State of Texas Goverment ()

AWS Proof-of-Concept Environment with Terraform

Document Control Information

Document Information

|  |  |
| --- | --- |
| Document Identification |  |
| Document Name |  |
| Project Name | Cloud Network Migration |
| Client | State of Texas |
| Document Author |  |
| Document Version | 1.0 |
| Document Status | Edit Draft 4.0 |
| Date Released |  |
| File Name |  |

Document Edit History

| Version | Date | Additions/Modifications | Prepared/Revised by |
| --- | --- | --- | --- |
| 1.0 | 06/19/20 | Initial documentation | Roberto Otero |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Document Review/Approval History

| Version | Date | Name | Organization/Title | Comments |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Distribution of Final Document

The following people are designated recipients of the final version of this document:

| Name | Organization/Title |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

Table of Contents

[1 Introduction 4](#_Toc40736683)

[1.1 Purpose 4](#_Toc40736684)

[1.2 Scope and Objectives 4](#_Toc40736685)

[2 Configuring hardening playbook in awx tower 5](#_Toc40736686)

[2.1 5](#_Toc40736687)

[2.2 5](#_Toc40736688)

[2.3 5](#_Toc40736689)

[2.4 5](#_Toc40736690)

[3 Example 6](#_Toc40736691)

[3.1 6](#_Toc40736692)

[4 Example 7](#_Toc40736693)

[4.1 example 7](#_Toc40736694)

[5 Example 8](#_Toc40736695)

[5.1 example 8](#_Toc40736696)

[5.2 example 8](#_Toc40736697)

[6 Appendix 9](#_Toc40736698)

# Introduction



### Purpose Scope

This document aims to provide a detailed plan and architecture for the creation of a proof-of-concept environment in AWS using Terraform. It outlines the required components, their configurations, and the steps to deploy the environment.

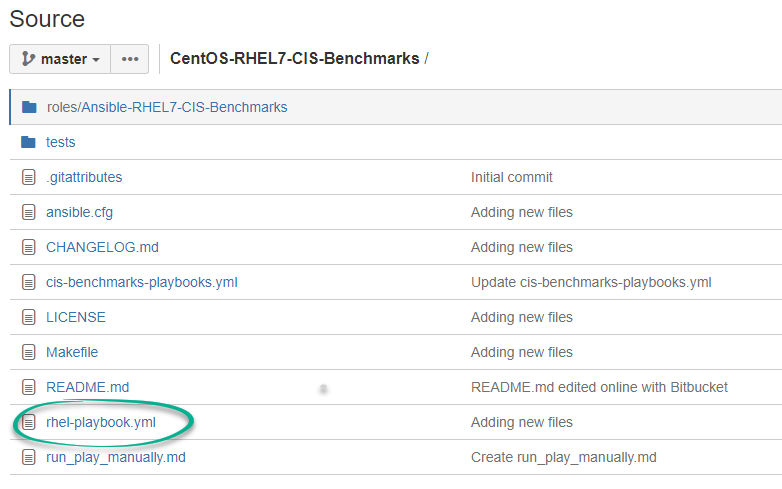
Scope and Objectives

The setup and configuration instructions are for hardening playbooks in AWX tower:

* Login

# RedHat CIS Hardening Playbook Overview

The playbook rhel-playnook.yml will be used to call the role: Ansible-RHEL7-CIS-Benchmarks



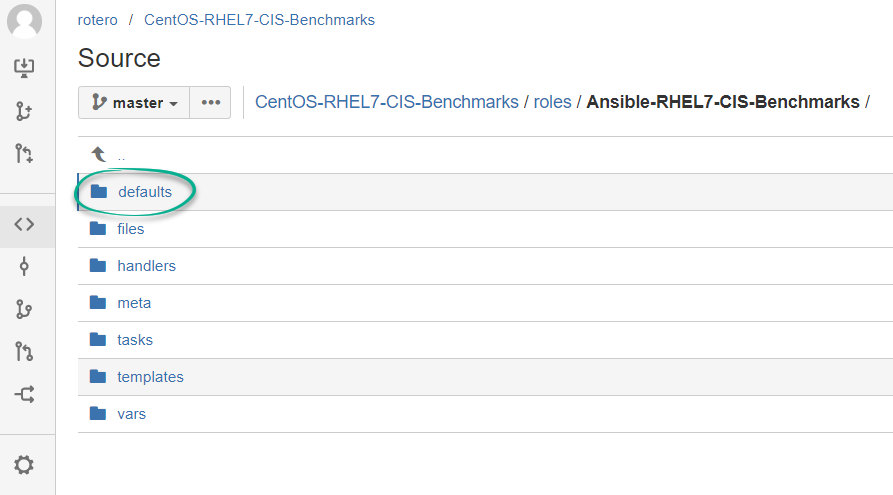
The rhel-playnook.yml can be customized to exclude certain benchmarks labels:

Example of task exclusion in default folder where the main.yml text file exist:



Values which modify the behavior of the role can be modified on the main.yml located in the role’s directory default folder:

CentOS-RHEL7-CIS-Benchmarks/roles/Ansible-RHEL7-CIS-Benchmarks/defaults/main.yml



**Installing and configuring Ansible CIS Benchmarks – Command line**

Best practice is to create a service account as ansible id which would manage the security harden process.

Download Ansible-RHEL7-CIS-Benchmarks from GitHub

<https://github.com/HarryHarcourt/Ansible-RHEL7-CIS-Benchmarks>

Upload to home directory for ansible service account and unzip

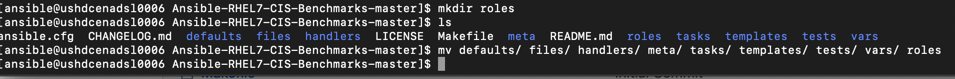
A picture containing food

Description automatically generated

[ansible@ushdcenadsl0006 ~]$ unzip Ansible-RHEL7-CIS-Benchmarks-master.zip

Create roles folder in Ansible-RHEL7-CIS-Benchmarks-master directory

Move the following directories to roles/ Ansible-RHEL7-CIS-Benchmarks – defaults, files, handlers, meta, tasks, templates, tests, vars



Create cis-benchmark-playbooks.yml in using vi in Ansible-RHEL7-CIS-Benchmarks-master directory and add the following lines

A picture containing drawing

Description automatically generated

- hosts: localhost  
 connection: local  
 gather\_facts: true  
 become: yes

roles:  
 - Ansible-RHEL7-CIS-Benchmarks

Update main.yml playbook in roles/vars directory and add – “7.8”

A screenshot of a cell phone

Description automatically generated

**To run the cis-benchjmark-playbooks.yml change directory to the home of Ansible-RHEL7-CIS-Benchmarks-master**

[ansible@ushdcenadsl0006 Ansible-RHEL7-CIS-Benchmarks-master]$ ansible-playbook cis-benchmark-playbooks.yml -t 1.1.1.1

**To run only specific task of the playbook use the number for example 1.1.1.1**

Output:

A screenshot of a cell phone

Description automatically generated

**Running with -C option**

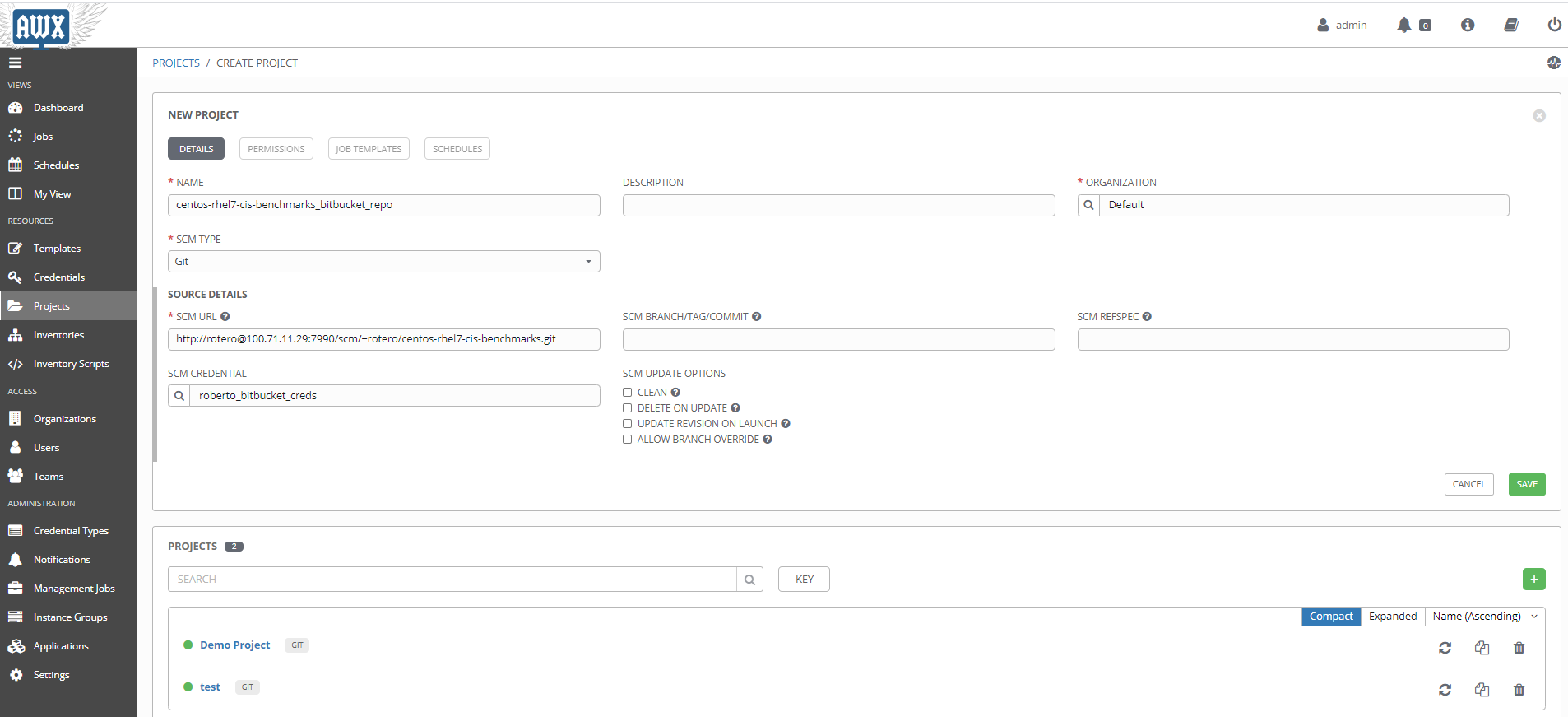
[ansible@ushdcenadsl0006 Ansible-RHEL7-CIS-Benchmarks-master]$ ansible-playbook -C cis-benchmark-playbooks.yml -t 6.2.6

-C, --check don't make any changes; instead, try to predict some of the changes that may occur

# Configure and setup RedHat hardening playbook repository in awx tower

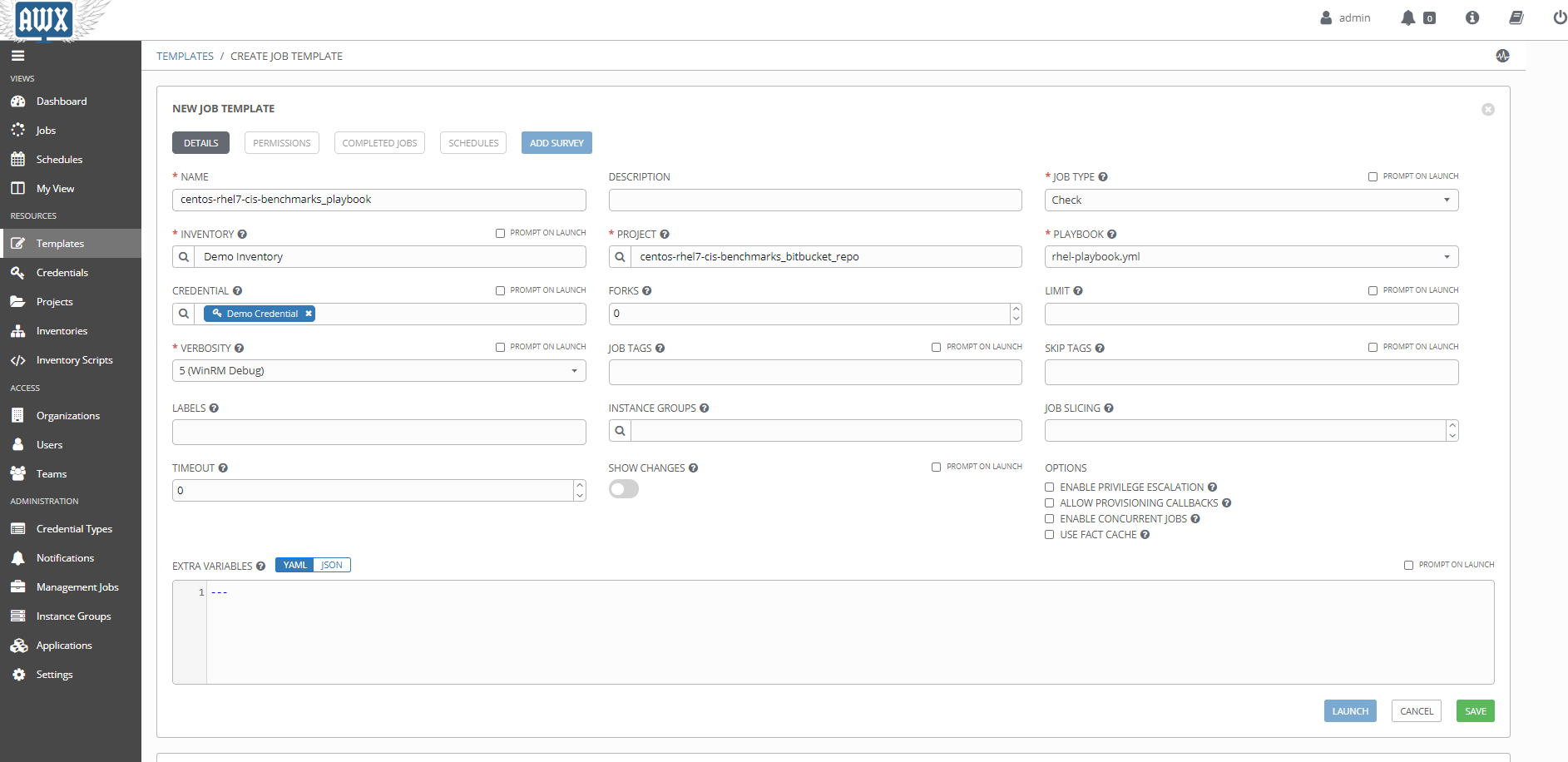
Create a project with a name then add repo url under source details:

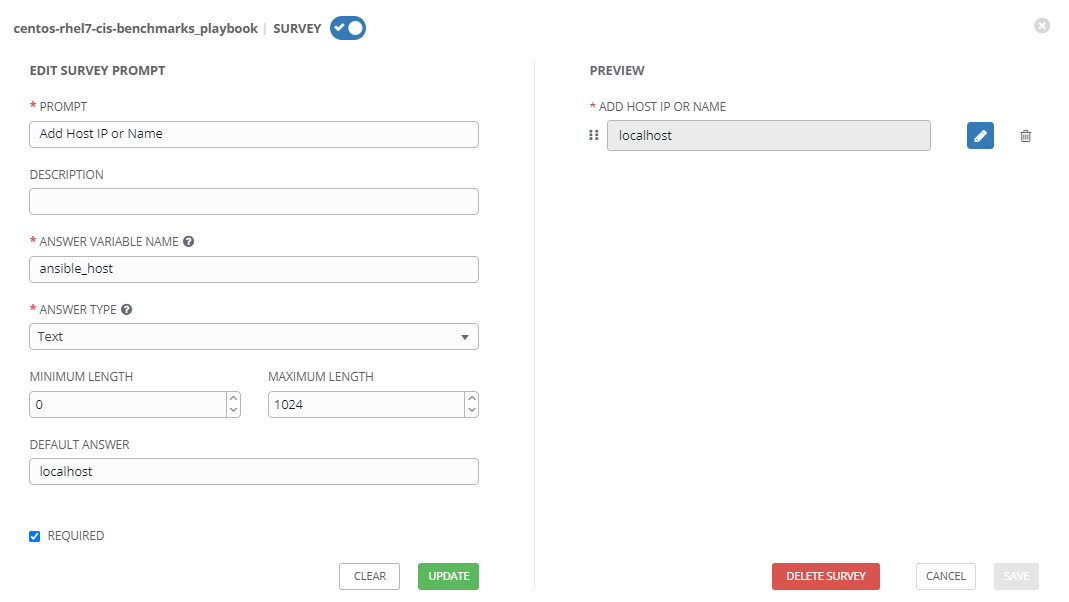
Example repo name: centos-rhel7-cis-benchmarks\_bitbucket\_repo



Create job template to run Redhat hardening playbook.

Create template add a descriptive name, import project repository then save and launch template.





Create survey to target specific server’s using a variable:

* Add name + description of prompt
* Add variable: ansible\_host
* Add answer type in our case is our localhost will use this as default

# Check and update /etc/sudoers files

Validate system administrator access who has been provided access

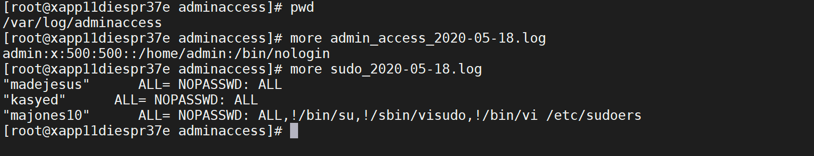
Validate system administrators who has been provided root and admin access on the server. In this example kasyed and madejesus was approved to have root access through sudo.



If the SOG ID of the system administrators are not listed in /etc/sudoers file, then proceed of updating similar output listed above.

# Validate logs file

Check logs files for sudo and admin logs to confirm the adminaccess script job completed



If there are no output logs for sudo and admin, re-run the adminaccess script manually to generate the logs files.

# Confirm Splunk services are running

Confirm Splunk services are running and listening on proper port

Sudo to splunk service account ID and confirm the splunk services has been started on port 8089

$ /data/splunkforwarder/bin/splunk set deploy-poll 167.195.161.39:8089

$ /data/splunkforwarder/bin/splunk restart

If the splunk services are not able to start on 8089 then a firewall request is required to be submitted to open the port and allow to communicate to the splunk server.

If the splunk tool is not installed on the server, request for the splunk installation documentation.

Confirm with splunk administrator logs being consumed and reporting on dashboard

Contact Deloitte project team splunk administrator Karthik K LV to confirm that logs are being consumed onto splunk reporting dashboard.

# Appendix

1. Installing nmap package

A screenshot of a cell phone

Description automatically generated

Check for the goferd communication

Satellite goferd agent

[root@xapt11diespt02e etc]# /usr/sbin/ss -napt | grep 5647

ESTAB 0 0 167.195.161.133:38020 167.195.91.81:5647 users:(("python",10940,9))

<https://www.hackingarticles.in/generating-scan-reports-using-nmap-output-scan/>

# Architecture

The components that make up this solution are defined below. These components work together to provide the necessary access, control, security and reporting necessary for the GA IES project.

1. Nmap

**About Deloitte**

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's 165,000 professionals are committed to becoming the standard of excellence.

Deloitte's professionals are unified by a collaborative culture that fosters integrity, outstanding value to markets and clients, commitment to each other, and strength from cultural diversity. They enjoy an environment of continuous learning, challenging experiences, and enriching career opportunities. Deloitte's professionals are dedicated to strengthening corporate responsibility, building public trust, and making a positive impact in their communities.

Deloitte refers to one or more of Deloitte Touche Tohmatsu, a Swiss Verein, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu and its member firms. Please see <http://www.deloitte.com/us/about> for a detailed description of the legal structure of Deloitte LLP and its subsidiaries.

Internal Usage Statement

This publication is for internal distribution and use only among personnel of Deloitte Touche Tohmatsu, its member firms, and its and their affiliates. Deloitte Touche Tohmatsu, its member firms, and its and their affiliates shall not be responsible for any loss whatsoever sustained by any person who relies on this publication.

Copyright © 2012 Deloitte Development LLC. All rights reserved.

Member of Deloitte Touche Tohmatsu