



Data Collector 참조 - 서비스

Data Infrastructure Insights

NetApp
January 10, 2025

목차

Data Collector 참조 - 서비스	1
노드 데이터 수집	1
ActiveMQ 데이터 수집기	3
Apache Data Collector	5
데이터 수집기 영사	8
Couchbase 데이터 수집기	9
Couchbase Data Collector	11
Docker Data Collector 를 참조하십시오	13
Elasticsearch Data Collector(Elasticsearch Data Collector)	19
Flink Data Collector	21
Hadoop Data Collector	26
HAProxy 데이터 수집기	32
JVM 데이터 수집기	37
Kafka 데이터 수집기	40
Kibana 데이터 수집기	43
Kubernetes Monitoring Operator 설치 및 구성	45
Memcached Data Collector	60
MongoDB 데이터 수집기	62
MySQL 데이터 수집기	65
netstat 데이터 수집기	68
Nginx 데이터 수집기	69
PostgreSQL Data Collector	71
Puppet Agent Data Collector	73
Redis Data Collector를 참조하십시오	75

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 객체와 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 OS	수신된 바이트 전송된 바이트 패킷 Outbound 폐기된 패킷 Outbound 오류 수신된 패킷 수신 오류 패킷 수신 패킷 송신 패킷

설정

설정 및 문제 해결 정보는 페이지에서 찾을 ["Agent 구성"](#) 수 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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 페이지에서 찾을 수 ["지원"](#) 있습니다.

Apache Data Collector

이 데이터 수집기는 테넌트의 Apache 서버에서 데이터를 수집할 수 있습니다.

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. 서버 구성 방법에 대한 자세한 내용은 Apache 모듈 설명서를 참조하십시오. 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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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 'od_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
```

'mod_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 유틸 작업자당 총 기간 로드 평균(마지막 1m) 로드 평균(마지막 15m) 로드 평균(마지막 5m) 초당 프로세스 요청 수 총 액세스 총 기간 총 KBScoreytes 보드 폐쇄 점수보드 DNS 조회 점수보드 완료 점수보드 유틸 정리 점수판 유지 점수보드 열기 점수보드 읽기 점수보드 대기 시작 Scoreboard 전송

문제 해결

추가 정보는 페이지에서 찾을 수 ["지원"](#) 있습니다.

데이터 수집기 영사

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Consul에서 메트릭을 수집합니다.

설치

1. 관측성 > 수집기 * 에서 * + Data Collector * 를 클릭합니다. 영사를 선택합니다.

Agent를 수집하도록 구성하지 않은 경우 테넌트에 대한 메시지가 ["에이전트를 설치합니다"](#) 표시됩니다.

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 ["영사 문서"](#) 수 있습니다.

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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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 "Couchbase 설명서"수 있습니다.

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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).

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 "Couchbase DB 문서"수 있습니다.

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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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.

Agent를 수집하도록 구성하지 않은 경우 테넌트에 대한 메시지가 ["에이전트를 설치합니다"](#) 표시됩니다.

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 **Docker**에 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 페이지에서 찾을 수 ["지원"](#) 있습니다.

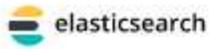
Elasticsearch Data Collector(Elasticsearch Data Collector)

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"[에이전트 설치](#)".
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 "Elasticsearch 문서"수 있습니다.

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:
Elasticsearch Cluster(Elasticsearch 클러스터)	네임스페이스 클러스터	노드 IP 노드 이름 클러스터 상태

오브젝트:	식별자:	특성:
Elasticsearch Node(Elasticsearch 노드)	네임스페이스 클러스터 ES 노드 ID ES 노드 IP ES 노드	영역 ID입니다

문제 해결

추가 정보는 페이지에서 찾을 수 ["지원"](#)있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"["에이전트 설치"](#).
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  
  ##
```

- 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 중입니다

졸로키아 에이전트 용기

모든 개별 구성 요소의 경우 Jolokia 에이전트 JAR 파일 버전을 다운로드해야 합니다. 에 대해 테스트한 버전은 WAS입니다. "[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	클러스터 네임스페이스 작업 ID 작업 ID입니다	서버 노드 이름 작업 이름 하위 작업 인덱스 작업 시도 ID 작업 시도 수 작업 이름 작업 관리자 ID 노드 IP 현재 입력 워터마크	풀 사용 버퍼의 버퍼 대기열 길이 버퍼 아웃 풀 사용 버퍼 아웃 대기열 길이 로컬 수 버퍼의 버퍼 수 로컬/초 단위 버퍼 수 로컬/초 단위 버퍼 수 원격 초당 원격 수 원격 수 버퍼 수 원격 per second의 버퍼 수 두 번째 Rate Number Buffers Out Number Buffers Out per Second Count Number Buffers Out per Second Rate Local Number Bytes in Local Per Second Rate Local Per Second Rate Number Bytes In Remote Number Bytes in Remote Per Second Count Number Number in Remote. Number Bytes In Remote. Number Number Number Bytes In Second. Remote. Number Count Number Bytes in Second 초당 속도 수 바이트 아웃 초당 바이트 수 초당 바이트 수 초당 바이트 수 초당 레코드 수 초당 레코드 수 수 초당 레코드 수 수 수 레코드 수 초당 레코드 수 레코드 수 레코드 수 초당 레코드 수 수 레코드 수 초당 레코드 수 아웃 속도 수

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 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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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.

- 수집용 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"[에이전트 설치](#)".
- 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 WAS입니다. "[졸로키아 에이전트 1.6.0](#)"

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

NameNode입니다

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 NameNode입니다

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.

NodeManager를 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.

JobHistoryServer를 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:
Hadoop 보조 NameNode	클러스터 네임스페이스 서버	노드 이름 노드 IP 컴파일 정보 버전
Hadoop NodeManager를 참조하십시오	클러스터 네임스페이스 서버	노드 이름 노드 IP입니다
Hadoop ResourceManager를 참조하십시오	클러스터 네임스페이스 서버	노드 이름 노드 IP입니다
Hadoop DataNode를 참조하십시오	클러스터 네임스페이스 서버	노드 이름 노드 IP 클러스터 ID 버전
Hadoop NameNode입니다	클러스터 네임스페이스 서버	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
Hadoop JobHistoryServer를 참조하십시오	클러스터 네임스페이스 서버	노드 이름 노드 IP입니다

문제 해결

추가 정보는 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"[에이전트 설치](#)".
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
  ## <url> for the endpoint. ie http://10.10.3.33:1936/haproxy?stats
```

- 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 프런트엔드	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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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 "JVM 설명서"수 있습니다.

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
JVM	네임스페이스 JVM입니다	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 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 시간 가비지 수집기 병렬 배유 컬렉션 수 가비지 수집기 병렬 배유 수집 시간

문제 해결

추가 정보는 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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.
  ## 192.168.1.1 or 127.0.0.1)
```

- 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

Jolokia 에이전트 jar 파일이 있어야 하는 "다운로드되었습니다"버전입니다. 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.password -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:
Kafka 브로커	클러스터 네임스페이스 브로커	노드 이름 노드 IP입니다

문제 해결

추가 정보는 페이지에서 찾을 수 ["지원"](#)있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"[에이전트 설치](#)".
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 `'password'` 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 "Kibana 설명서"수 있습니다.

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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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

"필수 구성 요소" Kubernetes Monitoring Operator를 설치 또는 업그레이드하기 전에 설명서를 참조하십시오.

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
- 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. 이전 Kubernetes 운영자의 경우 **업그레이드 중** 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 대한 자세한 내용을 읽을 수 **"구성 옵션"** 있습니다.
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 **프록시를 구성하는 중**입니다 읽습니다.

사용자 지정 리포지토리가 있는 경우 정보를 **사용자 지정/프라이빗 Docker 저장소 사용** 읽습니다.

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

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

최신 Kubernetes Monitoring Operator로 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 오퍼레이터
 - **최신 컨테이너 이미지를 가져오는 중입니다** 사용자 지정 리포지토리를 사용하고 있는지 확인합니다.

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 오퍼레이터
* <<installing-the-kubernetes-monitoring-operator, 설치합니다>> 최신 연산자.

- 동일한 클러스터 이름을 사용합니다.
- 최신 운영자 YAML 파일을 다운로드한 후 배포하기 전에 agent_backup.YAML에서 발견된 모든 사용자 정의를 다운로드한 operator-config.YAML에 이식하십시오.
- **최신 컨테이너 이미지를 가져오는 중입니다** 사용자 지정 리포지토리를 사용하고 있는지 확인합니다.

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 ["이 페이지"](#)참조하십시오.

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. 최신 버전의 연산자는 의 목록을 ["사용 가능한 설정"](#)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 테넌트에서 프록시를 사용할 수 있는 두 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

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>/ci-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.

톨러러스와 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. 노드에 사용자 지정 테인트를 구성하여 모든 노드에서 Pod가 실행되지 않도록 설정한 경우, 해당 테인트에 대한 * 톨러레이션 * 을 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 "오염과 내약입니다"자세히 알아보십시오.

로 돌아갑니다 "[* NetApp Kubernetes 모니터링 오퍼레이터 설치 * 페이지](#)"

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 `_kindsTolgnoreFromWatch: "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 모니터링 운영자 이미지 서명 확인

운영자의 이미지 및 배포한 모든 관련 이미지는 NetApp에 의해 서명됩니다. Cosign 도구를 사용하여 설치하기 전에 이미지를 수동으로 확인하거나 Kubernetes 승인 컨트롤러를 구성할 수 있습니다. 자세한 내용은 ["Kubernetes 문서" 참조하십시오.](#)

이미지 서명을 확인하는 데 사용되는 공개 키는 `_선택 사항: 운영자 이미지를 개인 저장소에 업로드하십시오.` > 이미지 서명 공개 키 `_`의 모니터링 운영자 설치 파일에서 사용할 수 있습니다

이미지 서명을 수동으로 확인하려면 다음 단계를 수행하십시오.

1. Image Pull Snippet(이미지 가져오기 스니펫)을 복사하여 실행합니다
2. 메시지가 나타나면 리포지토리 암호를 복사하여 입력합니다
3. 이미지 서명 공개 키(예: `dii-image-signing.pub`)를 저장합니다.
4. 코사인을 사용하여 영상을 확인합니다. 다음 코사인 사용 예를 참조하십시오

```
$ 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 발생할 경우 시도해 볼 수 있는 몇 가지 사항은 다음과 같습니다.

<p>문제:</p>	<p>다음을 시도해 보십시오.</p>
<p>Kubernetes 영구 볼륨과 해당 백엔드 스토리지 장치 간의 하이퍼링크/연결이 표시되지 않습니다. 내 Kubernetes 영구 볼륨은 스토리지 서버의 호스트 이름을 사용하여 구성됩니다.</p>	<p>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>
<p>E0901 15:21:39.962145 1 리플렉터.go:178]k8s.io/kube-state-metrics/internal/store/builder.go:352: * v1.목록에 실패했습니다. MutatingWebhookConfiguration: 서버에서 요청된 리소스 E0901 15:21:43.168352.kls.tu2o.tu2352: revm.u2352.u2352.u2o.testimeu2352.u2n.u2352.u2o.u2o.u2352.testime-ve-v</p>	<p>이러한 메시지는 Kubernetes 버전이 1.20 미만인 경우 kube-state-metrics 버전 2.0.0 이상을 실행하는 경우에 발생할 수 있습니다. 쿠버네티스 버전을 얻으려면: <code>_kubctl version_kubbe-state-metrics 버전: _kubectl deploy/kube-state-metrics-o jsonpath='{..image}'</code> 이러한 메시지가 발생하지 않도록 사용자는 kube-state-metrics 구축을 수정하여 다음 Lallase를 비활성화할 수 있습니다. <code>_muthookconfigurations_webhookconfigurrett al_configuredconfig_webvalidateCLI_webvalidateus etausetauseuseuseuseuseuseuse 리소스 = certificationesigningrequests, configmap, crontobs, demonset, 배포, 끝점, 수평 포드자동크기, 링스, 작업, reflodritranges, namespaces, networkpolicies, nistentvolumes, persistentpersistent volumes, podin예산, replicatingfasts, repliceters, replicatingreallets, replicets, replicets, repliceties, replicenets, replicatinggreenets, replicets, replicenets, replicets, service.networksets, service.sets, service.sets, vistenets, visteneties, replicaturies.networksets, service.sets, reseties.networksets, replicaturies, inations, replicaticaturies, replicaturies, replicaturies, inations validingwebhookconfigurations, volumeAttachments"</code></p>
<p>Telegraf의 오류 메시지는 다음과 유사하지만 Telegraf가 시작되고 실행됩니다. Oct 11 14:23:41 IP-172-31-39-47 시스템[1]: 플러그인 기반 서버 에이전트를 시작하여 메트릭을 영향력 있는 xDB에 보고합니다. 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.\n"fc="gosnowflake.(* defaultLogger).Errorf" file="log.go:120" 10월 11:23:41 IP-1118-117-117-117-118-117-117" 오류: 무시되었습니다. open /etc/Telegraf/.cache/snowflake/OCSP_response_cache.json: no that file or directory \n" fc="gosnowflake.(* defaultLogger).Errorf" file="log.Go:120" Oct 11:41 IP-31-39-11:21:114:118-427:114:117-118-114:118-427] 텔레그래프 1.19.3 시작</p>	<p>이는 알려진 문제입니다. "이 GitHub 기사를 참조하십시오" 자세한 내용은 을 참조하십시오. Telegraf가 실행 중인 경우 사용자는 이러한 오류 메시지를 무시할 수 있습니다.</p>

문제:	다음을 시도해 보십시오.
Kubernetes에서 Telegraf 포드가 "mountstats 정보 처리 중 오류: mountstats 파일을 열지 못했습니다. /hostfs/proc/1/mountstats, 오류: open/hostfs/proc/1/mountstats: 사용 권한이 거부되었습니다." 오류를 보고합니다.	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 "OpenShift 지침" 참조하십시오.
Kubernetes에서 Telegraf ReplicaSet Pod가 다음 오류를 보고합니다: inputs.prometheus] [플러그인 오류: keypair /etc/Kubernetes/PKI/etcd/server.crt: /etc/Kubernetes/PKI/etcd/server.key: open /etc/cups/pi/etcd/server.crt: 해당 파일 또는 디렉토리가 없습니다	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, 텔레그라프 ReplicaSet, 텔레그라프-RS에 필요한 내약성을 추가한다. 예를 들어 ReplicaSet...kubtl을 편집하여 RS Telegraf-RS...를 편집하고 사양에 적절한 내약성을 추가합니다. 그런 다음 ReplicaSet 포드를 다시 시작합니다.
PSP/PSA 환경이 있습니다. 이 문제가 모니터링 오퍼레이터에게 영향을 미칩니까?	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 업그레이드합니다. 1. 설치 제거 이전 모니터링 운영자: kubectl delete agent-monitoring-NetApp NetApp-n NetApp-monitoring kubectl delete ns NetApp-monitoring kubectl delete clusterrole agent-manager-proxy-role-metrics-reader-role2 클러스터 바인딩 role2 설치합니다 모니터링 운영자의 최신 버전입니다.
오퍼레이터를 배포하는 데 문제가 발생했고 PSP/PSA를 사용하고 있습니다.	1. kubectl -n <name-space> edit agent 2 명령을 사용하여 에이전트를 편집합니다. '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. kubctl get psp(Pod 보안 정책이 제거되었음을 표시해야 함) kubctl get all-n <namespace>
grep -i psp(아무 것도 찾을 수 없다는 것을 표시해야 함)	"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. 자세히 보기 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> kubect1 -n netapp-monitoring get all kubect1 -n netapp-monitoring describe all kubect1 -n netapp-monitoring logs <monitoring-operator-pod> --all --containers=true kubect1 -n netapp-monitoring logs <telegraf-pod> --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. • 최소 커널 버전을 확인하려면 Pod 중 하나의 로그를 확인하십시오. 예:--{"CI-tenant-id":"your-tenant-id", "collector-cluster":"your-k8s-cluster-name", "environment":"prod", "level":"error", "msg":"가 검증에 실패했습니다. 이유: 커널 버전 3.10.0이 최소 커널 버전 4.18.0", "시간":"2022-11-09T08:23:08Z"}----- • Net-observer Pod는 Linux 커널 버전이 4.18.0 이상이어야 합니다. "uname -r" 명령을 사용하여 커널 버전을 확인하고 해당 버전이 4.18.0 이상인지 확인합니다</p>	<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. • Pending 상태인 POD를 확인하고 CPU 또는 메모리에 대한 리소스 문제가 발생하는지 확인합니다. 노드에서 필요한 메모리 및 CPU를 사용할 수 있는지 확인합니다.</p>	<p>Kubernetes 모니터링 운영자를 설치한 직후 [inputs.prometheus] 오류: 플러그인에서 http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics:get\http://kube-state-metrics.<namespace>.svc.cluster.local:8080/metrics:dial tcp:lookube-state-metrics.<namespace>.svc.no host cluster.local:no.local:no host.local:no.local:no</p>
<p>이 메시지는 일반적으로 새 오퍼레이터가 설치되어 있고 _Telegraf-RS_POD가 _KSM_POD가 가동되기 전에 작동 중일 때만 표시됩니다. 이러한 메시지는 모든 Pod가 실행되면 중지되어야 합니다.</p>	<p>클러스터에 존재하는 Kubernetes CronJobs에 대해 어떤 메트릭도 수집되지 않습니다.</p>

문제:	다음은 시도해 보십시오.
Kubernetes 버전을 확인합니다(예: <code>kubectl version</code>). 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 cronjob 리소스가 v1beta.cronjob에 있습니다. 따라서 kube-state-metrics는 cronjob 리소스를 찾을 수 없습니다.	운영자 설치 후, Telegraf-ds Pod는 CrashLoopBackOff로 진입하고 POD 로그는 "su:Authentication failure"를 나타낸다.
_AgentConfiguration_에서 Telegraf 섹션을 편집하고 _dockerMetricCollectionEnabled_를 false 로 설정합니다. 자세한 내용은 조작자를 "구성 옵션" 참조하십시오. ... 사양 : ... 텔레그라프 : ... -name:docker run-mode: -DemonSet 대체:-key:docker_unix_sock_placeholder 값: unix://run/docker.sock... ...	내 Telegraf 로그에 다음과 유사한 오류 메시지가 반복 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)
_AgentConfiguration_에서 Telegraf 섹션을 편집하고 increase_outputTimeout 을 10초로 편집합니다. 자세한 내용은 조작자를 "구성 옵션" 참조하십시오.	일부 이벤트 로그에 대한 _divedobject_data_가 없습니다.
위 섹션의 단계를 수행했는지 "권한"확인하십시오.	두 개의 모니터링 운영자 Pod가 실행 중인 것을 볼 수 있는데, 하나는 netapp-ci-monitoring-operator- <pod>이고 다른 하나는 monitoring-operator- <pod>입니다.
2023년 10월 12일부터 Data Infrastructure Insights는 사용자에게 더 나은 서비스를 제공하기 위해 운영자를 재고했습니다. 변경 사항을 완전히 채택하려면 반드시 기존 연산자를 제거합니다 AND를 준수해야 합니다.새 장치를 장착하십시오	저의 Kubernetes 이벤트가 예기치 않게 Data Infrastructure Insights에 대한 보고를 중단했습니다.
이벤트 내보내기 포드의 이름을 검색합니다. <pre>`kubectl -n netapp-monitoring get pods`</pre>	grep event-exporter

문제:	다음은 시도해 보십시오.
awk '{print \$1}'	<pre>sed 's/event-exporter./event-exporter/' "netapp-ci-event-exporter" 또는 "event-exporter"여야 합니다. 그런 다음 모니터링 에이전트를 편집하고 kubectl -n netapp-monitoring edit agent 이전 단계에서 찾은 적절한 이벤트 내보내기 포드 이름을 반영하도록 log_file 의 값을 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>fluent-bit:</p> <p>...</p> <p>- name: event-exporter-ci</p> <p>substitutions:</p> <p>- key: LOG_FILE</p> <p>values:</p> <p>- /var/log/containers/netapp-ci-event-exporter.log</p> <p>...</p> <p>....</p> <p>또는 상담원과 다시 설치합니다함께 할 설치 제거수도 있습니다.</p>
리소스 부족으로 인해 Kubernetes Monitoring Operator에 의해 구축된 Pod가 충돌하는 것을 볼 수 있습니다.	필요한 경우 Kubernetes 모니터링 운영자를 "구성 옵션" 참조하여 CPU 및/또는 메모리 한도를 늘리십시오.
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 이 "고장" 상태입니다. 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 "구성 옵션" 페이지를 참조하십시오.
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 <code>set_unprotected_to_true</code> 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. <code>_unprotected_configuration</code> 옵션에 대한 자세한 내용은 "구성 옵션" 페이지를 참조하십시오.

문제:	다음은 시도해 보십시오.
다음과 유사한 Telegraf의 경고 메시지가 표시됩니다. <code>_W! [input.diskio] "vdc"에 대한 디스크 이름을 수집할 수 없습니다. /dev/vdc 읽기 오류: 해당 파일 또는 디렉토리 _</code>	Kubernetes 모니터링 운영자의 경우 이러한 경고 메시지는 양호하며 무시해도 됩니다. 또는 AgentConfiguration에서 Telegraf 섹션을 편집하고 <code>_runDsPrivileged_</code> 를 true로 설정합니다. 자세한 내용은 " 오퍼레이터 구성 옵션 " 참조하십시오.
내 fluent-bit POD가 다음 오류로 인해 실패하고 있습니다. <code>[2024/10/16 14:16:23] [ERROR] [/src/fluent-bit/plugins/in_tail/fs_fs_inotify.c:360 errno=24] 열려 있는 파일이 너무 많습니다. [ERROR</code>	<p>클러스터에서 <code>_fsnotify_settings</code>를 변경해 보십시오.</p> <pre> 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> </pre> <p>Fluent-bit을 다시 시작합니다.</p> <p>참고: 이러한 설정을 노드 재시작 시에도 계속 유지하려면 <code>_/etc/sysctl.conf_</code>에 다음 줄을 입력해야 합니다</p> <pre> fs.inotify.max_user_instances=<something larger than current setting> fs.inotify.max_user_watches=<something larger than current setting> </pre>

추가 정보는 페이지 또는 에서 찾을 ["지원" Data Collector 지원 매트릭스](#) 수 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"에이전트 설치".
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 "멤버시드 위키"수 있습니다.

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
멤버시드	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 페이지에서 찾을 수 "지원"있습니다.

MongoDB 데이터 수집기

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 MongoDB에서 메트릭을 수집합니다.

설치

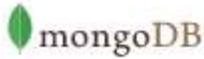
1. 관측성 > 수집기 * 에서 * + Data Collector * 를 클릭합니다. MongoDB를 선택하십시오.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.

2. 수집용 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"[에이전트 설치](#)".

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://10.10.3.30:27017
```

- 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 "MongoDB 설명서" 수 있습니다.

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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"[에이전트 설치](#)".
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 "MySQL 설명서"수 있습니다.

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 플러시 명령 수락 처리기 커밋 InnoDB 버퍼 풀 바이트 데이터 키 블록이 플러시되지 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 페이지에서 찾을 수 ["지원"](#)있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다"에이전트 설치".
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 페이지에서 찾을 수 ["지원"](#) 있습니다.

Nginx 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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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 수집을 사용하려면 Nginx를 사용하도록 설정해야 "`HTTP_STUB_STATUS_MODULE`"합니다.

추가 정보는 에서 찾을 "[Nginx 문서](#)"수 있습니다.

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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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 "PostgreSQL 문서"수 있습니다.

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 페이지에서 찾을 수 ["지원"](#) 있습니다.

Puppet Agent Data Collector

Data Infrastructure Insights는 이 데이터 수집기를 사용하여 Puppet Agent에서 메트릭을 수집합니다.

설치

- 관측성 > 수집기 * 에서 * + Data Collector * 를 클릭합니다. Puppet을 선택합니다.

Telegraf 에이전트가 설치된 운영 체제 또는 플랫폼을 선택합니다.
- 수집용 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
- 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.



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 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 페이지에서 찾을 수 ["지원"](#) 있습니다.

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 Agent를 아직 설치하지 않았거나 다른 운영 체제 또는 플랫폼에 대한 Agent를 설치하려면 지침 표시 를 클릭하여 지침을 확장합니다 ["에이전트 설치"](#).
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://192.168.1.100:6379
```

- 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 "Redis 문서"수 있습니다.

개체 및 카운터

다음 개체와 해당 카운터가 수집됩니다.

오브젝트:	식별자:	특성:	데이터 요소:
레드입니다	네임스페이스 서버		

문제 해결

추가 정보는 페이지에서 찾을 수 ["지원"](#) 있습니다.

저작권 정보

Copyright © 2025 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.