Project Summary

Project Overview

Create Ansible scripts to read / update configuration and Status information on a Firewall Appliance (Cisco Firepower Threat Defense (FTD))connecting via SSH. Developer does not need to know the FTD architecture – a Cisco Firepower Threat Defense (FTD) Subject Matter Expert (SME) is available to assist; SME is not a developer but understands the FTD Architecture / Configuration etc.

Project Summary

1) Assist in Setting/upgrading Ansible on CentOS 7 from version 2.4.2 to 2.7.
2) Create Ansible Scripts based on the scenarios detailed below.
3) Ansible Scripts for only one appliance architecture will be required (Cisco Firepower Threat Defense (FTD) version 6.4).
4) The connection to the appliance uses SSH.

Resources

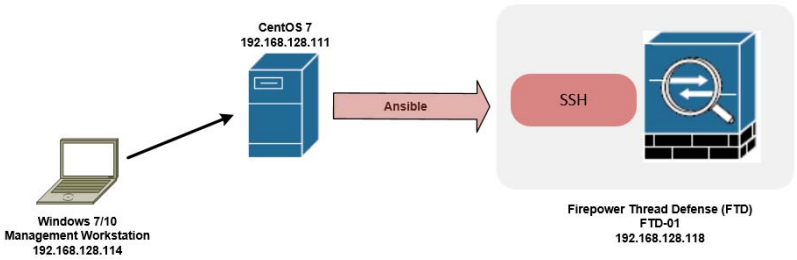
- Ansible for FirePower Threat Defense Documentation:

https://developer.cisco.com/site/ftd-ansible/

Test Environment Details

A test environment will be provided for testing.

- Host running CentOS 7 with Ansible 2.4.2 (will need to upgrade to 2.7) for testing.
- FTP Server to exchange files between Management Workstation and CentOs.
- Cisco FTD version 6.4 installed and configured.
- The topology shown below will be configured with TCTP/IP and all necessary initialization.



Project Details

1. Create Ansible Scripts to read / update information configuration and Status information from Cisco FTD using the SSH interface.
    a. The script will read the current configuration of the “Central Manager” configured on the FTD.
    b. The Script will display the following to the user.
        i. If a manger exists, display the information of the manager that is currently configured on the system and display a message “Login into the FTD and delete the Configured Manager.”

ii. If a Manger configuration does not exist display the following message, “No Manger is configured. Would you like to configure a manager (Y/N)?
iii. If the Answer is N, terminate the script and display the message “No manager configured due to user abort”.
iv. If the answer is Yes, prompt the user to enter the following information:
    1. Manager IP address (Example: 192.168.1.5)
    2. Secret Key (Example: cisco123)

    Note: no validation or error checking is required.

c. The commands on the FTD to view the configured Manger or add a Manager using an interactive SSH session are:

To view mangers:

```
> show managers
```

```
> configure manager add 192.168.128.11 cisco123
```

Note: the IP address 192.168.128.11 and cisco123 will be the variables read by the script and configured on the Appliance.