Deploy the ASA Container in a Docker Environment

You can deploy the ASA container (ASAc) in an open source Docker environment running on any cloud platform.

Overview

A container is a software package that bundles up code and associated requirements such as system libraries, system tools, default settings, runtime, and so on, to ensure that the application runs successfully in a computing environment. From Secure Firewall ASA version 9.22, you can deploy the ASA container (ASAc) in an open-source Docker environment.

Guidelines and Limitations to Deploy ASA Container in Docker Environment

- The ASA container (ASAc) solution is validated on open-source Kubernetes and Docker environments only.
- Other Kubernetes frameworks such as EKS, GKE, AKS, OpenShift, are not validated yet.
- The following features are not validated:
  - Upgrade

- High Availability
- Cluster
- IPv6
- Transparent mode

Licenses to Deploy ASA Container in Docker Environment

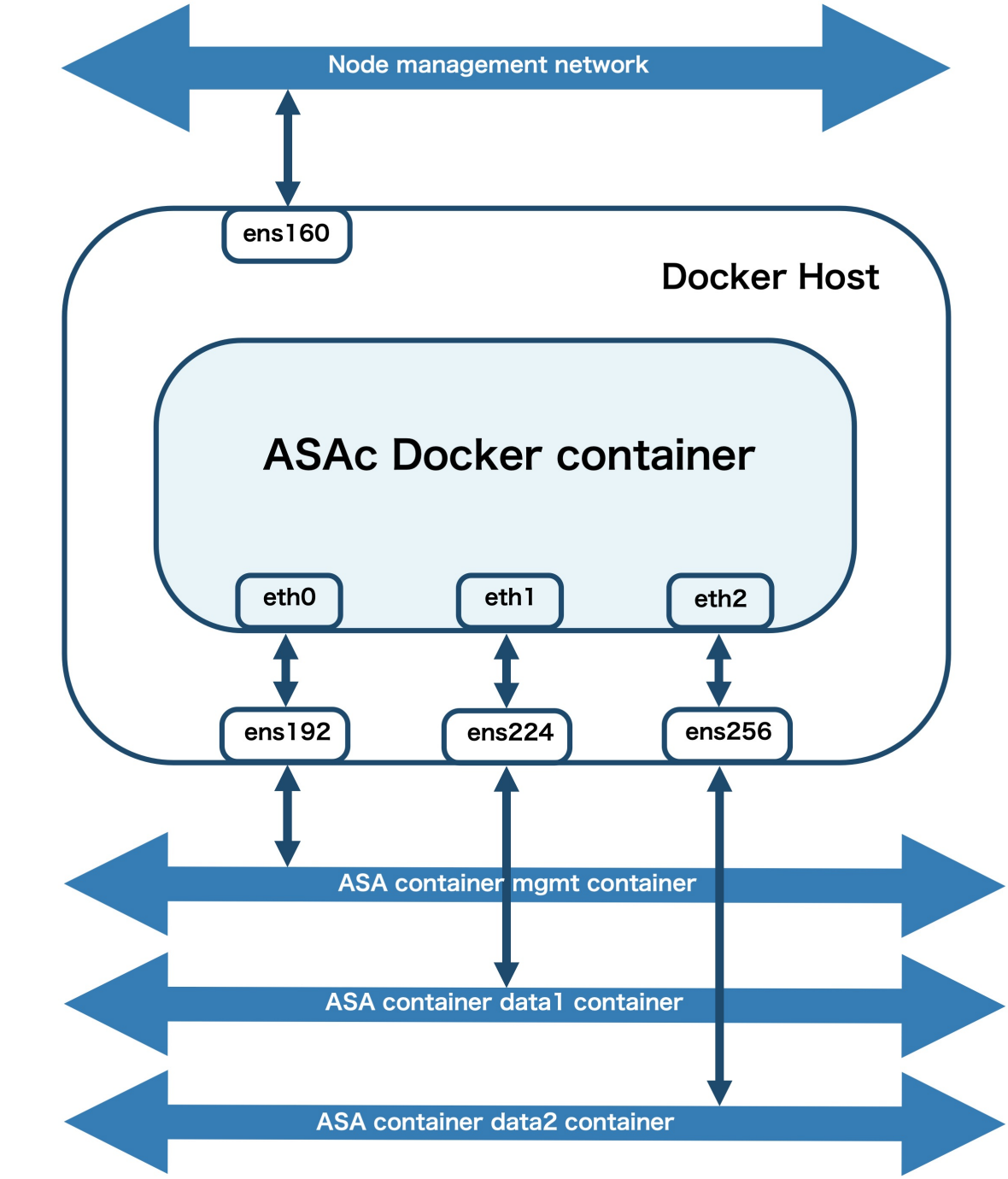
Use one of the following licenses to enable deployment of ASA container on Docker:

- ASAc5 - 1 vCPU, 2 GB RAM, and 100 Mbps rate limit
- ASAc10 - 1 vCPU, 2 GB RAM, and 1 Gbps rate limit

Components of Solution to Deploy ASA Container in Docker Environment

- Operating system
  - Ubuntu 20.04.6 LTS on docker host
- Macvlan network for configuration validation

Sample Topology to Deploy ASA Container in Docker Environment



In this sample topology, the ASA docker container has three virtual network interfaces –eth0, eth1, and eth2, that are connected to the following interfaces – ens192, ens224, and ens256. These interfaces are mapped to the ASAc mgmt, data1, and data2 networks. The interface ens160 is the node management interface.

Prerequisites to Deploy ASA Container in Docker Environment

- Ensure that Ubuntu 20.04.6 LTS is installed on the docket host.
- Allocate three virtual interfaces on the docker host for ASA container operations.
- Set up the docker host's management interface to be used for ssh access to the docker host.
- Enable Hugepages on the docker host.
- Set up Docker version 24.0.5 with macvlan network for configuration validation.

For more information on general Docker operations mentioned in these prerequisites, see Docker documentation.

Deploy ASA Container in Docker Environment

Perform the procedure given below to deploy ASA container (ASAc) in Docker environment.

Step 1 Set up the requirements mentioned in the Prerequisites to Deploy ASA Container in Docker Environment.

Step 2 Run the **route -n** command to verify the network interface configuration. In this example, ens160 is the node's management interface. The nodes ens192, ens224, and ens256, are mapped to the ASAc interfaces.

Note The outputs given below are sample outputs only.

```
ubuntu@k8s-worker:~$ route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
0.0.0.0         10.10.4.1       0.0.0.0         UG    100    0        0 ens160
10.10.4.0       0.0.0.0         255.255.255.224 U     0      0        0 ens160
10.10.4.1       0.0.0.0         255.255.255.255 UH    100    0        0 ens160
10.10.4.32      0.0.0.0         255.255.255.224 U     0      0        0 ens192
10.10.4.64      0.0.0.0         255.255.255.224 U     0      0        0 ens224
10.10.4.96      0.0.0.0         255.255.255.224 U     0      0        0 ens256
10.244.235.192  10.244.235.192  255.255.255.192 UG    0      0        0 vxlan.calico
10.244.254.128  0.0.0.0         255.255.255.192 U     0      0        0 *
172.17.0.0      0.0.0.0         255.255.0.0     U     0      0        0 docker0
```

Step 3 Run the **cat** command given below to verify hugepage configuration.

```
ubuntu@k8s-worker:~$ cat /proc/meminfo | grep -E 'HugePages_Total|HugePages_Free'
HugePages_Total:    2048
HugePages_Free:     2048
```

Step 4 Download the ASA docker tar bundle that includes the ASA container image from software.cisco.com.

Step 5 Load the docker tar bundle on the host.

```
$ docker load < asac9-22-1-1.tar
$ docker images
   REPOSITORY                                  TAG         IMAGE ID
   dockerhub.cisco.com/asac-dev-docker/asac    9.22.1.1    55f5dbc5f3aa
```

Step 6 Download the templates and other files from the **docker** folder in the ASAc GitHub repository.

Step 7 Run the **docker network create** command to create docker networks. The ASAc needs one management interface and two date interfaces for inside and outside networks. When docker starts, the docker networks are attached to the docker in alphabetical order. We recommend that you name the management interface in such a way that it is the first interface that is attached to the docker.

```
$ docker network create -d macvlan -o parent=ens192 asac_nw1
$ docker network create -d macvlan -o parent=ens224 asac_nw2
$ docker network create -d macvlan -o parent=ens256 asac_nw3
```

Step 8 Run the **docker network ls** command to verify that the networks have been created successfully.

```
$ docker network ls
NETWORK ID    NAME      DRIVER   SCOPE
06f5320016f8  asac_nw1  macvlan  local
258954fa5611  asac_nw2  macvlan  local
3a3cd7254087  asac_nw3  macvlan  local
```

Step 9 Verify the default parameter values present in the **day0-config** file. You can also update these values as per your requirement.

Step 10 Open the **start_docker_asac.sh** script to update configuration values for CPU, memory, container-name, and image repo name, as per your requirement.

Note Default configuration values are provided for the parameters in the start_docker_asac.sh script. Modify them only if required.

Step 11 Run the command given below to start ASAc in the docker environment.

```
$ ./<script-name> <asac-image-path-and-version> <asac-mgmt-nw> <asac-data1-nw> <asac-data2-nw>
```

```
$ ./start_docker_asac.sh dockerhub.cisco.com/asac-dev-docker/asac:9.22.1.1 asac_nw1 asac_nw2
asac_nw3
   Docker networks are provided..
   Starting ASA Build Container...
   docker create -it --privileged --cap-add=NET_RAW --network asac_nw1 --name asac -e ASAC_CPUS=1
-e ASAC_MEMORY=2048M -v /dev:/dev -v /home/ubuntu/standalone-asac/docker/day0-config:/asacday0-
config/day0-config:Z -v /home/ubuntu/standalone-asac/docker/interface-config:/mnt/disk0/
interface-config/interface-config:Z -e CORE_SIZE_LIMIT=200MB -e COREDUMP_PATH=/mnt/coredump_repo/
-e ASA_DOCKER=1 -e ASAC_STANDALONE_MODE=1 -e ASAC_ROOT_PRIVILEGE=1 --entrypoint /asa/bin/
lina_launcher.sh dockerhub.cisco.com/asac-dev-docker/asac:9.22.1.1

    Mount Points:
    ------------------------------------------------------------------------------------------
    Host                                                        Container
    ----                                                        ---------
    /dev                                                        /dev
    /home/ubuntu/standalone-asac/docker/day0-config        /asac-day0-config/day0-config
    /home/ubuntu/standalone-asac/docker/interface-config
/mnt/disk0/interface-config/interface-config
------------------------------------------------------------------------------------------
docker network connect asac_nw2 asac
```

```
docker network connect asac_nw3 asac
docker start asac
```

Validate ASA Container Deployment in Docker Environment

Validate successful ASA container deployment by checking the list of containers running on the docker host.

```
$ docker ps -a
CONTAINER ID IMAGE                                                    COMMAND
 CREATED       STATUS        PORTS  NAMES
6e5bff4dbcaf dockerhub.cisco.com/asac-dev-docker/asac:9.22.x.x   "/asa/bin/lina_launc…" 3
minutes ago Up 3 minutes         asac
```

Access ASA Container Deployment Logs in Docker Environment

Run the **docker logs asac** command to check the docker logs for troubleshooting any issues that may occur.

```
$ docker logs asac
Skip NVMe Device for ASAc mode
cdrom device /dev/sr0 found
mount: /mnt/cdrom: WARNING: source write-protected, mounted read-only.
Error: Encrypted file system support not in Linux kernel.
nr_overcommit_hugepages set to 128 for virtual platform
info: ASAc SSHd Directory Created
No interface-config file found at /interface-config, using default shared
file: /mnt/disk0/interface-config/interface-config
No day0-config file found at /day0-config, using default shared file:
/asac-day0-config/day0-config
info: ASAc Day 0 configuration installed.
info: ASAc Primay/backup Key installed
info: Running in vmware virtual environment.
....
INFO: Network Service reload not performed.
INFO: Power-On Self-Test in process.
.....................................
INFO: Power-On Self-Test complete.
INFO: Starting SW-DRBG health test...
INFO: SW-DRBG health test passed.
Creating trustpoint "_SmartCallHome_ServerCA" and installing certificate...
Trustpoint CA certificate accepted.
Creating trustpoint "_SmartCallHome_ServerCA2" and installing
certificate...
Trustpoint CA certificate accepted.
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa>
```

Access ASA Container in Docker Environment

Run the **docker attach asac** command to access the CLI of the ASA container (ASAc) and obtain required outputs. In this example, we access the CLI of the ASAc and run the **show version** command.

Note You can also use ASDM to access ASAc in a Docker environment.

```
ciscoasa> enable
Password: *********
ciscoasa# sh version
Cisco Adaptive Security Appliance Software Version 9.22
SSP Operating System Version 82.16(0.216i)
Device Manager Version 7.22
Compiled on Tue 28-Nov-23 14:37 GMT by builders
System image file is "Unknown, monitor mode tftp booted image"
Config file at boot was "startup-config"
ciscoasa up 9 mins 50 secs
Start-up time 36 secs
Hardware: ASAc, 2048 MB RAM, CPU Xeon E5 series 2100 MHz, 1 CPU (1
core)
BIOS Flash Firmware Hub @ 0x1, 0KB
0: Ext: Management0/0 : address is 0242.ac12.0002, irq 0
1: Ext: GigabitEthernet0/0 : address is 0242.ac13.0002, irq 0
2: Ext: GigabitEthernet0/1 : address is 0242.ac14.0002, irq 0
3: Int: Internal-Data0/0 : address is 0000.0100.0001, irq 0
```