

splunk® > 실습

Splunk 웹 서버 주소

http://<EC2 인스턴스 IP>:8000

admin의 비밀번호
로 변경 해주세요.

- 아이디 : admin
- 비밀번호 : changeme

Main 화면

splunk>


Administrator ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾ 찾기

앱 ⚙

>
검색 및 보고


+
새 앱 추가

Explore Splunk Enterprise ×




Product Tours

New to Splunk? Take a tour to help you on your way.




데이터 추가

Add or forward data to Splunk Enterprise. Afterwards, you may **필드 추가**.



데이터 탐색


데이터를 탐색하고 Hunk가 해당 데이터를 파싱하는 방식을 정의합니다.



Splunk 앱

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

달기



홈 대시보드 선택

데이터 수집

Main 화면

splunk> Administrator ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾ 찾기


앱 ⚙

>
검색 및 보고

+


Explore Splunk Enterprise

×




Product Tours

New to Splunk? Take a tour to help you on your way.




데이터 추가

Add or forward data to Splunk Enterprise. Afterwards, you may **필드 추가**.



데이터 탐색


데이터를 탐색하고 Hunk가 해당 데이터를 파싱하는 방식을 정의합니다.



Splunk 앱

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

닫기



홈 대시보드 선택


데이터 추가

- 업로드 : 웹서버 상에서 로컬에 있는 파일을 올릴 때 사용
- 모니터 : 소켓 통신 / Script / 파일 Tailing으로 Splunk 자체에서 데이터가 업데이트 되었는지 확인 해서 수집
- 포워딩 : Forwarder (Splunk 수집기)를 통해 수집

splunk> 앱 ▾ Administrat... ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾


데이터 추가

어떤 방법으로 데이터를 추가하시겠습니까?




업로드
내 컴퓨터의 파일

로컬 로그 파일
로컬에 있는 정형 파일(예: CSV)
[데이터 추가에 관한 튜토리얼](#)



모니터
이 Splunk 인덱서의 파일 및 포트

파일 - WMI - TCP/UDP - 스크립트
외부 데이터 원본에 대한 모듈화 입력



포워딩
Splunk 포워더의 데이터

파일 - TCP/UDP - 스크립트
[유니버설 포워더 설치 도움말](#)

Tutorial Data Download

- Wiki : <https://github.com/assistbig/bigdata/wiki/Tools#splunk>

Splunk

- Splunk Document : [Link](#)
- Splunk Tutorial
 - 자료 : Update 예정
 - Tutorial Data
 - Web Data : [\[Download\]](#)
 - Lookup Data : [\[Download\]](#)
 - Youtube - Basic Search Tutorial [\[Link\]](#)
 - Youtube - Creating Dashboard Tutorial [\[Link\]](#)
- Splunk Enterprise 6.4 Download (wget URL)

```
wget -O splunk-6.4.0-f2c836328108-Linux-x86_64.tgz 'https://www.splunk.com/bin/splu
```

Data Upload



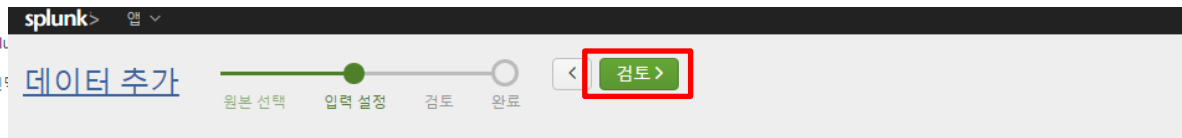
원본 선택

컴퓨터를 탐색하거나 파일을 아래의 대상 상자에 끌어놓아 Splunk에 업로드합니다.

미리보기는 이 아카이브 파일에 대해 지원되지 않지만, 인덱싱된 데이터는 검색할 수 있습니다.

선택된 파일: tutorialdata.zip

파일 선택



입력 설정

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



데이터 파일을 여기

업로드 가능한 파일의 최대 크기

Source type

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.

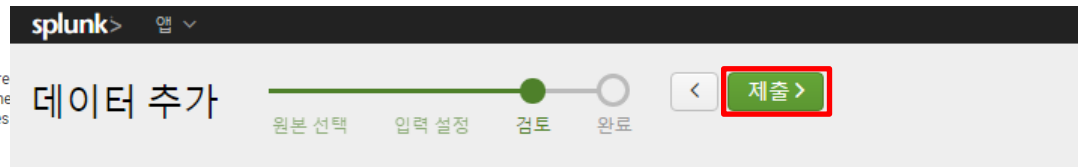
자동

선택

새로 만...

Host

When Splunk indexes data, each event receives a value that should be the name of the machine that generated the data. The type of input you choose determines the options available. [자세히 알아보기](#)



데이터 추가

원본 선택

입력 설정

검토

완료

제출

인덱스

Splunk stores incoming data as events in an index. The index is a destination for a source type for your data. A sandbox index is a configuration without impacting production. [자세히 알아보기](#)

검토

| | |
|-------------|------------------|
| 입력 유형 | 업로드된 파일 |
| 파일 이름 | tutorialdata.zip |
| Source Type | 자동 |
| Host | ip-172-31-8-33 |
| 인덱스 | 기본값 |

Tutorial Data

- **access.log : Web Access data (buttercupgames 가상의 웹사이트)**

```
175.44.24.82 - - [22/Feb/2016:18:44:40] "POST /product.screen?productId=WC-SH-A01&JSESSIONID=SD7SL9FF5ADFF5066 HTTP 1.1" 200 3067 "http://www.buttercupgames.com/product.screen?productId=WC-SH-A01" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 307
142.233.200.21 - - [22/Feb/2016:19:20:13] "GET show.do?productId=SF-BVS-01&JSESSIONID=SD6SL8FF4ADFF5218 HTTP 1.1" 404 1329 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-13" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" 674
```

- **secure.log : security data**

```
Mon Feb 22 2016 00:15:06 mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0)
Mon Feb 22 2016 00:15:06 mailsv1 sshd[3759]: Failed password for nagios from 194.8.74.23 port 3769 ssh2
Mon Feb 22 2016 00:15:08 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351
```

- **Vendor sales data**

```
[22/Feb/2016:18:23:07] VendorID=5037 Code=C AcctID=5317605039838520
[22/Feb/2016:18:23:22] VendorID=9108 Code=A AcctID=2194850084423218
[22/Feb/2016:18:23:49] VendorID=1285 Code=F AcctID=8560077531775179
[22/Feb/2016:18:23:59] VendorID=1153 Code=D AcctID=4433276107716482
```

SPL 실습

SPL 실습 – Keyword와 Field를 활용한 기본 검색

1. Keyword 검색

- buttercupgames

2. 논리 검색 (error, fail, failure, failed, severe 검색)

- buttercupgames (error OR fail* OR severe)

3. Field로 검색

- sourcetype="access_*

4. 구매 성공한 건에 대한 로그 검색

- sourcetype=access_* status=200 action=purchase

5. 구매 실패 건에 대한 로그 검색

- sourcetype=access_* status!=200 action=purchase

6. 접근 에러건에 대한 로그 검색

- (error OR fail* OR severe) OR (status=404 OR status=500 OR status=503)

SPL 실습 - 기본 통계 실습

1. 데이터 수 Count
 - `index=main | stats count`
2. Sourcetype 별 데이터 수 Count
 - `index=main | stats count by sourcetype`
3. 시간 흐름별 데이터 수 Count
 - `index=main | timechart count`
 - `index=main | timechart span=1h count`
4. 여러 통계를 한번에 하기
 - `index=main sourcetype=access_* status=200 action=purchase clientip=87.194.216.51 | stats count, dc(productId), values(productId) by clientip`
5. Product Category ID별 기본 통계 (top / rare)
 - `index=main sourcetype=access_* status=200 action=purchase | top categoryId`
 - `index=main sourcetype=access_* status=200 action=purchase | rare categoryId`
6. IP별 접근 Product Category 순위 조회
 - `index=main sourcetype=access_* status=200 action=purchase | top categoryId by clientip`
7. IP별 접근 Product Category 순위 조회 (상위 2위까지)
 - `index=main sourcetype=access_* status=200 action=purchase | top limit=2 categoryId by clientip`

SPL 실습 - 필드 필터링, 수정 추가

1. 원하는 필드만 테이블로 만들기

- `index=main sourcetype=access_combined_wcookie | table _time, clientip, categoryId, JSESSIONID`

2. 원하는 필드만 남겨두거나 제거하기

- `index=main sourcetype=access_combined_wcookie | table _time, clientip, categoryId, JSESSIONID | fields+ _time, clientip`
- `index=main sourcetype=access_combined_wcookie | table _time, clientip, categoryId, JSESSIONID | fields- categoryId`

3. Eval을 활용해 데이터 처리 (참고 : [Splunk Eval Functions](#))

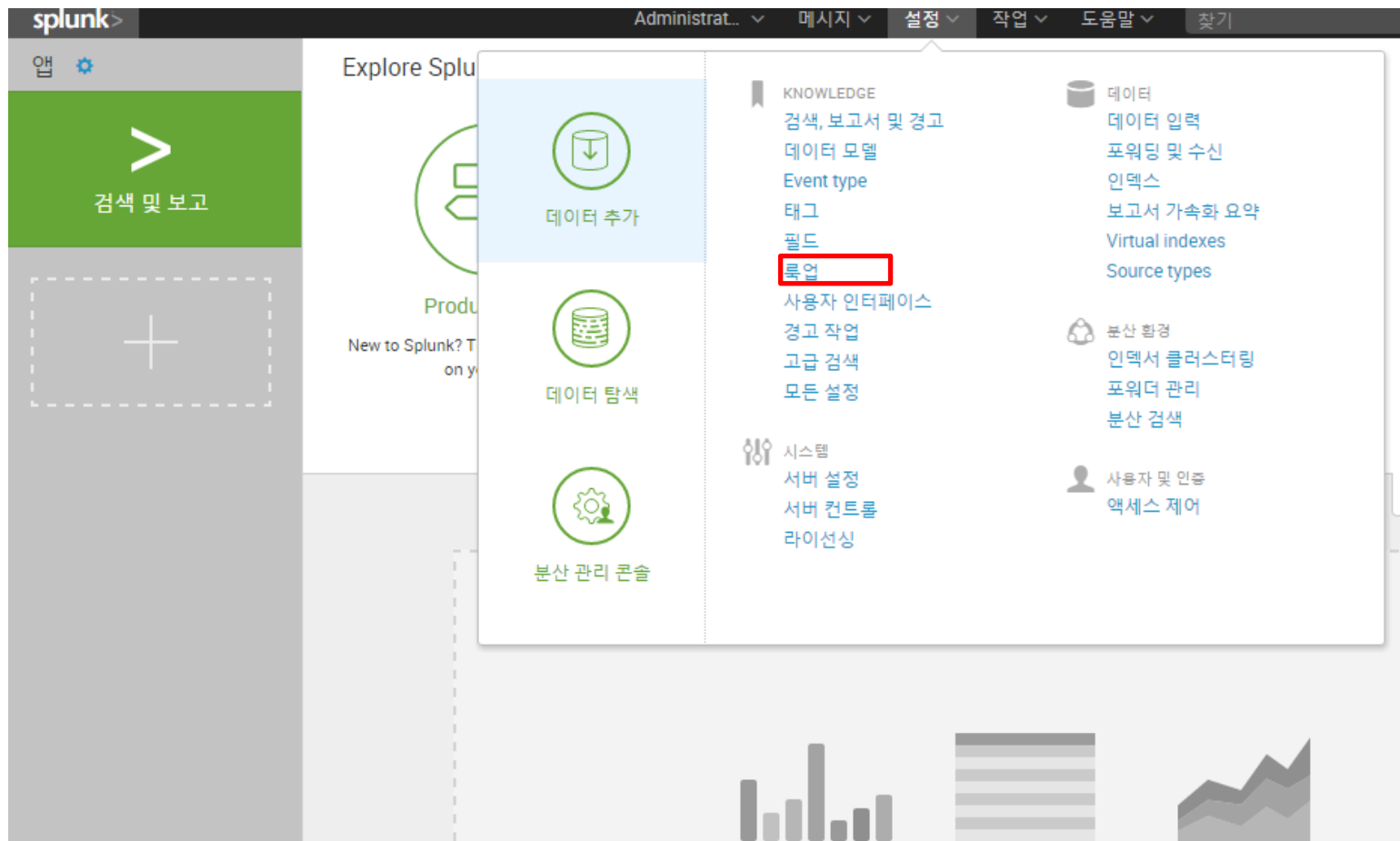
- `index=main sourcetype=access_* status=200 action=purchase | top limit=2 categoryId by clientip | eval percent=round(percent, 0) | eval percent = percent + "%" | eval value=count + " (" + percent + ")"`
- `index=main sourcetype="access*" | eval status_desc=case(status==200, "정상", status==404, "에러", status==500, "에러", status==503, "에러")`

4. xyseries를 활용한 테이블 만들기

- `index=main sourcetype=access_* status=200 action=purchase | stats count by clientip, productId | xyseries clientip productId count`

Lookup 실습

Lookup 파일 등록 및 활용



Lookup 파일 등록 및 활용

splunk> 앱 ▾ Administrat... ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾

룩업

룩업을 만들고 설정합니다.

| | |
|--|--------------------|
| 룩업 테이블 파일 기존 룩업 테이블을 나열하거나 새 파일을 업로드합니다. | 작업 새로 추가 |
| 룩업 정의 기존 룩업 정의를 편집하거나 새 파일 기반 또는 외부 룩업을 정의합니다. | 새로 추가 |
| 자동 룩업 기존 자동 룩업을 편집하거나 자동으로 실행할 새 룩업을 설정합니다. | 새로 추가 |

splunk> 앱 ▾

새로 추가

룩업 » 룩업 테이블 파일 » 새로 추가

대상 앱 *
search ▾

룩업 파일 업로드
파일 선택 prices.csv

Select either a plaintext CSV file, a gzipped CSV file, or a KMZ/KML file.
The maximum file size that can be uploaded through the browser is 500MB.

대상 파일 이름 *
prices.csv

Enter the name this lookup table file will have on the Splunk server. If you are uploading a gzipped CSV file, we recommend a filename ending in ".gz". For a KMZ/KML file, we recommend a filename ending in ".kmz".

취소 **저장**

Search 앱으로 변경


prices.csv 파일 업로드

검색창에서 사용할 Lookup 파일 이름 지정

Lookup 파일 권한 설정

splunk > 앱 ▾ Administrat... ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾ 찾기

룩업 테이블 파일
룩업 » 룩업 테이블 파일

앱 컨텍스트 Search & Reporting (search) ▾ 소유자 모두 ▾ 

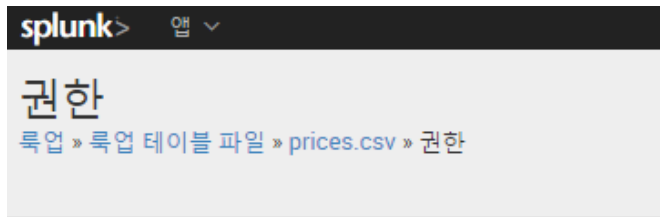
☐ 이 앱 컨텍스트에서 만든 개체만 표시 [자세히 알아보기](#)

새로 만들기

5개 항목 중 1-5 표시 페이지당 결과 25 ▾

| 경로 ▾ | 소유자 ▾ | App ▾ | 공유 중 ▾ | 상태 ▾ | 작업 |
|--|--------|--------|----------|-------|---------|
| /home/ubuntu/splunk/etc/apps/search/lookups/geo_attr_countries.csv | 소유자 없음 | search | 전역 권한 | 사용 가능 | 이동 삭제 |
| /home/ubuntu/splunk/etc/apps/search/lookups/geo_attr_us_states.csv | 소유자 없음 | search | 전역 권한 | 사용 가능 | 이동 삭제 |
| /home/ubuntu/splunk/etc/apps/search/lookups/geo_countries.kmz | 소유자 없음 | search | 전역 권한 | 사용 가능 | 이동 삭제 |
| /home/ubuntu/splunk/etc/apps/search/lookups/geo_us_states.kmz | 소유자 없음 | search | 전역 권한 | 사용 가능 | 이동 삭제 |
| /home/ubuntu/splunk/etc/users/admin/search/lookups/prices.csv | admin | search | 비공개 권한 | 사용 가능 | 이동 삭제 |

Lookup 파일 권한 설정



Object이(가) 나타나야 함

☐ 비공개 유지 ☐ 이 앱만(search) ☒ 모든 앱

권한

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

취소

Lookup 파일이 로딩 되는지 확인 검색창에서 아래 명령어로 확인

- | inputlookup prices.csv

The screenshot shows the Splunk search interface with the command 'inputlookup prices.csv' entered in the search bar. The results are displayed in a table with 5 columns: Code, price, productId, product_name, and sale_price. There are 15 results in total.

| Code | price | productId | product_name | sale_price |
|------|-------|-----------|-----------------------------------|------------|
| A | 24.99 | DB-SG-G01 | Mediocre Kingdoms | 19.99 |
| B | 39.99 | DC-SG-G02 | Dream Crusher | 24.99 |
| C | 24.99 | FS-SG-G03 | Final Sequel | 16.99 |
| D | 24.99 | WC-SH-G04 | World of Cheese | 19.99 |
| E | 9.99 | WC-SH-T0 | World of Cheese Tee | 6.99 |
| F | 4.99 | PZ-SG-G05 | Puppies vs. Zombies | 1.99 |
| G | 19.99 | CU-PG-G06 | Curling 2014 | 16.99 |
| H | 39.99 | MB-AG-G07 | Manganiello Bros. | 24.99 |
| I | 9.99 | MB-AG-T0 | Manganiello Bros. Tee | 6.99 |
| J | 39.99 | FI-AG-G08 | Orvil the Wolverine | 24.99 |
| K | 24.99 | BS-AG-G09 | Benign Space Debris | 19.99 |
| L | 19.99 | SC-MG-G10 | SIM Cubicle | 16.99 |
| M | 5.99 | WC-SH-A01 | Holy Blade of Gouda | 2.99 |
| N | 3.99 | WC-SH-A02 | Fire Resistance Suit of Provolone | 1.99 |

Lookup 실습

index=main sourcetype=access_* status=200 action=purchase

| top limit=1 productId by clientip

| lookup prices.csv productId OUTPUT product_name sale_price

등록된 Lookup
파일 이름

Lookup
Key Column

Lookup
Output Column

새로운 검색

index=main sourcetype=access_* status=200 action=purchase | top limit=1 productId by clientip | lookup prices.csv productId OUTPUT product_name sale_price

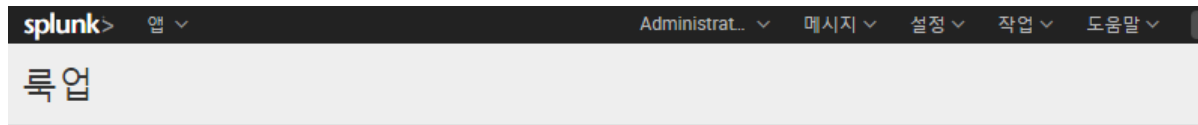
10,448 개 이벤트 (16/04/19 13:26:53.000 이전) No Event Sampling

작업

페이지당 20개

| clientip | productId | count | percent | product_name | sale_price |
|----------------|-----------|-------|-----------|-------------------|------------|
| 107.3.146.207 | SC-MG-G10 | 12 | 16.666667 | SIM Cubicle | 16.99 |
| 108.65.113.83 | SC-MG-G10 | 8 | 22.222222 | SIM Cubicle | 16.99 |
| 109.169.32.135 | MB-AG-G07 | 10 | 16.666667 | Manganiello Bros. | 24.99 |
| 110.138.30.229 | SC-MG-G10 | 4 | 25.000000 | SIM Cubicle | 16.99 |
| 110.159.208.78 | WC-SH-G04 | 6 | 14.285714 | World of Cheese | 19.99 |

자동 Lookup (1/2) – 룩업 정의



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.

작업



자동 Lookup (1/2) – 룩업 정의

룩업 정의

룩업 » 룩업 정의

search에서 "prices.csv"를(를) 성공적으로 저장했습니다.

앱 컨텍스트 Search & Reporting (search) ▼

소유자 모두 ▼

☐ 이 앱 컨텍스트에서 만든 개체만 표시 [자세히 알아보기](#)

새로 만들기

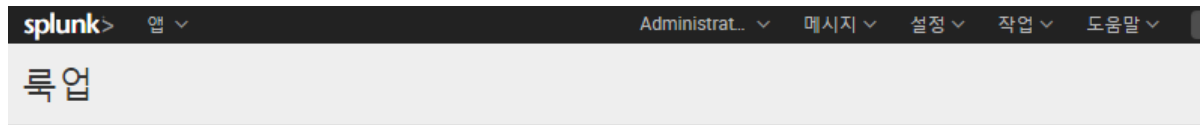
6개 항목 중 1-6 표시

페이지당 결과

| 이름 ▾ | 유형 ▾ | 지원되는 필드 ▾ | 룩업 파일 ▾ | 소유자 ▾ | App ▾ | 공유 중 ▾ | 상 |
|------------------------------------|----------|---|------------------------|--------|--------|----------|---|
| dnslookup | external | clienthost,clientip | | 소유자 없음 | system | 전역 권한 | 스 |
| geo_attr_countries | file | country,region_wb,region_un,subregion,continent,iso2,iso3 | geo_attr_countries.csv | 소유자 없음 | search | 전역 권한 | 스 |
| geo_attr_us_states | file | state_name,state_fips,state_code | geo_attr_us... | | | 전역 권한 | 스 |
| geo_countries | geo | None | geo_countries | 소유자 없음 | | 전역 권한 | 스 |
| geo_us_states | geo | None | geo_us_states.kmz | 소유자 없음 | search | 전역 권한 | 스 |
| prices.csv | file | productId,product_name,price,sale_price,Code | prices.csv | admin | search | 비공개 권한 | 스 |

권한 전역으로 풀어주세요 ^^

자동 Lookup (2/2) – 자동 룩업



룩업을 만들고 설정합니다.

룩업 테이블 파일

기존 룩업 테이블을 나열하거나 새 파일을 업로드합니다.

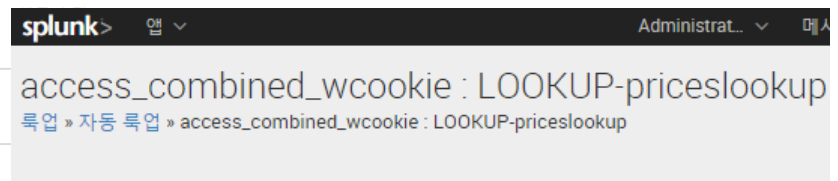
룩업 정의

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

자동 룩업

기존 자동 룩업을 편집하거나 자동으로 실행할 새 룩업을 설정합니다.

작업



룩업 테이블 *

prices.csv

룩업 입력 필드

productid = productid 삭제

= 삭제

다른 필드 추가

룩업 출력 필드

product_name = product_name 삭제

sale_price = sale_price 삭제

= 삭제

다른 필드 추가

☐ 필드 값 덮어쓰기

취소

자동 Lookup (2/2) – 자동 록업

splunk> 앱: 검색 및 ... Administrat... 메시지 설정 작업 도움말 찾기

검색 피벗 보고서 경고 대시보드 검색 및 보

새로운 검색 다른 이름으로 저장 달

index=main sourcetype=access_combined_wcookie 전체 시간 C

✓ 79,064 개 이벤트 (16/04/19 13:46:46.000 이전) No Event Sampling 작업 || ▶ ↻ ⬇ ⚡ 스마트 모드

이벤트 (79,064) 패턴 통계 시각화

시간 표시를 형식 지정 축소

< 필드 숨기기 모든 필드

선택된 필드

- a host 1
- a product_name 12
- a productId 16
- # sale_price 5
- a source 3
- a sourcetype 1

관심 있는 필드

- a action 5
- # bytes 100+
- a categoryId 8
- a clientip 100+
- # date_hour 24
- # date_mday 8
- # date_minute 60

product_name

12 값, 54.492% 이벤트 선택됨 예 아니요

보고서
상위 값 시간별 상위 값 회귀 값

이 필드가 있는 이벤트

| 상위 10개 값 | 개수 | % | |
|-----------------------------------|-------|---------|--|
| World of Cheese | 4,650 | 10.793% | |
| SIM Cubicle | 4,556 | 10.575% | |
| Mediocre Kingdoms | 4,500 | 10.445% | |
| Dream Crusher | 3,948 | 9.163% | |
| Fire Resistance Suit of Provolone | 3,794 | 8.806% | |
| Manganiello Bros. | 3,626 | 8.416% | |
| Final Sequel | 3,532 | 8.198% | |
| Holy Blade of Gouda | 3,250 | 7.543% | |
| Puppies vs. Zombies | 2,982 | 6.921% | |
| Orvil the Wolverine | 2,936 | 6.814% | |

sourcetype = access_combined_wcookie

> 16/04/02 91.205.189.15 - - [02/Apr/2016:18:22:15] "GET /category.screen?categoryId=SH

자동 Lookup (2/2) – 자동 룩업

splunk> 앱 ▾ Administrat... ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾ 찾기

자동 룩업

룩업 » 자동 룩업

search에서 "priceslookup"을(를) 성공적으로 저장했습니다.

앱 컨텍스트 Search & Reporting (search) ▾ 소유자 모두 ▾ 

☐ 이 앱 컨텍스트에서 만든 개체만 표시 [자세히 알아보기](#)

[새로 만들기](#)

1개 항목 중 1-1 표시

페이지당 결과 25 ▾

| 이름 ▾ | 룩업 ▾ | 소유자 ▾ | 앱 ▾ | 공유 중 ▾ | 상태 ▾ | 작업 |
|---|--|-------|--------|-----------------|-------|--|
| access_combined_wcookie : LOOKUP-priceslookup | prices.csv productId AS productId OUTPUTNEW product_name AS product_name sales_price AS sales_price | admin | search | 비공개 권한 | 사용 가능 | 복제 이동 삭제 |

권한 전역으로 풀어주세요 ^^

필드 추출

Secure Sourcetype

splunk> 앱: 검색 및 보고 ▾ Administrator ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾ 찾기

검색 피벗 보고서 경고 대시보드 검색 및 보고

새로운 검색 다른 이름으로 저장 ▾ 닫기

index=main sourcetype=secure 전체 시간 ▾ 🔍

✓ 80,176 개 이벤트 (16/04/19 14:33:01.000 이전) No Event Sampling ▾ 작업 ▾ || ▾ → ↺ ⬇ ⚡ 스마트 모드 ▾

이벤트 (80,176) 패턴 통계 시각화

시간 표시를 형식 지정 ▾ —축소 +선택 항목 확대/축소 ×선택 취소 클립당 1일

리스트 ▾ /형식 ▾ 페이지당 20개 ▾ <이전 1 2 3 4 5 6 7 8 9 ... 다음>

< 필드 숨기기 모든 필드

선택된 필드
a host 1
a source 4
a sourcetype 1

관심 있는 필드
date_hour 1
date_mday 8
date_minute 1
a date_month 2
date_second 6
a date_wday 7
date_year 1
a date_zone 1
a index 1
linecount 1
a punct 9
a splunk_server 1
timeendpos 1
timestartpos 1

5개의 추가 필드
⚡ 새 필드 추출

| i | 시간 | 이벤트 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|------|--|---|----|----|---|----|-----|--|----------------|---|--|--|-------------------------------------|---|--|--|--------|---|-----|----------------------------------|------|---|--|--------------------------------------|---|---|--|--|----------------|---|------|----------------------------------|-------------------------------|---|-----|----------------------------------|-----|---|
| ▽ | 16/04/02 0:15:06.000 | Thu Apr 02 2016 00:15:06 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 <div>이벤트 작업 ▾</div> <table><thead><tr><th>유형</th><th>필드</th><th>값</th><th>작업</th></tr></thead><tbody><tr><td>선택됨</td><td><input checked="" type="checkbox"/> host ▾</td><td>ip-172-31-8-33</td><td>▽</td></tr><tr><td></td><td><input checked="" type="checkbox"/> source ▾</td><td>tutorialdata.zip:/mailsv/secure.log</td><td>▽</td></tr><tr><td></td><td><input checked="" type="checkbox"/> sourcetype ▾</td><td>secure</td><td>▽</td></tr><tr><td>이벤트</td><td><input type="checkbox"/> index ▾</td><td>main</td><td>▽</td></tr><tr><td></td><td><input type="checkbox"/> linecount ▾</td><td>1</td><td>▽</td></tr><tr><td></td><td><input type="checkbox"/> splunk_server ▾</td><td>ip-172-31-8-33</td><td>▽</td></tr><tr><td>시간 ⚙</td><td><input type="checkbox"/> _time ▾</td><td>2016-04-02T00:15:06.000+00:00</td><td>▽</td></tr><tr><td>기본값</td><td><input type="checkbox"/> punct ▾</td><td>...</td><td>▽</td></tr></tbody></table> | 유형 | 필드 | 값 | 작업 | 선택됨 | <input checked="" type="checkbox"/> host ▾ | ip-172-31-8-33 | ▽ | | <input checked="" type="checkbox"/> source ▾ | tutorialdata.zip:/mailsv/secure.log | ▽ | | <input checked="" type="checkbox"/> sourcetype ▾ | secure | ▽ | 이벤트 | <input type="checkbox"/> index ▾ | main | ▽ | | <input type="checkbox"/> linecount ▾ | 1 | ▽ | | <input type="checkbox"/> splunk_server ▾ | ip-172-31-8-33 | ▽ | 시간 ⚙ | <input type="checkbox"/> _time ▾ | 2016-04-02T00:15:06.000+00:00 | ▽ | 기본값 | <input type="checkbox"/> punct ▾ | ... | ▽ |
| 유형 | 필드 | 값 | 작업 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 선택됨 | <input checked="" type="checkbox"/> host ▾ | ip-172-31-8-33 | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> source ▾ | tutorialdata.zip:/mailsv/secure.log | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <input checked="" type="checkbox"/> sourcetype ▾ | secure | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 이벤트 | <input type="checkbox"/> index ▾ | main | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <input type="checkbox"/> linecount ▾ | 1 | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | <input type="checkbox"/> splunk_server ▾ | ip-172-31-8-33 | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 시간 ⚙ | <input type="checkbox"/> _time ▾ | 2016-04-02T00:15:06.000+00:00 | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 기본값 | <input type="checkbox"/> punct ▾ | ... | ▽ | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > | 16/04/02 0:15:06.000 | Thu Apr 02 2016 00:15:06 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = ip-172-31-8-33 source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > | 16/04/02 0:15:06.000 | Thu Apr 02 2016 00:15:06 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = ip-172-31-8-33 source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > | 16/04/02 0:15:06.000 | Thu Apr 02 2016 00:15:06 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for user ns harpe by (uid=0) host = ip-172-31-8-33 source = tutorialdata.zip:/mailsv/secure.log sourcetype = secure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| > | 16/04/02 0:15:06.000 | Thu Apr 02 2016 00:15:06 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Secure Raw Data

| i | 이벤트 |
|---|--|
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharpe by (uid=0) |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[93483]: Server listening on :: port 22. |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[3759]: Failed password for nagios from 194.8.74.23 port 3769 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[4994]: Failed password for invalid user guest from 194.8.74.23 port 2294 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[60445]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[2605]: Failed password for invalid user itmadmin from 194.8.74.23 port 4692 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5333]: Failed password for invalid user inet from 194.8.74.23 port 4564 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[3014]: Failed password for invalid user operator from 194.8.74.23 port 1491 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[4907]: Failed password for invalid user irc from 194.8.74.23 port 1956 ssh2 |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[87066]: pam_unix(sshd:session): session opened for user djohnson by (uid=0) |
| > | Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5085]: Failed password for invalid user harrison from 194.8.74.23 port 3756 ssh2 |

새 필드 추출

splunk> 앱: 검색 및 보고 Administrator

검색 피벗 보고서 경고 대시보드

새로운 검색

index=main sourcetype=secure

80,176 개 이벤트 (16/04/19 14:33:01.000 이전) No Event Sampling

이벤트 (80,176) 패턴 통계 시각화

시간 표시줄 형식 지정 축소 선택 항목 확대/축소 선택 취소

원시 형식 페이지당 20개

< 필드 숨기기 모든 필드

선택된 필드
a host 1
a source 4
a sourcetype 1

관심 있는 필드
date_hour 1
date_mday 8
date_minute 1
a date_month 2
date_second 6
a date_wday 7
date_year 1
a date_zone 1
a index 1
linecount 1
a punct 9
a splunk_server 1
timeendpos 1
timestartpos 1

5개의 추가 필드
새 필드 추출

i 이벤트

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[5276]: Failed password for invalid user appserver fr

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 por

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[5258]: Failed password for invalid user testuser fro

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for u

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 p

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[3760]: Failed password for invalid user mongodb from

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 por

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 pc

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[93483]: Server listening on :: port 22.

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[5801]: Failed password for invalid user desktop from

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[3759]: Failed password for nagios from 194.8.74.23 p

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[5979]: Failed password for invalid user cyrus from 1

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[4994]: Failed password for invalid user guest from 1

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[60445]: pam_unix(sshd:session): session opened for u

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[2605]: Failed password for invalid user itmadmin fro

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[5333]: Failed password for invalid user inet from 19

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[3014]: Failed password for invalid user operator fro

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[4907]: Failed password for invalid user irc from 194

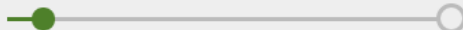
> Thu Apr 02 2016 00:15:06 mailsv1 sshd[87066]: pam_unix(sshd:session): session opened for u

> Thu Apr 02 2016 00:15:06 mailsv1 sshd[5085]: Failed password for invalid user harrison fro

새 필드 추출

splunk> 앱: 검색 및 보고 ▼

검색 피벗 보고서 경고 대시보드

필드 추출  다음 >

샘플 선택 Select method 필드 선택 저장

샘플 이벤트 선택

Choose a source or source type, select a sample event, and click Next to go to the next step. The field extractor will use the event to extract fields. [자세히 알아보기](#) [직접 정규식을 작성하겠습니다.](#)

Source type **secure**

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2

이벤트

✓ 1,000 개 이벤트 (16/04/19 14:37:12.000 이전)

필터 적용 샘플: 1,000 events ▼ 모든 이벤트 ▼

_raw

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharp by (uid=0)

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2

Thu Apr 02 2016 00:15:06 mailsrv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2

추출하려는 패턴이
있는 event 선택

추출 방식 선정

splunk> 앱: 검색 및 ... Administrat... 메시지 설정 작업 도움말 찾기

검색 피벗 보고서 경고 대시보드 검색 및 보

필드 추출

샘플 선택

Select method

필드 선택

저장

< 다음 >


기존 필드 >

Select Method

Indicate the method you want to use to extract your field(s). [자세히 알아보기](#)
[직접 정규식을 작성하겠습니다.](#)


Source type **secure**

```
Thu Apr 02 2016 00:15:06 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2
```



정규식

Splunk Enterprise will extract fields using a Regular Expression.



Delimiters

Splunk Enterprise will extract fields using a delimiter (such as commas, spaces, or characters). Use this method for delimited data like comma separated values (CSV files).

필드추출 등록

splunk> 앱: 검색 및 ... Administrat... 메시지 설정 작업 도움말 찾기

검색 피벗 보고서 경고 대시보드 검색 및 보고

필드 추출

샘플 선택 Select method 필드 선택 Validate 저장

기존 필드 >

필드 선택

Highlight one or more values in the sample event to create fields. You can indicate one value is required, meaning it must exist on to match. Click on highlighted values in the sample event to modify them. To highlight text that is already part of an existing extraction, turn off the existing extractions. 자세히 알아보기

Thu Apr 02 2016 00:15:06 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2

추출 필수

필드 이름 user_name

샘플 값 appserver

Add Extraction

더블 클릭

필드추출 확인

정규식 편집을 통해 추출패턴 수정

이벤트

user_name

✓ 1,000 개 이벤트 (16/04/19 14:41:38.000 이전)

Original search included: ? ☒

페이지당 20개 ▾

< 이전

1

2

3

4

5

6

7

8

9

...

다음 >

필터

적용

샘플: 1,000 events ▾

모든 이벤트 ▾

모든 이벤트

일지

불일치

| | _raw | user_name |
|---|---|-----------|
| ✓ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 | appserver |
| ✗ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 | |
| ✓ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 | testuser |
| ✗ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[21881]: pam_unix(sshd:session): session closed for user nsharpe by (uid=0) | |
| ✗ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[1165]: Failed password for apache from 194.8.74.23 port 4604 ssh2 | |
| ✓ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 | mongodb |
| ✗ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 | |
| ✗ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[1930]: Failed password for games from 194.8.74.23 port 3007 ssh2 | |
| ✗ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[93483]: Server listening on :: port 22. | |
| ✓ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[5801]: Failed password for invalid user desktop from 194.8.74.23 port 2285 ssh2 | desktop |
| ✗ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[3759]: Failed password for nagios from 194.8.74.23 port 3769 ssh2 | |
| ✓ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[5979]: Failed password for invalid user cyrus from 194.8.74.23 port 3417 ssh2 | cyrus |
| ✓ | Thu Apr 02 2016 00:15:06 mailsv1 sshd[4994]: Failed password for invalid user guest from 194.8.74.23 port 2294 ssh2 | guest |

필드추출된 필드 활용

splunk> 앱: 검색 및 보고 ▾ Administrator ▾ 메시지 ▾ 설정 ▾ 작업 ▾ 도움말 ▾ 찾기

검색 피벗 보고서 경고 대시보드 검색 및 보고

새로운 검색 다른 이름으로 저장 ▾ 달기

index=main sourcetype=secure | stats count by user_name | 전체 시간 ▾ 🔍

✓ 80,176 개 이벤트 (16/04/19 14:48:02.000 이전) No Event Sampling ▾ 작업 ▾ || ▢ ➔ 📄 ⬇ ⚡ 스마트 모드 ▾

이벤트 패턴 통계 (113) 시각화

페이지당 20개 ▾ 🔍 형식 ▾ 미리보기 ▾ < 이전 1 2 3 4 5 6 다음 >

| user_name ⚙ | count ⚙ |
|---------------|---------|
| abc | 144 |
| adm | 162 |
| admin | 1876 |
| administrator | 2040 |
| agushto | 130 |
| alex | 130 |
| amanda | 180 |
| amavis | 146 |
| angel | 182 |
| appserver | 446 |
| art | 176 |
| ben | 154 |
| bfsuser | 148 |
| brian | 156 |
| carrie | 160 |
| couchdb | 150 |
| customer | 188 |
| cyrus | 180 |
| dasusr1 | 152 |
| db | 1040 |

index=main sourcetype=secure
| stats count by user_name