What is Splunk?

Theo wikipedia, **Splunk** là một phần mềm tầm cỡ enterprise (ứng dụng lớn dùng cho doanh nghiệp) được dùng để giám sát, báo cáo và phân tích dữ liệu máy tính tạo ra bở các ứng dụng, các hệ thống, và cơ sở hạ tầng mạng của doanh nghiệp. Splunk cho phép người dùng tìm kiếm, giám sát, và phân tích dữ liệu do máy (các thiết bị) tạo ra thông qua một giao diện web thân thiện với người dùng, mạnh, và rất linh hoạt. Splunk tạo các chỉ mục và tham chiếu dữ liệu theo thời gian thực, trong một kho dữ liệu mà người dùng có thể dễ dàng tìm kiếm, xem các biểu đồ, báo cáo, các cảnh báo thông qua bảng điều khiển (dashboard).

Mục tiêu của Splunk là làm cho dữ liệu của máy tính có thể được truy xuất xuyên suốt trong tổ chức, và xác định các khuôn mẫu dữ liệu được định nghĩa sẵn (các dấu hiệu virus, dấu hiệu của tấn công..), cung cấp các metric, chuẩn đoán các vấn đề xảy ra, và làm cho hoạt động kinh doanh của tổ chức trở nên thông minh hơn, trong tầm kiểm soát hơn. Splunk là một công nghệ được dùng để quản lý ứng dụng, an ninh, và linh hoạt, cũng như trong kinh doanh lẫn phân tíchweb.

Cái tên "Splunk" có nguồn gốc từ spelunking, có nghĩa là thích khai phá hang động.

Xem Chủ tịch và CEO của Splunk nói chiện tại:

http://www.splunk.com/view/SP-CAAAFV2

Download

Splunk ở đâu? --> http://www.splunk.co...c=wiki_download

System Requirements: (ver4.2.3 - lastest 16/10/2011)

- Hệ điều hành

- Solaris 9, 10 (x86, SPARC)
- Linux Kernel vers 2.6.x and above (x86: 32 and 64-bit)
- FreeBSD 6.1 and 6.2 (x86: 32 and 64-bit)

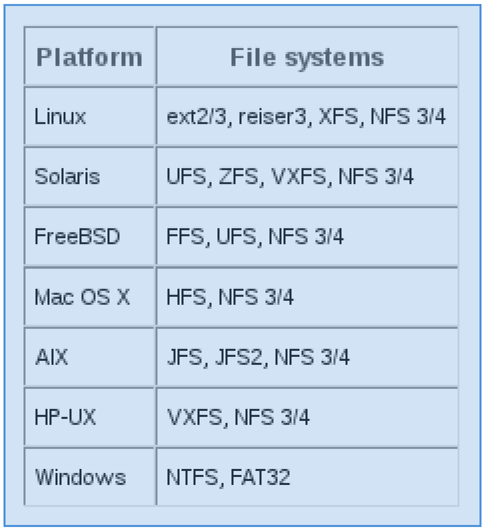
- Windows Server 2003/2003 R2 (64-bit, supported but not recommended on 32-bit)
- Windows Server 2008/2008 R2 (64-bit, supported but not recommended on 32-bit)
- Windows XP (32-bit)
- Windows Vista (32-bit, 64-bit)
- Windows 7 (32-bit, 64-bit)
- MacOSX 10.5 and 10.6 (32-bit & 64bit in one download, **10.6 is only supported in 32-bit mode**)
- AIX 5.2, 5.3, and 6.1
- HP-UX 11iv2 (11.22) and 11iv3 (11.31) (PA-RISC or Itanium, **gnu tar is required to unpack the tar.gz archive**)

- Trình duyệt

- Firefox 2, 3, and 4
- Firefox 3.5 (with Splunk version 4.0.6 and later)
- Internet Explorer 6, 7, 8, and 9
- Safari 3
- Chrome 9

kèm với flash player phiên bản mới nhất

- Hệ thống tập tin



Platform	File systems
Linux	ext2/3, reiser3, XFS, NFS 3/4
Solaris	UFS, ZFS, VXFS, NFS 3/4
FreeBSD	FFS, UFS, NFS 3/4
Mac OS X	HFS, NFS 3/4
AIX	JFS, JFS2, NFS 3/4
HP-UX	VXFS, NFS 3/4
Windows	NTFS, FAT32

Các thành phần của Splunk

- Indexer

Cung cấp chức năng lập chỉ mục cho dữ liệu trên local và từ xa, chứa kho dữ liệu chính của Splunk, cũng như Splunk web.

Search peer là một bộ lập chỉ mục tiếp nhận các yêu cầu dịch vụ từ search head trong một hệ thống được triển khai phân tán. Search peer đôi khi cũng được gọi là các indexer node.

- Search head

Là một thành phần chức năng của splunk được cấu hình để tìm kiếm phân tán trong các indexer, hoặc các search peer. Các search head có thể thiết lập là chuyên dụng làm một nhiệm vụ là index hoặc không, tùy thuộc vào chúng có thực hiện việc index hay không. Một search head chuyên dụng không index chính nó (internal indexing). Thay vào đó, chúng lấy các kết quả từ các remote search peer.

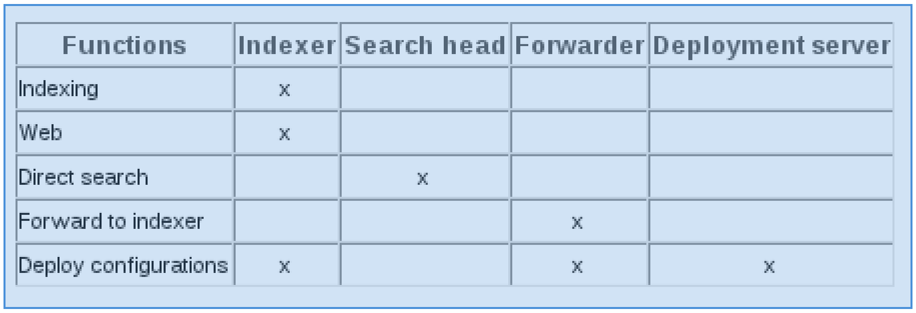
- Forwarder

Là một thành phần chức năng của Splunk, các forwarder forward dữ liệu tới các remote indexer để lập chỉ mục và lưu trữ. Trong nhiều trường hợp, chúng không tự lập chỉ mục cho dữ liệu.

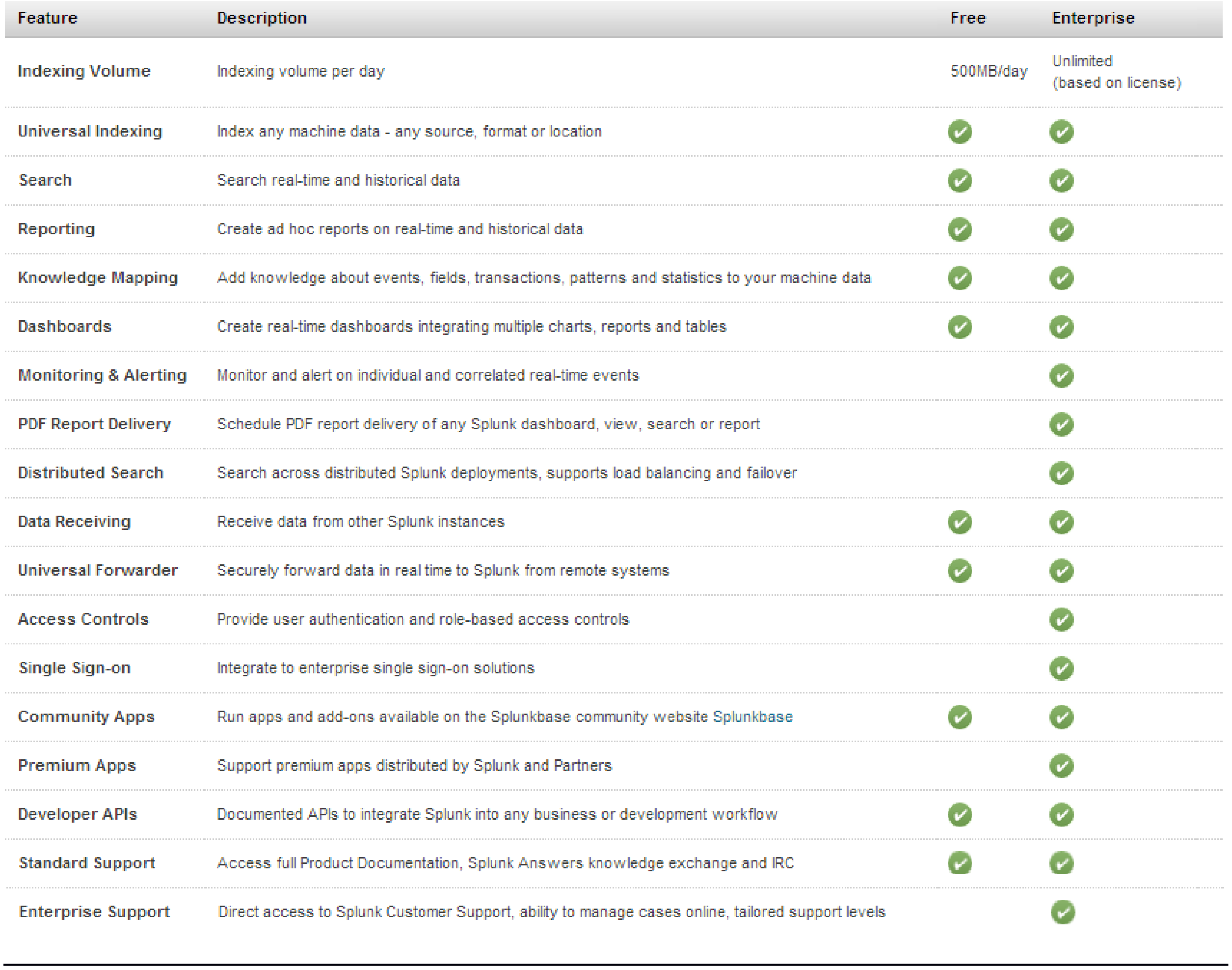
- Deployment server

Các indexer, và forwarder đều có thể đóng vai trò của các deployment server. Một deployment server phân tán các thông tin cấu hình để chạy Splunk thông qua cơ chế **push**, được kích hoạt thông qua cấu hình.

- Các chức năng tổng quát



Functions	Indexer	Search head	Forwarder	Deployment server
Indexing	x			
Web	x			
Direct search		x		
Forward to indexer			x	
Deploy configurations	x		x	x



Feature	Description	Free	Enterprise
Indexing Volume	Indexing volume per day	500MB/day	Unlimited (based on license)
Universal Indexing	Index any machine data - any source, format or location	✓	✓
Search	Search real-time and historical data	✓	✓
Reporting	Create ad hoc reports on real-time and historical data	✓	✓
Knowledge Mapping	Add knowledge about events, fields, transactions, patterns and statistics to your machine data	✓	✓
Dashboards	Create real-time dashboards integrating multiple charts, reports and tables	✓	✓
Monitoring & Alerting	Monitor and alert on individual and correlated real-time events		✓
PDF Report Delivery	Schedule PDF report delivery of any Splunk dashboard, view, search or report		✓
Distributed Search	Search across distributed Splunk deployments, supports load balancing and failover		✓
Data Receiving	Receive data from other Splunk instances	✓	✓
Universal Forwarder	Securely forward data in real time to Splunk from remote systems	✓	✓
Access Controls	Provide user authentication and role-based access controls		✓
Single Sign-on	Integrate to enterprise single sign-on solutions		✓
Community Apps	Run apps and add-ons available on the Splunkbase community website Splunkbase	✓	✓
Premium Apps	Support premium apps distributed by Splunk and Partners		✓
Developer APIs	Documented APIs to integrate Splunk into any business or development workflow	✓	✓
Standard Support	Access full Product Documentation, Splunk Answers knowledge exchange and IRC	✓	✓
Enterprise Support	Direct access to Splunk Customer Support, ability to manage cases online, tailored support levels		✓

Splunk Command Line Reference:
http://docs.splunk.com/Documentation/Splunk/latest/Admin/AccessandusetheCLIonaremoteserver
Note: the CLI may ask you to authenticate – it's asking for the LOCAL credentials, so if you haven't changed the admin password on the forwarder, you should use admin/changeme

Steps for Installing/Configuring Linux forwarders:

Step 1: Download Splunk Universal Forwarder:
http://www.splunk.com/download/universalforwarder
(64bit package if applicable!)

Step 2: Install Forwarder

```
dpkg -i splunkforwarder.deb
```

Install into opt/splunkforwarder/

Step 3: Enable boot-start/init script:

```
/opt/splunkforwarder/bin/splunk enable boot-start
```

(start splunk: /opt/splunkforwarder/splunk start)

Step 4: Enable Receiving input on the Index Server
Configure the Splunk Index Server to receive data, either in the manager:
Manager -> sending and receiving -> configure receiving -> new
or via the CLI:

```
/opt/splunk/bin/splunk enable listen 9997
```

Where 9997 (default) is the receiving port for Splunk Forwarder connections

Step 5: Configure Forwarder connection to Index Server:

```
/opt/splunkforwarder/bin/splunk add forward-server hostname.domain:9997
```

(where hostname.domain is the index server, and 9997 is the receiving port you create on the Indexer:
Manager -> sending and receiving -> configure receiving -> new)

Step 6: Test Forwarder connection:

```
/opt/splunkforwarder/bin/splunk list forward-server
```

Step 7: Add Data:

```
/opt/splunkforwarder/bin/splunk add monitor /path/to/app/logs/ -index main   -sourcetype %app%
```

Where /path/to/app/logs/ is the path to application logs on the host that you want to bring into Splunk, and %app% is the name you want to associate with that type of data

This will create a file: inputs.conf in /opt/splunk/etc/apps/search/local/ -- here is some documentation on inputs.conf:
http://docs.splunk.com/Documentation/Splunk/4.3.2/admin/Inputsconf

Note: System logs in /var/log/ are covered in the configuration part of Step 7. If you have application logs in /var/log/*/

Step 8 (Optional): Install and Configure UNIX app on Indexer and *nix forwarders:
On the Splunk Server, go to Apps -> Manage Apps -> Find more Apps Online -> Search for 'unix' -> Install
Restart Splunk if prompted, Open UNIX app -> Configure

Once you've configured the UNIX app on the server, copy /opt/splunk/etc/apps/unix/ from server to /opt/splunkforwarder/etc/apps/unix/ on forwarder
Restart the Splunk forwarder (/opt/splunkforwarder/bin/splunk restart)

Note: The data collected by the unix app is by default placed into a separate index called 'os' so it will not be searchable within splunk unless you either go through the UNIX app, or include the following in your search query: "index=os" or "index=os OR index=main" (don't paste doublequotes)

Step 9 (Optional): Customize UNIX app configuration on forwarders:
Look at inputs.conf in /opt/splunkforwarder/etc/apps/unix/local/ and /opt/splunkforwarder/etc/apps/unix/default/
The ~default/inputs. path shows what the app can do, but everything is disabled. The ~local/inputs.conf shows what has been enabled – if you want to change polling intervals or disable certain scripts, make the changes in ~local/inputs.conf.

Step 10 (Optional): Configure File System Change Monitoring (for configuration files):
http://docs.splunk.com/Documentation/Splunk/4.3.2/Data/Monitorchangestoyourfilesystem

Note that Splunk also has a centralized configuration management server called Deployment Server. This can be used to define server classes and push out specific apps and configurations to those classes. So you may want to have your production servers class have the unix app configured to execute those scripts listed in ~local/inputs at the default values, but maybe your QA servers only need a few of the full stack, and at longer polling intervals. Using Deployment Server, you can configure these classes, configure the app once centrally, and push the appropriate app/configuration to the right systems.

link

Step 7 add data is failing for me, i dont see its creating inputs.conf file under /etc/apps/search/local .. i dont have local directory in that path.. i am trying this on linux.. what am i doing wrong.. my splunk version is 4.3.4

In handler 'monitor': Parameter index: Index 'main' does not exist. Please provide a valid index.

(14 Sep, 15:42)rajeshgajula

If the command is giving you an error then it likely won't write to the inputs.conf file. Strange that the main index doesn't exist yet...try leaving off the '-index main' part. The main index is where new data goes by default anyways.

(21 Sep, 12:36)MillerTime

1

to install and run as the user 'splunk', which is preferable to running as 'root':

log on and su to root.

```
rpm -i splunk_install_file.rpm

su splunk -c "/opt/splunkforwarder/bin/splunk start --accept-license"

/opt/splunkforwarder/bin/splunk enable boot-start -user splunk

su splunk -c "/opt/splunkforwarder/bin/splunk edit user admin -password <your new password> -auth admin:changeme"


#optional if you want to use the Deployment Server feature of your splunk server.

su splunk -c "/opt/splunkforwarder/bin/splunk set deploy-poll <ip:port>"


/etc/init.d/splunk restart
```

Put all of that in a script, and you'll have a nice clean start.

/k

☆☆☆☆☆

0 ratings

Description

The OPSEC LEA for Check Point add-on for Linux allows you to index your Check Point firewall logs in Splunk 4.0 or later. The add-on components include a binary that communicates with your Check Point SmartCenter via the OPSEC LEA protocol over an SSL connection to retrieve the FireWall-1 log information, and a scripted input that pulls the logs into Splunk.

This description assumes that you have already downloaded and installed Splunk, that you can navigate to the Splunk UI, and that you are familiar with the Check Point Server. For information on downloading Splunk, see the Installation Manual. For information on scripted inputs in Splunk, see Set up custom (scripted) inputs in the Admin manual.

Requirements

Splunk versions:

Platforms:

OPSEC LEA versions:

Package:

Set up your environment

1. Scripted inputs inherit Splunk's environment, so be sure to clear environment variables which may affect your script's operation. In particular, make sure the library variable (commonly known as `LD_LIBRARY_PATH` on Linux) is set up correctly.

2. Linux `gcc` version 4.x usually has `libstdc++.so.6` installed. To use this add-on, you need to

install `libstdc++.so.5`.

Download and untar the Splunk OPSEC add-on

Once you have your environment set up correctly, you can download and untar the add-on on your Splunk server. It creates a `$SPLUNK_HOME/etc/apps/lea-loggrabber-splunk` directory on your machine.

The following steps show how to configure the add-on to communicate with Check Point.

Modify Check Point

Before configuring the add-on, you need to set up Check Point according to the instructions in the Check Point documentation. If you are comfortable with Check Point configuration, you may skip this section. Make sure to set up certificates and keys on the Linux box.

Enable a LEA server

The LEA client must communicate with a LEA Server. To set up a server:

1. Log into the box running the Check Point server.

2. Edit `$FWDIR/conf/fwopsec.conf` and add the following lines:

```
lea_server auth_port 18184
lea_server auth_type ssl_opsec
```

3. Restart the FW1 engine using the following commands:

```
cpstop
cpstart
```

Modify Check Point rules

To allow access for LEA traffic you need to add rules to accept traffic on FW1:

1. Open the main Check Point configuration (Policy Editor).

2. Enable an FW1_ica_pull (accept) rule and add an FW1_lea traffic (accept) rule.

Create OPSEC server application

Before installing and configuring the add-on, you must add a LEA OPSEC server to the Check Point configuration. This establishes a SIC trust between the add-on and FW1. To do this:

1. In the Check Point SmartDashboard, click on Manage > Servers and OPSEC applications.

2. Click New to open a configuration screen for adding an entry.

3. Name your entry *SplunkLEA*.

4. Select *User defined* from the Vendor menu and make sure *LEA* is selected in Client Entities.

5. Click Communication and enter a one-time password for the Activation Key. Important: Make a note of this password, as you will use it to retrieve the OPSEC app certificate.

6 Click Initialize. Check Point responds with a DN. You need this DN later for the `opsec_sic_name` in the `lea.conf` file.

7. Click OK to return the Servers and OPSEC Applications screen, then click Close.

Set up keys

You need to create an authentication key for your FW1 machine and place it in the correct location for the add-on installation.

Retrieve OPSEC app certificate

First, extract the certificate for your OPSEC:

1. Use the following utility to perform the extraction. Enter the one-time password you created in Create OPSEC server application/Step 5 for the password:

```
cd opsec-tools/<linux22>
./opsec_pull_cert -h <ip of Check Point box> -n <object> -p <password>
```

For example:

```
opsec_pull_cert -h 10.1.1.96 -n SplunkLEA -p <password>
```

This will produce a file in the current directory called `opsec.p12`.

Create FW1 authentication key

You need to create an authentication key on the FW1 machine. To do this over an SSL connection:

1. Perform `putkey` in the firewall. Important: Make a note of the secret key you enter, as you will need it to retrieve the key on the Linux box.

```
fw putkey -opsec -ssl <Destination IP address of the linux box>

Enter secret key: *********
Again secret key: *********
```

2. Make sure to note the secret key; you need it to retrieve the authentication key on the Linux box.

Retrieve FW1 authentication key

To retrieve the key you just created and and install it on the Linux box:

1. Log into the Linux box and enter the following:

```
cd opsec-tools/<linux22>
opsec_putkey -ssl -port 18184 <Source IP address of Check Point box>
```

2. When prompted, enter the secret key you used for the `putkey` utility (in the previous section).

You should see something like:

```
Please enter secret key: *****
Please enter secret key again: *****
FW: Received new control security key from <Source IP address of
checkpoint box>

Authentication with <Source IP address of checkpoint box> initialized
successfully
```

This generates the following files: `sslauthkeys.C` and `sslsess.C`

Configure LEA client

Start by verifying the LEA client configuration:

1. Open the `$SPLUNK_HOME/etc/apps/lea-loggrabber-splunk/default/lea.conf` file and ensure it is populated with the proper values:

```
opsec_sic_name "CN=SplunkLEA,O=directory..3sapn8" //DN obtained from
```

```
"Create OPSEC Application" step
opsec_sslca_file <path to opsec.p12>
lea_server ip <ip of FW1 box>
lea_server auth_port 18184
lea_server auth_type ssl_opsec
lea_server opsec_entity_sic_name "cn=cp_mgmt,o=directory..3sapn8" //To
retrieve opsec_entity_sic_name, double-click on the main Check Point
object
```

Note: To retrieve the server SIC entity name for the `opsec_entity_sic_name` from the Policy Editor, select *Network Objects* from the Manage menu in the Policy Editor, choose the network object for your management server and click Edit. The DN for `opsec_entity_sic_name` is listed under Secure Internal Communication in the Workstation Properties window.

Configure and use the Splunk OPSEC add-on

Once you have the LEA client up and communicating, you can configure the Splunk add-on to pull the logs.

Configure the add-on

To configure the add-on on your Splunk server:

1. Copy `opsec.p12`, `sslauthkeys.C` and `sslsess.C` into the `lea-loggrabber-splunk/bin/` directory. If you configured Check Point according to the instructions in the first part of this topic, these files will be present in the `opsec-tools/<linux22>` directory on the Linux box. If you skipped the first part of this topic because you have already configured Check Point, use `opsec_putkey` to retrieve these keys.

2. Copy the `lea-loggrabber-splunk` directory to your $SPLUNK_HOME/etc/apps directory. (e.g. `/opt/splunk/etc/apps`). This creates a `$SPLUNK_HOME/etc/apps/lea-loggrabber-splunk` directory.

3. Modify the file paths in the `lea-loggrabber.sh` file as follows:

```
#!/bin/bash

cd /opt/splunk/etc/apps/lea-loggrabber-splunk/bin
./lea_loggrabber --lea-config-file /opt/splunk/etc/apps/lea-
loggrabber-splunk/default/lea.conf
```

4. Make sure `lea-loggrabber.sh` and `lea-loggrabber` have execute rights by applying `chmod`

`755` on the two files.

5. (Optional) Configure the polling interval used by the Splunk server to retrieve CheckPoint firewall logs. To set the polling interval, replace the contents of `/opt/splunk/etc/apps/lea-loggrabber-splunk/default/inputs.conf` with the following lines and set the `interval` to your desired value (in seconds):

```
[script://./bin/lea-loggrabber.sh]
interval = 60
sourcetype = opsec
disabled = false
```

6. You must restart Splunk to see the changes.

Access Check Point FW logs via the Splunk GUI

Splunk retrieves the latest logs from the Check Point firewall automatically (e.g. every 60 seconds). To view the logs in Splunk:

1. Start Splunk and navigate to the Splunk GUI. A new source type, `opsec`, appears under sourcetype in the Splunk GUI.

2. To view events from your Check Point firewall logs, type

```
sourcetype=opsec
```

and press Enter.

3. Use the Fields pull-down menu to view the fields defined for the Check Point firewall logs.

Configure multiple targets

To communicate with more than one Check Point target, create multiple instances of the app in `$SPLUNK_HOME/etc/apps`. You will need to restart Splunk once all instances are configured.

Reference

This section describes the add-on's configuration files and lists the fields for the `opsec` source type.

Configuration files

There are three relevant configuration files in the `lea-bundle` directory:

- `inputs.conf` is a Splunk configuration file. The default configuration will place any information from your Check Point target in the main index with sourcetype "opsec". See the Splunk documentation for information on how to modify this configuration.
- `props.conf` is a Splunk configuration file. It is used to recognize the time format used by the Check Point firewall logs. Read the Splunk documentation for further details.
- `lea.conf` is the file containing connection information between the loggrabber agent and the Check Point target. The default configuration contains values for unauthenticated, clear sessions between the loggrabber agent and the Check Point target. Documentation for configuring a more secure channel on the loggrabber agent's side is available in the doc directory. Substantial configuration is required on the Checkpoint side. Consult your Checkpoint documentation for that information.

Sourcetype and fields

The Splunk source type for Check Point logs is `opsec`.

Splunk extracts the key value pairs from the Check Points records and creates the corresponding fields. It also creates three additional fields to manage your Check Point records:

Field
`filename`
`fileid`
`loc`