



Sensor Linux Install

CB v4.2.5.150311.1434

March 11, 2015

Contents

Overview	1
Installation	1
Upgrade	3
Known Issues	4

Overview

This document outlines the steps to install/upgrade the Carbon Black Linux sensor.

Installation

Prerequisites

1. A Carbon Black enterprise server installation \geq 4.2.2
2. Openssl version 1.0.1 or higher

The Carbon Black Linux sensor installation is currently a manual process and consists of two primary steps, 1) Installing the sensor files on the Carbon Black server for distribution to endpoints and 2) installing the sensor package on the endpoints.

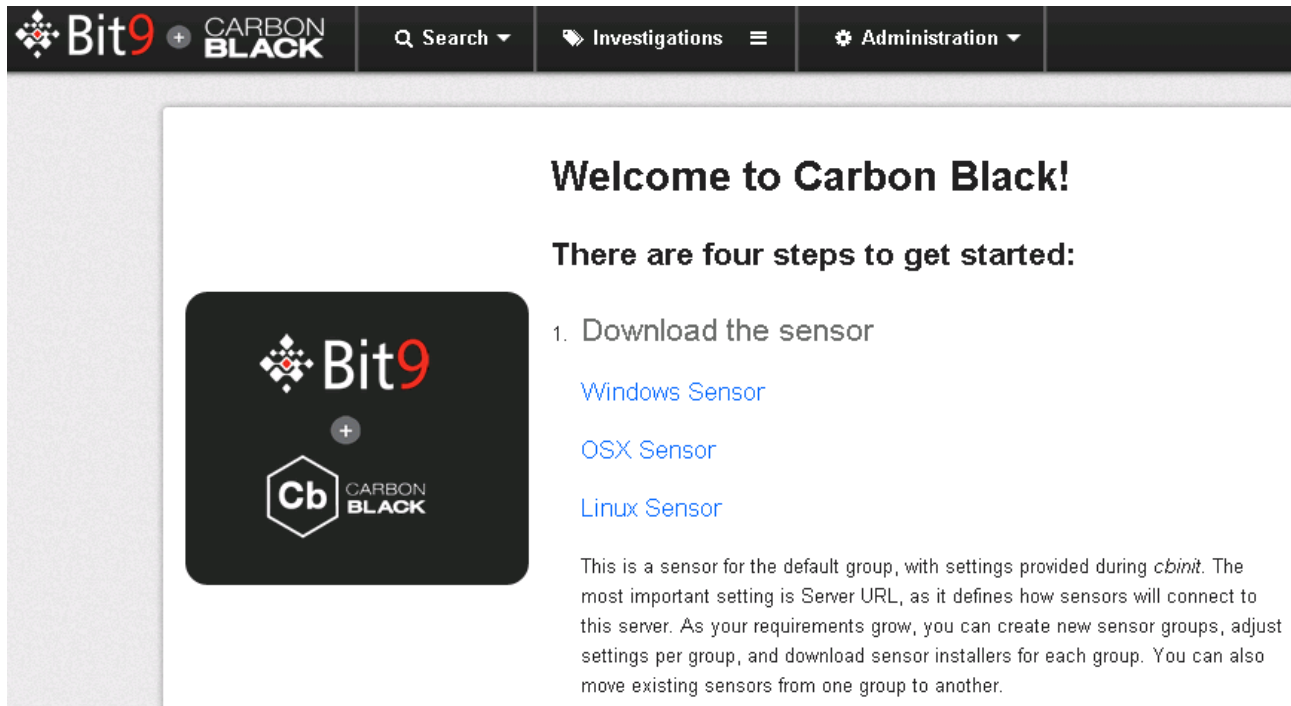
Note With Carbon Black enterprise server installation \geq 4.2.2 and the Linux sensor rpm installed on the Carbon Black Server, those users with Web UI access can download the Default Sensor group Linux sensor installer package from the main Carbon Black splash page or from the sensor group “Download Sensor Installer” dropdown for those groups that user has read permissions to. If the installer package is downloaded via the Web page links then creation of the Linux sensor installation package outlined below can be skipped.

Installing the Sensor files on the Carbon Black server With version 4.2.2 Carbon Black repo and higher, the Linux sensor is available for download and installation on the Carbon Black server via the YUM packaging system. Download and install the Linux sensor files to the server by following these steps:

1. Verify the repo configured on the server has access to the Linux sensor rpm by running: `yum info cb-linux-sensor`
2. Stop the Carbon Black Services by issuing this command: `service cb-enterprise stop`
3. Install the Linux sensor package on your Carbon Black server: `yum install cb-linux-sensor` and answer Y to the confirmation
4. Start the Carbon Black Services by issuing this command: `service cb-enterprise start`

Download the Sensor package from the Carbon Black GUI or manually create it Please follow the steps in “Installing the Sensor files on the Carbon Black server” before performing any of these steps.

1. Download the Linux sensor package for the Default Sensor group by clicking on the “Linux Sensor” link on the main splash page after logging into the Carbon Black server.



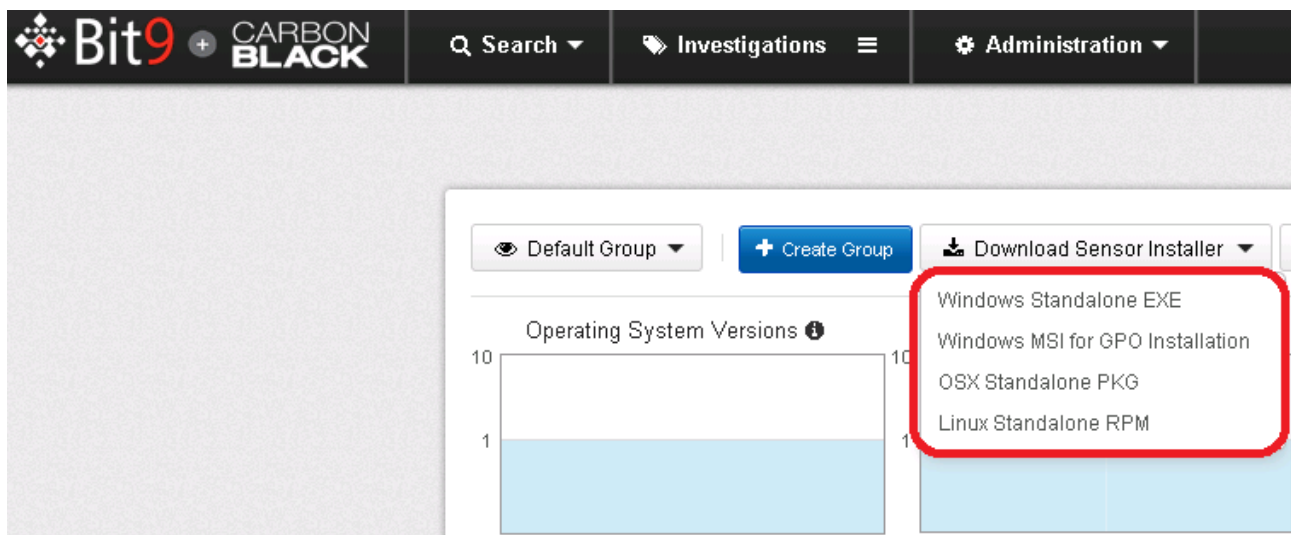
Welcome to Carbon Black!

There are four steps to get started:

1. Download the sensor
 - [Windows Sensor](#)
 - [OSX Sensor](#)
 - [Linux Sensor](#)

This is a sensor for the default group, with settings provided during *cbinit*. The most important setting is Server URL, as it defines how sensors will connect to this server. As your requirements grow, you can create new sensor groups, adjust settings per group, and download sensor installers for each group. You can also move existing sensors from one group to another.

Or When logged as a user with read permissions for a specific sensor group, the user can navigate to the Sensor Group page (Administration / Sensor link), select the “Download Sensor Installer” button and select “Linux Standalone RPM”. The browser will inform you of the Sensor package file download, save the package to disk.



Operating System Versions

Download Sensor Installer

- Windows Standalone EXE
- Windows MSI for GPO Installation
- OSX Standalone PKG
- Linux Standalone RPM

2. Or manually create the Linux sensor installation package.

The installation package is created on the Carbon Black enterprise server. A script is used to package the installer files with the server settings.

Install the Carbon Black Linux sensor files on the server using the steps “Installing the Sensor files on the Carbon Black server” above and then execute the following command:

```
/usr/share/cb/cbsensorinstallergen --installer-file=[path to Linux .rpm file],[path to Linux .sh file] --os=linux --package-path=[dir path to save the output package]
```

The `--sensor-group` option can also be used to target the installer to a specific sensor group. This is defaulted to "Default Group". The `--help` option displays command line help for the script.

The output file is a gzipped tarfile that contains the installer, an installer script (.sh) and the `sensorsettings.ini` that are required for installation. A `readme.txt` is also included that includes the CB server and sensor group name that a sensor would register with upon installation.

3. Install the Linux sensor installation package on a Linux client(s)

Copy the .tar.gz sensor installation package to the client.

Untar the .tar.gz file (do not just open, the contents need to be unzipped on disk).

Execute the .sh file and follow any installation prompts. This will install the Linux sensor using the configuration provided in the `sensorsettings.ini` file.

At this point, the Linux sensor will be installed and running. The sensors pane in the enterprise server administrative interface should show the sensor as registered and checking in.

Upgrade

Prerequisites

1. A Carbon Black enterprise server installation $\geq 4.2.2$
2. A Linux endpoint running a previous version of the Carbon Black Linux Sensor
3. A newer version of the Linux sensor downloaded and installed on the Carbon Black Server (see Installation, Prerequisites, step #3)

Linux clients that are running the Carbon Black Linux sensor can be upgraded automatically via the server or manually at the endpoint. Currently, the server based Linux sensor upgrade is a global (all-or-none) setting in the `cb.conf` file on the Carbon Black enterprise server. Unlike the installer package, the Linux sensor upgrade .tar.gz file does not require any preprocessing.

To enable a Linux sensor upgrade package for deployment via the server, the following steps are required:

1. Install the Linux sensor package on your Carbon Black server by following the "Installing the Sensor files on the Carbon Black server" step.
2. Modify the `cb.conf` setting `SensorUpgradeLinux`
When no upgrade is desired, this setting is set to *Manual* or *None*
To enable the Linux sensors to upgrade to the newer sensor, change this setting to the version number of the Linux sensor upgrade package used in step 1.
Example: `SensorUpgradeLinux=4.2.1.12345`
3. Restart Carbon Black Enterprise
Example: `service cb-enterprise restart`

On the next checkin, the Linux sensors will perform the upgrade to the new linux sensor version.

To upgrade a linux sensor manually follow these steps: Please follow the steps in "Installing the Sensor files on the Carbon Black server" before performing any of these steps.

1. Download via the Carbon Black GUI or generate a Carbon Black Linux Sensor installer tar.gz by following the steps in the above section named "Download the Sensor package from the Carbon Black GUI or manually create it"
2. Copy the Linux sensor installation package to the Linux client(s) that will be upgraded
3. Untar the .tar.gz file (do not just open, the contents need to be unzipped on disk).

4. Uninstall the current Linux sensor by running the following command `/opt/cbsensor/sensoruninstall.sh`. At this point the endpoint will stop reporting events and binaries to the Carbon Black server.
5. Install the new sensor version by running the `.sh` file in the location where the new sensor install package was untared. At this point, the Linux sensor will be installed and running. The sensors pane in the enterprise server administrative interface should show the sensor as registered and checking in.

Known Issues

LNX-52 Sensor needs to detect the Bit9 agent The sensor currently does not detect the Bit9 agent running on the same platform. Which results in the server displaying that the Bit9 agent is not installed.

LNX-53 Linux Sensor not display correct power state The sensor does not update the checkin message with the correct state information, Which results in incorrect display of power state at the server,

LNX-62 port sensor proxy support to linux sensor The sensor does not have support to connect to the Carbon Black server via a proxy.

LNX-68 sensordiag.sh should collect sensor_comms.log file in addition to the other collected logs The sensor supports generating more detailed communication errors which currently are not collected by the diagnostics script.

LNX-69 update linux sensor to use openssl mitigation for poodle vulnerability The sensor currently uses the Openssl shared library available on the system. Which may not have received the security updates for Poodle.

LNX-70 verify netconn IP:dnsname mapping is updated on new name resolving to existing IP The sensor does not update it DNS cache when the ip to name mapping has changed for a host and will report the old name.

LNX-71 Update for Redhat 7 support The sensor currently does not have Redhat/CentOS 7 support built in.

LNX-74 Provide an answer for “CB on CB” The sensor should not be run on a system where a high volume of processes can be created per day (> 10000 a day), as this may impact responsiveness of the Carbon Black server.

Integrations with Bit9 that are not available Process watch lists Process links from Bit9 to Carbon Black