VMWARE VSPHERE 6.5 STIG ANSIBLE DOCUMENTATION

Version 1, Release 2

June 2020

Developed by DISA for the DoD

TABLE OF CONTENTS

Page

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 the VMware vSphere 6.5 Virtual Machine STIG and most of the VMware vSphere 6.5 ESXi 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 Installing pyVmomi

Ansible VMware modules are written on top of the pyVmomi Python library. Follow its installation instructions to install it here.

2.3 Extracting

Unzip the **`vSphere65STIG-ansible.zip`**.

3. CONFIGURATION

3.1 Hosts

Edit the provided **hosts** file to use the correct hostname/address to the VMware host for your environment. Edit the **hosts.vmware.yml** file to use the correct hostname/address to the VMware vCenter server, server username, and server password for your environment.

3.2 Vars

Edit the provided **vcenter_vars.yml** file to use the correct hostname/address to the VMware vCenter server, the server username, and server password. Edit the provided **esxi_vars.yml** to include the list of cluster names in your environment.

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 only the variables to customize from the variables named in the **roles/vSphere65STIG/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 104393, you would set the "Manage" attribute equal to **False**. If you wanted to set STIG rule ID 104457's size limit to 4096, you would set the "**_tools_setinfo_sizeLimit_Value**" attribute to **'4096'**.

```
vSphere65STIG_stigrule_104393_Manage: False
vSphere65STIG_stigrule_104393_isolation_tools_copy_disable: 'true'

vSphere65STIG_stigrule_104457_Manage: True
vSphere65STIG_stigrule_104457_tools_setinfo_sizeLimit_Value: '4096'
```

To use the newly created, custom variables file, edit either **vSphere65STIG-ESXi.yml or vSphere65STIG.yml** to include it. See the highlighted lines to add below:

```
- hosts: localhost
  gather_facts: no
  vars_files:
    - vcenter_vars.yml
    - esxi_vars.yml
    - /path/to/custom/vars.yml
  roles:
  - vSphere65STIG
```

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

4. OTHER CONSIDERATIONS

4.1 Known Bugs

There is currently a bug in Ansible's vmware_guest module preventing idempotent setting of customvalues for VMs, see: https://github.com/ansible/ansible/pull/49800

4.2 SSL Certificates

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

4.3 Vaulting Secrets

If protection of secrets such as addresses or credentials is required, Ansible provides a means to vault specific files, see: https://docs.ansible.com/ansible/latest/user_guide/vault.html

4.4 Host Key Checking

If an error about host keys is encountered, either first login to the ESXi server 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

4.5 Dual playbooks

This Ansible role requires two Ansible playbooks to enforce the STIGs. Most of the STIG rules are accomplished via the **`vSphere65STIG`** playbook while the **`vSphere65STIG-ESXi`** playbook enforces ESXi server specific settings that cannot be managed via pyVmomi. The included site.yml executes both of these playbooks, but either of the playbooks can be ran independently via the following commands:

```
ansible-playbook -v -k -i hosts -i hosts.vmware.yml vSphere65STIG.yml
```

or

```
ansible-playbook -v -k -i hosts -i hosts.vmware.yml vSphere65STIG-ESXi.yml
```