Docker and Wazuh Installation Guide



|  |  |  |  |
| --- | --- | --- | --- |
| Date | Name | Description | Version |
| 12/12/2022 | Caitlin Parker | Created first Draft | 1.0 |
|  |  |  |  |
|  |  |  |  |

## Version Control

# Docker Installation

1. Connect to the VM that Docker and Wazuh need to be installed on via SSH.
2. The following command will install docker.
   * **sudo apt install docker.io** [1]
   * When prompted type **y**. This will start to install Docker. The install can take a while
3. Check the status of docker as sometimes it will start after the installation and sometimes it has to be manually started.
   * To check the status, use the following command:  
     **sudo systemctl status docker** [1]
   * To enable docker use the following command:  
     **sudo system enable --now docker** [1]
4. Test that docker has installed and is running properly with the following command:
   * **sudo docker hello-world** [1]
   * There will be an error message saying that the image cannot be found. If the docker is set up and working correctly the following should be seen underneath.  
     *“Hello from Docker!  
     This message shows that your installation appears to be working correctly.”*
5. Next is to install compose which will allow you to run multiple docker containers at one time. [2] First check that the package index is up to date before installing Compose.
   * **sudo apt-get update** [3]
   * **sudo apt-get install docker-compose-plugin** [3]

# Wazuh Installation

1. To install Wazuh repository onto an Ubuntu VM use the following commands.
   * **apt-get install gnupg apt-transport-https** [4]
   * **curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo apt-key add –** [4]
   * **echo "deb https://packages.wazuh.com/4.x/apt/ stable main" | sudo tee -a /etc/apt/sources.list.d/wazuh.list** [4]
   * **sudo apt-get-update** [4]
2. Once the repository has been downloaded the Wazuh Agent can be installed.
   * **WAZUH\_MANAGER="10.0.0.2" sudo apt-get install wazuh-agent** [4]
3. Check the status of the wazuh-agent to see if it needs to be activated.
   * **sudo systemctl status wazuh-agent** [4]
   * If not enabled run the following commands.  
     **sudo systemctl daemon-reload** [4]  
     **sudo systemctl enable wazuh0agent** [4]  
     **sudo start wazuh-agent** [4]
4. Wazuh-manager only works when the version is greater than or equal to that of the Wazuh agent. To make sure everything keeps working updates will need to be disabled for wazuh agent. [4]
   * **sudo sed -i "s/^deb/#deb/" /etc/apt/sources.list.d/wazuh.list** [4]
   * **sudo apt-get update** [4]

References

[1] ProgrammingKnowledge (2020, May. 18). *How to install Docker on Ubuntu 20.0.4 LTS Focal Fossa* [Website]. Available: <https://youtu.be/aMKUuaga85A>

[2] Docker Docs (n.a.). *Docker Compose: Overview* [website]. Available: <https://docs.docker.com/compose/>

[3] Docker Docs (n.a.). *Install the Compose plugin* [website]. Available: <https://docs.docker.com/compose/install/linux/>

[4] wazuh (n.a.). *Deploying Wazuh agents on Linux endpoints* [website]. Available: <https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-linux.html>