Syslog Templates Developer Guide

CB v4.2.5.150311.1434

March 11, 2015

Contents

Carbon Black Syslog Templates Developer Guide

Purpose & Audience

The purpose of this document is to describe how to use Carbon Black syslog templates to build custom-formatted syslog notifications on Carbon Black Watchlist and Feed hits and Binary Information events. The intended audience are developers interested in modifying the format of Carbon Black syslog output.

For documentation on the out-of-the-box syslog watchlist format and usage, please see the Carbon Black Syslog User Guide.

Background

Carbon Black logs all Watchlist and Feed hits and Binary Information events to syslog with the program name prefix `cb-notifications-`. By default, these are written to log files at `/var/log/cb/notifications` based on the syslog configuration at `/etc/rsyslog.d/cb-coreservices`. There is one file for all hits, one file for each watchlist and each feed. Per-file watchlists include the watchlist id in the program name and log file name, while per-file feeds include the feed id in the program name and log file name. Binary information events are logged in a separate file.

For example, the directory listing below contains four log files: one for all watchlist and feed hits, another for just hits to watchlist id 10, another for just hits to feed id 8, and a fourth one for all binary information events:

```
[root@localhost coreservices]# ll /var/log/cb/notifications/*.log
-rw-------. Jun  9 15:30 /var/log/cb/notifications/cb-all-notifications.log
-rw-------. Jun  9 15:30 /var/log/cb/notifications/cb-notifications-watchlist-10.log
-rw-------. Jun  9 18:02 /var/log/cb/notifications/cb-notifications-feed-8.log
-rw-------. Jun  9 18:04 /var/log/cb/notifications/cb-notifications-binaryinfo.log
```

Syslog routing for all Carbon Black logs, including watchlist hits, is configurable by users via standard syslog configuration. See the Carbon Black Syslog Integration Guide for more detail.

Syslog Format

Each watchlist hit is a series of key value pairs. The keys present are different for binary and process watchlists.

Example - A process watchlist hit for watchlist 10 “TOR Nodes”:

```
Aug 12 15:00:03 [26070] <warning>  reason=watchlist.hit type=event process_guid=00000001-0
segment_id=1 host='SQLSRV-4' sensor_id=1 watchlist_id=10 watchlist_name='TOR Nodes' start_
group='Default Group' process_md5='a7fe32828ab2f76404cbb21f6dcad423' process_name='winscp.
process_path='c:\program files (x86)\winscp\winscp.exe' last_update='2014-08-12T18:47:50.6
alliance_updated_tor='2014-05-06T17:15:23Z' alliance_data_tor='['TOR-Node-38.229.70.52']'
alliance_link_tor='http://www.torproject.org'
```

Example - A binary watchlist hit on watchlist 11 “Interesting MD5”:

```
Aug 12 15:00:03 [26070] <warning>  reason=watchlist.hit type=module md5=B84E2D174DC84916A5
host='SQLSRV-4' sensor_id=1 watchlist_id=11 watchlist_name='Interesting MD5' first_seen='2
group=['Default Group'] desc='Windows Security Center ISV API' company_name='Microsoft Cor
product_name='Microsoft® Windows® Operating System' product_version='6.1.7600.16385'
file_version='6.1.7600.16385 (win7_rtm.090713-1255)' signed='Signed' alliance_updated_srst
alliance_score_srstrust='-100' alliance_data_srstrust='['b84e2d174dc84916a536572bb8f691a8'
alliance_link_srstrust='https://services.bit9.com/Services/extinfo.aspx?ak=b8b4e631d4884ad
```

Templates

Syslog output is formatted using Jinja2 templates. There is a command line utility at `/usr/share/cb/cbsyslog` to support:

```
# /usr/share/cb/cbsyslog --help
Usage: cbsyslog.py [options]

This utility provides an interface for testing Carbon Black's notifications
syslog output.

Options:
  -h, --help            show this help message and exit
  -v, --verbose         Provide more detailed output.
  -l, --list-events     When this option is specified, the tool will simply
                        output the list of events which can be sent to syslog
                        and exit
  -e EVENT_NAME, --event=EVENT_NAME
                        This option is required in order to identify the
                        specific event type that should be used. Use --list-
                        events option to get a list event names that can be
                        passed here
  -g, --get             Saves the system default templates to the current
                        directory.
  -t TEMPLATE, --template=TEMPLATE
                        Templates the syslog message using the specified
                        template instead of the system default.
  -f, --fire            Fires the syslog message through rsyslog.
  -q QUERY, --query=QUERY
                        Process the first document matching this query string.
```

Use the `--get` switch to write the system default templates to the local directory:

```
# /usr/share/cb/cbsyslog --get
# ll
-rw-rw-r--. 1 root root 246 May 22 00:16 binaryinfo.group.observed.template
-rw-rw-r--. 1 root root 285 May 22 00:16 binaryinfo.host.observed.template
-rw-rw-r--. 1 root root 221 May 22 00:16 binaryinfo.observed.template
-rw-rw-r--. 1 root root 194 May 22 00:16 feed.ingress.hit.binary.template
-rw-rw-r--. 1 root root 210 May 22 00:16 feed.ingress.hit.process.template
-rw-rw-r--. 1 root root 194 May 22 00:16 feed.storage.hit.binary.template
-rw-rw-r--. 1 root root 243 May 22 00:16 feed.storage.hit.process.template
-rw-rw-r--. 1 root root 575 May 22 00:16 watchlist.hit.binary.template
-rw-rw-r--. 1 root root 460 May 22 00:16 watchlist.hit.process.template
```

The templates are given a context with a single python dictionary called `doc` that contains the set of all possible key value pairs. To view the set of all possible keys, use the Jinja For loop to iterate over the keys in the doc with this template:

Create a 'forloop.txt' template with the following contents:

```
{% for k in doc %}{{k}}={{doc[k]}} {% endfor %}
```

Then use the `--template` switch to output all of the available keys for a specific event type:

```
# /usr/share/cb/cbsyslog --template ./forloop.txt --event watchlist.hit.process
process_md5=506708142bc63daba64f2d3ad1dcd5bf sensor_id=15 modload_count=45
filemod_count=0 servername=cbent-qa-nodesvr02 watchlist_id=-1
watchlist_name=SyslogTest id=1068044553602656801 group=SetSensor
hostname=CB-WIN81X64-01 last_update=2014-02-28T02:29:00.09Z
start=2014-02-28T02:29:00.043Z netconn_count=0 username=SYSTEM
process_name=googleupdate.exe path=c:\program files (x86)\google\update\googleupdate.exe
regmod_count=1 segment_id=1 host_type=workstation cb_version=4.1.1.140225.1913
childproc_count=0 unique_id=0ed274dc-ddc6-ea21-0000-000000000001
```

To get a list of available event types, use –list-events option:

```
[root@localhost mytemplates]# /usr/share/cb/cbsyslog --list-events
binaryinfo.group.observed
binaryinfo.host.observed
binaryinfo.observed
feed.ingress.hit.binary
feed.ingress.hit.process
feed.storage.hit.binary
feed.storage.hit.process
watchlist.hit.binary
watchlist.hit.process
```

Overriding the System Default Templates

After developing a new template, add one of the following entries to `/etc/cb/cb.conf` to use it:

```
BinaryInfoSyslogTemplateGroupObserved=/etc/cb/my_bininfo_group_observed_template.txt
BinaryInfoSyslogTemplateHostObserved=/etc/cb/my_bininfo_host_observed_template.txt
BinaryInfoSyslogTemplateObserved=/etc/cb/my_bininfo_observed_template.txt FeedIngressSyslo
FeedIngressSyslogTemplateProcess=/etc/cb/my_feed_ingress_process_template.txt
FeedStorageSyslogTemplateBinary=/etc/cb/my_feed_storage_binary_template.txt
FeedStorageSyslogTemplateProcess=/etc/cb/my_feed_storage_process_template.txt
WatchlistSyslogTemplateBinary=/etc/cb/my_wathlist_process_template.txt WatchlistSyslogTemp
```

The watchlist searcher process will automatically pick up the new template at the next watchlist hit.

Available Keys by Event Type

binaryinfo.observed

Key	Description	Example
md5	MD5 of the observed binary module	44C0CBADFF00F3930B6A0 1EEAA405C6F
scores	List of alliance feed scores that the binary is tagged with	[50, 100, 75]
watchlists	List of strings, each one identifying a watchlist that was matched with binary	[“x”, “a”]
event_timestamp	Event timestamp	1400695113.17

binaryinfo.group.observed

Same as binaryinfo.observed, plus:

Key	Description	Example
group	Name of the sensor group where binary was observed	Default Group

binaryinfo.host.observed

Same as binaryinfo.observed, plus:

Key	Description	Example
hostname	Name of the host endpoint where binary was observed	PANTHER
sensor_id	Sensor identifier of the endpoint where binary was observed	1

feed.ingress.hit.binary

Key	Description	Example
md5	MD5 of a binary module that triggered feed hit	44C0CBADFF00F3930B6A0 1EEAA405C6F
report_id	ID of the report that was matched	report_01
ioc_type	Type of the IOC that was matched	dns
ioc_value	IOC value that was matched	www.google.com
ioc_attr	Additional attributes on the IOC value that was matched	{port:80, protocol:tcp}
hostname	Hostname of the machine where feed hit was detected	PANTHER
sensor_id	Sensor ID of the endpoint	1
cb_version	Carbon Black Server version	4.1.0.140204.501
server_name	Name of Carbon Black server	cbserver

feed_id	ID of the feed that was matched	15
feed_name	Name of the feed that was matched	mdl
event_timestamp	Time of the event	1400695113.17

feed.storage.hit.binary

Key	Description	Example
md5	MD5 of a binary module that triggered feed hit	44C0CBADFF00F3930B6A0 1EEAA405C6F
report_id	ID of the report that was matched	report_01
ioc_type	Type of the IOC that was matched	dns
ioc_value	IOC value that was matched	www.google.com
ioc_attr	Additional attributes on the IOC value that was matched	{port:80, protocol:tcp}
hostname	Hostname of the machine where feed hit was detected	PANTHER
sensor_id	Sensor ID of the endpoint	1
cb_version	Carbon Black Server version	4.1.0.140204.501
server_name	Name of Carbon Black server	cbserver
feed_id	ID of the feed that was matched	15
feed_name	Name of the feed that was matched	mdl
event_timestamp	Time of the event	1400695113.17
copied_mod_len	Number of bytes collected.	73544
endpoint	Hostname and sensor id of the endpoint binary was first observed on	[PANTHER|2]
group	First sensor group this binary was observed on	[Default Group]
digsig_issuer	If digitally signed, the issuer.	VeriSign Class 3 Code Signing 2010 CA
digsig_publisher	If digitally signed, the publisher.	Google Inc
digsig_result	If digitally signed, the result. Contains one of the following eight possible values: Signed, Unsigned, Bad Signature, Invalid Signature, Expired, Invalid Chain, Untrusted Root, Explicit Distrust.	Signed
digsig_result_code	*internal use*	0
digsig_sign_time	If digitally signed, the time of signing.	2014-02-02T04:42:00Z
digsig_subject	If digitally signed, the subject.	Google Inc
is_executable_imag e	True if the binary is an EXE (versus DLL or SYS)	True
is_64bit	True if architecture is x64.	True
md5	MD5 of the process, the parent, a child process, a loaded module or written file.	44C0CBADFF00F3930B6A0 1EEAA405C6F

observed_filename	Full path to the executable backing this process.	c:\program files (x86)\google\chrome \application\wow_h elper.exe
orig_mod_len	Size in bytes of binary at time of collection.	73544
os_type	Operating System type of the host.	windows
server_added_times tamp	The time this binary was first seen by the server.	2014-02-04T07:50:56.9 17Z
server_name	Name of Carbon Black server	cbserver
watchlist_<id>	For each watchlist that matched this binary timestamp of match	'2014-02-04T07:55:03. 007Z'
file_version	File version version string from FILEVERSIONINFO	
product_name	Product name string from FILEVERSIONINFO	
company_name	Company name string from FILEVERSIONINFO	
internal_name	Internal name string from FILEVERSIONINFO	
original_filename	Original name string from FILEVERSIONINFO	
file_desc	File description string from FILEVERSIONINFO	
product_desc	Product description string from FILEVERSIONINFO	
comments	Comment string from FILEVERSIONINFO	
legal_copyright	Legal copyright string from FILEVERSIONINFO	
legal_trademark	Legal trademark string from FILEVERSIONINFO	
private_build	Private build string from FILEVERSIONINFO	
special_build	Special build string from FILEVERSIONINFO	
product_version	Product name string from FILEVERSIONINFO	

feed.ingress.hit.process

Key	Description	Example
process_id	Process document identifier	6012886846294712642
report_id	ID of the report that was matched	report_01
ioc_type	Type of the IOC that was matched	dns
ioc_value	IOC value that was matched	www.google.com
ioc_attr	Additional attributes on the IOC value that was matched	{port:80, protocol:tcp}
hostname	Hostname of the machine where feed hit was detected	PANTHER
sensor_id	Sensor ID of the endpoint	1

cb_version	Carbon Black Server version	4.1.0.140204.501
server_name	Name of Carbon Black server	cbserver
feed_id	ID of the feed that was matched	15
feed_name	Name of the feed that was matched	mdl
event_timestamp	Time of the event	1400695113.17

feed.storage.hit.process

Key	Description	Example
process_id	Process document identifier	6012886846294712642
segment_id	Process document segment identifier	1
report_id	ID of the report that was matched	report_01
ioc_type	Type of the IOC that was matched	dns
ioc_value	IOC value that was matched	www.google.com
ioc_attr	Additional attributes on the IOC value that was matched	{port:80, protocol:tcp}
hostname	Hostname of the machine where feed hit was detected	PANTHER
sensor_id	Sensor ID of the endpoint	1
cb_version	Carbon Black Server version	4.1.0.140204.501
server_name	Name of Carbon Black server	cbserver
feed_id	ID of the feed that was matched	15
feed_name	Name of the feed that was matched	mdl
event_timestamp	Time of the event	1400695113.17
childproc_count	Total count of child processes created by this process.	0
cmdline	Process command line	“c:\net.exe” /user
filemod_count	Total count of file mods by this process.	0
group	Sensor group this sensor was assigned to, at the time of process execution.	Default Group
host_type	Type of the computer: workstation, server, or domain controller.	server
last_update	Last activity in this process in computer’s local time.	2014-02-04T16:23:22.5 47Z
modload_count	Total count of module loads by this process.	45
netconn_count	Total count of network connections by this process.	0
os_type	Operating System type of the host.	windows
parent_name	Name of parent process.	svchost.exe

parent_md5	MD5 of the parent process.	506708142bc63daba64f2 d3ad1dcd5bf
parent_pid	Parent process pid.	2532
parent_unique_id	Parent process unique Id.	68d37769-03b8-6cfa-00 00-000000000001
path	Full path to the executable backing this process.	c:\program files (x86)\google\update \googleupdate.exe
process_md5	MD5 of the executable backing this process.	506708142bc63daba64f2 d3ad1dcd5bf
process_name	Filename of the executable backing this process.	googleupdate.exe
process_pid	Process pid	44988
regmod_count	Total count of registry mods by this process.	0
start	Start time of this process in computer's local time.	2014-02-04T16:23:22.5 16Z
unique_id	Process unique Id	68d37769-03b8-6cfa-00 00-000000000001
username	User context the process executed with.	SYSTEM
watchlist_id	Watchlist that matched (-1 is the internal syslog test)	-1
watchlist_name	Name of watchlist that matched	SyslogTest

watchlist.hit.process

Key	Description	Example
cb_version	Carbon Black Server version	4.1.0.140204.501
childproc_count	Total count of child processes created by this process.	0
cmdline	Process command line	"c:\net.exe" /user
filemod_count	Total count of file mods by this process.	0
group	Sensor group this sensor was assigned to, at the time of process execution.	Default Group
host_type	Type of the computer: workstation, server, or domain controller.	server
hostname	Hostname of the computer the process executed on.	PANTHER
id	*internal use*	7553512292948143354
last_update	Last activity in this process in computer's local time.	2014-02-04T16:23:22.5 47Z
modload_count	Total count of module loads by this process.	45
netconn_count	Total count of network connections by this process.	0
os_type	Operating System type of the host	windows

parent_unique_id	Parent process unique Id	68d37769-03b8-6cfa-00 00-000000000001
path	Full path to the executable backing this process.	c:\program files (x86)\google\update \googleupdate.exe
process_md5	MD5 of the executable backing this process.	506708142bc63daba64f2 d3ad1dcd5bf
parent_pid	Parent process pid	2532
process_name	Filename of the executable backing this process.	googleupdate.exe
process_pid	Process pid	44988
regmod_count	Total count of registry mods by this process.	0
segment_id	*internal use*	1
sensor_id	The internal Carbon Black sensor guid of the computer this process executed on.	6
server_name	Name of Carbon Black server	cbserver
start	Start time of this process in computer's local time.	2014-02-04T16:23:22.5 16Z
unique_id	Process unique Id	68d37769-03b8-6cfa-00 00-000000000001
username	User context the process executed with.	SYSTEM
watchlist_id	Watchlist that matched (-1 is the internal syslog test)	-1
watchlist_name	Name of watchlist that matched	SyslogTest

watchlist.hit.binary

Key	Description	Example
cb_version	Carbon Black Server version	4.1.0.140204.501
copied_mod_len	Number of bytes collected.	73544
endpoint	Hostname and sensor id of the endpoint binary was first observed on	[PANTHER|2]
group	First sensor group this binary was observed on	[Default Group]
digsig_issuer	If digitally signed, the issuer.	VeriSign Class 3 Code Signing 2010 CA
digsig_publisher	If digitally signed, the publisher.	Google Inc
digsig_result	If digitally signed, the result. Contains one of the following eight possible values: Signed, Unsigned, Bad Signature, Invalid Signature, Expired, Invalid Chain, Untrusted Root, Explicit Distrust.	Signed
digsig_result_code	*internal use*	0
digsig_sign_time	If digitally signed, the time of signing.	2014-02-02T04:42:00Z

digsig_subject	If digitally signed, the subject.	Google Inc
is_executable_imag e	True if the binary is an EXE (versus DLL or SYS)	True
is_64bit	True if architecture is x64.	True
md5	MD5 of the process, the parent, a child process, a loaded module or written file.	44C0CBADFF00F3930B6A0 1EEAA405C6F
observed_filename	Full path to the executable backing this process.	c:\program files (x86)\google\chrome \application\wow_h elper.exe
orig_mod_len	Size in bytes of binary at time of collection.	73544
os_type	Operating System type of the host.	windows
server_added_times tamp	The time this binary was first seen by the server.	2014-02-04T07:50:56.9 17Z
server_name	Name of Carbon Black server	cbserver
signed	*internal use*	Signed
timestamp	Time binary was seen	2014-02-04T07:50:56.9 17Z
watchlist_name	Name of watchlist that matched this binary	SyslogTest
watchlists	All Watchlists that matched this binary	[{‘wid’: ‘5’, ‘value’: ‘2014-02-04T07:55:03. 007Z’}]
file_version	File version version string from FILEVERSIONINFO	
product_name	Product name string from FILEVERSIONINFO	
company_name	Company name string from FILEVERSIONINFO	
internal_name	Internal name string from FILEVERSIONINFO	
original_filename	Original name string from FILEVERSIONINFO	
file_desc	File description string from FILEVERSIONINFO	
product_desc	Product description string from FILEVERSIONINFO	
comments	Comment string from FILEVERSIONINFO	
legal_copyright	Legal copyright string from FILEVERSIONINFO	
legal_trademark	Legal trademark string from FILEVERSIONINFO	
private_build	Private build string from FILEVERSIONINFO	
special_build	Special build string from FILEVERSIONINFO	
product_version	Product name string from FILEVERSIONINFO	