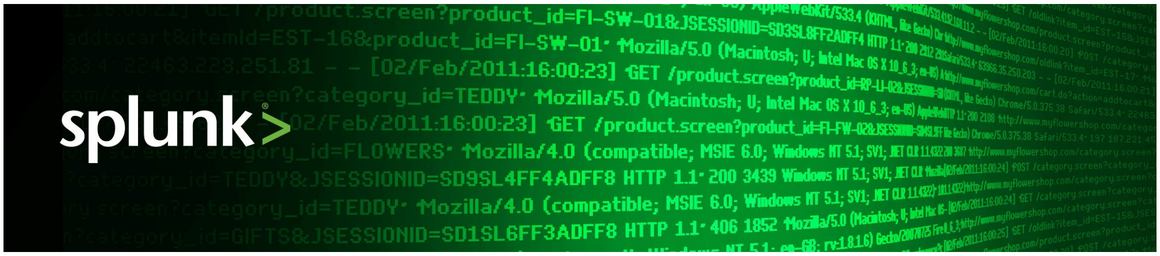

Splunk® Enterprise Data Model and Pivot Tutorial 6.2.2

About the Data Model and Pivot Tutorial

Generated: 2/23/2018 11:52 am

About the Data Model and Pivot Tutorial

This tutorial guides you through adding data to your Splunk deployment, building simple data models from this tutorial data, and creating new pivots from the data models.

Prerequisites for this tutorial

This tutorial assumes that you have access to a Splunk deployment. If you are using Splunk Enterprise and need instructions for installing and starting the product, see the following topics in the *Search Tutorial*.

- Install Splunk Enterprise on Linux, Windows, or Mac OS X
- Start Splunk Enterprise and launch Splunk Web

What's covered in this tutorial?

A breakdown of what you will find in each of the sections of this tutorial follows.

- **Introduction** describes the pre-requisites and system requirements for completing this tutorial. It also describes **Splunk Web**, which is the interface for using Splunk Enterprise and Pivot.
- **Part 1: Getting data into Splunk Enterprise** walks you through adding the tutorial data into Splunk Enterprise. The tutorial data, which is a sample data set composed of web server and MySQL logs for a fictional online game store, is included for download in this chapter.
- **Part 2: Building a data model** walks you through creating a new data model, defining the root object, editing object attributes, defining child attributes.
- **Part 3: Designing a Pivot report** walks you through creating and saving Pivot tables and charts.
- **Part 4: Creating dashboards** walks you through creating new dashboards and adding Pivots to new and existing dashboards.

Using a PDF of the tutorial

Do not copy and paste searches or regular expressions directly from the PDF into Splunk Web. In some cases, doing so causes errors because of hidden characters that are included in the PDF formatting.