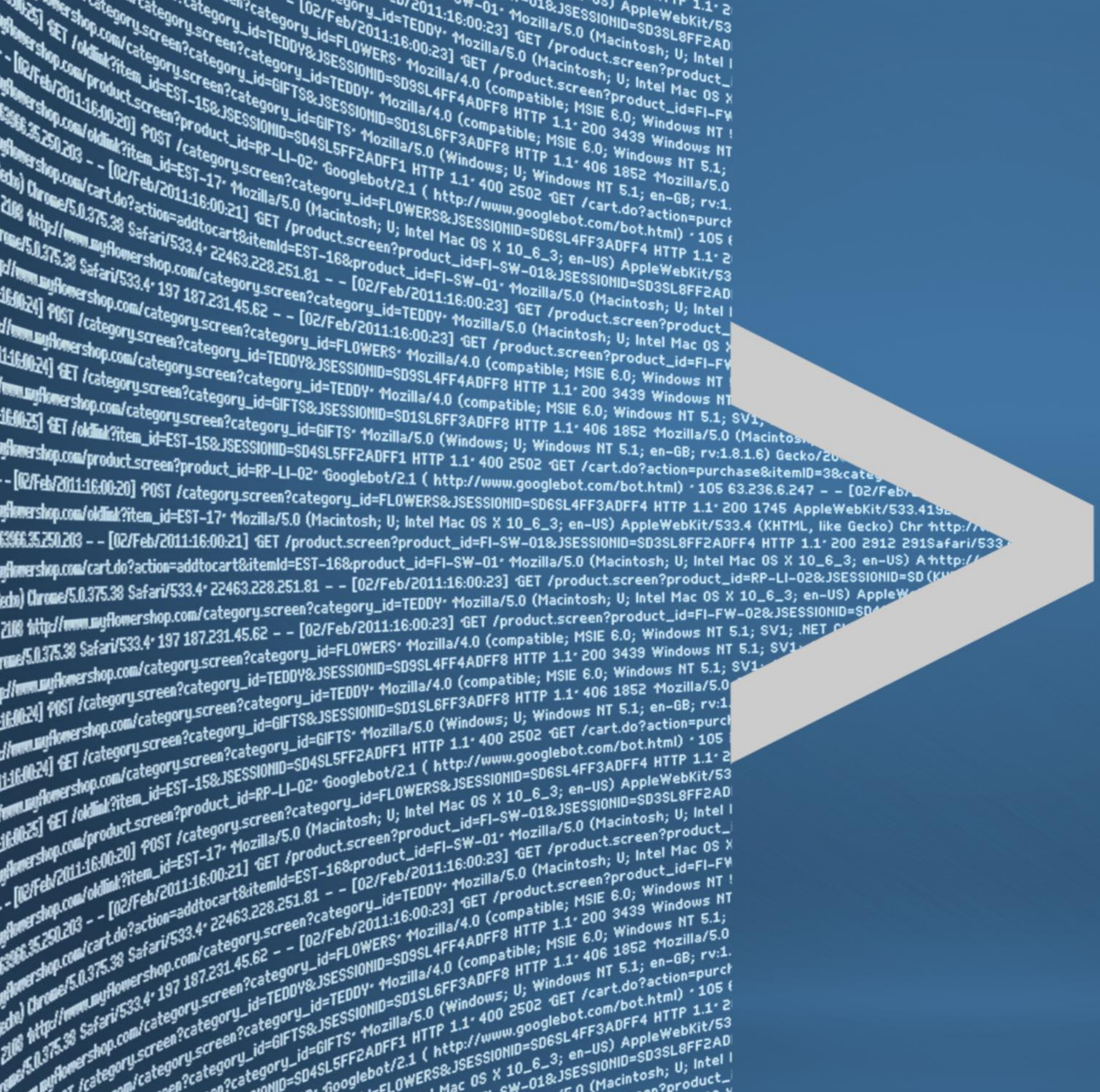
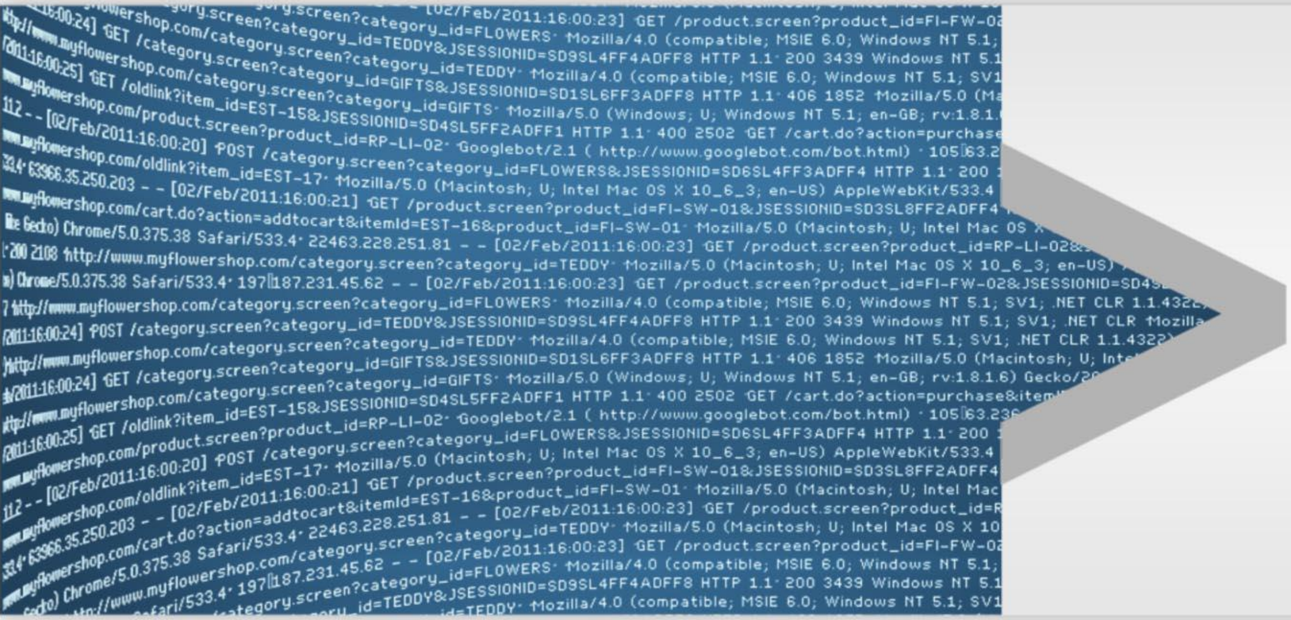


Splunk Bootcamp User Session 1 Day (V6.2)

MOS

MOS Asia Inc.



Splunk
Windows Version Install Guide

Install Guide

1. 신규 Splunk 버전을 설치합니다.

   - Splunk_Software 폴더의 Splunk-6.x.x-xxxx-release.msi 파일을 PC사양에 맞춰 설치합니다.

     * 64 Bit : splunk-6.x.x-xxxxxx-x64-release.msi

     * 32 Bit : splunk-6.x.x-xxxxxx-x86-release.msi

2. Splunk Instance Start

   - 윈도우 CMD 프롬프트로 들어갑니다.

     ```
     * Windows 64bit    : cd C:\Program Files\Splunk\bin
     * Windows 32bit    : cd C:\Program Files\Splunk\bin
     ```

   - Splunk를 시작 합니다. “ splunk.exe start “ 입력

Install Guide

3. 설치된 신규 인스턴스로 Splunk 시작!

   > 웹 브라우저로 http://127.0.0.1:8000 혹은 localhost:8000으로 접근하여
   ID = admin / PW = changeme 로 로그인합니다.

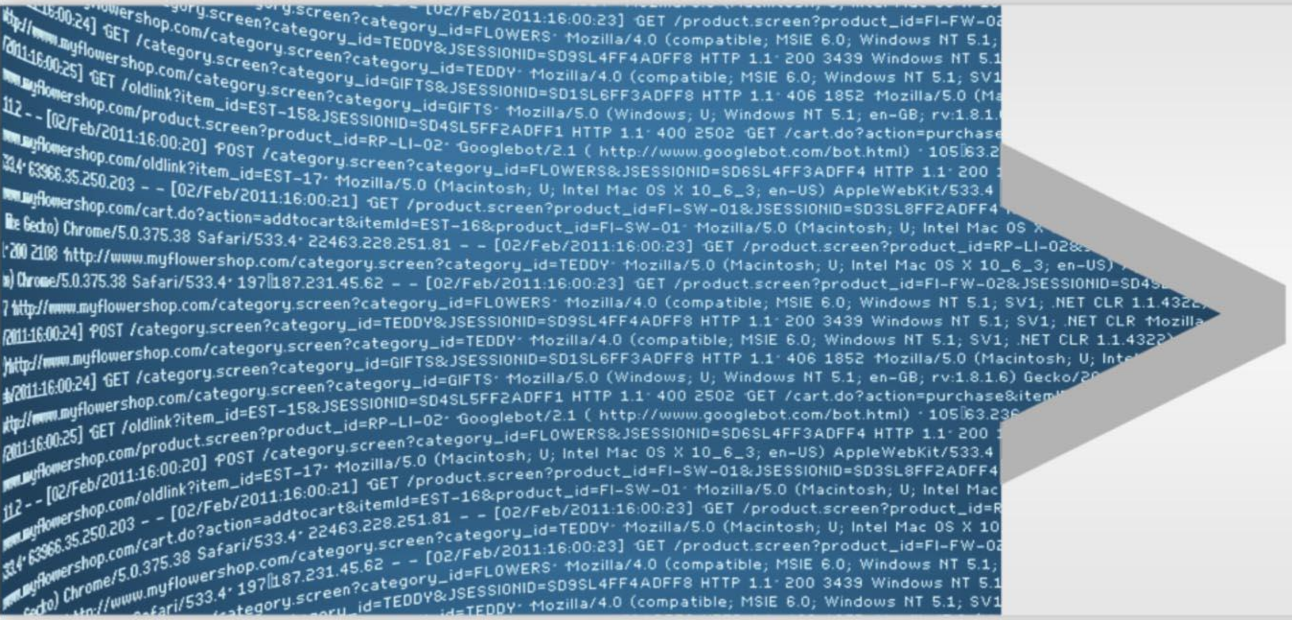
4. Browser 권장 : IE는 인터페이스 호환성 문제가 발생할 가능성이 있어
   Chrome, FireFox 사용을 **권장**합니다.
   IE는 11버전부터 **권장**합니다.

Install Guide

5. Splunk가 설치 되지 않을 시!

- 윈도우에 따라서 설치가 되지 않을 시 다음의 zip파일을 압축 해제 후에 옮겨서 실행합니다.
  - splunk-6.x.x-xxxxxx-x64-release.zip을 압축 해제 후 C:\Program Files에 splunk이름으로 넣습니다.
  - splunk_service_create.bat를 관리자 권한으로 실행합니다.
  - 제어판 – 서비스에서 splunkd 서비스 등록 확인합니다.
- 윈도우 CMD 프롬프트로 들어갑니다.

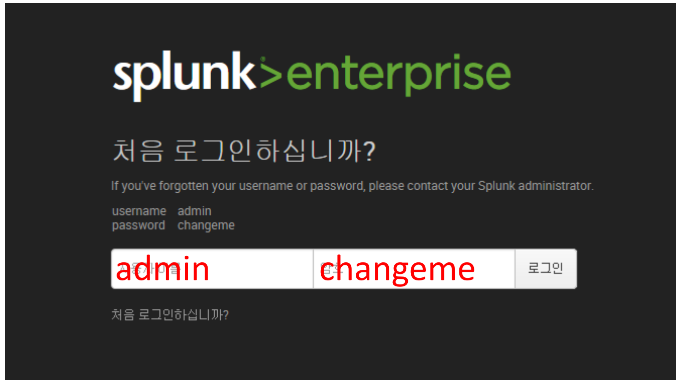
  * Windows CMD : cd C:\Program Files\Splunk\bin
- Splunk를 시작 합니다. “ splunk.exe start “ 입력



Splunk UI 소개

Splunk UI 소개

>로그인 화면



splunk>enterprise

처음 로그인하십니까?

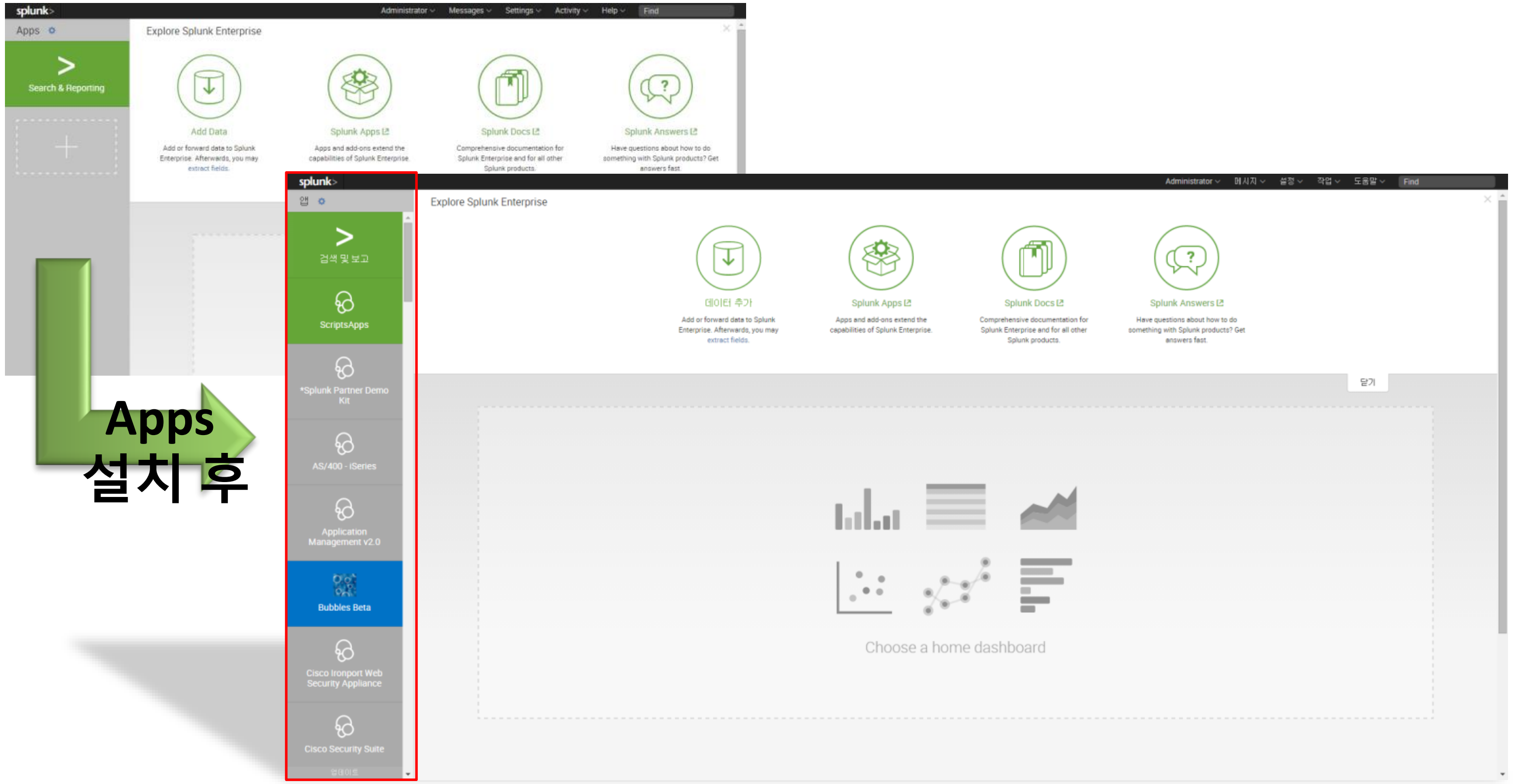
If you've forgotten your username or password, please contact your Splunk administrator.

username admin
password changeme

admin | changeme | 로그인

처음 로그인하십니까?

>메인 화면



Add or forward data to Splunk Enterprise. Afterwards, you may extract fields.

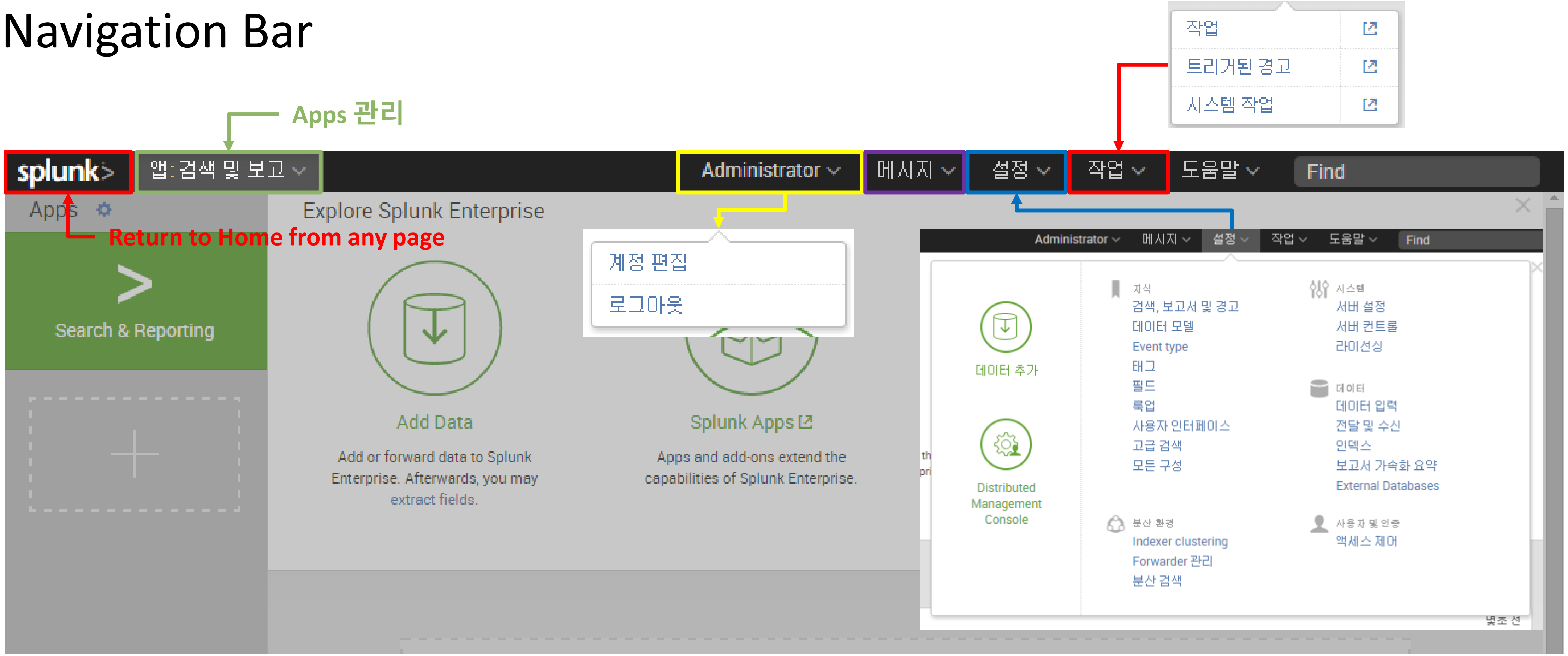
Apps and add-ons extend the capabilities of Splunk Enterprise.

Comprehensive documentation for Splunk Enterprise and for all other Splunk products.

Have questions about how to do something with Splunk products? Get answers fast.

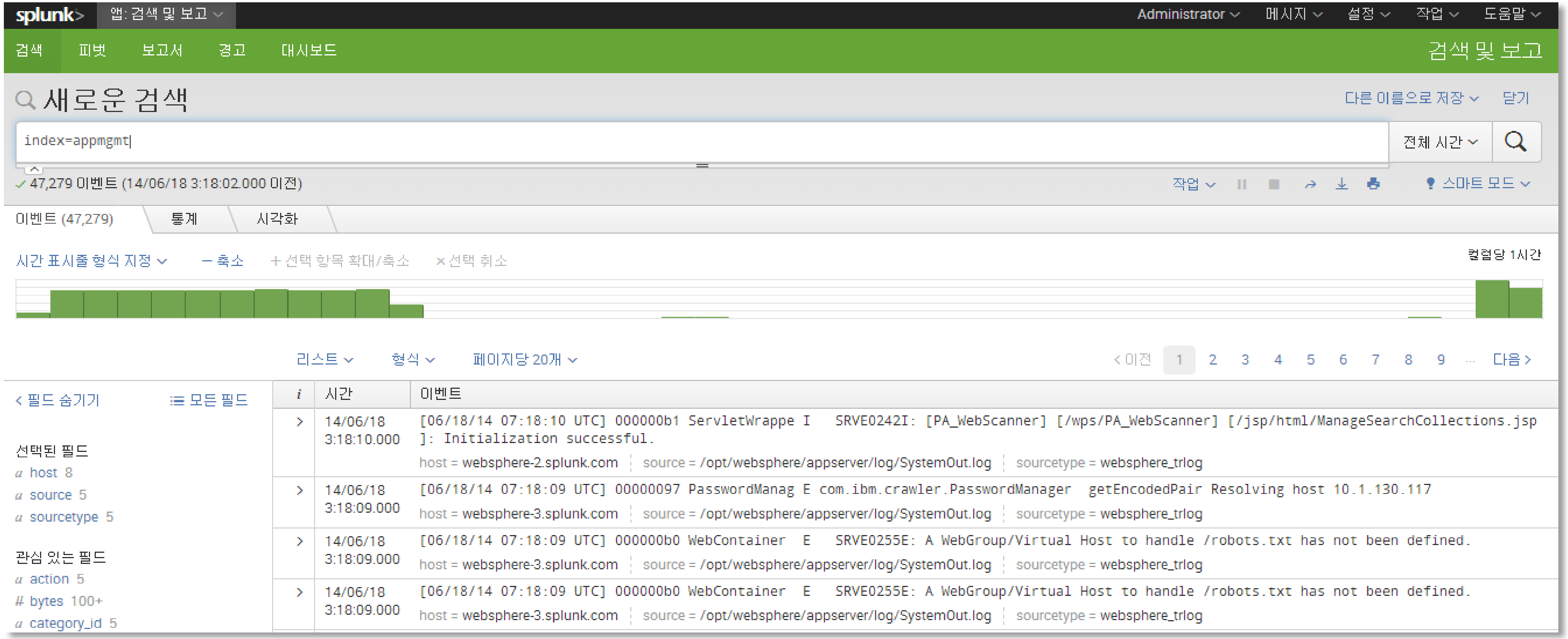
Splunk UI 소개

> Navigation Bar



Splunk UI 소개

> SEARCH 화면



```
index=appmgmt
```

✓ 47,279 이벤트 (14/06/18 3:18:02.000 이전)

선택된 필드
- a host 8
- a source 5
- a sourcetype 5

관심 있는 필드
- a action 5
- # bytes 100+
- a category_id 5

시간	이벤트

14/06/18 3:18:10.000	`[06/18/14 07:18:10 UTC] 000000b1 ServletWrappe I   SRVE0242I: [PA_WebScanner] [/wps/PA_WebScanner] [/jsp/html/ManageSearchCollections.jsp ]: Initialization successful.`
	host = websphere-2.splunk.com ¦ source = /opt/websphere/appserver/log/SystemOut.log ¦ sourcetype = websphere_trlog

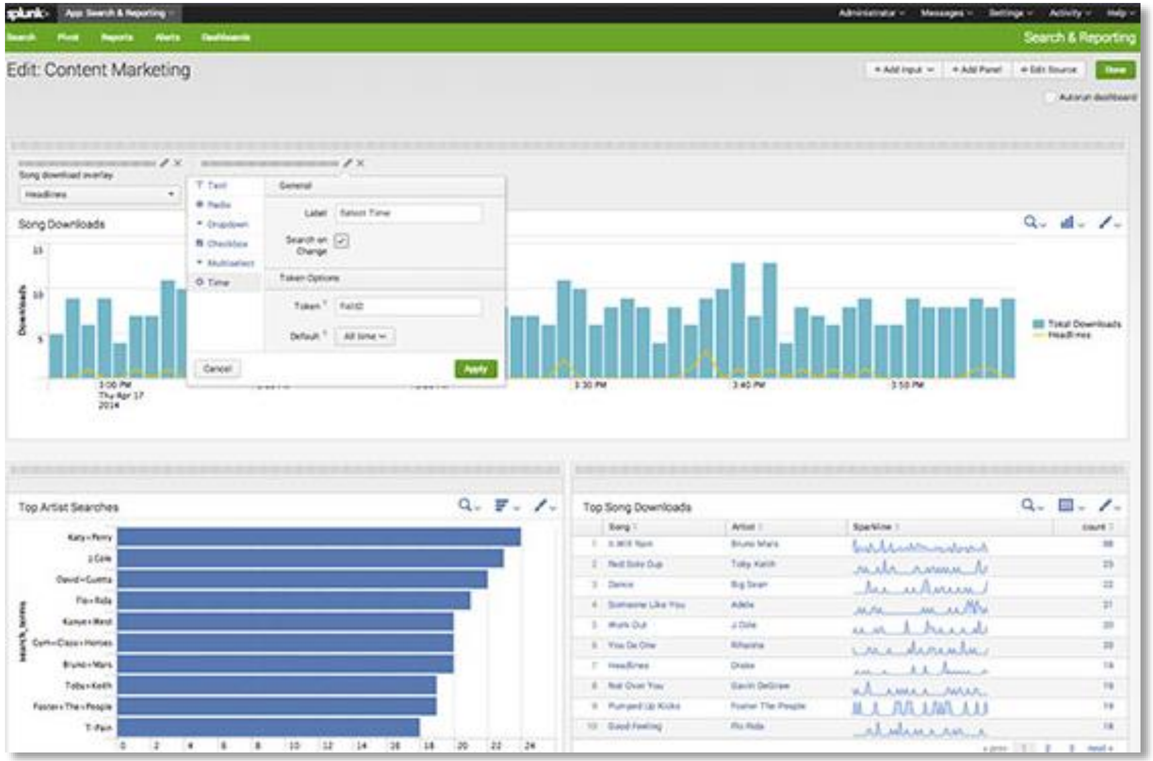
14/06/18 3:18:09.000	`[06/18/14 07:18:09 UTC] 00000097 PasswordManag E com.ibm.crawler.PasswordManager  getEncodedPair Resolving host 10.1.130.117`
	host = websphere-3.splunk.com ¦ source = /opt/websphere/appserver/log/SystemOut.log ¦ sourcetype = websphere_trlog

14/06/18 3:18:09.000	`[06/18/14 07:18:09 UTC] 000000b0 WebContainer  E   SRVE0255E: A WebGroup/Virtual Host to handle /robots.txt has not been defined.`
	host = websphere-3.splunk.com ¦ source = /opt/websphere/appserver/log/SystemOut.log ¦ sourcetype = websphere_trlog

14/06/18 3:18:09.000	`[06/18/14 07:18:09 UTC] 000000b0 WebContainer  E   SRVE0255E: A WebGroup/Virtual Host to handle /robots.txt has not been defined.`
	host = websphere-3.splunk.com ¦ source = /opt/websphere/appserver/log/SystemOut.log ¦ sourcetype = websphere_trlog

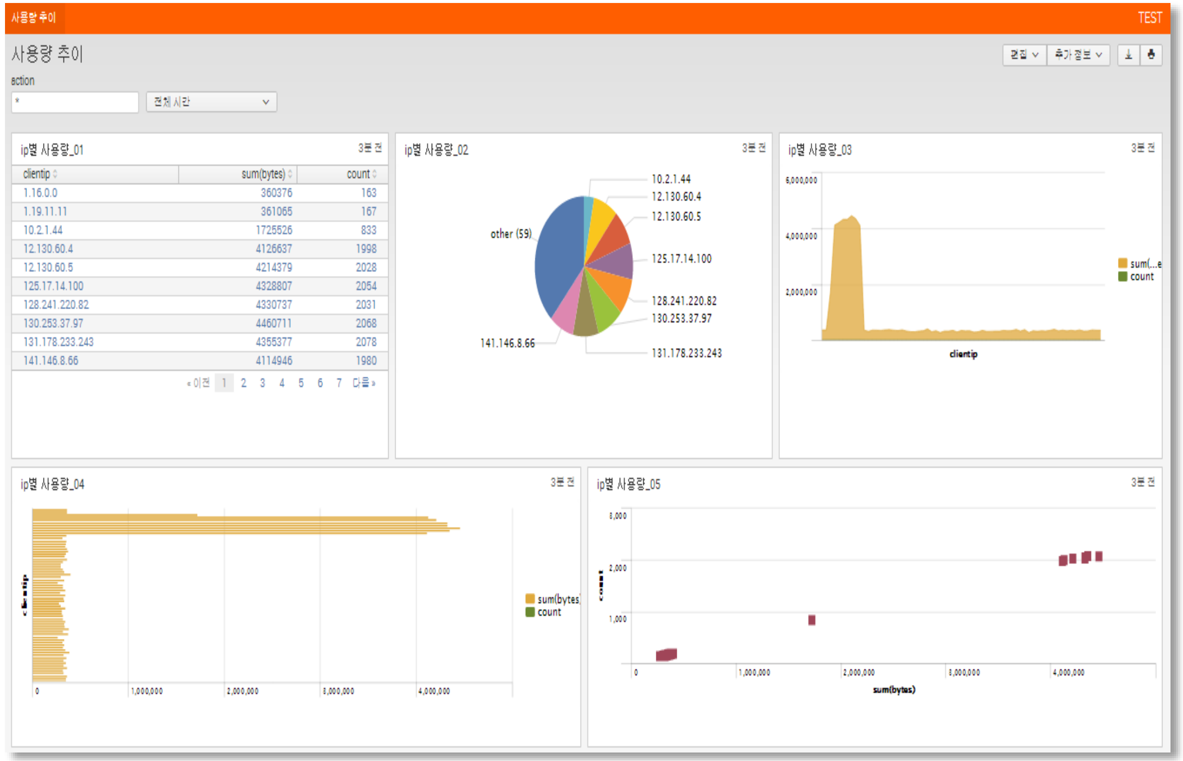
Splunk UI 소개

> DASHBOARD 화면



Top Song Downloads

	Song	Artist	Sparkline	count
1	It Will Rain	Bruno Mars		38
2	Red Solo Cup	Toby Keith		25
3	Dance	Big Sean		22
4	Someone Like You	Adele		21
5	Work Out	J.Cole		20
6	You Da One	Rihanna		20
7	Headlines	Drake		19
8	Not Over You	Gavin DeGraw		19
9	Pumped Up Kicks	Foster The People		19
10	Good Feeling	Flo Rida		18



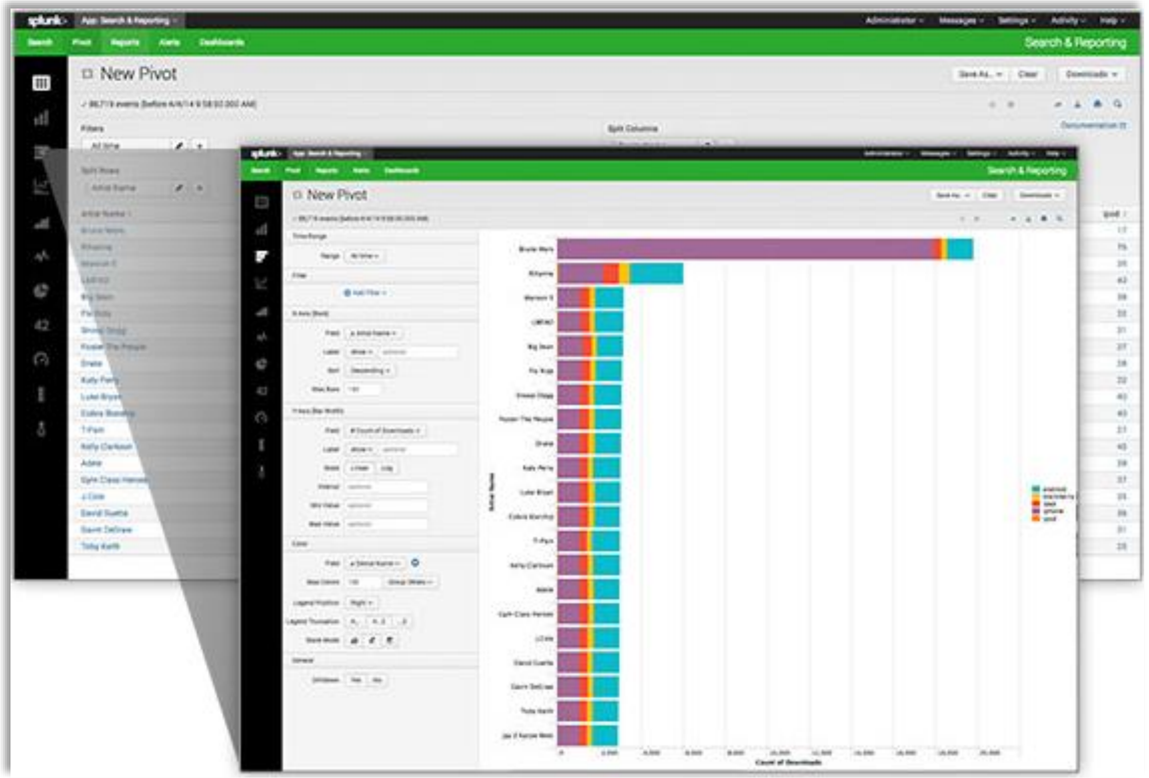
ip별 사용량_01 3분 전

clientip	sum(bytes)	count
1.16.0.0	360376	163
1.19.11.11	361065	167
10.2.1.44	1725526	833
12.130.60.4	4126637	1998
12.130.60.5	4214379	2028
125.17.14.100	4328807	2054
128.241.220.82	4330737	2031
130.253.37.97	4460711	2068
131.178.233.243	4355377	2078
141.146.8.66	4114946	1980

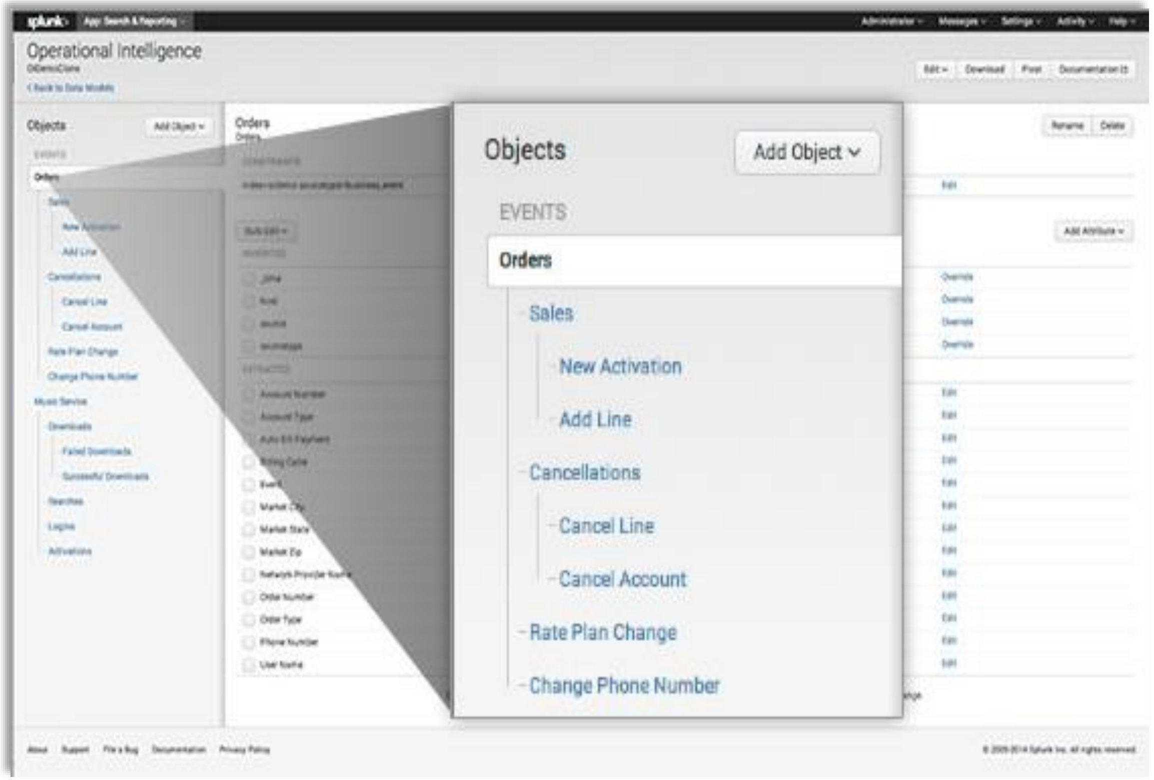
« 이전 1 2 3 4 5 6 7 다음 »

Splunk UI 소개

> PIVOT 화면



> DATA MODEL



splunk>
App: Search & Reporting
Operational Intelligence
Objects
Add Object
EVENTS
Orders
Sales
New Activation
Add Line
Cancellations
Cancel Line
Cancel Account
Rate Plan Change
Change Phone Number
Rename
Delete
Add Attribute