Table of Contents

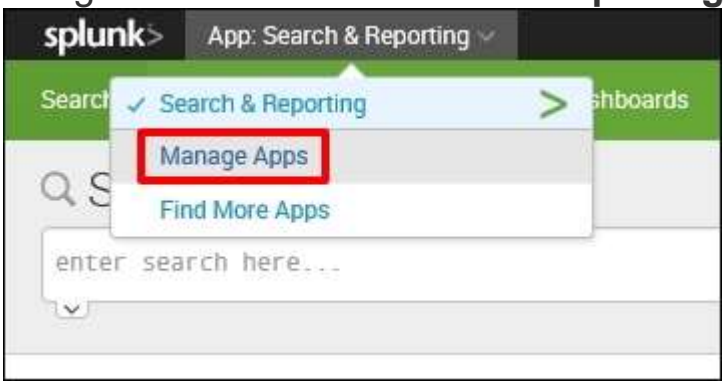
Creating a Splunk app 2
Populating data with Eventgen 6
NOTE 6
NOTE 6
Installing an add-on 7
Configuring Eventgen 10
Viewing the Destinations app 12

Creating a Splunk app

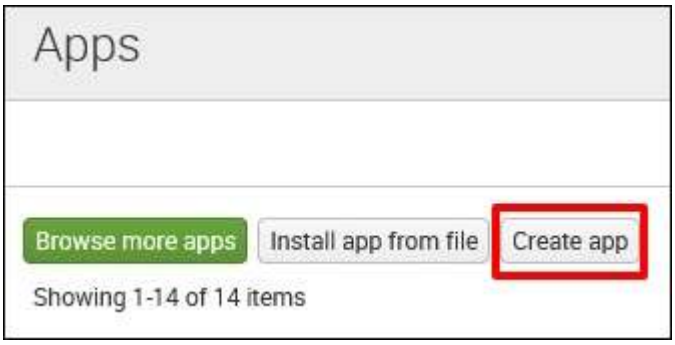
It is good practice to create a custom Splunk app to isolate all the changes you make in Splunk. You may never have created an app before, but you will quickly see it is not very difficult. Here we will create a basic app called **Destinations** that we will use throughout this book:

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:



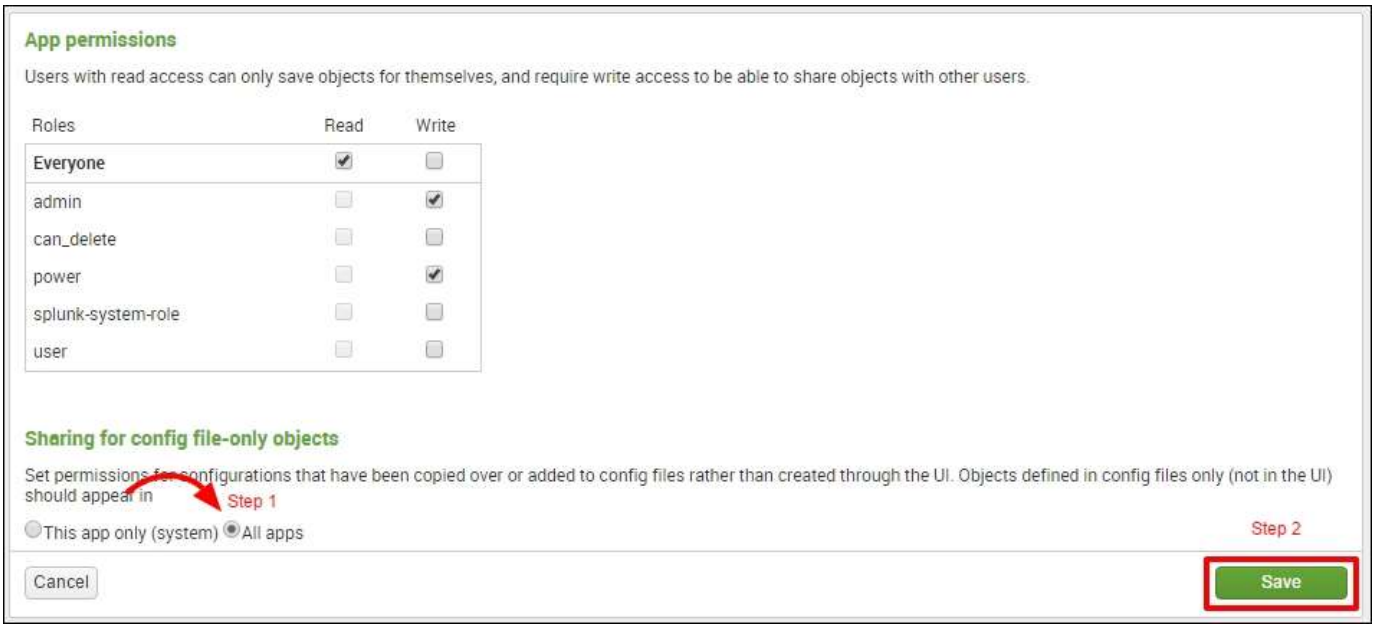
4. Finally, populate the forms with the following information to complete the app creation. When you are done, click on the **Save** button to create your first Splunk app:

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:

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 chapter. Use the following screenshot as a guide:



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

If you need more detailed information about Eventgen, you can follow the project's GitHub repository at https://github.com/splunk/eventgen/.

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 book, 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:

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

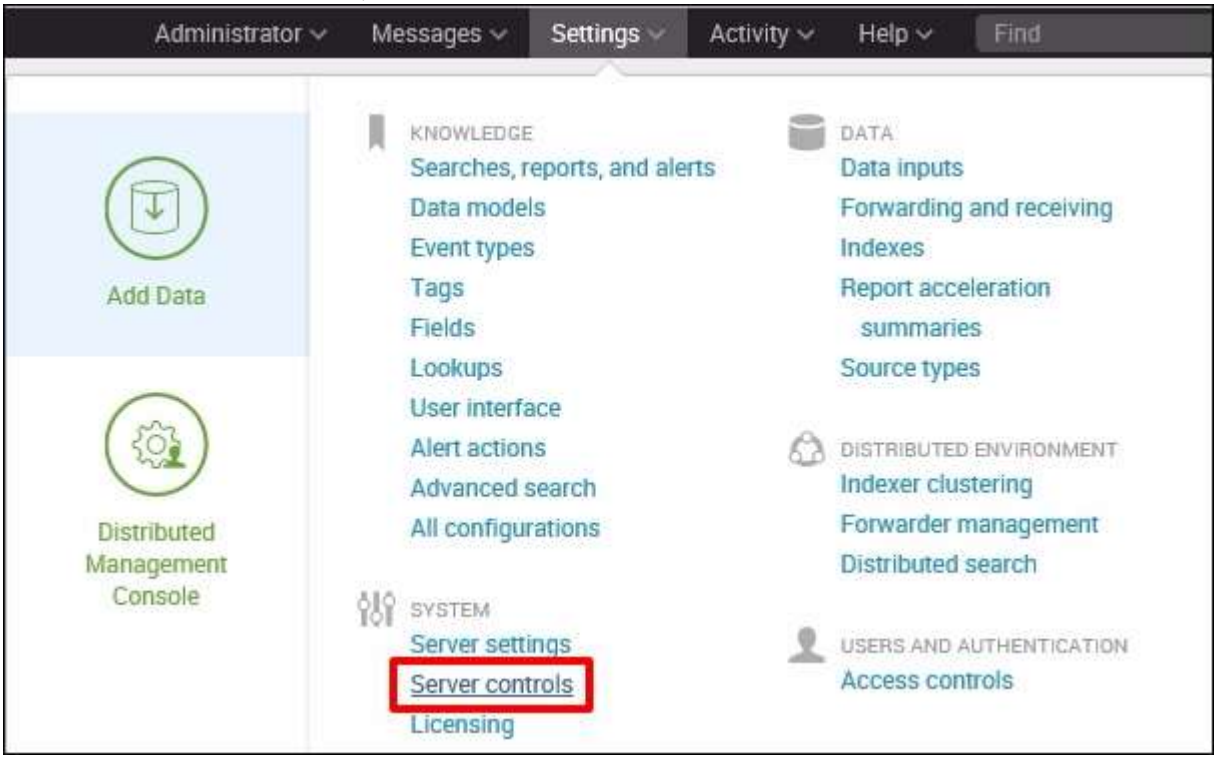
   In the prompt, type **D**. Verify the contents of the folder using the following command:

```
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
```

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



7. 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:

8. 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.
9. Go to the **Manage Apps** page and confirm that the `SA-EventGen`application is installed:

You have successfully installed a Splunk add-on.

Configuring Eventgen

We are almost there. Proceed by first downloading the exercise materials that will be used in this book. Open an Administrator command prompt and make sure you are in the root of the `C:` drive. If you are using Git, clone the entire project with this Git command:

```
C:\> git clone https://github.com/ericksond/splunk-essentials.git
```

You can alternatively just download the ZIP file and extract it in your computer using https://github.com/ericksond/splunk-essentials/archive/master.zip.

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:

```
C:\> icacls c:\Splunk\etc\apps\destinations\local\eventgen.conf
      /grant SYSTEM:F
```

   A successful output of this command will look like this:

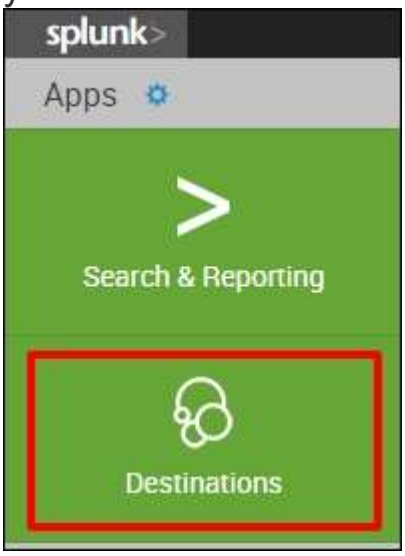
```
processed file:
c:\Splunk\etc\apps\destinations\local\eventgen.conf

Successfully processed 1 files; Failed processing 0 files
```

6. Restart Splunk.

Viewing the Destinations app

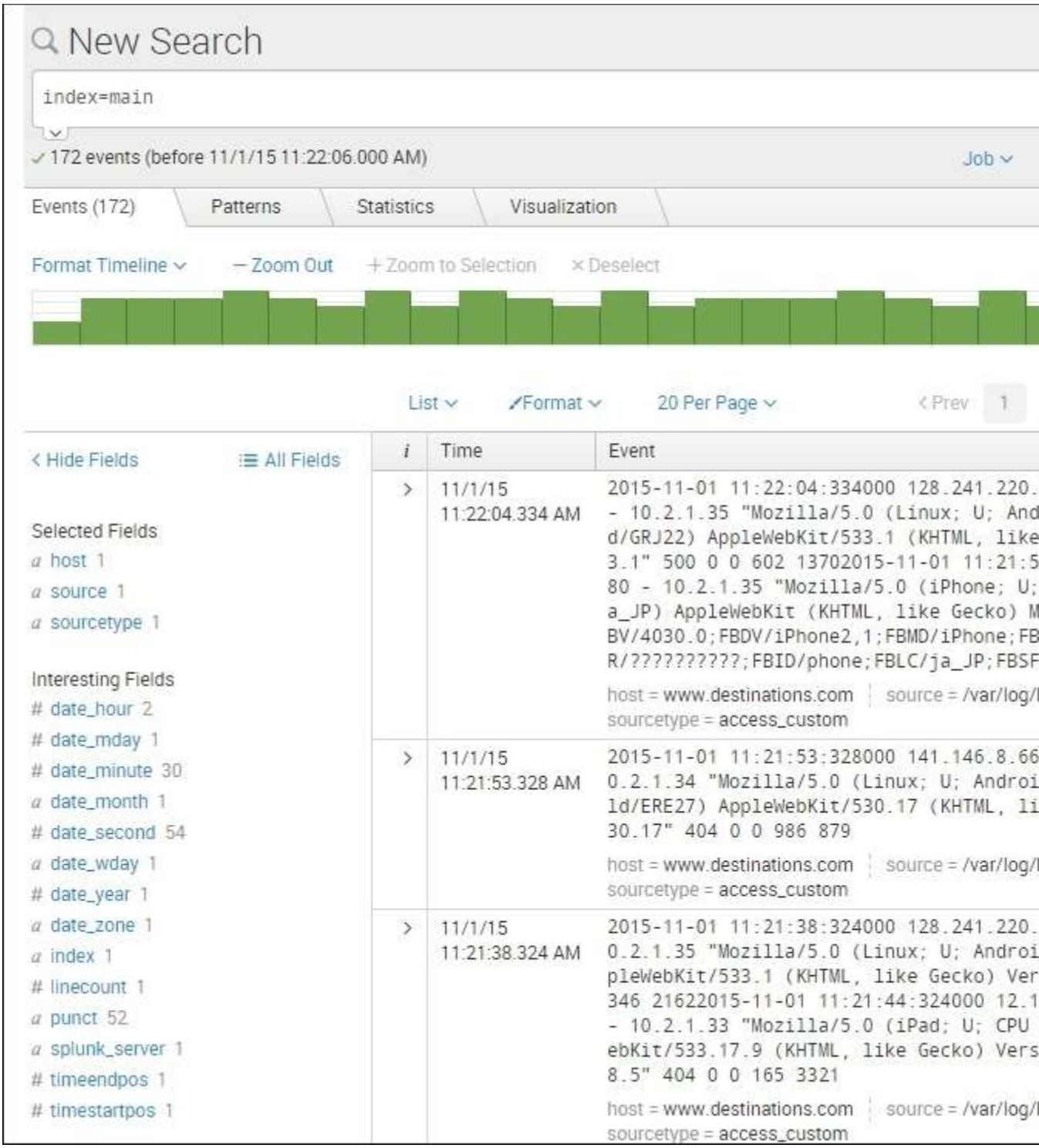
Next we will see our Destinations app in action! Remember that we have configured it to draw events from a prototype web company. That is what we did when we set it up to work with Eventgen. Now let's look at some of our data:

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



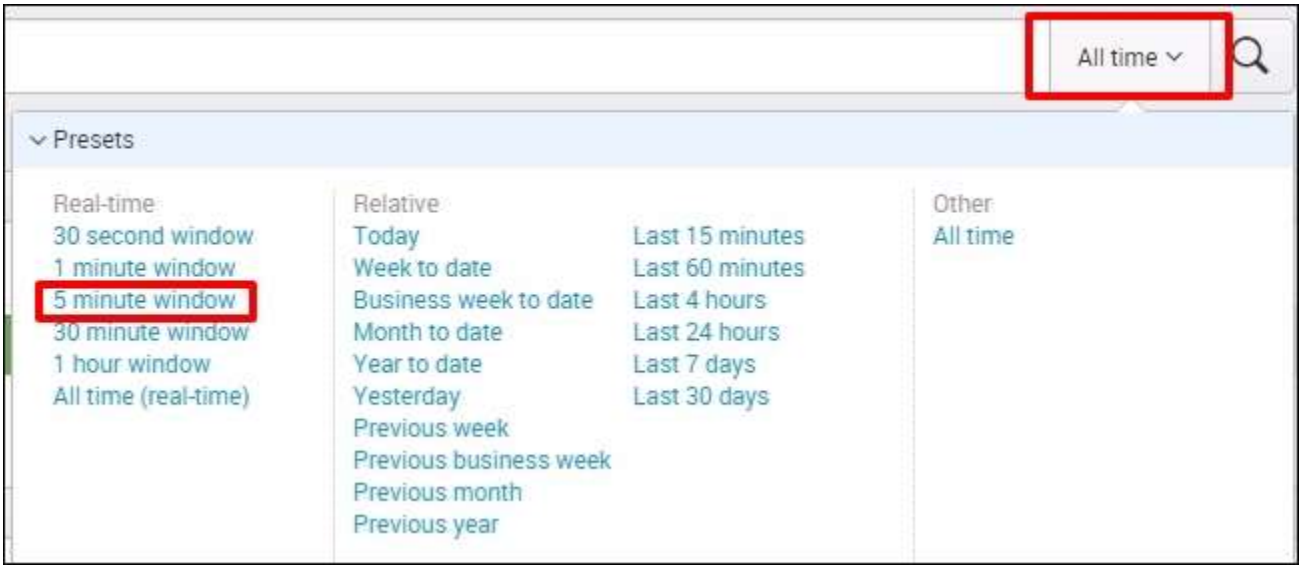
2. In the **Search** field, type this search query and select **Enter**:

```
3. SPL> index=main
```



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.