Server Install

CB v4.2.5.150311.1434

March 11, 2015

Contents

Important Note on Security Software

By installing this software, you are taking on certain risks. In particular:

- The sensor is lightweight but low-level Windows systems software that includes a service and drivers. As with any low-level software, there is a risk of the Carbon Black sensor introducing stability or security issues.
- The Enterprise Server exposes web APIs over HTTP and/or HTTPS to both users of the web UI and the sensors. As with any server software, it is possible improper handling in these APIs could lead to unwanted code execution by a third party. Standard Linux server techniques involving limiting access, use of iptables, etc. go a long way to mitigating this risk.
- As with any web application, it is possible for an attacker to compromise access to the server via hijacking the browser session. The flip side is it is possible the data in the server itself - which is ultimately generated on Windows boxes that may be compromised - may be compromised. It is recommended to follow normal security precautions, such as running the browser with least privilege.

Overview

The Carbon Black Enterprise Server installation consists of three primary steps:

1. Get and install a RPM from Carbon Black. This RPM does *not* install the enterprise server. It does set up a yum repo and installs a SSL client certificate that allows the full enterprise server to be downloaded and installed.
2. Download the enterprise server using the yum repo setup in step 1.
3. Install the enterprise server. This is a two-step process that involves both “yum install” and running a simple configuration script.

The entire process can be completed in about ten minutes, assuming reasonable download speed.

Terminology

The following table provides high-level descriptions of certain Carbon Black specific functionality:

- **Enterprise Server** - This is the CentOS server which exists on the deployed network. It receives data from sensors, stores and indexes that data, and provides access to the data via the web interface.
- **Sensor** - Sensors are lightweight data-gatherers that are installed on Windows hosts on the deployed network. They gather event data on the Windows hosts and securely deliver it to the Enterprise Server for storage and indexing.
- **Alliance Server** - The Alliance Server is a server managed by Carbon Black that augments the functionality of the Carbon Black Enterprise server. If so configured, the Enterprise Server will analyze certain types of collected data and provide notifications, via e-mail, of potentially malicious activity.

Enterprise Server Hardware & Software Prerequisites

Carbon Black software has certain baseline and recommend hardware and software requirements. They are listed in the table below.

From a high-level, the Carbon Black server requires a CentOS 6.4 or 6.5 x64 server running on commodity hardware. The server is responsible for the processing and storage of potentially large quantities of collected data. Therefore, RAM, disk space, and processing power are all beneficial in terms of providing a performant system.

Note on Low-Volume Installation Resource Requirements The Carbon Black server will install on systems with much less than the recommended minimum specifications.

For the purposes of testing on tens of Windows computers or fewer, the server has very low resource requirements. The requirements increase as the number of simultaneous Windows hosts increases. Systems with as little as 4 GB of RAM can be used in low-volume scenarios, such as those with fewer than 25 active sensors.

Please contact Carbon Black support (support@bit9.com) with questions about these scenarios. Depending on your situation, it may be advisable to apply several minor configuration tweaks to optimize performance.

Component	Requirements	Notes
Operating System	CentOS 6.x x64	See Notes (1)
Processor	8 Physical Cores @ 2.5GHz	More is better
RAM	16GB minimum	See Notes (2)
Storage	500GB minimum	See Notes (3)
Storage Configuration	All physical storage should be accessible on a single mount point	See Notes (4)
Alliance Connectivity	Server must have access to api.alliance.carbonblack.com, either directly or via a web proxy	

Notes

1. Ensure to use the x64 and NOT the i386 version of CentOS. A minimal CentOS installation is acceptable; a full installation also works.
2. RAM requirements vary widely based on the number of installed sensors. A sensor is installed on each Windows computer that Carbon Black monitors. 16GB is a baseline number for server RAM. 32GB is recommended as a production minimum. As a very rough rule of thumb, we recommend 20MB of RAM per active sensor. For lab environments with fewer than 50 Windows computers, 16GB is sufficient.
3. Storage requirements depend on two core variables: the number of installed Carbon Black sensors and the number of days sensor data is maintained. Exact storage requirements are *highly* dependent upon the activity level and type observed by the sensors. Assuming all event types are enabled and stored locally, a conservative estimate is 8MB/host/day. For example, installing Carbon Black on 5000 Windows computers and keeping data for 30 days requires 8MB * 5000 * 30, or ~1TB.
4. Carbon Black recommends all storage be usable via a single mount point. Advanced installation options allow for different mount points to be used under certain circumstances, but this is not recommended.
5. Carbon Black production systems also need good, fast disks with high concurrency. (i.e., SSDs or an array) Slower disks can be mitigated, to a degree, with more RAM allocated to the filesystem cache.

Perimeter Firewall Requirements

Internet connectivity is required on the Enterprise Server in two scenarios, as described in the below table. Connectivity is required via outbound TCP.

Scenario	Description	Endpoint
Carbon Black Yum Repository	The RPM installer sets up a yum repository. Access to this yum repository is required in order to download the Enterprise Server.	yum.carbonblack.com:443
Carbon Black Alliance Server	The Enterprise Server can be configured to provide further analysis, including analysis via partners such as VirusTotal.	api.alliance.carbonblack.com:443
CentOS Yum Repository	The standard CentOS Yum repository servers used during Carbon Black Enterprise Server installation to download standard packages	mirror.centos.org:80

Quick Installation Steps

1. Install the release RPM: `rpm -Uvh carbon-black-release-1.0.0-1.el6.x86_64.rpm`
2. Install cb-enterprise: `yum install cb-enterprise`
3. Run cbinit: `/usr/share/cb/cbinit` *(only required on the first install)*
4. Start the services: `service cb-enterprise start`

Detailed installation

If you already have the Enterprise Server installed, DO NOT perform these steps. Instead, see the “Upgrade Steps” section later in this document.

Following the installation steps in this section will likely result in the loss of all data, including configuration and event data collected from sensors.

1. Verify the server you intend to install Carbon Black Enterprise Server 3 meets requirements. Please see “Hardware & Software Prerequisites” later in this document.
2. Verify the server has Internet connectivity. See section on “Enterprise Server Internet Connectivity Requirements” for more details.
3. Procure an installation RPM from Carbon Black. This requires interaction, by e-mail, with Carbon Black.
4. Install the RPM
    1. Verify you are running with root access
    2. Install the RPM using `rpm -Uvh carbon-black-release-1.0.0-1.el6.x86_64.rpm`
    3. [OPTIONAL] Verify that the Carbon Black [cb] yum repository was set up in /etc/yum.repos.d/CarbonBlack.repo
    4. [OPTIONAL] Verify that the Carbon Black SSL client certificate was installed in /etc/cb/certs/carbonblack-alliance-client.key

```
[root@ScottCbServer yum.repos.d]# rpm -Uvh carbon-black-release-1.0.0-1.el6.x86_64.rpm
[root@ScottCbServer yum.repos.d]# pwd
/etc/yum.repos.d
[root@ScottCbServer yum.repos.d]# cat CarbonBlack.repo
[cb]
```

```
name=cb
baseurl=https://yum.carbonblack.com/enterprise/stable/x86_64/repodata
gpgcheck=0
enabled=1

[root@ScottCbServer yum.repos.d]#
```

5. Install the Carbon Black Enterprise Server

    5. Verify that your computer's date and time settings are accurate. Incorrect date/time settings can result to failures in SSL negotiation, which is required for yum downloads.
    6. yum install cb-enterprise
    7. You may be prompted to install the CentOS GPG key. Please do so if and when prompted.
    8. If your environment requires that outbound firewall exceptions be made, ensure that the exceptions documented in the "Enterprise Server Internet Connectivity Requirements" section of this document are followed. You will also have to update /etc/yum.repos.d/CentOS-Base.repo to enable the baseurl of http://mirror.centos.org.
    9. Yum supports the use of web proxies. We are not aware of a way to use yum with NTLM-authenticated web proxies.

```
[kyle@localhost yum.repos.d]$ sudo yum install cb-enterprise
```

6. Configure the Carbon Black Enterprise Server as desired:

    10. run /usr/share/cb/cbinit
    11. It is best to back up the SSL certificate generated to protect sensor-to-server communications, as prompted by cbinit
    12. When viewing the license agreement, use "q" to exit the editor

```
[kyle@localhost yum.repos.d]$ sudo /usr/share/cb/cbinit
[sudo] password for kyle:

------------------------------------------------------------------------------
CARBON BLACK ENTERPRISE SERVER - INITIALIZATION
------------------------------------------------------------------------------


Thank you for installing Carbon Black Enterprise Server. This tool will
guide you through a few setup steps which are necessary in order to finalize
the installation of the server.

------------------------------------------------------------------------------
    END USER LICENSE AGREEMENT
------------------------------------------------------------------------------

Please, review and accept the End User License Agreement before proceeding
with the server setup

Hit 'return' to open the agreement and 'q' when you're done reading it:

    <AGREEMENT>

Do you accept the license agreement [yes/no]: yes

------------------------------------------------------------------------------
STORAGE LOCATION
------------------------------------------------------------------------------

Please choose a data storage location with as much space as possible.  If needed,
```

```
refer to the Carbon Black Data Storage Guidelines document.

Enter path for data storage location [/var/cb/data]: (Pressed enter)

You picked: /var/cb/data

--------------------------------------------------------------------------------
   ADMINISTRATOR ACCOUNT
--------------------------------------------------------------------------------


Here you configure your GLOBAL ADMINISTRATOR account.
This account is the most powerful account on the server.

Be sure to put a valid e-mail address if you want to take full advantage
of Carbon Black's notification system.

Verify Account Information...
          Username: kyle
        First Name: Kyle
         Last Name: Beaumont
            E-Mail: kyle.beaumont@my.org
          Password:
  Confirm password:

Verify Account Information:
          Username: Kyle
        First Name: kyle
         Last Name: Beaumont
            E-Mail: kyle.beaumont@my.org
Is this correct [Y/n]: y

--------------------------------------------------------------------------------
  SENSOR COMMUNICATIONS
--------------------------------------------------------------------------------

You need to configure the address that the sensors will talk to.  This needs to
be an ip-address or domain name that is reachable by the sensor machines.

This can be different per sensor-group and can be changed later, but it is
easiest if you put in the valid address now.

Default sensor group server URL: https://192.168.12.119:443

Would you like to keep the default [Y/n]:

--------------------------------------------------------------------------------
  HELP IMPROVE YOUR CARBON BLACK EXPERIENCE
--------------------------------------------------------------------------------


We are constantly looking for ways to make the Carbon Black user experience
better.  Please help us achieve this goal by allowing automatic reporting of
usage, resource, and sensor statistics to our technology and support teams.

You can later change your mind, too, by going here:

  >>> Administration -> Settings -> Communications

Do you want your Cb Server to submit statistics and feedback information
back to Bit9? [Y/n]:
```

```
--------------------------------------------------------------------------------
  BIT9 ALLIANCE
--------------------------------------------------------------------------------


Be notified of any binary flagged by VirusTotal.  Information such as the
filename, MD5 hash and parent process will be shared with the Bit9 Alliance
partners, including VirusTotal.

All information is anonymized to the extent reasonably practicable before being
shared with Bit9 Alliance partners. The applicable terms and conditions are set
forth in and subject to your Bit9 License Agreement. For further information
on what information is collected and shared by the Bit9 Alliance Server, please
visit http://carbonblack.com/collaboration.

You can change this setting at any time in the Carbon Black web console:

>>> Administration -> Sensors -> Edit Settings (for a particular group)

If you enable this, you will then be prompted to either enable or disable the
uploading of unknown binaries.

Do you want the default sensor group to have Bit9 Alliance connectivity
enabled? [Y/n]:

Detect new variants of known malware by sharing the full binary content of
unknown executable files.  Binaries will be uploaded and shared with the
Bit9 Alliance partners, including VirusTotal.  Any binary submitted to the
Bit9 Alliance is deleted on the local Carbon Black server, saving disk space.

All information is anonymized to the extent reasonably practicable before being
shared with Bit9 Alliance partners. The applicable terms and conditions are set
forth in and subject to your Bit9 License Agreement. For further information
on what information is collected and shared by the Bit9 Alliance server,
please visit http://carbonblack.com/collaboration.

You can change this setting at any time in the Carbon Black web console:

    >>> Administration -> Sensors -> Edit Settings (for a particular group)

Do you want the default sensor group to submit unknown binaries to the
Bit9 Alliance? [y/N]: y

Please confirm that you want to scan unknown binaries with VirusTotal
[y/N]: y

--------------------------------------------------------------------------------
  SECURITY - SSL CERTIFICATE GENERATION
--------------------------------------------------------------------------------

Generating self-signed HTTPS Server certificate...

Generating self-signed HTTPS Sensor CA certificate...


Carbon Black Enterprise Server uses a SSL certificate to establish secure
communications between sensors and the server.

Should the certificate and/or its private key be lost, sensors will no longer
be able to communicate with the Enterprise Server.
```

```
We recommend backing up the SSL certificate files at this time by running:

/usr/share/cb/cbssl backup --out <backup_file_name>

IMPORTANT: Backup file must be securely stored.  Anyone with access to the
information contained in that file will be able to compromise the security
of sensor-server communications and potentially compromise the security of
the computers on which the sensors run.
--------------------------------------------------------------------------------
  SENSOR COMMUNICATIONS
--------------------------------------------------------------------------------

You need to configure the address that the sensors will talk to.  This needs to
be an ip-address or domain name that is reachable by the sensor machines.

This can be different per sensor-group and can be changed later, but it is
easiest if you put in the valid address now.

Default sensor group server URL: https://192.168.12.119:443

Would you like to keep the default [Y/n]:

--------------------------------------------------------------------------------
  HELP IMPROVE YOUR CARBON BLACK EXPERIENCE
--------------------------------------------------------------------------------


We are constantly looking for ways to make the Carbon Black user experience
better.  Please help us achieve this goal by allowing automatic reporting of
usage, resource, and sensor statistics to our technology and support teams.

You can later change your mind, too, by going here:

   >>> Administration -> Settings -> Communications

Do you want your Cb Server to submit statistics and feedback information
back to Bit9? [Y/n]:

--------------------------------------------------------------------------------
  BIT9 ALLIANCE
--------------------------------------------------------------------------------


Be notified of any binary flagged by VirusTotal.  Information such as the
filename, MD5 hash and parent process will be shared with the Bit9 Alliance
partners, including VirusTotal.

All information is anonymized to the extent reasonably practicable before being
shared with Bit9 Alliance partners. The applicable terms and conditions are set
forth in and subject to your Bit9 License Agreement. For further information
on what information is collected and shared by the Bit9 Alliance Server, please
visit http://carbonblack.com/collaboration.

You can change this setting at any time in the Carbon Black web console:

  >>> Administration -> Sensors -> Edit Settings (for a particular group)

If you enable this, you will then be prompted to either enable or disable the
uploading of unknown binaries.
```

```
Do you want the default sensor group to have Bit9 Alliance connectivity
enabled? [Y/n]:

Detect new variants of known malware by sharing the full binary content of
unknown executable files.  Binaries will be uploaded and shared with the
Bit9 Alliance partners, including VirusTotal.  Any binary submitted to the
Bit9 Alliance is deleted on the local Carbon Black server, saving disk space.

All information is anonymized to the extent reasonably practicable before being
shared with Bit9 Alliance partners. The applicable terms and conditions are set
forth in and subject to your Bit9 License Agreement. For further information
on what information is collected and shared by the Bit9 Alliance server,
please visit http://carbonblack.com/collaboration.

You can change this setting at any time in the Carbon Black web console:

>>> Administration -> Sensors -> Edit Settings (for a particular group)

Do you want the default sensor group to submit unknown binaries to the
Bit9 Alliance? [y/N]: y

Please confirm that you want to scan unknown binaries with VirusTotal
 [y/N]: y


-------------------------------------------------------------------------------
  SECURITY - SSL CERTIFICATE GENERATION
-------------------------------------------------------------------------------

Generating self-signed HTTPS Server certificate...

Generating self-signed HTTPS Sensor CA certificate...


Carbon Black Enterprise Server uses a SSL certificate to establish secure
communications between sensors and the server.

Should the certificate and/or its private key be lost, sensors will no longer
be able to communicate with the Enterprise Server.

We recommend backing up the SSL certificate files at this time by running:

/usr/share/cb/cbssl backup --out <backup_file_name>

IMPORTANT: Backup file must be securely stored.  Anyone with access to the
information contained in that file will be able to compromise the security
of sensor-server communications and potentially compromise the security of
the computers on which the sensors run.


Continue [return]:

-------------------------------------------------------------------------------
 BIT9 ALLIANCE
-------------------------------------------------------------------------------


Be notified of any binary flagged by VirusTotal.  Information such as the
filename, MD5 hash and parent process will be shared with the Bit9 Alliance
partners, including VirusTotal.
```

```
All information is anonymized to the extent reasonably practicable before being
shared with Bit9 Alliance partners. The applicable terms and conditions are set
forth in and subject to your Bit9 License Agreement. For further information
on what information is collected and shared by the Bit9 Alliance Server, please
visit http://carbonblack.com/collaboration.

You can change this setting at any time in the Carbon Black web console:

    >>> Administration -> Sensors -> Edit Settings (for a particular group)

If you enable this, you will then be prompted to either enable or disable the
uploading of unknown binaries.

Do you want the default sensor group to have Bit9 Alliance connectivity
enabled? [Y/n]:

Detect new variants of known malware by sharing the full binary content of
unknown executable files.  Binaries will be uploaded and shared with the
Bit9 Alliance partners, including VirusTotal.  Any binary submitted to the
Bit9 Alliance is deleted on the local Carbon Black server, saving disk space.

All information is anonymized to the extent reasonably practicable before being
shared with Bit9 Alliance partners. The applicable terms and conditions are set
forth in and subject to your Bit9 License Agreement. For further information
on what information is collected and shared by the Bit9 Alliance server,
please visit http://carbonblack.com/collaboration.

You can change this setting at any time in the Carbon Black web console:

  >>> Administration -> Sensors -> Edit Settings (for a particular group)

Do you want the default sensor group to submit unknown binaries to the
Bit9 Alliance? [y/N]: y

Please confirm that you want to scan unknown binaries with VirusTotal
[y/N]: y


------------------------------------------------------------------------------
  SECURITY - SSL CERTIFICATE GENERATION
------------------------------------------------------------------------------

Generating self-signed HTTPS Server certificate...

Generating self-signed HTTPS Sensor CA certificate...


Carbon Black Enterprise Server uses a SSL certificate to establish secure
communications between sensors and the server.

Should the certificate and/or its private key be lost, sensors will no longer
be able to communicate with the Enterprise Server.

We recommend backing up the SSL certificate files at this time by running:

/usr/share/cb/cbssl backup --out <backup_file_name>

IMPORTANT: Backup file must be securely stored.  Anyone with access to the
information contained in that file will be able to compromise the security
of sensor-server communications and potentially compromise the security of
the computers on which the sensors run.
```

```
Continue [return]:

--------------------------------------------------------------------------------
  SECURITY - IPTABLES CONFIGURATION
--------------------------------------------------------------------------------

Carbon Black Enterprise Server listens on a number of TCP/IP ports. If
iptables firewall is running on the host machine, iptables must be configured
to allow incoming connections on these ports.

To get a list iptables rules that need to be added to current host
configuration, you can run '/usr/share/cb/cbcheck iptables -l' at any time and
apply the rules manually.  Alternatively, Carbon Black Server setup and
configuration tools can take over management of iptables configuration and
apply updates whenever they are needed.

Would you like Carbon Black Server to manage iptables [Y/n]:
Applying iptables rules:
   -I INPUT 5 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT

iptables: Saving firewall rules to /etc/sysconfig/iptables:[  OK  ]

--------------------------------------------------------------------------------
  SETTING UP POSTGRESQL DATABASE
--------------------------------------------------------------------------------

Initializing Carbon Black Server PostgreSQL Instance...

The files belonging to this database system will be owned by user "cb".
This user must also own the server process.

The database cluster will be initialized with locale "en_US.UTF-8".
The default text search configuration will be set to "english".

Data page checksums are disabled.

creating directory /var/cb/data/pgsql ... ok
creating subdirectories ... ok
selecting default max_connections ... 100
selecting default shared_buffers ... 128MB
creating configuration files ... ok
creating template1 database in /var/cb/data/pgsql/base/1 ... ok
initializing pg_authid ... ok
setting password ... ok
initializing dependencies ... ok
creating system views ... ok
loading system objects' descriptions ... ok
creating collations ... ok
creating conversions ... ok
creating dictionaries ... ok
setting privileges on built-in objects ... ok
creating information schema ... ok
loading PL/pgSQL server-side language ... ok
vacuuming database template1 ... ok
copying template1 to template0 ... ok
copying template1 to postgres ... ok
syncing data to disk ... ok

Success. You can now start the database server using:
```

```
 /usr/pgsql-9.3/bin/postgres -D /var/cb/data/pgsql
   or
 /usr/pgsql-9.3/bin/pg_ctl -D /var/cb/data/pgsql -l logfile start

waiting for server to start.... done
server started
Creating core model DB schema...
Creating alliance model DB schema...
waiting for server to shut down.... done
server stopped

-----------------------------------------------------------------------------
   SETUP COMPLETE!
-----------------------------------------------------------------------------


Server setup has COMPLETED successfully.

Do you want to start the services [Y/n]:
```

7. Configure firewall

    13. Open port 443 if you did not allow the cbinit script to automation do that for you

    ```
    Applying iptables rules:
       -I INPUT 5 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
    ```

    14. [OPTIONAL] Open port 80 to allow use of web UI and sensor communications via unsecured channel. This is not required and only recommended for exploration or troubleshooting.

```
[kyle@localhost yum.repos.d]$ sudo vim /etc/sysconfig/iptables

# Firewall configuration written by system-config-firewall
# Manual customization of this file is not recommended.
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
-A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
-A INPUT -p icmp -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -m state --state NEW -m tcp -p tcp --dport 22 -j ACCEPT
-A INPUT -j REJECT --reject-with icmp-host-prohibited
-A FORWARD -j REJECT --reject-with icmp-host-prohibited
 # New additions to the IPTABLES for carbon black
-A INPUT -m state --state NEW -m tcp -p tcp --dport 443 -j ACCEPT
COMMIT
```

8. Log in to the Carbon Black Enterprise Server web user interface

    15. [https://<your centos server address>/](http://localhost/)
    16. Use the username and password set up in the cbinit script
    17. As of this time, **only** Google Chrome is supported. In our internal, testing, Firefox, Opera and IE10 or higher should work. IE requires the browser to NOT be in compatibility mode. Servers in the same subnet as the broswer are automatically connected in this mode.

Upgrade Steps

If you are UPGRADING the server, please follow the steps in this section.

Standalone Server

1. On the server, stop the Carbon Black services: `service cb-enterprise stop`
2. Update the Carbon Black services: `yum install cb-enterprise`
3. Restart the Carbon Black services: `service cb-enterprise start`

Clustered Server

1. On the Master server, navigate to the cb install directory (defaults to /usr/share/cb) and stop the Carbon Black services: `cbcluster stop`
2. Update the Carbon Black services on all nodes: `yum install cb-enterprise`
3. Restart the Carbon Black services: `cbcluster start`

Improvements of Carbon Black will occasionally require a utility called `cbupgrade` to be used after `yum install cb-enterprise` to migrate the database schema or alliance feed data. The operator will be notified of this requirement when attempting to start the cb-enterprise services. In a clustered Server configuration, this utility will need to be run on all nodes before restarting the cluster. When running this utility in a clustered environment, be sure to answer 'NO' when asked to start the CB services, the administrator will need to use 'cbcluster' to start the clustered server.

Important Notes Regarding Upgrades and New Sensor Versions

A new server version *may* include a new sensor version. Please check the release notes or contact support@bit9.com if there are any questions.

If a new sensor version is included, you will need to make a decision as to if you want the sensor to be deployed immediately to existing sensor installations, or if you want to install only server updates.

This can be configured via the web UI. Log in to the web UI, navigate to the 'Sensors' page, and edit the group settings for each active group:

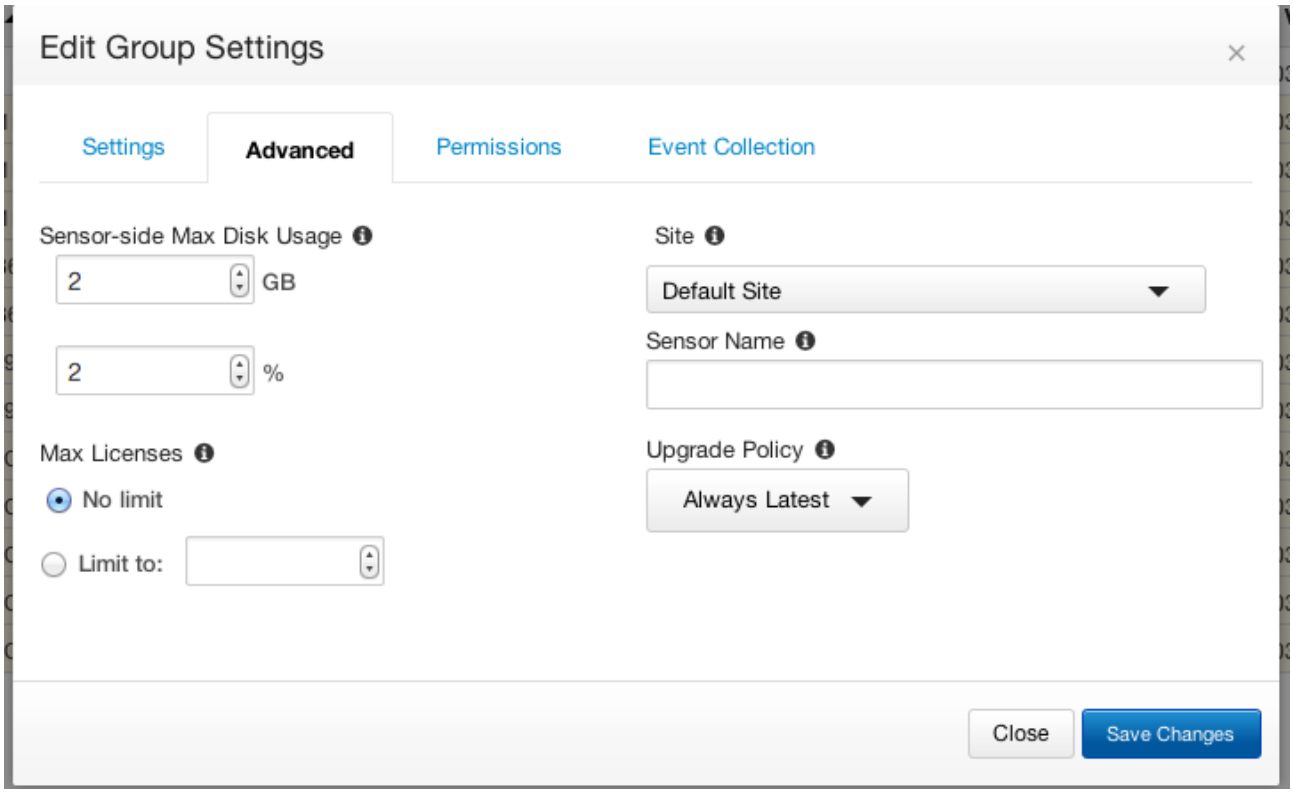

Figure 1: Group settings dialog

Under the 'Advanced' tab, find the "Upgrade Policy" setting. If this is set to "Always Latest", the server will automatically sensors to the latest sensor version. If you want to keep the sensors at a specific version, select that version number from the dropdown *prior* to upgrade. If you want to continue using whatever sensor versions are already installed, regardless of version, select 'Manual'.

What Next?

At this point the Carbon Black Enterprise Server is installed. It should be accessible via the web UI, on port 443 with a self-signed certificate. If you have opened port 80, the web UI is also accessible via HTTP on port 80.

The next step, especially in a test environment, is to download a sensor installer and install one or more sensors on Windows computers to being collecting data. This is accomplished using the following steps:

1. Log into the web UI
2. Navigate to the 'Sensors' page using the 'Administration' drop-down at the top of the web UI.
3. Click the 'Edit Settings' button; this is the fourth button from the left in the 'Sensors' page.
4. Under the 'Settings' tab, verify that the 'Server' field is correct. If this field is not correct, the sensors will not be able to communicate with the server. **It is important to note that this IP or name must be** ** *usable by the sensor* ** - if the Carbon Black Enterprise Server 'appears' as a different IP from the locally bound IP to the sensor hosts, use the appropriate IP or name.
5. If no changes are necessary, exit the dialog using the 'Close' button. Otherwise, use the 'Save Changes' button to save the changes.
6. Click the 'Download Sensor Installer' button; this is the third button from the left on the 'Sensors' page.
7. Choose the 'Standalone EXE' option
8. When downloaded, transfer the resultant ZIP file to a Windows computer (XPSP3 or higher, either 32- or 64-bit).
9. Extract the contents of the ZIP file.
10. Execute the installer. On Vista, Windows 7, Windows 8, Windows Server 2008, and Windows Server 2012, you will be prompted for elevation as required.

Troubleshooting

Server logs are found at `/var/log/cb`. Logs are organized into subdirectories by component, as described here:

Component	Description
allianceclient	The Alliance Client communicates with the Carbon Black Alliance server, and allows for notifications of VirusTotal alerts among other capabilities.
cbfs-http	The core event data processing component. This component manages incoming event data from the sensors, indexes, and stores the data.
coreservices	Provides access to functionaltity via web APIs to both the web UI and to sensors. Nearly all UI issues should result in log entries for coreservices.
job-runner	The Carbon Black server uses cron jobs to provide various scheduled maintenance, data trimming, and similar tasks.
pgsql	The Carbon Black server uses Postgres SQL to store administrative data. Event data gathered from the sensors is not stored in Posgres.

There are also a series of troubleshooting scripts found in `/usr/share/cb`:

Script	Description

cbdiag	Dumps verbose troubleshooting information, including logs and configuration, to a gzip archive. This file can be analyzed offline or provided to Carbon Black with support requests.
sensor_report	Generates a log of all registered sensors, with an emphasis of calling out error conditions.
cbpasswd	Resets a user's password. Can only be run as root.

Troubleshooting The Sensor

The sensor is installed in the following directory:

`%WINDIR%\CarbonBlack`

Installation logs can be found at:

`%WINDIR%\CarbonBlack\InstallLogs`

The current sensor log is at:

`%WINDIR%\CarbonBlack\Sensor.log`

Additional sensor control can be performed by issuing a control request to the sensor. This is done using the following command line:

`sc control carbonblack <CONTROLCODE>`

There are two supported control codes:

Control Code	Description
200	Trigger a connection attempt to the Carbon Black server. In most cases, this will be a near-immediate connection attempt. Exceptions are during sensor startup and shutdown, and if any outstanding connection or connection attempt to the server is in progress. For example, if an eventlog or other data is currently being uploaded to the server, or if an attempt to connect to the server is in progress, the triggered attempt will not occur until after the current operation is complete.
201	Trigger a dump of diagnostic data to the `%WINDIR%\CarbonBlack\Diagnostics` directory.

A summary of the diagnostic logs dumped with the 201 code is as follows:

Log	Description
`EventConverter.log`	Internal memory state for event conversion
`EventLogger.log`	Top-level event logging statistics
`NetConnEvents.log`	Network event logging statistics
`RawEventStats.log`	Internal statistics for the conversion of raw events (generated by the core sensor driver) to event messages that are ultimately stored on the CB server
`SensorComms.log`	History of the last 100 network communication attempts between the sensor and the server
`SensorComponents.log`	Current state of the internal sensor components

The sensor installer writes configuration data to the registry under `HKLM\Software\CarbonBlack\Config`. Configuation data includes the server address, the SSL public key used to verify the authenticity of the server, and event collection masks.

The below screenshot, of regedit, provides an example of what that configuration data may look like in the registry:

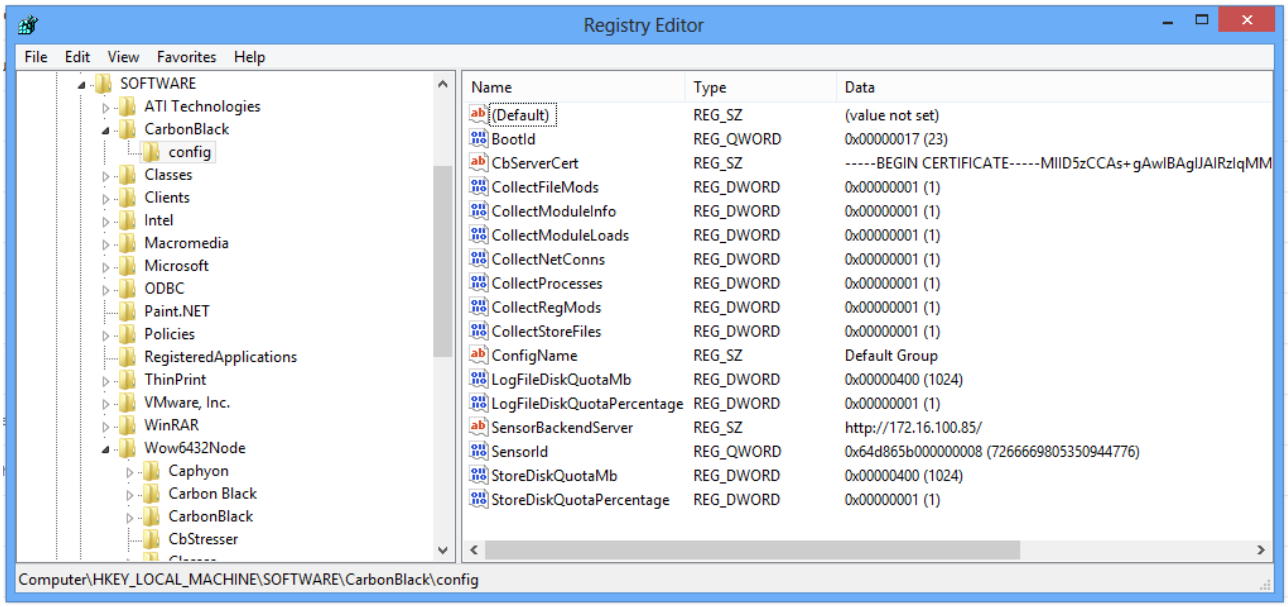

Figure 2: Typical registry settings

If this data is missing - in particular, if the `SensorBackendServer` or `CbServerCert` values are missing - the sensor will not be able to communicate with the server.