데이터 수집기 참조 - 서비스

Data Infrastructure Insights

NetApp
February 18, 2026

목차

데이터 수집기 참조 - 서비스

노드 데이터 수집

Data Infrastructure Insights 에이전트를 설치한 노드에서 메트릭을 수집합니다.

설치

1. *관찰성 > 수집기*에서 운영 체제/플랫폼을 선택합니다. 통합 데이터 수집기(Kubernetes, Docker, Apache 등)를 설치하면 노드 데이터 수집도 구성됩니다.
2. 지침에 따라 에이전트를 구성하세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

객체 및 카운터

다음 객체와 해당 카운터는 노드 메트릭으로 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
노드 파일 시스템	노드 UUID 장치 경로 유형	노드 IP 노드 이름 노드 OS 모드	사용 가능한 Inode 사용 가능한 Inode 사용된 총 Inode 사용된 총 Inode 사용된 총 Inode
노드 디스크	노드 UUID 디스크	노드 IP 노드 이름 노드 OS	IO 시간 진행 중인 총 IOPS 읽기 바이트(초당) 읽기 시간 총 읽기(초당) 가중 IO 시간 총 쓰기 바이트(초당) 쓰기 시간 총 쓰기(초당) 현재 디스크 대기열 길이 쓰기 시간 읽기 시간 IO 시간
노드 CPU	노드 UUID CPU	노드 IP 노드 이름 노드 OS	시스템 CPU 사용량 사용자 CPU 사용량 유휴 CPU 사용량 프로세서 CPU 사용량 인터럽트 CPU 사용량 DPC CPU 사용량

물체:	식별자:	속성:	데이터 포인트:
마디	노드 UUID	노드 IP 노드 이름 노드 OS	커널 부팅 시간 커널 컨텍스트 스위치(초당) 커널 엔트로피 사용 가능 커널 인터럽트(초당) 포크된 커널 프로세스(초당) 메모리 활성 메모리 사용 가능 총 메모리 사용 가능 메모리 버퍼링된 메모리 캐시된 메모리 커밋 한도 커밋된 메모리 메모리 더티 메모리 사용 가능 메모리 높음 사용 가능 메모리 높음 총 메모리 초대형 페이지 크기 메모리 초대형 페이지 사용 가능 메모리 초대형 페이지 총 메모리 낮음 사용 가능 메모리 낮음 총 메모리 매핑된 메모리 페이지 테이블 메모리 공유 메모리 슬랩 메모리 스왑 캐시된 메모리 스왑 사용 가능 메모리 스왑 총 메모리 총 메모리 사용 가능 총 메모리 사용 가능 총 메모리 사용 가능 메모리 Vmalloc 청크 메모리 Vmalloc 총 메모리 Vmalloc 사용 메모리 와이어드 메모리 쓰기 저장 총 메모리 쓰기 저장 임시 메모리 캐시 오류 메모리 수요 제로 오류 메모리 페이지 오류 메모리 페이지 메모리 비페이지 메모리 페이지된 메모리 캐시 코어 메모리 대기 캐시 일반 메모리 대기 캐시 예약 메모리 전환 오류 프로세스 차단된 프로세스 죽은 프로세스 유휴 프로세스 페이징 프로세스 실행 중인 프로세스 휴면 프로세스 중지된 프로세스 총 프로세스 총 프로세스 총 스레드 프로세스 알 수 없는 프로세스 좀비 프로세서 대기열 길이 스왑 여유 스왑 총 사용된 스왑 총 사용된 스왑 스왑 인 스왑 아웃 시스템 가동 시간 시스템 CPU 수 시스템 사용자 수 시스템 호출

물체:	식별자:	속성:	데이터 포인트:
노드 네트워크	네트워크 인터페이스 노드 UUID	노드 이름 노드 IP 노드 OS	수신 바이트 전송 바이트 송신 패킷 삭제된 패킷 송신 오류 수신 패킷 삭제된 패킷 수신 오류 패킷 수신 패킷 송신 패킷

설정

설정 및 문제 해결 정보는 다음에서 찾을 수 있습니다."에이전트 구성" 페이지.

ActiveMQ 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 ActiveMQ에서 메트릭을 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. ActiveMQ를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. + 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[ActiveMQ 구성]

설정

정보는 다음에서 찾을 수 있습니다. "ActiveMQ 문서"

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
ActiveMQ 큐	네임스페이스 큐 포트 서버	노드 이름 노드 IP 노드 UUID	소비자 수 대기열 제거 수 대기열 삽입 수 대기열 크기

물체:	식별자:	속성:	데이터 포인트:
ActiveMQ 구독자	클라이언트 ID 연결 ID 포트 서버 네임스페이스	활성 대상 노드 이름 노드 IP 노드 UUID 노드 OS 선택기 구독	Dequeue Count Dispatched Count Dispatched Queue Size Enqueue Count Pending Queue Size
ActiveMQ 주제	주제 포트 서버 네임스페이스	노드 이름 노드 IP 노드 UUID 노드 OS	소비자 수 대기열 제거 수 대기열 삽입 수 크기

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

아파치 데이터 수집기

이 데이터 수집기를 사용하면 테넌트의 Apache 서버에서 데이터를 수집할 수 있습니다.

필수 조건

- Apache HTTP 서버를 설정하고 제대로 실행해야 합니다.
- 에이전트 호스트/VM에 sudo 또는 관리자 권한이 있어야 합니다.
- 일반적으로 Apache *mod_status* 모듈은 Apache 서버의 '/server-status?auto' 위치에 페이지를 노출하도록 구성됩니다. 사용 가능한 모든 필드를 수집하려면 *ExtendedStatus* 옵션을 활성화해야 합니다. 서버를 구성하는 방법에 대한 자세한 내용은 Apache 모듈 설명서를 참조하세요. https://httpd.apache.org/docs/2.4/mod/mod_status.html#enable

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Apache를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[아파치 구성]

설정

Apache HTTP 서버용 Telegraf 플러그인은 'mod_status' 모듈이 활성화되어야 합니다. 이 기능을 활성화하면 Apache HTTP 서버는 브라우저에서 볼 수 있거나 Apache HTTP 서버 구성의 모든 상태를 추출하기 위해 스크래핑할 수 있는 HTML 엔드포인트를 노출합니다.

호환성:

구성은 Apache HTTP 서버 버전 2.4.38을 기준으로 개발되었습니다.

mod_status 활성화:

'mod_status' 모듈을 활성화하고 노출하려면 두 단계가 필요합니다.

- 활성화 모듈
- 모듈에서 통계 노출

활성화 모듈:

모듈 로딩은 '/usr/local/apache/conf/httpd.conf' 아래의 구성 파일에 의해 제어됩니다. 구성 파일을 편집하고 다음 줄의 주석 처리를 제거합니다.

```
LoadModule status_module modules/mod_status.so
Include conf/extra/httpd-info.conf
```

모듈에서 통계 공개:

'mod_status'의 노출은 '/usr/local/apache2/conf/extra/httpd-info.conf' 아래의 설정 파일에 의해 제어됩니다. 해당 구성 파일에 다음 내용이 있는지 확인하세요(적어도 다른 지시어는 있어야 합니다).

```
# 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
```

'mod_status' 모듈에 대한 자세한 지침은 다음을 참조하세요."Apache 문서"

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
아파치	네임스페이스 서버	노드 IP 노드 이름 포트 상위 서버 구성 생성 상위 서버 MPM 생성 서버 가동 시간이 중지됨	바쁜 작업자 요청당 바이트 수 초당 바이트 수 CPU 자식 시스템 CPU 자식 사용자 CPU 부하 CPU 시스템 CPU 사용자 비동기 연결 종료 비동기 연결 유지 비동기 연결 쓰기 연결 요청당 총 기간 유휴 작업자 부하 평균(마지막 1m) 부하 평균(마지막 15m) 부하 평균(마지막 5m) 프로세스 초당 요청 총 액세스 총 기간 총 KByte 점수판 닫기 점수판 DNS 조회 점수판 완료 점수판 유휴 정리 점수판 유지 점수판 로깅 점수판 열기 점수판 읽기 점수판 전송 점수판 시작 점수판 대기

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

영사 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Consul에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. 영사를 선택하세요.

   수집을 위해 에이전트를 구성하지 않은 경우 다음 메시지가 표시됩니다."에이전트를 설치하다" 세입자에 대한.

   에이전트가 이미 구성되어 있는 경우 적절한 운영 체제나 플랫폼을 선택하고 *계속*을 클릭합니다.

2. Consul 구성 화면의 지침에 따라 데이터 수집기를 구성하세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

설정

정보는 다음에서 찾을 수 있습니다."영사 문서" .

영사를 위한 객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
영사	네임스페이스 확인 ID 서비스 노드	노드 IP 노드 OS 노드 UUID 노드 이름 서비스 이름 이름 서비스 ID 상태 확인	중대한 통과 경고

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Couchbase 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Couchbase에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Couchbase를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. + 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[Couchbase 구성]

설정

정보는 다음에서 찾을 수 있습니다."Couchbase 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
카우치베이스 노드	네임스페이스 클러스터 Couchbase 노드 호스트 이름	노드 이름 노드 IP	메모리 사용 가능 메모리 총계
카우치베이스 버킷	네임스페이스 버킷 클러스터	노드 이름 노드 IP	사용된 데이터 데이터 가져오기 사용된 디스크 항목 수 사용된 메모리 초당 작업 사용된 할당량

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

CouchDB 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 CouchDB에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. CouchDB를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[CouchDB 구성]

설정

정보는 다음에서 찾을 수 있습니다."CouchDB 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
카우치DB	네임스페이스 서버	노드 이름 노드 IP	인증 캐시 적중 인증 캐시 미스 데이터베이스 읽기 데이터베이스 쓰기 데이터베이스 열기 열기 OS 파일 최대 요청 시간 최소 요청 시간 Httpd 요청 메서드 복사 Httpd 요청 메서드 삭제 Httpd 요청 메서드 가져오기 Httpd 요청 메서드 헤드 Httpd 요청 메서드 포스트 Httpd 요청 메서드 넣기 상태 코드 200 상태 코드 201 상태 코드 202 상태 코드 301 상태 코드 304 상태 코드 400 상태 코드 401 상태 코드 403 상태 코드 404 상태 코드 405 상태 코드 409 상태 코드 412 상태 코드 500

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Docker 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Docker에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Docker를 선택하세요.

   수집을 위해 에이전트를 구성하지 않은 경우 다음 메시지가 표시됩니다."에이전트를 설치하다" 세입자에 대한.

   에이전트가 이미 구성되어 있는 경우 적절한 운영 체제나 플랫폼을 선택하고 *계속*을 클릭합니다.

2. Docker 구성 화면의 지침에 따라 데이터 수집기를 구성합니다. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[Docker 구성]

설정

Docker용 Telegraf 입력 플러그인은 지정된 UNIX 소켓이나 TCP 엔드포인트를 통해 메트릭을 수집합니다.

호환성

구성은 Docker 버전 1.12.6을 기준으로 개발되었습니다.

설정하기

UNIX 소켓을 통해 **Docker**에 액세스하기

Telegraf 에이전트가 베어메탈에서 실행 중인 경우 다음을 실행하여 docker Unix 그룹에 telegraf Unix 사용자를 추가합니다.

```
 sudo usermod -aG docker telegraf
Telegraf 에이전트가 Kubernetes Pod 내에서 실행되는 경우, 소켓을 볼륨으로 Pod에 매핑하여 Docker Unix 소켓을 노출한 다음 해당 볼륨을 /var/run/docker.sock에 마운트합니다.  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 제공된 Data Infrastructure Insights 설치 프로그램은 이 매핑을 자동으로 처리합니다.

TCP 엔드포인트를 통해 **Docker**에 액세스

기본적으로 Docker는 암호화되지 않은 액세스에는 포트 2375를 사용하고 암호화된 액세스에는 포트 2376을 사용합니다.

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
도커 엔진	네임스페이스 Docker 엔진	노드 이름 노드 IP 노드 UUID 노드 OS Kubernetes 클러스터 Docker 버전 단위	메모리 컨테이너 컨테이너 일시 중지된 컨테이너 실행 중인 컨테이너 중지된 CPU Go 루틴 이미지 리스너 사용된 이벤트 파일 설명자 사용 가능한 데이터 데이터 총 사용된 데이터 메타데이터 사용 가능한 메타데이터 총 사용된 메타데이터 풀 블록 크기

물체:	식별자:	속성:	데이터 포인트:
도커 컨테이너	네임스페이스 컨테이너 이름 Docker 엔진	Kubernetes 컨테이너 해시 Kubernetes 컨테이너 포트 Kubernetes 컨테이너 재시작 횟수 Kubernetes 컨테이너 종료 메시지 경로 Kubernetes 컨테이너 종료 메시지 정책 Kubernetes Pod 종료 유예 기간 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 Docker 버전 Kubernetes IO 구성 확인됨 Kubernetes IO 구성 소스 OpenShift IO SCC Kubernetes 설명 Kubernetes 표시 이름 OpenShift 태그 Kompose 서비스 Pod 템플릿 해시 컨트롤러 개정판 해시 Pod 템플릿 생성 라이선스 스키마 빌드 날짜 스키마 라이선스 스키마 이름 스키마 URL 스키마 VCS URL 스키마 공급업체 스키마 버전 스키마 스키마 버전 유지 관리자 고객 Pod Kubernetes StatefulSet Pod 이름 테넌트 웹 콘솔 아키텍처 권한 소스 URL 빌드 날짜 RH 빌드 호스트 RH 구성 요소 배포 범위 설치 릴리스 실행 요약 제거 VCS 참조 VCS 유형 공급업체 버전 상태 컨테이너 ID	메모리 활성 익명 메모리 활성 파일 메모리 캐시 메모리 계층적 제한 메모리 비활성 익명 메모리 비활성 파일 메모리 제한 메모리 매핑된 파일 메모리 최대 사용량 메모리 페이지 오류 메모리 페이지 주요 오류 메모리 페이지 인 메모리 페이지 아웃 메모리 상주 집합 크기 메모리 상주 집합 크기 초대형 메모리 총 활성 익명 메모리 총 활성 파일 메모리 총 캐시 메모리 총 비활성 익명 메모리 총 비활성 파일 메모리 총 매핑된 파일 메모리 총 페이지 오류 메모리 총 페이지 주요 오류 메모리 총 페이지 인 메모리 총 페이지 아웃 메모리 총 상주 집합 크기 메모리 총 상주 집합 크기 초대형 메모리 총 제거 불가 메모리 제거 불가 메모리 사용량 메모리 사용량 백분율 종료 코드 OOM 종료 PID 시작 실패 연속

물체:	식별자:	속성:	데이터 포인트:
Docker 컨테이너 블록 IO	네임스페이스 컨테이너 이름 장치 Docker 엔진	Kubernetes 컨테이너 해시 Kubernetes 컨테이너 포트 Kubernetes 컨테이너 재시작 횟수 Kubernetes 컨테이너 종료 메시지 경로 Kubernetes 컨테이너 종료 메시지 정책 Kubernetes Pod 종료 유예 기간 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 Docker 버전 Kubernetes 구성 확인 Kubernetes 구성 소스 OpenShift SCC Kubernetes 설명 Kubernetes 표시 이름 OpenShift 태그 스키마 스키마 버전 Pod 템플릿 해시 컨트롤러 개정 해시 Pod 템플릿 생성 Kompose 서비스 스키마 빌드 날짜 스키마 라이선스 스키마 이름 스키마 공급업체 고객 Pod Kubernetes StatefulSet Pod 이름 테넌트 웹 콘솔 빌드 날짜 라이선스 공급업체 아키텍처 권한 소스 URL RH 빌드 호스트 RH 구성 요소 배포 범위 설치 유지 관리자 릴리스 실행 요약 제거 VCS 참조 VCS 유형 버전 스키마 URL 스키마 VCS URL 스키마 버전 컨테이너 ID	IO 서비스 바이트 재귀적 비동기 IO 서비스 바이트 재귀적 읽기 IO 서비스 바이트 재귀적 동기 IO 서비스 바이트 재귀적 총 IO 서비스 바이트 재귀적 쓰기 IO 서비스 재귀적 비동기 IO 서비스 재귀적 읽기 IO 서비스 재귀적 동기 IO 서비스 재귀적 총 IO 서비스 재귀적 쓰기
Docker 컨테이너 네트워크	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 삭제 RX 바이트 RX 오류 RX 패킷 TX 삭제 TX 바이트 TX 오류 TX 패킷

물체:	식별자:	속성:	데이터 포인트:
Docker 컨테이너 CPU	네임스페이스 컨테이너 이름 CPU Docker 엔진	Kubernetes 컨테이너 해시 Kubernetes 컨테이너 포트 Kubernetes 컨테이너 재시작 횟수 Kubernetes 컨테이너 종료 메시지 경로 Kubernetes 컨테이너 종료 메시지 정책 Kubernetes Pod 종료 유예 기간 Kubernetes 구성 확인됨 Kubernetes 구성 소스 OpenShift SCC 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 개정판 해시 Pod 템플릿 생성 Kompose 서비스 스키마 빌드 날짜 스키마 라이선스 스키마 이름 스키마 공급업체 고객 Pod Kubernetes StatefulSet Pod 이름 테넌트 웹 콘솔 빌드 날짜 라이선스 공급업체 아키텍처 권한 소스 URL RH 빌드 호스트 RH 구성 요소 배포 범위 설치 유지 관리자 릴리스 실행 요약 제거 VCS 참조 VCS 유형 버전 스키마 URL 스키마 VCS URL 스키마 버전 컨테이너 ID	제한 기간 제한 제한 기간 제한 제한 시간 커널 모드 사용량 사용자 모드 사용량 사용량 백분율 시스템 사용량 총계

문제 해결

문제:	다음을 시도해 보세요:
구성 페이지의 지침을 따른 후에도 Data Infrastructure Insights 에서 Docker 메트릭이 보이지 않습니다.	Telegraf 에이전트 로그에서 다음 오류가 보고되는지 확인하세요: E! 플러그인 [inputs.docker]에서 오류가 발생했습니다. Docker 데몬 소켓에 연결하려고 하는 동안 권한이 거부되었습니다. 이 오류가 발생한 경우 위에 지정된 대로 Telegraf 에이전트가 Docker Unix 소켓에 액세스할 수 있도록 필요한 조치를 취하세요.

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Elasticsearch 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Elasticsearch에서 메트릭을 수집합니다.

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Elasticsearch를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. + 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[Elasticsearch 구성]

설정

정보는 다음에서 찾을 수 있습니다."Elasticsearch 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:
Elasticsearch 클러스터	네임스페이스 클러스터	노드 IP 노드 이름 클러스터 상태
Elasticsearch 노드	네임스페이스 클러스터 ES 노드 ID ES 노드 IP ES 노드	존 ID

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

플링크 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Flink에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. 플링크를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[플링크 구성]

설정

전체 Flink 배포에는 다음 구성 요소가 포함됩니다.

JobManager: Flink 기본 시스템입니다. 일련의 작업 관리자를 조정합니다. 고가용성 설정에서는 시스템에 두 개 이상의 JobManager가 있습니다. TaskManager: Flink 연산자가 실행되는 곳입니다. Flink 플러그인은 telegraf의 Jolokia 플러그인을 기반으로 합니다. 모든 Flink 구성 요소에서 정보를 수집해야 하므로 JMX는 모든 구성 요소에서 Jolokia를 통해 구성되고 노출되어야 합니다.

호환성

구성은 Flink 버전 1.7.0을 기준으로 개발되었습니다.

설정하기

졸로키아 에이전트 자

모든 개별 구성 요소에 대해 Jolokia 에이전트 jar 파일 버전을 다운로드해야 합니다. 테스트된 버전은 다음과 같습니다. "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

JobManager가 Jolokia API를 노출하도록 구성하려면 노드에서 다음 환경 변수를 설정한 다음 JobManager를 다시 시작합니다.

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

Jolokia(8778)의 경우 다른 포트를 선택할 수 있습니다. Jolokia를 잠글 내부 IP가 있는 경우 "모두 포함" 0.0.0.0을 자신의 IP로 바꿀 수 있습니다. 이 IP는 Telegraf 플러그인에서 접근할 수 있어야 합니다.

작업 관리자

Jolokia API를 노출하도록 TaskManager를 구성하려면 노드에서 다음 환경 변수를 설정한 다음 TaskManager를 다시 시작합니다.

```
 export FLINK_ENV_JAVA_OPTS="-javaagent:/opt/flink/lib/jolokia-jvm-1.6.0-agent.jar=port=8778,host=0.0.0.0"
```

Jolokia(8778)의 경우 다른 포트를 선택할 수 있습니다. Jolokia를 잠글 내부 IP가 있는 경우 "모두 포함" 0.0.0.0을 자신의 IP로 바꿀 수 있습니다. 이 IP는 Telegraf 플러그인에서 접근할 수 있어야 합니다.

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
Flink 작업 관리자	클러스터 네임스페이스 서버	노드 이름 작업 관리자 ID 노드 IP	네트워크 사용 가능 메모리 세그먼트 네트워크 총 메모리 세그먼트 가비지 수집 PS MarkSweep 카운트 가비지 수집 PS MarkSweep 시간 가비지 수집 PS Scavenge 카운트 가비지 수집 PS Scavenge 시간 커밋된 힙 메모리 힙 메모리 초기화 힙 메모리 최대 사용된 힙 메모리 스레드 수 데몬 스레드 수 최대 스레드 수 시작된 총 스레드 수
플링크 잡	클러스터 네임스페이스 서버 작업 ID	노드 이름 작업 이름 노드 IP 마지막 체크포인트 외부 경로 재시작 시간	가동 중지 시간 전체 재시작 마지막 체크포인트 정렬 버퍼링 마지막 체크포인트 기간 마지막 체크포인트 크기 완료된 체크포인트 수 실패한 체크포인트 수 진행 중인 체크포인트 수 체크포인트 수 가동 시간

물체:	식별자:	속성:	데이터 포인트:
Flink 작업 관리자	클러스터 네임스페이스 서버	노드 이름 노드 IP	가비지 수집 PS MarkSweep 카운트 가비지 수집 PS MarkSweep 시간 가비지 수집 PS Scavenge 카운트 가비지 수집 PS Scavenge 시간 힙 메모리 커밋됨 힙 메모리 초기화 힙 메모리 최대 사용 힙 메모리 등록된 작업 관리자 수 실행 중인 작업 수 사용 가능한 작업 슬롯 작업 슬롯 총 스레드 수 데몬 스레드 수 최대 스레드 수 시작된 총 스레드 수
플링크 작업	클러스터 네임스페이스 작업 ID 작업 ID	서버 노드 이름 작업 이름 하위 작업 인덱스 작업 시도 ID 작업 시도 번호 작업 이름 작업 관리자 ID 노드 IP 현재 입력 워터마크	풀에 있는 버퍼 사용량 버퍼에 있는 큐 길이 버퍼에 있는 풀에 있는 버퍼 사용량 버퍼에 있는 큐 길이 수 로컬에 있는 버퍼 수 초당 로컬에 있는 버퍼 수 개수 초당 로컬에 있는 버퍼 수 원격에 있는 버퍼 수 초당 원격에 있는 버퍼 수 초당 원격에 있는 버퍼 수 초당 버퍼 수 버퍼 출력 수 초당 버퍼 출력 수 초당 버퍼 출력 수 초당 속도 수 로컬에 있는 바이트 수 초당 로컬에 있는 바이트 수 초당 로컬에 있는 바이트 수 초당 속도 수 원격에 있는 바이트 수 초당 원격에 있는 바이트 수 초당 원격에 있는 바이트 수 초당 원격에 있는 바이트 수 초당 속도 수 바이트 출력 수 초당 바이트 출력 수 초당 바이트 출력 수 초당 바이트 출력 속도 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수 초당 레코드 수

물체:	식별자:	속성:	데이터 포인트:
Flink 작업 연산자	클러스터 네임스페이스 작업 ID 운영자 ID 작업 ID	서버 노드 이름 작업 이름 운영자 이름 하위 작업 인덱스 작업 시도 ID 작업 시도 번호 작업 이름 작업 관리자 ID 노드 IP	현재 입력 워터마크 현재 출력 워터마크 수 초당 레코드 수신 수 초당 레코드 수신 수 초당 레코드 수신 속도 초당 레코드 수신 수 초당 레코드 수신 속도 초당 레코드 송신 수 초당 레코드 송신 속도 지연 레코드 삭제 할당된 파티션 바이트 사용 속도 커밋 대기 시간 평균 커밋 대기 시간 최대 커밋 속도 커밋 실패 커밋 성공 연결 종료 속도 연결 수 연결 생성 속도 수 페치 대기 시간 평균 페치 대기 시간 최대 페치 속도 페치 크기 평균 페치 크기 최대 페치 제한 시간 평균 페치 제한 시간 최대 하트비트 속도 수신 바이트 속도 IO 비율 IO 시간 평균(ns) IO 대기 비율 IO 대기 시간 평균(ns) 조인 속도 조인 시간 평균 마지막 하트비트 전 네트워크 IO 속도 발신 바이트 속도 레코드 사용 속도 레코드 지연 최대 요청당 레코드 평균 요청 속도 요청 크기 평균 요청 크기 최대 응답 속도 선택 속도 동기화 속도 동기화 시간 평균 하트비트 응답 시간 최대 조인 시간 최대 동기화 시간 최대

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Hadoop 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Hadoop에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Hadoop을 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.

3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[Hadoop 구성] [Hadoop 구성]

설정

전체 Hadoop 배포에는 다음 구성 요소가 포함됩니다.

- NameNode: Hadoop 분산 파일 시스템(HDFS)의 기본 시스템입니다. 일련의 DataNode를 조정합니다.
- 보조 NameNode: 기본 NameNode에 대한 웜 페일오버입니다. Hadoop에서는 NameNode로의 승격이 자동으로 발생하지 않습니다. 보조 NameNode는 NameNode로부터 정보를 수집하여 필요할 때 승격될 준비를 합니다.
- DataNode: 데이터의 실제 소유자입니다.
- ResourceManager: 컴퓨팅 기본 시스템(Yarn). 일련의 NodeManager를 조정합니다.
- NodeManager: 컴퓨팅 리소스. 애플리케이션을 실행하기 위한 실제 위치입니다.
- JobHistoryServer: 모든 구직 기록 관련 요청을 처리하는 역할을 담당합니다.

Hadoop 플러그인은 Telegraf의 Jolokia 플러그인을 기반으로 합니다. 모든 Hadoop 구성 요소에서 정보를 수집해야 하는 요구 사항으로, JMX는 모든 구성 요소에서 Jolokia를 통해 구성되고 노출되어야 합니다.

호환성

구성은 Hadoop 버전 2.9.2를 기준으로 개발되었습니다.

설정하기

졸로키아 에이전트 자

모든 개별 구성 요소에 대해 Jolokia 에이전트 jar 파일 버전을 다운로드해야 합니다. 테스트된 버전은 다음과 같습니다. "졸로키아 에이전트 1.6.0" .

아래 지침에서는 다운로드한 jar 파일(jolokia-jvm-1.6.0-agent.jar)이 '/opt/hadoop/lib/' 위치에 있다고 가정합니다.

네임노드

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.
```

보조 네임노드

Jolokia API를 노출하도록 Secondary NameNode를 구성하려면 <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.
```

데이터노드

Jolokia API를 노출하도록 DataNode를 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.
```

리소스매니저

Jolokia API를 노출하도록 ResourceManager를 구성하려면 <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.
```

노드매니저

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

Jolokia API를 노출하도록 JobHistoryServer를 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.
```

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:
Hadoop 보조 네임노드	클러스터 네임스페이스 서버	노드 이름 노드 IP 컴파일 정보 버전
Hadoop 노드 매니저	클러스터 네임스페이스 서버	노드 이름 노드 IP
Hadoop 리소스 관리자	클러스터 네임스페이스 서버	노드 이름 노드 IP
하둡 데이터노드	클러스터 네임스페이스 서버	노드 이름 노드 IP 클러스터 ID 버전

물체:	식별자:	속성:
Hadoop 네임노드	클러스터 네임스페이스 서버	노드 이름 노드 IP 트랜잭션 ID 마지막 로드 이후 마지막 쓰기 시간 편집 HA 상태 파일 시스템 상태 블록 풀 ID 클러스터 ID 컴파일 정보 고유 버전 개수 버전
Hadoop JobHistoryServer	클러스터 네임스페이스 서버	노드 이름 노드 IP

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

HAProxy 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 HAProxy에서 메트릭을 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. HAProxy를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. + 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[HAProxy 구성]

설정

HAProxy용 Telegraf 플러그인은 HAProxy Stats 활성화에 의존합니다. 이는 HAProxy에 내장된 구성이지만 기본적으로 활성화되어 있지 않습니다. HAProxy를 활성화하면 브라우저에서 볼 수 있거나 모든 HAProxy 구성의 상태를 추출하기 위해 스크래핑할 수 있는 HTML 엔드포인트가 노출됩니다.

호환성:

구성은 HAProxy 버전 1.9.4를 기준으로 개발되었습니다.

설정:

통계를 활성화하려면 haproxy 구성 파일을 편집하고 '기본값' 섹션 뒤에 다음 줄을 추가하고, 사용자 이름/비밀번호 및 /또는 haproxy URL을 사용하세요.

```
stats enable
stats auth myuser:mypassword
stats uri  /haproxy?stats
```

다음은 통계가 활성화된 단순화된 예시 구성 파일입니다.

```
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
```

완전하고 최신의 지침은 다음을 참조하세요."HAProxy 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
HAProxy 프런트엔드	네임스페이스 주소 프록시	노드 IP 노드 이름 프록시 ID 모드 프로세스 ID 세션 속도 제한 서버 ID 세션 제한 상태	바이트 입력 바이트 출력 캐시 적중 캐시 조회 압축 우회된 바이트 압축 바이트 입력 압축 바이트 출력 압축 응답 연결 속도 연결 속도 최대 연결 수 연결 규칙에 의해 거부된 총 요청 수 보안 문제로 인해 거부된 요청 수 보안 문제로 인해 거부된 응답 수 세션 규칙에 의해 거부된 요청 수 요청 오류 응답 1xx 응답 2xx 응답 3xx 응답 4xx 응답 5xx 응답 기타 가로채기된 요청 수 세션 속도 세션 속도 최대 요청 속도 요청 속도 최대 요청 수 총 세션 수 세션 수 최대 세션 수 총 요청 수 다시 쓰기
HAProxy 서버	네임스페이스 주소 프록시 서버	노드 IP 노드 이름 확인 완료 시간 확인 하강 구성 확인 상태 값 확인 상승 구성 확인 상태 프록시 ID 마지막 변경 시간 마지막 세션 시간 모드 프로세스 ID 서버 ID 상태 가중치	활성 서버 백업 서버 바이트 입력 바이트 출력 체크 다운 체크 실패 클라이언트 중단 연결 연결 평균 시간 다운타임 총 거부된 응답 연결 오류 응답 오류 응답 1xx 응답 2xx 응답 3xx 응답 4xx 응답 5xx 응답 선택된 다른 서버 총 대기열 현재 대기열 최대 대기열 평균 시간 초당 세션 초당 세션 최대 연결 재사용 응답 시간 평균 세션 세션 최대 서버 전송 중단 세션 총 세션 총 시간 평균 요청 재전송 요청 재시도 요청 다시 쓰기

물체:	식별자:	속성:	데이터 포인트:
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 입력 바이트 출력 캐시 적중 캐시 조회 체크 다운 클라이언트 중단 압축 우회된 바이트 압축 바이트 입력 바이트 압축 바이트 출력 압축 응답 연결 연결 평균 시간 가동 중지 시간 보안 문제로 인해 거부된 총 요청 보안 문제로 인해 거부된 응답 연결 오류 응답 오류 응답 1xx 응답 2xx 응답 3xx 응답 4xx 응답 5xx 응답 선택된 다른 서버 총 대기열 현재 대기열 최대 대기열 평균 시간 초당 세션 초당 세션 최대 요청 총 연결 재사용 응답 시간 평균 세션 세션 최대 서버 전송 중단 세션 총 세션 총 시간 평균 요청 재전송 요청 재시도 요청 다시 쓰기

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

JVM 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 JVM에서 메트릭을 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. JVM을 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. + 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[JVM 구성]

설정

정보는 다음에서 찾을 수 있습니다."JVM 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
제이비엠	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 로드됨 클래스 로드됨 총 클래스 언로드됨 메모리 힙 커밋됨 메모리 힙 초기화 메모리 힙 사용됨 최대 메모리 힙 사용됨 메모리 힙 없음 커밋됨 메모리 힙 없음 초기화 메모리 힙 없음 최대 메모리 힙 없음 사용됨 메모리 개체 마무리 보류 OS 프로세서 사용 가능 OS 커밋됨 가상 메모리 크기 OS 사용 가능 물리적 메모리 크기 OS 사용 가능 스왑 공간 크기 OS 최대 파일 설명자 수 OS 열린 파일 설명자 수 OS 프로세서 CPU 부하 OS 프로세서 CPU 시간 OS 시스템 CPU 부하 OS 시스템 부하 평균 OS 총 물리적 메모리 크기 OS 총 스왑 공간 크기 스레드 데몬 수 스레드 피크 수 스레드 수 스레드 시작 스레드 수 가비지 컬렉터 복사 수집 수 가비지 컬렉터 복사 수집 시간 가비지 컬렉터 마크 스윕 수집 수 가비지 컬렉터 마크 스윕 수집 시간 가비지 컬렉터 G1 이전 세대 수집 수 가비지 컬렉터 G1 이전 세대 수집 시간 가비지 컬렉터 G1 젊은 세대 수집 수 가비지 컬렉터 G1 젊은 세대 수집 시간 가비지 컬렉터 동시 Mark-sweep 수집 횟수 가비지 수집기 동시 Mark-sweep 수집 시간 가비지 수집기 병렬 수집 횟수 가비지 수집기 병렬 수집 시간 가비지 수집기 병렬 청소 Mark-sweep 수집 횟수 가비지 수집기 병렬 청소 Mark-sweep 수집 시간 가비지 수집기 병렬 청소 수집 횟수 가비지 수집기 병렬 청소 수집 시간

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

카프카 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Kafka에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. 카프카를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. + 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[카프카 구성]

설정

카프카 플러그인은 텔레그라프의 졸로키아 플러그인을 기반으로 합니다. 모든 Kafka 브로커에서 정보를 수집해야 하는 요구 사항으로, JMX는 모든 구성 요소에서 Jolokia를 통해 구성되고 노출되어야 합니다.

호환성

구성은 Kafka 버전 0.11.0.2를 기준으로 개발되었습니다.

설정 중

아래의 모든 지침은 카프카 설치 위치가 '/opt/kafka'라고 가정합니다. 아래 지침을 설치 위치에 맞게 조정할 수 있습니다.

졸로키아 에이전트 자

Jolokia 에이전트 jar 파일은 다음 버전이어야 합니다."다운로드됨" . 테스트에 사용된 버전은 Jolokia 에이전트 1.6.0입니다.

아래 지침에서는 다운로드한 jar 파일(jolokia-jvm-1.6.0-agent.jar)이 '/opt/kafka/libs/' 위치에 있다고 가정합니다.

카프카 브로커스

Jolokia API를 노출하도록 Kafka Brokers를 구성하려면 'kafka-run-class.sh' 호출 바로 앞의 <KAFKA_HOME>/bin/kafka-server-start.sh에 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 예에서는 'hostname -I'를 사용하여 'RMI_HOSTNAME' 환경 변수를 설정하고 있습니다. 여러 IP 머신에서 RMI 연결에 필요한 IP를 수집하려면 이 설정을 조정해야 합니다.

JMX(위의 9999)와 Jolokia(8778)에 대해 다른 포트를 선택할 수 있습니다. Jolokia를 잠글 내부 IP가 있는 경우 "모두 포함" 0.0.0.0을 자신의 IP로 바꿀 수 있습니다. 이 IP는 Telegraf 플러그인에서 접근할 수 있어야 합니다. 인증을 원하지 않으면 '-Dcom.sun.management.jmxremote.authenticate=false' 옵션을 사용할 수 있습니다. 사용 시 모든 책임은 사용자에게 있습니다.

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:
카프카 브로커	클러스터 네임스페이스 브로커	노드 이름 노드 IP

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

키바나 데이터 수집기

Data Infrastructure Insights 이 데이터 수집기를 사용하여 Kibana에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. 키바나를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.

[키바나 구성]

설정

정보는 다음에서 찾을 수 있습니다."Kibana 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
키바나	네임스페이스 주소	노드 IP 노드 이름 버전 상태	동시 연결 힙 최대 사용 힙 초당 요청 응답 시간 평균 응답 시간 최대 가동 시간

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Kubernetes 모니터링 운영자 설치 및 구성

Data Infrastructure Insights Kubernetes 컬렉션을 위한 *Kubernetes Monitoring Operator*를 제공합니다. 새로운 운영자를 배포하려면 *Kubernetes > Collectors > +Kubernetes Collector*로 이동합니다.

Kubernetes Monitoring Operator를 설치하기 전에

를 참조하십시오"필수 조건" Kubernetes Monitoring Operator를 설치하거나 업그레이드하기 전에 설명서를 참조하세요.

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

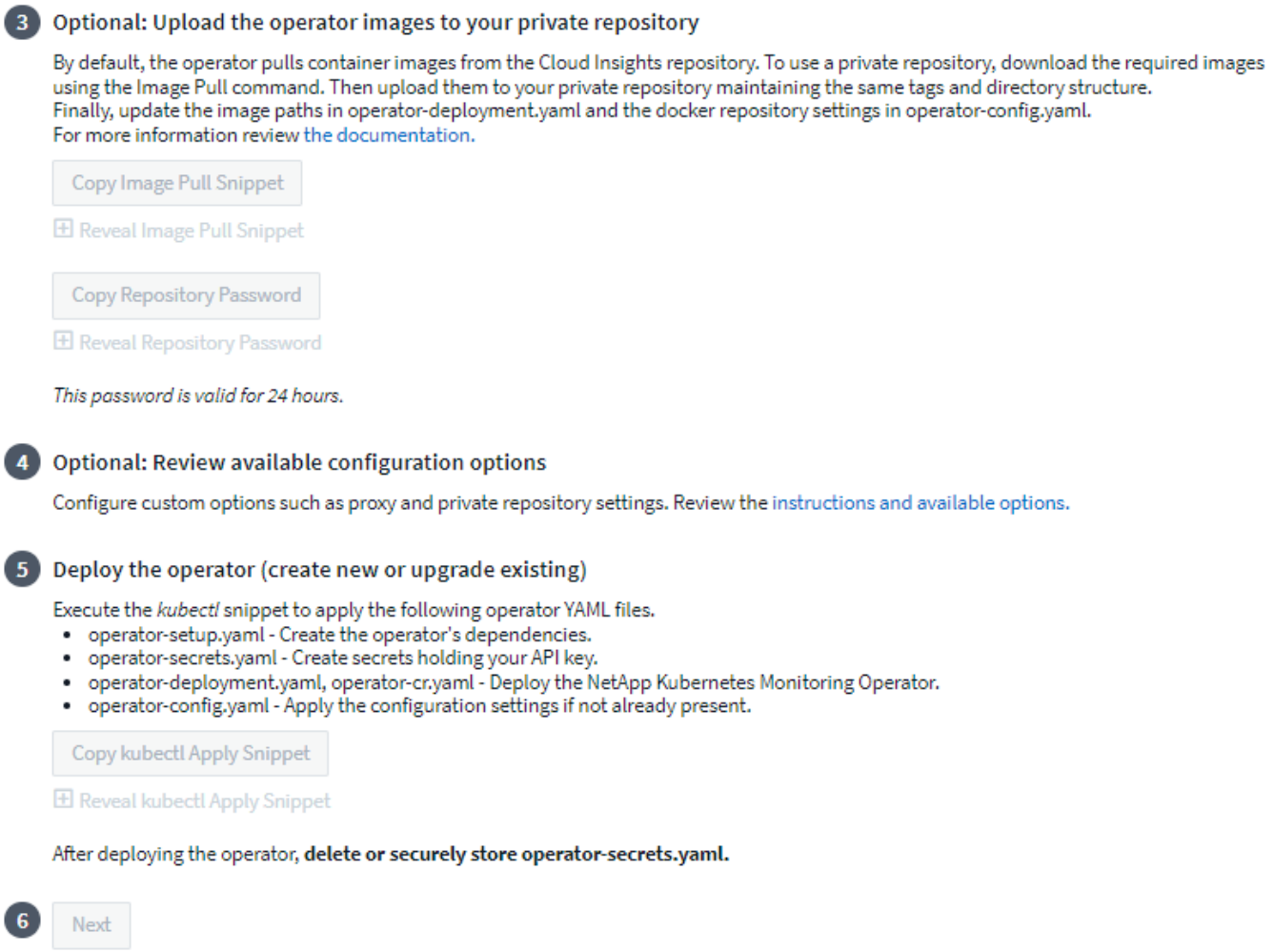
2 Download the operator YAML files

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.



Kubernetes에 **Kubernetes Monitoring Operator** 에이전트를 설치하는 단계:

1. 고유한 클러스터 이름과 네임스페이스를 입력하세요. 만약 당신이라면업그레이드 이전 Kubernetes Operator에서 동일한 클러스터 이름과 네임스페이스를 사용합니다.
2. 이를 입력하면 다운로드 명령 스니펫을 클립보드에 복사할 수 있습니다.
3. 스니펫을 *bash* 창에 붙여넣고 실행합니다. Operator 설치 파일이 다운로드됩니다. 스니펫에는 고유 키가 있으며 24시간 동안 유효합니다.
4. 사용자 정의 또는 개인 저장소가 있는 경우 선택 사항인 이미지 풀 스니펫을 복사하여 *bash* 셸에 붙여넣고 실행합니다. 이미지를 가져온 후 개인 저장소에 복사하세요. 동일한 태그와 폴더 구조를 유지하세요. _operator-deployment.yaml_의 경로와 _operator-config.yaml_의 docker 저장소 설정을 업데이트합니다.
5. 원하는 경우 프록시나 개인 저장소 설정 등 사용 가능한 구성 옵션을 검토하세요. 더 자세히 읽어보세요"구성 옵션" .
6. 준비가 되면 kubectl Apply 스니펫을 복사하고, 다운로드하고, 실행하여 Operator를 배포합니다.
7. 설치가 자동으로 진행됩니다. 완료되면 다음 버튼을 클릭하세요.
8. 설치가 완료되면 다음 버튼을 클릭하세요. *operator-secrets.yaml* 파일도 삭제하거나 안전하게 저장하세요.

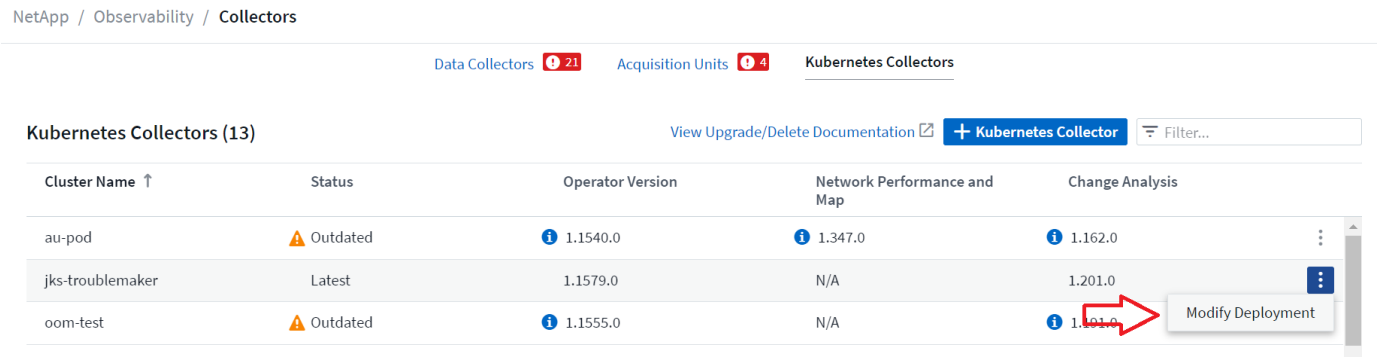
사용자 정의 저장소가 있는 경우 다음을 읽어보세요.사용자 정의/개인 Docker 저장소 사용 .

Kubernetes 모니터링 구성 요소

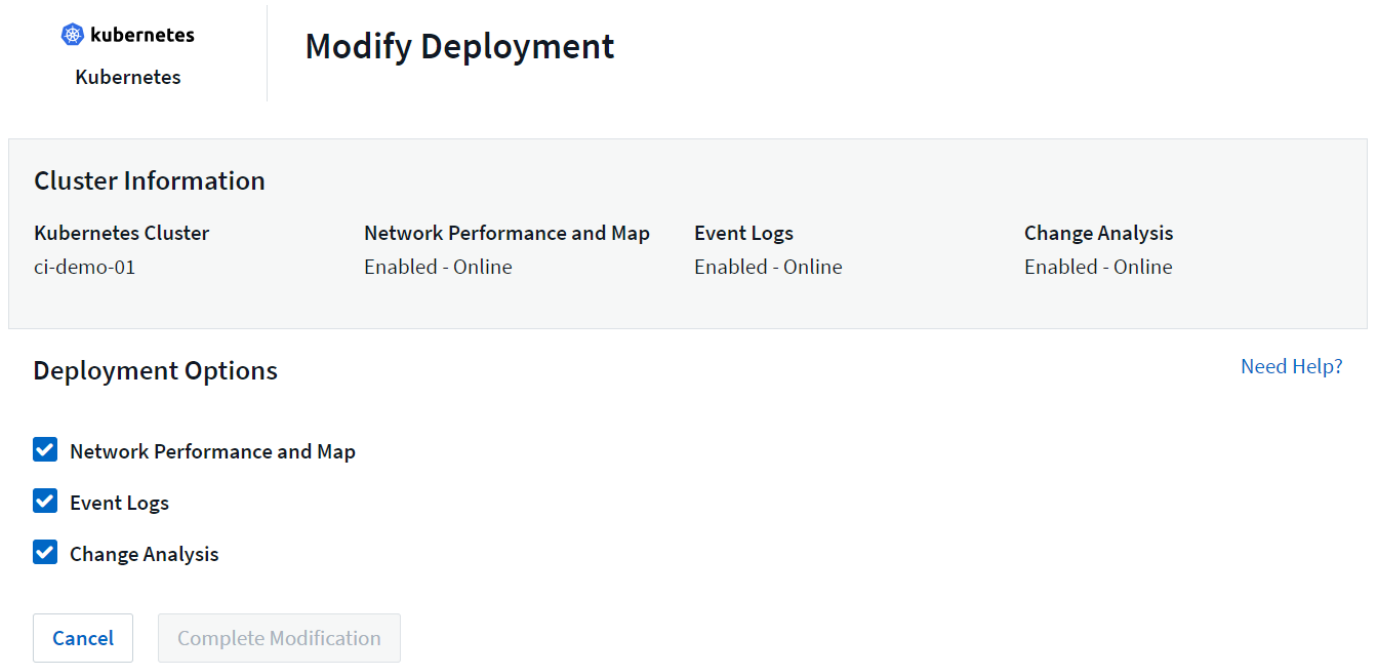
Data Infrastructure Insights Kubernetes Monitoring은 네 가지 모니터링 구성 요소로 구성됩니다.

- 클러스터 메트릭
- 네트워크 성능 및 맵(선택 사항)
- 이벤트 로그(선택 사항)
- 변경 분석(선택 사항)

위의 선택적 구성 요소는 각 Kubernetes 수집기에서 기본적으로 활성화됩니다. 특정 수집기에 대한 구성 요소가 필요하지 않다고 판단되면 *Kubernetes > 수집기*로 이동하여 화면 오른쪽에 있는 수집기의 "세 개의 점" 메뉴에서 _배포 수정_을 선택하여 해당 구성 요소를 비활성화할 수 있습니다.



화면에는 각 구성 요소의 현재 상태가 표시되며 필요에 따라 해당 수집기의 구성 요소를 비활성화하거나 활성화할 수 있습니다.



최신 Kubernetes Monitoring Operator로 업그레이드

DII 푸시 버튼 업그레이드

DII Kubernetes Collectors 페이지를 통해 Kubernetes Monitoring Operator를 업그레이드할 수 있습니다. 업그레이드하려는 클러스터 옆에 있는 메뉴를 클릭하고 _업그레이드_를 선택하세요. 운영자는 이미지 서명을 확인하고, 현재 설치의 스냅샷을 촬영한 후 업그레이드를 수행합니다. 몇 분 안에 운영자 상태가 업그레이드 진행 중에서 최신으로 바뀌는 것을 볼 수 있습니다. 오류가 발생하면 오류 상태를 선택하여 자세한 내용을 확인하고 아래의 푸시 버튼 업그레이드 문제 해결 표를 참조하세요.

개인 저장소를 사용한 푸시 버튼 업그레이드

운영자가 개인 저장소를 사용하도록 구성된 경우 운영자를 실행하는 데 필요한 모든 이미지와 해당 서명이 저장소에서 사용 가능한지 확인하세요. 업그레이드 과정에서 누락된 이미지로 인한 오류가 발생하면 해당 이미지를 저장소에 추가한 후 업그레이드를 다시 시도하세요. 이미지 서명을 저장소에 업로드하려면 다음과 같이 공동 서명 도구를 사용하고 3번 선택 사항에서 지정한 모든 이미지에 대한 서명을 업로드해야 합니다. 운영자 이미지를 개인 저장소에 업로드 > 이미지 풀 스니펫

```
cosign copy example.com/src:v1 example.com/dest:v1
#Example
cosign copy <DII container registry>/netapp-monitoring:<image version>
<private repository>/netapp-monitoring:<image version>
```

이전에 실행 중이던 버전으로 롤백

푸시 버튼 업그레이드 기능을 사용하여 업그레이드한 후 7일 이내에 현재 버전의 운영자를 사용하는 데 어려움이 발생하는 경우, 업그레이드 프로세스 중에 생성된 스냅샷을 사용하여 이전에 실행 중이던 버전으로 다운그레이드할 수 있습니다. 롤백하려는 클러스터 옆에 있는 메뉴를 클릭하고 _롤백_을 선택합니다.

수동 업그레이드

기존 Operator와 함께 _AgentConfiguration_이 존재하는지 확인합니다(네임스페이스가 기본값인 _netapp-monitoring_이 아닌 경우 적절한 네임스페이스로 대체하십시오):

```
 kubectl -n netapp-monitoring get agentconfiguration netapp-ci-monitoring-
configuration
_AgentConfiguration_이 존재하는 경우:
```

- 설치하다기존 연산자보다 최신 연산자가 우선합니다.
  - 당신이 있는지 확인하십시오최신 컨테이너 이미지 가져오기 사용자 정의 저장소를 사용하는 경우.

_AgentConfiguration_이 존재하지 않는 경우:

- Data Infrastructure Insights 에서 인식하는 클러스터 이름을 기록해 두세요(네임스페이스가 기본 netapp-monitoring이 아닌 경우 적절한 네임스페이스로 대체하세요).

```
 kubectl -n netapp-monitoring get agent -o
jsonpath='{.items[0].spec.cluster-name}'
* 기존 Operator의 백업을 만듭니다(네임스페이스가 기본 netapp-monitoring이 아닌 경우
적절한 네임스페이스로 대체).
```

```
 kubectl -n netapp-monitoring get agent -o yaml > agent_backup.yaml
* <<to-remove-the-kubernetes-monitoring-operator,제거>>기존 운영자.
* <<installing-the-kubernetes-monitoring-operator,설치하다>>최신 운영자.
```

- 동일한 클러스터 이름을 사용하세요.
- 최신 Operator YAML 파일을 다운로드한 후 배포하기 전에 _agent_backup.yaml_에서 찾은 모든 사용자 지정 항목을 다운로드한 _operator-config.yaml_로 이식합니다.
- 당신이 있는지 확인하십시오최신 컨테이너 이미지 가져오기 사용자 정의 저장소를 사용하는 경우.

Kubernetes 모니터링 운영자 중지 및 시작

Kubernetes Monitoring Operator를 중지하려면:

```
 kubectl -n netapp-monitoring scale deploy monitoring-operator
--replicas=0
Kubernetes Monitoring Operator를 시작하려면:
```

```
kubectl -n netapp-monitoring scale deploy monitoring-operator --replicas=1
```

제거 중

Kubernetes Monitoring Operator를 제거하려면

Kubernetes Monitoring Operator의 기본 네임스페이스는 "netapp-monitoring"입니다. 고유한 네임스페이스를 설정한 경우 이 명령과 이후의 모든 명령 및 파일에서 해당 네임스페이스를 대체합니다.

다음 명령을 사용하여 모니터링 운영자의 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>
```
참고: 첫 번째 명령에서 "리소스를 찾을 수 없습니다"라는 메시지가 반환되면 다음 지침에 따라 이전 버전의 모니터링 운영자를 제거하세요.

다음 명령을 순서대로 실행하세요. 현재 설치 환경에 따라 일부 명령은 '개체를 찾을 수 없습니다'라는 메시지를 반환할 수 있습니다. 이런 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>
```

이전에 보안 컨텍스트 제약 조건이 생성된 경우:

```
kubectl delete scc telegraf-hostaccess
```

Kube-state-metrics에 대하여

NetApp Kubernetes Monitoring Operator는 다른 인스턴스와의 충돌을 피하기 위해 자체 kube-state-metrics를 설치합니다.

Kube-State-Metrics에 대한 정보는 다음을 참조하세요."이 페이지" .

운영자 구성/사용자 정의

이 섹션에는 운영자 구성 사용자 정의, 프록시 작업, 사용자 정의 또는 개인 Docker 저장소 사용, OpenShift 작업 등에 대한 정보가 포함되어 있습니다.

구성 옵션

가장 일반적으로 수정되는 설정은 *AgentConfiguration* 사용자 정의 리소스에서 구성할 수 있습니다. *operator-config.yaml* 파일을 편집하여 운영자를 배포하기 전에 이 리소스를 편집할 수 있습니다. 이 파일에는 주석 처리된 설정 예가 포함되어 있습니다. 목록을 확인하세요"사용 가능한 설정" 최신 버전의 연산자에 대해서.

다음 명령을 사용하여 운영자가 배포된 후에도 이 리소스를 편집할 수 있습니다.

```
 kubectl -n netapp-monitoring edit AgentConfiguration
```
배포된 운영자 버전이 _AgentConfiguration_을 지원하는지 확인하려면 다음 명령을 실행하십시오:

```
 kubectl get crd agentconfigurations.monitoring.netapp.com
```
"서버 오류(찾을 수 없음)" 메시지가 표시되면 AgentConfiguration을 사용하려면 먼저 운영자를 업그레이드해야 합니다.

프록시 지원 구성

테넌트에 프록시를 사용하여 Kubernetes Monitoring Operator를 설치할 수 있는 두 곳이 있습니다. 이는 동일하거나 별도의 프록시 시스템일 수 있습니다.

- 설치 코드 조각을 실행하는 동안 필요한 프록시("curl" 사용)는 조각이 실행되는 시스템을 Data Infrastructure Insights 환경에 연결합니다.
- 대상 Kubernetes 클러스터가 Data Infrastructure Insights 환경과 통신하는 데 필요한 프록시

이 두 가지 중 하나 또는 둘 다에 프록시를 사용하는 경우 Kubernetes Operating Monitor를 설치하려면 먼저 프록시가 Data Infrastructure Insights 환경과의 원활한 통신을 허용하도록 구성되어 있는지 확인해야 합니다. 프록시가 있고 Operator를 설치하려는 서버/VM에서 Data Infrastructure Insights 에 액세스할 수 있는 경우 프록시가 올바르게 구성된 것일 가능성이 높습니다.

Kubernetes Operating Monitor를 설치하는 데 사용되는 프록시의 경우, Operator를 설치하기 전에 *http_proxy/https_proxy* 환경 변수를 설정하세요. 일부 프록시 환경에서는 _no_proxy 환경 변수를 설정해야 할 수도 있습니다.

변수를 설정하려면 Kubernetes Monitoring Operator를 설치하기 전에 시스템에서 다음 단계를 수행하세요.

1. 현재 사용자에 대해 *https_proxy* 및/또는 *http_proxy* 환경 변수를 설정합니다.
   a. 설정 중인 프록시에 인증(사용자 이름/비밀번호)이 없는 경우 다음 명령을 실행합니다.

```
 export https_proxy=<proxy_server>:<proxy_port>
```
.. 설정 중인 프록시에 인증(사용자 이름/비밀번호)이 있는 경우 다음 명령을 실행하세요.

```
export
http_proxy=<proxy_username>:<proxy_password>@<proxy_server>:<proxy_po
rt>
```

Kubernetes 클러스터가 Data Infrastructure Insights 환경과 통신하는 데 사용되는 프록시의 경우, 이 지침을 모두 읽은 후 Kubernetes Monitoring Operator를 설치하세요.

Kubernetes 모니터링 오퍼레이터를 배포하기 전에 *operator-config.yaml_*의 *_AgentConfiguration* 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 정의 또는 개인 **Docker** 저장소 사용

기본적으로 Kubernetes Monitoring Operator는 Data Infrastructure Insights 저장소에서 컨테이너 이미지를 가져옵니다. 모니터링 대상으로 Kubernetes 클러스터를 사용하고 해당 클러스터가 사용자 정의 또는 개인 Docker 저장소나 컨테이너 레지스트리에서만 컨테이너 이미지를 가져오도록 구성된 경우 Kubernetes Monitoring Operator에 필요한 컨테이너에 대한 액세스를 구성해야 합니다.

NetApp Monitoring Operator 설치 타일에서 "이미지 풀 스니펫"을 실행합니다. 이 명령은 Data Infrastructure Insights 저장소에 로그인하고, 운영자에 대한 모든 이미지 종속성을 끌어오고, Data Infrastructure Insights 저장소에서 로그아웃합니다. 메시지가 표시되면 제공된 저장소 임시 비밀번호를 입력하세요. 이 명령은 옵션 기능을 포함하여 운영자가 사용하는 모든 이미지를 다운로드합니다. 이 이미지가 어떤 기능에 사용되는지 아래에서 확인하세요.

핵심 운영자 기능 및 Kubernetes 모니터링

- 넷앱 모니터링
- ci-kube-rbac-프록시
- ci-ksm
- ci-텔레그라프
- distroless-root-user

이벤트 로그

- ci-fluent-bit
- ci-kubernetes-이벤트-내보내기

네트워크 성능 및 맵

- ci-net-observer

회사 정책에 따라 운영자 Docker 이미지를 개인/로컬/엔터프라이즈 Docker 저장소에 푸시합니다. 저장소에 있는 이미지 태그와 해당 이미지의 디렉토리 경로가 Data Infrastructure Insights 저장소의 이미지 태그와 디렉토리 경로와 일치하는지 확인하세요.

operator-deployment.yaml에서 monitoring-operator 배포를 편집하고 모든 이미지 참조를 수정하여 개인 Docker 저장소를 사용합니다.

```
image: <docker repo of the enterprise/corp docker repo>/ci-kube-rbac-
proxy:<ci-kube-rbac-proxy version>
image: <docker repo of the enterprise/corp docker repo>/netapp-
monitoring:<version>
```

_operator-config.yaml_의 _AgentConfiguration_을 편집하여 새 docker 리포지토리 위치를 반영하세요. 개인 리포지토리에 대한 새 imagePullSecret을 생성하세요. 자세한 내용은 _https://kubernetes.io/docs/tasks/configure-pod-container/pull-image-private-registry/_를 참조하세요.

```
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
```

장기 비밀번호용 **API** 액세스 토큰

일부 환경(예: 프록시 저장소)에는 Data Infrastructure Insights docker 저장소에 대한 장기 암호가 필요합니다. 설치 시 UI에서 제공되는 암호는 24시간 동안만 유효합니다. 이 암호 대신 API 액세스 토큰을 docker 저장소 암호로 사용할 수 있습니다. 이 암호는 API 액세스 토큰이 유효한 동안 유효합니다. 이 용도로 새 API 액세스 토큰을 생성하거나 기존 토큰을 사용할 수 있습니다.

"여기를 읽어보세요" 새 API 액세스 토큰 생성 지침을 참조하십시오.

다운로드한 *operator-secrets.yaml* 파일에서 기존 API 액세스 토큰을 추출하려면 사용자는 다음을 실행할 수 있습니다.

```
grep '\.dockerconfigjson' operator-secrets.yaml |sed 's/.*\.dockerconfigjson:
//g' |base64 -d |jq
```

실행 중인 오퍼레이터 설치에서 기존 API Access Token을 추출하려면 다음 명령을 실행하면 됩니다.

```
kubectl -n netapp-monitoring get secret netapp-ci-docker -o
jsonpath='{.data.\.dockerconfigjson}' |base64 -d |jq
```

OpenShift 지침

OpenShift 4.6 이상 버전을 사용하는 경우, *operator-config.yaml* 파일의 *AgentConfiguration* 설정을 수정하여 *runPrivileged* 설정을 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 추가 보안 수준을 구현할 수 있습니다.

관용과 오염

netapp-ci-telegraf-ds, *netapp-ci-fluent-bit-ds*, 및 *netapp-ci-net-observer-l4-ds* DaemonSets는 모든 노드에서 데이터를 올바르게 수집하기 위해 클러스터의 모든 노드에 Pod를 예약해야 합니다. 해당 운영자는 잘 알려진 몇 가지 *오염*을 허용하도록 구성되었습니다. 노드에서 사용자 정의 오염을 구성하여 모든 노드에서 포드가 실행되지 않도록 한 경우 해당 오염에 대한 *허용*을 생성할 수 있습니다."_AgentConfiguration_에서" . 클러스터의 모든 노드에 사용자 정의 테인을 적용한 경우 운영자 포드를 예약하고 실행할 수 있도록 운영자 배포에 필요한 허용 범위도 추가해야 합니다.

Kubernetes에 대해 자세히 알아보기"오염과 관용" .

로 돌아가기"* NetApp Kubernetes 모니터링 운영자 설치* 페이지"

비밀에 대한 참고 사항

Kubernetes Monitoring Operator가 클러스터 전체의 비밀을 볼 수 있는 권한을 제거하려면 설치하기 전에 *operator-setup.yaml* 파일에서 다음 리소스를 삭제하세요.

```
 ClusterRole/netapp-ci<namespace>-agent-secret
 ClusterRoleBinding/netapp-ci<namespace>-agent-secret
```

업그레이드인 경우 클러스터에서 리소스도 삭제하세요.

```
 kubectl delete ClusterRole/netapp-ci-<namespace>-agent-secret-clusterrole
 kubectl delete ClusterRoleBinding/netapp-ci-<namespace>-agent-secret-
clusterrolebinding
```

변경 분석이 활성화된 경우 *AgentConfiguration* 또는 _operator-config.yaml_을 수정하여 변경 관리 섹션의 주석 처리를 제거하고 변경 관리 섹션 아래에 _kindsToIgnoreFromWatch: '"secrets"'_를 포함합니다. 이 줄에서 작은따옴표와 큰따옴표의 존재와 위치에 주목하세요.

```
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 모니터링 운영자 이미지 서명 확인

운영자의 이미지와 배포하는 모든 관련 이미지는 NetApp 에서 서명합니다. cosign 도구를 사용하여 설치 전에 이미지를 수동으로 검증하거나 Kubernetes 입장 컨트롤러를 구성할 수 있습니다. 자세한 내용은 다음을 참조하세요."쿠버네티스 문서" .

이미지 서명을 확인하는 데 사용되는 공개 키는 선택 사항: 운영자 이미지를 개인 저장소에 업로드 > 이미지 서명 공개 키 아래의 모니터링 운영자 설치 타일에서 사용할 수 있습니다.

이미지 서명을 수동으로 확인하려면 다음 단계를 수행하세요.

1. 이미지 풀 스니펫을 복사하여 실행하세요.
2. 메시지가 표시되면 저장소 비밀번호를 복사하여 입력하세요.
3. 이미지 서명 공개 키(예시에서는 dii-image-signing.pub)를 저장합니다.
4. 공동 서명을 사용하여 이미지를 확인하세요. 다음은 공동 서명 사용의 예입니다.

```
$ cosign verify --key dii-image-signing.pub --insecure-ignore-sct
--insecure-ignore-tlog <repository>/<image>:<tag>
Verification for <repository>/<image>:<tag> --
The following checks were performed on each of these signatures:
  - The cosign claims were validated
  - The signatures were verified against the specified public key
[{"critical":{"identity":{"docker-
reference":"<repository>/<image>"},"image":{"docker-manifest-
digest":"sha256:<hash>"},"type":"cosign container image
signature"},"optional":null}]
```

문제 해결

Kubernetes Monitoring Operator를 설정하는 데 문제가 발생하면 다음을 시도해 보세요.

문제:	다음을 시도해 보세요:
Kubernetes 영구 볼륨과 해당 백엔드 스토리지 장치 사이에 하이퍼링크/연결이 보이지 않습니다. 내 Kubernetes 영구 볼륨은 스토리지 서버의 호스트 이름을 사용하여 구성됩니다.	기존 Telegraf 에이전트를 제거하는 단계를 따른 다음, 최신 Telegraf 에이전트를 다시 설치합니다. Telegraf 버전 2.0 이상을 사용해야 하며, Kubernetes 클러스터 스토리지는 Data Infrastructure Insights 에서 적극적으로 모니터링되어야 합니다.
로그에서 다음과 유사한 메시지가 표시됩니다. E0901 15:21:39.962145 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: *v1.MutatingWebhookConfiguration을 나열하는 데 실패했습니다. 서버가 요청한 리소스를 찾을 수 없습니다. E0901 15:21:43.168161 1 reflector.go:178] k8s.io/kube-state-metrics/internal/store/builder.go:352: *v1.Lease를 나열하는 데 실패했습니다. 서버가 요청한 리소스를 찾을 수 없습니다(get leases.coordination.k8s.io) 등.	Kubernetes 버전이 1.20 미만인 경우 kube-state-metrics 버전 2.0.0 이상을 실행하는 경우 이러한 메시지가 나타날 수 있습니다. Kubernetes 버전을 가져오려면: *kubectl version* kube-state-metrics 버전을 가져오려면: *kubectl get deploy/kube-state-metrics -o jsonpath='{..image}'* 이러한 메시지가 발생하지 않도록 하려면 사용자는 kube-state-metrics 배포를 수정하여 다음 임대를 비활성화할 수 있습니다. *mutatingwebhookconfigurations validatingwebhookconfigurations volumeattachments resources* 보다 구체적으로 다음 CLI 인수를 사용할 수 있습니다. resources=certificatesigningrequests, configmaps, cronjobs, daemonsets, deployments,endpoints,horizontalpodautoscalers, ingresses, jobs, limitranges, namespaces, networkpolicies, nodes, persistentvolumeclaims, persistentvolumes, poddisruptionbudgets, pods,replicasets,replicationcontrollers,resourcequotas , secrets,services,statefulsets,storageclasses 기본 리소스 목록은 다음과 같습니다. "certificatesigningrequests, configmaps, cronjobs, daemonsets, deployments, endpoints, horizontalpodautoscalers, ingresses, jobs, leases, limitranges, mutatingwebhookconfigurations, namespaces, networkpolicies, nodes, persistentvolumeclaims, persistentvolumes, poddisruptionbudgets, pods, replicasets, replicationcontrollers, resourcequotas, secrets, services,statefulsets,storageclasses, validatingwebhookconfigurations,volumeattachments"

문제:	다음을 시도해 보세요:
Telegraf에서 다음과 유사한 오류 메시지가 표시되지만 Telegraf는 시작되고 실행됩니다. 10월 11일 14:23:41 ip-172-31-39-47 systemd[1]: InfluxDB에 메트릭을 보고하기 위한 플러그인 기반 서버 에이전트가 시작되었습니다. 10월 11일 14:23:41 ip-172-31-39-47 telegraf[1827]: time="2021-10-11T14:23:41Z" level=error msg="캐시 디렉토리를 생성하지 못했습니다. /etc/telegraf/.cache/snowflake, err: mkdir /etc/telegraf/.ca che: 권한이 거부되었습니다. 무시되었습니다.\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="열지 못했습니다. 무시됨. open /etc/telegraf/.cache/snowflake/ocsp_response_cache.json: 해당 파일이나 디렉토리가 없습니다.\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 나! Telegraf 1.19.3 시작하기	이는 알려진 문제입니다. 참조하다"이 GitHub 문서" 자세한 내용은. Telegraf가 실행되는 동안 사용자는 이러한 오류 메시지를 무시할 수 있습니다.
Kubernetes에서 Telegraf 포드가 다음 오류를 보고합니다. "마운트 통계 정보 처리 중 오류 발생: 마운트 통계 파일(/hostfs/proc/1/mountstats)을 열 수 없습니다. 오류: /hostfs/proc/1/mountstats를 엽니다. 권한이 거부되었습니다."	SELinux가 활성화되어 있고 적용되어 있는 경우 Telegraf 포드가 Kubernetes 노드의 /proc/1/mountstats 파일에 액세스하지 못할 가능성이 높습니다. 이러한 제한을 극복하려면 에이전트 구성을 편집하고 runPrivileged 설정을 활성화하세요. 자세한 내용은 OpenShift 지침을 참조하세요.
Kubernetes에서 Telegraf ReplicaSet 포드가 다음 오류를 보고합니다. [inputs.prometheus] 플러그인 오류: 키 쌍 /etc/kubernetes/pki/etcd/server.crt:/etc/kubernetes/pki/etcd/server.key를 로드할 수 없습니다. /etc/kubernetes/pki/etcd/server.crt를 엽니다. 해당 파일이나 디렉토리가 없습니다.	Telegraf ReplicaSet 포드는 마스터 또는 etcd로 지정된 노드에서 실행되도록 설계되었습니다. 이러한 노드 중 하나에서 ReplicaSet 포드가 실행되고 있지 않으면 이러한 오류가 발생합니다. 마스터/etcd 노드에 오염이 있는지 확인하세요. 그렇다면 Telegraf ReplicaSet, telegraf-rs에 필요한 허용 범위를 추가합니다. 예를 들어, ReplicaSet을 편집합니다… kubectl edit rs telegraf-rs …그리고 사양에 적절한 허용 범위를 추가합니다. 그런 다음 ReplicaSet 포드를 다시 시작합니다.
저는 PSP/PSA 환경을 사용하고 있습니다. 이것이 모니터링 운영자에게 영향을 미칩니까?	Kubernetes 클러스터가 Pod 보안 정책(PSP) 또는 Pod 보안 승인(PSA)을 적용하여 실행되는 경우 최신 Kubernetes 모니터링 운영자로 업그레이드해야 합니다. PSP/PSA를 지원하는 현재 운영자로 업그레이드하려면 다음 단계를 따르세요. 1. 제거 이전 모니터링 연산자: kubectl delete agent agent-monitoring-netapp -n netapp-monitoring kubectl delete ns netapp-monitoring kubectl delete crd agents.monitoring.netapp.com kubectl delete clusterrole agent-manager-role agent-proxy-role agent-metrics-reader kubectl delete clusterrolebinding agent-manager-rolebinding agent-proxy-rolebinding agent-cluster-admin-rolebinding 2. 설치하다 모니터링 운영자의 최신 버전입니다.

문제:	다음을 시도해 보세요:
Operator를 배포하려고 하다가 문제가 발생했고, PSP/PSA를 사용 중입니다.	1. 다음 명령을 사용하여 에이전트를 편집합니다: kubectl -n <네임스페이스> edit agent 2. 'security-policy-enabled'를 'false'로 표시합니다. 이렇게 하면 Pod 보안 정책과 Pod 보안 입장이 비활성화되고 운영자가 배포할 수 있습니다. 다음 명령을 사용하여 확인하세요. kubectl get psp(Pod 보안 정책이 제거되었음을 표시해야 함) kubectl get all -n <네임스페이스>
grep -i psp(아무것도 발견되지 않았음을 표시해야 함)	"ImagePullBackoff" 오류가 발생했습니다.
이러한 오류는 사용자 지정 또는 개인 Docker 저장소가 있고 Kubernetes Monitoring Operator가 이를 올바르게 인식하도록 아직 구성하지 않은 경우 나타날 수 있습니다. 더 읽어보세요 사용자 정의/개인 저장소 구성에 대한 정보입니다.	모니터링 운영자 배포에 문제가 있는데, 현재 문서에서는 이를 해결하는 데 도움이 되지 않습니다.

다음 명령의 출력을 캡처하거나 기록해 두고 기술 지원팀에 문의하세요.
`kubectl -n netapp-monitoring get all`
`kubectl -n netapp-monitoring describe all`
`kubectl -n netapp-monitoring logs <monitoring-operator-pod> --all-containers=true`
`kubectl -n netapp-monitoring logs <telegraf-pod> --all-containers=true`
	Operator 네임스페이스의 net-observer(워크로드 맵) 포드는 CrashLoopBackOff에 있습니다.

이러한 포드는 네트워크 관찰을 위한 워크로드 맵 데이터 수집기에 해당합니다. 다음을 시도해 보세요. • 포드 중 하나의 로그를 확인하여 최소 커널 버전을 확인하세요. 예: ---- {"ci-tenant-id":"your-tenant-id","collector-cluster":"your-k8s-cluster-name","environment":"prod","level":"error","msg":"유효성 검사에 실패했습니다. 이유: 커널 버전 3.10.0은 최소 커널 버전 4.18.0보다 낮습니다.","time":"2022-11-09T08:23:08Z"} ---- • Net-observer 포드에는 Linux 커널 버전이 최소 4.18.0이어야 합니다. "uname -r" 명령을 사용하여 커널 버전을 확인하고 버전이 4.18.0 이상인지 확인하세요.	Pod는 Operator 네임스페이스(기본값: netapp-monitoring)에서 실행되지만 쿼리의 워크로드 맵이나 Kubernetes 메트릭에 대한 데이터가 UI에 표시되지 않습니다.
K8S 클러스터의 노드에서 시간 설정을 확인하세요. 정확한 감사 및 데이터 보고를 위해서는 NTP(Network Time Protocol) 또는 SNTP(Simple Network Time Protocol)를 사용하여 에이전트 컴퓨터의 시간을 동기화하는 것이 좋습니다.	Operator 네임스페이스의 일부 net-observer 포드가 보류 상태입니다.

문제:	다음을 시도해 보세요:
Net-observer는 DaemonSet이며 k8s 클러스터의 각 노드에서 Pod를 실행합니다. • 보류 상태인 포드를 확인하고 CPU 또는 메모리 리소스 문제가 발생하는지 확인하세요. 노드에서 필요한 메모리와 CPU를 사용할 수 있는지 확인하세요.	Kubernetes Monitoring Operator를 설치한 직후 로그에 다음과 같은 내용이 표시됩니다. [inputs.prometheus] 플러그인 오류: http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics에 대한 HTTP 요청을 만드는 중 오류가 발생했습니다. http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics를 가져옵니다. tcp 다이얼: kube-state-metrics.<namespace>.svc.cluster.local을 조회합니다. 해당 호스트가 없습니다.
이 메시지는 일반적으로 새로운 운영자가 설치되고 *ksm* 포드가 작동하기 전에 *telegraf-rs* 포드가 작동할 때만 나타납니다. 모든 포드가 실행되면 이러한 메시지는 더 이상 표시되지 않습니다.	내 클러스터에 있는 Kubernetes CronJob에 대해 수집된 메트릭이 보이지 않습니다.
Kubernetes 버전을 확인하세요(예: `kubectl version`). v1.20.x 이하인 경우 이는 예상되는 제한 사항입니다. Kubernetes Monitoring Operator와 함께 배포된 kube-state-metrics 릴리스는 v1.CronJob만 지원합니다. Kubernetes 1.20.x 이하에서는 CronJob 리소스가 v1beta.CronJob에 있습니다. 결과적으로 kube-state-metrics는 CronJob 리소스를 찾을 수 없습니다.	운영자를 설치한 후, telegraf-ds 포드가 CrashLoopBackOff에 진입하고 포드 로그에 "su: 인증 실패"가 표시됩니다.
_AgentConfiguration_에서 telegraf 섹션을 편집하고, _dockerMetricCollectionEnabled_를 false로 설정하세요. 자세한 내용은 operator의 "구성 옵션"를 참조하세요. … spec: … telegraf: … - name: docker run-mode: - DaemonSet substitutions: - key: DOCKER_UNIX_SOCK_PLACEHOLDER value: unix:///run/docker.sock … …	Telegraf 로그에서 다음과 유사한 오류 메시지가 반복해서 나타납니다. E! [에이전트] outputs.http에 쓰는 중 오류가 발생했습니다. 게시물 "https://<tenant_url>/rest/v1/lake/ingest/influxdb": 컨텍스트 마감일이 초과되었습니다(헤더를 기다리는 동안 Client.Timeout이 초과되었습니다).
_AgentConfiguration_의 telegraf 섹션을 편집하고 _outputTimeout_을 10초로 늘립니다. 자세한 내용은 운영자에게 문의하세요."구성 옵션" .	일부 이벤트 로그에 대한 *involvedobject* 데이터가 없습니다.
다음 단계를 따랐는지 확인하세요."권한" 위 섹션 참조.	두 개의 모니터링 운영자 포드가 실행 중인 것을 보는 이유는 무엇입니까? 하나는 netapp-ci-monitoring-operator-<pod>이고 다른 하나는 monitoring-operator-<pod>입니다.
2023년 10월 12일부터 Data Infrastructure Insights 사용자에게 더 나은 서비스를 제공하기 위해 운영자를 리팩토링했습니다. 이러한 변경 사항을 완전히 적용하려면 다음을 수행해야 합니다.이전 연산자를 제거하세요 그리고새로운 것을 설치하다 .	내 Kubernetes 이벤트가 예기치 않게 Data Infrastructure Insights 에 보고를 중단했습니다.
이벤트 내보내기 포드의 이름을 검색합니다. `kubectl -n netapp-monitoring get pods`	grep event-exporter

문제:	다음을 시도해 보세요:
awk '{print $1}'	sed 's/event-exporter./event-exporter/'` "netapp-ci-event-exporter" 또는 "event-exporter"여야 합니다. 다음으로 모니터링 에이전트를 편집합니다. `kubectl -n netapp-monitoring edit agent`, 그리고 LOG_FILE의 값을 이전 단계에서 찾은 적절한 이벤트 내보내기 포드 이름을 반영하도록 설정합니다. 보다 구체적으로, LOG_FILE은 "/var/log/containers/netapp-ci-event-exporter.log" 또는 "/var/log/containers/event-exporter*.log"로 설정되어야 합니다. …. fluent-bit: … - name: event-exporter-ci substitutions: - key: LOG_FILE values: - /var/log/containers/netapp-ci-event-exporter*.log … …. 또는 다음도 가능합니다.제거 그리고다시 설치하다 대리인.
Kubernetes Monitoring Operator가 배포한 Pod가 리소스가 부족하여 충돌하는 현상이 발생합니다.	Kubernetes Monitoring Operator를 참조하세요."구성 옵션" 필요에 따라 CPU 및/또는 메모리 한도를 늘립니다.
이미지가 누락되었거나 구성이 잘못되어 netapp-ci-kube-state-metrics 포드가 시작되지 않거나 준비되지 않았습니다. 이제 StatefulSet이 멈춰 있고 구성 변경 사항이 netapp-ci-kube-state-metrics 포드에 적용되지 않습니다.	StatefulSet은 다음과 같습니다."고장난" 상태. 모든 구성 문제를 해결한 후 netapp-ci-kube-state-metrics 포드를 반송합니다.
Kubernetes Operator 업그레이드를 실행한 후 netapp-ci-kube-state-metrics 포드가 시작되지 않고 ErrImagePull(이미지를 가져오는 데 실패) 오류가 발생합니다.	포드를 수동으로 재설정해보세요.
Kubernetes 클러스터의 로그 분석에서 "maxEventAgeSeconds보다 오래되어 이벤트가 삭제되었습니다"라는 메시지가 관찰되었습니다.	Operator *agentconfiguration_*을 수정하고 *_event-exporter-maxEventAgeSeconds*(즉, 60초), *event-exporter-kubeQPS*(즉, 100), *event-exporter-kubeBurst*(즉, 500)를 늘립니다. 이러한 구성 옵션에 대한 자세한 내용은 다음을 참조하세요."구성 옵션" 페이지.
Telegraf는 잠글 수 있는 메모리가 부족하여 경고하거나 충돌합니다.	기본 운영 체제/노드에서 Telegraf의 잠금 가능 메모리 한도를 늘려보세요. 한도를 늘리는 것이 불가능한 경우 NKMO 에이전트 구성을 수정하고 *unprotected_*를 *_true_*로 설정하세요. 이렇게 하면 *Telegraf*는 잠긴 메모리 페이지를 예약하지 않습니다. 복호화된 비밀이 디스크로 옮겨갈 수 있으므로 보안 위험이 발생할 수 있지만, 잠긴 메모리를 예약할 수 없는 환경에서 실행할 수 있습니다. _보호되지 않은 구성 옵션에 대한 자세한 내용은 다음을 참조하세요."구성 옵션" 페이지.

문제:	다음을 시도해 보세요:
Telegraf에서 다음과 유사한 경고 메시지를 보았습니다: _W! [inputs.diskio] "vdc"에 대한 디스크 이름을 수집할 수 없습니다. /dev/vdc를 읽는 중 오류가 발생했습니다. 해당 파일이나 디렉토리가 없습니다.	Kubernetes 모니터링 오퍼레이터의 경우 이러한 경고 메시지는 무해하며 무시해도 됩니다. 또는 AgentConfiguration에서 telegraf 섹션을 편집하고 _runDsPrivileged_를 true로 설정하십시오. 자세한 내용은 "운영자 구성 옵션"을(를) 참조하십시오.

내 fluent-bit pod가 다음 오류로 인해 실패하고 있습니다. [2024/10/16 14:16:23] [오류] [/src/fluent-bit/plugins/in_tail/tail_fs_inotify.c:360 errno=24] 열려 있는 파일이 너무 많습니다. [2024/10/16 14:16:23] [오류] 입력 tail.0을 초기화하지 못했습니다. [2024/10/16 14:16:23] [오류] [엔진] 입력 초기화에 실패했습니다.	클러스터에서 *fsnotify* 설정을 변경해보세요.
	
	`sudo sysctl fs.inotify.max_user_instances (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_instances=<something larger than current setting>`
	
	`sudo sysctl fs.inotify.max_user_watches (take note of setting)`
	
	`sudo sysctl fs.inotify.max_user_watches=<something larger than current setting>`
	
	Fluent-bit를 다시 시작합니다.
	
	참고: 노드 재시작 시에도 이러한 설정을 유지하려면 _/etc/sysctl.conf_에 다음 줄을 넣어야 합니다.
	
	`fs.inotify.max_user_instances=<something larger than current setting>`
	`fs.inotify.max_user_watches=<something larger than current setting>`

문제:	다음을 시도해 보세요:
Telegraf DS Pod는 TLS 인증서의 유효성을 검사할 수 없어 Kubernetes 입력 플러그인이 HTTP 요청을 수행하지 못한다는 오류를 보고하고 있습니다. 예를 들어: E! [inputs.kubernetes] 플러그인 오류: HTTP 요청을 만드는 중 오류가 발생했습니다."<a href="https://<kubelet_IP>:10250/stats/summary":" class="bare">https://<kubelet_IP>:10250/stats/summary": 얻다"<a href="https://<kubelet_IP>:10250/stats/summary":" class="bare">https://<kubelet_IP>:10250/stats/summary": tls: 인증서 확인에 실패했습니다: x509: IP SAN이 포함되어 있지 않으므로 <kubelet_IP>에 대한 인증서를 확인할 수 없습니다.	이는 kubelet이 자체 서명된 인증서를 사용하거나 지정된 인증서에 인증서 *Subject Alternative Name* 목록에 <kubelet_IP>가 포함되지 않은 경우 발생합니다. 이를 해결하려면 사용자가 다음을 수정할 수 있습니다. "에이전트 구성" , _telegraf:insecureK8sSkipVerify_를 _true_로 설정합니다. 이렇게 하면 Telegraf 입력 플러그인이 검증을 건너뛰도록 구성됩니다. 또는 사용자는 kubelet을 구성할 수 있습니다."서버TLS부트스트랩" 그러면 'certificates.k8s.io' API에서 인증서 요청이 트리거됩니다.
Fluent-bit 포드에서 다음과 같은 오류가 발생하고 포드를 시작할 수 없습니다: 026/01/12 20:20:32] [error] [sqldb] error=unable to open database file [2026/01/12 20:20:32] [error] [input:tail:tail.0] db: could not create 'in_tail_files' table [2026/01/12 20:20:32] [error] [input:tail:tail.0] could not open/create database [2026/01/12 20:20:32] [error] failed initialize input tail.0 [2026/01/12 20:20:32] [error] [engine] input initialization failed	DB 파일이 있는 호스트 디렉터리에 적절한 읽기/쓰기 권한이 있는지 확인하십시오. 특히, 호스트 디렉터리는 루트가 아닌 사용자에게 읽기/쓰기 권한을 부여해야 합니다. 기본 DB 파일 위치는 fluent-bit-dbFile *agentconfiguration* 옵션으로 재정의하지 않는 한 /var/log/입니다. SELinux가 활성화된 경우 fluent-bit-seLinuxOptionsType agentconfiguration 옵션을 'spc_t'로 설정해 보십시오.

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지 또는"데이터 수집기 지원 매트릭스" .

Memcached 데이터 수집기

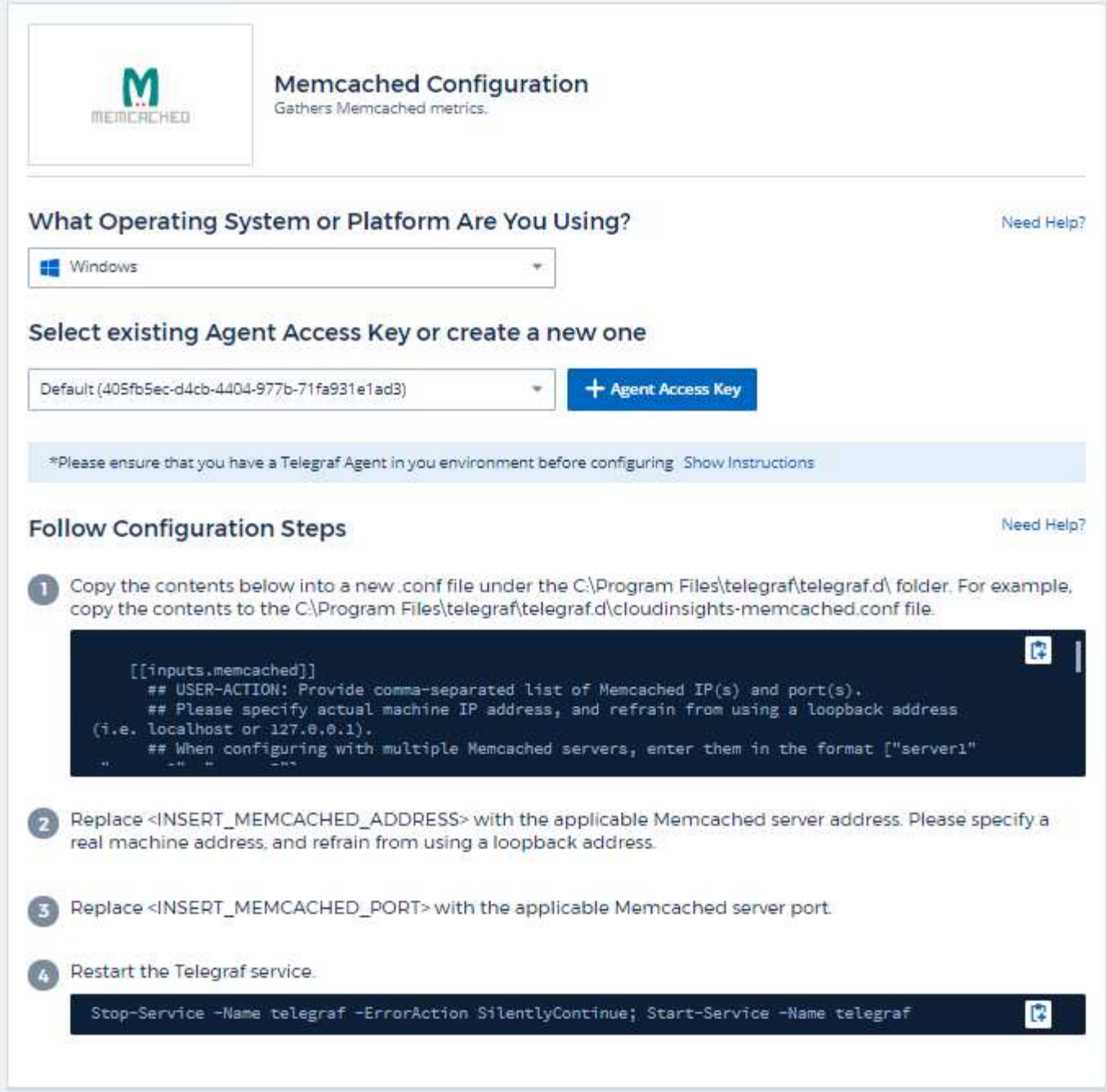
Data Infrastructure Insights 이 데이터 수집기를 사용하여 Memcached에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Memcached를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.



설정

정보는 다음에서 찾을 수 있습니다."Memcached 위키" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
멤캐시드	네임스페이스 서버	노드 IP 노드 이름	연결 수락 처리된 인증 요청 실패한 인증 사용된 바이트 읽은 바이트(초당) 쓴 바이트(초당) CAS Badval CAS Hits CAS Misses 플러시 요청(초당) Get 요청(초당) Set 요청(초당) Touch 요청(초당) 연결 양보(초당) 연결 구조 열린 연결 현재 저장된 항목 Decr 요청 Hits(초당) Decr 요청 Misss(초당) 삭제 요청 Hits(초당) 삭제 요청 Misss(초당) 제거된 항목 유효한 제거 만료된 항목 Get Hits(초당) Get Misss(초당) 사용된 해시 바이트 해시 확장 중 해시 전원 수준 증가 요청 Hits(초당) 증가 요청 Misss(초당) 서버 최대 수신 바이트 비활성화 회수된 작업자 스레드 수 열린 연결 총 저장된 항목 Touch Hits Touch 서버 가동 시간 누락

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

MongoDB 데이터 수집기

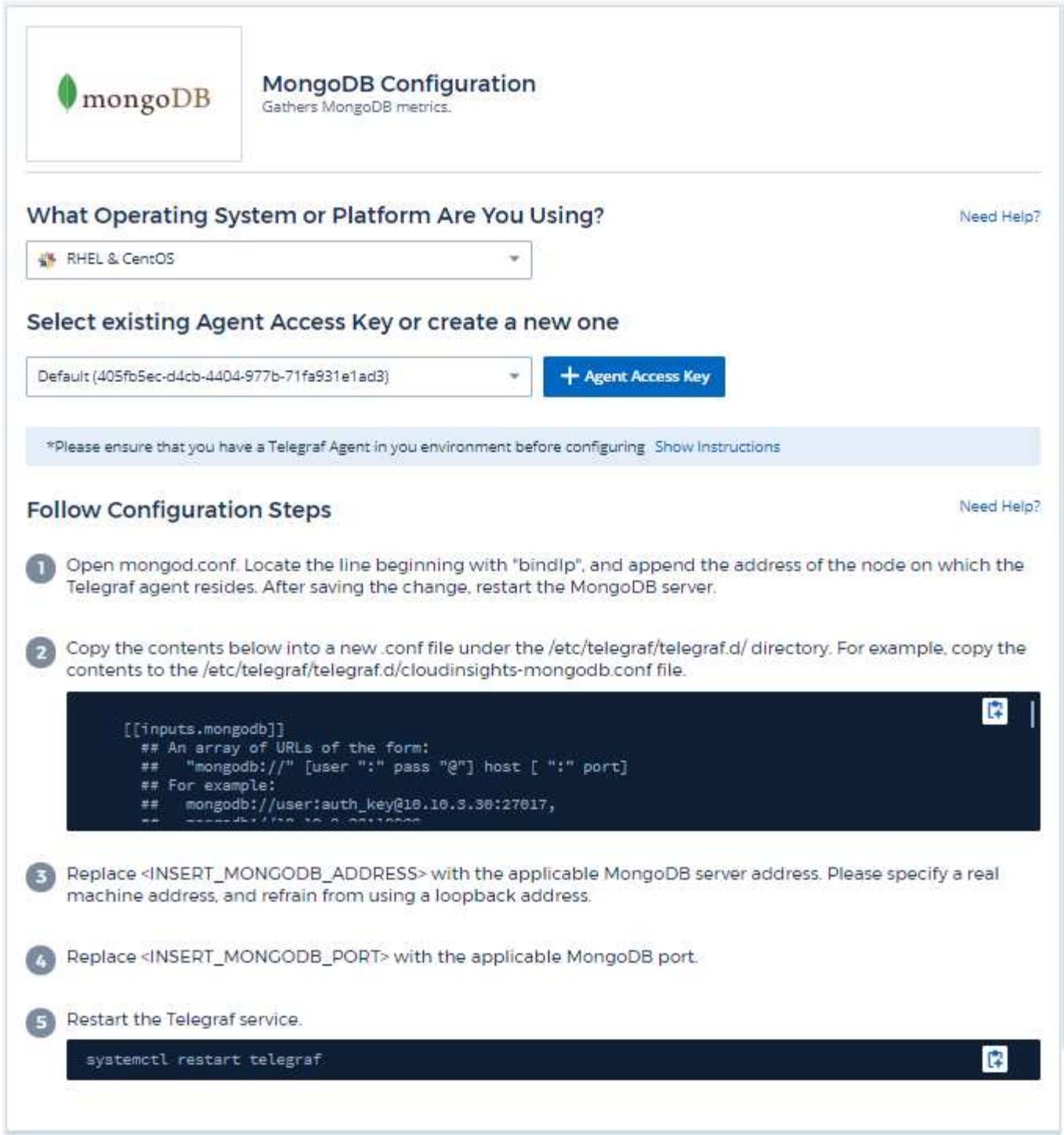
Data Infrastructure Insights 이 데이터 수집기를 사용하여 MongoDB에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. MongoDB를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.



설정

정보는 다음에서 찾을 수 있습니다."MongoDB 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
몽고디비	네임스페이스 호스트 이름		
몽고DB 데이터베이스	네임스페이스 호스트 이름 데이터베이스 이름		

문제 해결

정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

MySQL 데이터 수집기

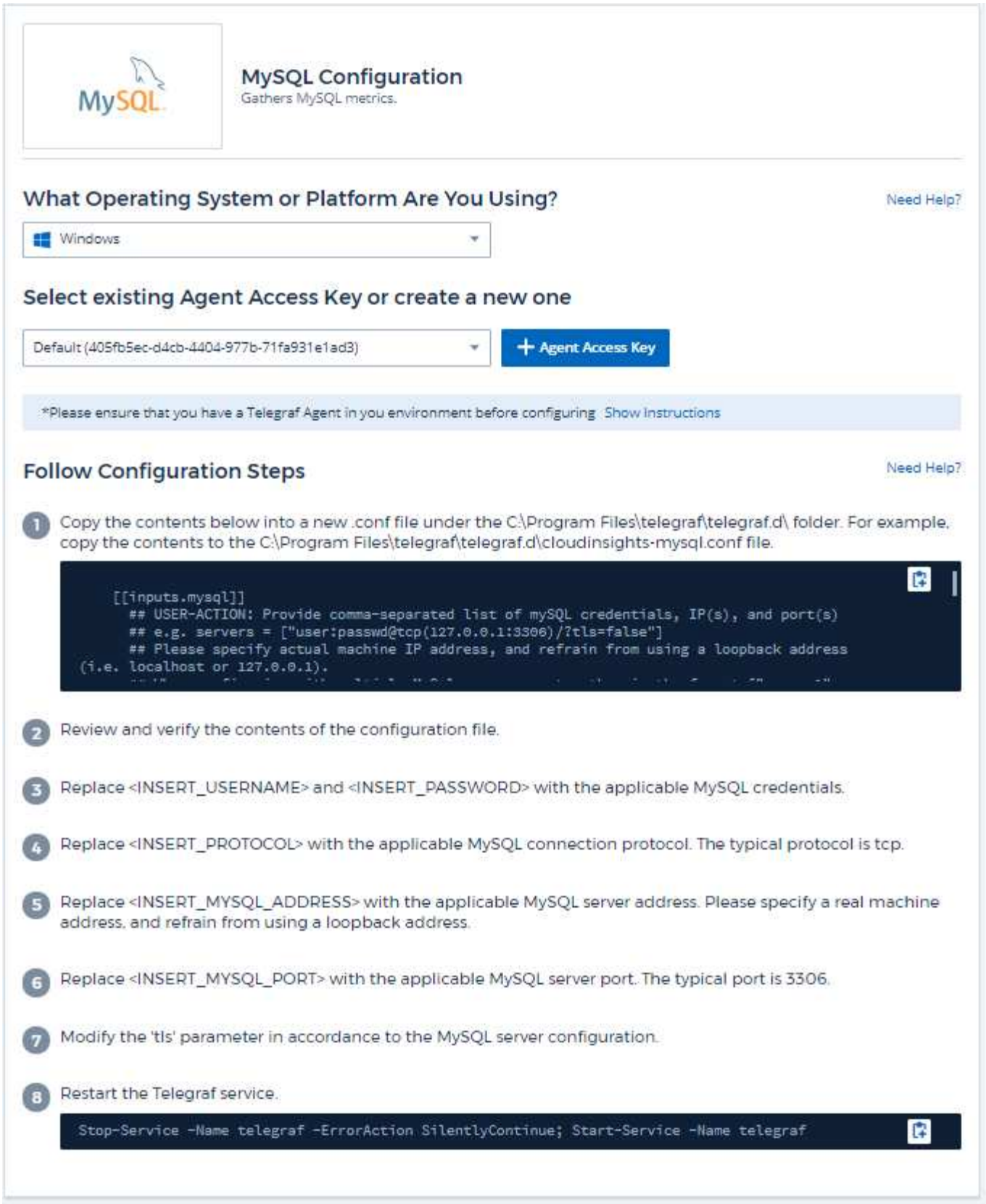
Data Infrastructure Insights 이 데이터 수집기를 사용하여 MySQL에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. MySQL을 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.



설정

정보는 다음에서 찾을 수 있습니다."MySQL 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
MySQL	네임스페이스 MySQL 서버	노드 IP 노드 이름	중단된 클라이언트(초당) 중단된 연결(초당) RX 바이트(초당) TX 바이트(초당) 명령 관리(초당) 명령 이벤트 변경 명령 함수 변경 명령 인스턴스 변경 명령 프로시저 변경 명령 서버 변경 명령 테이블 변경 명령 테이블스페이스 변경 명령 사용자 변경 명령 분석 명령 키 캐시에 할당 명령 시작 명령 Binlog 명령 프로시저 호출 명령 DB 변경 명령 마스터 변경 명령 복제 필터 변경 명령 확인 명령 체크섬 명령 커밋 명령 DB 생성 명령 이벤트 생성 명령 함수 생성 명령 인덱스 생성 명령 프로시저 생성 명령 서버 생성 명령 테이블 생성 명령 트리거 생성 명령 UDF 생성 명령 사용자 생성 명령 뷰 생성 명령 Dealloc SQL 연결 오류 수락 생성된 임시 디스크 테이블 지연 오류 플러시 명령 핸들러 커밋 InnoDB 버퍼 풀 바이트 데이터 키 블록 플러시되지 않음 키 읽기 요청 키 쓰기 요청 키 쓰기 최대 실행 시간 초과 최대 사용 연결 열린 파일 성능 스키마 계정 손실 준비된 문장 수 Qcache 사용 가능한 블록 쿼리 질문 전체 조인 선택 전체 범위 조인 선택 범위 검사 선택 스캔 테이블 잠금 즉시

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Netstat 데이터 수집기

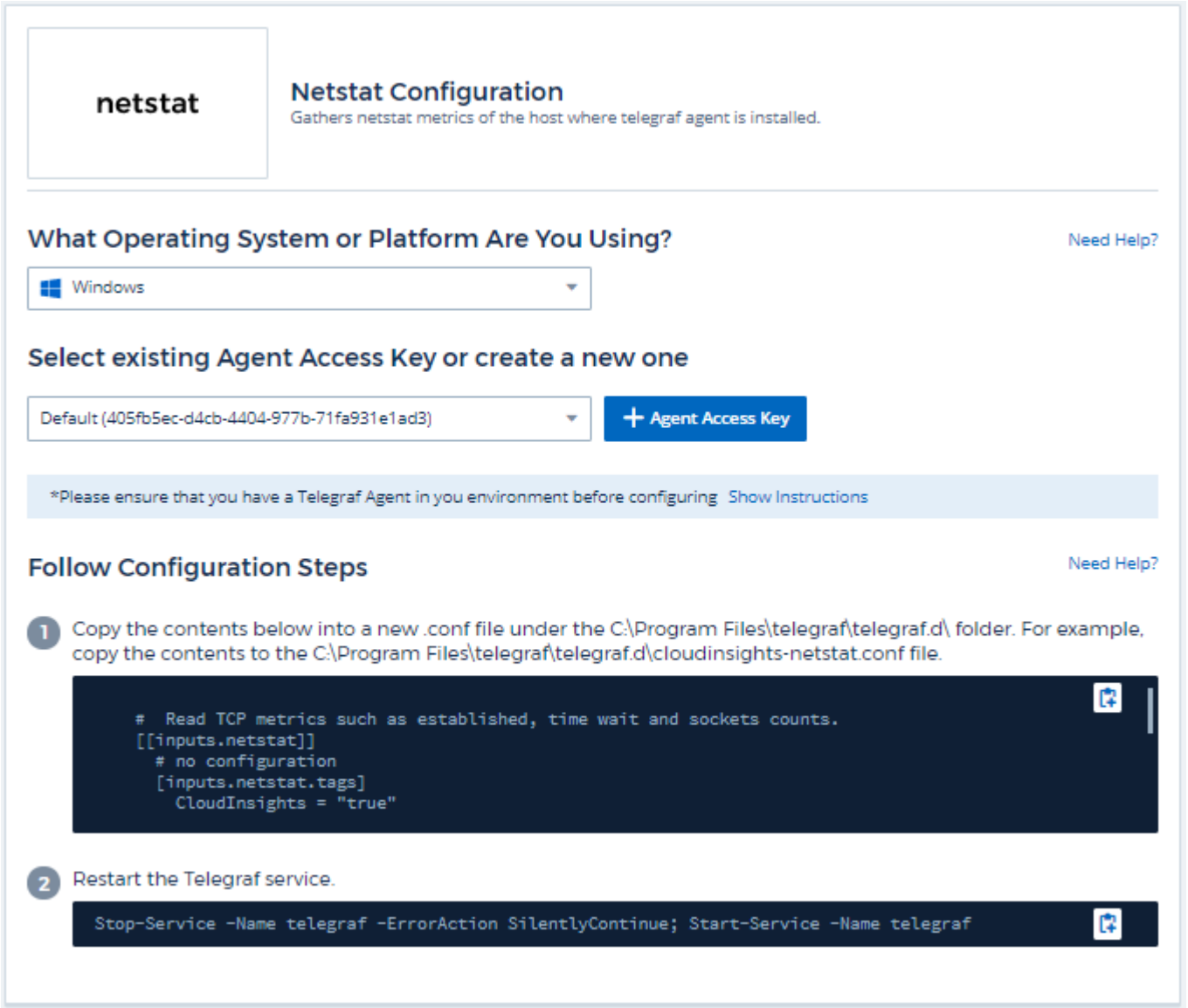
Data Infrastructure Insights 이 데이터 수집기를 사용하여 Netstat 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Netstat을 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.



설정

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
넷스탯	노드 UUID	노드 IP 노드 이름	

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Nginx 데이터 수집기

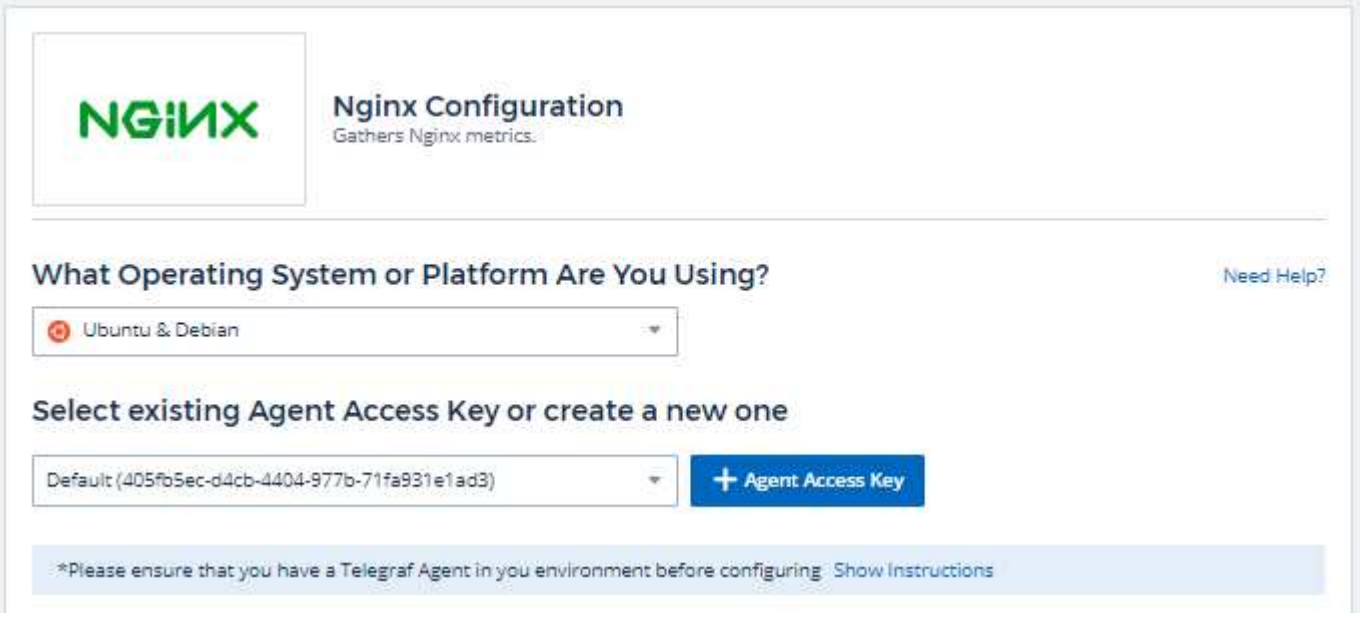
Data Infrastructure Insights 이 데이터 수집기를 사용하여 Nginx에서 지표를 수집합니다.

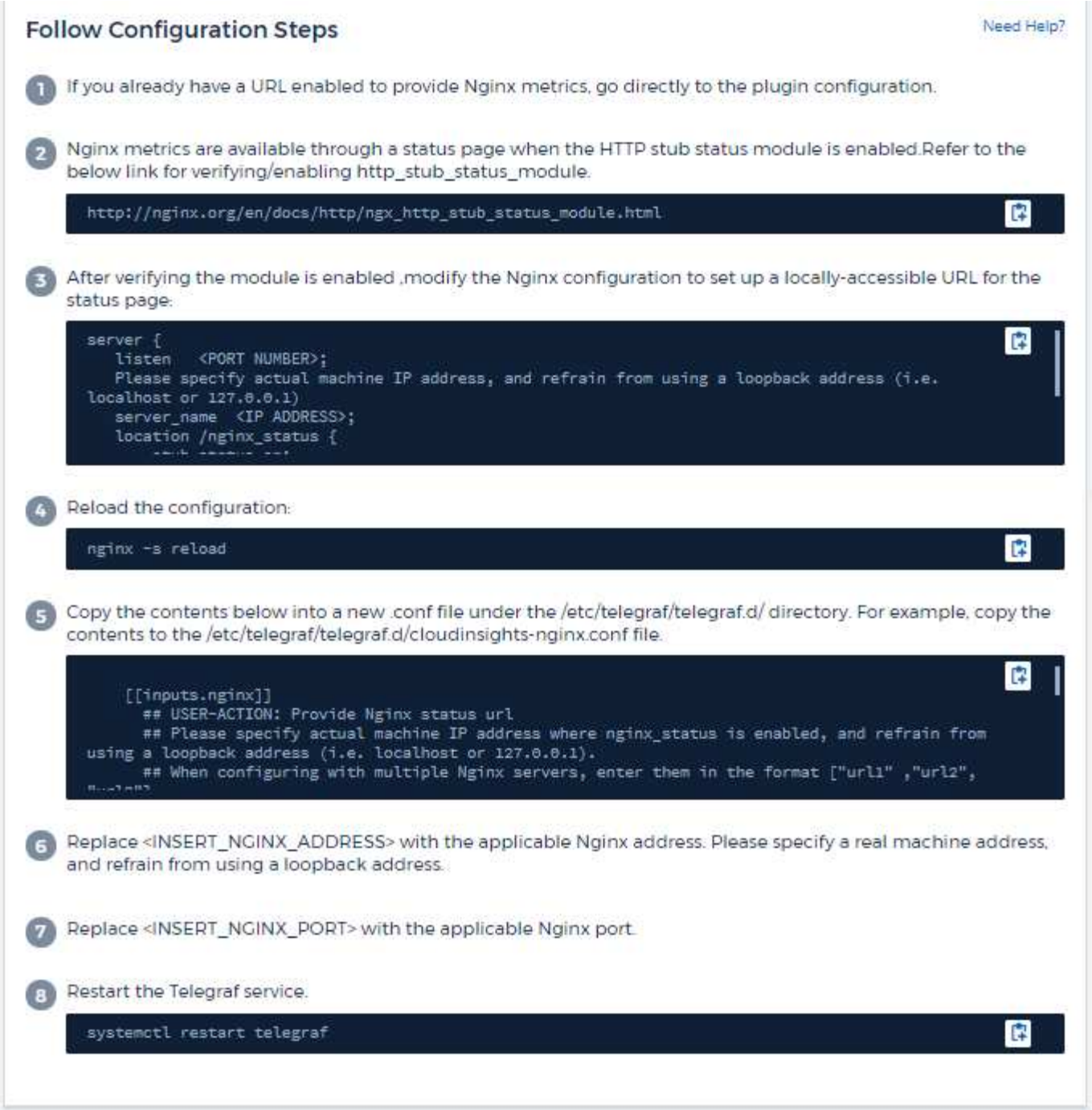
설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Nginx를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. + 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.





설정

Nginx 메트릭 수집에는 Nginx가 필요합니다."http_stub_status_module" 활성화됩니다.

추가 정보는 다음에서 찾을 수 있습니다."Nginx 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
엔진엑스	네임스페이스 서버	노드 IP 노드 이름 포트	활성 처리된 읽기 요청 수락 대기 쓰기

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

PostgreSQL 데이터 수집기

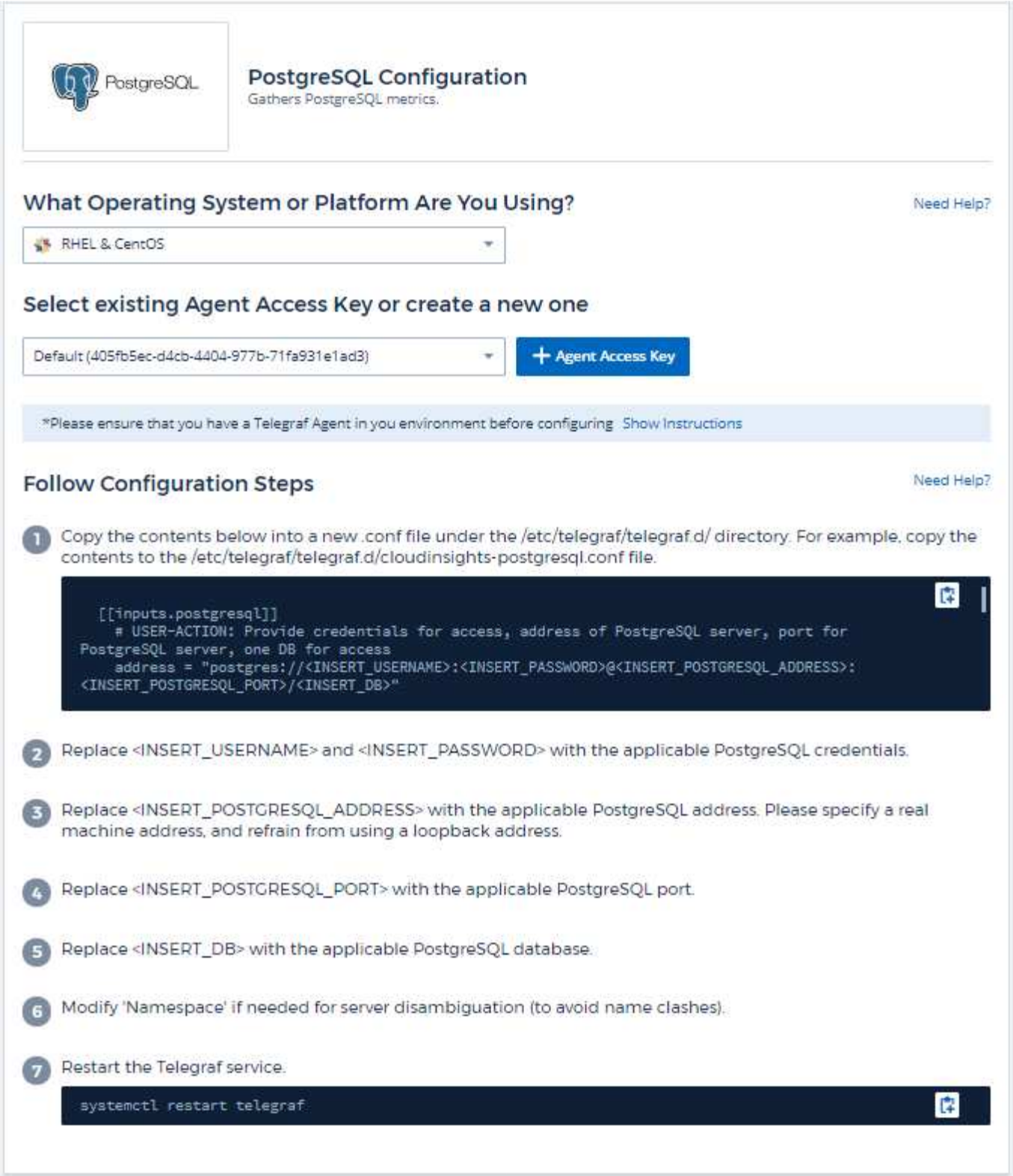
Data Infrastructure Insights 이 데이터 수집기를 사용하여 PostgreSQL에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. PostgreSQL을 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.



설정

정보는 다음에서 찾을 수 있습니다."PostgreSQL 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
PostgreSQL 서버	네임스페이스 데이터베이스 서버	노드 이름 노드 IP	버퍼 할당 버퍼 백엔드 버퍼 백엔드 파일 동기화 버퍼 체크포인트 버퍼 정리 체크포인트 동기화 시간 체크포인트 쓰기 시간 체크포인트 요청 체크포인트 시간 제한 최대 쓰기 정리
PostgreSQL 데이터베이스	네임스페이스 데이터베이스 서버	데이터베이스 OID 노드 이름 노드 IP	블록 읽기 시간 블록 쓰기 시간 블록 히트 블록 읽기 충돌 교착 상태 클라이언트 수 임시 파일 바이트 임시 파일 수 삭제된 행 페치된 행 삽입된 행 반환된 행 업데이트된 트랜잭션 커밋된 트랜잭션 롤백된 트랜잭션

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

퍼펫 에이전트 데이터 수집기

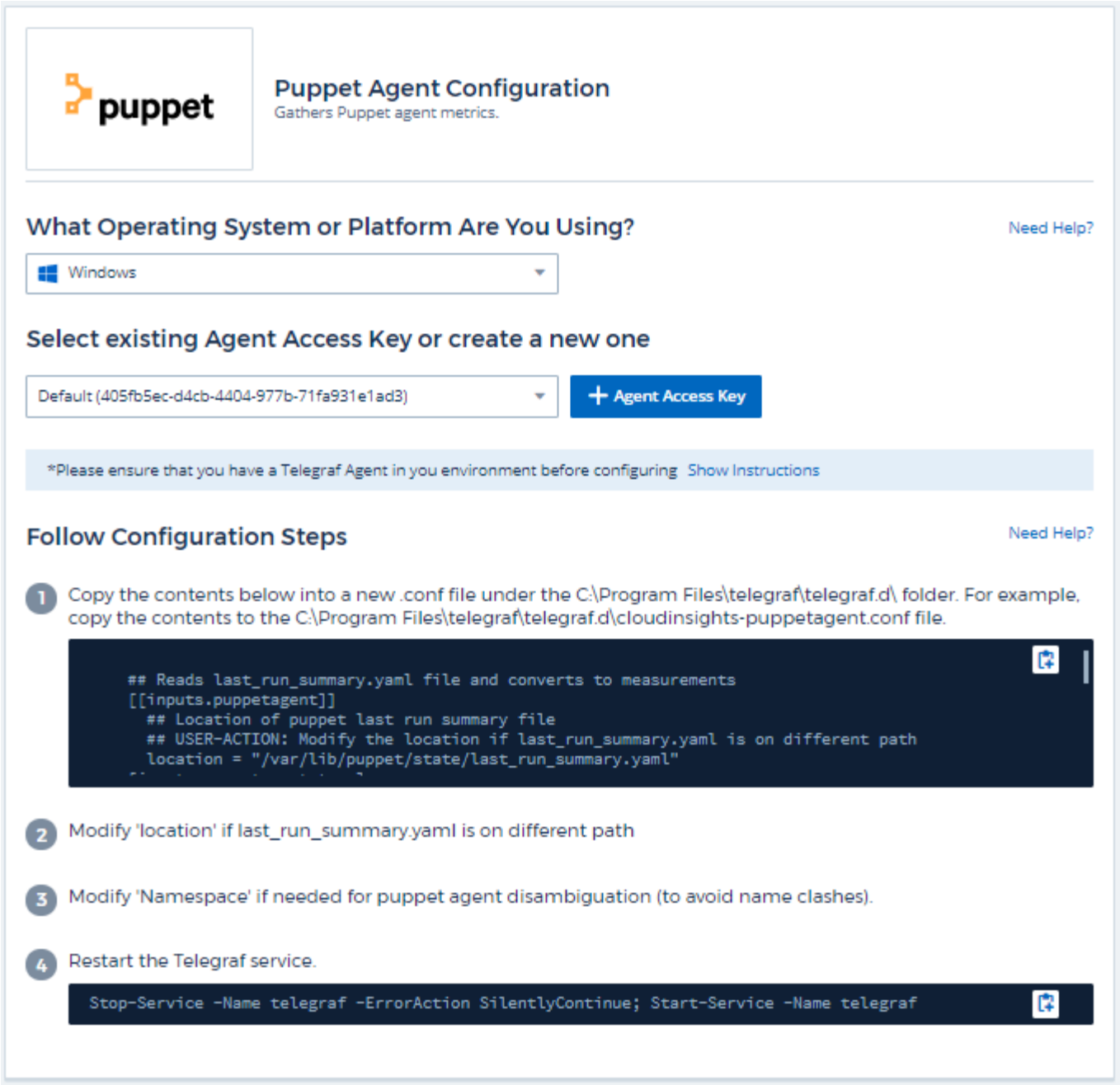
Data Infrastructure Insights 이 데이터 수집기를 사용하여 Puppet Agent에서 지표를 수집합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. 꼭두각시를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.



설정

정보는 다음에서 찾을 수 있습니다. "퍼펫 문서"

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:

퍼펫 에이전트	네임스페이스 노드 UUID	노드 이름 위치 노드 IP 버전 구성 문자열 버전 Puppet	변경 총 이벤트 실패 이벤트 성공 이벤트 총 리소스 변경된 리소스 실패한 리소스 재시작 실패한 리소스 동기화되지 않은 리소스 재시작된 리소스 예약된 리소스 건너뛴 리소스 총 시간 앵커 시간 구성 검색 시간 Cron 시간 실행 시간 파일 시간 Filebucket 시간 Lastrun 시간 패키지 시간 예약 시간 서비스 시간 Sshauthorizedkey 시간 총 시간 사용자

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.

Redis 데이터 수집기

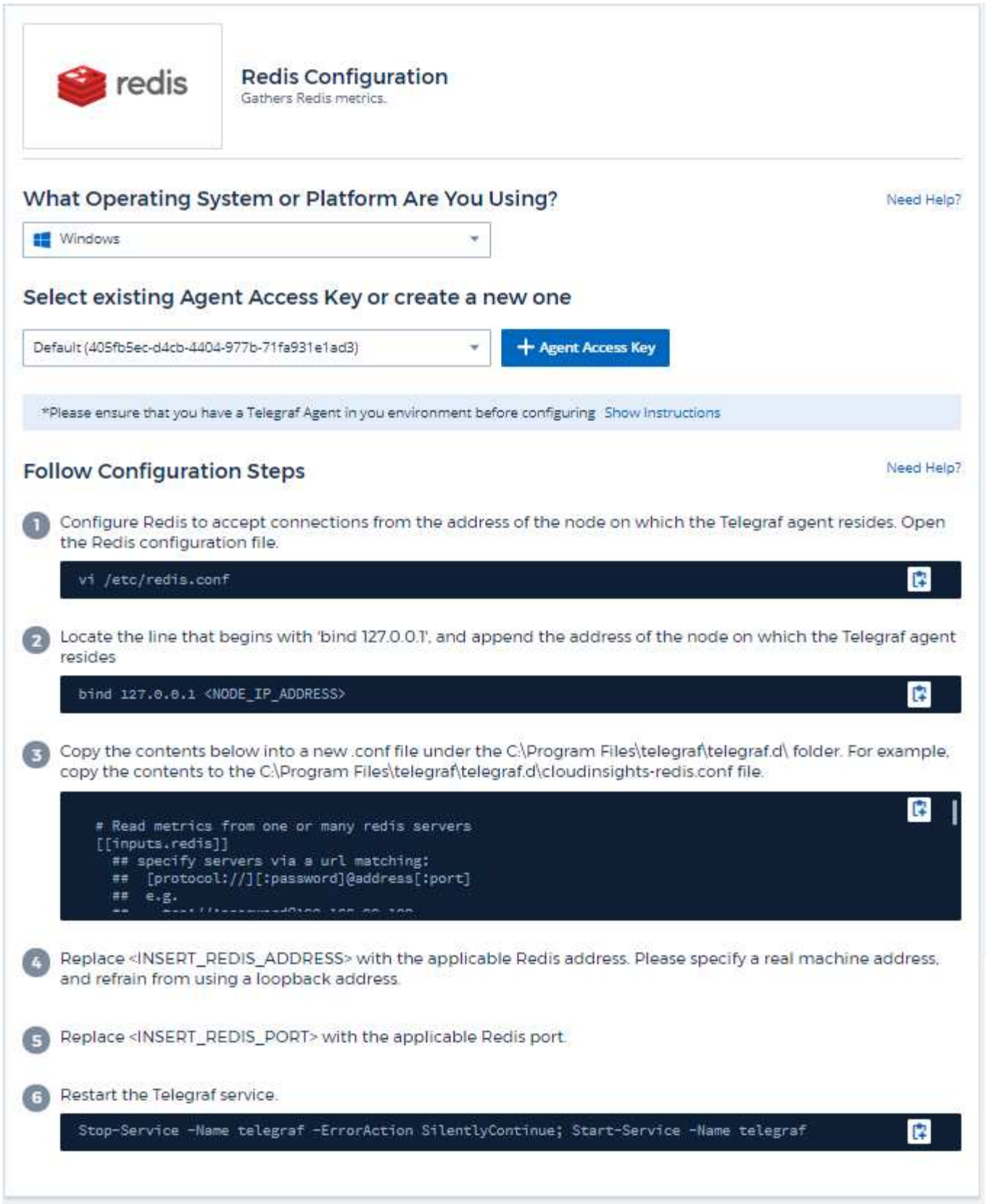
Data Infrastructure Insights 이 데이터 수집기를 사용하여 Redis에서 지표를 수집합니다. Redis는 데이터베이스, 캐시, 메시지 브로커로 사용되는 오픈 소스 인메모리 데이터 구조 저장소로, 문자열, 해시, 목록, 집합 등의 데이터 구조를 지원합니다.

설치

1. *관찰성 > 수집기*에서 *+데이터 수집기*를 클릭합니다. Redis를 선택하세요.

   Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택하세요.

2. 수집을 위한 에이전트를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 에이전트를 설치하려는 경우 _지침 표시_를 클릭하여 확장합니다."에이전트 설치" 지침.
3. 이 데이터 수집기와 함께 사용할 에이전트 액세스 키를 선택하세요. **+** 에이전트 액세스 키 버튼을 클릭하면 새로운 에이전트 액세스 키를 추가할 수 있습니다. 모범 사례: 데이터 수집기를 OS/플랫폼별로 그룹화하려는 경우에만 다른 에이전트 액세스 키를 사용하세요.
4. 데이터 수집기를 구성하려면 구성 단계를 따르세요. 지침은 데이터 수집에 사용하는 운영 체제나 플랫폼의 유형에 따라 다릅니다.



설정

정보는 다음에서 찾을 수 있습니다."Redis 문서" .

객체 및 카운터

다음 객체와 카운터가 수집됩니다.

물체:	식별자:	속성:	데이터 포인트:
레디스	네임스페이스 서버		

문제 해결

추가 정보는 다음에서 찾을 수 있습니다."지원하다" 페이지.