Splunk® Light Installation Manual 6.6.3

Generated: 9/13/2017 2:20 pm

Table of Contents

Install Splunk Light

System requirements for Splunk Light

This topic defines the computing requirements for running Splunk Light.

Hardware requirements

The following are the minimum and recommended hardware requirements for running Splunk Light.

Platform	Minimum supported hardware	Recommended hardware
Non-Windows platforms	1x1.4 GHz CPU, 1 GB RAM	2x six-core, 2+ GHz CPU, 12 GB RAM, Redundant Array of Independent Disks (RAID) 0 or 1+0, with a 64 bit OS installed.
Windows platforms	Intel Nehalem CPU or equivalent at 2 GHz, 2 GB RAM	2x six-core, 2+ GHz CPU, 12 GB RAM, Redundant Array of Independent Disks (RAID) 0 or 1+0, with a 64 bit OS installed.

Operating system support

The following tables list the computing platforms (operating system and architecture) supported by Splunk Light and the Universal Forwarder, including *nix and Windows operating systems.

Unix operating systems

Unix operating system	Architecture	Splunk Light	Universal Forwarder
Linux, 2.6 and later	x86 (64-bit)	**X**	**X**
	x86 (32-bit)		**D**
Linux, 3.x and later	x86 (64-bit)	**X**	**X**
	x86 (32-bit)		**D**
Mac OS X 10.10	Intel		**D**

Mac OS X 10.11 and 10.12	Intel	**X**	**X**

Windows operating systems

Windows operating system	Architecture	Splunk Light	Universal Forwarder
Windows Server 2008 R2	x86 (64-bit)	**D**	**D**
Windows Server 2012, Server 2012 R2, and Server 2016	x86 (64-bit)	**X**	**X**
Windows 8, 8.1, and 10	x86 (64-bit)	**X**	**X**
	x86 (32-bit)	**X**	**X**

X indicates software is available for this platform.
D indicates deprecated. Support for this platform might be removed in a future release.
An empty box indicates software is not supported for this platform.

File system support

Splunk Light supports the following file systems.

Platform	File systems
Windows	NTFS and FAT32
Mac OS X	HFS and NFS 3/4
Linux	ext2, ext3, ext4, btrfs, XFS, and NFS 3/4

Browser support

Splunk Light supports the following browsers.

Browser	Versions
Firefox	Latest
Internet Explorer	11
Safari	Latest
Chrome	Latest

Install Splunk Light using Windows

The topic includes instructions for installing Splunk Light on Windows using the MSI package.

You can download Splunk Light from Splunk.com.

Before you install

Do not install Splunk Light on a system that currently has Splunk Enterprise installed.

Choose the Windows user Splunk should run as

When you install Splunk Light on Windows, the software provides an opportunity to select the Windows user that it should run as. The user that Splunk Light runs as determines what Splunk Light can monitor.

- The Local System user has access to all data on the local machine by default, but nothing else.
- A user other than Local System has access to whatever data you want, but you must give the user that access before you install Splunk Light.

For more information about Windows users, see Choose the Windows user Splunk should run as in the Splunk Enterprise *Installation Manual*. The user you choose has specific ramifications on what you need to do prior to installing the software.

Splunk Light for Windows and antivirus software

Software with a device driver that intermediates between Splunk Light and the operating system can impact the performance of your Splunk Light instance. In the case of antivirus software, you can configure it to avoid on-access scanning of Splunk Light installation directories and processes before you install.

Install Splunk Light using the MSI package

1. Double-click the MSI installer file.

The installer runs and displays the **Splunk Light Installer** panel.

2. (Optional) To view the license agreement, click the **View License Agreement** button.

3. To continue the installation, select **Check this box to accept the License Agreement**.

This activates the **Customize Installation** and **Install** buttons.

4. (Optional) Click **Customize Options** to change any of the following default settings.

- The Splunk Light installation directory. By default, this directory is `\Program Files\Splunk` on the system drive (the drive that booted your Windows system.)
- The management and web ports for Splunk Light. By default, the management port is `8089` and the Web port is `8000`.
- The type of user. By default, Splunk Light runs as the Local System user.

5. Click **Install** to install Splunk Light with the defaults.

The installer runs and displays the **Installation Complete** panel.

6. (Optional) Select **Launch browser with Splunk** and **Create Start Menu Shortcut**.

7. Click **Finish**.

Start and launch Splunk Light

If you checked the box in Step 6 of the installation, Splunk Light starts and launches in a supported browser after the install finishes. This step also creates a short cut for Splunk Light in the Windows Start Menu: **Splunk Light > Splunk Light**. When you select this short cut, Splunk Light starts and launches in a supported browser, pointing to http://localhost:8000.

You can also start Splunk Light using the Windows Services Manager. To access Splunk Light after you start it from the Windows Services Manager, open a browser and navigate to http://localhost:8000, or the host name and web port you set during installation.

Log in using the default credentials: username: `admin` and password: `changeme`.

The first time you log into Splunk Light successfully, it prompts you right away to change your password. You can do so by entering a new password and clicking the **Change password** button, or you can click **Skip** and change your password later.

Install Splunk Light using Mac OS X

You can install Splunk Light on Mac OS X using the DMG package, which is the graphical installer, or the .tgz file.

You can download Splunk Light from Splunk.com.

Do not install Splunk Light on a system that currently has Splunk Enterprise installed.

Install Splunk Light using the graphical installer

1. Double-click the **DMG** file to launch the Splunk Light installer.

2. Double-click the **Install Splunk** icon on the installer launch view.

The Introduction dialog displays, which lists version and copyright information.

3. Click **Continue**.

4. Read the software license agreement and click **Continue**.

5. Click **Agree** to accept the software license agreement terms.

6. On the Installation Type dialog, select one of the following:

- For a standard installation, click **Install**.
- To change the installation location, click **Change Install Location** and select a new location to install the software. Click **Continue** and **Install**.

A separate dialog displays asking you to confirm you want to install new software.

7. Enter your operating system password and click **Install Software**.

The Summary view displays indicating the installation is complete and successful.

8. Click **Close**.

A separate dialog displays indicating Splunk needs to perform a brief initialization.

9. Click **OK**.

10. Click **Start and Show Splunk** to launch the Splunk Light user interface.

The installer places a shortcut to Splunk Light on your Desktop.

Install Splunk Light using the .tgz file

1. Move the .tgz file to the directory where you want to install Splunk Light.

For example, to install it into `/Applications`, use:

```
mv splunk_package_name.tgz /Applications
```

2. In the installation directory, use the `tar` command to expand the file.

```
tar xvzf <splunk_package_location_dir> /splunk_package_name.tgz
```

3. Start Splunk Light.

```
splunk/bin/splunk start --accept-license
```

Install Splunk Light using Linux

The topic includes instructions for installing Splunk Light on Linux using the RPM package, the DEB package, and the .tgz file.

You can download Splunk Light from Splunk.com.

Before you install

Do not install Splunk Light on a system that currently has Splunk Enterprise installed.

Create the splunk user

When you run the installation as `root` and use the RPM package or the DEB package, Splunk Light creates the `splunk` user.

Check user permissions

After you create the Splunk user, make sure that it has permissions to read and execute the installer file.

Decide where to install Splunk

The RPM and DEB packages install Splunk Light into `/opt/splunk` by default. You can specify another directory for the RPM install.

The .tgz file installs into the current working directory. If you want to install it into another directory, move the file there before you install.

Install Splunk Light using the RPM package

To follow these installation instructions, replace `splunk_package_name.rpm` with the name of the installer package you downloaded.

1. Run the `rpm` command.

Use the folllowing to install Splunk Light into the default directory.

```
rpm -i splunk_package_name.rpm
```

Use `--prefix` to select another installation directory.

```
rpm -i --prefix=/opt/new_directory splunk_package_name.rpm
```

2. Start Splunk Light.

```
splunk start --accept-license
```

3. (Optional) To boot-start Splunk Light, add the following to `/etc/init.d`.

```
./splunk start --accept-license
./splunk enable boot-start
```

Install Splunk Light using the DEB package

To follow these installation instructions, replace `splunk_package_name.deb` with the name of the installer package you downloaded.

1. Run the `dpkg` command to install Splunk Light into the default directory.

```
dpkg -i splunk_package_name.deb
```

You cannot install the DEB package into another directory.

2. Start Splunk Light.

```
splunk start --accept-license
```

Install Splunk Light using the .tgz file

To follow these installation instructions, replace `splunk_package_name.tgz` with the name of the installer package you downloaded.

1. Move the .tgz file to the directory you want to install Splunk Light.

For example, to install it into `/opt/splunk`, use:

```
mv splunk_package_name.tgz /opt/splunk
```

2. In the installation directory, use the `tar` command to expand the file.

```
tar xvzf splunk_package_name.tgz
```

3. Start Splunk Light.

```
splunk start --accept-license
```

Run Splunk Light as a non-root user

You can run Splunk Light as any user on the local system that has the appropriate permissions.

- Read the files and directories that it is configured to monitor or index. Some files and directories require root or superuser access to be indexed.

- Write to the Splunk Light directory and execute any scripts that are configured to work with your alerts of scripted inputs.
- Bind to the network ports it monitors. Network ports below 1024 are reserved ports that only the root user can bind to.

On Windows

When you run the Windows installer for Splunk Light, you can select the user to run. The user that you select determines what data Splunk Light can monitor. The Local System user can access all data on the local machine, but nothing else. To run as other existing users, you need to define their access before you install Splunk Light.

You must install as a domain user to do any of the following actions.

- Read Event Logs remotely.
- Collect performance counters remotely.
- Read network shares for log files.
- Monitor Active Directory.

On Mac OSX and Linux

Follow these steps to run Splunk Light as a non-root user called `splunkuser`.

1. As the `root` user, create the user and group `splunk`.

- On Mac OSX, use the **System Preferences > Accounts** panels to create the user `splunkuser` and group `splunk`.

- On Linux, run the following commands:

```
useradd splunkuser
groupadd splunk
```

Note: The `splunkuser` requires access to `/dev/urandom` to generate the certs for the product.

2. As the `root` user, install Splunk Light using one of the packages that is not a tar file.

Note: After the installation finishes, do not start Splunk Light.

3. Change the ownership of the `$SPLUNK_HOME` directory and its contents to the `splunk` user.

```
chown -R splunkuser:splunk $SPLUNK_HOME
```

4. As `splunkuser`, start Splunk Light. You have two options to do this.

- Log out from `root` and log in as `splunkuser`. Then, run:

```
$SPLUNK_HOME/bin/splunk start
```

- Use `sudo` or `su` to start Splunk Light as `splunkuser`

```
sudo -H -u splunkuser $SPLUNK_HOME/bin/splunk start
```

Install a Universal Forwarder

Install and deploy a universal forwarder for Splunk Light

You can use the Splunk **universal forwarder** to collect and forward data from other machines to your Splunk Light instance or Splunk Light cloud service. The universal forwarder is a separate Splunk software product that you need to install and configure before you can add a receiving data input in the Splunk Light instance.

For more information about getting data into a Splunk Light instance, see:

- Forward data to Splunk Light using Microsoft Windows in the *Getting Started Manual*.
- Forward data to Splunk Light using Linux in the *Getting Started Manual*.
- Forward data to Splunk Light using Macintosh OS X in the *Getting Started Manual*.

For information about getting data into Splunk Light cloud service, see About forwarding data to a Splunk Light cloud service in the *Splunk Light Cloud Service* manual.

Administer Splunk Light

Customize the Splunk Light login page

Learn how to customize Splunk Light login page components.

Add custom text

Customize the Splunk Light login page with plain or HTML formatted text.

Prerequisite

Review the `login_content` setting details in the web.conf spec file.

Steps

1. Check the `$SPLUNK_HOME/etc/system/local/` directory for a `web.conf` file. Use one of the following options.

File already exists in the directory	File does not exist in the directory
Locate the `[settings]` stanza in the file.	1. Create a new file called `web.conf` in the directory. 2. Add a `[settings]` stanza in the file.

2. In the local `web.conf` file, add or edit the `login_content` string under the `[settings]` stanza.

   ```
   login_content = <content_string>
   ```

   Ensure that the text and formatting are no longer than one line in the configuration file. See the custom text example.
3. Restart the Splunk instance to view the change.

Example

```
[settings]
login_content = This is a <b>production server</b>.<br>For expensive
searches try: <a href="http://server2:8080">server2</a>
```

Customize the Splunk Light background image

If you are using Splunk Light on-premises version, you can customize the login page background to display a custom image, a default image, or no image.

Splunk Light users can also configure the login page background image using the `loginCustomBackgroundImage` and `loginBackgroundImageOption` settings in `$SPLUNK_HOME/etc/system/local/web.conf`. See the web.conf spec file for more information.

This feature is not available for Splunk Light cloud service.

Prerequisites

If you are adding a custom image, make sure that the image file meets the following requirements.

- Use a `.jpg`, `.jpeg`, or `.png` formatted file.
- A landscape oriented image is recommended.
- The maximum file size is 20MB.
- The suggested minimum image size is 1024x640 pixels.

Steps

1. Log into the Splunk instance and navigate to **System** > **Server settings** > **Login background**.
2. Select one of the following options.

Background option	Description
Custom image	To use a custom background, upload the image file and click **Choose**.
Default image	Use the default background image.
No image	Do not display an image on the login page.

3. Use the **Preview** screen to preview the login page customization.
4. Click **Save**.
5. Restart the Splunk instance to view the changes.

Add a custom logo

Customize the login page logo.

Prerequisites

- The maximum image size is 485px wide and 100px high. If the image exceeds these limits, the image is automatically resized.
- Review the `loginCustomLogo` setting details in the web.conf spec file.

Steps

1. (Optional) If you are using an image file, put it into the following directory location.
   `$SPLUNK_HOME/etc/apps/<app_name>/appserver/static/logo`
2. Check the `$SPLUNK_HOME/etc/system/local/` directory for a `web.conf` file. Use one of the following options.

File already exists in the directory	File does not exist in the directory
Locate the `[settings]` stanza in the file.	1. Create a new file called `web.conf` in the directory. 2. Add a `[settings]` stanza in the file.

3. In the local `web.conf` file, add or edit the `loginCustomLogo` setting under the `[settings]` stanza. Indicate the `loginCustomLogo` file path or an image URL.
4. Restart the Splunk instance to view the change.

Use a custom favicon

Add a custom favicon to use across Splunk Web.

Prerequisites

- Review the `customFavicon` setting details in the web.conf spec file.
- Make sure that the favicon image file meets the following requirements.
  - ♦ Use only an `.ico` formatted file.
  - ♦ The image must be square. No other image shapes are supported.

Steps

1. Put the image file into the following directory location.
   `$SPLUNK_HOME/etc/apps/<app_name>/appserver/static/customfavicon`
2. Check the `$SPLUNK_HOME/etc/system/local/` directory for a `web.conf` file. Use one of the following options.

File already exists in the directory	File does not exist in the directory
Locate the `[settings]` stanza in the file.	1. Create a new file called `web.conf` in the directory. 2. Add a `[settings]` stanza in the file.

3. In the local `web.conf` file, add or edit the `customFavicon` setting under the `[settings]` stanza. Indicate the `customFavicon` file path.
4. Restart the Splunk instance to view the change.

Share Splunk Light performance data

You can opt in to automatically share certain data about your license usage and deployment performance with Splunk Inc ("Splunk"). Splunk uses this data to make decisions about future product development.

Splunk apps and add-ons

In addition to the data enumerated in this topic, certain apps or add-ons might collect additional data. Check the documentation for the apps and add-ons that you have installed on your instance.

For example, the Splunk App for AWS collects additional usage data. See Sending usage data to Splunk for the Splunk App for AWS for details.

Opt in or out of sharing usage data

You can choose to send both, either, or neither of two types of usage data:

- **License usage data** describing your active licenses and the amount of data you index.
- **Anonymized usage data** about your deployment performance and usage, including session data.

The first time you run Splunk Web on a search head as an admin or equivalent, you are presented with a modal. The options on the modal are as follows:

- Click **Skip** to suppress the modal permanently for the user who clicks **Skip**. Use this option to defer the decision to a different admin.
- Click **OK** to confirm your choice and suppress the modal permanently for all users.

Neither category of usage data is sent unless you click **OK** with one or both boxes checked. You can opt in or out at any time by navigating to **System > Instrumentation**.

If you opt out, the searches that gather the data on your system do not run, and no usage data is sent.

The ability to enable or disable instrumentation is controlled by the `edit_telemetry_settings` capability.

See Update checker data below for information about a smaller category of data controlled separately.

What usage data is collected

For license usage data and the anonymized usage data that is not session data, you can view what data has been sent in Splunk Web.

1. Navigate to **System > Instrumentation**.
2. Under the relevant data category ("Anonymized Usage Data" or "License Usage Data"), click **View Log**.
3. Select a time range, then click **View Selected Data**.

This log of data is available only after the first run of the collection (see Feature footprint).

To view the remaining anonymized usage data, the session data, use Javascript logging in your browser. Look for network events sent to a URL containing `splkmobile`. Events are triggered by actions such as navigating to a new page in Splunk Web.

See Update checker data below for information about a smaller category of data controlled separately.

The following tables describe the data collected if you opt in to both usage data programs and do not turn off update checker. The usage data is in JSON format tagged with a field named "component."

New for Splunk Light 6.6.x

The following pieces of data are collected starting with Splunk Light version 6.6.0 but not 6.5.x. For descriptions and examples, see the tables that follow.

- Start of user session:
    - Deployment ID
    - Event ID
    - Experience ID
    - Hashed user ID
    - Splunk instance GUID for the instance generating session data
- Page views
- Dashboard performance
- Pivot usage
- Performance metrics for the searches that collect usage data

Upon upgrade, you are presented with an opt-in modal advising you of additional data collection. No telemetry data is collected (including the fields collected pre-6.6.0) until you confirm your selection, either in the opt-in modal or in **System > Instrumentation**.

Types of data collected by Splunk Light

Splunk Light collects the following types of data:

- Anonymized usage data (including session data)
- License usage data
- Update checker data

Note that additional data might be collected by certain apps or add-ons. See the app or add-on documentation for details.

Anonymized usage data

Description	Component(s)	Note
Active license group and subgroup, total license stack quota, license pool quota, license pool consumption, total	`licensing.stack`	

license consumption, license stack type		
License IDs	`licensing.stack`	Sent for both reporting types, but persisted only for users opting in to license usage reporting.
Number of nodes in indexer cluster, replication factor and search factor for indexer cluster	`deployment.clustering.indexer`	
GUID, host, number of cores by type (virtual/physical), CPU architecture, memory size, storage (partition) capacity, OS/version, Splunk version	`deployment.node`	For each indexer or search head
Number of hosts, number of Splunk software instances, OS/version, CPU architecture, Splunk software version, distribution of forwarding volume	`deployment.forwarders`	For forwarders

Core utilization, storage utilization, memory usage, indexing throughput, search latency	`deployment.node`
	`performance.indexing`
	`performance.search`	

Indexing volume, number of events, number of hosts, source type name	`usage.indexing.sourcetype`	
Number of active users	`usage.users.active`	
	`usage.search.type`	

Number of searches of each type, distribution of concurrent searches	`usage.search.concurrent`	
App name, page name, locale, number of users, number of page loads	`usage.app.page`	Session data.
deploymentID = identifier for deployment, eventID = identifier for this specific event, experienceID = identifier for this session, userID = hashed username, data.guid = guid for Splunk Enterprise instance serving page	`app.session.session_start`	Session data. Triggered when user is first authenticated.
Page views	`app.session.pageview`	Session data. Triggered when user visits a new page.
Dashboard characteristics	`app.session.dashboard.pageview`	Session data. Triggered when a dashboard is loaded.
Pivot characteristics.	`app.session.pivot.load`	Session data. Triggered when a pivot is loaded.
Pivot changes	`app.session.pivot.interact`	Session data. Triggered when a change is made to a pivot.
Search page interaction.	`app.session.search.interact`	Session data. Triggered with interaction with search page.

License usage data

Description	Component(s)	Note
	`licensing.stack`	

Active license group and subgroup, total license stack quota, total license pool consumption, license stack type, license pool quota, license pool consumption		
License IDs	`licensing.stack`	Sent for both reporting types, but persisted only for users opting in to license usage reporting.

Update checker data

Update checker data is sent by your browser soon after you log into Splunk Light. The data is sent to Splunk. Splunk uses the data to understand the number of customers using older versions of software, and Splunk Light uses the data to display a message in Splunk Web when a new version is available.

To view the data that is sent, watch Javascript network traffic as you log into Splunk Web. The data is sent inside a call to quickdraw.splunk.com.

You can turn off update checker data reporting in web.conf, by setting the `updateCheckerBaseURL` attribute to 0. See About configuration files in the Splunk Enterprise *Admin Manual*.

Description	Example
CPU architecture	x86_64
Operating system	Linux
Product	light
Splunk roles	admin
License group, subgroup, and GUID	Light, Production, <GUID>
Splunk software version	6.6.0

Data samples

Anonymized usage data

Click **Expand** to view examples of the data that is collected.

Component	Data category	Example

deployment.clustering.indexer	Clustering configuration	{
		"host": "docteam-unix-5",
		"summaryReplication": true,
		"siteReplicationFactor": null,
		"enabled": true,
		"multiSite": false,
		"searchFactor": 2,
		"siteSearchFactor": null,
		"timezone": "-0700",
		"replicationFactor": 3
		}

deployment.forwarders	Forwarder architecture, forwarding volume	{
		"hosts": 168,
		"instances": 497,
		"architecture": "x86_64",
		"os": "Linux",
		"splunkVersion": "6.6.0",
		"type": "uf",
		"bytes": {
		"min": 389,
		"max": 2291497,
		"total": 189124803,
		"p10": 40960,
		"p20": 139264,
		"p30": 216064,
		"p40": 269312,
		"p50": 318157,
		"p60": 345088,
		"p70": 393216,
		"p80": 489472,
		"p90": 781312
		}
		}

deployment.node	Host architecture, utilization	{
		"guid":
		"123309CB-ABCD-4BB9-9B6A-185316600F23",
		"host": "docteam-unix-3",
		"os": "Linux",
		"osExt": "Linux",
		"osVersion": "3.10.0-123.el7.x86_64",
		"splunkVersion": "6.6.0",
		"cpu": {
		"coreCount": 2,
		"utilization": {
		"min": 0.01,
		"p10": 0.01,
		"p20": 0.01,
		"p30": 0.01,
		"p40": 0.01,
		"p50": 0.02,

		"p60": 0.02,
		"p70": 0.03,
		"p80": 0.03,
		"p90": 0.05,
		"max": 0.44
		},
		"virtualCoreCount": 2,
		"architecture": "x86_64"
		},
		"memory": {
		"utilization": {
		"min": 0.26,
		"max": 0.34,
		"p10": 0.27,
		"p20": 0.28,
		"p30": 0.28,
		"p40": 0.28,
		"p50": 0.29,
		"p60": 0.29,
		"p70": 0.29,
		"p80": 0.3,
		"p90": 0.31
		},
		"capacity": 3977003401
		},
		"disk": {
		"fileSystem": "xfs",
		"capacity": 124014034944,
		"utilization": 0.12
		}
		}

licensing.stack	Licensing quota and consumption	{
		"type": "download-trial",
		"guid":
		"4F735357-F278-4AD2-BBAB-139A85A75DBB",
		"product": "light",
		"name": "download-trial",
		"licenseIDs": [
		"553A0D4F-3B7B-4AD5-B241-89B94386A
		],
		"quota": 524288000,
		"pools": [
		{
		"quota": 524288000,
		"consumption": 304049405
		}
		],
		"consumption": 304049405,
		"subgroup": "Production",
		"host": "docteam-unix-9"
		}

performance.indexing	Indexing throughput and volume	{
		"host": "docteam-unix-5",
		"thruput": {
		"min": 412,
		"max": 9225,
		"total": 42980219,
		"p10": 413,
		"p20": 413,
		"p30": 431,
		"p40": 450,
		"p50": 474,
		"p60": 488,
		"p70": 488,
		"p80": 488,
		"p90": 518
		}
		}

performance.search	Search runtime statistics	{
		"latency": {
		"min": 0.01,
		"max": 1.33,
		"p10": 0.02,
		"p20": 0.02,
		"p30": 0.05,
		"p40": 0.16,
		"p50": 0.17,
		"p60": 0.2,
		"p70": 0.26,
		"p80": 0.34,
		"p90": 0.8
		}
		}

app.session.dashboard.pageview		
app.session.pivot.interact		
app.session.pivot.load		
app.session.search.interact		

app.session.pageview		{
		"component": "app.session.pageview",
		"timestamp": 1490252394,
		"visibility": "anonymous",
		"experienceID":
		"0afeff4c-da15-58ba-e826-c3e89009074d",
		"userID":
		"bba2504e427e0eebcee94192aeeb124eb9ae83fc"
		"version": "2",
		"eventID":
		"c918b567-6dbf-c68f-f3bd-39650fcb0e69",
		"data": {

		"app": "launcher", "page": "home" }, "deploymentID": "SPLUNKQA-7efb1644-e209-4afb-90ea-d7cddf77 }

app.session.session_start		{
		"component": "app.session.session_star
		"timestamp": 1490252394,
		"visibility": "anonymous",
		"experienceID":
		"0efeff4c-da15-50ba-e826-c3e89109074d",
		"userID":
		"bba2504e427e0eebcee94192aweb124eb9ae83fc"
		"version": "2",
		"eventID":
		"cd5634e1-19c3-e088-53v5-7ee328608a4c",
		"data": {
		"app": "launcher",
		"splunkVersion": "6.6.0",
		"os": "Ubuntu",
		"browser": "Firefox",
		"browserVersion": "38.0",
		"locale": "en-US",
		"device": "Linux x86_64",
		"osVersion": "not available",
		"page": "home",
		"guid":
		"2550FC44-64E5-43P5-AS44-6ABD84C91E42"
		},
		"deploymentID":
		"SPLUNKQA-7efb1644-q209-4afb-90ea-d7cddf07
		}

usage.app.page	App page users and views	{
		"app": "search",
		"locale": "en-US",
		"occurrences": 1,
		"page": "datasets",
		"users": 1
		}

usage.indexing.sourcetype	Indexing by source type	{
		"name": "vendor_sales",
		"bytes": 2026348,
		"events": 30245,
		"hosts:" 1
		}

usage.search.concurrent	Search concurrency	{
		"host": "docteam-unix-5"
		"searches": {

		"min": 1, "max": 11, "p10": 1, "p20": 1, "p30": 1, "p40": 1, "p50": 1, "p60": 1, "p70": 1, "p80": 2, "p90": 3 } }

`usage.search.type`	Searches by type	{
		"ad-hoc": 1428,
		"scheduled": 225
		}

`usage.users.active`	Active users	{
		"active": 23
		}

License usage data

Click **Expand** to view examples of the data that is collected.

Component	Data category	Example

`licensing.stack`	Licensing quota and consumption	{
		"type": "download-trial",
		"guid":
		"4F735357-F278-4AD2-BBAB-139A85A75DBB",
		"product": "light",
		"name": "download-trial",
		"licenseIDs": [
		"553A0D4F-3B7B-4AD5-B241-89B94386A07F"
		],
		"quota": 524288000,
		"pools": [
		{
		"quota": 524288000,
		"consumption": 304049405
		}
		],
		"consumption": 304049405,
		"subgroup": "Production",
		"host": "docteam-unix-9"
		}

Update checker data

Click **Expand** to view examples of the data that is collected.

Data category	Example
CPU architecture	x86_64
Operating system	Linux
Product	light
Splunk roles	admin
License group, subgroup, and GUID	Light, Production, <GUID>
Splunk software version	6.6.0

What data is not collected

The following kinds of data are not collected:

- Unhashed usernames or passwords.
- Indexed data that you ingest into your Splunk platform instance.

How usage data is handled

When you enable instrumentation, usage data is transported directly to Splunk through its MINT infrastructure. Data received is securely stored within on-premises servers at Splunk with restricted access.

Anonymized usage data is aggregated, and is used by Splunk to analyze usage patterns so that Splunk can improve its products and benefit customers. License IDs collected are used only to verify that data is received from a valid Splunk product and persisted only for users opting into license usage reporting. These license IDs help Splunk analyze how different Splunk products are being deployed across the population of users and are not attached to any anonymized usage data.

See the Splunk Privacy Policy for more information.

Why send license usage data

Certain license programs require that you report your license usage. The easiest way to do this is to opt in to automatically send this information to Splunk.

If you do not opt in to automatic license data sharing, you can send this data manually. On a search head, log into Splunk Web. Select **System > Instrumentation** and follow the instructions for exporting the data to your local directory.

Feature footprint

Anonymized usage and license usage data is summarized and sent once per day, starting at 3:05 a.m.

Session data and update checker data is sent from your browser as the events are generated. The performance implications are negligible.

About searches

If you opt in to anonymized usage and license usage data reporting, your Splunk Light deployment collects data through ad hoc searches. All searches run in sequence, starting at 3:05 a.m.. All searches are triggered with a scripted input. See Configure the priority of scheduled reports in the Splunk Enterprise *Reporting Manual*.

About internal log files

If you enable license usage reporting, the first time product instrumentation runs, it creates a new file in `$SPLUNK_HOME/var/log/splunk`. The file is called `license_usage_summary.log` and is limited in size to 25 MB. The file is indexed to a new internal index, `_telemetry`. The `_telemetry` index is retained for two years by default and is limited in size to 256 MB.

After the searches run, the data is packaged and sent to Splunk, Inc.

The app resides in the file system at `$SPLUNK_HOME/etc/apps/splunk_instrumentation`.

License Splunk Light

About Splunk Light licensing

Splunk Light licenses control the indexing volume and feature set of the Splunk Light product.

Splunk Light license types

The following table lists the different license types available for Splunk Light.

License Type	Description
Splunk Light Trial	Included with the download package. Offers a daily indexing volume capacity up to 5GB and up to 5 administrator or user accounts. Access to all features for 30 days. When the trial expires, you are advised of your license usage to date and a license size is recommended based upon your usage. You can buy a paid license or use the free term-based license.
Splunk Light Free	Offers a daily indexing volume capacity up to 500MB and has one admin account. Access to all features, with the exception of alerting. This license is term-based and valid for one year, with renewals beyond one year available by contacting Splunk.
Splunk Light Perpetual	Offers a daily indexing volume capacity up to 20GB and up to 5 administrator or user accounts.
Splunk Light Term	Offers a daily indexing volume capacity up to 20GB and up to 5 administrator or user accounts. You can renew this license at the end of its subscription term.

Splunk Light features by license type

The following table lists the Splunk Light features enabled by the license type.

Features	Splunk Light Trial	Splunk Light Free	Splunk Light
Daily Indexing Volume	Up to 5GB	Up to 500MB	Up to 20GB
Search and Reporting	Yes	Yes	Yes

Dashboards	Yes	Yes	Yes
Alerting	Yes	No	Yes
Accounts	Up to 5, Admin and User	1 Admin	Up to 5, Admin and User
Add-ons	Yes	Yes	Yes

Exceeding your license

Warnings and violations occur when you exceed the maximum daily indexing volume allowed for your license.

Warnings when you exceed your volume

If you exceed your daily indexing volume on any calendar day, you get a warning. The message persists for fourteen days. You have until midnight to resolve it before it counts against the total number of warnings within the rolling 30-day period.

License violations after five warnings

If you have five or more warnings in a rolling 30-day period, you are in violation of your license. During a license violation period, the following actions occur.

- Splunk Light continues to index your data.
- Search is disabled, except for searches to the `_internal` index.

Although you cannot search existing or incoming data inputs, you can use search to troubleshoot the licensing issue.

Search capabilities return when you have fewer than five warnings in the previous 30 days or when you apply a reset license.

License expiration

When your Splunk Light license is nearing expiration, a message appears in your Splunk Light instance before the expiration date. You have options to renew, upgrade, or revert your license, as defined in this section.

Splunk Light Term license expiration

If your Splunk Light term license expires, you have the following options.

- Purchase and install a new Splunk Light paid license (perpetual or term).
- Purchase and install a Splunk Enterprise license to upgrade to Splunk Enterprise.
    - When you upgrade to Splunk Enterprise, your data, searches, alerts, knowledge objects, and settings migrate seamlessly. **If you have add-ons enabled, they remain active and appear in the Apps browser view of Splunk Enterprise.
- Revert to the Splunk Light Free license.
    - When you revert your instance to Splunk Light Free, your instance is limited to a single account with administrator privileges. Previous settings such as accounts, passwords, and configurations persist, but you cannot modify them in Splunk Light Free. See Logging in after you revert to Splunk Light Free in the Splunk Light *Installation Manual*.
    - If you upgrade this instance to Splunk Light (or upgrade to Splunk Enterprise), your previous configurations are restored.

Log in after you revert to Splunk Light Free

If you have more than one admin account configured on the Splunk Light instance, after you revert to Splunk Light Free the login account becomes the admin account that is first in alphabetical order. You can change this setting.

1. Stop Splunk Light Free.
2. Back up the original `<SPLUNK_HOME>/etc/passwd` file.
3. Edit `<SPLUNK_HOME>/etc/passwd file` to remove all entries except one Admin user.
4. Start Splunk Light Free.
5. Log in using the Admin account you saved.

   When you upgrade back to Splunk Light or Splunk Enterprise, restore the `passwd` file from the original backup.

Splunk Light Trial license expiration

Your Splunk Light Trial license has a 30-day term. When your Splunk Light Trial expires, you have the following options.

- Purchase and install a new Splunk Light paid license (perpetual or term).
- Purchase and install a Splunk Enterprise license to upgrade to Splunk Enterprise.
- Convert your Splunk Light Trial license to a Splunk Light Free license. If you convert to a Splunk Light free license, you might lose much of the

capacity available with your Splunk Light trial license. To retain your capacity, upgrade to a Splunk Light perpetual or term license.

Splunk Light Free license expiration

Your Splunk Light Free license has a one-year term. When your Splunk Light Free license expires, you have the following options.

- Purchase and install a new Splunk Light paid license (perpetual or term.)
- Purchase and install a Splunk Enterprise license to upgrade to Splunk Enterprise.
- Request another Splunk Light Free license by contacting Splunk.

For more information, see About upgrading and migrating Splunk Light and Update your Splunk Light license in the *Installation Manual*.

Update your Splunk Light license

Update your Splunk Light license or add a new license to:

- Convert from a trial or free license to a paid license.
- Convert from a trial to a free license.
- Expand the indexing capacity of an existing license.
- Extend the term of an existing license, including a paid or free license.
- Reset an existing license.

Add a license

1. Open the sidebar menu and select **System** > **Licensing**.

The following screenshot shows the Licensing page for an instance running Splunk Light Trial.

2. Click **Add License**.

3. Add your license.

There are a few options for adding a license:

- Drop a new license file into the **Drop your license file here** box.
- Click **Select a file** to select your new license file to upload.
- Click **copy & paste the license XML directly...** to drop an XML text file into the dialog.
- If you do not have a license and want to purchase a Splunk Light license or renew your Splunk Light Free license, click **Get a new license** and you are redirected to the Splunk e-store.

4. Click **Add** or **Upgrade**, depending on the license you are adding.

5. Click **Restart Now,** as you must restart your Splunk Light instance to activate your new license.

6. After the restart is successful, click **OK** to log back into Splunk Light.

7. Log into Splunk Light to start using your new licensed version.

To see your new license information, use the sidebar menu and navigate to **System > Licensing** and your new license information is displayed.

Upgrade and Migrate Splunk Light

About upgrading and migrating Splunk Light

Splunk Light supports several upgrade and migration options, including upgrading or migrating to Splunk Enterprise 6.2.x and later.

Supported upgrade and migration paths

You can choose from several paths to upgrade, downgrade, and migrate between the products as described in the table. For a product comparison, see Splunk Light versus Splunk Enterprise Comparison.

If you are upgrading or migrating to Splunk Light cloud service or Splunk Cloud, contact Splunk sales.

Type	Path	Description
Product Upgrade	Splunk Light to Splunk Enterprise	Occurs when you convert Splunk Light (Perpetual, Term, Trial, or Free) to Splunk Enterprise. See Upgrade from Splunk Light to Splunk Enterprise.
Upgrade	Splunk Light to a new version of Splunk Light	Occurs when you upgrade to a new version of Splunk Light. See Upgrade Splunk Light to a new version of Splunk Light.
Upgrade	Splunk Light Trial to Splunk Light	Occurs when you convert from the trial version to either a perpetual or term license version. See Upgrade Splunk Light to a new version of Splunk Light.
Upgrade	Splunk Light Free to Splunk Light	Occurs when you convert from the free version to either a perpetual or term license version. See Upgrade Splunk Light to a new version of Splunk Light.

Downgrade	Splunk Light to Splunk Light Free	Occurs when your term license expires and the product reverts to the free version. See Downgrade Splunk Light to Splunk Light Free.
Downgrade	Splunk Light Trial to Splunk Light Free	Occurs when your trial license expires and the product reverts to the free version. See Downgrade Splunk Light to Splunk Light Free.
Downgrade-Upgrade	Splunk Light to Splunk Light Free to Splunk Light	Occurs when your term license expires, and then you renew with either a perpetual or term license version.

Before you upgrade Splunk Light

Read this topic before you upgrade to learn important information and tips about the Splunk Light upgrade process.

Review Release Notes and Known Issues

For the version of Splunk Light you are upgrading to, review the associated release notes and known issues.

Back up your existing deployment

Always back up your existing Splunk Light deployment before you perform any upgrade or migration.

You can manage upgrade risk by using technology that lets you restore your Splunk Light installation and data to a state prior to the upgrade, whether that is external backups, disk or file system snapshots, or other means. When backing up your Splunk Light data, consider the $SPLUNK_HOME directory and any indexes outside of it.

For more information about backing up your Splunk Light deployment, see the Back up configuration information in the Splunk Enterprise *Admin Manual* and Back up indexed data in the Splunk Enterprise *Managing Indexers and Clusters Manual*.

Upgrade universal forwarders

Upgrading universal forwarders is a different process than upgrading Splunk Light. Before upgrading your universal forwarders, see the appropriate upgrade topic for your operating system:

- Upgrade the Windows universal forwarder
- Upgrade the universal forwarder for *nix systems

To learn about interoperability and compatibility between indexers and forwarders, see Indexer and universal forwarder compatibility in the Splunk Enterprise *Forwarding Data Manual*.

Important upgrade information and changes

Here are some things that you should be aware of when installing the new version:

The instrumentation feature adds a new internal index and can increase disk space usage

The instrumentation feature of Splunk Light, which lets you share Splunk Light performance statistics with Splunk after you opt in, includes a new internal index which can cause disk space usage to rise on hosts that you upgrade. You can opt out of sharing performance data by following the instructions at Share Splunk Light peformance data in the Splunk Light *Installation Manual*.

For Linux, confirm that the introspection directory has the correct permissions

If you run Splunk Light on Linux as a non-root user, and use an RPM to upgrade, the RPM writes the `$SPLUNK_HOME/var/log/introspection` directory as root. This can cause errors when you attempt to start the instance later. To prevent this, `chown` the `$SPLUNK_HOME/var/log/introspection` directory to the user that Splunk Light runs as after upgrading and before restarting Splunk Light or Splunk Enterprise.

For Linux, Splunk Enterprise support for running multiple searches on a single process could increase memory usage

As of version 6.5, Splunk Enterprise can launch multiple searches on a single process on *nix hosts.

When you upgrade, you should see improved search performance, but you might also see increased memory usage.

This change is not applicable on Windows instances of Splunk Enterprise.

Splunk Enterprise now identifies search commands that could negatively impact performance

In an effort to improve security and performance, some Search Processing Language (SPL) commands have been tagged with a variable that prompts Splunk Enterprise to warn you about performance impact when you use them in a search query. After an upgrade, you might see a warning message that a search that you run has commands that might have risky side effects.

Support for Internet Explorer versions 9 and 10 has been removed

Microsoft has announced that support for all versions of Internet Explorer below version 11 has ended as of January 12, 2016. Owing to that announcement, Splunk has ended support for Splunk Web for these same versions. This might result in a suboptimal browsing experience in Internet

When you upgrade, you should also upgrade the version of Internet Explorer that you use to 11 or later. An alternative is to use another browser that Splunk supports.

New installation and upgrade procedures

The Windows version of Splunk Light and Splunk Enterprise has a more streamlined installation and upgrade workflow. The installer now assumes specific defaults (for new installations) and retains existing settings (for upgrades) by default. To make any changes from the default on installations, you must check the "Customize options" button. During upgrades, your only option is to accept the license agreement.

This feature was introduced in Splunk Enterprise 6.2, but we retain it here for those who upgrade to 6.5 from earlier versions.

Changes have been made to support more granular authorization for Windows inputs

Splunk Enterprise has been updated to allow for more control when using Windows inputs like Network Monitoring and Host Monitoring. If you use Splunk Enterprise as a user with a role that does not inherit from other roles, it is possible that the user might not be able to access certain Windows inputs.

This change was introduced in Splunk Enterprise 6.4, but we retain it here for those who upgrade to 6.5 from earlier versions.

No support for enabling Federal Information Processing Standards (FIPS) after an upgrade

There is no supported upgrade path from a Splunk Enterprise system with enabled Secure Sockets Layer (SSL) certificates to a system with FIPS enabled. If you need to enable FIPS, you must do so on a new installation.

The default behavior for translating security identifiers (SID) and globally unique identifiers (GUIDs) when monitoring Windows Event Log data has changed

The `etc_resolve_ad_obj` attribute, which controls whether or not Splunk Enterprise attempts to resolve SIDs and GUIDs when it monitors event log channels, is now disabled by default for all channels. When you upgrade, any `inputs.conf` monitor stanzas that do not explicitly define this attribute will no longer perform this translation.

This change was introduced in Splunk Enterprise 6.2, but we retain it here for those who upgrade to 6.5 from earlier versions.

Upgrade or downgrade Splunk Light

This topic describes upgrading or downgrading Splunk Light. Paths include:

- Upgrade Splunk Light to Spunk Enterprise.
- Upgrade Splunk Light to a new version of Splunk Light.
- Downgrade Splunk Light to Splunk Light Free.

If you are upgrading or migrating to Splunk Light cloud service or Splunk Cloud, contact Splunk sales.

Upgrade Splunk Light to Splunk Enterprise

Upgrade Splunk Light (licensed, trial, or free) to a licensed version of Splunk Enterprise. Before you upgrade, note:

- Downgrading from Splunk Enterprise to Splunk Light is not supported.
- When you upgrade from Splunk Light to Splunk Enterprise, add-ons that you enabled continue to be active. You can access them from the Apps view in Splunk Enterprise.
- By default, Splunk Light Home is the Search summary view. When you upgrade to Splunk Enterprise, clicking on the Splunk logo in the navigation bar opens the Search summary view, instead of Splunk Enterprise Home. To change the default app to Home, select **launcher** in the Splunk Enterprise **Access controls** settings page for the role or individual user.

Obtain a new Splunk Enterprise license

1. In your Splunk Light instance, go to **System > Licensing**
2. Click **e-Store.**
3. Click **Buy** in the page header to review your license options to purchase Splunk Enterprise.
4. Click **Contact Us** (sales@splunk.com) to purchase and obtain a new license key, which is typically a .lic file.

Upgrade to Splunk Enterprise

1. In your Splunk Light instance, go to **System > Licensing**.
2. Click **Add License**.
3. Add your new license key file. You can drop your license file into the dialog, select a file, or copy and paste the license XML.
4. After your license successfully validates, click **Upgrade to Enterprise**.
5. Click **Restart Now**, as a restart is required to upgrade to Splunk Enterprise.
6. Click **OK** when restart is successful.
7. Log back into Splunk Enterprise.

Upgrade Splunk Light to a new version of Splunk Light

When you upgrade to a new version of Splunk Light (licensed, trial, or free), you install the new Splunk Light package directly over your existing deployment of Splunk Light. You can upgrade using Splunk Web or the command line.

Upgrade to new version of Splunk Light using Splunk Web

1. Before you upgrade, back up all of your files.
2. Confirm you are logged out of your current instance of Splunk Light.
3. Confirm that no other processes can automatically start Splunk Light.
4. Obtain a new version of a Splunk Light installation package.

5. Launch and install the new Splunk Light installation package, following the installation wizard prompts. See the Splunk Light *Installation Manual* for more information about installing on your operating system.
6. At the end of the installation wizard, a message displays stating "Welcome! You have upgraded Splunk. If your configuration files are out of date, they will be automatically updated. Is this okay?" Click **Yes, go ahead.** Splunk Light installs directly over your existing deployment.
7. Splunk Light starts and overrides the previous version.

Upgrade to new version of Splunk Light using the command line

1. Before you upgrade, back up all of your files.
2. Open a shell prompt on the host that has the instance that you want to upgrade.
3. Change to the $SPLUNK_HOME/bin directory.
4. Run the $SPLUNK_HOME/bin/splunk stop command to stop the instance.
5. Confirm that no other processes can automatically start Splunk Light.
6. To upgrade and migrate, install the Splunk Light package directly over your existing deployment.
7. Run the $SPLUNK_HOME/bin/splunk start command.
8. After you review the changes and are ready to proceed with migration and upgrade, run $SPLUNK_HOME/bin/splunk start again.

Downgrade Splunk Light to Splunk Light Free

When you downgrade from Splunk Light (licensed or trial) to Splunk Light Free, your instance limits to the Splunk Light Free features and capabilities. If you had multiple accounts on this instance, the Splunk Light Free license restricts your access to a single administrator account. Your previous account settings, passwords, and configurations persist, but you cannot modify them in Splunk Light Free. If you upgrade this instance back to Splunk Light (or upgrade to Splunk Enterprise), your previous configurations restore.

Note: If you have a Splunk Light trial instance, and it is nearing expiration, you receive notifications that your instance is about to expire. You need to convert from Splunk Light Trial to Splunk Light Free before expiration, otherwise you will be unable to access your instance. If your license is expired, you receive a notice indicating your license is expired, and you can either get a license, add a license, or change to Splunk Light Free. If your license is expired and you continue to ingest data, you might be locked out of your account due to license violations. See License violations after five warnings and License expiration.

Meet the Splunk Light AMI

About the Splunk Insights for AWS Cloud Monitoring AMI

Splunk Insights for AWS Cloud Monitoring is available as an Amazon Machine Image on the Amazon Web Services Marketplace for Splunk products.

The Splunk Insights for AWS Cloud Monitoring AMI is available on Splunk Light. Contact Splunk sales for license information and pricing. To upgrade your Splunk Light license, see About upgrading and migrating Splunk Light in the *Installation Manual*.

Get the Splunk Insights for AWS Cloud Monitoring AMI

You can find the Splunk Insights for AWS Cloud Monitoring AMI on the **AWS Marketplace.**

1. Go to the AWS Marketplace for Splunk Insights for AWS Cloud Monitoring.

2. From the Splunk Insights for AWS Cloud Monitoring page, click **Continue**.

Note: Sign in or create an AWS account to continue.

3. On the **Launch on EC2** page, choose an EC2 instance type. Make sure you select an instance type large enough to handle what you want Splunk Insights for AWS Cloud Monitoring to do for you. The default is C3.L.

4. Click **1-Click Launch**

5. In your security group, note the ports that are open.

- TCP (554)
- UDP, 8089 (management)
- 8000 (splunkweb)
- 9997 (fwder)
- 22 (SSH)
- 443 (SSL/https)

Start using the Splunk Insights for AWS Cloud Monitoring AMI

If you already started a copy of the Splunk Insights for AWS Cloud Monitoring AMI on the AWS Marketplace, then you have an instance of Splunk Light running as the Splunk user. It will start when the virtual machine starts.

Find Splunk Web

1. In your EC2 Management Console, find your instance running Splunk Light. Note the Splunk Light **instance ID** and **public IP**.

2. Copy and paste the **public IP** into a new browser tab. Do not hit enter yet.

3. Append **:8000** to the end of the IP address and hit enter.

4. Log into Splunk Light with the credentials:

- username: admin
- password: <instance id from management console>

5. On the next screen, set a new password.

Upgrade

Upgrade Splunk Light version

See How to upgrade Splunk Light in the Splunk Light *Installation Manual*. Be sure to run a backup before you begin the upgrade.

Upgrade your AWS storage capacity

See the AWS documentation about Amazon EBS.

Upgrade your AWS compute capacity

See the AWS documentation about Amazon EC2.

Get help

To file a Splunk Support ticket (as Community Support), sign up on splunk.com. Other community resources for help include Answers, IRC #splunk on efnet, and the Splunk Enterprise documentation.

Get started with Splunk App for AWS

Get started with Splunk App for AWS

The Splunk App for AWS provides end-to-end security, operational and cost management insights for your AWS environment, including:

- A pre-built knowledge base of dashboards, reports, and alerts that deliver real-time visibility into your environment.
- Easy-to-configure data inputs for your AWS Config, Config Rules, CloudWatch, CloudTrail, Billing, S3, VPC Flow Log, Inspector, and Metadata inputs.
- A logical topology dashboard that displays your entire AWS infrastructure.

Follow the steps below to configure an AWS account with the Splunk App for AWS, and see the image which displays the workflow.

Step 1: Planning and prerequisites

Review the following before starting the installation and configuration of your AWS account and the Splunk App for AWS.

AWS planning and prerequisites
Admin role permissions are required.
More than one AWS account can be installed.
Know your AWS Account Access Key ID and AWS Account Secret Access Key.
Consider your Amazon Machine Image (AMI) disk space availability and retention. • For best performance, consider adding Amazon Elastic Block Store (Amazon EBS) which provides network-attached storage (NAS) for use with your EC2 instances. • After you create, attach, and mount an Amazon EBS volume to your instance, you can use it just as you would use a physical hard drive on your computer. Each volume can be attached to only one EC2 instance, but you can detach an Amazon EBS volume from one EC2 instance and attach it to another. • You can attach multiple Amazon EBS volumes to an EC2 instance, and you can also stripe your data across multiple volumes. • You can back up the data on your Amazon EBS volumes by creating snapshots, which are stored in Amazon S3. You can create a new Amazon EBS volume from a snapshot and then attach it to an EC2 instance. • For more information about Amazon EBS Volumes, see http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/EBSVolumes.html.
For the AWS General Reference, see http://docs.aws.amazon.com/general/latest/gr/Welcome.html.
Splunk Insights for AWS Cloud Monitoring
The Splunk Insights for AWS Cloud Monitoring is available as an Amazon Machine Image on the AWS Web Service Marketplace for Splunk products. • The Splunk Insights for AWS Cloud Monitoring is available for Splunk Light, in which the Splunk App for AWS and the Splunk Add-on for Amazon Web Services are pre-installed and do not need to be configured. Version requirements are listed below.
Splunk Light 6.6.2 and later. Versions include: • Splunk Insights for AWS Cloud Monitoring AMI, obtained through the Amazon Web Services Marketplace for Splunk products. The Splunk Insights for AWS Cloud Monitoring AMI is a Splunk Light instance with pre-installed Splunk App for AWS and Splunk Add-on for Amazon Web

Services. • Splunk Light on-premises and cloud versions, available from Splunk.com. Access the Splunk App for AWS and Splunk Add-on for Amazon Web Services through the Apps and Add-on page in Splunk Light.
Splunk App for AWS 5.0 and later, installed • For Splunk Insights for AWS Cloud Monitoring AMI version, a Splunk Light instance with the pre-installed Splunk App for AWS. • For Splunk Light on-premises and cloud versions, the Splunk App for AWS is available from the Apps and Add-on page in Splunk Light.
Splunk Add-on for Amazon Web Services 4.1.2 and later, installed (required for Splunk App for AWS functionality). • For Splunk Insights for AWS Cloud Monitoring AMI version, a Splunk Light instance with the pre-installed Splunk Add-on for Amazon Web Services. • For Splunk Light on-premises and cloud versions, the Splunk Add-on for Amazon Web Services is available from the Apps and Add-on page in Splunk Light.

Step 2: In your AWS account, configure services and permissions

In your AWS account, configure services and permissions to allow the Splunk App for AWS to access your AWS data.

1. Configure AWS services.

   a. In order for the Splunk App for AWS to collect data from your AWS account, you must first enable or configure the services that produce the data (AWS Config, CloudTrail, and so on). Splunk recommends that you enable all AWS services, otherwise some of the dashboards in the Splunk App for AWS will not fully populate.
   b. For more for information about how to configure AWS services, see Configure your AWS services for the Splunk App for AWS

2. Configure AWS permissions and policies.

   a. In order for the Splunk App for AWS to access the data in your AWS account, you must assign one or more AWS accounts to an IAM role with the permissions required by those services. You can use the AWS Policy Generator tool to collect all permissions into

one centrally managed policy, which you can then apply to the IAM group used by the account(s) that the Splunk App for AWS uses to connect to your AWS environment.
b. For an example policy that contains all permissions for all inputs, and for more information about configuring permissions for AWS services, see Configure your AWS permissions for the Splunk App for AWS.

Step 3: In Splunk Light, install the App and Add-on

Skip this step if you have a Splunk Insights for AWS Cloud Monitoring AMI instance, as the Splunk App for AWS is the default application in Splunk Light. The Splunk App for AWS and the Splunk Add-on for Amazon Web Services are pre-installed.

If you have a Splunk Light on-premises or cloud instance, install the following.

1. Install the Splunk Add-on for Amazon Web Services.

a. In Splunk Light, go to the sidebar menu and select **Data > Add-ons.**
b. Find the Splunk Add-on for Amazon Web Services and click **Install**.
c. Enter your Splunk **username** and **password**.
d. Select that you have read the terms and conditions of the license agreement.
e. Click **Login and install.**
f. Restart Splunk.

2. Install the Splunk App for AWS.

a. In Splunk Light, go to the sidebar menu and select **Data > Add-ons.**
b. Find the Splunk App for AWS and click **Install**.
c. Enter your Splunk **username** and **password**.
d. Select that you have read the terms and conditions of the license agreement.
e. Click **Login and install.**
f. Restart Splunk.

Step 4: In Splunk Light, add your AWS account and configure data sources

In your Splunk Light instance, add at least one AWS account to use for data collection, and configure your data sources (inputs) to get your AWS data into Splunk Light. You will need your AWS Account Access Key ID and AWS Secret Access Key. Splunk suggests you configure all the data sources listed to populate all dashboards. Each data source has instructions in the user dialog about how to add and configure the input.

1. Add your AWS account to your Splunk Light instance.

> **a.** In Splunk Light, go to the App for AWS page and click **Configure**.
> **b.** Under Accounts, click **Add AWS Account.**
> **c.** Enter a **friendly name**.
> **d.** Add your **AWS Account Access Key ID**.
> **e.** Add your **AWS Secret Access Key**.
> **f.** Click **Add**.

2. Configure data sources.

> **a.** Click **Set up** for the data source.
> **b.** Follow the instructions at the top of the dialog to configure the input.
> See the Learn more link within the dialog, or Inputs overview for the Splunk App for AWS for information about specific data sources.

Step 5: Work with dashboards, alerts, and reports

See the following for information about the tools available in the Splunk App for AWS to analyze your AWS data.

- To access and analyze your data, see the dashboards, alerts, and reports provided by the Splunk App for AWS, see Get your data for the Splunk App for AWS.
- For detailed information about using dashboards for your AWS data, see the Splunk App for AWS Dashboard Reference.