





# DOCKER ENTERPRISE 2.X LINUX/UNIX STIG ANSIBLE DOCUMENTATION

## Version 1, Release 1

## October 2019

## Developed by DISA for the DoD

# TABLE OF CONTENTS

**Page**

**1. BACKGROUND ..... 1**
**2. INSTALLATION ..... 2**
2.1 Installing Ansible ..... 2
2.2 Extracting ..... 2
**3. CONFIGURATION ..... 3**
3.1 Hosts ..... 3
3.2 Vars ..... 3
3.3 Simple ..... 3
3.4 Custom ..... 3
**4. OTHER CONSIDERATIONS ..... 4**
4.1 Config Settings Always Changed ..... 4
4.2 Manual Restart ..... 4
4.3 “bridge-nf-call-ip6tables is disabled” Warnings ..... 4
4.4 Ubuntu Rules ..... 4
4.5 SSL Certifactes ..... 4
4.6 Host Key Checking ..... 4
4.7 Usage of Non-root Users ..... 4
4.8 Default File Locations ..... 4

# 1. BACKGROUND

Ansible is an open source, cross-platform configuration management solution used to define and enforce system and application configurations. This package provides Ansible configurations that implement most of the Docker Enterprise 2.x Linux/Unix STIG. While the content has been tested during development, all possible system and environmental factors could not be tested. Before using this content in a production environment, please perform testing with the intended settings in your own test environment. There is no mandate to use this content; it is published as a resource to assist in the application of security guidance to your systems. Use it in the manner and to the extent that it assists with this goal.

# 2. INSTALLATION

The following instructions are for standalone installation using ansible-playbook for testing purposes. A production environment may additionally use Ansible Tower. See here for details.

## 2.1 Installing Ansible

Newer versions of Ansible are in the Red Hat Enterprise Linux 7 EPEL repository. To install it, run the following:

```
sudo yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
sudo yum install ansible
```

For other installation methods, see here.

## 2.2 Extracting

Unzip the **dockerEESTIG-ansible.zip**.

# 3. CONFIGURATION

## 3.1 Hosts

Edit the provided **`hosts`** file to use the correct hostname/address and SSH username to the Docker UCP host for your environment.

## 3.2 Vars

Edit the provided **`UCP_vars.yml`** file to use the correct IP address, username, password, and temporary configuration file path to the Docker UCP host. Edit the provided **`DTR_vars.yml`** to use the correct IP address, username, and password to the Docker DTR host.

## 3.3 Simple

To apply the default STIG Ansible configuration, run the **`enforce.sh`** script to enforce the STIG. To tailor the configuration, follow the steps in the next section.

## 3.4 Custom

To customize, create a YAML (.yml) file containing just the variables to customize from the variables named in the **`roles/dockerEESTIG/defaults/main.yml`** file. This file contains configuration data to define which configuration settings to manage and the values for these settings. Edit the newly created configuration file in a text editor to best suit each system's requirements as needed. For example, if you wanted to turn off STIG rule ID 104763, you would set the "Manage" attribute equal to **`False`**. If you wanted to set STIG rule ID 104767's value to **`true`** you would set the **`_reportAnalytics_Value`**" attribute to **`'true'`**.

```
dockerEESTIG_stigrule_104763_Manage: False
dockerEESTIG_stigrule_104763_createRepositoryOnPush_Option: 'createRepositoryOnPush'
dockerEESTIG_stigrule_104763_createRepositoryOnPush_Value: 'true'

dockerEESTIG_stigrule_104767_Manage: True
dockerEESTIG_stigrule_104767_reportAnalytics_Option: 'reportAnalytics'
dockerEESTIG_stigrule_104767_reportAnalytics_Value: 'true'
```

To use the newly created, custom variables file, edit **`site.yml`** to include it. See the highlighted line to add below:

```
- hosts: all
  gather_facts: no
  vars_files:
    - UCP_vars.yml
    - DTR_vars.yml
    - /path/to/custom/vars.yml
  roles:
  - dockerEESTIG
```

For more information on variables, see here. For more information on YAML, see here.

# 4. OTHER CONSIDERATIONS

## 4.1 Config Settings Always Changed

Due to a limitation in Ansible missing a TOML module, configuration of these settings is done in a way that is not properly whitespace aware. As a result of Docker autoformatting the whitespace, Ansible marks these settings as changed every time.

## 4.2 Manual Restart

Since restarting the Docker service with improper configuration can result in various errors, STIG rules which require Docker service restarts do not restart the service. It is sufficient to restart the Docker service after verifying Docker's configuration then running the following command: **`sudo systemctl restart docker`**

## 4.3 "bridge-nf-call-ip6tables is disabled" Warnings

These warnings are not harmful and can safely be ignored. For more information, see https://wiki.libvirt.org/page/Net.bridge.bridge-nf-call_and_sysctl.conf

## 4.4 Ubuntu Rules

The assumed operating system is RHEL 7. There are two Ubuntu-specific rules included in this content, but the rules are disabled by default. Re-enable them if you are on Ubuntu.

## 4.5 SSL Certificates

By default, the validation of SSL certificates is enabled. For testing purposes, validation checking can be disabled by setting **`do_validate_certs`** to **`False`** in **`UCP_vars.yml`**. To setup SSL certificate validation, see here:
https://docs.ansible.com/ansible/latest/scenario_guides/vmware_scenarios/vmware_requirements.html

## 4.6 Host Key Checking

If an error about host keys is encountered, you may need to either first login via SSH to the Docker UCP host and accept the key manually, or follow the Ansible suggestions here for alternate configurations:
https://docs.ansible.com/ansible/latest/user_guide/intro_getting_started.html#host-key-checking

## 4.7 Usage of Non-root Users

As this content requires root-level access, if not logging in as a root user, add the following to the **`hosts`** file for each line of each applicable host: **`ansible_become=yes`**
This will allow Ansible to become the root user from the remote user via sudo.

## 4.8 Default File Locations

Some STIG rules use default file locations for certain files. If these defaults are not applicable, configure them to custom file locations as described in section 3.2. Reference the **`roles/dockerEESTIG/defaults/main.yml`** file for which STIG rules are affected.