Sensor Troubleshooting

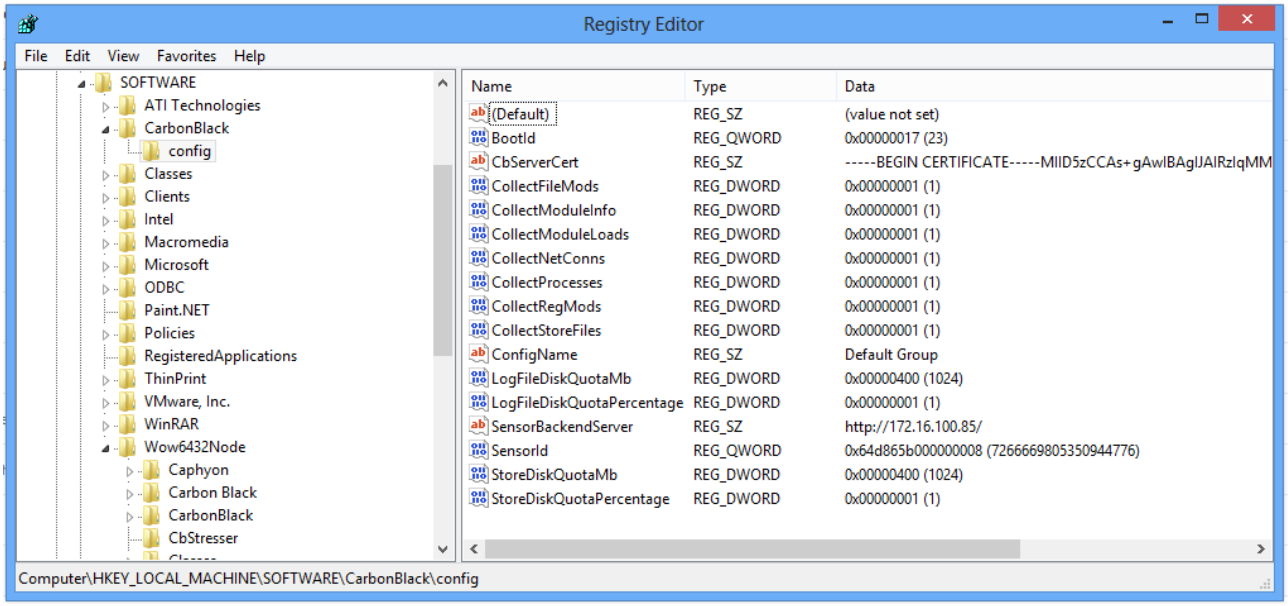
CB v4.2.5.150311.1434

March 11, 2015

Contents

Basic installation

1. Carbon Black installs at `%WINDIR%\CarbonBlack\\`. Confirm this directory exists.
2. Confirm presence of installation logs at `%WINDIR%\CarbonBlack\InstallLogs\\`. Review latest log for errors.
3. Confirm presence of current sensor log at `%WINDIR%\CarbonBlack\Sensor.log`. Review for errors.
4. Confirm settings in registry key at `HKLM\Software\CarbonBlack\Config`. A typical configuration looks like:



Detailed logs 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.

Control code 201 dumps the following logs:

Log	Description
`EventConverter.log`	Internal memory state for event conversion
`EventLogger.log`	Top-level event logging statistics
`MachineStatistics.log`	General System, Process and Kernel Statistics
`ModuleInfo.log`	Internal module 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 screenshot below demonstrates:

1. No `Diagnostics` directory
2. `sc control carbonblack 201` and the expected `sc.exe` output.
3. A populated `Diagnostics` directory with `SensorComms.log`


Administrator: Command Prompt
C:\Windows\CarbonBlack>dir
Volume in drive C is OSDisk
Volume Serial Number is 3C9C-F25D
Directory of C:\Windows\CarbonBlack
05/20/2013 04:28 PM <DIR> .
05/20/2013 04:28 PM <DIR> ..
05/15/2013 01:44 PM 3,052,536 cb.exe
05/20/2013 04:28 PM <DIR> DebugLogs
05/20/2013 04:28 PM <DIR> eventlogs
05/17/2013 04:32 PM <DIR> InstallLogs
05/20/2013 04:28 PM 0 Sensor.LOG
05/15/2013 04:16 PM 47 SensorUpgrade.LOG
05/17/2013 04:32 PM 167,872 uninst.exe
05/15/2013 04:15 PM <DIR> upgrade
4 File(s) 3,220,455 bytes
6 Dir(s) 620,578,656,256 bytes free
C:\Windows\CarbonBlack>sc control carbonblack 201
SERVICE_NAME: carbonblack
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0
C:\Windows\CarbonBlack>dir Diagnostics\SensorComms.log
Volume in drive C is OSDisk
Volume Serial Number is 3C9C-F25D
Directory of C:\Windows\CarbonBlack\Diagnostics
05/20/2013 04:28 PM 822 SensorComms.log
1 File(s) 822 bytes
0 Dir(s) 620,578,500,608 bytes free
C:\Windows\CarbonBlack>

Debugging sensor communications

After `sc control carbonblack 201`, the `%WINDIR%\CarbonBlack\Diagnostics\\` directory will include `SensorComms.log`. That log file will contain data in the following format:

```
Server URL:    https://x.x.x.x:443

Time                 | URL                                          | HRESULT    | Code  |
-------------------- + -------------------------------------------- + ---------- + ----- +
2013-05-20 21:28:38  | https://x.x.x.x:443/sensor/register          | 0x00000000 | 0     |
2013-05-20 21:28:38  | https://x.x.x.x:443/sensor/checkin           | 0x00000000 | 0     |
2013-05-20 21:28:38  | https://x.x.x.x:443/data/eventlog/submit     | 0x00000000 | 0     |

continuation of log

| DurationMs | TxBytes  | RxBytes  | Throttle KB/s
+ ---------- + -------- + -------- + --------------------
| 577        | 300      | 10       | 100
| 312        | 402      | 104      | 100
| 249        | 4328     | 0        | 0
```

The columns represent the following information:

Column	Description
Time	the time (UTC) of the connection attempt
URL	the URL used
HRESULT	the result of the operation as a raw HRESULT (0x00000000 is success)
Code	the result processed code. This can vary based on HRESULT source, but can be the HTTP code (404, 500), a Win32 error (net helpmsg code), or other codes.
DurationMs	duration of the connection attempt in milliseconds.
TxBytes	bytes transmitted, not including HTTP headers.
RxBytes	bytes received, not including HTTP headers.
Throttle KB/s	rate at which the connection was throttled in KB/s; 0 indicates it was unthrottled.

These can be used to troubleshoot sensor to server communication errors.