Building a Zero-Touch VM appliance

Author: Richard Devera
Reviewer: Matthew Krattenmaker
Version: 0.9

Prerequisite

- Knowledge of CentOS
- Command-line Linux
- mkfs.vfat or dosfstools installed in CentOS
- Assumes virtual network assignment and IP address is 10.1.1.0/24

Motivation:

Partner has a need to build VM appliances quickly and duplicated on-demand from the POC data center. Most installations are done manually or preconfigured a completed installation as an OVA/OVF and copied as needed (current method).

The current method has a few limitations:

1. The licenses must be current and requires manual installation when out of licenses are expired.

2. Modifications to the VM's require manual installation and changes need to be done manually to keep versions up to date.

This document outlines different methods for creating an unattended, hands-free installation. The document is still in work, but is the first step to creating a baseline.

Steps:

Summary of the steps used to install a custom Check Point VM appliance using preconfigured configuration files.

1. Install GAIA automatically via config file
2. Configure the appliance from the CLI using config_system
3. Use the Check Point API to install rules

During a normal software DVD installation, the installation requires manual entry of basic networking and disk partitions information which is requested prior to installing the packages. The example file below, gaia.conf, is read by the OS during the initial installation as a file mounted on a floppy drive. The file gaia.conf contains parameters (see table below) that populates the required parameters to complete the package

installation. A floppy drive image is required to be built and the shell script, (see mk_floppy_img script).

Example Configuration

```
Interface:eth0
IP:10.1.1.254
Mask:255.255.255.0
Route:10.1.1.1
DHCP:0
lv_log:20000
lv_current:10000
atEnd:shutdown
```

Figure 1 – gaia.conf

Table 1 - Floppy Configuration Keywords

Key Word	Description	Example	Notes
Interface	Configured Interface name	`Interface:eth0`	Mandatory
IP	Interface IP	`IP:192.168.1.1`	Mandatory
Mask	Interface network Mask	`Mask:255.255.255.0`	Mandatory
Route	Default network route address	`Route:192.168.1.254`	Mandatory
DHCP	Interface requires DHCP	`DHCP:0`	Optional: 0=disable, 1=enable
lv_log	Set the size of the log file	`lv_log:20000`	Optional: size in MB
lv_current	Set the size of the root partition	`Lv_current:10000`	Optional: size in MB
atEnd	What to do at the end of the installtion	`atEnd:waitforkey`	Optional Options: • **reboot** – reboot at the end • **waitforkey** – stop on last screen • **shutdown** – shutdown at end ***(Default setting)***

A Install GAIA automatically via config file

Useful tips during installation (Credit https://wiki.centos.org/TipsAndTricks/KickStart)

Alt-F1

The installation dialog when using text or cmdline
Alt-F2
A shell prompt
Alt-F3
The install log displaying messages from install program
Alt-F4
The system log displaying messages from kernel, etc.
Alt-F5
All other messages
Alt-F7
The installation dialog when using the graphical installer

A floppy drive must be created to build a no-touch GAIA installation this can be down several different ways, this document will create a floppy image through VMworkstation and CentOS. A scriptfile is included in this document if scripting is required.

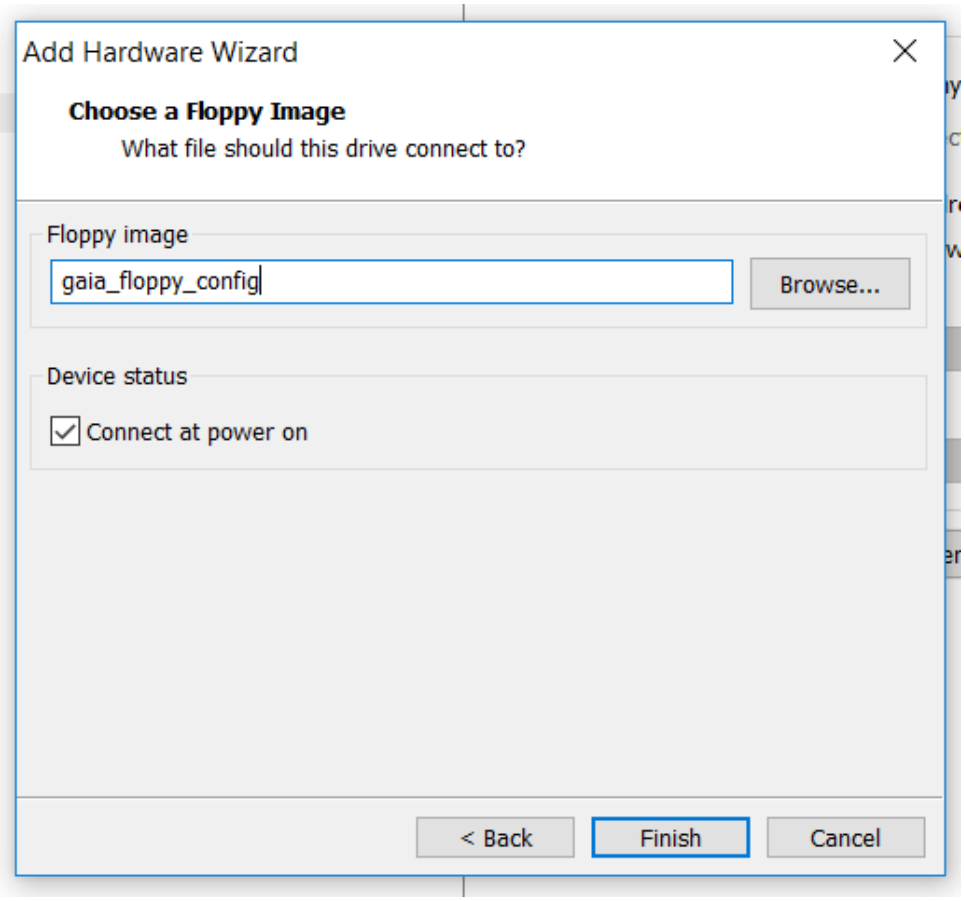
There are two methods in creating a Floppy Image

- Create using VMware Workstation
- Create using the script in Figure 1 - Floppy Image Script File (mk_floppy_img.sh)
- Create using software (ie magiciso)

Steps for Using VMware Workstation

1. Assuming you have Centos running
2. Under the Virtual Machine settings, Add a Floppy Drive to the Virtual Machine

3. Choose “Create a blank floppy image”
4. Save the image as gaia_floppy_config



5. Boot Centos appliance
6. The next steps require dosfstools to be installed.
7. Verify floppy drive installed on /dev/fd0
    a. dmesg | grep Floppy
    b. In this example the output is /dev/fd0

```
[root@localhost ~]# dmesg | grep Floppy
[    4.693633] Floppy drive(s): fd0 is 1.44M
[root@localhost ~]#
```

8. Make a new “vfat” filesystem the floppy drive
    a. /sbin/mkfs.vfat /dev/fd0

9. Mount the floppy drive
    a. mkdir /mnt/floppy
    b. mount –t vfat –o rw /dev/fd0 /mnt/floppy

10. Create and edit the file gaia.conf
    a. vi /mnt/floppy/gaia.conf
    b. Add the following configuration parameters found in **Error! Reference source not found.**
    c. Save and unmount the file system
        i. umount /dev/fd0

Examples if creating using a script file.

A. Create a shell script in CentOS show below Figure 1 - Floppy Image Script File (mk_floppy_img.sh)

```
#!/bin/bash
# Create floppy disk

mount_point="/tmp/floppy_image"
image_name="/tmp/floppy.flp"
configuration_file="gaia.conf"
fs_type="vfat"

if [ ! -d $mount_point ]
then
     mkdir  $mount_point
fi
/sbin/mkfs.fat -C $image_name 1440
mount -o loop -t $fs_type $image_name $mount_point
# Add content to image
cat > ${mount_point}/${configuration_file} <<EOF
Interface:eth0
IP:192.168.1.1
Mask:255.255.255.0
Route:192.168.1.254
DHCP:0
lv_log:20000
lv_current:10000
atEnd:reboot
EOF

sleep 2
umount $mount_point
cp $image_name .
```

Figure 1 - Floppy Image Script File (mk_floppy_img.sh)

B. Install GAIA OS

1. Create a New Virtual Machine
2. In the Settings, Add a floppy drive image and use the floppy image created above.
    a. From the steps above, gaia_floppy.flp is the image file used.

3. The VM image will default to removable media, so the default boot device will need to be changed.
    a. Prior to booting, be sure to Power Up to Firmware and verify the CDrom will boot prior Removable media.
    b. Select Save and Continue
4. Remove the floppy device
5. Boot the VM until the installation
6. Proceed to step C

Options: After boot, you can save a snapshot of this configuration as this is the base configuration prior to running the First Time Wizard Configuration.

C. Create First Time Wizard Configuration File for the Management server

1. Create a First Time Wizard installation configuration file to build a unique management or gateway
    a. Use **sk69701 -** How to run the First Time Configuration Wizard through CLI in GAIA R76 and above
    b. See below configuration file **ftw_management.cfg** as an example for a Smart Manager
2. Copy the ftw_management.cfg from

    a. https://github.com/rickdevera/checkpoint_automation

3. Open ftw_management.cfg and verify the following paramenters

Verfity the following parameters

a. install_security_management=”true”
b. install_security_gateway=”false”
c. install_mgmt_primary=”true”
d. admin_hash is set to the password using openssl; the default in the file is vpn123.
e.

Configure the IP address of the management

f. ipaddr_v4=10.1.1.101
g. masklen_v4=24
h. default_gw_v4=10.1.1.254

Configure DNS

i. primary=10.1.1.2
j. secondary=8.8.8.8

Figure 2 - First Time Configuration Installation file (ftw_management.cfg)

```
#############################################################################
#                                                                           #
#                        Products configuration                             #
#                                                                           #
#    For keys below set "true"/"false" after '='  within the quotes         #
#############################################################################
# Install Security Management.
install_security_managment="true"

# Install Security Gateway.
install_security_gw="false"

# Performance Pack
install_ppak="false"

# Enable DAIP (dynamic ip) gateway.
# Should be "false" if CXL or Security Management enabled
gateway_daip="false"

# Enable/Disable CXL.
gateway_cluster_member="false"

# Optional parameters, only one of the parameters below can be "true".
# If no primary of secondary specified, log server will be installed.
# Requires Security Management to be installed.
install_mgmt_primary="true"
install_mgmt_secondary="false"

# Provider-1 parameters
# e.g: install_mds_primary=true
#      install_mds_secondary=false
#      install_mlm=false
#      install_mds_interface=eth0
install_mds_primary="false"
install_mds_secondary="false"
install_mlm="false"
install_mds_interface=
# Automatically download Blade Contracts and other important data (highly recommended)
# It is highly recommended to keep this setting enabled, to ensure smooth operation of
Check Point products.
# for more info see sk94508
#
# possible values: "true" / "false"
download_info="true"

# Improve product experience by sending data to Check Point
# If you enable this setting, the Security Management Server and Security Gateways may
upload data that will
# help Check Point provide you with optimal services.
# for more info see sk94509
#
# possible values: "true" / "false"
upload_info="false"
```

```
# In case of Smart1 SmartEvent appliance, choose
# Security Management only, log server will be installed automatically
#############################################################################
#                                                                           #
#       Operating System configuration - optional section                   #
#                                                                           #
#               For keys below set value after '='                          #
#############################################################################

# Password (hash) of user admin.
# To get hash of admin password from configured system:
#       dbget passwd:admin:passwd
# OR
#       grep admin /etc/shadow | cut -d: -f2
#
# IMPORTANT! In order to preserve the literal value of each character
# in hash, enclose hash string within the quotes.
#       e.g admin_hash='put_here_your_hash_string'
#
# Optional parameter
# below is the has for vpn123.  Can be generated using
# openssl password -1 -salt <salt>
# or
# openssl password -1 -salt $(openssl rand -base64 6)
#
admin_hash='$1$PR5ij6N3$tyHK2iCxIGpZx6DEBYtIT/'

# Interface name, optional parameter
iface=eth0

# Management interface IP in dotted format (e.g. 1.2.3.4),
# management interface mask length (in range 0-32, e,g 24 ) and
# default gateway.
# Pay attention, that if you run first time configuration remotely
# and you change IP, in order to maintain the connection,
# an old IP address will be retained  as a secondary IP address.
# This secondary IP address can be delete later.
# Your session will be disconnected after first time configuration
# process.
# Optional parameter, requires "iface" to be specified
# IPv6 address format: 0000:1111:2222:3333:4444:5555:6666:7777
# ipstat_v4 manually/off
# ipstat_v6 manually/off
ipstat_v4=manually
ipaddr_v4=10.1.1.254
masklen_v4=24
default_gw_v4=192.168.1.254

ipstat_v6=off
ipaddr_v6=
masklen_v6=
default_gw_v6=

# Host Name e.g host123, optional parameter
hostname=management

# Domain Name e.g. checkpoint.com, optional parameter
domainname=
```

```
Time Zone in format Area/Region (e.g America/New_York or Etc/GMT-5)
# Pay attention that GMT offset should be in classic UTC notation:
# GMT-5 is 5 hours behind UTC (i.e. west to Greenwich)
# Enclose time zone string within the quotes.
# Optional parameter
timezone='America/Chicago'

# NTP servers
# NTP parameters are optional
ntp_primary=
ntp_primary_version=
ntp_secondary=
ntp_secondary_version=

# DNS - IP address of primary, secondary, tertiary DNS servers
# DNS parameters are optional.
primary=192.168.103.2
secondary=8.8.8.8
tertiary=4.2.2.2

# Proxy Settings - Address and port of Proxy server
# Proxy Settings are optional
proxy_address=
proxy_port=

#############################################################################
#                                                                           #
#                        Post installation parameters                       #
#                                                                           #
#    For keys below set "true"/"false" after '='  within the quotes         #
#############################################################################
# Optional parameter, if not specified the default is false
reboot_if_required="false"
```

4. Use SCP to copy the ftw_management.cfg file to the appliance. Be sure the default shell used for admin is set to /bin/bash.

    a. *clish> set user admin shell /bin/bash*
    b. clish> *save config*

5. Login to appliance
6. Log into expert mode
    a. Verify config file and check for errors
        i. run “config_system –f ftw_management.cfg –dry_run
    b. After successful verification
        i. run “config_system –f ftw_management.cfg –dry_run

7. Reboot the system upon completion
8. Logon to WebUI to verify configuration.

Next Steps: In Progress :

1. Save as template in ESX with different deployments
2. Use Ansible to build POC environment