

Session 1 - Splunk in Action

Splunk, whose name was inspired by the process of exploring caves, or *spelunking*, helps analysts, operators, programmers, and many others explore many types of data, including raw machine data from their organizations, by collecting, analyzing, and acting on them. This multinational company, cofounded by Michael Baum, Rob Das, and Erik Swan, has a core product called Splunk Enterprise. This product manages searches, inserts, deletes, filters, and analyzes big data that is generated by machines, as well as many other types of data.

NOTE

Throughout the book, we will be covering the fundamental, barebones concepts of Splunk so you can learn quickly and efficiently. We reserve any deep discussion of concepts to Splunk's online documentation. Where necessary, we provide links to help provide you with the practical skills, and examples, so you can get started quickly. All images and exercise materials used in this book are available online.

With very little time, you can achieve direct results using Splunk, which you can access through a free enterprise trial license. While this license limits you to 500 MB of data ingested per day, it will allow you to quickly get up to speed with Splunk and learn the essentials of this powerful software.

The exercises in this section may look challenging at first, but if you follow what we've written closely, we believe you will quickly learn the fundamentals you need to use Splunk effectively. Together, we will make the most of the Trial License and give you a visible result that you can use to create valuable insights for your company (and, if you like, proudly show to your friends and coworkers).

Your Splunk.com account

First you will need to register for a Splunk.com account. This is the account that you will use if you decide to purchase a license later. Go ahead and do this now. From here on, the password you use for your Splunk.com account will be referred to as your Splunk.com password.

Obtaining a Splunk.com account

To obtain your Splunk.com account, perform the following steps:

1. Go to the Splunk signup page at <http://www.splunk.com>.
2. In the upper right hand corner, click on **My Account | Sign Up**.
3. Enter the information requested.
4. Create a username and password.

You will then need to download the Splunk Enterprise software. Go to <http://download.splunk.com> and select the Splunk Enterprise free download. Choose your operating system, being careful to select 32- or 64-bit (whichever is appropriate in your case; most should select 64-bit, which most computers today use). For Windows, download the *.msi file. For Mac OS X, download the *.dmg file. In this book, we will work with Version 6.4.1 or later.

The installation is very straightforward. Follow the steps for your particular operating system, whether it be Windows or Mac OS X.

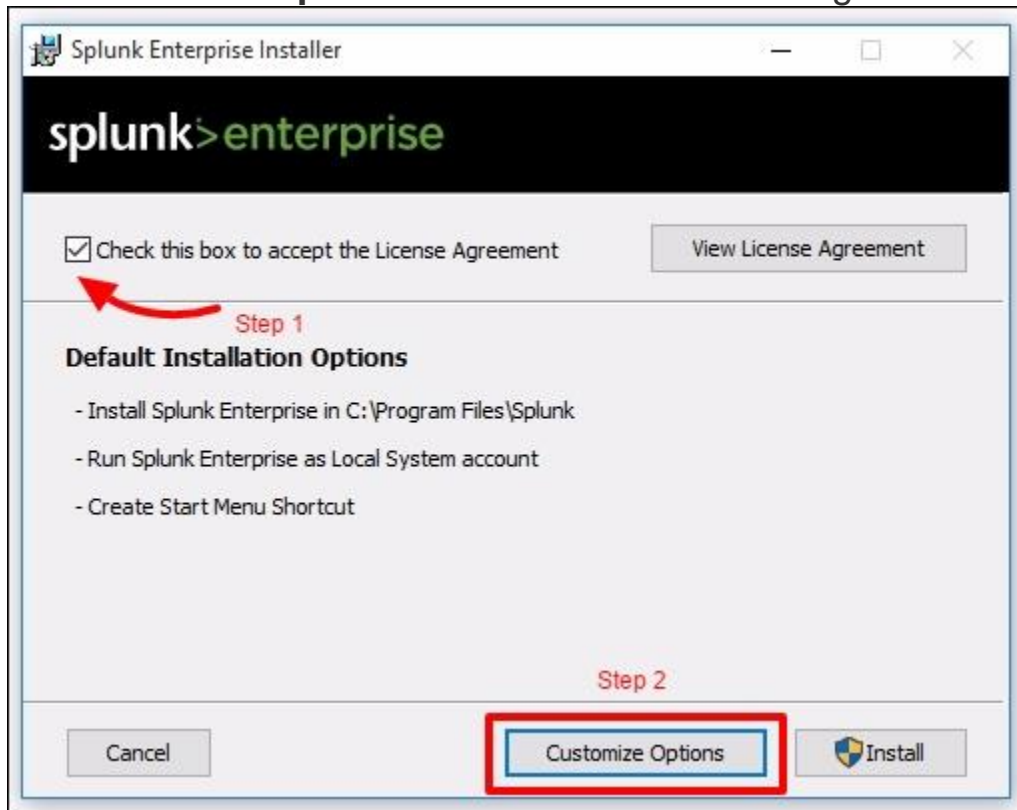
NOTE

Make sure that there is no previous installation of Splunk in your system. If there is, uninstall the old version before proceeding with the next steps.

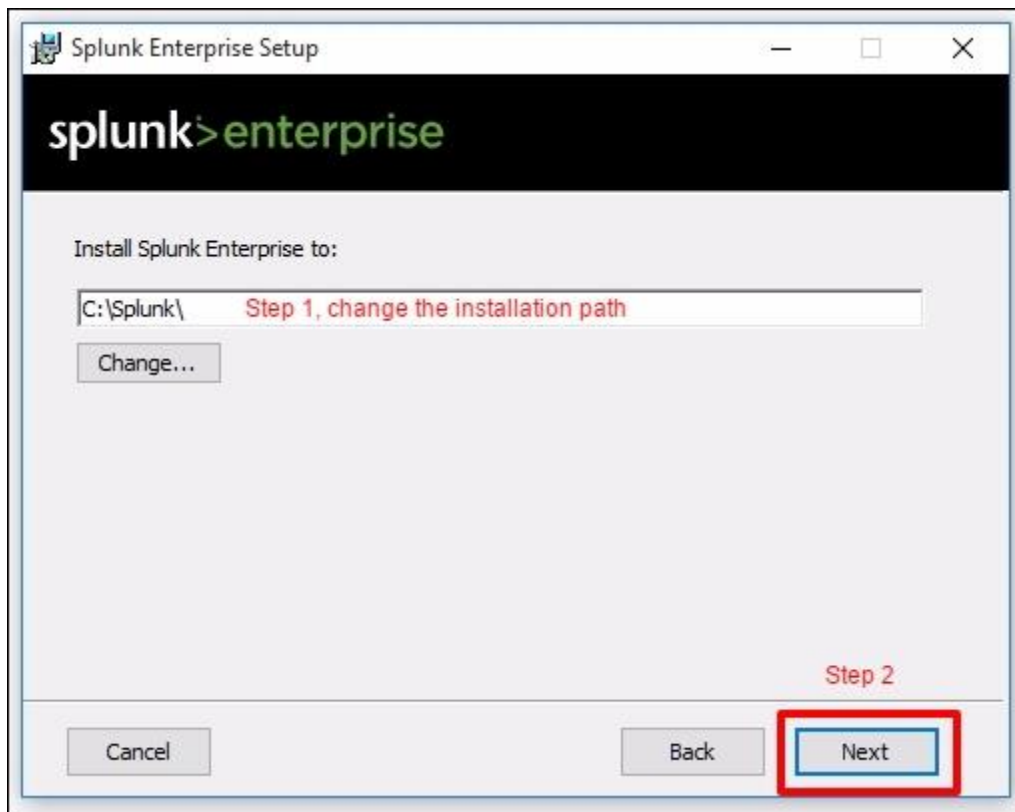
Installing Splunk on Windows

These are the instructions you need to follow to install Splunk on your Windows desktop. Take your time and do not rush the installation. Many chapters in this book will rely on these steps:

1. Run the installer that you downloaded.
2. Check the box to accept the License Agreement and then click on **Customize Options** as shown in the following screenshot:



3. Change the **installation path** to `c:\Splunk`. You will thank us later as it simplifies issuing **Splunk CLI (command-line interface)** commands. This is also a best practice used by modern Windows administrators. Remember to eliminate white spaces in directory names as well, as it causes complications with scripting. Click on **Next** to continue as seen in the following screenshot:



4. Install Splunk Enterprise as the **Local System** and then click on **Next**.
5. Leave the checkbox selected to **Create Start Menu Shortcut**.
6. Click on **Install**.
7. Wait for the installation to complete.
8. Click on **Finish** to complete the installation. It will attempt to launch Splunk for the first time in your default browser.

NOTE

Throughout the book, you will see references to `$SPLUNK_HOME`. This will be the installation directory of Splunk. In Windows, as a convention used in this book, `$SPLUNK_HOME` will be at `C:\Splunk`.

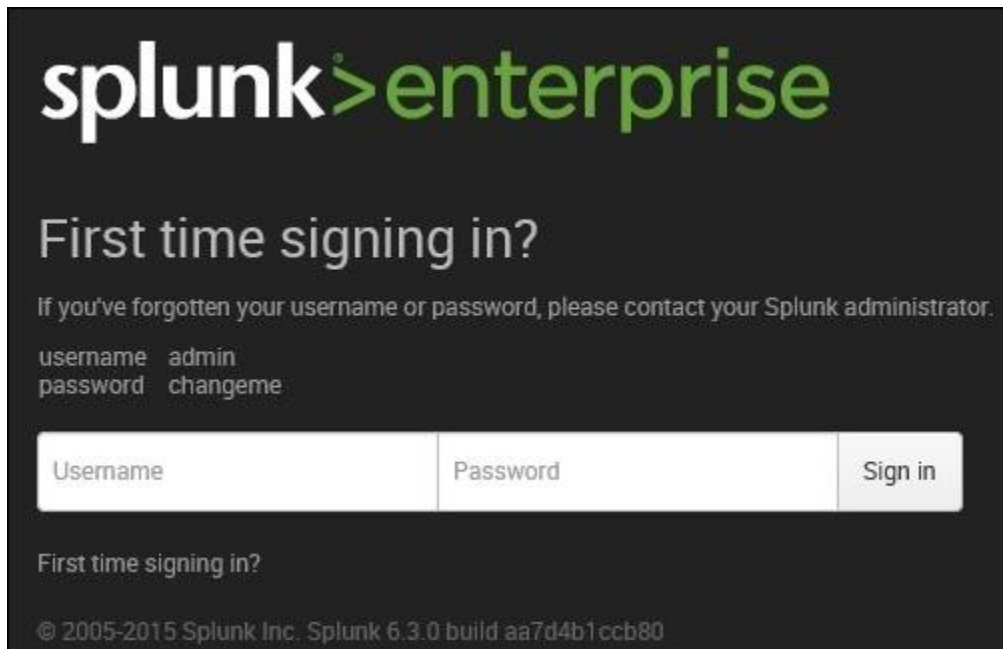
Logging in the first time

Launch the application the first time in your default browser. You can also manually access the Splunk web page via the `http://localhost:8000` URL.

NOTE

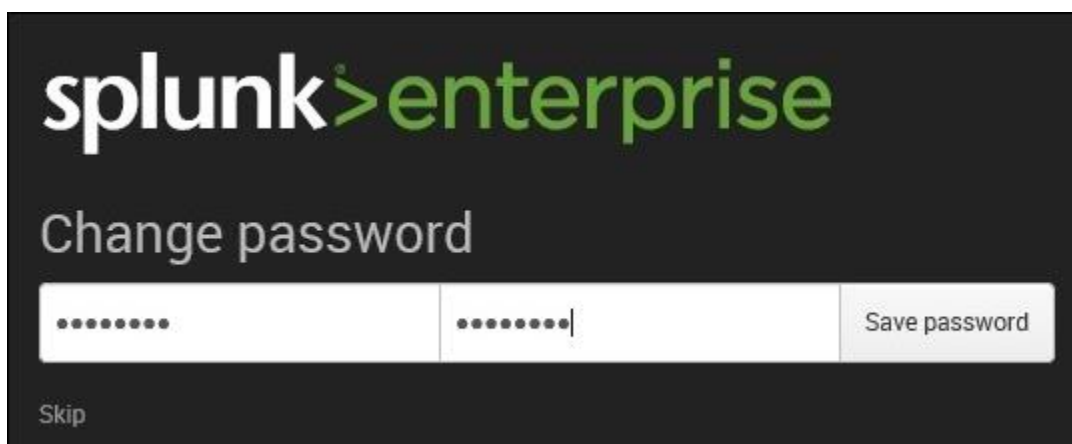
Splunk requires you to use a modern browser. It supports most versions of Google Chrome, Firefox, and newer versions of Internet Explorer. It may not support older versions of Internet Explorer.

Log in with the default username and password (**admin : changeme**) as indicated in the following screenshot:



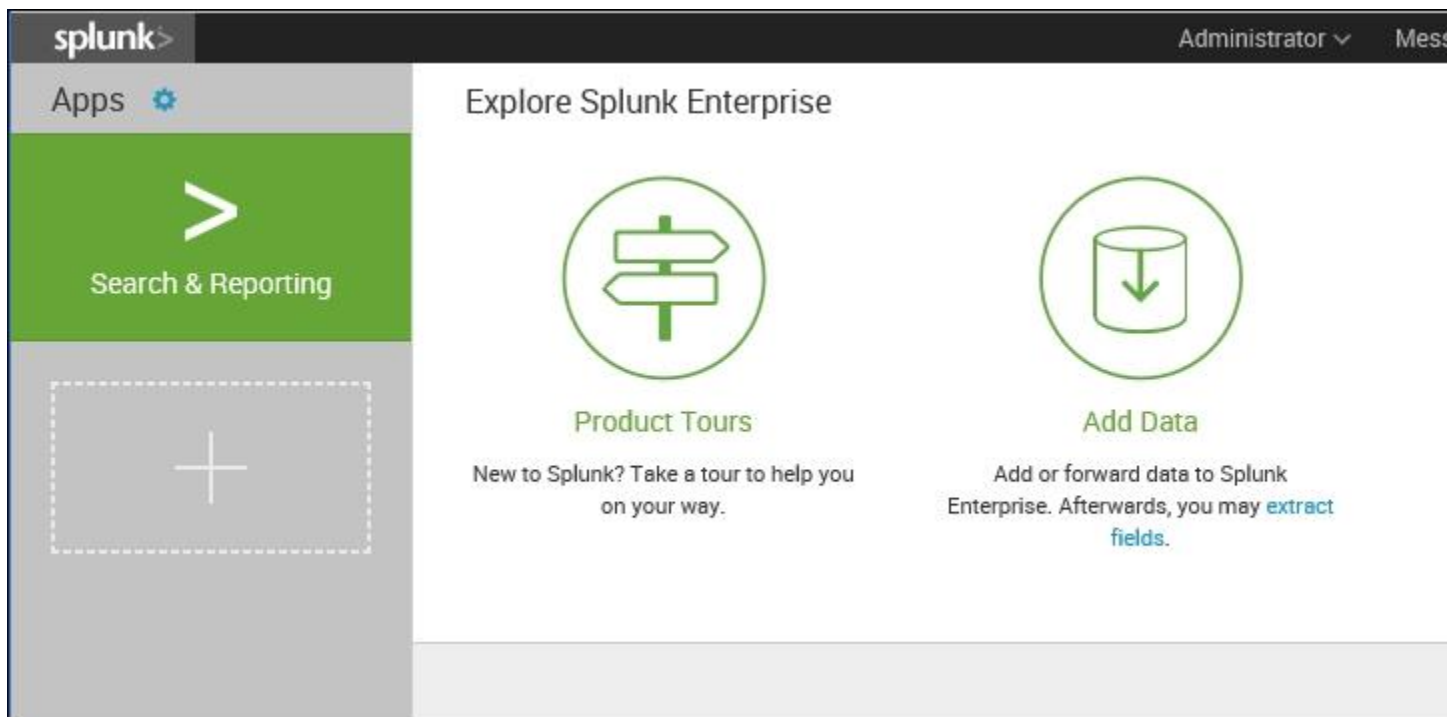
The screenshot shows the Splunk Enterprise login interface. At the top is the 'splunk>enterprise' logo. Below it, the text 'First time signing in?' is displayed. A message states: 'If you've forgotten your username or password, please contact your Splunk administrator.' Below this, the default credentials are listed: 'username admin' and 'password changeme'. There are three input fields: 'Username', 'Password', and a 'Sign in' button. At the bottom, there is a link for 'First time signing in?' and a copyright notice: '© 2005-2015 Splunk Inc. Splunk 6.3.0 build aa7d4b1ccb80'.

The next step is to change the default administrator password, while keeping the default username. Do not skip this step. Make security an integral part of your day-to-day routine. Choose a password that will be secure:



The screenshot shows the 'Change password' page in Splunk Enterprise. It features the 'splunk>enterprise' logo at the top. Below the logo, the text 'Change password' is displayed. There are two password input fields, each containing a series of dots. To the right of the second field is a 'Save password' button. At the bottom left, there is a 'Skip' link.

Assuming all goes well, you will now see the default Splunk **Search & Reporting** dashboard:



Run a simple search

You are finally ready to run your very first Splunk search query:

1. Go ahead and create your first Splunk search query. Click on the **Search & Reporting** app. You will be introduced to Splunk's very own internal index: this is Splunk's way of *splunking* itself (or collecting detailed information on all its underlying processes).
2. In the **New Search** input, type in the following search query (more about the **Search Processing Language (SPL)** in, [Chapter 3, Search Processing Language](#)):

3. `SPL> index=_internal sourcetype=splunkd`

NOTE

The `SPL>` prefix will be used as a convention in this book to indicate a `Search` command as opposed to the `c:\>` prefix which indicates a Windows command.

4. This search query will have as an output the raw events from the `metrics.log` file that is stored in the `_internal` index. A log file keeps track of every event that takes place in the system. The `_internal` index keeps track of every event that occurs and makes it easily accessible.
5. Take a look at these raw events, as shown in the following screenshot. You will see fields listed on the left side of the screen. The important **Selected Fields** are **host**, **source**, and **sourcetype**. We will go into more detail about these later, but suffice it to say that you will frequently search on one of these, as we have done here. As you can see from the highlighted fields, we indicated that we were looking for events where `sourcetype=splunkd`. Underneath **Selected Fields**, you will see **Interesting Fields**. As you can tell, the purposes of many of these fields are easy to guess:

The screenshot shows the Splunk search results interface. At the top, it indicates 2,138 events from 10/31/15 5:48:48.000 AM to 10/31/15 6:03:48.000 AM. Below this is a timeline visualization with a green bar representing the event data. The main panel displays a list of events. The left sidebar shows the 'Selected Fields' (host, source, sourcetype) and 'Interesting Fields' (component, cpu_seconds, cumulative_hits, current_size, current_size_kb, date_hour, date_mday, date_minute).

i	Time	Event
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=thruput, instantaneous_kbps=1.048615, instantaneous_eps=4.129061, average_kbps=0.943057, total_k_processed=31135.000000, kb=32.506836, ev=128.000000 host = WIN-DT11F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=syslog_output, instantaneous_kbps=0.000000, instantaneous_eps=0.000000, average_kbps=0.000000, total_k_processed=0.000000, kb=0.000000, ev=0.000000 host = WIN-DT11F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=thruput, name=index_thruput, instantaneous_kbps=1.048615, instantaneous_eps=3.516154, average_kbps=0.942937, total_k_processed=31131.000000, kb=32.506836, ev=109.000000 host = WIN-DT11F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd
>	10/31/15 6:03:42.401 AM	10-31-2015 06:03:42.401 -0400 INFO Metrics - group=queue, name=winparsing, max_size_kb=500, current_size_kb=0, current_size=0, largest_size=0, smallest_size=0 host = WIN-DT11F5NUKEN source = C:\Splunk\var\log\splunk\metrics.log sourcetype = splunkd

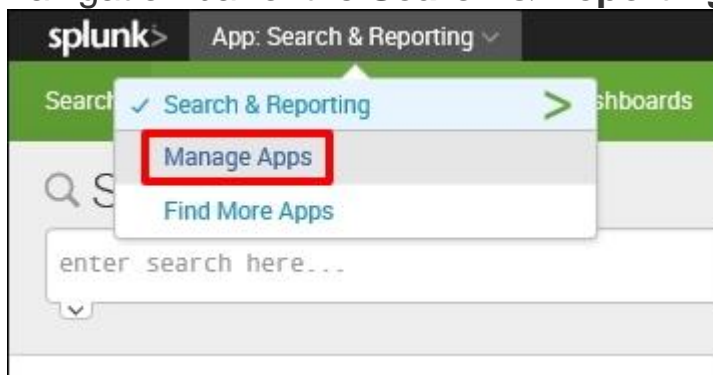
Creating a Splunk app

It is good practice to create a custom Splunk app to isolate all the changes you make in Splunk. You may never have created an app before, but you will quickly see it is not very difficult. Here we will create a basic app called **Destinations** that we will use throughout this book:

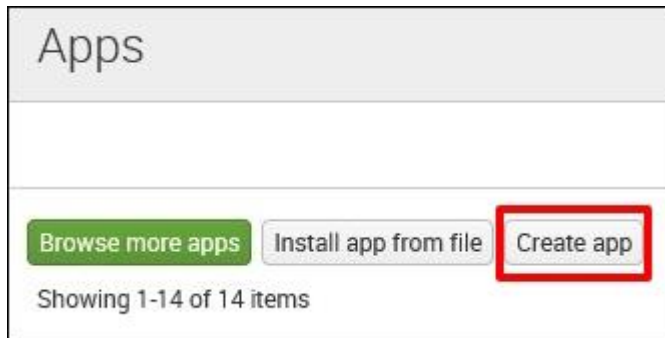
1. Let's access the **Manage Apps** page. There are two ways to do this; you may either click on the **Apps** icon at the *home page* as shown in the following screenshot:



2. Or select **Manage Apps** from the app dropdown in the top navigation bar of the **Search & Reporting** app:



3. At the **Manage Apps** page, click on the **Create app** icon as shown in the following screenshot:



4. Finally, populate the forms with the following information to complete the app creation. When you are done, click on the **Save** button to create your first Splunk app:

Add new

[Apps](#) » Add new

Name

Destinations

Give your app a friendly name for display in Splunk Web.

Folder name *

destinations

This name maps to the app's directory in \$SPLUNK_HOME/etc/apps/.

Version

1.0

App version.

Visible

☐ No ☒ Yes

Only apps with views should be made visible.

Author

Your Name Goes Here

Name of the app's owner.

Description

A custom Splunk application for Destinations

Enter a description for your app.

Template

barebones

These templates contain example views and searches.

Upload asset

Browse...

Can be any html, js, or other file to add to your app.

Cancel

5. You have just created your very first Splunk app. Notice that it now appears in the list of apps and it has a status of **Enabled**, meaning it is ready to be used:

Name ▾	Folder name ▾	Version ▾	Update checking ▾	Visible ▾
SplunkForwarder	SplunkForwarder		Yes	No
SplunkLightForwarder	SplunkLightForwarder		Yes	No
Webhook Alert Action	alert_webhook	6.3.0	Yes	No
Apps Browser	appsbrowser	6.3.0	Yes	Yes
Destinations	destinations	None	Yes	Yes
framework	framework		Yes	No
Getting started	gettingstarted	1.0	Yes	Yes

We will use this bare bones app to complete the exercises in this book, but first we need to make a few important changes:

1. Click the **Permissions** link as show in the preceding screenshot.
2. In the next window, under the **Sharing for config file-only objects** section, select **All apps**.

These steps will ensure that the application will be accessible to the Eventgen add-on that will be installed later in the guide. Use the following screenshot as a guide:

App permissions

Users with read access can only save objects for themselves, and require write access to be able to share objects with other users.

Roles	Read	Write
Everyone	<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"/>

Sharing for config file-only objects

Set permissions for configurations that have been copied over or added to config files rather than created through the UI. Objects defined in config files only (not in the UI) should appear in

☐ This app only (system) ☒ All apps

Cancel Save

Splunk permissions are always composed of three columns: **Roles**, **Read**, and **Write**. A role refers to certain authorizations or permissions that can be taken on by a user. Selecting **Read** for a particular role grants the set of users in the role permission to view the object. Selecting **Write** will allow the set of users to modify the object. In the preceding screenshot, everyone (all users) will have access to view the Destinations app, but only the admin (you) and a power user can modify it.

Populating data with Eventgen

Machine data is the information produced by the many functions carried out by computers and other mechanical machines. If you work in an environment that is rich in machine data, you will most likely have many sources of readily-available machine inputs for Splunk. However, to facilitate learning in this book, we will use a Splunk add-on called the **Splunk Eventgen** to easily build real-time and randomized web log data. This is the type of data that would be produced by a web-based e-commerce company.

NOTE

Here's an important tip. Make it a habit to always launch your command prompt in Administrator mode. This allows you to use commands that are unhindered by Windows security:

1. Right-click on the Windows Start menu icon and select **Search**. In Windows 7, you can click on the Windows icon and the search window will be directly above it. In Windows 10, there is a search bar named **Cortana** next to the Windows icon that you can type into. They both have the same underlying function.
2. In the search bar, type `cmd`.
3. In the search results, look for `command.exe` (Windows 7) or a command prompt (Windows 10), right-click on it, then select **Run as administrator**.

NOTE

Familiarize yourself with this step. Throughout the rest of the class, you will be frequently asked to open a command prompt in Administrator mode. You will know if you are in Administrator mode, as it will say Administrator: Command Prompt in the title of the command prompt window.

Installing an add-on

A Splunk add-on extends and enhances the base functionality of Splunk. They also typically enrich data from source for easier analysis. In this section, you will be installing your first add-on called **Splunk Eventgen** that will help us pre-populate Splunk with real-time simulated web data:

1. First we need to install the Eventgen add-on. If you have Git (<https://git-scm.com>) installed on your machine, you may clone the entire project onto your machine with the following command:

```
2. C:\> git clone https://github.com/splunk/eventgen.git
```
3. You may also download the ZIP file from the Eventgen's public repository, <http://github.com/splunk/eventgen>, and extract it onto your machine. The download ZIP button is in the lower-right corner of the GitHub repository page.



4. After extracting the ZIP file, copy the entire `eventgen` directory into the `$SPLUNK_HOME/etc/apps/` folder. You may need to rename it from `eventgen-master` to `SA-EventGen` if you manually downloaded the ZIP file. The trailing slashes are important. Now open an administrator command prompt and execute the following command:

```
C:\> xcopy eventgen c:\Splunk\etc\apps\SA-Eventgen /O /X /E /H /K
```

In the prompt, type **D**. Verify the contents of the folder using the following command:

```
C:\> dir c:\Splunk\etc\apps\SA-Eventgen
```

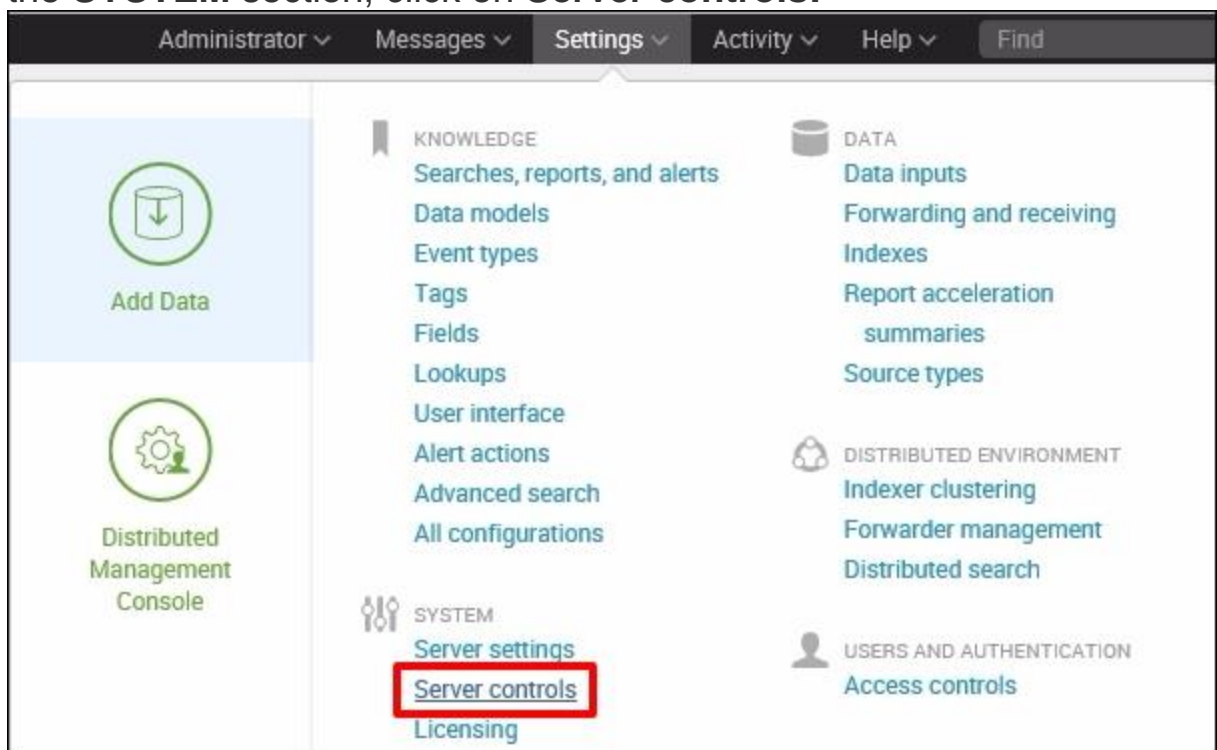
These are the contents of the recently-copied [SA-Eventgen](#) folder as shown in the following screenshot:

```
C:\>dir c:\Splunk\etc\apps\SA-Eventgen
Volume in drive C has no label.
Volume Serial Number is 282F-E3E3

Directory of c:\Splunk\etc\apps\SA-Eventgen

02/04/2016  03:58 AM    <DIR>          .
02/04/2016  03:58 AM    <DIR>          ..
02/04/2016  03:42 AM             162  .gitignore
02/04/2016  03:58 AM    <DIR>          bin
02/04/2016  03:42 AM             677  build.sh
02/04/2016  03:42 AM            1,596  build.xml
02/04/2016  03:58 AM    <DIR>          default
02/04/2016  03:58 AM    <DIR>          lib
02/04/2016  03:42 AM            11,560  LICENSE
02/04/2016  03:58 AM    <DIR>          metadata
02/04/2016  03:58 AM    <DIR>          README
02/04/2016  03:42 AM            11,945  README.md
02/04/2016  03:58 AM    <DIR>          samples
02/04/2016  03:58 AM    <DIR>          tests
                    5 File(s)          25,940 bytes
                    9 Dir(s)  49,145,090,048 bytes free
```

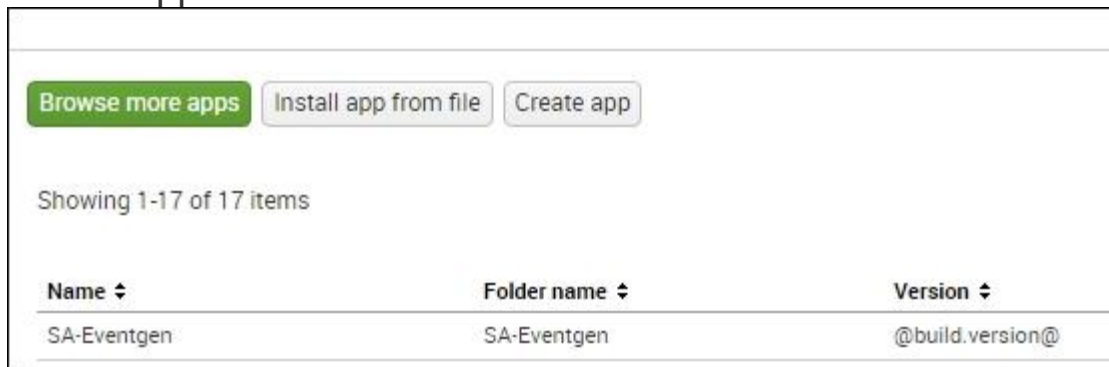
5. Restart Splunk by selecting the **Settings** dropdown, and under the **SYSTEM** section, click on **Server controls**:



6. On the **Server controls** page, click on the **Restart Splunk** button as shown in the following screenshot. Click **OK** when asked to confirm the restart:



7. The web interface will first notify you that Splunk is restarting in the background, then it will tell you that the restart has been successful. Every time Splunk is restarted, you will be prompted to log in with your credentials. Go ahead and log in.
8. Go to the **Manage Apps** page and confirm that the [SA-EventGen](#) application is installed:



You have successfully installed a Splunk add-on.

Controlling Splunk

There are several different ways to stop, start, or restart Splunk. The easiest way is to do it from the web interface, as demonstrated in the preceding section. The web interface, however, only allows you to restart your Splunk instance. It does not offer any other control options.

In Windows, you can also control Splunk through the **Splunkd Service** as shown in the following screenshot. The *d* in the service name, denoting *daemon*, means a background process. Note that the second service, **splunkweb**, is not running. Do not try to start **splunkweb** as it is deprecated and is only there for legacy purposes. The Splunk web application is now bundled in **Splunkd Service**:

 Software Protection	Enables the ...	Automatic (D...	Network S...	
 Splunkd Service	Splunkd is t...	Running	Automatic	Local Syste...
 splunkweb (legacy purposes only)	The splunk...	Automatic	Local Syste...	
 Spot Verifier	Verifies pote...	Manual (Trig...	Local Syste...	

The best way to control Splunk is by using the **command-line interface (CLI)**. It may require a little effort to do it, but using the CLI is an essential skill to learn. Remember to always use command prompts in Administrator mode.

In the console or command prompt, type in the following command and hit **Enter** on your keyboard:

```
C:\> cd \Splunk\bin
```

Here `cd` is a command that means *change directory*.

While in the `C:\Splunk\bin` directory, issue the following command to restart Splunk:

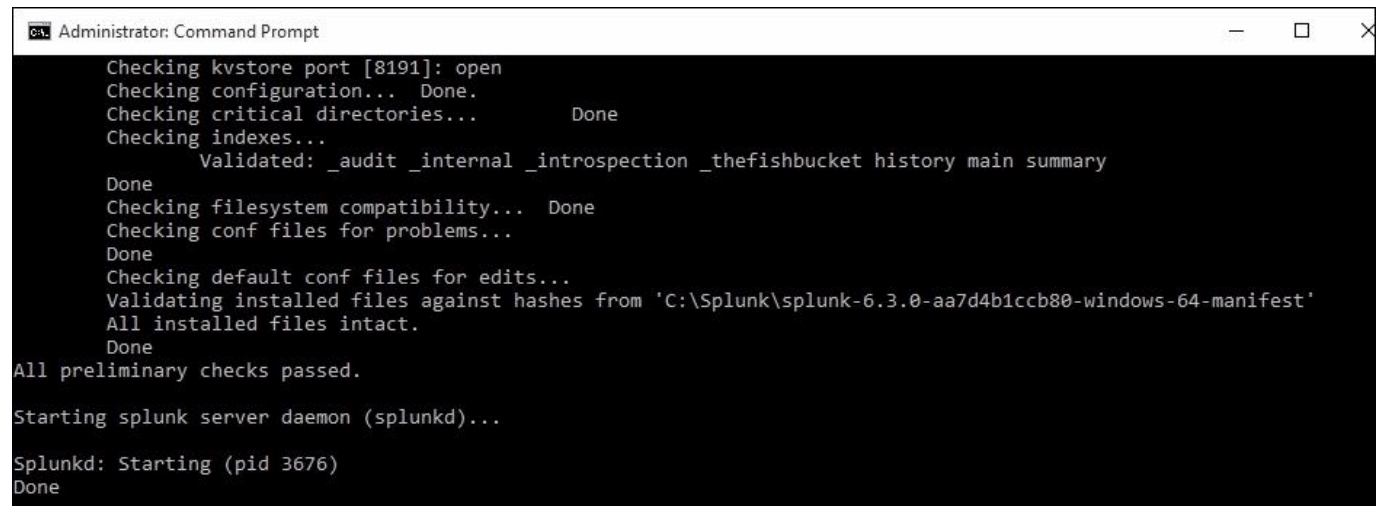
```
C:\> C:\Splunk\bin> splunk restart
```

After issuing this command, `splunkd` will go through its restart process. Here are the other basic parameters that you can pass to the Splunk application to control Splunk:

- `splunk status`: Tells you if splunkd is running or not
- `splunk stop`: Stops splunkd and all its processes
- `splunk start`: Starts splunkd and all its processes
- `splunk restart`: Restarts splunkd and all its processes

Doing this in the console gives the added benefit of verbose messages. A verbose message is a message with a lot of information in it. Such messages can be useful for making sure the system is working correctly or troubleshooting any errors.

A successful restart of splunkd has the following output (which may vary):



```
Administrator: Command Prompt
Checking kvstore port [8191]: open
Checking configuration... Done.
Checking critical directories... Done
Checking indexes...
    Validated: _audit _internal _introspection _thefishbucket history main summary
Done
Checking filesystem compatibility... Done
Checking conf files for problems...
Done
Checking default conf files for edits...
Validating installed files against hashes from 'C:\Splunk\splunk-6.3.0-aa7d4b1ccb80-windows-64-manifest'
All installed files intact.
Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...

Splunkd: Starting (pid 3676)
Done
```

Configuring Eventgen

We are almost there. Proceed by first downloading the exercise materials that will be used in this class. Open an Administrator command prompt and make sure you are in the root of the `c:` drive.

The Eventgen configuration you will need for the exercises in this book has been packaged and is ready to go. We are not going into the details of how to configure Eventgen. If you are interested in learning more about Eventgen, visit the project page at <http://github.com/splunk/eventgen>.

Follow these instructions to proceed:

1. Extract the project ZIP file into your local machine. Open an administrator console and CD into the directory where you extracted the file.

2. Create a new `samples` directory in the Destinations Splunk app. The path of this new directory will be `$SPLUNK_HOME/etc/apps/destinations/samples`:

```
C:\> mkdir c:\splunk\etc\apps\destinations\samples
```

3. Copy all the `*.sample` files from `/labs/chapter01/eventgen` of the extracted project directory into the newly-created `samples` directory. You can also copy and paste using the GUI if you prefer it:

```
C:\> copy splunk-essentials\labs\chapter01\eventgen\*.sample  
c:\Splunk\etc\apps\destinations\samples\
```

4. Now copy the `eventgen.conf` into the `$SPLUNK_HOME/etc/apps/destinations/local` directory. You can also copy and paste using the GUI if you prefer it:

```
C:\> copy splunk-essentials\labs\chapter01\eventgen\eventgen.conf  
c:\Splunk\etc\apps\destinations\local\
```

5. Grant the `SYSTEM` account full access permissions to the `eventgen.conf` file. This is a very important step. You can either do it using the following `icacls` command or change it using the Windows GUI:

```
6. C:\> icacls c:\Splunk\etc\apps\destinations\local\eventgen.conf
```

7. `/grant SYSTEM:F`

A successful output of this command will look like this:

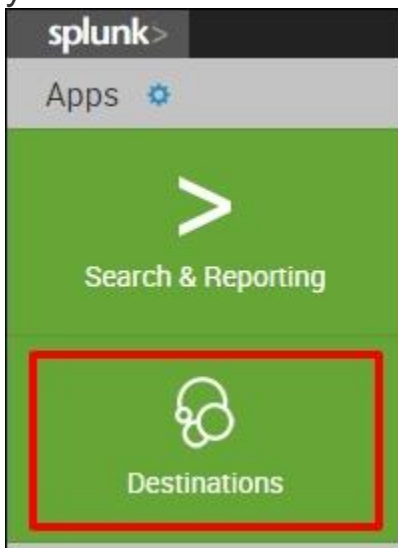
```
processed file:
c:\Splunk\etc\apps\destinations\local\eventgen.conf
Successfully processed 1 files; Failed processing 0 files
```

8. Restart Splunk.

Viewing the Destinations app

Next we will see our Destinations app in action! Remember that we have configured it to draw events from a prototype web company. That is what we did when we set it up to work with Eventgen. Now let's look at some of our data:

1. After a successful restart, log back in to Splunk and proceed to your new Destinations app:



2. In the **Search** field, type this search query and select **Enter**:

3. `SPL> index=main`

New Search

index=main

✓ 172 events (before 11/1/15 11:22:06.000 AM)

Job

Events (172)

Patterns

Statistics

Visualization

Format Timeline

– Zoom Out

+ Zoom to Selection

× Deselect

List

Format

20 Per Page

< Prev

1

< Hide Fields

All Fields

Selected Fields

a host 1

a source 1

a sourcetype 1

Interesting Fields

date_hour 2

date_mday 1

date_minute 30

a date_month 1

date_second 54

a date_wday 1

date_year 1

a date_zone 1

a index 1

linecount 1

a punct 52

a splunk_server 1

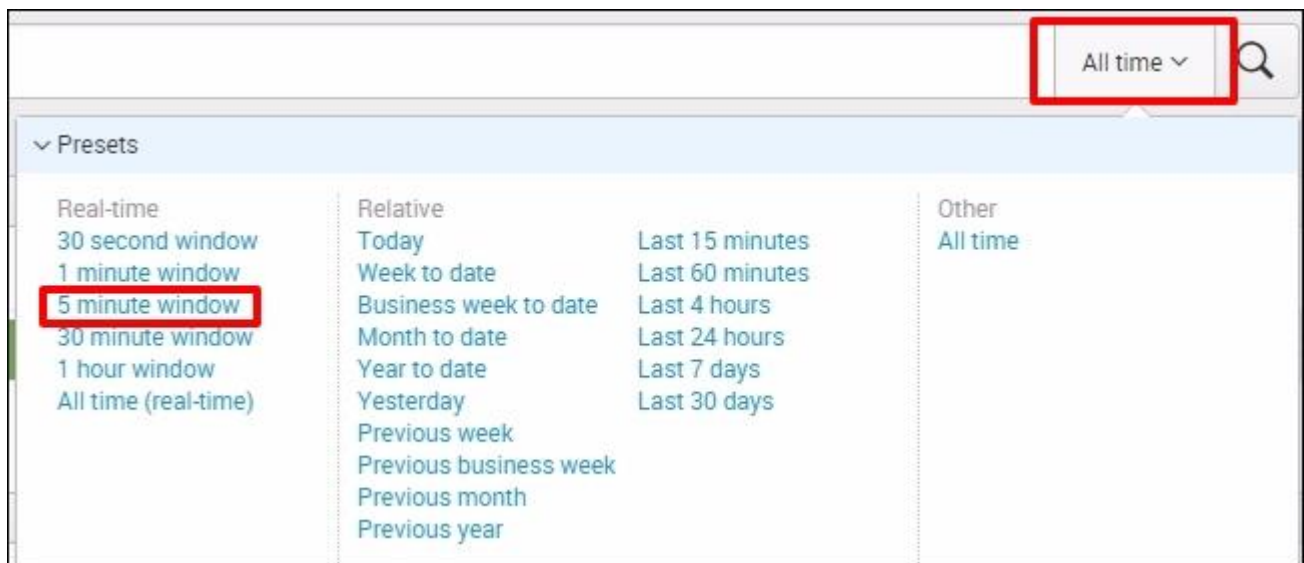
timeendpos 1

timestartpos 1

i	Time	Event
>	11/1/15 11:22:04.334 AM	2015-11-01 11:22:04:334000 128.241.220.0.2.1.35 "Mozilla/5.0 (Linux; U; And d/GRJ22) AppleWebKit/533.1 (KHTML, like 3.1" 500 0 0 602 13702015-11-01 11:21:580 - 10.2.1.35 "Mozilla/5.0 (iPhone; U; a_JP) AppleWebKit (KHTML, like Gecko) M BV/4030.0;FBDV/iPhone2,1;FBMD/iPhone;FB R/???????????;FBID/phone;FBLC/ja_JP;FBSF host = www.destinations.com source = /var/log/ sourcetype = access_custom
>	11/1/15 11:21:53.328 AM	2015-11-01 11:21:53:328000 141.146.8.660.2.1.34 "Mozilla/5.0 (Linux; U; Androi ld/ERE27) AppleWebKit/530.17 (KHTML, li 30.17" 404 0 0 986 879 host = www.destinations.com source = /var/log/ sourcetype = access_custom
>	11/1/15 11:21:38.324 AM	2015-11-01 11:21:38:324000 128.241.220.0.2.1.35 "Mozilla/5.0 (Linux; U; Androi pleWebKit/533.1 (KHTML, like Gecko) Ver 346 21622015-11-01 11:21:44:324000 12.1 - 10.2.1.33 "Mozilla/5.0 (iPad; U; CPU ebKit/533.17.9 (KHTML, like Gecko) Vers 8.5" 404 0 0 165 3321 host = www.destinations.com source = /var/log/ sourcetype = access_custom

Examine the event data that your new app is enabling to come into Splunk. You will see a lot of references to browsers, systems, and so forth: the kinds of information that make a web-based e-commerce company run.

Try changing the time range to **Real-time (5 minute window)** to see the data flow in before your eyes:



Congratulations! You now have real-time web log data that we can use in subsequent chapters.

Creating your first dashboard

Now that we have data ingested, it is time to use it in order to derive something meaningful out of it. You are still in the Destinations app, correct? We will show you the basic routine when creating new dashboards and dashboard panels.

Copy and paste the following search query in the **Search Field**, then hit **Enter**:

```
SPL> index=main /booking/confirmation earliest=-24h@h |  
timechart  
count span=15m
```

After the search results render, click on the **Visualization** tab. This will switch your view into visualization so you can readily see how your data will look. By default, it should already be using the **Column Chart** as shown in the following screenshot. If it does not, then use the screenshot as a guide on how to set it:

New Search

index=main /booking/confirmation earliest=-24h@h | timechart count span=15m

✓ 1 event (7/10/16 7:00:00.000 AM to 7/11/16 7:55:37.819 AM) No Event Sampling ▾

Events Patterns Statistics (100) Visualization

Column Chart ▾ Format ▾

Recommended

- Line Chart
- Area Chart
- Column Chart** 42 ▾

Splunk Visualizations

- Line Chart
- Area Chart
- Column Chart
- Horizontal Bar Chart
- Pie Chart
- Scatter Plot
- World Map
- 42 ▾
- Gauge Chart
- Bar Chart

Find more visualizations [↗](#)

Column Chart
Compare values or fields.

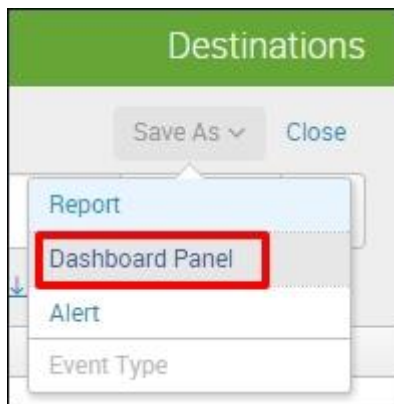
Search Fragment
| stats count by comparison_category

6:00 PM

_time

2016-07-10 07:15:00

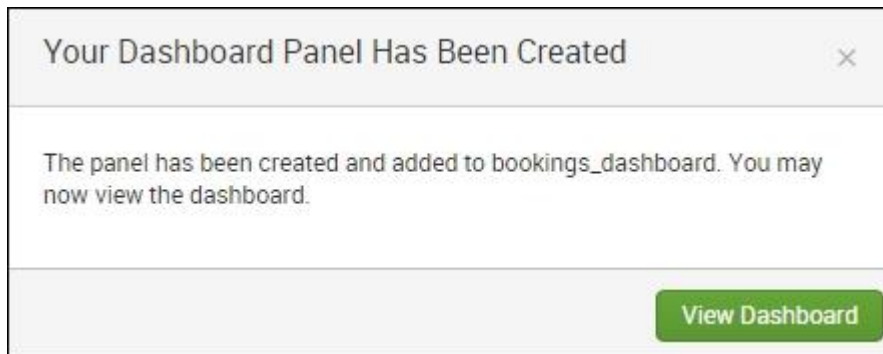
Now that you can see your **Column Chart**, it is time to save it as a dashboard. Click on **Save As** in the upper-right corner of the page, then select **Dashboard Panel** as shown in the following screenshot:



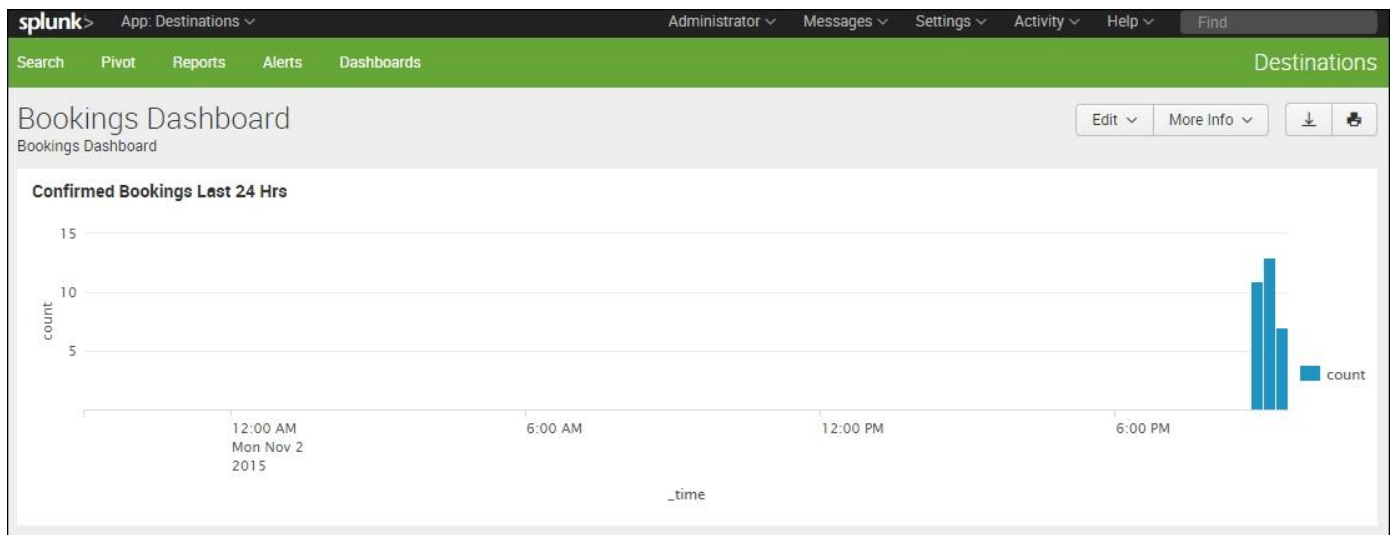
Now let's fill up that dashboard panel information, as seen in the following screenshot. Make sure to select the **Shared in App** in the **Dashboard Permissions** section:

A screenshot of a "Save As Dashboard Panel" dialog box. The dialog has a title bar with a close button. Inside, there are several fields and buttons. The "Dashboard" section has "New" and "Existing" buttons. The "Dashboard Title" field contains "Bookings Dashboard". The "Dashboard ID" field contains "bookings_dashboard" with a note below it: "Can only contain letters, numbers and underscores." The "Dashboard Description" field contains "Bookings Dashboard". The "Dashboard Permissions" section has "Private" and "Shared in App" buttons, with "Shared in App" highlighted by a red box. Below this, the "Panel Title" field contains "Confirmed Bookings Last 24 Hrs". The "Panel Powered By" field contains "Q Inline Search". The "Panel Content" section has "Statistics" and "Column" buttons, with "Column" highlighted by a red box. At the bottom, there are "Cancel" and "Save" buttons.

Finish up by clicking **View Dashboard** in the next prompt:



You have created your very first Splunk dashboard with a panel that tells you the number of confirmed bookings in the last 24 hours at 15-minute intervals. Time to show it to your boss!



Take that well-deserved coffee break. You now have a fully-functional Splunk installation with live data. Leave Splunk running for 2 hours or so. After a few hours, you can stop Splunk if you need to rest for a bit to suppress indexing and restart it when you're ready to proceed into the next chapters. Do you recall how to control Splunk from the command line?

```
C:\> C:\Splunk\bin> splunk stop
C:\Splunk\bin> splunk start
```

Summary

In this section, you learned a number of basic Splunk concepts that you need to get started with this powerful tool. You learned how to install Splunk and configure a new Splunk app. You ran a simple search to ensure that the application is functional. You then installed a Splunk add-on called Eventgen, which you used to populate dummy data into Splunk in real time. You were shown how to control Splunk using the web user interface and the command-line interface. Finally, you created your very first Splunk dashboard. Now we will go on in the next section, *Bringing in Data*, to learn more about how to input data.