Sensor Osx Install

CB v4.2.7.150629.0500

July 10, 2015

Contents

Overview

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

Installation

Prerequisites

```
1. A Carbon Black enterprise server installation >= 4.2.2
```

The Carbon Black OSX 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.

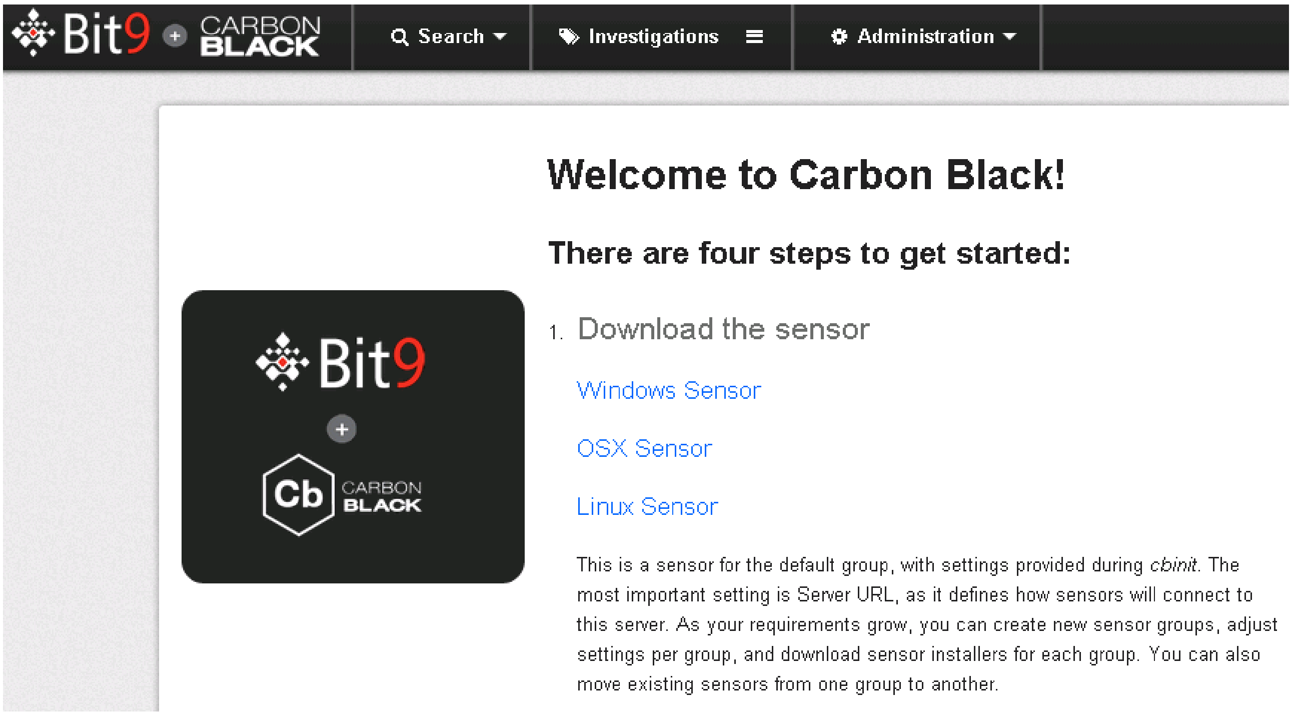
Note With Carbon Black enterprise server installation >=4.2.2 and the OSX sensor rpm installed on the Carbon Black Server, those users with Web UI access can download the Default Sensor group OSX sensor installer package from the main Carbon Black splash page or from the sensor group "Download Sensor 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 OSX 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 OSX sensor is available for download and installation on the Carbon Black server via the YUM packaging system. Download and install the OSX sensor files to the server by following these steps:

1. Verify the repo configured on the server has access to the OSX sensor rpm by running: `yum info cb-osx-sensor`
2. Stop the Carbon Black Services by issuing this command: `service cb-enterprise stop`
3. Install the OSX sensor package on your Carbon Black server: `yum install cb-osx-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 OSX sensor package for the Default Sensor group by clicking on the “OSX 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

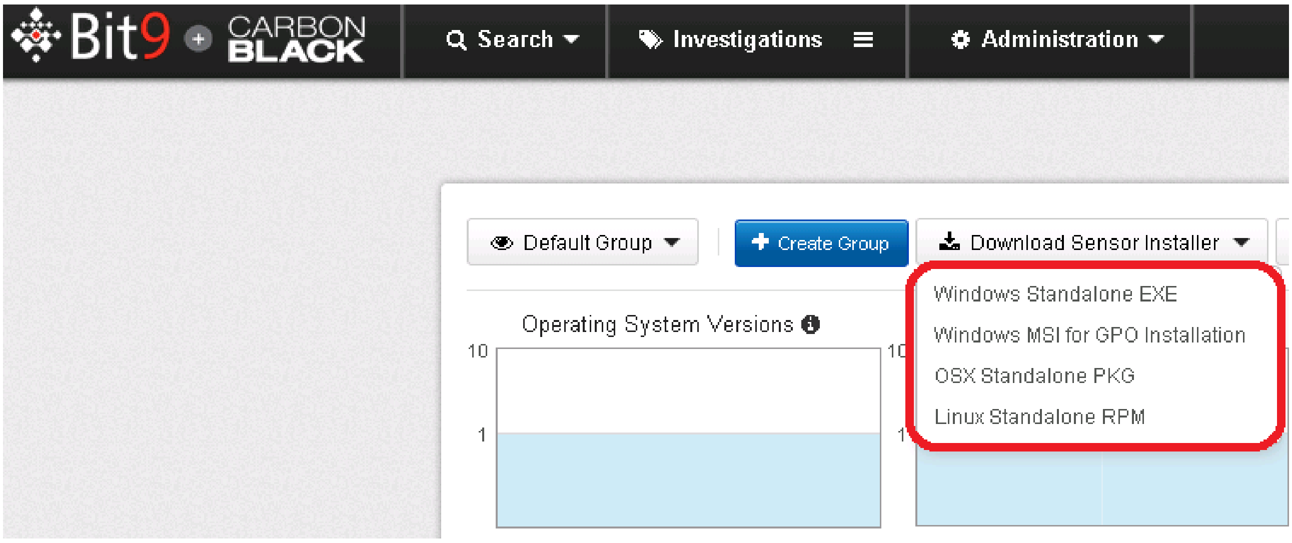
Windows Sensor

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 “OSX Standalone PKG”. The browser will inform you of the Sensor package file download, save the package to disk.



2. Or manually create the OSX sensor installation package.

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

   Execute the following command:

   ```
   /usr/share/cb/cbsensorinstallergen –installer-file=[path to OSX .pkg file] –os=osx –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 .zip that contains the installer and the sensorsettings.ini that are required for installation.

3. Install the OSX sensor installation package on an OSX client(s)

   Copy the .zip sensor installation package to the client.

   Unzip the .zip file (do not just open, the contents need to be unzipped on disk).

   Execute the .pkg file and follow the installation prompts. This will install the OSX sensor using the configuration provided in the sensorsettings.ini file.

At this point, the OSX 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 >= 4.2.2

2. A OSX endpoint running a previous version of the Carbon Black OSX Sensor

3. A newer version of the OSX sensor downloaded and installed on the Carbon Black
Server (see Installation, Prerequisites, step #3)
```

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

To enable an OSX sensor upgrade package for deployment, the following steps are required:

1. Install the OSX 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 *SensorUpgradeOsx*

   When no upgrade is desired, this setting is set to *Manual* or *None*

   To enable the OSX sensors to upgrade to the newer sensor, change this setting to the version number of the OSX sensor upgrade package installed in Upgrade step 1.

   Example: *SensorUpgradeOsx=4.1.0.12345*

3. Restart Carbon Black Enterprise

   Example: *service cb-enterprise restart*

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

To upgrade a OSX sensor manually, follow these steps:

1. Download via the Carbon Black GUI or generate a Carbon Black OSX Sensor installer zip 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 OSX sensor installation package to the OSX client(s) that will be upgraded

3. Unzip the zip file (do not just open, the contents need to be unzipped on disk).

4. Uninstall the current OSX sensor by running the following command */Applications/CarbonBlack/sensoruninst.sh*. At this point the endpoint will stop reporting events and binaries to the Carbon Black server.

5. Install the new sensor version by executing the .pkg file in the location where the new sensor install package was unzipped. At this point, the OSX 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

OSX-112 Cut off text in window provided to user when sensorsettings.ini is not present during GUI install of sensor package This is just an incovenience and does not effect functionality in any way.

OSX-117 Mac Sensor does not detect the presence of the Bit9 Platform 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.

OSX-133 Utilities console display CbOsxSensorService: BUG in libdispatch client The sensor reports that a file being deleted is not longer present. This does not effect functionality in any way.

OSX-140 port proxy support to osx sensor The sensor does not have support to connect to the Carbon Black server via a proxy.

OSX-141 occassional UDP connections on dest port 53 outtbound to 0.0.0.0 observed This IPADDR_ANY and valid given where the packet is being hooked.

OSX-144 Mac Sensor display 0x80CB003D (61) - bad content encoding

This will happen when the Ethernet cable is removed and replaced. The error is transient and does not effect functionality.

OSX-145 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.

OSX-146 update mac sensor to avoid poodle vulnerability The sensor is built with an older version of the Openssl library which
needs to be updated.

OSX-148 verify name resolution overwrites previous name:ip mapping with same 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.

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