	Carbon Black VDI Configuration 14-Apr-2014 Cb-Support@Bit9.com

Introduction

The purpose of this document is to describe how to configure Carbon Black to operate within a non-persistent VDI environment.

Sections

Carbon Black Server Configuration

1. Edit the /etc/cb/cb.conf file and add the following values:

```
NewRegistrationCallbackModulePath=/usr/share/cb/plugins/default_new_sensor_registration_callback.py
NewRegistrationCallbackClassName=DefaultNewRegistrationCallback
```

2. Restart cb-enterprise:
   a. Clustered environment (on master run):
      /usr/share/cb/cbcluster stop
      /usr/share/cb/cbcluster start
   b. Non Clustered:
      service cb-enterprise stop
      service cb-enterprise start

3. Endpoints with sensor installs that have the sensor ID set to 0 will get the sensor ID they received when they originally registered with the Carbon Black server. New sensors brought online that have not previously registered will get the next available sensor ID.

Note: In a VDI environment where the master image is allowed to communicate with the Carbon Black server after the sensor install the “GPO Configuration” section will need to be followed to ensure all instantiated instances are reset to a sensor ID of 0 before they register with the Carbon Black server.

Manual Configuration

The requirement is that the Sensor ID is set back to 0 at system shutdown. A common practice for VDI maintenance is to power on a VDI image in “private” mode, make modifications, and then power back down to make available for sessions. This process identifies the steps required to manually set the Sensor ID to 0 before making the image available for sessions.

Wrap up Script Configuration

One option to reset the sensor ID to 0 on the VDI master image is a “wrapup” script designed to be executed after modifications are made to the “private” VDI session can access. This option is desired in instances where a “wrapup” process already exists as this is the easiest configuration to implement.

OPTION 0: Utilize “Wrapup” Script

Create “Wrapup” Script

1. Open notepad.exe
2. Copy the below text into the notepad window:

C:\windows\system32\reg.exe ADD HKLM\Software\CarbonBlack\config /v SensorId /t REG_QWORD /d 0 /f

3. Click File → Save As
4. Choose a safe location that the “private” VDI session can access
5. Name the file as below:

CbSensorIDReset.bat

6. Click Ok
7. Close out notepad.exe

Execute “Wrapup” Script on private VDI Session

1. Browse to the location where *CbSensorIDReset.bat* resides
2. Double click the file

GPO Configurations

There are two options to reset the sensor ID to 0 if the VDI master image is allowed to communicate with the Carbon Black server. Option 1 is the preferred option because this allows the sensor ID to remain in the registry for the life of the VDI instantiation.

Assumption: The GPO is applied and linked to the OU where the Computers reside that require the VDI configuration.

OPTION 1: Assign computer shutdown scripts to a GPO

3. Open Group Policy Object Editor.

4. In the console tree, Follow this path: Group Policy object/Computer Configuration/Windows Settings/Scripts (Startup/Shutdown)
5. In the details pane, double-click Shutdown.
6. In the Shutdown Properties dialog box, click Add.
7. Script Name:

```
C:\windows\system32\reg.exe
```

8. In the Script Parameters:

```
ADD HKLM\Software\CarbonBlack\config /v SensorId /t REG_QWORD /d 0 /f
```

9. Click Ok (twice)
10. Close out the Group Policy Editor

OPTION 2: Apply a Registry Item

1. Open Group Policy Object Editor.
2. In the console tree under Computer Configuration, expand the Preferences folder, and then expand the Windows Settings folder.
3. Right-click the Registry node, point to New, and select Registry Item.
4. In the New Registry Item dialog box, select Update and enter the following values:

```
HIVE: HKEY_LOCAL_MACHINE
Key Path: SOFTWARE\CarbonBlack\config
Value type: REG_QWORD
Value Data: 0
Base: Hexadecimal
```

5. Click OK.
6. Close out the Group Policy Editor