STAC Reference Platform[1]

1 Introduction

The following sections will detail the configuration of the STAC Reference Platform; consisting of:

- Hardware Platform (NUC)
- Disk partitions and volumes on the NUC SSD
- File System installed on the volumes
- Linux Kernel
- Linux Distribution
- Daemons started by Systemd
- Docker Server
- Docker Containers
- Challenge Programs and STAC Baseline Image
- Procedures for performing reference installation
- Reference Network Environment Configuration

2 Hardware

The hardware Platform will be a NUC, model NUC5i5RYH, with following key specifications:
(http://www.intel.com/content/www/us/en/nuc/nuc-kit-nuc5i5ryh.html)

- CPU
  - Intel(R) Core(TM) i5-5250U CPU @ 1.60GHz
    (http://ark.intel.com/products/84984/Intel-Core-i5-5250U-Processor-3M-Cache-up-to-2_70-GHz)
    - Two 64-bit Cores, each with base operating frequency of 1.6GHz
      - Support Intel Turbo Boost up to 2.7GHz however this will be disabled through BIOS for the reference platform
      - Support Intel Speed Step for lower frequency operation (will disable frequency reduction through cpupower.service configuration)
      - Support Intel Hyper Threading, providing 2 logical processors per Core for a total of 4 logical processors
    - Front Side Bus frequency of 1600 MHz

[1] The Apogee Research effort on STAC is funded by the United States Airforce Research Lab (AFRL) and the Defense Advanced Research Projects Agency (DARPA) under Contract Number FA8750-15-C-0089. THE VIEWS AND CONCLUSIONS CONTAINED IN THIS DOCUMENT ARE THOSE OF THE AUTHORS AND SHOULD NOT BE INTERPRETED AS REPRESENTING THE OFFICIAL POLICIES, EITHER EXPRESSED OR IMPLIED, OF THE DEFENSE ADVANCED RESEARCH PROJECTS AGENCY OR THE US GOVERNMENT.

- Memory Architecture
  - L1 cache (32 KiB I-cache, 32 KiB D-cache per Core)
  - L2 cache (256 KiB per Core)
  - L3 cache (3 MiB)
  - External Memory: 16GiB DDR3L, 1333/1600MHz (64 bit) – max transfer rate of 25.6GB/s
    (Memory Crucial 16GiB Kit 2-8GiB PC3-12800 DDR3 KIT - Model # ct2kit102464BF160B)
- Storage
  - 250 GB SSD (Samsung 850 EVO M.2 Sata 6Gb/s - Model # mz-n5e250bw)
    (see disk partitioning below)
- Network
  - 10/100/1000 Mbps Ethernet (Wi-Fi disabled)
    MTU size of loopback interface will be configured as 1500

3 Disk Partitioning and Logical Volumes

The solid state drive (/dev/sda) will be partitioned as follows:

- sda1: 200 MiB for EFI, GRUB2
- sda2: 500 MiB for kernel images
- sda3: 68 GiB, managed by LVM2 as 3 logical volumes:
  - centos-root (root filesystem, mounted at '/'): 50 GiB
  - centos-home (user home directories, mounted at '/home/') : 10 GiB
  - centos-swap (swap space) 8000 MiB
- sda4: 40 GiB, managed by LVM2 as 2 logical volumes:
  - vg-docker-data (pool of data for docker images): 35 GiB
  - vg-docker-metadata (metadata for managing above pool): 4.9 GiB
- sda5: Optional 20 GiB "Hot Partition" for installation of Docker Images on "Bare Metal"

4 File System

XFS File-system will be installed on centos-root and centos-home volumes.

5 Linux Kernel

The Linux kernel will be 3.10.0:

- 64 bit kernel 3.10.0-229.el7.x86_64
- Started as follows by GRUB2:

```
/vmlinuz-3.10.0-229.el7.x86_64 root=/dev/mapper/centos-root ro
rd.lvm.lv=centos/root rd.lvm.lv=centos/swap crashkernel=auto rhgb
quiet LANG=en_US.UTF-8
```

- For this engagement, no restrictions on processor selection will be enforced upon the kernel scheduler. All four logical processors (2 cores, each with 2 logical processors due to hyper

threading) may be allocated by the kernel scheduler to each thread, as well as the interrupt handlers.

Detailed kernel configuration may be provided separately.

6 Linux Distribution

The Linux distribution will be Centos 7:

- CentOS Linux release 7.1.1503 (Core)
- Minimal installation w. Ethernet enabled (DHCP) (as reference, see anaconda-ks.cfg below)
- Systemd target “multi-user.target” (login through ssh or console)
- User ‘stac’ with ‘/home/stac’ home directory and ‘wheel’ group membership (for sudo access)

```
#version=RHEL7
# System authorization information
auth --enableshadow --passalgo=sha512
# Use CDROM installation media
cdrom
# Use graphical install
graphical
# Run the Setup Agent on first boot
firstboot –enable
ignoredisk --only-use=sda
# Keyboard layouts
keyboard --vckeymap=us --xlayouts='us'
# System language
lang en_US.UTF-8
# Network information
network  --bootproto=dhcp --device=enp0s25 --ipv6=auto –activate
network  --hostname=localhost.localdomain
#Root password
rootpw –lock
# System timezone
timezone America/New_York –isUtc
user --groups=wheel --name=stac --
password=$6$O41JeGbbtBigPt6Z$d.lhTowUG.iFIJFC/BnOfiICrBuk57qJK1fbLDNXqtqs2EN0C3
me.Ainliq5yoVd.Nlbl/.Uzn5Xy/sXKy.9T0 --iscrypted --gecos="stac"
# System bootloader configuration
bootloader --append=" crashkernel=auto" --location=mbr --boot-drive=sda
# Partition clearing information
clearpart  --initlabel --list=sda5,sda4,sda3,sda2,sda1
# Disk partitioning information
part /boot --fstype="xfs" --ondisk=sda --size=500
part pv.695 --fstype="lvmpv" --ondisk=sda --size=69448
part /boot/efi --fstype="efi" --ondisk=sda --size=200 --
fsoptions="umask=0077,shortname=winnt"
volgroup centos --pesize=4096 pv.695
logvol /  --fstype="xfs" --size=51200 --name=root --vgname=centos
logvol swap  --fstype="swap" --size=8000 --name=swap --vgname=centos
logvol /home  --fstype="xfs" --size=10240 --name=home --vgname=centos
%packages
@core
```

```
kexec-tools
%end
%addon com_redhat_kdump --enable --reserve-mb='auto'
%end
```

7 Daemons

The minimal installation includes the following running daemons (after the install script described in section 11 has installed `docker`, and disabled `firewalld, tuned, crond, Postfix, and NetworkManager`):

```
systemd-journal
lvmetad
systemd-udevd
auditd
irqbalance
rsyslogd
systemd-logind
dbus-daemon
login
sshd
dhclient
docker
```

Note: In future engagements, the `irqbalance` daemon may become configured such as to process interrupts on specific processors.

8 Docker Server

Docker will be installed on the reference platform:

- Docker version 1.9.1 (docker-engine-1.9.1-1.el7.centos.x86_64.rpm); installed through a script provided by STAC-EL (see section 11).
- The following Docker configuration options will be set; such as to apply direct-lvm storage (dedicated volumes for storage of docker images; managed as a pool of logical volumes)
  - –storage-driver=devicemapper
  - –storage-opt dm.datadev=/dev/vg-docker/data
  - –storage-opt dm.metadatadev=/dev/vg-docker/metadata
- The following Docker configuration option will be set; such as to apply XFS filesystem for docker images:
  - –storage-opt dm.fs=xfs
- The following Docker configuration option will be set; as workaround for a bug in docker related to Systemd management of Docker cgroup settings (the default w/o this option):
  - –exec-opt native.cgroupdriver=cgroupfs
- The Linux user ‘stac’ will be added to the Linux group ‘docker’, such as to allow execution of docker commands without sudo.

9 Docker Containers

Challenge Programs will be managed as Docker Containers, hosted by a STAC Docker Registry installed on the reference platform. Challenge Programs will be pulled and run from this STAC Registry through a script (`manage_stac_docker_registry_<version>.sh`).

- Challenge Programs will be run within Docker Containers; started with the following options:
  - –net=host (in order to disable NAT'ing between Docker container and localhost)
- No (cgroup) restrictions will be enforced on Docker Containers for access to the resources of the reference platform.

10 Challenge Programs and STAC Baseline Image

Challenge Programs will be Java bytecode, run within a Docker Container consisting of an XFS filesystem with the following layers:

- STAC Base Image:
  - Centos 7.1.1503 (tag centos:7.1.1503 from `hub.docker.com`)
    - No services/daemons running within container unless installed by Challenge Program
  - Java Runtime Environment java-1.7.0-openjdk-1.7.0.85-2.6.1.2.el7_1.x86_64.rpm (available at http://vault.centos.org/7.1.1503/updates/x86_64)
- Challenge Program and its dependencies
  - Challenge Programs will be run with JIT disabled (i.e. with the -Xint setting)

11 Installation Walk-through

The following describes procedures for performing a STAC Reference Installation on a fresh NUC:

1) Connect NUC to a monitor, keyboard, mouse, and Ethernet (with DHCP server reachable on the network)

2) Disable Intel Turbo Boost through BIOS Settings (boot + f2)

3) Install CentOS 7.1.1503 from Minimal Installation CD/DVD, as downloaded from e.g.:

   `http://vault.centos.org/7.1.1503/isos/x86_64/CentOS-7-x86_64-Minimal-1503-01.iso`

   NOTE: After powering up the NUC, press F10, then select the **UEFI** Bootloader option from the CD/DVD.

   Apply following selections:

   - Select "Minimal Install" with no Add-Ons
   - Select "I will configure partitioning", do not select "Encrypt my data"

- Configure the following partitions:
  - /boot/efi
    - Mount Point /boot/efi
    - Device Type "Standard Partition"
    - File System "EFI System Partition"
    - Desired Capacity 200MiB
  - /boot
    - Mount Point /boot
    - Device Type “Standard Partition”
    - File System XFS
    - Desired Capacity 500MiB
  - /
    - Mount Point /
    - Device Type LVM
    - File System XFS
    - Volume Group centos
    - Name root
    - Desired Capacity 50 GiB
  - /home
    - Mount Point /home
    - Device Type LVM
    - File System XFS
    - Volume Group centos
    - Name home
    - Desired Capacity 25 GiB
  - Swap
    - Mount Point : None
    - Device Type LVM
    - File System swap
    - Volume Group centos
    - Name swap
    - Desired Capacity 8000 MiB
- Select following network settings:
  - Ethernet ON
  - Wireless OFF
- Create stac user:
  - Full name stac
  - User name stac
  - Make user administrator
  - Require a password to use this account
  - Password stacme (click Done twice since password is weak)

4) Following CentOS installation, reboot and login as stac. Then determine the IP address assigned by DHCP by typing “`ip addr list`”

5) Download the following "STAC Reference Platform Configuration" script, found in the STAC GIT Repository to the NUC (e.g. using scp):

```
STAC_Reference_Platform_Install.v2.3.sh
```

6) From the NUC (console or through ssh connection), run the script:

```
sudo ./STAC_Reference_Platform_Install.v2.3.sh all
```

The script will remove some daemons, install the `cpupower Systemd` service, and finally download and install the `docker` service.

7) Reboot the NUC

12 Reference Network Environment

For Engagements 1 – 4 all challenge programs and proofs are run on a single Reference NUC with network communications over Localhost.