

빅데이터 툴 활용 및 분석방법

2020. 02.

한국지능형사물인터넷협회

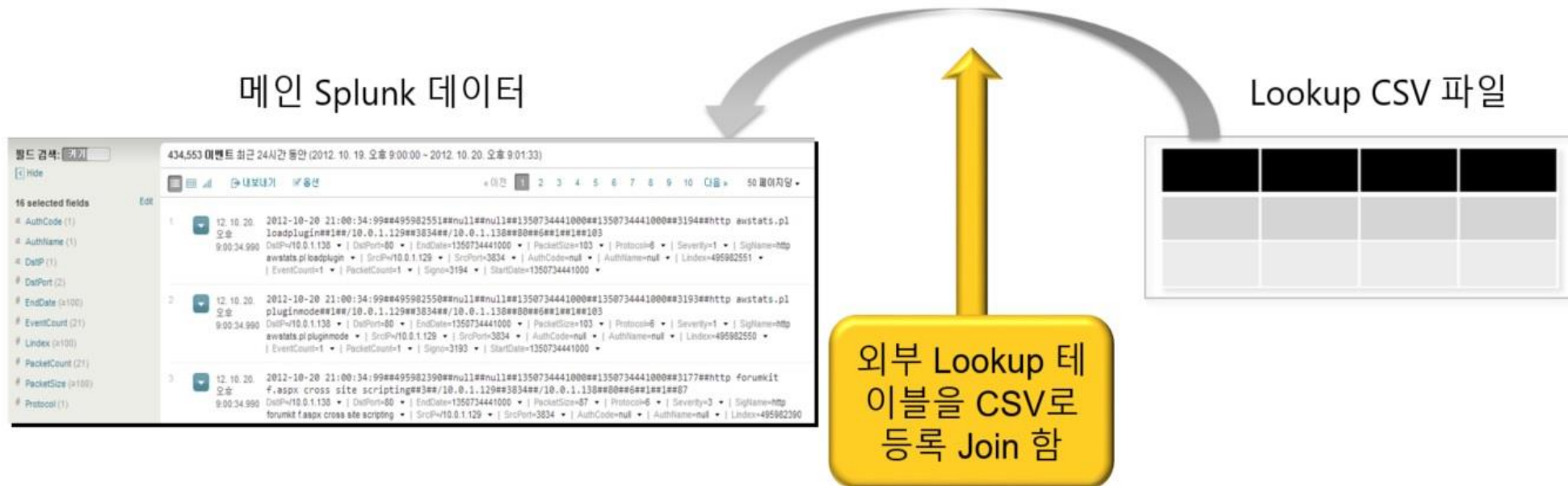
Contents

1. 필드 값 록업
2. 데이터 모델 및 피벗
3. 스프링크 앱
4. 대시보드 만들기

1. 필드 값 룩업

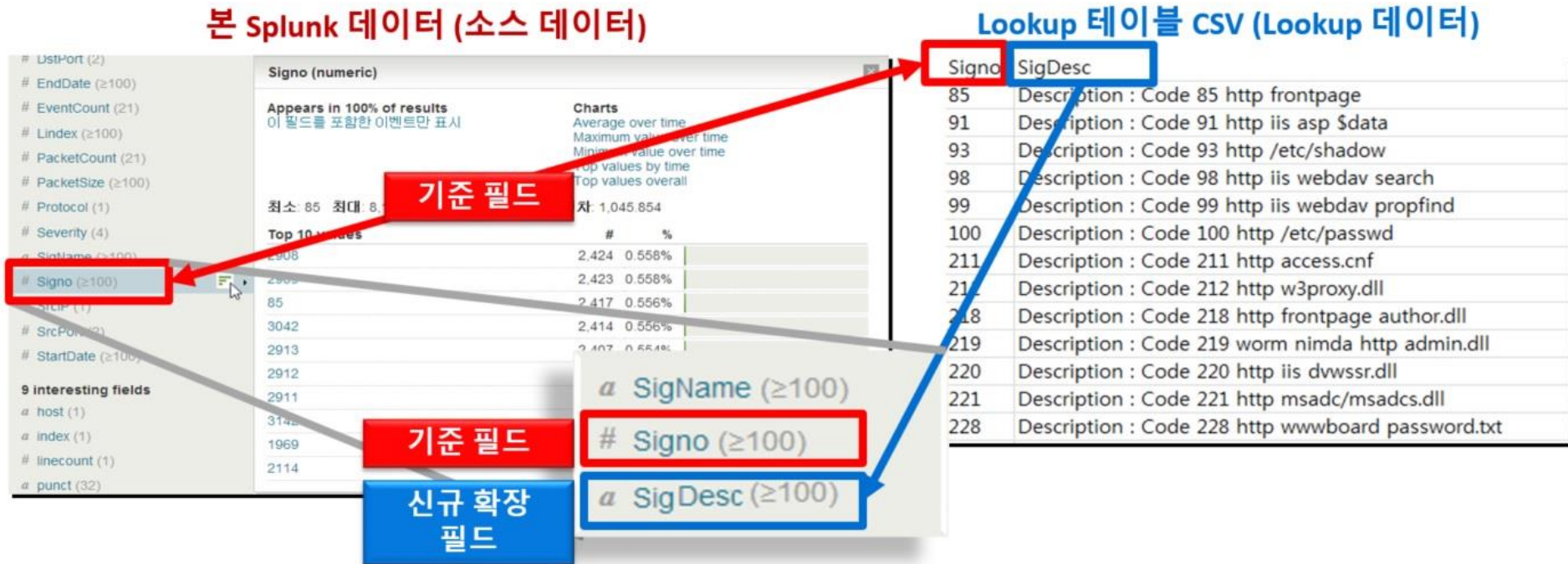
■ 기본 설명 및 예제

- 이벤트 데이터의 필드와 일치하는 필드를 외부 CSV파일에서 참조 할 수 있는 기능
- Splunk에 있는 데이터를 특정 공통적인 필드 기준으로 외부 CSV형태의 Table과 Join 하는 기능
 - 예제1 : Splunk 내의 에러 로그와 외부 에러 코드 설명 확장.
 - 예제2 : 사용자 ID 필드 정보와 사용자 이름, 전화번호, 부서, 성별의 필드 확장.



■ 기본 설명 및 예제

- Splunk내의 Signo라는 필드를 기준으로, 외부 테이블 Signo의 세부 내용 정보 필드를 확장 합니다.



■ 록업 파일 업로드 하기

- 설정 - 록업 - 록업테이블파일 - 새로 추가

■ 록업 관련 명령어

- inputlookup
 - 록업 테이블 전체 데이터 보기
- outputlookup
 - 수집 데이터로 록업 테이블 생성
- lookup
 - 수집 데이터와 록업 테이블 조인

■ Lookup 명령어 사용 예

- inputlookup

시간 설정 요구되지 않음

파이프 라인으로 시작

전체 시간

록업 파일 명

The screenshot shows the Splunk search interface. The search bar contains the command `inputlookup geo_attr_countries.csv`. The search results show 255 results. The results table has columns: continent, country, iso2, iso3, region_un, region_wb, and subregion. The first few rows of the table are:

continent	country	iso2	iso3	region_un	region_wb	subregion
North America	Aruba	AW	ABW	Americas	Latin America & Caribbean	Caribbean
Asia	Afghanistan	AF	AFG	Asia	South Asia	Southern Asia
Africa	Angola	AO	AGO	Africa	Sub-Saharan Africa	Middle Africa
North America	Anguilla	AI	AIA	Americas	Latin America & Caribbean	Caribbean
Europe	Albania	AL	ALB	Europe	Europe & Central Asia	Southern Europe
Oceania	American Samoa	AS	ASM	Oceania	East Asia & Pacific	Polynesia

| inputlookup geo_attr_countries.csv

■ Lookup 명령어 사용 예

- outputlookup

룩업 테이블로 만들고 싶은 검색 수행

The screenshot shows the Splunk Search interface. The search bar contains the query: `index=* | bucket _time span=1h | stats count by sourcetype _time | stats avg(count) as avg by sourcetype | outputlookup avg.csv`. A red box highlights the entire query, and another red box highlights the `outputlookup avg.csv` command. Red arrows point from the explanatory text to these boxes.

Below the search bar, the results are displayed in a table. The table has two columns: `sourcetype` and `avg`. The data is as follows:

sourcetype	avg
audittrail	429.272727
first_install-too_small	4.000000
kvstore	189.428571
mongod	83.000000
scheduler	3.000000
splunk_disk_objects	65.142857
splunk_migration	1.000000

Index=* | bucket _time span=1h | stats count by sourcetype _time | stats avg(count) as avg by sourcetype | outputlookup avg.csv

■ Lookup 명령어 사용 예

- lookup

새로운 검색

index=_* | stats count by sourcetype | lookup avg.csv sourcetype OUTPUT avg as avg_cnt | where count > avg_cnt

다른 이름으로 저장 ▾ 닫기

✓ 13,011 개 이벤트 (17/02/15 15:56:00.000 ~ 17/02/15 16:56:04.000) 이벤트 샘플링 없음 ▾

이벤트 패턴 통계 (4) 시각화

페이지당 20개 ▾ 형식 ▾ 미리보기 ▾

sourcetype ▾	count ▾	avg_cnt ▾
kvstore	211	192.428571
splunk_disk_objects	72	66.857143
splunk_resource_usage	2944	2672.285714
splunkd	7934	6313.647059

조인 대상 룩업 파일 명

조인 키

불러올 필드명

```
Index=_* | stats count by sourcetype | lookup avg.csv sourcetype OUTPUT avg as avg_cnt  
| where count > avg_cnt
```

■ 기본 설명

- 룩업 설정의 3가지 절차
 - 룩업 테이블 파일
 - 기존 룩업 테이블을 나열하거나 새 파일을 업로드
 - 룩업 정의
 - 특정 이벤트에 대하여 룩업을 적용하거나 편집
 - 자동 룩업
 - 특정 이벤트에 대하여 룩업 명령어(lookup) 없이, 호출 시 적용되는 필드 자동화를 적용하거나 편집

■ 룩업 파일 업로드 하기

- 설정 - 룩업 - 룩업테이블 파일 - 새로 추가

■ 자동 룩업 : 검색 시 해당 데이터에 모두 자동으로 룩업 테이블 적용

- 룩업 테이블 파일
 - Lookup 파일을 업로드
- 룩업 정의
 - Lookup 정책 등록
- 자동 lookup
 - 특정 Sourcetype에 대하여 호출 시 lookup 명령어 없이도 적용 필드가 자동 연결되도록 설정

룩업

룩업을 만들고 설정합니다.

룩업 테이블 파일

기존 룩업 테이블을 나열하거나 새 파일을 업로드합니다.

룩업 정의

기존 룩업 정의를 편집하거나 새 파일 기반 또는 외부 룩업을 정의합니다.

자동 룩업

기존 자동 룩업을 편집하거나 자동으로 실행할 새 룩업을 설정합니다.

자동 룩업 설정

kr_product_name 필드 불러오기

■ Step 1: Lookup 파일 등록

- Splunk 데이터와 JOIN할 외부 데이터 테이블 파일을 등록
 - product_kr.csv라는 파일을 Splunk내에 업로드 하여 product_kr.csv라는 Lookup Table 명으로 등록합니다.
 - 업로드 파일은 CSV 나 CSV를 gzip으로 압축한 파일을 사용할 수 있습니다.
 - 이후 등록 되면 해당 Lookup 자원을 권한을 눌러 “전역”으로 공유 합니다.

새로 추가
룩업 > 룩업 테이블 파일 > 새로 추가

대상 앱 search

룩업 파일 업로드 product_kr.csv

일반 텍스트 CSV 파일, gzip된 CSV 파일 또는 KMZ/KML 파일을 선택하십시오.
브라우저를 통해 업로드할 수 있는 최대 파일 크기는 500MB입니다.

대상 파일 이름 * product_kr.csv

Splunk 서버에서 이 룩업 테이블 파일의 이름을 입력하십시오. gzip된 CSV 파일을 업로드하는 경우 ".gz"로 끝나는 파일 이름을 입력하십시오. 일반 텍스트 CSV 파일을 업로드하는 경우 ".csv"로 끝나는 파일 이름을 사용하는 것이 좋습니다. KMZ/KML 파일의 경우 ".kmz"/".kml"로 끝나는 파일 이름을 사용하는 것이 좋습니다.

C:\Program Files\Splunk\etc\apps\search\lookups\product_kr.csv

admin

search

전역 | 권한

자동 룩업 설정

kr_product_name 필드 불러오기

■ Step 2: Lookup 정의

- 업로드한 외부 파일로 Splunk에서 사용할 Lookup 정책 등록
 - product_kr이란 이름으로 데이터 조회 정책을 만들고 Step 1에서 업로드 한 “product_kr.csv”라는 Lookup Table 과의 연관성을 정의.
 - 이후 등록이 완료되면 해당 Lookup 자원의 권한을 눌러 “전역”으로 공유 합니다.

새로 추가
[룩업](#) > [룩업 정의](#) > 새로 추가

대상 앱

Name *

유형

룩업 파일 *

[룩업 테이블 파일을 만들고 관리합니다.](#)

☐ 시간 기반 룩업 설정

☐ 고급 옵션

productId,kr_product_name,kr_price,kr_tdf_price,kr_call_flwrs_price

product_kr.csv

admin

search

전역 | 권한

자동 룩업 설정

kr_product_name 필드 불러오기

■ Step 3 : 특정 Sourcetype 에 자동 필드 호출

- 정의된 Lookup Table을 사용하여 자동으로 필드 JOIN
 - Step 2에서 적용한 “product_kr”라는 Lookup Table을 사용하여 조인할 대상 sourcetype을 **access_combined_wcookie**로 지정하고, 공통 필드인 productId를 기준으로 조인하여, Product Name 필드를 가져와 확장하도록 설정 합니다.
 - 이후 등록 되면 해당 Lookup 자원을 권한을 눌러 “전역”으로 공유 합니다.

새로 추가
룩업 > 자동 룩업 > 새로 추가

대상 앱	search		
Name *	product_kr		
룩업 테이블 *	product_kr		
적용 대상	sourcetype	값 *	access_combined_wcookie
룩업 입력 필드	productId	=	<div>삭제</div>
<div>+ 다른 필드 추가</div>			
룩업 출력 필드	kr_product_name	=	<div>삭제</div>
<div>+ 다른 필드 추가</div>			
<input checked="" type="checkbox"/> 필드 값 덮어쓰기			

취소

저장

자동 룩업 설정

kr_product_name 필드 불러오기

■ Step 4 : 자동 lookup의 결과 확인

- 정의된 Lookup Table을 확인
 - index="tutorialdata" sourcetype=access_combined_wcookie

The screenshot shows the Splunk interface with a list of fields on the left and a detailed view of the 'kr_product_name' field on the right. The 'kr_product_name' field is highlighted in the list, and its configuration is shown in a modal window. The modal window displays the field name, a description, and a table of the top 10 products.

Field List (Left):

- # date_year 1
- a date_zone 1
- a file 14
- a ident 1
- a index 1
- a itemId 14
- a JSESSIONID 100+
- a kr_product_name 10
- # linecount 1
- a method 2
- # other 100+
- a productId 16
- a punct 98
- a referer 100+
- a referer_domain 4
- a req_time 100+
- a splunk_server 1
- # status 9
- # timeendpos 7
- # timestartpos 7
- a uri 100+

Field Configuration Modal (Right):

kr_product_name

10 값, 50.395% 이벤트

보고서

상위 값 시간별 상위 값 희귀 값

이 필드가 있는 이벤트

상위 10개 값	개수	%
틀립 부케	2,325	11.67%
믹스 장비 부케	2,278	11.434%
달콤한 부케	2,250	11.294%
빨간 장비	2,052	10.3%
생일 부케	1,974	9.909%
달콤한 꿈 부케	1,942	9.748%
케이크 서빙 세트	1,897	9.522%
계절 과일 바구니	1,813	9.1%
초코릭 고백 쿠키	1,766	8.864%

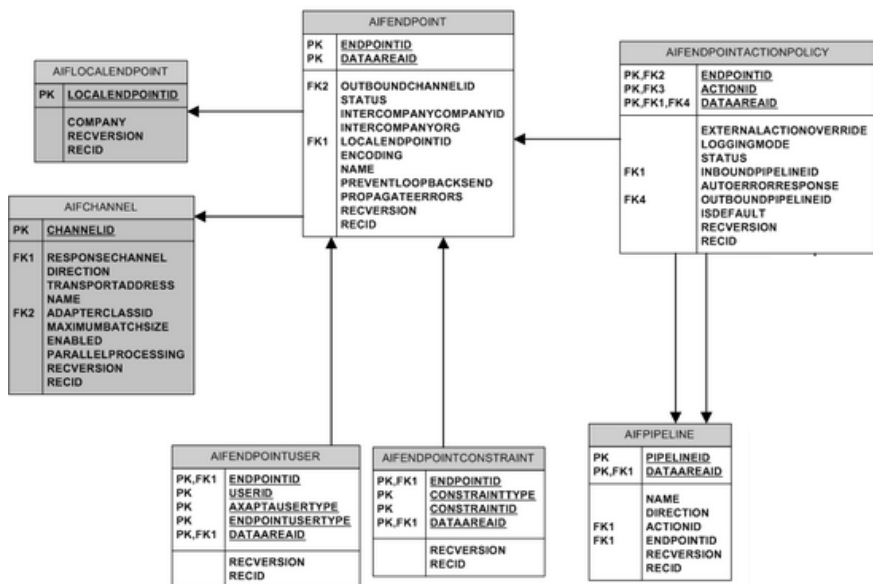
2. 데이터 모델 및 피벗

데이터 모델이란?

데이터 모델 및 피벗

■ 데이터 모델은 현업 데이터의 분석을 도와 줍니다

- 데이터의 Semantic 지식 구조를 사전 정의하고 상, 하위 구조를 포함하는 데이터 모형
- 설정이 저장되어 있다가 검색 시 Dynamic하게 반영
- 특화된 검색과 분석을 가능하게 하고 Pivot기능의 바탕



Extractions

Lookups

Evals

■ 데이터 모델 Object 유형

- Root Object : 최 상위 Object로 여러 Child Object를 생성/관리 한다.
- Event Object : Data를 분류해 제약 조건에 의해 추가한 것을 말한다.
- Search Object : Data Model안에 Object를 통계 명령을 사용하여 검색 할 기능을 갖고 있는 Object
- Transaction Object : Data Model 내에 존재하는 하나 이상의 Event, Transaction, search Object 내의 Data 구성 집합을 기반으로 또 다른 Object 구조를 만든다.
- Child Object : 상위 Object의 자식 개념의 Object로 상위 Object가 제한한 부분의 조건을 상속 받는다.

■ 데이터 모델의 성격

- 상 하위 구조로 구성되며 Constraints와 Attribute를 상위 Object에서 상속 받으며, 또한 개별 순위의 Object만이 Constraint와 Attribute들을 포함할 수 있다.

데이터 모델 확인

데이터 모델 및 피벗

■ 모델 확인

- 설정 - 데이터모델에서 확인.

The screenshot shows the Splunk Admin console interface. The top navigation bar includes 'Administrator', '1 메시지', '설정', '작업', '도움말', and a search bar. The left sidebar contains '데이터 추가' and '모니터링 콘솔'. The main content area is titled '데이터 모델' and includes a description: '데이터 모델을 사용하면 피벗 도구에서 쉽게 보고서를 생성할 수 있습니다. 자세히 알아보기'. Below this is a table listing data models.

이	제목	유형	작업	앱	소유자	공유 중
>	Splunk's Internal Audit Logs - SAMPLE	데이터 모델	편집 피벗	search	nobody	앱
>	Splunk's Internal Server Logs - SAMPLE	데이터 모델	편집 피벗	search	nobody	앱

데이터 모델 및 피벗

- SAMPLE 확인
 - Splunk 설치 시 SAMPLE로 들어가 있는 모델

Splunk's Internal Audit Logs - SAMPLE

internal_audit_logs

< 모든 데이터 모델

데이터 집합

이벤트

Audit

- Searches
- Modify Splunk Configs

데이터 집합 추가 ▼

Audit

Audit

이름 변경 삭제

제약조건

index=_audit

제약조건 편집

일괄 편집 ▼

필드 추가 ▼

상속됨

_time	시간	
<input type="checkbox"/> host	문자열	재정의
<input type="checkbox"/> source	문자열	재정의
<input type="checkbox"/> sourcetype	문자열	재정의

■ Pivot 필요성

- Splunk의 쿼리에 대한 지식 없이도 고객이 원하는 정보만을 표현하는 맞춤형 서비스가 가능하다.
- 간단한 Drop and Down 만으로 Data를 신속하게 설계하며, 시각화 함으로써 Data를 다양한 측면으로 활용 할 수 있다.

■ Pivot 사용법

- Data Model을 통해 Data 조직과 이벤트로의 구체적이며 세부적인 접근을 할 수 있다.
- Splunk에 기본적으로 설치되어 있는 Pivot 앱 실행으로 관리자가 설정해 놓은 범위 안에서 손쉽게 고객이 원하는 Data의 추출이 가능하다.

■ Pivot

- 모델 화면에서 피벗 메뉴를 확인

2 데이터 모델 앱: Search & Reporting(search) ▼ 앱에서 생성됨 ▼ 소유자: 모두 ▼

필터

 페이지당 20개 ▼

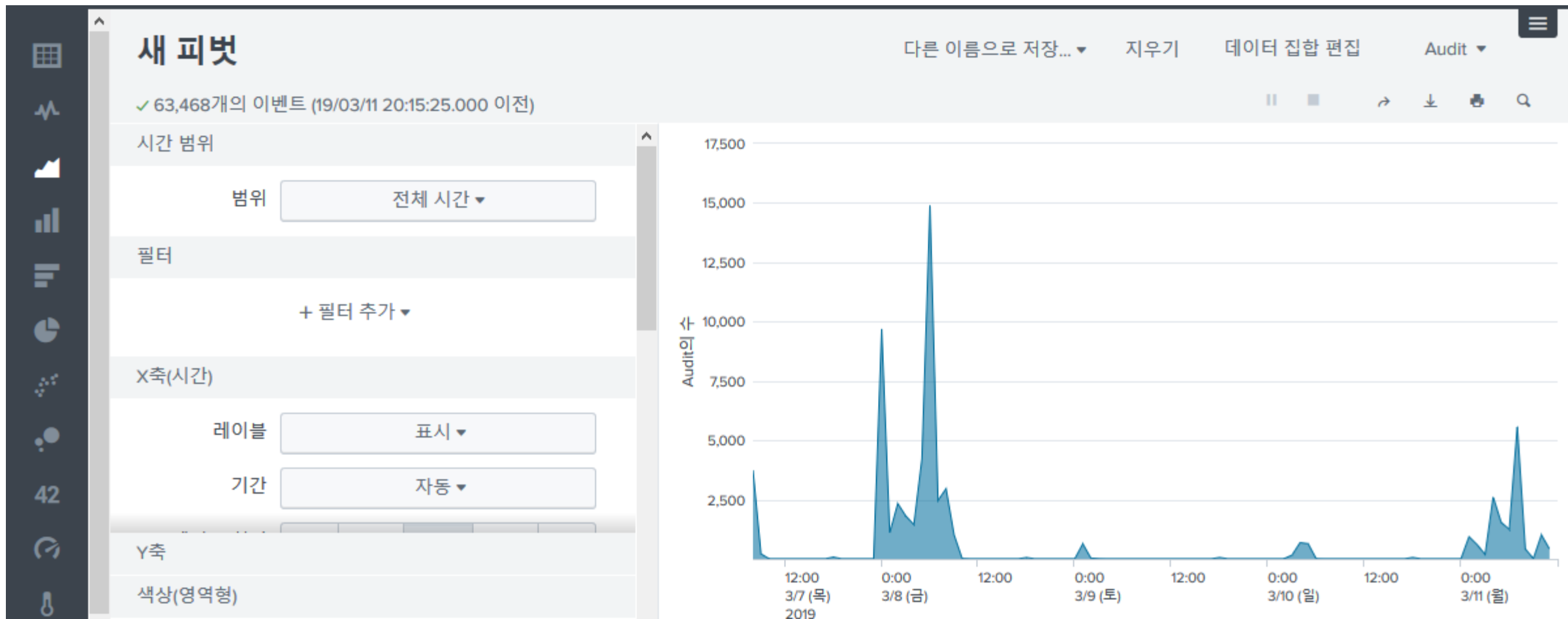
i	제목 ▲	유형 ◆	작업 ⚡	앱 ◆	소유자 ◆	공유 중 ◆
>	Splunk's Internal Audit Logs - SAMPLE	데이터 모델	편집 ▼ 피벗	search	nobody	앱
>	Splunk's Internal Server Logs - SAMPLE	데이터 모델	편집 ▼ 피벗	search	nobody	앱

- 3개의 층으로 된 모델에서 원하는 데이터가 있는 부분을 선택

데이터 집합 선택		데이터 집합 편집
i	3개의 개체 - Splunk's Internal Audit Logs - SAMPLE	
>	Audit	
>	Searches	
>	Modify Splunk Configs	

■ Pivot

- 모델 화면에서 피벗 메뉴를 확인
 - 여러 차트를 지정하면서 바로 결과를 확인 할 수 있다.



3. 스프링크 앱

■ App

- Splunk 내에 하나의 애플리케이션으로 구성하여 여러 종류의 데이터 뷰를 체계화하고 UI를 연계 정리한 것
- 예제 : “Splunk for Cisco Security”나 “DB connect” App

■ Add-on

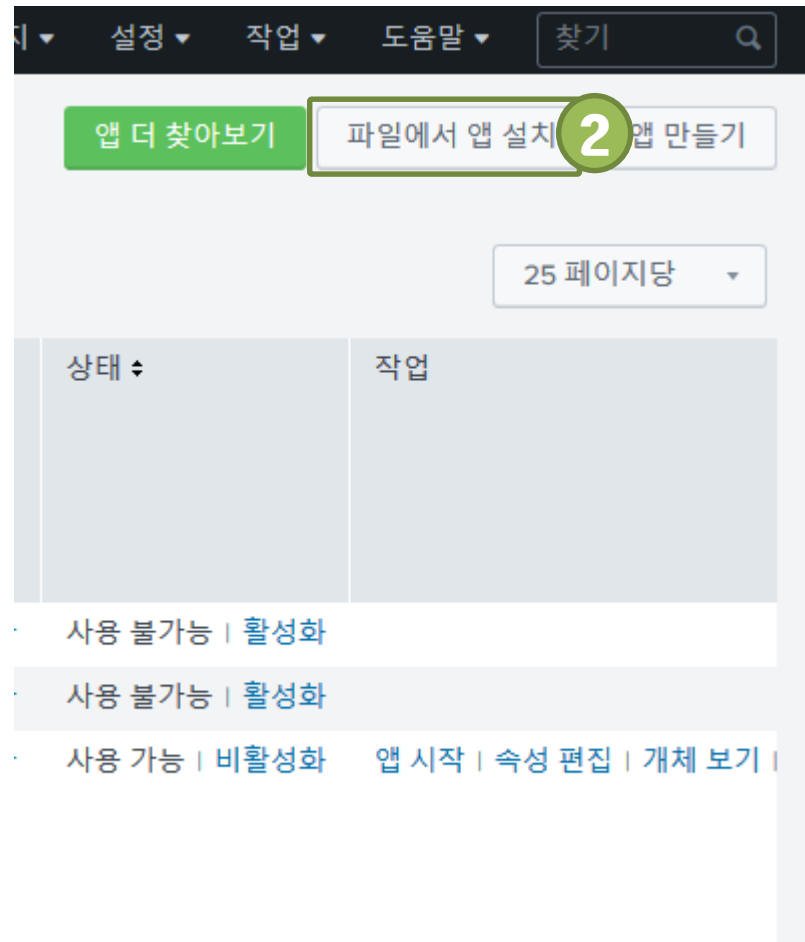
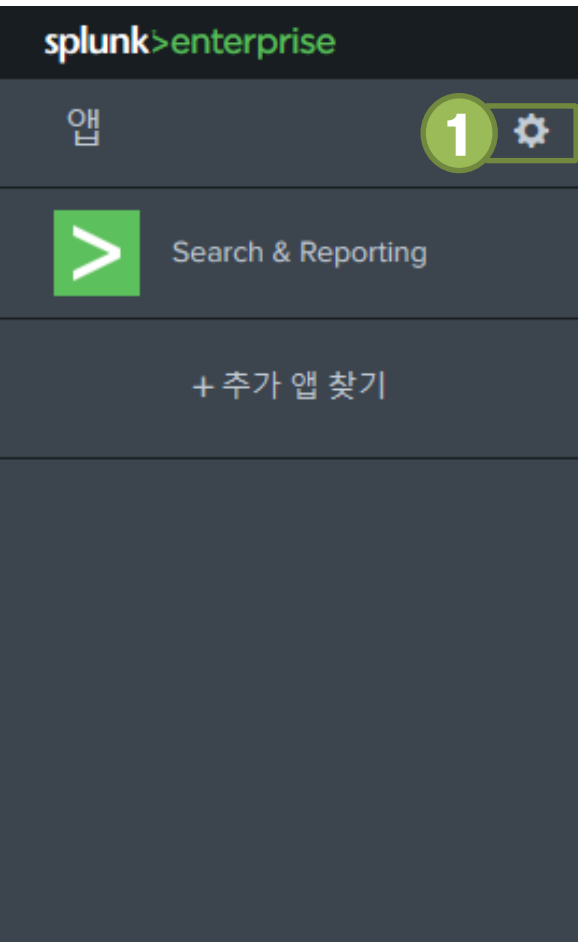
- Splunk에 추가적인 자원(예 : command, 데이터 인지 룰)을 제공하여 기능을 확장해 주는 모듈

APP 설치 방법

스플링크 설치 및 소개

■ 추가적인 앱을 설치하는 방법

- 예 : splunk-machine-learning-toolkit_450.tgz

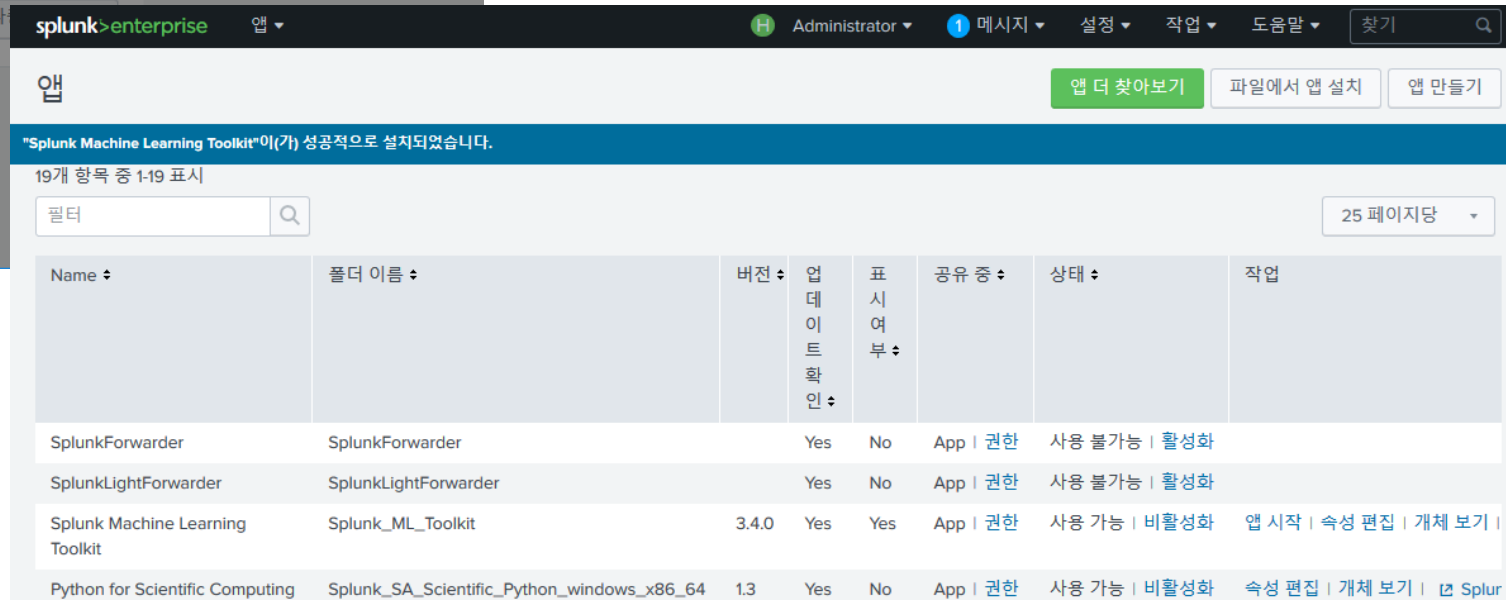
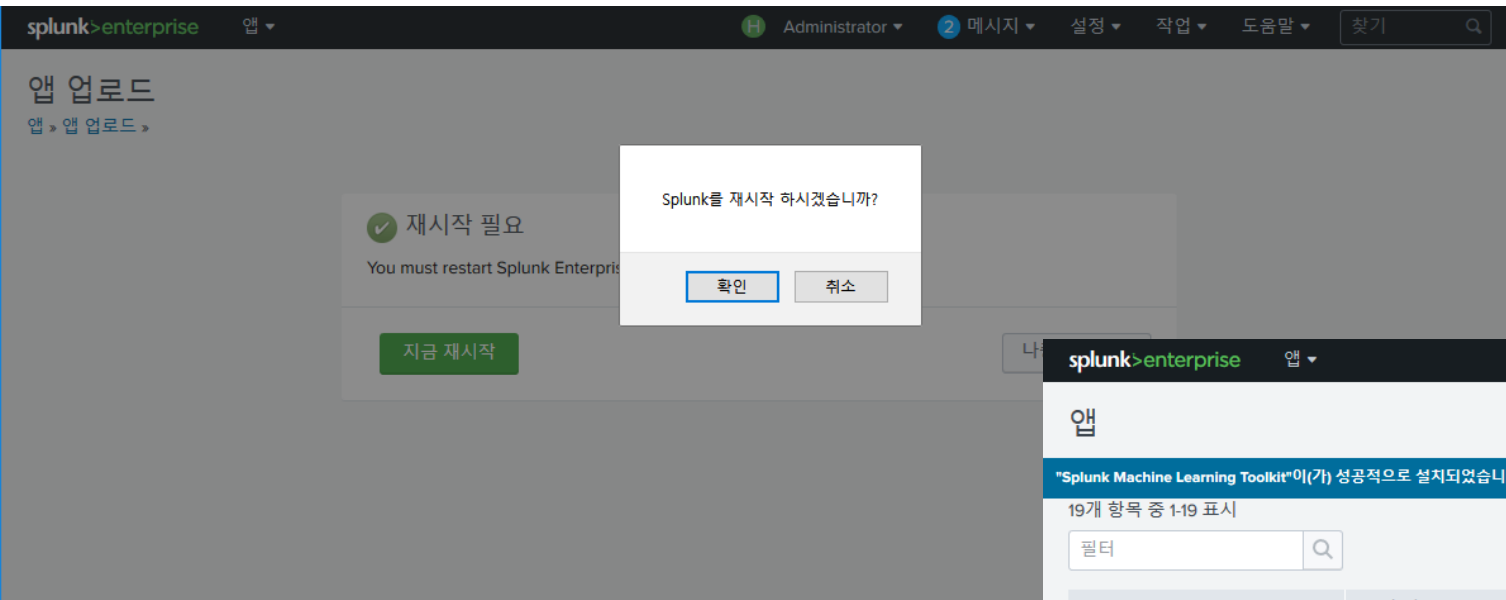


APP 설치 방법

스플링크 설치 및 소개

■ 추가적인 앱을 설치하는 방법

- 예 : splunk-machine-learning-toolkit_450.tgz
- 앱에 따라서 재시작 메시지가 나오며 메시지가 나올 시 재시작을 해야 원활하게 앱을 사용 가능

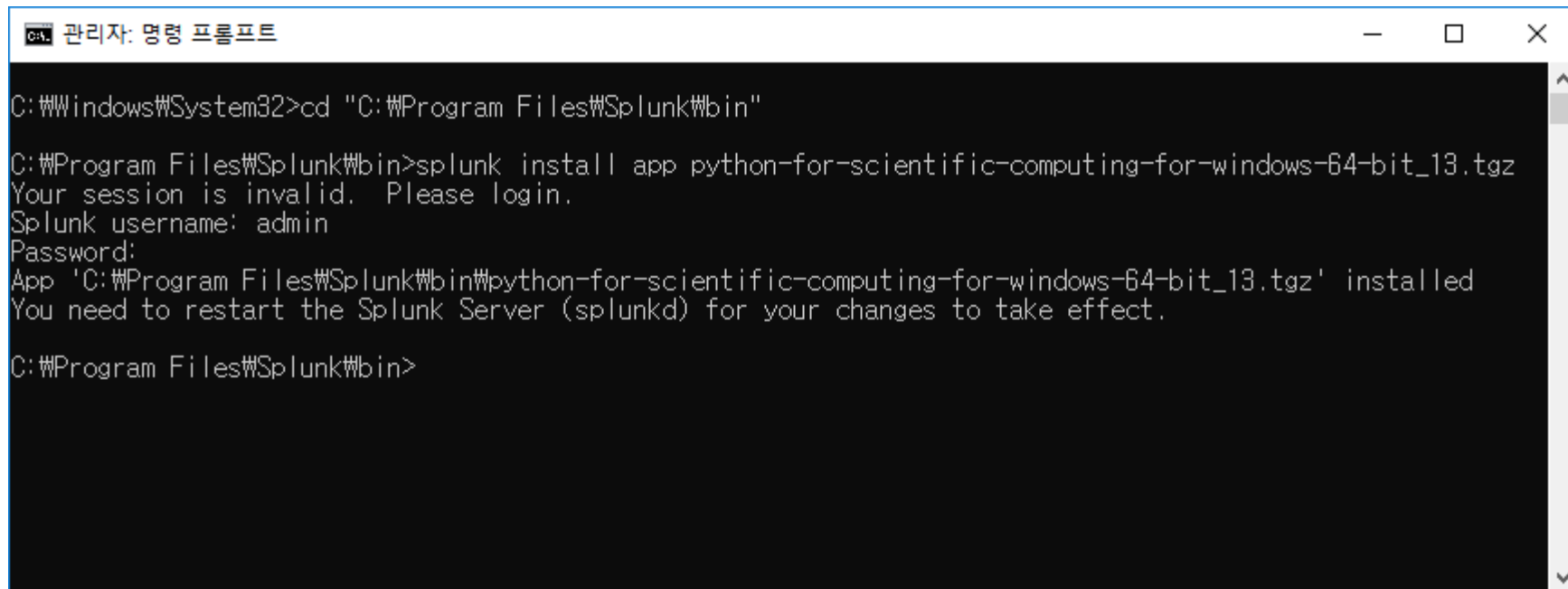


APP 설치 방법

스플링크 설치 및 소개

■ 커맨드 수동 설치

- 앱을 "C:\Program Files\Splunk\bin" 경로에 복사 또는 알 수 있는 경로에 위치
- cmd를 관리자 권한으로 실행
- cd "C:\Program Files\Splunk\bin" 로 스플링크 설치 경로로 이동
- splunk install app <앱파일명>
- splunk remove app <앱명>



```
관리자: 명령 프롬프트

C:\Windows\System32>cd "C:\Program Files\Splunk\bin"

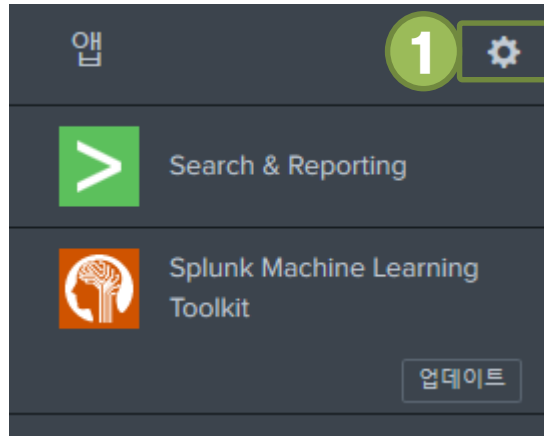
C:\Program Files\Splunk\bin>splunk install app python-for-scientific-computing-for-windows-64-bit_13.tgz
Your session is invalid. Please login.
Splunk username: admin
Password:
App 'C:\Program Files\Splunk\bin\python-for-scientific-computing-for-windows-64-bit_13.tgz' installed
You need to restart the Splunk Server (splunkd) for your changes to take effect.

C:\Program Files\Splunk\bin>
```

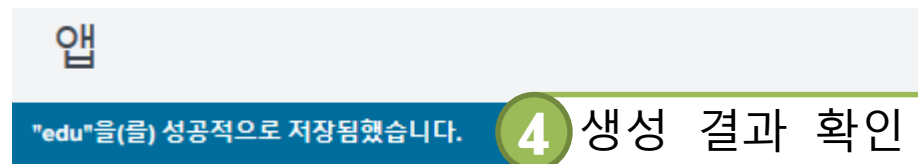
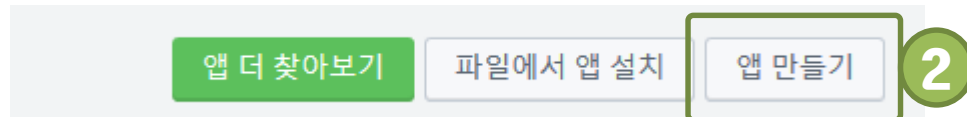
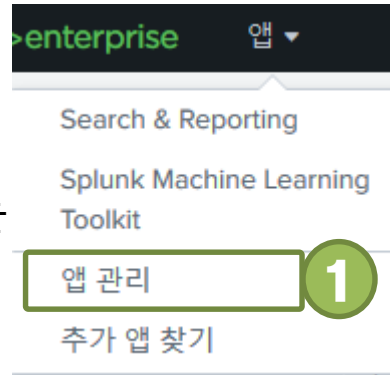
신규 APP 생성

스플링크 앱

■ 신규 App을 “앱” 기능에서 “앱 관리”으로 생성합니다.



또는



새로 추가
앱 > 새로 추가

3 원하는 내용 입력

Name: 교육앱
Splunk Web에 표시하려면 이름을 앱에 제공하십시오.

폴더 이름: edu
이 이름은 \$SPLUNK_HOME/etc/apps/의 앱 디렉터리에 매핑됩니다.

버전: 0.0.1
앱 버전입니다.

표시 여부: ☐ 아니요 ☒ 예
뷰가 포함된 앱만 표시 가능하도록 설정할 수 있습니다.

작성자:
앱 소유자의 이름입니다.

설명: Splunk 교육 데모 앱
앱에 대한 설명을 입력하십시오.

템플릿: barebones
이 템플릿에는 예제 뷰와 검색이 포함되어 있습니다.

자산 업로드: 선택한 파일이 없습니다.
html, js 또는 기타 파일을 앱에 추가할 수 있습니다.

APP 권한 설정

스플링크 앱

■ 생성된 App은 다양한 사용자 권한을 제어할 수 있게 구성

교육앱

edu

0.0.1

Yes

Yes

App | 권한

사용 가능

앱 시작 | 속성 편집 | 개체 보기

앱 권한

읽기 권한을 가진 사용자는 개체를 저장만 할 수 있고 다른 사용자와 개체를 공유하려면 쓰기 권한이 필요합니다.

역할	읽기	쓰기
모든 사용자	<input checked="" type="checkbox"/>	<input type="checkbox"/>
admin	<input type="checkbox"/>	<input checked="" type="checkbox"/>
can_delete	<input type="checkbox"/>	<input type="checkbox"/>
power	<input type="checkbox"/>	<input checked="" type="checkbox"/>
splunk-system-role	<input type="checkbox"/>	<input type="checkbox"/>
user	<input type="checkbox"/>	<input type="checkbox"/>

config 파일 전용 개체에 대한 공유

UI를 통해 만들어진 설정이 아닌 config 파일에 복사되거나 추가된 설정에 대한 권한을 설정합니다.

UI가 아닌 config 파일에 정의된 개체만 나타나야 합니다.

☒ 이 앱만(system) ☐ 모든 앱

취소

저장

모든 설정

Knowledge Object 재할당

1개 항목 중 1:1 표시

App 교육앱 (edu)

소유자 모두

앱에서 생성됨

필터


25 페이지당

Name	설정 유형	소유자	App	공유 중	상태
default	nav	소유자 없음	edu	App 권한	사용 가능


APP 메뉴 설정

스플링크 앱

■ 앱에 추가하는 대시보드 등을 메뉴 바에 추가/구성 변경



데이터 추가



모니터링 콘솔

지식

검색, 보고서 및 경고

데이터 모델

Event type

태그

필드

특언

사용자 인터페이스

경고

고급

모든

시스템

서버

서버

Instru

라이선

데이터

데이터 입력

전달 및 수신

인덱스

보고서 가속화 요약

Source Type

분산 환경

인텔리гент

사용자 인터페이스

뷰, 대시보드 및 탐색 메뉴를 만들고 편집합니다.

시간 범위	+ 새로 추가
뷰	+ 새로 추가
PDF 스케줄 보기	
탐색 메뉴	

■ 앱에 추가하는 대시보드 등을 메뉴 바에 추가/구성 변경

탐색 메뉴 XML * 탐색 메뉴 XML 설정을 입력 및 편집합니다.

탐색 이름 ▾

default

<

일반 텍스트

```
<nav search_view="search" color="#50C05C">
  <view name="search" default="true" />
  <view name="analysis_workspace" />
  <view name="datasets" />
  <view name="reports" />
  <view name="alerts" />
  <view name="dashboards" />
</nav>
```

- 가능 옵션
 - view name: 대시보드 이름
 - collection label: 드릴다운 메뉴 설정
 - saved name : 보고서 이름

APP 메뉴 설정

스플링크 앱

■ 앱에 추가하는 대시보드 등을 메뉴 바에 추가/구성 변경

탐색 이름 ▾

default

<

- 가능 옵션
 - view name: 대시보드 이름
 - collection label: 드릴다운 메뉴 설정
 - saved name : 보고서 이름

splunk>enterprise 앱: Search & Reporting ▾

검색 메트릭 데이터 집합 collection ▾

검색

여기에 검색을 입력

이벤트 샘플링 없음 ▾

보고서
경고
대시보드

탐색 메뉴 XML * 탐색 메뉴 XML 설정을 입력 및 편집합니다.

```
<nav search_view="search" color="#5CC05C">
  <view name="search" default="true" />
  <view name="analysis_workspace" />
  <view name="dataset" />
  <collection label="collection">
    <view name="reports" />
    <view name="alerts" />
    <view name="dashboards" />
  </collection>
</nav>
```

4. 대시보드 만들기

■ 데이터 시각화

- 데이터를 분석 툴에서 제공되는 차트를 이용해서 시각화 합니다.
- 각 검색에 대해서 보고서 형식으로 저장을 하여 빠르게 통계에 대해 시각적으로 확인이 가능합니다.
- 한 대시보드로 구성 시 여러 내용에 대해서 하나의 화면에서 확인 할 수 있습니다.



■ 보고서 정의 및 필요성

- 데이터에 대한 검색 또는 피벗을 나중에 재사용하기 위해서 보고서로 저장
- 작성한 후 보고서를 사용하여 다양한 작업이 가능
- 대시보드 패널로 사용하거나 자체로 예약된 작업 수행 가능

■ 데이터를 이용한 보고서 작성

- 지역별로 충전소 현황

▶ 예제 코드

```
index="eco_car"  
| rex field=소재지도로명주소 "(?<city>[가-힣]*)"  
| stats count by city
```

새로운 검색

```
index="eco_car"  
| rex field=소재지도로명주소 "(?<city>[가-힣]*)"  
| stats count by city
```

✓ 2,400개의 이벤트 (19/03/12 9:22:52.000 이전) 이벤트 샘플링 없음 ▼

작업 ▼ || ■ → 다른 이름으로 저장 ▼ 닫기

이벤트 패턴 통계 (17) 시각화

페이지당 20개 ▼ 형식 미리보기 ▼

city ▼

count ▼

강원도

■ 데이터를 이용한 보고서 작성

- 지역별로 충전소 현황

보고서로 저장

제목

count_by_city

설명

선택 사항

콘텐츠

시간 범위 선택기

예

검색

데이터 집합

보고서

경고

대시보드

>

Search & Reporting

보고서

보고서는 단일 검색을 기반으로 하며 시각화 요소, 통계 또는 이벤트가 포함될 수 있습니다. 보고서를 볼 이름을 클릭하십시오. 피벗 또는 검색에서 보고서를 열고 매개 변수를 상세히 지정하거나 데이터를 추가로 탐색하십시오.

7 보고서

모두

사용자

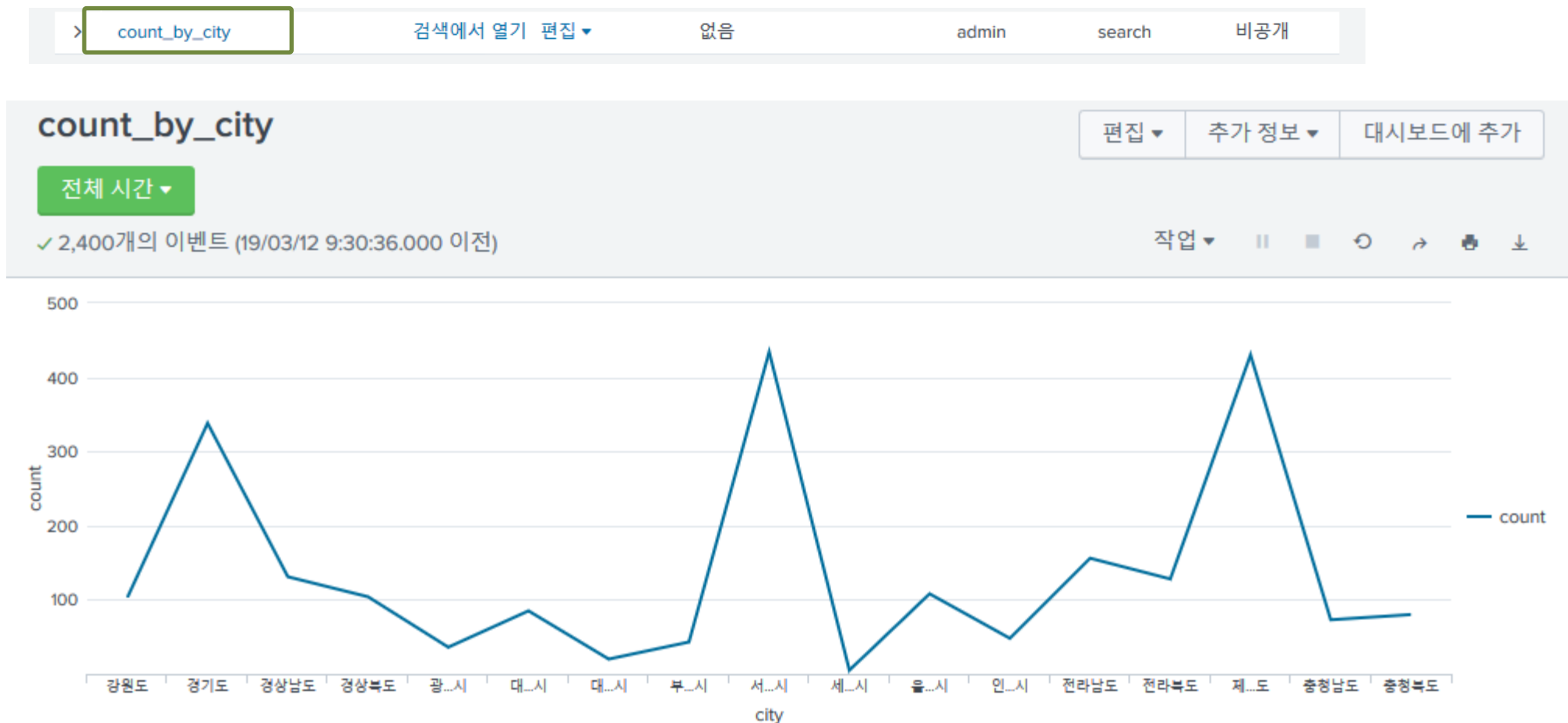
이 앱

필터

i	제목 ^	작업	다음 예약 시간 ⇅	소유자 ⇅	앱 ⇅	공유 중 ⇅
>	Errors in the last 24 hours	검색에서 열기 편집 ▾	없음	nobody	search	앱
>	Errors in the last hour	검색에서 열기 편집 ▾	없음	nobody	search	앱
>	License Usage Data Cube	검색에서 열기 편집 ▾	없음	nobody	search	앱
>	Messages by minute last 3 hours	검색에서 열기 편집 ▾	없음	nobody	search	앱
>	Orphaned scheduled searches	검색에서 열기 편집 ▾	없음	nobody	search	앱
>	Splunk errors last 24 hours	검색에서 열기 편집 ▾	없음	nobody	search	앱
>	count_by_city	검색에서 열기 편집 ▾	없음	admin	search	비공개

■ 데이터를 이용한 보고서 작성

- 지역별로 충전소 현황



■ 대시보드용 보고서 작성 예제

시도별 현황

▶ 예제

- “시도별현황 ” 이라고 하는 이름으로 아래의 쿼리를 검색하고 차트로 설정한 후에 보고서로 저장 (원형차트)

▶ 예제 코드

```
index="eco_car"
```

```
| rex field=소재지도로명주소 "(?<city>[가-힣]*)"
```

```
| stats count by city
```


■ 대시보드용 보고서 작성 예제

시도별 주차료부과여부 현황

▶ 예제

- “시도별주차료부과여부현황”이라고 하는 이름으로 아래의 쿼리를 검색하고 차트로 설정한 후에 보고서로 저장 (세로막대형차트)

▶ 예제 코드

```
index="eco_car"
```

```
| rex field=소재지도로명주소 "(?<city>[가-힣]*)"
```

```
| stats count(eval('주차료부과여부'=="Y")) as YES, count(eval('주차료부과여부'=="N")) as NO by city
```

■ 대시보드용 보고서 작성 예제

시도별 맵 현황

▶ 예제

- “시도별맵현황”이라고 하는 이름으로 아래의 쿼리를 검색하고 차트로 설정한 후에 보고서로 저장 (클러스터맵 – 보고서에서는 전체 지도가 기본 옵션)

▶ 예제 코드

```
index="eco_car"
```

```
| rex field=소재지도로명주소 "(?<city>[가-힣]*)"
```

```
| geostats count latfield=위도 longfield=경도 by city globallimit=0
```

■ 대시보드 정의 및 필요성

- 대시보드는 미리 정의된 검색, 차트, 경고 및 보고서, 뷰를 시각화 하여 쉽게 웹상에서 관리 할 수 있는 환경을 제공
- 대시보드에는 한 화면에 여러 시각화 요소 및 다양한 웹 기반의 요소를 구성할 수 있는 인터페이스를 제공하며, 빠르게 시각화 및 여러 분석 서비스 기능을 구성



■ 신규 대시보드 생성

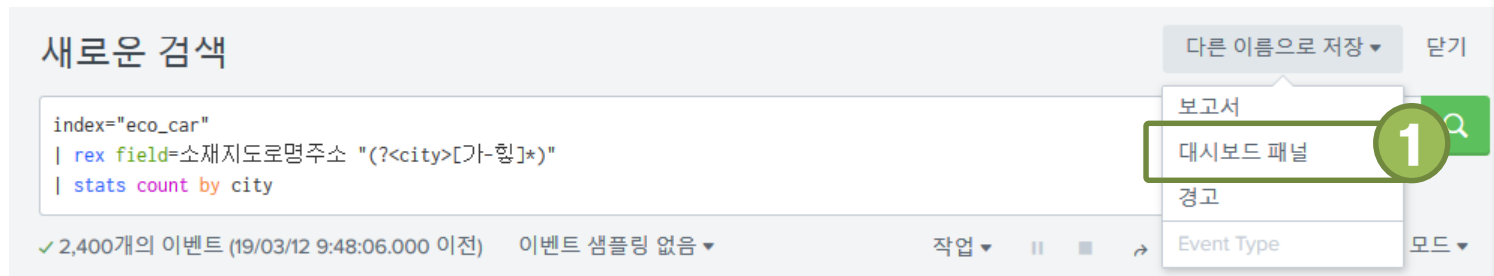
▶ 예제

- 시도별 현황 검색문을 작성 후 시각화를 선택 - 다른 이름으로 저장 - 대시보드 패널

index="eco_car"

| rex field=소재지도로명주소 "(?<city>[가-힣]*)"

| stats count by city



대시보드 패널이 생성되었습니다.

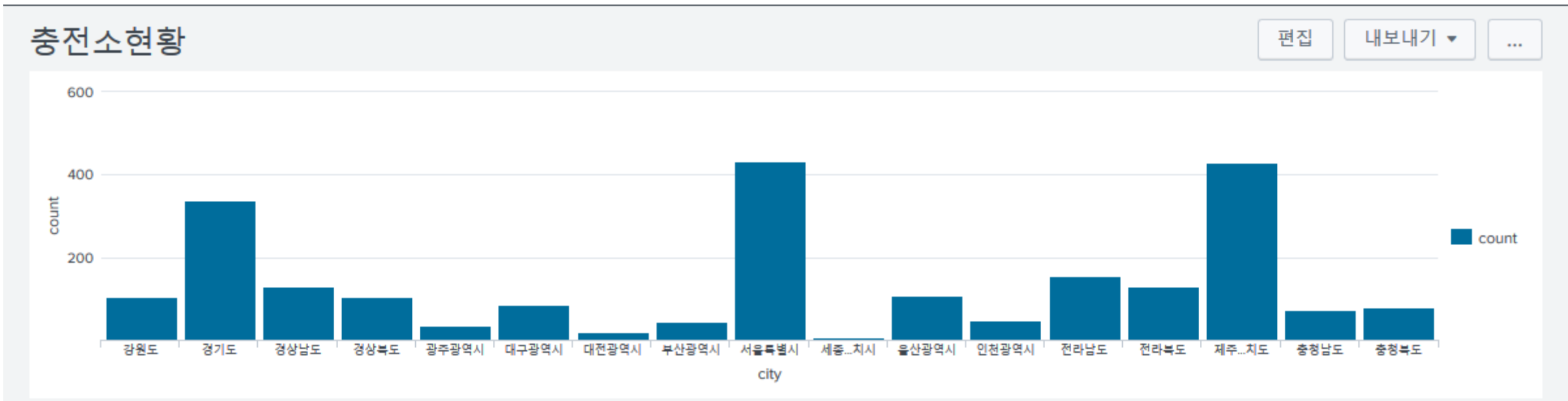
패널이 생성되어 eco_station에 추가되었습니다. 이제 대시보드를 볼 수 있습니다.

3

대시보드 보기



■ 신규 대시보드 생성



■ 대시보드 패널 추가 및 수정

- 대시보드 패널은 대시보드 화면에서 UI를 이용하여 기본적인 추가 및 수정이 가능

▶ 예제 코드

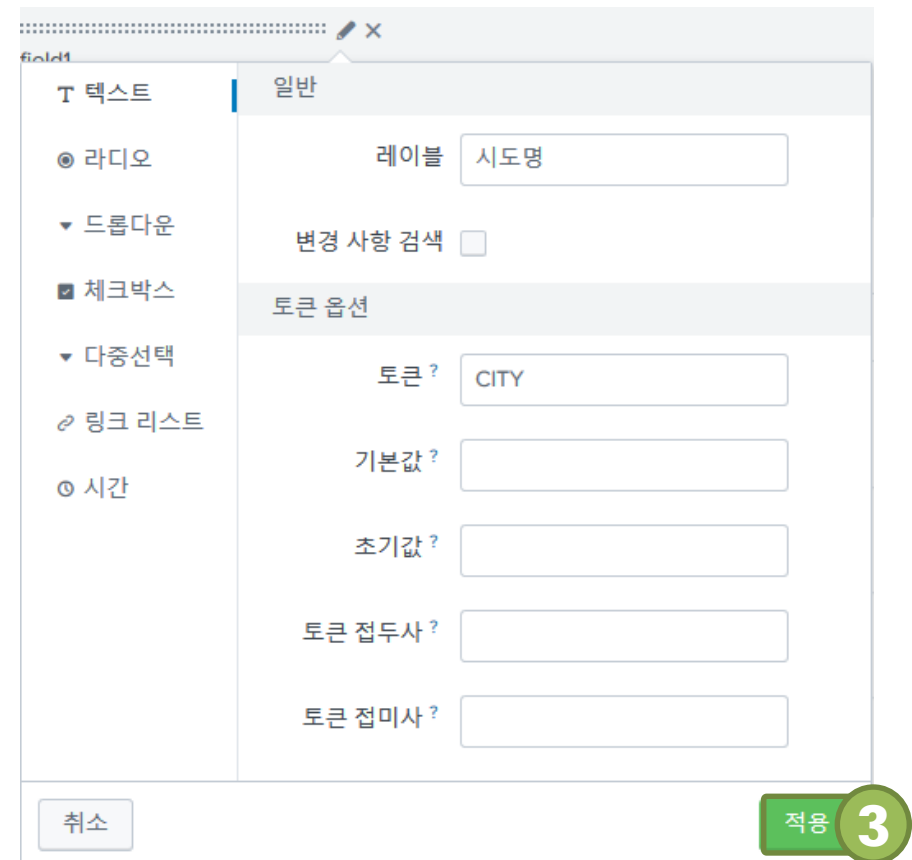
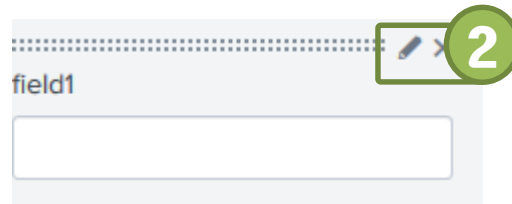
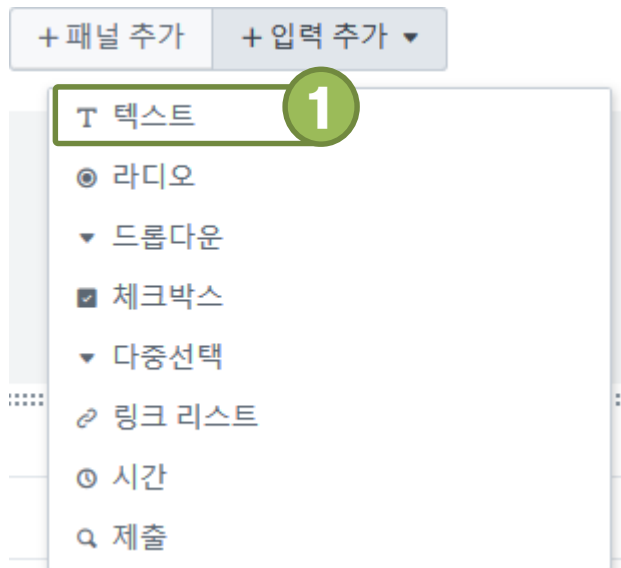
- 편집 -> + 패널추가 -> 새로 만들기 -> 원하는 차트를 선택 및 패널 추가

`index="eco_car" | stats count by 급속충전가능여부`

The screenshot illustrates the steps to add a new panel to a dashboard in Splunk Enterprise. The interface shows the '대시보드 편집' (Dashboard Edit) view. The '+ 패널 추가' (Add Panel) button is highlighted with a green box and a red circle with the number 1. A dropdown menu is open, showing various chart types. The 'Column Chart' option is highlighted with a blue bar and a red circle with the number 2. The '새로 만들기 Column Chart' (New Column Chart) dialog is open, showing the '대시보드에 추가' (Add to Dashboard) button, time range settings, content title '급속충전가능여부 차트', and the search query 'index="eco_car" | stats count by 급속충전가능여부'.

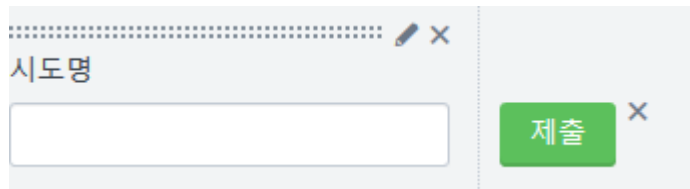
■ 대시보드 필드셋 입력 추가

- 대시보드 패널은 입력박스를 사용하여 응답형 인터페이스를 지정할 수 있음
- 토큰이라고 하는 전달되는 변수를 사용(\$로 감싸는 영문변수)



■ 대시보드 필드셋 입력 추가

- 검색을 변경하여 토큰 적용



검색 편집

제목

검색 문자열

```
index="eco_car"
| rex field=소재지도로명주소 "(?<city>[가-힣]*)"
| stats count by city
| search city="*$CITY$"
```

검색 실행

시간 범위

시간 선택기 사용 ▼

전체 시간 ▶

자동 새로 고침 지연?

자동 새로 고침 없음 ▼

표시기 새로 고침

진행률 표시줄 ▼

▶ 예제 코드

```
index="eco_car"
| rex field=소재지도로명주소 "(?<city>[가-힣]*)"
| stats count by city | search city="*$CITY$"
```


■ 대시보드 필드셋 입력 추가

- 토큰 적용 확인

충전소현황

시도명

제출

필터 숨기기

편집

내보내기 ▼

...

! 검색에서 입력을 기다리는 중...



Contents

5. 데이터 주입 및 검색

6. 데이터 시각화

7. 대시보드용 시나리오

5. 데이터 주입 및 검색 실습


데이터 주입 1

데이터 주입 및 검색

■ K water 공공데이터개방포털

- http://opendata.kwater.or.kr/pubdata/rwiswater/water_flux.do?seq_no=132

OPEN DATA
공공데이터



분류 체계

- 수자원 (8)
- 수도 (4)
- 수질 (3)
- 기술 (1)
- 기타 (1)

서비스 유형

- SHEET (16)
- CHART (0)
- MAP (0)
- Open API (16)
- LOD (12)
- 별도제공 (0)

공공데이터

실시간 수도정보 유량(시간) 메타정보


K-water가 관리하는 정수장 및 공급과정의 실시간 유량 정보


SHEET

OPEN API


LOD

시설구분


정수장 

성남정수장 

일별자료

2020-02-01 

~

2020-02-12 

검색

파일변환저장

XLS

CSV

XML

JSON

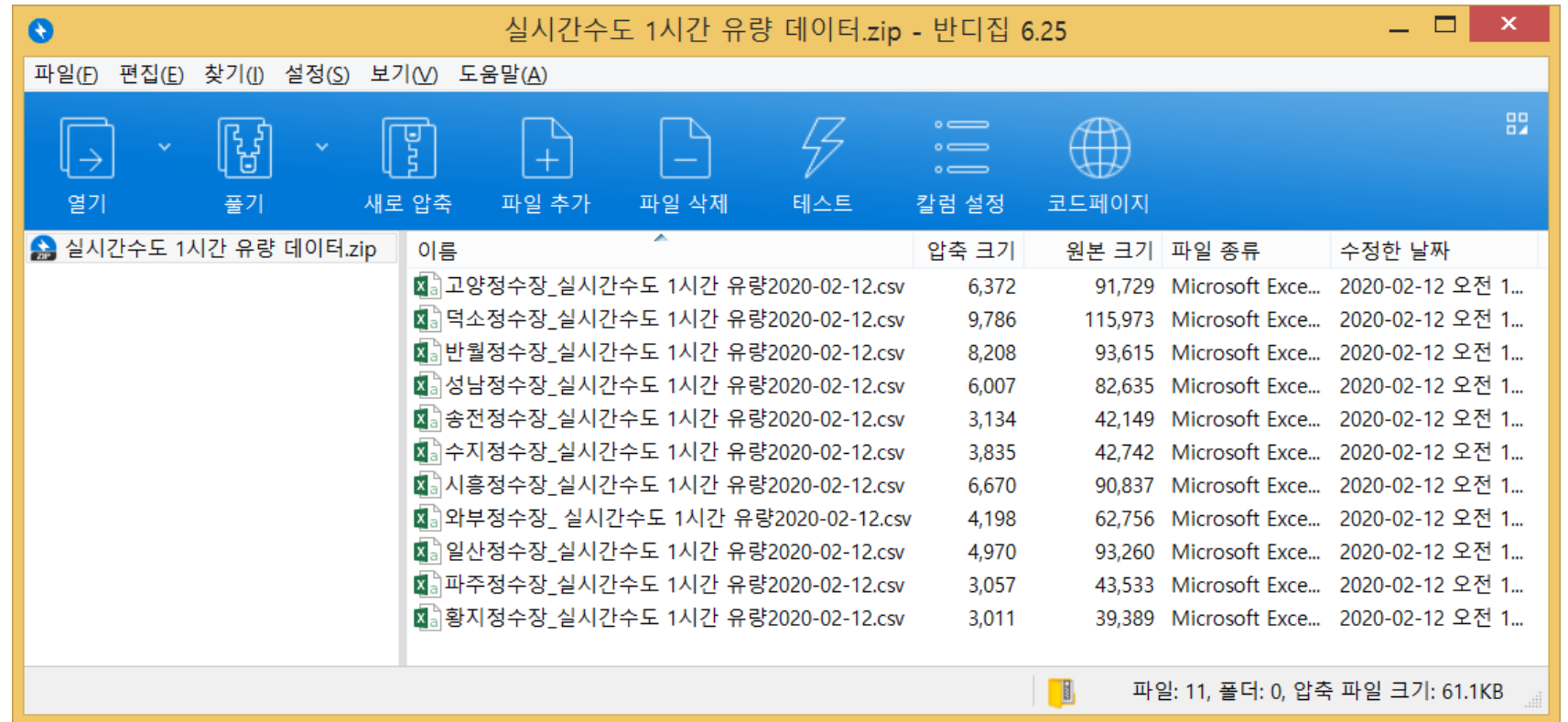
발생일자	시설명	시설관리번호	유량	단위	자료 수집 TAG 설명	TAGSN	데이터항목구분	변경일자
2020021210	성남정수장	4113112313	13904	m	성남(정) 4단계 송수 유량 적산차	4883	D	
2020021210	성남정수장	4113112313	13852.2333	m/h	성남(정) 4단계 송수 유량	4879	F	
2020021210	성남정수장	4113112313	12192	m	성남(정) 3단계 송수 유량 적산차	4877	D	
2020021210	성남정수장	4113112313	12220.3125	m/h	성남(정) 3단계 송수 유량 순시	4872	F	
2020021209	성남정수장	4113112313	13984	m	성남(정) 4단계 송수 유량 적산차	4883	D	
2020021209	성남정수장	4113112313	13992.0667	m/h	성남(정) 4단계 송수 유량	4879	F	
2020021209	성남정수장	4113112313	11808	m	성남(정) 3단계 송수 유량 적산차	4877	D	

데이터 주입 1

데이터 주입 및 검색

■ K water 공공데이터개방포털 – 정수장 실시간 수도정보 유량 데이터

- 데이터 확인 – 압축파일



데이터 주입 1

데이터 주입 및 검색

■ K water 공공데이터개방포털 – 정수장 실시간 수도정보 유량 데이터

- 데이터 확인 – 압축파일 내의 데이터는 지역만 다르고 동일 형태의 데이터

발생일자	시설명	시설관리번호	압력	단위	자료 수집 TAG 설명	TAGSN	변경일자
2020021203	일산정수장	4128112315	1520	m³	고양 일산(정) 능곡 계통 송수 유량 적산차	13823	
2020021203	일산정수장	4128112315	-48	m³/h	일산(정) 능곡계통송수유량순시	5202	
2020021203	일산정수장	4128112315	4530	m³	고양 일산(정) 일산 계통 송수 유량 적산차	13828	
2020021203	일산정수장	4128112315	1403	m³/h	일산(정) 일산계통송수유량순시	5201	
2020021202	일산정수장	4128112315	1240	m³	고양 일산(정) 능곡 계통 송수 유량 적산차	13823	
2020021202	일산정수장	4128112315	-48	m³/h	일산(정) 능곡계통송수유량순시	5202	
2020021202	일산정수장	4128112315	4500	m³	고양 일산(정) 일산 계통 송수 유량 적산차	13828	
2020021202	일산정수장	4128112315	1403	m³/h	일산(정) 일산계통송수유량순시	5201	
2020021201	일산정수장	4128112315	1260	m³	고양 일산(정) 능곡 계통 송수 유량 적산차	13823	
2020021201	일산정수장	4128112315	-48	m³/h	일산(정) 능곡계통송수유량순시	5202	
2020021201	일산정수장	4128112315	4450	m³	고양 일산(정) 일산 계통 송수 유량 적산차	13828	
2020021201	일산정수장	4128112315	1403	m³/h	일산(정) 일산계통송수유량순시	5201	
2020021124	일산정수장	4128112315	1250	m³	고양 일산(정) 능곡 계통 송수 유량 적산차	13823	
2020021124	일산정수장	4128112315	-48	m³/h	일산(정) 능곡계통송수유량순시	5202	
2020021124	일산정수장	4128112315	4380	m³	고양 일산(정) 일산 계통 송수 유량 적산차	13828	
2020021124	일산정수장	4128112315	1403	m³/h	일산(정) 일산계통송수유량순시	5201	
2020021123	일산정수장	4128112315	1160	m³	고양 일산(정) 능곡 계통 송수 유량 적산차	13823	
2020021123	일산정수장	4128112315	-48	m³/h	일산(정) 능곡계통송수유량순시	5202	
2020021123	일산정수장	4128112315	3890	m³	고양 일산(정) 일산 계통 송수 유량 적산차	13828	

데이터 주입 1

데이터 주입 및 검색

■ K water 공공데이터개방포털 – 정수장 실시간 수도정보 유량 데이터

- 데이터 입력 – 업로드
 - 설정 – 데이터 추가 - 업로드

splunk>enterprise

앱 ▾

H Administrator ▾

메시지 ▾

설정 ▾

작업 ▾

도움말 ▾

찾기 🔍

데이터 추가

원본 선택

Source Type 설정

입력 설정

검토

완료

< 뒤로


다음 >

원본 선택

컴퓨터를 탐색하거나 파일을 아래의 대상 상자에 끌어놓아 Splunk에 업로드할 파일을 선택합니다. [자세히 알아보기](#)

선택한 파일:

파일 선택



실시간수도 1시간 유량_반월,성남,시흥,와부

데이터 파일을 여기에 놓습니다.

데이터 주입 1

데이터 주입 및 검색

■ K water 공공데이터개방포털 – 정수장 실시간 수도정보 유량 데이터

- 데이터 입력 – sourcetype 지정 – 기존에 저장되어 있는 것을 선택하거나 새로 만들

Source type

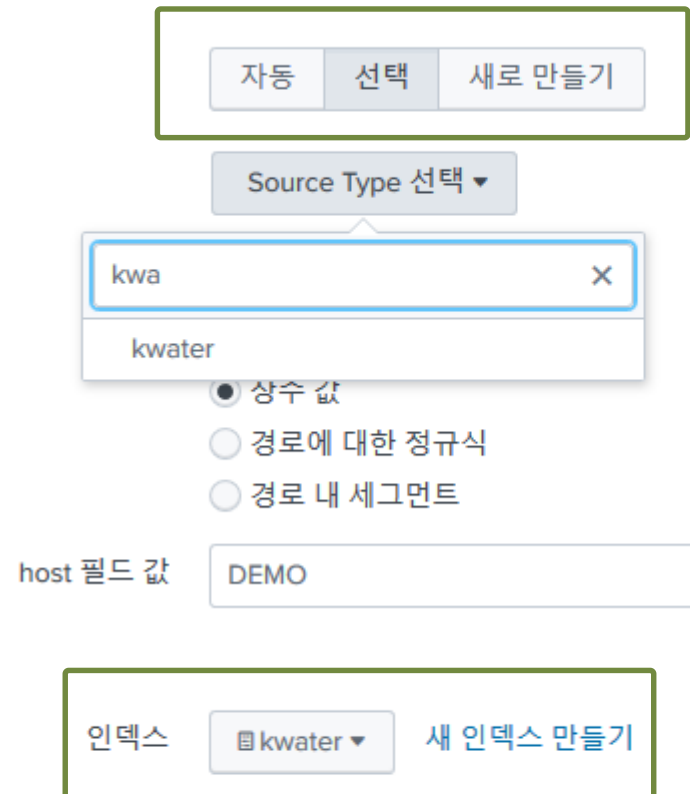
source type은 Splunk가 모든 수신 데이터에 할당하는 기본 필드 중 하나입니다. 이는 Splunk에 사용자가 가져온 데이터 종류를 알려주므로, Splunk가 인덱싱 중에 지능적으로 데이터를 포맷할 수 있습니다. 그리고 이 방식으로 데이터를 분류하여, 쉽게 데이터를 검색할 수 있습니다.

Host

Splunk가 데이터를 인덱싱할 때 각 이벤트는 "host" 값을 수신합니다. 호스트 값은 이벤트가 발생하는 컴퓨터의 이름이어야 합니다. 사용자가 선택한 입력의 유형에 따라 사용 가능한 설정 옵션이 결정됩니다. [자세히 알아보기](#)

인덱스

Splunk는 수신한 데이터를 지정된 인덱스에 이벤트로 저장합니다. 데이터에 대한 source type을 파악하는 데 문제가 있는 경우 "테스트용" 인덱스를 만들어 사용할 것을 고려하십시오. 테스트용 인덱스를 사용하여 프로덕션 인덱스에 영향을 주지 않고 설정 문제를 해결할 수 있습니다. 나중에 언제든지 이 설정을 변경할 수 있습니다. [자세히 알아보기](#)



자동 선택 새로 만들기

Source Type 선택 ▼

kwa ×

kwater

☒ 상수 값

☐ 경로에 대한 정규식

☐ 경로 내 세그먼트

host 필드 값 DEMO

인덱스 kwater ▼ 새 인덱스 만들기

데이터 주입 1

데이터 주입 및 검색

■ K water 공공데이터개방포털 – 정수장 실시간 수도정보 유량 데이터

- 데이터 확인

새로운 검색

다른 이름으로 저장

닫기

source="실시간수도 1시간 유량 데이터.zip:*" host="DEMO" index="kwater" sourcetype="kwater"

전체 시간

Q

✓ 9,707개의 이벤트 (20/02/12 15:46:46.000 이전) 이벤트 샘플링 없음

작업

||

■

↶

↷

↓

! 스마트 모드

이벤트 (9,707)패턴통계시각화

시간 표시줄 형식 지정

– 축소

+ 선택 항목 확대/축소

× 선택 취소

컬럼당 1일

리스트

↗ 형식

페이지당 20개

< 이전

1

2

3

4

5

6

7

8

...

다음 >

< 필드 숨기기

≡ 모든 필드

선택한 필드

a host 1

a source 11

a sourcetype 1

관심 필드

date_mday 12

a date_month 1

a date_wday 7

date_year 1

a date_zone 1

a index 1

linecount 1

a punct 22


i	시간	이벤트
>	20/02/12 11:00:00.000	2020021211, 황지정수장, 4219012371, 784, m³/h, 황지(정) 유출유량 순시, 3349, host = DEMO source = 실시간수도 1시간 유량 데이터.zip:.\E²ÁöÄ¼öÄä_½Ç½Ä¹¼öµµ 1½Ä¹ Ä²·202... sourcetype = kwater
>	20/02/12 11:00:00.000	2020021211, 황지정수장, 4219012371, 800, m³, 정수장 유출유량적산차, 19158, host = DEMO source = 실시간수도 1시간 유량 데이터.zip:.\E²ÁöÄ¼öÄä_½Ç½Ä¹¼öµµ 1½Ä¹ Ä²·202... sourcetype = kwater
>	20/02/12 11:00:00.000	2020021211, 파주정수장, 4148012318, 416, m³, 고양 파주(정) 정수 유출 유량 적산차, 19166, host = DEMO source = 실시간수도 1시간 유량 데이터.zip:.\EÄÄÖÄ¼öÄä_½Ç½Ä¹¼öµµ 1½Ä¹ Ä²·20... sourcetype = kwater
>	20/02/12 11:00:00.000	2020021211, 파주정수장, 4148012318, 4194, m³/h, 파주(정) 원수 유입유량, 44381, host = DEMO source = 실시간수도 1시간 유량 데이터.zip:.\EÄÄÖÄ¼öÄä_½Ç½Ä¹¼öµµ 1½Ä¹ Ä²·20... sourcetype = kwater
>	20/02/12 11:00:00.000	2020021211, 일산정수장, 4128112315, 1403, m³/h, 일산(정) 일산계통송수유량순시, 5201, host = DEMO source = 실시간수도 1시간 유량 데이터.zip:.\Ä³ëÄ¼öÄä_½Ç½Ä¹¼öµµ 1½Ä¹ Ä²·202... sourcetype = kwater
>	20/02/12	2020021211, 일산정수장, 4128112315, 3730, m³, 고양 일산(정) 일산 계통 송수 유량 적산차, 13828,

데이터 주입 2

데이터 주입 및 검색

■ 해양기상 통계자료 (2018년, 2019년 각 1월, 2월)

- <https://marineweather.nmpnt.go.kr/statistic/selectStatisticList.do>

국립해양측위정보원

소개실시간 해양기상정보해양기상 통계자료해양기상정보 서비스

해양기상 통계자료

🏠 > 해양기상 통계자료

해양기상 통계자료

통계자료

※ '기간'은 7일까지만 검색 가능합니다.

검색부산청전체기간2018-01-012018-01-07

지방청	표지	일시	풍향(°)	유향(°)	파향(°)	기온(℃)	수온(℃)	시정(km)	풍속(m/s)	유속(kn)	파고(m)	기압(hPa)	습도(%)	염분(psu)
부산청	남형제도등표	2018-01-07 23:13	346		0	8	0	0	3.7	0	0	1015.1	63	0
부산청	가덕도등대	2018-01-07 23:13	323		0	5.7	0	0	6.2	0	0	1005.7	66	0
부산청	신항유도등부표(랜비)	2018-01-07 23:13	109		0	22.6	13	0	9.1	0.2	0	1018	58	28
부산청	감천항유도등부표(랜비)	2018-01-07 23:13	180		0	8	13.7	0	7.4	0.3	0	1015.1	55	32
부산청	목도등대(나무섬등대)	2018-01-07 23:12	342		0	8.9	0	0	9.3	0	0	1009	66	0
부산청	부산항신항다목적부두	2018-01-07 23:12	0		0	0	0	10.7	0	0	0		0	0
부산청	부산항신항소형선부두등대	2018-01-07 23:11	0		0	0	0	7	0	0	0		0	0

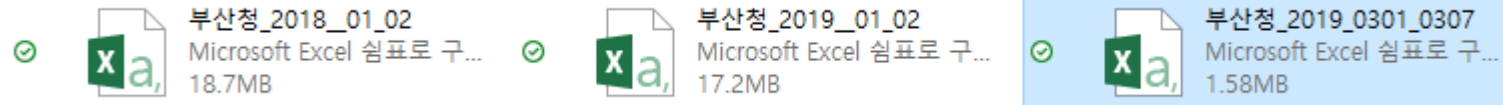
데이터 주입 2

데이터 주입 및 검색

■ 해양기상 통계자료 (2018년, 2019년 각 1월, 2월)

- <https://marineweather.nmpnt.go.kr/statistic/selectStatisticList.do>

- 3가지 데이터



- 원본이 엑셀이어서 csv로 편집. UTF-8로 변환.

데이터 주입 2

데이터 주입 및 검색

■ 해양기상 통계자료 (2019년 3월)

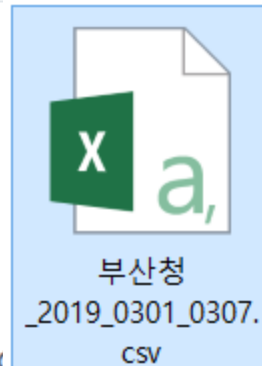
- 데이터 입력
 - 부산청_2019_0301_0307.csv로 먼저 sourcetype을 생성하고 나머지를 입력

원본 선택

컴퓨터를 탐색하거나 파일을 아래의 대상 상자에 끌어놓아 Splunk에 업로드할 파일을 선택합니다. [자세히 알아보기](#)

선택한 파일: 선택한 파일이 없습니다.

파일 선택



데이터 파일은 여기서 업로드 가능합니다.

업로드 가능한 파일의 최대 크기는 500Mb입니다.

데이터 주입 2

데이터 주입 및 검색

■ 해양기상 통계자료 (2019년 3월)

- 데이터 입력 - sourcetype 생성 (marineweather)

Source type: csv **1**

다른 이름으로 저장 **2**

> 타임스탬프

> Delimited settings

> 고급

테이블	형식	페이지당 20개	< 이전	1	2	3	4	5	6	7	8	...	다음 >
	_time	기압	기온	수온	습도	시정	염분	일시	지방청	표지	풍속	풍향	
1	19/03/01 0:03:00.000					7.8		2019-03-01 00:03	부산청	부산항신항 다목적부두			
2	19/03/01 0:03:00.000					6.5		2019-03-01 00:03	부산청	부산항신항 소형선부두 드래			
3	19/03/01 0:04:00.000	1012.6	10.5		64.0								
4	19/03/01 0:04:00.000	1007.1	9.2		59.0								
5	19/03/01 0:04:00.000	1017.1	8.9		66.0								
6	19/03/01 0:04:00.000	1017.8	9.9	11.7	75.0								
7	19/03/01 0:05:00.000	1017.5	10.1	14.1	59.0								
8	19/03/01 0:08:00.000	1017.5	10.2	14.1	60.0	19.0		2019-03-01 00:08	부산청	감천항유도 등부표(랜비)	2.7	164.0	

Source Type 저장

이름

marineweather

설명

범주

구조적

앱

Search & Reporting

취소

저장

■ 해양기상 통계자료 (2019년 3월)

- 데이터 입력 – host 필드 값 지정 (DEMO)

입력 설정

이 데이터 입력에 대해 다음과 같은 추가 매개 변수를 필요에 따라 설정하십시오.

호스트

Splunk 플랫폼이 데이터를 인덱싱할 때 각 이벤트는 "host" 값을 수신합니다. 호스트 값은 이벤트가 발생하는 컴퓨터의 이름이어야 합니다. 사용자가 선택한 입력 유형에 따라 사용 가능한 설정 옵션이 결정됩니다. [자세히 알아보기](#)

- ☒ 상수 값
- ☐ 경로에 대한 정규식
- ☐ 경로 내 세그먼트

host 필드 값

DEMO

인덱스

Splunk 플랫폼은 수신한 데이터를 선택된 인덱스에 이벤트로 저장합니다. 데이터의 source type을 파악하는 데 문제가 있는 경우 "테스트용" 인덱스를 만들어서 사용할 수 있습니다. 테스트용 인덱스를 사용하면 프로덕션 인덱스에 영향을 주지 않고 설정 문제를 해결할 수 있습니다. 나중에 언제든지 이 설정을 변경할 수 있습니다. [자세히 알아보기](#)

인덱스

marineweather ▼

[새 인덱스 만들기](#)

데이터 주입 2

데이터 주입 및 검색

■ 해양기상 통계자료 (2019년 3월)

- 데이터 입력 - 인덱스 생성 (marineweather)
 - 인덱스 만들기

새 인덱스

일반 설정

인덱스 이름

marineweather

인덱스 이름(예: INDEX_NAME)을 설정하십시오. index=INDEX_NAME을 사용하여 검색하십시오.

인덱스 데이터 유형

이벤트

메트릭

저장할 데이터 유형(이벤트 기반 또는 메트릭)

홈 경로

optional

Hot/warm db 경로입니다. 기본적으로 비워 두십시오(\$SPLUNK_DB/INDEX_NAME/db).

Cold 경로

optional

Cold db 경로입니다. 기본적으로 비워 두십시오(\$SPLUNK_DB/INDEX_NAME/colddb).

Thawed 경로

optional

Thawed/resurrected db 경로입니다. 기본적으로 비워 두십시오(\$SPLUNK_DB/INDEX_NAME/thaweddb).

데이터 무결성 검사

Enable

Disable

Splunk에서 데이터 무결성을 목적으로 데이터의 모든 조각에 대해 해시를 계산하도록 하려면 이 옵션을 활성화합니다.

6. 데이터 시각화

■ 해양기상 통계자료

- 필드 확인하기

source="부산청_2019_0301_0307.csv" host="DEMO" index="marineweather" sourcetype="marineweather" 전체 시간 🔍

✓ 19,339개의 이벤트 (20/02/12 16:02:12.000 이전) 이벤트 샘플링 없음 ▼ 작업 || ▢ ↶ ↷ ⬇

상세 모드 ▼

이벤트 (19,339) 패턴 통계 시각화

시간 표시줄 형식 지정 ▼ - 축소 + 선택 항목 확대/축소 x 선택 취소 컬럼당 1시간

리스트 ▾ 형식 페이지당 20개 ▾ < 이전 1 2 3 4 5 6 7 8 ... 다음 >

< 필드 숨기기 ≡ 모든 필드

선택한 필드

- a host 1
- a source 1
- a sourcetype 1

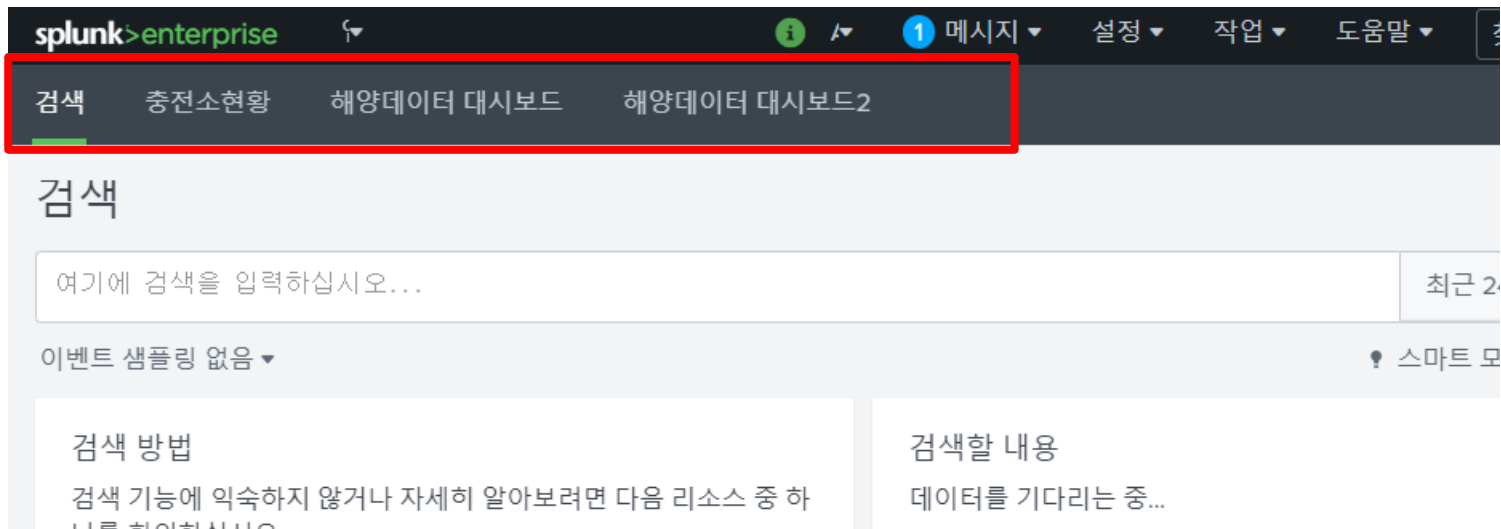
관심 필드

- # date_hour 24
- # date_mday 7
- # date_minute 60
- a date_month 1
- a date_wday 7
- # date_year 1
- a date_zone 1
- a index 1
- # linecount 1
- a punct 10
- a splunk_server 1
- # timeendpos 8

i	시간	이벤트
>	19/03/07 23:59:00.000	부산청, 부산항유도등부표(랜비), 2019-03-07 23:59,,,,,, host = DEMO source = 부산청_2019_0301_0307.csv sourcetype = marineweather
>	19/03/07 23:59:00.000	부산청, 가덕도등대, 2019-03-07 23:59,,,,,, host = DEMO source = 부산청_2019_0301_0307.csv sourcetype = marineweather
>	19/03/07 23:59:00.000	부산청, 목도등대(나무섬등대), 2019-03-07 23:59,,,,,, host = DEMO source = 부산청_2019_0301_0307.csv sourcetype = marineweather
>	19/03/07 23:59:00.000	부산청, 오륙도등대, 2019-03-07 23:59,,,,,, host = DEMO source = 부산청_2019_0301_0307.csv sourcetype = marineweather
>	19/03/07 23:58:00.000	부산청, 부산항신항중앙c호등부표, 2019-03-07 23:58,10.0,,8.5,11.8,,2.1,,1021.1,68.0,19.0 host = DEMO source = 부산청_2019_0301_0307.csv sourcetype = marineweather
>	19/03/07 23:58:00.000	부산청, 부산항신항다목적부두, 2019-03-07 23:58,,,,,15.7,,,, host = DEMO source = 부산청_2019_0301_0307.csv sourcetype = marineweather
>	19/03/07 23:57:00.000	부산청, 부산항신항소형선부두등대, 2019-03-07 23:57,,,,,9.3,,,, host = DEMO source = 부산청_2019_0301_0307.csv sourcetype = marineweather

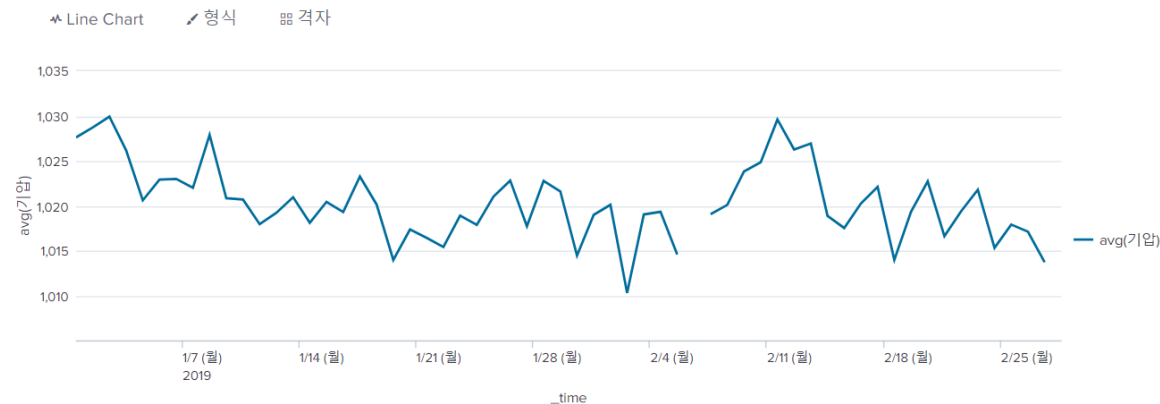
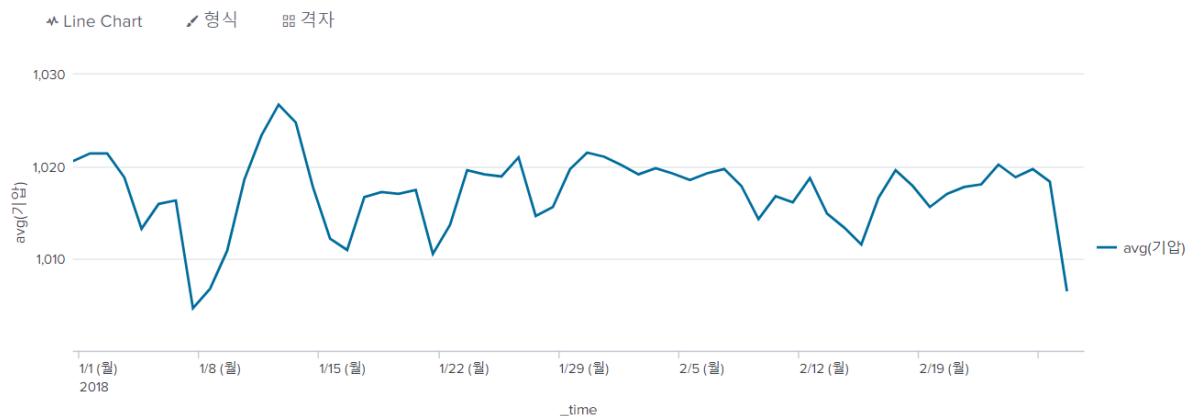
■ 해양기상 통계자료

- 차트 그리기
 - 추가 차트앱 설치
: chart.tgz 설치
 - 차트앱 상단 메뉴 변경해보기 (view name: eco_station, marineweather, marineweather2)



■ 해양기상 통계자료

- 차트 그리기
 - timechart를 이용한 검색 실행해보기
 - 연간 비교해보기(일별 평균 기압: 2018년 1월~2월 VS 2019년 1월~2월)



- 보고서로 저장해 보기

대시보드 작성

대시보드용 시나리오

■ 대시보드 참고

- Edit Drilldown
- 대시보드 - 편집 - 패널 에서 확인

드릴다운 편집기

×

On Click

작업 없음

✓ 작업 없음
검색에 연결
대시보드에 연결
보고서에 연결
사용자 지정 URL에 연결
이 대시보드에 있는 토큰 관리
페이지 내 드릴다운 작업 활성화

취소

적용

드릴다운 편집기

×

On Click

사용자 지정 URL에 연결

URL

예를 들어 /app/search/datasets 또는 https://www.splunk.com 같은 상대 URL 또는 절대 URL을 사용합니다.

☒ 새 탭에서 열기

취소

적용

드릴다운 편집기

×

On Click

이 대시보드에 있는 토큰 관리

<set>, <eval> 및 <unset>을 사용하여 토큰 값을 업데이트할 수 있습니다. 그러면 대시보드와 양식에서 반응 콘텐츠를 만들거나 변경 사항을 표시하는 데 유용할 수 있습니다. [자세히 알아보기](#)

설정

토큰 이름

=

Token value

×

+ 새로 추가

예: form.host = \$click.value2\$ 또는 host = \$row.host\$

취소

적용

7. 대시보드용 시나리오

■ 해양기상 통계자료

- 대시보드 작성
- 토큰을 이용한 동적인 대시보드 만들기
 - 토큰을 이용하여 패널을 동적으로 보여주기
 - 토큰을 처리하기
 - 드릴다운을 통하여 다른 대시보드에 결과값 넘겨주기

대시보드 작성

대시보드용 시나리오

■ 대시보드 완성 예제 1

해양데이터 대시보드

표지

편집

내보내기 ▾

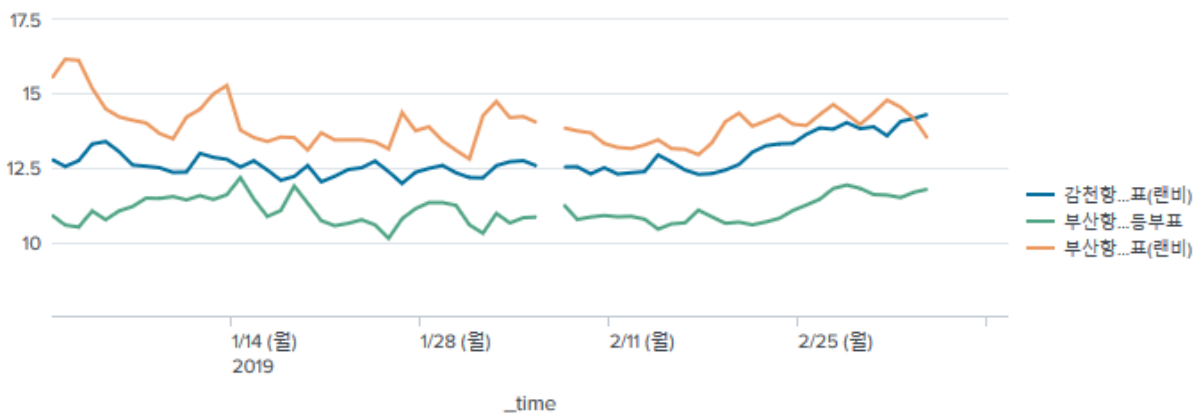
...

전체 ▾

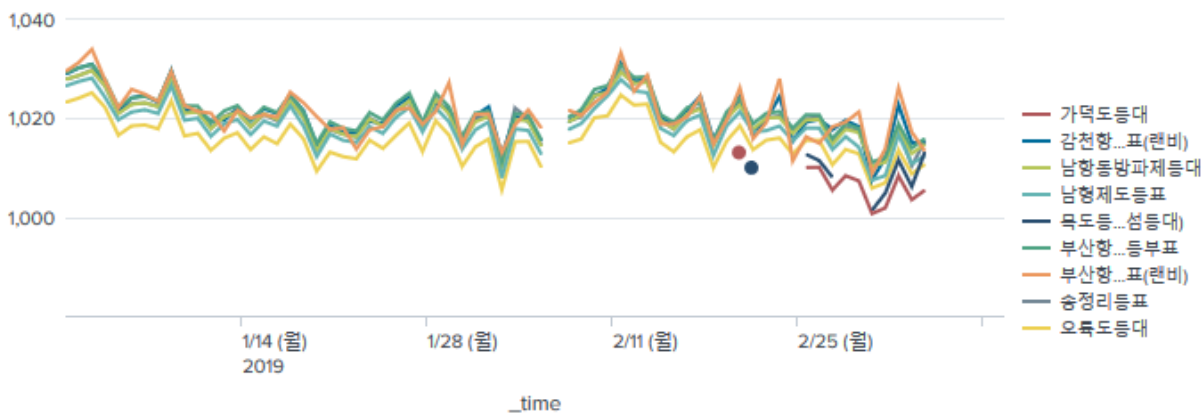
제출

필터 숨기기

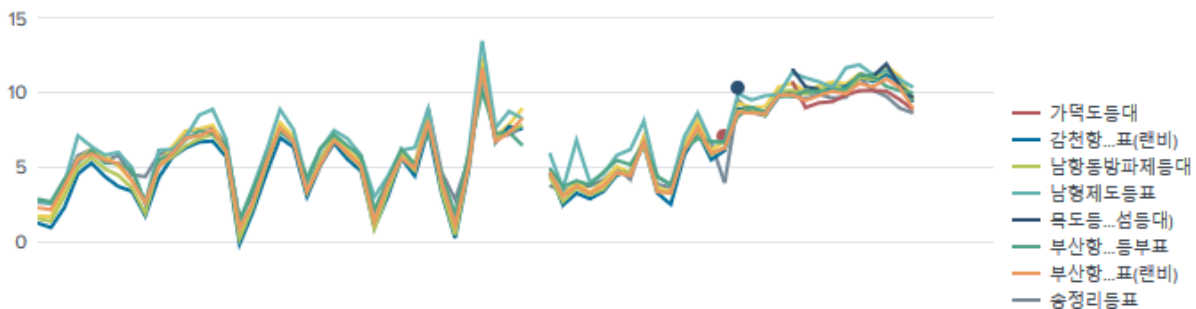
수온평균



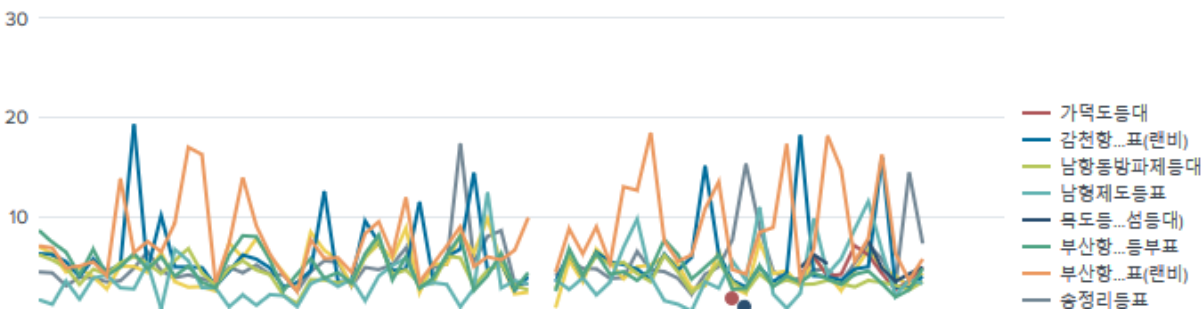
기압평균



기온평균



풍속평균



대시보드 작성

대시보드용 시나리오

■ 대시보드 완성 예제 2

해양데이터 대시보드2

[편집](#)[내보내기 ▼](#)[...](#)

표지

측정값

오버레이필드

시간

감천항유도등부표(... ▼) ×

염분 ×

수온 ×

기압 ×

기온 ×

풍속 ×

습도 ×

기압평균 ×

연간 누계 ▼

제출

필터 숨기기

여러값 비교해보기 (감천항유도등부표(랜비))



감사합니다
