



# Data Infrastructure Insights 설명서

## Data Infrastructure Insights

NetApp  
September 26, 2024

# 목차

Data Infrastructure Insights 설명서	1
데이터 인프라 Insights를 통해 얻을 수 있는 이점	1
시작하기	1
Data Infrastructure Insights의 새로운 기능	2
2024년 9월	2
2024년 8월	2
2024년 7월	4
2024년 6월	5
2024년 5월	5
2024년 4월	6
2024년 3월	7
2024년 2월	8
2024년 1월	11
2023년 12월	12
2023년 11월	15
2023년 10월	16
2023년 9월	18
2023년 8월	21
2023년 7월	24
2023년 6월	27
2023년 5월	28
2023년 4월	29
2023년 3월	32
2023년 1월	33
2022년 12월	33
2022년 11월	35
2022년 10월	35
2022년 9월	36
2022년 8월	37
2022년 6월	42
2022년 5월	45
2022년 4월	46
2022년 3월	49
2022년 2월	50
2021년 12월	51
2021년 11월	53
2021년 10월	54
2021년 9월	56
2021년 8월	57

2021년 6월	58
2021년 5월	61
2021년 4월	62
2021년 2월	65
2021년 1월	66
2020년 12월	68
2020년 11월	68
2020년 10월	69
2020년 9월	70
2020년 8월	72
2020년 7월	72
2020년 6월	80
2020년 5월	81
2020년 4월	84
2020년 2월	86
2020년 1월	87
2019년 12월	89
2019년 11월	89
2019년 10월	89
2019년 9월	90
2019년 8월	91
2019년 7월	92
2019년 6월	92
2019년 5월	93
2019년 4월	93
2019년 3월	94
2019년 2월	94
2019년 1월	95
2018년 12월	95
2018년 11월	95
Data Infrastructure Insights 온보딩	97
NetApp BlueXP 계정 생성	97
Data Infrastructure Insights 무료 평가판을 시작하십시오	97
로그인 후 이동	98
로그아웃하는 중입니다	98
보안	99
Data Infrastructure Insights 보안	99
정보 및 지역	101
SecurityAdmin 도구	103
시작하기	115
피처 튜토리얼	115

데이터 수집 중 .....	116
대시보드 갤러리에서 가져오기 .....	142
사용자 계정 및 역할 .....	143
Data Infrastructure Insights 데이터 수집기 목록 .....	152
Data Infrastructure Insights 구독 .....	156
평가판 .....	156
구독이 만료된 경우 어떻게 해야 하나요? .....	157
가입 * 이 만료된 경우 어떻게 해야 하나요? .....	157
모듈 평가 .....	157
구독 옵션 .....	158
가입하려면 어떻게 해야 하나요? .....	159
구독 상태를 확인하십시오 .....	160
사용 관리를 봅니다 .....	161
직접 구독하고 평가판을 건너뛰십시오 .....	162
권한 ID 추가 .....	162
관찰 가능성 .....	163
대시보드 만들기 .....	163
쿼리 작업 .....	205
인사이트 .....	220
모니터링 및 경고 .....	227
주석 작업 .....	302
응용 프로그램 작업 .....	311
자동 장치 해상도 .....	313
자산 페이지 정보 .....	328
보고 .....	343
쿠버네티스 .....	420
Kubernetes 클러스터 개요 .....	420
NetApp Kubernetes 모니터링 운영자를 설치 또는 업그레이드하기 전에 .....	421
Kubernetes Monitoring Operator 설치 및 구성 .....	425
Kubernetes 모니터링 운영자 구성 옵션 .....	442
Kubernetes 클러스터 세부 정보 페이지 .....	454
Kubernetes 네트워크 성능 모니터링 및 맵 .....	458
Kubernetes 변경 분석 .....	466
ONTAP 핵심 요소 .....	471
개요 .....	471
데이터 보호 .....	472
보안 .....	473
경고 .....	476
검토할 수 있습니다 .....	477
네트워킹 .....	478
워크로드 .....	478



관리자 및 기타 작업	480
Data Infrastructure Insights API를 참조하십시오	480
환경 모니터링	491
워크로드 보안	497
스토리지 워크로드 보안 정보	497
시작하기	497
경고	536
법의학	542
자동 응답 정책	552
허용된 파일 형식 정책	554
ONTAP Autonomous 랜섬웨어 Protection과 통합	555
ONTAP 액세스와의 통합이 거부되었습니다	557
사용자 액세스 차단	559
워크로드 보안: 공격 시뮬레이션	564
경고, 경고 및 에이전트/데이터 소스 수집기 상태에 대한 이메일 알림 구성	567
워크로드 보안 API	568
문제 해결	571
일반적인 Data Infrastructure Insights 문제 해결	571
Linux에서 획득 장치 문제 해결	572
Windows의 획득 장치 문제 해결	575
실패한 데이터 수집기 조사	578
Data Infrastructure Insights Data Collector 지원 매트릭스	579
HP Enterprise 3PAR/Alletra 9000/Primera StoreServ 스토리지	579
Amazon AWS EC2	593
Amazon AWS S3	598
Microsoft Azure NetApp Files를 참조하십시오	603
Brocade 파이버 채널 스위치	610
Brocade Network Advisor HTTP입니다	620
Brocade FOS REST	627
Cisco MDS 및 Nexus 패브릭 스위치	632
결속력	642
EMC Celerra(SSH)	650
EMC CLARiX(NaviCLI)	659
EMC Data Domain(SSH)	674
EMC ECS	681
Dell EMC Isilon 및 PowerScale REST	687
Dell EMC Isilon/PowerScale(CLI)	701
EMC PowerStore REST	714
EMC RecoverPoint(HTTP)	724
EMC ScaleIO 및 PowerFlex REST	727
EMC Symmetrix CLI를 참조하십시오	735
Dell Unisphere REST입니다	749

EMC VNX(SSH)	757
EMC VNXe 및 Unity Unisphere(CLI)	772
EMC VPLEX를 참조하십시오	782
EMC XtremIO(HTTP)	790
NetApp E-Series를 통해 비즈니스 이점을 제공합니다	801
Google 클라우드 컴퓨팅	813
HDS HCP(HTTPS)	819
HiCommand 장치 관리자	824
Hitachi Ops 센터	838
HDS HNAS(CLI)	847
HPE Nimble/Alletra 6000 스토리지	855
Huawei OceanStor(REST/HTTPS)	863
IBM Cleversafe	875
IBM DS 8K(DSCLI)	880
IBM PowerVM(SSH)	887
IBM SVC(CLI)	891
IBM XIV 및 A9000(XIVCLI)	905
Infinidat(HTTP)	913
Microsoft Azure 컴퓨팅	921
Microsoft Hyper-V를 참조하십시오	926
NetApp 7 모드	936
NetApp Cloud Volumes Service를 참조하십시오	953
NetApp ONTAP용 Amazon FSx	959
NetApp clustered Data ONTAP 8.1.1 이상	973
NetApp SolidFire 8.1 이상	1000
NetApp StorageGRID(HTTPS)	1012
Nutanix 스토리지(REST)	1021
OpenStack(REST API/SSH)	1033
Oracle ZFS(HTTPS)	1037
Pure Storage FlashArray(HTTP)	1050
Red Hat RHV(REST)	1061
Rubrik 스토리지	1066
NetApp HCI 가상 센터	1072
AWS 기반 VMware 클라우드	1081
VMware vSphere(웹 서비스)	1088
참조 지원	1101
지원을 요청하는 중입니다	1101
Data Collector 참조 - 인프라	1106
Data Collector 참조 - 서비스	1215
개체 아이콘 참조	1300
법적 고지	1302
저작권	1302

상표.....	1302
특허.....	1302
개인 정보 보호 정책.....	1302
오픈 소스.....	1302

# Data Infrastructure Insights 설명서

NetApp 데이터 인프라 인사이트(이전의 Cloud Insights)는 전체 인프라에 대한 가시성을 제공하는 클라우드 인프라 모니터링 툴입니다. 데이터 인프라 Insight를 사용하면 퍼블릭 클라우드 및 프라이빗 데이터 센터를 비롯한 모든 리소스에 대한 모니터링, 문제 해결 및 최적화 등이 가능합니다.

## 데이터 인프라 Insights를 통해 얻을 수 있는 이점

Data Infrastructure Insights는 하이브리드 멀티 클라우드 모니터링 기능을 제공하여 인프라 및 워크로드에 대한 전체 스택을 관찰할 수 있도록 지원합니다.

- Kubernetes를 포함한 이기종 인프라 및 워크로드의 데이터 수집기가 있습니다
- Open Telegraf Collector 및 개방형 API를 통해 간편하게 통합할 수 있습니다
- 포괄적인 경고 및 알림
- 지능형 통찰력을 위한 머신 러닝
- 리소스 활용률 최적화
- 디스플레이 소음을 최소화하여 질문에 답할 수 있는 고급 필터가 포함된 기본 제공 또는 사용자 지정 가능한 대시보드
- ONTAP 스토리지 작업의 상태를 확인해 보십시오
- 랜섬웨어 또는 데이터 폐기 공격으로부터 가장 중요한 비즈니스 자산 보호

---

## 시작하기

- **"\* 시작하기 \*** 데이터 인프라 인사이트 활용 방법
- 가입했습니다. 이제 어떻게 해야 할까요?"**데이터 획득**"  
"사용자 설정 중"
- 멋집니다! 다음 단계  
"자산 준비:주석 달기"  
"원하는 자산 찾기:쿼리"  
"원하는 데이터 보기: 대시보드"  
"모니터링 및 경고"  
"데이터 보안"
- 정말 멋진 곳이에요! 이제 준비가 되었습니다 **"\* 가입 \***.

# Data Infrastructure Insights의 새로운 기능

NetApp은 제품과 서비스를 지속적으로 개선 및 개선하고 있습니다. 다음은 Data Infrastructure Insights(이전의 Cloud Insights)에서 사용할 수 있는 몇 가지 최신 기능입니다.

## 2024년 9월

이전의 **Cloud Insights**인 **Data Infrastructure Insights**를 소개합니다

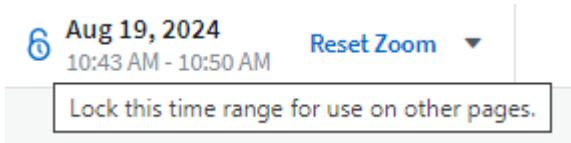
2024년 9월 24일 화요일에 NetApp은 Cloud Insights의 이름을 \* Data Infrastructure Insights \* (DII)로 공식 변경했습니다. 이 발표는 Haiyan Song이 주요 무대 기조 프레젠테이션과 Insight 컨퍼런스 제품 보도 자료를 통해 Insight 사용자 컨퍼런스에서 진행되었습니다.

DII 서비스는 동일하게 유지되며 기능에 변경 또는 수정이 없습니다. 이는 모든 IT 인프라에 대한 기능과 서비스 이름을 보다 효과적으로 조정하기 위한 이름입니다.

## 2024년 8월

해당 시간 범위에 해당하는 데이터를 봅니다

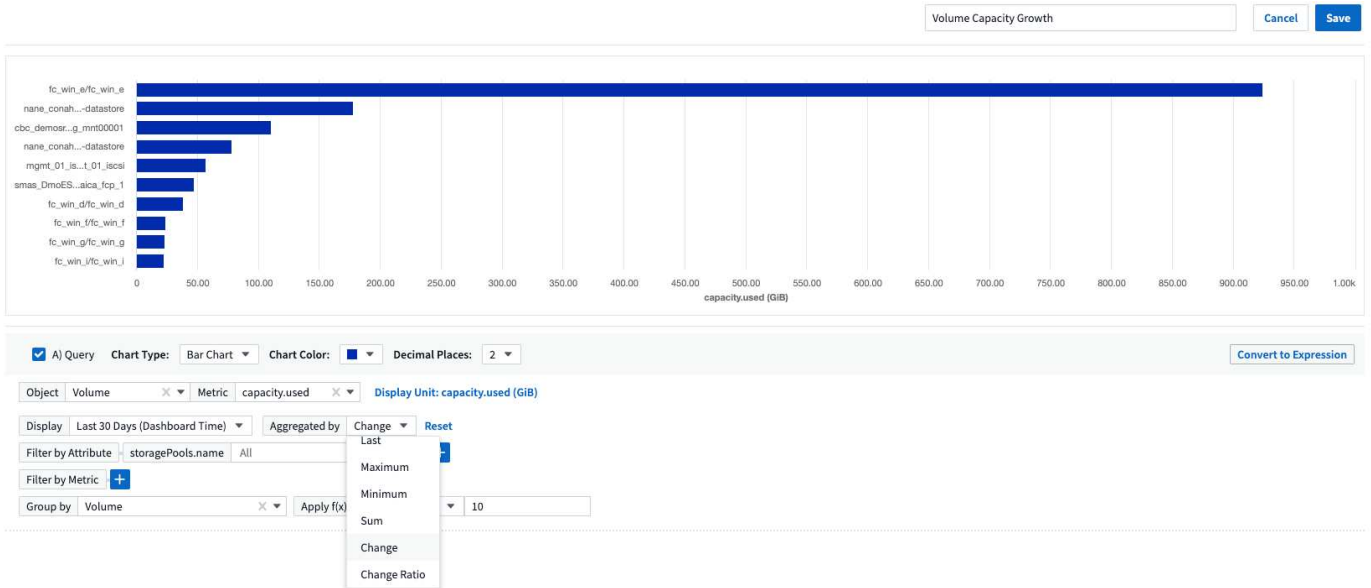
경고 조사? 차트를 확대하시겠습니까? 이러한 작업은 해당 페이지의 시간 범위를 변경합니다. 이제 해당 시간 범위를 잠그고, 다른 Cloud Insights 페이지를 탐색하고, 잠긴 시간 범위에 해당하는 데이터를 볼 수 있습니다. 조사 및 문제 해결이 훨씬 더 쉬워졌습니다!



## 변경 및 변경 비율(%) 분석

변경 비율 시간 집계는 시간 경과에 따른 메트릭 값의 중요한 변화와 추세를 식별하는 데 도움이 됩니다. 이러한 인사이트는 특정 시간 동안 용량이 대폭 증가하거나 단일 포트 성능의 변화와 같은 변경 사항을 이해하는 데 핵심적인 역할을 합니다.

- \* 변경 \* - 선택한 기간 내에 두 지점 사이의 메트릭 변화를 관찰합니다.
- \* Change Ratio \* - 선택한 기간 내에 두 지점 사이의 비례 변화를 초기 지점에 대해 관찰합니다.




## 로그 쿼리 결과를 .csv로 내보냅니다

로그 쿼리 결과를 볼 때 새로운 "내보내기" 버튼을 클릭하여 최대 10,000개의 행을 .csv로 쉽게 내보낼 수 있습니다. 따라서 데이터 접근성이 향상되고 데이터 분석 및 보고가 간편해지며 다른 Data Processing 툴과 원활하게 통합됩니다.

### Log Entries

Last updated 08/15/2024 1:01:49 PM  

timestamp ↓	source	message	

## 시간별 알림 해결

이제 Cloud Insights에서는 모니터링되는 메트릭이 지정된 기간 동안 허용 가능한 범위 내에 있을 때 알림을 해결할 수 있는 옵션을 제공합니다. 이를 통해 여러 경고를 하나로 통합하여 정의된 임계값을 초과하는 메트릭과 관련된 잡음을 반복적으로 줄여 진정한 문제에 집중할 수 있습니다.

### 3 Define alert resolution

Resolve when the metric returns to the acceptable range

Resolve when the metric is within the acceptable range for

15

Minute(s) ▼

Minute(s)

Hour(s)

Day(s)

# 2024년 7월

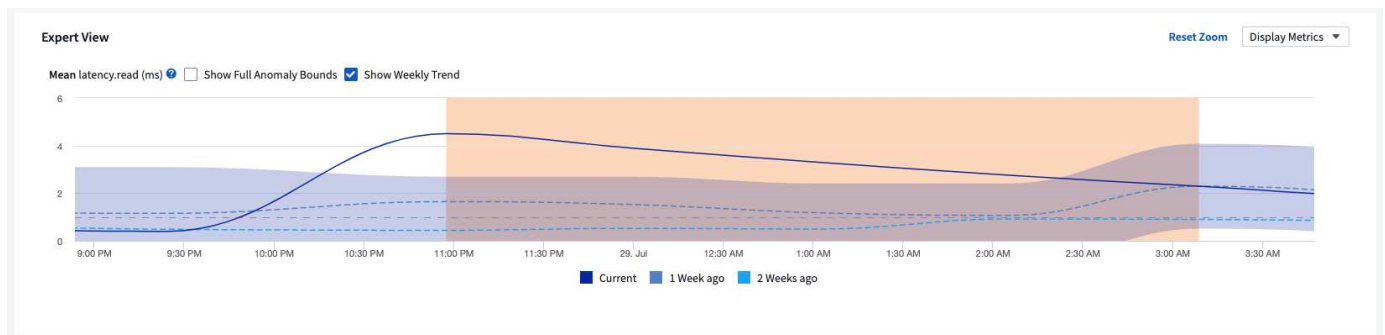
## AIOps:비정상 상태 감지

Cloud Insights는 머신 러닝을 사용하여 사용자 환경에서 예기치 않은 데이터 패턴 변경을 감지하고 사전 예방적 알림을 제공하여 문제를 조기에 파악할 수 있도록 지원합니다.

데이터 센터는 하루 중 다른 시간과 요일에 서로 다른 방식으로 동작합니다. Cloud Insights는 주별 계절성을 사용하여 각 날짜와 시간에 대한 과거 행동을 비교합니다.

이상 징후 감지 모니터링은 "정상"의 정의가 불분명하거나 시간이 지남에 따라 동작이 변경되는 경우 또는 수동으로 임계값을 정의하기가 어려운 대량의 데이터로 작업하는 경우 등에 대한 알림을 제공할 수 있습니다.

이와 같은 이상 현상이 선택한 오브젝트 메트릭에서 발생할 경우 새로운 "이상 징후 감지 모니터" 경고 메시지가 나타납니다.



## 워크로드 보안 개선

- NFS 4.1 지원 \*

SVM Data Collector는 이제 ONTAP 9.15.1 이상의 \* NFS 4.1 \* 을 포함한 최대 NFS 버전을 지원합니다.

- 새로운 포렌식 활동 API \*

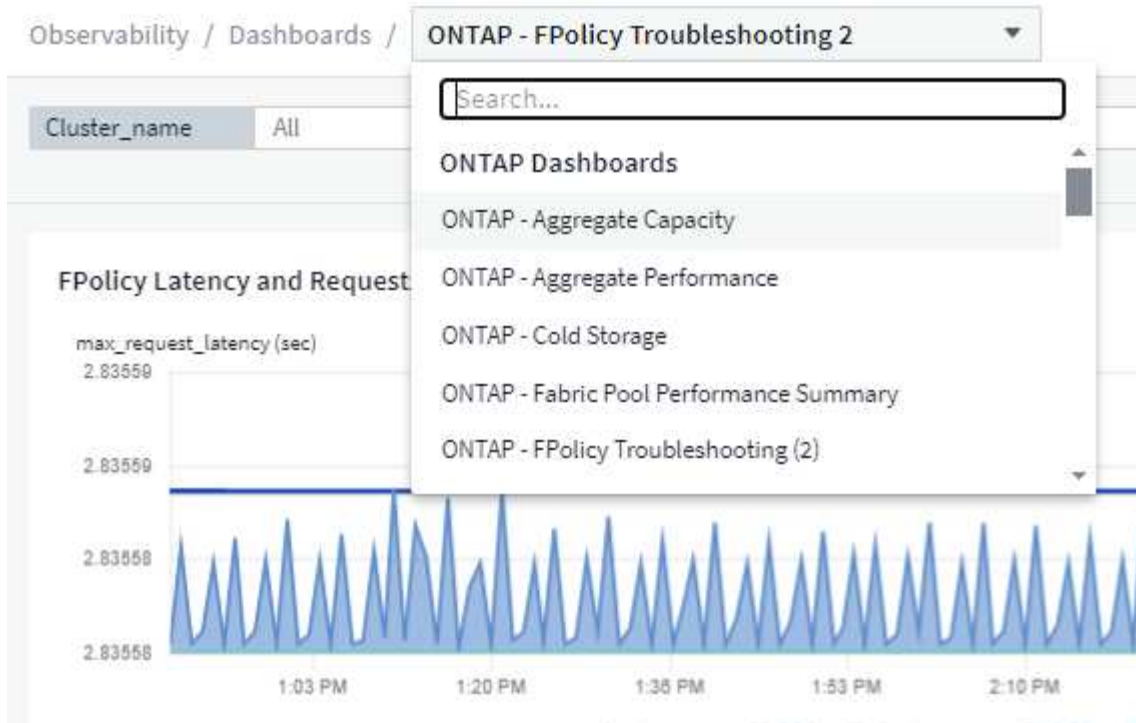
법의학 활동에 "[API를 참조하십시오](#)" 새 버전이 있습니다. Forensics 작업을 위해 API를 호출할 때 \* cloudsecure\_forensics.activities.v2 \* API를 사용합니다.

이 API를 여러 번 호출하는 경우 최상의 결과를 얻으려면 호출이 병렬로 수행되는 것이 아니라 순차적으로 수행되도록 해야 합니다. 여러 병렬 호출로 인해 API 시간이 초과될 수 있습니다.

## 간편한 대시보드 탐색

이 기능은 운영 워크플로우를 간소화하고 팀 간의 협업을 보다 쉽게 수행할 수 있도록 해 줍니다.

대시보드를 그룹화하면 필요한 가시성을 빠르게 얻을 수 있으며, 이제 새로운 탐색 메뉴를 통해 자리를 잃지 않고 서로 다른 대시보드 간에 이동할 수 있으므로 인프라를 쉽게 탐색하고 관리할 수 있습니다. 대시보드 그룹을 운영 Runbook과 연계하여 환경을 더욱 개선할 수 있습니다.



## 2024년 6월

### 운영 체제 지원

Cloud Insights 획득 장치 외에 다음과 같은 운영 체제가 지원됩니다 **"이미 지원됩니다"**:

- Red Hat Enterprise Linux 8.9, 8.10, 9.4
- 로키 9.4
- AlmaLinux 9.3 및 9.4

## 2024년 5월

### 시간에 따라 자동으로 경고 해결

로그 경고는 시간에 따라 해결할 수 있습니다. 경고 조건이 더 이상 발생하지 않으면 Cloud Insights는 지정된 시간이 경과한 후 자동으로 경고를 해결할 수 있습니다. 알림을 분, 시간 또는 일 단위로 해결할 수 있습니다.



### 3 Define alert resolution

- Resolve instantly
- Resolve based on criteria

- Resolve automatically after   if the condition **above** stops occurring.
- Resolve based on log entry i

Day(s) ▼

Minute(s)

Hour(s)

Day(s)

## 2024년 4월

### Kubernetes에 대한 iSCSI 지원

이제 Cloud Insights는 Kubernetes와 연결된 iSCSI 스토리지를 매핑하는 기능을 지원하므로 Kubernetes 네트워크 맵을 사용하여 더 빠르게 문제를 해결하고 Reporting을 통해 비용 청구 또는 쇼백 보고서를 제공할 수 있습니다.

The screenshot displays the NetApp Cloud Insights interface. On the left, the 'Workload Map' shows a network diagram with nodes for 'order', 'order-postgres', 'payment', and 'order-postgres-pv'. A tooltip for 'order-postgres-pv' shows 'connections\_total: 1'. On the right, the 'Persistent Volume' details panel is open, showing a summary of the 'ci-demo-01' ISCSI volume. It includes storage metrics for IOPS (35.88 IO/s), Latency (0.54 ms), Throughput (143.78 KB/s), and Used Capacity (60.16%). A table at the bottom shows the 'Backend Storage Performance' for the 'order-postgres-pv' workload, managed by Helm, using NFS storage with 60.16% capacity used out of 80.84 GB total.

PV Name	Workload	Type	Backend Storage	Used Capacity (%)	Total Cap (GiB)
order-postgres-pv	order-postgres	NFS	cvoPostgresProd05:dataVolume06	60.16	80.84

## 운영 체제 지원

Cloud Insights 획득 장치 외에 다음과 같은 운영 체제가 지원됩니다 "이미 지원됩니다":

- Oracle Enterprise Linux 8.8
- Red Hat Enterprise Linux 8.8
- 로키 9.3
- openSUSE 리프 15.1 ~ 15.5
- SUSE Enterprise Linux Server 15, 15 SP2~15 SP5

## 2024년 3월

### 워크로드 보안 에이전트 세부 정보

각 워크로드 보안 에이전트에는 자체 시작 페이지가 있으며, 이 페이지에서 에이전트와 연결된 설치된 데이터 및 사용자 디렉터리 수집기는 물론 에이전트에 대한 요약 정보를 쉽게 볼 수 있습니다.

#### Agent Summary

<b>Name</b> agent-1	<b>Connection Status</b> Connected - <a href="#">Need Help?</a>
<b>IP</b> 10.11.12.13	<b>Last Reported</b> a few seconds ago Mar 5, 2024 9:40 AM
<b>Version</b> 1.602.0	

#### Installed Data Collectors

[+ Data Collector](#)

Name ↑	Status	Type	Cluster/SVM IP	SVM Name	Last Reported	
<a href="#">DSC</a>	Running	ONTAP SVM	10.102.103.104	sgornall_svm	a few seconds ago Mar 5, 2024 9:40 AM	⋮

#### Installed User Directory Collectors

[+ User Directory Collector](#)

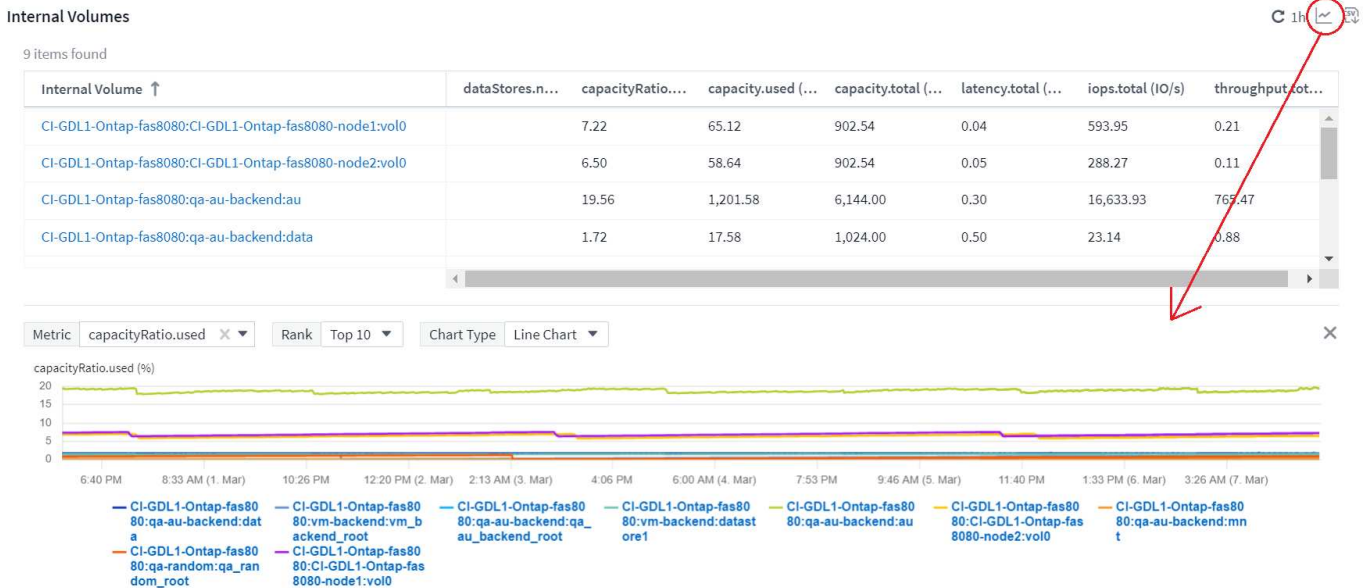
Name ↑	Status	Type	Server	Forest Name/Search Base	Last Reported	
<a href="#">AD_EditRename</a>	Running	Active Directory	10.200.203.204	wslab1.netapp.com	a few seconds ago Mar 5, 2024 9:40 AM	⋮

## 더 많은 데이터를 보다 빠르게 차트로 작성할 수 있습니다

자산의 시작 페이지에서 데이터를 분석할 때 전문가 보기 차트에 데이터를 추가하는 것은 매우 간단합니다. 랜딩 페이지의 각 테이블에 대해 개체 유형에 관련 데이터가 있는 경우 해당 개체 위로 마우스를 가져가면 "전문가 보기에 추가" 아이콘이 표시됩니다. 이 아이콘을 선택하면 해당 개체가 추가 리소스에 추가되고 전문가 보기 차트에 표시됩니다.

2 items found

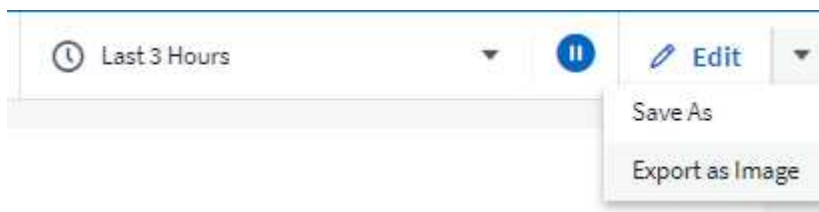
또는 랜딩 페이지 표의 데이터를 자체 차트로 표시하려는 경우도 있습니다. 간단히 `_Show Chart_icon`을 선택하여 표 아래의 차트를 엽니다.



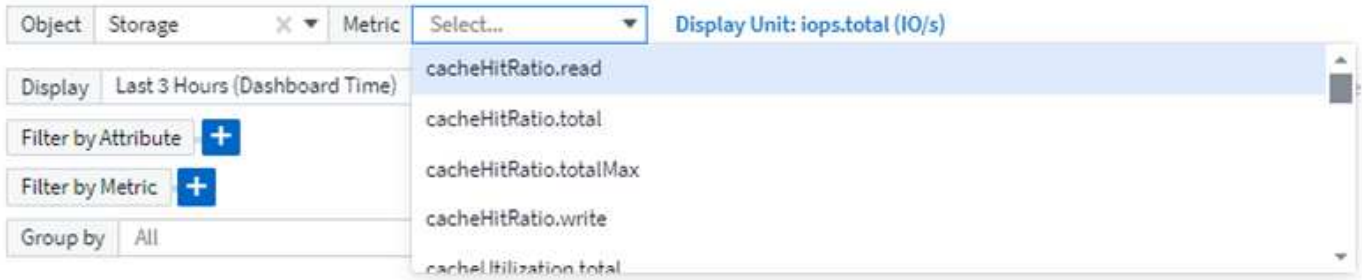
## 2024년 2월

### 사용 편의성 개선

오른쪽 드롭다운 메뉴에서 `_Export as Image_`를 선택하여 현재 대시보드의 \* 스냅샷 \* 을 저장합니다. Cloud Insights는 현재 위젯 상태의 .PNG를 생성합니다.



- 오브젝트 및 메트릭 선택 \* 위젯, 모니터 등의 경우 그 어느 때보다 쉽게 선택할 수 있습니다 원하는 개체 유형을 선택한 다음 별도의 드롭다운에서 해당 개체와 관련된 메트릭을 선택합니다.



- 데이터 수집기 및 수집 장치 내보내기 \* 는 해당 페이지 상단의 아이콘을 선택하여 .csv로 목록을 표시합니다.



도움말 > 지원 \* 페이지를 재구성했으므로 필요한 항목을 더 쉽게 찾을 수 있습니다. NetApp은 귀하의 요청에 따라 이 페이지에 \* API Swagger \* 및 사용자 설명서에 직접 링크를 추가했습니다.

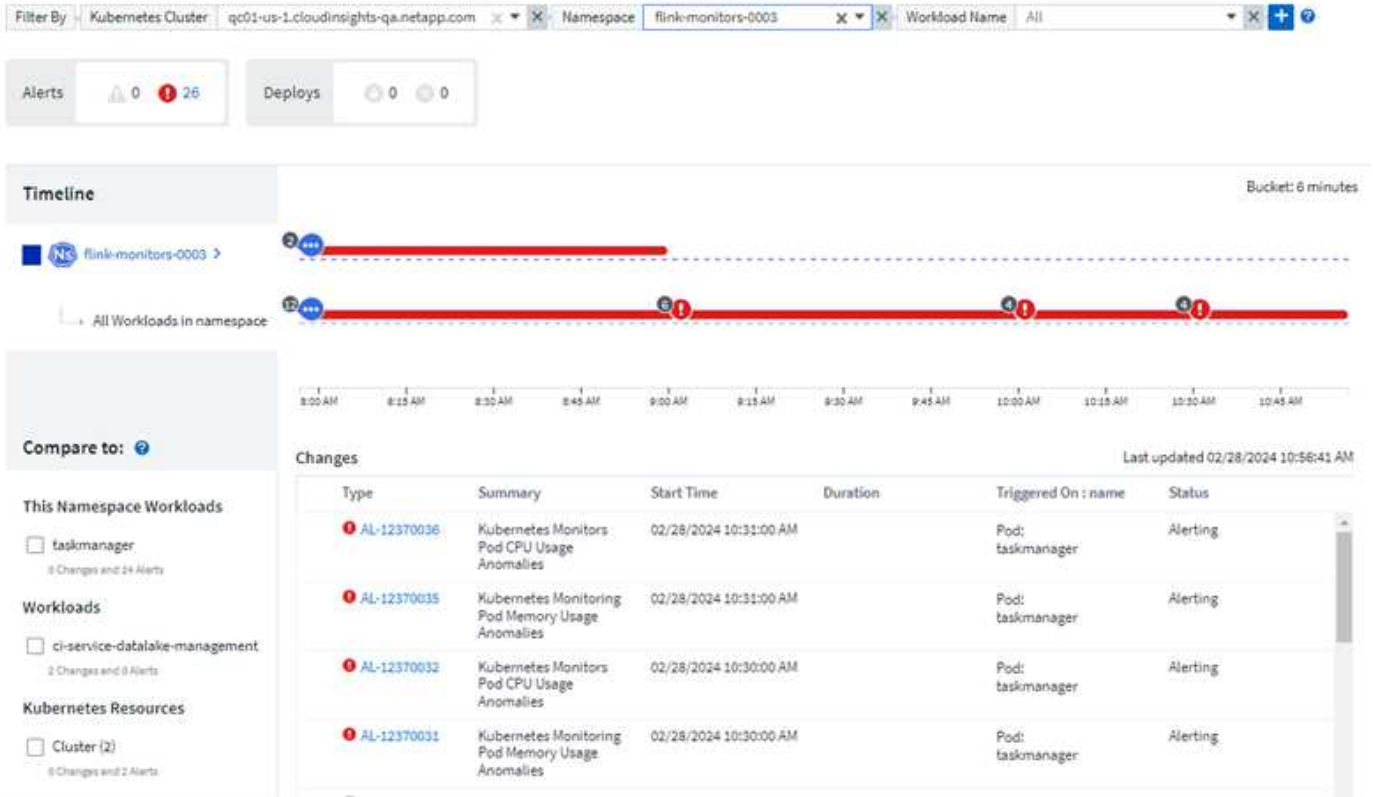
**API Access:**  
 To integrate Cloud Insights with other applications see the [Cloud Insights API List and documentation.](#)

- 링크 \* 경고 목록 페이지의 "triggeredOn" 열에 있는 링크 \* 해당 개체에 랜딩 페이지를 사용할 수 있는 경우 해당 랜딩 페이지로 이동합니다.

alertId	triggeredTime ↓	currentSeverity	monitor	triggeredOn
AL-12371406	4 minutes ago Feb 28, 2024 4:50 PM	Warning	Kubernetes Cluster Saturation	Kubernetes_Cluster: <a href="#">gcs01-us-1.cloudinsights.netapp.com</a>

## 네임스페이스의 모든 변경 내용을 확인합니다

이제 Kubernetes 변경 분석을 통해 클러스터 및 네임스페이스를 선택할 때 변경 일정을 확인할 수 있습니다. 이전에는 작업량도 선택해야 했습니다. 클러스터 및 네임스페이스에서 필터링하면 해당 네임스페이스의 모든 워크로드 변경 타임라인이 한 줄에 표시됩니다.



## 경고에 대한 관련 로그

로그 경고를 볼 때 관련 로그 항목이 새 테이블에 표시됩니다. 로그 항목은 알림과 동일한 소스 및 시간 내에 발생하고 동일한 조건이 적용되는 경우 연결됩니다. 더 자세히 살펴보려면 "Analyze Logs"를 선택하십시오.

### Related Logs

[Analyze Logs](#)

timestamp ↓	message
02/28/2024 11:07:21 AM	iscsi.loginFailure: ISCSI: iSCSI login failure, 'Invalid TargetName iqn.1992-08.com.netapp:sn.6ed012db378611ee8f24005056b3dcd8:vs.3 from Initiator iqn.1994-05.com.redhat:dc7292e4b936 at IP address 10.192.38.34'
02/28/2024 11:06:24 AM	iscsi.loginFailure: ISCSI: iSCSI login failure, 'Invalid TargetName iqn.1992-08.com.netapp:sn.091b27ae993c11ee9765005056b3f163:vs.3 from Initiator iqn.1994-05.com.redhat:e861299d2ffc at IP address 10.192.33.88'
02/28/2024 11:06:24 AM	iscsi.loginFailure: ISCSI: iSCSI login failure, 'Invalid TargetName iqn.1992-08.com.netapp:sn.091b27ae993c11ee9765005056b3f163:vs.3 from Initiator iqn.1994-05.com.redhat:e861299d2ffc at IP address 10.192.33.88'

## ONTAP 스위치 데이터를 수집합니다

Cloud Insights는 ONTAP 시스템의 백엔드 스위치에서 데이터를 수집할 수 있습니다. 데이터 수집기의 *Advanced Configuration* 섹션에서 수집을 활성화하고 ONTAP 시스템이 제공하도록 구성되었는지 확인합니다 "스위치 정보" 을 (를) 가지고 있습니다 "권한" 설정.

## 워크로드 보안 Data Collector API

대규모 환경에서는 새로운 Data Collector API를 사용하여 워크로드 보안 수집기 생성을 자동화할 수 있습니다. Admin > API Access > API Documentation \* 으로 이동한 후 \_Workload Security\_API 유형을 선택하여 자세히 알아보십시오.

# 2024년 1월

## 아직 사용하지 않은 Cloud Insights 기능을 사용해 보십시오

Cloud Insights의 초기 평가판 외에 의 이점을 활용할 수도 있습니다 "모듈 평가". 예를 들어, Cloud Insights를 구독하고 스토리지 및 가상 머신을 모니터링한 경우, Kubernetes를 환경에 추가하면 Kubernetes 관측성 30일 평가판을 자동으로 시작합니다. Kubernetes 관측성 관리형 유닛 사용은 평가 기간이 만료될 때까지 구독한 자격 조건에 포함되지 않습니다.

## 내 워크로드가 얼마나 정상적인가?

워크로드 상태는 \* Kubernetes > Explore > 워크로드 \* 페이지에서 한눈에 확인할 수 있으므로 제대로 작동하는 워크로드와 도움이 필요할 수 있는 워크로드를 빠르게 확인할 수 있습니다. 상태 문제가 인프라, 네트워크 또는 구성 변경과 관련되어 있는지 쉽게 식별하고 드릴다운하여 근본 원인을 분석합니다.

Workload Name	Health ↓	Running Pods	Desired Pods	Compute & Storage	Network	Changes	Namespace	Kubernetes Cluster
<a href="#">point-of-sale &gt;</a>	Unhealthy	0	1	Critical		0	<a href="#">netapp-fitness-store-01 &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">frontend &gt;</a>	Unhealthy	2	2		Critical	0	<a href="#">netapp-fitness-store-01 &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">catalog &gt;</a>	Healthy	1	1	Critical (Resolved)		2	<a href="#">netapp-fitness-store-01 &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">billing-g &gt;</a>	Healthy	1	1			13	<a href="#">netapp-fitness-store-01 &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">cart &gt;</a>	Healthy	1	1			0	<a href="#">netapp-fitness-store-01 &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">cart-red &gt;</a>	Healthy	1	1			0	<a href="#">netapp-fitness-store-01 &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">catalog &gt;</a>	Healthy	1	1			0	<a href="#">netapp-fitness-store-01 &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">chaos-c &gt;</a>	Healthy	3	3			0	<a href="#">chaos-mesh &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">chaos-d &gt;</a>	Healthy	6	7			0	<a href="#">chaos-mesh &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">chaos-dashboard &gt;</a>	Healthy	1	1			0	<a href="#">chaos-mesh &gt;</a>	<a href="#">ci-demo-01 &gt;</a>
<a href="#">chaos-dns-server &gt;</a>	Healthy	1	1			0	<a href="#">chaos-mesh &gt;</a>	<a href="#">ci-demo-01 &gt;</a>

## Data Collector 업데이트

### Data Domain ID입니다

Data Domain Collector는 페일오버 이벤트 전반에 걸쳐 HA 시스템을 더 잘 식별할 수 있도록 개선되었습니다. 이 변경 사항으로 인해 HA 시스템에서 Data Domain 어플라이언스를 \* 한 번 \* 재식별할 수 있게 되어 해당 자산의 주석이 제거됩니다(이러한 스토리지가 다시 식별되기 때문에). 주석을 Data Domain 객체에 다시 연결해야 합니다.

## 향상된 랜섬웨어 감지 ML 알고리즘

워크로드 보안에는 가장 정교한 공격을 더 빠르고 정확하게 감지하는 새로운 2세대 랜섬웨어 감지 ML 알고리즘이 포함되어 있습니다.

행동의 "계절성": 주말 행동은 평일 또는 오후의 아침 행동과 다른 패턴을 따를 수 있습니다. 워크로드 보안 알고리즘은 이러한 계절성을 고려합니다.

## 더 이상 사용되지 않는 기능

기능이 발전함에 따라 기능이 더 이상 사용되지 않는 경우가 있습니다. 다음은 Cloud Insights에서 더 이상 사용되지 않는 몇 가지 특징과 기능입니다.

워크로드 보안 **REST** 클라우드시큐어\_**forensics.activities.v1 API**는 더 이상 사용되지 않습니다

\_cloudsecure\_forensics.activities.v1\_API는 더 이상 사용되지 않습니다. 이 API는 스토리지 워크로드 보안 환경의 엔터티와 연결된 작업에 대한 정보를 반환합니다. 이 API는 cloudsecure\_forensics.activities.\*v2\*\_로 대체되었습니다.

이 API에 대한 Get은 이전에 다음을 반환했습니다.

```
{
  "count": 24594,
  "limit": 1000,
  "offset": 0,
  "results": [
    {
      "accessLocation":
```

이 API는 이제 다음을 반환합니다.

```
{
  "limit": 1000,
  "meta": {
    "page": {
      "after": "lvlvk3pp.4cpzcg4kpybl",
      "before": "lvlxy3dz.4cq5ajdn19fk",
      "size": 1000
    }
  },
  "results": [
    {
      "accessLocation": "10.249.6.220",
```

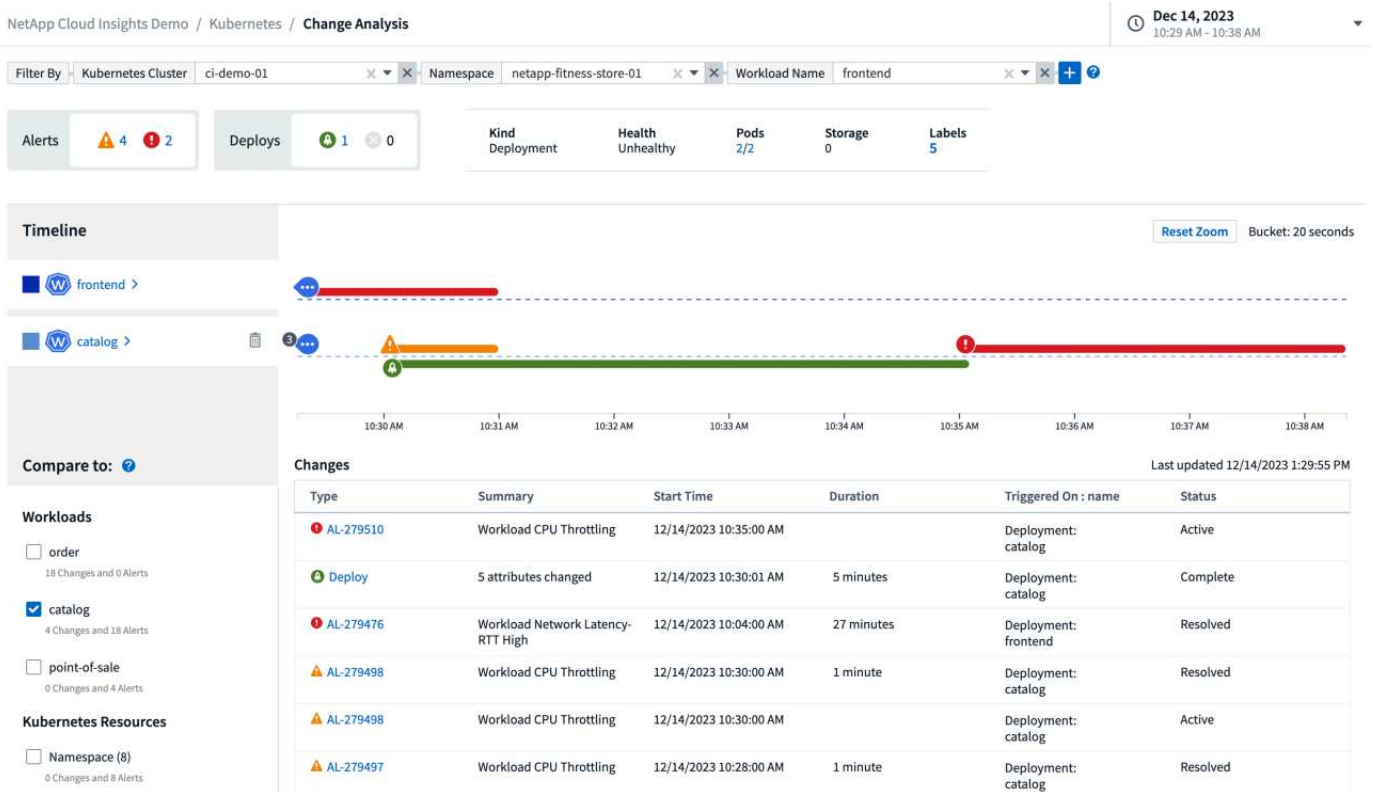
자세한 내용은 [Admin > API Access > API Documentation > Workload Security](#)의 Swagger 설명서를 참조하십시오.

## 2023년 12월



## 한 눈에 변경 분석

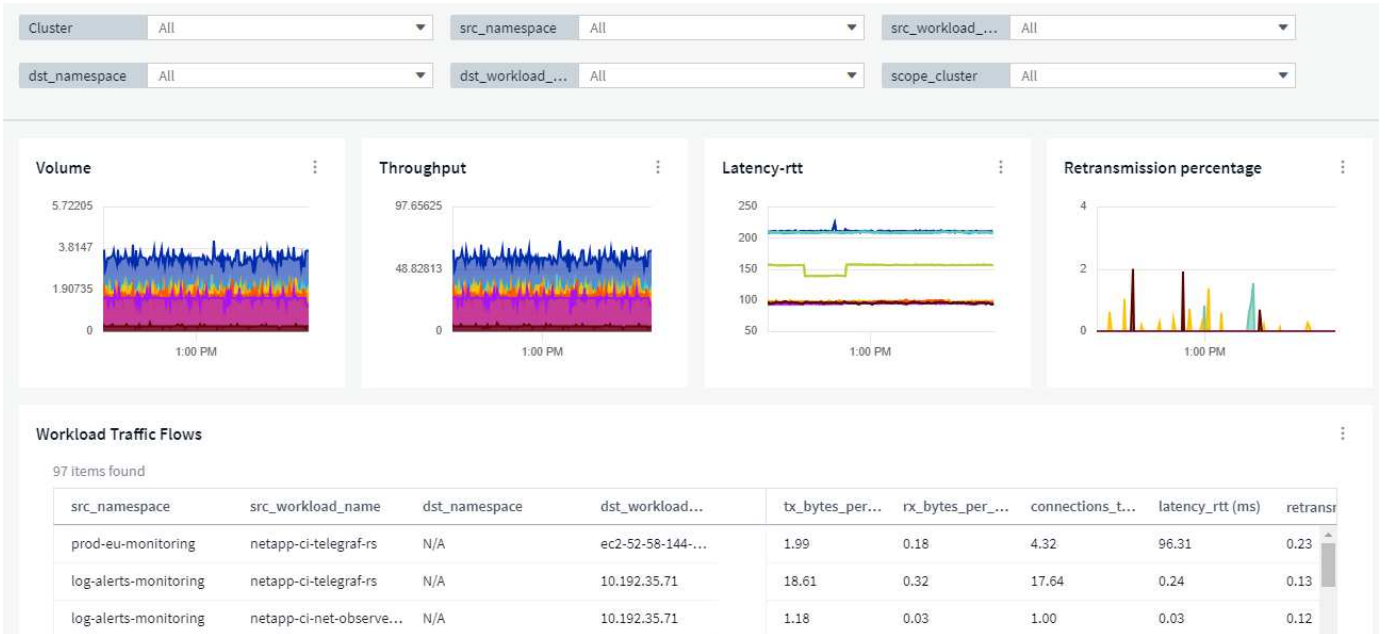
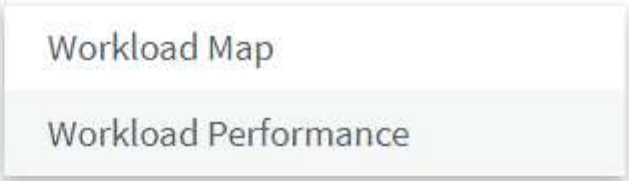
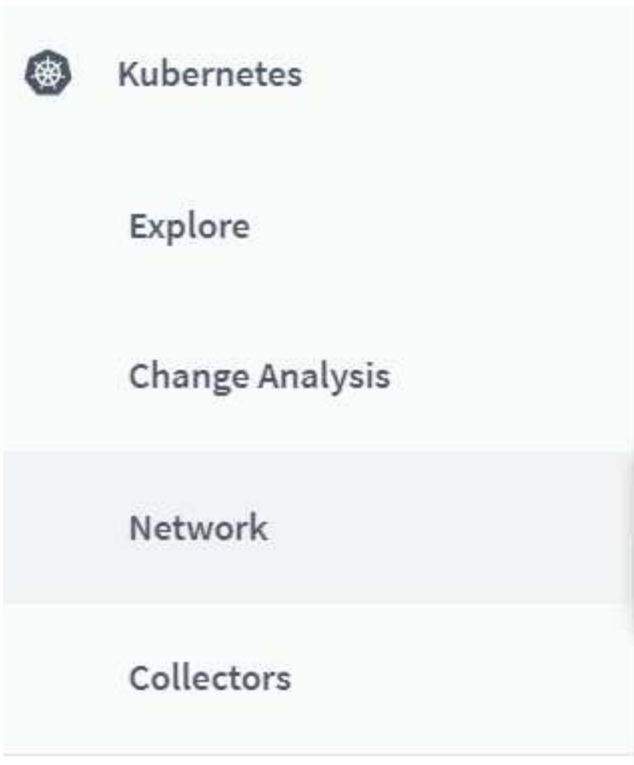
쿠버네티스 "변경 분석" Kubernetes 환경의 최근 변화에 대한 올인원 뷰를 제공합니다. 알림 및 배포 상태를 즉시 확인할 수 있습니다. 변경 분석을 사용하여 모든 배포 및 구성 변경을 추적하고 Kubernetes 서비스, 인프라 및 클러스터의 상태 및 성능과 상호 연관시킬 수 있습니다.



## Kubernetes 워크로드 성능 대시보드

포괄적인 Kubernetes 워크로드 성능 대시보드에서 워크로드 성능을 한눈에 파악할 수 있습니다. 볼륨, 처리량, 지연 시간, 재전송 추세에 대한 그래프와 환경의 각 네임스페이스에 대한 워크로드 트래픽 표를 빠르게 확인합니다. 필터를 사용하면 관심 영역에 쉽게 집중할 수 있습니다.





### 한 화면에서 세부 정보를 쿼리합니다

쿼리에서 행을 선택하면 선택한 행에 대한 속성, 주석 및 메트릭 세부 정보를 보여 주는 측면 패널이 열리고 개체의 랜딩 페이지로 드릴링할 필요 없이 유용한 정보를 제공합니다. 행 또는 측면 패널의 링크를 통해 쉽게 탐색할 수 있습니다.

The screenshot displays the Cloud Insights interface. On the left, a table lists 29 items found, with columns for 'agent.node\_diskio' and 'io\_time'. The right pane shows the 'agent.node\_diskio Details' for a specific agent, including attributes like 'agent\_node\_ip', 'agent\_node\_name', 'agent\_node\_os', and 'agent\_node\_uuid', along with metrics such as 'io\_time (ms)', 'iops\_in\_progress', 'merged\_reads (rds/s)', and 'merged\_writes (wrs/s)'.

## 데이터 수집기 업데이트:

- \* Brocade FOS REST \*: 이 수집기는 "미리보기"에서 이동되었으며 현재 일반적으로 사용할 수 있습니다. 참고 사항:
  - FOS는 FOS 8.2에서 REST API를 도입했습니다. 하지만 라우팅과 같은 일부 기능은 9.0의 REST API 기능만 제공되었습니다.
  - 일부 <8.2>와 혼합 FOS 자산으로 구성된 패브릭이 있는 경우 Cloud Insights FOS REST Collector는 이러한 이전 자산을 검색하지 못합니다. FOS REST Collector를 편집하고 해당 Collector에서 제외할 장치의 IPv4 주소 목록을 심표로 구분하여 작성할 수 있습니다.
- \* SELinux \*: Cloud Insights는 SELinux 시행이 활성화된 Linux 환경 내에서 운영의 안정성을 보장하기 위해 Linux 수집 장치의 초기 설치에 대한 개선 사항을 포함합니다. 이러한 개선 사항은 IMPACT\_NEW\_AU 배포에만 적용됩니다. AU 업그레이드와 관련된 SELinux 문제가 있는 경우 NetApp 지원 팀에 문의하여 SELinux 구성을 수정하십시오.

## 2023년 11월

### 워크로드 보안: Collector를 일시 중지/다시 시작합니다

워크로드 보안에서 수집기가 `_running_state`에 있으면 데이터 수집기를 일시 중지할 수 있습니다. 수집기에 대한 "세 개의 점" 메뉴를 열고 일시 중지를 선택합니다. Collector가 일시 중지되는 동안 ONTAP에서 수집된 데이터는 없고 Collector에서 ONTAP로 전송되는 데이터는 없습니다. 다시 수집을 시작하려면 다시 시작을 선택하십시오.

## 스토리지 노드 지원 정보입니다

스토리지 노드 랜딩 페이지에서 *User Data* 섹션은 지원 제공 서비스, 현재 상태, 지원 상태 및 보증 종료 날짜에 대한 정보를 한 눈에 제공합니다. 현재 Cloud Insights는 NetApp 장치에 대해서만 이 정보를 자동 게시합니다. 또한 이러한 지원 필드는 주석이므로 쿼리 및 대시보드에서 사용할 수 있습니다.

### User Data

[+ Annotation](#)

#### Serial Number Active

Yes

#### Serial Number Support Status

Y

#### Support Offering

WARRANTY

#### Warranty End Date

12/31/2023

## VMware 태그를 Cloud Insights 주석에 매핑합니다

를 클릭합니다 "VMware" Data Collector를 사용하면 VMware에 구성된 동일한 이름의 태그로 Cloud Insights 텍스트 주석을 채울 수 있습니다.

## FOS 9.1.1c 이상 펌웨어에 대한 Brocade CLI Collector 안정성 향상

9.1.1c 펌웨어를 실행하는 일부 Brocade 파이버 채널 스위치에서 특정 CLI 명령의 출력 앞에 "mott" 로그인 배너 텍스트 또는 기본 암호 변경에 대한 사용자 경고가 표시될 수 있습니다. Brocade CLI Collector는 이러한 두 가지 유형의 불필요한 텍스트를 무시하도록 개선되었습니다.

이 개선 사항 이전에는 가상 패브릭이 없는 FOS 9.1.1c 스위치만 이 컬렉터 유형으로 검색할 수 있었습니다.

## 2023년 10월

### 향상된 워크로드 보안

워크로드 보안은 다음과 같이 개선되었습니다.

- \* 액세스 거부 \*: 워크로드 보안은 ONTAP와 통합되어 수신됩니다. "액세스 거부됨" 이벤트입니다. 추가 분석 및 자동 응답 계층을 제공합니다.
- \* 허용 파일 유형 \*: 알려진 파일 확장자에 대한 랜섬웨어 공격이 감지되면 해당 파일 확장자를 에 추가할 수 있습니다. "허용되는 파일 형식" 불필요한 경고를 방지하기 위한 목록

## 모듈 시험

Cloud Insights의 초기 평가판 외에 이 이점을 활용할 수도 있습니다 "모듈 평가". 예를 들어, 이미 Infrastructure 관측성에 가입하고 Kubernetes를 환경에 추가하고 있는 경우 Kubernetes 관측성 30일 시험판에 자동으로 등록됩니다. 평가 기간이 끝날 때까지만 Kubernetes 관측성 관리형 유닛 사용에 대한 요금이 부과됩니다.

## 지정된 도메인에 대한 액세스를 제한합니다

관리자 및 계정 소유자는 이제 이 기능을 사용할 수 있습니다 "Cloud Insights 액세스를 제한합니다" 전자 메일 도메인으로 지정합니다. 관리자 > 사용자 관리 \* 로 이동하고 도메인 제한 버튼을 선택합니다.

### Restrict Domains

Select which domains have access to Cloud Insights:

No restrictions (Cloud Insights available on all domains)

Limit access to default domains (acme.com, gmail.com, netapp.com) ?

Limit access to defaults and following domains

[Learn more about domain restriction.](#)

## Data Collector 업데이트

다음 데이터 수집기/획득 장치 변경 사항이 있습니다.

- \* Isilon/PowerScale REST \*: *emc\_isilon.node\_pool.\** 이름으로 Cloud Insights의 향상된 분석 기능에 다양한 새로운 특성 및 메트릭이 추가되었습니다. 이러한 카운터와 속성을 통해 사용자는 대시보드를 구축하고 *\_node\_pool\_capacity* 소비를 모니터링할 수 있습니다. 서로 다른 하드웨어 노드 모델로 구축된 Isilon 클러스터를 사용하는 사용자는 여러 노드 풀을 갖게 되며, 노드 풀 레벨에서 HDD/SSD/총 용량 소비를 이해하는 것은 모니터링과 계획에 모두 유용합니다.
- \* Rubrik \* "서비스 계정" 인증 지원: Cloud Insights의 Rubrik Collector는 이제 기존의 HTTP 기본 인증(사용자 이름 및 암호)과 사용자 이름 + 비밀 + 조직 ID가 필요한 Rubrik의 서비스 계정 접근 방식을 모두 지원합니다.

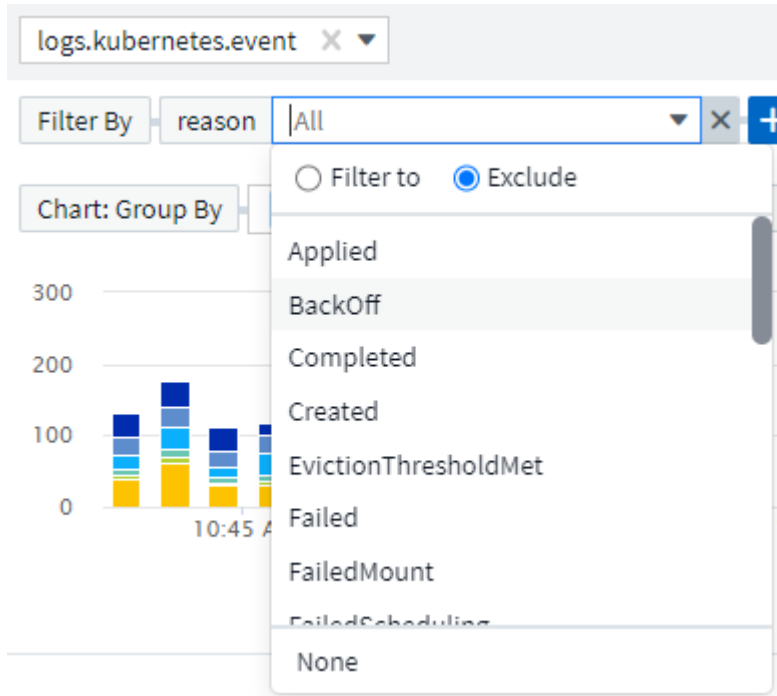
# 2023년 9월

로그에서 원하는 항목을 쉽게 찾을 수 있습니다

로그 쿼리(\* 관측성 > 로그 쿼리 > + 새 로그 쿼리 \*)에는 많은 수가 포함됩니다 "개선 사항" 로그 탐색이 더 쉽고 더 많은 정보를 제공합니다.

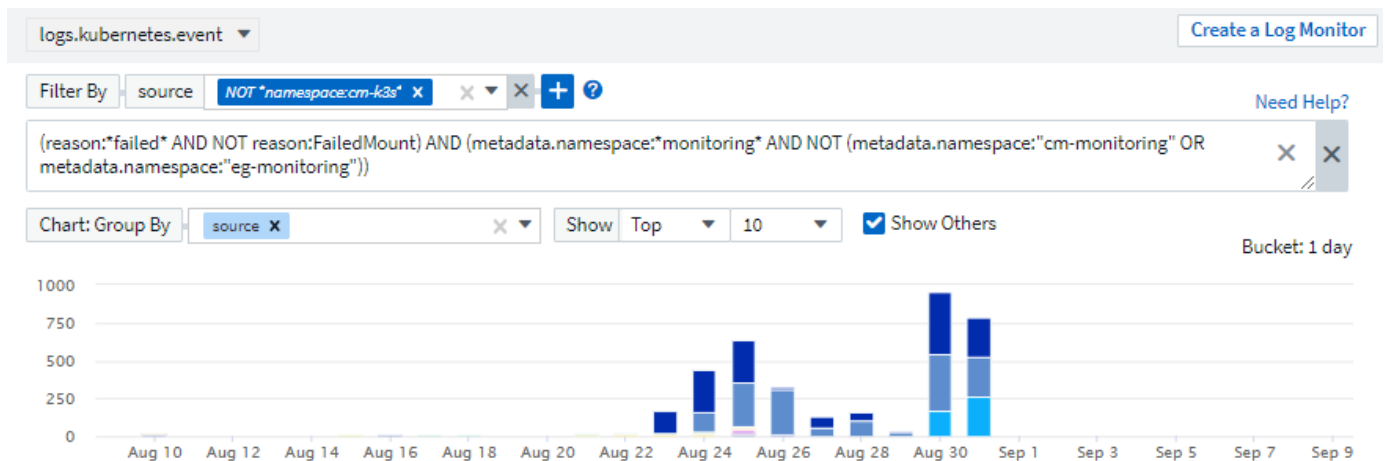
## 포함/제외

값을 필터링할 때 필터와 일치하는 \* 포함 \* 또는 \* 제외 \* 결과를 선택할 수 있습니다. "제외"를 선택하면 "Not <value>" 필터가 생성됩니다. 단일 필터에서 포함 및 제외 값을 결합할 수 있습니다.



## 고급 쿼리

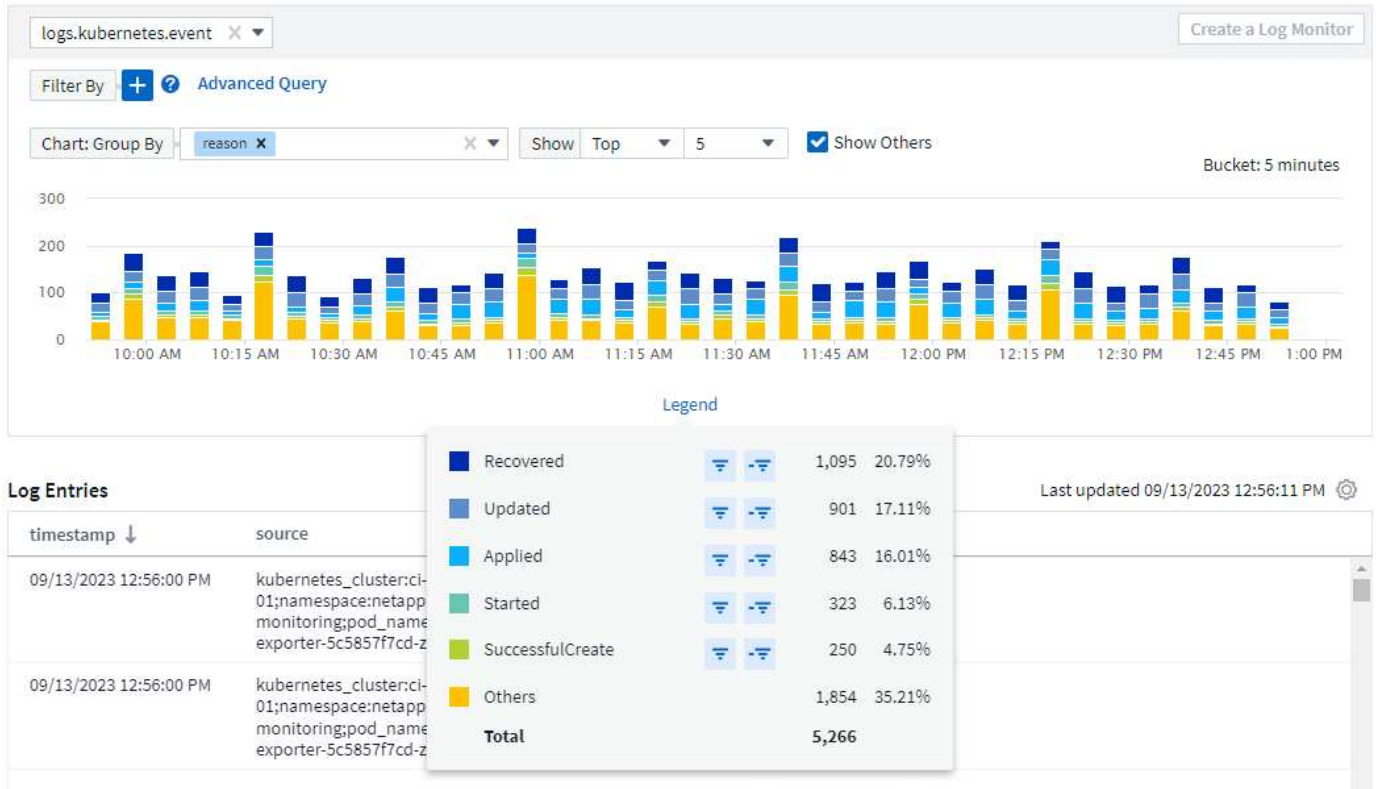
- 고급 쿼리 \* 는 AND, NOT, OR, 와일드카드 등을 사용하여 값을 결합 또는 제외하고 "자유 형식" 필터를 만들 수 있는 기회를 제공합니다



"필터 기준"과 "고급 쿼리"는 "및"로 함께 표시되어 단일 쿼리를 형성합니다. 결과 목록과 차트에 결과가 표시됩니다.

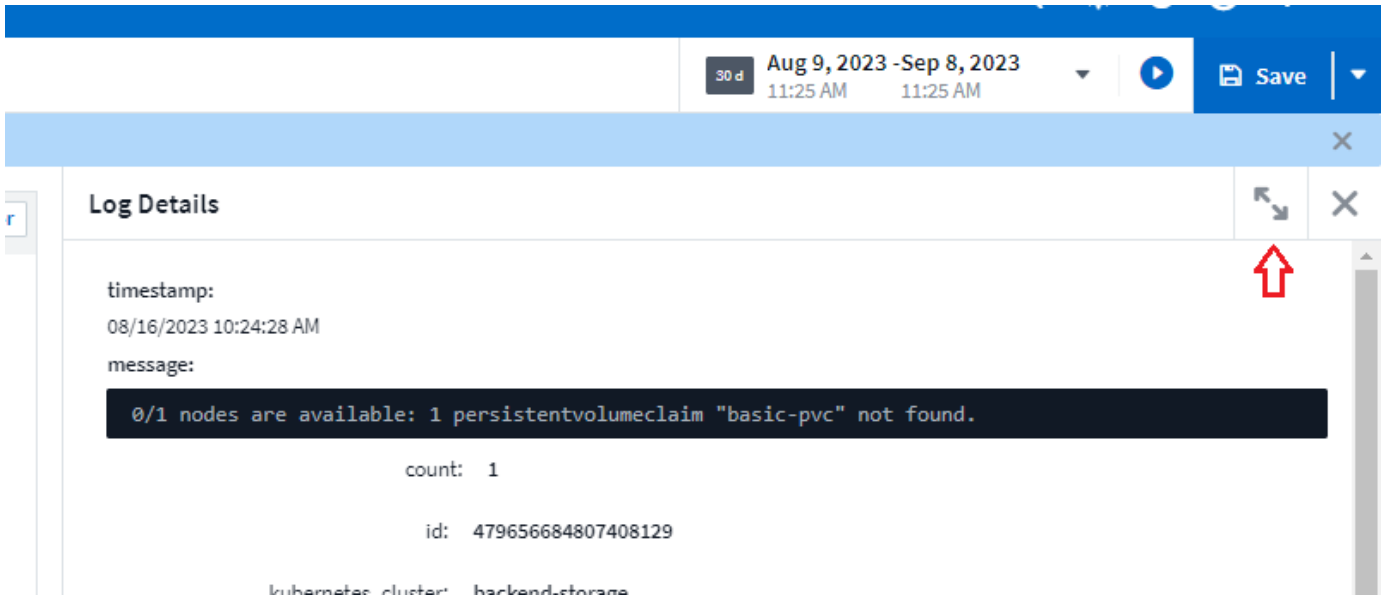
## 차트의 그룹화

Group By \* 에 대한 로그 속성을 선택하면 목록과 차트에 현재 필터의 결과가 표시됩니다. 차트에서 열이 색으로 그룹화되어 있습니다. 차트의 열 위로 마우스를 이동하면 차트 범례를 확장할 때 표시되는 전체 정보와 유사하게 특정 항목에 대한 세부 정보가 표시됩니다. 범례에서는 특정 그룹화에 대해 포함 또는 제외 필터를 설정하도록 선택할 수도 있습니다.



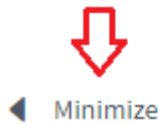
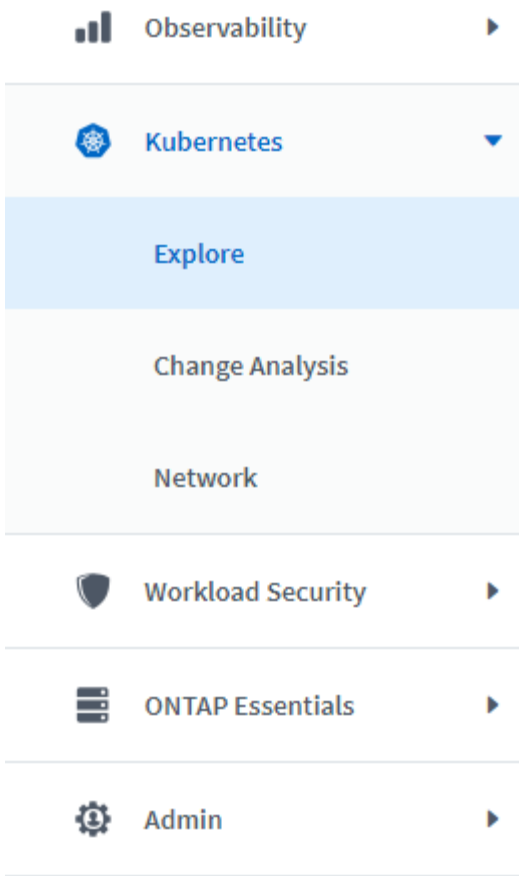
## "유동" 로그 세부 정보 패널

로그 쿼리를 사용하여 로그를 탐색할 때 목록에서 항목을 선택하면 해당 항목에 대한 세부 정보 패널이 열립니다. 이제 슬라이드 아웃 패널 "Floating(부동)"(즉, 화면의 나머지 부분에 표시됨) 또는 "In Page(페이지 내)"(즉, 페이지 내 자체 프레임으로 표시됨)를 표시하도록 선택할 수 있습니다. 이러한 보기 사이를 전환하려면 패널의 오른쪽 상단 모서리에 있는 "페이지/부동" 버튼을 선택합니다.



## 메뉴를 축소합니다

메뉴 아래에 있는 "최소화" 버튼을 선택하여 왼쪽 Cloud Insights 탐색 메뉴를 축소할 수 있습니다. 메뉴가 최소화된 상태에서 아이콘 위에 마우스를 올려 놓으면 열리는 섹션이 표시됩니다. 아이콘을 선택하면 메뉴가 열리고 해당 섹션으로 바로 이동합니다.



## 데이터 수집기 개선

Cloud Insights를 사용하면 데이터 수집기 정보를 보다 쉽게 표시하고 찾을 수 있습니다.

- \* 데이터 수집기 목록 \* 처리는 더 효율적입니다. 즉, 이 목록을 표시하고 탐색하는 데 걸리는 시간이 크게 단축됩니다. 많은 데이터 수집기가 있는 대규모 환경의 경우 데이터 수집기를 나열할 때 성능이 크게 향상됩니다.
- 데이터 수집기 지원 매트릭스 \* 는 .pdf 파일에서 .html 기반 페이지로 이동하므로 탐색이 더 빠르고 유지 관리가 용이합니다. 새로운 매트릭스는 다음 웹 사이트에서 확인하십시오. [https://docs.netapp.com/us-en/cloudinsights/reference\\_data\\_collector\\_support\\_matrix.html](https://docs.netapp.com/us-en/cloudinsights/reference_data_collector_support_matrix.html)

## 2023년 8월

### Isilon/PowerScale 로그 및 고급 분석 데이터 수집

Isilon REST 및 PowerScale REST Collector에는 다음과 같은 향상된 기능이 포함되어 있습니다.



- Isilon 로그 이벤트는 쿼리 및 알림에 사용할 수 있습니다
- Isilon Advanced Analytic 속성은 쿼리, 대시보드 및 알림에 사용할 수 있습니다.
  - EMC\_Isilon.cluster입니다
  - emc\_isilon.node
  - emc\_isilon.node\_disk
  - emc\_isilon.net\_iface

이러한 기능은 Isilon REST 및/또는 PowerScale REST Collector 사용자에게 기본적으로 설정됩니다. NetApp는 Isilon CLI 기반 Collector를 사용하는 사용자가 위와 같은 개선 사항을 받으려면 새로운 REST API 기반 Collector로 마이그레이션할 것을 적극 권장합니다.

## 개선된 워크로드 맵

워크로드 맵은 보다 유용하고 노이즈가 적으며, 동일한 워크로드와 통신하는 경우 유사한 모든 외부 서비스를 하나의 노드로 그룹화하여 그래프의 복잡성을 줄이고 서비스 상호 연결 방식을 더 쉽게 이해할 수 있도록 합니다.

그룹화된 노드를 선택하면 해당 노드와 관련된 각 외부 서비스에 대한 네트워크 트래픽 메트릭이 포함된 상세 테이블이 표시됩니다.

## Kubernetes 관리 유닛 사용 조정

NetApp Kubernetes 모니터링 담당자와 기본 인프라 데이터 수집기(예: VMware)가 Kubernetes 클러스터 환경에서 컴퓨팅 리소스를 계산하는 경우 관리되는 장치의 수를 가장 효율적으로 카운트할 수 있도록 이러한 리소스 사용이 조정됩니다. Kubernetes MU 조정 사항은 요약 및 사용 탭 모두에서 관리자 > 구독 페이지에서 확인할 수 있습니다.

요약 탭:

Managed Unit (MU) Usage Calculator [Estimate Renewal Cost](#)

<input checked="" type="checkbox"/> Infrastructure Observability <a href="#">?</a>	82	Hosts	289.47	Raw TiB	55.75	Object TiB	Current Usage	Managed Units = 114.75
<input checked="" type="checkbox"/> Kubernetes Observability <a href="#">?</a>	64	vCPUs	Current Usage					Managed Units = 16
Adjustments:								
<input checked="" type="checkbox"/> Kubernetes Observability <a href="#">?</a>	2	Hosts	Adjustment for duplicate Infrastructure Observability Hosts					Managed Units = (1)
								Consumed Managed Units = 130/500

사용 탭:

Infrastructure Observability **Kubernetes Observability**

Installed Cluster Agents (3) [?](#)

Name	vCPUs	Metered Managed Units	Managed Units Adjustment	Consumed Managed Units ↓
oc4-kp	48	12.00	(0.00)	12.00
july-deploy	8	2.00	(0.00)	2.00
twonode	8	2.00	(1.00)	1.00

## 수집기/획득 변경:

다음 데이터 수집기/획득 장치 변경 사항이 있습니다.

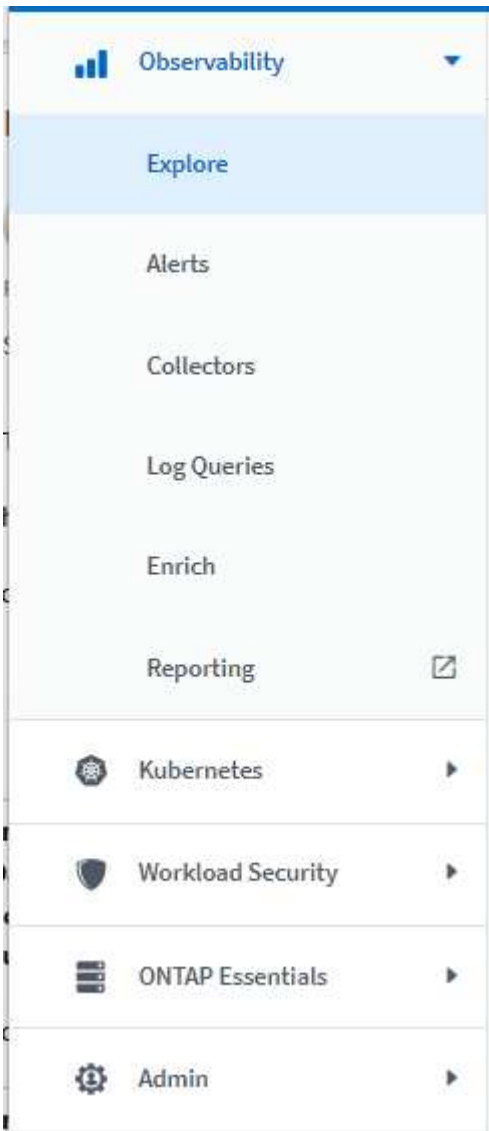
- 이제 Acquisition Unit은 RHEL 8.7을 지원합니다.

## 개선된 메뉴

고객의 워크플로우를 더욱 효과적으로 지원할 수 있도록 좌측 탐색 메뉴를 업데이트했습니다. `_Kubernetes_` 와 같은 새로운 최상위 항목은 고객의 요구 사항에 대한 액세스를 가속화하며, 통합된 관리자 콘솔은 테넌트 소유자 역할을 지원합니다.

다음은 몇 가지 변경 사항의 추가 예입니다.

- 최상위 `_관측성_` 메뉴는 데이터 검색, 경고 및 로그 쿼리를 보여줍니다
- 관측성 및 워크로드 보안을 위한 'API 액세스' 기능은 단일 메뉴 아래에 있습니다
- 마찬가지로, 관측성 및 워크로드 보안 '알림' 기능도 한 가지 메뉴로 제공됩니다



다음은 각 메뉴에서 찾을 수 있는 기능의 간단한 목록입니다.

관측성:

- 탐색(대시보드, 메트릭 쿼리, 인프라 인사이트)
- 경고(모니터 및 경고)
- 수집기(데이터 수집기 및 획득 장치)
- 로그 쿼리
- 보강(주석 및 주석 규칙, 응용 프로그램, 장치 해상도)
- 보고

#### 쿠버네티스:

- 클러스터 탐색 및 네트워크 맵

#### 워크로드 보안:

- 경고
- 법의학
- 수집기
- 정책

#### ONTAP 요약:

- 데이터 보호
- 보안
- 경고
- 검토할 수 있습니다
- 네트워킹
- 워크로드
- VMware

#### 관리자:

- API 액세스
- 감사
- 알림
- 구독 정보
- 사용자 관리

## 2023년 7월

### 최근 변경 내용 표시

이제 Data Collector 시작 페이지에 최근 변경 사항 목록이 포함됩니다. 데이터 수집기 랜딩 페이지 맨 아래에 있는 "최근 변경 사항" 버튼을 클릭하면 최근 데이터 수집기 변경 사항이 표시됩니다.

## Changes Reported by This Data Collector (1)

Time ↓	Change
07/06/2023 6:39:12 PM	<div><input type="checkbox"/> <b>Storage CI-GDL1-Ontap-fas8080 configuration changed</b> Property <b>Display IP</b> is changed from "10.192.122.10" to "10.192.122.12" Property <b>Manage URL</b> is changed from "HTTPS://10.192.122.10:443" to "HTTPS://10.192.122.12:443"</div>

[Hide Recent Changes](#)

## 운전자 개선

에서는 다음과 같은 개선 사항이 이루어졌습니다 "[Kubernetes 운전자](#)" 배포:

- Docker 메트릭 수집을 무시하는 옵션입니다
- Telegraf Demonsets 및 Replicasets에 대한 허용 기준을 추가하고 사용자 지정할 수 있습니다

## Insight: 콜드 스토리지 부가세 반환 청구액

를 클릭합니다 "[ONTAP 콜드 스토리지 파악 비용 재확보](#)" 이제 FlexGroups를 지원하며 모든 고객이 사용할 수 있습니다.

## 작업자 이미지 서명

NetApp Kubernetes 모니터링 운영자용 개인 저장소를 사용하는 고객의 경우, 이제 오퍼레이터 설치 중에 이미지 서명 공개 키를 복사하여 다운로드한 소프트웨어의 정품 여부를 확인할 수 있습니다. 사용자 이미지를 개인 리포지토리에 업로드 \_ 하는 선택적 단계 동안 \_ 이미지 서명 공개 키 복사 \_ 버튼을 선택합니다.

[Copy Image Signature Public Key](#)

[Reveal Image Signature Public Key](#)

```
-----BEGIN PUBLIC KEY-----
MIIBojANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBigKCAYEAAoA/Iww7C/1DfDrwYKwPL
hJzSbT7BnsV/j6Wh/U9Qv4MWhYPCT/uW8ucMPkIHK56bVeiy1di23TL16p+M7y2y
Jjg8SYJdEE0Llopj+X6W/N00B4kHMDlV8VXzJ0lk3zcT2NHiySzB/IYicTfheIpI
hJzSbT7BnsV/j6Wh/U9Qv4MWhYPCT/uW8ucMPkIHK56bVeiy1di23TL16p+M7y2y
NiX7KwYpG6K8YSIW89MvTwbAr7S76liw8Um6VsnsXF655h3dd769UhahiQqv6Z5
```

## 쿼리의 집계, 조건부 서식 및 기타

집계, 단위 선택, 조건부 서식 및 열 이름 바꾸기는 대시보드 테이블 위젯의 가장 유용한 기능 중 하나이며, 이제 이러한 기능을 에서 사용할 수 있습니다 "[쿼리](#)".

143 items found

Table Row Grouping	Metrics & Attributes
agent.node_diskio ↑	io_time (ms)
nvme0n1	20,604,960.00
nvme0n1	29,184,970.00
nvme0n1	4,642,684.00
nvme0n1	31,918,988.00
nvme0n1	29,258,256.00
nvme0n1	18,022,164.00
nvme0n1	28,483,300.00
nvme0n1	69,835,016.00
nvme0n1	15,952,780.00
nvme0n1	44,169,696.00
nvme0n1	12,138,928.00
nvme0n1	5,234,528.00
nvme0n1	34,260,552.00

Aggregation

Group By: Avg

Time Aggregate By: Last

Unit Display

Base Unit: millisecond (ms)

Displayed In: millisecond (ms)

Conditional Formatting Reset

If value is: > (Greater than)

Warning: Optional ms

Critical: Optional ms

Rename Column

이러한 기능은 현재 통합 유형 데이터(Kubernetes, ONTAP 고급 메트릭 등)에 사용할 수 있으며, 인프라 오브젝트 (스토리지, 볼륨, 스위치 등)에 대해 곧 제공될 예정입니다.

## 감사를 위한 API

이제 API를 사용하여 감사된 이벤트를 쿼리하거나 내보낼 수 있습니다. 관리자 > API 액세스로 이동하여 자세한 내용을 보려면 `_API Documentation_link`를 선택하십시오.

# audit

POST

`/audit/export` Export audit data

POST

`/audit/query` Run a query for audit

## 데이터 수집기: Trident 이코노미

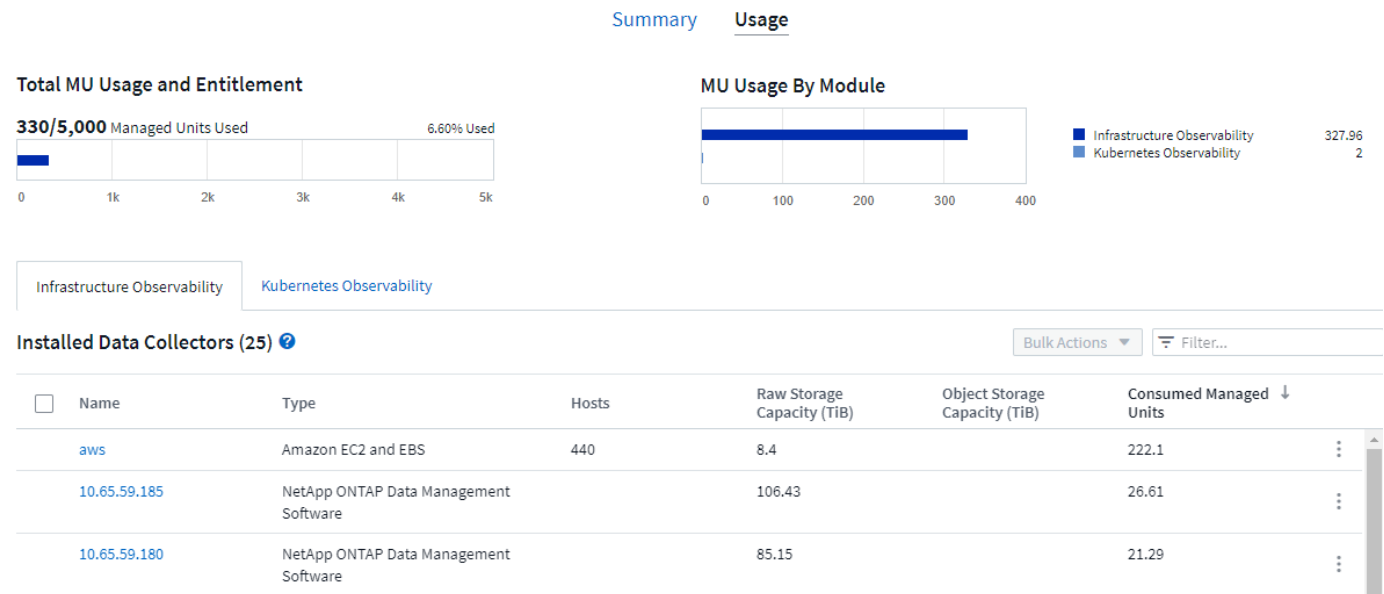
Cloud Insights는 이제 Trident 이코노미 드라이버를 지원하므로 다음과 같은 이점을 누릴 수 있습니다.

- Pod-ONTAP Qtree 매핑 및 성능 메트릭에 대한 가시성을 제공합니다.
- Kubernetes Pod에서 백엔드 스토리지로 원활하게 문제를 해결하고 쉽게 탐색할 수 있습니다
- 모니터의 백엔드 성능 문제를 사전 예방적으로 감지합니다

## 2023년 6월

### 사용 현황을 확인합니다

2023년 6월부터 Cloud Insights는 기능 세트를 기준으로 관리되는 장치 사용에 대한 분석을 제공합니다. 이제 인프라의 관리 장치(MU) 사용량과 Kubernetes와 연결된 MU 사용량을 빠르게 확인하고 모니터링할 수 있습니다.



## Kubernetes Network Monitoring and Map은 모든 경우에 사용할 수 있습니다

를 클릭합니다 "\_Kubernetes 네트워크 성능 및 맵\_" Kubernetes 워크로드 간의 종속성을 매핑하여 문제 해결을 단순화함으로써 Kubernetes 네트워크 성능 지연 시간 및 이상 징후를 실시간으로 파악하여 사용자에게 영향을 미치기 전에 성능 문제를 식별합니다. 많은 고객이 미리 보기 중에 유용하다고 확인했으며, 이제 모두가 즐길 수 있습니다.

### 수집기/획득 변경:

다음 데이터 수집기/획득 장치 변경 사항이 있습니다.

- Data Domain 및 Cohesity MU는 40TiB:1MU로 측정됩니다.
- 이제 인수 장치는 RHEL 및 Rocky 9.0 및 9.1을 지원합니다.

## 새로운 ONTAP Essentials 대시보드

다음 ONTAP Essentials 대시보드는 미리 보기 환경에서 사용할 수 있으며 이제 모든 사용자가 사용할 수 있습니다.

- 보안 대시보드
- 데이터 보호 대시보드(로컬 및 원격 보호 개요 포함)

## 추가 시스템 모니터

Cloud Insights에는 다음과 같은 시스템 모니터가 포함되어 있습니다.

- 스토리지 VM FCP 서비스를 사용할 수 없습니다
- 스토리지 VM iSCSI 서비스를 사용할 수 없습니다

# 2023년 5월

## Kubernetes 모니터링 오퍼레이터 설치가 개선되었습니다

의 설치 및 구성 "[NetApp Kubernetes 모니터링 운영자](#)" 다음과 같은 향상된 기능으로 그 어느 때보다 쉬워졌습니다.

- 방법입니다 "[구성 설정](#)" 자체 문서화된 단일 구성 파일로 저장됩니다.
- Kubernetes Monitoring Operator 이미지를 개인 저장소에 업로드하기 위한 단계별 지침입니다.
- 사용자 지정 구성을 유지하면서 Kubernetes Monitoring을 업그레이드하는 단일 명령으로 간단하게 업그레이드할 수 있습니다.
- 보안 향상: API 키가 비밀을 안전하게 관리하고 있습니다.
- CI/CD 자동화 툴을 손쉽게 통합 및 구축할 수 있습니다.

## 스토리지 가상화

Cloud Insights는 로컬 스토리지가 있는 스토리지 어레이와 다른 스토리지 어레이의 가상화를 구분할 수 있습니다. 이를 통해 비용을 관련시키고 프런트 엔드와 성능을 인프라 백 엔드와 구별할 수 있습니다.

### Storage Summary

**Model:**  
V-Series

**Vendor:**  
NetApp

**Family:**  
V-Series

**Serial Number:**  
1306894

**IP:**  
192.168.7.41

**Virtualized Type:**  
Virtual

**Backend Storage:**  
[Sym-000050074300343](#)

**Microcode Version:**  
8.0.2 7-Mode

**Raw Capacity:**  
0.0 GiB

**Latency - Total:**  
N/A

**IOPS - Total:**  
N/A

**Throughput - Total:**  
N/A

**Management:**

**FC Fabrics Connected:**  
7

**Alert Monitors:**

## 새 Webhook 매개 변수

을 생성할 때 "웹훅" 이제 Webhook 정의에 다음 매개 변수를 포함할 수 있습니다.

- %%TriggeredOnKeys%%
- %%TriggeredOnValues%%입니다

## Kubernetes 데이터에 대한 리포팅

PV(영구적 볼륨), PVC, 워크로드, 클러스터, 네임스페이스를 비롯한 Cloud Insights에서 수집된 Kubernetes 데이터를 이제 보고, 차지백, 추세, 예측, TTF 계산, 기타 Kubernetes 메트릭의 비즈니스 보고 기능을 제공합니다.

## 새 고객에 대해 활성화된 기본 ONTAP 시스템 모니터

새로운 Cloud Insights 환경에서는 많은 ONTAP 시스템 모니터가 기본적으로 활성화(즉, 재개)됩니다. 이전 버전에서는 대부분의 모니터가 \_ 일시 중지됨 \_ 상태로 기본 설정되어 있습니다. 회사마다 비즈니스 요구 사항이 다르기 때문에 항상 을 살펴보는 것이 좋습니다 "시스템 모니터" 사용자 환경에서 경고 요구에 따라 각 항목을 일시 중지하거나 다시 시작합니다.

---

## 2023년 4월

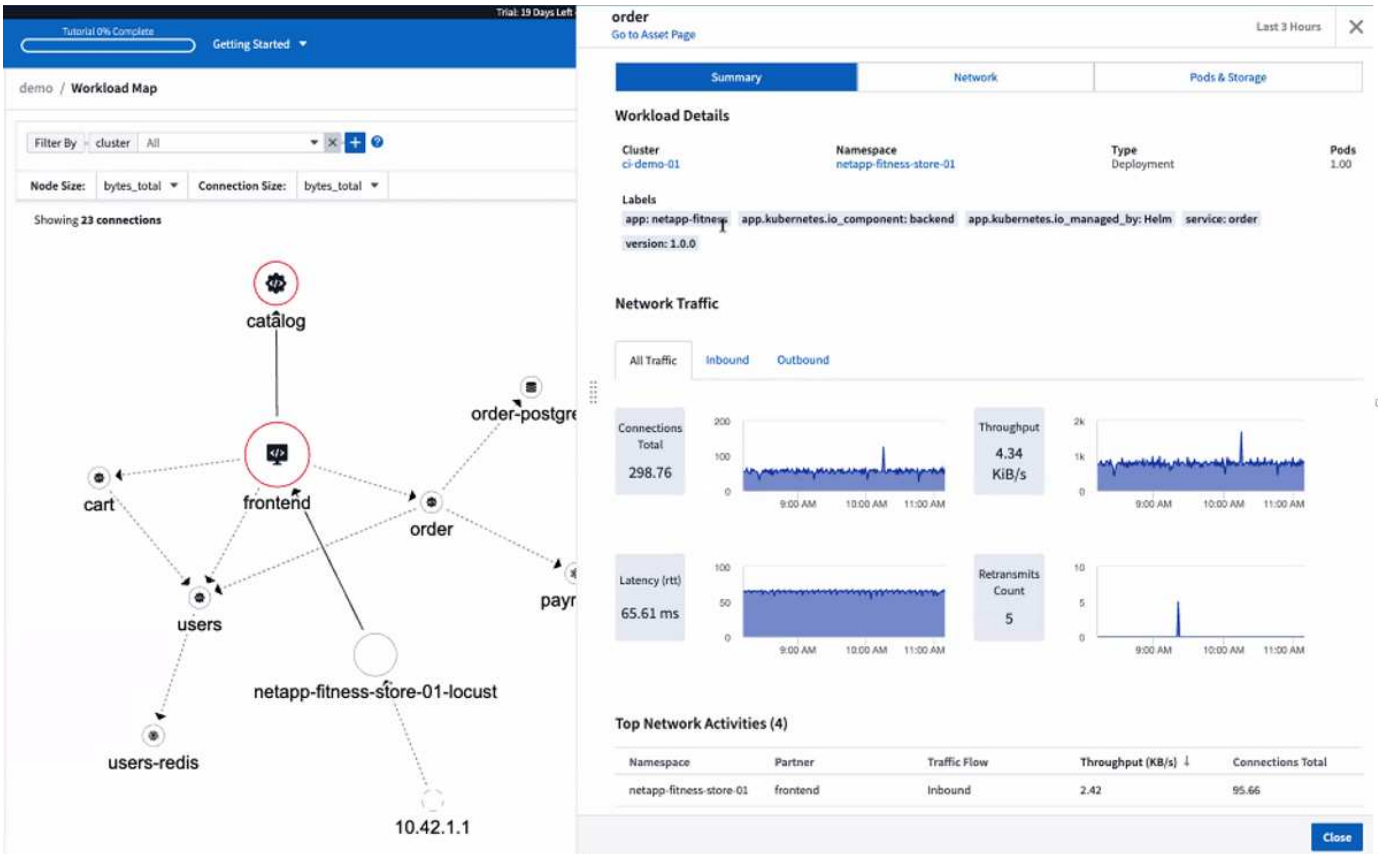
### Kubernetes 성능 모니터링 및 맵

를 클릭합니다 "[Kubernetes 네트워크 성능 및 맵](#)" Kubernetes 워크로드 간의 종속성을 매핑하여 문제 해결을 간소화합니다. Kubernetes 네트워크 성능 지연 시간 및 이상 징후를 실시간으로 파악하여 사용자에게 영향을 미치기 전에 성능 문제를 식별할 수 있습니다. 이 기능은 조직이 Kubernetes 트래픽 흐름을 분석하고 감사하여 전체 비용을 절감할 수 있도록 도와줍니다.

주요 기능: • 워크로드 맵은 Kubernetes 워크로드 종속성 및 흐름을 제공하고 네트워크 및 성능 문제를 강조합니다. • Kubernetes Pod, 워크로드 및 노드 간의 네트워크 트래픽을 모니터링하고, 트래픽 및 지연 문제의 원인을 식별합니다. • 수신, 송신, 지역 간 및 교차 영역 네트워크 트래픽을 분석하여 전체 비용을 절감합니다.

"Slideout" 세부 정보를 보여주는 워크로드 맵:





Kubernetes 성능 모니터링 및 맵은 으로 제공됩니다 **"미리보기"** 피쳐.

## ONTAP Essentials 보안 대시보드

를 클릭합니다 **"보안 대시보드"** 하드웨어 및 소프트웨어 볼륨 암호화, 랜섬웨어 방지 상태 및 클러스터 인증 방법에 대한 차트를 보여 주는 현재의 보안 상황을 즉시 확인할 수 있습니다. 보안 대시보드는 로 사용할 수 있습니다 **"미리보기"** 피쳐.

**ONTAP Essentials**

- Overview
- Data Protection
- Security
- Alerts
- Infrastructure
- Networking
- Workloads
- Workload Security**

We want your input to improve the user experience of NetApp Products. Share your feedback.

**Volume Encryption**

7/119 Encrypted

Hardware:	2
Software:	2
Hardware and Software:	3
Unencrypted:	112

**SVM Anti-Ransomware Status**

6/20 Enabled

Cloud Insights Workload Security:	2
ONTAP ARP:	4
Unprotected:	14

Protect with Cloud Insights Workload Security

**Cluster Authentication Methods**

Authentication Methods		Certificates
SAML	AD/LDAP	Expiring in <60 Days
0	2	0
Certificate	Local	Expired
2	5	1

**Clusters (5)**

Cluster	Compliance	Volume Encryption (%)	Protected by ONTAP ARP (%)	Protected by Workload Sec...	Details
aws-54985490-55275986-aws	Not Compliant	0.00	0.00	0.00	🔍
ocisedev	Not Compliant	0.00	0.00	40.00	🔍
rtp-sa-cl04	Not Compliant	0.00	0.00	0.00	🔍
C1_sti43-vs1im-ucs513w_1678253476	Compliant	77.78	50.00	0.00	🔍
dineshtscluster-1	Compliant	0.00	0.00	0.00	🔍

[View Security Hardening Guide](#)

## ONTAP 콜드 스토리지 재확보

Reclaim ONTAP 냉장 보관 Insight는 ONTAP 시스템의 볼륨에 대한 콜드 용량, 잠재적 비용/전력 절감 및 권장 조치 항목에 대한 데이터를 제공합니다.

**84 Workloads on storage umeng-aff300-01-02 contains a total of 1.2 TiB of cold data.**

You could lower costs 5.6% a year and reduce your carbon footprint by moving cold storage to the cloud.

Detected: 16 days ago, 9:21 AM (ACTIVE)  
Apr 14, 2023 12:06PM

Estimated Yearly Cost Savings\*

\$1,228.80

**Move 1.2 TiB of data to the cloud**

Current Storage (TiB)

Category	Value (TiB)
Used	3.9
Optimized (Estimate)	2.7

kWh Reduction Yearly Savings\*\*

76.75 kWh

\*Visit the [NetApp TCO Calculator](#) for your actual cost savings. Go to [Annotation Page](#) to edit the cloud tier cost in the tier annotation.

\*\* Based on average disk power consumption

**Hold or cycle down available storage**

2 x 1 TiB SSDs = 76.75 kWh per year \*\*

Insight에서 다음과 같은 질문에 답변할 수 있습니다.

- 스토리지 클러스터의 콜드 데이터는 (a) 고비용의 SSD 디스크, (b) HDD 디스크, (c) 가상 디스크에 있습니까?
- 최적화되지 않은 스토리지와 관련하여 가장 큰 기여 요인은 무엇입니까?
- 특정 워크로드에서 데이터가 콜드 상태가 된 기간(일)은 얼마입니까?

\_Reclaim ONTAP 냉장 보관 \_ 은(는) 로 간주됩니다 "\_미리보기\_" 변경될 수 있습니다.

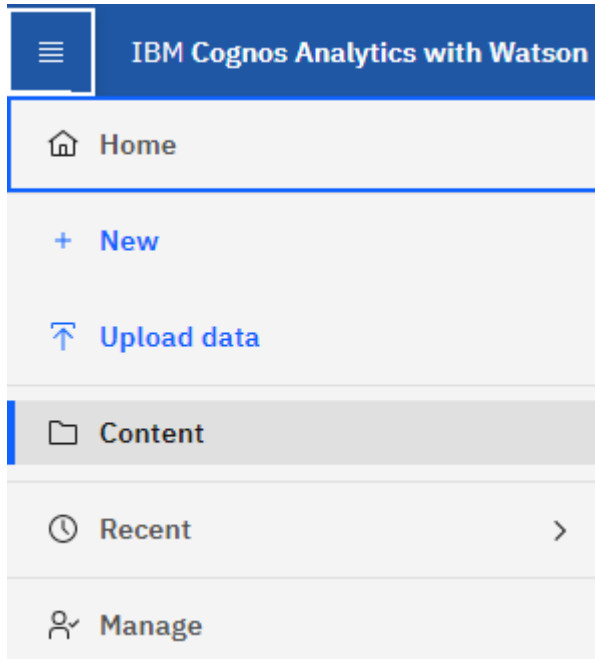
## 구독 알림은 배너 메시지도 제어합니다

구독 알림을 받는 사람 설정(관리자 > 알림) 또한 구독 관련 제품 내 배너 알림을 볼 사용자를 제어합니다.

**i** Your subscription is expiring in 2 days. [View Subscription](#)

## 보고 기능이 새롭게 추가되었습니다

Cloud Insights 보고 화면의 모양이 새롭게 바뀌었고 일부 메뉴 탐색이 변경되었음을 알 수 있습니다. 이러한 화면 및 탐색 변경 사항은 현재 에서 업데이트되었습니다 "[보고 문서](#)".



## 모니터가 기본적으로 일시 중지되었습니다

새로운 Cloud Insights 환경에서는 이 점에 유의하십시오 "[시스템 정의 모니터](#)" 기본적으로 경고 알림을 보내지 않습니다. 모니터에 대해 하나 이상의 전달 방법을 추가하여 알림을 받을 모니터에 대한 알림을 활성화해야 합니다. 기존 Cloud Insights 환경의 경우 현재 \_ 일시 중지됨 \_ 상태에 있는 시스템 정의 모니터에 대해 default\_global\_notification 수신자 목록이 제거되었습니다. 사용자 정의 알림은 현재 활성화된 시스템 정의 모니터에 대한 알림 설정과 마찬가지로 변경되지 않습니다.

## API 미터링 탭을 찾고 계십니까?

API 미터링 기능이 가입 페이지에서 \* 관리자 > API 액세스 \* 페이지로 이동했습니다.

## 2023년 3월

### ONTAP 9.9+용 클라우드 연결은 더 이상 사용되지 않습니다

ONTAP 9.9 이상의 데이터 수집기에 대한 클라우드 연결이 더 이상 사용되지 않습니다. 2023년 4월 4일부터 사용자

환경의 Cloud Connection 데이터 수집기는 더 이상 데이터를 수집하지 않으며 폴링 시 오류를 표시합니다. 클라우드 연결 데이터 수집기는 후속 업데이트에서 Cloud Insights에서 완전히 제거됩니다.

2023년 4월 4일 이전에는 클라우드 연결에서 현재 수집한 ONTAP 시스템의 새로운 NetApp ONTAP 데이터 관리 소프트웨어 데이터 수집기를 구성해야 합니다. ["자세한 정보"](#).

---

## 2023년 1월

### 새 로그 모니터

거의 20개를 추가했습니다 ["추가 시스템 모니터"](#) 끊어진 상호 연결 링크, 하트비트 문제 등에 대해 경고합니다. 또한 SnapMirror 자동 재동기화, MetroCluster 미러링 및 FabricPool 미러 재동기화 변경 사항을 알리기 위해 세 개의 새로운 데이터 보호 로그 모니터가 추가되었습니다.

이러한 모니터 중 일부는 기본적으로 `_ENABLED_`로 설정됩니다. 이러한 모니터에 대해 경고를 표시하지 않으려면 `_PAUSE_`로 설정해야 합니다. 또한 이러한 모니터는 알림을 전달하도록 구성되지 않았습니다. e-메일 또는 웹 후크를 통해 알림을 보내려면 이러한 모니터에서 알림 수신자를 구성해야 합니다.

### 모든 대시보드 테이블 위젯에 대한 **.csv** 내보내기

데이터에 대한 접근성을 보장하는 것이 매우 중요합니다. 쿼리하는 데이터 유형(자산 또는 통합)에 관계없이 모든 메트릭 쿼리, 대시보드 테이블 위젯 및 객체 랜딩 페이지에 대해 CSV 내보내기를 사용할 수 있습니다.

이제 열 선택, 열 이름 바꾸기, 단위 변환과 같은 데이터 사용자 지정 기능도 새로운 내보내기 기능에 포함됩니다.

---

## 2022년 12월

### Cloud Insights 평가판 을 통해 랜섬웨어 차단 및 기타 보안 기능을 탐색하십시오

오늘부터 새로운 Cloud Insights 평가판을 신청하면 랜섬웨어 탐지 및 자동화된 사용자 차단 응답 정책과 같은 보안 기능을 탐색할 수 있습니다. 평가판을 신청하지 않았다면 지금 바로 등록하세요!

### Kubernetes 워크로드에는 고유한 랜딩 페이지가 있습니다

워크로드는 Kubernetes 환경의 핵심 부분이므로 Cloud Insights은 현재 이러한 워크로드에 대한 랜딩 페이지를 제공합니다. Kubernetes 워크로드에 영향을 미치는 문제를 여기 에서 확인, 탐색 및 해결할 수 있습니다.

Filter By + ⓘ

1/1

Pods: Current / Desired

-

Up-to-date Unavailable

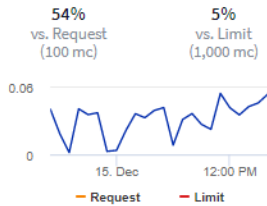
Namespace <b>dockerimage-monitoring</b>	Type <b>ReplicaSet</b>	Date Created <b>Dec 9, 2022 4:37 PM</b>
--	---------------------------	--

Labels

-

54mc

CPU

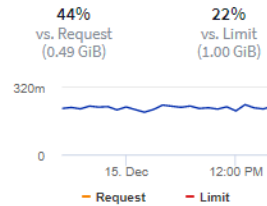


Highest CPU Demand by Pod

2.8m telegraf-rs-2xsj2

0.22GiB

Memory



Highest Memory Demand by Pod

0.21 GiB telegraf-rs-2xsj2

0.00GiB

Total PVC Capacity claimed

Pods (1)

Pod Name ↑	Status	Healthy Containers	cpu_usage_nanocores (mc)	memory_rss_bytes (GiB)
telegraf-rs-2xsj2	● Healthy Running	1 of 1	3	0.21

## 체크섬을 확인하십시오

Windows 및 Linux용 에이전트를 설치하는 동안 체크섬 값을 제공하도록 요청했으며 이는 좋은 생각이라고 생각합니다. 주요 내용은 다음과 같습니다.

### ☐ Manually Verifying Telegraf Checksums

The Cloud Insights agent installer performs integrity checks, but some users may want to perform their own verifications before installing or applying downloaded artifacts.

For more information, read about [verifying checksums](#) before proceeding to the next step.

The SHA256 checksum for this telegraf.pkg is:

```
cbd0d8d0512b65fbc0c786d8d0512b651de0e1cf003e0a0d9df01d8d0512b65
```

## 로그 경고가 개선되었습니다

### 그룹화 기준

로그 모니터를 만들거나 편집할 때 이제 "그룹화 기준" 속성을 설정하여 보다 집중적인 경고를 허용할 수 있습니다. 모니터 정의의 "필터" 설정 아래에서 "그룹화 기준" 속성을 찾습니다.

## 1 Select the log to monitor

Log Source logs.netapp.ems

Filter By ems.ems\_message\_type Nblade.vscanConnBackPressure x x ems.cluster\_vendor NetApp x x

ems.cluster\_model FAS\* x AFF\* x ASA\* x Fdvm\* x + ?

Group By ems.cluster\_uuid x ems.cluster\_vendor x ems.cluster\_model x ems.cluster\_name x  
ems.svm\_uuid x ems.svm\_name x

이렇게 변경하면 모니터 정의의 "그룹화 기준" 측면을 정규화하여 메트릭 모니터와 로그 모니터를 기능 패리티로 가져옵니다. 이 패리티를 통해 고객은 추가 사용자 지정을 위해 모든 \* 시스템 정의의 기본 모니터를 복제/복제할 수 있습니다.

복제 중

이제 변경 로그, Kubernetes 로그 및 Data Collector 로그 모니터를 복제(복제)할 수 있습니다. 이렇게 하면 특정 정의에 맞게 수정할 수 있는 새 사용자 지정 로그 모니터가 생성됩니다.

Data Collection (4) + Monitor Bulk Actions Filter...

<input type="checkbox"/>	Name	Metric / Parameters	Severity	Time Frame	Status
<input type="checkbox"/>	Acquisition Unit Heartbeat-Critical	logs.cloud_insights.acquisition (source = acquisition_unit:, acquisition_unit.status = "Heartbeat Overdue", acquisition_unit.overdue_time >= 600 sec)	<span style="color: red;">!</span> Critical	Once	Active
<input type="checkbox"/>	Acquisition Unit Heartbeat-Warning	logs.cloud_insights.acquisition (source = acquisition_unit:, acquisition_unit.status = "Heartbeat Overdue", acquisition_unit.overdue_time >= 300 sec)	<span style="color: orange;">!</span> Warning	Once	Active

Duplicate  
Pause

## 비즈니스 연속성을 위한 SnapMirror를 포함하는 새로운 기본 ONTAP 모니터 11개

거의 12개의 새로운 기능이 추가되었습니다 **"시스템 모니터"** SMBC(비즈니스 연속성을 위한 SnapMirror): SMBC 인증서 및 ONTAP 중개자의 변경 사항을 경고합니다.

## 2022년 11월

### 40개 이상의 새로운 보안, 데이터 수집 및 CVO 모니터!

NetApp은 수십 개의 새로운 시스템 정의 모니터를 추가하여 Cloud Volumes, Security 및 Data Protection의 잠재적 문제를 경고합니다. 이 모니터에 대해 자세히 알아보십시오 **"여기"**.

## 2022년 10월

**ONTAP Autonomous** 랜섬웨어 보호 통합을 통해 더 정확하고 우수한 랜섬웨어 탐지 기능을 제공합니다

Cloud Secure은 ONTAP과의 통합을 통해 랜섬웨어 탐지 기능을 개선합니다 **"자율 랜섬웨어 보호"** (ARP)

Cloud Secure는 잠재적인 볼륨 파일 암호화 작업에 대한 ONTAP ARP 이벤트를 수신합니다

- 볼륨 암호화 이벤트와 사용자 활동의 상관 관계를 분석하여 손상을 일으키는 원인을 파악하고,
- 자동 응답 정책을 구현하여 공격을 차단합니다.
- 영향을 받은 파일을 식별하여 신속하게 복구하고 데이터 침해 조사를 수행할 수 있습니다.

## 2022년 9월

기본 버전에서 사용할 수 있는 모니터입니다

ONTAP "기본 모니터" 이제 Cloud Insights Basic Edition에서 사용할 수 있습니다. 여기에는 70개 이상의 인프라 모니터와 30개의 워크로드 예가 포함됩니다.

### ONTAP Power 및 StorageGRID 대시보드

대시보드 갤러리에는 ONTAP 전원 및 온도에 대한 새로운 대시보드와 StorageGRID에 대한 4개의 대시보드가 포함되어 있습니다. 사용자 환경에서 ONTAP 전력 메트릭 및/또는 StorageGRID 데이터를 수집하는 경우 Gallery \* 에서 \* + 를 선택하여 이러한 대시보드를 가져옵니다.

표에서 임계값 표시 상태를 한 눈에 파악할 수 있습니다

조건부 서식을 사용하면 테이블 위젯에서 경고 수준 및 위험 수준 임계값을 설정하고 강조 표시하여 이상값 및 예외적인 데이터 지점에 대한 즉각적인 가시성을 얻을 수 있습니다.

Table Row Grouping	Expanded Detail	Metrics & Attributes	capacity.provisioned (GiB)
All	Storage Pool	capacityRatio.used (%)	
All (14)	--	95.15	
--	rtp-sa-cl06-02:aggr_data1_rtp_sa_cl06_02	0.79	
--	rtp-sa-cl06-01:aggr_data1_rtp_sa_cl06_01	2.45	
--	rtp-sa-cl06-02:aggr0_rtp_sa_cl06_02_root	95.15	
--	rtp-sa-cl06-01:aggr0_rtp_sa_cl06_01_root	95.15	

Formatting:  Show Expanded Details    Conditional Formatting: Background Color + Icon     Show  In Range as green

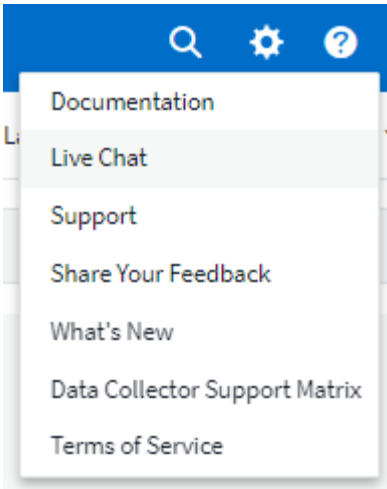
Conditional Formatting Settings:  
If value is: > (Greater than)  
Warning: 70 %  
Critical: 90 %

### 보안 모니터

Cloud Insights는 ONTAP 시스템에서 FIPS 모드가 비활성화되었음을 감지하면 알림을 표시합니다. 에 대해 자세히 알아보십시오 "시스템 모니터"이 공간을 통해 곧 출시될 보안 모니터를 더 많이 확보할 수 있습니다!

어디서나 채팅할 수 있습니다

새로운 \* 도움말 > 라이브 채팅 \* 링크를 선택하여 Cloud Insights 화면에서 NetApp 지원 전문가와 채팅할 수 있습니다. 도움말은 "?"에서 확인할 수 있습니다. 아이콘을 클릭합니다.



## 보다 가시적인 통찰력

환경에서 가 발생하는 경우 "통찰력" Stress\_or\_Kubernetes Namespaces running of Space \_ 아래의 공유 리소스 등, 이제 영향을 받는 리소스의 자산 랜딩 페이지에는 Insight 자체에 대한 링크가 포함되어 보다 신속한 탐색 및 문제 해결을 제공합니다.

## 새 데이터 수집기

- Amazon S3(Preview에서 사용 가능)
- Brocade FOS 9.0.x
- Dell/EMC PowerStore 3.0.0.0입니다

## 기타 **Data Collector** 업데이트

이제 모든 데이터 소스가 획득 장치 업데이트 및/또는 패치 후 성능 풀링을 재개하도록 최적화되었습니다.

## 운영 체제 지원

Cloud Insights 획득 장치 외에 다음과 같은 운영 체제가 지원됩니다 **"이미 지원됩니다"**:

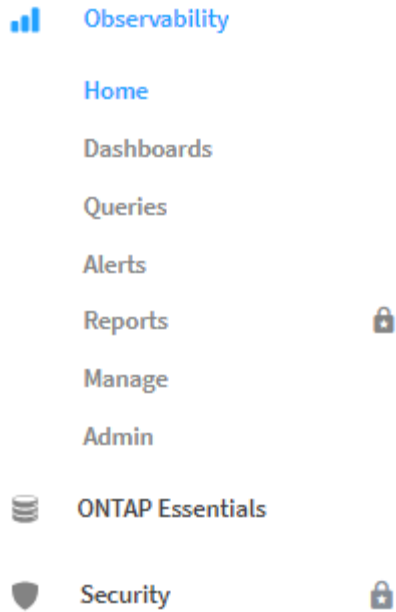
- Red Hat Enterprise Linux 8.5, 8.6

# 2022년 8월

## Cloud Insights의 새로운 디자인!

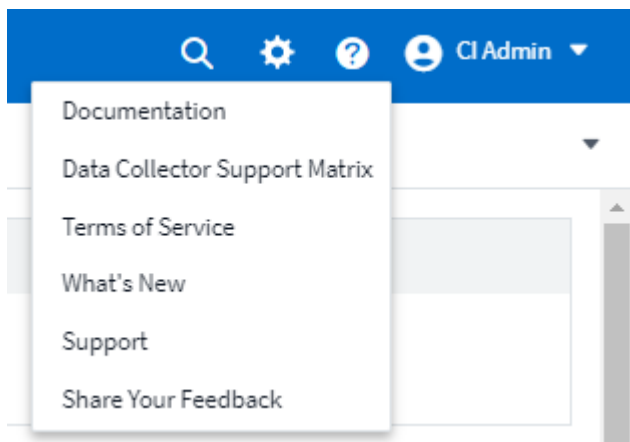
이번 달부터 "모니터링 및 최적화"는 \* 관찰 가능성 \* 으로 이름이 바뀌었습니다. 여기에서 대시보드, 쿼리, 알림 및 보고와 같은 자주 사용하는 기능을 모두 찾을 수 있습니다. 또한 새로운 \* 보안 \* 메뉴에서 Cloud Secure를 찾으십시오. 메뉴만 변경되었으며 기능은 동일하게 유지됩니다.





도움말 \* 메뉴를 찾으십니까?

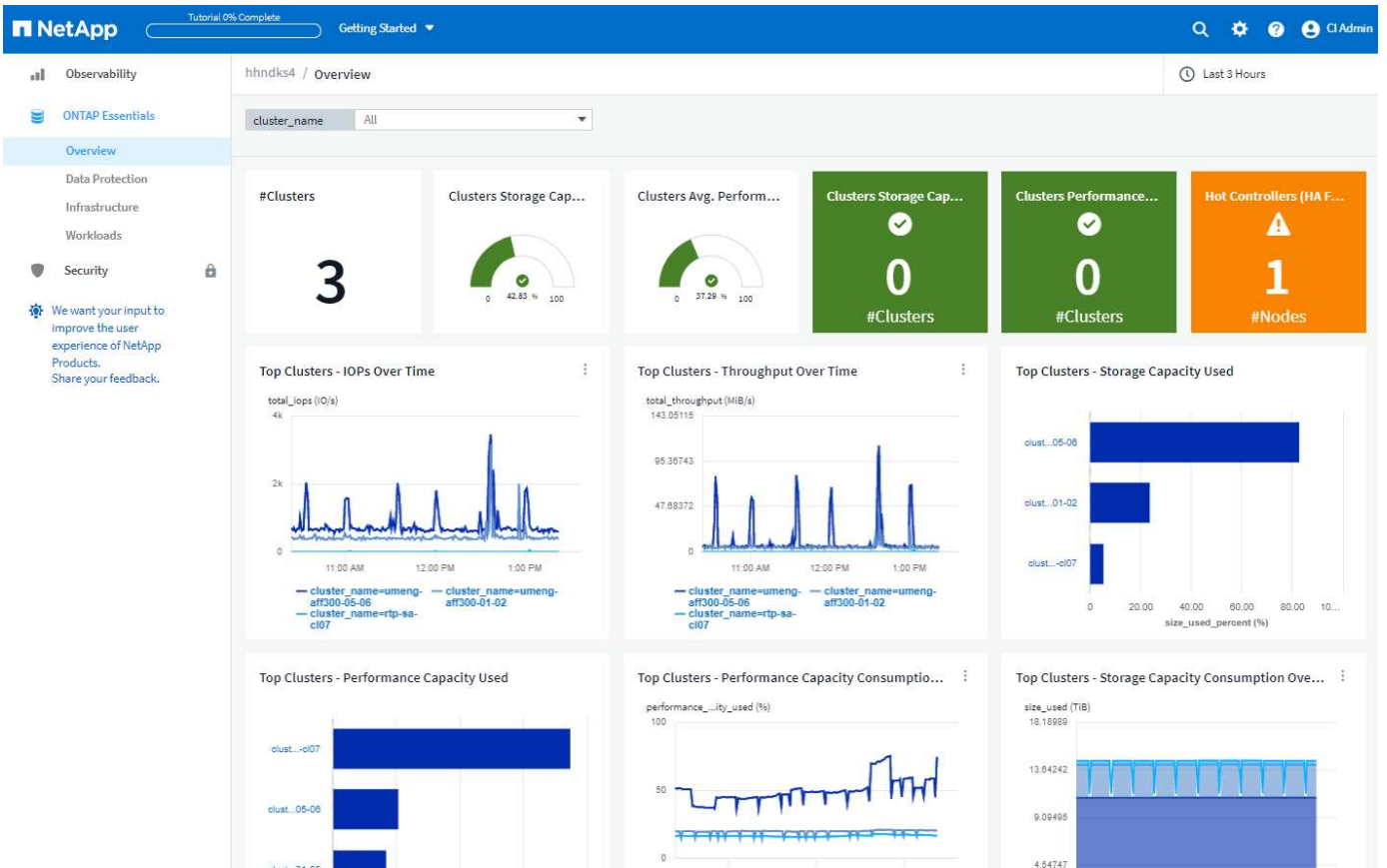
이제 화면 오른쪽 상단에 도움을 받을 수 있습니다.



### 어디서부터 시작해야 할지 잘 모르십니까? **ONTAP** 필수품을 확인해 보세요!

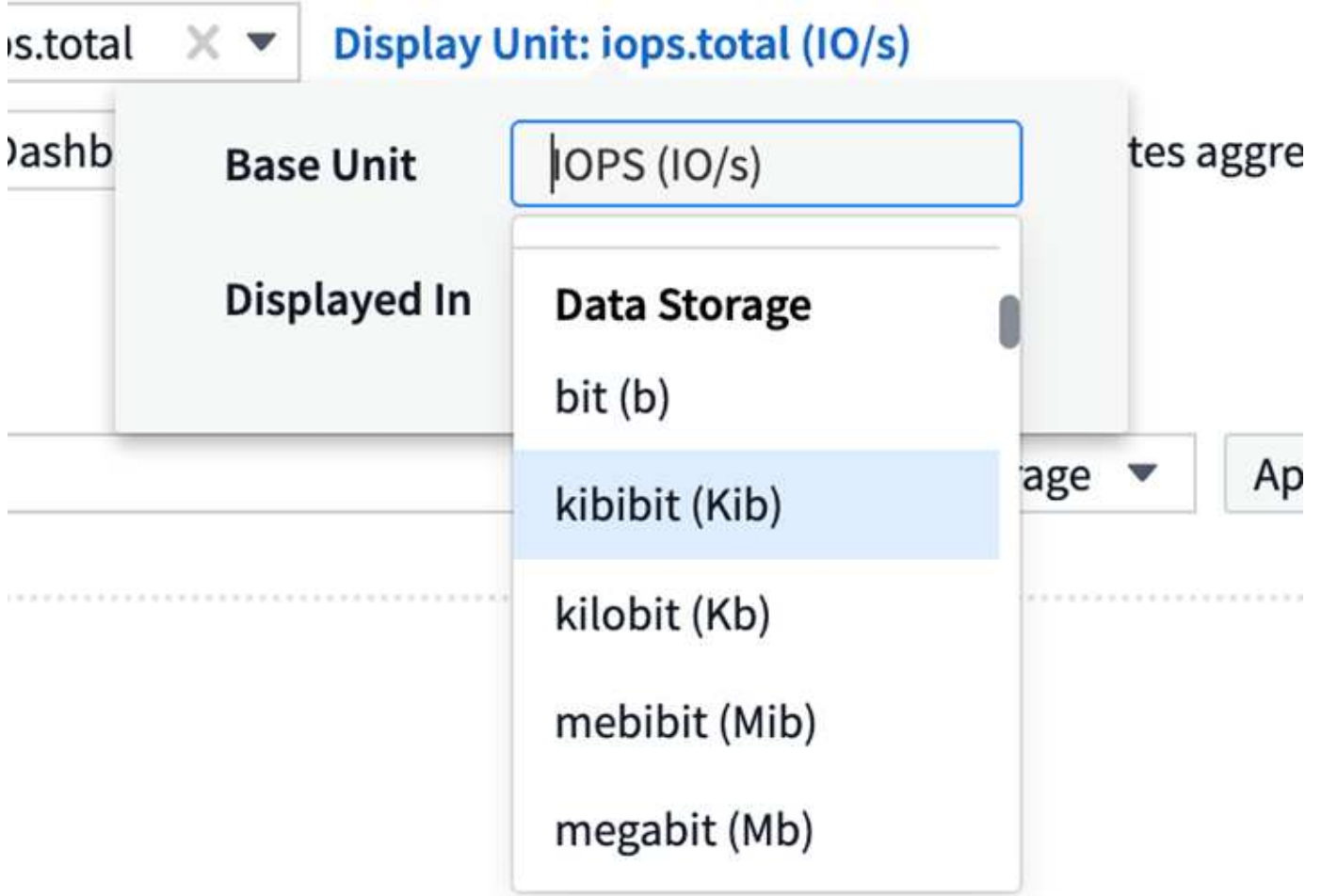
"\* **ONTAP 필수 요소** \*" 는 스토리지 용량 및 성능에 대한 완벽한 예측을 비롯하여 NetApp ONTAP 인벤토리, 워크로드 및 데이터 보호에 대한 자세한 보기를 제공하는 대시보드 및 워크플로우 세트입니다. 높은 활용률로 실행 중인 컨트롤러가 있는지 확인할 수도 있습니다. ONTAP 필수 요소 는 NetApp ONTAP의 모든 모니터링 요구를 충족하는 데 이상적인 장소입니다!

모든 버전에서 제공되는 ONTAP Essentials는 기존 ONTAP 운영자 및 관리자에게 직관적 기능을 제공하도록 설계되어 ActiveIQ Unified Manager에서 서비스 기반 관리 툴로 간편하게 전환할 수 있습니다.



## 스토리지 데이터 제품군이 병합됩니다

여러분이 요청하셨는데, 이제 모든 것이 가능합니다. 이제 스토리지 기본 2 및 기본 10 데이터 유닛이 비트 및 바이트에서 테비비트 및 테라바이트에 이르는 하나의 제품군으로 결합되어 대시보드에 데이터를 쉽게 표시할 수 있습니다. 데이터 전송 속도는 또한 자체 빅 제품군이기도 합니다.



내 스토리지에서 사용하는 전력은 얼마나 됩니까?

NetApp\_ONTAP.storage\_shelf, NetApp\_ONTAP.system\_node, NetApp\_ONTAP.cluster(전력 소비만 해당) 메트릭을 사용하여 ONTAP 스토리지 쉘프 및 노드 전력 소비량, 온도 및 팬 속도를 표시하고 모니터링합니다.

Cloud Insights (Trial) Tutorial 0% Complete Getting Started

diwltk / All Metric Queries / Storage Shelf Last 3 Hours Save

netapp\_ontap.storage\_shelf

Filter By + ?

Group cluster\_name x

2 items found in 2 groups

Table Row Grouping	Expanded Detail	Metrics & Attributes							
cluster_name	netapp_ontap.storage_s...	average_...	power	min_ambient...	min_temperat...	max_temperat...	average_temp...	average_fan_s...	min_fan_spe
rtp-sa-cl06 (1)	1.0	23.00	0.26	23.00	25.00	38.00	30.86	2,997.50	2,970.00
umeng-aff300-01-02 (1)	1.1	27.00	0.15	27.00	30.00	41.00	32.40	2,970.00	2,940.00

## 미리보기에서 점진 피쳐

다음 기능은 미리 보기에서 제외되었으며 현재 모든 고객이 사용할 수 있습니다.

* 피쳐 *	* 설명 *
공간이 부족되는 Kubernetes 네임스페이스	Space Insight에서 실행되는 Kubernetes 네임스페이스를 사용하면 공간이 부족할 위험이 있는 Kubernetes 네임스페이스의 워크로드를 볼 수 있으며 각 공간이 가득 채워지기 전의 남은 일 수에 대한 추정치가 있습니다. <a href="#">"자세히 보기"</a>
스트레스 상태의 공유 리소스	Stress insight 아래의 공유 리소스는 AI/ML을 사용하여 리소스 경합이 사용자 환경에서 성능 저하를 일으키는 위치를 자동으로 식별하고, 해당 환경의 영향을 받는 워크로드를 강조 표시하고, 문제 해결을 위한 권장 조치를 제공하여 성능 문제를 보다 빠르게 해결합니다. <a href="#">"자세히 보기"</a>
Cloud Secure – 공격에 대한 사용자 액세스를 차단합니다	공격이 감지될 때 사용자 액세스를 차단하는 기능을 통해 업무상 중요한 데이터를 더욱 안전하게 보호할 수 있습니다. 자동 응답 정책을 사용하거나 알림 또는 사용자 세부 정보 페이지에서 수동으로 액세스를 차단할 수 있습니다. <a href="#">"자세히 보기"</a>

## 데이터 수집 상태는 어떻습니까?

Cloud Insights는 획득 장치에 대해 2개의 새로운 하트비트 모니터와 데이터 수집기 오류를 경고하는 2개의 모니터를 제공합니다. 이러한 정보는 데이터 수집 문제를 신속하게 경고하는 데 사용할 수 있습니다.

이제 `_Data Collection_monitor` 그룹에서 다음 모니터를 사용할 수 있습니다.

- 획득 장치 하트비트 - 중요
- 획득 장치 하트비트 - 경고
- Collector 실패
- 수집기 경고

이러한 모니터는 기본적으로 `_ 일시 중지됨 _` 상태입니다. 데이터 수집 문제에 대한 알림을 받으려면 이 기능을 활성화하십시오.

## 자동 갱신 API 토큰

이제 API 액세스 토큰을 자동 갱신으로 설정할 수 있습니다. 이 기능을 활성화하면 만료된 토큰에 대해 새/업데이트된 API 액세스 토큰이 자동으로 생성됩니다. 만료 예정인 토큰을 사용하는 Cloud Insights 에이전트는 해당 신규/업데이트된 API 액세스 토큰을 사용하도록 자동으로 업데이트되므로 계속해서 원활하게 작동할 수 있습니다. 토큰을 만들 때 "토큰 자동 갱신" 상자를 선택하기만 하면 됩니다. 이 기능은 현재 Kubernetes 플랫폼에서 최신 NetApp Kubernetes 모니터링 운영자가 있는 Cloud Insights 에이전트에서 지원됩니다.

## Basic Edition은 이전보다 더 많은 기능을 제공합니다

평가판 사용 기간이 종료되었지만 구독이 귀하에게 적합한지 아직 확인할 수 없습니다. Basic Edition에서는 항상 현재

ONTAP 데이터 수집기에서 Cloud Insights를 계속 사용할 수 있지만, 이제 VMware 버전, 토폴로지 및 IOPS/처리량/지연 시간 데이터를 계속 캡처할 수 있습니다. 스토리지 시스템에 대한 프리미엄 지원을 받는 NetApp 고객은 Cloud Insights도 지원할 수 있습니다.

## 자세한 내용을 원하십니까?

도움말 > 지원 페이지의 \* 학습 센터 \* 섹션에서 NetApp University Cloud Insights 과정 오퍼링에 대한 링크를 확인하십시오!

## 운영 체제 지원

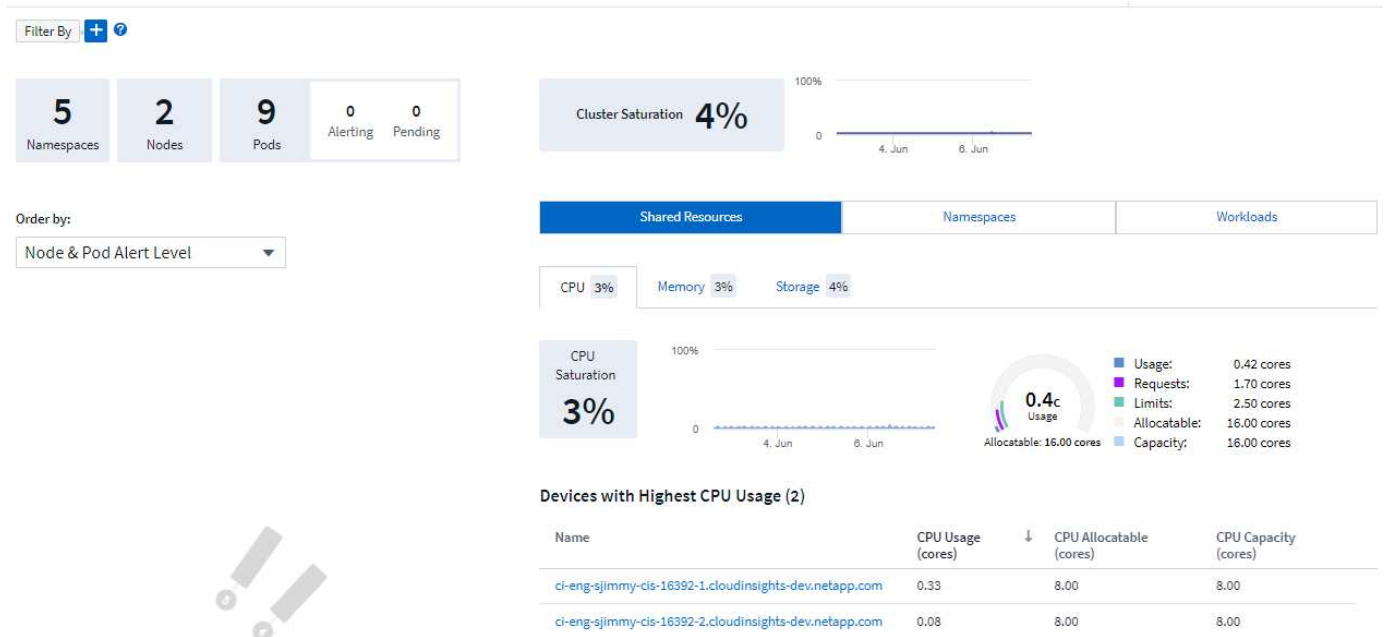
다음 운영 체제는 Cloud Insights 획득 장치 외에 추가로 지원됩니다 **"이미 지원됩니다"**:

- Windows 11

# 2022년 6월

## Kubernetes 클러스터 포화 및 기타 세부 정보

Cloud Insights은 채도 세부 정보와 네임스페이스 및 워크로드에 대한 명확한 뷰를 제공하는 향상된 클러스터 세부 정보 페이지를 통해 Kubernetes 환경을 이전보다 쉽게 탐색할 수 있도록 지원합니다.



또한 클러스터 목록 페이지에서는 노드, Pod, 네임스페이스 및 워크로드 수에 더해 채도를 빠르게 확인할 수 있습니다.

Filter By + ?

Clusters (2)

Name ↑	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setoK3s	4	2	3	4	2	9	5	7

## Kubernetes 클러스터의 사용 중인 지 얼마나 됩니까?

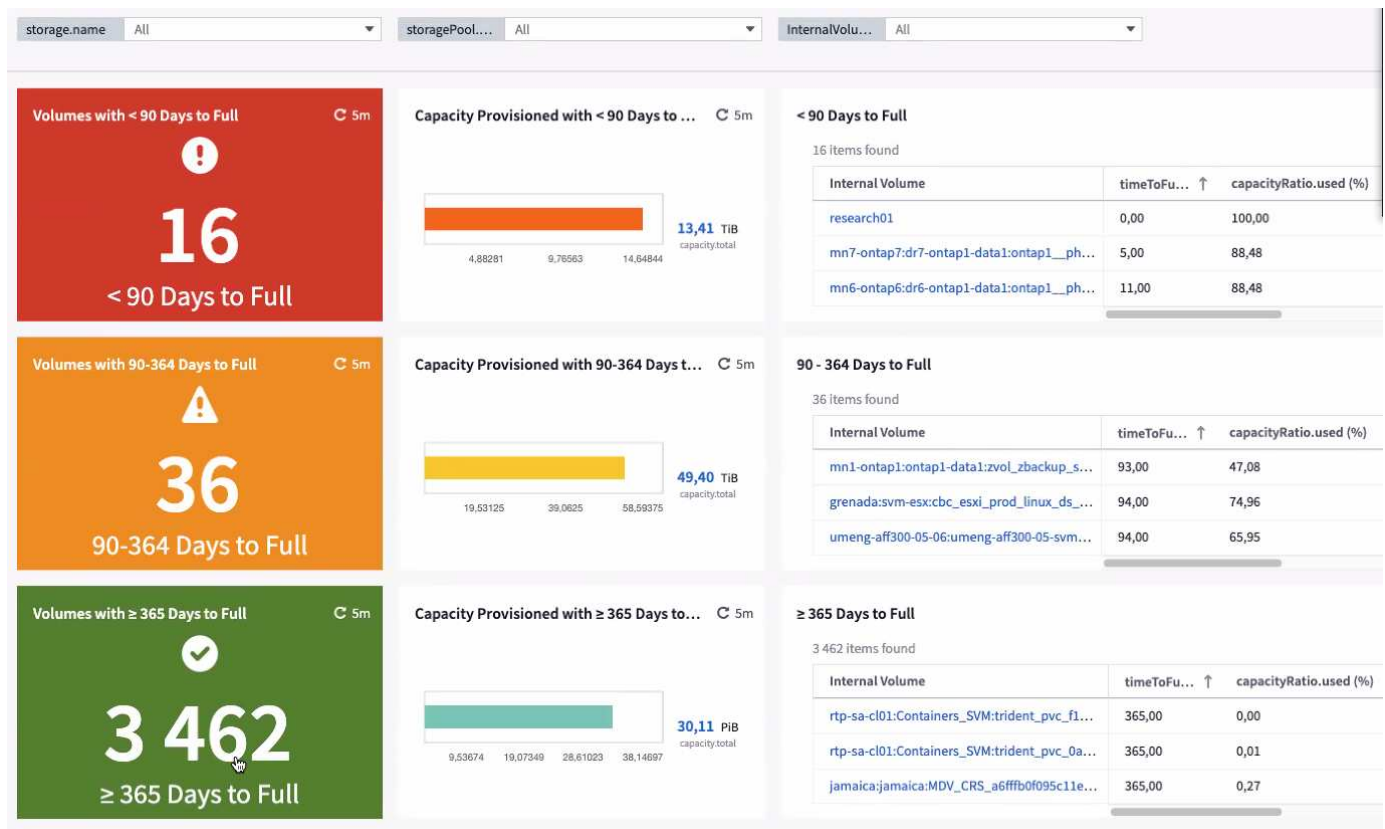
클러스터가 이제 막 시작되었습니까, 아니면 오랜 디지털 수명을 경험했습니까? `_Age_`는 Kubernetes 노드에 대해 수집된 시간 메트릭으로 추가되었습니다.

2 items found in 2 groups

Table Row Grouping	Expanded Detail	Metrics & Attributes
<input type="checkbox"/> node_name ↑	kubernetes_cluster	kubernetes.node
<input type="checkbox"/> ci-aumonitor-1 (1)	aumonitor	ci-aumonitor-1
<input type="checkbox"/> ci-aumonitor-2 (1)	aumonitor	ci-aumonitor-2

## 용량 시간 대 전체 예측

Cloud Insights는 모니터링되는 각 내부 볼륨에 대해 용량이 소진될 때까지 일 수를 예측하는 대시보드를 제공합니다. 이러한 가치는 중단 위험을 크게 줄이는 데 도움이 될 수 있습니다.

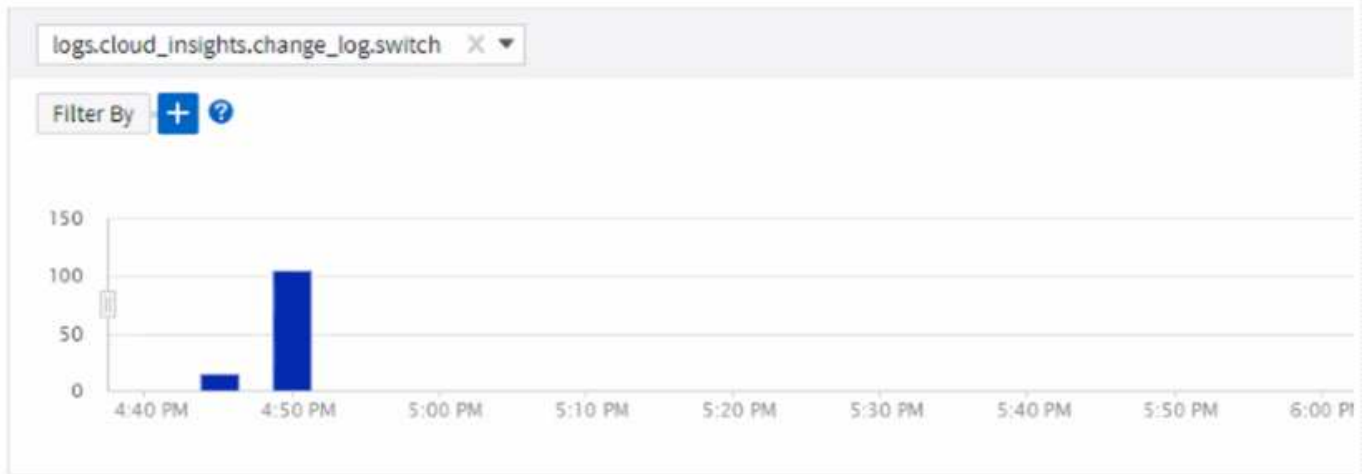


TTF 카운터는 스토리지, 스토리지 풀 및 볼륨에도 사용할 수 있습니다. 이러한 객체에 대한 추가 대시보드가 필요하면 이 공간을 계속 주시하십시오.

전체 예상 소요 시간이 \_Preview\_ 에서 벗어났고 모든 고객에게 돌아옵니다.

## 내 환경에서 변경된 사항은 무엇입니까?

ONTAP 변경 로그 항목은 로그 탐색기에서 볼 수 있습니다.



### Log Entries

timestamp ↓	name	object_type	message
06/08/2022 4:52:51 PM	<a href="#">fc19</a>	Port	Port with name:fc19 has been created
06/08/2022 4:52:51 PM	<a href="#">fc20</a>	Port	Port with name:fc20 has been created
06/08/2022 4:52:51 PM	<a href="#">fc23</a>	Port	Port with name:fc23 has been created
06/08/2022 4:52:51 PM	<a href="#">fc22</a>	Port	Port with name:fc22 has been created

## 운영 체제 지원

Cloud Insights 획득 장치 외에 다음과 같은 운영 체제가 지원됩니다 ["이미 지원됩니다"](#):

- CentOS 스트림 9
- Windows 2022

## Telegraf 에이전트를 업데이트했습니다

Telegraf 통합 데이터 수집용 에이전트가 버전 \* 1.22.3 \* 으로 업데이트되어 성능 및 보안이 향상되었습니다. 업데이트를 원하는 사용자는 의 해당 업그레이드 섹션을 참조할 수 있습니다 ["Agent 설치"](#) 문서화: 이전 버전의 에이전트는 사용자 작업 없이 계속 작동합니다.

## 피처 미리보기

Cloud Insights는 다양하고 흥미로운 새로운 미리 보기 기능을 정기적으로 강조하고 있습니다. 이러한 기능 중 하나 이상을 미리 보려면 에 문의하십시오 ["NetApp 세일즈 팀"](#) 를 참조하십시오.

* 피처 *	* 설명 *
공간이 부족되는 Kubernetes 네임스페이스	Space Insight에서 실행되는 _Kubernetes 네임스페이스를 사용하면 공간이 부족할 위험이 있는 Kubernetes 네임스페이스의 워크로드를 볼 수 있으며 각 공간이 가득 채워지기 전의 남은 일 수에 대한 추정치가 있습니다. <a href="#">"자세히 보기"</a>
Cloud Secure – 공격에 대한 사용자 액세스를 차단합니다	공격이 감지될 때 사용자 액세스를 차단하는 기능을 통해 업무상 중요한 데이터를 더욱 안전하게 보호할 수 있습니다. 자동 응답 정책을 사용하거나 알림 또는 사용자 세부 정보 페이지에서 수동으로 액세스를 차단할 수 있습니다. <a href="#">"자세히 보기"</a>
스트레스 상태의 공유 리소스	Stress Insight 아래의 _공유 리소스는 AI/ML을 사용하여 리소스 경합이 사용자 환경에서 성능 저하를 일으키는 위치를 자동으로 식별하고, 해당 환경의 영향을 받는 워크로드를 강조 표시하고, 문제 해결을 위한 권장 조치를 제공하여 성능 문제를 보다 빠르게 해결합니다. <a href="#">"자세히 보기"</a>

## 2022년 5월

### NetApp Support와 실시간 채팅

이제 NetApp 지원 담당자와 실시간으로 채팅할 수 있습니다. 도움말 > 지원 페이지에서 채팅 아이콘을 클릭하거나 "연락처" 섹션에서 \_Chat\_를 클릭하여 채팅 세션을 시작합니다. Standard 및 Premium Edition 사용자의 경우 채팅 지원은 미국 평일에 제공됩니다.



### Kubernetes 운영자

Cloud Insights의 고급 Kubernetes 모니터링 및 클러스터 탐색기를 사용하여 쉽게 시작 및 실행할 수 있습니다.

를 클릭합니다 ["Kubernetes 모니터링 운영자"](#) (NKMO)는 Cloud Insights Insights를 위한 Kubernetes를 설치하는 데 권장되는 방법입니다. 더 적은 수의 단계로 보다 유연하게 모니터링을 구성할 수 있을 뿐만 아니라 K8s 클러스터에서 실행 중인 다른 소프트웨어를 모니터링할 수 있는 기회도 더 많아집니다.

자세한 정보와 사전 요구 사항을 보려면 위의 링크를 클릭하십시오

### API를 사용하여 사용자 및 초대 관리

이제 Cloud Insights의 강력한 API를 사용하여 사용자 및 초대를 관리할 수 있습니다. 자세한 내용은 [API Swagger 문서](#)를 참조하십시오.



## 데이터 수집 경고

Collector 실패로 인해 중요한 메트릭을 놓치지 마십시오!

새로운 을 사용하면 데이터 수집기를 훨씬 쉽게 추적할 수 있습니다 "경고" 데이터 수집기 및 획득 장치 고장입니다. 이러한 모니터는 기본적으로 \_일시 중지됨\_입니다. 활성화하려면 모니터 페이지로 이동하여 "획득 장치 종료" 및 "수집기 실패"를 찾아서 재개합니다.

## ONTAP 스토리지 변경 사항에 대한 알림을 표시합니다

예기치 않은 스토리지 변경으로 인해 운영 중단이 발생하는 것을 방지할 수 있습니다.

이제 ONTAP 시스템에서 FlexVols, 노드 및 SVM의 수정 또는 제거가 감지될 때 Cloud Insights를 구성할 수 있습니다.

## 피처 미리보기

Cloud Insights는 다양하고 흥미로운 새로운 미리 보기 기능을 정기적으로 강조하고 있습니다. 이러한 기능 중 하나 이상을 미리 보려면 에 문의하십시오 "NetApp 세일즈 팀" 를 참조하십시오.

* 피처 *	* 설명 *
공간이 부족되는 Kubernetes 네임스페이스	Space_Insight에서 실행되는 _Kubernetes 네임스페이스를 사용하면 공간이 부족할 위험이 있는 Kubernetes 네임스페이스의 워크로드를 볼 수 있으며 각 공간이 가득 채워지기 전의 남은 일 수에 대한 추정치가 있습니다. <a href="#">"자세히 보기"</a>
내부 볼륨 및 볼륨 용량 시간 대 전체 예측	Cloud Insights는 각 내부 볼륨 및 모니터링되는 볼륨에 대한 용량이 소진될 때까지 일 수를 늘릴 수 있습니다. 이 값은 운영 중단의 위험을 크게 줄이는 데 도움이 될 수 있습니다.
Cloud Secure – 공격에 대한 사용자 액세스를 차단합니다	공격이 감지될 때 사용자 액세스를 차단하는 기능을 통해 업무상 중요한 데이터를 더욱 안전하게 보호할 수 있습니다. 자동 응답 정책을 사용하거나 알림 또는 사용자 세부 정보 페이지에서 수동으로 액세스를 차단할 수 있습니다. <a href="#">"자세히 보기"</a>
스트레스 상태의 공유 리소스	Stress_insight 아래의 _공유 리소스는 AI/ML을 사용하여 리소스 경합이 사용자 환경에서 성능 저하를 일으키는 위치를 자동으로 식별하고, 해당 환경의 영향을 받는 워크로드를 강조 표시하고, 문제 해결을 위한 권장 조치를 제공하여 성능 문제를 보다 빠르게 해결합니다. <a href="#">"자세히 보기"</a>

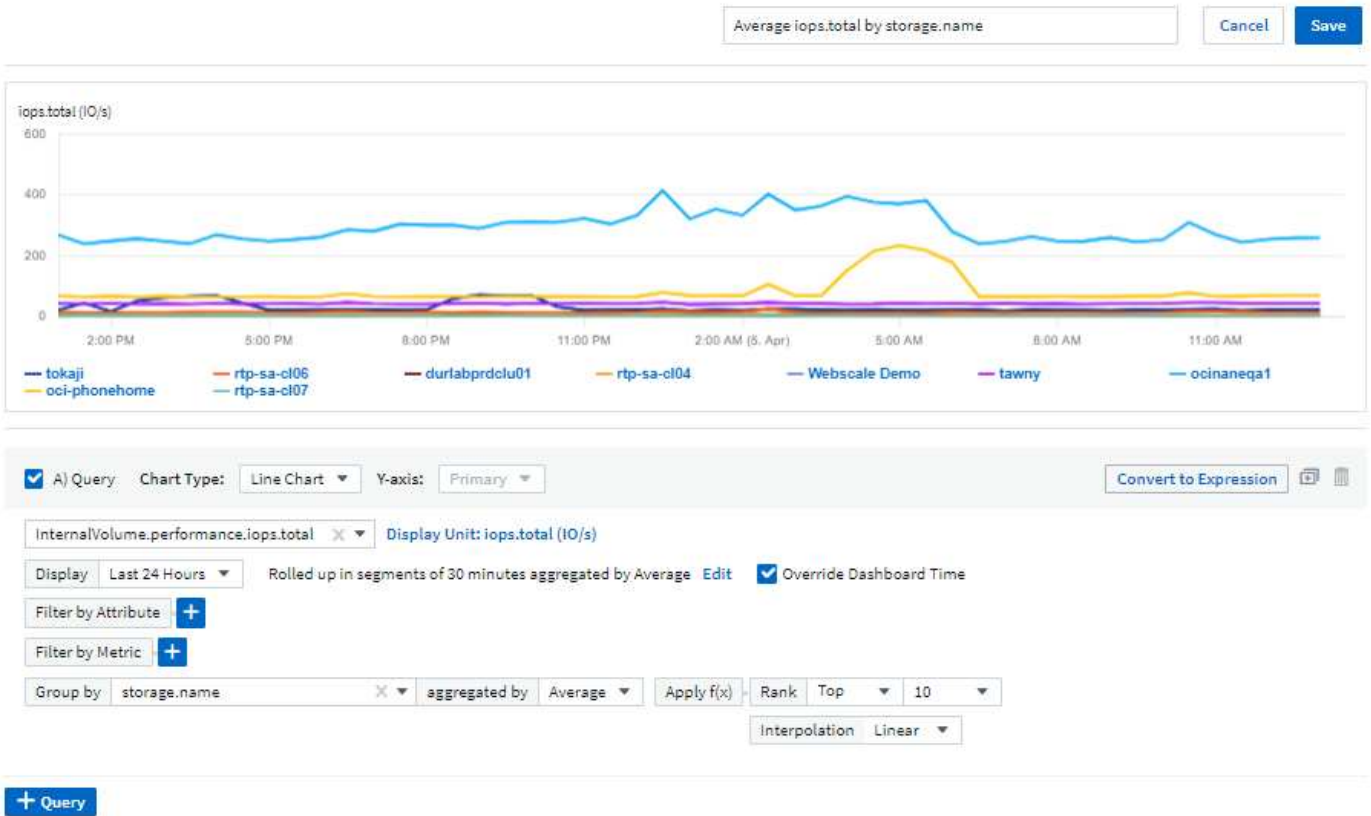
## 2022년 4월

귀하의 의견을 공유해 주십시오!

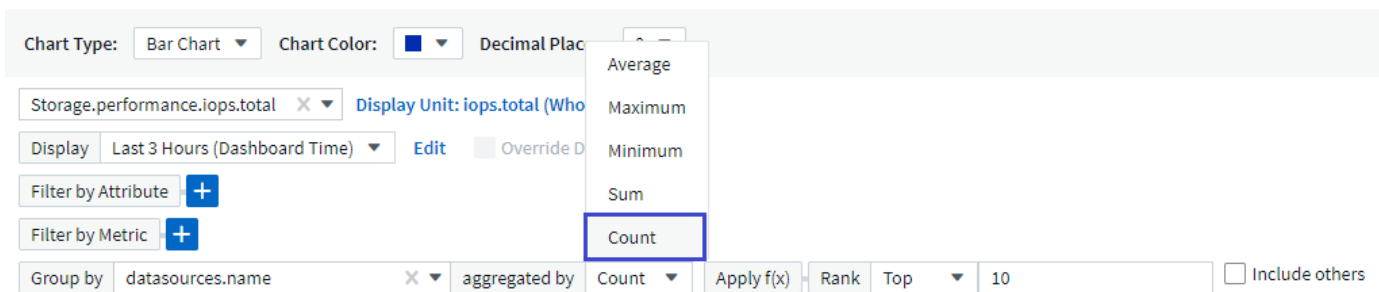
Cloud Insights를 형성하는 데 도움이 되는 정보를 제공해 주십시오. NetApp의 \* Insights to Action \* 프로그램에 참여하시면 포인트와 상품을 드립니다. **"\* 지금 등록하십시오 \*"**

## 업데이트된 대시보드 편집기

대시보드 생성 도구를 더욱 쉽게 데이터를 보다 빠르게 시각화할 수 있도록 개편했습니다. Cloud Insights의 "대시보드" 페이지로 이동하여 기존 대시보드를 편집하거나 대시보드 갤러리에서 대시보드를 추가하거나 자신의 대시보드를 새로 만들어 확인할 수 있습니다.



새로운 Count 집계 메서드도 도입되었습니다. 가로 막대형 차트, 세로 막대형 차트 및 원형 차트 위젯에서 데이터를 그룹화하면 선택한 메트릭에 대한 관련 개체의 수를 쉽고 빠르게 표시할 수 있습니다.



또한 꺾은선형 차트를 사용하여 세 가지 중 하나를 선택할 수 있습니다 "보간" 방법:

- 없음 - 보간이 수행되지 않습니다
- 선형 - 기존 점 사이의 데이터 점을 보간합니다
- 계단 - 이전 데이터 지점을 보간된 데이터 지점으로 사용합니다

## Kubernetes Infrastructure에 대한 모니터링 개선

Cloud Insights는 Pod, 데모 세트, 복제 및 복제를 생성 또는 제거할 때와 새 구축이 생성될 때 알림을 보내 Kubernetes 환경의 변경 사항을 계속 파악할 수 있습니다. Kubernetes에서는 기본적으로 `_paused_state` 가 모니터링되므로 필요한 특정 상태만 사용하도록 설정해야 합니다.

### 피처 미리보기

Cloud Insights는 다양하고 흥미로운 새로운 미리 보기 기능을 정기적으로 강조하고 있습니다. 이러한 기능 중 하나 이상을 미리 보려면 에 문의하십시오 "[NetApp 세일즈 팀](#)" 를 참조하십시오.

* 피처 *	* 설명 *
내부 볼륨 및 볼륨 용량 시간 대 전체 예측	Cloud Insights는 각 내부 볼륨 및 모니터링되는 볼륨에 대한 용량이 소진될 때까지 일 수를 늘릴 수 있습니다. 이 값은 운영 중단 위험을 크게 줄이는 데 도움이 될 수 있습니다.
Cloud Secure – 공격에 대한 사용자 액세스를 차단합니다	공격이 감지될 때 사용자 액세스를 차단하는 기능을 통해 업무상 중요한 데이터를 더욱 안전하게 보호할 수 있습니다. 자동 응답 정책을 사용하거나 알림 또는 사용자 세부 정보 페이지에서 수동으로 액세스를 차단할 수 있습니다. " <a href="#">자세히 보기</a> "
스트레스 상태의 공유 리소스	스트레스 분석 아래의 공유 리소스는 AI/ML을 사용하여 리소스 경합이 사용자 환경에서 성능 저하를 일으키는 위치를 자동으로 식별하고, 해당 환경의 영향을 받는 워크로드를 강조 표시하고, 문제 해결을 위한 권장 조치를 제공하여 성능 문제를 보다 신속하게 해결합니다. " <a href="#">자세히 보기</a> "

### 새 데이터 수집기

- \* Cohesity SmartFiles \* - 이 REST API 기반 수집기는 Cohesity 클러스터를 획득하여 "뷰"(CI 내부 볼륨)와 다양한 노드를 검색하고 성능 메트릭을 수집합니다.

### 기타 Data Collector 업데이트

다음 데이터 수집기에서 성능 데이터의 수집 및 표시가 향상되었습니다.

- Brocade CLI를 사용합니다
- Dell/EMC VPLEX, PowerStore, Isilon/PowerScale, VNX Block/CLARiX CLI, XtremIO, Unity/VNXe
- Pure FlashArray입니다

이러한 성능 향상 기능은 VMware 및 Cisco와 모든 NetApp 데이터 수집기에서 이미 제공되며 향후 몇 개월 동안 다른 모든 데이터 수집기에 제공될 예정입니다.

# 2022년 3월

## ONTAP 9.9+용 클라우드 연결

를 클릭합니다 "ONTAP 9.9 이상을 위한 NetApp 클라우드 연결" 데이터 수집기는 외부 수집 장치를 설치할 필요가 없으므로 문제 해결, 유지 관리 및 초기 배포를 간소화할 수 있습니다.

## NetApp ONTAP 모니터를 위한 새로운 FSx

새로운 를 사용하면 NetApp ONTAP 환경을 위한 FSx를 쉽게 모니터링할 수 있습니다 "시스템 정의 모니터" 인프라 (메트릭)와 워크로드(로그) 모두에 대해

FSX Infrastructure (1)		<a href="#">+ Monitor</a>	Bulk Actions ▾	Filter...	
<input type="checkbox"/>	Name	Metric / Parameters	Severity	Time Frame	Status
<input type="checkbox"/>	FSx Volume Cache Miss Ratio	netapp_ontap.workload_volume.cache_miss_ratio	⚠ Warning @ > 95 % 🚨 Critical @ > 100 %	For 30 minutes	⏸ Paused

FSX Workload Examples (5)		<a href="#">+ Monitor</a>	Bulk Actions ▾	Filter...	
<input type="checkbox"/>	Name	Metric / Parameters	Severity	Time Frame	Status
<input type="checkbox"/>	FSx Snapshot Reserve Space is Full	netapp_ontap.workload_volume.snapshot_size_used_percent	⚠ Warning @ > 90 % 🚨 Critical @ > 95 %	Once	⏸ Paused
<input type="checkbox"/>	FSx Volume Capacity is Full	netapp_ontap.workload_volume.size_used_percent	⚠ Warning @ > 85 % 🚨 Critical @ > 95 %	Once	⏸ Paused
<input type="checkbox"/>	FSx Volume High Latency	netapp_ontap.workload_volume.total_latency	⚠ Warning @ > 1,000 μs 🚨 Critical @ > 2,000 μs	For 5 minutes	⏸ Paused
<input type="checkbox"/>	FSx Volume Inodes Limit	netapp_ontap.workload_volume.inodes_used_percent	⚠ Warning @ > 85 % 🚨 Critical @ > 95 %	Once	⏸ Paused
<input type="checkbox"/>	FSx Volume Qtree Quota Overcommit	netapp_ontap.workload_volume.qtree_quota_commit_percent	⚠ Warning @ > 95 % 🚨 Critical @ > 100 %	Once	⏸ Paused

## 새로운 Cloud Secure 기능을 모두 사용할 수 있습니다

다음과 같은 Cloud Secure 기능을 통해 이전보다 훨씬 더 안전한 환경을 구현할 수 있습니다.

* 피처 *	* 설명 *
데이터 삭제 - 파일 삭제 공격 탐지	비정상적인 대규모 파일 삭제 작업을 감지하고, 악의적인 사용자의 악의적인 파일 액세스를 차단하고, 자동 응답 정책을 통해 자동 스냅샷을 생성합니다.
경고 및 경고에 대한 별도의 알림	경고 및 경고 알림을 별도의 수신자에게 전송하여 올바른 팀이 정보를 계속 받을 수 있도록 합니다

## Telegraf 에이전트를 업데이트했습니다

Telegraf 통합 데이터 수집용 에이전트가 성능 및 보안 향상을 통해 버전 \* 1.21.2 \* 로 업데이트되었습니다. 업데이트를 원하는 사용자는 의 해당 업그레이드 섹션을 참조할 수 있습니다 "Agent 설치" 문서화: 이전 버전의 에이전트는 사용자 작업 없이 계속 작동합니다.

## Data Collector 업데이트

- Broadcom Fibre Channel 스위치 데이터 수집기는 각 인벤토리 폴링에서 실행되는 CLI 명령 수를 줄이도록 최적화되었습니다.
- 

## 2022년 2월

### Cloud Insights는 Apache log4j 취약점을 해결합니다

고객 보안은 NetApp의 최우선 과제입니다. Cloud Insights는 최신 Apache log4j 취약점을 해결하기 위한 소프트웨어 라이브러리 업데이트를 포함합니다.

NetApp 제품 보안 권고 웹 사이트에서 다음을 참조하십시오.

["CVE-2021-44228"](#)

["CVE-2021-45046"](#)

["CVE-2021-45105"](#)

취약성 및 NetApp의 대응 방법은 [에서](#) 자세히 알아볼 수 있습니다 ["NetApp 뉴스룸"](#).

### Kubernetes 네임스페이스 세부 정보 페이지

이제 클러스터의 네임스페이스에 대한 정보 상세 페이지를 통해 Kubernetes 환경을 이전보다 효율적으로 탐색할 수 있습니다. 네임스페이스 세부 정보 페이지는 모든 백엔드 스토리지 리소스 및 용량 사용률을 포함하여 네임스페이스에서 사용되는 모든 자산에 대한 요약を提供합니다.

Filter By + ?

5  
Pods

2  
Healthy

3  
Alerting

3  
Pending

Status  
Active

Labels  
-

Resource Quotas  
2

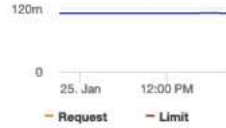
1,016mc  
CPU



Highest CPU Demand by Pod

998.69m	folding-at-home-16353...
17.02m	db-backup-85447c7767...

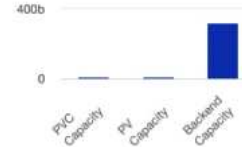
0.1GiB  
Memory



Highest Memory Demand by Pod

0.1 GiB	folding-at-home-16353...
<0.01 GiB	db-backup-85447c776...

0.78GiB  
Total PVC Capacity claimed



Highest Storage Demand by PVC

0.39 GiB	nfs2
0.39 GiB	nfs

#### Storage (2)

persistentvolumeclaim ↑	persistentvolume	pv_type	backend	backend_capacity_total_bytes (GiB)	backend_capacity_us
nfs	nfs	NFS	-		
nfs2	nfs2	NFS	tokaji:tokaji_svm_vvol_nfs:tokaji_svm_k n_ops	300 GiB	35.49 GiB

#### Workloads (3)

owner_name ↑	owner_kind	cpu_usage_nanocores (mcores)	kube_pod_container_resource_requests_memory_bytes (GiB)
db-backup	Deployment	17 mc	0.68 GiB
db-workload	Deployment		1.46 GiB
folding-at-home-1635372863	Deployment	999 mc	0.13 GiB

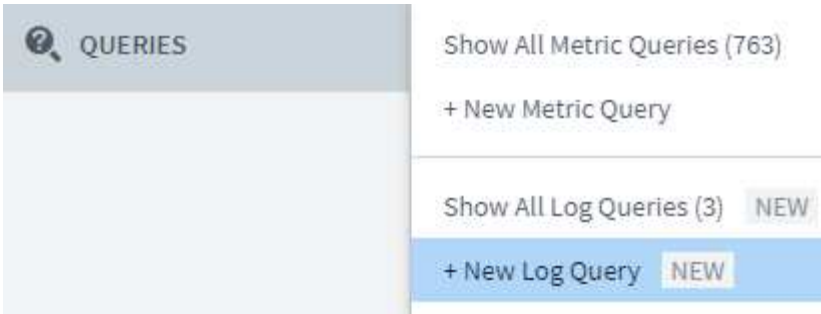
## 2021년 12월

### ONTAP 시스템을 위한 더욱 긴밀한 통합

NetApp 이벤트 관리 시스템(EMS)과의 새로운 통합으로 ONTAP 하드웨어 장애에 대한 알림을 더욱 간편하게 제공합니다. "탐색 및 경고" Cloud Insights의 낮은 수준의 ONTAP 메시지를 통해 문제 해결 워크플로우를 알리고 개선하고 ONTAP 요소 관리 툴링에 대한 의존도를 더욱 줄입니다.

### 로그를 쿼리하는 중입니다

ONTAP 시스템의 경우 Cloud Insights 쿼리에는 강력한 기능이 포함되어 있습니다. "로그 탐색기" EMS 로그 항목을 쉽게 조사하고 문제를 해결할 수 있습니다.



## Data Collector 레벨 알림입니다.

경고용 시스템 정의 및 사용자 정의 생성 모니터 외에도 ONTAP 데이터 수집기에 대한 알림 알림을 설정할 수 있으므로 다른 모니터 경고와 상관없이 수집기 레벨 알림에 대한 수신자를 지정할 수 있습니다.

## Cloud Secure 역할의 유연성 향상

에 따라 사용자에게 Cloud Secure 기능에 대한 액세스 권한을 부여할 수 있습니다 "역할" 관리자가 설정:

역할	Cloud Secure 액세스
관리자	알림, Forensics, 데이터 수집기, 자동화된 응답 정책 및 Cloud Secure용 API를 비롯한 모든 Cloud Secure 기능을 수행할 수 있습니다. 관리자는 다른 사용자를 초대할 수도 있지만 Cloud Secure 역할만 할당할 수 있습니다.
사용자	알림을 확인 및 관리하고 Forensics를 볼 수 있습니다. 사용자 역할은 알림 상태를 변경하고, 메모를 추가하고, 스냅샷을 수동으로 생성하고, 사용자 액세스를 차단할 수 있습니다.
게스트	알림 및 Forensics를 볼 수 있습니다. 게스트 역할은 알림 상태를 변경하거나, 메모를 추가하거나, 스냅샷을 수동으로 생성하거나, 사용자 액세스를 차단할 수 없습니다.

## 운영 체제 지원

CentOS 8.x 지원은 \* CentOS 8 Stream \* 지원으로 대체됩니다. CentOS 8.x는 2021년 12월 31일에 생산이 종료됩니다.

## Data Collector 업데이트

공급업체 변경 사항을 반영하기 위해 여러 Cloud Insights 데이터 수집기 이름이 추가되었습니다.

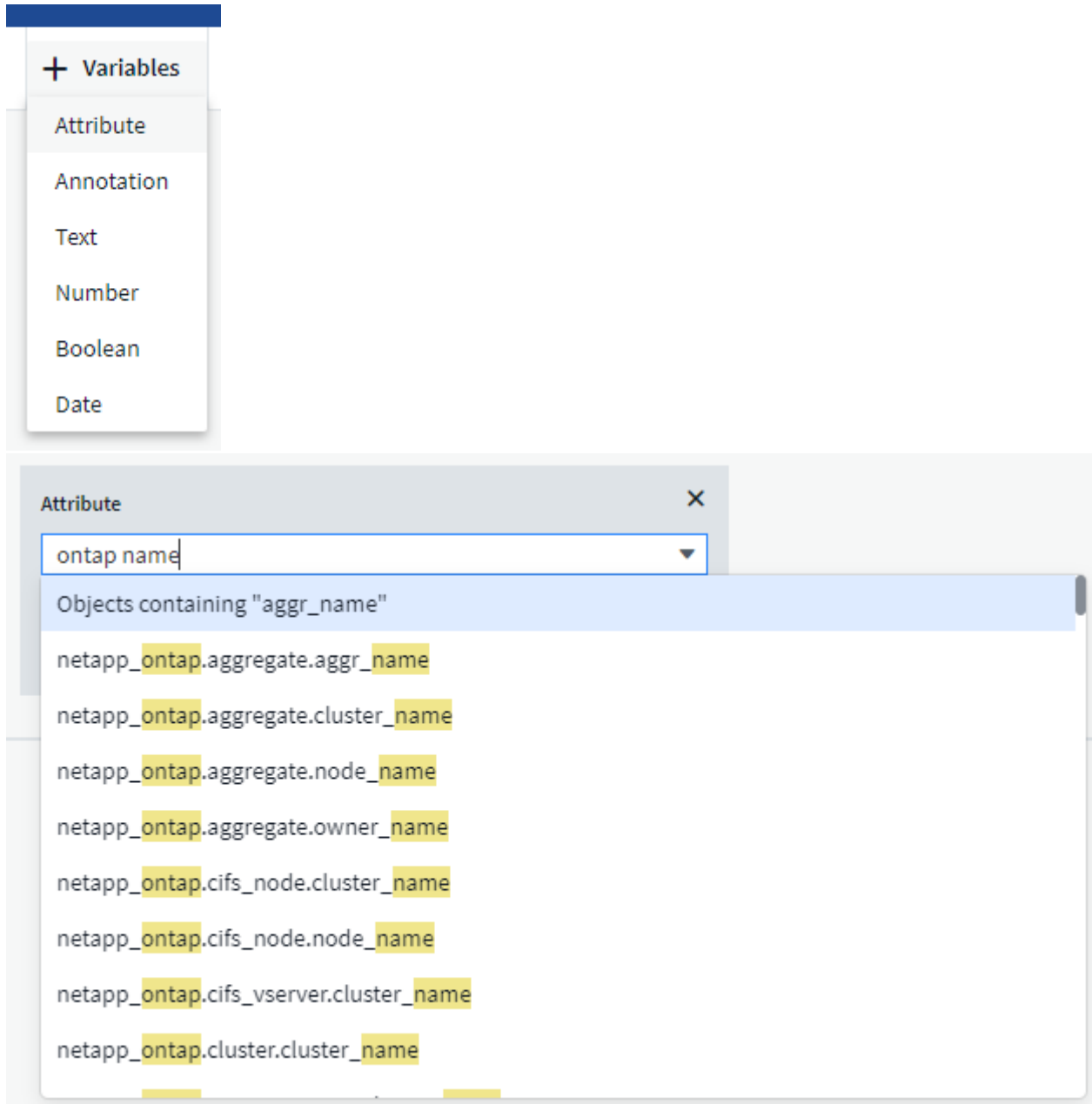
공급업체/모델	이전 이름
Dell EMC PowerScale	Isilon
HPE Alletra 9000/Primera	3PAR입니다
HPE Alletra 6000	민첩성

# 2021년 11월

## Adaptive 대시보드

\_위젯에서 변수를 사용하는 기능과 속성에 대한 새 변수.

이제 대시보드는 그 어느 때보다 강력하고 유연해졌습니다. 속성 변수가 포함된 적응형 대시보드를 구축하여 대시보드를 즉시 빠르게 필터링할 수 있습니다. 기존 및 기타 기존 구성 요소 사용 "변수" 이제 하나의 상위 레벨 대시보드를 생성하여 전체 환경에 대한 메트릭을 확인하고 리소스 이름, 유형, 위치 등을 기준으로 완벽하게 필터링할 수 있습니다. 위젯에서 숫자 변수를 사용하여 원시 메트릭과 비용(예: 서비스형 스토리지의 경우 GB당 비용)을 연결합니다.



## API를 통해 보고 데이터베이스에 액세스합니다

타사 보고, ITSM 및 자동화 통과와 통합을 위한 향상된 기능: Cloud Insights의 강력한 기능 ["API를 참조하십시오"](#) 사용자가 Cognos 보고 환경을 거치지 않고 Cloud Insights 보고 데이터베이스를 직접 쿼리할 수 있습니다.



## VM 랜딩 페이지의 POD 테이블

VM과 Kubernetes Pod를 원활하게 탐색할 수 있습니다. 향상된 문제 해결 및 성능 여유 공간 관리를 위해 관련 Kubernetes Pod 테이블이 VM 랜딩 페이지에 표시됩니다.

Kubernetes Pods 5m

15 items found

pod_name ↑	kubernetes_cluster	namespace	owner_kind	owner_name
calico-kube-controllers-649b7b795b-kt2n	ci-rancher	kube-system	ReplicaSet	calico-kube-controllers-649b7b795b
canal-mpvix	ci-rancher	kube-system	DaemonSet	canal
cattle-cluster-agent-74c7797cc5-b9jhz	ci-rancher	cattle-system	ReplicaSet	cattle-cluster-agent-74c7797cc5
cattle-node-agent-bn225	ci-rancher	cattle-system	DaemonSet	cattle-node-agent
coredns-autoscaler-79599b9dc6-dtwpj	ci-rancher	kube-system	ReplicaSet	coredns-autoscaler-79599b9dc6

## Data Collector 업데이트

- 이제 ECS가 스토리지 및 노드에 대한 펌웨어를 보고합니다
- Isilon은 신속한 검색을 개선했습니다
- Azure NetApp Files는 성능 데이터를 더 빠르게 수집합니다
- StorageGRID에서 SSO(Single Sign-On) 지원
- Brocade CLI가 X 및 -4 모델을 올바르게 보고합니다

## 추가 운영 체제가 지원됩니다

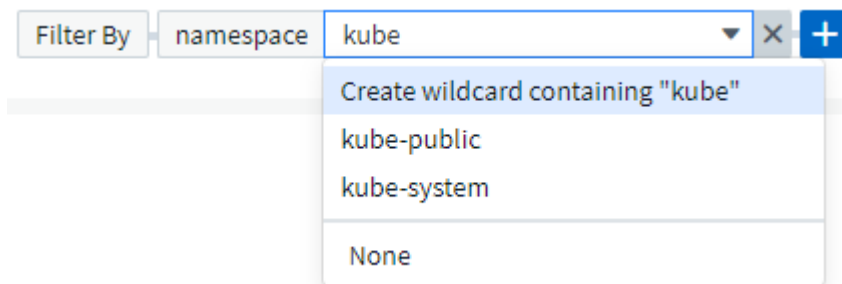
Cloud Insights 획득 장치는 이미 지원되는 운영 체제 외에도 다음과 같은 운영 체제를 지원합니다.

- CentOS(64비트) 8.4
- Oracle Enterprise Linux(64비트) 8.4
- Red Hat Enterprise Linux(64비트) 8.4

## 2021년 10월

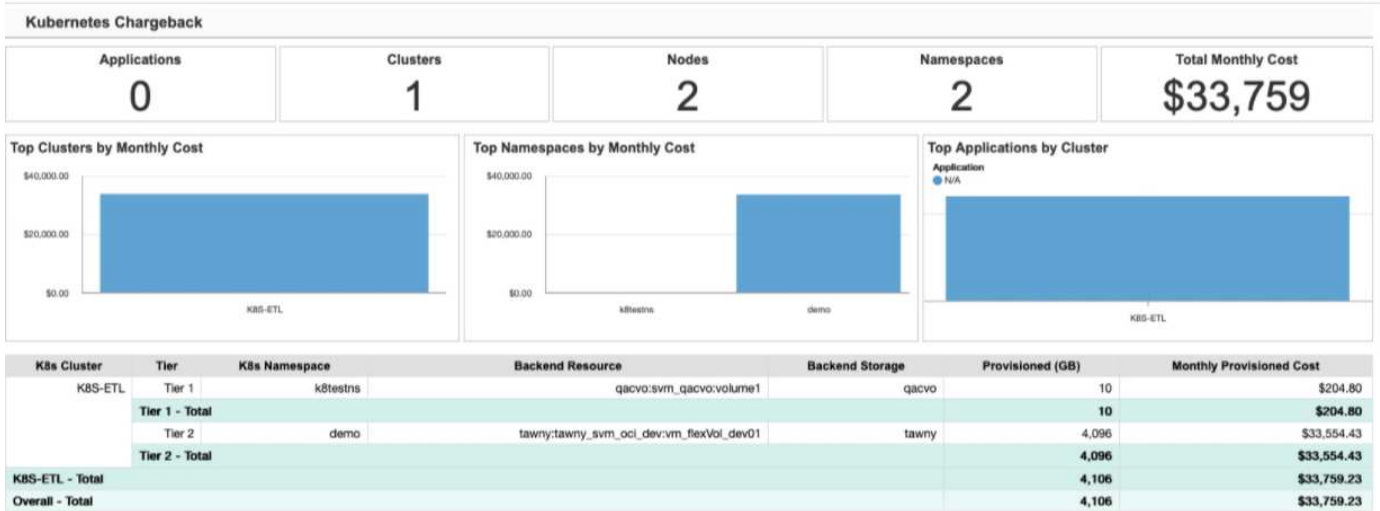
### K8S 탐색기 페이지의 필터

"Kubernetes 탐색기" 페이지 필터를 사용하면 Kubernetes 클러스터, 노드 및 포드 탐색에 대해 표시되는 데이터를 집중적으로 제어할 수 있습니다.



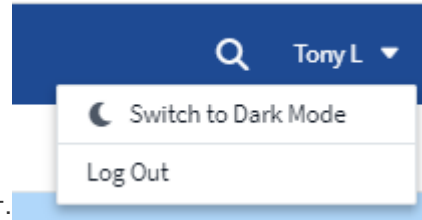
## 보고를 위한 K8s 데이터

이제 Kubernetes 데이터를 Reporting에서 사용할 수 있으므로 비용 청구 또는 기타 보고서를 생성할 수 있습니다. Kubernetes 차지백 데이터를 리포팅으로 전달하려면 Kubernetes 클러스터 및 해당 백 엔드 스토리지로부터 데이터를 받고 Cloud Insights에 연결되어 있어야 합니다. 백 엔드 스토리지로부터 수신된 데이터가 없는 경우 Cloud Insights는 Kubernetes 오브젝트 데이터를 리포팅으로 보낼 수 없습니다.

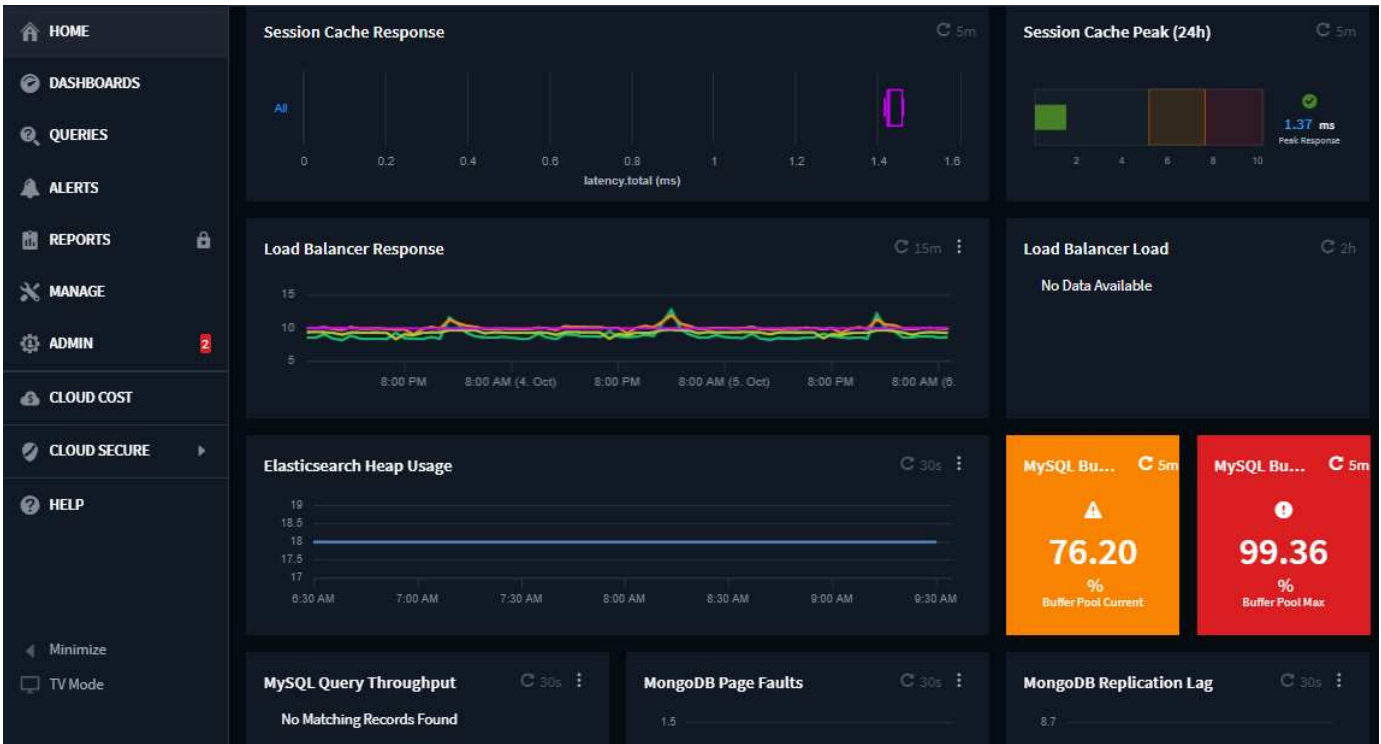


## 어두운 테마가 도착했습니다

여러분 중 다수가 어두운 테마를 요청했고, Cloud Insights는 그 해답을 제공해 왔습니다. 밝은 테마와 어두운 테마 간에



전환하려면 사용자 이름 옆에 있는 드롭다운을 클릭합니다.



## Data Collector 지원

Cloud Insights 데이터 수집기 중 몇 가지 기능이 개선되었습니다. 다음은 몇 가지 주요 사항입니다.

- ONTAP용 Amazon FSx의 새 수집기입니다

## 2021년 9월

### 이제 성능 정책이 모니터됩니다

모니터링 및 경고 기능은 Cloud Insights 전반에 걸쳐 성능 정책과 위반을 대체했습니다. "모니터를 통한 경고" 귀사의 환경에서 잠재적인 문제 또는 동향을 보다 유연하게 파악하고 파악할 수 있습니다.

### 모니터의 자동 완성 추천 단어, 와일드카드 및 식

경고를 위해 모니터를 생성할 때 필터를 직접 입력할 수 있는 것은 예측 가능한 일이므로 모니터에 대한 메트릭이나 속성을 쉽게 검색하고 찾을 수 있습니다. 또한 입력한 텍스트를 기반으로 와일드카드 필터를 만들 수 있는 옵션이 제공됩니다.

## 1 Select a metric to monitor

StoragePool.performance.utilization.read

Filter By name sas1

Group Avg

Unit Displayed In

Create wildcard containing "sas1"

tawny03:tawny03sas1

tawny04:tawny04sas1

None

## Telegraf 에이전트를 업데이트했습니다

Telegraf 통합 데이터 수집용 에이전트가 버전 \* 1.19.3 \* 으로 업데이트되었으며 성능 및 보안 기능이 향상되었습니다. 업데이트를 원하는 사용자는 의 해당 업그레이드 섹션을 참조할 수 있습니다 "[Agent 설치](#)" 문서화: 이전 버전의 에이전트는 사용자 작업 없이 계속 작동합니다.

## Data Collector 지원

Cloud Insights 데이터 수집기 중 몇 가지 기능이 개선되었습니다. 다음은 몇 가지 주요 사항입니다.

- Microsoft Hyper-V Collector는 이제 WMI 대신 PowerShell을 사용합니다
- Azure VM 및 VHD Collector는 이제 병렬 호출로 인해 최대 10배 더 빠릅니다
- HPE Nimble은 이제 통합 및 iSCSI 구성을 지원합니다

또한 데이터 수집 기능을 향상 개선하고 있기 때문에 다음과 같은 최근 변경 사항이 있습니다.

- EMC Powerstore의 새 Collector입니다
- Hitachi Ops Center의 새로운 Collector입니다
- Hitachi Content Platform의 새로운 수집가
- 향상된 ONTAP 수집기로 Fabric 풀 보고
- 스토리지 풀 및 볼륨 성능을 통해 ANF 향상
- 스토리지 노드 및 스토리지 성능은 물론 버킷 단위의 객체 수가 포함된 EMC ECS가 향상되었습니다
- 스토리지 노드 및 Qtree 메트릭을 통해 EMC Isilon을 개선했습니다
- 볼륨 QoS 제한 메트릭을 통해 EMC Symmetrix를 개선했습니다
- 스토리지 노드의 상위 일련 번호가 포함된 향상된 IBM SVC 및 EMC PowerStore

## 2021년 8월

## 새 감사 페이지 사용자 인터페이스

를 클릭합니다 "감사 페이지"에서는 더욱 깔끔한 인터페이스를 제공하며 이제 감사 이벤트를 .csv 파일로 내보낼 수 있습니다.

## 향상된 사용자 역할 관리

Cloud Insights에서는 이제 사용자 역할 및 액세스 제어를 보다 자유롭게 할당할 수 있습니다. 이제 사용자는 모니터링, 보고 및 Cloud Secure에 대해 개별적으로 세분화된 사용 권한을 할당할 수 있습니다.

즉, 모니터링, 최적화 및 보고 기능에 대한 관리 액세스 권한을 더 많이 허용하면서 중요한 Cloud Secure 감사 및 활동 데이터에 대한 액세스를 필요한 사용자에게만 제한할 수 있습니다.

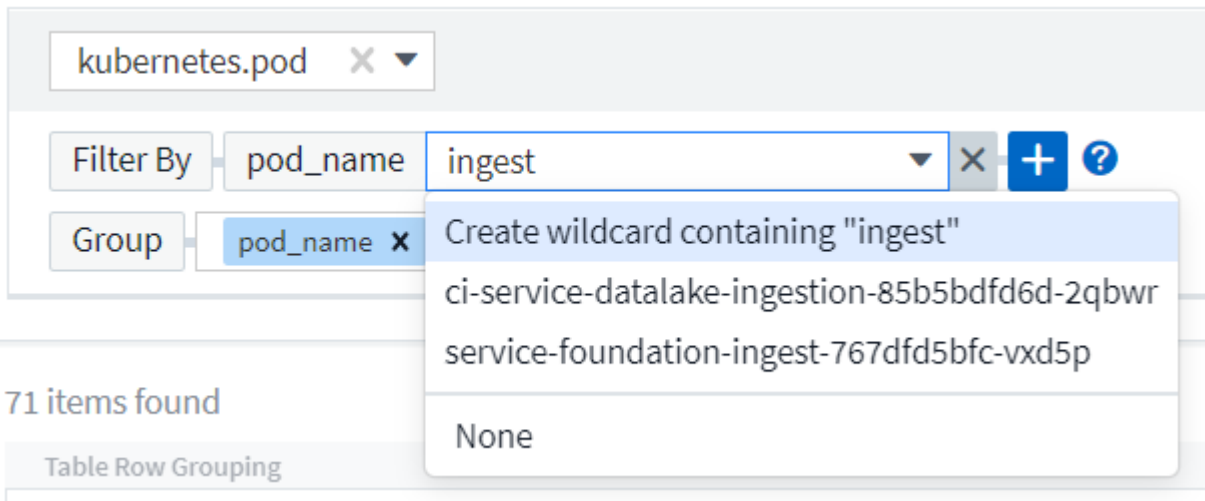
"자세한 내용을 확인하십시오" Cloud Insights 설명서의 다양한 액세스 수준에 대해 설명합니다.

## 2021년 6월

### 필터의 자동 완성 추천 단어, 와일드카드 및 식

이 Cloud Insights 릴리스에서는 쿼리 또는 위젯에서 필터링할 수 있는 모든 이름과 값을 알 필요가 없습니다. 필터링을 할 때 간단히 입력을 시작하면 Cloud Insights에서 텍스트를 기반으로 값을 제안합니다. 위젯에 표시할 애플리케이션 이름 또는 Kubernetes 속성을 미리 살펴볼 필요가 없습니다.

필터에 입력하면 선택할 수 있는 결과의 스마트 목록과 현재 텍스트를 기반으로 \* 와일드카드 필터 \* 를 만드는 옵션이 표시됩니다. 이 옵션을 선택하면 와일드카드 식과 일치하는 모든 결과가 반환됩니다. 물론 필터에 추가할 개별 값을 여러 개 선택할 수도 있습니다.



또한 NOT 또는 OR을 사용하여 필터에 \* 식 \* 을 만들거나 "없음" 옵션을 선택하여 필드의 null 값을 필터링할 수 있습니다.

에 대해 자세히 알아보십시오 "필터링 옵션" 쿼리 및 위젯.

## Edition에서 사용할 수 있는 API입니다

Cloud Insights의 강력한 API는 그 어느 때보다 쉽게 액세스할 수 있으며, 알림 API는 이제 Standard 및 Premium Edition에서 사용할 수 있습니다. 각 에디션에 대해 다음 API를 사용할 수 있습니다.

API 범주	기본	표준	프리미엄
획득 장치	✓	✓	✓
데이터 수집	✓	✓	✓
경고		✓	✓
자산		✓	✓
데이터 수집		✓	✓

## Kubernetes PV 및 Pod의 가시성

Cloud Insights는 Kubernetes 환경의 백엔드 스토리지에 대한 가시성을 제공하므로 Kubernetes Pod 및 PVS(Persistent Volumes)에 대한 통찰력을 얻을 수 있습니다. 이제 PV 카운터를 통해 단일 Pod에서 PV로, 그리고 백엔드 스토리지 장치로 가는 모든 방법으로 IOPS, 지연 시간 및 처리량과 같은 PV 카운터를 추적할 수 있습니다.

볼륨 또는 내부 볼륨 랜딩 페이지에는 다음 두 개의 새로운 테이블이 표시됩니다.

### Kubernetes PVs

5m

2 items found

PV ↑	Cluster	PV Capacity (GiB)	Phase	StorageClass
<a href="#">cvo-shared-storage-pv</a>	<a href="#">QA_K8S_CLUSTER</a>	0.73	Bound	
<a href="#">test-mysql-shared-storage-pv</a>	<a href="#">QA_K8S_CLUSTER</a>	7.32	Bound	

### Kubernetes Pods

5m

2 items found


Pod ↑	Cluster	Namespace	PV	Workload Type	Workload	Latency - Total ...	IOPS - 1
<a href="#">cvo-mypod-pvc</a>	<a href="#">QA_K8S_CLUSTER</a>	k8testns	<a href="#">cvo-shared-storage</a>				0.00
<a href="#">test-mysql-0</a>	<a href="#">QA_K8S_CLUSTER</a>	k8testns	<a href="#">test-mysql-shared-</a>	StatefulSet	test-mysql	0.19	2.72

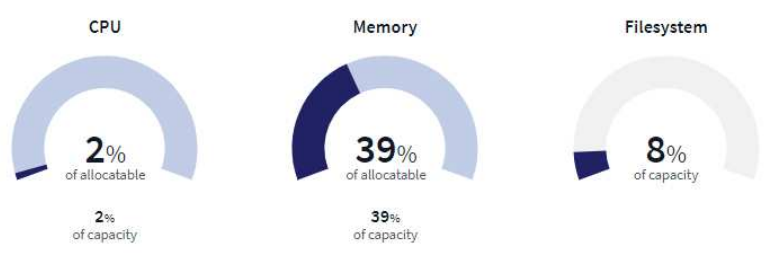
이러한 새 테이블을 활용하려면 현재 Kubernetes 에이전트를 제거하고 새로 설치하는 것이 좋습니다. 또한 Kubbe-State-Metrics 버전 2.1.0 이상을 설치해야 합니다.

## Kubernetes 노드에서 VM 링크까지


이제 Kubernetes 노드 페이지에서 노드의 VM 페이지를 클릭하여 열 수 있습니다. VM 페이지에는 노드 자체에 대한 링크도 포함되어 있습니다.

14 Pods  
 14 Healthy 0 Alerting


Labels - Node IP 10.30.27.178 Virtual Machine **main-ci-node-general-1b-05** 



Pods		Containers	
Status ↑	Name	Healthy Containers	Namespace
Healthy	Running	ci-service-assets-bcb7447c-lsk29	1 of 1 oci
Healthy	Running	ci-service-webui-rest-74b89f5d8-nvlog	1 of 1 oci
Healthy	Running	filebeat-gg7r7	1 of 1 kube-system
Healthy	Running	ovs-vbjzd	1 of 1 openshift-sdn

NetApp /  main-ci-node-general-1b-05

### Virtual Machine Summary 5m

<b>Power State:</b> On  <b>Guest State:</b> Running  <b>Datastore:</b> i-01b052b8d843994e7  <b>CPU Utilization - Total:</b> 3.89 %  <b>Memory Utilization - Total:</b> N/A  <b>Memory:</b> 32.0 GB  <b>Capacity - Total:</b> 200.0 GB  <b>Capacity - Used:</b> N/A	<b>Latency - Total:</b> 1.21 ms  <b>IOPS - Total:</b> 11.06 IO/s  <b>Throughput - Total:</b> 0.06 MB/s  <b>DNS Name:</b> ip-10-178.ec2.internal  <b>IP:</b>  <b>OS:</b> CentOS Linux 7 x86_64 HVM EBS ENA 1901_01-  <b>Processors:</b> 8  <b>Hypervisor Name:</b> us-east-1b	<b>Hypervisor IP:</b> US-EAST-1B  <b>Hypervisor OS:</b> Amazon AWS EC2  <b>Hypervisor FC Fabrics:</b> 0  <b>Hypervisor CPU Utilization:</b> N/A  <b>Hypervisor Memory Utilization:</b> N/A  <b>Kubernetes Node:</b> <a href="#">ip-10-30-27-178.ec2.internal</a>   <b>Alert Monitors:</b> <a href="#">VM Capacity</a> <a href="#">VM IOPS</a>  <a href="#">View Topology</a>
--	---	---

## 성능 정책을 대체하는 경고 모니터

여러 임계값, 웹훅 및 이메일 알림 전송, 단일 인터페이스를 사용하는 모든 메트릭의 경고 등의 추가 이점을 제공하기 위해 Cloud Insights는 표준 및 프리미엄 에디션 고객을 \* 성능 정책 \* 에서 \* 모니터 \* 로 2021년 7월과 8월 사이에 변환합니다. 에 대해 자세히 알아보십시오 "경고 및 모니터" 그리고 이 흥미로운 변화에 계속 귀를 집중하세요.

## Cloud Secure는 NFS를 지원합니다

Cloud Secure는 이제 ONTAP 데이터 수집을 위해 NFS를 지원합니다. SMB 및 NFS 사용자 액세스를 모니터링하여 랜섬웨어 공격으로부터 데이터를 보호합니다. 또한 Cloud Secure는 NFS 사용자 특성 수집을 위해 Active-Directory 및 LDAP 사용자 디렉토리를 지원합니다.

## Cloud Secure 스냅샷 제거

Cloud Secure는 스냅샷 삭제 설정을 기반으로 스냅샷을 자동으로 삭제하여 저장소 공간을 절약하고 수동 스냅샷 삭제 필요성을 줄입니다.

### Snapshot Purge Settings

Define purge periods to automatically delete snapshots taken by Cloud Secure.

**Attack Automated Response**

Delete Snapshot after

**Warning Automated Response**

Delete Snapshot after

**User Created**

Delete Snapshot after

## Cloud Secure 데이터 수집 속도

이제 단일 데이터 수집기 에이전트 시스템이 Cloud Secure에 초당 최대 20,000개의 이벤트를 게시할 수 있습니다.

## 2021년 5월

4월에 적용한 변경 사항은 다음과 같습니다.

### Telegraf 에이전트를 업데이트했습니다

Telegraf 통합 데이터 수집용 에이전트가 성능 및 보안 향상을 통해 버전 1.17.3으로 업데이트되었습니다. 업데이트를 원하는 사용자는 의 해당 업그레이드 섹션을 참조할 수 있습니다 "[Agent 설치](#)" 문서화: 이전 버전의 에이전트는 사용자 작업 없이 계속 작동합니다.



## 경고에 정정 조치를 추가합니다

이제 모니터 생성 또는 수정 시 추가 정보 및/또는 수정 조치는 물론 선택적 설명을 추가할 수 있습니다. \* 경고 설명 추가 \* 섹션을 입력합니다. 설명이 경고와 함께 전송됩니다. insights and corrective actions\_field는 경고 처리에 대한 자세한 단계 및 지침을 제공할 수 있으며, 경고 랜딩 페이지의 요약 섹션에 표시됩니다.

### 4 Add an alert description (optional)

**Add a description**

Enter a description that will be sent with this alert (1024 character limit)

**Add insights and corrective actions**

Enter a url or details about the suggested actions to fix the issue raised by the alert

## 모든 에디션용 Cloud Insights API

이제 모든 버전의 Cloud Insights에서 API 액세스를 사용할 수 있습니다. 이제 Basic Edition 사용자는 획득 장치 및 데이터 수집기 작업을 자동화할 수 있으며 Standard Edition 사용자는 메트릭을 쿼리하고 사용자 지정 메트릭을 수집할 수 있습니다. Premium Edition은 모든 API 범주의 모든 사용을 계속 허용합니다.

API 범주	기본	표준	프리미엄
획득 장치	✓	✓	✓
데이터 수집	✓	✓	✓
자산		✓	✓
데이터 수집		✓	✓
데이터 웨어하우스			✓

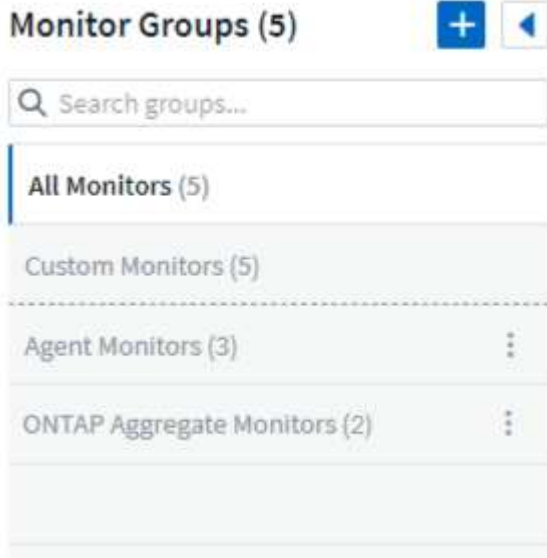
API 사용에 대한 자세한 내용은 를 참조하십시오 ["API 설명서"](#).

## 2021년 4월

### 보다 간편한 모니터 관리

**"모니터 그룹화"** 환경의 모니터 관리를 간소화합니다. 이제 여러 모니터를 하나로 그룹화하여 일시 중지할 수 있습니다. 예를 들어 인프라 스택에서 업데이트가 발생하는 경우 클릭 한 번으로 모든 장치에서 경고를 일시 중지할 수 있습니다.

모니터 그룹은 ONTAP 장치의 향상된 관리를 Cloud Insights에 제공하는 흥미로운 새 기능의 첫 번째 부분입니다.



## Webhook를 사용한 향상된 경고 옵션

많은 상용 응용 프로그램이 지원됩니다 "Webhook" 표준 입력 인터페이스로 사용 가능합니다. 이제 Cloud Insights는 이러한 다양한 전달 채널을 지원하며 Slack, PagerDuty, Teams 및 AchAN등에 대한 기본 템플릿을 제공할 뿐 아니라 사용자 지정 가능한 일반 웹 후크를 제공하여 다른 많은 애플리케이션을 지원합니다.

### 3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook	Notify team on Critical, Warning	Use Webhook(s) PagerDuty Trigger
	Notify team on Resolved	Use Webhook(s) PagerDuty Resolve

## 개선된 장치 식별

모니터링 및 문제 해결 기능을 개선하고 정확한 보고 기능을 제공하기 위해 IP 주소 또는 기타 식별자 대신 장치 이름을 이해하는 것이 좋습니다. Cloud Insights는 이제 이러한 규칙 기반 접근 방식을 사용하여 환경에 있는 스토리지 및 물리적 호스트 디바이스의 이름을 식별하는 자동 방법을 통합합니다 "**\* 장치 해상도 \***", \* 관리 \* 메뉴에서 사용할 수 있습니다.

## 더 많은 것을 요청하셨습니다!

고객이 자주 사용하는 질문에는 데이터 범위를 시각화하는 기본 옵션이 더 많이 추가되었으므로, 시간 범위 선택을 통해 서비스 전체에서 사용할 수 있는 다음과 같은 다섯 가지 새로운 선택 사항이 추가되었습니다.

- 마지막 30분
- 최근 2시간
- 최근 6시간

- 최근 12시간
- 최근 2일

## 하나의 **Cloud Insights** 환경에서 다중 구독

4월 2일부터 Cloud Insights는 단일 Cloud Insights 인스턴스에서 고객에 대해 동일한 에디션 유형의 여러 구독을 지원합니다. 이를 통해 고객은 Cloud Insights 서브스크립션의 일부를 인프라 구매와 상호 연계할 수 있습니다. 여러 서브스크립션에 대한 지원은 NetApp 세일즈 팀에 문의하십시오.

## 경로를 선택합니다

Cloud Insights를 설정하는 동안 모니터링 및 알림 또는 랜섬웨어 및 내부자 위협 감지로 시작할지 여부를 선택할 수 있습니다. Cloud Insights는 선택한 경로를 기반으로 시작 환경을 구성합니다. 나중에 언제든지 다른 경로를 구성할 수 있습니다.

## Cloud Secure 온보딩이 더욱 간편해졌습니다

또한 새로운 단계별 설정 검사 목록을 통해 Cloud Secure 사용을 훨씬 쉽게 시작할 수 있습니다.

NetApp CDS Sa... / **Getting Started with Cloud Secure**



### Secure Your Data from Ransomware & Insider Threat

- Ransomware & insider threat detection
- User data access auditing

#### Setting up Cloud Secure

- ✓ Add an [Agent](#) on server or VM to collect data ([system requirements](#) [🔗](#)).
- ✓ Configure a [User Directory Collector](#) to collect user attributes from active directories (optional step).
- ✓ Configure a [Data Collector](#) to collect file access activity on your storage devices.
- ✓ Define [Automated Response Policies](#) to take automatic action in the event of an attack.

User activity data will appear in the [Forensics](#) section

항상 그렇듯이, 여러분의 제안을 듣고 싶습니다! [ng-cloudinsights-customerfeedback@netapp.com](mailto:ng-cloudinsights-customerfeedback@netapp.com) 으로 이메일을 보내주세요.

# 2021년 2월

## Telegraf 에이전트를 업데이트했습니다

Telegraf 통합 데이터를 수집하는 에이전트가 취약점 및 버그 수정을 포함한 버전 1.17.0으로 업데이트되었습니다.

## Cloud Cost Analyzer

과거, 현재 및 예상 지출에 대한 상세 비용 분석을 제공하여 귀사의 환경에서 클라우드 사용량에 대한 가시성을 제공하는 클라우드 비용을 지원하는 Spot by NetApp의 기능을 체험해 보십시오. Cloud Cost 대시보드에서는 클라우드 비용을 명확하게 파악하고 개별 워크로드, 계정 및 서비스를 세부적으로 확인할 수 있습니다.

Cloud Cost는 다음과 같은 주요 과제를 해결할 수 있습니다.

- 클라우드 비용 추적 및 모니터링
- 폐기물 및 잠재적 최적화 영역 식별
- 실행 가능한 작업 항목 제공

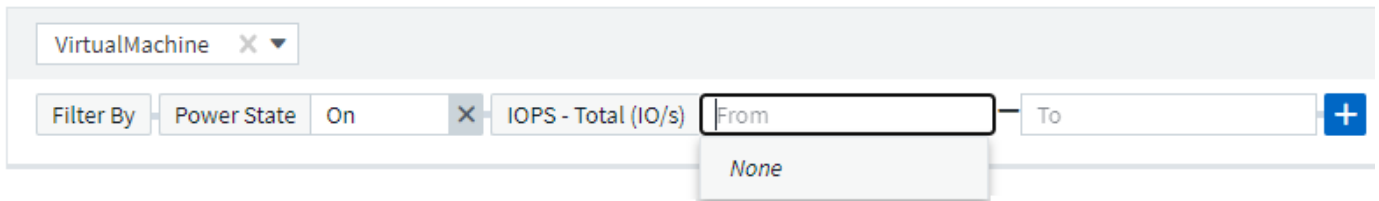
클라우드 비용은 모니터링에 중점을 둡니다. 자동 비용 절감 및 환경 최적화를 사용하려면 NetApp 계정을 전체 Spot으로 업그레이드하십시오.

## 필터를 사용하여 Null 값이 있는 개체를 쿼리합니다

이제 Cloud Insights에서는 필터를 사용하여 null/none 값을 갖는 속성 및 메트릭을 검색할 수 있습니다. 다음 위치의 모든 속성/메트릭에 대해 이 필터링을 수행할 수 있습니다.

- [여기](#)를 클릭합니다
- 대시보드 위젯 및 페이지 변수
- [여기](#)를 클릭합니다
- 모니터를 생성할 때

null/none 값을 필터링하려면 해당 필터 드롭다운에 표시될 때 `_None_` 옵션을 선택하면 됩니다.



## 다중 지역 지원

오늘부터 전 세계 여러 지역에서 Cloud Insights 서비스를 제공하여 미국 이외의 지역에 거주하는 고객의 성능을 향상시키고 보안을 강화합니다. Cloud Insights/Cloud Secure는 환경이 구축된 지역에 따라 정보를 저장합니다.

[여기](#)를 클릭합니다 "여기" 를 참조하십시오.

# 2021년 1월

## 추가 **ONTAP** 메트릭의 이름이 변경되었습니다

ONTAP 시스템에서 데이터 수집의 효율성을 높이기 위한 지속적인 노력의 일환으로, 다음과 같은 ONTAP 메트릭의 이름이 변경되었습니다.

이러한 메트릭을 사용하여 기존 대시보드 위젯이나 쿼리를 작성한 경우 새 메트릭 이름을 사용하려면 해당 위젯을 편집하거나 다시 생성해야 합니다.

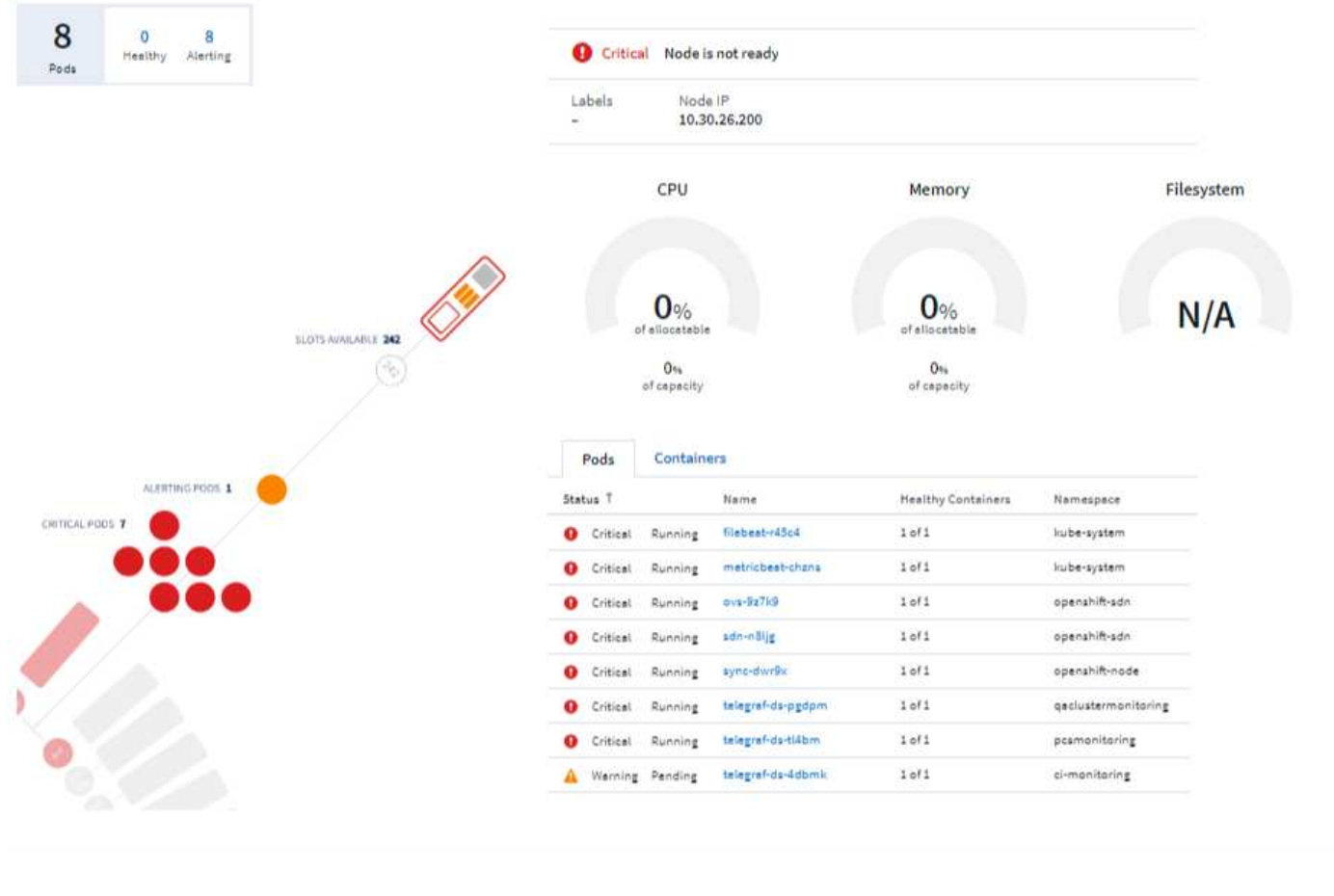
이전 메트릭 이름	새 메트릭 이름
netapp_ontap.disk_f성분.total_transfers	NetApp_ONTAP.DISK_FURNENT.TOTAL_IOPS
netapp_ontap.disk.total_transfers	NetApp_ONTAP.disk.total_IOPS입니다
NetApp_ONTAP.FCP_lif.read_data를 참조하십시오	NetApp_ONTAP.FCP_lif.read_throughput을 지정합니다
NetApp_ONTAP.FCP_lif.write_data를 참조하십시오	NetApp_ONTAP.FCP_lif.write_throughput을 지정합니다
NetApp_ONTAP.iscsi_lif.read_data를 참조하십시오	NetApp_ONTAP.iscsi_lif.read_throughput을 참조하십시오
NetApp_ONTAP.iscsi_lif.write_data를 참조하십시오	NetApp_ONTAP.iscsi_lif.write_throughput을 설정합니다
netapp_ontap.lif.recv_data를 참조하십시오	netapp_ontap.lif.recv_throughput을 지정합니다
netapp_ontap.lif.sent_data	netapp_ontap.lif.sent_throughput
NetApp_ONTAP.LUN.read_data를 참조하십시오	NetApp_ONTAP.LUN.read_throughput을 설정합니다
NetApp_ONTAP.LUN.write_data를 참조하십시오	NetApp_ONTAP.LUN.write_throughput을 지정합니다
NetApp_ONTAP.NIC_COMMON.Rx_바이트	NetApp_ONTAP.NIC_COMMON.Rx_Throughput
NetApp_ONTAP.NIC_COMMON.TX_바이트	netapp_ontap.nic_common.tx_throughput을 지정합니다
NetApp_ONTAP.path.read_data를 입력합니다	NetApp_ONTAP.path.read_throughput을 지정합니다
NetApp_ONTAP.path.write_data를 입력합니다	netapp_ontap.path.write_throughput을 지정합니다
NetApp_ONTAP.path.total_data를 나타냅니다	NetApp_ONTAP.path.total_throughput을 지정합니다
NetApp_ONTAP.policy_group.read_data를 참조하십시오	NetApp_ONTAP.policy_group.read_throughput을 설정합니다
NetApp_ONTAP.policy_group.write_data를 나타냅니다	NetApp_ONTAP.policy_group.write_throughput을 설정합니다
NetApp_ONTAP.policy_group.other_data를 지정합니다	NetApp_ONTAP.policy_group.other_throughput을 설정합니다
NetApp_ONTAP.policy_group.total_data를 나타냅니다	NetApp_ONTAP.policy_group.total_throughput을 지정합니다
NetApp_ONTAP.SYSTEM_NODE.DISK_DATA_READ를 참조하십시오	NetApp_ONTAP.system_node.disk_throughput_read를 참조하십시오

이전 메트릭 이름	새 메트릭 이름
NetApp_ONTAP.system_node.disk_data_Written	NetApp_ONTAP.system_node.disk_throughput_Written
NetApp_ONTAP.SYSTEM_NODE.HDD_DATA_READ를 참조하십시오	NetApp_ONTAP.system_node.hdd_throughput_read를 참조하십시오
NetApp_ONTAP.system_node.hdd_data_Written	NetApp_ONTAP.system_node.hdd_throughput_Written
NetApp_ONTAP.SYSTEM_NODE.SSD_DATA_READ를 참조하십시오	NetApp_ONTAP.system_node.ssd_throughput_read를 참조하십시오
NetApp_ONTAP.system_node.ssd_data_Written	NetApp_ONTAP.system_node.ssd_throughput_Written
netapp_ontap.system_node.net_data_recv	netapp_ontap.system_node.net_throughput_recv
netapp_ontap.system_node.net_data_sent	netapp_ontap.system_node.net_throughput_sent
NetApp_ONTAP.SYSTEM_NODE.FCP_DATA_REV	NetApp_ONTAP.system_node.fcp_throughput_recv를 지정합니다
NetApp_ONTAP.SYSTEM_NODE.FCP_DATA_Sent	NetApp_ONTAP.system_node.fcp_throughput_sent를 보냈습니다
NetApp_ONTAP.volume_node.cifs_read_data를 입력합니다	NetApp_ONTAP.volume_node.cifs_read_throughput을 지정합니다
NetApp_ONTAP.volume_node.cifs_write_data를 입력합니다	NetApp_ONTAP.volume_node.cifs_write_throughput을 지정합니다
NetApp_ONTAP.VOLUME_NODE.NFS_READ_DATA	NetApp_ONTAP.volume_node.nfs_read_throughput을 지정합니다
NetApp_ONTAP.VOLUME_NODE.NFS_WRITE_DATA	NetApp_ONTAP.volume_node.nfs_write_throughput을 지정합니다
NetApp_ONTAP.volume_node.iscsi_read_data를 참조하십시오	NetApp_ONTAP.volume_node.iscsi_read_throughput을 지정합니다
NetApp_ONTAP.VOLUME_NODE.ISCSI_WRITE_DATA	NetApp_ONTAP.volume_node.iscsi_write_throughput을 지정합니다
NetApp_ONTAP.VOLUME_NODE.FCP_READ_DATA	NetApp_ONTAP.volume_node.fcp_read_throughput을 지정합니다
NetApp_ONTAP.VOLUME_NODE.FCP_WRITE_DATA	NetApp_ONTAP.volume_node.fcp_write_throughput을 지정합니다
NetApp_ONTAP.volume.read_data를 참조하십시오	NetApp_ONTAP.volume.read_throughput을 설정합니다
NetApp_ONTAP.volume.write_data를 참조하십시오	NetApp_ONTAP.volume.write_throughput을 설정합니다
netapp_ontap.워크로드.read_data	netapp_ontap.워크로드.read_throughput을 선택합니다
netapp_ontap.워크로드.write_data	netapp_ontap.워크로드.write_throughput
NetApp_ONTAP.워크로드_볼륨.읽기_데이터	NetApp_ONTAP.워크로드_볼륨.읽기_처리량
NetApp_ONTAP.워크로드_볼륨.write_data	NetApp_ONTAP.Workload_volume.write_throughput을 설정합니다

## 새로운 Kubernetes Explorer를 도입했습니다

를 클릭합니다 ["Kubernetes 탐색기"](#) 단순한 Kubernetes 클러스터 토폴로지 뷰를 제공하므로 비전문가도 클러스터 레벨에서 컨테이너 및 스토리지에 이르는 문제와 증속성을 빠르게 식별할 수 있습니다.

Kubernetes 환경에서 클러스터, 노드, Pod, 컨테이너, 스토리지의 상태, 사용 상태 및 상태에 대한 Kubernetes Explorer의 세부 정보를 사용하여 다양한 정보를 살펴볼 수 있습니다.



## 2020년 12월

### 단순한 Kubernetes 설치

Kubernetes Agent 설치를 간소화하여 더 적은 수의 사용자 상호 작용이 필요합니다. ["Kubernetes Agent 설치 중"](#) Kubernetes 데이터 수집도 포함됩니다.

## 2020년 11월

### 추가 대시보드

다음과 같은 새로운 ONTAP 중심 대시보드가 갤러리에 추가되었으며 가져올 수 있습니다.

- ONTAP: 성능 및 용량을 집계합니다
- ONTAP FAS/AFF - 용량 활용률
- ONTAP FAS/AFF - 클러스터 용량
- ONTAP FAS/AFF 효율성
- ONTAP FAS/AFF-FlexVol 성능
- ONTAP FAS/AFF 노드 운영/최적의 포인트
- ONTAP FAS/AFF - 사전 사후 용량 효율성
- ONTAP: 네트워크 포트 작동
- ONTAP: 노드 프로토콜 성능
- ONTAP: 노드 워크로드 성능(프런트엔드)
- ONTAP: 프로세서
- ONTAP: SVM 워크로드 성능(프런트엔드)
- ONTAP: 볼륨 워크로드 성능(프런트엔드)

## 테이블 위젯에서 열 이름 바꾸기

편집 모드에서 위젯을 열고 열 상단의 메뉴를 클릭하여 테이블 위젯의 *Metrics* 및 *Attributes* 섹션에서 열 이름을 바꿀 수 있습니다. 새 이름을 입력하고 `_Save_`를 클릭하거나 `_Reset_`를 클릭하여 열을 원래 이름으로 다시 설정합니다.

이는 테이블 위젯의 열 표시 이름에만 영향을 미치며, 메트릭/속성 이름은 기본 데이터 자체에서 변경되지 않습니다.

Metrics & Attributes	
Metric Name	⋮
qa-ots-cl01	▼ Rename Column <span style="float: right;">Reset</span> <input type="text" value="Metric Name"/>
ngslabc90	
kuat	
hkdemo-cluster	

## 2020년 10월

### 통합 데이터의 기본 확장

이제 테이블 위젯 그룹화를 통해 Kubernetes, ONTAP 고급 데이터 및 에이전트 노드 메트릭의 기본 확장이 가능합니다. 예를 들어, `Kubernetes_Nodes_BY_Cluster_`를 그룹화할 경우 각 클러스터에 대한 테이블에 행이 표시됩니다. 그런 다음 각 클러스터 행을 확장하여 노드 오브젝트 목록을 볼 수 있습니다.



## Basic Edition 기술 지원

이제 표준 및 프리미엄 버전 외에 Cloud Insights Basic Edition 가입자에 대한 기술 지원을 받을 수 있습니다. 또한 Cloud Insights는 NetApp 지원 티켓 생성을 위한 워크플로우를 간소화했습니다.

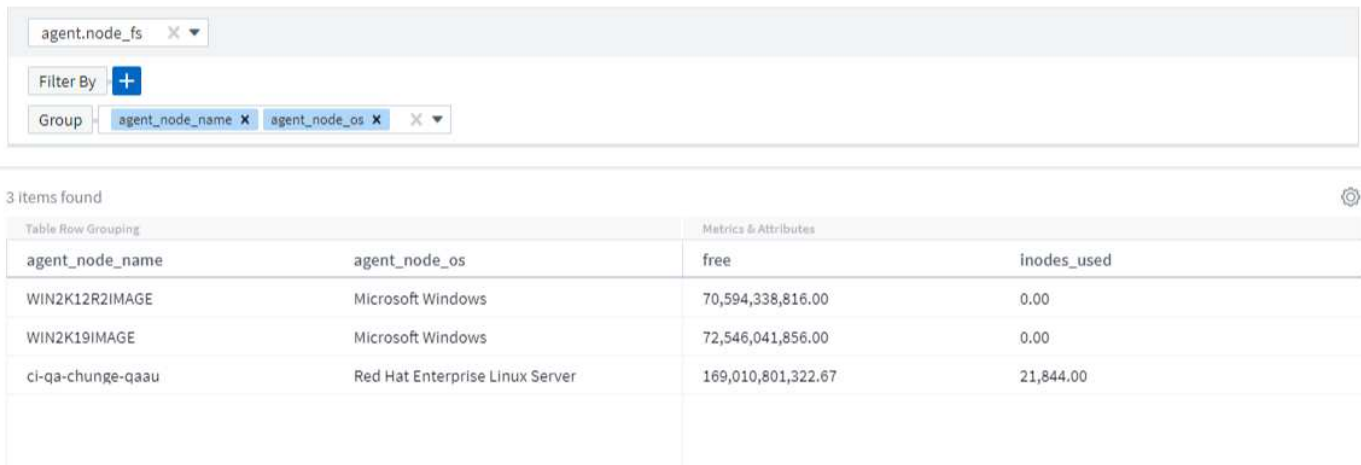
## Cloud Secure 공용 API

Cloud Secure 지원 "REST API" 활동 및 경고 정보에 액세스합니다. 이 작업은 Cloud Secure 관리 UI를 통해 생성된 API 액세스 토큰을 사용하여 수행되며, 이 UI는 REST API에 액세스하는 데 사용됩니다. 이러한 REST API에 대한 Swagger 문서는 Cloud Secure와 통합됩니다.

## 2020년 9월

### 통합 데이터가 있는 쿼리 페이지

Cloud Insights 쿼리 페이지는 통합 데이터(예: Kubernetes, ONTAP 고급 메트릭 등)를 지원합니다. 통합 데이터로 작업할 때 쿼리 결과 테이블에는 왼쪽에 개체/그룹화가 있는 "분할 화면" 보기와 오른쪽에 개체 데이터(특성/메트릭)가 표시됩니다. 통합 데이터를 그룹화하기 위해 여러 특성을 선택할 수도 있습니다.



The screenshot shows a query interface with the following components:

- Query: agent.node\_fs
- Filter By: +
- Group: agent\_node\_name, agent\_node\_os
- 3 Items found

Table Row Grouping		Metrics & Attributes	
agent_node_name	agent_node_os	free	inodes_used
WIN2K12R2IMAGE	Microsoft Windows	70,594,338,816.00	0.00
WIN2K19IMAGE	Microsoft Windows	72,546,041,856.00	0.00
ci-qa-chunge-qaau	Red Hat Enterprise Linux Server	169,010,801,322.67	21,844.00

### 테이블 위젯에서 단위 표시 형식

이제 메트릭/카운터 데이터(예: 기가바이트, MB/초 등)를 표시하는 열의 테이블 위젯에서 단위 표시 형식을 사용할 수 있습니다. 메트릭의 표시 단위를 변경하려면 열 머리글에서 "점 3개" 메뉴를 클릭하고 "단위 표시"를 선택합니다. 사용 가능한 단위 중에서 선택할 수 있습니다. 사용 가능한 단위는 표시 열의 메트릭 데이터 유형에 따라 달라집니다.

Table Widget Override Dashboard Time Last 3 Hours

agent.node

Filter By + Group agent\_node\_name

8 items found

agent_node_name ↑	mem.used (GiB)
ci-qa-avinashp-k8-bakra-1	12.41
ci-qa-avinashp-k8-bakra-2	9.31
ci-qa-avinashp-k8-bakra-3	4.46
ci-qa-avinashp-k8-bakra-4	1.15
ci-qa-avinashp-k8swheel-1	15.23

> Aggregation

▼ Unit Display

Base Unit byte (B)

Displayed In gibibyte (GiB)

Cancel Save

## 획득 장치 세부 정보 페이지

이제 획득 장치에 자체 랜딩 페이지가 있어 각 AU에 유용한 세부 정보와 문제 해결에 도움이 되는 정보를 제공합니다. 를 클릭합니다 ["AU 세부 정보 페이지"](#) AU의 데이터 수집기에 대한 링크와 유용한 상태 정보를 제공합니다.

## Cloud Secure Docker 종속성이 제거되었습니다

Cloud Secure의 Docker 의존성이 제거되었습니다. Cloud Secure 에이전트를 설치하는 데 Docker가 더 이상 필요하지 않습니다.

## 보고 사용자 역할

보고 기능이 있는 Cloud Insights 프리미엄 에디션이 있는 경우 사용자 환경의 모든 Cloud Insights 사용자는 보고 응용 프로그램(즉 Cognos). 메뉴에서 \* 보고서 \* 링크를 클릭하면 자동으로 보고에 로그인됩니다.

Cloud Insights의 사용자 역할에 따라 가 결정됩니다 ["보고 사용자 역할"](#):

Cloud Insights 역할	보고 역할	보고 권한
게스트	소비자	에서는 보고서를 보고 일정을 잡고 실행할 수 있으며 언어 및 표준 시간대와 같은 개인 기본 설정을 설정할 수 있습니다. 소비자는 보고서를 만들거나 관리 작업을 수행할 수 없습니다.
사용자	저자	는 모든 소비자 기능을 수행할 뿐 아니라 보고서 및 대시보드를 생성 및 관리할 수 있습니다.
관리자	관리자	보고서 구성, 보고 작업 종료 및 재시작 등의 모든 관리 작업과 모든 작성자 기능을 수행할 수 있습니다.



Cloud Insights 보고는 500MU 이상의 환경에서 사용할 수 있습니다.



현재 Premium Edition 고객이고 보고서를 보관하려는 경우 이 내용을 읽어보십시오 ["기존 고객을 위한 중요 참고 사항"](#).

## 데이터 수집용 새로운 API 범주입니다

Cloud Insights는 \* 데이터 수집 \* API 범주를 추가하여 사용자 지정 데이터 및 에이전트를 보다 강력하게 제어할 수 있도록 합니다. 이 API 범주와 기타 API 범주에 대한 자세한 내용은 Cloud Insights에서 \* 관리자 > API 액세스 \* 로 이동하고 [API Documentation\\_link](#)를 클릭하여 확인할 수 있습니다. AU 세부 정보 페이지와 AU 목록 페이지에 표시되는 메모 필드에서 AU에 메모를 첨부할 수도 있습니다.

## 2020년 8월

### 모니터링 및 경고

현재 스토리지 오브젝트, VM, EC2 및 포트에 대한 성능 정책을 설정하는 기능 외에도 Cloud Insights Standard Edition에는 이제 기능이 포함되어 있습니다 **"모니터를 구성합니다"** Kubernetes, ONTAP 고급 메트릭 및 Telegraf 플러그인의 통합 데이터 임계치 경고를 트리거할 각 개체 메트릭에 대한 모니터를 만들고, 경고 수준 또는 위험 수준 임계값에 대한 조건을 설정하고, 각 수준에 대해 원하는 이메일 수신자를 지정하기만 하면 됩니다. 그러면 됩니다 **"알림을 보고 관리합니다"** 추세를 추적하거나 문제를 해결합니다.



## 2020년 7월


### Cloud Secure\_스냅샷\_조치 수행

Cloud Secure는 악의적인 활동이 감지되면 스냅샷을 자동으로 생성하여 데이터를 보호하고 데이터가 안전하게 백업되도록 합니다.

랜섬웨어 공격 또는 기타 비정상적인 사용자 활동이 감지되면 스냅샷을 생성하는 자동화된 응답 정책을 정의할 수 있습니다. 알림 페이지에서 수동으로 스냅샷을 생성할 수도 있습니다.

## 자동 스냅샷 촬영

Potential Attack Detail / Ransomware Attack Jul 26, 2020  
2:38 AM - 5:38 AM



**POTENTIAL ATTACK: AL\_307**  
Ransomware Attack

**Detected**  
4 days ago  
Jul 26, 2020 3:38 AM

**Action Taken**  
Snapshots Taken

**Status**  
In Progress

Last snapshots taken by **Amit Schwartz**  
Jul 30, 2020 2:54 PM

Re-Take Snapshots

How To:  
Restore Entities

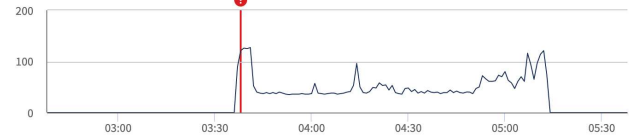
**Total Attack Results**

1	0	5148
Affected Volumes	Deleted Files	Encrypted Files


5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

*This is potentially a sign of ransomware attack.*  
The extension "crypt" was added to each file.

**Encrypted Files**  
Activity per minute



**Related Users**



**Ewen Hall**  
Developer  
Engineering

**5148**  
Encrypted Files

**Detected**  
4 days ago  
Jul 26, 2020 3:38 AM

**Action Taken**  
Snapshots Taken

## 수동 스냅샷


**Cloud Insights** Abhi Basu Thakur

MONITOR & OPTIMIZE Alerts / **Nabilah Howell had an abnormal change in activity rate** Jul 23, 2020 - Jul 26, 2020  
1:44 AM - 1:44 AM

CLOUD SECURE

- ALERTS
- FORENSICS
- ADMIN
- HELP

**Alert Detail**



**WARNING: AL\_306**  
**Nabilah Howell had an abnormal change in activity rate.**

**Detected**  
5 days ago  
Jul 25, 2020 1:44 PM

**Action Taken**  
None

**Status**  
New

*Recommendation: Setup an Automated Response Policy*  
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. Try it now.

Take Snapshots

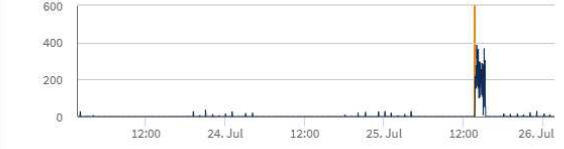
How To:  
Restore Entities

**Nabilah Howell's Activity Rate Change**

Typical	Alert	
122.8	210	↑ 71%
Activities Per Minute	Activities Per Minute	

Nabilah Howell's activity rate grew 71% over their typical average.

**Activity Rate**  
Activity per 5 minutes



## 메트릭/카운터 업데이트

Cloud Insights UI 및 REST API에서 사용할 수 있는 용량 카운터는 다음과 같습니다. 이전에는 이러한 카운터는 데이터 웨어하우스/보고에만 사용할 수 있었습니다.

개체 유형	카운터
스토리지	용량 - 스페어 물리적 용량 - 실패한 물리적 용량
스토리지 풀	데이터 용량 - 사용된 데이터 용량 - 총 기타 용량 - 사용된 기타 용량 - 총 용량 - 물리적 용량 - 소프트 제한값
내부 볼륨	Data Capacity - Used Data Capacity - Total Other Capacity - Used Other Capacity - Total Clone Saved Capacity - Total

## Cloud Secure 잠재적 공격 탐지

Cloud Secure는 이제 랜섬웨어와 같은 잠재적인 공격을 탐지합니다. 경고 목록 페이지에서 경고를 클릭하여 다음을 보여 주는 세부 정보 페이지를 엽니다.

- 공격 시간
- 연결된 사용자 및 파일 작업
- 조치를 취했습니다
- 보안 침해 가능성을 추적하는 데 도움이 되는 추가 정보입니다

잠재적인 랜섬웨어 공격을 보여주는 경고 페이지



잠재적인 랜섬웨어 공격에 대한 상세 페이지



POTENTIAL ATTACK: AL\_305  
Ransomware Attack

Detected  
5 days ago  
Jul 11, 2020 4:02 AM

Action Taken  
None

Status  
New

#### Total Attack Results

1 Affected Volumes | 0 Deleted Files | 4173 Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.  
The extension "crypt" was added to each file.

#### Encrypted Files

Activity per minute



#### Related Users



**Kristjan Egilsson**  
Accountant  
Finance

4173  
Encrypted Files

Detected  
5 days ago  
Jul 11, 2020 4:02 AM

Action Taken  
None



Username  
us035  
  
Email  
Egilsson@netapp.com  
  
Phone  
387224312607

Department  
Finance  
  
Manager  
Lyndsey Maddox

#### Top Activity Types

Activity per minute  
Last access location: 10.197.144.115

[View Activity Detail](#)



## AWS를 통해 Premium Edition을 구독하십시오

Cloud Insights 평가판을 사용하면 됩니다 "자체 구독" AWS Marketplace에서 Cloud Insights Standard Edition 또는 Premium Edition으로 이동합니다. 이전에는 AWS Marketplace를 통해서만 Standard Edition으로 자체 구독할 수 있었습니다.

## 향상된 테이블 위젯

대시보드/자산 페이지 테이블 위젯에는 다음과 같은 개선 사항이 포함되어 있습니다.

- "분할 화면" 보기: 테이블 위젯은 왼쪽의 오브젝트/그룹화와 오른쪽의 오브젝트 데이터(특성/메트릭)를 표시합니다.

GroupBy All  Override Dashboard Time 🕒 ✕

index\_0.index\_0 ✕

Filter By + Group agent\_version ✕ !

1 Item found ⚙️

Table Row Grouping		Metrics & Attributes				
agent_version	value	consumer	protocol_name	level0	level1	
Java/1.8.0_242	1,649.80	CloudInsights	GENERATED	simulated	N/A	

- 다중 속성 그룹화: 통합 데이터(Kubernetes, ONTAP 고급 메트릭, Docker 등)의 경우 그룹화할 속성을 여러 개 선택할 수 있습니다. 선택한 그룹화 속성에 따라 데이터가 표시됩니다.

통합 데이터와 그룹화(편집 모드에 표시):

Table Widget - Integration Data Example  Override Dashboard Time 🕒 Last 7 Days ✕

index\_0.index\_0 ✕

Filter By + Group agent\_version ✕ name ✕ protocol\_name ✕ !

500 Items found ⚙️

Table Row Grouping			Metrics & Attributes				
agent_version	name	protocol_name	value	consumer	protocol_name	level0	level1
Java/1.8.0_242	simulated.shinchaku-client-1010.counter.2...	GENERATED	1,597.16	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1008.counter.1...	GENERATED	1,604.92	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1015.counter.1...	GENERATED	1,684.82	CloudInsights	GENERATED	simulated	shinchaku-
Java/1.8.0_242	simulated.shinchaku-client-1008.counter.0...	GENERATED	1,677.15	CloudInsights	GENERATED	simulated	shinchaku-

Cancel Save

- 인프라스트럭처 데이터(스토리지, EC2, VM, 포트 등)는 이전과 같은 단일 속성을 기준으로 그룹화됩니다. 개체가 아닌 특성으로 그룹화하면 그룹 행을 확장하여 그룹 내의 모든 개체를 볼 수 있습니다.

인프라 데이터를 사용하여 그룹화(표시 모드에 표시):

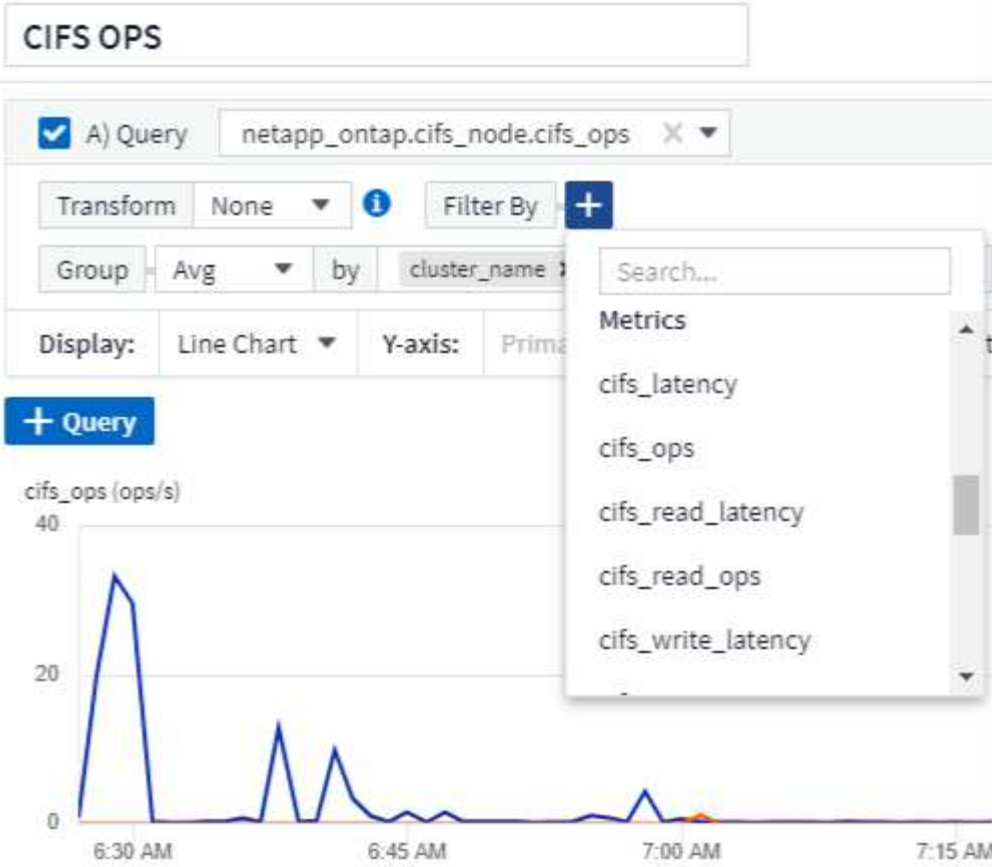
GroupBy Date 🔄 1h

4 items found in 2 groups

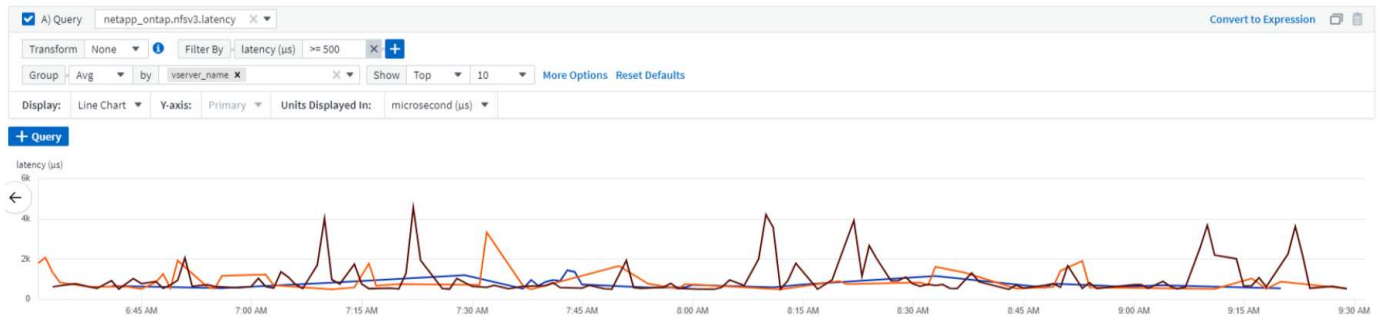
Active Date	Storage Node	Cache Hit Ratio - Total (%)	IOPS - Total (IO...	IOPS - Write (I...	Latency
06/01/2020 (1)	ocinaneqa1-01	N/A	N/A	N/A	N/A
06/01/2020	ocinaneqa1-01	N/A	N/A	N/A	N/A
N/A (3)	--	N/A	N/A	N/A	N/A

## 메트릭 필터링

이제 위젯에서 객체의 속성을 필터링하는 것 외에도 메트릭을 필터링할 수 있습니다.



통합 데이터(Kubernetes, ONTAP 고급 데이터 등)를 사용할 경우, 메트릭 필터링은 필터가 데이터 시리즈의 집계 값에 대해 작동하고 잠재적으로 전체 오브젝트를 차트에서 제거할 수 있는 인프라 데이터(스토리지, VM, 포트 등)와 달리 표시된 데이터 시리즈에서 개별/일치하지 않는 데이터 요소를 제거합니다.

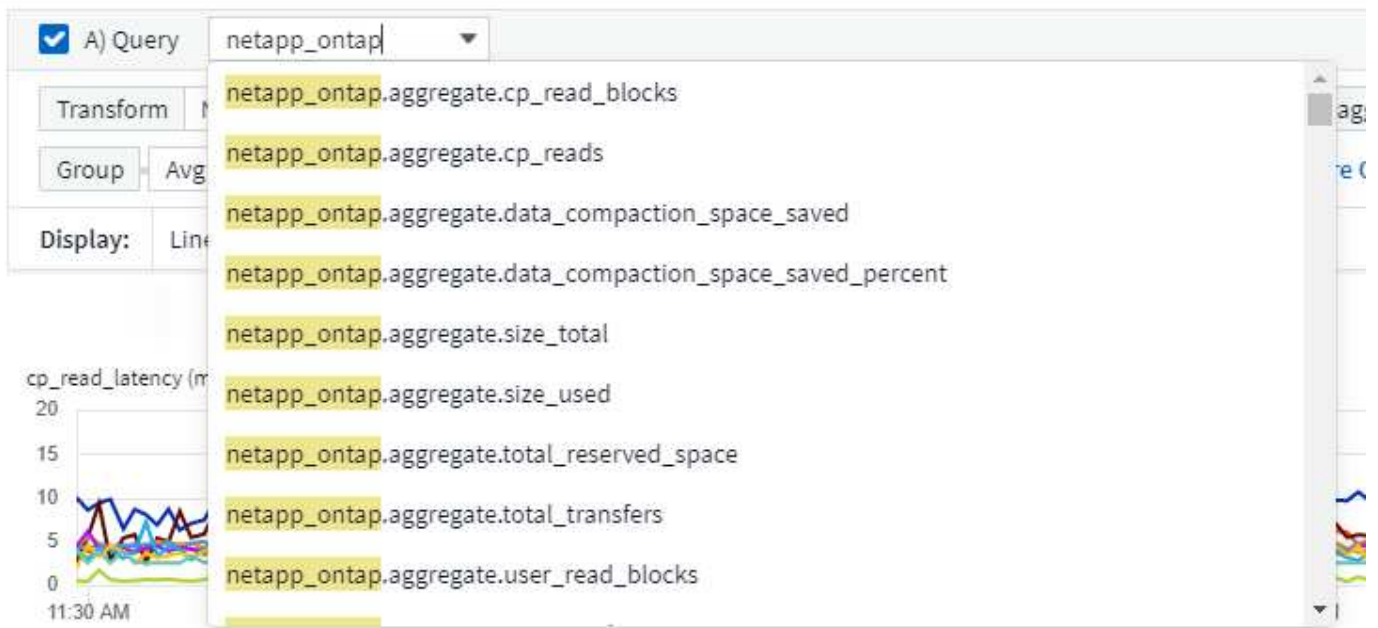


## ONTAP 고급 카운터 데이터

Cloud Insights는 ONTAP 장치에서 수집된 다양한 카운터 및 메트릭을 제공하는 NetApp의 ONTAP별 \* 고급 카운터 데이터 \* 를 활용합니다. ONTAP 고급 카운터 데이터는 모든 NetApp ONTAP 고객에게 제공됩니다. 이러한 메트릭을 통해 Cloud Insights 위젯 및 대시보드에서 사용자 지정 및 광범위한 시각화를 수행할 수 있습니다.

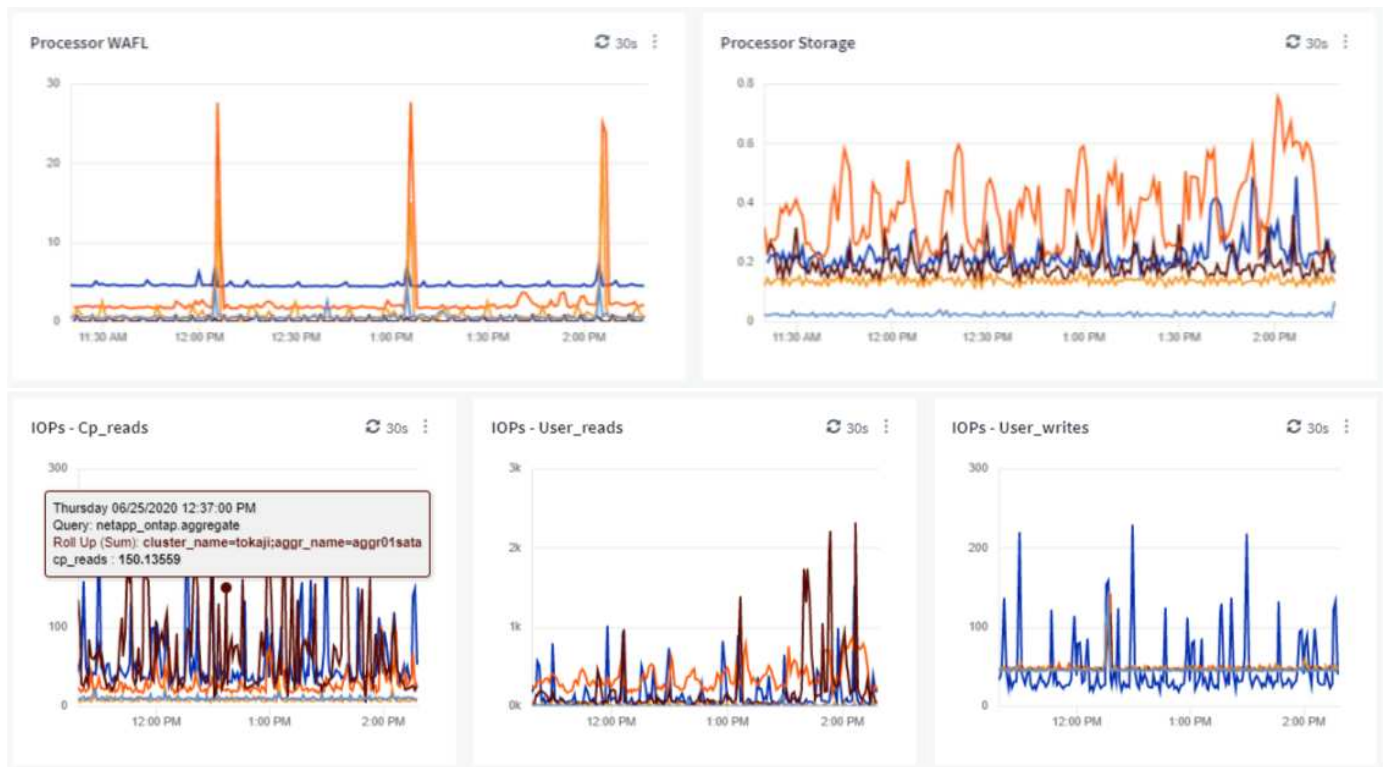
ONTAP 고급 카운터는 위젯 쿼리에서 "NetApp\_ONTAP"을 검색하고 카운터 중에서 선택하여 찾을 수 있습니다.





카운터 이름의 추가 부분을 입력하여 검색을 구체화할 수 있습니다. 예를 들면 다음과 같습니다.

- *lif*
- 골재\_
- *offbox\_Vscan\_server*
- 있습니다



다음 사항에 유의하십시오.

- 새 ONTAP 데이터 수집기에 대해 고급 데이터 수집이 기본적으로 활성화됩니다. 기존 ONTAP 데이터 수집기에 대한 고급 데이터 수집을 활성화하려면 데이터 수집기를 편집하고 `_고급 구성_` 섹션을 확장합니다.
- 7-Mode ONTAP에서는 고급 데이터 수집을 사용할 수 없습니다.

## 고급 카운터 대시보드

Cloud Insights에는 *Aggregate* 성능, 볼륨 워크로드, 프로세서 활동 등의 항목에 대한 ONTAP 고급 카운터를 시각화하는 데 도움이 되도록 미리 디자인된 다양한 대시보드가 제공됩니다. ONTAP 데이터 수집기가 하나 이상 구성되어 있는 경우 대시보드 목록 페이지의 대시보드 갤러리에서 가져올 수 있습니다.

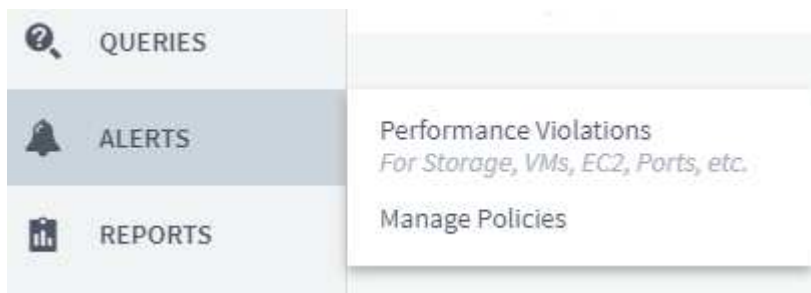
## 자세한 정보

ONTAP 고급 데이터에 대한 자세한 내용은 다음 링크를 참조하십시오.

- <https://mysupport.netapp.com/site/tools/tool-eula/netapp-harvest> (참고: NetApp Support에 로그인해야 합니다.)
- <https://nabox.org/faq/>

## 정책 및 위반 메뉴

성능 정책 및 위반 사항은 \* 알림 \* 메뉴에서 확인할 수 있습니다. 정책 및 위반 기능은 변경되지 않습니다.



## Telegraf 에이전트를 업데이트했습니다

Telegraf 통합 데이터 수집용 에이전트가 로 업데이트되었습니다 "버전 1.14" 여기에는 버그 수정, 보안 수정 및 새 플러그인이 포함됩니다.

참고: Kubernetes 플랫폼에서 Kubernetes 데이터 수집기를 구성할 때 "clusterrole" 특성에 대한 권한이 부족하여 로그에 "HTTP 상태 403 사용 금지" 오류가 표시될 수 있습니다.

이 문제를 해결하려면 끝점 액세스 클러스터 역할의 `_rules` 섹션에 강조 표시된 다음 Teleraf 포드를 다시 시작합니다.

```

rules:
- apiGroups:
  - ""
  - apps
  - autoscaling
  - batch
  - extensions
  - policy
  - rbac.authorization.k8s.io
attributeRestrictions: null
resources:
- nodes/metrics
- nodes/proxy <== Add this line
- nodes/stats
- pods <== Add this line
verbs:
- get
- list <== Add this line

```

## 2020년 6월

### 단순화된 Data Collector 오류 보고

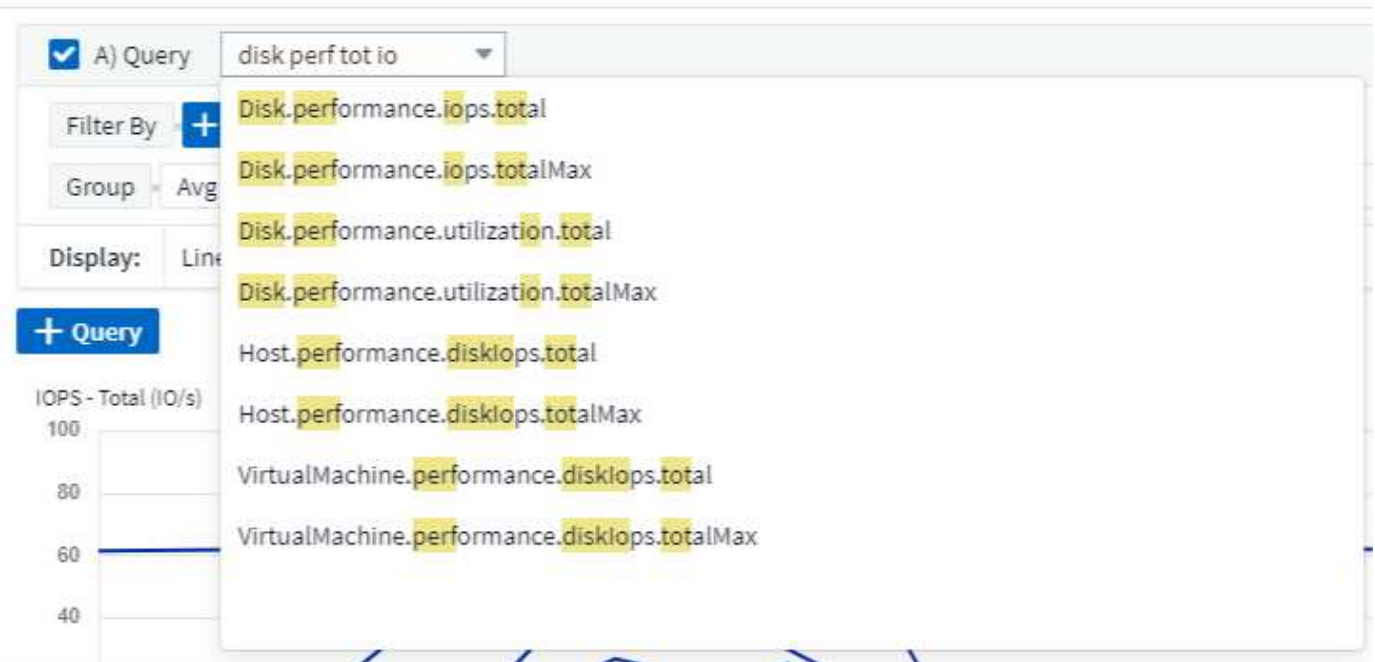
데이터 수집기 페이지의 *Send Error Report* 단추를 사용하면 데이터 수집기 오류를 쉽게 보고할 수 있습니다. 버튼을 클릭하면 오류에 대한 기본 정보가 NetApp으로 전송되고 문제 조사에 대한 프롬프트가 표시됩니다. 이 버튼을 누르면 Cloud Insights에서 NetApp에 통보되었음을 인정하고 오류 보고서 버튼을 사용하여 해당 데이터 수집기에 대한 오류 보고서를 전송할 수 있음을 표시합니다. 이 버튼은 브라우저 페이지를 새로 고칠 때까지 비활성 상태로 유지됩니다.



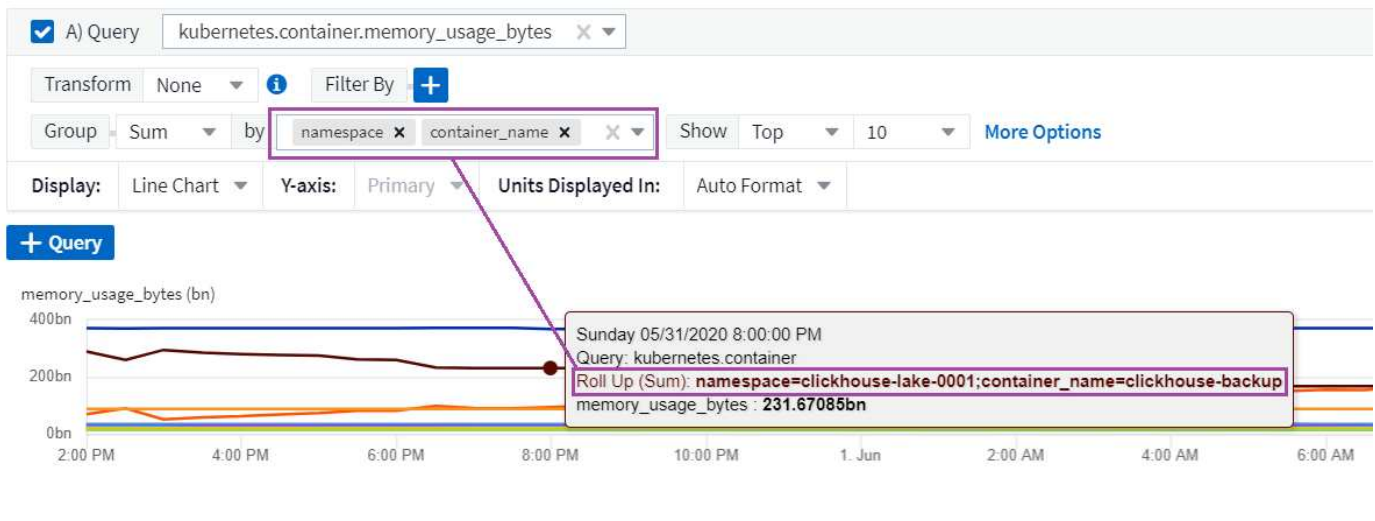
### 위젯 개선

대시보드 위젯에서 다음과 같은 개선 사항이 개선되었습니다. 이러한 개선 사항은 미리 보기 기능으로 간주되므로 일부 Cloud Insights 환경에서는 사용하지 못할 수 있습니다.

- 새로운 오브젝트/메트릭 선택기: 오브젝트(스토리지, 디스크, 포트, 노드 등) 및 관련 메트릭(IOPS, 지연 시간, CPU 수 등)을 강력한 검색 기능을 갖춘 단일 포함 드롭다운의 위젯에서 사용할 수 있습니다. 드롭다운에 부분 용어를 여러 개 입력할 수 있으며, Cloud Insights는 해당 조건을 충족하는 모든 객체 메트릭을 나열합니다.



- 다중 태그 그룹화: 통합 데이터(Kubernetes 등)를 사용하여 작업할 때는 여러 태그/속성으로 데이터를 그룹화할 수 있습니다. 예를 들어, Kubernetes 네임스페이스 및 컨테이너 이름별로 메모리 사용을 합합니다.



## 2020년 5월

### 보고 사용자 역할

보고를 위해 다음 역할이 추가되었습니다.

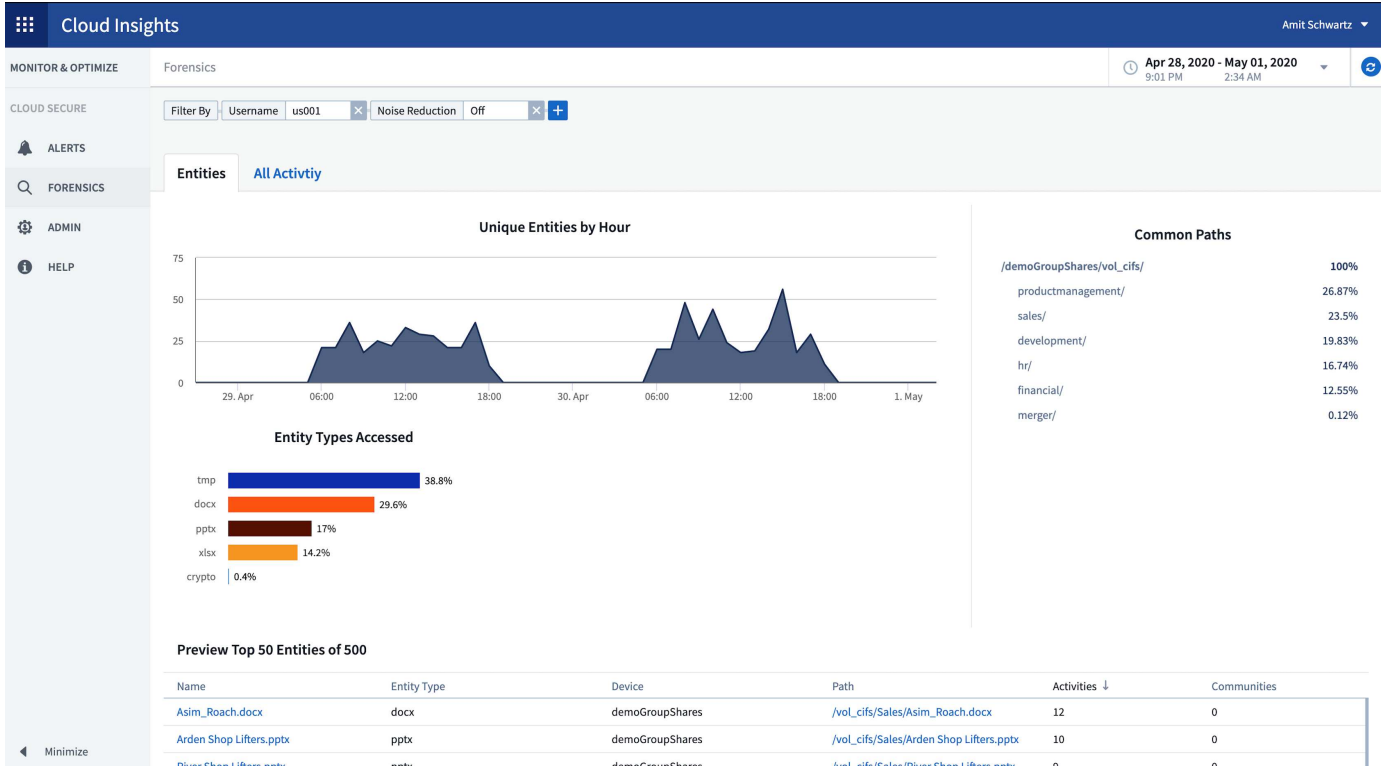
- Cloud Insights 소비자: 보고서를 실행하고 볼 수 있습니다
- Cloud Insights 작성자: 소비자 기능을 수행하고 보고서 및 대시보드를 생성 및 관리할 수 있습니다
- Cloud Insights 관리자: 작성자 기능은 물론 모든 관리 작업을 수행할 수 있습니다

## Cloud Secure 업데이트

Cloud Insights에는 다음과 같은 최근 Cloud Secure 변경 사항이 포함되어 있습니다.

Forensics > Activity Forensics 페이지에서 사용자 활동을 분석하고 조사하기 위한 두 가지 보기를 제공합니다.

- 사용자 활동에 초점을 맞춘 활동 보기(어떤 작업? 수행 위치)
- 요소 보기 - 사용자가 액세스한 파일에 중점을 둡니다.



또한 알림 이메일 알림에는 이제 알림 페이지에 대한 직접 링크가 포함되어 있습니다.

## 대시보드 그룹화

대시보드 그룹화를 통해 더 나은 성능을 얻을 수 있습니다 "대시보드 관리" 대해 알 수 있습니다. 스토리지 또는 가상 머신 등의 "원스톱" 관리를 위해 관련 대시보드를 그룹에 추가할 수 있습니다.

그룹은 사용자별로 사용자 지정되므로 한 사람의 그룹은 다른 사람의 그룹과 다를 수 있습니다. 필요한 만큼 그룹을 포함할 수 있으며 각 그룹에 원하는 만큼의 대시보드를 포함할 수 있습니다.

## Dashboard Groups (3)



All Dashboards (60)

My Dashboards (11)

Storage Group (7) ⋮

## Dashboards (7)



Name ↑

Dashboard - Storage Cost

Dashboard - Storage IO Detail

Dashboard - Storage Overview

Gauges Storage Performance

Storage Admin - Which nodes are in high demand?

Storage Admin - Which pools are in high demand?

Storage IOPs

## 대시보드 고정

즐거찾기가 항상 목록의 맨 위에 표시되도록 대시보드를 고정할 수 있습니다.

## Dashboards (7)



Name ↑

✈ Dashboard - Storage Overview

✈ Storage Admin - Which nodes are in high demand?

✈ Storage IOPs

Dashboard - Storage Cost

Dashboard - Storage IO Detail

Gauges Storage Performance

Storage Admin - Which pools are in high demand?

## TV 모드 및 자동 새로 고침

"TV 모드 및 자동 새로 고침" 대시보드 또는 자산 페이지에 데이터를 거의 실시간으로 표시할 수 있습니다.

- \* TV 모드 \* 는 깔끔한 디스플레이를 제공합니다. 탐색 메뉴가 숨겨지므로 데이터 디스플레이에 더 많은 화면 공간을 제공합니다.
- 대시보드 및 자산 랜딩 페이지의 위젯에 있는 데이터 \* 선택한 대시보드 시간 범위(또는 대시보드 시간을 재정의하도록 설정된 경우 위젯 시간 범위)에 따라 새로 고침 간격(매 10초)에 따라 자동으로 새로 고침 \*.

TV 모드와 자동 새로 고침이 결합되어 Cloud Insights 데이터를 실시간으로 볼 수 있어 원활한 데모 또는 사내 모니터링에 적합합니다.

## 2020년 4월

### 새로운 대시보드 시간 범위 선택

대시보드 및 기타 Cloud Insights 페이지의 시간 범위 선택에는 `_Last 1 Hour_`와 `_Last 15 Minutes_`가 포함됩니다.

### Cloud Secure 업데이트

Cloud Insights에는 다음과 같은 최근 Cloud Secure 변경 사항이 포함되어 있습니다.

- 사용자가 권한, 소유자 또는 그룹 소유권을 변경하는지 여부를 감지하기 위해 파일 및 폴더 메타데이터 변경 인식 기능이 향상되었습니다.
- 사용자 활동 보고서를 CSV로 내보냅니다.

Cloud Secure는 파일 및 폴더에 대한 모든 사용자 액세스 작업을 모니터링하고 감사합니다. 활동 감사를 통해 내부 보안 정책을 준수하고 PCI, GDPR, HIPAA 등의 외부 규정 준수 요구 사항을 충족하고 데이터 침해 및 보안 사고 조사를 수행할 수 있습니다.

### 기본 대시보드 시간입니다

이제 대시보드의 기본 시간 범위는 24시간이 아닌 3시간입니다.

### 최적화된 집계 시간

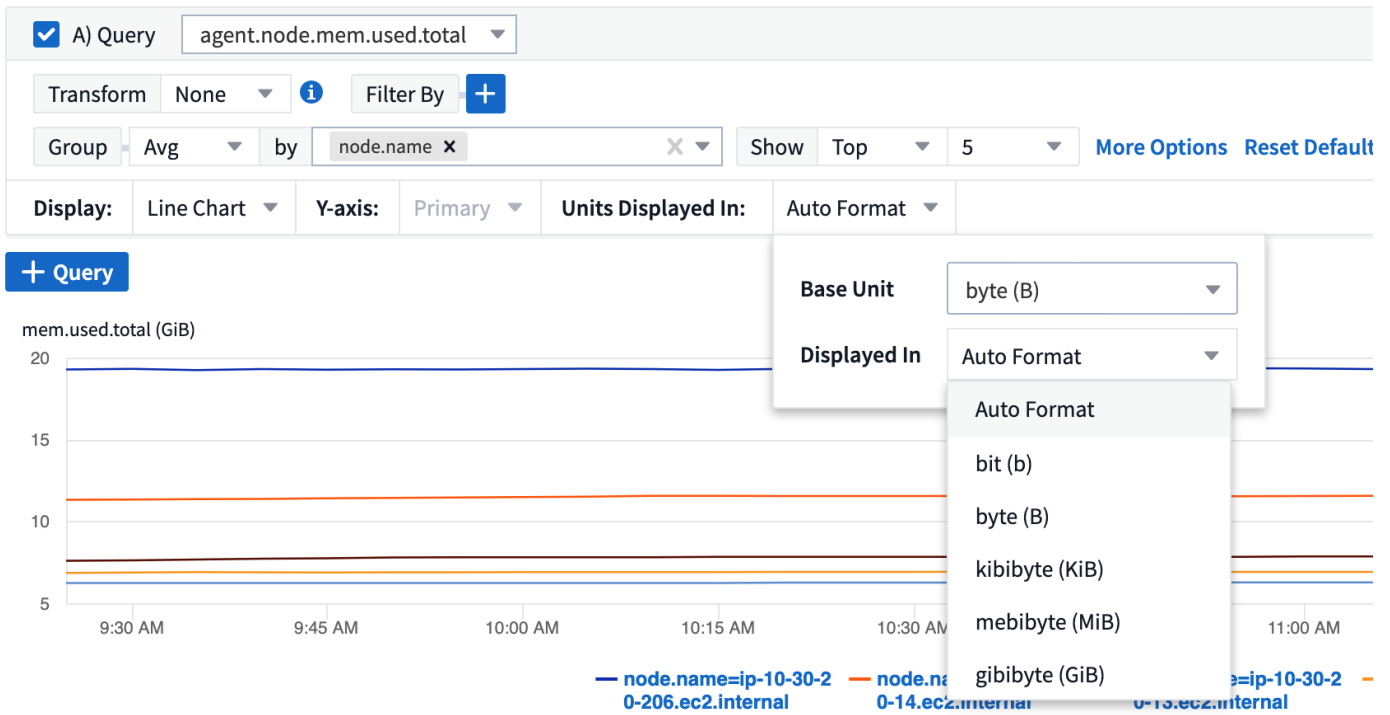
최적화 **"시간 집계"** 시계열 위젯(라인, 스프라인, 면적 및 누적 면적 차트)의 간격이 3시간 및 24시간 대시보드/위젯 시간 범위에 더 자주 표시되므로 데이터를 더 빠르게 차트 작성할 수 있습니다.

- 3시간 범위는 1분 집계 간격으로 최적화됩니다. 이전에는 5분이 소요되었습니다.
- 24시간 시간 범위는 30분 집계 간격으로 최적화됩니다. 이전에는 1시간이었습니다.

사용자 지정 간격을 설정하여 최적화된 집계를 재정의할 수 있습니다.

### 단위 자동 형식을 표시합니다

대부분의 위젯에서 Cloud Insights는 값을 표시할 기본 단위를 알고 있습니다(예: *Megabytes*, 수천, *percentage*, *milliseconds(ms)*, 기타 등등 **"자동 서식 지정"** 가장 읽기 쉬운 장치로 위젯입니다. 예를 들어, 1,234,567,890바이트의 데이터 값은 1.23 기비바이트로 자동 포맷됩니다. 대부분의 경우 Cloud Insights는 취득 데이터에 가장 적합한 형식을 알고 있습니다. 최상의 형식을 모르는 경우 또는 자동 서식을 무시하려는 위젯에서 원하는 형식을 선택할 수 있습니다.



## API를 사용하여 주석을 가져옵니다

Cloud Insights 프리미엄 에디션의 강력한 API를 통해 지금 바로 사용할 수 있습니다 "주석 불러오기" 그런 다음 .csv 파일을 사용하여 개체에 할당합니다. 같은 방법으로 응용 프로그램을 가져오고 업무 엔티티를 할당할 수도 있습니다.

**ASSETS.import**

PUT /assets/import Import assets from a CSV file.

Import annotations and applications from the given CSV file. The format of the CSV file is following:

```

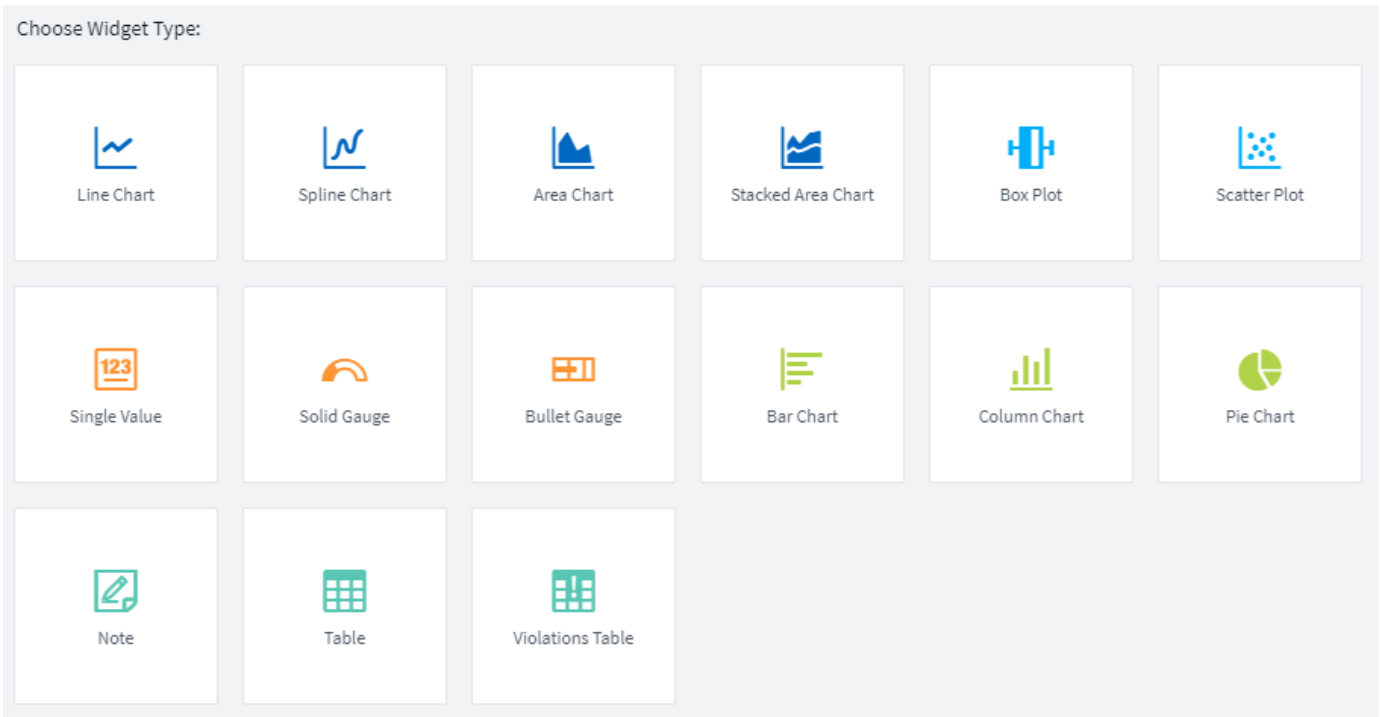
Project
, <Annotation Type> [, <Annotation Type> ...] [, Application] [, Tenant] [, Line_Of_Business] [, Business_Unit] [,
<Object Type Value 1>, <Object Name or Key 1>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 2>, <Object Name or Key 2>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 3>, <Object Name or Key 3>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
...
<Object Type Value N>, <Object Name or Key N>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]

```

## 간단한 위젯 선택기

모든 위젯 유형을 한 번에 하나의 보기로 표시하는 새로운 위젯 선택기로 대시보드와 자산 랜딩 페이지에 위젯을 추가하는 것이 더 쉬워졌습니다. 따라서 사용자는 더 이상 위젯 유형 목록을 스크롤하여 추가할 위젯을 찾을 필요가 없습니다. 관련 위젯은 새로운 셀렉터에서 가까운 색으로 조정되고 그룹화됩니다.





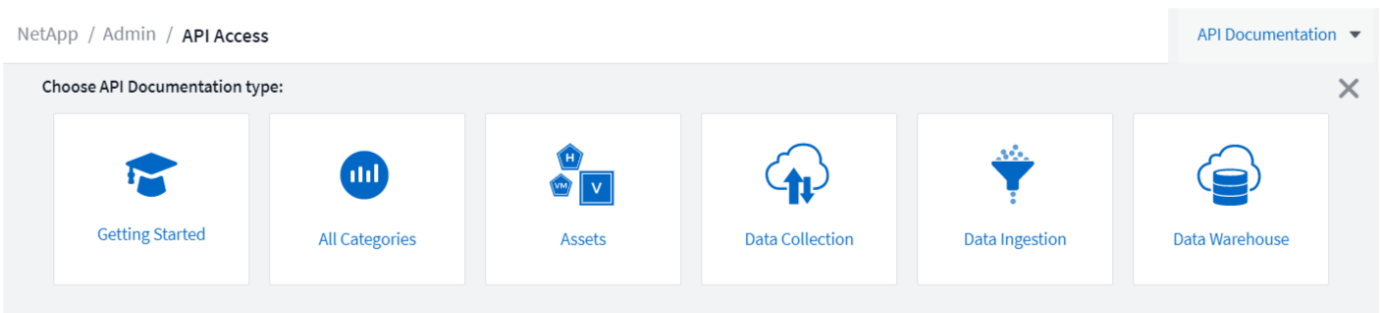
## 2020년 2월

### Premium Edition을 사용하는 API

Cloud Insights 프리미엄 에디션은 와 함께 제공됩니다 **"강력한 API"** Cloud Insights를 CMDB 또는 기타 티켓 시스템과 같은 다른 애플리케이션과 통합하는 데 사용할 수 있습니다.

자세한 Swagger 기반 정보는 \* API Documentation \* 링크 아래의 \* Admin > API ACCESS \* 에서 확인할 수 있습니다. Swagger는 API에 대한 간단한 설명 및 사용 정보를 제공하며 사용자 환경에서 각 API를 사용해 볼 수 있습니다.

Cloud Insights API는 액세스 토큰을 사용하여 자산 또는 컬렉션과 같은 API 범주에 대한 권한 기반 액세스를 제공합니다.



### Data Collector 추가 후 초기 폴링

이전에는 새 데이터 수집기를 구성한 후 Cloud Insights는 즉시 데이터 수집기를 폴링하여 `_INVENTORY_DATA`를 수집하지만 구성된 성능 폴링 간격(일반적으로 15분)이 될 때까지 기다렸다가 `initial_performance_data`를 수집합니다.

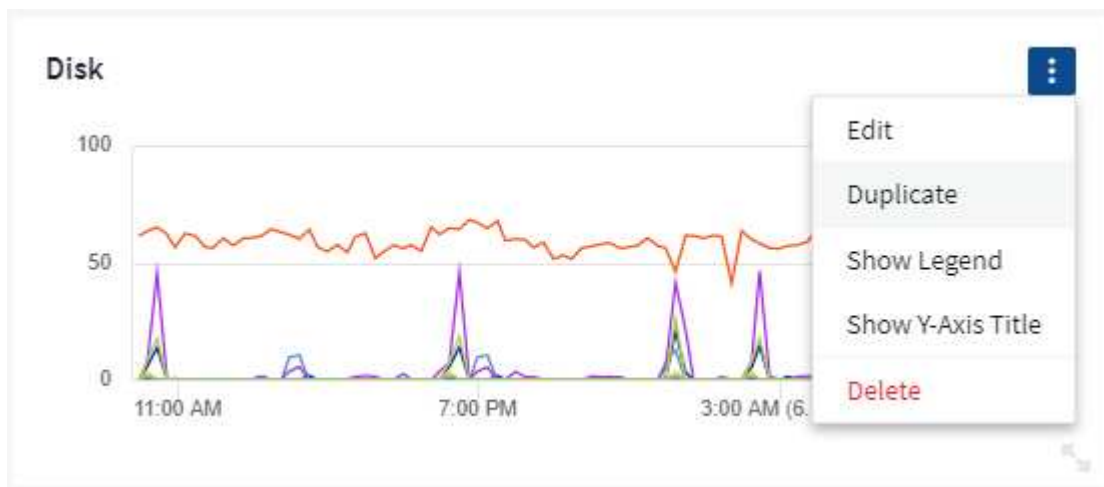
그런 다음 두 번째 성능 폴링을 시작하기 전에 다른 간격을 기다리게 됩니다. 이는 새 데이터 수집기에서 의미 있는 데이터를 획득하기 전에 최대 \_30분\_이 걸리기 때문입니다.

데이터 수집기 "폴링" 첫 번째 성능 폴링이 완료된 후 몇 초 이내에 두 번째 성능 폴링이 발생하면서 인벤토리 폴링 직후 초기 성능 폴링이 크게 개선되었습니다. 이를 통해 Cloud Insights는 매우 짧은 시간 내에 대시보드와 그래프에 유용한 데이터를 표시할 수 있습니다.

이 폴링 동작은 기존 데이터 수집기의 구성을 편집한 후에도 발생합니다.

## 간편한 위젯 복제

대시보드 또는 랜딩 페이지에서 위젯의 복사본을 만드는 것이 그 어느 때보다 쉬워졌습니다. 대시보드 편집 모드에서 위젯의 메뉴를 클릭하고 \* 복제 \* 를 선택합니다. 위젯 편집기가 시작되고, 원래 위젯의 구성이 미리 채워지고 위젯 이름에 "copy" 접미사가 붙습니다. 필요한 사항을 쉽게 변경하고 새 위젯을 저장할 수 있습니다. 위젯은 대시보드 하단에 배치되며 필요에 따라 배치할 수 있습니다. 모든 변경이 완료되면 대시보드를 저장해야 합니다.



## SSO(Single Sign-On)

Cloud Insights 프리미엄 에디션을 사용하면 관리자가 \* 를 활성화할 수 있습니다"SSO(Single Sign-On)"개별적으로 초대할 필요 없이 회사 도메인의 모든 사용자에게 대해 Cloud Insights에 대한 \* (SSO) 액세스. SSO를 사용하면 동일한 도메인 이메일 주소를 가진 모든 사용자가 회사 자격 증명을 사용하여 Cloud Insights에 로그인할 수 있습니다.



SSO는 Cloud Insights 프리미엄 버전에서만 사용할 수 있으며 Cloud Insights에 대해 사용하려면 먼저 구성해야 합니다. SSO 구성에는 이 포함됩니다 "ID 페더레이션" 부터 살펴보십시오. 페더레이션을 사용하면 SSO 사용자가 회사 디렉터리의 자격 증명을 사용하여 NetApp Cloud Central 계정에 액세스할 수 있습니다.

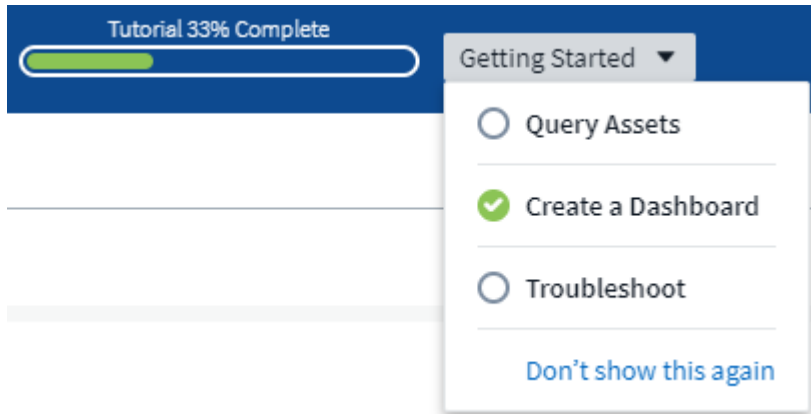
## 2020년 1월

### REST API에 대한 Swagger 문서

Swagger는 Cloud Insights에서 사용 가능한 REST API를 각각 설명하고 사용 및 구문을 설명합니다. Cloud Insights API에 대한 자세한 내용은 에서 확인할 수 있습니다 "문서화".

## 기능 자습서 진행률 표시줄

기능 자습서 검사 목록이 상단 배너로 이동되었으며 이제 진행률 표시기가 나타납니다. 자습서는 각 사용자가 해제할 때까지 사용할 수 있으며 Cloud Insights에서 항상 사용할 수 있습니다 "문서화".



## 획득 장치 변경

이미 설치된 AU와 이름이 같은 호스트 또는 VM에 AU(획득 장치)를 설치할 때 Cloud Insights는 AU 이름을 "\_1", "\_2"에 추가하여 고유한 이름을 보장합니다. 이는 Cloud Insights에서 먼저 제거하지 않고 동일한 VM에서 AU를 제거하고 다시 설치하는 경우에도 마찬가지입니다. 다른 AU 이름을 모두 원하십니까? 문제 없습니다. 설치 후 AU의 이름을 바꿀 수 있습니다.

## 위젯에서 최적화된 시간 집계

위젯에서 설정한 \_Optimized\_Time 집계 간격이나 \_Custom\_interval 중에서 선택할 수 있습니다. Optimized Aggregation은 선택한 대시보드 시간 범위(또는 대시보드 시간을 재정의하는 경우 위젯 시간 범위)를 기반으로 올바른 시간 간격을 자동으로 선택합니다. 대시보드 또는 위젯 시간 범위가 변경되면 간격이 동적으로 변경됩니다.

## "Cloud Insights 시작하기" 프로세스가 간편해졌습니다

Cloud Insights 사용을 시작하는 프로세스가 간소화되어 처음 설정하는 과정이 보다 원활하고 간편해졌습니다. 초기 데이터 수집기를 선택하고 지침을 따르기만 하면 됩니다. Cloud Insights에서 데이터 수집기 구성 및 필요한 에이전트 또는 획득 장치를 안내합니다. 대부분의 경우 하나 이상의 초기 대시보드를 가져와 환경을 신속하게 파악할 수 있습니다 (단, Cloud Insights에서 의미 있는 데이터를 수집하는 데 최대 30분이 소요됩니다).

추가 개선사항:

- 획득 장치 설치는 더 간단하며 더 빨리 실행됩니다.
- 알파벳 순 데이터 수집기 선택 항목을 사용하면 원하는 항목을 쉽게 찾을 수 있습니다.
- 개선된 Data Collector 설정 지침은 쉽게 따를 수 있습니다.
- 숙련된 사용자는 버튼 클릭 한 번으로 시작 프로세스를 건너뛸 수 있습니다.
- 새로운 진행률 표시줄에 현재 진행 중인 위치가 표시됩니다.



## 2019년 12월

비즈니스 엔티티는 필터에 사용할 수 있습니다

비즈니스 엔티티 주석은 쿼리, 위젯, 성능 정책 및 랜딩 페이지의 필터에 사용할 수 있습니다.

단일 값 및 게이지 위젯과 "모두"에 의해 롤다운된 모든 위젯에 대해 드릴다운 사용 가능

단일 값 또는 게이지 위젯의 값을 클릭하면 위젯에서 사용된 첫 번째 쿼리의 결과를 보여주는 쿼리 페이지가 열립니다. 또한 데이터가 "모두"에 의해 롤업된 위젯에 대한 범례를 클릭하면 위젯에서 사용된 첫 번째 쿼리의 결과를 보여주는 쿼리 페이지가 열립니다.

평가 기간이 연장되었습니다

Cloud Insights 무료 평가판을 신청하는 신규 사용자는 30일 이내에 제품을 평가할 수 있습니다. 이는 이전의 14일 시험 기간에 비해 증가한 것입니다.

관리 단위 계산

Cloud Insights의 관리 단위(MU) 계산이 다음과 같이 변경되었습니다.

- 관리 유닛 1개 = 호스트 2개(가상 또는 물리적 시스템)
- 1개의 관리 유닛 = 물리적 또는 가상 디스크의 포맷되지 않은 용량 4TB

이러한 변경을 통해 기존 Cloud Insights 서브스크립션을 사용하여 모니터링할 수 있는 환경 용량이 두 배로 효과적으로 늘어납니다.

## 2019년 11월

## 2019년 10월

보고

"\* Cloud Insights 보고 \*" 은 미리 정의된 보고서를 보거나 사용자 지정 보고서를 만들 수 있는 비즈니스 인텔리전스 도구입니다. 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

Cloud Insights 보고 기능을 사용하면 비용 청구, 소비 분석 및 예측 같은 영역에 대한 맞춤형 보고서를 생성할 수 있으며 다음과 같은 질문에 답할 수 있습니다.

- 보유하고 있는 재고는 무엇입니까?
- 내 재고는 어디에 있습니까?
- 누가 우리의 자산을 사용하고 있습니까?
- 비즈니스 유닛에 할당된 스토리지에 대한 비용청구는 무엇입니까?
- 추가 스토리지 용량을 구입할 때까지 얼마나 걸립니까?
- 사업부가 적절한 스토리지 계층에 맞게 조정됩니까?
- 월, 분기 또는 연도별로 스토리지 할당이 어떻게 변경됩니까?

보고는 Cloud Insights\* Premium Edition\*에서 사용할 수 있습니다.

## Active IQ의 향상된 기능

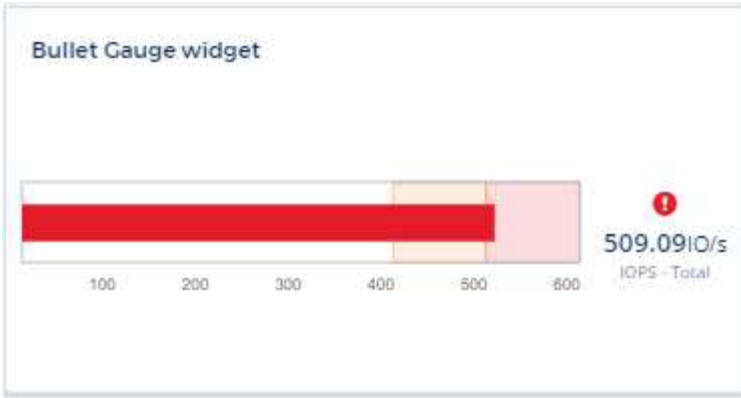
"Active IQ 위험" 이제 대시보드 표 위젯에서 사용할 수 있을 뿐만 아니라 쿼리할 수 있는 객체로 사용할 수 있습니다. 다음과 같은 위험 개체 특성이 포함됩니다. \* 범주 \* 완화 범주 \* 잠재적 영향 \* 위험 세부 정보 \* 심각도 \* 소스 \* 스토리지 \* 스토리지 노드 \* UI 범주

## 2019년 9월

### 새 게이지 위젯

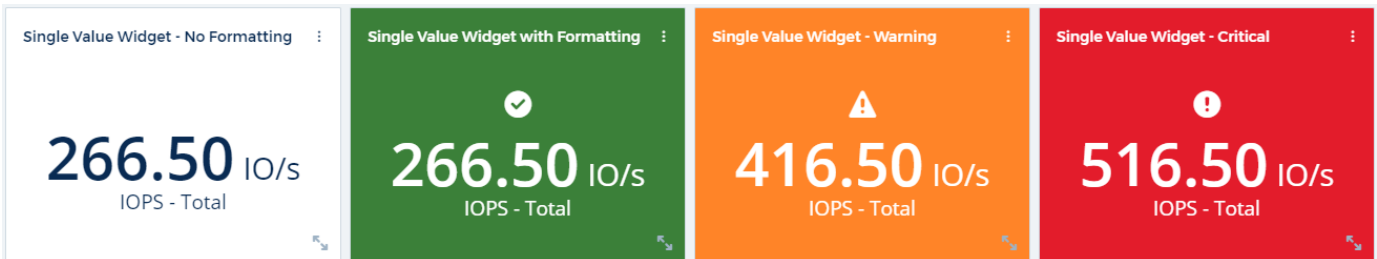
지정한 임계값을 기준으로 한 시선을 사로잡는 색상으로 대시보드에 단일 값 데이터를 표시하는 데 사용할 수 있는 두 가지 새로운 위젯이 있습니다. 단색 게이지 \* 또는 \* 글머리 기호 게이지 \* 를 사용하여 값을 표시할 수 있습니다. 경고 범위 내에 있는 값은 주황색으로 표시됩니다. 위험 범위의 값은 빨간색으로 표시됩니다. 경고 임계값 미만의 값은 녹색으로 표시됩니다.





## 단일 값 위젯에 대한 조건부 색 서식

이제 설정한 임계값에 따라 배경색이 지정된 단일 값 위젯을 표시할 수 있습니다.



## 온보딩 중 사용자 초대

온보딩 프로세스 중 언제든지 관리자 > 사용자 관리 > + 사용자 를 클릭하여 Cloud Insights 환경에 추가 사용자를 초대할 수 있습니다. Onboarding이 완료되고 데이터가 수집되면 `_Guest_or_User_roles`를 사용하는 사용자는 더 큰 이점을 누릴 수 있습니다.

## Data Collector 상세 페이지 개선

데이터 수집기 세부 정보 페이지가 읽기 쉬운 형식으로 오류를 표시하도록 개선되었습니다. 이제 오류가 페이지의 개별 테이블에 표시되고, 데이터 수집기에 여러 오류가 발생할 경우 각 오류가 별도의 줄에 표시됩니다.

# 2019년 8월

## 올과 사용 가능한 데이터 수집기

데이터 수집기를 환경에 추가할 때 구독 수준 또는 모든 데이터 수집기에 따라 사용 가능한 데이터 수집기만 표시하도록 필터를 설정할 수 있습니다.

## ActiveIQ 통합

Cloud Insights는 NetApp ActiveIQ에서 데이터를 수집하여 NetApp 고객과 고객의 하드웨어/소프트웨어 시스템에 일련의 시각화, 분석 및 기타 지원 관련 서비스를 제공합니다. Cloud Insights는 ONTAP 데이터 관리 시스템과 통합됩니다. 을 참조하십시오 "Active IQ" 를 참조하십시오.

---

## 2019년 7월

### 대시보드 개선 사항

대시보드와 위젯이 다음과 같은 변경 사항으로 개선되었습니다.

- Sum, Min, Max, Avg 외에도 \* Count \* 는 단일 값 위젯에서 롤업하는 옵션입니다. "Count"로 롤업할 때 Cloud Insights는 개체가 활성 상태인지 여부를 확인하고 활성 개체만 카운트에 추가합니다. 결과 숫자는 집계 및 필터의 영향을 받습니다.
- 단일 값 위젯에서 결과 숫자를 0, 1, 2, 3 또는 4개의 소수 자릿수로 표시하도록 선택할 수 있습니다.
- 꺾은선형 차트는 단일 카운터를 플롯할 때 축 레이블과 단위를 표시합니다.
- 모든 메트릭에 대한 모든 시계열 위젯에서 서비스 통합 데이터에 \* Transform \* 옵션을 사용할 수 있습니다. 시간 시리즈 위젯(라인, 스프라인, 영역, 스택 영역)의 모든 서비스 통합(Telegraf) 카운터 또는 메트릭의 경우 원하는 방법을 선택할 수 있습니다 **"값을 변환합니다"**. 없음(표시 값 - 현재 상태), 합계, 델타, 누적 등

### 기본 버전으로 다운그레이드

지난 7일 동안 설문을 성공적으로 완료한 사용 가능한 NetApp 장치가 구성되지 않은 경우 Basic Edition으로 다운그레이드할 수 없으며 오류 메시지가 표시됩니다.

### Kubbe-State-Metrics 수집 중

를 클릭합니다 **"Kubernetes Data Collector를 참조하십시오"** 이제 kubbe-state-metrics 플러그인에서 객체와 카운터를 수집하여 Cloud Insights에서 모니터링할 수 있는 메트릭의 수와 범위를 크게 확장할 수 있습니다.

---

## 2019년 6월

### Cloud Insights 에디션

Cloud Insights는 고객의 예산과 비즈니스 요구에 맞게 다양한 버전으로 제공됩니다. NetApp Support 계정이 유효한 기존 NetApp 고객은 무료 \* Basic Edition \* 을 통해 7일 동안 데이터를 보존하고 NetApp 데이터 수집기에 액세스할 수 있습니다. 또는 \* Standard Edition \* 을 통해 지원되는 모든 데이터 수집기에 대한 액세스, 전문가 기술 지원 등을 이용할 수 있습니다. 사용 가능한 기능에 대한 자세한 내용은 NetApp을 참조하십시오 **"Cloud Insights"** 사이트.

### 새로운 인프라 데이터 수집기: NetApp HCI

- **"NetApp HCI 가상 센터"** 인프라 데이터 수집기로 추가되었습니다. HCI 가상 센터 데이터 수집기는 NetApp HCI 호스트 정보를 수집하며 가상 센터 내의 모든 개체에 대해 읽기 전용 권한이 필요합니다.

HCI 데이터 수집기는 HCI 가상 센터에서만 가져옵니다. 스토리지 시스템에서 데이터를 수집하려면 NetApp도 구성해야 합니다 **"SolidFire"** 데이터 수집기.

## 2019년 5월

### 새로운 서비스 데이터 수집기: Kapacitor

- "[Kapacitor](#)" 은(는) 서비스를 위한 데이터 수집기로 추가되었습니다.

### Telegraf를 통한 서비스 통합

Cloud Insights는 이제 스위치 및 스토리지와 같은 인프라 장치에서 데이터를 수집하는 것은 물론, 를 사용하여 다양한 운영 체제 및 서비스에서 데이터를 수집합니다 "[텔레프도 요원으로 등장했다](#)" 통합 데이터 수집용. Telegraf는 메트릭을 수집 및 보고하는 데 사용할 수 있는 플러그인 기반 에이전트입니다. 입력 플러그인은 시스템/OS에 직접 액세스하거나 타사 API를 호출하거나 구성된 스트림을 수신함으로써 에이전트로 원하는 정보를 수집하는 데 사용됩니다.

현재 지원되는 통합에 대한 설명서는 \* [참조 및 지원](#) \* 의 왼쪽 메뉴에서 찾을 수 있습니다.

### 스토리지 가상 시스템 자산

- Cloud Insights에서 SVM(스토리지 가상 머신)을 자산으로 사용할 수 있습니다. SVM에는 자체 자산 랜딩 페이지가 있으며 검색, 쿼리 및 필터에 표시 및 사용할 수 있습니다. SVM은 대시보드 위젯과 주식에도 사용할 수 있습니다.

### 획득 장치 시스템 요구 사항 감소

- 획득 장치(AU) 소프트웨어의 시스템 CPU 및 메모리 요구 사항이 감소했습니다. 새로운 요구 사항은 다음과 같습니다.

* 구성 요소 *	* 이전 요건 *	* 새로운 요구사항 *
CPU 코어	4	2
메모리	16GB	8GB

### 추가 플랫폼 지원

- 현재 추가된 플랫폼은 다음과 같습니다 "[Cloud Insights에 대해 지원됩니다](#)":

리눅스	Windows
CentOS 7.3 64비트 CentOS 7.4 64비트 CentOS 7.6 64비트 Debian 9 64비트 Red Hat Enterprise Linux 7.3 64비트 Red Hat Enterprise Linux 7.4 64비트 Red Hat Enterprise Linux 7.6 64비트 Ubuntu Server 18.04 LTS	Microsoft Windows 10 64비트 Microsoft Windows Server 2008 R2 Microsoft Windows Server 2019

## 2019년 4월

### 태그별로 가상 머신을 필터링합니다

다음 데이터 수집기를 구성할 때 태그 또는 레이블에 따라 데이터 모음에서 가상 컴퓨터를 포함하거나 제외하도록 필터링할 수 있습니다.



- ["Amazon EC2"](#)
  - ["Azure를 지원합니다"](#)
  - ["Google 클라우드 플랫폼"](#)
- 

## 2019년 3월

### 구독 관련 이벤트에 대한 이메일 알림

- 이메일을 보낼 수신자를 선택할 수 있습니다 ["알림"](#) 향후 평가판 만료 또는 구독한 계정 변경 등의 구독 관련 이벤트가 발생하는 경우 다음 중 이러한 알림의 수신자를 선택할 수 있습니다.
  - 모든 계정 소유자
  - 모든 관리자
  - 사용자가 지정하는 추가 전자 메일 주소입니다

### 추가 대시보드

- 다음 새로운 AWS 중심 ["대시보드"](#) 갤러리에 추가되었으며 가져올 수 있습니다.
    - AWS 관리 - 수요가 많은 EC2는 무엇입니까?
    - 지역별 AWS EC2 인스턴스 성능
- 

## 2019년 2월

### AWS 하위 계정에서 수집 중

- Cloud Insights 지원 ["AWS 하위 계정에서 컬렉션"](#) 단일 데이터 수집기 내에서 Cloud Insights가 하위 계정에서 수집하도록 AWS 환경을 구성해야 합니다.

### 데이터 수집기 이름 지정

- 이제 Data Collector 이름에는 문자, 숫자 및 밑줄 외에도 마침표(.), 하이픈(-) 및 공백()이 포함될 수 있습니다. 이름은 공백, 마침표 또는 하이픈으로 시작하거나 끝날 수 없습니다.

### Windows용 획득 장치

- Windows 서버/VM에서 Cloud Insights 획득 장치를 구성할 수 있습니다. 창을 검토합니다 ["필수 구성 요소"](#) 를 설치하기 전에 ["획득 장치 소프트웨어"](#).
-

## 2019년 1월

### "소유자" 필드를 보다 쉽게 읽을 수 있습니다

- 대시보드 및 쿼리 목록에서 "소유자" 필드의 데이터는 이전에 사용자에게 친숙한 소유자 이름 대신 인증 ID 문자열이었습니다. 이제 "소유자" 필드에 보다 간단하고 읽기 쉬운 소유자 이름이 표시됩니다.

### 구독 페이지의 관리 단위 구분

- Admin > Subscription \* 페이지에 나열된 각 데이터 수집기에 대해 호스트 및 스토리지에 대한 관리 단위(MU) 수와 총계를 볼 수 있습니다.

## 2018년 12월

### UI 로드 시간 개선

- Cloud Insights UI(사용자 인터페이스)의 초기 로딩 시간이 크게 개선되었습니다. UI의 새로 고침 시간은 메타데이터가 로드된 경우에도 이와 같은 개선 효과를 얻을 수 있습니다.

### 데이터 수집기 대량 편집

- 여러 데이터 수집기에 대한 정보를 동시에 편집할 수 있습니다. 관측성 > 수집기 \* 페이지에서 각 항목의 왼쪽 확인란을 선택하고 \* Bulk Actions \* 버튼을 클릭하여 수정할 데이터 수집기를 선택합니다. 편집 \* 을 선택하고 필요한 필드를 수정합니다.

선택한 데이터 수집기는 동일한 공급업체 및 모델이어야 하며 동일한 획득 장치에 있어야 합니다.

### 지원 및 가입 페이지는 온보딩 중에 제공됩니다

- 온보딩 워크플로우 중에 \* 도움말 > 지원 \* 및 \* 관리 > 구독 \* 페이지로 이동할 수 있습니다. 이 페이지에서 다시 돌아오면 브라우저 탭을 닫지 않은 경우 온보딩 워크플로우로 돌아갑니다.

## 2018년 11월

### NetApp 영업 또는 AWS 마켓플레이스를 통해 구독하십시오

- Cloud Insights 구독 및 청구 기능은 이제 NetApp을 통해 직접 이용할 수 있습니다. 이 외에도 AWS Marketplace를 통해 셀프 서비스 방식으로 구독할 수 있습니다. Admin > Subscription \* 페이지에 새로운 \* Contact Sales \* 링크가 표시됩니다. 환경 하나 또는 하나 이상의 Managed Unit(MU)이 있을 것으로 예상되는 고객의 경우 연락처 영업 링크를 통해 NetApp 세일즈 팀에 문의하는 것이 좋습니다.

### 텍스트 주석 하이퍼링크

- 이제 텍스트 유형 주석에 하이퍼링크를 포함할 수 있습니다.

## 온보딩 연습

- 이제 Cloud Insights는 새 환경에 로그인하기 위한 첫 번째 사용자(관리자 또는 계정 소유자)의 온보딩 연습을 제공합니다. 이 연습에서는 획득 장치 설치, 초기 데이터 수집기 구성 및 하나 이상의 유용한 대시보드를 선택하는 과정을 안내합니다.

## 갤러리에서 대시보드를 가져옵니다

- 온보딩 중에 대시보드를 선택하는 것 외에도 \* 대시보드 > 모든 대시보드 표시 \* 를 통해 대시보드를 가져오고 \* + 갤러리 \* 에서 \* 를 클릭할 수 있습니다.

## 대시보드 복제

- 대시보드 목록 페이지에 대시보드를 복제하는 기능이 각 대시보드의 옵션 메뉴와 \_Save\_menu 에서 대시보드의 기본 페이지 자체에 선택 항목으로 추가되었습니다.

## Cloud Central 제품 메뉴

- 다른 NetApp Cloud Central 제품으로 전환할 수 있는 메뉴가 화면 오른쪽 상단 모서리로 이동했습니다.

# Data Infrastructure Insights 온보딩

데이터 인프라 인사이트 작업을 시작하기 전에 \* NetApp BlueXP \* 포털에 등록해야 합니다. NetApp BlueXP 로그인을 이미 가지고 있는 경우 몇 가지 간단한 단계를 통해 데이터 인프라 인사이트 무료 평가판을 시작할 수 있습니다.

## NetApp BlueXP 계정 생성

NetApp 클라우드 서비스를 시작하려면 로 이동하십시오 **"\* NetApp BlueXP \*"** 를 클릭하고 \* 시작하기 \* 를 클릭합니다.

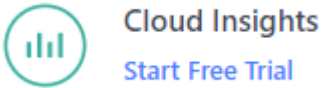
- 아직 등록하지 않은 경우 \* 등록 \* 을 선택합니다
- 유효한 업무용 전자 메일 주소를 입력하고 암호를 선택하십시오.
- 회사 이름과 전체 이름을 입력합니다.
- 이용 약관에 동의하고 \* 계속 \* 을 선택합니다.
- BlueXP가 시작하는 과정을 안내합니다.

## NetApp BlueXP 로그인을 이미 가지고 있는 경우에는 어떻게 해야 할까요?

NetApp BlueXP 계정이 있는 경우 에서 \* 로그인 \* 을 선택하면 됩니다 **"\* NetApp BlueXP \*"** 포털 페이지.

이메일 주소와 비밀번호를 입력합니다. 그런 다음 NetApp의 클라우드 오퍼링 페이지로 이동합니다.

Data Infrastructure Insights를 선택합니다.



## Data Infrastructure Insights 무료 평가판을 시작하십시오

Data Infrastructure Insights에 처음 로그인하는 경우 Data Infrastructure Insights 제품 아래에서 \* 무료 평가판 시작 \* 을 클릭합니다. Data Infrastructure Insights는 환경을 상주할 지역을 선택하는 등 회사 환경을 생성하는 과정을 안내합니다.

Please choose your AWS region.



환경 생성이 완료되면 BlueXP 자격 증명을 사용하여 로그인하여 Data Infrastructure Insights의 30일 무료 평가판을 시작할 수 있습니다. 이 평가판을 통해 Data Infrastructure Insights에서 제공하는 기능을 살펴볼 수 있습니다.

무료 평가판에서는 "구독을 시작합니다"언제든지 Data Infrastructure Insights를 사용할 수 있습니다. 구독하면 현재 구독에 따라 Data Infrastructure Insights 기능을 사용할 수 있습니다.

## 로그인 후 이동

환경이 생성되면 언제든지 NetApp BlueXP 포털에 로그인하고 \* 데이터 인프라 인사이트 \* 로 이동 \* 을 클릭하면 됩니다. Data Infrastructure Insights 환경으로 바로 이동할 수 있습니다.

또한 Data Infrastructure Insights 환경 URL에서 브라우저를 직접 열 수 있습니다. 예를 들면 다음과 같습니다.

```
\https://<environment-prefix>.c01.cloudinsights.netapp.com/
```

URL은 각 사용자의 초대 이메일에도 포함되어 있어 간단한 액세스와 북마크 기능을 제공합니다. 사용자가 BlueXP에 아직 로그인하지 않은 경우 로그인하라는 메시지가 표시됩니다.



신규 사용자가 환경 URL에 액세스하려면 먼저 BlueXP에 대한 액세스를 등록해야 합니다.

새 환경에 처음 로그인할 때 에서 로 설정하는 과정을 안내합니다 **"\* 데이터 수집 시작 \***".

## 로그아웃하는 중입니다

Data Infrastructure Insights에서 로그아웃하려면 \* 사용자 이름 \* 을 클릭하고 \* 로그아웃 \* 을 선택합니다. BlueXP 로그인 화면으로 돌아갑니다.



데이터 인프라 Insights에서 로그아웃하면 BlueXP 에서 로그아웃됩니다. BlueXP 로그인을 사용하는 다른 NetApp 클라우드 서비스에서도 로그아웃됩니다.

## 비활성 시간 초과

기본적으로 BlueXP는 6시간(360분) 동안 활동이 없는 경우 사용자를 로그아웃합니다. 활동에 관계없이 사용자는 7일 후에 로그아웃됩니다.

# 보안

## Data Infrastructure Insights 보안

NetApp에게 제품 및 고객 데이터 보안은 무엇보다도 중요합니다. Data Infrastructure Insights는 릴리스 라이프사이클 전반에 걸쳐 보안 모범 사례를 준수하여 고객 정보와 데이터를 최상의 방법으로 보호합니다.

### 보안 개요

#### 물리적 보안

Data Infrastructure Insights 운영 인프라는 AWS(Amazon Web Services)에서 호스팅됩니다. 건물, 문에 사용되는 잠금 또는 키를 비롯한 Data Infrastructure Insights 프로덕션 서버에 대한 물리적 및 환경적 보안 관련 제어가 AWS에서 관리됩니다. AWS에 따라: “물리적 액세스는 비디오 감시, 침입 탐지 시스템 및 기타 전자 수단을 활용하는 전문 보안 직원이 경계와 건물 진입점에서 모두 제어합니다. 공인 직원은 다중 요소 인증 메커니즘을 사용하여 데이터 센터 바닥에 액세스합니다.”

Data Infrastructure Insights는 "공유 책임 모델" AWS에서 설명한 의 모범 사례를 따릅니다.

#### 제품 보안

Data Infrastructure Insights는 애자일 원칙에 따라 개발 라이프사이클을 따르므로 릴리스 주기 개발 방법론에 비해 보안 지향 소프트웨어 결함을 보다 신속하게 해결할 수 있습니다. 지속적인 통합 방법을 사용하여 기능 및 보안 변경 사항에 신속하게 대응할 수 있습니다. 변경 관리 절차 및 정책은 변경 발생 시기와 방법을 정의하고 운영 환경의 안정성을 유지하는 데 도움이 됩니다. 영향력 있는 변경 사항은 생산 환경에 배포하기 전에 공식적으로 전달, 조정, 적절하게 검토 및 승인됩니다.

#### 네트워크 보안

Data Infrastructure Insights 환경의 리소스에 대한 네트워크 액세스는 호스트 기반 방화벽으로 제어됩니다. 각 리소스(예: 로드 밸런서 또는 가상 머신 인스턴스)에는 인바운드 트래픽을 해당 리소스가 기능을 수행하는 데 필요한 포트만 제한하는 호스트 기반 방화벽이 있습니다.

Data Infrastructure Insights는 침입 감지 서비스를 비롯한 다양한 메커니즘을 사용하여 프로덕션 환경의 보안 이상 징후를 모니터링합니다.

#### 위험 평가

Data Infrastructure Insights 팀은 위험 치료 계획을 통해 적절히 관리할 수 있도록 위험을 식별하고 평가하는 체계적이고 반복 가능한 방법을 제공하는 공식화된 위험 평가 프로세스를 따릅니다.

#### 데이터 보호

Data Infrastructure Insights 운영 환경은 모든 서비스 및 구성 요소에 대해 여러 가용 영역을 사용하는 매우 이중화된 인프라에 설정됩니다. 가용성이 높고 이중화된 컴퓨팅 인프라를 활용하는 동시에 중요한 데이터가 정기적으로 백업되고 복원이 정기적으로 테스트됩니다. 공식적인 백업 정책 및 절차는 비즈니스 활동 중단에 영향을 최소화하고 정보 시스템 또는 재해의 실패로부터 비즈니스 프로세스를 보호하며 시기 적절하고 적절한 재개를 보장합니다.

## 인증 및 액세스 관리

Data Infrastructure Insights에 대한 모든 고객은 https를 통한 브라우저 UI 상호 작용을 통해 액세스할 수 있습니다. 인증은 타사 서비스인 Auth0을 통해 수행됩니다. NetApp은 이를 모든 클라우드 데이터 서비스의 인증 계층으로 중앙 집중화하고 있습니다.

Data Infrastructure Insights는 Data Infrastructure Insights 운영 환경에 대한 논리적 액세스와 관련하여 "최소 권한" 및 "역할 기반 액세스 제어"를 비롯한 업계 모범 사례를 따릅니다. 액세스 권한은 엄격한 요구 사항에 따라 제어되며 다중 요소 인증 메커니즘을 사용하는 권한이 있는 일부 직원에게만 부여됩니다.

## 고객 데이터의 수집 및 보호

모든 고객 데이터는 공용 네트워크를 통해 전송 중에 암호화되고 저장된 데이터는 암호화됩니다. Data Infrastructure Insights는 TLS(전송 계층 보안) 및 업계 표준 AES-256 알고리즘을 포함한 기술을 사용하여 시스템의 다양한 지점에서 암호화를 활용하여 고객 데이터를 보호합니다.

## 고객 프로비저닝 해제

이메일 알림은 고객에게 구독이 만료됨을 알리기 위해 다양한 간격으로 발송됩니다. 구독이 만료되면 UI가 제한되고 데이터 수집을 위한 유예 기간이 시작됩니다. 그러면 고객에게 이메일을 통해 알립니다. 평가판 구독의 경우 14일의 유예 기간이 있으며 유료 구독 계정의 유예 기간은 28일입니다. 유예 기간이 만료된 후 고객은 이메일을 통해 계정을 2일 이내에 삭제할 것이라는 알림을 받습니다. 유료 고객은 서비스 종료 요청을 직접 할 수도 있습니다.

만료된 테넌트 및 모든 관련 고객 데이터는 유예 기간이 끝났거나 고객의 계정 종료 요청이 확인된 경우 Data Infrastructure Insights Operations(SRE) 팀에서 삭제합니다. 두 경우 모두 SRE 팀은 API 호출을 실행하여 계정을 삭제합니다. API 호출은 테넌트 인스턴스와 모든 고객 데이터를 삭제합니다. 동일한 API를 호출하고 고객 테넌트 상태를 "삭제됨"인지 확인하여 고객 삭제를 확인합니다.

## 보안 사고 관리

Data Infrastructure Insights는 NetApp의 제품 보안 사고 대응 팀(PSIRT) 프로세스와 통합되어 알려진 취약점을 찾고, 평가하고, 해결합니다. PSIRT는 고객 보고서, 내부 엔지니어링 및 CVE 데이터베이스와 같이 널리 알려진 소스를 비롯한 여러 채널의 취약점 정보를 포함합니다.

Data Infrastructure Insights 엔지니어링 팀에서 문제를 감지한 경우 팀은 PSIRT 프로세스를 시작하고 문제를 평가 및 잠재적으로 해결합니다.

또한 Data Infrastructure Insights 고객 또는 연구자가 Data Infrastructure Insights 제품의 보안 문제를 식별하고 이 문제를 기술 지원팀에 보고하거나 NetApp의 사고 대응 팀에 직접 보고할 수도 있습니다. 이 경우 Data Infrastructure Insights 팀은 PSIRT 프로세스를 시작하고 문제를 평가 및 잠재적으로 해결합니다.

## 취약점 및 침투 테스트

Data Infrastructure Insights는 업계 모범 사례를 따르며 내부 및 외부 보안 전문가와 회사를 통해 정기적인 취약성 및 모의 해킹 테스트를 수행합니다.

## 보안 인식 교육

모든 Data Infrastructure Insights 직원은 각 직원이 각자의 역할에 맞는 특정 보안 관련 과제를 처리할 수 있도록 개별 역할에 맞게 개발된 보안 교육을 이수해야 합니다.

## 규정 준수

Data Infrastructure Insights는 외부의 인가된 CPA 회사를 통해 SOC 2 감사 완료와 더불어 보안성, 프로세스 및 서비스에 대한 독립된 제3자 감사 및 검증을 수행합니다.

## NetApp 보안 권고

NetApp의 사용 가능한 보안 보고서를 볼 수 있습니다 ["여기"](#).

## 정보 및 지역

NetApp은 고객 정보의 보안을 매우 중요하게 생각합니다. Data Infrastructure Insights에서 정보를 저장하는 방법과 위치를 확인하십시오.

### Data Infrastructure Insights는 어떤 정보를 저장합니까?

Data Infrastructure Insights는 다음 정보를 저장합니다.

- 성능 데이터

성능 데이터는 모니터링되는 장치/소스의 성능에 대한 정보를 제공하는 시계열 데이터입니다. 예를 들어, 스토리지 시스템에서 제공되는 입출력 수, FiberChannel 포트의 처리량, 웹 서버에서 제공하는 페이지 수, 데이터베이스의 응답 시간 등이 여기에 포함됩니다.

- 재고 데이터

인벤토리 데이터는 모니터링되는 디바이스/소스와 해당 소스 구성 방법을 설명하는 메타데이터로 구성됩니다. 여기에는 설치된 하드웨어 및 소프트웨어 버전, 스토리지 시스템의 디스크 및 LUN, CPU 코어, 가상 머신의 RAM 및 디스크, 데이터베이스의 테이블스페이스, SAN 스위치의 포트 수와 유형, 디렉토리/파일 이름(스토리지 워크로드 보안이 설정된 경우) 등이 포함됩니다.

- 구성 데이터

이 요약에는 모니터링된 장치의 호스트 이름 또는 IP 주소, 폴링 간격, 시간 초과 값 등 고객 인벤토리 및 작업을 관리하는 데 사용되는 고객이 제공한 구성 데이터가 요약되어 있습니다.

- 비밀

비밀은 Data Infrastructure Insights Acquisition Unit에서 고객 장치 및 서비스에 액세스하는 데 사용하는 자격 증명으로 구성됩니다. 이러한 자격 증명은 강력한 비대칭 암호화를 사용하여 암호화되며 개인 키는 획득 장치에만 저장되며 고객 환경을 떠나지 않습니다. 권한 있는 Data Infrastructure Insights SRE도 이 설계 때문에 일반 텍스트로 고객 비밀에 액세스할 수 없습니다.

- 기능 데이터

이 데이터는 NetApp에서 클라우드 데이터 서비스를 제공하여 생성되는 것으로, 클라우드 데이터 서비스의 개발, 구축, 운영, 유지보수, 보안에 대해 NetApp에 알려줍니다. 기능 데이터에는 고객 정보 또는 개인 정보가 포함되어 있지 않습니다.

- 사용자 액세스 데이터



사용자 권한 부여와 관련된 데이터를 포함하여 NetApp BlueXP 이 지역 데이터 인프라 인사이트 사이트와 통신할 수 있도록 하는 인증 및 액세스 정보입니다.

- 스토리지 워크로드 보안 사용자 디렉토리 데이터

워크로드 보안 기능이 활성화되어 있고 고객이 사용자 디렉토리 수집기를 사용하도록 선택한 경우 시스템은 사용자 표시 이름, 회사 이메일 주소 및 Active Directory에서 수집한 기타 정보를 저장합니다.



사용자 디렉토리 데이터는 Data Infrastructure Insights/Workload Security 자체의 사용자에게 대한 데이터가 아니라 워크로드 보안 사용자 디렉토리 데이터 수집기에서 수집한 사용자 디렉토리 정보를 말합니다.

- 인프라 및 서비스 리소스에서 명시적 개인 데이터 \* 가 수집되지 않습니다. 수집된 정보는 성능 메트릭, 구성 정보 및 인프라 메타데이터로만 구성되며, NetApp의 자동 지원 및 ActiveIQ를 비롯한 수많은 공급업체 Phone-Home과 매우 유사합니다. 그러나 고객의 명명 규칙에 따라 공유, 볼륨, VM, qtree, 응용 프로그램 등에 개인 식별 정보가 포함될 수 있습니다.

워크로드 보안이 설정된 경우 시스템은 SMB 또는 기타 공유에서 파일 및 디렉토리 이름을 추가로 확인합니다. 여기에는 개인 식별 정보가 포함될 수 있습니다. 고객이 워크로드 보안 사용자 디렉토리 수집기를 활성화하면(기본적으로 Active Directory를 통해 Windows SID를 사용자 이름에 매핑), 표시 이름, 회사 이메일 주소 및 선택된 추가 속성이 Data Infrastructure Insights에 의해 수집되고 저장됩니다.

또한 Data Infrastructure Insights에 대한 액세스 로그는 유지 관리되며 서비스에 로그인하는 데 사용되는 사용자의 IP 및 이메일 주소를 포함합니다.

## 내 정보는 어디에 저장되니까?

Data Infrastructure Insights는 환경이 생성되는 지역에 따라 정보를 저장합니다.

다음 정보는 호스트 영역에 저장됩니다.

- 카운터 및 성능 메트릭을 포함한 원격 측정 및 자산/객체 정보
- 획득 장치 정보
- 기능 데이터
- Data Infrastructure Insights 내의 사용자 활동에 대한 정보 감사
- 워크로드 보안 Active Directory 정보
- 워크로드 보안 감사 정보

다음 정보는 Data Infrastructure Insights 환경을 호스팅하는 지역에 상관없이 미국에 있습니다.

- 사이트/계정 소유자와 같은 환경 사이트("테넌트"라고도 함) 정보
- 사용자 승인과 관련된 모든 작업을 포함하여 NetApp BlueXP 이 지역별 데이터 인프라 인사이트 사이트와 통신할 수 있도록 하는 정보.
- Data Infrastructure Insights 사용자와 테넌트 간의 관계와 관련된 정보입니다.

## 호스트 영역

호스트 영역은 다음과 같습니다.

- 미국: 동쪽편 - 1
- EMEA: EU-CENTRAL-1
- APAC: AP-남동-2

## 추가 정보

다음 링크에서 NetApp의 개인 정보 보호 및 보안에 대해 자세히 확인할 수 있습니다.

- ["보안 센터"](#)
- ["국가 간 데이터 전송"](#)
- ["기업 규칙을 구속하는 중입니다"](#)
- ["타사 데이터 요청에 대한 응답"](#)
- ["NetApp 개인 정보 보호 원칙"](#)

## SecurityAdmin 도구

Data Infrastructure Insights에는 환경을 향상된 보안으로 운영할 수 있는 보안 기능이 포함되어 있습니다. 암호화, 암호 해싱의 개선, 내부 사용자 암호 변경 기능, 암호 암호화 및 암호 해독을 위한 키 쌍 등의 기능이 있습니다.

중요한 데이터를 보호하려면 설치 또는 업그레이드 후에 기본 키와 `_Acquisition_user` 암호를 변경하는 것이 좋습니다.

데이터 소스의 암호화된 암호는 사용자가 데이터 수집기 구성 페이지에 입력할 때 공개 키를 사용하여 암호를 암호화하는 Data Infrastructure Insights에 저장됩니다. Data Infrastructure Insights에는 데이터 수집기 암호를 해독하는 데 필요한 개인 키가 없습니다. AUS(Acquisition Unit)에만 데이터 수집기 암호를 해독하는 데 필요한 데이터 수집기 개인 키가 있습니다.

## 업그레이드 및 설치 고려 사항

Insight 시스템에 기본이 아닌 보안 구성(예: 암호 키 다시 입력)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.

## 획득 장치의 보안 관리

SecurityAdmin 도구를 사용하면 Data Infrastructure Insights의 보안 옵션을 관리할 수 있으며 획득 장치 시스템에서 실행됩니다. 보안 관리에는 키 및 암호 관리, 사용자가 만들고 복원한 보안 구성을 기본 설정으로 저장 및 복원하는 작업이 포함됩니다.

## 시작하기 전에

- 획득 장치 소프트웨어(SecurityAdmin 도구 포함)를 설치하려면 AU 시스템에 대한 관리자 권한이 있어야 합니다.
- 나중에 SecurityAdmin 도구에 액세스해야 하는 관리자가 아닌 사용자가 있는 경우 `_cisys_group`에 추가해야 합니다. AU 설치 중에 `_cisys_group`이 생성됩니다.

AU 설치 후 다음 위치 중 하나에 있는 획득 장치 시스템에서 SecurityAdmin 도구를 찾을 수 있습니다.

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

## SecurityAdmin 도구 사용

대화형 모드(-i)에서 SecurityAdmin 도구를 시작합니다.



명령줄에서 암호를 전달하지 않도록 대화형 모드에서 SecurityAdmin 도구를 사용하는 것이 좋습니다. 이 도구는 로그에 캡처될 수 있습니다.

다음 옵션이 표시됩니다.

```
[root@ci-qa-xitij-cis2-28594linau bin]# ./securityadmin -i
Select Action:

1 - Backup
2 - Restore
3 - Register / Update External Key Retrieval Script
4 - Rotate Encryption Keys
5 - Reset to Default Keys
6 - Change Truststore Password
7 - Change Keystore Password
8 - Encrypt Collector Password
9 - Exit

Enter your choice: █
```

### 1. \* 백업 \*

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

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

볼트 백업은 중요한 정보를 포함하기 때문에 안전하게 유지하는 것이 좋습니다.

### 2. \* 복원 \*

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

복원은 여러 서버의 암호 및 키를 동기화하는 데 사용할 수 있습니다. 예를 들어 다음 단계를 사용합니다. 1) AU의 암호화 키 변경 2) 볼트 백업을 작성합니다. AUS 각각에 볼트 백업을 복원합니다.

### 3. \* 외부 키 검색 스크립트 등록/업데이트 \*

외부 스크립트를 사용하여 장치 암호를 암호화 또는 해독하는 데 사용되는 AU 암호화 키를 등록하거나 변경합니다.

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

참고 이 옵션은 Linux에서만 사용할 수 있습니다.

SecurityAdmin 도구와 함께 사용자 고유의 키 검색 스크립트를 사용하는 경우 다음 사항을 염두에 두십시오.

- 현재 지원되는 알고리즘은 최소 2048비트의 RSA입니다.
- 스크립트는 개인 키와 공개 키를 일반 텍스트로 반환해야 합니다. 스크립트는 암호화된 개인 키와 공개 키를 반환하지 않아야 합니다.
- 스크립트는 원시 인코딩된 내용을 반환해야 합니다(PEM 형식만 해당).
- 외부 스크립트에는 `_execute_permissions` 가 있어야 합니다.

### 4. \* 암호화 키 회전 \*

암호화 키를 회전합니다(현재 키 등록 취소 및 새 키 등록). 외부 키 관리 시스템의 키를 사용하려면 공개 키 ID와 개인 키 ID를 지정해야 합니다

### 5. \* 기본 키로 재설정 \*

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

### 6. \* truststore 암호 변경 \*

truststore의 암호를 변경합니다.

### 7. \* Keystore 암호 변경 \*

키 저장소의 암호를 변경합니다.

### 8. \* Collector 암호 암호화 \*

데이터 수집기 암호를 암호화합니다.

### 9. \* 종료 \*

SecurityAdmin 도구를 종료합니다.

구성할 옵션을 선택하고 화면의 지시를 따릅니다.

## 도구를 실행할 사용자 지정

보안을 중요시하는 통제된 환경에서 `_cisys_group`이 없지만 특정 사용자가 SecurityAdmin 도구를 실행하기를 원할 수

있습니다.

수동으로 AU 소프트웨어를 설치하고 액세스할 사용자/그룹을 지정하면 이 작업을 수행할 수 있습니다.

- API를 사용하여 CI 설치 프로그램을 AU 시스템에 다운로드하고 압축을 풉니다.
  - 1회 인증 토큰이 필요합니다. API Swagger 설명서(\_Admin > API Access \_ 및 \_API Documentation\_link 선택)를 참조하여 \_get/au/oneTimeToken\_API 섹션을 찾습니다.
  - 토큰이 있으면 \_get/au/installers/{platform}/{version}\_API를 사용하여 설치 관리자 파일을 다운로드합니다. 설치 프로그램 버전과 함께 플랫폼(Linux 또는 Windows)을 제공해야 합니다.
- 다운로드한 설치 관리자 파일을 AU 시스템에 복사하고 압축을 풉니다.
- 파일이 포함된 폴더로 이동하고 설치 관리자를 루트로 실행하고 사용자 및 그룹을 지정합니다.

```
./cloudinsights-install.sh <User> <Group>
```

지정된 사용자 및/또는 그룹이 없으면 해당 사용자 및/또는 그룹이 생성됩니다. 사용자는 SecurityAdmin 도구에 액세스할 수 있습니다.

## 프록시를 업데이트 또는 제거하는 중입니다

SecurityAdmin 도구는 \_-pr\_parameter로 도구를 실행하여 획득 장치에 대한 프록시 정보를 설정하거나 제거하는 데 사용할 수 있습니다.

```
[root@ci-eng-linau bin]# ./securityadmin -pr
usage: securityadmin -pr -ap <arg> | -h | -rp | -upr <arg>
```

The purpose of this tool is to enable reconfiguration of security aspects of the Acquisition Unit such as encryption keys, and proxy configuration, etc. For more information about this tool, please check the Data Infrastructure Insights Documentation.

```
-ap,--add-proxy <arg>          add a proxy server.  Arguments: ip=ip
                                port=port user=user password=password
                                domain=domain
                                (Note: Always use double quote(") or single
                                quote(') around user and password to escape
                                any special characters, e.g., <, >, ~, `, ^,
                                !
                                For example: user="test" password="t'!<@1"
                                Note: domain is required if the proxy auth
                                scheme is NTLM.)

-h,--help

-rp,--remove-proxy             remove proxy server

-upr,--update-proxy <arg>      update a proxy.  Arguments: ip=ip port=port
                                user=user password=password domain=domain
                                (Note: Always use double quote(") or single
                                quote(') around user and password to escape
                                any special characters, e.g., <, >, ~, `, ^,
                                !
                                For example: user="test" password="t'!<@1"
                                Note: domain is required if the proxy auth
                                scheme is NTLM.)
```

예를 들어 프록시를 제거하려면 다음 명령을 실행합니다.

```
[root@ci-eng-linau bin]# ./securityadmin -pr -rp
명령을 실행한 후 획득 장치를 다시 시작해야 합니다.
```

프록시를 업데이트하려면 명령은 입니다

```
./securityadmin -pr -upr <arg>
```

## 외부 키 검색

UNIX 셸 스크립트를 제공할 경우 획득 장치에서 이를 실행하여 키 관리 시스템에서 \* 개인 키 \* 및 \* 공개 키 \* 를 검색할

수 있습니다.

키를 검색하기 위해 Data Infrastructure Insights에서 스크립트를 실행하고 두 가지 매개 변수(*key id\_and\_key type*)를 전달합니다. `_Key id_`를 사용하여 키 관리 시스템의 키를 식별할 수 있습니다. `_키 유형_`은(는) "public" 또는 "private"입니다. 키 유형이 "public"인 경우 스크립트는 공개 키를 반환해야 합니다. 키 유형이 "private"인 경우 개인 키를 반환해야 합니다.

키를 다시 획득 장치로 보내려면 스크립트는 키를 표준 출력으로 인쇄해야 합니다. 스크립트는 `PRINT_ONLY_THE` 키를 표준 출력으로 가져와야 합니다. 다른 텍스트는 표준 출력으로 인쇄해서는 안 됩니다. 요청된 키가 표준 출력으로 인쇄되면 스크립트는 종료 코드가 0인 상태에서 종료되어야 합니다. 다른 반환 코드는 오류로 간주됩니다.

이 스크립트는 획득 장치와 함께 스크립트를 실행하는 SecurityAdmin 도구를 사용하여 획득 장치에 등록해야 합니다. 스크립트에는 root 및 "cisys" 사용자에게 대해 `_READ_AND_EXECUTE_` 권한이 있어야 합니다. 등록 후 셸 스크립트가 수정되면 수정된 셸 스크립트를 획득 장치에 다시 등록해야 합니다.

입력 매개 변수: 키 ID	고객 키 관리 시스템에서 키를 식별하는 데 사용되는 키 식별자입니다.
입력 매개 변수: 키 유형	퍼블릭 또는 프라이빗.
출력	요청된 키를 표준 출력으로 인쇄해야 합니다. 현재 2048비트 RSA 키가 지원됩니다. 키는 다음과 같은 형식으로 인코딩되고 인쇄되어야 합니다.  개인 키 형식 - PEM, DER로 인코딩된 PKCS8 PrivateKeyInfo RFC 5958  공개 키 형식 - PEM, DER로 인코딩된 X.509 SubjectPublicKeyInfo RFC 5280
종료 코드	종료 코드 0을(를) 성공했습니다. 다른 모든 종료 값은 실패로 간주됩니다.
스크립트 권한	스크립트에는 루트 및 "cisys" 사용자에게 대한 읽기 및 실행 권한이 있어야 합니다.
로그	스크립트 실행이 기록됩니다. 로그는 -  <code>/var/log/netapp/cloudinsights/SecurityAdmin/securityadmin.log</code> 으로 이동합니다  <code>/var/log/netapp/cloudinsights/acq/acq.log</code> 를 참조하십시오

## API에서 사용하기 위한 암호 암호화

옵션 8에서는 암호를 암호화하고 API를 통해 데이터 수집기로 전달할 수 있습니다.

대화형 모드에서 SecurityAdmin 도구를 시작하고 옵션 8: `_Encrypt Password_` 를 선택합니다.

```
securityadmin.sh -i
```

암호화할 암호를 입력하라는 메시지가 표시됩니다. 입력한 문자는 화면에 표시되지 않습니다. 메시지가 나타나면 암호를 다시 입력합니다.

또는 스크립트에서 명령을 사용할 경우 명령줄에서 "-enc" 매개 변수와 함께 \_SecurityAdmin.sh\_를 사용하여 암호화되지 않은 암호를 전달합니다.

```
securityadmin -enc mypassword  
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLI 예"]
```

암호화된 암호가 화면에 표시됩니다. 선행 또는 후행 기호를 포함하여 전체 문자열을 복사합니다.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i  
Select Action:  
  
1 - Backup  
2 - Restore  
3 - Change Encryption Keys  
4 - Reset to Default Keys  
5 - Check for Default Encryption Keys  
6 - Change Truststore Password  
7 - Change Keystore Password  
8 - Encrypt Password  
9 - Exit  
  
Enter your choice: 8  
Please enter your password to encrypt:  
Please confirm your password to encrypt:  
  
Your Encrypted Password below  
  
ciYJAMpdEncBsLQwF2gobbiER14Jrwb7tLW0fYhu0dERGZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/Zk1Bd8ggJiQ+tS/LZkmJ6XKgTDcf3LGn8UqzOy  
Rn0v5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreYLfpju0G5UmeZz1KGCT0aBTggrI/JIYyyn4wZLnG0w21  
LGm59vor70GU0iKZYabLd+7LpsdCCBi1eF86BCj2RkxX0of891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVklviCZ/WqkyQ==
```

암호화된 암호를 데이터 수집기에 보내려면 데이터 수집 API를 사용할 수 있습니다. 이 API의 Swagger는 \* Admin > API Access \* 에서 확인할 수 있으며 "API Documentation" 링크를 클릭하십시오. "데이터 수집" API 유형을 선택합니다. data\_collection.data\_collector\_heading 아래에서 이 예제에 대한 \_/collector/datasources\_POST API를 선택합니다.



**POST** /collector/datasources Create a data collector

Create a data collector

**Parameters** Try it out

Name	Description
preEncrypted boolean (query)	Optional, defaults to false. If preEncrypted query parameter set to true, directs server to treat all passed secret values as already encrypted  Default value : false

Request body required application/json

Example Value | Schema

```
{
  "acquisitionUnit": {
    "additionalProp1": "string",
    "additionalProp2": "string"
  }
}
```

\_preEncrypted\_option을 \_True\_로 설정하면 API 명령을 통해 전달하는 모든 암호는 \* 이미 암호화된 \* 로 처리되며 API는 암호를 다시 암호화하지 않습니다. API를 구축할 때 이전에 암호화된 암호를 적절한 위치에 붙여 넣기만 하면 됩니다.

<https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true>

```
{
  "name": "cdot-aaaaa",
  "config": {
    "dsTypeId": "93",
    "vendorModelId": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
            "J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnIBVsAWyLmORxFAw
            vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHftvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
            4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
            +nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQlM9QAYPoyw/JT0nXHDuf683uE
            K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

## API에서 사용하기 위한 암호 암호화

옵션 8에서는 암호를 암호화하고 API를 통해 데이터 수집기로 전달할 수 있습니다.

대화형 모드에서 SecurityAdmin 도구를 시작하고 옵션 8: `_Encrypt Password _` 를 선택합니다.

```
securityadmin.sh -i
```

암호화할 암호를 입력하라는 메시지가 표시됩니다. 입력한 문자는 화면에 표시되지 않습니다. 메시지가 나타나면 암호를 다시 입력합니다.

또는 스크립트에서 명령을 사용할 경우 명령줄에서 "-enc" 매개 변수와 함께 `_SecurityAdmin.sh_`를 사용하여 암호화되지 않은 암호를 전달합니다.

```
securityadmin -enc mypassword  
image:SecurityAdmin_Encrypt_Key_API_CLI_Example.png["CLI 예"]
```

암호화된 암호가 화면에 표시됩니다. 선행 또는 후행 기호를 포함하여 전체 문자열을 복사합니다.

```
[root@ci-eng-srivardh-learn bin]# securityadmin.sh -i  
Select Action:  
  
1 - Backup  
2 - Restore  
3 - Change Encryption Keys  
4 - Reset to Default Keys  
5 - Check for Default Encryption Keys  
6 - Change Truststore Password  
7 - Change Keystore Password  
8 - Encrypt Password  
9 - Exit  
  
Enter your choice: 8  
Please enter your password to encrypt:  
Please confirm your password to encrypt:  
  
Your Encrypted Password below  
  
ciYJAMPdEncBsLQwF2gobbiERl4Jrwb7tLW0FYhu0dERGZU3L+uWfcCXdNSXTWr6SFuumwsWVFib3h78vnM0s6vM7G/2k1Bd8ggJiQ+tS/LZkmJ6XKgTDcf3LGn8UqzQy  
Rn0v5jJBGip6nCysrt9dapsEiRVHrMJVr8btGYbb4Zoz62qudMfW9uQdm3qyzSKbIY0L0An89yDPC0kDkaXreyLfpju0G5UmeZz1KGCT0aBTggri/JIYyrr4w2ZLnG0w21  
LGm59vor70GU0iKZYablD+7LpsdCCBi1eF86BCj2RkxX0of891sHN+E7zTvZEofdGVWepc7b/HNah5XiXgVk1viCZ/WqkyQ==
```

암호화된 암호를 데이터 수집기에 보내려면 데이터 수집 API를 사용할 수 있습니다. 이 API의 Swagger는 \* Admin > API Access \* 에서 확인할 수 있으며 "API Documentation" 링크를 클릭하십시오. "데이터 수집" API 유형을 선택합니다. `data_collection.data_collector_heading` 아래에서 이 예제에 대한 `_/collector/datasources_POST` API를 선택합니다.

POST /collector/datasources Create a data collector

Create a data collector

Parameters Try it out

Name	Description
preEncrypted boolean (query)	Optional, defaults to false. If preEncrypted query parameter set to true, directs server to treat all passed secret values as already encrypted  Default value : false

Request body required application/json

Example Value | Schema

```
{  
  "acquisitionUnit": {  
    "additionalProp1": "string",  
    "additionalProp2": "string"  }  
}
```

\_preEncrypted\_option을 \_True\_로 설정하면 API 명령을 통해 전달하는 모든 암호는 \* 이미 암호화된 \* 로 처리되며 API는 암호를 다시 암호화하지 않습니다. API를 구축할 때 이전에 암호화된 암호를 적절한 위치에 붙여 넣기만 하면 됩니다.

<https://<TENANT URL>/rest/v1/collector/datasources?preEncrypted=true>

```
{
  "name": "cdot-aaaaa",
  "config": {
    "dsTypeid": "93",
    "vendorModelid": "1",
    "packages": [
      {
        "id": "foundation",
        "displayName": "Inventory",
        "isMandatory": true,
        "attributes": {
          "RELEASESTATUS": "OFFICIAL",
          "enabled": true,
          "ip": "10.62.219.30",
          "user": "admin",
          "password":
            "J8bepjwz9oNknfs6mcqbz3zuEThZQp1VyTk+1wE05gWwmmj1u0CB688nfOnB1xnIBVsAWyLmORxFAw
            vcDCvGbTraqp/+nT0k94LO8Z7Q04I5KqhHftvINGU54S4IVLWiMIFj8kSU4RhMvNNNq5Tarz0gJZhWR+
            4RoNF+84R/uFFGwKeblrwfHxWZZMoW7pEJ2kzLFBtBzx2mUvRP0kn6AFbyS4+DM2YTPQkSk3W2Gzc
            +nfPDDyH8Tq6AM5WsVCKqnZAa2ZIY1FxMkKT7iFt5oiYnl93ka7OrQlM9QAYPoyw/JT0nXHDuf683uE
            K32yn9CgxNGXy5NcNzRurdFNb5w=="
        }
      },
      {
        "id": "storageperformance",
        "displayName": "Array Performance",
        "isMandatory": false,
        "attributes": {
          "password": "this will not be encrypted on the server side"
        }
      }
    ]
  },
  "acquisitionUnit": {
    "id": "1"
  }
}
```

# 시작하기

## 피처 튜토리얼

Data Infrastructure Insights에는 데이터를 빠르고 쉽게 찾고, 문제를 해결하고, 기업 환경에 대한 통찰력을 제공할 수 있는 유용한 기능이 포함되어 있습니다. 강력한 쿼리를 사용하여 데이터를 쉽게 찾고, 대시보드에서 데이터를 시각화하고, 설정한 데이터 임계값에 대한 전자 메일 알림을 보낼 수 있습니다.

Data Infrastructure Insights에는 이러한 기능을 이해하고 비즈니스 통찰력 전략을 보다 잘 구현하는 데 도움이 되는 다양한 비디오 자습서가 포함되어 있습니다. Data Infrastructure Insights 환경에 액세스할 수 있는 모든 사용자는 이 자습서를 활용할 수 있습니다.

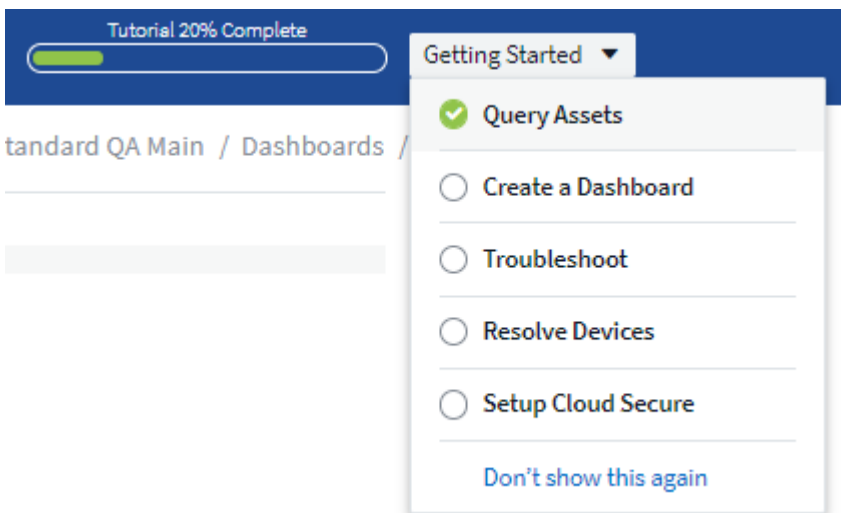
### 소개

Data Infrastructure Insights의 작동 방식을 설명하는 간단한 자습서를 시청하십시오.

▶ <https://docs.netapp.com/ko-kr/cloudinsights//media/howTo.mp4> (video)

### 체크리스트 및 비디오 자습서

Data Infrastructure Insights 사이트에 표시되는 \* 시작 체크리스트 \* 에는 몇 가지 유용한 작업 및 개념 목록이 포함되어 있습니다. 체크리스트에서 항목을 선택하면 해당 개념에 대한 적절한 Data Infrastructure Insights 페이지로 이동합니다. 예를 들어, `_Create a Dashboard_item`을 클릭하면 Data Infrastructure Insights \* Dashboards \* 페이지가 열립니다.



페이지 상단에는 대시보드를 만드는 방법을 보여주는 비디오 자습서에 대한 링크가 있습니다. 동영상을 원하는 횟수만큼 볼 수 있습니다. 해당 비디오에 대해 이 `_link`를 다시 표시하지 않습니다. 비디오를 해제할 때까지 대시보드 페이지로 이동할 때마다 사용할 수 있습니다.

 [Learn How to Create a Dashboard](#) [Watch Video](#) [Got it! Don't show this again.](#)

비디오를 한 번 이상 시청한 후 체크리스트의 **\_대시보드 생성\_** 항목이 체크 아웃되어 튜토리얼을 완료했음을 나타냅니다. 그런 다음 다음 다음 다음 자습서로 진행할 수 있습니다.



원하는 순서대로 튜토리얼을 볼 수 있습니다.

점검 목록을 해제합니다

점검 목록 맨 아래에 있는 **\_다시 표시하지 않음\_** 링크를 클릭할 때까지 시작 점검 목록이 사이트에 표시됩니다. 체크리스트를 없앤 후에도 메시지 헤더 표시줄에서 각 자습서를 해제할 때까지 해당하는 각 Data Infrastructure Insights 페이지에서 자습서를 계속 사용할 수 있습니다.

## 자습서를 봅니다

데이터 쿼리

▶ <https://docs.netapp.com/ko-kr/cloudinsights//media/Queries.mp4> (video)

대시보드 생성

▶ <https://docs.netapp.com/ko-kr/cloudinsights//media/Dashboards.mp4> (video)

문제 해결

▶ <https://docs.netapp.com/ko-kr/cloudinsights//media/Troubleshooting.mp4> (video)

장치 확인

▶ [https://docs.netapp.com/ko-kr/cloudinsights//media/AHR\\_small.mp4](https://docs.netapp.com/ko-kr/cloudinsights//media/AHR_small.mp4) (video)

## 데이터 수집 중

데이터 수집을 시작하는 중입니다

Data Infrastructure Insights에 등록하고 환경에 처음으로 로그인하면 다음 단계에 따라 데이터 수집 및 관리를 시작합니다.

데이터 수집기는 스토리지 디바이스, 네트워크 스위치, 가상 머신 등의 데이터 소스에서 정보를 검색합니다. 수집된 정보는 분석, 검증, 모니터링 및 문제 해결에 사용됩니다.

Data Infrastructure Insights에서는 세 가지 유형의 데이터 수집기를 사용할 수 있습니다.

- 인프라(스토리지 장치, 네트워크 스위치, 컴퓨팅 인프라)
- 운영 체제(예: VMware 또는 Windows)
- 서비스(예: Kafka)

지원되는 공급업체 및 모델에서 첫 번째 데이터 수집기를 선택합니다. 나중에 데이터 수집기를 쉽게 추가할 수 있습니다.

획득 장치를 설치합니다

\_Infrastructure\_data 수집기를 선택한 경우 데이터를 Data Infrastructure Insights에 주입하려면 획득 장치가 필요합니다. 수집할 데이터 센터의 서버나 VM에 획득 장치 소프트웨어를 다운로드하여 설치해야 합니다. 단일 획득 장치는 여러 데이터 수집기에 사용할 수 있습니다.



ONTAP Data  
Management  
Software

## Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

### What Operating System or Platform Are You Using?

Linux

Linux Versions Supported ⓘ Production Best Practices ⓘ

### Installation Instructions

[Need Help?](#)

#### 1 Copy Installer Snippet

*This snippet has a unique key valid for 24 hours for this Acquisition Unit only.*

Reveal Installer Snippet

#### 2 Paste the snippet into a bash shell to run the installer.

#### 3 Waiting for Acquisition Unit to connect...

- 를 따릅니다 "지침" 획득 장치를 설치하기 위해 표시됩니다. 획득 장치 소프트웨어가 설치되면 계속 버튼이 표시되고 다음 단계로 진행할 수 있습니다.

#### 3 Continue New acquisition unit detected!

필요한 경우 나중에 추가 획득 장치를 설정할 수 있습니다. 예를 들어, 서로 다른 영역의 데이터 센터에서 정보를 수집하는 여러 획득 단위를 원할 수 있습니다.

## Data Collector - Infrastructure를 구성합니다

Infrastructure\_data Collector의 경우 표시되는 데이터 수집기 필드를 작성하라는 메시지가 표시됩니다.

- 데이터 수집기에 고유하고 의미 있는 이름을 지정합니다.
- 장치에 연결할 자격 증명(사용자 이름 및 암호)을 적절하게 입력합니다.
- Configuration\_and\_Advanced Configuration\_sections에 다른 필수 필드를 입력합니다.
- 데이터 수집기를 저장하려면 \* 수집기 추가 \* 를 클릭합니다.

나중에 추가 데이터 수집기를 구성할 수 있습니다.

## Data Collector 구성 - 운영 체제 및 서비스



운영 체제:

Operating System\_data Collector의 경우 Data Infrastructure Insights Agent를 설치할 플랫폼(Linux, Windows)을 선택합니다. 서비스에서 데이터를 수집하려면 하나 이상의 에이전트가 있어야 합니다. 또한 에이전트는 Data Infrastructure Insights에서 사용할 데이터를 호스트 자체에서 수집합니다. 이 데이터는 위젯 등에서 "노드" 데이터로 분류됩니다

- 에이전트 호스트 또는 VM에서 터미널 또는 명령 창을 열고 표시된 명령을 붙여 넣어 에이전트를 설치합니다.
- 설치가 완료되면 \* 설치 완료 \* 를 클릭합니다.

서비스:

Service\_data Collector의 경우 타일을 클릭하여 해당 서비스에 대한 지침 페이지를 엽니다.

- 플랫폼과 상담원 액세스 키를 선택합니다.
- 해당 플랫폼에 에이전트가 설치되어 있지 않은 경우 지침에 따라 에이전트를 설치합니다.
- 데이터 수집기 지침 페이지를 열려면 \* 계속 \* 을 클릭합니다.
- 지침에 따라 데이터 수집기를 구성합니다.
- 구성이 완료되면 \* 설치 완료 \* 를 클릭합니다.

대시보드를 추가합니다

구성(스토리지, 스위치 등)하기 위해 선택한 초기 데이터 수집기의 유형에 따라 하나 이상의 관련 대시보드를 가져옵니다. 예를 들어, 스토리지 데이터 수집기를 구성한 경우 스토리지 관련 대시보드 세트를 가져오고, 하나는 Data Infrastructure Insights 홈 페이지로 설정됩니다. 대시보드 > 모든 대시보드 표시 \* 목록에서 홈 페이지를 변경할 수 있습니다.

나중에 또는 를 사용하여 추가 대시보드를 가져올 수 있습니다 "[자신만의 고유한 구성](#)".

그뿐이야

초기 설정 프로세스를 완료하면 사용자 환경에서 데이터 수집이 시작됩니다.

초기 설정 프로세스가 중단된 경우(예: 브라우저 창을 닫은 경우) 다음 단계를 수동으로 수행해야 합니다.

- Data Collector를 선택합니다
- 메시지가 나타나면 Agent 또는 Acquisition Unit(획득 장치)을 설치합니다
- Data Collector를 구성합니다

유용한 정의

Data Infrastructure Insights 데이터 수집기 또는 기능에 대해 설명할 때 다음 정의가 유용할 수 있습니다.

- 수집기 수명 주기: 수집기는 수명 주기에서 다음 상태 중 하나에 속합니다.
  - \* Preview \*: 제한된 용량 또는 제한된 대상 고객에게만 제공됩니다. "[피처 미리보기](#)" 그리고 데이터 수집기는 미리보기 기간 이후 GA될 것으로 예상됩니다. 미리 보기 기간은 대상 또는 기능에 따라 다릅니다.
  - \* GA \*: Edition 또는 기능 세트를 기반으로 모든 고객이 일반적으로 사용할 수 있는 기능 또는 데이터 수집기입니다.

- \* 더 이상 사용되지 않음 \*: 더 이상 기능적으로 지속 가능하지 않은 데이터 수집기에 적용됩니다. 더 이상 사용되지 않는 데이터 수집기는 기능적으로 업데이트된 최신 데이터 수집기로 대체되는 경우가 많습니다.
- \* 삭제됨 \*: 제거되었으며 더 이상 사용할 수 없는 데이터 수집기입니다.
- 획득 장치: 데이터 수집기를 호스팅하는 전용 컴퓨터(일반적으로 가상 머신)입니다. 이 컴퓨터는 일반적으로 모니터링되는 항목과 동일한 데이터 센터/VPC에 위치합니다.
- 데이터 소스: 하드웨어 또는 소프트웨어 스택과 통신하는 모듈입니다. 장치와 통신하기 위해 AU 컴퓨터에서 실행되는 구성 및 코드로 구성됩니다.

## 획득 장치 요구 사항

인프라스트럭처 데이터 수집기(스토리지, VM, 포트, EC2 등)로부터 정보를 가져오려면 획득 장치(AU)를 설치해야 합니다. 획득 장치를 설치하기 전에 운영 체제, CPU, 메모리 및 디스크 공간 요구 사항을 충족하는지 확인해야 합니다.

### 요구 사항

구성 요소	Linux 요구 사항	Windows 요구 사항
운영 체제	<p>다음 중 하나의 라이선스 버전을 실행하는 컴퓨터:</p> <ul style="list-style-type: none"> <li>* CentOS (64비트): 7.2 ~ 7.9, 8.1 ~ 8.4, Stream 8, Stream 9</li> <li>* AlmaLinux 9.3 및 9.4</li> <li>* 데비안 (64비트): 9와 10</li> <li>* OpenSUSE Leap 15.1에서 15.5까지</li> <li>* Oracle Enterprise Linux(64비트): 7.5 - 7.9, 8.1 - 8.8</li> <li>* Red Hat Enterprise Linux(64비트): 7.2 - 7.9, 8.1 - 8.10, 9.1 - 9.4</li> <li>* Rocky 9.0 ~ 9.4</li> <li>* SUSE Enterprise Linux Server 15, 15 SP2 ~ 15 SP5</li> <li>* Ubuntu 서버: 18.04, 20.04, 22.04 LTS</li> <li>* 위의 플랫폼에서 SELinux</li> </ul> <p>이 컴퓨터는 다른 응용 프로그램 수준 소프트웨어를 실행하지 않아야 합니다. 전용 서버가 권장됩니다.</p> <p>SELinux를 실행하는 경우 획득 장치 시스템에서 다음 명령을 실행하는 것이 좋습니다.</p> <pre>sudo semanage fcontext -a -t usr_t "/opt/netapp/cloudinsights(/. *)?" sudo restorecon -R/opt/netapp/cloudinsights 를 참조하십시오</pre>	<p>다음 중 하나의 라이선스 버전을 실행하는 컴퓨터: * Microsoft Windows 10 64비트 * Microsoft Windows Server 2012 * Microsoft Windows Server 2012 R2 * Microsoft Windows Server 2016 * Microsoft Windows Server 2019 * Microsoft Windows Server 2022 * Microsoft Windows 11 이 컴퓨터는 다른 응용 프로그램 수준 소프트웨어를 실행하지 않아야 합니다. 전용 서버가 권장됩니다.</p>

CPU	CPU 코어 2개	동일합니다
메모리	8GB RAM	동일합니다
사용 가능한 디스크 공간입니다	50GB(100GB 권장) Linux의 경우 다음과 같은 방법으로 디스크 공간을 할당해야 합니다. /opt/NetApp 10GB(대규모 환경의 경우 20GB) /var/log/netapp 40GB(대규모 환경의 경우 80GB) /tmp 설치 중 최소 1GB 사용 가능	50GB
네트워크	100Mbps/1Gbps 이더넷 연결, 정적 IP 주소, 획득 장치에서 *.cloudinsights.NetApp.com 또는 데이터 인프라 인사이트 환경(예: https://<environment_id>.c01.cloudinsights.NetApp.com)으로의 포트 80 또는 443 연결이 필요합니다. 획득 장치와 각 데이터 수집기 사이의 요구 사항은 에 대한 지침을 " <a href="#">데이터 수집기</a> "참조하십시오. 조직에서 인터넷 액세스에 프록시 사용을 요구하는 경우 조직의 프록시 동작을 이해하고 Data Infrastructure Insights가 작동하려면 특정 예외를 찾아야 할 수 있습니다. 예를 들어, 조직에서 기본적으로 액세스를 차단하며 특정 웹 사이트/도메인에 대한 액세스는 예외로 허용됩니까? 이 경우 예외 목록에 다음 도메인을 추가해야 합니다. *.cloudinsights.NetApp.com 자세한 내용은 프록시 " <a href="#">여기(Linux)</a> " 또는 에 대해 읽어보십시오" <a href="#">여기(Windows)</a> ".	동일합니다
권한	획득 장치 서버의 sudo 권한. /tmp는 Exec 기능과 함께 마운트되어야 합니다.	획득 장치 서버에 대한 관리자 권한
바이러스 검사		설치하는 동안 모든 바이러스 스캐너를 완전히 비활성화해야 합니다. 설치 후 획득 장치 소프트웨어에서 사용하는 경로는 바이러스 검사에서 제외되어야 합니다.

#### 추가 권장 사항

- 정확한 감사 및 데이터 보고를 위해 \* NTP(Network Time Protocol) \* 또는 \* SNTP(Simple Network Time Protocol) \* 를 사용하여 획득 장치 시스템의 시간을 동기화하는 것이 좋습니다.

#### 사이징 관련

8GB 메모리와 50GB의 디스크 공간만 갖춘 Data Infrastructure Insights Acquisition Unit을 시작할 수 있지만 대규모

환경에서는 다음과 같은 질문을 해야 합니다.

다음 사항을 예상하십니까?

- 이 획득 장치에서 2,500개 이상의 가상 머신 또는 10개의 대규모(>2개 노드) ONTAP 클러스터, Symmetrix 또는 HDS/HPE VSP/XP 스토리지를 검색하십니까?
- 이 획득 장치에 75개 이상의 총 데이터 수집기를 배포하시겠습니까?

위의 "예"로 답할 때마다 AU에 8GB의 메모리와 50GB의 디스크 공간을 추가하는 것이 좋습니다. 예를 들어, 둘 다에 "예"를 선택한 경우 150GB 이상의 디스크 공간이 있는 24GB 메모리 시스템을 구축해야 합니다. Linux에서 로그 위치에 추가할 디스크 공간입니다.

사이징에 대한 추가 질문은 NetApp 지원에 문의하십시오.

추가 **Federal Edition** 요구 사항

- Data Infrastructure Insights Federal Edition 클러스터에 Acquisition Unit을 설치하는 경우 기본 운영 체제에 적절한 엔트로피 소스가 있어야 합니다. Linux 시스템에서는 일반적으로 `_rng-tools_`를 설치하거나 하드웨어 RNG(Random Number Generation)를 사용하여 이 작업을 수행합니다. 획득 장치 시스템에서 이 요구 사항이 충족되는지 확인하는 것은 고객의 책임입니다.

## 획득 장치 구성

Data Infrastructure Insights는 로컬 서버에 설치된 하나 이상의 획득 장치를 사용하여 장치 데이터를 수집합니다. 각 획득 장치는 여러 개의 데이터 수집기를 호스팅할 수 있으며, 이 수집기는 분석을 위해 장치 메트릭을 Data Infrastructure Insights로 전송합니다.

이 항목에서는 획득 장치를 추가하는 방법과 환경에서 프록시를 사용할 때 필요한 추가 단계에 대해 설명합니다.



정확한 감사 및 데이터 보고를 위해 \* NTP(Network Time Protocol) \* 또는 \* SNTP(Simple Network Time Protocol) \* 를 사용하여 획득 장치 시스템의 시간을 동기화하는 것이 좋습니다.

Data Infrastructure Insights 보안에 대해 ["여기"](#)알아보십시오.

## Linux 획득 장치 추가

시작하기 전에

- 시스템에서 프록시를 사용하는 경우 획득 장치를 설치하기 전에 프록시 환경 변수를 설정해야 합니다. 자세한 내용은 [참조하십시오 프록시 환경 변수를 설정합니다.](#)

### Linux 획득 장치 설치 단계

1. Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. 관측성 > 수집기 > 촬영 단위 > + 촬영 단위 \* 를 클릭합니다

시스템에 *Install Acquisition Unit*(획득 장치 설치) 대화 상자가 표시됩니다. Linux 를 선택합니다.

## Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

### What Operating System or Platform Are You Using?

Linux Versions Supported

Production Best Practices

### Installation Instructions

[Need Help?](#)

#### 1 Copy Installer Snippet

*This snippet has a unique key valid for 24 hours for this Acquisition Unit only.*

Reveal Installer Snippet

#### 2 Paste the snippet into a bash shell to run the installer.

#### 3 Waiting for Acquisition Unit to connect...

1. 획득 장치를 호스팅하는 서버 또는 VM이 권장 시스템 요구 사항을 충족하는지 확인합니다.
2. 서버에서 지원되는 Linux 버전을 실행하고 있는지 확인합니다. 지원되는 버전 목록을 보려면 `_OS` 버전 지원됨 (I)\_을 클릭합니다.
3. 대화 상자의 설치 명령 스니펫을 획득 장치를 호스팅할 서버 또는 VM의 터미널 창으로 복사합니다.
4. Bash 셸에서 명령을 붙여 넣고 실행합니다.

#### 작업을 마친 후

- 획득 장치의 상태를 확인하려면 \* 관측성 > 수집기 > 획득 장치 \* 를 클릭합니다.
- 획득 장치 로그는 `/var/log/netapp/클라우드 볼거리/acq/acq.log` 에서 액세스할 수 있습니다
- 다음 스크립트를 사용하여 획득 장치를 제어합니다.
  - `cloudinsights-service.sh` (stop, start, restart, check the status)
- 다음 스크립트를 사용하여 획득 장치를 제거합니다.
  - `cloudinsights-uninstall.sh`

#### 프록시 환경 변수를 설정합니다

프록시를 사용하는 환경에서는 획득 장치를 추가하기 전에 프록시 환경 변수를 설정해야 합니다. 프록시 구성에 대한 지침은 *Add Acquisition Unit*(획득 장치 추가) 대화 상자에 나와 있습니다.

1. In\_Ha Proxy Server? \_을(를) 클릭합니다
2. 명령을 텍스트 편집기에 복사하고 필요에 따라 프록시 변수를 설정합니다.

참고: 프록시 사용자 이름 및 암호 필드의 특수 문자 제한: '%' 및 '!'에 유의하십시오. 사용자 이름 필드에 허용됩니다. ':', '%' 및 '!' 암호 필드에 허용됩니다.

3. BASH 셸을 사용하여 터미널에서 편집된 명령을 실행합니다.

#### 4. 획득 장치 소프트웨어를 설치합니다.

##### 프록시 구성

획득 장치는 양방향/상호 인증을 사용하여 Data Infrastructure Insights 서버에 연결합니다. 인증을 받으려면 클라이언트 인증서를 Data Infrastructure Insights 서버로 전달해야 합니다. 이렇게 하려면 데이터의 암호를 해독하지 않고 https 요청을 Data Infrastructure Insights 서버로 전달하도록 프록시를 설정해야 합니다.

가장 간단한 방법은 프록시/방화벽에서 와일드카드 구성을 지정하여 Data Infrastructure Insights와 통신하는 것입니다. 예를 들면 다음과 같습니다.

```
*.cloudinsights.netapp.com
```



와일드카드에서는 별표(\*)를 사용하는 것이 일반적이지만 프록시/방화벽 구성에서는 다른 형식을 사용할 수 있습니다. 사용자 환경에서 올바른 와일드카드 사양을 확인하려면 프록시 설명서를 참조하십시오.

프록시 구성에 대한 자세한 내용은 NetApp에서 확인할 수 있습니다 "[Knowledgebase를 참조하십시오](#)".

##### 프록시 URL 보기

온보딩 중에 데이터 수집기를 선택할 때 \* 프록시 설정 \* 링크를 클릭하거나 \* 도움말 > 지원 \* 페이지의 프록시 설정 아래에 있는 링크를 클릭하여 프록시 끝점 URL을 볼 수 있습니다. 다음과 같은 테이블이 표시됩니다.

### Proxy Settings

If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

Close

작업 환경에 워크로드 보안이 있는 경우 구성된 엔드포인트 URL도 이 목록에 표시됩니다.

##### Windows 획득 장치 추가

##### Windows 획득 장치 설치 단계

1. 획득 장치 서버/VM에 관리자 권한이 있는 사용자로 로그인합니다.
2. 해당 서버에서 브라우저 창을 열고 Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
3. 관측성 > 수집기 > 촬영 단위 > + 촬영 단위 \* 를 클릭합니다.

시스템에 *Install Acquisition Unit*(획득 장치 설치) 대화 상자가 표시됩니다. Windows 를 선택합니다.


# Install Acquisition Unit

Cloud Insights collects device data via one or more Acquisition Units installed on local servers. Each Acquisition Unit can host multiple Data Collectors, which send device metrics to Cloud Insights for analysis.

## What Operating System or Platform Are You Using?

 Windows ▼

Windows Versions Supported 

Production Best Practices 

## Installation Instructions

[Need Help?](#)

1

2

*This access key is a unique key valid for 24 hours for this Acquisition Unit only.*

3 Paste access key into installer when prompted.

4 Please ensure you have copied and pasted the access key into the installer.

1. 획득 장치를 호스팅하는 서버 또는 VM이 권장 시스템 요구 사항을 충족하는지 확인합니다.
2. 서버에서 지원되는 Windows 버전을 실행 중인지 확인합니다. 지원되는 버전 목록을 보려면 `_OS 버전 지원됨(I)_`을 클릭합니다.
3. 다운로드 설치 프로그램(Windows 64비트) \* 단추를 클릭합니다.
4. 액세스 키를 복사합니다. 설치 중에 이 작업이 필요합니다.
5. 획득 장치 서버/VM에서 다운로드한 설치 프로그램을 실행합니다.
6. 메시지가 나타나면 설치 마법사에 액세스 키를 붙여 넣습니다.
7. 설치하는 동안 프록시 서버 설정을 제공할 수 있는 기회가 제공됩니다.

### 작업을 마친 후

- 획득 장치의 상태를 확인하려면 \* > 관측성 > 수집기 > 획득 장치 \* 를 클릭합니다.
- 설치 디렉터리>\Cloud Insights\Acquisition Unit\log\acq.log 에서 획득 장치 로그에 액세스할 수 있습니다
- 다음 스크립트를 사용하여 획득 장치의 상태를 중지, 시작, 다시 시작 또는 확인합니다.

```
cloudinsights-service.sh
```

### 프록시 구성

획득 장치는 양방향/상호 인증을 사용하여 Data Infrastructure Insights 서버에 연결합니다. 인증을 받으려면 클라이언트 인증서를 Data Infrastructure Insights 서버로 전달해야 합니다. 이렇게 하려면 데이터의 암호를 해독하지 않고 https 요청을 Data Infrastructure Insights 서버로 전달하도록 프록시를 설정해야 합니다.

가장 간단한 방법은 프록시/방화벽에서 와일드카드 구성을 지정하여 Data Infrastructure Insights와 통신하는 것입니다. 예를 들면 다음과 같습니다.

```
*.cloudinsights.netapp.com
```



와일드카드에서는 별표(\*)를 사용하는 것이 일반적이지만 프록시/방화벽 구성에서는 다른 형식을 사용할 수 있습니다. 사용자 환경에서 올바른 와일드카드 사양을 확인하려면 프록시 설명서를 참조하십시오.

프록시 구성에 대한 자세한 내용은 NetApp에서 확인할 수 있습니다 "[Knowledgebase를 참조하십시오](#)".

## 프록시 URL 보기

온보딩 중에 데이터 수집기를 선택할 때 \* 프록시 설정 \* 링크를 클릭하거나 \* 도움말 > 지원 \* 페이지의 프록시 설정 아래에 있는 링크를 클릭하여 프록시 끝점 URL을 볼 수 있습니다. 다음과 같은 테이블이 표시됩니다.

**Proxy Settings** ✕

**!** If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjkso.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

[Close](#)

작업 환경에 워크로드 보안이 있는 경우 구성된 엔드포인트 URL도 이 목록에 표시됩니다.

## 획득 장치 제거

획득 장치 소프트웨어를 제거하려면 다음을 수행합니다.

### • Windows: \*

Windows\* 획득 장치를 제거하는 경우:

1. 획득 장치 서버/VM에서 제어판을 열고 \* 프로그램 제거 \* 를 선택합니다. 제거할 Data Infrastructure Insights Acquisition Unit 프로그램을 선택합니다.
2. 제거 를 클릭하고 화면의 지시를 따릅니다.

### Linux: \*

Linux\* 획득 장치를 제거하는 경우:



1. 획득 장치 서버/VM에서 다음 명령을 실행합니다.

```
sudo cloudinsights-uninstall.sh -p
```

. 설치 제거에 대한 도움말을 보려면 다음을 실행합니다.

```
sudo cloudinsights-uninstall.sh --help
```

• Windows 및 Linux: \*



• AU 제거 후 \*:

1. Data Infrastructure Insights에서 \* 관측성 > 수집기 로 이동하여 \* Acquisition Units \* 탭을 선택합니다.
2. 제거할 획득 장치 오른쪽에 있는 옵션 단추를 클릭하고 `_Delete_`를 선택합니다. 데이터 수집기가 할당되지 않은 경우에만 획득 단위를 삭제할 수 있습니다.



연결된 데이터 수집기가 있는 획득 장치(AU)는 삭제할 수 없습니다. 원래 AU를 삭제하기 전에 모든 AU의 데이터 수집기를 다른 AU로 이동합니다(수집기를 편집하고 다른 AU를 선택하기만 하면 됨).

옆에 별표가 있는 획득 장치가 장치 해상도에 사용되고 있습니다. 이 AU를 제거하기 전에 장치 해상도에 사용할 다른 AU를 선택해야 합니다. 다른 AU 위에 마우스를 놓고 "점 3개" 메뉴를 열어 "장치 해상도에 사용"을 선택합니다.

cbc-cloudinsights-au   10.65.57.18

This Acquisition Unit is used for Device Resolution.

## 획득 장치 재설치

동일한 서버/VM에 획득 장치를 다시 설치하려면 다음 단계를 수행해야 합니다.

시작하기 전에

획득 장치를 다시 설치하기 전에 별도의 서버/VM에 임시 획득 장치가 구성되어 있어야 합니다.

단계

1. 획득 장치 서버/VM에 로그인하고 AU 소프트웨어를 제거합니다.
2. Data Infrastructure Insights 환경에 로그인하고 \* 관측성 > 수집기 \* 로 이동합니다.
3. 각 데이터 수집기에 대해 오른쪽에 있는 옵션 메뉴를 클릭하고 `_Edit_`를 선택합니다. 임시 획득 장치에 데이터 수집기를 지정하고 \* Save \* (저장 \*)를 클릭합니다.

동일한 유형의 여러 데이터 수집기를 선택하고 \* Bulk Actions \* 버튼을 클릭할 수도 있습니다. Edit\_를 선택하고 데이터 수집기를 임시 획득 장치에 할당합니다.

4. 모든 데이터 수집기를 임시 획득 장치로 이동한 후 \* 관측성 > 수집기 \* 로 이동하여 \* Acquisition Units \* 탭을 선택합니다.

- 재설치할 획득 장치 오른쪽에 있는 옵션 버튼을 클릭하고 `_Delete_`를 선택합니다. 데이터 수집기가 할당되지 않은 경우에만 획득 단위를 삭제할 수 있습니다.
- 이제 원본 서버/VM에 획득 장치 소프트웨어를 다시 설치할 수 있습니다. 획득 장치 \* 를 클릭하고 위의 지침에 따라 획득 장치를 설치합니다.
- 획득 장치가 다시 설치되면 데이터 수집기를 획득 장치에 다시 할당합니다.

## AU 세부 정보 보기

획득 장치(AU) 세부 정보 페이지는 AU에 유용한 세부 정보와 문제 해결에 도움이 되는 정보를 제공합니다. AU 세부 정보 페이지에는 다음 섹션이 포함되어 있습니다.

- 다음을 보여주는 \* 요약 \* 섹션:
  - 획득 장치의 \* 이름 \* 및 \* IP \*
  - AU의 현재 연결 \* 상태
  - \* 마지막으로 보고된 \* 데이터 수집기 폴링 시간입니다
  - AU 장비의 \* 운영 체제 \*
  - AU에 대한 현재 \* 참고 \* 이 필드를 사용하여 AU에 대한 설명을 입력합니다. 이 필드에는 가장 최근에 추가한 메모가 표시됩니다.
- 각 데이터 수집기에 대해 표시되는 AU \* Data Collector \* 표:
  - \* 이름 \* - 추가 정보가 있는 데이터 수집기의 세부 정보 페이지로 드릴다운하려면 이 링크를 클릭합니다
  - \* 상태 \* - 성공 또는 오류 정보
  - \* 유형 \* - 공급업체/모델
  - 데이터 수집기의 \* IP \* 주소입니다
  - 현재 \* 영향 \* 수준
  - \* Last Acquired \* Time(마지막 획득 \* 시간) - 데이터 수집기가 마지막으로 성공적으로 폴링된 시간입니다

### Acquisition Unit Summary

<b>Name</b> xp-linux	<b>Connection Status</b> OK - <a href="#">Need Help?</a>	<b>Operating System</b> Linux	<b>Note</b>
<b>IP</b> 10.197.120.145	<b>Last Reported</b> 2 minutes ago		

### Data Collectors (3)

+ Data Collector
Bulk Actions

<input type="checkbox"/>	Name ↑	Status	Type	IP	Impact	Last Acquired	
<input type="checkbox"/>	foo	<span style="color: red;">!</span> Inventory failed	NetApp Data ONTAP 7-Mode	foo	Low	Never	⋮
<input type="checkbox"/>	xp-cisco	All successful	Cisco MDS Fabric Switches	10.197.136.66		2 minutes ago	⋮
<input type="checkbox"/>	xpcdot26	All successful	NetApp ONTAP Data Management Software	10.197.136.26		8 minutes ago	⋮

각 데이터 수집기에 대해 "점 3개" 메뉴를 클릭하여 데이터 수집기를 복제, 편집, 폴링 또는 삭제할 수 있습니다. 이 목록에서 여러 데이터 수집기를 선택하여 대량 작업을 수행할 수도 있습니다.

획득 장치를 다시 시작하려면 페이지 상단의 \* Restart \* (재시작 \*) 버튼을 클릭합니다. 연결 문제가 발생할 경우 이 버튼을 선택하여 AU에 \* 연결 \* 복원을 시도합니다.

## 데이터 수집을 위한 에이전트 구성(Windows/Linux)

Data Infrastructure Insights는 "텔레그라프"통합 데이터 수집을 위한 에이전트로 를 사용합니다. Telegraf는 메트릭, 이벤트 및 로그를 수집 및 보고하는 데 사용할 수 있는 플러그인 기반 서버 에이전트입니다. 입력 플러그인은 시스템/OS에 직접 액세스하거나 타사 API를 호출하거나 구성된 스트림(예 Kafka, statsd 등). 출력 플러그인은 수집된 메트릭, 이벤트 및 로그를 에이전트에서 Data Infrastructure Insights로 전송하는 데 사용됩니다.

Data Infrastructure Insights의 현재 Telegraf 버전은 \* 1.24.0 \* 입니다.

Kubernetes에 설치하는 방법에 대한 자세한 내용은 를 참조하십시오 ["NetApp Kubernetes 모니터링 운영자"](#) 페이지.



정확한 감사 및 데이터 보고를 위해 \* NTP(Network Time Protocol) \* 또는 \* SNTP(Simple Network Time Protocol) \* 를 사용하여 Agent 시스템의 시간을 동기화하는 것이 좋습니다.



Agent를 설치하기 전에 설치 파일을 확인하려면 의 아래 섹션을 참조하십시오 [체크섬을 확인하는 중입니다.](#)

### Agent 설치

서비스 데이터 수집기를 설치하고 아직 Agent를 구성하지 않은 경우 해당 운영 체제에 대한 Agent를 먼저 설치하라는 메시지가 표시됩니다. 이 항목에서는 다음과 같은 운영 체제에 Telegraf 에이전트를 설치하는 지침을 제공합니다.

- [Windows](#)
- [RHEL 및 CentOS](#)
- [Ubuntu 및 Debian](#)

사용 중인 플랫폼에 관계없이 에이전트를 설치하려면 먼저 다음을 수행해야 합니다.

1. 에이전트에 사용할 호스트에 로그인합니다.
2. Data Infrastructure Insights 환경에 로그인하고 \* 관측성 > 수집기 \* 로 이동합니다.
3. Data Collector \* 를 클릭하고 설치할 데이터 수집기를 선택합니다.
4. 호스트에 적합한 플랫폼 선택(Windows, Linux)
5. 각 플랫폼의 나머지 단계를 따릅니다.



호스트에 에이전트를 설치한 후에는 해당 호스트에 에이전트를 다시 설치할 필요가 없습니다.



서버/VM에 에이전트를 설치하면 Data Infrastructure Insights는 사용자가 구성하는 모든 데이터 수집기에서 수집하는 것 외에도 해당 시스템에서 메트릭을 수집합니다. 이러한 메트릭은 로 수집됩니다 [. ""노드" 메트릭"](#)



프록시를 사용하는 경우 Telegraf 에이전트를 설치하기 전에 해당 플랫폼의 프록시 지침을 읽으십시오.

로그 위치

Telegraf 로그 메시지는 기본적으로 stdout에서 다음 로그 파일로 리디렉션됩니다.

- RHEL/CentOS:/var/log/Telegraf/telegraf.log
- Ubuntu/Debian:/var/log/Telegraf/telegraf.log
- Windows:C:\Program Files\Telegraf\telegraf.log

## Windows

전제 조건:

- PowerShell을 설치해야 합니다
- 프록시 뒤에 있는 경우 \* Windows\*용 프록시 지원 구성 섹션의 지침을 따라야 합니다.

## Windows에 대한 프록시 지원 구성



환경에서 프록시를 사용하는 경우 를 설치하기 전에 이 섹션을 읽어 보십시오.



아래 단계에서는 `_http_proxy/https_proxy_environment` 변수를 설정하는 데 필요한 작업을 간략히 설명합니다. 일부 프록시 환경에서는 `_no_proxy` 환경\_변수를 설정해야 할 수도 있습니다.

프록시 뒤에 있는 시스템의 경우, 다음과 같이 Telegraf 에이전트를 설치하기 전에 `_https_proxy_and/or_http_proxy_environment` 변수 \* 를 설정하십시오.

```
[System.Environment]::SetEnvironmentVariable("https_proxy",  
"<proxy_server>:<proxy_port>",  
[System.EnvironmentVariableTarget]::Machine)
```

에이전트 설치 중



## Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

Select existing API Access Token or create a new one

KEY1 (...Zqlk0c)

+ API Access Token

### Installation Instructions

[Need Help?](#)

1

Copy Agent Installer Snippet

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

Reveal Agent Installer Snippet

2

Open a PowerShell window as administrator and paste the snippet

3

Complete Setup

**Windows**에서 에이전트를 설치하는 단계:

1. 상담원 액세스 키를 선택합니다.
2. 에이전트 설치 대화 상자에서 명령 블록을 복사합니다. 클립보드 아이콘을 클릭하여 명령을 빠르게 클립보드에 복사할 수 있습니다.
3. PowerShell 창을 엽니다
4. 명령을 PowerShell 창에 붙여넣고 Enter 키를 누릅니다.
5. 명령은 적절한 에이전트 설치 프로그램을 다운로드하고 설치하고 기본 구성을 설정합니다. 완료되면 에이전트 서비스가 다시 시작됩니다. 명령에 고유한 키가 있으며 24시간 동안 유효합니다.
6. 마침 \* 또는 \* 계속 \* 을 클릭합니다

에이전트를 설치한 후 다음 명령을 사용하여 서비스를 시작/중지할 수 있습니다.

```
Start-Service telegraf  
Stop-Service telegraf
```

### Agent를 제거합니다

Windows에서 에이전트를 제거하려면 PowerShell 창에서 다음을 수행합니다.

1. Telegraf 서비스를 중지하고 삭제합니다.

```
Stop-Service telegraf  
sc.exe delete telegraf
```

2. trustore에서 인증서를 제거합니다.

```
cd Cert:\CurrentUser\Root
//rm E5FB7B68C08B1CA902708584C274F8EFC7BE8ABC
rm 1A918038E8E127BB5C87A202DF173B97A05B4996
```

3. C:\Program Files\Telegraf\_폴더를 삭제하여 바이너리, 로그 및 구성 파일을 제거합니다
4. 레지스트리에서 \_SYSTEM\CurrentControlSet\Services\EventLog\Application\Telegraf\_key를 제거합니다

### Agent 업그레이드 중

Telegraf 에이전트를 업그레이드하려면 다음을 수행합니다.

1. Telegraf 서비스를 중지하고 삭제합니다.

```
Stop-Service telegraf
sc.exe delete telegraf
```

2. 레지스트리에서 \_SYSTEM\CurrentControlSet\Services\EventLog\Application\Telegraf\_key를 삭제합니다
3. Delete\_C:\Program Files\Telegraf\Telegraf.conf \_
4. Delete\_C:\Program Files\Telegraf\Telegraf.exe \_
5. "새 에이전트를 설치합니다".

### RHEL 및 CentOS

전제 조건:

- curl, sudo, ping, sha256sum, openssl, 그리고 디미데드도 있습니다
- 프록시 뒤에 있는 경우 \* RHEL/CentOS \* 용 프록시 지원 구성 섹션의 지침을 따라야 합니다.

### RHEL/CentOS에 대한 프록시 지원 구성



환경에서 프록시를 사용하는 경우 를 설치하기 전에 이 섹션을 읽어 보십시오.



아래 단계에서는 \_http\_proxy/https\_proxy\_environment 변수를 설정하는 데 필요한 작업을 간략히 설명합니다. 일부 프록시 환경에서는 \_no\_proxy 환경\_변수를 설정해야 할 수도 있습니다.

프록시 뒤에 있는 시스템의 경우 Telegraf 에이전트를 설치하기 전에 \* 다음 단계를 수행하십시오.

1. 현재 사용자에게 대한 \_https\_proxy\_and/or\_http\_proxy\_environment 변수를 설정합니다.

```
export https_proxy=<proxy_server>:<proxy_port>
. /etc/default/Telegraf_를 생성하고
_https_proxy_and/or_http_proxy_variable 에 대한 정의를 삽입합니다.
```

```
https_proxy=<proxy_server>:<proxy_port>
```

## 에이전트 설치 중



### Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

#### Select existing API Access Token or create a new one

default\_ingestion\_api\_key1 (...xEKVyK)

+ API Access Token

Production Best Practices ?

#### Installation Instructions

[Need Help?](#)

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).
- 2 [Copy Agent Installer Snippet](#)  
This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)  
[Reveal Agent Installer Snippet](#)
- 3 Open a terminal window and paste the snippet in a Bash shell (requires curl, sudo, ping, sha256sum, and dmidcode).
- 4 [Complete Setup](#)

RHEL/CentOS에 에이전트를 설치하는 단계:

1. 상담원 액세스 키를 선택합니다.
2. 에이전트 설치 대화 상자에서 명령 블록을 복사합니다. 클립보드 아이콘을 클릭하여 명령을 빠르게 클립보드에 복사할 수 있습니다.
3. Bash 창을 엽니다
4. Bash 창에 명령을 붙여넣고 Enter 키를 누릅니다.
5. 명령은 적절한 에이전트 설치 프로그램을 다운로드하고 설치하고 기본 구성을 설정합니다. 완료되면 에이전트 서비스가 다시 시작됩니다. 명령에 고유한 키가 있으며 24시간 동안 유효합니다.
6. 마침 \* 또는 \* 계속 \* 을 클릭합니다

에이전트를 설치한 후 다음 명령을 사용하여 서비스를 시작/중지할 수 있습니다.

운영 체제에서 systemd(CentOS 7+ 및 RHEL 7+)를 사용하는 경우:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

운영 체제에서 systemd(CentOS 7+ 및 RHEL 7+)를 사용하지 않는 경우:

```
sudo service telegraf start
sudo service telegraf stop
```

## Agent를 제거합니다

RHEL/CentOS에서 에이전트를 제거하려면 Bash 터미널에서 다음을 수행합니다.

### 1. Telegraf 서비스 중지:

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

### 2. Telegraf 에이전트를 제거합니다.

```
yum remove telegraf
. 뒤에 남아 있을 수 있는 구성 또는 로그 파일을 제거합니다.
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

## Agent 업그레이드 중

Telegraf 에이전트를 업그레이드하려면 다음을 수행합니다.

### 1. Telegraf 서비스 중지:

```
systemctl stop telegraf (If your operating system is using systemd
(CentOS 7+ and RHEL 7+)
/etc/init.d/telegraf stop (for systems without systemd support)
```

### 2. 이전 Telegraf 에이전트를 제거합니다.

```
yum remove telegraf
. xref:{relative_path}#rhel-and-centos["새 에이전트를 설치합니다"].
```

## Ubuntu 및 Debian



전제 조건:

- curl, sudo, ping, sha256sum, openssl, 그리고 디미데드도 있습니다
- 프록시 뒤에 있는 경우 Ubuntu/Debian\*용 프록시 지원 구성 섹션의 지침을 따라야 합니다.

### Ubuntu/Debian에 대한 프록시 지원 구성



환경에서 프록시를 사용하는 경우 를 설치하기 전에 이 섹션을 읽어 보십시오.



아래 단계에서는 `_http_proxy/https_proxy_environment` 변수를 설정하는 데 필요한 작업을 간략히 설명합니다. 일부 프록시 환경에서는 `_no_proxy` 환경\_변수를 설정해야 할 수도 있습니다.

프록시 뒤에 있는 시스템의 경우 Telegraf 에이전트를 설치하기 전에 \* 다음 단계를 수행하십시오.

1. 현재 사용자에게 대한 `_https_proxy_and/or_http_proxy_environment` 변수를 설정합니다.

```
export https_proxy=<proxy_server>:<proxy_port>
. /etc/default/telegraf를 만들고 _https_proxy_and/or_http_proxy_variable에
대한 정의를 삽입합니다.
```

```
https_proxy=<proxy_server>:<proxy_port>
```

에이전트 설치 중



### Install Agent

Quickly setup an agent in your environment and immediately start monitoring data

#### Select existing API Access Token or create a new one

default\_ingestion\_api\_key1 (...xEKVyK)

+ API Access Token

Production Best Practices ?

#### Installation Instructions

[Need Help?](#)

- 1 For environments operating behind a proxy server, follow the instructions to [configure proxy support to install and run Telegraf](#).

- 2 [Copy Agent Installer Snippet](#)

This snippet has a unique key and is valid for 24 hours. Already have an agent in your environment? [View Troubleshooting](#)

[Reveal Agent Installer Snippet](#)

- 3 Open a terminal window and paste the snippet in a Bash shell (requires curl, sudo, ping, sha256sum, and dmidcode).

- 4 [Complete Setup](#)

**Debian** 또는 **Ubuntu**에 에이전트를 설치하는 단계:

1. 상담원 액세스 키를 선택합니다.
2. 에이전트 설치 대화 상자에서 명령 블록을 복사합니다. 클립보드 아이콘을 클릭하여 명령을 빠르게 클립보드에 복사할 수 있습니다.
3. Bash 창을 엽니다
4. Bash 창에 명령을 붙여넣고 Enter 키를 누릅니다.
5. 명령은 적절한 에이전트 설치 프로그램을 다운로드하고 설치하고 기본 구성을 설정합니다. 완료되면 에이전트 서비스가 다시 시작됩니다. 명령에 고유한 키가 있으며 24시간 동안 유효합니다.
6. 마침 \* 또는 \* 계속 \* 을 클릭합니다

에이전트를 설치한 후 다음 명령을 사용하여 서비스를 시작/중지할 수 있습니다.

운영 체제에서 **systemd**를 사용하는 경우:

```
sudo systemctl start telegraf
sudo systemctl stop telegraf
```

운영 체제에서 **systemd**를 사용하지 않는 경우:

```
sudo service telegraf start
sudo service telegraf stop
```

**Agent**를 제거합니다

Ubuntu/Debian에서 에이전트를 제거하려면 Bash 터미널에서 다음을 실행합니다.

1. Telegraf 서비스 중지:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

2. Telegraf 에이전트를 제거합니다.

```
dpkg -r telegraf
. 뒤에 남아 있을 수 있는 구성 또는 로그 파일을 제거합니다.
```

```
rm -rf /etc/telegraf*
rm -rf /var/log/telegraf*
```

## Agent 업그레이드 중

Telegraf 에이전트를 업그레이드하려면 다음을 수행합니다.

### 1. Telegraf 서비스 중지:

```
systemctl stop telegraf (If your operating system is using systemd)
/etc/init.d/telegraf stop (for systems without systemd support)
```

### 2. 이전 Telegraf 에이전트를 제거합니다.

```
dpkg -r telegraf
. xref:{relative_path}#ubuntu-and-debian["새 에이전트를 설치합니다"] .
```

체크섬을 확인하는 중입니다

Data Infrastructure Insights 에이전트 설치 관리자가 무결성 검사를 수행하지만 일부 사용자는 다운로드한 아티팩트를 설치하거나 적용하기 전에 자체 검증을 수행할 수 있습니다. 이 작업은 설치 프로그램을 다운로드하고 다운로드한 패키지에 대한 체크섬을 생성한 다음 설치 지침에 표시된 값과 체크섬을 비교하여 수행할 수 있습니다.

설치하지 않고 설치 프로그램 패키지를 다운로드합니다

다운로드 전용 작업(기본 다운로드 및 설치와 반대)을 수행하기 위해 사용자는 UI에서 가져온 에이전트 설치 명령을 편집하고 뒤에 오는 "설치" 옵션을 제거할 수 있습니다.

다음 단계를 수행하십시오.

1. 지시에 따라 Agent Installer 스니펫을 복사합니다.
2. 코드 조각을 명령 창에 붙여 넣는 대신 텍스트 편집기에 붙여 넣습니다.
3. 명령에서 뒤에 오는 "--install"(Linux) 또는 "-install"(Windows)을 제거합니다.
4. 텍스트 편집기에서 전체 명령을 복사합니다.
5. 이제 명령 창(작업 디렉토리)에 붙여넣고 실행합니다.

Windows 이외의 경우(이러한 예는 Kubernetes에 해당하고, 실제 스크립트 이름은 다를 수 있음):

- 다운로드 및 설치(기본값):

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H
./$installerName --download --install
* 다운로드 전용:
```

```
installerName=cloudinsights-kubernetes.sh ... && sudo -E -H
./$installerName --download
```

참:

- 다운로드 및 설치(기본값):

```
!$($installerName=".cloudinsights-windows.ps1") ... -and  
$(&$installerName -download -install)  
* 다운로드 전용:
```

```
!$($installerName=".cloudinsights-windows.ps1") ... -and  
$(&$installerName -download)
```

download-only 명령은 Data Infrastructure Insights에서 작업 디렉토리로 필요한 모든 아티팩트를 다운로드합니다. 아티팩트에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 설치 스크립트
- 환경 파일입니다
- YAML 파일
- 체크섬 파일(SHA256.signed 또는 SHA256.PS1로 끝남)

육안 검사를 통해 설치 스크립트, 환경 파일 및 YAML 파일을 확인할 수 있습니다.

체크섬 값을 생성합니다

체크섬 값을 생성하려면 해당 플랫폼에 대해 다음 명령을 수행합니다.

- RHEL/Ubuntu:

```
sha256sum <package_name>  
* 참:
```

```
Get-FileHash telegraf.zip -Algorithm SHA256 | Format-List
```

체크섬을 확인합니다

체크섬 파일에서 필요한 체크섬을 추출합니다

- 비 Windows:

```
openssl smime -verify -in telegraf*.sha256.signed -CAfile  
netapp_cert.pem -purpose any -nosigs -noverify  
* 참:
```

```
(Get-Content telegraf.zip.sha256.ps1 -First 1).ToUpper()
```

다운로드한 패키지를 설치합니다

모든 아티팩트가 만족스럽게 확인되면 다음을 실행하여 에이전트 설치를 시작할 수 있습니다.

비 Windows:

```
sudo -E -H ./<installation_script_name> --install  
참:
```

```
.\cloudinsights-windows.ps1 -install
```

문제 해결

상담원 설정에 문제가 있는 경우 다음과 같은 방법을 시도해 보십시오.

문제:	다음을 시도해 보십시오.
새 플러그인을 구성하고 Telegraf를 다시 시작한 후 Teleraf가 시작되지 않습니다. 로그에 다음과 유사한 오류가 표시됩니다. "[텔레그래프] 에이전트 실행 중 오류: 구성 파일 /etc/Telegraf/Telegraf.d/클라우드.conf: plugin outputs.http: line <linenumber>: 구성에서 ["use_system_proxy"] 필드를 지정했지만 사용되지 않았습니다."	설치된 Telegraf 버전이 오래되었습니다. 이 페이지의 단계를 따라 해당 플랫폼에 대해 Agent * 를 업그레이드합니다.
이전 설치에서 설치 프로그램 스크립트를 실행했는데 에이전트가 데이터를 전송하지 않습니다	Telegraf 에이전트를 제거한 다음 설치 스크립트를 다시 실행합니다. 해당 플랫폼에 대해 이 페이지의 * 에이전트 업그레이드 * 단계를 따릅니다.
Data Infrastructure Insights를 사용하여 에이전트를 이미 설치했습니다	호스트/VM에 이미 에이전트를 설치한 경우 에이전트를 다시 설치할 필요가 없습니다. 이 경우 Agent 설치 화면에서 해당 플랫폼 및 키를 선택하고 * 계속 * 또는 * 마침 * 을 클릭합니다.
이미 에이전트가 설치되어 있지만 Data Infrastructure Insights 설치 프로그램을 사용하지 않고 있습니다	이전 에이전트를 제거하고 Data Infrastructure Insights Agent 설치를 실행하여 적절한 기본 구성 파일 설정을 확인합니다. 완료되면 * 계속 * 또는 * 마침 * 을 클릭합니다.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## 데이터 수집기 구성

데이터 센터의 장치에서 데이터를 수집하도록 Data Infrastructure Insights 환경에서 Data Collector를 구성합니다.

## 시작하기 전에

- 데이터 수집을 시작하려면 먼저 획득 장치를 구성해야 합니다.
- 데이터를 수집하는 장치에 대한 자격 증명이 필요합니다.
- 데이터를 수집하는 모든 장치에는 장치 네트워크 주소, 계정 정보 및 암호가 필요합니다.

## 단계

1. Data Infrastructure Insights 메뉴에서 \* 관측성 > Collectors \* 를 클릭합니다

공급업체별로 정렬된 사용 가능한 데이터 Collector가 표시됩니다.

2. Collector \* 를 클릭하고 구성할 데이터 수집기를 선택합니다.

대화 상자에서 데이터 수집기를 구성하고 획득 장치를 추가할 수 있습니다.

3. 데이터 수집기의 이름을 입력합니다.
4. 추가 구성 필드를 추가하려면 \* 고급 구성 \* 을 클릭합니다. (일부 데이터 수집기는 고급 구성이 필요하지 않습니다.)
5. 구성 테스트 \* 를 클릭하여 데이터 수집기가 올바르게 구성되었는지 확인합니다.
6. Collector 추가 \* 를 클릭하여 구성을 저장하고 Data Infrastructure Insights 테넌트에 데이터 수집기를 추가합니다.

서비스의 데이터가 대시보드에 표시되거나 쿼리에 사용 가능하려면 폴링 기간을 최대 2회 정도 소요될 수 있습니다.

- 첫 번째 재고 조사: 즉시
- 초기 계획을 설정하기 위한 첫 번째 성능 데이터 폴링: 인벤토리 폴링 직후
- 2차 성능 설문: 1차 성능 설문 조사 완료 후 15초 이내

그런 다음 구성된 인벤토리 및 성능 폴링 간격에 따라 폴링이 진행됩니다.

## 데이터 수집기 획득 상태를 확인하는 중입니다

데이터 수집기는 Data Infrastructure Insights의 주요 정보 소스이므로 반드시 실행 상태를 유지해야 합니다.

데이터 수집기 상태는 자산 페이지의 오른쪽 상단 모서리에 "Acquired N minutes ago(N분 전 획득)" 메시지로 표시됩니다. 여기서 N은 자산의 데이터 수집기의 가장 최근 획득 시간을 나타냅니다. 획득 시간/날짜도 표시됩니다.

메시지를 클릭하면 데이터 수집기 이름, 상태 및 마지막으로 성공한 획득 시간이 있는 테이블이 표시됩니다. 관리자 로 로그인한 경우 테이블에서 데이터 수집기 이름 링크를 클릭하면 해당 데이터 수집기에 대한 세부 정보 페이지로 이동합니다.

## 구성된 데이터 수집기 관리

설치된 데이터 수집기 페이지에서는 Data Infrastructure Insights에 대해 구성된 데이터 수집기에 액세스할 수 있습니다. 이 페이지를 사용하여 기존 데이터 수집기를 수정할 수 있습니다.

## 단계

1. Data Infrastructure Insights 메뉴에서 \* 관측성 > Collectors \* 를 클릭합니다

Available Data Collector 화면이 표시됩니다.

2. 설치된 데이터 수집기 \* 를 클릭합니다

설치된 모든 데이터 수집기 목록이 표시됩니다. 이 목록은 Collector 이름, 상태, 수집기가 액세스하는 IP 주소 및 장치에서 데이터를 마지막으로 획득한 시점을 제공합니다. 이 화면에서 수행할 수 있는 작업은 다음과 같습니다.

- 폴링 제어
- 데이터 수집기 자격 증명을 변경합니다
- 클론 데이터 수집기

### Data Collector 폴링 제어

데이터 수집기를 변경한 후 변경 내용을 확인하기 위해 즉시 폴링하거나, 문제 해결 중에 데이터 수집기의 데이터 수집을 1일, 3일 또는 5일 동안 연기할 수 있습니다.

단계

1. Data Infrastructure Insights 메뉴에서 \* 관측성 > Collectors \* 를 클릭합니다
2. 설치된 데이터 수집기 \* 를 클릭합니다
3. 변경할 Data Collector의 왼쪽에 있는 확인란을 선택합니다
4. [벌크 작업]을 클릭하고 수행할 폴링 작업을 선택합니다.

대량 작업은 여러 Data Collector에서 동시에 수행할 수 있습니다. 데이터 수집기를 선택하고 \* Bulk Action \* 메뉴에서 수행할 작업을 선택합니다.

### 데이터 수집기 정보 편집

기존 데이터 수집기 설정 정보를 편집할 수 있습니다.

단일 데이터 수집기를 편집하려면:

1. Data Infrastructure Insights 메뉴에서 \* 관측성 > 수집기 \* 를 클릭하여 설치된 Data Collector 목록을 엽니다.
2. 수정할 데이터 수집기 오른쪽에 있는 옵션 메뉴에서 \* 편집 \* 을 클릭합니다.

Collector 편집 대화 상자가 열립니다.

3. 변경 사항을 입력하고 \* Test Configuration \* (구성 테스트 \*)을 클릭하여 새 구성을 테스트하거나 \* Save \* (저장 \*)를 클릭하여 구성을 저장합니다.

여러 데이터 수집기를 편집할 수도 있습니다.

1. 변경할 각 데이터 수집기의 왼쪽에 있는 확인란을 선택합니다.
2. [벌크 작업] \* 버튼을 클릭하고 [편집]을 선택하여 [데이터 수집기 편집] 대화상자를 엽니다.
3. 위와 같이 필드를 수정합니다.



선택한 데이터 수집기는 동일한 공급업체 및 모델이어야 하며 동일한 획득 장치에 있어야 합니다.

여러 데이터 수집기를 편집할 때 Data Collector Name(데이터 수집기 이름) 필드에 "Mixed(혼합)"가 표시되고 편집할 수 없습니다. 사용자 이름 및 암호와 같은 다른 필드는 "혼합"으로 표시되며 편집할 수 있습니다. 선택한 데이터 수집기에서 동일한 값을 공유하는 필드는 현재 값을 표시하고 편집할 수 있습니다.

여러 데이터 수집기를 편집할 때 \* Test Configuration \* 버튼을 사용할 수 없습니다.

## 데이터 수집기를 클론 중입니다

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. Data Infrastructure Insights 메뉴에서 \* 관측성 > Collectors \* 를 클릭합니다.
2. 설치된 데이터 수집기 \* 를 클릭합니다.
3. 복사할 데이터 수집기 왼쪽에 있는 확인란을 클릭합니다.
4. 선택한 데이터 수집기 오른쪽에 있는 옵션 메뉴에서 \* 클론 \* 을 클릭합니다.

Clone Data Collector 대화 상자가 표시됩니다.

5. 필수 필드에 새 정보를 입력합니다.
6. 저장 \* 을 클릭합니다.

### 작업을 마친 후

클론 작업은 다른 모든 속성 및 설정을 복사하여 새 데이터 수집기를 생성합니다.

## 데이터 수집기에 대한 대량 작업을 수행합니다

여러 데이터 수집기에 대한 일부 정보를 동시에 편집할 수 있습니다. 이 기능을 사용하면 폴링을 시작하고, 폴링을 연기하고, 여러 데이터 수집기에 대한 폴링을 다시 시작할 수 있습니다. 또한 여러 데이터 수집기를 삭제할 수 있습니다.

### 단계

1. Data Infrastructure Insights 메뉴에서 \* 관측성 > Collectors \* 를 클릭합니다
2. 설치된 데이터 수집기 \* 를 클릭합니다
3. 수정할 데이터 수집기 왼쪽에 있는 확인란을 클릭합니다.
4. 오른쪽의 옵션 메뉴에서 수행할 옵션을 클릭합니다.

### 작업을 마친 후

선택한 작업은 데이터 수집기에서 수행됩니다. 데이터 수집기를 삭제하도록 선택하면 작업을 준수해야 하는 대화 상자가 표시됩니다.

## 실패한 데이터 수집기 조사

데이터 수집기에 오류 메시지와 높음 또는 중간 수준의 영향이 있는 경우 연결된 정보가 있는 데이터 수집기 요약 페이지를 사용하여 이 문제를 조사해야 합니다.



다음 단계를 사용하여 실패한 데이터 수집기에 대한 원인을 확인합니다. 데이터 수집기 오류 메시지는 \* Admin \* (관리) 메뉴 및 \* Installed Data Collector \* (설치된 데이터 수집기 \*) 페이지에 표시됩니다.

단계

1. Admin \* > \* Data Collector \* > \* Installed Data Collector \* 를 클릭합니다.
2. 실패한 데이터 수집기의 연결된 이름 을 클릭하여 요약 페이지를 엽니다.
3. 요약 페이지에서 메모 영역을 확인하여 다른 엔지니어가 이 오류를 조사할 수도 있는 메모를 읽습니다.
4. 성능 메시지를 기록합니다.
5. 추가 정보를 표시하려면 이벤트 시각표 그래프의 세그먼트 위로 마우스 포인터를 이동합니다.
6. 장치에 대한 오류 메시지를 선택하고 이벤트 타임라인 아래에 표시된 다음 메시지 오른쪽에 표시되는 오류 세부 정보 아이콘을 클릭합니다.

오류 세부 정보에는 오류 메시지 텍스트, 가능한 원인, 사용 중인 정보 및 문제 해결을 위해 시도할 수 있는 권장 사항이 포함됩니다.

7. 이 Data Collector 영역에 의해 보고된 장치 영역에서 목록을 필터링하여 관심 있는 장치만 표시할 수 있으며 장치의 연결된 \* 이름 \* 을 클릭하여 해당 장치의 자산 페이지를 표시할 수 있습니다.
8. 데이터 수집기 요약 페이지로 돌아가면 페이지 하단에 있는 \* 최근 변경 사항 표시 \* 영역에서 문제를 발생시킨 최근 변경 사항이 있는지 확인합니다.

## 대시보드 갤러리에서 가져오기

Data Infrastructure Insights는 데이터에 대한 비즈니스 통찰력을 제공하기 위해 여러 가지 권장 대시보드를 제공합니다. 각 대시보드에는 특정 질문에 답하거나 현재 사용자 환경에서 수집 중인 데이터와 관련된 특정 문제를 해결하는 데 도움이 되도록 설계된 위젯이 포함되어 있습니다.

갤러리에서 대시보드를 가져오려면 다음을 실행합니다.

1. 대시보드 > 대시보드 \* 를 선택합니다
2. Gallery \* 에서 \* + 를 클릭합니다

권장 대시보드 \* 목록이 표시됩니다. 각 대시보드의 이름은 대시보드가 해결할 수 있는 특정 질문으로 지정됩니다. 대시보드를 이용하면 AWS, NetApp, 스토리지, VMware, VMware 등 다양한 유형의 오브젝트 관련 질문에 있습니다

3. 목록에서 하나 이상의 대시보드를 선택하고 \* 대시보드 추가 \* 를 클릭합니다. 대시보드 목록에 이러한 대시보드가 표시됩니다.

권장 대시보드 외에 현재 데이터와 관련이 없는 \* 추가 대시보드 \* 를 가져올 수도 있습니다. 예를 들어, 현재 설치된 스토리지 데이터 수집기가 없지만 나중에 일부 수집기를 구성할 계획이라면 스토리지 관련 대시보드를 가져오도록 선택할 수 있습니다. 이러한 대시보드는 표시할 수 있지만 하나 이상의 스토리지 데이터 수집기가 구성될 때까지 관련 데이터를 표시하지 않을 수 있습니다.

관리자 또는 계정 소유자 역할이 있는 사용자는 대시보드 갤러리에서 가져올 수 있습니다.

## 사용자 계정 및 역할

Data Infrastructure Insights는 최대 4개의 사용자 계정 역할(계정 소유자, 관리자, 사용자 및 게스트)을 제공합니다. 각 계정에는 아래 표에 명시된 특정 권한 수준이 할당됩니다. 사용자는 "초대되었습니다" Data Infrastructure Insights에서 특정 역할을 할당하거나 "SSO(Single Sign-On) 인증" 기본 역할을 사용하여 이를 통해 로그인할 수 있습니다. SSO 인증은 Data Infrastructure Insights Premium Edition의 기능으로 제공됩니다.

### 사용 권한 수준

관리자 권한이 있는 계정을 사용하여 사용자 계정을 만들거나 수정합니다. 각 사용자 계정에는 다음 권한 수준에서 각 Data Infrastructure Insights 기능에 대한 역할이 할당됩니다.

역할	관찰 가능성	워크로드 보안	보고	관리자
계정 소유자	Administrator와 동일합니다	Administrator와 동일합니다	Administrator와 동일합니다	SSO 인증 및 ID 페더레이션 구성을 관리할 뿐 아니라 관리자와 동일합니다. 추가 소유자를 할당할 수도 있습니다.
관리자	모든 관측성 기능과 데이터 수집기 관리를 수행할 수 있습니다.	경고, Forensics, 데이터 수집기, 자동화된 응답 정책 및 보안을 위한 API 토큰을 포함한 모든 보안 기능을 수행할 수 있습니다. 관리자는 다른 사용자를 초대할 수도 있지만 보안 역할만 할당할 수 있습니다.	보고 API 토큰 관리, 보고서 구성, 보고 작업 종료 및 재시작 등의 모든 관리 작업을 포함한 모든 사용자/작성자 기능을 수행할 수 있습니다. 관리자는 다른 사용자를 초대할 수도 있지만 보고 역할만 할당할 수 있습니다.	다른 사용자를 초대할 수 있지만 관측성 역할만 할당할 수 있습니다. SSO 구성을 볼 수는 있지만 수정할 수는 없습니다. API 액세스 토큰을 생성하고 관리할 수 있습니다. 감사 정보를 볼 수 있습니다. 구독 정보, 사용 현황 및 기록을 볼 수 있습니다. 전역 경고 알림 및 구독 알림 수신자 목록을 관리할 수 있습니다.
사용자	대시보드, 쿼리, 알림, 주석, 주석 규칙, 장치 해상도를 관리할 수 있습니다.	알림을 확인 및 관리하고 Forensics를 볼 수 있습니다. 사용자 역할은 알림 상태를 변경하고, 메모를 추가하고, 스냅샷을 수동으로 생성하고, 사용자 액세스 제한을 관리할 수 있습니다.	모든 게스트/소비자 기능을 수행할 수 있을 뿐 아니라 보고서 및 대시보드를 생성 및 관리할 수 있습니다.	사용할 수 없습니다

역할	관찰 가능성	워크로드 보안	보고	관리자
게스트	자산 페이지, 대시보드, 알림에 대한 읽기 전용 액세스를 제공하며 쿼리를 보고 실행할 수 있습니다.	알림 및 Forensics를 볼 수 있습니다. 게스트 역할은 알림 상태를 변경하거나, 메모를 추가하거나, 스냅샷을 수동으로 생성하거나, 사용자 액세스를 제한할 수 없습니다.	에서는 보고서를 보고 일정을 잡고 실행할 수 있으며 언어 및 표준 시간대와 같은 개인 기본 설정을 설정할 수 있습니다. 게스트/소비자는 보고서를 만들거나 관리 작업을 수행할 수 없습니다.	사용할 수 없습니다

관리자 권한이 있는 사용자의 수를 제한하는 것이 가장 좋습니다. 최대 계정 수는 사용자 또는 게스트 계정이어야 합니다.

### 사용자 역할별 **Data Infrastructure Insights** 권한

다음 표에서는 각 사용자 역할에 부여된 Data Infrastructure Insights 권한을 보여 줍니다.

피처	관리자/계정 소유자	사용자	게스트
획득 단위: 추가/수정/삭제	예	해당 없음	해당 없음
경고 *: 생성/수정/삭제	예	예	해당 없음
경고 *: 보기	예	예	예
주석 규칙: 생성/실행/수정/삭제	예	예	해당 없음
주석: 생성/수정/할당/보기/제거/삭제	예	예	해당 없음
API 액세스 *: 생성/이름 바꾸기/비활성화/해지	예	해당 없음	해당 없음
응용 프로그램: 생성/보기/수정/삭제	예	예	해당 없음
자산 페이지: 수정	예	예	해당 없음
자산 페이지: 보기	예	예	예
감사: 보기	예	해당 없음	해당 없음
클라우드 비용	예	해당 없음	해당 없음
보안	예	해당 없음	해당 없음
대시보드: 생성/수정/삭제	예	예	해당 없음
대시보드: 보기	예	예	예
데이터 수집기: 추가/수정/폴링/삭제	예	해당 없음	해당 없음
알림: 보기	예	예	예
알림: 수정	예	해당 없음	해당 없음
쿼리: 생성/수정/삭제	예	예	해당 없음

쿼리: 보기/실행	예	예	예
장치 해상도	예	예	해당 없음
보고서 *: 보기/실행	예	예	예
보고서 *: 생성/수정/삭제/일정	예	예	해당 없음
가입: 보기/수정	예	해당 없음	해당 없음
사용자 관리: 초대/추가/수정/비활성화	예	해당 없음	해당 없음

- Premium Edition이 필요합니다

## 사용자를 초대하여 계정 만들기

새 사용자 계정은 BlueXP를 통해 생성됩니다. 사용자는 이메일을 통해 보낸 초대에 응답할 수 있지만 BlueXP 계정이 없는 경우 사용자는 BlueXP 초대를 수락할 수 있도록 BlueXP에 등록해야 합니다.

### 시작하기 전에

- 사용자 이름은 초대의 전자 메일 주소입니다.
- 할당할 사용자 역할을 이해합니다.
- 암호는 등록 프로세스 중에 사용자가 정의합니다.

### 단계

1. Data Infrastructure Insights에 로그인합니다
2. 메뉴에서 \* Admin > User Management \* 를 클릭합니다

사용자 관리 화면이 표시됩니다. 화면에는 시스템의 모든 계정 목록이 표시됩니다.

3. 사용자 \* 를 클릭합니다

사용자 초대 \* 화면이 표시됩니다.

4. 이메일 주소 또는 여러 주소를 입력하여 초대를 보냅니다.

- 참고: \* 여러 주소를 입력하면 모두 동일한 역할로 생성됩니다. 여러 명의 사용자만 동일한 역할로 설정할 수 있습니다.

5. Data Infrastructure Insights의 각 기능에 대한 사용자 역할을 선택합니다.



선택할 수 있는 기능 및 역할은 특정 관리자 역할에서 액세스할 수 있는 기능에 따라 다릅니다. 예를 들어 보고에만 관리자 역할이 있는 경우 사용자를 보고의 모든 역할에 할당할 수 있지만 관찰 가능성 또는 보안에 대한 역할을 할당할 수는 없습니다.

**Invite Users**
✕

You can invite people to join by sending them an invitation link. Inviting users is the easiest way to get your team to collaborate. Invitations expire after 14 days

test@net.com ✕

**Monitor & Optimize Role**

Guest ▼

**Cloud Secure Role**

Administrator ▼

Cancel

Invite

#### 6. 초대 \* 를 클릭합니다

초대가 사용자에게 전송됩니다. 사용자는 14일 내에 초대를 수락할 수 있습니다. 사용자가 초대를 수락하면 해당 사용자가 NetApp Cloud Portal로 이동하게 되며 초대장의 이메일 주소를 사용하여 등록하게 됩니다. 이메일 주소에 대한 기존 계정이 있는 경우 간단하게 로그인한 다음 Data Infrastructure Insights 환경에 액세스할 수 있습니다.

### 기존 사용자의 역할 수정

보조 계정 소유자 \* 로 추가하는 등 기존 사용자의 역할을 수정하려면 다음 단계를 따르십시오.

1. 관리자 > 사용자 관리 \* 를 클릭합니다. 화면에 시스템의 모든 계정 목록이 표시됩니다.
2. 변경할 계정의 사용자 이름을 클릭합니다.
3. 필요에 따라 각 Data Infrastructure Insights 기능 세트에서 사용자 역할을 수정합니다.
4. 변경 내용 저장 \_ 을(를) 클릭합니다.

보조 계정 소유자를 지정합니다

계정 소유자 역할을 다른 사용자에게 할당하려면 관찰 가능성의 계정 소유자로 로그인해야 합니다.

1. 관리자 > 사용자 관리 \* 를 클릭합니다.
2. 변경할 계정의 사용자 이름을 클릭합니다.

3. 사용자 대화 상자에서 \* 소유자로 할당 \* 을 클릭합니다.


4. 변경 사항을 저장합니다.

**Daniel** ✕

---

<b>Email</b>	<b>Last Login</b>
user.name@netapp.com	a year ago

---

[Learn about the permissions provided by each role](#) 

**Owner Role**

[Assign as Owner](#)

**Monitor & Optimize Role**

Administrator ▼

**Cloud Secure Role**

Administrator ▼

---

[Delete User](#) [Cancel](#) [Save Changes](#)

계정 소유자는 원하는 만큼 많을 수 있지만 소유자 역할은 선택한 사용자만 하도록 제한하는 것이 가장 좋습니다.

## 사용자 삭제

관리자 역할을 가진 사용자는 사용자 이름을 클릭하고 대화 상자에서 \_사용자 삭제\_를 클릭하여 사용자(예: 더 이상 회사에 없는 사용자)를 삭제할 수 있습니다. 사용자가 Data Infrastructure Insights 환경에서 제거됩니다.

사용자가 생성한 대시보드, 쿼리 등은 사용자가 제거된 후에도 Data Infrastructure Insights 환경에서 계속 사용할 수 있습니다.

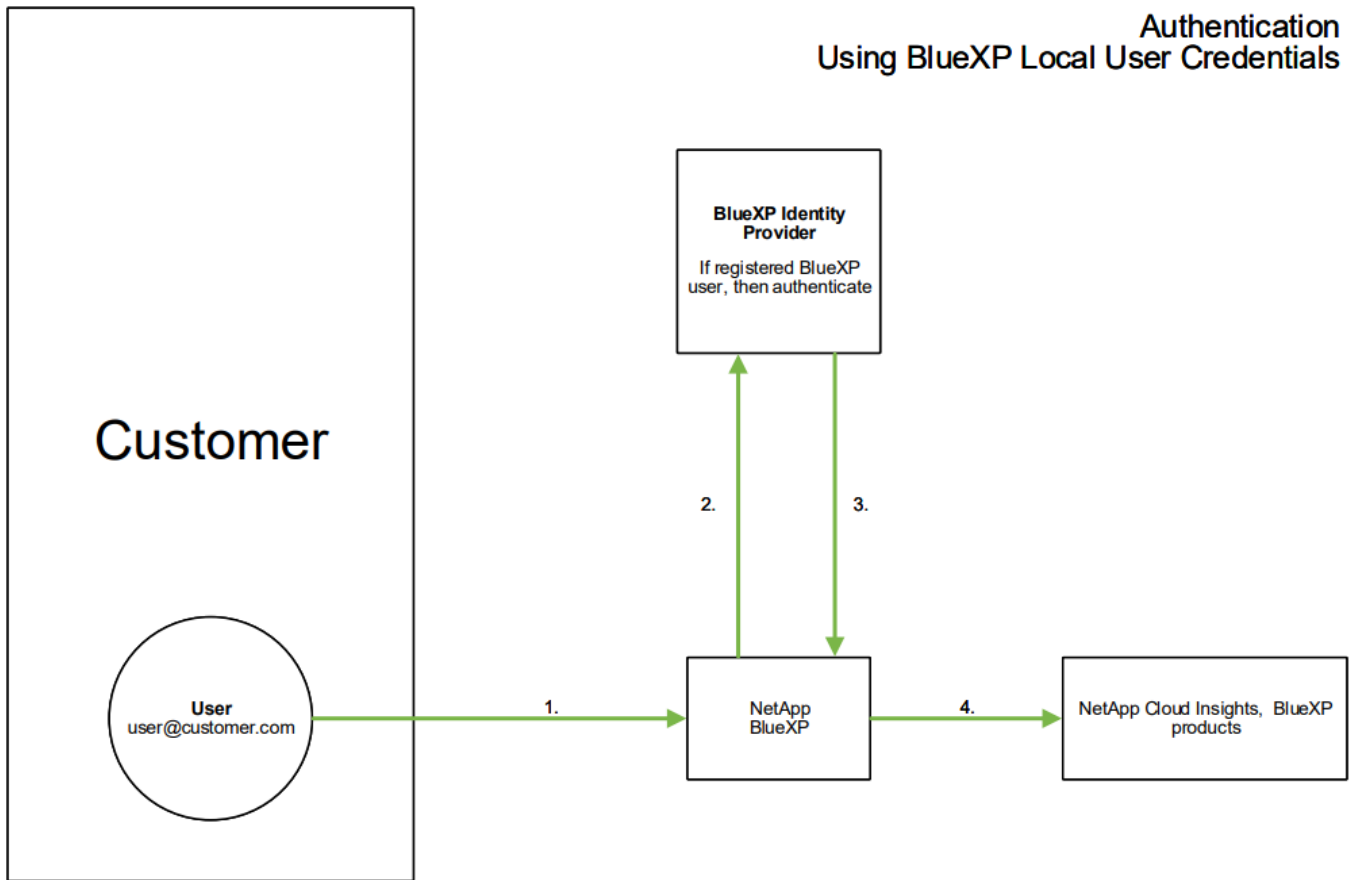
## SSO(Single Sign-On) 및 ID 페더레이션

ID 페더레이션이란 무엇입니까?

ID 페더레이션 사용:

- 기업 디렉토리에서 고객의 자격 증명을 사용하여 고객의 ID 관리 시스템에 인증을 위임하고 MFA(Multi-Factor Authentication)와 같은 자동 인증 정책을 수행합니다.
- 사용자는 모든 NetApp BlueXP 서비스(단일 사인온)에 한 번 로그인합니다.

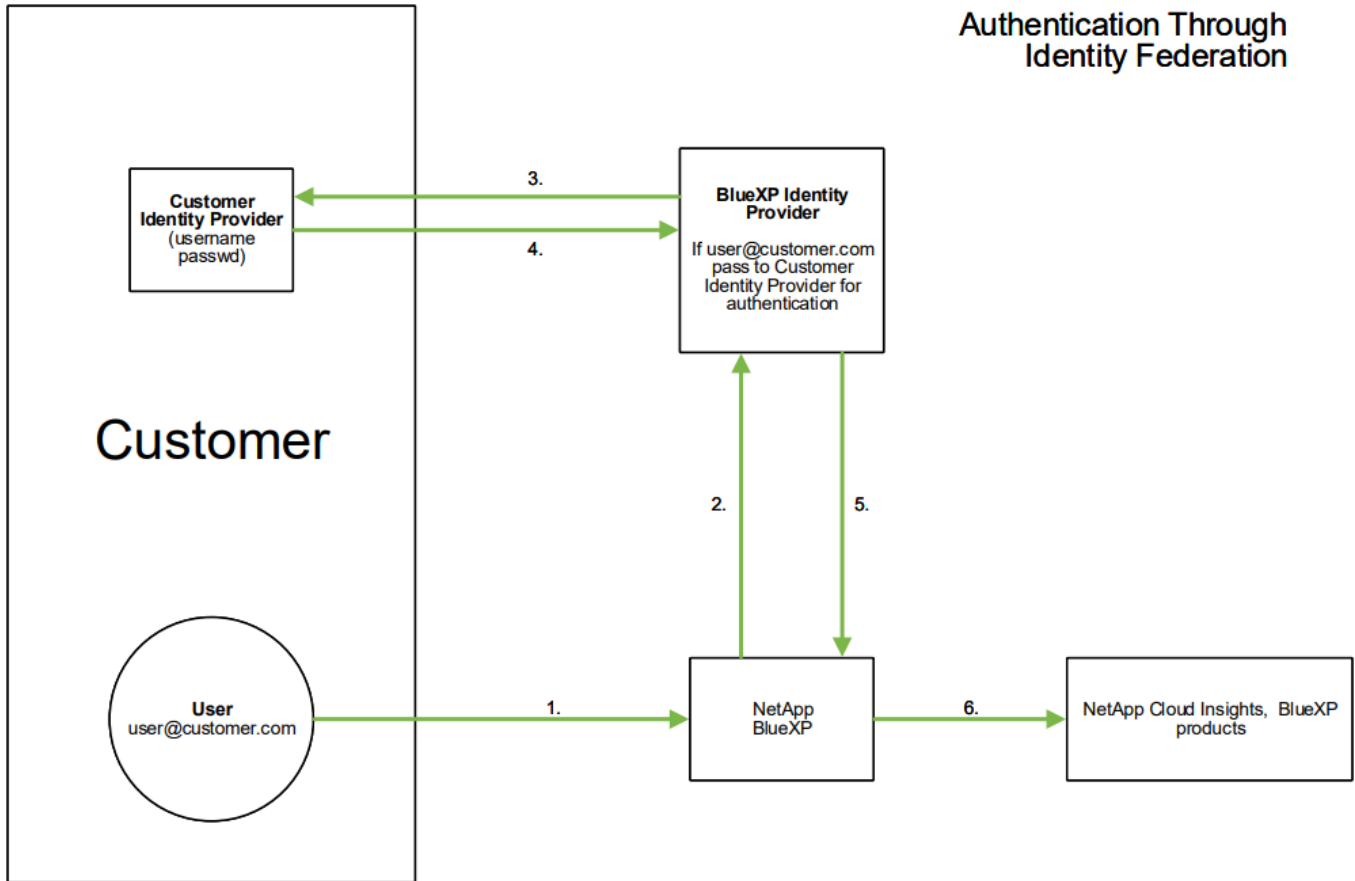
모든 클라우드 서비스의 NetApp BlueXP에서 사용자 계정을 관리합니다. 기본적으로 인증은 BlueXP 로컬 사용자 프로필을 통해 수행됩니다. 다음은 이 프로세스에 대한 간단한 개요입니다.



그러나 일부 고객은 자신의 ID 공급자를 사용하여 Data Infrastructure Insights 및 기타 NetApp BlueXP 서비스에 대한 사용자를 인증하려고 합니다. ID 페더레이션 사용하면 NetApp BlueXP 계정은 회사 디렉터리의 자격 증명을 사용하여 인증됩니다.

다음은 이 프로세스의 간단한 예입니다.

## Authentication Through Identity Federation



위 다이어그램에서 사용자가 Data Infrastructure Insights에 액세스할 때 해당 사용자는 인증을 위해 고객의 ID 관리 시스템으로 연결됩니다. 계정이 인증되면 사용자는 Data Infrastructure Insights 테넌트 URL로 연결됩니다.

**ID 페더레이션을 사용하도록 설정하는 중입니다**

BlueXP는 Auth0을 사용하여 Identity Federation을 구현하고 ADFS(Active Directory Federation Services) 및 Microsoft Azure AD(Active Directory) 등의 서비스와 통합됩니다. ID 페더레이션을 구성하려면 을 참조하십시오 "[BlueXP Federation 지침](#)".



데이터 인프라 Insights에서 SSO를 사용하려면 먼저 BlueXP ID 페더레이션을 구성해야 합니다.

BlueXP 에서 변경되는 ID 페더레이션은 데이터 인프라 통찰력뿐만 아니라 모든 NetApp BlueXP 서비스에도 적용된다는 것을 이해하는 것이 중요합니다. 고객은 자신이 소유한 각 BlueXP 제품의 NetApp 팀과 이 변경 사항에 대해 논의하여 사용 중인 구성이 ID Federation과 연동되는지 또는 계정을 조정해야 하는 경우, 고객은 ID 페더레이션의 변경에 내부 SSO 팀을 참여시켜야 합니다.

또한 ID 페더레이션이 활성화되면 회사 ID 공급자를 변경(SAML에서 Microsoft AD로 이동)할 때 사용자 프로필을 업데이트하기 위해 BlueXP의 문제 해결/변경/주의가 필요할 수 있음을 인지해야 합니다.

이 문제나 다른 페더레이션 문제에 대해 에서 지원 티켓을 열 수 있습니다 [https://mysupport.netapp.com/site/help bluexp.netapp.com](https://mysupport.netapp.com/site/help/bluexp.netapp.com) > **Federation Issues** 범주를 선택합니다.

**SSO(Single Sign-On) 사용자 자동 프로비저닝**

관리자는 사용자를 초대하는 것 외에도 사내 도메인의 모든 사용자를 개별적으로 초대하지 않고도 \* SSO(Single Sign-



On) 사용자 자동 프로비저닝 \* 에 대한 Data Infrastructure Insights 액세스를 활성화할 수 있습니다. SSO를 사용하면 동일한 도메인 이메일 주소를 가진 모든 사용자가 회사 자격 증명을 사용하여 Data Infrastructure Insights에 로그인할 수 있습니다.



\_SSO 사용자 자동 프로비저닝 \_ 은(는) Data Infrastructure Insights Premium Edition에서 사용할 수 있으며, Data Infrastructure Insights에서 사용하려면 먼저 구성해야 합니다. SSO 사용자 자동 프로비저닝 구성에는 "ID 페더레이션"위의 섹션에 설명된 대로 NetApp BlueXP 를 통해 포함됩니다. 페더레이션을 사용하면 SAML(Security Assertion Markup Language) 및 OIDC(OpenID Connect)와 같은 공개 표준을 사용하여 기업 디렉터리의 자격 증명을 사용하여 NetApp BlueXP 계정에 액세스할 수 있습니다.

SSO 사용자 자동 프로비저닝 \_ 을(를) 구성하려면 \* 관리자 > 사용자 관리 \* 페이지에서 먼저 BlueXP ID 페더레이션을 설정해야 합니다. 배너에서 \* Set Up Federation \* 링크를 선택하여 BlueXP Federation으로 이동합니다. 구성이 완료되면 Data Infrastructure Insights 관리자가 SSO 사용자 로그인을 활성화할 수 있습니다. 관리자가 SSO 사용자 자동 프로비저닝 을(를) 사용하도록 설정할 경우, 모든 SSO 사용자(예: 게스트 또는 사용자)의 기본 역할을 선택합니다. SSO를 통해 로그인하는 사용자는 이 기본 역할을 갖게 됩니다.

Set up Identity Federation to sign in using your organization credentials.

Dismiss

Set Up Federation

관리자가 단일 사용자를 기본 SSO 역할(예: 관리자로 설정)에서 승격하려고 하는 경우가 있습니다. 사용자는 \* Admin > User Management \* 페이지에서 오른쪽 메뉴를 클릭하고 \_Assign Role\_ 을 선택하여 이 작업을 수행할 수 있습니다. 이러한 방식으로 명시적 역할이 할당된 사용자는 \_SSO 사용자 자동 프로비저닝 \_ 이(가) 이후에 비활성화되더라도 계속해서 Data Infrastructure Insights에 액세스할 수 있습니다.

사용자에게 더 이상 상승된 역할이 필요하지 않으면 메뉴를 클릭하여 사용자 \_ 제거 \_ 를 수행할 수 있습니다. 사용자가 목록에서 제거됩니다. SSO 사용자 자동 프로비저닝 \_ 이(가) 활성화된 경우 기본 역할을 사용하여 SSO를 통해 Data Infrastructure Insights에 계속 로그인할 수 있습니다.

SSO 사용자 표시 \* 확인란의 선택을 취소하여 SSO 사용자를 숨기도록 선택할 수 있습니다.

그러나 다음 중 하나에 해당하는 경우 \_SSO 사용자 자동 프로비저닝 \_ 을 활성화하지 마십시오.

- 조직에 둘 이상의 Data Infrastructure Insights 테넌트가 있습니다
- 조직에서는 페더레이션 도메인의 모든 사용자가 Data Infrastructure Insights 테넌트에 대한 일정 수준의 자동 액세스 권한을 갖기를 원하지 않습니다. \_ 이 시점에는 \_ 옵션을 사용하여 그룹을 사용하여 역할 액세스를 제어할 수 없습니다.


## 도메인별 액세스 제한

Data Infrastructure Insights는 사용자가 지정한 도메인에만 대한 사용자 액세스를 제한할 수 있습니다. 관리자 > 사용자 관리 \* 페이지에서 "도메인 제한"을 선택합니다.

## Restrict Domains



Select which domains have access to Cloud Insights:

- No restrictions (Cloud Insights available on all domains)
- Limit access to default domains (acme.com, gmail.com, netapp.com) 
- Limit access to defaults and following domains

legal.acme.com ✕

anvils.acme.com ✕

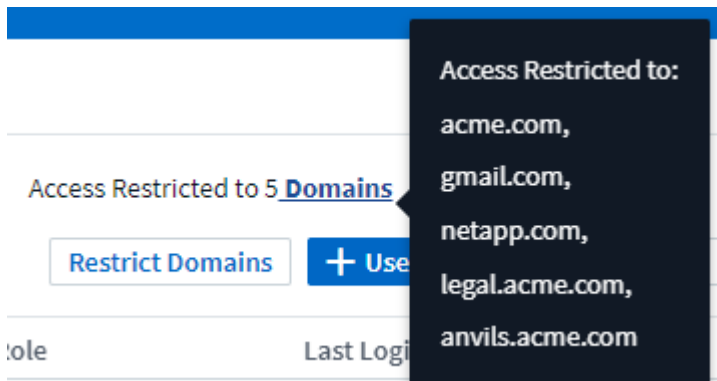
[Learn more about domain restriction.](#) 

Cancel

Save

다음과 같은 선택 사항이 제시됩니다.

- 제한 없음: Data Infrastructure Insights는 도메인에 관계없이 사용자가 계속 액세스할 수 있습니다.
- 기본 도메인에 대한 액세스 제한: 기본 도메인은 Data Infrastructure Insights 환경 계정 소유자가 사용하는 도메인입니다. 이러한 도메인은 항상 액세스할 수 있습니다.
- 기본 및 지정한 도메인으로 액세스를 제한합니다. 기본 도메인 외에 Data Infrastructure Insights 환경에 액세스할 수 있는 모든 도메인을 나열합니다.



The screenshot shows the 'Restrict Domains' dialog box with a dropdown menu open. The dropdown menu is titled 'Access Restricted to:' and lists the following domains: acme.com, gmail.com, netapp.com, legal.acme.com, and anvils.acme.com. The dialog box also shows a 'Restrict Domains' button and a '+ Use' button.

# Data Infrastructure Insights 데이터 수집기 목록

Data Infrastructure Insights는 여러 공급업체 및 서비스에서 제공하는 다양한 데이터 수집기를 지원합니다.

데이터 수집기는 다음 유형에 따라 분류됩니다.

- 인프라: 스토리지 어레이, 스위치, 하이퍼바이저 또는 백업 장치와 같은 공급업체 장치에서 수집
- 서비스: Kubernetes 또는 Docker와 같은 서비스에서 구입 통합 \_ 이라고도 합니다.

Data Infrastructure Insights에서 지원하는 데이터 수집기의 사전순 목록:

데이터 수집기	유형
"Amazon EC2 및 EBS"	검토할 수 있습니다
"스토리지로 AWS S3 저장"	인프라structure
"NetApp ONTAP용 Amazon FSx"	검토할 수 있습니다
"아파치"	서비스
"Azure NetApp Files"	검토할 수 있습니다
"Azure VM 및 VHD"	검토할 수 있습니다
"BNA(Brocade Network Advisor)"	검토할 수 있습니다
"Brocade 파이버 채널 스위치"	검토할 수 있습니다
"Brocade FOS REST "	검토할 수 있습니다
"Cisco MDS 패브릭 스위치"	검토할 수 있습니다
"영사"	서비스
"바로 Couchbase입니다"	서비스
"Couchbase"	서비스
"Cohesity SmartFiles를 참조하십시오"	검토할 수 있습니다
"Dell EMC Data Domain을 참조하십시오"	검토할 수 있습니다
"Dell EMC ECS를 참조하십시오"	검토할 수 있습니다
"Dell EMC PowerScale(이전의 Isilon)"	검토할 수 있습니다
"Dell EMC Isilon/PowerScale REST"	검토할 수 있습니다
"Dell EMC PowerStore"	검토할 수 있습니다
"Dell EMC RecoverPoint를 참조하십시오"	검토할 수 있습니다
"Dell EMC ScaleIO/PowerFlex를 참조하십시오 "	검토할 수 있습니다
"Dell EMC Unity"	검토할 수 있습니다
"Dell EMC Unisphere REST"	검토할 수 있습니다
"Dell EMC VMAX/PowerMax 장치 제품군"	검토할 수 있습니다

데이터 수집기	유형
"Dell EMC VNX 블록 스토리지"	검토할 수 있습니다
"Dell EMC VNX File"	검토할 수 있습니다
"Dell EMC VNX 유니파이드"	검토할 수 있습니다
"Dell EMC VPLEX"	검토할 수 있습니다
"Dell EMC XtremIO"	검토할 수 있습니다
"Dell XC 시리즈"	검토할 수 있습니다
"Docker 를 참조하십시오"	서비스
"Elasticsearch(Elasticsearch)"	서비스
"플링크"	서비스
"후지쯔 ETERNUS DX"	검토할 수 있습니다
"Google 컴퓨팅 및 스토리지"	검토할 수 있습니다
"하둡"	서비스
"HAProxy"	서비스
"Hitachi Content Platform(HCP)"	검토할 수 있습니다
"Hitachi Vantara Command Suite"	검토할 수 있습니다
"Hitachi Vantara NAS 플랫폼"	검토할 수 있습니다
"Hitachi Ops 센터"	검토할 수 있습니다
"HP Enterprise Alletra 6000(이전의 Nimble) 스토리지"	검토할 수 있습니다
"HP Enterprise Alletra 9000/Primera(이전 3PAR) 스토리지"	검토할 수 있습니다
"HP Enterprise 명령 보기"	검토할 수 있습니다
"Huawei OceanStor 및 Dorado Devices"	검토할 수 있습니다
"IBM Cleversafe"	검토할 수 있습니다
"IBM CS 시리즈"	검토할 수 있습니다
"IBM PowerVM"	검토할 수 있습니다
"IBM SVC(SAN Volume Controller)"	검토할 수 있습니다
"IBM 시스템 스토리지 DS8000 시리즈"	검토할 수 있습니다
"IBM XIV 및 A9000 스토리지"	검토할 수 있습니다
"Infinidat .Box"	검토할 수 있습니다
"자바"	서비스
"카프카"	서비스
"Kapacitor"	서비스
"키바나"	서비스

데이터 수집기	유형
"쿠버네티스"	서비스
"Lenovo HX 시리즈"	검토할 수 있습니다
"멤캐시드"	서비스
"Microsoft Azure NetApp Files를 참조하십시오"	검토할 수 있습니다
"Microsoft Hyper-V를 참조하십시오"	검토할 수 있습니다
"MongoDB"	서비스
"MySQL"	서비스
"NetApp Cloud Volumes ONTAP를 참조하십시오"	검토할 수 있습니다
"AWS용 NetApp Cloud Volumes Services"	검토할 수 있습니다
"ONTAP 9.9 이상을 위한 NetApp 클라우드 연결"	검토할 수 있습니다
"NetApp Data ONTAP 7-Mode 를 참조하십시오"	검토할 수 있습니다
"NetApp E-Series를 통해 비즈니스 이점을 제공합니다"	검토할 수 있습니다
"NetApp E-Series REST "	검토할 수 있습니다
"NetApp ONTAP용 Amazon FSx"	검토할 수 있습니다
"NetApp HCI 가상 센터"	검토할 수 있습니다
"NetApp ONTAP 데이터 관리 소프트웨어"	검토할 수 있습니다
"NetApp ONTAP REST 수집기입니다 "	검토할 수 있습니다
"NetApp ONTAP Select를 참조하십시오"	검토할 수 있습니다
"NetApp SolidFire All-Flash 어레이"	검토할 수 있습니다
"NetApp StorageGRID를 참조하십시오"	검토할 수 있습니다
"netstat"	서비스
"Nginx"	서비스
"노드"	서비스
"Nutanix NX 시리즈"	검토할 수 있습니다
"더 적합하였습니다"	검토할 수 있습니다
"OpenZFS 를 선택합니다"	서비스
"Oracle ZFS Storage Appliance"	검토할 수 있습니다
"PostgreSQL"	서비스
"Puppet 에이전트"	서비스
"Pure Storage 플래시 어레이"	검토할 수 있습니다
"Red Hat 가상화"	검토할 수 있습니다
"레드입니다"	서비스
"RethinkDB를 참조하십시오"	서비스

데이터 수집기	유형
"RHEL 및 AMP, CentOS"	서비스
"Rubrik CDM 스토리지"	검토할 수 있습니다
"Ubuntu 및 amp; Debian"	서비스
"VMware vSphere를 참조하십시오"	검토할 수 있습니다
"Windows"	서비스
"ZooKeeper"	서비스

# Data Infrastructure Insights 구독

Data Infrastructure Insights를 시작하는 것은 다음 3단계만 거치면 됩니다.


- 에서 계정을 등록하십시오 **"\* NetApp BlueXP \*** 를 다운로드하십시오.
- **"\* 무료 평가판 \***"Data Infrastructure Insights에 등록하여 사용 가능한 기능을 살펴보십시오.
- \* Data Infrastructure Insights에 가입 \* 하여 **"NetApp 영업"**직접 또는 을 통해 지속적으로 데이터에 액세스할 수 **"AWS 마켓플레이스 를 참조하십시오"**있습니다.

등록 프로세스 중에 Data Infrastructure Insights 환경을 호스팅할 글로벌 지역을 선택할 수 있습니다. 자세한 내용은 데이터 인프라 인사이트 를 참조하십시오**"정보 및 지역"**.

Data Infrastructure Insights Basic 및 Premium 버전에서 사용할 수 있는 기능에 대한 전체 비교는 **"Data Infrastructure Insights 가격 책정"**페이지를 참조하십시오.



비활성 Data Infrastructure Insights Basic Edition 환경이 삭제되고 해당 리소스가 회수됩니다. 연속 7일 동안 수집된 데이터가 없는 경우, 연속으로 30일 동안 사용자 활동이 없는 경우 환경은 비활성 상태로 간주됩니다. Data Infrastructure Insights는 알림을 전송하고 환경이 삭제되기 4일의 유예 기간을 제공합니다.

Data Infrastructure Insights를 사용하는 동안 자물쇠 아이콘이  표시되면 이 기능을 현재 구독에서 사용할 수 없거나 제한된 형식으로 사용할 수 있음을 의미합니다. 전체 액세스를 위해 해당 기능을 구독하십시오. 일부 기능은 구독하기 전에 사용할 수 **모듈 평가** 있습니다.

## 평가판

Data Infrastructure Insights에 등록하면 환경이 활성 상태인 경우 Data Infrastructure Insights의 30일 무료 평가판을 이용하십시오. 이 평가판을 통해 자체 환경에서 Data Infrastructure Insights가 제공하는 기능을 살펴볼 수 있습니다.

평가 기간 동안 언제든지 Data Infrastructure Insights를 구독할 수 있습니다. Data Infrastructure Insights에 가입하면 확장된 **"\* 제품 지원 \***" 옵션과 함께 데이터에 중단 없이 액세스할 수 있습니다.

무료 평가판이 거의 끝나가면 Data Infrastructure Insights에 배너가 표시됩니다 배너 내에는 `_View Subscription_link`가 있으며, 이 링크를 클릭하면 \* Admin → Subscription \* 페이지가 열립니다. 관리자가 아닌 사용자는 배너를 볼 수 있지만 구독 페이지로 이동할 수 없습니다.



Data Infrastructure Insights를 평가하는 데 추가 시간이 필요하고 평가판이 4일 이내에 만료되도록 설정된 경우 30일 동안 평가판을 추가로 연장할 수 있습니다. 평가판을 한 번만 연장할 수 있습니다. 평가판이 만료된 경우 연장할 수 없습니다.

## AWS 마켓플레이스를 통해 평가하십시오

AWS Marketplace를 통해 무료 평가판을 등록할 수도 있습니다. AWS Marketplace 무료 평가판에서는 33일의 평가판 기간 동안 Data Infrastructure Insights에 액세스할 수 있으며 최대 499개의 **관리 단위**MU(Multi-up)까지 사용할 수 있습니다.

참고: 499MU 이상을 구성하는 경우 "위반" 상태를 입력합니다. 평가판이 위반되는 경우 구성된 MU 수를 줄이거나 Data Infrastructure Insights에 가입하여 위반이 해결될 때까지 일부 Data Infrastructure Insights 기능에 액세스할 수

없습니다.

AWS Marketplace 무료 평가판을 연장할 수 없습니다. 평가 중에 언제든지 \* Admin → Subscription \* 페이지를 방문하여 Data Infrastructure Insights Basic Edition으로 다운그레이드하거나 유료 Data Infrastructure Insights 구독으로 변경할 수 있습니다.

## 평가판이 만료된 경우 어떻게 합니까?

무료 평가판이 만료되었고 Data Infrastructure Insights를 아직 구독하지 않은 경우 구독할 때까지 기능이 제한됩니다. 데이터 수집이 중지될 수 있으며 몇 주 후에는 데이터 보존 정책에 따라 데이터가 삭제됩니다.

## 구독이 만료된 경우 어떻게 해야 합니까?

Data Infrastructure Insights에 가입했지만 구독이 만료된 경우, 구독을 갱신하기 위한 5일의 유예 기간이 주어집니다. 이 유예 기간 동안에는 모든 Data Infrastructure Insights 기능이 활성 상태로 유지됩니다.

유예 기간이 경과하면 갱신할 때까지 Data Infrastructure Insights 기능이 일시 중단됩니다. 갱신하려면 \* 관리 > 구독 \* 페이지를 참조하거나 NetApp 세일즈 팀에 문의하십시오.



유예 기간이 종료될 때까지 수집된 Data Infrastructure Insights 데이터는 유예 기간 후 30일 동안 그대로 유지됩니다. 이 시간 내에 구독을 갱신하면 유예 기간이 경과할 때까지 모든 데이터를 사용할 수 있습니다.

## 가입 \* 이 만료된 경우 어떻게 해야 합니까?

Data Infrastructure Insights에 가입했지만 구독이 만료된 경우, 구독을 갱신하기 위한 5일의 유예 기간이 주어집니다. 이 유예 기간 동안에는 모든 Data Infrastructure Insights 기능이 활성 상태로 유지됩니다.

유예 기간이 경과하면 갱신할 때까지 Data Infrastructure Insights 기능이 일시 중단됩니다. 갱신하려면 \* 관리 > 구독 \* 페이지를 참조하거나 NetApp 세일즈 팀에 문의하십시오.



Data Infrastructure Insights 데이터는 유예 기간 후 30일 동안 그대로 유지됩니다. 이 시간 내에 구독을 갱신하면 유예 기간이 경과할 때까지 모든 데이터를 사용할 수 있습니다.

## 모듈 평가

모듈 평가 \* 를 활용할 수도 있습니다. 예를 들어, 인프라 관측성을 이미 구독하고 있지만 Kubernetes를 환경에 추가하고 있는 경우, NetApp Kubernetes 모니터링 운영자를 설치하는 시점부터 Kubernetes 관측성 30일 평가를 자동으로 시작합니다. 평가 기간이 끝날 때까지만 Kubernetes 관측성 관리형 유닛 사용에 대한 요금이 부과됩니다.



평가 후 새 관리형 유닛(MU) 사용에 대한 비용이 청구되므로 이에 따라 계획을 세워야 합니다. 모듈 평가가 종료되면 서비스 중단을 방지하기 위해 MU를 더 추가해야 하는 경우 알림이 표시됩니다.

사용 \* 탭의 \* 관리 > 구독 \* 페이지에서 관리 유닛의 사용을 모니터링할 수 있습니다.



Total Usage and Entitlement



Usage By Module



Infrastructure Observability | Kubernetes Observability

Installed Data Collectors (2) Bulk Actions Filter...

<input type="checkbox"/>	Name	Type	Hosts	Raw Storage Capacity (TiB)	Select Object Storage Capacity (TiB)	Metered Managed Units	Managed Units Adjustment	Consumed Managed Units	
<input type="checkbox"/>	rtp-sa-ef540-02	NetApp E-Series	0	40	0	10	(0)	10	⋮
<input type="checkbox"/>	CDS-User-01	Amazon EC2 and EBS	6	8	0	5	(0)	5	⋮



A Module Evaluation 은(는) Trial 이 아닙니다. - Dell은 고객에게 Data Infrastructure Insights 서비스를 사용하여 적합성 및 구매 가능성을 확인하는 무료 평가판 기간을 제공할 때 이 용어 평가판을 사용합니다. 모듈 평가는 다릅니다. 유료 고객이 최근 몇 달 동안 유료 구독에 사용하지 않았던 Data Infrastructure Insights 모듈을 사용해 볼 수 있도록 하는 것입니다. 평가가 활성화되면 새로 구성된 모듈에 대한 요금이 면제됩니다. 작업 중인 고객 환경은 아직 구독 중이며 무료 평가판으로 전환되지 않았습니다. 구독이 변경되지 않았습니다.

### 평가자

모듈 평가 중에는 모듈에 사용된 리소스에 대한 MU 사용량이 변경되지 않습니다. 그러나 Summary tab에 있는 \* Estimator \* 를 열어 평가 후 MU 비용이 어떻게 부과되는지 확인하고 향후 필요한 MU의 수를 사용하여 "What if" 시나리오를 연습할 수 있습니다. 추정기를 종료하여 숫자를 재설정합니다.

Managed Unit (MU) Usage Estimate Renewal Cost

<input checked="" type="checkbox"/> Infrastructure Observability <span>?</span>	20 Hosts	20 Raw TiB	0 Object TiB	Current Usage	Managed Units = 15
<input checked="" type="checkbox"/> Kubernetes Observability <span>?</span>	40 vCPUs	Current Usage			Managed Units = 10

모듈 옆에 있는 확인란을 선택하여 예상 비용에서 전체 모듈의 MU를 추가하거나 제거합니다.

Estimator를 사용하면 현재 구독 기간을 유지하고 라이선스가 부여된 관리 유닛 수를 늘리는 추가 기능 또는 현재 구독 시 구입할 갱신 구독의 갱신 옵션을 확인할 수 있습니다 기간 종료.

고객은 구독당 한 번만 모듈 평가를 받을 수 있습니다.

### 구독 옵션

구독하려면 \* 관리자 → 구독 \* 으로 이동하십시오. \* Subscribe \* 버튼 외에도 설치된 데이터 수집기를 보고 예상 측량을 계산할 수 있습니다. 일반적인 환경의 경우 셀프 서비스 AWS Marketplace 버튼을 클릭합니다. 사용자 환경에 1,000개 이상의 관리되는 단위가 포함되거나 포함될 것으로 예상되는 경우 볼륨 가격 책정을 이용할 수 있습니다.

## 관측성 계측

Data Infrastructure Insights 인프라 관측성 및 Kubernetes 관측성은 \* Managed Unit \* 에 따라 측정됩니다. 관리되는 유닛의 사용은 인프라 환경에서 관리되는 \* 호스트 또는 가상 머신 \* 수와 \* 포맷되지 않은 용량 \* 의 양에 따라 계산됩니다.

- 관리 유닛 1개 = 호스트 2개(가상 또는 물리적 시스템)
- 1 관리 유닛 = 4TiB의 물리적 디스크 또는 가상 디스크 포맷 안 됨 용량
- 1개의 관리형 유닛 = 일부 보조 스토리지의 포맷되지 않은 용량 40TiB(AWS S3, Cohesity SmartFiles, Dell EMC Data Domain, Dell EMC ECS, Hitachi Content Platform, IBM Cleversafe, NetApp StorageGRID, Rubrik 포함).
- 1개의 관리형 유닛 = Kubernetes의 vCPU 4개
  - 1 관리 유닛 K8 조정 = 2개의 노드 또는 호스트도 인프라에서 모니터링됨

사용자 환경에 1,000개 이상의 관리되는 장치가 포함되거나 포함될 것으로 예상되는 경우 \* Volume Pricing \* 을 받을 자격이 있으며 NetApp 영업 팀에 연락하여 구독을 신청하라는 메시지가 표시됩니다. 을 참조하십시오 [아래에 있습니다](#) 를 참조하십시오.

## 워크로드 보안 측정

워크로드 보안은 관측성 측정과 동일한 접근 방식을 사용하여 클러스터에 의해 측정됩니다.

워크로드 보안 \* 탭의 \* Admin > Subscription \* 페이지에서 워크로드 보안 사용을 볼 수 있습니다.

Admin / Subscription



기존 워크로드 보안 서브스크립션의 MU 사용량이 조정되어 노드 사용량이 관리되는 유닛을 소비하지 않습니다. Data Infrastructure Insights는 사용이 허가된 사용에 대한 준수를 보장하기 위해 사용량을 측정합니다.

## 가입하려면 어떻게 해야 합니까?

관리 유닛 수가 1,000개 미만인 경우 NetApp 세일즈 또는 을 통해 구독할 수 있습니다 [자체 구독](#) 출처: AWS

## NetApp Sales Direct를 통해 구독하십시오

예상 관리 단위 수가 1,000 이상인 경우 를 클릭합니다 **\*\* 영업팀에 문의 \*\*** NetApp 세일즈 팀을 통해 구독하는 단추

NetApp 세일즈 담당자에게 데이터 인프라 인사이트 \* 일련 번호 \* 를 제공하여 유료 구독을 데이터 인프라 인사이트 환경에 적용할 수 있도록 해야 합니다. 일련 번호는 Data Infrastructure Insights 평가판 환경을 고유하게 식별하며 \* Admin > Subscription \* 페이지에서 찾을 수 있습니다.

## AWS Marketplace를 통해 직접 구독



기존 Data Infrastructure Insights 평가판 계정에 AWS Marketplace 구독을 적용하려면 계정 소유자 또는 관리자여야 합니다. 또한 AWS(Amazon Web Services) 계정이 있어야 합니다.

Amazon Marketplace 링크를 클릭하면 AWS "데이터 인프라 인사이트" 구독 페이지가 열리고 구독을 완료할 수 있습니다. 계산기에 입력한 값은 AWS 가입 페이지에 채워지지 않습니다. 이 페이지에서 총 관리 단위 수를 입력해야 합니다.

총 관리 단위 수를 입력하고 12개월 또는 36개월 가입 기간을 선택한 후 \* 계정 설정 \* 을 클릭하여 가입 프로세스를 완료합니다.

AWS 구독 프로세스가 완료되면 Data Infrastructure Insights 환경으로 다시 돌아갑니다. 또는 환경이 더 이상 활성 상태가 아닌 경우(예: 로그아웃한 경우) NetApp BlueXP 로그인 페이지로 이동합니다. Data Infrastructure Insights에 다시 로그인하면 구독이 활성화됩니다.



AWS Marketplace 페이지에서 \* 계정 설정 \* 을 클릭한 후 1시간 이내에 AWS 가입 프로세스를 완료해야 합니다. 1시간 이내에 완료하지 않으면 \* 계정 설정 \* 을 다시 클릭하여 프로세스를 완료해야 합니다.

문제가 있고 가입 프로세스가 제대로 완료되지 않으면 환경에 로그인할 때 "평가판 버전" 배너가 계속 표시됩니다. 이 경우 \* Admin > Subscription \* 으로 이동하여 구독 프로세스를 반복할 수 있습니다.

## 구독 상태를 확인하십시오

가입이 활성화되면 \* 관리자 > 구독 \* 페이지에서 구독 상태 및 관리되는 유닛 사용량을 확인할 수 있습니다.

구독 \* 요약 \* 탭에는 다음과 같은 항목이 표시됩니다.

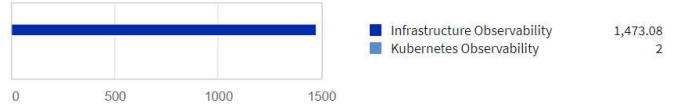
- 최신 버전
- 가입 일련 번호
- 현재 MU 권한

사용 \* 탭은 현재 MU 사용량 및 데이터 수집기별로 해당 사용량을 분석하는 방법을 보여줍니다.

Total Usage and Entitlement



Usage by Module



Infrastructure Observability Kubernetes Observability

Last updated 04/11/2024 2:25:33 PM

Installed Data Collectors (90)

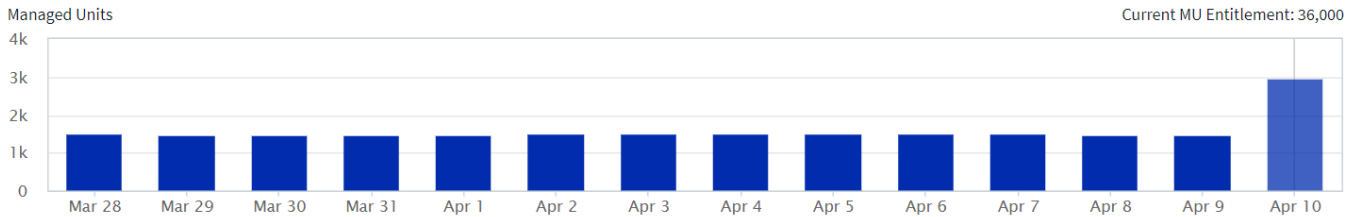
Bulk Actions Filter...

Name	Type	Hosts	Raw Storage Capacity (TiB)	Select Secondary Storage Capacity (TiB)	Metered MUs	MUs Adjustmer
muccbc_vcenter01	VMware vSphere	310	0.00	0.00	155.00	(0.00)

History \* 탭은 지난 7-90일 동안의 MU 사용량에 대한 정보를 제공합니다. 차트의 열 위로 마우스를 가져가면 모듈별 분류(예: 관측성, Kubernetes)가 제공됩니다.

Last 14 days

Consumption by Module



Legend

04/10/2024	
Infrastructure Observability	2,939.53
Kubernetes Observability	11.00
<b>Total Metered MUs (rounded)</b>	<b>2,951</b>

## 사용 관리를 봅니다

Usage Management 탭에는 Managed Unit 사용량에 대한 개요와 Collector 또는 Kubernetes Cluster에 의한 Managed Unit Consumption을 세분하는 탭이 표시됩니다.



Unformatted Capacity Managed Unit 수는 환경의 총 물리적 용량의 합계를 반영하며 가장 가까운 관리되는 단위로 반올림됩니다.



관리되는 유닛의 합계는 요약 섹션의 데이터 수집기 수와 약간 다를 수 있습니다. 관리 단위 수가 가장 가까운 관리 단위로 반올림되기 때문입니다. Data Collector 목록에서 이러한 숫자의 합계는 상태 섹션의 총 관리 단위 수보다 약간 높을 수 있습니다. 요약 섹션에는 구독에 대한 실제 관리 단위 수가 반영됩니다.

사용량이 구독 금액을 거의 또는 초과하는 경우 데이터 수집기를 삭제하거나 Kubernetes 클러스터 모니터링을 중지하여 사용량을 줄일 수 있습니다. "점 3개" 메뉴를 클릭하고 `_Delete_`를 선택하여 이 목록의 항목을 삭제합니다.

## 구독 사용량을 초과하면 어떻게 됩니까?

관리되는 장치 사용량이 전체 구독 금액의 80%, 90% 및 100%를 초과하면 경고가 표시됩니다.

* 사용량이 다음을 초과할 경우: *	* 이 경우/권장되는 작업은 다음과 같습니다. *
<ul style="list-style-type: none"> <li>• 80% *</li> </ul>	정보 배너가 표시됩니다. 별도의 조치가 필요하지 않습니다.
<ul style="list-style-type: none"> <li>• 90% *</li> </ul>	경고 배너가 표시됩니다. 구독한 관리 단위 수를 늘릴 수 있습니다.
<ul style="list-style-type: none"> <li>• 100% *</li> </ul>	오류 배너는 다음 중 하나를 수행할 때까지 표시됩니다. <ul style="list-style-type: none"> <li>• 데이터 수집기를 제거하여 관리 유닛 사용량이 구독 금액 이하가 되도록 합니다</li> <li>• 구독한 관리되는 유닛 수를 늘리려면 구독을 수정하십시오</li> </ul>

## 직접 구독하고 평가판을 건너뛰십시오

또한 "[AWS 마켓플레이스 를 참조하십시오](#)" 평가판 환경을 만들지 않고 에서 Data Infrastructure Insights를 직접 구독할 수도 있습니다. 가입이 완료되고 환경이 설정되면 즉시 가입됩니다.

## 권한 ID 추가

데이터 인프라 인사이트 와 함께 번들로 제공되는 유효한 NetApp 제품을 소유한 경우 해당 제품 일련 번호를 기존 Data Infrastructure Insights 구독에 추가할 수 있습니다. 예를 들어, NetApp Astra Control Center를 구매한 경우 Astra Control Center 라이선스 일련 번호를 사용하여 Data Infrastructure Insights에서 구독을 식별할 수 있습니다. Data Infrastructure Insights는 이 `A_Entitlement ID` \_를 나타냅니다.

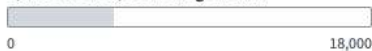
Data Infrastructure Insights 구독에 권한 ID를 추가하려면 \* Admin > Subscription \* 페이지에서 `_ + Entitlement ID` \_를 클릭합니다.

### Subscription Summary

NetApp Serial Number: 95001014387268156333  
Active Edition: Premium  
[+ Entitlement ID](#)

#### Usage and Entitlement

5,122 out of 18,000 Managed Units



Hosts: 1,388 Managed Units (2,776 Hosts)

Unformatted Capacity: 3,734 Managed Units (14,934 TB)

#### Subscription Details

36 Months (Premium Edition)

Expires: March 3rd, 2022



[Modify Subscription](#)

[Estimate Cost](#)

# 관찰 가능성

## 대시보드 만들기

### 대시보드 개요

Data Infrastructure Insights는 다양한 위젯을 사용하여 사용자 지정 대시보드를 생성할 수 있도록 함으로써 사용자가 인프라 데이터의 운영 뷰를 생성할 수 있는 유연성을 제공하며, 각 위젯은 데이터를 표시하고 차트화할 수 있는 광범위한 유연성을 제공합니다.



이 섹션의 예는 설명을 위한 것이며 가능한 모든 시나리오를 다루지는 않습니다. 이 문서의 개념 및 단계를 사용하여 자신의 대시보드를 만들어 특정 요구 사항에 맞는 데이터를 강조할 수 있습니다.

### 대시보드 생성

다음 두 위치 중 하나에 새 대시보드를 만듭니다.

- 대시보드 > [+새 대시보드] \*
- 대시보드 > 모든 대시보드 표시 > \* [+대시보드] \* 버튼을 클릭합니다

### 대시보드 컨트롤

대시보드 화면에는 다음과 같은 몇 가지 컨트롤이 있습니다.

- \* 시간 선택기 \*: 최근 15분에서 최근 30일까지 또는 최대 31일의 사용자 지정 시간 범위에 대한 대시보드 데이터를 볼 수 있습니다. 개별 위젯에서 이 전역 시간 범위를 재정의할 수 있습니다.
- \* 편집 \* 버튼: 이 버튼을 선택하면 편집 모드가 활성화되며, 이 모드를 통해 대시보드를 변경할 수 있습니다. 새 대시보드는 기본적으로 편집 모드로 열립니다.
- \* 저장 \* 버튼: 대시보드를 저장하거나 삭제할 수 있습니다.

Save \* 를 클릭하기 전에 새 이름을 입력하여 현재 대시보드의 이름을 바꿀 수 있습니다.

- \* 위젯 추가 \* 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

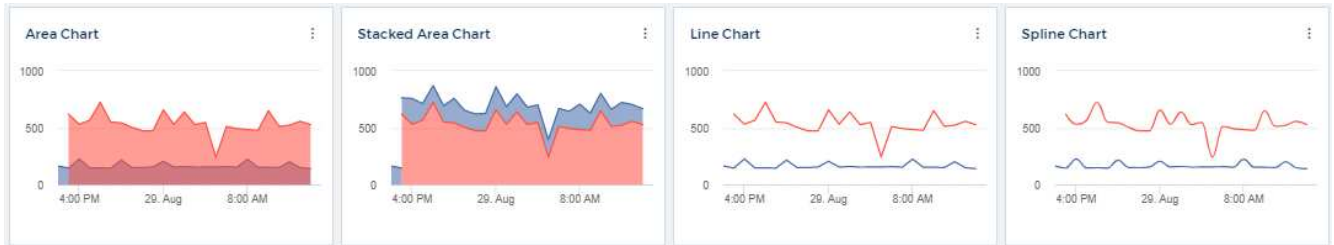
다음 위젯 유형 중에서 선택할 수 있습니다.

- \* 표 위젯 \*: 선택한 필터 및 열에 따라 데이터를 표시하는 테이블 테이블 데이터를 축소 및 확장할 수 있는 그룹으로 결합할 수 있습니다.

4 items found in 2 groups

Active Date	Storage Node	Cache Hit Ratio - Total (%)	IOPS - Total (IO...	IOPS - Write (L...	Latency
06/01/2020 (1)	ocinaneqa1-01	N/A	N/A	N/A	N/A
06/01/2020	ocinaneqa1-01	N/A	N/A	N/A	N/A
N/A (3)	--	N/A	N/A	N/A	N/A

- \* 선, 자유곡선, 영역, 누적 영역형 차트 \*: 시간 경과에 따라 성능 및 기타 데이터를 표시할 수 있는 시계열 차트 위젯입니다.



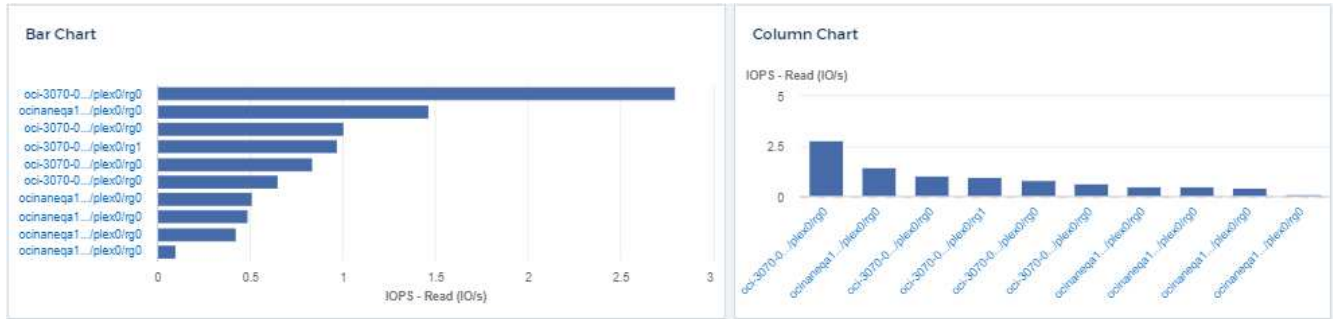
- \* 단일 값 위젯 \*: 카운터로부터 직접 유도하거나 쿼리 또는 표현식을 사용하여 계산할 수 있는 단일 값을 표시할 수 있는 위젯. 색 서식 임계값을 정의하여 값이 예상 범위, 경고 범위 또는 위험 범위에 있는지 여부를 표시할 수 있습니다.



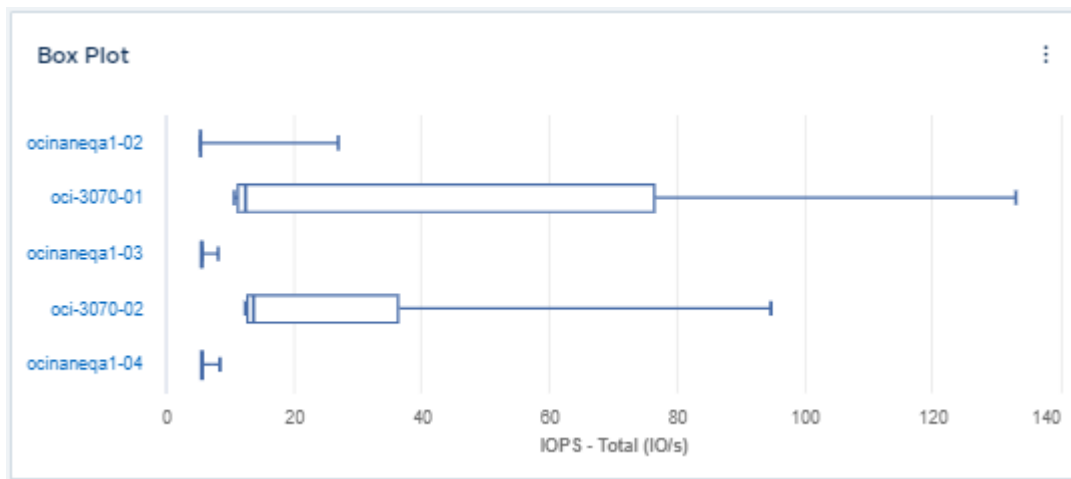
- \* 게이지 위젯 \*: 기존(솔리드) 게이지 또는 글머리 기호 게이지에 단일 값 데이터를 표시하고 "경고" 또는 "위험" 값을 기준으로 색상을 표시합니다 "사용자 지정".



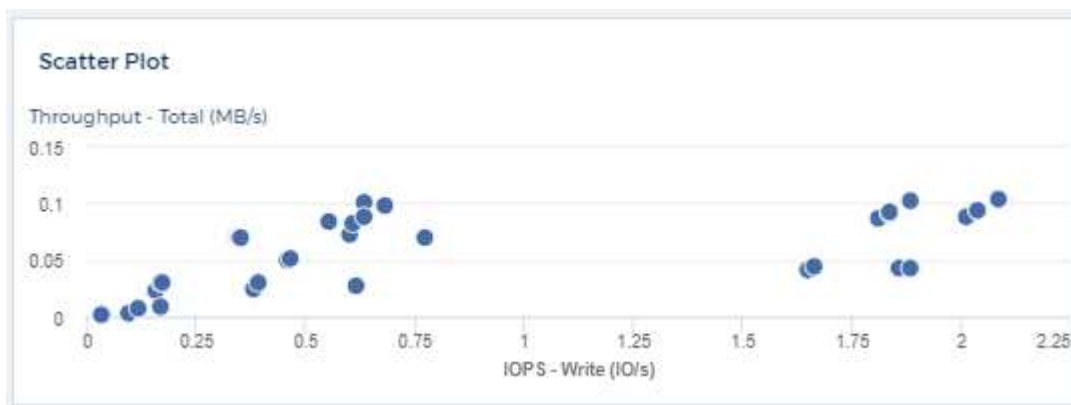
- \* 막대, 세로 막대형 차트 \*: 위쪽 또는 아래쪽 N 값(예: 용량별 상위 10개 스토리지 또는 하위 5개 볼륨 IOPS 기준)을 표시합니다.



- \* 상자 도표 도표 \*: 단일 차트에서 데이터의 최소, 최대, 중앙값 및 하위 사분점과 상위 사분위 사이의 범위에 대한 플롯.

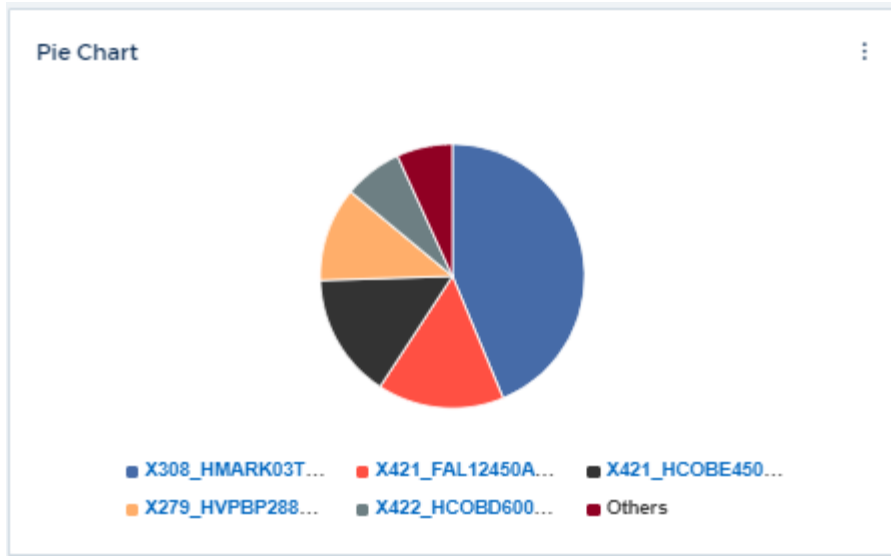


- \* 산란 플롯 차트 \*: IOPS 및 지연 시간과 같은 점으로 관련 데이터를 플롯합니다. 이 예에서는 높은 처리량과 낮은 IOPS를 갖춘 자산을 빠르게 찾을 수 있습니다.

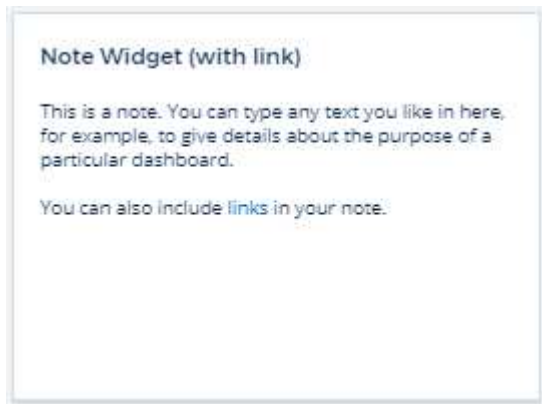


- \* 파이 차트 \*: 데이터를 총계의 한 부분으로 표시하는 전통적인 파이 차트.





- \* 메모 위젯 \*: 최대 1000자의 무료 텍스트



- \* 알림 표 \*: 최대 1,000개의 알림을 표시합니다.

이러한 기능 및 기타 대시보드 기능에 대한 자세한 설명을 보려면 ["여기를 클릭하십시오"](#).

대시보드를 홈 페이지로 설정

다음 방법 중 하나를 사용하여 환경의 \* 홈 페이지 \* 로 설정할 대시보드를 선택할 수 있습니다.

- 대시보드 > 모든 대시보드 표시 \* 로 이동하여 사용자 환경의 대시보드 목록을 표시합니다. 원하는 대시보드 오른쪽의 옵션 메뉴를 클릭하고 \* 홈 페이지로 설정 \* 을 선택합니다.
- 목록에서 대시보드를 클릭하여 대시보드를 엽니다. 상단 모서리에 있는 드롭다운 메뉴를 클릭하고 \* 홈 페이지로 설정 \* 을 선택합니다.

## 대시보드 기능

대시보드와 위젯은 데이터가 표시되는 방식을 매우 유연하게 지원합니다. 다음은 사용자 지정 대시보드를 최대한 활용하는 데 도움이 되는 몇 가지 개념입니다.

## 위젯 이름 지정

위젯은 첫 번째 위젯 쿼리에 대해 선택한 오브젝트, 메트릭 또는 속성을 기반으로 자동으로 이름이 지정됩니다. 위젯에 대한 그룹화를 선택한 경우 "그룹화 기준" 특성이 자동 명명(집계 방법 및 메트릭)에 포함됩니다.

The screenshot shows a configuration interface for a widget. At the top, there is a text input field containing the expression "Maximum cpu.time\_active by agent\_node\_ip". Below this, there are three colored labels: "C" (orange), "B" (blue), and "A" (purple). The main configuration area includes a "Query" section with "A) Query" checked, "Chart Type" set to "Bar Chart", "Chart Color" set to blue, and "Decimal Places" set to 2. Below this, the "Object" is "agent.node", the "Metric" is "cpu.time\_active", and the "Display Unit" is "cpu.time\_active (None)". The "Aggregated by" dropdown is set to "Last". The "Group by" dropdown is set to "agent\_node\_ip", and the "aggregated by" dropdown is set to "Maximum". The "Apply f(x)" dropdown is set to "Rank", and the "Rank" dropdown is set to "Top", with a value of "10".

새 개체 또는 그룹화 특성을 선택하면 자동 이름이 업데이트됩니다.

자동 위젯 이름을 사용하지 않으려면 새 이름을 입력하기만 하면 됩니다.

## 위젯 배치 및 크기

모든 대시보드 위젯은 특정 대시보드의 필요에 따라 배치 및 사이징할 수 있습니다.

## 위젯 복제

대시보드 편집 모드에서 위젯의 메뉴를 클릭하고 \* 복제 \* 를 선택합니다. 위젯 편집기가 시작되고, 원래 위젯의 구성이 미리 채워지고 위젯 이름에 "copy" 접미사가 붙습니다. 필요한 사항을 쉽게 변경하고 새 위젯을 저장할 수 있습니다. 위젯은 대시보드 하단에 배치되며 필요에 따라 배치할 수 있습니다. 모든 변경이 완료되면 대시보드를 저장해야 합니다.

## 위젯 범례 표시 중

대시보드의 대부분의 위젯은 범례와 함께 또는 범례 없이 표시할 수 있습니다. 다음 방법 중 하나를 사용하여 위젯의 범례를 대시보드에서 설정하거나 해제할 수 있습니다.

- 대시보드를 표시할 때 위젯에서 \* 옵션 \* 버튼을 클릭하고 메뉴에서 \* 범례 표시 \* 를 선택합니다.

위젯에 표시된 데이터가 변경되면 해당 위젯에 대한 범례가 동적으로 업데이트됩니다.

범례가 표시될 때 범례가 나타내는 자산의 랜딩 페이지를 탐색할 수 있으면 범례가 해당 자산 페이지에 대한 링크로 표시됩니다. 범례에 "모두"가 표시되면 링크를 클릭하면 위젯의 첫 번째 쿼리에 해당하는 쿼리 페이지가 표시됩니다.

## 메트릭 혁신

Data Infrastructure Insights는 위젯(특히 Kubernetes, ONTAP 고급 데이터, Telegraf 플러그인 등 "사용자 지정" 또는 통합 메트릭이라는 메트릭)의 특정 메트릭에 대해 다양한 \* 변환 \* 옵션을 제공하므로 데이터를 다양한 방식으로 표시할 수 있습니다. 변환될 수 있는 메트릭을 위젯에 추가하면 다음과 같은 변환 선택 사항을 제공하는 드롭다운이 표시됩니다.

## 없음

데이터는 조작 없이 그대로 표시됩니다.

## 속도

현재 값을 이전 관찰 이후의 시간 범위로 나눈 값입니다.

## 누적

이전 값과 현재 값의 합계를 누적하는 값입니다.

## 델타

이전 관찰 값과 현재 값의 차이

## 델타 요금

델타 값을 이전 관찰 이후의 시간 범위로 나눈 값

## 누적 속도

누적 값을 이전 관찰 이후의 시간 범위로 나눈 값입니다.

메트릭을 변환해도 기본 데이터 자체는 변경되지 않고 데이터가 표시되는 방식만 변경됩니다.

## 대시보드 위젯 쿼리 및 필터

### 쿼리

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 위젯 쿼리에서 필터링

다음은 필터를 최대한 활용하기 위해 할 수 있는 몇 가지 사항입니다.

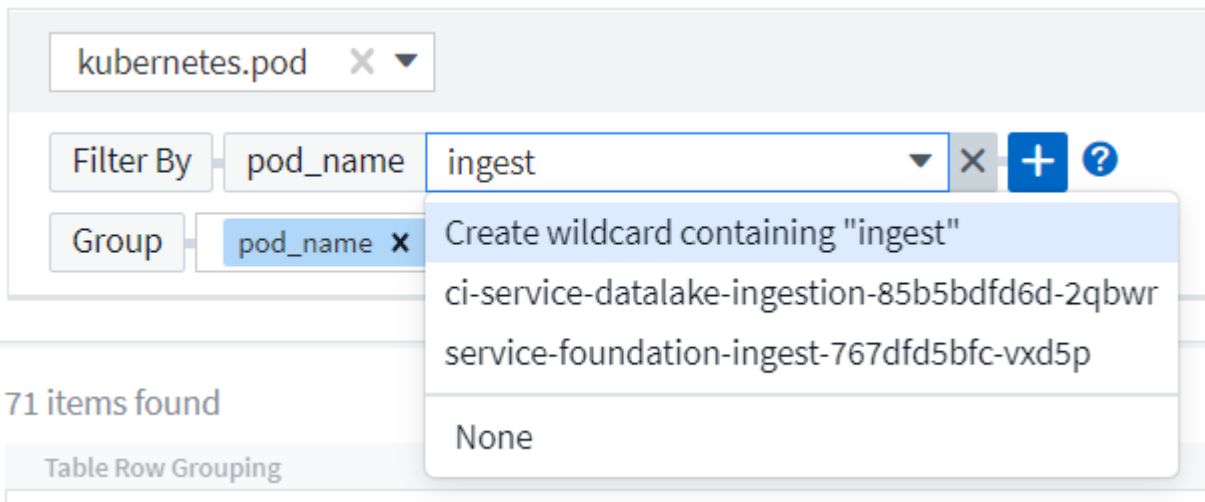
### 정확한 일치 필터링

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.

정확히 일치하는 필터를 사용하여 호스트 이름과 같은 특정 리소스를 찾을 수 있습니다. 호스트 이름 '마케팅'만 찾되 '마케팅-보스턴', '마케팅-보스턴' 등은 제외하려면 "마케팅"이라는 이름을 큰따옴표로 묶기만 하면 됩니다.

### 와일드카드와 식

쿼리 또는 대시보드 위젯에서 텍스트 또는 목록 값을 필터링할 때 입력을 시작하면 현재 텍스트를 기반으로 \* 와일드카드 필터 \* 를 만드는 옵션이 표시됩니다. 이 옵션을 선택하면 와일드카드 식과 일치하는 모든 결과가 반환됩니다. NOT 또는 OR을 사용하여 \* 식 \* 을 만들거나 "없음" 옵션을 선택하여 필드의 null 값을 필터링할 수도 있습니다.



와일드카드 또는 식(예 NOT, 또는, "없음" 등)이 필터 필드에 진한 파란색으로 표시됩니다. 목록에서 직접 선택한 항목은 연한 파란색으로 표시됩니다.

kubernetes.pod X ▼

Filter By pod\_name \*ingest\* X ci-service-audit-5f775dd975-brfdc X X ▼ X + ?

Group pod\_name X X ▼

3 items found

Table Row Grouping

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

와일드카드 및 식 필터링은 텍스트 또는 목록과 함께 사용할 수 있지만 수치, 날짜 또는 부울은 사용할 수 없습니다.

상황에 맞는 미리 입력 제안 기능을 통한 고급 텍스트 필터링

위젯 쿼리의 필터링은 `_contextual_`입니다. 필드에 대한 필터 값 또는 값을 선택하면 해당 쿼리에 대한 다른 필터에 해당 필터와 관련된 값이 표시됩니다. 예를 들어, 특정 `object_Name_`에 대한 필터를 설정할 때 `_Model_`에 대해 필터링할 필드는 해당 개체 이름과 관련된 값만 표시합니다.

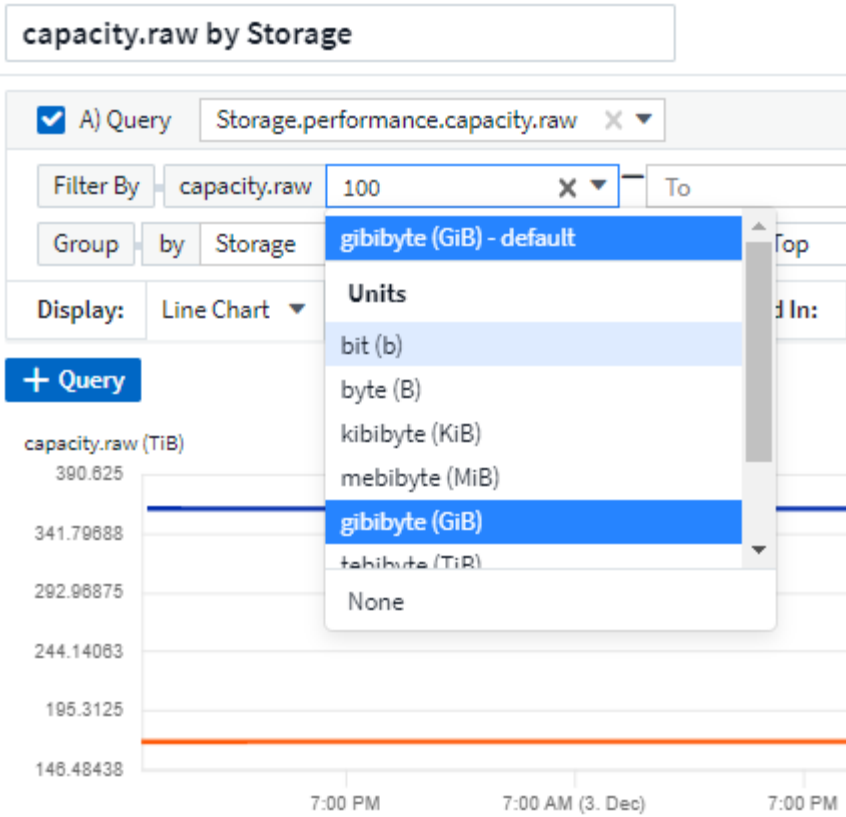
상황별 필터링은 대시보드 페이지 변수에도 적용됩니다(텍스트 형식 특성 또는 주석에만 해당). 한 변수에 대해 파일러 값을 선택하면 관련 개체를 사용하는 다른 모든 변수는 해당 관련 변수의 컨텍스트에 따라 가능한 필터 값만 표시됩니다.

텍스트 필터만 상황에 맞는 미리 보기 형식 제안을 표시합니다. 날짜, Enum(목록) 등은 미리 제안된 형식을 표시하지 않습니다. 즉, Enum(즉 목록) 필드에 필터를 설정할 수 있고 다른 텍스트 필드를 컨텍스트로 필터링할 수 있습니다. 예를 들어, 데이터 센터와 같은 Enum 필드에서 값을 선택하면 다른 필터는 해당 데이터 센터의 모델/이름만 표시하지만 그 반대는 표시하지 않습니다.

선택한 시간 범위는 필터에 표시된 데이터에 대한 컨텍스트도 제공합니다.

필터 장치 선택

필터 필드에 값을 입력할 때 차트에 값을 표시할 단위를 선택할 수 있습니다. 예를 들어, 원시 용량을 기준으로 필터링하여 기본 용량 GiB로 표시하거나, TiB와 같은 다른 형식을 선택할 수 있습니다. 대시보드에 값이 TiB로 표시된 차트가 여러 개이고 모든 차트에 일관된 값이 표시되도록 하려는 경우에 유용합니다.



### 추가 필터링 개선

다음은 필터를 더욱 구체화하는 데 사용할 수 있습니다.

- 별표를 사용하면 모든 항목을 검색할 수 있습니다. 예를 들면, 다음과 같습니다.

```
vol*rhel
```

"vol"로 시작하고 "rhel"로 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\*

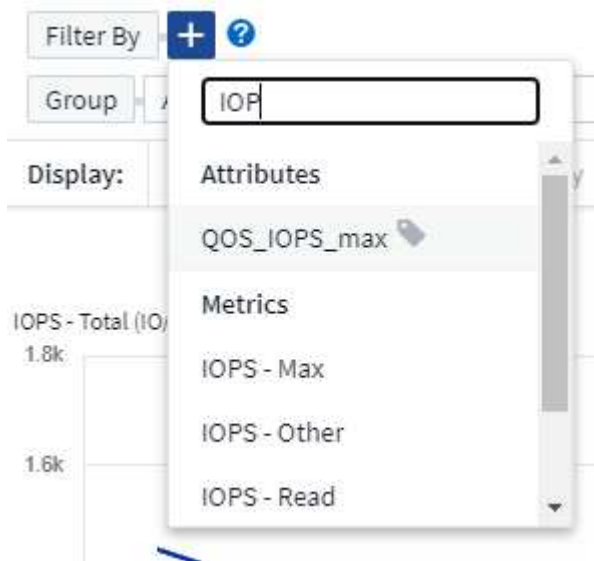
"EMC"로 시작하지 않는 모든 항목을 찾습니다. 을 사용할 수 있습니다

NOT \*

값이 없는 필드를 표시합니다.

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.



그룹화 및 집계

그룹화(압연)

위젯에 표시되는 데이터는 획득 중에 수집된 기본 데이터 포인트로부터 그룹화됩니다(롤업이라고도 함). 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 그룹화할 수 있습니다.

- \* Average \*: 각 행을 내부 데이터의 `_average_`로 표시합니다.
- \* Maximum \* (최대 \*): 각 행을 기본 데이터의 `_maximum_`으로 표시합니다.
- \* 최소 \*: 각 행을 내부 데이터의 `_최소_`로 표시합니다.
- \* Sum \*: 각 행을 원본 데이터의 `_sum_`으로 표시합니다.
- \* Count \*: 지정된 기간 내에 데이터를 보고한 개체의 `_count_`을 표시합니다. 대시보드 시간 범위에 따라 `_Entire Time Window_`를 선택할 수 있습니다.

## 단계

그룹화 방법을 설정하려면 다음을 실행합니다.

1. 위젯의 쿼리에서 자산 유형 및 메트릭(예: *Storage*) 및 메트릭(예: *Performance IOPS Total*)을 선택합니다.
2. Group \* 의 경우 롤업 방법(예: *Average*)을 선택하고 데이터를 롤업할 특성 또는 메트릭을 선택합니다(예: *Data Center*).

위젯이 자동으로 업데이트되고 각 데이터 센터의 데이터가 표시됩니다.

또한 원본으로 사용하는 데이터의 *\_ALL\_* 을 차트 또는 테이블로 그룹화할 수도 있습니다. 이 경우 위젯의 각 쿼리에 대해 하나의 줄이 표시됩니다. 이 라인은 모든 기본 자산에 대해 선택한 메트릭 또는 메트릭의 평균, 최소, 최대, 합계 또는 개수를 표시합니다.

데이터가 "모두"로 그룹화된 위젯에 대한 범례를 클릭하면 위젯에 사용된 첫 번째 쿼리의 결과를 보여주는 쿼리 페이지가 열립니다.

쿼리에 대한 필터를 설정한 경우 데이터는 필터링된 데이터를 기준으로 그룹화됩니다.

모든 필드(예: *Model*)별로 위젯을 그룹화하도록 선택한 경우에도 차트 또는 테이블에 해당 필드의 데이터를 올바르게 표시하려면 해당 필드를 기준으로 필터링해야 합니다.

## 데이터 집계

데이터 포인트를 분, 시간 또는 일 단위로 집계하여 속성(선택한 경우)에 의해 데이터가 롤업되기 전에 시계열 차트(선, 영역 등)를 추가로 정렬할 수 있습니다. 데이터 요소를 *Average*, *Maximum*, *Minimum*, *Sum* 또는 *\_Count\_* 에 따라 집계하도록 선택할 수 있습니다.

긴 시간 범위와 함께 작은 간격이 있을 경우 "집계 간격 때문에 데이터 요소가 너무 많습니다." 경고가 나타날 수 있습니다. 간격이 작고 대시보드 기간을 7일로 늘릴 경우 이 내용이 표시될 수 있습니다. 이 경우 Insight는 더 작은 기간을 선택할 때까지 집계 간격을 일시적으로 늘립니다.

막대 차트 위젯과 단일 값 위젯에서 데이터를 집계할 수도 있습니다.

대부분의 자산 카운터는 기본적으로 *Average\_* 로 집계됩니다. 일부 카운터는 기본적으로 *\_Max*, *Min* 또는 *\_Sum\_* 으로 집계됩니다. 예를 들어 포트 오류는 기본적으로 *\_Sum\_* 으로 집계되며, 여기서 스토리지 IOPS는 *\_Average\_* 로 집계됩니다.

## 위/아래 결과 표시

차트 위젯에서 롤업 데이터에 대한 \* 상위 \* 또는 \* 하위 \* 결과를 표시하고 제공된 드롭다운 목록에서 결과 수를 선택할 수 있습니다. 표 위젯에서 모든 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. 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.

## 테이블 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 테이블 위젯 유형에서만 사용할 수 있습니다.

### 그룹화 예제(롤업 설명 포함)

표 위젯을 사용하면 데이터를 그룹화하여 보다 쉽게 표시할 수 있습니다.

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 \_ Virtual Machine \_ 을(를) 선택합니다.
3. 열 선택기를 클릭하고 \_하이퍼바이저 이름\_ 과 \_IOPS - 합계\_ 를 선택합니다.

이제 이러한 열이 표에 표시됩니다.

4. IOPS가 없는 VM은 무시하고 총 IOPS가 1보다 큰 VM만 포함해보겠습니다. Filter by \* \*\* \* [+ ] \* 버튼을 클릭하고 \_IOPS - Total\_ 을 선택합니다. any\_ 를 클릭하고 \* From \* 필드에 \* 1 \* 을 입력합니다. 받는 사람 \* 필드는 비워둡니다. Enter 키를 누르고 필터 필드를 클릭하여 필터를 적용합니다.

이제 표에는 총 IOPS가 1보다 크거나 같은 모든 VM이 표시됩니다. 테이블에 그룹이 없습니다. 모든 VM이 표시됩니다.

5. Group By [+ ] \* 버튼을 클릭합니다.

표시된 속성 또는 주석별로 그룹화할 수 있습니다. 모든 VM을 단일 그룹에 표시하려면 \_ALL\_ 을 선택합니다.

성능 메트릭에 대한 열 머리글은 \* 롤업 \* 옵션이 포함된 "세 점" 메뉴를 표시합니다. 기본 롤업 방법은 \_ Average \_ 입니다. 즉, 그룹에 표시된 숫자는 그룹 내의 각 VM에 대해 보고된 총 IOPS의 평균입니다. 이 열을 \_ Average, Sum, Minimum\_ or \_Maximum\_ 으로 롤업하도록 선택할 수 있습니다. 성능 메트릭이 포함된 모든 열을 개별적으로 롤업할 수 있습니다.



6. ALL\_을 클릭하고 \_하이퍼바이저 이름\_을 선택합니다.

이제 VM 목록이 하이퍼바이저별로 그룹화됩니다. 각 하이퍼바이저를 확장하여 해당 하이퍼바이저에서 호스팅되는 VM을 볼 수 있습니다.

7. 저장 \* 을 클릭하여 테이블을 대시보드에 저장합니다. 원하는 대로 위젯의 크기를 조정하거나 이동할 수 있습니다.

8. 대시보드를 저장하려면 \* 저장 \* 을 클릭합니다.

#### 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 기본 데이터의 평균(*avg*)을 표시하는 것입니다. 데이터의 합계, 최소 또는 최대값을 표시하도록 선택할 수도 있습니다.

#### 대시보드 시간 범위 선택기

대시보드 데이터의 시간 범위를 선택할 수 있습니다. 선택한 시간 범위와 관련된 데이터만 대시보드의 위젯에 표시됩니다. 다음 시간 범위 중에서 선택할 수 있습니다.

- 최근 15분
- 마지막 30분
- 마지막 60분
- 최근 2시간
- 최근 3시간(기본값)
- 최근 6시간
- 최근 12시간
- 최근 24시간
- 최근 2일
- 지난 3일

- 최근 7일
- 지난 30일
- 사용자 지정 시간 범위

사용자 지정 시간 범위를 사용하면 최대 31일 연속 선택할 수 있습니다. 이 범위에 대한 시작 시간 및 종료 시간을 설정할 수도 있습니다. 기본 시작 시간은 선택한 첫 번째 날짜의 오전 12:00이고 기본 종료 시간은 선택한 마지막 날짜의 오후 11:59입니다. 적용 \* 을 클릭하면 사용자 지정 시간 범위가 대시보드에 적용됩니다.

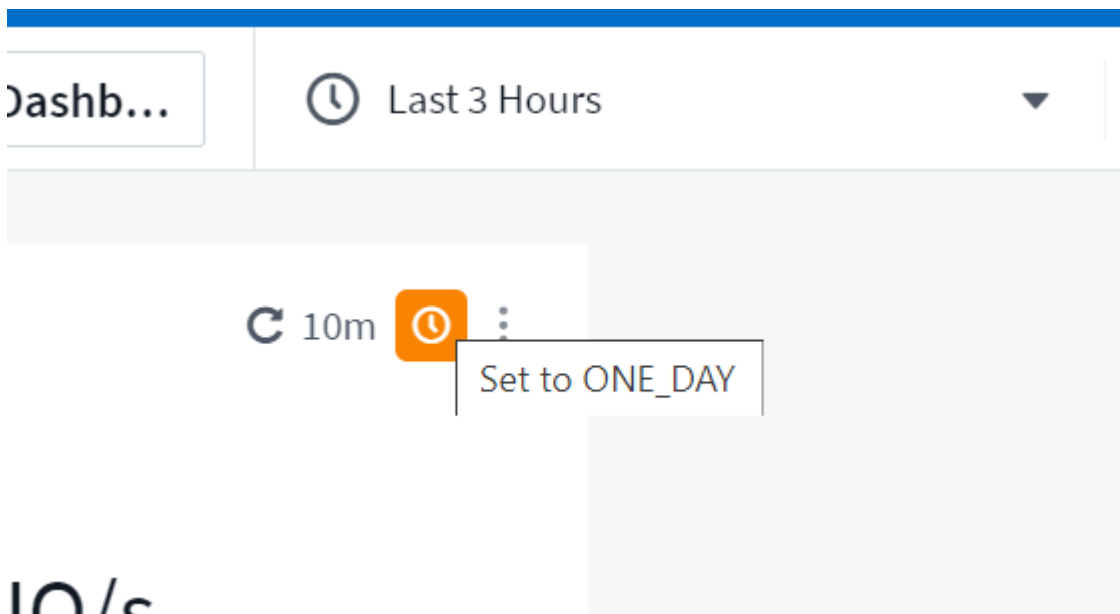
#### 개별 위젯에서 대시보드 시간 재정의

개별 위젯에서 기본 대시보드 시간 범위 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 표시된 시간 범위를 선택하고 위젯을 대시보드에 저장합니다.

위젯은 대시보드 자체에서 선택한 기간에 관계없이 위젯에 설정된 시간 프레임에 따라 데이터를 표시합니다.

한 위젯에 대해 설정한 기간은 대시보드의 다른 위젯에 영향을 주지 않습니다.



#### 기본 및 보조 축

메트릭마다 차트에서 보고하는 데이터에 대해 서로 다른 측정 단위를 사용합니다. 예를 들어, IOPS를 볼 때 측정 단위는 초당 I/O 작업 수(IOPS)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

이 예제에서는 차트 위젯의 기본 및 보조 축 개념을 보여 줍니다.

1. 대시보드를 만들거나 엽니다. 꺾은선형 차트, 스플라인 차트, 영역형 차트 또는 누적 영역형 차트 위젯을 대시보드에 추가합니다.
2. 자산 유형(예: *Storage*)을 선택하고 첫 번째 메트릭으로 `_IOPS-Total_`을 선택합니다. 원하는 필터를 설정하고 원하는 경우 롤업 방법을 선택합니다.

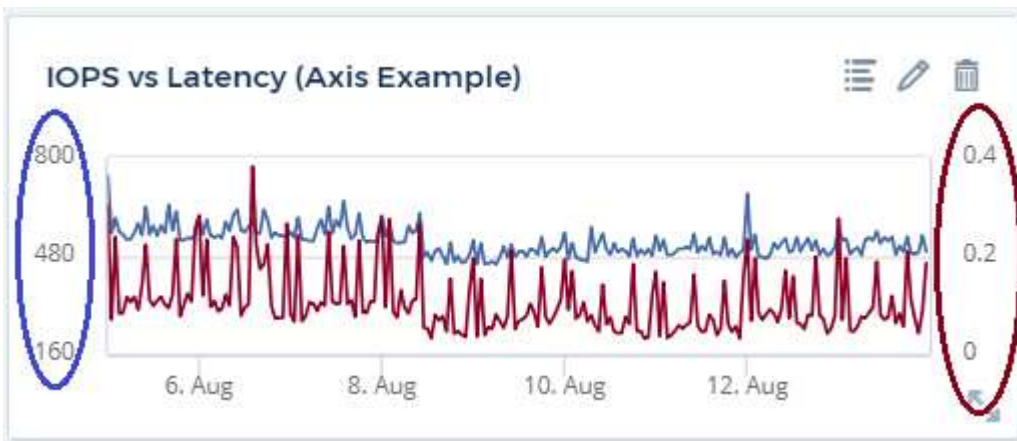
IOPS 선이 차트에 표시되고, 눈금은 왼쪽에 표시됩니다.

3. 차트에 두 번째 줄을 추가하려면 \* [+Query] \* 를 클릭합니다. 이 라인의 경우 메트릭에 대해 `_Latency-Total_`을 선택합니다.

차트 아래쪽에 선이 평평하게 표시됩니다. IOPS 라인과 동일한 스케일로 `_`이(가) 그려지기 때문입니다.

4. 지연 시간 쿼리에서 \* Y축: 보조 \* 를 선택합니다.

이제 지연 시간 선이 차트 오른쪽에 표시되는 자체 배율로 그려집니다.



### 위젯의 식

대시보드에서 모든 시계열 위젯(선, 자유곡선, 영역, 누적 영역) 막대 차트, 세로 막대형 차트, 원형 차트 또는 테이블 위젯을 사용하면 선택한 메트릭에서 표현식을 작성하고 이러한 표현식의 결과를 단일 그래프(또는 의 경우 열)에 표시할 수 있습니다 **표 위젯**)를 클릭합니다. 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 쓰는 데 직접 영향을 받지 않는 IOPS에 대한 가시성을 제공합니다.

식에 변수를 사용할 수 있습니다(예: `$var1 * 100`).

표현식 예: 읽기 **IOPS** 백분율

이 예에서는 총 IOPS의 백분율로 읽기 IOPS를 표시하려고 합니다. 이 수식을 다음과 같은 수식으로 생각할 수 있습니다.

$$\text{Read Percentage} = (\text{Read IOPS} / \text{Total IOPS}) \times 100$$

이 데이터는 대시보드의 선 그래프에 표시할 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

### 단계

1. 새 대시보드를 만들거나 편집 모드에서 기존 대시보드를 엽니다.

2. 대시보드에 위젯을 추가합니다. 영역표 \* 를 선택합니다.

위젯이 편집 모드로 열립니다. 기본적으로 쿼리는 `_IOPS - Total_for_Storage_assets`를 보여 줍니다. 원하는 경우 다른 자산 유형을 선택합니다.

3. 오른쪽에 있는 \* Expression \* 으로 변환 링크를 클릭합니다.

현재 쿼리가 식 모드로 변환됩니다. 표현식 모드에서는 자산 유형을 변경할 수 없습니다. Expression 모드에 있는 동안 링크는 \* 쿼리 \* 로 되돌리기 \* 로 변경됩니다. 언제든지 쿼리 모드로 다시 전환하려면 이 옵션을 클릭합니다. 모드 간을 전환하면 필드가 기본값으로 재설정됩니다.

지금 Expression 모드를 사용할 수 있습니다.

4. 이제 \* IOPS-Total \* 메트릭은 알파벳 변수 필드 " \* A \* "에 있습니다. " \* b \* " 변수 필드에서 \* 선택 \* 을 클릭하고 \* IOPS - 읽기 \* 를 선택합니다.

변수 필드 다음에 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. 읽기 백분율 = (읽기 IOPS/총 IOPS) x 100을 알고 있으므로 이 식을 다음과 같이 씁니다.

$(b / a) * 100$

- Label \* 필드는 표현식을 식별합니다. 레이블을 "읽기 백분율"으로 변경하거나 의미 있는 레이블을 변경합니다.
- 단위 \* 필드를 "%" 또는 "%"로 변경합니다.

선택한 스토리지 디바이스에 대한 IOPS 읽기 백분율이 차트에 표시됩니다. 원하는 경우 필터를 설정하거나 다른 롤업 방법을 선택할 수 있습니다. 합계 를 롤업 방법으로 선택하면 모든 백분율 값이 함께 추가되며, 이 값은 100%보다 높아질 수 있습니다.

6. 차트를 대시보드에 저장하려면 \* 저장 \* 을 클릭합니다.

식 예: "System" I/O

예 2: 데이터 소스에서 수집된 메트릭 중 읽기, 쓰기 및 총 IOPS가 있습니다. 그러나 데이터 소스에서 보고하는 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.

$System\ IOPS = Total\ IOPS - (Read\ IOPS + Write\ IOPS)$

그런 다음 이 데이터를 대시보드의 선 그래프로 표시할 수 있습니다. 이렇게 하려면 다음 단계를 수행하십시오.

## 단계

1. 새 대시보드를 만들거나 편집 모드에서 기존 대시보드를 엽니다.
2. 대시보드에 위젯을 추가합니다. 꺾은선형 차트 \* 를 선택합니다.

위젯이 편집 모드로 열립니다. 기본적으로 쿼리는 `_IOPS - Total_for_Storage_assets`를 보여 줍니다. 원하는 경우 다른 자산 유형을 선택합니다.

3. Roll Up \* 필드에서 `_Sum_By_All_`을 선택합니다.

차트는 총 IOPS의 합계를 표시하는 선을 표시합니다.

4. 쿼리 복사본을 만들려면 `_Duplicate this Query_`icon을 클릭하십시오.

쿼리의 복제본이 원본 아래에 추가됩니다.

5. 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.

6. 이제 `_IOPS-Total_metric`이 알파벳 변수 필드 " \* A \* "에 있습니다. `IOPS-Total_`을 클릭하고 `_IOPS-Read_`로 변경합니다.
7. " \* b\*" 변수 필드에서 \* 선택 \* 을 클릭하고 `_IOPS-쓰기_`를 선택합니다.
8. 식 \* 필드에서 각 변수에 해당하는 문자를 사용하여 식을 작성합니다. 간단히 다음과 같이 표현해 보겠습니다.

```
a + b
```

표시 섹션에서 이 식에 대해 \* 영역형 차트 \* 를 선택합니다.

9. Label \* 필드는 표현식을 식별합니다. 레이블을 "System IOPS" 또는 의미 있는 레이블로 변경합니다.

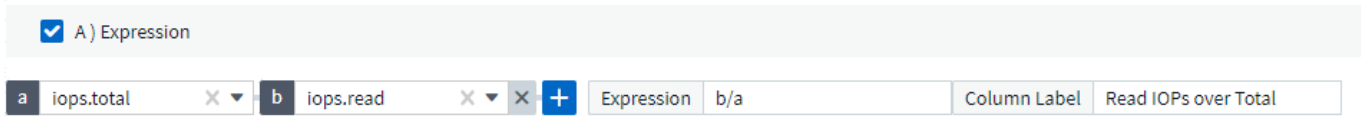
이 차트에는 총 IOPS가 선형 차트로 표시되며, 아래에 읽기 및 쓰기 IOPS의 조합이 나와 있는 영역 차트가 표시됩니다. 이 두 가지 간의 공백은 데이터 읽기 또는 쓰기 작업과 직접 관련이 없는 IOPS를 나타냅니다. 이는 "시스템" IOPS입니다.

10. 차트를 대시보드에 저장하려면 \* 저장 \* 을 클릭합니다.

식에 변수를 사용하려면 변수 이름을 입력합니다(예: `$var1 * 100`). 식에는 숫자 변수만 사용할 수 있습니다.

## 테이블 위젯의 식

테이블 위젯은 식을 약간 다르게 처리합니다. 하나의 테이블 위젯에 최대 5개의 표현식을 포함할 수 있으며 각 표현식은 테이블에 새 칼럼으로 추가됩니다. 각 식은 계산을 수행할 값을 최대 5개까지 포함할 수 있습니다. 열에 의미 있는 이름을 쉽게 지정할 수 있습니다.



## 변수

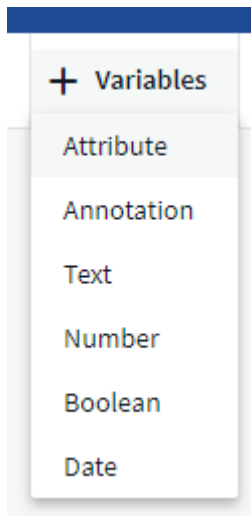
변수를 사용하면 대시보드의 일부 또는 모든 위젯에 표시된 데이터를 한 번에 변경할 수 있습니다. 하나 이상의 위젯에서 공통 변수를 사용하도록 설정하면 한 곳에서 변경한 경우 각 위젯에 표시된 데이터가 자동으로 업데이트됩니다.

대시보드 변수는 여러 가지 형식으로 제공되며 서로 다른 필드에서 사용할 수 있으며 명명 규칙을 따라야 합니다. 이러한 개념은 여기에 설명되어 있습니다.

### 변수 유형

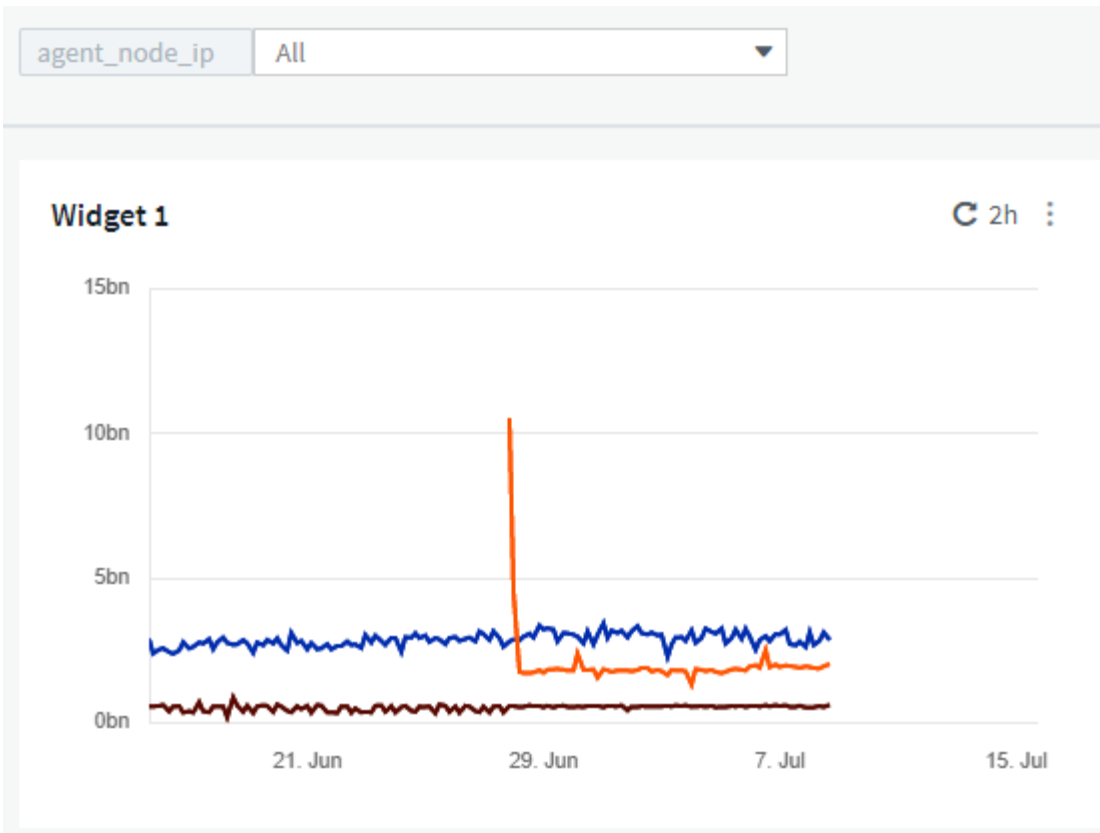
변수는 다음 형식 중 하나일 수 있습니다.

- \* 특성 \*: 오브젝트의 특성 또는 메트릭을 사용하여 필터링합니다
- \* 주식 \*: 미리 정의된 을 사용합니다 "주식" 위젯 데이터를 필터링합니다.
- \* 텍스트 \*: 영숫자 문자열입니다.
- \* 숫자 \*: 숫자 값입니다. 위젯 필드에 따라 단독으로 사용하거나 "시작" 또는 "받는 사람" 값으로 사용합니다.
- \* 부울 \*: 값이 True/False, Yes/No인 필드에 사용합니다. 부울 변수의 경우 예, 아니요, 없음, 모두 중에서 선택할 수 있습니다.
- \* 날짜 \*: 날짜 값입니다. 위젯의 구성에 따라 "보낸 사람" 또는 "받는 사람" 값으로 사용합니다.

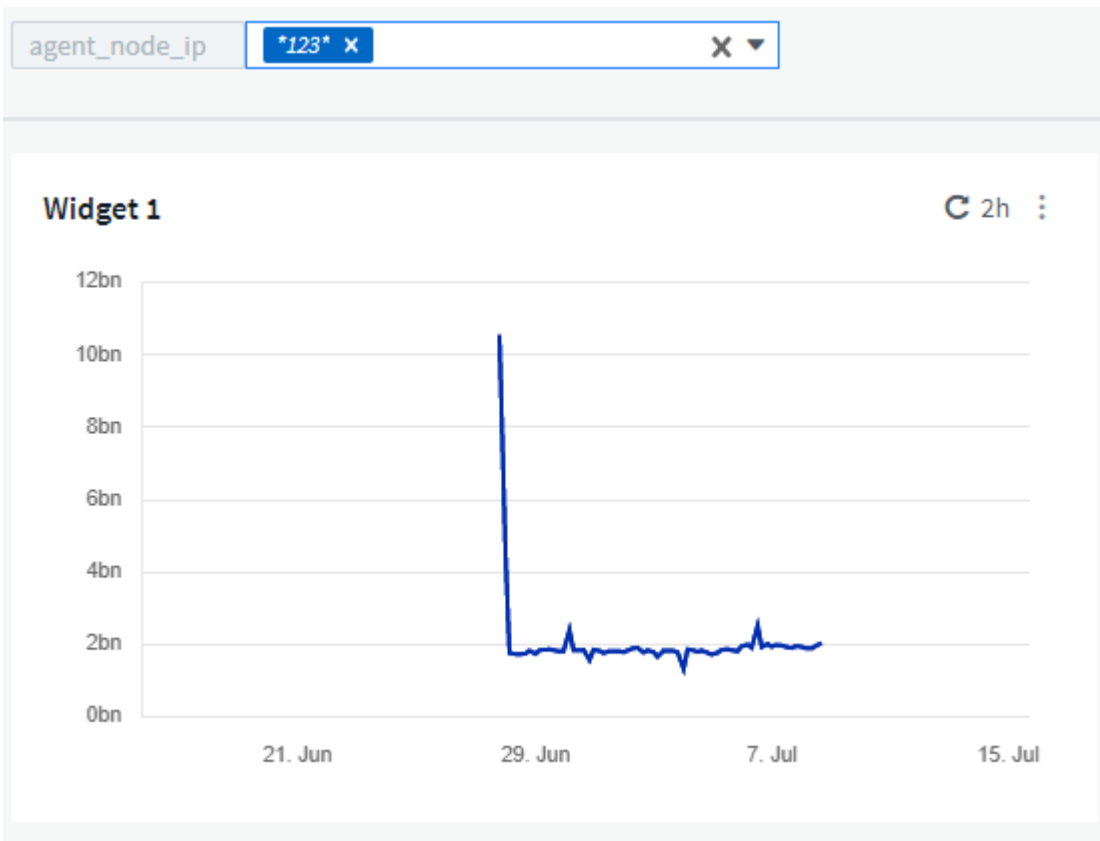


### 속성 변수

특성 유형 변수를 선택하면 지정된 특성 값 또는 값이 포함된 위젯 데이터를 필터링할 수 있습니다. 아래 예는 상담원 노드의 사용 가능한 메모리 추세를 표시하는 라인 위젯을 보여줍니다. 현재 모든 IP를 표시하도록 설정된 에이전트 노드 IP에 대한 변수를 만들었습니다.

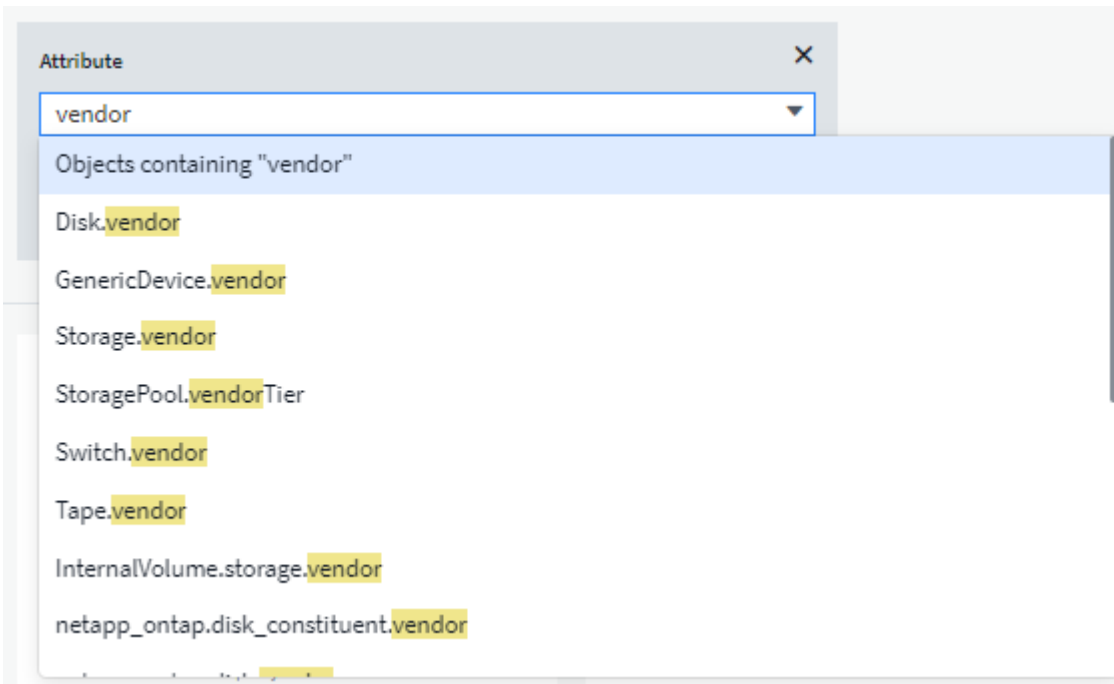


그러나 환경에 있는 개별 서버넷의 노드만 일시적으로 보려면 변수를 특정 에이전트 노드 IP 또는 IP로 설정하거나 변경할 수 있습니다. 여기서는 "123" 서버넷의 노드만 보고 있습니다.

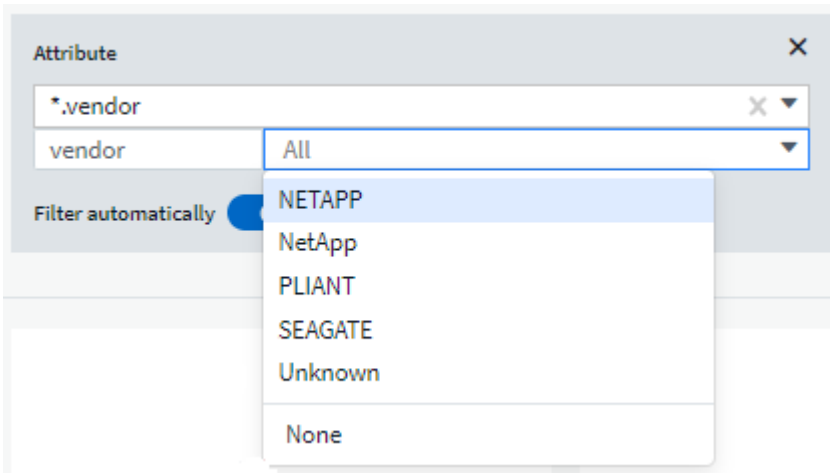




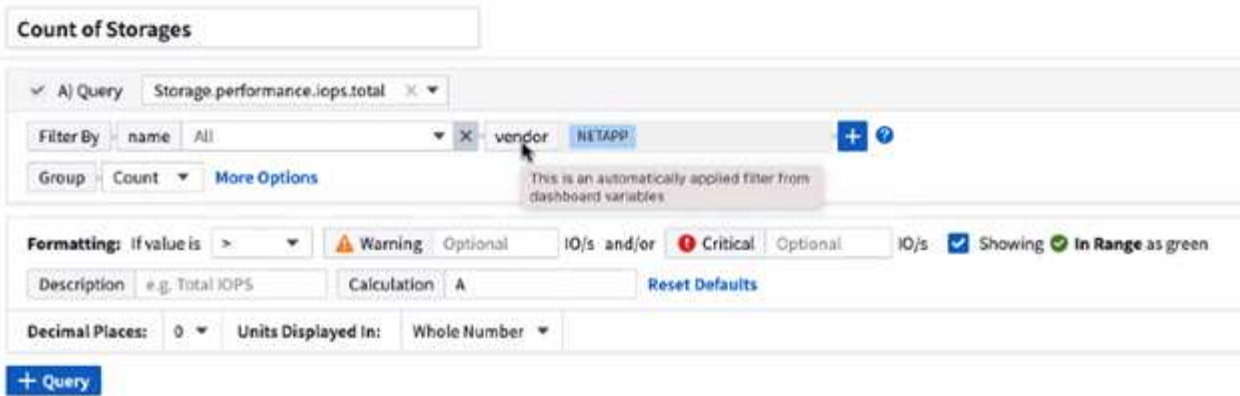
변수 필드에 `_.vendor_`를 지정하여 오브젝트 유형(예: `"vendor"` 특성이 있는 오브젝트)과 관계없이 특정 특성을 가진 `_ALL_OBJECT`에 필터를 설정할 수도 있습니다. 와일드카드 옵션을 선택한 경우 `"."`를 입력할 필요가 없습니다. 데이터 인프라 통찰력에서 이 정보를 제공합니다.



변수 값에 대한 선택 항목 목록을 드롭다운하면 결과가 필터링되어 대시보드의 개체를 기반으로 사용 가능한 공급업체만 표시됩니다.



특성 필터가 관련된(즉, 위젯의 객체에 `_.vendor attribute _`이(가) 포함된) 대시보드에서 위젯을 편집하면 특성 필터가 자동으로 적용된다는 것을 알 수 있습니다.

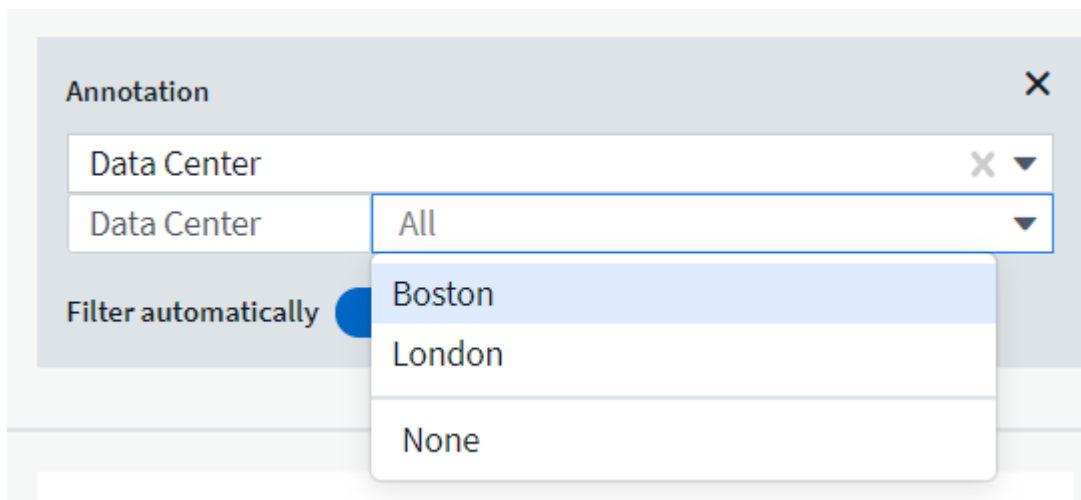


# 14

변수를 적용하는 것은 선택한 속성 데이터를 변경하는 것처럼 쉽습니다.

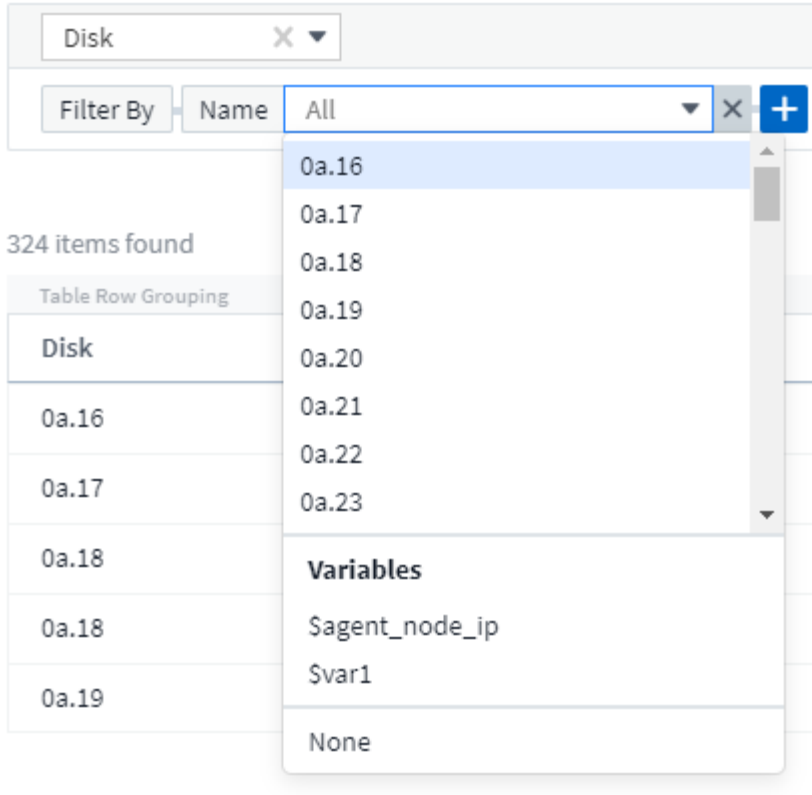
주석 변수

주석 변수를 선택하면 같은 데이터 센터에 속하는 개체와 같이 해당 주석과 관련된 개체를 필터링할 수 있습니다.



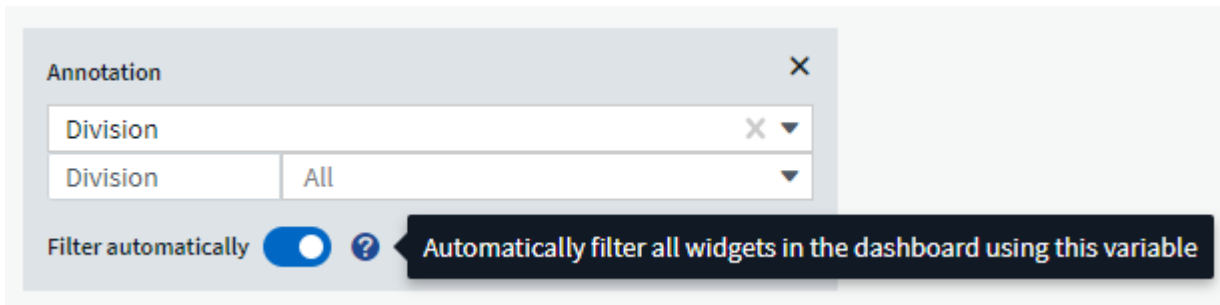
텍스트, 숫자, 날짜 또는 부울 변수입니다

*Text*, *Number*, *Boolean* 또는 *\_Date\_*의 변수 유형을 선택하여 특정 속성과 연결되지 않은 일반 변수를 만들 수 있습니다. 변수가 생성되면 위젯 필터 필드에서 변수를 선택할 수 있습니다. 위젯에서 필터를 설정할 때 필터에 대해 선택할 수 있는 특정 값 외에도 대시보드에 대해 생성된 모든 변수가 목록에 표시됩니다. 이러한 변수는 드롭다운에서 "변수" 섹션 아래에 그룹화되며 이름이 "\$"로 시작됩니다. 이 필터에서 변수를 선택하면 대시보드 자체의 변수 필드에 입력한 값을 검색할 수 있습니다. 필터에서 해당 변수를 사용하는 모든 위젯은 동적으로 업데이트됩니다.



### 변수 필터 범위

대시보드에 주석 또는 특성 변수를 추가하면 대시보드의 `_ALL_widgets`에 변수가 적용될 수 있습니다. 즉, 대시보드의 모든 위젯에 변수에 설정된 값에 따라 필터링된 결과가 표시됩니다.



이와 같이 속성 및 주석 변수만 자동으로 필터링할 수 있습니다. 비 주석 또는 - 속성 변수는 자동으로 필터링할 수 없습니다. 이러한 유형의 변수를 사용하려면 개별 위젯을 각각 구성해야 합니다.

변수를 설정한 위젯에만 적용되도록 자동 필터링을 비활성화하려면 "필터 자동" 슬라이더를 클릭하여 비활성화합니다.

개별 위젯에서 변수를 설정하려면 편집 모드에서 위젯을 열고 `_Filter by_` 필드에서 특정 주석 또는 속성을 선택합니다. 주석 변수를 사용하면 하나 이상의 특정 값을 선택하거나 변수 이름(앞에 "\$"로 표시됨)을 선택하여 대시보드 수준에서 변수를 입력할 수 있습니다. Attribute 변수에도 동일하게 적용됩니다. 변수를 설정한 위젯만 필터링된 결과를 표시합니다.

변수의 필터링은 `_contextual_`입니다. 변수의 필터 값 또는 값을 선택하면 페이지의 다른 변수에 해당 필터와 관련된 값만 표시됩니다. 예를 들어, 변수 필터를 특정 `storage_Model_`로 설정할 때 `storage_Name_`에 대해 filter로 설정된 모든 변수는 해당 모델과 관련된 값만 표시합니다.

식에 변수를 사용하려면 식의 일부로 변수 이름을 입력합니다(예:  $\$var1 * 100$ ). 식에는 숫자 변수만 사용할 수 있습니다. 식에 숫자 주석 또는 특성 변수를 사용할 수 없습니다.

변수의 필터링은 `_contextual`입니다. 변수의 필터 값 또는 값을 선택하면 페이지의 다른 변수에 해당 필터와 관련된 값만 표시됩니다. 예를 들어, 변수 필터를 특정 `storage_Model_`로 설정할 때 `storage_Name_`에 대해 filter로 설정된 모든 변수는 해당 모델과 관련된 값만 표시합니다.

### 변수 이름 지정

변수 이름:

- a-z, 0-9, 마침표(.), 밑줄(\_) 및 공백()만 포함해야 합니다.
- 20자를 초과할 수 없습니다.
- 대소문자를 구분합니다. `$CityName` 및 `$cityname`은 다른 변수입니다.
- 기존 변수 이름과 같을 수 없습니다.
- 비워둘 수 없습니다.

### 게이지 위젯 서식 지정

단색 및 글머리 기호 게이지 위젯을 사용하여 `Warning` 및/또는 `_Critical_levels`에 대한 임계값을 설정하여 지정한 데이터를 명확하게 표시할 수 있습니다.

이러한 위젯에 대한 서식을 설정하려면 다음 단계를 수행하십시오.

1. 임계값 이상의 값(>) 또는 보다 작은 값(<)을 강조 표시할지 여부를 선택합니다. 이 예제에서는 임계값 수준보다 큰 (>) 값을 강조 표시합니다.
2. "경고" 임계값에 대한 값을 선택합니다. 위젯에 이 수준보다 큰 값이 표시되면 게이지가 주황색으로 표시됩니다.
3. "Critical" 임계값에 대한 값을 선택합니다. 이 수준보다 큰 값을 사용하면 게이지가 빨간색으로 표시됩니다.

선택적으로 게이지의 최소 및 최대 값을 선택할 수 있습니다. 최소값보다 낮은 값은 게이지를 표시하지 않습니다. 최대값보다 높은 값은 전체 게이지를 표시합니다. 최소값 또는 최대값을 선택하지 않으면 위젯이 위젯의 값에 따라 최적 최소값 및 최대값을 선택합니다.



### 단일 값 위젯 포맷 중

단일 값 위젯에서 경고(주황색) 및 위험(빨간색) 임계값을 설정하는 것 외에도 "범위 내" 값(경고 수준 미만)이 녹색 또는 흰색 배경으로 표시되도록 선택할 수 있습니다.



단일 값 위젯 또는 게이지 위젯에서 링크를 클릭하면 위젯의 첫 번째 쿼리에 해당하는 쿼리 페이지가 표시됩니다.

### 표 위젯 포매팅

단일 값 및 게이지 위젯과 마찬가지로 표 위젯에서 조건부 서식을 설정하여 색 및/또는 특수 아이콘으로 데이터를 강조 표시할 수 있습니다.



조건부 서식은 현재 Data Infrastructure Insights Federal Edition에서 사용할 수 없습니다.

조건부 서식을 사용하면 테이블 위젯에서 경고 수준 및 위험 수준 임계값을 설정하고 강조 표시하여 이상값 및 예외적인 데이터 지점에 대한 즉각적인 가시성을 얻을 수 있습니다.

14 items found in 1 group

Table Row Grouping	Expanded Detail	Metrics & Attributes	capacity.provisioned (GiB)
All	Storage Pool	capacityRatio.used (%)	
All (14)	--	95.15	
--	rtp-sa-cl06-02:aggr_data1_rtp_sa_cl06_02	0.79	
--	rtp-sa-cl06-01:aggr_data1_rtp_sa_cl06_01	2.45	
--	rtp-sa-cl06-02:aggr0_rtp_sa_cl06_02_root	95.15	
--	rtp-sa-cl06-01:aggr0_rtp_sa_cl06_01_root	95.15	

Formatting:  Show Expanded Details    Conditional Formatting: Background Color + Icon     Show  In Range as green

capacity.provisioned (GiB)

> Aggregation

> Unit Display

Conditional Formatting Reset

If value is > (Greater than)

Warning 70 %

Critical 90 %

> Rename Column

조건부 서식은 표의 각 열에 대해 별도로 설정됩니다. 예를 들어 용량 열에 대한 임계값 집합 하나와 처리량 열에 대한 임계값 집합을 선택할 수 있습니다.

열의 단위 표시를 변경하면 조건부 서식이 그대로 유지되고 값의 변경 내용이 반영됩니다. 아래 이미지는 표시 단위가 다르지만 동일한 조건부 서식을 보여줍니다.

capacity.used (GiB) ↓	throughput.total (MiB/s)
40,754.06	
10,313.56	
9,544.84	
8,438.99	
6,671.72	

throughput.total (MiB/s)

> Aggregation

> Unit Display

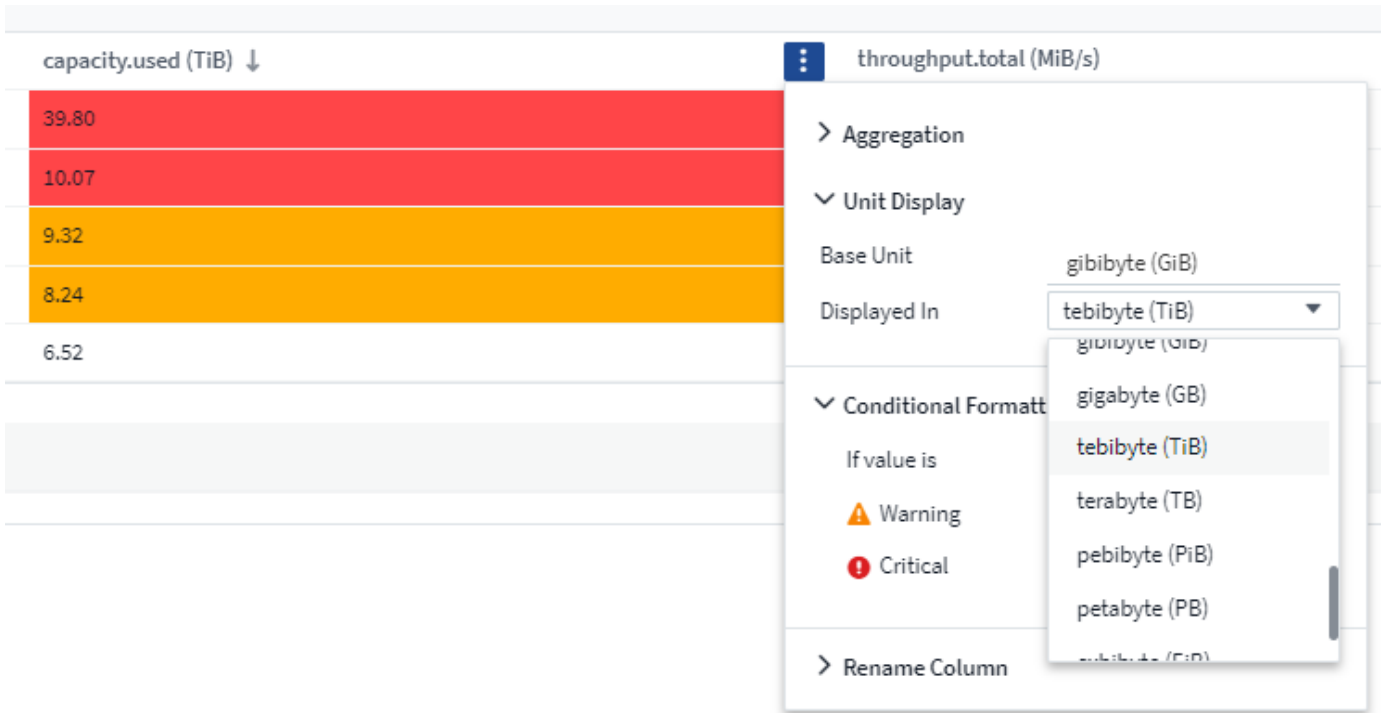
Conditional Formatting Reset

If value is > (Greater than)

Warning 8000 GiB

Critical 10000 GiB

> Rename Column

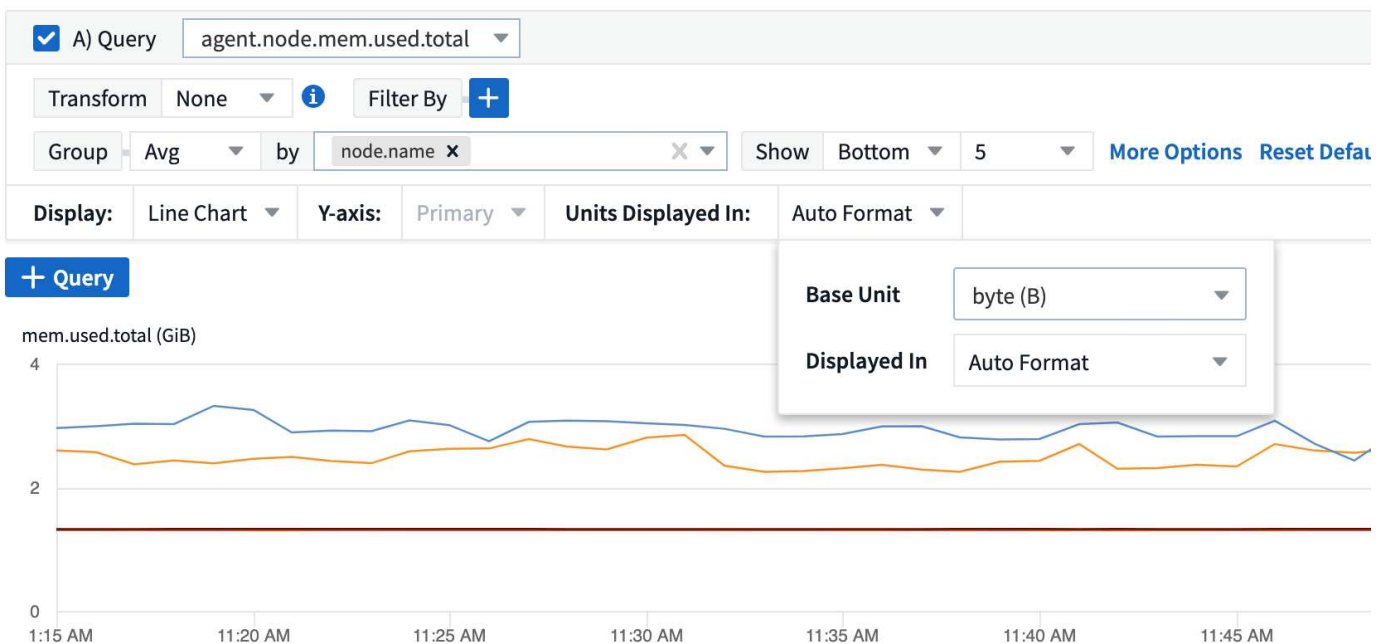


조건 서식을 색, 아이콘 또는 둘 모두로 표시할지 여부를 선택할 수 있습니다.

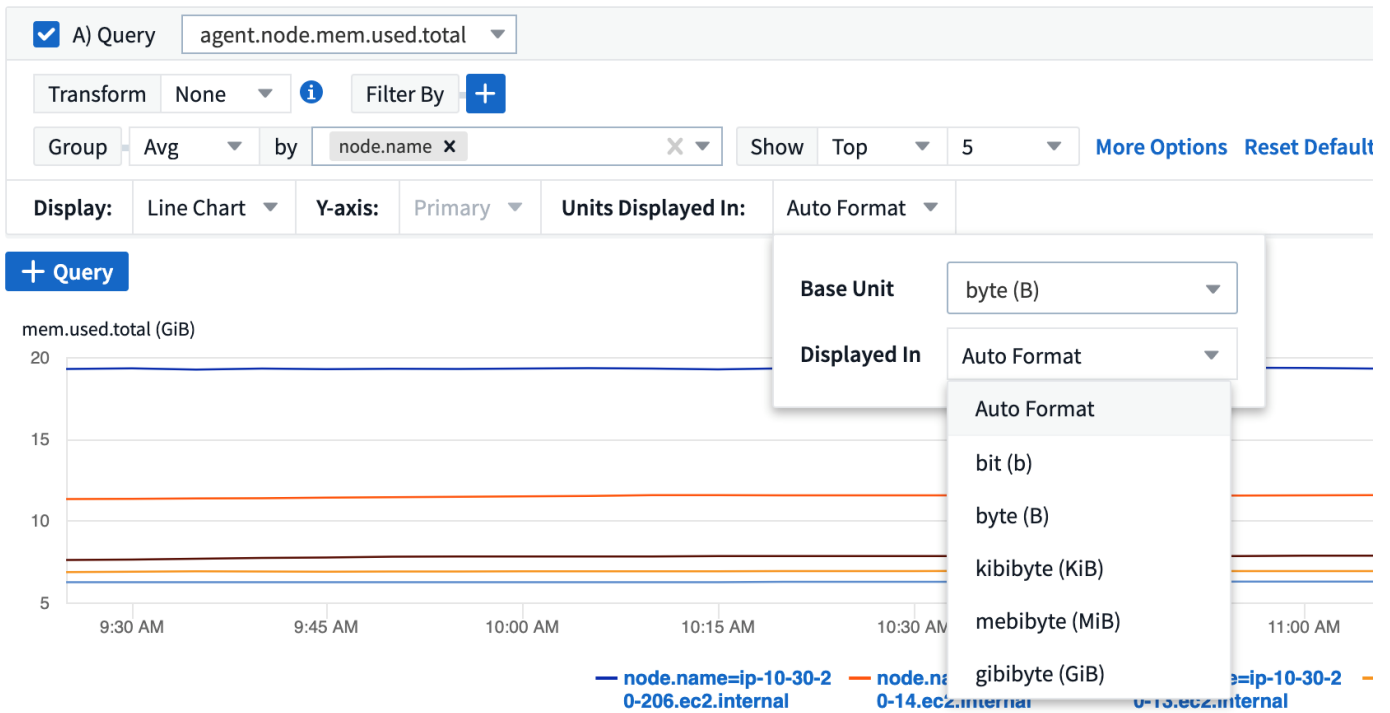
### 데이터를 표시할 단위 선택

대시보드의 대부분의 위젯에서는 값을 표시할 단위를 지정할 수 있습니다(예: *Megabytes*, 수천, 백분율, 밀리초(*ms*)). 대부분의 경우 Data Infrastructure Insights는 가져오는 데이터에 가장 적합한 형식을 알고 있습니다. 최상의 형식을 모르는 경우 원하는 형식을 설정할 수 있습니다.

아래 선형 차트 예에서 위젯에 대해 선택한 데이터는 `_bytes_` (기본 IEC 데이터 단위: 아래 표 참조)로 알려져 있으므로 기본 단위는 자동으로 'byte (B)'로 선택됩니다. 그러나 데이터 값이 기비바이트(GiB)로 표시될 만큼 크기 때문에 Data Infrastructure Insights는 기본적으로 값을 GiB로 자동 포맷합니다. 그래프의 Y축은 표시 단위로 'GiB'를 나타내고, 모든 값은 해당 단위를 기준으로 표시됩니다.

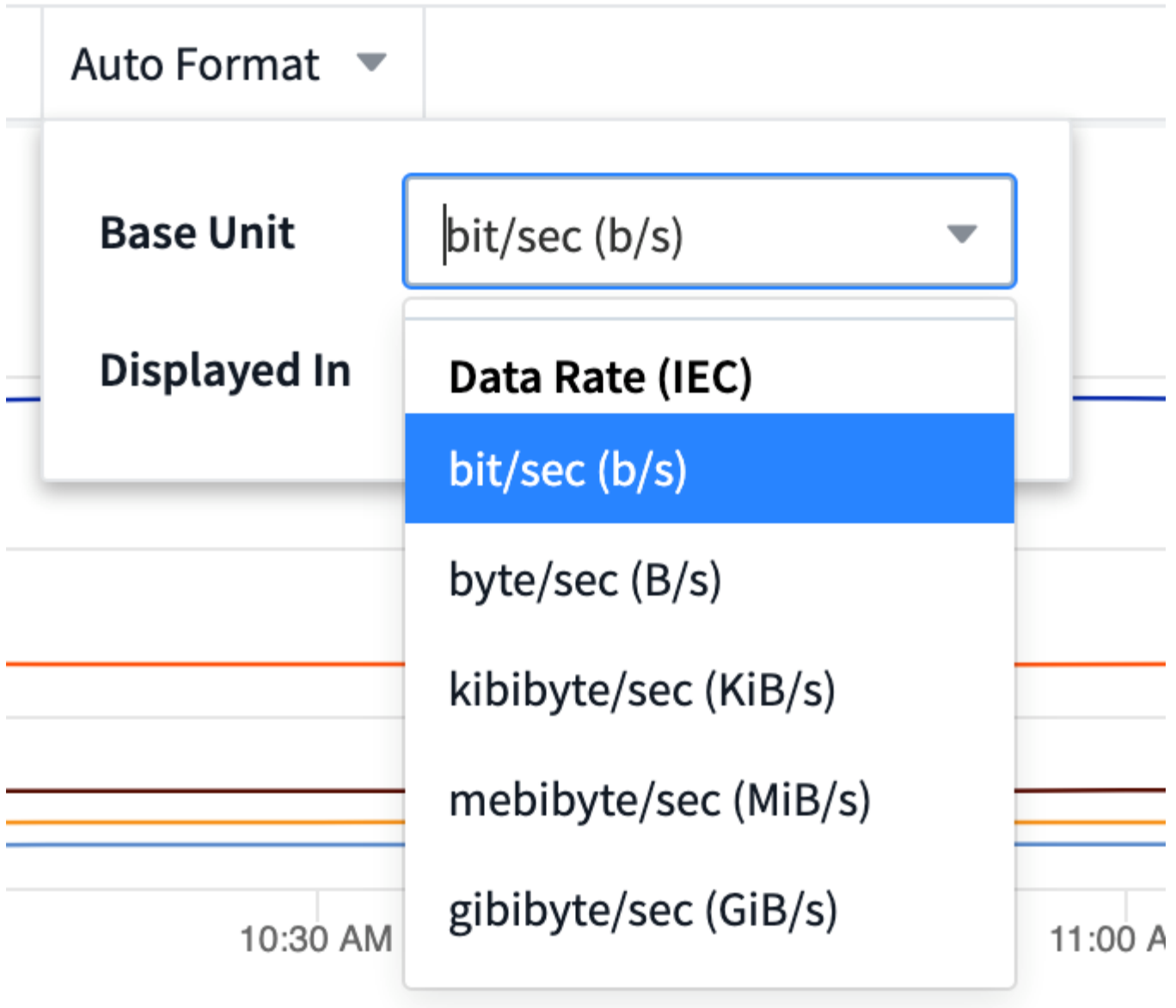


그래프를 다른 단위로 표시하려면 값을 표시할 다른 형식을 선택할 수 있습니다. 이 예제의 기본 단위는 `_byte_` 이므로 지원되는 "byte-based" 형식 중 하나를 선택할 수 있습니다: bit (b), byte (B), kibibyte (KiB), mebibyte (MiB), gibibyte (GiB). Y축 레이블과 값은 선택한 형식에 따라 변경됩니다.



베이스 유닛을 알 수 없는 경우 에서 단위를 지정할 수 있습니다 "사용 가능한 단위" 또는 직접 입력합니다. 기본 단위를 지정한 후 를 선택하여 적절한 지원 형식 중 하나로 데이터를 표시할 수 있습니다.





설정을 지우고 다시 시작하려면 \* 기본값 재설정 \* 을 클릭합니다.

자동 서식에 대한 단어

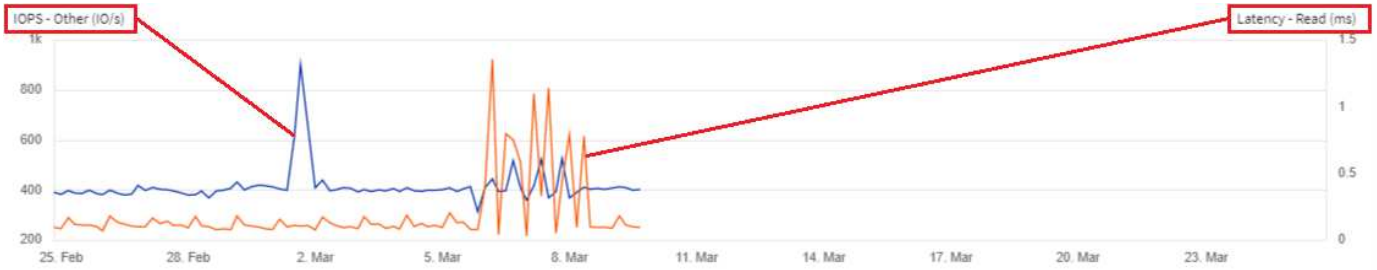
대부분의 메트릭은 1,234,567,890바이트와 같이 가장 작은 단위의 데이터 수집기에서 보고됩니다. 기본적으로 Data Infrastructure Insights는 가장 읽기 쉬운 표시를 위해 값의 형식을 자동으로 지정합니다. 예를 들어, 1,234,567,890바이트의 데이터 값은 1.23\_Gibytes\_로 자동 포맷됩니다. 이를 \_메비바이트\_와 같은 다른 형식으로 표시하도록 선택할 수 있습니다. 그에 따라 값이 표시됩니다.



Data Infrastructure Insights는 미국 영어 번호 명명 표준을 사용합니다. 미국 "십억"은 "천 백만"에 해당합니다.

여러 쿼리가 있는 위젯

두 개의 쿼리가 있는 시간 시리즈 위젯(예: 선, 스플라인, 영역, 스택 영역)이 둘 다 기본 Y축을 플롯하는 경우 기본 단위는 Y축 상단에 표시되지 않습니다. 하지만 위젯에 기본 Y축에 쿼리가 있고 보조 Y축에 쿼리가 있는 경우 각 항목의 기본 단위가 표시됩니다.



위젯에 쿼리가 3개 이상 있는 경우 Y축에 기본 단위가 표시되지 않습니다.

사용 가능한 단위

다음 표에는 범주별로 사용 가능한 모든 단위가 나와 있습니다.

* 범주 *	* 단위 *
통화	센센트 달러
데이터(IEC)	비트 바이트 kibibibibyte bibyte tebibibyte exbibyte
데이터 속도(IEC)	Bit/sec byte/sec kibibibibyte/sec mibibibibibyte/sec tibibibyte/sec pebibyte/sec
데이터(미터법)	킬로바이트 메가바이트 테라바이트(TB)
DataRate(Metric)	킬로바이트/초 메가바이트/초 기가바이트/초 페타바이트/초 페타바이트/초 엑사바이트/초
IEC	키비 미비 티비 피비 엑비
십진수	1억 2천만 조
백분율	백분율
시간	1분 2초 동안 나노초 초
온도	섭씨 화씨
주파수	헤르츠 킬로헤르츠 메가헤르츠 기가헤르츠
CPU	나노코레스 마이크로코어 밀리코레스 코어 킬로코레스 메가코레스 테라코레스 페타코레스 텍사코레스
처리량	I/O 작업/초 작업/초 요청/초 읽기/초 쓰기/초 작업/분 읽기 /분 쓰기/분

### TV 모드 및 자동 새로 고침

대시보드 및 자산 랜딩 페이지의 위젯에 있는 데이터는 선택한 대시보드 시간 범위에 따라 결정된 새로 고침 간격에 따라 자동으로 새로 고쳐집니다. 새로 고침 간격은 위젯이 시계열(선, 스플라인, 영역, 누적 영역형 차트) 또는 비시계열(다른 모든 차트)인지 여부를 기준으로 합니다.

대시보드 시간 범위	Time - 시리즈 새로 고침 간격입니다	Non-Time-Series Refresh Interval(비시간 시리즈 새로 고침 간격)
최근 15분	10초	1분

마지막 30분	15초	1분
마지막 60분	15초	1분
최근 2시간	30초	5분
최근 3시간	30초	5분
최근 6시간	1분	5분
최근 12시간	5분	10분
최근 24시간	5분	10분
최근 2일	10분	10분
지난 3일	15분	15분
최근 7일	1시간	1시간
지난 30일	2시간	2시간

각 위젯은 위젯의 오른쪽 상단 모서리에 자동 새로 고침 간격을 표시합니다.

사용자 지정 대시보드 시간 범위에는 자동 새로 고침을 사용할 수 없습니다.

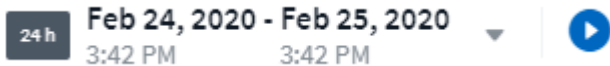
TV 모드 \* 와 함께 사용할 경우 자동 새로 고침을 통해 대시보드 또는 자산 페이지에 거의 실시간으로 데이터를 표시할 수 있습니다. TV 모드는 간결한 화면을 제공합니다. 탐색 메뉴는 숨겨져 있으며, 편집 단추처럼 데이터 디스플레이에 더 많은 화면 공간을 제공합니다. TV 모드는 일반적인 Data Infrastructure Insights 시간 제한을 무시하고 인증 보안 프로토콜에 의해 수동으로 또는 자동으로 로그아웃될 때까지 디스플레이를 활성 상태로 유지합니다.



NetApp BlueXP의 사용자 로그인 시간 제한은 7일이므로 Data Infrastructure Insights는 이 이벤트에서도 로그아웃해야 합니다. 다시 로그인하면 대시보드가 계속 표시됩니다.

- TV 모드를 활성화하려면 TV 모드 버튼을 클릭합니다.
- TV 모드를 비활성화하려면 화면 왼쪽 상단의 \* Exit \* (종료 \*) 버튼을 클릭합니다.

오른쪽 상단의 일시 중지 버튼을 클릭하여 자동 새로 고침을 일시적으로 중단할 수 있습니다. 일시 중지된 동안 대시보드 시간 범위 필드에 일시 중지된 데이터의 활성 시간 범위가 표시됩니다. 자동 새로 고침이 일시 중지되어 있는 동안 데이터가 계속 수집되고 업데이트됩니다. 데이터 자동 새로 고침을 계속하려면 재개 버튼을 클릭합니다.



### 대시보드 그룹

그룹화를 사용하면 관련 대시보드를 보고 관리할 수 있습니다. 예를 들어 사용자 환경의 스토리지 전용 대시보드 그룹을 가질 수 있습니다. 대시보드 그룹은 \* 대시보드 > 모든 대시보드 표시 \* 페이지에서 관리됩니다.

## Dashboard Groups (3)



Search groups..

All Dashboards (60)

My Dashboards (11)

Storage Group (7)

## Dashboards (7)



Name ↑

Dashboard - Storage Cost

Dashboard - Storage IO Detail

Dashboard - Storage Overview

Gauges Storage Performance

Storage Admin - Which nodes are in high demand?

Storage Admin - Which pools are in high demand?

Storage IOPs

기본적으로 두 그룹이 표시됩니다.

- \* 모든 대시보드 \* 는 소유자에 관계 없이 생성된 모든 대시보드를 나열합니다.
- \* 내 대시보드 \* 는 현재 사용자가 만든 대시보드만 나열합니다.

각 그룹에 포함된 대시보드 수가 그룹 이름 옆에 표시됩니다.

새 그룹을 생성하려면 \* "+" 새 대시보드 그룹 생성 \* 버튼을 클릭합니다. 그룹 이름을 입력하고 \* 그룹 생성 \* 을 클릭합니다. 해당 이름으로 빈 그룹이 생성됩니다.

그룹에 대시보드를 추가하려면 사용자 환경의 모든 대시보드를 표시하려면 \_All Dashboards\_ 그룹을 클릭하고, 보유한 대시보드만 표시하려면 \_My Dashboards\_ 를 클릭하고 다음 중 하나를 수행합니다.

- 단일 대시보드를 추가하려면 대시보드 오른쪽에 있는 메뉴를 클릭하고 \_Add to Group\_ 을 선택합니다.
- 그룹에 여러 개의 대시보드를 추가하려면 각 대시보드 옆에 있는 확인란을 클릭하여 선택한 다음 \* Bulk Actions \* 버튼을 클릭하고 \_Add to Group\_ 을 선택합니다.

\_Remove from Group\_ 을(를) 선택하여 동일한 방식으로 현재 그룹에서 대시보드를 제거합니다. 모든 대시보드 또는 \_내 대시보드\_ 그룹에서 대시보드를 제거할 수 없습니다.






그룹에서 대시보드를 제거해도 Data Infrastructure Insights에서 대시보드는 삭제되지 않습니다. 대시보드를 완전히 제거하려면 대시보드를 선택하고 \_Delete\_ 를 클릭합니다. 이렇게 하면 해당 그룹이 속해 있는 모든 그룹에서 해당 그룹이 제거되고 더 이상 모든 사용자가 사용할 수 없게 됩니다.

### 즐거찾기 대시보드를 고정합니다

대시보드 목록의 맨 위에 자주 사용하는 대시보드를 고정하여 더 세부적으로 관리할 수 있습니다. 대시보드를 고정하려면 목록에서 대시보드 위로 마우스를 가져가면 표시되는 압정 단추를 클릭하면 됩니다.

대시보드 핀/고정 해제는 개별 사용자 기본 설정이며 대시보드가 속한 그룹(또는 그룹)과 무관합니다.

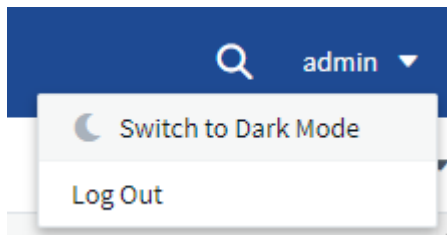
## Dashboards (7)

<input type="checkbox"/>	Name ↑
	<a href="#">Dashboard - Storage Overview</a>
	<a href="#">Storage Admin - Which nodes are in high demand?</a>
	<a href="#">Storage IOPs</a>
	<a href="#">Dashboard - Storage Cost</a>
	<a href="#">Dashboard - Storage IO Detail</a>
	<a href="#">Gauges Storage Performance</a>
	<a href="#">Storage Admin - Which pools are in high demand?</a>

### 어두운 테마

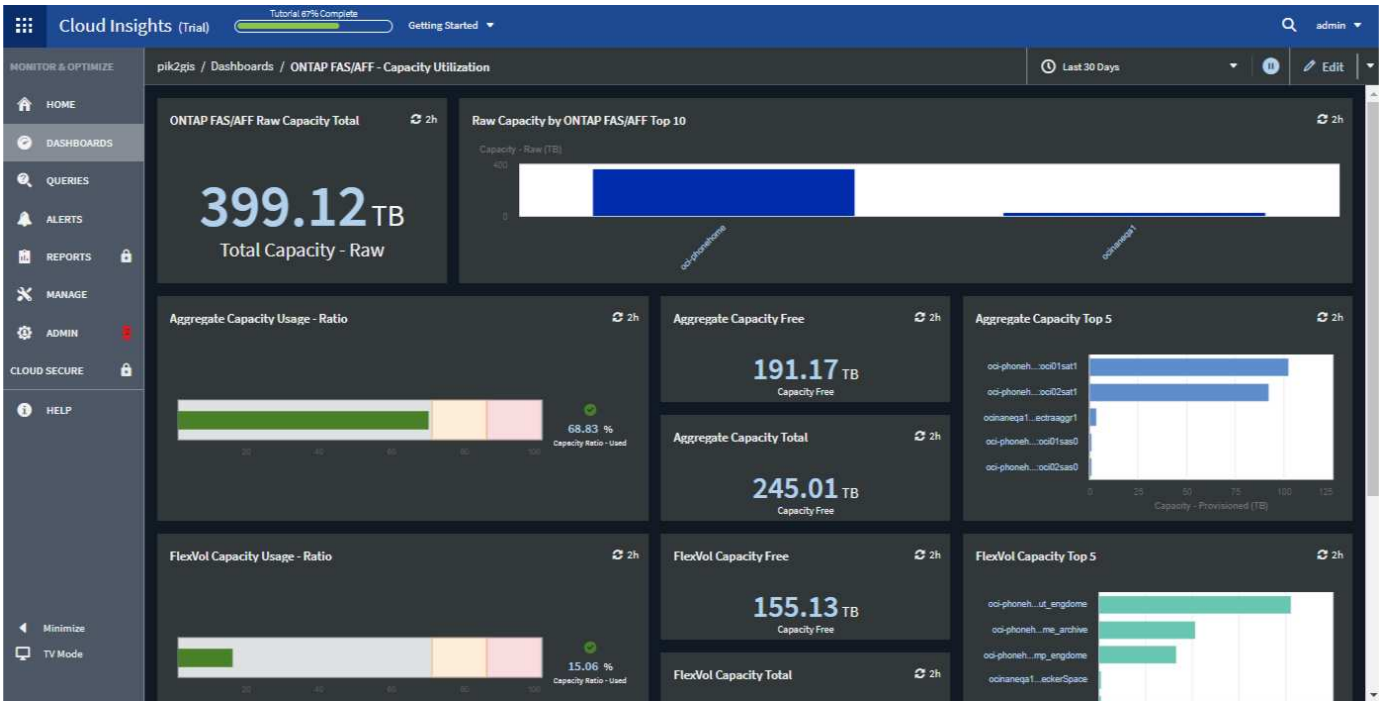
밝은 테마(기본값)를 사용하여 데이터 인프라 인사이트(Data Infrastructure Insights)를 표시하도록 선택할 수 있습니다. 이 테마는 어두운 텍스트가 있는 밝은 배경을 사용하여 대부분의 화면을 표시하며 어두운 테마는 밝은 텍스트가 있는 어두운 배경을 사용합니다.

밝은 테마와 어두운 테마 사이를 전환하려면 화면 오른쪽 위에 있는 사용자 이름 단추를 클릭하고 원하는 테마를 선택합니다.

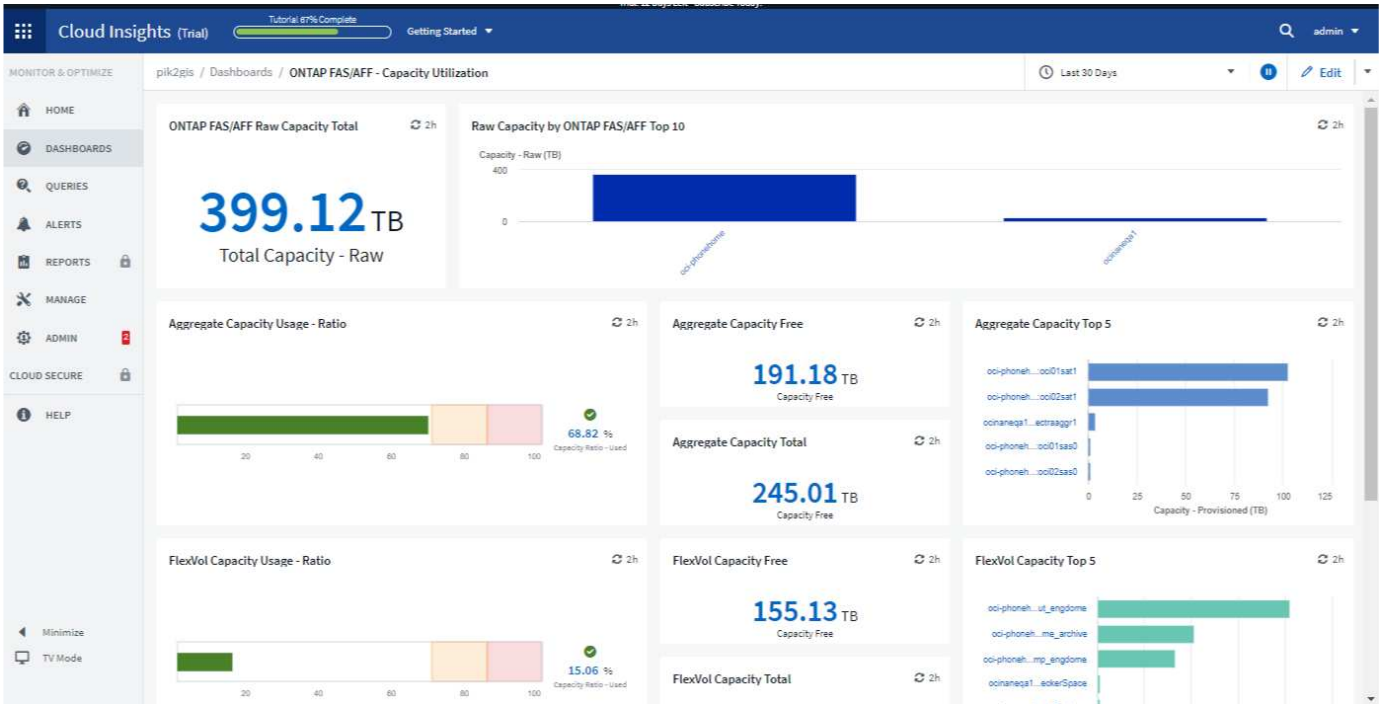


### 어두운 테마 대시보드 보기

:



### 밝은 테마 대시보드 보기



특정 위젯 차트와 같은 일부 화면 영역은 어두운 주제에서 보는 동안에도 밝은 배경을 표시합니다.

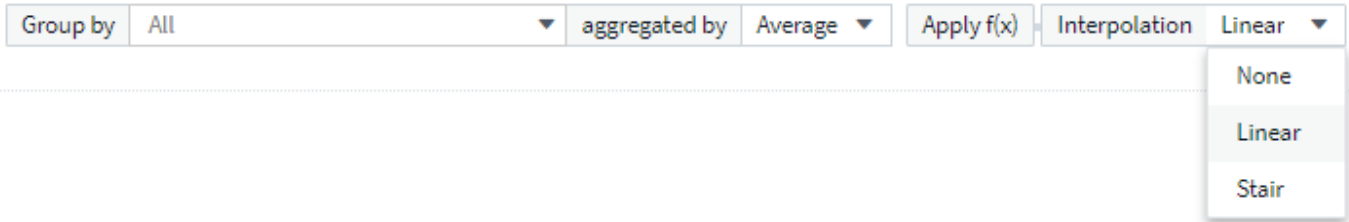
### 선형 차트 보간

여러 데이터 수집기는 서로 다른 간격으로 데이터를 폴링합니다. 예를 들어, 데이터 수집기 A는 15분마다 폴링하는 반면 데이터 수집기 B는 5분마다 폴링합니다. 선형 차트 위젯(스플라인, 영역 및 누적 영역형 차트)이 여러 데이터 수집기에서 단일 선으로 이 데이터를 집계하는 경우(예: 위젯이 "모두"로 그룹화되는 경우) 그리고 5분마다 라인을 새로 고치면 수집기 B의 데이터가 정확하게 표시될 수 있으며 컬렉터 A의 데이터에 차이가 있을 수 있으므로 컬렉터 A가 다시 폴링을 할 때까지 집계에 영향을 줄 수 있습니다.

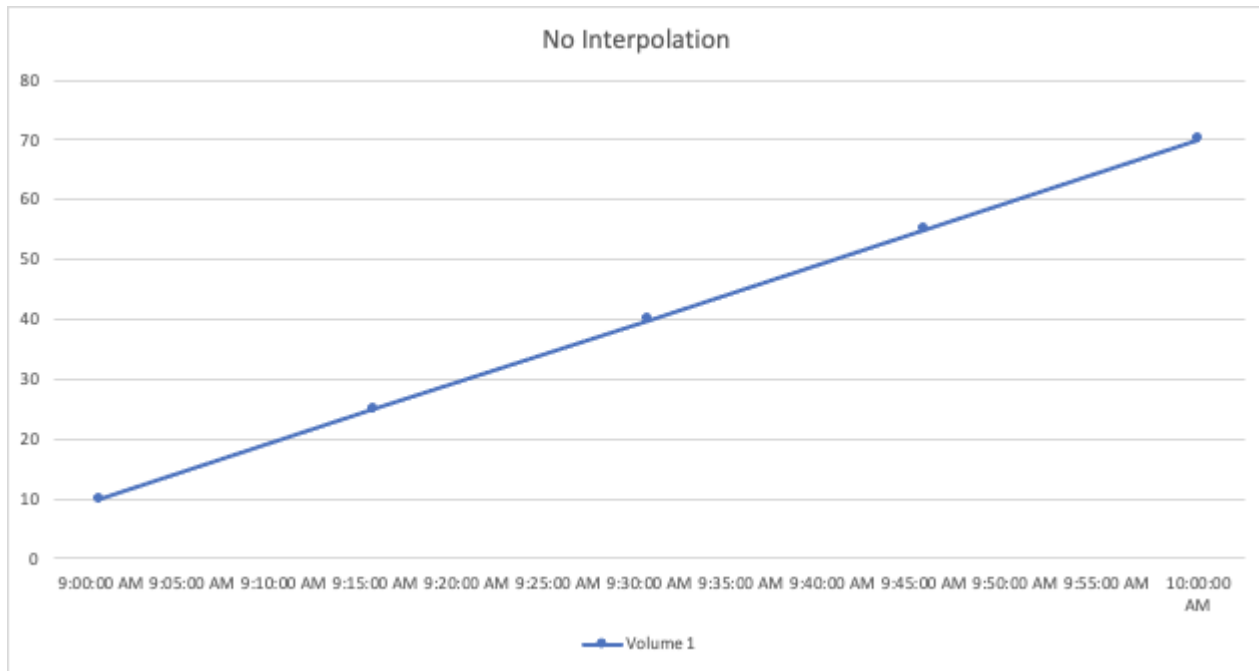
이러한 문제를 완화하기 위해 Data Infrastructure Insights는 데이터 수집기가 다시 폴링할 때까지 주변 데이터 포인트를 사용하여 데이터에 대해 "최상의 추측"을 수행합니다. 위젯의 그룹화를 조정하여 언제든지 각 데이터 수집기의 개체 데이터를 개별적으로 볼 수 있습니다.

#### 보간 방법

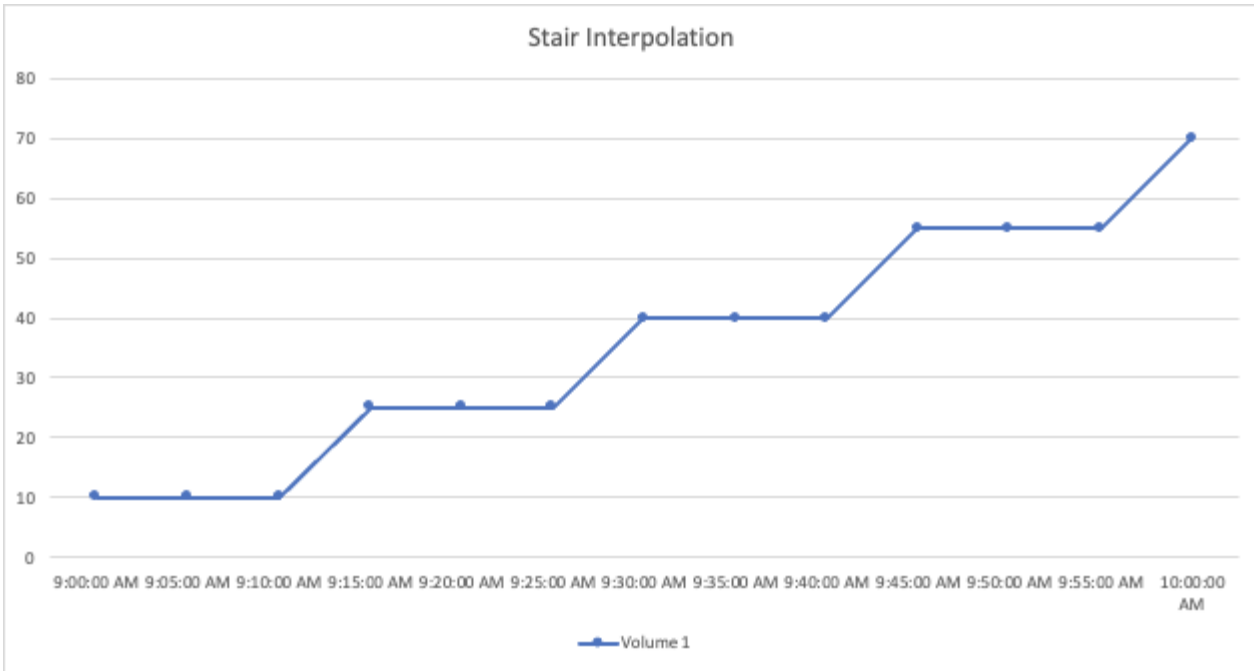
선형 차트(또는 스플라인, 영역 또는 누적 영역형 차트)를 만들거나 수정할 때 보간 방법을 세 가지 유형 중 하나로 설정할 수 있습니다. "그룹화 기준" 섹션에서 원하는 보간을 선택합니다.



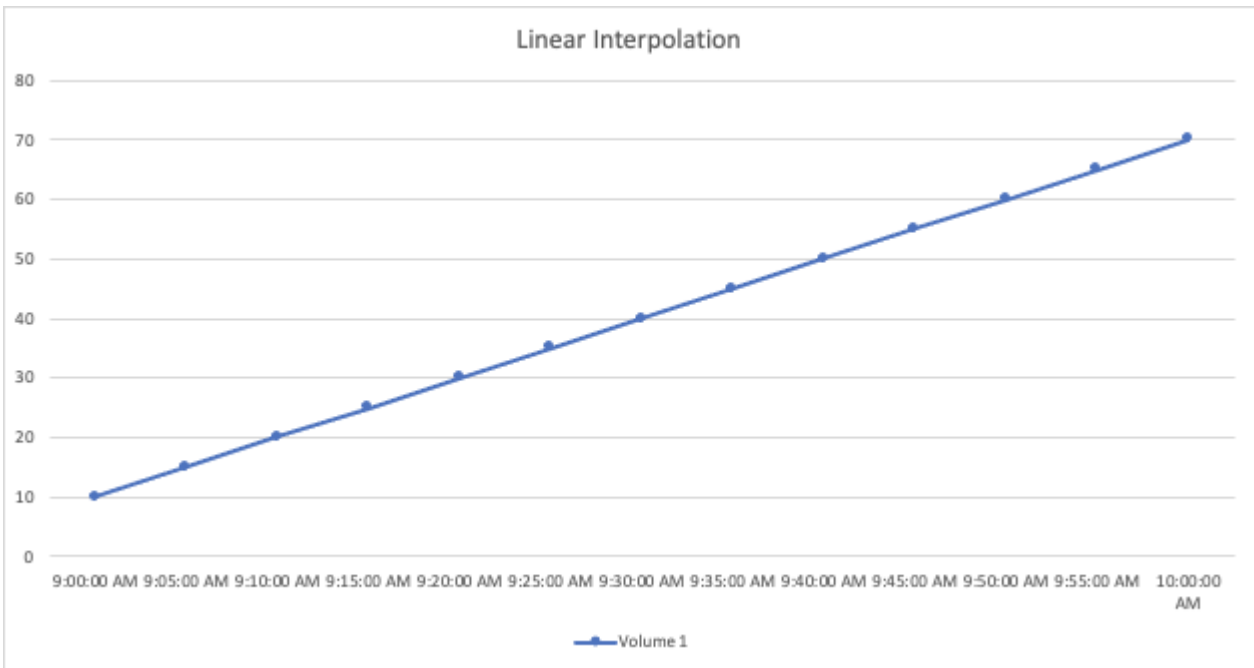
- \* 없음 \*: 아무 것도 하지 않습니다. 즉, 사이에 점을 생성하지 마십시오.



- \* 계단 \*: 이전 점 값에서 점이 생성됩니다. 직진 시 일반적인 "계단" 레이아웃으로 표시됩니다.



- \* 선형 \*: 두 점 사이의 값으로 점이 생성됩니다. 두 점을 연결하는 선과 같지만 추가(보간) 데이터 점이 있는 선을 생성합니다.



## 대시보드 예제

대시보드 예: 가상 머신 성능

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(VM) 성능에 대한 운영 통찰력을 제공하는 위젯이 포함된 대시보드를 만드는 방법을 보여 줍니다. 이 예제를 따르고 특정 요구 사항을 충족하기 위한 위젯을 생성하면 프론트엔드 가상



머신 성능과 비교하여 백엔드 스토리지 성능을 시각화하거나 VM 지연 시간과 I/O 요구 사항을 확인하는 등의 작업을 수행할 수 있습니다.

이 작업에 대해

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 대시보드를 사용자 지정하여 선택한 성능 데이터를 강조하고 비교할 수 있습니다.

단계

1. 관리 권한이 있는 사용자로 Insight에 로그인합니다.
2. 대시보드 \* 메뉴에서 \* [+새 대시보드] \* 를 선택합니다.  
 새 대시보드 \* 페이지가 열립니다.
3. 페이지 맨 위에 대시보드의 고유 이름(예: "애플리케이션별 VM 성능")을 입력합니다.
4. 대시보드를 새 이름으로 저장하려면 \* 저장 \* 을 클릭합니다.
5. 이제 위젯을 추가해 보겠습니다. 필요한 경우 \* 편집 \* 아이콘을 클릭하여 편집 모드를 활성화합니다.
6. 위젯 추가 \* 아이콘을 클릭하고 \* 표 \* 를 선택하여 대시보드에 새 테이블 위젯을 추가합니다.

위젯 편집 대화 상자가 열립니다. 표시된 기본 데이터는 사용자 환경의 모든 스토리지에 대한 것입니다.

**Table Widget** 🔄 10m

1,746 items found in 71 groups

Hypervisor Name ↑	Virtual Machine	Capacity - Total (GB)	IOPS - Total (IO/s)	Latency - Total (ms)
10.197.143.53 (9)	--	1,690.58	1.80	12.04
10.197.143.54 (7)	--	1,707.60	4.62	12.69
10.197.143.57 (11)	--	1,509.94	1.14	1.15
10.197.143.58 (10)	--	1,818.34	5.83	2.57
AzureComputeDefaultAvailabilitySet (363)	--	N/A	N/A	N/A
anandh9162020113920-rg-avset.anandh91620201	--	N/A	N/A	N/A
anandh916202013287-rg-avset.anandh91620201	--	N/A	N/A	N/A
anandh91720201288-rg-avset.anandh91720201	--	N/A	N/A	N/A
anjalivIngrun48-rg-avset.anjalivIngrun48-rg.398	--	N/A	N/A	N/A
anjalivIngrun50-rg-avset.anjalivIngrun50-rg.398	--	N/A	N/A	N/A
batutiscanaryHA97a-rg-avset.batutiscanaryha97	--	N/A	N/A	N/A
batutiscanarvHA97b-rg-avset.batutiscanarvha97	--	N/A	N/A	N/A

1. 이 위젯을 사용자 지정할 수 있습니다. 상단의 Name 필드에서 "Widget 1"을 삭제하고 "Virtual Machine Performance table"을 입력합니다.

2. 자산 유형 드롭다운을 클릭하고 `_Storage_to_Virtual Machine_` 을 변경합니다.

테이블 데이터가 변경되어 사용자 환경의 모든 가상 시스템이 표시됩니다.

3. 표에 몇 개의 열을 추가해 보겠습니다. 오른쪽의 Gear 아이콘을 클릭하고 하이퍼바이저 이름, `IOPS - Total` 및 `_Latency - Total_` 을 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.

4. 이 실습에서는 사용 중이 아닌 VM을 제외하므로 총 IOPS가 10개 미만인 VM을 필터링하겠습니다. Filter by \* 옆에 있는 \* [+ ] \* 버튼을 클릭하고 `_IOPS - Total_` 을 선택합니다. 임의의 \* 를 클릭하고 \* 보낸 사람 \* 필드에 "10"을 입력합니다. 받는 사람 \* 필드는 비워 둡니다. 필터 필드를 출력하거나 Enter 키를 눌러 필터를 설정합니다.

이제 표에는 총 IOPS가 10개 이상인 VM만 표시됩니다.

5. 결과를 그룹화하여 테이블을 더 축소할 수 있습니다. Group By \* (그룹화 기준) 옆의 \* [+ ] \* 버튼을 클릭하고 그룹화할 필드(예: `Application_or_Hypervisor name`)를 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.

Hypervisor name ↓	Name	Hypervisor name	IOPS - Total (IO/s)	Latency - Total (ms)
+ us-east-1d (62)		us-east-1d		1.94
+ us-east-1c (80)		us-east-1c		0.80
+ us-east-1b (1)	TBDemoEnv	us-east-1b	32.66	0.70
+ us-east-1a (38)		us-east-1a	121.22	0.81

1. 표 위젯을 원하는 대로 사용자 정의했으면 \* [Save] \* (저장) \* 버튼을 클릭합니다.

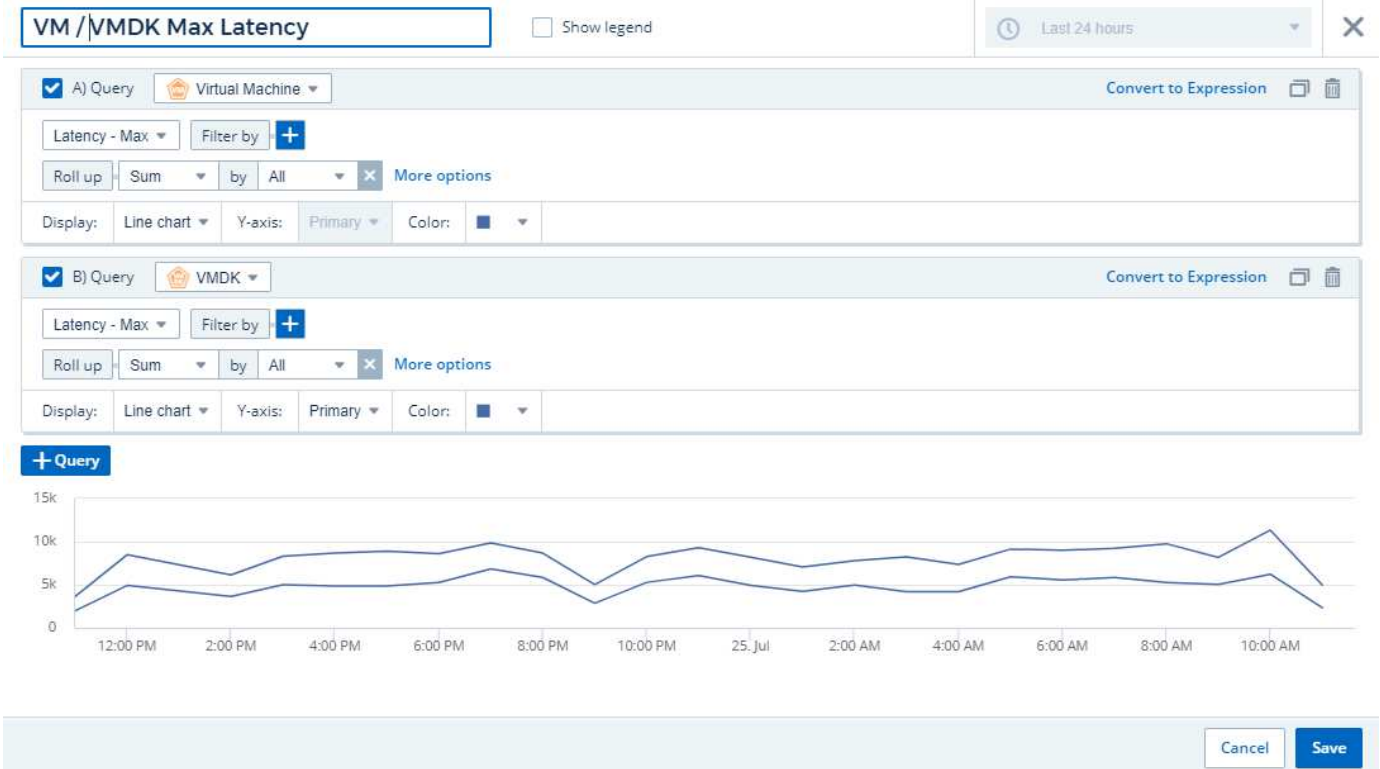
테이블 위젯이 대시보드에 저장됩니다.

오른쪽 아래 모서리를 끌어 대시보드에서 위젯의 크기를 조정할 수 있습니다. 위젯을 더 넓게 만들어 모든 열을 명확하게 표시합니다. Save \* 를 클릭하여 현재 대시보드를 저장합니다.

다음으로 몇 가지 차트를 추가하여 VM 성능을 보여 드리겠습니다. VM 지연 시간을 VMDK 지연 시간과 비교하여 선형 차트를 만들어 보겠습니다.

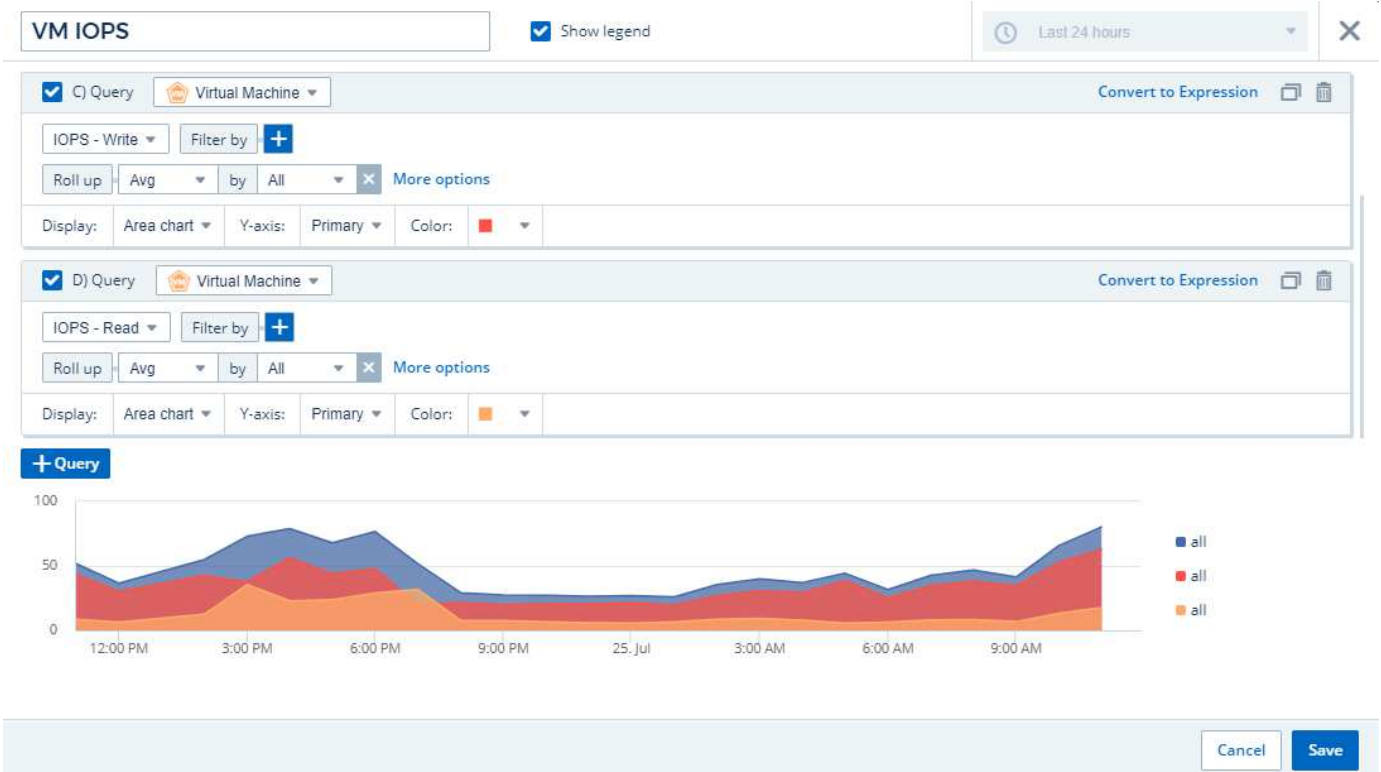
1. 필요한 경우 대시보드에서 \* 편집 \* 아이콘을 클릭하여 편집 모드를 활성화합니다.

2. [Add widget] \* 아이콘을 클릭하고 `_Line Chart_`를 선택하여 대시보드에 새 선형 차트 위젯을 추가합니다.
3. 위젯 편집 \* 대화 상자가 열립니다. 이 위젯의 이름을 "VM/VMDK 최대 지연 시간"으로 지정합니다.
4. Virtual Machine \* 을 선택하고 `_Latency-Max_`를 선택합니다. 원하는 필터를 설정하거나 \* Filter by \* 를 비워 둡니다. 롤업 \* 의 경우 `_Sum_by_all_`을 선택합니다. 이 데이터를 `_Line Chart_`로 표시하고 `_Y-Axis_AS_Primary_`로 둡니다.
5. [+Query] \* 버튼을 클릭하여 두 번째 데이터 라인을 추가합니다. 이 행에 대해 `_VMDK_와_대기_시간 - 최대_`를 선택합니다. 원하는 필터를 설정하거나 \* Filter by \* 를 비워 둡니다. 롤업 \* 의 경우 `_Sum_by_all_`을 선택합니다. 이 데이터를 `_Line Chart_`로 표시하고 `_Y-Axis_AS_Primary_`로 둡니다.
6. 이 위젯을 대시보드에 추가하려면 \* [Save] \* 를 클릭합니다.



다음으로 단일 차트에서 VM 읽기, 쓰기 및 총 IOPS를 보여 주는 차트를 추가합니다.

1. [Add widget] \* 아이콘을 클릭하고 `_Area Chart_`를 선택하여 대시보드에 새 영역 차트 위젯을 추가합니다.
2. 위젯 편집 대화 상자가 열립니다. 이 위젯 이름 "VM IOPS"
3. Virtual Machine \* 을 선택하고 `_IOPS - Total_`을 선택합니다. 원하는 필터를 설정하거나 \* Filter by \* 를 비워 둡니다. 롤업 \* 의 경우 `_Sum_by_all_`을 선택합니다. 이 데이터를 `_Area Chart_`로 표시하고 `_Y-Axis_AS_Primary_`로 둡니다.
4. [+Query] \* 버튼을 클릭하여 두 번째 데이터 라인을 추가합니다. 이 행에 대해 \* Virtual Machine \* 을 선택하고 `_IOPS - 읽기_`를 선택합니다.
5. 세 번째 데이터 행을 추가하려면 \* [+Query] \* 버튼을 클릭합니다. 이 행에 대해 \* Virtual Machine \* 을 선택하고 `_IOPS-Write_`를 선택합니다.
6. 이 위젯에 대한 범례를 대시보드에 표시하려면 \* 범례 표시 \* 를 클릭합니다.



1. 이 위젯을 대시보드에 추가하려면 \* [Save] \* 를 클릭합니다.

다음으로 VM과 연결된 각 애플리케이션의 VM 처리량을 보여 주는 차트를 추가합니다. 이에 대해 롤업 기능을 사용할 것입니다.

1. [Add widget] \* 아이콘을 클릭하고 \_Line Chart\_를 선택하여 대시보드에 새 선형 차트 위젯을 추가합니다.
2. 위젯 편집 대화 상자가 열립니다. 이 위젯의 이름을 "애플리케이션별 VM 처리량"으로 지정합니다.
3. Virtual Machine을 선택하고 Throughput - Total을 선택합니다. 원하는 필터를 설정하거나 필터를 비워 둡니다. 롤업에서 "최대"를 선택하고 "응용 프로그램" 또는 "이름"을 선택합니다. 상위 10개 애플리케이션을 표시합니다. 이 데이터를 선형 차트로 표시하고 Y축을 1차 로 둡니다.
4. 이 위젯을 대시보드에 추가하려면 \* [Save] \* 를 클릭합니다.

위젯 상단의 아무 곳이나 마우스 버튼을 누른 채 새 위치로 드래그하여 대시보드에서 위젯을 이동할 수 있습니다.

오른쪽 아래 모서리를 끌어 위젯 크기를 조정할 수 있습니다.

변경한 후에는 대시보드를 \* [Save] \* (저장)합니다.

최종 VM 성능 대시보드는 다음과 같습니다.



## 대시보드 및 위젯에 대한 모범 사례

대시보드와 위젯의 강력한 기능을 최대한 활용할 수 있도록 도와주는 팁과 요령.

### 적합한 메트릭 찾기

Data Infrastructure Insights는 데이터 수집기에서 데이터 수집기마다 다른 이름을 사용하여 카운터와 메트릭을 획득합니다.

대시보드 위젯에 대한 적절한 메트릭이나 카운터를 검색할 때 원하는 메트릭이 생각하려는 메트릭과 다른 이름으로 표시될 수 있다는 점에 유의하십시오. Data Infrastructure Insights의 드롭다운 목록은 일반적으로 알파벳이지만, 경우에 따라 목록에 해당 용어가 표시되지 않을 수 있습니다. 예를 들어 "물리적 용량" 및 "사용된 용량"과 같은 용어는 대부분의 목록에 함께 나타나지 않습니다.

- 모범 사례 \*: 필터 기준 또는 열 선택기와 같은 위치의 필드에 있는 검색 기능을 사용하여 원하는 항목을 찾습니다. 예를 들어, "CAP"를 검색하면 목록에서 어떤 상황이 발생하든 이름에 "capacity"가 포함된 모든 메트릭이 표시됩니다. 그런 다음 해당 짧은 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 용량 프로비저닝된 용량 스토리지 풀 용량 <Other asset type> 기록된 용량
디스크 속도	최저 디스크 속도 최소 성능 디스크 유형입니다
호스트	하이퍼바이저 호스트
하이퍼바이저	호스트가 하이퍼바이저입니다
마이크로코드	펌웨어

이름	별칭 하이퍼바이저 이름 스토리지 이름 <기타 자산 유형> 이름 단순 이름 리소스 이름 Fabric 별칭
읽기/쓰기	Partial R/W Pending Writes IOPS - Write Written Capacity Latency - Read Cache Utilization - Read 를 참조하십시오
가상 머신	VM은 가상입니다

이것은 포괄적인 목록이 아닙니다. 다음은 가능한 검색어의 예일 뿐입니다.

#### 적합한 자산 찾기

위젯 필터 및 검색에서 참조할 수 있는 자산은 자산 유형에 따라 다릅니다.

대시보드 및 자산 페이지에서 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 볼륨 VMDK 가상 머신 볼륨
하이퍼바이저	가상 시스템은 하이퍼바이저 호스트입니다
호스트	내부 볼륨 클러스터 호스트 가상 머신
패브릭	포트

이것은 포괄적인 목록이 아닙니다.

모범 사례: 목록에 나타나지 않는 특정 자산 유형을 필터링하는 경우 대체 자산 유형에 대한 쿼리를 작성합니다.

#### 분산 플롯 예: 축 알기

산포도 위젯에서 카운터의 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.

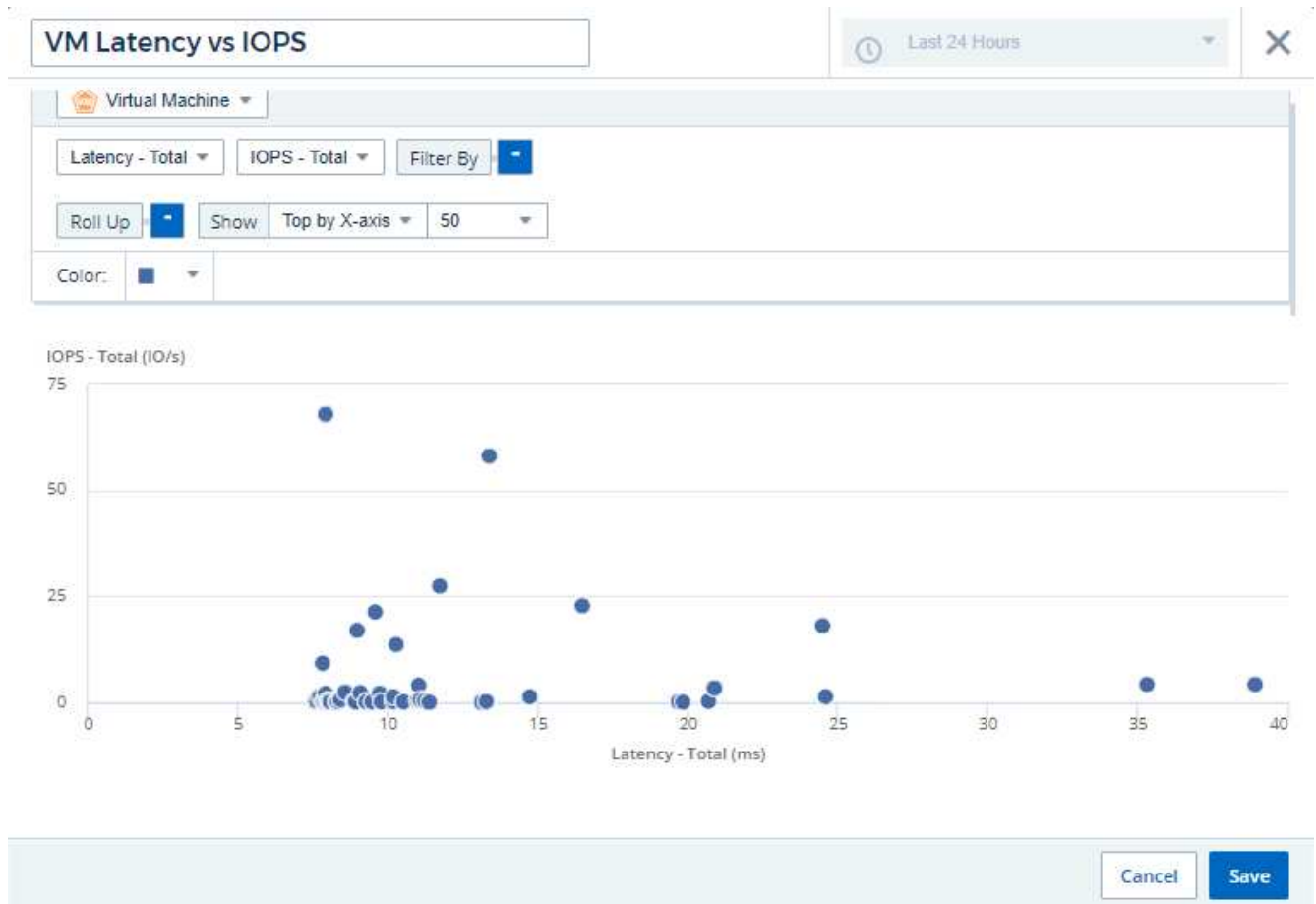
#### 단계

1. 편집 모드에서 대시보드를 만들거나 열고 \* Scatter Plot Chart \* 위젯을 추가합니다.
2. 예를 들어, \_Virtual Machine\_ 과 같은 자산 유형을 선택합니다.
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.



- 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.



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 총 IOPS가 가장 높은 상위 100개 VM을 표시합니다. Y축 \* 기준으로 \* Top으로 변경하면 총 지연 시간이 가장 긴 상위 100개 VM이 다시 한 번 표시됩니다.

산포도 차트에서 지점을 클릭하여 해당 자원의 자산 페이지로 드릴다운할 수 있습니다.

## 쿼리 작업

### 쿼리에 사용된 자산

쿼리를 사용하면 사용자 선택 기준(예: 주식)에 따라 사용자 환경에서 자산과 메트릭을 세분화된 수준으로 검색하여 네트워크를 모니터링하고 문제를 해결할 수 있습니다.

자산에 주석을 자동으로 할당하는 주식 규칙은 `_Require_a` 쿼리입니다.

사용자 환경에서 물리적 또는 가상 인벤토리 자산(및 관련 메트릭)이나 Kubernetes 또는 ONTAP 고급 데이터와 같이 통합 시 제공되는 메트릭을 쿼리할 수 있습니다.

### 인벤토리 자산

쿼리, 대시보드 위젯 및 맞춤형 자산 랜딩 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.

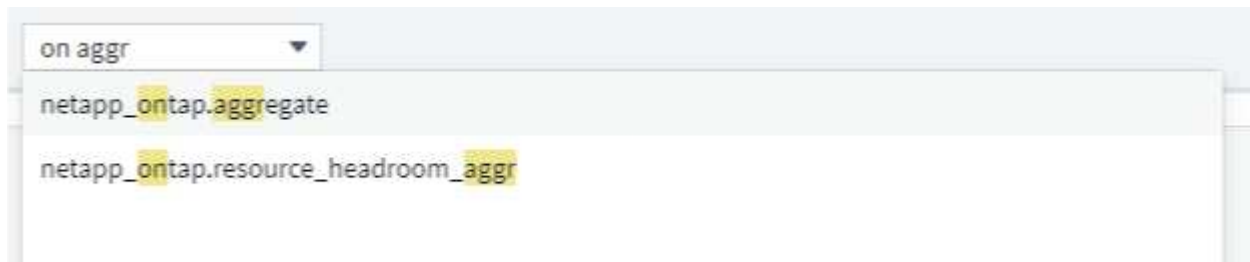
- 응용 프로그램



- 데이터 저장소
- 디스크
- 패브릭
- 일반 장치
- 호스트
- 내부 볼륨
- iSCSI 세션
- iSCSI 네트워크 포털
- 경로
- 포트
- qtree입니다
- 할당량
- 공유
- 스토리지
- 스토리지 노드
- 스토리지 풀
- 스토리지 가상 시스템(SVM)
- 스위치
- 테이프
- VMDK입니다
- 가상 머신
- 볼륨
- Zone(영역)
- 존 구성원

#### 통합 메트릭

인벤토리 자산과 관련 성능 메트릭을 쿼리하는 것 외에도 Kubernetes 또는 Docker에서 생성되거나 ONTAP 고급 메트릭과 함께 제공되는 \* 통합 데이터 \* 메트릭도 쿼리할 수 있습니다.



## 쿼리 만들기

쿼리를 사용하면 환경 내의 자산을 세부 수준에서 검색할 수 있으므로 원하는 데이터를 필터링하고 원하는 대로 결과를 정렬할 수 있습니다.

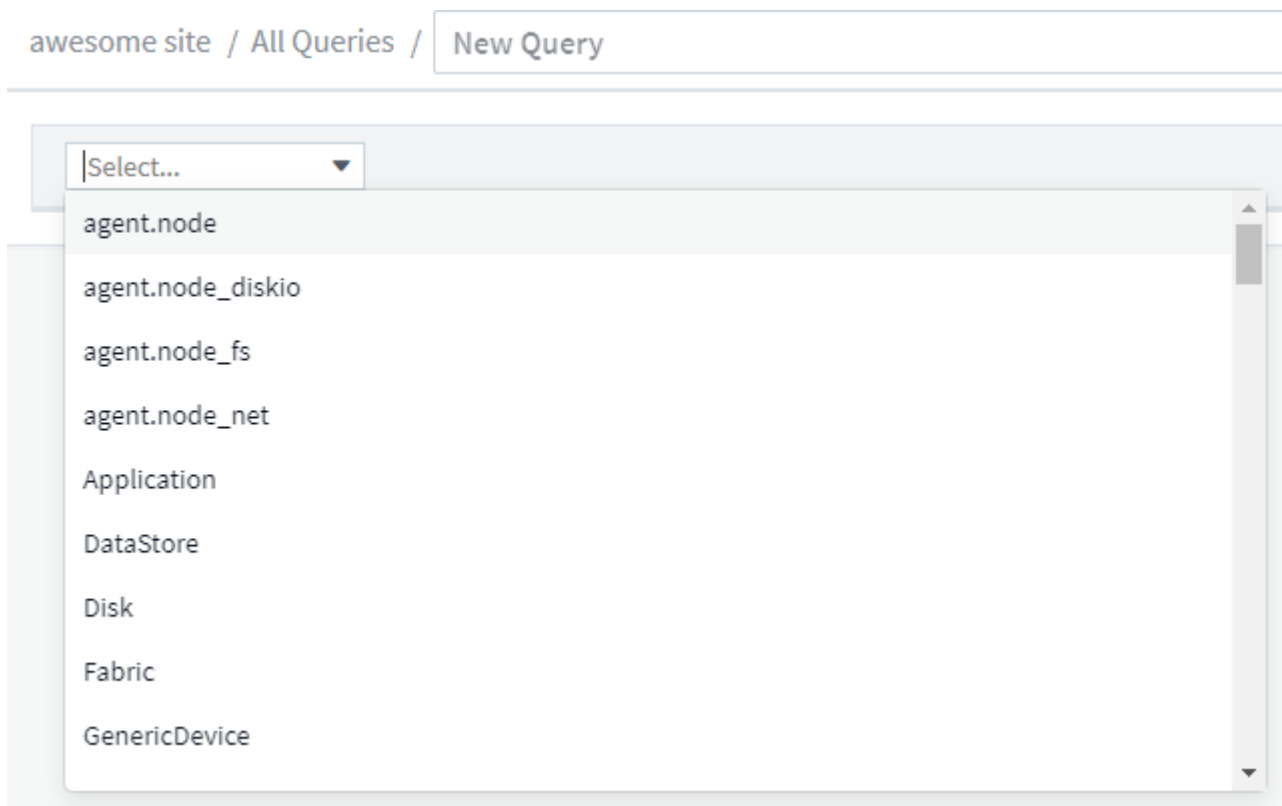
예를 들어, `_volumes_`에 대한 쿼리를 생성하고, 선택한 볼륨과 관련된 특정 `_storages_`를 찾기 위한 필터를 추가하고, 다른 필터를 추가하여 선택한 저장소의 "Tier 1"과 같은 특정 `_annotation_`을 찾을 수 있습니다. 마지막으로, 다른 필터를 추가하여 25보다 큰 `_IOPS-읽기(입출력/초)_`를 가진 모든 스토리지를 찾습니다. 결과가 표시되면 쿼리와 관련된 정보 열을 오름차순 또는 내림차순으로 정렬할 수 있습니다.

참고: 자산을 취득하는 새 데이터 수집기가 추가되거나 주석 또는 응용 프로그램 할당이 이루어진 경우 쿼리를 인덱싱한 후에만 이러한 새 자산, 주석 또는 응용 프로그램을 쿼리할 수 있습니다. 인덱싱은 정기적으로 예약된 간격이나 주석 규칙 실행과 같은 특정 이벤트 중에 발생합니다.

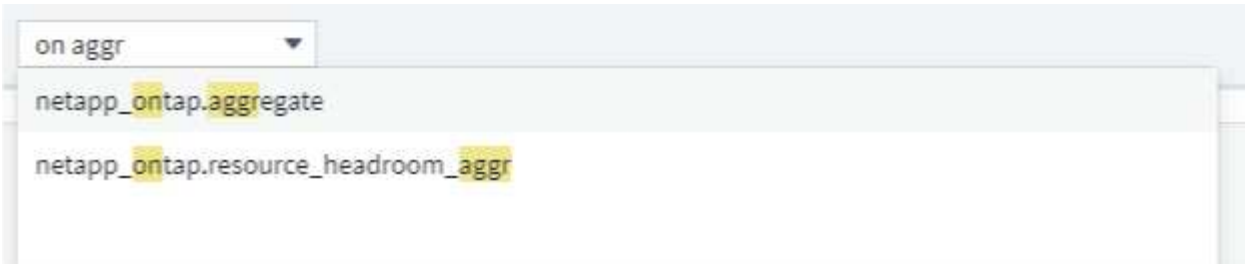
쿼리 만들기는 매우 간단합니다.

1. 쿼리 > \* + 새 쿼리 \* 로 이동합니다.
2. '선택...' 목록에서 쿼리할 개체 유형을 선택합니다. 목록을 스크롤하거나 입력을 시작하여 검색 중인 항목을 보다 빠르게 찾을 수 있습니다.

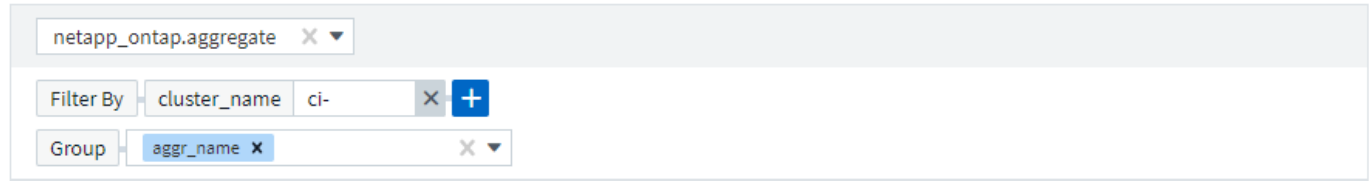
스크롤 목록:



검색 입력:



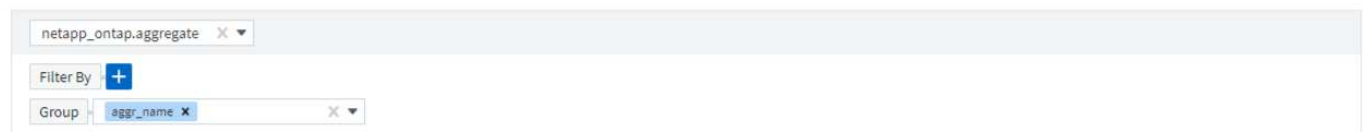
필터 기준 \* 필드에서 \* + \* 버튼을 클릭하여 필터를 추가하여 쿼리 범위를 좁힐 수 있습니다. 오브젝트 또는 속성별로 행을 그룹화합니다. 통합 데이터(Kubernetes, ONTAP 고급 메트릭 등)를 사용할 경우 원하는 경우 여러 가지 특성을 기준으로 그룹화할 수 있습니다.



5 items found

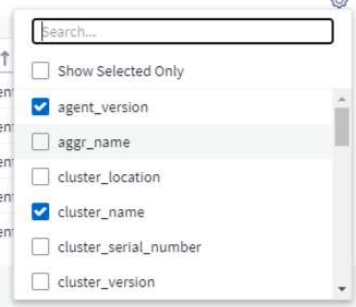
Table Row Grouping	Metrics & Attributes	
aggr_name	cp_read_blocks	cluster_name ↓
oci02sat0	0.59	oci-phonehome
oci02sat1	0.15	oci-phonehome
oci02sat2	212.64	oci-phonehome
oci01sat0	0.39	oci-phonehome
oci01sat1	48.89	oci-phonehome

쿼리 결과 목록에는 검색된 개체 유형에 따라 여러 개의 기본 열이 표시됩니다. 열을 추가, 제거 또는 변경하려면 표 오른쪽에 있는 기어 아이콘을 클릭합니다. 사용 가능한 열은 자산/메트릭 유형에 따라 달라집니다.



14 items found

Table Row Grouping	Metrics & Attributes	
aggr_name	cp_read_blocks	agent_version ↑
aggr0_optimus_02	1.72	Apache-HttpClie
aggr1_optimus_02	408.84	Apache-HttpClie
ocinaneqa1_04_aggr0	6.19	Apache-HttpClie
ocinaneqa1_03_aggr0	6.48	Apache-HttpClie
oci02sat0	1.04	Apache-HttpClie



집계, 단위, 조건부 서식 선택

## 집계 및 단위

"값" 열의 경우 표시된 값이 집계되는 방식을 선택하고 해당 값이 표시되는 단위를 선택하여 쿼리 결과를 더욱 구체화할 수 있습니다. 이러한 옵션은 열 상단 모서리에 있는 "점 3개" 메뉴를 선택하면 찾을 수 있습니다.

143 items found

Table Row Grouping	Metrics & Attributes
agent.node_diskio ↑	io_time (ms)
nvme0n1	20,604,960.00
nvme0n1	29,184,970.00
nvme0n1	4,642,684.00
nvme0n1	31,918,988.00
nvme0n1	29,258,256.00
nvme0n1	18,022,164.00
nvme0n1	28,483,300.00
nvme0n1	69,835,016.00
nvme0n1	15,952,780.00
nvme0n1	44,169,696.00
nvme0n1	12,138,928.00
nvme0n1	5,234,528.00
nvme0n1	34,260,552.00

▼ Aggregation

Group By: Avg

Time Aggregate By: Last

▼ Unit Display

Base Unit: millisecond (ms)

Displayed In: millisecond (ms)

▼ Conditional Formatting Reset

If value is: > (Greater than)

Warning: Optional ms

Critical: Optional ms

> Rename Column

## 단위

값을 표시할 단위를 선택할 수 있습니다. 예를 들어, 선택한 열에 원시 용량이 표시되고 값이 GiB로 표시되지만 원하는 경우 Unit Display(단위 표시) 드롭다운에서 TiB를 선택하면 됩니다.

## 집계

표시된 값이 기본 데이터에서 "평균"으로 집계된 경우 동일한 토큰으로 그러나 모든 값의 합계를 표시하려면 *Group By* 드롭다운(그룹화된 값에 합계를 표시하려면) 또는 *Time Aggregate by* 드롭다운(행 값에 원본으로 사용하는 데이터의 합계를 표시하려면)에서 "Sum"을 선택합니다.

그룹화된 데이터 요소를 *\_Avg*, *Max*, *Min* 또는 *Sum* 별로 집계하도록 선택할 수 있습니다.

개별 행 데이터는 *\_Average*, 획득된 마지막 데이터 지점, 최대값, 최소값 또는 합계\_를 기준으로 집계할 수 있습니다.

## 조건부 서식

조건부 서식을 사용하면 쿼리 결과 목록에서 경고 수준 및 위험 수준 임계값을 강조 표시하여 이상값 및 예외적인 데이터 지점에 대한 즉각적인 가시성을 얻을 수 있습니다.

143 items found

Table Row Grouping	Metrics & Attributes
agent.node_diskio ↑	io_time (sec)
nvme0n1	20,604.96
nvme0n1	29,184.97
nvme0n1	4,642.68
nvme0n1	31,918.99
nvme0n1	29,258.26
nvme0n1	18,022.16
nvme0n1	28,483.30
nvme0n1	69,835.02
nvme0n1	15,952.78

> Aggregation

> Unit Display

Conditional Formatting Reset

If value is: > (Greater than)

Warning: 10000 sec

Critical: 20000 sec

> Rename Column

조건부 서식은 각 열에 대해 별도로 설정됩니다. 예를 들어 용량 열에 대한 임계값 집합 하나와 처리량 열에 대한 임계값 집합을 선택할 수 있습니다.

### 열 이름 바꾸기

열 이름을 바꾸면 쿼리 결과 목록에 표시된 이름이 변경됩니다. 쿼리 목록을 .csv로 내보내는 경우 결과 파일에도 새 열 이름이 표시됩니다.

### 저장

원하는 결과를 표시하도록 쿼리를 구성한 후 \* 저장 \* 버튼을 클릭하여 나중에 사용할 수 있도록 쿼리를 저장할 수 있습니다. 의미 있고 고유한 이름을 지정합니다.

### 필터링에 대한 추가 정보

#### 와일드카드와 식

쿼리 또는 대시보드 위젯에서 텍스트 또는 목록 값을 필터링할 때 입력을 시작하면 현재 텍스트를 기반으로 \* 와일드카드 필터 \* 를 만드는 옵션이 표시됩니다. 이 옵션을 선택하면 와일드카드 식과 일치하는 모든 결과가 반환됩니다. NOT 또는 OR을 사용하여 \* 식 \* 을 만들거나 "없음" 옵션을 선택하여 필드의 null 값을 필터링할 수도 있습니다.

kubernetes.pod X ▼

Filter By pod\_name ingest X + ?

Group pod\_name X

- Create wildcard containing "ingest"
- ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
- service-foundation-ingest-767dfd5bfc-vxd5p
- None

71 items found

Table Row Grouping

와일드카드 또는 식(예 NOT, 또는, "없음" 등)이 필터 필드에 진한 파란색으로 표시됩니다. 목록에서 직접 선택한 항목은 연한 파란색으로 표시됩니다.

The screenshot shows a search interface with a dropdown menu set to 'kubernetes.pod'. Below it, a 'Filter By' section shows 'pod\_name' with two active filters: '\*ingest\*' (highlighted in blue) and 'ci-service-audit-5f775dd975-brfdc'. There are also buttons for adding (+) and removing (x) filters, and a help icon (?). A 'Group' section below shows 'pod\_name' as the selected group.

3 items found

pod_name
ci-service-audit-5f775dd975-brfdc
ci-service-datalake-ingestion-85b5bdfd6d-2qbwr
service-foundation-ingest-767dfd5bfc-vxd5p

와일드카드 및 식 필터링은 텍스트 또는 목록과 함께 사용할 수 있지만 수치, 날짜 또는 부울은 사용할 수 없습니다.

필터 다듬기

다음을 사용하여 필터를 구체화할 수 있습니다.

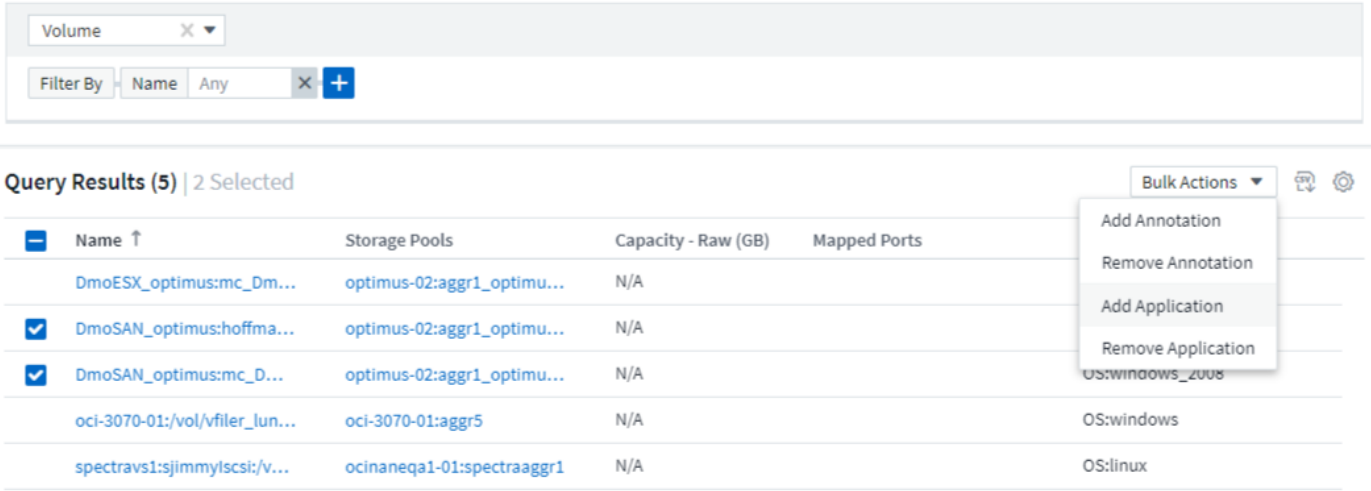
필터	기능	예	결과
* (별표)	모든 것을 검색할 수 있습니다	볼륨 * rhel	"vol"로 시작하고 "rhel"로 끝나는 모든 리소스를 반환합니다.
? (물음표)	특정 수의 문자를 검색할 수 있습니다	BOS-PRD??- S12	BOS-PRD <b>12</b> -S12, BOS-PRD <b>23</b> -S12 등을 반환합니다
또는	여러 요소를 지정할 수 있습니다	FAS2240 또는 CX600 또는 FAS3270	FAS2440, CX600 또는 FAS3270을 반환합니다
아닙니다	검색 결과에서 텍스트를 제외할 수 있습니다	EMC가 아님 *	"EMC"로 시작하지 않는 모든 항목을 반환합니다.
없음	모든 필드에서 NULL 값을 검색합니다	없음	대상 필드가 비어 있는 결과를 반환합니다
NOT *	_text-only_fields에서 NULL 값을 검색합니다	NOT *	대상 필드가 비어 있는 결과를 반환합니다

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 와일드카드 처리되지 않습니다. 연산자 또는 는 큰따옴표로 묶으면 리터럴 문자열로 처리됩니다.

쿼리 결과가 있습니다. 이제 어떻게 해야 합니까?

쿼리를 사용하면 주석을 추가하거나 자산을 응용 프로그램에 할당할 수 있습니다. 애플리케이션 또는 주석은 재고 자산(디스크, 스토리지 등)에만 할당할 수 있습니다. 통합 메트릭은 주석 또는 애플리케이션 할당에 사용할 수 없습니다.

쿼리에서 생성된 자산에 주석 또는 응용 프로그램을 할당하려면 결과 테이블 왼쪽의 확인란 옆을 사용하여 자산을 선택한 다음 오른쪽의 \* Bulk Actions \* 버튼을 클릭합니다. 선택한 자산에 적용할 작업을 선택합니다.



주석 규칙에는 쿼리가 필요합니다

를 구성하는 경우 "주석 규칙" 각 규칙에 사용할 기본 쿼리가 있어야 합니다. 하지만 위에서 살펴본 것처럼 쿼리를 필요한 만큼 광범위하고 좁힐 수 있습니다.

## 쿼리 보기

쿼리를 보고 자산을 모니터링하고 쿼리에 자산과 관련된 데이터가 표시되는 방식을 변경할 수 있습니다.

단계

1. Data Infrastructure Insights 테넌트에 로그인합니다.
2. 쿼리 \* 를 클릭하고 \* 모든 쿼리 표시 \* 를 선택합니다. 다음 중 하나를 실행하여 쿼리가 표시되는 방식을 변경할 수 있습니다.
3. 필터 상자에 텍스트를 입력하여 특정 쿼리를 표시할 수 있습니다.
4. 열 머리글의 화살표를 클릭하여 쿼리 테이블의 열 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다.
5. 열 크기를 조정하려면 파란색 막대가 나타날 때까지 열 머리글 위로 마우스를 가져갑니다. 마우스를 막대 위에 놓고 오른쪽이나 왼쪽으로 끕니다.
6. 열을 이동하려면 열 머리글을 클릭하고 오른쪽 또는 왼쪽으로 끕니다.

쿼리 결과를 스크롤할 때 Data Infrastructure Insights에서 데이터 수집기를 자동으로 폴링하면 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 내보내면 데이터를 분석하거나 다른 응용 프로그램으로 가져올 수 있습니다.

단계

1. Data Infrastructure Insights에 로그인합니다.
2. 쿼리 \* 를 클릭하고 \* 모든 쿼리 표시 \* 를 선택합니다.

쿼리 페이지가 표시됩니다.

3. 쿼리를 클릭합니다.
4. 을 클릭합니다  쿼리 결과를 .csv 파일로 내보냅니다.



CSV로 내보내기는 대시보드 테이블 위젯의 "점 3개" 메뉴와 대부분의 랜딩 페이지 테이블에서도 사용할 수 있습니다.

내보낸 데이터에는 현재 필터링, 열 및 표시된 열 이름이 반영됩니다.

참고: 자산 이름에 쉼표가 나타나면 자산 이름과 올바른 .csv 형식을 유지하면서 내보내기 시 이름이 따옴표로 묶입니다.

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.

1. Excel에서 새 시트를 엽니다.
2. "데이터" 탭에서 "텍스트에서"를 선택합니다.
3. 원하는 .csv 파일을 찾아 "가져오기"를 클릭합니다.
4. 가져오기 마법사에서 "구분 기호로 분리됨"을 선택하고 다음을 클릭합니다.
5. 구분 기호로 "쉼표"를 선택하고 다음 을 클릭합니다.
6. 원하는 열을 선택하고 열 데이터 형식으로 "텍스트"를 선택합니다.
7. 마침 을 클릭합니다.

개체가 Excel에서 올바른 형식으로 표시되어야 합니다.

## 쿼리 수정 또는 삭제

쿼리 중인 자산에 대한 검색 기준을 변경하려는 경우 쿼리와 연결된 조건을 변경할 수 있습니다.



## 쿼리 수정

### 단계

1. Explore \* 를 클릭하고 \* All Metric Queries \* 를 선택합니다.

쿼리 페이지가 표시됩니다.

2. 쿼리 이름을 클릭합니다
3. 쿼리에 조건을 추가하려면 열 아이콘 을 클릭하고 목록에서 메트릭 또는 특성을 선택합니다.

필요한 모든 변경을 수행한 경우 다음 중 하나를 수행합니다.

- 저장 \* 버튼을 클릭하여 처음에 사용된 이름으로 쿼리를 저장합니다.
- 저장 \* 버튼 옆에 있는 드롭다운을 클릭하고 \* 다른 이름으로 저장 \* 을 선택하여 다른 이름으로 쿼리를 저장합니다. 이렇게 해도 원본 쿼리는 덮어쓰지 않습니다.
- 저장 \* 버튼 옆에 있는 드롭다운을 클릭하고 \* 이름 바꾸기 \* 를 선택하여 처음에 사용한 쿼리 이름을 변경합니다. 원본 쿼리를 덮어씁니다.
- 저장 \* 버튼 옆에 있는 드롭다운을 클릭하고 \* 변경 내용 취소 \* 를 선택하여 쿼리를 마지막으로 저장된 변경 내용으로 되돌립니다.

## 쿼리 삭제

쿼리를 삭제하려면 \* 쿼리 \* 를 클릭하고 \* 모든 쿼리 표시 \* 를 선택한 후 다음 중 하나를 실행합니다.

1. 쿼리 오른쪽에 있는 "세 점" 메뉴를 클릭하고 \* 삭제 \* 를 클릭합니다.
2. 쿼리 이름을 클릭하고 \* 저장 \* 드롭다운 메뉴에서 \* 삭제 \* 를 선택합니다.

## 테이블 값 복사 중

테이블의 값을 클립보드로 복사하여 검색 상자 또는 기타 응용 프로그램에서 사용할 수 있습니다.

이 작업에 대해

테이블 또는 쿼리 결과의 값을 클립보드로 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: 단일 값 필드의 경우 필드 위에 마우스를 놓고 나타나는 클립보드 아이콘을 클릭합니다. 검색 필드 또는 기타 응용 프로그램에서 사용할 수 있도록 값이 클립보드에 복사됩니다.

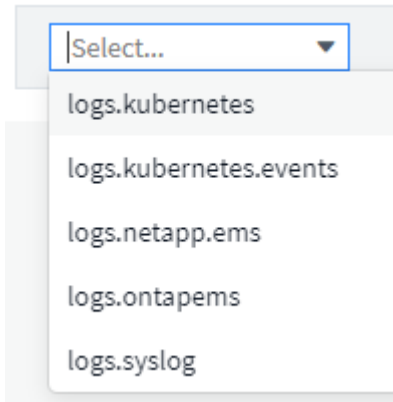
이 방법을 사용하면 자산에 연결된 값만 복사할 수 있습니다. 단일 값(예: 비목록)이 포함된 필드에만 복사 아이콘이 있습니다.

## 로그 탐색기

Data Infrastructure Insights 로그 탐색기는 시스템 로그를 쿼리하는 강력한 도구입니다. 또한 조사에 도움이 될 뿐 아니라 특정 로그 트리거가 활성화될 때 경고를 제공하기 위해 로그 쿼리를 모니터에 저장할 수도 있습니다.

로그 탐색을 시작하려면 \* 로그 쿼리 > + 새 로그 쿼리 \* 를 클릭합니다.

목록에서 사용 가능한 로그를 선택합니다.



쿼리에 사용할 수 있는 로그 유형은 사용자 환경에 따라 다를 수 있습니다. 시간이 지남에 따라 추가 로그 유형을 추가할 수 있습니다.

필터를 설정하여 쿼리 결과를 세부적으로 조정할 수 있습니다. 예를 들어, 오류를 표시하는 모든 로그 메시지를 찾으려면 "failed"라는 단어가 포함된 \_messages\_에 대한 필터를 설정합니다.



필터 필드에 원하는 텍스트를 입력할 수 있습니다. Data Infrastructure Insights에서 입력할 때 해당 문자열이 포함된 와일드카드 검색을 생성하라는 메시지를 표시합니다.

결과는 표시된 각 기간의 로그 인스턴스 수를 보여 주는 그래프에 표시됩니다. 그래프 아래에는 로그 항목이 템플릿입니다. 선택한 시간 범위에 따라 그래프와 항목이 자동으로 새로 고쳐집니다.

2gebjfo / All Log Queries /  Last 3 Hours Save

logs.netapp.ems

Filter By message "failed" + ? Create a Log Monitor

Bucket: 5 minutes

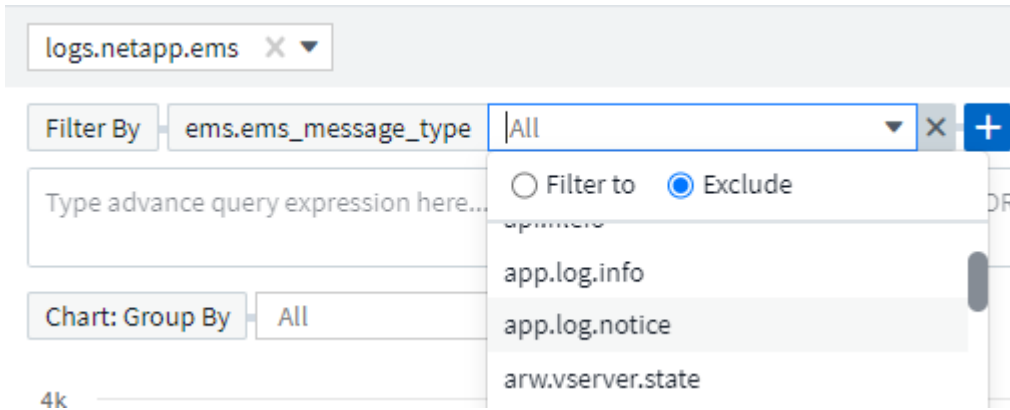
**Log Entries** Last updated 10/21/2021 11:04:56 AM

timestamp	source	message
10/21/2021 10:55:39 AM	agent:EmsCollector;cluster:a0d561f7-7a66-11e2-9699-123478563412;node:889d3681-79d0-11e2-85aa-811faf325b91;	monitor.chassisPowerSupply.degraded: Chassis power supply 1 is degraded: PSU1 Power Output has failed
10/21/2021 10:55:39 AM	agent:EmsCollector;cluster:a0d561f7-7a66-11e2-9699-123478563412;node:889d3681-79d0-11e2-85aa-811faf325b91;	monitor.chassisPowerSupply.degraded: Chassis power supply 1 is degraded: PSU1 has failed
10/21/2021 10:54:40 AM	agent:EmsCollector;cluster:a0d561f7-7a66-11e2-9699-123478563412;node:9ee4fbd1-79d0-11e2-b141-412d63ec6497;	monitor.chassisPowerSupply.degraded: Chassis power supply 1 is degraded: PSU1 Power Output has failed

## 필터링

### 포함/제외

로그를 필터링할 때 \* 입력 문자열을 \* 포함(예: "필터 대상") 또는 \* 제외 \* 로 선택할 수 있습니다. 제외된 문자열은 완료된 필터에 "Not <string>"로 표시됩니다.



와일드카드 또는 식(예 NOT, 또는, "없음" 등)이 필터 필드에 진한 파란색으로 표시됩니다. 목록에서 직접 선택한 항목은 연한 파란색으로 표시됩니다.



언제든지 \_ 로그 모니터 생성 \_ 을(를) 클릭하여 현재 필터를 기반으로 새 모니터를 생성할 수 있습니다.

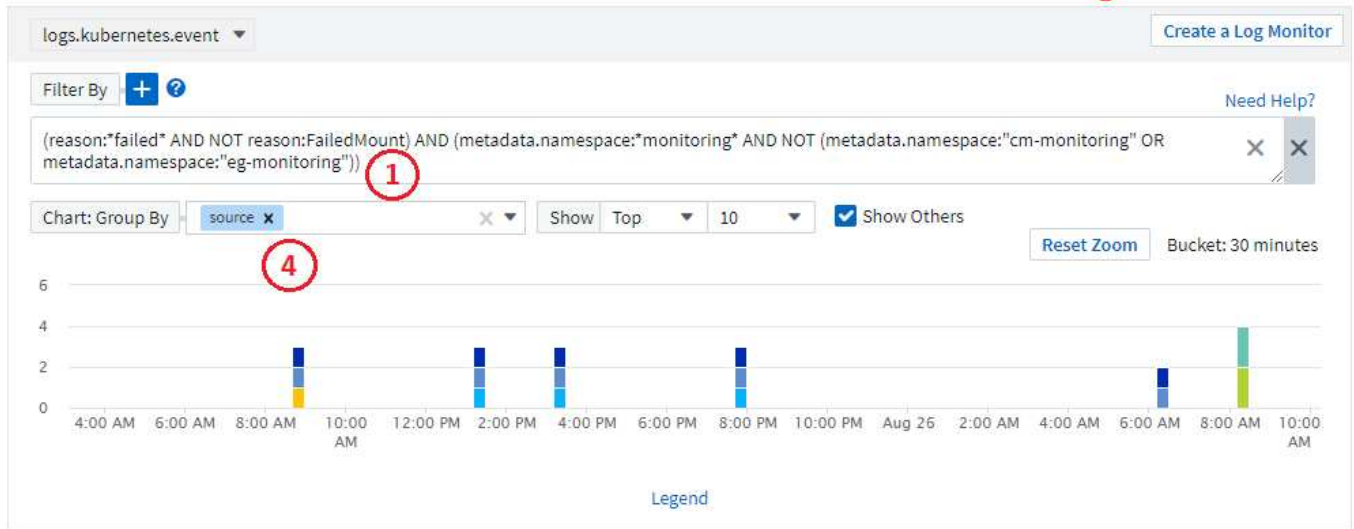
### 고급 필터링

쿼리 또는 대시보드 위젯에서 텍스트 또는 목록 값을 필터링할 때 입력을 시작하면 현재 텍스트를 기반으로 \* 와일드카드 필터 \* 를 만드는 옵션이 표시됩니다. 이 옵션을 선택하면 와일드카드 식과 일치하는 모든 결과가 반환됩니다. NOT, AND, OR를 사용하여 식을 만들거나 "없음" 옵션을 선택하여 null 값을 필터링할 수도 있습니다.



필터링을 작성할 때는 쿼리를 자주 저장해야 합니다. 고급 쿼리는 "자유 형식" 문자열 입력이며, 빌드할 때 구문 분석 오류가 발생할 수 있습니다.

이 화면 이미지에서 \_logs.kubernetes.event\_log의 고급 쿼리에 대해 필터링된 결과를 보여 줍니다. 이 페이지에 많은 일이 일어나고 있으며, 이미지 아래에 설명되어 있습니다:

Log Entries 2Last updated 08/30/2023 9:54:13 AM ⚙

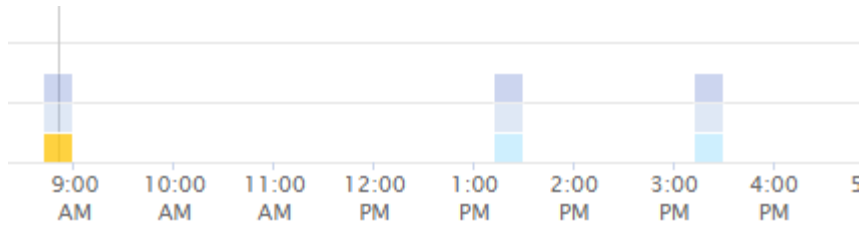
timestamp	source	message	metadata.namespace ↑	reason
08/26/2023 8:40:28 AM	kubernetes_cluster:eg-stream;namespace:33994-monitoring;pod_name:event-exporter-5db67db995-bxmkf;	Error: context deadline exceeded	k3s-cm-monitoring	Failed
08/26/2023 8:40:28 AM	kubernetes_cluster:eg-stream;namespace:ph-monitoring;pod_name:event-exporter-c4446976c-jxrdc;	Error: context deadline exceeded	k3s-cm-monitoring	Failed
08/26/2023 8:40:29 AM	kubernetes_cluster:eg-	Error: failed to reserve	k3s-cm-monitoring	Failed

1. 이 고급 쿼리 문자열은 다음을 필터링합니다.

- "failed"라는 단어가 포함되지만 "FailedMount"라는 특정 이유가 있는 것은 아닌 `_REASON_`을 사용하여 로그 항목을 필터링합니다.
- "모니터링"이라는 단어를 포함하여 `metadata.namespace`을 포함하는 모든 항목을 포함하지만 "CM 모니터링" 또는 "예 모니터링"의 특정 네임스페이스는 제외합니다.

위의 경우 "cm-모니터링"과 "예-모니터링"은 모두 대시("-)를 포함하므로 문자열을 큰따옴표로 포함하거나 구문 분석 오류가 표시됩니다. 대시, 공백 등이 포함되지 않은 문자열은 따옴표로 묶을 필요가 없습니다. 확실하지 않은 경우 문자열을 따옴표로 묶어 보십시오.

2. "필터 기준" 값 및 고급 쿼리 필터를 포함하여 현재 필터의 결과가 결과 목록에 표시됩니다. 표시된 열을 기준으로 목록을 정렬할 수 있습니다. 추가 열을 표시하려면 "기어" 아이콘을 선택합니다.
3. 특정 기간 내에 발생한 로그 결과만 표시하도록 그래프를 확대했습니다. 여기에 표시된 시간 범위는 현재 확대/축소 수준을 반영합니다. 확대/축소 재설정 `_` 버튼을 선택하여 확대/축소 수준을 현재 Data Infrastructure Insights 시간 범위로 다시 설정합니다.
4. 차트 결과는 `_source_field`별로 그룹화되어 있습니다. 차트는 각 열의 결과를 색상으로 그룹화하여 표시합니다. 차트의 열 위로 마우스를 이동하면 특정 항목에 대한 세부 정보가 표시됩니다.



Friday 08/25/2023 08:51:00 AM

<span style="color: blue;">■</span> kubernetes_cluster:vanilla25;namespace:docker-monitoring;pod_name:event-exporter-7d468bbf5b-8bzqt;	1	33.33%
<span style="color: blue;">■</span> kubernetes_cluster:vanilla25;namespace:eg-monitoring;pod_name:event-exporter-7c4cb666d6-xd9mb;	1	33.33%
<span style="color: yellow;">■</span> kubernetes_cluster:vanilla25;namespace:oc-k3s-monitoring;pod_name:event-exporter-99d5fcd8-lbg99;	1	33.33%
<b>Total</b>	<b>3</b>	

## 필터 다듬기

다음을 사용하여 필터를 구체화할 수 있습니다.

필터	기능
* (별표)	모든 것을 검색할 수 있습니다
? (물음표)	특정 수의 문자를 검색할 수 있습니다
또는	여러 요소를 지정할 수 있습니다
아닙니다	검색 결과에서 텍스트를 제외할 수 있습니다
없음	모든 필드에서 NULL 값을 검색합니다
NOT *	_text-only_fields에서 NULL 값을 검색합니다

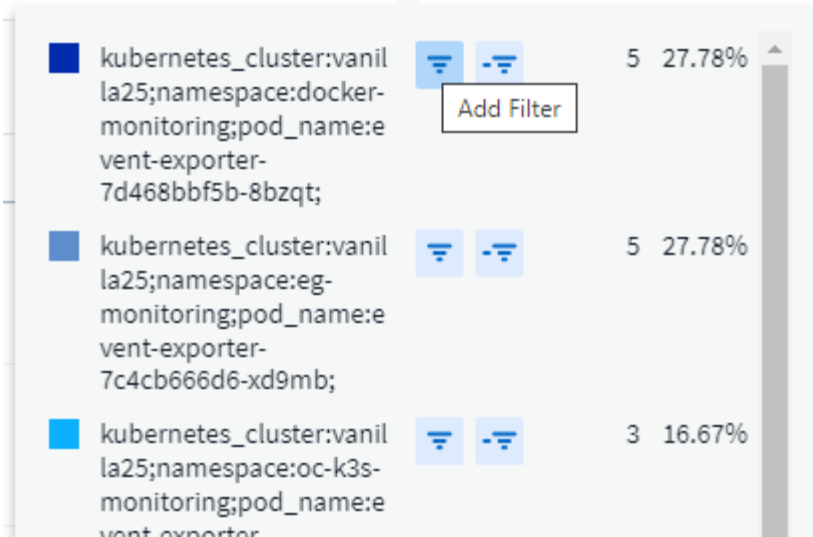
필터 문자열을 큰따옴표로 묶으면 Insight는 첫 번째 견적과 마지막 견적 사이의 모든 항목을 정확히 일치하는 것으로 간주합니다. 따옴표 안에 있는 모든 특수 문자나 연산자는 리터럴로 처리됩니다. 예를 들어 "\*"를 필터링하면 리터럴 별표로 된 결과가 반환되고, 이 경우 별표는 와일드카드로 처리되지 않습니다. 연산자 또는 는 큰따옴표로 묶으면 리터럴 문자열로 처리됩니다.

단순 필터를 고급 쿼리 필터와 결합할 수 있습니다. 결과 필터는 둘 중 "AND"입니다.

## 차트 범례

차트 아래의 Legend 에도 몇 가지 놀라운 점이 있습니다. 범례에 표시된 각 결과(현재 필터 기반)에 대해 해당 줄의 결과만 표시하거나(필터 추가) 해당 줄에 대한 결과만 표시하는 옵션(제외 필터 추가)이 있습니다. 차트 및 로그 항목 목록이 업데이트되어 선택 항목에 따른 결과가 표시됩니다. 이 필터링을 제거하려면 범례를 다시 열고 [X]를 선택하여 범례 기반 필터를 지웁니다.

### Legend



The screenshot shows a legend table with three entries. Each entry has a blue square icon, a filter icon (a funnel with a minus sign), and a count with a percentage. A tooltip 'Add Filter' is visible over the first filter icon.

Filter Label	Count	Percentage
kubernetes_cluster:vanila25;namespace:docker-monitoring;pod_name:event-exporter-7d468bbf5b-8bzqt;	5	27.78%
kubernetes_cluster:vanila25;namespace:eg-monitoring;pod_name:event-exporter-7c4cb666d6-xd9mb;	5	27.78%
kubernetes_cluster:vanila25;namespace:oc-k3s-monitoring;pod_name:event-exporter-	3	16.67%

### 로그 세부 정보

목록에서 로그 항목의 아무 곳이나 클릭하면 해당 항목에 대한 세부 정보 창이 열립니다. 여기에서 이벤트에 대한 자세한 정보를 확인할 수 있습니다.

선택한 필드를 현재 필터에 추가하려면 "Add Filter(필터 추가)"를 클릭합니다. 로그 항목 목록은 새 필터에 따라 업데이트됩니다.

## Log Details



### timestamp

09/20/2021 9:03:36 PM

### message

2021-09-20T15:33:36Z E! [processors.execcd] stderr: "Total time to process mountstats file: /hostfs/proc/1/mountstats, was: 0s"

id: 227814532095936770

node\_name: ci-auto-dsacq-insights-1.cloudinsights-dev.netapp.com

Add Filter



source: telegraf-ds-dfcc5

type: logs.kubernetes

### kubernetes

kubernetes.annotations.openshift.io\_scc: telegraf-hostaccess

kubernetes.container\_hash: ci-registry.name.openenglab.netapp.com:8077/telegraf@sha256:00b45a7cc0761c

## 문제 해결

여기에서 로그 쿼리 문제 해결을 위한 제안 사항을 찾을 수 있습니다.

* 문제: *	* 사용해 보세요. *
로그 쿼리에 "디버그" 메시지가 표시되지 않습니다	디버그 로그 메시징이 수집되지 않았습니다. 원하는 메시지를 캡처하려면 관련 메시지 심각도를 <code>_INFORMATIONAL</code> , <code>ERROR</code> , <code>ALERT</code> , <code>EMERGENCY</code> , 또는 <code>_NOTICE_LEVEL</code> 로 변경합니다.

## 인사이트

### 인사이트

Insights를 사용하면 리소스 사용량과 이러한 리소스가 다른 리소스에 미치는 영향 또는 전체 분석에 소요되는 시간을 파악할 수 있습니다.

다양한 Insights를 사용할 수 있습니다. 대시보드 > 인사이트 \* 로 이동하여 심층 분석을 시작합니다. 기본 탭에서 활성 Insights(현재 발생하고 있는 Insights)를 보거나 `_Inactive Insights` 탭에서 비활성 Insights를 볼 수 있습니다. Inactive Insights는 이전에 활성화되었지만 더 이상 발생하지 않는 Insights입니다.

## Insight 유형

### 스트레스 상태의 공유 리소스

워크로드가 큰 경우 공유 리소스에 있는 다른 워크로드의 성능이 저하될 수 있습니다. 이렇게 하면 공유 리소스가 스트레스를 받게 됩니다. Data Infrastructure Insights는 리소스 포화 및 환경의 영향을 조사하는 데 도움이 되는 툴을 제공합니다. "[자세한 정보](#)"

### 공간이 부족되는 Kubernetes 네임스페이스

Space Insight가 없는 Kubernetes 네임스페이스에서는 공간이 부족할 위험이 있는 Kubernetes 네임스페이스의 워크로드를 볼 수 있으며 각 공간이 가득 채워지기 전의 남은 일 수에 대한 추정치가 있습니다. "[자세한 정보](#)"

### ONTAP 콜드 스토리지 재확보

Reclaim ONTAP 냉장 보관\_Insight는 ONTAP 시스템의 볼륨에 대한 콜드 용량, 잠재적 비용/전력 절감 및 권장 조치 항목에 대한 데이터를 제공합니다. "[자세한 정보](#)"



이것은 `_Preview_feature` 이며 개선 사항이 있을 때 시간이 지남에 따라 변경될 수 있습니다. "[자세한 정보](#)" Data Infrastructure Insights Preview 기능 정보

## 인사이트: 부하 상태의 공유 리소스

워크로드가 큰 경우 공유 리소스에 있는 다른 워크로드의 성능이 저하될 수 있습니다. 이렇게 하면 공유 리소스가 스트레스를 받게 됩니다. Data Infrastructure Insights는 리소스 포화 및 환경의 영향을 조사하는 데 도움이 되는 툴을 제공합니다.

### 용어

작업 부하 또는 리소스 영향에 대해 이야기할 때 다음 정의가 유용합니다.

까다로운 워크로드 \* 는 현재 공유 스토리지 풀의 다른 리소스에 영향을 미치는 것으로 식별된 워크로드입니다. 이러한 워크로드는 더 높은 IOPS(예:)를 유도하여 영향을 받는 워크로드의 IOPS를 줄입니다. 수요가 많은 워크로드를 \_ 이(가) 많이 사용되는 워크로드라고 합니다.

영향을 받는 워크로드 \* 는 공유 스토리지 풀에서 많은 비용이 소모되는 워크로드의 영향을 받는 워크로드입니다. 이러한 워크로드는 까다로운 워크로드로 인해 IOPS 및/또는 지연 시간이 감소되고 있습니다.

Data Infrastructure Insights에서 주요 컴퓨팅 워크로드를 찾지 못한 경우 볼륨 또는 내부 볼륨 자체가 워크로드로 인식됩니다. 이는 까다롭고 영향을 받는 작업 부하에 모두 적용됩니다.

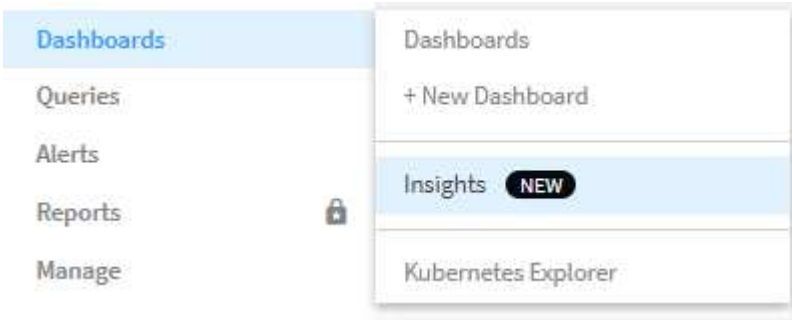
- Shared Resource Saturation \* 은 IOPS에 영향을 주는 비율과 `_baseline_`의 비율입니다.
- 기준 \* 은 감지된 포화 직전의 시간 내에 각 작업 부하에 대해 보고된 최대 데이터 포인트로 정의됩니다.

IOPS가 공유 스토리지 풀의 다른 리소스 또는 워크로드에 영향을 미치는 것으로 확인되면 \* 경합 \* 또는 \* 채도 \* 가 발생합니다.

### 까다로운 작업 부하

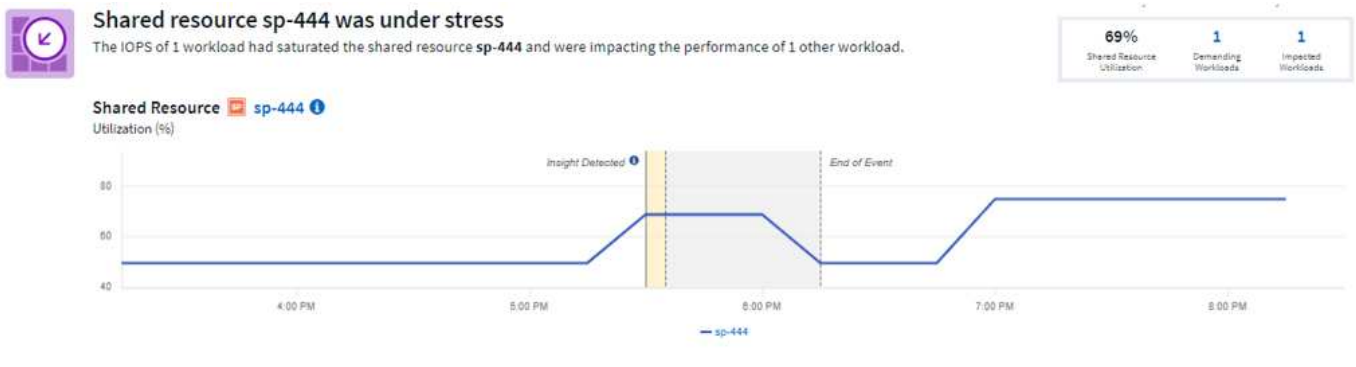
공유 리소스의 까다롭고 영향을 받는 워크로드를 확인하려면 \* 대시보드 > 인사이트 \* 를 클릭하고 스트레스 \* 인사이트에서 \* 공유 리소스 \* 를 선택합니다.





Data Infrastructure Insights에는 포화가 감지된 모든 워크로드의 목록이 표시됩니다. Data Infrastructure Insights는 하나 이상의 까다로운 리소스 \* 또는 \*영향을 받은 리소스 가 감지된 워크로드를 표시합니다.

워크로드에 대한 세부 정보 페이지를 보려면 워크로드를 클릭합니다. 위 차트에는 경합/포화가 발생하는 공유 리소스(예: 스토리지 풀)의 작업이 표시됩니다.



다음 두 개의 차트는 까다로운 작업 부하의 \_요구\_ 워크로드 및 \_영향\_을 보여 줍니다.





각 표 아래에는 경합에 영향을 주거나 영향을 받는 워크로드 및/또는 리소스 목록이 나와 있습니다. 예를 들어 VM과 같은 리소스를 클릭하면 해당 리소스에 대한 세부 정보 페이지가 열립니다. 워크로드를 클릭하면 관련된 포드가 표시된 쿼리 페이지가 열립니다. 링크가 빈 쿼리를 열 경우 영향을 받는 POD가 더 이상 활성 경합에 속하지 않기 때문일 수 있습니다. 쿼리의 시간 범위를 수정하여 더 크거나 더 집중된 시간 범위에서 창 목록을 볼 수 있습니다.

포화도를 해결하려면 어떻게 해야 합니까?

환경의 포화 가능성을 줄이거나 제거하기 위해 취할 수 있는 여러 단계가 있습니다. 이 정보는 페이지의 \* + Show Recommendations \* 링크를 확장하여 표시됩니다. 다음은 몇 가지 시도해볼 수 있는 사항입니다.

- IOPS가 높은 소비자를 이동하세요

"greedy" 워크로드를 포화도가 낮은 스토리지 풀로 이동합니다. 불필요한 비용이나 추가 경쟁 상황을 피하기 위해 워크로드를 이동하기 전에 이러한 풀의 계층 및 용량을 평가하는 것이 좋습니다.

- QoS(서비스 품질) 정책 구현

사용 가능한 리소스를 충분히 확보하기 위해 워크로드별로 QoS 정책을 구현하면 스토리지 풀의 포화를 줄일 수 있습니다. 이것은 장기적인 솔루션입니다.

- 리소스를 더 추가합니다

공유 리소스(예: 스토리지 풀)가 IOPS 포화 지점에 도달한 경우 풀에 더 많은 또는 더 빠른 디스크를 추가하면 사용 가능한 충분한 리소스를 확보하여 포화도를 줄일 수 있습니다.

마지막으로, \* Insight Link 복사 \* 를 클릭하여 페이지 URL을 클립보드에 복사하여 동료와 보다 쉽게 공유할 수 있습니다.

## 인사이트: Kubernetes 네임스페이스가 공간 부족입니다

귀사의 환경에서 공간이 부족하게 되는 것은 결코 좋은 일이 아닙니다. Data Infrastructure Insights를 사용하면 Kubernetes 영구 볼륨이 가득 차기 전의 시간을 예측할 수 있습니다.

Space\_Insight에서 실행되는 Kubernetes 네임스페이스 를 사용하면 공간이 부족할 위험이 있는 Kubernetes 네임스페이스의 워크로드를 확인할 수 있으며, 각 영구 볼륨이 꽉 차게 되기 전의 남은 일 수에 대한 추정치가 있습니다.

이 Insight는 \* 대시보드 > 인사이트 \* 로 이동하여 볼 수 있습니다.

## Kubernetes Namespaces Running Out of Space (3)

Description	Estimated Days to Full	Workloads at Risk	Detected ↓
<a href="#">1 workload at risk on es</a>	35	1	2 days ago
<a href="#">1 workload at risk on manager</a>	24	1	2 days ago
<a href="#">2 workloads at risk on cloudinsights</a>	1	2	2 days ago

워크로드를 클릭하여 Insight의 세부 정보 페이지를 엽니다. 이 페이지에는 워크로드 용량 추세를 보여 주는 그래프와 다음을 보여 주는 표가 표시됩니다.

- 워크로드 이름
- 영구 볼륨이 영향을 받습니다
- 예상 전체 시간(일)
- 영구 볼륨 용량
- 백엔드 스토리지 리소스가 영향을 받으며, 현재 사용 중인 용량이 총 용량을 초과하게 됩니다. 이 링크를 클릭하면 백엔드 볼륨에 대한 상세 랜딩 페이지가 표시됩니다.

### Workloads at risk (2)

Workloads	Persistent Volume (pvClaim)	Time to Full (Days) ↓	Persistent Volume Capacity (GiB)	Backend Storage Resource (Capacity Used)
multi (1)	pv1 (pvc1)	1	4.00	internal-volume-601 60.00% (3.00/5.00 GiB)
taskmanager (1)	pv1 (pvc1)	1	4.00	internal-volume-601 60.00% (3.00/5.00 GiB)

공간이 부족할 경우 어떻게 해야 할까요?

Insight(인사이트) 페이지에서 \* + Show Recommendations(권장 사항 표시) \* 를 클릭하여 가능한 해결책을 확인합니다. 공간 부족 시 가장 쉬운 옵션은 항상 용량을 추가하는 것입니다. Data Infrastructure Insights에서는 목표 60일 예측에 전체 시간을 늘려 줄 수 있는 최적의 용량을 보여줍니다. 다른 권장 사항도 나와 있습니다.

### Show Recommendations

- Get time to full back up to 60 days by adding more capacity to backend resources  
Add to the following resources to bring time-to-full up to ideal capacity.

Backend Resource ↓	Current Capacity (time to full)		Recommended Capacity to Add		Ideal Capacity (time to full)
internal-volume-601	2.00 GiB 1 Days	+	518.79 GiB	=	520.79 GiB 60 Days
- Use NetApp Astra Trident with your K8s to automatically grow capacity  
Astra Trident can keep your capacity lean without risk of running out of space.

[Learn more about Astra Trident](#)

[Copy Insight Link](#)

또한 이 Insight에 대한 편리한 링크를 복사하여 페이지에 책갈피를 지정하거나 팀과 쉽게 공유할 수도 있습니다.

## 인사이트: ONTAP 냉장 보관 확보

Reclaim ONTAP 냉장 보관\_Insight는 ONTAP 시스템의 볼륨에 대한 콜드 용량, 잠재적 비용/전력 절감 및 권장 조치 항목에 대한 데이터를 제공합니다.

이러한 Insights를 보려면 \* 대시보드 > 인사이트 \* 로 이동하여 \_Reclaim ONTAP 냉장 보관\_Insight를 살펴봅니다. 이 Insight는 Data Infrastructure Insights가 콜드 스토리지를 감지한 경우에만 영향을 받는 스토리지를 나열하며, 그렇지 않으면 "모두 지우기" 메시지가 표시됩니다.


30일 미만의 콜드 데이터는 표시되지 않습니다.

### Reclaim ONTAP Cold Storage (3)

Description	Cold data storage(TiB)	Workloads with cold data	Detected ↓
<a href="#">0.30 TiB of cold data on storage rtp-sa-cl04</a>	0.30	45	an hour ago
<a href="#">1.22 TiB of cold data on storage umeng-aff300-01-02</a>	1.22	84	16 days ago
<a href="#">11.62 TiB of cold data on storage rtp-sa-cl01</a>	11.62	171	16 days ago

Insight 설명은 "콜드" 데이터로 감지된 데이터의 양과 데이터가 상주하는 스토리지를 빠르게 표시합니다. 또한, 콜드 데이터가 포함된 워크로드 수도 제공합니다.


목록에서 Insight를 선택하면 Cloud로 데이터를 이동하거나, 비구현 디스크를 순환시키기 위한 권장 사항과 이러한 권장 사항을 구현함으로써 실현할 수 있는 예상 비용 및 전력 절감 효과를 포함한 자세한 정보가 표시된 페이지가 열립니다. 이 페이지에는 예도 편리한 링크가 제공됩니다 "NetApp의 TCO 계산기" 그래서 수치를 시험해 볼 수 있습니다.



**150 Workloads on storage rtp-sa-cl01 contains a total of 9.5 TiB of cold data.**

You could lower costs 9.3% a year and reduce your carbon footprint by moving cold storage to the cloud.

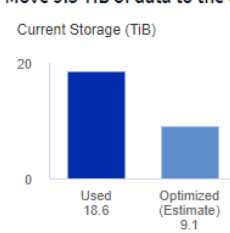
Detected: 2 months ago, 9:21 AM (ACTIVE)  
May 19, 2023 10:05AM



Estimated Yearly Cost Savings\*


**\$9,728.00**

Move 9.5 TiB of data to the cloud



Current Storage (TiB)

Used: 18.6, Optimized (Estimate): 9.1



kWh Reduction Yearly Savings\*\*

**368.73 kWh**

\*Visit the [NetApp TCO Calculator](#) for your actual cost savings. Go to [Annotation Page](#) to edit the cloud tier cost in the tier annotation.

\*\* Based on average disk power consumption

### 권장 사항

Insight(인사이트) 페이지에서 \* Recommendations(권장 사항) \* 를 확장하여 다음 옵션을 탐색합니다.

- 사용되지 않는 워크로드(좀비)를 저렴한 HDD(스토리지 계층)로 이동

zombie 플래그, 콜드 스토리지 및 일 수를 활용하여 가장 낮은 데이터와 가장 큰 양의 데이터를 찾아 워크로드를 저렴한 스토리지 계층(예: 하드 디스크 스토리지를 사용하는 스토리지 풀)으로 이동합니다. 워크로드가 30일 이상 심각한 IO 요청을 받지 않은 경우 "좀비"로 간주됩니다.

- 사용하지 않는 워크로드를 삭제합니다

사용 중이 아닌 워크로드를 확인하고 아카이빙을 고려하거나 스토리지 시스템에서 제거합니다.

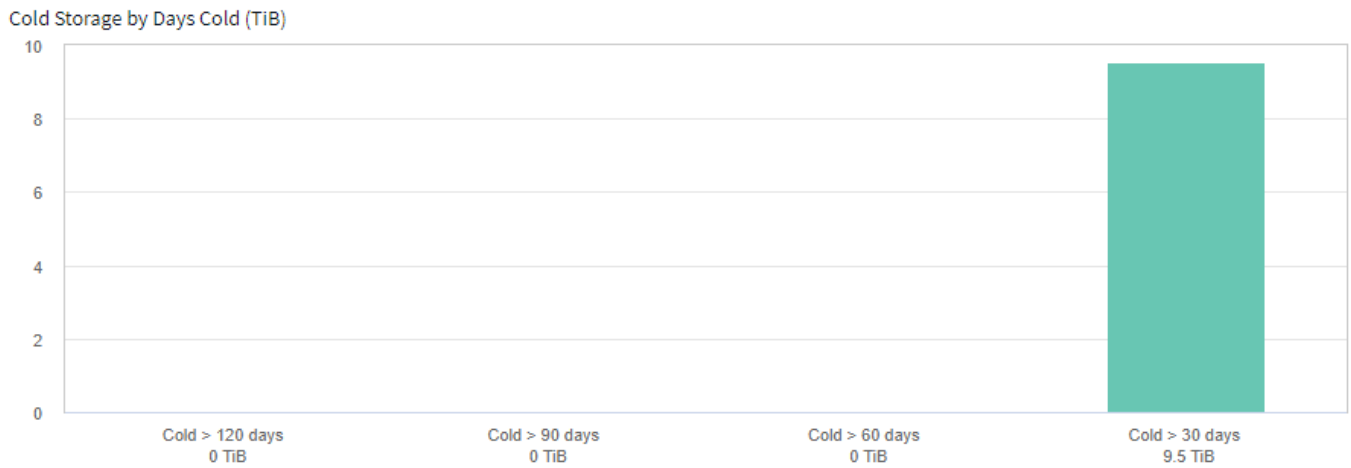
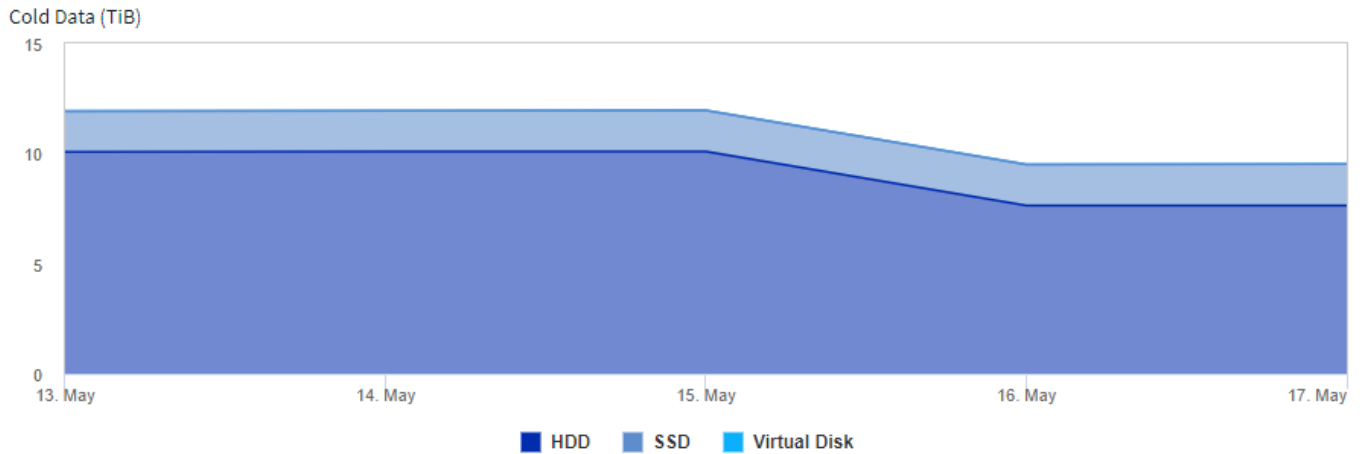
- NetApp의 Fabric Pool 솔루션을 고려해 보십시오

NetApp의 "Fabric Pool 솔루션" 콜드 데이터를 저비용 클라우드 스토리지에 자동으로 계층화하여 성능 계층의 효율성을 높이고 원격 데이터 보호를 제공합니다.

시각화 및 탐색

그래프 및 표는 추가 추세 정보를 제공할 뿐만 아니라 개별 작업 부하를 분석할 수 있게 해 줍니다.

### Cluster Cold Storage Trend [Show Details](#)



Workloads with cold data (150) [View all workloads](#)

Filter...

Workloads	# Days cold	Total Size (GiB)	Cold Data Size (GiB)	Percent Cold (%)	Is Zombie	Disk Type
SelectPool	31	8,192.00	1,714.21	20.93	N A	SAS
nj_UCS_VMw_Infrastructure	31	5,120.00	934.74	18.26	N A	SAS
Oracle_SAP_DS_220	31	2,048.00	861.97	42.09	N A	SSD
rtp_sa_workspace	31	13,000.00	741.32	5.70	N A	SAS
vc220_migrate	31	4,311.58	685.30	15.89	N A	SAS
H01_shared	31	998.25	646.55	64.77	N A	SSD
ProdSelectPool	31	8,192.00	555.30	6.78	N A	SAS
vcenter_migrate	31	6,144.00	475.99	7.75	N A	SAS
rtp_sa_mgmt_apps	31	4,096.00	449.26	10.97	N A	SAS
SOFTWARE	31	600.00	365.54	60.92	N A	SAS
DP_Migrate	31	7,168.00	347.20	4.84	N A	SAS

## 모니터링 및 경고

### 모니터를 통한 경고

모니터를 생성하여 네트워크 리소스와 관련된 문제를 알리기 위해 알림을 트리거하는 임계값을 설정합니다. 예를 들어, 다양한 프로토콜에 대해 `_node write latency`에 대해 경고하는 모니터를 생성할 수 있습니다.



모니터 및 경고는 모든 Data Infrastructure Insights 에디션에서 사용할 수 있지만 Basic Edition에는 다음 사항이 적용됩니다. \* 한 번에 최대 5개의 사용자 지정 모니터만 활성화할 수 있습니다. 5개 이상의 모니터는 에서 생성되거나 `_Paused_state`로 이동됩니다. \* VMDK, 가상 머신, 호스트 및 데이터 저장소 메트릭 모니터는 지원되지 않습니다. 이러한 메트릭에 대해 생성된 모니터가 있는 경우 일시 중지되고 Basic Edition으로 다운그레이드할 때 다시 시작할 수 없습니다.

모니터를 사용하면 스토리지, VM, EC2 및 포트와 같은 "인프라" 객체에서 생성되는 메트릭과 Kubernetes, ONTAP 고급 메트릭, Teleraf 플러그인과 같이 "통합" 데이터에 대한 임계값을 설정할 수 있습니다. 이러한 `_metric_monitor`는 경고 수준 또는 위험 수준 임계값을 초과할 때 사용자에게 경고합니다.

또한 지정된 `_log events`가 감지되면 경고를 트리거하는 모니터를 생성할 수도 있습니다.

Data Infrastructure Insights는 귀사의 환경에 다양한 솔루션을 "시스템 정의 모니터"제공합니다.

### 보안 모범 사례

Data Infrastructure Insights 경고는 사용자 환경의 데이터 포인트와 추세를 강조하도록 설계되었으며, Data

Infrastructure Insights를 사용하면 유효한 이메일 주소를 경고 수신자로 입력할 수 있습니다. 보안 환경에서 작업하는 경우 알림을 받는 사람 또는 알림에 액세스할 수 있는 사람을 특히 주의하십시오.

## 메트릭 또는 로그 모니터?

1. Data Infrastructure Insights 메뉴에서 \* Alerts > Manage Monitors \* 를 클릭합니다

모니터 목록 페이지가 표시되고 현재 구성된 모니터가 표시됩니다.

2. 기존 모니터를 수정하려면 목록에서 모니터 이름을 클릭합니다.
3. 모니터를 추가하려면 \* + Monitor \* 를 클릭합니다.



새 모니터를 추가하면 메트릭 모니터 또는 로그 모니터를 생성하라는 메시지가 표시됩니다.

- `_Metric_monitor` 인프라스트럭처 또는 성능 관련 트리거에 대한 경고
- `_Log_` 는 로그 관련 작업에 대한 경고를 모니터링합니다

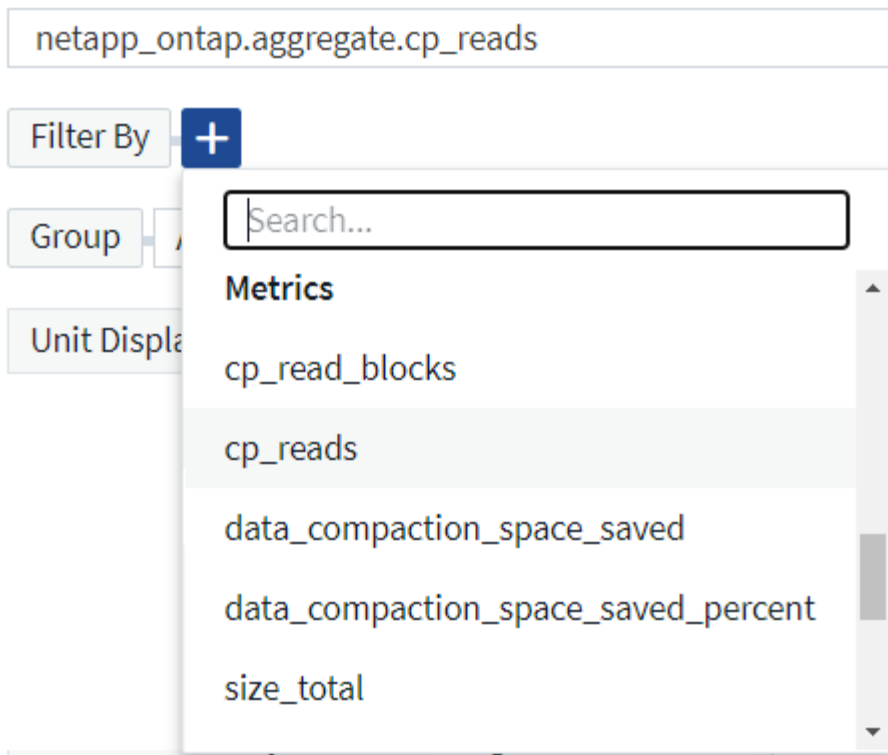
모니터 유형을 선택하면 모니터 구성 대화 상자가 표시됩니다. 구성은 생성 중인 모니터 유형에 따라 다릅니다.

## 메트릭 모니터

1. 드롭다운에서 모니터링할 객체 유형 및 메트릭을 검색하고 선택합니다.

모니터링할 객체 속성 또는 메트릭을 좁히도록 필터를 설정할 수 있습니다.

## 1 Select a metric to monitor



통합 데이터(Kubernetes, ONTAP 고급 데이터 등)를 사용할 경우, 메트릭 필터링은 필터가 데이터 시리즈의 집계 값에 대해 작동하고 잠재적으로 전체 오브젝트를 차트에서 제거할 수 있는 인프라 데이터(스토리지, VM, 포트 등)와 달리 표시된 데이터 시리즈에서 개별/일치하지 않는 데이터 요소를 제거합니다.



다중 조건 모니터(예: IOPS > X 및 지연 시간 > Y)를 생성하려면 첫 번째 조건을 임계값으로 정의하고 두 번째 조건을 필터로 정의합니다.

모니터의 조건을 정의합니다.

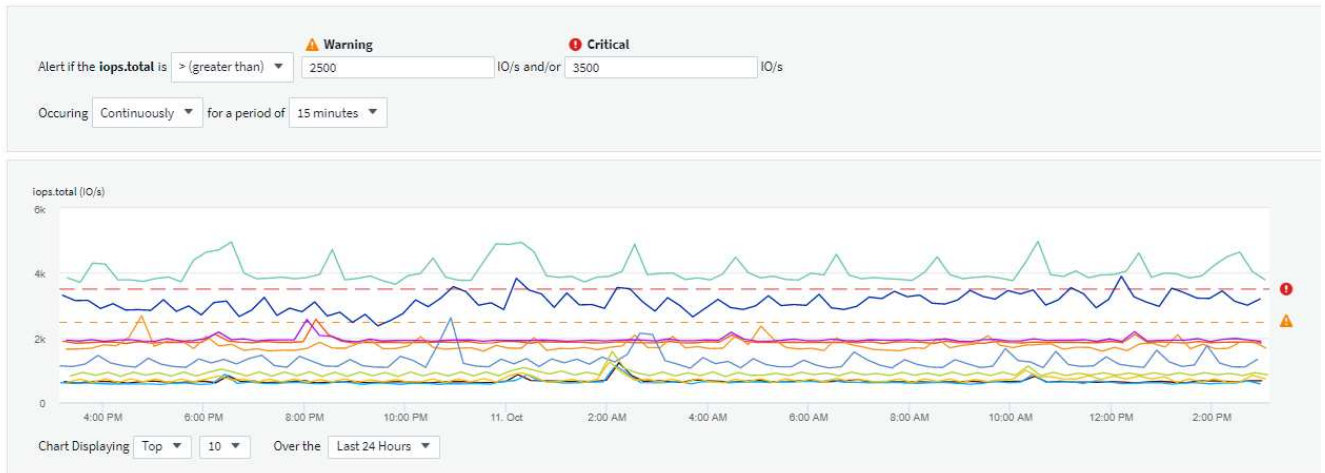
1. 모니터링할 개체 및 메트릭을 선택한 후 경고 수준 및/또는 위험 수준 임계값을 설정합니다.
2. Warning\_level의 경우 예에서는 200을 입력합니다. 이 경고 수준을 나타내는 파선이 예제 그래프에 표시됩니다.
3. Critical\_level의 경우 400을 입력합니다. 이 요주의 수준을 나타내는 점선이 예제 그래프에 표시됩니다.

그래프에는 기록 데이터가 표시됩니다. 그래프의 경고 및 위험 수준 선은 모니터의 시각적 표시이므로 각 경우에 모니터가 경고를 트리거할 수 있는 시점을 쉽게 확인할 수 있습니다.

4. 발생 간격에 대해 15분 동안 \_Continuously\_를 선택하십시오.

임계값이 위반될 때 알림을 트리거하거나 임계값이 일정 기간 동안 연속 위반이 될 때까지 대기하도록 선택할 수 있습니다. 이 예에서는 총 IOPS 피크가 경고 또는 위험 수준보다 높을 때마다 알림을 받지 않고 모니터링된 개체가 적어도 15분 동안 이러한 수준 중 하나를 지속적으로 초과할 때만 경고를 받고 싶습니다.





경고 해결 동작을 정의합니다

메트릭 모니터 경고 해결 방법을 선택할 수 있습니다. 두 가지 선택 사항이 제시됩니다.

- 메트릭이 허용 가능한 범위로 돌아오면 해결합니다.
- 메트릭이 1분에서 7일 사이의 지정된 시간 동안 허용 가능한 범위 내에 있을 때 해결합니다.

로그 모니터

로그 모니터 \* 를 만들 때는 먼저 사용 가능한 로그 목록에서 모니터링할 로그를 선택합니다. 그런 다음 위와 같이 사용 가능한 속성을 기준으로 필터링할 수 있습니다. 하나 이상의 "그룹화 기준" 속성을 선택할 수도 있습니다.



로그 모니터 필터는 비워 둘 수 없습니다.

### 1 Select the log to monitor

Log Source: logs.netapp.ems

Filter By: ems.ems\_message\_type, Nblade.vscanConnBackPressure, ems.cluster\_vendor: NetApp

ems.cluster\_model: FAS\*, AFF\*, ASA\*, Fdvm\*

Group By: ems.cluster\_uuid, ems.cluster\_vendor, ems.cluster\_model, ems.cluster\_name, ems.svm\_uuid, ems.svm\_name

경고 동작을 정의합니다

위에서 정의한 조건이 한 번(즉, 즉시) 발생할 때 심각도 수준이 *Critical*, *Warning* 또는 *Informational* 인 경우 경고를 표시하거나 조건이 두 번 이상 발생할 때까지 경고를 보내도록 모니터를 만들 수 있습니다.

경고 해결 동작을 정의합니다

로그 모니터 알림의 해결 방법을 선택할 수 있습니다. 세 가지 선택 사항이 있습니다.

- 즉시 해결 \*: 추가 조치 없이 즉시 경고가 해결됩니다
- \* 시간 기준 해결 \*: 지정된 시간이 경과한 후 경고가 해결됩니다

- \* 로그 항목에 따라 해결 \*: 후속 로그 작업이 발생하면 경고가 해결됩니다. 예를 들어, 개체가 "사용 가능"으로 기록된 경우

- Resolve instantly
- Resolve based on time
- Resolve based on log entry

Log Source

Filter By

이상 징후 감지 모니터

1. 드롭다운에서 모니터링할 객체 유형 및 메트릭을 검색하고 선택합니다.

모니터링할 객체 속성 또는 메트릭을 좁히도록 필터를 설정할 수 있습니다.

### 1 Select a metric anomaly to monitor

Object

Filter by Attribute  

Filter by Metric  

Group by

Unit Displayed In

모니터의 조건을 정의합니다.

1. 모니터링할 개체 및 메트릭을 선택한 후 이상이 감지된 조건을 설정합니다.

- 선택한 메트릭 \* 이 예측 경계를 넘어 \* 스파이크하거나 \* 이 해당 경계 아래로 떨어지거나 \* 스파이크가 경계 위로 또는 아래로 떨어질 때 이상 징후를 감지할지 여부를 선택합니다.
- 감지의 \* 감도 \* 를 설정합니다. \* 낮음 \* (더 적은 이상 징후를 감지함), \* 보통 \* 또는 \* 높음 \* (더 많은 이상 징후를 감지함).
- 경고를 기타 \* 경고 \* 또는 \* 위험 \* 으로 설정합니다.
- 원하는 경우 선택한 메트릭이 설정된 임계값 미만일 때 이상 징후를 무시하면서 노이즈를 줄이도록 선택할 수 있습니다.

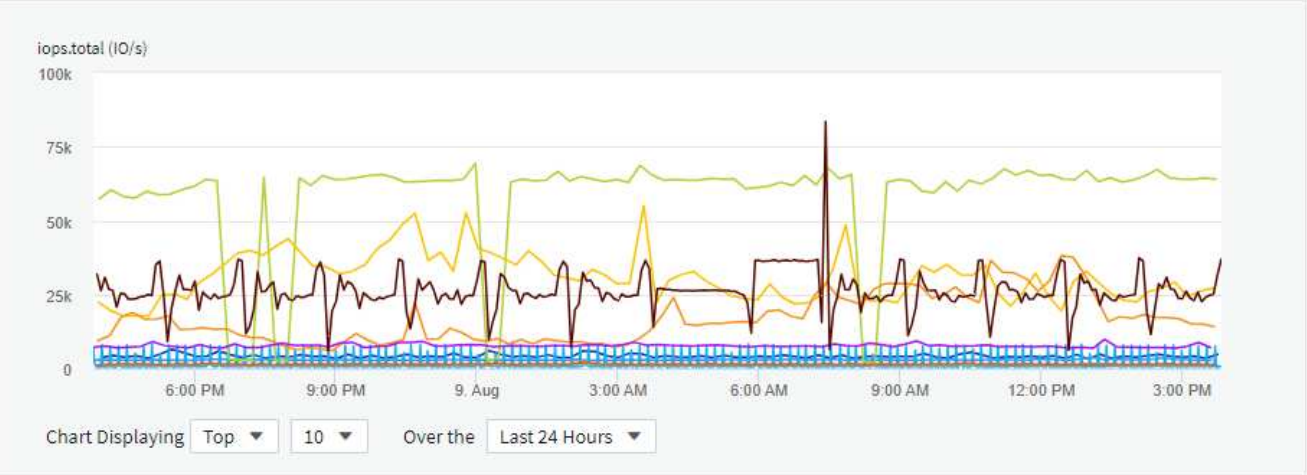
## 2 Define the monitor's conditions

Trigger alert when **performance.iops.total** Spikes above ▼ the predicted bounds.

Set sensitivity: Low (detect fewer anomalies) ▼

Alert severity: Critical ▼

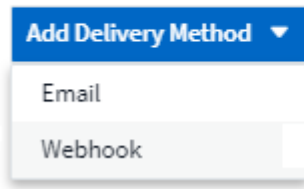
To reduce noise, ignore anomalies when **performance.iops.total** is below Optional IO/s



알림 유형 및 수신자를 선택합니다

팀 알림 설정 \_ 섹션에서 전자 메일 또는 Webhook를 통해 팀에 알리도록 선택할 수 있습니다.

## 3 Set up team notification(s) (alert your team via email, or Webhook)



- 이메일을 통한 경고: \*

알림 알림을 받을 e-메일 수신자를 지정합니다. 필요한 경우 경고 또는 위험 경고에 대해 다른 수신자를 선택할 수 있습니다.

### 3 Set up team notification(s)

The screenshot shows two identical sections for setting up email notifications. Each section has a 'Notify team on' dropdown menu and an 'Add Recipients (Required)' input field. The first section has 'Critical, Resolved' selected in the dropdown, with 'Critical' and 'Resolved' checked in the expanded list. Its recipients are 'user\_1@email.com' and 'user\_2@email.com'. The second section has 'Warning' selected in the dropdown and its recipient is 'user\_3@email.com'.

- Webhook를 통해 알림: \*

알림 알림에 사용할 웹 후크를 지정합니다. 필요한 경우 경고 또는 위험 경고에 대해 다른 Webhook을 선택할 수 있습니다.

### 3 Set up team notification(s) (alert your team via email, or Webhook)

The screenshot shows three rows for setting up Webhook notifications. Each row is labeled 'By Webhook' and includes a 'Notify team on' dropdown menu, a 'Slack' label, and a 'Use Webhook(s)' input field. The first row has 'Critical' selected, the second has 'Resolved', and the third has 'Warning'. Each 'Use Webhook(s)' field contains 'Slack' and 'Teams' tags.



ONTAP 데이터 수집기 알림은 클러스터/데이터 수집기와 관련된 특정 모니터 알림보다 우선합니다. Data Collector 자체에 대해 설정한 받는 사람 목록에는 데이터 수집기 경고가 표시됩니다. 활성 데이터 수집기 경고가 없는 경우 모니터에서 생성된 알림이 특정 모니터 수신자에게 전송됩니다.

시정 조치 또는 추가 정보 설정

추가 정보 및/또는 수정 조치는 \* 경고 설명 추가 \* 섹션을 작성하여 추가할 수 있습니다. 설명은 최대 1024자까지 가능하며 경고와 함께 전송됩니다. 인사이트/수정 조치 필드는 최대 67,000자까지 가능하며 알림 랜딩 페이지의 요약 섹션에 표시됩니다.

이러한 필드에서는 경고를 수정하거나 해결하는 데 필요한 메모, 링크 또는 단계를 제공할 수 있습니다.

#### 4 Add an alert description (optional)

<b>Add a description</b>	<input type="text" value="Enter a description that will be sent with this alert (1024 character limit)"/>
<b>Add insights and corrective actions</b>	<input type="text" value="Enter a url or details about the suggested actions to fix the issue raised by the alert"/>

모니터를 저장합니다

1. 필요한 경우 모니터에 대한 설명을 추가할 수 있습니다.
2. 모니터에 의미 있는 이름을 지정하고 \* 저장 \* 을 클릭합니다.

새 모니터가 활성 모니터 목록에 추가됩니다.

모니터 목록

모니터 페이지에는 현재 구성된 모니터가 나열되며 다음과 같은 정보가 표시됩니다.

- 모니터 이름
- 상태
- 객체/메트릭이 모니터링되고 있습니다
- 모니터 상태

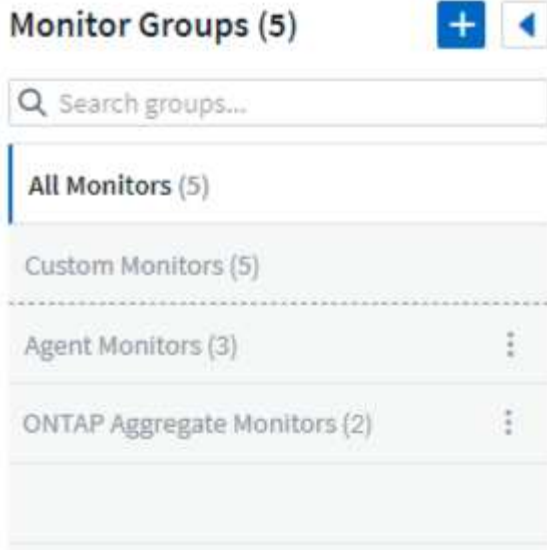
모니터 오른쪽에 있는 메뉴를 클릭하고 \* Pause \* (일시 중지 \*)를 선택하여 개체 유형의 모니터링을 일시적으로 일시 중지할 수 있습니다. 모니터링을 다시 시작할 준비가 되면 \* Resume \* (재개 \*)을 클릭합니다.

메뉴에서 \* 복제 \* 를 선택하여 모니터를 복사할 수 있습니다. 그런 다음 새 모니터를 수정하고 객체/메트릭, 필터, 조건, 이메일 수신자 등을 변경할 수 있습니다

모니터가 더 이상 필요하지 않은 경우 메뉴에서 \* Delete \* 를 선택하여 삭제할 수 있습니다.

모니터 그룹

그룹화를 사용하면 관련 모니터를 보고 관리할 수 있습니다. 예를 들어 사용자 환경의 스토리지 전용 모니터 그룹을 사용하거나 특정 수신자 목록과 관련된 모니터를 사용할 수 있습니다.



다음과 같은 모니터 그룹이 표시됩니다. 그룹에 포함된 모니터 수가 그룹 이름 옆에 표시됩니다.

- \* 모든 모니터 \* 는 모든 모니터를 나열합니다.
- \* 사용자 지정 모니터 \* 는 사용자가 생성한 모든 모니터를 나열합니다.
- \* 일시 중단된 모니터 \* 는 Data Infrastructure Insights에 의해 일시 중단된 시스템 모니터를 나열합니다.
- 또한 데이터 인프라 통찰력에는 "[시스템 정의 모니터](#)" ONTAP 인프라 및 워크로드 모니터를 포함하여 하나 이상의 그룹이 나열되는 다수의 \* 시스템 모니터 그룹 \* 이 표시됩니다.



사용자 지정 모니터는 일시 중지, 재개, 삭제 또는 다른 그룹으로 이동할 수 있습니다. 시스템 정의 모니터는 일시 중지 및 재개할 수 있지만 삭제하거나 이동할 수는 없습니다.

#### 일시 중지된 모니터

이 그룹은 Data Infrastructure Insights가 하나 이상의 모니터를 일시 중단한 경우에만 표시됩니다. 과도한 또는 지속적인 경고를 생성하는 경우 모니터가 일시 중단될 수 있습니다. 모니터가 사용자 지정 모니터인 경우 상태를 변경하여 연속 경고를 방지한 다음 모니터를 다시 시작합니다. 서스펜션의 원인이 되는 문제가 해결되면 모니터가 Suspended Monitors 그룹에서 제거됩니다.

#### 시스템 정의 모니터

사용자 환경에 모니터에 필요한 장치 및/또는 로그 가용성이 포함되어 있는 경우 이러한 그룹은 Data Infrastructure Insights에서 제공하는 모니터를 표시합니다.

시스템 정의 모니터는 수정하거나 다른 그룹으로 이동하거나 삭제할 수 없습니다. 그러나 시스템 모니터를 복제하고 복제본을 수정하거나 이동할 수 있습니다.

시스템 모니터에는 ONTAP 인프라(스토리지, 볼륨 등) 또는 워크로드(예: 로그 모니터) 또는 기타 그룹의 모니터가 포함될 수 있습니다. NetApp은 고객의 필요와 제품 기능을 지속적으로 평가하고 있으며 필요에 따라 시스템 모니터 및 그룹을 업데이트하거나 추가합니다.

#### 사용자 지정 모니터 그룹

필요에 따라 모니터를 포함할 그룹을 직접 만들 수 있습니다. 예를 들어 모든 스토리지 관련 모니터에 대해 그룹을 설정할 수 있습니다.

새 사용자 정의 모니터 그룹을 생성하려면 \* "+" 새 모니터 그룹 생성 \* 버튼을 클릭합니다. 그룹 이름을 입력하고 \* 그룹 생성 \* 을 클릭합니다. 해당 이름으로 빈 그룹이 생성됩니다.

그룹에 모니터를 추가하려면 \_All Monitors\_group(권장)으로 이동하여 다음 중 하나를 수행합니다.

- 단일 모니터를 추가하려면 모니터 오른쪽에 있는 메뉴를 클릭하고 \_Add to Group\_을 선택합니다. 모니터를 추가할 그룹을 선택합니다.
- 모니터 이름을 클릭하여 모니터의 편집 보기를 열고 *Associate to a monitor group* 섹션에서 그룹을 선택합니다.

## 5 Associate to a monitor group (optional)



그룹을 클릭하고 메뉴에서 \_Remove from Group\_을 선택하여 모니터를 제거합니다. 모든 모니터 또는 \_Custom Monitors\_ 그룹에서 모니터를 제거할 수 없습니다. 이러한 그룹에서 모니터를 삭제하려면 모니터 자체를 삭제해야 합니다.

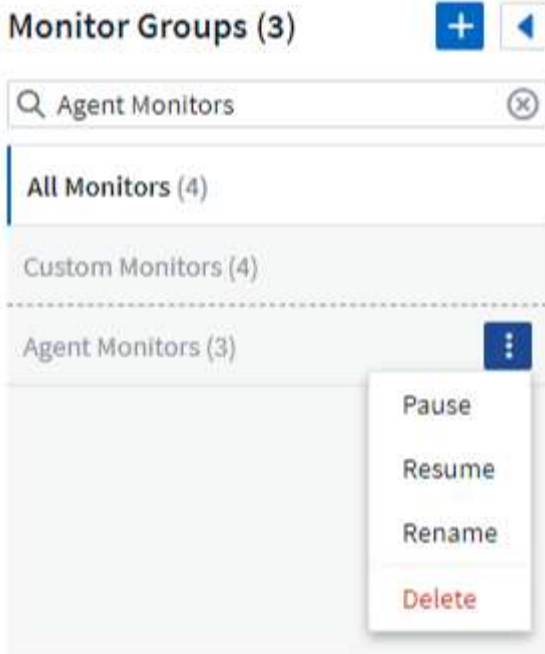


그룹에서 모니터를 제거해도 Data Infrastructure Insights에서 모니터가 삭제되지는 않습니다. 모니터를 완전히 제거하려면 모니터를 선택하고 \_Delete\_를 클릭합니다. 또한 이 작업은 해당 그룹이 속한 그룹에서 제거되며 더 이상 모든 사용자가 사용할 수 없습니다.

또한 \_Move to Group\_ 을(를) 선택하여 같은 방식으로 모니터를 다른 그룹으로 이동할 수도 있습니다.

그룹의 모든 모니터를 한 번에 일시 중지하거나 다시 시작하려면 해당 그룹의 메뉴를 선택하고 \_Pause\_or\_Resume\_을 클릭합니다.

동일한 메뉴를 사용하여 그룹의 이름을 바꾸거나 그룹을 삭제합니다. 그룹을 삭제해도 Data Infrastructure Insights에서 모니터가 삭제되지는 않으며 \_모든 모니터\_에서 계속 사용할 수 있습니다.



## 시스템 정의 모니터

Data Infrastructure Insights에는 메트릭 및 로그 모두에 대해 다수의 시스템 정의 모니터가 포함되어 있습니다. 사용 가능한 시스템 모니터는 사용자 환경에 있는 데이터 수집기에 따라 다릅니다. 따라서 데이터 수집기가 추가되거나 구성이 변경되면 Data Infrastructure Insights에서 사용할 수 있는 모니터가 변경될 수 있습니다.

"[시스템 정의 모니터](#)" Data Infrastructure Insights에 포함된 모니터에 대한 설명은 페이지를 참조하십시오.

## 추가 정보

- "[경고 보기 및 해제](#)"

## 모니터에서 경고 보기 및 관리

Data Infrastructure Insights는 이 초과되면 경고를 "[모니터링된 임계값](#)" 표시합니다.



모니터 및 경고는 Data Infrastructure Insights Standard Edition 이상에서 사용할 수 있습니다.

## 경고 보기 및 관리

알림을 보고 관리하려면 다음을 수행합니다.

1. 경고 > 모든 경고 \* 페이지로 이동합니다.
2. 최대 1,000개의 최근 알림 목록이 표시됩니다. 필드의 열 머리글을 클릭하여 모든 필드에서 이 목록을 정렬할 수 있습니다. 목록에 다음 정보가 표시됩니다. 이러한 열 중 일부만 기본적으로 표시됩니다. "기어" 아이콘을 클릭하여 표시할 열을 선택할 수 있습니다.
  - \* 경고 ID \*: 시스템에서 생성한 고유 경고 ID
  - \* Triggered Time \*: 관련 모니터가 경고를 트리거한 시간입니다
  - 현재 심각도 \* (활성 경고 탭): 활성 경고의 현재 심각도입니다



- 상위 심각도 \* (해결된 경고 탭). 경고가 해결되기 전의 최대 심각도입니다
- \* Monitor \*: 경고를 트리거하도록 구성된 모니터
- \* triggered on \*: 모니터링되는 임계값이 위반된 개체입니다
- \* 상태 \*: 현재 경고 상태, `_New_or_in process _`
- \* 활성 상태 \*: `_Active_or_Resolved _`
- \* 조건 \*: 경고를 트리거한 임계값 조건
- \* Metric \*: 모니터링되는 임계값이 위반된 개체의 메트릭입니다
- \* 모니터 상태 \*: 경고를 트리거한 모니터의 현재 상태입니다
- 시정 조치 있음: 경고에 권장 수정 조치가 있습니다. 경고 페이지를 열어 이를 확인합니다.

알림 오른쪽에 있는 메뉴를 클릭하고 다음 중 하나를 선택하여 알림을 관리할 수 있습니다.

- \* 진행 중 \* - 경고가 조사 중이거나 계속 열려 있어야 함을 나타냅니다
- \* 해제 \* 를 클릭하여 활성 경고 목록에서 경고를 제거합니다.

각 알림의 왼쪽에 있는 확인란을 선택하고 `_Change Selected Alerts Status_`를 클릭하여 여러 알림을 관리할 수 있습니다.

경고 ID를 클릭하면 경고 세부 정보 페이지가 열립니다.

#### 경고 세부 정보 페이지

경고 세부 정보 페이지는 경고 조사관이 입력한 `_요약_`, `_전문가 보기_` 개체 데이터와 관련된 그래프, 모든 `_관련 자산_` 및 `_코멘트_` 을 포함하여 경고에 대한 추가 세부 정보를 제공합니다.

## Alert Summary

### Monitor:

Volume Total Data

### Triggered On:

cluster\_name: tawny  
aggr\_name: Multiple\_Values

### Duration / Time Triggered:

1d 6h / Jun 9, 2020 2:22 AM

### Top Severity:

● Critical

### Metric:

① netapp\_ontap.workload\_volume.total\_data

### Condition:

Average total\_data is > (greater than) 0m and/or 0m all the time in 2-hour window.

### Filters Applied:

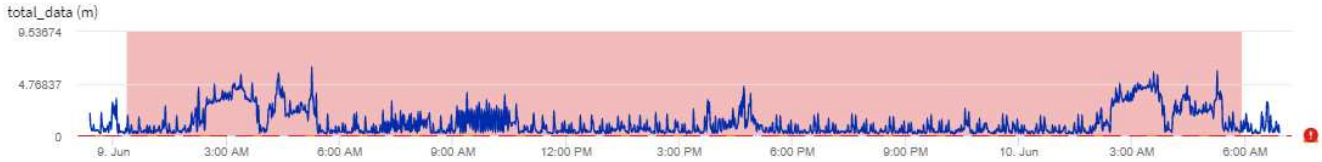
cluster\_name: Any

### Status:

New

## Expert View

Display Metrics ▾



## Related Alerts

1 item found

Alert ID	Active Status	Triggered Time ↓	Top Severity	Monitor	Triggered On	Status
AL-46769	Resolved	a day ago Jun 9, 2020 2:22 AM	<span style="color: red;">●</span> Critical	Volume Total Data	cluster_name: tawny aggr_name: Multiple_Values	New

## Comments

There are no comments yet on this alert.

[+ Comment](#)

## 데이터가 없을 때 경고합니다

Data Infrastructure Insights와 같은 실시간 시스템에서는 모니터 분석을 트리거하여 알림 생성 여부를 결정하기 위해 다음 두 가지 중 하나에 의존합니다.

- 다음 데이터 형식 도착
- 데이터포인트 없이 충분히 기다렸을 때 사용할 타이머

데이터 도착이 느리거나 데이터 도착이 없는 경우와 마찬가지로, 데이터 도착 속도가 "실시간"으로 알림을 트리거하기에 충분하지 않기 때문에 타이머 메커니즘을 대신 사용할 필요가 있습니다. 따라서 일반적으로 "분석 창을 닫고 현재 보유한 것을 살펴보기 전에 얼마나 기다려야 합니까?"가 표시됩니다. 너무 오래 기다리면 경고를 빠르게 생성하지 않아 유용하게 사용할 수 없습니다.

장기 데이터 손실 전에 마지막 데이터 지점에서 조건이 위반된다는 것을 알리는 30분 창이 있는 모니터를 사용하는 경우 Monitor에서 메트릭 복구를 확인하는 데 사용할 다른 정보를 받지 않았거나 조건이 지속되었음을 알 수 있기 때문에 경고가 생성됩니다.

## "영구 활성화" 경고

모니터링된 개체에 \* 항상 \* 이 존재하도록(예: IOPS > 1 또는 지연 시간 > 0) 모니터를 구성할 수 있습니다. 이러한 모니터는 종종 '테스트' 모니터로 생성된 후 잊어버리는 경우가 많습니다. 이러한 모니터는 구성 객체에 대해 영구적으로 열려 있는 알림을 생성하는데, 이로 인해 시간이 지남에 따라 시스템 스트레스 및 안정성 문제가 발생할 수 있습니다.

이를 방지하기 위해 Data Infrastructure Insights는 7일 후에 모든 "영구 활성화" 경고를 자동으로 닫습니다. 기본 모니터 조건이 계속 존재할 수 있으므로 거의 즉시 새 경고가 발행될 수 있지만 "항상 활성화" 경고가 닫히면 발생할 수 있는 시스템 스트레스가 완화됩니다.

## 이메일 알림 구성

구독 관련 알림에 대한 전자 메일 목록과 성능 정책 임계값 위반 알림을 위한 받는 사람의 글로벌 전자 메일 목록을 구성할 수 있습니다.

알림 이메일 수신자 설정을 구성하려면 \* 관리자 > 알림 \* 페이지로 이동하여 \_Email\_ 탭을 선택하십시오.

### Subscription Notification Recipients

Send subscription related notifications to the following:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

name@email.com ✕

Save

### Global Monitor Notification Recipients

Default email recipients for monitor related notifications:

- All Account Owners
- All Monitor & Optimize Administrators
- Additional Email Addresses

Save

## 구독 알림 수신자

구독 관련 이벤트 알림을 받는 사람을 구성하려면 "구독 알림 받는 사람" 섹션으로 이동하십시오. 구독 관련 이벤트에 대해 다음 수신자 중 일부 또는 전체에 이메일 알림을 보내도록 선택할 수 있습니다.

- 모든 계정 소유자
- All\_Monitor 및 Optimize\_Administrators
- 사용자가 지정하는 추가 전자 메일 주소입니다

다음은 보낼 수 있는 알림 유형과 사용자가 수행할 수 있는 사용자 작업의 예입니다.

* 알림: *	* 사용자 조치: *
평가판 또는 구독이 업데이트되었습니다	에서 구독 세부 정보를 검토합니다 "구독" 페이지
구독은 90일 후에 만료됩니다. 구독은 30일 후에 만료됩니다	"자동 갱신"이 활성화된 경우 작업이 필요하지 않습니다 "NetApp 영업" 구독을 갱신하려면

평가판은 2일 후에 종료됩니다	에서 평가판을 갱신합니다 "구독" 페이지. 평가판을 한 번 갱신할 수 있습니다. 연락처 "NetApp 영업" 를 클릭하여 구독을 구매합니다
평가판 또는 구독이 만료되었습니다. 48시간 이내에 계정 데이터 수집이 중지됩니다. 48시간 후에는 계정이 삭제됩니다	연락처 "NetApp 영업" 를 클릭하여 구독을 구매합니다

### 경고를 위한 글로벌 수신자 목록

알림의 전자 메일 알림은 알림의 모든 작업에 대해 알림 받는 사람 목록으로 전송됩니다. 글로벌 수신자 목록에 알림 메시지를 보내도록 선택할 수 있습니다.

글로벌 경고 수신자를 구성하려면 \* Global Monitor Notification Recipients \* 섹션에서 원하는 수신자를 선택합니다.

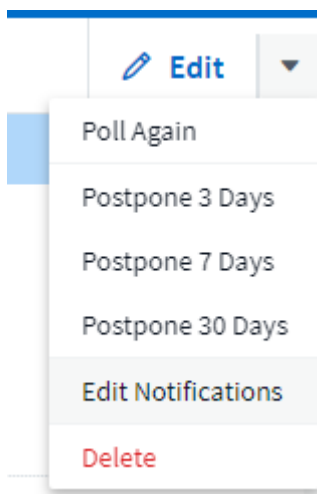
모니터를 만들거나 수정할 때 항상 개별 모니터의 전체 수신자 목록을 재정의할 수 있습니다.



ONTAP 데이터 수집기 알림은 클러스터/데이터 수집기와 관련된 특정 모니터 알림보다 우선합니다. Data Collector 자체에 대해 설정한 받는 사람 목록에는 데이터 수집기 경고가 표시됩니다. 활성 데이터 수집기 경고가 없는 경우 모니터에서 생성된 알림이 특정 모니터 수신자에게 전송됩니다.

### ONTAP 알림 편집

스토리지 랜딩 페이지의 오른쪽 위 드롭다운에서 \_알림 편집\_을 선택하여 ONTAP 클러스터에 대한 알림을 수정할 수 있습니다.



여기에서 위험, 경고, 정보 및/또는 해결된 경고에 대한 알림을 설정할 수 있습니다. 각 시나리오는 선택한 글로벌 수신자 목록 또는 다른 수신자에게 알릴 수 있습니다.



By Email

Notify team on

Critical, Warn... ▾

Send to

- Global Monitor Recipient List
- Other Email Recipients

email@email.one X

email2@email2.two X |

Notify team on

Resolved ▾

Send to

- Global Monitor Recipient List
- Other Email Recipients

By Webhook

Enable webhook notification to add recipients

## 시스템 모니터

Data Infrastructure Insights에는 메트릭 및 로그 모두에 대해 다수의 시스템 정의 모니터가 포함되어 있습니다. 사용 가능한 시스템 모니터는 사용자 환경에 있는 데이터 수집기에 따라 다릅니다. 따라서 데이터 수집기가 추가되거나 구성이 변경되면 Data Infrastructure Insights에서 사용할 수 있는 모니터가 변경될 수 있습니다.



대부분의 시스템 모니터는 기본적으로 *Paused* 상태입니다. 모니터의 *\_Resume\_* 옵션을 선택하여 시스템 모니터를 활성화할 수 있습니다. *Data Collector*에서 *\_고급 카운터 데이터 수집 및 ONTAP EMS 로그 수집 활성화\_*가 활성화되어 있는지 확인합니다. 이러한 옵션은 *\_고급 구성\_* 아래의 ONTAP

Enable ONTAP EMS log collection

데이터 수집기에서 찾을 수 있습니다.  Opt in for Advanced Counter Data Collection rollout.

## 모니터 설명

시스템 정의 모니터는 사전 정의된 메트릭 및 조건과 기본 설명 및 수정 작업으로 구성되어 있으며 수정할 수 없습니다. 시스템 정의 모니터의 알림 수신자 목록을 수정할 수 있습니다. 메트릭, 조건, 설명 및 수정 조치를 보거나 수신자 목록을 수정하려면 시스템 정의 모니터 그룹을 열고 목록에서 모니터 이름을 클릭합니다.

시스템 정의 모니터 그룹은 수정하거나 제거할 수 없습니다.

다음 시스템 정의 모니터를 표시된 그룹에서 사용할 수 있습니다.

- \* ONTAP 인프라 \* 에는 ONTAP 클러스터의 인프라 관련 문제에 대한 모니터가 포함됩니다.
- \* ONTAP 워크로드 예시 \* 에는 워크로드 관련 문제에 대한 모니터가 포함됩니다.
- 두 그룹의 모니터는 기본적으로 `_Paused_state`입니다.

다음은 현재 Data Infrastructure Insights에 포함된 시스템 모니터입니다.

## 메트릭 모니터

모니터 이름	심각도입니다	모니터 설명	수정 조치
Fibre Channel 포트 사용률 높음	심각	Fibre Channel 프로토콜 포트는 고객 호스트 시스템과 ONTAP LUN 간의 SAN 트래픽을 수신하고 전송하는 데 사용됩니다. 포트 사용률이 높을 경우 그러면 병목 현상이 발생하고 궁극적으로 Fibre Channel 프로토콜 워크로드의 성능에 영향을 줍니다. 경고 알림은 네트워크 트래픽의 균형을 맞추기 위해 계획된 조치를 취해야 함을 나타냅니다. 심각한 경고는 서비스 중단이 임박했음을 나타내며 네트워크 균형을 맞추기 위해 긴급 조치를 취해야 함을 나타냅니다 서비스 연속성을 보장하기 위한 트래픽.	중요 임계값이 위반되면 즉각적인 조치를 고려하여 서비스 중단을 최소화하십시오. 1. 사용률이 낮은 다른 FCP 포트에 워크로드 이동 특정 LUN의 트래픽은 ONTAP의 QoS 정책 또는 호스트 측 구성을 통해 필수 작업으로만 제한하면 FCP 포트의 사용률을 가볍게 할 수 있습니다. 경고 임계값이 위반될 경우 다음 조치를 취하십시오. 1. 포트 활용률이 더 많은 포트에 분산되도록 데이터 트래픽을 처리하도록 더 많은 FCP 포트를 구성합니다. 사용률이 낮은 다른 FCP 포트에 워크로드 이동 특정 LUN의 트래픽은 ONTAP의 QoS 정책 또는 호스트 측 구성을 통해 필수 작업으로만 제한하면 FCP 포트의 사용률을 가볍게 할 수 있습니다.

LUN 지연 시간 높음	심각	<p>LUN은 데이터베이스와 같이 성능에 민감한 애플리케이션에서 주로 발생하는 I/O 트래픽을 처리하는 객체입니다. LUN 지연 시간이 높으면 애플리케이션 자체가 어려움을 겪을 수 있고 작업을 수행할 수 없게 됩니다. 경고 알림은 LUN을 적절한 노드 또는 Aggregate로 이동하기 위해 계획된 작업을 수행해야 함을 나타냅니다. 심각한 알림은 서비스 중단이 임박했음을 나타내며 긴급 조치를 취해야 함을 나타냅니다 서비스 연속성을 보장합니다. 다음은 미디어 유형 SSD에서 최대 1-2밀리초, SAS에서 최대 8-10밀리초, SATA HDD에서 17-20밀리초에 기반한 예상 지연 시간입니다</p>	<p>중요 임계값이 위반되면 다음 작업을 수행하여 서비스 중단을 최소화할 수 있습니다. LUN 또는 해당 볼륨에 QoS 정책이 연결되어 있는 경우 임계값 제한을 평가하고 LUN 워크로드가 조절되고 있는지 확인하십시오. 경고 임계값이 위반될 경우 다음 조치를 취하십시오. 1. 애그리게이트에도 높은 사용률이 발생하는 경우 LUN을 다른 애그리게이트로 이동합니다. 2.노드 사용률이 높은 경우 볼륨을 다른 노드로 이동하거나 노드의 총 워크로드를 줄입니다. 3.LUN 또는 해당 볼륨에 연결된 QoS 정책이 있는 경우 임계값 제한을 평가하고 LUN 워크로드가 조절되는 원인이 되는지 확인합니다.</p>
네트워크 포트 사용률 높음	심각	<p>네트워크 포트는 고객 호스트 시스템과 ONTAP 볼륨 간에 NFS, CIFS 및 iSCSI 프로토콜 트래픽을 수신하고 전송하는 데 사용됩니다. 포트 활용률이 높은 경우 병목 현상이 발생하고 궁극적으로 NFS 성능과 CIFS 및 iSCSI 워크로드... 경고 알림은 네트워크 트래픽의 균형을 맞추기 위해 계획된 조치를 취해야 함을 나타냅니다.... 긴급 경고는 서비스 중단이 임박했음을 나타내며, 서비스 연속성을 보장하기 위해 네트워크 트래픽의 균형을 맞추기 위해 긴급 조치를 취해야 함을 나타냅니다.</p>	<p>중요 임계값이 위반되면 다음과 같은 즉각적인 조치를 수행하여 서비스 중단을 최소화하십시오. 1. ONTAP의 QoS 정책 또는 호스트 측 분석을 통해 네트워크 포트 활용률을 감소시키고 특정 볼륨의 트래픽을 필수 작업으로만 제한합니다. 사용률이 낮은 다른 네트워크 포트를 사용하도록 하나 이상의 볼륨을 구성합니다. 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 고려하십시오. 1. 포트 사용률이 더 많은 포트에 분산되도록 데이터 트래픽을 처리할 네트워크 포트를 더 많이 구성합니다. 사용률이 낮은 다른 네트워크 포트를 사용하도록 하나 이상의 볼륨을 구성합니다.</p>

<p>NVMe 네임스페이스 지연 시간 높음</p>	<p>심각</p>	<p>NVMe 네임스페이스는 데이터베이스와 같이 성능에 민감한 응용 프로그램에 의해 구동되는 I/O 트래픽을 제공하는 개체입니다. NVMe 네임스페이스 대기 시간이 길다는 것은 응용 프로그램 자체가 어려움을 겪을 수 있고 작업을 수행할 수 없음을 의미합니다. 경고 알림은 LUN을 적절한 노드 또는 Aggregate로 이동하기 위해 계획된 작업을 수행해야 함을 나타냅니다. 심각한 알림은 서비스 중단이 임박했음을 나타내며 긴급 조치를 취해야 함을 나타냅니다 서비스 연속성을 보장합니다.</p>	<p>중요 임계값이 위반되면 즉시 조치를 수행하여 서비스 중단을 최소화하십시오. NVMe 네임스페이스 또는 해당 볼륨에 QoS 정책이 할당된 경우 NVMe 네임스페이스 워크로드의 제한이 유발되는 경우 제한 임계값을 평가해 보십시오. 경고 임계값이 위반되면 다음 조치를 취하십시오. 1. 애그리게이트에도 높은 사용률이 발생하는 경우 LUN을 다른 애그리게이트로 이동합니다. 2.노드 사용률이 높은 경우 볼륨을 다른 노드로 이동하거나 노드의 총 워크로드를 줄입니다. NVMe 네임스페이스 또는 해당 볼륨에 QoS 정책이 할당된 경우 NVMe 네임스페이스 워크로드가 제한되지 않도록 제한 임계값을 평가합니다.</p>
<p>Qtree 용량 팍 참</p>	<p>심각</p>	<p>qtree는 논리적으로 정의된 파일 시스템으로, 볼륨 내의 루트 디렉토리에 있는 특수 하위 디렉토리로 존재할 수 있습니다. 각 qtree에는 볼륨 용량 내에 트리에 저장되는 데이터의 양을 제한하는 할당량 정책이 정의된 기본 공간 할당량 또는 할당량이 있습니다.... 경고 알림은 공간을 늘리기 위해 계획된 작업을 수행해야 함을 나타냅니다.... 긴급 알림은 서비스 중단이 임박했음을 나타냅니다 서비스 연속성을 보장하기 위해 여유 공간을 확보하기 위해 비상 조치를 취해야 합니다.</p>	<p>중요 임계값이 위반되면 즉각적인 조치를 고려하여 서비스 중단을 최소화하십시오. 1. 성장을 수용할 수 있도록 qtree의 공간을 늘리십시오. 2. 불필요한 데이터를 삭제하여 공간을 확보하십시오. 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 취하십시오. 1. 성장을 수용할 수 있도록 qtree의 공간을 늘리십시오. 필요 없는 데이터를 삭제하여 공간을 확보하십시오.</p>



Qtreet 용량 하드 제한입니다	심각	<p>qtree는 논리적으로 정의된 파일 시스템으로, 볼륨 내의 루트 디렉토리에 있는 특수 하위 디렉토리로 존재할 수 있습니다. 각 qtree에는 볼륨의 사용자 데이터 증가를 제어하고 총 용량을 초과하지 않도록 데이터를 저장하는 데 사용되는 공간 할당량이 KBytes 단위로 측정됩니다.... qtree는 소프트웨어 스토리지 용량 할당량을 유지하여 사용자에게 전체 용량에 도달하기 전에 미리 경고를 제공합니다 qtree의 용량 할당량 제한이며 더 이상 데이터를 저장할 수 없습니다. Qtreet에 저장된 데이터의 양을 모니터링하면 사용자가 무중단 데이터 서비스를 받을 수 있습니다.</p>	<p>중요 임계값이 위반되면 다음과 같은 즉각적인 조치를 수행하여 서비스 중단을 최소화하십시오. 1. 증가량을 수용하기 위해 트리 공간 할당량을 늘립니다. 2. 사용자에게 트리에서 불필요한 데이터를 삭제하여 공간을 확보하도록 지시합니다</p>
Qtreet 용량 소프트웨어 제한값	경고	<p>qtree는 논리적으로 정의된 파일 시스템으로, 볼륨 내의 루트 디렉토리에 있는 특수 하위 디렉토리로 존재할 수 있습니다. 각 qtree에는 볼륨의 사용자 데이터 증가를 제어하고 총 용량을 초과하지 않도록 데이터를 저장하는 데 사용할 수 있는 공간 할당량이 KBytes 단위로 측정되었습니다.... qtree는 에 도달하기 전에 사용자에게 사전 경고를 제공하는 소프트웨어 스토리지 용량 할당량을 유지합니다 qtree의 총 용량 할당량 제한이며 더 이상 데이터를 저장할 수 없습니다. Qtreet에 저장된 데이터의 양을 모니터링하면 사용자가 무중단 데이터 서비스를 받을 수 있습니다.</p>	<p>경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 고려하십시오. 1. 성장에 맞게 트리 공간 할당량을 늘립니다. 2.트리에서 불필요한 데이터를 삭제하여 공간을 확보하도록 사용자에게 지시합니다.</p>

Qtree 파일 하드 제한입니다	심각	<p>qtree는 논리적으로 정의된 파일 시스템으로, 볼륨 내의 루트 디렉토리에 있는 특수 하위 디렉토리로 존재할 수 있습니다. 각 qtree에는 볼륨 내에서 관리 가능한 파일 시스템 크기를 유지하기 위해 포함할 수 있는 파일 수의 할당량이 있습니다....</p> <p>qtree는 트리에 있는 새 파일이 거부되는 한도를 초과하여 하드 파일 번호 할당량을 유지합니다. Qtree 내에서 파일 수를 모니터링하면 사용자가 무중단 데이터 서비스를 받을 수 있습니다.</p>	<p>중요 임계값이 위반되면 즉각적인 조치를 고려하여 서비스 중단을 최소화하십시오. 1. qtree의 파일 수 할당량을 늘립니다. qtree 파일 시스템에서 필요 없는 파일을 삭제합니다.</p>
Qtree 파일 소프트 제한값	경고	<p>qtree는 논리적으로 정의된 파일 시스템으로, 볼륨 내의 루트 디렉토리에 있는 특수 하위 디렉토리로 존재할 수 있습니다. 각 qtree에는 볼륨 내에서 관리할 수 있는 파일 시스템 크기를 유지하기 위해 포함할 수 있는 파일 수의 할당량이 있습니다....</p> <p>qtree는 사용자에게 경고를 보내기 위해 소프트 파일 번호 할당량을 유지하므로, qtree 및 의 파일 제한에 도달하기 전에 미리 경고를 제공합니다 추가 파일을 저장할 수 없습니다. Qtree 내에서 파일 수를 모니터링하면 사용자가 무중단 데이터 서비스를 받을 수 있습니다.</p>	<p>경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 취하십시오. 1. qtree의 파일 수 할당량을 늘립니다. qtree 파일 시스템에서 필요 없는 파일을 삭제합니다.</p>

<p>스냅샷 예비 공간이 가득 찼습니다</p>	<p>심각</p>	<p>애플리케이션 및 고객 데이터를 저장하려면 볼륨의 스토리지 용량이 필요합니다. 스냅샷 예약 공간이라고 하는 이 공간의 일부는 데이터를 로컬로 보호할 수 있는 스냅샷을 저장하는 데 사용됩니다. ONTAP 볼륨에 새로 저장되거나 업데이트된 데이터가 많을수록 더 많은 스냅샷 용량이 사용되며 향후 새 데이터 또는 업데이트된 데이터에 더 적은 스냅샷 스토리지 용량을 사용할 수 있습니다. 볼륨 내의 스냅샷 데이터 용량이 전체 스냅샷 예비 공간에 도달하면 고객이 새 스냅샷 데이터를 저장할 수 없게 되고 볼륨의 데이터에 대한 보호 수준이 감소할 수 있습니다. 사용된 볼륨 스냅샷 용량을 모니터링하면 데이터 서비스의 연속성이 보장됩니다.</p>	<p>중요 임계값이 위반되면 즉각적인 조치를 고려하여 서비스 중단을 최소화하십시오. 1. 스냅샷 예비 공간이 가득 찼을 때 볼륨의 데이터 공간을 사용하도록 스냅샷을 구성합니다. 2. 불필요한 일부 오래된 스냅샷을 삭제하여 공간을 확보하십시오. 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 취하십시오. 1. 증가량을 수용하기 위해 볼륨 내에서 스냅샷 예비 공간을 늘립니다. 스냅샷 예비 공간이 가득 찼을 때 볼륨의 데이터 공간을 사용하도록 스냅샷을 구성합니다.</p>
<p>스토리지 용량 제한</p>	<p>심각</p>	<p>스토리지 풀(애그리게이트)이 가득 차는 경우 I/O 작업의 속도가 느려지고 결국 중지되어 스토리지 운영 중단이 발생합니다. 경고 알림은 최소 여유 공간을 복원하기 위해 계획된 작업을 곧 수행해야 함을 나타냅니다. 긴급 경고는 서비스 중단이 임박했음을 나타내며, 서비스 연속성을 보장하기 위해 공간을 확보하기 위해 긴급 조치를 취해야 합니다.</p>	<p>중요 임계값이 위반되면 즉시 다음 작업을 고려하여 서비스 중단을 최소화합니다. 1. 중요하지 않은 볼륨에서 스냅샷을 삭제합니다. 중요하지 않은 워크로드이고 스토리지 복제본에서 복구할 수 있는 볼륨 또는 LUN을 삭제합니다.... 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 계획하십시오. 1. 하나 이상의 볼륨을 다른 스토리지 위치로 이동합니다. 스토리지 용량을 추가합니다. 3. 스토리지 효율성 설정을 변경하거나 비활성 데이터를 클라우드 스토리지로 계층화합니다.</p>

스토리지 성능 제한	심각	<p>스토리지 시스템의 성능 제한이 도달하면 작업이 느려지고 지연 시간이 초과되며 워크로드 및 애플리케이션이 장애를 시작할 수 있습니다. ONTAP는 작업 부하에 대한 스토리지 풀 사용률을 평가하고 사용된 성능 비율을 예측합니다.... 경고 알림은 스토리지 풀 로드를 줄이기 위해 계획된 작업을 수행해야 하며, 이를 통해 스토리지 풀 성능을 충분히 유지할 수 있도록 보장합니다. 심각한 알림은 이를 나타냅니다 서비스 연속성을 보장하기 위해 스토리지 풀 로드를 줄이기 위해 성능 저하가 임박하고 긴급 조치를 취해야 합니다.</p>	<p>중요 임계값이 위반되면 다음과 같은 즉각적인 조치를 수행하여 서비스 중단을 최소화하십시오. 1. 스냅샷 또는 SnapMirror 복제와 같은 예약된 작업을 일시 중단합니다. 2.유휴 비필수 워크로드... 경고 임계값이 위반되면 즉시 다음 조치를 취하십시오. 1. 하나 이상의 워크로드를 다른 스토리지 위치로 이동합니다. AFF(스토리지 노드) 또는 FAS(디스크 셸프)를 더 추가하고 워크로드를 재배 포함합니다. 3. 워크로드 특성 변경(블록 크기, 애플리케이션 캐싱)</p>
사용자 할당량 용량 하드 제한입니다	심각	<p>ONTAP는 볼륨 내의 볼륨, 파일 또는 디렉토리에 액세스할 권한이 있는 Unix 또는 Windows 시스템의 사용자를 인식합니다. 결과적으로 ONTAP를 통해 고객은 Linux 또는 Windows 시스템의 사용자 또는 사용자 그룹에 대한 스토리지 용량을 구성할 수 있습니다. 사용자 또는 그룹 정책 할당량은 사용자가 자신의 데이터에 사용할 수 있는 공간의 양을 제한합니다. 이 할당량의 하드 제한에서는 볼륨 내에서 사용되는 용량이 전체 용량 할당량에 도달하기 전에 사용자에게 통지할 수 있습니다. 사용자 또는 그룹 할당량 내에 저장된 데이터의 양을 모니터링하면 사용자가 중단 없는 데이터 서비스를 받을 수 있습니다.</p>	<p>중요 임계값이 위반되면 다음과 같은 즉각적인 조치를 수행하여 서비스 중단을 최소화하십시오. 1. 확장을 수용하기 위해 사용자 또는 그룹 할당량의 공간을 늘립니다. 사용자 또는 그룹에 원치 않는 데이터를 삭제하여 공간을 확보하도록 지시합니다.</p>

<p>사용자 할당량 용량 소프트웨어 제한입니다</p>	<p>경고</p>	<p>ONTAP은 볼륨 내의 볼륨, 파일 또는 디렉토리에 액세스할 권한이 있는 Unix 또는 Windows 시스템의 사용자를 인식합니다. 결과적으로 ONTAP를 통해 고객은 Linux 또는 Windows 시스템의 사용자 또는 사용자 그룹에 대한 스토리지 용량을 구성할 수 있습니다. 사용자 또는 그룹 정책 할당량은 사용자가 자신의 데이터에 사용할 수 있는 공간의 양을 제한합니다. 이 할당량의 소프트웨어 제한값을 사용하면 볼륨 내에서 사용되는 용량이 총 용량 할당량에 도달할 때 사용자에게 사전 알림을 보낼 수 있습니다. 사용자 또는 그룹 할당량 내에 저장된 데이터의 양을 모니터링하면 사용자가 중단 없는 데이터 서비스를 받을 수 있습니다.</p>	<p>경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 취하십시오. 1. 확장을 수용하기 위해 사용자 또는 그룹 할당량의 공간을 늘립니다. 필요 없는 데이터를 삭제하여 공간을 확보하십시오.</p>
<p>볼륨 용량이 가득 찼습니다</p>	<p>심각</p>	<p>애플리케이션 및 고객 데이터를 저장하려면 볼륨의 스토리지 용량이 필요합니다. ONTAP 볼륨에 더 많은 데이터를 저장할수록 이후 데이터에 대한 스토리지 가용성이 줄어듭니다. 볼륨 내의 데이터 스토리지 용량이 총 스토리지 용량에 도달하면 스토리지 용량 부족으로 인해 고객이 데이터를 저장할 수 없게 될 수 있습니다. 사용된 볼륨 스토리지 용량을 모니터링하면 데이터 서비스의 연속성이 보장됩니다.</p>	<p>중요 임계값이 위반되면 다음과 같은 즉각적인 조치를 수행하여 서비스 중단을 최소화하십시오. 1. 성장에 맞춰 볼륨 공간을 늘리십시오. 필요 없는 데이터를 삭제하여 공간을 확보하십시오. 스냅샷 복사본이 스냅샷 예비 공간보다 더 많은 공간을 차지하는 경우 이전 스냅샷을 삭제하거나 볼륨 스냅샷 자동 삭제를 활성화합니다.... 경고 임계값이 위반되면 다음과 같은 즉시 조치를 취하십시오. 1. 증가량을 수용하기 위해 볼륨의 공간을 늘립니다. 2. 스냅샷 복사본이 스냅샷 예비 공간보다 더 많은 공간을 차지하는 경우, 이전 스냅샷을 삭제하거나 볼륨 스냅샷 자동 삭제를 활성화합니다....</p>

볼륨 inode 제한	심각	<p>파일을 저장하는 볼륨은 인덱스 노드(inode)를 사용하여 파일 메타데이터를 저장합니다. 볼륨이 inode 할당을 소진할 때 더 이상 파일을 추가할 수 없습니다.... 경고 알림은 사용 가능한 inode 수를 늘리기 위해 계획된 작업을 수행해야 함을 나타냅니다.... 긴급 경고는 파일 제한 고갈이 임박했음을 나타내며, 서비스 연속성을 보장하기 위해 inode를 확보하기 위해 긴급 조치를 취해야 함을 나타냅니다.</p>	<p>중요 임계값이 위반되면 다음과 같은 즉각적인 조치를 수행하여 서비스 중단을 최소화하십시오. 1. 볼륨에 대한 inode 값을 늘립니다. inode 값이 이미 최대값에 있는 경우 파일 시스템이 최대 크기를 초과하여 확장되었기 때문에 볼륨을 두 개 이상의 볼륨으로 분할합니다. 2.FlexGroup를 사용하면 대용량 파일 시스템을 쉽게 수용할 수 있습니다. 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 취하십시오. 1. 볼륨에 대한 inode 값을 늘립니다. inode 값이 이미 최대값에 있는 경우 파일 시스템이 최대 크기를 초과하여 확장되었기 때문에 볼륨을 두 개 이상의 볼륨으로 분할합니다. FlexGroup를 사용하면 대용량 파일 시스템을 쉽게 수용할 수 있습니다</p>
볼륨 지연 시간 높음	심각	<p>볼륨은 DevOps 애플리케이션, 홈 디렉토리, 데이터베이스를 비롯한 성능에 민감한 애플리케이션에서 주로 발생하는 I/O 트래픽을 처리하는 객체입니다. 볼륨 지연 시간이 길다는 것은 애플리케이션 자체에서 문제를 겪고 있으며 작업을 수행할 수 없음을 의미합니다. 볼륨 지연 시간을 모니터링하는 것은 애플리케이션의 일관된 성능을 유지하는 데 매우 중요합니다. 다음은 미디어 유형-SSD에서 최대 1-2밀리초, SAS에서 최대 8-10밀리초, SATA HDD에서 17-20밀리초를 기준으로 한 예상 지연 시간입니다.</p>	<p>중요 임계값이 위반되면 다음과 같은 즉각적인 조치를 수행하여 서비스 중단을 최소화할 수 있습니다. 볼륨에 QoS 정책이 할당된 경우 볼륨 워크로드의 임계치가 조절되는 경우를 대비하여 제한 임계값을 평가합니다. 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 고려하십시오. 1. 애그리게이트에도 높은 사용률이 발생하는 경우 볼륨을 다른 애그리게이트로 이동합니다. 볼륨에 QoS 정책이 할당된 경우 볼륨 워크로드의 제한이 발생하는 경우 해당 제한 임계값을 평가합니다. 3.노드 사용률도 높을 경우 볼륨을 다른 노드로 이동하거나 노드의 총 워크로드를 줄입니다.</p>
모니터 이름	심각도입니다	모니터 설명	수정 조치

<p>노드 높은 지연 시간</p>	<p>경고/위험</p>	<p>노드 지연 시간이 노드의 애플리케이션 성능에 영향을 줄 수 있는 수준에 도달했습니다. 노드 지연 시간이 짧아 애플리케이션의 일관된 성능을 보장할 수 있습니다. 미디어 유형에 따른 예상 지연 시간은 SSD 최대 1-2밀리초, SAS 최대 8-10밀리초, SATA HDD 17-20 밀리초입니다.</p>	<p>중요 임계값이 위반되면 서비스 중단을 최소화하기 위해 즉각적인 조치를 취해야 합니다. 1. 예약된 작업, 스냅샷 또는 SnapMirror 복제를 일시 중지합니다. 2. QoS 제한을 통해 낮은 우선 순위 워크로드의 요구 감소 3. 중요하지 않은 워크로드를 비활성화할 경우 경고 임계값이 위반될 때 즉시 조치를 고려합니다. 1. 하나 이상의 워크로드를 다른 스토리지 위치로 이동 2. QoS 제한을 통해 낮은 우선 순위 워크로드의 요구 감소 3. 스토리지 노드(AFF) 또는 디스크 헬프(FAS) 추가 및 워크로드 재배포 4. 워크로드 특성 변경(블록 크기, 애플리케이션 캐싱 등)</p>
<p>노드 성능 제한</p>	<p>경고/위험</p>	<p>노드 성능 활용률은 입출력 및 노드에서 지원하는 애플리케이션의 성능에 영향을 줄 수 있는 수준에 도달했습니다. 낮은 노드 성능 활용으로 애플리케이션의 일관된 성능을 보장합니다.</p>	<p>중요 임계값이 위반될 경우 서비스 중단을 최소화하기 위해 즉각적인 조치를 취해야 합니다. 1. 예약된 작업, 스냅샷 또는 SnapMirror 복제를 일시 중지합니다. 2. QoS 제한을 통해 낮은 우선 순위 워크로드의 요구 감소 3. 중요하지 않은 워크로드를 사용하지 않는 경우 경고 임계값이 위반될 경우 다음 작업을 고려하십시오. 1. 하나 이상의 워크로드를 다른 스토리지 위치로 이동 2. QoS 제한을 통해 낮은 우선 순위 워크로드의 요구 감소 3. 스토리지 노드(AFF) 또는 디스크 헬프(FAS) 추가 및 워크로드 재배포 4. 워크로드 특성 변경(블록 크기, 애플리케이션 캐싱 등)</p>

<p>스토리지 VM 높은 지연 시간</p>	<p>경고/위험</p>	<p>스토리지 VM(SVM)의 지연 시간이 스토리지 VM의 애플리케이션 성능에 영향을 줄 수 있는 수준에 도달했습니다. 스토리지 VM 지연 시간이 짧아 애플리케이션의 일관된 성능이 보장됩니다. 미디어 유형에 따른 예상 지연 시간은 SSD 최대 1-2 밀리초, SAS 최대 8-10밀리초, SATA HDD 17-20 밀리초입니다.</p>	<p>중요 임계값이 위반되면 QoS 정책이 할당된 스토리지 VM의 볼륨에 대한 임계값 제한을 즉시 평가하여 볼륨 워크로드가 조절되는지 확인합니다. 경고 임계값이 위반되면 즉시 다음 작업을 고려하십시오. 1. 애그리게이트에도 높은 사용률이 발생하는 경우 스토리지 VM의 일부 볼륨을 다른 애그리게이트로 이동합니다. QoS 정책이 할당된 스토리지 VM의 볼륨에 대해 볼륨 워크로드가 조절되는 경우 임계값 제한을 평가합니다 3. 노드에 높은 사용률이 발생한 경우 스토리지 VM의 일부 볼륨을 다른 노드로 이동하거나 노드의 총 워크로드를 줄입니다</p>
<p>사용자 할당량 파일 하드 제한입니다</p>	<p>심각</p>	<p>볼륨 내에서 생성된 파일 수가 중요 한도에 도달했으며 추가 파일을 생성할 수 없습니다. 저장된 파일 수를 모니터링하면 사용자가 중단 없는 데이터 서비스를 받을 수 있습니다.</p>	<p>중요 임계값이 위반될 경우 서비스 중단을 최소화하기 위해 즉각적인 조치가 필요합니다. 다음 조치를 고려하십시오. 1. 특정 사용자에게 파일 개수 할당량을 늘립니다. 2. 필요 없는 파일을 삭제하여 특정 사용자의 파일 할당량에 대한 부담을 줄입니다</p>
<p>사용자 할당량 파일 소프트 제한입니다</p>	<p>경고</p>	<p>볼륨 내에서 생성된 파일 수가 할당량의 임계값 제한에 도달했으며 심각한 한도에 근접했습니다. 할당량이 위험 제한에 도달하면 추가 파일을 생성할 수 없습니다. 사용자가 저장한 파일 수를 모니터링하면 사용자가 중단 없는 데이터 서비스를 받을 수 있습니다.</p>	<p>경고 임계값이 위반될 경우 즉시 조치를 고려하십시오. 1. 특정 사용자 할당량에 대한 파일 개수 할당량을 늘립니다. 2. 필요 없는 파일을 삭제하여 특정 사용자의 파일 할당량에 대한 부담을 줄입니다</p>



볼륨 캐시 비적중 비율입니다	경고/위험	볼륨 캐시 비적중 비율은 캐시에서 반환되지 않고 디스크에서 반환된 클라이언트 애플리케이션의 읽기 요청 비율입니다. 즉, 볼륨이 설정된 임계값에 도달했음을 의미합니다.	중요 임계값이 위반되면 서비스 중단을 최소화하기 위해 즉각적인 조치를 취해야 합니다. 1. 일부 워크로드를 볼륨 노드에서 이동하여 IO 로드를 줄입니다 2. 아직 볼륨 노드에 있지 않은 경우 Flash Cache 3을 구매하여 추가하여 WAFL 캐시를 높입니다. QoS 제한을 통해 동일한 노드에서 낮은 우선 순위 워크로드의 요구를 줄입니다. 경고 임계값이 위반될 때 즉시 조치를 고려하십시오. 1. 일부 워크로드를 볼륨 노드에서 이동하여 IO 로드를 줄입니다 2. 아직 볼륨 노드에 있지 않은 경우 Flash Cache 3을 구매하여 추가하여 WAFL 캐시를 높입니다. QoS 제한을 통해 동일한 노드에서 낮은 우선 순위 워크로드의 요구를 줄입니다 4. 워크로드 특성 변경(블록 크기, 애플리케이션 캐싱 등)
볼륨 Qtree 할당량 오버커밋	경고/위험	볼륨 Qtree 할당량 오버커밋은 qtree 할당량에 의해 볼륨이 초과 커밋된 것으로 간주되는 비율을 지정합니다. 볼륨에 대해 qtree 할당량의 설정 임계값에 도달했습니다. 볼륨 qtree 할당량 초과 할당을 모니터링하면 사용자가 무중단 데이터 서비스를 받을 수 있습니다.	중요 임계값이 위반되면 서비스 중단을 최소화하기 위해 즉각적인 조치를 취해야 합니다. 1. 볼륨 2 의 공간을 늘립니다. 경고 임계값이 위반되면 원치 않는 데이터를 삭제한 다음 볼륨 공간을 늘리는 것이 좋습니다.

## 맨 위로

### 로그 모니터

모니터 이름	심각도입니다	설명	수정 조치
--------	--------	----	-------

AWS 자격 증명이 초기화되지 않았습니다	정보	이 이벤트는 모듈이 초기화되기 전에 클라우드 자격 증명 스템드에서 AWS(Amazon Web Services) IAM(Identity and Access Management) 역할 기반 자격 증명에 액세스하려고 할 때 발생합니다.	시스템뿐만 아니라 클라우드 자격 증명 스템드가 초기화를 완료할 때까지 기다립니다.
클라우드 계층에 연결할 수 없습니다	심각	스토리지 노드가 클라우드 계층 오브젝트 저장소 API에 연결할 수 없습니다. 일부 데이터에 액세스할 수 없습니다.	온프레미스 제품을 사용하는 경우 다음 수정 조치를 수행하십시오. ... "network interface show" 명령을 사용하여 인터클러스터 NIF가 온라인이고 작동하는지 확인합니다. ... 대상 노드 인터클러스터 NIF에 대해 "ping" 명령을 사용하여 오브젝트 저장소 서버에 대한 네트워크 연결을 확인합니다. ... 다음 사항을 확인합니다. ... 개체 저장소의 구성이 변경되지 않았는지 확인합니다. ... 로그인 및 연결 정보는 여전히 유효합니다.... 문제가 지속되면 NetApp 기술 지원 팀에 문의하십시오. Cloud Volumes ONTAP를 사용하는 경우 다음과 같은 수정 조치를 수행하십시오. ... 오브젝트 저장소 구성이 변경되지 않았는지 확인합니다. 로그인 및 연결 정보가 여전히 유효한지 확인하십시오. 문제가 지속되면 NetApp 기술 지원 팀에 문의하십시오.
디스크 사용 중단	정보	이 이벤트는 디스크에 장애가 발생했거나, 제거 중이거나, 유지보수 센터에 진입했기 때문에 디스크가 서비스에서 제거된 경우에 발생합니다.	없음.

FlexGroup 구성 요소 팍 참	심각	FlexGroup 볼륨 내의 구성요소가 가득 차면 서비스가 중단될 수 있습니다. FlexGroup 볼륨에서 파일을 생성하거나 확장할 수 있습니다. 그러나 구성요소에 저장된 파일은 수정할 수 없습니다. 결과적으로 FlexGroup 볼륨에 대해 쓰기 작업을 수행하려고 할 때 예기치 않은 공간 부족 오류가 나타날 수 있습니다.	"volume modify -files + X" 명령을 사용하여 FlexGroup 볼륨에 용량을 추가하는 것이 좋습니다.... 또는 FlexGroup 볼륨에서 파일을 삭제합니다. 그러나 어떤 파일이 구성 요소인지 결정하기는 어렵습니다.
FlexGroup 구성 요소 거의 가득 참	경고	FlexGroup 볼륨 내의 구성요소에 공간이 거의 부족하기 때문에 서비스가 중단될 수 있습니다. 파일을 만들고 확장할 수 있습니다. 그러나 구성 요소 공간이 부족한 경우 구성 요소에서 파일을 추가하거나 수정하지 못할 수 있습니다.	"volume modify -files + X" 명령을 사용하여 FlexGroup 볼륨에 용량을 추가하는 것이 좋습니다.... 또는 FlexGroup 볼륨에서 파일을 삭제합니다. 그러나 어떤 파일이 구성 요소인지 결정하기는 어렵습니다.
FlexGroup 구성 요소 inode가 거의 없습니다	경고	FlexGroup 볼륨 내의 구성요소는 inode에 거의 포함되어 있지 않습니다. 이로 인해 서비스가 중단될 수 있습니다. 구성요소에서 평균 보다 적은 생성 요청을 받습니다. 이 요청은 더 많은 inode가 있는 구성 요소에게 라우팅되므로 FlexGroup 볼륨의 전반적인 성능에 영향을 줄 수 있습니다.	"volume modify -files + X" 명령을 사용하여 FlexGroup 볼륨에 용량을 추가하는 것이 좋습니다.... 또는 FlexGroup 볼륨에서 파일을 삭제합니다. 그러나 어떤 파일이 구성 요소인지 결정하기는 어렵습니다.
FlexGroup 구성 요소 inode가 없습니다	심각	FlexGroup 볼륨의 구성요소에 inode가 부족하기 때문에 서비스가 중단될 수 있습니다. 이 구성요소에는 새 파일을 생성할 수 없습니다. 이로 인해 FlexGroup 볼륨 전체에 걸쳐 콘텐츠의 전체적인 균형이 맞지 않을 수 있습니다.	"volume modify -files + X" 명령을 사용하여 FlexGroup 볼륨에 용량을 추가하는 것이 좋습니다.... 또는 FlexGroup 볼륨에서 파일을 삭제합니다. 그러나 어떤 파일이 구성 요소인지 결정하기는 어렵습니다.
LUN을 오프라인 상태로 전환합니다	정보	이 이벤트는 LUN을 수동으로 오프라인 상태로 전환할 때 발생합니다.	LUN을 다시 온라인 상태로 전환합니다.

본체 팬 고장	경고	하나 이상의 메인 유닛 팬에 장애가 발생했습니다. 시스템은 계속 작동합니다. 그러나 이 상태가 너무 오래 지속되면 과열 상태가 자동 종료를 트리거할 수 있습니다.	장애가 발생한 팬을 재장착합니다. 오류가 지속되면 교체합니다.
주 장치 팬이 경고 상태입니다	정보	이 이벤트는 하나 이상의 메인 유닛 팬이 경고 상태에 있을 때 발생합니다.	과열되지 않도록 표시된 팬을 교체합니다.
NVRAM 배터리가 부족합니다	경고	NVRAM 배터리 용량이 매우 부족합니다. 배터리가 방전되면 데이터가 손실될 수 있습니다....시스템에서 AutoSupport 또는 "Call Home" 메시지를 생성하여 NetApp 기술 지원 부서 및 구성된 대상(구성된 경우)에게 전송합니다. AutoSupport 메시지를 성공적으로 전달하면 문제 확인 및 해결이 크게 향상됩니다.	다음 해결 조치를 수행하십시오.... "system node environment sensors show" 명령을 사용하여 배터리의 현재 상태, 용량 및 충전 상태를 확인하십시오.... 최근에 배터리를 교체했거나 시스템이 장시간 작동하지 않은 경우, 배터리를 모니터링하여 배터리가 올바르게 충전되고 있는지 확인하십시오. 배터리 작동 시간이 계속해서 중요 수준 이하로 감소하면 NetApp 기술 지원 부서에 문의하십시오. 스토리지 시스템이 자동으로 종료됩니다.
서비스 프로세서가 구성되지 않았습니다	경고	이 이벤트는 서비스 프로세서(SP)를 구성하도록 알리기 위해 매주 발생합니다. SP는 시스템에 통합되어 원격 액세스 및 원격 관리 기능을 제공하는 물리적 디바이스입니다. SP의 전체 기능을 사용하도록 구성해야 합니다.	"system service-processor network modify" 명령을 사용하여 SP를 구성합니다. 필요한 경우 "system service-processor network show" 명령을 사용하여 SP의 MAC 주소를 얻습니다.... "system service-processor network show" 명령을 사용하여 SP 네트워크 구성을 확인합니다.... SP가 "system service-processor AutoSupport invoke" 명령을 사용하여 AutoSupport e-메일을 보낼 수 있는지 확인합니다. 참고: 이 명령을 실행하기 전에 AutoSupport e-메일 호스트 및 수신자를 ONTAP에서 구성해야 합니다.

서비스 프로세서가 오프라인 상태입니다	심각	모든 SP 복구 작업이 수행되더라도 ONTAP는 더 이상 서비스 프로세서 (SP)로부터 하트비트를 수신하지 않습니다. ONTAP는 SP 없이는 하드웨어 상태를 모니터링할 수 없습니다.... 하드웨어 손상 및 데이터 손실을 방지하기 위해 시스템이 종료됩니다. SP가 오프라인이 될 때 즉시 알림을 받을 수 있도록 패닉 알림을 설정합니다.	다음 작업을 수행하여 시스템 전원을 껐다가 켭니다....새시에서 컨트롤러를 당겨 뽑니다 ...컨트롤러를 다시 밀어 넣습니다.... 컨트롤러를 다시 켭니다... 문제가 지속되면 컨트롤러 모듈을 교체합니다.
헬프 팬 실패	심각	표시된 냉각 팬 또는 헬프 팬 모듈에 장애가 발생했습니다. 헬프 내의 디스크가 냉각 공기 흐름이 충분하지 않아 디스크 장애가 발생할 수 있습니다.	다음 수정 조치를 수행하십시오.... 팬 모듈이 완전히 장착되고 고정되었는지 확인하십시오. 참고: 일부 디스크 헬프의 전원 공급 장치 모듈에 팬이 통합되어 있습니다.... 문제가 지속되면 팬 모듈을 교체하십시오.... 그래도 문제가 지속되면 NetApp 기술 지원 부서에 지원을 요청하십시오.
메인 장치 팬 오류로 인해 시스템을 작동할 수 없습니다	심각	하나 이상의 메인 유닛 팬에 장애가 발생하여 시스템 작동이 중단되었습니다. 이로 인해 데이터가 손실될 수 있습니다.	결함이 있는 팬을 교체합니다.
할당되지 않은 디스크	정보	시스템에 할당되지 않은 디스크가 있습니다. 용량이 낭비되고 있으며 시스템의 구성 오류 또는 부분 구성 변경이 적용될 수 있습니다.	"disk show -n" 명령을 사용하여 할당되지 않은 디스크를 확인합니다.... "disk assign" 명령을 사용하여 시스템에 디스크를 할당합니다.
바이러스 백신 서버 사용 중	경고	바이러스 백신 서버가 너무 바빠서 새 검사 요청을 수락할 수 없습니다.	이 메시지가 자주 발생하는 경우 SVM에서 생성되는 바이러스 검사 로드를 처리할 수 있는 바이러스 백신 서버가 충분한지 확인합니다.

IAM 역할에 대한 AWS 자격 증명이 만료되었습니다	심각	Cloud Volume ONTAP에 액세스할 수 없습니다. IAM(Identity and Access Management) 역할 기반 자격 증명 만료되었습니다. 이 자격 증명은 AWS(Amazon Web Services) 메타데이터 서버에서 IAM 역할을 사용하여 수집되며 Amazon S3(Amazon Simple Storage Service)에 API 요청을 서명하는 데 사용됩니다.	다음을 수행합니다....AWS EC2 관리 콘솔에 로그인합니다....인스턴스 페이지로 이동합니다... .Cloud Volumes ONTAP 구축을 위한 인스턴스를 찾고 해당 상태를 확인합니다....인스턴스와 관련된 AWS IAM 역할이 유효하고 인스턴스에 대한 적절한 권한이 부여되었는지 확인합니다.
IAM 역할에 대한 AWS 자격 증명을 찾을 수 없습니다	심각	클라우드 자격 증명 스레드는 AWS 메타데이터 서버에서 AWS(Amazon Web Services) IAM(Identity and Access Management) 역할 기반 자격 증명을 획득할 수 없습니다. 자격 증명은 Amazon S3(Amazon Simple Storage Service)에 API 요청을 서명하는 데 사용됩니다. 클라우드 볼륨 ONTAP에 액세스할 수 없습니다.	다음을 수행합니다....AWS EC2 관리 콘솔에 로그인합니다....인스턴스 페이지로 이동합니다... .Cloud Volumes ONTAP 구축을 위한 인스턴스를 찾고 해당 상태를 확인합니다....인스턴스와 관련된 AWS IAM 역할이 유효하고 인스턴스에 대한 적절한 권한이 부여되었는지 확인합니다.
IAM 역할에 대한 AWS 자격 증명이 잘못되었습니다	심각	IAM(Identity and Access Management) 역할 기반 자격 증명 유효하지 않습니다. 이 자격 증명은 AWS(Amazon Web Services) 메타데이터 서버에서 IAM 역할을 사용하여 수집되며 Amazon S3(Amazon Simple Storage Service)에 API 요청을 서명하는 데 사용됩니다. Cloud Volume ONTAP에 액세스할 수 없습니다.	다음을 수행합니다....AWS EC2 관리 콘솔에 로그인합니다....인스턴스 페이지로 이동합니다... .Cloud Volumes ONTAP 구축을 위한 인스턴스를 찾고 해당 상태를 확인합니다....인스턴스와 관련된 AWS IAM 역할이 유효하고 인스턴스에 대한 적절한 권한이 부여되었는지 확인합니다.

<p>AWS IAM 역할을 찾을 수 없습니다</p>	<p>심각</p>	<p>IAM(Identity and Access Management) 역할 스레드는 AWS 메타데이터 서버에서 AWS(Amazon Web Services) IAM 역할을 찾을 수 없습니다. IAM 역할은 Amazon S3(Amazon Simple Storage Service)에 API 요청을 서명하는 데 사용되는 역할 기반 자격 증명을 취득해야 합니다. 클라우드 볼륨 ONTAP에 액세스할 수 없습니다.</p>	<p>다음을 수행합니다....AWS EC2 관리 콘솔에 로그인합니다....인스턴스 페이지로 이동합니다... .Cloud Volumes ONTAP 구축을 위한 인스턴스를 찾고 해당 상태를 확인합니다....인스턴스와 관련된 AWS IAM 역할이 유효한지 확인합니다.</p>
<p>AWS IAM 역할이 잘못되었습니다</p>	<p>심각</p>	<p>AWS 메타데이터 서버에서 AWS(Amazon Web Services) IAM(ID 및 액세스 관리) 역할이 잘못되었습니다. 클라우드 볼륨 ONTAP에 액세스할 수 없습니다.</p>	<p>다음을 수행합니다....AWS EC2 관리 콘솔에 로그인합니다....인스턴스 페이지로 이동합니다... .Cloud Volumes ONTAP 구축을 위한 인스턴스를 찾고 해당 상태를 확인합니다....인스턴스와 관련된 AWS IAM 역할이 유효하고 인스턴스에 대한 적절한 권한이 부여되었는지 확인합니다.</p>
<p>AWS 메타데이터 서버 연결에 실패했습니다</p>	<p>심각</p>	<p>IAM(Identity and Access Management) 역할 스레드는 AWS(Amazon Web Services) 메타데이터 서버와 통신 링크를 설정할 수 없습니다. Amazon S3(Amazon Simple Storage Service)에 API 요청을 서명하는 데 사용되는 AWS IAM 역할 기반 자격 증명을 입수하기 위해 통신을 설정해야 합니다. 클라우드 볼륨 ONTAP에 액세스할 수 없습니다.</p>	<p>다음을 수행합니다....AWS EC2 관리 콘솔에 로그인합니다....인스턴스 페이지로 이동합니다... .Cloud Volumes ONTAP 구축의 인스턴스를 찾아 상태를 확인합니다.</p>

FabricPool 공간 사용 제한에 거의 도달했습니다	경고	용량 라이선스 공급자가 사용하는 오브젝트 저장소의 전체 클러스터 전체 FabricPool 공간 사용이 라이선스 한도에 거의 도달했습니다.	"storage aggregate object-store show-space" 명령을 사용하여 각 FabricPool 스토리지 계층에서 사용하는 라이선스 용량의 비율을 확인합니다.... 계층화 정책 "snapshot" 또는 "backup"이 있는 볼륨에서 "volume snapshot delete" 명령을 사용하여 공간을 지웁니다.... 새 라이선스를 설치합니다 클러스터에 라이선스 용량을 늘립니다.
FabricPool 공간 사용 제한에 도달했습니다	심각	용량 라이선스가 있는 공급자의 오브젝트 저장소에 대한 전체 클러스터 전체 FabricPool 공간 사용량이 라이선스 제한에 도달했습니다.	"storage aggregate object-store show-space" 명령을 사용하여 각 FabricPool 스토리지 계층에서 사용하는 라이선스 용량의 비율을 확인합니다.... 계층화 정책 "snapshot" 또는 "backup"이 있는 볼륨에서 "volume snapshot delete" 명령을 사용하여 공간을 지웁니다.... 새 라이선스를 설치합니다 클러스터에 라이선스 용량을 늘립니다.
Aggregate에 대한 반환에 실패했습니다	심각	이 이벤트는 대상 노드가 오브젝트 저장소에 연결할 수 없을 때 스토리지 페일오버(SFO) 반환의 일부로 애그리게이트를 마이그레이션하는 동안 발생합니다.	다음 수정 작업을 수행합니다. ... "network interface show" 명령을 사용하여 인터클러스터 LIF가 온라인이고 작동하는지 확인합니다. ... 대상 노드 인터클러스터 LIF에 대해 "ping" 명령을 사용하여 오브젝트 저장소 서버에 대한 네트워크 연결을 확인합니다. ... "aggregate object-store config show" 명령을 사용하여 오브젝트 저장소 구성이 변경되지 않았는지, 로그인 및 연결 정보가 여전히 정확한지 확인하십시오.... 또는 반환 명령의 "파트너 필요 대기" 매개 변수에 대해 false 를 지정하여 오류를 재정의할 수 있습니다. 자세한 정보나 지원이 필요하면 NetApp 기술 지원 부서에 문의하십시오.



<p>HA 인터커넥트 다운</p>	<p>경고</p>	<p>고가용성(HA) 인터커넥트가 다운되었습니다. 페일오버를 사용할 수 없는 경우 서비스 중단 위험이 있습니다.</p>	<p>수정 조치는 플랫폼에서 지원하는 HA 인터커넥트 링크의 수와 유형, 그리고 인터커넥트가 중단된 이유에 따라 다릅니다. 링크가 다운된 경우:... HA 쌍의 두 컨트롤러가 모두 작동하는지 확인하십시오.... 외부에서 연결된 링크의 경우 상호 연결 케이블이 제대로 연결되어 있는지, 그리고 해당되는 경우 소형 폼 팩터 플러그 가능 장치(SFP)가 두 컨트롤러에 제대로 장착되어 있는지 확인하십시오.... 내부적으로 연결된 링크의 경우, 링크를 비활성화 및 다시 활성화합니다. "IC LINK OFF" 및 "IC LINK ON" 명령을 차례로 사용합니다. ... 링크가 비활성화된 경우 "IC link on" 명령을 사용하여 링크를 활성화합니다. ... 피어가 연결되지 않은 경우 "IC LINK OFF" 및 "IC LINK ON" 명령을 사용하여 링크를 하나씩 차례로 비활성화 및 재활성화하십시오. 문제가 지속되면 NetApp 기술 지원 팀에 문의하십시오.</p>
--------------------	-----------	--	--

<p>사용자당 최대 세션 수가 초과되었습니다</p>	<p>경고</p>	<p>TCP 연결을 통해 사용자당 허용되는 최대 세션 수를 초과했습니다. 세션 설정 요청은 일부 세션이 해제될 때까지 거부됩니다. ...</p>	<p>다음 수정 조치를 수행하십시오. ... 클라이언트에서 실행되는 모든 응용 프로그램을 검사하고 제대로 작동하지 않는 응용 프로그램을 종료합니다.... 클라이언트를 재부팅합니다.... 새 응용 프로그램이나 기존 응용 프로그램으로 인해 문제가 발생하는지 확인합니다.... 새 응용 프로그램이 있으면 "cifs option modify -max -Opens -same -file -per -tree" 명령을 사용하여 클라이언트에 대해 더 높은 임계값을 설정합니다. 클라이언트가 예상대로 작동하지만 더 높은 임계값이 필요한 경우도 있습니다. 클라이언트에 대해 더 높은 임계값을 설정하려면 고급 권한이 있어야 합니다. 기존 응용 프로그램으로 인해 문제가 발생한 경우 클라이언트에 문제가 있을 수 있습니다. 자세한 정보 또는 지원 정보는 NetApp 기술 지원 부서에 문의하십시오.</p>
------------------------------	-----------	--	---

<p>파일당 열기 최대 시간이 초과되었습니다</p>	<p>경고</p>	<p>TCP 연결을 통해 파일을 열 수 있는 최대 횟수를 초과했습니다. 이 파일을 열기 위한 모든 요청은 파일의 일부 열린 인스턴스를 닫기 전까지 거부됩니다. 이는 일반적으로 비정상적인 응용 프로그램 동작을 나타냅니다.</p>	<p>다음 수정 조치를 수행합니다.... 이 TCP 연결을 사용하여 클라이언트에서 실행되는 응용 프로그램을 검사합니다. 응용 프로그램이 실행되고 있기 때문에 클라이언트가 제대로 작동하지 않을 수 있습니다.... 클라이언트를 재부팅합니다.... 새 응용 프로그램이나 기존 응용 프로그램으로 인해 문제가 발생하는지 확인합니다.... 새 응용 프로그램이 있으면 "cifs option modify -max -Opens -same -file -per -tree" 명령을 사용하여 클라이언트에 대해 더 높은 임계값을 설정합니다. 클라이언트가 예상대로 작동하지만 더 높은 임계값이 필요한 경우도 있습니다. 클라이언트에 대해 더 높은 임계값을 설정하려면 고급 권한이 있어야 합니다. 기존 응용 프로그램으로 인해 문제가 발생한 경우 클라이언트에 문제가 있을 수 있습니다. 자세한 정보 또는 지원 정보는 NetApp 기술 지원 부서에 문의하십시오.</p>
------------------------------	-----------	--	---

<p>NetBIOS 이름이 충돌합니다</p>	<p>심각</p>	<p>NetBIOS 이름 서비스가 원격 컴퓨터에서 이름 등록 요청에 대해 부정적인 응답을 받았습니다. 일반적으로 NetBIOS 이름 또는 별칭의 충돌로 인해 발생합니다. 따라서 클라이언트가 클러스터에 있는 올바른 데이터 서비스 노드에 연결하거나 데이터에 액세스하지 못할 수 있습니다.</p>	<p>NetBIOS 이름 또는 별칭에 충돌이 있는 경우 다음 수정 작업 중 하나를 수행합니다. 다음 중 하나를 수행합니다. ... "vserver cifs delete -alias alias -vserver vserver" 명령을 사용하여 중복 NetBIOS 별칭을 삭제합니다.... 중복 이름을 삭제하고 "vserver cifs create-alias -vserver vserver" 명령을 사용하여 새 이름으로 별칭을 추가하여 NetBIOS 별칭 이름을 바꿉니다. 별칭을 구성하지 않고 NetBIOS 이름에 충돌이 있는 경우 "vserver cifs delete -vserver vserver vserver" 및 "vserver cifs create -cifs -server netbiosname" 명령을 사용하여 CIFS 서버의 이름을 바꿉니다. 참고: CIFS 서버를 삭제하면 데이터에 액세스할 수 없습니다. ... NetBIOS 이름을 제거하거나 원격 시스템에서 NetBIOS 이름을 변경합니다.</p>
<p>NFSv4 저장소 풀이 소진되었습니다</p>	<p>심각</p>	<p>NFSv4 저장소 풀이 모두 소모되었습니다.</p>	<p>이 이벤트 후 NFS 서버가 10분 이상 응답하지 않는 경우 NetApp 기술 지원 팀에 문의하십시오.</p>
<p>등록된 스캔 엔진이 없습니다</p>	<p>심각</p>	<p>바이러스 백신 커넥터가 ONTAP에 등록된 검사 엔진이 없다는 알림을 표시합니다. "scan-mandatory(스캔-필수)" 옵션이 활성화된 경우 데이터를 사용할 수 없게 될 수 있습니다.</p>	<p>다음 수정 조치를 수행하십시오. 바이러스 백신 서버에 설치된 스캔 엔진 소프트웨어가 ONTAP과 호환되는지 확인하십시오.... 로컬 루프백을 통해 바이러스 백신 커넥터에 연결하도록 스캔 엔진 소프트웨어가 실행 및 구성되어 있는지 확인하십시오.</p>
<p>Vscan 연결이 없습니다</p>	<p>심각</p>	<p>ONTAP에는 바이러스 스캔 요청에 대한 Vscan 연결이 없습니다. "scan-mandatory(스캔-필수)" 옵션이 활성화된 경우 데이터를 사용할 수 없게 될 수 있습니다.</p>	<p>스캐너 풀이 올바르게 구성되어 있고 바이러스 백신 서버가 활성화되어 있고 ONTAP에 연결되어 있는지 확인합니다.</p>

노드 루트 볼륨 공간이 부족합니다	심각	시스템에서 루트 볼륨의 공간이 위험할 정도로 부족하다는 것을 감지했습니다. 노드가 완전히 작동하지 않습니다. 데이터 LIF는 노드에서 NFS 및 CIFS 액세스가 제한되므로 클러스터 내에서 페일오버되었을 수 있습니다. 관리 기능은 노드에서 루트 볼륨의 공간을 지우는 로컬 복구 절차로 제한됩니다.	다음 수정 조치를 수행하십시오. ... 이전 Snapshot 복사본을 삭제하거나 /mroot 디렉토리에서 더 이상 필요하지 않은 파일을 삭제하거나 루트 볼륨 용량을 확장하여 루트 볼륨의 공간을 확보하십시오.... 컨트롤러를 재부팅합니다.... 자세한 정보나 지원이 필요하다면 NetApp 기술 지원 부서에 문의하십시오.
존재하지 않는 관리자 공유	심각	Vscan 문제: 클라이언트가 존재하지 않는 ONTAP_admin\$ 공유에 연결하려고 했습니다.	Vscan이 언급된 SVM ID에 대해 활성화되어 있는지 확인합니다. SVM에서 Vscan을 활성화하면 SVM에 대해 ONTAP_admin\$ 공유가 자동으로 생성됩니다.
NVMe 네임스페이스 공간 부족	심각	공간 부족으로 인한 쓰기 실패로 인해 NVMe 네임스페이스가 오프라인 상태로 전환되었습니다.	볼륨에 공간을 추가한 다음 "vserver NVMe namespace modify" 명령을 사용하여 NVMe 네임스페이스를 온라인으로 전환합니다.
NVMe - 유예 기간 활성화	경고	이 이벤트는 NVMe-oF(NVMe over Fabrics) 프로토콜이 사용 중일 때 라이선스의 유예 기간이 활성화 상태일 때 매일 발생합니다. NVMe-oF의 경우, 라이선스 유예 기간이 만료된 후 라이선스가 필요합니다. 라이선스 유예 기간이 끝나면 NVMe-oF 기능이 비활성화됩니다.	세일즈 담당자에게 문의하여 NVMe-oF 라이선스를 얻은 후 클러스터에 추가하거나 클러스터에서 모든 NVMe-oF 구성 인스턴스를 제거하십시오.
NVMe - 유예 기간이 만료되었습니다	경고	NVMe-oF(NVMe over Fabrics) 라이선스 유예 기간이 끝났고 NVMe-of 기능이 비활성화되었습니다.	NVMe-oF 라이선스를 얻고 클러스터에 추가하려면 세일즈 담당자에게 문의하십시오.
NVMe - 유예 기간 시작	경고	ONTAP 9.5 소프트웨어로 업그레이드하는 동안 NVMe-oF(NVMe over Fabrics) 구성이 감지되었습니다. NVMe-oF의 경우, 라이선스 유예 기간이 만료된 후 라이선스가 필요합니다.	NVMe-oF 라이선스를 얻고 클러스터에 추가하려면 세일즈 담당자에게 문의하십시오.

객체 저장소 호스트를 확인할 수 없습니다	심각	오브젝트 저장소 서버 호스트 이름은 IP 주소로 확인할 수 없습니다. 오브젝트 저장소 클라이언트는 IP 주소로 확인하지 않으면 오브젝트 저장소 서버와 통신할 수 없습니다. 따라서 데이터에 액세스할 수 없습니다.	DNS 구성을 확인하여 호스트 이름이 IP 주소로 올바르게 구성되었는지 확인합니다.
오브젝트 저장소 클러스터 간 LIF가 다운되었습니다	심각	오브젝트 저장소 클라이언트는 오브젝트 저장소 서버와 통신할 운영 LIF를 찾을 수 없습니다. 인터클러스터 LIF가 작동할 때까지 노드가 오브젝트 저장소 클라이언트 트래픽을 허용하지 않습니다. 따라서 데이터에 액세스할 수 없습니다.	"네트워크 인터페이스 show-role 인터클러스터" 명령을 사용하여 인터클러스터 LIF 상태를 확인합니다.... 인터클러스터 LIF가 올바르게 구성되어 있고 작동하는지 확인합니다.... 인터클러스터 LIF가 구성되지 않은 경우 "네트워크 인터페이스 create-role" 명령을 사용하여 인터클러스터 LIF 상태를 추가합니다.
오브젝트 저장소 서명 불일치	심각	오브젝트 저장소 서버로 전송된 요청 서명이 클라이언트가 계산한 서명과 일치하지 않습니다. 따라서 데이터에 액세스할 수 없습니다.	비밀 액세스 키가 올바르게 구성되었는지 확인합니다. 올바르게 구성된 경우 NetApp 기술 지원 팀에 지원을 문의하십시오.
readdir 시간 초과	심각	readdir 파일 작업이 WAFL에서 실행할 수 있는 시간 제한을 초과했습니다. 이는 디렉토리가 매우 크거나 희소하기 때문일 수 있습니다. 수정 조치를 권장합니다.	다음 수정 작업을 수행합니다. ... 다음 'dig' 권한 nodeswell CLI 명령을 사용하여 readdir 파일 작업이 완료된 최근 디렉토리에 대한 정보를 찾습니다. WAFL readdir 알림이 표시됩니다.... 디렉토리가 스파스 또는 NOT로 표시되는지 확인합니다.... 디렉토리가 스파스(Sparse)로 표시된 경우 디렉토리의 내용을 새 디렉토리에 복사하여 디렉토리 파일의 스파를 제거하는 것이 좋습니다. ... 디렉토리가 스파스(Sparse)로 표시되지 않고 디렉토리가 큰 경우 디렉토리의 파일 항목 수를 줄여 디렉토리 파일의 크기를 줄이는 것이 좋습니다.

<p>집계 재배치에 실패했습니다</p>	<p>심각</p>	<p>이 이벤트는 대상 노드가 오브젝트 저장소에 연결할 수 없을 때 애그리게이트의 재배치 중에 발생합니다.</p>	<p>다음 수정 작업을 수행합니다. ... "network interface show" 명령을 사용하여 인터클러스터 NIF가 온라인이고 작동하는지 확인합니다. ... 대상 노드 인터클러스터 NIF에 대해 "ping" 명령을 사용하여 오브젝트 저장소 서버에 대한 네트워크 연결을 확인합니다. ... "aggregate object-store config show" 명령을 사용하여 오브젝트 저장소 구성이 변경되지 않고 로그인 및 연결 정보가 여전히 정확한지 확인하십시오.... 또는 재배치 명령의 "override-destination-checks" 매개 변수를 사용하여 오류를 재정의할 수 있습니다.... 자세한 정보 또는 지원을 받으려면 NetApp 기술 지원 부서에 문의하십시오.</p>
<p>새도 복사본 실패</p>	<p>심각</p>	<p>Microsoft Server 백업 및 복원 서비스 작업인 VSS(Volume Shadow Copy Service)가 실패했습니다.</p>	<p>이벤트 메시지에 제공된 정보를 사용하여 다음을 확인하십시오....새도 복사본 구성이 활성화되어 있습니까?...적절한 라이선스가 설치되어 있습니까? 새도 복사본 작업이 수행되는 공유는 무엇입니까?... 공유 이름이 올바릅니까?... 공유 경로가 존재합니까?... 새도 복사본 세트 및 해당 새도 복사본의 상태는 무엇입니까?</p>
<p>스토리지 스위치 전원 공급 장치에 장애가 발생했습니다</p>	<p>경고</p>	<p>클러스터 스위치에 전원 공급 장치가 없습니다. 중복성이 감소되어 정전 위험이 있으며 추가적인 전원 장애가 발생할 수 있습니다.</p>	<p>다음 수정 조치를 수행하십시오.... 클러스터 스위치에 전원을 공급하는 전원 공급 장치가 켜져 있는지 확인하십시오.... 전원 코드가 전원 공급 장치에 연결되어 있는지 확인하십시오.... 문제가 지속되면 NetApp 기술 지원 부서에 문의하십시오.</p>

CIFS 인증이 너무 많습니다	경고	많은 인증 협상이 동시에 발생했습니다. 이 클라이언트의 불완전한 새 세션 요청이 256개 있습니다.	클라이언트가 256개 이상의 새 연결 요청을 생성한 이유를 조사합니다. 오류가 발생한 이유를 확인하려면 클라이언트 또는 애플리케이션의 공급업체에 문의해야 할 수 있습니다.
관리자 공유에 대한 권한이 없는 사용자 액세스	경고	로그인한 사용자가 허용되지 않더라도 클라이언트가 권한이 있는 ONTAP_admin\$ 공유에 연결을 시도했습니다.	다음 수정 조치를 수행하십시오.... 언급된 사용자 이름과 IP 주소가 활성 Vscan 스캐너 풀 중 하나에 구성되어 있는지 확인하십시오.... "vserver scanner pool show-active" 명령을 사용하여 현재 활성화된 스캐너 풀 구성을 확인하십시오.
바이러스가 검색되었습니다	경고	Vscan 서버에서 저장소 시스템에 오류를 보고했습니다. 이는 일반적으로 바이러스가 발견되었음을 나타냅니다. 그러나 Vscan 서버의 다른 오류로 인해 이 이벤트가 발생할 수 있습니다.... 파일에 대한 클라이언트 액세스가 거부됩니다. Vscan 서버는 설정 및 구성에 따라 파일을 정리하거나 격리하거나 삭제할 수 있습니다.	"syslog" 이벤트에 보고된 Vscan 서버의 로그를 확인하여 감염된 파일을 성공적으로 정리, 격리 또는 삭제할 수 있는지 확인하십시오. 이 작업을 수행할 수 없는 경우 시스템 관리자가 파일을 수동으로 삭제해야 할 수 있습니다.
볼륨 오프라인	정보	이 메시지는 볼륨이 오프라인으로 설정되었음을 나타냅니다.	볼륨을 다시 온라인으로 설정합니다.
볼륨 제한	정보	이 이벤트는 유연한 볼륨이 제한되었음을 나타냅니다.	볼륨을 다시 온라인으로 설정합니다.
스토리지 VM 중지 성공	정보	이 메시지는 'vserver stop' 작업이 성공할 때 발생합니다.	'vserver start' 명령을 사용하여 스토리지 VM에서 데이터 액세스를 시작하십시오.
노드 패닉	경고	이 이벤트는 패닉이 발생할 때 발생합니다	NetApp 고객 지원 센터에 문의하십시오.

## 맨 위로

랜섬웨어 방지 로그 모니터

모니터 이름	심각도입니다	설명	수정 조치
--------	--------	----	-------



스토리지 VM 안티 랜섬웨어 모니터링 비활성화됨	경고	스토리지 VM의 랜섬웨어 방지 모니터링은 비활성화되어 있습니다. 스토리지 VM을 보호하기 위해 랜섬웨어 방지 기능을 활성화합니다.	없음
스토리지 VM 안티 랜섬웨어 모니터링 활성화(학습 모드)	정보	스토리지 VM의 랜섬웨어 방지 모니터링은 학습 모드에서 활성화됩니다.	없음
Volume Anti-랜섬웨어 모니터링 활성화	정보	볼륨에 대한 랜섬웨어 방지 모니터링이 활성화됩니다.	없음
볼륨 안티 랜섬웨어 모니터링 비활성화됨	경고	볼륨에 대한 랜섬웨어 방지 모니터링이 비활성화됩니다. 랜섬웨어를 차단 하여 볼륨을 보호합니다.	없음
Volume Anti-랜섬웨어 모니터링 활성화(학습 모드)	정보	볼륨에 대한 랜섬웨어 방지 모니터링은 학습 모드에서 활성화됩니다.	없음
볼륨 안티 랜섬웨어 모니터링 일시 중지(학습 모드)	경고	볼륨에 대한 랜섬웨어 방지 모니터링은 학습 모드에서 일시 중지됩니다.	없음
볼륨 안티 랜섬웨어 모니터링이 일시 중지되었습니다	경고	볼륨에 대한 랜섬웨어 방지 모니터링이 일시 중지됩니다.	없음
Volume Anti-랜섬웨어 모니터링 비활성화	경고	볼륨에 대한 랜섬웨어 방지 모니터링이 비활성화되어 있습니다.	없음
랜섬웨어 활동이 감지되었습니다	심각	감지된 랜섬웨어로부터 데이터를 보호하기 위해 원래 데이터를 복원하는 데 사용할 수 있는 스냅샷 복사본이 생성되었습니다. 시스템은 AutoSupport 기술 지원 부서 및 구성된 모든 대상으로 또는 "Call Home" 메시지를 생성하고 전송합니다. AutoSupport 메시지는 문제 확인 및 해결을 향상시킵니다.	랜섬웨어 활동을 개선하려면 "final-document-name"을 참조하십시오.

## 맨 위로

### NetApp ONTAP 모니터링용 FSX

모니터 이름	임계값	모니터 설명	수정 조치
--------	-----	--------	-------

<p>FSX 볼륨 용량이 가득 찼습니다</p>	<p>경고 @&gt;85%... 위험@&gt;95%</p>	<p>애플리케이션 및 고객 데이터를 저장하려면 볼륨의 스토리지 용량이 필요합니다. ONTAP 볼륨에 더 많은 데이터를 저장할수록 이후 데이터에 대한 스토리지 가용성이 줄어듭니다. 볼륨 내의 데이터 스토리지 용량이 총 스토리지 용량에 도달하면 스토리지 용량 부족으로 인해 고객이 데이터를 저장할 수 없게 될 수 있습니다. 사용된 볼륨 스토리지 용량을 모니터링하면 데이터 서비스의 연속성이 보장됩니다.</p>	<p>중요 임계값이 위반될 경우 서비스 중단을 최소화하기 위해 즉각적인 조치가 필요합니다.... 1. 여유 공간을 확보하기 위해 더 이상 필요하지 않은 데이터를 삭제하는 것이 좋습니다</p>
<p>FSX 볼륨 높은 지연 시간</p>	<p>경고 @&gt;1000 μs... Critical@&gt;2000 μs</p>	<p>볼륨은 DevOps 애플리케이션, 홈 디렉토리, 데이터베이스를 비롯하여 성능에 민감한 애플리케이션에서 주로 발생하는 IO 트래픽을 처리하는 객체입니다. 볼륨 지연 시간이 길다는 것은 애플리케이션 자체에서 문제를 겪고 있으며 작업을 수행할 수 없음을 의미합니다. 볼륨 지연 시간을 모니터링하는 것은 애플리케이션의 일관된 성능을 유지하는 데 매우 중요합니다.</p>	<p>중요 임계값이 위반될 경우 서비스 중단을 최소화하기 위해 즉각적인 조치가 필요합니다.... 1. 볼륨에 QoS 정책이 할당된 경우 볼륨 워크로드의 임계치가 조절되는 경우를 대비하여 제한 임계값을 평가합니다. ... 경고 임계값이 위반되면 즉시 다음 작업을 수행합니다. ... 1. 볼륨에 QoS 정책이 할당되어 있는 경우 볼륨 워크로드의 임계치가 조절되는 경우를 대비하여 제한 임계값을 평가합니다....2. 노드의 사용률도 높은 경우 볼륨을 다른 노드로 이동하거나 노드의 총 워크로드를 줄입니다.</p>

<p>FSX 볼륨 inode 제한</p>	<p>경고 @&gt;85%... 위험@&gt;95%</p>	<p>파일을 저장하는 볼륨은 인덱스 노드(inode)를 사용하여 파일 메타데이터를 저장합니다. 볼륨이 inode 할당을 처리할 때 더 이상 파일을 추가할 수 없습니다. 경고 알림은 사용 가능한 inode 수를 늘리기 위해 계획된 작업을 수행해야 함을 나타냅니다. 위험 경고는 파일 제한 소진이 임박했음을 나타내며, 서비스 연속성을 보장하기 위해 inode를 확보하기 위해 긴급 조치를 취해야 합니다</p>	<p>중요 임계값이 위반될 경우 서비스 중단을 최소화하기 위해 즉각적인 조치가 필요합니다.... 1. 볼륨에 대한 inode 값을 늘리는 것을 고려하십시오. inode 값이 이미 최대값에 있는 경우 파일 시스템이 최대 크기를 초과하여 확장되었기 때문에 볼륨을 두 개 이상의 볼륨으로 분할하는 것을 고려하십시오... 경고 임계값이 위반될 경우 즉시 다음 조치를 취하십시오 : 1. 볼륨에 대한 inode 값을 늘리는 것을 고려하십시오. inode 값이 이미 최대값에 있는 경우 파일 시스템이 최대 크기를 초과하여 확장되었기 때문에 볼륨을 두 개 이상의 볼륨으로 분할하는 것이 좋습니다</p>
<p>FSX 볼륨 Qtree 할당량 오버커밋</p>	<p>경고 @&gt;95%... 위험@&gt;100%</p>	<p>볼륨 Qtree 할당량 오버 커밋은 qtree 할당량에 의해 볼륨이 초과 커밋된 것으로 간주되는 비율을 지정합니다. 볼륨에 대해 qtree 할당량의 설정 임계값에 도달했습니다. 볼륨 qtree 할당량 초과 할당을 모니터링하면 사용자가 무중단 데이터 서비스를 받을 수 있습니다.</p>	<p>중요 임계값이 위반되면 서비스 중단을 최소화하기 위해 즉각적인 조치를 취해야 합니다. 1. 불필요한 데이터 삭제... 경고 임계값이 위반되면 볼륨 공간을 늘리는 것을 고려하십시오.</p>

<p>FSX 스냅샷 예비 공간이 가득 찹습니다</p>	<p>경고 @&gt;90%... 위험@&gt;95%</p>	<p>애플리케이션 및 고객 데이터를 저장하려면 볼륨의 스토리지 용량이 필요합니다. 스냅샷 예약 공간이라고 하는 이 공간의 일부는 데이터를 로컬로 보호할 수 있는 스냅샷을 저장하는 데 사용됩니다. ONTAP 볼륨에 새로 저장되거나 업데이트된 데이터가 많을수록 더 많은 스냅샷 용량이 사용되며 향후 새 데이터 또는 업데이트된 데이터에 더 적은 스냅샷 스토리지 용량을 사용할 수 있습니다. 볼륨 내의 스냅샷 데이터 용량이 전체 스냅샷 예비 공간에 도달하면 고객이 새 스냅샷 데이터를 저장할 수 없게 되고 볼륨의 데이터에 대한 보호 수준이 감소할 수 있습니다. 사용된 볼륨 스냅샷 용량을 모니터링하면 데이터 서비스의 연속성이 보장됩니다.</p>	<p>중요 임계값이 위반될 경우 서비스 중단을 최소화하기 위해 즉각적인 조치가 필요합니다.... 1. 스냅샷 예비 공간이 가득 찼을 때 볼륨의 데이터 공간을 사용하도록 스냅샷을 구성하는 것이 좋습니다. 2. 공간을 확보하기 위해 더 이상 필요하지 않을 수 있는 오래된 스냅샷을 일부 삭제하는 것을 고려하십시오... 경고 임계값이 위반될 경우 다음 작업을 곧 수행하십시오 : 1. 증가량을 수용하기 위해 볼륨 내에서 스냅샷 예비 공간을 늘리는 것을 고려하십시오. 2. 스냅샷 예비 공간이 가득 찼을 때 볼륨의 데이터 공간을 사용하도록 스냅샷을 구성하는 것이 좋습니다</p>
<p>FSX 볼륨 캐시 비적중 비율입니다</p>	<p>경고 @&gt;95%... 위험@&gt;100%</p>	<p>볼륨 캐시 비적중 비율은 캐시에서 반환되지 않고 디스크에서 반환된 클라이언트 애플리케이션의 읽기 요청 비율입니다. 즉, 볼륨이 설정된 임계값에 도달했음을 의미합니다.</p>	<p>중요 임계값이 위반되면 서비스 중단을 최소화하기 위해 즉각적인 조치를 취해야 합니다. 1. 일부 워크로드를 볼륨 노드에서 이동하여 IO 로드를 줄입니다 2. QoS 제한을 통해 동일한 노드에서 낮은 우선 순위 워크로드의 요구를 줄입니다. 경고 임계값이 위반될 때 즉시 조치를 고려하십시오. 1. 일부 워크로드를 볼륨 노드에서 이동하여 IO 로드를 줄입니다 2. QoS 제한을 통해 동일한 노드에서 낮은 우선 순위 워크로드의 요구를 줄입니다 3. 워크로드 특성 변경(블록 크기, 애플리케이션 캐싱 등)</p>

맨 위로

K8s 모니터

모니터 이름	설명	수정 조치	심각도/임계값
--------	----	-------	---------

영구 볼륨 지연 시간 높음	높은 영구 볼륨 대기 시간은 애플리케이션 자체에서 문제를 겪고 있으며 작업을 수행할 수 없음을 의미합니다. 애플리케이션의 일관된 성능을 유지하려면 지속적인 볼륨 지연 시간을 모니터링하는 것이 중요합니다. 다음은 미디어 유형-SSD에서 최대 1-2밀리초, SAS에서 최대 8-10밀리초, SATA HDD에서 17-20밀리초를 기준으로 한 예상 지연 시간입니다.	즉각적인 조치 중요 임계값이 위반되는 경우 서비스 중단을 최소화하기 위한 즉각적인 조치를 고려하십시오. 볼륨에 QoS 정책이 할당된 경우 볼륨 워크로드의 임계값이 제한될 수 있도록 제한 임계값을 평가합니다. 곧 수행할 조치 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 계획하십시오. 스토리지 풀의 사용을 또한 높은 경우 볼륨을 다른 스토리지 풀로 이동합니다. 볼륨에 QoS 정책이 할당된 경우 볼륨 워크로드의 제한이 발생하는 경우 해당 제한 임계값을 평가합니다. 3.컨트롤러에 사용률도 높은 경우 볼륨을 다른 컨트롤러로 이동하거나 컨트롤러의 총 워크로드를 줄입니다.	경고 @ > 6,000 $\mu$ s 긴급 @ > 12,000 $\mu$ s
클러스터 메모리 포화 높음	클러스터 할당 가능한 메모리 포화도가 높습니다. 클러스터 CPU 포화도는 메모리 사용량의 합계를 모든 K8 노드에 걸쳐 할당 가능한 메모리의 합계로 나눈 값으로 계산됩니다.	노드 추가 예약되지 않은 노드를 수정합니다. 적합한 크기의 Pod를 사용하므로 노드의 메모리 공간을 확보할 수 있습니다.	경고 @ > 80% 치명적 @ > 90%
포드 연결 실패	이 알림은 POD를 사용한 볼륨 연결이 실패한 경우에 발생합니다.		경고
높은 재전송 속도	높은 TCP 재전송 속도입니다	네트워크 정체 확인 - 많은 네트워크 대역폭을 사용하는 워크로드를 식별합니다. Pod CPU 활용률이 높은지 확인합니다. 하드웨어 네트워크 성능을 확인합니다.	경고 @ > 10% 심각 @ > 25%
노드 파일 시스템 용량 높음	노드 파일 시스템 용량 높음	- 응용 프로그램 파일을 위한 충분한 공간이 있는지 확인하기 위해 노드 디스크의 크기를 늘립니다. - 응용 프로그램 파일 사용량을 줄입니다.	경고 @ > 80% 치명적 @ > 90%

워크로드 네트워크 지터 높음	높은 TCP 지터(높은 지연 시간/응답 시간 변동)	네트워크 혼잡을 확인합니다. 많은 네트워크 대역폭을 사용하는 워크로드를 식별합니다. Pod CPU 활용률이 높은지 확인합니다. 하드웨어 네트워크 성능을 확인합니다	경고 @ > 30ms 치명적 @ > 50ms
영구 볼륨 처리량	영구 볼륨의 Mbps 임계값은 영구 볼륨이 사전 정의된 성능 기대치를 초과할 때 관리자에게 경고하는 데 사용할 수 있으며, 다른 영구 볼륨에 영향을 줄 수 있습니다. 이 모니터를 활성화하면 SSD의 영구 볼륨의 일반적인 처리량 프로필에 적합한 알림이 생성됩니다. 이 모니터는 사용자 환경의 모든 영구 볼륨에 적용됩니다. 이 모니터를 복제하거나 스토리지 클래스에 적합한 임계값을 설정하여 모니터링 목표에 따라 경고 및 위험 임계값을 조정할 수 있습니다. 이중화 모니터는 사용자 환경에서 영구 볼륨의 하위 세트에 더욱 초점을 맞춤 구성할 수 있습니다.	즉각적인 조치 중요 임계값이 위반되는 경우 서비스 중단을 최소화하기 위해 즉각적인 조치를 계획합니다. 볼륨에 대한 QoS Mbps 제한을 도입합니다. 볼륨에서 워크로드의 이상 징후를 유도하는 애플리케이션을 검토합니다. 곧 수행할 조치 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 취하도록 계획하십시오. 볼륨에 대한 QoS Mbps 제한을 도입합니다. 볼륨에서 워크로드의 이상 징후를 유도하는 애플리케이션을 검토합니다.	경고 @ > 10,000MB/s 중요 @ > 15,000MB/s
OOM이 사망할 위험이 있는 컨테이너	컨테이너의 메모리 제한이 너무 낮게 설정되어 있습니다. 컨테이너가 퇴거(메모리 부족) 위험이 있습니다.	컨테이너 메모리 제한을 늘립니다.	경고 @ > 95%
워크로드 다운	워크로드에 정상 상태의 Pod가 없습니다.		긴급 @ <1
영구 볼륨 청구가 바인딩되지 않았습니다	이 알림은 PVC에서 바인딩이 실패한 경우에 발생합니다.		경고
ResourceQuota Mem 제한을 초과하려고 합니다	네임스페이스에 대한 메모리 제한이 ResourceQuota를 초과합니다		경고 @ > 80% 치명적 @ > 90%
ResourceQuota Mem 초과 요청	네임스페이스에 대한 메모리 요청이 ResourceQuota를 초과하려고 합니다		경고 @ > 80% 치명적 @ > 90%
노드 생성에 실패했습니다	구성 오류로 인해 노드를 예약할 수 없습니다.	구성 실패의 원인은 Kubernetes 이벤트 로그를 확인하십시오.	심각

영구 볼륨 재확보에 실패했습니다	볼륨이 자동 재확보에 실패했습니다.		경고 @ > 0 B
컨테이너 CPU 임계치 조절	컨테이너의 CPU 제한이 너무 낮게 설정되어 있습니다. 컨테이너 프로세스 속도가 느려집니다.	컨테이너 CPU 한도를 늘립니다.	경고 @ > 95% 심각 @ > 98%
서비스 로드 밸런서를 삭제하지 못했습니다			경고
영구 볼륨 IOPS	영구 볼륨의 IOPS 임계값은 영구 볼륨이 사전 정의된 성능 기대치를 초과할 때 관리자에게 경고하는 데 사용할 수 있습니다. 이 모니터를 활성화하면 지속성 볼륨의 일반적인 IOPS 프로필에 적합한 알림이 생성됩니다. 이 모니터는 사용자 환경의 모든 영구 볼륨에 적용됩니다. 경고 및 임계 임계값은 이 모니터를 복제한 후 작업 부하에 적합한 임계값을 설정하여 모니터링 목표에 따라 조정할 수 있습니다.	즉각적인 조치 중요 임계값이 위반되는 경우 서비스 중단을 최소화하기 위해 즉각적인 조치를 계획합니다. 볼륨에 대한 QoS IOPS 제한을 소개합니다. 볼륨에서 워크로드의 이상 징후를 유도하는 애플리케이션을 검토합니다. 곧 수행할 조치 경고 임계값이 위반되면 다음과 같은 즉각적인 조치를 계획하십시오. 볼륨에 대한 QoS IOPS 제한을 소개합니다. 볼륨에서 워크로드의 이상 징후를 유도하는 애플리케이션을 검토합니다.	경고 @ > 20,000 IO/s 중요 @ 25,000 IO/s 이상
서비스 로드 밸런서를 업데이트하지 못했습니다			경고
POD 마운트 실패	이 알림은 포드에서 마운트가 실패한 경우에 발생합니다.		경고
노드 PID 압력	(Linux) 노드에서 사용 가능한 프로세스 식별자가 제거 임계값 아래로 떨어졌습니다.	많은 프로세스를 생성하고 사용 가능한 프로세스 ID의 노드를 굵는 포드를 찾아 수정합니다. PodPidsLimit를 설정하여 너무 많은 프로세스를 생성하는 Pod 또는 컨테이너로부터 노드를 보호합니다.	심각 @ > 0

포드 이미지 풀 실패	Kubernetes가 Pod 컨테이너 이미지를 가져오지 못했습니다.	- POD 구성에서 POD의 이미지를 올바르게 입력했는지 확인하십시오. - 이미지 태그가 레지스트리에 있는지 확인하십시오. - 이미지 레지스트리의 자격 증명을 확인합니다. - 레지스트리 연결 문제를 확인합니다. - 당신은 공공 레지스트리 공급자가 부과하는 요금 제한에 도달하지 않았는지 확인하십시오.	경고
작업이 너무 깁니다	작업이 너무 오래 실행 중입니다		경고 @ > 1시간 중요 @ > 5시간
노드 메모리 높음	노드 메모리 사용량이 많습니다	노드 추가 예약되지 않은 노드를 수정합니다. 적합한 크기의 Pod를 사용하므로 노드의 메모리 공간을 확보할 수 있습니다.	경고 @ > 85% 치명적 @ > 90%
ResourceQuota CPU 제한을 초과하려고 합니다	네임스페이스에 대한 CPU 제한이 ResourceQuota를 초과합니다		경고 @ > 80% 치명적 @ > 90%
포드 충돌 루프 백오프	Pod가 충돌하여 여러 번 다시 시작하려고 했습니다.		심각 @ > 3
노드 CPU 높음	노드 CPU 사용량이 많습니다.	노드 추가 예약되지 않은 노드를 수정합니다. Pod를 적합한 크기로 구성하여 노드의 CPU를 확보합니다.	경고 @ > 80% 치명적 @ > 90%
워크로드 네트워크 지연 시간 RTT 높음	높은 TCP RTT(Round Trip Time) 대기 시간	네트워크 정체 확인  많은 네트워크 대역폭을 사용하는 워크로드를 식별합니다. Pod CPU 활용률이 높은지 확인합니다. 하드웨어 네트워크 성능을 확인합니다.	경고 @ > 150ms 긴급 @ > 300ms
작업이 실패했습니다	노드 충돌 또는 재부팅, 리소스 소진, 작업 시간 초과 또는 Pod 스케줄링 실패로 인해 작업이 성공적으로 완료되지 않았습니다.	Kubernetes 이벤트 로그에서 실패 원인을 확인하십시오.	경고 @ > 1



며칠 후 영구 볼륨이 가득 찹니다	영구 볼륨은 며칠 후 공간이 부족해집니다	- 응용 프로그램 파일을 위한 충분한 공간이 있는지 확인하기 위해 볼륨 크기를 늘립니다. - 애플리케이션에 저장된 데이터의 양을 줄입니다.	경고 @ < 8일 긴급 @ < 3일
노드 메모리 압력	노드에 메모리가 부족합니다. 사용 가능한 메모리가 제거 임계값에 도달했습니다.	노드 추가 예약되지 않은 노드를 수정합니다. 적합한 크기의 Pod를 사용하므로 노드의 메모리 공간을 확보할 수 있습니다.	심각 @ > 0
노드가 준비되지 않았습니다	노드가 5분 동안 준비되지 않았습니다	노드에 CPU, 메모리 및 디스크 리소스가 충분한지 확인합니다. 노드 네트워크 연결을 확인하십시오. Kubernetes 이벤트 로그에서 실패 원인을 확인하십시오.	긴급 @ < 1
영구 볼륨 용량 높음	영구 볼륨 백엔드 사용 용량이 많습니다.	- 응용 프로그램 파일을 위한 충분한 공간이 있는지 확인하기 위해 볼륨 크기를 늘립니다. - 애플리케이션에 저장된 데이터의 양을 줄입니다.	경고 @ > 80% 치명적 @ > 90%
서비스 로드 밸런서를 만들지 못했습니다	서비스 로드 밸런서를 만들지 못했습니다		심각
워크로드 복제본 불일치	일부 Pod는 현재 배포 또는 데모 세트에 사용할 수 없습니다.		경고 @ > 1
ResourceQuota CPU 초과 요청	네임스페이스에 대한 CPU 요청이 ResourceQuota를 초과합니다		경고 @ > 80% 치명적 @ > 90%
높은 재전송 속도	높은 TCP 재전송 속도입니다	네트워크 정체 확인 - 많은 네트워크 대역폭을 사용하는 워크로드를 식별합니다. Pod CPU 활용률이 높는지 확인합니다. 하드웨어 네트워크 성능을 확인합니다.	경고 @ > 10% 심각 @ > 25%
노드 디스크 압력	노드의 루트 파일 시스템 또는 이미지 파일 시스템에서 사용 가능한 디스크 공간 및 inode가 제거 임계값을 충족했습니다.	- 응용 프로그램 파일을 위한 충분한 공간이 있는지 확인하기 위해 노드 디스크의 크기를 늘립니다. - 응용 프로그램 파일 사용량을 줄입니다.	심각 @ > 0

클러스터 CPU 포화 높음	클러스터 할당 가능한 CPU 포화도가 높습니다. 클러스터 CPU 포화도는 CPU 사용량의 합계를 모든 K8 노드에 걸쳐 할당 가능한 CPU의 합계로 나눈 값으로 계산됩니다.	노드 추가 예약되지 않은 노드를 수정합니다. Pod를 적합한 크기로 구성하여 노드의 CPU를 확보합니다.	경고 @ > 80% 치명적 @ > 90%
----------------	--	--	---------------------------

맨 위로

로그 모니터를 변경합니다

모니터 이름	심각도입니다	모니터 설명
내부 볼륨이 검색되었습니다	정보 제공	이 메시지는 내부 볼륨이 검색될 때 나타납니다.
내부 볼륨 수정됨	정보 제공	이 메시지는 내부 볼륨이 수정될 때 나타납니다.
스토리지 노드가 검색되었습니다	정보 제공	이 메시지는 스토리지 노드가 검색될 때 발생합니다.
스토리지 노드가 제거되었습니다	정보 제공	이 메시지는 스토리지 노드가 제거될 때 나타납니다.
스토리지 풀이 검색되었습니다	정보 제공	이 메시지는 스토리지 풀이 검색될 때 나타납니다.
스토리지 가상 머신이 검색되었습니다	정보 제공	이 메시지는 스토리지 가상 머신이 검색될 때 발생합니다.
스토리지 가상 머신이 수정되었습니다	정보 제공	이 메시지는 스토리지 가상 머신이 수정된 경우에 발생합니다.

맨 위로

데이터 수집 모니터

모니터 이름	설명	수정 조치
획득 장치 종료	Data Infrastructure Insights Acquisition Unit은 업그레이드의 일환으로 정기적으로 다시 시작하여 새로운 기능을 도입합니다. 이는 일반적인 환경에서 한 달에 한 번 이하 발생합니다. 새로 다시 시작된 획득 장치가 Data Infrastructure Insights를 사용하여 등록을 완료했음을 확인하는 Resolution(해결) 메시지가 표시된 후 바로 획득 장치가 종료되었다는 경고 경고가 표시됩니다. 일반적으로 이 등록 종료 주기는 5~15분 정도 소요됩니다.	경고가 자주 발생하거나 15분 이상 지속되는 경우 획득 장치, 네트워크 및 AU를 인터넷에 연결하는 모든 프록시를 호스팅하는 시스템의 작동을 확인하십시오.

Collector 실패	데이터 수집기의 폴링에 예기치 않은 실패 상황이 발생했습니다.	Data Infrastructure Insights의 데이터 수집기 페이지를 방문하여 상황에 대해 자세히 알아보십시오.
수집기 경고	이 경고는 일반적으로 데이터 수집기 또는 대상 시스템의 잘못된 구성 때문에 발생할 수 있습니다. 구성을 재검토하여 향후 경고를 방지합니다. 또한 데이터 수집기가 가능한 모든 데이터를 수집한, 완성도 미만이 아닌 데이터를 검색하는 것이 원인일 수 있습니다. 이는 데이터 수집 중에 상황이 변경되는 경우(예: 데이터 수집 시작 시점에 데이터가 캡처되기 전에 가상 시스템이 삭제된 경우) 발생할 수 있습니다.	데이터 수집기 또는 대상 시스템의 구성을 확인합니다. Collector Warning용 모니터는 다른 모니터 유형보다 더 많은 경고를 보낼 수 있으므로 문제 해결을 수행하지 않는 한 알림 수신자를 설정하지 않는 것이 좋습니다.

## 맨 위로

### 보안 모니터

모니터 이름	임계값	모니터 설명	수정 조치
AutoSupport HTTPS 전송이 비활성화되었습니다	경고 @<1	AutoSupport는 전송 프로토콜을 위해 HTTPS, HTTP 및 SMTP를 지원합니다. AutoSupport 메시지는 기본적으로 민감하므로 NetApp 지원에 AutoSupport 메시지를 보낼 때 HTTPS를 기본 전송 프로토콜로 사용하는 것이 좋습니다.	HTTPS를 AutoSupport 메시지의 전송 프로토콜로 설정하려면 다음 ONTAP 명령을 실행합니다. ... 시스템 노드 AutoSupport modify -transport https
SSH에 대한 클러스터 비보안 암호	경고 @<1	SSH가 * CBC로 시작하는 암호 등의 안전하지 않은 암호를 사용하고 있음을 나타냅니다.	CBC 암호를 제거하려면 다음 ONTAP 명령을 실행합니다. ... 보안 ssh remove -vserver <admin vserver> -cipherers AES256-CBC, AES192-CBC, aes128-CBC, 3DES-CBC
클러스터 로그인 배너 비활성화됨	경고 @<1	ONTAP 시스템에 액세스하는 사용자에게 대해 로그인 배너가 비활성화되었음을 나타냅니다. 로그인 배너를 표시하면 시스템 액세스 및 사용에 대한 기대치를 설정하는 데 도움이 됩니다.	클러스터에 대한 로그인 배너를 구성하려면 다음 ONTAP 명령을 실행하십시오. ... 보안 로그인 배너 modify -vserver <admin svm> -message "권한이 있는 사용자로 액세스 제한"

클러스터 피어 통신이 암호화되지 않았습니다	경고 @<1	재해 복구, 캐싱 또는 백업을 위해 데이터를 복제할 때 ONTAP 클러스터 간에 유선으로 데이터를 전송하는 동안 해당 데이터를 보호해야 합니다. 소스 클러스터와 대상 클러스터 모두에서 암호화를 구성해야 합니다.	ONTAP 9.6 이전에 생성된 클러스터 피어 관계에서 암호화를 활성화하려면 소스 및 대상 클러스터를 9.6으로 업그레이드해야 합니다. 그런 다음 "클러스터 피어 수정" 명령을 사용하여 소스 및 대상 클러스터 피어 모두에서 클러스터 피어링 암호화를 사용하도록 변경합니다. 자세한 내용은 ONTAP 9용 NetApp 보안 강화 가이드 를 참조하십시오.
기본 로컬 관리자 사용	경고 @>0	잠금 명령을 사용하여 불필요한 기본 관리자 사용자(기본 제공) 계정을 잠금(비활성화)하는 것이 좋습니다. 주로 암호가 업데이트되거나 변경되지 않은 기본 계정입니다.	기본 제공 "admin" 계정을 잠그려면 다음 ONTAP 명령을 실행합니다. ... 보안 로그인 잠금 -사용자 이름 admin
FIPS 모드가 비활성화되었습니다	경고 @<1	FIPS 140-2 규정 준수를 활성화하면 TLSv1 및 SSLv3이 비활성화되고 TLSv1.1 및 TLSv1.2만 활성화됩니다. ONTAP는 FIPS 140-2 규정 준수를 사용하는 경우 TLSv1 및 SSLv3을 활성화하지 못하도록 합니다.	클러스터에서 FIPS 140-2 규정 준수를 활성화하려면 고급 권한 모드에서 다음 ONTAP 명령을 실행합니다. ... 보안 구성 수정 - 인터페이스 SSL -is -FIPS -enabled true입니다
로그 전달이 암호화되지 않았습니다	경고 @<1	syslog 정보의 오프로드는 침입의 범위 또는 설치 공간을 단일 시스템 또는 솔루션으로 제한하는 데 필요합니다. 따라서 syslog 정보를 안전한 스토리지 또는 보존 위치로 안전하게 오프로딩하는 것이 좋습니다.	로그 전달 대상이 생성되면 해당 프로토콜을 변경할 수 없습니다. 암호화된 프로토콜로 변경하려면 다음 ONTAP 명령을 사용하여 로그 전달 대상을 삭제하고 다시 만듭니다. 클러스터 로그 전달 create-destination <destination ip> - 프로토콜 tcp 암호화

MD5 해시 암호입니다	경고 @>0	ONTAP 사용자 계정 암호에 대해 보다 안전한 SHA-512 해시 기능을 사용할 것을 적극 권장합니다. 덜 안전한 MD5 해시 기능을 사용하는 계정은 SHA-512 해시 함수로 마이그레이션해야 합니다.	사용자 계정이 암호를 변경하도록 하여 보다 안전한 SHA-512 솔루션으로 마이그레이션하는 것이 좋습니다.... MD5 해시 기능을 사용하는 암호로 계정을 잠그려면 다음 ONTAP 명령을 실행하십시오. ... 보안 로그인 잠금 -vserver* -username* -hash -function md5
구성된 NTP 서버가 없습니다	경고 @<1	클러스터에 구성된 NTP 서버가 없음을 나타냅니다. 이중화 및 최적의 서비스를 위해 최소 3개의 NTP 서버를 클러스터에 연결하는 것이 좋습니다.	NTP 서버를 클러스터에 연결하려면 ONTAP cluster time-service ntp server create -server <NTP server host name or ip address> 명령을 실행합니다
NTP 서버 수가 낮습니다	경고 @ <3	클러스터에 구성된 NTP 서버가 3개 미만임을 나타냅니다. 이중화 및 최적의 서비스를 위해 최소 3개의 NTP 서버를 클러스터에 연결하는 것이 좋습니다.	NTP 서버를 클러스터에 연결하려면 다음 ONTAP 명령을 실행합니다. ... 클러스터 시간 서비스 NTP 서버 create-server <NTP 서버 호스트 이름 또는 IP 주소>
원격 셸 사용	경고 @>0	원격 셸은 ONTAP 솔루션에 대한 명령줄 액세스를 설정하는 안전한 방법이 아닙니다. 원격 셸은 보안 원격 액세스를 위해 비활성화해야 합니다.	보안 원격 액세스를 위해 SSH(Secure Shell)를 사용하는 것이 좋습니다.... 클러스터에서 원격 셸을 비활성화하려면 고급 권한 모드에서 다음 ONTAP 명령을 실행합니다.... 보안 프로토콜 수정 - 응용 프로그램 rsh 지원 false
스토리지 VM 감사 로그가 비활성화되었습니다	경고 @<1	SVM에 대해 감사 로깅이 비활성화되었음을 나타냅니다.	가상 서버에 대한 감사 로그를 구성하려면 다음 ONTAP 명령을 실행하십시오. vserver audit enable -vserver <svm>
SSH에 대한 스토리지 VM 보안 암호가 안전하지 않습니다	경고 @<1	SSH가 * CBC로 시작하는 암호 등의 안전하지 않은 암호를 사용하고 있음을 나타냅니다.	CBC 암호를 제거하려면 다음 ONTAP 명령을 실행하십시오. ... 보안 ssh remove -vserver <vserver> -cipherers AES256-CBC, AES192-CBC, aes128-CBC, 3DES-CBC

스토리지 VM 로그인 배너가 비활성화되었습니다	경고 @<1	시스템에서 SVM에 액세스하는 사용자에게 대해 로그인 배너가 비활성화되었음을 나타냅니다. 로그인 배너를 표시하면 시스템 액세스 및 사용에 대한 기대치를 설정하는 데 도움이 됩니다.	클러스터에 대한 로그인 배너를 구성하려면 다음 ONTAP 명령을 실행하십시오. ... 보안 로그인 배너 modify -vserver <svm> -message "권한이 있는 사용자로 액세스 제한"
텔넷 프로토콜 사용	경고 @>0	텔넷은 ONTAP 솔루션에 대한 명령줄 액세스를 설정하는 안전한 방법이 아닙니다. 안전한 원격 액세스를 위해 텔넷을 비활성화해야 합니다.	보안 원격 액세스를 위해 SSH(Secure Shell)를 사용하는 것이 좋습니다. 클러스터에서 텔넷을 비활성화하려면 고급 권한 모드에서 다음 ONTAP 명령을 실행합니다.... 보안 프로토콜 수정 - 응용 프로그램 텔넷 사용 false

## 맨 위로

### 데이터 보호 모니터

모니터 이름	임계값	모니터 설명	수정 조치
LUN 스냅샷 복사본을 위한 공간이 부족합니다	(Filter Contains_LUNs=Yes) 경고 @> 95%...위험@> 100%	애플리케이션 및 고객 데이터를 저장하려면 볼륨의 스토리지 용량이 필요합니다. 스냅샷 예약 공간이라고 하는 이 공간의 일부는 데이터를 로컬로 보호할 수 있는 스냅샷을 저장하는 데 사용됩니다. ONTAP 볼륨에 새로 저장되거나 업데이트된 데이터가 많을수록 더 많은 스냅샷 용량이 사용되며 향후 새 데이터 또는 업데이트된 데이터에 더 적은 스냅샷 스토리지 용량을 사용할 수 있습니다. 볼륨 내의 스냅샷 데이터 용량이 총 스냅샷 예약 공간에 도달하면 새 스냅샷 데이터를 저장할 수 없게 되고 볼륨의 LUN에 있는 데이터에 대한 보호 수준이 저하될 수 있습니다. 사용된 볼륨 스냅샷 용량을 모니터링하면 데이터 서비스의 연속성이 보장됩니다.	즉각적인 조치 심각한 임계값이 위반될 경우 서비스 중단을 최소화하기 위한 즉각적인 조치를 고려하십시오. 1. 스냅샷 예비 공간이 가득 찼을 때 볼륨의 데이터 공간을 사용하도록 스냅샷을 구성합니다. 2. 오래된 원치 않는 스냅샷을 삭제하여 공간을 확보하십시오. 곧 수행할 작업 경고 임계값이 위반될 경우 다음과 같은 즉각적인 조치를 취하십시오. 1. 증가량을 수용하기 위해 볼륨 내에서 스냅샷 예비 공간을 늘립니다. 스냅샷 예비 공간이 가득 찼을 때 볼륨의 데이터 공간을 사용하도록 스냅샷을 구성합니다.

SnapMirror 관계 지연	경고 @>150%... 위험@>300%	SnapMirror 관계 지연은 스냅샷 타임스탬프와 대상 시스템의 시간 사이의 차이입니다. lag_time_percent는 SnapMirror 정책의 스케줄 간격에 대한 지연 시간의 비율입니다. 지연 시간이 스케줄 간격과 같으면 lag_time_percent가 100%가 됩니다. SnapMirror 정책에 스케줄이 없는 경우 lag_time_percent가 계산되지 않습니다.	"SnapMirror show" 명령을 사용하여 SnapMirror 상태를 모니터링합니다. "SnapMirror show-history" 명령을 사용하여 SnapMirror 전송 기록을 확인합니다
------------------	--------------------------	---	--

## 맨 위로

### CVO(Cloud Volume) 모니터

모니터 이름	CI 심각도	모니터 설명	수정 조치
CVO 디스크 서비스 중단	정보	이 이벤트는 디스크에 장애가 발생했거나, 제거 중이거나, 유지보수 센터에 진입했기 때문에 디스크가 서비스에서 제거된 경우에 발생합니다.	없음
스토리지 풀의 CVO 기브백에 실패했습니다	심각	이 이벤트는 대상 노드가 오브젝트 저장소에 연결할 수 없을 때 스토리지 페일오버(SFO) 반환의 일부로 애그리게이트를 마이그레이션하는 동안 발생합니다.	"network interface show" 명령을 사용하여 인터클러스터 LIF가 온라인이고 작동하는지 확인하는 수정 조치를 수행하십시오. 대상 노드 LIF 인터클러스터 LIF에서 "ping" 명령을 사용하여 오브젝트 저장소 서버에 대한 네트워크 연결을 확인하십시오. "aggregate object-store config show" 명령을 사용하여 오브젝트 저장소 구성이 변경되지 않고 로그인 및 연결 정보가 여전히 정확한지 확인하십시오. 또는 반환 명령의 "파트너 필요 대기" 매개 변수에 대해 false 를 지정하여 오류를 재정의할 수 있습니다. 자세한 정보 또는 지원 정보는 NetApp 기술 지원 부서에 문의하십시오.

<p>CVO HA 인터커넥트가 다운되었습니다</p>	<p>경고</p>	<p>고가용성(HA) 인터커넥트가 다운되었습니다. 페일오버를 사용할 수 없는 경우 서비스 중단 위험이 있습니다.</p>	<p>수정 조치는 플랫폼에서 지원하는 HA 인터커넥트 링크의 수와 유형, 그리고 인터커넥트가 중단된 이유에 따라 다릅니다. 링크가 다운된 경우: HA 쌍의 두 컨트롤러가 모두 작동하는지 확인합니다. 외부 연결 링크의 경우 상호 연결 케이블이 올바르게 연결되어 있고, 가능한 경우 소형 폼 팩터 SFP(Pluggable)가 두 컨트롤러 모두에 제대로 장착되어 있는지 확인합니다. 내부적으로 연결된 링크의 경우 "IC link off" 및 "IC link on" 명령을 사용하여 링크를 차례로 비활성화하고 다시 활성화합니다. 링크가 비활성화된 경우 "IC link on" 명령을 사용하여 링크를 활성화합니다. 피어가 연결되지 않은 경우 "IC link off(IC 링크 꺼짐)" 및 "IC link on(IC 링크 켜짐)" 명령을 사용하여 링크를 차례로 비활성화하고 다시 활성화합니다. 문제가 지속되면 NetApp 기술 지원 팀에 문의하십시오.</p>
------------------------------	-----------	--	--



<p>CVO 사용자당 최대 세션 수를 초과했습니다</p>	<p>경고</p>	<p>TCP 연결을 통해 사용자당 허용되는 최대 세션 수를 초과했습니다. 세션 설정 요청은 일부 세션이 해제될 때까지 거부됩니다.</p>	<p>클라이언트에서 실행되는 모든 응용 프로그램을 검사하고 제대로 작동하지 않는 응용 프로그램을 모두 종료하십시오. 클라이언트를 재부팅합니다. 새 애플리케이션이나 기존 애플리케이션에 의해 문제가 발생하는지 확인:새 애플리케이션인 경우 "cifs option modify -max -Opens -same -file -per -tree" 명령을 사용하여 클라이언트에 대해 더 높은 임계값을 설정합니다. 클라이언트가 예상대로 작동하지만 더 높은 임계값이 필요한 경우도 있습니다. 클라이언트에 대해 더 높은 임계값을 설정하려면 고급 권한이 있어야 합니다. 기존 응용 프로그램으로 인해 문제가 발생한 경우 클라이언트에 문제가 있을 수 있습니다. 자세한 정보 또는 지원 정보는 NetApp 기술 지원 부서에 문의하십시오.</p>
---------------------------------	-----------	--	---

<p>CVO NetBIOS 이름이 충돌합니다</p>	<p>심각</p>	<p>NetBIOS 이름 서비스가 원격 컴퓨터에서 이름 등록 요청에 대해 부정적인 응답을 받았습니다. 일반적으로 NetBIOS 이름 또는 별칭의 충돌로 인해 발생합니다. 따라서 클라이언트가 클러스터에 있는 올바른 데이터 서비스 노드에 연결하거나 데이터에 액세스하지 못할 수 있습니다.</p>	<p>다음 수정 작업 중 하나를 수행합니다. NetBIOS 이름 또는 별칭에 충돌이 있는 경우 다음 중 하나를 수행합니다. "vserver cifs delete -alias -vserver vserver vserver" 명령을 사용하여 중복 NetBIOS 별칭을 삭제합니다. "vserver cifs create-alias alias -vserver vserver" 명령을 사용하여 중복 이름을 삭제하고 새 이름으로 별칭을 추가하여 NetBIOS 별칭 이름을 변경합니다. 별칭이 구성되지 않고 NetBIOS 이름에 충돌이 있는 경우 "vserver cifs delete -vserver vserver vserver" 및 "vserver cifs create -cifs -server netbiosname" 명령을 사용하여 CIFS 서버의 이름을 변경하십시오. 참고: CIFS 서버를 삭제하면 데이터에 액세스할 수 없습니다. 원격 시스템에서 NetBIOS 이름을 제거하거나 NetBIOS 이름을 변경합니다.</p>
<p>CVO NFSv4 저장소 풀이 소진되었습니다</p>	<p>심각</p>	<p>NFSv4 저장소 풀이 모두 소모되었습니다.</p>	<p>이 이벤트 후 NFS 서버가 10분 이상 응답하지 않는 경우 NetApp 기술 지원 팀에 문의하십시오.</p>
<p>CVO 노드 패닉</p>	<p>경고</p>	<p>이 이벤트는 패닉이 발생할 때 발생합니다</p>	<p>NetApp 고객 지원 센터에 문의하십시오.</p>
<p>CVO 노드 루트 볼륨 공간이 부족합니다</p>	<p>심각</p>	<p>시스템에서 루트 볼륨의 공간이 위험할 정도로 부족하다는 것을 감지했습니다. 노드가 완전히 작동하지 않습니다. 데이터 LIF는 노드에서 NFS 및 CIFS 액세스가 제한되므로 클러스터 내에서 페일오버되었을 수 있습니다. 관리 기능은 노드에서 루트 볼륨의 공간을 지우는 로컬 복구 절차로 제한됩니다.</p>	<p>다음 수정 작업을 수행합니다. 이전 Snapshot 복사본을 삭제하거나, /mroot 디렉토리에서 더 이상 필요하지 않은 파일을 삭제하거나, 루트 볼륨 용량을 확장하여 루트 볼륨의 공간을 확보합니다. 컨트롤러를 재부팅합니다. 자세한 정보 또는 지원 정보는 NetApp 기술 지원 부서에 문의하십시오.</p>

CVO가 존재하지 않는 관리자 공유	심각	Vscan 문제: 클라이언트가 존재하지 않는 ONTAP_admin\$ 공유에 연결하려고 했습니다.	Vscan이 언급된 SVM ID에 대해 활성화되어 있는지 확인합니다. SVM에서 Vscan을 활성화하면 SVM에 대해 ONTAP_admin\$ 공유가 자동으로 생성됩니다.
CVO Object Store 호스트를 확인할 수 없습니다	심각	오브젝트 저장소 서버 호스트 이름은 IP 주소로 확인할 수 없습니다. 오브젝트 저장소 클라이언트는 IP 주소로 확인하지 않으면 오브젝트 저장소 서버와 통신할 수 없습니다. 따라서 데이터에 액세스할 수 없습니다.	DNS 구성을 확인하여 호스트 이름이 IP 주소로 올바르게 구성되었는지 확인합니다.
CVO Object Store 클러스터 간 LIF가 다운되었습니다	심각	오브젝트 저장소 클라이언트는 오브젝트 저장소 서버와 통신할 운영 LIF를 찾을 수 없습니다. 인터클러스터 LIF가 작동할 때까지 노드가 오브젝트 저장소 클라이언트 트래픽을 허용하지 않습니다. 따라서 데이터에 액세스할 수 없습니다.	"network interface show-role 인터클러스터" 명령을 사용하여 인터클러스터 LIF 상태를 확인합니다. 인터클러스터 LIF가 올바르게 구성되고 작동하는지 확인합니다. 인터클러스터 LIF가 구성되지 않은 경우 "네트워크 인터페이스 create-role 인터클러스터" 명령을 사용하여 이를 추가하십시오.
CVO 객체 저장소 서명 불일치	심각	오브젝트 저장소 서버로 전송된 요청 서명이 클라이언트가 계산한 서명과 일치하지 않습니다. 따라서 데이터에 액세스할 수 없습니다.	비밀 액세스 키가 올바르게 구성되었는지 확인합니다. 올바르게 구성된 경우 NetApp 기술 지원 팀에 지원을 문의하십시오.

<p>CVO QoS 모니터 메모리 최대값에 도달하였습니다</p>	<p>심각</p>	<p>QoS 하위 시스템의 동적 메모리가 현재 플랫폼 하드웨어에 대한 한계에 도달했습니다. 일부 QoS 기능은 제한된 범위에서 작동할 수 있습니다.</p>	<p>일부 활성 워크로드 또는 스트림을 삭제하여 메모리를 확보하십시오. "statistics show -object workload -counter ops" 명령을 사용하여 활성 상태인 워크로드를 확인합니다. 활성 워크로드는 0이 아닌 작업을 표시합니다. 그런 다음 "Workload delete &lt;workload_name&gt;" 명령을 여러 번 사용하여 특정 워크로드를 제거합니다. 또는 "stream delete-workload &lt;워크로드 이름&gt; *" 명령을 사용하여 활성 작업 부하에서 연결된 스트림을 삭제합니다.</p>
<p>CVO readdir 시간 초과</p>	<p>심각</p>	<p>readdir 파일 작업이 WAFL에서 실행할 수 있는 시간 제한을 초과했습니다. 이는 디렉토리가 매우 크거나 희소하기 때문일 수 있습니다. 수정 조치를 권장합니다.</p>	<p>다음 수정 작업을 수행합니다. readdir 파일 작업이 완료된 최근 디렉토리에 대한 정보를 찾으려면 다음 'diag' 권한 nodeswell CLI 명령을 사용합니다. WAFL readdir notice show. 디렉토리가 스파스 또는 NOT로 표시되는지 확인합니다. 디렉토리가 스파스 (Sparse)로 표시되는 경우 디렉토리 파일의 스파를 제거하기 위해 디렉토리의 내용을 새 디렉토리에 복사하는 것이 좋습니다. 디렉토리가 스파스 (Sparse)로 표시되지 않고 디렉토리가 큰 경우 디렉토리의 파일 항목 수를 줄여 디렉토리 파일의 크기를 줄이는 것이 좋습니다.</p>

CVO 스토리지 풀 재배치에 실패했습니다	심각	이 이벤트는 대상 노드가 오브젝트 저장소에 연결할 수 없을 때 애그리게이트의 재배치 중에 발생합니다.	"network interface show" 명령을 사용하여 인터클러스터 LIF가 온라인이고 작동하는지 확인하는 수정 조치를 수행하십시오. 대상 노드 LIF 인터클러스터 LIF에서 "ping" 명령을 사용하여 오브젝트 저장소 서버에 대한 네트워크 연결을 확인하십시오. "aggregate object-store config show" 명령을 사용하여 오브젝트 저장소 구성이 변경되지 않고 로그인 및 연결 정보가 여전히 정확한지 확인하십시오. 또는 relocation 명령의 "override-destination-checks" 매개 변수를 사용하여 오류를 재정의할 수 있습니다. 자세한 정보 또는 지원 정보는 NetApp 기술 지원 부서에 문의하십시오.
CVO 새도우 복제가 실패했습니다	심각	Microsoft Server 백업 및 복원 서비스 작업인 VSS(Volume Shadow Copy Service)가 실패했습니다.	이벤트 메시지에 제공된 정보를 사용하여 다음을 확인하십시오. 새도 복제본 구성이 활성화되어 있습니까? 적절한 라이선스가 설치되어 있습니까? 새도우 복제본 작업은 어떤 공유에서 수행됩니까? 공유 이름이 올바른가? 공유 경로가 존재합니까? 새도 복사본 세트와 해당 새도 복사본의 상태는 무엇입니까?
CVO 스토리지 VM 중지 성공	정보	이 메시지는 'vserver stop' 작업이 성공할 때 발생합니다.	'vserver start' 명령을 사용하여 스토리지 VM에서 데이터 액세스를 시작하십시오.
CVO가 CIFS 인증을 너무 많이 했습니다	경고	많은 인증 협상이 동시에 발생했습니다. 이 클라이언트의 불완전한 새 세션 요청이 256개 있습니다.	클라이언트가 256개 이상의 새 연결 요청을 생성한 이유를 조사합니다. 오류가 발생한 이유를 확인하려면 클라이언트 또는 애플리케이션의 공급업체에 문의해야 할 수 있습니다.

CVO 할당되지 않은 디스크	정보	시스템에 할당되지 않은 디스크가 있습니다. 용량이 낭비되고 있으며 시스템의 구성 오류 또는 부분 구성 변경이 적용될 수 있습니다.	다음 수정 조치를 수행하십시오. "disk show -n" 명령을 사용하여 할당되지 않은 디스크를 확인합니다. "disk assign" 명령을 사용하여 시스템에 디스크를 할당합니다.
CVO 관리자 공유에 대한 무단 사용자 액세스	경고	로그인한 사용자가 허용되지 않더라도 클라이언트가 권한이 있는 ONTAP_admin\$ 공유에 연결을 시도했습니다.	다음 교정 조치를 수행하십시오. 언급된 사용자 이름과 IP 주소가 활성 Vscan 스캐너 풀 중 하나에 구성되어 있는지 확인하십시오. "vserver vscan scanner pool show-active" 명령을 사용하여 현재 활성화된 스캐너 풀 구성을 확인합니다.
CVO 바이러스가 감지되었습니다	경고	Vscan 서버에서 저장소 시스템에 오류를 보고했습니다. 이는 일반적으로 바이러스가 발견되었음을 나타냅니다. 그러나 Vscan 서버의 다른 오류로 인해 이 이벤트가 발생할 수 있습니다. 파일에 대한 클라이언트 액세스가 거부됩니다. Vscan 서버는 설정 및 구성에 따라 파일을 정리하거나 격리하거나 삭제할 수 있습니다.	"syslog" 이벤트에 보고된 Vscan 서버의 로그를 확인하여 감염된 파일을 성공적으로 정리, 격리 또는 삭제할 수 있는지 확인하십시오. 이 작업을 수행할 수 없는 경우 시스템 관리자가 파일을 수동으로 삭제해야 할 수 있습니다.
CVO 볼륨 오프라인	정보	이 메시지는 볼륨이 오프라인으로 설정되었음을 나타냅니다.	볼륨을 다시 온라인으로 설정합니다.
CVO 볼륨 제한	정보	이 이벤트는 유연한 볼륨이 제한되었음을 나타냅니다.	볼륨을 다시 온라인으로 설정합니다.

## 맨 위로

### SMBC(비즈니스 연속성을 위한 SnapMirror) 증재자 로그 모니터

모니터 이름	심각도입니다	모니터 설명	수정 조치
ONTAP 증재자가 추가되었습니다	정보	이 메시지는 ONTAP 증재자가 클러스터에 성공적으로 추가될 때 발생합니다.	없음

ONTAP 중재자를 액세스할 수 없습니다	심각	이 메시지는 ONTAP 중재자를 용도 변경하거나 중재자 패키지가 중재자 서버에 더 이상 설치되지 않은 경우에 발생합니다. 따라서 SnapMirror 페일오버가 가능하지 않습니다.	"SnapMirror 중재자 제거" 명령을 사용하여 현재 ONTAP 중재자의 구성을 제거합니다. "SnapMirror 중재자 추가" 명령을 사용하여 ONTAP 중재자에 대한 액세스를 재구성합니다.
ONTAP 중재자가 제거되었습니다	정보	이 메시지는 ONTAP 중재자가 클러스터에서 성공적으로 제거되면 발생합니다.	없음
ONTAP 중재자 연락할 수 없음	경고	이 메시지는 클러스터에서 ONTAP 중재자를 연결할 수 없을 때 발생합니다. 따라서 SnapMirror 페일오버가 가능하지 않습니다.	"network ping" 및 "network traceroute" 명령을 사용하여 ONTAP 중재자에 대한 네트워크 연결을 확인합니다. 문제가 지속되면 "SnapMirror 중재자 제거" 명령을 사용하여 현재 ONTAP 중재자의 구성을 제거합니다. "SnapMirror 중재자 추가" 명령을 사용하여 ONTAP 중재자에 대한 액세스를 재구성합니다.
SMBC CA 인증서가 만료되었습니다	심각	이 메시지는 ONTAP 중재자 CA(인증 기관) 인증서가 만료된 경우에 발생합니다. 따라서 ONTAP 중재자를 위한 모든 추가 통신은 가능하지 않습니다.	"SnapMirror 중재자 제거" 명령을 사용하여 현재 ONTAP 중재자의 구성을 제거합니다. ONTAP 중재자 서버에서 새 CA 인증서를 업데이트합니다. "SnapMirror 중재자 추가" 명령을 사용하여 ONTAP 중재자에 대한 액세스를 재구성합니다.
SMBC CA 인증서가 만료됩니다	경고	이 메시지는 ONTAP 중재자 CA(인증 기관) 인증서가 향후 30일 내에 만료될 때 발생합니다.	이 인증서가 만료되기 전에 "SnapMirror 중재자 제거" 명령을 사용하여 현재 ONTAP 중재자의 구성을 제거합니다. ONTAP 중재자 서버에서 새 CA 인증서를 업데이트합니다. "SnapMirror 중재자 추가" 명령을 사용하여 ONTAP 중재자에 대한 액세스를 재구성합니다.

SMBC 클라이언트 인증서가 만료되었습니다	심각	이 메시지는 ONTAP 중재자 클라이언트 인증서가 만료된 경우에 발생합니다. 따라서 ONTAP 중재자를 위한 모든 추가 통신은 가능하지 않습니다.	"SnapMirror 중재자 제거" 명령을 사용하여 현재 ONTAP 중재자의 구성을 제거합니다. "SnapMirror 중재자 추가" 명령을 사용하여 ONTAP 중재자에 대한 액세스를 재구성합니다.
SMBC 클라이언트 인증서가 만료됩니다	경고	이 메시지는 ONTAP 중재자 클라이언트 인증서가 향후 30일 내에 만료될 예정인 경우 발생합니다.	이 인증서가 만료되기 전에 "SnapMirror 중재자 제거" 명령을 사용하여 현재 ONTAP 중재자의 구성을 제거합니다. "SnapMirror 중재자 추가" 명령을 사용하여 ONTAP 중재자에 대한 액세스를 재구성합니다.
SMBC 관계가 동기화되지 않았습니다. 참고: UM에는 이 항목이 없습니다	심각	이 메시지는 SMBC(Business Continuity용 SnapMirror) 관계의 상태가 "동기화 중"에서 "동기화 중단"으로 변경되면 발생합니다. 이 RPO = 0으로 인해 데이터 보호가 중단됩니다.	소스 볼륨과 대상 볼륨 간의 네트워크 연결을 확인합니다. 대상에서 "SnapMirror show" 명령을 사용하고 소스에서 "SnapMirror list-destinations" 명령을 사용하여 SMBC 관계 상태를 모니터링합니다. 자동 재동기화는 관계를 다시 "동기화 중" 상태로 전환하려고 시도합니다. 재동기화가 실패하면 클러스터의 모든 노드가 쿼럼에 있고 정상 상태인지 확인합니다.
SMBC 서버 인증서가 만료되었습니다	심각	이 메시지는 ONTAP 중재자 서버 인증서가 만료된 경우에 발생합니다. 따라서 ONTAP 중재자를 위한 모든 추가 통신은 가능하지 않습니다.	"SnapMirror 중재자 제거" 명령을 사용하여 현재 ONTAP 중재자의 구성을 제거합니다. ONTAP 중재자 서버에서 새 서버 인증서를 업데이트합니다. "SnapMirror 중재자 추가" 명령을 사용하여 ONTAP 중재자에 대한 액세스를 재구성합니다.



SMBC 서버 인증서가 만료됩니다	경고	이 메시지는 ONTAP 증재자 서버 인증서가 향후 30일 이내에 만료될 예정인 경우 발생합니다.	이 인증서가 만료되기 전에 "SnapMirror 증재자 제거" 명령을 사용하여 현재 ONTAP 증재자의 구성을 제거합니다. ONTAP 증재자 서버에서 새 서버 인증서를 업데이트합니다. "SnapMirror 증재자 추가" 명령을 사용하여 ONTAP 증재자에 대한 액세스를 재구성합니다.
--------------------	----	---	---

## 맨 위로

추가 전원, 하트비트 및 기타 시스템 모니터

모니터 이름	심각도입니다	모니터 설명	수정 조치
디스크 쉘프 전원 공급 장치가 검색되었습니다	정보 제공	이 메시지는 전원 공급 장치가 디스크 쉘프에 추가될 때 나타납니다.	없음
디스크 쉘프 전원 공급 장치가 제거되었습니다	정보 제공	이 메시지는 디스크 쉘프에서 전원 공급 장치를 제거할 때 발생합니다.	없음
MetroCluster 자동 비계획 전환 비활성화됨	심각	이 메시지는 예상치 못한 자동 전환 기능이 비활성화된 경우에 나타납니다.	클러스터의 각 노드에 대해 "MetroCluster modify -node -name <nodename> -automatic -switchover -onfailure true" 명령을 실행하여 자동 전환을 활성화하십시오.
MetroCluster 스토리지 브리지에 연결할 수 없습니다	심각	관리 네트워크를 통해 스토리지 브리지에 연결할 수 없습니다	1) SNMP에서 브리지를 모니터링하는 경우 "network interface show" 명령을 사용하여 노드 관리 LIF가 작동 중인지 확인합니다. "network ping" 명령을 사용하여 브리지가 활성 상태인지 확인합니다. 브리지가 대역 내에서 모니터링되는 경우 브리지에 대한 패브릭 케이블을 확인한 다음 브리지의 전원이 켜져 있는지 확인합니다.
MetroCluster 브리지 온도 비정상 - 위험 미만	심각	파이버 채널 브리지의 센서가 임계 임계값보다 낮은 온도를 보고하고 있습니다.	스토리지 브리지에서 팬의 작동 상태를 확인합니다. 2) 브리지가 권장 온도 조건에서 작동하는지 확인합니다.

모니터 이름	심각도입니다	모니터 설명	수정 조치
MetroCluster 브리지 온도 비정상 - 위험 초과	심각	파이버 채널 브리지의 센서가 임계 임계값보다 높은 온도를 보고하고 있습니다.	"storage bridge show-cooling" 명령을 사용하여 스토리지 브리지에서 새시 온도 센서의 작동 상태를 확인합니다. 스토리지 브리지가 권장 온도 조건에서 작동하는지 확인합니다.
MetroCluster Aggregate는 뒤쳐져 있습니다	경고	스위치백 중에는 aggregate가 남겨졌습니다.	1) "aggr show" 명령을 사용하여 애그리게이트 상태를 확인합니다. 2) 애그리게이트가 온라인 상태인 경우 "MetroCluster 스위치백" 명령을 사용하여 원래 소유자에게 돌려줍니다.
MetroCluster 파트너 간의 모든 링크가 다운되었습니다	심각	RDMA 상호 연결 어댑터와 인터클러스터 LIF가 피어링된 클러스터에 대한 연결이 끊어졌거나 피어링된 클러스터가 다운되었습니다.	인터클러스터 LIF가 작동 중인지 확인합니다. LIF가 다운된 경우 인터클러스터 LIF를 복구합니다. 2) "cluster peer ping" 명령을 사용하여 피어링된 클러스터가 작동 중인지 확인합니다. 피어링된 클러스터가 다운된 경우 MetroCluster 재해 복구 가이드를 참조하십시오. 3) Fabric MetroCluster의 경우 백엔드 Fabric ISL이 실행 중인지 확인합니다. 백엔드 Fabric ISL이 다운된 경우 복구합니다. 4) 비 패브릭 MetroCluster 구성의 경우 RDMA 상호 연결 어댑터 간 케이블 연결이 올바른지 확인합니다. 링크가 다운된 경우 케이블을 다시 구성하십시오.

모니터 이름	심각도입니다	모니터 설명	수정 조치
피어링 네트워크를 통해 MetroCluster 파트너에게 연결할 수 없습니다	심각	피어 클러스터에 대한 연결이 끊어집니다.	포트가 올바른 네트워크 /스위치에 연결되어 있는지 확인합니다. 인터클러스터 LIF가 피어링된 클러스터에 연결되어 있는지 확인합니다. 3) "cluster peer ping" 명령을 사용하여 피어링된 클러스터가 작동 중인지 확인합니다. 피어링된 클러스터가 다운된 경우 MetroCluster 재해 복구 가이드를 참조하십시오.
MetroCluster 인터스위치 모든 링크가 다운되었습니다	심각	스토리지 스위치의 모든 ISL(Inter-Switch Link)이 다운되었습니다.	스토리지 스위치의 백엔드 패브릭 ISL 복구 2) 파트너 스위치가 가동되고 해당 ISL이 작동하는지 확인합니다. xWDM 장치와 같은 중간 장비가 작동하는지 확인합니다.
스토리지 스택 SAS 링크에 대한 MetroCluster 노드 연결이 다운되었습니다	경고	SAS 어댑터 또는 연결된 케이블에 결함이 있을 수 있습니다.	SAS 어댑터가 온라인 상태이고 실행 중인지 확인합니다. 물리적 케이블 연결이 단단히 연결되어 있고 작동하는지 확인하고 필요한 경우 케이블을 교체합니다. SAS 어댑터가 디스크 쉘프에 연결되어 있는 경우 IOM 및 디스크가 제대로 장착되었는지 확인합니다.
MetroCluster FC Initiator 링크를 사용할 수 없습니다	심각	FC 이니시에이터 어댑터에 장애가 발생했습니다.	FC Initiator 링크가 훼손되지 않았는지 확인합니다. FC Initiator 어댑터의 작동 상태를 확인하려면 "system node run-node local -command storage show adapter" 명령을 사용하십시오.
FC-VI 인터커넥트 링크가 다운되었습니다	심각	FC-VI 포트의 물리적 링크가 오프라인 상태입니다.	FC-VI 링크가 손상되지 않았는지 확인합니다. FC-VI 어댑터의 물리적 상태가 "MetroCluster interconnect adapter show" 명령을 사용하여 "up" 상태인지 확인합니다. 3. 구성에 패브릭 스위치가 포함되어 있는 경우 케이블이 제대로 연결되고 구성되었는지 확인합니다.

모니터 이름	심각도입니다	모니터 설명	수정 조치
MetroCluster 스페어 디스크는 뒤에 남겨집니다	경고	스위치백을 진행하는 동안 스페어 디스크가 남겨졌습니다.	디스크에 오류가 발생하지 않은 경우 "MetroCluster 스위치백" 명령을 사용하여 원래 소유자에게 디스크를 반환하십시오.
MetroCluster 스토리지 브리지 포트가 다운되었습니다	심각	스토리지 브리지의 포트가 오프라인입니다.	"storage bridge show-ports" 명령을 사용하여 스토리지 브리지에 있는 포트의 작동 상태를 확인합니다. 포트에 대한 논리적 및 물리적 연결을 확인합니다.
MetroCluster 스토리지 스위치 팬에 장애가 발생했습니다	심각	스토리지 스위치의 팬에 장애가 발생했습니다.	"storage switch show-cooling" 명령을 사용하여 스위치의 팬이 올바르게 작동하는지 확인합니다. 2) 팬 FRU가 제대로 삽입되고 작동하는지 확인합니다.
MetroCluster 스토리지 스위치에 연결할 수 없습니다	심각	관리 네트워크를 통해 스토리지 스위치에 연결할 수 없습니다.	1) "network interface show" 명령을 사용하여 노드 관리 LIF가 작동 중인지 확인합니다. 2) "network ping" 명령을 사용하여 스위치가 활성 상태인지 확인합니다. 스위치에 로그인한 후 SNMP 설정을 확인하여 스위치가 SNMP를 통해 연결할 수 있는지 확인합니다.
MetroCluster 스위치 전원 공급 장치에 장애가 발생했습니다	심각	스토리지 스위치의 전원 공급 장치가 작동하지 않습니다.	1) "storage switch show-error-switch-name <switch name>" 명령을 사용하여 오류 세부 정보를 확인합니다. 2) "storage switch show-power-switch-name <switch name>" 명령을 사용하여 결함이 있는 전원 공급 장치를 식별합니다. 3) 전원 공급 장치가 스토리지 스위치의 새시에 제대로 삽입되어 있고 완전히 작동하는지 확인합니다.
MetroCluster 스위치 온도 센서 고장	심각	Fibre Channel 스위치의 센서가 작동하지 않습니다.	"storage switch show-cooling" 명령을 사용하여 스토리지 스위치의 온도 센서의 작동 상태를 확인합니다. 스위치가 권장 온도 조건에서 작동하는지 확인합니다.

모니터 이름	심각도입니다	모니터 설명	수정 조치
MetroCluster 스위치 온도가 비정상입니다	심각	파이버 채널 스위치의 온도 센서가 비정상적인 온도를 보고했습니다.	"storage switch show-cooling" 명령을 사용하여 스토리지 스위치의 온도 센서의 작동 상태를 확인합니다. 스위치가 권장 온도 조건에서 작동하는지 확인합니다.
서비스 프로세서 하트비트가 누락되었습니다	정보 제공	이 메시지는 ONTAP가 서비스 프로세서(SP)로부터 예상된 "하트비트" 신호를 수신하지 못하는 경우에 발생합니다. 이 메시지와 함께 SP의 로그 파일이 디버깅을 위해 전송됩니다. ONTAP가 통신을 복구하려고 SP를 재설정합니다. SP가 재부팅되는 동안 최대 2분 동안 SP를 사용할 수 없습니다.	NetApp 기술 지원 팀에 문의하십시오.
서비스 프로세서 하트비트가 중지되었습니다	경고	이 메시지는 ONTAP가 더 이상 서비스 프로세서 (SP)로부터 하트비트를 수신하지 않을 때 발생합니다. 하드웨어 설계에 따라 시스템이 데이터를 계속 제공하거나 데이터 손실이나 하드웨어 손상을 방지하기 위해 시스템 종료를 결정할 수 있습니다. 시스템은 계속해서 데이터를 제공하지만 SP가 작동하지 않을 수 있기 때문에 시스템에서 어플라이언스 다운, 부팅 오류 또는 OFW(Open Firmware) POST(Power-On Self-Test) 오류에 대한 알림을 보낼 수 없습니다. 시스템이 구성되면 AutoSupport(또는 'Call Home') 메시지를 생성하여 NetApp 기술 지원 부서 및 구성된 대상에 전송합니다. AutoSupport 메시지를 성공적으로 전달하면 문제 확인 및 해결이 크게 향상됩니다.	시스템이 종료된 경우, 하드 전원을 껐다가 다시 켭니다. 새시에서 컨트롤러를 잡아당겨 빼고 다시 밀어 넣은 다음 시스템 전원을 켭니다. 전원 껐다 켜기 후에도 문제가 계속 발생하거나 주의를 기울여야 하는 다른 조건이 있는 경우 NetApp 기술 지원 부서에 문의하십시오.

맨 위로

## 추가 정보

- ["경고 보기 및 해제"](#)

## Webhook를 사용한 알림

Webhook을 사용하면 사용자 지정된 Webhook 채널을 사용하여 다양한 응용 프로그램에 경고 알림을 보낼 수 있습니다.

Slack, PagerDuty, Teams, Teams, Teams 등 대부분의 상용 응용 프로그램은 Webhook를 표준 입력 인터페이스로 지원합니다. Data Infrastructure Insights는 일반 맞춤형 Webhook 채널을 지원하므로 이러한 제공 채널의 대부분을 지원할 수 있습니다. Webhook에 대한 정보는 이 응용 프로그램 웹 사이트에서 찾을 수 있습니다. 예를 들어 Slack은 ["유용한 가이드입니다"](#)를 제공합니다.

여러 개의 웹훅 채널을 만들 수 있으며, 각 채널은 서로 다른 용도로 사용됩니다. 즉, 별도의 애플리케이션, 다른 수신자 등을 만들 수 있습니다

Webhook 채널 인스턴스는 다음 요소로 구성됩니다.

이름	고유한 이름입니다
URL	웹 후크 대상 URL. URL과 함께 <i>http://</i> 또는 <i>https://</i> 접두사가 포함됩니다
방법	GET, POST - 기본값은 POST입니다
사용자 정의 머리글	여기에 사용자 정의 머리글 행을 지정합니다
메시지 본문	메시지 본문을 여기에 놓습니다
기본 경고 매개변수	에는 webhook에 대한 기본 매개 변수가 나와 있습니다
사용자 지정 매개 변수 및 암호	사용자 지정 매개 변수 및 암호를 사용하면 고유한 매개 변수와 암호와 같은 보안 요소를 추가할 수 있습니다

## Webhook 생성

Data Infrastructure Insights Webhook을 생성하려면 \* Admin > Notifications \* 로 이동하고 \* Webhook \* 탭을 선택합니다.

다음 이미지는 Slack에 대해 구성된 웹훅 예를 보여 줍니다.

## Edit a Webhook

Name

Slack Test

Template Type

Slack

URL

https://hooks.slack.com/services/<token>

Method

POST

Custom Header

Content-Type: application/json  
Accept: application/json

Message Body

```
{
  "blocks": [
    {
      "type": "section",
      "text": {
        "type": "mrkdwn",
        "text": "**Cloud Insights Alert - %%alertid%%*  
Severity - *%%severity%%**"
      }
    }
  ],
}
```

Cancel

Test Webhook

Save Webhook

각 필드에 적절한 정보를 입력하고 완료되면 "저장"을 클릭합니다.

"Webhook 테스트" 버튼을 클릭하여 연결을 테스트할 수도 있습니다. 이렇게 하면 선택한 방법에 따라 정의된 URL에 "메시지 본문"(대체 없음)이 전송됩니다.

Data Infrastructure Insights Webhook은 여러 가지 기본 매개 변수로 구성됩니다. 또한 사용자 지정 매개 변수 또는 암호를 직접 만들 수도 있습니다.


## Default Alert Parameters

Name	Description
%%alertDescription%%	Alert description
%%alertId%%	Alert ID
%%alertRelativeUrl%%	Relative URL to the Alert page. To build alert link use https://%%cloudInsightsHostName%%%%alertRelativeUrl%%
%%metricName%%	Monitored metric
%%monitorName%%	Monitor name
%%objectType%%	Monitored object type
%%severity%%	Alert severity level
%%alertCondition%%	Alert condition
%%triggerTime%%	Alert trigger time in GMT ("Tue, 27 Oct 2020 01:20:30 GMT")
%%triggerTimeEpoch%%	Alert trigger time in Epoch format (milliseconds)
%%triggeredOn%%	Triggered On (key:value pairs separated by commas)
%%value%%	Metric value that triggered the alert
%%cloudInsightsLogoUrl%%	Cloud Insights logo URL
%%cloudInsightsHostname%%	Cloud Insights Hostname (concatenate with relative URL to build alert link)

## Custom Parameters and Secrets

Name	Value	Description
------	-------	-------------

No Data Available

 Parameter

매개 변수: 해당 매개 변수는 무엇이며 어떻게 사용합니까?

경고 매개 변수는 알림에 따라 채워지는 동적 값입니다. 예를 들어, %%TriggeredOn% 매개 변수는 경고가 트리거된 개체로 대체됩니다.

이 섹션에서 대체는 "Webhook 테스트" 버튼을 클릭할 때 `_not_Performed` 가 됩니다. 이 버튼은 `_%_` 대체를 나타내는 페이로드를 전송하지만 데이터를 대체하지는 않습니다.



사용자 지정 매개 변수 및 암호

이 섹션에서는 원하는 사용자 지정 매개 변수 및/또는 암호를 추가할 수 있습니다. 보안상의 이유로 암호를 정의한 경우 웹 후크 생성자만 이 웹 후크 채널을 수정할 수 있습니다. 다른 사람에게는 읽기 전용입니다. URL/헤더에서 %<secret\_name>%(으)로 비밀을 사용할 수 있습니다.

**Webhook** 목록 페이지

Webhooks 목록 페이지에 이름, 만든 사람, 만든 사람, 상태, 보안, 및 마지막으로 보고된 필드

모니터에서 **Webhook** 알림 선택

에서 웹 후크 알림을 선택합니다 "모니터링", \* 경고 > 모니터 관리 \* 로 이동하여 원하는 모니터를 선택하거나 새 모니터를 추가합니다. 팀 알림 설정 섹션에서 전달 방법으로 \_Webhook\_을 선택합니다. 경고 수준(위험, 경고, 해결)을 선택한 다음 원하는 웹 후크를 선택합니다.

### 3 Set up team notification(s) (alert your team via email, or Webhook)

By Webhook

Notify team on

Critical, Warning, Resolved

Use Webhook

Please Select

Search...

ci-alerts-notifications-dev

ci-alerts-notifications-qa

**Webhook** 예:

에 대한 Webhook "슬랙"에 대한 Webhook "PagerDuty"에 대한 Webhook "팀"에 대한 Webhook "불화"

## 주석 작업

주석 정의

Data Infrastructure Insights를 사용자 정의하여 회사 요구사항에 대한 데이터를 추적할 때 주석이라는 특수 메모를 정의하고 자산에 할당할 수 있습니다.

자산 수명 종료, 데이터 센터, 건물 위치, 스토리지 계층 또는 불륨 서비스 수준과 같은 정보를 사용하여 자산에 주석을 할당할 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.

- 주석을 기준으로 자산을 필터링합니다.

## 기본 주석 유형

Data Infrastructure Insights는 몇 가지 기본 주석 유형을 제공합니다. 이러한 주석을 사용하여 데이터를 필터링하거나 그룹화할 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 Data Infrastructure Insights에서 제공하는 주석 유형이 나와 있습니다.

주석 유형	설명	유형
별칭	리소스에 대한 사용자 친화적인 이름입니다	텍스트
컴퓨팅 리소스 그룹	호스트 및 VM 파일 시스템 데이터 수집기에서 사용하는 그룹 할당	목록
데이터 센터	물리적 위치	목록
핫	사용량이 많은 디바이스를 정기적으로 또는 용량 임계값으로 사용합니다	부울
참고	리소스와 연결된 메모입니다	테스트
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
일몰	해당 디바이스에 새 할당을 수행할 수 없는 임계값을 설정합니다. 계획된 마이그레이션 및 기타 보류 중인 네트워크 변경에 유용합니다.	날짜
스위치 레벨	스위치에 대한 범주를 설정하기 위한 사전 정의된 옵션. 일반적으로 이러한 지정은 편집할 수 있지만 장치의 수명 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, 계층 및 위반 심각성은 시스템 수준 주석으로, 삭제하거나 이름을 바꿀 수 없습니다. 할당된 값만 변경할 수 있습니다.

## 사용자 정의 주식 작성

주석을 사용하여 비즈니스 요구에 맞는 맞춤형 비즈니스 관련 데이터를 자산에 추가할 수 있습니다. Data Infrastructure Insights는 일련의 기본 주석을 제공하지만 다른 방식으로 데이터를 보려는 경우도 있습니다. 사용자 지정 주석의 데이터는 스토리지 제조업체, 볼륨 수 및 성능 통계와 같이 이미 수집된 장치 데이터를 보완합니다. 주석을 사용하여 추가한 데이터는 Data Infrastructure Insights에서 검색되지 않습니다.

### 단계

1. Data Infrastructure Insights 메뉴에서 \* 관리 > 주석 \* 을 클릭합니다.

주석 페이지에는 주석 목록이 표시됩니다.

2. 추가 \* 를 클릭합니다
3. 주석의 \* 이름 \* 과 \* 설명 \* 을 입력합니다.

이 필드에는 최대 255자까지 입력할 수 있습니다.

4. Type \* 을 클릭한 다음 이 주석에 허용되는 데이터 유형을 나타내는 다음 옵션 중 하나를 선택합니다.

### 주석 유형

#### 부울

yes 및 no를 선택할 수 있는 드롭다운 목록을 만듭니다 예를 들어 "직접 연결" 주석은 부울입니다.

#### 날짜

이렇게 하면 날짜가 들어 있는 필드가 만들어집니다. 예를 들어, 주석이 날짜가 될 경우 이를 선택합니다.

#### 목록

다음 중 하나를 생성합니다.

- 드롭다운 고정 목록

다른 사용자가 장치에 이 주석 유형을 할당하는 경우 목록에 값을 더 추가할 수 없습니다.

- 드롭다운 유연한 목록

이 목록을 만들 때 즉시 새 값 추가 옵션을 선택하면 다른 사용자가 장치에 이 주석 유형을 할당할 때 목록에 값을 더 추가할 수 있습니다.

#### 번호

주석을 지정하는 사용자가 숫자를 입력할 수 있는 필드를 만듭니다. 예를 들어, 주석 유형이 "바닥"인 경우 사용자는 "숫자"의 값 유형을 선택하고 바닥 번호를 입력할 수 있습니다.

#### 텍스트

자유 형식 텍스트를 허용하는 필드를 만듭니다. 예를 들어, 주석 유형으로 "Language"를 입력하고 값 유형으로 "Text"를 선택한 다음 언어를 값으로 입력할 수 있습니다.



유형을 설정하고 변경 사항을 저장한 후에는 주석 유형을 변경할 수 없습니다. 유형을 변경해야 하는 경우 주석을 삭제하고 새 주석을 만들어야 합니다.

1. 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 주석을 적용할 때 새 주식 값을 추가할 수 없습니다. 그러면 고정 목록이 생성됩니다.

b. 값 \* 및 \* 설명 \* 필드에 값과 설명을 입력합니다.

c. 추가 값을 추가하려면 \* + 추가 + \* 를 클릭합니다.

d. 휴지통 아이콘을 클릭하여 값을 삭제합니다.

2. 저장 \* 을 클릭합니다

주식이 주식 페이지의 목록에 나타납니다.

작업을 마친 후

UI에서는 주석을 즉시 사용할 수 있습니다.

## 주석 사용

주석을 작성하고 모니터하는 자산에 할당할 수 있습니다. 주석은 물리적 위치, 수명 종료, 스토리지 계층 또는 볼륨 서비스 수준과 같은 자산에 대한 정보를 제공하는 메모입니다.

### 주석 정의

주석을 사용하여 비즈니스 요구에 맞는 맞춤형 비즈니스 관련 데이터를 자산에 추가할 수 있습니다. Data Infrastructure Insights는 자산 라이프사이클(생일 또는 수명 종료), 건물 또는 데이터 센터 위치, 계층과 같은 기본 주석 세트를 제공하지만, 데이터를 다른 방식으로 보려는 경우도 있습니다.

사용자 지정 주석의 데이터는 스위치 제조업체, 포트 수 및 성능 통계와 같이 이미 수집된 장치 데이터를 보완합니다. 주석을 사용하여 추가한 데이터는 Data Infrastructure Insights에서 검색되지 않습니다.

### 시작하기 전에

- 환경 데이터를 연결해야 하는 업계 용어를 나열하십시오.
- 환경 데이터를 연결해야 하는 기업 용어를 나열하십시오.
- 사용할 수 있는 기본 주석 유형을 식별합니다.
- 만들어야 하는 사용자 지정 주석을 식별합니다. 주석을 자산에 할당하려면 먼저 주석을 작성해야 합니다.

주석을 작성하려면 다음 단계를 따르십시오.

### 단계

1. Data Infrastructure Insights 메뉴에서 \* 관측성 > 보강하기 > 주석 \* 을 클릭합니다
2. 새 주석을 만들려면 \* + Annotation \* (주석 \*)을 클릭합니다.
3. 이름, 설명 및 새 주석의 유형을 입력합니다.

예를 들어, 다음을 입력하여 데이터 센터 4에서 자산의 물리적 위치를 정의하는 텍스트 주석을 작성합니다.

- "Location(위치)"과 같은 주석 이름을 입력합니다.
- "Physical location is Data Center 4"와 같이 주석이 설명하는 내용을 입력합니다.
- "텍스트"와 같이 주석의 '유형'을 입력합니다.

## 자산에 주석 수동 할당

자산에 주석을 지정하면 비즈니스와 관련된 방식으로 자산을 정렬, 그룹화 및 보고할 수 있습니다. 주석 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. Data Infrastructure Insights 환경에 로그인합니다.
2. 주석을 적용할 자산을 찾습니다.
  - 쿼리, dashard 위젯에서 선택 또는 검색을 통해 자산을 찾을 수 있습니다. 원하는 자산을 찾았으면 링크를 클릭하여 자산의 랜딩 페이지를 엽니다.
3. 자산 페이지의 사용자 데이터 섹션에서 \* + 주석 \* 을 클릭합니다.
4. 주석 추가 대화 상자가 표시됩니다.
5. 목록에서 주석을 선택합니다.
6. 값을 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.
7. 저장 \* 을 클릭합니다.

주석을 지정한 후 주석 값을 변경하려면 주석 필드를 클릭하고 다른 값을 선택합니다. fly\_option에서 \_Add new values를 선택한 목록 유형의 주석인 경우 기존 값을 선택하는 것 외에도 새 값을 입력할 수 있습니다.

## 주석 규칙을 사용하여 주석 지정

사용자가 정의한 기준에 따라 자산에 주석을 자동으로 할당하려면 주석 규칙을 구성합니다. Data Infrastructure Insights는 이러한 규칙을 기반으로 자산에 주석을 할당합니다. 또한 Data Infrastructure Insights는 두 가지 기본 주석 규칙을 제공합니다. 이러한 규칙은 필요에 따라 수정하거나 사용하지 않으려는 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 주식 유형을 편집할 수 있지만, 미리 유형을 정의해야 합니다.

단계

1. 관리 > 주식 규칙 \* 을 클릭합니다

주식 규칙 페이지에는 기존 주식 규칙 목록이 표시됩니다.

2. 추가 \* 를 클릭합니다.

3. 다음을 수행합니다.

- a. 이름 \* 상자에 규칙을 설명하는 고유한 이름을 입력합니다.

이 이름은 주식 규칙 페이지에 표시됩니다.

- b. Query \* 를 클릭하고 에셋에 주석을 적용하는 데 사용되는 쿼리를 선택합니다.

- c. Annotation(주식) \* 을 클릭하고 적용할 주석을 선택합니다.

- d. 값 \* 을 클릭하고 주식 값을 선택합니다.

예를 들어 주식으로 생일 을 선택한 경우 값의 날짜를 지정합니다.

- e. 저장 \* 을 클릭합니다

- f. 모든 규칙을 즉시 실행하려면 \* 모든 규칙 실행 \* 을 클릭합니다. 그렇지 않으면 규칙들이 정기적으로 예약된 간격으로 실행됩니다.

## 주식 규칙 작성

주식 규칙을 사용하여 정의한 기준에 따라 여러 자산에 주석을 자동으로 적용할 수 있습니다. Data Infrastructure Insights는 이러한 규칙을 기반으로 자산에 주석을 할당합니다. Cloud Insight에서 주식 규칙을 평가할 때 개별 자산 페이지에 수동으로 설정된 주석이 규칙 기반 주석보다 우선합니다.

시작하기 전에

주식 규칙에 대한 쿼리를 만들어야 합니다.

단계

1. Data Infrastructure Insights 메뉴에서 \* 관리 > 주식 규칙 \* 을 클릭합니다.

2. 새 주식 규칙을 추가하려면 \* + 규칙 \* 을 클릭합니다.

규칙 추가 대화 상자가 표시됩니다.

3. 다음을 수행합니다.

- a. 이름 \* 상자에 규칙을 설명하는 고유한 이름을 입력합니다.

주식 규칙 페이지에 이름이 나타납니다.

- b. Query \* 를 클릭하고 Data Infrastructure Insights에서 주석이 적용되는 자산을 식별하는 데 사용하는 쿼리를 선택합니다.

c. Annotation(주식) \* 을 클릭하고 적용할 주석을 선택합니다.

d. 값 \* 을 클릭하고 주식 값을 선택합니다.

예를 들어 주석으로 생일 을 선택한 경우 값의 날짜를 지정합니다.

e. 저장 \* 을 클릭합니다

f. 모든 규칙을 즉시 실행하려면 \* 모든 규칙 실행 \* 을 클릭합니다. 그렇지 않으면 규칙들이 정기적으로 예약된 간격으로 실행됩니다.



대규모 Data Infrastructure Insights 환경에서는 주식 규칙을 실행하는 데 시간이 오래 걸리는 것처럼 보일 수 있습니다. 이는 인덱서가 먼저 실행되고 규칙을 실행하기 전에 완료되어야 하기 때문입니다. 인덱서는 Data Infrastructure Insights에서 데이터에서 새 개체 또는 업데이트된 개체 및 카운터를 검색하거나 필터링할 수 있는 기능을 제공합니다. 규칙 엔진은 인덱서가 업데이트를 완료할 때까지 기다렸다가 규칙을 적용합니다.

### 주식 규칙 수정

주식 규칙을 수정하여 규칙 이름, 주식, 주식 값 또는 규칙과 연결된 쿼리를 변경할 수 있습니다.

#### 단계

1. Data Infrastructure Insights 메뉴에서 \* 관리 > 주식 규칙 \* 을 클릭합니다.

주식 규칙 페이지에는 기존 주식 규칙 목록이 표시됩니다.

2. 수정할 주식 규칙을 찾습니다.

필터 상자에 값을 입력하여 주식 규칙을 필터링하거나 페이지 번호를 클릭하여 페이지별로 주식 규칙을 찾아볼 수 있습니다.

3. 수정할 규칙의 메뉴 아이콘을 클릭합니다.

4. 편집 \* 을 클릭합니다

규칙 편집 대화 상자가 표시됩니다.

5. 주식 규칙 이름, 주식, 값 또는 쿼리를 수정합니다.

### 규칙 순서 변경

주식 규칙은 규칙 목록의 맨 위에서 맨 아래로 처리됩니다. 규칙이 처리되는 순서를 변경하려면 다음을 실행합니다.

#### 단계

1. 이동할 규칙의 메뉴 아이콘을 클릭합니다.

2. 원하는 위치에 규칙이 나타날 때까지 필요에 따라 \* 위로 이동 \* 또는 \* 아래로 이동 \* 을 클릭합니다.

한 자산에서 동일한 주석을 업데이트하는 여러 규칙을 실행할 때 첫 번째 규칙(위에서 아래로 실행)이 주석을 적용하고 자산을 업데이트한 다음 두 번째 규칙이 적용되지만 이전 규칙에 의해 이미 설정된 주석은 변경되지 않습니다.

## 주석 규칙 삭제

더 이상 사용되지 않는 주석 규칙을 삭제할 수 있습니다.

### 단계

1. Data Infrastructure Insights 메뉴에서 \* 관리 > 주석 규칙 \* 을 클릭합니다.

주석 규칙 페이지에는 기존 주석 규칙 목록이 표시됩니다.

2. 삭제할 주석 규칙을 찾습니다.

필터 상자에 값을 입력하여 주석 규칙을 필터링하거나 페이지 번호를 클릭하여 페이지별로 주석 규칙을 찾아볼 수 있습니다.

3. 삭제할 규칙의 메뉴 아이콘을 클릭합니다.

4. 삭제 \* 를 클릭합니다

규칙을 삭제할 것인지 묻는 확인 메시지가 표시됩니다.

5. 확인 \* 을 클릭합니다

## 주석 불러오기

Data Infrastructure Insights에는 CSV 파일에서 주석 또는 애플리케이션을 가져오고 사용자가 지정한 오브젝트에 할당하는 API가 포함되어 있습니다.



Data Infrastructure Insights API는 \* Data Infrastructure Insights Premium Edition \* 에서 사용할 수 있습니다.

### 가져오기

Admin > API Access \* 링크에는 가 포함되어 있습니다 "문서화" 자산/가져오기 \* API. 이 문서에는 .csv 파일 형식에 대한 정보가 포함되어 있습니다.

```
Project
, <Annotation Type> [, <Annotation Type> ...] [, Application] [, Tenant] [, Line_Of_Business] [, Business_Unit] [,
<Object Type Value 1>, <Object Name or Key 1>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 2>, <Object Name or Key 2>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
<Object Type Value 3>, <Object Name or Key 3>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
...
<Object Type Value N>, <Object Name or Key N>, <Annotation Value> [, <Annotation Value> ...] [, <Application>] [, <Tenant>] [, <Line_Of_Business>] [, <Business_Unit>] [,
<Project>]
```

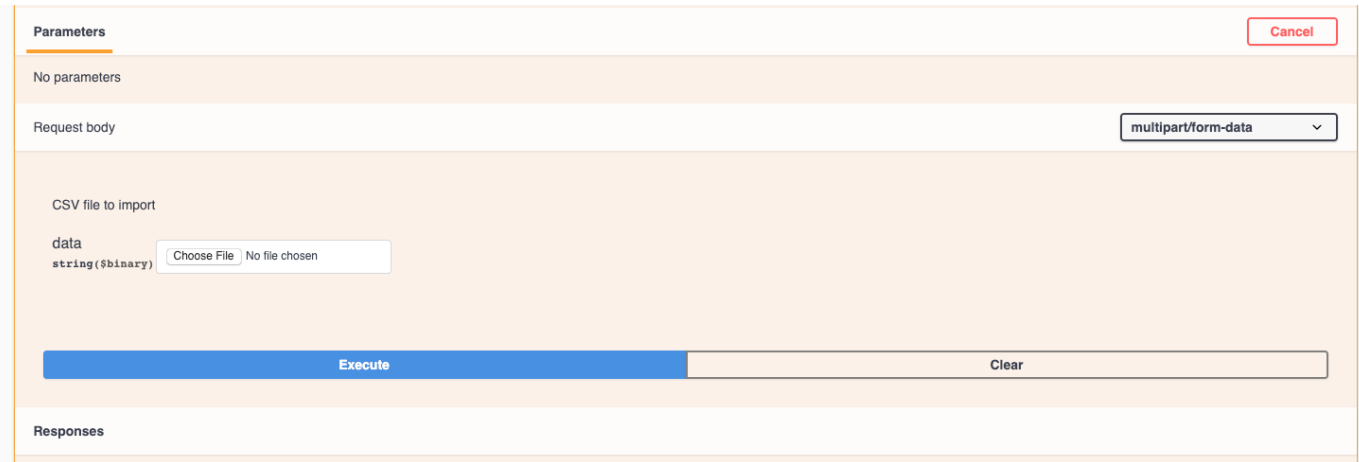
### CSV 파일 형식

CSV 파일의 일반 형식은 다음과 같습니다. 파일의 첫 번째 줄은 가져오기 필드를 정의하고 필드 순서를 지정합니다. 각 주석 또는 애플리케이션에 대해 별도의 선이 표시됩니다. 모든 필드를 정의할 필요는 없습니다. 그러나 후속 주석 선은 정의 선과 같은 순서를 따라야 합니다.



[Object Type] , [Object Name or ID] , Annotation Type [, Annotation Type, ...] [, Application] [, Tenant] [, Line\_Of\_Business] [, Business\_Unit] [, Project]  
 CSV 파일의 예는 API 설명서를 참조하십시오.

API swagger 내에서 .csv 파일에서 주석을 가져오고 할당할 수 있습니다. 사용할 파일을 선택하고 \_Execute\_ 버튼을 클릭하기만 하면 됩니다.



### 가져오기 동작

가져오는 개체와 개체 형식에 따라 가져오기 작업 중에 데이터가 추가, 병합 또는 교체됩니다. 가져오는 동안 다음 동작을 염두에 두십시오.

- 대상 시스템에 동일한 이름을 가진 주석이 없는 경우 주석 또는 애플리케이션을 추가합니다.
- 주석 유형이 목록이고 이름이 같은 주석이 대상 시스템에 있는 경우 주석을 병합합니다.
- 주석 유형이 목록 이외의 주석 유형이고 대상 시스템에 동일한 이름의 주석이 있는 경우 주석을 대체합니다.

참고: 이름이 같지만 유형이 다른 주석이 대상 시스템에 있는 경우 가져오기에 실패합니다. 개체가 실패한 주석에 따라 달라지는 경우 이러한 개체는 부정확하거나 원치 않는 정보를 표시할 수 있습니다. 가져오기 작업이 완료된 후에는 모든 주석 종속성을 확인해야 합니다.

- 주석 값이 비어 있으면 해당 주석이 개체에서 제거됩니다. 상속된 주석은 영향을 받지 않습니다.
- 날짜 유형 주석 값은 UNIX 시간으로 밀리초 단위로 전달되어야 합니다.
- 볼륨 또는 내부 볼륨에 주석을 달 때 오브젝트 이름은 "->" 구분 기호를 사용하여 스토리지 이름과 볼륨 이름의 조합입니다. 예: \_<스토리지 이름>-><볼륨 이름> \_
- 개체 이름에 심표가 포함된 경우 전체 이름은 큰따옴표로 묶어야 합니다. 예: \_ "NetApp1, NetApp2"->023F\_
- 스토리지, 스위치 및 포트에 주석 달기 기능을 추가하면 '응용 프로그램' 열이 무시됩니다.
- Tenant, Line\_of\_Business, Business\_Unit 및/또는 Project는 업무 엔티티를 만듭니다. 모든 업무 엔티티와 마찬가지로 모든 값을 비워둘 수 있습니다.

다음 개체 유형에 주석을 추가할 수 있습니다.

개체 유형	이름 또는 키
호스트	ID-><id> 또는 <Name> 또는 <IP>
VM	ID-><id> 또는 <Name>
스토리지 풀	ID-><id> 또는 <Storage Name>-><Storage Pool Name>
내부 볼륨	ID-><id> 또는 <스토리지 이름>-><내부 볼륨 이름>
볼륨	ID-><id> 또는 <Storage Name>-><Volume Name>
스토리지	ID-><id> 또는 <Name> 또는 <IP>
스위치	ID-><id> 또는 <Name> 또는 <IP>
포트	ID-><id> 또는 <WWN>
qtree입니다	ID-><id> 또는 <스토리지 이름>-><내부 볼륨 이름>-><Qtree 이름>
공유	ID-><id> 또는 <스토리지 이름>-><내부 볼륨 이름>-><공유 이름>-><프로토콜>[-><Qtree 이름(기본 Qtree의 경우 선택 사항)>]

## 응용 프로그램 작업

### 애플리케이션별로 자산 사용 추적

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 항목에서는 마케팅 팀이 Exchange 전자 메일에 사용하는 가상 시스템의 사용을 추적하는 예를 제공합니다.

사용자 환경에서 사용되는 애플리케이션을 식별하고 각 애플리케이션을 사용하여 그룹 또는 사업부를 메모하기 위해 다음과 유사한 테이블을 만들 수 있습니다.

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

이 표는 마케팅 팀이 Exchange 애플리케이션을 사용한다는 것을 보여줍니다. Exchange의 가상 시스템 활용률을 추적하여 스토리지를 추가해야 하는 시기를 예측할 수 있습니다. Exchange 애플리케이션을 모든 마케팅 가상 머신에 연결할 수 있습니다.

1. 이름이 \_Exchange\_인 응용 프로그램을 만듭니다
2. 쿼리 > + 새 쿼리 \* 로 이동하여 가상 머신에 대한 새 쿼리를 만들거나 기존 VM 쿼리를 선택합니다(해당하는 경우).

마케팅 팀의 VM에 모두 "\*" Mkt\*" 문자열이 포함된 이름이 있다고 가정하면 쿼리를 만들어 VM 이름을 "Mkt"로 필터링합니다.

3. VM을 선택합니다.
4. Bulk Actions > Add Applications \* 를 사용하여 VM을 \_Exchange\_ 응용 프로그램과 연결합니다.
5. 원하는 응용 프로그램을 선택하고 \* Save \* (저장 \*)를 클릭합니다.
6. 완료되면 \* 쿼리를 \* 저장 \* 합니다.

## 응용 프로그램 만들기

사용자 환경에서 실행 중인 특정 애플리케이션과 관련된 데이터를 추적하려면 Cloud Insights에서 애플리케이션을 정의할 수 있습니다.

시작하기 전에

애플리케이션을 업무 엔티티에 연결하려면 애플리케이션을 정의하기 전에 업무 엔티티를 생성해야 합니다.

이 작업에 대해

Cloud Insights를 사용하면 사용 또는 비용 보고와 같은 애플리케이션에 연결된 자산의 데이터를 추적할 수 있습니다.

단계

1. Cloud Insights 메뉴에서 \* 관측성 > 보강하기 > 애플리케이션 \* 을 클릭합니다. 를 선택합니다

응용 프로그램 추가 대화 상자가 표시됩니다.

2. 응용 프로그램의 고유한 이름을 입력합니다.
3. 응용 프로그램의 우선 순위를 선택합니다.
4. 저장 \* 을 클릭합니다.

애플리케이션을 정의한 후 자산에 할당할 수 있습니다.

자산에 애플리케이션 할당

이 절차에서는 호스트에 애플리케이션을 예로 할당합니다. 호스트, 가상 머신, 볼륨 또는 내부 볼륨을 애플리케이션에 할당할 수 있습니다.

단계

1. 응용 프로그램에 할당할 자산을 찾습니다.
2. 쿼리 > + 새 쿼리 \* 를 클릭하고 호스트를 검색합니다.
3. 애플리케이션과 연결할 호스트 왼쪽의 확인란을 클릭합니다.
4. 대량 작업 > 응용 프로그램 추가 \* 를 클릭합니다.
5. 자산을 할당할 애플리케이션을 선택합니다.

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.



관련 자산이 많은 환경의 경우 해당 자산에 대한 애플리케이션 할당 상속에 몇 분이 걸릴 수 있습니다. 관련 자산이 많은 경우 상속에 더 많은 시간을 할애하십시오.

작업을 마친 후

호스트에 애플리케이션을 할당한 후 나머지 자산을 애플리케이션에 할당할 수 있습니다. 응용 프로그램의 랜딩 페이지에 액세스하려면 \* 관리 > 응용 프로그램 \* 을 클릭하고 생성한 응용 프로그램을 선택합니다.

## 자동 장치 해상도

### 자동 장치 해상도 개요

Data Infrastructure Insights를 사용하여 모니터링할 모든 장치를 식별해야 합니다. 작업 환경의 성능 및 재고를 정확하게 추적하려면 식별이 필요합니다. 일반적으로 사용자 환경에서 검색된 대부분의 장치는 \_ 자동 장치 해상도 \_ 를 통해 식별됩니다.

데이터 수집기를 구성한 후에는 스위치, 스토리지 시스템, 하이퍼바이저 및 VM의 가상 인프라를 비롯한 환경의 디바이스가 식별됩니다. 그러나 이 경우 일반적으로 사용자 환경의 디바이스 중 100%는 식별되지 않습니다.

데이터 수집기 유형 장치를 구성한 후 가장 좋은 방법은 장치 해결 규칙을 활용하여 사용자 환경에 남아 있는 알 수 없는 장치를 식별하는 것입니다. 장치 해상도를 통해 알 수 없는 장치를 다음 장치 유형으로 해결할 수 있습니다.

- 물리적 호스트
- 지원합니다
- 테이프

디바이스 확인 후 알 수 없는 것으로 남아 있는 디바이스는 일반 디바이스로 간주되어 쿼리 및 대시보드에도 표시할 수 있습니다.

차례로 생성된 규칙은 사용자 환경에 추가되는 것과 유사한 특성을 가진 새 디바이스를 자동으로 식별합니다. 경우에 따라 장치 해결을 통해 Data Infrastructure Insights 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.

- \* Fibre Channel Identify \* 에는 자동 디바이스 확인을 통해 확인되지 않은 Fibre Channel 디바이스의 목록 WWN 및 포트 정보가 포함되어 있습니다. 이 탭은 식별된 디바이스의 비율도 식별합니다.
- \* IP Address Identify \* 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 파이버 채널 장치 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.

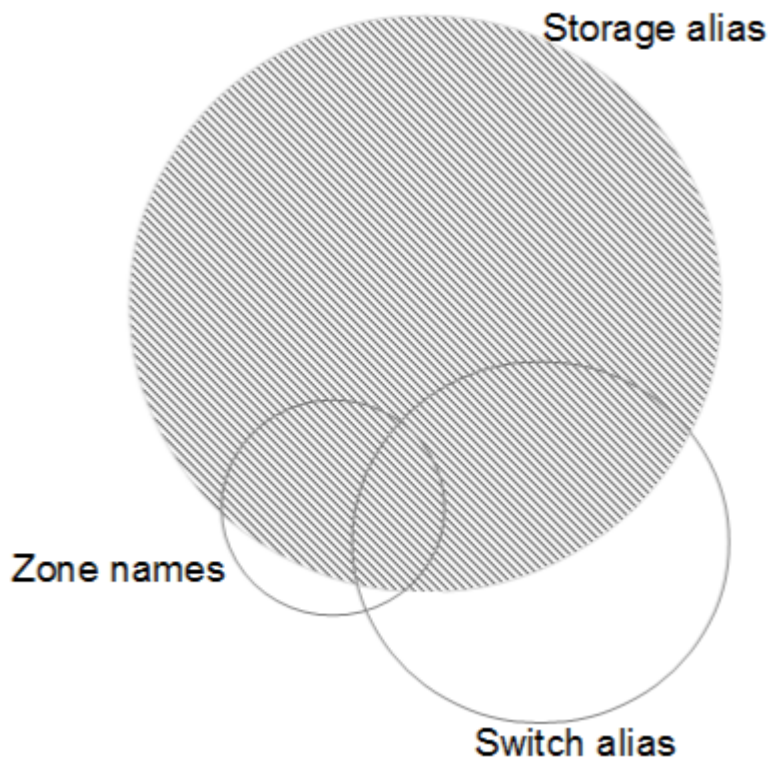
### 시작하기 전에

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?
- 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.

## 장치 식별 단계

일반적으로 다음과 유사한 워크플로를 사용하여 사용자 환경에서 장치를 식별합니다. 식별은 반복적인 프로세스이며 규칙을 계획하고 구체화하는 여러 단계가 필요할 수 있습니다.

- 있습니다
- 계획 규칙
- 규칙 작성/수정
- 결과를 검토합니다
- 추가 규칙을 생성하거나 수동으로 장치를 식별합니다
- 완료



사용자 환경에 알 수 없는 장치(알 수 없는 장치 또는 일반 장치)가 있고 이후에 폴링 시 이러한 장치를 식별하는 데이터 소스를 구성하면 더 이상 일반 장치로 표시되거나 계산되지 않습니다.

관련: "장치 해상도 규칙을 만드는 중입니다"

"파이버 채널 장치 해상도"

"IP 장치 해상도"

"장치 해상도 기본 설정 지정"

## 장치 해상도 규칙

디바이스 확인 규칙을 생성하여 현재 Data Infrastructure Insights에서 자동으로 식별되지 않는 호스트, 스토리지 및 테이프를 식별합니다. 생성하는 규칙은 현재 환경에 있는 디바이스를 식별하고 유사한 디바이스를 환경에 추가할 때 식별합니다.

장치 해상도 규칙을 만드는 중입니다

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	* 포함된 호스트 또는 테이프 이름이 포함된 스토리지 별칭 * 포함된 호스트 또는 테이프 이름이 포함된 스위치 별칭 * 포함된 호스트 이름이 포함된 영역 이름
소스에서 디바이스 이름을 추출하는 데 사용되는 방법입니다	현재 상태 그대로 * (SRM에서 이름 추출) * 구분 기호 * 정규식
DNS 조회	DNS를 사용하여 호스트 이름을 확인할지 여부를 지정합니다

자동 해결 규칙 탭에서 규칙을 만듭니다. 다음 단계에서는 규칙 생성 프로세스를 설명합니다.

절차를 참조하십시오

1. 관리 > 장치 해상도 \* 를 클릭합니다
2. 자동 해결 규칙 \* 탭에서 \* + 호스트 규칙 \* 또는 \* + 테이프 규칙 \* 을 클릭합니다.

해상도 규칙 \* 화면이 표시됩니다.



정규식 만들기에 대한 도움말과 예제를 보려면 [\\_View Matching criteria\\_](#) 링크를 클릭하십시오.

3. Type \* 목록에서 식별하려는 장치를 선택합니다.

Host\_or\_Tape\_를 선택할 수 있습니다.

4. 소스 \* 목록에서 호스트를 식별하는 데 사용할 소스를 선택합니다.

Data Infrastructure Insights에는 선택한 소스에 따라 다음 응답이 표시됩니다.

- a. \* Zones \* 에는 Data Infrastructure Insights에서 식별해야 하는 영역 및 WWN이 나열됩니다.
- b. \* SRM \* 에는 Data Infrastructure Insights로 식별해야 하는 식별되지 않은 별칭이 나열됩니다
- c. \* 스토리지 별칭 \* 은 Data Infrastructure Insights에서 식별해야 하는 스토리지 별칭 및 WWN을 나열합니다
- d. \* Switch alias \* 는 Data Infrastructure Insights에서 식별해야 하는 스위치 별칭을 나열합니다

5. Method\* 목록에서 호스트를 식별하기 위해 사용할 방법을 선택합니다.

출처	방법
SRM	As As As - 구분 기호, 정규식
스토리지 별칭입니다	구분 기호, 정규식
별칭 전환	구분 기호, 정규식
존	구분 기호, 정규식

◦ Delimiters를 사용하는 규칙에는 구분 기호 및 호스트 이름의 최소 길이가 필요합니다. 호스트 이름의 최소 길이는 Data Infrastructure Insights에서 호스트를 식별하는 데 사용해야 하는 문자 수입니다. Data Infrastructure Insights는 이 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_12ep0_`의 입력 슬링에 대해 다음과 같은 결과가 나타납니다.

- `vipsnq03_hba3_emcp3_12ep0`을 입력합니다
- `vipsnq03_hba3_emcp3`
- `hba3 emc3_12ep0`
- `vipsnq03_hba3`
- `emc3_12ep0`을 참조하십시오
- `hba3_emc3`
- `vipsnq03`
- `12ep0`
- `emc3`
- `hba3`

◦ 정규식을 사용하는 규칙에는 정규식, 형식 및 케이스 민감도 선택이 필요합니다.

6. AR 실행 \* 을 클릭하여 모든 규칙을 실행하거나, 버튼의 아래쪽 화살표를 클릭하여 생성한 규칙(그리고 AR의 마지막 전체 실행 이후 생성된 기타 규칙)을 실행합니다.

규칙 실행 결과는 \* FC Identify \* (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.

절차를 참조하십시오

1. Data Infrastructure Insights 웹 UI에 로그인합니다.
2. 관리 > 장치 해상도 \* 를 클릭합니다
3. 장치 해상도 \* 화면에서 \* AR 실행 \* 버튼의 아래쪽 화살표를 클릭합니다.
4. 업데이트를 시작하려면 \* 업데이트 \* 를 클릭합니다.

규칙 지원 수동 식별

이 기능은 특정 규칙 또는 규칙 목록(일회성 재정렬 포함 또는 제외)을 실행하여 알 수 없는 호스트, 스토리지 및 테이프 디바이스를 확인하려는 경우에 사용됩니다.

시작하기 전에

식별되지 않은 다수의 장치가 있고 다른 장치를 성공적으로 식별하는 여러 규칙이 있습니다.



소스에 호스트 또는 장치 이름의 일부만 포함되어 있는 경우 정규식 규칙을 사용하여 서식을 지정하여 누락된 텍스트를 추가합니다.

절차를 참조하십시오

1. Data Infrastructure Insights 웹 UI에 로그인합니다.
2. 관리 > 장치 해상도 \* 를 클릭합니다
3. 파이버 채널 식별 \* 탭을 클릭합니다.  
  
시스템은 해상도 상태와 함께 장치를 표시합니다.
4. 식별되지 않은 여러 장치를 선택합니다.
5. Bulk Actions \* 를 클릭하고 \* Set host resolution \* 또는 \* Set tape resolution \* 을 선택합니다.

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.

Data Infrastructure Insights는 호스트 해결 프로세스를 방법이 나타나는 순서대로, 맨 위에 있는 방법부터 시작합니다.

적용되는 규칙이 있으면 규칙 이름이 규칙 옆에 표시되고 수동으로 식별됩니다.



관련:"[파이버 채널 장치 해상도](#)"  
"[IP 장치 해상도](#)"  
"[장치 해상도 기본 설정 지정](#)"

## 파이버 채널 장치 해상도

Fibre Channel 식별 화면에는 호스트가 자동 디바이스 확인으로 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*의 상태가 포함되어 있으며 장치를 식별하는 데 사용되는 규칙을 식별합니다. 누락된 디바이스의 상태는 *\_Unidentified*입니다. 식별에서 특별히 제외된 장치는 *\_excluded* 상태입니다. 장치 식별의 총 범위는 이 페이지에 나와 있습니다.

Fibre Channel Identify(파이버 채널 식별) 화면의 왼쪽에 있는 여러 디바이스를 선택하여 대량 작업을 수행합니다. 장치 위로 마우스를 가져가서 목록 맨 오른쪽에 있는 *\_Identify\_or\_Unidentify\_buttons*를 선택하여 단일 장치에서 작업을 수행할 수 있습니다.

Total Coverage\_link는 구성에 사용할 수 있는 식별된 장치 수/장치 수를 목록으로 표시합니다.

- SRM 별칭
- 스토리지 별칭입니다
- 별칭 전환
- 존
- 사용자 정의

### Fibre Channel 디바이스를 수동으로 추가합니다

디바이스 해상도 Fibre Channel 식별 탭에서 사용할 수 있는 *Manual Add* 기능을 사용하여 Data Infrastructure Insights에 파이버 채널 디바이스를 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 파이버 채널 장치를 수동으로 추가할 수 있습니다.

절차를 참조하십시오

1. Data Infrastructure Insights 웹 UI에 로그인합니다
2. 관리 > 장치 해상도 \* 를 클릭합니다
3. 파이버 채널 식별 \* 탭을 클릭합니다.
4. 추가 \* 버튼을 클릭합니다.

장치 추가 \* 대화 상자가 표시됩니다

5. WWN 또는 IP 주소, 디바이스 이름을 입력하고 디바이스 유형을 선택합니다.

입력한 디바이스가 Fibre Channel Identify 탭의 디바이스 목록에 추가됩니다. 규칙은 `_Manual_`로 식별됩니다.

### CSV 파일에서 Fibre Channel 디바이스 ID 가져오기

CSV 파일의 장치 목록을 사용하여 파이버 채널 장치 ID를 Data Infrastructure Insights 장치 해상도로 수동으로 가져올 수 있습니다.

#### 1. 시작하기 전에

장치 식별 정보를 장치 해상도로 직접 가져오려면 올바른 형식의 .csv 파일이 있어야 합니다. 파이버 채널 장치용 .csv 파일에는 다음 정보가 필요합니다.

WWN입니다	IP	이름	유형
--------	----	----	----

데이터 필드는 아래 예와 같이 따옴표로 묶어야 합니다.

```
"WWN", "IP", "Name", "Type"  
"WWN:2693", "ADDRESS2693 | IP2693", "NAME-2693", "HOST"  
"WWN:997", "ADDRESS997 | IP997", "NAME-997", "HOST"  
"WWN:1860", "ADDRESS1860 | IP1860", "NAME-1860", "HOST"
```



가장 좋은 방법은 먼저 Fibre Channel 식별 정보를 .csv 파일로 내보내고, 해당 파일을 원하는 대로 변경한 다음 파일을 다시 Fibre Channel Identify로 가져오는 것입니다. 이렇게 하면 예상 열이 올바른 순서로 표시됩니다.

Fibre Channel 식별 정보를 가져오려면 다음을 수행합니다.

1. Data Infrastructure Insights 웹 UI에 로그인합니다.
2. 관리 > 장치 해상도 \* 를 클릭합니다
3. 파이버 채널 식별 \* 탭을 선택합니다.
4. Identify(식별) > Identify from file(파일에서 식별) \* 버튼을 클릭합니다.
5. 가져올 .csv 파일이 들어 있는 폴더로 이동하고 원하는 파일을 선택합니다.

입력한 디바이스가 Fibre Channel Identify 탭의 디바이스 목록에 추가됩니다. "규칙"은 수동으로 식별됩니다.

### Fibre Channel 디바이스 식별 정보를 .csv 파일로 내보내는 중입니다

Data Infrastructure Insights 장치 해상도 기능에서 기존 파이버 채널 장치 ID를 .csv 파일로 내보낼 수 있습니다. 장치 ID를 수정하여 Data Infrastructure Insights로 다시 가져온 다음 내보낸 ID와 원래 일치하는 장치와 유사한 장치를 식별하는 데 사용할 수 있도록 장치 ID를 내보낼 수 있습니다.


이 작업에 대해

이 시나리오에는 .csv 파일에서 쉽게 편집한 다음 시스템으로 다시 가져올 수 있는 유사한 속성이 장치에 있는 경우에 사용할 수 있습니다.

Fibre Channel 디바이스 ID를 .csv 파일로 내보낼 때 파일에는 다음 정보가 표시된 순서대로 포함됩니다.

WWN입니다	IP	이름	유형
--------	----	----	----

절차를 참조하십시오

1. Data Infrastructure Insights 웹 UI에 로그인합니다.
2. 관리 > 장치 해상도 \* 를 클릭합니다
3. 파이버 채널 식별 \* 탭을 선택합니다.
4. ID를 내보낼 Fibre Channel 디바이스를 선택합니다.
5. 내보내기 \* 를 클릭합니다  단추를 클릭합니다.

CSV 파일을 열 것인지 파일을 저장할 것인지 선택합니다.

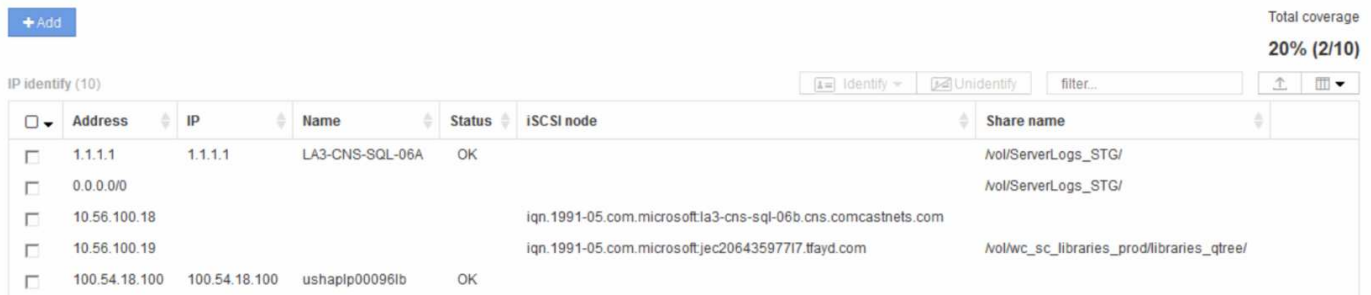
관련:"IP 장치 해상도"

"장치 해상도 규칙을 만드는 중입니다"

"장치 해상도 기본 설정 지정"

## 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.



<input type="checkbox"/>	Address	IP	Name	Status	iSCSI node	Share name
<input type="checkbox"/>	1.1.1.1	1.1.1.1	LA3-CNS-SQL-06A	OK		/vol/ServerLogs_STG/
<input type="checkbox"/>	0.0.0.0/0					/vol/ServerLogs_STG/
<input type="checkbox"/>	10.56.100.18				iqn.1991-05.com.microsoft:ia3-cns-sql-06b.cns.comcastnets.com	
<input type="checkbox"/>	10.56.100.19				iqn.1991-05.com.microsoft:jec20643597717.tfyd.com	/vol/wc_sc_libraries_prod/libraries_qtree/
<input type="checkbox"/>	100.54.18.100	100.54.18.100	ushapl00096ib	OK		

### 수동으로 IP 장치 추가

IP 식별 화면에서 사용할 수 있는 수동 추가 기능을 사용하여 Data Infrastructure Insights에 IP 장치를 수동으로 추가할 수 있습니다.

절차를 참조하십시오

1. Data Infrastructure Insights 웹 UI에 로그인합니다.
2. 관리 > 장치 해상도 \* 를 클릭합니다
3. IP 주소 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 주소 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.

#### 1. 시작하기 전에

장치 식별 정보를 장치 해상도 기능으로 직접 가져오려면 올바른 형식의 .csv 파일이 있어야 합니다. IP 장치용 .csv 파일에는 다음 정보가 필요합니다.

주소	IP	이름
----	----	----

데이터 필드는 아래 예와 같이 따옴표로 묶어야 합니다.

```
"Address", "IP", "Name"
"ADDRESS6447", "IP6447", "NAME-6447"
"ADDRESS3211", "IP3211", "NAME-3211"
"ADDRESS593", "IP593", "NAME-593"
```



가장 좋은 방법은 먼저 IP 주소 식별 정보를 .csv 파일로 내보내고 해당 파일에서 원하는 대로 변경한 다음 파일을 다시 IP 주소 식별로 가져오는 것입니다. 이렇게 하면 예상 열이 올바른 순서로 표시됩니다.

### IP 장치 ID를 .csv 파일로 내보내는 중입니다

Data Infrastructure Insights 장치 해상도 기능에서 기존 IP 장치 ID를 .csv 파일로 내보낼 수 있습니다. 장치 ID를 수정하여 Data Infrastructure Insights로 다시 가져온 다음 내보낸 ID와 원래 일치하는 장치와 유사한 장치를 식별하는 데 사용할 수 있도록 장치 ID를 내보낼 수 있습니다.

이 작업에 대해

1. 이 시나리오는 .csv 파일에서 쉽게 편집한 다음 시스템으로 다시 가져올 수 있는 유사한 속성이 장치에 있는 경우에 사용할 수 있습니다.

IP 장치 ID를 .csv 파일로 내보낼 때 파일은 다음 정보를 표시된 순서대로 포함합니다.

주소	IP	이름
----	----	----

절차를 참조하십시오

1. Data Infrastructure Insights 웹 UI에 로그인합니다.
2. 관리 > 장치 해상도 \* 를 클릭합니다
3. IP 주소 식별 \* 탭을 선택합니다.
4. ID를 내보내려는 IP 장치 또는 장치를 선택합니다.
5. 내보내기 \* 를 클릭합니다 단추를 클릭합니다.

CSV 파일을 열 것인지 파일을 저장할 것인지 선택합니다.

관련: "파이버 채널 장치 해상도"  
"장치 해상도 규칙을 만드는 중입니다"  
"장치 해상도 기본 설정 지정"

## 기본 설정 탭에서 옵션 설정

장치 해상도 기본 설정 탭에서는 자동 해결 일정을 생성하고, 식별에서 포함하거나 제외할 스토리지 및 테이프 벤더를 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.

\_manually\_를 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.
- IP 자동 확인: 을 선택하여 DNS 조회를 사용하여 NFS 공유에 액세스하는 iSCSI 이니시에이터 및 호스트에 대해 자동 호스트 확인을 활성화할 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 `_Tape Only_`로 설정된 WWN에만 적용됩니다.

참고 항목: "정규식 예제"

## 정규식 예

정규식 방법을 소스 명명 전략으로 선택한 경우 정규식 예제를 Data Infrastructure Insights 자동 해결 방법에 사용되는 고유한 식에 대한 가이드로 사용할 수 있습니다.

### 정규식 서식 지정

Data Infrastructure Insights 자동 확인에 대한 정규식을 만들 때 *format* 필드에 값을 입력하여 출력 형식을 구성할 수 있습니다.

기본 설정은 \1입니다. 즉, 정규식과 일치하는 영역 이름이 정규식에서 만든 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. 형식 필드에 상수 텍스트를 추가하여 출력에 상수 텍스트를 삽입할 수도 있습니다.

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]+)_.*
괄호 세 세트가 있으므로 변수 \1, \2 및 \3이 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.

예

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 \*<sub>1</sub>\* 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 <sub>1</sub> 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 건너뜁니다.

- 영역: \*Z\_E2FHDBS01\_E1NETAPP
- 호스트 이름: \*E2FHDBS01
- RegExp: \*. \*?\_(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

- 존: `* A_VSAN3_SR48KENT_A_CX2578_SPA0`
- 호스트 이름: `* SR48KENT`
- RegExp: `* _[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]*)_.*
```

이 식으로 계산한 후 \1 변수는 `_myComputerName123_`만 포함합니다.

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 `AT`로 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 `T`여야 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

- Zone: \* myComputerName123\_HBA1\_Symm1\_FA1
- 호스트 이름: \* myComputerName123
- RegExp: \* ([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

RegExp:(. \*) \_.\*

예 9

이 예제에서는 1\_ 이후의 모든 것과 두 번째 \_ 까지의 모든 것을 찾습니다.

- 영역: \* Z\_MyComputerName\_StorageName
- 호스트 이름: \* MyComputerName
- RegExp: \*. \*?\_(. \*) \_.\*?

예 10

이 예제에서는 영역 예제에서 "MyComputerName123"을 추출합니다.

- 존: \* storage1\_Switch1\_MyComputerName123A\_A1\_FC1

storage2\_Switch2\_MyComputerName123B\_A2\_FC2 를 참조하십시오

storage3\_Switch3\_MyComputerName123T\_A3\_FC3

- 호스트 이름: \* MyComputerName123
- RegExp: \*. \*?.\*?([a-zA-Z0-9]+) \* [ABT].\*

#### 예 11

- 존: \* storage1\_Switch1\_MyComputerName123A\_A1\_FC1
- 호스트 이름: \* MyComputerName123A
- RegExp: \*. \*?. \*?\_([a-zA-Z0-9]+)\_.\*? \_

#### 예 12

^(circumflex 또는 caret) \* 대괄호 안에 \* \* 는 식을 부정합니다. 예를 들어 [^FF]는 대문자 또는 소문자 F를 제외한 모든 것을 의미하고 [^a-z]는 소문자 a ~ z를 제외한 모든 것을 의미합니다. 위의 경우 \_ 을 제외한 모든 내용을 의미합니다. format 문은 출력 호스트 이름에 "-"를 추가합니다.

- 존: \* MHS\_apps44\_d\_a\_10a0\_0429
- 호스트 이름: \* MHS-apps44-d
- RegExp: \* () \_ ([AB]). \* 데이터 인프라 통찰력의 형식:\1-\2([\ ])\_([\ ]). \* 데이터 인프라 통찰력의 형식:\1-\2-\3

#### 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\EDOC01C1\EDOC01N1
- 호스트 이름: \* E2801N1
- RegExp: \* \\. \*?. \*?\\. \*?\. \*?)

#### 예 14

이 예에서는 영역 예에서 "PD-RV-W-AD-2"를 추출합니다.

- 존: \* PD\_D-PD-RV-W-AD-2\_01
- 호스트 이름: \* PD-RV-W-AD-2
- RegExp: \* -(.\*-ld). \*

#### 예 15

이 경우 형식 설정은 호스트 이름에 "US-BV-"를 추가합니다.

- 영역: \* SRV\_USBVM11\_F1
- 호스트 이름: \* US-BV-M11
- RegExp: \* SRV\_USBV([A-Za-Z0-9]+)\_F[12]
- 형식: \* US-BV-\1

## 자산 페이지 정보

## 자산 페이지 개요

자산 페이지는 자산의 현재 상태를 요약하고 자산 및 관련 자산에 대한 추가 정보에 대한 링크를 포함합니다.

### 자산 페이지 유형

Data Infrastructure Insights는 다음 자산에 대한 자산 페이지를 제공합니다.

- 가상 머신
- 스토리지 가상 시스템(SVM)
- 볼륨
- 내부 볼륨
- 호스트(하이퍼바이저 포함)
- 스토리지 풀
- 스토리지
- 데이터 저장소
- 응용 프로그램
- 스토리지 노드
- qtree입니다
- 디스크
- VMDK입니다
- 포트
- 스위치
- 패브릭

표시된 데이터의 시간 범위를 변경합니다

기본적으로 자산 페이지에는 지난 24시간 동안의 데이터가 표시되지만 표시되는 데이터 세그먼트는 다른 고정 시간 범위 또는 사용자 지정 시간 범위를 선택하여 변경하거나 더 적은 데이터 또는 더 많은 데이터를 볼 수 있습니다.

자산 유형에 관계없이 모든 자산 페이지에 있는 옵션을 사용하여 표시된 데이터의 시간 세그먼트를 변경할 수 있습니다. 시간 범위를 변경하려면 상단 표시줄에 표시된 시간 범위를 클릭하고 다음 시간 세그먼트 중에서 선택합니다.

- 최근 15분
- 마지막 30분
- 마지막 60분
- 최근 2시간
- 최근 3시간(기본값)
- 최근 6시간

- 최근 12시간
- 최근 24시간
- 최근 2일
- 지난 3일
- 최근 7일
- 지난 30일
- 사용자 지정 시간 범위

사용자 지정 시간 범위를 사용하면 최대 31일 연속 선택할 수 있습니다. 이 범위에 대한 시작 시간 및 종료 시간을 설정할 수도 있습니다. 기본 시작 시간은 선택한 첫 번째 날짜의 오전 12:00이고 기본 종료 시간은 선택한 마지막 날짜의 오후 11:59입니다. 적용 을 클릭하면 자산 페이지에 사용자 지정 시간 범위가 적용됩니다.

자산 페이지 요약 섹션뿐 아니라 페이지의 모든 테이블 또는 사용자 정의 위젯에 있는 정보는 선택한 시간 범위에 따라 자동으로 새로 고쳐집니다. 현재 새로 고침 빈도는 요약 섹션의 오른쪽 상단 모서리와 페이지의 관련 테이블 또는 위젯에 표시됩니다.

사용자 지정 위젯을 추가합니다

자체 위젯을 모든 자산 페이지에 추가할 수 있습니다. 추가한 위젯은 해당 유형의 모든 객체에 대한 자산 페이지에 표시됩니다. 예를 들어 스토리지 자산 페이지에 사용자 지정 위젯을 추가하면 모든 스토리지 자산에 대한 자산 페이지에 해당 위젯이 표시됩니다.

## Objects In-Context의 필터링입니다

자산의 랜딩 페이지에서 위젯을 구성할 때 `_in-context_filters`를 설정하여 현재 자산과 직접 관련된 객체만 표시할 수 있습니다. 기본적으로 위젯을 추가하면 환경에서 선택한 유형의 `_ALL_OBJECTS`가 표시됩니다. 상황 내 필터를 사용하면 현재 자산과 관련된 데이터만 표시할 수 있습니다.

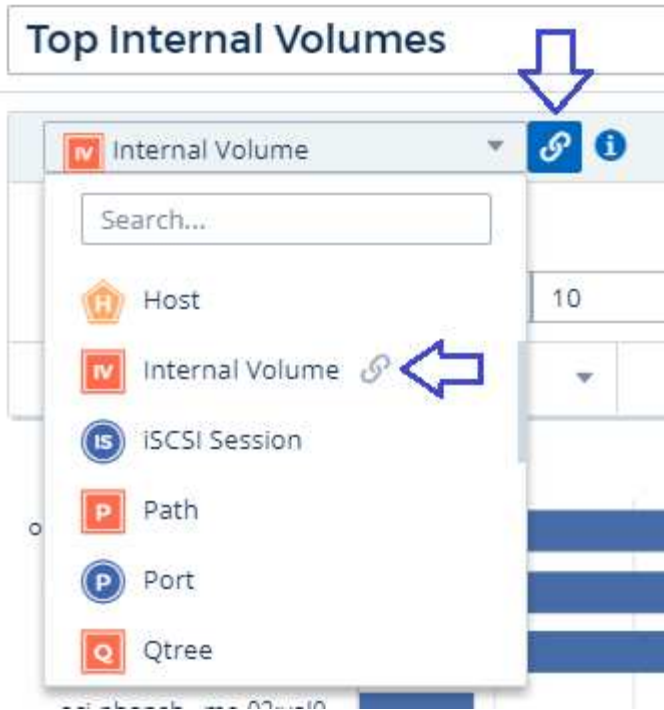
대부분의 자산 랜딩 페이지에서 위젯을 사용하여 현재 자산과 관련된 개체를 필터링할 수 있습니다. 필터 드롭다운에서 링크 아이콘을 표시하는 개체 유형을 컨텍스트에 따라 현재 자산으로 필터링할 수 있습니다.

예를 들어 스토리지 자산 페이지에서 막대 차트 위젯을 추가하여 해당 스토리지에서만 내부 볼륨의 상위 IOPS를 표시할 수 있습니다. 기본적으로 위젯을 추가하면 환경에 `_ALL_INTERNAL` 볼륨이 표시됩니다.

현재 스토리지 자산의 내부 볼륨만 표시하려면 다음을 수행합니다.

단계

1. 모든 \* 스토리지 \* 자산에 대한 자산 페이지를 엽니다.
2. Edit[편집] \* 를 클릭하여 Edit[편집] 모드에서 자산 페이지를 엽니다.
3. Add Widget \* 을 클릭하고 `_Bar Chart_`를 선택합니다.
4. 막대 차트에 표시할 개체 유형에 대해 \* 내부 볼륨 \* 을 선택합니다. 내부 볼륨 개체 유형 옆에 링크 아이콘이 있습니다. "Linked(연결됨)" 아이콘은 기본적으로 활성화되어 있습니다.



5. IOPS - Total \_ 을 선택하고 원하는 추가 필터를 설정합니다.
6. 옆에 있는 [X]를 클릭하여 \* 롤업 \* 필드를 축소합니다. Show \* (표시 \*) 필드가 표시됩니다.
7. 상위 10개 표시를 선택합니다.
8. 위젯을 저장합니다.

막대 차트에는 현재 스토리지 자산에 있는 내부 볼륨만 표시됩니다.

위젯이 모든 스토리지 객체의 자산 페이지에 표시됩니다. 위젯에서 상황 내 링크가 활성화된 경우 막대 차트는 현재 표시된 스토리지 자산에만 관련된 내부 볼륨에 대한 데이터를 표시합니다.

개체 데이터의 연결을 해제하려면 위젯을 편집하고 개체 유형 옆에 있는 링크 아이콘을 클릭합니다. 링크가 비활성화되고 해당 환경의 \_ALL\_objects에 대한 데이터가 차트에 표시됩니다.

을 사용할 수도 있습니다 "위젯 \* 의 특수 변수" 랜딩 페이지에 자산 관련 정보를 표시합니다.

## 자산 페이지 요약 섹션

자산 페이지의 요약 섹션에는 메트릭이나 성능 정책이 우려할 만한 원인인지 여부를 비롯한 자산에 대한 일반 정보가 표시됩니다. 잠재적 문제 영역은 빨간색 원으로 표시됩니다.

요약 섹션의 정보는 물론 자산 페이지의 모든 테이블 또는 사용자 정의 위젯에서 선택한 시간 범위에 따라 자동으로 새로 고쳐집니다. 요약 섹션, 표 및 모든 사용자 지정 위젯의 오른쪽 위 모서리에 현재 새로 고침 빈도가 표시됩니다.

## Virtual Machine Summary

5m

### Power State:

On

### Guest State:

Running

### Datastore:

[i-00cc58b5c47a69271](#)

### CPU Utilization - Total:

13.82 %

### Memory Utilization - Total:

N/A

### Memory:

32.0 GB

### Capacity - Total:

200.0 GB

### Capacity - Used:

N/A

### Latency - Total:

6.35 ms

### IOPS - Total:

 316.59 IO/s

### Throughput - Total:

68.81 MB/s

### DNS Name:

ip-10-30-23-12.ec2.internal

### IP:

10.30.23.12

### OS:

CentOS Linux 7 x86\_64 HVM  
EBS ENA 1901\_01-b7ee8a69-  
ee97-4a49-9e68-afaae216db2e-  
ami-05713873c6794f575.4  
x86\_64

### Processors:

8

### Hypervisor Name:

us-east-1a

### Hypervisor IP:

US-EAST-1A-052113251141

### Hypervisor OS:

Amazon AWS EC2

### Hypervisor FC Fabrics:

0

### Hypervisor CPU Utilization:

N/A

### Hypervisor Memory

#### Utilization:

N/A

### Alert Monitors:

[High Latency VMs](#)

[Instance CPU Under-utilized](#)

[View Topology](#)

참고: 요약 섹션에 표시되는 정보는 보고 있는 자산의 유형에 따라 달라집니다.

자산 링크를 클릭하여 자산 페이지를 볼 수 있습니다. 예를 들어 스토리지 노드를 보는 경우 링크를 클릭하여 연결된 스토리지의 자산 페이지를 볼 수 있습니다.

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.

해당하는 경우 경고 링크를 클릭하여 자산과 관련된 경고 및 모니터를 볼 수 있습니다.

### 토폴로지

특정 자산 페이지의 요약 섹션에는 자산 토폴로지 및 해당 연결을 볼 수 있는 링크가 포함되어 있습니다.

토폴로지는 다음 자산 유형에 사용할 수 있습니다.

- 응용 프로그램

- 디스크
- 패브릭
- 호스트
- 내부 볼륨
- 포트
- 스위치
- 가상 머신
- VMDK입니다
- 볼륨

**Internal Volume**

Storage: [barbados1,barbados2](#)

Storage Pool: [barbados1.agg1](#)

Status: Online

Type: FlexVol

UUID:

SVM/vfiler: vfiler0

Capacity - Total: 1.0 GB

Capacity - Used: 0.0 GB

Snapshot: <0.1 GB

Latency - Total: 0.02 ms

Storage Pool Utilization: 0.68 %

IOPS - Total: 0.13 IO/s

Datstore:

Deduplication Savings: 0.0 %

Thin Provisioned: No

Replication Source(s):

Performance Policies: [Find High Latency FlexVols](#)

[View Topology](#)

**Topology**

ocise-esx-1431... → NAS → barbados1,bar...

Close

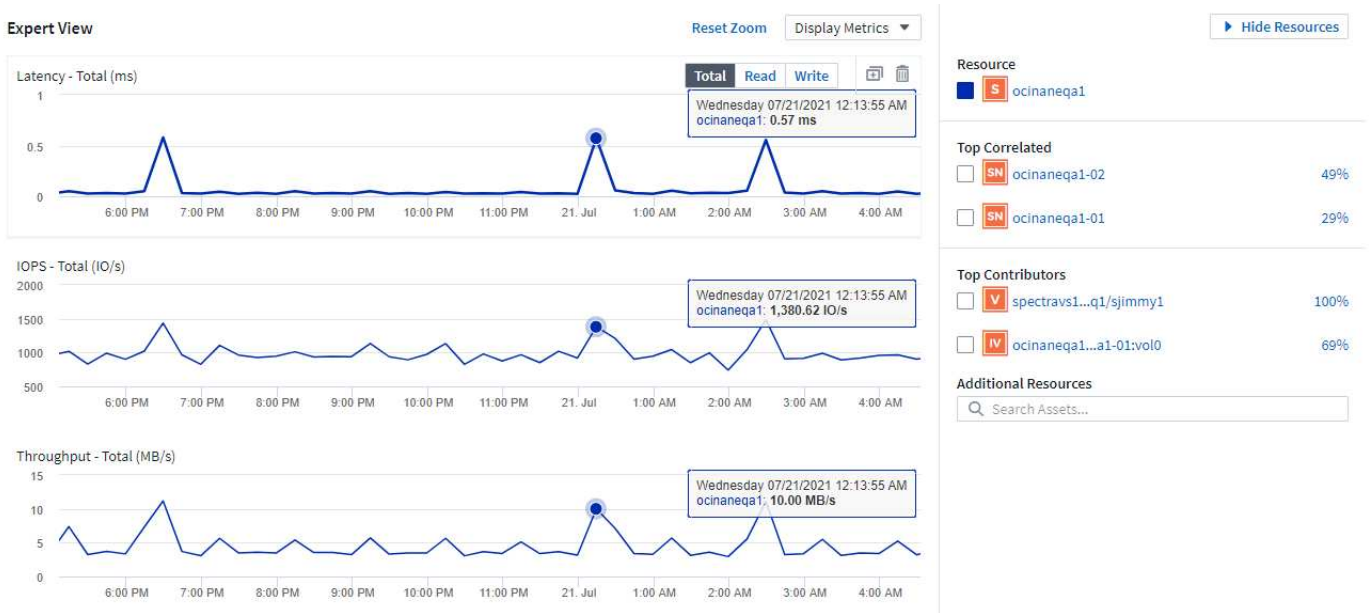
## 전문가 뷰

자산 페이지의 전문가 보기 섹션을 사용하면 성능 차트 및 관련 자산에 선택한 기간이 있는 컨텍스트에서 적용 가능한 모든 메트릭에 따라 기본 자산의 성능 샘플을 볼 수 있습니다. 데이터 수집기가 폴링 및 업데이트된 데이터를 획득하면 차트의 데이터가 자동으로 새로 고쳐집니다.



전문가 보기 섹션을 사용합니다

다음은 스토리지 자산 페이지의 전문가 보기 섹션의 예입니다.



선택한 기간의 성능 차트에서 확인할 메트릭을 선택할 수 있습니다. Display Metrics \_ 드롭다운을 클릭하고 나열된 메트릭 중에서 선택합니다.

Resources\* 섹션에는 기본 자산의 이름과 성능 차트의 기본 자산을 나타내는 색상이 표시됩니다. 성능 차트에서 보려는 자산이 \* 상위 상관 관계 \* 섹션에 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.

- 워크로드 보존

에는 호스트, 네트워크 및 스토리지와 같은 다른 공유 리소스에 영향을 미치거나 영향을 받는 자산이 나와 있습니다. 이러한 리소스를 `_greedy_and_degraded_resources` 라고 합니다.

### 전문가 보기의 알림

알림은 자산 랜딩 페이지의 전문가 보기 섹션에도 표시됩니다. 여기에는 알림의 시간과 지속 시간, 알림을 트리거한 모니터 조건이 표시됩니다.



### 전문가 뷰 메트릭 정의

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. 선택할 수 있는 메트릭은 자산 유형에 따라 다릅니다.

* 미터법 *	* 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 깁니다	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)	총계: 초당 메가바이트 단위의 IP 데이터가 전송 및 수신된 총 속도입니다.
읽기:IP 처리량(수신):	IP 데이터가 수신된 평균 속도(MB/초)입니다.
쓰기:IP 처리량(전송):	IP 데이터가 전송된 평균 속도(MB/초)입니다.
지연 시간(총, 읽기, 쓰기)	지연 시간(R&W): 고정된 시간 내에 데이터를 가상 시스템에 읽거나 쓰는 비율. 이 값은 초당 메가바이트로 측정됩니다.
지연 시간:	데이터 저장소에 있는 가상 머신의 평균 응답 시간입니다.
최고 지연 시간:	데이터 저장소의 가상 시스템에서 가장 높은 응답 시간입니다.
링크 실패	샘플링 기간 동안 포트에서 감지된 링크 장애 수입입니다.
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) %	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 불륨 (또는 NetApp LUN)이 잘못 정렬되었음을 나타냅니다. CLARiX의 경우 이 값은 총 IOPS 수로 나눈 스트라이프 크로싱 수입입니다.
포트 오류	샘플링 기간/지정된 기간 동안의 포트 오류 보고.
신호 손실 카운트	신호 손실 오류 수입입니다. 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 수입입니다. 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 수입입니다.

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. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.

- 특정 자산을 검색하여 선택합니다.
- 대시보드 위젯에서 자산을 선택합니다.
- 자산 집합을 쿼리하고 결과 목록에서 하나를 선택합니다.

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. 이러한 섹션과 관련된 자산이 없으면 표시되지 않습니다.

2. 메트릭 표시 \* 를 클릭하고 표시할 메트릭을 선택하여 메트릭에 대한 성능 차트를 추가할 수 있습니다.

선택한 각 메트릭에 대해 별도의 차트가 표시됩니다. 선택한 기간의 데이터가 차트에 표시됩니다. 자산 페이지의 오른쪽 위 모서리에 있는 다른 기간을 클릭하거나 차트를 확대하여 기간을 변경할 수 있습니다.

메트릭 표시 \* 를 클릭하여 차트를 선택 취소합니다. 메트릭에 대한 성능 차트가 전문가 보기에서 제거됩니다.

3. 자산에 따라 다음 중 하나를 클릭하여 차트 위에 커서를 놓고 해당 차트에 표시되는 메트릭 데이터를 변경할 수 있습니다.

- 읽기, 쓰기 또는 합계 를 선택합니다
- TX, Rx 또는 Total

기본값은 합계입니다.

선택한 기간 동안 메트릭 값이 어떻게 변경되는지 확인하려면 차트의 데이터 요소 위로 커서를 끌어다 놓습니다.

4. 자원 섹션에서는 성능 차트에 관련 자산을 추가할 수 있습니다.

- Top Correlated \*, \* Top Contributor \*, \* greedy \* 및 \* Degraded \* 섹션에서 관련 자산을 선택하여 해당 자산의 데이터를 선택한 각 메트릭의 성능 차트에 추가할 수 있습니다.

자산을 선택하면 자산 옆에 색상 블록이 표시되어 차트의 데이터 요소 색상을 나타냅니다.

5. 추가 자원 창을 숨기려면 \* 리소스 숨기기 \* 를 클릭합니다. Resources \* 를 클릭하여 창을 표시합니다.

- 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 보지 않으려면 휴지통 아이콘을 클릭하여 삭제합니다.

## 사용자 데이터 섹션

자산 페이지의 사용자 데이터 섹션이 표시되고 응용 프로그램 및 주식과 같은 사용자 정의 데이터를 변경할 수 있습니다.

사용자 데이터 섹션을 사용하여 응용 프로그램을 할당하거나 수정합니다

사용자 환경에서 실행 중인 애플리케이션을 특정 자산(호스트, 가상 머신, 볼륨, 내부 볼륨, Qtree, 있습니다. 사용자 데이터 섹션을 사용하면 자산에 할당된 애플리케이션을 추가, 변경 또는 제거할 수 있습니다. 볼륨을 제외한 이러한 모든 자산 유형에 대해 둘 이상의 애플리케이션을 할당할 수 있습니다.

단계

1. 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
  - a. 자산 목록을 쿼리한 다음 목록에서 하나를 선택합니다.
  - b. 대시보드에서 자산 이름을 찾아 클릭합니다.
  - c. 검색을 수행하고 결과에서 자산을 선택합니다.

자산 페이지가 표시됩니다. 페이지의 사용자 데이터 섹션에는 현재 할당된 응용 프로그램 또는 주식이 표시됩니다.

할당된 응용 프로그램을 변경하거나 응용 프로그램 또는 추가 응용 프로그램을 할당하려면 \* 응용 프로그램 \* 목록을 드롭다운하여 자산에 할당할 응용 프로그램을 선택합니다. 을 입력하여 응용 프로그램을 검색하거나 목록에서 하나를 선택할 수 있습니다.

응용 프로그램을 제거하려면 응용 프로그램 목록을 드롭다운하고 응용 프로그램을 선택 취소합니다.

**User Data(사용자 데이터)** 섹션을 사용하여 주석을 할당하거나 수정합니다

Data Infrastructure Insights를 사용자 정의하여 회사 요구사항에 대한 데이터를 추적할 때 주식이라는 특수 메모를 정의하고 자산에 할당할 수 있습니다. 자산 페이지의 사용자 데이터 섹션에는 자산에 할당된 주석이 표시되며 해당 자산에 할당된 주석을 변경할 수도 있습니다.

단계

1. 자산에 주석을 추가하려면 자산 페이지의 사용자 데이터 섹션에서 \* + 주식 \* 을 클릭합니다.
2. 목록에서 주석을 선택합니다.

3. 값을 클릭하고 선택한 주식 유형에 따라 다음 중 하나를 수행합니다.
  - a. 주식 유형이 목록, 날짜 또는 부울인 경우 목록에서 값을 선택합니다.
  - b. 주식 유형이 텍스트인 경우 값을 입력합니다.
4. 저장 을 클릭합니다.

주식이 자산에 할당됩니다. 나중에 쿼리를 사용하여 주식을 기준으로 자산을 필터링할 수 있습니다.

주석을 지정한 후 주식 값을 변경하려면 주식 목록을 드롭다운하고 다른 값을 입력합니다.

fly\_option에서 Add new values를 선택한 목록 유형의 주식인 경우 기존 값을 선택하는 것 외에도 새 값을 추가하도록 입력할 수 있습니다.

## 자산 페이지 관련 경고 섹션

자산 페이지의 관련 경고 섹션을 사용하면 자산에 할당된 모니터로 인해 사용자 환경에서 발생하는 모든 경고를 볼 수 있습니다. 모니터는 사용자가 설정한 조건에 따라 알림을 생성하며, 이를 통해 영향을 파악하고 문제의 영향과 근본 원인을 빠르고 효과적으로 수정할 수 있습니다.

다음 예에서는 자산 페이지에 표시되는 일반적인 관련 경고 섹션을 보여 줍니다.

**Related Alerts** ⋮

16 items found

Alert ID	Active Status	Triggered Time ↓	Top Severity	Monitor	Triggered On	Status
AL-146777	Resolved	5 minutes ago Jul 28, 2021 4:01 PM	Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146748	Resolved	11 minutes ago Jul 28, 2021 3:55 PM	Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146711	Resolved	23 minutes ago Jul 28, 2021 3:43 PM	Critical	Workload IOPS	workload_volume_name: podAuVol-wid12074	New
AL-146704	Resolved	25 minutes ago	Warning	Workload IOPS	workload_volume_name: podAuVol-wid12074	New

관련 경고 섹션에서는 자산에 할당된 모니터 조건의 결과로 네트워크에서 발생하는 경고를 보고 관리할 수 있습니다.

### 단계

- 다음 중 하나를 수행하여 자산 페이지를 찾습니다.
  - Search(검색) 영역에 자산 이름을 입력한 다음 목록에서 자산을 선택합니다.
  - 대시보드 위젯에서 자산 이름을 클릭합니다.
  - 자산 집합을 쿼리하고 결과 목록에서 On을 선택합니다.

자산 페이지가 표시됩니다. 관련 경고 섹션에는 알림이 트리거된 시간과 경고의 현재 상태 및 경고를 트리거한 모니터가 표시됩니다. 경고 ID를 클릭하여 추가 조사를 위한 경고의 랜딩 페이지를 열 수 있습니다.

## 스토리지 가상화

Data Infrastructure Insights는 로컬 스토리지가 있는 스토리지 어레이 또는 다른 스토리지 어레이의 가상화를 통해 구분할 수 있습니다. 이를 통해 비용을 관련시키고 프런트 엔드와 성능을 인프라 백 엔드와 구별할 수 있습니다.

## Table Widget의 가상화

스토리지 가상화를 확인하는 가장 쉬운 방법 중 하나는 가상화된 유형을 보여주는 대시보드 표 위젯을 생성하는 것입니다. 위젯에 대한 쿼리를 작성할 때 "virtualizedType"을 그룹화 또는 필터에 추가하기만 하면 됩니다.

Storage X ▾

Display Last 3 Hours (Dashboard Time) ▾  Override Dashboard Time

Filter by Attribute +

Filter by Metric +

Group by virtualizedType X ▾

결과 테이블 위젯은 사용자 환경의 *Standard*, *Backend* 및 *\_Virtual\_storages*를 보여 줍니다.

### Storage by virtualizedType

50 items found in 4 groups

virtualizedType ↑	Storage
Backend (5)	--
Backend	Sym-Perf
Backend	Sym-000050074300343
Backend	CX600_26_CK00351029326
Backend	VNX8000_46_CK00351029346
Backend	Sym-000050074300324
Standard (36)	--
Virtual (8)	--

랜딩 페이지에는 가상화된 정보가 표시됩니다

스토리지, 볼륨, 내부 볼륨 또는 디스크 랜딩 페이지에서는 관련 가상화 정보를 볼 수 있습니다. 예를 들어 아래 스토리지 랜딩 페이지에서 이 스토리지가 가상 스토리지이며 적용되는 백엔드 스토리지 시스템임을 확인할 수 있습니다. 랜딩 페이지의 관련 테이블에도 해당하는 가상화 정보가 표시됩니다.

## Storage Summary

Model:  
V-Series

Vendor:  
NetApp

Family:  
V-Series

Serial Number:  
1306894

IP:  
192.168.7.41

Virtualized Type:  
Virtual

Backend Storage:  
Sym-000050074300343

Microcode Version:  
8.0.2 7-Mode

Raw Capacity:  
0.0 GiB

Latency - Total:  
N/A

IOPS - Total:  
N/A

Throughput - Total:  
N/A

Management:

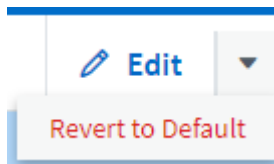
FC Fabrics Connected:  
7

Alert Monitors:

기존 랜딩 페이지 및 대시보드

현재 환경에 사용자 지정된 랜딩 페이지 또는 대시보드가 있는 경우 기본적으로 모든 가상화 정보가 자동으로 표시되지 않습니다. 그러나 사용자 지정 대시보드 또는 랜딩 페이지(사용자 지정 내용을 다시 구현해야 함)를 `_Default_Any`로 되돌리거나 원하는 가상화 특성 또는 메트릭을 포함하도록 관련 위젯을 수정할 수 있습니다.

`_기본값으로 되돌리기_`는 사용자 지정 대시보드 또는 랜딩 페이지 화면의 오른쪽 상단에서 사용할 수 있습니다.



## 자산 및 경고 검색을 위한 힌트 및 팁

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 `_application_`을 반환합니다.

### \* 검색에 사용되는 구 \*

구문은 "VNX LUN 5"와 같이 큰따옴표로 묶은 단어 그룹입니다. 큰따옴표를 사용하여 이름이나 속성에 공백이 포함된 문서를 검색할 수 있습니다.

### \* 부울 연산자 \*

부울 연산자 또는 AND, NOT를 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, `_storage` 또는 `netapp` 은(는) `_storage` \_ 또는 `_NetApp` \_ 이(가) 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, `_storage` 및 `netapp`은 `_storage`와 `_NetApp`이 둘 다 포함된 문서를 검색합니다.

단어 및 대신 `* & *` 기호를 사용할 수 있습니다.

아닙니다

NOT 연산자를 사용하면 NOT가 포함된 모든 문서가 검색 결과에서 제외됩니다. 예를 들어, `storage not NetApp` 은(는) `_storage`만 포함되어 있고 `_NetApp`은 포함하지 않는 문서를 검색합니다.

NOT 단어 대신 `!* *` 기호를 사용할 수 있습니다.

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"의 세 가지 키워드로 분할됩니다. 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 모델별로 스토리지를 검색할 수 있습니다.

UI는 범주 별로 검색 결과를 표시하며 범주 당 상위 3개 결과를 표시합니다. 예상한 개체를 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	"스토리지" 네임 공급업체 모델
스토리지 풀	"storagepool" 이름 스토리지 공급업체 스토리지 모델 이름에 대한 스토리지 일련 번호의 스토리지 IP 주소 모든 연결된 디스크의 모든 내부 볼륨 이름에 대한 이름입니다
내부 볼륨	스토리지 공급업체의 스토리지 일련 번호 스토리지 풀 이름에 대한 스토리지 IP 주소의 "내부 볼륨" 이름입니다. 연결된 모든 애플리케이션의 모든 공유 이름에 대한 스토리지 풀 이름입니다
볼륨	스토리지 공급업체 스토리지 모델의 스토리지 IP 주소에 대한 스토리지 풀 이름의 모든 내부 볼륨 이름 "volume" 이름 레이블 이름입니다
스토리지 노드	스토리지 공급업체 스토리지 모델의 스토리지 일련 번호에 대한 스토리지 IP 주소의 "storagenode" 이름입니다

범주	인덱싱된 용어
호스트	"호스트" 이름 IP는 연결된 모든 애플리케이션의 이름을 지정합니다
데이터 저장소	"datastore" name virtual center IP name of all volumes names of all internal volumes
가상 머신	"VirtualMachine" 이름 DNS 이름 IP 주소 모든 연결된 응용 프로그램의 모든 데이터 저장소 이름에 대한 호스트 IP 주소의 이름입니다
스위치(일반 및 NPV)	"스위치" IP 주소 WWN 이름 일련 번호 모델 Fabric의 도메인 ID 이름입니다
응용 프로그램	"애플리케이션" 이름 부서 프로젝트의 테넌트 라인
테이프	"테이프" IP 주소 이름 일련 번호 공급업체
포트	"포트" WWN 이름입니다
패브릭	"fabric" WWN 이름입니다
스토리지 가상 시스템(SVM)	"storagevirtualmachine" 이름 UUID

## 보고

### Data Infrastructure Insights 보고 개요

Data Infrastructure Insights 보고는 사전 정의된 보고서를 보거나 사용자 지정 보고서를 생성할 수 있는 비즈니스 인텔리전스 툴입니다.



보고 기능은 Data Infrastructure Insights에서 사용할 수 ["Premium Edition을 참조하십시오"](#) 있습니다.

Data Infrastructure Insights 보고를 통해 다음 작업을 수행할 수 있습니다.

- 미리 정의된 보고서를 실행합니다
- 사용자 지정 보고서를 만듭니다
- 보고서의 형식 및 전달 방법을 사용자 지정합니다
- 보고서가 자동으로 실행되도록 예약합니다
- 이메일 보고서
- 색상을 사용하여 데이터의 임계값을 표시합니다

Data Infrastructure Insights Reporting은 비용 청구, 소비 분석 및 예측과 같은 영역에 대한 사용자 지정 보고서를 생성할 수 있으며 다음과 같은 질문에 대한 답변에 도움이 될 수 있습니다.

- 보유하고 있는 재고는 무엇입니까?
- 내 재고는 어디에 있습니까?
- 누가 우리의 자산을 사용하고 있습니까?
- 비즈니스 유닛에 할당된 스토리지에 대한 비용청구는 무엇입니까?

- 추가 스토리지 용량을 구입할 때까지 얼마나 걸립니까?
- 사업부가 적절한 스토리지 계층에 맞게 조정됩니까?
- 월, 분기 또는 연도별로 스토리지 할당이 어떻게 변경됩니까?

## Data Infrastructure Insights 보고 액세스

메뉴에서 \* Reports \* 링크를 클릭하여 Data Infrastructure Insights Reporting에 액세스할 수 있습니다.

보고 인터페이스로 이동합니다. Data Infrastructure Insights는 보고 엔진에 IBM Cognos Analytics를 사용합니다.

## ETL이란?

보고 작업 시 "데이터 웨어하우스" 및 "ETL"이라는 용어를 듣게 됩니다. ETL은 "추출, 변환 및 로드"를 의미합니다. ETL 프로세스는 Data Infrastructure Insights에서 수집된 데이터를 검색하여 데이터를 Reporting에서 사용할 형식으로 변환합니다. "데이터 웨어하우스"는 보고에 사용할 수 있는 수집된 데이터를 말합니다.

ETL 프로세스는 다음과 같은 개별 프로세스를 포함합니다.

- \* Extract \*: Data Infrastructure Insights에서 데이터를 가져옵니다.
- \* Transform \*: Data Infrastructure Insights에서 추출되는 데이터에 비즈니스 로직 규칙 또는 함수를 적용합니다.
- \* Load \* (로드 \*): 변환된 데이터를 보고에서 사용할 데이터 웨어하우스로 저장합니다.

## Data Infrastructure Insights 보고 사용자 역할

Data Infrastructure Insights Premium Edition with Reporting이 있는 경우 사용자 환경의 모든 Data Infrastructure Insights 사용자는 보고 애플리케이션(예: Cognos)에 대한 SSO(Single Sign-On)도 로그인할 수 있습니다. 메뉴에서 \* Reports \* 링크를 클릭하면 자동으로 Reporting에 로그인됩니다.

Data Infrastructure Insights의 사용자 역할에 따라 보고 사용자 역할이 결정됩니다.

Data Infrastructure Insights 역할	보고 역할	보고 권한
게스트	소비자	에서는 보고서를 보고 일정을 잡고 실행할 수 있으며 언어 및 표준 시간대와 같은 개인 기본 설정을 설정할 수 있습니다. 소비자는 보고서를 만들거나 관리 작업을 수행할 수 없습니다.
사용자	저자	는 모든 소비자 기능을 수행할 뿐 아니라 보고서 및 대시보드를 생성 및 관리할 수 있습니다.
관리자	관리자	보고서 구성, 보고 작업 종료 및 재시작 등의 모든 관리 작업과 모든 작성자 기능을 수행할 수 있습니다.

다음 표에서는 각 보고 역할에 사용할 수 있는 기능을 보여 줍니다.

피쳐	소비자	저자	관리자
팀 콘텐츠 탭에서 보고서를 봅니다	예	예	예
보고서를 실행합니다	예	예	예
보고서 예약	예	예	예
외부 파일을 업로드합니다	아니요	예	예
작업을 생성합니다	아니요	예	예
스토리 만들기	아니요	예	예
보고서 작성	아니요	예	예
패키지 및 데이터 모듈을 생성합니다	아니요	예	예
관리 작업을 수행합니다	아니요	아니요	예
HTML 항목 추가/편집	아니요	아니요	예
HTML 항목으로 보고서를 실행합니다	예	예	예
사용자 정의 SQL 추가/편집	아니요	아니요	예
사용자 지정 SQL을 사용하여 보고서를 실행합니다	예	예	예

## 보고(Cognos) 전자 메일 기본 설정 지정

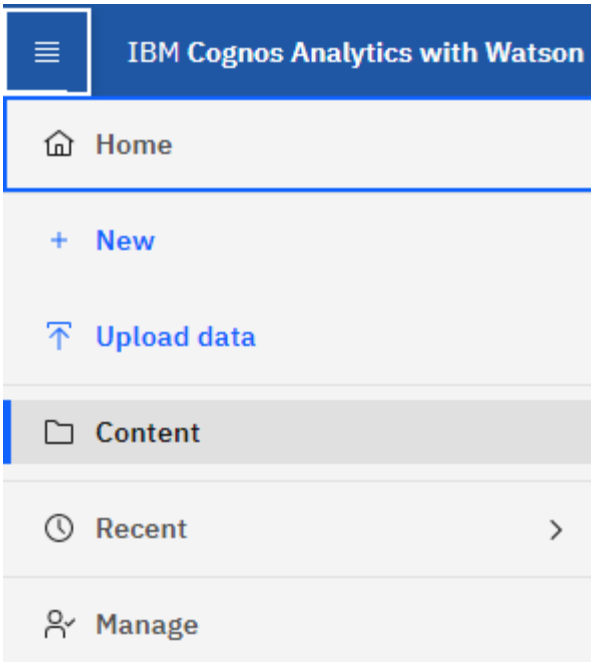


Data Infrastructure Insights 보고(즉, Cognos 애플리케이션)에서 사용자 이메일 기본 설정을 변경하면 현재 세션에 대해서만 해당 기본 설정이 활성화\_됩니다. Cognos에서 로그아웃했다가 다시 로그인하면 이메일 기본 설정이 재설정됩니다.

**SSO**를 활성화하기 위해 기존 환경을 준비하기 위해 어떤 단계를 수행해야 합니까?

보고서가 보존되도록 하려면 다음 단계를 사용하여 모든 보고서를 `_My Content_to_Team Content_`에서 마이그레이션합니다. 이 작업은 사용자 환경에서 SSO를 활성화하기 전에 수행해야 합니다.

1. 메뉴 > 콘텐츠 \* 로 이동합니다



1. 팀 콘텐츠 \_ \* 에서 새 폴더를 만듭니다
  - a. 여러 사용자가 생성된 경우, 중복된 이름으로 보고서를 덮어쓰지 않도록 각 사용자에게 대해 별도의 폴더를 만드십시오
2. My Content\_로 이동합니다
3. 보존하려는 모든 보고서를 선택합니다.
4. 메뉴 오른쪽 상단에서 "복사 또는 이동"을 선택합니다.
5. 팀 내용 \_ 에서 새로 만든 폴더로 이동합니다
6. "복사 대상" 또는 "이동 대상" 버튼을 사용하여 새로 만든 폴더에 보고서를 붙여 넣습니다
7. Cognos에 대해 SSO가 활성화되면 계정을 생성하는 데 사용된 이메일 주소로 Data Infrastructure Insights에 로그인합니다.
8. Cognos 내의 \_Team Content\_폴더로 이동하고 이전에 저장된 보고서를 다시 \_My Content\_로 복사 또는 이동합니다.

미리 정의된 보고서를 쉽게 만들 수 있습니다

Data Infrastructure Insights Reporting은 다수의 일반적인 보고 요구사항을 해결하는 미리 정의된 보고서를 포함하고 있어 이해 관계자가 스토리지 인프라에 대해 합리적인 의사 결정을 내리는 데 필요한 중요한 통찰력을 제공합니다.



보고 기능은 Data Infrastructure Insights에서 사용할 수 ["Premium Edition을 참조하십시오"](#) 있습니다.

Data Infrastructure Insights Reporting Portal에서 미리 정의된 보고서를 생성하고 다른 사용자에게 e-메일로 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.

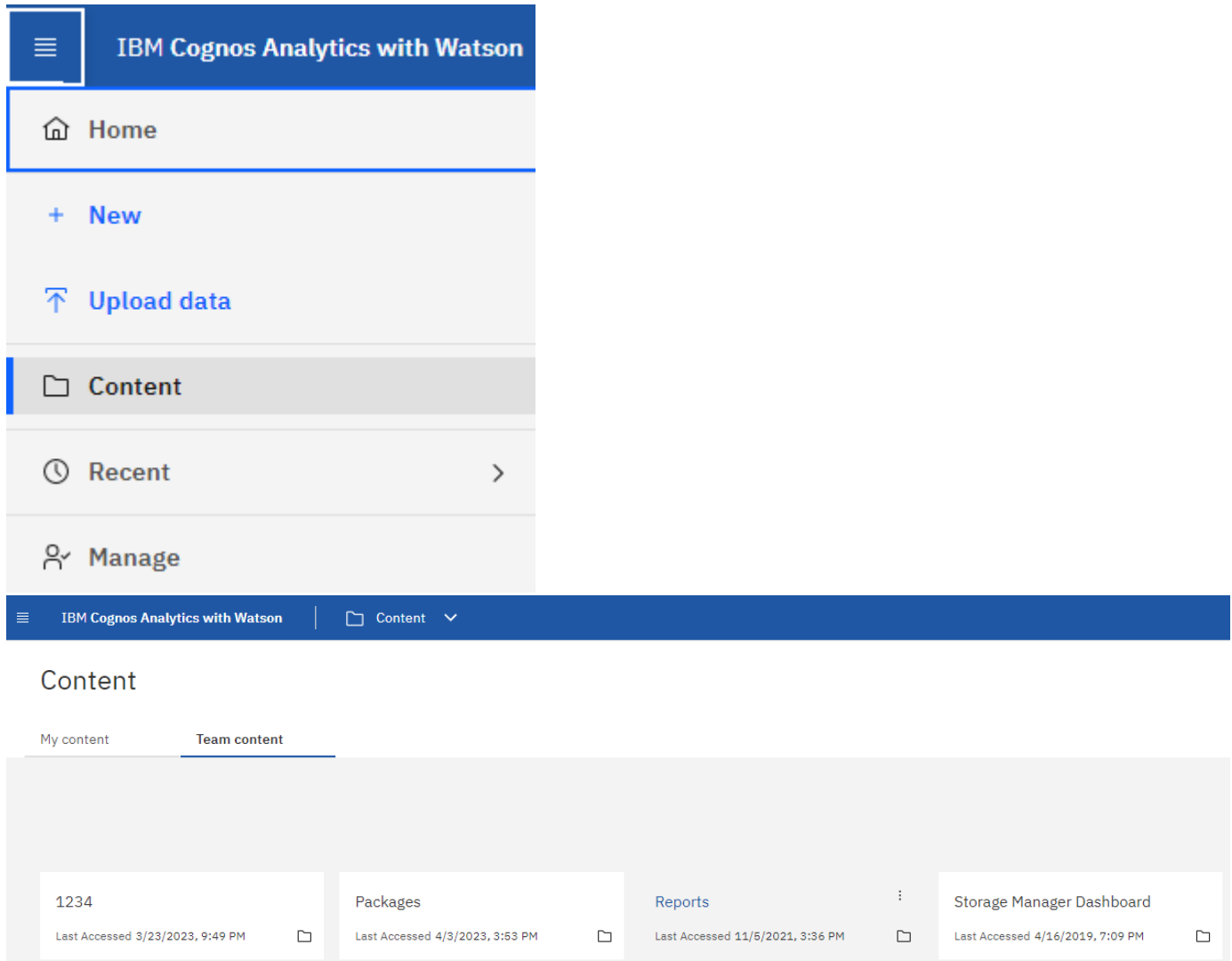
사전 정의된 보고서에는 인벤토리, 스토리지 용량, 비용 청구, 성능, 스토리지 효율성, 클라우드 비용 데이터입니다. 이러한 사전 정의된 보고서를 수정하고 수정 사항을 저장할 수 있습니다.

HTML, PDF, CSV, XML 등 다양한 형식의 보고서를 생성할 수 있습니다. Excel을 클릭합니다.

미리 정의된 보고서로 이동합니다

보고 포털을 열면 *Team Content* 폴더가 Data Infrastructure Insights 보고서에 필요한 정보 유형을 선택하기 위한 시작점입니다.

1. 왼쪽 탐색 창에서 \* 콘텐츠 > 팀 콘텐츠 \* 를 선택합니다.
2. 미리 정의된 보고서에 액세스하려면 \* Reports \* 를 선택합니다.



사전 정의된 보고서를 사용하여 일반적인 질문에 답합니다

다음 미리 정의된 보고서는 \* 팀 콘텐츠 > 보고서 \* 에서 사용할 수 있습니다.

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.

## 비용 청구

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.

## 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 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.

### 성과 기록표

스코어카드 보고서는 Data Infrastructure Insights에서 취득한 모든 자산에 대한 요약과 일반 상태를 제공합니다. 상태는 녹색, 노란색 및 빨간색 플래그로 표시됩니다.

- 녹색은 정상 상태를 나타냅니다
- 노란색은 환경에 잠재적인 문제가 있음을 나타냅니다
- 빨간색은 주의가 필요한 문제를 나타냅니다

보고서의 모든 필드는 보고서와 함께 제공되는 데이터 사전에 설명되어 있습니다.

### 스토리지 요약 정보

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.

## 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.

### Aggregate 별 NetApp 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.



스토리지의 **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.

## Storage Manager 대시보드

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.



보고 기능은 Data Infrastructure Insights에서 사용할 수 ["Premium Edition을 참조하십시오"](#) 있습니다.

요약

팀 콘텐츠에서 \* 스토리지 관리자 대시보드 \* 를 선택하면 트래픽 및 스토리지에 대한 정보를 제공하는 여러 보고서가 제공됩니다.

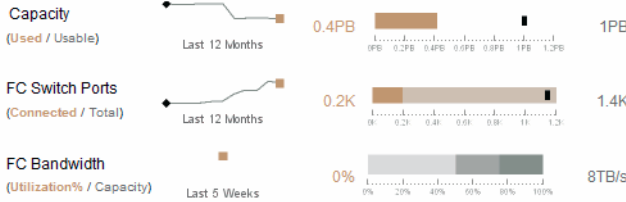
스토리지 관리자 보고서 \* 는 스토리지 환경의 다양한 측면에 대한 컨텍스트 정보를 포함하는 7개의 구성 요소로 구성되어 있습니다. 스토리지 서비스의 측면에 대해 드릴다운하여 가장 관심 있는 섹션에 대한 심층 분석을 수행할 수 있습니다.

## NetApp Storage Manager Dashboard

(Data as of Jan 28, 2016)

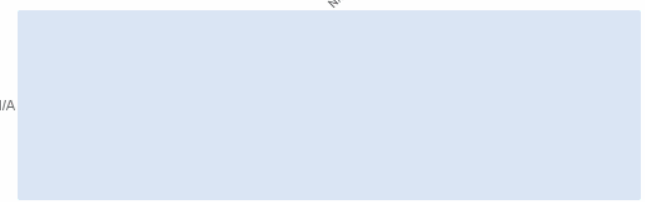
### Summary

History (Target, Actual, Forecast, Low, Mid, High)



### Data Centers Time to Full

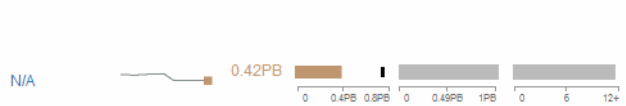
(<3 months, 3-6 months, >6 months)



### Storage Tiers Capacity

(Target, Actual, Forecast)

Last 12 Months Used Capacity Total Capacity Months to Full



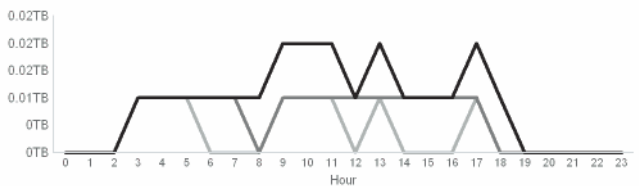
### Top 10 Applications

Last 12 Months Used Allocated Response Time (Acceptable)

Application	Last 12 Months	Used	Allocated	Response Time	Acceptable
Hadoop	■	11.7TB	■	1ms	■
Applicatio..	—	0.2TB	■	0ms	■
Applicatio..	■	0TB	■	3ms	■
Applicatio..	—	0TB	■	2ms	■
JUICE	—	0TB	■	2ms	■
SaproX4	■	0TB	■	1ms	■
Twilight	—	0TB	■	1ms	■

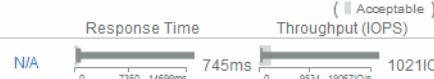
### Daily Storage Traffic (Terabytes)

Daily mean for last 6 months, Daily mean for last 7 days, Yesterday



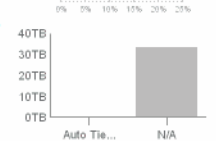
### Storage Tiers Daily Performance

(Acceptable)



### Orphaned Capacity

35TB 3.4%



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 있으며, 이를 통해 타겟을 기준으로 투사 및 원하는 실제 사용 현황을 비교하고 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 사용량, 사용량 예측 및 용량 목표를 위해 제공된 값과 함께 표시됩니다. 이 값은 구성할 수 있습니다. 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(일일 스토리지 트래픽)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 모든 데이터 센터와 모든 계층을 비교하여 예측 성장률을 기반으로 각 스토리지 계층의 각 데이터 센터에 남아 있는 용량을 표시합니다. 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. 구성에 의해 분리된 스토리지는 호스트에 스토리지가 할당된 상황을 설명합니다. 그러나 구성이 제대로 수행되지 않아 호스트가 스토리지를 액세스할 수 없습니다. 성능에 의해 고립된 스토리지는 호스트가 액세스할 수 있도록 올바르게 구성된 경우에 발생합니다. 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.

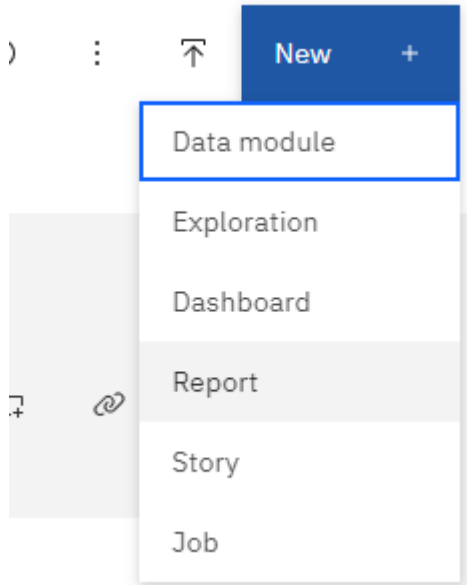
계층을 클릭하여 선택한 계층의 구성 및 성능에 의해 분리된 것으로 식별된 모든 볼륨을 표시하는 분리된 스토리지 세부 정보 보고서를 표시할 수 있습니다. 이 보고서에서 스토리지, 스토리지 풀 또는 볼륨을 클릭하면 해당 리소스의 현재 상태를 요약하는 자산 페이지가 표시됩니다.

## 보고서 작성(예)

이 예제의 단계를 사용하여 여러 데이터 센터에서 스토리지 및 스토리지 풀의 물리적 용량에 대한 간단한 보고서를 생성할 수 있습니다.

단계

1. 메뉴 > 콘텐츠 > 팀 콘텐츠 > 보고서 \* 로 이동합니다
2. 화면 오른쪽 상단에서 \* [New +] \* 를 선택합니다
3. Report \* 를 선택합니다



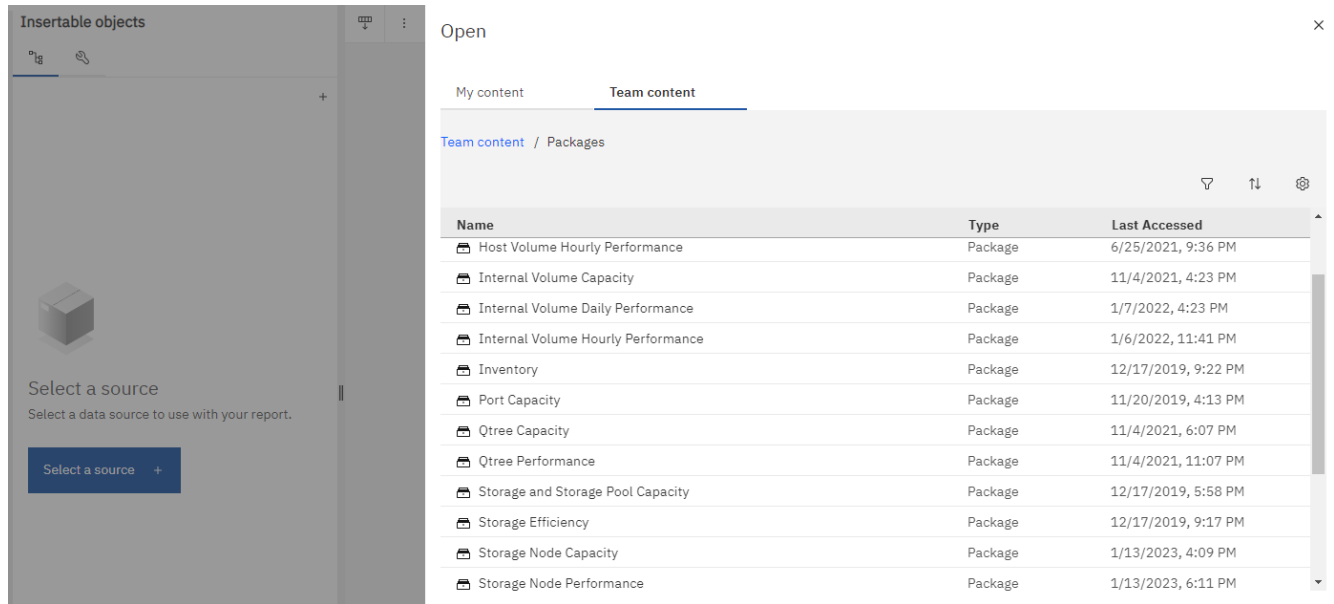
4. 템플릿 \* 탭에서 \_blank\_를 선택합니다

소스 및 데이터 탭이 표시됩니다

5. 열기 \* 소스 + \* 를 선택합니다
6. 팀 콘텐츠 \* 에서 \* 패키지 \* 를 엽니다

사용 가능한 패키지 목록이 표시됩니다.

7. 스토리지 및 스토리지 풀 용량 \* 을 선택합니다



8. 열기 \* 를 선택합니다

보고서에 사용할 수 있는 스타일이 표시됩니다.

9. 목록 \* 을 선택합니다

목록 및 쿼리에 적절한 이름을 추가합니다

10. OK \* 를 선택합니다

11. 물리적 용량 \_ 을(를) 확장합니다

12. Data Center \_ 의 가장 낮은 수준으로 확장합니다

13. 데이터 센터 \_ 를 보고 미천장에 끌어다 놓습니다.

14. Capacity(MB) \_ 을(를) 확장합니다

15. Capacity(MB)\_를 보고 입천장에 끌어다 놓습니다.

16. Drag\_Used Capacity (MB) \_ 을(를) Reporting palate 로 이동합니다.

17. Run \* (실행 \*) 메뉴에서 출력 유형을 선택하여 보고서를 실행합니다.



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

보고서의 출력 형식과 배달, 보고서 속성 또는 일정, 전자 메일 보고서를 사용자 지정할 수 있습니다.

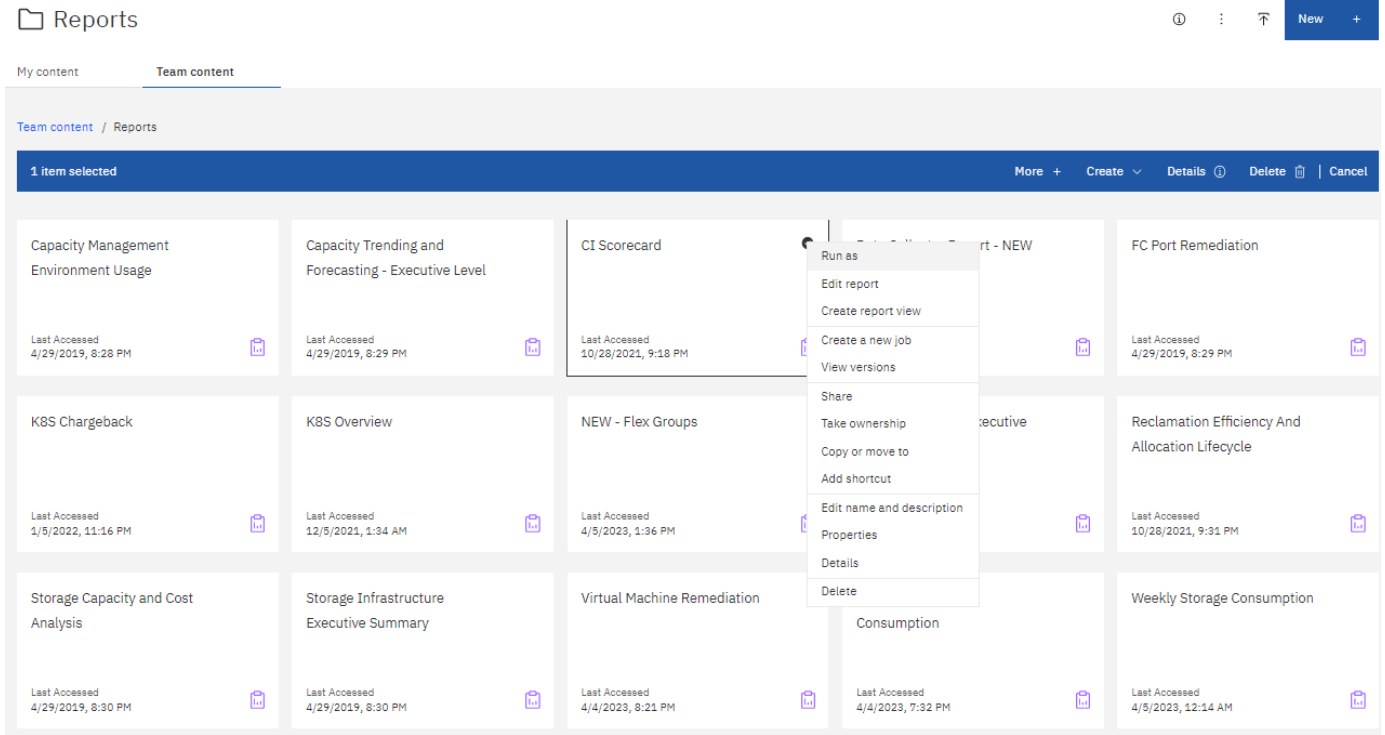


보고 기능은 Data Infrastructure Insights에서 사용할 수 ["Premium Edition을 참조하십시오"](#) 있습니다.

## 보고서의 출력 형식 및 배달 사용자 지정

보고서의 형식 및 전달 방법을 사용자 지정할 수 있습니다.

1. Data Infrastructure Insights 보고 포털에서 \* 메뉴 > 콘텐츠 > 내 콘텐츠/팀 콘텐츠 \* 로 이동합니다. 사용자 정의할 보고서 위에 마우스를 올려 놓고 "점 3개" 메뉴를 엽니다.

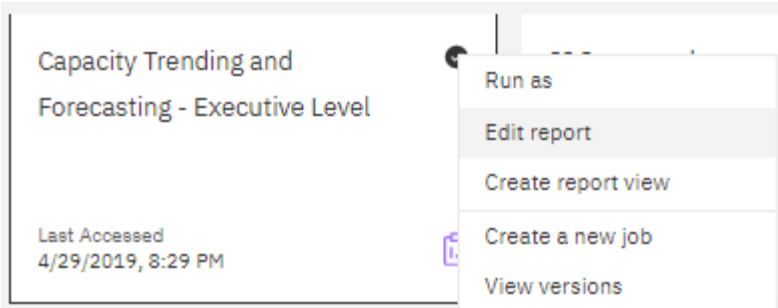


1. 속성 > 일정 \* 을 클릭합니다
2. 다음 옵션을 설정할 수 있습니다.
  - \* 보고서를 실행하려는 경우 별표 \* 를 사용합니다.
  - 보고서 형식 및 배달(저장, 인쇄, 전자 메일) 및 보고서의 언어 에 대해 \* 옵션 \* 을 선택합니다.
3. 선택한 항목을 사용하여 보고서를 생성하려면 \* Save \* (저장 \*)를 클릭합니다.

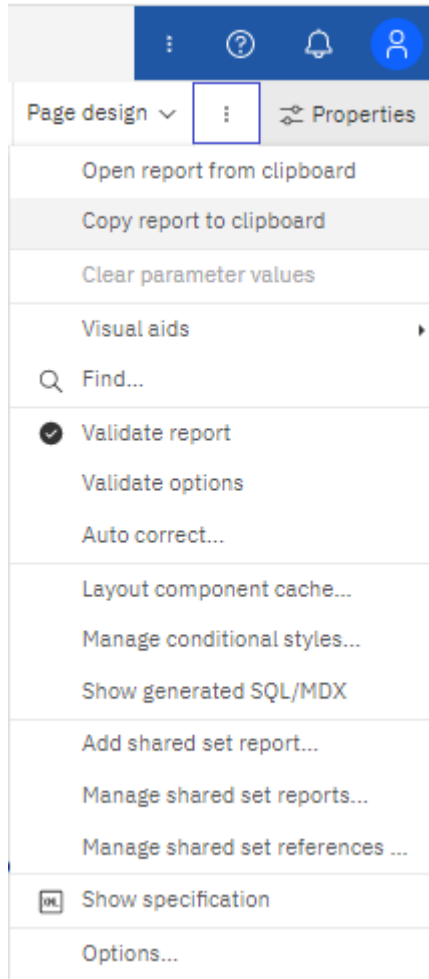
보고서를 클립보드로 복사합니다

이 프로세스를 사용하여 보고서를 클립보드로 복사합니다.

1. 복사할 보고서 선택(\* 메뉴 > 콘텐츠 > 내 콘텐츠 또는 팀 콘텐츠 \*)
2. 보고서 드롭다운 메뉴에서 \_ 보고서 편집 \_ 을 선택합니다



3. 화면 오른쪽 상단에서 "속성" 옆에 있는 "점 3개" 메뉴를 엽니다.
4. 클립보드로 보고서 복사 \* 를 선택합니다.



클립보드에서 보고서를 엽니다

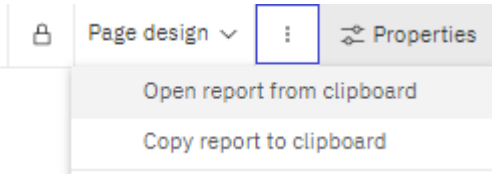
이전에 클립보드에 복사한 보고서 설정을 열 수 있습니다.

이 작업 정보 새 보고서를 만들거나 복사된 보고서로 바꿀 기존 보고서를 열어 시작합니다. 아래 단계는 새 보고서를 위한 것입니다.

1. 메뉴 > + 새로 만들기 > 보고서 \* 를 선택하고 빈 보고서를 만듭니다.
2. 화면 오른쪽 상단에서 "속성" 옆에 있는 "점 3개" 메뉴를 엽니다.



3. 클립보드에서 보고서 열기 \* 를 선택합니다.



1. 복사한 코드를 창에 붙여 넣고 \* OK \* 를 선택합니다.
2. 플로피 디스크 아이콘을 선택하여 보고서를 저장합니다.
3. 보고서를 저장할 위치(My Content, Team Content 또는 새 폴더 만들기)를 선택합니다.
4. 새 보고서에 의미 있는 이름을 지정하고 \* Save \* 를 선택합니다.

### 기존 보고서 편집

기본 위치에서 파일을 편집하면 다음 보고서 카탈로그를 새로 고칠 때 해당 보고서를 덮어쓸 위험이 있습니다. 편집한 보고서를 새 이름으로 저장하거나 기본이 아닌 위치에 저장하는 것이 좋습니다.

### 문제 해결

다음은 보고와 관련된 문제 해결을 위한 제안 사항입니다.

* 문제: *	* 사용해 보세요. *
이메일을 통해 보고서를 보내도록 예약하는 경우 로그인한 사용자의 이름이 이메일의 "받는 사람" 필드에 미리 채워집니다. 그러나 이름은 "성 이름"(이름, 공백, 성) 형식입니다. 이 주소는 유효한 이메일 주소가 아니므로 예약된 보고서가 실행될 때 이메일이 전송되지 않습니다.	이메일을 통해 보고서를 보내도록 예약할 때 미리 채워진 이름을 지우고 "받는 사람" 필드에 올바른 형식의 유효한 이메일 주소를 입력합니다.

### 사용자 정의 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.



보고 기능은 Data Infrastructure Insights에서 사용할 수 ["Premium Edition을 참조하십시오"](#) 있습니다.

이 섹션의 예에서는 Data Infrastructure Insights 보고 데이터 모델에 사용할 수 있는 다음 프로세스를 보여 줍니다.

- 보고서로 답할 질문 식별
- 결과를 지원하는 데 필요한 데이터 결정
- 보고서의 데이터 요소 선택

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 않거나 일부 데이터 요소에 대해 "N/A"가 표시될 수 있습니다.

보고서를 디자인하기 전에 다음 작업을 완료합니다.

- 모두 구성 "**데이터 수집기**" 있습니다.
- 사용자 환경의 장치 및 리소스에 대한 주식(예: 계층, 데이터 센터 및 부서)을 입력합니다. Data Infrastructure Insights Reporting은 내역 정보를 수집하므로 보고서를 생성하기 전에 주석을 안정적으로 유지하는 것이 좋습니다.

## 보고서 작성 프로세스

사용자 지정("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 결과 계획

보고서 작성 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 관계는 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.

보고서를 디자인할 때 몇 가지 팁이 도움이 될 수 있습니다.

- 현재 데이터 또는 기간별 데이터를 사용해야 하는지 여부를 결정합니다.

대부분의 보고서는 Data Infrastructure Insights에서 사용할 수 있는 최신 데이터만 보고하면 됩니다.

- Data Infrastructure Insights Reporting은 용량 및 성능에 대한 기간별 정보를 제공하지만 인벤토리는 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

Data Infrastructure Insights에는 미리 정의된 보고서를 선택하거나 사용자 지정 보고서를 생성할 수 있는 몇 가지 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.
- 고급 데이터 마트는 단순 데이터 마트에서 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 모델입니다

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

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? 8 내부 볼륨에서 할당된 용량과 사용된 용량은 어떻게 됩니까?

## Port Capacity 데이터 모델입니다

스위치 포트 연결, 포트 상태 및 포트 속도에 대한 질문에 시간 경과에 따른 답변을 얻을 수 있습니다. 새 스위치 구입을 계획하는 데 도움이 되는 다음과 같은 질문에 답할 수 있습니다. 데이터 센터, 스위치 공급업체 및 포트 속도에 따라 리소스(포트) 가용성을 예측하는 포트 소비 예측을 생성하려면 어떻게 해야 합니까?

- 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, 애플리케이션, 계층, 서비스 수준 등 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 씬 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 씬 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. 이는 Data Infrastructure Insights의 가상 머신 보기에서 VM 자체에 대해 프로비저닝된 크기를 보여 주는 프로비저닝된 용량과는 다릅니다.

### 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 씬 프로비저닝된 데이터 센터 용량은 어느 정도입니까?
- 복제용으로 예약해야 하는 데이터 센터 용량은 얼마나 됩니까?

### 차지백 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 엔티티가 볼륨에 할당되지 않고 qtree에 할당된 경우, 차지백 보고서는 qtree에 따른 차지백을 표시합니다.
  - 비즈니스 엔티티가 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 프로세스 를 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 데이터로 답변할 수 있는 질문입니다

- 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 디바이스를 식별합니까?
- 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 이러한 보고서의 대부분은 `_hourly_data`, `_Daily_data` 또는 둘 다 해당됩니다. 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 재계층화에 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 Data Infrastructure Insights는 장치에서 사용되는 용량을 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?

#### 데이터 모델 팩트 및 차원 테이블

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.

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 봅시다. 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.

## API를 통해 보고 데이터베이스에 액세스합니다

Data Infrastructure Insights의 강력한 API를 사용하면 Cognos 보고 환경을 거치지 않고도 Data Infrastructure Insights 보고 데이터베이스를 직접 쿼리할 수 있습니다.



이 문서에서는 Data Infrastructure Insights Premium Edition에서 사용할 수 있는 Data Infrastructure Insights 보고 기능에 대해 설명합니다.

### OData입니다

Data Infrastructure Insights Reporting API는 "OData v4"보고 데이터베이스 쿼리에 대한 (Open Data Protocol) 표준을 따릅니다. 자세한 내용 또는 자세한 내용은 OData 를 ["이 자습서"](#)참조하십시오.

모든 요청은 URL\_\[https://<Data 인프라 인사이트 URL >/REST/v1/dwh-management/odData\\_](https://<Data 인프라 인사이트 URL >/REST/v1/dwh-management/odData_)로 시작합니다

### APIKey를 생성하는 중입니다

에 대해 자세히 ["Data Infrastructure Insights API를 참조하십시오"](#)알아보세요.

API 키를 생성하려면 다음을 수행합니다.

- Data Infrastructure Insights 환경에 로그인하고 \* Admin > API Access \* 를 선택합니다.



- “+API 액세스 토큰”을 클릭합니다.
- 이름 및 설명을 입력합니다.
- 유형으로 \_ 데이터 웨어하우스 \_ 를 선택합니다.
- 권한을 읽기/쓰기로 설정합니다.
- 욕망 만료 날짜를 설정합니다.
- "저장"을 클릭한 다음 \* 키를 복사하여 안전한 곳에 저장합니다 \*. 나중에 전체 키에 액세스할 수 없습니다.

APIkeys는 에 적합합니다 [Sync](#) 또는 [Async](#).

### 테이블 직접 쿼리

API 키가 있으면 이제 보고 데이터베이스의 직접 쿼리를 수행할 수 있습니다. 전체 <https://<Data 인프라 인사이트 URL>/REST/v1/dwh-management/OData>가 아니라 표시 목적으로 <https://.../odata/>으로 URL을 단순화할 수 있습니다

과 같은 간단한 쿼리를 사용해 보세요

- [https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh\\_custom](https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh_custom)
- [https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh\\_inventory](https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh_inventory) 를 입력합니다
- [https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh\\_inventory/storage](https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh_inventory/storage)
- [https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh\\_inventory/disk](https://<Data 인프라 인사이트 URL>/rest/v1/dwh-management/odata/dwh_inventory/disk)
- [https://&#8230;&#8203;/odata/dwh\\_custom/custom\\_queries](https://&#8230;&#8203;/odata/dwh_custom/custom_queries) 으로 문의하십시오

### REST API 예제

모든 호출의 URL은 [\\_https://<Data 인프라 인사이트 URL>/REST/v1/dwh-management/odata/](https://<Data 인프라 인사이트 URL>/REST/v1/dwh-management/odata/)입니다.

- `Get/{schema}/**` - 보고 데이터베이스에서 데이터를 검색합니다.

형식: [\\_https://<Data 인프라 인사이트 URL>/REST/v1/dwh-management/OData/<schema\\_name>/<query>](https://<Data 인프라 인사이트 URL>/REST/v1/dwh-management/OData/<schema_name>/<query>)\_

예:

```
https://<domain>/rest/v1/dwh-
management/odata/dwh_inventory/fabric?$count=true&$orderby=name
```

결과:

```

{
  "@odata.context": "$metadata#fabric",
  "@odata.count": 2,
  "value": [
    {
      "id": 851,
      "identifier": "10:00:50:EB:1A:40:3B:44",
      "wwn": "10:00:50:EB:1A:40:3B:44",
      "name": "10:00:50:EB:1A:40:3B:44",
      "vsanEnabled": "0",
      "vsanId": null,
      "zoningEnabled": "0",
      "url": "https://<domain>/web/#/assets/fabrics/941716"
    },
    {
      "id": 852,
      "identifier": "10:00:50:EB:1A:40:44:0C",
      "wwn": "10:00:50:EB:1A:40:44:0C",
      "name": "10:00:50:EB:1A:40:44:0C",
      "vsanEnabled": "0",
      "vsanId": null,
      "zoningEnabled": "0",
      "url": "https://<domain>/web/#/assets/fabrics/941836"
    }
  ]
}

```

## 유용한 힌트

보고 API 쿼리 작업 시 다음 사항을 염두에 두십시오.

- 쿼리 페이로드는 올바른 JSON 문자열이어야 합니다
- 쿼리 페이로드는 한 줄에 포함되어야 합니다
- 큰따옴표는 이스케이프되어야 합니다. 즉, \"
- 탭은 \t로 지원됩니다
- 의견을 피합니다
- 소문자 테이블 이름이 지원됩니다

추가 사항:

- 헤더 2개 필요:
  - 이름 "X-CloudInsights - ApiKey"
  - 속성 값 "<apikey>"

API 키는 Data Infrastructure Insights 환경과 관련이 있습니다.

## 동기식 또는 비동기식?

기본적으로 API 명령은 `_synchronous_mode`에서 작동하므로 요청을 보내고 응답이 즉시 반환됩니다. 그러나 쿼리를 실행하는 데 시간이 오래 걸릴 수 있으므로 요청 시간이 초과될 수 있습니다. 이 문제를 해결하려면 요청을 비동기적으로 실행할 수 있습니다. 비동기 모드에서 요청은 실행을 모니터링할 수 있는 URL을 반환합니다. URL이 준비되면 결과가 반환됩니다.

비동기 모드에서 쿼리를 실행하려면 머리글을 추가합니다 **Prefer: respond-async** 요청에 보냅니다. 성공적으로 실행되면 응답에 다음 헤더가 포함됩니다.

```
Status Code: 202 (which means ACCEPTED)
preference-applied: respond-async
location: https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncStatus/<token>
```

위치 URL을 쿼리하면 응답이 아직 준비되지 않은 경우 동일한 헤더가 반환되고 응답이 준비되면 상태 200으로 반환됩니다. 응답 내용은 텍스트 형식이며 원본 쿼리의 http 상태와 일부 메타데이터를 포함하고 그 다음에 원본 쿼리의 결과가 나옵니다.

```
HTTP/1.1 200 OK
OData-Version: 4.0
Content-Type: application/json;odata.metadata=minimal
oDataResponseSizeCounted: true

{ <JSON_RESPONSE> }
```

모든 비동기 쿼리 목록과 준비된 쿼리를 보려면 다음 명령을 사용합니다.

```
GET https://<Data Infrastructure Insights URL>/rest/v1/dwh-
management/odata/dwh_custom/asyncList
응답의 형식은 다음과 같습니다.
```

```

{
  "queries" : [
    {
      "Query": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-
management/odata/dwh_custom/heavy_left_join3?$count=true",
      "Location": "https://<Data Infrastructure Insights
URL>/rest/v1/dwh-management/odata/dwh_custom/asyncStatus/<token>",
      "Finished": false
    }
  ]
}

```

## 보고를 위해 기록 데이터를 보관하는 방법

Data Infrastructure Insights는 다음 표에 나와 있는 것처럼 데이터 마트와 데이터의 세분성을 기반으로 보고에 사용할 기간별 데이터를 보존합니다.

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	35일
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	35일
성능 마트	하이퍼바이저 성능	매일	13개월
성능 마트	VMDK 성능	매시간	35일
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)
-------	-------	-------	----------------------

## Data Infrastructure Insights 보고 스키마 다이어그램

이 문서에서는 보고 데이터베이스에 대한 스키마 다이어그램을 제공합니다. 이 포함된 파일을 다운로드할 수도 있습니다 "[스키마 테이블](#)".

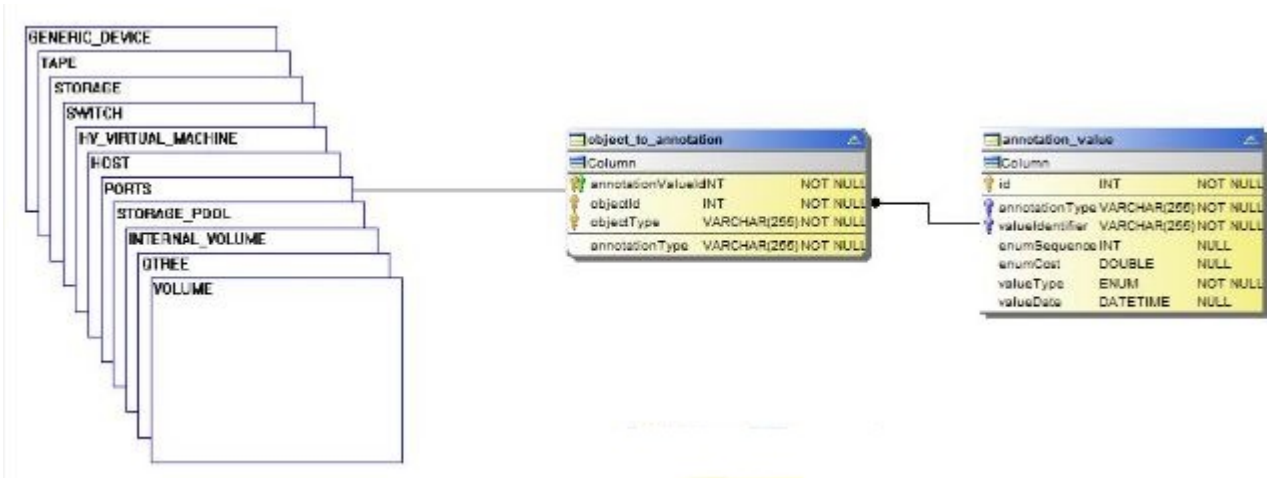


보고 기능은 Data Infrastructure Insights에서 사용할 수 "[Premium Edition을 참조하십시오](#)"있습니다.

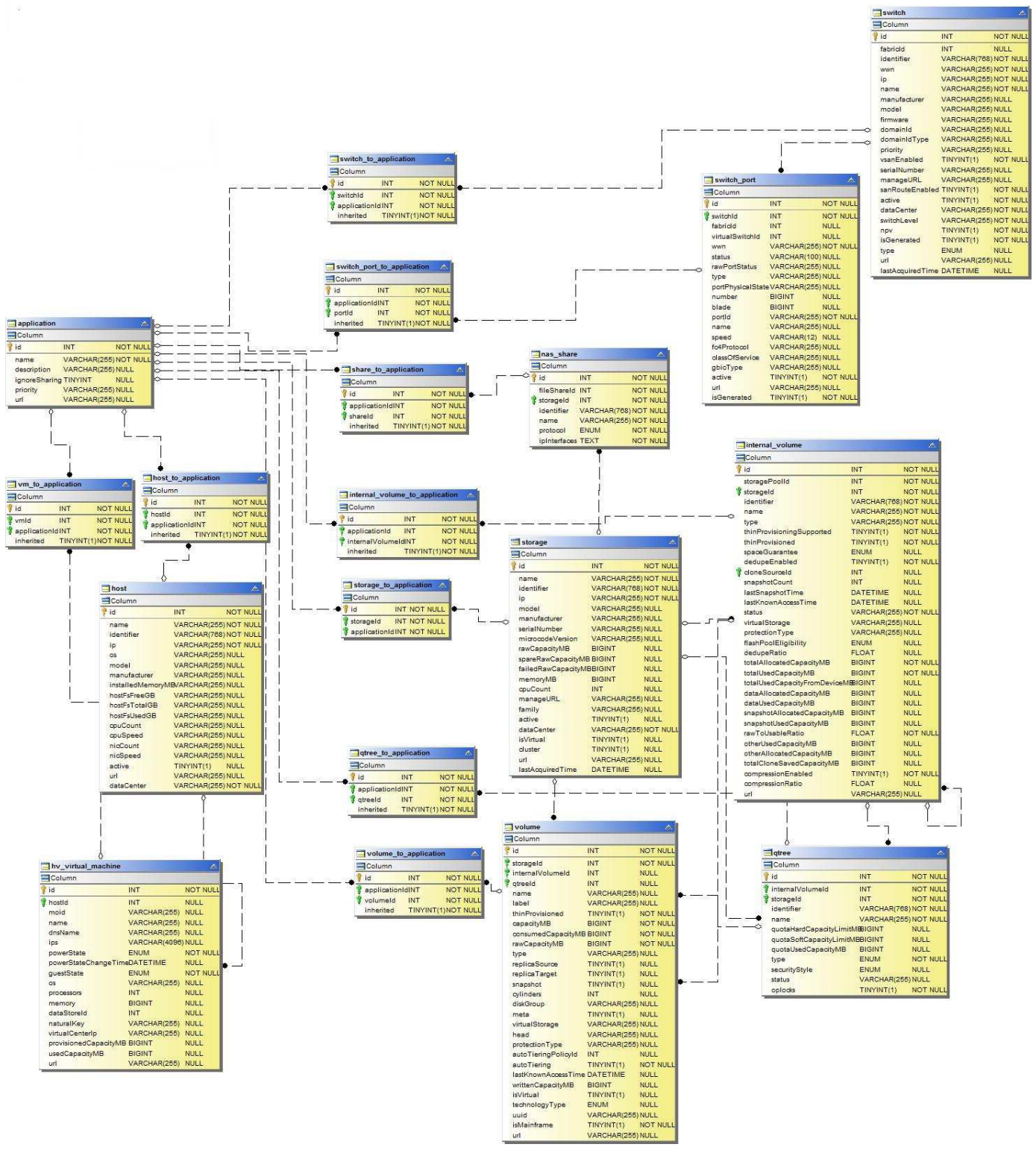
재고 데이터 마트

다음 이미지는 재고 데이터마트에 대해 설명합니다.

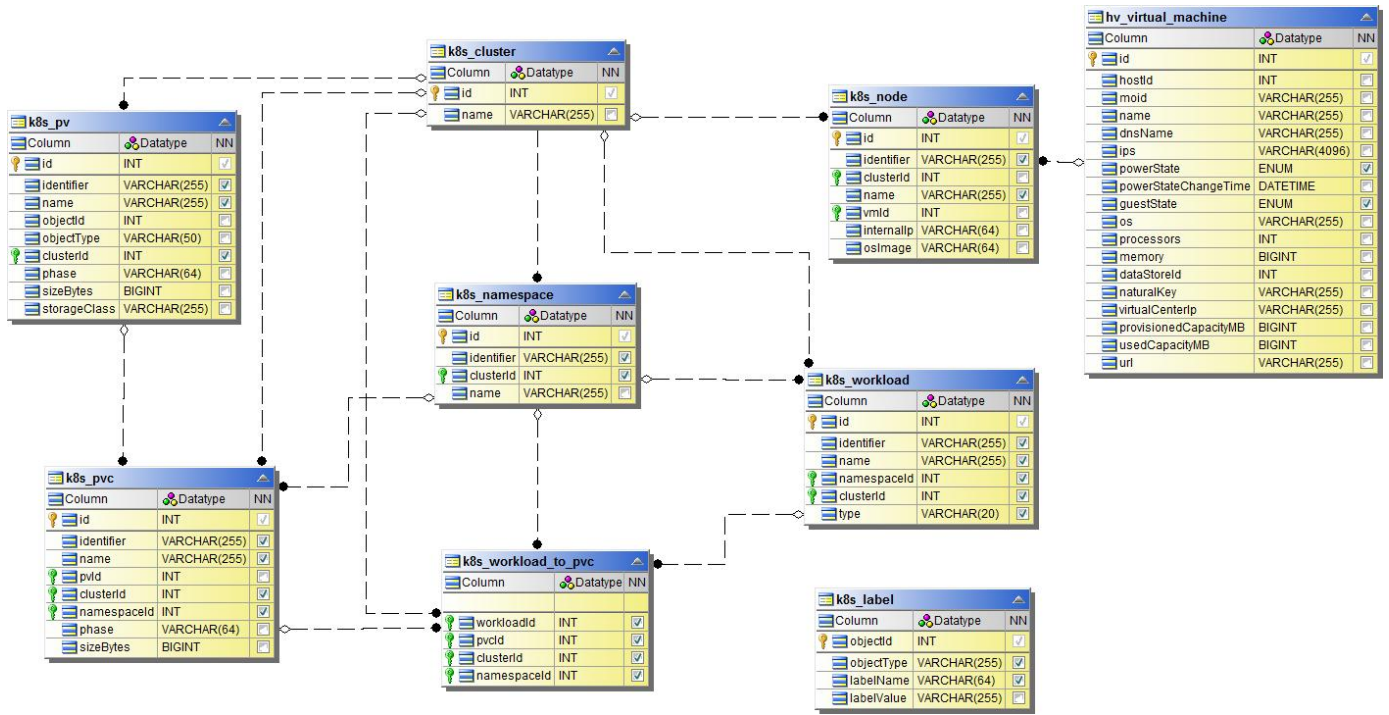
주석



응용 프로그램

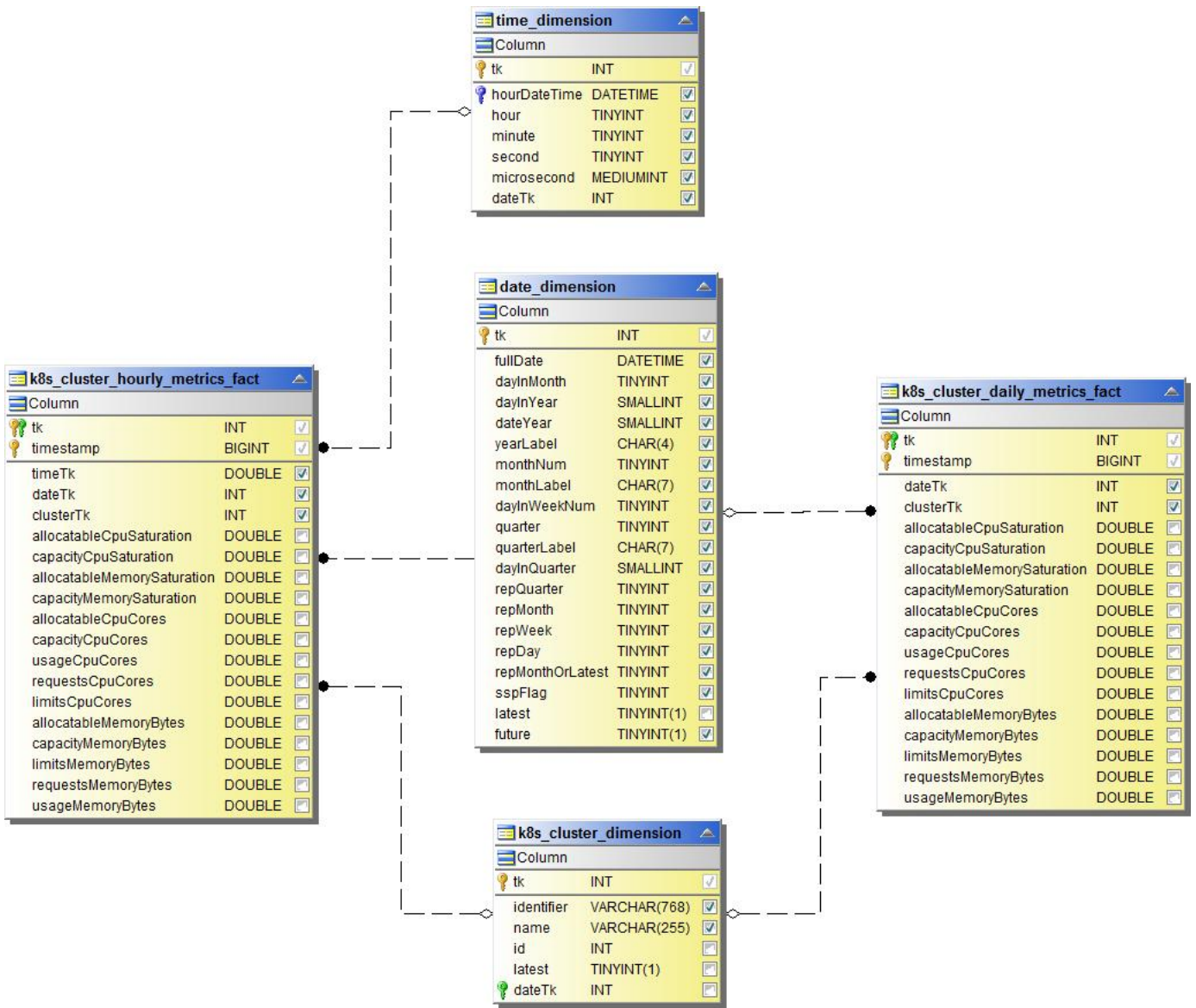


Kubernetes 메트릭



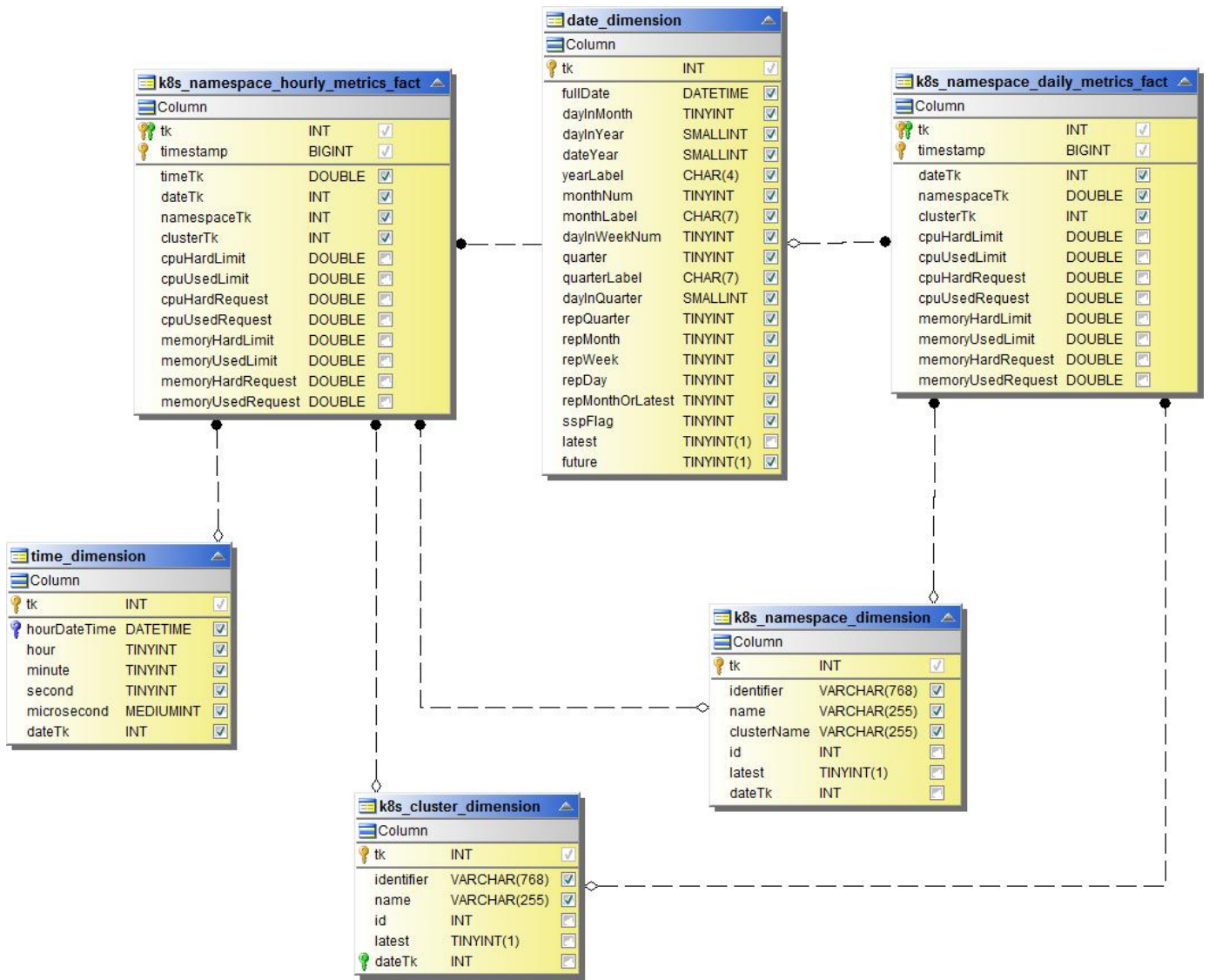
## Kubernetes 클러스터 메트릭 정보



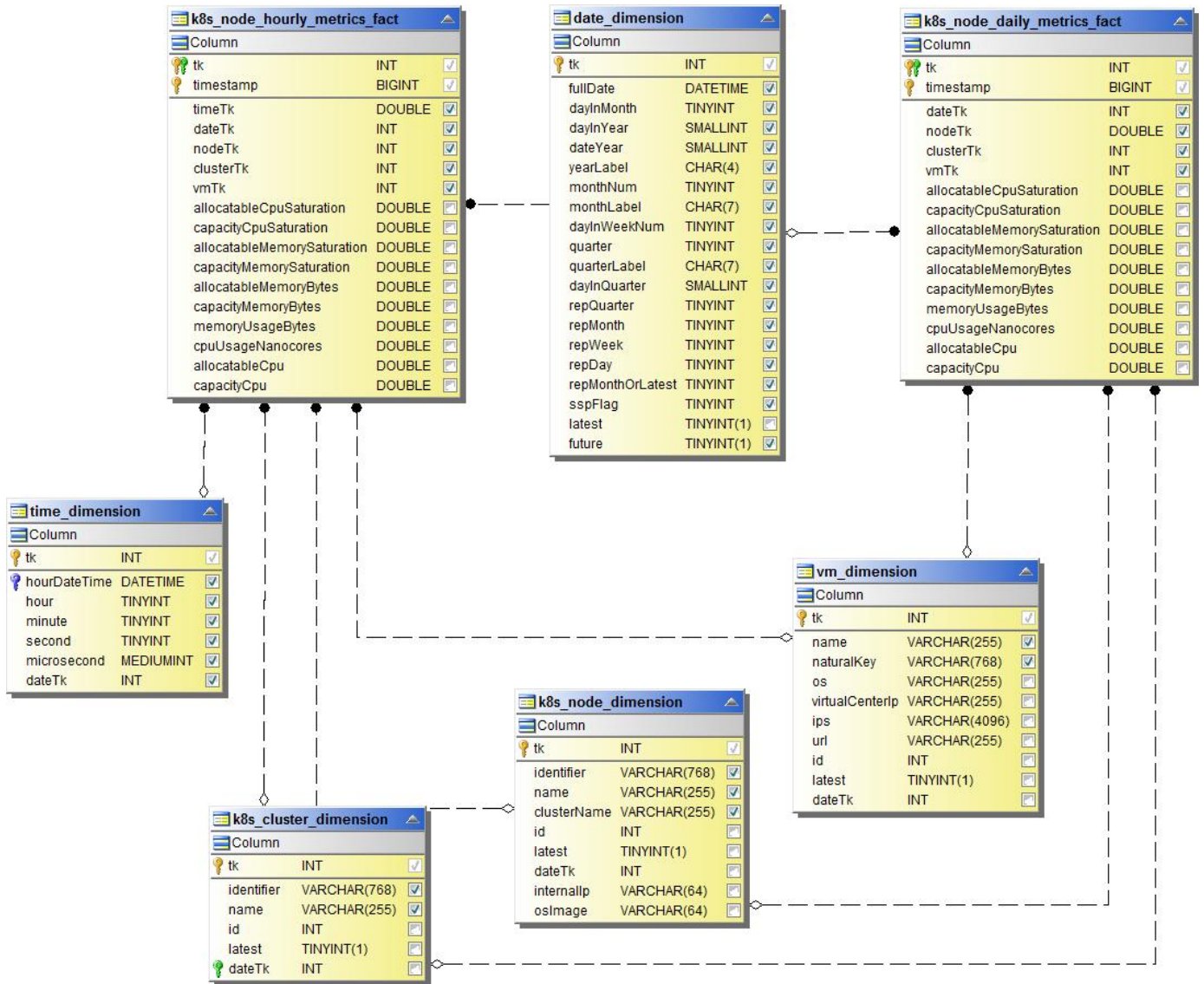


## Kubernetes 네임스페이스 메트릭 팩트

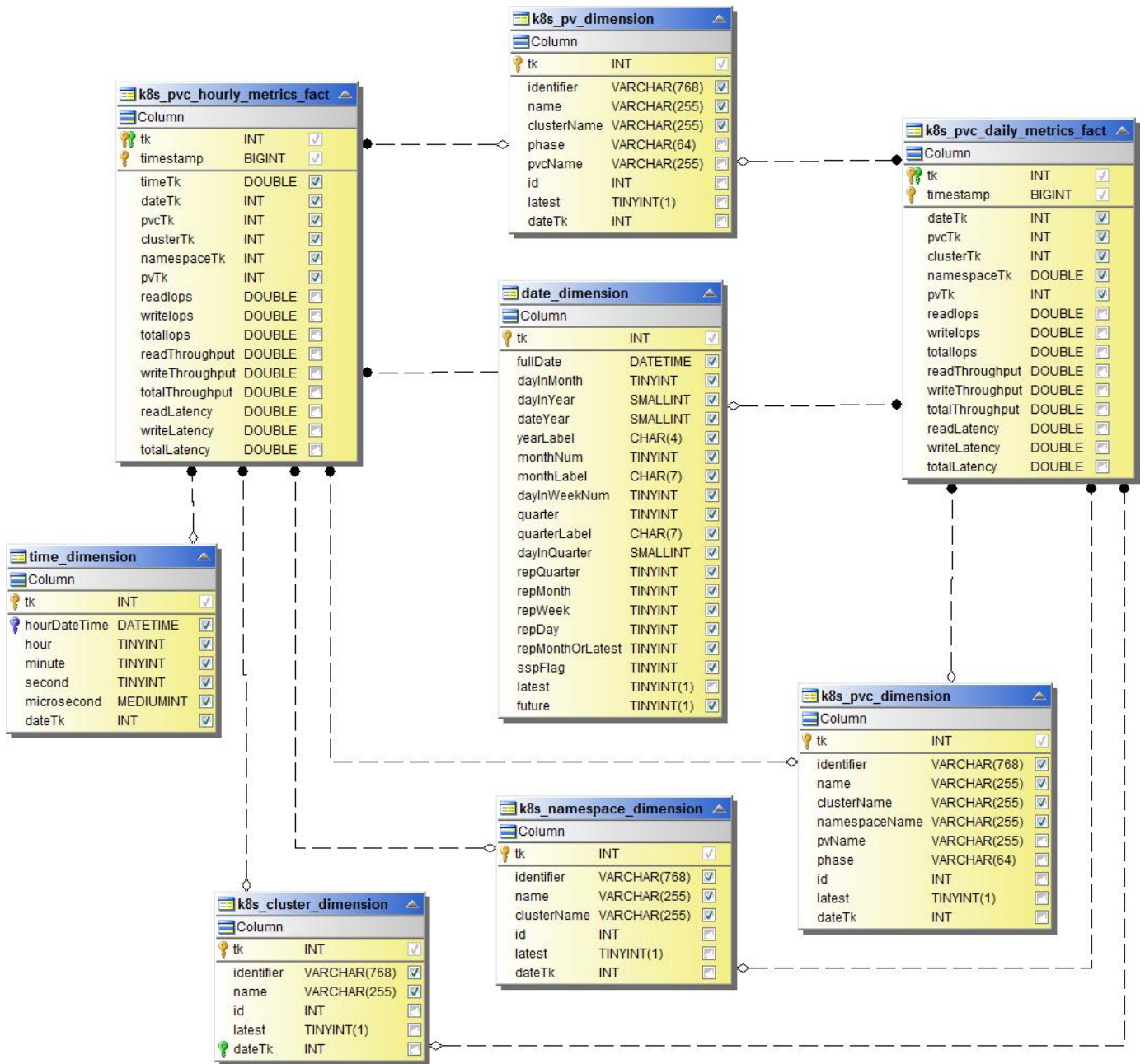




## Kubernetes 노드 메트릭 팩트

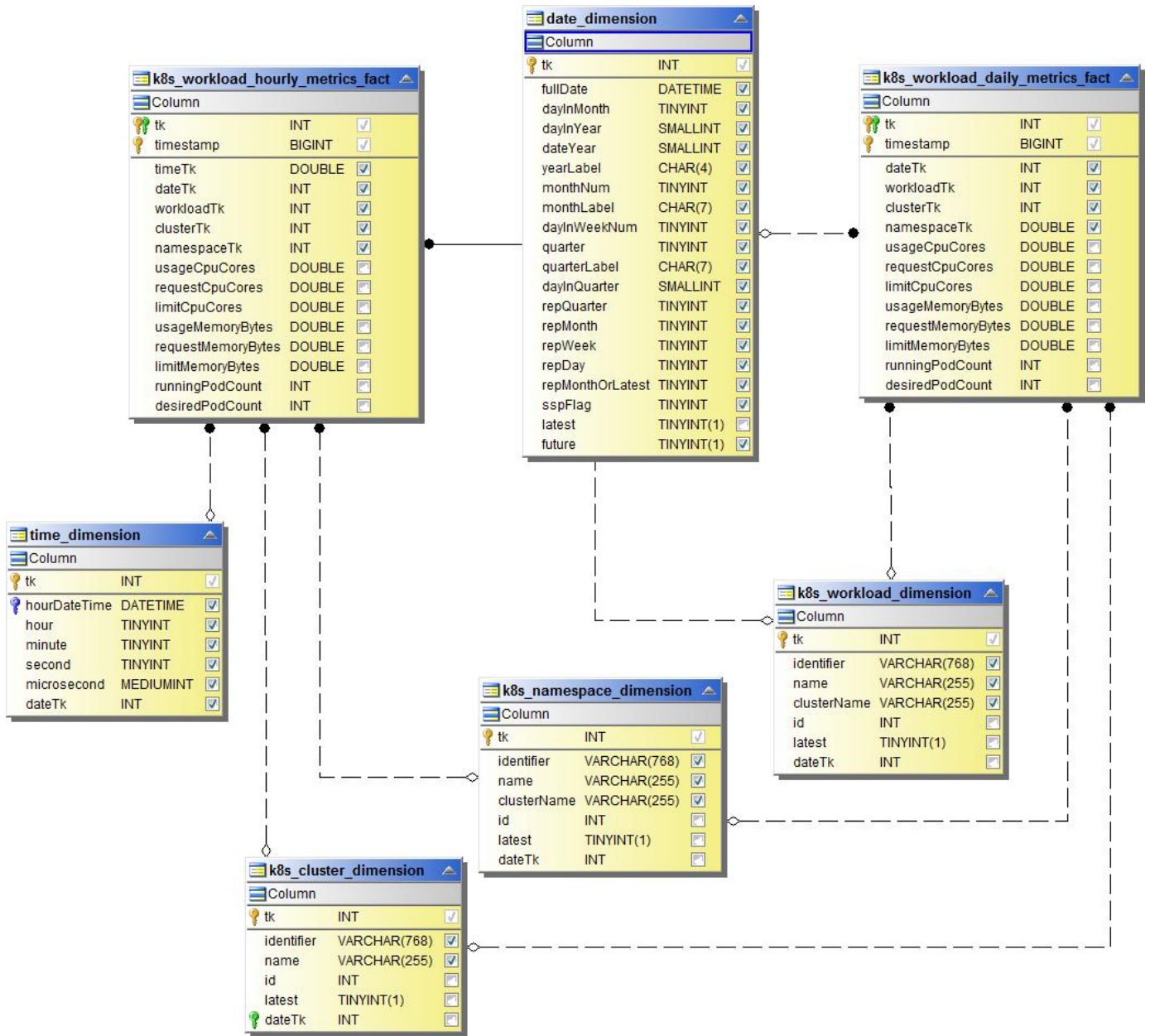


## Kubernetes PVC 메트릭 정보

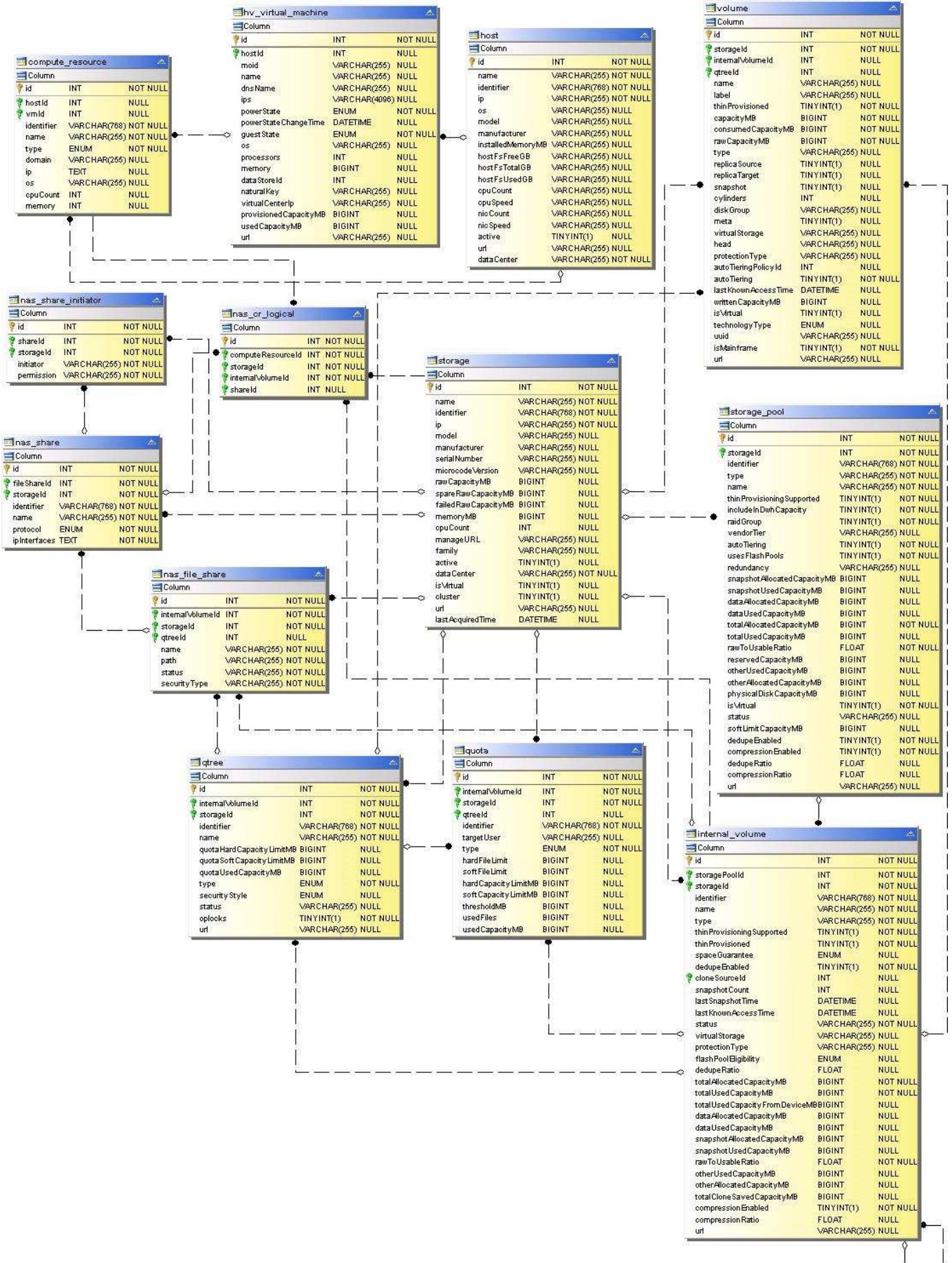


## Kubernetes 워크로드 메트릭 팩트



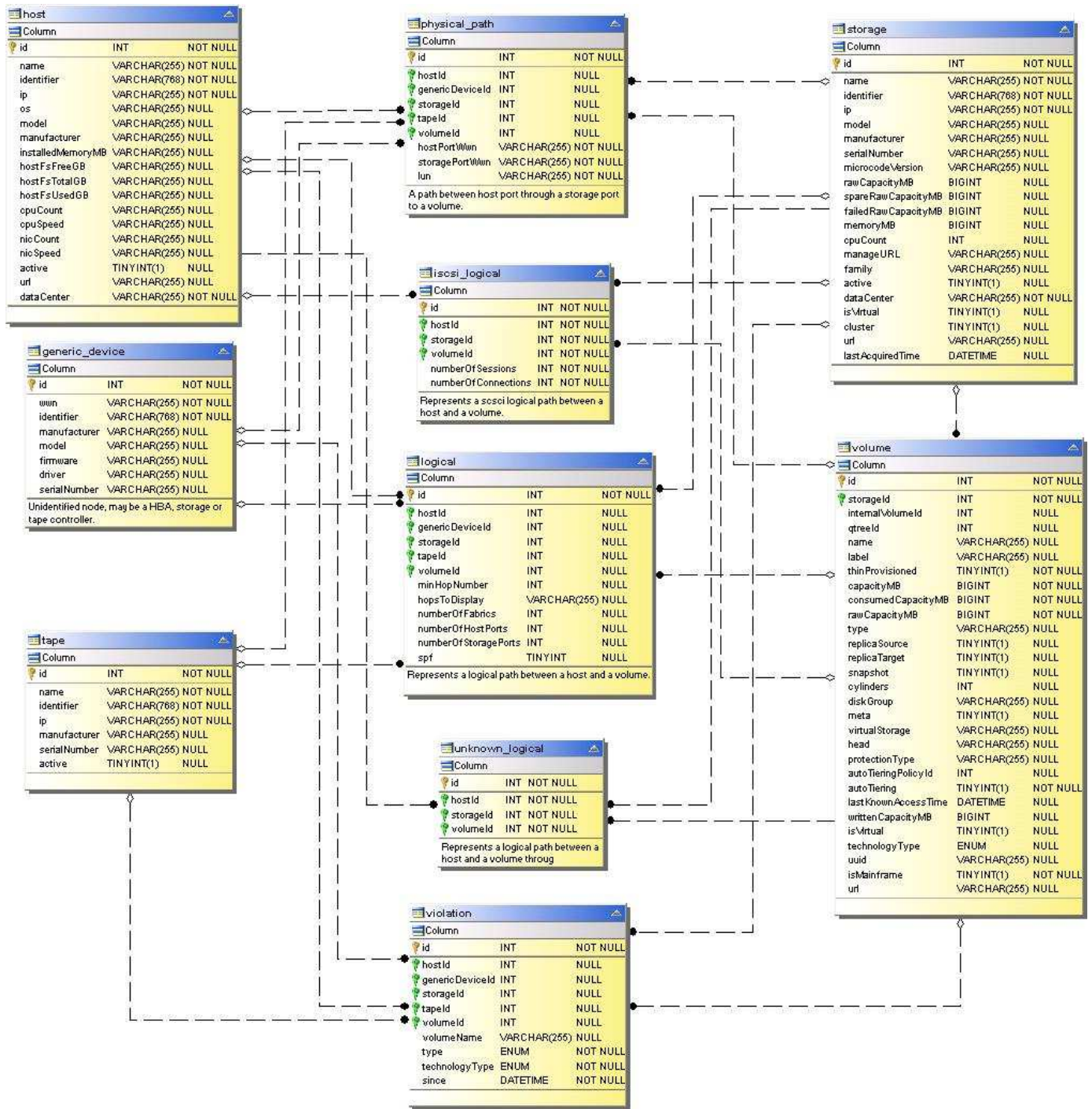


NAS

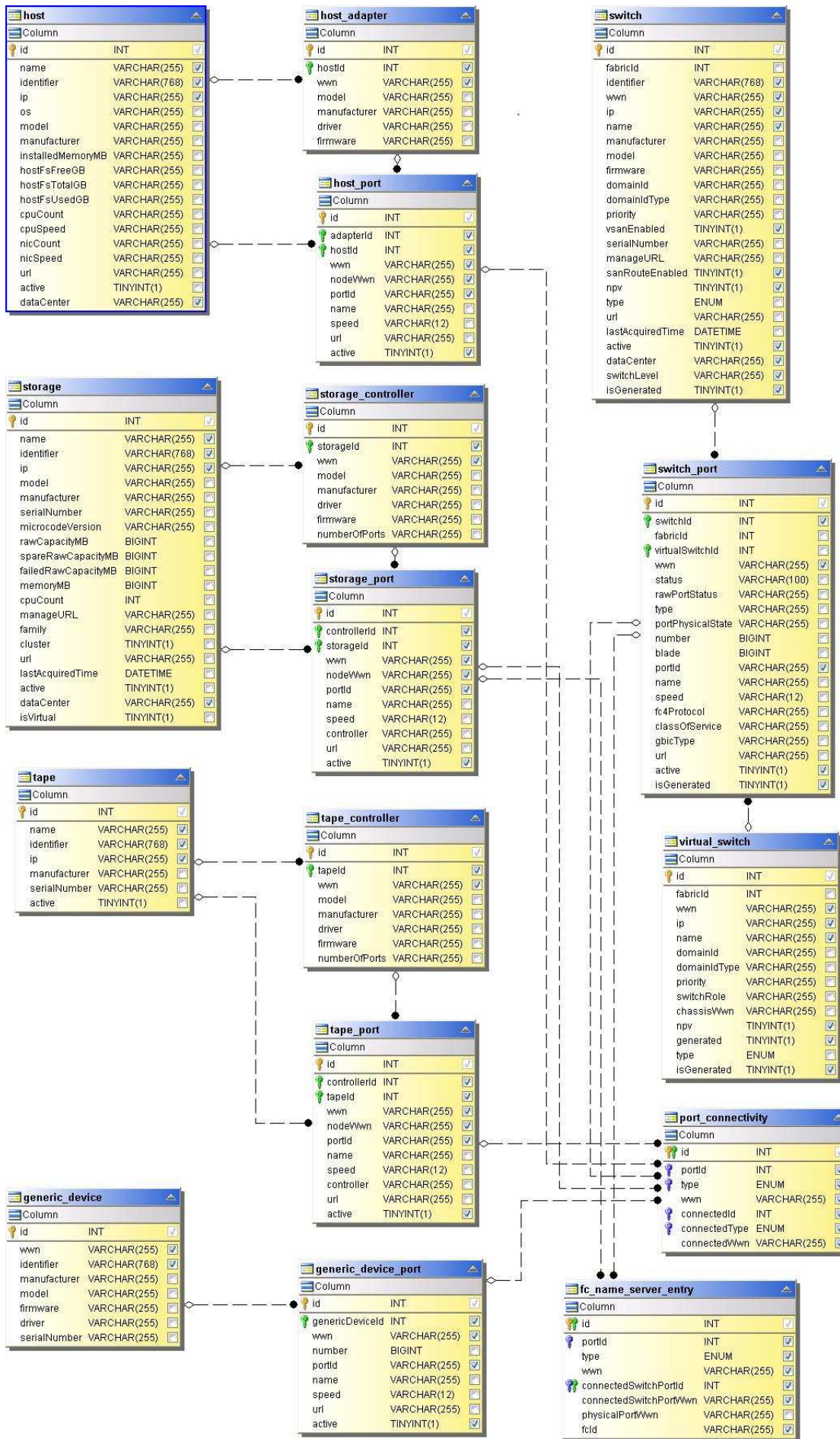




## 경로 및 위반

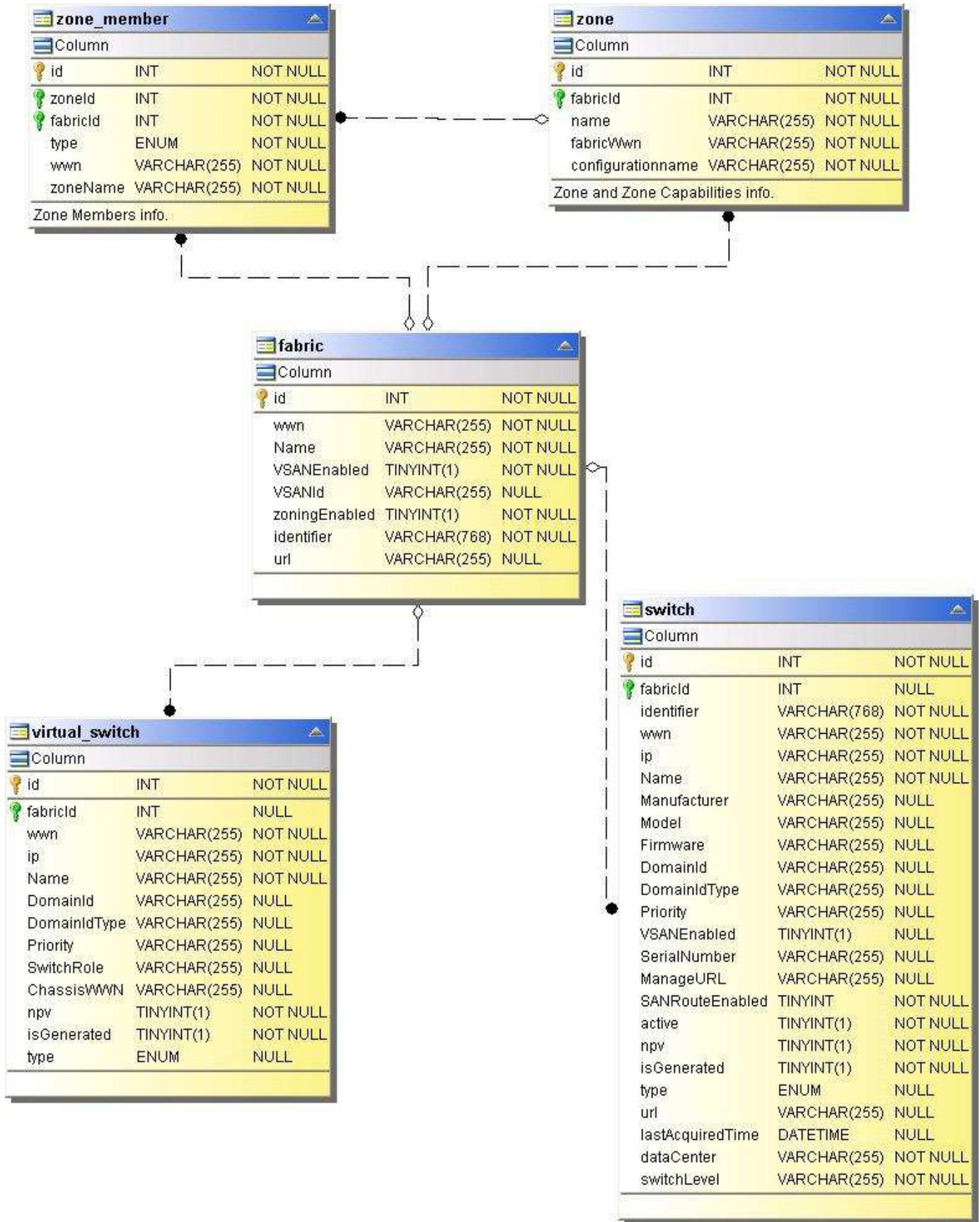


## 포트 연결



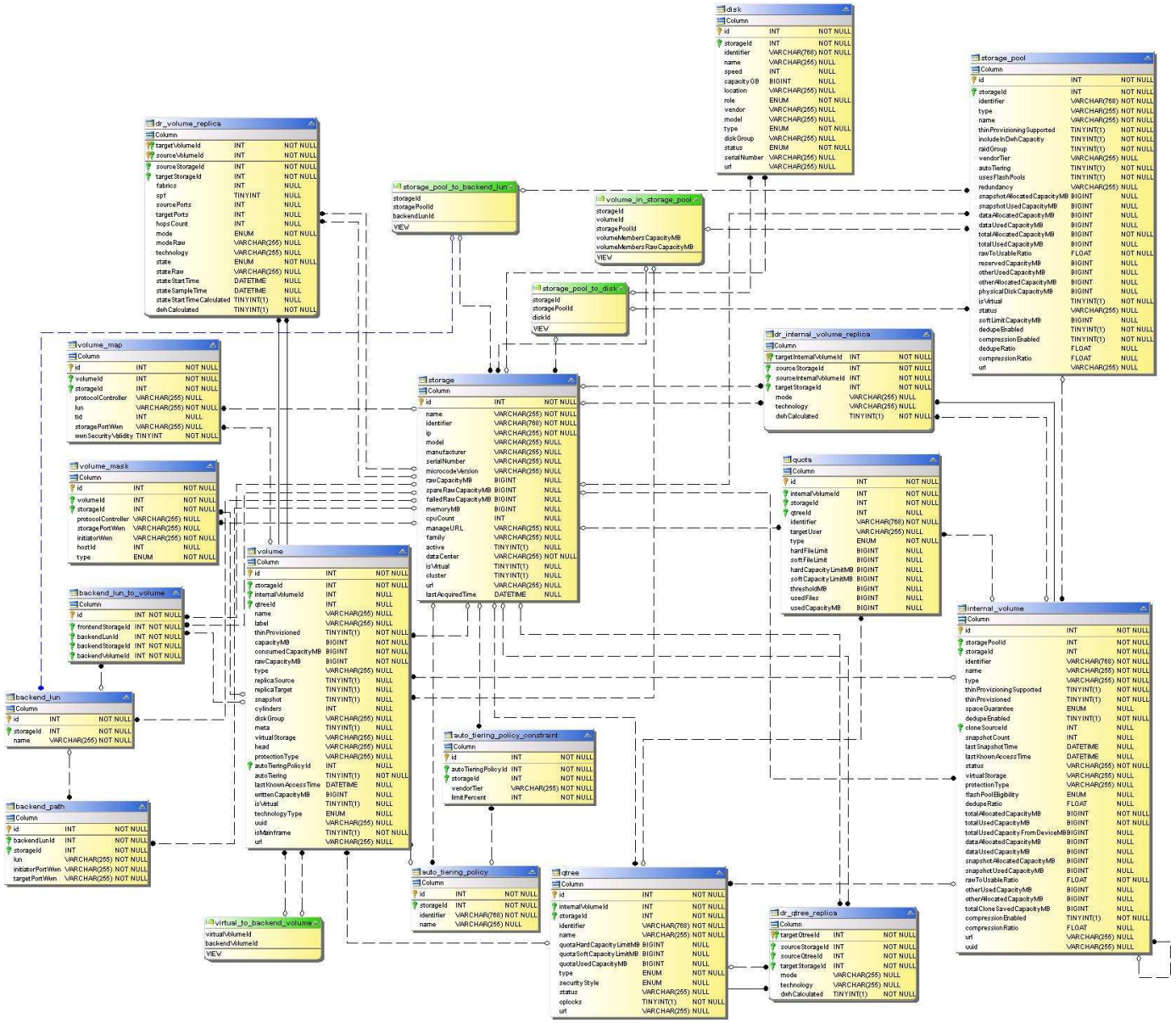


SAN 패브릭

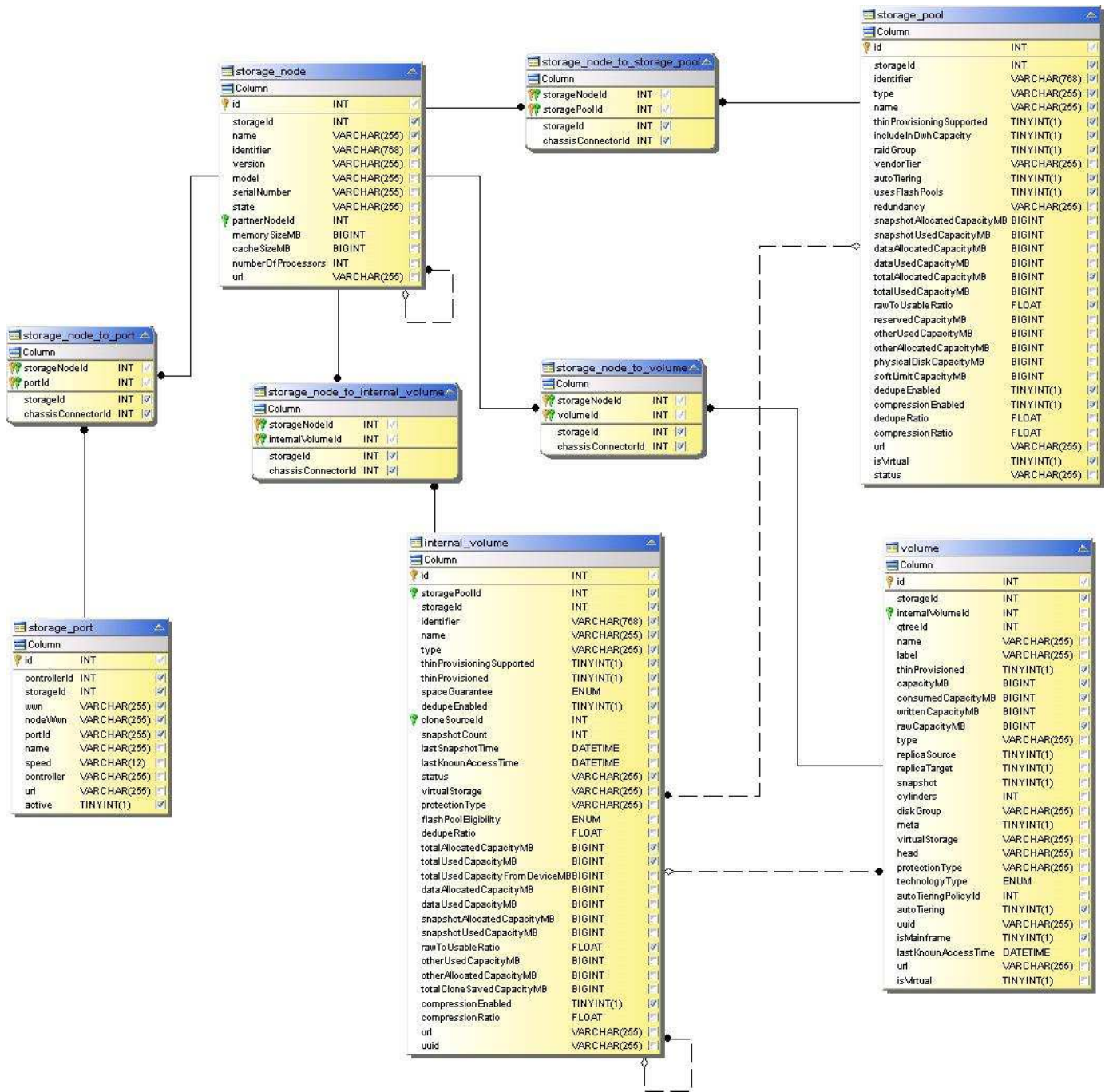




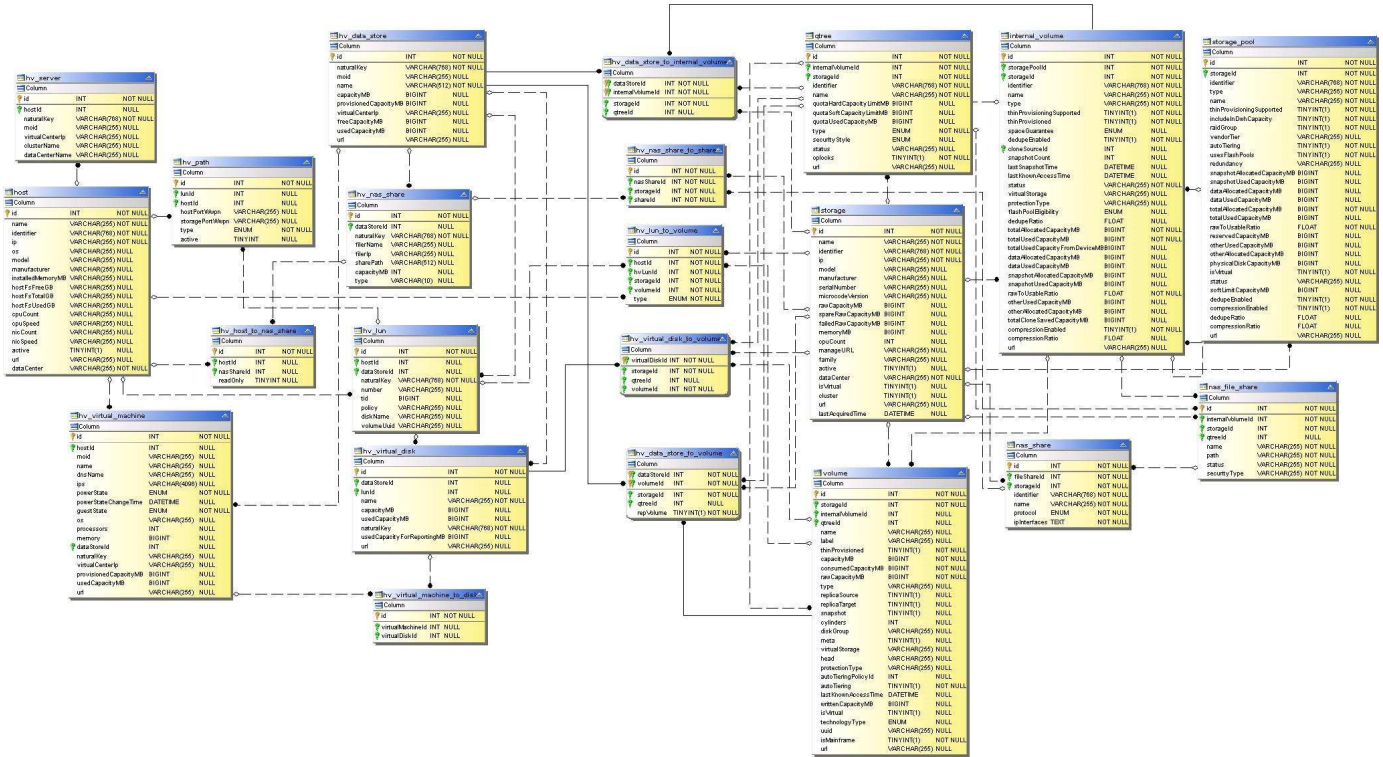
# 스토리지



# 스토리지 노트



VM

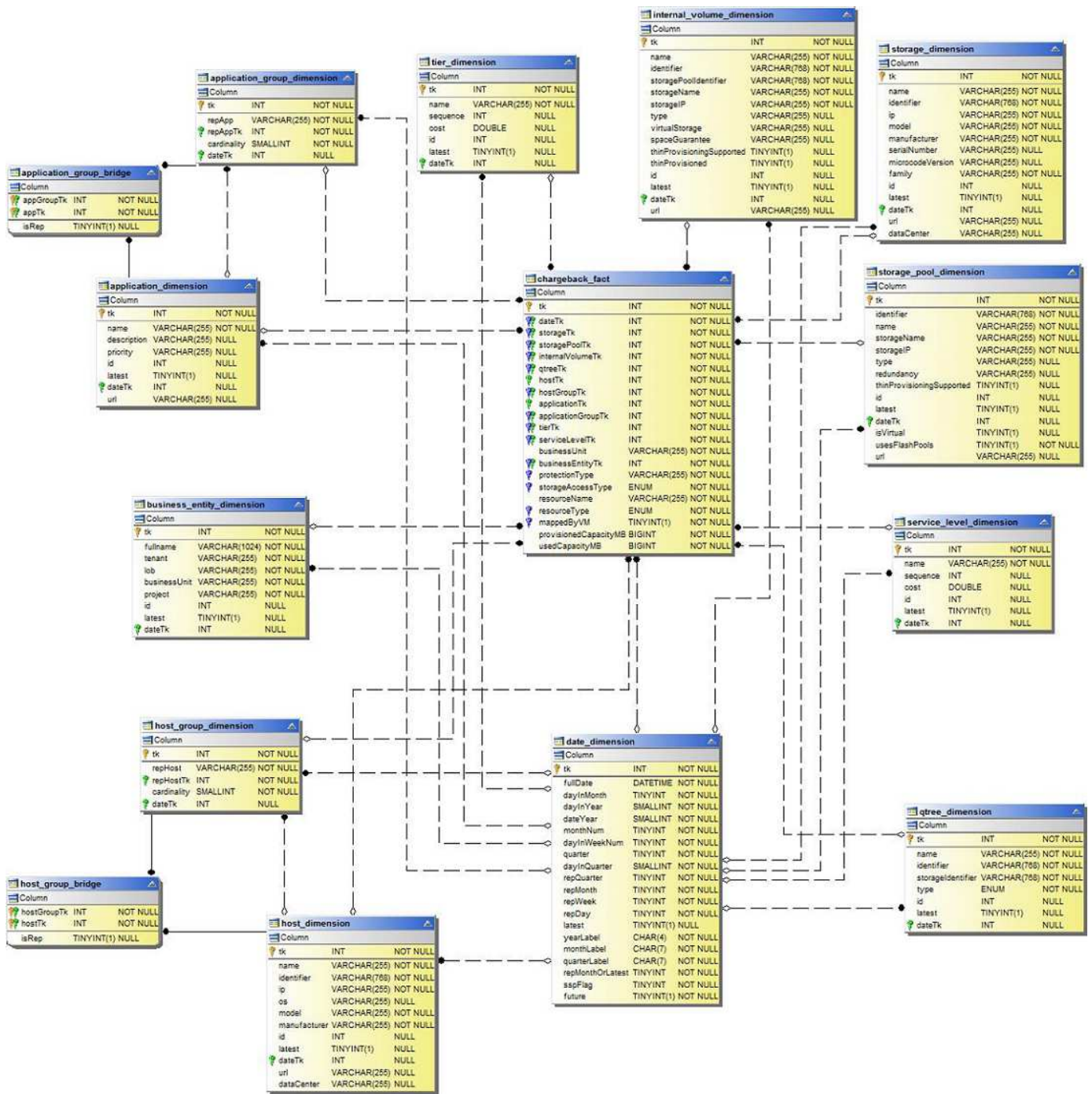


용량 데이터 매트

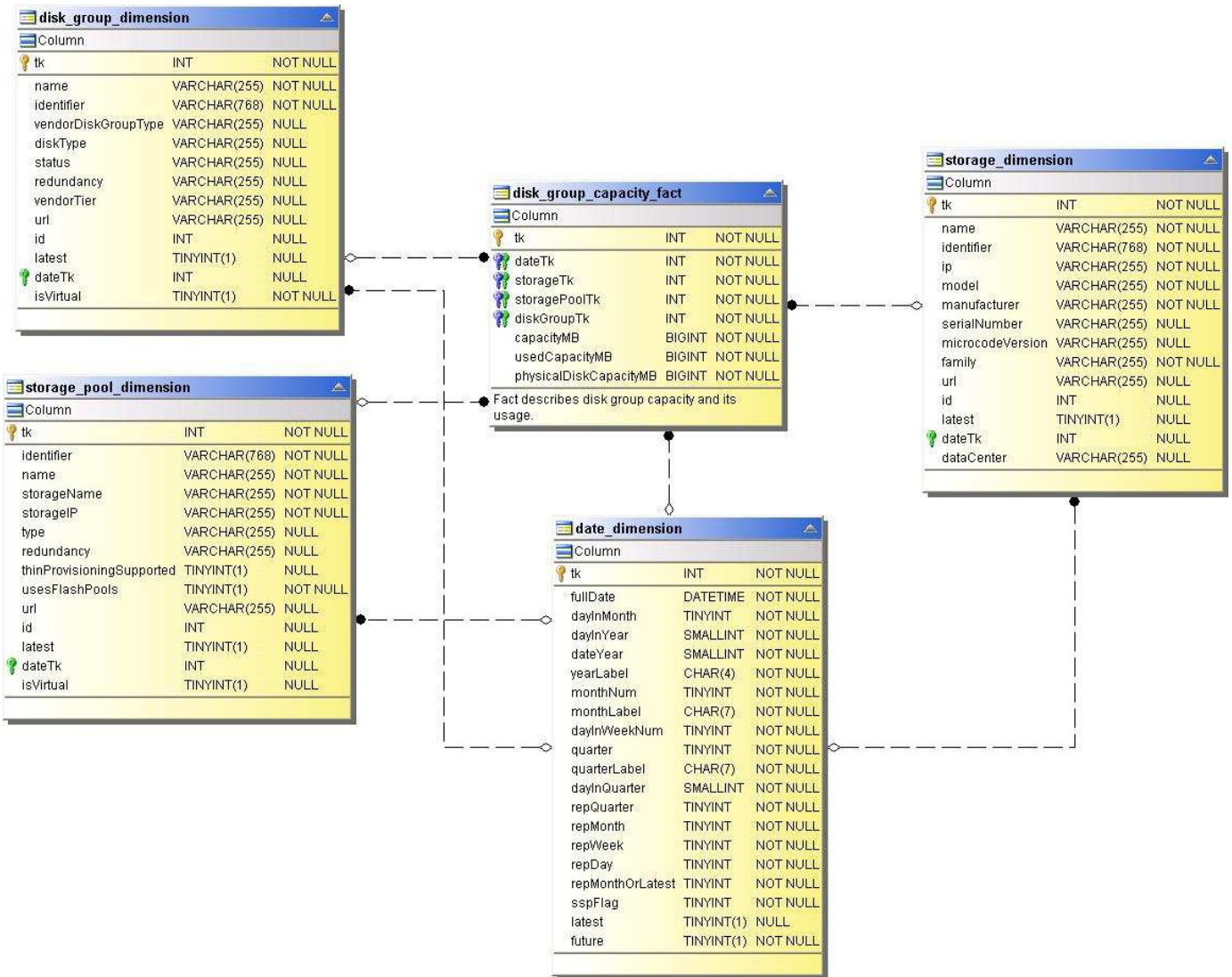
다음 이미지는 용량 데이터 매트에 대해 설명합니다.

비용 청구

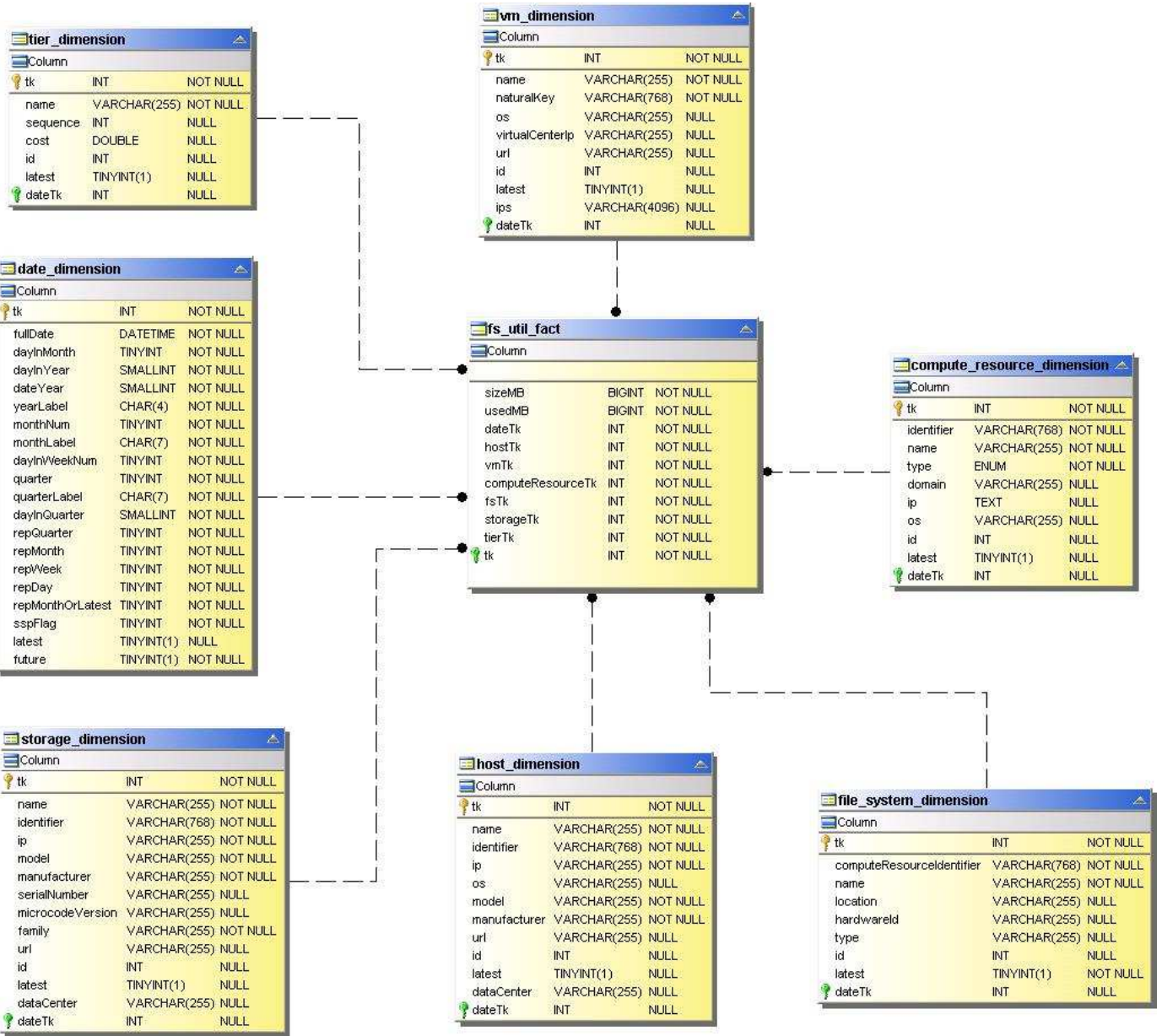




디스크 그룹 용량

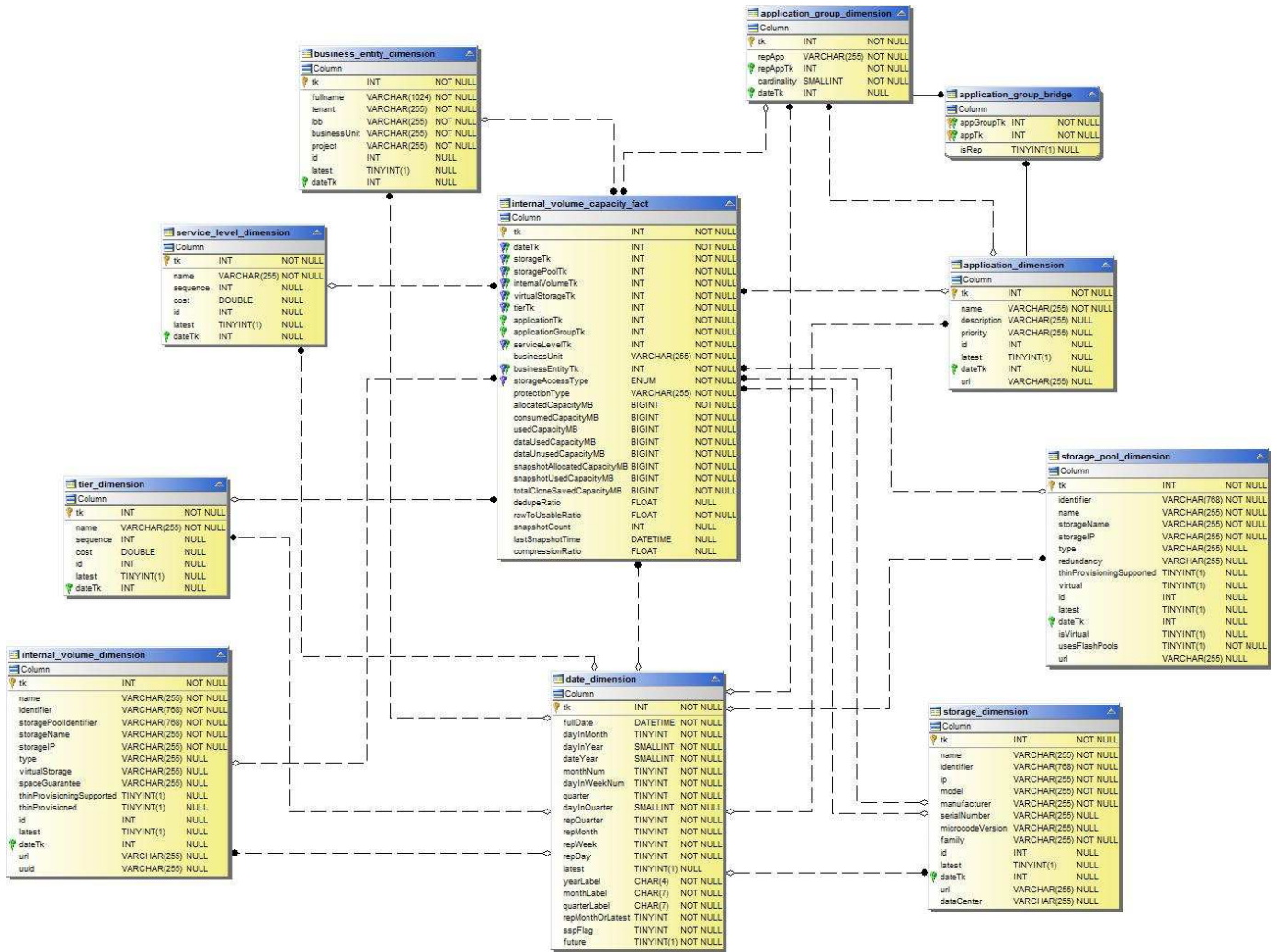


파일 시스템 활용률

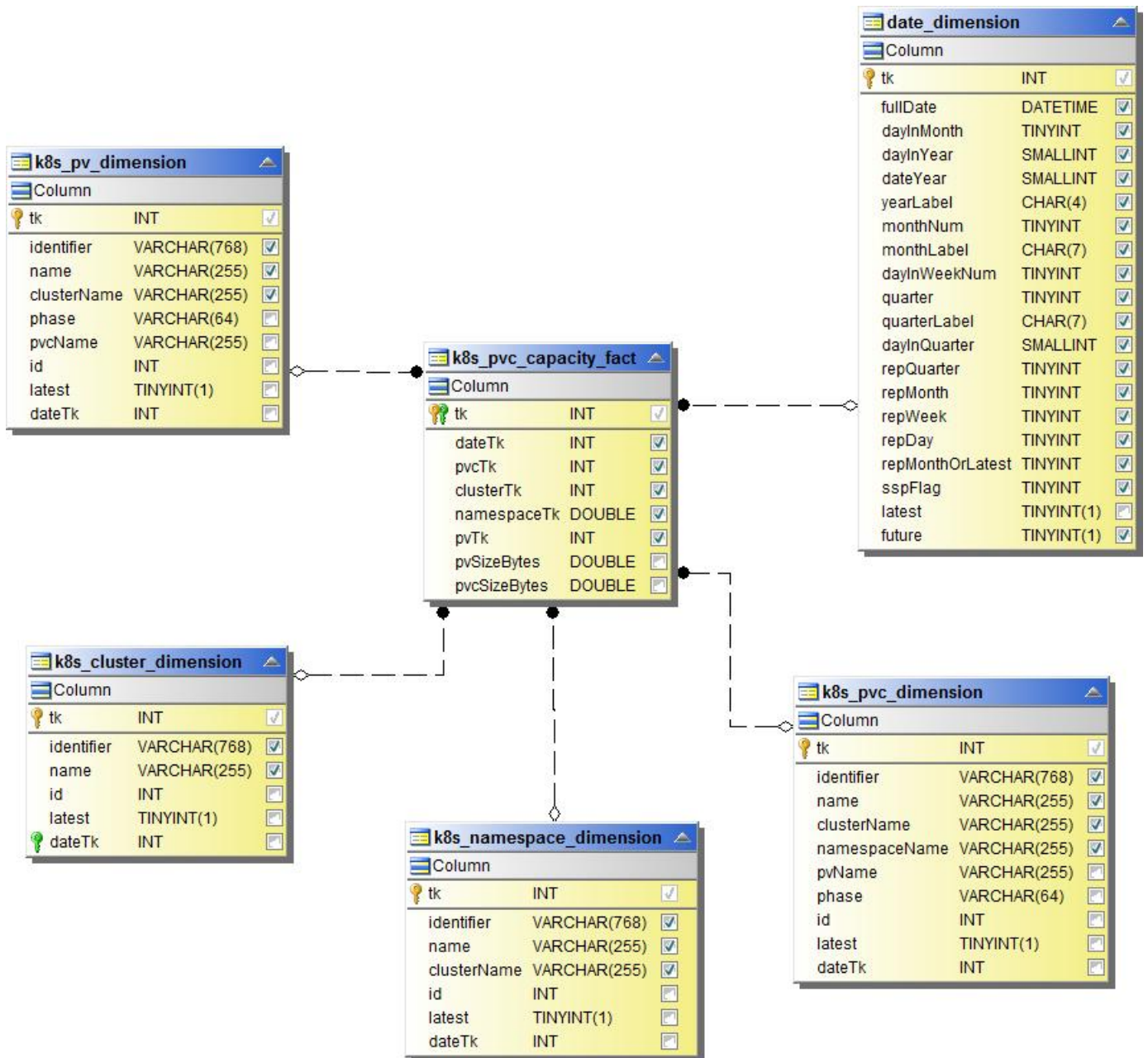


내부 볼륨 용량



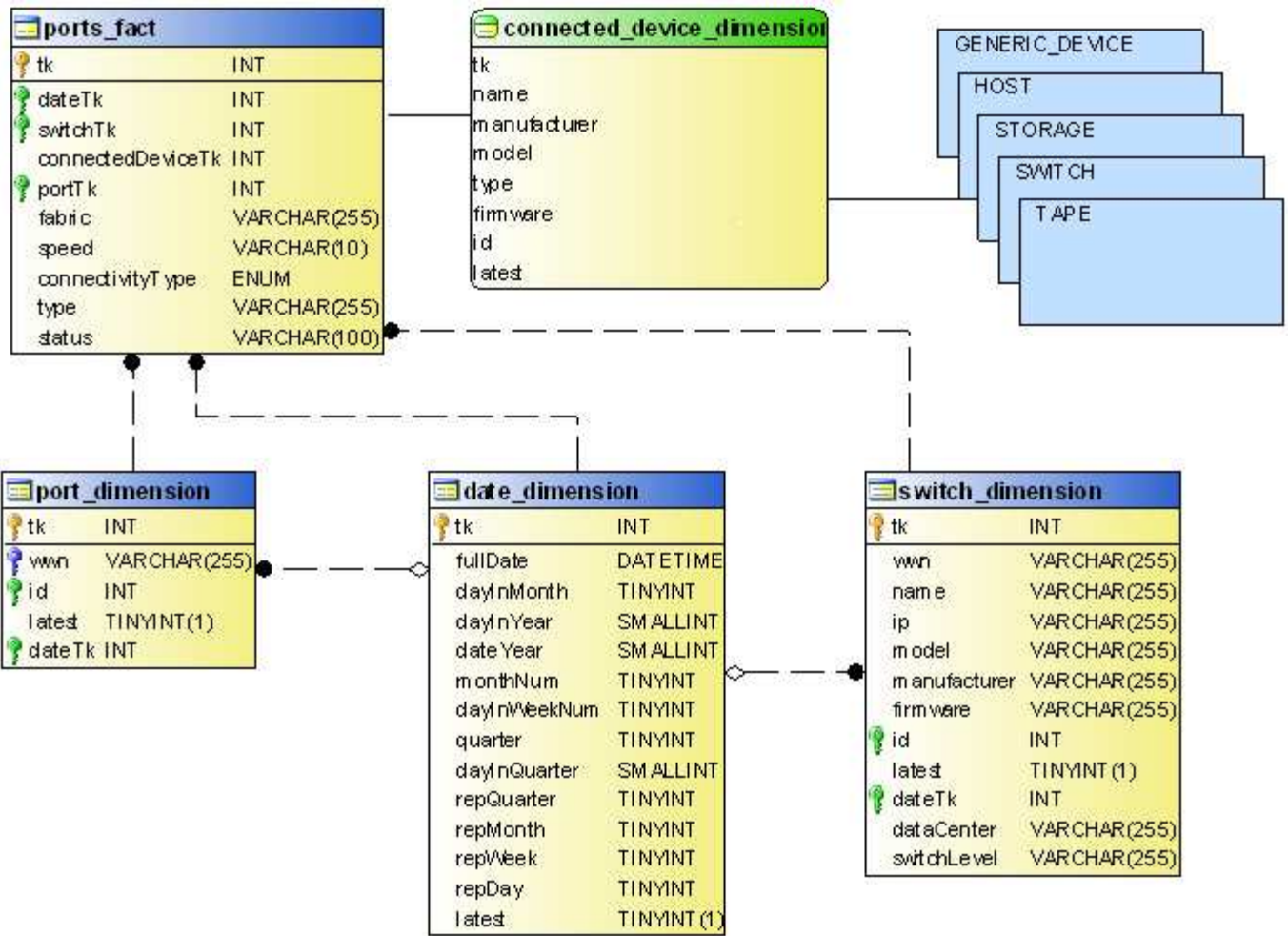


## Kubernetes PV 용량

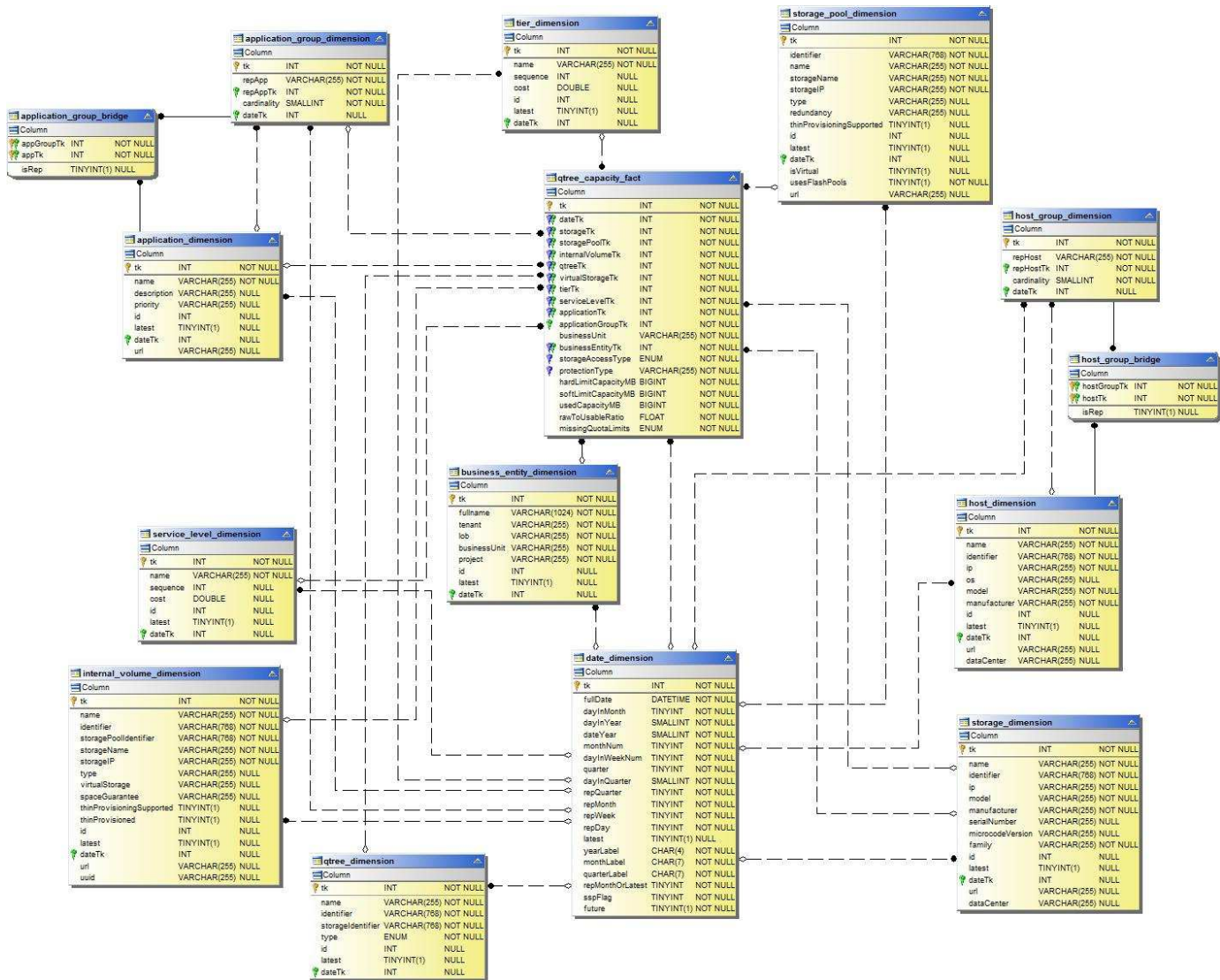


포트 용량





Qtree 용량



스토리지 용량 효율성

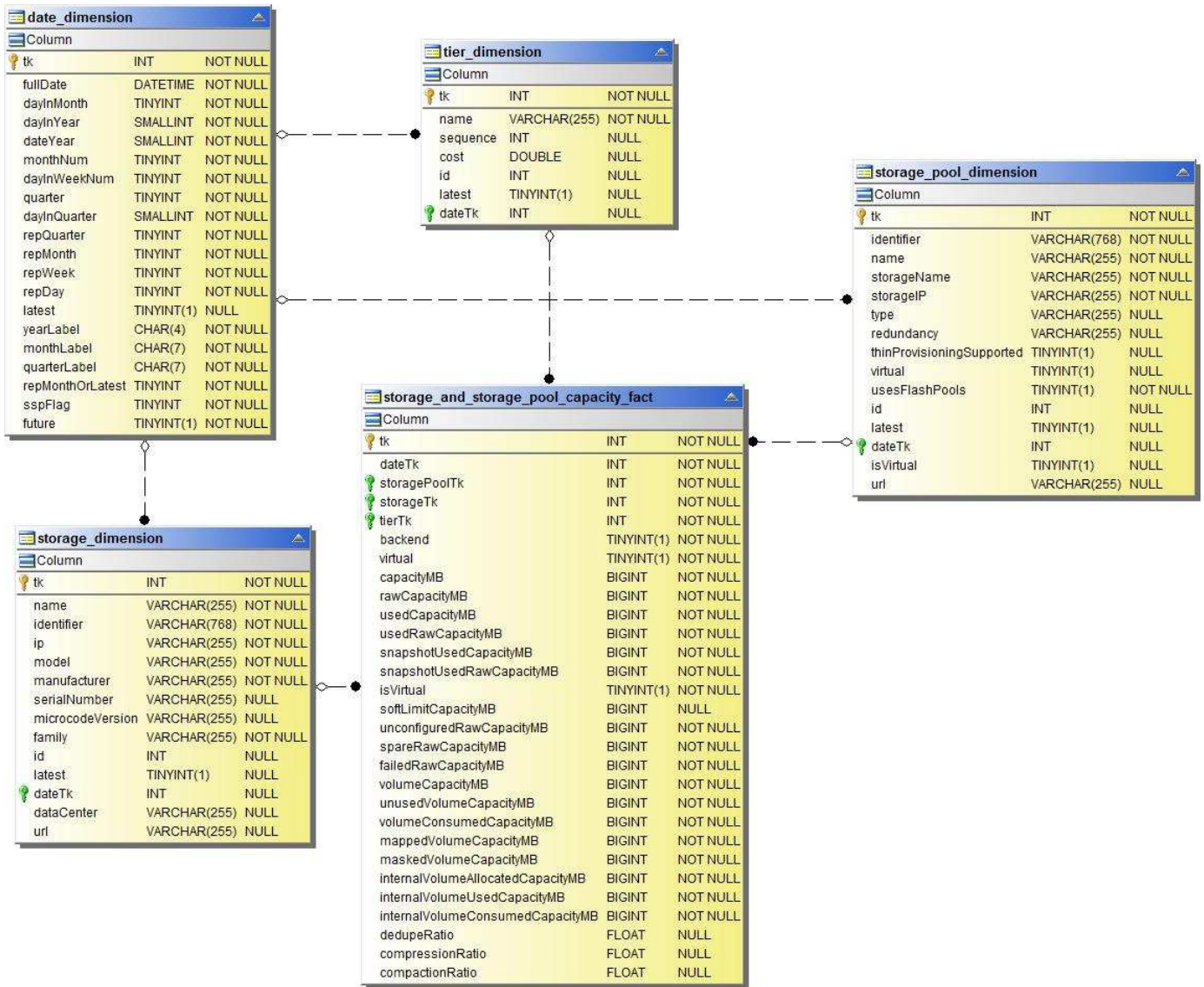
efficiency_fact			
Column			
tk	INT	NOT NULL	
dateTk	INT	NOT NULL	
storageTk	INT	NOT NULL	
rawCapacityMB	BIGINT	NOT NULL	
backendCapacityMB	BIGINT	NOT NULL	
storageTechnology	VARCHAR(255)	NULL	
gainMB	BIGINT	NOT NULL	
lossMB	BIGINT	NOT NULL	
potentialGainMB	BIGINT	NOT NULL	
potentialLossMB	BIGINT	NOT NULL	

date_dimension			
Column			
tk	INT	NOT NULL	
fullDate	DATETIME	NOT NULL	
dayInMonth	TINYINT	NOT NULL	
dayInYear	SMALLINT	NOT NULL	
dateYear	SMALLINT	NOT NULL	
monthNum	TINYINT	NOT NULL	
dayInWeekNum	TINYINT	NOT NULL	
quarter	TINYINT	NOT NULL	
dayInQuarter	SMALLINT	NOT NULL	
repQuarter	TINYINT	NOT NULL	
repMonth	TINYINT	NOT NULL	
repWeek	TINYINT	NOT NULL	
repDay	TINYINT	NOT NULL	
latest	TINYINT(1)	NULL	
yearLabel	CHAR(4)	NOT NULL	
monthLabel	CHAR(7)	NOT NULL	
quarterLabel	CHAR(7)	NOT NULL	
repMonthOrLatest	TINYINT	NOT NULL	
sspFlag	TINYINT	NOT NULL	
future	TINYINT(1)	NOT NULL	

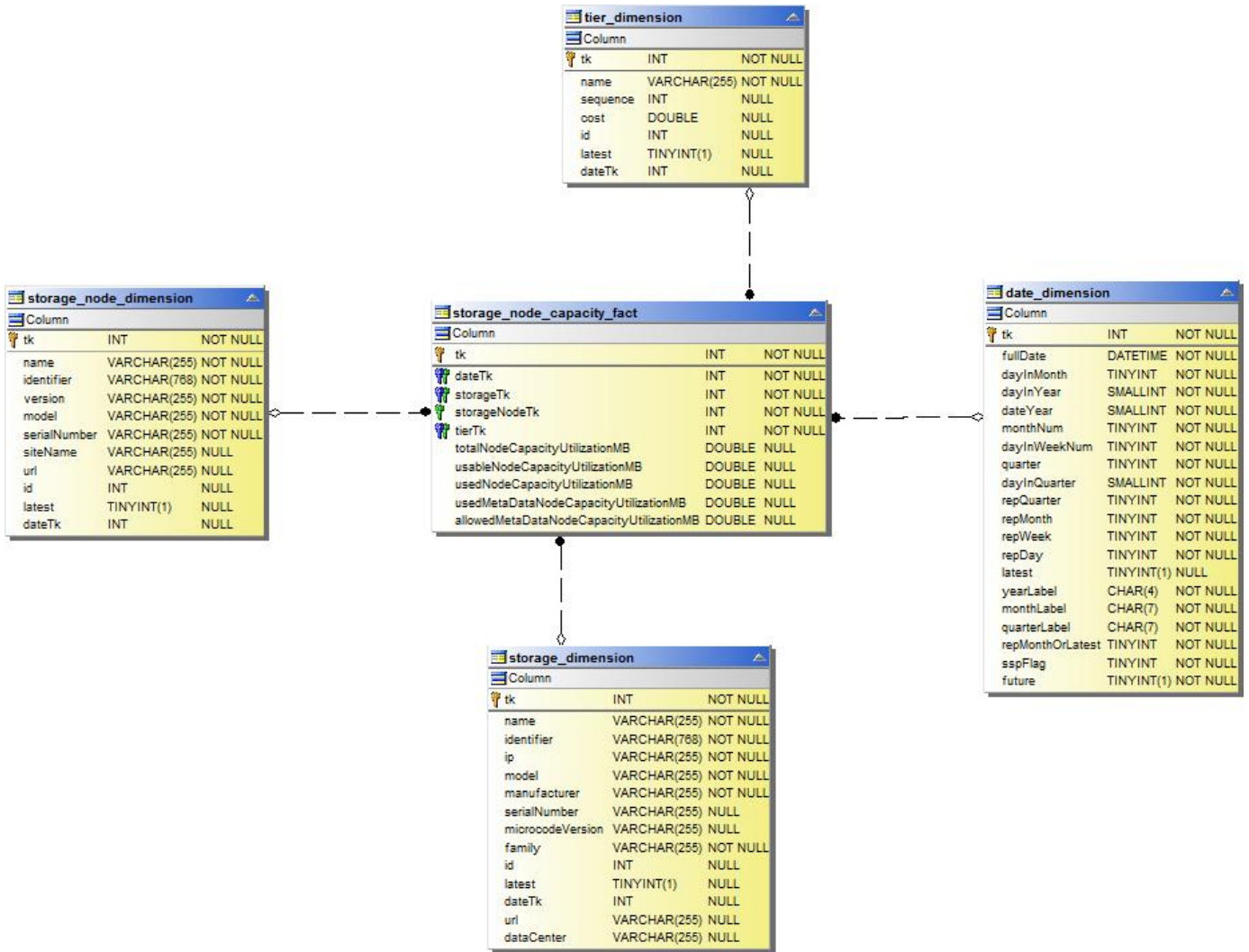
storage_dimension			
Column			
tk	INT	NOT NULL	
name	VARCHAR(255)	NOT NULL	
identifier	VARCHAR(768)	NOT NULL	
ip	VARCHAR(255)	NOT NULL	
model	VARCHAR(255)	NOT NULL	
manufacturer	VARCHAR(255)	NOT NULL	
serialNumber	VARCHAR(255)	NULL	
microcodeVersion	VARCHAR(255)	NULL	
family	VARCHAR(255)	NOT NULL	
id	INT	NULL	
latest	TINYINT(1)	NULL	
dateTk	INT	NULL	
url	VARCHAR(255)	NULL	
dataCenter	VARCHAR(255)	NULL	

스토리지 및 스토리지 풀 용량

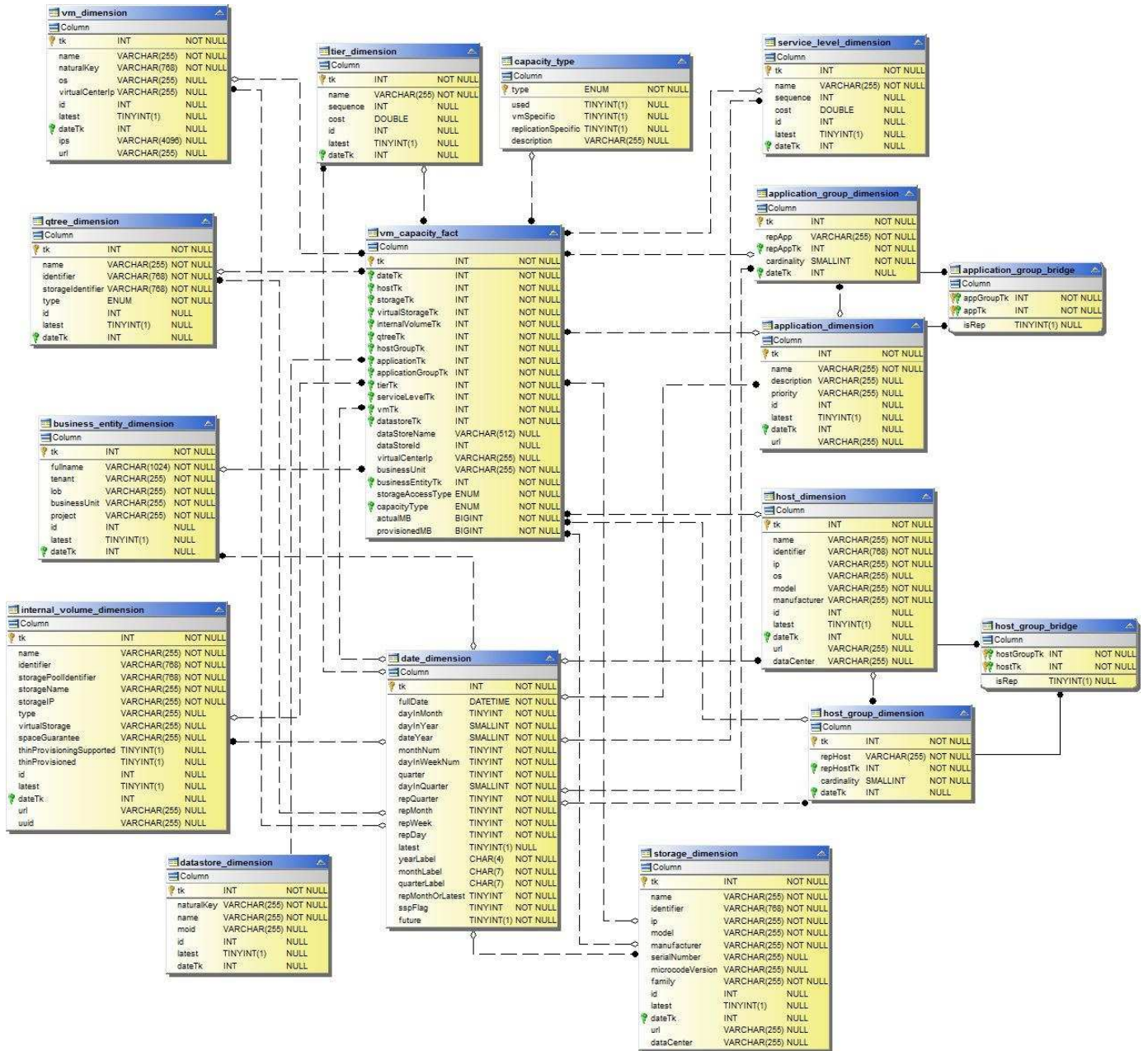




스토리지 노드 용량

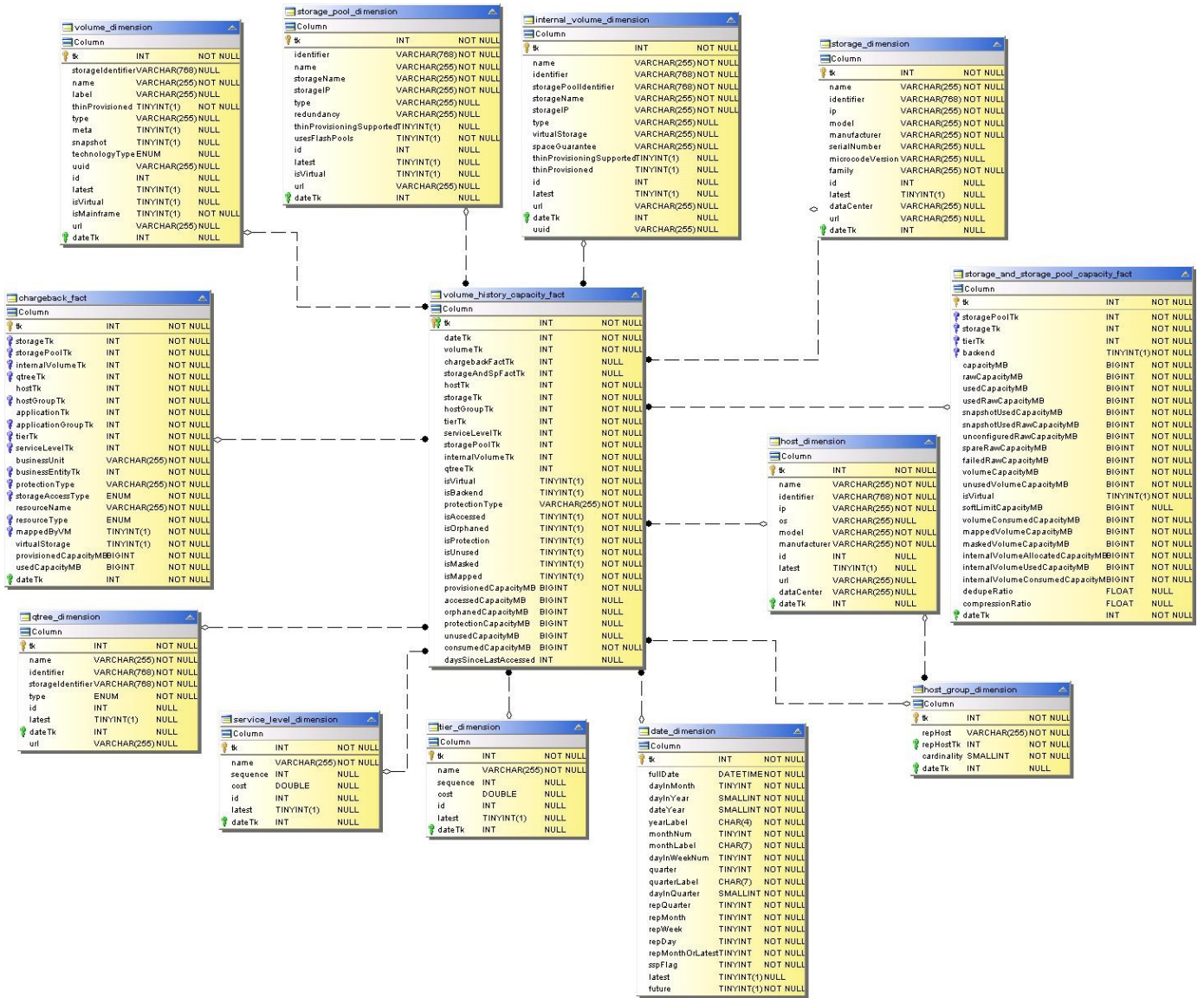


VM 용량



제품 용량

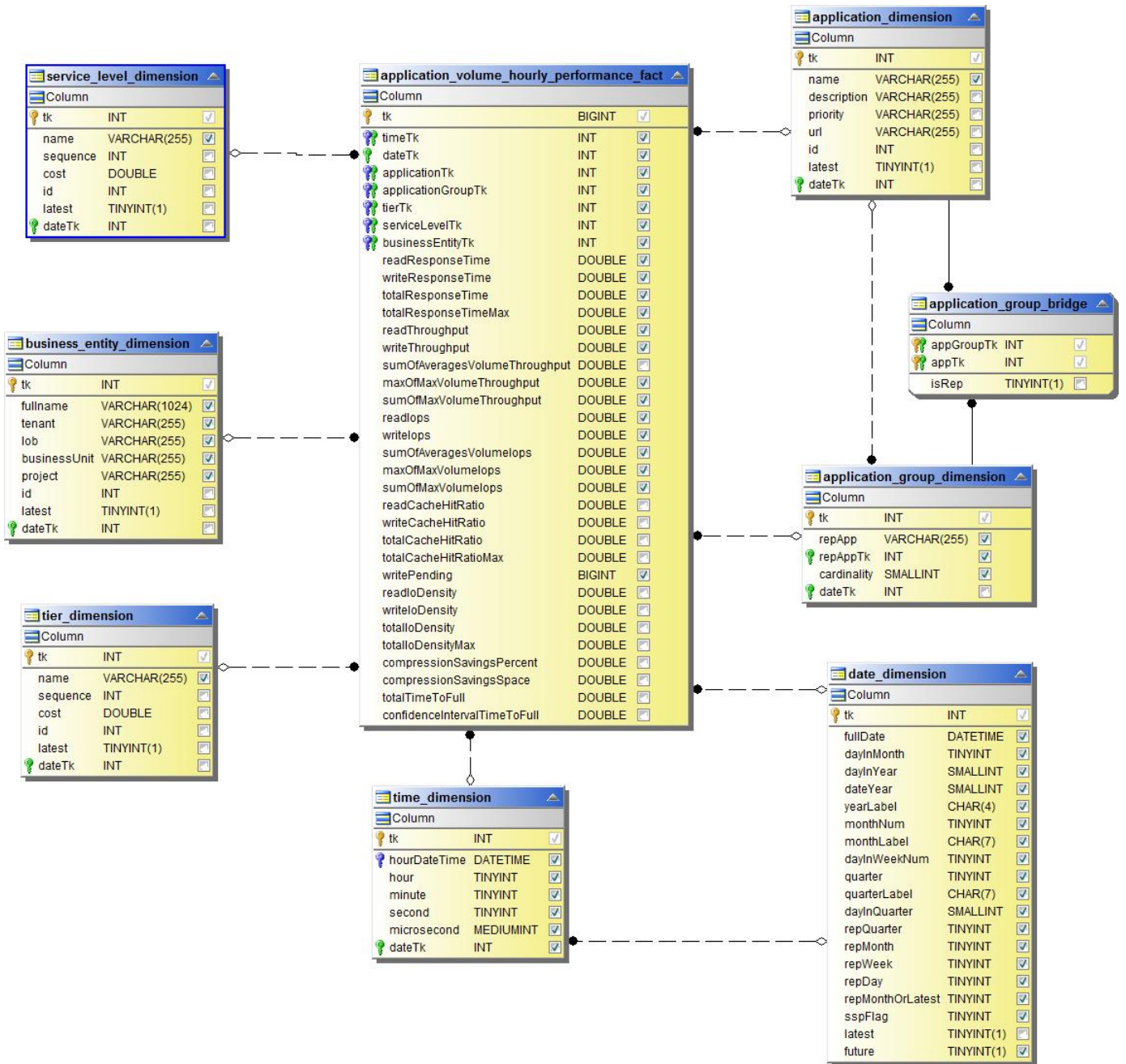




## 성능 데이터 센터

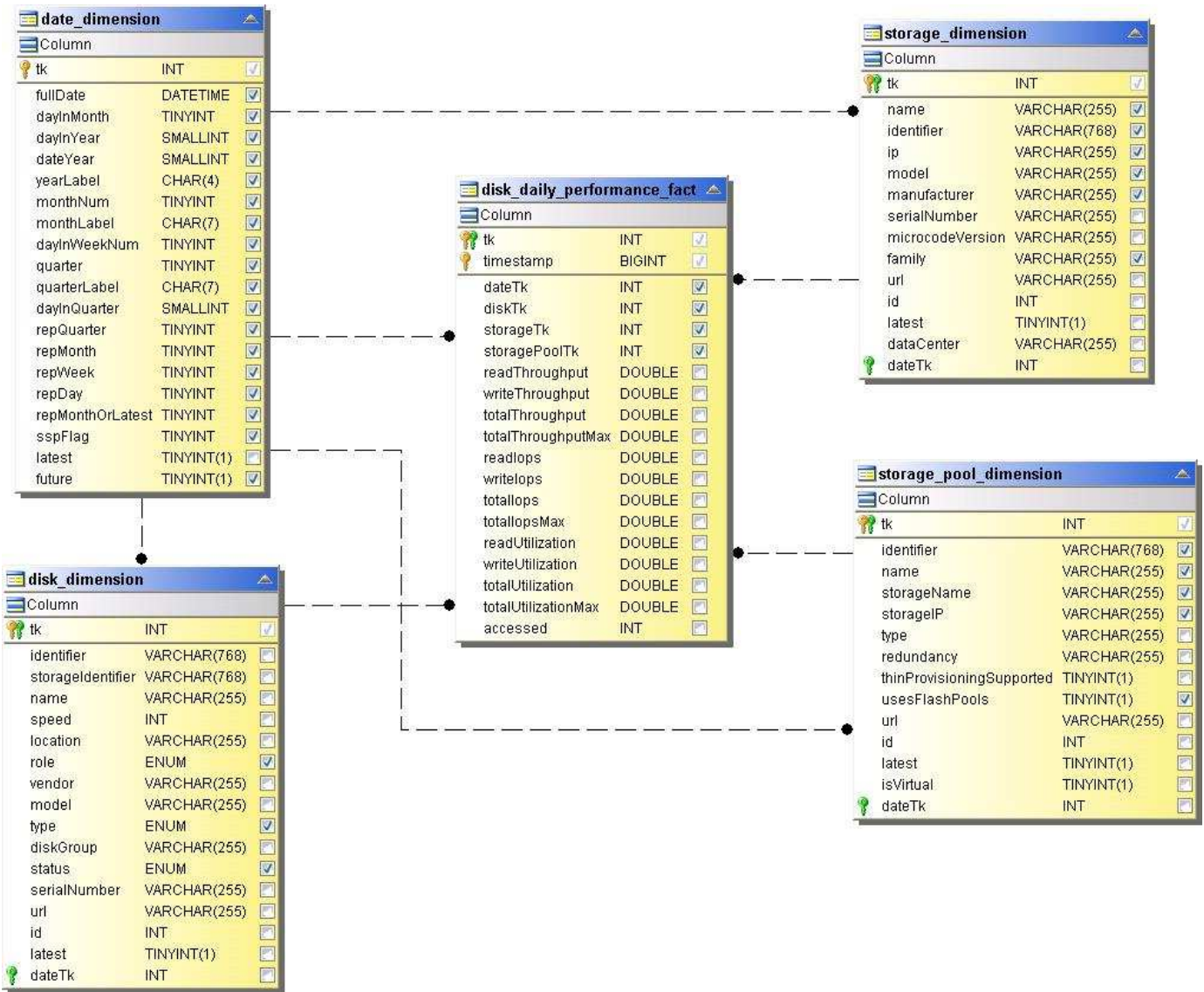
다음 이미지는 성능 데이터 마트에 대해 설명합니다.

애플리케이션 볼륨의 시간별 성능

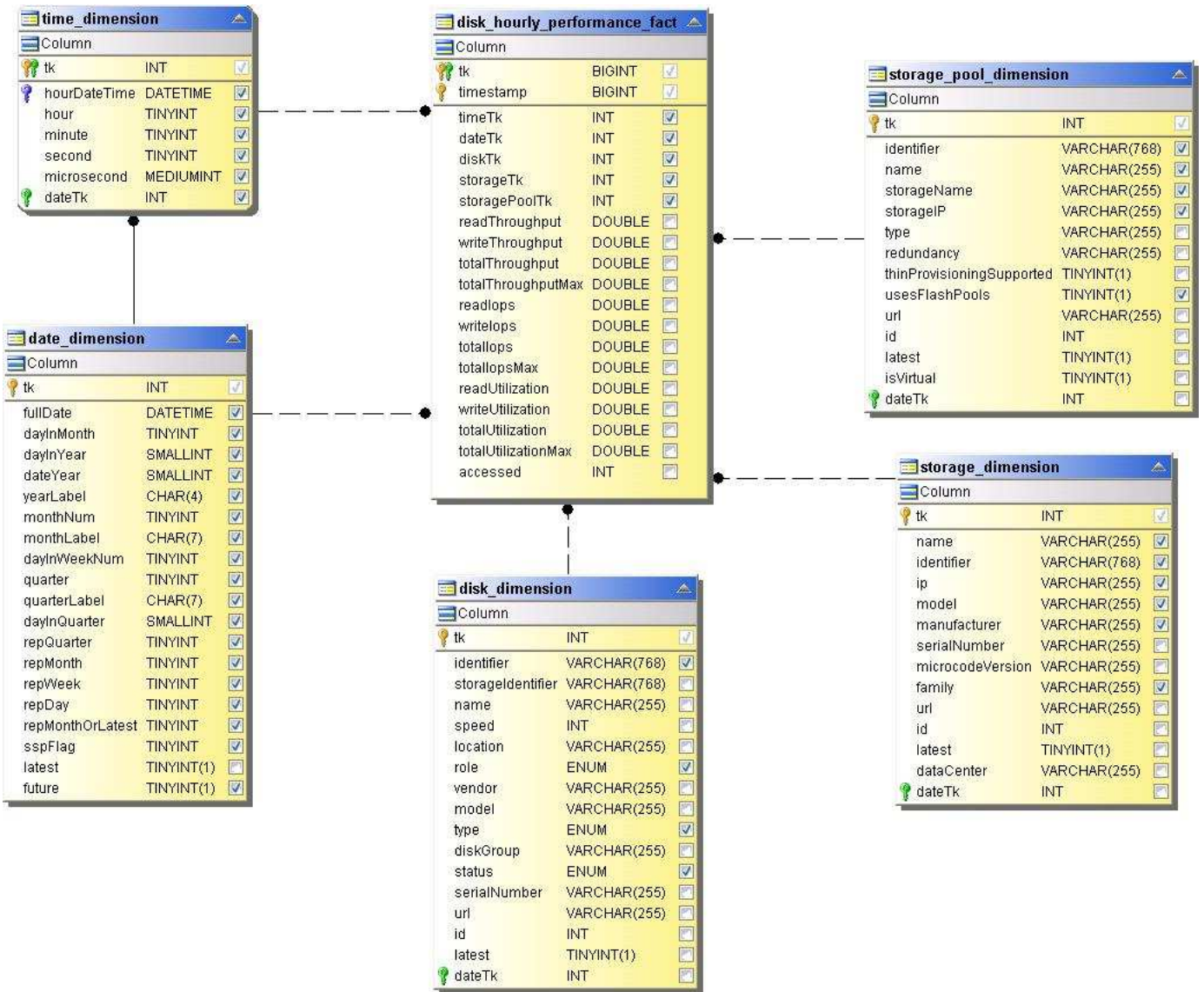


디스크 일일 성능

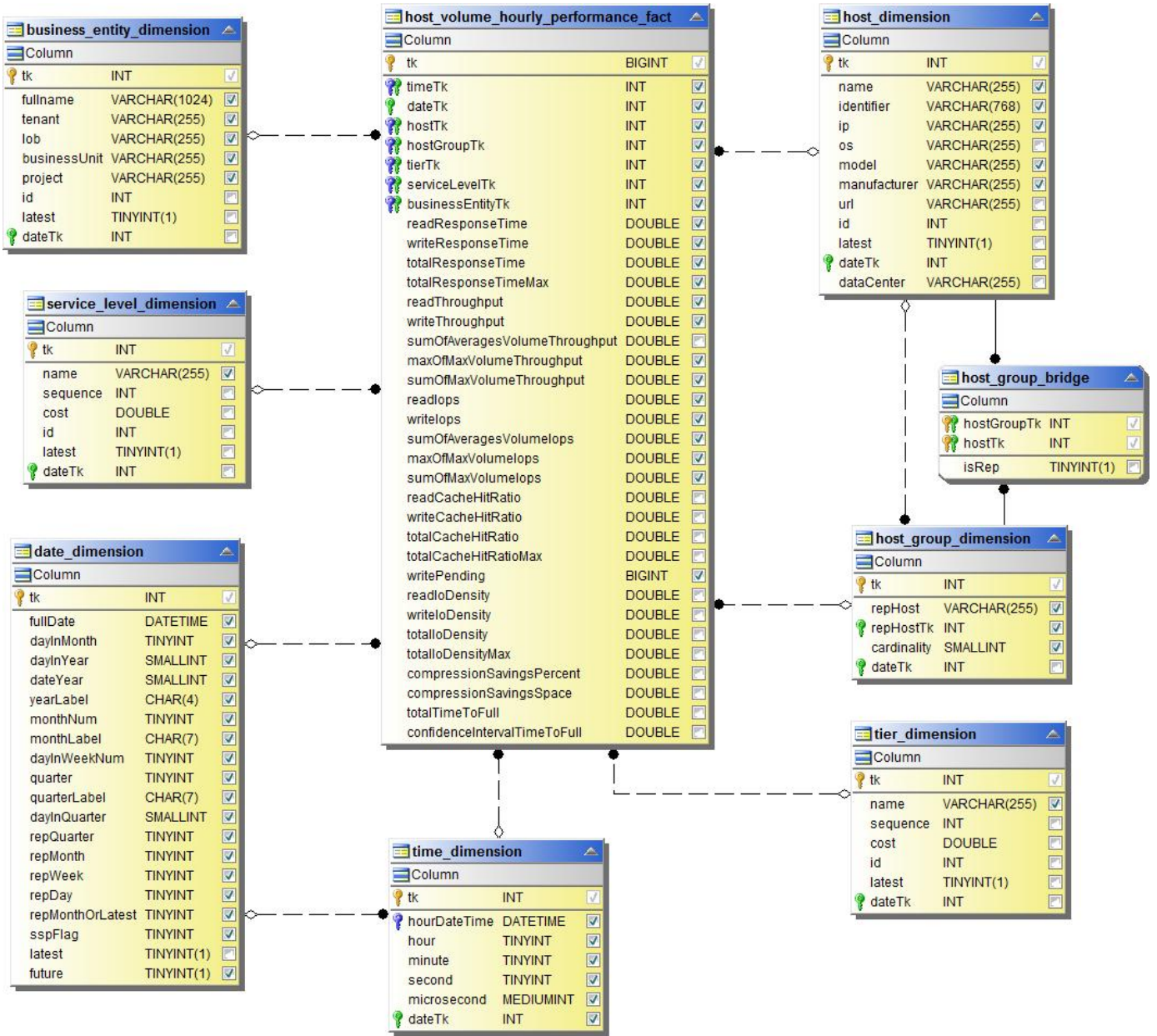




디스크 시간별 성능

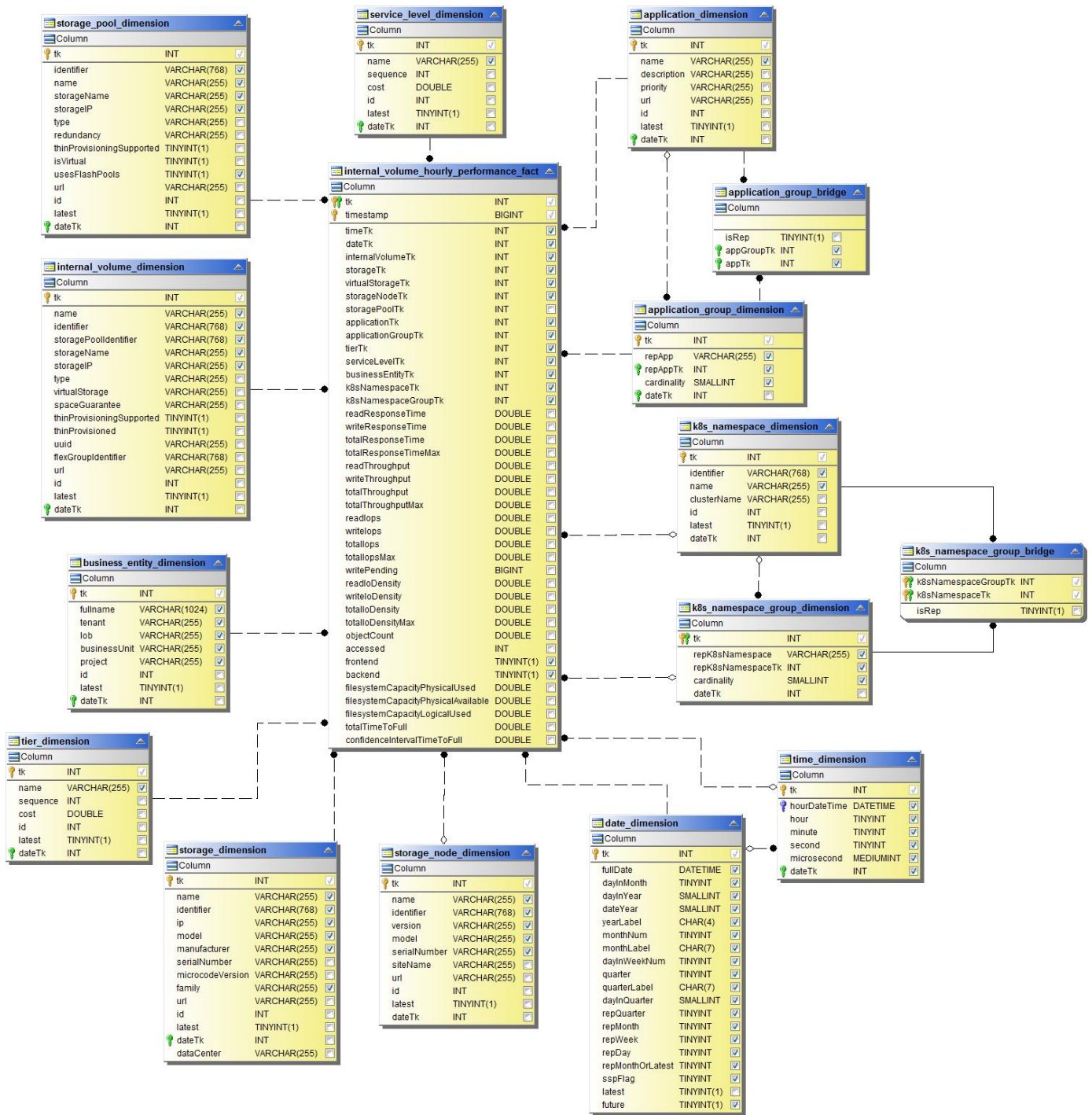


호스트 시간별 성능

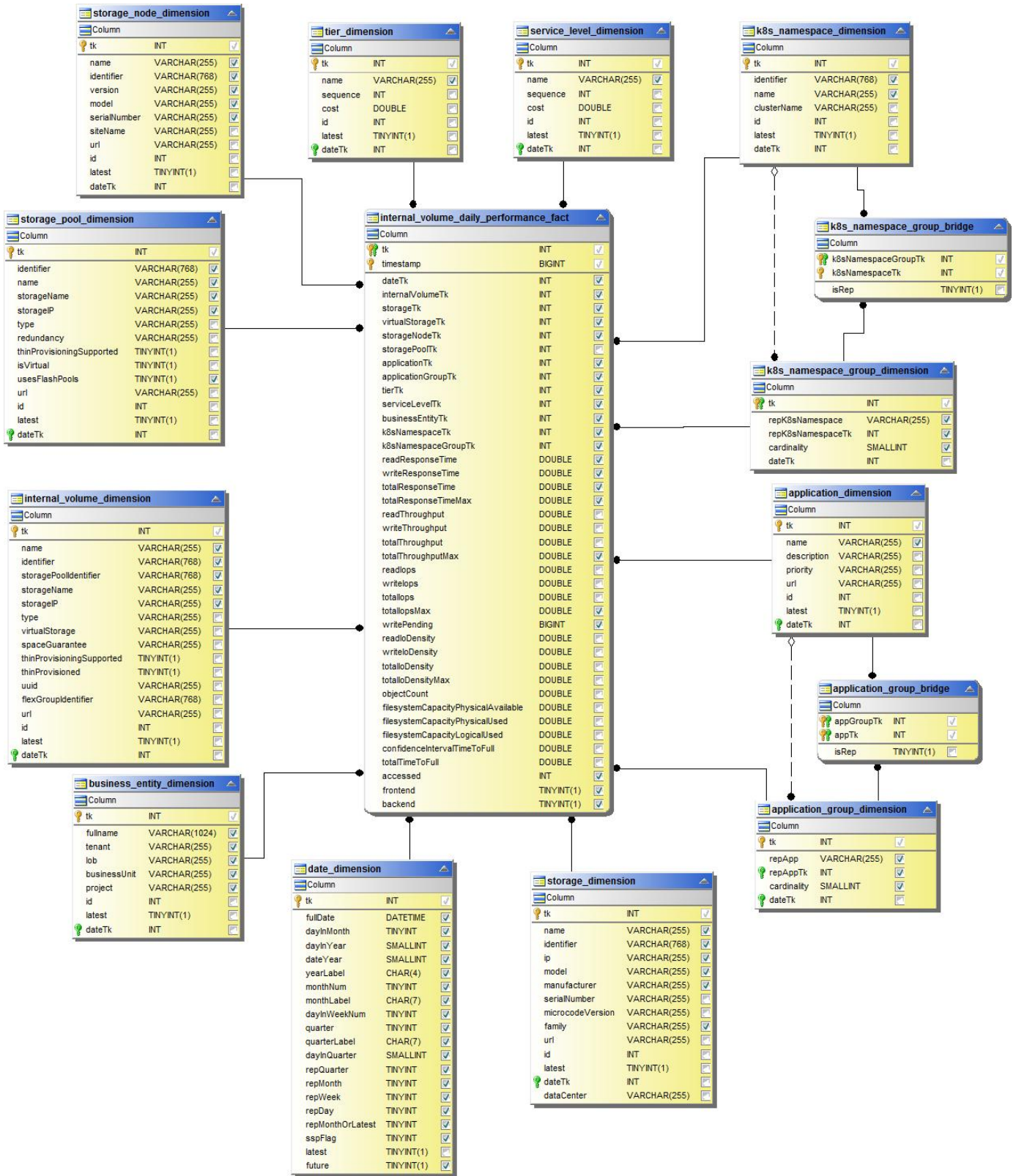


내부 볼륨 시간별 성능



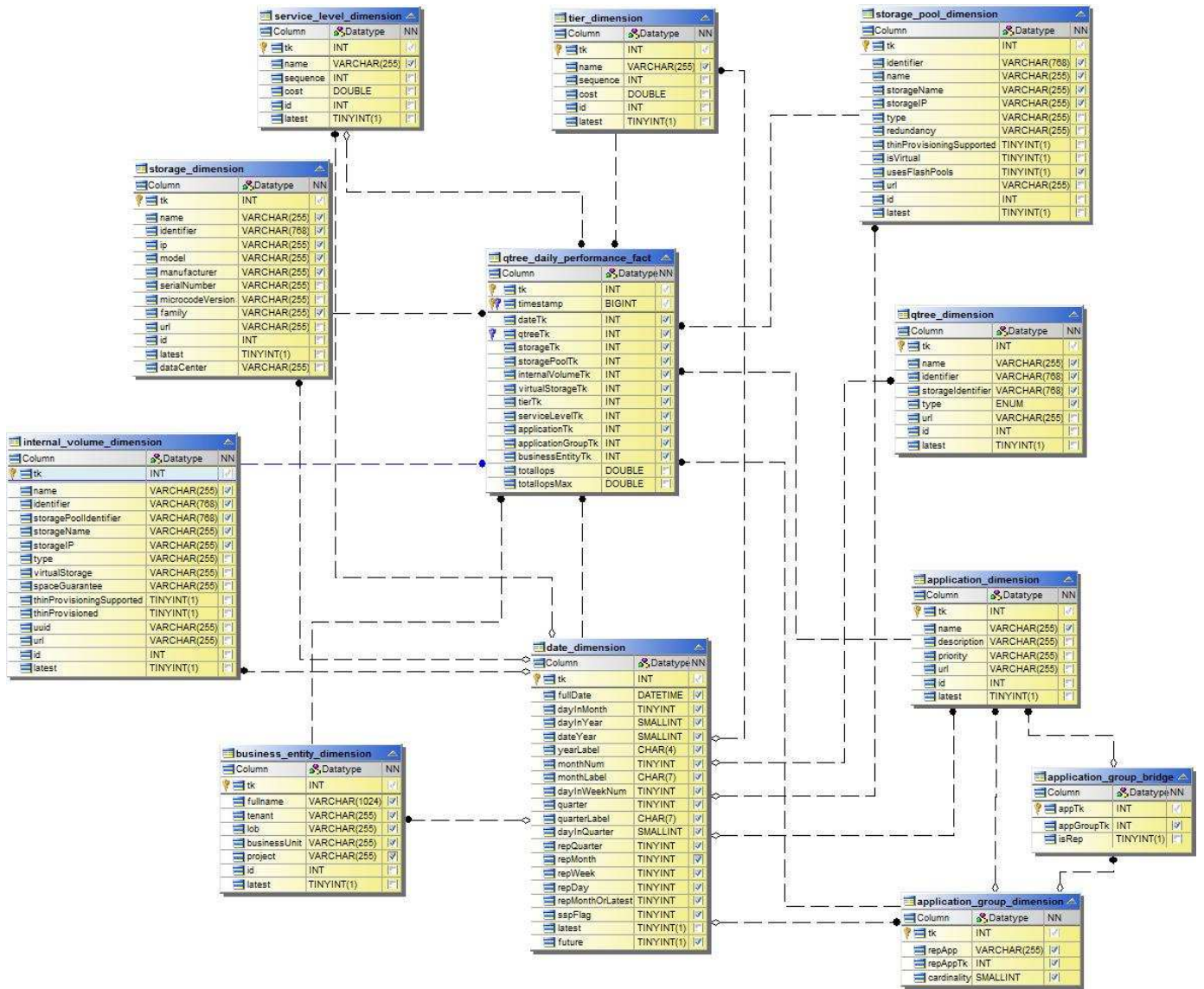


내부 볼륨 일일 성능

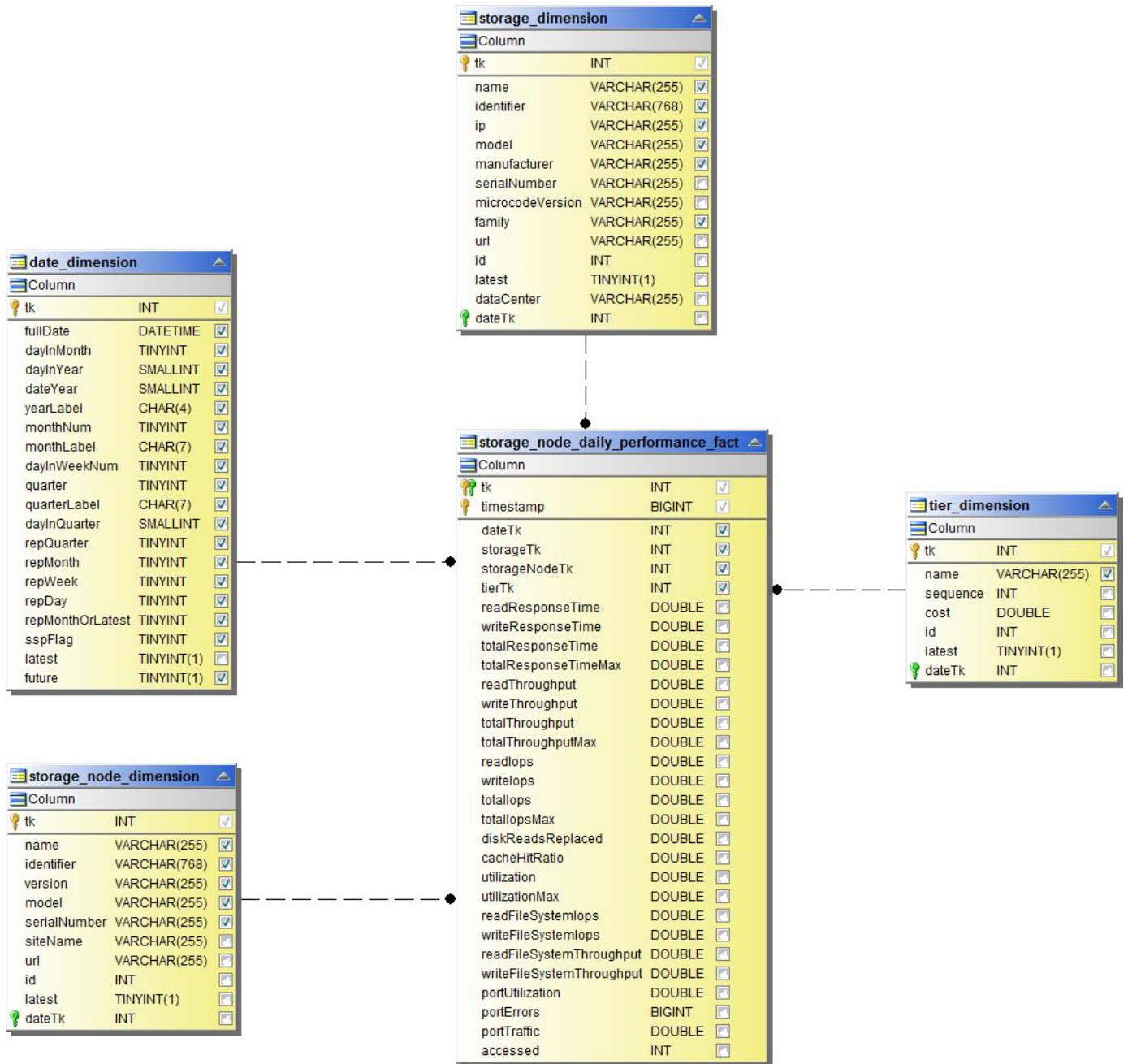


Qtree 일별 성능

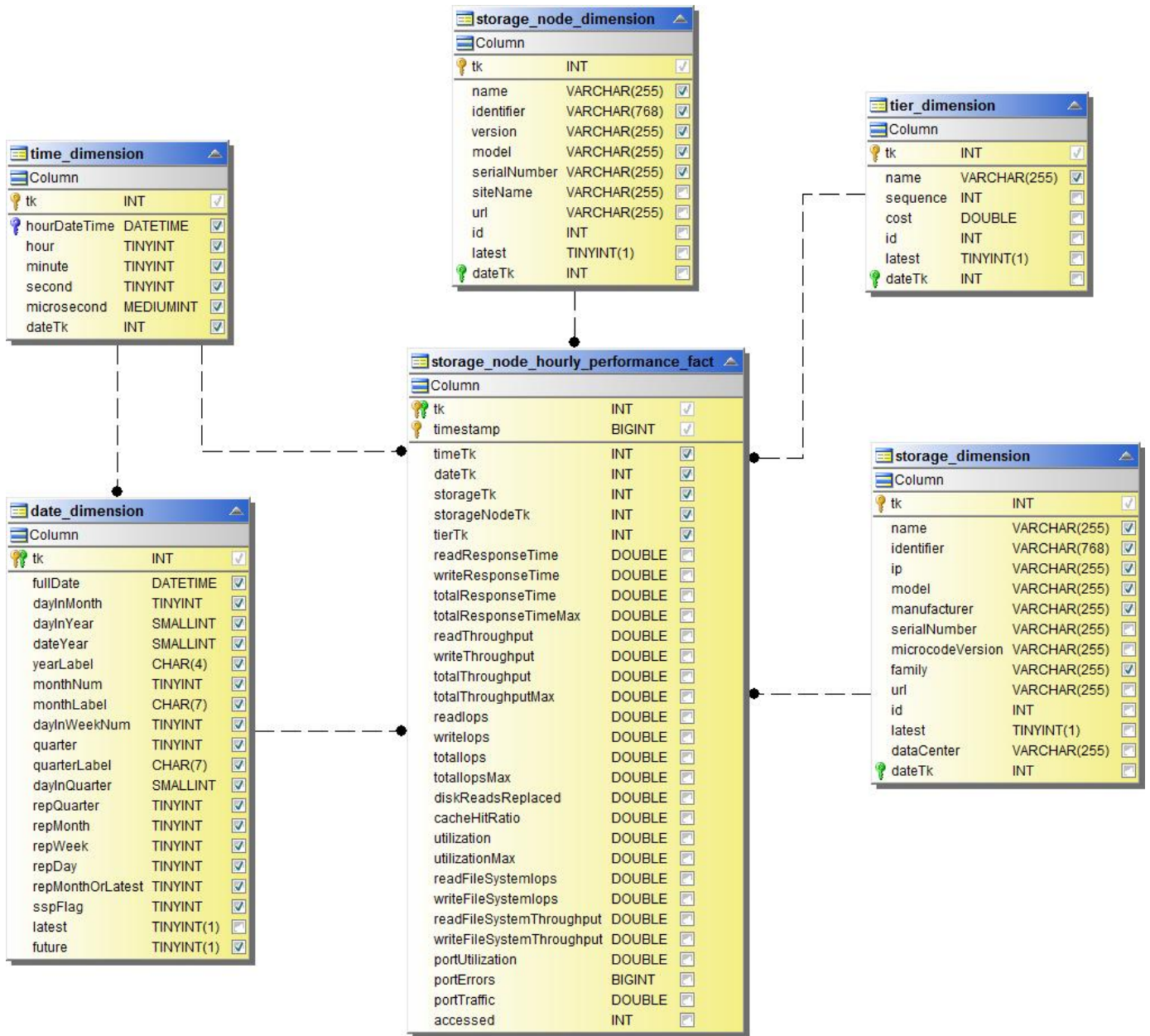




스토리지 노드 일별 성능

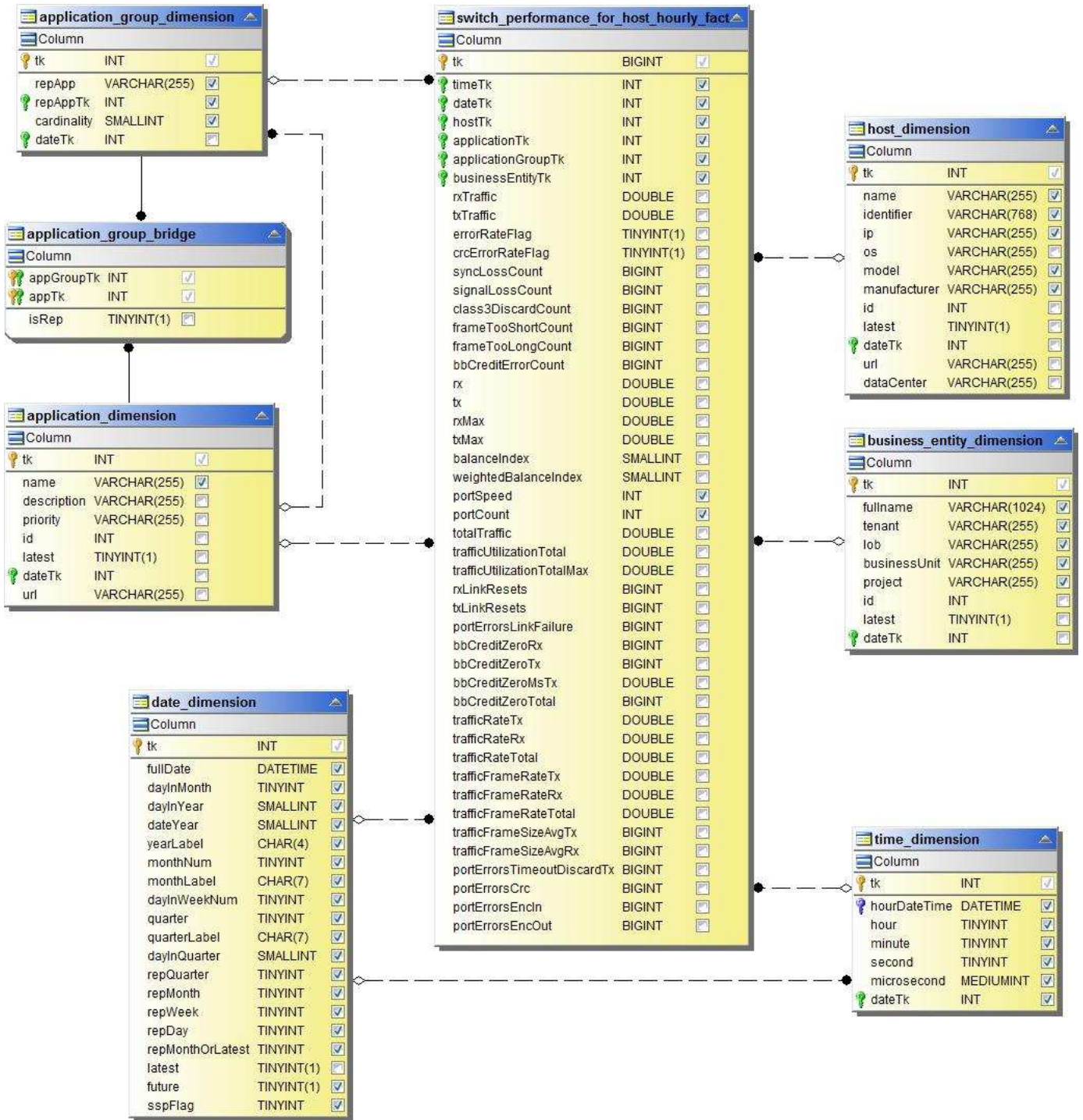


스토리지 노드 시간별 성능 향상

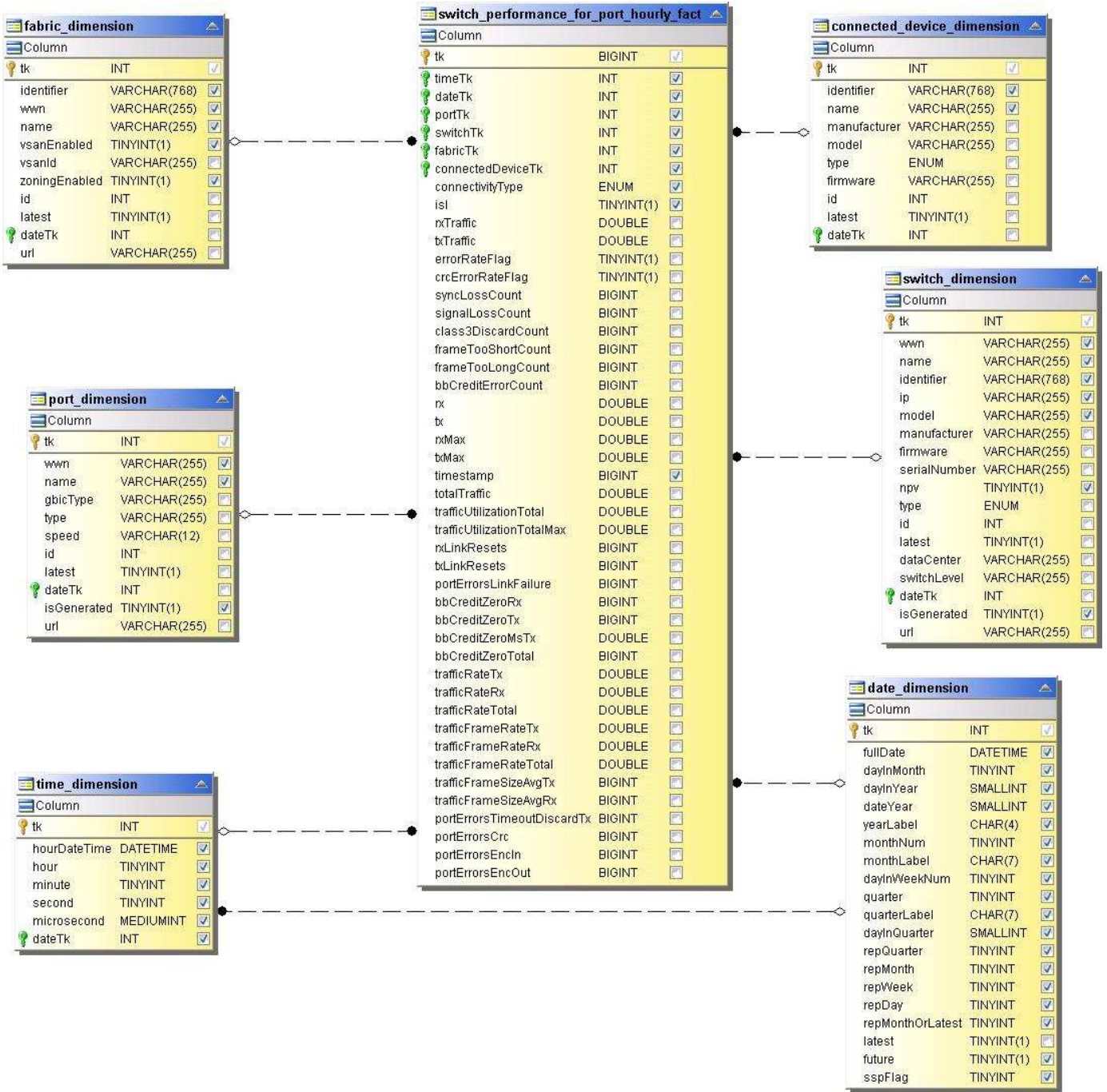


호스트에 대한 시간별 성능 전환



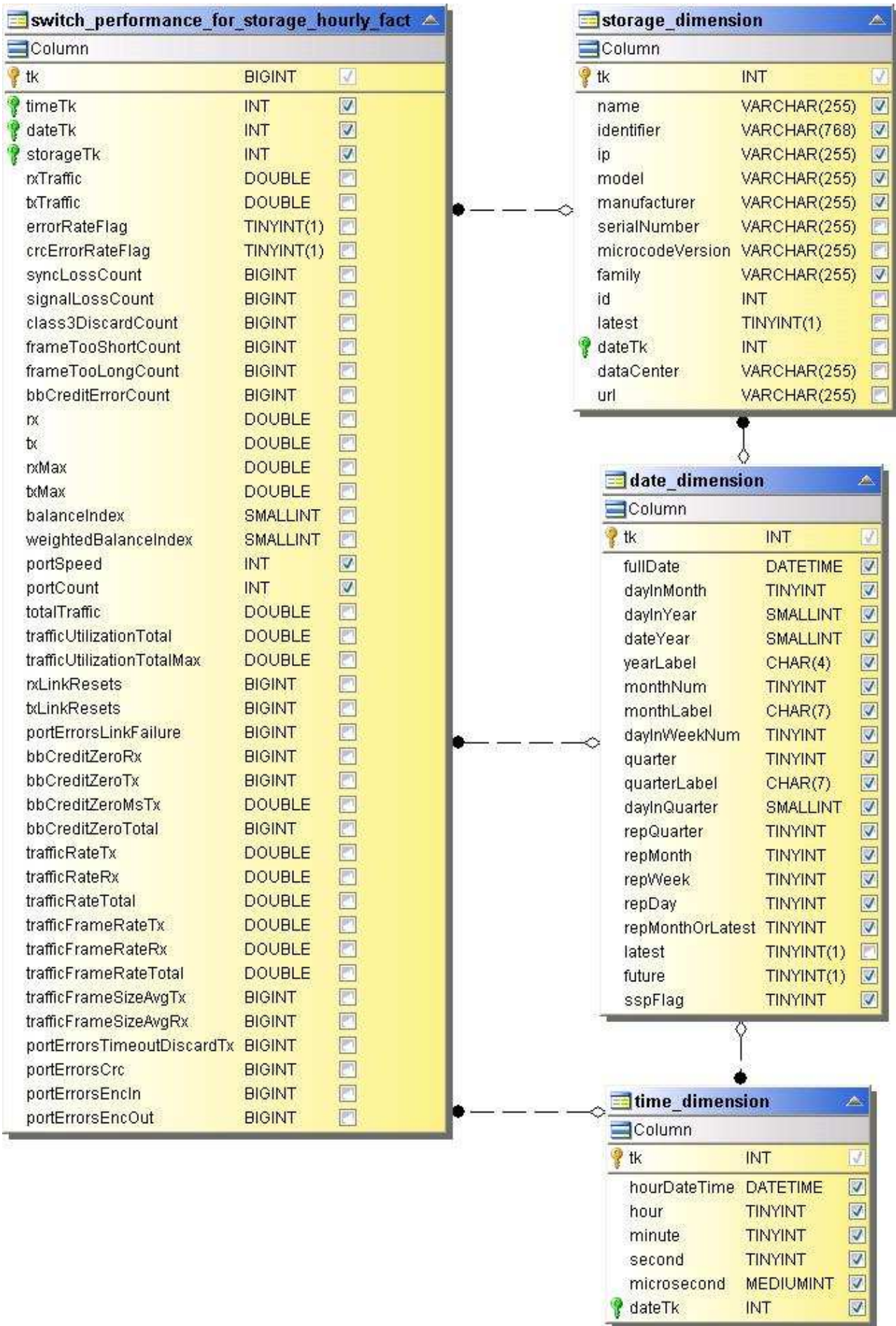


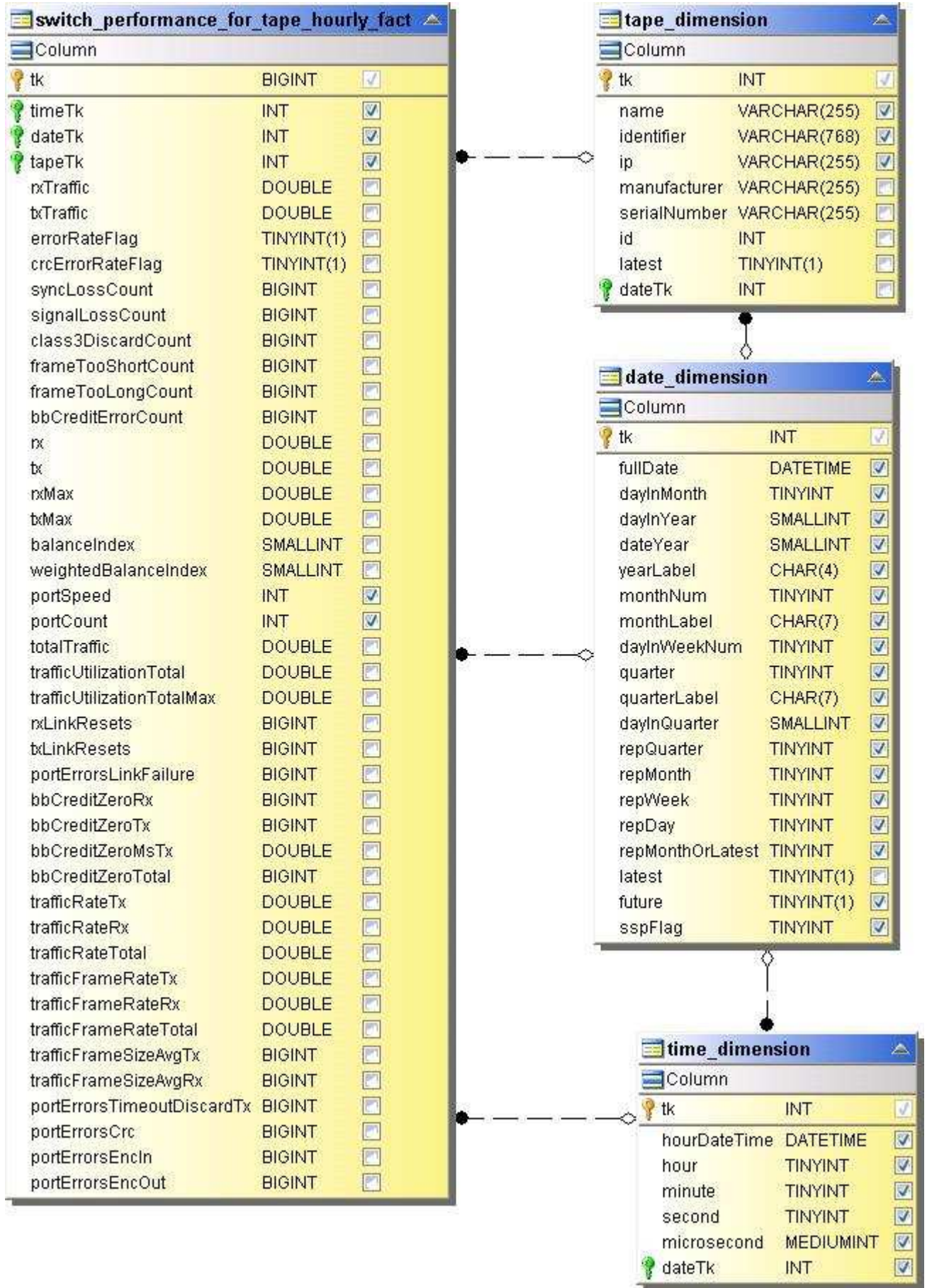
포트의 시간별 성능 전환



스토리지에 대한 시간별 성능 전환

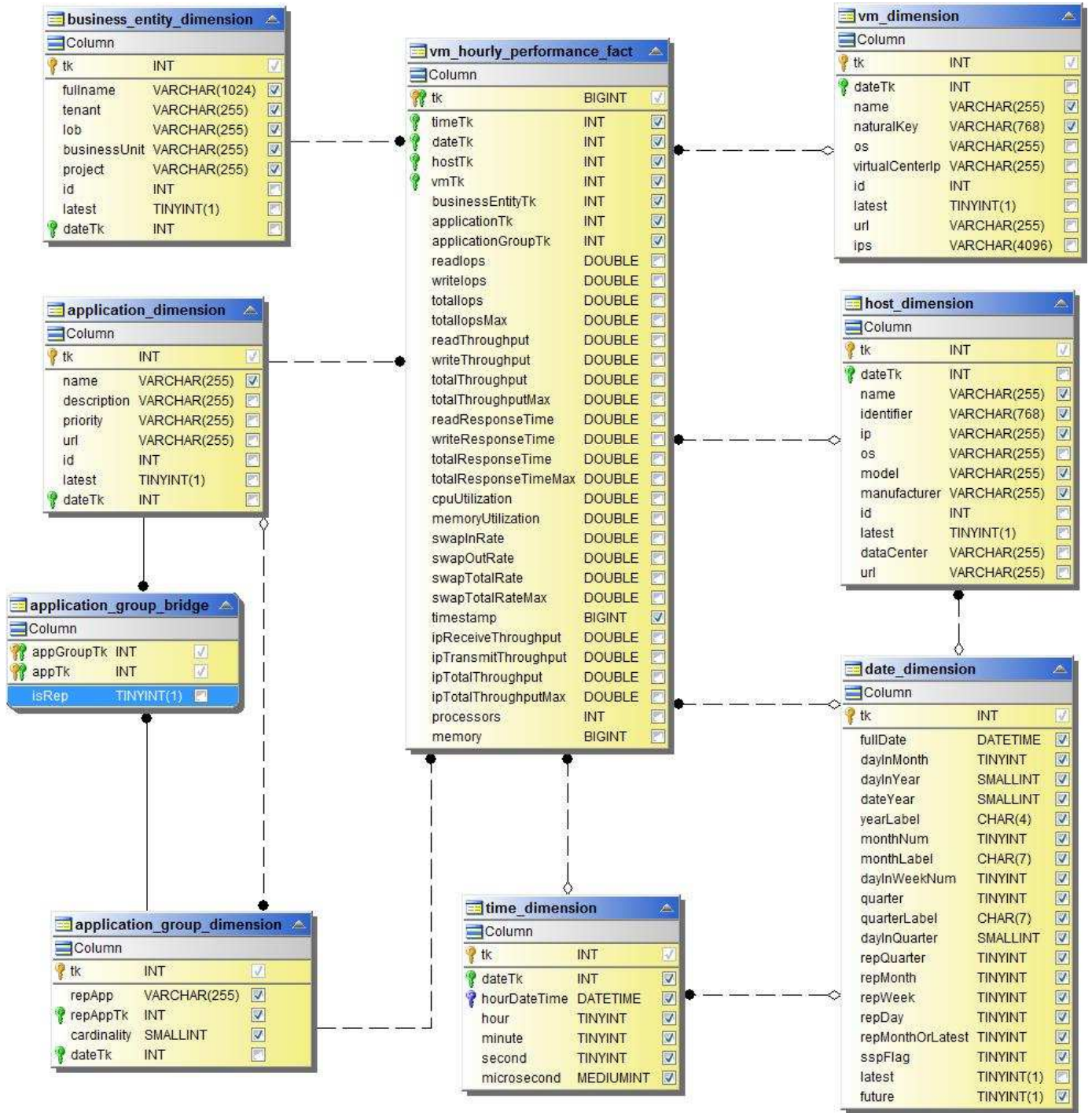




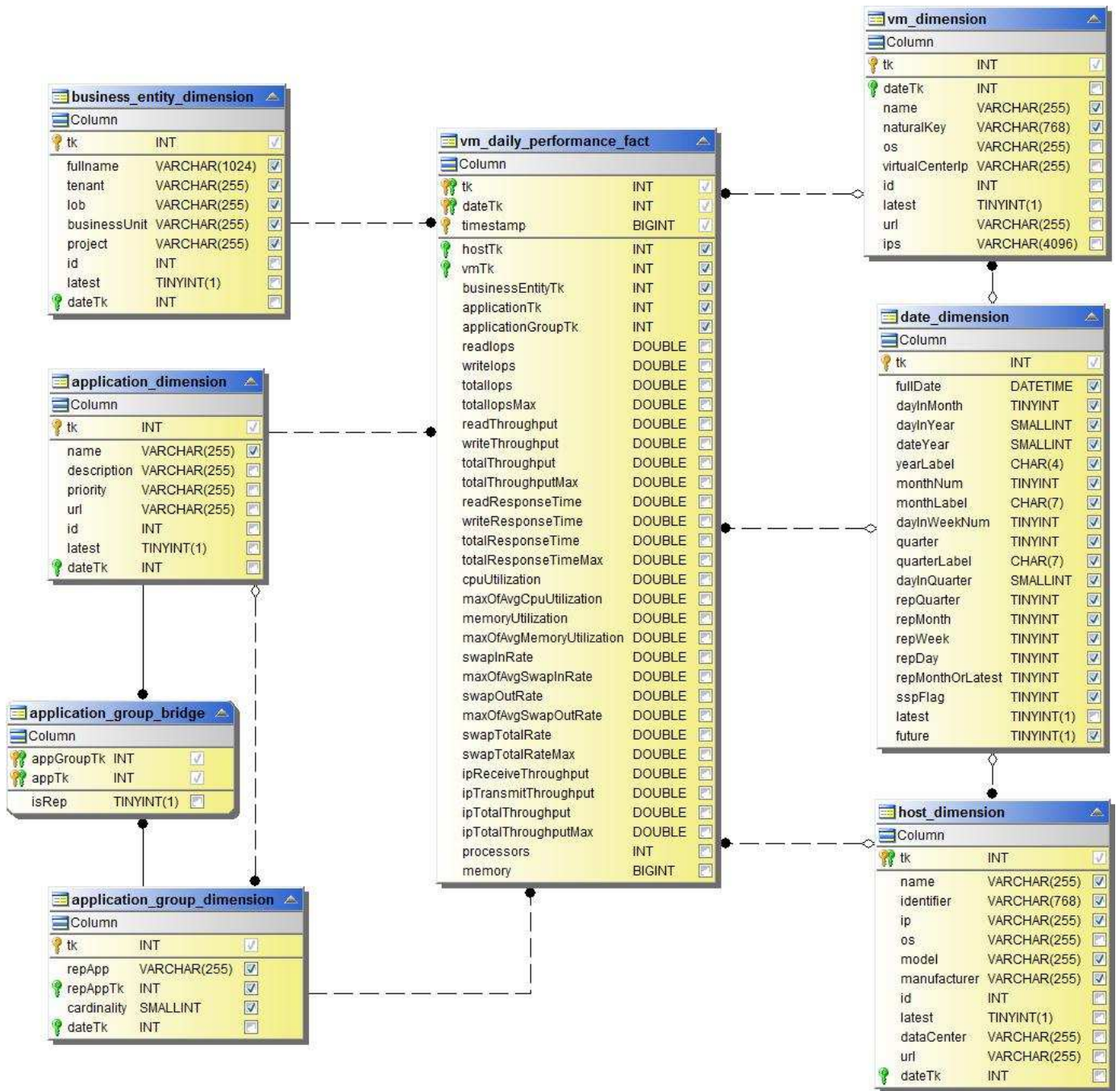




VM 성능

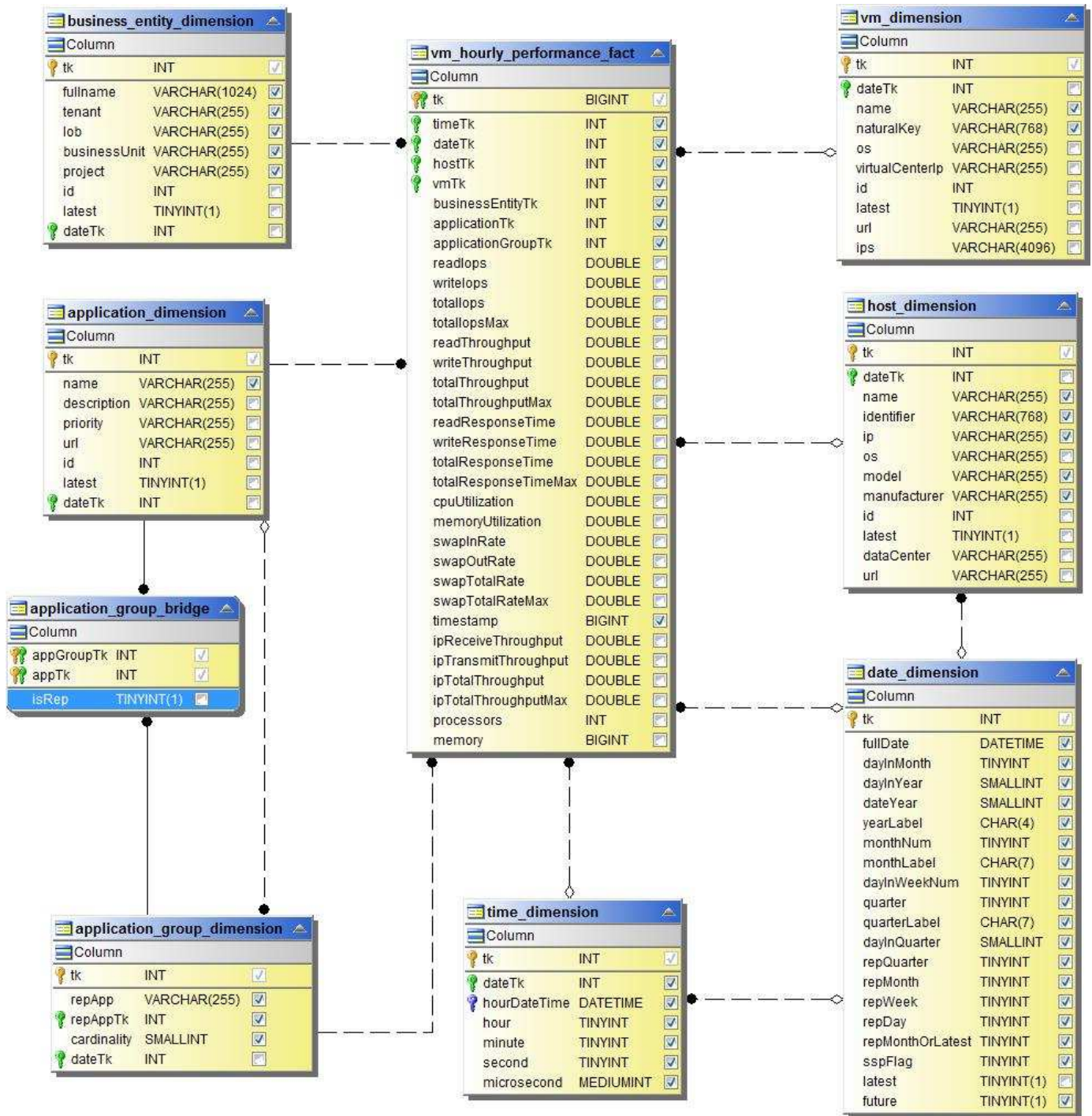


호스트의 VM 일일 성능

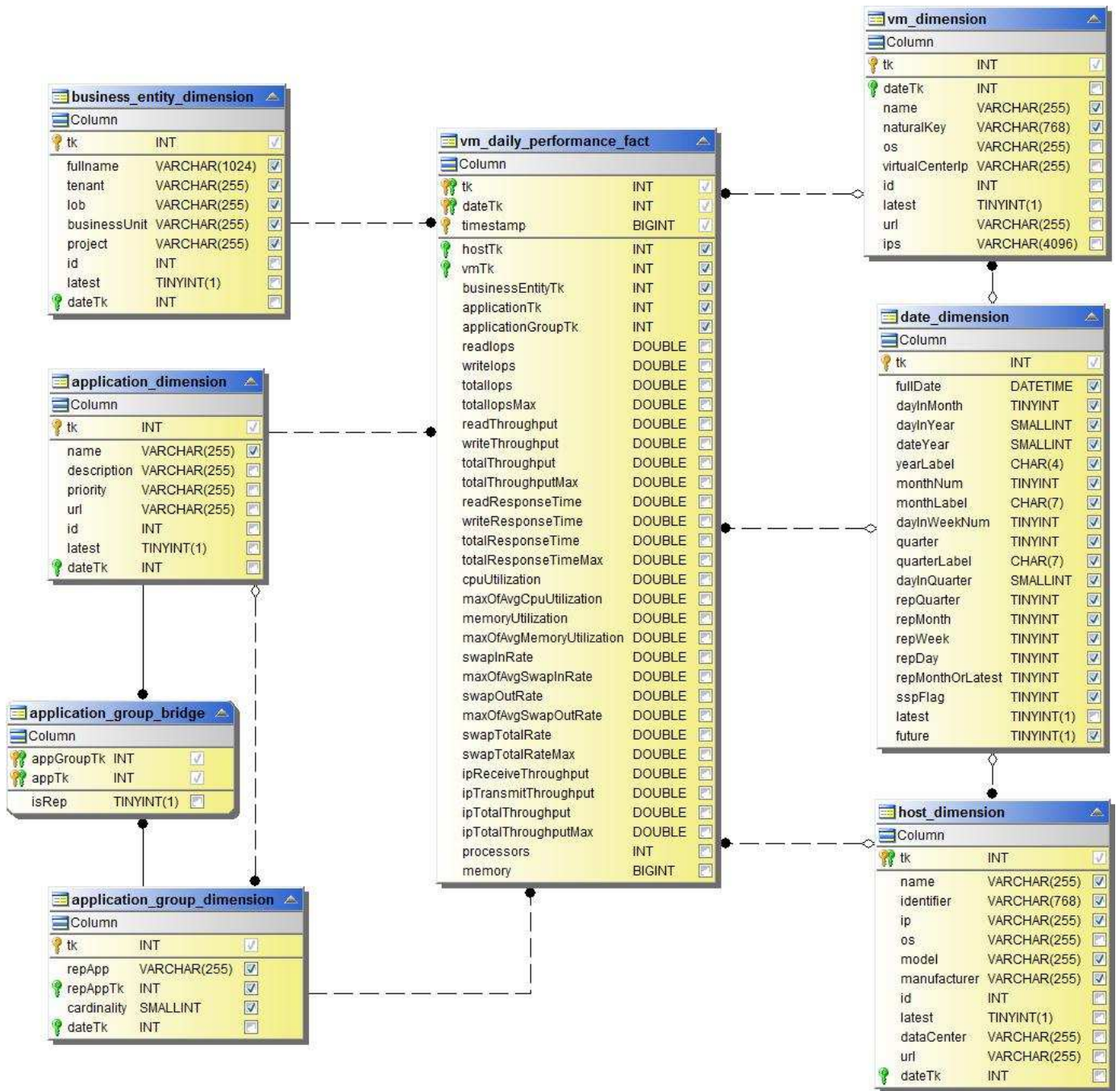


호스트에 대한 VM 시간별 성능



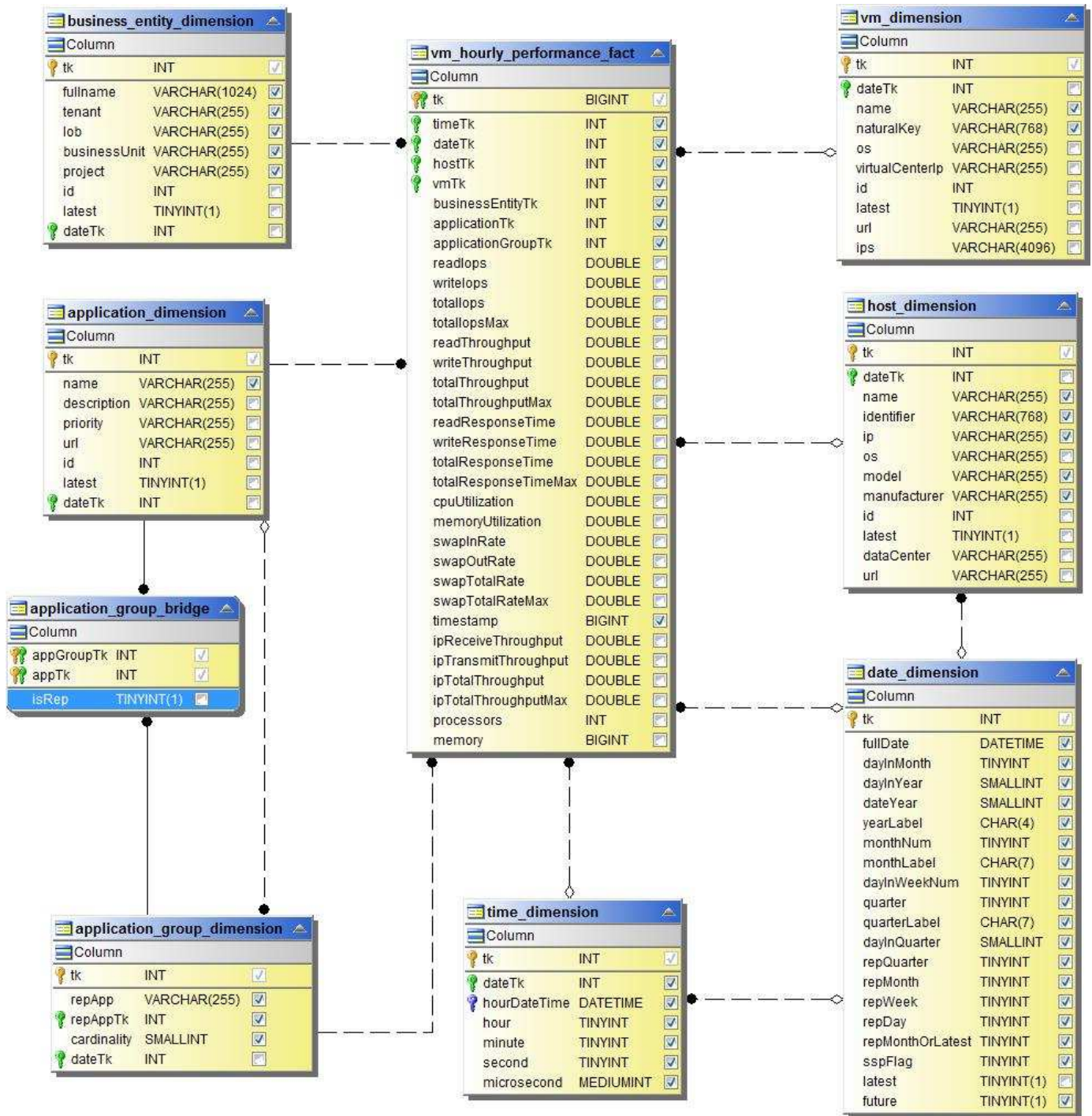


호스트의 VM 일일 성능

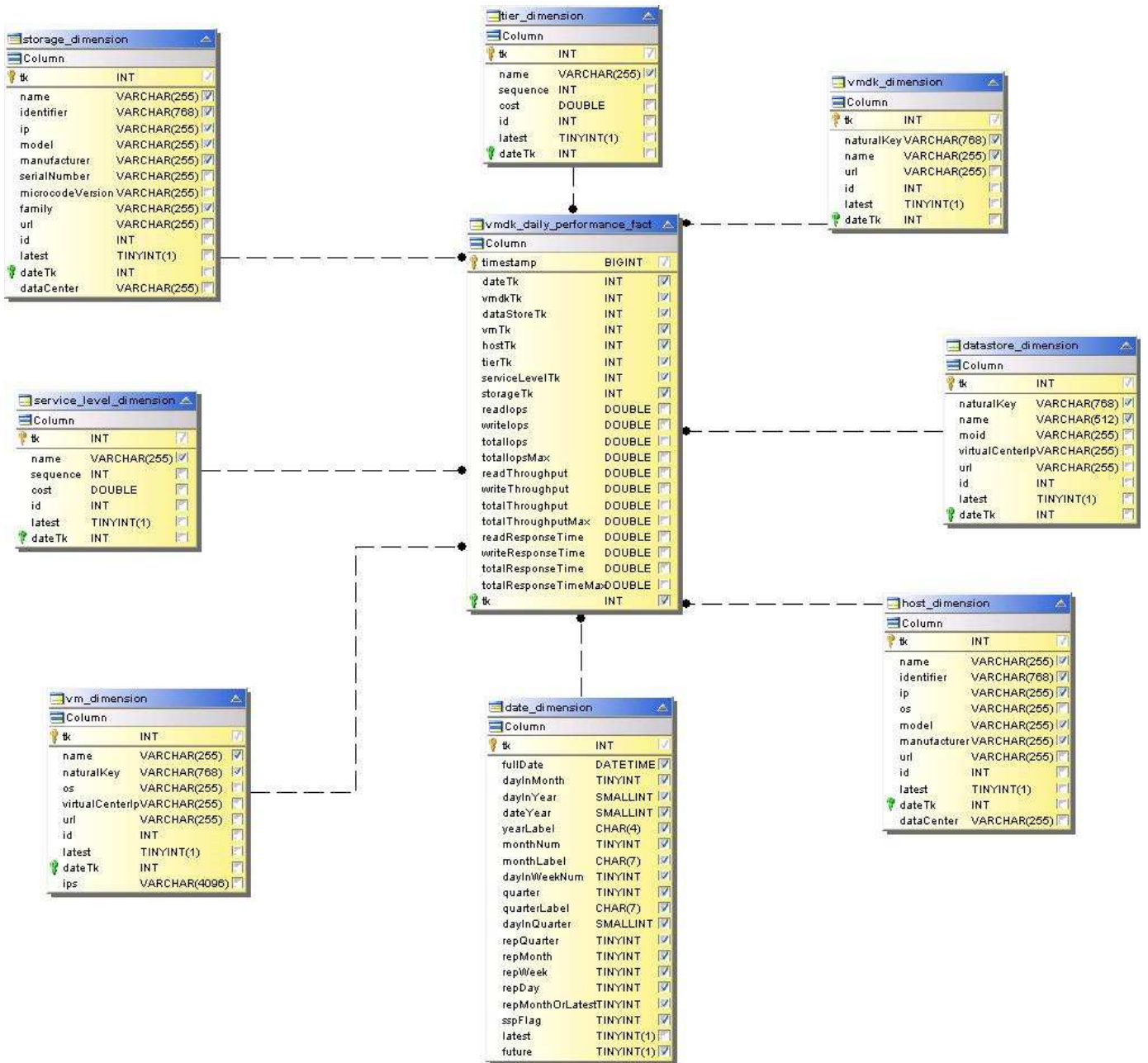


호스트에 대한 VM 시간별 성능

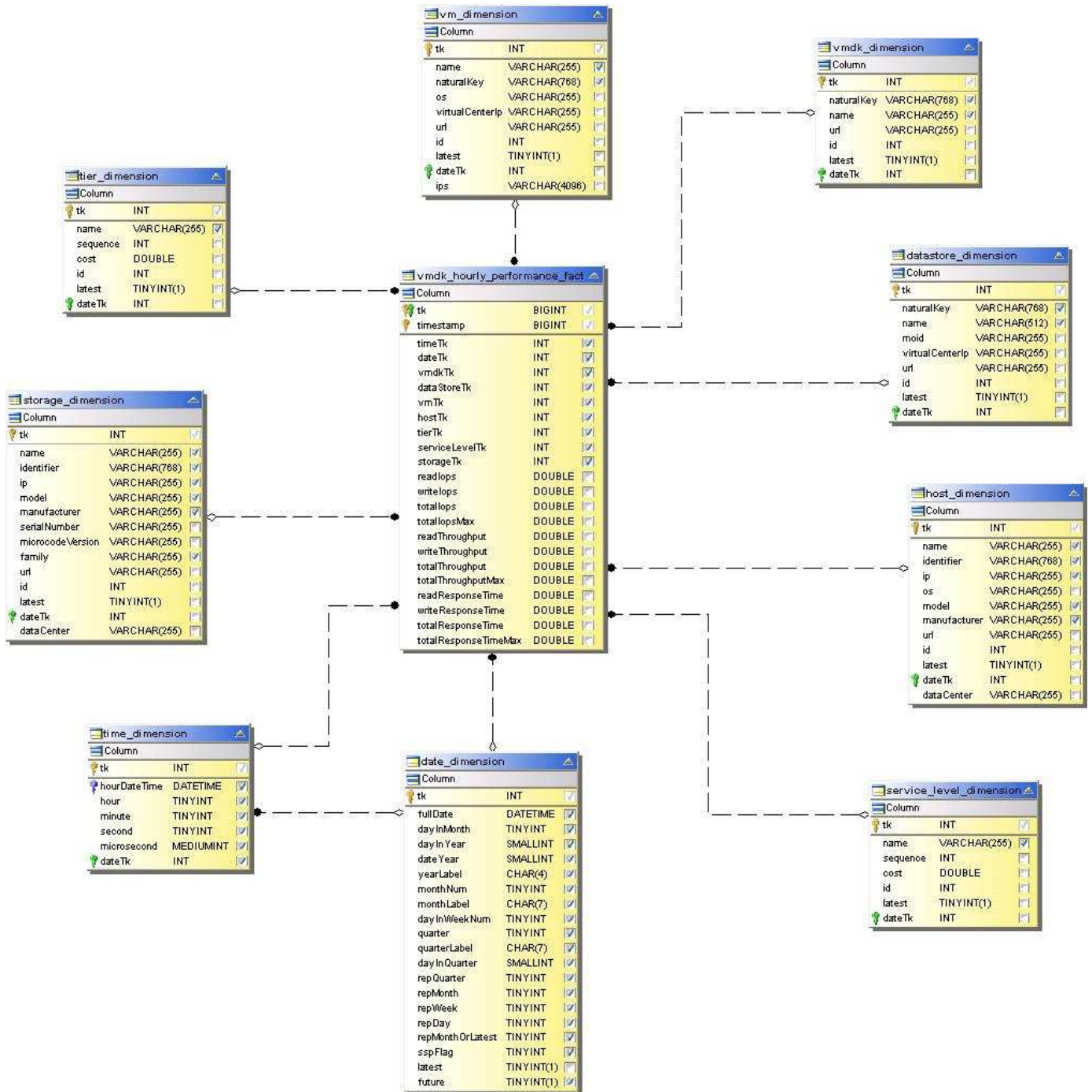




VMDK 일별 성능

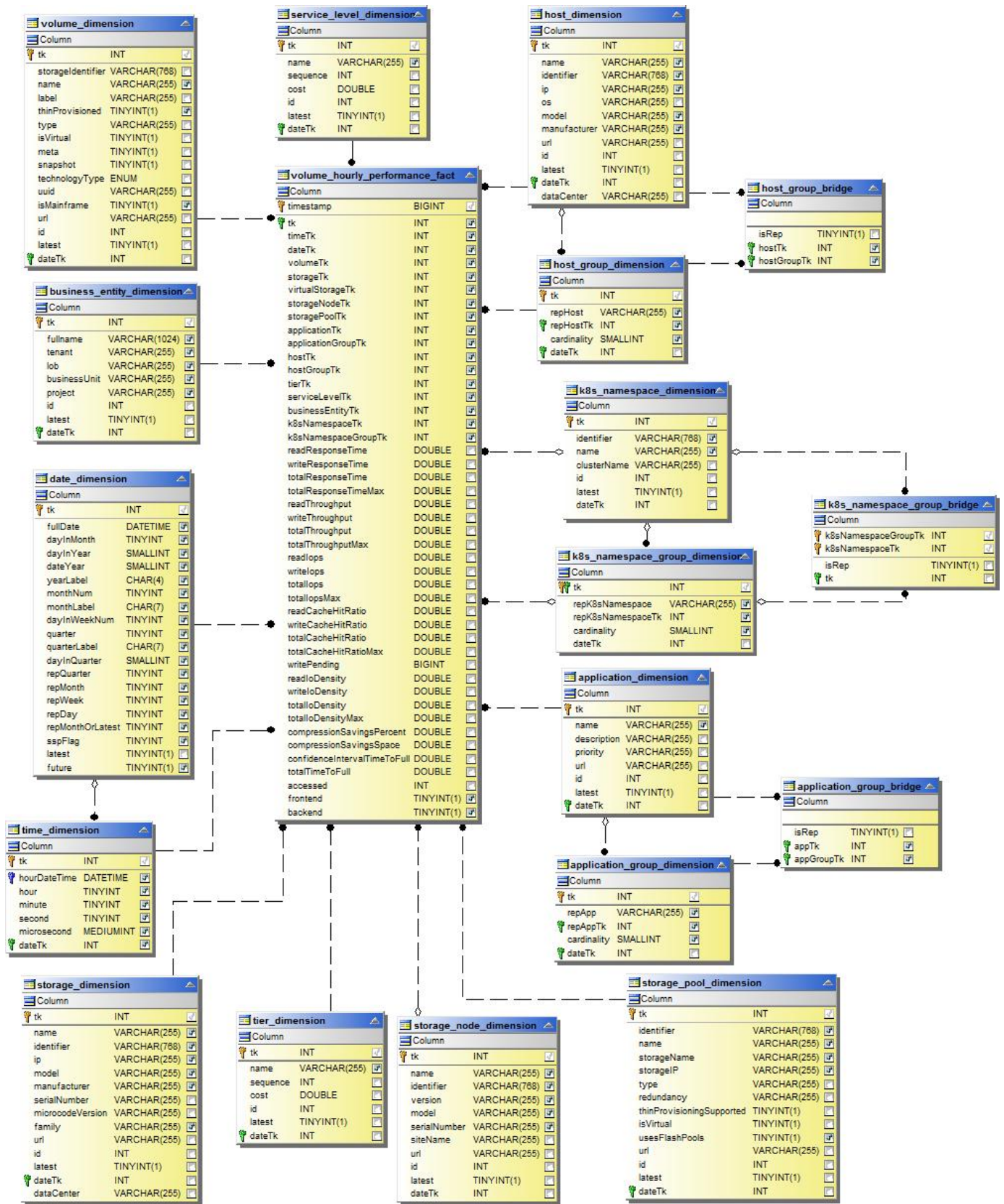


## VMDK의 시간별 성능

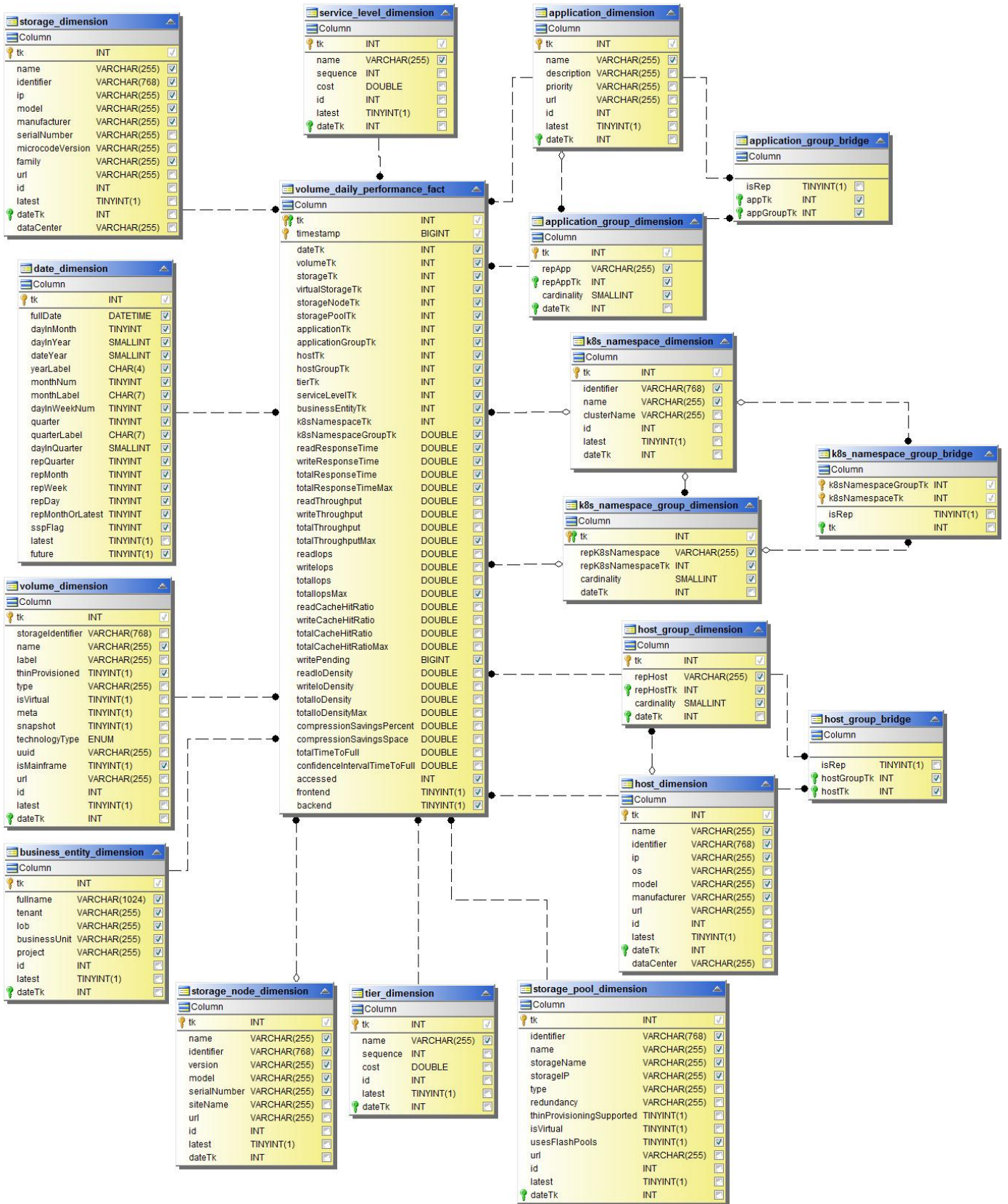


볼륨 시간별 성능





볼륨 일일 성능



## 데이터 인프라 인사이트 보고용 스키마

이 스키마 테이블 및 다이어그램은 Data Infrastructure Insights 보고에 대한 참조로 제공됩니다.

"\* 스키마 테이블 \*" PDF 형식. 링크를 클릭하여 열거나 마우스 오른쪽 단추를 클릭하고 \_다른 이름으로 저장...\_을 선택하여 다운로드합니다.

"\* 스키마 다이어그램 \*"



보고 기능은 Data Infrastructure Insights에서 사용할 수 ["Premium Edition을 참조하십시오"](#) 있습니다.



# 쿠버네티스

## Kubernetes 클러스터 개요

Data Infrastructure Insights Kubernetes Explorer는 Kubernetes 클러스터의 전체 상태 및 사용량을 보여주기 위한 강력한 툴이며 조사 영역을 쉽게 드릴다운할 수 있습니다.

대시보드 > Kubernetes Explorer \* 를 클릭하면 Kubernetes 클러스터 목록 페이지가 열립니다. 이 개요 페이지에는 사용자 환경의 Kubernetes 클러스터 테이블이 포함되어 있습니다.



Name ↑	Overall Saturation (%)	CPU Saturation (%)	Memory Saturation (%)	Storage Saturation (%)	Nodes	Pods	Namespaces	Workloads
self	56	25	56	31	2	63	18	68
setok3s	4	2	3	4	2	9	5	7

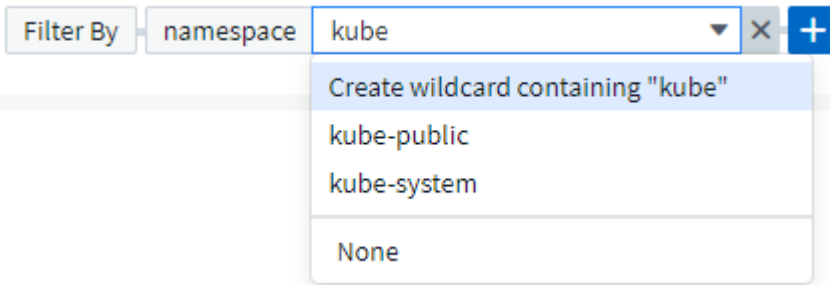
### 클러스터 목록

클러스터 목록에는 사용자 환경의 각 클러스터에 대한 다음 정보가 표시됩니다.

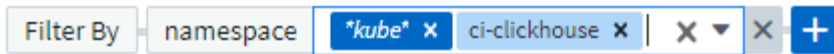
- 클러스터 \* 이름 . 클러스터 이름을 클릭하면 가 열립니다 " 상세 페이지 "\*" 클러스터에 대해.
- \* 채도 \* 백분율. 전체 채도란 CPU, 메모리 또는 저장소 채도가 가장 높은 것입니다.
- 클러스터의 \* 노드 수 \* 입니다. 이 번호를 클릭하면 노드 목록 페이지가 열립니다.
- 클러스터의 Pod 수 이 번호를 클릭하면 창 목록 페이지가 열립니다.
- 클러스터의 \* 네임스페이스 \* 수입니다. 이 번호를 클릭하면 네임스페이스 목록 페이지가 열립니다.
- 클러스터에 있는 \* 워크로드 \* 수. 이 번호를 클릭하면 워크로드 목록 페이지가 열립니다.

### 필터 다듬기

필터링을 할 때 입력을 시작하면 현재 텍스트를 기반으로 \* 와일드카드 필터 \* 를 만들 수 있는 옵션이 표시됩니다. 이 옵션을 선택하면 와일드카드 식과 일치하는 모든 결과가 반환됩니다. NOT 또는 And를 사용하여 \* 식 \* 을 만들거나 "없음" 옵션을 선택하여 필드의 null 값을 필터링할 수도 있습니다.



와일드카드 또는 식(예 NOT, 및, "없음" 등)은 필터 필드에 진한 파란색으로 표시됩니다. 목록에서 직접 선택한 항목은 연한 파란색으로 표시됩니다.



Kubernetes 필터는 상황에 따라 다릅니다. 예를 들어 특정 노드 페이지에 있는 경우 pod\_NAME 필터는 해당 노드에 관련된 Pod만 나열합니다. 또한 특정 네임스페이스에 대한 필터를 적용하는 경우 pod\_NAME 필터는 해당 네임스페이스에 있는 \_ 및 \_ 노드에 포드만 나열합니다.

와일드카드 및 식 필터링은 텍스트 또는 목록과 함께 사용할 수 있지만 수치, 날짜 또는 부울은 사용할 수 없습니다.

## NetApp Kubernetes 모니터링 운영자를 설치 또는 업그레이드하기 전에

를 설치 또는 업그레이드하기 전에 이 정보를 읽으십시오 ["Kubernetes 모니터링 운영자"](#).

구성 요소	요구 사항
Kubernetes 버전	Kubernetes v1.20 이상
Kubernetes 배포	AWS EKS(Elastic Kubernetes Service) Azure Kubernetes 서비스(AKS) Google Kubernetes Engine(GKE) Red Hat OpenShift RKE(Rancher Kubernetes Engine) VMware Tanzu입니다
리눅스 OS	Data Infrastructure Insights는 Arm64 아키텍처로 실행되는 노드를 지원하지 않습니다. 네트워크 모니터링: Linux 커널 버전 4.18.0 이상을 실행해야 합니다. Photon OS는 지원되지 않습니다.
라벨	Data Infrastructure Insights는 Kubernetes v1.20 이상 플랫폼에서 다음과 같은 Kubernetes 레이블을 찾는 Kubernetes 노드 선택기를 지정하여 Linux를 실행하는 Kubernetes 노드 모니터링을 지원합니다. Kubernetes.IO/OS=Linux Rancher+Cattle.IO as 오케스트레이션/Kubernetes 플랫폼: cool.IO/OS=Linux
명령	curl 및 kubectl 명령을 사용할 수 있어야 합니다. 최상의 결과를 얻으려면 이러한 명령을 경로에 추가하십시오.
연결성	kubettl CLI는 대상 K8s 클러스터와 통신하도록 구성되고 Data Infrastructure Insights 환경에 인터넷에 연결되어 있습니다. 설치하는 동안 프록시 뒤에 있는 경우 작업자 설치 섹션의 지침을 <a href="#">"프록시 지원을 구성하는 중입니다"</a> <a href="#">"따르십시오"</a> . 정확한 감사 및 데이터 보고를 위해 NTP(Network Time Protocol) 또는 SNTP(Simple Network Time Protocol)를 사용하여 Agent 시스템의 시간을 동기화합니다.
기타	OpenShift 4.6 이상에서 실행 중인 경우 를 따라야 합니다 <a href="#">"OpenShift 지침"</a> 이러한 사전 요구 사항이 충족되었는지 확인하는 것 외에도



구성 요소	요구 사항
API 토큰	Operator를 다시 배포하는 경우(예: 업데이트 또는 교체) 새 API 토큰을 생성할 필요가 없습니다. 이전 토큰을 다시 사용할 수 있습니다.

## 시작하기 전에 유의해야 할 중요 사항

을(를) 사용하여 실행 중인 경우 [프록시](#), 가 있습니다 [사용자 지정 리포지토리](#) 또는 을(를) 사용하고 있습니다 [OpenShift](#) 다음 섹션을 주의 깊게 읽으십시오.

에 대해서도 읽어 보세요 [권한](#).

프록시 지원을 구성하는 중입니다

NetApp Kubernetes Monitoring Operator를 설치하기 위해 사용자 환경에서 프록시를 사용할 수 있는 두 가지 위치가 있습니다. 이러한 시스템은 동일하거나 별도의 프록시 시스템일 수 있습니다.

- 설치 코드 스니펫을 실행하는 동안("curl" 사용) 프록시를 사용하여 스니펫이 실행되는 시스템을 Data Infrastructure Insights 환경에 연결해야 합니다
- Data Infrastructure Insights 환경과 통신하는 데 필요한 프록시입니다

둘 중 하나 또는 둘 모두에 프록시를 사용하는 경우 NetApp Kubernetes 운영 모니터를 설치하려면 먼저 프록시가 데이터 인프라 인사이트 환경과 제대로 통신할 수 있도록 구성되었는지 확인해야 합니다. 예를 들어, 운영자를 설치할 서버/VM에서 Data Infrastructure Insights에 액세스하고 Data Infrastructure Insights에서 바이너리를 다운로드할 수 있어야 합니다.

NetApp Kubernetes 운영 모니터를 설치하는 데 사용되는 프록시에 대해 Operator를 설치하기 전에 `_http_proxy/https_proxy_environment` 변수를 설정하십시오. 일부 프록시 환경에서는 `_no_proxy` 환경\_변수를 설정해야 할 수도 있습니다.

변수를 설정하려면 \* NetApp Kubernetes Monitoring Operator를 설치하기 전에 \* 시스템에서 다음 단계를 수행하십시오.

1. 현재 사용자에게 대한 `_https_proxy_and/or_http_proxy_environment` 변수를 설정합니다.
  - a. 설정 중인 프록시에 인증(사용자 이름/암호)이 없으면 다음 명령을 실행합니다.

```
export https_proxy=<proxy_server>:<proxy_port>
.. 설정 중인 프록시에 인증 (사용자 이름/암호) 이 있는 경우 다음 명령을 실행합니다.
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Kubernetes 클러스터가 데이터 인프라 인사이트 환경과 통신하는 데 사용되는 프록시의 경우, 이 지침을 모두 읽은 후 NetApp Kubernetes 모니터링 운영자를 설치합니다.

NetApp Kubernetes Monitoring Operator를 구축하기 전에 operator-config.yaml에서 AgentConfiguration의 프록시 섹션을 구성하십시오.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
  ...
```

### 사용자 지정 또는 프라이빗 **Docker** 저장소 사용

기본적으로 NetApp Kubernetes 모니터링 운영자는 Data Infrastructure Insights 저장소에서 컨테이너 이미지를 가져옵니다. 모니터링을 위한 타겟으로 사용되는 Kubernetes 클러스터가 있고 해당 클러스터가 사용자 지정 또는 프라이빗 Docker 저장소 또는 컨테이너 레지스트리에서만 컨테이너 이미지를 풀도록 구성된 경우 NetApp Kubernetes Monitoring Operator가 필요로 하는 컨테이너에 대한 액세스를 구성해야 합니다.

NetApp 모니터링 오퍼레이터 설치 타일에서 "이미지 풀 스니펫"을 실행합니다. 이 명령은 Data Infrastructure Insights 저장소에 로그인하고 운영자의 모든 이미지 종속성을 가져온 다음 Data Infrastructure Insights 저장소에서 로그아웃합니다. 메시지가 표시되면 제공된 리포지토리 임시 암호를 입력합니다. 이 명령은 옵션 기능을 포함하여 오퍼레이터가 사용하는 모든 이미지를 다운로드합니다. 이러한 이미지가 사용되는 기능은 아래를 참조하십시오.

### 핵심 운영자 기능 및 Kubernetes 모니터링

- NetApp - 모니터링
- kubbe-RBAC-proxy입니다
- Kudbe-state-metrics를 나타냅니다
- 텔레그라프
- distroless-root-user.(거리 없는 루트 사용자)

### 이벤트 로그

- 유창한 비트
- Kubernetes - 이벤트 - 수출자

## 네트워크 성능 및 맵

- CI-NET-관찰자

회사 정책에 따라 운영 Docker 이미지를 프라이빗/로컬/엔터프라이즈 Docker 저장소로 밀어 넣습니다. 리포지토리에 있는 이러한 이미지에 대한 이미지 태그와 디렉터리 경로가 Data Infrastructure Insights 리포지토리에 있는 이미지와 일치하는지 확인합니다.

운영자 배포에서 모니터링 - 운영자 배포를 편집합니다. YAML을 편집하고 모든 이미지 참조를 수정하여 개인 Docker 저장소를 사용하십시오.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

operator-config.yaml에서 AgentConfiguration을 편집하여 새로운 Docker 저장소 위치를 반영하십시오. 개인 리포지토리에 대한 새 imagePullSecret을 만듭니다. 자세한 내용은 <https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/> 참조하십시오

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
  from as compared to CI's docker registry
  # Please see documentation for
  xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
  private-docker-repository[using a custom or private docker repository].
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
  private docker registry
  dockerImagePullSecret: docker-secret-name
```

## OpenShift 지침

OpenShift 4.6 이상에서 실행 중인 경우 \_operator-config.yaml\_에서 AgentConfiguration을 편집하여 \_Privileged\_setting\_을 활성화해야 합니다.

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift는 일부 Kubernetes 구성 요소에 대한 액세스를 차단할 수 있는 수준 높은 보안을 구현할 수 있습니다.

## 권한

모니터링 중인 클러스터에 ClusterRole이 없는 사용자 지정 리소스가 포함되어 있는 경우 "보려는 애그리게이트", 이벤트 로그로 이러한 리소스를 모니터링하려면 운영자에게 수동으로 이러한 리소스에 대한 액세스 권한을 부여해야 합니다.

1. edit\_operator-additional-permissions.yaml\_를 설치하기 전이나 설치 후 resource\_ClusterRole/<namespace>-additional-permissions\_를 편집합니다
2. 동사 ["get", "watch", "list"]를 사용하여 원하는 apiGroups 및 리소스에 대한 새 규칙을 만듭니다.  
<https://kubernetes.io/docs/reference/access-authn-authz/rbac/> 를 참조하십시오
3. 변경 사항을 클러스터에 적용합니다


## Kubernetes Monitoring Operator 설치 및 구성

Data Infrastructure Insights는 Kubernetes 컬렉션을 위한 \* Kubernetes Monitoring Operator \* 를 제공합니다. Kubernetes > Collectors > + Kubernetes Collector \* 로 이동하여 새 연산자를 구축합니다.

### Kubernetes Monitoring Operator를 설치하기 전에

를 참조하십시오 "필수 구성 요소" Kubernetes Monitoring Operator를 설치 또는 업그레이드하기 위한 문서화.

### Kubernetes 모니터링 운영자 설치

 **kubernetes**  
Kubernetes

## Deploy NetApp Monitoring Operator

Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.

Select existing API Access Token or create a new one

KEY2024 (...vw6NdM) + API Access Token Production Best Practices ?

### Installation Instructions Need Help?

Please review the [pre-requisites](#) for installing the NetApp Kubernetes Monitoring Operator. To update an existing operator installation please follow [these steps](#).

- 1 Define Kubernetes cluster name and namespace**  
Provide the Kubernetes cluster name and specify a namespace for deploying the monitoring components.  

Cluster	Namespace
<input type="text" value="clustername"/>	<input type="text" value="netapp-monitoring"/>
- 2 Download the operator YAML files**  
Execute the following download command in a *bash* prompt.  

*This snippet includes a unique access key that is valid for 24 hours.*

### 3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure. Finally, update the image paths in operator-deployment.yaml and the docker repository settings in operator-config.yaml. For more information review [the documentation](#).

Copy Image Pull Snippet

Reveal Image Pull Snippet

Copy Repository Password

Reveal Repository Password

*This password is valid for 24 hours.*

### 4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the [instructions and available options](#).

### 5 Deploy the operator (create new or upgrade existing)

Execute the `kubectl` snippet to apply the following operator YAML files.

- operator-setup.yaml - Create the operator's dependencies.
- operator-secrets.yaml - Create secrets holding your API key.
- operator-deployment.yaml, operator-cr.yaml - Deploy the NetApp Kubernetes Monitoring Operator.
- operator-config.yaml - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store operator-secrets.yaml**.

### 6 Next

Kubernetes에 **Kubernetes Monitoring Operator** 에이전트를 설치하는 단계:

1. 고유한 클러스터 이름 및 네임스페이스를 입력합니다. 있는 경우 **업그레이드 중** 이전 Kubernetes Operator에서 동일한 클러스터 이름과 네임스페이스를 사용합니다.
2. 이러한 내용을 입력하면 다운로드 명령 스크립트를 클립보드에 복사할 수 있습니다.
3. 스크립트를 `_bash_window`에 붙여 넣고 실행합니다. 오퍼레이터 설치 파일이 다운로드됩니다. 스크립트에는 고유한 키가 있으며 24시간 동안 유효합니다.
4. 사용자 지정 또는 개인 리포지토리가 있는 경우 선택적 이미지 풀 스크립트를 복사하여 `_bash_shell`에 붙여 넣고 실행합니다. 이미지를 가져온 후 개인 저장소에 복사합니다. 동일한 태그 및 폴더 구조를 유지해야 합니다. `operator-deployment.YAML_`의 경로와 `_operator-config.YAML_`의 Docker 리포지토리 설정을 업데이트합니다.
5. 필요한 경우 프록시 또는 개인 리포지토리 설정과 같은 사용 가능한 구성 옵션을 검토합니다. 에 대해 자세히 알아볼 수 있습니다 "[구성 옵션](#)".
6. 준비가 되면 `kubeck Apply` 스크립트를 복사하고 다운로드한 다음 실행하여 Operator 를 배포합니다.
7. 설치가 자동으로 진행됩니다. 완료되면 `Next` 단추를 클릭합니다.
8. 설치가 완료되면 `Next` 단추를 클릭합니다. 또한 `_operator-비밀.YAML_` 파일을 삭제하거나 안전하게 보관하십시오.

프록시를 사용하는 경우 정보를 읽습니다 [프록시를 구성하는 중입니다](#).

사용자 지정 리포지토리가 있는 경우 정보를 읽습니다 [사용자 지정/프라이빗 Docker 저장소 사용](#).

## Kubernetes 모니터링 구성 요소

Data Infrastructure Insights Kubernetes Monitoring은 네 가지 모니터링 구성 요소로 이루어져 있습니다.


- 클러스터 메트릭입니다
- 네트워크 성능 및 맵(옵션)
- 이벤트 로그(선택 사항)
- 변경 분석(옵션)

위의 옵션 구성 요소는 각 Kubernetes Collector에 대해 기본적으로 활성화되어 있습니다. 특정 수집기에 구성 요소가 필요하지 않다고 결정한 경우 \* Kubernetes > Collectors \* 로 이동한 후 화면 오른쪽의 수집기의 "세 가지 점" 메뉴에서 \_Modify Deployment\_를 선택하여 비활성화할 수 있습니다.

NetApp / Observability / Collectors

Cluster Name ↑	Status	Operator Version	Network Performance and Map	Change Analysis	
au-pod	⚠ Outdated	1.1540.0	1.347.0	1.162.0	⋮
jks-troublemaker	Latest	1.1579.0	N/A	1.201.0	⋮
oom-test	⚠ Outdated	1.1555.0	N/A	1.101.0	⋮ Modify Deployment

화면에는 각 구성 요소의 현재 상태가 표시되며 필요한 경우 해당 Collector에 대한 구성 요소를 비활성화하거나 활성화할 수 있습니다.

 **kubernetes**  
Kubernetes

### Modify Deployment

#### Cluster Information

Kubernetes Cluster  
ci-demo-01

Network Performance and Map  
Enabled - Online

Event Logs  
Enabled - Online

Change Analysis  
Enabled - Online

#### Deployment Options

[Need Help?](#)

- Network Performance and Map
- Event Logs
- Change Analysis

Cancel

Complete Modification

업그레이드 중

최신 **Kubernetes Monitoring Operator**로 업그레이드하십시오

기존 운영자와 함께 AgentConfiguration이 존재하는지 확인합니다(네임스페이스가 DEFAULT\_NetApp-MONITORING\_이 아닌 경우 해당 네임스페이스를 대체합니다).

```
kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-configuration
```

AgentConfiguration이 있는 경우:

- **설치합니다** 기존 오퍼레이터에 대한 최신 운영자.
  - 항상 확인하십시오 **최신 컨테이너 이미지를 가져오는 중입니다** 사용자 지정 리포지토리를 사용하는 경우

AgentConfiguration이 없는 경우:

- 데이터 인프라 인사이트 에서 인식된 클러스터 이름을 기록합니다(네임스페이스가 기본 NetApp-monitoring이 아닌 경우 해당 네임스페이스를 대체).

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

\* 기존 운영자의 백업을 생성합니다 (네임스페이스가 기본 NetApp 모니터링이 아닌 경우 적절한 네임스페이스를 대체) .

```
kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
```

\* <<to-remove-the-kubernetes-monitoring-operator, 설치 제거>> 기존 연산자.  
\* <<installing-the-kubernetes-monitoring-operator, 설치합니다>> 최신 운영자.

- 동일한 클러스터 이름을 사용합니다.
- 최신 운영자 YAML 파일을 다운로드한 후 배포하기 전에 agent\_backup.YAML에서 발견된 모든 사용자 정의를 다운로드한 operator-config.YAML에 이식하십시오.
- 항상 확인하십시오 **최신 컨테이너 이미지를 가져오는 중입니다** 사용자 지정 리포지토리를 사용하는 경우

## Kubernetes 모니터링 오퍼레이터 중지 및 시작

Kubernetes 모니터링 운영자를 중지하려면 다음을 따르십시오.

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=0
```

Kubernetes 모니터링 운영자를 시작하려면 다음을 따르십시오.

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

## 제거 중

### Kubernetes Monitoring Operator를 제거합니다

Kubernetes Monitoring Operator의 기본 네임스페이스는 "netapp-monitoring"입니다. 고유한 네임스페이스를 설정한 경우 이러한 네임스페이스 및 모든 후속 명령 및 파일로 대체합니다.

다음 명령을 사용하여 모니터링 연산자의 최신 버전을 제거할 수 있습니다.

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

모니터링 운영자가 자체 전용 네임스페이스에 배포된 경우 네임스페이스를 삭제합니다.

```
kubectl delete ns <NAMESPACE>
```

첫 번째 명령이 "리소스를 찾을 수 없음"을 반환하면 다음 지침에 따라 모니터링 연산자의 이전 버전을 제거합니다.

다음 명령을 순서대로 실행합니다. 현재 설치에 따라 이러한 명령 중 일부는 '개체를 찾을 수 없음' 메시지를 반환할 수 있습니다. 이러한 메시지는 무시해도 됩니다.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

보안 컨텍스트 제약 조건이 이전에 생성된 경우:

```
kubectl delete scc telegraf-hostaccess
```

### Kube-state-metrics 정보

NetApp Kubernetes Monitoring Operator는 다른 인스턴스와 충돌을 피하기 위해 고유한 kube-state-metrics를



설치합니다.

Kube-State-Metrics에 대한 자세한 내용은 [를 참조하십시오 "이 페이지"](#).

## 오퍼레이터 구성/사용자 지정

이 섹션에서는 운영자 구성을 사용자 지정하거나, 프록시를 사용하거나, 사용자 지정 또는 개인 Docker 리포지토리를 사용하거나, OpenShift를 사용하는 방법에 대한 정보를 제공합니다.

### 설정 옵션

가장 일반적으로 수정된 설정은 `_AgentConfiguration_custom` 리소스에서 구성할 수 있습니다. 운영자를 배포하기 전에 `_operator-config.YAML_file`을 편집하여 이 리소스를 편집할 수 있습니다. 이 파일에는 주석 처리된 설정 예가 포함되어 있습니다. 의 목록을 참조하십시오 ["사용 가능한 설정"](#) 를 참조하십시오.

다음 명령을 사용하여 연산자를 배포한 후에 이 리소스를 편집할 수도 있습니다.

```
kubectl -n netapp-monitoring edit AgentConfiguration
```

배포된 버전의 운영자가 AgentConfiguration을 지원하는지 확인하려면 다음 명령을 실행합니다.

```
kubectl get crd agentconfigurations.monitoring.netapp.com
```

"서버에서 오류 발생 (NotFound)" 메시지가 표시되는 경우 AgentConfiguration을 사용하려면 먼저 연산자를 업그레이드해야 합니다.

### 프록시 지원을 구성하는 중입니다

Kubernetes Monitoring Operator를 설치하기 위해 사용자 환경에서 프록시를 사용할 수 있는 위치는 두 곳입니다. 이러한 시스템은 동일하거나 별도의 프록시 시스템일 수 있습니다.

- 설치 코드 스니펫을 실행하는 동안("curl" 사용) 프록시를 사용하여 스니펫이 실행되는 시스템을 Data Infrastructure Insights 환경에 연결해야 합니다
- Data Infrastructure Insights 환경과 통신하는 데 필요한 프록시입니다

이 중 하나 또는 둘 모두에 프록시를 사용하는 경우 Kubernetes 운영 모니터를 설치하려면 먼저 프록시가 Data Infrastructure Insights 환경과 통신할 수 있도록 구성되었는지 확인해야 합니다. 프록시가 있고 운영자를 설치하려는 서버/VM에서 Data Infrastructure Insights에 액세스할 수 있는 경우 프록시가 제대로 구성된 것일 수 있습니다.

Kubernetes 운영 모니터를 설치하는 데 사용되는 프록시의 경우 Operator를 설치하기 전에 `_http_proxy/https_proxy_environment` 변수를 설정합니다. 일부 프록시 환경에서는 `_no_proxy` 환경\_변수를 설정해야 할 수도 있습니다.

변수를 설정하려면 Kubernetes Monitoring Operator를 설치하기 \* 전에 \* 시스템에서 다음 단계를 수행하십시오.

1. 현재 사용자에게 대한 `_https_proxy_and/or_http_proxy_environment` 변수를 설정합니다.
  - a. 설정 중인 프록시에 인증(사용자 이름/암호)이 없으면 다음 명령을 실행합니다.

```
export https_proxy=<proxy_server>:<proxy_port>
.. 설정 중인 프록시에 인증 (사용자 이름/암호)이 있는 경우 다음 명령을 실행합니다.
```

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Kubernetes 클러스터가 Data Infrastructure Insights 환경과 통신하는 데 사용되는 프록시의 경우 이 모든 지침을 읽은 후 Kubernetes Monitoring Operator를 설치합니다.

Kubernetes 모니터링 연산자를 배포하기 전에 operator-config.yaml에서 AgentConfiguration의 프록시 섹션을 구성합니다.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
    Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
  ...
```

### 사용자 지정 또는 프라이빗 Docker 저장소 사용

기본적으로 Kubernetes Monitoring Operator는 Data Infrastructure Insights 저장소에서 컨테이너 이미지를 가져옵니다. Kubernetes 클러스터를 모니터링 대상으로 사용하고 있고 해당 클러스터가 사용자 지정 또는 프라이빗 Docker 저장소 또는 컨테이너 레지스트리에서 컨테이너 이미지만을 가져오도록 구성된 경우, Kubernetes Monitoring Operator가 필요한 컨테이너에 대한 액세스를 구성해야 합니다.

NetApp 모니터링 오퍼레이터 설치 타일에서 "이미지 풀 스니펫"을 실행합니다. 이 명령은 Data Infrastructure Insights 저장소에 로그인하고 운영자의 모든 이미지 종속성을 가져온 다음 Data Infrastructure Insights 저장소에서 로그아웃합니다. 메시지가 표시되면 제공된 리포지토리 임시 암호를 입력합니다. 이 명령은 옵션 기능을 포함하여

오퍼레이터가 사용하는 모든 이미지를 다운로드합니다. 이러한 이미지가 사용되는 기능은 아래를 참조하십시오.

#### 핵심 운영자 기능 및 Kubernetes 모니터링

- NetApp - 모니터링
- ci-kube-RBAC-프록시
- CI - KSM을 참조하십시오
- CI - 텔레그래프
- distroless-root-user.(거리 없는 루트 사용자)

#### 이벤트 로그

- CI 플루언트 비트
- ci-kubernetes-event-exporter를 의미합니다

#### 네트워크 성능 및 맵

- CI-NET-관찰자

회사 정책에 따라 운영 Docker 이미지를 프라이빗/로컬/엔터프라이즈 Docker 저장소로 밀어 넣습니다. 리포지토리에 있는 이러한 이미지에 대한 이미지 태그와 디렉터리 경로가 Data Infrastructure Insights 리포지토리에 있는 이미지와 일치하는지 확인합니다.

운영자 배포에서 모니터링 - 운영자 배포를 편집합니다. YAML을 편집하고 모든 이미지 참조를 수정하여 개인 Docker 저장소를 사용하십시오.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-  
proxy:<ci-kube-rbac-proxy version>  
image: <docker repo of the enterprise/corp docker repo>/netapp-  
monitoring:<version>
```

operator-config.yaml에서 AgentConfiguration을 편집하여 새로운 Docker 저장소 위치를 반영하십시오. 개인 리포지토리에 대한 새 imagePullSecret을 만듭니다. 자세한 내용은 <https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/> 참조하십시오

```

agent:
  ...
  # An optional docker registry where you want docker images to be pulled
  # from as compared to CI's docker registry
  # Please see documentation link here:
  xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
  private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
  private docker registry
  dockerImagePullSecret: docker-secret-name

```

## OpenShift 지침

OpenShift 4.6 이상에서 실행 중인 경우 `_operator-config.yaml_`에서 `AgentConfiguration`을 편집하여 `_Privileged_setting`을 활성화해야 합니다.

```

# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true

```

OpenShift는 일부 Kubernetes 구성 요소에 대한 액세스를 차단할 수 있는 수준 높은 보안을 구현할 수 있습니다.

## 비밀에 대한 참고 사항

Kubernetes 모니터링 운영자가 클러스터 전체의 비밀을 볼 수 있는 권한을 제거하려면 설치하기 전에 `_operator-setup.yaml_file_`에서 다음 리소스를 삭제하십시오.

```

ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding

```

업그레이드인 경우 클러스터에서 리소스도 삭제합니다.

```

kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding

```

변경 분석이 활성화된 경우 `_AgentConfiguration_or_operator-config.yaml_`를 수정하여 변경 관리 섹션의 주석을 해제하고 변경 관리 섹션 아래에 `_kindsToIgnoreFromWatch: ""비밀""_`를 포함시킵니다. 이 줄에서 작은따옴표와 큰따옴표의 존재 및 위치를 확인합니다.

```
# change-management:
...
# # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
# # Each kind will have to be prefixed by its apigroup
# # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
kindsToIgnoreFromWatch: '"secrets"'
...
```

## Kubernetes 체크섬 확인 중

Data Infrastructure Insights 에이전트 설치 관리자가 무결성 검사를 수행하지만 일부 사용자는 다운로드한 아티팩트를 설치하거나 적용하기 전에 자체 검증을 수행할 수 있습니다. 기본 다운로드 및 설치 대신 다운로드 전용 작업을 수행하기 위해 이러한 사용자는 UI에서 가져온 에이전트 설치 명령을 편집하고 뒤에 오는 "설치" 옵션을 제거할 수 있습니다.

다음 단계를 수행하십시오.

1. 지시에 따라 Agent Installer 스크립트를 복사합니다.
2. 코드 조각을 명령 창에 붙여 넣는 대신 텍스트 편집기에 붙여 넣습니다.
3. 명령에서 뒤에 오는 "--install"을 제거합니다.
4. 텍스트 편집기에서 전체 명령을 복사합니다.
5. 이제 명령 창(작업 디렉토리)에 붙여넣고 실행합니다.
  - 다운로드 및 설치(기본값):

```
installerName=cloudinsights-rhel_centos.sh ... && sudo -E -H
./$installerName --download --install
** 다운로드 전용:
```

```
installerName=cloudinsights-rhel_centos.sh ... && sudo -E -H
./$installerName --download
```

download-only 명령은 Data Infrastructure Insights에서 작업 디렉토리로 필요한 모든 아티팩트를 다운로드합니다. 아티팩트에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 설치 스크립트
- 환경 파일입니다
- YAML 파일
- 서명된 체크섬 파일(SHA256.signed)
- 서명 확인을 위한 PEM 파일(NetApp\_cert.pem)

육안 검사를 통해 설치 스크립트, 환경 파일 및 YAML 파일을 확인할 수 있습니다.

PEM 파일의 지문이 다음과 같은 것인지 확인하여 PEM 파일을 확인할 수 있습니다.

```
1A918038E8E127BB5C87A202DF173B97A05B4996  
보다 구체적으로,
```

```
openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem  
서명된 체크섬 파일은 PEM 파일을 사용하여 확인할 수 있습니다.
```

```
openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose  
any  
모든 아티팩트가 만족스럽게 확인되면 다음을 실행하여 에이전트 설치를 시작할 수 있습니다.
```

```
sudo -E -H ./<installation_script_name> --install
```

톨레랑스와 얼룩을 볼 수 있습니다

NetApp-CI-Telegraf-DS\_*netapp-ci-fluent-bit-DS* 및 *netapp-ci-net-observer-L4-DS* Demets는 모든 노드에서 데이터를 올바르게 수집하기 위해 클러스터의 모든 노드에 Pod를 예약해야 합니다. 운영자는 잘 알려진 일부 \* 얼룩을 견딜 수 있도록 구성되었습니다. 노드에서 사용자 지정 얼룩을 구성하여 모든 노드에서 Pod가 실행되지 않도록 하는 경우 이러한 얼룩에 대해 \* 공차 \* 를 생성할 수 있습니다 "[상담원 구성 \\_에서](#)". 클러스터의 모든 노드에 사용자 지정 얼룩을 적용한 경우 운영자 포드를 예약 및 실행할 수 있도록 운영자 구축에 필요한 허용 오차도 추가해야 합니다.

Kubernetes에 대해 자세히 알아보십시오 "[오염과 내약입니다](#)".

로 돌아갑니다 "[\\* NetApp Kubernetes 모니터링 오퍼레이터 설치 \\* 페이지](#)"

## 문제 해결

Kubernetes Monitoring Operator를 설정하는 데 문제가 발생할 경우 시도해 볼 수 있는 몇 가지 사항은 다음과 같습니다.

문제:	다음은 시도해 보십시오.
Kubernetes 영구 볼륨과 해당 백엔드 스토리지 장치 간의 하이퍼링크/연결이 표시되지 않습니다. 내 Kubernetes 영구 볼륨은 스토리지 서버의 호스트 이름을 사용하여 구성됩니다.	기존 Telegraf 에이전트를 제거한 다음 최신 Telegraf 에이전트를 다시 설치하는 단계를 따릅니다. Telegraf 버전 2.0 이상을 사용 중이고 Kubernetes 클러스터 스토리지를 Data Infrastructure Insights에서 능동적으로 모니터링해야 합니다.

<p>문제:</p> <p>로그에 다음과 같은 메시지가 표시됩니다.</p> <pre>E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: * v1.mutatingWebhookConfiguration: 서버에서 요청한 리소스를 찾을 수 없습니다 E0901 15:21:43.168161 반사판.go:178] k8s.io/kube- state-metrics/internal/store/builder.go:352: 목록*v1. 임대: 서버가 요청된 리소스를 찾을 수 없습니다(Get leases.coordination.k8s.io). 등</pre>	<p>다음을 시도해 보십시오.</p> <p>이러한 메시지는 Kubernetes 버전이 1.20 미만인 경우 kube-state-metrics 버전 2.0.0 이상을 실행하는 경우에 발생할 수 있습니다.</p> <p>Kubernetes 버전 가져오기:</p> <p><i>kubectf</i> 버전 _</p> <p><i>kube-state-metrics</i> 버전을 얻으려면:</p> <pre>_kubectf get deploy/kube-state-metrics -o jsonpath='{..image}'</pre> <p>이러한 메시지가 발생하지 않도록 하기 위해 사용자는 kube-state-metrics 배포를 수정하여 다음 임대 서비스를 비활성화할 수 있습니다.</p> <pre>mutatingwebhookconfiguration validatingwebhookconfiguration _volumeAttachments 리소스 _</pre> <p>보다 구체적으로 다음과 같은 CLI 인수를 사용할 수 있습니다.</p> <p>리소스 = certificatesigningrequests, configmap, cronjobs, demonset, 배포, 엔드포인트, 수평적 podautoscalers, ingresses, 작업, 제한 범위, 네임스페이스, 네트워크 정책, 노드, 영구 볼륨권, podrightiondecudies, 포드, 자원 컨트롤러, 리플리케이션, 풀 소스, 서비스</p> <p>기본 리소스 목록은 다음과 같습니다.</p> <p>"인증 요청, 구성 맵, cronjobs, demonset, 배포, 엔드포인트, 수평 포드오토칼러, ingresses, 작업, 임대, 제한 범위, mutatingwebhookconfiguration, 네임스페이스, 네트워크 정책, 노드, 지속형, 지속형, 지속형, 볼륨, 볼륨 구성, 복제, 웹후크구성, 볼륨 첨부 파일 확인"</p>
--	---

<p>문제:</p> <p>Telegraf에서 다음과 유사한 오류 메시지가 표시되지만 Telegraf가 시작되고 실행됩니다.</p> <p>10월 11일 14:23:41 IP-172-31-39-47 systemd [1]: 인플루엔자 DB에 메트릭을 보고하기 위한 플러그인 기반 서버 에이전트를 시작했습니다.</p> <p>10월 11일 14:23:41 IP-172-31-39-47 Telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="캐시 디렉토리를 만들지 못했습니다. /etc/Telegraf/.cache/snowflake, err:mkdir/etc/Telegraf/.ca CHE: 권한이 거부되었습니다. 무시됨 \n "func="gosnowflake.(* defaultLogger).Errorf" file="log.Go:120" 10월 11일 14:23:41 IP-172-31-39-47 Telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="를 열지 못했습니다. 무시되었습니다. /etc/Telegraf/.cache/snowflake/OCSP_response_cache.json을 엽니다. 해당 없음 파일 또는 디렉터리\n"func="gosnowflake.(* defaultLogger).Errorf" file="log.Go:120" 10월 11일 14:23:41 IP-172-31-39-47 Telegraf[1827]:2021-10-11T14:23:41Z !! 텔레그래프 1.19.3 시작</p>	<p>다음을 시도해 보십시오.</p> <p>이는 알려진 문제입니다. 을 참조하십시오 <a href="#">"이 GitHub 기사를 참조하십시오"</a> 를 참조하십시오. Telegraf가 실행 중인 경우 사용자는 이러한 오류 메시지를 무시할 수 있습니다.</p>
<p>Kubernetes에서 Telegraf POD가 다음 오류를 보고합니다.</p> <p>"mountstats 정보 처리 중 오류 발생: mountstats 파일을 열지 못했습니다. /hostfs/proc/1/mountstats, 오류: open/hostfs/proc/1/mountstats: permission denied"</p>	<p>SELinux가 설정되어 있고 강제 적용되는 경우 Telegraf 포드가 Kubernetes 노드의 /proc/1/mountstats 파일에 액세스하지 못할 수 있습니다. 이 제한을 해결하려면 agentconfiguration을 편집하고 runPrivileged 설정을 활성화하십시오. 자세한 내용은 를 참조하십시오 <a href="#">"OpenShift 지침"</a>.</p>
<p>Kubernetes에서 내 Telegraf ReplicaSet POD가 다음 오류를 보고합니다.</p> <p>[inputs.prometheus] 플러그인 오류: keypair /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: open/etc/Kubernetes/pki/etcd/server.crt: 해당 파일 또는 디렉토리가 없습니다</p>	<p>Telegraf ReplicaSet POD는 마스터나 etcd로 지정된 노드에서 실행되도록 설계되었습니다. ReplicaSet 포드가 이러한 노드 중 하나에서 실행되고 있지 않으면 이러한 오류가 발생합니다. 마스터/etcd 노드에 문제가 있는지 확인합니다. 만약 그렇다면, 텔레그래프 ReplicaSet, 텔레그래프-RS에 필요한 내약성을 추가한다.</p> <p>예를 들어 ReplicaSet을 편집합니다.</p> <p>kubectl 편집 RS Telegraf-RS</p> <p>... 그리고 사양에 적절한 공차를 추가합니다. 그런 다음 ReplicaSet 포드를 다시 시작합니다.</p>



문제:	다음은 시도해 보십시오.
PSP/PSA 환경이 있습니다. 이 문제가 모니터링 오퍼레이터에게 영향을 미칩니까?	<p>Kubernetes 클러스터가 PSP(Pod Security Policy) 또는 PSA(Pod Security Admission)를 적용한 상태에서 실행되는 경우 최신 Kubernetes Monitoring Operator로 업그레이드해야 합니다. 다음 단계에 따라 PSP/PSA를 지원하는 현재 오퍼레이터로 업그레이드하십시오.</p> <p>1. <a href="#">설치 제거</a> 이전 모니터링 오퍼레이터:</p> <pre>kubectl delete agent-monitoring-netapp-n netapp-monitoring kubectl delete ns NetApp-monitoring kubectl 삭제 CRD agents.monitoring.netapp.com clusterrole agent-manager-role agent-proxy-role agent-metrics-reader를 삭제합니다 clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 을 삭제합니다</pre> <p>2. <a href="#">설치합니다</a> 모니터링 운영자의 최신 버전</p>
오퍼레이터를 배포하는 데 문제가 발생했고 PSP/PSA를 사용하고 있습니다.	<p>다음 명령을 사용하여 에이전트를 편집합니다.</p> <pre>kubectl -n &lt;name-space&gt; 편집 에이전트</pre> <p>'보안 정책 사용'을 '거짓'으로 표시합니다. 이렇게 하면 Pod 보안 정책 및 Pod 보안 입장이 비활성화되고 운영자가 배포할 수 있습니다. 다음 명령을 사용하여 확인합니다.</p> <pre>kubectl get psp(Pod 보안 정책이 제거됨) kubectl get all -n &lt;namespace&gt;</pre>
grep -i psp (아무것도 발견되지 않았음을 보여줌)	"ImagePullBackoff" 오류가 표시됩니다
이러한 오류는 사용자 지정 또는 전용 Docker 리포지토리가 있고 Kubernetes Monitoring Operator가 해당 리포지토리를 제대로 인식하도록 아직 구성하지 않은 경우 나타날 수 있습니다. <a href="#">자세히 보기</a> 사용자 지정/개인 저장소 구성 정보	모니터링 운영자 구축에 문제가 있는데 현재 설명서를 참조해도 문제를 해결하는 데 도움이 되지 않습니다.

<p>문제:</p> <p>다음 명령의 출력을 캡처하거나 기록해 두고 기술 지원 팀에 문의하십시오.</p> <pre>kubectl -n netapp-monitoring get all kubectl -n netapp-monitoring describe all kubectl -n netapp-monitoring logs &lt;monitoring-operator-pod&gt; --all -containers=true kubectl -n netapp-monitoring logs &lt;telegraf-pod&gt; --all -containers=true</pre>	<p>다음을 시도해 보십시오.</p> <p>Operator 네임스페이스의 NET-observer(워크로드 맵) 포드는 CrashLoopBackOff에 있습니다</p>
<p>이러한 포드는 네트워크 관찰 가능성을 위한 워크로드 맵 데이터 수집기에 해당합니다. 다음을 시도해 보십시오.</p> <ul style="list-style-type: none"> <li>• 최소 커널 버전을 확인하려면 pods 중 하나의 로그를 확인하십시오. 예를 들면 다음과 같습니다. — {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"유효성 검사에 실패했습니다. 이유: 커널 버전 3.10.0이 최소 커널 버전 4.18.0", "time":"2022-11-09T08:23:08Z"}보다 작습니다 —</li> <li>• Net-observer Pod를 사용하려면 Linux 커널 버전이 4.18.0 이상이어야 합니다. "uname -r" 명령을 사용하여 커널 버전을 확인하고 해당 버전이 4.18.0 이상인지 확인합니다</li> </ul>	<p>Pod는 운영자 네임스페이스(기본값: NetApp-모니터링)에서 실행되지만, 워크로드 맵 또는 Kubernetes 메트릭에 대한 UI에는 데이터가 표시되지 않습니다</p>
<p>K8S 클러스터의 노드에서 시간 설정을 확인합니다. 정확한 감사 및 데이터 보고를 위해 NTP(Network Time Protocol) 또는 SNTP(Simple Network Time Protocol)를 사용하여 Agent 시스템의 시간을 동기화하는 것이 좋습니다.</p>	<p>Operator 네임스페이스의 일부 NET-observer Pod가 Pending 상태입니다</p>
<p>Net-observer는 DemonSet로, k8s 클러스터의 각 노드에서 포드를 실행합니다.</p> <ul style="list-style-type: none"> <li>• 보류 중인 Pod를 확인하고 CPU 또는 메모리에 리소스 문제가 있는지 확인합니다. 노드에서 필요한 메모리 및 CPU를 사용할 수 있는지 확인합니다.</li> </ul>	<p>Kubernetes Monitoring Operator를 설치한 직후 로그에 다음이 표시됩니다.</p> <pre>[inputs.prometheus] 플러그인에서 오류 발생:\http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics:get\http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics:다이얼 tcp:lookup kube-state-metrics.&lt;namespace&gt;.svc.cluster.local: 해당 호스트가 없습니다</pre>

문제:	다음을 시도해 보십시오.
이 메시지는 일반적으로 새 오퍼레이터가 설치되어 있고 <code>_Telegraf-RS_POD</code> 가 <code>_KSM_POD</code> 가 가동되기 전에 작동 중일 때만 표시됩니다. 이러한 메시지는 모든 Pod가 실행되면 중지되어야 합니다.	클러스터에 존재하는 Kubernetes CronJobs에 대해 어떤 메트릭도 수집되지 않습니다.
Kubernetes 버전 확인(예 <code>kubectl version</code> )를 클릭합니다. v1.20.x 이하일 경우 이는 예상되는 제한 사항입니다. Kubernetes Monitoring Operator와 함께 배포된 kube-state-metrics 릴리스는 v1.cronjob만 지원합니다. Kubernetes 1.20.x 이하에서는 <code>crontjob</code> 리소스가 v1beta.crontjob에 있습니다. 따라서 kube-state-metrics는 <code>crontjob</code> 리소스를 찾을 수 없습니다.	운영자 설치 후, Telegraf-ds Pod는 <code>CrashLoopBackOff</code> 로 진입하고 POD 로그는 "su:Authentication failure"를 나타낸다.
<code>_AgentConfiguration_</code> 에서 <code>Telegraf</code> 섹션을 편집하고 <code>_dockerMetricCollectionEnabled_</code> 를 <code>false</code> 로 설정합니다. 자세한 내용은 조작자를 "구성 옵션" 참조하십시오. 참고: <i>Data Infrastructure Insights Federal Edition</i> 을 사용하는 경우 <code>Docker</code> 소켓에 액세스하려면 <code>Telegraf</code> 컨테이너를 루트로 실행하거나 <code>_su_</code> 를 사용하여 <code>Telegraf</code> 사용자를 <code>Docker</code> 그룹에 추가해야 하기 때문에 <code>_su_</code> 사용이 제한된 사용자는 <code>Docker</code> 메트릭을 수집할 수 없습니다. <code>Docker</code> 메트릭 수집 및 <code>_su_</code> 의 사용은 기본적으로 활성화되어 있습니다. 이 두 가지를 모두 사용하지 않으려면 <code>_AgentConfiguration_</code> 파일에서 <code>_Telegraf.docker_entry</code> 를 제거하십시오. ... spec:... Telegraf:... -name:docker run-mode: -DemonSet 대체:- key:docker_unix_sock_placeholder 값: unix://run/docker.sock... ..	Telegraf 로그에 다음과 유사한 오류 메시지가 반복적으로 표시됩니다.  E! [agent] 출력에 쓰는 중 오류가 발생했습니다. http: POST "https://<tenant_url>/REST/v1/lake/injest/influxdb": 컨텍스트 기한 초과(클라이언트. 헤더 대기 중 시간 초과)
<code>_AgentConfiguration_</code> 에서 <code>Telegraf</code> 섹션을 편집하고 <code>increase_outputTimeout_</code> 을 10초로 편집합니다. 자세한 내용은 조작자를 참조하십시오 "구성 옵션".	일부 이벤트 로그에 대한 <code>_divedobject_data</code> 가 없습니다.
의 단계를 수행했는지 확인합니다 "권한" 섹션을 참조하십시오.	두 개의 모니터링 운영자 Pod가 실행 중인 것을 볼 수 있는데, 하나는 <code>netapp-ci-monitoring-operator-&lt;pod&gt;</code> 이고 다른 하나는 <code>monitoring-operator-&lt;pod&gt;</code> 입니다.
2023년 10월 12일부터 Data Infrastructure Insights는 사용자에게 더 나은 서비스를 제공하기 위해 운영자를 재고했습니다. 변경 사항을 완전히 채택하려면 반드시 <a href="#">기존 연산자를 제거합니다</a> AND를 준수해야 합니다. <a href="#">새 장치를 장착하십시오</a>	저의 Kubernetes 이벤트가 예기치 않게 Data Infrastructure Insights에 대한 보고를 중단했습니다.
이벤트 내보내기 포드의 이름을 검색합니다.  <pre>`kubectl -n netapp-monitoring get pods`</pre>	<code>grep event-exporter</code>

문제:	다음을 시도해 보십시오.
<pre>awk '{print \$1}'</pre>	<pre>sed 's/event-exporter./event-exporter/' "netapp-ci-event-exporter" 또는 "event-exporter"여야 합니다. 그런 다음 모니터링 에이전트를 편집합니다 `kubectl -n netapp-monitoring edit agent`를 입력하고 log_file 의 값을 이전 단계에서 찾은 적절한 이벤트 내보내기 포드 이름을 반영하도록 설정합니다. 보다 구체적으로 log_file을 "/var/log/containers/netapp-ci- event-exporter.log" 또는 "/var/log/containers/event- exporter .log"로 설정해야 합니다.</pre> <p>....</p> <p><b>fluent-bit:</b></p> <p>...</p> <p><b>- name: event-exporter-ci</b></p> <p><b>substitutions:</b></p> <p><b>- key: LOG_FILE</b></p> <p><b>values:</b></p> <p><b>- /var/log/containers/netapp-ci-event-exporter.log</b></p> <p>...</p> <p>....</p> <p>또는, 하나를 할 수도 있습니다 <a href="#">설치 제거 및 다시 설치합니다</a> 에이전트</p>
리소스 부족으로 인해 Kubernetes Monitoring Operator에 의해 구축된 Pod가 충돌하는 것을 볼 수 있습니다.	Kubernetes 모니터링 운영자를 참조하십시오 <a href="#">"구성 옵션"</a> 필요한 경우 CPU 및/또는 메모리 제한을 늘립니다.
이미지가 없거나 잘못된 구성으로 인해 NetApp-ci-kube-state 메트릭 Pod가 시작되지 않거나 준비되지 않았습니다. 이제 StatefulSet이 중단되고 구성 변경 사항이 NetApp-ci-kube-state-metrics Pod에 적용되지 않습니다.	StatefulSet 은 에 있습니다 <a href="#">"고장"</a> 상태. 구성 문제를 해결한 후에는 NetApp-ci-kube-state-metrics Pod를 바운스하게 만들 수 있습니다.
Kubernetes Operator 업그레이드를 실행하고 ErrImagePull(이미지를 가져오지 못함)을 throw하는 후 NetApp-ci-kube-state-metrics Pod가 시작되지 않습니다.	포드 재설정을 수동으로 시도하십시오.
"이벤트가 maxEventAgeSeconds보다 오래된 것으로 폐기됨" 메시지가 Log Analysis에서 내 Kubernetes 클러스터에 대해 관찰되고 있습니다.	Operator_agentconfiguration_을 수정하고 <i>event-exporter-maxEventAgeSeconds</i> (예: 60s), <i>event-exporter-kubeQPS</i> (예: 100) 및 <i>event-exporter-kubeBurst</i> (예: 500)를 증가시킵니다. 이러한 구성 옵션에 대한 자세한 내용은 를 참조하십시오 <a href="#">"구성 옵션"</a> 페이지.
Telegraf는 잠금 가능한 메모리가 부족하다는 경고 또는 충돌에 대해 경고합니다.	기본 운영 체제/노드에서 Telegraf의 잠금 가능한 메모리 제한을 늘리십시오. 제한을 늘리는 것이 옵션이 아닌 경우 NKMO agentconfiguration과 <i>set_unprotected_to_true</i> 를 수정합니다. 그러면 Telegraf가 잠긴 메모리 페이지를 예약하지 않도록 지시합니다. 암호 해독된 암호가 디스크로 교체될 수 있기 때문에 보안 위험이 발생할 수 있지만 잠긴 메모리를 예약할 수 없는 환경에서 실행할 수 있습니다. <i>_unprotected_configuration</i> 옵션에 대한 자세한 내용은 를 참조하십시오 <a href="#">"구성 옵션"</a> 페이지.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Kubernetes 모니터링 운영자 구성 옵션

를 클릭합니다 "[Kubernetes 모니터링 운영자](#)" 구성을 사용자 지정할 수 있습니다.

아래 표에는 \_AgentConfiguration\_ 파일에 사용할 수 있는 옵션이 나와 있습니다.

구성 요소	옵션을 선택합니다	설명
에이전트		운영자가 설치할 수 있는 모든 구성품에 공통으로 적용되는 구성 옵션. 이러한 옵션은 "글로벌" 옵션으로 간주할 수 있습니다.
	dockerRepo	DockerRepo는 Data Infrastructure Insights Docker 저장소와 비교하여 고객의 전용 Docker Repos에서 이미지를 가져오도록 재정의합니다. 기본값은 Data Infrastructure Insights Docker 저장소입니다
	dockerImagePullSecret	선택 사항: 고객의 비공개 리포의 비밀
	클러스터 이름	모든 고객 클러스터에서 클러스터를 고유하게 식별하는 자유 텍스트 필드입니다. Data Infrastructure Insights 테넌트 전체에서 고유해야 합니다. 기본값은 고객이 "클러스터 이름" 필드의 UI에 입력하는 것입니다
	프록시 형식: 프록시: 서버: 포트: 사용자 이름: 암호: 프록시 없음: 텔레그라프프록시 사용: isAuProxyEnabled: 사용 안 함: isFluentbitProxyEnabled: isCollectorProxyEnabled(isCollectorProxyEnabled):	프록시를 설정하는 선택 사항입니다. 일반적으로 고객의 기업 대리인입니다.
텔레그라프		작업자의 Telegraf 설치를 사용자 정의할 수 있는 구성 옵션
	수집 간격	메트릭 수집 간격(초)(최대 = 60초)
	dsCpuLimit 를 선택합니다	Telegraf DS의 CPU 제한
	dsMemLimit	Telegraf DS의 메모리 제한
	dsCpuRequest 를 참조하십시오	Telegraf DS에 대한 CPU 요청
	dsMemRequest입니다	Telegraf DS에 대한 메모리 요청

구성 요소	옵션을 선택합니다	설명
	rsCpuLimit	Telegraf RS의 CPU 제한
	메모리 제한	Telegraf RS의 메모리 제한
	rsCpuRequest 를 참조하십시오	Telegraf RS에 대한 CPU 요청
	rsMemRequest입니다	Telegraf RS에 대한 메모리 요청
	runPrivileged(권한이	권한 모드에서 Telegraf 컨테이너를 실행합니다. k8s 노드에서 SELinux가 설정된 경우 이 값을 TRUE로 설정합니다
	BatchSize(부atchSize)	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	백혈구 한계	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	RoundInterval(라운드 간격	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	콜렉션 지터	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	정밀도	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	FlushInterval(플러시간격	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	플러시지터	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	출력 제한 시간	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	dsTolerations 를 선택합니다	텔레그라프 - DS 추가 허용.
	RsTolerations를 선택합니다	Telegraf-RS 추가 허용.
	SkipProcessorsAfterAggregators 를 참조하십시오	을 참조하십시오 <a href="#">"Telegraf 구성 문서"</a>
	보호되지 않음	자세한 내용은 다음을 참조하십시오 <a href="#">"알려진 Telegraf 문제입니다"</a> . setting_unprotected_는 Kubernetes 모니터링 운영자에게 에서 Telegraf를 실행하도록 지시합니다 --unprotected 깃발.
Kudbe-state-metrics를 나타냅니다		작업자의 kudbe 상태 메트릭 설치를 사용자 지정할 수 있는 구성 옵션입니다
	cpuLimit	kubbe-state-metrics 구축을 위한 CPU 제한입니다
	MemLimit	kubbe-state-metrics 구축을 위한 MEM 한도
	cpuRequest입니다	kubbe 상태 메트릭 구축을 위한 CPU 요청입니다
	MemRequest입니다	MEM은 kudo 상태 메트릭 배포를 요청합니다
	리소스	캡처할 리소스의 심표로 구분된 목록입니다. 예: cronjobs, demonset, 배포, 링스, 작업, 네임스페이스, 노드, persistentvolumeclaims, persistentvolumes, dPOD, replicaset, resourcequotas, 서비스, statefulsets
	공차	Kudbe-state-metrics 추가 공약입니다.

구성 요소	옵션을 선택합니다	설명
	라벨	kuba-state-metrics가 캡처해야 하는 심표로 구분된 리소스 목록입니다  예: cronjobs=[*], demonsets=[*], 배포=[*], 링스=[*], 작업=[*], 네임스페이스=[*], 노드=[*], persistentvolumeclaims=[*], persistentvolumes=[*], pod=[*], replicaset=[*], resourcequotas=[*], services=[*], statefulsets=[*]
로그		운영자의 로그 수집 및 설치를 사용자 정의할 수 있는 구성 옵션입니다
	readFromHead(readFromHead)	참/거짓, 유창한 비트가 로그에서 로그를 읽어야 합니다
	시간 초과	시간 초과(초)
	dnsMode를 선택합니다	TCP/UDP, DNS 모드
	유창한 비트 내약성	Fluent-bit-DS 추가 허용.
	이벤트-수출자-내약성	이벤트-수출자 추가 허용.
	event-exporter-maxEventAgeSeconds입니다	이벤트 내보내기 최대 이벤트 기간. 을 참조하십시오 <a href="https://github.com/jkroepke/resmoio-kubernetes-event-exporter">https://github.com/jkroepke/resmoio-kubernetes-event-exporter</a>
	runPrivileged(권한이)	Fluent Bit이 시작되지 않고 데이터베이스를 열거나 만들려고 하면 runPrivileged를 true로 설정합니다.
워크로드 맵		작업자의 작업량 맵 수집 및 설치를 사용자 정의할 수 있는 구성 옵션입니다
	cpuLimit	순 관찰자 DS에 대한 CPU 제한입니다
	MemLimit	순 관찰자 DS에 대한 MEM 한도
	cpuRequest입니다	net observer DS에 대한 CPU 요청입니다
	MemRequest입니다	net observer DS에 대한 MEM 요청
	MetricAggregationInterval입니다	메트릭 집계 간격(초)
	bpfPollInterval입니다	BPF 폴링 간격(초)
	enableDNSLookup	True/false, DNS 조회를 사용하도록 설정합니다
	L4-공차	NET-observer-L4-DS 추가 허용 오차
	runPrivileged(권한이)	참/거짓 - Kubernetes 노드에서 SELinux가 활성화된 경우 runprivileged 를 true 로 설정합니다.
변경 관리		Kubernetes 변경 관리 및 분석에 대한 구성 옵션
	cpuLimit	change-observer-watch-RS에 대한 CPU 제한값입니다
	MemLimit	change-observer-watch-RS에 대한 MEM 한계

구성 요소	옵션을 선택합니다	설명
	cpuRequest입니다	change-observer-watch-RS에 대한 CPU 요청입니다
	MemRequest입니다	change-observer-watch-RS에 대한 MEM 요청
	FailureDeclarationInterval Mins 를 참조하십시오	실패한 워크로드 배포가 실패로 표시되는 간격(분)입니다
	deployAggrIntervalSeconds입니다	작업 부하 배포 진행 중 이벤트가 전송되는 빈도입니다
	비작업 로드 AggrIntervalSeconds입니다	비워크로드 구축이 결합되고 전송되는 빈도입니다
	TERmsToRedact 를 참조하십시오	env 이름 및 데이터 맵에서 사용되는 정규식 집합으로, 값이 교정됩니다 예제 용어: "pwd", "password", "token", "apikey", "api-key", "JWT"
	AdditionalKindsToWatch 를 참조하십시오	수집기에서 감시하는 기본 종류 집합에서 볼 수 있는 추가 종류의 심표로 구분된 목록
	KindsToIgnoreFromWatch 를 참조하십시오	수집기에서 감시하는 기본 종류의 집합에서 감시하는 것을 무시할 수 있는 심표로 구분된 종류의 목록입니다
	LogRecordAggrIntervalSeconds입니다	수집기에서 CI로 로그 레코드를 보내는 빈도입니다
	시계의 내약성	change-observer-watch-DS 추가 허용 오차. 축약된 단일 선 형식만 해당. 예: '{key:taint1,operator:exists,effect:NoSchedule}, {key:taint2,operator:exists,effect:NoExecute}'

## AgentConfiguration 파일 예

다음은 샘플\_AgentConfiguration\_파일입니다.

```

apiVersion: monitoring.netapp.com/v1alpha1
kind: AgentConfiguration
metadata:
  name: netapp-ci-monitoring-configuration
  namespace: "netapp-monitoring"
  labels:
    installed-by: nkmo-netapp-monitoring

spec:
  # # You can modify the following fields to configure the operator.
  # # Optional settings are commented out and include default values for
  # # reference
  # # To update them, uncomment the line, change the value, and apply
  # # the updated AgentConfiguration.
  agent:

```



```

# # [Required Field] A uniquely identifiable user-friendly
clustername.
# # clusterName must be unique across all clusters in your Data
Infrastructure Insights environment.
  clusterName: "my_cluster"

# # Proxy settings. The proxy that the operator should use to send
metrics to Data Infrastructure Insights.
# # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#configuring-proxy-
support
# proxy:
#   server:
#   port:
#   noproxy:
#   username:
#   password:
#   isTelegrafProxyEnabled:
#   isFluentbitProxyEnabled:
#   isCollectorsProxyEnabled:

# # [Required Field] By default, the operator uses the CI repository.
# # To use a private repository, change this field to your repository
name.
# # Please see documentation here: https://docs.netapp.com/us-
en/cloudinsights/task_config_telegraf_agent_k8s.html#using-a-custom-or-
private-docker-repository
  dockerRepo: 'docker.c01.cloudinsights.netapp.com'
# # [Required Field] The name of the imagePullSecret for dockerRepo.
# # If you are using a private repository, change this field from
'netapp-ci-docker' to the name of your secret.
  dockerImagePullSecret: 'netapp-ci-docker'

# # Allow the operator to automatically rotate its ApiKey before
expiration.
# tokenRotationEnabled: 'true'
# # Number of days before expiration that the ApiKey should be
rotated. This must be less than the total ApiKey duration.
# tokenRotationThresholdDays: '30'

telegraf:
# # Settings to fine-tune metrics data collection. Telegraf config
names are included in parenthesis.
# # See
https://github.com/influxdata/telegraf/blob/master/docs/CONFIGURATION.md#agent

```

```

# # The default time telegraf will wait between inputs for all plugins
(interval). Max=60
# collectionInterval: '60s'
# # Maximum number of records per output that telegraf will write in
one batch (metric_batch_size).
# batchSize: '10000'
# # Maximum number of records per output that telegraf will cache
pending a successful write (metric_buffer_limit).
# bufferLimit: '150000'
# # Collect metrics on multiples of interval (round_interval).
# roundInterval: 'true'
# # Each plugin waits a random amount of time between the scheduled
collection time and that time + collection_jitter before collecting inputs
(collection_jitter).
# collectionJitter: '0s'
# # Collected metrics are rounded to the precision specified. When set
to "0s" precision will be set by the units specified by interval
(precision).
# precision: '0s'
# # Time telegraf will wait between writing outputs (flush_interval).
Max=collectionInterval
# flushInterval: '60s'
# # Each output waits a random amount of time between the scheduled
write time and that time + flush_jitter before writing outputs
(flush_jitter).
# flushJitter: '0s'
# # Timeout for writing to outputs (timeout).
# outputTimeout: '5s'

# # telegraf-ds CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# dsCpuLimit: '750m'
# dsMemLimit: '800Mi'
# dsCpuRequest: '100m'
# dsMemRequest: '500Mi'

# # telegraf-rs CPU/Mem limits and requests.
# rsCpuLimit: '3'
# rsMemLimit: '4Gi'
# rsCpuRequest: '100m'
# rsMemRequest: '500Mi'

# # Skip second run of processors after aggregators
# skipProcessorsAfterAggregators: 'true'

```

```
# # telegraf additional tolerations. Use the following abbreviated
single line format only.
```

```
# # Inspect telegraf-rs/-ds to view tolerations which are always
present.
```

```
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
```

```
# dsTolerations: ''
```

```
# rsTolerations: ''
```

```
# If telegraf warns of insufficient lockable memory, try increasing
the limit of lockable memory for Telegraf in the underlying operating
system/node. If increasing the limit is not an option, set this to true
to instruct Telegraf to not attempt to reserve locked memory pages. While
this might pose a security risk as decrypted secrets might be swapped out
to disk, it allows for execution in environments where reserving locked
memory is not possible.
```

```
# unprotected: 'false'
```

```
# # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
```

```
# runPrivileged: 'false'
```

```
# # Collect container Block IO metrics.
```

```
# dsBlockIOEnabled: 'true'
```

```
# # Collect NFS IO metrics.
```

```
# dsNfsIOEnabled: 'true'
```

```
# # Collect kubernetes.system_container metrics and objects in the
kube-system|cattle-system namespaces for managed kubernetes clusters (EKS,
AKS, GKE, managed Rancher). Set this to true if you want collect these
metrics.
```

```
# managedK8sSystemMetricCollectionEnabled: 'false'
```

```
# # Collect kubernetes.pod_volume (pod ephemeral storage) metrics.
Set this to true if you want to collect these metrics.
```

```
# podVolumeMetricCollectionEnabled: 'false'
```

```
# # Declare Rancher cluster as managed. Set this to true if your
Rancher cluster is managed as opposed to on-premise.
```

```
# isManagedRancher: 'false'
```

```
# # If telegraf-rs fails to start due to being unable to find the etcd
crt and key, manually specify the appropriate path here.
```

```
# rsHostEtcdCrt: ''
```

```
# rsHostEtcdKey: ''
```

```

# kube-state-metrics:
# # kube-state-metrics CPU/Mem limits and requests.
# cpuLimit: '500m'
# memLimit: '1Gi'
# cpuRequest: '100m'
# memRequest: '500Mi'

# # Comma-separated list of resources to enable.
# # See resources in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
# resources:
'cronjobs,daemonsets,deployments,ingresses,jobs,namespace,nodes,persistentvolumes,persistentvolumes,pods,replicasets,resourcequotas,services,statefulsets'

# # Comma-separated list of metrics to enable.
# # See metric-allowlist in https://github.com/kubernetes/kube-state-
metrics/blob/main/docs/cli-arguments.md
# metrics:
'kube_cronjob_created,kube_cronjob_status_active,kube_cronjob_labels,kube_daemonset_created,kube_daemonset_status_current_number_scheduled,kube_daemonset_status_desired_number_scheduled,kube_daemonset_status_number_available,kube_daemonset_status_number_misscheduled,kube_daemonset_status_number_ready,kube_daemonset_status_number_unavailable,kube_daemonset_status_observed_generation,kube_daemonset_status_updated_number_scheduled,kube_daemonset_metadata_generation,kube_daemonset_labels,kube_deployment_status_replicas,kube_deployment_status_replicas_available,kube_deployment_status_replicas_unavailable,kube_deployment_status_replicas_updated,kube_deployment_status_observed_generation,kube_deployment_spec_replicas,kube_deployment_spec_paused,kube_deployment_spec_strategy_rollingupdate_max_unavailable,kube_deployment_spec_strategy_rollingupdate_max_surge,kube_deployment_metadata_generation,kube_deployment_labels,kube_deployment_created,kube_job_created,kube_job_owner,kube_job_status_active,kube_job_status_succeeded,kube_job_status_failed,kube_job_labels,kube_job_status_start_time,kube_job_status_completion_time,kube_namespace_created,kube_namespace_labels,kube_namespace_status_phase,kube_node_info,kube_node_labels,kube_node_role,kube_node_spec_unschedulable,kube_node_created,kube_persistentvolume_capacity_bytes,kube_persistentvolume_status_phase,kube_persistentvolume_labels,kube_persistentvolume_info,kube_persistentvolume_claim_ref,kube_persistentvolumeclaim_access_mode,kube_persistentvolumeclaim_info,kube_persistentvolumeclaim_labels,kube_persistentvolumeclaim_resource_requests_storage_bytes,kube_persistentvolumeclaim_status_phase,kube_pod_info,kube_pod_start_time,kube_pod_completion_time,kube_pod_owner,kube_pod_labels,kube_pod_status_phase,kube_pod_status_ready,kube_pod_status_scheduled,kube_pod_container_info,kube_pod_container_status_waiting,kube_pod_container_status_waiting_reason,kube_pod_c

```

```
ontainer_status_running,kube_pod_container_state_started,kube_pod_containe
r_status_terminated,kube_pod_container_status_terminated_reason,kube_pod_c
ontainer_status_last_terminated_reason,kube_pod_container_status_ready,kub
e_pod_container_status_restarts_total,kube_pod_overhead_cpu_cores,kube_pod
_overhead_memory_bytes,kube_pod_created,kube_pod_deletion_timestamp,kube_p
od_init_container_info,kube_pod_init_container_status_waiting,kube_pod_ini
t_container_status_waiting_reason,kube_pod_init_container_status_running,k
ube_pod_init_container_status_terminated,kube_pod_init_container_status_te
rminated_reason,kube_pod_init_container_status_last_terminated_reason,kube
_pod_init_container_status_ready,kube_pod_init_container_status_restarts_t
otal,kube_pod_status_scheduled_time,kube_pod_status_unschedulable,kube_pod
_spec_volumes_persistentvolumeclaims_readonly,kube_pod_container_resource
_requests_cpu_cores,kube_pod_container_resource_requests_memory_bytes,kube
_pod_container_resource_requests_storage_bytes,kube_pod_container_resource
_requests_ephemeral_storage_bytes,kube_pod_container_resource_limits_cpu_co
res,kube_pod_container_resource_limits_memory_bytes,kube_pod_container_res
ource_limits_storage_bytes,kube_pod_container_resource_limits_ephemeral_st
orage_bytes,kube_pod_init_container_resource_limits_cpu_cores,kube_pod_ini
t_container_resource_limits_memory_bytes,kube_pod_init_container_resource
_limits_storage_bytes,kube_pod_init_container_resource_limits_ephemeral_sto
rage_bytes,kube_pod_init_container_resource_requests_cpu_cores,kube_pod_in
it_container_resource_requests_memory_bytes,kube_pod_init_container_resour
ce_requests_storage_bytes,kube_pod_init_container_resource_requests_epheme
ral_storage_bytes,kube_replicaset_status_replicas,kube_replicaset_status_r
eady_replicas,kube_replicaset_status_observed_generation,kube_replicaset_s
pec_replicas,kube_replicaset_metadata_generation,kube_replicaset_labels,ku
be_replicaset_created,kube_replicaset_owner,kube_resourcequota,kube_resour
cequota_created,kube_service_info,kube_service_labels,kube_service_created
,kube_service_spec_type,kube_statefulset_status_replicas,kube_statefulset
_status_replicas_current,kube_statefulset_status_replicas_ready,kube_statef
ulset_status_replicas_updated,kube_statefulset_status_observed_generation,
kube_statefulset_replicas,kube_statefulset_metadata_generation,kube_statef
ulset_created,kube_statefulset_labels,kube_statefulset_status_current_revi
sion,kube_statefulset_status_update_revision,kube_node_status_capacity,kub
e_node_status_allocatable,kube_node_status_condition,kube_pod_container_re
source_requests,kube_pod_container_resource_limits,kube_pod_init_container
_resource_limits,kube_pod_init_container_resource_requests'
```

```
## Comma-separated list of Kubernetes label keys that will be used in
the resources' labels metric.
```

```
## See metric-labels-allowlist in https://github.com/kubernetes/kube-state-metrics/blob/main/docs/cli-arguments.md
```

```
# labels:
```

```
'cronjobs=[*],daemonsets=[*],deployments=[*],ingresses=[*],jobs=[*],namesp
aces=[*],nodes=[*],persistentvolumeclaims=[*],persistentvolumes=[*],pods=[
*],replicasets=[*],resourcequotas=[*],services=[*],statefulsets=[*]'
```

```

# # kube-state-metrics additional tolerations. Use the following
abbreviated single line format only.
# # No tolerations are applied by default
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# tolerations: ''

# # kube-state-metrics shards. Increase the number of shards for
larger clusters if telegraf RS pod(s) experience collection timeouts
# shards: '2'

# # Settings for the Events Log feature.
# logs:
# # Set runPrivileged to true if Fluent Bit fails to start, trying to
open/create its database.
# runPrivileged: 'false'

# # If Fluent Bit should read new files from the head, not tail.
# # See Read_from_Head in
https://docs.fluentbit.io/manual/pipeline/inputs/tail
# readFromHead: "true"

# # Network protocol that Fluent Bit should use for DNS: "UDP" or
"TCP".
# dnsMode: "UDP"

# # DNS resolver that Fluent Bit should use: "LEGACY" or "ASYNC"
# fluentBitDNSResolver: "LEGACY"

# # Logs additional tolerations. Use the following abbreviated single
line format only.
# # Inspect fluent-bit-ds to view tolerations which are always
present. No tolerations are applied by default for event-exporter.
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# fluent-bit-tolerations: ''
# event-exporter-tolerations: ''

# # event-exporter CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# event-exporter-cpuLimit: '500m'
# event-exporter-memLimit: '1Gi'
# event-exporter-cpuRequest: '50m'
# event-exporter-memRequest: '100Mi'

```

```
# # event-exporter max event age.
# # See https://github.com/jkroepke/resmoio-kubernetes-event-exporter
# event-exporter-maxEventAgeSeconds: '10'

# # event-exporter client-side throttling
# # Set kubeBurst to roughly match your events per minute and
kubeQPS=kubeBurst/5
# # See https://github.com/resmoio/kubernetes-event-
exporter#troubleshoot-events-discarded-warning
# event-exporter-kubeQPS: 20
# event-exporter-kubeBurst: 100

# # fluent-bit CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# fluent-bit-cpuLimit: '500m'
# fluent-bit-memLimit: '1Gi'
# fluent-bit-cpuRequest: '50m'
# fluent-bit-memRequest: '100Mi'

# # Settings for the Network Performance and Map feature.
# workload-map:
# # netapp-ci-net-observer-l4-ds CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# cpuLimit: '500m'
# memLimit: '500Mi'
# cpuRequest: '100m'
# memRequest: '500Mi'

# # Metric aggregation interval in seconds. Min=30, Max=120
# metricAggregationInterval: '60'

# # Interval for bpf polling. Min=3, Max=15
# bpfPollInterval: '8'

# # Enable performing reverse DNS lookups on observed IPs.
# enableDNSLookup: 'true'

# # netapp-ci-net-observer-l4-ds additional tolerations. Use the
following abbreviated single line format only.
# # Inspect netapp-ci-net-observer-l4-ds to view tolerations which are
always present.
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# l4-tolerations: ''
```

```

# # Set runPrivileged to true if SELinux is enabled on your Kubernetes
nodes.
# # Note: In OpenShift environments, this is set to true
automatically.
# runPrivileged: 'false'

# change-management:
# # change-observer-watch-rs CPU/Mem limits and requests.
# # See https://kubernetes.io/docs/concepts/configuration/manage-
resources-containers/
# cpuLimit: '1'
# memLimit: '1Gi'
# cpuRequest: '500m'
# memRequest: '500Mi'

# # Interval in minutes after which a non-successful deployment of a
workload will be marked as failed
# failureDeclarationIntervalMins: '30'

# # Frequency at which workload deployment in-progress events are sent
# deployAggrIntervalSeconds: '300'

# # Frequency at which non-workload deployments are combined and sent
# nonWorkloadAggrIntervalSeconds: '15'

# # A set of regular expressions used in env names and data maps whose
value will be redacted
# termsToRedact: '"pwd", "password", "token", "apikey", "api-key",
"api_key", "jwt", "accesskey", "access_key", "access-key", "ca-file",
"key-file", "cert", "cafile", "keyfile", "tls", "crt", "salt",
".dockerconfigjson", "auth", "secret"'

# # A comma separated list of additional kinds to watch from the
default set of kinds watched by the collector
# # Each kind will have to be prefixed by its apigroup
# # Example: '"authorization.k8s.io.subjectaccessreviews"'
# additionalKindsToWatch: ''

# # A comma separated list of additional field paths whose diff is
ignored as part of change analytics. This list in addition to the default
set of field paths ignored by the collector.
# # Example: '"metadata.specTime", "data.status"'
# additionalFieldsDiffToIgnore: ''

# # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector

```



```

# # Each kind will have to be prefixed by its apigroup
# # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
# kindsToIgnoreFromWatch: ''

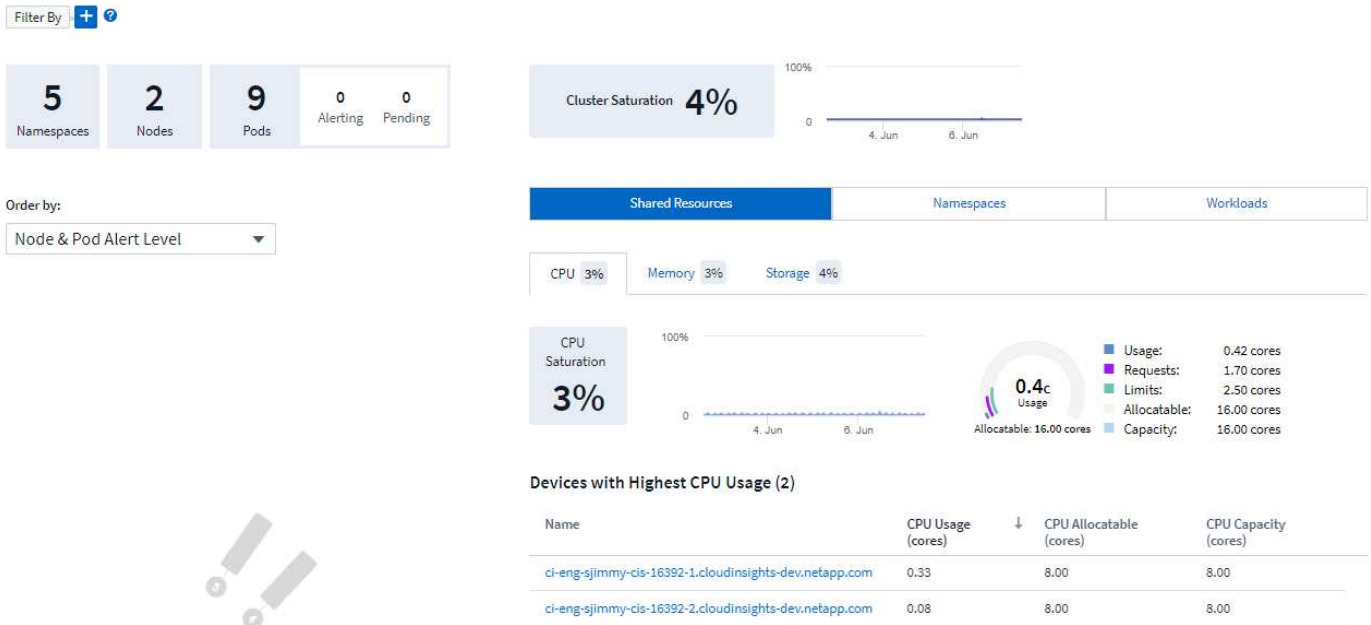
# # Frequency with which log records are sent to CI from the collector
# logRecordAggrIntervalSeconds: '20'

# # change-observer-watch-ds additional tolerations. Use the following
abbreviated single line format only.
# # Inspect change-observer-watch-ds to view tolerations which are
always present.
# # Example: '{key: taint1, operator: Exists, effect:
NoSchedule},{key: taint2, operator: Exists, effect: NoExecute}'
# watch-tolerations: ''

```

## Kubernetes 클러스터 세부 정보 페이지

Kubernetes 클러스터 세부 정보 페이지에는 Kubernetes 클러스터에 대한 자세한 개요가 표시됩니다.



### 네임스페이스, 노드 및 Pod 수

페이지 맨 위의 숫자는 클러스터의 네임스페이스, 노드 및 포드의 총 개수와 현재 경고 및 보류 중인 포드의 수를 보여줍니다.

## 공유 리소스 및 채도

상세 페이지의 오른쪽 위에는 현재 비율로 클러스터 채도가 표시되고, 시간의 경과에 따른 최근 추세를 보여 주는 그래프가 표시됩니다. 클러스터 포화도는 각 시점마다 CPU, 메모리 또는 스토리지 포화도가 가장 높은 것입니다.

그 아래 페이지는 기본적으로 CPU, 메모리 및 스토리지 탭이 있는 \* 공유 리소스 \* 사용을 보여줍니다. 각 탭은 시간에 따른 채도 백분율 및 추세를 추가 사용 세부 정보와 함께 표시합니다. 스토리지의 경우 표시된 값은 독립적으로 계산되는 백엔드 및 파일 시스템 포화도의 값입니다.

사용량이 가장 높은 장치는 하단의 테이블에 표시됩니다. 이 장치를 탐색하려면 아무 링크나 클릭하십시오.

## 네임스페이스

Namespaces 탭에는 Kubernetes 환경의 모든 네임스페이스 목록이 표시됩니다. 이 목록에는 CPU 및 메모리 사용량과 각 네임스페이스의 워크로드 수가 표시됩니다. 이름 링크를 클릭하여 각 네임스페이스를 탐색합니다.

Shared Resources	Namespaces	Workloads	
<b>Namespaces (5)</b>			
Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Workload Count
<a href="#">netapp-monitoring</a>	0.25	0.38	4
<a href="#">kube-system</a>	0.01	0.03	3
<a href="#">kube-public</a>	0.00	0.00	0
<a href="#">kube-node-lease</a>	0.00	0.00	0
<a href="#">default</a>	0.00	<0.01	1

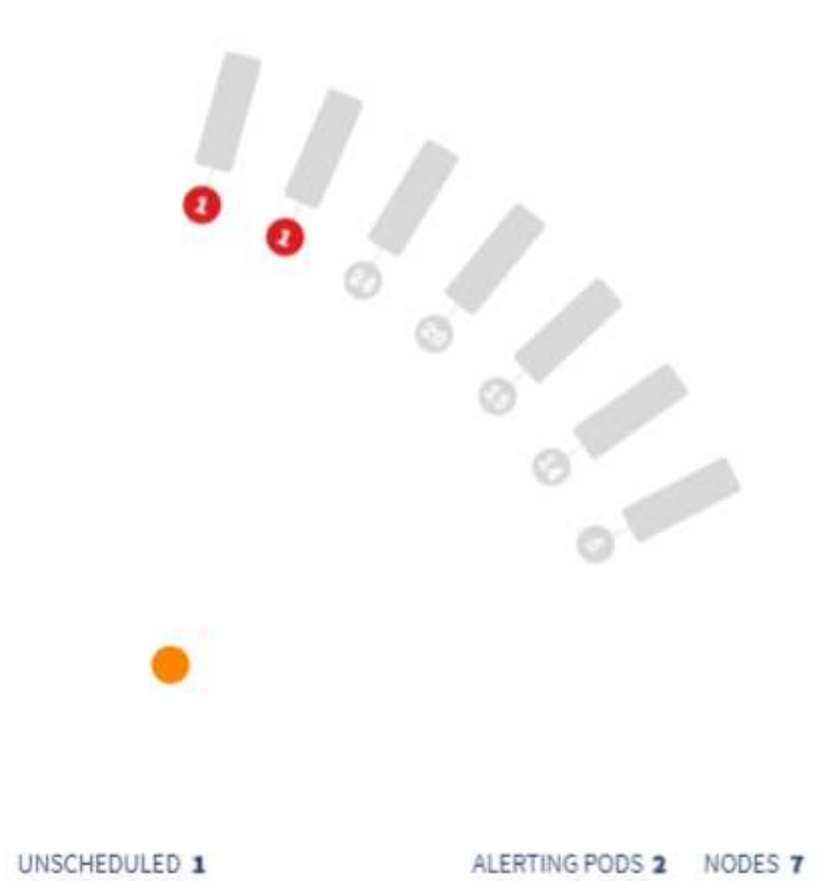
## 워크로드

마찬가지로 워크로드 탭에는 각 네임스페이스의 워크로드 목록이 표시되며 CPU 및 메모리 사용량이 표시됩니다. Namespace 를 클릭하면 각 에 드릴이 연결됩니다.

### Workloads (8)

Name ↓	CPU Usage (cores)	Memory Usage (GiB)	Namespace
telegraf-rs-lf9gg	0.24	0.24	netapp-monitoring
telegraf-ds-k957c	0.01	0.10	netapp-monitoring
nginx	0.00	<0.01	default
monitoring-operator-6fcf4755ff-p2cs6	<0.01	0.02	netapp-monitoring
metrics-server-7b4f8b595-f7j9f	<0.01	0.01	kube-system
local-path-provisioner-64d457c485-289gx	<0.01	0.01	kube-system
kube-state-metrics-7995866f8c-t8c49	<0.01	0.01	netapp-monitoring
coredns-5d69dc75db-nkw5p	<0.01	0.01	kube-system

### 클러스터 "휠"



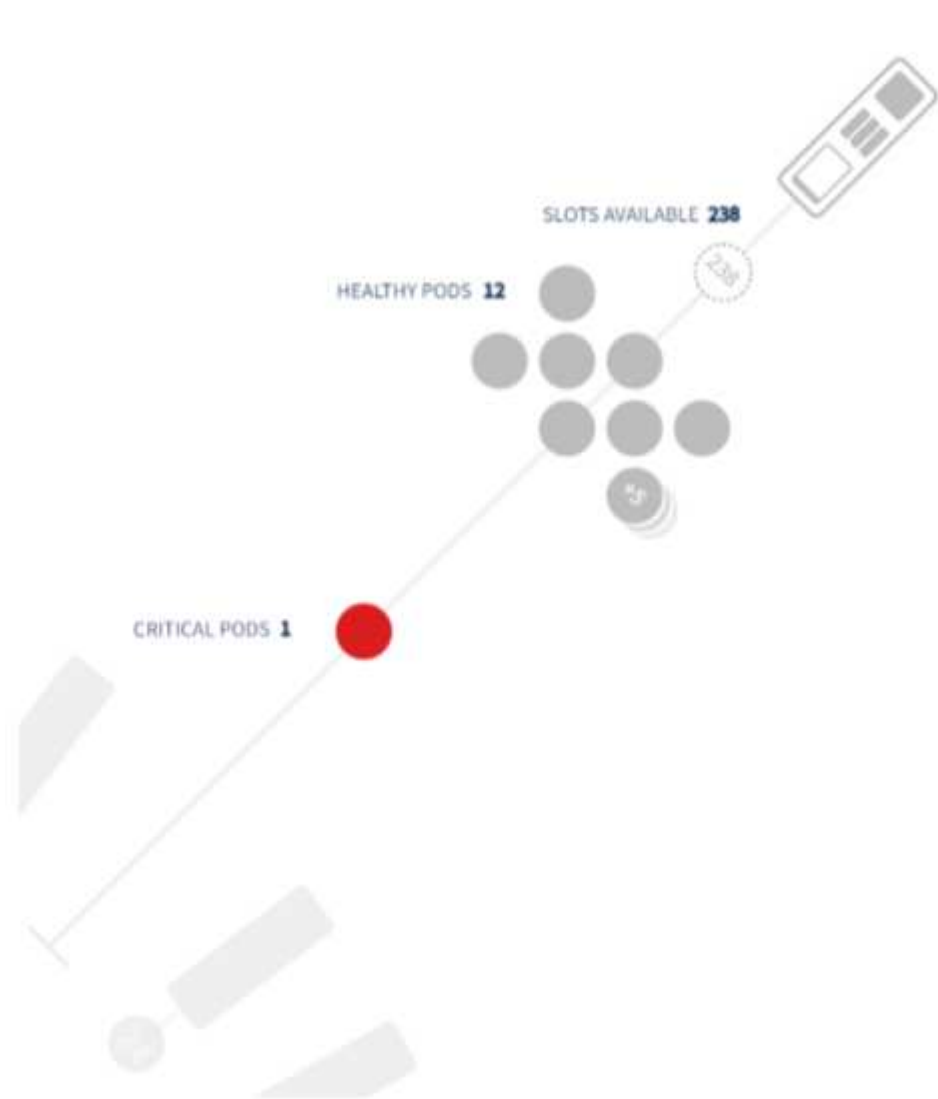
클러스터 "Wheel" 섹션은 노드 및 POD 상태를 한눈에 파악할 수 있도록 하여 자세한 정보를 확인할 수 있습니다. 클러스터에 페이지의 이 영역에 표시할 수 있는 것보다 많은 노드가 포함된 경우 사용 가능한 버튼을 사용하여 휠을 돌릴 수 있습니다.

경고 Pod 또는 노드가 빨간색으로 표시됩니다. "경고" 영역은 주황색으로 표시됩니다. 예약되지 않은(즉, 연결되지 않은) 포드는 클러스터 "휠"의 하단 모서리에 표시됩니다.

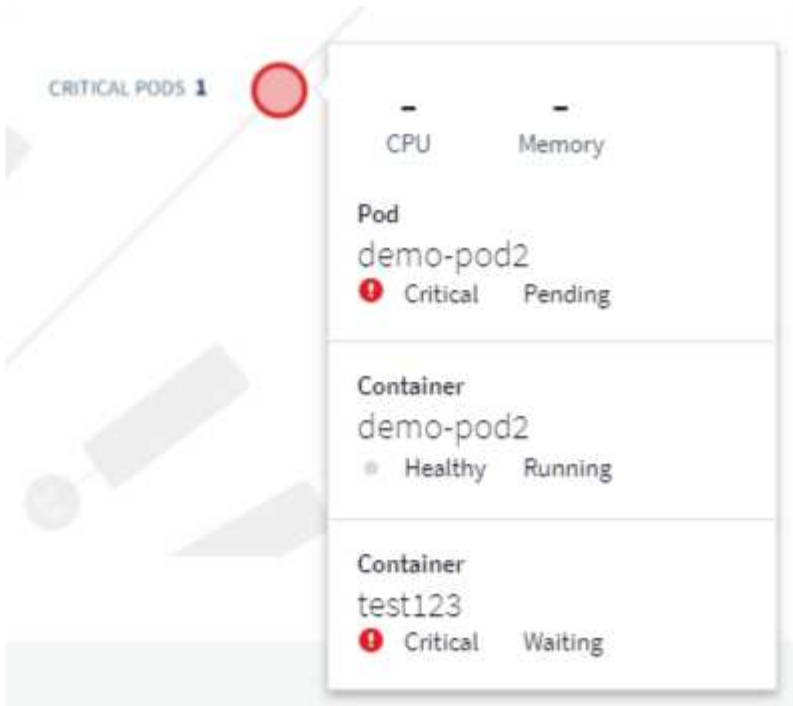
POD(원) 또는 Node(막대) 위로 마우스를 이동하면 노드의 보기가 확장됩니다.



해당 보기에서 Pod 또는 노드를 클릭하면 확장된 노드 보기로 확대됩니다.



여기에서 요소 위로 마우스를 가져가면 해당 요소에 대한 세부 정보가 표시됩니다. 예를 들어, 이 예제에서 중요 POD 위에 마우스를 놓으면 해당 POD에 대한 세부 정보가 표시됩니다.



노드 요소 위로 마우스를 이동하면 파일 시스템, 메모리 및 CPU 정보를 볼 수 있습니다.



### 게이지에 대한 참고 사항

Memory 및 CPU 게이지는 `_allocatable capacity_`와 `_total capacity_`에 대해 `_used_`를 표시하기 때문에 세 가지 색상으로 표시됩니다.

## Kubernetes 네트워크 성능 모니터링 및 맵

Kubernetes 네트워크 성능 모니터링 및 맵 기능은 서비스 간 종속성(워크로드라고도 함)을 매핑하여 문제 해결을 간소화하고 네트워크 성능 지연 시간 및 이상 징후를 실시간으로 확인하여 사용자에게 영향을 미치기 전에 성능 문제를 식별합니다.

이 기능은 조직이 Kubernetes 트래픽 흐름을 분석하고 감사하여 전체 비용을 절감할 수 있도록 도와줍니다.

- 주요 기능: • 워크로드 맵은 Kubernetes 워크로드 종속성 및 흐름을 제공하고 네트워크 및 성능 문제를 강조합니다. • Kubernetes Pod, 워크로드 및 노드 간의 네트워크 트래픽을 모니터링하고, 트래픽 및 지연 문제의 원인을 식별합니다. • 수신, 송신, 지역 간 및 교차 영역 네트워크 트래픽을 분석하여 전체 비용을 절감합니다.

## 필수 구성 요소

Kubernetes Network Performance Monitoring and Map을 사용하려면 먼저 을 구성해야 합니다 "NetApp Kubernetes 모니터링 운영자" 를 눌러 이 옵션을 활성화합니다. 오퍼레이터 배포 중에 "네트워크 성능 및 맵" 확인란을 선택하여 활성화합니다. Kubernetes 랜딩 페이지로 이동하여 "배포 수정"을 선택하여 이 옵션을 활성화할 수도 있습니다.



### Configure Data Acquisition

Review Kubernetes cluster information and choose additional data to collect.

#### Cluster Information

Kubernetes Cluster stream8	Network Performance and Map Disabled	Events Log Disabled
-------------------------------	---	------------------------

#### Deployment Options

[Need Help?](#)

- Network Performance and Map
- Events Log

Complete Setup

## 모니터

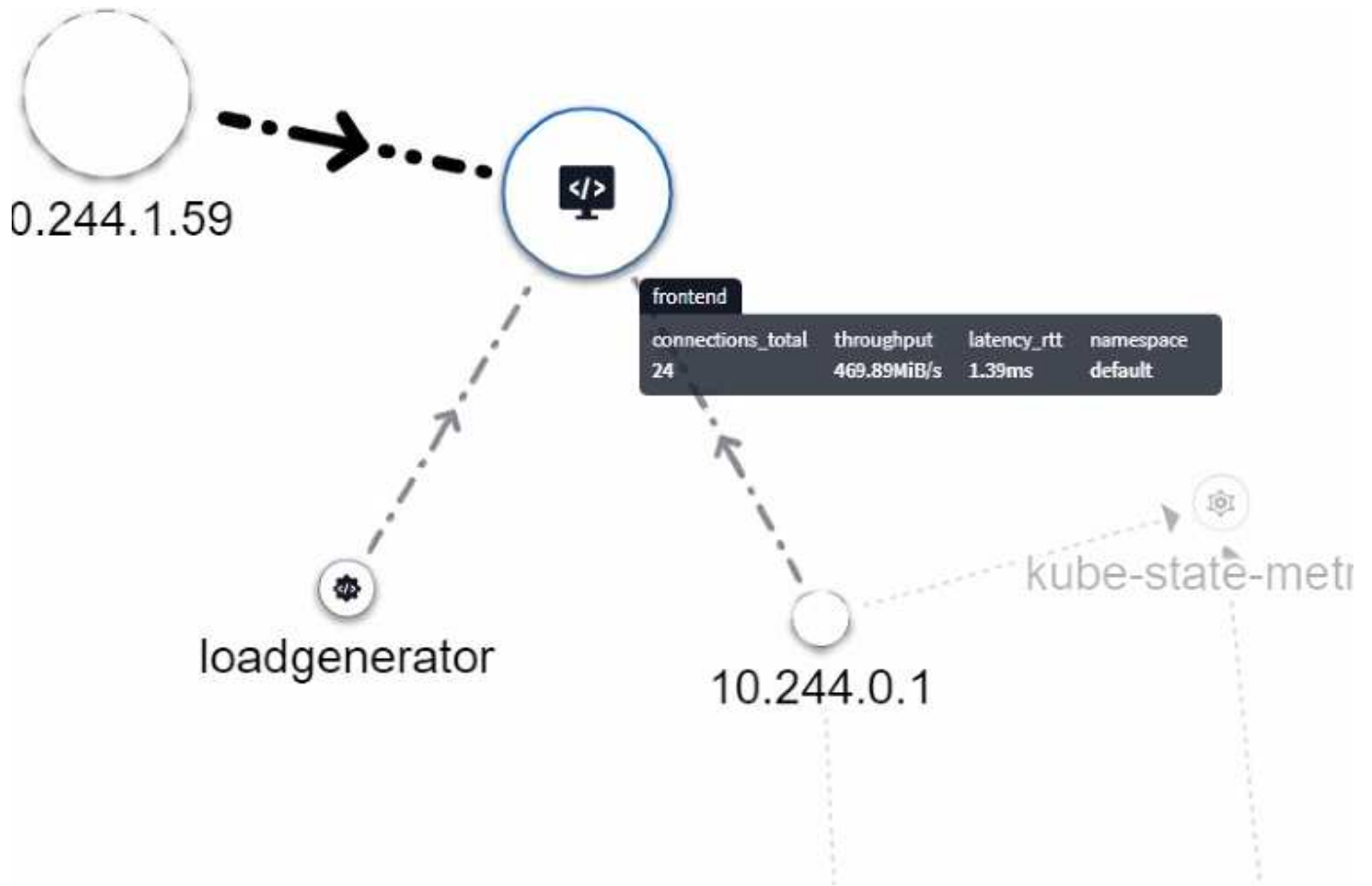
워크로드 맵을 사용하여 "모니터"정보를 파생시킵니다. Data Infrastructure Insights는 다양한 기본 Kubernetes Monitor를 제공합니다(이는 기본적으로 `_ Paused _`일 수 있습니다. 원하는 모니터를 *Resume*(예: 활성화)하거나, Kubernetes 객체에 대한 사용자 지정 모니터를 생성할 수 있습니다. 이 경우 워크로드 맵도 사용됩니다.

아래의 모든 오브젝트 유형에 대해 Data Infrastructure Insights 메트릭 경고를 생성할 수 있습니다. 데이터가 기본 개체 유형별로 그룹화되어 있는지 확인합니다.

- Kubernetes 워크로드
- Kubernetes 발병
- kubernetes.deployment
- 쿠버네티스.crontjob을 제공합니다
- Kubernetes, 작업
- 복제 복제
- Kubernetes.statefulset입니다
- 선택하십시오
- kubernetes.network\_traffic\_l4

## 지도

지도에는 서비스/작업 부하 및 상호 관계가 표시됩니다. 화살표는 교통 방향을 표시합니다. 작업 부하 위로 마우스를 가져가면 다음 예에서와 같이 해당 작업 부하에 대한 요약 정보가 표시됩니다.



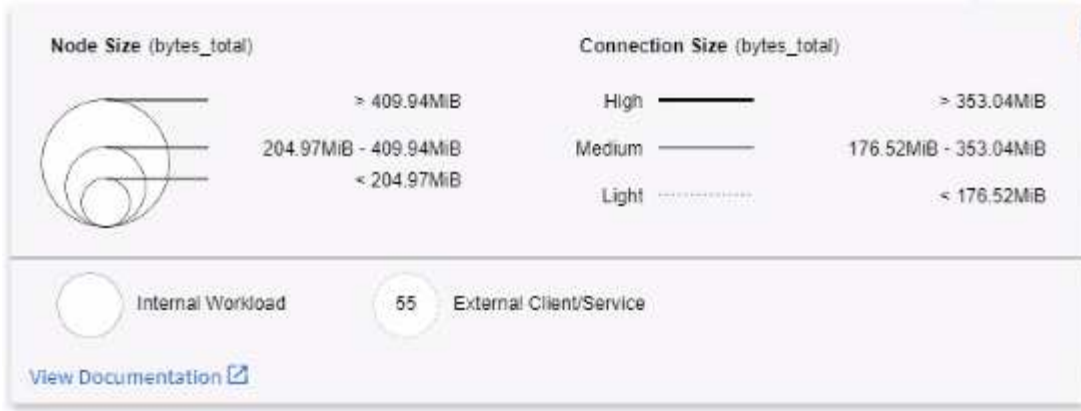
원 안에 있는 아이콘은 다양한 서비스 유형을 나타냅니다. 아이콘은 기본 개체에 있는 경우에만 표시됩니다 [라벨](#).



각 원의 크기는 노드 크기를 나타냅니다. 이러한 크기는 상대적이며 브라우저 확대/축소 수준 또는 화면 크기가 실제 원형 크기에 영향을 줄 수 있습니다. 같은 방법으로, 트래픽 회선 스타일은 연결 크기를 한 눈에 볼 수 있게 합니다. 굵은 실선은 트래픽이 높고 밝은 점선은 트래픽이 적습니다.

원 안에 있는 숫자는 서비스에서 현재 처리 중인 외부 연결의 수입입니다.





## 워크로드 세부 정보 및 알림

색상으로 표시된 원은 워크로드에 대한 경고 또는 위험 수준 경고를 나타냅니다. 원 위로 마우스를 가져가면 문제 요약이 표시됩니다. 원을 클릭하여 자세히 표시된 슬라이드 아웃 패널을 엽니다.

The screenshot displays the NetApp Cloud Insights interface. On the left is a navigation sidebar with options like Home, Dashboards, Queries, Alerts, and Reports. The main area shows a 'Workload Map' with a network diagram of services including 'netapp-fitness-store-01-locust', 'coredns', 'point-of-sale', 'payment', 'frontend', 'order', 'users', 'order-postgres', 'users-redis', 'cart', and 'users-mongo'. A 'payment' workload is highlighted with a red circle. On the right, a 'payment' workload details panel is open, showing 'Summary', 'Network', and 'Pods & Storage' tabs. The 'Alerts Detected (2)' section shows two warnings:

alertid	triggeredTime	currentSeverity	monitor	triggeredOn	activeStatus
AL-683	5 days ago Apr 5, 2023 7:57 AM	Resolved	Workload Network Latency-RTT High (Outdated)	Src_Cluster: ci-demo-01 Src_Namespace: netapp-fitness-store-01 Src_Workload_Name: payment Src_Workload_Kind: Deployment	Resolved
AL-630	7 days ago Apr 3, 2023 10:26 AM	Resolved	Workload Network Latency-RTT High (Outdated)	Src_Cluster: ci-demo-01	Resolved

Below the alerts is a 'Network Traffic' section with a bar chart showing connections and throughput.

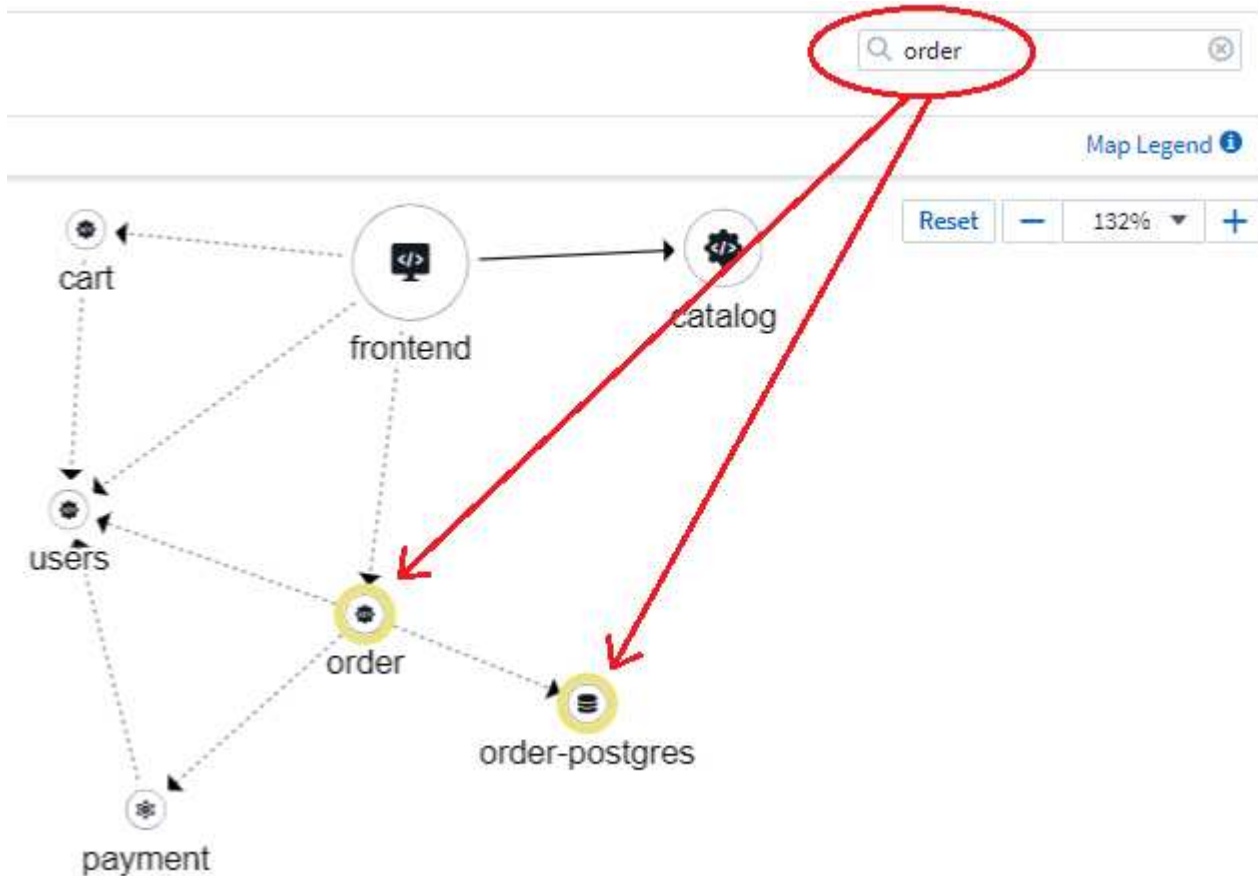
## 찾기 및 필터링

다른 Data Infrastructure Insights 기능과 마찬가지로 필터를 쉽게 설정하여 원하는 특정 오브젝트 또는 워크로드 특성에 집중할 수 있습니다.

Filter By: cluster All scope\_cluster All

Node Size: bytes\_total Connection Size: bytes\_total

마찬가지로 *Find* 필드에 문자열을 입력하면 일치하는 워크로드가 강조 표시됩니다.



## 워크로드 레이블

지도에서 표시되는 워크로드 유형(예: 원 아이콘)을 식별하려면 워크로드 레이블이 필요합니다. 레이블은 다음과 같이 파생됩니다.

- 일반 용어로 실행 중인 서비스/애플리케이션의 이름입니다
- 소스가 POD인 경우:
  - 레이블은 POD의 워크로드 레이블에서 파생됩니다
  - 작업 부하에 대한 예상 레이블: `app.Kubernetes.io/component`
  - 라벨 이름 참조: <https://kubernetes.io/docs/concepts/overview/working-with-objects/common-labels/>
  - 권장 라벨:
    - 프론트 엔드

- 백엔드
- 데이터베이스
- 캐시
- 대기열
- 카프카

• 소스가 Kubernetes 클러스터 외부에 있는 경우:

- Data Infrastructure Insights는 DNS 확인된 이름을 구문 분석하여 서비스 유형을 추출합니다.

예를 들어, DNS Resolved 이름이 `_s3.eu-north-1.amazonaws.com` 인 경우 Resolved 이름은 서비스 유형으로 `get_s3_`로 구문 분석됩니다.

## 깊이 잠들어 보세요

워크로드를 마우스 오른쪽 버튼으로 클릭하면 더 자세히 살펴볼 수 있는 추가 옵션이 제공됩니다. 예를 들어, 여기에서 해당 워크로드의 연결을 확대하여 볼 수 있습니다.



또는 세부 정보 슬라이드 아웃 패널을 열어 *Summary*, *Network* 또는 *Pod & Storage* 탭을 직접 볼 수 있습니다.



Summary	<b>Network</b>	Pods & Storage
---------	----------------	----------------

Network Activities - Inbound (1) 

src_workload...	src_namespace	src_workload_...	throughpu... ↓	connections_t...	latency_rtt (ms)	tcp_retransmit...
netapp-fitness...	locust	Deployment	14,193,748.78	653.19	3.74	2,578.00

Network Activities - Outbound (4) 

dst_workloa...	dst_namespace	dst_workload_...	throughpu... ↓	connections_t...	latency_rtt (ms)	tcp_retransmit...
catalog	netapp-fitness-...	Deployment	14,166,417.02	2,425.07	149.37	13,850.00
cart	netapp-fitness-...	Deployment	12,479.90	638.97	65.10	0.00
order	netapp-fitness-...	Deployment	4,515.16	161.84	65.07	0.00

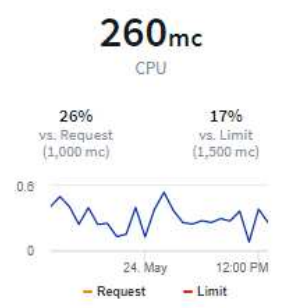
마지막으로, \_자산 페이지로 이동 \_을(를) 선택하면 워크로드에 대한 상세 자산 랜딩 페이지가 열립니다.

Filter By + ?

**2/2**  
Pods: Current / Desired

2 Up-to-date    0 Unavailable

Namespace <b>netapp-fitness-store-01</b>	Type <b>Deployment</b>	Date Created <b>Apr 11, 2023 11:34 AM</b>
Labels -		



Highest CPU Demand by Pod

- 132.76m frontend-7...9f8f-284kb
- 127.55m frontend-7...9f8f-gd8mk



Highest Memory Demand by Pod

- 0.09 GiB frontend-7...9f8f-284kb
- 0.09 GiB frontend-7...9f8f-gd8mk

**0.00GiB**  
Total PVC Capacity claimed

Pods (2)

Pod Name ↑	Status	Healthy Containers	cpu_usage_nanocores (mc)	memory_rss_bytes (GiB)
frontend-7fccd9f8f-284kb	● Healthy Running	1 of 1	133	0.09
frontend-7fccd9f8f-gd8mk	● Healthy Running	1 of 1	128	0.09

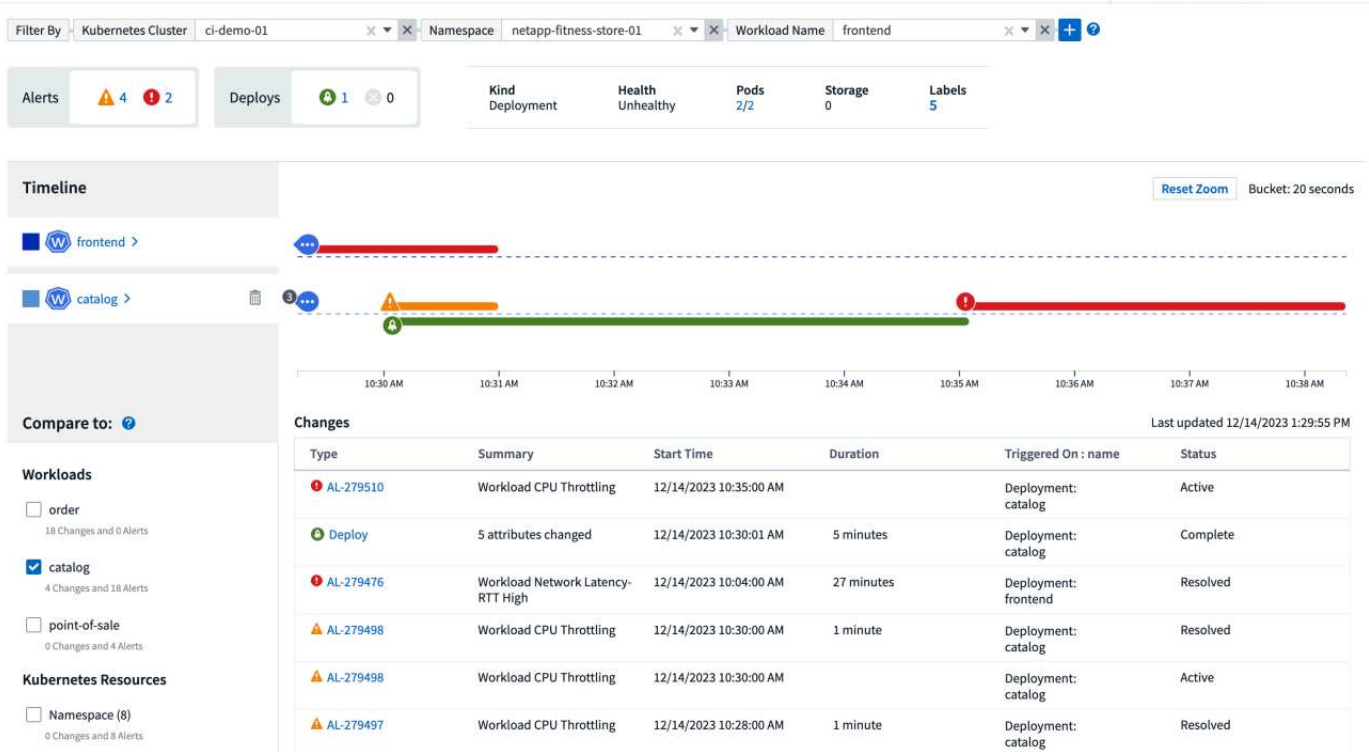
## Kubernetes 변경 분석

Kubernetes Change Analytics는 Kubernetes 환경의 최근 변경에 대한 올인원 뷰를 제공합니다. 알림 및 배포 상태를 즉시 확인할 수 있습니다. 변경 분석을 사용하여 모든 배포 및 구성 변경을 추적하고 Kubernetes 서비스, 인프라 및 클러스터의 상태 및 성능과 상호 연관시킬 수 있습니다.

변경 분석은 어떻게 도움이 됩니까?

- 멀티 테넌트 Kubernetes 환경에서는 잘못 구성된 변경으로 인해 중단이 발생할 수 있습니다. Change Analytics는 워크로드 상태와 구성 변경의 상태를 보고 상호 연관시킬 수 있는 단일 창을 제공하여 이러한 작업을 지원합니다. 이는 동적 Kubernetes 환경 문제를 해결하는 데 도움이 될 수 있습니다.

Kubernetes 변경 분석을 보려면 \* Kubernetes > 변경 분석 \* 으로 이동하십시오.



현재 선택한 Data Infrastructure Insights 시간 범위에 따라 페이지가 자동으로 새로 고쳐집니다. 시간 범위가 작을수록 화면 새로 고침이 더 자주 발생합니다.

## 필터링

Data Infrastructure Insights의 모든 기능과 마찬가지로 변경 목록을 필터링하는 것도 직관적입니다. 페이지 상단에서 Kubernetes 클러스터, 네임스페이스 또는 워크로드의 값을 입력하거나 선택하거나 [+] 버튼을 선택하여 자체 필터를 추가할 수 있습니다.

특정 클러스터, 네임스페이스 및 워크로드(사용자가 설정한 다른 필터 포함)로 필터링하면 해당 클러스터의 해당 네임스페이스에 있는 해당 워크로드에 대한 배포 타임라인과 경고가 표시됩니다. 그래프를 클릭하고 끌어서 보다 구체적인 시간 범위에 초점을 맞춰 확대합니다.

Filter By: Kubernetes Cluster stream-54 | Namespace: kube-system | Workload Name: coredns

Alerts: 0 Warning, 8 Critical | Deploys: 0 Success, 0 Failed

Kind: Deployment | Health: Healthy | Pods: 1/1 | Storage: 0 | Labels: 3

Timeline: Bucket: 6 minutes

Timeline visualization showing alerts for 'coredns' workload.

Changes table (Last updated 11/28/2023 3:17:05 PM):

Type	Summary	Start Time	Duration	Triggered On : name	Status
AL-2982989	once Workload Down copy	11/28/2023 3:07:00 PM	1 minute	Deployment: coredns	Resolved
AL-2982989	once Workload Down copy	11/28/2023 3:07:00 PM		Deployment: coredns	Active
AL-2982887	once Workload Down copy	11/28/2023 3:01:00 PM	1 minute	Deployment: coredns	Resolved
AL-2982887	once Workload Down copy	11/28/2023 3:01:00 PM		Deployment: coredns	Active
AL-2982782	once Workload Down copy	11/28/2023 2:57:00 PM	0 milliseconds	Deployment: coredns	Resolved
AL-2982782	once Workload Down copy	11/28/2023 2:57:00 PM		Deployment: coredns	Active
AL-2982441	once Workload Down copy	11/28/2023 2:32:00 PM	1 minute	Deployment: coredns	Resolved
AL-2982441	once Workload Down copy	11/28/2023 2:32:00 PM		Deployment: coredns	Active

## 빠른 상태

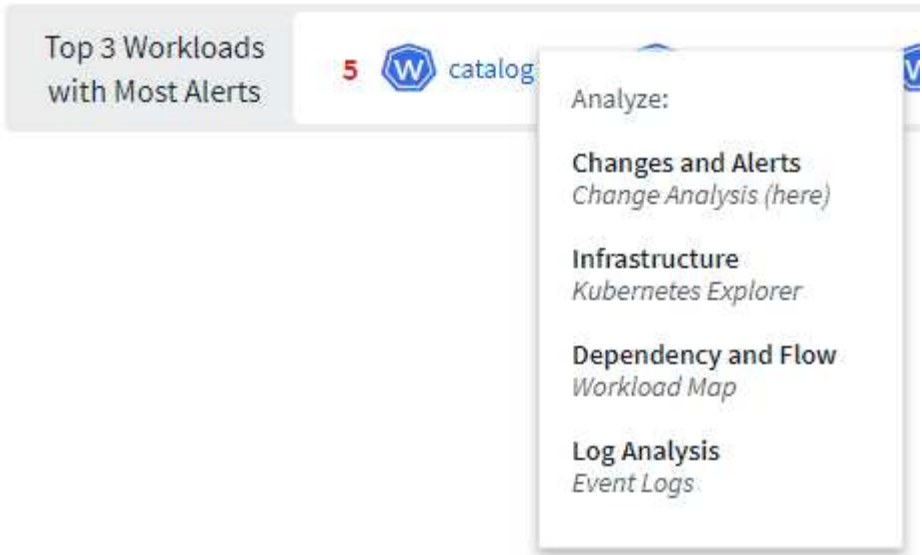
필터링 영역 아래에는 여러 개의 상위 수준 표시기가 있습니다. 왼쪽에는 경고(Warning) 및 위험(Critical)의 수가 표시됩니다. 이 수에는 `_Active_` 와 `_Resolved_alerts_` 가 포함됩니다. Active\_alerts만 보려면 "Status"에 대한 필터를 설정하고 "Active"를 선택합니다.

Alerts: 6 Warning, 17 Critical

배포 상태도 여기에 표시됩니다. 기본적으로 `Started, Complete` 및 `_Failed_deployments_`의 개수가 표시됩니다. Only\_Failed\_Deployments를 보려면 "Status"에 필터를 설정하고 "Failed"를 선택합니다.

Deploys: 36 Success, 4 Failed

다음 워크로드로는 경고가 가장 많은 상위 3개 워크로드가 있습니다. 각 워크로드 옆의 빨간색 숫자는 해당 워크로드와 관련된 알람 수를 나타냅니다. 워크로드 링크를 클릭하여 인프라(Kubernetes Explorer), 종속성(워크로드 맵) 또는 로그 분석(이벤트 로그)을 탐색합니다.



### 세부 정보 패널

목록에서 변경을 선택하면 변경 사항을 자세히 설명하는 패널이 열립니다. 예를 들어 실패한 배포를 선택하면 배포 요약, 시작 및 종료 시간, 기간, 배포가 트리거된 위치, 해당 리소스를 탐색할 수 있는 링크가 표시됩니다. 또한 실패 이유, 관련 변경 사항 및 관련 이벤트도 표시합니다.



## Deploy Failed



### Summary

#### Start Time

10/18/2023 2:40:01 PM

#### End Time

10/18/2023 2:50:02 PM

#### Duration

10 minutes

#### Triggered On

 ci-demo-01 >

 netapp-fitness-store-01 >

 billing-accounts >

#### Triggered On : kind

Deployment

### Failure Detail

#### Reason For Failure

ProgressDeadlineExceeded - ReplicaSet "billing-accounts-6ddc7df546" has timed out progressing.

#### Message

Failed deploy

### Changes (2)

Attribute Name	Previous	New
spec.template.spec.containers[0].image	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.0	210811600188.dkr.ecr.us-east-1.amazonaws.com/sm-billing-accounts-apis:1.0.09
metadata.annotations.deployment.kubernetes.io/revision	2964	2965

[All Changes Diff](#)

### Associated Events

[Event Logs](#)

Close

마찬가지로 경고를 선택하면 경고를 트리거한 모니터와 경고에 대한 시각적 타임라인을 보여 주는 차트를 비롯하여 알림에 대한 세부 정보가 제공됩니다.

# ONTAP 핵심 요소

ONTAP Essentials는 ONTAP 인벤토리 및 워크로드를 상세하게 보여주는 대시보드 및 워크플로 집합입니다. ONTAP Essentials에서 작업할 때 사용되는 용어는 다음과 같습니다.

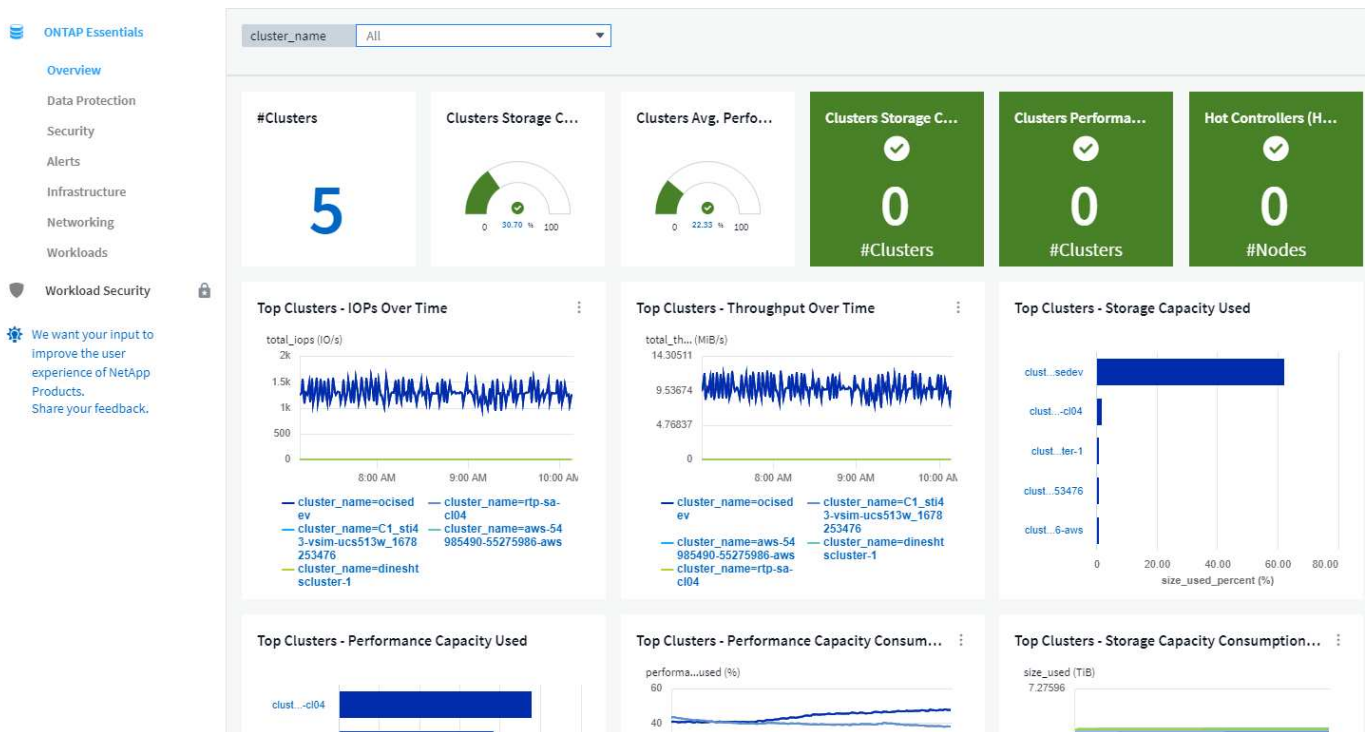
- 인프라/인벤토리: 사용자 데이터에 스토리지/네트워킹 서비스를 제공하는 객체입니다
- 워크로드: 사용자가 데이터를 읽고 쓸 수 있도록 인터페이스를 제공하는 객체입니다.
- 데이터 보호: NetApp 데이터 보호 기술을 사용하여 보호할 수 있는 오브젝트

ONTAP와 관련된 추가 용어와 정의를 를 참조하십시오 ["ONTAP 데이터 수집기"](#) 문서화:

ONTAP Essentials를 사용하려면 지난 7일 이내에 수집된 데이터를 포함하는 ONTAP 데이터 수집기 중 최소한 한 명이 있어야 합니다.

## 개요

탐색을 시작하려면 기본 데이터 인프라 인사이트 메뉴에서 \* ONTAP 필수 \* 를 선택합니다.



개요 \* 대시보드에는 전체 용량 및 성능 백분율과 함께 사용자 환경의 클러스터 수와 같은 유용한 정보가 표시됩니다. 또한 스토리지 용량 또는 성능 용량이 공간 부족해질 때까지 예상 일 수에 대한 예측 데이터도 볼 수 있습니다. 또한, 인프라에서 CPU가 65% 이상인 컨트롤러가 실행 중이면 파일오버가 발생할 가능성이 있는 클러스터 상황에 놓입니다. ONTAP Essentials는 이러한 컨트롤러를 "핫" 컨트롤러로 표시합니다.

정보 그래프를 통해 시간 경과에 따른 성능 및 용량 사용량 분석 정보를 확인할 수 있습니다. 이러한 각 그래프 또는 데이터 요소를 탐색 또는 조사의 시작 지점으로 사용할 수 있습니다.

참고: "일 대 전체" 숫자 "0"(영)은 전체 일 수가 90일 이상 예상됨을 나타냅니다. 즉, 시스템이 곧 공간이 부족해질 위험이 없습니다.

# 데이터 보호

데이터 보호 \* 페이지는 \* 스냅샷 복사본 \* 또는 \* SnapMirror 정책 \* 으로 보호되는 볼륨의 상태를 표시합니다.

Local Protection Overview \_ 섹션에서 이 차트는 스냅샷 복사본으로 보호되는 볼륨에 대한 다음 정보를 제공합니다.

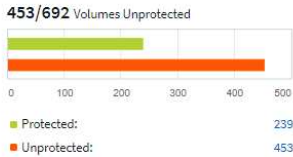
- 보호되지 않는 볼륨뿐만 아니라 스냅샷 복사본으로 보호되는 볼륨의 수입입니다.
- 스냅샷 복사본에 대해 예약 공간을 사용 중이거나 초과하는 볼륨 수입입니다.
- 특정 범위의 스냅샷 복사본 수(예: 10개 미만의 복사본, 10개~200개 등)

원격 보호 개요 \_ 섹션에서 차트에는 SnapMirror 정책으로 보호되는 볼륨과 관련된 정보가 나와 있습니다.

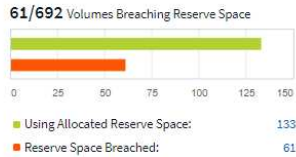
- 정상 상태가 아닌 SnapMirror 관계 수입입니다.
- 지연 상태에 따라 RPO(복구 지점 목표)가 지연되는 SnapMirror 관계 수
- 볼륨 SnapMirror, SVM 관계, FlexGroup SnapMirror 관계, SMBC(SnapMirror Business Continuity) 일관성 그룹 관계, 보호되지 않는 볼륨 등과 같이 SnapMirror 볼륨 보호 유형으로 보호되는 관계 수입입니다.
- 비동기 미러, 비동기 볼트, 비동기 MirrorVault, StrictSync 및 Sync와 같은 SnapMirror 관계 유형으로 보호되는 관계 수입입니다.

## Local Protection Overview

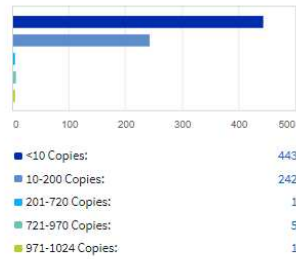
### Snapshot Volume Protection



### Snapshot Reserve Space

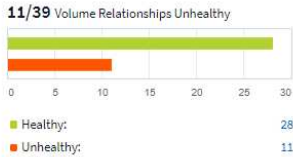


### Snapshot Copy Count

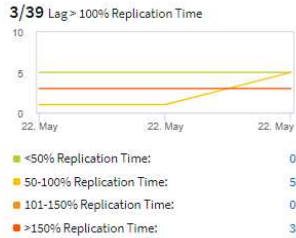


## Remote Protection Overview

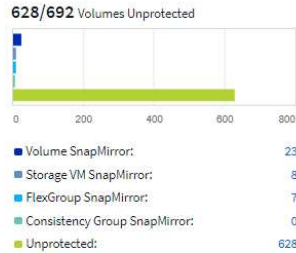
### Unhealthy SnapMirror Relationships



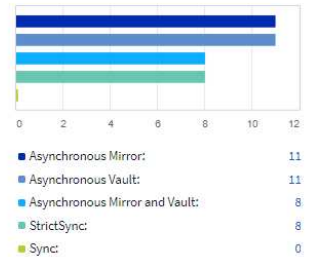
### SnapMirror Volume Lag



### SnapMirror Volume Protection



### SnapMirror Relationship Types



페이지 하단의 \_Clusters\_GRID에서는 다음과 관련된 세부 정보를 제공합니다.

- 스냅샷으로 보호되지 않는 볼륨입니다.
- 볼륨이 스냅샷 예비 공간을 침범합니다.
- SnapMirror 정책으로 보호되지 않는 볼륨 및 지연을 경험하는 SnapMirror 관계
- 비정상적인 SnapMirror 관계:

Clusters (6)

Cluster	Volumes Not Protected by Snapshots ↓	Volumes Breaching Snapshot Reserve Space	Volumes Not Protected by SnapMirror	SnapMirror Relationships Experiencing Lag	Unhealthy SnapMirror Relationships
rtp-sa-cl01	304	1	393	0	1
umeng-aff300-01-02	123	20	160	1	3
annapook-vsimg12	7	4	7	0	3
C1_sti11-vsimg-ucs574m_168321	0	0	0	0	0
C1_sti43-vsimg-ucs513w_167825	0	0	0	0	0
ci-cs-fas8060-01-02	0	0	0	0	0

## 보안

보안 대시보드에서는 하드웨어 및 소프트웨어 볼륨 암호화, 랜섬웨어 방지 상태 및 클러스터 인증 방법에 대한 차트를 보여 주는 현재 보안 상황을 즉시 확인할 수 있습니다. 보안 기준은 에 정의된 권장 사항을 기반으로 평가됩니다 "ONTAP 9 \* 에 대한 \* NetApp 보안 강화 가이드".

암호화 또는 랜섬웨어 차단 수치 중 하나를 선택하여 환경에 대해 자세히 알아볼 수 있습니다.

ONTAP Essentials

- Overview
- Data Protection
- Security
- Alerts
- Infrastructure
- Networking
- Workloads
- Workload Security 🔒

We want your input to improve the user experience of NetApp Products. Share your feedback.

**Volume Encryption**

7/119 Encrypted

**SVM Anti-Ransomware Status**

6/20 Enabled

Protect with Cloud Insights Workload Security

**Cluster Authentication Methods**

Authentication Methods		Certificates
0	2	0
2	5	1

**Clusters (5)**

Cluster	Compliance	Volume Encryption (%)	Protected by ONTAP ARP (%)	Protected by Workload Sec...	Details
aws-54985490-55275986-aws	⚠️ Not Compliant	0.00	0.00	0.00	<a href="#">🔗</a>
ocisedev	⚠️ Not Compliant	0.00	0.00	40.00	<a href="#">🔗</a>
rtp-sa-cl04	⚠️ Not Compliant	0.00	0.00	0.00	<a href="#">🔗</a>
C1_sti43-vsimg-ucs513w_1678253476	✅ Compliant	77.78	50.00	0.00	<a href="#">🔗</a>
dineshtscluster-1	✅ Compliant	0.00	0.00	0.00	<a href="#">🔗</a>






[View Security Hardening Guide](#) 📄

ONTAP Essentials 보안 대시보드는 환경을 모니터링하여 클러스터 규정 준수 상태를 확인합니다. 을 참조하십시오 "클러스터 규정 준수 범주" 을 참조하십시오. ONTAP Essentials는 다음 모니터를 사용하여 준수 여부를 결정합니다.

모니터 이름	특성 이름(클러스터 세부 정보에 표시됨)	특성 규정 준수 값
FIPS 모드가 비활성화되었습니다	FIPS 모드	활성화됨
SSH에 대한 클러스터 비보안 암호	보안 SSH 설정	예
텔넷 프로토콜 사용	텔넷	사용 안 함
원격 셸 사용	원격 셸	사용 안 함
기본 로컬 관리자 사용	기본 관리자 사용자입니다	사용 안 함
MD5 해시 암호입니다	MD5가 사용 중입니다	아니요

모니터 이름	특성 이름(클러스터 세부 정보에 표시됨)	특성 규정 준수 값
클러스터 피어 통신이 암호화되지 않았습니다	클러스터 피어링	암호화/피어 없음
AutoSupport HTTPS 전송이 비활성화되었습니다	HTTPS를 사용하는 AutoSupport	예
NTP 서버가 구성되지 않았습니다	Network Time Protocol의 약어입니다	구성됨
NTP 서버 수가 부족합니다	Network Time Protocol의 약어입니다	구성됨
클러스터 로그인 배너 비활성화됨	로그인 배너	활성화됨
로그 전달이 암호화되지 않았습니다	로그 전달이 암호화되었습니다	예

위의 모니터가 비활성화된 경우 클러스터 세부 정보에는 해당 보안 규정 준수 속성에 대한 값이 '선택되지 않음'으로 표시됩니다.

Cluster	Compliance
<a href="#">aws-54985490-55275986-aws</a>	 Not Compliant
<a href="#">ocisedev</a>	 Not Compliant
<a href="#">rtp-sa-cl04</a>	 Not Compliant
<a href="#">C1_sti43-vsimm-ucs513w_1678253476</a>	 Compliant
<a href="#">dineshtscluster-1</a>	 Compliant

SVM의 경우 보안 대시보드에서 다음 모니터를 확인합니다.


모니터 이름	속성 이름(스토리지 VM 설정에 표시됨)	특성 규정 준수 값
SSH에 대한 스토리지 VM 보안 암호가 안전하지 않습니다	보안 SSH 설정	예
스토리지 VM 로그인 배너가 비활성화되었습니다	로그인 배너	활성화됨
스토리지 VM 감사 로그가 비활성화되었습니다	감사 로그	활성화됨


클러스터 목록에서 각 클러스터에 대해 *View Details*를 선택하여 *\_Cluster*, *Storage VM*, 또는 *\_Anti-랜섬웨어\_*에 대한 현재 설정을 보여주는 "slideout" 패널을 엽니다.

클러스터 세부 정보에는 연결 상태, 인증서 정보 등이 포함됩니다
















Cluster Name:  C1\_sti43-vsimsim-ucs513w\_1678253476



Cluster Settings 

Storage VM Settings 






















Storage VM Anti-Ransomware 

Settings	Status
FIPS mode	 Disabled
Secure SSH Settings	 Not Checked
Telnet	 Disabled
Remote Shell	 Disabled
Default Admin User	 Enabled
MD5 in use	 No
Cluster Peering	 No Peer
AutoSupport using HTTPS	 Yes
Network Time Protocol	 Only 1 server is configured
Login Banner	 Not Checked
Log Forwarding Encrypted	N/A
Valid Cluster Certificate	 Yes
Certificate Issuer Type	 Self-Signed
SAML Users Configured	 No
LDAP Users Configured	 Yes
Active Directory Users Configured	 Yes

Close

스토리지 VM 세부 정보에는 감사 및 SSH 정보가 표시됩니다

Cluster Name:  rtp-sa-cl04

Cluster Settings 	Storage VM Settings 	Storage VM Anti-Ransomware 	
Storage VM	Login Banner	Audit Log	Secure SSH Settings
mattsvm07_04	 Disabled	N/A	 Yes
sf-svmdr1	 Disabled	N/A	 Yes
ss_balajicifs	 Disabled	N/A	 Yes
ss_balajicifs_1_encrypted	 Disabled	N/A	 Yes
test1	 Enabled	 Disabled	 Yes
test2	 Disabled	N/A	 Yes
test3	 Disabled	N/A	 Yes
cl04_data_svm1	 Enabled	 Enabled	 Yes

안티 랜섬웨어 세부 정보는 스토리지 VM이 ONTAP의 랜섬웨어 방지 보호 또는 데이터 인프라 인사이트 워크로드 보안으로 보호되는지 여부를 보여줍니다. ONTAP ARP 열은 ONTAP 시스템에 구성된 ONTAP의 온보드 Anti-랜섬웨어 방지 프로그램의 현재 상태를 표시합니다. Data Infrastructure Insights 워크로드 보안은 해당 열에서 "보호"를 선택하여 활성화할 수 있습니다.

Cluster Name:  ocisedev



Cluster Settings 	Storage VM Settings 	Storage VM Anti-Ransomware 
Storage VM	Protected by Workload Security	Protected by ONTAP ARP
CloudComplianceSVM	<input type="button" value="Protect"/>	N/A
t1appSVM01	<input type="button" value="Protect"/>	N/A
tawny_mirror	<input type="button" value="Protect"/>	N/A
demoGroupShares	 Protected	N/A
demoGroupShares2 	 Protected	N/A

## 경고

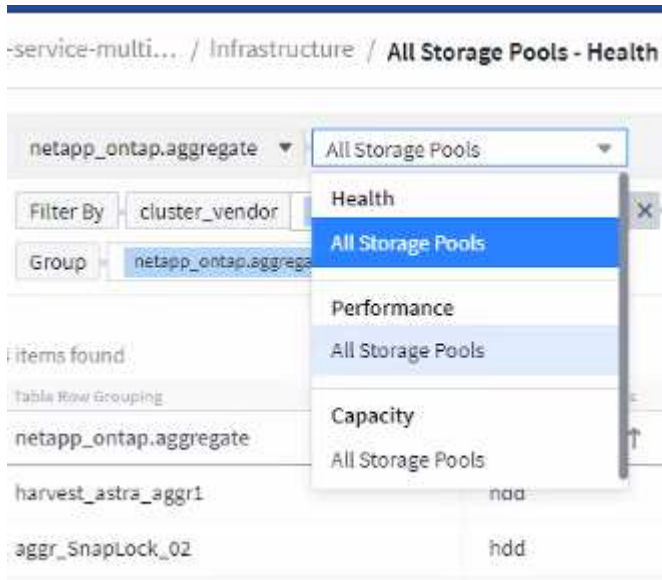
이 곳에서 사용자 환경의 활성 알림을 확인하고 잠재적인 문제를 신속하게 파악할 수 있습니다. 해결된 알림을 보려면 `_Resolved_` 탭을 선택합니다.



Filter By	triggeredOn	cluster_vendor: NetApp	status	New	In process	currentSeverity	Warning	Critical
<b>Alerts (28)</b> <span style="float: right;">Change All Alerts Status</span>								
alertId	triggeredTime	currentSeverity	monitor	triggeredOn	status	hasCorrective Actions		
AL-169	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO NTP Server Count is ...	cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_model: CDvM200	New	✓		
AL-172	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO Default Local Admin ...	cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_model: CDvM200	New	✓		
AL-168	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO Storage VM Login Ba...	cluster_model: CDvM200 cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e vserver_uuid: 08f5ffb0-be52-11ed-9476-eb015bbf1f0e vserver_name: vs0	New	✓		
AL-171	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO Cluster Login Banner...	cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_model: CDvM200	New	✓		
AL-170	3 hours ago Mar 9, 2023 7:12 AM	Warning	CVO FIPS Mode Disabled	cluster_name: aws-54985490-55275986-aws cluster_vendor: NetApp cluster_uuid: 3407e797-be51-11ed-9476-eb015bbf1f0e cluster_model: CDvM200	New	✓		

## 검토할 수 있습니다

ONTAP Essentials \* 인프라 \* 페이지에서는 모든 기본 ONTAP 객체에 대해 사전 구축된(추가 사용자 지정 가능) 쿼리를 사용하여 클러스터 상태와 성능을 확인할 수 있습니다. 탐색할 오브젝트 유형(클러스터, 스토리지 풀 등)을 선택하고 상태 또는 성능 정보를 표시할지 여부를 선택합니다. 필터를 설정하여 개별 시스템에 대해 자세히 설명합니다.



클러스터 상태를 보여 주는 인프라 페이지

:



## 네트워킹

ONTAP Essentials 네트워킹에서는 FC, NVMe FC, 이더넷 및 iSCSI 인프라에 대한 뷰를 제공합니다. 이 페이지에서는 클러스터의 포트 및 해당 노드에 대해 살펴볼 수 있습니다.

### ONTAP Essentials

#### Overview

#### Data Protection

#### Alerts

#### Infrastructure

#### Networking

#### Workloads

Active (86) Resolved (0)

alertId	triggeredTime ↓	currentSeverity	monitor	triggeredOn	status	hasCorrective Actions
AL-356704	12 hours ago Sep 9, 2022 2:16 AM	Critical	Snapshot Reserve Space ...	cluster_name: rtp-sa-cl04 vserver_name: test_ran volume_name: thick_vol_2 cluster_uuid: f34cd2c8-f1b3-11e9-b97f-00a0985f6587 cluster_vendor: NetApp cluster_model: AFF8040	New	✓
AL-355988	a day ago Sep 8, 2022 11:00 AM	Warning	User Quota Capacity Soft ...	cluster_name: rtp-sa-cl06 volume: qtreevol1 quota_type: user user_or_group: 16716 cluster_uuid: da294f0d-ad92-11e6-9969-00a0987b8fe8 cluster_vendor: NetApp cluster_model: FAS2552	New	✓

## 워크로드

사용자 환경의 LUN/볼륨, NFS 또는 SMB 공유 또는 qtree에서 워크로드를 확인하고 탐색합니다.



netapp\_ontap.lun All LUNs

Filter By cluster\_vendor NetApp

Group netapp\_ontap.lun

13 items found

Table Row Grouping	Metrics & Attributes								
netapp_ontap.lun	total_late...	total_iops (IO/s)	total_through...	size (B)	size_used (B)	volume	vserver_name	aggregate_name	node
/vol/ste/ste	0.00	0.00	0.00	53,694,627,840...	0.00	ste	vs_test	umeng_aff300...	ui
/vol/kubebug/kubebuglun1	0.00	0.00	0.00	85,905,637,376...	1,489,985,536.00	kubebug	vs_test	umeng_aff300...	ui
/vol/trident_pvc_3ef5a87c_4149_44e8_8113...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_3e...	vs_test	umeng_aff300...	ui
/vol/trident_pvc_0bf4ffd4_3f11_4d63_aa01_...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_0b...	vs_test	umeng_aff300...	ui
/vol/NSLM_VOL_LUN_1597772263794/matts...	0.00	0.00	0.00	1,073,741,824.00	0.00	NSLM_VOL_LU...	VMware_test	aggr_data_01_...	rt
/vol/mattlun12345/mattlun12345	0.00	0.00	0.00	1,073,741,824.00	0.00	mattlun12345	VMware_test	aggr_data_01_...	rt
/vol/kubebug1/kubebuglun2	0.00	0.00	0.00	85,904,826,368...	0.00	kubebug1	vs_test	umeng_aff300...	ui
/vol/trident_pvc_d66d7f51_a623_4fc3_8cda...	0.00	0.00	0.00	1,073,741,824.00	0.00	trident_pvc_d6...	vs_test	umeng_aff300...	ui
/vol/Rah/Rah	0.00	0.00	0.00	57,576,960.00	0.00	Rah	vs_test	umeng_aff300...	ui
/vol/chap_test_lun_vol/chap_test_lun	0.00	0.00	0.00	107,374,182,40...	0.00	chap_test_lun...	VMware_test	aggr_data_01_...	rt
/vol/windows_iscsi_example/windows_iscsi...	0.00	0.00	1.04	1,073,741,824.00	10,911,744.00	windows_iscsi...	VMware_test	aggr_data_01_...	rt
/vol/vol_test/lun1	0.04	0.10	0.00	1,073,741,824.00	0.00	vol_test	vs_test	umeng_aff300...	ui
/vol/osc_iscsi_vol01/osc_iscsi_vol01	2.11	116.83	2,737,374.33	4,398,046,511,1...	2,535,381,008,3...	osc_iscsi_vol01	osc	umeng_aff300...	ui

# 관리자 및 기타 작업

## Data Infrastructure Insights API를 참조하십시오

Data Infrastructure Insights API를 사용하면 NetApp 고객 및 독립 소프트웨어 공급업체 (ISV)가 CMDB 또는 기타 티켓팅 시스템과 같은 다른 애플리케이션과 Data Infrastructure Insights를 통합할 수 있습니다.

Data Infrastructure Insights API는 현재 에디션을 기반으로 사용할 수 있습니다.

API 유형	기본	표준	프리미엄
획득 장치	✓	✓	✓
데이터 수집	✓	✓	✓
경고		✓	✓
자산		✓	✓
데이터 수집		✓	✓
로그 수집		✓	✓

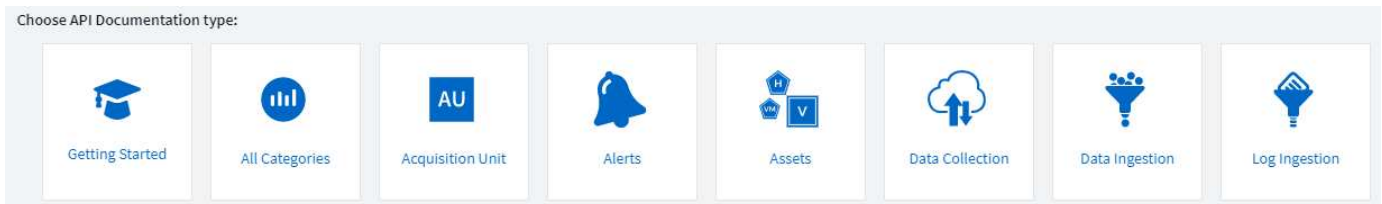
또한 Data Infrastructure Insights "기능 세트 역할"에 따라 액세스 가능한 API가 결정됩니다. 사용자 및 게스트 역할은 관리자 역할보다 권한이 적습니다. 예를 들어 Monitor and Optimize에서 관리자 역할이 있지만 Reporting에서 사용자 역할은 데이터 웨어하우스를 제외한 모든 API 유형을 관리할 수 있습니다.

### API 액세스에 대한 요구 사항

- 액세스 권한을 부여하기 위해 API 액세스 토큰 모델이 사용됩니다.
- API 토큰 관리는 관리자 역할을 가진 Data Infrastructure Insights 사용자가 수행합니다.

### API 설명서(Swagger)

최신 API 정보는 Data Infrastructure Insights에 로그인하여 \* Admin > API access \* 로 이동하여 확인할 수 있습니다. API Documentation \* 링크를 클릭합니다.



API 설명서는 Swagger 기반의 API에 대한 간단한 설명과 사용 정보를 제공하며, 사용자 환경에서 사용할 수 있습니다. 사용자 역할 및/또는 Data Infrastructure Insights 버전에 따라 사용 가능한 API 유형이 다를 수 있습니다.

POST

/assets/annotations Create annotation definition



## Parameters

Try it out

No parameters

Request body

application/json



Request body should include required name, type, optional description and enumValues (if enum type). Enums should contain name and label. Example:

```
{
  "name": "StorageLocation",
  "type": "FIXED_ENUM",
  "description": "Storage Location",
  "enumValues": [
    {
      "name": "PT_LISBON",
      "label": "Lisbon (Portugal)"
    },
    {
      "name": "US_WALTHAM",
      "label": "Waltham (USA)"
    }
  ]
}
```

[Example Value](#) | [Schema](#)

```
{ }
```

## API 액세스 토큰

Data Infrastructure Insights API를 사용하기 전에 하나 이상의 \* API 액세스 토큰 \* 을 생성해야 합니다. 액세스 토큰은 지정된 API 유형에 사용되며 읽기 및/또는 쓰기 권한을 부여할 수 있습니다. 각 액세스 토큰의 만료일을 설정할 수도 있습니다. 지정된 유형의 모든 API는 액세스 토큰에 대해 유효합니다. 각 토큰은 사용자 이름 또는 암호의 무효입니다.

액세스 토큰을 만들려면 다음을 수행합니다.

- Admin > API Access \* 를 클릭합니다
- API 액세스 토큰 \* 을 클릭합니다
  - 토큰 이름을 입력하십시오
  - API 유형을 선택합니다
  - 이 API 액세스에 대해 부여된 권한을 지정합니다
  - 토큰 만료 지정



토큰은 클립보드로 복사하고 생성 과정 중에 저장하는 경우에만 사용할 수 있습니다. 토큰을 만든 후에는 검색할 수 없으므로 토큰을 복사하여 안전한 위치에 저장하는 것이 좋습니다. 토큰 생성 화면을 닫기 전에 \* API 액세스 토큰 복사 \* 버튼을 클릭하라는 메시지가 표시됩니다.

토큰을 비활성화, 활성화 및 취소할 수 있습니다. 비활성화된 토큰을 활성화할 수 있습니다.

토큰은 고객의 관점에서 API에 대한 범용 액세스를 허용하며, 자신의 테넌트의 범위에서 API에 대한 액세스를 관리합니다. 고객 관리자는 Data Infrastructure Insights 백 엔드 직원의 직접적인 개입 없이 이러한 토큰을 부여 및 취소할 수 있습니다.

응용 프로그램은 사용자가 액세스를 성공적으로 인증 및 승인한 후 액세스 토큰을 받은 다음 대상 API를 호출할 때 액세스 토큰을 자격 증명으로 전달합니다. 전달된 토큰은 API에 토큰의 베어러가 API에 액세스할 수 있는 권한이 있음을 알리고 권한 부여 중에 부여된 범위에 의해 지정된 특정 작업을 수행하도록 합니다.

액세스 토큰이 전달되는 HTTP 헤더는 \* X-CloudInsights-ApiKey: \* 입니다.

예를 들어, 다음을 사용하여 스토리지 자산을 검색할 수 있습니다.

```
curl https://<tenant_host_name>/rest/v1/assets/storages -H 'X-CloudInsights-ApiKey:<API_Access_Token>'
```

여기서 `<API_Access_Token>`은 API 액세스 생성 중에 저장한 토큰입니다.

사용할 API에 대한 예는 Swagger 페이지를 참조하십시오.

## API 유형

Data Infrastructure Insights API는 범주를 기반으로 하며 현재 다음 유형이 포함되어 있습니다.

- 자산 유형에 자산, 쿼리 및 검색 API가 포함되어 있습니다.
  - 자산: 최상위 객체를 열거하고 특정 오브젝트 또는 오브젝트 계층을 검색합니다.
  - 쿼리: Data Infrastructure Insights 쿼리를 검색 및 관리합니다.
  - 가져오기: 주식이나 응용 프로그램을 가져와 개체에 할당합니다
  - 검색: 개체의 고유 ID 또는 전체 이름을 모르는 상태에서 특정 개체를 찾습니다.
- 데이터 수집 형식은 데이터 수집기를 검색하고 관리하는 데 사용됩니다.
- 데이터 수집 유형은 텔레그래프 에이전트와 같은 수집 데이터와 사용자 지정 메트릭을 검색 및 관리하는 데 사용됩니다
- 로그 수집은 로그 데이터를 검색하고 관리하는 데 사용됩니다

시간이 지나면 추가 유형 및/또는 API를 사용할 수 있습니다. 최신 API 정보는 에서 확인할 수 있습니다 ["API Swagger 문서"](#).

사용자가 액세스할 수 있는 API 유형은 ["사용자 역할"](#)각 Data Infrastructure Insights 기능 세트(모니터링, 워크로드 보안, 보고)에 있는 유형에 따라서도 달라집니다.

## 재고 탐색

이 섹션에서는 Data Infrastructure Insights 개체의 계층 구조를 이동하는 방법을 설명합니다.

## 상위 수준 개체

개별 개체는 고유 URL (JSON의 "자체")을 통해 요청에서 식별되며 개체 유형 및 내부 ID에 대한 지식이 필요합니다. 일부 최상위 객체(호스트, 스토리지 등)의 경우 REST API를 통해 전체 컬렉션에 액세스할 수 있습니다.

API URL의 일반적인 형식은 다음과 같습니다.

```
https://<tenant>/rest/v1/<type>/<object>
```

예를 들어 `_mysite.c01.cloudinsights.netapp.com_` 이라는 테넌트에서 모든 스토리지를 검색하려면 요청 URL은 다음과 같습니다.

```
https://mysite.c01.cloudinsights.netapp.com/rest/v1/assets/storages
```

## 하위 및 관련 개체

Storage 와 같은 최상위 개체를 사용하여 다른 자식 및 관련 개체를 이동할 수 있습니다. 예를 들어, 특정 스토리지에 대한 모든 디스크를 검색하려면 스토리지 "자체" URL을 `/disks`와 연결합니다. 예를 들면 다음과 같습니다.

```
https://<tenant>/rest/v1/assets/storages/4537/disks
```

## 확장

많은 API 명령은 \* Expand \* 매개 변수를 지원하며, 이는 관련 객체의 객체 또는 URL에 대한 추가 세부 정보를 제공합니다.

일반적인 확장 매개 변수 중 하나는 `_ Expand _` 입니다. 응답에는 객체에 대해 사용 가능한 모든 특정 확장 목록이 포함됩니다.

예를 들어, 다음을 요청할 경우:

```
https://<tenant>/rest/v1/assets/storages/2782?expand=_expands
```

API는 다음과 같이 객체에 대해 사용 가능한 모든 확장을 반환합니다.

```

{
  "id": "1247936",
  "self": "/rest/v1/assets/storages/1247936",
  "name": "amsprdclu01",
  "simpleName": "amsprdclu01",
  "naturalKey": "5DF483F0-1729-11DC-9A79-123478563412",
  "ip": "10.64.0.132",
  "serialNumber": "1-80-000011",
  "model": "FAS3270,FAS6290",
  "vendor": "NetApp",
  "microcodeVersion": "8.1.3 clustered Data ONTAP",
  "capacity": {
    "description": "Storage Capacity",
    "unitType": "MB",
    "total": {
      "value": 8.23185105E8
    }
  },
  "storagePools": {
    "value": 5.43220974E8
  }
},
"isActive": true,
"createTime": "2013-05-07T16:52:21-0700",
"family": "FAS3200,FAS6200",
"managementUrl": null,
"virtualizedType": "STANDARD",
"protocols":
[
  "NAS",
  "NFS",
  "CIFS",
  "FC",
  "ISCSI"
],
"expands": {
  "performance": {
    "url": "/rest/v1/assets/storages/1247936/performance",
    "name": "Performance Data"
  },
  "storageNodes": {
    "url": "/rest/v1/assets/storages/1247936/storageNodes",
    "name": "Storage Storage Nodes"
  },
  "storagePools": {
    "url": "/rest/v1/assets/storages/1247936/storagePools",
    "name": "Storage Storage Pools"
  },
  "storageResources": {
    "url": "/rest/v1/assets/storages/1247936/storageResources",
    "name": "Storage Storage Resources"
  },
  "internalVolumes": {
    "url": "/rest/v1/assets/storages/1247936/internalVolumes",
    "name": "Storage Internal Volumes"
  },
  "volumes": {
    "url": "/rest/v1/assets/storages/1247936/volumes",
    "name": "Storage Volumes"
  },
  "disks": {
    "url": "/rest/v1/assets/storages/1247936/disks",
    "name": "Disks"
  },
  "datasources": {
    "url": "/rest/v1/assets/storages/1247936/datasources",
    "name": "Storage Datasources"
  },
  "ports": {
    "url": "/rest/v1/assets/storages/1247936/ports",
    "name": "Storage Ports"
  },
  "annotations": {
    "url": "/rest/v1/assets/storages/1247936/annotations",
    "name": "Storage Annotations"
  },
  "qtrees": {
    "url": "/rest/v1/assets/storages/1247936/qtrees",
    "name": "Qtrees"
  }
},
}

```

각 확장에는 데이터, URL 또는 둘 다 포함됩니다. Expand 매개 변수는 다음과 같은 여러 가지 및 중첩 특성을 지원합니다.

```
https://<tenant>/rest/v1/assets/storages/2782?expand=performance,storageResources.storage
```

확장을 사용하면 하나의 응답에서 많은 관련 데이터를 가져올 수 있습니다. NetApp은 한 번에 너무 많은 정보를 요청하지 않을 것을 권장합니다. 이로 인해 성능 저하가 발생할 수 있습니다.

이를 방지하기 위해 최상위 컬렉션 요청은 확장할 수 없습니다. 예를 들어, 모든 스토리지 오브젝트의 확장 데이터를 한 번에 요청할 수 없습니다. 클라이언트는 개체 목록을 검색한 다음 확장할 특정 개체를 선택해야 합니다.

## 성능 데이터

성능 데이터는 여러 장치에 걸쳐 별도의 샘플로 수집됩니다. Data Infrastructure Insights는 1시간마다(기본값) 성능 샘플을 집계하고 요약합니다.

API를 사용하면 샘플과 요약된 데이터에 모두 액세스할 수 있습니다. 성능 데이터가 있는 개체의 경우 성능 요약을 `_EXPORTED=performance_`로 사용할 수 있습니다. 성능 기록 시간 시리즈는 `nested_expand=performance.history_`를 통해 사용할 수 있습니다.

성능 데이터 오브젝트의 예는 다음과 같습니다.

- 스토리지성능
- StoragePoolPerformance
- PortPerformance(포트 성능)
- 디스크 성능

성능 메트릭에는 설명 및 유형이 있으며 성능 요약 컬렉션이 포함되어 있습니다. 예: 지연 시간, 트래픽 및 속도.

성능 요약에는 시간 범위(1시간, 24시간, 3일 등)에 대해 단일 성능 카운터를 사용하여 계산된 설명, 단위, 샘플 시작 시간, 샘플 종료 시간 및 요약된 값(현재, 최소, 최대, 평균 등)의 모음이 있습니다.



Details

Response body

```
{
  "self": "/rest/v1/assets/storages/1/performance",
  "cacheHitRatio": {
    "read": {
      "description": "Cache Hit Ratio - Read",
      "unitType": "%",
      "start": null,
      "end": null,
      "current": null,
      "min": null,
      "max": null,
      "avg": null,
      "sum": null,
      "isDownsampled": false
    },
    "write": {
      "description": "Cache Hit Ratio - Write",
      "unitType": "%",
      "start": null,
      "end": null,
      "current": null,
      "min": null,
      "max": null,
      "avg": null,
      "sum": null,
      "isDownsampled": false
    }
  }
}
```

Self

Performance Metric

Response body

```
}
},
"history": [
  [
    1578418848140,
    {
      "latency.total": 1.30578,
      "latency.read": 3.64681,
      "ioDensity.read": 9.62065,
      "iops.write": 686.35502,
      "ioDensity.total": 31.36259,
      "capacity.raw": 80024.92772,
      "throughput.read": 7.32371,
      "iops.total": 1488.7974,
      "latency.write": 0.39495,
      "ioDensity.write": 14.45856,
      "iops.read": 456.69703,
      "capacity.storagePools": 56058.1041,
      "throughput.write": 14.59581,
      "throughput.total": 21.91953
    }
  ],
  [
    1578419748198,
    {

```

History

Timestamp

Counter Values

결과 Performance Data 사전에는 다음과 같은 키가 있습니다.

- "self"는 개체의 고유 URL입니다

- "기록"은 카운터 값의 타임 스탬프 및 맵 쌍 목록입니다
- 다른 모든 사전 키("diskThroughput" 등)는 성능 메트릭의 이름입니다.

각 성능 데이터 오브젝트 유형에는 고유한 성능 메트릭 세트가 있습니다. 예를 들어, 가상 머신 성능 개체는 성능 메트릭으로 "diskThroughput"을 지원합니다. 지원되는 각 성능 메트릭은 메트릭 사전에 나와 있는 특정 "성능 범주"입니다. Data Infrastructure Insights는 이 문서의 뒷부분에 나열된 몇 가지 성능 메트릭 유형을 지원합니다. 각 성능 메트릭 사전에는 이 성능 메트릭에 대한 사람이 읽을 수 있는 설명과 성능 요약 카운터 항목 집합인 "설명" 필드도 있습니다.

성능 요약 카운터는 성능 카운터의 요약입니다. 카운터에 대한 최소, 최대 및 평균 등의 일반적인 집계 값과 최근 관찰 값, 요약 데이터에 대한 시간 범위, 카운터에 대한 단위 유형 및 데이터에 대한 임계값을 제공합니다. 임계값은 선택 사항이므로 나머지 속성은 필수입니다.

성능 요약은 다음 유형의 카운터에 사용할 수 있습니다.

- 읽기 – 읽기 작업에 대한 요약입니다
- Write – 쓰기 작업의 요약입니다
- 총계 - 모든 작업의 요약입니다. 읽기 및 쓰기의 단순한 합계보다 높을 수 있으며 다른 작업도 포함될 수 있습니다.
- Total Max – 모든 작업에 대한 요약입니다. 지정된 시간 범위의 최대 총 값입니다.

## 객체 성과 지표

API는 사용자 환경의 객체에 대한 세부 메트릭을 반환할 수 있습니다. 예를 들면 다음과 같습니다.

- IOPS(초당 입출력 요청 수), 지연 시간 또는 처리량과 같은 스토리지 성능 메트릭
- 트래픽 활용률, BB Credit Zero 데이터 또는 포트 오류와 같은 스위치 성능 메트릭

를 참조하십시오 ["API Swagger 문서"](#) 각 오브젝트 유형에 대한 메트릭에 대한 정보를 참조하십시오.

## 성능 기록 데이터

기록 데이터는 성능 데이터에 타임 스탬프 및 카운터 맵 쌍의 목록으로 표시됩니다.

기록 카운터는 성능 메트릭 개체 이름을 기반으로 명명됩니다. 예를 들어, 가상 시스템 성능 개체는 "diskThroughput"을 지원하므로 기록 맵에는 "diskThroughput.read", "diskThroughput.write" 및 "diskThroughput.total"이라는 키가 포함됩니다.



타임스탬프는 UNIX 시간 형식입니다.

다음은 디스크의 성능 데이터 JSON의 예입니다.

```

"performance": {
  "self": "/rest/v1/assets/disks/4013931/performance",
  "iops": {
    "performanceCategory": "IOPS",
    "description": "Disk IOPS",
    "read": {
      "description": "Disk Read Iops",
      "unitType": "IO/s",
      "start": 1399305599999,
      "end": 1402604368055,
      "current": 1,
      "min": 0,
      "max": 6,
      "avg": 0.5532
    },
    [...]
  },
  "total": {
    "description": "Disk Total Throughput",
    "unitType": "MB/s",
    "start": 1399305599999,
    "end": 1402604368055,
    "current": 0,
    "min": 0,
    "max": 2,
    "avg": 0.1702
  }
},
"history":
[
  [
    1399300412690,
    {
      "utilization.total": 12,
      "iops.total": 26,
      "iops.write": 22,
      "iops.read": 4,
      "throughput.read": 0,
      "utilization.read": 2.12,
      "throughput.total": 5,
      "utilization.write": 10.24,
      "throughput.write": 5
    }
  ]
]

```

## 용량 특성이 있는 오브젝트

용량 속성이 있는 개체는 기본 데이터 형식과 CapacityItem 을 사용하여 표시합니다.

### 용량 항목

용량항목은 단일 논리 용량 단위입니다. 이 개체의 상위 개체에 의해 정의된 단위로 "값"과 "상위 임계값"이 있습니다. 또한 용량 값의 구성 방법을 설명하는 선택적 분석 맵을 지원합니다. 예를 들어 100TB StoragePool의 총 용량은 100의 값을 갖는 CapacityItem입니다. 이 분석 결과는 "데이터"에 할당된 60TB 및 "스냅샷"에 대해 40TB로 표시될 수 있습니다.

### 참고

"HighThreshold"는 해당 메트릭의 시스템 정의 임계값을 나타내며, 클라이언트는 이 임계값을 사용하여 허용되는 구성 범위를 벗어난 값에 대한 경고 또는 시각적 신호를 생성할 수 있습니다.

다음은 여러 용량 카운터가 있는 StoragePools의 용량을 보여 줍니다.

## StoragePoolCapacity

Model properties:

```
{
  description: string
  unitType: 'MB' or 'GB' or 'TB' or 'KiB' or 'MiB' or 'TiB'
  total: CapacityItem
  used: CapacityItem
  provisioned: CapacityItem
  reservedCapacity: CapacityItem
  softLimit: Double
  rawToUsableRatio: Double
  isDedupeEnabled: boolean
  dedupeSavings: NumericValueWithUnit
  isCompressionEnabled: boolean
  compressionSavings: NumericValueWithUnit
  isThinProvisioningSupported: boolean
}
```

close

검색을 사용하여 개체를 검색합니다

검색 API는 시스템에 대한 간단한 진입점입니다. API에 대한 유일한 입력 매개 변수는 자유 형식 문자열이며 결과 JSON에는 분류된 결과 목록이 포함되어 있습니다. 유형은 스토리지, 호스트, 데이터 저장소 등과 같이 인벤토리에서 서로 다른 자산 유형입니다. 각 형식에는 검색 조건과 일치하는 형식의 개체 목록이 포함됩니다.

Data Infrastructure Insights는 확장 가능한(광범위한 개방형) 솔루션으로서 타사 오케스트레이션, 비즈니스 관리, 변경 제어 및 티켓팅 시스템뿐만 아니라 사용자 지정 CMDB 통합과도 통합할 수 있습니다.

Cloud Insight의 RESTful API는 데이터를 간단하고 효과적으로 이동할 수 있을 뿐 아니라 사용자가 데이터에 원활하게 액세스할 수 있도록 하는 기본적인 통합 지점입니다.

## API 토큰 비활성화 또는 해지

API 토큰을 일시적으로 비활성화하려면 API 토큰 목록 페이지에서 API에 대한 "점 3개" 메뉴를 클릭하고 `_Disable_`을 선택합니다. 언제든지 같은 메뉴를 사용하여 `_Enable_`을 선택하여 토큰을 다시 활성화할 수 있습니다.

API 토큰을 영구적으로 제거하려면 메뉴에서 "해지"를 선택합니다. 해지된 토큰은 다시 사용할 수 없습니다. 새 토큰을 만들어야 합니다.

API Access Tokens (252) + API Access Token Bulk Actions Filter...

<input type="checkbox"/>	Name ↑	Description	Token	API Type	Permission	Expires On	Status	
<input type="checkbox"/>	10.197.120.70		...RpTMJ4	Data Ingestion	Write Only	11/06/2021	Expired	
	22		...nUBDhe	Data Ingestion	Write Only	06/17/2022	Enabled	Disable
	22TOKEN2010560		...8gXq7K	All Categories	Read Only	06/17/2022	Enabled	Edit Description
	ActiveIQ_POC_token		...scmES6	Data Ingestion	Read/Write	11/12/2021	Expired	Revoke

## 만료된 API 액세스 토큰 회전

API 액세스 토큰의 만료 날짜가 있습니다. API 액세스 토큰이 만료되면 사용자는 읽기/쓰기 권한이 있는 *Data* 수집 유형의 새 토큰을 생성하고 만료된 토큰 대신 새로 생성된 토큰을 사용하도록 텔레그래프를 다시 구성해야 합니다. 아래 단계에서는 이 작업을 수행하는 방법을 자세히 설명합니다.

### 쿠버네티스

이러한 명령은 기본 네임스페이스 "NetApp-모니터링"을 사용합니다. 고유한 네임스페이스를 설정한 경우 이러한 네임스페이스 및 모든 후속 명령 및 파일로 대체합니다.

참고: 최신 NetApp Kubernetes Monitoring Operator가 설치되어 있고 재생 가능한 API 액세스 토큰을 사용하는 경우, 만료되는 토큰이 자동으로 새/업데이트된 API 액세스 토큰으로 대체됩니다. 아래 나열된 수동 단계를 수행할 필요는 없습니다.

- NetApp Kubernetes Monitoring Operator를 편집합니다.

```
kubectl -n netapp-monitoring edit agent agent-monitoring-netapp
* 이전 API 토큰을 새 API 토큰으로 대체하여 _spec.output-sink.api-key_value를 수정합니다.
```

```
spec:
...
  output-sink:
    - api-key:<NEW_API_TOKEN>
```

### RHEL/CentOS 및 Debian/Ubuntu

- Telegraf 구성 파일을 편집하고 이전 API 토큰의 모든 인스턴스를 새 API 토큰으로 교체합니다.

```
sudo sed -i.bkup 's/<OLD_API_TOKEN>/<NEW_API_TOKEN>/g'
/etc/telegraf/telegraf.d/*.conf
* 텔레그래프를 다시 시작합니다.
```

```
sudo systemctl restart telegraf
```

### Windows

- C:\Program Files\Telegraf\Telegraf.d\_의 각 Telegraf 구성 파일에 대해 이전 API 토큰의 모든 인스턴스를 새 API 토큰으로 교체합니다.

```
cp <plugin>.conf <plugin>.conf.bkup
(Get-Content <plugin>.conf).Replace('<OLD_API_TOKEN>',
'<NEW_API_TOKEN>') | Set-Content <plugin>.conf
```

- 텔레그래프를 다시 시작합니다.

```
Stop-Service telegraf
Start-Service telegraf
```

## 환경 모니터링

### 감사

예상되는 변경 사항(추적 대상) 또는 예상치 못한 변경 사항(문제 해결)을 모두 식별하려면 Data Infrastructure Insights 시스템 이벤트 및 사용자 활동의 감사 추적을 볼 수 있습니다.

#### 감사된 이벤트 보기

감사 페이지를 보려면 메뉴에서 \* 관리자 > 감사 \* 를 클릭합니다. 감사 페이지가 표시되어 각 감사 항목에 대해 다음 세부 정보를 제공합니다.

- \* Time \* - 이벤트 또는 활동의 날짜 및 시간입니다
- \* 사용자 \* - 작업을 시작한 사용자입니다
- \* 역할 \* - Data Infrastructure Insights에서 사용자의 역할(게스트, 사용자, 관리자)
- \* IP \* - 이벤트와 연결된 IP 주소입니다
- \* 조치 \* - 활동 유형(예: 로그인, 생성, 업데이트)
- \* 범주 \* - 활동 범주입니다
- \* 세부 정보 \* - 활동 세부 정보

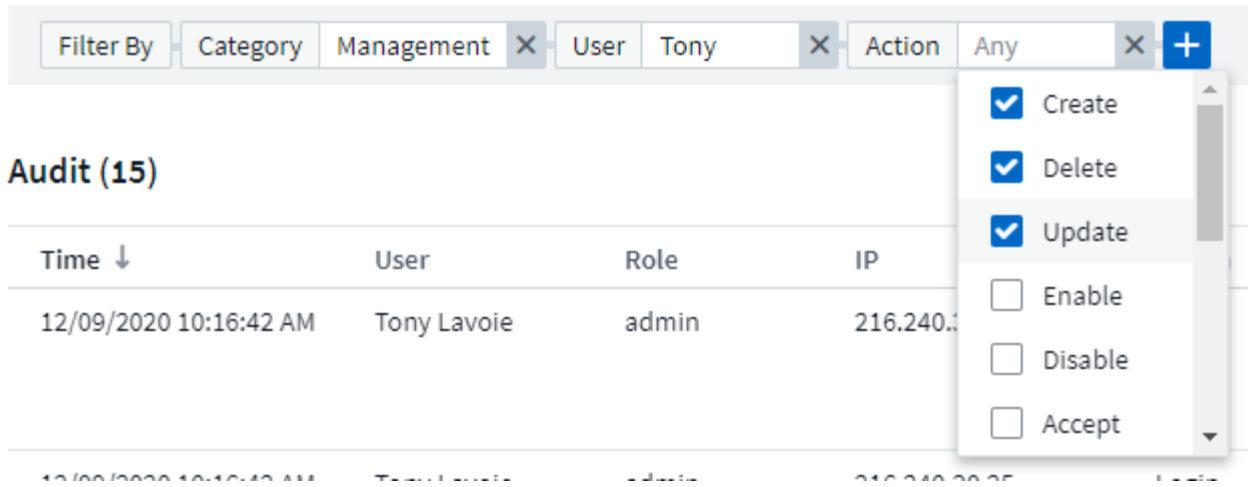
#### 감사 항목 표시

감사 항목을 보는 방법에는 여러 가지가 있습니다.

- 특정 기간(1시간, 24시간, 3일 등)을 선택하여 감사 항목을 표시할 수 있습니다.
- 열 머리글의 화살표를 클릭하여 항목의 정렬 순서를 오름차순(위쪽 화살표) 또는 내림차순(아래쪽 화살표)으로 변경할 수 있습니다.

기본적으로 테이블에는 항목이 내림차순으로 표시됩니다.

- 필터 필드를 사용하여 테이블에서 원하는 항목만 표시할 수 있습니다. [+] 버튼을 클릭하여 추가 필터를 추가합니다.



필터링에 대한 추가 정보

다음 중 하나를 사용하여 필터를 구체화할 수 있습니다.

필터	기능	예	결과
* (별표)	모든 것을 검색할 수 있습니다	볼륨 * rhel	"vol"로 시작하고 "rhel"로 끝나는 모든 리소스를 반환합니다.
? (물음표)	특정 수의 문자를 검색할 수 있습니다	BOS-PRD??- S12	BOS-PRD12-S12, BOS-PRD23-S12 등을 반환합니다
또는	여러 요소를 지정할 수 있습니다	FAS2240 또는 CX600 또는 FAS3270	FAS2440, CX600 또는 FAS3270을 반환합니다
아닙니다	검색 결과에서 텍스트를 제외할 수 있습니다	EMC가 아님 *	"EMC"로 시작하지 않는 모든 항목을 반환합니다.
없음	선택한 필드에서 공백/NULL/없음을 검색합니다	없음	대상 필드가 비어 있지 않은 결과를 반환합니다
NOT *	위의 _None_ 과 마찬가지로 이 양식을 사용하여 _text-only_fields_에서 NULL 값을 검색할 수도 있습니다	NOT *	대상 필드가 비어 있지 않은 결과를 반환합니다.
""	정확하게 일치하는 항목을 검색합니다	"NetApp ""	리터럴 문자열 _NetApp*_ 을 포함한 결과를 반환합니다

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 또는 는 큰따옴표로 묶으면 리터럴 문자열로 처리됩니다.

## 감사된 이벤트 및 조치

Data Infrastructure Insights에서 감사한 이벤트와 작업은 다음과 같은 광범위한 영역으로 분류될 수 있습니다.

- \* 사용자 계정 \*: 로그인, 로그아웃, 역할 변경 등

예: \_ 사용자 \* Tony Lavoie \* 는 \* 10.1.120.15 \* 에서 로그인했으며 사용자 에이전트 \* Mozilla/5.0(Windows NT 10.0; Win64; x64) AppleWebKit/537.36(KHTML, Gecko 등) Chrome/85.0.4183.121 Safari/537.36 \*, 로그인 방법 \* BlueXP 포털 로그인 \_ \*

- \* 획득 장치 \*: 생성, 삭제 등

예: \_ 획득 장치 \* AU - Boston-1 \* 제거됨 \_.

- \* Data Collector \*: 추가, 제거, 수정, 연기/재개, 획득 단위 변경, 시작/중지 등

예: *DataSource \* FlexPod Lab \* 제거됨*, 공급업체 \* *NetApp \**, 모델 \* *ONTAP 데이터 관리 소프트웨어 \**, *IP \* 192.168.106.5 \**.

- \* 응용 프로그램 \*: 추가, 개체에 할당, 제거 등

예: \_ 내부 볼륨 \* ocisedev: t1appSVM01: t1appFlexVol01 \* 응용 프로그램에 추가됨 \* Test App\_ \*.

- \* 주식 \*: 추가, 할당, 제거, 주식 규칙 작업, 주식 값 변경, 등

예: \_ 주식 값 \* Boston \* 주식 유형 \* SalesOffice\_ \* 에 추가되었습니다.

- \* 쿼리 \*: 추가, 제거 등

예: \_ 쿼리 \* TL 판매 쿼리 \* 가 \_ 에 추가됩니다.

- \* Monitor \*: 추가, 제거 등

예: Monitor\_Aggregr 크기 - CI 경고 알림 Dev\_Updated


- \* 알림 \*: 이메일 변경 등

예: Recipient\_CI-alerts-notifications-dl\_created

## 감사 이벤트 내보내기

감사 표시 결과를 .csv 파일로 내보내면 데이터를 분석하거나 다른 응용 프로그램으로 가져올 수 있습니다.

### 단계

1. 감사 페이지에서 원하는 시간 범위와 원하는 필터를 설정합니다. Data Infrastructure Insights는 사용자가 설정한 필터링 및 시간 범위와 일치하는 감사 항목만 내보냅니다.
2. Export \_ 버튼을 클릭합니다  테이블 오른쪽 위에 있습니다.

표시된 감사 이벤트는 최대 10,000개의 행까지 .csv 파일로 내보내집니다.



## 감사 데이터 보존

Data Infrastructure Insights가 감사 데이터를 유지하는 시간은 다음 에디션에 기준으로 합니다.

- Basic Edition: 감사 데이터는 30일 동안 보존됩니다
- Standard 및 Premium Edition: 감사 데이터는 1년 + 1일 동안 보존됩니다

보존 시간보다 오래된 감사 항목은 자동으로 제거됩니다. 사용자 조작이 필요하지 않습니다.

## 문제 해결

여기에서 감사 관련 문제를 해결할 수 있는 제안 사항을 찾을 수 있습니다.

* 문제: *	* 사용해 보세요. *
모니터를 내보냈다는 감사 메시지가 표시됩니다.	맞춤형 모니터 구성의 내보내기는 일반적으로 새 기능을 개발 및 테스트하는 동안 NetApp 엔지니어가 사용합니다. 이 메시지가 표시되지 않을 것으로 예상되면 감사 대상 작업에 명명된 사용자의 작업을 탐색하거나 지원 부서에 문의하십시오.

## Active IQ

넷앱 "Active IQ" 하드웨어/소프트웨어 시스템의 NetApp 고객에게 일련의 시각화, 분석 및 기타 지원 관련 서비스를 제공합니다. Active IQ에서 보고하는 데이터는 시스템 문제 해결을 개선하고 장치와 관련된 최적화 및 예측 분석에 대한 통찰력을 제공할 수 있습니다.



ActiveIQ는 Data Infrastructure Insights Federal Edition에서 사용할 수 없습니다.

데이터 인프라 Insights는 Active IQ에서 모니터링 및 보고하는 NetApp clustered Data ONTAP 스토리지 시스템의 \* 위험 \* 을 수집합니다. 스토리지 시스템에 대해 보고된 위험은 해당 장치에서 데이터 수집의 일부로 Data Infrastructure Insights에 의해 자동으로 수집됩니다. Active IQ 위험 정보를 수집하려면 데이터 인프라 인사이트 에 적절한 데이터 수집기를 추가해야 합니다.

Data Infrastructure Insights에는 Active IQ에서 모니터링 및 보고하지 않는 ONTAP 시스템의 위험 데이터가 표시되지 않습니다.

보고된 위험은 `_STORAGE_AND_STORAGE_NODE_ASSET` 랜딩 페이지의 "위험" 표에 나와 있습니다. 이 표에는 위험 세부 정보, 위험 범주 및 잠재적 영향이 나와 있으며, 스토리지 노드의 모든 위험을 요약하는 Active IQ 페이지 링크가 제공됩니다(NetApp 지원 어카운트 로그인 필요).

Object ↑	Risk Detail	Category	Potential Impact	Source
tawny01	The following certificates have expired or are expiring within 30 days: Expired: 53CF9553, 53C504D4, 53D671B4, Expiring within 30 days: None	System Configuration	Clients may not be able to connect to the cluster over secure (SSL based) protocols.	Active IQ <a href="#">🔗</a>
tawny01	None of the NIS servers configured for SVM(s) tawny_svm_oci_markic can be contacted.	CIFS Protocol	Potential CIFS and NFS outages may occur.	Active IQ <a href="#">🔗</a>
tawny01	ONTAP version 8.3.2 has entered the Self-Service Support period.	ONTAP	Self-Service Support is the time period where NetApp does not provide support for a version of a software product, but related documentation is still available on the NetApp Support Site.	Active IQ <a href="#">🔗</a>

보고된 위험의 수도 랜딩 페이지의 요약 위젯에 표시되며 해당 Active IQ 페이지에 대한 링크도 표시됩니다. storage\_landing 페이지에서 count는 모든 기본 스토리지 노드의 위험을 합한 값입니다.

**Storage Summary**

<b>Model:</b> FAS6210	<b>Microcode Version:</b> 8.3.2 clustered Data ONTAP	<b>Management:</b> <a href="https://10.197.143.25:443">HTTPS://10.197.143.25:443</a>
<b>Vendor:</b> NetApp	<b>Raw Capacity:</b> 80,024.3 GB	<b>FC Fabrics Connected:</b> 0
<b>Family:</b> FAS6200	<b>Latency - Total:</b> 0.77 ms	<b>Performance Policies:</b>
<b>Serial Number:</b> 1-80-000013	<b>IOPS - Total:</b> 1,819.19 IO/s	<b>Risks:</b> 108 risks detected by Active IQ
<b>IP:</b> 10.197.143.25	<b>Throughput - Total:</b> 41.69 MB/s	

### Active IQ 페이지를 엽니다

Active IQ 페이지에 대한 링크를 클릭할 때 현재 Active IQ 계정에 로그인되어 있지 않은 경우 다음 단계를 수행하여 스토리지 노드의 Active IQ 페이지를 표시해야 합니다.

1. 데이터 인프라 인사이트 요약 위젯 또는 위험 표에서 "Active IQ" 링크를 클릭합니다.
2. NetApp Support 계정에 로그인하십시오. Active IQ의 스토리지 노드 페이지로 직접 이동됩니다.

### 위험을 쿼리하는 중입니다

Data Infrastructure Insights에서 스토리지 또는 스토리지 노드 쿼리에 \* monitoring.count \* 열을 추가할 수 있습니다. 반환된 결과에 Active IQ가 모니터링된 스토리지 시스템이 포함된 경우 monitoring.count 열에 스토리지 시스템 또는 노드의 위험 수가 표시됩니다.

### 대시보드

위젯(예: 원형 차트, 표 위젯, 막대, 열, 분산형 플롯, 및 단일 가치 위젯)을 활용하여 Active IQ에서 모니터링하는 NetApp clustered Data ONTAP 시스템의 스토리지 및 스토리지 노드에 대한 오브젝트 위험을 시각화합니다. "오브젝트 위험"은 스토리지 또는 스토리지 노드가 초점의 개체인 이러한 위젯에서 열 또는 메트릭으로 선택할 수 있습니다.

### Object Risks by Array

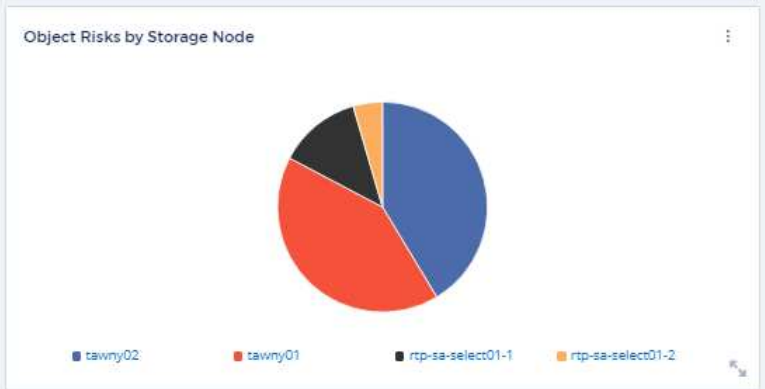
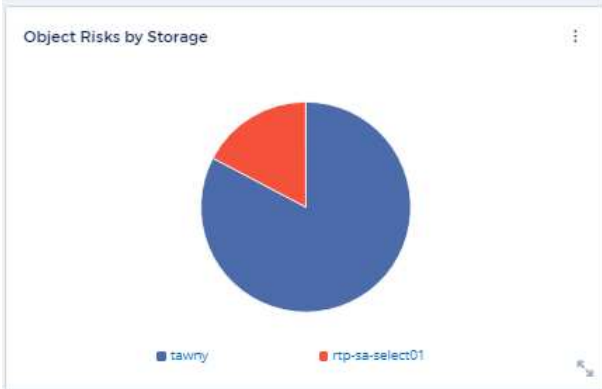
12 items found

Name	Object Risks ↓
tawny	110
rtp-sa-select01	23
rtp-sa-cl02	N/A
rtp-sa-cl07	N/A
oci-phonehome	N/A
durlabprdfs01	N/A
oci-3070-01	N/A

### Object Risks by Node

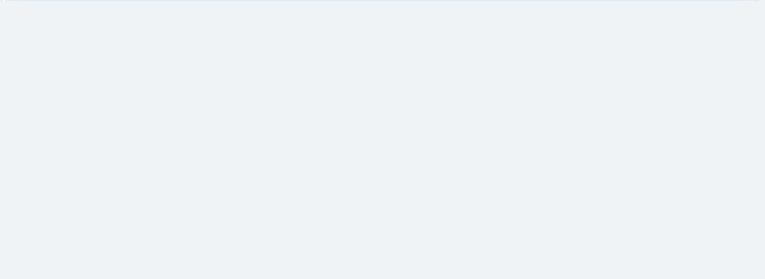
25 items found

Name	Object Risks ↓
tawny02	55
tawny01	55
rtp-sa-select01-1	17
rtp-sa-select01-2	6
tnode02	N/A
rtp-sa-cl06-01	N/A
rtp-sa-cl06-02	N/A



### Total Storage Risks

**133.00**  
Object Risks



# 워크로드 보안

## 스토리지 워크로드 보안 정보

Data Infrastructure Insights 스토리지 워크로드 보안(이전의 Cloud Secure)은 내부자 위협에 대한 실행 가능한 인텔리전스를 사용하여 데이터를 보호하는 데 도움이 됩니다. 또한 하이브리드 클라우드 환경 전반에서 모든 기업 데이터 액세스에 대한 중앙 집중식 가시성과 제어를 제공하여 보안 및 규정 준수 목표를 충족할 수 있습니다.



Data Infrastructure Insights Federal Edition에서는 워크로드 보안을 사용할 수 없습니다.

### 가시성

온프레미스 또는 클라우드에 저장된 주요 기업 데이터에 대한 사용자 액세스를 중앙 집중식으로 파악하고 제어할 수 있습니다.

데이터 액세스 및 제어에 대한 시기 적절하고 정확한 가시성을 제공하지 못하는 도구 및 수동 프로세스를 대체합니다. 워크로드 보안은 클라우드 및 사내 스토리지 시스템 모두에서 고유하게 작동하며 악의적인 사용자 동작에 대한 실시간 경고를 제공합니다.

### 보호

악의적인 사용자 또는 손상된 사용자가 조직 데이터를 악용하지 못하도록 고급 머신 러닝 및 이상 징후 탐지를 통해 보호합니다.

고급 머신 러닝 및 사용자 동작에 대한 이상 탐지 기능을 통해 비정상적인 데이터 액세스를 경고합니다.

### 규정 준수

온프레미스 또는 클라우드에 저장된 중요한 기업 데이터에 대한 사용자 데이터 액세스를 감사하여 기업의 규정 준수를 보장할 수 있습니다.

## 시작하기

### 워크로드 보안 시작

워크로드 보안을 사용하여 사용자 작업을 모니터링하려면 먼저 완료해야 하는 구성 작업이 있습니다.

워크로드 보안 시스템은 에이전트를 사용하여 스토리지 시스템에서 액세스 데이터를 수집하고 디렉토리 서비스 서버에서 사용자 정보를 수집합니다.

데이터 수집을 시작하려면 먼저 다음을 구성해야 합니다.

작업	관련 정보
----	-------

Agent를 구성합니다	"상담원 요구 사항"  "상담원 추가"  "* 비디오 *: 에이전트 배포"
사용자 디렉터리 커넥터를 구성합니다	"사용자 디렉토리 커넥터를 추가합니다"  "* 비디오 *: Active Directory 연결"
데이터 수집기를 구성합니다	Workload Security > Collector * 를 클릭합니다  구성할 데이터 수집기를 클릭합니다.  설명서의 Data Collector 공급업체 참조 섹션을 참조하십시오.  "* 비디오 *: ONTAP SVM 연결"
사용자 계정을 생성합니다	"사용자 계정 관리"
문제 해결	"* 비디오 *: 문제 해결"

워크로드 보안은 다른 톨과도 통합될 수 있습니다. 예를 들면, 다음과 같습니다. "[이 가이드를 참조하십시오](#)" Splunk와 통합 시,

### 워크로드 보안 에이전트 요구 사항

반드시 해야 합니다 "[Agent를 설치합니다](#)" 데이터 수집기에서 정보를 얻기 위해 Agent를 설치하기 전에 운영 체제, CPU, 메모리 및 디스크 공간 요구 사항을 충족하는지 확인해야 합니다.

구성 요소	Linux 요구 사항
운영 체제	다음 중 하나의 라이선스 버전을 실행하는 컴퓨터: * CentOS 8 Stream(64비트), SELinux * OpenSUSE Leap 15.3 - 15.5(64비트) * Oracle Linux 8.6 - 8.8, 9.1에서 9.2(64비트) * Red Hat Enterprise Linux 8.6 - 8.8, 9.1 - 9.2(64비트), SELinux * Rocky 9.2(64비트), SELinux * SUSE Linux Enterprise Server 15 SP3 - 15 SP3(64비트) * Ubuntu 20.04 LTS 및 22.04 LTS(64비트) 이 컴퓨터는 다른 응용 프로그램 수준 소프트웨어를 실행하지 않아야 합니다. 전용 서버가 권장됩니다.
명령	설치를 위해 '압축 해제'가 필요합니다. 또한 설치, 스크립트 실행 및 제거에 'SUDO su -' 명령이 필요합니다.
CPU	CPU 코어 4개
메모리	16GB RAM

구성 요소	<b>Linux</b> 요구 사항
사용 가능한 디스크 공간입니다	<p>디스크 공간은 다음과 같은 방식으로 할당되어야 합니다. /opt/NetApp 36GB(파일 시스템 생성 후 최소 35GB의 여유 공간)</p> <p>참고: 파일 시스템을 생성할 수 있도록 추가 디스크 공간을 할당하는 것이 좋습니다. 파일 시스템에 최소 35GB의 여유 공간이 있는지 확인합니다.</p> <p>/opt가 NAS 스토리지에서 마운트된 폴더인 경우 로컬 사용자가 이 폴더에 액세스할 수 있는지 확인합니다. 로컬 사용자에게 이 폴더에 대한 권한이 없는 경우 에이전트 또는 데이터 수집기를 설치하지 못할 수 있습니다. 를 참조하십시오 <b>"문제 해결"</b> 섹션을 참조하십시오.</p>
네트워크	100Mbps~1Gbps 이더넷 연결, 정적 IP 주소, 모든 디바이스에 대한 IP 연결 및 워크로드 보안 인스턴스(80 또는 443)에 대한 필수 포트.

참고: 워크로드 보안 에이전트는 Data Infrastructure Insights 수집 장치 및/또는 에이전트와 동일한 시스템에 설치할 수 있습니다. 그러나 별도의 컴퓨터에 설치하는 것이 가장 좋습니다. 동일한 시스템에 설치된 경우 아래와 같이 디스크 공간을 할당하십시오.

사용 가능한 디스크 공간입니다	Linux의 경우 디스크 공간을 50GB~55GB로, /opt/NetApp 25-30 GB/var/log/NetApp 25GB로 할당해야 합니다
------------------	--

#### 추가 권장 사항

- NTP(Network Time Protocol) \* 또는 \* SNTP(Simple Network Time Protocol) \* 를 사용하여 ONTAP 시스템과 에이전트 시스템의 시간을 동기화하는 것이 좋습니다.

#### 클라우드 네트워크 액세스 규칙

미국 \* 기반 \* 워크로드 보안 환경:

프로토콜	포트	출처	목적지	설명
TCP	443	워크로드 보안 에이전트	site_name> .cs01.cloudinsights.netapp.com <site_name> .c01.cloudinsights.netapp.com <site_name> .c02.cloudinsights.netapp.com 을 참조하십시오	Data Infrastructure Insights에 액세스
TCP	443	워크로드 보안 에이전트	gateway.c01.cloudinsights.netapp.com agentlogin.cs01.cloudinsights.netapp.com	인증 서비스에 대한 액세스

유럽 기반 \* 워크로드 보안 환경:

프로토콜	포트	출처	목적지	설명
TCP	443	워크로드 보안 에이전트	site_name> .cs01-eu-1.cloudinsights.netapp.com <site_name> .c01-eu-1.cloudinsights.netapp.com <site_name> .c02-eu-1.cloudinsights.netapp.com 을 참조하십시오	Data Infrastructure Insights에 액세스
TCP	443	워크로드 보안 에이전트	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-eu-1.cloudinsights.netapp.com	인증 서비스에 대한 액세스

APAC 기반 \* 워크로드 보안 환경의 경우:

프로토콜	포트	출처	목적지	설명
TCP	443	워크로드 보안 에이전트	site_name> .cs01-ap-1.cloudinsights.netapp.com <site_name> .c01-ap-1.cloudinsights.netapp.com <site_name> .c02-ap-1.cloudinsights.netapp.com 을 참조하십시오	Data Infrastructure Insights에 액세스
TCP	443	워크로드 보안 에이전트	gateway.c01.cloudinsights.netapp.com agentlogin.cs01-ap-1.cloudinsights.netapp.com	인증 서비스에 대한 액세스

네트워크 내 규칙

프로토콜	포트	출처	목적지	설명
TCP	389(LDAP) 636(LDAPS/START-TLS)	워크로드 보안 에이전트	LDAP 서버 URL입니다	LDAP에 연결합니다
TCP	443	워크로드 보안 에이전트	클러스터 또는 SVM 관리 IP 주소(SVM 수집기 구성에 따라 다름)	ONTAP와의 API 통신

프로토콜	포트	출처	목적지	설명
TCP	35000-55000	SVM 데이터 LIF IP 주소	워크로드 보안 에이전트	Fpolicy 이벤트에 대해 ONTAP에서 워크로드 보안 에이전트의 통신 ONTAP가 워크로드 보안 에이전트(있는 경우)에 방화벽을 포함하여 이벤트를 보내려면 이러한 포트를 워크로드 보안 에이전트에 개방해야 합니다. 이러한 포트를 * 모두 * 예약할 필요는 없지만 이 범위 내에 예약하는 포트가 있어야 합니다. 우선 100개 이하의 포트를 예약하여 필요한 경우 늘리는 것이 좋습니다.
TCP	7	워크로드 보안 에이전트	SVM 데이터 LIF IP 주소	Agent에서 SVM 데이터 LIF로 예고
SSH를 클릭합니다	22	워크로드 보안 에이전트	클러스터 관리	CIFS/SMB 사용자 차단에 필요합니다.

## 시스템 사이징

를 참조하십시오 ["이벤트 속도 검사기"](#) 사이징에 대한 정보를 제공하는 문서입니다.

## 워크로드 보안 에이전트 설치

워크로드 보안(이전의 Cloud Secure)은 하나 이상의 에이전트를 사용하여 사용자 활동 데이터를 수집합니다. 에이전트는 사용자 환경의 장치에 연결하여 워크로드 보안 SaaS 계층으로 전송되는 데이터를 수집하여 분석할 수 있습니다. 을 참조하십시오 ["상담원 요구 사항"](#) 에이전트 VM을 구성합니다.

### 시작하기 전에

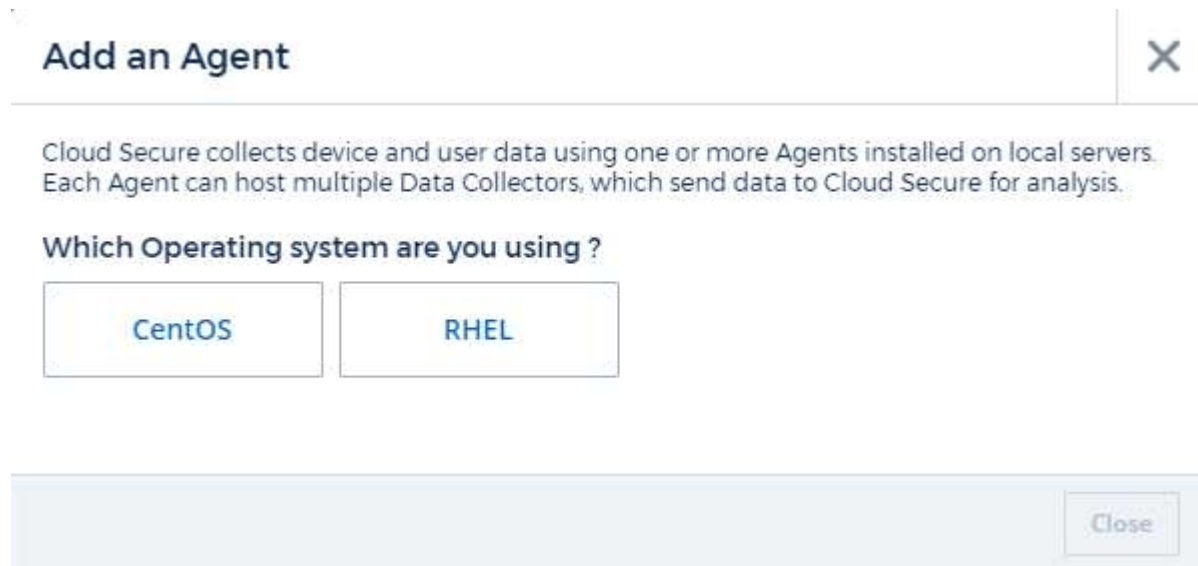
- 설치, 스크립트 실행 및 제거에 sudo 권한이 필요합니다.
- 에이전트를 설치하는 동안 로컬 user\_cssys\_와 로컬 group\_cssys\_가 시스템에 생성됩니다. 권한 설정에서 로컬 사용자 생성을 허용하지 않고 대신 Active Directory가 필요한 경우 사용자 이름이 \_cssys\_인 사용자를 Active Directory 서버에 만들어야 합니다.
- Data Infrastructure Insights 보안에 대해 알아볼 수 ["여기"](#) 있습니다.

### Agent 설치 단계

1. 워크로드 보안 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. Collector > Agents > + Agent \* 를 선택합니다



Agent 추가 페이지가 표시됩니다.



3. 에이전트 서버가 최소 시스템 요구 사항을 충족하는지 확인합니다.
4. 에이전트 서버가 지원되는 Linux 버전을 실행 중인지 확인하려면 `_VERSION SUPPORTED (l)_` 을(를) 클릭합니다.
5. 네트워크에서 프록시 서버를 사용하는 경우 프록시 섹션의 지침에 따라 프록시 서버 세부 정보를 설정하십시오.



## 네트워크 구성

로컬 시스템에서 다음 명령을 실행하여 워크로드 보안에서 사용할 포트를 엽니다. 포트 범위에 대한 보안 문제가 있는 경우, 보다 낮은 포트 범위를 사용할 수 있습니다(예: 35000:35100). 각 SVM은 포트 2개를 사용합니다.

### 단계

1. 'SUDO firewall-cmd—permanent—zone=public—add-port=35000-55000/tcp'로 설정합니다
2. 'SUDO firewall-cmd — reload

플랫폼에 따라 다음 단계를 따르십시오.

- CentOS 7.x/RHEL 7.x \*:
  1. 'SUDO iptables - save | grep 35000'

### 샘플 출력:

```
-A IN_public_allow -p tcp -m tcp --dport 35000:55000 -m conntrack
-ctstate NEW,UNTRACKED -j ACCEPT
* CentOS 8.x/RHEL 8.x *:
```

1. SUDO firewall-cmd—zone=public—list-ports|grep 35000'(CentOS 8의 경우)

### 샘플 출력:

```
35000-55000/tcp
```

## 현재 버전에서 에이전트 "고정"

기본적으로 Data Infrastructure Insights 워크로드 보안은 에이전트를 자동으로 업데이트합니다. 일부 고객은 다음 중 하나가 발생할 때까지 Agent를 현재 버전으로 유지하는 자동 업데이트를 일시 중지할 수 있습니다.

- 고객이 Agent 자동 업데이트를 재개합니다.
- 30일이 지났습니다. 30일은 Agent가 일시 중지된 날이 아니라 가장 최근의 Agent 업데이트 날짜부터 시작됩니다.

이러한 각 경우에 에이전트는 다음 워크로드 보안 새로 고침 시 업데이트됩니다.

자동 에이전트 업데이트를 일시 중지하거나 다시 시작하려면 `_cloudsecure_config.agent_aps`:

## cloudsecure\_config.agents



GET	/v1/cloudsecure/agents	Retrieve all agents.	🔒
POST	/v1/cloudsecure/agents/configuration	Pin all agents under tenant	🔒
DELETE	/v1/cloudsecure/agents/configuration	Unpin all agents under tenant	🔒
POST	/v1/cloudsecure/agents/{agentId}/configuration	Pin an agent under tenant	🔒
DELETE	/v1/cloudsecure/agents/{agentId}/configuration	Unpin an agent under tenant	🔒
GET	/v1/cloudsecure/agents/{agentUuid}	Retrieve an agent by agentUuid.	🔒

일시 중지 또는 다시 시작 작업이 적용되는 데 최대 5분이 소요될 수 있습니다.

현재 Agent 버전은 \* 워크로드 보안 > 수집기 \* 페이지의 \* 에이전트 \* 탭에서 볼 수 있습니다.

### Installed Agents (15)

Name ↑	IP Address	Version	Status
agent-1396	10.128.218.124	1.625.0	Connected

### 상담원 오류 문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제:	해상도:
Agent 설치가 /opt/netapp/cloudsecure/agent/logs/agent.log 폴더를 생성하지 못하고 install.log 파일은 관련 정보를 제공하지 않습니다.	이 오류는 에이전트의 부트스트래핑 중에 발생합니다. 로그 파일이 로거가 초기화되기 전에 발생하므로 이 오류는 로그 파일에 기록되지 않습니다. 오류는 표준 출력으로 리디렉션되며 journalctl -u cloudsecure-agent.service 명령을 사용하여 서비스 로그에 표시됩니다. 이 명령을 사용하여 문제를 추가로 해결할 수 있습니다. est
에이전트 설치가 '이 Linux 배포는 지원되지 않습니다. 설치를 종료하는 중입니다.	이 오류는 지원되지 않는 시스템에 Agent를 설치하려고 할 때 나타납니다. 을 참조하십시오 " <a href="#">상담원 요구 사항</a> ".
"-bash:unzip:command not found" 오류와 함께 에이전트 설치가 실패했습니다.	압축을 푼 다음 설치 명령을 다시 실행합니다. 시스템에 Yum이 설치되어 있는 경우 "yum install unzip"을 시도하여 unzip 소프트웨어를 설치합니다. 그런 다음 Agent 설치 UI에서 명령을 다시 복사하여 CLI에 붙여 넣어 설치를 다시 실행합니다.

문제:	해상도:
에이전트가 설치되어 실행 중입니다. 하지만 상담원이 갑자기 중지되었습니다.	<p>Agent 시스템에 SSH를 연결합니다. 를 통해 상담원 서비스의 상태를 확인합니다 <code>sudo systemctl status cloudsecure-agent.service</code>. 로그에 "Failed to start Workload Security daemon service(워크로드 보안 데몬 서비스를 시작하지 못했습니다)"라는 메시지가 표시되는지 확인합니다. <code>cssys</code> 사용자가 Agent 시스템에 있는지 여부를 확인합니다. 루트 권한으로 다음 명령을 하나씩 실행하고 <code>cssys</code> 사용자 및 그룹이 있는지 확인합니다.</p> <pre>sudo id cssys</pre> <p><code>sudo groups cssys`</code> 아무 것도 없는 경우 중앙 모니터링 정책이 <code>cssys</code> 사용자를 삭제했을 수 있습니다. 다음 명령을 실행하여 <code>cssys</code> 사용자 및 그룹을 수동으로 생성합니다.</p> <pre>`sudo useradd cssys` `sudo groupadd cssys`</pre> <p>다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다.</p> <pre>`sudo systemctl restart cloudsecure-agent.service`</pre> <p>여전히 실행되지 않는 경우 다른 문제 해결 옵션을 확인하십시오.</p>
Agent에 50개 이상의 데이터 수집기를 추가할 수 없습니다.	데이터 수집기는 50개만 에이전트에 추가할 수 있습니다. Active Directory, SVM 및 기타 수집기와 같은 모든 수집기 유형의 조합이 될 수 있습니다.
UI에 Agent가 NOT_Connected 상태임 이 표시됩니다.	Agent를 다시 시작하는 단계입니다. Agent 시스템에 SSH를 연결합니다. 다음 명령을 실행하여 에이전트 서비스를 다시 시작합니다. <code>sudo systemctl restart cloudsecure-agent.service`</code> 3. 'SUDO <code>systemctl status cloudsecure-agent.service`</code> 를 통해 상담원 서비스의 상태를 확인합니다. 4. 상담원은 연결된 상태로 이동해야 합니다.
에이전트 VM이 Zscaler 프록시 뒤에 있으며 에이전트 설치가 실패합니다. Zscaler 프록시의 SSL 검사로 인해 워크로드 보안 인증서는 Zscaler CA에 의해 서명된 것으로 표시되므로 에이전트가 통신을 신뢰하지 않습니다.	.cloudinsights.netapp.com URL의 Zscaler 프록시에서 SSL 검사를 비활성화합니다. Zscaler가 SSL 검사를 수행하고 인증서를 대체하는 경우 Workload Security가 작동하지 않습니다.
에이전트를 설치하는 동안 압축 해제 후 설치가 중단됩니다.	<p>"<code>chmod 755-rf</code>" 명령이 실패했습니다. 작업 디렉토리에 파일이 있고 다른 사용자에게 속해 있으며 해당 파일의 사용 권한을 변경할 수 없는 루트가 아닌 <code>sudo</code> 사용자가 에이전트 설치 명령을 실행하는 경우 명령이 실패합니다. <code>chmod</code> 명령이 실패하여 나머지 설치가 실행되지 않습니다. "cloudsecure"라는 새 디렉토리를 생성합니다. 해당 디렉토리로 이동합니다. 전체 "토큰 =....."을 복사하여 붙여 넣습니다. ... / <code>cloudsecure-agent-install.sh</code>" 설치 명령을 입력하고 Enter 키를 누릅니다. 4. 설치를 계속할 수 있어야 합니다.</p>

<p>문제:</p> <p>Agent가 여전히 SaaS에 연결할 수 없는 경우 NetApp Support로 사례를 여십시오. Data Infrastructure Insights 일련 번호를 제공하여 케이스를 생성하고 언급된 대로 로그에 로그를 첨부합니다.</p>	<p>해상도:</p> <p>케이스에 로그를 첨부하려면 1. 루트 권한으로 다음 스크립트를 실행하고 출력 파일(cloudsecure-agent-symptoms.zip)을 공유합니다. a. /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 2. 루트 권한으로 다음 명령을 하나씩 실행하고 출력을 공유합니다. a. ID cssys b. 그룹 cssys c. CAT/etc/OS - 릴리스</p>
<p>cloudsecure-agent-symptom-collector.sh 스크립트가 실패하고 다음 오류가 표시됩니다. [root@machine tmp]#/opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh 서비스 로그 수집 애플리케이션 로그 수집 에이전트 상태 스냅샷 생성 에이전트 디렉토리 구조 스냅샷 생성..... . ..... . /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent-symptom-collector.sh:line 52:zip: 명령을 찾을 수 없음 오류: /tmp/cloudsecure-agent-symptoms.zip 생성하지 못했습니다</p>	<p>zip 도구가 설치되지 않았습니다. "yum install zip" 명령을 실행하여 zip 툴을 설치합니다. 그런 다음 cloudsecure-agent-symptom-collector.sh 를 다시 실행합니다.</p>
<p>useradd를 사용하여 에이전트 설치가 실패했습니다. 디렉토리 /home/cssys를 생성할 수 없습니다</p>	<p>이 오류는 권한 부족으로 인해 /home 아래에 사용자의 로그인 디렉토리를 만들 수 없는 경우에 발생할 수 있습니다. 해결 방법은 cssys 사용자를 생성하고 다음 명령을 사용하여 로그인 디렉토리를 수동으로 추가하는 것입니다. <code>sudo useradd user_name -m -d home_DIR</code> -m: 사용자의 홈 디렉토리가 없는 경우 생성합니다. d: 사용자의 로그인 디렉토리 값으로 HOME_DIR을 사용하여 새 사용자가 생성됩니다. 예를 들어, <code>_sudo useradd cssys -m -d /cssys_는 user_cssys_를</code> 추가하고 root 아래에 로그인 디렉토리를 만듭니다.</p>
<p>설치 후 에이전트가 실행되고 있지 않습니다. <code>Systemctl status cloudsecure-agent.service</code> 다음과 같이 표시합니다. [root@demo~]#systemctl status cloudsecure-agent.service agent.service – Workload Security Agent Daemon Service loaded: loaded(/usr/lib/systemd/system/cloudsecure-agent.service; enabled; vendor preset: disabled) Active: 활성화(자동 재시작) (결과: 종료 코드) Tue 2021:12:26 PDT; 228.2s 시작 에이전트 pid=25pid=secure agent.pid/service: 25889(code=Exited, status=126), Aug 03 21:12:26 demo systemd [1]: cloudsecure-agent.service: main process 종료, code=Exited, status=126/n/a Aj8 03 21:12:26 demo systemd [1]: unit cloudsecure-agent.service failed state. 8월 03 21:12:26 데모 시스템[1]: cloudsecure-agent.service 실패.</p>	<p>cssys_user에 설치 권한이 없을 수 있으므로 이 작업은 실패할 수 있습니다. /opt/netapp가 NFS 마운트이고 _cssys_user가 이 폴더에 대한 액세스 권한이 없는 경우 설치가 실패합니다. _cssys_는 워크로드 보안 설치 관리자가 생성한 로컬 사용자이며 마운트된 공유에 액세스할 권한이 없을 수 있습니다. cssys_user를 사용하여 /opt/netapp/cloudsecure/agent/bin/cloudsecure-agent에 액세스하여 이를 확인할 수 있습니다. "사용 권한 거부"를 반환하면 설치 권한이 없는 것입니다. 마운트된 폴더 대신 컴퓨터에 로컬 디렉토리에 설치합니다.</p>

문제:	해상도:
Agent가 처음에 프록시 서버를 통해 연결되었고 Agent 설치 중에 프록시가 설정되었습니다. 이제 프록시 서버가 변경되었습니다. Agent의 프록시 구성을 변경하려면 어떻게 해야 하나요?	agent.properties 를 편집하여 프록시 세부 정보를 추가할 수 있습니다. 다음 단계를 따르십시오. 1. 속성 파일이 포함된 폴더로 변경합니다. cd /opt/netapp/cloudsecure/conf 2. 즐겨찾기 텍스트 편집기를 사용하여 편집할 agent.properties 파일을 엽니다. 다음 행을 추가하거나 수정합니다. agent_proxy_host=scspa1950329001.vm.netapp.com agent_proxy_port=80 agent_proxy_user=pxuser agent_proxy_password=pass1234 4. 파일을 저장합니다. 에이전트를 다시 시작합니다. sudo systemctl cloudsecure-agent.service 다시 시작합니다

## 워크로드 보안 에이전트를 삭제하는 중입니다

Workload Security Agent를 삭제하면 Agent와 연결된 모든 데이터 수집기가 먼저 삭제되어야 합니다.

### 상담원 삭제



Agent를 삭제하면 Agent와 연결된 모든 Data Collector가 삭제됩니다. 다른 에이전트로 데이터 수집기를 구성하려는 경우 에이전트를 삭제하기 전에 Data Collector 구성의 백업을 만들어야 합니다.

### 시작하기 전에

1. 에이전트와 연결된 모든 데이터 수집기가 워크로드 보안 포털에서 삭제되었는지 확인합니다.

참고: 연결된 모든 수집기가 중지 상태인 경우 이 단계를 무시하십시오.

### 에이전트를 삭제하는 단계:

1. 에이전트 VM에 SSH를 수행하고 다음 명령을 실행합니다. 메시지가 표시되면 "y"를 입력하여 계속합니다.

```
sudo /opt/netapp/cloudsecure/agent/install/cloudsecure-agent-uninstall.sh
Uninstall CloudSecure Agent? [y|N]:
```

2. Workload Security > Collector > Agents \* 를 클릭합니다

구성된 에이전트 목록이 표시됩니다.

3. 삭제하려는 상담원의 옵션 메뉴를 누릅니다.
4. 삭제 \* 를 클릭합니다.

시스템에 \* Delete Agent \* 페이지가 표시됩니다.

5. 삭제를 확인하려면 \* 삭제 \* 를 클릭합니다.

## AD(Active Directory) 사용자 디렉토리 수집기 구성

Active Directory 서버에서 사용자 속성을 수집하도록 워크로드 보안을 구성할 수 있습니다.

시작하기 전에

- 이 작업을 수행하려면 Data Infrastructure Insights 관리자 또는 계정 소유자여야 합니다.
- Active Directory 서버를 호스팅하는 서버의 IP 주소가 있어야 합니다.
- 사용자 디렉터리 커넥터를 구성하기 전에 Agent를 구성해야 합니다.

사용자 디렉토리 수집기를 구성하는 단계입니다

1. 워크로드 보안 메뉴에서 다음을 클릭합니다.

- Collectors > 사용자 디렉토리 수집기 > + 사용자 디렉토리 수집기 \* 를 선택하고 \* Active Directory \* 를 선택합니다

사용자 디렉토리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉토리 수집기를 구성합니다.

이름	설명
이름	사용자 디렉토리의 고유 이름입니다. 예: <i>GlobalADCollector</i>
에이전트	목록에서 구성된 에이전트를 선택합니다
서버 IP/도메인 이름	Active Directory를 호스팅하는 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다
포리스트 이름	디렉터리 구조의 포리스트 수준입니다. 포리스트 이름을 사용하면 SVM에 있는 것과 같은 <i>x.x.y.z</i> ⇒ 직접 도메인 이름을 사용할 수 있습니다. <i>dc=x, dc=y, dc=z</i> ⇒ 상대 고유 이름 [예: <i>dc=HQ, dc=CompanyName, dc=com</i> ] 또는 다음과 같이 지정할 수 있습니다. <i>OU=engineering,DC=HQ,DC=CompanyName,DC=com</i> [특정 OU 엔지니어링으로 필터링하기] <i>]CN=username,OU=engineering,DC=CompanyName,DC=NetApp,DC=com</i> [OU<engineering>에서 특정 사용자만 가져오려면] <i>_CN=Acrobat=Users,CN=Users,DC=Users,DC=Users,DC=CompanyName=Active,MA_DC=Users,CompanyName=Trusted,DC=Active_DC=CompanyName=CompanyName=Users=Active,DC=CompanyName=CompanyName=CompanyName=Users,DC=CompanyName=CompanyName=A,DC=Users,DC=CompanyName=</i>
DN 바인딩	사용자가 디렉터리를 검색할 수 있습니다. 예: <i>username@companyname.com</i> 또는 <i>username@domainname.com</i> 또한 도메인 읽기 전용 권한이 필요합니다. 사용자는 보안 그룹 <i>_읽기 전용 도메인 컨트롤러_</i> 의 구성원이어야 합니다.



암호를 바인딩합니다	디렉터리 서버 암호(예: Bind DN에서 사용되는 사용자 이름의 암호)
프로토콜	LDAP, LDAPS, LDAP-START-TLS
포트	포트를 선택합니다

Active Directory에서 기본 속성 이름이 수정된 경우 다음 Directory Server 필수 속성을 입력합니다. 이러한 속성 이름은 대부분 Active Directory에서 `_not_modified`입니다. 이 경우 기본 속성 이름을 사용하여 간단하게 진행할 수 있습니다.

속성	Directory Server의 속성 이름입니다
표시 이름	이름
SID	객체 ID입니다
사용자 이름	sAMAccountName

다음 특성을 추가하려면 선택적 특성 포함 을 클릭합니다.

속성	Directory Server의 속성 이름입니다
이메일 주소	메일
전화 번호	전화 번호
역할	제목
국가	CO
상태	상태
부서	부서
사진	축소판 그림
관리자 DN	관리자
그룹	멤버

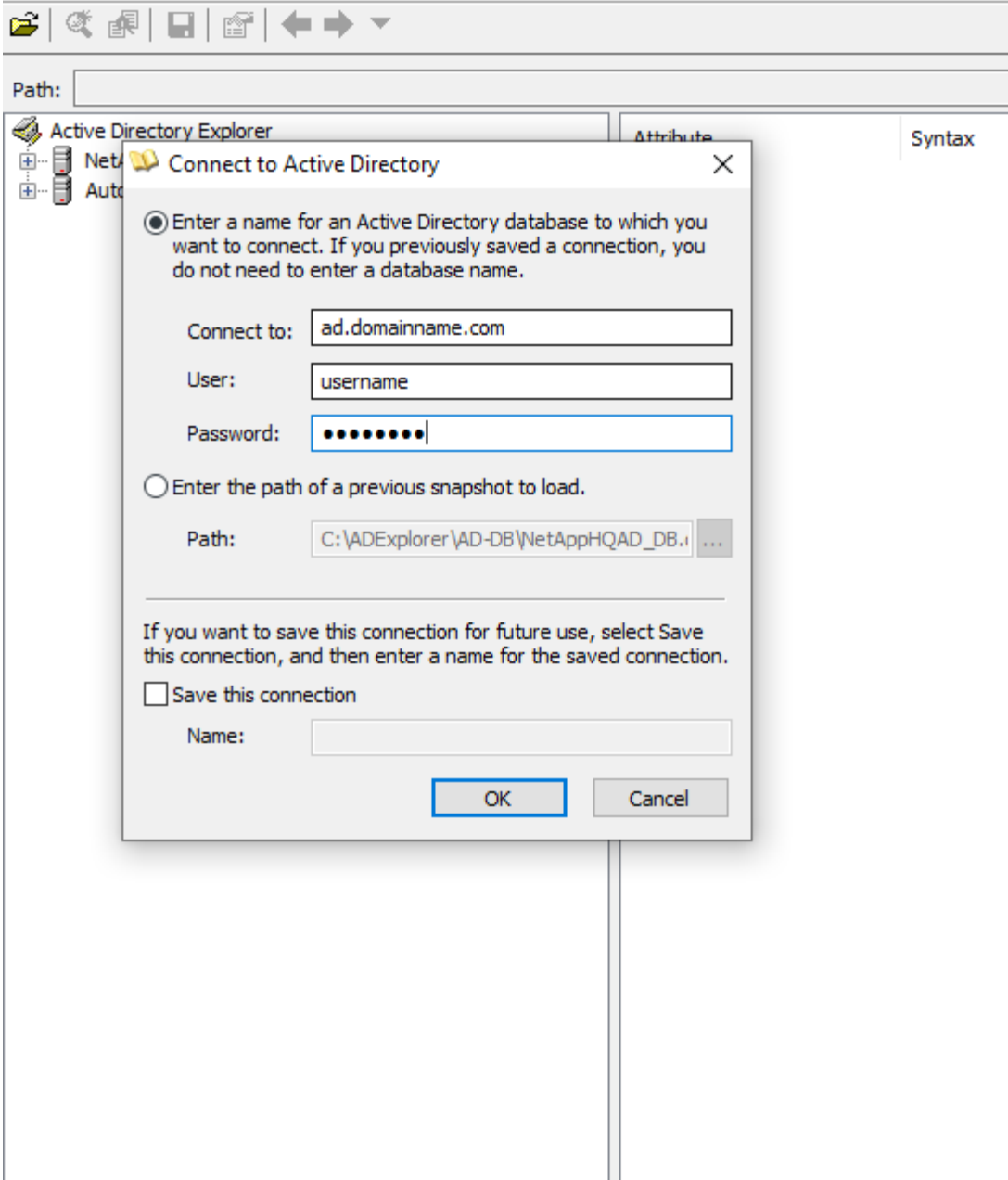
사용자 디렉토리 수집기 구성을 테스트하는 중입니다

다음 절차를 사용하여 LDAP 사용자 권한 및 속성 정의의 유효성을 검사할 수 있습니다.

- 다음 명령을 사용하여 워크로드 보안 LDAP 사용자 권한을 검증합니다.

```
"ldapsearch-o LDIF-Wrap=no-ll-x-b" dc=netapp,dc=com"-h 10.235.40.29-p 389-DAdministrator@netapp.com -W"
```

- AD 탐색기를 사용하여 AD 데이터베이스를 탐색하고, 개체 속성 및 특성을 보고, 사용 권한을 보고, 개체의 스키마를 보고, 저장하고 다시 실행할 수 있는 정교한 검색을 실행할 수 있습니다.
  - 설치합니다 **"AD 탐색기"** AD 서버에 연결할 수 있는 모든 Windows 시스템에서
  - AD 디렉토리 서버의 사용자 이름/암호를 사용하여 AD 서버에 연결합니다.



### 사용자 디렉토리 수집기 구성 오류 문제 해결

다음 표에서는 수집기 구성 중에 발생할 수 있는 알려진 문제와 해결 방법을 설명합니다.

문제:	해상도:
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 서버에 대해 잘못된 자격 증명이 제공되었습니다."라는 오류가 표시됩니다.	잘못된 사용자 이름 또는 암호가 제공되었습니다. 올바른 사용자 이름 및 암호를 편집하고 제공하십시오.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "DN=DC=HQ, DC=domainname, DC=com에 해당하는 객체를 포리스트 이름으로 가져오지 못했습니다."라는 오류가 표시됩니다.	잘못된 포리스트 이름이 제공되었습니다. 올바른 포리스트 이름을 편집하고 제공하십시오.

문제:	해상도:
도메인 사용자의 선택적 속성이 워크로드 보안 사용자 프로필 페이지에 나타나지 않습니다.	이는 CloudSecure에 추가된 선택적 속성의 이름과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 올바른 선택적 속성 이름을 편집하고 제공하십시오.
"LDAP 사용자를 검색하지 못했습니다. 실패 원인: 서버에 연결할 수 없습니다. 연결이 null입니다."	<i>Restart</i> 단추를 클릭하여 수집기를 다시 시작합니다.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다.	필수 필드(서버, 포리스트-이름, 바인드-DN, 바인드-암호)에 대해 유효한 값을 제공했는지 확인합니다. bind-DN 입력이 항상 'Administrator@<domain_forest_name>' 또는 도메인 관리자 권한이 있는 사용자 계정으로 제공되는지 확인합니다.
사용자 디렉토리 커넥터를 추가하면 '다시 시도 중' 상태가 됩니다. "Collector의 상태를 정의할 수 없습니다. 원인 TCP 명령 [Connect(localhost:35012, None, List(), some(seconds), true)] 오류가 java.net.ConnectionException:Connection refused 때문에 실패했습니다."	AD 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 연결을 설정하지 못했습니다."라는 오류가 표시됩니다.	AD 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다.
사용자 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "설정을 로드하지 못했습니다. 원인: DataSource 구성에 오류가 있습니다. 특정 이유: /connector/conf/application.conf: 70: ldap.ldap-port에 숫자가 아닌 유형 문자열이 있습니다."	잘못된 포트 값이 제공되었습니다. AD 서버에 대한 기본 포트 값 또는 올바른 포트 번호를 사용해 보십시오.
나는 필수 속성을 시작했는데 효과가 있었습니다. 옵션 특성 데이터를 추가한 후 선택적 특성 데이터를 AD에서 가져오지 않습니다.	이는 CloudSecure에 추가된 옵션 속성과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 올바른 필수 또는 선택적 속성 이름을 편집하고 제공하십시오.
Collector를 다시 시작한 후 AD 동기화는 언제 발생합니까?	수집기가 다시 시작된 후 즉시 AD 동기화가 수행됩니다. 약 30만 명의 사용자가 있는 사용자 데이터를 가져오는 데 약 15분이 소요되며, 12시간마다 자동으로 새로 고쳐집니다.
사용자 데이터가 AD에서 CloudSecure로 동기화됩니다. 언제 데이터가 삭제됩니까?	새로 고침이 없는 경우 사용자 데이터는 13개월 동안 유지됩니다. 테넌트가 삭제되면 데이터가 삭제됩니다.
사용자 디렉토리 커넥터를 사용하면 '오류' 상태가 됩니다. "커넥터가 오류 상태입니다. 서비스 이름: usersLdap. 실패 원인: LDAP 사용자를 검색하지 못했습니다. 실패 원인:80090308:LdapErr:DSID-0C090453, 설명:AcceptSecurityContext 오류, 데이터 52e, v3839"	잘못된 포리스트 이름이 제공되었습니다. 올바른 포리스트 이름을 제공하는 방법은 위의 을 참조하십시오.

문제:	해상도:
전화 번호가 사용자 프로필 페이지에 채워지지 않습니다.	이는 Active Directory의 속성 매핑 문제 때문일 수 있습니다. Active Directory에서 사용자 정보를 가져오는 특정 Active Directory 수집기를 편집합니다. 2.알림 옵션 속성에 따라 "전화 번호" 필드 이름이 Active Directory 속성 '전화 번호'에 매핑되어 있습니다. 4.이제 위에 설명된 대로 Active Directory 탐색기 도구를 사용하여 Active Directory를 탐색하고 올바른 속성 이름을 확인하십시오. Active Directory에 사용자의 전화 번호가 있는 '전화 번호'라는 속성이 있는지 확인합니다. 5.Active Directory에서 'phonenumber'로 수정되었다고 가정해 보겠습니다. 그런 다음 CloudSecure 사용자 디렉토리 수집기를 편집합니다. 옵션 속성 섹션에서 '전화 번호'를 '전화 번호'로 바꿉니다. Active Directory Collector를 저장하면 수집기가 다시 시작되고 사용자의 전화 번호가 표시되며 사용자 프로필 페이지에 동일한 번호가 표시됩니다.
AD(Active Directory) 서버에서 암호화 인증서(SSL)가 활성화된 경우 워크로드 보안 사용자 디렉토리 수집기는 AD 서버에 연결할 수 없습니다.	사용자 디렉토리 수집기를 구성하기 전에 AD 서버 암호화를 비활성화하십시오. 사용자 세부 정보를 가져오면 13개월 동안 표시됩니다. 사용자 세부 정보를 가져온 후 AD 서버의 연결이 끊기면 AD에서 새로 추가된 사용자들 가져오지 않습니다. 다시 가져오려면 사용자 디렉토리 수집기를 AD에 연결해야 합니다.
Active Directory의 데이터는 CloudInsights Security에 있습니다. CloudInsights에서 모든 사용자 정보를 삭제하려는 경우	CloudInsights 보안에서는 Active Directory 사용자 정보만 삭제할 수 없습니다. 사용자를 삭제하려면 전체 테넌트를 삭제해야 합니다.

## LDAP Directory Server Collector 구성

LDAP 디렉토리 서버에서 사용자 속성을 수집하도록 워크로드 보안을 구성합니다.

시작하기 전에

- 이 작업을 수행하려면 Data Infrastructure Insights 관리자 또는 계정 소유자여야 합니다.
- LDAP 디렉토리 서버를 호스팅하는 서버의 IP 주소가 있어야 합니다.
- LDAP 디렉토리 커넥터를 구성하기 전에 Agent를 구성해야 합니다.

사용자 디렉토리 수집기를 구성하는 단계입니다

1. 워크로드 보안 메뉴에서 다음을 클릭합니다.

- Collectors > 사용자 디렉토리 수집기 > + 사용자 디렉토리 수집기 \* 를 선택하고 \* LDAP 디렉토리 서버 \* 를 선택합니다

사용자 디렉토리 추가 화면이 표시됩니다.

다음 표에 필요한 데이터를 입력하여 사용자 디렉토리 수집기를 구성합니다.

이름	설명
이름	사용자 디렉토리의 고유 이름입니다. 예: <i>GlobalLDAPCollector</i>

에이전트	목록에서 구성된 에이전트를 선택합니다
서버 IP/도메인 이름	LDAP 디렉토리 서버를 호스팅하는 서버의 IP 주소 또는 FQDN(정규화된 도메인 이름)입니다
검색 기준	LDAP 서버 검색 기반의 검색 기준을 사용하면 SVM에 있는 대로 <i>x.x.y.z</i> ⇒직접 도메인 이름 형식을 모두 사용할 수 있습니다. <i>dc=x, dc=y, dc=z</i> ⇒ 상대 고유 이름 [예: <i>dc=HQ, dc=CompanyName, dc=com</i> ] 또는 다음과 같이 지정할 수 있습니다. <i>OU=engineering,DC=HQ,DC=CompanyName,DC=com</i> [특정 OU 엔지니어링으로 필터링하기] <i>]CN=username,OU=engineering,DC=CompanyName,DC=NetApp,DC=com</i> [OU<engineering>에서 특정 사용자만 가져오려면] <i>CN=Acrobat,Users,CN=Users,DC=Users,DC=CompanyName=Boston,DC=CompanyName=CompanyN,DC=CompanyUS,DC=CompanyName=Users,DC=CompanyName=CompanyS,DC=CompanyName=CompanyName=CompanyName=CompanyName=CompanyName=CompanyName=CompanyName=CompanyName=</i>
DN 바인딩	사용자가 디렉터리를 검색할 수 있습니다. 예를 들어 <i>uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyName,dc=com</i> <i>uid=john,cn=users,cn=accounts,dc=dorp,dc=company,dc=com</i> for a user <a href="mailto:john@dorp.company.com">john@dorp.company.com</a> 입니다. <i>dorp.company.com</i>
계정	사용자
요한입니다	강혜린
암호를 바인딩합니다	디렉터리 서버 암호(예: Bind DN에서 사용되는 사용자 이름의 암호)
프로토콜	LDAP, LDAPS, LDAP-START-TLS
포트	포트를 선택합니다

LDAP Directory Server에서 기본 속성 이름이 수정된 경우 다음 Directory Server 필수 속성을 입력합니다. 대부분의 경우 이러한 속성 이름은 LDAP Directory Server에서 `_not_modified`입니다. 이 경우 기본 속성 이름을 사용하여 간단하게 진행할 수 있습니다.

속성	Directory Server의 속성 이름입니다
표시 이름	이름
UNIXID	uidNumber(uidNumber)
사용자 이름	UID

다음 특성을 추가하려면 선택적 특성 포함 을 클릭합니다.

속성	Directory Server의 속성 이름입니다
이메일 주소	메일

전화 번호	전화 번호
역할	제목
국가	CO
상태	상태
부서	부서 번호
사진	사진
관리자 DN	관리자
그룹	멤버

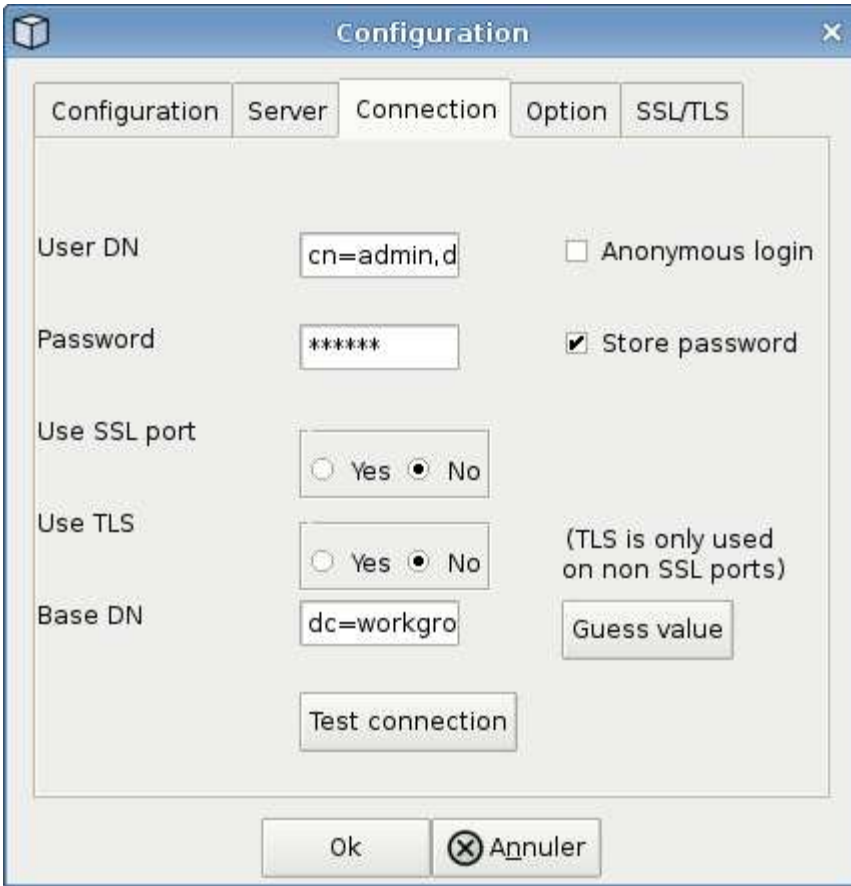
사용자 디렉토리 수집기 구성을 테스트하는 중입니다

다음 절차를 사용하여 LDAP 사용자 권한 및 속성 정의의 유효성을 검사할 수 있습니다.

- 다음 명령을 사용하여 워크로드 보안 LDAP 사용자 권한을 검증합니다.

```
ldapsearch -D "uid=john
,cn=users,cn=accounts,dc=dorp,dc=company,dc=com" -W -x -LLL -o ldif-
wrap=no -b "cn=accounts,dc=dorp,dc=company,dc=com" -H
ldap://vmwipaapp08.dorp.company.com
* LDAP 탐색기를 사용하여 LDAP 데이터베이스를 탐색하고, 개체 속성 및 속성을 보고,
권한을 보고, 개체의 스키마를 보고, 저장하고 다시 실행할 수 있는 정교한 검색을 실행할 수
있습니다.
```

- LDAP 탐색기를 설치합니다 또는 Java LDAP Explorer를 선택합니다 LDAP 서버에 연결할 수 있는 모든 Windows 시스템에서
- LDAP 디렉토리 서버의 사용자 이름/암호를 사용하여 LDAP 서버에 연결합니다.



### LDAP 디렉토리 수집기 구성 오류 문제 해결

다음 표에서는 수집기 구성 중에 발생할 수 있는 알려진 문제와 해결 방법을 설명합니다.

문제:	해상도:
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 서버에 대해 잘못된 자격 증명이 제공되었습니다."라는 오류가 표시됩니다.	잘못된 바인딩 DN 또는 바인딩 비밀번호 또는 검색 기준을 제공했습니다. 올바른 정보를 편집하고 제공하십시오.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "DN=DC=HQ, DC=domainname, DC=com에 해당하는 객체를 포리스트 이름으로 가져오지 못했습니다."라는 오류가 표시됩니다.	잘못된 검색 기준을 제공했습니다. 올바른 포리스트 이름을 편집하고 제공하십시오.
도메인 사용자의 선택적 속성이 워크로드 보안 사용자 프로필 페이지에 나타나지 않습니다.	이는 CloudSecure에 추가된 선택적 속성의 이름과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 필드는 대/소문자를 구분합니다. 올바른 선택적 속성 이름을 편집하고 제공하십시오.
"LDAP 사용자를 검색하지 못했습니다. 실패 원인: 서버에 연결할 수 없습니다. 연결이 null입니다."	<b>Restart</b> 단추를 클릭하여 수집기를 다시 시작합니다.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다.	필수 필드(서버, 포리스트-이름, 바인드-DN, 바인드-암호)에 대해 유효한 값을 제공했는지 확인합니다. bind-DN 입력은 항상 uid=ldapuser,cn=users,cn=accounts,dc=domain,dc=companyName,dc=com으로 제공되어야 합니다.

문제:	해상도:
LDAP 디렉토리 커넥터를 추가하면 '다시 시도 중' 상태가 됩니다. "수집기의 상태를 확인하지 못하여 다시 시도하는 중" 오류가 표시됩니다.	올바른 서버 IP 및 검색 기준을 제공했는지 확인합니다. //
LDAP 디렉토리를 추가하는 동안 다음과 같은 오류가 표시됩니다. "2회 재시도 내에 Collector의 상태를 확인하지 못했습니다. 수집기를 다시 시작하십시오(오류 코드: AGENT008)."	올바른 서버 IP 및 검색 기준을 제공했는지 확인합니다
LDAP 디렉토리 커넥터를 추가하면 '다시 시도 중' 상태가 됩니다. "Collector의 상태를 정의할 수 없습니다. 원인 TCP 명령 [Connect(localhost:35012, None, List(), some(,seconds), true)] 오류가 java.net.ConnectionException:Connection refused 때문에 실패했습니다."	AD 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다. ///
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "LDAP 연결을 설정하지 못했습니다."라는 오류가 표시됩니다.	LDAP 서버에 대해 잘못된 IP 또는 FQDN이 제공되었습니다. 올바른 IP 주소 또는 FQDN을 편집하고 입력합니다. 또는 잘못된 포트 값이 제공되었습니다. LDAP 서버에 대한 기본 포트 값 또는 올바른 포트 번호를 사용해 보십시오.
LDAP 디렉토리 커넥터를 추가하면 '오류' 상태가 됩니다. "설정을 로드하지 못했습니다. 원인: DataSource 구성에 오류가 있습니다. 특정 이유: /connector/conf/application.conf: 70: ldap.ldap-port에 숫자가 아닌 유형 문자열이 있습니다."	잘못된 포트 값이 제공되었습니다. AD 서버에 대한 기본 포트 값 또는 올바른 포트 번호를 사용해 보십시오.
나는 필수 속성을 시작했는데 효과가 있었습니다. 옵션 특성 데이터를 추가한 후 선택적 특성 데이터를 AD에서 가져오지 않습니다.	이는 CloudSecure에 추가된 옵션 속성과 Active Directory의 실제 속성 이름이 일치하지 않기 때문일 수 있습니다. 올바른 필수 또는 선택적 속성 이름을 편집하고 제공하십시오.
Collector를 다시 시작한 후 LDAP 동기화는 언제 이루어집니까?	LDAP 동기화는 수집기가 다시 시작된 직후에 수행됩니다. 약 30만 명의 사용자가 있는 사용자 데이터를 가져오는 데 약 15분이 소요되며, 12시간마다 자동으로 새로 고쳐집니다.
사용자 데이터가 LDAP에서 CloudSecure로 동기화됩니다. 언제 데이터가 삭제됩니까?	새로 고침이 없는 경우 사용자 데이터는 13개월 동안 유지됩니다. 테넌트가 삭제되면 데이터가 삭제됩니다.
LDAP 디렉토리 커넥터를 사용하면 '오류' 상태가 됩니다. "커넥터가 오류 상태입니다. 서비스 이름: usersLdap. 실패 원인: LDAP 사용자를 검색하지 못했습니다. 실패 원인:80090308:LdapErr:DSID-0C090453, 설명:AcceptSecurityContext 오류, 데이터 52e, v3839"	잘못된 포리스트 이름이 제공되었습니다. 올바른 포리스트 이름을 제공하는 방법은 위의 을 참조하십시오.



문제:	해상도:
전화 번호가 사용자 프로필 페이지에 채워지지 않습니다.	이는 Active Directory의 속성 매핑 문제 때문일 수 있습니다. Active Directory에서 사용자 정보를 가져오는 특정 Active Directory 수집기를 편집합니다. 2.알림 옵션 속성에 따라 "전화 번호" 필드 이름이 Active Directory 속성 '전화 번호'에 매핑되어 있습니다. 4.이제 위에 설명된 대로 Active Directory 탐색기 도구를 사용하여 LDAP 디렉터리 서버를 검색하고 올바른 속성 이름을 확인하십시오. LDAP 디렉터리에 사용자의 전화 번호가 있는 '전화 번호'라는 속성이 있는지 확인합니다. LDAP 디렉터리에서 'phonenummer'로 수정되었다고 가정해 보겠습니다. 그런 다음 CloudSecure 사용자 디렉토리 수집기를 편집합니다. 옵션 속성 섹션에서 '전화 번호'를 '전화 번호'로 바꿉니다. Active Directory Collector를 저장하면 수집기가 다시 시작되고 사용자의 전화 번호가 표시되며 사용자 프로필 페이지에 동일한 번호가 표시됩니다.
AD(Active Directory) 서버에서 암호화 인증서(SSL)가 활성화된 경우 워크로드 보안 사용자 디렉토리 수집기는 AD 서버에 연결할 수 없습니다.	사용자 디렉토리 수집기를 구성하기 전에 AD 서버 암호화를 비활성화하십시오. 사용자 세부 정보를 가져오면 13개월 동안 표시됩니다. 사용자 세부 정보를 가져온 후 AD 서버의 연결이 끊기면 AD에서 새로 추가된 사용자를 가져오지 않습니다. 다시 가져오려면 사용자 디렉토리 수집기를 AD에 연결해야 합니다.

## ONTAP SVM Data Collector 구성

워크로드 보안은 데이터 수집기를 사용하여 디바이스에서 파일 및 사용자 액세스 데이터를 수집합니다.

시작하기 전에

- 이 데이터 수집기는 다음 구성 요소를 통해 지원됩니다.
  - Data ONTAP 9.2 이상 버전 최상의 성능을 얻으려면 9.13.1 이상의 Data ONTAP 버전을 사용하십시오.
  - SMB 프로토콜 버전 3.1 이하
  - ONTAP 9.15.1 이상이 설치된 NFS 4.1까지의 NFS 버전
  - FlexGroup는 ONTAP 9.4 이상 버전에서 지원됩니다
  - ONTAP Select가 지원됩니다
- 데이터 유형 SVM만 지원됩니다. 무한 확장 볼륨이 있는 SVM은 지원되지 않습니다.
- SVM에는 여러 가지 하위 유형이 있습니다. 이 중 *DEFAULT*, *SYNC\_SOURCE* 및 *SYNC\_DESTINATION* 만 지원됩니다.
- 상담원 "**구성해야 합니다**" 데이터 수집기를 구성하기 전에
- 올바르게 구성된 사용자 디렉토리 커넥터가 있는지 확인합니다. 그렇지 않으면 이벤트가 인코딩된 사용자 이름을 표시하고 "Activity Forensics(활동 포렌식)" 페이지에 사용자의 실제 이름(Active Directory에 저장된 이름)을 표시하지 않습니다.
- • ONTAP 영구 저장소는 9.14.1부터 지원됩니다.

- 최적의 성능을 위해 FPolicy 서버를 스토리지 시스템과 동일한 서브넷에 구성해야 합니다.
- 다음 두 가지 방법 중 하나를 사용하여 SVM을 추가해야 합니다.
  - 클러스터 IP, SVM 이름, 클러스터 관리 사용자 이름 및 암호를 사용합니다. 이 방법은 \* \_ 을(를) 사용하는 것이 좋습니다
    - SVM 이름은 ONTAP에 표시된 대로 대소문자를 구분합니다.
  - SVM Vserver 관리 IP, 사용자 이름 및 암호를 사용합니다
  - 전체 관리자 클러스터/SVM 관리 사용자 이름 및 암호를 사용할 수 없거나 사용할 수 없는 경우 에 설명된 대로 더 낮은 권한으로 사용자 지정 사용자를 생성할 수 있습니다 "권한에 대한 참고 사항" 섹션을 참조하십시오. 이 맞춤형 사용자는 SVM 또는 클러스터 액세스를 위해 생성할 수 있습니다.
    - ◦ 아래 "권한에 대한 참고 사항" 섹션에서 언급한 csrole 이상의 권한이 있는 역할을 가진 AD 사용자를 사용할 수도 있습니다. 을 참조하십시오 "ONTAP 설명서".
- 다음 명령을 실행하여 SVM에 올바른 애플리케이션이 설정되었는지 확인합니다.

```
clustershell::> security login show -vserver <vservename> -user-or
-group-name <username>
```

#### 예제 출력

```
Vserver: svmname
-----
User/Group          Application  Authentication Method  Role Name  Acct Locked  Second Authentication Method
Name              Method
-----
vsadmin            http        password    vsadmin    no       none
vsadmin            ontapi     password    vsadmin    no       none
vsadmin            ssh        password    vsadmin    no       none
3 entries were displayed.
```

- SVM에 CIFS 서버가 구성되어 있는지 확인합니다. 클러스터 셸: >'vserver cifs show'  
SVM 이름, CIFS 서버 이름 및 추가 필드가 반환됩니다.
- SVM vsadmin 사용자의 암호를 설정합니다. 사용자 지정 사용자 또는 클러스터 관리자를 사용하는 경우 이 단계를 건너뛰십시오. clustershell::>'보안 로그인 비밀번호 - 사용자 이름 vsadmin - vserver svmname'입니다
- 외부 액세스를 위해 SVM vsadmin 사용자의 잠금을 해제합니다. 사용자 지정 사용자 또는 클러스터 관리자를 사용하는 경우 이 단계를 건너뛰십시오. clustershell::>'보안 로그인 잠금 해제 - 사용자 이름 vsadmin - vserver svmname'입니다
- 데이터 LIF의 방화벽 정책이 'GMT'(이하 '데이터')로 설정되어 있는지 확인합니다. 전용 관리 리소를 사용하여 SVM을 추가하는 경우에는 이 단계를 건너뛰십시오. clustershell::>'network interface modify -lif <SVM\_data\_LIF\_name> - firewall-policy mgmt'
- 방화벽이 활성화된 경우 Data ONTAP 데이터 수집기를 사용하여 포트에 대한 TCP 트래픽을 허용하도록 정의된 예외가 있어야 합니다.

을 참조하십시오 "상담원 요구 사항" 를 참조하십시오. 이는 클라우드에 설치된 온프레미스 에이전트 및 에이전트에 적용됩니다.

- Cloud ONTAP SVM을 모니터링하기 위해 AWS EC2 인스턴스에 에이전트를 설치한 경우 에이전트와 스토리지는 동일한 VPC에 있어야 합니다. 개별 VPC에 있는 경우 VPC 간에 유효한 경로가 있어야 합니다.

사용자 액세스 차단을 위한 필수 조건

에 대해 다음 사항을 염두에 두십시오 "[사용자 액세스 차단](#)":

이 기능을 사용하려면 클러스터 레벨 자격 증명이 필요합니다.

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: *CsUser*)를 사용하는 경우 아래 단계에 따라 사용자를 차단하는 워크로드 보안에 권한을 부여합니다.

클러스터 자격 증명이 있는 *CsUser*의 경우 ONTAP 명령줄에서 다음을 수행하십시오.

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

## 사용 권한에 대한 참고 사항

클러스터 관리 IP \* 를 통해 추가할 때의 권한:

클러스터 관리 관리자 사용자를 사용하여 워크로드 보안이 ONTAP SVM 데이터 수집기에 액세스할 수 없는 경우 아래 명령에 나와 있는 역할을 사용하여 "CsUser"라는 새 사용자를 생성할 수 있습니다. 클러스터 관리 IP를 사용하도록 워크로드 보안 데이터 수집기를 구성할 때 "CsUser"의 사용자 이름 "CsUser"와 암호를 사용합니다.

새 사용자를 생성하려면 클러스터 관리 관리자 사용자 이름/암호를 사용하여 ONTAP에 로그인하고 ONTAP 서버에서 다음 명령을 실행합니다.

```
security login role create -role csrole -cmddirname DEFAULT -access
readonly
```

```

security login role create -role csrole -cmddirname "vserver fpolicy"
-access all
security login role create -role csrole -cmddirname "volume snapshot"
-access all -query "-snapshot cloudsecure_*"
security login role create -role csrole -cmddirname "event catalog"
-access all
security login role create -role csrole -cmddirname "event filter" -access
all
security login role create -role csrole -cmddirname "event notification
destination" -access all
security login role create -role csrole -cmddirname "event notification"
-access all
security login role create -role csrole -cmddirname "security certificate"
-access all

```

```

security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole
security login create -user-or-group-name csuser -application ssh
-authmethod password -role csrole

```

**vVserver** 관리 IP \* 를 통해 추가할 때의 권한:

클러스터 관리 관리자 사용자를 사용하여 워크로드 보안이 ONTAP SVM 데이터 수집기에 액세스할 수 없는 경우 아래 명령에 나와 있는 역할을 사용하여 "CsUser"라는 새 사용자를 생성할 수 있습니다. 워크로드 보안 데이터 수집기에서 SVM 관리 IP를 사용하도록 구성할 때 "CsUser"의 사용자 이름 "CsUser"와 암호를 사용합니다.

새 사용자를 생성하려면 클러스터 관리 관리자 사용자 이름/암호를 사용하여 ONTAP에 로그인하고 ONTAP 서버에서 다음 명령을 실행합니다. 쉽게 사용할 수 있도록 이러한 명령을 텍스트 편집기에 복사하고 ONTAP에서 다음 명령을 실행하기 전에 <vservername>을(를) SVM 이름으로 바꾸십시오.

```

security login role create -vserver <vservername> -role csrole -cmddirname
DEFAULT -access none

```

```

security login role create -vserver <vservername> -role csrole -cmddirname
"network interface" -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
version -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
volume -access readonly
security login role create -vserver <vservername> -role csrole -cmddirname
vserver -access readonly

```

```
security login role create -vserver <vservername> -role csrole -cmddirname
"vserver fpolicy" -access all
security login role create -vserver <vservername> -role csrole -cmddirname
"volume snapshot" -access all
```

```
security login create -user-or-group-name csuser -application ontapi
-authmethod password -role csrole -vserver <vservername>
```

**ONTAP** 자율적 랜섬웨어 방어 및 **ONTAP** 액세스에 대한 권한이 거부되었습니다

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: *CsUser*)를 사용하는 경우, 아래 단계를 따라 워크로드 보안에 권한을 부여하여 ONTAP에서 ARP 관련 정보를 수집합니다.

자세한 내용은 정보를 참조하십시오 ["ONTAP 액세스와의 통합이 거부되었습니다"](#)

및 ["ONTAP Autonomous 랜섬웨어 Protection과 통합"](#)

데이터 수집기를 구성합니다

구성 단계

1. Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. Workload Security > Collector > + Data Collector \* 를 클릭합니다

사용 가능한 데이터 Collector가 표시됩니다.

3. NetApp SVM 타일 위로 마우스를 가져가 \* + Monitor \* 를 클릭합니다.

ONTAP SVM 구성 페이지가 표시됩니다. 각 필드에 필요한 데이터를 입력합니다.

필드에 입력합니다	설명
이름	Data Collector의 고유 이름입니다
에이전트	목록에서 구성된 에이전트를 선택합니다.
관리 IP를 통해 연결 대상:	클러스터 IP 또는 SVM 관리 IP를 선택합니다
클러스터/SVM 관리 IP 주소	위에서 선택한 항목에 따라 클러스터 또는 SVM의 IP 주소입니다.
SVM 이름	SVM 이름(클러스터 IP를 통해 연결할 때 이 필드 필요)
사용자 이름	클러스터 IP를 통해 추가할 때 SVM/클러스터에 액세스하는 사용자 이름 옵션은 1입니다. 클러스터 관리 2. 'CsUser' 3. CsUser와 유사한 역할을 가진 AD 사용자. SVM IP를 통해 추가할 때 선택할 수 있는 옵션은 다음과 같습니다. 4. vsadmin 5. 'CsUser' 6. CsUser와 유사한 역할을 하는 AD-사용자 이름입니다.

암호	위의 사용자 이름에 대한 암호입니다
공유/볼륨 필터링	이벤트 컬렉션에서 공유/볼륨을 포함할지 또는 제외할지 여부를 선택합니다
제외/포함할 전체 공유 이름을 입력합니다	이벤트 컬렉션에서 제외하거나 포함할(적절한 경우) 공유의 심표로 구분된 목록입니다
제외/포함할 전체 볼륨 이름을 입력합니다	이벤트 컬렉션에서 제외하거나 포함할(적절한 경우) 심표로 구분된 볼륨 목록입니다
폴더 액세스를 모니터링합니다	이 옵션을 선택하면 폴더 액세스 모니터링에 대한 이벤트가 활성화됩니다. 이 옵션을 선택하지 않아도 폴더 생성/이름 변경 및 삭제가 모니터링됩니다. 이 기능을 활성화하면 모니터링되는 이벤트 수가 증가합니다.
ONTAP 전송 버퍼 크기를 설정합니다	ONTAP Fpolicy 전송 버퍼 크기를 설정합니다. 9.8p7 이전의 ONTAP 버전을 사용하고 성능 문제가 발생하면 ONTAP 전송 버퍼 크기를 변경하여 ONTAP 성능을 향상시킬 수 있습니다. 이 옵션이 표시되지 않고 탐색 중인 경우 NetApp 지원에 문의하십시오.

#### 작업을 마친 후

- 설치된 데이터 수집기 페이지에서 각 수집기 오른쪽에 있는 옵션 메뉴를 사용하여 데이터 수집기를 편집합니다. 데이터 수집기를 다시 시작하거나 데이터 수집기 구성 속성을 편집할 수 있습니다.

#### Metro Cluster에 대한 권장 구성

Metro 클러스터에는 다음을 사용하는 것이 좋습니다.

1. 데이터 수집기 2개를 소스 SVM에 연결하고 다른 데이터 수집기를 타겟 SVM에 연결합니다.
2. 데이터 수집기는 `_Cluster IP_`로 연결해야 합니다.
3. 언제든지 한 데이터 수집기가 실행 중이어야 하며, 다른 데이터 수집기는 오류가 발생합니다.

현재 '실행 중인' SVM의 데이터 수집기는 `_running_`으로 표시됩니다. 현재 '가장 위에 있는' SVM의 데이터 수집기는 `_Error_`로 표시됩니다.

4. 전환이 있을 때마다 데이터 수집기의 상태가 '실행 중'에서 '오류'로, 또는 그 반대로 변경됩니다.
5. 데이터 수집기가 오류 상태에서 실행 상태로 이동하는 데 최대 2분이 걸립니다.

#### 서비스 정책

ONTAP 버전 9.9.1의 서비스 정책을 사용하는 경우 데이터 소스 수집기에 연결하려면 데이터 서비스 `data-nfs` 및/또는 `_data-cifs_`와 함께 `_data-fPolicy-client_service_`가 필요합니다.

예:

```
Testcluster-1::*> net int service-policy create -policy only_data_fpolicy
-allowed-addresses 0.0.0.0/0 -vserver aniket_svm
-services data-cifs,data-nfs,data,-core,data-fpolicy-client
(network interface service-policy create)
```

9.9.1 이전의 ONTAP 버전에서는 `_data-FPolicy-client_`를 설정할 필요가 없습니다.

## 데이터 수집기 재생 - 일시 중지

이제 컬렉터의 kebab 메뉴에 2개의 새 작업이 표시됩니다(일시 중지 및 다시 시작).

Data Collector가 `_running_state`인 경우 수집을 일시 중지할 수 있습니다. 수집기에 대한 "세 개의 점" 메뉴를 열고 일시 중지를 선택합니다. Collector가 일시 중지되는 동안 ONTAP에서 수집된 데이터는 없고 Collector에서 ONTAP로 전송되는 데이터는 없습니다. 즉, Fpolicy 이벤트가 ONTAP에서 데이터 수집기로, 그리고 그 안에서 데이터 인프라 Insights로 이동하지 않습니다.

Collector가 일시 중지된 동안 ONTAP에 새 볼륨 등이 생성되면 워크로드 보안이 데이터를 수집하지 않고 해당 볼륨 등이 대시보드나 테이블에 반영되지 않습니다.

다음 사항에 유의하십시오.

- 일시 중지된 수집기에 구성된 설정에 따라 스냅샷 삭제가 수행되지 않습니다.
- ONTAP ARP와 같은 EMS 이벤트는 일시 중지된 Collector에서 처리되지 않습니다. 즉, ONTAP에서 랜섬웨어 공격을 식별하면 Data Infrastructure Insights 워크로드 보안이 해당 이벤트를 파악할 수 없습니다.
- 일시 중지된 수집기에 대해 상태 알림 이메일이 전송되지 않습니다.
- 수동 또는 자동 작업(예: 스냅샷 또는 사용자 차단)은 일시 중지된 수집기에서 지원되지 않습니다.
- 에이전트 또는 수집기 업그레이드, 에이전트 VM 다시 시작/재부팅 또는 에이전트 서비스 다시 시작 시 일시 중지된 수집기는 `_Paused_state`에 남아 있습니다.
- 데이터 수집기가 `_Error_state`인 경우 수집기를 `_Paused_state`로 변경할 수 없습니다. 일시 중지 버튼은 수집기의 상태가 `_running_`인 경우에만 활성화됩니다.
- 에이전트의 연결이 끊어진 경우 수집기를 `_Paused_state`로 변경할 수 없습니다. Collector가 `_stopped_state`로 이동하고 Pause 버튼이 비활성화됩니다.

## 영구 저장

영구 저장소는 ONTAP 9.14.1 이상에서 지원됩니다. 볼륨 이름 지침은 ONTAP 9.14부터 9.15까지 다양합니다.

영구 저장소는 수집기 편집/추가 페이지에서 확인란을 선택하여 활성화할 수 있습니다. 이 확인란을 선택하면 볼륨 이름을 수락할 수 있는 텍스트 필드가 표시됩니다. 볼륨 이름은 영구 저장을 활성화하기 위한 필수 필드입니다.

- ONTAP 9.14.1의 경우 기능을 활성화하기 전에 볼륨을 생성하고 *Volume Name* 필드에 동일한 이름을 제공해야 합니다. 권장 볼륨 크기는 16GB입니다.
- ONTAP 9.15.1의 경우 수집기에서 *Volume Name* 필드에 제공된 이름을 사용하여 16GB 크기로 볼륨이 자동으로 생성됩니다.

영구 저장소에 대한 특정 권한이 필요합니다(일부 또는 모두 이미 존재할 수 있음).

클러스터 모드:

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <cluster-name>
```

**SVM 모드:**


```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <vserver-name>
security login rest-role create -role csrestrole -api /api/cluster/jobs/
-access readonly -vserver <vserver-name>
```

**문제 해결**

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

오류의 경우, \_Status\_ 열에서 \_more detail\_ 을 클릭하여 오류에 대한 세부 정보를 확인하십시오.

**Installed Data Collectors**

Name	Status	Type	Agent
9.8_vs1	 Error <a href="#">more detail</a>	ONTAP SVM	agent-11

<b>문제:</b>	<b>해상도:</b>
Data Collector는 일정 시간 동안 실행되며 임의 시간 후 중지되며, "오류 메시지: 커넥터가 오류 상태입니다. 서비스 이름: 감사. 장애 원인: 외부 FPolicy 서버가 과부하 상태입니다."	ONTAP의 이벤트 발생률은 상담원 박스가 처리할 수 있는 것보다 훨씬 높았습니다. 따라서 연결이 종료되었습니다. 연결이 끊겼을 때 CloudSecure의 최대 트래픽을 확인합니다. 이는 * CloudSecure > Activity Forensics > All Activity * 페이지에서 확인할 수 있습니다. 최대 집계된 트래픽이 Agent Box에서 처리할 수 있는 트래픽보다 높은 경우 Agent Box에서 Collector 배포를 사이징하는 방법에 대한 이벤트 속도 검사기 페이지를 참조하십시오. 2021년 3월 4일 이전에 Agent 상자에 Agent를 설치한 경우, Agent 상자에서 echo 'net.core.rmem_max=8388608'> /etc/sysctl.conf echo'net.ipv4.tcp_rmem=4096 2097152 838608'> /etc/sysctl.sysctl.UI를 다시 시작한 후 다시 시작합니다.



<p>문제:</p> <p>수집기가 오류 메시지를 보고합니다: "SVM의 데이터 인터페이스에 연결할 수 있는 커넥터에서 로컬 IP 주소를 찾을 수 없습니다."</p>	<p>해상도:</p> <p>이는 ONTAP 측의 네트워킹 문제 때문일 가능성이 가장 높습니다. 다음 단계를 따르십시오.</p> <p>SVM 데이터 lif 또는 SVM과의 연결을 차단하는 관리 lif에 방화벽이 없는지 확인합니다.</p> <p>클러스터 관리 IP를 통해 SVM을 추가할 때 SVM의 데이터 거짓과 관리 거짓이 에이전트 VM에서 핑되도록 하십시오. 문제가 발생한 경우, lif에 대한 게이트웨이, 넷마스크 및 경로를 확인하십시오.</p> <p>클러스터 관리 IP를 사용하여 ssh를 통해 클러스터에 로그인하고 에이전트 IP를 Ping할 수도 있습니다. 에이전트 IP가 Ping할 수 있는지 확인합니다.</p> <p><i>network ping -vserver &lt;vserver name&gt; -destination &lt;Agent IP&gt; -lif &lt;Lif Name&gt; -show -detail</i></p> <p>Ping할 수 없는 경우 ONTAP의 네트워크 설정이 올바른지 확인하여 Agent 시스템이 Ping할 수 있도록 합니다.</p> <p>3.클러스터 IP를 통해 연결을 시도했으나 작동하지 않는 경우 SVM IP를 통해 직접 연결을 시도하십시오. SVM IP를 통해 연결하는 단계는 위 섹션을 참조하십시오.</p> <p>SVM IP 및 vsadmin 자격 증명을 통해 수집기를 추가하는 동안 SVM LIF에서 데이터 및 관리 역할이 활성화되어 있는지 확인합니다. 이 경우 SVM LIF로 ping을 수행할 수 있지만 SVM LIF에 대한 SSH는 작동하지 않습니다. SVM 관리 전용 LIF를 생성한 후 이 SVM 관리 전용 LIF를 통해 연결을 시도하십시오.</p> <p>그래도 작동하지 않으면 새 SVM LIF를 생성하고 LIF를 통해 연결을 시도합니다. 서브넷 마스크가 올바르게 설정되었는지 확인합니다.</p> <p>6.고급 디버깅:</p> <p>a) ONTAP에서 패킷 추적을 시작합니다.  B) CloudSecure UI에서 데이터 수집기를 SVM에 연결합니다.  c) 오류가 나타날 때까지 기다립니다. ONTAP에서 패킷 추적을 중지합니다.  d) ONTAP에서 패킷 추적을 엽니다. 이 위치에서 사용할 수 있습니다</p> <p><i>https://&lt;cluster_mgmt_ip&gt;/SPI/&lt;clustername&gt;/etc/log/packet_traces/</i></p> <p>e) ONTAP에서 에이전트 상자로 SYN이 있는지 확인합니다.  f) ONTAP의 SYN이 없는 경우 ONTAP의 방화벽 문제입니다.  g) ONTAP에서 방화벽을 열어 ONTAP가 에이전트 상자를 연결할 수 있도록 합니다.</p>
---	---

문제:	해상도:
<p>메시지: "[hostname:&lt;IP Address&gt;에 대한 ONTAP 유형을 확인하지 못했습니다. 이유: 스토리지 시스템에 대한 접속 오류 &lt;IP 주소&gt;: 호스트에 연결할 수 없습니다 (호스트에 연결할 수 없음)"</p>	<p>올바른 SVM IP 관리 주소 또는 클러스터 관리 IP가 제공되었는지 확인합니다. 연결할 SVM 또는 클러스터에 SSH를 연결합니다. 연결이 완료되면 SVM 또는 클러스터 이름이 올바른지 확인합니다.</p>
<p>오류 메시지: "커넥터가 오류 상태입니다. service.name: 감사. 실패 이유: 외부 FPolicy 서버가 종료되었습니다."</p>	<p>1.방화벽이 에이전트 시스템에서 필요한 포트를 차단하고 있을 가능성이 높습니다. 에이전트 시스템이 SVM에서 연결할 수 있도록 포트 범위 35000-55000/TCP가 열려 있는지 확인합니다. 또한 ONTAP 측 차단 통신에서 에이전트 시스템로의 방화벽이 활성화되어 있지 않은지 확인합니다. 에이전트 상자에 다음 명령을 입력하고 포트 범위가 열려 있는지 확인합니다. <code>_sudo iptables -save</code></p>
<p>grep 3500 * _Sample 출력은 다음과 같아야 합니다. <code>_ -a in_public_allow -p tcp -m -dport 35000 -m contrack -ctstate new -j accept_3</code>. SVM에 로그인하고 다음 명령을 입력한 후 ONTAP와의 통신을 차단하는 방화벽이 설정되어 있는지 확인합니다. <code>_system services firewall show _system services firewall policy show _</code> "방화벽 명령을 확인합니다" ONTAP 측면</p> <p>4.모니터링하려는 SVM/클러스터에 SSH를 연결합니다. CIFS, NFS 프로토콜 지원)을 사용하여 SVM 데이터 거점에서 에이전트 상자를 ping하고 ping이 작동하는지 확인합니다. <code>_network ping -vserver &lt;vserver name&gt; -destination &lt;Agent IP&gt; -lif &lt;LIF Name&gt; -show-detail</code> 만약 Ping할 수 없으면 ONTAP의 네트워크 설정이 올바른지 확인하여 에이전트 시스템이 Ping할 수 있도록 합니다. 데이터 수집기 2개를 통해 테넌트에 단일 SVM을 두 번 추가하면 이 오류가 표시됩니다. UI를 통해 데이터 수집기 중 하나를 삭제합니다. 그런 다음 UI를 통해 다른 데이터 수집기를 다시 시작합니다. 그러면 데이터 수집기가 "실행 중" 상태를 표시하고 SVM에서 이벤트를 수신하기 시작합니다. 기본적으로 테넌트에서 1개의 SVM은 1개의 데이터 수집기를 통해 한 번만 추가해야 합니다. 1 SVM은 2개의 데이터 수집기를 통해 두 번 추가해서는 안 됩니다. 서로 다른 두 가지 워크로드 보안 환경(테넌트)에서 동일한 SVM을 추가한 경우 마지막 SVM은 항상 성공합니다. 두 번째 수집기는 FPolicy를 자체 IP 주소로 구성하고 첫 번째 것을 시작합니다. 따라서 첫 번째 수집기는 이벤트 수신을 중지하고 "감사" 서비스가 오류 상태로 전환됩니다. 이를 방지하려면 각 SVM을 단일 환경에서 구성합니다.</p> <p>7.서비스 정책이 올바르게 구성되지 않은 경우에도 이 오류가 발생할 수 있습니다. ONTAP 9.8 이상에서는 데이터 소스 수집기에 연결하기 위해 데이터 서비스 데이터 서비스 데이터(NFS 및/또는 데이터 CIFS)와 함께 데이터 FPolicy 클라이언트 서비스가 필요합니다. 또한 데이터 -FPolicy-클라이언트 서비스는 모니터링되는 SVM에 대한 데이터 거점과 연결되어야 합니다.</p>	<p>활동 페이지에 이벤트가 표시되지 않습니다.</p>

<p>문제:</p>	<p>해상도:</p>
<p>ONTAP Collector가 "실행 중" 상태인지 확인합니다. 예 인 경우 일부 파일을 열어 CIFS 클라이언트 VM에서 일부 CIFS 이벤트가 생성되는지 확인합니다. 2.활동이 표시되지 않으면 SVM에 로그인하여 다음 명령을 입력하십시오. &lt;SVM&gt; 이벤트 로그에 -소스 FPolicy_FPolicy와 관련된 오류가 없는지 확인하십시오. 3.활동이 표시되지 않으면 SVM에 로그인하십시오. 다음 명령을 입력합니다. _&lt;SVM&gt;FPolicy show_Check 접두사 "cloudsecure"로 명명된 FPolicy 정책이 설정되어 있고 상태가 "on"인지 확인합니다. 설정되지 않으면 Agent가 SVM에서 명령을 실행할 수 없을 가능성이 높습니다. 페이지 시작 부분에 설명된 모든 필수 구성 요소가 준수되었는지 확인하십시오.</p>	<p>SVM Data Collector가 오류 상태이고 오류 메시지가 "에이전트가 수집기에 연결하지 못했습니다"입니다.</p>
<p>1.Agent가 과부하되어 데이터 소스 수집기에 연결할 수 없을 가능성이 높습니다. 2.Agent에 연결된 데이터 소스 Collector의 수를 확인합니다. 또한 UI의 "모든 활동" 페이지에서 데이터 플로우 속도를 확인합니다. 초당 작업 수가 상당히 많은 경우 다른 에이전트를 설치하고 일부 데이터 소스 Collector를 새 에이전트로 이동합니다.</p>	<p>SVM Data Collector에서 "fpolicy.server.connectError: Node가 FPolicy 서버 "12.195.15.146"과 연결을 설정하지 못했습니다(이유: "Select Timed Out")"라는 오류 메시지를 표시합니다.</p>
<p>SVM/클러스터에서 방화벽이 활성화됩니다. FPolicy 엔진이 FPolicy 서버에 연결할 수 없습니다. 자세한 정보를 얻는 데 사용할 수 있는 ONTAP의 CLI는 이벤트 로그 표시 - 소스 FPolicy입니다. FPolicy는 오류 이벤트 로그 표시 - 소스 FPolicy - 필드 이벤트, 작업, 설명입니다. 자세한 내용은 표시됩니다."<b>방화벽 명령을 확인합니다</b>" ONTAP 측면</p>	<p>오류 메시지: "커넥터가 오류 상태입니다. 서비스 이름: 감사. 장애 원인: SVM에서 유효한 데이터 인터페이스(역할: 데이터, 데이터 프로토콜: NFS 또는 CIFS 또는 둘 다, 상태: UP)를 찾을 수 없습니다."</p>
<p>운영 인터페이스(데이터 및 데이터 프로토콜 역할을 CIFS/NFS로 사용)가 있는지 확인합니다.</p>	<p>데이터 수집기는 오류 상태가 된 다음 일정 시간이 지나면 실행 중 상태가 되고 다시 오류 상태로 돌아갑니다. 이 주기가 반복됩니다.</p>
<p>이 문제는 일반적으로 다음 시나리오에서 발생합니다. 1. 추가된 데이터 수집기가 여러 개 있습니다. 이러한 동작을 보여 주는 데이터 수집기는 이러한 데이터 수집기에 1개의 SVM이 추가됩니다. 즉, 2개 이상의 데이터 수집기가 1개의 SVM에 연결됩니다. 데이터 수집기 1개가 1개의 SVM에 연결되는지 확인합니다. 동일한 SVM에 연결된 다른 데이터 수집기를 삭제합니다.</p>	<p>커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 원인: 구성하지 못했습니다(SVM svmname에 대한 정책). 이유: 'FPolicy.policy.scope-modify:"연방" 내의 '포함할' 요소에 대해 잘못된 값이 지정되었습니다.</p>
<p>공유 이름은 따옴표 없이 지정해야 합니다. ONTAP SVM DSC 구성을 편집하여 공유 이름을 수정하십시오. _INCLUDE 및 EXCLUDE_ 는 긴 공유 이름 목록에 사용할 수 없습니다. 포함 또는 제외할 공유 수가 많은 경우 대신 볼륨별 필터링을 사용합니다.</p>	<p>클러스터에 사용되지 않는 기존 fpolicies가 있습니다. 워크로드 보안을 설치하기 전에 이러한 작업을 어떻게 해야 하나요?</p>

<p>문제:</p> <p>사용되지 않는 기존 FPolicy 설정이 연결되지 않은 경우에도 모두 삭제하는 것이 좋습니다. 워크로드 보안에서는 접두사 "cloudsecure_"를 사용하여 FPolicy를 생성합니다. 사용되지 않는 다른 모든 FPolicy 구성은 삭제할 수 있습니다. FPolicy 목록을 표시하는 CLI 명령: <code>_FPolicy show_steps</code> FPolicy 구성을 삭제하는 방법: <code>_FPolicy disable -vserver &lt;svmname&gt; -policy -name &lt;policy_name&gt; _FPolicy scope delete -vserver &lt;svmname&gt; _FPolicy -policy -name &lt;policy_name&gt; _FPolicy_vserver_name &lt;정책 삭제 -vserver_name &lt;policy_name&gt;</code></p>	<p>해상도:</p> <p>워크로드 보안을 활성화한 후 ONTAP 성능에 영향을 미침: 지연 시간이 산발적으로 높고 IOPS가 산발적으로 낮아지는 경우</p>
<p>워크로드 보안과 함께 ONTAP를 사용할 때 ONTAP에서 지연 시간 문제가 나타날 수 있습니다. 다음과 같은 여러 가지 가능한 이유가 있습니다. "<a href="#">1372994를 참조하십시오</a>", "<a href="#">141515152를 참조하십시오</a>", "<a href="#">1438207을 참조하십시오</a>", "<a href="#">1479704</a>", "<a href="#">1354659를 참조하십시오</a>". 이러한 모든 문제는 ONTAP 9.13.1 이상에서 수정되었으며 이러한 최신 버전 중 하나를 사용하는 것이 좋습니다.</p>	<p>데이터 수집기가 오류 중입니다. 이 오류 메시지를 표시합니다. "오류: 커넥터가 오류 상태입니다. 서비스 이름: 감사. 실패 원인: SVM svm_test에서 정책을 구성하지 못했습니다. 이유: ZAPI 필드에 값이 없습니다. 이벤트 "</p>
<p>NFS 서비스만 구성하여 새로운 SVM으로 시작하십시오. 워크로드 보안에서 ONTAP SVM 데이터 수집기 추가 CIFS는 SVM을 위한 허용 프로토콜로 구성된 동시에 워크로드 보안에서 ONTAP SVM Data Collector를 추가합니다. 워크로드 보안의 데이터 수집기에 오류가 표시될 때까지 기다립니다. SVM에 CIFS 서버가 구성되어 있지 않으므로 왼쪽에 표시된 이 오류는 워크로드 보안으로 표시됩니다. ONTAP SVM 데이터 수집기를 편집하고 CIFS를 허용된 프로토콜로 선택 취소하십시오. 데이터 수집기를 저장합니다. NFS 프로토콜만 활성화된 상태에서 실행됩니다.</p>	<p>Data Collector에 다음과 같은 오류 메시지가 표시됩니다. "오류: 2회 재시도에서 Collector 상태를 확인하지 못했습니다. Collector를 다시 시작하십시오(오류 코드: AGENT008)."</p>
<p>Data Collector 페이지에서 오류를 제공하는 데이터 수집기의 오른쪽으로 스크롤하고 3개의 점 메뉴를 클릭합니다. 편집 _을(를) 선택합니다. 데이터 수집기의 암호를 다시 입력합니다. Save _ 버튼을 눌러 데이터 수집기를 저장합니다. Data Collector가 다시 시작되고 오류가 해결되어야 합니다.</p> <p>2.Agent 시스템이 CPU 또는 RAM 여유 공간이 부족할 수 있습니다. 이것이 바로 DSC가 실패하는 이유입니다. 시스템의 에이전트에 추가되는 데이터 수집기 수를 확인하십시오. 20개를 초과하는 경우 Agent 시스템의 CPU 및 RAM 용량을 늘리십시오. CPU와 RAM이 증가되면 DSC가 초기화 중 상태로 전환되었다가 자동으로 실행 상태로 전환됩니다. 의 사이징 가이드를 참조하십시오 "<a href="#">이 페이지</a>".</p>	<p>SVM 모드를 선택하면 Data Collector에서 오류가 발생합니다.</p>

그래도 문제가 발생하면 \* 도움말 > 지원 \* 페이지에 나와 있는 지원 링크를 참조하십시오.

## NetApp ONTAP Collector용 Cloud Volumes ONTAP 및 Amazon FSx 구성

워크로드 보안은 데이터 수집기를 사용하여 디바이스에서 파일 및 사용자 액세스 데이터를 수집합니다.

### Cloud Volumes ONTAP 스토리지 구성

워크로드 보안 에이전트를 호스팅하도록 단일 노드/HA AWS 인스턴스를 구성하려면 OnCommand Cloud Volumes ONTAP 설명서를 참조하십시오. <https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/index.html>

구성이 완료되면 단계에 따라 SVM을 설정합니다. [https://docs.netapp.com/us-en/cloudinsights/task\\_add\\_collector\\_svm.html](https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html)

### 지원되는 플랫폼

- Cloud Volumes ONTAP - 사용 가능한 모든 클라우드 서비스 공급자에서 지원됩니다. 예: Amazon, Azure, Google Cloud
- ONTAP 아마존 FSx

### 에이전트 시스템 구성

에이전트 시스템은 클라우드 서비스 공급자의 각 서브넷에 구성되어야 합니다. [Agent Requirements] 에서 네트워크 액세스에 대해 자세히 알아보십시오.

다음은 AWS에서 Agent를 설치하는 단계입니다. 클라우드 서비스 공급자에 적용되는 것과 동일한 단계를 Azure 또는 Google Cloud에서 설치를 위해 수행할 수 있습니다.

AWS에서 다음 단계를 수행하여 워크로드 보안 에이전트로 사용할 시스템을 구성합니다.

다음 단계를 수행하여 워크로드 보안 에이전트로 사용할 시스템을 구성합니다.

### 단계

1. AWS 콘솔에 로그인하고 EC2-Instances 페이지로 이동한 후 `_Launch instance_`를 선택합니다.
2. 이 페이지에서 언급한 대로 적절한 버전의 RHEL 또는 CentOS AMI를 선택합니다. [https://docs.netapp.com/us-en/cloudinsights/concept\\_cs\\_agent\\_requirements.html](https://docs.netapp.com/us-en/cloudinsights/concept_cs_agent_requirements.html)
3. Cloud ONTAP 인스턴스가 상주하는 VPC 및 서브넷을 선택합니다.
4. 할당된 리소스로 `T2.xLarge`(vCPU 4개 및 16GB RAM)를 선택합니다.
  - a. EC2 인스턴스를 만듭니다.
5. YUM 패키지 관리자를 사용하여 필요한 Linux 패키지를 설치합니다.
  - a. `install_wget_and_unzip_native` Linux 패키지를 설치합니다.

### 워크로드 보안 에이전트를 설치합니다

1. Data Infrastructure Insights 환경에 관리자 또는 계정 소유자로 로그인합니다.
2. Workload Security \* Collector \* 로 이동한 후 \* Agents \* 탭을 클릭합니다.
3. \* + Agent \* 를 클릭하고 RHEL을 대상 플랫폼으로 지정합니다.

4. Agent 설치 명령을 복사합니다.
5. 로그인한 RHEL EC2 인스턴스에 Agent Installation 명령을 붙여 넣습니다. 이렇게 하면 워크로드 보안 에이전트가 설치되어 모든 가 제공됩니다 "상담원 필수 구성 요소" 충족됩니다.

자세한 단계는 [https://docs.netapp.com/us-en/cloudinsights/task\\_cs\\_add\\_agent.html#steps-to-install-agent](https://docs.netapp.com/us-en/cloudinsights/task_cs_add_agent.html#steps-to-install-agent) 링크를 참조하십시오

## 문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제	해상도
"워크로드 보안: Amazon FxSN 데이터 수집기에 대한 ONTAP 유형을 확인하지 못했습니다." 오류가 데이터 수집기에 표시됩니다. 고객은 새로운 Amazon FSxN 데이터 수집기를 워크로드 보안에 추가할 수 없습니다. 에이전트에서 포트 443의 FSxN 클러스터에 대한 연결이 시간 초과입니다. 방화벽 및 AWS 보안 그룹에는 통신을 허용하는 데 필요한 규칙이 활성화되어 있습니다. 에이전트가 이미 구축되어 있으며 동일한 AWS 계정에도 있습니다. 이 동일한 에이전트를 사용하여 나머지 NetApp 장치를 연결 및 모니터링합니다(모두 작동).	fsxadmin LIF 네트워크 세그먼트를 에이전트의 보안 규칙에 추가하여 이 문제를 해결합니다. 포트가 확실하지 않은 경우 모든 포트가 허용됩니다.

## 사용자 관리

워크로드 보안 사용자 계정은 Cloud Insights를 통해 관리됩니다.

Cloud Insights는 계정 소유자, 관리자, 사용자 및 게스트의 네 가지 사용자 계정 수준을 제공합니다. 각 계정에는 특정 권한 수준이 할당됩니다. 관리자 권한이 있는 사용자 계정은 사용자를 생성 또는 수정하고 각 사용자에게 다음 워크로드 보안 역할 중 하나를 할당할 수 있습니다.

역할	워크로드 보안 액세스
관리자	알림, Forensics, 데이터 수집기, 자동화된 응답 정책 및 워크로드 보안을 위한 API를 비롯한 모든 워크로드 보안 기능을 수행할 수 있습니다. 관리자는 다른 사용자를 초대할 수도 있지만 워크로드 보안 역할만 할당할 수 있습니다.
사용자	알림을 확인 및 관리하고 Forensics를 볼 수 있습니다. 사용자 역할은 알림 상태를 변경하고, 메모를 추가하고, 스냅샷을 수동으로 생성하고, 사용자 액세스를 제한할 수 있습니다.
게스트	알림 및 Forensics를 볼 수 있습니다. 게스트 역할은 알림 상태를 변경하거나, 메모를 추가하거나, 스냅샷을 수동으로 생성하거나, 사용자 액세스를 제한할 수 없습니다.

## 단계

1. 워크로드 보안에 로그인합니다
2. 메뉴에서 \* Admin > User Management \* 를 클릭합니다

Cloud Insights의 사용자 관리 페이지로 전달됩니다.

3. 각 사용자에게 대해 원하는 역할을 선택합니다.

새 사용자를 추가하는 동안 원하는 역할(일반적으로 사용자 또는 게스트)을 선택하기만 하면 됩니다.

사용자 계정 및 역할에 대한 자세한 내용은 Cloud Insights에서 확인할 수 있습니다 "[사용자 역할](#)" 문서화:

## SVM Event Rate Checker(에이전트 크기 지정 가이드)

이벤트 속도 검사기는 ONTAP SVM 데이터 수집기를 설치하기 전에 SVM에서 NFS/SMB의 결합된 이벤트 속도를 확인하여 에이전트 시스템 한 대를 모니터링할 수 있는 SVM의 수를 확인하는 데 사용됩니다. 이벤트 속도 검사기를 크기 조정 가이드로 사용하여 보안 환경을 계획할 수 있습니다.

Agent는 최대 50개의 데이터 수집기를 지원할 수 있습니다.

요구 사항:

- 클러스터 IP
- 클러스터 관리자 사용자 이름 및 암호입니다



이 스크립트를 실행할 때 이벤트 속도를 확인할 SVM을 위해 ONTAP SVM Data Collector를 실행해야 합니다.

단계:

1. CloudSecure의 지침에 따라 Agent를 설치합니다.
2. 에이전트가 설치되면 sudo 사용자로 `_server_data_rate_checker.sh_script`를 실행합니다.

```
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

. 이 스크립트를 사용하려면 Linux 시스템에 `_sshpas_`를 설치해야 합니다. 두 가지 방법으로 설치할 수 있습니다.

a. 다음 명령을 실행합니다.

```
linux_prompt> yum install sshpass
```

.. 그렇지 않으면 웹에서 Linux 시스템으로 `_sshpas_`를 다운로드하고 다음 명령을 실행합니다.

```
linux_prompt> rpm -i sshpass
```

3. 메시지가 표시되면 올바른 값을 입력합니다. 예를 보려면 아래를 참조하십시오.

- 스크립트는 약 5분 정도 소요됩니다.
- 실행이 완료되면 스크립트가 SVM의 이벤트 속도를 인쇄합니다. 콘솔 출력에서 SVM당 이벤트 속도를 확인할 수 있습니다.

```
"Svm svm_rate is generating 100 events/sec".
```

각 ONTAP SVM Data Collector를 단일 SVM과 연결할 수 있습니다. 즉, 각 데이터 수집기에서 단일 SVM에서 생성되는 이벤트 수를 받을 수 있습니다.

다음 사항에 유의하십시오.

- 이 표를 일반 사이징 가이드로 사용합니다. 코어 및/또는 메모리의 수를 늘려 지원되는 데이터 수집기 수를 최대 50개까지 늘릴 수 있습니다.

에이전트 시스템 구성	SVM 데이터 수집기 수	Agent Machine이 처리할 수 있는 최대 이벤트 속도
4코어, 16GB	10개의 데이터 수집기	초당 20,000개의 이벤트
4코어, 32GB	20개의 데이터 수집기	초당 20,000개의 이벤트

- 총 이벤트를 계산하려면 해당 에이전트에 대해 생성된 모든 SVM에 대해 생성된 이벤트를 추가합니다.
- 피크 시간 동안 스크립트가 실행되지 않거나 피크 트래픽을 예측하기 어려운 경우 이벤트 속도 버퍼를 30%로 유지합니다.

B+C는 A보다 작아야 합니다. 그렇지 않으면 Agent 시스템이 모니터링하지 못합니다.

즉, 단일 에이전트 시스템에 추가할 수 있는 데이터 수집기의 수는 아래 공식을 준수해야 합니다.

```
Sum of all Event rate of all Data Source Collectors + Buffer Event rate of 30% < 20000 events/second
를 참조하십시오 xref:{relative_path}concept_cs_agent_requirements.html["상담원 요구 사항"] 페이지를 참조하십시오.
```

예

SVM이 각각 100개, 200개, 300개의 이벤트를 생성한다고 가정해 보겠습니다.

다음 수식을 적용합니다.

```
(100+200+300) + [(100+200+300)*30%] = 600+180 = 780events/sec
780 events/second is < 20000 events/second, so the 3 SVMs can be monitored via one agent box.
```

콘솔 출력은 현재 작업 디렉토리의 파일 이름 *FPolicy\_stat\_<SVM 이름>.log*에서 Agent 시스템에서 사용할 수



있습니다.

스크립트는 다음과 같은 경우에 잘못된 결과를 제공할 수 있습니다.

- 잘못된 자격 증명, IP 또는 SVM 이름이 제공됩니다.
- 이름, 시퀀스 번호 등이 동일한 기존 FPolicy에서 오류가 발생합니다.
- 실행 중에 스크립트가 갑자기 중지됩니다.

스크립트 실행의 예는 다음과 같습니다.

```
[root@ci-cs-data agent]#  
/opt/netapp/cloudsecure/agent/install/svm_event_rate_checker.sh
```

```
Enter the cluster ip: 10.192.139.166  
Enter the username to SSH: admin  
Enter the password:  
Getting event rate for NFS and SMB events.  
Available SVMs in the Cluster  
-----  
QA_SVM  
Stage_SVM  
Qa-fas8020  
Qa-fas8020-01  
Qa-fas8020-02  
audit_svm  
svm_rate  
vs_new  
vs_new2
```

```

-----
Enter [1/5] SVM name to check (press enter to skip): svm_rate
Enter [2/5] SVM name to check (press enter to skip): audit_svm
Enter [3/5] SVM name to check (press enter to skip):
Enter [4/5] SVM name to check (press enter to skip):
Enter [5/5] SVM name to check (press enter to skip):
Running check for svm svm_rate...
Running check for svm audit_svm...
Waiting 5 minutes for stat collection
Stopping sample svm_rate_sample
Stopping sample audit_svm_sample
fpolicy stats of svm svm_rate is saved in fpolicy_stat_svm_rate.log
Svm svm_rate is generating 100 SMB events/sec and 100 NFS events/sec
Overall svm svm_rate is generating 200 events/sec
fpolicy stats of svm audit_svm is saved in fpolicy_stat_audit_svm.log
Svm audit_svm is generating 200 SMB events/sec and 100 NFS events/sec
Overall svm audit_svm is generating 300 events/sec

```

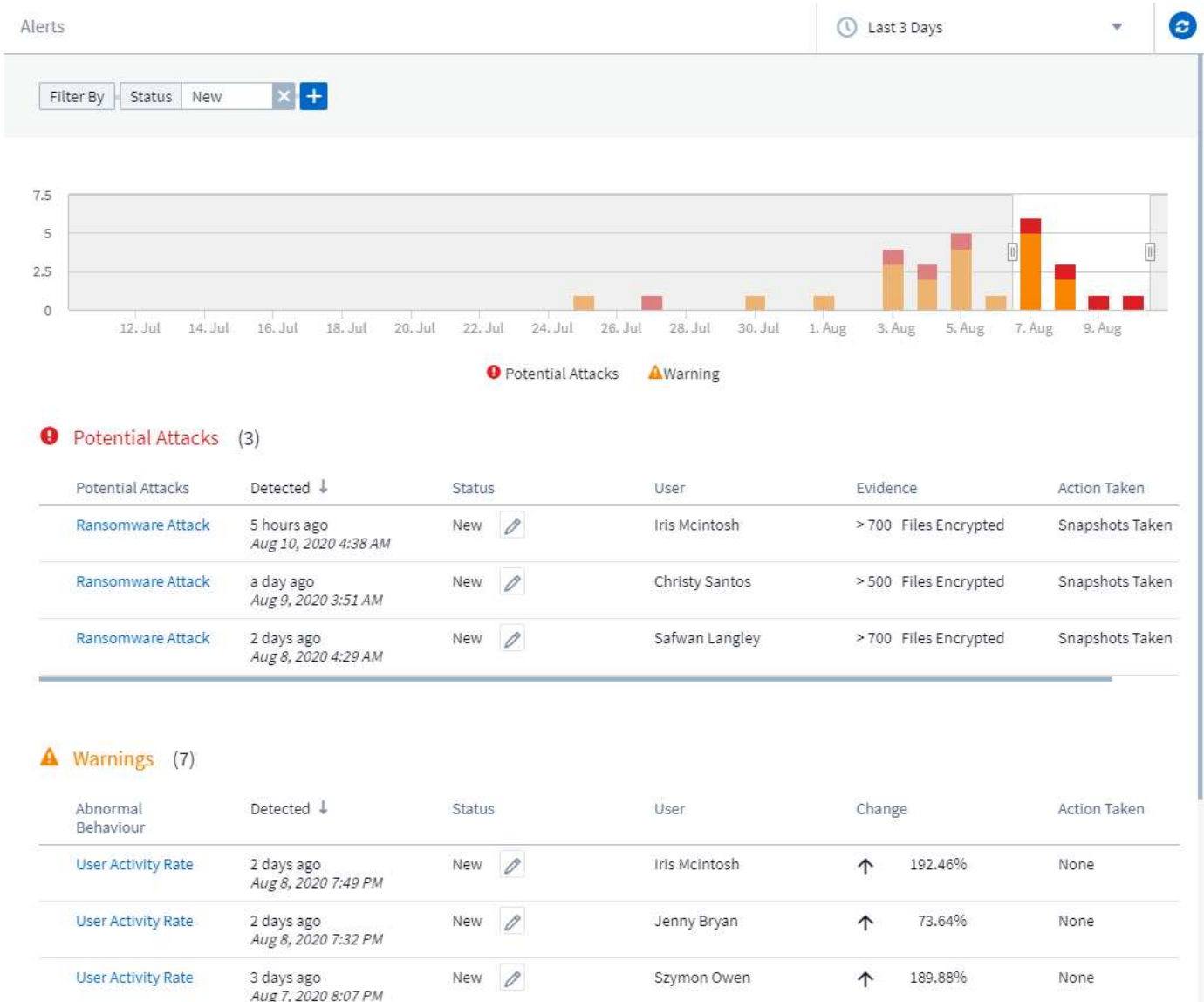
```
[root@ci-cs-data agent]#
```

## 문제 해결

질문	답변
워크로드 보안용으로 이미 구성된 SVM에서 이 스크립트를 실행하면 SVM에서 기존 FPolicy 구성을 사용하기만 합니까, 아니면 임시 FPolicy 구성을 사용하여 프로세스를 실행합니까?	워크로드 보안용으로 이미 구성된 SVM에 대해서도 이벤트 속도 검사기를 실행할 수 있습니다. 아무런 영향도 미치지 않아야 합니다.
스크립트를 실행할 수 있는 SVM의 수를 늘릴 수 있습니까?	예. 스크립트를 편집하고 SVM의 최대 수를 5개에서 원하는 수로 변경하면 됩니다.
SVM 수를 늘릴 경우 스크립트 실행 시간이 늘어집니까?	아니요 이 스크립트는 SVM 수가 증가하더라도 최대 5분 동안 실행됩니다.
스크립트를 실행할 수 있는 SVM의 수를 늘릴 수 있습니까?	예. 스크립트를 편집하고 SVM의 최대 수를 5개에서 원하는 수로 변경해야 합니다.
SVM 수를 늘릴 경우 스크립트 실행 시간이 늘어집니까?	아니요 이 스크립트는 SVM 수가 증가하더라도 최대 5분 동안 실행됩니다.
기존 에이전트에서 이벤트 속도 검사기를 실행하면 어떻게 됩니까?	이미 있는 에이전트에 대해 이벤트 속도 검사기를 실행하면 SVM에서 지연 시간이 증가할 수 있습니다. 이 증가율은 기본적으로 이벤트 속도 검사기가 실행되는 동안 일시적으로 발생합니다.

# 경고

워크로드 보안 경고 페이지에는 최근 공격 및/또는 경고의 타임라인이 표시되며 각 문제에 대한 세부 정보를 볼 수 있습니다.



# 경고

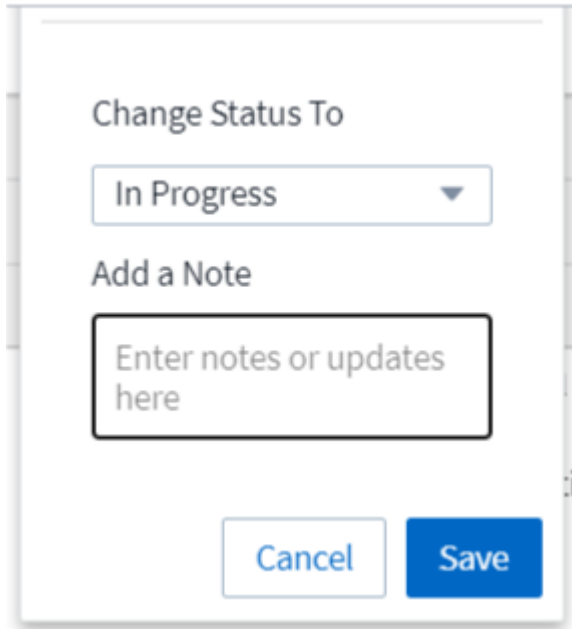
경고 목록에는 선택한 시간 범위에서 발생한 잠재적 공격 및/또는 경고의 총 수와 해당 시간 범위에서 발생한 공격 및/또는 경고 목록이 표시된 그래프가 표시됩니다. 그래프에서 시작 시간 및 종료 시간 슬라이더를 조정하여 시간 범위를 변경할 수 있습니다.

각 경고에 대해 다음이 표시됩니다.

- 잠재적 공격: \*
- The\_potential attack\_type(예: 랜섬웨어 또는 태업)
- 잠재적 공격이 \_ 탐지된 날짜 및 시간입니다 \_

- 알림의 \_ 상태 \_:
  - \* New \* (새로 만들기 \*): 새 경고의 기본값입니다.
  - \* 진행 중 \*: 팀 구성원 또는 구성원이 알림을 조사 중입니다.
  - \* 해결됨 \*: 팀 구성원이 경고를 해결됨으로 표시했습니다.
  - \* 해제됨 \*: 경고가 거짓 긍정 또는 예상된 동작으로 무시되었습니다.

관리자는 알림의 상태를 변경하고 조사에 도움이 되는 메모를 추가할 수 있습니다.



- 동작을 통해 경고가 트리거된 \_User\_입니다
- \_evidence\_ of the attack(예: 많은 수의 파일이 암호화됨)
- 수행된 조치 \_ (예: 스냅샷이 촬영됨)
- 경고: \*
- 경고를 트리거한 \_ 비정상적인 동작 \_
- 동작이 \_detected\_인 날짜 및 시간입니다
- 알림의 *Status*(신규, 진행 중 등)
- 동작을 통해 경고가 트리거된 \_User\_입니다
- Change \_ 에 대한 설명(예: 파일 액세스의 비정상적인 증가)
- 조치 \_

## 필터 옵션

경고를 필터링하는 방법은 다음과 같습니다.

- 알림의 \_ 상태 \_
- Note\_의 특정 텍스트입니다

- 공격 유형/경고 \_
- 작업이 경고/경고를 트리거한 \_User\_입니다

## 경고 세부 정보 페이지

경고 목록 페이지에서 경고 링크를 클릭하여 경고에 대한 세부 정보 페이지를 열 수 있습니다. 경고 세부 정보는 공격 유형 또는 경고 유형에 따라 다를 수 있습니다. 예를 들어, 랜섬웨어 공격 세부 정보 페이지에 다음 정보가 표시될 수 있습니다.

### 요약 섹션:

- 공격 유형(랜섬웨어, 태업) 및 경고 ID(워크로드 보안에서 할당)
- 공격이 감지된 날짜 및 시간입니다
- 작업이 수행됨(예: 자동 스냅샷이 작성됨) 스냅샷 시간은 요약 섹션 바로 아래에 표시됩니다.)
- 상태(신규, 진행 중 등)

### 공격 결과 섹션:

- 영향을 받는 볼륨 및 파일 수
- 감지에 대한 관련 요약
- 공격 중 파일 작업을 보여주는 그래프입니다

### 관련 사용자 섹션:

이 섹션에서는 잠재적 공격에 관련된 사용자에게 대한 상세 정보를 보여 주며, 여기에는 사용자의 상위 활동 그래프가 포함됩니다.

Alerts 페이지(이 예제에서는 잠재적인 랜섬웨어 공격을 보여 줍니다.)

Filter By



### ⚠ Potential Attacks (1)

Potential Attacks	Detected ↓	Status	User	Evidence	Action Taken
<a href="#">Ransomware Attack</a>	5 days ago Jul 11, 2020 4:02 AM	New	Kristjan Egilsson	> 700 Files Encrypted	None

### ⚠ Warnings (0)

Abnormal Behaviour	Detected ↓	Status	User	Change	Action Taken
No Data Available					

세부 정보 페이지(이 예에서는 잠재적인 랜섬웨어 공격을 보여줍니다):



POTENTIAL ATTACK: AL\_305  
Ransomware Attack

Detected  
5 days ago  
Jul 11, 2020 4:02 AM

Action Taken  
None

Status  
New

#### Total Attack Results

1 Affected Volumes | 0 Deleted Files | 4173 Encrypted Files

4173 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.  
The extension "crypt" was added to each file.

#### Encrypted Files

Activity per minute



#### Related Users



**Kristjan Egilsson**  
Accountant  
Finance

4173  
Encrypted Files

Detected  
5 days ago  
Jul 11, 2020 4:02 AM

Action Taken  
None



Username  
us035  
  
Email  
Egilsson@netapp.com  
  
Phone  
387224312607

Department  
Finance  
  
Manager  
Lyndsey Maddox

#### Top Activity Types

Activity per minute  
Last access location: 10.197.144.115

[View Activity Detail](#)



## \_스냅샷 작업 수행

워크로드 보안은 악의적인 활동이 감지되면 스냅샷을 자동으로 생성하여 데이터를 보호하고 데이터가 안전하게 백업되도록 합니다.

을 정의할 수 있습니다 "자동화된 응답 정책" 랜섬웨어 공격 또는 기타 비정상적인 사용자 활동이 감지되면 스냅샷을 생성합니다. 알림 페이지에서 수동으로 스냅샷을 생성할 수도 있습니다.

자동 스냅샷 촬영

:



**POTENTIAL ATTACK: AL\_307**  
Ransomware Attack

**Detected**  
4 days ago  
Jul 26, 2020 3:38 AM

**Action Taken**  
Snapshots Taken

**Status**  
In Progress

Last snapshots taken by  
Amit Schwartz  
Jul 30, 2020 2:54 PM

How To:  
[Restore Entities](#)

[Re-Take Snapshots](#)

**Total Attack Results**

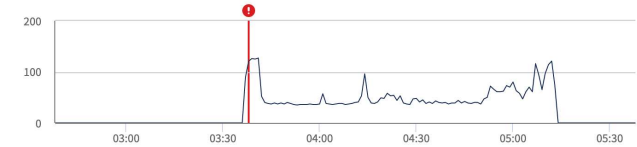
**1** Affected Volumes | **0** Deleted Files | **5148** Encrypted Files

5148 Files have been copied, deleted, and potentially encrypted by 1 user account.

This is potentially a sign of ransomware attack.  
The extension "crypt" was added to each file.

**Encrypted Files**

Activity per minute



**Related Users**



**Ewen Hall**  
Developer  
Engineering

**5148**  
Encrypted Files

**Detected**  
4 days ago  
Jul 26, 2020 3:38 AM

**Action Taken**  
Snapshots Taken

수동 스냅샷

:

Cloud Insights
Abhi Basu Thakur

---

MONITOR & OPTIMIZE Alerts / **Nabilah Howell had an abnormal change in activity rate**
Jul 23, 2020 - Jul 26, 2020  
1:44 AM 1:44 AM

CLOUD SECURE

- 🔔 ALERTS
- 🔍 FORENSICS
- ⚙️ ADMIN
- 📘 HELP

Minimize

**Alert Detail**

**WARNING: AL\_306**

**Nabilah Howell had an abnormal change in activity rate.**

**Detected**  
5 days ago  
Jul 25, 2020 1:44 PM

**Action Taken**  
None

**Status**  
New

*Recommendation: Setup an Automated Response Policy*  
An Automated Response Policy will trigger measures to contain the damage automatically when a future attack is detected. [Try it now.](#)

Take Snapshots
How To:  
Restore Entities

**Nabilah Howell's Activity Rate Change**

Typical	Alert	↑ 71%
<b>122.8</b>	<b>210</b>	
Activities Per Minute	Activities Per Minute	

*Nabilah Howell's activity rate grew 71% over their typical average.*

**Activity Rate**

Activity per 5 minutes

경고 알림

알림의 전자 메일 알림은 알림의 모든 작업에 대해 알림 받는 사람 목록으로 전송됩니다. 알림 수신자를 구성하려면 \* Admin > Notifications \* 를 클릭하고 각 수신자의 이메일 주소를 입력합니다.

보존 정책

경고 및 경고는 13개월 동안 유지됩니다. 13개월 이전의 경고 및 경고가 삭제됩니다. 워크로드 보안 환경이 삭제된 경우

541



환경과 관련된 모든 데이터도 삭제됩니다.

## 문제 해결

문제:	다음을 시도해 보십시오.
ONTAP에서 매일 매시간 스냅샷을 생성하는 경우가 있습니다. WS(Workload Security) 스냅샷이 영향을 줍니까? WS 스냅샷은 시간별 스냅샷 위치를 차지합니까? 기본 시간별 스냅샷이 중지됩니까?	워크로드 보안 스냅샷은 시간별 스냅샷에 영향을 주지 않습니다. WS 스냅샷은 매시간 스냅샷 공간을 차지하지 않으며 이전과 같이 계속되어야 합니다. 기본 시간별 스냅샷은 중지되지 않습니다.
ONTAP에서 최대 스냅샷 수에 도달하면 어떻게 됩니까?	최대 스냅샷 수에 도달하면 후속 스냅샷 찍기가 실패하고 워크로드 보안에서 스냅샷이 가득 찼다는 오류 메시지가 표시됩니다. 사용자는 가장 오래된 스냅샷을 삭제하기 위해 스냅샷 정책을 정의해야 합니다. 그렇지 않으면 스냅샷이 생성되지 않습니다. ONTAP 9.3 이전 버전에서는 볼륨에 최대 255개의 스냅샷 복사본이 포함될 수 있습니다. ONTAP 9.4 이상에서는 볼륨에 최대 1023개의 스냅샷 복사본을 포함할 수 있습니다. 에 대한 자세한 내용은 ONTAP 설명서를 참조하십시오 " <a href="#">스냅샷 삭제 정책 설정 중</a> ".
워크로드 보안에서 스냅샷을 생성할 수 없습니다.	스냅샷을 생성하는 데 사용되는 역할에 <a href="https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions">https://docs.netapp.com/us-en/cloudinsights/task_add_collector_svm.html#a-note-about-permissions</a> [proper 권한이 할당된 링크가 있는지 확인합니다. 스냅샷 촬영을 위한 적절한 액세스 권한으로 <code>_csrole_이(가) 생성되었는지 확인합니다. 보안 로그인 역할 <code>create -vserver &lt;vservername&gt; -role csrole -cmddirname "volume snapshot" -access all</code></code>
워크로드 보안에서 제거된 SVM에 대한 이전 경고에 대해 스냅샷이 실패하고, 이후에 다시 추가됩니다. SVM을 다시 추가한 후에 발생하는 새 경고의 경우 스냅샷이 생성됩니다.	이는 드문 시나리오입니다. 이 문제가 발생하는 경우 ONTAP에 로그인하고 이전 알림에 대해 스냅샷을 수동으로 생성합니다.
Alert Details_ 페이지에서 <i>Take Snapshot</i> 버튼 아래에 "Last attempt failed" 오류 메시지가 표시됩니다. 오류 위로 마우스를 가져가면 "ID가 있는 데이터 수집기에 대해 API 호출 명령이 시간 초과되었습니다"라는 메시지가 표시됩니다.	이는 SVM의 LIF가 ONTAP에서 <code>_disabled_state</code> 인 경우 SVM 관리 IP를 통해 데이터 수집기를 워크로드 보안에 추가할 때 발생할 수 있습니다. ONTAP에서 특정 LIF를 설정하고 워크로드 보안에서 <code>_trigger_Take Snapshot manually_</code> 를 트리거합니다. 그러면 스냅샷 작업이 성공합니다.

## 법의학

### 법의학 - 모든 활동

모든 활동 페이지에서는 워크로드 보안 환경의 엔터티에 대해 수행되는 작업을 이해할 수 있습니다.

### 모든 활동 데이터 검토

Forensics > Activity Forensics \* 를 클릭하고 \* All Activity \* 탭을 클릭하여 All Activity 페이지에 액세스합니다. 이

페이지에서는 다음 정보를 중심으로 사용자 환경의 활동에 대한 개요를 제공합니다.

- Activity History \_(활동 내역)를 보여주는 그래프(선택한 전역 시간 범위에 따라 분당 5분/10분에 액세스됨)  
그래프에서 사각형을 드래그하여 그래프를 확대할 수 있습니다. 확대/축소된 시간 범위를 표시하기 위해 전체 페이지가 로드됩니다. 확대하면 사용자가 축소할 수 있는 버튼이 표시됩니다.
- 활동 유형 \_의 차트. 활동 유형별 활동 기록 데이터를 얻으려면 해당 X축 레이블 링크를 클릭합니다.
- 엔티티 유형 \_에 대한 활동 차트. 엔티티 유형별로 활동 기록 데이터를 가져오려면 해당 X축 레이블 링크를 클릭합니다.
- All Activity\_data의 목록입니다

\_ \* All Activity \* \_ 표에는 다음 정보가 표시됩니다. 이러한 열 중 일부만 기본적으로 표시됩니다. "기어" 아이콘을 클릭하여 표시할 열을 선택할 수 있습니다.

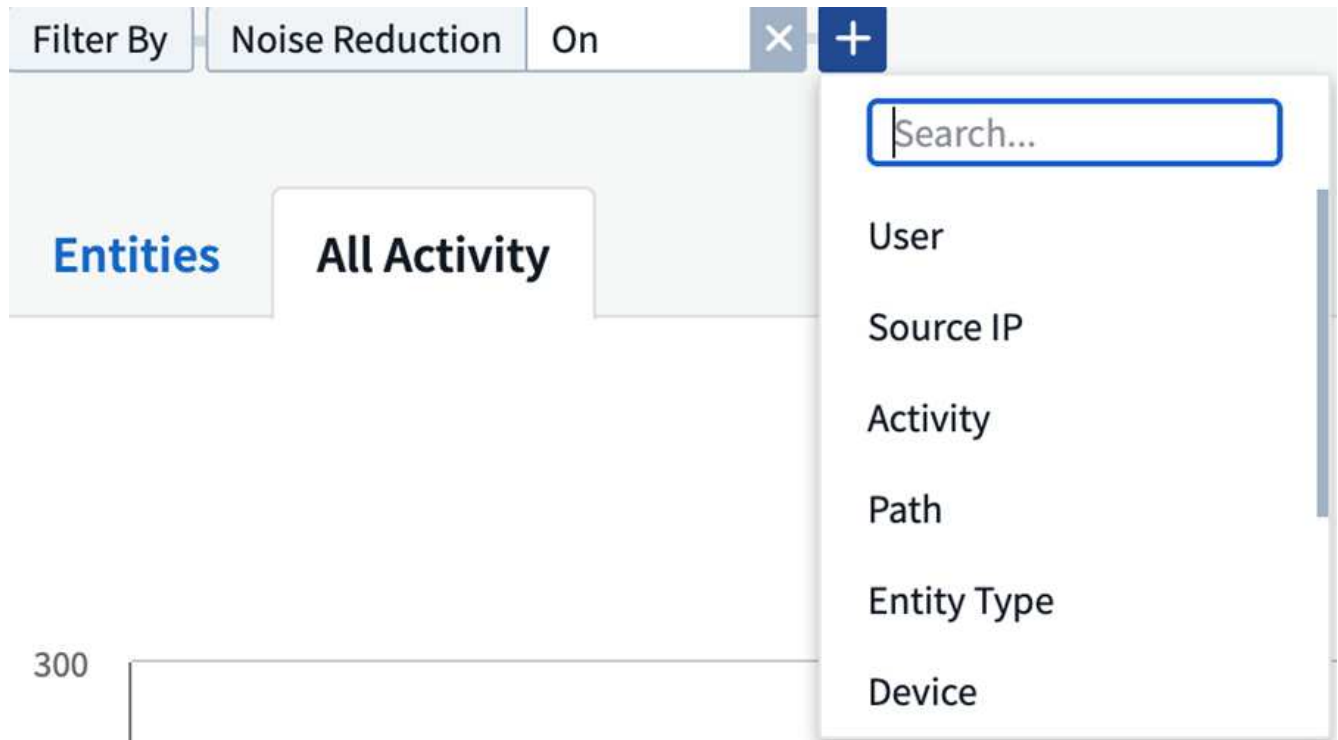
- 마지막 액세스의 연도, 월, 일 및 시간을 포함하여 엔티티에 액세스한 \* 시간.
- 엔티티에 액세스한 \* 사용자 \*입니다 "[사용자 정보](#)".
- 사용자가 수행한 \* 작업 \*. 지원되는 유형은 다음과 같습니다.
  - \* 그룹 소유권 변경 \* - 파일 또는 폴더의 그룹 소유권이 변경됩니다. 그룹 소유권에 대한 자세한 내용은 을 참조하십시오 "[이 링크](#)."
  - \* 소유자 변경 \* - 파일 또는 폴더의 소유권이 다른 사용자로 변경됩니다.
  - \* 권한 변경 \* - 파일 또는 폴더 권한이 변경됩니다.
  - \* 생성 \* - 파일 또는 폴더를 생성합니다.
  - \* 삭제 \* - 파일 또는 폴더를 삭제합니다. 폴더가 삭제되면 해당 폴더 및 하위 폴더에 있는 모든 파일에 대해 \_DELETE\_events가 획득됩니다.
  - \* 읽기 \* - 파일을 읽습니다.
  - \* 메타데이터 읽기 \* - 폴더 모니터링 활성화 옵션만 해당. Windows에서 폴더를 열거나 Linux의 폴더 내에서 "ls"를 실행하면 생성됩니다.
  - \* 이름 바꾸기 \* - 파일 또는 폴더의 이름을 바꿉니다.
  - \* 쓰기 \* - 데이터가 파일에 기록됩니다.
  - \* 메타데이터 쓰기 \* - 파일 메타데이터는 예를 들어 권한이 변경되었습니다.
  - \* 기타 변경 \* - 위에 설명되지 않은 기타 이벤트. 매핑되지 않은 모든 이벤트는 "기타 변경" 작업 유형에 매핑됩니다. 파일 및 폴더에 적용됩니다.
- 에 대한 링크가 있는 엔티티에 대한 \* 경로 \*입니다 "[엔티티 세부 정보 데이터](#)"
- 엔티티(예: 파일) 확장자(.doc, .docx, .tmp 등)를 포함한 \* 엔티티 유형 \*
- 엔티티가 상주하는 \* 장치 \*
- 이벤트를 가져오는 데 사용되는 \* 프로토콜 \*입니다.
- 원본 파일의 이름을 바꿀 때 이름 바꾸기 이벤트에 사용되는 \* Original Path \*입니다. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 테이블에 추가합니다.
- 요소가 있는 \* 볼륨 \*. 이 열은 기본적으로 표에 표시되지 않습니다. 열 선택기를 사용하여 이 열을 테이블에 추가합니다.

## Forensic 활동 기록 데이터 필터링

데이터를 필터링하는 데 사용할 수 있는 두 가지 방법이 있습니다.

1. 테이블의 필드 위로 마우스를 가져가서 표시되는 필터 아이콘을 클릭합니다. 이 값은 top\_Filter by\_list의 해당 필터에 추가됩니다.
2. Filter by\_ 필드에 입력하여 데이터를 필터링합니다.

상단 '필터 기준' 위젯에서 \* [+ ] \* 버튼을 클릭하여 적절한 필터를 선택합니다.



검색 텍스트를 입력합니다

Enter 키를 누르거나 필터 상자 바깥쪽을 클릭하여 필터를 적용합니다.

다음 필드를 사용하여 Forensic Activity 데이터를 필터링할 수 있습니다.

- Activity \* 유형.
- 엔터티에 액세스한 소스 IP \* 입니다. 유효한 소스 IP 주소를 큰따옴표로 묶어야 합니다(예: "10.1.1.1."). "10.1.1.", "10.1.\*" 등과 같은 불완전한 IP는 작동하지 않습니다.
- 프로토콜 특정 작업을 가져오려면 \* 프로토콜 \* 을 선택합니다.
- \* 작업을 수행하는 사용자의 사용자 이름 \* 입니다. 필터링할 정확한 사용자 이름을 입력해야 합니다. 부분 사용자 이름 또는 접두사가 붙은 부분 사용자 이름 또는 ' \* '로 접미사를 바꾼 검색은 작동하지 않습니다.
- \* 노이즈 감소 \* - 사용자가 최근 2시간 내에 생성한 파일을 필터링합니다. 사용자가 액세스하는 임시 파일(예: .tmp 파일)을 필터링하는 데에도 사용됩니다.
- 활동을 수행하는 사용자의 \* 도메인 \*. 필터링할 \* 정확한 도메인 \* 을 제공해야 합니다. 부분 도메인 또는 부분 도메인 앞에 와일드카드(' \* ')가 있거나 접미사가 붙은 부분 도메인 검색은 작동하지 않습니다. \_None\_은(는) 누락된 도메인을 검색하기 위해 지정할 수 있습니다.

다음 필드에는 특수 필터링 규칙이 적용됩니다.

- **Entity Type**, entity(파일) 확장자를 사용하는 경우 - 따옴표 안에 정확한 엔터티 유형을 지정하는 것이 좋습니다. 예: `_ "txt" _`.
- \*엔터티의 경로\* - 디렉터리 경로 필터(경로 문자열 / 로 끝나는)를 최대 4개까지 입력하여 더 빠른 결과를 얻을 수 있습니다. 예: `/home/userX/nested1/nested2/_or"/home/userX/nested1/nested2/"_`. 자세한 내용은 아래 표를 참조하십시오.
- \* 사용자 \* 활동 수행 - 따옴표 안에 정확한 사용자를 지정하는 것이 좋습니다. 예: `_ "관리자" _`.
- 엔터티가 상주하는 \* 장치 \* (SVM)
- \* 볼륨 \* 요소가 상주하는 곳입니다
- 원본 파일의 이름을 바꿀 때 이름 바꾸기 이벤트에 사용되는 \* Original Path \* 입니다.

필터링 시 위의 필드는 다음 항목의 대상이 됩니다.

- 정확한 값은 따옴표 안에 있어야 합니다. 예: `"searchText"`
- 와일드카드 문자열은 따옴표를 포함하지 않아야 합니다. 예: `searchText, \* searchText*`, 는 'earchtext'가 포함된 문자열을 필터링합니다.
- 접두사가 있는 문자열(예: `searchText*`)은 'earchtext'로 시작하는 문자열을 검색합니다.

활동 포렌식 필터 예:

사용자가 필터 식을 적용했습니다	예상 결과	성능 평가	설명
경로 = /home/userX/nested1/nested2/ 또는 /home/userX/nested1/nested2/ * 또는 "/home/userX/nested1/nested2/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	빠릅니다	디렉터리 검색은 최대 4개의 디렉터리가 빠릅니다.
경로 = /home/userX/nested1/ 또는 /home/userX/nested1/ * 또는 "/home/userX/nested1/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	빠릅니다	디렉터리 검색은 최대 4개의 디렉터리가 빠릅니다.
경로 = /home/userX/nested1/test * 또는 /home/userX/nested1/test	지정된 경로 regex 아래의 모든 파일과 폴더의 반복적인 조회(테스트 * 는 파일 또는 디렉터리 또는 둘 다를 의미할 수 있음)	느린 속도	디렉터리+파일 정규식 검색은 디렉터리 검색보다 검색 속도가 느립니다.

사용자가 필터 식을 적용했습니다	예상 결과	성능 평가	설명
경로 = /home/userX/nested1/nested2/nested3/ 또는 /home/userX/nested1/nested2/nested3/ * 또는 "/home/userX/nested1/nested2/nested3/"	지정된 디렉토리 아래의 모든 파일과 폴더의 반복적인 조회	느린 속도	4개 이상의 디렉터리 검색은 검색 속도가 느립니다.
경로 = \ userX/nested1/test *	지정된 와일드카드 경로 문자열(test * 는 파일 또는 디렉터리 또는 둘 모두를 의미할 수 있음)에 있는 모든 파일과 폴더의 반복적인 조회	가장 느립니다	선행 와일드카드 검색은 가장 느린 검색입니다.
기타 모든 비 경로 기반 필터. 사용자 및 엔터티 유형 필터는 다음표로 묶는 것이 좋습니다. 예: User="Administrator" Entity Type="txt"		빠릅니다	

#### 참고:

1. 선택한 시간 범위가 3일 이상인 경우 모든 활동 아이콘 옆에 표시된 활동 수는 30분으로 반올림됩니다. 예: 9월 1일 오전 10시 15분부터 9월 7일 오전 10시 15분까지의 시간 범위에는 9월 1일 오전 10시부터 9월 7일 오전 10시 30분까지 활동 카운트가 표시됩니다.
2. 마찬가지로, 선택한 시간 범위가 3일 이상이면 활동 유형, 활동 유형, 활동 기록 그래프에 표시된 카운트 메트릭도 30분으로 반올림됩니다.

#### 법의학적 활동 기록 데이터 정렬

활동 기록 데이터는 시간, 사용자, 소스 IP, 활동, \_ 및 \_Entity Type 별로 정렬할 수 있습니다. 기본적으로 테이블은 Descending\_time\_order를 기준으로 정렬됩니다. 즉, 최신 데이터가 먼저 표시됩니다. Device\_and\_Protocol\_fields에 대해 정렬이 사용되지 않습니다.

#### 비동기 내보내기에 대한 사용자 안내서

##### 개요

스토리지 워크로드 보안의 비동기식 내보내기 기능은 대규모 데이터 내보내기를 처리하도록 설계되었습니다.

단계별 가이드: 비동기 내보내기를 사용하여 데이터 내보내기

1. \* 내보내기 시작 \* : 내보내기에 대해 원하는 시간 기간과 필터를 선택하고 내보내기 버튼을 클릭합니다.
2. \* 내보내기가 완료될 때까지 대기 \* : 처리 시간은 몇 분에서 몇 시간까지 소요될 수 있습니다. 포렌식 페이지를 몇 번 새로 고쳐야 할 수 있습니다. 내보내기 작업이 완료되면 "마지막 내보내기 CSV 파일 다운로드" 버튼이 활성화됩니다.
3. \* 다운로드 \* : "마지막 생성 내보내기 파일 다운로드" 버튼을 클릭하여 .zip 형식으로 내보낸 데이터를 가져옵니다. 이 데이터는 사용자가 다른 비동기 내보내기를 시작하거나 3일이 경과할 때까지 다운로드할 수 있습니다. 이 버튼은

다른 비동기 내보내기가 시작될 때까지 활성화된 상태로 유지됩니다.

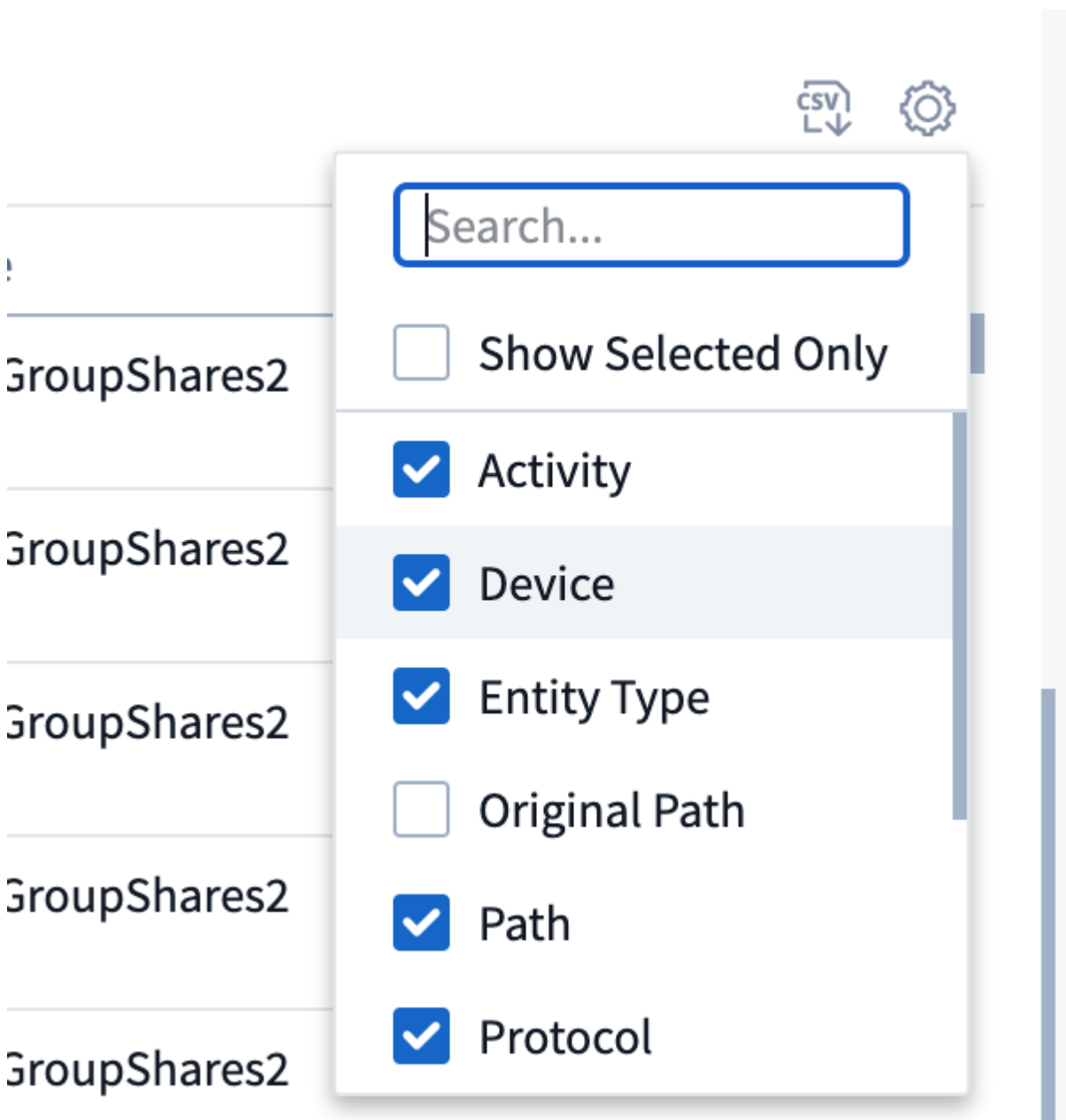
4. \* 제한 사항 \*:

- 비동기 다운로드 수는 현재 사용자당 1개, 테넌트당 3개로 제한됩니다.
- 내보낸 데이터는 최대 100만 개의 레코드로 제한됩니다.

API를 통해 포렌식 데이터를 추출하는 샘플 스크립트는 에이전트의 `_opt/NetApp/cloudsecure/agent/export-script/`에 있습니다. 스크립트에 대한 자세한 내용은 이 위치에 있는 Readme 파일을 참조하십시오.

모든 활동에 대한 열 선택

ALLACTIVITY\_TABLE에는 기본적으로 선택 열이 표시됩니다. 열을 추가, 제거 또는 변경하려면 테이블 오른쪽에 있는 기어 아이콘을 클릭하고 사용 가능한 열 목록에서 선택합니다.



## 활동 기록 보존

활성 워크로드 보안 환경에서는 활동 기록이 13개월 동안 유지됩니다.

## 포렌식 페이지의 필터 적용 가능성

필터	기능	예	이 필터에 적용 가능합니다	이러한 필터에는 적용되지 않습니다	결과
* (별표)	모든 것을 검색할 수 있습니다	Auto * 03172022 검색 텍스트에 하이픈 또는 밑줄이 포함된 경우 대괄호로 표현식을 지정합니다. 예: svm-123 검색에는 (svm *)	사용자, 경로, 엔터티 유형, 장치, 볼륨, 원래 경로		"Auto"로 시작하고 "03172022"로 끝나는 모든 리소스를 반환합니다.
? (물음표)	특정 수의 문자를 검색할 수 있습니다	AutoSabotageUs er1_03172022?	사용자, 엔터티 유형, 장치, 볼륨		AutoSabotageUs er1_03172022A, AutoSabotageUs er1_03172022B, AutoSabotageUs er1_031720225 등을 반환합니다
또는	여러 요소를 지정할 수 있습니다	AutoSabotageUs er1_03172022 또는 AutoRansomUse r4_03162022	사용자, 도메인, 경로, 엔터티 유형, 원래 경로		AutoSabotageUs er1_03172022 또는 AutoRansomUse r4_03162022 중 하나를 반환합니다
아닙니다	검색 결과에서 텍스트를 제외할 수 있습니다	AutoRansomUse r4_03162022가 아닙니다	사용자, 도메인, 경로, 엔터티 유형, 원래 경로	장치	"AutoRansomUs er4_03162022" 로 시작하지 않는 모든 항목을 반환합니다.
없음	모든 필드에서 NULL 값을 검색합니다	없음	도메인		대상 필드가 비어 있는 결과를 반환합니다

## 경로/원래 경로 검색

/을(를) 사용하거나 사용하지 않고 검색 결과는 다릅니다

/AutoDir1/AutoFile 을 선택합니다	작동합니다
자동 방향1/자동 파일	작동하지 않습니다
/AutoDir1/AutoFile(Dir1)	dir1 부분 부분 부분 부분 부분 부분 문자열이 작동하지 않습니다
"/AutoDir1/AutoFile03242022"	정확한 검색이 가능합니다

자동 * 03242022	작동하지 않습니다
AutoSabotageUser1_03172022?	작동하지 않습니다
/AutoDir1/AutoFile03242022 또는 /AutoDir1/AutoFile03242022	작동합니다
NOT/AutoDir1/AutoFile03242022	작동합니다
NOT/AutoDir1	작동합니다
NOT/AutoFile03242022	작동하지 않습니다
*	모든 항목을 표시합니다

### 로컬 루트 SVM 사용자 활동 변경

로컬 루트 SVM 사용자가 작업을 수행하는 경우 NFS 공유가 마운트된 클라이언트의 IP가 사용자 이름에 고려되며, 이 IP는 포렌식 작업 및 사용자 활동 페이지 모두에서 root@<ip-address-of-the-client>로 표시됩니다.

예를 들면 다음과 같습니다.

- SVM-1이 워크로드 보안에 의해 모니터링되고 해당 SVM의 루트 사용자가 IP 주소가 10.197.12.40인 클라이언트에 공유를 마운트하는 경우, 포렌식 활동 페이지에 표시되는 사용자 이름은 root@10.197.12.40 입니다.
- 동일한 SVM-1이 IP 주소가 10.197.12.41인 다른 클라이언트에 마운트되는 경우 법의학 활동 페이지에 표시되는 사용자 이름은 root@10.197.12.41 입니다.
- IP 주소별로 NFS 루트 사용자 활동을 분리하는 데 사용됩니다. 이전에는 모든 활동이 IP 구분 없이 \_root\_user 만 수행하는 것으로 간주되었습니다.

### 문제 해결

문제	시도해 보십시오
<p>“All Activities(모든 활동)” 테이블의 ‘User(사용자)’ 열 아래에 사용자 이름이 “LDAP:HQ.COMPANYNAME.COM:S-1-5-21-3577637-1906459482-1437260136-1831817” 또는 “LDAP:default:80038003”으로 표시됩니다.</p>	<p>가능한 원인은 다음과 같습니다.</p> <ol style="list-style-type: none"> <li>1. 아직 구성된 사용자 디렉토리 수집기가 없습니다. 하나를 추가하려면 * Workload Security &gt; Collector &gt; User Directory Collector * 로 이동하고 * + User Directory Collector * 를 클릭합니다. Active Directory_or_LDAP Directory Server_를 선택합니다.</li> <li>2. 사용자 디렉토리 수집기가 구성되었지만 중지되었거나 오류 상태입니다. Collectors &gt; User Directory Collectors * 로 이동하여 상태를 확인하십시오. 을 참조하십시오 <a href="#">"사용자 디렉토리 수집기 문제 해결"</a> 문제 해결 팁에 대한 문서 섹션.</li> </ol> <p>올바르게 구성하면 24시간 내에 자동으로 이름이 확인됩니다.</p> <p>그래도 해결되지 않으면 올바른 사용자 데이터 수집기를 추가했는지 확인합니다. 사용자가 실제로 추가된 Active Directory/LDAP Directory Server에 속하는지 확인합니다.</p>



<p>일부 NFS 이벤트는 UI에서 표시되지 않습니다.</p>	<p>다음을 확인하십시오. 1. POSIX 속성이 설정된 AD 서버의 사용자 디렉토리 수집기는 UI에서 활성화된 unixid 속성으로 실행해야 합니다. 2. NFS 액세스를 수행하는 모든 사용자는 UI 3의 사용자 페이지에서 검색할 때 표시됩니다. 원시 이벤트(사용자가 아직 검색되지 않은 이벤트)는 NFS 4에서 지원되지 않습니다. NFS 내보내기에 대한 익명 액세스는 모니터링되지 않습니다. NFS 버전이 NFS4.1 보다 적게 사용되었는지 확인합니다.</p>
<p>Forensics_All Activity_or_Entities_pages의 필터에 별표(*)와 같은 와일드카드 문자가 포함된 일부 문자를 입력하면 페이지가 매우 느리게 로드됩니다.</p>	<p>검색 문자열의 별표(\)는 모든 항목을 검색합니다. 그러나 <code>* &lt;searchTerm&gt;_</code> 또는 <code>* &lt;searchTerm&gt; *</code> 과(와) 같은 선행 와일드카드 문자열은 쿼리 속도를 느리게 만듭니다. 보다 나은 성능을 얻으려면 접두사 문자열을 대신 <code>&lt;searchTerm&gt;*</code> 형식으로 사용합니다(즉, 별표( )<code>after_a</code> 검색 용어를 추가합니다). 예: <code>_ * testvolume_or * test * volume_</code> 대신 <code>testvolume *</code> 문자열을 사용하십시오. 디렉토리 검색을 사용하여 지정된 폴더 아래의 모든 활동을 재귀적으로 봅니다(계층 검색). 예: <code>/path1/path2/path3/</code> 또는 <code>"/path1/path2/path3/"</code>는 <code>/path1/path2/path3</code> 아래의 모든 활동을 재귀적으로 나열합니다. 또는 All Activity(모든 활동) 탭 아래의 "Add to Filter(필터에 추가)" 옵션을 사용합니다.</p>
<p>경로 필터를 사용할 때 "상태 코드 500/503으로 요청 실패" 오류가 발생합니다.</p>	<p>레코드를 필터링하려면 더 작은 날짜 범위를 사용하십시오.</p>
<p>Forensic UI에서 <code>_PATH_FILTER</code>를 사용할 때 데이터가 느리게 로드되고 있습니다.</p>	<p>더 빠른 결과를 위해 디렉토리 경로 필터(경로 문자열 / 로 끝나는)를 최대 4개까지 사용하는 것이 좋습니다. 예를 들어 디렉토리 경로가 <code>/aa/bbb/cc/dd</code>인 경우 <code>/aa/bb/cc/dd/</code> 또는 <code>"/aa/bbb/cc/dd/"</code>를 검색하여 데이터를 더 빨리 로드합니다.</p>

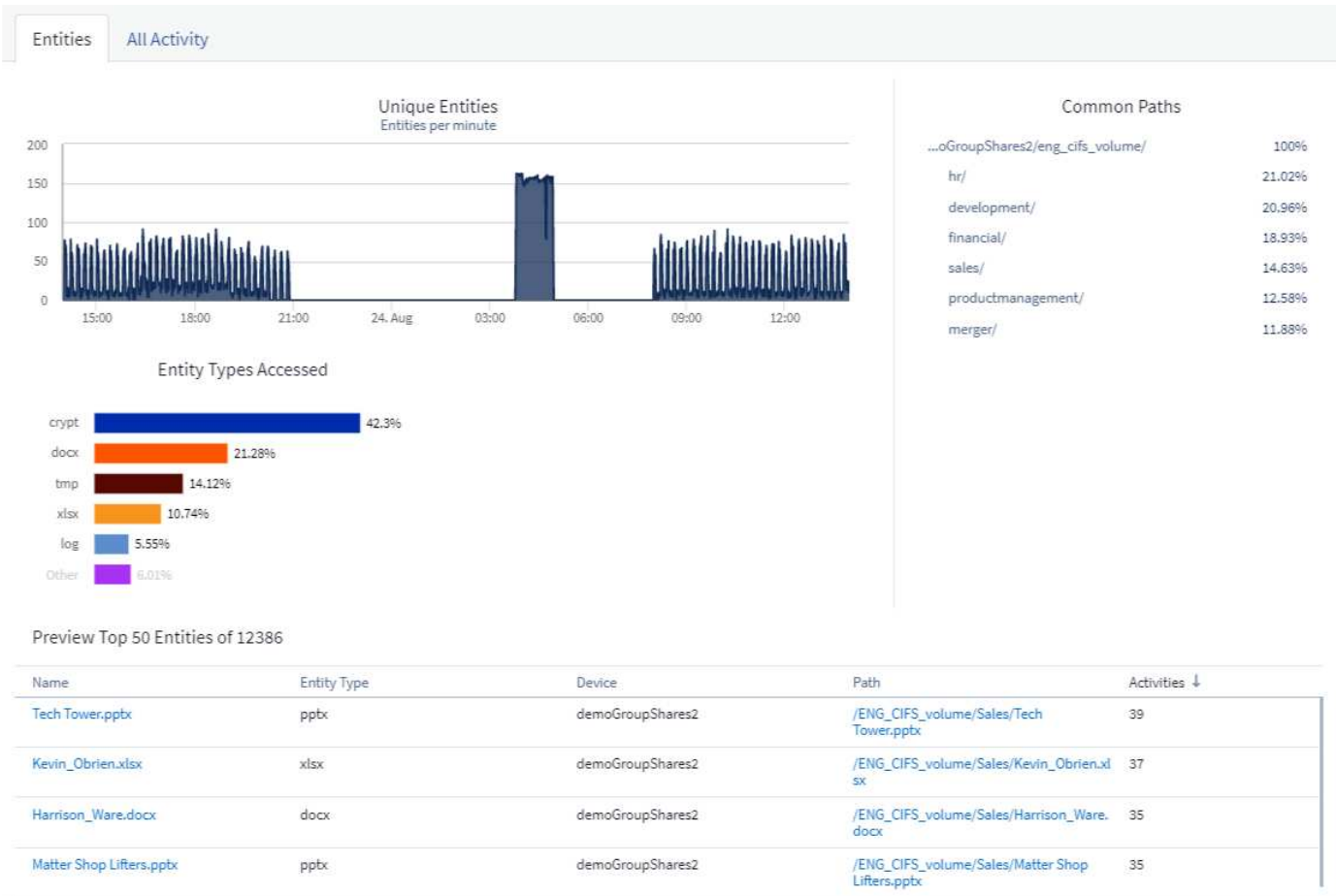
## 포렌식 엔터티 페이지

Forensics Entities 페이지에는 사용자 환경의 엔티티 활동에 대한 자세한 정보가 제공됩니다.

### 엔터티 정보 검사

Forensics > Activity Forensics \* 를 클릭하고 `_Entities_` 탭을 클릭하여 Entities 페이지에 액세스합니다.

이 페이지에서는 사용자 환경의 엔티티 활동에 대한 개요를 제공하고 다음 정보를 강조 표시합니다. \* 분당 `_` 개의 고유 엔터티가 표시된 그래프 \* 액세스된 `_` \* 액세스 엔터티 유형의 차트 \* 전체 엔터티 수 중 `_` 상위 50개 엔터티의 분류 \*



목록에서 엔티티를 클릭하면 엔티티의 개요 페이지가 열리고 이름, 유형, 장치 이름, 가장 많이 액세스되는 위치 IP 및 경로 등의 세부 정보와 사용자, IP, 경로 등의 엔티티 동작이 표시됩니다. 엔티티에 마지막으로 액세스한 시간입니다.



Entity Overview

### Entity Profile

<b>Name</b> Kevin_Obrien.xlsx	<b>Most Accessed Location</b> 10.197.144.115	<b>Size</b> 91 KB
<b>Type</b> xlsx	<b>Device Name</b> demoGroupShares2	<b>Path</b> /ENG_CIFS_volume/Sales/Kevin_Obrien.xlsx

### Entity Behaviour

<b>Recent Activity</b>	<b>Operations (last 7 days)</b>
Last accessed : 12 minutes ago Aug 24, 2020 2:02 PM	Read :89
Last accessed by: Tyrique Ray	Read Metadata :22
Last accessed from : 10.197.144.115	Other Activities :43

## Forensic 사용자 개요

각 사용자에게 대한 정보는 사용자 개요 에 나와 있습니다. 이러한 뷰를 사용하여 사용자 특성, 관련

엔터티 및 최근 활동을 파악할 수 있습니다.

#### 사용자 프로필

사용자 프로필 정보에는 사용자의 연락처 정보 및 위치가 포함됩니다. 프로필은 다음 정보를 제공합니다.

- 사용자의 이름입니다
- 사용자의 이메일 주소입니다
- 사용자 관리자
- 사용자의 전화 연락처입니다
- 사용자의 위치입니다

#### 사용자 행동

사용자 동작 정보는 사용자가 수행한 최근 작업 및 작업을 식별합니다. 이 정보에는 다음이 포함됩니다.

- 최근 활동
  - 마지막 액세스 위치입니다
  - 활동 그래프
  - 경고
- 최근 7일 동안의 작업
  - 작업 수

#### 새로 고침 간격

사용자 목록은 12시간마다 새로 고쳐집니다.

#### 보존 정책

다시 새로 고치지 않으면 사용자 목록이 13개월 동안 유지됩니다. 13개월 후 데이터가 삭제됩니다. 워크로드 보안 환경이 삭제된 경우 환경과 관련된 모든 데이터가 삭제됩니다.

## 자동 응답 정책

응답 정책은 공격 또는 비정상적인 사용자 동작이 발생하는 경우 스냅샷을 생성하거나 사용자 액세스를 제한하는 등의 작업을 트리거합니다.

특정 장치 또는 모든 장치에 정책을 설정할 수 있습니다. 응답 정책을 설정하려면 \* Admin > Automated Response Policies \* 를 선택하고 해당 \* + Policy \* 버튼을 클릭합니다. 공격에 대한 정책 또는 경고에 대한 정책을 만들 수 있습니다.

## Add Attack Policy ✕

**Policy Name\***



---

**For Attack Type(s) \***

Ransomware Attack

Data Destruction - File Deletion

**On Device**

All Devices ▼

+ Another Device

---

**Actions**

Take Snapshot ?

Block User File Access ?

**Time Period**

12 hours ▼

Cancel
Save

고유한 이름으로 정책을 저장해야 합니다.

자동 응답 작업(예: 스냅샷 생성)을 사용하지 않으려면 해당 작업을 선택 해제하고 정책을 저장하면 됩니다.

지정된 디바이스 또는 모든 디바이스(선택된 경우)에 대해 알림이 트리거되면 자동 응답 정책이 데이터의 스냅샷을 생성합니다. 에서 스냅샷 상태를 볼 수 있습니다 ["경고 세부 정보 페이지"](#).

를 참조하십시오 ["사용자 액세스 제한"](#) 페이지로 이동하여 IP를 통한 사용자 액세스 제한에 대한 자세한 내용을 확인하십시오.

정책 드롭다운 메뉴에서 옵션을 선택하여 자동 응답 정책을 수정하거나 일시 중지할 수 있습니다.

워크로드 보안은 스냅샷 삭제 설정에 따라 하루에 한 번씩 스냅샷을 자동으로 삭제합니다.

## Snapshot Purge Settings



Define purge periods to automatically delete snapshots taken by Cloud Secure.

### Attack Automated Response

Delete Snapshot after

### Warning Automated Response

Delete Snapshot after

### User Created

Delete Snapshot after

Cancel

Save

## 허용된 파일 형식 정책

알려진 파일 확장명에 대한 랜섬웨어 공격이 감지되고 경고 화면에서 경고가 생성되는 경우 불필요한 경고를 방지하기 위해 해당 파일 확장명을 `_allowed file types_list`에 추가할 수 있습니다.

Workload Security > Policies \* 로 이동한 후 `_Allowed File Type Policies_tab`으로 이동합니다.

[Automated Response Policies](#)

[Allowed File Types Policies](#)

## Allowed File Types Policies

Ransomware alerts will not be triggered for the following file types:

허용된 파일 유형\_목록에 추가되면 해당 허용된 파일 유형에 대한 랜섬웨어 공격 경고가 생성되지 않습니다. `_allowed File Types_policy`는 랜섬웨어 탐지에만 적용됩니다.

예를 들어, 이름이 `_test.txt` 인 파일의 이름이 `_test.txt.abc_` 로 변경되고 Workload Security가 `_.abc_extension` 으로 인해 랜섬웨어 공격을 감지하는 경우 `_.abc_extension` 을 `_allowed file types_list` 에 추가할 수 있습니다. 목록에 추가된 후에는 `_.abc_extension` 을 가진 파일에 대해 랜섬웨어 공격이 더 이상 생성되지 않습니다.

허용되는 파일 형식은 정확히 일치하는 파일(예: `".abc"`) 또는 식(예: `". * type"`, `".type *"` 또는 `" * type *"`)일 수 있습니다. `".a * c"`, `".p * f"` 형식의 식은 지원되지 않습니다.

## ONTAP Autonomous 랜섬웨어 Protection과 통합

ONTAP ARP(Autonomous 랜섬웨어 보호) 기능은 NAS(NFS 및 SMB) 환경에서 워크로드 분석을 사용하여 랜섬웨어 공격을 나타낼 수 있는 비정상적인 파일 내 작업을 사전에 감지하여 경고합니다.

ARP에 대한 추가 세부 정보와 라이선스 요구 사항을 찾을 수 있습니다 ["여기"](#).

워크로드 보안은 ONTAP와 통합되어 ARP 이벤트를 수신하고 추가 분석 및 자동 응답 계층을 제공합니다.

워크로드 보안은 ONTAP에서 ARP 이벤트를 수신하고 다음 작업을 수행합니다.

1. 볼륨 암호화 이벤트와 사용자 활동의 상관 관계를 분석하여 손상을 일으키는 원인을 식별합니다.
2. 자동 응답 정책 구축(정의된 경우)
3. 포렌식 기능 제공:
  - 고객이 데이터 침해 조사를 수행할 수 있도록 허용합니다.
  - 영향을 받은 파일을 파악하여 복구 시간을 단축하고 데이터 침해 조사를 수행할 수 있습니다.

### 필수 구성 요소

1. 최소 ONTAP 버전: 9.11.1
2. ARP 사용 볼륨. ARP를 활성화하는 방법에 대한 세부 정보를 찾을 수 있습니다 ["여기"](#). ARP는 OnCommand 시스템 관리자를 통해 활성화해야 합니다. 워크로드 보안은 ARP를 활성화할 수 없습니다.
3. 워크로드 보안 수집기는 클러스터 IP를 통해 추가해야 합니다.
4. 이 기능을 사용하려면 클러스터 레벨 자격 증명이 필요합니다. 즉, SVM을 추가할 때 클러스터 레벨 자격 증명을 사용해야 합니다.

### 사용자 권한이 필요합니다

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: `CsUser`)를 사용하는 경우, 아래 단계를 따라 워크로드 보안에 권한을 부여하여 ONTAP에서 ARP 관련 정보를 수집합니다.

클러스터 자격 증명을 사용하여 `_CsUser_` 의 경우 ONTAP 명령줄에서 다음을 수행합니다.

```


security login rest-role create -role arwrole -api /api/storage/volumes
-access readonly -vserver <cluster_name>
security login rest-role create -api /api/security/anti-ransomware -access
readonly -role arwrole -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role arwrole

```

기타 구성에 대한 자세한 정보 "[ONTAP 권한](#)".

## 샘플 알림

ARP 이벤트로 인해 생성된 샘플 경고는 다음과 같다.



**POTENTIAL ATTACK: AL\_1315**  
Ransomware Attack

**Detected**  
5 months ago  
Oct 20, 2022 3:06 AM

**Action Taken**  
Access Blocked on 5 SVMs  
Snapshots Taken

**Status**  
New

Blocked permanently by auto response policy

Last snapshots taken by auto response policy Oct 20, 2022 3:09 AM

How To: [Restore Entities](#)

Change Block Period
Re-Take Snapshots

Unblock User

### Total Attack Results

<b>1</b> Affected Volumes	<b>83</b> Deleted Files	<b>81</b> Encrypted Files
------------------------------	----------------------------	------------------------------

81 Files have been copied, deleted, and potentially encrypted by 1 user account.

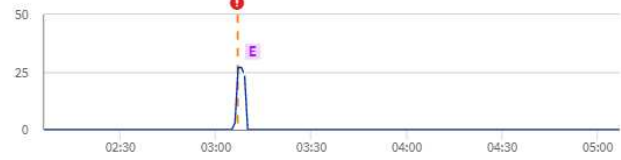
The extension "osiris" was added to each file.

High Confidence Detection

Ransomware behavior and in-file encryption activities were detected.


### Encrypted Files

Activity per minute



E Encryption activity in files

### Related Users



**Jamelia Graham**  
Business Partner  
HR

User/IP Access

Blocked

**81**  
Encrypted Files

**Detected**  
5 months ago  
Oct 20, 2022 3:06 AM

☰

---

Username  
us024

Domain  
cslab.netapp.com

Email  
Graham@netapp.com

Phone  
9251140014

Department  
HR

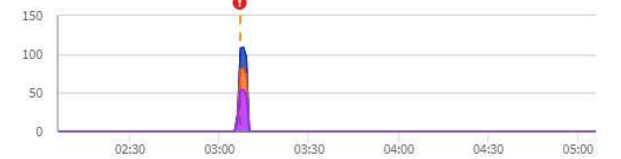
Manager  
[Iwan Holt](#)

Location  
WA

### Top Activity Types

Activity per minute  
Last accessed from: 10.193.113.247

View Activity Detail



556

### Access Limitation History for This User (3)

Time	Action	Duration	Action Taken by	Response	Blocked IPs on NFS
Oct 20, 2022 3:09 AM	Block <a href="#">more detail</a>	Never Expires		Automatic	none
Mar 10, 2022 4:59 AM	Unblock		system	Blocking Expired	10.197.144.115
Mar 10, 2022 3:57 AM	Block <a href="#">more detail</a>	1h		Automatic	10.197.144.115

### Affected Devices/Volumes

Device ↑	Volume	Encrypted Files	Associated Snapshot Taken
subprod_rtp	stargazer	81	Oct 20, 2022 3:09 AM cloudsecure_attack_auto Automatic _1666249787062 <a href="#">Take Snapshot</a>

고신뢰도 배너는 공격이 파일 암호화 활동과 함께 랜섬웨어 동작을 보여발생했음을 나타냅니다. 암호화된 파일 그래프는 ARP 솔루션이 볼륨 암호화 작업을 감지한 타임스탬프를 나타냅니다.

## 제한 사항

SVM이 워크로드 보안에 의해 모니터링되지 않지만 ONTAP에서 생성된 ARP 이벤트가 있는 경우, 해당 이벤트는 워크로드 보안에서 계속 수신되고 표시됩니다. 그러나 알림과 관련된 Forensic 정보 및 사용자 매핑은 캡처되거나 표시되지 않습니다.

## 문제 해결

알려진 문제와 해결 방법은 다음 표에 설명되어 있습니다.

문제:	해상도:
공격이 감지된 후 24시간 이내에 이메일 경고가 수신됩니다. UI에 Data Infrastructure Insights 워크로드 보안이 이메일을 수신하기 24시간 전에 경고가 표시됩니다.	ONTAP이 Data Infrastructure Insights 워크로드 보안(예: 워크로드 보안)으로 _Ransomware detected_Event를 전송하면 이메일이 전송됩니다. 이벤트에는 공격 목록과 타임 스탬프가 포함됩니다. 워크로드 보안 UI는 첫 번째 공격 파일의 경고 타임스탬프를 표시합니다. ONTAP은 특정 개수의 파일이 인코딩될 때 _Ransomware Detected_Event를 데이터 인프라 인사이트 로 전송합니다. 따라서 알림이 UI에 표시되는 시간과 이메일을 보낸 시간 사이에 차이가 있을 수 있습니다.

## ONTAP 액세스와의 통합이 거부되었습니다

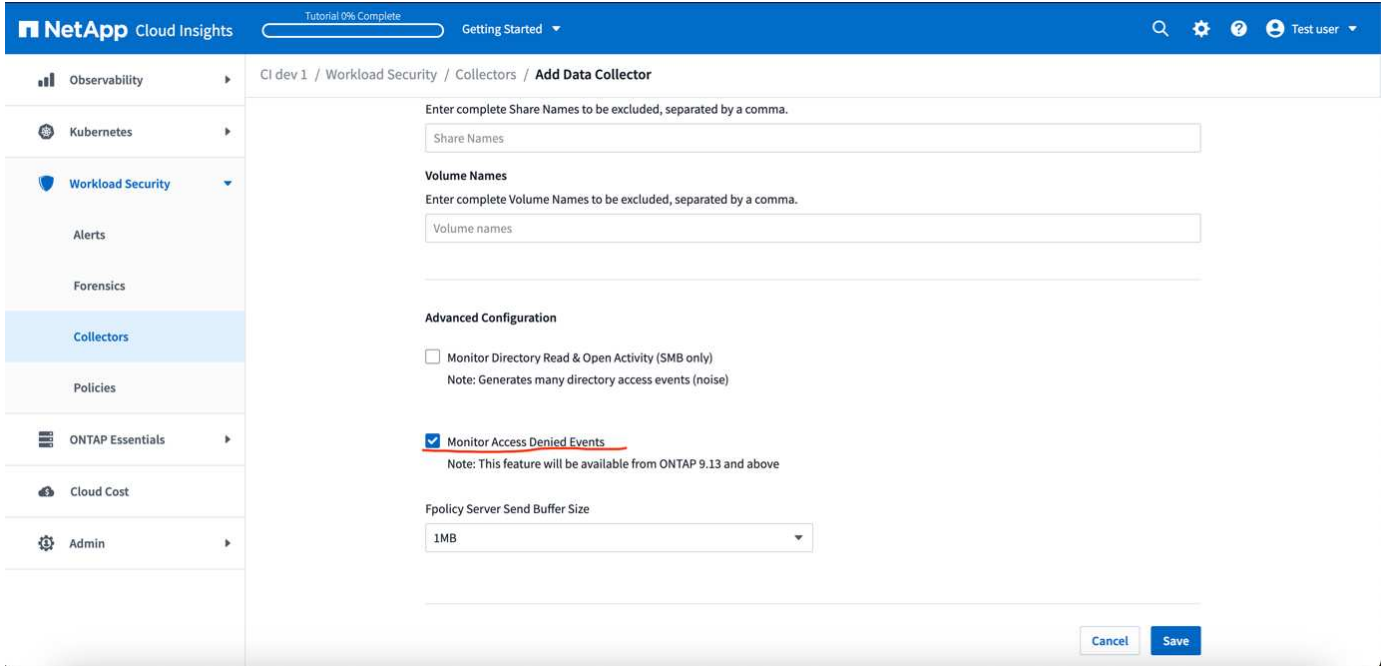
ONTAP 액세스 거부 기능은 NAS 환경(NFS 및 SMB)에서 워크로드 분석을 사용하여 실패한 파일 작업을 사전에 감지하여 경고합니다(예: 권한이 없는 작업을 수행하려는 사용자). 특히 보안 관련 오류의 경우 이러한 파일 작업 알림 실패 시 초기에 내부자 공격을 차단하는 데 도움이 됩니다.

Data Infrastructure Insights 워크로드 보안은 ONTAP과 통합되어 액세스 거부 이벤트를 수신하고 추가적인 분석 및 자동 응답 계층을 제공합니다.

### 필수 구성 요소



- 최소 ONTAP 버전: 9.13.0.
- 워크로드 보안 관리자는 고급 구성 아래에서 액세스 거부 이벤트 모니터링 확인란을 선택하여 새 수집기를 추가하거나 기존 수집기를 편집하는 동안 액세스 거부 기능을 활성화해야 합니다.



## 사용자 권한이 필요합니다

클러스터 관리 자격 증명을 사용하여 Data Collector를 추가하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한이 있는 사용자 지정 사용자(예: *CsUser*)를 사용하여 수집기를 추가하는 경우, 아래 단계에 따라 ONTAP에 액세스 거부 이벤트를 등록하는 데 필요한 권한을 워크로드 보안에 부여합니다.

cluster\_credentials를 사용하는 CsUser의 경우 ONTAP 명령줄에서 다음 명령을 실행합니다. \_csrestrole\_은(는) 사용자 지정 역할이고 \_csUser\_는 ONTAP 사용자 지정 사용자입니다.

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <cluster_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole
```

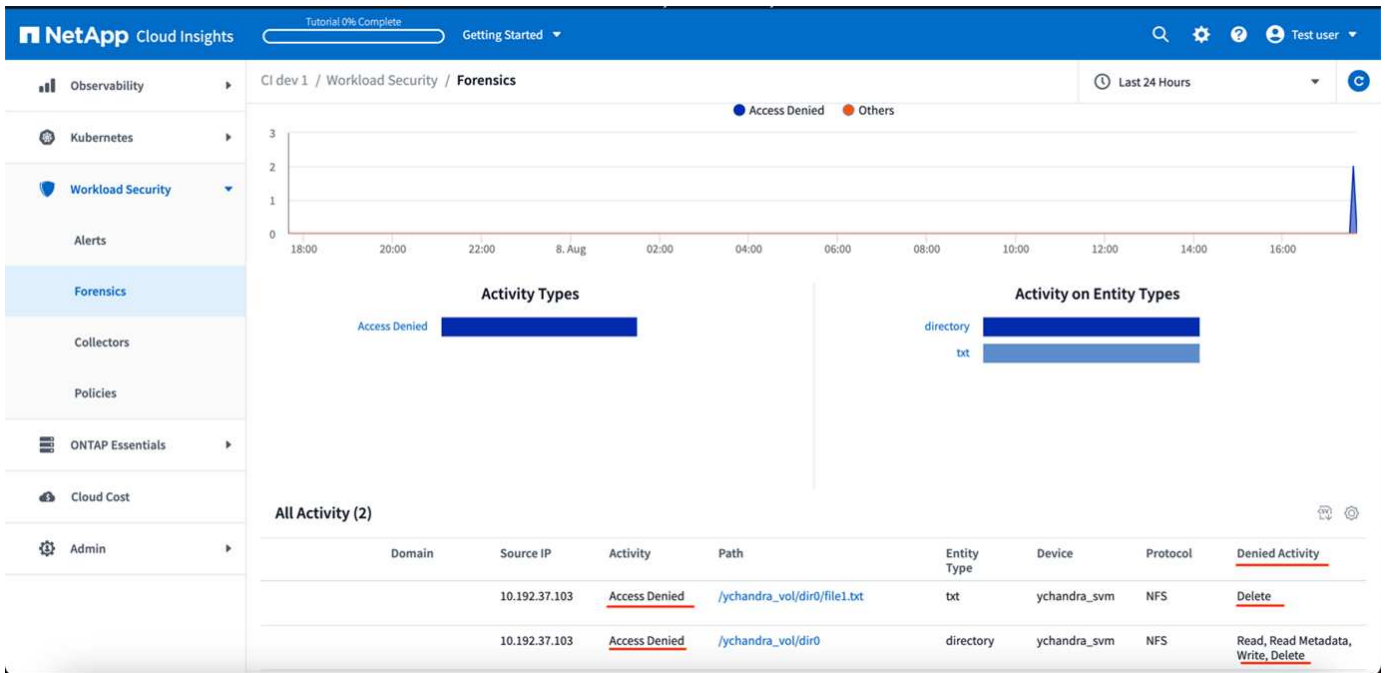
csUser with \_SVM\_credentials의 경우 ONTAP 명령줄에서 다음 명령을 실행합니다.

```
security login rest-role create -role csrestrole -api
/api/protocols/fpolicy -access all -vserver <svm_name>
security login create -user-or-group-name csuser -application http
-authmethod password -role csrestrole -vserver <svm_name>
```

기타 구성에 대한 자세한 정보 "[ONTAP 권한](#)".

## 액세스가 거부되었습니다

ONTAP 시스템에서 이벤트를 가져오면 워크로드 보안 포렌식 페이지에 액세스 거부 이벤트가 표시됩니다. 표시되는 정보 외에도 기어 아이콘에서 테이블에 *WARGED Activity* 열을 추가하여 특정 작업에 대해 누락된 사용자 권한을 볼 수 있습니다.



## 사용자 액세스 차단

공격이 감지되면 워크로드 보안에서 파일 시스템에 대한 사용자 액세스를 차단하여 공격을 차단할 수 있습니다. 자동 응답 정책을 사용하거나 알림 또는 사용자 세부 정보 페이지에서 수동으로 액세스를 차단할 수 있습니다.

사용자 액세스를 차단할 때는 차단 기간을 정의해야 합니다. 선택한 기간이 끝나면 사용자 액세스가 자동으로 복원됩니다. 액세스 차단은 SMB 및 NFS 프로토콜 모두에서 지원됩니다.

사용자가 SMB 및 호스트 시스템의 IP 주소에 대해 직접 차단되어 NFS에 대한 공격이 차단됩니다. 이러한 시스템 IP 주소는 워크로드 보안에서 모니터링하는 SVM(Storage Virtual Machine)에 액세스하지 못하도록 차단됩니다.

예를 들어, 워크로드 보안이 10개의 SVM을 관리하고 자동 응답 정책이 4개의 SVM에 대해 구성되었다고 가정해 보겠습니다. 4개의 SVM 중 하나에서 공격이 발생한 경우 10개의 SVM에서 사용자의 액세스가 차단됩니다. 원래 SVM에 대해 스냅샷이 여전히 촬영됩니다.

SMB용으로 구성된 SVM 4개, NFS용으로 구성된 SVM 1개와 NFS 및 SMB용으로 구성된 나머지 2개가 있는 경우 4개의 SVM 중 하나에서 공격이 발생한 경우 모든 SVM이 차단됩니다.

### 사용자 액세스 차단을 위한 필수 조건

이 기능을 사용하려면 클러스터 레벨 자격 증명이 필요합니다.

클러스터 관리 자격 증명을 사용하는 경우 새 권한이 필요하지 않습니다.

사용자에게 부여된 권한으로 사용자 지정 사용자(예: *CsUser*)를 사용하는 경우 아래 단계에 따라 사용자를 차단하는 워크로드 보안에 권한을 부여합니다.

클러스터 자격 증명이 있는 *CsUser*의 경우 ONTAP 명령줄에서 다음을 수행하십시오.

```
security login role create -role csrole -cmddirname "vserver export-policy
rule" -access all
security login role create -role csrole -cmddirname set -access all
security login role create -role csrole -cmddirname "vserver cifs session"
-access all
security login role create -role csrole -cmddirname "vserver services
access-check authentication translate" -access all
security login role create -role csrole -cmddirname "vserver name-mapping"
-access all
```

의 사용 권한 섹션을 검토하십시오 ["ONTAP SVM Data Collector 구성"](#) 페이지를 참조하십시오.

## 이 기능을 활성화하는 방법은 무엇입니까?

- 워크로드 보안에서 \* 워크로드 보안 > 정책 > 자동화된 대응 정책 \* 으로 이동합니다. 공격 정책 \* 을 선택합니다.
- 사용자 파일 액세스 차단 \_ 을(를) 선택합니다.

## 자동 사용자 액세스 차단을 설정하는 방법은 무엇입니까?

- 새 공격 정책을 만들거나 기존 공격 정책을 편집합니다.
- 공격 정책을 모니터링해야 하는 SVM을 선택합니다.
- “Block User File Access(사용자 파일 액세스 차단)” 확인란을 클릭합니다. 이 옵션을 선택하면 기능이 활성화됩니다.
- “Time Period(기간)”에서 차단 적용 기간을 선택합니다.
- 자동 사용자 차단을 테스트하려면 을 통해 공격을 시뮬레이션할 수 있습니다 ["시뮬레이션된 스크립트"](#).

## 시스템에 차단된 사용자가 있는지 어떻게 알 수 있습니까?

- 경고 목록 페이지에서 사용자가 차단된 경우 화면 상단에 배너가 표시됩니다.
- 배너를 클릭하면 “Users(사용자)” 페이지로 이동합니다. 여기에서 차단된 사용자 목록을 볼 수 있습니다.
- “Users(사용자)” 페이지에는 “User/IP Access(사용자/IP 액세스)”라는 열이 있습니다. 이 열에서 현재 사용자 차단 상태가 표시됩니다.

## 사용자 액세스를 수동으로 제한 및 관리합니다

- 경고 세부 정보 또는 사용자 세부 정보 화면으로 이동한 다음 해당 화면에서 사용자를 수동으로 차단 또는 복원할 수 있습니다.

## 사용자 액세스 제한 기록

경고 세부 정보 및 사용자 세부 정보 페이지의 사용자 패널에서 사용자의 액세스 제한 기록에 대한 감사(시간, 작업(차단, 차단 해제), 기간, 수행한 작업, NFS에 대한 수동/자동 및 영향을 받는 IP

### 이 기능을 비활성화하는 방법은 무엇입니까?

언제든지 이 기능을 비활성화할 수 있습니다. 시스템에 제한된 사용자가 있는 경우 먼저 액세스 권한을 복원해야 합니다.

- 워크로드 보안에서 \* 워크로드 보안 > 정책 > 자동화된 대응 정책 \* 으로 이동합니다. 공격 정책 \* 을 선택합니다.
- 선택 취소(선택 취소) \_ 사용자 파일 액세스 차단 \_.

이 기능은 모든 페이지에서 숨겨집니다.

### NFS에 대한 IP를 수동으로 복구합니다

워크로드 보안 평가판이 만료되었거나 에이전트/수집기가 중단된 경우 다음 단계를 사용하여 ONTAP에서 IP를 수동으로 복원합니다.

1. SVM에 모든 익스포트 정책을 나열하십시오.

```
contrail-qa-fas8020::> export-policy rule show -vserver <svm name>
```

Vserver	Policy Name	Rule Index	Access Protocol	Client Match	RO Rule
svm0	default	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm1	default	4	cifs, nfs	0.0.0.0/0	any
svm2	test	1	nfs3, nfs4, cifs	cloudsecure_rule, 10.11.12.13	never
svm3	test	3	cifs, nfs, flexcache	0.0.0.0/0	any

4 entries were displayed.

2. 각 RuleIndex를 지정하여 "cloudsecure\_rule"이 Client match인 SVM의 모든 정책 전반에 걸쳐 규칙을 삭제합니다. 워크로드 보안 규칙은 일반적으로 1입니다.

```
contrail-qa-fas8020::*> export-policy rule delete -vserver <svm name>  
-policyname * -ruleindex 1
```

- 워크로드 보안 규칙이 삭제되었는지 확인합니다 (선택적 단계 확인) .

```

contrail-qa-fas8020::*> export-policy rule show -vserver <svm name>
      Policy          Rule   Access  Client      RO
Vserver  Name             Index  Protocol Match      Rule
-----  -
svm0     default          4      cifs,      0.0.0.0/0    any
          nfs
svm2     test             3      cifs,      0.0.0.0/0    any
          nfs,
          flexcache
2 entries were displayed.

```

## SMB용 사용자를 수동으로 복원합니다

워크로드 보안 평가판이 만료되었거나 에이전트/수집기가 중단된 경우 다음 단계를 사용하여 ONTAP에서 사용자를 수동으로 복원합니다.

사용자 목록 페이지에서 워크로드 보안에서 차단된 사용자 목록을 가져올 수 있습니다.

1. cluster\_admin\_credentials를 사용하여 ONTAP 클러스터(사용자 차단을 해제할 위치)에 로그인합니다. (Amazon FSx의 경우 FSx 자격 증명으로 로그인합니다.)
2. 다음 명령을 실행하여 모든 SVM에서 SMB용 워크로드 보안으로 차단된 모든 사용자를 나열합니다.

```
vserver name-mapping show -direction win-unix -replacement " "
```

```

Vserver:   <vservename>
Direction: win-unix
Position  Hostname          IP Address/Mask
-----  -
1         -                    -                Pattern: CSLAB\\US040
          Replacement:
2         -                    -                Pattern: CSLAB\\US030
          Replacement:
2 entries were displayed.

```

위 출력에서 두 명의 사용자가 CSLAB 도메인과 함께 차단되었습니다(US030, US040).

1. 위 출력에서 위치를 확인한 후 다음 명령을 실행하여 사용자 차단을 해제합니다.

```
vserver name-mapping delete -direction win-unix -position <position>
```

. 다음 명령을 실행하여 사용자의 차단 해제 여부를 확인합니다.

```
vserver name-mapping show -direction win-unix -replacement " "
```

이전에 차단한 사용자에게 대해서는 어떤 항목도 표시되지 않아야 합니다.

## 문제 해결

문제	시도해 보십시오
일부 사용자는 공격이 있어도 제한을 받지 않습니다.	SVM용 Data Collector 및 Agent가 <code>_Running_</code> 상태인지 확인합니다. Data Collector와 Agent가 중지된 경우 워크로드 보안에서 명령을 전송할 수 없습니다. 이는 사용자가 이전에 사용되지 않은 새 IP가 있는 시스템에서 스토리지에 액세스했을 수 있기 때문입니다. 제한은 사용자가 스토리지에 액세스하는 데 사용하는 호스트의 IP 주소를 통해 수행됩니다. 제한된 IP 주소 목록을 보려면 UI(알림 세부 정보 > 이 사용자의 액세스 제한 기록 > 영향을 받는 IP)를 확인하십시오. 사용자가 제한된 IP와 다른 IP를 가진 호스트에서 스토리지에 액세스하는 경우 사용자는 여전히 제한되지 않은 IP를 통해 스토리지를 액세스할 수 있습니다. 사용자가 IP가 제한된 호스트에서 액세스를 시도하는 경우 스토리지를 액세스할 수 없습니다.
액세스 제한을 수동으로 클릭하면 "이 사용자의 IP 주소가 이미 제한되었습니다"라는 메시지가 나타납니다.	제한할 IP가 이미 다른 사용자로부터 제한되어 있습니다.
정책을 수정할 수 없습니다. 원인: 해당 명령에 대해 권한이 없습니다.	CsUser 사용 시, 위에서 설명한 대로 사용자에게 권한이 부여되는지 확인
NFS에 대한 사용자(IP 주소) 차단은 작동하지만 SMB/CIFS에 대해서는 "SID를 DomainName으로 변환하지 못했습니다. 이유 시간 초과: 소켓이 설정되지 않았습니다."	ssh를 수행할 권한이 <code>_CsUser_</code> 에 없는 경우 이 문제가 발생할 수 있습니다. (클러스터 레벨에서 접속한 다음 사용자가 ssh를 수행할 수 있는지 확인합니다.) <code>_CsUser_role</code> 에는 이러한 권한이 필요합니다. <a href="https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking">https://docs.netapp.com/us-en/cloudinsights/cs_restrict_user_access.html#prerequisites-for-user-access-blocking</a> 클러스터 자격 증명을 사용하여 <code>_CsUser_</code> 의 경우 ONTAP 명령줄에서 다음을 수행합니다. 보안 로그인 역할 create-role csrole-cmddirname "vserver export-policy rule" -access all security login role create -role csrole -cmddirname set -access all security login role create-role -cmdname "vserver cifs session" -access all security login role create-role -cmddirname "vserver services access-check authentication translate" -access all security login에 액세스하십시오 role create-role csrole-cmddirname "vserver name-mapping" -access all if <code>_CsUser_</code> 가 사용되지 않고 클러스터 레벨의 admin 사용자가 사용되는 경우 admin 사용자가 ONTAP에 대한 ssh 권한을 가지고 있는지 확인합니다.

문제	시도해 보십시오
Error Message_SID translate failed. __reason: 255: Error: command failed: 해당 명령에 대해 승인되지 않았습니니다. Error: "access-check"는 인식할 수 없는 command _입니다. 사용자가 차단되어야 합니다.	이 문제는 _CsUser_에 올바른 권한이 없을 때 발생할 수 있습니다. 자세한 내용은 <a href="#">"사용자 액세스 차단을 위한 필수 조건"</a> 참조하십시오. 권한을 적용한 후에는 ONTAP 데이터 수집기 및 사용자 디렉터리 데이터 수집기를 다시 시작하는 것이 좋습니다. 필요한 권한 명령은 다음과 같습니다. --- 보안 로그인 역할 create-role csrole-cmddirname "vserver export-policy rule" - 모든 보안 로그인 역할 create-role csrole-cmddirname "vserver cifs session" - access 모든 보안 로그인 역할 create-role 로그인 역할 -dirname role create -role csrole -cmddirname "vserver name -mapping" -access all-----

## 워크로드 보안: 공격 시뮬레이션

이 페이지의 지침을 사용하여 포함된 랜섬웨어 시뮬레이션 스크립트를 사용하여 워크로드 보안을 테스트 또는 시연하기 위한 공격을 시뮬레이션할 수 있습니다.

### 시작하기 전에 주의해야 할 사항

- 랜섬웨어 시뮬레이션 스크립트는 Linux에서만 작동합니다.
- 이 스크립트는 워크로드 보안 에이전트 설치 파일과 함께 제공됩니다. 워크로드 보안 에이전트가 설치된 모든 시스템에서 사용할 수 있습니다.
- 워크로드 보안 에이전트 시스템 자체에서 스크립트를 실행할 수 있으며 다른 Linux 시스템을 준비할 필요가 없습니다. 그러나 스크립트를 다른 시스템에서 실행하려면 스크립트를 복사하여 거기에서 실행하기만 하면 됩니다.

### 샘플 파일이 1,000개 이상 있어야 합니다

이 스크립트는 암호화할 파일이 있는 폴더가 있는 SVM에서 실행되어야 합니다. 해당 폴더 및 하위 폴더 내에 1,000개 이상의 파일이 있는 것이 좋습니다. 파일이 비어 있으면 안 됩니다. 같은 사용자를 사용하여 파일을 만들고 암호화하지 마십시오. 워크로드 보안은 이 작업을 저위험 작업으로 간주하므로 경고를 생성하지 않습니다(즉, 동일한 사용자가 방금 생성한 파일을 수정함).

에 대한 지침은 아래를 참조하십시오 ["비어 있지 않은 파일을 프로그래밍 방식으로 만듭니다"](#).

### 시뮬레이터를 실행하기 전에 필요한 지침:

1. 암호화된 파일이 비어 있지 않은지 확인합니다.
2. 50개 이상의 파일을 암호화해야 합니다. 적은 수의 파일이 무시됩니다.
3. 동일한 사용자로 여러 번 공격을 실행하지 마십시오. 몇 번 지나면 워크로드 보안에서는 이 사용자 동작을 학습하고 이것이 사용자의 정상적인 동작이라고 가정합니다.
4. 동일한 사용자가 방금 만든 파일은 암호화하지 마십시오. 사용자가 방금 만든 파일을 변경하는 것은 위험한 작업으로 간주되지 않습니다. 대신 다른 사용자가 만든 파일을 사용하거나 파일을 만들고 암호화하는 데 몇 시간이 걸릴 수 있습니다.

## 시스템을 준비합니다

먼저 타겟 볼륨을 시스템에 마운트합니다. NFS 마운트 또는 CIFS 내보내기를 마운트할 수 있습니다.

Linux에서 NFS 내보내기를 마운트하려면

```
mount -t nfs -o vers=4.0 10.193.177.158:/svmvoll /mntpt
mount -t nfs -o vers=4.0 Vserver data IP>:/nfsvol /destinationlinuxfolder
```

NFS 버전 4.1을 마운트하지 마십시오. Fpolicy에서 지원되지 않습니다.

Linux에서 CIFS를 마운트하려면

```
mount -t cifs //10.193.77.91/sharedfolderincluster
/root/destinationfolder/ -o username=raisa
다음으로 Data Collector를 설정합니다.
```

1. 아직 수행하지 않은 경우 워크로드 보안 에이전트를 구성합니다.
2. 아직 수행하지 않은 경우 SVM 데이터 수집기를 구성합니다.

## 랜섬웨어 시뮬레이터 스크립트를 실행합니다

1. 워크로드 보안 에이전트 시스템에 로그인(ssh)합니다.
2. `./opt/NetApp/cloudsecure/agent/install_`로 이동합니다
3. 매개 변수 없이 시뮬레이터 스크립트를 호출하여 사용 현황을 확인합니다.

```
# pwd
/opt/netapp/cloudsecure/agent/install
# ./ransomware_simulator.sh
Error: Invalid directory provided.
Usage: ./ransomware_simulator.sh [-e] [-d] [-i <input_directory>]
      -e to encrypt files (default)
      -d to restore files
      -i <input_directory> - Files under the directory to be encrypted
```

```
Encrypt command example: ./ransomware_simulator.sh -e -i
/mnt/audit/reports/
Decrypt command example: ./ransomware_simulator.sh -d -i
/mnt/audit/reports/
```



## 테스트 파일을 암호화합니다

파일을 암호화하려면 다음 명령을 실행합니다.

```
# ./ransomware_simulator.sh -e -i /root/for/  
Encryption key is saved in /opt/netapp/cloudsecure/cloudsecure-agent-  
1.251.0/install/encryption-key,  
which can be used for restoring the files.  
Encrypted /root/for/File000.txt  
Encrypted /root/for/File001.txt  
Encrypted /root/for/File002.txt  
...
```

## 파일을 복원합니다

암호를 해독하려면 다음 명령을 실행합니다.

```
[root@scspa2527575001 install]# ./ransomware_simulator.sh -d -i /root/for/  
File /root/for/File000.txt is restored.  
File /root/for/File001.txt is restored.  
File /root/for/File002.txt is restored.  
...
```

## 스크립트를 여러 번 실행합니다

사용자에 대한 랜섬웨어 공격을 생성한 후 다른 사용자로 전환하여 추가 공격을 생성하십시오. 워크로드 보안은 사용자 행동을 학습하고 동일한 사용자에게 대해 짧은 기간 내에 반복되는 랜섬웨어 공격에 대해 경고하지 않습니다.

## 프로그래밍 방식으로 파일을 만듭니다

파일을 만들기 전에 먼저 데이터 수집기 처리를 중지하거나 일시 중지해야 합니다.

데이터 수집기를 Agent에 추가하기 전에 다음 단계를 수행하십시오. 이미 데이터 수집기를 추가한 경우 데이터 수집기를 편집하고 잘못된 암호를 입력한 다음 저장합니다. 이렇게 하면 데이터 수집기가 일시적으로 오류 상태가 됩니다. 참고: 원래 암호를 기록해 두십시오!



권장 옵션은 입니다 ["수집기를 일시 중지합니다"](#) 파일을 작성하기 전에.]

시뮬레이션을 실행하기 전에 먼저 암호화할 파일을 추가해야 합니다. 암호화할 파일을 대상 폴더에 수동으로 복사하거나 스크립트(아래 예 참조)를 사용하여 프로그래밍 방식으로 파일을 만들 수 있습니다. 어떤 방법을 사용하든 1,000개 이상의 파일을 복사합니다.

프로그래밍 방식으로 파일을 만들도록 선택한 경우 다음을 수행합니다.

1. 에이전트 상자에 로그인합니다.
2. 파일러의 SVM에서 Agent 시스템으로 NFS 내보내기를 마운트합니다. CD를 해당 폴더에 넣습니다.

3. 이 폴더에서 createfiles.sh 라는 파일을 만듭니다

4. 다음 줄을 해당 파일에 복사합니다.

```
for i in {000..1000}
do
    echo hello > "File${i}.txt"
done
echo 3 > /proc/sys/vm/drop_caches ; sync
```

5. 파일을 저장합니다.

6. 파일에 대한 실행 권한 확인:

```
chmod 777 ./createfiles.sh
. 스크립트를 실행합니다.
```

```
./createfiles.sh
```

현재 폴더에 1000개의 파일이 생성됩니다.

7. 데이터 수집기를 다시 활성화합니다

1단계에서 데이터 수집기를 비활성화한 경우 데이터 수집기를 편집하고 올바른 암호를 입력한 후 저장합니다. 데이터 수집기가 다시 실행 중 상태인지 확인합니다.

8. 다음 단계를 수행하기 전에 수집기를 일시 중지한 경우 을 참조하십시오 "[수집기를 다시 시작합니다](#)".

## 경고, 경고 및 에이전트/데이터 소스 수집기 상태에 대한 이메일 알림 구성

워크로드 보안 경고 수신자를 구성하려면 \* Admin > Notifications \* 를 클릭하고 각 수신자의 적절한 섹션에 이메일 주소를 입력합니다.

### 잠재적 공격 경고 및 경고

potential attack\_alert 알림을 보내려면 \_ Send potential attack Alerts \_ 섹션에 받는 사람의 전자 메일 주소를 입력합니다. e-메일 알림은 알림의 모든 작업에 대해 알림 받는 사람 목록으로 전송됩니다.

Warning\_notifications를 보내려면 \_ Send Warning Alerts 섹션에 받는 사람의 이메일 주소를 입력합니다.

### 에이전트 및 Data Collector 상태 모니터링

알림을 통해 에이전트 및 데이터 소스의 상태를 모니터링할 수 있습니다.

에이전트 또는 데이터 소스 수집기가 작동하지 않는 경우 알림을 받으려면 \_ 데이터 수집 상태 경고 \_ 섹션에 받는

사람의 전자 메일 주소를 입력합니다.

다음 사항에 유의하십시오.

- 상태 알림은 에이전트/수집기가 최소 1시간 동안 보고를 중지한 후에만 전송됩니다.
- 특정 24시간 동안 에이전트 또는 데이터 수집기의 연결이 끊어진 경우에도 지정된 수신자에게 하나의 이메일 알림만 전송됩니다.
- Agent가 고장 날 경우 한 번에 하나의 경고가 전송됩니다(수집기당 1개가 아님). 이메일에는 영향을 받는 모든 SVM의 목록이 포함됩니다.
- Active Directory 수집 장애는 경고로 보고되며 랜섬웨어 감지에 영향을 주지 않습니다.
- 이제 시작 설정 목록에 새 `_Configure email notifications_` 단계가 포함됩니다.

## Agent 및 Data Collector 업그레이드 알림 수신

- "데이터 수집 상태 알림"에 이메일 ID를 입력합니다.
- "업그레이드 알림 사용" 확인란이 활성화됩니다.
- 에이전트 및 Data Collector 업그레이드 e-메일 알림은 예정된 업그레이드 하루 전에 e-메일 ID로 전송됩니다.

## 문제 해결

* 문제: *	* 사용해 보세요. *
"Data Collector 상태 알림"에 이메일 ID가 있지만 알림을 받지 않습니다.	알림 이메일은 NetApp Data Infrastructure Insights 도메인, 즉 <code>_accounts@service.clou</code> <code>dinsights.NetApp.com_</code> 에서 발송되었습니다. 일부 회사는 외부 도메인에서 보낸 전자 메일을 차단합니다. NetApp Data Infrastructure Insights 도메인의 외부 알림을 화이트리스트로 등록했는지 확인합니다.

## 워크로드 보안 API

워크로드 보안 API를 통해 NetApp 고객과 ISV(독립 소프트웨어 공급업체)는 워크로드 보안을 CMDB 또는 기타 티켓 시스템과 같은 다른 애플리케이션과 통합할 수 있습니다.

API 액세스 요구 사항:

- 액세스 권한을 부여하기 위해 API 액세스 토큰 모델이 사용됩니다.
- API 토큰 관리는 관리자 역할을 가진 워크로드 보안 사용자에게 의해 수행됩니다.

## API 설명서(Swagger)

최신 API 정보는 Workload Security에 로그인하고 `* Admin > API Access *`로 이동하여 확인할 수 있습니다. API Documentation \* 링크를 클릭합니다. API 설명서는 Swagger 기반의 제품으로, API에 대한 간략한 설명과 사용 정보를 제공하고 사용자 환경에서 사용할 수 있습니다.



Forensics Activity API를 호출하는 경우 `cloudsecure_forensics.activities`. \* v2 \* API를 사용합니다. 이 API를 여러 번 호출하는 경우 호출이 병렬로 발생하지 않고 순차적으로 발생했는지 확인합니다. 여러 병렬 호출로 인해 API 시간이 초과될 수 있습니다.

## API 액세스 토큰

워크로드 보안 API를 사용하기 전에 하나 이상의 \* API 액세스 토큰 \* 을 생성해야 합니다. 액세스 토큰은 읽기 권한을 부여합니다. 각 액세스 토큰의 만료일을 설정할 수도 있습니다.

액세스 토큰을 만들려면 다음을 수행합니다.

- Admin > API Access \* 를 클릭합니다
- API 액세스 토큰 \* 을 클릭합니다
- 토큰 이름 \* 을 입력합니다
- 토큰 만료 \* 를 지정합니다



토큰은 클립보드로 복사하고 생성 과정 중에 저장하는 경우에만 사용할 수 있습니다. 토큰을 만든 후에는 검색할 수 없으므로 토큰을 복사하여 안전한 위치에 저장하는 것이 좋습니다. 토큰 생성 화면을 닫기 전에 API 액세스 토큰 복사 버튼을 클릭하라는 메시지가 표시됩니다.

토큰을 비활성화, 활성화 및 취소할 수 있습니다. 비활성화된 토큰을 활성화할 수 있습니다.

토큰은 고객의 관점에서 API에 대한 범용 액세스를 부여하여 자체 환경의 범위 내에서 API에 대한 액세스를 관리합니다.

응용 프로그램은 사용자가 액세스를 성공적으로 인증 및 승인한 후 액세스 토큰을 받은 다음 대상 API를 호출할 때 액세스 토큰을 자격 증명으로 전달합니다. 전달된 토큰은 API에 토큰의 베어러가 API에 액세스할 수 있는 권한이 있음을 알리고 권한 부여 중에 부여된 범위에 따라 특정 작업을 수행하도록 합니다.

액세스 토큰이 전달되는 HTTP 헤더는 \* X-CloudInsights-ApiKey: \* 입니다

예를 들어, 다음을 사용하여 스토리지 자산을 검색할 수 있습니다.

```
curl https://<tenant_host_name>/rest/v1/cloudsecure/activities -H 'X-CloudInsights-ApiKey: <API_Access_Token>'
```

여기서 `<API_Access_Token>`은 API 액세스 키를 생성하는 동안 저장한 토큰입니다.

자세한 정보는 \* Admin > API Access \* 의 `_API Documentation_link`에서 확인할 수 있습니다.

## API를 통해 데이터를 추출하는 스크립트

워크로드 보안 에이전트에는 요청된 시간 범위를 더 작은 배치로 나누어 v2 API에 대한 병렬 호출을 용이하게 하기 위한 내보내기 스크립트가 포함되어 있습니다.

스크립트는 `_opt/NetApp/cloudsecure/agent/export-script _`에 있습니다. 동일한 디렉토리에 있는 README 파일은 사용 지침을 제공합니다.

다음은 스크립트를 호출하는 명령 예입니다.

```
python3 data-export.py --tenant_url <tenant
id>.cs01.cloudinsights.netapp.com --access_key %ACCESS_KEY% --path_filter
"<dir path>" --user_name "<user>" --from_time "01-08-2024 00:00:00"
--to_time "31-08-2024 23:59:59" --iteration_interval 12 --num_workers 3
```

주요 파라미터: --iteration\_interval 12: 요청한 시간 범위를 12시간 간격으로 분할합니다.  
--num\_workers 3: 3개의 스레드를 사용하여 이러한 간격을 병렬로 가져옵니다.

# 문제 해결

## 일반적인 Data Infrastructure Insights 문제 해결

여기에서 Data Infrastructure Insights의 문제 해결을 위한 제안을 찾을 수 있습니다.

도 참조하십시오 "[Linux 획득 장치 문제 해결](#)" 및 "[Windows 획득 장치 문제 해결](#)".

### 로그인 문제

* 문제: *	* 사용해 보세요. *
Data Infrastructure Insights는 6시간마다 자동으로 로그아웃됩니다	이는 비활성화된 브라우저 타사 쿠키가 원인입니다. 사용자는 모든 타사 쿠키를 사용하도록 브라우저를 구성하거나 더 좁은 예외 목록을 사용하여 Data Infrastructure Insights를 사용하도록 설정할 수 있습니다. 예: 브라우저의 설정을 엽니다. "모든 쿠키 허용" 옵션을 선택합니다. * 또는 * "타사 쿠키 차단"을 선택하고 <code>_[\*].auth0.com_</code> 및 <code>[_*].NetApp.com_</code> 에 대한 예외를 추가합니다. Microsoft Edge는 Chrome과 동일한 형식의 예외 항목을 접습니다. Firefox에서 쿠키 예외는 간단히 <code>_auth0.com_</code> 및 <code>_netapp.com_</code> 로 지정됩니다.
BlueXP 계정이 있지만 BlueXP에 로그인할 수 없습니다.	에서 티켓을 엽니다 <a href="https://mysupport.netapp.com/site/help">https://mysupport.netapp.com/site/help</a> . <a href="https://mysupport.netapp.com/site/help">blueXP.netapp.com</a> > 계정/로그인 문제 또는 <a href="https://mysupport.netapp.com/site/help">bluexp.netapp.com</a> > 페더레이션 문제 범주를 선택합니다. 이는 특히 BlueXP 문제 또는 질문을 대상으로 한 것입니다. 기타 모든 Data Infrastructure Insights 기술 지원 문제는 에 문의하십시오 " <a href="#">NetApp 지원</a> ".
Data Infrastructure Insights에 초대를 받았지만 "인증되지 않음"이라는 메시지가 표시됩니다.	BlueXP 계정에 등록했는지 또는 조직에서 BlueXP를 통해 SSO 로그인을 사용하는지 확인하십시오. BlueXP 프로필 이메일 주소가 Data Infrastructure Insights 시작 이메일에 표시된 이메일 주소와 일치하는지 확인하십시오. 이메일이 일치하지 않으면 올바른 이메일 주소로 새 초대를 요청하십시오.
BlueXP 에서 로그아웃했고 Data Infrastructure Insights에서 자동으로 로그아웃되었습니다.	NetApp 클라우드 서비스 전체에서 SSO(Single Sign-On)가 모든 Data Infrastructure Insights 세션에서 로그아웃됩니다. 여러 Data Infrastructure Insights 계정에 액세스할 수 있는 경우 한 계정에서 로그아웃하면 모든 활성 세션이 로그아웃됩니다. 계정에 액세스하려면 다시 로그인하십시오.
며칠 후에 자동으로 로그아웃되었습니다.	NetApp 클라우드 계정은 며칠 간격으로 다시 인증해야 합니다(현재 BlueXP 설정은 7일). 계정에 액세스하려면 다시 로그인하십시오.
"더 이상 로그인할 수 없습니다"라는 오류 메시지가 나타납니다.	Data Infrastructure Insights에 대한 액세스 권한을 확인하려면 계정 관리자에게 문의하십시오. BlueXP 프로필 이메일 주소가 Data Infrastructure Insights 시작 이메일에 표시된 이메일 주소와 일치하는지 확인하십시오

* 문제: *	* 사용해 보세요. *
기타 로그인 오류	Chrome에서 시크릿 모드를 시도하거나 브라우저 기록, 쿠키 및 캐시를 지웁니다. 다른 브라우저 프로필(예 Chrome - 사람 추가).

## 기타 문제

* 질문: *	* 답변: *
Qtree 하드 할당량이 쿼리에 올바르게 표시되지만 소프트 할당량이 볼륨의 총 용량으로 표시됩니다. 맞습니까?	수동으로 설정하거나 Trident를 통해 설정하는 하드 할당량만 설정된 할당량으로 표시됩니다. 하드 할당량을 지정하지 않으면 Qtree 용량이 내부 볼륨 용량이 됩니다.
동일한 Qtree에 수동으로 소프트 할당량과 하드 할당량이 모두 설정되어 있지만 표시되는 총 용량은 하드 할당량입니다. 맞습니까?	예. 하드 할당량이 지정된 경우 총 용량으로 표시됩니다.
Cognos 보고서 일정 시간을 입력할 때 일정 시간에 "m"이 추가로 나타나는 경우가 있습니다. 예를 들어 시간을 "02:15 PM"으로 입력하면 "02:15 PMM"(또는 PMM)이라는 추가 문자를 추가할 수 있습니다. 바깥쪽을 클릭하면 "오전 2:15"로 변경됩니다.	예약 시간을 다시 입력하십시오. 전체 "AM" 또는 "PM" 문자를 입력하지 않도록 주의하십시오. "AM"에는 "A"를, "PM"에는 "P"를 입력하면 됩니다. 추가 문자가 표시되지 않으면 예약 시간이 올바르게 설정됩니다.
보고서를 저장할 수 있지만 저장된 보고서를 다시 열면 일정 시간에 AM 또는 PM을 입력했는지 여부에 관계없이 예약 시간이 오전(예: 오전)으로 표시됩니다.	

## 리소스

추가 문제 해결 팁은 에서 찾을 수 있습니다 ["NetApp 기술 자료"](#) (지원 로그인 필요)

추가 지원 정보는 Data Infrastructure Insights 페이지에서 확인할 수 ["지원"](#) 있습니다.

활성 Data Infrastructure Insights에 가입되어 있는 경우 다음 지원 옵션을 사용할 수 있습니다.

["전화"](#)

["지원 티켓"](#)

자세한 내용은 를 ["Data Infrastructure Insights 지원 문서"](#) 참조하십시오.

## Linux에서 획득 장치 문제 해결

여기에서는 Linux 서버의 획득 장치 관련 문제를 해결하기 위한 제안 사항을 확인할 수 있습니다.

* 문제: *	* 사용해 보세요. *
---------	--------------

<p>획득 장치 * 탭의 * 관측성 &gt; 수집기 * 페이지에 AU 상태가 "인증서 만료됨" 또는 "인증서 해지됨"으로 표시됩니다.</p>	<p>AU 오른쪽의 메뉴를 클릭하고 * 연결 복원 * 을 선택합니다. 지침에 따라 획득 장치를 복원합니다: 1. 획득 장치(AU) 서비스를 중지합니다. Copy Stop Command _ (복사 중지 명령) 버튼을 클릭하여 명령을 클립보드로 빠르게 복사한 다음, 이 명령을 획득 장치 시스템의 명령 프롬프트에 붙여넣을 수 있습니다. AU의 <i>/var/lib/netapp/클라우드 볼거리/acq/conf_folder</i>에 "token"이라는 파일을 생성합니다. 3.Copy Token 단추를 클릭하고 이 토큰을 만든 파일에 붙여 넣습니다. AU 서비스를 다시 시작합니다. Copy Restart Command _ 버튼을 클릭하고 AU의 명령 프롬프트에 명령을 붙여 넣습니다.</p>
<p>획득 장치 서버 서비스를 시작할 때 권한이 거부되었습니다</p>	<p>AU가 SELinux에 설치된 경우 SE를 <code>_permissive_mode</code>로 설정해야 합니다. <code>_Enforcing_mode</code>는 지원되지 않습니다. SELinux를 허용 모드로 설정한 후 AU 서비스를 다시 시작합니다. "<a href="#">자세한 정보</a>".</p>
<p>서버 요구 사항이 충족되지 않았습니다</p>	<p>획득 장치 서버 또는 VM이 을 충족하는지 확인합니다 "<a href="#">요구 사항</a>"</p>
<p>네트워크 요구 사항이 충족되지 않았습니다</p>	<p>획득 장치 서버/VM이 포트 443을 통한 SSL 연결을 통해 데이터 인프라 인사이트 환경(&lt;environment-name&gt;.c01.cloudinsights.NetApp.com)에 액세스할 수 있는지 확인합니다. 다음 명령을 실행합니다. <code>_ping &lt;environment-name&gt; .c01.cloudinsights.NetApp.com</code> <code>traceroute &lt;environment-name&gt; .c01.cloudinsights.NetApp.com</code> <code>curl\https://NetApp.c01.coudinsights.NetApp.com__wget_sights.&lt;environment-name&gt;</code></p>
<p>프록시 서버가 올바르게 구성되지 않았습니다</p>	<p>프록시 설정을 확인하고 필요한 경우 획득 장치 소프트웨어를 제거/재설치하여 올바른 프록시 설정을 입력합니다. 1."curl"을 시도합니다. 프록시에 대한 "man curl" 정보/문서를 참조하십시오. — proxy, — proxy- * (curl은 많은 프록시 설정을 지원하므로 와일드카드 " * "입니다.) 2."wget"을 시도합니다. 프록시 옵션에 대한 문서를 확인합니다.</p>
<p>획득 서비스를 시작하는 동안 자격 증명 오류가 발생하여 Data Infrastructure Insights에서 획득 장치 설치가 실패했습니다(acq.log에 표시됨).</p>	<p>이 문제는 프록시 자격 증명에 특수 문자가 포함되기 때문에 발생할 수 있습니다. AU(<code>sudo 클라우드 -uninstall.sh</code>)를 제거하고 특수 문자를 사용하지 않고 다시 설치합니다.</p>
<p>Linux: 누락된 라이브러리/파일을 찾을 수 없습니다</p>	<p>Linux 획득 장치 서버/VM에 필요한 모든 라이브러리가 있는지 확인합니다. 예를 들어, <code>_unzip_library</code>가 서버에 설치되어 있어야 합니다. <code>unzip_library</code>를 설치하려면 Acquisition Unit 설치 스크립트를 실행하기 전에 <code>_ * sudo yum install unzip * _</code> 명령을 실행하십시오</p>
<p>권한 문제</p>	<p><code>sudo_permissions</code> 를 사용하여 사용자로 로그인했는지 확인합니다</p>



획득이 실행되지 않음:	acq.log 수집: /opt/netapp/클라우드 sudresights/acq/logs(Linux) Acquisition Service를 다시 시작합니다. sudo cloudinsights-service.sh 다시 시작합니다
데이터 수집 문제:	"오류 보고서 전송" 버튼을 클릭하여 Data Collector 랜딩 페이지에서 오류 보고서를 보냅니다
상태: 하트비트 실패	획득 장치(AU)는 리스를 갱신하기 위해 60초마다 Data Infrastructure Insights에 하트비트를 전송합니다. 네트워크 문제나 응답이 없는 Data Infrastructure Insights로 인해 하트비트 호출이 실패하는 경우 AU의 임대 시간이 업데이트되지 않습니다. AU의 임대 시간이 만료되면 Data Infrastructure Insights에 "Heartbeat Failed(하트비트 실패)" 상태가 표시됩니다. 문제 해결 단계: 획득 장치 서버와 CloudInsights 간의 네트워크 연결을 확인합니다. 획득 장치 서비스가 실행 중인지 확인합니다. 서비스가 실행되고 있지 않으면 서비스를 시작합니다. 획득 장치 로그(/var/log/netapp/클라우드 볼거리/acq/acq.log)를 확인하여 오류가 있는지 확인합니다.
"하트비트 오류:" 메시지가 표시됩니다	이 오류는 획득 장치와 Data Infrastructure Insights 환경 간의 통신이 1분 이상 중단되는 네트워크 중단이 발생할 경우 발생할 수 있습니다. AU와 Data Infrastructure Insights 간의 연결이 안정적이고 활성 상태인지 확인합니다.
획득 장치를 다시 설치할 때 "ValueError: /opt/netapp/cloudinsights(/. *)에 대한 파일 컨텍스트"가 표시됩니다. 이미 정의됨".	SELinux가 설치된 시스템에서는 이 오류 메시지가 다음에 나타날 수 있습니다 cloudinsights-uninstall.sh -p 이(가) 실행되고 획득 장치를 다시 설치해야 합니다. 명령을 실행합니다 semanage fcontext -d -t usr t "/opt/netapp/cloudinsights(/.*)?" 문제를 해결하고 메시지를 제거해야 합니다.

## 프록시 및 방화벽에 대한 고려 사항

조직에서 인터넷 액세스에 프록시 사용을 요구하는 경우 조직의 프록시 동작을 이해하고 Data Infrastructure Insights가 작동하려면 특정 예외를 찾아야 할 수 있습니다. 다음 사항에 유의하십시오.

- 첫째, 조직에서 기본적으로 액세스를 차단하며 특정 웹 사이트/도메인에 대한 액세스는 예외로 허용됩니까? 이 경우 예외 목록에 다음 도메인을 추가해야 합니다.

```
*.cloudinsights.netapp.com
```

Data Infrastructure Insights 수집 장치는 물론, Data Infrastructure Insights를 사용한 웹 브라우저에서의 상호 작용은 모두 해당 도메인 이름을 가진 호스트에 전달됩니다.

- 둘째, 일부 프록시는 NetApp에서 생성되지 않은 디지털 인증서를 사용하여 Data Infrastructure Insights 웹 사이트를 가장하여 TLS/SSL 검사를 수행하려고 합니다. Data Infrastructure Insights Acquisition Unit의 보안 모델은 기본적으로 이러한 기술과 호환되지 않습니다. Data Infrastructure Insights 획득 장치가 Data Infrastructure Insights에 성공적으로 로그인하여 데이터 검색을 용이하게 하려면 이 기능을 제외한 위의 도메인 이름도 필요합니다.

프록시가 트래픽 검사를 위해 설정된 경우 Data Infrastructure Insights 환경을 프록시 구성의 예외 목록에 추가해야 합니다. 이 예외 목록의 형식 및 설정은 프록시 환경 및 도구에 따라 다르지만 일반적으로 AU가 이러한 서버와 제대로 통신할 수 있도록 하려면 Data Infrastructure Insights 서버의 URL을 이 예외 목록에 추가해야 합니다.

가장 간단한 방법은 Data Infrastructure Insights 도메인 자체를 예외 목록에 추가하는 것입니다.

`*.cloudinsights.netapp.com`

프록시가 트래픽 검사를 위해 설정되지 않은 경우 예외 목록이 필요하지 않을 수 있습니다. Data Infrastructure Insights를 예외 목록에 추가해야 하는지 또는 프록시 및/또는 방화벽 구성으로 인해 Data Infrastructure Insights를 설치하거나 실행하는 데 문제가 있는 경우 프록시 관리 팀에 문의하여 프록시의 SSL 차단 처리를 설정합니다.

### 프록시 엔드포인트 보기

온보딩 중에 데이터 수집기를 선택할 때 \* 프록시 설정 \* 링크를 클릭하거나 \* 도움말 > 지원 \* 페이지의 프록시 설정 아래에 있는 링크를 클릭하여 프록시 끝점을 볼 수 있습니다. 다음과 같은 테이블이 표시됩니다. 작업 환경에 워크로드 보안이 있는 경우 구성된 엔드포인트 URL도 이 목록에 표시됩니다.

**Proxy Settings** ✕

i If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjks0.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

Close

### 리소스

추가 문제 해결 팁은 에서 찾을 수 있습니다 ["NetApp 기술 자료"](#) (지원 로그인 필요)

추가 지원 정보는 Data Infrastructure Insights 페이지에서 확인할 수 ["지원"](#) 있습니다.

## Windows의 획득 장치 문제 해결

여기에서는 Windows 서버의 획득 장치 관련 문제를 해결하기 위한 제안 사항을 확인할 수 있습니다.

* 문제: *	* 사용해 보세요. *
---------	--------------

<p>획득 장치 * 탭의 * 관측성 &gt; 수집기 * 페이지에 AU 상태가 "인증서 만료됨" 또는 "인증서 해지됨"으로 표시됩니다.</p>	<p>AU 오른쪽의 메뉴를 클릭하고 * 연결 복원 * 을 선택합니다. 지침에 따라 획득 장치를 복원합니다: 1. 획득 장치(AU) 서비스를 중지합니다. Copy Stop Command _ (복사 중지 명령) 버튼을 클릭하여 명령을 클립보드로 빠르게 복사한 다음, 이 명령을 획득 장치 시스템의 명령 프롬프트에 붙여넣을 수 있습니다. AU의 <i>c:\Program Files\Cloud Insights\Acquisition Unit\conf</i> 폴더에 "token"이라는 이름의 파일을 생성합니다. 3.Copy Token_ 단추를 클릭하고 이 토큰을 만든 파일에 붙여 넣습니다. AU 서비스를 다시 시작합니다. Copy Restart Command _ 버튼을 클릭하고 AU의 명령 프롬프트에 명령을 붙여 넣습니다.</p>
<p>서버 요구 사항이 충족되지 않았습니다</p>	<p>획득 장치 서버 또는 VM이 을 충족하는지 확인합니다 "요구 사항"</p>
<p>네트워크 요구 사항이 충족되지 않았습니다</p>	<p>획득 장치 서버/VM이 포트 443을 통한 SSL 연결을 통해 데이터 인프라 인사이트 환경(&lt;environment-name&gt;.c01.cloudinsights.NetApp.com)에 액세스할 수 있는지 확인합니다. 다음 명령을 실행합니다. <code>_ping &lt;environment-name&gt; &lt;environment-name&gt;.c01.cloudinsights.NetApp.com</code> <code>tracert &lt;environment-name&gt;.c01.cloudinsights.NetApp.com</code> <code>curl https://NetApp.c01.coudinsights.NetApp.com__wget_sights.&lt;environment-name&gt;</code></p>
<p>프록시 서버가 올바르게 구성되지 않았습니다</p>	<p>프록시 설정을 확인하고 필요한 경우 획득 장치 소프트웨어를 제거/재설치하여 올바른 프록시 설정을 입력합니다. 1."curl"을 시도합니다. 프록시에 대한 "man curl" 정보/문서를 참조하십시오. — proxy, — proxy- * (curl은 많은 프록시 설정을 지원하므로 와일드카드 " * "입니다.) 2."wget"을 시도합니다. 프록시 옵션에 대한 문서를 확인합니다.</p>
<p>획득 서비스를 시작하는 동안 자격 증명 오류가 발생하여 Data Infrastructure Insights에서 획득 장치 설치가 실패했습니다(acq.log에 표시됨).</p>	<p>이 문제는 프록시 자격 증명에 특수 문자가 포함되기 때문에 발생할 수 있습니다. AU(<i>sudo</i> 클라우드 - <i>uninstall.sh</i>)를 제거하고 특수 문자를 사용하지 않고 다시 설치합니다.</p>
<p>권한 문제</p>	<p>관리자 권한이 있는 사용자로 로그인했는지 확인합니다</p>
<p>획득이 실행되지 않습니다</p>	<p>acq.log 의 _&lt;설치 디렉토리&gt;\Cloud Insights\Acquisition Unit\log_folder에서 정보를 찾을 수 있습니다. Windows 서비스를 통해 획득을 다시 시작합니다</p>
<p>데이터 수집 문제</p>	<p>"오류 보고서 전송" 버튼을 클릭하여 Data Collector 랜딩 페이지에서 오류 보고서를 보냅니다</p>

<p>상태: 하트비트 실패</p>	<p>획득 장치(AU)는 리스를 갱신하기 위해 60초마다 Data Infrastructure Insights에 하트비트를 전송합니다. 네트워크 문제나 응답이 없는 Data Infrastructure Insights로 인해 하트비트 호출이 실패하는 경우 AU의 임대 시간이 업데이트되지 않습니다. AU의 임대 시간이 만료되면 Data Infrastructure Insights에 "Heartbeat Failed(하트비트 실패)" 상태가 표시됩니다. 문제 해결 단계: * 획득 장치 서버와 CloudInsights 사이의 네트워크 연결을 확인합니다. * 획득 장치 서비스가 실행 중인지 확인합니다. 서비스가 실행되고 있지 않으면 서비스를 시작합니다. * 획득 장치 로그(&lt;설치 디렉토리&gt;:\Program Files\Cloud Insights\Acquisition Unit\log\acq.log)를 확인하여 오류가 있는지 확인합니다.</p>
<p>"하트비트 오류: 메시지가 표시됩니다"</p>	<p>이 오류는 획득 장치와 Data Infrastructure Insights 환경 간의 통신이 1분 이상 중단되는 네트워크 중단이 발생할 경우 발생할 수 있습니다. AU와 Data Infrastructure Insights 간의 연결이 안정적이고 활성 상태인지 확인합니다.</p>

## 프록시 및 방화벽에 대한 고려 사항

조직에서 인터넷 액세스에 프록시 사용을 요구하는 경우 조직의 프록시 동작을 이해하고 Data Infrastructure Insights가 작동하려면 특정 예외를 찾아야 할 수 있습니다. 다음 사항에 유의하십시오.

- 첫째, 조직에서 기본적으로 액세스를 차단하며 특정 웹 사이트/도메인에 대한 액세스는 예외로 허용됩니까? 이 경우 예외 목록에 다음 도메인을 추가해야 합니다.

\*.cloudinsights.netapp.com

Data Infrastructure Insights 수집 장치는 물론, Data Infrastructure Insights를 사용한 웹 브라우저에서의 상호 작용은 모두 해당 도메인 이름을 가진 호스트에 전달됩니다.

- 둘째, 일부 프록시는 NetApp에서 생성되지 않은 디지털 인증서를 사용하여 Data Infrastructure Insights 웹 사이트를 가장하여 TLS/SSL 검사를 수행하려고 합니다. Data Infrastructure Insights Acquisition Unit의 보안 모델은 기본적으로 이러한 기술과 호환되지 않습니다. Data Infrastructure Insights 획득 장치가 Data Infrastructure Insights에 성공적으로 로그인하여 데이터 검색을 용이하게 하려면 이 기능을 제외한 위의 도메인 이름도 필요합니다.

## 프록시 엔드포인트 보기

온보딩 중에 데이터 수집기를 선택할 때 \* 프록시 설정 \* 링크를 클릭하거나 \* 도움말 > 지원 \* 페이지의 프록시 설정 아래에 있는 링크를 클릭하여 프록시 끝점을 볼 수 있습니다. 다음과 같은 테이블이 표시됩니다. 작업 환경에 워크로드 보안이 있는 경우 구성된 엔드포인트 URL도 이 목록에 표시됩니다.

If your organization requires proxy usage for internet access, you need to understand your organization's proxy behavior and seek certain exceptions for Cloud Insights to work. The simplest way is to add the following domains to the exception list:

Hostname	Port	Protocol	Methods	Endpoint URL Purpose
qtrjks0.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Tenant
00b1100.1234.abcd.12bc.a1b2c3ef56a7.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Ingestion
aulogin.proxyserver.cloudinsights-dev.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Acquisition Unit Authentication
portal.proxy.cloud.netapp.com	443	https	GET, POST, PATCH, PUT, DELETE	Gateway

Close

## 리소스

추가 문제 해결 팁은 에서 찾을 수 있습니다 ["NetApp 기술 자료"](#) (지원 로그인 필요)

추가 지원 정보는 Data Infrastructure Insights 페이지에서 확인할 수 ["지원"](#) 있습니다.

## 실패한 데이터 수집기 조사

데이터 수집기에 오류 메시지와 높음 또는 중간 수준의 영향이 있는 경우 연결된 정보가 있는 데이터 수집기 요약 페이지를 사용하여 이 문제를 조사해야 합니다.

다음 단계를 사용하여 실패한 데이터 수집기에 대한 원인을 확인합니다. 데이터 수집기 오류 메시지는 \* Admin \* (관리) 메뉴 및 \* Installed Data Collector \* (설치된 데이터 수집기 \*) 페이지에 표시됩니다.

### 단계

1. Admin \* > \* Data Collector \* > \* Installed Data Collector \* 를 클릭합니다.
2. 실패한 데이터 수집기의 연결된 이름 을 클릭하여 요약 페이지를 엽니다.
3. 요약 페이지에서 메모 영역을 확인하여 다른 엔지니어가 이 오류를 조사할 수도 있는 메모를 읽습니다.
4. 성능 메시지를 기록합니다.
5. 추가 정보를 표시하려면 이벤트 시각표 그래프의 세그먼트 위로 마우스 포인터를 이동합니다.
6. 장치에 대한 오류 메시지를 선택하고 이벤트 타임라인 아래에 표시된 다음 메시지 오른쪽에 표시되는 오류 세부 정보 아이콘을 클릭합니다.

오류 세부 정보에는 오류 메시지 텍스트, 가능한 원인, 사용 중인 정보 및 문제 해결을 위해 시도할 수 있는 권장 사항이 포함됩니다.

7. 이 Data Collector 영역에 의해 보고된 장치 영역에서 목록을 필터링하여 관심 있는 장치만 표시할 수 있으며 장치의 연결된 \* 이름 \* 을 클릭하여 해당 장치의 자산 페이지를 표시할 수 있습니다.
8. 데이터 수집기 요약 페이지로 돌아가면 페이지 하단에 있는 \* 최근 변경 사항 표시 \* 영역에서 문제를 발생시킨 최근 변경 사항이 있는지 확인합니다.

# Data Infrastructure Insights Data Collector 지원 매트릭스

데이터 수집기 지원 매트릭스는 공급업체 및 모델 정보를 포함하여 Data Infrastructure Insights에서 지원하는 데이터 수집기에 대한 참조를 제공합니다.

## HP Enterprise 3PAR/Alletra 9000/Primera StoreServ 스토리지

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
HPE Alletra 9080	3.1.1(MU1)
HPE_3PAR 20450	3.1.2(MU3)
HPE_3PAR 20800	3.1.3(MU1)
HPE_3PAR 20850	3.1.3(MU2)
HPE_3PAR 20850_R2	3.1.3(MU3)
HPE_3PAR 7200c	3.2.1(MU3)
HPE_3PAR 7400	3.2.1(MU5)
HPE_3PAR 7440c	3.2.2
HPE_3PAR 7450c	3.2.2(MU2)
HPE_3PAR 8200	3.2.2(MU4)
HPE_3PAR 8400	3.2.2(MU6)
HPE_3PAR 8440	3.3.1(MU1)
HPE_3PAR 8450	3.3.1(MU2)
HPE_3PAR 9450	3.3.1(MU5)
HPE_3PAR A630	3.3.2
HPE_3PAR A650	3.3.2(MU1)
HPE_3PAR A670	4.4.1 릴리스 유형: 표준 지원 릴리스
HP_3PAR 20800	4.5.11 릴리스 유형: 확장 지원 릴리스
HP_3PAR 7200	4.5.3 릴리스 유형: 연장 지원 릴리스
HP_3PAR 7200c	4.5.7 릴리스 유형: 확장 지원 릴리스
HP_3PAR 7400	9.5.8 릴리스 유형: 연장 지원 릴리스
HP_3PAR 7400c	
HP_3PAR 7450c	
HP_3PAR 8200	
HP_3PAR 8400	
InServ F400	
InServ T400	
InServ T800입니다	
InServ V400	

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
580					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		스토리지 포트	구현되었습니다	SSH를 클릭합니다	
제품	범주	위치/속성	상태	SSH를 클릭합니다	추가 정보
	볼륨 마스크	이니시에이터	구현되었습니다	SSH를 클릭합니다	
		프로토콜 컨트롤러	구현되었습니다	SSH를 클릭합니다	
		스토리지 포트	구현되었습니다	SSH를 클릭합니다	
		유형	틈	SSH를 클릭합니다	
	볼륨 참조	이름	구현되었습니다	SSH를 클릭합니다	
		스토리지 IP	구현되었습니다	SSH를 클릭합니다	
	WWN 별칭	호스트 별칭	구현되었습니다	SSH를 클릭합니다	
		개체 유형	구현되었습니다	SSH를 클릭합니다	
		출처	구현되었습니다	SSH를 클릭합니다	
		WWN입니다	구현되었습니다	SSH를 클릭합니다	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
588					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	볼륨	읽기 캐시 적중률입니다	구현되었습니다	SMI-S	
		총 캐시 적중률입니다	구현되었습니다	SMI-S	
		캐시 적중률 쓰기	구현되었습니다	SMI-S	
		물리적 용량	구현되었습니다	SMI-S	
		총 용량	구현되었습니다	SMI-S	
		사용된 용량	구현되었습니다	SMI-S	
		사용된 용량 비율	구현되었습니다	SMI-S	
		기록된 용량 비율	구현되었습니다	SMI-S	
		IOPS 읽기	구현되었습니다	SMI-S	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	SMI-S	
		IOPS 쓰기	구현되었습니다	SMI-S	
		읽기 지연 시간	구현되었습니다	SMI-S	
		총 지연 시간	구현되었습니다	SMI-S	
		지연 시간 쓰기	구현되었습니다	SMI-S	
		부분 차단된 비율	구현되었습니다	SMI-S	
		처리량 읽기	구현되었습니다	SMI-S	
		총 처리량	구현되었습니다	SMI-S	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	SMI-S	
		쓰기 보류 중	구현되었습니다	SMI-S	총 쓰기 보류 중

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
3PAR SMI-S의 경우	SMI-S	HTTP/HTT PS	5988/5989		참	참	참	참
3PAR CLI	SSH를 클릭합니다	SSH를 클릭합니다	22		참	거짓	참	참

맨 위로

# Amazon AWS EC2

이 데이터 수집기에서 지원하는 모델 및 버전:

<b>API 버전</b>
2014년 10월 1일

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
594					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		제조업체	구현되었습니다	HTTPS	
제품	범주	이름	구현되었습니다	HTTPS	추가 정보
		피처/속성 OID	상태 구현되었습니다	사용되는 프로토콜입니다	
	정보	API 설명	구현되었습니다	HTTPS	
		API 이름	구현되었습니다	HTTPS	
		API 버전	구현되었습니다	HTTPS	
		데이터 원본 이름	구현되었습니다	HTTPS	정보
		날짜	구현되었습니다	HTTPS	
		개시자 ID	구현되었습니다	HTTPS	
		발신자 키	구현되었습니다	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					



제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜	응답 디스크 읽기 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	VM	총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		사용된 용량 비율	구현되었습니다	HTTPS	
		총 CPU 사용률	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		disklops.total	구현되었습니다	HTTPS	
		디스크 IOPs 쓰기	구현되었습니다	HTTPS	
		읽기 지연 시간	구현되었습니다	HTTPS	
		총 지연 시간	구현되었습니다	HTTPS	
		지연 시간 쓰기	구현되었습니다	HTTPS	
		디스크 처리량 읽기	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	총 디스크 처리량 읽기
		디스크 처리량 쓰기	구현되었습니다	HTTPS	
		IP 처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	총 IP 처리량
		ipThroughput.wri te입니다	구현되었습니다	HTTPS	
		총 메모리 사용률	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
EC2 API를 참조하십시오	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## Amazon AWS S3

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
S3	2010년 8월 1일

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
600					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

					(그런데 이미 있는 모든 디스크의 합계)
제품	범주	확장/속성	구현되었습니다	사용되는 프로토콜입니다	추가요청 가상화 장치입니까?
	스토리지 풀	DWh 용량에 포함	구현되었습니다	HTTPS	ACQ에서 Cotnrol까지, DWH 용량에서는 스토리지 풀이 흥미롭습니다
		이름	구현되었습니다	HTTPS	
		물리적 디스크 용량(MB)	구현되었습니다	HTTPS	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	HTTPS	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	HTTPS	가용 용량을 물리적 용량으로 변환하는 비율입니다
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		신 프로비저닝이 지원됩니다	구현되었습니다	HTTPS	이 내부 볼륨이 볼륨 계층에 대한 신 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?
성능	내부 볼륨	총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		사용된 용량 비율	구현되었습니다	HTTPS	
		총 오브젝트	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
S3 API를 지원합니다	HTTPS	HTTPS	443		참	참	참	참

맨 위로

# Microsoft Azure NetApp Files를 참조하십시오

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델
2019년 6월 1일	Azure NetApp Files

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
604					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

(그런데 이미 있는 모든 디스크의 합계)

제품	범주	확장/속성	구현되었습니다	확장되는 프로토콜입니다	추가요청 가상화 장치입니까?
	스토리지 풀	데이터 할당 용량	틈	HTTPS	데이터에 할당된 용량입니다
		사용된 데이터 용량	구현되었습니다	HTTPS	
		DWh 용량에 포함	구현되었습니다	HTTPS	ACQ에서 Cotnrol까지, DWH 용량에서는 스토리지 풀이 흥미롭습니다
		이름	구현되었습니다	HTTPS	
		물리적 디스크 용량(MB)	구현되었습니다	HTTPS	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	HTTPS	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	HTTPS	가용 용량을 물리적 용량으로 변환하는 비율입니다
		상태	구현되었습니다	HTTPS	
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		씬 프로비저닝이 지원됩니다	구현되었습니다	HTTPS	이 내부 볼륨이 볼륨 계층에 대한 씬 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	HTTPS	
		사용된 총 용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능	내부 볼륨	총 지연 시간	구현되었습니다		
		IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다
		읽기 지연 시간	구현되었습니다		
		IOPS 기타	구현되었습니다		
		IOPS 쓰기	구현되었습니다		
		처리량 읽기	구현되었습니다		
		처리량 쓰기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		총 IOPS	구현되었습니다		
		지연 시간 쓰기	구현되었습니다		
		총 용량	구현되었습니다		
		사용된 용량	구현되었습니다		
		사용된 스냅샷 용량 비율	구현되었습니다		시간 시리즈로 보고됩니다
		사용된 용량 비율	구현되었습니다		
		총 데이터 용량	구현되었습니다		
		사용된 데이터 용량	구현되었습니다		
		사용된 스냅샷 용량	구현되었습니다		
		StoragePool 디스크입니다	IOPS 읽기	구현되었습니다	
		총 IOPS	구현되었습니다		
		IOPS 쓰기	구현되었습니다		
		처리량 읽기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Azure NetApp Files REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## Brocade 파이버 채널 스위치

이 데이터 수집기에서 지원하는 모델 및 버전:



모델	펌웨어 버전입니다
178.0	v5.3.2c
183.0	V6.2.1b
Brocade 200E	V6.2.2g
Brocade 300E	v6.3.2
Brocade 3900	v6.4.1a
Brocade 4024 내장	v6.4.2
Brocade 48000	v6.4.2a
Brocade 5000	v7.0.0
Brocade 5100	v7.0.1b
Brocade 5300	v7.1.0c
Brocade 5480 임베디드	v7.3.0c
Brocade 6505	v7.3.1d
Brocade 6510	v7.4.1d
Brocade 6520	v7.4.1f
Brocade 6548	v7.4.2a
Brocade 7800	v7.4.2c
Brocade 7840	v7.4.2d
브로케이드 DCX	v7.4.2g
Brocade DCX-4S 백본	v7.4.2g_CVR_824494_01
Brocade DCX8510-4	v7.4.2시간
Brocade DCX8510-8	v7.4.2j1
Brocade G610	v8.0.2a
Brocade G620	v8.0.2c
Brocade G630	v8.0.2d입니다
Brocade G720	v8.1.2g
Brocade M5424 임베디드	v8.1.2j 를 참조하십시오
Brocade X6-4	v8.1.2k
Brocade X6-8	버전 8.2.0
Brocade X7-4	버전 8.2.0b
Brocade X7-8	버전 8.2.1c
	버전 8.2.1
	v8.2.2a
	버전 8.2.2b
	v8.2.2c
	v8.2.2D입니다
	v8.2.2d4
	버전 8.2.3
	버전 8.2.3a
	v8.2.3a1을 참조하십시오
	버전 8.2.3b
	v8.2.3c
	v8.2.3c1을 참조하십시오
	v9.0.0b
	v9.0.1a
	v9.0.1b4
	v9.0.1c
	v9.0.1d
	v9.0.1e
	v9.0.1e1
	v9.1.0b
	v9.1.1
	v9.1.1_01
	v9.1.1b

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
614					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		이름	구현되었습니다	수동 입력	
제품	범주	WWN입입니다	장해되었습니다	SSH를 클릭합니다	추가 정보
	WWN 별칭	호스트 별칭	구현되었습니다	SSH를 클릭합니다	
		개체 유형	구현되었습니다	SSH를 클릭합니다	
		출처	구현되었습니다	SSH를 클릭합니다	
		WWN입입니다	구현되었습니다	SSH를 클릭합니다	
	Zone(영역)	영역 이름	구현되었습니다	SSH를 클릭합니다	
	존 구성원	유형	틈	SSH를 클릭합니다	
		WWN입입니다	구현되었습니다	SSH를 클릭합니다	
	조닝 기능	활성 설정	구현되었습니다	SSH를 클릭합니다	
		구성 이름	구현되었습니다	SSH를 클릭합니다	
		기본 영역 지정 동작	구현되었습니다	SSH를 클릭합니다	
		WWN입입니다	구현되었습니다	SSH를 클릭합니다	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

		트래픽 프레임 속도	구현되었습니다	SNMP를 선택합니다	
제품	범주	평균 트래픽 프레임 속도	구현되었습니다	SNMP를 선택합니다	추가 정보
		트래픽 프레임 속도	구현되었습니다	SNMP를 선택합니다	
		평균 프레임 크기	구현되었습니다	SNMP를 선택합니다	트래픽의 평균 프레임 크기입니다
		Tx 프레임	구현되었습니다	SNMP를 선택합니다	트래픽 평균 프레임 크기입니다
		트래픽 속도	구현되었습니다	SNMP를 선택합니다	
		총 트래픽 속도	구현되었습니다	SNMP를 선택합니다	
		트래픽 속도	구현되었습니다	SNMP를 선택합니다	
		트래픽 활용률	구현되었습니다	SNMP를 선택합니다	
		트래픽 활용률	구현되었습니다	SNMP를 선택합니다	총 트래픽 활용도
		트래픽 활용률	구현되었습니다	SNMP를 선택합니다	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Brocade SNMP를 사용합니다	SNMP를 선택합니다	SNMPv1, SNMPv2, SNMPv3	161		참	참	참	참
Brocade SSH	SSH를 클릭합니다	SSH를 클릭합니다	22		거짓	거짓	참	참
데이터 소스 마법사 구성	수동 입력				참	참	참	참

맨 위로

## Brocade Network Advisor HTTP입니다

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
14.4.1	Brocade 5300	v7.2.1a
14.4.3	Brocade 6510	v7.3.1a
14.4.4	Brocade 6520	v7.4.1b
14.4.5	Brocade 6548	v7.4.2d
	Brocade DCX 8510-8	버전 8.2.3b
	Brocade G620	v8.2.3c
	DS-6620B 를 참조하십시오	v9.0.1a
	EMC Connectrix ED-DCX8510-8B	v9.0.1b
		v9.0.1e1

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
622					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		모델	구현되었습니다	HTTP/S를 참조하십시오	
제품	범주	지원됩니다	장해되었습니다	사용자를 참조하십시오	추가 정보
	WWN 별칭	호스트 별칭	구현되었습니다	HTTP/S를 참조하십시오	
		개체 유형	구현되었습니다	HTTP/S를 참조하십시오	
		출처	구현되었습니다	HTTP/S를 참조하십시오	
		WWN입니다	구현되었습니다	HTTP/S를 참조하십시오	
	Zone(영역)	영역 이름	구현되었습니다	HTTP/S를 참조하십시오	
	존 구성원	유형	틈	HTTP/S를 참조하십시오	
		WWN입니다	구현되었습니다	HTTP/S를 참조하십시오	
	조닝 기능	활성 설정	구현되었습니다	HTTP/S를 참조하십시오	
		구성 이름	구현되었습니다	HTTP/S를 참조하십시오	
		WWN입니다	구현되었습니다	HTTP/S를 참조하십시오	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능	포트	bbCreditZero.total	구현되었습니다	HTTP/S를 참조하십시오	
		BB 크레딧	구현되었습니다	HTTP/S를 참조하십시오	
		bbCreditZeroMs	구현되었습니다	HTTP/S를 참조하십시오	
		portErrors.class3 Disccard	구현되었습니다	HTTP/S를 참조하십시오	
		포트 오류.CRC	구현되었습니다	HTTP/S를 참조하십시오	
		포트 오류입니다	구현되었습니다	HTTP/S를 참조하십시오	
		포트 오류입니다	구현되었습니다	HTTP/S를 참조하십시오	짧은 프레임으로 인해 포트 오류가 발생했습니다
		portErrors.linkFailure 를 참조하십시오	구현되었습니다	HTTP/S를 참조하십시오	포트 오류 링크 오류입니다
		포트 오류입니다	구현되었습니다	HTTP/S를 참조하십시오	포트 오류 신호 손실
		포트 오류입니다	구현되었습니다	HTTP/S를 참조하십시오	포트 오류 동기화 손실
		포트 오류입니다	구현되었습니다	HTTP/S를 참조하십시오	포트 오류 시간 초과가 삭제됩니다
		포트 오류입니다	구현되었습니다	HTTP/S를 참조하십시오	총 포트 오류입니다
		트래픽 속도	구현되었습니다	HTTP/S를 참조하십시오	
		총 트래픽 속도	구현되었습니다	HTTP/S를 참조하십시오	
		트래픽 속도	구현되었습니다	HTTP/S를 참조하십시오	
		트래픽 활용률	구현되었습니다	HTTP/S를 참조하십시오	
		트래픽 활용률	구현되었습니다	HTTP/S를 참조하십시오	총 트래픽 활용도
		트래픽 활용률	구현되었습니다	HTTP/S를 참조하십시오	

이 데이터 수집기에서 사용하는 관리 API:

<b>API</b> 를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Brocade Network Advisor REST API	HTTP/HTTPS	HTTP/HTTPS	80/443		참	참	참	참

맨 위로

## Brocade FOS REST

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
Brocade 6505 Brocade G720 Brocade X6-8	v8.2.3c v8.2.3c1을 참조하십시오 v9.0.1e1 v9.1.1b

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
628					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



		유형	틈	HTTPS	
제품	범주	vSAN이 활성화되었습니다	구현되었습니다	HTTPS	추가 정보
		피치/속성 WWN입니다	상태 구현되었습니다	사용되는 브라우저입니다	
	알 수 없음	드라이버	구현되었습니다	HTTPS	
		펌웨어	구현되었습니다	HTTPS	
		제조업체	구현되었습니다	HTTPS	
		모델	구현되었습니다	HTTPS	
		WWN입니다	구현되었습니다	HTTPS	
	WWN 별칭	호스트 별칭	구현되었습니다	HTTPS	
		개체 유형	구현되었습니다	HTTPS	
		출처	구현되었습니다	HTTPS	
		WWN입니다	구현되었습니다	HTTPS	
	Zone(영역)	영역 이름	구현되었습니다	HTTPS	
	존 구성원	유형	틈	HTTPS	
		WWN입니다	구현되었습니다	HTTPS	
	조닝 기능	활성 설정	구현되었습니다	HTTPS	
		구성 이름	구현되었습니다	HTTPS	
		기본 영역 지정 동작	구현되었습니다	HTTPS	
		WWN입니다	구현되었습니다	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

		트래픽 프레임 속도	구현되었습니다	HTTPS	
제품	범주	트래픽 프레임 크기	구현되었습니다	HTTPS는 사용되는 프로토콜입니다	트래픽의 평균 프레임 크기입니다
		Tx 프레임	구현되었습니다	HTTPS	트래픽 평균 프레임 크기입니다
		트래픽 속도	구현되었습니다	HTTPS	
		총 트래픽 속도	구현되었습니다	HTTPS	
		트래픽 속도	구현되었습니다	HTTPS	
		트래픽 활용률	구현되었습니다	HTTPS	
		트래픽 활용률	구현되었습니다	HTTPS	총 트래픽 활용도
		트래픽 활용률	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Brocade FOS REST API	HTTPS		443		참	참	참	참

맨 위로

## Cisco MDS 및 Nexus 패브릭 스위치

이 데이터 수집기에서 지원하는 모델 및 버전:



모델	펌웨어 버전입니다
8978-E04	3.3(1c)
CN1610	4.1(3a)
DS-C9124-2-K9	5.0(1a)
DS-C9124-K9	5.0(3)N2(3.11e)
DS-C9132T-K9	5.0(3)N2(3.23o)
DS-C9134-K9를 참조하십시오	5.0(3)N2(4.01d)
DS-C9148-16P-K9	5.0(3)N2(4.04e)
DS-C9148-32P-K9	5.0(3)N2(4.13e)
DS-C9148-48P-K9	5.0(3)N2(4.13i)
DS-C9148S-K9	5.0(3)N2(4.21e)
DS-C9148T-K9	5.0(3)N2(4.21j)
DS-C9222I-K9	5.0(3)N2(4.21k)
DS-C9250I-K9	5.0(3)N2(4.22c)
DS-C9396S-K9	5.0(8)
DS-C9396T-K9	5.2(2D)
DS-C9506 을 참조하십시오	5.2(3)N2(2.28g)
DS-C9509를 참조하십시오	5.2(6a)
DS-C9513을 참조하십시오	5.2(8)
DS-C9706 을 참조하십시오	5.2(8b)
DS-C9710	5.2(8C)
DS-C9718	5.2(8일)
DS-HP-8GFC-K9	5.2(8F)
DS-HP-FC-K9 를 참조하십시오	5.2(8G)
N5K-C5548UP	5.2(8시간)
N5K-C5596UP	5.2(8i)
N5K-C56128P	6.2(1)
N5K-C5696Q	6.2(11)
UCS-FI-6248UP 을 참조하십시오	6.2(11b)
UCS-FI-6296UP 을 참조하십시오	6.2(11C)
UCS-FI-6332	6.2(11e)
UCS-FI-6332-16UP 을 참조하십시오	6.2(13)
UCS-FI-6454	6.2(13a)
	6.2(15)
	6.2(17)
	6.2(19)
	6.2(21)
	6.2(23)
	6.2(25)
	6.2(27)
	6.2(29)
	6.2(31)
	6.2(33)
	6.2(5)
	6.2(5a)
	6.2(7)
	6.2(9)
	6.2(9a)
	6.2(9c)
	7.3(0) D1(1)
	7.3(0) DY(1)
	7.3(1) DY(1)
	7.3(1)N1(1)
	7.3(13)N1(1)
	7.3(6)N1(1)

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
636					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		이름	구현되었습니다	SNMP를 선택합니다	
제품	범주	WWN입 니다	장 해되었습니다	SNMP를 선택 합니다	추가 정보
	WWN 별칭	호스트 별칭	구현되었습니다	SNMP를 선택합니다	
		개체 유형	구현되었습니다	SNMP를 선택합니다	
		출처	구현되었습니다	SNMP를 선택합니다	
		WWN입니다	구현되었습니다	SNMP를 선택합니다	
	Zone(영역)	영역 이름	구현되었습니다	SNMP를 선택합니다	
		영역 유형	구현되었습니다	SNMP를 선택합니다	
	존 구성원	유형	틈	SNMP를 선택합니다	
		WWN입니다	구현되었습니다	SNMP를 선택합니다	
	조닝 기능	활성 설정	구현되었습니다	SNMP를 선택합니다	
		구성 이름	구현되었습니다	SNMP를 선택합니다	
		기본 영역 지정 동작	구현되었습니다	SNMP를 선택합니다	
		병합 컨트롤	구현되었습니다	SNMP를 선택합니다	
		WWN입니다	구현되었습니다	SNMP를 선택합니다	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

		트래픽 프레임 속도	구현되었습니다	SNMP를 선택합니다	
제품	범주	편차/폭행임 크기	구현되었습니다	SNMP를 선택합니다	트래픽의 평균 프레임 크기입니다
		Tx 프레임	구현되었습니다	SNMP를 선택합니다	트래픽 평균 프레임 크기입니다
		트래픽 속도	구현되었습니다	SNMP를 선택합니다	
		총 트래픽 속도	구현되었습니다	SNMP를 선택합니다	
		트래픽 속도	구현되었습니다	SNMP를 선택합니다	
		트래픽 활용률	구현되었습니다	SNMP를 선택합니다	
		트래픽 활용률	구현되었습니다	SNMP를 선택합니다	총 트래픽 활용도
		트래픽 활용률	구현되었습니다	SNMP를 선택합니다	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Cisco SNMP를 참조하십시오	SNMP를 선택합니다	SNMPv1(재고만), SNMPv2, SNMPv3	161		참	참	참	참

맨 위로

## 결속력

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
C2500입니다	6.5.1f_release - 20210913_13f6a4bf
C2505	6.5.1f_u1_release-20211027_9e4e40cb
C4000 컴퓨팅 노드	6.6.0d_u6_release - 20221204_c03629f0
C4600 을 참조하십시오	6.8.1_release-20220807_6c9115ef
C5036을 참조하십시오	6.8.1_u1_release-20221022_6f58ed2a
C5066을 참조하십시오	6.8.1_U2_RELEASE-20230412_5ced2ed3
C6025를 참조하십시오	6.8.1_u3_release-20230509_1e641b74
C6035를 참조하십시오	7.0_u1_release-20230222_8995f044
C6055를 참조하십시오	
PXG1을 참조하십시오	
UCS-C240M5H10	

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
644					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		일련 번호	구현되었습니다		
제품	범주	UUID입니다	구현되었습니다	사용되는 프로토콜입니다	추가 정보 소프트웨어 버전
		피처/속성 버전	구현되었습니다		
	스토리지 풀	압축 활성화	구현되었습니다		스토리지 풀에 압축이 설정되어 있습니다
		중복 제거가 설정되었습니다	구현되었습니다		스토리지 풀에 중복 제거가 설정되어 있는지 여부
		중복제거 절약	구현되었습니다		중복 제거 축소율 (백분율)
		DWh 용량에 포함	구현되었습니다		ACQ에서 Cotnrol까지, DWH 용량에서는 스토리지 풀이 흥미롭습니다
		이름	구현되었습니다		
		물리적 디스크 용량(MB)	구현되었습니다		스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다		이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다		가용 용량을 물리적 용량으로 변환하는 비율입니다
		상태	구현되었습니다		
		스토리지 풀 ID입니다	구현되었습니다		
		싌 프로비저닝이 지원됩니다	구현되었습니다		이 내부 볼륨이 볼륨 계층에 대한 싌 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다		
		사용된 총 용량입니다	구현되었습니다		총 용량 (MB)입니다
		유형	틈		
		가상	구현되었습니다		스토리지 가상화 장치입니까?
		암호화	구현되었습니다		

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보	
성능	디스크	IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다	
		총 IOPS	구현되었습니다			
		IOPS 쓰기	구현되었습니다			
		처리량 읽기	구현되었습니다			
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)	
		처리량 쓰기	구현되었습니다			
		총 활용률입니다	구현되었습니다			
	내부 볼륨	총 용량	구현되었습니다			
		사용된 용량 비율	구현되었습니다			
		사용된 용량	구현되었습니다			
	Qtree. 10 이상	스토리지	총 지연 시간	구현되었습니다		
			IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다
		읽기 지연 시간	구현되었습니다			IOPS 쓰기
		구현되었습니다			처리량 읽기	구현되었습니다
				처리량 쓰기	구현되었습니다	
			총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		총 IOPS	구현되었습니다			지연 시간 쓰기
		구현되었습니다			총 활용률입니다	구현되었습니다
				StoragePool 디스크입니다	IOPS 읽기	구현되었습니다
		디스크의 읽기 IOPS 수입니다			IOPS 쓰기	구현되었습니다
					처리량 읽기	구현되었습니다
					처리량 쓰기	구현되었습니다
					총 처리량	구현되었습니다
					총 IOPS	구현되었습니다
			평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)			

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Cohesity REST API입니다	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## EMC Celerra(SSH)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
NS-480FC NSX입니다 VG8을 참조하십시오 VNX5200 을 참조하십시오 VNX5300 을 참조하십시오 VNX5400 을 참조하십시오 VNX5600 을 참조하십시오 VNX7600 을 참조하십시오	5.5.38-1 을 참조하십시오 6.0.65-2 7.1.76-4 7.1.79-8 7.1.83-2 8.1.21-266 8.1.21-303 8.1.9-155

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

					(그것이 있는 모든 디스크의 합계)
제품	범주	좌측/속성	구현되었습니다	SSH를 클릭합니다	추요량 가상화 장치입니까?
	스토리지 풀	데이터 할당 용량	틈	SSH를 클릭합니다	데이터에 할당된 용량입니다
		사용된 데이터 용량	구현되었습니다	SSH를 클릭합니다	
		중복 제거가 설정되었습니다	구현되었습니다	SSH를 클릭합니다	스토리지 풀에 중복 제거가 설정되어 있는지 여부
		DWh 용량에 포함	구현되었습니다	SSH를 클릭합니다	ACQ에서 Cotnrol까지, DWH 용량에서는 스트로지 풀이 흥미롭습니다
		이름	구현되었습니다	SSH를 클릭합니다	
		RAID 그룹	구현되었습니다	SSH를 클릭합니다	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	SSH를 클릭합니다	가용 용량을 물리적 용량으로 변환하는 비율입니다
		스냅샷 할당 용량	틈	SSH를 클릭합니다	할당된 스냅샷 용량(MB)입니다
		사용된 스냅샷 용량	구현되었습니다	SSH를 클릭합니다	
		스토리지 풀 ID입니다	구현되었습니다	SSH를 클릭합니다	
		썬 프로비저닝이 지원됩니다	구현되었습니다	SSH를 클릭합니다	이 내부 볼륨이 볼륨 계층에 대한 썬 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	SSH를 클릭합니다	
		사용된 총 용량입니다	구현되었습니다	SSH를 클릭합니다	총 용량 (MB)입니다
		유형	틈	SSH를 클릭합니다	
		가상	구현되었습니다	SSH를 클릭합니다	스토리지 가상화 장치입니까?

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Celerra CLI를 참조하십시오	SSH를 클릭합니다	SSH를 클릭합니다			참	거짓	참	참

맨 위로

## EMC CLARiX(NaviCLI)

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
6.23	AX4-5F8	04.28.000.5.710
6.26	CX3-20f	04.30.000.5.525
6.28	CX3-40f	05.32.000.5.218
7.30	CX4-480	05.32.000.5.219
7.32	VNX5100 을 참조하십시오	05.32.000.5.221
7.33	VNX5200 을 참조하십시오	05.32.000.5.225
	VNX5300 을 참조하십시오	05.32.000.5.249
	VNX5400 을 참조하십시오	05.33.000.5.074
	VNX5500을 참조하십시오	05.33.009.5.155
	VNX5600 을 참조하십시오	05.33.009.5.184
	VNX5700	05.33.009.5.186
	VNX5800 을 참조하십시오	05.33.009.5.218
	VNX7600 을 참조하십시오	05.33.009.5.231
	VNX8000 을 참조하십시오	05.33.009.5.236
		05.33.009.5.238
		05.33.009.6.305
		05.33.021.5.256
		05.33.021.5.266
		2.23.50.5.710입니다
		3.26.20.5.011
		3.26.40.5.029

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
660					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		스토리지 풀 ID입니다	구현되었습니다	CLI를 참조하십시오	
제품	범주	파워/속도/용량	장해되었습니다	이 용량은 정확하지 않습니다	추가 정보
	WWN 별칭	호스트 별칭	구현되었습니다	CLI를 참조하십시오	
		IP	구현되었습니다	CLI를 참조하십시오	
		개체 유형	구현되었습니다	CLI를 참조하십시오	
		출처	구현되었습니다	CLI를 참조하십시오	
		WWN입니다	구현되었습니다	CLI를 참조하십시오	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		총 활용률입니다	구현되었습니다	CLI를 참조하십시오	
제품	범주	파싱속성기	장해되었습니다	이 항목은 참조하지 않습니다	추가 정보
	블록	읽기 캐시 적중률입니다	구현되었습니다	CLI를 참조하십시오	
		총 캐시 적중률입니다	구현되었습니다	CLI를 참조하십시오	
		캐시 적중률 쓰기	구현되었습니다	CLI를 참조하십시오	
		물리적 용량	구현되었습니다	CLI를 참조하십시오	
		총 용량	구현되었습니다	CLI를 참조하십시오	
		사용된 용량	구현되었습니다	CLI를 참조하십시오	
		사용된 용량 비율	구현되었습니다	CLI를 참조하십시오	
		IOPS 읽기	구현되었습니다	CLI를 참조하십시오	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	CLI를 참조하십시오	
		IOPS 쓰기	구현되었습니다	CLI를 참조하십시오	
		읽기 지연 시간	구현되었습니다	CLI를 참조하십시오	
		총 지연 시간	구현되었습니다	CLI를 참조하십시오	
		지연 시간 쓰기	구현되었습니다	CLI를 참조하십시오	
		부분 차단된 비율	구현되었습니다	CLI를 참조하십시오	
		처리량 읽기	구현되었습니다	CLI를 참조하십시오	
		총 처리량	구현되었습니다	CLI를 참조하십시오	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	CLI를 참조하십시오	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Navi CLI를 참조하십시오	CLI를 참조하십시오		6389,2162,2163,443(HTTPS) / 80(HTTP)		참	참	참	거짓

맨 위로

## EMC Data Domain(SSH)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
DD VE의 약어입니다	6.1.2.051-633576
DD2200	6.1.2.20-606786
DD2500을 지원합니다	6.1.2.50-632120
DD3300 을 참조하십시오	6.2.0.30-629757
DD4200	6.2.0.35-635767
DD6300	6.2.1.30-663869
DD6800을 참조하십시오	6.2.1.40-671977
DD6900	6.2.1.60-686365 를 참조하십시오
DD7200	7.10.0.0-1017741
DD9300을 참조하십시오	7.10.1.0-1042928
DD9400을 참조하십시오	7.2.0.30-663847 을 참조하십시오
DD9500	7.2.0.50-671975
DD9800을 참조하십시오	7.2.0.60-682124
DD990을 참조하십시오	7.2.0.70-686759 를 참조하십시오
DD9900입니다	7.2.0.90-692270
	7.6.0.20-689174
	7.6.0.30-690691
	7.7.0.7-1007134
	7.7.1.10-1011247
	7.7.2.011-1011427
	7.7.2.10-1011249
	7.7.3.0-1011963
	7.7.4.0-1017976
	7.7.5.1-1040473
	7.7.5.11-1046187
	7.8.0-1008134

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		할당된 총 용량입니다	구현되었습니다	SSH를 클릭합니다	
제품	범주	최대 총 용량입니다	공해되었습니다	SSH를 클릭합니다	총 용량보 (MB)입니다
		유형	틈	SSH를 클릭합니다	
		가상	구현되었습니다	SSH를 클릭합니다	스토리지 가상화 장치입니까?

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Data Domain CLI를 참조하십시오	SSH를 클릭합니다	SSH를 클릭합니다	22		참	참	참	참

맨 위로

## EMC ECS

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
ECS를 참조하십시오	3.6.1.1 3.6.1.3 3.6.2.1 3.6.2.4.4를 참조하십시오 3.7.0.0 3.7.0.3 3.7.0.4 를 참조하십시오 3.7.0.5 3.8.0.1 3.8.0.2 를 참조하십시오

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
682					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		사용 가능 용량(MB)	구현되었습니다	HTTPS	
제품	범주	최대 사용 가능 용량 활용도(MB)입니다	구현되었습니다	HTTPS 프로토콜입니다	추가 정보
	스토리지 풀	DWh 용량에 포함	구현되었습니다	HTTPS	ACQ에서 Cotnroi까지, DWH 용량에서는 스토리지 풀이 흥미롭습니다
		이름	구현되었습니다	HTTPS	
		물리적 디스크 용량(MB)	구현되었습니다	HTTPS	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	HTTPS	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	HTTPS	가용 용량을 물리적 용량으로 변환하는 비율입니다
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		싌 프로비저닝이 지원됩니다	구현되었습니다	HTTPS	이 내부 볼륨이 볼륨 계층에 대한 싌 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	HTTPS	
		사용된 총 용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능	내부 볼륨	총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		사용된 용량 비율	구현되었습니다	HTTPS	
		총 오브젝트	구현되었습니다	HTTPS	
	스토리지	총 IOPS	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	HTTPS	
	스토리지 노드	총 IOPS	구현되었습니다	HTTPS	
		총 노드 용량 활용률	구현되었습니다	HTTPS	
		노드 용량 활용률 사용 가능	구현되었습니다	HTTPS	
		사용된 노드 용량 활용도	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	HTTPS	
	StoragePool 디스크입니다	용량이 프로비저닝되었습 니다	구현되었습니다	HTTPS	
		물리적 용량	구현되었습니다	HTTPS	
		총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		과도 커밋 용량 비율	구현되었습니다	HTTPS	시간 시리즈로 보고됩니다
		사용된 용량 비율	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
EMC ECS REST API를 참조하십시오	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## Dell EMC Isilon 및 PowerScale REST

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
A200	9.1.0.11
A2000을 참조하십시오	9.1.0.6
A300	9.2.1.10
a3000입니다	9.2.1.11
F200	9.2.1.12
F600 을 참조하십시오	9.2.1.16
F800을 누릅니다	9.2.1.19
F900	9.2.1.21
H400을 누릅니다	9.2.1.6
H500	9.2.1.7
NL410	9.2.1.9
S210	9.4.0.11입니다
X210	9.4.0.12입니다
X400	9.4.0.13
X410	9.4.0.14
	9.4.0.5
	9.4.0.7
	9.5.0.3
	버전 8.0.0.4
	버전 8.0.0.6입니다
	버전 8.0.0.7
	v8.1.2.0
	버전 8.2.2.0

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
688					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		지원합니다			클라우드에 대한 신 프로비저닝을 지원하는지 여부
제품	범주	활형속총 용량입니다	장해되었습니다	사용되는 프로토콜입니다	추가 정보
		사용된 총 용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

					디스크에서 읽기 및 쓰기)(MB/s)
제품	범주	처리량 쓰기	구현되었습니다	HTTPS	추가 정보
		피처/속성 총 활용률입니다	상태 구현되었습니다	사용되는 프로토콜입니다	
	StoragePool 디스크입니다	용량이 프로비저닝되었습 니다	구현되었습니다	HTTPS	
물리적 용량		구현되었습니다	HTTPS		
총 용량		구현되었습니다	HTTPS		
사용된 용량		구현되었습니다	HTTPS		
과도 커밋 용량 비율		구현되었습니다	HTTPS	시간 시리즈로 보고됩니다	
사용된 용량 비율		구현되었습니다	HTTPS		
총 데이터 용량		구현되었습니다	HTTPS		
사용된 데이터 용량		구현되었습니다	HTTPS		
IOPS 읽기		구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다	
총 IOPS		구현되었습니다	HTTPS		
IOPS 쓰기		구현되었습니다	HTTPS		
기타 총 용량		구현되었습니다	HTTPS		
기타 사용된 용량		구현되었습니다	HTTPS		
스냅샷 예약 용량입니다		구현되었습니다	HTTPS		
사용된 스냅샷 용량		구현되었습니다	HTTPS		
사용된 스냅샷 용량 비율		구현되었습니다	HTTPS	시간 시리즈로 보고됩니다	
처리량 읽기		구현되었습니다	HTTPS		
총 처리량		구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)	
처리량 쓰기		구현되었습니다	HTTPS		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
EMC Isilon 및 PowerScale REST API	HTTPS		443		참	참	참	참

맨 위로

## Dell EMC Isilon/PowerScale(CLI)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
A200	9.1.0.10
A2000을 참조하십시오	9.1.0.12
A300	9.1.0.16
F200	9.1.0.18
F800을 누릅니다	9.1.0.19
F900	9.1.0.7
H400을 누릅니다	9.2.1.11
H500	9.2.1.13
H600을 참조하십시오	9.2.1.15
H700을 참조하십시오	9.2.1.22
NL400	9.2.1.7
NL410	9.2.1.9
S210	9.3.0.3
X200	9.4.0.0
X210	9.4.0.10입니다
X400	9.4.0.12입니다
X410	9.4.0.13 9.4.0.14 9.4.0.6입니다 9.4.0.7 v7.1.1.8)을 참조하십시오 v7.2.0.5 v7.2.1.3 v7.2.1.6 버전 8.0.0.4 버전 8.0.0.6입니다 버전 8.0.0.7 v8.0.1.1 v8.1.2.0 버전 8.2.2.0

이 데이터 수집기에서 지원하는 제품:





제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



		UUID입니다	구현되었습니다	SSH를 클릭합니다	
제품	범주	관리/백업지 주소	장해되었습니다	SSH를 클릭합니다	추가 정보
	스토리지 풀	데이터 할당 용량	틈	SSH를 클릭합니다	데이터에 할당된 용량입니다
		사용된 데이터 용량	구현되었습니다	SSH를 클릭합니다	
		DWh 용량에 포함	구현되었습니다	SSH를 클릭합니다	ACQ에서 Cotnrol까지, DWH 용량에서는 스토리지 풀이 흥미롭습니다
		이름	구현되었습니다	SSH를 클릭합니다	
		물리적 디스크 용량(MB)	구현되었습니다	SSH를 클릭합니다	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	SSH를 클릭합니다	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	SSH를 클릭합니다	가용 용량을 물리적 용량으로 변환하는 비율입니다
		스냅샷 할당 용량	틈	SSH를 클릭합니다	할당된 스냅샷 용량(MB)입니다
		사용된 스냅샷 용량	구현되었습니다	SSH를 클릭합니다	
		스토리지 풀 ID입니다	구현되었습니다	SSH를 클릭합니다	
		씬 프로비저닝이 지원됩니다	구현되었습니다	SSH를 클릭합니다	이 내부 볼륨이 볼륨 계층에 대한 씬 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	SSH를 클릭합니다	
		사용된 총 용량입니다	구현되었습니다	SSH를 클릭합니다	총 용량 (MB)입니다
		유형	틈	SSH를 클릭합니다	
		가상	구현되었습니다	SSH를 클릭합니다	스토리지 가상화 장치입니까?

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		처리량 쓰기	구현되었습니다	SSH를 클릭합니다	
제품	범주	현재 사용 중입니다	장애되었습니다	SSH를 클릭합니다	추가 정보
	StoragePool 디스크입니다	용량이 프로비저닝되었습니다	구현되었습니다	SSH를 클릭합니다	
		물리적 용량	구현되었습니다	SSH를 클릭합니다	
		총 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 용량	구현되었습니다	SSH를 클릭합니다	
		과도 커밋 용량 비율	구현되었습니다	SSH를 클릭합니다	시간 시리즈로 보고됩니다
		사용된 용량 비율	구현되었습니다	SSH를 클릭합니다	
		총 데이터 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 데이터 용량	구현되었습니다	SSH를 클릭합니다	
		스냅샷 예약 용량입니다	구현되었습니다	SSH를 클릭합니다	
		사용된 스냅샷 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 스냅샷 용량 비율	구현되었습니다	SSH를 클릭합니다	시간 시리즈로 보고됩니다

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Isilon SSH	SSH를 클릭합니다	SSH를 클릭합니다	22		참	거짓	참	참

맨 위로

## EMC PowerStore REST

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
PowerStore 1000T입니다	2.0.1.3
PowerStore 1200T	2.1.1.0
PowerStore 3000T	2.1.1.1
PowerStore 3200T	3.0.0.1
PowerStore 5000T	3.2.0.0
PowerStore 5000X	3.2.0.1
PowerStore 9000T	3.2.1.0
PowerStore 9200T	

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
716					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		용량입니다			(MB)입니다
		유형	틈		
제품	범주	확장/속성	공해되었습니다	사용되는 프로토콜입니다	추요량만 가상화 장치입니까?
	볼륨	용량	구현되었습니다		사용된 스냅샷 용량(MB)입니다
		접합 경로	구현되었습니다		
		이름	구현되었습니다		
		총 물리적 용량입니다	구현되었습니다		총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		스토리지 풀 ID입니다	구현되었습니다		
		씬 프로비저닝되었습 니다	구현되었습니다		
		유형	틈		
		UUID입니다	구현되었습니다		
		사용된 용량	구현되었습니다		
		QoS - 정책	구현되었습니다		
	볼륨 맵	LUN을 클릭합니다	구현되었습니다		백엔드 LUN의 이름입니다
		마스킹이 필요합니다	구현되었습니다		
		프로토콜 컨트롤러	구현되었습니다		
		스토리지 포트	구현되었습니다		
		유형	틈		
	볼륨 마스크	이니시에이터	구현되었습니다		
		프로토콜 컨트롤러	구현되었습니다		
		유형	틈		
	WWN 별칭	호스트 별칭	구현되었습니다		
		개체 유형	구현되었습니다		
		출처	구현되었습니다		
		WWN입니다	구현되었습니다		

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)		처리량 쓰기
제품	범주	피처/속성	사용되는 프로토콜입니다		추가 정보
	구현되었습니다			볼륨	물리적 용량
	구현되었습니다				총 용량
	구현되었습니다				사용된 용량
	구현되었습니다				사용된 용량 비율
	구현되었습니다				IOPS 읽기
	구현되었습니다		디스크의 읽기 IOPS 수입니다		총 IOPS
	구현되었습니다				IOPS 쓰기
	구현되었습니다				읽기 지연 시간
	구현되었습니다				총 지연 시간
	구현되었습니다				지연 시간 쓰기
	구현되었습니다				처리량 읽기
	구현되었습니다				총 처리량
	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)		처리량 쓰기

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
EMC PowerStore REST API를 참조하십시오	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## EMC RecoverPoint(HTTP)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
RecoverPoint를 참조하십시오	5.1.P1(C.15) 5.1.SP4.P1(H.89) 5.1.SP4.P2(H.101) 5.1.SP4.P3(H.109) 5.1.SP4.P4(H.97)

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	좌측/속성	구현되었습니다	지원되는 프로토콜입니다	(그런데 이미 있는 모든 디스크의 합계) 추요량만 가상화 장치입니까?
	스토리지 노드	메모리 크기	탐	HTTPS	장치 메모리(MB)
		모델	구현되었습니다	HTTPS	
		이름	구현되었습니다	HTTPS	
		프로세서 수	구현되었습니다	HTTPS	장치 CPU
		일련 번호	구현되었습니다	HTTPS	
		상태	구현되었습니다	HTTPS	장치 상태를 설명하는 자유 텍스트입니다
		UUID입니다	구현되었습니다	HTTPS	
		버전	구현되었습니다	HTTPS	소프트웨어 버전
		저장소 동기화	모드를 선택합니다	구현되었습니다	HTTPS
	모드 Enum		구현되었습니다	HTTPS	
	소스 스토리지		구현되었습니다	HTTPS	
	소스 볼륨		구현되었습니다	HTTPS	
	상태		구현되었습니다	HTTPS	장치 상태를 설명하는 자유 텍스트입니다
	상태 번호		구현되었습니다	HTTPS	
	타겟 스토리지		구현되었습니다	HTTPS	
	타겟 볼륨		구현되었습니다	HTTPS	
	제공합니다		구현되었습니다	HTTPS	스토리지 효율성이 변경되는 기술입니다

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
RecoverPoint REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## EMC ScaleIO 및 PowerFlex REST

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
ScaleIO를 참조하십시오	R2_6.1100.113 을 참조하십시오 R2_6.1100.115 를 참조하십시오 R3_0.1400.101 을 참조하십시오 R3_5.1200.104 을 참조하십시오 R3_6.500.113을 참조하십시오 R3_6.700.103을 참조하십시오

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		용량입니다			(MB)입니다
		유형	틈	HTTPS	
제품	범주	파쳐/속성	공해되었습니다	사용되는 프로토콜입니다	추뵐량만 가상화 장치입니까?
	볼륨	용량	구현되었습니다	HTTPS	사용된 스냅샷 용량(MB)입니다
		접합 경로	구현되었습니다	HTTPS	
		이름	구현되었습니다	HTTPS	
		총 물리적 용량입니다	구현되었습니다	HTTPS	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		씬 프로비저닝되었습니다	구현되었습니다	HTTPS	
		UUID입니다	구현되었습니다	HTTPS	
		호스트 IP입니다	구현되었습니다	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					



		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	
	스토리지 노드	IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다		
		IOPS 쓰기	구현되었습니다		
		읽기 지연 시간	구현되었습니다		
		총 지연 시간	구현되었습니다		
		지연 시간 쓰기	구현되었습니다		
		처리량 읽기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다		
		StoragePool 디스크입니다	IOPS 읽기	구현되었습니다	
	IOPS 쓰기		구현되었습니다		
	처리량 읽기		구현되었습니다		
	처리량 쓰기		구현되었습니다		
	총 처리량		구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
	총 IOPS		구현되었습니다		
	볼륨	물리적 용량	구현되었습니다		
		총 용량	구현되었습니다		
		IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다		
		IOPS 쓰기	구현되었습니다		
		처리량 읽기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
EMC ScaleIO 및 PowerFlex REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## EMC Symmetrix CLI를 참조하십시오

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
v10.0.0.0	DMX3-24	5773.198.142(168D0000) 빌드 5
v10.0.1.0	DMX4-24	5876.272.177(16F40000) 빌드 39
V7.6.2.67	PMax2000을 참조하십시오	5876.286.194(16F40000) 빌드 115
V8.3.0.22	PowerMax_2000	5876.309.196(16F40000) 빌드 162
V8.3.0.6을 참조하십시오	PowerMax_8000	5977.1131.1131(17590000) 빌드
V8.4.0.7	VMAX-1	551
V8.4.0.9	VMAX100K	5977.1151.1151(17590000) 빌드 45
V9.1.0.18	VMAX10K입니다	5977.1151.1151(17590000) 빌드 59
V9.1.0.5	VMAX200K입니다	5977.1151.1151(17590000) 빌드 60
V9.1.0.6입니다	VMAX250F 를 참조하십시오	5977.1151.1151(17590000) 빌드 9
V9.2.0.0	VMAX400K	5978.479.479(175A0000) 빌드 195
V9.2.1.0	VMAX40K입니다	5978.711.711(175A0000) 빌드 113
V9.2.1.1	VMAX450F 를 참조하십시오	5978.711.711(175A0000) 빌드 139
V9.2.1.2	VMAX850F 를 참조하십시오	5978.711.711(175A0000) 빌드 149
V9.2.2.0	VMAX950F 를 참조하십시오	5978.711.711(175A0000) 빌드 194
V9.2.3.0		5978.711.711(175A0000) 빌드 196
V9.2.3.1		5978.711.711(175A0000) 빌드 220
V9.2.3.4		5978.711.711(175A0000) 빌드 239
V9.2.3.5		5978.711.711(175A0000) 빌드 252
V9.2.3.6		5978.711.711(175A0000) 빌드 267
V9.2.4.1		5978.711.711(175A0000) 빌드 278
V9.2.4.2		5978.711.711(175A0000) 빌드 287
		5978.711.711(175A0000) 빌드 335
		5978.711.711(175A0000) 빌드 365
		5978.711.711(175A0000) 빌드 366
		5978.711.711(175A0000) 빌드 388
		5978.711.711(175A0000) 빌드 416
		5978.711.711(175A0000) 빌드 436
		5978.711.711(175A0000) 빌드 438
		5978.711.711(175A0000) 빌드 448
		5978.711.711(175A0000) 빌드 461
		5978.711.711(175A0000) 빌드 480
		5978.711.711(175A0000) 빌드 484
		5978.711.711(175A0000) 빌드 502
		5978.711.711(175A0000) 빌드 529
		5978.711.711(175A0000) 빌드 8

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		사용된 용량	구현되었습니다		
제품	블록 참조 범주	이름	구현되었습니다	사용되는 프로토콜입니다	추가 정보
		피처/속성 스토리지 IP	상태 구현되었습니다		
	WWN 별칭	호스트 별칭	구현되었습니다		
		개체 유형	구현되었습니다		
		출처	구현되었습니다		
		WWN입니다	구현되었습니다		

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	볼륨	읽기 캐시 적중률입니다	구현되었습니다		
		총 캐시 적중률입니다	구현되었습니다		
		캐시 적중률 쓰기	구현되었습니다		
		물리적 용량	구현되었습니다		
		총 용량	구현되었습니다		
		사용된 용량	구현되었습니다		
		쓰인 용량	구현되었습니다		
		사용된 용량 비율	구현되었습니다		
		기록된 용량 비율	구현되었습니다		
		IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다		
		IOPS 쓰기	구현되었습니다		
		읽기 지연 시간	구현되었습니다		
		총 지연 시간	구현되었습니다		
		지연 시간 쓰기	구현되었습니다		
		처리량 읽기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다		
	쓰기 보류 중	구현되었습니다		총 쓰기 보류 중	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
SYMCLI를 참조하십시오	CLI를 참조하십시오		2707		참	참	참	참
Symmetrix SMI- S입니다	SMI-S	HTTP/HTT PS	5988/5989		참	거짓	거짓	참

맨 위로

# Dell Unisphere REST입니다

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
v10.0.0.5	PowerMax_2000	5978.479.479 빌드 350
v10.0.1.3 버전	PowerMax_2500입니다	5978.711.711 빌드 252
V9.2.1.6	PowerMax_8000	5978.711.711 빌드 278 빌드 278
V9.2.3.20	VMAX250F 를 참조하십시오	5978.711.711 빌드 287
V9.2.3.22	VMAX950F 를 참조하십시오	5978.711.711 빌드 329 빌드 329
V9.2.3.4		5978.711.711 빌드 365
V9.2.4.1		5978.711.711 빌드 365
		5978.711.711 빌드 376
		5978.711.711 빌드 388 빌드 388
		5978.711.711 빌드 416
		5978.711.711 빌드 435
		5978.711.711 빌드 448
		5978.711.711 빌드 461 빌드 461
		5978.711.711 빌드 481 빌드 481
		5978.711.711 빌드 484
		5978.711.711 빌드 484 빌드 484
		5978.711.711 빌드 502
		6079.125.0 빌드 53 빌드 53
		6079.175.0 빌드 0

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
750					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		UUID입니다	구현되었습니다	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까? 추가 정보
제품	범주	피처/속성 스토리지 그룹	상태 구현되었습니다	사용되는 프로토콜입니다	
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	WWN 별칭	호스트 별칭	구현되었습니다	HTTPS	
		개체 유형	구현되었습니다	HTTPS	
		출처	구현되었습니다	HTTPS	
		WWN입니다	구현되었습니다	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

	HTTPS		IOPS 읽기	구현되었습니다	HTTPS
제품	뎀추크의 읽기 IOPS 수입니다	최대 IOPS	구현되었습니다	HTTPS는 사용되는 프로토콜입니다	추가 정보
	IOPS 쓰기	구현되었습니다	HTTPS		스냅샷 예약 용량입니다
	구현되었습니다	HTTPS		사용된 스냅샷 용량 비율	구현되었습니다
	HTTPS	시간 시리즈로 보고됩니다	처리량 읽기	구현되었습니다	HTTPS
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
	처리량 쓰기	구현되었습니다	HTTPS		총 활용률입니다
	구현되었습니다	HTTPS		볼륨	물리적 용량
	구현되었습니다	HTTPS			총 용량
	구현되었습니다	HTTPS			사용된 용량
	구현되었습니다	HTTPS			사용된 용량 비율
	구현되었습니다	HTTPS			기록된 용량 비율
	구현되었습니다	HTTPS			IOPS 읽기
	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다		총 IOPS
	구현되었습니다	HTTPS			IOPS 쓰기
	구현되었습니다	HTTPS			읽기 지연 시간
	구현되었습니다	HTTPS			총 지연 시간
	구현되었습니다	HTTPS			지연 시간 쓰기
	구현되었습니다	HTTPS			처리량 읽기
	구현되었습니다	HTTPS			총 처리량
	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)		처리량 쓰기

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Dell Unisphere API를 참조하십시오	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## EMC VNX(SSH)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
VNX5300 을 참조하십시오	05.33.009.5.231
VNX5400 을 참조하십시오	7.1.76-4
VNX5700	7.1.80-3 을 참조하십시오
VNX5800 을 참조하십시오	8.1.9-232

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		이중화	구현되었습니다	SSH를 클릭합니다	이중화 레벨
제품	범주	피치속 유형	상정할 수 없습니다	SSH를 클릭합니다	추가 정보
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	SSH를 클릭합니다	백엔드 LUN의 이름입니다
		스토리지 포트	구현되었습니다	SSH를 클릭합니다	
		프로토콜 컨트롤러	구현되었습니다	SSH를 클릭합니다	
		유형	틈	SSH를 클릭합니다	
	볼륨 마스크	스토리지 포트	구현되었습니다	SSH를 클릭합니다	
		이니시에이터	구현되었습니다	SSH를 클릭합니다	
		프로토콜 컨트롤러	구현되었습니다	SSH를 클릭합니다	
		유형	틈	SSH를 클릭합니다	
	WWN 별칭	출처	구현되었습니다	SSH를 클릭합니다	
		호스트 별칭	구현되었습니다	SSH를 클릭합니다	
		WWN입니다	구현되었습니다	SSH를 클릭합니다	
		개체 유형	구현되었습니다	SSH를 클릭합니다	
		IP	구현되었습니다	SSH를 클릭합니다	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
770					

		총 활용률입니다	구현되었습니다	SSH를 클릭합니다	
제품	범주	파워 사용성기	장애되었습니다	SSH를 클릭합니다	추가 정보
	스토리지	실패한 물리적 용량	구현되었습니다	SSH를 클릭합니다	
		물리적 용량	구현되었습니다	SSH를 클릭합니다	
		예비 물리적 용량	구현되었습니다	SSH를 클릭합니다	스페어 디스크의 물리적 용량 (스페어가 있는 모든 디스크의 합계)
		StoragePools 용량	구현되었습니다	SSH를 클릭합니다	
		IOPS 기타	구현되었습니다	SSH를 클릭합니다	
		IOPS 읽기	구현되었습니다	SSH를 클릭합니다	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	SSH를 클릭합니다	
		IOPS 쓰기	구현되었습니다	SSH를 클릭합니다	
		읽기 지연 시간	구현되었습니다	SSH를 클릭합니다	
		총 지연 시간	구현되었습니다	SSH를 클릭합니다	
		지연 시간 쓰기	구현되었습니다	SSH를 클릭합니다	
		처리량 읽기	구현되었습니다	SSH를 클릭합니다	
		총 처리량	구현되었습니다	SSH를 클릭합니다	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	SSH를 클릭합니다	
		스토리지 노드	IOPS 읽기	구현되었습니다	SSH를 클릭합니다
	총 IOPS		구현되었습니다	SSH를 클릭합니다	
	IOPS 쓰기		구현되었습니다	SSH를 클릭합니다	
	총 활용률입니다		구현되었습니다	SSH를 클릭합니다	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
VNX SSH 및 CLI	SSH를 클릭합니다	SSH를 클릭합니다	22		참	거짓	참	참

맨 위로

## EMC VNXe 및 Unity Unisphere(CLI)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
Unity 300	3.1.17.10223906
유니티 300F	3.1.17.10229825
유니티 350F	4.1.2.9257522
Unity 380	4.2.1.9535982
유니티 380F	4.2.3.9670635
Unity 400	4.5.1.0.5.001
유니티 400F	5.0.2.0.5.009
유니티 450F	5.0.6.0.5.008
유니티 480F	5.0.8.0.5.007
Unity 500	5.1.2.0.5.007
유니티 550F	5.1.3.0.5.003
유니티 600	5.2.1.0.5.013
유니티 600F	5.2.2.0.5.004
유니티 650F	5.2.0.6.201
유니티 680F	5.3.0.0.5.120
유니티 880	
VNXe3200	

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		용량입니다			(MB)입니다
		유형	틈	HTTPS	
제품	범주	확장/속성	공해되었습니다	확장되는 프로토콜입니다	추가요청 가상화 장치입니까?
	저장소 동기화	모드를 선택합니다	구현되었습니다	HTTPS	
		모드 Enum	구현되었습니다	HTTPS	
		소스 스토리지	구현되었습니다	HTTPS	
		소스 볼륨	구현되었습니다	HTTPS	
		상태	구현되었습니다	HTTPS	장치 상태를 설명하는 자유 텍스트입니다
		상태 번호	구현되었습니다	HTTPS	
		타겟 스토리지	구현되었습니다	HTTPS	
		타겟 볼륨	구현되었습니다	HTTPS	
		제공합니다	구현되었습니다	HTTPS	스토리지 효율성이 변경되는 기술입니다
	볼륨	용량	구현되었습니다	HTTPS	사용된 스냅샷 용량(MB)입니다
		접합 경로	구현되었습니다	HTTPS	
		이름	구현되었습니다	HTTPS	
		총 물리적 용량입니다	구현되었습니다	HTTPS	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		썸 프로비저닝되었습니다	구현되었습니다	HTTPS	
		UUID입니다	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
780					

	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다		총 IOPS
제품	구현되었습니다	HTTPS			IOPS 쓰기
	범주 구현되었습니다	피쳐/속성 HTTPS	상태	사용되는 프로토콜입니다	추가 정보 총 활용률입니다
	구현되었습니다	HTTPS		StoragePool 디스크입니다	용량이 프로비저닝되었습 니다
	구현되었습니다	HTTPS			물리적 용량
	구현되었습니다	HTTPS			용량 소프트 제한값
	구현되었습니다	HTTPS			총 용량
	구현되었습니다	HTTPS			사용된 용량
	구현되었습니다	HTTPS			과도 커밋 용량 비율
	구현되었습니다	HTTPS	시간 시리즈로 보고됩니다		사용된 용량 비율
	구현되었습니다	HTTPS			IOPS 읽기
	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다		총 IOPS
	구현되었습니다	HTTPS			IOPS 쓰기
	구현되었습니다	HTTPS			처리량 읽기
	구현되었습니다	HTTPS			총 처리량
	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)		처리량 쓰기
	구현되었습니다	HTTPS		블룸	물리적 용량
	구현되었습니다	HTTPS			총 용량
	구현되었습니다	HTTPS			사용된 용량
	구현되었습니다	HTTPS			사용된 용량 비율
	구현되었습니다	HTTPS			IOPS 읽기
	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다		총 IOPS
	구현되었습니다	HTTPS			IOPS 쓰기
	구현되었습니다	HTTPS			총 지연 시간
	구현되었습니다	HTTPS			처리량 읽기
	구현되었습니다	HTTPS			총 처리량
	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)		처리량 쓰기



이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
VNXe 및 Unisphere CLI	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## EMC VPLEX를 참조하십시오

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
VPLEX	5.4.1.00.00.07 5.4.1.01.00.05 6.2.0.03.00.02 6.2.0.04.00.07 6.2.0.05.00.11 6.2.0.07.00.02 를 참조하십시오

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		UUID입니다	구현되었습니다	HTTP/S를 참조하십시오	
제품	범주	파싱/속성	공해되었습니다	HTTP/S를 참조하십시오	추가요청 가상화 장치입니까?
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTP/S를 참조하십시오	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTP/S를 참조하십시오	
		스토리지 포트	구현되었습니다	HTTP/S를 참조하십시오	
		유형	틈	HTTP/S를 참조하십시오	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTP/S를 참조하십시오	
		프로토콜 컨트롤러	구현되었습니다	HTTP/S를 참조하십시오	
		스토리지 포트	구현되었습니다	HTTP/S를 참조하십시오	
		유형	틈	HTTP/S를 참조하십시오	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
788					

		처리량 쓰기	구현되었습니다	SSH를 클릭합니다	
제품	범주	평균 처리량입니다	구현되었습니다	SSH를 클릭합니다	추가 정보
	StoragePool 디스크입니다	용량이 프로비저닝되었습니다	구현되었습니다	SSH를 클릭합니다	
		총 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 용량	구현되었습니다	SSH를 클릭합니다	
		과도 커밋 용량 비율	구현되었습니다	SSH를 클릭합니다	시간 시리즈로 보고됩니다
		사용된 용량 비율	구현되었습니다	SSH를 클릭합니다	
		기타 총 용량	구현되었습니다	SSH를 클릭합니다	
		기타 사용된 용량	구현되었습니다	SSH를 클릭합니다	
	볼륨	물리적 용량	구현되었습니다	SSH를 클릭합니다	
		총 용량	구현되었습니다	SSH를 클릭합니다	
		총 IOPS	구현되었습니다	SSH를 클릭합니다	
		읽기 지연 시간	구현되었습니다	SSH를 클릭합니다	
		총 지연 시간	구현되었습니다	SSH를 클릭합니다	
		지연 시간 쓰기	구현되었습니다	SSH를 클릭합니다	
		처리량 읽기	구현되었습니다	SSH를 클릭합니다	
		총 처리량	구현되었습니다	SSH를 클릭합니다	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	SSH를 클릭합니다	

이 데이터 수집기에서 사용하는 관리 API:



API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
EMC VPLEX CLI를 참조하십시오	SSH를 클릭합니다	SSH를 클릭합니다	22		참	참	참	참
EMC VPLEX API를 참조하십시오	HTTP/HTTPS	HTTP/HTTPS	80/443		참	참	참	참

맨 위로

## EMC XtremIO(HTTP)

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
6.2.1	1개의 벽돌 및 125TB	4.0.27-1
6.2.2	1개의 벽돌 및 24TB	4.0.31-11
6.3.1	Brick 1개 및 26TB	6.1.0-99_X2
6.3.2	1개의 벽돌 및 31TB	6.3.3-8_X2
6.3.3	Brick 1개 및 62TB	6.4.0-22_X2
6.4.0	Brick 1개 및 8TB	6.4.0-36_HotFix_2_X2
	1X10TB입니다	
	1x20TB	
	1X40TB	
	Brick 2개 및 52TB	
	2개의 Brick과 62TB	
	2개의 Brick 및 76TB	
	2개의 벽돌 및 83TB	
	2X10TB	
	2x20TB	
	2X40TB	
	Brick 3개 및 251TB	
	3개의 벽돌 및 283TB	
	4개의 Brick 및 125TB	
	4개의 벽돌 및 503TB	
	4개의 Brick 및 628TB	
	4개의 Brick 및 754TB	
	4x20TB	
	4X40TB	
	6x20TB	

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



		UUID입니다	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
제품	범주	파싱/속성	공해되었습니다	사용되는 프로토콜입니다	추요량만 가상화 장치입니까?
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		유형	틈	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

		평균 처리량	구현되었습니다	HTTPS	평균 디스크 성능 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	
	StoragePool 디스크입니다	용량이 프로비저닝되었습 니다	구현되었습니다	HTTPS	
		물리적 용량	구현되었습니다	HTTPS	
		총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		과도 커밋 용량 비율	구현되었습니다	HTTPS	시간 시리즈로 보고됩니다
		사용된 용량 비율	구현되었습니다	HTTPS	
		총 데이터 용량	구현되었습니다	HTTPS	
		사용된 데이터 용량	구현되었습니다	HTTPS	
		볼륨	물리적 용량	구현되었습니다	HTTPS
	총 용량		구현되었습니다	HTTPS	
	사용된 용량		구현되었습니다	HTTPS	
	사용된 용량 비율		구현되었습니다	HTTPS	
	IOPS 읽기		구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
	총 IOPS		구현되었습니다	HTTPS	
	IOPS 쓰기		구현되었습니다	HTTPS	
	읽기 지연 시간		구현되었습니다	HTTPS	
	총 지연 시간		구현되었습니다	HTTPS	
	지연 시간 쓰기		구현되었습니다	HTTPS	
	부분 차단된 비율		구현되었습니다	HTTPS	
	처리량 읽기		구현되었습니다	HTTPS	
	총 처리량		구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
	처리량 쓰기		구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
EMC XtremIO REST API	HTTPS	HTTPS	443		참	참	참	참

[맨 위로](#)

## NetApp E-Series를 통해 비즈니스 이점을 제공합니다

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
2600입니다	08.40.60.01
2660을 참조하십시오	8.10.14.0
2680입니다	8.20.11.0
2702를 참조하십시오	8.20.27.0
2704	8.20.30.0
2800B 이하	8.20.5.0
2804	8.20.8.0
2806	8.25.14.0
3000입니다	8.25.6.0
5480	8.30.1.0
5486입니다	8.40.0.1
5488입니다	8.40.0.3
5504	8.40.20.0입니다
5564	8.40.30.3
5600	8.40.40.0
5700입니다	8.40.50.0
5700B	8.40.60.1
6000입니다	8.40.60.2 를 참조하십시오
	8.40.60.3
	8.42.20.0입니다
	8.50.0.3
	8.50.0.4
	8.51.0.0
	8.52.0.0
	8.52.0.1
	8.53.0.1
	8.53.0.4
	8.62.0.0
	8.62.0.2 를 참조하십시오
	8.63.0.2 를 참조하십시오
	8.70.0.3 이상
	8.71.2.0
	8.71.3.0
	8.72.0.0
	8.72.1.0
	8.72.2.0
	8.73.0.0
	8.74.0.0
	8.74.1.0
	8.74.2.0
	8.74.3.0
	8.75.0.0

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	용량입니다	구현되었습니다	RMI	총 용량 (MB)입니다 추가 정보
		사용된 총 용량입니다 피처/속성 유형	상태 틈	사용되는 이벤트콜입니다	
		가상	구현되었습니다	RMI	스토리지 가상화 장치입니까?
	볼륨	용량	구현되었습니다	RMI	사용된 스냅샷 용량(MB)입니다
		디스크 유형	사용할 수 없습니다	RMI	
		이름	구현되었습니다	RMI	
		총 물리적 용량입니다	구현되었습니다	RMI	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		이중화	구현되었습니다	RMI	이중화 레벨
		스토리지 풀 ID입니다	구현되었습니다	RMI	
		쓴 프로비저닝되었습니다	구현되었습니다	RMI	
		유형	틈	RMI	
		UUID입니다	구현되었습니다	RMI	
		사용된 용량	구현되었습니다	RMI	
		가상	구현되었습니다	RMI	스토리지 가상화 장치입니까?
		쓰인 용량	구현되었습니다	RMI	호스트가 이 볼륨에 쓴 총 용량(MB)입니다
		볼륨 맵	LUN을 클릭합니다	구현되었습니다	RMI
	스토리지 포트		구현되었습니다	RMI	
	유형		틈	RMI	
	볼륨 마스크	이니시에이터	구현되었습니다	RMI	
		스토리지 포트	구현되었습니다	RMI	
		유형	틈	RMI	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
808					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	읽기 사용률	구현되었습니다	RMI	추가 정보
		총 활용률입니다 피처/속성 사용률 쓰기	구현되었습니다 상태 구현되었습니다	RMI 사용되는 프로토콜입니다	
볼륨		읽기 캐시 적중률입니다	구현되었습니다	RMI	
		총 캐시 적중률입니다	구현되었습니다	RMI	
		캐시 적중률 쓰기	구현되었습니다	RMI	
		물리적 용량	구현되었습니다	RMI	
		총 용량	구현되었습니다	RMI	
		사용된 용량	구현되었습니다	RMI	
		쓰인 용량	구현되었습니다	RMI	
		사용된 용량 비율	구현되었습니다	RMI	
		기록된 용량 비율	구현되었습니다	RMI	
		IOPS 읽기	구현되었습니다	RMI	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	RMI	
		IOPS 쓰기	구현되었습니다	RMI	
		읽기 지연 시간	구현되었습니다	RMI	
		총 지연 시간	구현되었습니다	RMI	
		지연 시간 쓰기	구현되었습니다	RMI	
		처리량 읽기	구현되었습니다	RMI	
		총 처리량	구현되었습니다	RMI	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
처리량 쓰기	구현되었습니다	RMI			

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
SANtricity API를 참조하십시오	RMI	TCP			참	참	거짓	거짓

맨 위로

# Google 클라우드 컴퓨팅

이 데이터 수집기에서 지원하는 모델 및 버전:

<b>API 버전</b>
V1

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
814					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		제조업체	구현되었습니다	HTTPS	
제품	범주	이름	구현되었습니다	HTTPS	추가 정보
		피처/속성 OID	상태 구현되었습니다	사용되는 프로토콜입니다	
	정보	API 설명	구현되었습니다	HTTPS	
		API 이름	구현되었습니다	HTTPS	
		API 버전	구현되었습니다	HTTPS	
		데이터 원본 이름	구현되었습니다	HTTPS	정보
		날짜	구현되었습니다	HTTPS	
		개시자 ID	구현되었습니다	HTTPS	
		발신자 키	구현되었습니다	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	응답 디스크 읽기 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	VM	총 용량	구현되었습니다	HTTPS	
		총 CPU 사용률	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		disklops.total	구현되었습니다	HTTPS	
		디스크 IOPs 쓰기	구현되었습니다	HTTPS	
		총 지연 시간	구현되었습니다	HTTPS	
		디스크 처리량 읽기	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	총 디스크 처리량 읽기
		디스크 처리량 쓰기	구현되었습니다	HTTPS	
		IP 처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	총 IP 처리량
		ipThroughput.wri te입니다	구현되었습니다	HTTPS	
		총 메모리 사용률	구현되었습니다	HTTPS	
		swapRate.inRate	구현되었습니다	HTTPS	
		스왑 속도	구현되었습니다	HTTPS	
		총 스왑 속도	구현되었습니다	HTTPS	
	예약 대기 시간	구현되었습니다	HTTPS	예약 대기 시간 비율	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Google Compute Platform REST API를 참조하십시오	HTTPS		443		참	참	참	참

맨 위로

# HDS HCP(HTTPS)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
Hitachi 콘텐츠 플랫폼	9.3.7.2 9.5.0.121입니다

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
820					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?
제품	스토리지 노드 범주	이름	구현되었습니다	HTTPS	추가 정보
		피처/속성 UUID입니다	구현되었습니다	사용되는 프로토콜입니다	
	스토리지 풀	DWh 용량에 포함	구현되었습니다	HTTPS	ACQ에서 Cotnrol까지, DWH 용량에서는 스트로지 풀이 흥미롭습니다
		이름	구현되었습니다	HTTPS	
		물리적 디스크 용량(MB)	구현되었습니다	HTTPS	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	HTTPS	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	HTTPS	가용 용량을 물리적 용량으로 변환하는 비율입니다
		소프트 제한값(MB)	구현되었습니다	HTTPS	볼륨 생성 또는 크기 조정 작업 중에 정의된 논리 볼륨 크기입니다
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		씬 프로비저닝이 지원됩니다	구현되었습니다	HTTPS	이 내부 볼륨이 볼륨 계층에 대한 씬 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	HTTPS	
		사용된 총 용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능	내부 볼륨	총 오브젝트	구현되었습니다		
	스토리지	실패한 물리적 용량	구현되었습니다		
		물리적 용량	구현되었습니다		
		예비 물리적 용량	구현되었습니다		스페어 디스크의 물리적 용량 (스페어가 있는 모든 디스크의 합계)
		StoragePools 용량	구현되었습니다		
		처리량 읽기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다		
		스토리지 노드	처리량 읽기	구현되었습니다	
	총 처리량		구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
	처리량 쓰기		구현되었습니다		
	총 활용률입니다		구현되었습니다		
	StoragePool 디스크입니다	총 용량	구현되었습니다		
		사용된 용량 비율	구현되었습니다		
		용량이 프로비저닝되었습니다	구현되었습니다		
		사용된 용량	구현되었습니다		
		물리적 용량	구현되었습니다		
		용량 소프트 제한값	구현되었습니다		
		과도 커밋 용량 비율	구현되었습니다		시간 시리즈로 보고됩니다

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
HDS HCP REST API	HTTPS	HTTPS	9090		참	참	참	참

맨 위로

## HiCommand 장치 관리자

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
7.6.1	DF850MH	0983/A-H
8.7.7	DF850S를 참조하십시오	0988/H-S
8.8.1	HM800을 참조하십시오	DKC: 60-08-22
8.8.3	HM850을 참조하십시오	DKC: 60-08-65
8.8.5	P9500을 참조하십시오	DKC: 70-06-46
	RAID700	DKC: 70-06-67-00/00
	RAID800	DKC: 80-06-80
	VSP5000 을 참조하십시오	DKC: 80-06-82-00/00
	XP24000	DKC: 80-06-86-00/00
	XP7입니다	DKC: 80-06-87
		DKC: 80-06-88-00/00
		DKC: 80-06-91
		DKC: 80-06-91-00/00
		DKC: 80-06-93-00/00
		DKC: 83-05-45-40/00
		DKC: 83-05-45-60/00
		DKC: 83-05-46-60/00
		DKC: 83-05-47-60/00
		DKC: 83-05-48-40/00
		DKC: 83-05-48-60/00
		DKC: 88-08-08-60/00
		DKC: 88-08-09-60/00
		DKC: 90-08-81-00/00
		DKC: 90-08-83-00/01
		SVP: 60-08-21/00
		SVP: 60-08-54/00
		SVP: 70-06-32/00
		SVP: 70-06-51/00
		SVP: 80-06-76/02
		SVP: 80-06-78/00
		SVP: 80-06-81/00
		SVP: 80-06-82/00
		SVP: 80-06-83/00
		SVP: 80-06-86/00
		SVP: 80-06-88/00
		SVP: 83-05-49-40/00
		SVP: 83-05-49-60/00
		SVP: 83-05-50-60/00
		SVP: 83-05-51-60/00
		SVP: 83-05-52-40/00
		SVP: 83-05-52-60/00
		SVP: 88-08-10-60/00
		SVP: 88-08-11-60/00
		SVP: 90-08-81/00
		SVP: 90-08-83/00

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		유형	특	HDS XML API입니다	
제품	범주	사용된 용량	장해되었습니다	사용된 용량 API입니다	추가 정보
		가상	구현되었습니다	HDS XML API입니다	스토리지 가상화 장치입니까?
볼륨 맵	LUN을 클릭합니다	마스킹이 필요합니다	구현되었습니다	HDS XML API입니다	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HDS XML API입니다	
		스토리지 포트	구현되었습니다	HDS XML API입니다	
		이니시에이터	구현되었습니다	HDS XML API입니다	
볼륨 마스크	프로토콜 컨트롤러	스토리지 포트	구현되었습니다	HDS XML API입니다	
		이름	구현되었습니다	HDS XML API입니다	
		스토리지 풀 ID입니다	구현되었습니다	HDS XML API입니다	
볼륨 멤버	순위	실린더	구현되었습니다	HDS XML API입니다	
		용량	구현되었습니다	HDS XML API입니다	사용된 스냅샷 용량(MB)입니다
		총 물리적 용량입니다	구현되었습니다	HDS XML API입니다	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		사용된 용량	구현되었습니다	HDS XML API입니다	
		호스트 별칭	구현되었습니다	HDS XML API입니다	
		개체 유형	구현되었습니다	HDS XML API입니다	
		출처	구현되었습니다	HDS XML API입니다	
WWN 별칭	WWN입니다	구현되었습니다	HDS XML API입니다		
		구현되었습니다	HDS XML API입니다		
		구현되었습니다	HDS XML API입니다		
		구현되었습니다	HDS XML API입니다		

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		총 처리량	구현되었습니다	내보내기/CLI	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
제품	범주	피처/속성 총 IOPS	상태 구현되었습니다	사용되는 변수명입니다	
	StoragePool 디스크입니다	총 용량	구현되었습니다	내보내기/CLI	
		사용된 용량 비율	구현되었습니다	내보내기/CLI	
		용량이 프로비저닝되었습 니다	구현되었습니다	내보내기/CLI	
		사용된 용량	구현되었습니다	내보내기/CLI	
		물리적 용량	구현되었습니다	내보내기/CLI	
		용량 소프트 제한값	구현되었습니다	내보내기/CLI	
		과도 커밋 용량 비율	구현되었습니다	내보내기/CLI	시간 시리즈로 보고됩니다
	볼륨	총 지연 시간	구현되었습니다	내보내기/CLI	
		IOPS 읽기	구현되었습니다	내보내기/CLI	디스크의 읽기 IOPS 수입니다
		읽기 지연 시간	구현되었습니다	내보내기/CLI	
		읽기 캐시 적중률입니다	구현되었습니다	내보내기/CLI	
		IOPS 쓰기	구현되었습니다	내보내기/CLI	
		총 캐시 적중률입니다	구현되었습니다	내보내기/CLI	
		캐시 적중률 쓰기	구현되었습니다	내보내기/CLI	
		처리량 읽기	구현되었습니다	내보내기/CLI	
		처리량 쓰기	구현되었습니다	내보내기/CLI	
		총 처리량	구현되었습니다	내보내기/CLI	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		총 IOPS	구현되었습니다	내보내기/CLI	
	지연 시간 쓰기	구현되었습니다	내보내기/CLI		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
내보내기 유틸리티(U SPV)/SNM CLI(AMS)	내보내기/C LI				거짓	거짓	거짓	거짓



API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
HiCommand 장치 관리자 XML API	HDS XML API입니다	HTTP/HTTPS	2001년		참	참	참	참

맨 위로

## Hitachi Ops 센터

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
VSP 5100입니다	80-06-92-00/00:01-65-03/05
VSP 5500	83-05-46-60/00:01-65-03/05
VSP F1500을 참조하십시오	83-05-47-40/00:01-65-03/05
VSP F600 을 참조하십시오	83-05-48-40/00:01-65-03/05
VSP G800을 참조하십시오	90-08-81-00/00:01-65-03/05
	90-08-82-00/00:01-65-2005년 3월

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		프로토콜 컨트롤러	구현되었습니다		
제품	범주	스토리지 포트 피처/속성 유형	구현되었습니다 상태 틈	사용되는 프로토콜입니다	추가 정보
		볼륨 마스크	이니시에이터		
		프로토콜 컨트롤러	구현되었습니다		
		스토리지 포트 유형	구현되었습니다 틈		



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
846					

제품	범주	피처/속성 총 IOPS	상태 구현되었습니다	사용되는 프로토콜입니다	읽기 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	StoragePool 디스크입니다	총 용량	구현되었습니다		
		사용된 용량 비율	구현되었습니다		
		용량이 프로비저닝되었습 니다	구현되었습니다		
		사용된 용량	구현되었습니다		
		물리적 용량	구현되었습니다		
		용량 소프트 제한값	구현되었습니다		
		과도 커밋 용량 비율	구현되었습니다		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시 오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Hitachi Ops Center REST API를 사용할 수 있습니다	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## HDS HNAS(CLI)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
G600을 참조하십시오	13.9.6918.05
G800을 참조하십시오	14.5.7413.01
HNAS 4080을 참조하십시오	14.6.7520.04
HNAS 4100	
N800을 참조하십시오	

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
848					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



		메모리 크기	틈	SSH를 클릭합니다	장치 메모리(MB)
제품	범주	픽처 생성 수	장해되었습니다	SSH를 클릭합니다	장치 정보
	스토리지 풀	스토리지 풀 ID입니다	구현되었습니다	SSH를 클릭합니다	
		이름	구현되었습니다	SSH를 클릭합니다	
		유형	틈	SSH를 클릭합니다	
		신 프로비저닝이 지원됩니다	구현되었습니다	SSH를 클릭합니다	이 내부 볼륨이 볼륨 계층에 대한 신 프로비저닝을 지원하는지 여부
		DWh 용량에 포함	구현되었습니다	SSH를 클릭합니다	ACQ에서 Cotnrol까지, DWH 용량에서는 스트로지 풀이 흥미롭습니다
		중복 제거가 설정되었습니다	구현되었습니다	SSH를 클릭합니다	스토리지 풀에 중복 제거가 설정되어 있는지 여부
		가상	구현되었습니다	SSH를 클릭합니다	스토리지 가상화 장치입니까?
		RAID 그룹	구현되었습니다	SSH를 클릭합니다	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		사용된 스냅샷 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 데이터 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 총 용량입니다	구현되었습니다	SSH를 클릭합니다	총 용량 (MB)입니다
		할당된 총 용량입니다	구현되었습니다	SSH를 클릭합니다	
		원시 대 가용 비율	구현되었습니다	SSH를 클릭합니다	가용 용량을 물리적 용량으로 변환하는 비율입니다

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
HDS HNAS CLI를 참조하십시오	SSH를 클릭합니다	SSH를 클릭합니다	22		참	참	참	참

맨 위로

## HPE Nimble/Alletra 6000 스토리지

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
V1	6030 AF1000 AF20Q AF3000을 참조하십시오 AF40을 참조하십시오 AF5000을 참조하십시오 CS1000입니다 CS300을 참조하십시오 CS3000을 참조하십시오 CS500을 참조하십시오 CS5000을 참조하십시오 HF20을 참조하십시오 HF20H를 참조하십시오 HF40을 참조하십시오 HF60을 참조하십시오	5.0.10.0-742719-OPT 5.0.7.0-604814-OPT 5.0.8.0-677726-OPT 5.2.1.1000-1017822-OPT 5.2.1.400-796142-선택 5.2.1.600-841103-옵션 5.2.1.700-882343-OPT 5.2.1.800-930936-OPT 5.2.1.900-1003439-OPT 6.0.0.300-956221 - 옵션 6.0.0.400-991061-OPT 6.1.1.200-1020304-옵션 6.1.1.300-1028597-OPT

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
856					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다 추가 정보
		사용된 총 용량입니다 피처/속성 유형	상태 틈	사용되는 프로토콜입니다	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?
	볼륨	용량	구현되었습니다	HTTPS	사용된 스냅샷 용량(MB)입니다
		이름	구현되었습니다	HTTPS	
		총 물리적 용량입니다	구현되었습니다	HTTPS	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		이중화	구현되었습니다	HTTPS	이중화 레벨
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		싌 프로비저닝되었습 니다	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
		UUID입니다	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?
		압축 활성화	구현되었습니다	HTTPS	
		암호화	구현되었습니다	HTTPS	
		볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS
	마스킹이 필요합니다		구현되었습니다	HTTPS	
	프로토콜 컨트롤러		구현되었습니다	HTTPS	
	스토리지 포트		구현되었습니다	HTTPS	
	유형		틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	WWN 별칭	호스트 별칭	구현되었습니다	HTTPS	
		개체 유형	구현되었습니다	HTTPS	
		출처	구현되었습니다	HTTPS	
		WWN입니다	구현되었습니다	HTTPS	



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	평균 디스크 성능 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	볼륨	물리적 용량	구현되었습니다	HTTPS	
		총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		사용된 용량 비율	구현되었습니다	HTTPS	
		총 압축 절감액	구현되었습니다	HTTPS	
		압축 절약 공간	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	HTTPS	
		IOPS 쓰기	구현되었습니다	HTTPS	
		읽기 지연 시간	구현되었습니다	HTTPS	
		총 지연 시간	구현되었습니다	HTTPS	
		지연 시간 쓰기	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
HP Nimble REST API입니다	HTTPS	HTTPS	5392		참	거짓	참	참

맨 위로

## Huawei OceanStor(REST/HTTPS)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
5300 V5	V300R001C01을 참조하십시오
5500 V3	V300R002C10
5500 V5	V300R006C20을 참조하십시오
5800 V3	V300R006C50입니다
도라도 5000 V6 SAS	V500R007C10
도라도 6000 V3	V500R007C30을 참조하십시오
Dorado 6000 V6 NVMe를 지원합니다	V600R003C00입니다
	V600R005C03을 참조하십시오

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		용량입니다			(MB)입니다
		유형	틈	HTTPS	
제품	범주	파서/속성	공해되었습니다	사용되는 프로토콜입니다	추요량만 가상화 장치입니까?
	볼륨	용량	구현되었습니다	HTTPS	사용된 스냅샷 용량(MB)입니다
		접합 경로	구현되었습니다	HTTPS	
		이름	구현되었습니다	HTTPS	
		총 물리적 용량입니다	구현되었습니다	HTTPS	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		이중화	구현되었습니다	HTTPS	이중화 레벨
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		씬 프로비저닝되었습니다	구현되었습니다	HTTPS	
		UUID입니다	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	총 IOPS	구현되었습니다	HTTPS	
		지연 시간 쓰기 피치/속성	구현되었습니다	HTTPS	추가 정보
		총 활용률입니다	구현되었습니다	사용되는 프로토콜입니다	
볼륨	읽기 캐시 적중률입니다	구현되었습니다	HTTPS		
	총 캐시 적중률입니다	구현되었습니다	HTTPS		
	캐시 적중률 쓰기	구현되었습니다	HTTPS		
	물리적 용량	구현되었습니다	HTTPS		
	총 용량	구현되었습니다	HTTPS		
	사용된 용량	구현되었습니다	HTTPS		
	사용된 용량 비율	구현되었습니다	HTTPS		
	IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다	
	총 IOPS	구현되었습니다	HTTPS		
	IOPS 쓰기	구현되었습니다	HTTPS		
	읽기 지연 시간	구현되었습니다	HTTPS		
	총 지연 시간	구현되었습니다	HTTPS		
	지연 시간 쓰기	구현되었습니다	HTTPS		
	처리량 읽기	구현되었습니다	HTTPS		
	총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)	
	처리량 쓰기	구현되었습니다	HTTPS		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Huawei OceanStor REST API	HTTPS	HTTPS	8088		참	참	참	참
Huawei OceanStor 성능 REST API	HTTPS	HTTPS	8088		참	거짓	참	참

맨 위로

# IBM Cleversafe

---

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
876					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		UUID입니다	구현되었습니다	HTTPS	
제품	범주	버전 피쳐/속성 관리 페이지 주소	구현되었습니다 상태 구현되었습니다	HTTPS 사용되는 프로토콜입니다	소프트웨어 버전 추가 정보
		스토리지 풀	DWh 용량에 포함	구현되었습니다	HTTPS
		이름	구현되었습니다	HTTPS	
		물리적 디스크 용량(MB)	구현되었습니다	HTTPS	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	HTTPS	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	HTTPS	가용 용량을 물리적 용량으로 변환하는 비율입니다
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		씬 프로비저닝이 지원됩니다	구현되었습니다	HTTPS	이 내부 볼륨이 볼륨 계층에 대한 씬 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	HTTPS	
		사용된 총 용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
IBM Cleversafe REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

# IBM DS 8K(DSCLI)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
2107-951 을 참조하십시오	7.6.31.4250
2107-961 을 참조하십시오	7.51.1400
2107-985 를 참조하십시오	7.8.57.18
2107-996 을 참조하십시오	7.9.21.91
	7.9.32.126

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		용량입니다			(MB)입니다
		유형	틈	DSNI	
제품	범주	과처/속성	궁해되었습니다	DSNI는 사용되는 프로토콜입니다	추요량과 가상화 장치입니까?
	볼륨	용량	구현되었습니다	DSNI	사용된 스냅샷 용량(MB)입니다
		디스크 유형	사용할 수 없습니다	DSNI	
		접합 경로	구현되었습니다	DSNI	
		이름	구현되었습니다	수동 입력	
		총 물리적 용량입니다	구현되었습니다	DSNI	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		스토리지 풀 ID입니다	구현되었습니다	DSNI	
		씬 프로비저닝되었습니다	구현되었습니다	DSNI	
		유형	틈	DSNI	
		사용된 용량	구현되었습니다	DSNI	
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	DSNI	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	DSNI	
		스토리지 포트	구현되었습니다	DSNI	
	볼륨 마스크	이니시에이터	구현되었습니다	DSNI	
		프로토콜 컨트롤러	구현되었습니다	DSNI	
		스토리지 포트	구현되었습니다	DSNI	
	WWN 별칭	호스트 별칭	구현되었습니다	DSNI	
		호스트 OS입니다	구현되었습니다	DSNI	
		개체 유형	구현되었습니다	DSNI	
		출처	구현되었습니다	DSNI	
		WWN입니다	구현되었습니다	DSNI	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	읽기 사용률	구현되었습니다	DSNI	
		총 활용률입니다 피처/속성 사용률 쓰기	구현되었습니다 상태 구현되었습니다	DSNI 사용되는 DSNI DSNI	추가 정보
볼륨		읽기 캐시 적중률입니다	구현되었습니다	DSNI	
		총 캐시 적중률입니다	구현되었습니다	DSNI	
		캐시 적중률 쓰기	구현되었습니다	DSNI	
		물리적 용량	구현되었습니다	DSNI	
		총 용량	구현되었습니다	DSNI	
		IOPS 읽기	구현되었습니다	DSNI	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	DSNI	
		IOPS 쓰기	구현되었습니다	DSNI	
		읽기 지연 시간	구현되었습니다	DSNI	
		총 지연 시간	구현되었습니다	DSNI	
		지연 시간 쓰기	구현되었습니다	DSNI	
		처리량 읽기	구현되었습니다	DSNI	
		총 처리량	구현되었습니다	DSNI	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	DSNI	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
데이터 소스 마법사 구성	수동 입력				참	참	참	참
IBM DS CLI를 참조하십시오	DSNI	DSNI			참	참	참	참

맨 위로

## IBM PowerVM(SSH)

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		가상디스크 OID	구현되었습니다	SSH를 클릭합니다	
제품	범주	가상 Machine OID입니다	구현되었습니다	SSH를 클릭합니다	추가 정보
	호스트	호스트 CPU 수입니다	구현되었습니다	SSH를 클릭합니다	
		호스트가 메모리를 설치했습니다	구현되었습니다	SSH를 클릭합니다	
		호스트 모델	구현되었습니다	SSH를 클릭합니다	
		NIC 수	구현되었습니다	SSH를 클릭합니다	
		IPS	구현되었습니다	SSH를 클릭합니다	
		제조업체	구현되었습니다	SSH를 클릭합니다	
		이름	구현되었습니다	SSH를 클릭합니다	
		OID	구현되었습니다	SSH를 클릭합니다	
		플랫폼 유형	구현되었습니다	SSH를 클릭합니다	
	정보	데이터 원본 이름	구현되었습니다	SSH를 클릭합니다	정보
		날짜	구현되었습니다	SSH를 클릭합니다	
		개시자 ID	구현되었습니다	SSH를 클릭합니다	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
IBM Hardware Management Console SSH 액세스	SSH를 클릭합니다	SSH를 클릭합니다	22		참	거짓	참	참

맨 위로

## IBM SVC(CLI)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
2072-12F	1.5.2.7
2072-12G	1.6.1.2
2072-2N4를 참조하십시오	1.6.1.4
2072-324	1.6.1.5
2072-3H4	7.5.0.11
2072-3N4를 참조하십시오	7.5.0.12
2076-124 를 참조하십시오	7.7.1.8 을 참조하십시오
2076-12F	7.8.1.14
2076-224 를 참조하십시오	7.8.1.6
2076-24F	7.8.1.8
2076-24G	8.2.1.10
2076-624 를 참조하십시오	8.2.1.11
2076-724 를 참조하십시오	8.2.1.14
2076-824 를 참조하십시오	8.2.1.9
2076-AF6	8.3.1.1
2076-AFF	8.3.1.2
2077-24F	8.3.1.5
2077-424 를 참조하십시오	8.3.1.6
2078-12F	8.3.1.7
2078-224 를 참조하십시오	8.3.1.9
2078-24C	8.4.0.10입니다
2078-24F	8.4.0.11입니다
2078-324 를 참조하십시오	8.4.0.6
2078-424 를 참조하십시오	8.4.0.7
2078-4H4	8.4.0.8
2078-92G	8.4.0.9.에서 다시 시작합니다
2078-AF3	8.5.0.5
4657-924 를 참조하십시오	8.5.0.6.6을 참조하십시오
4662-12G	8.5.0.7
4662-6H2	8.5.0.8
4666-AH8을 참조하십시오	8.5.0.9입니다
9843-AE2	8.5.2.2
9843-AE3	8.5.3.1
9846-AG8	8.5.4.0
9848-AE2	
9848-AF7	
9848-AF8	
9848-AG8	
서비스	

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		스킨 응용	구현되었습니다	SSH를 클릭합니다	호스트가 이 볼륨에 쓴 총 용량(MB)입니다
제품	범주	압축/활성화	장해되었습니다	SSH를 클릭합니다	추가 정보
		암호화	구현되었습니다	SSH를 클릭합니다	
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	SSH를 클릭합니다	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	SSH를 클릭합니다	
		스토리지 포트	구현되었습니다	SSH를 클릭합니다	
	볼륨 마스크	이니시에이터	구현되었습니다	SSH를 클릭합니다	
		프로토콜 컨트롤러	구현되었습니다	SSH를 클릭합니다	
		스토리지 포트	구현되었습니다	SSH를 클릭합니다	
		유형	틈	SSH를 클릭합니다	
	WWN 별칭	호스트 별칭	구현되었습니다	SSH를 클릭합니다	
		개체 유형	구현되었습니다	SSH를 클릭합니다	
		출처	구현되었습니다	SSH를 클릭합니다	
		WWN입니다	구현되었습니다	SSH를 클릭합니다	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
900					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		총 활용률입니다	구현되었습니다	SSH를 클릭합니다	
제품	범주	파워 사용률 쓰기	장해되었습니다	SSH를 클릭합니다	추가 정보
	볼륨	읽기 캐시 적중률입니다	구현되었습니다	SSH를 클릭합니다	
		총 캐시 적중률입니다	구현되었습니다	SSH를 클릭합니다	
		캐시 적중률 쓰기	구현되었습니다	SSH를 클릭합니다	
		물리적 용량	구현되었습니다	SSH를 클릭합니다	
		총 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 용량	구현되었습니다	SSH를 클릭합니다	
		쓰인 용량	구현되었습니다	SSH를 클릭합니다	
		사용된 용량 비율	구현되었습니다	SSH를 클릭합니다	
		기록된 용량 비율	구현되었습니다	SSH를 클릭합니다	
		IOPS 읽기	구현되었습니다	SSH를 클릭합니다	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	SSH를 클릭합니다	
		IOPS 쓰기	구현되었습니다	SSH를 클릭합니다	
		읽기 지연 시간	구현되었습니다	SSH를 클릭합니다	
		총 지연 시간	구현되었습니다	SSH를 클릭합니다	
		지연 시간 쓰기	구현되었습니다	SSH를 클릭합니다	
		처리량 읽기	구현되었습니다	SSH를 클릭합니다	
		총 처리량	구현되었습니다	SSH를 클릭합니다	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	SSH를 클릭합니다	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
IBM SVC CLI를 참조하십시오	SSH를 클릭합니다	SSH를 클릭합니다	22		참	거짓	참	참

맨 위로

## IBM XIV 및 A9000(XIVCLI)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
415 A14를 참조하십시오	10.2.4.e 12.3.2.c

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
906					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		유형	특	XIV CLI	
제품	범주	사용된 용량 피치/속성 압축 활성화	구현되었습니다 상태 구현되었습니다	XIV CLI 사용되는 정보를 제공합니다	추가 정보
		볼륨 맵	LUN을 클릭합니다	구현되었습니다	XIV CLI
		프로토콜 컨트롤러	구현되었습니다	XIV CLI	
	볼륨 마스크	이니시에이터	구현되었습니다	XIV CLI	
		프로토콜 컨트롤러	구현되었습니다	XIV CLI	
	WWN 별칭	호스트 별칭	구현되었습니다	XIV CLI	
		호스트 OS입니다	구현되었습니다	XIV CLI	
		개체 유형	구현되었습니다	XIV CLI	
		출처	구현되었습니다	XIV CLI	
		WWN입니다	구현되었습니다	XIV CLI	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

		사용된 용량	구현되었습니다	DSNI	
		물리적 용량	구현되었습니다	DSNI	
제품	범주	파괴/삭제 용량 비율	장해되었습니다	DSNI는 사용되는 프로토콜입니다	취급 정백으로 보고됩니다
	볼륨	총 지연 시간	구현되었습니다	DSNI	
		읽기 지연 시간	구현되었습니다	DSNI	
		IOPS 쓰기	구현되었습니다	DSNI	
		압축 절약 공간	구현되었습니다	DSNI	
		처리량 읽기	구현되었습니다	DSNI	
		총 IOPS	구현되었습니다	DSNI	
		지연 시간 쓰기	구현되었습니다	DSNI	
		IOPS 읽기	구현되었습니다	DSNI	디스크의 읽기 IOPS 수입니다
		읽기 캐시 적중률입니다	구현되었습니다	DSNI	
		총 압축 절감액	구현되었습니다	DSNI	
		총 캐시 적중률입니다	구현되었습니다	DSNI	
		캐시 적중률 쓰기	구현되었습니다	DSNI	
		처리량 쓰기	구현되었습니다	DSNI	
		총 처리량	구현되었습니다	DSNI	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
IBM DS CLI를 참조하십시오	DSNI	DSNI			참	참	참	참
IBM XIV CLI	XIV CLI	TCP	7778		참	거짓	참	거짓

맨 위로

## Infinidat(HTTP)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
F6230 F6240을 참조하십시오 F6303)을 참조하십시오 F6304를 참조하십시오	6.0.31.0 7.0.14.20

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		용량입니다			(MB)입니다
		유형	틈	HTTPS	
제품	범주	좌측/속성	공해되었습니다	좌측은 프로토콜입니다	추가요청 가상화 장치입니까?
	볼륨	이름	구현되었습니다	HTTPS	
		접합 경로	구현되었습니다	HTTPS	
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		UUID입니다	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?
		스핀 프로비저닝되었습니다	구현되었습니다	HTTPS	
		복제본 소스	구현되었습니다	HTTPS	
		복제 타겟	구현되었습니다	HTTPS	
		스냅샷	구현되었습니다	HTTPS	
		용량	구현되었습니다	HTTPS	사용된 스냅샷 용량(MB)입니다
		총 물리적 용량입니다	구현되었습니다	HTTPS	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		사용된 용량	구현되었습니다	HTTPS	
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
	WWN 별칭	출처	구현되었습니다	HTTPS	
		호스트 별칭	구현되었습니다	HTTPS	
		WWN입니다	구현되었습니다	HTTPS	
		개체 유형	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Infinidat REST API를 참조하십시오	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## Microsoft Azure 컴퓨팅

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전
2018년 6월 1일

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
922					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		제조업체	구현되었습니다	HTTPS	
제품	범주	이름	구현되었습니다	HTTPS	추가 정보
		피처/속성 OID	상태 구현되었습니다	사용되는 프로토콜입니다	
	정보	API 설명	구현되었습니다	HTTPS	
		API 이름	구현되었습니다	HTTPS	
		API 버전	구현되었습니다	HTTPS	
		데이터 원본 이름	구현되었습니다	HTTPS	정보
		날짜	구현되었습니다	HTTPS	
		개시자 ID	구현되었습니다	HTTPS	
		발신자 키	구현되었습니다	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능	데이터 저장소	용량이 프로비저닝되었습 니다	구현되었습니다	HTTPS	
		총 용량	구현되었습니다	HTTPS	
		과도 커밋 용량 비율	구현되었습니다	HTTPS	시간 시리즈로 보고됩니다
	가상 디스크	총 용량	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	HTTPS	
		IOPS 쓰기	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	HTTPS	
	VM	총 CPU 사용률	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		disklops.total	구현되었습니다	HTTPS	
		디스크 IOPs 쓰기	구현되었습니다	HTTPS	
		디스크 처리량 읽기	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	총 디스크 처리량 읽기
		디스크 처리량 쓰기	구현되었습니다	HTTPS	
		IP 처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	총 IP 처리량
		ipThroughput.wri te입니다	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:



API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Microsoft Azure 컴퓨팅 REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## Microsoft Hyper-V를 참조하십시오

---

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		가상디스크 OID	구현되었습니다	WMI를 선택합니다	
제품	범주	가상 Machine OID입니다	구현되었습니다	WMI를 선택합니다	추가 정보
	호스트	호스트 CPU 수입니다	구현되었습니다	WMI를 선택합니다	
		호스트 CPU 속도	구현되었습니다	WMI를 선택합니다	
		호스트 도메인	구현되었습니다	WMI를 선택합니다	
		호스트가 메모리를 설치했습니다	구현되었습니다	WMI를 선택합니다	
		호스트 모델	구현되었습니다	WMI를 선택합니다	
		NIC 수	구현되었습니다	WMI를 선택합니다	
		NIC 속도	구현되었습니다	WMI를 선택합니다	
		IPS	구현되었습니다	WMI를 선택합니다	
		제조업체	구현되었습니다	WMI를 선택합니다	
		이름	구현되었습니다	WMI를 선택합니다	
		OID	구현되었습니다	WMI를 선택합니다	
		플랫폼 유형	구현되었습니다	WMI를 선택합니다	
		iSCSI 노드	호스트 별칭	구현되었습니다	WMI를 선택합니다
	노드 이름		구현되었습니다	WMI를 선택합니다	
	OID		구현되었습니다	WMI를 선택합니다	
	유형		틈	WMI를 선택합니다	
	정보	데이터 원본 이름	구현되었습니다	WMI를 선택합니다	정보
		날짜	구현되었습니다	WMI를 선택합니다	
		개시자 ID	구현되었습니다	WMI를 선택합니다	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

				WS-Management(W S 관리)	디스크에서 읽기 및 쓰기)(MB/s)
제품	범주	처리량 쓰기 피쳐/속성	구현되었습니다	WS-Management(W S 관리)입니다	추가 정보
		총 용량	구현되었습니다	WS-Management(W S 관리)	
	VM	사용된 용량	구현되었습니다	WS-Management(W S 관리)	
		사용된 용량 비율	구현되었습니다	WS-Management(W S 관리)	
		총 CPU 사용률	구현되었습니다	WS-Management(W S 관리)	
		IOPS 읽기	구현되었습니다	WS-Management(W S 관리)	디스크의 읽기 IOPS 수입니다
		disklops.total	구현되었습니다	WS-Management(W S 관리)	
		디스크 IOPs 쓰기	구현되었습니다	WS-Management(W S 관리)	
		총 지연 시간	구현되었습니다	WS-Management(W S 관리)	
		디스크 처리량 읽기	구현되었습니다	WS-Management(W S 관리)	
		처리량 읽기	구현되었습니다	WS-Management(W S 관리)	총 디스크 처리량 읽기
		디스크 처리량 쓰기	구현되었습니다	WS-Management(W S 관리)	
		IP 처리량 읽기	구현되었습니다	WS-Management(W S 관리)	
		총 처리량	구현되었습니다	WS-Management(W S 관리)	총 IP 처리량
		ipThroughput.write입니다	구현되었습니다	WS-Management(W S 관리)	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
PowerShell을 사용합니다	WS-Management(WS 관리)	HTTP	5985입니다		참	거짓	거짓	참
WMI를 선택합니다	WMI를 선택합니다	WMI를 선택합니다	135번		참	거짓	참	참

맨 위로

## NetApp 7 모드

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
1.12	FAS2040	7.3.6
1.14	FAS2050	8.1.1 7-Mode
1.17	FAS2220	8.1.3P2 7-Mode(8.1.3P2 7-모드)
1.19	냉각 아키텍처	8.1.4P1 7-Mode(8.1.4P1 7-Mode)
1.20	FAS2240-4	8.1.4P10 7-Mode
1.21	FAS2520	8.1.4P9D18 7-Mode
	FAS2554	8.2.1 7-Mode
	FAS3140	8.2.2 7-Mode
	FAS3160	8.2.3 7-Mode
	FAS3210	8.2.3P2 7-Mode
	FAS3220	8.2.3P3 7-Mode
	FAS3240	8.2.4 7-Mode
	FAS3250	8.2.4P2 7-Mode
	FAS3270	8.2.4P4 7-Mode의 약어입니다
	FAS6240	8.2.4P5 7-Mode를 참조하십시오
	함께 사용 가능	8.2.4P6 7-Mode를 참조하십시오
	FAS8020	8.2.5 7-Mode
	FAS8040	8.2.5P1 7-Mode의 약어입니다
	FAS8060	8.2.5P2 7-Mode
	FAS8080	8.2.5P4 7-Mode의 약어입니다
	N6070 을 참조하십시오	8.2.5P5 7-Mode
	N6240	8.2P3 7-Mode(8.2P3 7-모드)
	V3240을 참조하십시오	8.2P4 7-Mode의 약어입니다
		Data ONTAP 릴리즈 7.3.3
		Data ONTAP 릴리즈 7.3.4
		Data ONTAP 릴리즈 8.2.5 7-Mode

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

	볼륨 맵	LUN을 클릭합니다	구현되었습니다		백엔드 LUN의 이름입니다
제품	범주	프로토콜 컨트롤러 피처/속성 유형	구현되었습니다 상태 틈	사용되는 프로토콜입니다	추가 정보
		볼륨 마스크	이니시에이터	구현되었습니다	
		프로토콜 컨트롤러	구현되었습니다		
		스토리지 포트	구현되었습니다		
		유형	틈		

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		읽기 사용률	구현되었습니다		
제품	범주	총 활용률입니다	구현되었습니다	사용되는 프로토콜입니다	추가 정보
		피처/속성 사용률 쓰기	상태 구현되었습니다		
	볼륨	물리적 용량	구현되었습니다		
		총 용량	구현되었습니다		
		사용된 용량	구현되었습니다		
		사용된 용량 비율	구현되었습니다		
		IO 밀도 읽기	구현되었습니다		
		총 IO 밀도	구현되었습니다		
		쓰기 IO 밀도	구현되었습니다		
		IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다		
		IOPS 쓰기	구현되었습니다		
		읽기 지연 시간	구현되었습니다		
		총 지연 시간	구현되었습니다		
		지연 시간 쓰기	구현되었습니다		
		부분 차단된 비율	구현되었습니다		
		처리량 읽기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다		
		쓰기 보류 중	구현되었습니다		총 쓰기 보류 중

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시 오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
NetApp 7 모드 ZAPI	없습니다	없습니다			참	참	참	참

맨 위로

## NetApp Cloud Volumes Service를 참조하십시오

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
AWS 클라우드 볼륨	V1

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	장애가 발생한 디스크의 물리적 용량(장애가 발생한 모든 디스크의 합계)
	스토리지 풀	스토리지 풀 ID입니다	구현되었습니다		
		이름	구현되었습니다		
		유형	틈		
		씬 프로비저닝이 지원됩니다	구현되었습니다		이 내부 볼륨이 볼륨 계층에 대한 씬 프로비저닝을 지원하는지 여부
		DWh 용량에 포함	구현되었습니다		ACQ에서 Control까지, DWH 용량에서는 스토리지 풀이 흥미롭습니다
		가상	구현되었습니다		스토리지 가상화 장치입니까?
		RAID 그룹	구현되었습니다		이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		사용된 스냅샷 용량	구현되었습니다		
		사용된 데이터 용량	구현되었습니다		
		데이터 할당 용량	틈		데이터에 할당된 용량입니다
		사용된 총 용량입니다	구현되었습니다		총 용량 (MB)입니다
		할당된 총 용량입니다	구현되었습니다		
		물리적 디스크 용량(MB)	구현되었습니다		스토리지 풀의 물리적 용량으로 사용됩니다
		원시 대 가용 비율	구현되었습니다		가용 용량을 물리적 용량으로 변환하는 비율입니다

이 데이터 수집기에서 사용하는 관리 API:

<b>API</b> 를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Cloud Volumes Service REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## NetApp ONTAP용 Amazon FSx

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
ONTAP용 FSX	Data ONTAP

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

	VirtualMachine 내부 볼륨 참조	각각의 볼륨 ID입니다	구현되었습니다	HTTPS	
제품	VirtualMachine StoragePool LREF	스토리지 풀 ID입니다	구현되었습니다 상태	HTTPS 사용되는 프로토콜입니다	추가 정보
	VirtualMachine 볼륨 참조입니다	볼륨 이름	구현되었습니다	HTTPS	
	볼륨	용량	구현되었습니다	HTTPS	사용된 스냅샷 용량(MB)입니다
		디스크 그룹	구현되었습니다	HTTPS	디스크 그룹 유형입니다
		접합 경로	구현되었습니다	HTTPS	
		마지막으로 알려진 액세스 시간입니다	구현되었습니다	HTTPS	볼륨에 대한 마지막 액세스 권한
		이름	구현되었습니다	HTTPS	
		qtree ID입니다	구현되었습니다	HTTPS	qtree의 고유 ID입니다
		총 물리적 용량입니다	구현되었습니다	HTTPS	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		실패 프로비저닝되었습니다	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
		UUID입니다	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		암호화	구현되었습니다	HTTPS	
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능	스토리지	오류 발생 디스크	구현되었습니다	HTTPS	
	스토리지 노드	총 캐시 적중률입니다	구현되었습니다	HTTPS	
		총 디스크 읽기 교체됨	구현되었습니다	HTTPS	
		총 활용률입니다	구현되었습니다	HTTPS	
	qtree를 입력합니다		구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
NetApp ONTAP API를 참조하십시오	HTTP/HTTPS	HTTP/HTTPS	80/443		참	참	참	참

[맨 위로](#)

## NetApp clustered Data ONTAP 8.1.1 이상

이 데이터 수집기에서 지원하는 모델 및 버전:





모델	펌웨어 버전입니다
AFF-A150 을 참조하십시오	8.2.3P5
AFF-A200	8.3.0
AFF-A220	8.3.1로 업그레이드하기
AFF-A250	8.3.1P2
AFF-A300	8.3.2
AFF-A320을 참조하십시오	8.3.2P12
AFF-A400, 즉	8.3.2P2 를 참조하십시오
AFF-A700	8.3.2P5
AFF-A700s	9.0.1
AFF-A800	9.1.0
AFF-A900	9.1.0P1
AFF-C190 를 참조하십시오	9.1.0P10
AFF-C250을 참조하십시오	9.1.0P11
AFF-C400 을 참조하십시오	9.1.0P12
AFF-C800을 참조하십시오	9.1.0P14
AFF8020	9.1.0P15
AFF8040	9.1.0P17
AFF8060	9.1.0P19
AFF8080	9.1.0P20
CDvM100을 참조하십시오	9.1.0P5
CDvM200을 참조하십시오	9.1.0P7
DM5000H를 참조하십시오	9.1.0P8
냉각 아키텍처	9.10.0
FAS2240-4	9.10.1
FAS2520	9.10.1P1
FAS2552	9.10.1P10
FAS2554	9.10.1P11
FAS2620	9.10.1P12
FAS2650	9.10.1P13
FAS2720	9.10.1P2
FAS2750	9.10.1P3입니다
FAS3220	9.10.1P4
FAS3250	9.10.1P5
FAS3270	9.10.1P6
500f로 설정합니다	9.10.1P7
FAS6210 을 참조하십시오	9.10.1P8
FAS6220	9.10.1P9
FAS8020	9.11.0P1
FAS8040	9.11.1
FAS8060	9.11.1P1
FAS8080	10월 11일
FAS8200	9.11.1P2
FAS8300	9.11.1P3입니다
FAS8700	9.11.1P4
FAS9000	9.11.1P5
FAS9500	9.11.1P6
FASDvM300	9.11.1P7
SIMBOX를 참조하십시오	9.11.1P8
V6240	9.11.1P9
	9.11.1X12
	9.11.1X26
	9.12.1
	9.12.1P1
	9.12.1P2

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		QoS Limit Raw(QoS 제한 원시 피치/속성 QoS - 정책	구현되었습니다	HTTPS	
제품	범주		상태 구현되었습니다	사용되는 프로토콜입니다	추가 정보
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	평균 디스크 성능 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	볼륨	물리적 용량	구현되었습니다	HTTPS	
		총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		사용된 용량 비율	구현되었습니다	HTTPS	
		IO 밀도 읽기	구현되었습니다	HTTPS	
		총 IO 밀도	구현되었습니다	HTTPS	
		쓰기 IO 밀도	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	HTTPS	
		IOPS 쓰기	구현되었습니다	HTTPS	
		읽기 지연 시간	구현되었습니다	HTTPS	
		총 지연 시간	구현되었습니다	HTTPS	
		지연 시간 쓰기	구현되었습니다	HTTPS	
		부분 차단된 비율	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
	처리량 쓰기	구현되었습니다	HTTPS		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
NetApp ONTAP API를 참조하십시오	HTTP/HTT PS	HTTP/HTT PS	80/443		참	참	참	참

맨 위로

## NetApp SolidFire 8.1 이상

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
H410S-2	11.1.0.72
H610S-2	11.5.0.63
H610S-4를 참조하십시오	11.7.0.76
SF19210	11.8.0.23
SF2405 를 참조하십시오	12.0.0.333을 참조하십시오
SF38410	12.2.0.777입니다
SF4805 를 참조하십시오	12.3.0.958
SF9605 를 참조하십시오	12.3.1.103
SF9608	12.3.1.165
FCN001 을 참조하십시오	12.3.2.3
H300S	12.5.0.897
H410S-0	12.7.0.380입니다
H410S-1	
H410S-2	
H500S를 참조하십시오	
H610S-1	
H610S-2	
H610S-4를 참조하십시오	
H610S2를 참조하십시오	
SF19210	
SF38410	
SF4805 를 참조하십시오	
SF9605 를 참조하십시오	

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1002					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		프로토콜 컨트롤러	구현되었습니다	HTTPS	
제품	범주	스토리지 포트 피처/속성 유형	구현되었습니다 상태 틈	HTTPS 사용되는 프로토콜입니다	추가 정보
		볼륨 마스크	이니시에이터	구현되었습니다	HTTPS
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트 유형	구현되었습니다 틈	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
1010					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		중복제거 절약 공간	구현되었습니다	HTTPS	
제품	범주	기타 총 용량 피쳐/속성	구현되었습니다	HTTPS	추가 정보
		기타 사용된 용량	구현되었습니다	사용되는 프로토콜입니다	
	볼륨	물리적 용량	구현되었습니다	HTTPS	
		총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		사용된 용량 비율	구현되었습니다	HTTPS	
		총 압축 절감액	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	HTTPS	
		IOPS 쓰기	구현되었습니다	HTTPS	
		읽기 지연 시간	구현되었습니다	HTTPS	
		총 지연 시간	구현되었습니다	HTTPS	
		지연 시간 쓰기	구현되었습니다	HTTPS	
		부분 차단된 비율	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	HTTPS	
	총 활용률입니다	구현되었습니다	HTTPS		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
SolidFire REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## NetApp StorageGRID(HTTPS)

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	모델	펌웨어 버전입니다
3.0	Webscale입니다	11.2.0
3.2		11.4.0
3.3		11.4.0.3
3.4		11.4.0.4
3.5		11.5.0.1
		11.5.0.11
		11.5.0.2
		11.5.0.3
		11.5.0.6.6을 참조하십시오
		11.5.0.7
		11.5.0.8
		11.5.0.9입니다
		11.6.0
		11.6.0.1
		11.6.0.10
		11.6.0.2
		11.6.0.4
		11.6.0.5
		11.6.0.7
		11.6.0.8
		11.6.0.9
		11.7.0

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1014					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		사용된 노드 용량 활용도 메타 데이터(MB)입니다	구현되었습니다	HTTPS	
제품	범주	피쳐/속성 사이트 이름	상태 구현되었습니다	사용되는 프로토콜입니다	추가 정보
		스토리지 풀	DWh 용량에 포함 구현되었습니다	HTTPS	ACQ에서 Cotnroi까지, DWH 용량에서는 스트로지 풀이 흥미롭습니다
		이름	구현되었습니다	HTTPS	
		물리적 디스크 용량(MB)	구현되었습니다	HTTPS	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	HTTPS	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	HTTPS	가용 용량을 물리적 용량으로 변환하는 비율입니다
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		싌 프로비저닝이 지원됩니다	구현되었습니다	HTTPS	이 내부 볼륨이 볼륨 계층에 대한 싌 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	HTTPS	
		사용된 총 용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	읽기 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보	
	StoragePool 디스크입니다	용량이 프로비저닝되었습 니다	구현되었습니다			
물리적 용량		구현되었습니다			총 용량	
구현되었습니다				사용된 용량	구현되었습니다	
			과도 커밋 용량 비율	구현되었습니다		
시간 시리즈로 보고됩니다		사용된 용량 비율	구현되었습니다			

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
StorageG RID REST API를 참조하십시오	HTTPS	HTTPS	443		참	거짓	참	참

맨 위로

## Nutanix 스토리지(REST)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
HPE DL360-8 G10	6.5.1.6
NX-3060-G6을 참조하십시오	6.5.2
NX-3170-G6	6.5.2.5
NX-8035-G6을 참조하십시오	6.5.2.6
NX-8150-G7	6.5.2.7
HPE DL360-8 G10	6.5.3
HPE DL380-12 G10	6.5.3.1
NX-3060-G5	
NX-3170-G7	
NX-5155-G6	
NX-8035-G6을 참조하십시오	
NX-8035-G7을 참조하십시오	
NX-8150-G7	
NX-8150-G8을 참조하십시오	

이 데이터 수집기에서 지원하는 제품:





제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



		용량입니다			(MB)입니다
		유형	틈	HTTPS	
제품	범주	파싱/속성	궁해되었습니다	서버는 프로토콜입니다	추요량과 가상화 장치입니까?
	볼륨	용량	구현되었습니다	HTTPS	사용된 스냅샷 용량(MB)입니다
		접합 경로	구현되었습니다	HTTPS	
		이름	구현되었습니다	HTTPS	
		qtree ID입니다	구현되었습니다	HTTPS	qtree의 고유 ID입니다
		총 물리적 용량입니다	구현되었습니다	HTTPS	총 물리적 용량 (스토리지에 있는 모든 디스크의 합계)
		이중화	구현되었습니다	HTTPS	이중화 레벨
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		씬 프로비저닝되었습니다	구현되었습니다	HTTPS	
		UUID입니다	구현되었습니다	HTTPS	
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTPS	백엔드 LUN의 이름입니다
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	
	볼륨 마스크	이니시에이터	구현되었습니다	HTTPS	
		프로토콜 컨트롤러	구현되었습니다	HTTPS	
		스토리지 포트	구현되었습니다	HTTPS	
		유형	틈	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)		처리량 쓰기
제품	범주	피처/속성	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)	사용되는 프로토콜입니다	추가 정보
	구현되었습니다	HTTPS		볼륨	IOPS 읽기
	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다		총 IOPS
	구현되었습니다	HTTPS			IOPS 쓰기
	구현되었습니다	HTTPS			읽기 지연 시간
	구현되었습니다	HTTPS			총 지연 시간
	구현되었습니다	HTTPS			지연 시간 쓰기
	구현되었습니다	HTTPS			처리량 읽기
	구현되었습니다	HTTPS			총 처리량
	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)		처리량 쓰기

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Nutanix REST API를 참조하십시오	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## OpenStack(REST API/SSH)

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1034					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		노드 이름	구현되었습니다	HTTPS	
제품	범주	OID 피처/속성 유형	구현되었습니다 상태 틈	HTTPS 사용되는 프로토콜입니다	추가 정보
		정보	데이터 원본 이름	구현되었습니다	HTTPS
		날짜	구현되었습니다	HTTPS	
		개시자 ID	구현되었습니다	HTTPS	
		발신자 키	구현되었습니다	HTTPS	
성능	데이터 저장소	총 용량	구현되었습니다		
		사용된 용량 비율	구현되었습니다		
		용량이 프로비저닝되었습 니다	구현되었습니다		
		사용된 용량	구현되었습니다		
		과도 커밋 용량 비율	구현되었습니다		시간 시리즈로 보고됩니다
	호스트	총 CPU 사용률	구현되었습니다		
		총 메모리 사용률	구현되었습니다		
	가상 디스크	읽기 지연 시간	구현되었습니다		
		총 지연 시간	구현되었습니다		
		지연 시간 쓰기	구현되었습니다		

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시 오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
OpenStack REST API를 참조하십시 오	HTTPS	HTTPS	443		참	거짓	참	참
OpenStack SSH를 참조하십시 오	SSH를 클릭합니다	SSH를 클릭합니다	22		참	거짓	참	참

맨 위로

## Oracle ZFS(HTTPS)

이 데이터 수집기에서 지원하는 모델 및 버전:



모델	펌웨어 버전입니다
Sun ZFS Storage 7330	1-1.1
Sun ZFS Storage 7335	1-1.2
Sun ZFS Storage 7350	1-1.3
Sun ZFS Storage 7370	1-1.34
Sun ZFS Storage 7420	1-1.4
Sun ZFS Storage 7430	2013.06.05.6.12
Sun ZFS Storage 7450	2013.06.05.6.15
	2013.06.05.7.21
	2013.06.05.7.24
	2013.06.05.7.25
	2013.06.05.7.26
	2013.06.05.8.0
	2013.06.05.8.26
	2013.06.05.8.29
	2013.06.05.8.35
	2013.06.05.8.37
	2013.06.05.8.47
	2013.06.05.8.50
	2013.06.05.8.53
	2013.06.05.8.6
	2013.06.05.8.7

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		사용된 용량	구현되었습니다	HTTP/S를 참조하십시오	
제품	범주	미정확성	장해되었습니다	사용된 용량을 정확히 집계된다	취종형 백벨
	볼륨 맵	LUN을 클릭합니다	구현되었습니다	HTTP/S를 참조하십시오	백엔드 LUN의 이름입니다
		스토리지 포트	구현되었습니다	HTTP/S를 참조하십시오	
		마스킹이 필요합니다	구현되었습니다	HTTP/S를 참조하십시오	
		프로토콜 컨트롤러	구현되었습니다	HTTP/S를 참조하십시오	
		유형	틈	HTTP/S를 참조하십시오	
	볼륨 마스크	스토리지 포트	구현되었습니다	HTTP/S를 참조하십시오	
		이니시에이터	구현되었습니다	HTTP/S를 참조하십시오	
		프로토콜 컨트롤러	구현되었습니다	HTTP/S를 참조하십시오	
		유형	틈	HTTP/S를 참조하십시오	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
1048					

제품	범주	구현되었습니다 상태	구현되었습니다	사용되는 프로토콜입니다	추가 정보
		처리량 쓰기 피처/속성 총 활용률입니다	구현되었습니다		디스크에서 읽기 및 쓰기)(MB/s)
	스토리지 노드 데이터	키	구현되었습니다		
		서버 ID입니다	구현되었습니다		
		처리량 읽기	구현되었습니다		
		처리량 쓰기	구현되었습니다		
		총 처리량	구현되었습니다		평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		IOPS 읽기	구현되었습니다		디스크의 읽기 IOPS 수입니다
		IOPS 쓰기	구현되었습니다		
		총 IOPS	구현되었습니다		
		총 캐시 적중률입니다	구현되었습니다		
		총 활용률입니다	구현되었습니다		
	StoragePool 디스크입니다	총 IOPS	구현되었습니다		
		총 용량	구현되었습니다		
		사용된 용량 비율	구현되었습니다		
		총 데이터 용량	구현되었습니다		
		용량이 프로비저닝되었습 니다	구현되었습니다		
		사용된 데이터 용량	구현되었습니다		
		사용된 용량	구현되었습니다		
		기타 사용된 용량	구현되었습니다		
		물리적 용량	구현되었습니다		
		과도 커밋 용량 비율	구현되었습니다		시간 시리즈로 보고됩니다
		사용된 스냅샷 용량	구현되었습니다		
		사용된 스냅샷 용량 비율	구현되었습니다		시간 시리즈로 보고됩니다

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Oracle ZFS REST API	HTTP/HTTPS	HTTP/HTTPS	215		참	참	참	참

맨 위로

## Pure Storage FlashArray(HTTP)

이 데이터 수집기에서 지원하는 모델 및 버전:

모델	펌웨어 버전입니다
DFSC1을 참조하십시오	4.8.8
FA-420	5.3.14
FA-450입니다	5.3.15
FA-C40R3을 참조하십시오	5.3.17
FA-C60 을 참조하십시오	5.3.18
FA-C60R3을 참조하십시오	5.3.20
FA-X10R2를 참조하십시오	5.3.21
FA-X10R3을 참조하십시오	5.3.6
FA-X20R2를 참조하십시오	5.3.8
FA-X20R3을 참조하십시오	6.1.10
FA-X50R2	6.1.11
FA-X50R3을 참조하십시오	6.1.13
FA-X70R2	6.1.14
FA-X70R3을 참조하십시오	6.1.15
FA-X90R2	6.1.17
FA-X90R3을 참조하십시오	6.1.18
FA-XL130을 참조하십시오	6.1.19
FA-XL170)을 참조하십시오	6.1.21
FA-m10r2	6.1.22
FA-M20 을 참조하십시오	6.1.23
FA-m20r2	6.1.5
FA-M50	6.2.13
FA-m50r2	6.2.7
FA-M70 을 참조하십시오	6.2.9
FA-m70r2	6.3.10
FA-X70을 참조하십시오	6.3.11
	6.3.12
	6.3.2
	6.3.5
	6.3.6
	6.3.7
	6.3.9
	6.4.3
	6.4.4
	6.4.5

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1052					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		스토리지 포트	구현되었습니다	HTTP/S를 참조하십시오	
제품	범주	위형/속성	용태	사용되는 참조하십시오	추가 정보
	볼륨 마스크	이니시에이터	구현되었습니다	HTTP/S를 참조하십시오	
		프로토콜 컨트롤러	구현되었습니다	HTTP/S를 참조하십시오	
		스토리지 포트	구현되었습니다	HTTP/S를 참조하십시오	
		유형	틈	HTTP/S를 참조하십시오	
	WWN 별칭	호스트 별칭	구현되었습니다	HTTP/S를 참조하십시오	
		개체 유형	구현되었습니다	HTTP/S를 참조하십시오	
		출처	구현되었습니다	HTTP/S를 참조하십시오	
		WWN입니다	구현되었습니다	HTTP/S를 참조하십시오	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 프로토콜입니다	평균 디스크 읽기 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보		
StoragePool 디스크입니다	용량이 프로비저닝되었습 니다	용량이 프로비저닝되었습 니다	구현되었습니다				
		물리적 용량	구현되었습니다				
		총 용량	구현되었습니다				
		사용된 용량	구현되었습니다				
		과도 커밋 용량 비율	구현되었습니다			시간 시리즈로 보고됩니다	
		사용된 용량 비율	구현되었습니다				
		총 데이터 용량	구현되었습니다				
		사용된 데이터 용량	구현되었습니다				
		기타 사용된 용량	구현되었습니다				
		사용된 스냅샷 용량	구현되었습니다				
		사용된 스냅샷 용량 비율	구현되었습니다			시간 시리즈로 보고됩니다	
		볼륨	물리적 용량	물리적 용량	구현되었습니다		
				총 용량	구현되었습니다		
				사용된 용량	구현되었습니다		
사용된 용량 비율	구현되었습니다						
IOPS 읽기	구현되었습니다					디스크의 읽기 IOPS 수입니다	
총 IOPS	구현되었습니다						
IOPS 쓰기	구현되었습니다						
읽기 지연 시간	구현되었습니다						
총 지연 시간	구현되었습니다						
지연 시간 쓰기	구현되었습니다						
처리량 읽기	구현되었습니다						
총 처리량	구현되었습니다					평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)	
처리량 쓰기	구현되었습니다						

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Pure Storage REST API	HTTP/HTTPS	HTTP/HTTPS	80/443		참	참	참	참

[맨 위로](#)

## Red Hat RHV(REST)

이 데이터 수집기에서 지원하는 제품:



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1062					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		프로비저닝된 용량	구현되었습니다	HTTP/S를 참조하십시오	
제품	범주	비밀성	장해되었습니다	사용되는 참조를 참조하십시오	추가 정보
VirtualMachine 디스크		OID	구현되었습니다	HTTP/S를 참조하십시오	
		VirtualMachine OID입니다	구현되었습니다	HTTP/S를 참조하십시오	
		가상디스크 OID	구현되었습니다	HTTP/S를 참조하십시오	
호스트		OID	구현되었습니다	HTTP/S를 참조하십시오	
		이름	구현되었습니다	HTTP/S를 참조하십시오	
		IPS	구현되었습니다	HTTP/S를 참조하십시오	
		플랫폼 유형	구현되었습니다	HTTP/S를 참조하십시오	
		호스트가 메모리를 설치했습니다	구현되었습니다	HTTP/S를 참조하십시오	
		제조업체	구현되었습니다	HTTP/S를 참조하십시오	
		호스트 모델	구현되었습니다	HTTP/S를 참조하십시오	
		호스트 CPU 수입니다	구현되었습니다	HTTP/S를 참조하십시오	
		호스트 CPU 속도	구현되었습니다	HTTP/S를 참조하십시오	
		NIC 수	구현되었습니다	HTTP/S를 참조하십시오	
		NIC 속도	구현되었습니다	HTTP/S를 참조하십시오	
iSCSI 노드		OID	구현되었습니다	HTTP/S를 참조하십시오	
		노드 이름	구현되었습니다	HTTP/S를 참조하십시오	
		유형	틈	HTTP/S를 참조하십시오	
정보		데이터 원본 이름	구현되었습니다	HTTP/S를 참조하십시오	정보
		개시자 ID	구현되었습니다	HTTP/S를 참조하십시오	
		날짜	구현되었습니다	HTTP/S를 참조하십시오	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Red Hat RHEV REST API	HTTPS	HTTPS	443		참	참	참	참

[맨 위로](#)

## Rubrik 스토리지

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전	펌웨어 버전입니다
v5.3	5.3.3-P1-19391 6.0.3-P3-13584 7.0.2-p4-15876 7.0.3-P1-15949 8.0.3-P2-22743 을 참조하십시오

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



		용량(MB)	구현되었습니다	HTTPS	
제품	범주	사용된 노드 용량 활용도(MB)입니다	구현되었습니다	HTTPS	
		피처/속성 사이트 이름	상태 구현되었습니다	사용되는 브라우저입니다	추가 정보
	스토리지 풀	사용된 데이터 용량	구현되었습니다	HTTPS	
		DWh 용량에 포함	구현되었습니다	HTTPS	ACQ에서 Cotnrol까지, DWH 용량에서는 스토리지 풀이 흥미롭습니다
		이름	구현되었습니다	HTTPS	
		기타 중고 용량(MB)	구현되었습니다	HTTPS	데이터 및 스냅샷 이외의 용량
		물리적 디스크 용량(MB)	구현되었습니다	HTTPS	스토리지 풀의 물리적 용량으로 사용됩니다
		RAID 그룹	구현되었습니다	HTTPS	이 StoragePool이 RAID 그룹인지 여부를 나타냅니다
		원시 대 가용 비율	구현되었습니다	HTTPS	가용 용량을 물리적 용량으로 변환하는 비율입니다
		사용된 스냅샷 용량	구현되었습니다	HTTPS	
		스토리지 풀 ID입니다	구현되었습니다	HTTPS	
		씬 프로비저닝이 지원됩니다	구현되었습니다	HTTPS	이 내부 볼륨이 볼륨 계층에 대한 씬 프로비저닝을 지원하는지 여부
		할당된 총 용량입니다	구현되었습니다	HTTPS	
		사용된 총 용량입니다	구현되었습니다	HTTPS	총 용량 (MB)입니다
		유형	틈	HTTPS	
		가상	구현되었습니다	HTTPS	스토리지 가상화 장치입니까?
		실제 사용된 용량 백분율	구현되었습니다	HTTPS	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					

					디스크에서 읽기 및 쓰기)(MB/s)
제품	범주	처리량 쓰기 피처/속성 총 활용률입니다	구현되었습니다 상태 구현되었습니다	HTTPS 사용되는 프로토콜입니다	추가 정보
		StoragePool 디스크입니다	물리적 용량	구현되었습니다	HTTPS
		총 용량	구현되었습니다	HTTPS	
		사용된 용량	구현되었습니다	HTTPS	
		사용된 용량 비율	구현되었습니다	HTTPS	
		사용된 데이터 용량	구현되었습니다	HTTPS	
		IOPS 읽기	구현되었습니다	HTTPS	디스크의 읽기 IOPS 수입니다
		총 IOPS	구현되었습니다	HTTPS	
		IOPS 쓰기	구현되었습니다	HTTPS	
		기타 사용된 용량	구현되었습니다	HTTPS	
		사용된 스냅샷 용량	구현되었습니다	HTTPS	
		처리량 읽기	구현되었습니다	HTTPS	
		총 처리량	구현되었습니다	HTTPS	평균 디스크 총 속도(모든 디스크에서 읽기 및 쓰기)(MB/s)
		처리량 쓰기	구현되었습니다	HTTPS	

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입 니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습 니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
Rubrik 스토리지 REST API	HTTPS	HTTPS	443		참	참	참	참

맨 위로

## NetApp HCI 가상 센터

이 데이터 수집기에서 지원하는 모델 및 버전:

**API 버전**

VMware vCenter Server 6.7.0 빌드 - 10244857  
VMware vCenter Server 6.7.0 빌드 - 14368073  
VMware vCenter Server 7.0.3 빌드 - 19234570  
VMware vCenter Server 7.0.3 빌드 - 20150588  
VMware vCenter Server 7.0.3 빌드 - 20395099  
VMware vCenter Server 7.0.3 빌드 - 20990077  
VMware vCenter Server 7.0.3 빌드 - 21477706  
VMware vCenter Server 7.0.3 빌드 - 21784236  
VMware vCenter Server 8.0.1 빌드 - 21815093

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1074					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	이름	구현되었습니다	웹 서비스	
		OID	구현되었습니다	웹 서비스	추가 정보
		피처/속성 플랫폼 유형	상태 구현되었습니다	사용되는 웹 서비스 호스트입니다	
iSCSI 노드	호스트 별칭	구현되었습니다	웹 서비스		
	노드 이름	구현되었습니다	웹 서비스		
	OID	구현되었습니다	웹 서비스		
	유형	틈	웹 서비스		
정보	API 설명	구현되었습니다	웹 서비스		
	API 이름	구현되었습니다	웹 서비스		
	API 버전	구현되었습니다	웹 서비스		
	클라이언트 API 이름입니다	구현되었습니다	웹 서비스		
	클라이언트 API 버전	구현되었습니다	웹 서비스		
	데이터 원본 이름	구현되었습니다	웹 서비스	정보	
	날짜	구현되었습니다	웹 서비스		
	개시자 ID	구현되었습니다	웹 서비스		



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
1078					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		swapRate.inRate	구현되었습니다	웹 서비스	
제품	범주	스왑 속도 피치/속성	구현되었습니다	웹 서비스	추가 정보
		총 스왑 속도	구현되었습니다	웹 서비스	
	VM	cpuCoSchedulingDelayTimePercent.total	구현되었습니다	웹 서비스	
		cpuDemandToEntityPercent.total 입니다	구현되었습니다	웹 서비스	
		유휴 CPU 시간입니다	구현되었습니다	웹 서비스	유휴 시간(백분율)
		CPU 대기 시간입니다	구현되었습니다	웹 서비스	총 CPU 대기 시간(백분율)
		총 CPU 사용률	구현되었습니다	웹 서비스	
		IOPS 읽기	구현되었습니다	웹 서비스	디스크의 읽기 IOPS 수입니다
		disklops.total	구현되었습니다	웹 서비스	
		디스크 IOPs 쓰기	구현되었습니다	웹 서비스	
		읽기 지연 시간	구현되었습니다	웹 서비스	
		총 지연 시간	구현되었습니다	웹 서비스	
		지연 시간 쓰기	구현되었습니다	웹 서비스	
		디스크 처리량 읽기	구현되었습니다	웹 서비스	
		처리량 읽기	구현되었습니다	웹 서비스	총 디스크 처리량 읽기
		디스크 처리량 쓰기	구현되었습니다	웹 서비스	
		IP 처리량 읽기	구현되었습니다	웹 서비스	
		총 처리량	구현되었습니다	웹 서비스	총 IP 처리량
		ipThroughput.write 입니다	구현되었습니다	웹 서비스	
		총 메모리 사용률	구현되었습니다	웹 서비스	
		swapRate.inRate	구현되었습니다	웹 서비스	
		스왑 속도	구현되었습니다	웹 서비스	
	총 스왑 속도	구현되었습니다	웹 서비스		
	예약 대기 시간	구현되었습니다	웹 서비스	예약 대기 시간 비율	

이 데이터 수집기에서 사용하는 관리 API:

<b>API</b> 를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
VMware REST API	웹 서비스	HTTP/HTTPS	80/443		참	참	참	참

[맨 위로](#)

## AWS 기반 VMware 클라우드

이 데이터 수집기에서 지원하는 모델 및 버전:

API 버전
VMware vCenter Server 7.0.3 빌드 - 20532039
VMware vCenter Server 7.0.3 빌드 - 20870699
VMware vCenter Server 8.0.0 빌드 - 21709157

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1082					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		호스트 CPU 속도	구현되었습니다	웹 서비스	
제품	범주	NIC 수	구현되었습니다	웹 서비스	추가 정보
		피처/속성 NIC 속도	상태 구현되었습니다	사용되는 웹 호스트입니다	
	정보	데이터 원본 이름	구현되었습니다	웹 서비스	정보
		개시자 ID	구현되었습니다	웹 서비스	
		날짜	구현되었습니다	웹 서비스	
		API 이름	구현되었습니다	웹 서비스	
		API 버전	구현되었습니다	웹 서비스	
		API 설명	구현되었습니다	웹 서비스	
		클라이언트 API 이름입니다	구현되었습니다	웹 서비스	
		클라이언트 API 버전	구현되었습니다	웹 서비스	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	구현되었습니다	구현되었습니다	구현되었습니다	구현되었습니다
		총 IOPS 피처/속성 지연 시간 쓰기	구현되었습니다	웹 서비스 사용되는 웹 호스트입니다	디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
	VM	지연 시간 쓰기	구현되었습니다	웹 서비스	
		총 처리량	구현되었습니다	웹 서비스	총 IP 처리량
		스왑 속도	구현되었습니다	웹 서비스	
		디스크 IOPS 쓰기	구현되었습니다	웹 서비스	
		cpuCoSchedulingDelayTimePercent.total	구현되었습니다	웹 서비스	
		IOPS 읽기	구현되었습니다	웹 서비스	디스크의 읽기 IOPS 수입니다
		총 메모리 사용률	구현되었습니다	웹 서비스	
		유휴 CPU 시간입니다	구현되었습니다	웹 서비스	유휴 시간(백분율)
		읽기 지연 시간	구현되었습니다	웹 서비스	
		cpuDemandToEntityPercent.total 입니다	구현되었습니다	웹 서비스	
		총 지연 시간	구현되었습니다	웹 서비스	
		ipThroughput.write 입니다	구현되었습니다	웹 서비스	
		IP 처리량 읽기	구현되었습니다	웹 서비스	
		디스크 처리량 읽기	구현되었습니다	웹 서비스	
		CPU 대기 시간입니다	구현되었습니다	웹 서비스	총 CPU 대기 시간(백분율)
		swapRate.inRate	구현되었습니다	웹 서비스	
		디스크 처리량 쓰기	구현되었습니다	웹 서비스	
		총 CPU 사용률	구현되었습니다	웹 서비스	
		예약 대기 시간	구현되었습니다	웹 서비스	예약 대기 시간 비율
		diskIops.total	구현되었습니다	웹 서비스	
		총 스왑 속도	구현되었습니다	웹 서비스	
		처리량 읽기	구현되었습니다	웹 서비스	총 디스크 처리량 읽기

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
VMware REST API	웹 서비스	HTTP/HTTPS	80/443		참	참	참	참

맨 위로

## VMware vSphere(웹 서비스)

이 데이터 수집기에서 지원하는 모델 및 버전:



## API 버전

VMware ESXi 6.0.0 빌드 - 10719132  
VMware ESXi 6.0.0 빌드 - 2494585  
VMware ESXi 6.0.0 빌드 - 5572656  
VMware ESXi 6.0.0 빌드 - 9313334  
VMware ESXi 6.5.0 빌드 - 14990892  
VMware ESXi 6.5.0 빌드 - 5969303  
VMware ESXi 7.0.0 빌드 - 15843807  
VMware ESXi 7.0.3 빌드 - 20036589  
VMware ESXi 7.0.3 빌드 - 20328353  
VMware ESXi 7.0.3 빌드 - 20842708  
VMware vCenter Server 5.0.0 빌드 - 3073236  
VMware vCenter Server 5.0.0 빌드 - 455964  
VMware vCenter Server 5.0.0 빌드 - 623373  
VMware vCenter Server 5.1.0 빌드 - 3814779  
VMware vCenter Server 5.5.0 빌드 - 1750787  
VMware vCenter Server 5.5.0 빌드 - 2442329  
VMware vCenter Server 5.5.0 빌드 - 3000241  
VMware vCenter Server 5.5.0 빌드 - 3252642  
VMware vCenter Server 5.5.0 빌드 - 3721164  
VMware vCenter Server 5.5.0 빌드 - 4180647  
VMware vCenter Server 5.5.0 빌드 - 6516310  
VMware vCenter Server 5.5.0 빌드 - 9911218  
VMware vCenter Server 6.0.0 빌드 - 13638472  
VMware vCenter Server 6.0.0 빌드 - 14510545  
VMware vCenter Server 6.0.0 빌드 - 2776511  
VMware vCenter Server 6.0.0 빌드 - 3634793  
VMware vCenter Server 6.0.0 빌드 - 3634794  
VMware vCenter Server 6.0.0 빌드 - 5960847  
VMware vCenter Server 6.0.0 빌드 - 7924803  
VMware vCenter Server 6.0.0 빌드 - 8803875  
VMware vCenter Server 6.0.0 빌드 - 9313458  
VMware vCenter Server 6.5.0 빌드 - 1096411  
VMware vCenter Server 6.5.0 빌드 - 15679215  
VMware vCenter Server 6.5.0 빌드 - 17590285  
VMware vCenter Server 6.5.0 빌드 - 17994927  
VMware vCenter Server 6.5.0 빌드 - 18499837  
VMware vCenter Server 6.5.0 빌드 - 18711281  
VMware vCenter Server 6.5.0 빌드 - 19261680  
VMware vCenter Server 6.5.0 빌드 - 20510539  
VMware vCenter Server 6.5.0 빌드 - 7119157  
VMware vCenter Server 6.7.0 빌드 - 10244857  
VMware vCenter Server 6.7.0 빌드 - 11727113  
VMware vCenter Server 6.7.0 빌드 - 13007421  
VMware vCenter Server 6.7.0 빌드 - 13639324  
VMware vCenter Server 6.7.0 빌드 - 14368073  
VMware vCenter Server 6.7.0 빌드 - 15129973  
VMware vCenter Server 6.7.0 빌드 - 15679289  
VMware vCenter Server 6.7.0 빌드 - 17137327  
VMware vCenter Server 6.7.0 빌드 - 18010599  
VMware vCenter Server 6.7.0 빌드 - 18485185  
VMware vCenter Server 6.7.0 빌드 - 18831049  
VMware vCenter Server 6.7.0 빌드 - 19299595  
VMware vCenter Server 6.7.0 빌드 - 19832247  
VMware vCenter Server 6.7.0 빌드 - 19832280

이 데이터 수집기에서 지원하는 제품:

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
기초					
1092					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------



제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		이름	구현되었습니다	웹 서비스	
제품	범주	OID	구현되었습니다	웹 서비스	추가 정보
		피처/속성 플랫폼 유형	상태 구현되었습니다	사용되는 웹 서비스입니다	
	iSCSI 노드	호스트 별칭	구현되었습니다	웹 서비스	
		노드 이름	구현되었습니다	웹 서비스	
		OID	구현되었습니다	웹 서비스	
		유형	틈	웹 서비스	
	정보	API 설명	구현되었습니다	웹 서비스	
		API 이름	구현되었습니다	웹 서비스	
		API 버전	구현되었습니다	웹 서비스	
		클라이언트 API 이름입니다	구현되었습니다	웹 서비스	
		클라이언트 API 버전	구현되었습니다	웹 서비스	
		데이터 원본 이름	구현되었습니다	웹 서비스	정보
		날짜	구현되었습니다	웹 서비스	
		개시자 ID	구현되었습니다	웹 서비스	

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
성능					
1096					

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

제품	범주	피처/속성	상태	사용되는 프로토콜입니다	추가 정보
----	----	-------	----	-----------------	-------

		총 처리량	구현되었습니다	웹 서비스	응답 디스크 읽기 속도(모든 디스크에서 읽기 및 쓰기)(MB/s) 추가 정보
제품	범주	피처/속성 처리량 쓰기	상태 구현되었습니다	사용되는 웹 서비스입니다	
	VM	총 용량	구현되었습니다	웹 서비스	
		사용된 용량	구현되었습니다	웹 서비스	
		사용된 용량 비율	구현되었습니다	웹 서비스	
		cpuCoSchedulingDelayTimePercent.total	구현되었습니다	웹 서비스	
		cpuDemandToEntityPercent.total 입니다	구현되었습니다	웹 서비스	
		유휴 CPU 시간입니다	구현되었습니다	웹 서비스	유휴 시간(백분율)
		CPU 대기 시간입니다	구현되었습니다	웹 서비스	총 CPU 대기 시간(백분율)
		총 CPU 사용률	구현되었습니다	웹 서비스	
		IOPS 읽기	구현되었습니다	웹 서비스	디스크의 읽기 IOPS 수입니다
		disklops.total	구현되었습니다	웹 서비스	
		디스크 IOPs 쓰기	구현되었습니다	웹 서비스	
		읽기 지연 시간	구현되었습니다	웹 서비스	
		총 지연 시간	구현되었습니다	웹 서비스	
		지연 시간 쓰기	구현되었습니다	웹 서비스	
		디스크 처리량 읽기	구현되었습니다	웹 서비스	
		처리량 읽기	구현되었습니다	웹 서비스	총 디스크 처리량 읽기
		디스크 처리량 쓰기	구현되었습니다	웹 서비스	
		IP 처리량 읽기	구현되었습니다	웹 서비스	
		총 처리량	구현되었습니다	웹 서비스	총 IP 처리량
		ipThroughput.write 입니다	구현되었습니다	웹 서비스	
		총 메모리 사용률	구현되었습니다	웹 서비스	
		swapRate.inRate	구현되었습니다	웹 서비스	
		스왑 속도	구현되었습니다	웹 서비스	
		총 스왑 속도	구현되었습니다	웹 서비스	
		예약 대기 시간	구현되었습니다	웹 서비스	예약 대기 시간 비율

이 데이터 수집기에서 사용하는 관리 API:

API를 참조하십시오	사용되는 프로토콜입니다	전송 계층 프로토콜이 사용됩니다	들어오는 포트가 사용되었습니다	발신 포트가 사용됩니다	인증을 지원합니다	'읽기 전용' 자격 증명만 필요합니다	암호화를 지원합니다	방화벽 친화적(정적 포트)
VMware REST API	웹 서비스	HTTP/HTTPS	80/443		참	참	참	참


[맨 위로](#)

# 참조 지원

## 지원을 요청하는 중입니다

Data Infrastructure Insights에서 \* 도움말 > 지원 \* 을 클릭하여 지원 옵션에 액세스할 수 있습니다. 사용 가능한 지원 옵션은 Data Infrastructure Insights Edition에 따라 다릅니다.

<b>Cloud Insights Support</b> NetApp Serial Number: 123456789011234567890 AWS Customer ID: AbCdEfGhI12345678990zyxWVU Support activation is required to enable support with NetApp through web ticket or phone. Activate Support at <a href="https://register.netapp.com">register.netapp.com</a> . <input checked="" type="checkbox"/> Check this box to allow NetApp access to your instance of Cloud Insights.		<b>Contact Us</b> Need help with Cloud Insights? Technical Support: <a href="#">Open a Support Ticket</a>   <a href="#">Phone (P1)</a>   <a href="#">Chat</a> Sales: Have questions regarding your subscription? <a href="#">Contact Sales</a> .	
<b>Knowledge Base</b> Search through the <a href="#">Cloud Insights Knowledge Base</a> to find helpful articles.	<b>Documentation Center</b> Visit the <a href="#">Cloud Insights Documentation Center</a> to find step by step instructions to help you get the most out of Cloud Insights.	<b>Communities</b> Join the <a href="#">Cloud Insights Community</a> to follow ongoing discussions or create a new one.	<b>Feedback</b> We value your input. <a href="#">Your feedback</a> helps us improve Cloud Insights.
<b>Learning Center</b> Cloud Insights Course List: <ul style="list-style-type: none"><li><a href="#">Hybrid Cloud Resource Management</a></li><li><a href="#">Cloud Insights Fundamentals</a></li><li><a href="#">Cloud Resource Management</a></li><li><a href="#">Cloud Secure</a></li></ul>		<b>Cloud Education All-Access Pass:</b> Visit and subscribe the <a href="#">Cloud Education All-Access Pass</a> to get unlimited access to our best cloud learning resources.	<b>Course Catalog:</b> Browse the <a href="#">Learning Services Product Catalog</a> to find all the courses that are relevant to you.
<b>Proxy Settings</b> Need to setup proxy exceptions? Click <a href="#">here</a> to learn more.			



## 지원 권한 활성화 중

Data Infrastructure Insights는 평가판 모드에서 실행할 때 셀프 서비스 및 이메일 지원을 제공합니다. 서비스에 가입한 후에는 지원 권한을 활성화하는 것이 좋습니다. 지원 권한을 활성화하면 온라인 채팅, 웹 티켓 시스템 및 전화를 통해 기술 지원에 액세스할 수 있습니다. 기본 지원 모드는 등록이 완료될 때까지 셀프 서비스로 설정됩니다. [세부 정보](#)아래를 참조하십시오.

최초 구독 프로세스 중에 Data Infrastructure Insights 인스턴스에서 "950"부터 20자릿수의 NetApp 일련 번호가 생성됩니다. 이 NetApp 일련 번호는 귀하의 계정과 연결된 Data Infrastructure Insights 가입을 나타냅니다. 지원 자격을 활성화하려면 NetApp 일련 번호를 등록해야 합니다. NetApp에서는 두 가지 지원 등록 옵션을 제공합니다.

1. 기존 NetApp Support 사이트(NSS) SSO 계정을 가진 사용자(예: 현재 NetApp 고객)
2. 기존 NetApp Support Site(NSS) SSO 계정이 없는 새로운 NetApp 고객



옵션 1: 기존 **NSS(NetApp Support Site) SSO** 계정을 가진 사용자를 위한 단계

단계

1. NetApp 등록 웹 사이트로 이동합니다 <https://register.netapp.com>
2. "이미 NetApp 고객으로 등록되어 있습니다."를 선택하고 데이터 인프라 인사이트 를 제품군으로 선택합니다. 청구 공급자(NetApp 또는 AWS)를 선택하고 Data Infrastructure Insights 사용자 인터페이스의 도움말 > 지원 메뉴를 참조하여 일련 번호와 NetApp 구독 이름 또는 AWS 고객 ID를 제공하십시오.

### Cloud Insights Support

**NetApp Serial Number:** 95011122233344455512      **NetApp Subscription Name:** A-000012345

Support activation is required to enable support with NetApp through chat, ticket or phone. Activate Support at [register.netapp.com](https://register.netapp.com).

Check this box to allow NetApp access to your instance of Cloud Insights.

3. 기존 고객 등록 양식을 작성하고 \* 제출 \* 을 클릭합니다.

### Existing Customer Registration

The fields marked with \* are mandatory

First Name*	<input type="text" value="Test"/>
Last Name*	<input type="text" value="Cloud2"/>
Company*	<input type="text" value="NetApp Inc. (VSA Only)"/>
Email Address*	<input type="text" value="ng-cloudvol-csd1@netapp.com"/>
Product Line*	<input type="text" value="Cloud Insights"/>
Billing Provider*	<input type="text" value="NetApp"/>
Cloud Insights Serial #*	<input type="text" value="e.g. 95012235021303893918"/>
NetApp Subscription Name*	<input type="text" value="e.g. A-S0000100"/>

[Add another Serial #](#)

4. 오류가 발생하지 않으면 "Registration Submitted successfully(등록 제출됨)" 페이지로 이동합니다. 등록에 사용되는 NSS SSO 사용자 이름과 연결된 이메일 주소는 몇 분 이내에 "Your product is now eligible for support"라는 이메일을 받게 됩니다.
5. Data Infrastructure Insights NetApp 일련 번호에 대한 일회성 등록입니다.

옵션 2: 기존 **NetApp Support** 사이트(NSS) SSO 계정이 없는 새로운 **NetApp** 고객을 위한 단계

단계

1. NetApp 등록 웹 사이트로 이동합니다 <https://register.netapp.com>
2. "등록된 NetApp 고객이 아닙니다."를 선택하고 아래 예시 양식에 필요한 정보를 입력합니다.


## New Customer Registration

**IMPORTANT:** After submitting, a confirmation email will be sent to the email address filled-in the form. Please click the validation link in that email to complete the registration.

The fields marked with \* are mandatory

First Name*	<input type="text"/>
Last Name*	<input type="text"/>
Company*	<input type="text"/>
Email Address*	<input type="text"/>
Office Phone*	<input type="text"/>
Alternate Phone	<input type="text"/>
Address Line 1*	<input type="text"/>
Address Line 2	<input type="text"/>
Postal Code / City*	<input type="text"/>
State/Province / Country*	<input type="text"/> - Select - <span style="float: right;">▼</span>
NetApp Reference SN	<input type="text"/>
If you currently own a NetApp product, please provide the Serial Number for that product here in order to speed-up the validation process	
Product Line*	Cloud Insights <span style="float: right;">▼</span>
Billing Provider *	NetApp <span style="float: right;">▼</span>
Cloud Insights Serial # * <span style="font-size: x-small;"> ⓘ</span>	<input type="text" value="e.g. 95012235021303893918"/>
NetApp Subscription Name * <span style="font-size: x-small;"> ⓘ</span>	<input type="text" value="e.g. A-S0000100"/>
	<a href="#">Add another Serial #</a>

**Security check:** Enter the characters shown in the image to verify your ➡



1. Data Infrastructure Insights \_을(를) 제품 라인으로 선택합니다. 청구 공급자(NetApp 또는 AWS)를 선택하고 Data Infrastructure Insights 사용자 인터페이스의 도움말 > 지원 메뉴를 참조하여 일련 번호와 NetApp 구독 이름 또는 AWS 고객 ID를 제공하십시오.

## Cloud Insights Support

NetApp Serial Number:  
95011122233344455512

NetApp Subscription Name:  
A-000012345

Support activation is required to enable support with NetApp through chat, ticket or phone.  
Activate Support at [register.netapp.com](https://register.netapp.com).

Check this box to allow NetApp access to your instance of Cloud Insights.

- 오류가 발생하지 않으면 "Registration Submitted successfully(등록 제출됨)" 페이지로 이동합니다. 등록에 사용되는 NSS SSO 사용자 이름과 연결된 이메일 주소는 몇 시간 이내에 "Your product is now eligible for support"라는 이메일을 받게 됩니다.
- 또한 새로운 NetApp 고객은 NSS(NetApp Support Site) 사용자 계정을 생성하여 향후 등록을 해야 하며 기술 지원 채팅 및 웹 티켓 지원을 위한 지원 포털에 액세스해야 합니다. 이 링크는 <https://mysupport.netapp.com/eservice/public/now.do> 있습니다. 프로세스를 신속하게 처리하기 위해 새로 등록된 Data Infrastructure Insights 일련 번호를 제공할 수 있습니다.
- Data Infrastructure Insights NetApp 일련 번호는 1회 등록입니다.

### 지원 정보 얻기

NetApp는 다양한 방식으로 데이터 인프라 인사이트를 지원합니다. 기술 자료(KB) 기사 또는 NetApp 커뮤니티 등 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. Data Infrastructure Insights 에디션(Basic \*, Standard, Premium)을 구독하는 사용자의 경우 전화 또는 웹 티켓팅을 통해 기술 지원을 받을 수 있습니다. NSS(NetApp Support Site) SSO 계정은 케이스 관리와 함께 웹 티켓에 필요합니다.

모든 NetApp 스토리지 시스템에 적어도 프리미엄 지원 수준이 적용되는 한 \* Support는 Basic Edition에서 제공됩니다.

셀프 서비스 지원:

이러한 지원 옵션은 평가판 모드에서 사용할 수 있으며 연중무휴 24시간 무료로 제공됩니다.

- [\\*https://kb.NetApp.com/Special:Search?query=cloud+insights\[Knowledgebase\]](https://kb.NetApp.com/Special:Search?query=cloud+insights[Knowledgebase]) \*

+ 이 섹션의 링크를 클릭하면 관련 문서, 사용 방법 등을 검색할 수 있는 NetApp 기술 문서로 이동합니다.

- ["문서화"](#)

설명서 링크를 클릭하면 이 설명서 센터로 이동합니다.

- ["커뮤니티"](#)

커뮤니티 링크를 클릭하면 NetApp Data Infrastructure Insights 커뮤니티로 이동하여 동료 및 전문가와 교류할 수 있습니다.

xref.: [\\*\\* 피드백 \\*\\*](#) 데이터 인프라 인사이트를 개선하는 데 도움이 되는 링크도 있습니다.

## 구독 지원

위의 자체 지원 옵션 외에도, 모니터링되는 NetApp 제품 또는 서비스에 대해 Data Infrastructure Insights에 가입하거나 유료 지원이 있는 경우 NetApp 지원 엔지니어와 협력하여 문제를 해결할 수 있습니다.



에 등록하려면 등록해야 합니다 [지원을 활성화합니다](#) NetApp Cloud 제품: 등록하려면 NetApp로 이동하십시오 "[클라우드 데이터 서비스 지원 등록](#)".

지원 세션 중에 NetApp 지원 엔지니어가 데이터 인프라 인사이트 환경에 액세스할 수 있도록 확인란을 선택하는 것이 좋습니다. 그러면 엔지니어가 문제를 해결하고 신속하게 해결할 수 있습니다. 문제가 해결되거나 지원 세션이 종료된 경우 확인란을 선택 취소할 수 있습니다.

다음 방법 중 하나를 사용하여 지원을 요청할 수 있습니다. 다음 지원 옵션을 사용하려면 활성 Data Infrastructure Insights에 가입되어 있어야 합니다.

- **"\* 전화 \***
- **"\* 지원 티켓 \***
- **\* 채팅 \*** - NetApp 지원 담당자와 연결하여 지원을 받을 수 있습니다(평일에만 해당). 채팅은 Data Infrastructure Insights 화면의 오른쪽 위에 있는 \* 도움말 > 라이브 채팅 \* 메뉴 옵션에서 확인할 수 있습니다.

을 클릭하여 영업 지원을 요청할 수도 있습니다 **"\* 영업팀에 문의 \*** 링크.

Data Infrastructure Insights 일련 번호는 서비스 내에 \* 도움말 > 지원 \* 메뉴를 통해 표시됩니다. 서비스에 액세스하는데 문제가 있고 이전에 NetApp에 일련 번호를 등록한 경우 다음과 같이 NetApp Support 사이트에서 Data Infrastructure Insights 일련 번호 목록을 볼 수도 있습니다.

- [mysupport.netapp.com](https://mysupport.netapp.com) 에 로그인합니다
- Products > My Products 메뉴 탭에서 제품군 "SaaS Data Infrastructure Insights"를 사용하여 등록된 모든 일련 번호를 찾습니다.

## View Installed Systems

### Selection Criteria

- ▶ Select:  Then, enter Value:    
Enter the entire value, or use asterisk (\*) for wildcard searches. (Wildcard search does not apply to Serial Numbers)  
Wildcard searches may take some time.  
Enter the Cluster Serial Number value without dashes.

- OR -

- ▶ Search Type\*:  Product Family (optional):   
City (optional):  State/Province (optional):   
Postal Code (optional):  Country (optional):

### Details

If you see any discrepancies or errors in the information shown below, please submit [Feedback](#) and be sure to include the serial nu

## Data Infrastructure Insights Data Collector 지원 매트릭스

에서 지원되는 데이터 수집기에 대한 정보 및 세부 정보를 보거나 다운로드할 수 \* [Data Infrastructure Insights 데이터 수집기 지원 매트릭스](#) \*, 역할 = 있습니다.

학습 센터

구독과 관계없이 \* 도움말 > 지원 \* 은 데이터 인프라 Insights를 최대한 활용할 수 있도록 여러 NetApp University 과정 오퍼링에 연결됩니다. 확인해 보세요!

## Data Collector 참조 - 인프라

공급업체별 참조 자료

이 섹션의 항목에서는 공급업체별 참조 정보를 제공합니다. 대부분의 경우 데이터 수집기 구성은 간단합니다. 경우에 따라 데이터 수집기를 올바르게 구성하기 위해 추가 정보나 명령이 필요할 수 있습니다.

데이터 수집기에 대한 정보를 보려면 왼쪽의 메뉴에서 \* vendor \* 를 클릭하십시오.

### Amazon EC2 데이터 수집기 구성

Data Infrastructure Insights는 Amazon EC2 데이터 수집기를 사용하여 EC2 인스턴스로부터 인벤토리 및 성능 데이터를 가져옵니다.

요구 사항

Amazon EC2 장치에서 데이터를 수집하려면 다음 정보가 있어야 합니다.

- 다음 중 하나가 있어야 합니다.
  - IAM 역할 인증을 사용하는 경우 Amazon EC2 클라우드 계정에 대한 \* IAM Role \* 입니다. IAM Role은 AWS 인스턴스에 획득 장치가 설치된 경우에만 적용됩니다.
  - IAM 액세스 키 인증을 사용하는 경우 Amazon EC2 클라우드 계정의 \* IAM 액세스 키 \* ID 및 비밀 액세스 키
- "조직 목록" 권한이 있어야 합니다
- 포트 443 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. Amazon EC2 SDK, REST 또는 쿼리 API 작업을 사용하는 경우 액세스 키를 사용하여 EC2에 만드는 프로그래밍 방식 요청에 서명할 수 있습니다. 이러한 키는 아마존에서 귀하의 계약과 함께 제공됩니다.

구성

아래 표에 따라 데이터 수집기 필드에 데이터를 입력합니다.

필드에 입력합니다	설명
AWS 지역	AWS 지역을 선택하십시오
IAM 역할	AWS의 AU에서 획득한 경우에만 사용합니다. 에 대한 자세한 내용은 아래를 참조하십시오 <a href="#">IAM 역할</a> .
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.
API 요청에 대한 AWS 청구 내용을 알고 있습니다	Data Infrastructure Insights 폴링을 통해 생성된 API 요청에 대해 AWS가 청구한다는 이해도를 확인하려면 이 점검 목록을 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)	기본값은 60입니다
태그별로 VM 필터링에 적용하려면 '제외' 또는 '포함'을 선택합니다	데이터를 수집할 때 태그별로 VM을 포함할지 제외할지 여부를 지정합니다. '포함'을 선택한 경우 태그 키 필드를 비워 둘 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)	기본값은 1800입니다
CloudWatch Agent 메트릭 네임스페이스	데이터를 수집할 EC2/EBS의 네임스페이스입니다. 이 네임스페이스의 기본 메트릭 이름이 변경되면 Data Infrastructure Insights에서 이름이 바뀐 데이터를 수집하지 못할 수 있습니다. 기본 메트릭 이름은 그대로 두는 것이 좋습니다.

## IAM 액세스 키

액세스 키는 IAM 사용자 또는 AWS 계정 루트 사용자에게 대한 장기 자격 증명입니다. 액세스 키는 AWS CLI 또는 AWS API(직접 또는 AWS SDK 사용)에 프로그래밍 방식으로 요청을 서명하는 데 사용됩니다.

액세스 키는 액세스 키 ID와 비밀 액세스 키의 두 부분으로 구성됩니다. IAM Role `_authentication`과 달리 `_IAM Access Key_authentication`을 사용할 때는 요청 인증을 위해 액세스 키 ID와 비밀 액세스 키를 함께 사용해야 합니다. 자세한 내용은 의 [아마존 문서](#)를 참조하십시오 "[액세스 키](#)".

## IAM 역할

IAM Access Key 인증과 달리 `_IAM Role_authentication`을 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.

자세한 내용은 아마존 문서를 참조하십시오 ["IAM 역할"](#).

참고: IAM 역할은 획득 장치가 AWS 인스턴스에서 실행 중인 경우에만 사용할 수 있습니다.

### Amazon 태그를 Data Infrastructure Insights 주석에 매핑

Amazon EC2 데이터 수집기에는 EC2에 구성된 태그로 Data Infrastructure Insights 주석을 채울 수 있는 옵션이 포함되어 있습니다. 주석 이름은 EC2 태그로 정확하게 지정해야 합니다. Data Infrastructure Insights는 항상 같은 이름의 텍스트 유형 주석을 채우고 다른 유형(숫자, 부울 등)의 주석을 채우려는 "최선의 시도"를 합니다. 주석이 다른 유형이고 데이터 수집기가 주석을 채우지 못할 경우 주석을 제거하고 텍스트 유형으로 다시 생성해야 할 수 있습니다.

AWS는 대소문자를 구분하지만 Data Infrastructure Insights는 대소문자를 구분하지 않습니다. 따라서 Data Infrastructure Insights에서 "owner"라는 주석을 생성하고 EC2에서 "owner", "owner" 및 "owner"라는 태그를 생성하면 모든 EC2 변형 "owner"가 Cloud Insight의 "소유자" 주석에 매핑됩니다.

### 추가 지역 포함

AWS Data Collector \* 고급 구성 \* 섹션에서 추가 영역을 포함하도록 \* 추가 영역 포함 \* 필드를 심포 또는 세미콜론으로 구분하여 설정할 수 있습니다. 기본적으로 이 필드는 모든 미국 AWS 지역에서 수집하는 \*`_us-`. \*`_` \* 로 설정됩니다. `on_all_regions`를 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 중

Data Infrastructure Insights는 단일 AWS 데이터 수집기 내에서 AWS용 하위 계정 수집을 지원합니다. 이 컬렉션에 대한 구성은 AWS 환경에서 수행됩니다.

- 기본 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.
- Data Infrastructure Insights AWS Data Collector \* 고급 구성 \* 섹션의 \* 교차 계정 역할 \* 필드에 이 역할 이름 문자열을 입력합니다.
- Collector가 설치된 계정에는 `_delegate` 액세스 권한이 있는 `administrator_Privileges`가 있어야 합니다. ["AWS 설명서"](#) 자세한 내용은 를 참조하십시오.

모범 사례: AWS Predefined `_AmazonEC2ReadOnlyAccess_policy`를 EC2 기본 계정에 할당하는 것이 좋습니다. 또한 데이터 소스에서 구성된 사용자는 AWS를 쿼리하기 위해 미리 정의된 `_AWSOrganizationReadOnlyAccess_policy` 이상을 할당해야 합니다.

Data Infrastructure Insights가 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"

문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## NetApp ONTAP 데이터 수집기를 위한 Amazon FSx

이 데이터 수집기는 NetApp ONTAP용 Amazon FSx에서 인벤토리 및 성능 데이터를 가져옵니다. 이 데이터 수집기는 Data Infrastructure Insights 서비스 지역에서 점증적으로 사용할 수 있게 됩니다. Data Infrastructure Insights 환경에 이 수집기 아이콘이 보이지 않으면 영업 담당자에게 문의하십시오.



이 데이터 인프라 인사이트 수집기에는 `_Filesystem-scoped_role`을 가진 ONTAP 사용자가 필요합니다. **"역할 및 규칙"**사용 가능한 옵션은 AWS 설명서를 검토하십시오. 현재 AWS는 Filesystem Scope인 `_fsxadmin_`의 한 가지 사용자 역할만 지원합니다. 이 역할은 Data Infrastructure Insights Collector에 사용되는 적절한 역할입니다. 사용자는 `http`, `ontapi`, `ssh` 등 세 가지 응용 프로그램을 모두 할당해야 합니다.

용어

Data Infrastructure Insights는 FSx-NetApp 데이터 수집기에서 인벤토리 및 성능 데이터를 가져옵니다. 획득한 각 자산 유형에 대해 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
클러스터	스토리지
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨

### FSX-NetApp 용어

다음 용어는 FSx-NetApp 스토리지 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

스토리지

- 모델 – 이 클러스터 내에서 고유한 개별 모델 이름을 심표로 구분한 목록입니다.
- 공급업체 – AWS
- 일련 번호 – 스토리지 일련 번호입니다.
- IP – 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다.



- 물리적 용량 – FSx 파일 시스템에 할당된 모든 SSD 스토리지에 대한 기본 2 합계.
- 지연 시간 – 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. Data Infrastructure Insights는 이러한 가치를 직접 소싱하는 것이 좋지만, 그렇게 할 경우에는 그렇지 않은 경우가 많습니다. Data Infrastructure Insights는 이러한 기능을 제공하는 어레이 대신 일반적으로 개별 내부 볼륨의 통계에서 도출된 IOPS 가중 계산을 수행합니다.
- 처리량 – 내부 볼륨에서 집계됩니다. 관리 - 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Data Infrastructure Insights 데이터 소스에 의해 프로그래밍 방식으로 생성되었습니다.

#### 스토리지 풀

- 스토리지 – 이 풀이 상주하는 스토리지 시스템입니다. 필수입니다.
- 형식 - 가능성 목록 목록의 설명 값입니다. 일반적으로 "집계" 또는 "RAID 그룹"이 됩니다.
- 용량 – 이 값은 논리적 사용 용량, 가용 용량 및 총 논리적 용량, 그리고 이 용량 전체에서 사용된 비율입니다.
- IOPS – 이 스토리지 풀에 할당된 모든 볼륨의 IOPS 합계입니다.
- 처리량 – 이 스토리지 풀에 할당된 모든 볼륨의 총 처리량입니다.

#### 요구 사항

다음은 이 데이터 수집기를 구성하고 사용하기 위한 요구 사항입니다.

- ssh, ontapi, http 등 세 개의 응용 프로그램이 할당된 "fsxadmin" 역할의 계정에 액세스할 수 있어야 합니다
- 계정 세부 정보에는 사용자 이름 및 암호가 포함됩니다.
- 포트 요구 사항: 443

#### 구성

필드에 입력합니다	설명
NetApp 관리 IP	NetApp 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	NetApp 클러스터의 사용자 이름입니다
암호	NetApp 클러스터의 암호입니다

#### 고급 메트릭스

이 데이터 수집기는 NetApp ONTAP 스토리지용 FSx에서 다음 고급 메트릭을 수집합니다.

- FPolicy를 참조하십시오
- NFSv3
- NFSv3:노드
- NFSv4
- NFSv4\_1
- NFSv4\_1: node
- NFSv4: node

- policy\_group입니다
- qtree입니다
- 볼륨
- workload\_volume

FSx CLI 및 API 명령은 Data Infrastructure Insights ZAPI가 수집하지 않는 일부 용량 값을 검색하므로 Data Infrastructure Insights에서 스토리지 풀에 대한 값 등 특정 용량 값이 FSx 자체에 있는 값과 다를 수 있습니다.

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
수신 401 HTTP 응답 또는 13003 ZAPI 오류 코드 및 ZAPI는 "불충분한 권한" 또는 "이 명령에 대해 인증되지 않음"을 반환합니다.	사용자 이름과 암호, 사용자 권한/권한을 확인합니다.
ZAPI는 "cluster role is not cluster_mgmt LIF" 를 반환합니다.	AU는 클러스터 관리 IP와 통신해야 합니다. IP를 확인하고 필요한 경우 다른 IP로 변경합니다
재시도 후 ZAPI 명령이 실패합니다	AU가 클러스터와 통신 문제를 겪고 있습니다. 네트워크, 포트 번호 및 IP 주소를 확인합니다. 또한 사용자는 AU 시스템의 명령줄에서 명령을 실행해야 합니다.
AU가 HTTP를 통해 ZAPI에 연결하지 못했습니다	ZAPI 포트가 일반 텍스트를 허용하는지 확인합니다. AU가 SSL 소켓에 일반 텍스트를 보내려고 하면 통신이 실패합니다.
SSLException 과 통신이 실패합니다	AU가 파일러의 일반 텍스트 포트에 SSL을 전송하려고 합니다. ZAPI 포트가 SSL을 허용하는지 또는 다른 포트를 사용하는지 확인합니다.
추가 연결 오류: ZAPI 응답에는 오류 코드 13001, "데이터베이스가 열려 있지 않습니다." ZAPI 오류 코드가 60이고 응답에는 "API가 시간에 완료되지 않았습니다."가 포함되어 있습니다. ZAPI 응답에는 "initialize_session() returned NULL environment" ZAPI가 포함되어 있습니다. ZAPI 오류 코드는 14007이고 응답에는 "노드가 정상 상태가 아닙니다"가 포함되어 있습니다.	네트워크, 포트 번호 및 IP 주소를 확인합니다. 또한 사용자는 AU 시스템의 명령줄에서 명령을 실행해야 합니다.

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## Azure 컴퓨팅 데이터 수집기 구성

Data Infrastructure Insights는 Azure 컴퓨팅 데이터 수집기를 사용하여 Azure 컴퓨팅 인스턴스의 인벤토리 및 성능 데이터를 가져옵니다.

### 요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 포트 요구 사항: 443 HTTPS
- Azure OAuth 2.0 리디렉션 URI(login.microsoftonline.com)
- Azure 관리 REST IP(management.azure.com)
- Azure Resource Manager IP(management.core.windows.net)
- Azure 서비스 주 응용 프로그램(클라이언트) ID(리더 역할 필요)
- Azure 서비스 주 인증 키(사용자 암호)
- Data Infrastructure Insights 검색을 위해 Azure 계정을 설정해야 합니다.

계정이 올바르게 구성되고 Azure에 애플리케이션을 등록하면 Data Infrastructure Insights를 통해 Azure 인스턴스를 검색하는 데 필요한 자격 증명이 제공됩니다. 다음 링크는 검색을 위해 계정을 설정하는 방법을 설명합니다. <https://docs.microsoft.com/en-us/azure/active-directory/develop/howto-create-service-principal-portal>

### 구성

아래 표에 따라 데이터 수집기 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

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 선택한 경우 태그 키 필드를 비워 둘 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)	기본값은 300입니다

### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## Broadcom의

### Brocade Network Advisor 데이터 수집기

Data Infrastructure Insights는 Brocade Network Advisor 데이터 수집기를 사용하여 Brocade 스위치의 인벤토리 및 성능 데이터를 가져옵니다.

#### 용어

Data Infrastructure Insights는 Brocade Network Advisor 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
스위치	스위치
포트	포트
가상 패브릭, 물리적 패브릭	패브릭
논리 스위치	논리 스위치

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

이 데이터 수집기를 구성하려면 다음이 필요합니다.

- Data Infrastructure Insights 수집 장치는 BNA 서버의 TCP 포트 443에 대한 연결을 시작합니다. BNA 서버는 버전 14.2.1 이상을 실행해야 합니다.
- Brocade Network Advisor 서버 IP 주소입니다
- 관리자 계정에 대한 사용자 이름 및 암호
- 포트 요구 사항: HTTP/HTTPS 443

#### 구성

필드에 입력합니다	설명
Brocade Network Advisor 서버 IP입니다	Network Advisor 서버의 IP 주소입니다
사용자 이름	스위치의 사용자 이름입니다
사용자 이름	관리자 사용자 이름입니다
암호	관리자 암호입니다

#### 고급 구성

필드에 입력합니다	설명
연결 유형	HTTPS(기본 포트 443) 또는 HTTP(기본 포트 80)

필드에 입력합니다	설명
연결 포트를 재정의합니다	비어 있는 경우 연결 유형 필드에서 기본 포트를 사용하고, 그렇지 않으면 사용할 연결 포트를 입력합니다
암호	스위치에 대한 암호입니다
재고 폴링 간격(분)	기본값은 40입니다
보고서 액세스 게이트웨이	액세스 게이트웨이 모드에 장치를 포함하려면 선택합니다
성능 폴링 간격(초)	기본값은 1800입니다

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
둘 이상의 노드가 Access Gateway 포트에 로그인되었거나 데이터 수집기가 Access Gateway 장치를 검색하지 못했다는 메시지를 받습니다.	NPV 디바이스가 올바르게 작동하고 있고 연결된 모든 WWN이 예상되는지 확인합니다. NPV 장치를 직접 얻지 마십시오. 대신 핵심 패브릭 스위치를 인수하면 NPV 장치 데이터가 수집됩니다.

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

#### Brocade FC 스위치 데이터 수집기

Data Infrastructure Insights는 Brocade FC 스위치(SSH) 데이터 소스를 사용하여 계수 OS(운영 체제) 펌웨어 4.2 이상을 실행하는 Brocade 또는 브랜드가 변경된 스위치 장치의 인벤토리를 검색합니다. FC 스위치와 액세스 게이트웨이 모드의 디바이스가 모두 지원됩니다.

#### 용어

Data Infrastructure Insights는 Brocade FC 스위치 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
스위치	스위치
포트	포트
가상 패브릭, 물리적 패브릭	패브릭
Zone(영역)	Zone(영역)
논리 스위치	논리 스위치
가상 볼륨	볼륨
LSAN 구역	IVR 영역

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

- 데이터 인프라 인사이트 획득 장치(AU)는 인벤토리 데이터를 수집하기 위해 Brocade 스위치의 TCP 포트 22에 대한 연결을 시작합니다. 또한 AU는 성능 데이터 수집을 위해 UDP 포트 161에 대한 연결을 시작합니다.
- Fabric의 모든 스위치에 IP 연결이 있어야 합니다. 패브릭에서 모든 스위치 검색 확인란을 선택한 경우 Data Infrastructure Insights는 패브릭의 모든 스위치를 식별하지만, 이러한 추가 스위치를 검색하려면 IP 연결이 필요합니다.
- Fabric의 모든 스위치에서 동일한 계정이 전 세계적으로 필요합니다. PuTTY(오픈 소스 터미널 에뮬레이터)를 사용하여 액세스를 확인할 수 있습니다.
- SNMP 성능 폴링을 위해 Fabric의 모든 스위치에 포트 161과 162가 열려 있어야 합니다.
- SNMP 읽기 전용 커뮤니티 문자열

## 구성

필드에 입력합니다	설명
스위치 IP	EFC 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	스위치의 사용자 이름입니다
암호	스위치에 대한 암호입니다
SNMP를 선택합니다	SNMP 버전입니다
SNMP 커뮤니티 문자열	스위치에 액세스하는 데 사용되는 SNMP 읽기 전용 커뮤니티 문자열입니다
SNMP 사용자 이름입니다	SNMP 사용자 이름입니다
SNMP 암호	SNMP 암호입니다

## 고급 구성

필드에 입력합니다	설명
패브릭 이름	데이터 수집기에서 보고할 Fabric 이름입니다. 패브릭 이름을 WWN으로 보고하려면 공백으로 두십시오.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 15입니다.
제외된 장치	폴링에서 제외할 장치 ID의 심표로 구분된 목록입니다
관리자 도메인이 활성화되었습니다	관리자 도메인을 사용하는 경우 선택합니다
MPR 데이터 검색	다중 프로토콜 라우터에서 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 시간입니다. 기본값은 10입니다.
패브릭의 모든 스위치를 살펴보십시오	Fabric의 모든 스위치를 검색하려면 선택합니다
HBA와 을 선택합니다 영역 별칭	HBA 또는 영역 별칭을 사용할지 여부를 선택합니다

필드에 입력합니다	설명
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.
SNMP 인증 프로토콜	SNMP 인증 프로토콜(SNMP v3만 해당)
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호(SNMP v3만 해당)
SNMP 재시도	SNMP 재시도 횟수입니다

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
Brocade 데이터 소스의 인벤토리 획득에 실패하고 다음 오류 [com.onaro.sanscreen.acquisition.framework.datasour ce.BaseDataSource] Error 2 out of 2:<datasour ce.name> [Internal error] - unable to generate the model for device <IP>(2개 중 <날짜><시간> 오류 [오류 2 of 2: <데이터 소스 이름> [내부 오류] - 장치의 모델을 생성할 수 없습니다.) 프롬프트([Device name<name>]: 장치 <IP>에 대한 모델을 생성할 수 없습니다. 프롬프트 감지 중 오류 발생)	이 문제는 Brocade 스위치가 프롬프트와 함께 돌아오는데 시간이 너무 오래 걸리고 기본 시간 초과가 5초일 때 발생할 수 있습니다. Data Infrastructure Insights의 데이터 수집기의 고급 구성 설정에서 _SSH 배너 대기 시간 초과(초)_를 더 높은 값으로 늘리십시오.
오류: "Data Infrastructure Insights가 잘못된 새시 역할을 수신했습니다."	이 데이터 원본에 구성된 사용자에게 새시 역할 권한이 부여되었는지 확인합니다.
오류: "새시 IP 주소가 일치하지 않습니다."	새시 IP 주소를 사용하도록 데이터 소스 구성을 변경합니다.
Access Gateway 포트에 두 개 이상의 노드가 로그인되었다는 메시지를 받습니다	NPV 디바이스가 올바르게 작동하고 있고 연결된 모든 WWN이 예상되는지 확인합니다. NPV 장치를 직접 얻지 마십시오. 대신 핵심 패브릭 스위치를 인수하면 NPV 장치 데이터가 수집됩니다.
성능 수집이 "SNMP 요청 전송 중 시간 초과"와 함께 실패합니다.	쿼리 변수 및 스위치 구성에 따라 일부 쿼리가 기본 시간 제한을 초과할 수 있습니다. " <a href="#">자세한 정보</a> ".

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

#### Brocade FOS REST Data Collector

Data Infrastructure Insights는 Brocade FOS REST Collector를 사용하여 FabricOS(FabricOS) 펌웨어 8.2 이상을 실행하는 Brocade 스위치 장치의 인벤토리 및 성능을 검색합니다.

참고: FOS의 기본 "사용자" 수준은 장치의 모든 논리적 측면을 Data Infrastructure Insights에서 볼 수 있는 기능이 충분하지 않습니다. "새시 역할"이 활성화된 사용자 계정과 스위치에서 구성된 모든 가상 패브릭에 대한 권한이 필요합니다.

다음은 FOS 디바이스에 대한 SSH 세션에서 Data Infrastructure Insights 사용에 대한 "최소 권한" 사용자 계정을

생성하는 방법의 예입니다.

```
userConfig—add NetAppCIUser-r user-l 1-128-c user-p QWERTY!
```

이렇게 하면 암호가 "QWERTY!"인 "NetAppCIUser" 사용자가 생성됩니다. 이 사용자는 128개의 가능한 모든 가상 Fabric(-l)에서 "user" 역할(-r)을 갖습니다. 또한 이 사용자는 사용자 수준 액세스 권한이 할당된 필수 "새시" 역할(-c)을 갖습니다.

기본적으로 이 컬렉터는 스위치가 속한 모든 패브릭의 일부인 모든 FOS 장치를 검색하려고 시도합니다.

#### 용어

Data Infrastructure Insights는 Brocade FOS REST 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
스위치	스위치
포트	포트
가상 패브릭, 물리적 패브릭	패브릭
Zone(영역)	Zone(영역)
논리 스위치	논리 스위치
LSAN 구역	IVR 영역

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- Fabric의 모든 스위치에 TCP 연결이 있어야 합니다. 이 데이터 수집기 유형은 패브릭의 각 장치에 대해 HTTP와 HTTPS를 모두 원활하게 시도합니다. fabric\_에서 모든 스위치 검색 확인란을 선택하면 Data Infrastructure Insights에서 패브릭의 모든 스위치를 식별하지만, 이러한 추가 스위치를 검색하려면 TCP 연결이 필요합니다.
- Fabric의 모든 스위치에서 동일한 계정이 전 세계적으로 필요합니다. 장치의 웹 인터페이스를 사용하여 액세스를 확인할 수 있습니다.

#### 구성

필드에 입력합니다	설명
스위치 IP	FOS 스위치의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	스위치의 사용자 이름입니다
암호	스위치에 대한 암호입니다

#### 고급 구성

필드에 입력합니다	설명
제외된 장치	폴링에서 제외할 장치 IPv4 주소의 심표로 구분된 목록입니다.



필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60입니다.
패브릭의 모든 스위치를 살펴보십시오	패브릭의 모든 스위치를 검색하려면 선택합니다.
HBA와 을 선택합니다 영역 별칭	HBA 또는 존 별칭을 사용할지 여부를 선택합니다.
연결 유형	HTTP 또는 HTTPS.
이 설정은 장치별로 먼저 사용을 시도하는 프로토콜 C만 변경합니다. 기본값이 실패할 경우 C가 자동으로 반대 프로토콜을 시도합니다	TCP 포트를 재정의합니다
기본값을 사용하지 않는 경우 포트를 지정합니다.	성능 폴링 간격(초)

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
테스트 기능은 프로토콜에 액세스할 수 없다는 경고 메시지를 표시합니다	특정 Brocade FOS 8.2+ 장치는 HTTP 또는 HTTPS에서만 통신하려고 합니다. - 스위치에 디지털 인증서가 설치되어 있는 경우 암호화되지 않은 HTTP와 HTTPS를 사용하여 통신하려고 하면 스위치에서 HTTP 오류가 발생합니다. 테스트 기능은 HTTP와 HTTPS 모두와 통신을 시도합니다. - 테스트에서 한 프로토콜이 통과한다고 말하면 수집기를 안전하게 저장할 수 있으며 다른 프로토콜이 실패해도 걱정할 필요가 없습니다. 수집기는 수집 중에 두 프로토콜을 모두 시도하며 두 프로토콜이 작동하지 않을 경우에만 실패합니다.
오류: "Data Infrastructure Insights가 잘못된 새시 역할을 수신했습니다."	이 데이터 원본에 구성된 사용자에게 새시 역할 권한이 부여되었는지 확인합니다.
오류: "새시 IP 주소가 일치하지 않습니다."	새시 IP 주소를 사용하도록 데이터 소스 구성을 변경합니다.
403 금지됨으로 인해 재고가 실패합니다	이는 단순히 잘못된 자격 증명이거나, 사용자가 충분히 강력한 역할을 사용하려 한다는 것을 나타낼 수 있습니다. "사용자" 수준의 사용자에게 필요한 "새시 역할" 권한이 없거나 기본값이 아닌 가상 패브릭에 대한 액세스 권한을 볼 수 없다는 점을 기억하십시오.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Cisco MDS Fabric 스위치 데이터 수집기

Data Infrastructure Insights는 Cisco MDS 패브릭 스위치 데이터를 사용하여 Cisco MDS 패브릭 스위치 및 FC 서비스가 활성화된 다양한 Cisco Nexus FCoE 스위치의 인벤토리를 검색합니다.

또한 이 데이터 수집기를 사용하여 NPV 모드에서 실행되는 여러 Cisco 장치 모델을 검색할 수 있습니다.

## 용어

Data Infrastructure Insights는 Cisco FC 스위치 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
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

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 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

## 구성

필드에 입력합니다	설명
Cisco 스위치 IP	스위치의 IP 주소 또는 정규화된 도메인 이름입니다
SNMP 버전	V1, V2 또는 V3을 선택합니다. 성능 획득을 위해서는 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)

필드에 입력합니다	설명
SNMP 개인 정보 보호 암호	SNMP 개인 정보 보호 암호
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
제외된 장치	폴링에서 제외할 장치 IP의 심표로 구분된 목록입니다
포함된 장치	폴링에 포함할 장치 IP의 심표로 구분된 목록입니다
장치 유형을 확인하십시오	자신을 Cisco 장치로 명시적으로 광고하는 장치만 수락하려면 선택합니다
첫 번째 별칭 유형	별칭 해상도에 대한 첫 번째 기본 설정을 제공합니다. 다음 중에서 선택합니다. * Device Alias * 필요에 따라 모든 구성 명령에 사용할 수 있는 포트 WWN(pwwn)의 사용자 친화적인 이름입니다. Cisco MDS 9000 제품군의 모든 스위치는 분산 장치 별칭(장치 별칭)을 지원합니다. * 없음 * 별칭을 보고하지 않습니다. * 포트 설명 * 포트 목록에서 포트를 식별하는 데 도움이 되는 설명입니다. * 존 별칭 (모두) * 활성 구성에만 사용할 수 있는 포트의 사용자 친화적인 이름입니다. 이것이 기본값입니다.
두 번째 별칭 유형	별칭 해상도에 대한 두 번째 기본 설정을 제공합니다
세 번째 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)

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
오류: 새시를 검색하지 못했습니다. 스위치가 검색되지 않았습니다	<ul style="list-style-type: none"> <li>• IP가 구성된 장치에 Ping 수행</li> <li>• Cisco Device Manager GUI를 사용하여 장치에 로그인</li> <li>• CLI를 사용하여 장치에 로그인</li> <li>• SNMP walk를 실행합니다</li> </ul>
오류: 장치가 Cisco MDS 스위치가 아닙니다	<ul style="list-style-type: none"> <li>• 장치에 대해 구성된 데이터 소스 IP가 올바른지 확인</li> <li>• Cisco Device Manager GUI를 사용하여 장치에 로그인</li> <li>• CLI를 사용하여 장치에 로그인</li> </ul>

문제:	다음을 시도해 보십시오.
오류: Data Infrastructure Insights에서 스위치의 WWN을 가져올 수 없습니다.	FC 또는 FCoE 스위치가 아닐 수 있으므로 지원되지 않을 수 있습니다. 데이터 소스에 구성된 IP/FQDN이 실제로 FC/FCoE 스위치인지 확인합니다.
오류: NPV 스위치 포트에 로그인한 노드가 두 개 이상 있습니다	NPV 스위치의 직접 획득을 비활성화합니다
오류: 스위치에 연결할 수 없습니다	<ul style="list-style-type: none"> <li>• 장치가 작동 중인지 확인</li> <li>• IP 주소 및 수신 대기 포트 확인</li> <li>• 장치에 Ping 수행</li> <li>• Cisco Device Manager GUI를 사용하여 장치에 로그인</li> <li>• CLI를 사용하여 장치에 로그인</li> <li>• SNMP walk 실행</li> </ul>

## 성능

문제:	다음을 시도해 보십시오.
오류: SNMP v1에서 성능 획득을 지원하지 않습니다	<ul style="list-style-type: none"> <li>• 데이터 소스 편집 및 스위치 성능 비활성화</li> <li>• SNMP v2 이상을 사용하도록 데이터 소스 및 스위치 구성을 수정합니다</li> </ul>

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## Cohesity SmartFiles 데이터 수집기

이 REST API 기반 수집기는 Cohesity 클러스터를 획득하여 "Views"(Data Infrastructure Insights 내부 볼륨으로) 및 다양한 노드를 검색하고 성능 메트릭을 수집합니다.

### 구성

필드에 입력합니다	설명
Cohesity 클러스터 IP	Cohesity 클러스터의 IP 주소입니다
사용자 이름	Cohesity 클러스터의 사용자 이름입니다
암호	Cohesity 클러스터에 사용되는 암호입니다

### 고급 구성

필드에 입력합니다	설명
TCP 포트	Cohesity 클러스터와의 TCP 통신에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.
성능 폴링 간격(분)	성능 폴링 간격입니다. 기본값은 900초입니다.

### 문제 해결

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## Dell

### Dell EMC XC Series 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Dell EMC XC 시리즈 스토리지 어레이에 대한 인벤토리 및 성능 정보를 검색합니다.

#### 구성

필드에 입력합니다	설명
PRISM 외부 IP 주소	XC 서버의 IP 주소입니다
사용자 이름	XC 서버의 사용자 이름입니다
암호	XC 서버에 사용되는 암호입니다

#### 고급 구성

필드에 입력합니다	설명
TCP 포트	XC 서버와의 TCP 통신에 사용되는 포트입니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.
성능 폴링 간격(분)	성능 폴링 간격입니다. 기본값은 300초입니다.

#### 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Dell EMC

### Dell EMC Data Domain 데이터 수집기

이 데이터 수집기는 Dell EMC Data Domain 중복 제거 스토리지 시스템에서 인벤토리 및 성능 정보를 수집합니다. 이 데이터 수집기를 구성하려면 따라야 하는 특정 구성 지침 및 사용 권장 사항이 있습니다.

#### 용어

Data Infrastructure Insights는 Data Domain Data Collector에서 다음과 같은 인벤토리 정보를 가져옵니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
스토리지	스토리지
FC 포트	포트
파일 시스템	내부 볼륨

공급업체/모델 기간	Data Infrastructure Insights 용어
할당량	할당량
NFS 및 CIFS 공유	파일 공유

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 콜릿의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 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 사이의 간격입니다. 기본값은 20입니다.
SSH 포트	SSH 서비스 포트입니다

문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### EMC ECS 데이터 수집기 구성

이 데이터 수집기는 EMC ECS 스토리지 시스템에서 인벤토리 및 성능 데이터를 가져옵니다. 구성을 위해 Data Collector에는 ECS 클러스터의 IP 주소 또는 호스트 이름과 사용자 이름 및 암호가 필요합니다.



Dell EMC ECS는 다른 물리적 TB에서 관리 단위 비율로 측정됩니다. 40TB의 포맷되지 않은 ECS 용량마다 1개의 용량이 충전됩니다 "[관리 장치\(MU\)](#)".

용어

Data Infrastructure Insights는 ECS 데이터 수집기에서 다음과 같은 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	Data Infrastructure Insights 용어
클러스터	스토리지
테넌트	스토리지 풀
버킷	내부 볼륨
디스크	디스크

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- ECS 클러스터의 IP 주소 또는 호스트 이름입니다
- ECS 시스템의 사용자 이름 및 암호
- 포트 4443(HTTPS). ECS 시스템의 TCP 포트 4443에 대한 아웃바운드 연결이 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 사용자 ID입니다	ECS의 사용자 ID입니다
암호	ECS에 사용되는 암호입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 360분입니다.

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
오류: 사용자 인증에 실패했습니다.	이 장치에 대한 자격 증명이 올바른지 확인하십시오.

#### 성능

문제:	다음을 시도해 보십시오.
오류: 수집된 데이터가 충분하지 않습니다.	<ul style="list-style-type: none"> <li>• 로그 파일에서 수집 타임 스탬프를 확인하고 그에 따라 폴링 간격을 수정합니다.</li> <li>• 더 오랜 시간 동안 기다립니다</li> </ul>

문제:	다음을 시도해 보십시오.
오류: 성능 폴링 간격이 너무 큼니다.	로그 파일 <code>logfile</code> 에서 수집 타임 스탬프를 확인하고 그에 따라 폴링 간격을 수정합니다

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### Dell EMC PowerScale 데이터 수집기

Data Infrastructure Insights는 Dell EMC PowerScale(이전 Isilon) SSH 데이터 수집기를 사용하여 PowerScale 스케일 아웃 NAS 스토리지의 인벤토리 및 성능 데이터를 가져옵니다.

#### 용어

Data Infrastructure Insights는 이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
파일 시스템	내부 볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- PowerScale 스토리지에 대한 관리자 권한
- PowerScale 클러스터의 IP 주소입니다
- 포트 22에 대한 SSH 액세스

#### 구성

필드에 입력합니다	설명
IP 주소입니다	PowerScale 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	PowerScale 클러스터의 사용자 이름입니다
암호	PowerScale 클러스터에 사용되는 암호입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 20입니다.



필드에 입력합니다	설명
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.
SSH 포트	SSH 서비스 포트입니다. 기본값은 22입니다.

문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

인벤토리

문제:	다음을 시도해 보십시오.
"유효하지 않은 로그인 자격 증명" 오류 메시지 "역할 기반 관리를 위해 명령이 활성화되지 않았습니다. 루트 사용자 액세스가 필요합니다."	* 사용자가 장치에서 다음 명령을 실행할 수 있는 권한이 있는지 확인합니다. > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * 마법사에 사용된 자격 증명이 장치 자격 증명과 일치하는지 확인합니다
"내부 오류" 오류 메시지와 함께 "명령 <사용자 명령> 실행이 <현재 권한>과(와) 함께 실패했습니다. sudo 명령 실행 권한 문제"	사용자에게 장치에서 다음 명령을 실행할 수 있는 sudo 권한이 있는지 확인합니다

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

**Dell EMC Isilon/PowerScale REST 데이터 수집기**

Data Infrastructure Insights는 Dell EMC Isilon/PowerScale REST 데이터 수집기를 사용하여 Dell EMC Isilon 또는 PowerScale 스토리지에서 인벤토리 및 성능 데이터를 가져옵니다. 이 Collector는 OneFS 8.0.0+를 실행하는 스토리지를 지원합니다.

용어

Data Infrastructure Insights는 이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
OneFS 파일 시스템	내부 볼륨
OneFS 파일 시스템	스토리지 풀
qtree입니다	qtree입니다

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 사용자 계정 및 암호 이 계정은 admin/root가 아니어야 하지만 서비스 계정에 상당한 수의 읽기 전용 권한을 부여해야 합니다. 아래 표를 참조하십시오
- Dell EMC Isilon/PowerScale 클러스터의 IP 주소/정규화된 도메인 이름입니다
- 포트 8080에 대한 HTTPS 액세스
- OneFS 8.0.0 이상을 실행하는 Isilon/PowerScale 클러스터

권한 이름	설명	R(읽기) 또는 RW(읽기+쓰기)
isi_PRIV_LOGIN_PAPI	플랫폼 API	R
isi_PRIV_SYS_TIME	시간	R
isi_PRIV_AUTH	인증	R
isi_PRIV_ROLE	권한	R
isi_PRIV_devices를 참조하십시오	장치	R
isi_PRIV_EVENT	이벤트	R
isi_PRIV_HDFS입니다	HDFS입니다	R
isi_PRIV_NDMP	NDMP	R
isi_PRIV_NETWORK	네트워크	R
isi_priv_nfs를 선택합니다	NFS 를 참조하십시오	R
isi_PRIV_PAPI_CONFIG	플랫폼 API를 구성합니다	R
isi_PRIV_quota를 입력합니다	할당량	R
isi_PRIV_SmartPools를 참조하십시오	SmartPools를 참조하십시오	R
isi_PRIV_smb입니다	중소기업	R
isi_PRIV_statistics	통계	R
isi_PRIV_SWIFT	스위프트	R
isi_PRIV_JOB_ENGINE	작업 엔진	R

구성

필드에 입력합니다	설명
Isilon IP 주소입니다	Isilon 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Isilon의 사용자 이름입니다
암호	Isilon에 사용되는 암호입니다

## 고급 구성

필드에 입력합니다	설명
HTTPS 포트	기본값은 8080입니다.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 20입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

## 인벤토리

문제:	다음을 시도해 보십시오.
"유효하지 않은 로그인 자격 증명" 오류 메시지 "역할 기반 관리를 위해 명령이 활성화되지 않았습니다. 루트 사용자 액세스가 필요합니다."	* 사용자가 장치에서 다음 명령을 실행할 수 있는 권한이 있는지 확인합니다. > isi version osrelease > isi status -q > isi status -n > isi devices -d %s > isi license * 마법사에 사용된 자격 증명이 장치 자격 증명과 일치하는지 확인합니다
"내부 오류" 오류 메시지와 함께 "명령 <사용자 명령> 실행이 <현재 권한>과(와) 함께 실패했습니다. sudo 명령 실행 권한 문제"	사용자에게 장치에서 다음 명령을 실행할 수 있는 sudo 권한이 있는지 확인합니다

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Dell EMC PowerStore 데이터 수집기

EMC PowerStore 데이터 수집기는 EMC PowerStore 스토리지에서 인벤토리 정보를 수집합니다. 구성을 위해 데이터 수집기는 스토리지 프로세서의 IP 주소와 읽기 전용 사용자 이름 및 암호를 필요로 합니다.

EMC PowerStore 데이터 수집기는 PowerStore가 다른 스토리지 시스템 간에 조정하는 볼륨 간 복제 관계를 수집합니다. Data Infrastructure Insights는 각 PowerStore 클러스터의 스토리지 시스템을 보여 주며 해당 클러스터의 노드 및 스토리지 포트에 대한 인벤토리 데이터를 수집합니다. 스토리지 풀 또는 볼륨 데이터가 수집되지 않습니다.

## 용어

Data Infrastructure Insights는 이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
호스트	호스트
host_volume_mapping을 선택합니다	host_volume_mapping을 선택합니다
하드웨어("extra_details" 객체 아래에 드라이브가 있음): 드라이브	디스크

공급업체/모델 기간	<b>Data Infrastructure Insights 용어</b>
어플라이언스	스토리지 풀
클러스터	스토리지
노드	스토리지노드
fc_port 를 선택합니다	포트
볼륨	볼륨
내부 볼륨	파일 시스템

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 스토리지 프로세서의 IP 주소 또는 정규화된 도메인 이름입니다
- 읽기 전용 사용자 이름 및 암호

#### 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.

Cloud Insight의 PowerStore 성능 수집을 통해 PowerStore의 5분 단위 소스 데이터를 사용할 수 있습니다. 따라서 Data Infrastructure Insights는 5분 간격으로 해당 데이터를 폴링하며, 이는 구성할 수 없습니다.

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

#### Dell EMC RecoverPoint 데이터 수집기

EMC RecoverPoint 데이터 수집기의 주요 활용 사례는 RecoverPoint 스토리지 어플라이언스가 제공하는 볼륨 간 복제 관계를 검색하는 것입니다. 이 Collector는 RecoverPoint 어플라이언스 자체를 검색합니다. Dell/EMC는 이 수집기에서 지원하지 않는

## VM을 위한 VMware 백업 솔루션, 즉 "VM을 위한 RecoverPoint"를 판매합니다

구성을 위해 데이터 수집기는 스토리지 프로세서의 IP 주소와 읽기 전용 사용자 이름 및 암호를 필요로 합니다.

EMC RecoverPoint 데이터 수집기는 RecoverPoint가 다른 스토리지 시스템 간에 조정하는 볼륨 간 복제 관계를 수집합니다. Data Infrastructure Insights는 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

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 스토리지 프로세서의 IP 주소 또는 정규화된 도메인 이름입니다
- 읽기 전용 사용자 이름 및 암호
- 포트 443을 통한 REST API 액세스

### 구성

필드에 입력합니다	설명
RecoverPoint의 주소입니다	RecoverPoint 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	RecoverPoint 클러스터의 사용자 이름입니다
암호	RecoverPoint 클러스터에 사용되는 암호입니다

### 고급 구성

필드에 입력합니다	설명
TCP 포트	RecoverPoint 클러스터에 접속하는 데 사용되는 TCP 포트입니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 20분입니다.
제외된 클러스터	폴링 시 제외할 클러스터 ID 또는 이름의 쉼표로 구분된 목록입니다.

### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

### Dell EMC ScaleIO/PowerFlex 데이터 수집기

ScaleIO/PowerFlex 데이터 수집기는 ScaleIO 및 PowerFlex 스토리지에서 인벤토리 정보를 수집합니다. 이 데이터 수집기를 구성하려면 ScaleIO/PowerFlex 게이트웨이 주소와 관리자 사용자 이름 및 암호가 필요합니다.

## 용어

Data Infrastructure Insights는 ScaleIO/PowerFlex 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
MDM(Meta Data Manager) 클러스터	스토리지
SDS(ScaleIO/PowerFlex 데이터 서버)	스토리지 노드
스토리지 풀	스토리지 풀
볼륨	볼륨
장치	디스크

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

- Admin 사용자 계정에 대한 읽기 전용 액세스
- 포트 요구 사항: HTTPS 포트 443

## 구성

필드에 입력합니다	설명
ScaleIO/PowerFlex 게이트웨이	쉼표(,) 또는 세미콜론(;)으로 구분된 ScaleIO/PowerFlex 게이트웨이의 IP 주소 또는 FQDN
사용자 이름	ScaleIO/PowerFlex 장치에 로그인하는 데 사용되는 관리자 사용자 이름입니다
암호	ScaleIO/PowerFlex 장치에 로그인하는 데 사용되는 암호입니다

## 고급 구성

인벤토리 확인란을 클릭하여 인벤토리 수집을 활성화합니다.

필드에 입력합니다	설명
HTTPS 포트	443
재고 폴링 간격(분)	기본값은 60입니다.
연결 시간 초과(초)	기본값은 60입니다.

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## EMC Unity 데이터 수집기 구성

Dell EMC Unity(이전의 VNXe) 데이터 수집기는 VNXe 유니파이드 스토리지 시스템에 대한 인벤토리 지원을 제공합니다. Data Infrastructure Insights는 현재 iSCSI 및 NAS 프로토콜을 지원합니다.

### 요구 사항

- Unity 데이터 수집기는 CLI를 기반으로 하며, VNXe 데이터 수집기가 있는 획득 장치에 Unisphere for Unity CLI(uemcli.exe)를 설치해야 합니다.
- uemcli.exe 은 전송 프로토콜로 HTTPS를 사용하므로 획득 장치에서 Unity에 대한 HTTPS 연결을 시작할 수 있어야 합니다.
- Unity 장치의 IP 주소 또는 정규화된 도메인 이름입니다
- 데이터 수집기에서 사용할 수 있는 읽기 전용 사용자가 적어도 있어야 합니다.
- 포트 443의 HTTPS가 필요합니다
- EMC Unity 데이터 수집기는 인벤토리에 대한 NAS 및 iSCSI 지원을 제공합니다. Fibre Channel 볼륨은 검색되지만 Data Infrastructure Insights는 FC 매핑, 마스킹 또는 스토리지 포트에 대해 보고하지 않습니다.

### 용어

Data Infrastructure Insights는 Unity 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
스토리지	스토리지
프로세서	스토리지 노드
스토리지 풀	스토리지 풀
일반 iSCSI 블록 정보, VMware VMFS	공유
복제 원격 시스템	동기화
iSCSI 노드	iSCSI 타겟 노드
iSCSI 초기자	iSCSI 대상 초기자

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

### 구성

필드에 입력합니다	설명
Unity 스토리지	Unity 장치의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Unity 장치의 사용자 이름입니다
암호	Unity 장치의 암호입니다

필드에 입력합니다	설명
실행 가능한 UEMCLI에 대한 전체 경로	uemcli.exe_executable이 포함된 폴더의 전체 경로입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40분입니다
Unity CLI 포트	Unity CLI에 사용되는 포트입니다
성능 폴링 간격(초)	기본값은 300입니다.

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
"Failed to execute external utility"(외부 유틸리티 실행 실패) 및 "Failed to find Unisphere executable uemcli" 오류 메시지	* IP 주소, 사용자 이름 및 암호가 올바른지 확인 * Data Infrastructure Insights 획득 유닛에 Unisphere CLI가 설치되어 있는지 확인 * 데이터 소스 구성에서 Unisphere CLI 설치 디렉토리가 올바른지 확인 * 데이터 소스 구성에서 VNXe의 IP가 올바른지 확인합니다. Data Infrastructure Insights 획득 장치에서 CMD를 열고 구성된 설치 디렉터리(\${INSTALLDIR})로 변경합니다. uemcli -d <your IP> -u <your ID>/sys/general show 를 입력하여 VNXe 디바이스에 대한 접속을 시도합니다

추가 정보는 에서 찾을 수 있습니다 ["지원" 페이지](#) 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

#### Dell EMC VMAX 및 PowerMax 장치 제품군 데이터 수집기

Data Infrastructure Insights는 Solutions Enabler symcli 명령을 사용 중인 환경의 기존 Solutions Enabler 서버와 함께 사용하여 EMC VMAX 및 PowerMax 스토리지를 검색합니다. 기존 Solutions Enabler 서버는 게이트키퍼 볼륨에 액세스하여 VMAX/PowerMax 스토리지에 접속할 수 있습니다.

#### 요구 사항

이 데이터 수집기를 구성하기 전에 Data Infrastructure Insights가 기존 Solutions Enabler 서버의 포트 2707에 TCP로 연결되어 있는지 확인해야 합니다. Data Infrastructure Insights는 해당 서버의 "symcfg list" 출력에 표시된 대로 이 서버에 대해 "로컬"인 모든 Symmetrix 스토리지를 검색합니다.

- SMI-S Provider 애플리케이션을 사용하는 EMC Solutions Enabler(CLI)는 획득 유닛 서버에 설치되어 있어야 하며 버전이 Solutions Enabler Server에서 실행 중인 버전과 동일하거나 그 이전이어야 합니다.
- 올바르게 구성된 {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.
- 관리 Solutions Enabler 서버의 IP 주소입니다
- SE(Solutions Enabler) 서버에 대한 관리자 권한
- SE 소프트웨어의 읽기 전용 사용자 이름 및 암호
- Unisphere for VMAX 애플리케이션은 SMI-S Provider 설치를 통해 관리되는 EMC VMAX 및 PowerMax sstorage 스토리지에 대한 통계를 실행 및 수집해야 합니다
- 성능에 대한 액세스 검증: 획득 장치의 웹 브라우저에서 `_https://<SMI-S Hostname or IP>:5989/ecomconfig_`로 이동합니다. 여기서 "SMI-S 호스트 이름 또는 IP"는 SMI-S 서버의 IP 주소 또는 호스트 이름입니다. 이 URL은 EMC SMI-S("ECOM") 서비스의 관리 포털용 URL로, 로그인 팝업을 받게 됩니다.
- 사용 권한은 Solutions Enabler 서버의 데몬 구성 파일에 선언되어야 하며, 일반적으로 `_var/symapi/config/daemon_users_`에서 확인할 수 있습니다

다음은 적절한 cisys 권한이 있는 예제 파일입니다.

```

root@cernciaukc101:/root
14:11:25 # tail /var/symapi/config/daemon_users
###
###      Refer to the storrdfd(3) man page for additional details.
###
###      As noted above, only authorized users can perform stord daemon
control
###      operations (e.g., shutdown).
#####
#####
# smith          storrdfd
cisys storapid <all>

```

용어

Data Infrastructure Insights는 EMC VMAX/PowerMax 데이터 소스에서 다음과 같은 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	Data Infrastructure Insights 용어
디스크	디스크
디스크 그룹	디스크 그룹
스토리지	스토리지
책임자	스토리지 노드
디바이스 풀, SRP(Storage Resource Pool)	스토리지 풀
디바이스 TDEV	볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 구성

- 참고: \* SMI-S 사용자 인증이 활성화되지 않은 경우 Data Infrastructure Insights 데이터 수집기의 기본값이 무시됩니다.

필드에 입력합니다	설명
서비스 이름	_netcnfg_file에 지정된 서비스 이름입니다
CLI의 전체 경로입니다	Symmetrix CLI가 포함된 폴더의 전체 경로입니다
SMI-S 호스트 IP 주소입니다	SMI-S 호스트의 IP 주소입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40분입니다.
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	데이터를 수집할 때 아래 어레이 목록을 포함할지 제외할지 여부를 지정합니다.
인벤토리 필터 장치 목록	포함하거나 제외할 장치 ID의 심프로로 구분된 목록입니다
연결 캐싱	접속 캐싱 방법 선택: * 로컬은 검색할 Symmetrix 스토리지에 대한 Fibre Channel 접속이 있고 게이트키퍼 볼륨에 액세스할 수 있는 Solutions Enabler 서버에서 Cloud Insights 획득 서비스가 실행되고 있음을 의미합니다. 이 문제는 일부 RAU(Remote Acquisition Unit) 구성에서 확인할 수 있습니다. * remote_cached가 기본값이며 대부분의 경우에 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. * 참고: * 이 설정은 "symcfg list" 출력에 의해 원격으로 나열된 스토리지와 관련된 Data Infrastructure Insights 동작을 변경하지 않습니다. Data Infrastructure Insights는 이 명령으로 local로 표시된 장치에서만 데이터를 수집합니다.
SMI-S 프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다. 사용된 기본 포트도 표시합니다.
SMIS-Port를 재정의합니다	비어 있는 경우 연결 유형 필드에서 기본 포트를 사용하고, 그렇지 않으면 사용할 연결 포트를 입력합니다
SMI-S 사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
SMI-S 암호	SMI-S Provider 호스트의 사용자 이름입니다

필드에 입력합니다	설명
성능 폴링 간격(초)	성능 폴링 간격(기본값 1000초)
목록을 지정하려면 '제외' 또는 '포함'을 선택합니다	성능 데이터를 수집할 때 아래 스토리지 목록을 포함할지 제외할지 여부를 지정합니다
성능 필터 장치 목록	포함하거나 제외할 장치 ID의 심프로로 구분된 목록입니다

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

문제:	다음을 시도해 보십시오.
오류: 요청되는 기능에 현재 라이선스가 없습니다	SYMAPI 서버 라이선스를 설치합니다.
오류: 장치를 찾을 수 없습니다	Symmetrix 디바이스가 Solutions Enabler 서버에 의해 관리되도록 구성되었는지 확인합니다. - symcfg list -v를 실행하여 구성된 Symmetrix 디바이스 목록을 확인합니다.
오류: 서비스 파일에서 요청한 네트워크 서비스를 찾을 수 없습니다	Solutions Enabler 서비스 이름이 Solutions Enabler용 netcnfg 파일로 정의되어 있는지 확인합니다. 이 파일은 일반적으로 Solutions Enabler 클라이언트 설치의 SYMAPI\config\ 아래에 있습니다.
오류: 원격 클라이언트/서버 핸드셰이크가 실패했습니다	검색하려는 Solutions Enabler 호스트에서 최신 storsrvd.log * 파일을 확인합니다.
오류: 클라이언트 인증서의 일반 이름이 유효하지 않습니다	Solutions Enabler 서버에서 _hosts_file을 편집하여 획득 장치의 호스트 이름이 Solutions Enabler 서버의 storsrvd.log 에 보고된 IP 주소로 확인되도록 합니다.
오류: 기능이 메모리를 가져올 수 없습니다	시스템에서 Solutions Enabler를 실행할 수 있는 사용 가능한 메모리가 충분한지 확인합니다
오류: Solutions Enabler가 필요한 모든 데이터를 제공할 수 없습니다.	Solutions Enabler의 상태 및 로드 프로필을 조사합니다
오류: • Solutions Enabler 서버 8.x에서 Solutions Enabler 7.x와 함께 수집하면 "symcfg list -tdev" CLI 명령이 잘못된 데이터를 반환할 수 있습니다 • Solutions Enabler Server 8.3 이상에서 Solutions Enabler 8.1.0 이전 버전을 사용하여 취합한 경우 "symcfg list -SRP" CLI 명령은 잘못된 데이터를 반환할 수 있습니다.	동일한 Solutions Enabler 주요 릴리즈를 사용하고 있는지 확인합니다
"알 수 없는 코드" 메시지와 함께 데이터 수집 오류가 표시됩니다.	Solutions Enabler 서버의 데몬 구성 파일에 사용 권한이 선언되지 않은 경우 이 메시지가 표시될 수 있습니다(참조 <a href="#">요구 사항</a> 위) SE 클라이언트 버전이 SE 서버 버전과 일치하는 것으로 가정합니다. 이 오류는 /var/symapi/config/daemon_users 구성 파일에서 필요한 데몬 권한으로 _cisys_user(Solutions Enabler 명령을 실행하는)를 구성하지 않은 경우에도 발생할 수 있습니다. 이 문제를 해결하려면 /var/symapi/config/daemon_users 파일을 편집하고 isys 사용자에게 storapid 데몬에 대해 지정된 <all> 권한이 있는지 확인합니다. 예: 14:11:25#tail/var/symapi/config/daemon_users... 시스의 storapid <all>입니다

추가 정보는 에서 찾을 수 있습니다 "지원" 페이지 또는 에 있습니다 "Data Collector 지원 매트릭스".

## Dell EMC VNX Block Storage(NaviCLI) 데이터 수집기

Data Infrastructure Insights는 Dell EMC VNX Block Storage(NaviSec) 데이터 수집기 (이전의 CLARiX)를 사용하여 인벤토리 및 성능 데이터를 얻습니다.

### 용어

Data Infrastructure Insights는 EMC VNX Block Storage Data Collector에서 다음과 같은 인벤토리 정보를 가져옵니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
스토리지	스토리지
스토리지 프로세서	스토리지 노드
이 풀, RAID 그룹입니다	스토리지 풀
LUN을 클릭합니다	볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

### 요구 사항

데이터를 수집하려면 다음 요구 사항을 충족해야 합니다.

- 각 VNX 블록 스토리지 프로세서의 IP 주소입니다
- VNX 블록 스토리지 시스템에 대한 읽기 전용 Navisphere 사용자 이름 및 암호입니다
- Data Infrastructure Insights AU에 Naviseccli를 설치해야 합니다
- 액세스 검증: Data Infrastructure Insights AU에서 사용자 이름과 암호를 사용하여 각 스토리지에 NaviSecCLI를 실행합니다.
- 포트 요구 사항: 80, 443
- naviseccli 버전이 스토리지의 최신 FLARE 코드와 일치해야 합니다
- 성능을 위해서는 통계 로깅을 활성화해야 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> 명령
```

### 구성

필드에 입력합니다	설명
VNX Block 스토리지 IP 주소입니다	VNX 블록 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다

필드에 입력합니다	설명
사용자 이름	VNX 블록 스토리지 디바이스에 로그인하는 데 사용되는 이름입니다.
암호	VNX 블록 스토리지 디바이스에 로그인하는 데 사용되는 암호입니다.
naviseccli.exe 의 CLI 경로	_naviseccli.exe_ 실행 파일이 포함된 폴더의 전체 경로입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40분입니다.
범위	보안 클라이언트 범위 기본값은 Global 입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
오류: <ul style="list-style-type: none"> <li>• 에이전트가 실행되고 있지</li> <li>• naviseccli를 찾지 못했습니다</li> <li>• 명령을 실행하지 못했습니다</li> </ul>	<ul style="list-style-type: none"> <li>• Navisphere CLI가 Cloud Insight 수집 장치에 설치되어 있는지 확인합니다</li> <li>• 데이터 수집기 구성 마법사에서 "보안 클라이언트 사용" 옵션을 선택하지 않았으며 Navisphere CLI의 비보안 버전이 설치되어 있지 않습니다.</li> <li>• 데이터 수집기 구성에서 Navisphere CLI 설치 디렉토리가 올바른지 확인합니다</li> <li>• Data Collector 구성에서 VNX 블록 스토리지의 IP가 올바른지 확인합니다.</li> <li>• Data Infrastructure Insights 수집 장치에서:             <ul style="list-style-type: none"> <li>◦ CMD를 엽니다.</li> <li>◦ 디렉토리를 구성된 설치 디렉토리로 변경합니다</li> <li>◦ "navicli -h{ip} getagent"를 입력하여 VNX 블록 스토리지 디바이스와 연결을 시도합니다({IP}를 실제 IP로 대체).</li> </ul> </li> </ul>

문제:	다음을 시도해 보십시오.
오류: 4.29 emc235848 emc241018 getall에서 호스트 별칭 정보를 구문 분석하지 못했습니다	이는 스토리지 자체에 있는 호스트 이니시에이터 데이터베이스의 FLARE 29 손상 문제로 인해 발생할 수 있습니다. EMC 기술 자료 문서 emc235848, emc241018을 참조하십시오. 또한 확인할 수도 있습니다 <a href="https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128">https://now.netapp.com/Knowledgebase/solutionarea.asp?id=kb58128</a>
오류: 메타 LUN을 검색할 수 없습니다. Java-jar navicli.jar 실행 중 오류가 발생했습니다	<ul style="list-style-type: none"> <li>• 보안 클라이언트를 사용하도록 데이터 수집기 구성 수정(권장)</li> <li>• NaviCLI.exe 또는 naviseccli.exe 의 CLI 경로에 navicli.jar 을 설치합니다</li> <li>• 참고: EMC Navisphere 버전 6.26에서는 navicli.jar 버전이 더 이상 사용되지 않습니다</li> <li>• navicli.jar 은 <a href="http://powerlink.emc.com">http://powerlink.emc.com</a> 에서 이용할 수 있습니다</li> </ul>
오류: 구성된 IP 주소의 서비스 프로세서에서 스토리지 폴이 디스크를 보고하지 않습니다	두 서비스 프로세서 IP를 심표로 구분하여 데이터 수집기를 구성합니다
오류: 수정본 불일치 오류입니다	<ul style="list-style-type: none"> <li>• 이 문제는 대개 VNX 블록 스토리지 디바이스에서 펌웨어를 업데이트하지만 NaviCLI.exe 설치를 업데이트하지 않아 발생합니다. 다른 펌웨어를 사용하는 다른 장치가 있지만 하나의 CLI만 설치된 경우(다른 펌웨어 버전 사용) 이 문제가 발생할 수도 있습니다.</li> <li>• 디바이스와 호스트가 모두 동일한 버전의 소프트웨어를 실행하고 있는지 확인합니다. <ul style="list-style-type: none"> <li>◦ Data Infrastructure Insights Acquisition Unit(Data Infrastructure Insights 획득 장치)에서 명령줄 창을 엽니다</li> <li>◦ 디렉토리를 구성된 설치 디렉토리로 변경합니다</li> <li>◦ "navicli -h &lt;ip&gt; getagent"를 입력하여 CLARiX 디바이스에 접속합니다.</li> <li>◦ 처음 두 줄의 버전 번호를 찾습니다. 예: "에이전트 수정: 6.16.2(0.1)"</li> <li>◦ 첫 번째 줄에서 버전을 찾아 비교합니다. 예: "Navisphere CLI 개정 6.07.00.04.07"</li> </ul> </li> </ul>
오류: 지원되지 않는 구성 - Fibre Channel 포트가 없습니다	디바이스가 Fibre Channel 포트가 구성되어 있지 않습니다. 현재 FC 구성만 지원됩니다. 이 버전/펌웨어가 지원되는지 확인합니다.

추가 정보는 에서 찾을 수 있습니다 "지원" 페이지 또는 에 있습니다 "Data Collector 지원 매트릭스".

## Dell EMC VNX File(이전의 Celerra Unified Storage System) 데이터 수집기

이 데이터 수집기는 VNX File Storage System에서 인벤토리 정보를 가져옵니다. 구성을 위해 이 데이터 수집기는 스토리지 프로세서의 IP 주소와 읽기 전용 사용자 이름 및 암호가 필요합니다.

### 용어

Data Infrastructure Insights는 VNX File Data Collector에서 다음과 같은 인벤토리 정보를 가져옵니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
Celerra Network Server/Celerra 스토리지 풀입니다	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

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 요구 사항

이 데이터 수집기를 구성하려면 다음이 필요합니다.

- 스토리지 프로세서의 IP 주소입니다
- 읽기 전용 사용자 이름 및 암호
- SSH 포트 22

### 구성

필드에 입력합니다	설명
VNX File IP 주소입니다	VNX File 디바이스의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	VNX File 디바이스에 로그인하는 데 사용되는 이름입니다
암호	VNX File 디바이스에 로그인하는 데 사용되는 암호입니다

### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 20분입니다.

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
오류: DART 업데이트가 진행되는 동안 계속할 수 없습니다	가능한 해결 방법: 데이터 수집기를 일시 중지하고 DART 업그레이드가 완료될 때까지 기다린 후 다른 획득 요청을 시도하십시오.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### Dell EMC VNX Unified 데이터 수집기 구성

구성을 위해 Dell EMC VNX Unified(SSH) 데이터 수집기는 Control Station의 IP 주소와 읽기 전용 사용자 이름 및 암호를 필요로 합니다.

### 용어

Data Infrastructure Insights는 이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
디스크 폴더	디스크 그룹
파일 시스템	내부 볼륨
스토리지	스토리지
스토리지 프로세서	스토리지 노드
스토리지 풀, RAID 그룹	스토리지 풀
LUN을 클릭합니다	볼륨
Data Mover입니다	컨트롤러
Data Mover에 마운트된 파일 시스템입니다	파일 공유
CIFS 및 NFS 익스포트	공유
디스크 볼륨	백엔드 LUN

### 요구 사항

VNX(SSH) 데이터 수집기를 구성하려면 다음이 필요합니다.

- Celerra Control Station에 대한 VNX IP 주소 및 자격 증명
- 읽기 전용 사용자 이름 및 암호.
- 데이터 수집기는 DART OS NAS 헤드를 활용하여 백엔드 스토리지에 대해 NaviCLI/NaviSecCLI 명령을 실행할



수 있습니다

### 구성

필드에 입력합니다	설명
VNX IP 주소입니다	VNX Control Station의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	VNX Control Station의 사용자 이름입니다
암호	VNX Control Station의 암호입니다

### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40분입니다.
성능 폴링 간격(초).	성능 폴링 간격입니다. 기본값은 300초입니다.

### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

### EMC VPLEX 데이터 수집기 구성

이 데이터 수집기는 EMC VPLEX 스토리지 시스템에서 인벤토리 및 성능 데이터를 가져옵니다. 구성을 위해 데이터 수집기는 VPLEX 서버의 IP 주소와 관리 수준 도메인 계정이 필요합니다.



Data Infrastructure Insights가 SCP 기반 파일 복제본을 통해 검색하는 .csv 파일 및 로그를 채우려면 VPLEX 클러스터에서 Data Infrastructure Insights의 성능 아카이브 서비스가 작동해야 합니다. NetApp은 많은 VPLEX 펌웨어 업그레이드/관리 스테이션 업데이트로 인해 이 기능이 작동하지 않는 것을 목격했습니다. 이러한 업그레이드를 계획 중인 고객은 계획된 업그레이드로 인해 이 기능이 작동 불능 상태가 될 수 있는지 사전에 Dell/EMC에 문의할 수 있으며, 그러한 경우 성능 가시성의 차이를 최소화하기 위해 어떻게 다시 활성화할 수 있습니까? Cloud Insight의 VPLEX 성능 코드는 각 폴링에서 예상되는 모든 파일이 있는지, 그리고 파일이 제대로 업데이트되는지 평가합니다. 파일이 누락되었거나 오래된 경우 Data Infrastructure Insights에서 성능 수집 오류를 기록합니다.

### 용어

Data Infrastructure Insightst는 VPLEX 데이터 수집기에서 다음과 같은 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	Data Infrastructure Insights 용어
클러스터	스토리지
엔진	스토리지 노드
장치, 시스템 범위	백엔드 스토리지 풀입니다
가상 볼륨	볼륨

공급업체/모델 기간	Data Infrastructure Insights 용어
프런트엔드 포트, 백엔드 포트	포트
분산 장치	저장소 동기화
스토리지 보기	볼륨 맵, 볼륨 마스크
스토리지 볼륨	백엔드 LUN
ITL	백엔드 경로

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- VPLEX Management Console의 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.

#### 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
성능 원격 IP 주소	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. 기본값은 443입니다.
재고 폴링 간격(분)	기본값은 20분입니다.
연결 재시도 횟수입니다	기본값은 3입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 600초입니다.
재시도 횟수	기본값은 2입니다.

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
오류: 사용자 인증에 실패했습니다.	이 장치에 대한 자격 증명이 올바른지 확인하십시오.

### 성능

문제:	다음을 시도해 보십시오.
오류: 5.3 이하 버전의 VPLEX 성능은 지원되지 않습니다.	VPLEX를 5.3 이상으로 업그레이드합니다
오류: 수집된 데이터가 충분하지 않습니다.	• 로그 파일에서 수집 타임 스탬프를 확인하고 그에 따라 폴링 간격을 수정합니다. • 더 오랜 시간 동안 기다립니다
오류: 영구 로그 파일이 업데이트되지 않습니다.	영구 로그 파일을 업데이트하려면 EMC 지원 부서에 문의하십시오
오류: 성능 폴링 간격이 너무 큼니다.	로그 파일 $\{\logfile\}$ 에서 수집 타임 스탬프를 확인하고 그에 따라 폴링 간격을 수정합니다
오류: VPLEX 관리 콘솔의 성능 원격 IP 주소가 구성되지 않았습니다.	데이터 소스를 편집하여 VPLEX Management Console의 Performance Remote IP 주소를 설정합니다.
오류: 디렉터에서 보고된 성능 데이터가 없습니다	• 시스템 성능 모니터가 올바르게 실행되고 있는지 확인하십시오. • 시스템 성능 모니터 로그 파일을 업데이트하려면 EMC 지원 부서에 문의하십시오

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Dell EMC XtremIO 데이터 수집기

EMC XtremIO 데이터 수집기는 EMC XtremIO 스토리지 시스템에서 인벤토리 및 성능 데이터를 가져옵니다.

### 요구 사항

EMC XtremIO(HTTP) 데이터 수집기를 구성하려면 다음이 필요합니다.

- XtremIO 관리 서버(XMS) 호스트 주소
- 관리자 권한이 있는 계정입니다
- 포트 443(HTTPS)에 대한 액세스

### 용어

Data Infrastructure Insights는 EMC XtremIO 데이터 수집기에서 다음 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 소스를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	<b>Data Infrastructure Insights 용어</b>
디스크(SSD)	디스크
클러스터	스토리지
컨트롤러	스토리지 노드
볼륨	볼륨
LUN 매핑	볼륨 맵
타겟 FC 이니시에이터	볼륨 마스크

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- XtremIO 관리 서버(XMS) 호스트 IP 주소
- XtremIO의 관리자 사용자 이름 및 암호

#### 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 포트입니다. 기본값은 443입니다.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Fujitsu ETERNUS 데이터 수집기

Fujitsu ETERNUS 데이터 수집기는 스토리지 시스템에 대한 관리 수준 액세스를 사용하여 인벤토리 데이터를 가져옵니다.

## 용어

Data Infrastructure Insights는 Fujitsu ETERNUS 스토리지에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
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), 유연한 계층 볼륨(FTV), 와이드 스트라이핑 볼륨(WSV)	볼륨
채널 어댑터	컨트롤러

참고: 일반적인 용어 매핑일 뿐이며 이 데이터 수집의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

이 데이터 수집기를 구성하려면 다음이 필요합니다.

- ETERNUS 저장소의 IP 주소로, 침표로 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	ETERNUS 저장 장치의 암호입니다

## 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 20분입니다.

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

## 인벤토리

문제:	다음을 시도해 보십시오.
"Error Retrieving data(데이터 검색 오류)" 및 "Error finding Prompt CLI(프롬프트 프롬프트 CLI를 찾는 동안 오류 발생)" 또는 "Error finding prompt at end of shell results(셸 결과	발생 원인: 스토리지 시스템에 페이지 스크롤이 활성화되어 있습니다. 가능한 해결 방법: * set clienv -show -more -scroll disable 명령을 실행하여 페이지 스크롤을 해제해 보십시오
"Connecting error(연결 오류)"와 "Failed to instantiate an SSH connection to storage(스토리지에 대한 SSH 연결을 인스턴스화하지 못했습니다)" 또는 "Failed to instantiate a connection to VirtualCenter(VirtualCenter 연결을 인스턴스화하지 못했습니다)"라는 오류 메시지	가능한 원인: * 잘못된 자격 증명. * 잘못된 IP 주소입니다. * 네트워크 문제. * 스토리지가 중단되거나 응답하지 않을 수 있습니다. 가능한 해결 방법: * 입력한 자격 증명 및 IP 주소를 확인합니다. * SSH 클라이언트를 사용하여 스토리지와 통신을 시도합니다.

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## NetApp Google Compute 데이터 수집기입니다

이 데이터 수집기는 Google Compute 클라우드 플랫폼 구성의 인벤토리 및 성능 수집을 지원합니다. 이 수집기는 하나의 Google 조직 내의 모든 프로젝트 내의 모든 컴퓨팅 리소스를 검색합니다. Data Infrastructure Insights로 검색할 Google 조직이 여러 개 있는 경우 조직당 하나의 Data Infrastructure Insights 수집기를 배포해야 합니다.

### 구성

필드에 입력합니다	설명
조직 ID입니다	이 수집기로 검색할 조직 ID입니다. 서비스 계정이 둘 이상의 조직을 볼 수 있는 경우 이 필드는 필수입니다
GCP 프로젝트를 ID로 필터링하려면 '제외' 또는 '포함'을 선택하십시오	Data Infrastructure Insights에 가져올 프로젝트 리소스를 제한하려는 경우
프로젝트 ID	"제외 선택"..." 값의 값에 따라 검색 또는 검색에서 필터링하려는 프로젝트 ID 목록입니다. 기본 목록은 비어 있습니다
클라이언트 ID입니다	Google Cloud Platform 구성의 클라이언트 ID입니다
여기에 Google 자격 증명 파일의 내용을 복사하여 붙여 넣습니다	클라우드 플랫폼 계정에 대한 Google 자격 증명을 이 필드에 복사합니다

### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다
'제외' 또는 '포함'을 선택하여 레이블별로 VM 필터링에 적용합니다	데이터를 수집할 때 레이블별로 VM을 포함할지 제외할지 여부를 지정합니다. '포함'을 선택한 경우 라벨 키 필드는 비워 둘 수 없습니다.

필드에 입력합니다	설명
VM을 필터링할 키 및 값에 레이블을 지정합니다	VM의 레이블 키 및 값과 일치하는 키와 값을 필터링하여 포함/제외할 VM(및 연결된 디스크)을 선택하려면 * + 필터 레이블 * 을 클릭합니다. 레이블 키는 필수 항목이며 레이블 값은 선택 사항입니다. 레이블 값이 비어 있으면 레이블 키와 일치하는 한 VM이 필터링됩니다.
성능 폴링 간격(초)	기본값은 1800초입니다

## 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## HP 엔터프라이즈

### HP Enterprise Alletra 9000/Primera Storage 데이터 수집기

Data Infrastructure Insights는 HP Enterprise Alletra 9000/HP Enterprise Primera(이전 3PAR) 데이터 수집기를 사용하여 인벤토리 및 성능을 검색합니다.

## 용어

Data Infrastructure Insights는 이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

필드에 입력합니다	설명
물리 디스크	디스크
스토리지 시스템	스토리지
컨트롤러 노드	스토리지 노드
공통 프로비저닝 그룹	스토리지 풀
가상 볼륨	볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

이 데이터 수집기를 구성하려면 다음이 필요합니다.

- InServ 클러스터의 IP 주소 또는 FQDN입니다
- 인벤토리의 경우 StoreServ 서버에 대한 읽기 전용 사용자 이름 및 암호입니다
- 성능을 위해 StoreServ 서버에 대한 읽기-쓰기 사용자 이름 및 암호
- 포트 요구 사항: 22(인벤토리 수집), 5988 또는 5989(성능 수집) [참고: 성능은 StoreServ OS 3.x+에서 지원됩니다.]
- 성능 수집을 위해 SSH를 통해 스토리지에 로그인하여 SMI-S가 설정되어 있는지 확인합니다.

## 구성

필드에 입력합니다	설명
스토리지 IP 주소입니다	StoreServ 클러스터의 스토리지 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	StoreServ 서버의 사용자 이름입니다
암호	StoreServ 서버에 사용되는 암호입니다
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 사이의 간격입니다. 기본값은 40분입니다.
SMI-S 접속	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다
SMI-S 기본 포트를 재정의합니다	비어 있는 경우 SMI-S 접속의 기본 포트를 사용하고, 그렇지 않은 경우 사용할 접속 포트를 입력합니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
"showsys" 명령으로 결과가 반환되지 않습니다.	명령줄에서 "showsys" 및 "showversion -a"를 실행하고 버전이 스토리지에서 지원되는지 확인합니다.

### 성능

문제:	다음을 시도해 보십시오.
연결 또는 로그인하지 못했습니다. 공급자 초기화에 실패했습니다.	숫자로만 구성된 스토리지 이름은 SMI-S 서버에 문제를 일으킬 수 있습니다. 스토리지 이름을 변경해 보십시오.
구성된 SMI-S 사용자에게 도메인이 없습니다	구성된 SMI-S 사용자에게 적절한 도메인 권한을 부여합니다
Data Infrastructure Insights는 SMI-S 서비스에 연결 /로그인할 수 없다고 합니다.	CI AU와 스토리지 사이에 5988 또는 5989로의 TCP 연결을 차단하는 방화벽이 없는지 확인합니다. 이 작업이 완료되고 방화벽이 없음을 확인한 경우 어레이에 SSH를 사용하고 "showcim" 명령을 사용하여 확인해야 합니다. 서비스 활성화 여부 확인 * HTTPS가 활성화되어 있는지 * HTTPS 포트는 5989여야 합니다. 모든 포트가 활성화되어 있으면 "stopcim"을 수행한 다음 "startcim"을 시도하여 CIM을 다시 시작할 수 있습니다(예 SMI-S 서비스).



추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## HP Enterprise Command View 데이터 수집기

HP Enterprise Command View Advanced Edition 데이터 수집기는 CVAE(Command View Advanced Edition) 서버를 통해 XP 및 P9500 어레이 검색을 지원합니다. Data Infrastructure Insights는 표준 Command View API를 사용하여 CVAE와 통신하여 인벤토리 및 성능 데이터를 수집합니다.

### 용어

Data Infrastructure Insights는 HP Enterprise Command View 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
개발	디스크
저널 풀	디스크 그룹
스토리지	스토리지
포트 컨트롤러	스토리지 노드
스토리지 그룹, DP 풀	스토리지 풀
논리 유닛, LDEV	볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 재고 요건

재고 데이터를 수집하려면 다음이 있어야 합니다.

- CVAE 서버의 IP 주소입니다
- CVAE 소프트웨어 및 피어 권한에 대한 읽기 전용 사용자 이름 및 암호입니다
- 포트 요구 사항: 2001

### 성능 요구사항

성능 데이터를 수집하려면 다음 요구사항을 충족해야 합니다.

- HDS USP, USP V 및 VSP 성능
  - 성능 모니터에 라이선스가 있어야 합니다.
  - 모니터링 스위치를 활성화해야 합니다.
  - 내보내기 도구(Export.exe)를 Data Infrastructure Insights AU에 복사하고 위치로 추출해야 합니다. CI Linux AUS에서 "cisys"에 읽기 및 실행 권한이 있는지 확인합니다.
  - 내보내기 도구 버전은 대상 스토리지의 마이크로코드 버전과 일치해야 합니다.
- AMS 성능:

- 성능 모니터에 라이선스가 있어야 합니다.
- SNM2(Storage Navigator Modular 2) CLI 유틸리티는 Data Infrastructure Insights AU에 설치됩니다.
- 네트워크 요구 사항
  - 내보내기 도구는 Java 기반이며, RMI를 사용하여 스토리지와 통화할 수 있습니다. 이러한 도구는 각 호출에서 소스 및 대상 TCP 포트를 동적으로 협상할 수 있기 때문에 방화벽에는 적합하지 않을 수 있습니다. 또한, 모델 스토리지의 내보내기 도구는 네트워크 전체에서 다르게 작동할 수 있습니다. 모델의 요구 사항은 HPE를 참조하십시오

구성

필드에 입력합니다	설명
명령 보기 서버	Command View 서버의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	Command View 서버의 사용자 이름입니다.
암호	Command View 서버에 사용되는 암호입니다.
디바이스 - VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지	VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지를 위한 장치 목록입니다. 각 스토리지에는 * 스토리지의 IP:IP 주소가 필요합니다. * 사용자 이름: 스토리지의 사용자 이름 * 암호: 내보내기 유틸리티 jar 파일이 포함된 저장소 * 폴더의 암호입니다
SNM2Devices - WMS/SMS/AMS 저장소	WMS/SMS/AMS 저장소에 대한 장치 목록입니다. 각 스토리지에는 * 스토리지의 IP:IP 주소가 필요합니다. * Storage Navigator CLI 경로: SNM2 CLI 경로 * 계정 인증 유효: 유효한 계정 인증을 선택하려면 선택합니다. * 사용자 이름: 스토리지의 사용자 이름 * 암호: 암호
성능 조정 관리자 를 선택합니다	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

참고: HDS USP, USP V 및 VSP에서 모든 디스크는 둘 이상의 스토리지 그룹에 속할 수 있습니다.

고급 구성

필드에 입력합니다	설명
명령 보기 서버 포트	Command View Server에 사용되는 포트입니다
HTTPS가 활성화되었습니다	HTTPS를 활성화하려면 선택합니다
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 제외 또는 포함	포함하거나 제외할 장치 ID 또는 배열 이름의 심표로 구분된 목록입니다

호스트 관리자를 쿼리합니다	호스트 관리자를 쿼리하려면 선택합니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300입니다.

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
오류: 사용자에게 충분한 권한이 없습니다	더 많은 권한이 있는 다른 사용자 계정을 사용하거나 데이터 수집기에 구성된 사용자 계정의 권한을 늘리십시오
오류: 저장소 목록이 비어 있습니다. 장치가 구성되지 않았거나 사용자에게 충분한 권한이 없습니다	* 장치가 구성되었는지 확인하려면 DeviceManager를 사용합니다. * 더 많은 권한이 있는 다른 사용자 계정을 사용하거나 사용자 계정의 권한을 늘리십시오
오류: HDS 스토리지 어레이가 며칠 동안 새로 고쳐지지 않았습니다	HP CommandView AE에서 이 어레이가 새로 고쳐지지 않는 이유를 조사합니다.

#### 성능

문제:	다음을 시도해 보십시오.
오류: * 내보내기 유틸리티 실행 중 오류 * 외부 명령 실행 중 오류	* 데이터 인프라 인사이트 획득 장치에 내보내기 유틸리티가 설치되어 있는지 확인 * 데이터 수집기 구성에서 내보내기 유틸리티 위치가 올바른지 확인 * 데이터 수집기 구성에서 USP/R600 어레이의 IP가 올바른지 확인 * 데이터 수집기 구성에서 사용자 이름 및 암호가 올바른지 확인 * 구성 된 마이크로 어레이 코드와 호환되는지 확인 후 CMD 스토리지 디렉토리 내보내기를 사용하여 구성 runWin.bat
오류: 대상 IP에 대한 내보내기 도구 로그인에 실패했습니다	* 사용자 이름/암호가 올바른지 확인 * 이 HDS 데이터 수집기에 대한 사용자 ID 생성 * 이 어레이를 획득하도록 구성된 다른 데이터 수집기가 없는지 확인합니다
오류: Export tools logged "Unable to get time range for monitoring".	* 스토리지에서 성능 모니터링이 활성화되었는지 확인합니다. * Data Infrastructure Insights 외부에서 내보내기 도구를 호출하여 문제가 Data Infrastructure Insights 외부에 있는지 확인하십시오.
오류: * 구성 오류: 스토리지 어레이가 내보내기 유틸리티에서 지원되지 않음 * 구성 오류: 스토리지 어레이가 Storage Navigator Modular CLI에서 지원되지 않습니다	* 지원되는 스토리지 어레이만 구성합니다. * "장치 목록 필터"를 사용하여 지원되지 않는 스토리지 배열을 제외합니다.
오류: * 외부 명령 실행 중 오류 * 구성 오류: 스토리지 어레이가 인벤토리에서 보고되지 않음 * 구성 오류: 내보내기 폴더에 jar 파일이 없습니다	* 내보내기 유틸리티 위치를 확인합니다. * 문제가 되는 스토리지 배열이 Command View 서버에 구성되어 있는지 확인합니다. * 성능 폴링 간격을 60초의 배수로 설정합니다.

문제:	다음을 시도해 보십시오.
오류: * 오류 Storage navigator CLI * auperform 명령 실행 중 오류 * 외부 명령 실행 중 오류	* Storage Navigator Modular CLI가 데이터 인프라 인사이트 획득 장치에 설치되어 있는지 확인 * Storage Navigator Modular CLI 위치가 데이터 수집기 구성에서 올바른지 확인 * 데이터 수집기 구성에 WMS/SMS/SMS 어레이의 IP가 올바른지 확인 * Storage Navigator Modular CLI 버전이 데이터 수집기의 마이크로 코드 버전과 호환되는지 확인 * 다음과 같이 구성된 스토리지 참조 디렉토리에서 "CMD-exe"를 실행하여 스토리지 구성 해제 명령을 실행하여 스토리지 디렉토리를 여십시오.
오류: 구성 오류: 인벤토리에서 스토리지 배열을 보고하지 않았습니다	Command View 서버에 해당 스토리지 배열이 구성되어 있는지 확인합니다
오류: * 스토리지가 Storage Navigator에 등록되지 않았습니다. Modular 2 CLI * 어레이가 Storage Navigator에 등록되지 않았습니다. Modular 2 CLI * 구성 오류: 스토리지 어레이가 StorageNavigator Modular CLI에 등록되지 않았습니다	* 명령 프롬프트를 열고 디렉터리를 구성된 경로로 변경합니다. * "set=STONAVM_HOME=" 명령을 실행합니다. * "autunitref" 명령 실행 * 출력에 배열 세부 정보가 포함되어 있지 않은 경우 명령 출력에 IP * 가 포함된 배열의 세부 정보가 포함되어 있는지 확인하고 Storage Navigator CLI를 사용하여 어레이를 등록합니다. -명령 프롬프트를 열고 디렉터리를 구성된 경로로 변경합니다. -"set=STONAVM_HOME=" 명령을 실행합니다. -"aunitaddauto-ip \${ip}" 명령을 실행합니다. \${ip}을(를) 실제 IP로 바꿉니다

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### HPE Alletra 6000 데이터 수집기

HP Enterprise Alletra 6000(이전의 Nimble) 데이터 수집기는 Alletra 6000 스토리지 어레이의 인벤토리 및 성능 데이터를 지원합니다.

#### 용어

Data Infrastructure Insights는 이 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
스토리지	스토리지
디스크	디스크
볼륨	볼륨
수영장	스토리지 풀
이니시에이터	스토리지 호스트 별칭입니다
컨트롤러	스토리지 노드
Fibre Channel 인터페이스	컨트롤러

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

스토리지 시스템에서 인벤토리 및 구성 데이터를 수집하려면 다음이 있어야 합니다.

- 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.
- "Operator" 수준 이상의 역할을 가진 어레이에 대한 유효한 사용자 이름과 암호가 있어야 합니다. "게스트" 역할에 이니시에이터 구성을 이해할 수 있는 충분한 액세스 권한이 없습니다.
- 포트 5392가 어레이에서 열려 있어야 합니다.

스토리지 어레이에서 성능 데이터를 수집하려면 다음이 있어야 합니다.

- 스토리지에서 NimbleOS 4.0.0 이상을 실행해야 합니다
- 어레이에 볼륨이 구성되어 있어야 합니다. NimbleOS의 유일한 성능 API는 볼륨에 대한 것이며 모든 통계 Data Infrastructure Insights 보고서는 볼륨 통계에서 도출됩니다

## 구성

필드에 입력합니다	설명
스토리지 관리 IP 주소입니다	FQDN(정규화된 도메인 이름) 또는 스토리지 관리 IP 주소입니다.
사용자 이름	스토리지의 사용자 이름입니다
암호	어레이의 암호입니다

## 고급 구성

필드에 입력합니다	설명
포트	Nimble REST API에서 사용하는 포트입니다. 기본값은 5392입니다.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.

참고: 기본 성능 폴링 간격은 300초이며 변경할 수 없습니다. 이 간격은 HPE Alletra 6000에서 유일하게 지원됩니다.

## Hitachi Data Systems를 통해

### Hitachi Vantara Command Suite 데이터 수집기

Hitachi Vantara Command Suite 데이터 수집기는 HiCommand Device Manager 서버를 지원합니다. Data Infrastructure Insights는 표준 HiCommand API를 사용하여 HiCommand Device Manager 서버와 통신합니다.

## 용어

Data Infrastructure Insights는 Hitachi Vantara Command Suite 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가

표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
개발	디스크
저널 풀	디스크 그룹
스토리지	스토리지
포트 컨트롤러	스토리지 노드
어레이 그룹, HDS 풀	스토리지 풀
논리 유닛, LDEV	볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 스토리지

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 "name" 속성에서 직접 가져옵니다
- 모델 - GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 "arrayType" 특성에서 직접 제공됩니다
- 공급업체 – HDS
- 제품군 - GetStorageArray XML API 호출을 통해 HDS HiCommand Device Manager의 "arrayFamily" 특성에서 직접 제공됩니다
- IP – 어레이의 모든 IP 주소 목록이 아니라 어레이의 관리 IP 주소입니다
- 물리적 용량 – 디스크 역할에 관계없이 이 시스템에 있는 모든 디스크의 총 용량 합계를 나타내는 Base2 값입니다.

### 스토리지 풀

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 이외의 용도로 전용인 경우(예: 저널링, 스냅샷)
  - 씬 프로비저닝 - HDP 풀인 경우
  - RAID 그룹 – 다음과 같은 몇 가지 이유로 볼 수 없습니다.

Data Infrastructure Insights는 모든 비용에서 용량을 두 배로 늘리는 것을 피한다는 강력한 입장을 취하고 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. Data Infrastructure Insights에서 기본 RAID 그룹과 풀을 모두 그대로 보고하면 해당 기본 용량의 합계가 디스크 합계를 크게 초과합니다.

대신 Data Infrastructure Insights의 HDS Command Suite 데이터 수집기는 풀 볼륨의 용량별로 RAID Group의 크기를 임의로 축소합니다. 이로 인해 Data Infrastructure Insights가 RAID 그룹을 전혀 보고하지 않을 수

있습니다. 또한 결과 RAID 그룹은 Data Infrastructure Insights WebUI에 표시되지 않지만 DWH(Data Infrastructure Insights Data Warehouse)로 전달되도록 플래그가 지정됩니다. 이러한 의사 결정의 목적은 대부분의 사용자가 신경 쓰지 않는 것에 대한 UI 혼란을 방지하는 것입니다. HDS 어레이에 50MB의 여유 공간이 있는 RAID 그룹이 있는 경우 의미 있는 결과를 얻기 위해 이 여유 공간을 사용할 수 없습니다.

- 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 합계에 의해 이 비율에 의해 초과 할당되었습니다."라는 파생된 값입니다.
- 스냅샷 - 이 풀의 스냅샷 사용을 위해 예약된 용량을 표시합니다

## 스토리지 노드

다음 용어는 HDS 스토리지 노드 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

- 이름 - 모놀리식 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 모든 포트에 매핑된 볼륨이 표시됩니다

## 재고 요건

재고 데이터를 수집하려면 다음이 있어야 합니다.

- 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)
- 사용자 이름과 암호를 사용하여 HiCommand Device Manager 소프트웨어에 로그인합니다
- HiCommand 장치 관리자\http://<HiCommand\_Device\_Manager\_IP>:2001/service/StorageManager에 대한 액세스를 확인합니다

## 성능 요구사항

성능 데이터를 수집하려면 다음 요구사항을 충족해야 합니다.

- HDS USP, USP V 및 VSP 성능
  - 성능 모니터에 라이선스가 있어야 합니다.
  - 모니터링 스위치를 활성화해야 합니다.
  - 내보내기 도구(Export.exe)를 Data Infrastructure Insights AU에 복사해야 합니다.
  - 내보내기 도구 버전은 대상 스토리지의 마이크로코드 버전과 일치해야 합니다.
- AMS 성능:
  - NetApp은 Data Infrastructure Insights에서 성능 데이터를 검색하는 데 사용할 전용 서비스 계정을 AMS 어레이에 생성하는 것이 좋습니다. Storage Navigator는 사용자 계정만 스토리지에 동시에 로그인할 수 있도록 합니다. Data Infrastructure Insights가 관리 스크립트나 HiCommand와 동일한 사용자 계정을 사용하도록

하면 동시 사용자 계정 로그인 한도로 인해 Data Infrastructure Insights, 관리 스크립트 또는 HiCommand가 스토리지와 통신하지 못할 수 있습니다

- 성능 모니터에 라이선스가 있어야 합니다.
- SNM2(Storage Navigator Modular 2) CLI 유틸리티는 Data Infrastructure Insights AU에 설치해야 합니다.

#### 구성

필드에 입력합니다	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	VSP G1000(R800), VSP(R700), HUS VM(HM700) 및 USP 스토리지를 위한 장치 목록입니다. 각 스토리지에는 * 스토리지의 IP:IP 주소가 필요합니다. * 사용자 이름: 스토리지의 사용자 이름 * 암호: 내보내기 유틸리티 jar 파일이 포함된 저장소 * 폴더의 암호입니다
SNM2Devices - WMS/SMS/AMS 저장소	WMS/SMS/AMS 저장소에 대한 장치 목록입니다. 각 스토리지에는 * 스토리지의 IP:IP 주소가 필요합니다. * Storage Navigator CLI 경로: SNM2 CLI 경로 * 계정 인증 유효: 유효한 계정 인증을 선택하려면 선택합니다. * 사용자 이름: 스토리지의 사용자 이름 * 암호: 암호
성능 조정 관리자 를 선택합니다	다른 성능 옵션을 재정의합니다
튜닝 관리자 호스트	튜닝 관리자의 IP 주소 또는 정규화된 도메인 이름입니다
조정 관리자 포트를 재정의합니다	비어 있는 경우 Choose Tuning Manager for Performance 필드에서 기본 포트를 사용하고, 그렇지 않으면 사용할 포트를 입력합니다
튜닝 관리자 사용자 이름	Tuning Manager의 사용자 이름입니다
조정 관리자 암호	Tuning Manager 암호

참고: HDS USP, USP V 및 VSP에서 모든 디스크는 둘 이상의 스토리지 그룹에 속할 수 있습니다.

#### 고급 구성

필드에 입력합니다	설명
연결 유형	HTTPS 또는 HTTP도 기본 포트를 표시합니다
HiCommand 서버 포트	HiCommand 장치 관리자에 사용되는 포트입니다
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.
내보내기 제한 시간(초)	내보내기 유틸리티 시간 초과. 기본값은 300입니다.

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
오류: 사용자에게 충분한 권한이 없습니다	더 많은 권한이 있는 다른 사용자 계정을 사용하거나 데이터 수집기에 구성된 사용자 계정의 권한을 늘리십시오
오류: 저장소 목록이 비어 있습니다. 장치가 구성되지 않았거나 사용자에게 충분한 권한이 없습니다	* 장치가 구성되었는지 확인하려면 DeviceManager를 사용합니다. * 더 많은 권한이 있는 다른 사용자 계정을 사용하거나 사용자 계정의 권한을 늘리십시오
오류: HDS 스토리지 어레이가 며칠 동안 새로 고쳐지지 않았습니다	HDS HiCommand에서 이 어레이를 새로 고치지 않는 이유를 조사하십시오.

#### 성능

문제:	다음을 시도해 보십시오.
오류: * 내보내기 유틸리티 실행 중 오류 * 외부 명령 실행 중 오류	* 데이터 인프라 인사이트 획득 장치에 내보내기 유틸리티가 설치되어 있는지 확인 * 데이터 수집기 구성에서 내보내기 유틸리티 위치가 올바른지 확인 * 데이터 수집기 구성에서 USP/R600 어레이의 IP가 올바른지 확인 * 데이터 수집기 구성에서 사용자 이름 및 암호가 올바른지 확인 * 구성 된 마이크로 어레이 코드와 호환되는지 확인 후 CMD 스토리지 디렉토리 내보내기를 사용하여 구성 runWin.bat
오류: 대상 IP에 대한 내보내기 도구 로그인에 실패했습니다	* 사용자 이름/암호가 올바른지 확인 * 이 HDS 데이터 수집기에 대한 사용자 ID 생성 * 이 어레이를 획득하도록 구성된 다른 데이터 수집기가 없는지 확인합니다
오류: Export tools logged "Unable to get time range for monitoring".	* 스토리지에서 성능 모니터링이 활성화되었는지 확인합니다. * Data Infrastructure Insights 외부에서 내보내기 도구를 호출하여 문제가 Data Infrastructure Insights 외부에 있는지 확인하십시오.
오류: * 구성 오류: 스토리지 어레이가 내보내기 유틸리티에서 지원되지 않음 * 구성 오류: 스토리지 어레이가 Storage Navigator Modular CLI에서 지원되지 않습니다	* 지원되는 스토리지 어레이만 구성합니다. * "장치 목록 필터"를 사용하여 지원되지 않는 스토리지 배열을 제외합니다.
오류: * 외부 명령 실행 중 오류 * 구성 오류: 스토리지 어레이가 인벤토리에서 보고되지 않음 * 구성 오류: 내보내기 폴더에 jar 파일이 없습니다	* 내보내기 유틸리티 위치를 확인합니다. * 문제가 있는 스토리지 어레이가 HiCommand 서버에서 구성되었는지 확인합니다. * 성능 폴링 간격을 60초의 배수로 설정합니다.

문제:	다음을 시도해 보십시오.
오류: * 오류 Storage navigator CLI * auperform 명령 실행 중 오류 * 외부 명령 실행 중 오류	* Storage Navigator Modular CLI가 데이터 인프라 인사이트 획득 장치에 설치되어 있는지 확인 * Storage Navigator Modular CLI 위치가 데이터 수집기 구성에서 올바른지 확인 * 데이터 수집기 구성에 WMS/SMS/SMS 어레이의 IP가 올바른지 확인 * Storage Navigator Modular CLI 버전이 데이터 수집기의 마이크로 코드 버전과 호환되는지 확인 * 다음과 같이 구성된 스토리지 참조 디렉토리에서 "CMD-exe"를 실행하여 스토리지 구성 해제 명령을 실행하여 스토리지 디렉토리를 여십시오.
오류: 구성 오류: 인벤토리에서 스토리지 배열을 보고하지 않았습니다	문제가 있는 스토리지 어레이가 HiCommand 서버에 구성되어 있는지 확인합니다
오류: * 스토리지가 Storage Navigator에 등록되지 않았습니다. Modular 2 CLI * 어레이가 Storage Navigator에 등록되지 않았습니다. Modular 2 CLI * 구성 오류: 스토리지 어레이가 StorageNavigator Modular CLI에 등록되지 않았습니다	*명령 프롬프트를 열고 디렉토리를 구성된 경로로 변경합니다 *“set=STONAVM_HOME=” 명령을 실행합니다. *“auunitref” 명령을 실행합니다. * 명령 출력에 IP가 있는 어레이의 세부 정보가 포함되어 있는지 확인합니다 * 출력에 스토리지 세부 정보가 포함되지 않은 경우 Storage Navigator CLI를 사용하여 어레이를 등록합니다. - 명령 프롬프트를 열고 디렉토리를 구성된 경로로 변경합니다 - “set=STONAVM_HOME=” 명령을 실행합니다. - "auunitaddauto-IP <ip>" 명령을 실행합니다. <ip>를 올바른 IP로 교체합니다.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### Hitachi Vantara NAS 데이터 수집기 구성

Hitachi Vantara NAS 데이터 수집기는 HDS NAS 클러스터 검색을 지원하는 인벤토리 및 구성 데이터 수집기입니다. Data Infrastructure Insights는 NFS 및 CIFS 공유, 파일 시스템(내부 볼륨) 및 스패(스토리지 풀)를 검색할 수 있도록 지원합니다.

#### 용어

Data Infrastructure Insights는 HNAS 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
계층	디스크 그룹
클러스터	스토리지
노드	스토리지 노드
스팬	스토리지 풀
시스템 드라이브	백엔드 LUN
파일 시스템	내부 볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- 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.

#### 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 사이의 간격입니다. 기본값은 30분입니다.

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
"연결 오류" 및 "셸 채널 설정 오류:" 또는 "셸 채널 열기 오류" 오류 메시지	네트워크 연결 문제 또는 SSH가 잘못 구성되어 있을 수 있습니다. 대체 SSH 클라이언트와의 연결을 확인합니다
"Command: XXX has timed out" 오류 메시지와 함께 "Timeout" 또는 "Error Retrieving data"가 표시됩니다.	* 대체 SSH 클라이언트 * 증가 시간 초과로 명령을 시도하십시오
"연결 중 오류 발생" 또는 "잘못된 로그인 자격 증명"과 "장치와 통신할 수 없음:" 오류 메시지	* IP 주소 확인 * 사용자 이름 및 암호 확인 * 대체 SSH 클라이언트와의 연결 확인

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

#### 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

Data Infrastructure Insights는 이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
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" 모듈이 설치되어 있어야 합니다. 스토리지 어레이가 Ops Center "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.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Infinidat .Box 데이터 수집기

Infinidat .NET(HTTP) 데이터 수집기는 Infinidat Microsoft .Box 스토리지 시스템에서 인벤토리 정보를 수집하는 데 사용됩니다.

### 용어

Data Infrastructure Insights는 Infinidat InfiniBox 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
스토리지 풀	스토리지 풀
노드	컨트롤러
파일 시스템	내부 볼륨
파일 시스템	파일 공유
파일 시스템 내보내기	공유

### 요구 사항

다음은 이 데이터 수집기를 구성할 때 필요한 요구 사항입니다.

- IP 주소 또는 FQDN이 필요합니다
- 관리자 사용자 ID 및 암호
- REST API를 통한 포트 443

### 구성

필드에 입력합니다	설명
서비스 박스 호스트	IP 주소 또는 Management Node의 정규화된 도메인 이름입니다
사용자 이름	작업 영역 관리 노드에 대한 사용자 이름입니다

필드에 입력합니다	설명
암호	작업 영역 관리 노드에 대한 암호입니다

#### 고급 구성

필드에 입력합니다	설명
TCP 포트	TCP 포트는 Microsoft Windows Server에 연결하는 데 사용됩니다. 기본값은 443입니다.
재고 폴링 간격입니다	재고 조사 사이의 간격입니다. 기본값은 60분입니다.

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### Huawei OceStor 데이터 수집기

Data Infrastructure Insights는 Huawei OceanStor(REST/HTTPS) 데이터 수집기를 사용하여 Huawei OceanStor 및 OceanStor Dorado 스토리지의 인벤토리 및 성능을 검색합니다.

#### 용어

Data Infrastructure Insights는 Huawei OceanStor로부터 다음과 같은 인벤토리 및 성능 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
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
iSCSI 링크 대상	iSCSI 타겟 노드
iSCSI 링크 초기자	iSCSI 이니시에이터 노드입니다
디스크	디스크
LUN을 클릭합니다	볼륨

#### 요구 사항

이 데이터 수집기를 구성하려면 다음 요구 사항이 필요합니다.

- 장치 IP 주소입니다

- 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 포트입니다. 기본값은 8088입니다.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.
성능 폴링 간격(초).	기본값은 300초입니다.

## 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## IBM을 선택합니다

### IBM Cleversafe 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 IBM Cleversafe 스토리지 시스템의 인벤토리 및 성능 데이터를 검색합니다.



IBM Cleversafe는 관리 단위 비율과 다른 원시 TB로 측정되었습니다. 40TB의 포맷되지 않은 IBM Cleversafe 용량마다 1로 비용이 청구됩니다 "[관리 장치\(MU\)](#)".

## 용어

Data Infrastructure Insights는 IBM Cleversafe 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
스토리지 풀	스토리지 풀
컨테이너	내부 볼륨

공급업체/모델 기간	<b>Data Infrastructure Insights 용어</b>
컨테이너	파일 공유
NFS 공유	공유

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- 클러스터의 외부 데이터 서비스 IP 주소입니다
- 관리자 사용자 이름 및 암호
- 포트 9440

#### 구성

필드에 입력합니다	설명
관리자 IP 또는 호스트 이름입니다	관리 노드의 IP 주소 또는 호스트 이름입니다
사용자 이름입니다	슈퍼 사용자 또는 시스템 관리자 역할을 가진 사용자 계정의 사용자 이름입니다
암호	슈퍼 사용자 또는 시스템 관리자 역할을 가진 사용자 계정의 암호입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다.
HTTP 연결 시간 초과(초)	HTTP 제한 시간(초)

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

#### IBM CS 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 IBM CS 스토리지 시스템의 인벤토리 및 성능 데이터를 검색합니다.

#### 용어

Data Infrastructure Insights는 IBM CS 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	<b>Data Infrastructure Insights 용어</b>
스토리지 풀	스토리지 풀



공급업체/모델 기간	Data Infrastructure Insights 용어
컨테이너	내부 볼륨
컨테이너	파일 공유
NFS 공유	공유

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- 클러스터의 외부 데이터 서비스 IP 주소입니다
- 관리자 사용자 이름 및 암호
- 포트 9440

#### 구성

필드에 입력합니다	설명
PRISM 외부 IP 주소	클러스터의 외부 데이터 서비스 IP 주소입니다
사용자 이름입니다	Admin 계정의 사용자 이름입니다
암호	Admin 계정의 암호입니다

#### 고급 구성

필드에 입력합니다	설명
TCP 포트	IBM CS 어레이에 연결하는 데 사용되는 TCP 포트입니다. 기본값은 9440입니다.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

#### IBM 시스템 스토리지 DS8000 시리즈 데이터 수집기

IBM DS(CLI) 데이터 수집기는 DS6xxx 및 DS8xxx 장치에 대한 인벤토리 및 성능 데이터 수집을 지원합니다.

DS3xxx, DS4xxx 및 DS5xxx 장치는 에서 ["NetApp E-Series 데이터 수집기"](#) 지원됩니다. 지원되는 모델 및 펌웨어 버전은 Data Infrastructure Insights 지원 매트릭스를 참조하십시오.

#### 용어

Data Infrastructure Insights는 IBM DS 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다.

이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크 드라이브 모듈	디스크
스토리지 이미지	스토리지
익스텐트 풀	스토리지 노드
고정 블록 볼륨	볼륨
호스트 FC 이니시에이터(매핑)	볼륨 마스크

참고: 일반적인 용어 매핑일 뿐이며 이 데이터 수집의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

이 데이터 수집기를 구성하려면 다음이 필요합니다.

- 각 DS 배열의 IP 주소입니다
- 각 DS 어레이에 대한 읽기 전용 사용자 이름 및 암호
- Data Infrastructure Insights AU:IBM\_dscli\_에 설치된 타사 소프트웨어
- 액세스 유효성 검사: 사용자 이름과 암호를 사용하여 Run\_dscli\_commands 를 실행합니다
- 포트 요구 사항: 80, 443 및 1750

#### 구성

필드에 입력합니다	설명
DS 스토리지	DS device의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	DS CLI의 사용자 이름입니다
암호	DS CLI의 암호입니다
_dscli_실행 파일 경로입니다	dscli_executable의 전체 경로입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 간격(분). 기본값은 40입니다.
스토리지 표시 이름	IBM DS 스토리지 어레이의 이름입니다
재고 제외 장치	인벤토리 수집에서 제외할 장치 일련 번호의 쉼표로 구분된 목록입니다
성능 폴링 간격(초)	기본값은 300입니다.
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

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

## 인벤토리

문제:	다음을 시도해 보십시오.
오류 포함: CMUC00192E, CMUC00191E 또는 CMUC00190E	* 입력한 자격 증명 및 IP 주소를 확인합니다. * 웹 관리 콘솔\https://<ip>:8452/DS8000/콘솔을 통해 어레이와 통신하십시오. <ip>를 데이터 수집기가 구성된 IP로 교체합니다.
오류: * 프로그램을 실행할 수 없음 * 명령 실행 중 오류	* 데이터 인프라 인사이트 획득 장치에서 CLI의 홈 디렉토리/lib에서 CMD * Open CLI.CFG 파일을 열고, Java_install 속성을 확인하고, 해당 환경에 맞게 값을 편집합니다. * 이 시스템에 설치된 Java 버전을 표시하고, "java-version"을 입력합니다. * CLI 명령에 지정된 IBM 스토리지 장치의 IP 주소를 Ping합니다. * 위 항목 모두 정상적으로 작동했다면 CLI 명령을 수동으로 실행하십시오

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## IBM PowerVM 데이터 수집기 구성

IBM PowerVM(SSH) 데이터 수집기는 하드웨어 관리 콘솔(HMC)에서 관리하는 IBM POWER 하드웨어 인스턴스에서 실행되는 가상 파티션에 대한 정보를 수집하는 데 사용됩니다.

## 용어

Data Infrastructure Insights는 IBM POWER 하드웨어 인스턴스에서 실행되는 가상 파티션에서 인벤토리 정보를 수집합니다. 획득한 각 자산 유형에 대해 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
hdisk	가상 디스크
관리 대상 시스템	호스트
LPAR, VIO 서버	가상 머신
볼륨 그룹	데이터 저장소
물리적 볼륨	LUN을 클릭합니다

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

이 데이터 수집기를 구성하고 사용하려면 다음 요구 사항을 충족해야 합니다.

- HMC(Hardware Management Console)의 IP 주소
- SSH를 통해 HMC(Hardware Management Console)에 대한 액세스를 제공하는 사용자 이름 및 암호입니다

- 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

필드에 입력합니다	설명
HMC(Hardware Management Console) IP 주소입니다	PowerVM 하드웨어 관리 콘솔의 IP 주소 또는 정규화된 도메인 이름입니다
HMC 사용자	하드웨어 관리 콘솔의 사용자 이름입니다
암호	하드웨어 관리 콘솔에 사용되는 암호입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 20분입니다.
SSH 포트	SSH에서 PowerVM에 사용되는 포트입니다
암호	하드웨어 관리 콘솔에 사용되는 암호입니다
재시도 횟수	인벤토리 재시도 횟수입니다
장치 제외	제외할 장치 ID 또는 표시 이름의 쉼표로 구분된 목록입니다

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

#### IBM SAN Volume Controller 데이터 수집기 구성

IBM SVC(SAN Volume Controller) 데이터 수집기는 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 Data Infrastructure Insights 지원 매트릭스를 참조하십시오.

#### 용어

Data Infrastructure Insights는 IBM SVC 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다.

이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
Mdisk 그룹	스토리지 풀
vDisk를 선택합니다	볼륨
Mdisk	백엔드 LUN 및 경로입니다

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 재고 요건

- 각 SVC 클러스터의 IP 주소입니다
- 포트 22를 사용할 수 있습니다
- 읽기 전용 사용자 이름 및 암호

### 성능 요구사항

- SVC 콘솔은 모든 SVC 클러스터에 필수이며 SVC 검색 기반 패키지에 필요합니다.
- 자격 증명은 클러스터 노드에서 구성 노드로 성능 파일을 복사하는 경우에만 관리 액세스 레벨이 필요합니다.
- SSH를 통해 SVC 클러스터에 연결하고 `_svctask startstats -interval 1_`을 실행하여 데이터 수집을 활성화합니다

참고: 또는 SVC 관리 사용자 인터페이스를 사용하여 데이터 수집을 사용하도록 설정합니다.

### 구성

필드에 입력합니다	설명
클러스터 IP 주소	SVC 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
재고 사용자 이름입니다	SVC CLI의 사용자 이름입니다
재고 암호	SVC CLI의 암호입니다

### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40분입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.
덤프된 통계 파일 정리	덤프된 통계 파일을 정리하려면 이 확인란을 선택합니다

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

문제:	다음을 시도해 보십시오.
오류: "구성 노드에서 실행되지 않아 명령을 시작할 수 없습니다."	명령은 구성 노드에서 실행해야 합니다.

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

문제:	다음을 시도해 보십시오.
오류: "구성 노드에서 실행되지 않아 명령을 시작할 수 없습니다."	명령은 구성 노드에서 실행해야 합니다.

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## IBM XIV/A9000 데이터 수집기 구성

IBM XIV 및 A9000(CLI) 데이터 수집기는 XIV 명령줄 인터페이스를 사용하여 인벤토리 데이터를 수집하는 동시에 7778 포트에서 SMI-S 공급자를 실행하는 XIV/A9000 스토리지에 대한 SMI-S 호출을 수행하여 성능 수집을 수행합니다.

## 용어

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
스토리지 시스템	스토리지
스토리지 풀	스토리지 풀
볼륨	볼륨

## 요구 사항

이 데이터 수집기를 구성하고 사용하려면 다음 요구 사항을 충족해야 합니다.

- 포트 요구 사항: TCP 포트 7778
- 읽기 전용 사용자 이름 및 암호
- XIV CLI는 AU에 설치해야 합니다

## 성능 요구사항

다음은 성능 수집에 대한 요구 사항입니다.

- SMI-S Agent 1.4 이상
- 스토리지에서 실행되는 SMI-S 호환 CIMService 대부분의 XIV 스토리지에는 기본적으로 CIMServer가 설치되어 있습니다.

- CIMServer에 대한 사용자 로그인이 제공되어야 합니다. 스토리지 구성 및 속성에 대한 전체 읽기 액세스 권한이 있어야 합니다.
- SMI-S 네임스페이스. 기본값은 root/ibm입니다. CIMServer에서 구성할 수 있습니다.
- 포트 요구 사항: HTTP의 경우 5988, HTTPS의 경우 5989.
- SMI-S 성능 수집에 대한 계정을 생성하는 방법은 다음 링크를 참조하십시오. [https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc\\_V41.doc/fqz0\\_t\\_adding\\_cim\\_agent.html](https://www.ibm.com/docs/en/products?topic=/com.ibm.tpc_V41.doc/fqz0_t_adding_cim_agent.html)

#### 구성

필드에 입력합니다	설명
XIV IP 주소입니다	XIV 스토리지의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	XIV 스토리지의 사용자 이름입니다
암호	XIV 스토리지의 암호입니다
XIV CLI 디렉토리에 대한 전체 경로	XIV CLI가 포함된 폴더의 전체 경로입니다
SMI-S 호스트 IP 주소입니다	SMI-S 호스트의 IP 주소입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 40분입니다.
SMI-S 프로토콜	SMI-S 공급자에 연결하는 데 사용되는 프로토콜입니다. 기본 포트도 표시합니다.
SMI-S 포트를 재정의합니다	비어 있는 경우 연결 유형 필드에서 기본 포트를 사용하고, 그렇지 않으면 사용할 연결 포트를 입력합니다
사용자 이름	SMI-S Provider 호스트의 사용자 이름입니다
암호	SMI-S Provider 호스트의 암호입니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Lenovo 데이터 수집기

Data Infrastructure Insights는 Lenovo 데이터 수집기를 사용하여 Lenovo HX 스토리지 시스템의 인벤토리 및 성능 데이터를 검색합니다.

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- PRISM 외부 IP 주소

- 관리자 사용자 이름 및 암호
- TCP 포트 요구 사항: 9440

## 구성

필드에 입력합니다	설명
PRISM 외부 IP 주소	클러스터의 외부 데이터 서비스 IP 주소입니다
사용자 이름입니다	Admin 계정의 사용자 이름입니다
암호	Admin 계정의 암호입니다

## 고급 구성

필드에 입력합니다	설명
TCP 포트	어레이에 연결하는 데 사용되는 TCP 포트입니다. 기본값은 9440입니다.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

## 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## 마이크로소프트

### Azure NetApp Files 데이터 수집기 구성

Data Infrastructure Insights는 Azure NetApp Files 데이터 수집기를 사용하여 인벤토리 및 성능 데이터를 획득합니다.

#### 요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- 포트 요구 사항: 443 HTTPS
- Azure 관리 REST IP(management.azure.com)
- Azure 서비스 주 클라이언트 ID(사용자 계정)
- Azure 서비스 주 인증 키(사용자 암호)
- Data Infrastructure Insights 검색을 위해 Azure 계정을 설정해야 합니다.

계정이 올바르게 구성되고 Azure에 애플리케이션을 등록하면 Data Infrastructure Insights를 통해 Azure 인스턴스를 검색하는 데 필요한 자격 증명이 제공됩니다. 다음 링크에서는 검색을 위해 계정을 설정하는 방법에 대해 설명합니다.



구성

아래 표에 따라 데이터 수집기 필드에 데이터를 입력합니다.

필드에 입력합니다	설명
Azure 서비스 기본 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 60입니다

문제 해결

- ANF 데이터 수집기에서 사용하는 자격 증명은 ANF 볼륨이 포함된 Azure 구독에 액세스할 수 없습니다.
- Reader 액세스로 인해 성능 수집이 실패하는 경우 리소스 그룹 수준에서 Contributor 액세스 권한을 부여해 보십시오.

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

**Microsoft Hyper-V 데이터 수집기**

Microsoft Hyper-V 데이터 수집기는 가상화된 서버 컴퓨팅 환경에서 인벤토리 및 성능 데이터를 가져옵니다. 이 데이터 수집기는 독립 실행형 Hyper-V 호스트를 검색할 수도 있고, 전체 클러스터를 검색할 수도 있습니다. 독립 실행형 호스트 또는 클러스터당 하나의 Collector를 생성할 수도 있습니다.

용어

Data Infrastructure Insights는 Microsoft Hyper-V(WMI)에서 다음과 같은 인벤토리 정보를 가져옵니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
가상 하드 디스크	가상 디스크
호스트	호스트
가상 머신	가상 머신
CSV(Cluster Shared Volumes), 파티션 볼륨	데이터 저장소

공급업체/모델 기간	Data Infrastructure Insights 용어
인터넷 SCSI 장치, 다중 경로 SCSI LUN	LUN을 클릭합니다
Fibre Channel 포트	포트

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

요구 사항

이 데이터 수집기를 구성하려면 다음이 필요합니다.

- Hyper-V를 사용하려면 데이터 수집 및 원격 액세스/관리를 위해 포트 5985를 열어야 합니다.
- 클러스터 또는 독립 실행형 하이퍼바이저의 IP 주소 또는 FQDN입니다. 부동 클러스터 호스트 이름 또는 IP를 사용하는 것이 가장 신뢰할 수 있는 방법일 수 있습니다. 이는 수집기가 클러스터의 특정 노드 중 하나만 가리키는 것과 비교할 수 있습니다.
- 클러스터의 모든 하이퍼바이저에서 작동하는 관리 수준 사용자 계정입니다.
- WinRM은 모든 하이퍼바이저에서 활성화되어 있어야 합니다
- 포트 요구 사항: Windows 2003 및 이전 버전의 경우 1024-65535로 할당된 WMI 및 동적 TCP 포트를 통해 135번 포트 및 Windows 2008의 경우 49152-65535번 포트.
- 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 하이퍼바이저에서 각 게스트에서 Data Infrastructure Insights에 더 많은 데이터를 사용할 수 있습니다. 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"](#)



Hyper-V 데이터 수집기는 Windows 획득 장치가 필요합니다.

구성

필드에 입력합니다	설명
클러스터 IP 주소 또는 부동 클러스터 FQDN입니다	클러스터의 IP 주소 또는 정규화된 도메인 이름 또는 클러스터링되지 않은 독립 실행형 하이퍼바이저입니다
사용자 이름	하이퍼바이저의 관리자 사용자 이름입니다
암호	하이퍼바이저의 암호입니다
DNS 도메인 접미사	하이퍼바이저의 FQDN을 렌더링하기 위해 단순 호스트 이름과 결합된 호스트 이름 접미사

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 20분입니다.

## 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## 넷업

### NetApp Cloud Volumes ONTAP 데이터 수집기

이 데이터 수집기는 Cloud Volumes ONTAP 구성에서 인벤토리 수집을 지원합니다.

#### 구성

필드에 입력합니다	설명
NetApp 관리 IP 주소입니다	클라우드 볼륨 ONTAP의 IP 주소입니다
사용자 이름	Cloud Volumes ONTAP의 사용자 이름입니다
암호	위 사용자의 암호입니다

#### 고급 구성

필드에 입력합니다	설명
연결 유형	HTTPS 권장. 기본 포트도 표시합니다.
통신 포트를 재정의합니다	기본값이 아닌 경우 사용할 포트입니다.
재고 폴링 간격(분)	기본값은 60분입니다.
인벤토리 동시 스레드 수입니다	동시 스레드 수입니다.
HTTPS에 TLS를 강제로 적용합니다	HTTPS를 통해 TLS를 강제 적용합니다
자동으로 넷그룹을 조회합니다	자동으로 넷그룹을 조회합니다
넷그룹 확장	셸 또는 파일을 선택합니다
HTTP 읽기 제한 시간(초)	기본값은 30초입니다
응답을 UTF-8로 강제 적용합니다	응답을 UTF-8로 강제 적용합니다
성능 폴링 간격(분)	기본값은 900초입니다.
성능 동시 스레드 수입니다	동시 스레드 수입니다.
고급 카운터 데이터 수집	Data Infrastructure Insights가 아래 목록에서 고급 메트릭을 수집하도록 하려면 이 옵션을 선택합니다.

## 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### AWS용 NetApp Cloud Volumes Services 데이터 수집기

이 데이터 수집기는 AWS용 NetApp Cloud Volumes Services 구성의 인벤토리 수집을

지원합니다.

구성

필드에 입력합니다	설명
Cloud Volumes Region(Cloud Volumes 영역)	NetApp Cloud Volumes Services for AWS의 지역
API 키	Cloud Volumes API 키입니다
비밀 키	Cloud Volumes 암호 키입니다

고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다

문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

문제:	다음은 시도해 보십시오.
다음과 유사한 오류가 발생했습니다. '요청을 실행하지 못했습니다. <AWS 지역 엔드포인트>:8080 [<AWS 지역 엔드포인트>/AWS 지역 엔드포인트 IP>] 실패: 연결 시간 초과: https://<AWS 지역 엔드포인트 FQDN 가져오기 >:8080/v1/스토리지/IPHTTP 범위/1.1'	"프록시" Data Infrastructure Insights에서 수집 장치와 통신하는 데 사용되는 Data Infrastructure Insights와 Data Collector 자체 간에 통신하지 않습니다. 다음과 같은 몇 가지 방법을 시도해 볼 수 있습니다. 획득 장치가 FQDN을 확인하고 필요한 포트에 도달할 수 있는지 확인하십시오. 프록시가 오류 메시지의 지정된 끝점에 도달할 필요가 없는지 확인합니다. curl(말림)은 획득 장치와 끝점 사이의 통신을 테스트하는 데 사용할 수 있습니다. 이 테스트에 프록시를 사용하고 있지 * 않은지 확인하십시오. 예: root@acquisitionunit #curl-s-H accept: application/json-H "Content-type: application/json" -H API-key:<데이터 수집기 자격 증명에 사용되는 api 키 -H secret-key:"NetApp KB 문서 "<데이터 수집기 자격 증명에 사용된 비밀 키>-X https://<AWS 지역 엔드포인트 가져오기 >:8080/v1/IP1/스토리지/IPRanges 를 참조하십시오.

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

### NetApp ONTAP 데이터 관리 소프트웨어 데이터 수집기

이 데이터 수집기는 ONTAP 계정에서 읽기 전용 API 호출을 사용하여 ONTAP를 실행하는 스토리지 시스템에서 인벤토리 및 성능 데이터를 가져옵니다. 또한 이 데이터 수집기는 지원을 가속화하기 위해 클러스터 응용 프로그램 레지스트리에 레코드를 만듭니다.

용어

Data Infrastructure Insights는 ONTAP 데이터 수집기에서 인벤토리 및 성능 데이터를 가져옵니다. 획득한 각 자산

유형에 대해 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
RAID 그룹	디스크 그룹
클러스터	스토리지
노드	스토리지 노드
집계	스토리지 풀
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨

### ONTAP 데이터 관리 용어

다음 용어는 ONTAP 데이터 관리 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

#### 스토리지

- 모델 – 이 클러스터 내에서 심표로 구분된 고유한 개별 노드 모델 이름의 목록입니다. 클러스터의 모든 노드가 동일한 모델 유형인 경우 하나의 모델 이름만 표시됩니다.
- 공급업체 - 동일한 공급업체 이름 새 데이터 소스를 구성하는 경우 표시됩니다.
- 일련 번호 – 스토리지 일련 번호입니다. ONTAP 데이터 관리와 같은 클러스터 아키텍처 스토리지 시스템에서 이 일련 번호는 개별 "스토리지 노드" 일련 번호보다 덜 유용할 수 있습니다.
- IP – 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다.
- 마이크로코드 버전 – 펌웨어.
- 물리적 용량 – 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2의 합계.
- 지연 시간 – 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. Data Infrastructure Insights는 이러한 가치를 직접 소싱하는 것이 좋지만, 그렇게 할 경우에는 그렇지 않은 경우가 많습니다. Data Infrastructure Insights는 이러한 기능을 제공하는 어레이 대신 일반적으로 개별 내부 볼륨의 통계에서 도출된 IOPS 가중 계산을 수행합니다.
- 처리량 – 내부 볼륨에서 집계됩니다. 관리 - 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Data Infrastructure Insights 데이터 소스에 의해 프로그래밍 방식으로 생성되었습니다.

#### 스토리지 풀

- 스토리지 – 이 풀이 상주하는 스토리지 시스템입니다. 필수입니다.
- 형식 - 가능성 목록 목록의 설명 값입니다. 일반적으로 "집계" 또는 "RAID 그룹"이 됩니다.
- 노드 – 이 스토리지 배열의 아키텍처가 특정 스토리지 노드에 속해 있는 경우, 이 스토리지 배열의 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 체계. RAID\_DP는 이중 패리티이고, RAID\_TP는 삼중 패리티입니다.

- 용량 – 이 값은 논리적 사용 용량, 가용 용량 및 총 논리적 용량, 그리고 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 – 스토리지 풀 아키텍처가 스냅샷 전용 영역에 해당 용량의 일부를 할당하는 경우 사용된 스냅샷 용량 및 총 용량입니다. MetroCluster 구성의 ONTAP은 이 문제를 나타낼 가능성이 높지만, 다른 ONTAP 구성은 더 적습니다.
- 사용률 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 사용 중 가장 높은 비율을 나타내는 백분율 값입니다. 디스크 사용률이 반드시 스토리지 성능과 강력한 상관 관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 재구축, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지의 복제 구현으로 인해 디스크 사용률이 높아지고 내부 볼륨 또는 볼륨 작업 부하로 표시되지 않을 수 있습니다.
- IOPS – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다. 처리량 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다.

## 스토리지 노드

- 스토리지 – 이 노드가 속한 스토리지 시스템입니다. 필수입니다.
- HA 파트너 – 노드가 1개 노드로 페일오버되고 다른 1개 노드만 페일오버되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다.
- 상태 - 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다.
- 모델 - 노드의 모델 이름입니다.
- 버전 - 디바이스의 버전 이름입니다.
- 일련 번호 - 노드 일련 번호입니다.
- 메모리 – 사용 가능한 경우 베이스 2 메모리.
- 사용률 – ONTAP에서는 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 넘는 지속적인 값이 관찰될 경우, 이는 낮은 크기 조절을 나타내는 것입니다. 컨트롤러/노드가 충분히 크지 않거나 회전 디스크가 부족하여 쓰기 워크로드를 흡수할 수 없습니다.
- IOPS – 노드 개체의 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 지연 시간 – 노드 개체의 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 처리량 – 노드 개체의 ONTAP ZAPI 호출에서 직접 파생됩니다.
- 프로세서 - CPU 수입니다.

## 요구 사항

다음은 이 데이터 수집기를 구성하고 사용하기 위한 요구 사항입니다.

- 읽기 전용 API 호출에 대해 구성된 관리자 계정에 대한 액세스 권한이 있어야 합니다.
- 계정 세부 정보에는 사용자 이름 및 암호가 포함됩니다.
- 포트 요구 사항: 80 또는 443
- 계정 권한:
  - 기본 SVM에 대해 ontapi 애플리케이션에 대한 읽기 전용 역할 이름
  - 추가적인 선택적 쓰기 권한이 필요할 수 있습니다. 아래의 사용 권한에 대한 참고 사항을 참조하십시오.

- ONTAP 라이선스 요구 사항:
  - 파이버 채널 검색에 필요한 FCP 라이선스 및 매핑/마스킹된 볼륨

### ONTAP 스위치 메트릭을 수집하기 위한 권한 요구 사항

Data Infrastructure Insights에는 ONTAP 클러스터 스위치 데이터를 수집기 고급 구성 설정에서 옵션으로 수집하는 기능이 있습니다. 데이터 인프라 인사이트 수집기에서 이를 활성화할 뿐 아니라, "스위치 정보" 권한 스위치 데이터를 데이터 인프라 인사이트(Insights)로 전송할 수 있도록 ONTAP 시스템 \* 자체를 구성하고 올바르게 설정되었는지 확인해야 합니다.

#### 구성

필드에 입력합니다	설명
NetApp 관리 IP	NetApp 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다
사용자 이름	NetApp 클러스터의 사용자 이름입니다
암호	NetApp 클러스터의 암호입니다

#### 고급 구성

필드에 입력합니다	설명
연결 유형	HTTP(기본 포트 80) 또는 HTTPS(기본 포트 443)를 선택합니다. 기본값은 HTTPS입니다
통신 포트를 재정의합니다	기본값을 사용하지 않으려면 다른 포트를 지정하십시오
재고 폴링 간격(분)	기본값은 60분입니다.
HTTPS용 TLS	HTTPS를 사용하는 경우에만 TLS를 프로토콜로 허용합니다
자동으로 넷그룹을 조회합니다	엑스포트 정책 규칙에 대한 자동 넷그룹 조회를 설정합니다
넷그룹 확장	넷그룹 확장 전략. file_or_shell_을 선택합니다. 기본값은 _shell_입니다.
HTTP 읽기 제한 시간(초)	기본값은 30입니다
응답을 UTF-8로 강제 적용합니다	데이터 수집기 코드가 CLI의 응답을 UTF-8로 해석하도록 합니다
성능 폴링 간격(초)	기본값은 900초입니다.
고급 카운터 데이터 수집	ONTAP 통합을 활성화합니다. ONTAP 고급 카운터 데이터를 폴에 포함하려면 이 옵션을 선택합니다. 목록에서 원하는 카운터를 선택합니다.
클러스터 스위치 메트릭입니다	Data Infrastructure Insights가 클러스터 스위치 데이터를 수집할 수 있도록 허용합니다. 참고 "스위치 정보" 권한: 데이터 인프라 인사이트 측에서 이 기능을 활성화하는 동시에 스위치 데이터를 데이터 인프라 인사이트 로 보낼 수 있도록 ONTAP 시스템을 구성해야 합니다. 아래의 "권한에 대한 참고 사항"을 참조하십시오.

## ONTAP 전력 측정 기준

여러 ONTAP 모델이 모니터링 또는 알림에 사용할 수 있는 데이터 인프라 Insights에 대한 전력 메트릭을 제공합니다. 아래의 지원 모델과 지원되지 않는 모델 목록은 포괄하지는 않지만 몇 가지 지침을 제공해야 합니다. 일반적으로 모델이 목록에 있는 모델과 동일한 제품군에 속하는 경우 지원은 동일해야 합니다.

지원되는 모델:

A200  
A220  
A250  
A300  
A320  
A400  
A700  
A700s를 참조하십시오  
A800  
A900  
C190  
FAS2240-4  
FAS2552  
FAS2650  
FAS2720  
FAS2750  
FAS8200  
FAS8300  
FAS8700  
FAS9000

지원되지 않는 모델:

FAS2620  
FAS3250  
FAS3270  
500f로 설정합니다  
FAS6280  
FAS/AFF 8020  
FAS/AFF 8040  
FAS/AFF 8060  
FAS/AFF 8080

사용 권한에 대한 참고 사항

많은 데이터 인프라 인사이트 ONTAP 대시보드가 고급 ONTAP 카운터를 사용하기 때문에 데이터 수집기 고급 구성 섹션에서 \* 고급 카운터 데이터 수집 \* 을 활성화해야 합니다.

또한 ONTAP API에 대한 쓰기 권한이 활성화되어 있는지도 확인해야 합니다. 이 경우 일반적으로 필요한 권한이 있는 클러스터 수준의 계정이 필요합니다.

클러스터 수준에서 Data Infrastructure Insights에 대한 로컬 계정을 생성하려면 클러스터 관리 관리자 사용자 이름 /암호를 사용하여 ONTAP에 로그인하고 ONTAP 서버에서 다음 명령을 실행합니다.

1. 시작하기 전에 관리자\_계정으로 ONTAP에 로그인해야 하며 `_DIAGNOSTIC-LEVEL` 명령 을 활성화해야 합니다.



2. 다음 명령을 사용하여 읽기 전용 역할을 만듭니다.

```
security login role create -role ci_readonly -cmddirname DEFAULT -access
readonly
security login role create -role ci_readonly -cmddirname security
-access readonly
security login role create -role ci_readonly -access all -cmddirname
{cluster application-record create}
```

3. 다음 명령을 사용하여 읽기 전용 사용자를 생성합니다. create 명령을 실행하면 이 사용자의 암호를 입력하라는 메시지가 표시됩니다.

```
security login create -username ci_user -application ontapi
-authentication-method password -role ci_readonly
```

AD/LDAP 계정을 사용하는 경우 명령은 여야 합니다

```
security login create -user-or-group-name DOMAIN\aduser/adgroup
-application ontapi -authentication-method domain -role ci_readonly
클러스터 스위치 데이터를 수집하는 경우:
```

```
security login rest-role create -role ci_readonly -api
/api/network/ethernet -access readonly
```

그 결과로 생성되는 역할 및 사용자 로그인은 다음과 같습니다. 실제 출력은 다음과 같이 다를 수 있습니다.

```
Role Command/ Access
Vserver Name Directory Query Level
-----
cluster1 ci_readonly DEFAULT read only
cluster1 ci_readonly security readonly
```

```
cluster1::security login> show
Vserver: cluster1
Authentication Acct
UserName      Application      Method          Role Name      Locked
-----
ci_user       ontapi          password        ci_readonly    no
```



ONTAP 액세스 제어가 올바르게 설정되어 있지 않으면 Data Infrastructure Insights REST 호출이 실패하여 장치의 데이터 갭이 생길 수 있습니다. 예를 들어, 데이터 인프라 인사이트 수집기에서 이 기능을 활성화했지만 ONTAP에 대한 권한을 구성하지 않은 경우 획득이 실패합니다. 또한 역할이 이전에 ONTAP에 정의되어 있고 REST API 기능을 추가하는 경우 `_http_`가 역할에 추가되었는지 확인합니다.

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
수신 401 HTTP 응답 또는 13003 ZAPI 오류 코드 및 ZAPI는 "불충분한 권한" 또는 "이 명령에 대해 인증되지 않음"을 반환합니다.	사용자 이름과 암호, 사용자 권한/권한을 확인합니다.
클러스터 버전이 8.1 미만임	클러스터 최소 지원 버전은 8.1입니다. 최소 지원 버전으로 업그레이드하십시오.
ZAPI는 "cluster role is not cluster_mgmt LIF" 를 반환합니다.	AU는 클러스터 관리 IP와 통신해야 합니다. IP를 확인하고 필요한 경우 다른 IP로 변경합니다
오류: "7 모드 파일러는 지원되지 않습니다."	이 데이터 수집기를 사용하여 7 모드 파일러를 검색할 경우 이 문제가 발생할 수 있습니다. 대신 IP를 cDOT 클러스터를 가리키도록 변경합니다.
재시도 후 ZAPI 명령이 실패합니다	AU가 클러스터와 통신 문제를 겪고 있습니다. 네트워크, 포트 번호 및 IP 주소를 확인합니다. 또한 사용자는 AU 시스템의 명령줄에서 명령을 실행해야 합니다.
AU가 HTTP를 통해 ZAPI에 연결하지 못했습니다	ZAPI 포트가 일반 텍스트를 허용하는지 확인합니다. AU가 SSL 소켓에 일반 텍스트를 보내려고 하면 통신이 실패합니다.
SSLException 과 통신이 실패합니다	AU가 파일러의 일반 텍스트 포트에 SSL을 전송하려고 합니다. ZAPI 포트가 SSL을 허용하는지 또는 다른 포트를 사용하는지 확인합니다.
추가 연결 오류: ZAPI 응답에는 오류 코드 13001, "데이터베이스가 열려 있지 않습니다." ZAPI 오류 코드가 60이고 응답에는 "API가 시간에 완료되지 않았습니다."가 포함되어 있습니다. ZAPI 응답에는 "initialize_session() returned NULL environment" ZAPI가 포함되어 있습니다. ZAPI 오류 코드는 14007이고 응답에는 "노드가 정상 상태가 아닙니다"가 포함되어 있습니다.	네트워크, 포트 번호 및 IP 주소를 확인합니다. 또한 사용자는 AU 시스템의 명령줄에서 명령을 실행해야 합니다.

#### 성능

문제:	다음을 시도해 보십시오.
"ZAPI에서 성능을 수집하지 못했습니다." 오류	일반적으로 <code>perf stat</code> 이 실행되지 않기 때문입니다. 각 노드에서 <code>&gt;_system node systemshell-node * -command "spmctl -h cmd -stop;spmctl -h cmd -exec" _</code> 명령을 실행합니다

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## NetApp ONTAP REST 데이터 수집기

이 데이터 수집기는 REST API 호출을 사용하여 ONTAP 9.14.1 이상을 실행하는 스토리지 시스템에서 인벤토리, EMS 로그 및 성능 데이터를 수집합니다. 이전 릴리스의 ONTAP 시스템의 경우 ZAPI 기반 "NetApp ONTAP 데이터 관리 소프트웨어" 수집기 유형을 사용하십시오.



ONTAP REST Collector는 이전 ONTAPI 기반 Collector를 대체하는 용도로 사용할 수 있습니다. 따라서 수집되거나 보고되는 메트릭에는 차이가 있을 수 있습니다. ONTAPI와 REST의 차이점에 대한 자세한 내용은 를 참조하십시오 "[ONTAP 9.14.1 ONTAPI-REST 매핑](#)" 문서화:

### 요구 사항

다음은 이 데이터 수집기를 구성하고 사용하기 위한 요구 사항입니다.

- 필요한 액세스 권한이 있는 사용자 계정에 대한 액세스 권한이 있어야 합니다. 새 REST 사용자/역할을 생성하는 경우 관리자 권한이 필요합니다.
  - Data Infrastructure Insights는 주로 읽기 요청을 하지만 Data Infrastructure Insights에서 ONTAP 어레이에 등록하려면 일부 쓰기 권한이 필요합니다. 바로 아래의 `_권한에 대한 참고_`를 참조하십시오.
- ONTAP 버전 9.14.1 이상
- 포트 요구 사항: 443

### 사용 권한에 대한 참고 사항

많은 데이터 인프라 인사이트 ONTAP 대시보드가 고급 ONTAP 카운터를 사용하기 때문에 데이터 수집기 고급 구성 섹션에서 \* 고급 카운터 데이터 수집 사용 \* 을 사용하도록 설정해야 합니다.

클러스터 수준에서 Data Infrastructure Insights에 대한 로컬 계정을 생성하려면 클러스터 관리 관리자 사용자 이름 /암호를 사용하여 ONTAP에 로그인하고 ONTAP 서버에서 다음 명령을 실행합니다.

1. 시작하기 전에 관리자\_계정으로 ONTAP에 로그인해야 하며 `_DIAGNOSTIC-LEVEL` 명령 을 활성화해야 합니다.
2. `type_admin_`인 가상 서버의 이름을 검색합니다. 이 이름은 이후의 명령에서 사용됩니다.

```
vserver show -type admin
```

. 다음 명령을 사용하여 역할을 생성합니다.

```
security login rest-role create -role {role name} -api /api -access  
readonly  
security login rest-role create -role {role name} -api  
/api/cluster/agents -access all  
vserver services web access create -name spi -role {role name} -vserver  
{vserver name as retrieved above}  
security login create -user-or-group-name {username} -application http  
-authentication-method password -role {role name}
```

- 다음 명령을 사용하여 읽기 전용 사용자를 생성합니다. create 명령을 실행하면 이 사용자의 암호를 입력하라는 메시지가 표시됩니다.

```
security login create -username ci_user -application http
-authentication-method password -role ci_readonly
```

AD/LDAP 계정을 사용하는 경우 명령은 여야 합니다

```
security login create -user-or-group-name DOMAIN\aduser/adgroup
-application http -authentication-method domain -role ci_readonly
```

그 결과로 생성되는 역할 및 사용자 로그인은 다음과 같습니다. 실제 출력은 다음과 같이 다를 수 있습니다.

```
security login rest-role show -vserver <vserver name> -role restRole
```

Vserver	Role	API	Access
-----	-----	-----	-----
<vserver name>	restRole	/api	readonly
		/api/cluster/agents	all

2 entries were displayed.

```
security login show -vserver <vserver name> -user-or-group-name restUser
```

Vserver: <vserver name>

User/Group	Authentication	Acct
-----	-----	-----
restUser	http password	no none

#### 마이그레이션

이전 ONTAP(ontapi) 데이터 수집기에서 최신 ONTAP REST 수집기로 마이그레이션하려면 다음을 수행합니다.

- REST Collector를 추가합니다. 이전 Collector에 대해 구성된 사용자 이외의 다른 사용자에게 대한 정보를 입력하는 것이 좋습니다. 예를 들어, 위의 권한 섹션에 표시된 사용자를 사용합니다.
- 이전 Collector를 일시 중지하면 데이터가 계속 수집되지 않습니다.
- 새 휴면 수집기가 최소 30분 동안 데이터를 수집하도록 합니다. 이 시간 동안 "정상"으로 표시되지 않는 데이터는 무시합니다.

4. 휴지 기간 후, 휴지 수집기가 취득을 계속하는 동안 데이터가 안정화해야 합니다.

원하는 경우 이 동일한 프로세스를 사용하여 이전 컬렉터로 돌아갈 수 있습니다.

#### 구성

필드에 입력합니다	설명
ONTAP 관리 IP 주소입니다	NetApp 클러스터의 IP 주소 또는 정규화된 도메인 이름입니다. 클러스터 관리 IP/FQDN이어야 합니다.
ONTAP REST 사용자 이름입니다	NetApp 클러스터의 사용자 이름입니다
ONTAP REST 암호입니다	NetApp 클러스터의 암호입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다.
성능 폴링 간격(초)	기본값은 60초입니다.
고급 카운터 데이터 수집	ONTAP 고급 카운터 데이터를 폴에 포함하려면 이 옵션을 선택합니다. 기본적으로 사용됩니다.
EMS 이벤트 수집을 활성화합니다	ONTAP EMS 로그 이벤트 데이터를 포함하려면 선택합니다. 기본적으로 사용됩니다.
EMS 폴링 간격(초)	기본값은 60초입니다.

#### 용어

Data Infrastructure Insights는 ONTAP 데이터 수집기에서 인벤토리, 로그 및 성능 데이터를 수집합니다. 획득한 각 자산 유형에 대해 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
RAID 그룹	디스크 그룹
클러스터	스토리지
노드	스토리지 노드
집계	스토리지 풀
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨
스토리지 가상 시스템/Vserver	스토리지 가상 머신

#### ONTAP 데이터 관리 용어

다음 용어는 ONTAP 데이터 관리 스토리지 자산 랜딩 페이지에서 찾을 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

## 스토리지

- 모델 – 이 클러스터 내에서 심표로 구분된 고유한 개별 노드 모델 이름의 목록입니다. 클러스터의 모든 노드가 동일한 모델 유형인 경우 하나의 모델 이름만 표시됩니다.
- 공급업체 - 동일한 공급업체 이름 새 데이터 소스를 구성하는 경우 표시됩니다.
- 일련 번호 – 스토리지 UUID입니다
- IP – 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다.
- 마이크로코드 버전 – 펌웨어.
- 물리적 용량 – 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2의 합계.
- 지연 시간 – 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. Data Infrastructure Insights는 이러한 가치를 직접 소싱하는 것이 좋지만, 그렇게 할 경우에는 그렇지 않은 경우가 많습니다. Data Infrastructure Insights는 이러한 기능을 제공하는 어레이 대신 일반적으로 개별 내부 볼륨의 통계에서 도출된 IOPS 가중 계산을 수행합니다.
- 처리량 – 내부 볼륨에서 집계됩니다. 관리 - 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Data Infrastructure Insights 데이터 소스에 의해 프로그래밍 방식으로 생성되었습니다.

## 스토리지 풀

- 스토리지 – 이 풀이 상주하는 스토리지 시스템입니다. 필수입니다.
- 형식 - 가능성 목록 목록의 설명 값입니다. 일반적으로 "집계" 또는 "RAID 그룹"이 됩니다.
- 노드 – 이 스토리지 배열의 아키텍처가 특정 스토리지 노드에 속해 있는 경우, 이 스토리지 배열의 이름은 해당 랜딩 페이지의 하이퍼링크로 표시됩니다.
- Flash Pool 사용 – 예/아니오 가치 – 이 SATA/SAS 기반 풀에 캐싱 가속화에 SSD가 사용됩니까?
- 중복 – RAID 레벨 또는 보호 체계. RAID\_DP는 이중 패리티이고, RAID\_TP는 삼중 패리티입니다.
- 용량 – 이 값은 논리적 사용 용량, 가용 용량 및 총 논리적 용량, 그리고 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 – 스토리지 풀 아키텍처가 스냅샷 전용 영역에 해당 용량의 일부를 할당하는 경우 사용된 스냅샷 용량 및 총 용량입니다. MetroCluster 구성의 ONTAP는 이 문제를 나타낼 가능성이 높지만, 다른 ONTAP 구성은 더 적습니다.
- 사용률 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 사용 중 가장 높은 비율을 나타내는 백분율 값입니다. 디스크 사용률이 반드시 스토리지 성능과 강력한 상관 관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 재구축, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지의 복제 구현으로 인해 디스크 사용률이 높아지고 내부 볼륨 또는 볼륨 작업 부하로 표시되지 않을 수 있습니다.
- IOPS – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다. 처리량 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다.

## 스토리지 노드

- 스토리지 – 이 노드가 속한 스토리지 시스템입니다. 필수입니다.
- HA 파트너 – 노드가 1개 노드로 페일오버되고 다른 1개 노드만 페일오버되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다.
- 상태 - 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다.

- 모델 - 노드의 모델 이름입니다.
- 버전 - 디바이스의 버전 이름입니다.
- 일련 번호 - 노드 일련 번호입니다.
- 메모리 – 사용 가능한 경우 베이스 2 메모리.
- 사용률 – ONTAP에서는 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 넘는 지속적인 값이 관찰될 경우, 이는 낮은 크기 조정을 나타내는 것입니다. 컨트롤러/노드가 충분히 크지 않거나 회전 디스크가 부족하여 쓰기 워크로드를 흡수할 수 없습니다.
- IOPS – 노드 개체의 ONTAP REST 호출에서 직접 파생됩니다.
- 지연 시간 – 노드 개체의 ONTAP REST 호출에서 직접 파생됩니다.
- 처리량 – 노드 개체의 ONTAP REST 호출에서 직접 파생됩니다.
- 프로세서 - CPU 수입니다.

#### ONTAP 전력 측정 기준

여러 ONTAP 모델이 모니터링 또는 알림에 사용할 수 있는 데이터 인프라 Insights에 대한 전력 메트릭을 제공합니다. 아래의 지원 모델과 지원되지 않는 모델 목록은 포괄하지는 않지만 몇 가지 지침을 제공해야 합니다. 일반적으로 모델이 목록에 있는 모델과 동일한 제품군에 속하는 경우 지원은 동일해야 합니다.

지원되는 모델:

A200  
A220  
A250  
A300  
A320  
A400  
A700  
A700s를 참조하십시오  
A800  
A900  
C190  
FAS2240-4  
FAS2552  
FAS2650  
FAS2720  
FAS2750  
FAS8200  
FAS8300  
FAS8700  
FAS9000

지원되지 않는 모델:

FAS2620  
FAS3250  
FAS3270  
500f로 설정합니다  
FAS6280

FAS/AFF 8020  
 FAS/AFF 8040  
 FAS/AFF 8060  
 FAS/AFF 8080

문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

<p>문제:</p>	<p>다음을 시도해 보십시오.</p>
<p>ONTAP REST 데이터 수집기를 생성하려고 하면 다음과 같은 오류가 표시됩니다.        구성: 10.193.70.14: 10.193.70.14의 ONTAP REST API를 사용할 수 없음: 10.193.70.14 /api/cluster:400 잘못된 요청을 가져오지 못했습니다</p>	<p>이는 REST API 기능이 없는 9.6)와 같은 ONTAP ONTAP 어레이가 원인일 수 있습니다. ONTAP 9.14.1은 ONTAP REST Collector에서 지원하는 최소 ONTAP 버전입니다. 사전 REST ONTAP 릴리스에서 "400 Bad Request" 응답이 예상되어야 합니다.</p> <p>REST를 지원하지만 9.14.1 이상이 아닌 ONTAP 버전의 경우 다음과 같은 메시지가 표시될 수 있습니다.        구성: 10.193.98.84: 10.193.98.84의 ONTAP REST API 사용 불가: 10.193.98.84: 10.193.98.84: ONTAP REST API at 10.193.98.84 사용 가능: cheryl5-cluster-2 9.10.1 a3cb3247-3d3c-11ee-8ff3-005056b364a7</p>
<p>ONTAP ontapi 수집기가 데이터를 표시하는 비어 있거나 "0" 메트릭이 표시됩니다.</p>	<p>ONTAP REST는 ONTAP 시스템에서만 내부적으로 사용되는 메트릭은 보고하지 않습니다. 예를 들어, 시스템 애그리게이트는 ONTAP REST에서 수집되지 않고 "data" 유형의 SVM만 수집됩니다.</p> <p>0개 또는 빈 데이터를 보고할 수 있는 ONTAP REST 메트릭의 다른 예:</p> <p>InternalVolumes: Rest가 vol0을 더 이상 보고하지 않습니다.        집계: REST가 더 이상 aggr0을 보고하지 않습니다.        스토리지: 대부분의 메트릭은 내부 볼륨 메트릭의 롤업이며 위의 영향을 받습니다.        스토리지 가상 시스템: REST는 더 이상 '데이터'(예: '클러스터', 'GMT', '노드')가 아닌 SVM 유형을 보고하지 않습니다.</p> <p>또한 기본 성능 폴링 기간이 15분에서 5분으로 변경되어 데이터가 있는 그래프의 모양이 변경될 수 있습니다. 폴링 빈도가 높으면 더 많은 데이터 포인트를 표시할 수 있습니다.</p>

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

**7-Mode 데이터 수집기에서 작동하는 NetApp Data ONTAP**

7-Mode에서 작동하는 Data ONTAP 소프트웨어를 사용하는 스토리지 시스템의 경우, 7-Mode 데이터 수집기를 사용합니다. 이 수집기는 CLI를 사용하여 용량 및 성능 데이터를 얻습니다.



## 용어

Data Infrastructure Insights는 NetApp 7-Mode 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. 획득한 각 자산 유형에 대해 이 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.



이 데이터 수집기는 입니다 "사용되지 않음".

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	디스크
RAID 그룹	디스크 그룹
파일러	스토리지
파일러	스토리지 노드
집계	스토리지 풀
LUN을 클릭합니다	볼륨
볼륨	내부 볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

이 데이터 수집기를 구성하고 사용하려면 다음이 필요합니다.

- FAS 스토리지 컨트롤러 및 파트너의 IP 주소입니다.
- 포트 443
- 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

필드에 입력합니다	설명
스토리지 시스템의 주소입니다	NetApp 스토리지 시스템의 IP 주소 또는 정규화된 도메인 이름입니다

필드에 입력합니다	설명
사용자 이름	NetApp 스토리지 시스템의 사용자 이름입니다
암호	NetApp 스토리지 시스템의 암호입니다
클러스터의 HA 파트너의 주소입니다	HA 파트너에 대한 IP 주소 또는 정규화된 도메인 이름입니다
클러스터에 있는 HA 파트너의 사용자 이름입니다	HA 파트너의 사용자 이름입니다
클러스터에 있는 HA 파트너 파일러의 암호	HA 파트너의 암호입니다

#### 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 20분입니다.
연결 유형	HTTPS 또는 HTTP도 기본 포트를 표시합니다
연결 포트를 재정의합니다	비어 있는 경우 연결 유형 필드에서 기본 포트를 사용하고, 그렇지 않으면 사용할 연결 포트를 입력합니다
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

#### 스토리지 시스템 접속입니다

이 데이터 수집기에 대한 기본 관리 사용자를 사용하는 대신 NetApp 스토리지 시스템에서 직접 관리 권한을 가진 사용자를 구성하여 데이터 수집기가 NetApp 스토리지 시스템에서 데이터를 획득할 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 - \*": 이 옵션을 사용하면 데이터 인프라 Insights에서 모든 NetApp 스토리지 API 명령을 실행할 수 있습니다.

ZAPI를 사용하려면 이 명령이 필요합니다.

- "login-http-admin": Data Infrastructure Insights가 HTTP를 통해 NetApp 스토리지에 연결할 수 있도록 하려면 이 옵션을 사용합니다. ZAPI를 사용하려면 이 명령이 필요합니다.
- "security-api-vfiler": 이 옵션을 사용하면 Data Infrastructure Insights에서 NetApp 스토리지 API 명령을 실행하여 vFiler 유닛 정보를 검색할 수 있습니다.
- "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, \_
- login-http-admin, api- \*, security-api-vfile, CLI -

### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
수신 401 HTTP 응답 또는 13003 ZAPI 오류 코드 및 ZAPI는 "불충분한 권한" 또는 "이 명령에 대해 인증되지 않음"을 반환합니다.	사용자 이름과 암호, 사용자 권한/권한을 확인합니다.
"명령 실행 실패" 오류	사용자가 장치에 대해 다음 권한을 가지고 있는지 확인합니다. • api- * • cli- • df • CLI-ifconfig • CLI-lun • CLI-operations • CLI-rdfile • cli-snap • login-http-admin • security-api-vfiler 또한 ONTAP 버전이 데이터 인프라 인사이트에서 지원되는지 확인하고 사용된 자격 증명과 장치 자격 증명이 일치하는지 확인합니다
클러스터 버전이 8.1 미만임	클러스터 최소 지원 버전은 8.1입니다. 최소 지원 버전으로 업그레이드하십시오.
ZAPI는 "cluster role is not cluster_mgmt LIF" 를 반환합니다.	AU는 클러스터 관리 IP와 통신해야 합니다. IP를 확인하고 필요한 경우 다른 IP로 변경합니다
오류: "7 모드 파일러는 지원되지 않습니다."	이 데이터 수집기를 사용하여 7 모드 파일러를 검색할 경우 이 문제가 발생할 수 있습니다. 대신 IP를 cDOT 파일러를 가리키도록 변경합니다.
재시도 후 ZAPI 명령이 실패합니다	AU가 클러스터와 통신 문제를 겪고 있습니다. 네트워크, 포트 번호 및 IP 주소를 확인합니다. 또한 사용자는 AU 시스템의 명령줄에서 명령을 실행해야 합니다.
AU가 ZAPI에 연결하지 못했습니다	IP/포트 연결을 확인하고 ZAPI 구성을 어설션합니다.
AU가 HTTP를 통해 ZAPI에 연결하지 못했습니다	ZAPI 포트가 일반 텍스트를 허용하는지 확인합니다. AU가 SSL 소켓에 일반 텍스트를 보내려고 하면 통신이 실패합니다.

문제:	다음을 시도해 보십시오.
SSLException 과 통신이 실패합니다	AU가 파일러의 일반 텍스트 포트에 SSL을 전송하려고 합니다. ZAPI 포트가 SSL을 허용하는지 또는 다른 포트를 사용하는지 확인합니다.
추가 연결 오류: ZAPI 응답에는 오류 코드 13001, "데이터베이스가 열려 있지 않습니다." ZAPI 오류 코드가 60이고 응답에는 "API가 시간에 완료되지 않았습니다."가 포함되어 있습니다. ZAPI 응답에는 "initialize_session() returned NULL environment" ZAPI가 포함되어 있습니다. ZAPI 오류 코드는 14007이고 응답에는 "노드가 정상 상태가 아닙니다"가 포함되어 있습니다.	네트워크, 포트 번호 및 IP 주소를 확인합니다. 또한 사용자는 AU 시스템의 명령줄에서 명령을 실행해야 합니다.
ZAPI에서 소켓 시간 초과 오류	파일러 연결 및/또는 시간 초과를 확인하십시오.
"C Mode 클러스터는 7 Mode 데이터 소스에서 지원되지 않습니다." 오류	IP를 확인하고 IP를 7-Mode 클러스터로 변경합니다.
"vFiler에 연결하지 못했습니다" 오류	구입 사용자 기능에는 최소한 API-* security-api-vFiler login-http-admin 파일러가 최소 ONTAPI 버전 1.7을 실행하고 있는지 확인합니다.

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

### NetApp E-Series 레거시 SANtricity API 데이터 수집기

NetApp E-Series 레거시 SANtricity API 데이터 수집기가 인벤토리 및 성능 데이터를 수집합니다. Collector는 동일한 구성을 사용하여 동일한 데이터를 보고하는 펌웨어 7.x+를 지원합니다.

#### 용어

Cloud INSIGHT는 NetApp E-Series 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	Data Infrastructure Insights 용어
디스크	디스크
볼륨 그룹	디스크 그룹
스토리지	스토리지
컨트롤러	스토리지 노드
볼륨 그룹	스토리지 풀
볼륨	볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### E-Series 용어(랜딩 페이지)

다음 용어는 NetApp E-Series 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

## 스토리지

- 모델 - 장치의 모델 이름입니다.
- Vendor – 새 데이터 소스를 구성할 때 표시되는 공급업체 이름입니다
- 일련 번호 – 스토리지 일련 번호입니다. NetApp Clustered Data ONTAP과 같은 클러스터 아키텍처 스토리지 시스템에서 이 일련 번호는 개별 “스토리지 노드” 일련 번호보다 덜 유용할 수 있습니다
- IP – 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다
- 마이크로코드 버전 – 펌웨어
- 물리적 용량 – 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2의 합계
- 지연 시간 – 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. Data Infrastructure Insights는 이러한 가치를 직접 소싱하는 것이 좋지만, 그렇게 할 경우에는 그렇지 않은 경우가 많습니다. Data Infrastructure Insights는 이러한 기능을 제공하는 어레이 대신 일반적으로 개별 볼륨의 통계에서 파생된 IOPS 가중 계산을 수행합니다.
- 처리량 – 처리량(throughput)을 보이는 스토리지의 총 호스트입니다. 어레이에서 직접 소싱하는 것이 가장 좋으며, 사용할 수 없는 경우 Data Infrastructure Insights에서는 볼륨의 처리량을 합산하여 이 가치를 도출합니다
- 관리 - 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Data Infrastructure Insights 데이터 소스에 의해 프로그래밍 방식으로 생성됩니다

## 스토리지 풀

- 스토리지 – 이 풀이 상주하는 스토리지 시스템입니다. 필수입니다
- 형식 - 가능성 목록 목록의 설명 값입니다. 가장 일반적인 것은 "씬 프로비저닝" 또는 "RAID 그룹"입니다.
- 노드 – 이 스토리지 배열의 아키텍처가 특정 스토리지 노드에 속해 있는 경우, 이 스토리지 배열의 이름은 해당 랜딩 페이지의 하이퍼링크로 표시됩니다
- Flash Pool을 사용합니다. 예/아니요 값입니다
- 중복 – RAID 레벨 또는 보호 체계. E-Series는 DDP 풀에 대해 “RAID 7”을 보고합니다
- 용량 – 이 값은 논리적 사용 용량, 가용 용량 및 총 논리적 용량, 그리고 이 용량 전체에서 사용된 비율입니다. 두 가지 가치 모두 E-Series의 "보존" 용량으로, E-Series의 자체 사용자 인터페이스에서 표시할 수 있는 것보다 더 많은 수와 비율을 제공합니다
- 과도하게 커밋된 용량 – 효율성 기술을 통해 스토리지 풀의 논리적 용량보다 큰 볼륨 또는 내부 볼륨 용량의 합계를 할당한 경우 여기에 있는 백분율 값은 0%보다 큽니다.
- 스냅샷 – 스토리지 풀 아키텍처가 스냅샷 전용 영역에 해당 용량의 일부를 할당하는 경우 사용된 스냅샷 용량 및 총 용량입니다
- 사용률 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 사용 중 가장 높은 비율을 나타내는 백분율 값입니다. 디스크 사용률이 반드시 스토리지 성능과 강력한 상관 관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 재구축, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지의 복제 구현으로 인해 디스크 사용률이 높아지고 볼륨 작업 부하로 표시되지 않을 수 있습니다.
- IOPS – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다. 특정 플랫폼에서 디스크 IOP를 사용할 수 없는 경우 이 값은 이 스토리지 풀에 있는 모든 볼륨의 볼륨 IOPS 합에서 가져옵니다
- 처리량 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다. 특정 플랫폼에서 디스크 처리량을 사용할 수 없는 경우 이 값은 이 스토리지 풀에 있는 모든 볼륨의 전체 볼륨 합에서 구할 수 있습니다

## 스토리지 노드

- 스토리지 – 이 노드가 속한 스토리지 시스템입니다. 필수입니다
- HA 파트너 – 노드가 1개 노드로 페일오버되고 다른 1개 노드만 페일오버되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다
- 상태 - 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다
- 모델 - 노드의 모델 이름입니다
- 버전 - 디바이스의 버전 이름입니다.
- 일련 번호 - 노드 일련 번호입니다
- 메모리 – 사용 가능한 경우 베이스 2 메모리
- 사용률 – 일반적으로 CPU 사용률 번호 또는 NetApp ONTAP의 경우 컨트롤러 스트레스 인덱스입니다. NetApp E-Series에서는 현재 활용률을 사용할 수 없습니다
- IOPS – 이 컨트롤러의 호스트 기반 IOP를 나타내는 숫자입니다. 이상적으로는 스토리지에서 직접 소싱하는 것이 이상적이며, 사용할 수 없는 경우 이 노드에 배타적으로 속하는 볼륨의 모든 IOP를 합산하여 계산됩니다.
- 지연 시간 – 이 컨트롤러의 일반적인 호스트 지연 시간 또는 응답 시간을 나타내는 숫자입니다. 이상적으로는 스토리지에서 직접 소싱하는 것이 이상적이며, 사용할 수 없는 경우 이 노드에 배타적으로 속하는 볼륨에서 IOPS 가중 계산을 수행하여 계산됩니다.
- 처리량 – 이 컨트롤러의 호스트 기반 처리량을 나타내는 숫자입니다. 이상적으로는 스토리지에서 직접 소싱하는 것이 이상적이며, 사용할 수 없는 경우 이 노드에 배타적으로 속하는 볼륨의 모든 처리량을 합산하여 계산됩니다.
- 프로세서 - CPU 수입니다

## 요구 사항

- 어레이에 있는 각 컨트롤러의 IP 주소입니다
- 포트 요구 사항 2463

## 구성

필드에 입력합니다	설명
심표로 구분된 Array SANtricity 컨트롤러 IP 목록입니다	스토리지 컨트롤러의 IP 주소 및/또는 정규화된 도메인 이름입니다

## 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 30분입니다
성능 폴링 간격 최대 3600초	기본값은 300초입니다

## 문제 해결

이 데이터 수집기에 대한 추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## NetApp E-Series REST 데이터 수집기

NetApp E-Series REST 데이터 수집기는 인벤토리 및 성능 데이터를 수집합니다. Collector는 동일한 구성을 사용하여 동일한 데이터를 보고하는 펌웨어 7.x+를 지원합니다. REST Collector는 스토리지 풀의 암호화 상태와 관련 디스크 및 볼륨의 암호화 상태를 모니터링하여 스토리지 노드 CPU 사용률을 성능 카운터로 제공합니다. 이는 레거시 SANtricity E-Series Collector에는 제공되지 않는 기능입니다.

### 용어

Cloud Insight는 NetApp E-Series에서 REST를 사용하여 다음 인벤토리 정보를 수집합니다. 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	Data Infrastructure Insights 용어
디스크	디스크
볼륨 그룹	디스크 그룹
스토리지	스토리지
컨트롤러	스토리지 노드
볼륨 그룹	스토리지 풀
볼륨	볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 요구 사항

- 어레이에 있는 각 컨트롤러의 IP 주소입니다
- 이 Collector는 \* 기본 REST API 기능 \* 을 갖춘 E-Series 모델 어레이만 지원합니다. E-Series 조직은 이전 E-Series 어레이에 대해 설치 가능한 REST API 배포를 오프 어레이에 출고합니다. 이 수집기는 이 시나리오를 지원하지 않습니다. 이전 스토리지 시스템을 사용하는 사용자는 Data Infrastructure Insights의 "[E-Series SANtricity API를 참조하십시오](#)" Collector를 계속 사용해야 합니다.
- "E-Series Controller IP addresses" 필드는 쉼표로 구분된 2개의 IP/호스트 이름으로 구성된 문자열을 지원합니다. 첫 번째 IP/호스트 이름에 액세스할 수 없는 경우 수집기는 두 번째 IP/호스트 이름을 지능적으로 시도합니다.
- HTTPS 포트: 기본값은 8443입니다.

### 구성

필드에 입력합니다	설명
E-Series 컨트롤러 IP 주소	스토리지 컨트롤러에 대해 쉼표로 구분된 IP 주소 및/또는 정규화된 도메인 이름입니다

### 고급 구성

필드에 입력합니다	설명
재고 풀링 간격(분)	기본값은 30분입니다
성능 풀링 간격 최대 3600초	기본값은 300초입니다

### E-Series 용어(랜딩 페이지)

다음 용어는 NetApp E-Series 자산 랜딩 페이지에서 볼 수 있는 오브젝트 또는 참조에 적용됩니다. 이러한 용어 중 다수는 다른 데이터 수집기에도 적용됩니다.

#### 스토리지

- 모델 - 장치의 모델 이름입니다.
- Vendor – 새 데이터 소스를 구성할 때 표시되는 공급업체 이름입니다
- 일련 번호 – 스토리지 일련 번호입니다. NetApp Clustered Data ONTAP과 같은 클러스터 아키텍처 스토리지 시스템에서 이 일련 번호는 개별 “스토리지 노드” 일련 번호보다 덜 유용할 수 있습니다
- IP – 일반적으로 데이터 소스에 구성된 IP 또는 호스트 이름이 됩니다
- 마이크로코드 버전 – 펌웨어
- 물리적 용량 – 역할에 관계없이 시스템의 모든 물리적 디스크에 대한 기본 2의 합계
- 지연 시간 – 읽기 및 쓰기 모두에서 호스트에서 발생하는 워크로드를 나타냅니다. Data Infrastructure Insights는 이러한 가치를 직접 소싱하는 것이 좋지만, 그렇게 할 경우에는 그렇지 않은 경우가 많습니다. Data Infrastructure Insights는 이러한 기능을 제공하는 어레이 대신 일반적으로 개별 볼륨의 통계에서 파생된 IOPS 가중 계산을 수행합니다.
- 처리량 – 처리량(throughput)을 보이는 스토리지의 총 호스트입니다. 어레이에서 직접 소싱하는 것이 가장 좋으며, 사용할 수 없는 경우 Data Infrastructure Insights에서는 볼륨의 처리량을 합산하여 이 가치를 도출합니다
- 관리 - 장치의 관리 인터페이스에 대한 하이퍼링크가 포함될 수 있습니다. 인벤토리 보고의 일부로 Data Infrastructure Insights 데이터 소스에 의해 프로그래밍 방식으로 생성됩니다

#### 스토리지 풀

- 스토리지 – 이 풀이 상주하는 스토리지 시스템입니다. 필수입니다
- 형식 - 가능성 목록 목록의 설명 값입니다. 가장 일반적인 것은 "씬 프로비저닝" 또는 "RAID 그룹"입니다.
- 노드 – 이 스토리지 배열의 아키텍처가 특정 스토리지 노드에 속해 있는 경우, 이 스토리지 배열의 이름은 해당 랜딩 페이지의 하이퍼링크로 표시됩니다
- Flash Pool을 사용합니다. 예/아니요 값입니다
- 중복 – RAID 레벨 또는 보호 체계. E-Series는 DDP 풀에 대해 “RAID 7”을 보고합니다
- 용량 – 이 값은 논리적 사용 용량, 가용 용량 및 총 논리적 용량, 그리고 이 용량 전체에서 사용된 비율입니다. 두 가지 가치 모두 E-Series의 "보존" 용량으로, E-Series의 자체 사용자 인터페이스에서 표시할 수 있는 것보다 더 많은 수와 비율을 제공합니다
- 과도하게 커밋된 용량 – 효율성 기술을 통해 스토리지 풀의 논리적 용량보다 큰 볼륨 또는 내부 볼륨 용량의 합계를 할당한 경우 여기에 있는 백분율 값은 0%보다 큽니다.
- 스냅샷 – 스토리지 풀 아키텍처가 스냅샷 전용 영역에 해당 용량의 일부를 할당하는 경우 사용된 스냅샷 용량 및 총 용량입니다
- 사용률 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 사용 중 가장 높은 비율을 나타내는 백분율 값입니다.



디스크 사용률이 반드시 스토리지 성능과 강력한 상관 관계가 있는 것은 아닙니다. 호스트 기반 워크로드가 없을 경우 디스크 재구축, 중복 제거 작업 등으로 인해 사용률이 높을 수 있습니다. 또한 많은 스토리지의 복제 구현으로 인해 디스크 사용률이 높아지고 볼륨 작업 부하로 표시되지 않을 수 있습니다.

- IOPS – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 IOPS 합계입니다. 특정 플랫폼에서 디스크 IOP를 사용할 수 없는 경우 이 값은 이 스토리지 풀에 있는 모든 볼륨의 볼륨 IOPS 합에서 가져옵니다
- 처리량 – 이 스토리지 풀에 용량을 제공하는 모든 디스크의 총 처리량입니다. 특정 플랫폼에서 디스크 처리량을 사용할 수 없는 경우 이 값은 이 스토리지 풀에 있는 모든 볼륨의 전체 볼륨 합에서 구할 수 있습니다

## 스토리지 노드

- 스토리지 – 이 노드가 속한 스토리지 시스템입니다. 필수입니다
- HA 파트너 – 노드가 1개 노드로 페일오버되고 다른 1개 노드만 페일오버되는 플랫폼에서는 일반적으로 이 노드에 표시됩니다
- 상태 - 노드의 상태입니다. 배열이 데이터 소스에 의해 인벤토리를 작성할 수 있을 만큼 양호한 경우에만 사용할 수 있습니다
- 모델 - 노드의 모델 이름입니다
- 버전 - 디바이스의 버전 이름입니다.
- 일련 번호 - 노드 일련 번호입니다
- 메모리 – 사용 가능한 경우 베이스 2 메모리
- 사용률 – 일반적으로 CPU 사용률 번호 또는 NetApp ONTAP의 경우 컨트롤러 스트레스 인덱스입니다. NetApp E-Series에서는 현재 활용률을 사용할 수 없습니다
- IOPS – 이 컨트롤러의 호스트 기반 IOP를 나타내는 숫자입니다. 이상적으로는 스토리지에서 직접 소싱하는 것이 이상적이며, 사용할 수 없는 경우 이 노드에 배타적으로 속하는 볼륨의 모든 IOP를 합산하여 계산됩니다.
- 지연 시간 – 이 컨트롤러의 일반적인 호스트 지연 시간 또는 응답 시간을 나타내는 숫자입니다. 이상적으로는 스토리지에서 직접 소싱하는 것이 이상적이며, 사용할 수 없는 경우 이 노드에 배타적으로 속하는 볼륨에서 IOPS 가중 계산을 수행하여 계산됩니다.
- 처리량 – 이 컨트롤러의 호스트 기반 처리량을 나타내는 숫자입니다. 이상적으로는 스토리지에서 직접 소싱하는 것이 이상적이며, 사용할 수 없는 경우 이 노드에 배타적으로 속하는 볼륨의 모든 처리량을 합산하여 계산됩니다.
- 프로세서 - CPU 수입니다

## 문제 해결

이 데이터 수집기에 대한 추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## NetApp HCI 관리 서버 데이터 수집기 구성

NetApp HCI 관리 서버 데이터 수집기는 NetApp HCI 호스트 정보를 수집하고 관리 서버 내의 모든 개체에 대해 읽기 전용 권한을 필요로 합니다.

이 데이터 수집기는 \* NetApp HCI 관리 서버에서만 획득합니다 \*. 스토리지 시스템에서 데이터를 수집하려면 도 구성해야 합니다 ["NetApp SolidFire를 참조하십시오"](#) 데이터 수집기.

## 용어

Data Infrastructure Insights는 이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. 획득한 각 자산 유형에 대해 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
가상 디스크	디스크
호스트	호스트
가상 머신	가상 머신
데이터 저장소	데이터 저장소
LUN을 클릭합니다	볼륨
Fibre Channel 포트입니다	포트

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

## 요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- NetApp HCI 관리 서버의 IP 주소입니다
- NetApp HCI 관리 서버의 읽기 전용 사용자 이름 및 암호입니다
- NetApp HCI 관리 서버의 모든 개체에 대한 읽기 전용 권한
- NetApp HCI 관리 서버에서 SDK 액세스 – 일반적으로 이미 설정되어 있습니다.
- 포트 요구 사항: http-80 https-443
- 액세스 확인:
  - 위의 사용자 이름과 암호를 사용하여 NetApp HCI 관리 서버에 로그인합니다
  - SDK가 활성화되었는지 확인합니다. 텔넷 <VC\_IP> 443

## 설치 및 연결

필드에 입력합니다	설명
이름	데이터 수집기의 고유 이름입니다
획득 장치	획득 장치의 이름입니다

## 구성

필드에 입력합니다	설명
NetApp HCI 스토리지 클러스터 MVIP	관리 가상 IP 주소
SolidFire 관리 노드(mNode)	관리 노드 IP 주소입니다
사용자 이름입니다	NetApp HCI 관리 서버에 액세스하는 데 사용되는 사용자 이름입니다

필드에 입력합니다	설명
암호	NetApp HCI 관리 서버에 액세스하는 데 사용되는 암호입니다
vCenter 사용자 이름입니다	vCenter의 사용자 이름입니다
vCenter 암호	vCenter의 암호입니다

#### 고급 구성

고급 구성 화면에서 \* VM 성능 \* 확인란을 선택하여 성능 데이터를 수집합니다. 인벤토리 수집은 기본적으로 사용하도록 설정됩니다. 다음 필드를 구성할 수 있습니다.

필드에 입력합니다	설명
재고 폴링 간격(분)	귀가 명이 20개
VM 필터링 기준	클러스터, 데이터 센터 또는 ESX 호스트를 선택합니다
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	VM 포함 또는 제외 여부를 지정합니다
장치 목록을 필터링합니다	필터링할 VM 목록(심표로 구분 또는 값에서 심표를 사용하는 경우 세미콜론으로 구분) - ESX_host, 클러스터 및 데이터 센터별 필터링에만 사용
성능 폴링 간격(초)	기본값은 300입니다

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
오류: VM을 필터링하는 포함 목록은 비워 둘 수 없습니다	포함 목록을 선택한 경우 유효한 데이터 센터, 클러스터 또는 호스트 이름을 나열하여 VM을 필터링합니다
오류: IP에서 VirtualCenter에 대한 연결을 인스턴스화하지 못했습니다	가능한 해결 방법: * 입력한 자격 증명 및 IP 주소를 확인합니다. * 인프라 클라이언트를 사용하여 가상 센터와 통신해 보십시오. * Managed Object Browser(예: MOB)를 사용하여 Virtual Center와 통신해 보십시오.
오류: IP의 VirtualCenter에는 JVM에 필요한 일치하지 않는 인증서가 있습니다	가능한 해결책: * 권장: 더 강력한(예 1024비트) RSA 키. * 권장하지 않음: JDK.certpath 제약 조건을 활용하도록 JVM java.security 구성을 수정하십시오. disabledAlgorithms 512비트 RSA 키를 허용합니다. 에서 JDK 7 업데이트 40 릴리스 노트를 참조하십시오 "<a href="http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html" class="bare">http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"</a>

추가 정보는 에서 찾을 수 있습니다 "지원" 페이지 또는 에 있습니다 "Data Collector 지원 매트릭스".

## NetApp SolidFire All-Flash 어레이 데이터 수집기입니다

NetApp SolidFire All-Flash 어레이 데이터 수집기는 iSCSI 및 파이버 채널 SolidFire 구성 모두에서 인벤토리 및 성능 수집을 지원합니다.

SolidFire 데이터 수집기는 SolidFire REST API를 사용합니다. 데이터 수집기가 상주하는 수집 장치는 SolidFire 클러스터 관리 IP 주소의 TCP 포트 443에 대한 HTTPS 연결을 시작할 수 있어야 합니다. 데이터 수집기는 SolidFire 클러스터에서 REST API 쿼리를 수행할 수 있는 자격 증명이 필요합니다.

### 용어

Data Infrastructure Insights는 NetApp SolidFire All-Flash 어레이 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
드라이브	디스크
클러스터	스토리지
노드	스토리지 노드
볼륨	볼륨
Fibre Channel 포트입니다	포트
볼륨 액세스 그룹, LUN 할당	볼륨 맵
iSCSI 세션	볼륨 마스크

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 요구 사항

다음은 이 데이터 수집기를 구성하기 위한 요구 사항입니다.

- 관리 가상 IP 주소
- 읽기 전용 사용자 이름 및 자격 증명
- 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
연결 유형	연결 유형을 선택합니다
통신 포트	NetApp API에 사용되는 포트입니다
재고 폴링 간격(분)	기본값은 20분입니다
성능 폴링 간격(초)	기본값은 300초입니다

#### 문제 해결

SolidFire에서 오류를 보고하면 Data Infrastructure Insights에 다음과 같이 표시됩니다.

\_ 데이터 검색을 시도하는 동안 SolidFire 장치로부터 오류 메시지가 수신되었습니다. 호출은 <method>(<parameterString> )이었습니다. 장치의 오류 메시지는 다음과 같습니다(장치 설명서 확인). <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.

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

#### NetApp StorageGRID 데이터 수집기

NetApp StorageGRID 데이터 수집기는 StorageGRID 구성의 인벤토리 및 성능 수집을 지원합니다.



StorageGRID는 다른 물리적 TB에서 관리 단위 비율로 측정됩니다. 40TB의 포맷되지 않은 StorageGRID 용량마다 1로 충전됩니다 "[관리 장치\(MU\)](#)".

#### 용어

Data Infrastructure Insights는 NetApp StorageGRID 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. 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	Data Infrastructure Insights 용어
StorageGRID	스토리지
노드	노드
테넌트	스토리지 풀
버킷	내부 볼륨

## 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 주소입니다	StorageGRID 어플라이언스의 관리 가상 IP 주소입니다
사용자 이름	StorageGRID 어플라이언스에 로그인하는 데 사용되는 이름입니다
암호	StorageGRID 어플라이언스에 로그인하는 데 사용되는 암호입니다

## 고급 구성

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 60분입니다
성능 폴링 간격(초)	기본값은 900초입니다

## SSO(Single Sign-On)

를 클릭합니다 "StorageGRID" 펌웨어 버전은 해당 API 버전을 사용하며, 3.0 API 및 최신 버전은 SSO(Single Sign-On) 로그인을 지원합니다.

펌웨어 버전입니다	API 버전입니다	SSO(Single Sign On) 지원
11.1	2	아니요
11.2	3.0	예
11.5	3.3	예

## 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Nutanix NX 데이터 수집기

Data Infrastructure Insights는 Nutanix 데이터 수집기를 사용하여 Nutanix NX 스토리지 시스템의 인벤토리 및 성능 데이터를 검색합니다.

## 용어

Data Infrastructure Insights는 Nutanix 데이터 수집기에서 다음과 같은 인벤토리 정보를 수집합니다. Data

Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
스토리지 풀	스토리지 풀
Nutanix 컨테이너	내부 볼륨
Nutanix 컨테이너	파일 공유
NFS 공유	공유

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- 클러스터의 외부 데이터 서비스 IP 주소입니다
- volume\_groups를 사용하지 않는 한 읽기 전용 사용자 이름 및 암호가 필요합니다. 이 경우 Admin 사용자 이름과 암호가 필요합니다
- 포트 요구 사항: HTTPS 443

#### 구성

필드에 입력합니다	설명
PRISM 외부 IP 주소	클러스터의 외부 데이터 서비스 IP 주소입니다
사용자 이름입니다	Admin 계정의 사용자 이름입니다
암호	Admin 계정의 암호입니다

#### 고급 구성

필드에 입력합니다	설명
TCP 포트	Nutanix 어레이에 연결하는 데 사용되는 TCP 포트입니다. 기본값은 9440입니다.
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 60분입니다.
성능 폴링 간격(초)	성능 폴링 간격입니다. 기본값은 300초입니다.

#### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## OpenStack 데이터 수집기

OpenStack(REST API/KVM) 데이터 수집기는 모든 OpenStack 인스턴스에 대한 인벤토리 데이터를 수집하며 선택적으로 VM 성능 데이터를 가져옵니다.

## 요구 사항

- OpenStack 컨트롤러의 IP 주소입니다
- OpenStack 관리자 역할 자격 증명 및 Linux KVM 하이퍼바이저에 대한 sudo 액세스 admin 계정 또는 admin 등가 권한을 사용하지 않는 경우, 데이터 수집기 사용자 ID에 대해 휴식을 취할 기본 정책을 식별하기 위해 시행착오 및 오류를 사용해야 합니다.
- 성능 수집을 위해 OpenStack Gnocchi 모듈을 설치하고 구성해야 합니다. Gnocchi 구성은 각 하이퍼바이저에 대한 nova.conf 파일을 편집한 다음 각 하이퍼바이저에서 Nova Compute 서비스를 다시 시작하여 수행합니다. 옵션 이름이 OpenStack의 다양한 릴리즈에서 변경되었습니다.
  - 아이스하우스
  - 준오
  - 킬로
  - 리버티
  - 미타카
  - 뉴턴
  - 옥타
- CPU 통계의 경우 컴퓨팅 노드의 /etc/nova/nova.conf에서 “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
  - Gnocchi Performance Service용 8777
  - Glance 이미지 서비스의 경우 9292 \* 참고 \* 포트는 특정 서비스에 바인딩되며, 대규모 환경의 컨트롤러 또는 다른 호스트에서 서비스가 실행될 수 있습니다.

## 구성

필드에 입력합니다	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 이름입니다
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



필드에 입력합니다	설명
KVM Sudo 암호	KVM Sudo 암호

### 고급 구성

필드에 입력합니다	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
SSH 포트	SSH에 사용되는 포트입니다
SSH 프로세스 재시도	인벤토리 재시도 횟수입니다
재고 폴링 간격(분)	재고 조사 사이의 간격입니다. 기본값은 20분입니다.

### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
"정책 허용 안 함" 또는 "권한이 없습니다"로 시작하는 오류 메시지와 함께 "구성 오류"	* IP 주소 확인 * 사용자 이름 및 암호 확인

추가 정보는 [에서](#) 찾을 수 있습니다 ["지원"](#) 페이지 또는 [에](#) 있습니다 ["Data Collector 지원 매트릭스"](#).

## Oracle ZFS Storage Appliance 데이터 수집기

Data Infrastructure Insights는 Oracle ZFS Storage Appliance 데이터 수집기를 사용하여 인벤토리 및 성능 데이터를 수집합니다.

### 용어

Data Infrastructure Insights는 Oracle ZFS 데이터 수집기를 사용하여 재고 정보를 수집합니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크(SSD)	디스크
클러스터	스토리지
컨트롤러	스토리지 노드
LUN을 클릭합니다	볼륨
LUN 매핑	볼륨 맵

공급업체/모델 기간	Data Infrastructure Insights 용어
초기자, 대상	볼륨 마스크
공유	내부 볼륨

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

#### 요구 사항

- ZFS Controller-1 및 ZFS Controller-2의 호스트 이름
- 관리자 사용자 이름 및 암호
- 포트 요구 사항: 215 HTTP/HTTPS

#### 필수 성능 메트릭

Oracle ZFS 어플라이언스는 스토리지 관리자에게 성능 통계를 수집할 수 있는 많은 유연성을 제공합니다. Data Infrastructure Insights에서는 고가용성 쌍의 \_Each\_ 컨트롤러를 다음 메트릭을 캡처하도록 구성할 것으로 예상합니다.

- SMB2.ops [공유]
- NFS3.ops [share]
- NFS4.ops [share]
- NFS4-1.ops [공유]

컨트롤러가 이러한 중 일부 또는 전부를 캡처하지 못하면 Data Infrastructure Insights가 "내부 볼륨"의 워크로드를 수행하지 않거나 과소 보고할 수 있습니다.

#### 구성

필드에 입력합니다	설명
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
연결 유형	HTTPS 또는 HTTP도 기본 포트를 표시합니다
연결 포트를 재정의합니다	비어 있는 경우 연결 유형 필드에서 기본 포트를 사용하고, 그렇지 않으면 사용할 연결 포트를 입력합니다
인벤토리 폴링 간격입니다	기본값은 60초입니다
성능 폴링 간격(초)	기본값은 300입니다.

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
"잘못된 로그인 자격 증명"	ZFS 사용자 계정 및 암호를 확인합니다
"REST 서비스가 비활성화되었습니다" 오류 메시지와 함께 "구성 오류"	이 장치에서 REST 서비스가 활성화되어 있는지 확인합니다.
"User unauthorized for command" 오류 메시지와 함께 "구성 오류"	<p>이 오류는 구성된 사용자에게 대해 특정 역할(예: 'advanced_analytics')이 포함되지 않았기 때문일 수 있습니다.</p> <p>읽기 전용 역할을 가진 사용자에게 대해 분석 범위를 적용하면 오류가 제거될 수 있습니다. 다음 단계를 수행하십시오.</p> <ol style="list-style-type: none"><li>1. ZFS 시스템의 Configuration → Users 화면에서 해당 역할 위로 마우스를 이동한 후 두 번 클릭하여 편집할 수 있습니다</li><li>2. 범위 드롭다운 메뉴에서 "분석"을 선택합니다. 가능한 속성 목록이 나타납니다.</li><li>3. 맨 위에 있는 확인란을 클릭하면 세 개의 속성이 모두 선택됩니다.</li><li>4. 오른쪽에 있는 추가 버튼을 클릭합니다.</li><li>5. 팝업 창의 오른쪽 위에 있는 적용 단추를 클릭합니다. 팝업 창이 닫힙니다.</li></ol>

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## Pure Storage FlashArray 데이터 수집기

Data Infrastructure Insights는 Pure Storage FlashArray 데이터 수집기를 사용하여 인벤토리 및 성능 데이터를 수집합니다.

### 용어

Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 자산에 사용되는 가장 일반적인 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
드라이브(SSD)	디스크
스토리지	스토리지

공급업체/모델 기간	Data Infrastructure Insights 용어
컨트롤러	스토리지 노드
볼륨	볼륨
LUN 매핑	볼륨 맵
초기자, 대상	볼륨 마스크

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 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

필드에 입력합니다	설명
FlashArray 호스트 IP 주소입니다	스토리지 시스템의 IP 주소입니다
사용자 이름입니다	관리자 권한이 있는 사용자 이름입니다
관리자 권한이 있는 계정의 암호입니다	암호

#### 고급 구성

필드에 입력합니다	설명
연결 유형	HTTP 또는 HTTPS 를 선택합니다. 기본 포트도 표시합니다.
TCP 포트를 재정의합니다	비어 있는 경우 연결 유형 필드에서 기본 포트를 사용하고, 그렇지 않으면 사용할 연결 포트를 입력합니다
재고 폴링 간격(분)	기본값은 60분입니다
성능 폴링 간격(초)	기본값은 300입니다

#### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
"유효하지 않은 로그인 자격 증명"과 "정책이 허용되지 않음" 또는 "권한이 없습니다" 오류 메시지	Pure http 인터페이스를 통해 Pure 사용자 계정 및 암호의 유효성을 검사합니다

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## Red Hat 가상화 데이터 수집기

Data Infrastructure Insights는 Red Hat Virtualization 데이터 수집기를 사용하여 가상화된 Linux 및 Microsoft Windows 워크로드로부터 인벤토리 데이터를 수집합니다.

### 용어

Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 자산에 사용되는 가장 일반적인 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
디스크	가상 디스크
호스트	호스트
가상 머신	가상 머신
스토리지 도메인	데이터 저장소
논리 단위	LUN을 클릭합니다

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 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	스토리지 시스템의 IP 주소입니다
사용자 이름입니다	관리자 권한이 있는 사용자 이름입니다
관리자 권한이 있는 계정의 암호입니다	암호

### 고급 구성

필드에 입력합니다	설명
HTTPS 통신 포트	RHEV에 대한 HTTPS 통신에 사용되는 포트입니다
재고 폴링 간격(분)	기본값은 20분입니다.

### 문제 해결

이 Data Collector에 대한 추가 정보는 에서 확인할 수 있습니다 ["지원"](#) 페이지 또는 에 있습니다 ["Data Collector 지원 매트릭스"](#).

## Rubrik CDM Data Collector

Data Infrastructure Insights는 Rubrik 데이터 수집기를 사용하여 Rubrik 스토리지 어플라이언스로부터 인벤토리 및 성능 데이터를 가져옵니다.

### 용어

Data Infrastructure Insights는 Rubrik 데이터 수집기에서 다음 인벤토리 정보를 가져옵니다. Data Infrastructure Insights에서 구입한 각 자산 유형에 대해 이 자산에 사용되는 가장 일반적인 용어가 표시되어 있습니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
클러스터	스토리지, 스토리지 풀
노드	스토리지 노드
디스크	디스크

참고: 이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 소스의 모든 경우를 나타내는 것은 아닙니다.

### 요구 사항

이 데이터 수집기를 구성하려면 다음이 필요합니다.

- Data Infrastructure Insights 수집 장치가 Rubrik 클러스터에 대한 TCP 포트 443에 대한 연결을 시작합니다. 클러스터당 Collector 1개.
- Rubrik 클러스터 IP 주소
- 클러스터에 대한 사용자 이름 및 암호.
- Rubrik 클러스터 IP 주소 또는 호스트 이름.
- 기본 인증의 경우 클러스터에 대한 사용자 이름과 암호가 필요합니다. 서비스 계정 기반 인증을 사용하려면 서비스 계정, 암호 및 조직 ID가 필요합니다
- 포트 요구 사항: HTTPS 443

### 구성

필드에 입력합니다	설명
IP	Rubrik 클러스터의 IP 주소
사용자 이름입니다	클러스터의 사용자 이름입니다
암호	클러스터의 암호입니다

### 고급 구성

재고 폴링 간격(분)	기본값은 <b>60</b> 입니다
성능 폴링 간격(초)	기본값은 300입니다

## 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

### 인벤토리

문제:	다음을 시도해 보십시오.
하나 이상의 저장소가 생성되었다는 메시지가 표시됩니다.	클러스터가 올바르게 구성되어 있고 수집기가 단일 클러스터를 가리키고 있는지 확인합니다.
디스크 API가 더 많은 데이터를 반환한다는 경고가 수신되었습니다	추가 데이터를 얻으려면 지원 부서에 문의하십시오.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## VMware vSphere Data Collector 구성

VMware vSphere용 데이터 수집기는 VM 게스트 및 ESXi 호스트 성능 및 구성 정보를 수집하며 vSphere 내의 모든 개체에 대해 읽기 전용 Privileges이 필요합니다. 2024년 8월 현재 vSphere Collector는 vSphere 환경의 로그 메시지와 일부 VMware 관련 메트릭을 추가로 제공합니다. Data Infrastructure Insights는 vSphere 8.0.1 이상의 환경에서만 VMware 로그 정보를 검색할 수 있습니다. 마찬가지로 공급업체별 메트릭은 vSphere 7+ 환경에서만 지원됩니다. 따라서 이전 vSphere 인스턴스를 가리키는 경우 해당 Collector에서 로그 및/또는 공급업체별 메트릭 확인란을 비활성화할 수 있습니다.

### 용어

Data Infrastructure Insights는 VMware vSphere Data Collector에서 다음과 같은 인벤토리 정보를 가져옵니다. 획득한 각 자산 유형에 대해 자산에 가장 일반적으로 사용되는 용어가 표시됩니다. 이 데이터 수집기를 보거나 문제를 해결할 때 다음 용어를 염두에 두십시오.

공급업체/모델 기간	Data Infrastructure Insights 용어
가상 디스크	디스크
호스트	호스트
가상 머신	가상 머신
데이터 저장소	데이터 저장소
LUN을 클릭합니다	볼륨
Fibre Channel 포트입니다	포트

이러한 용어 매핑은 일반적인 용어 매핑일 뿐이며 이 데이터 수집기의 모든 경우를 나타내는 것은 아닙니다.

### 요구 사항

이 데이터 수집기를 구성하려면 다음 정보가 필요합니다.

- Virtual Center 서버의 IP 주소입니다

- Virtual Center의 읽기 전용 사용자 이름 및 암호
- Virtual Center 내의 모든 개체에 대해 읽기 전용 권한이 필요합니다.
- Virtual Center 서버에서 SDK 액세스 – 일반적으로 이미 설정되어 있습니다.
- 포트 요구 사항: http-80 https-443
- 액세스 확인:
  - 위의 사용자 이름과 암호를 사용하여 Virtual Center Client에 로그인합니다
  - SDK가 활성화되었는지 확인합니다. 텔넷 <VC\_IP> 443

#### 설치 및 연결

필드에 입력합니다	설명
이름	데이터 수집기의 고유 이름입니다
획득 장치	획득 장치의 이름입니다

#### 구성

필드에 입력합니다	설명
가상 센터 IP 주소	Virtual Center의 IP 주소입니다
사용자 이름입니다	Virtual Center에 액세스하는 데 사용되는 사용자 이름입니다
암호	Virtual Center에 액세스하는 데 사용되는 암호입니다

#### 고급 구성

고급 구성 화면에서 \* VM 성능 \* 확인란을 선택하여 성능 데이터를 수집합니다. 인벤토리 수집은 기본적으로 사용하도록 설정됩니다. 다음 필드를 구성할 수 있습니다.

필드에 입력합니다	설명
재고 폴링 간격(분)	기본값은 20입니다
VM 필터링	클러스터, 데이터 센터 또는 ESX 호스트를 선택합니다
목록을 지정하려면 '제외' 또는 '포함'을 선택하십시오	필터 목록(클러스터, 데이터 센터 및/또는 ESX_host) 생성
재시도 횟수입니다	기본값은 3입니다
통신 포트	기본값은 443입니다



장치 목록 필터링...	이 목록은 정확히 일치하는 문자열로 구성되어야 합니다. esx_host로 필터링하려는 경우 Data Infrastructure Insights 및 vSphere에 보고된 ESX 호스트의 정확한 "이름"을 심표로 구분하여 작성해야 합니다. 이러한 "이름"은 IP 주소, 단순 호스트 이름 또는 FQDN(정규화된 도메인 이름)일 수 있습니다. 이는 해당 호스트가 vSphere에 처음 추가될 때 이름이 어떻게 지정되었는지 기준으로 결정됩니다. 클러스터별로 필터링하는 경우 하이퍼바이저에서 CI가 보고한 Data Infrastructure Insights 스타일의 클러스터 이름을 사용합니다. - Data Infrastructure Insights는 vSphere 클러스터 이름에 vSphere 데이터센터 이름 앞에 슬래시("DC1/clusterA")를 붙입니다. Data Infrastructure Insights가 데이터 센터 DC1 내의 clusterA 하이퍼바이저에서 보고하는 클러스터 이름입니다.
성능 폴링 간격(초)	기본값은 300입니다

### VMware 태그를 Data Infrastructure Insights 주식에 매핑

VMware 데이터 수집기를 사용하면 Data Infrastructure Insights 주식을 VMware에 구성된 태그로 채울 수 있습니다. 주식의 이름은 VMware 태그와 동일하게 지정해야 합니다. Data Infrastructure Insights는 항상 같은 이름의 텍스트 유형 주석을 채우고 다른 유형(숫자, 부울 등)의 주석을 채우려는 "최선의 시도"를 합니다. 주석이 다른 유형이고 데이터 수집기가 주석을 채우지 못할 경우 주석을 제거하고 텍스트 유형으로 다시 생성해야 할 수 있습니다.

VMware 태그는 대소문자를 구분하지만 Data Infrastructure Insights 태그는 대소문자를 구분하지 않습니다. 따라서 Data Infrastructure Insights에서 "소유자"라는 주석을 작성하고 VMware에서 "소유자", "소유자" 및 "소유자"라는 태그를 생성하면 이러한 모든 "소유자" 변형은 Cloud Insight의 "소유자" 주식에 매핑됩니다.

다음 사항에 유의하십시오.

- Data Infrastructure Insights는 현재 NetApp 장치에 대한 지원 정보만 자동 게시합니다.
- 이 지원 정보는 주식 형식으로 유지되므로 이를 쿼리하거나 대시보드에서 사용할 수 있습니다.
- 사용자가 주식 값을 덮어쓰거나 비우는 경우 Data Infrastructure Insights에서 주석을 업데이트할 때 이 값은 하루에 한 번 자동으로 채워집니다.

### 문제 해결

이 데이터 수집기에서 문제가 발생할 경우 다음과 같은 방법을 시도해 보십시오.

#### 인벤토리

문제:	다음을 시도해 보십시오.
오류: VM을 필터링하는 포함 목록은 비워 둘 수 없습니다	포함 목록을 선택한 경우 유효한 데이터 센터, 클러스터 또는 호스트 이름을 나열하여 VM을 필터링합니다
오류: IP에서 VirtualCenter에 대한 연결을 인스턴스화하지 못했습니다	가능한 해결 방법: * 입력한 자격 증명 및 IP 주소를 확인합니다. * VMware Infrastructure Client를 사용하여 Virtual Center와 통신해 보십시오. * Managed Object Browser(예: MOB)를 사용하여 Virtual Center와 통신해 보십시오.

문제:	다음을 시도해 보십시오.
오류: IP의 VirtualCenter에는 JVM에 필요한 일치하지 않는 인증서가 있습니다	가능한 해결책: * 권장: 더 강력한(예 1024비트) RSA 키. * 권장하지 않음: JDK.certpath 제약 조건을 활용하도록 JVM java.security 구성을 수정하십시오. disabledAlgorithms 512비트 RSA 키를 허용합니다. 에서 JDK 7 업데이트 40 릴리스 노트를 참조하십시오 "<a href="http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html" class="bare">http://www.oracle.com/technetwork/java/javase/7u40-relnotes-2004172.html"</a>

추가 정보는 에서 찾을 수 있습니다 "지원" 페이지 또는 에 있습니다 "Data Collector 지원 매트릭스".

## Data Collector 참조 - 서비스

### 노드 데이터 수집

Data Infrastructure Insights는 에이전트를 설치하는 노드에서 메트릭을 수집합니다.

#### 설치

1. 관측성 > 수집기 \* 에서 운영 체제/플랫폼을 선택합니다. 통합 데이터 수집기(Kubernetes, Docker, Apache 등)를 설치하면 노드 데이터 수집도 구성됩니다.
2. 지침에 따라 에이전트를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.

#### 개체 및 카운터

다음 개체와 해당 카운터가 노드 메트릭으로 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
노드 파일 시스템	노드 UUID 디바이스 경로 유형입니다	노드 IP 노드 이름 노드 OS 모드	사용 가능한 inode 사용 가능한 inode 총 사용된 총 Inode 총 사용량입니다
노드 디스크	노드 UUID 디스크	노드 IP 노드 이름 노드 OS입니다	입출력 시간 총 IOPS 진행 중 읽기 바이트 수(초당) 읽기 시간 총 읽기 수(초 당) 가중 IO 시간 총 쓰기 바이트 수(초 당) 쓰기 시간 총 쓰기 시간 총 쓰기 시간(초 당) 현재 디스크 대기열 길이 쓰기 시간 읽기 시간 IO 시간입니다
노드 CPU	노드 UUID CPU입니다	노드 IP 노드 이름 노드 OS입니다	시스템 CPU 사용 사용자 CPU 사용 유휴 CPU 사용 프로세서 CPU 사용 중단 CPU 사용 DPC CPU 사용

오브젝트:	식별자:	특성:	데이터 요소:
노드	노드 UUID	노드 IP 노드 이름 노드 OS입니다	커널 부팅 시간 커널 컨텍스트 스위치(초 당) 커널 엔트로피 사용 가능한 커널 인터럽트(초 당) 커널 프로세스가 금지됨(초 당) 메모리 활성화 메모리 사용 가능한 총 메모리 버퍼 메모리 캐시 메모리 할당된 메모리 메모리 메모리 메모리 메모리 메모리 더티 메모리 사용 가능한 메모리 최고 메모리 전체 메모리 큰 페이지 크기 메모리 큰 페이지 메모리 여유 메모리 큰 페이지 전체 메모리 부족 메모리 매핑된 메모리 페이지 표 메모리 공유 메모리 슬랩 메모리 스왑 캐시된 메모리 스왑 사용 가능한 메모리 스왑 총 메모리 사용된 총 메모리 용량 Vmalloc 청크 메모리 Vmalloc 사용된 총 메모리 Vmalloc 사용된 메모리 배합 메모리 유선 메모리 Writeback TMP 메모리 캐시 오류 메모리 요청 제로 오류 메모리 페이지 오류 메모리 페이지 메모리 페이지 메모리 페이지 메모리 페이지 오류 NONPAGED 메모리 페이지징 메모리 코어 메모리 대기 캐시 일반 메모리 대기 캐시 예비 메모리 전환 장애 프로세스 차단 프로세스 정지 프로세스 유틸 프로세스 페이지징 프로세스 실행 프로세스 중단 프로세스 총 프로세스 총 프로세스 수 스레드 프로세스 수 없는 프로세스 Zombies 프로세서 대기열 길이 스왑 사용 가능한 총 스왑 총 사용된 용량 합계 스왑 아웃 시스템 가동 시간 시스템 Num CPU 시스템 Num Users 시스템 호출에서 사용된 스왑 교체

오브젝트:	식별자:	특성:	데이터 요소:
노드 네트워크	네트워크 인터페이스 노드 UUID	노드 이름 노드 IP 노드 OS입니다	수신된 바이트 전송된 바이트 패킷 Outbound 폐기된 패킷 Outbound 오류 수신된 패킷 수신 오류 패킷 수신 패킷 송신 패킷

## 설정

설치 및 문제 해결 정보는 에서 찾을 수 있습니다 ["Agent 구성"](#) 페이지.

## ActiveMQ 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 ActiveMQ에서 메트릭을 수집합니다.

## 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. ActiveMQ를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 ["에이전트 설치"](#) 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## ActiveMQ Configuration

Gathers ActiveMQ metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-activemq.conf file.

```
[[inputs.activemq]]
  ## Required ActiveMQ Endpoint, port
  ## USER-ACTION: Provide address of ActiveMQ, HTTP port for ActiveMQ
  server = "<INSERT_ACTIVEMQ_ADDRESS>"
  port = <INSERT_ACTIVEMQ_PORT>
```

- 2 Replace <INSERT\_ACTIVEMQ\_ADDRESS> with the applicable ActiveMQ server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT\_ACTIVEMQ\_PORT> with the applicable ActiveMQ server HTTP port.
- 4 Replace <INSERT\_ACTIVEMQ\_USERNAME> and <INSERT\_ACTIVEMQ\_PASSWORD> with the applicable ActiveMQ credentials.
- 5 Modify 'webadmin' if needed (if ActiveMQ server changes web admin root path).
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

설정

정보는 에서 찾을 수 있습니다 "[ActiveMQ 문서](#)"

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
ActiveMQ 대기열	네임스페이스 대기열 포트 서버	노드 이름 노드 IP 노드 UUID	소비자 수 대기열 대기열 수 대기열 크기
ActiveMQ 가입자	클라이언트 ID 연결 ID 포트 서버 네임스페이스	활성 대상 노드 이름 노드 IP 노드 UUID 노드 OS 선택기 가입입니다	발송된 대기열 수 디스패치 대기열 크기 대기열 대기열 수 보류 대기열 크기
ActiveMQ 주제	Topic Port Server 네임스페이스	노드 이름 노드 IP 노드 UUID 노드 OS	소비자 수 대기열 대기열 수 크기

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## Apache Data Collector

이 데이터 수집기는 사용자 환경의 Apache 서버에서 데이터를 수집할 수 있도록 합니다.

### 필수 구성 요소

- Apache HTTP Server를 설정하고 제대로 실행해야 합니다
- 에이전트 호스트/VM에 대한 sudo 또는 관리자 권한이 있어야 합니다
- 일반적으로 Apache\_mod\_status\_module은 Apache 서버의 '/server-status?auto' 위치에 페이지를 노출하도록 구성됩니다. 사용 가능한 필드를 모두 수집하려면 \_ExtendedStatus\_ 옵션을 활성화해야 합니다. 서버를 구성하는 방법에 대한 자세한 내용은 Apache 모듈 설명서를 참조하십시오. [https://httpd.apache.org/docs/2.4/mod/mod\\_status.html#enable](https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable)

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Apache를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_ 를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Apache Configuration

Gathers Apache metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Ensure that the Apache HTTP Server system you're going to gather metrics on has the 'mod\_status' module enabled and exposed. For details refer to the following document.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-apache.conf file.

```
[[inputs.apache]]
  ## An array of URLs to gather from, must be directed at the machine
  ## readable version of the mod_status page including the auto query string.
  ## USER-ACTION: Provide address of apache server, port for apache server, confirm path for
  server-status.
  ## Please specify actual machine IP address and provide full url as localhost address if -
```

- 3 Replace <INSERT\_APACHE\_ADDRESS> with the applicable Apache server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_APACHE\_PORT> with the applicable Apache server port.
- 5 Modify the '/server-status' path in accordance to the Apache server configuration.
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

## 설정

Apache의 HTTP Server용 Telegraf 플러그인은 활성화할 'mod\_status' 모듈에 의존합니다. 이 기능이 활성화되면 Apache의 HTTP Server는 브라우저에서 볼 수 있는 HTML 끝점을 노출하거나 모든 Apache의 HTTP Server 구성 상태를 추출하기 위해 스크래핑할 수 있습니다.

호환성:

Apache의 HTTP Server 버전 2.4.38을 기준으로 구성이 개발되었습니다.

**mod\_status** 활성화:

'od\_status' 모듈을 활성화하고 노출하려면 다음 두 단계를 수행해야 합니다.

- 모듈 활성화 중
- 모듈에서 통계를 노출합니다

활성화 모듈:

모듈 로딩은 '/usr/local/apache/conf/httpd.conf' 아래의 config 파일에 의해 제어됩니다. 구성 파일을 편집하고 다음 행의 주석을 제거합니다.

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

모듈에서 통계 노출:

'od\_status'의 노출은 '/usr/local/apache2/conf/extra/httpd-info.conf' 아래의 구성 파일에 의해 제어됩니다. 해당 구성 파일에 다음 항목이 있는지 확인합니다(최소한 다른 보호 지침이 있음).

```
# Allow server status reports generated by mod_status,
# with the URL of http://servername/server-status
<Location /server-status>
    SetHandler server-status
</Location>

#
# ExtendedStatus controls whether Apache will generate "full" status
# information (ExtendedStatus On) or just basic information
(ExtendedStatus
# Off) when the "server-status" handler is called. The default is Off.
#
ExtendedStatus On
```

'od\_status' 모듈에 대한 자세한 지침은 을 참조하십시오 ["Apache 문서"](#)

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.



오브젝트:	식별자:	특성:	데이터 요소:
아파치	네임스페이스 서버	노드 IP 노드 이름 포트 상위 서버 구성 생성 상위 서버 MPM 생성 서버 가동 시간이 중지 중입니다	초당 요청당 바쁜 작업자 바이트 CPU 하위 시스템 CPU 하위 시스템 CPU 사용자 CPU 로드 CPU 시스템 CPU 사용자 비동기 연결 닫기 비동기 연결 연결 연결 유지 연결 쓰기 연결 요청 유희 작업자당 총 기간 로드 평균(마지막 1m) 로드 평균(마지막 15m) 로드 평균(마지막 5m) 초당 프로세스 요청 수 총 액세스 총 기간 총 KB Scoreytes 보드 폐쇄 점수보드 DNS 조회 점수보드 완료 점수보드 유희 정리 점수판 유지 점수보드 열기 점수보드 읽기 점수보드 대기 시작 Scoreboard 전송

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

## 데이터 수집기 영사

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Consul에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. 영사를 선택합니다.

컬렉션에 대한 Agent를 구성하지 않은 경우 메시지가 표시됩니다 ["에이전트를 설치합니다"](#) 있습니다.

에이전트가 이미 구성되어 있는 경우 해당 운영 체제 또는 플랫폼을 선택하고 \* 계속 \* 을 클릭합니다.

2. SUL Configuration 화면의 지침에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.

### 설정

정보는 에서 찾을 수 있습니다 ["영사 문서"](#).

### 영사의 객체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
영사	네임스페이스 확인 ID 서비스 노드	노드 IP 노드 OS 노드 UUID 노드 이름 서비스 이름 이름 이름 확인 서비스 ID 상태	심각한 통과 경고

문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## Couchbase 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Couchbase에서 메트릭을 수집합니다.

설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Couchbase를 선택하십시오.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Couchbase Configuration

Gathers Couchbase metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-couchbase.conf file.

```
## Read metrics from one or many couchbase clusters
[[inputs.couchbase]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## http://username:password@127.0.0.1:8090
```

- 2 Replace <INSERT\_USERNAME> and <INSERT\_PASSWORD> with couchbase server account credentials.
- 3 Replace <INSERT\_COUCHBASE\_ADDRESS> with the applicable Couchbase address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_COUCHBASE\_PORT> with the applicable Couchbase port.
- 5 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

설정

정보는 에서 찾을 수 있습니다 "[Couchbase 설명서](#)".

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
Couchbase 노드	네임스페이스 클러스터 Couchbase 노드 호스트 이름입니다	노드 이름 노드 IP입니다	메모리 여유 메모리 합계
Couchbase 버킷	네임스페이스 버킷 클러스터	노드 이름 노드 IP입니다	사용된 데이터 사용된 데이터 사용된 디스크 항목 수 사용된 메모리 사용된 초당 작업 할당량

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

## Couchbase Data Collector

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Couchbase DB에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Couchbase를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_ 를 클릭하여 를 확장합니다 ["에이전트 설치"](#) 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## CouchDB Configuration

Gathers CouchDB metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-couchdb.conf file.

```
## Read CouchDB Stats from one or more servers
[[inputs.couchdb]]
  ## Works with CouchDB stats endpoints out of the box
  ## Multiple Hosts from which to read CouchDB stats:
  ## USER-ACTION: Provide comma-separated list of couchdb IP(s) and port(s).
```

- 2 Replace <INSERT\_COUCHDB\_ADDRESS> with the applicable CouchDB address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT\_COUCHDB\_PORT> with the applicable CouchDB port.
- 4 Modify the URL if CouchDB monitoring is exposed at different path
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

설정

정보는 에서 찾을 수 있습니다 "[Couchbase DB 문서](#)".

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
Couchbase	네임스페이스 서버	노드 이름 노드 IP입니다	인증 캐시 적중 인증 캐시 비적중 데이터베이스 읽기 데이터베이스 쓰기 열기 OS 파일 최대 요청 시간 최소 요청 시간 httpd 요청 메서드 복사 httpd 요청 메서드 삭제 httpd 요청 메서드 가져오기 요청 메서드 헤드 httpd 요청 메서드 게시 httpd 요청 메서드 상태 코드 200 상태 코드를 넣습니다 201 상태 코드 202 상태 코드 301 상태 코드 304 상태 코드 400 상태 코드 401 상태 코드 403 상태 코드 404 상태 코드 409 상태 코드 409 상태 코드 412 상태 코드 500

문제 해결

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

## Docker Data Collector 를 참조하십시오

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Docker에서 메트릭을 수집합니다.

설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Docker를 선택합니다.

컬렉션에 대한 Agent를 구성하지 않은 경우 메시지가 표시됩니다 ["에이전트를 설치합니다"](#) 있습니다.

에이전트가 이미 구성되어 있는 경우 해당 운영 체제 또는 플랫폼을 선택하고 \* 계속 \* 을 클릭합니다.

2. Docker Configuration 화면의 지침에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Docker Configuration

Gathers Docker metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-docker.conf` file.

```
[[inputs.docker]]
  ## Docker Endpoint
  ## To use TCP, set endpoint = "tcp://[[ip]:[port]]". By default, Docker uses port 2375 for
  unencrypted and 2376 for encrypted
  ## To use environment variables (ie, docker-machine), set endpoint = "ENV"
```

- 2 Replace `<INSERT_DOCKER_ENDPOINT>` with the applicable Docker endpoint.
- 3 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```

## 설정

Docker용 Telegraf 입력 플러그인은 지정된 UNIX 소켓 또는 TCP 끝점을 통해 메트릭을 수집합니다.

## 호환성

Docker 버전 1.12.6을 기준으로 구성이 개발되었습니다.

## 설정 중입니다

### UNIX 소켓을 통해 Docker 액세스

Telegraf 에이전트가 베어메탈에서 실행 중인 경우 다음을 실행하여 Telegraf Unix 사용자를 Docker Unix 그룹에 추가합니다.

```
sudo usermod -aG docker telegraf
```

Telegraf 에이전트가 Kubernetes Pod 내에서 실행 중인 경우 소켓을 POD에 볼륨으로 매핑한 다음 해당 볼륨을 /var/run/docker.sock에 마운트하여 Docker Unix 소켓을 표시합니다. 예를 들어 PodSpec에 다음을 추가합니다.

```
volumes:  
...  
- name: docker-sock  
hostPath:  
path: /var/run/docker.sock  
type: File
```

그런 다음 컨테이너에 다음을 추가합니다.

```
volumeMounts:  
...  
- name: docker-sock  
mountPath: /var/run/docker.sock
```

Kubernetes 플랫폼에 제공되는 Data Infrastructure Insights 설치 프로그램에서 이 매핑은 자동으로 관리됩니다.

TCP 엔드포인트를 통해 Docker에 액세스합니다

기본적으로 Docker는 암호화되지 않은 액세스에 포트 2375를 사용하고 암호화된 액세스에 포트 2376을 사용합니다.

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
Docker 엔진	네임스페이스 Docker 엔진	노드 이름 노드 IP 노드 UUID 노드 OS Kubernetes 클러스터 Docker 버전 유닛	메모리 컨테이너 일시 중지 컨테이너 실행 컨테이너 중지 CPU 이동 루틴 이미지 수신기 이벤트 사용 파일 설명자 데이터 사용 가능한 데이터 총 데이터 사용된 메타데이터 사용 가능한 메타데이터 총 메타데이터 사용된 풀 블록 크기



오브젝트:	식별자:	특성:	데이터 요소:
Docker 컨테이너	네임스페이스 컨테이너 이름 Docker 엔진	Kubernetes 컨테이너 해시 Kubernetes 컨테이너 포트 Kubernetes 컨테이너 재시작 Kubernetes 컨테이너 종료 메시지 경로 Kubernetes 컨테이너 종료 메시지 정책 Kubernetes Pod 종료 유예 기간 컨테이너 상태 컨테이너 버전 노드 이름 Kubernetes 컨테이너 로그 경로 Kubernetes 컨테이너 이름 Kubernetes 컨테이너 이름 Kubernetes Docker 유형 Kubernetes Pod 이름 Kubernetes Pod 네임스페이스 Kubernetes 네임스페이스 Kubernetes POD UID Kubernetes Sandbox ID 노드 IP 노드 UUID Docker 버전 Kubernetes IO Config Kubernetes Source OpenShift IO SCC Kubernetes 설명 Kubernetes Display Name OpenShift Tags Kompose Service Pod Template Hash Controller Revision Hash Pod Template Generation License Schema Build Date Schema Name Schema URL 스키마 VCS URL 스키마 공급업체 스키마 버전 스키마 버전 유지 관리 업체 고객 Pod Kubernetes StatefulSet Pod 이름 테넌트 WebConsole 아키텍처 권한 소스 URL 빌드 날짜 RH 빌드 호스트 RH 구성 요소 배포 범위 설치 릴리스 요약 제거 VCS 참조 VCS 유형 공급업체 버전 상태 컨테이너 ID	메모리 할성 익명 메모리 할성 파일 메모리 캐시 메모리 계층적 제한 메모리 비할성 익명 메모리 비할성 파일 메모리 제한 메모리 매핑된 파일 메모리 최대 사용 메모리 페이지 결함 메모리 페이지 주 결함 메모리 페이지 메모리 페이징 메모리 상주 세트 크기 메모리 상주 세트 크기 큰 메모리 총 할성 익명 메모리 총 할성 파일 메모리 총 캐시 메모리 총 비할성 익명 메모리 총 비할성 파일 메모리 총 매핑된 파일 메모리 총 페이지 오류 메모리 총 페이지 주요 오류 메모리 총 페이징 메모리 총 페이징 아웃 메모리 총 상주 세트 크기 메모리 총 상주 세트 크기 총 상주 세트 크기 총 메모리 총 메모리 총 크기 큰 메모리 총계 Unevitable 메모리 Useficable 메모리 사용량 메모리 사용량 종료 코드 OOM이 실패한 Streak에서 시작된 PID를 종료했습니다

오브젝트:	식별자:	특성:	데이터 요소:
Docker 컨테이너 블록 IO	네임스페이스 컨테이너 이름 장치 Docker 엔진	Kubernetes 컨테이너 해시 Kubernetes 컨테이너 포트 Kubernetes 컨테이너 재시작 Kubernetes 컨테이너 종료 메시지 경로 Kubernetes 컨테이너 종료 메시지 정책 Kubernetes Pod 종료 유예 기간 컨테이너 상태 컨테이너 버전 노드 이름 Kubernetes 컨테이너 로그 경로 Kubernetes 컨테이너 이름 Kubernetes 컨테이너 이름 Kubernetes Docker 유형 Kubernetes Pod 이름 Kubernetes Pod 네임스페이스 Kubernetes 네임스페이스 Kubernetes POD UID Kubernetes Sandbox ID 노드 IP 노드 UUID Docker 버전 Kubernetes Config Kubernetes 소스 OpenShift SCC Kubernetes 설명 Kubernetes 표시 이름 OpenShift 태그 스키마 버전 Pod 템플릿 해시 컨트롤러 수정 해시 템플릿 생성 Kompose 서비스 스키마 빌드 날짜 스키마 이름 스키마 공급업체 고객 Pod Kubernetes StatefulSet Pod 이름 테넌트 WebConsole 빌드 날짜 라이선스 공급업체 아키텍처 권한 소스 URL RH 빌드 호스트 RH 구성 요소 배포 범위 설치 유지 보수 관리자 릴리스 실행 요약 제거 VCS 참조 VCS 유형 버전 스키마 URL 스키마 VCS URL 스키마 버전 컨테이너 ID	입출력 서비스 바이트 재귀 비동기 입출력 서비스 바이트 재귀 읽기 입출력 서비스 바이트 재귀 동기화 입출력 서비스 바이트 재귀 총 입출력 서비스 바이트 재귀 입출력 서비스 재귀 입출력 서비스 재귀 입출력 서비스 재귀 입출력 재귀적 입출력 서비스 재귀적 입출력 서비스 재귀적 입출력 재귀적 입출력 서비스 입출력 재귀적 입출력 서비스 입출력 재귀적 쓰기
Docker 컨테이너 네트워크 를 참조하십시오	네임스페이스 컨테이너 이름 네트워크 Docker 엔진	컨테이너 이미지 컨테이너 상태 컨테이너 버전 노드 이름 노드 IP 노드 UUID 노드 OS K8s 클러스터 Docker 버전 컨테이너 ID	RX Drop된 RX Bytes RX Errors RX Packets TX Drop TX Bytes TX Errors TX Packet

오브젝트:	식별자:	특성:	데이터 요소:
Docker 컨테이너 CPU	네임스페이스 컨테이너 이름 CPU Docker Engine입니다	Kubernetes 컨테이너 해시 Kubernetes 컨테이너 포트 Kubernetes 컨테이너 재시작 Kubernetes 컨테이너 종료 메시지 경로 Kubernetes 컨테이너 종료 메시지 정책 Kubernetes Pod 종료 유예 기간 Kubernetes 구성 보기 Kubernetes 구성 소스 SCC OpenShift 컨테이너 이미지 컨테이너 상태 컨테이너 버전 노드 이름 Kubernetes 컨테이너 로그 경로 Kubernetes 컨테이너 이름 Kubernetes Docker 유형 Kubernetes Pod 이름 Kubernetes Pod 네임스페이스 Kubernetes Pod UID Kubernetes Sandbox ID 노드 IP 노드 UUID 노드 OS Kubernetes 클러스터 Docker 버전 Kubernetes 설명 Kubernetes 표시 이름 OpenShift 태그 스키마 버전 Pod 템플릿 해시 컨트롤러 수정 해시 템플릿 생성 Kompose 서비스 스키마 빌드 날짜 스키마 라이선스 스키마 이름 스키마 공급업체 고객 포드 Kubernetes StatefulSet Pod 이름 테넌트 WebConsole 빌드 날짜 라이선스 공급업체 아키텍처 권한 있는 소스 URL RH 빌드 호스트 RH 구성 요소 배포 범위 설치 유지 보수 관리자 릴리스 설치 요약 제거 VCS 참조 VCS 유형 버전 스키마 URL 스키마 VCS URL 스키마 버전 컨테이너 ID	제한 기간 제한 제한 제한된 기간 제한 사용자 모드 사용 비율 시스템 사용 총계의 커널 모드 사용에서 제한된 시간 사용 제한

문제 해결

문제:	다음을 시도해 보십시오.
구성 페이지의 지침을 따른 후 Data Infrastructure Insights에 Docker 메트릭이 표시되지 않습니다.	Telegraf 에이전트 로그를 확인하여 다음 오류를 보고하는지 확인합니다. E! 플러그인 오류 [inputs.docker]: Docker 데몬 소켓에 연결하려고 시도하는 동안 권한이 거부되었습니다. 필요한 경우 위에서 지정한 대로 Telegraf 에이전트 액세스를 Docker Unix 소켓에 제공하는 데 필요한 단계를 수행하십시오.

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

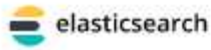
## Elasticsearch Data Collector(Elasticsearch Data Collector)

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Elasticsearch에서 메트릭을 수집합니다.

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Elasticsearch를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 ["에이전트 설치"](#) 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Elasticsearch Configuration

Gathers Elasticsearch metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-elasticsearch.conf file.

```
[[inputs.elasticsearch]]
  ## USER-ACTION: Provide comma-separated list of Elasticsearch servers.
  ## Note that for scenarios in which metrics from multiple Elasticsearch clusters are being
  ## sent to Cloud Insights, the Elasticsearch cluster names must be unique.
  ## Please specify actual machine IP address, and refrain from using a loopback address
```

- 2 Replace <INSERT\_ELASTICSEARCH\_ADDRESS> with the applicable Elasticsearch address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT\_ELASTICSEARCH\_PORT> with the applicable Elasticsearch port.
- 4 Restart the Telegraf service.

```
systemctl restart telegraf
```

설정

정보는 에서 찾을 수 있습니다 "[Elasticsearch 문서](#)".

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
Elasticsearch Cluster(Elasticsearch 클러스터)	네임스페이스 클러스터	노드 IP 노드 이름 클러스터 상태	마스터 노드 수 총 노드 수 사용 가능한 파일 시스템 데이터(바이트) 사용 가능한 파일 시스템 데이터(바이트) 파일 시스템 데이터 총 (바이트) JVM 스레드 OS 할당 프로세서 OS 메모리 사용 가능(바이트) OS 메모리 사용 가능 OS 메모리 총 메모리 사용 가능(바이트) OS 메모리 사용된 프로세스 CPU Indices 완료 크기 (바이트) 인덱스 수 지수 카운트 지수 문서 인덱스 문서 삭제된 색인 필드 데이터 승수 지수 필드 데이터 메모리 크기(바이트) 지수 쿼리 캐시 수 지수 지수 지수 지수 지수 지수 지수 지수 지수 세그먼트 수 지수 지수 메모리(바이트) 지수 1차 평균 지수 1차 지수 1차 지수 최소 지수 1차 지수 최소 지수 샤드 인덱스 복제 평균 색인 샤드 인덱스 복제 최대 색인 복제 최소 색인 복제 최소 색인 샤드 평균 색인 샤드 최대 색인 조각자 최대 색인 조각자 1차 색인 복제 색인 샤드 총 색인 저장소 크기(바이트)

오브젝트:	식별자:	특성:	데이터 요소:
Elasticsearch Node(Elasticsearch 노드)	네임스페이스 클러스터 ES 노드 ID ES 노드 IP ES 노드	영역 ID입니다	머신 러닝 활성화 머신 러닝 메모리 머신 러닝 최대 오픈 작업 X-Pack 설치 차단기 계정 추정 크기(바이트) 차단기 계정 제한 크기 (바이트) 차단기 회계 오버헤드 차단기 계정 가동식 차단기 현장 데이터 예상 크기(바이트) 차단기 필드 데이터 오버헤드 차단기 필드 데이터 비상정지 차단기 필드 데이터 비상정지 차단기 필드 데이터 비상정지 차단기 필드 데이터 비상정지 차단기 필드 데이터 비상정지 차단기 비행 중 자극 크기(바이트) 차단기 비행 중 제한 크기 (바이트) 차단기 비행 중 오버헤드 차단기 기내 비상정지 차단기 상위 추정 크기(바이트) 차단기 상위 제한 크기(바이트) 차단기 상위 오버헤드 차단기 상위 비상정지 차단기 요청 예상 크기(바이트) 차단기 요청 제한 크기(바이트) 차단기 요청 비상 차단기 요청 비상정지 데이터 파일 시스템 요청 (바이트) Filesystem Data Free (바이트) Filesystem Data Total (바이트) Filesystem IO Stats Devices Ops Filesystem IO Stats Read (KB) Filesystem IO Stats Devices Read Ops Filesystem IO Stats Write Ops Filesystem IO Stats Total Read (KB) Filesystem IO Stats Total Read (KB) Filesystem 입출력 통계 읽기 작업 파일 시스템 입출력 통계 총 쓰기(KB) 파일 시스템 입출력 통계 쓰기 작업 파일 시스템 사용 가능한 최소 사용량 예상치(바이트) 파일 시스템 사용 최소 사용량 예상치 합계(바이트) 파일 시스템 사용 가능한 디스크 파일 시스템 최대 사용량 예상치 합계(바이트) 파일

문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## Flink Data Collector

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Flink에서 메트릭을 수집합니다.

설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Flink 를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, [\\_지침 표시\\_](#)를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.





## Flink Configuration

Gathers Flink metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Flink JobManager(s) and Flink Task Manager(s). For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-flink.conf file.

```
## *****  
## JobManager  
## *****  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of flink Job Manager(s), port for jolokia, add one URL  
  ## USER-ACTION: Provide address(es) of flink Task Manager(s), port for jolokia, add one URL
```

- 3 Replace <INSERT\_FLINK\_JOBMANAGER\_ADDRESS> with the applicable Flink Job Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_FLINK\_TASKMANAGER\_ADDRESS> with the applicable Flink Task Manager address(es). Please specify a real machine address, and refrain from using a loopback address.
- 5 Replace <INSERT\_JOLOKIA\_PORT> with the applicable jolokia port.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Modify 'Cluster' if needed for Flink cluster designation.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

설정

전체 Flink 배포에는 다음 구성 요소가 포함됩니다.

JobManager: Flink 운영 시스템입니다. 일련의 TaskManager를 조정합니다. High Availability 설정에서 시스템에 JobManager가 두 개 이상 있습니다. TaskManager: Flink 연산자를 실행하는 위치입니다. Flink 플러그인은 Telegraf의 Jolokia 플러그인을 기반으로 합니다. 모든 Flink 구성 요소에서 정보를 수집하는 요구 사항과 같이 JMX는 모든 구성 요소에서 Jolokia를 통해 구성 및 노출되어야 합니다.

#### 호환성

구성은 Flink 버전 1.7.0을 기준으로 개발되었습니다.

#### 설정 종입니다

#### 졸로키아 에이전트 용기

모든 개별 구성 요소의 경우 Jolokia 에이전트 JAR 파일 버전을 다운로드해야 합니다. 에 대해 테스트한 버전은 [입니다 "졸로키아 에이전트 1.6.0"](#).

아래 지침에서는 다운로드한 jar 파일(jolokia-jvm-1.6.0-agent.jar)이 '/opt/Flink/lib/' 위치에 있다고 가정합니다.

#### 작업 관리자

JobManager를 구성하여 Jolokia API를 표시하려면 노드에서 다음 환경 변수를 설정한 다음 JobManager를 다시 시작하십시오.

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

졸로키아를 위한 다른 포트를 선택할 수 있습니다 (8778). 졸로키아를 잠그기 위한 내부 IP가 있는 경우 "모두 캐치" 0.0.0.0을 자신의 IP로 대체할 수 있습니다. 이 IP는 Telegraf 플러그인에서 액세스할 수 있어야 합니다.

#### 작업 관리자

Jolokia API를 노출하도록 TaskManager를 구성하려면 노드에서 다음 환경 변수를 설정한 다음 TaskManager를 다시 시작해야 합니다.

```
export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

졸로키아를 위한 다른 포트를 선택할 수 있습니다 (8778). 졸로키아를 잠그기 위한 내부 IP가 있는 경우 "모두 캐치" 0.0.0.0을 자신의 IP로 대체할 수 있습니다. 이 IP는 Telegraf 플러그인에서 액세스할 수 있어야 합니다.

#### 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
Flink 작업 관리자	클러스터 네임스페이스 서버	노드 이름 작업 관리자 ID 노드 IP입니다	네트워크 사용 가능 메모리 세그먼트 네트워크 총 메모리 세그먼트 가비지 컬렉션 PS MarkSweep Count 가비지 컬렉션 PS MarkSweep 시간 가비지 컬렉션 PS 스카버기 수 가비지 컬렉션 PS 스카버기 시간 힙 메모리 커밋된 힙 메모리 최대 힙 메모리 사용된 스레드 카운트 스레드 피크 스레드 카운트 스레드 카운트 스레드 카운트 스레드 카운트 총 시작
Flink 작업	클러스터 네임스페이스 서버 작업 ID입니다	노드 이름 작업 이름 노드 IP 마지막 체크포인트 외부 경로 재시작 시간	다운타임 전체 재시작 마지막 체크포인트 정렬 버퍼 마지막 체크포인트 기간 마지막 체크포인트 크기 완료된 체크포인트 수 실패한 체크포인트 수 진행 중인 체크포인트 수 체크포인트 가동 시간 수
Flink 작업 관리자	클러스터 네임스페이스 서버	노드 이름 노드 IP입니다	가비지 수집 PS MarkSweep Count 가비지 수집 PS MarkSweep Time 가비지 수집 PS 청소 횟수 가비지 수집 PS 청소 시간 힙 메모리 커밋된 힙 메모리 힙 메모리 최대 힙 메모리 사용된 메모리 등록된 작업 관리자 수 실행 작업 슬롯 사용 가능한 작업 슬롯 총 스레드 수 데몬 스레드 수 최대 스레드 수 스레드 수 총계 시작됨



오브젝트:	식별자:	특성:	데이터 요소:
Flink 작업 연산자	클러스터 네임스페이스 작업 ID 운영자 ID 작업 ID입니다	서버 노드 이름 작업 이름 연산자 이름 하위 작업 인덱스 작업 시도 ID 작업 시도 번호 작업 이름 작업 관리자 ID 노드 IP	현재 입력 워터마크 현재 출력 워터마크 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 지연 레코드 수 삭제된 할당된 파티션 바이트 소비 속도 커밋 지연 시간 평균 커밋 지연 시간 최대 커밋 속도 Commit 실패 Commit 성공 연결 종료 속도 연결 수 연결 생성 속도 카운트 지연 시간 평균 가져오기 지연 시간 최대 가져오기 속도 가져오기 평균 페치 크기 최대 페치 스로틀 시간 평균 페치 스로틀 시간 최대 하트비트 속도 수신 바이트 속도 IO 비율 평균 IO 시간(ns) IO 대기 비율 IO 대기 시간 평균(ns) 연결 속도 연결 시간 평균 마지막 하트비트 전 네트워크 IO 속도 발신 바이트 속도 레코드 소비 속도 레코드 지연 요청 평균 요청 속도 요청 크기 평균 요청 크기 최대 응답 속도 동기화 속도 동기화 시간 평균 하트비트 응답 최대 조인 시간 최대 동기화 시간 최대

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## Hadoop Data Collector

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Hadoop에서 메트릭을 수집합니다.

### 설치


1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Hadoop 선택

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침

표시\_를 클릭하여 를 확장합니다 "에이전트 설치" 지침.

- 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
- 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



### Hadoop Configuration

Gathers Hadoop metrics.

---

#### What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

---

#### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

## Follow Configuration Steps

Need Help?

- 1 Install Jolokia on your Hadoop NameNode, Secondary NameNode, DataNode(s), ResourceManager, NodeManager(s) and JobHistoryServer. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-hadoop.conf file.

```
#####  
# NAMENODE #  
#####  
[[inputs.jolokia2_agent]]  
  ## USER-ACTION: Provide address(es) of Hadoop NameNode, port for jolokia  
  ## Please specify real machine address and refrain from using a loopback address
```

- 3 Replace <INSERT\_HADOOP\_NAMENODE\_ADDRESS> with the applicable Hadoop NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT\_JOLOKIA\_PORT> with the NameNode's assigned Jolokia port.
- 4 Replace <INSERT\_HADOOP\_SECONDARYNAMENODE\_ADDRESS> with the applicable Hadoop Secondary NameNode address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT\_JOLOKIA\_PORT> with the Secondary NameNode's assigned Jolokia port.
- 5 Replace <INSERT\_HADOOP\_DATANODE\_ADDRESS> with the applicable Hadoop DataNode address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT\_JOLOKIA\_PORT> with the DataNode's assigned Jolokia port.
- 6 Replace <INSERT\_HADOOP\_RESOURCEMANAGER\_ADDRESS> with the applicable Hadoop ResourceManager address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT\_JOLOKIA\_PORT> with the ResourceManager's assigned Jolokia port.
- 7 Replace <INSERT\_HADOOP\_NODEMANAGER\_ADDRESS> with the applicable Hadoop NodeManager address(es). Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT\_JOLOKIA\_PORT> with the NodeManager's assigned Jolokia port.
- 8 Replace <INSERT\_HADOOP\_JOBHISTORYSERVER\_ADDRESS> with the applicable Hadoop Job History Server address. Please specify a real machine address, and refrain from using a loopback address. Replace corresponding <INSERT\_JOLOKIA\_PORT> with the Job History Server's assigned Jolokia port.
- 9 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 10 Modify 'Cluster' if needed for Hadoop cluster designation.
- 11 Restart the Telegraf service.

```
systemctl restart telegraf
```

### 설정

전체 Hadoop 구축에는 다음 구성 요소가 포함됩니다.

- NameNode: HDFS(Hadoop Distributed File System) 운영 시스템입니다. 일련의 DataNode를 조정합니다.



- Secondary NameNode: main NameNode에 대한 워م 페일오버입니다. Hadoop에서는 NameNode에 대한 프로모션이 자동으로 수행되지 않습니다. Secondary NameNode는 NameNode에서 정보를 수집하여 필요할 때 상황 이동할 수 있도록 준비합니다.
- DataNode: 데이터의 실제 소유자입니다.
- ResourceManager: 컴퓨팅 운영 시스템(YARN)입니다. 일련의 NodeManager를 조정합니다.
- NodeManager: 컴퓨팅 리소스로, 응용 프로그램 실행을 위한 실제 위치입니다.
- JobHistoryServer: 모든 작업 내역 관련 요청을 처리합니다.

Hadoop 플러그인은 Telegraf의 Jolokia 플러그인을 기반으로 합니다. 모든 Hadoop 구성 요소에서 정보를 수집하는 요구 사항과 같이 JMX는 모든 구성 요소에서 Jolokia를 통해 구성 및 노출되어야 합니다.

호환성

Hadoop 버전 2.9.2를 기준으로 구성이 개발되었습니다.

설정 중입니다

졸로키아 에이전트 용기

모든 개별 구성 요소의 경우 Jolokia 에이전트 JAR 파일 버전을 다운로드해야 합니다. 에 대해 테스트한 버전은 ["졸로키아 에이전트 1.6.0"](#).

아래 지침에서는 다운로드한 jar 파일(jolokia-jvm-1.6.0-agent.jar)이 '/opt/hADOOP/lib/' 위치에 있다고 가정합니다.

**NameNode**입니다

Jolokia API를 노출하도록 NameNode를 구성하려면 <Hadoop\_HOME>/etc/Hadoop/Hadoop-env.sh에서 다음을 설정할 수 있습니다.

```
export HADOOP_NAMENODE_OPTS="$HADOOP_NAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7800,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8000
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
You can choose a different port for JMX (8000 above) and Jolokia (7800).
If you have an internal IP to lock Jolokia onto you can replace the "catch
all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from
the telegraf plugin. You can use the option '-
Dcom.sun.management.jmxremote.authenticate=false' if you don't want to
authenticate. Use at your own risk.
```

**Secondary NameNode**입니다

보조 NameNode를 구성하여 Jolokia API를 표시하려면 <Hadoop\_HOME>/etc/Hadoop/Hadoop-env.sh에서 다음을 설정할 수 있습니다.



```
export HADOOP_SECONDARYNAMENODE_OPTS="$HADOOP_SECONDARYNAMENODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7802,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8002
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8002 above) and Jolokia (7802). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

### DataNode 를 선택합니다

Jolokia API를 노출하도록 DataNodes를 구성하려면 <Hadoop\_HOME>/etc/Hadoop/Hadoop-env.sh에서 다음을 설정할 수 있습니다.

```
export HADOOP_DATANODE_OPTS="$HADOOP_DATANODE_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7801,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8001
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8001 above) and Jolokia (7801). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

### ResourceManager 를 클릭합니다

ResourceManager를 구성하여 Jolokia API를 노출하려면 <Hadoop\_HOME>/etc/Hadoop/Hadoop-env.sh에서 다음을 설정할 수 있습니다.

```
export YARN_RESOURCEMANAGER_OPTS="$YARN_RESOURCEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7803,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8003
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8003 above) and Jolokia (7803). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

### **NodeManager**를 참조하십시오

NodeManagers가 Jolokia API를 노출하도록 구성하려면 <Hadoop\_HOME>/etc/Hadoop/Hadoop-env.sh에서 다음을 설정할 수 있습니다.

```
export YARN_NODEMANAGER_OPTS="$YARN_NODEMANAGER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7804,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8004
-Dcom.sun.management.jmxremote.ssl=false
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8004 above) and Jolokia (7804). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

### **JobHistoryServer**를 참조하십시오

JobHistoryServer가 Jolokia API를 표시하도록 구성하려면 <Hadoop\_Home>/etc/Hadoop/Hadoop-env.sh에서 다음을 설정할 수 있습니다.

```
export HADOOP_JOB_HISTORYSERVER_OPTS="$HADOOP_JOB_HISTORYSERVER_OPTS
-javaagent:/opt/hadoop/lib/jolokia-jvm-1.6.0
-agent.jar=port=7805,host=0.0.0.0 -Dcom.sun.management.jmxremote
-Dcom.sun.management.jmxremote.port=8005
-Dcom.sun.management.jmxremote.password.file=$HADOOP_HOME/conf/jmxremote.p
assword"
```

You can choose a different port for JMX (8005 above) and Jolokia (7805). If you have an internal IP to lock Jolokia onto you can replace the "catch all" 0.0.0.0 by your own IP. Notice this IP needs to be accessible from the telegraf plugin. You can use the option '-Dcom.sun.management.jmxremote.authenticate=false' if you don't want to authenticate. Use at your own risk.

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
Hadoop 보조 NameNode	클러스터 네임스페이스 서버	노드 이름 노드 IP 컴파일 정보 버전	GC 카운트 GC 사본 수 GC 마크 스왑 컴팩트 카운트 GC 번호 정보 임계값이 GC 번호 경고 임계값을 초과함 GC 시간 GC 복사 시간 GC 마크 스왑 컴팩트 시간 GC 총 추가 절전 시간 로그 오류 카운트 로그 치명적 카운트 로그 경고 카운트 메모리 힙 커밋됨 메모리 힙 최대 메모리 힙 사용된 메모리 최대 메모리 비 힙 커밋된 메모리 비 힙 사용된 스레드 차단된 스레드 새 스레드 Runnable 스레드 종료 스레드 시간 지정 대기 스레드 대기

오브젝트:	식별자:	특성:	데이터 요소:
Hadoop NodeManager를 참조하십시오	클러스터 네임스페이스 서버	노드 이름 노드 IP입니다	<p>컨테이너 할당된 메모리  할당 메모리 할당  Opportunistic 가상 코어  할당된 Opportunistic 가상  코어 할당 메모리 사용  가능한 가상 코어 사용  가능한 디렉토리 잘못된  로컬 디렉토리 불량 로그  캐시 크기 클린 컨테이너  시작 기간 평균 시간  컨테이너 시작 기간 작업  컨테이너의 실행 완료  컨테이너 실패 컨테이너  제거 컨테이너 실행  컨테이너 실행 컨테이너  실행 컨테이너 실행 실패  컨테이너 실행 컨테이너  실행 컨테이너 실행  컨테이너 실행 컨테이너  실행 안 됨 컨테이너 실행  컨테이너 실행 시작  컨테이너 실행 컨테이너  실행 컨테이너 오류  컨테이너에서 롤백 디스크  사용률 좋은 로컬 디렉토리  디스크 사용률 좋은 로그  디렉토리 바이트 삭제 전용  바이트 삭제 기회주의적인  바이트를 실행하는 공용  컨테이너 삭제 총 셔플 연결  임의 재생 출력 바이트 셔플  출력 실패 정상 GC 카운트  GC 마크 스윙 Compact  Count GC Number Info  Threshold Exceeded GC  Number Warning  Threshold Exceeded GC  Time GC Copy Time GC  Marks Sweep Time GC  Total Extra Sleep Time  Logs Error Count Logs  Fatal Count Logs Warn  Count Memory Heap  Committed Memory Heap  Hap Used Memory Max  메모리 비 힙 커밋된 메모리  비 힙 최대 메모리 비힙  사용된 스레드 차단된  스레드 새 스레드 Runnable  스레드 종료 스레드 시간  지정 대기 스레드 대기 중</p>

오브젝트:	식별자:	특성:	데이터 요소:
<p>Hadoop ResourceManager를 참조하십시오</p>	<p>클러스터 네임스페이스 서버</p>	<p>노드 이름 노드 IP입니다</p>	<p>ApplicationMaster 시작 지연 평균  ApplicationMaster 시작 지연 번호  ApplicationMaster 등록 지연 평균  ApplicationMaster 등록 지연 번호  NodeManager 활성 번호  NodeManager 축소 번호  NodeManager 손실 번호  NodeManager 재부팅 번호  NodeManager 종료 번호  NodeManager 정상 번호  NodeManager 메모리 제한  NodeManager 가상 코어 제한 사용된 용량  활성 애플리케이션  활성 사용자 집계 컨테이너  사전 할당된 집계 컨테이너  지정된 집계 컨테이너  릴리스된 집계 메모리 초  사전 제거된 집계 노드 로컬 컨테이너 할당된  애그리게이트 오프 스위치 컨테이너 할당된  애그리게이트 Ack 로컬 컨테이너 할당된  애그리게이트 가상 코어 초  사전 지정된 컨테이너  할당된 메모리 할당된 가상 코어 애플리케이션 시도 첫 번째 컨테이너 할당 지연  평균 시간 애플리케이션 시도 첫 번째 컨테이너 할당 지연  지연 수 응용 프로그램 완료  응용 프로그램 종료 응용 프로그램 실행 중 보류 중인  응용 프로그램 제출 메모리 사용 가능 가상 코어 사용  가능 컨테이너 보류 중  메모리 보류 가상 코어  예약된 메모리 예약된 가상 코어 예약된 메모리  ApplicationMaster 사용  가상 코어  ApplicationMaster 사용  용량 GC 카운트 GC 매수  카운트 GC 마크 스위프  Compact Count GC  Number Info 임계값이 GC  Number Warning 임계값을  초과함 GC Time GC Copy  Time GC Marks Sweep</p>

오브젝트:	식별자:	특성:	데이터 요소:
Hadoop DataNode를 참조하십시오	클러스터 네임스페이스 서버	노드 이름 노드 IP 클러스터 ID 버전	Transceiver Count 전송 진행 중 캐시 용량 캐시 사용 용량 DFS 사용 예상 용량 손실 마지막 볼륨 실패 비율 블록 수 캐시 블록 수 캐시 블록 수 캐시 블록 수 실패 볼륨 수 캐시 해제 실패 용량 남은 GC 수 GC 카운트 GC 스위프 컴팩트 카운트 GC 번호 정보 임계값이 GC 숫자 경고 임계값을 초과함 GC 시간 GC 복사 시간 GC 마크 스위프 컴팩트 시간 GC 총 추가 절전 시간 로그 오류 카운트 로그 치명적 카운트 로그 로그 경고 횟수 메모리 힙 커밋된 메모리 힙 최대 메모리 힙 사용된 메모리 최대 메모리 비힙 커밋됨 메모리 비힙 최대 메모리 비힙 사용된 스레드 차단된 스레드 새 스레드 Runnable 스레드 종료 스레드 시간 지정 대기 스레드 대기 중

오브젝트:	식별자:	특성:	데이터 요소:
Hadoop NameNode입니다	클러스터 네임스페이스 서버	<p>노드 이름 노드 IP 트랜잭션 ID 마지막 로드 이후 마지막으로 쓴 시간 HA 상태 파일 시스템 상태 블록 풀 ID 클러스터 ID 컴파일 정보 고유 버전 수 버전</p>	<p>블록 용량 블록 총 용량 사용된 총 용량 사용된 용량 비 DFS 블록 손상 예상 용량 손실 총 블록 수 초과 하트비트 만료 파일 총 파일 시스템 잠금 대기열 길이 블록 누락된 블록 블록 블록 블록 1개 클라이언트 활성 데이터 노드 비활성 데이터 노드 사용 중단 비활성 데이터 노드 사용 중단 라이브 데이터 노드 해독 암호화 존 수 데이터 노드 유지 보수 데이터 노드 아래 유지 보수 파일 입력 중단 유지 보수 데이터 노드의 라이브 노드 오래된 복제 보류 시간 초과 데이터 노드 메시지 보류 블록 삭제 보류 블록 복제 블록 복제 보류 지연 블록 복제 지연 블록 예약된 복제 스냅샷 스냅샷 스냅샷 스냅샷 스냅샷 스냅샷 디렉토리 데이터 노드 오래된 파일 총 로드 마지막 체크포인트 이후 총 동기화 수 총 트랜잭션 마지막 로그 롤 블록 이후 총 동기화 볼륨 장애 총 동기화 시간 총 객체 최대 작업 블록 추가 작업 허용 스냅샷 작업 차단 일괄 처리된 작업 차단 대기 중인 작업 블록 수신 및 삭제된 작업 보고서 평균 시간 작업 블록 보고서 번호 캐시 보고서 평균 시간 캐시 보고서 번호 작업 생성 파일 작업 생성 스냅샷 작업 생성 파일 작업 삭제 스냅샷 작업 삭제 스냅샷 작업 허용 스냅샷 작업 파일 삭제/출력 추가된 파일 생성된 파일 나열 파일 이름 변경된 파일 나열 시스템 로드 시간 작업 생성 EDEK 평균 시간 작업 생성 EDEK 작업 생성 추가 데이터 노드 블록 가져오기 위치 가져오기 평균 시간 가져오기 편집 번호 가져오기 이미지 가져오기 평균 시간 가져오기 이미지 번호 가져오기 작업 가져오기 링크 대상 작업</p>

오브젝트:	식별자:	특성:	데이터 요소:
Hadoop JobHistoryServer를 참조하십시오	클러스터 네임스페이스 서버	노드 이름 노드 IP입니다	GC 카운트 GC 사본 수 GC 마크 스왑 컴팩트 카운트 GC 번호 정보 임계값이 GC 번호 경고 임계값을 초과함 GC 시간 GC 복사 시간 GC 마크 스왑 컴팩트 시간 GC 총 추가 절전 시간 로그 오류 카운트 로그 치명적 카운트 로그 경고 카운트 메모리 힙 커밋된 메모리 힙 최대 메모리 힙 사용된 메모리 최대 메모리 비 힙 커밋된 메모리 비 힙 사용된 스레드 차단된 스레드 새 스레드 Runnable 스레드 종료 스레드 시간 지정 대기 스레드 대기

문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## HAProxy 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 HAProxy에서 메트릭을 수집합니다.

설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. HAProxy를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_ 를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.





## HAProxy Configuration

Gathers HAProxy metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Ensure that the HAProxy system you're going to gather metrics on has 'stats enable' option. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-haproxy.conf file.

```
# Read metrics of HAProxy, via socket or HTTP stats page
[[inputs.haproxy]]
  ## An array of address to gather stats about. Specify an ip on hostname
  ## with optional port. ie localhost, 10.10.3.33:1936, etc.
  ## Make sure you specify the complete path to the stats endpoint
  ## Exclude the address: 10.10.3.33:1936/10.10.3.33:1936/1936/1936/1936
```

- 3 Replace <INSERT\_HAPROXY\_ADDRESS> with the applicable HAProxy server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_HAPROXY\_PORT> with the applicable HAProxy server port.
- 5 Modify the 'haproxy?stats' path in accordance to the HAProxy server configuration.
- 6 Modify 'username' and 'password' in accordance to the HAProxy server configuration (if credentials are required).
- 7 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 8 Restart the Telegraf service.

```
systemctl restart telegraf
```

## 설정

Telegraf의 HAProxy 플러그인은 HAProxy 통계 지원에 의존합니다. 이 구성은 HAProxy에 내장되어 있지만 기본 제공되지는 않습니다. HAProxy를 활성화하면 브라우저에서 볼 수 있는 HTML 끝점이 노출되거나 모든 HAProxy

구성의 상태를 추출하기 위해 스크랩됩니다.

호환성:

HAProxy 버전 1.1.9.4에 따라 구성이 개발되었습니다.

설정:

통계를 활성화하려면 자체 사용자/암호 및/또는 haproxy URL을 사용하여 haproxy 구성 파일을 편집하고 'defaults' 섹션 뒤에 다음 줄을 추가하십시오.

```
stats enable
stats auth myuser:mypassword
stats uri /haproxy?stats
```

다음은 통계 기능이 설정된 간단한 구성 파일 예입니다.

```
global
  daemon
  maxconn 256

defaults
  mode http
  stats enable
  stats uri /haproxy?stats
  stats auth myuser:mypassword
  timeout connect 5000ms
  timeout client 50000ms
  timeout server 50000ms

frontend http-in
  bind *:80
  default_backend servers

frontend http-in9080
  bind *:9080
  default_backend servers_2

backend servers
  server server1 10.128.0.55:8080 check ssl verify none
  server server2 10.128.0.56:8080 check ssl verify none

backend servers_2
  server server3 10.128.0.57:8080 check ssl verify none
  server server4 10.128.0.58:8080 check ssl verify none
```

자세한 최신 지침은 을 참조하십시오 "[HAProxy 설명서](#)".

### 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
HAProxy 프론트엔드	네임스페이스 주소 프록시	노드 IP 노드 이름 프록시 ID 모드 프로세스 ID 세션 속도 제한 서버 ID 세션 제한 상태	바이트 아웃 캐시 적중 캐시 조회 압축 바이트 압축 바이트는 무시됨 압축 바이트 아웃 압축 응답 연결 속도 최대 연결 속도 연결 규칙 요청에 의해 거부된 연결 규칙 요청 보안 문제 응답으로 거부됨 세션 규칙 요청에 의해 거부 오류 응답 1xx 응답 2xx 응답 3xx 응답 4xx 응답 5xx 응답 기타 요청 인터셉트 세션 비율 세션 비율 최대 요청 비율 최대 요청 비율 최대 세션 총 세션 수 최대 세션 총 요청 다시 쓰기
HAProxy 서버	네임스페이스 주소 프록시 서버	노드 IP 노드 이름 검사 종료 시간 검사 가을 구성 검사 상태 값 검사 상승 구성 확인 프록시 ID 마지막 변경 시간 마지막 세션 시간 모드 프로세스 ID 서버 ID 상태 가중치	활성 서버 백업 서버 바이트 초과 확인 실패 클라이언트 중단 연결 평균 시간 중단 총 거부 응답 수 연결 오류 응답 응답 1xx 응답 2xx 응답 3xx 응답 4xx 응답 기타 서버 선택 총 대기열 현재 대기열 최대 대기열 평균 시간 세션 수 초당 두 번째 세션 최대 연결 재사용 응답 시간 평균 세션 최대 서버 전송 중단 세션 총 세션 총 세션 총 시간 평균 요청 재디스패치 요청 재시도 요청 다시 쓰기 요청 재시도

오브젝트:	식별자:	특성:	데이터 요소:
HAProxy 백엔드	네임스페이스 주소 프록시	노드 IP 노드 이름 프록시 ID 마지막 변경 시간 마지막 세션 시간 모드 프로세스 ID 서버 ID 세션 제한 상태 가중치	활성 서버 백업 서버 바이트 아웃 캐시 적중 횟수 캐시 조회 확인 다운로드 클라이언트는 압축 바이트 우회 압축 바이트 압축 바이트 아웃 압축 응답 바이트 아웃 압축 응답 연결 평균 시간 가동 중지 시간 총 요청 보안 문제 응답으로 거부 보안 문제 연결 오류 응답 응답 1xx 응답 2xx 응답 3xx 응답 4xx 응답 5xx 응답 기타 서버 선택한 총 대기열 현재 대기열 최대 대기열 초당 평균 시간 세션 최대 요청 총 연결 재사용 응답 시간 평균 세션 최대 서버 전송 세션 총 세션 중단 총 세션 총 시간 평균 요청 재디스패치 요청 재시도 요청 재시도 요청 다시 쓰기

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## JVM 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 JVM에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. JVM을 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Java Configuration

Gathers JVM metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your JVMs. For details refer to the following document.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-jvm.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  # USER-ACTION: Provide address(es) of JVM, port for jolokia, add one URL for each JVM in
  # your cluster
  # Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  # 10.1.1.1 or 127.0.0.1)
```

- 3 Replace <INSERT\_JVM\_ADDRESS> with the applicable JVM address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_JOLOKIA\_PORT> with the applicable JVM jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

설정

정보는 에서 찾을 수 있습니다 "[JVM 설명서](#)".

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
JVM	네임스페이스 JVM	OS 아키텍처 OS 이름 OS 버전 런타임 사양 런타임 사양 공급업체 런타임 사양 버전 가동 시간 런타임 VM 이름 런타임 VM 공급업체 런타임 VM 버전 노드 이름 노드 IP	클래스 로드 클래스 로드 총 클래스 언로드 메모리 힙 커밋 메모리 힙 초기화 메모리 힙 사용 최대 메모리 힙 사용 메모리 비 힙 커밋된 메모리 비 힙 초기화 메모리 비 힙 사용된 메모리 객체 비힙 사용 메모리 객체 보류 완료 OS 프로세서 사용 가능 OS 커밋된 가상 메모리 크기 OS 사용 가능 물리적 메모리 크기 OS 가용 스왑 공간 크기 OS 최대 파일 설명자 수 OS 열린 파일 설명자 수 OS 프로세서 CPU 로드 OS 프로세서 CPU 시간 OS 시스템 CPU 로드 OS 평균 로드 OS 총 물리적 메모리 크기 OS 총 스왑 공간 크기 스레드 데몬 수 스레드 피크 카운트 스레드 카운트 스레드 총 시작 카운트 가비지 수집기 복제 컬렉션 카운트 가비지 수집기 복제 컬렉션 시간 가비지 수집기 표시-스왑 컬렉션 카운트 가비지 수집기 G1 이전 세대 컬렉션 개수 가비지 수집기 G1 이전 세대 컬렉션 개수 가비지 수집기 G1 이전 세대 컬렉션 시간 가비지 수집기 G1 이전 세대 컬렉션 개수 가비지 수집기 G1 이전 세대 컬렉션 개수 가비지 수집기 G1 이전 세대 컬렉션 시간 가비지 수집기 G1 이전 세대 컬렉션 개수 가비지 수집기 G1 이전 세대 컬렉션 시간 가비지 수집기 동시 마크-스왑 컬렉션 개수 가비지 수집기 동시 마크-스왑 컬렉션 시간 가비지 수집기 병렬 컬렉션 수 가비지 수집기 병렬 컬렉션 시간 가비지 수집기 병렬 청소 컬렉션 수 가비지 수집기 병렬 청소 컬렉션 수 가비지 수집기 병렬 청소 컬렉션 수 가비지 수집기 병렬 청소 컬렉션 시간 가비지 수집기 병렬 배유 컬렉션 수 가비지 수집기 병렬 배유 수집 시간

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## Kafka 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Kafka에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Kafka를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Kafka Configuration

Gathers Kafka metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Install Jolokia on your Kafka brokers. For details refer to the following [document](#).
- 2 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-kafka.conf file.

```
# Read JMX metrics through Jolokia
[[inputs.jolokia2_agent]]
  ## USER-ACTION: Provide address(es) of kafka broker(s), port for jolokia, add one URL for
  ## each broker in your cluster
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  192.168.1.100:8761)
```

- 3 Replace <INSERT\_KAFKA\_BROKER\_ADDRESS> with the applicable Kafka broker address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_JOLOKIA\_PORT> with the applicable Kafka broker jolokia port.
- 5 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 6 Modify 'Cluster' if needed for Kafka cluster designation.
- 7 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

## 설정

Kafka 플러그인은 Telegraf의 Jolokia 플러그인을 기반으로 합니다. 모든 Kafka 브로커로부터 정보를 수집해야 하는 요구 사항과 같이 JMX는 졸로키아를 통해 모든 구성 요소에 대해 구성 및 노출되어야 합니다.



호환성

Kafka 버전 0.11.0.2에 따라 구성이 개발되었습니다.

설정 중입니다

아래의 모든 지침은 Kafka 설치 위치가 '/opt/Kafka'라고 가정합니다. 설치 위치를 반영하도록 아래 지침을 조정할 수 있습니다.

졸로키아 에이전트 용기

졸로키아 에이전트 JAR 파일의 버전이 필요합니다 "다운로드되었습니다". 시험 대상 버전은 졸로키아 에이전트 1.6.0이었습니다.

아래 지침에서는 다운로드한 jar 파일(jolokia-jvm-1.6.0-agent.jar)이 '/opt/Kafka/libs/' 위치에 있다고 가정합니다.

### Kafka Brokers의

Kafka Brokers가 Jolokia API를 사용하도록 구성하려면 'Kafka-run-class.sh' 호출 바로 앞의 <Kafka\_home>/bin/Kafka-server-start.sh에서 다음을 추가할 수 있습니다.

```
export JMX_PORT=9999
export RMI_HOSTNAME=`hostname -i`
export KAFKA_JMX_OPTS="-javaagent:/opt/kafka/libs/jolokia-jvm-1.6.0-
agent.jar=port=8778,host=0.0.0.0
-Dcom.sun.management.jmxremote.password.file=/opt/kafka/config/jmxremote.p
assword -Dcom.sun.management.jmxremote.ssl=false
-Djava.rmi.server.hostname=$RMI_HOSTNAME
-Dcom.sun.management.jmxremote.rmi.port=$JMX_PORT"
```

위의 예는 'hostname -i'를 사용하여 'RMI\_HOSTNAME' 환경 변수를 설정하는 것입니다. 여러 IP 시스템에서 RMI 연결에 관심 있는 IP를 수집하기 위해 이 설정을 변경해야 합니다.

JMX(위 9999) 및 Jolokia(8778)에 대해 다른 포트를 선택할 수 있습니다. 졸로키아를 잠그기 위한 내부 IP가 있는 경우 "모두 캐치" 0.0.0.0을 자신의 IP로 대체할 수 있습니다. 이 IP는 Telegraf 플러그인에서 액세스할 수 있어야 합니다. 인증을 원하지 않는 경우 '-Dcom.sun.management.jmxremote.authenticate=false' 옵션을 사용할 수 있습니다. 사용에 따르는 위험은 사용자가 부담합니다.

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.



오브젝트:	식별자:	특성:	데이터 요소:
Kafka 브로커	클러스터 네임스페이스 브로커	노드 이름 노드 IP입니다	복제본 관리자 Fetcher 최대 Lag ZooKeeper 클라이언트 연결 ZooKeeper 클라이언트 연결(15m 속도) ZooKeeper 클라이언트 연결(5m 속도) ZooKeeper 클라이언트 연결(평균 속도) ZooKeeper 클라이언트 연결(1m 속도) 복제본 관리자 파티션 수 스레드 수 데몬 스레드 수 피크 스레드 수 현재 스레드 카운트 시작된 총 오프라인 파티션 요청 생성 총 시간(50 백분위수) 요청 생성 총 시간(75번째 백분위수) 요청 생성 총 시간(95번째 백분위수) 요청 생성 총 시간(98번째 백분위수) 요청 생성 총 시간(999번째 백분위수) 생성 요청 총 시간(99번째 백분위수) 생성 요청 총 시간 최대 생성 요청 총 시간 평균 생성 요청 총 시간 최소 생성 요청 총 시간 Stddev 복제본 관리자 ISR 축소 복제본 관리자 ISR 축소(15m 비율) 복제본 관리자 ISR 축소(5m 속도) 복제본 관리자 ISR 축소(평균 속도) 복제본 관리자 ISR 축소(1m 속도) 요청 처리기 평균 유휴 요청 처리기 평균 유휴 상태(15m 속도) 요청 처리기 평균 유휴 상태(5m 속도) 요청 처리기 평균 유휴 상태(평균 속도) 요청 처리기 평균 유휴 상태(1m 속도) 가비지 수집 G1 이전 세대 카운트 가비지 수집 G1 이전 세대 시간 가비지 수집 G1 이전 세대 카운트 가비지 수집 G1 젊은 세대 시간 ZooKeeper 읽기 전용 연결 ZooKeeper 읽기 전용 연결(15m 속도) ZooKeeper 읽기 전용 연결(5m 속도) ZooKeeper 읽기 전용 연결(평균 속도) ZooKeeper 읽기 전용 연결(1m 비율) 네트워크 프로세서 평균 유휴 요청 Follower 총 시간(50% 백분위수) 요청 Fetch

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## Kibana 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Kibana에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Kibana를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_ 를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Kibana Configuration

Gathers Kibana metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Ubuntu & Debian

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-kibana.conf` file.

```
[[inputs.kibana]]
  ## specify a list of one or more Kibana servers
  ## USER-ACTION: Provide address of kibana server(s), port(s) for kibana server
  ## Please specify actual machine IP address, and refrain from using a loopback address (i.e.
  localhost or 127.0.0.1).
```

- 2 Replace `<INSERT_KIBANA_ADDRESS>` with the applicable Kibana server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace `<INSERT_KIBANA_PORT>` with the applicable Kibana server port.
- 4 Replace `'username'` and `'pa$$word'` with the applicable Kibana server authentication credentials as needed, and uncomment the lines.
- 5 Modify `'Namespace'` if needed for server disambiguation (to avoid name clashes).
- 6 Restart the Telegraf service.

```
systemctl restart telegraf
```

## 설정

정보는 에서 찾을 수 있습니다 "Kibana 설명서".

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
키바나	네임스페이스 주소	노드 IP 노드 이름 버전 상태	동시 접속 힙 최대 힙 사용된 초당 요청 응답 시간 평균 응답 시간 최대 가동 시간

문제 해결

추가 정보는 에서 찾을 수 있습니다 "지원" 페이지.


## Kubernetes Monitoring Operator 설치 및 구성

Data Infrastructure Insights는 Kubernetes 컬렉션을 위한 \* Kubernetes Monitoring Operator \* 를 제공합니다. Kubernetes > Collectors > + Kubernetes Collector \* 로 이동하여 새 연산자를 구축합니다.

Kubernetes Monitoring Operator를 설치하기 전에

를 참조하십시오 "필수 구성 요소" Kubernetes Monitoring Operator를 설치 또는 업그레이드하기 위한 문서화.

Kubernetes 모니터링 운영자 설치



**kubernetes**  
Kubernetes

### Deploy NetApp Monitoring Operator

Quickly install and configure a Kubernetes Operator to send cluster information to Cloud Insights.

**Select existing API Access Token or create a new one**

KEY2024 (...vw6NdM) ▼

+ API Access Token

Production Best Practices ?

**Installation Instructions** Need Help?

Please review the [pre-requisites](#) for installing the NetApp Kubernetes Monitoring Operator. To update an existing operator installation please follow [these steps](#).

- 1

**Define Kubernetes cluster name and namespace**

Provide the Kubernetes cluster name and specify a namespace for deploying the monitoring components.

Cluster	Namespace
clustername	netapp-monitoring
- 2

**Download the operator YAML files**

Execute the following download command in a *bash* prompt.

Copy Download Command Snippet

⊞ Reveal Download Command Snippet

*This snippet includes a unique access key that is valid for 24 hours.*

### 3 Optional: Upload the operator images to your private repository

By default, the operator pulls container images from the Cloud Insights repository. To use a private repository, download the required images using the Image Pull command. Then upload them to your private repository maintaining the same tags and directory structure. Finally, update the image paths in operator-deployment.yaml and the docker repository settings in operator-config.yaml. For more information review [the documentation](#).

Copy Image Pull Snippet

Reveal Image Pull Snippet

Copy Repository Password

Reveal Repository Password

*This password is valid for 24 hours.*

### 4 Optional: Review available configuration options

Configure custom options such as proxy and private repository settings. Review the [instructions and available options](#).

### 5 Deploy the operator (create new or upgrade existing)

Execute the `kubectl` snippet to apply the following operator YAML files.

- operator-setup.yaml - Create the operator's dependencies.
- operator-secrets.yaml - Create secrets holding your API key.
- operator-deployment.yaml, operator-cr.yaml - Deploy the NetApp Kubernetes Monitoring Operator.
- operator-config.yaml - Apply the configuration settings if not already present.

Copy kubectl Apply Snippet

Reveal kubectl Apply Snippet

After deploying the operator, **delete or securely store operator-secrets.yaml**.

### 6 Next

Kubernetes에 **Kubernetes Monitoring Operator** 에이전트를 설치하는 단계:

1. 고유한 클러스터 이름 및 네임스페이스를 입력합니다. 있는 경우 **업그레이드 중** 이전 Kubernetes Operator에서 동일한 클러스터 이름과 네임스페이스를 사용합니다.
2. 이러한 내용을 입력하면 다운로드 명령 스크립트를 클립보드에 복사할 수 있습니다.
3. 스크립트를 `_bash_window`에 붙여 넣고 실행합니다. 오퍼레이터 설치 파일이 다운로드됩니다. 스크립트에는 고유한 키가 있으며 24시간 동안 유효합니다.
4. 사용자 지정 또는 개인 리포지토리가 있는 경우 선택적 이미지 풀 스크립트를 복사하여 `_bash_shell`에 붙여 넣고 실행합니다. 이미지를 가져온 후 개인 저장소에 복사합니다. 동일한 태그 및 폴더 구조를 유지해야 합니다. `operator-deployment.YAML_`의 경로와 `_operator-config.YAML_`의 Docker 리포지토리 설정을 업데이트합니다.
5. 필요한 경우 프록시 또는 개인 리포지토리 설정과 같은 사용 가능한 구성 옵션을 검토합니다. 에 대해 자세히 알아보실 수 있습니다 "**구성 옵션**".
6. 준비가 되면 `kubeck Apply` 스크립트를 복사하고 다운로드한 다음 실행하여 Operator 를 배포합니다.
7. 설치가 자동으로 진행됩니다. 완료되면 `Next` 단추를 클릭합니다.
8. 설치가 완료되면 `Next` 단추를 클릭합니다. 또한 `_operator-비밀.YAML_` 파일을 삭제하거나 안전하게 보관하십시오.

프록시를 사용하는 경우 정보를 읽습니다 [프록시를 구성하는 중입니다](#).

사용자 지정 리포지토리가 있는 경우 정보를 읽습니다 [사용자 지정/프라이빗 Docker 저장소 사용](#).

## Kubernetes 모니터링 구성 요소

Data Infrastructure Insights Kubernetes Monitoring은 네 가지 모니터링 구성 요소로 이루어져 있습니다.

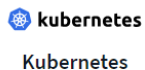
- 클러스터 메트릭입니다
- 네트워크 성능 및 맵(옵션)
- 이벤트 로그(선택 사항)
- 변경 분석(옵션)

위의 옵션 구성 요소는 각 Kubernetes Collector에 대해 기본적으로 활성화되어 있습니다. 특정 수집기에 구성 요소가 필요하지 않다고 결정한 경우 \* Kubernetes > Collectors \* 로 이동한 후 화면 오른쪽의 수집기의 "세 가지 점" 메뉴에서 \_Modify Deployment\_를 선택하여 비활성화할 수 있습니다.

NetApp / Observability / Collectors

Cluster Name ↑	Status	Operator Version	Network Performance and Map	Change Analysis	
au-pod	⚠ Outdated	1.1540.0	1.347.0	1.162.0	⋮
jks-troublemaker	Latest	1.1579.0	N/A	1.201.0	⋮
oom-test	⚠ Outdated	1.1555.0	N/A	1.191.0	⋮

화면에는 각 구성 요소의 현재 상태가 표시되며 필요한 경우 해당 Collector에 대한 구성 요소를 비활성화하거나 활성화할 수 있습니다.



## Modify Deployment

### Cluster Information

Kubernetes Cluster	Network Performance and Map	Event Logs	Change Analysis
ci-demo-01	Enabled - Online	Enabled - Online	Enabled - Online

### Deployment Options

[Need Help?](#)

- Network Performance and Map
- Event Logs
- Change Analysis

Cancel

Complete Modification

업그레이드 중



최신 **Kubernetes Monitoring Operator**로 업그레이드하십시오

기존 운영자와 함께 AgentConfiguration이 존재하는지 확인합니다(네임스페이스가 DEFAULT\_NetApp-MONITORING\_이 아닌 경우 해당 네임스페이스를 대체합니다).

```
kubectl -n netapp-monitoring get agentconfiguration netapp-monitoring-configuration
```

AgentConfiguration이 있는 경우:

- **설치합니다** 기존 오퍼레이터에 대한 최신 운영자.
  - 항상 확인하십시오 **최신 컨테이너 이미지를 가져오는 중입니다** 사용자 지정 리포지토리를 사용하는 경우

AgentConfiguration이 없는 경우:

- 데이터 인프라 인사이트 에서 인식된 클러스터 이름을 기록합니다(네임스페이스가 기본 NetApp-monitoring이 아닌 경우 해당 네임스페이스를 대체).

```
kubectl -n netapp-monitoring get agent -o jsonpath='{.items[0].spec.cluster-name}'
```

\* 기존 운영자의 백업을 생성합니다 (네임스페이스가 기본 NetApp 모니터링이 아닌 경우 적절한 네임스페이스를 대체) .

```
kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
```

\* <<to-remove-the-kubernetes-monitoring-operator, 설치 제거>> 기존 연산자.  
\* <<installing-the-kubernetes-monitoring-operator, 설치합니다>> 최신 운영자.

- 동일한 클러스터 이름을 사용합니다.
- 최신 운영자 YAML 파일을 다운로드한 후 배포하기 전에 agent\_backup.YAML에서 발견된 모든 사용자 정의를 다운로드한 operator-config.YAML에 이식하십시오.
- 항상 확인하십시오 **최신 컨테이너 이미지를 가져오는 중입니다** 사용자 지정 리포지토리를 사용하는 경우

## **Kubernetes** 모니터링 오퍼레이터 중지 및 시작

Kubernetes 모니터링 운영자를 중지하려면 다음을 따르십시오.

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=0
```

Kubernetes 모니터링 운영자를 시작하려면 다음을 따르십시오.

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

## 제거 중

**Kubernetes Monitoring Operator**를 제거합니다

Kubernetes Monitoring Operator의 기본 네임스페이스는 "netapp-monitoring"입니다. 고유한 네임스페이스를 설정한 경우 이러한 네임스페이스 및 모든 후속 명령 및 파일로 대체합니다.

다음 명령을 사용하여 모니터링 연산자의 최신 버전을 제거할 수 있습니다.

```
kubectl -n <NAMESPACE> delete agent -l installed-by=nkmo-<NAMESPACE>
kubectl -n <NAMESPACE> delete
clusterrole,clusterrolebinding,crd,svc,deploy,role,rolebinding,secret,sa
-l installed-by=nkmo-<NAMESPACE>
```

모니터링 운영자가 자체 전용 네임스페이스에 배포된 경우 네임스페이스를 삭제합니다.

```
kubectl delete ns <NAMESPACE>
```

첫 번째 명령이 "리소스를 찾을 수 없음"을 반환하면 다음 지침에 따라 모니터링 연산자의 이전 버전을 제거합니다.

다음 명령을 순서대로 실행합니다. 현재 설치에 따라 이러한 명령 중 일부는 '개체를 찾을 수 없음' 메시지를 반환할 수 있습니다. 이러한 메시지는 무시해도 됩니다.

```
kubectl -n <NAMESPACE> delete agent agent-monitoring-netapp
kubectl delete crd agents.monitoring.netapp.com
kubectl -n <NAMESPACE> delete role agent-leader-election-role
kubectl delete clusterrole agent-manager-role agent-proxy-role agent-
metrics-reader <NAMESPACE>-agent-manager-role <NAMESPACE>-agent-proxy-role
<NAMESPACE>-cluster-role-privileged
kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-
rolebinding agent-cluster-admin-rolebinding <NAMESPACE>-agent-manager-
rolebinding <NAMESPACE>-agent-proxy-rolebinding <NAMESPACE>-cluster-role-
binding-privileged
kubectl delete <NAMESPACE>-psp-nkmo
kubectl delete ns <NAMESPACE>
```

보안 컨텍스트 제약 조건이 이전에 생성된 경우:

```
kubectl delete scc telegraf-hostaccess
```

## Kube-state-metrics 정보

NetApp Kubernetes Monitoring Operator는 다른 인스턴스와 충돌을 피하기 위해 고유한 kube-state-metrics를 설치합니다.

Kube-State-Metrics에 대한 자세한 내용은 를 참조하십시오 ["이 페이지"](#).

## 오퍼레이터 구성/사용자 지정

이 섹션에서는 운영자 구성을 사용자 지정하거나, 프록시를 사용하거나, 사용자 지정 또는 개인 Docker 리포지토리를 사용하거나, OpenShift를 사용하는 방법에 대한 정보를 제공합니다.

### 설정 옵션

가장 일반적으로 수정된 설정은 `_AgentConfiguration_custom` 리소스에서 구성할 수 있습니다. 운영자를 배포하기 전에 `_operator-config.YAML_file`을 편집하여 이 리소스를 편집할 수 있습니다. 이 파일에는 주석 처리된 설정 예가 포함되어 있습니다. 의 목록을 참조하십시오 ["사용 가능한 설정"](#) 를 참조하십시오.

다음 명령을 사용하여 연산자를 배포한 후에 이 리소스를 편집할 수도 있습니다.

```
kubectl -n netapp-monitoring edit AgentConfiguration
```

배포된 버전의 운영자가 AgentConfiguration을 지원하는지 확인하려면 다음 명령을 실행합니다.

```
kubectl get crd agentconfigurations.monitoring.netapp.com
```

"서버에서 오류 발생 (NotFound)" 메시지가 표시되는 경우 AgentConfiguration을 사용하려면 먼저 연산자를 업그레이드해야 합니다.

프록시 지원을 구성하는 중입니다

Kubernetes Monitoring Operator를 설치하기 위해 사용자 환경에서 프록시를 사용할 수 있는 위치는 두 곳입니다. 이러한 시스템은 동일하거나 별도의 프록시 시스템일 수 있습니다.

- 설치 코드 스니펫을 실행하는 동안("curl" 사용) 프록시를 사용하여 스니펫이 실행되는 시스템을 Data Infrastructure Insights 환경에 연결해야 합니다
- Data Infrastructure Insights 환경과 통신하는 데 필요한 프록시입니다

이 중 하나 또는 둘 모두에 프록시를 사용하는 경우 Kubernetes 운영 모니터를 설치하려면 먼저 프록시가 Data Infrastructure Insights 환경과 통신할 수 있도록 구성되었는지 확인해야 합니다. 프록시가 있고 운영자를 설치하려는 서버/VM에서 Data Infrastructure Insights에 액세스할 수 있는 경우 프록시가 제대로 구성된 것일 수 있습니다.

Kubernetes 운영 모니터를 설치하는 데 사용되는 프록시의 경우 Operator를 설치하기 전에 `_http_proxy/https_proxy_environment` 변수를 설정합니다. 일부 프록시 환경에서는 `_no_proxy` 환경\_변수를 설정해야 할 수도 있습니다.

변수를 설정하려면 Kubernetes Monitoring Operator를 설치하기 \* 전에 \* 시스템에서 다음 단계를 수행하십시오.

1. 현재 사용자에게 대한 `_https_proxy_and/or_http_proxy_environment` 변수를 설정합니다.
  - a. 설정 중인 프록시에 인증(사용자 이름/암호)이 없으면 다음 명령을 실행합니다.

```
export https_proxy=<proxy_server>:<proxy_port>
```

.. 설정 중인 프록시에 인증 (사용자 이름/암호) 이 있는 경우 다음 명령을 실행합니다.

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_port>
```

Kubernetes 클러스터가 Data Infrastructure Insights 환경과 통신하는 데 사용되는 프록시의 경우 이 모든 지침을 읽은 후 Kubernetes Monitoring Operator를 설치합니다.

Kubernetes 모니터링 연산자를 배포하기 전에 operator-config.yaml에서 AgentConfiguration의 프록시 섹션을 구성합니다.

```
agent:
  ...
  proxy:
    server: <server for proxy>
    port: <port for proxy>
    username: <username for proxy>
    password: <password for proxy>

    # In the noproxy section, enter a comma-separated list of
    # IP addresses and/or resolvable hostnames that should bypass
    # the proxy
    noproxy: <comma separated list>

    isTelegrafProxyEnabled: true
    isFluentbitProxyEnabled: <true or false> # true if Events Log enabled
    isCollectorsProxyEnabled: <true or false> # true if Network
    Performance and Map enabled
    isAuProxyEnabled: <true or false> # true if AU enabled
  ...
  ...
```

사용자 지정 또는 프라이빗 **Docker** 저장소 사용

기본적으로 Kubernetes Monitoring Operator는 Data Infrastructure Insights 저장소에서 컨테이너 이미지를 가져옵니다. Kubernetes 클러스터를 모니터링 대상으로 사용하고 있고 해당 클러스터가 사용자 지정 또는 프라이빗 Docker 저장소 또는 컨테이너 레지스트리에서 컨테이너 이미지만을 가져오도록 구성된 경우, Kubernetes Monitoring Operator가 필요한 컨테이너에 대한 액세스를 구성해야 합니다.

NetApp 모니터링 오퍼레이터 설치 파일에서 "이미지 풀 스니펫"을 실행합니다. 이 명령은 Data Infrastructure Insights 저장소에 로그인하고 운영자의 모든 이미지 종속성을 가져온 다음 Data Infrastructure Insights 저장소에서 로그아웃합니다. 메시지가 표시되면 제공된 리포지토리 임시 암호를 입력합니다. 이 명령은 옵션 기능을 포함하여 오퍼레이터가 사용하는 모든 이미지를 다운로드합니다. 이러한 이미지가 사용되는 기능은 아래를 참조하십시오.

핵심 운영자 기능 및 Kubernetes 모니터링

- NetApp - 모니터링

- ci-kube-RBAC-프록시
- CI - KSM을 참조하십시오
- CI - 텔레그래프
- distroless-root-user.(거리 없는 루트 사용자)

#### 이벤트 로그

- CI 플루언트 비트
- ci-kubernetes-event-exporter를 의미합니다

#### 네트워크 성능 및 맵

- CI-NET-관찰자

회사 정책에 따라 운영 Docker 이미지를 프라이빗/로컬/엔터프라이즈 Docker 저장소로 밀어 넣습니다. 리포지토리에 있는 이러한 이미지에 대한 이미지 태그와 디렉터리 경로가 Data Infrastructure Insights 리포지토리에 있는 이미지와 일치하는지 확인합니다.

운영자 배포에서 모니터링 - 운영자 배포를 편집합니다. YAML을 편집하고 모든 이미지 참조를 수정하여 개인 Docker 저장소를 사용하십시오.

```
image: <docker repo of the enterprise/corp docker repo>/kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

operator-config.yaml에서 AgentConfiguration을 편집하여 새로운 Docker 저장소 위치를 반영하십시오. 개인 리포지토리에 대한 새 imagePullSecret을 만듭니다. 자세한 내용은 <https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/> 참조하십시오

```
agent:
  ...
  # An optional docker registry where you want docker images to be pulled
  from as compared to CI's docker registry
  # Please see documentation link here:
  xref:{relative_path}task_config_telegraf_agent_k8s.html#using-a-custom-or-
  private-docker-repository
  dockerRepo: your.docker.repo/long/path/to/test
  # Optional: A docker image pull secret that maybe needed for your
  private docker registry
  dockerImagePullSecret: docker-secret-name
```

#### OpenShift 지침

OpenShift 4.6 이상에서 실행 중인 경우 \_operator-config.yaml\_에서 AgentConfiguration을 편집하여

`_Privileged_setting`을 활성화해야 합니다.

```
# Set runPrivileged to true SELinux is enabled on your kubernetes nodes
runPrivileged: true
```

OpenShift는 일부 Kubernetes 구성 요소에 대한 액세스를 차단할 수 있는 수준 높은 보안을 구현할 수 있습니다.

비밀에 대한 참고 사항

Kubernetes 모니터링 운영자가 클러스터 전체의 비밀을 볼 수 있는 권한을 제거하려면 설치하기 전에 `_operator-setup.yaml_file` 에서 다음 리소스를 삭제하십시오.

```
ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-clusterrolebinding
```

업그레이드인 경우 클러스터에서 리소스도 삭제합니다.

```
kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

변경 분석이 활성화된 경우 `_AgentConfiguration_or_operator-config.yaml_`를 수정하여 변경 관리 섹션의 주석을 해제하고 변경 관리 섹션 아래에 `_kindsToIgnoreFromWatch: "비밀"_`를 포함시킵니다. 이 줄에서 작은따옴표와 큰따옴표의 존재 및 위치를 확인합니다.

```
# change-management:
...
# # A comma separated list of kinds to ignore from watching from the
default set of kinds watched by the collector
# # Each kind will have to be prefixed by its apigroup
# # Example: '"networking.k8s.io.networkpolicies,batch.jobs",
"authorization.k8s.io.subjectaccessreviews"'
kindsToIgnoreFromWatch: '"secrets"'
...
```

## Kubernetes 체크섬 확인 중

Data Infrastructure Insights 에이전트 설치 관리자가 무결성 검사를 수행하지만 일부 사용자는 다운로드한 아티팩트를 설치하거나 적용하기 전에 자체 검증을 수행할 수 있습니다. 기본 다운로드 및 설치 대신 다운로드 전용 작업을 수행하기 위해 이러한 사용자는 UI에서 가져온 에이전트 설치 명령을 편집하고 뒤에 오는 "설치" 옵션을 제거할 수 있습니다.

다음 단계를 수행하십시오.

1. 지시에 따라 Agent Installer 스니펫을 복사합니다.

2. 코드 조각을 명령 창에 붙여 넣는 대신 텍스트 편집기에 붙여 넣습니다.
3. 명령에서 뒤에 오는 "--install"을 제거합니다.
4. 텍스트 편집기에서 전체 명령을 복사합니다.
5. 이제 명령 창(작업 디렉토리)에 붙여넣고 실행합니다.

◦ 다운로드 및 설치(기본값):

```
installerName=cloudinsights-rhel_centos.sh ... && sudo -E -H
./$installerName --download --install
** 다운로드 전용:
```

```
installerName=cloudinsights-rhel_centos.sh ... && sudo -E -H
./$installerName --download
```

download-only 명령은 Data Infrastructure Insights에서 작업 디렉토리로 필요한 모든 아티팩트를 다운로드합니다. 아티팩트에는 다음이 포함되지만 이에 국한되지는 않습니다.

- 설치 스크립트
- 환경 파일입니다
- YAML 파일
- 서명된 체크섬 파일(SHA256.signed)
- 서명 확인을 위한 PEM 파일(NetApp\_cert.pem)

육안 검사를 통해 설치 스크립트, 환경 파일 및 YAML 파일을 확인할 수 있습니다.

PEM 파일의 지문이 다음과 같은 것인지 확인하여 PEM 파일을 확인할 수 있습니다.

```
1A918038E8E127BB5C87A202DF173B97A05B4996
보다 구체적으로,
```

```
openssl x509 -fingerprint -sha1 -noout -inform pem -in netapp_cert.pem
서명된 체크섬 파일은 PEM 파일을 사용하여 확인할 수 있습니다.
```

```
openssl smime -verify -in sha256.signed -CAfile netapp_cert.pem -purpose
any
모든 아티팩트가 만족스럽게 확인되면 다음을 실행하여 에이전트 설치를 시작할 수 있습니다.
```

```
sudo -E -H ./<installation_script_name> --install
```

톨레랑스와 얼룩을 볼 수 있습니다

NetApp-CI-Telegraf-DS\_*netapp-ci-fluent-bit-DS* 및 *netapp-ci-net-observer-L4-DS*\_Demets는 모든 노드에서 데이터를 올바르게 수집하기 위해 클러스터의 모든 노드에 Pod를 예약해야 합니다. 운영자는 잘 알려진 일부 \* 얼룩을 견딜 수 있도록 구성되었습니다. 노드에서 사용자 지정 얼룩을 구성하여 모든 노드에서 Pod가 실행되지 않도록 하는 경우 이러한 얼룩에 대해 \* 공차 \* 를 생성할 수 있습니다 "[상담원 구성\\_에서](#)". 클러스터의 모든 노드에 사용자 지정 얼룩을 적용한 경우 운영자 포드를 예약 및 실행할 수 있도록 운영자 구축에 필요한 허용 오차도 추가해야 합니다.

Kubernetes에 대해 자세히 알아보십시오 "[오염과 내약입니다](#)".

로 돌아갑니다 "[\\*\\* NetApp Kubernetes 모니터링 오퍼레이터 설치 \\* 페이지](#)"

### 문제 해결

Kubernetes Monitoring Operator를 설정하는 데 문제가 발생할 경우 시도해 볼 수 있는 몇 가지 사항은 다음과 같습니다.

문제:	다음은 시도해 보십시오.
Kubernetes 영구 볼륨과 해당 백엔드 스토리지 장치 간의 하이퍼링크/연결이 표시되지 않습니다. 내 Kubernetes 영구 볼륨은 스토리지 서버의 호스트 이름을 사용하여 구성됩니다.	기존 Telegraf 에이전트를 제거한 다음 최신 Telegraf 에이전트를 다시 설치하는 단계를 따릅니다. Telegraf 버전 2.0 이상을 사용 중이고 Kubernetes 클러스터 스토리지를 Data Infrastructure Insights에서 능동적으로 모니터링해야 합니다.



<p>문제:</p> <p>로그에 다음과 같은 메시지가 표시됩니다.</p> <pre>E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: * v1.mutatingWebhookConfiguration: 서버에서 요청한 리소스를 찾을 수 없습니다 E0901 15:21:43.168161 반사판.go:178] k8s.io/kube- state-metrics/internal/store/builder.go:352: 목록*v1. 임대: 서버가 요청된 리소스를 찾을 수 없습니다(Get leases.coordination.k8s.io). 등</pre>	<p>다음을 시도해 보십시오.</p> <p>이러한 메시지는 Kubernetes 버전이 1.20 미만인 경우 kube-state-metrics 버전 2.0.0 이상을 실행하는 경우에 발생할 수 있습니다.</p> <p>Kubernetes 버전 가져오기:</p> <p><i>kubectf</i> 버전 _</p> <p><i>kube-state-metrics</i> 버전을 얻으려면:</p> <pre>_kubectf get deploy/kube-state-metrics -o jsonpath='{..image}'</pre> <p>이러한 메시지가 발생하지 않도록 하기 위해 사용자는 kube-state-metrics 배포를 수정하여 다음 임대 서비스를 비활성화할 수 있습니다.</p> <pre>mutatingwebhookconfiguration validatingwebhookconfiguration _volumeAttachments 리소스 _</pre> <p>보다 구체적으로 다음과 같은 CLI 인수를 사용할 수 있습니다.</p> <p>리소스 = certificatesigningrequests, configmap, cronjobs, demonset, 배포, 엔드포인트, 수평적 podautoscalers, ingresses, 작업, 제한 범위, 네임스페이스, 네트워크 정책, 노드, 영구 볼륨권, podrightiondecudies, 포드, 자원 컨트롤러, 리플리케이션, 풀 소스, 서비스</p> <p>기본 리소스 목록은 다음과 같습니다.</p> <p>"인증 요청, 구성 맵, cronjobs, demonset, 배포, 엔드포인트, 수평 포드오토칼러, ingresses, 작업, 임대, 제한 범위, mutatingwebhookconfiguration, 네임스페이스, 네트워크 정책, 노드, 지속형, 지속형, 지속형, 볼륨, 볼륨 구성, 복제, 웹후크구성, 볼륨 첨부 파일 확인"</p>
--	---

<p>문제:</p> <p>Telegraf에서 다음과 유사한 오류 메시지가 표시되지만 Telegraf가 시작되고 실행됩니다.</p> <p>10월 11일 14:23:41 IP-172-31-39-47 systemd [1]: 인플루엔자 DB에 메트릭을 보고하기 위한 플러그인 기반 서버 에이전트를 시작했습니다.</p> <p>10월 11일 14:23:41 IP-172-31-39-47 Telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="캐시 디렉토리를 만들지 못했습니다. /etc/Telegraf/.cache/snowflake, err:mkdir/etc/Telegraf/.ca CHE: 권한이 거부되었습니다. 무시됨 \n "func="gosnowflake.(* defaultLogger).Errorf" file="log.Go:120" 10월 11일 14:23:41 IP-172-31-39-47 Telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="를 열지 못했습니다. 무시되었습니다. /etc/Telegraf/.cache/snowflake/OCSP_response_cache.json을 엽니다. 해당 없음 파일 또는 디렉터리\n"func="gosnowflake.(* defaultLogger).Errorf" file="log.Go:120" 10월 11일 14:23:41 IP-172-31-39-47 Telegraf[1827]:2021-10-11T14:23:41Z !! 텔레그래프 1.19.3 시작</p>	<p>다음을 시도해 보십시오.</p> <p>이는 알려진 문제입니다. 을 참조하십시오 <a href="#">"이 GitHub 기사를 참조하십시오"</a> 를 참조하십시오. Telegraf가 실행 중인 경우 사용자는 이러한 오류 메시지를 무시할 수 있습니다.</p>
<p>Kubernetes에서 Telegraf POD가 다음 오류를 보고합니다.</p> <p>"mountstats 정보 처리 중 오류 발생: mountstats 파일을 열지 못했습니다. /hostfs/proc/1/mountstats, 오류: open/hostfs/proc/1/mountstats: permission denied"</p>	<p>SELinux가 설정되어 있고 강제 적용되는 경우 Telegraf 포드가 Kubernetes 노드의 /proc/1/mountstats 파일에 액세스하지 못할 수 있습니다. 이 제한을 해결하려면 agentconfiguration을 편집하고 runPrivileged 설정을 활성화하십시오. 자세한 내용은 를 참조하십시오 <a href="#">"OpenShift 지침"</a>.</p>
<p>Kubernetes에서 내 Telegraf ReplicaSet POD가 다음 오류를 보고합니다.</p> <p>[inputs.prometheus] 플러그인 오류: keypair /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key: open/etc/Kubernetes/pki/etcd/server.crt: 해당 파일 또는 디렉토리가 없습니다</p>	<p>Telegraf ReplicaSet POD는 마스터나 etcd로 지정된 노드에서 실행되도록 설계되었습니다. ReplicaSet 포드가 이러한 노드 중 하나에서 실행되고 있지 않으면 이러한 오류가 발생합니다. 마스터/etcd 노드에 문제가 있는지 확인합니다. 만약 그렇다면, 텔레그래프 ReplicaSet, 텔레그래프-RS에 필요한 내약성을 추가한다.</p> <p>예를 들어 ReplicaSet을 편집합니다.</p> <p>kubectl 편집 RS Telegraf-RS</p> <p>... 그리고 사양에 적절한 공차를 추가합니다. 그런 다음 ReplicaSet 포드를 다시 시작합니다.</p>

문제:	다음은 시도해 보십시오.
PSP/PSA 환경이 있습니다. 이 문제가 모니터링 오퍼레이터에게 영향을 미칩니까?	<p>Kubernetes 클러스터가 PSP(Pod Security Policy) 또는 PSA(Pod Security Admission)를 적용한 상태에서 실행되는 경우 최신 Kubernetes Monitoring Operator로 업그레이드해야 합니다. 다음 단계에 따라 PSP/PSA를 지원하는 현재 오퍼레이터로 업그레이드하십시오.</p> <p>1. <a href="#">설치 제거</a> 이전 모니터링 오퍼레이터:</p> <pre>kubectl delete agent-monitoring-netapp-n netapp-monitoring kubectl delete ns NetApp-monitoring kubectl 삭제 CRD agents.monitoring.netapp.com clusterrole agent-manager-role agent-proxy-role agent-metrics-reader를 삭제합니다 clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 을 삭제합니다</pre> <p>2. <a href="#">설치합니다</a> 모니터링 운영자의 최신 버전</p>
오퍼레이터를 배포하는 데 문제가 발생했고 PSP/PSA를 사용하고 있습니다.	<p>다음 명령을 사용하여 에이전트를 편집합니다.</p> <pre>kubectl -n &lt;name-space&gt; 편집 에이전트</pre> <p>'보안 정책 사용'을 '거짓'으로 표시합니다. 이렇게 하면 Pod 보안 정책 및 Pod 보안 입장이 비활성화되고 운영자가 배포할 수 있습니다. 다음 명령을 사용하여 확인합니다.</p> <pre>kubectl get psp(Pod 보안 정책이 제거됨) kubectl get all -n &lt;namespace&gt;</pre>
grep -i psp (아무것도 발견되지 않았음을 보여줌)	"ImagePullBackoff" 오류가 표시됩니다
이러한 오류는 사용자 지정 또는 전용 Docker 리포지토리가 있고 Kubernetes Monitoring Operator가 해당 리포지토리를 제대로 인식하도록 아직 구성하지 않은 경우 나타날 수 있습니다. <a href="#">자세히 보기</a> 사용자 지정/개인 저장소 구성 정보	모니터링 운영자 구축에 문제가 있는데 현재 설명서를 참조해도 문제를 해결하는 데 도움이 되지 않습니다.

<p>문제:</p> <p>다음 명령의 출력을 캡처하거나 기록해 두고 기술 지원 팀에 문의하십시오.</p> <pre>kubectl -n netapp-monitoring get all kubectl -n netapp-monitoring describe all kubectl -n netapp-monitoring logs &lt;monitoring-operator-pod&gt; --all -containers=true kubectl -n netapp-monitoring logs &lt;telegraf-pod&gt; --all -containers=true</pre>	<p>다음을 시도해 보십시오.</p> <p>Operator 네임스페이스의 NET-observer(워크로드 맵) 포드는 CrashLoopBackOff에 있습니다</p>
<p>이러한 포드는 네트워크 관찰 가능성을 위한 워크로드 맵 데이터 수집기에 해당합니다. 다음을 시도해 보십시오.</p> <ul style="list-style-type: none"> <li>• 최소 커널 버전을 확인하려면 pods 중 하나의 로그를 확인하십시오. 예를 들면 다음과 같습니다. — {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"유효성 검사에 실패했습니다. 이유: 커널 버전 3.10.0이 최소 커널 버전 4.18.0", "time":"2022-11-09T08:23:08Z"}보다 작습니다 —</li> <li>• Net-observer Pod를 사용하려면 Linux 커널 버전이 4.18.0 이상이어야 합니다. "uname -r" 명령을 사용하여 커널 버전을 확인하고 해당 버전이 4.18.0 이상인지 확인합니다</li> </ul>	<p>Pod는 운영자 네임스페이스(기본값: NetApp-모니터링)에서 실행되지만, 워크로드 맵 또는 Kubernetes 메트릭에 대한 UI에는 데이터가 표시되지 않습니다</p>
<p>K8S 클러스터의 노드에서 시간 설정을 확인합니다. 정확한 감사 및 데이터 보고를 위해 NTP(Network Time Protocol) 또는 SNTP(Simple Network Time Protocol)를 사용하여 Agent 시스템의 시간을 동기화하는 것이 좋습니다.</p>	<p>Operator 네임스페이스의 일부 NET-observer Pod가 Pending 상태입니다</p>
<p>Net-observer는 DemonSet로, k8s 클러스터의 각 노드에서 포드를 실행합니다.</p> <ul style="list-style-type: none"> <li>• 보류 중인 Pod를 확인하고 CPU 또는 메모리에 리소스 문제가 있는지 확인합니다. 노드에서 필요한 메모리 및 CPU를 사용할 수 있는지 확인합니다.</li> </ul>	<p>Kubernetes Monitoring Operator를 설치한 직후 로그에 다음이 표시됩니다.</p> <pre>[inputs.prometheus] 플러그인에서 오류 발생:\http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics:get\http://kube-state-metrics.&lt;namespace&gt;.svc.cluster.local:8080/metrics:다이얼 tcp:lookup kube-state-metrics.&lt;namespace&gt;.svc.cluster.local: 해당 호스트가 없습니다</pre>

문제:	다음을 시도해 보십시오.
이 메시지는 일반적으로 새 오퍼레이터가 설치되어 있고 <code>_Telegraf-RS_POD</code> 가 <code>_KSM_POD</code> 가 가동되기 전에 작동 중일 때만 표시됩니다. 이러한 메시지는 모든 Pod가 실행되면 중지되어야 합니다.	클러스터에 존재하는 Kubernetes CronJobs에 대해 어떤 메트릭도 수집되지 않습니다.
Kubernetes 버전 확인(예 <code>kubectl version</code> )를 클릭합니다. v1.20.x 이하일 경우 이는 예상되는 제한 사항입니다. Kubernetes Monitoring Operator와 함께 배포된 kube-state-metrics 릴리스는 v1.cronjob만 지원합니다. Kubernetes 1.20.x 이하에서는 <code>crontjob</code> 리소스가 v1beta.crontjob에 있습니다. 따라서 kube-state-metrics는 <code>crontjob</code> 리소스를 찾을 수 없습니다.	운영자 설치 후, Telegraf-ds Pod는 <code>CrashLoopBackOff</code> 로 진입하고 POD 로그는 "su:Authentication failure"를 나타낸다.
<code>_AgentConfiguration_</code> 에서 <code>Telegraf</code> 섹션을 편집하고 <code>_dockerMetricCollectionEnabled_</code> 를 <code>false</code> 로 설정합니다. 자세한 내용은 조작자를 "구성 옵션" 참조하십시오. 참고: <i>Data Infrastructure Insights Federal Edition</i> 을 사용하는 경우 <code>Docker</code> 소켓에 액세스하려면 <code>Telegraf</code> 컨테이너를 루트로 실행하거나 <code>_su_</code> 를 사용하여 <code>Telegraf</code> 사용자를 <code>Docker</code> 그룹에 추가해야 하기 때문에 <code>_su_</code> 사용이 제한된 사용자는 <code>Docker</code> 메트릭을 수집할 수 없습니다. <code>Docker</code> 메트릭 수집 및 <code>_su_</code> 의 사용은 기본적으로 활성화되어 있습니다. 이 두 가지를 모두 사용하지 않으려면 <code>_AgentConfiguration_</code> 파일에서 <code>_Telegraf.docker_entry</code> 를 제거하십시오. ... spec:... Telegraf:... -name:docker run-mode: -DemonSet 대체:- key:docker_unix_sock_placeholder 값: unix://run/docker.sock... ..	Telegraf 로그에 다음과 유사한 오류 메시지가 반복적으로 표시됩니다.  E! [agent] 출력에 쓰는 중 오류가 발생했습니다. http: POST "https://<tenant_url>/REST/v1/lake/injest/influxdb": 컨텍스트 기한 초과(클라이언트. 헤더 대기 중 시간 초과)
<code>_AgentConfiguration_</code> 에서 <code>Telegraf</code> 섹션을 편집하고 <code>increase_outputTimeout_</code> 을 10초로 편집합니다. 자세한 내용은 조작자를 참조하십시오 "구성 옵션".	일부 이벤트 로그에 대한 <code>_divedobject_data</code> 가 없습니다.
의 단계를 수행했는지 확인합니다 "권한" 섹션을 참조하십시오.	두 개의 모니터링 운영자 Pod가 실행 중인 것을 볼 수 있는데, 하나는 <code>netapp-ci-monitoring-operator- &lt;pod&gt;</code> 이고 다른 하나는 <code>monitoring-operator- &lt;pod&gt;</code> 입니다.
2023년 10월 12일부터 Data Infrastructure Insights는 사용자에게 더 나은 서비스를 제공하기 위해 운영자를 재고했습니다. 변경 사항을 완전히 채택하려면 반드시 <a href="#">기존 연산자를 제거합니다</a> AND를 준수해야 합니다. <a href="#">새 장치를 장착하십시오</a>	저의 Kubernetes 이벤트가 예기치 않게 Data Infrastructure Insights에 대한 보고를 중단했습니다.
이벤트 내보내기 포드의 이름을 검색합니다.  <pre>`kubectl -n netapp-monitoring get pods`</pre>	<code>grep event-exporter</code>

문제:	다음은 시도해 보십시오.
<pre>awk '{print \$1}'</pre>	<pre>sed 's/event-exporter./event-exporter/' "netapp-ci-event-exporter" 또는 "event-exporter"여야 합니다. 그런 다음 모니터링 에이전트를 편집합니다 `kubectl -n netapp-monitoring edit agent`를 입력하고 log_file 의 값을 이전 단계에서 찾은 적절한 이벤트 내보내기 포드 이름을 반영하도록 설정합니다. 보다 구체적으로 log_file을 "/var/log/containers/netapp-ci- event-exporter.log" 또는 "/var/log/containers/event- exporter .log"로 설정해야 합니다.</pre> <p>....</p> <p><b>fluent-bit:</b></p> <p>...</p> <p><b>- name: event-exporter-ci</b></p> <p><b>substitutions:</b></p> <p><b>- key: LOG_FILE</b></p> <p><b>values:</b></p> <p><b>- /var/log/containers/netapp-ci-event-exporter.log</b></p> <p>...</p> <p>....</p> <p>또는, 하나를 할 수도 있습니다 <a href="#">설치 제거 및 다시 설치합니다</a> 에이전트</p>
리소스 부족으로 인해 Kubernetes Monitoring Operator에 의해 구축된 Pod가 충돌하는 것을 볼 수 있습니다.	Kubernetes 모니터링 운영자를 참조하십시오 <a href="#">"구성 옵션"</a> 필요한 경우 CPU 및/또는 메모리 제한을 늘립니다.
이미지가 없거나 잘못된 구성으로 인해 NetApp-ci-kube-state 메트릭 Pod가 시작되지 않거나 준비되지 않았습니다. 이제 StatefulSet이 중단되고 구성 변경 사항이 NetApp-ci-kube-state-metrics Pod에 적용되지 않습니다.	StatefulSet 은 에 있습니다 <a href="#">"고장"</a> 상태. 구성 문제를 해결한 후에는 NetApp-ci-kube-state-metrics Pod를 바운스하게 만들 수 있습니다.
Kubernetes Operator 업그레이드를 실행하고 ErrImagePull(이미지를 가져오지 못함)을 throw하는 후 NetApp-ci-kube-state-metrics Pod가 시작되지 않습니다.	포드 재설정을 수동으로 시도하십시오.
"이벤트가 maxEventAgeSeconds보다 오래된 것으로 폐기됨" 메시지가 Log Analysis에서 내 Kubernetes 클러스터에 대해 관찰되고 있습니다.	Operator_agentconfiguration_을 수정하고 <i>event-exporter-maxEventAgeSeconds</i> (예: 60s), <i>event-exporter-kubeQPS</i> (예: 100) 및 <i>event-exporter-kubeBurst</i> (예: 500)를 증가시킵니다. 이러한 구성 옵션에 대한 자세한 내용은 를 참조하십시오 <a href="#">"구성 옵션"</a> 페이지.
Telegraf는 잠금 가능한 메모리가 부족하다는 경고 또는 충돌에 대해 경고합니다.	기본 운영 체제/노드에서 Telegraf의 잠금 가능한 메모리 제한을 늘리십시오. 제한을 늘리는 것이 옵션이 아닌 경우 NKMO agentconfiguration과 <i>set_unprotected_to_true</i> 를 수정합니다. 그러면 Telegraf가 잠긴 메모리 페이지를 예약하지 않도록 지시합니다. 암호 해독된 암호가 디스크로 교체될 수 있기 때문에 보안 위험이 발생할 수 있지만 잠긴 메모리를 예약할 수 없는 환경에서 실행할 수 있습니다. <i>_unprotected_configuration</i> 옵션에 대한 자세한 내용은 를 참조하십시오 <a href="#">"구성 옵션"</a> 페이지.

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지 또는 에 있습니다 "[Data Collector 지원 매트릭스](#)".

## Memcached Data Collector

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Memcached에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Memcached 를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_ 를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Memcached Configuration

Gathers Memcached metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-memcached.conf file.

```
[[inputs.memcached]]
  ## USER-ACTION: Provide comma-separated list of Memcached IP(s) and port(s).
  ## Please specify actual machine IP address, and refrain from using a loopback address
  ## (i.e. localhost or 127.0.0.1).
  ## When configuring with multiple Memcached servers, enter them in the format ["server1"
```

- 2 Replace <INSERT\_MEMCACHED\_ADDRESS> with the applicable Memcached server address. Please specify a real machine address, and refrain from using a loopback address.
- 3 Replace <INSERT\_MEMCACHED\_PORT> with the applicable Memcached server port.
- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

설정

정보는 에서 찾을 수 있습니다 "[멤캐시드 위키](#)".

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.



오브젝트:	식별자:	특성:	데이터 요소:
멤캐시드	네임스페이스 서버	노드 IP 노드 이름	접속 수락 처리된 인증 요청 실패한 인증 요청 사용된 바이트 읽기(초 당) 쓴 바이트 수(초 당) CAS Badval CAS 적중 CAS 적중 횟수 CAS 비적중 횟수 플러시 요청(초 당) 요청 수 (초당) 설정 요청 수(초당) 터치 요청 수(초당) 연결 수 (초당) 연결 구조 현재 연결 열기 현재 저장 항목 요청 횟수(초) 감소 요청 횟수(초) 삭제 요청 횟수(초) 삭제 요청 횟수(초) 삭제 요청 실패 횟수(초 단위) 제거된 항목 유효한 종료 항목 만료 항목 적중 횟수(초 단위) 적중 횟수(초 단위) 실패 횟수(초 단위) 사용된 해시 바이트 해시가 확장 중입니다. 해시 전력 수준 절개 요청 횟수(초) 오류 요청 횟수(초) 서버 최대 바이트 수신 비활성화 Num Reclaimed Worker Threads 수신 해제 총 열려 있는 연결 수 저장된 총 항목 터치 적중 횟수 서버 가동 시간

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

## MongoDB 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 MongoDB에서 메트릭을 수집합니다.

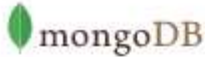
### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. MongoDB를 선택하십시오.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_ 를 클릭하여 를 확장합니다 ["에이전트 설치"](#) 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.

4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## MongoDB Configuration

Gathers MongoDB metrics.

---

### What Operating System or Platform Are You Using? [Need Help?](#)

RHEL & CentOS

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps [Need Help?](#)

- 1 Open mongod.conf. Locate the line beginning with "bindIp", and append the address of the node on which the Telegraf agent resides. After saving the change, restart the MongoDB server.
- 2 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-mongodb.conf file.

```
[[inputs.mongodb]]
  ## An array of URLs of the form:
  ## "mongodb://" [user ":" pass "@"] host [ ":" port]
  ## For example:
  ## mongodb://user:auth_key@10.10.3.30:27017,
  ## mongodb://10.10.0.0:27017
```
- 3 Replace <INSERT\_MONGODB\_ADDRESS> with the applicable MongoDB server address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_MONGODB\_PORT> with the applicable MongoDB port.
- 5 Restart the Telegraf service.

```
systemctl restart telegraf
```

설정

정보는 에서 찾을 수 있습니다 "MongoDB 설명서".

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
MongoDB	네임스페이스 호스트 이름		
MongoDB 데이터베이스	네임스페이스 호스트 이름 데이터베이스 이름입니다		

문제 해결

정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

## MySQL 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 MySQL에서 메트릭을 수집합니다.

설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. MySQL을 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 ["에이전트 설치"](#) 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## MySQL Configuration

Gathers MySQL metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-mysql.conf file.

```
[[inputs.mysql]]
  ## USER-ACTION: Provide comma-separated list of MySQL credentials, IP(s), and port(s)
  ## e.g. servers = ["user:passwd@tcp(127.0.0.1:3306)?tls=false"]
  ## Please specify actual machine IP address, and refrain from using a loopback address
  (i.e. localhost or 127.0.0.1).
```

- 2 Review and verify the contents of the configuration file.
- 3 Replace <INSERT\_USERNAME> and <INSERT\_PASSWORD> with the applicable MySQL credentials.
- 4 Replace <INSERT\_PROTOCOL> with the applicable MySQL connection protocol. The typical protocol is tcp.
- 5 Replace <INSERT\_MYSQL\_ADDRESS> with the applicable MySQL server address. Please specify a real machine address, and refrain from using a loopback address.
- 6 Replace <INSERT\_MYSQL\_PORT> with the applicable MySQL server port. The typical port is 3306.
- 7 Modify the 'tls' parameter in accordance to the MySQL server configuration.
- 8 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

설정

정보는 에서 찾을 수 있습니다 "MySQL 설명서".

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
MySQL	네임스페이스 MySQL Server	노드 IP 노드 이름	중단된 클라이언트(초당) 중단된 연결(초당) RX 바이트(초당) TX 바이트 (초당) 명령 Admin(초당) 명령 alter 이벤트 명령 alter 함수 명령 alter instance 명령 alter 프로시저 명령 alter 서버 명령 alter 테이블 명령 alter 테이블 공간 명령 alter 사용자 명령 alter 사용자 명령 alter 명령 assign to keycache 명령 시작 명령 binlog 명령 호출 프로시저 명령 변경 변경 마스터 명령 변경 Repl 필터 명령 검사 명령 체크섬 명령 실행 명령 생성 DB 명령 생성 이벤트 명령 생성 인덱스 명령 생성 프로시저 명령 생성 서버 명령 생성 테이블 명령 생성 트리거 명령 생성 UDF 명령 생성 사용자 명령 생성 보기 명령 생성 뷰 명령 생성 탈할당 SQL 연결 오류 생성된 TMP 디스크 테이블 지연 오류 플래시 명령 수락 처리기 커밋 InnoDB 버퍼 풀 바이트 데이터 키 블록이 플래시되지 않음 키 읽기 요청 키 쓰기 요청 키 쓰기 최대 실행 시간 초과 최대 사용된 연결 수 초과된 최대 파일 성능 스키마 계정 손실된 준비된 Stmt Count Qcache Free Blocks 쿼리 질문 전체 조인 선택 범위 선택 검사 선택 스캔 테이블 잠금 즉시 을 선택합니다

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## netstat 데이터 수집기


Data Infrastructure Insights는 이 데이터 수집기를 사용하여 netstat 메트릭을 수집합니다.

## 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. netstat를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 "에이전트 설치" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



### Netstat Configuration

Gathers netstat metrics of the host where telegraf agent is installed.

#### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

#### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

#### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-netstat.conf file.

```
# Read TCP metrics such as established, time wait and sockets counts.
[[inputs.netstat]]
# no configuration
[inputs.netstat.tags]
  CloudInsights = "true"
```
- 2 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

## 설정

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
netstat	노드 UUID	노드 IP 노드 이름	

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## Ngix 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Nginx에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Nginx를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_ 를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.

**NGINX** Nginx Configuration  
Gathers Nginx metrics.

What Operating System or Platform Are You Using? [Need Help?](#)

Ubuntu & Debian

Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)



## Follow Configuration Steps

[Need Help?](#)

1 If you already have a URL enabled to provide Nginx metrics, go directly to the plugin configuration.

2 Nginx metrics are available through a status page when the HTTP stub status module is enabled. Refer to the below link for verifying/enabling `http_stub_status_module`.

```
http://nginx.org/en/docs/http/nginx_http_stub_status_module.html
```

3 After verifying the module is enabled, modify the Nginx configuration to set up a locally-accessible URL for the status page:

```
server {  
    listen    <PORT NUMBER>;  
    Please specify actual machine IP address, and refrain from using a loopback address (i.e.  
    localhost or 127.0.0.1)  
    server_name <IP ADDRESS>;  
    location /nginx_status {  
        stub_status on;  
    }  
}
```

4 Reload the configuration:

```
nginx -s reload
```

5 Copy the contents below into a new `.conf` file under the `/etc/telegraf/telegraf.d/` directory. For example, copy the contents to the `/etc/telegraf/telegraf.d/cloudinsights-nginx.conf` file.

```
[[inputs.nginx]]  
  ## USER-ACTION: Provide Nginx status url  
  ## Please specify actual machine IP address where nginx_status is enabled, and refrain from  
  ## using a loopback address (i.e. localhost or 127.0.0.1).  
  ## When configuring with multiple Nginx servers, enter them in the format ["url1", "url2",  
  ## ...]
```

6 Replace `<INSERT_NGINX_ADDRESS>` with the applicable Nginx address. Please specify a real machine address, and refrain from using a loopback address.

7 Replace `<INSERT_NGINX_PORT>` with the applicable Nginx port.

8 Restart the Telegraf service.

```
systemctl restart telegraf
```

## 설정

Nginx 메트릭 컬렉션에는 Nginx가 필요합니다 "[HTTP\\_STUB\\_STATUS\\_MODULE](#)" 활성화합니다.

추가 정보는 에서 찾을 수 있습니다 "[Nginx 문서](#)".

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.



오브젝트:	식별자:	특성:	데이터 요소:
Nginx	네임스페이스 서버	노드 IP 노드 이름 포트	쓰기 대기 중인 활성 처리된 읽기 요청 허용

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 "[지원](#)" 페이지.

## PostgreSQL Data Collector

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 PostgreSQL에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. PostgreSQL을 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 "[에이전트 설치](#)" 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## PostgreSQL Configuration

Gathers PostgreSQL metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

RHEL & CentOS

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

[+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the /etc/telegraf/telegraf.d/ directory. For example, copy the contents to the /etc/telegraf/telegraf.d/cloudinsights-postgresql.conf file.

```
[[inputs.postgresql]]
# USER-ACTION: Provide credentials for access, address of PostgreSQL server, port for
PostgreSQL server, one DB for access
address = "postgres://<INSERT_USERNAME>:<INSERT_PASSWORD>@<INSERT_POSTGRESQL_ADDRESS>:
<INSERT_POSTGRESQL_PORT>/<INSERT_DB>"
```

- 2 Replace <INSERT\_USERNAME> and <INSERT\_PASSWORD> with the applicable PostgreSQL credentials.
- 3 Replace <INSERT\_POSTGRESQL\_ADDRESS> with the applicable PostgreSQL address. Please specify a real machine address, and refrain from using a loopback address.
- 4 Replace <INSERT\_POSTGRESQL\_PORT> with the applicable PostgreSQL port.
- 5 Replace <INSERT\_DB> with the applicable PostgreSQL database.
- 6 Modify 'Namespace' if needed for server disambiguation (to avoid name clashes).
- 7 Restart the Telegraf service.

```
systemctl restart telegraf
```

설정

정보는 에서 찾을 수 있습니다 "PostgreSQL 문서".

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
PostgreSQL 서버	Namespace 데이터베이스 서버	노드 이름 노드 IP입니다	할당된 버퍼 백엔드 버퍼 백엔드 파일 동기화 버퍼 체크포인트 버퍼 지우기 체크포인트 동기화 시간 체크포인트 쓰기 시간 체크포인트 요청 체크포인트 지정 시간 최대 쓰기 정리
PostgreSQL 데이터베이스	Namespace 데이터베이스 서버	데이터베이스 OID 노드 이름 노드 IP입니다	블록 읽기 시간 블록 쓰기 시간 블록 적중 횟수 블록 읽기 충돌 교착 상태 클라이언트 번호 임시 파일 바이트 임시 파일 수 행 삭제된 행 폐치 행 삽입 행 업데이트된 행 확정 트랜잭션 롤백업

## 문제 해결

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

## Puppet Agent Data Collector

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Puppet Agent에서 메트릭을 수집합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Puppet을 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, [\\_지침 표시\\_](#)를 클릭하여 를 확장합니다 ["에이전트 설치"](#) 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Puppet Agent Configuration

Gathers Puppet agent metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3) [+ Agent Access Key](#)

\*Please ensure that you have a Telegraf Agent in you environment before configuring [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-puppetagent.conf file.

```
## Reads last_run_summary.yaml file and converts to measurements
[[inputs.puppetagent]]
  ## Location of puppet last run summary file
  ## USER-ACTION: Modify the location if last_run_summary.yaml is on different path
  location = "/var/lib/puppet/state/last_run_summary.yaml"
```

- 2 Modify 'location' if last\_run\_summary.yaml is on different path
- 3 Modify 'Namespace' if needed for puppet agent disambiguation (to avoid name clashes).
- 4 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

## 설정

정보는 [여기](#) 에서 찾을 수 있습니다 "Puppet 문서"

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
-------	------	-----	---------

Puppet 에이전트	네임스페이스 노드 UUID	노드 이름 위치 노드 IP 버전 Configstring 버전 Puppet	변경 내용 총 이벤트 실패 이벤트 성공 이벤트 총 리소스 변경 실패 리소스 재시작 실패 리소스 OutOfSync 리소스 재시작 리소스 예약된 리소스 건너뛴 리소스 총 시간 앵커 시간 구성 시간 cron 시간 구성 파일 시간 실행 파일 시간 파일 시간 FilePucket 시간 Lastrun 시간 패키지 시간 예약 시간 서비스 시간 Sshauthorizedkey 시간 총계 시간 사용자
-------------	----------------	---	---

### 문제 해결

추가 정보는 에서 찾을 수 있습니다 ["지원"](#) 페이지.

### Redis Data Collector를 참조하십시오

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Redis에서 메트릭을 수집합니다. Redis는 데이터베이스, 캐시 및 메시지 브로커로 사용되는 오픈 소스 인메모리 데이터 구조 저장소로, 문자열, 해시, 목록, 집합 등의 데이터 구조를 지원합니다.

### 설치

1. 관측성 > 수집기 \* 에서 \* + Data Collector \* 를 클릭합니다. Redis를 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼용 에이전트를 설치하려는 경우, \_지침 표시\_를 클릭하여 를 확장합니다 ["에이전트 설치"](#) 지침.
3. 이 데이터 수집기에 사용할 Agent Access 키를 선택합니다. Agent 액세스 키 \* 버튼을 클릭하여 새 Agent 액세스 키를 추가할 수 있습니다. 모범 사례: OS/플랫폼별로 데이터 수집기를 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하십시오.
4. 구성 단계에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제 또는 플랫폼의 유형에 따라 다릅니다.



## Redis Configuration

Gathers Redis metrics.

### What Operating System or Platform Are You Using?

[Need Help?](#)

Windows

### Select existing Agent Access Key or create a new one

Default (405fb5ec-d4cb-4404-977b-71fa931e1ad3)

+ Agent Access Key

\*Please ensure that you have a Telegraf Agent in you environment before configuring. [Show Instructions](#)

### Follow Configuration Steps

[Need Help?](#)

- 1 Configure Redis to accept connections from the address of the node on which the Telegraf agent resides. Open the Redis configuration file.

```
vi /etc/redis.conf
```

- 2 Locate the line that begins with 'bind 127.0.0.1', and append the address of the node on which the Telegraf agent resides

```
bind 127.0.0.1 <NODE_IP_ADDRESS>
```

- 3 Copy the contents below into a new .conf file under the C:\Program Files\telegraf\telegraf.d\ folder. For example, copy the contents to the C:\Program Files\telegraf\telegraf.d\cloudinsights-redis.conf file.

```
# Read metrics from one or many redis servers
[[inputs.redis]]
  ## specify servers via a url matching:
  ## [protocol://][:password]@address[:port]
  ## e.g.
  ## http://username:password@127.0.0.1:6379
```

- 4 Replace <INSERT\_REDIS\_ADDRESS> with the applicable Redis address. Please specify a real machine address, and refrain from using a loopback address.

- 5 Replace <INSERT\_REDIS\_PORT> with the applicable Redis port.

- 6 Restart the Telegraf service.

```
Stop-Service -Name telegraf -ErrorAction SilentlyContinue; Start-Service -Name telegraf
```

설정

정보는 에서 찾을 수 있습니다 "Redis 문서".

## 개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
레드입니다	네임스페이스 서버		

## 문제 해결















추가 정보는 에서 찾을 수 있습니다 "지원" 페이지.

## 개체 아이콘 참조






Data Infrastructure Insights에 사용되는 오브젝트 아이콘입니다.

### 인프라 아이콘:

#### Storage

-  Backend Storage Array
-  Backend Volume
-  Disk
-  Internal Volume
-  Masking
-  Path
-  Q-Tree
-  Quota
-  Share
-  Storage
-  Storage Node
-  Storage Pool
-  Tape
-  Volume
-  Virtual Storage Array
-  Virtual Volume

#### Networking

-  Fabric
-  iSCSI Network Portal
-  iSCSI Session
-  NAS
-  NPV Switch
-  NPV Chassis
-  Port
-  Switch
-  Zone
-  Zone Members





#### Compute

-  Datastore
-  Host
-  Virtual Machine
-  VMDK

#### Application

-  Application

#### Misc.

-  Unknown
-  Generic
-  Violation
-  Failure

### Kubernetes 아이콘:



Cluster



Namespace



Workload



Node



Pod

Kubernetes Network Performance Monitoring 및 Map 아이콘:





# 법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

## 저작권

["https://www.netapp.com/company/legal/copyright/"](https://www.netapp.com/company/legal/copyright/)

## 상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

## 특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

## 개인 정보 보호 정책

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

## 오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이선스에 대한 정보를 제공합니다.

["데이터 인프라 인사이트\(이전의 Cloud Insights\)를 위한 고지 사항"](#)

["워크로드 보안 공지\(이전의 Cloud Secure\)"](#)

## 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.