GuardDog AI Container Deployment Guide

Steps to deploy a single container with Docker on RedHat Enterprise Linux

The following are the steps to configure the environment and get all the requirements in place to deploy the container image. These steps and the GuardDog AI container have been tested with RHEL versions 8.8, 8.9, 9.2, and 9.3. This guide assumes RHEL is already installed, configured and ready to deploy the GuardDog AI container.

Prerequisites, Assumptions and Additional Configurations

- ➔ Docker: At least Docker version 23.x must be installed on the system. For RHEL, follow the installation instructions in the next section.
- ➔ DNS Configuration: Necessary if you encounter problems downloading Docker images.
- ➔ Network Configurations: Make the necessary adjustments for effective communication within your network. Firewall rules are crucial to allow communication back and forth between the cloud and this container, please make sure you follow those and make the necessary changes before attempting to start the container.
- ➔ Host network interfaces: The container is prepared to work with the network interfaces presented to the host. Have those configured before running the container (vlans, logical, physical).
- ➔ Container runs with host networking access to be able to be completely functional. It will detect all ethernet interfaces and add them to the internal network configuration within the container.
- ➔ Container runs in privilege mode to be able to perform the functions it is designed for.
- ➔ It uses a persistent volume in order to be able to maintain its configuration throughout container and image updates and reboots.
- ➔ A license is needed to run the container, and this will be provided as part of the deployment process.

➔ The container is meant to be run following this guide utilizing the restart switch in the command to be able to have the container come back up when rebooting the host system.

This first set of requirements is to create an account in our system to get things started. Once this first section is completed, we will send an email with the necessary parameters and variables to run the container.

Create an account

1. Create an account at https://fido.guarddog.ai
2. Click on Sign Up
3. Fill out the short online form
4. Verify your account
5. Login with your account to fully activate it
6. Contact your sales representative and/or support to let us know you have completed this step and the email address you used for the account.

Once the account has been created, please send us an email to support@guarddog.ai to let us know you are ready to proceed to the next step.

Here are some additional instructions on how to set up Docker and other settings on your system.

Docker Installation on RHEL

1. Installation of yum-utils and Docker Repository Configuration

```
sudo yum install -y yum-utils
```

```
sudo yum-config-manager --add-repo
https://download.docker.com/linux/centos/docker-ce.repo
```

2. Docker Installation

```
sudo yum install docker-ce docker-ce-cli containerd.io –allowerasing
```

3. Start and Enable Docker

```
sudo systemctl start docker
```

```
sudo systemctl enable docker
```

4. Add User to Docker Group

```
sudo usermod -aG docker $USER
```

```
reboot
```

DNS Configuration for Docker on RHEL

In some cases, we have seen issues with DNS not being properly configured. This is the case all the times, but we wanted to include this additional step in case it is needed.

1. Disable DNS Management by NetworkManager

```
echo -e "[main]\ndns=none" | sudo tee /etc/NetworkManager/conf.d/90-dns-none.conf && sudo systemctl reload NetworkManager
```

2. Manually Set DNS Servers

```
echo -e "nameserver 8.8.8.8\nnameserver 8.8.4.4" | sudo tee -a /etc/resolv.conf
```

Disable Consistent Network Device Naming in RHEL

We have seen some strange behavior when the network interfaces naming is not configured correctly. This method allows us to use the standard naming convention. This is not mandatory and is only needed if issues are seen when running the container and when suggested by our engineering team.

1. Edit Kernel Parameters in GRUB

```
sudo sed -i 's/GRUB_CMDLINE_LINUX="\(.*\)"/GRUB_CMDLINE_LINUX="\1 net.ifnames=0 biosdevname=0"/' /etc/default/grub
```

2. Regenerate GRUB Configuration
    a. For BIOS systems:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

    b. For UEFI systems:

```
grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

3. System Reboot

```
reboot
```

Container Deployment

This step goes over the process of getting the latest container image downloaded from DockerHub and then the command needed to start the container. This command includes the license and some other parameters explained below.

Download Container Image

```
docker pull guarddogai/prod:latest
```

By now you should have received an email from us with the parameters needed for the docker run command below. In case you have not, please follow up with support.

Here is the command to start the container. Please make sure you follow the instructions to provide the right information when issuing the command.

```
docker run -it --cap-add NET_ADMIN --net=host --privileged --restart
always -v /etc/guarddog:/etc/guarddog --name gdai
guarddogai/prod:latest <DEVICE_NAME> <USER_EMAIL> <LICENSE_KEY>
```

<DEVICE_NAME>, indicates a friendly name for the container. This will show in the user interface to locate and identify the running container. This is assigned by the client and can be any name to make it easier to remember and organize deployments.

<USER_EMAIL>, this is the email address used to create the account at https://fido.guarddog.ai.

<LICENSE_KEY>, this is the license key that will be provided by GuardDog AI for each container to be deployed. The license is not transferable or cannot be interchangeably used with other containers.

You are now ready to start the container, please replace <DEVICE_NAME>, <USER_EMAIL>, and <LICENSE_KEY> with their corresponding values.

This is all you should need to do. Given that you had the network setup correctly following the firewall document you should have received, the container will start up and go through a series of checks to make sure it is able to communicate with the cloud. Then it will proceed to validate the license and, if valid, then to register with the system. The container is set up so that it automatically registers to your account in our system. Please allow for sufficient time to let the container complete the entire process. Although it is usually done within a few minutes, depending on how busy the network is and the bandwidth available, it may take several hours.