Script for basic configuration capture from bash CLI
Version: Level 002, v 00.09.01 and later

This is a script for execution at the bash CLI expert shell level, while not connected to Gaia web UI, that creates a set of output files with basic configuration data about the system where it is run, either management (SMS or MDM) or gateway. The script uses basic bash shell and Gaia clish commands to harvest data that may be relevant for later use in restoring configuration or duplicating setup.

There is no claim this information collected is complete for a restore, but is a work in progress, and may improve in the future to add more information.

This script does not replace important disaster recovery operations like Check Point Snapshot, Check Point Backup, Check Point Migrate (migrate export/import), or mds_backup; but augments the collection of data for easy re-use, documentation, or configuration check.

This script and others are located and updated regularly on GitHub under the main Check Point Gaia Bash scripts efforts.

Check Point Gaia Bash scripts repository:
GitHub - mybasementcloud/check_point_gaia_bash_scripts: Various bash scripts for Check Point Software Technologies Gaia …

Direct link to configuration capture script and history:
check_point_gaia_bash_scripts/config_capture at master · mybasementcloud/check_point_gaia_bash_scripts · GitHub

This script has been tested and utilized with Check Point releases R77, R77.30, R80, R80.10, and R80.20 [EA] with no difference in operation based on Jumbo Hotfix Implementation or Gaia kernel version. It works on Security Management Server (SMS), Log Servers, SmartEvent Servers, Multi-Domain Management (DMD) Multi-Domain Servers (MDS), Endpoint Security Servers (EPMS), and Gateways.

The script creates a number of files and also will create a set of file folders and subfolders in the folder [directory] where it is executed.
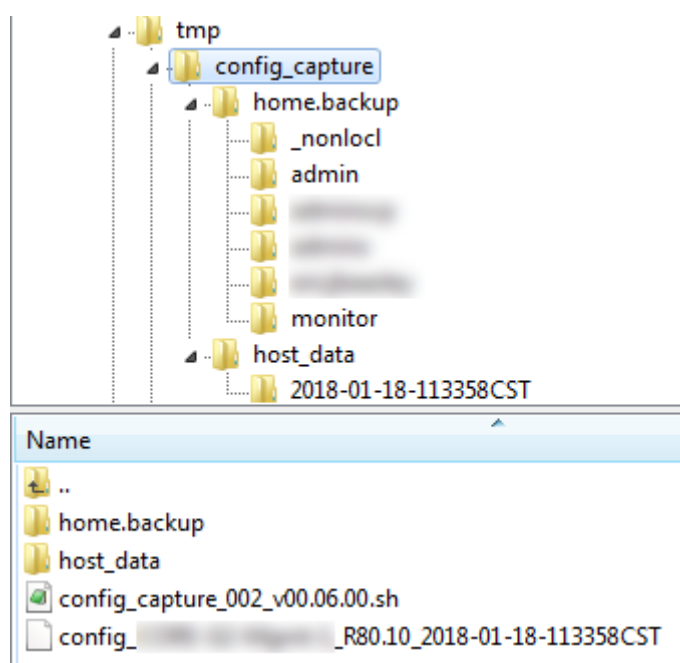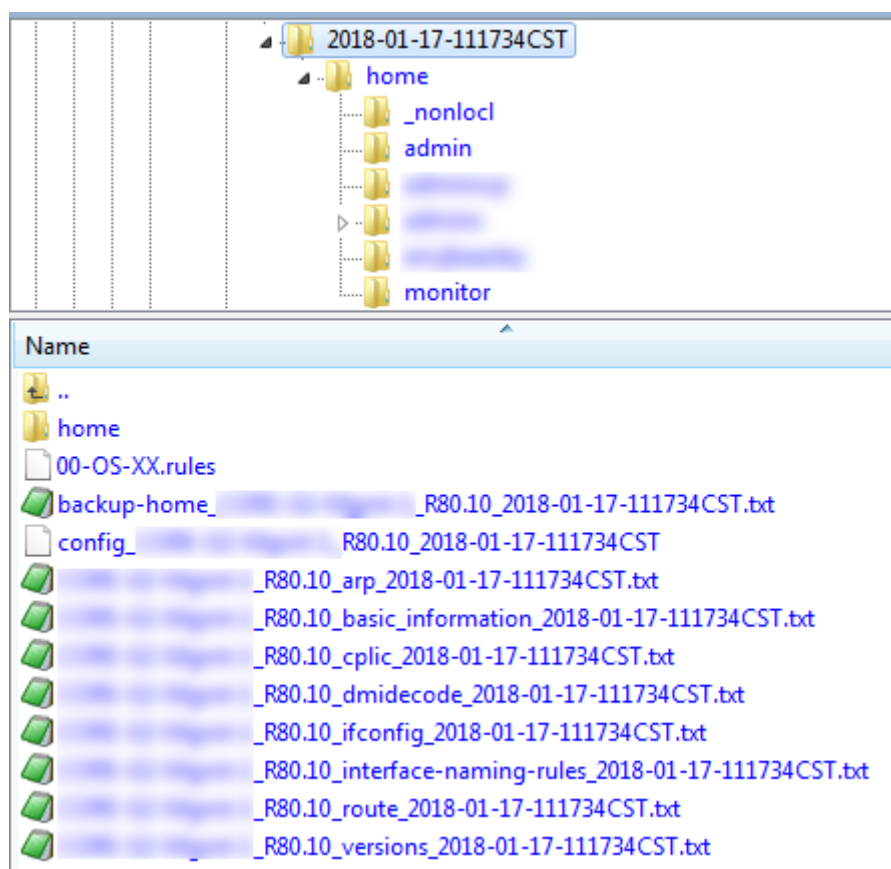

Example from an SMS

The script now accounts for whether it is run from a folder under /home/, such that it then generates the content in /var/tmp/ instead and should not fail or have issues with recursive copies like in version prior to v00.09.01.

It is still highly recommended to create a working folder set under /var/ for custom scripting operations.

Folders created:

- Folder "home.backup": this folder will contain a copy of the home folders content for recovery and backup, which is useful if there have been customizations made to those files. This folder is updated with the contents from the home folder each time the script is executed [from the same location]

- Folder "host_data": this folder is the primary repository for the data collected during execution, and also will include it's own copy of the home folders

    o Date-Time-Group folder for execution time results, based on YYYY-MM-DD-Time format with 24 hour time (Hour-Minute-Second) and time zone, for easy sorting and review.

        ▪ "home" folder for at time copy of executing user's home folder

host_data folder content:

Example from an SMS

This folder contains the sub-folder based on the execution time and date, represented by a Date-Time-Group named folder. The content of that Date-Time-Group folder is a folder for the executing user's home folder at time of execution, and the following files:

Script for basic configuration capture from bash CLI

Additional management data was added to document running management processes. This executes for Security Management Server, SmartEvent, Log Server, Multi-Domain Management Server, and Endpoint Security Management Server.

- o 00-OS-XX.rules
  This file is a copy of the 00-OS-XX.rules file located in "/etc/udev/rules.d/", that contains information about the interface names associated to a physical interface. This is useful for OpenServers, where adding hardware can change the association based on how the underlying Linux OS sees the interfaces from a hardware perspective, so having this original data can help restore configuration.

- o backup-home_yourhostname_<gaia-os-version>_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of the home folder copy operations and results.

- o config_yourhostname_<gaia-os-version>_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>
  Gaia clish configuration at time of execution. Useful to rebuild the system or for information that can be used in copy-paste operations for re-using settings easily via script.

- o yourhostname_<gaia-os-version>_arp_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of the current arp table at bash.

- o yourhostname_<gaia-os-version>_basic_information_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>T.txt
  Basic system information like current memory and disk utilization. This information may expand in future versions.

- o yourhostname_<gaia-os-version>_cplic_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of the Check Point licensing information at time of execution.

- o yourhostname_<gaia-os-version>_dmidecode_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of the dmidecode information at time of execution.

- o yourhostname_<gaia-os-version>_fwaccel-statistics_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of SecurXL statistics and information, useful to check if acceleration is impacted by rule based or if there are interesting trends or issues.

- o yourhostname_<gaia-os-version>_ifconfig_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of bash interface configuration.

- o yourhostname_<gaia-os-version>_interface-naming-rules_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of interface naming rules found in "/etc/udev/rules.d/00-OS-XX.rules" as an addition to the copied file.

- o yourhostname_<gaia-os-version>_route_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of bash level route information.

Script for basic configuration capture from bash CLI

- o yourhostname_<gaia-os-version>_versions_<date-time-group-of-execution_YYYY-MM-DD-HHMMSSTZ>.txt
  Dump of current version information from the different potential version sources for the installed system.

Future releases may update or change the information above, and the best source for the most current version is on GitHub:
check_point_gaia_bash_scripts/config_capture at master · mybasementcloud/check_point_gaia_bash_scripts · GitHub

This script contents and documentation is provided without any implied or expressed acceptance of liability, risk, or support; use is at the user's own risk.

For additional scripts and helpful Check Point administration tools, check out the root GitHub for Eric Beasley's MyBasementCloud at:

https://github.com/mybasementcloud?tab=repositories

Revision History:

Level 002 :

V 00.09.00   Updated approach to handling /home location as start of script and some related operations for attempting to address a problem with executing script if anyone has the Gaia web UI open, locking clish database. Expanded some collection of management data

V 00.07.00   Correct handling of "realpath" approach to work with pre-R80.10 new Kernel, which does not include the actual "realpath" executable, so can't perform the function.

V 00.06.00   Updated approach to handling "home" folders to capture all users' home folders versus just executing administrator. Also updated path handling to utilize "realpath" for the actual destination path to ensure that directory specific operations were correct.