



Sputnik Installation and Configuration Guide

Contents

Introduction.....	2
Installing Sputnik (Local Linux Machine).....	2
Sputnik Operation	2
Creating an Amazon EC2 instance for Sputnik.....	3
Configuring your EC2 Instance's Security Settings	4
Installing Sputnik (EC2).....	4

Introduction

Sputnik is Teradek's interface between Bond and your streaming destination. Sputnik is designed to run on a Linux computer either in the cloud (using Amazon's EC2 services) or on a local server with a single, publically addressable TCP port. For Amazon EC2 configuration, start with [Creating an Amazon EC2 instance for Sputnik](#), page 3.

Installing Sputnik (Local Linux Machine)

1. Download the Sputnik RPM file. This package contains the Sputnik binaries and configuration files.
2. Open your file browser and navigate to the directory containing the Sputnik RPM.
3. Double click to open your package manager and follow prompts to install Sputnik.
4. You will be prompted for an administrator password to complete the installation.

Note: As of Sputnik version 1.0, the following Linux distributions have been tested:

- Fedora 13
- Fedora 14
- Fedora 15
- Amazon Linux 2011
- Enterprise Linux 6

Sputnik Operation

1. To start Sputnik: `sudo service sputnik start`
2. To stop Sputnik: `sudo service sputnik stop`
3. To restart Sputnik: `sudo service sputnik restart`
4. Sputnik log file location: `/var/log/sputnik.log` (to view Sputnik's output while it is running, use `'tail -f /var/log/sputnik.log'`)
5. Sputnik configuration file location: `/etc/sputnik.conf`
 - i. Sputnik's configuration file contains two options – verbosity and the listening port. Sputnik must be restarted after any changes are made to the configuration.
 - ii. Verbosity: Set to 1 for minimal log messages, 2 for more detailed logging.
 - iii. Listening Port: Default is 5111. This option allows you to specify the TCP port that Sputnik uses to listen for connections from Bond devices.

Creating an Amazon EC2 instance for Sputnik

1. go to: <https://console.aws.amazon.com/s3/home>
2. Log in to your account, or sign up if you have not done so already.
3. Click the 'Amazon EC2' tab.
4. Select the appropriate Region on the left navigation pane.
5. Set up a new Security Group if you have not done so already. See Configuring your EC2 Instance's Security Settings, page 4 for details.
6. Select 'Instances' in the navigation pane.
7. Click the large 'Launch Instance' button.
8. Select 'Launch Classic Wizard.'
9. Select the 'Community AMIs' tab and wait for the AMI List to load.
10. Select 'Amazon Images' in the 'Viewing' dropdown and search for 'amzn-ami-2011.' Choose an i386 ami with 'instance-store' as the root device. Click the 'Select' button next to your chosen AMI. Your AMI name will look something like 'amzn-ami-2011.09.02.i386-S3.'
11. Choose your instance details. These details affect the pricing and resources available to you. For one or two encoders streaming to Sputnik, the 'm1.small' instance type should be sufficient.
12. Add a name to your instance by specifying it next to 'Name' in the 'Value' column on the tags page.
13. Create a Key-Pair.
14. Download the '.pem' permissions file. This file is required for SSH access to your Sputnik server. The permissions file can only be downloaded once from Amazon, so it may be wise to create a backup of the file.
15. Select the Security Group you configured in step 5 or configure a new one according to Configuring your EC2 Instance's Security Settings if you haven't already. Click Continue.
16. Review your settings and then click 'Launch.' After a short while your new EC2 instance will show as running in the Instances section of the AWS Management Console.
17. To give your EC2 instance a fixed address, Navigate to the 'Elastic IPs' section, click the 'Allocate New Address' button and confirm by clicking 'Yes, allocate' (make sure 'EC2' is selected).
18. Select the newly listed Address listing and click the 'Associate Address' button. Select your newly created instance and click 'Yes, Associate.'
19. Your Amazon EC2 instance should now be running and ready for Sputnik installation.
20. NOTE: For the most up-to-date documentation, consult Amazon's 'Get Started with EC2' guide, located at <http://docs.amazonwebservices.com/AWSEC2/latest/GettingStartedGuide/>

Configuring your EC2 Instance's Security Settings

1. Select 'Security Groups.'
2. Click 'Create Security Group.'
3. Enter a name and description for your security group. Make sure 'No VPC' is selected and click 'Yes, Create.'
4. Select the 'Inbound' tab, and create a new 'Custom TCP rule' for port 5111. This is the default port used for connections between Bond and Sputnik. Click 'Add Rule.' If
5. Create a new rule for SSH. This is required to access your EC2 instance to start, stop, or configure Sputnik.
6. After adding the rules, the listing on the right should look similar to the following:

TCP Port (Service)	Source	Action
5111	0.0.0.0/0	Delete
22 (SSH)	0.0.0.0/0	Delete

7. Click 'Apply Rule Changes' at the bottom of the Security Group pane.

Installing Sputnik (EC2)

Download the Sputnik RPM file. This package contains the Sputnik binaries and configuration files. For convenience, save the RPM file to the same directory as your permissions file (Creating an Amazon EC2 instance for Sputnik, step 13).

1. Mac/Linux users -- open a terminal and navigate to the directory where your permissions file is saved. Replace `<pem-file-location>` with the path to your permissions file.

```
$ cd <pem-file-location>
```
2. Modify the permissions of the `.pem` file using `chmod`. Replace `<pem-file.pem>` with the permissions file name.

```
$ chmod 400 <pem-file.pem>
```
3. Using `scp`, copy the file to your EC2 instance. You will need to use the IP address configured in Creating an Amazon EC2 instance for Sputnik, steps 16 and 17. Replace `<pem-file.pem>` with the permissions file name, `<sputnik-rpm>` with the Sputnik RPM name (and path if not in the same directory), and `<ip-address>` with the address of your EC2 instance.

```
$ scp -i <pem-file.pem> <sputnik-rpm> ec2-user@<ip-address>:~/
```

4. Connect via SSH to your Amazon EC2 instance. Replace `<pem-file.pem>` with the permissions file name and `<ip-address>` with the address of your EC2 instance.

```
$ ssh -i <pem-file.pem> ec2-user@<ip-address>
```
5. If you are prompted, type 'yes' to continue.
6. Install Sputnik using `yum`. Replace `<sputnik-rpm>` with the Sputnik RPM name. NOTE: type `ls` to view the contents of your current directory, this will display the RPM name, among other things.

```
$ sudo yum -y --nogpgcheck localinstall <sputnik-rpm>
```
7. Follow the instructions in Sputnik Operation, page **2** for information on configuring and running Sputnik.