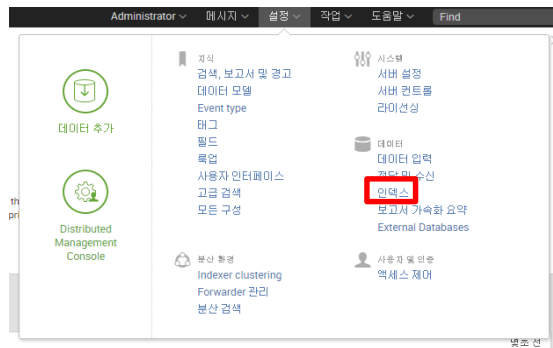




Splunk 데이터 주입

Splunk 데이터 주입

> 인덱스 생성



인덱스

50개 항목 중 1-25 표시

인덱스 이름	전체 인덱스의 최대 크기(MB)
._audit	500,000
._blocksignature	0
._internal	500,000
._introspection	500,000
._thefishbucket	500,000
appmgmt	10,000
bmon	500,000
cisco	500,000
citrix_ns	500,000
dynatrace	500,000
fs	500,000
faa	500,000

새로 추가

인덱스 » 새로 추가

인덱스 설정

인덱스 이름 *

mossplunkbootcamp

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

홈 경로

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

Cold 경로

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

Thawed 경로

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

전체 인덱스의 최대 크기(MB)

500000

전체 인덱스의 최대 크기입니다.

hot/warm/cold 버킷의 최대 크기(MB)

auto

버킷의 최대 대상 크기입니다. 높은 볼륨의 인덱스의 경우 'auto_high_volume'을 입력하십시오.

동결된 아카이브 경로

동결된 버킷 아카이브 경로입니다. Splunk가 동결된 버킷을 자동으로 아카이브하도록 하려면 이 항목을 설정하십시오.

취소

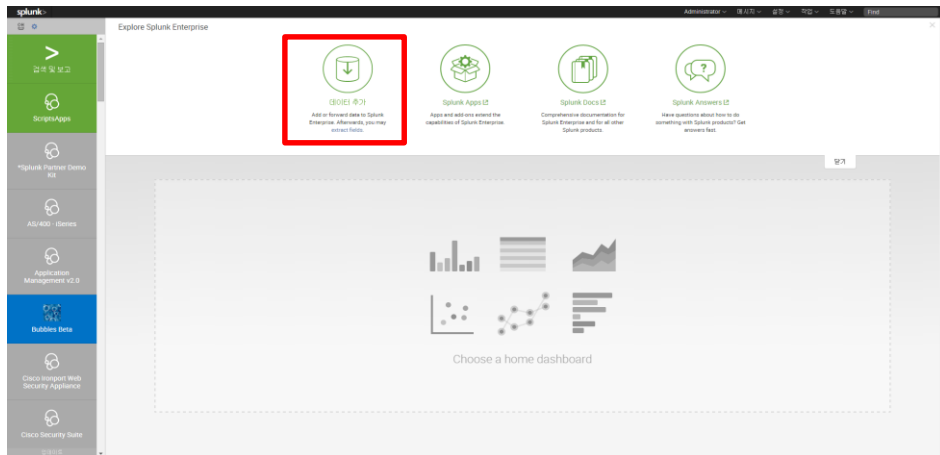
저장

Splunk 데이터 주입

> 데이터 추가 버튼



“Splunk Main 화면” 혹은 네비게이션 바의 “설정> 데이터 추가” 버튼을 누르면 데이터 주입 화면으로 이동합니다.




OR



Splunk 데이터 주입


> 데이터 추가 구성

데이터 추가
How do you want to add data?




upload
files from my computer

Local log files
Local structured files (e.g. CSV)
[Tutorial for adding data](#)



monitor
files and ports on this Splunk indexer

Files - WMI - TCP/UDP - Scripts
Modular inputs for external data sources



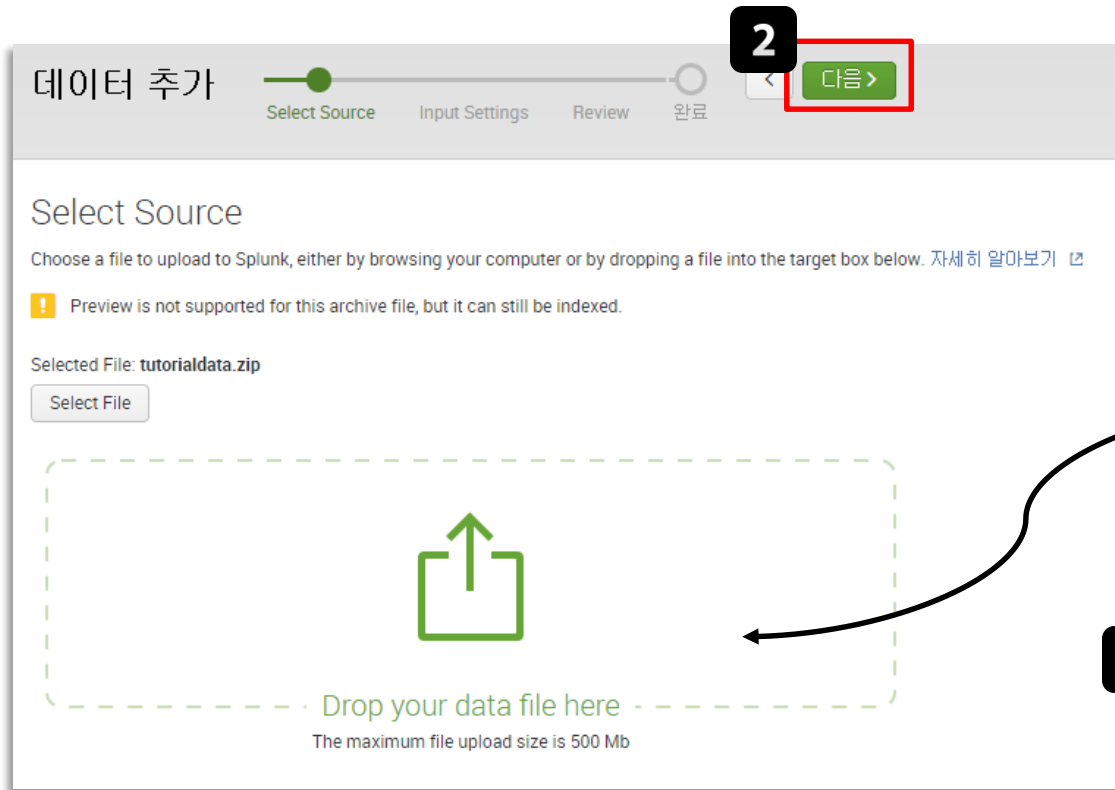
forward
data from Splunk forwarder

Files - TCP/UDP - Scripts
[Help me install the universal forwarder](#)



Splunk 데이터 주입

> 교육용 압축 데이터 파일 추가



1 Drag and drop



Splunk 데이터 주입

> Index 지정

데이터 추가

2

Review >

Select Source Input Settings Review 완료

Input Settings

Optionally set additional input parameters for this data input as follows:

Sourcetype

The source type is one of the default fields that Splunk assigns to all incoming data. It tells Splunk what kind of data you've got, so that Splunk can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

자동 선택 수동

Host

When Splunk indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates, and can be defined based either on the path to the source data, a regular expression, or a number that represents a segment of a file path. [자세히 알아보기](#)

Constant value Regular expression on path Segment in path

호스트 필드 값 MSDN-SPECIAL

인덱스

Splunk stores incoming data as events in the selected index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [자세히 알아보기](#)

1 Index 지정

인덱스 mossplunkbootcamp Create a new index 새로 고침

Splunk 데이터 주입

> 주입된 데이터 확인

데이터 추가

Select Source Input Settings **Review** 완료

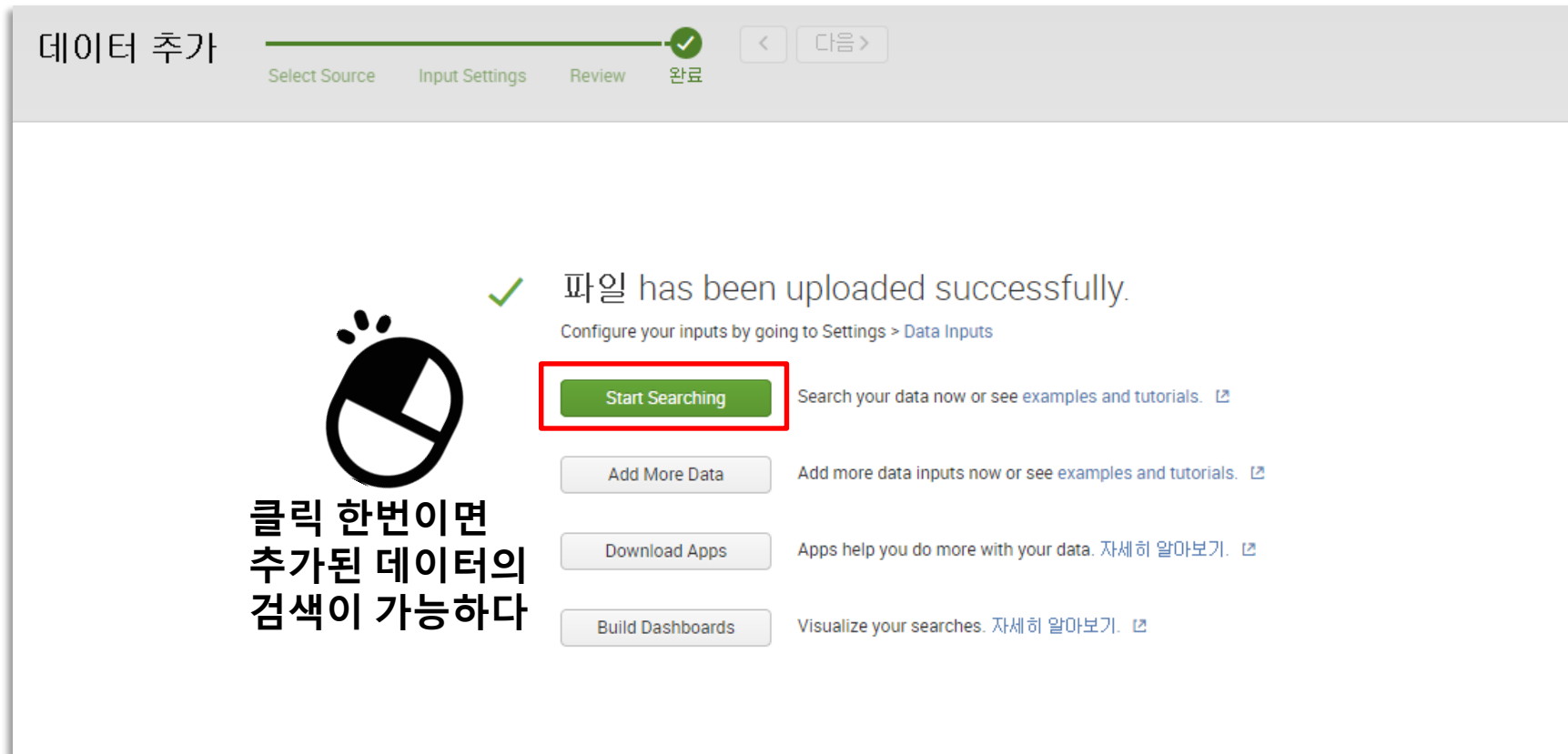
< 제출 >

Review

Input Type	Uploaded File
파일 이름	tutorialdata.zip
Sourcetype	자동
Host	MSDN-SPECIAL
인덱스	mossplunkbootcamp

Splunk 데이터 주입

> “검색 시작” 버튼을 통한 자동 검색



Splunk 데이터 주입

> 검색 창에서 이벤트 확인

The screenshot shows the Splunk web interface. At the top, there's a navigation bar with 'splunk>' and various menu items. Below that, a search bar is highlighted with a red box, containing the query: `source="tutorialdata.zip:*" host="MSDN-SPECIAL" index="mossplunkbootcamp"`. Below the search bar, there's a summary bar indicating 109,864 events. The main content area shows a list of events with columns for time, host, and event details. The interface is in Korean.

i	시간	이벤트
>	14/12/14 18:24:02.000	[14/Dec/2014:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = MSDN-SPECIAL source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	14/12/14 18:23:46.000	[14/Dec/2014:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = MSDN-SPECIAL source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	14/12/14 18:23:31.000	[14/Dec/2014:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = MSDN-SPECIAL source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	14/12/14 18:22:59.000	[14/Dec/2014:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = MSDN-SPECIAL source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	14/12/14 18:22:48.000	[14/Dec/2014:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740 host = MSDN-SPECIAL source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales
>	14/12/14 18:22:32.000	[14/Dec/2014:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834 host = MSDN-SPECIAL source = tutorialdata.zip:\vendor_sales\vendor_sales.log sourcetype = vendor_sales/vendor_sales

Splunk 데이터 주입

> 데이터가 보이지 않을 때

설정>엑세스 제어>역할>admin에서 "내부 인덱스가 아닌 모든 인덱스"를 추가해 줍니다.

기본적으로 검색된 인덱스

지정된 인덱스가 없을 경우 기본적으로 검색할 인덱스를 설정하십시오. 이 역할을 가진 사용자는 index= (예: "index=special_index")를

사용 가능한 인덱스

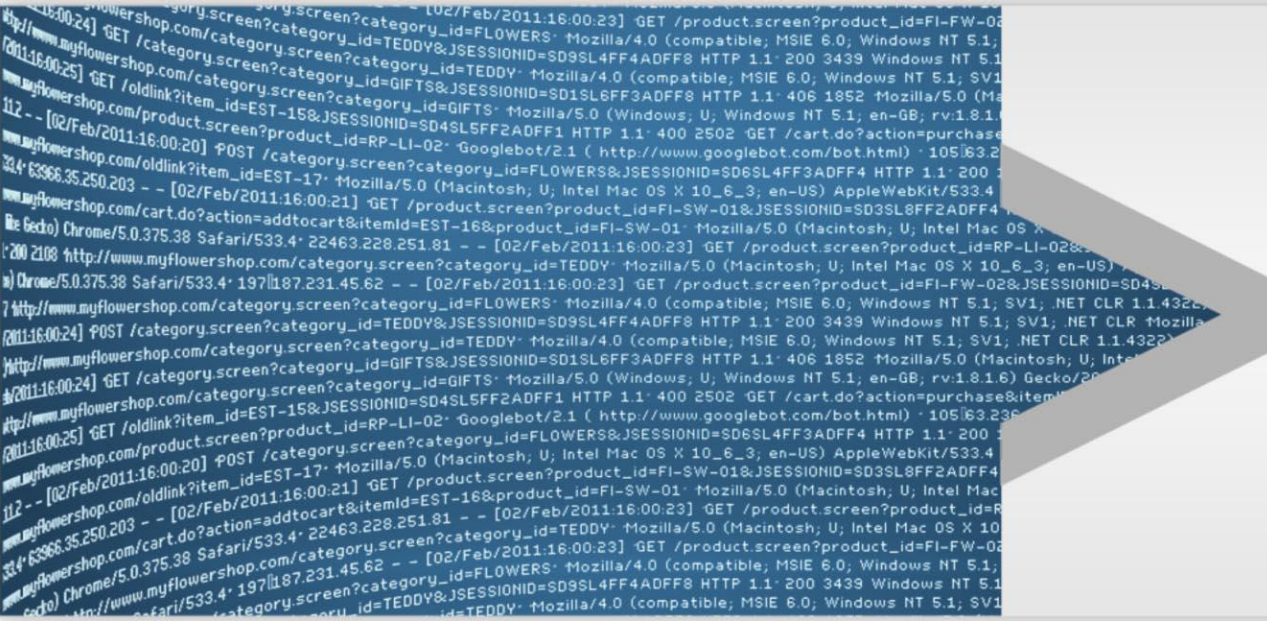
- ☒ 내부 인덱스가 아닌 모든 인덱스
- ☐ 모든 내부 인덱스
- ☒ _audit
- ☒ _blocksignature
- ☒ _internal

모두 추가 »

선택된 인덱스

« 모두 지우기

- ☒ 내부 인덱스가 아닌 모든 인덱스
- ☐ 모든 내부 인덱스

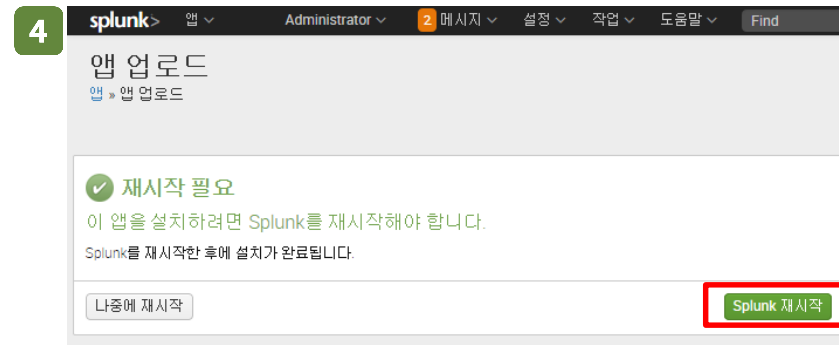
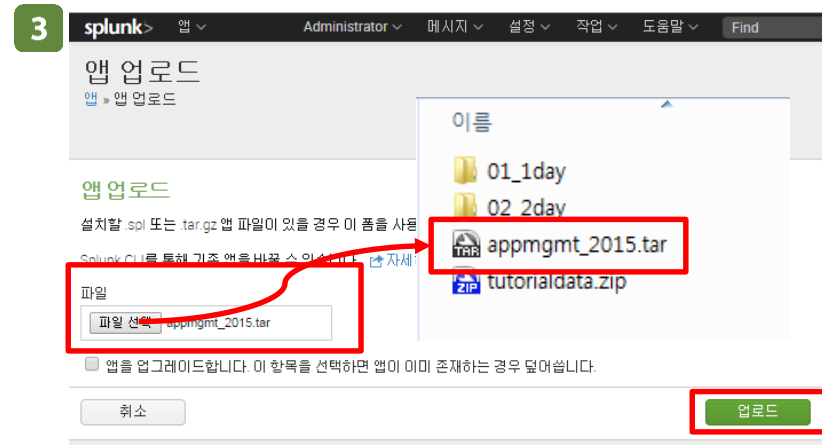
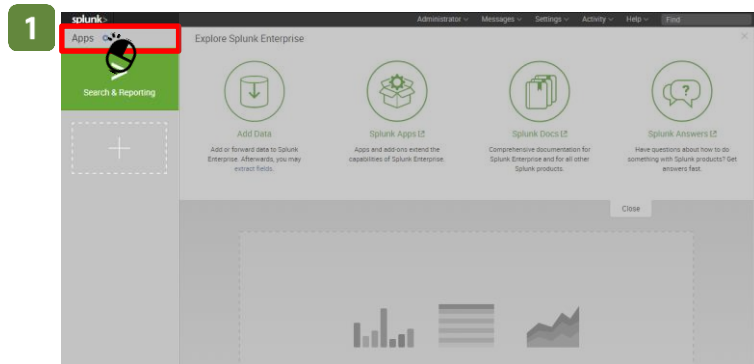


Splunk Appmgmt Apps 설치



Appmgmt Apps 설치

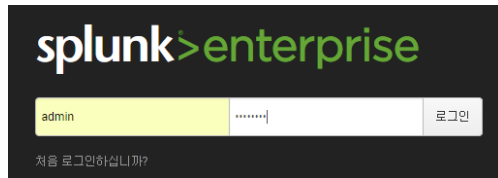
> Apps 설치



Appmgmt Apps 설치

> Apps 설치

검색 창에 Index=appmgmt를 입력하여 이벤트를 확인합니다.



The screenshot shows the Splunk search interface with the search bar containing 'index=appmgmt'. The results show 182,427 events. The interface includes a search bar, a results table, and a sidebar with filters.

Search results table:

i	시간	이벤트
>	15/02/05 9:15:28.192	131.178.233.243 - - [05/Feb/2015 00:15:28:192] "GET /product.screen?product_id=K9-BD-01&JSESSIONID=SD4SL3FF5ADFF3 HTTP 1.1" 404 1332 "http://shop.gourmet-shop.com/category.screen?category_id=BAKING" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 771 host = apache-1.splunk.com source = /opt/apache/log/access_combined.log sourcetype = access_combined
>	15/02/05 9:15:28.192	131.178.233.243 - - [05/Feb/2015 00:15:28:192] "GET /product.screen?product_id=K9-BD-01&JSESSIONID=SD4SL3FF5ADFF3 HTTP 1.1" 404 1332 "http://shop.gourmet-shop.com/category.screen?category_id=BAKING" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 771 host = apache-1.splunk.com source = C:\Program Files\Apache\Logs\access_combined.log sourcetype = access_combined
>	15/02/05 9:15:28.183	12.130.60.5 - - [05/Feb/2015 00:15:28:183] "GET /category.screen?category_id=TRUFFLES&JSESSIONID=SD2SL8FF7ADFF10 HTTP 1.1" 503 997 "http://shop.gourmet-shop.com/product.screen?product_id=K9-BD-01" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; .NET CLR 1.1.4322)" 299