Syslog User Guide

CB v4.2.5.150311.1434

March 11, 2015

Contents

Carbon Black Syslog User Guide

Purpose

The purpose of this document is to describe how Carbon Black events can be accessed via syslog.

For documentation on customizing the format of Carbon Black syslog events, please see the Carbon Black Syslog Template Developer Guide. For documentation on integrating with external platforms, see the Carbon Black Syslog Integration Guide.

Background

Carbon Black logs all Watchlist and Feed hits 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.

For example, the directory listing below contains three log files: one for all watchlist and feed hits, another for just hits to watchlist id 10 and another for just hits to feed id 8:

```
[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
```

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

Each feed hit is a series of key value pairs. By default a feed hit is logged only at the ingress, as the events arrive at the Carbon Black server. Optionally (when enabled via the `EnableSolrFeedNotifications` configuration option in `/etc/cb/cb.conf`), the feed hit is also logged when committed to persistent storage. In the latter case, the notification may contain additional key value pairs on the binary or process.

The keys present are different for binary and process feeds.

Example - A process ingress feed hit on feed 10 “tor”:

```
Aug 12 14:24:19 [26070] <warning>  reason=feed.ingress.hit type=event process_guid=0000000
host=’SERV12R2X64-01’ sensor_id=1 feed_id=10 feed_name=’tor’ ioc_type=’ipv4’ ioc_value=’38
protocol=’TCP’ port=’22’ timestamp=’1407867859.64’
```

Example - A process storage feed hit on feed 10 “tor”:

```
Aug 12 14:26:10 [26070] <warning>  reason=feed.storage.hit type=event process_guid=0000000
segment_id=1 host=’SERV12R2X64-01’ sensor_id=1 feed_id=10 feed_name=’tor’ ioc_type=’ipv4’
direction=’Outbound’ protocol=’TCP’ port=’22’ timestamp=’1407867970.49’ start_time=’2014-0
group=’Default Group’ process_md5=’a3ccfd0aa0b17fd23aa9fd0d84b86c05’ process_name=’putty.e
process_path=’c:\users\gakkor\desktop\putty.exe’ last_update=’2014-08-12T18:23:55.415Z’ al
alliance_score_tor=’0’ alliance_updated_tor=’2014-05-06T17:15:23.000Z’ alliance_data_tor=’
```

Example - A binary ingress feed hit on feed 2 “srstrust”

```
Aug 12 14:06:39 [26070] <warning>  reason=feed.ingress.hit type=module md5=B84E2D174DC8491
host=’SERV12R2X64-01’ sensor_id=1 feed_id=2 feed_name=’srstrust’ ioc_type=’md5’ ioc_value=
timestamp=’1407866781.79’
```

Example - A binary storage feed hit on feed 2 “srstrust”

```
Aug 12 14:06:39 [26070] <warning>  reason=feed.storage.hit type=module md5=B84E2D174DC8491
host=’SERV12R2X64-01’ sensor_id=1 feed_id=2 feed_name=’srstrust’ ioc_type=’md5’ ioc_value=
timestamp=’1407866797.20’ first_seen=’2014-08-12T18:06:22.190Z’ group=[’Default Group’] de
company_name=’Microsoft Corporation’ product_name=’MicrosoftÂ® WindowsÂ® Operating System
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
```

Syslog Format Details - Process Watchlists

This is the default Process template that produces the process watchlist hit for watchlist 10 above.

```
reason=watchlist.hit type=event process_guid={{doc['id']}} segment_id={{doc["segment_id"]}
sensor_id={{doc['sensor_id']}} watchlist_id={{doc['watchlist_id']}} watchlist_name='{{doc[
timestamp='{{doc['event_timestamp']}}' start_time='{{doc['start']}}' group='{{doc['group']
process_name='{{doc['process_name']}}' process_path='{{doc['path']}}' last_update='{{doc['
{% for k in doc %}{% if k.startswith("alliance_") %} {{k}}='{{doc[k]}}'{% endif %}{% endfor
```

Table of Process Watchlist key pairs and description.

Syslog label	doc reference	Description
reason	no doc reference	Text that describes the entry
type=event	no doc reference	This is text that describes the syslog entry
process_guid=	id	Process doc identifier
segment_id=	segment_id	Process doc segment identifier
host=	hostname	Hostname of the computer the process executed on.
sensor_id=	sensor_id	Sensor id of the computer the process executed on.
watchlist_id=	watchlist_id	Watchlist that matched (-1 is the internal syslog test)
watchlist_name=	watchlist_name	Name of watchlist that matched
timestamp=	event_timestamp	Epoch time of the wathclist hit event
start_time=	start	Start time of this process in computer's local time.
group=	group	Sensor group this sensor was assigned to, at the time of process execution.
process_md5=	process_md5	MD5 of the executable backing this process.
process_name=	process_name	Filename of the executable backing this process.
process_path=	path	Full path to the executable backing this process.
last_update=	last_update	Last activity in this process in computer's local time.
for if loops	*internal use*	required on process templates

Syslog Format Details - Binary Watchlists

This is the default Binary template that produces the binary watchlist hit for watchlist 11 above.

```
reason=watchlist.hit type=module md5={{doc["md5"]}} host='{{doc.get('hostname')}}' sensor_
watchlist_id={{doc['watchlist_id']}} watchlist_name='{{doc['watchlist_name']}}' timestamp=
first_seen='{{doc["server_added_timestamp"]}}' group={{doc["group"]}} desc='{{doc["file_de
company_name='{{doc["company_name"]}}' product_name='{{doc["product_name"]}}' product_vers
```

```
file_version='{{doc["file_version"]}}' signed='{{doc["signed"]}}'{% for k in doc %}{% if k
{{k}}='{{doc[k]}}'{% endif %}{% endfor %}
```

Table of Binary Watchlist key pairs and description.

Syslog label	doc reference	Description
reason	no doc reference	Text that describes the syslog entry
type=module	no doc reference	This is text that describes the syslog entry
md5=	md5	MD5 of the process, the parent, a child process, a loaded module or written file.
host=	hostname	Hostname of the computer the binary was observed
sensor_id=	sensor_id	Sensor id of the computer the binary was observed
watchlist_id=	watchlist_id	Watchlist that matched (-1 is the internal syslog test)
watchlist_name=	watchlist_name	Name of watchlist that matched
timestamp=	event_timestamp	Epoch time of the wathclist hit event
first_seen=	server_added_ timestamp	The time this binary was first seen by the server.
group=	group	First sensor group this binary was observed on
desc=	file_desc	File description string from FILEVERSIONINFO
company_name=	company_name	Company name string from FILEVERSIONINFO
product_name=	product_name	Product name string from FILEVERSIONINFO
product_version=	product_version	Product name string from FILEVERSIONINFO
file_version=	file_version	File version version string from FILEVERSIONINFO
signed=	signed	Digital signature status of the binary
for if loops	*internal use*	required on binary templates

Syslog Format Details - Ingress Process Feed hit

This is the default ingress process feed template that produces the process feed hit for feed 10 above

```
reason=feed.ingress.hit type=event process_guid={{doc['process_id']}} host='{{doc['hostnam
feed_id={{doc['feed_id']}} feed_name='{{doc['feed_name']}}' ioc_type='{{doc['ioc_type']}}'
{% for k in doc['ioc_attr'] %} {{k}}='{{doc['ioc_attr'][k]}}'{% endfor %} timestamp='{{doc
```

Table of Ingress Process Feed key pairs and description.

Syslog label	doc reference	Description
reason	no doc reference	Text that describes the syslog entry
type=event	no doc reference	This is text that describes the syslog entry
process_guid=	process_id	Process doc identifier
host=	hostname	Hostname of the machine where feed hit was detected
sensor_id=	sensor_id	Sensor ID of endpoint that 'saw' feed hit
feed_id=	feed_id	ID of the feed that that was matched
feed_name=	feed_name	Name of the feed that that was matched
ioc_type=	ioc_type	Type of the indicator that caused the hit
ioc_value=	ioc_value	Value of the indicator that matched
for if loops	ioc_attr	Optional attributes on the hit (if present)
timestamp=	event_timestamp	Epoch time of the feed hit event

Syslog Format Details - Storage Process Feed hit

This is the default storage process feed template that produces the process feed hit for feed 10 above

```
reason=feed.storage.hit type=event process_guid={{doc['process_id']}} segment_id={{doc['se
host='{{doc['hostname']}}' sensor_id={{doc['sensor_id']}} feed_id={{doc['feed_id']}} feed_
ioc_type='{{doc['ioc_type']}}' ioc_value='{{doc['ioc_value']}}'{% for k in doc['ioc_attr']
timestamp='{{doc['event_timestamp']}}' start_time='{{doc['start']}}' group='{{doc['group']
process_md5='{{doc['process_md5']}}' process_name='{{doc['process_name']}}' process_path='
last_update='{{doc['last_update']}}'{% for k in doc %}{% if k.startswith("alliance_") %} {
```

Table of Storage Process Feed key pairs and description.

Syslog label	doc reference	Description
reason	no doc reference	Text that describes the syslog entry
type=event	no doc reference	This is text that describes the syslog entry
process_guid=	process_id	Process doc identifier
segment_id=	segment_id	Process doc segment identifier
host=	hostname	Hostname of the machine where feed hit was detected
sensor_id=	sensor_id	Sensor ID of endpoint that 'saw' feed hit
feed_id=	feed_id	ID of the feed that that was matched
feed_name=	feed_name	Name of the feed that that was matched

ioc_type=	ioc_type	Type of the indicator that caused the hit
ioc_value=	ioc_value	Value of the indicator that matched
for if loops	ioc_attr	Optional attributes on the hit (if present)
timestamp=	event_timestamp	Epoch time of the feed hit event
start_time=	start	Start time of this process in computer's local time.
group=	group	Sensor group this sensor was assigned to, at the time of process execution.
process_md5=	process_md5	MD5 of the executable backing this process.
process_name=	process_name	Filename of the executable backing this process.
process_path=	path	Full path to the executable backing this process.
last_update=	last_update	Last activity in this process in computer's local time.
for if loops	*internal use*	required on process templates

Syslog Format Details - Ingress Binary Feed hit

This is the default ingress binary feed template that produces the binary feed hit from feed 2 above

```
reason=feed.ingress.hit type=module md5={{doc['md5']}} host='{{doc['hostname']}}' sensor_i
feed_id={{doc['feed_id']}} feed_name='{{doc['feed_name']}}' ioc_type='{{doc['ioc_type']}}'
'{% for k in doc['ioc_attr'] %} {{k}}='{{doc['ioc_attr'][k]}}'{% endfor %} timestamp='{{doc
```

Table of Ingress Binary Feed key pairs and description.

Syslog label	doc reference	Description
reason	no doc reference	Text that describes the entry
md5=	md5	MD5 of the process, the parent, a child process, a loaded module or written file.
host=	hostname	Hostname of the machine where feed hit was detected
sensor_id=	sensor_id	Sensor ID of endpoint that 'saw' feed hit
feed_id=	feed_id	ID of the feed that that was matched
feed_name=	feed_name	Name of the feed that that was matched
ioc_type=	ioc_type	Type of the indicator that caused the hit
ioc_value=	ioc_value	Value of the indicator that matched
for if loops	ioc_attr	Optional attributes on the hit (if present)
timestamp=	event_timestamp	Epoch time of the feed hit event

Syslog Format Details - Storage Binary Feed hit

This is the default storage binary feed template that produces the binary feed hit from feed 2 above

```
reason=feed.storage.hit type=module md5={{doc['md5']}} host='{{doc['hostname']}}' sensor_i
feed_id={{doc['feed_id']}} feed_name='{{doc['feed_name']}}' ioc_type='{{doc['ioc_type']}}'
'{% for k in doc['ioc_attr'] %} {{k}}='{{doc['ioc_attr'][k]}}'{% endfor %} timestamp='{{doc
first_seen='{{doc["server_added_timestamp"]}}' group={{doc["group"]}} desc='{{doc["file_de
company_name='{{doc["company_name"]}}' product_name='{{doc["product_name"]}}'
product_version='{{doc["product_version"]}}' file_version='{{doc["file_version"]}}'
signed='{{doc["digsig_result"]}}'{% for k in doc %}{% if k.startswith("alliance_") %}
{{k}}='{{doc[k]}}'{% endif %}{% endfor %}
```

Table of Storage Binary Feed key pairs and description.

Syslog label	doc reference	Description
reason	no doc reference	Text that describes the entry
md5=	md5	MD5 of the process, the parent, a child process, a loaded module or written file.
host=	hostname	Hostname of the machine where feed hit was detected
sensor_id=	sensor_id	Sensor ID of endpoint that 'saw' feed hit
feed_id=	feed_id	ID of the feed that that was matched
feed_name=	feed_name	Name of the feed that that was matched
ioc_type=	ioc_type	Type of the indicator that caused the hit
ioc_value=	ioc_value	Value of the indicator that matched
for if loops	ioc_attr	Optional attributes on the hit (if present)
timestamp=	event_timestamp	Epoch time of the feed hit event
first_seen=	server_added_ timestamp	The time this binary was first seen by the server.
group=	group	First sensor group this binary was observed on
desc=	file_desc	File description string from FILEVERSIONINFO
company_name=	company_name	Company name string from FILEVERSIONINFO
product_name=	product_name	Product name string from FILEVERSIONINFO
product_version=	product_version	Product name string from FILEVERSIONINFO
file_version=	file_version	File version version string from FILEVERSIONINFO
signed=	digsig_result	Digital signature status of the binary
for if loops	*internal use*	required on binary templates