데이터를 받게 됩니다.

Insight는 AWS의 "최종" 데이터를 한 달에 한 번 수집합니다. 이 컬렉션은 이전 달이 끝나고 며칠 후에 이루어지므로 AWS에서 실제 데이터를 마무리할 수 있습니다.

AWS 청구 데이터는 Insight의 데이터 웨어하우스로 전송되어 보고에 사용됩니다.

각 데이터 소스는 청구 가능한 단일 계정/사용자에 대해 구성되어야 합니다.

Insight의 클라우드 비용 데이터 보고

Insight에서 수집된 클라우드 비용 월간 데이터는 데이터 웨어하우스로 전송되며, Cloud Cost Datamart에서 보고서에 사용할 수 있습니다.

시작하기 전에

AWS에서 클라우드 비용 데이터를 수집하도록 구성된 데이터 소스가 있어야 합니다. 청구 가능한 각 사용자/계정에는 별도의 데이터 원본이 있어야 합니다.

Insight에서 데이터 수집을 시작하는 데 최소 36시간이 걸립니다.

데이터 웨어하우스로 데이터를 전송하기 위해 ETL이 적어도 한 번 실행되도록 합니다.


이 작업에 대해

데이터가 수집되어 데이터 웨어하우스로 전송된 후에는 미리 구성된 여러 보고서에서 데이터를 보거나 사용자 지정 보고서를 만들 수 있습니다. Insight는 데이터를 자체 클라우드 비용 데이터마트에 저장합니다.

사전 구성된 보고서 중 하나에서 클라우드 비용 데이터를 보려면

단계

1. 다음 방법 중 하나를 사용하여 Insight Reporting을 엽니다.

- 보고 포털 아이콘을 클릭합니다  Insight 서버 웹 UI 또는 데이터 웨어하우스 UI에서
- 다음 URL을 입력하여 직접 보고를 시작합니다. https://<dwh_server_name>:9300/p2pd/servlet/dispatch 또는 https://<dwh_server_name>:9300/bi (7.3.3 and later)

2. 보고에 로그인하면 * 공용 폴더 * 를 클릭하고 * 클라우드 비용 * 을 선택합니다.

3. Cloud Cost * 폴더에 있는 사용 가능한 보고서에서 AWS 청구 데이터를 보거나 * Packages * 폴더에서 사용 가능한 * Cloud Cost Datamart * 를 사용하여 사용자 정의 보고서를 만들 수 있습니다.

ServiceNow와 통합

OnCommand Insight는 ServiceNow 관리 소프트웨어와 통합되어 제품별로 제공하는 것보다 더 큰 가치를 제공합니다.

Python 스크립트를 사용하여 Insight는 ServiceNow와 데이터를 통합하여 다음 정보를 동기화할 수 있습니다.

- ServiceNow 서버에 대한 스토리지 자산 데이터
- ServiceNow 서버에 대한 호스트 및 VM URL입니다
- 호스트/VM과 스토리지 간의 관계

Service Now 통합을 위한 준비 및 사전 요구 사항

통합이 시작되기 전에 ServiceNow, Insight 및 Python 미들웨어 커넥터에 필요한 준비 및 사전 요구 사항이 충족되어야 합니다.

권장 워크플로

ServiceNow를 Insight와 통합할 경우 다음 워크플로우를 사용하는 것이 좋습니다.

1. 먼저 개발 인스턴스에 Python 미들웨어 커넥터를 배포합니다.
2. 개발 인스턴스에서 모든 고장이 식별되고 수정되었음을 확인했으면 테스트/단계 인스턴스에 커넥터를 배포합니다.
3. 스테이징 인스턴스에서 올바른 작업을 확인한 후 생산 인스턴스에 커넥터를 배포합니다.

이러한 단계에서 문제가 발견되면 롤백 단계를 수행하고 커넥터를 비활성화한 다음 문제를 해결하고 다시 배포합니다.

일반 전제 조건:

- 독립 실행형 호스트 또는 VM(권장) 또는 Insight 서버 호스트/VM을 사용하여 비톤 미들웨어 커넥터를 호스팅할 수 있습니다.
- 운영 Insight 서버를 백업하고 개발 인스턴스에 구축하는 것이 좋습니다.
- ServiceNow는 CMDB에서 서버를 정확하게 검색할 수 있어야 합니다.
- Insight는 스토리지 및 컴퓨팅 환경을 정확하게 검색 해야 합니다.
- 포트 443 및 80을 Insight Server 및 ServiceNow 인스턴스에 연결합니다.

ServiceNow 사전 요구 사항:

- 개발/테스트 인스턴스를 사용하는 것이 좋습니다.
- ServiceNow 업데이트 집합을 로드할 수 있는 권한.
- 사용자를 만들 수 있는 권한.
- ServiceNow 버전 Jakarta 이상

Insight 필수 요소:

- 개발/테스트 인스턴스를 사용하는 것이 좋습니다.
- 사용자 생성 권한(관리자 권한).
- Insight 버전 7.3.1 이상이 지원되지만 Insight를 최대한 활용하려면 최신 버전을 사용하십시오.

Python 미들웨어 커넥터 사전 요구 사항:

- Python 버전 3.6 이상이 설치되어 있습니다.
- Python을 설치할 때 모든 사용자를 활성화하려면 확인란을 선택합니다. 그러면 표준 애플리케이션 설치 위치에 대해 Python이 설정됩니다.
- Python을 설치할 때 설치 프로그램에서 경로를 업데이트할 수 있도록 확인란을 선택합니다. 그렇지 않으면 경로를 수동으로 업데이트해야 합니다.
- Python * pyysnow * 및 * requests * 라이브러리를 다운로드하십시오.

ServiceNow Python 커넥터 다운로드

ServiceNow 통합용 Python 커넥터를 다운로드하여 선택한 위치에 압축을 풀어야 합니다.

단계

1. 에서 * ServiceNow Integration 커넥터 * 를 다운로드합니다 "[NetApp Storefront](#)".
2. 예를 들어 .zip 파일의 압축을 폴더에 풉니다 c:\OCI2SNOW.

통합 커넥터 스크립트의 이름은 입니다 `oci_snow_sync.pyz`.

통합용 ServiceNow 구성

ServiceNow를 Insight와 통합하려면 몇 가지 설정 작업이 필요합니다.

이 작업에 대해

ServiceNow를 Insight와 통합할 때 다음 작업을 수행해야 합니다.

ServiceNow 측에서:

- 권한 상승 역할
- 업데이트 세트를 설치합니다
- 사용자를 설정합니다

Insight Side:

- ServiceNow 사용자를 추가합니다

Python 커넥터 측면:

- Python을 설치합니다

- 추가 라이브러리를 설치합니다
- 커넥터를 초기화한다
- config.ini 파일을 편집합니다
- 커넥터를 테스트합니다
- 커넥터를 동기화합니다
- 일별 작업 실행을 예약합니다

각 항목에 대해서는 다음 섹션에서 자세히 설명합니다.

권한 상승 역할

Insight와 통합하려면 ServiceNow 역할을 security_admin으로 승격해야 합니다.

단계

1. 관리자 권한으로 ServiceNow 인스턴스에 로그인합니다.
2. 시스템 관리자 * 드롭다운에서 * Elevate Roles * 를 선택하고 역할을 security_admin으로 승격합니다. 확인 을 클릭합니다.

업데이트 세트를 설치합니다

ServiceNow와 OnCommand Insight 간의 통합의 일부로, 데이터 추출 및 로드를 위해 커넥터에 특정 필드 및 테이블을 제공하기 위해 Service Now에 사전 구성된 데이터를 로드하는 Update Set을 설치해야 합니다.

단계

1. ""검색된 업데이트 집합""을 검색하여 ServiceNow에서 원격 업데이트 집합 테이블로 이동합니다.
2. XML*에서 업데이트 집합 가져오기 를 클릭합니다.
3. 업데이트 세트는 이전에 로컬 드라이브에 다운로드한 Python connector.zip 파일에 있습니다(이 예에서는 C:\OCI2SNOW 폴더)를 선택합니다 \update_sets 하위 폴더. 파일 선택 * 을 클릭하고 이 폴더에서 .xml 파일을 선택합니다. 업로드 * 를 클릭합니다.
4. 업데이트 세트가 로드되면 해당 업데이트 세트를 열고 * 업데이트 세트 미리 보기 * 를 클릭합니다.

오류가 감지되면 업데이트 집합을 커밋하기 전에 오류를 수정해야 합니다.

5. 오류가 없으면 * 업데이트 집합 커밋 * 을 클릭합니다.

업데이트 세트가 커밋되면 * 시스템 업데이트 세트 * > * 업데이트 소스 * 페이지에 표시됩니다.

ServiceNow 통합 - 사용자 설정

Insight에 연결하고 데이터를 동기화하려면 ServiceNow 사용자를 설정해야 합니다.

이 작업에 대해

단계

1. ServiceNow에서 서비스 계정을 생성합니다. ServiceNow에 로그인하고 * 시스템 보안 * > * 사용자 및 그룹 * > * 사용자 * 로 이동합니다. New * 를 클릭합니다.
2. 사용자 이름을 입력합니다. 이 예제에서는 통합 사용자로 ""OCI2SNOW""를 사용합니다. 이 사용자의 암호를 입력합니다.



이 사용 방법에서는 설명서에 ""OCI2SNOW""라는 이름의 서비스 계정 사용자를 사용합니다. 다른 서비스 계정을 사용할 수도 있지만 환경 전체에서 일관되는지 확인하십시오.

3. 메뉴 모음을 마우스 오른쪽 단추로 클릭하고 * 저장 * 을 클릭합니다. 이렇게 하면 역할을 추가하기 위해 이 사용자를 계속 사용할 수 있습니다.
4. 편집 * 을 클릭하고 이 사용자에게 다음 역할을 추가합니다.
 - 자산
 - import_transformer 를 선택합니다
 - REST_SERVICE
5. 저장 * 을 클릭합니다.
6. 이 동일한 사용자를 OnCommand Insight에 추가해야 합니다. 관리자 권한이 있는 사용자로 Insight에 로그인합니다.
7. Admin * > * Setup * 으로 이동하여 * Users * 탭을 클릭합니다.
8. Actions * 버튼을 클릭하고 * Add user * 를 선택합니다.
9. 이름으로 ""OCI2SNOW""를 입력합니다. 위에서 다른 사용자 이름을 사용한 경우 여기에 해당 이름을 입력하십시오. 위의 ServiceNow 사용자에게 대해 사용한 것과 동일한 암호를 입력합니다. 이메일 필드는 비워 둘 수 있습니다.
10. 이 사용자에게 * 사용자 * 역할을 할당합니다. 저장 * 을 클릭합니다.

Python 및 라이브러리를 설치합니다

Python은 Insight 서버 또는 독립 실행형 호스트 또는 VM에 설치할 수 있습니다.

단계

1. VM 또는 호스트에서 Python 3.6 이상을 다운로드합니다.
2. 사용자 지정 설치를 선택하고 다음 옵션을 선택합니다. 이러한 작업은 적절한 커넥터 스크립트 작업을 위해 필요하거나 강력하게 권장됩니다.
 - 모든 사용자에게 대한 시작 관리자를 설치합니다
 - 경로에 Python을 추가합니다
 - PIP 설치(Python에서 다른 패키지 설치 가능)
 - TK/TCL 및 IDLE을 장착하십시오
 - Python 테스트 제품군을 설치합니다
 - 모든 사용자에게 대해 py launcher를 설치합니다
 - 파일을 Python과 연결합니다

- 설치된 응용 프로그램의 바로 가기를 만듭니다
- 환경 변수에 비단뱀을 추가합니다
- 표준 라이브러리를 미리 컴파일합니다

3. Python을 설치한 후 "request" 및 "psnow" Python 라이브러리를 설치합니다. 다음 명령을 실행합니다. `python -m pip install requests pysnow`

- 참고: * 프록시 환경에서 작업 중일 때 이 명령이 실패할 수 있습니다. 이 문제를 해결하려면 파이썬 라이브러리 중 하나를 수동으로 다운로드하고 설치 요청을 하나씩 올바른 순서로 실행해야 합니다.

명령을 실행하면 여러 파일이 설치됩니다.

4. Python 라이브러리가 올바르게 설치되어 있는지 확인합니다. 다음 방법 중 하나를 사용하여 Python을 시작합니다.

- cmd 프롬프트를 열고 를 입력합니다 `python`
- Windows에서 * 시작 * 을 열고 * Python * > * python-<version>.exe * 를 선택합니다

5. Python 프롬프트에서 를 입력합니다 `modules`

Python은 모듈 목록을 수집하는 동안 잠시 기다려 달라고 요청하며, 그러면 모듈이 표시됩니다.

Python 미들웨어를 설정합니다

이제 Python과 필요한 라이브러리가 설치되었으므로 OnCommand Insight 및 ServiceNow와 통신하도록 미들웨어 커넥터를 구성할 수 있습니다.

단계

1. 커넥터 소프트웨어를 다운로드한 호스트 또는 VM에서 cmd 창을 관리자 로 열고 로 변경합니다 `\OCI2SNOW\` 폴더.

2. 빈 * config.ini* 파일을 생성하려면 스크립트를 초기화해야 합니다. 다음 명령을 실행합니다.

`oci_snow_sync.pyz init`

3. 텍스트 편집기에서 **config.inifile** 을 열고 [OCI] 섹션에서 다음과 같이 변경합니다.

- URL * 을 로 설정합니다 `https://&name.domain` 또는 `https://&ip address</code> Insight 인스턴스에 대해 .`
- 사용자 * 와 * 암호 * 를 OCI2SNOW 와 같이 생성된 Insight 사용자로 설정합니다.
- `include_off_vms` * 를 * false * 로 설정합니다

4. [Snow](눈) 섹션에서 다음 사항을 변경합니다.

- ServiceNow 인스턴스의 FQDN 또는 IP 주소로 * instance * 를 설정합니다
- 사용자 * 및 * 암호 * 를 ServiceNow 서비스 계정 사용자(예: OCI2SNOW)로 설정합니다.
- OCI URL*의 * 필드에서 * url * 필드를 `"u_oci_url"`로 설정합니다. 이 필드는 커넥터 OCI 업데이트 집합의 일부로 생성됩니다. 고객 환경에서 이 설정을 변경할 수 있지만 변경할 경우 여기서 ServiceNow에서 수정해야 합니다. 모범 사례는 이 필드를 그대로 두는 것입니다.
- `filter_status` * 필드를 `"설치됨, 재고 있음"`으로 설정합니다. 상태가 다른 경우 새 레코드를 업로드하기 전에 Insight 레코드와 일치하는 모든 레코드를 가져오려면 여기에서 해당 상태를 설정해야 합니다. 대부분의 경우 이 필드는 변경되지 않아야 합니다.

- `stale_status**` 값을 `"Retired"`로 설정합니다.

5. [프록시] 섹션은 프록시 서버를 사용하는 경우에만 필요합니다. 이 섹션을 사용해야 하는 경우 다음 설정을 확인하십시오.

- `; https = http://<host>:<port>`
- `;http= http://<host>:<port>`
- `; include_oci = True`
- `; include_snow = True`

6. 자세한 디버그 정보가 필요한 경우에만 [Log] 섹션을 편집합니다.

7. 커넥터를 테스트하려면 관리자 권한으로 cmd 프롬프트를 열고 \OCI2SNOW 폴더로 변경합니다. 다음 명령을 실행합니다. `oci_snow_sync.pyz test`

자세한 내용은 에서 확인할 수 있습니다 `logs\` 폴더.

커넥터 동기화 중

ServiceNow, Insight 및 커넥터가 올바르게 구성되면 커넥터를 동기화할 수 있습니다.

단계

1. cmd 프롬프트를 열고 \OCI2SNOW 폴더로 변경합니다.
2. 다음 명령을 두 번 실행합니다. 첫 번째 동기화는 항목을 업데이트하고 두 번째 동기화는 관계를 업데이트합니다.
`oci_snow_sync.pyz sync`
3. ServiceNow 인스턴스의 Storage Server 테이블이 채워져 있는지 확인합니다. 스토리지 서버를 열고 해당 스토리지와 관련된 리소스가 나열되는지 확인합니다.

동기화가 매일 수행되도록 예약 중입니다

Windows 작업 스케줄러를 사용하여 ServiceNow 커넥터를 자동으로 동기화할 수 있습니다.

이 작업에 대해

자동 동기화로 Insight 데이터를 ServiceNow로 정기적으로 이동합니다. 모든 예약 방법을 사용할 수 있습니다. 다음 단계에서는 Windows 작업 스케줄러를 사용하여 자동 동기화를 수행합니다.

단계

1. Windows 화면에서 * 시작 * 을 클릭하고 * 실행 * > * 작업 스케줄러 * 를 입력합니다.
2. 기본 작업 생성... * 을 클릭합니다
3. `"OCI2SNOW Connector Sync"`와 같은 의미 있는 이름을 입력합니다. 작업에 대한 설명을 입력합니다. 다음 * 을 클릭합니다.
4. 를 선택하여 * 매일 * 작업을 실행합니다. 다음 * 을 클릭합니다.
5. 작업을 실행할 시간을 선택합니다. 다음 * 을 클릭합니다.
6. 동작에서 * 프로그램 시작 * 을 선택합니다. 다음 * 을 클릭합니다.
7. Program/script * 필드에 를 입력합니다 `C:\OCI2SNOW\oci_snow_sync.pyz`. arguments * 필드에 를

입력합니다 sync. 시작 위치 * 필드에 를 입력합니다 C:\OCI2SNOW. 다음 * 을 클릭합니다.

8. 요약 정보를 검토하고 * 마침 * 을 클릭합니다.

이제 동기화가 매일 실행되도록 예약되었습니다.

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

<http://www.netapp.com/us/legal/copyright.aspx>

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/us/media/patents-page.pdf>

개인 정보 보호 정책

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

주의

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이선스에 대한 정보를 제공합니다.

"OnCommand Insight 7.3.15에 대한 고지 사항"

"OnCommand Insight 7.3.14에 대한 고지 사항"

"OnCommand Insight 7.3.13에 대한 고지 사항"

저작권 정보

Copyright © 2024 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

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

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

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

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

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

상표 정보

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