Server Predefined Watchlists

CB v4.2.5.150311.1434

March 11, 2015

Contents

Overview

This document describes how to add custom watchlists at server setup time, including how to specify watchlist ids.

Background & Purpose

Carbon Black Enterprise Server ships with a series of predefined watchlists. These “out of the box” watchlists are added to the Server configuration at server initialization time. Server initialization is accomplished by running cbinit.

Each watchlist is assigned a unique numeric incrementing id, starting with id 1. This id is used to “tag” process and binary documents on watchlist match. The id is also present in the default syslog output on watchlist match.

There may be reason to desire to control the id. The steps required to do this are documented here.

Step-by-Step Guide

1. All steps must be accomplished prior to running cbinit
2. Add one or more watchlist configuration files to /usr/share/cb/setup/watchlists. Watchlist configuration files are described below. Watchlist configuration files must have the .conf extension.
3. Configure a specific id for any watchlists that require it.
4. Configure ‘readonly’ mode for any watchlists that require it. Readonly mode is described below.
5. Run cbinit as per standard procedure.

Watchlist Configuration Files

Watchlist configuration files are standard configuration files with two sections:

1. [global]
2. [search_query]

The [global] section is used to specify general properties of the watchlist. There are four valid properties:

name The name of the watchlist. This does not have to be unique across watchlists, although for ease of use it should be so. The name is case-preserving and may include spaces.

This field is REQUIRED.

index_type The core SOLR index to be searched. Valid values are:

1. events
2. modules

Events corresponds to a process watchlist; modules corresponds to a binary watchlist.

This field is REQUIRED.

readonly When set to 'true', the UI restricts modification or deletion of the watchlist. The watchlist can still be modified or deleted via the Carbon Black API, but the UI disables all modifications and deletions. This disabling applies even to global administrators. The default value is 'false'.

This field is OPTIONAL.

id When set, this is the unique identifier of the watchlist. Ids must not be duplicated in multiple watchlist configuration files. The id is present in any tagged documents, and is also present in the default syslog output on watchlist hits. Likewise, searches can be performed based on the id of the watchlist.

This field is OPTIONAL.

The [search_query] section is used to specify the search criteria used for the watchlist. There are two valid properties:

cb.urlver Must be present and must be set to 1.

This field is REQUIRED.

q This is the query string. For details, please see the Carbon Black Query Parser documentation, or see the examples below.

This field is REQUIRED.

Example Watchlist Configuration Files

Read-only Process Watchlist [global] name=Filemods to Webroot index_type=events readonly=true

[search_query] cb.urlver=1 q=filemod:"\example\directory"

Read-only Binary Watchlist With Fixed Id [global] name=Filemods to Webroot index_type=modules read-only=true

[search_query] cb.urlver=1 q=is_executable_image:true