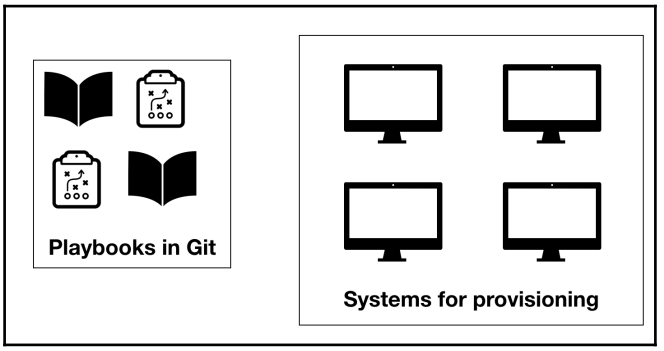
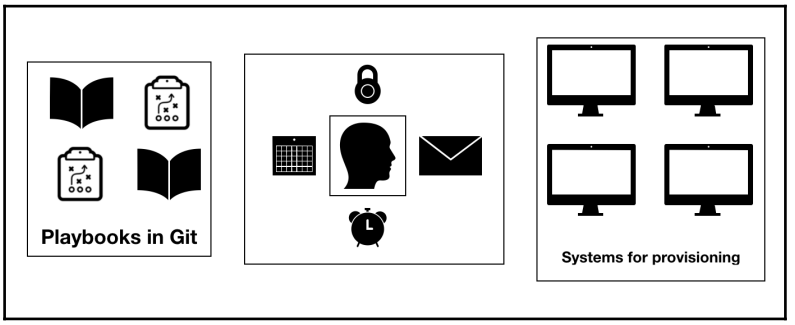
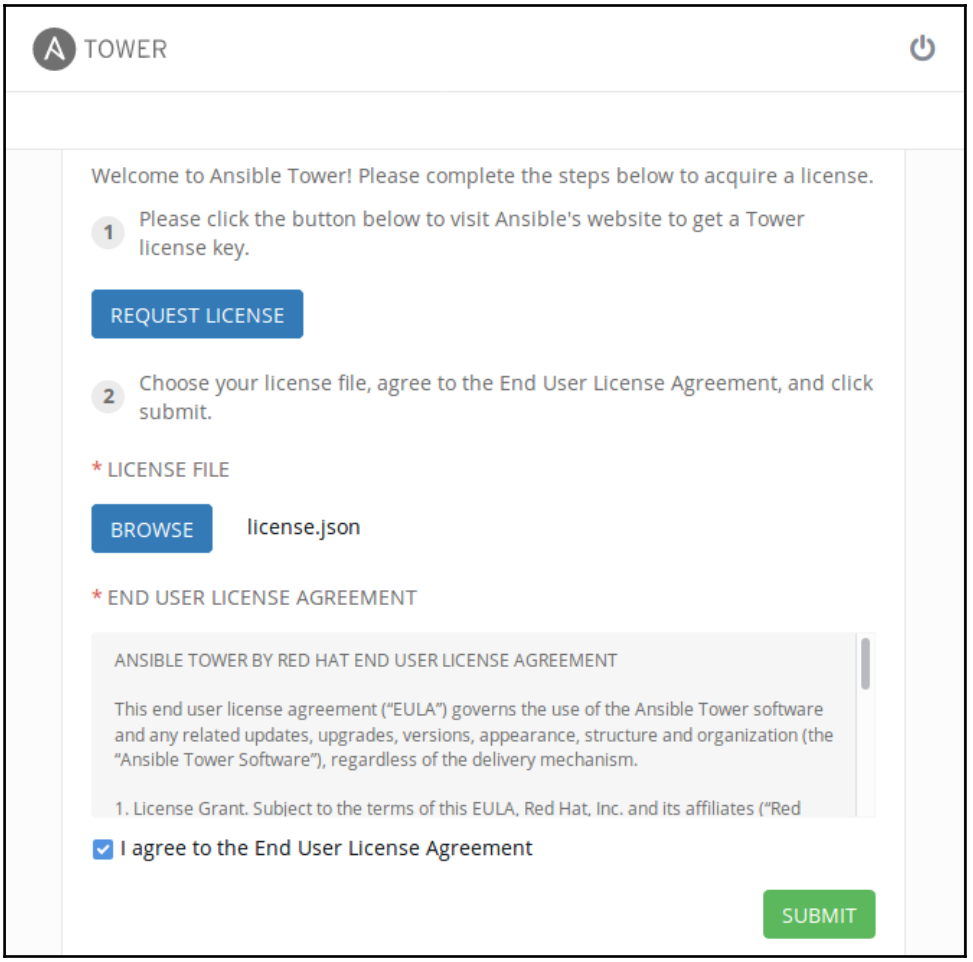
Chapter 02: Ansible Tower, Jenkins, and Other Automation Tools

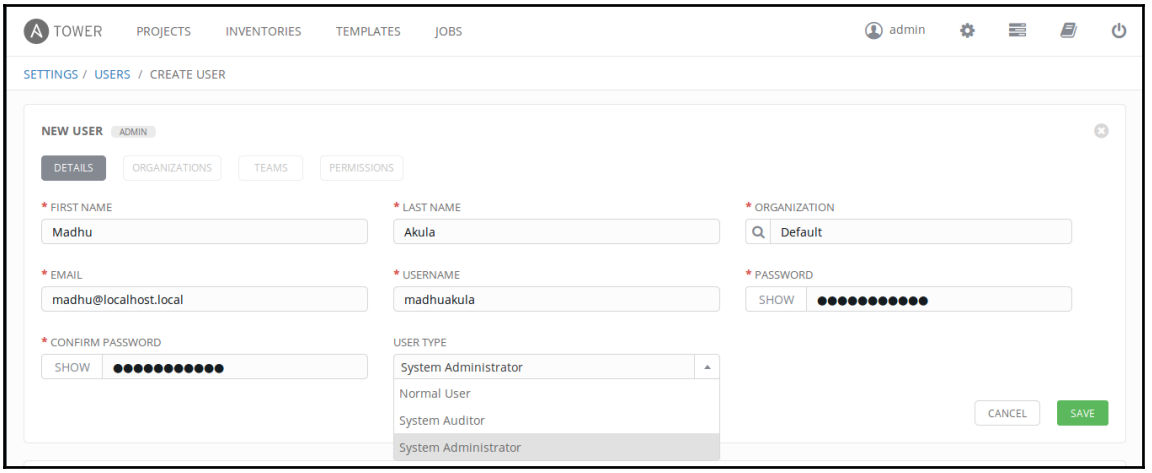





```
Welcome to Ansible Tower!

Log into the web interface here:

  https://10.42.0.42/

  Username: admin
  Password: LCBy27cxLStF

The documentation for Ansible Tower is available here:

  http://www.ansible.com/tower/

For help, visit  http://support.ansible.com/
```

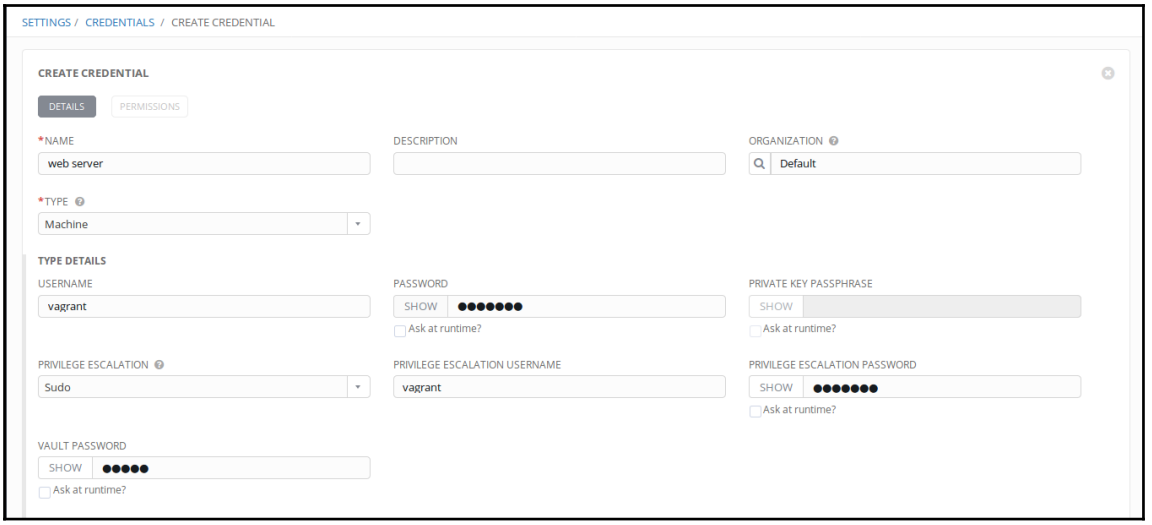

ANSIBLE
TOWER
by Red Hat
Welcome to Ansible Tower! Please sign in.
USERNAME
admin
PASSWORD
SIGN IN

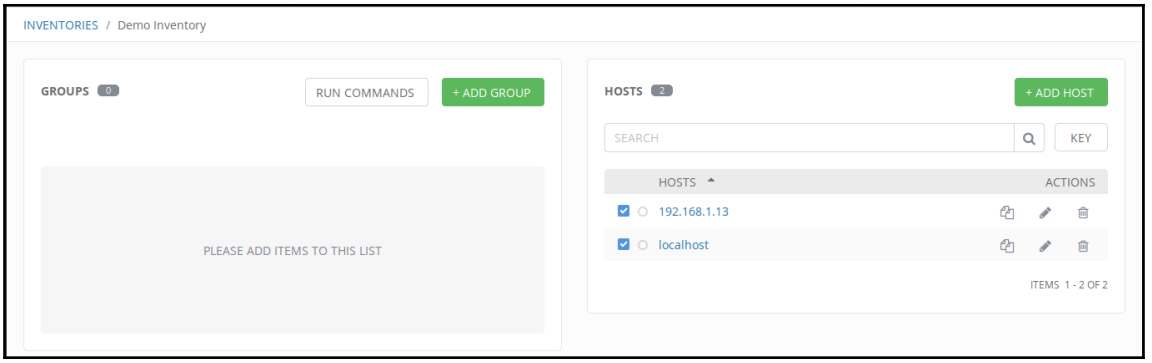

TOWER
Welcome to Ansible Tower! Please complete the steps below to acquire a license.
1
Please click the button below to visit Ansible's website to get a Tower license key.
REQUEST LICENSE
2
Choose your license file, agree to the End User License Agreement, and click submit.
* LICENSE FILE
BROWSE
license.json
* END USER LICENSE AGREEMENT
ANSIBLE TOWER BY RED HAT END USER LICENSE AGREEMENT
This end user license agreement ("EULA") governs the use of the Ansible Tower software and any related updates, upgrades, versions, appearance, structure and organization (the "Ansible Tower Software"), regardless of the delivery mechanism.
1. License Grant. Subject to the terms of this EULA, Red Hat, Inc. and its affiliates ("Red
I agree to the End User License Agreement
SUBMIT

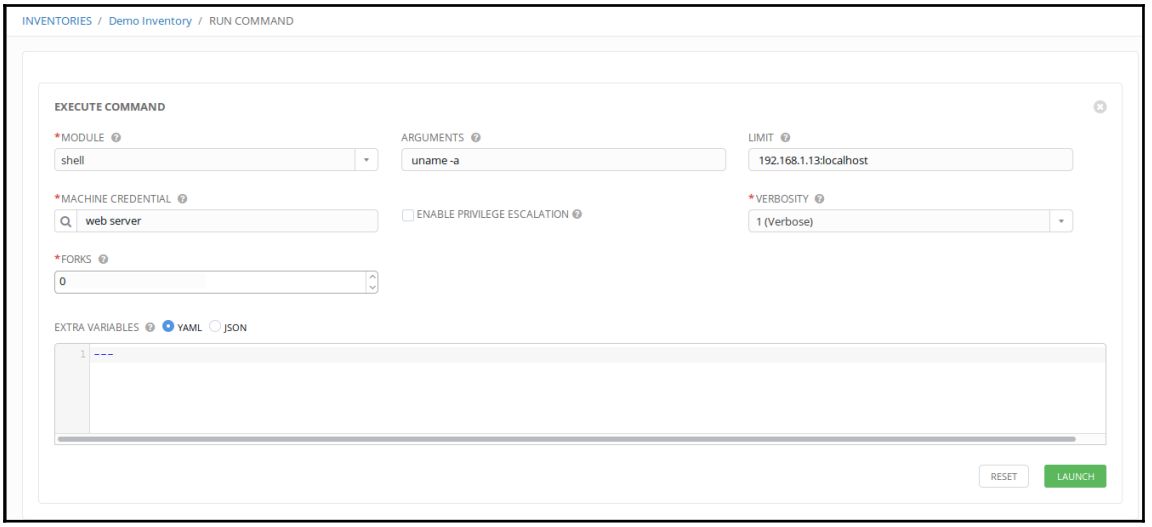

TOWER
PROJECTS
INVENTORIES
TEMPLATES
JOBS
admin
SETTINGS / USERS / CREATE USER
NEW USER
ADMIN
DETAILS
ORGANIZATIONS
TEAMS
PERMISSIONS
* FIRST NAME
Madhu
* LAST NAME
Akula
* ORGANIZATION
Default
* EMAIL
madhu@localhost.local
* USERNAME
madhuakula
* PASSWORD
SHOW
* CONFIRM PASSWORD
SHOW
USER TYPE
System Administrator
Normal User
System Auditor
System Administrator
CANCEL
SAVE


INVENTORIES / Demo Inventory / CREATE HOST
CREATE HOST
ON
* HOST NAME
192.168.1.13
DESCRIPTION
web server
VARIABLES
YAML
JSON
1

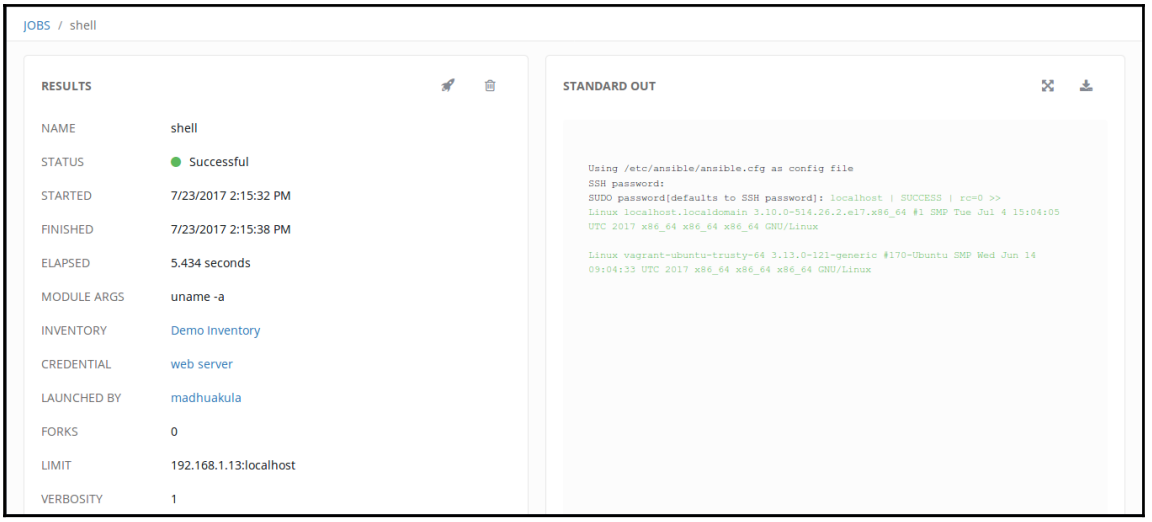
CANCEL
SAVE

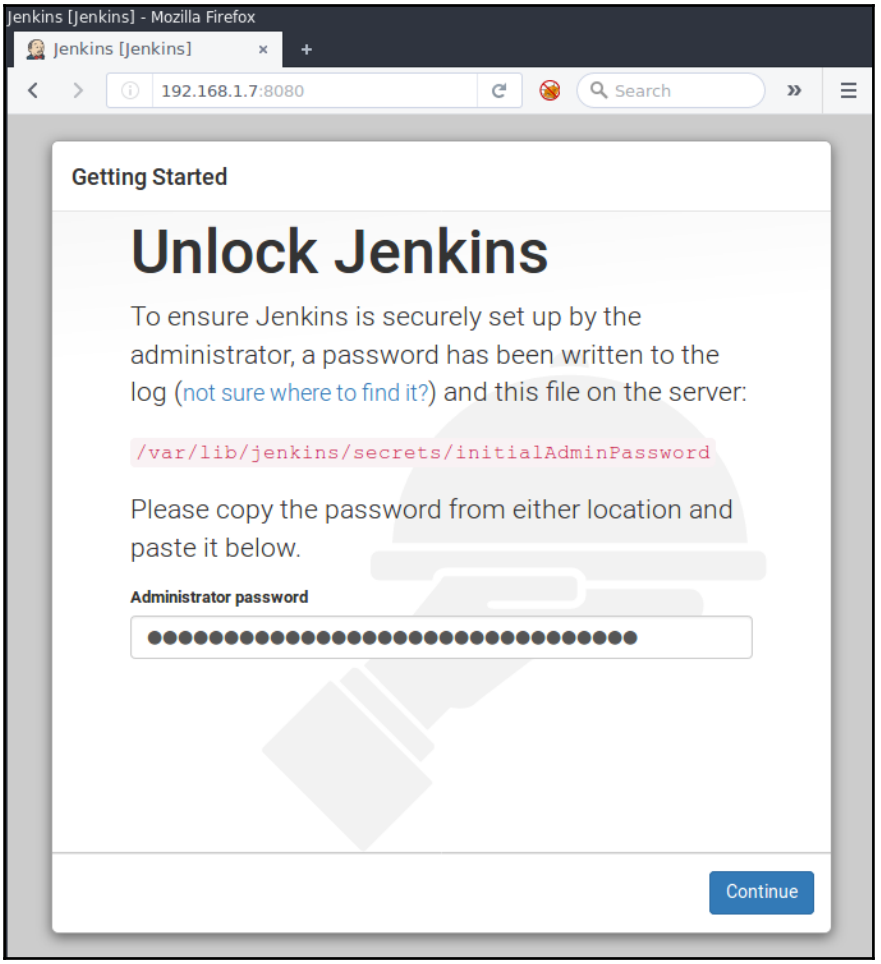

SETTINGS / CREDENTIALS / CREATE CREDENTIAL
CREATE CREDENTIAL
DETAILS
PERMISSIONS
*NAME
web server
DESCRIPTION
ORGANIZATION
Default
*TYPE
Machine
TYPE DETAILS
USERNAME
vagrant
PASSWORD
SHOW
Ask at runtime?
PRIVATE KEY PASSPHRASE
SHOW
Ask at runtime?
PRIVILEGE ESCALATION
Sudo
PRIVILEGE ESCALATION USERNAME
vagrant
PRIVILEGE ESCALATION PASSWORD
SHOW
Ask at runtime?
VAULT PASSWORD
SHOW
Ask at runtime?

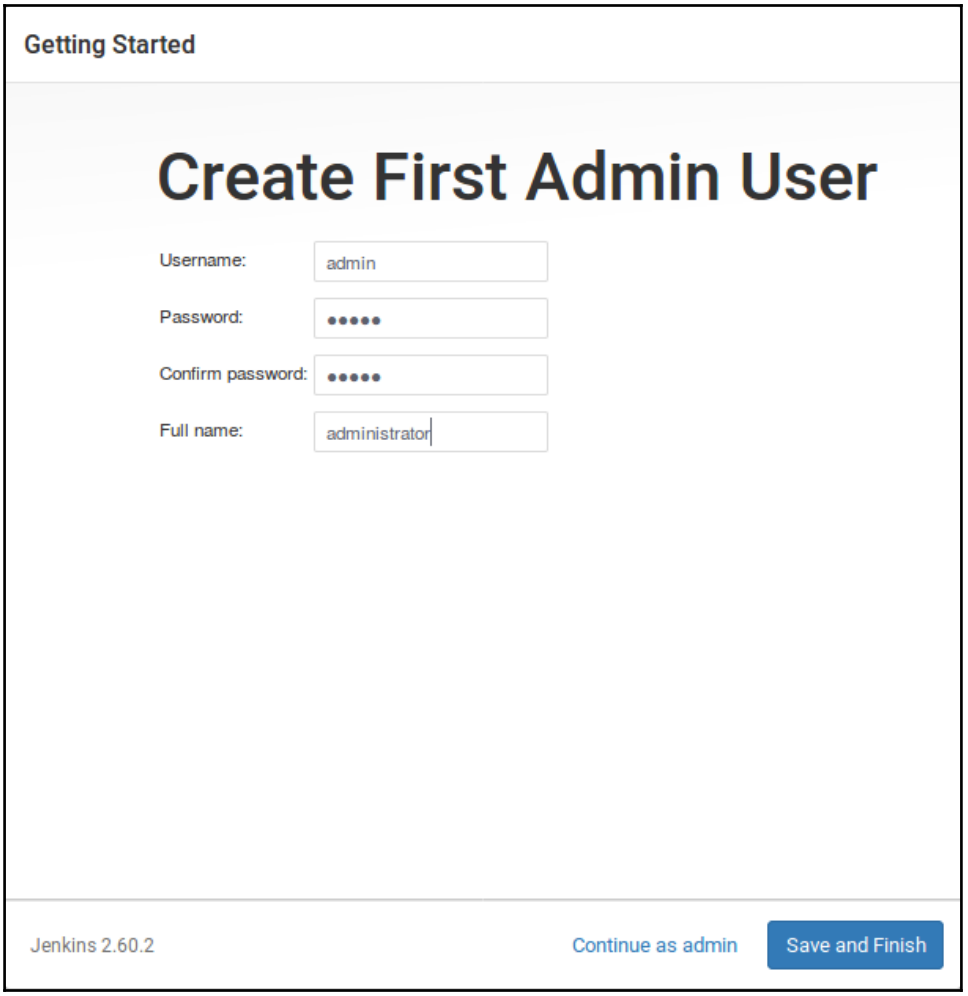

INVENTORIES / Demo Inventory
GROUPS 0
RUN COMMANDS
+ ADD GROUP
PLEASE ADD ITEMS TO THIS LIST
HOSTS 2
+ ADD HOST
SEARCH
KEY
HOSTS
ACTIONS
192.168.1.13
localhost
ITEMS 1 - 2 OF 2

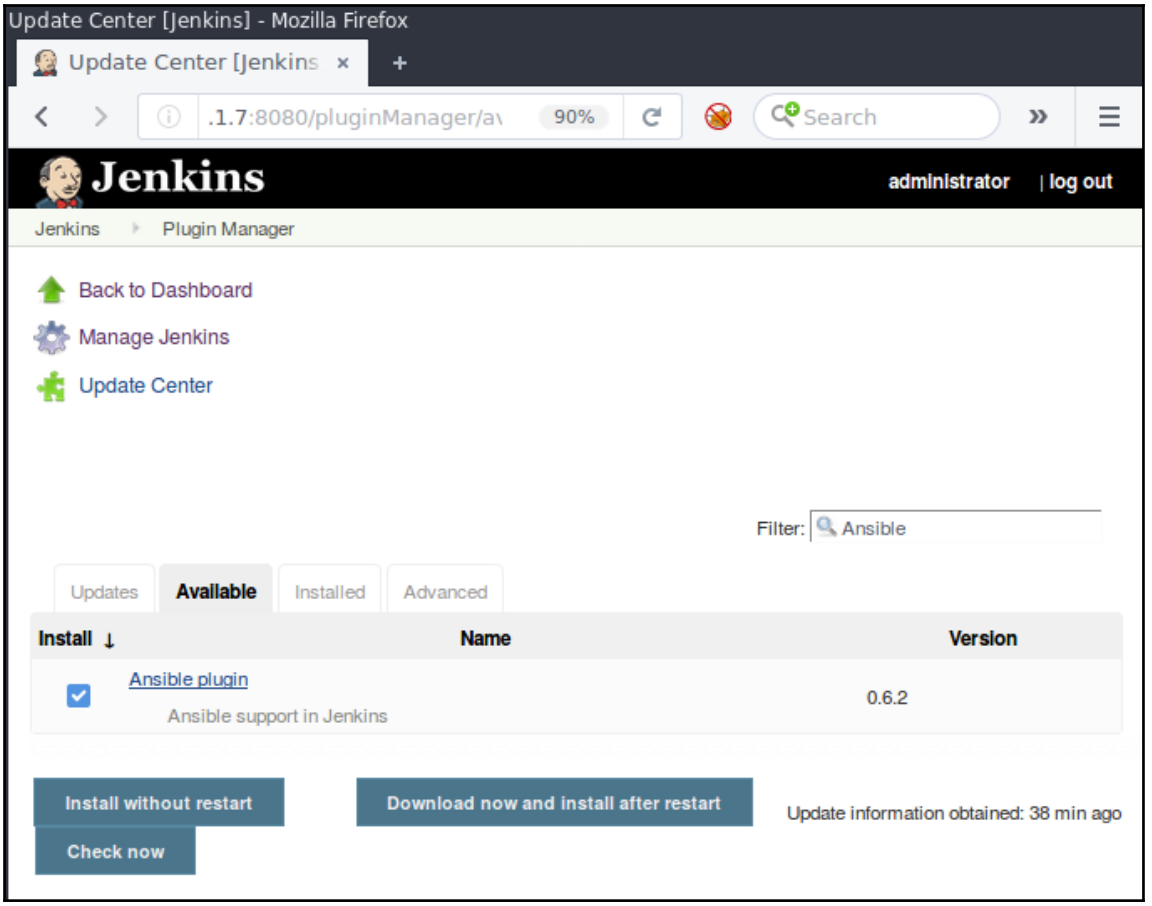

INVENTORIES / Demo Inventory / RUN COMMAND
EXECUTE COMMAND
*MODULE
shell
ARGUMENTS
uname -a
LIMIT
192.168.1.13:localhost
*MACHINE CREDENTIAL
web server
ENABLE PRIVILEGE ESCALATION
*VERBOSITY
1 (Verbose)
*FORKS
0
EXTRA VARIABLES
YAML
JSON

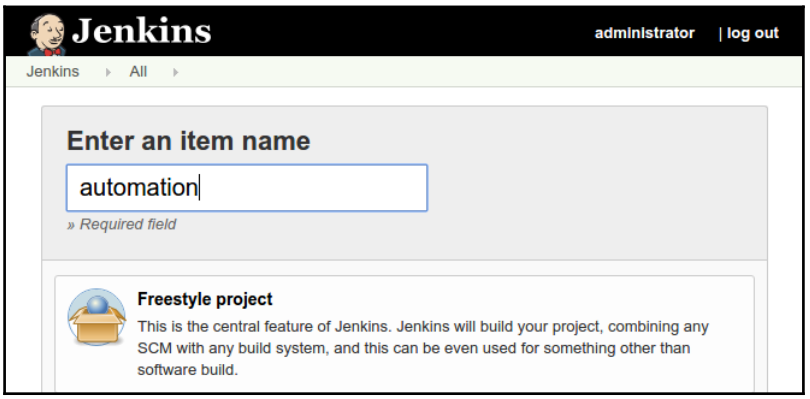
RESET
LAUNCH

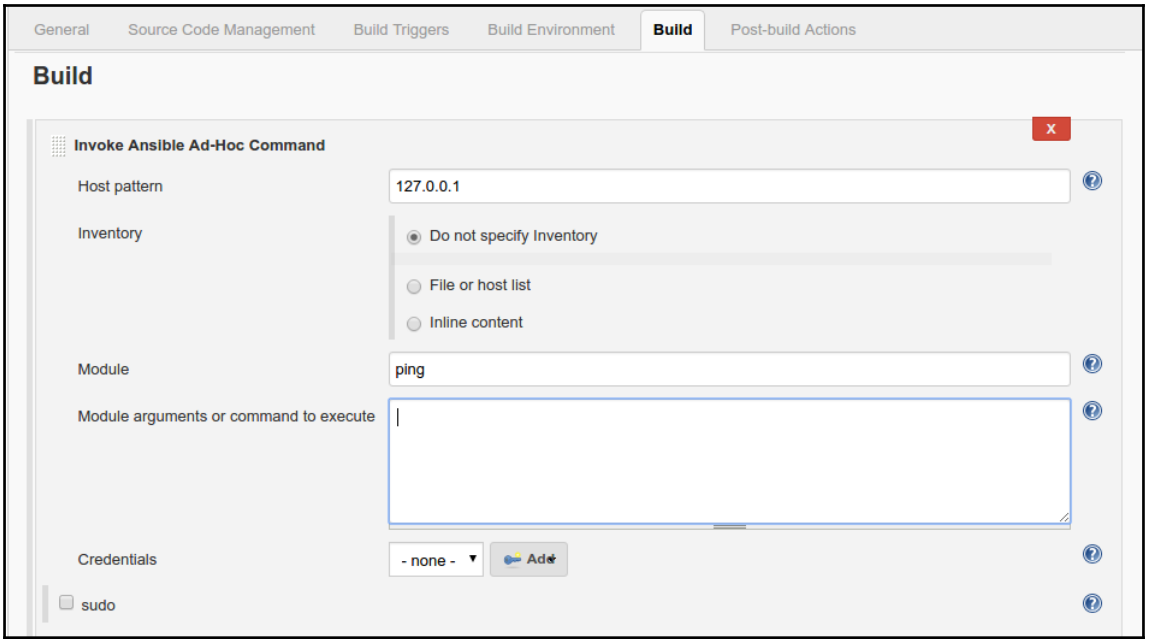

JOBS / shell
RESULTS
NAME shell
STATUS Successful
STARTED 7/23/2017 2:15:32 PM
FINISHED 7/23/2017 2:15:38 PM
ELAPSED 5.434 seconds
MODULE ARGS uname -a
INVENTORY Demo Inventory
CREDENTIAL web server
LAUNCHED BY madhuakula
FORKS 0
LIMIT 192.168.1.13:localhost
VERBOSITY 1
STANDARD OUT
Using /etc/ansible/ansible.cfg as config file
SSH password:
SUDO password[defaults to SSH password]: localhost | SUCCESS | rc=0 >>
Linux localhost.localdomain 3.10.0-514.26.2.el7.x86_64 #1 SMP Tue Jul 4 15:04:05 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
Linux vagrant-ubuntu-trusty-64 3.13.0-121-generic #170-Ubuntu SMP Wed Jun 14 09:04:33 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux

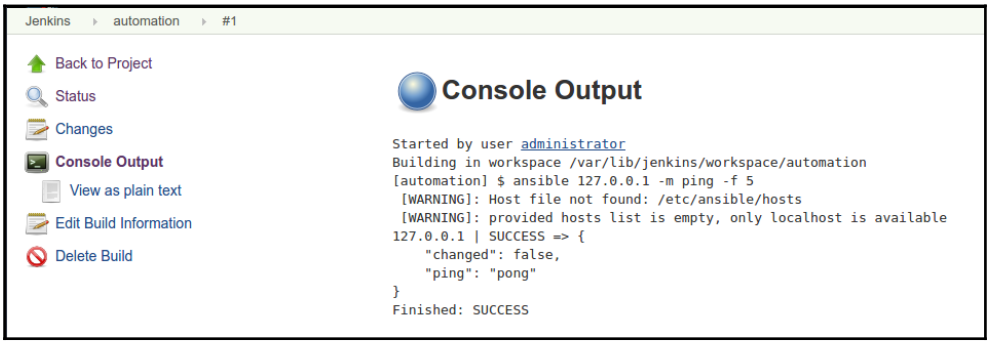

Jenkins [Jenkins] - Mozilla Firefox
Jenkins [Jenkins]
192.168.1.7:8080
Search
Getting Started
Unlock Jenkins
To ensure Jenkins is securely set up by the administrator, a password has been written to the log (not sure where to find it?) and this file on the server:
/var/lib/jenkins/secrets/initialAdminPassword
Please copy the password from either location and paste it below.
Administrator password
Continue

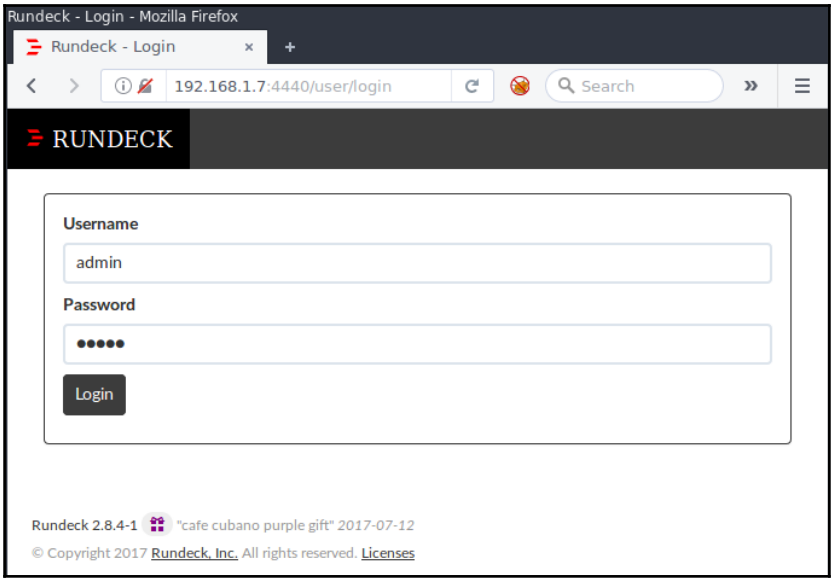

Getting Started
Create First Admin User
Username:
admin
Password:
Confirm password:
Full name:
administrator
Jenkins 2.60.2
Continue as admin
Save and Finish

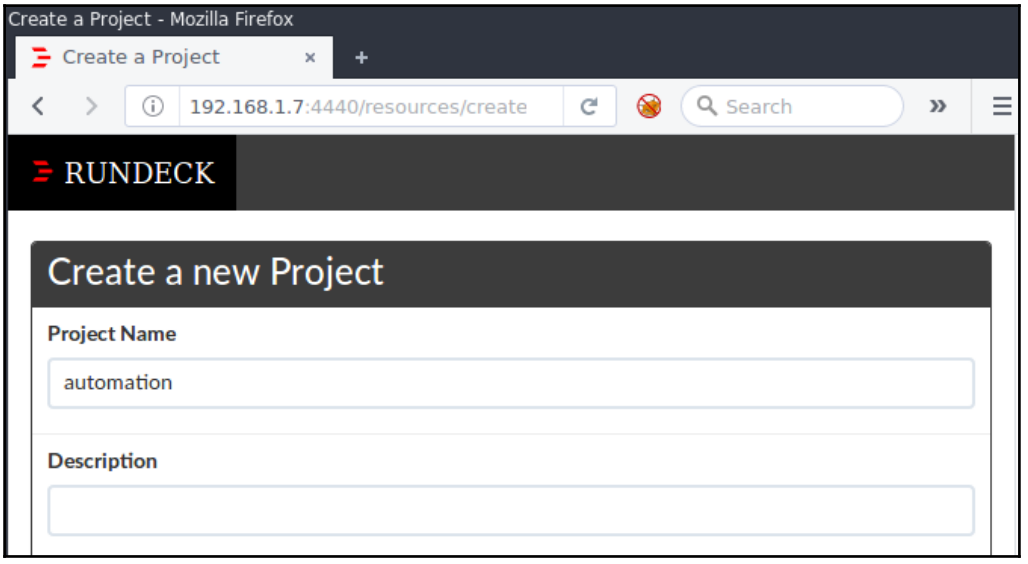

Update Center [Jenkins] - Mozilla Firefox
Update Center [Jenkins
.1.7:8080/pluginManager/a
90%
Search
Jenkins
administrator
| log out
Jenkins
Plugin Manager
Back to Dashboard
Manage Jenkins
Update Center
Filter:
Ansible
Updates
Available
Installed
Advanced
Install
Name
Version
Ansible plugin
Ansible support in Jenkins
0.6.2
Install without restart
Download now and install after restart
Update information obtained: 38 min ago
Check now

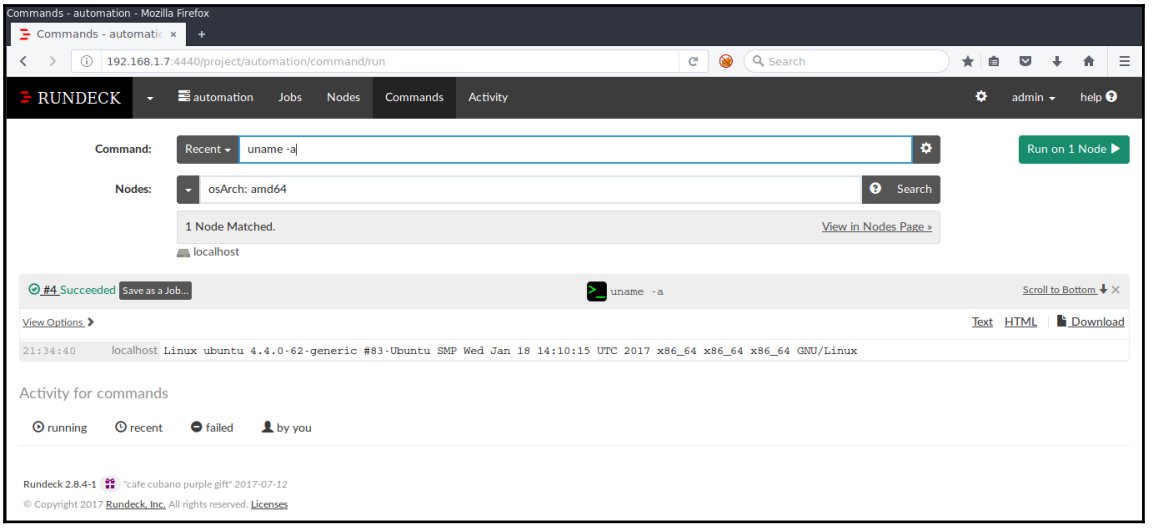

Jenkins
administrator
| log out
Jenkins
All
Enter an item name
automation
» Required field
Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.

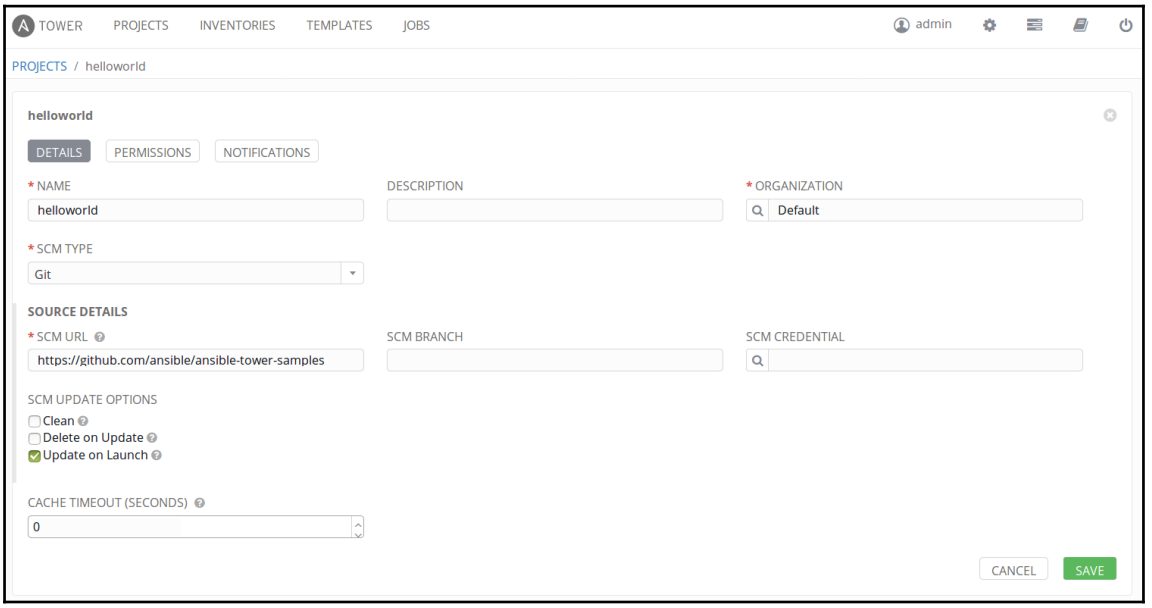

General
Source Code Management
Build Triggers
Build Environment
Build
Post-build Actions
Build
Invoke Ansible Ad-Hoc Command
Host pattern
127.0.0.1
Inventory
Do not specify Inventory
File or host list
Inline content
Module
ping
Module arguments or command to execute
Credentials
- none -
Add
sudo

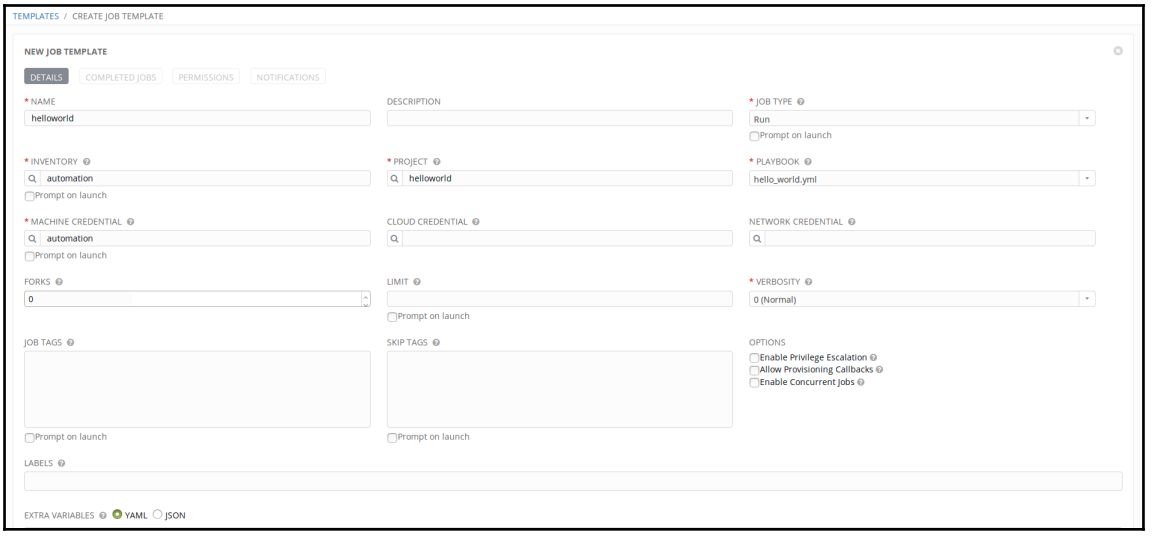

Jenkins
automation
#1
Back to Project
Status
Changes
Console Output
View as plain text
Edit Build Information
Delete Build
Console Output
Started by user administrator
Building in workspace /var/lib/jenkins/workspace/automation
[automation] $ ansible 127.0.0.1 -m ping -f 5
[WARNING]: Host file not found: /etc/ansible/hosts
[WARNING]: provided hosts list is empty, only localhost is available
127.0.0.1 | SUCCESS => {
"changed": false,
"ping": "pong"
}
Finished: SUCCESS

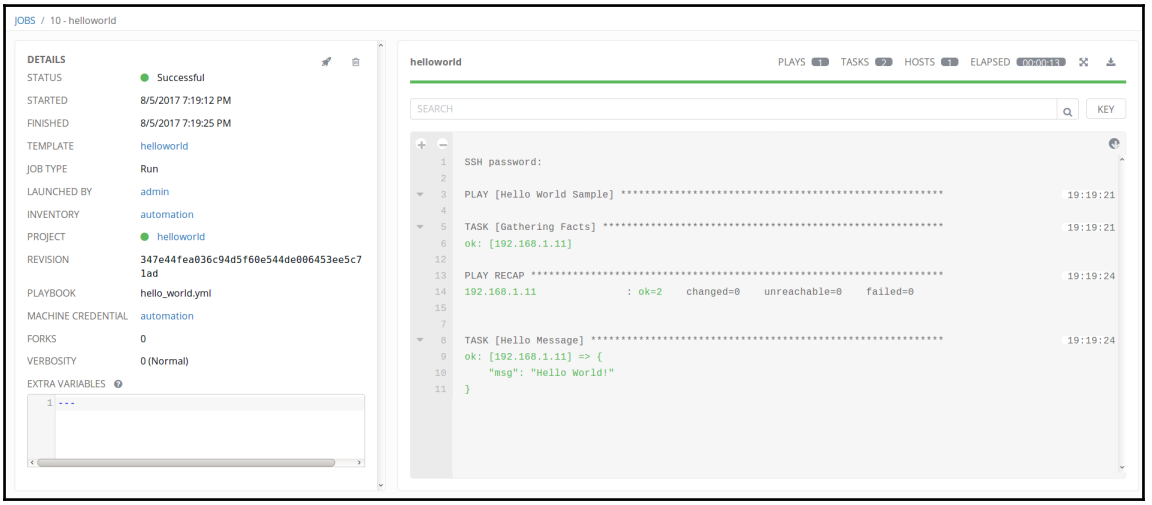

Rundeck - Login - Mozilla Firefox
Rundeck - Login
192.168.1.7:4440/user/login
Search
RUNDECK
Username
admin
Password
Login
Rundeck 2.8.4-1 "cafe cubano purple gift" 2017-07-12
© Copyright 2017 Rundeck, Inc. All rights reserved. Licenses


Create a Project - Mozilla Firefox
Create a Project
192.168.1.7:4440/resources/create
Search
RUNDECK
Create a new Project
Project Name
automation
Description

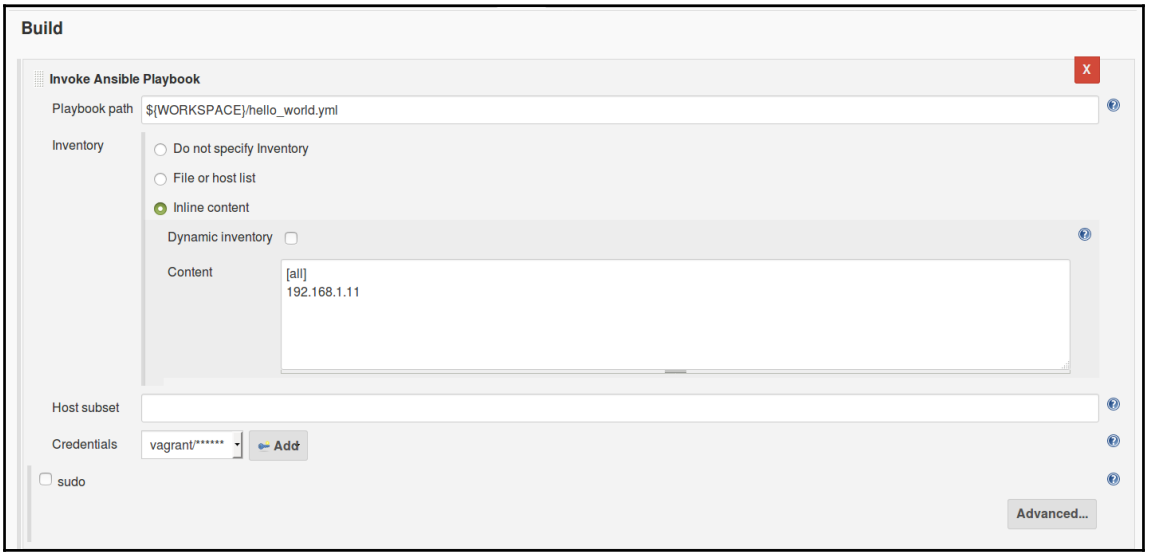

Commands - automation - Mozilla Firefox
192.168.1.7:4440/project/automation/command/run
RUNDECK
automation
Jobs
Nodes
Commands
Activity
admin
help
Command:
Recent
uname -a
Run on 1 Node
Nodes:
osArch: amd64
Search
1 Node Matched.
View in Nodes Page »
localhost
#4 Succeeded
Save as a Job...
uname -a
Scroll to Bottom
View Options
Text
HTML
Download
21:34:40 localhost Linux ubuntu 4.4.0-62-generic #83-Ubuntu SMP Wed Jan 18 14:10:15 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
Activity for commands
running
recent
failed
by you
Rundeck 2.8.4-1
"cafe cubano purple gift" 2017-07-12
© Copyright 2017 Rundeck, Inc. All rights reserved. Licenses


TOWER
PROJECTS
INVENTORIES
TEMPLATES
JOBS
admin
PROJECTS / helloworld
helloworld
DETAILS
PERMISSIONS
NOTIFICATIONS
* NAME
helloworld
DESCRIPTION
* ORGANIZATION
Default
* SCM TYPE
Git
SOURCE DETAILS
* SCM URL
https://github.com/ansible/ansible-tower-samples
SCM BRANCH
SCM CREDENTIAL
SCM UPDATE OPTIONS
Clean
Delete on Update
Update on Launch
CACHE TIMEOUT (SECONDS)
0
CANCEL
SAVE

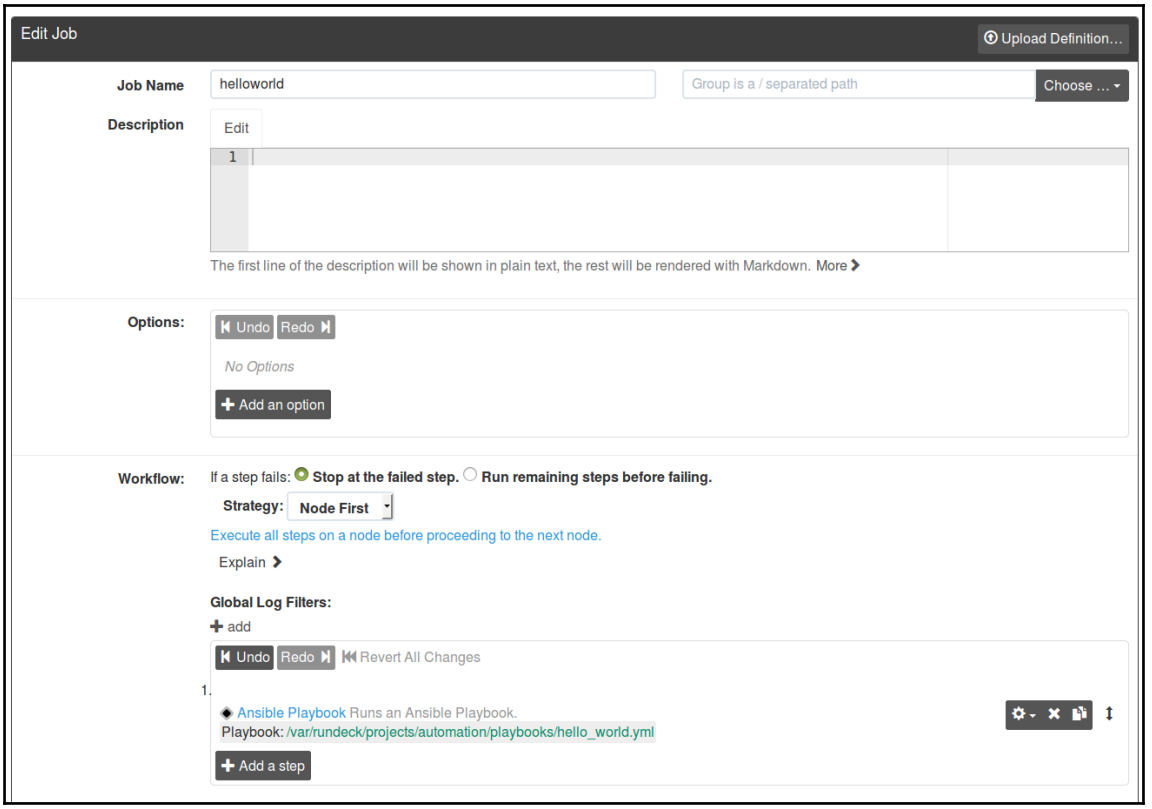

TEMPLATES / CREATE JOB TEMPLATE
NEW JOB TEMPLATE
DETAILS
COMPLETED JOBS
PERMISSIONS
NOTIFICATIONS
* NAME
helloworld
DESCRIPTION
* JOB TYPE
Run
Prompt on launch
* INVENTORY
automation
Prompt on launch
* PROJECT
helloworld
* PLAYBOOK
hello_world.yml
* MACHINE CREDENTIAL
automation
Prompt on launch
CLOUD CREDENTIAL
NETWORK CREDENTIAL
FORKS
0
LIMIT
Prompt on launch
* VERBOSITY
0 (Normal)
JOB TAGS
Prompt on launch
SKIP TAGS
Prompt on launch
OPTIONS
Enable Privilege Escalation
Allow Provisioning Callbacks
Enable Concurrent Jobs
LABELS
EXTRA VARIABLES
YAML
JSON

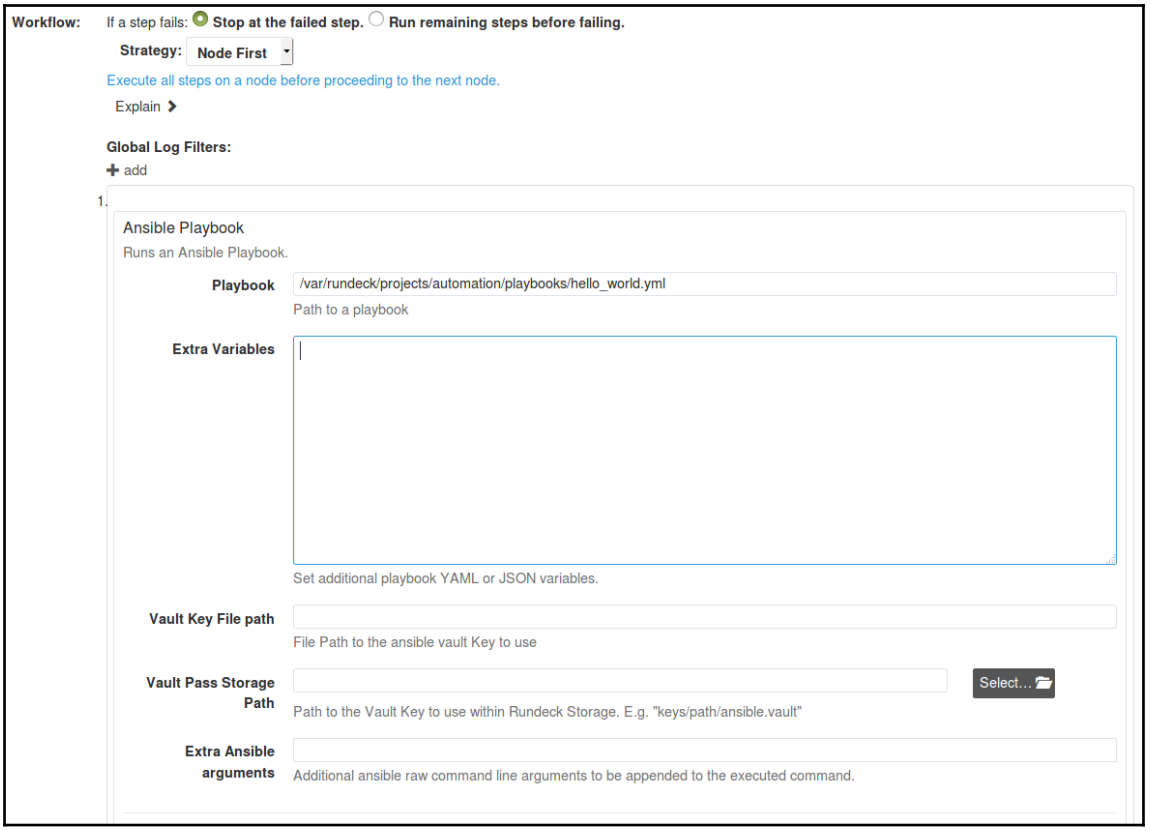

JOBS / 10 - helloworld
DETAILS
STATUS
Successful
STARTED
8/5/2017 7:19:12 PM
FINISHED
8/5/2017 7:19:25 PM
TEMPLATE
helloworld
JOB TYPE
Run
LAUNCHED BY
admin
INVENTORY
automation
PROJECT
helloworld
REVISION
347e44fea036c94d5f60e544de006453ee5c71ad
PLAYBOOK
hello_world.yml
MACHINE CREDENTIAL
automation
FORKS
0
VERBOSITY
0 (Normal)
EXTRA VARIABLES
---
helloworld
PLAYS 1
TASKS 2
HOSTS 1
ELAPSED 00:00:13
SEARCH
KEY
SSH password:
PLAY [Hello World Sample] ********** 19:19:21
TASK [Gathering Facts] ********** 19:19:21
ok: [192.168.1.11]
PLAY RECAP ********** 19:19:24
192.168.1.11 : ok=2 changed=0 unreachable=0 failed=0
TASK [Hello Message] ********** 19:19:24
ok: [192.168.1.11] => {
"msg": "Hello World!"
}

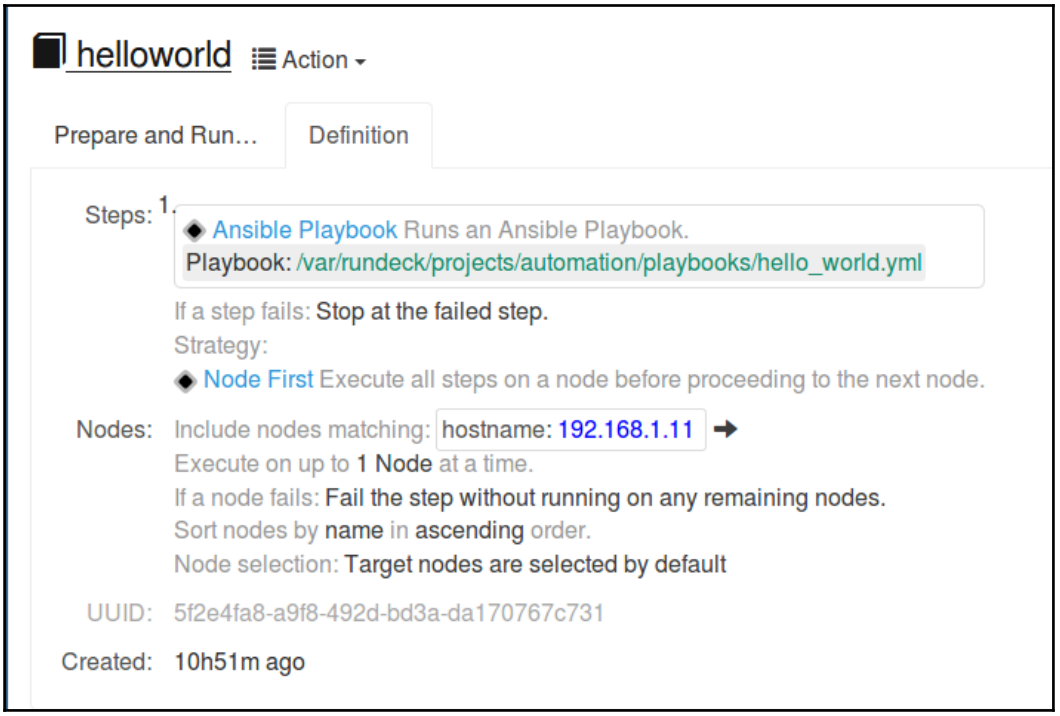

Source Code Management
None
Git
Repositories
Repository URL
https://github.com/ansible/ansible-tower-samples
Credentials
- none -
Add
Advanced...
Add Repository
Branches to build
Branch Specifier (blank for 'any')
*/master
Add Branch
Repository browser
(Auto)
Additional Behaviours
Add
Subversion

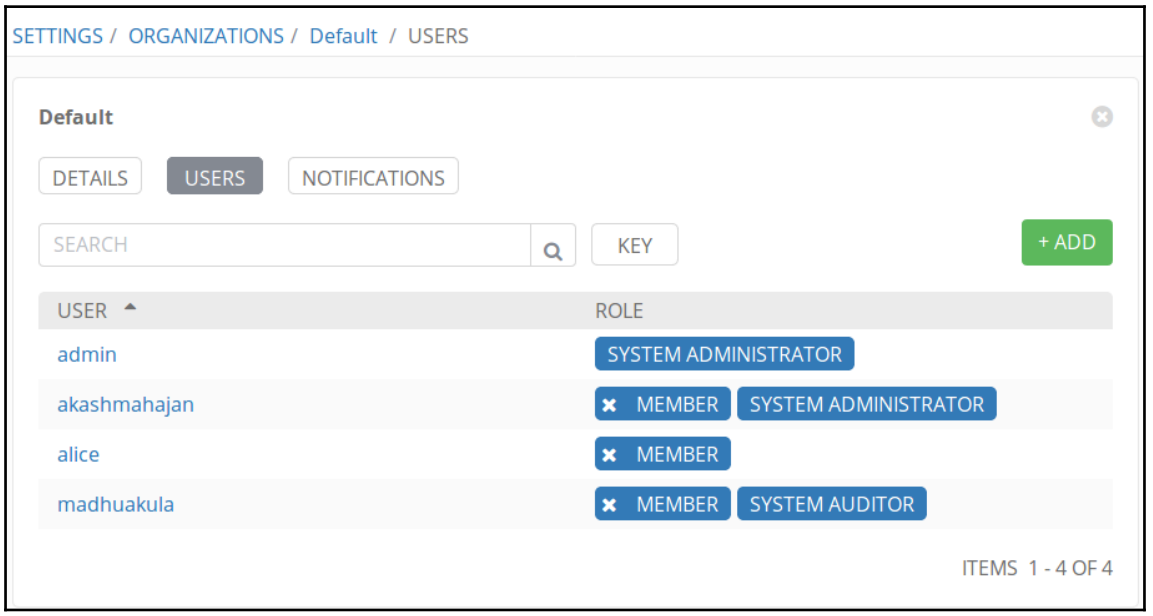

Build
Invoke Ansible Playbook
Playbook path
${WORKSPACE}/hello_world.yml
Inventory
Do not specify Inventory
File or host list
Inline content
Dynamic inventory
Content
[all]
192.168.1.11
Host subset
Credentials
vagrant/******
Add
sudo
Advanced...

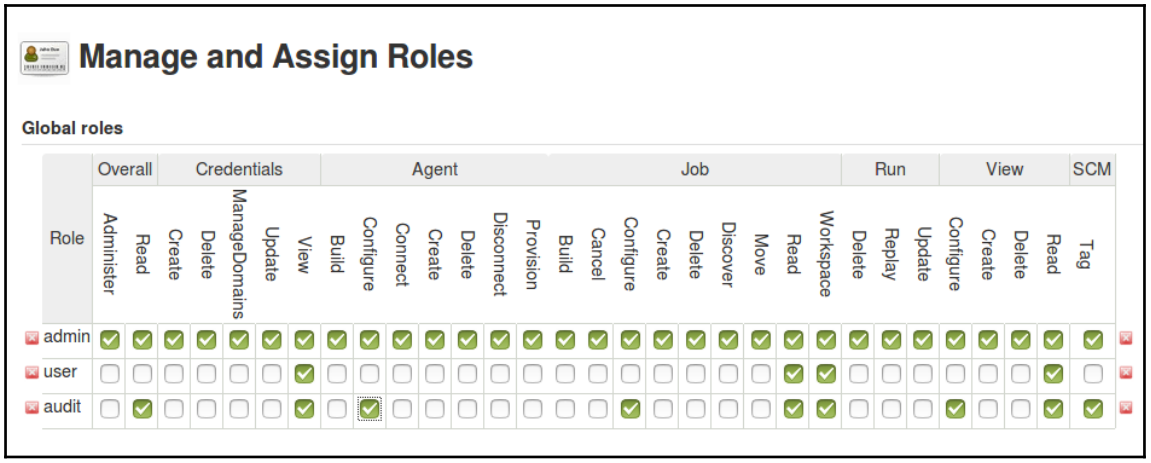

Jenkins
search
administrator | log out
Jenkins › automation › #13
Back to Project
Status
Changes
Console Output
View as plain text
Edit Build Information
Delete Build
Git Build Data
No Tags
Previous Build
Next Build
Console Output
Started by user administrator
Building in workspace /var/lib/jenkins/workspace/automation
> git rev-parse --is-inside-work-tree # timeout=10
Fetching changes from the remote Git repository
> git config remote.origin.url https://github.com/ansible/ansible-tower-samples # timeout=10
Fetching upstream changes from https://github.com/ansible/ansible-tower-samples
> git --version # timeout=10
using GIT_ASKPASS to set credentials
> git fetch --tags --progress https://github.com/ansible/ansible-tower-samples +refs/heads/*:refs/remotes/origin/*
> git rev-parse refs/remotes/origin/master^{commit} # timeout=10
> git rev-parse refs/remotes/origin/origin/master^{commit} # timeout=10
Checking out Revision 347e44fea036c94d5f60e544de006453ee5c71ad (refs/remotes/origin/master)
Commit message: "Initial hello world playbook"
> git config core.sparsecheckout # timeout=10
> git checkout -f 347e44fea036c94d5f60e544de006453ee5c71ad
> git rev-list 347e44fea036c94d5f60e544de006453ee5c71ad # timeout=10
[automation] $ sshpass ******** ansible-playbook /var/lib/jenkins/workspace/automation/hello_world.yml -i /tmp/inventory1378971762319225309.ini -f 5 -u vagrant -k
PLAY [Hello World Sample] **
GATHERING FACTS ***
ok: [192.168.1.11]
TASK: [Hello Message] ***
ok: [192.168.1.11] => {
"msg": "Hello World!"
}
PLAY RECAP **
192.168.1.11 : ok=2 changed=0 unreachable=0 failed=0
Finished: SUCCESS

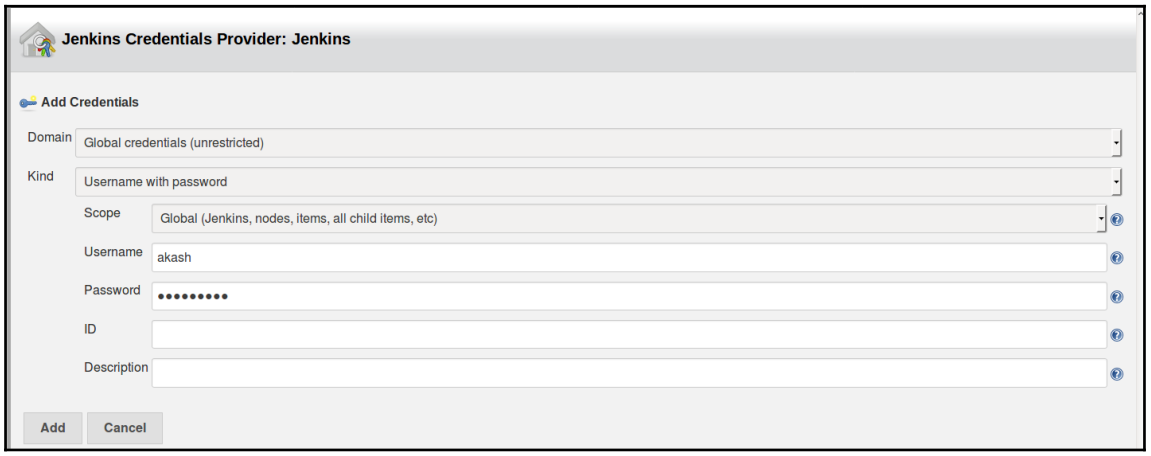

Edit Job
Upload Definition…
Job Name
helloworld
Group is a / separated path
Choose …
Description
Edit
1
The first line of the description will be shown in plain text, the rest will be rendered with Markdown. More
Options:
Undo
Redo
No Options
Add an option
Workflow:
If a step fails: Stop at the failed step. Run remaining steps before failing.
Strategy: Node First
Execute all steps on a node before proceeding to the next node.
Explain
Global Log Filters:
add
Undo
Redo
Revert All Changes
1.
Ansible Playbook Runs an Ansible Playbook.
Playbook: /var/rundeck/projects/automation/playbooks/hello_world.yml
Add a step

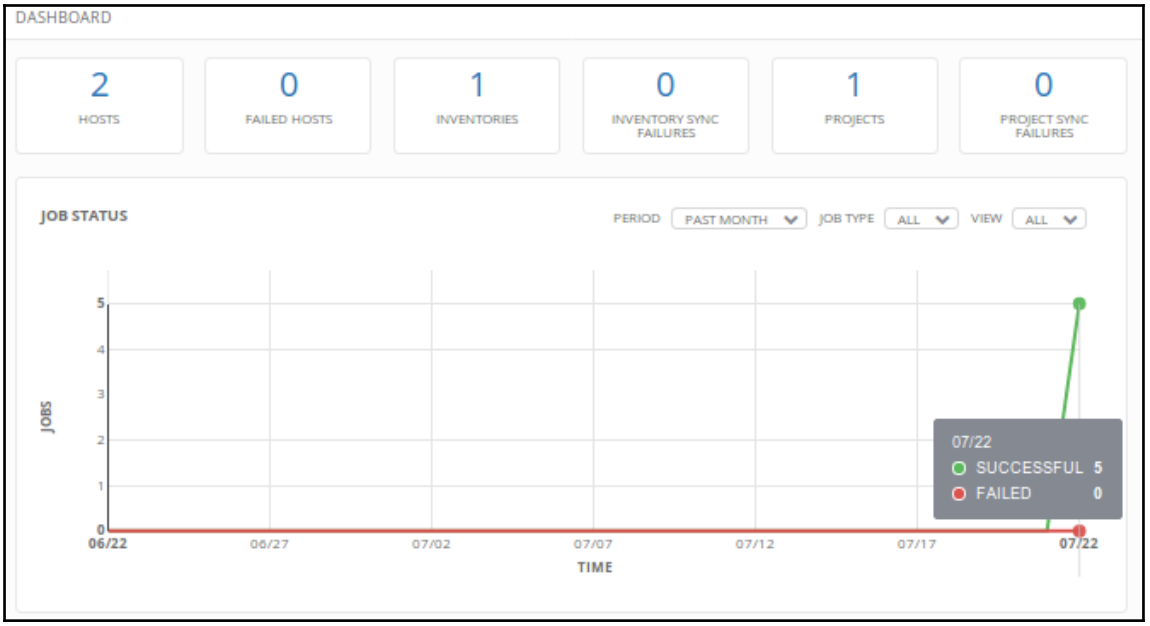

Workflow:
If a step fails: Stop at the failed step. Run remaining steps before failing.
Strategy: Node First
Execute all steps on a node before proceeding to the next node.
Explain
Global Log Filters:
add
1.
Ansible Playbook
Runs an Ansible Playbook.
Playbook
/var/rundeck/projects/automation/playbooks/hello_world.yml
Path to a playbook
Extra Variables
Set additional playbook YAML or JSON variables.
Vault Key File path
File Path to the ansible vault Key to use
Vault Pass Storage Path
Select...
Path to the Vault Key to use within Rundeck Storage. E.g. "keys/path/ansible.vault"
Extra Ansible arguments
Additional ansible raw command line arguments to be appended to the executed command.


helloworld
Action
Prepare and Run...
Definition
Steps: 1.
Ansible Playbook Runs an Ansible Playbook.
Playbook: /var/rundeck/projects/automation/playbooks/hello_world.yml
If a step fails: Stop at the failed step.
Strategy:
Node First Execute all steps on a node before proceeding to the next node.
Nodes: Include nodes matching: hostname: 192.168.1.11
Execute on up to 1 Node at a time.
If a node fails: Fail the step without running on any remaining nodes.
Sort nodes by name in ascending order.
Node selection: Target nodes are selected by default
UUID: 5f2e4fa8-a9f8-492d-bd3a-da170767c731
Created: 10h51m ago

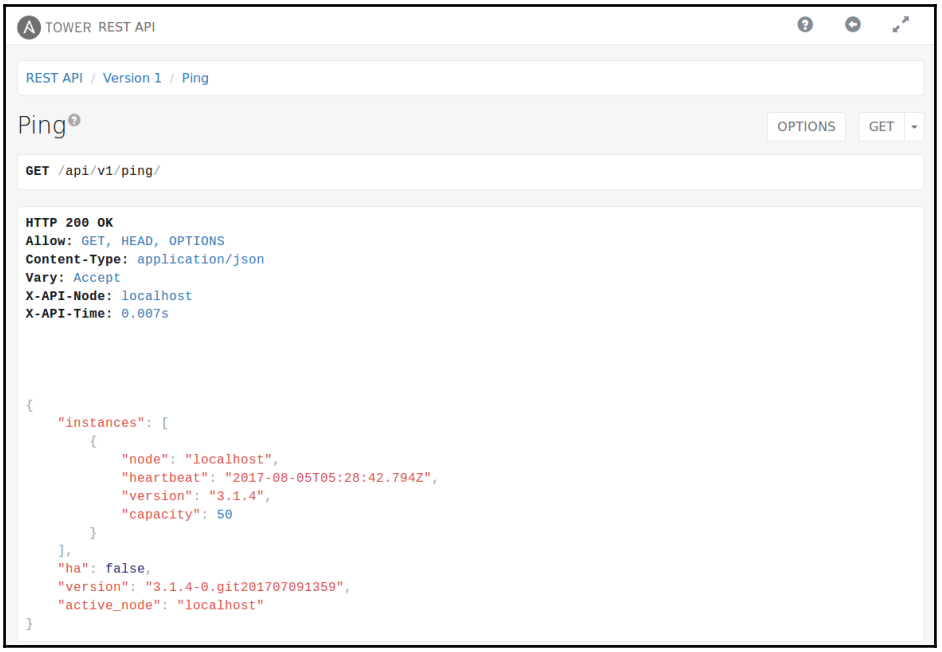

SETTINGS / ORGANIZATIONS / Default / USERS
Default
DETAILS
USERS
NOTIFICATIONS
SEARCH
KEY
+ ADD
USER
ROLE
admin
SYSTEM ADMINISTRATOR
akashmahajan
MEMBER
SYSTEM ADMINISTRATOR
alice
MEMBER
madhuakula
MEMBER
SYSTEM AUDITOR
ITEMS 1 - 4 OF 4

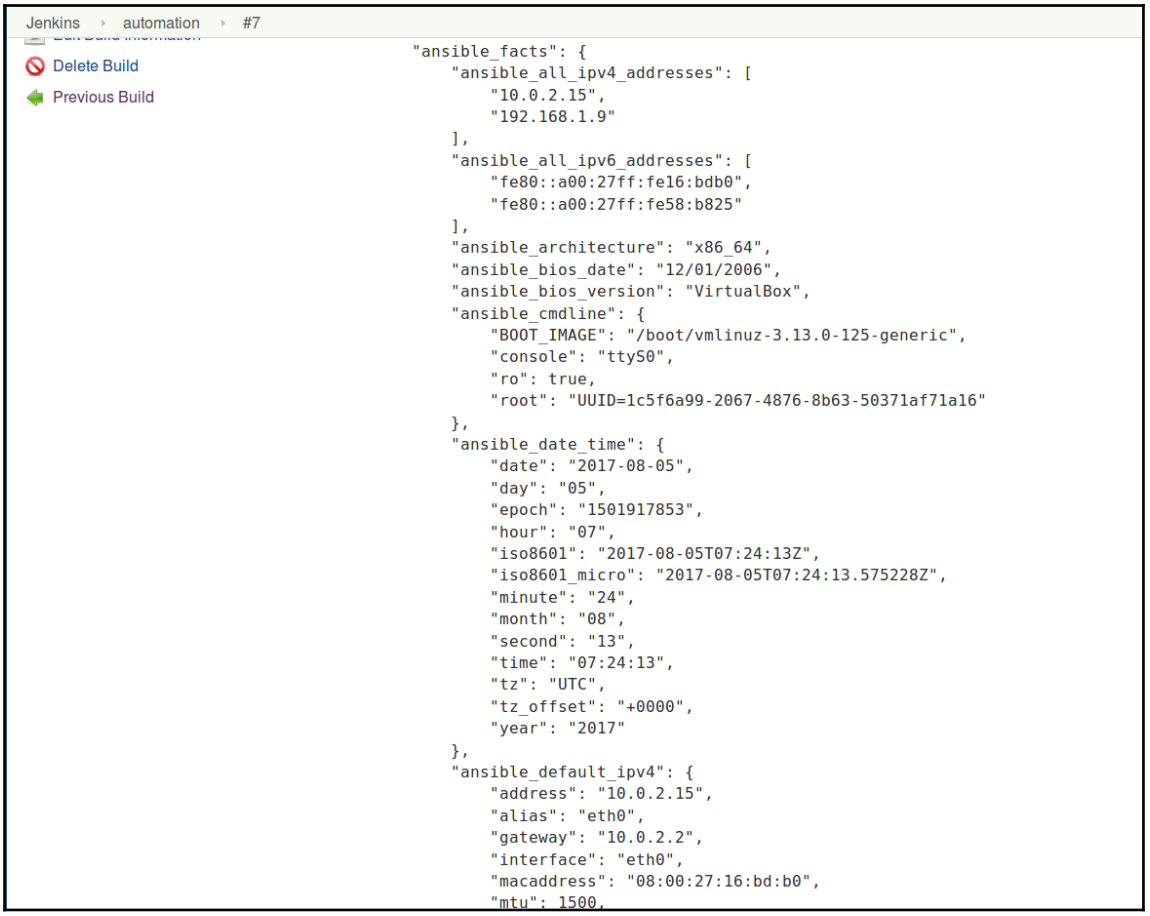

Manage and Assign Roles
Global roles
Role
Overall
Credentials
Agent
Job
Run
View
SCM
Administer
Read
Create
Delete
ManageDomains
Update
View
Build
Configure
Connect
Create
Delete
Disconnect
Provision
Build
Cancel
Configure
Create
Delete
Discover
Move
Read
Workspace
Delete
Replay
Update
Configure
Create
Delete
Read
Tag
admin
user
audit

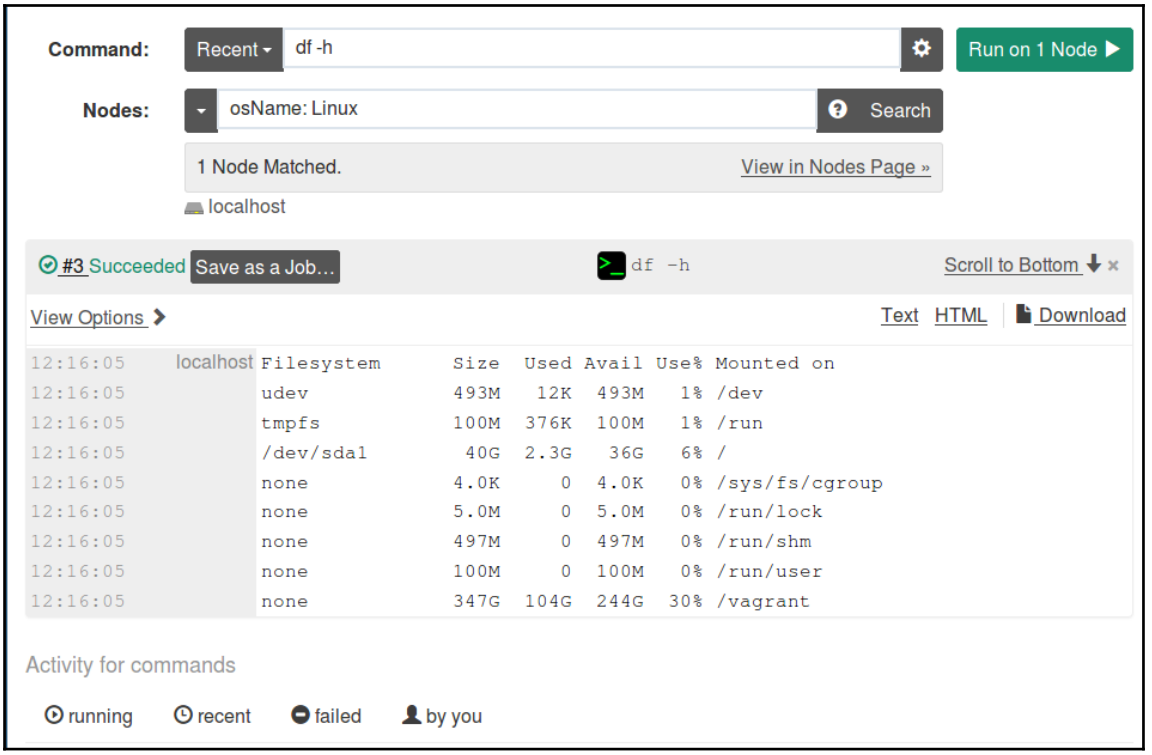

Jenkins Credentials Provider: Jenkins
Add Credentials
Domain
Global credentials (unrestricted)
Kind
Username with password
Scope
Global (Jenkins, nodes, items, all child items, etc)
Username
akash
Password
ID
Description
Add
Cancel

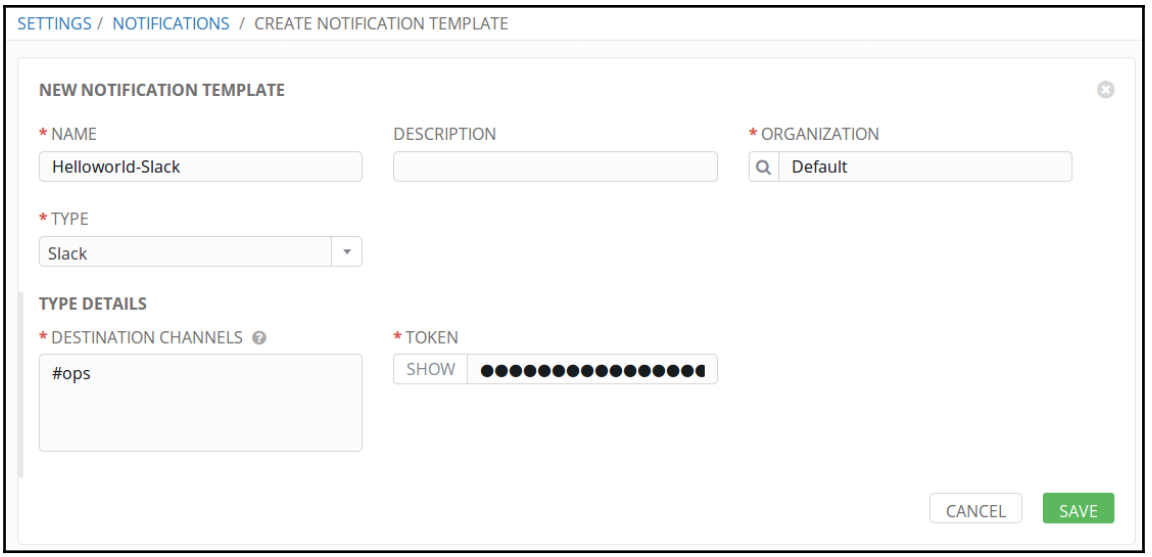

DASHBOARD
2
HOSTS
0
FAILED HOSTS
1
INVENTORIES
0
INVENTORY SYNC FAILURES
1
PROJECTS
0
PROJECT SYNC FAILURES
JOB STATUS
PERIOD
PAST MONTH
JOB TYPE
ALL
VIEW
ALL
JOBS
5
4
3
2
1
0
06/22
06/27
07/02
07/07
07/12
07/17
07/22
TIME
07/22
SUCCESSFUL 5
FAILED 0


STANDARD OUT
"ansible_facts": {
"ansible_all_ipv4_addresses": [
"192.168.1.7",
"10.0.2.15",
"10.42.0.42"
],
"ansible_all_ipv6_addresses": [
"fe80::a00:27ff:fe5d:a92f",
"fe80::a00:27ff:fe57:be11"
],
"ansible_apparmor": {
"status": "disabled"
},
"ansible_architecture": "x86_64",
"ansible_bios_date": "12/01/2006",
"ansible_bios_version": "VirtualBox",
"ansible_cmdline": {
"BOOT_IMAGE": "/vmlinuz-3.10.0-514.26.2.el7.x86_64",
"LANG": "en_US.UTF-8",
"crashkernel": "auto",
"quiet": true,

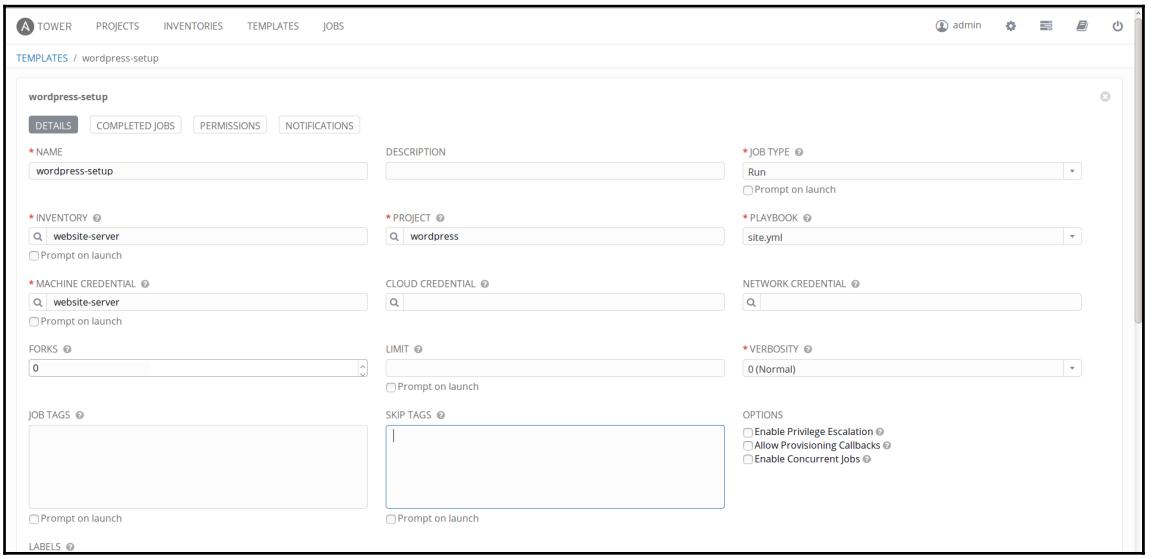

TOWER REST API
REST API / Version 1 / Ping
Ping
OPTIONS
GET
GET /api/v1/ping/
HTTP 200 OK
Allow: GET, HEAD, OPTIONS
Content-Type: application/json
Vary: Accept
X-API-Node: localhost
X-API-Time: 0.007s
{
"instances": [
{
"node": "localhost",
"heartbeat": "2017-08-05T05:28:42.794Z",
"version": "3.1.4",
"capacity": 50
}
],
"ha": false,
"version": "3.1.4-0.git201707091359",
"active_node": "localhost"
}

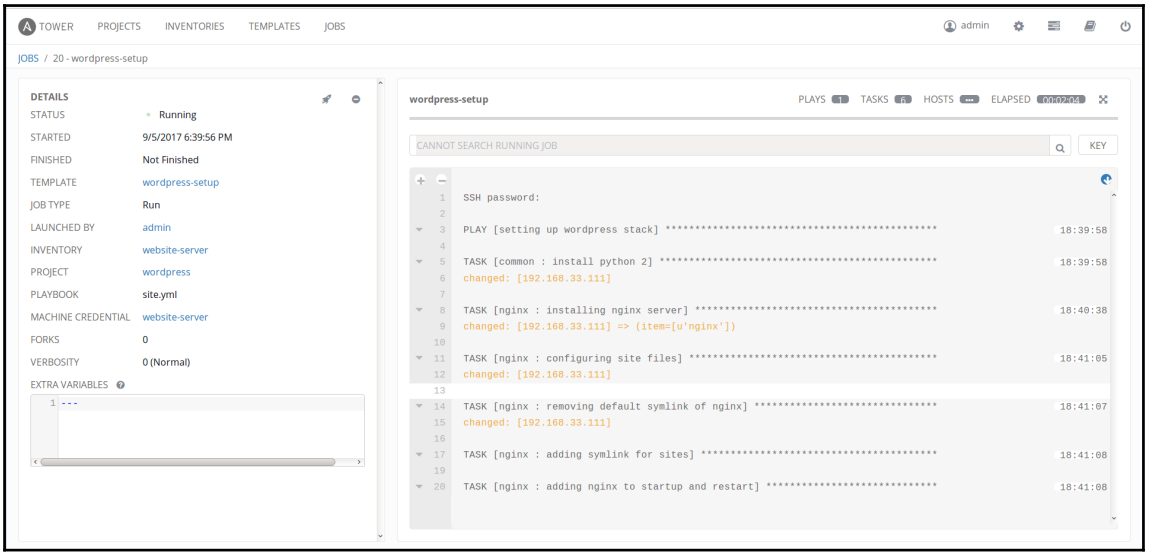

Jenkins
automation
#7
Delete Build
Previous Build
"ansible_facts": {
"ansible_all_ipv4_addresses": [
"10.0.2.15",
"192.168.1.9"
],
"ansible_all_ipv6_addresses": [
"fe80::a00:27ff:fe16:bdb0",
"fe80::a00:27ff:fe58:b825"
],
"ansible_architecture": "x86_64",
"ansible_bios_date": "12/01/2006",
"ansible_bios_version": "VirtualBox",
"ansible_cmdline": {
"BOOT_IMAGE": "/boot/vmlinuz-3.13.0-125-generic",
"console": "ttyS0",
"ro": true,
"root": "UUID=1c5f6a99-2067-4876-8b63-50371af71a16"
},
"ansible_date_time": {
"date": "2017-08-05",
"day": "05",
"epoch": "1501917853",
"hour": "07",
"iso8601": "2017-08-05T07:24:13Z",
"iso8601_micro": "2017-08-05T07:24:13.575228Z",
"minute": "24",
"month": "08",
"second": "13",
"time": "07:24:13",
"tz": "UTC",
"tz_offset": "+0000",
"year": "2017"
},
"ansible_default_ipv4": {
"address": "10.0.2.15",
"alias": "eth0",
"gateway": "10.0.2.2",
"interface": "eth0",
"macaddress": "08:00:27:16:bd:b0",
"mtu": 1500,

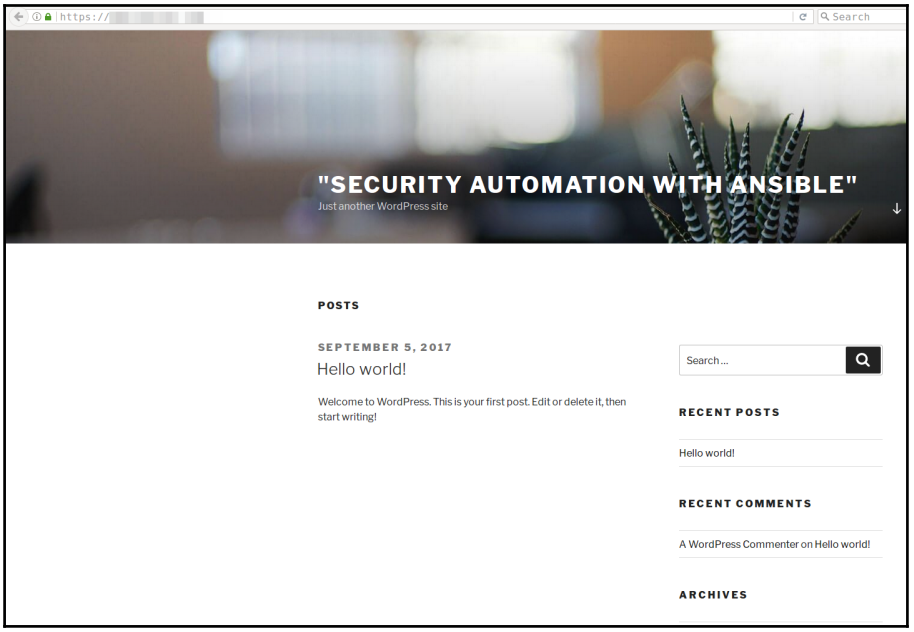

Command:
Recent
df -h
Run on 1 Node
Nodes:
osName: Linux
Search
1 Node Matched.
View in Nodes Page »
localhost
#3 Succeeded
Save as a Job…
df -h
Scroll to Bottom
View Options
Text
HTML
Download
12:16:05 localhost Filesystem Size Used Avail Use% Mounted on
12:16:05 udev 493M 12K 493M 1% /dev
12:16:05 tmpfs 100M 376K 100M 1% /run
12:16:05 /dev/sda1 40G 2.3G 36G 6% /
12:16:05 none 4.0K 0 4.0K 0% /sys/fs/cgroup
12:16:05 none 5.0M 0 5.0M 0% /run/lock
12:16:05 none 497M 0 497M 0% /run/shm
12:16:05 none 100M 0 100M 0% /run/user
12:16:05 none 347G 104G 244G 30% /vagrant
Activity for commands
running
recent
failed
by you

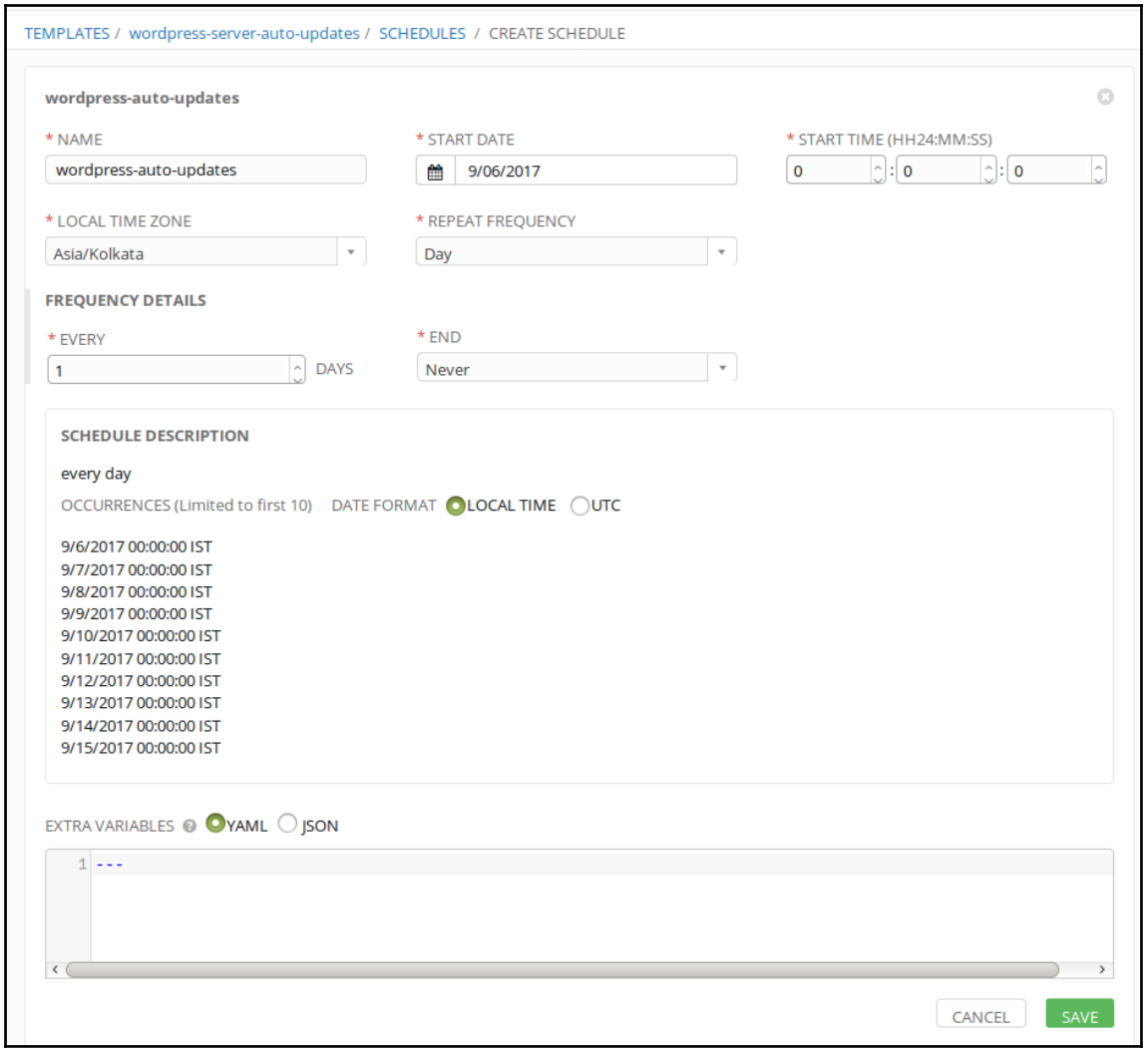

SETTINGS / NOTIFICATIONS / CREATE NOTIFICATION TEMPLATE
NEW NOTIFICATION TEMPLATE
* NAME
Helloworld-Slack
DESCRIPTION
* ORGANIZATION
Default
* TYPE
Slack
TYPE DETAILS
* DESTINATION CHANNELS
#ops
* TOKEN
SHOW
CANCEL
SAVE

Chapter 03: Setting Up a Hardened WordPress with Encrypted Automated Backups

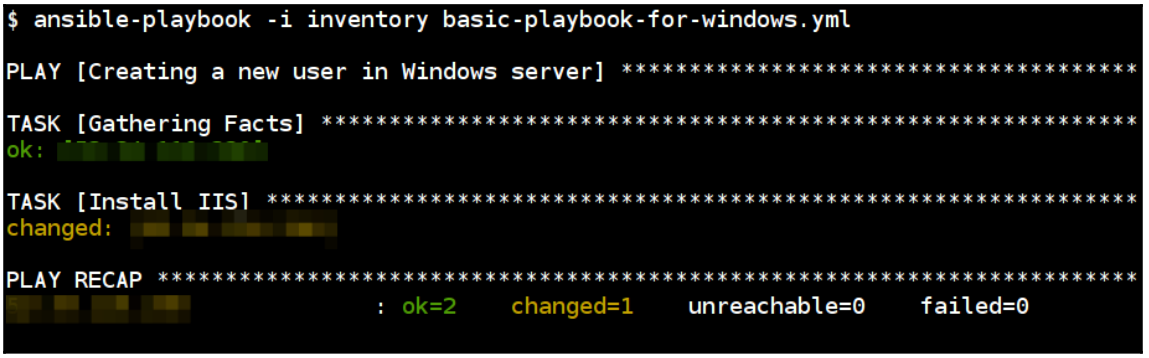




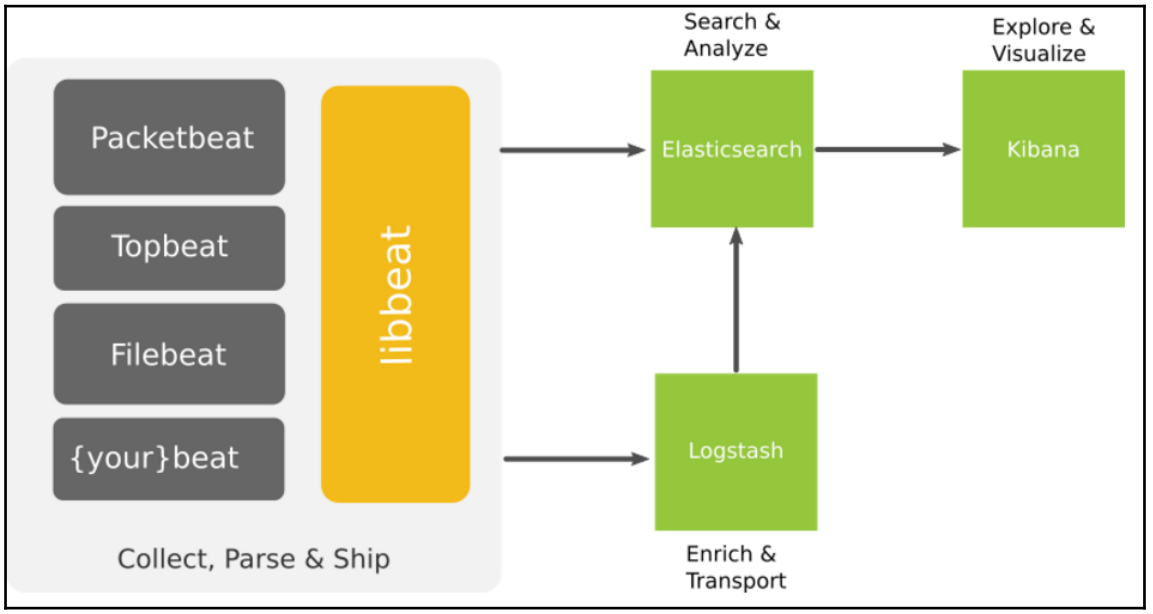

https://
Search
"SECURITY AUTOMATION WITH ANSIBLE"
Just another WordPress site
POSTS
SEPTEMBER 5, 2017
Hello world!
Welcome to WordPress. This is your first post. Edit or delete it, then start writing!
Search ...
RECENT POSTS
Hello world!
RECENT COMMENTS
A WordPress Commenter on Hello world!
ARCHIVES

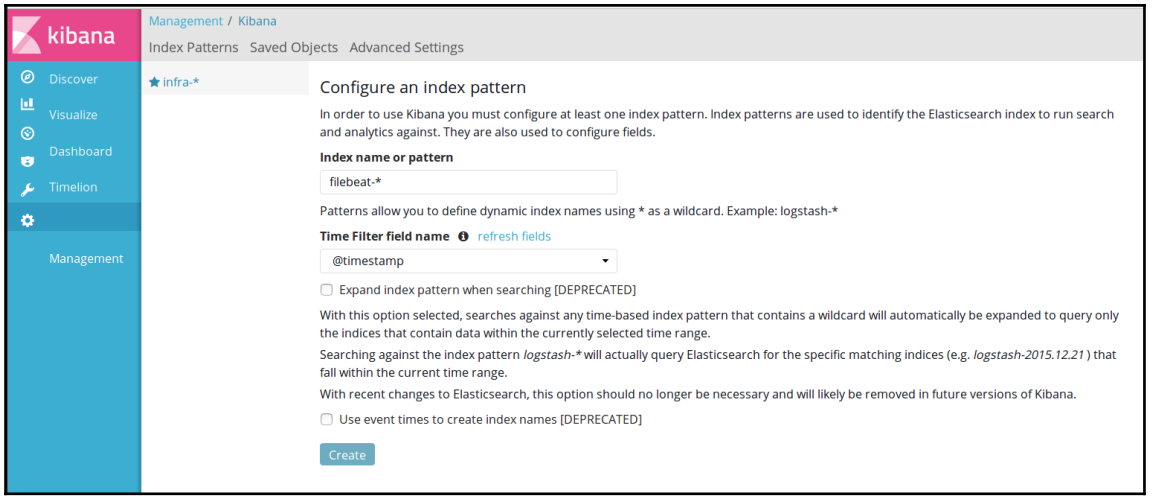


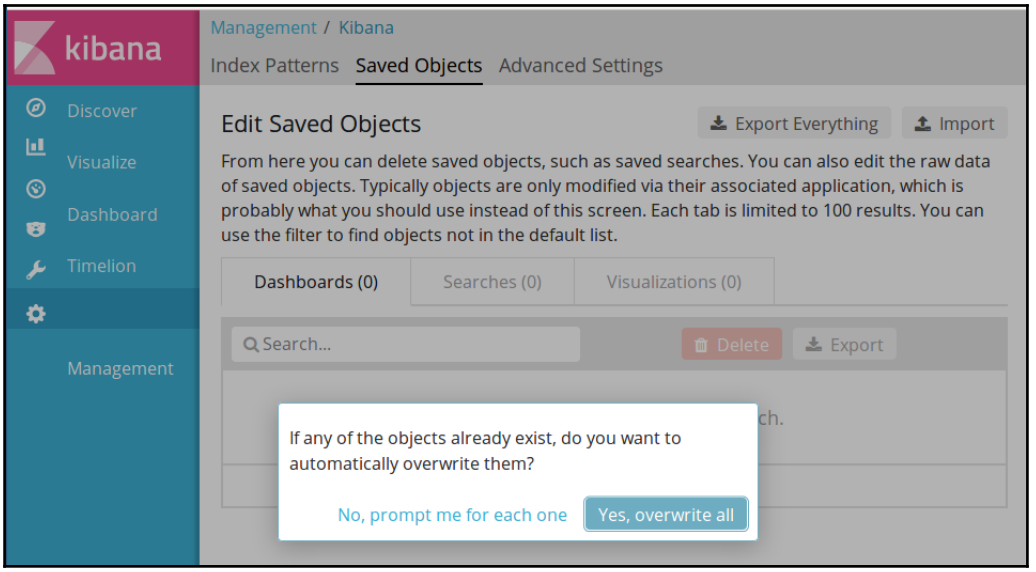

```
$ ansible -i inventory winblows -m win_ping
[redacted] | SUCCESS => {
    "changed": false,
    "ping": "pong"
}
```

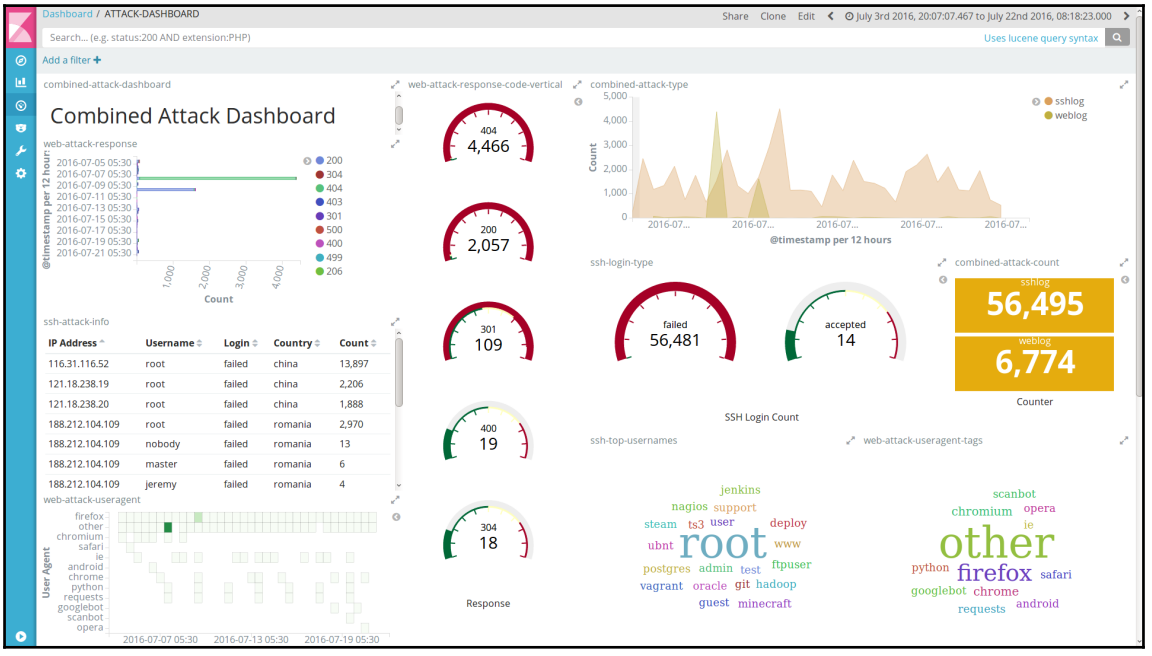

$ ansible-playbook -i inventory basic-playbook-for-windows.yml
PLAY [Creating a new user in Windows server] ************************************
TASK [Gathering Facts] **
ok:
TASK [Install IIS] **
changed:
PLAY RECAP **
: ok=2 changed=1 unreachable=0 failed=0

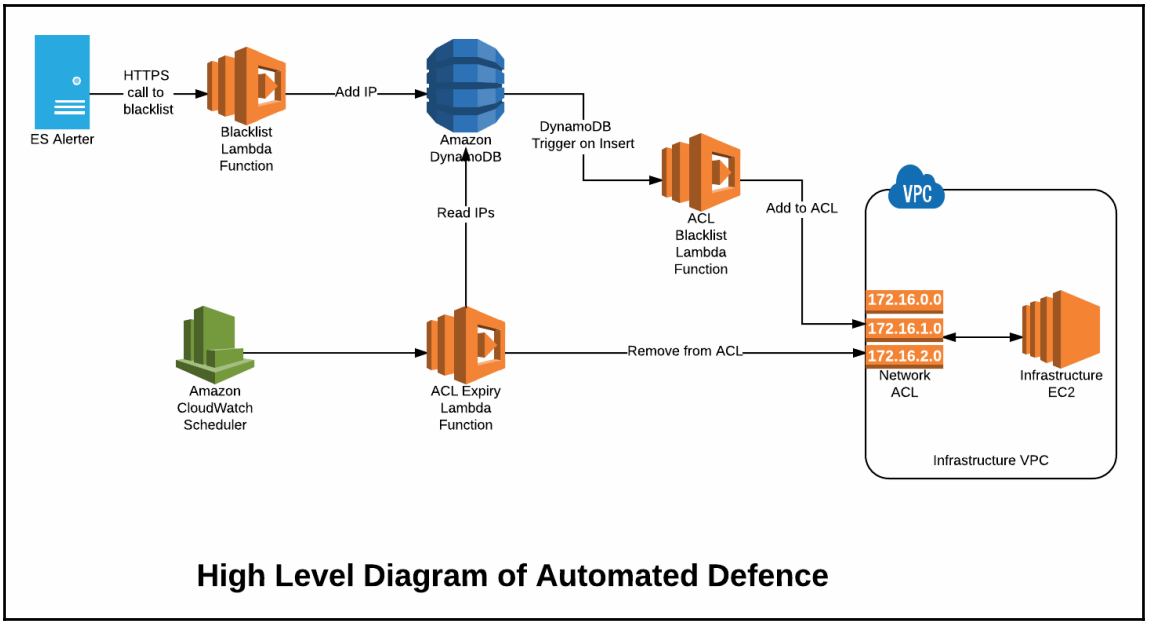
Chapter 04: Log Monitoring and Serverless Automated Defense (Elastic Stack in AWS)



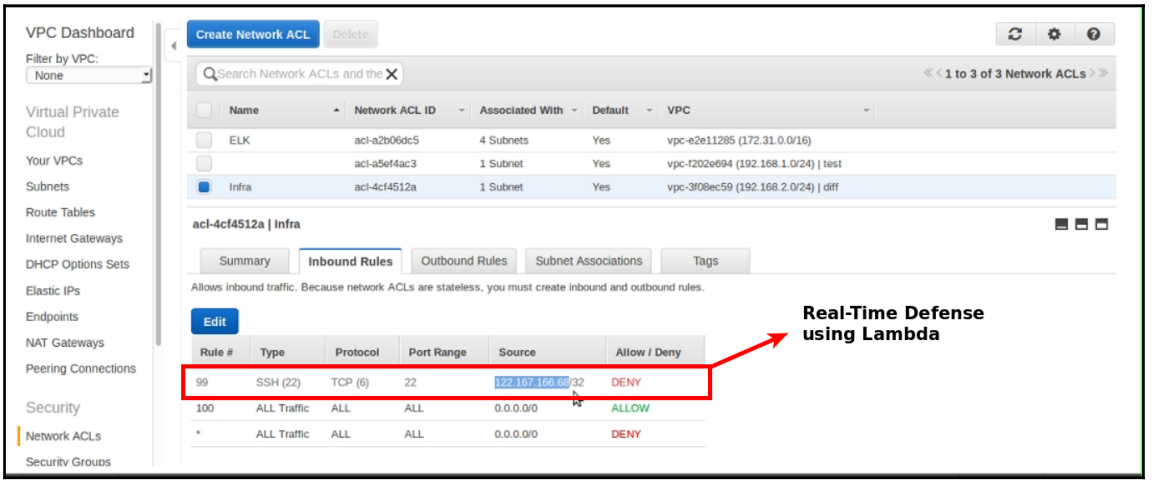



kibana
Management / Kibana
Index Patterns
Saved Objects
Advanced Settings
Discover
Visualize
Dashboard
Timelion
Management
Edit Saved Objects
Export Everything
Import
From here you can delete saved objects, such as saved searches. You can also edit the raw data of saved objects. Typically objects are only modified via their associated application, which is probably what you should use instead of this screen. Each tab is limited to 100 results. You can use the filter to find objects not in the default list.
Dashboards (0)
Searches (0)
Visualizations (0)
Search...
Delete
Export
If any of the objects already exist, do you want to automatically overwrite them?
No, prompt me for each one
Yes, overwrite all

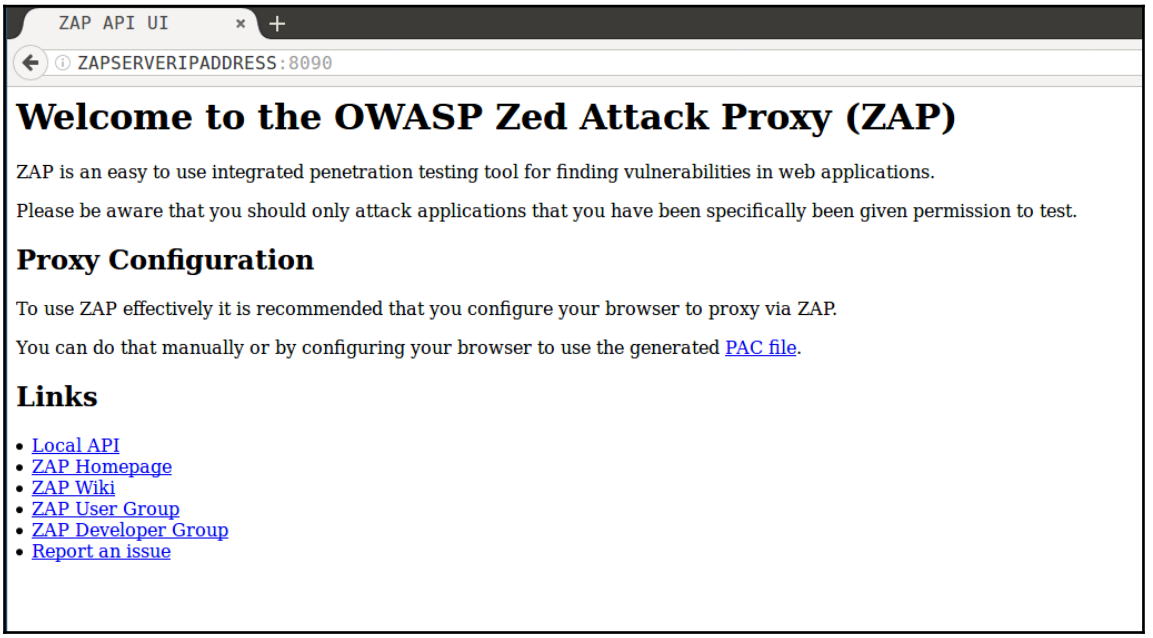

Dashboard / ATTACK-DASHBOARD
Share
Clone
Edit
July 3rd 2016, 20:07:07.467 to July 22nd 2016, 08:18:23.000
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter
combined-attack-dashboard
Combined Attack Dashboard
web-attack-response
web-attack-response-code-vertical
404
4,466
200
2,057
301
109
400
19
304
18
Response
combined-attack-type
sshlog
weblog
@timestamp per 12 hours
ssh-login-type
failed
56,481
accepted
14
SSH Login Count
combined-attack-count
sshlog
56,495
weblog
6,774
Counter
ssh-attack-info
IP Address
Username
Login
Country
Count
116.31.116.52 root failed china 13,897
121.18.238.19 root failed china 2,206
121.18.238.20 root failed china 1,888
188.212.104.109 root failed romania 2,970
188.212.104.109 nobody failed romania 13
188.212.104.109 master failed romania 6
188.212.104.109 jeremy failed romania 4
web-attack-useragent
User Agent
ssh-top-usernames
jenkins
nagios
support
steam
ts3
user
deploy
ubnt
root
www
postgres
admin
test
ftpuser
vagrant
oracle
git
hadoop
guest
minecraft
web-attack-useragent-tags
scanbot
chromium
opera
ie
other
python
firefox
safari
googlebot
chrome
requests
android

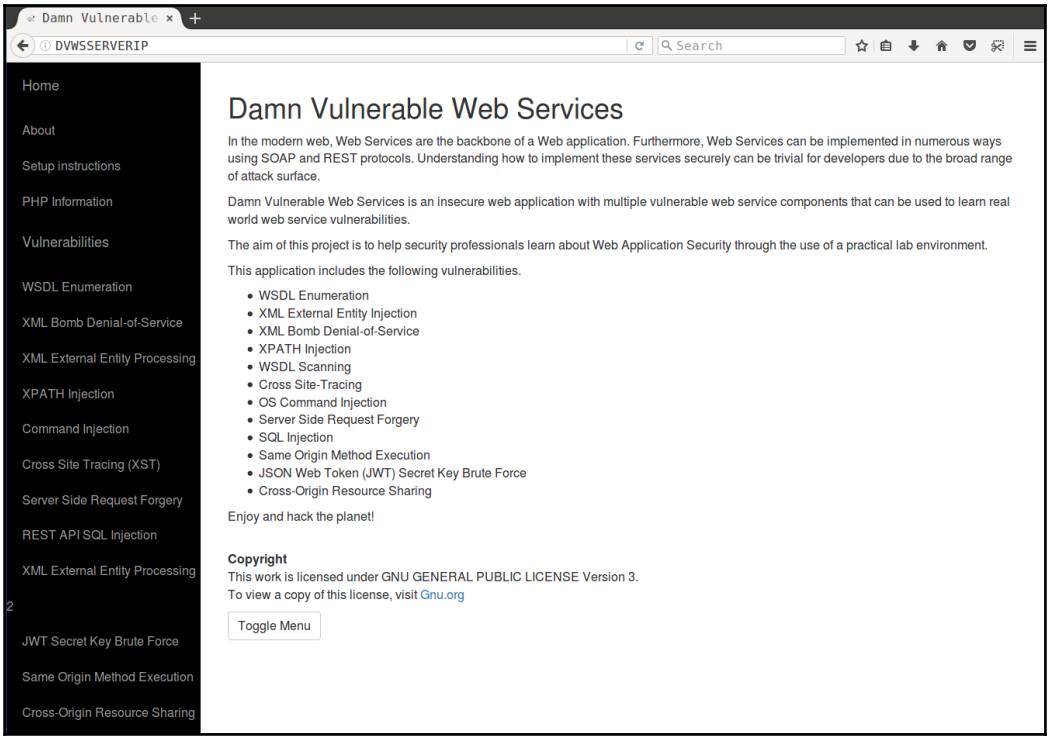


High Level Diagram of Automated Defence



Chapter 05: Automating Web Application Security Testing Using OWASP ZAP




Damn Vulnerable
DVWSSERVERIP
Search
Home
About
Setup instructions
PHP Information
Vulnerabilities
WSDL Enumeration
XML Bomb Denial-of-Service
XML External Entity Processing
XPATH Injection
Command Injection
Cross Site Tracing (XST)
Server Side Request Forgery
REST API SQL Injection
XML External Entity Processing
JWT Secret Key Brute Force
Same Origin Method Execution
Cross-Origin Resource Sharing
Damn Vulnerable Web Services
In the modern web, Web Services are the backbone of a Web application. Furthermore, Web Services can be implemented in numerous ways using SOAP and REST protocols. Understanding how to implement these services securely can be trivial for developers due to the broad range of attack surface.
Damn Vulnerable Web Services is an insecure web application with multiple vulnerable web service components that can be used to learn real world web service vulnerabilities.
The aim of this project is to help security professionals learn about Web Application Security through the use of a practical lab environment.
This application includes the following vulnerabilities.
WSDL Enumeration
XML External Entity Injection
XML Bomb Denial-of-Service
XPATH Injection
WSDL Scanning
Cross Site-Tracing
OS Command Injection
Server Side Request Forgery
SQL Injection
Same Origin Method Execution
JSON Web Token (JWT) Secret Key Brute Force
Cross-Origin Resource Sharing
Enjoy and hack the planet!
Copyright
This work is licensed under GNU GENERAL PUBLIC LICENSE Version 3.
To view a copy of this license, visit Gnu.org
Toggle Menu

ZAP Scanning Report

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	5
Informational	2

Alert Detail

Medium (Medium)	X-Frame-Options Header Not Set
Description	X-Frame-Options header is not included in the HTTP response to protect against 'ClickJacking' attacks.
URL	http://192.168.33.111/dvws/vulnerabilities/cors/?C=S;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.33.111/dvws/about.php
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.33.111/dvws/vulnerabilities/xst/?C=M;O=D
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.33.111/dvws/vulnerabilities/xxe2/
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.33.111/dvws/vulnerabilities/?C=N;O=A
Method	GET
Parameter	X-Frame-Options
URL	http://192.168.33.111/dvws/vulnerabilities/hiddendir/?C=M;O=A
Method	GET

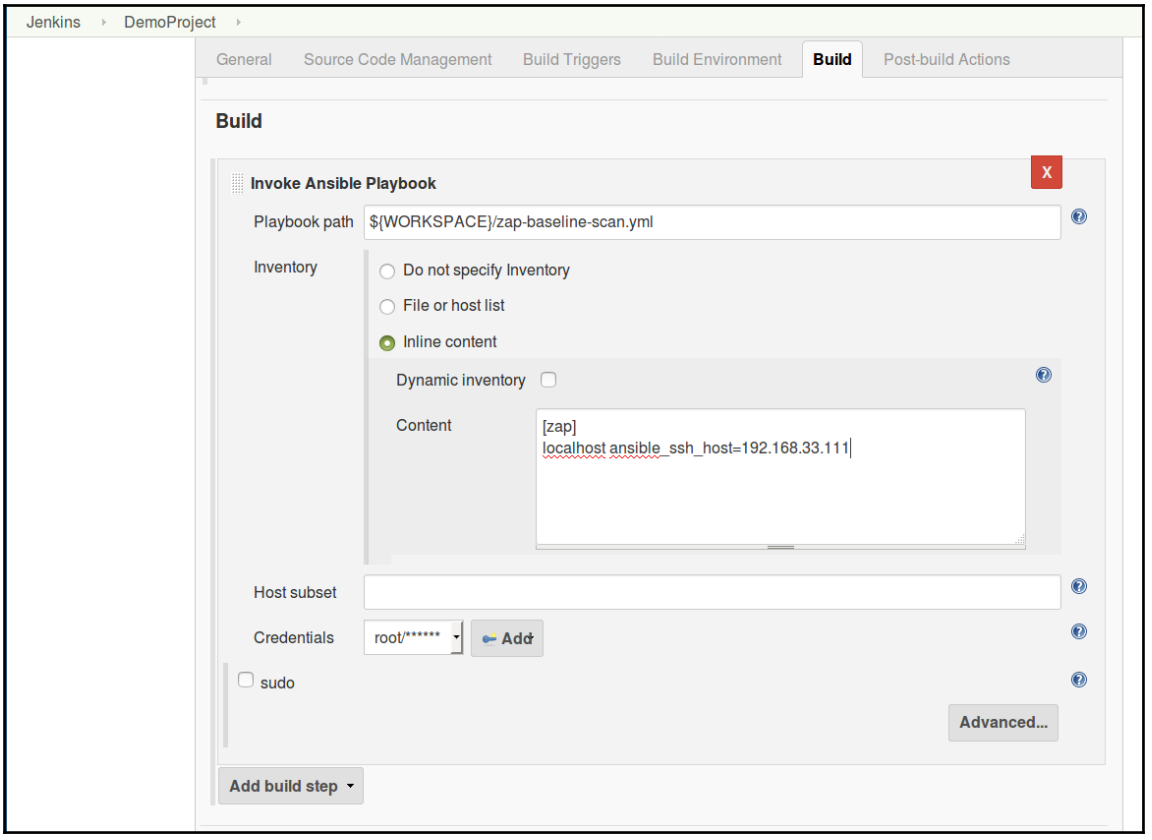
ZAP Scanning Report

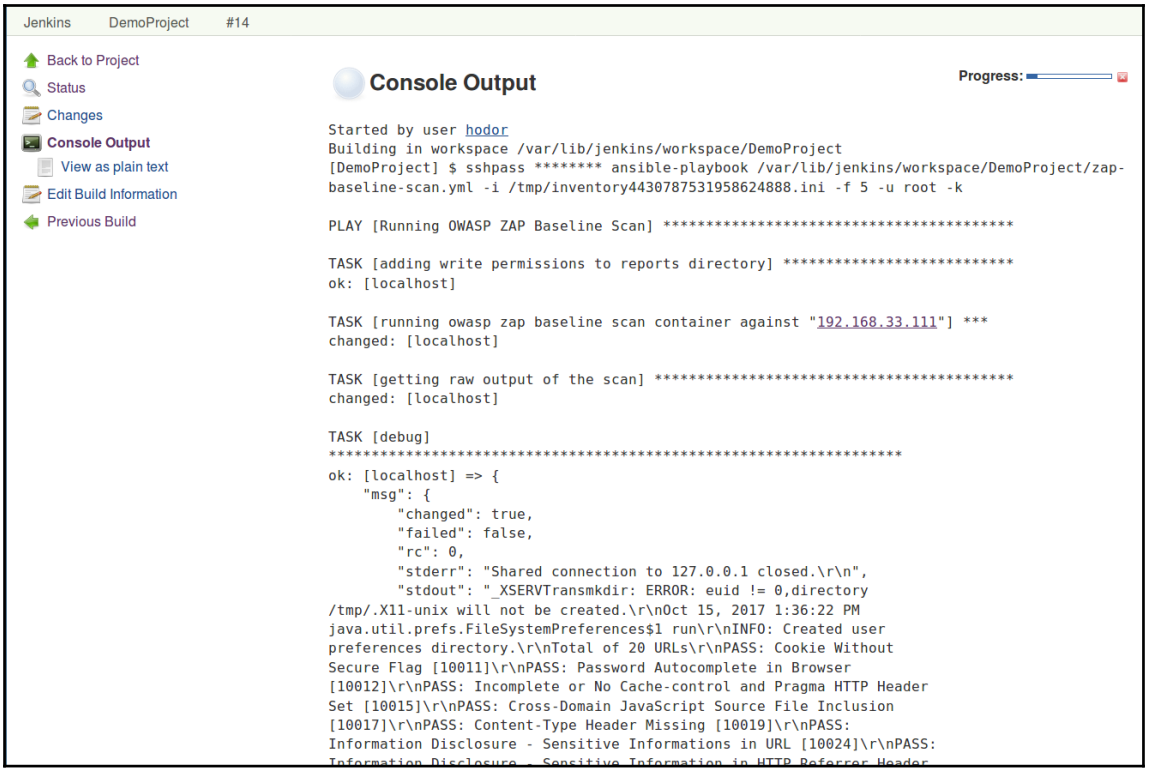
Summary of Alerts

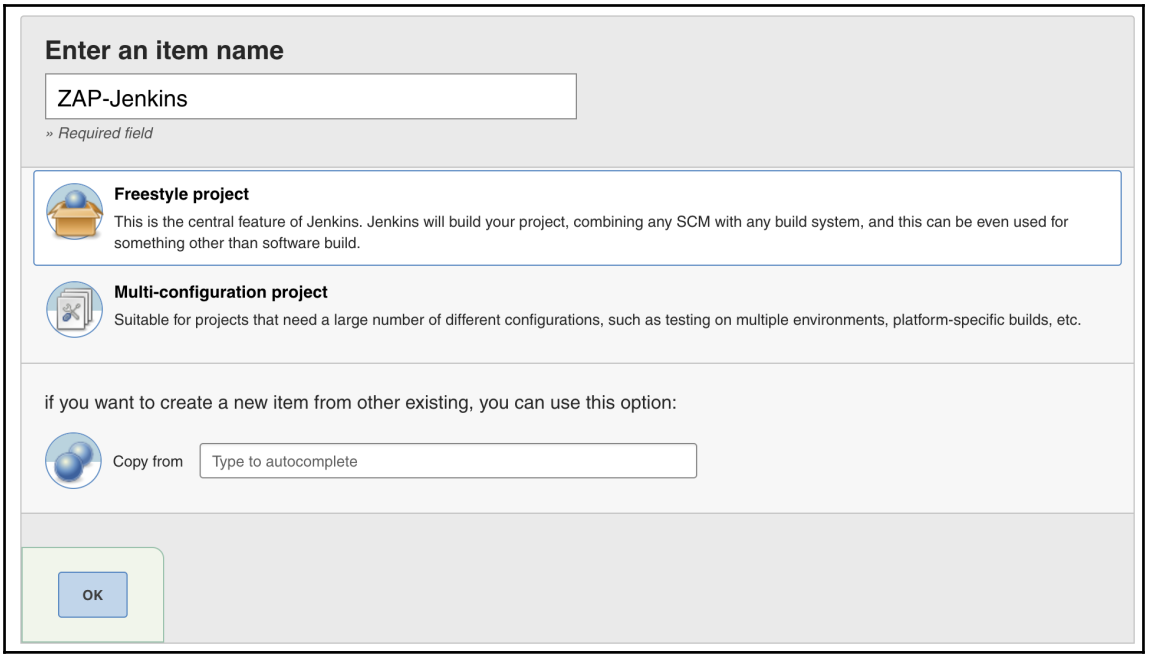
Risk Level	Number of Alerts
High	5
Medium	5
Low	5
Informational	2

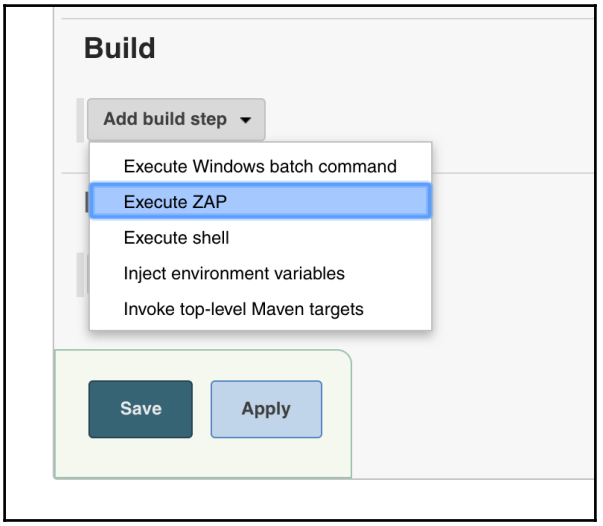
Alert Detail

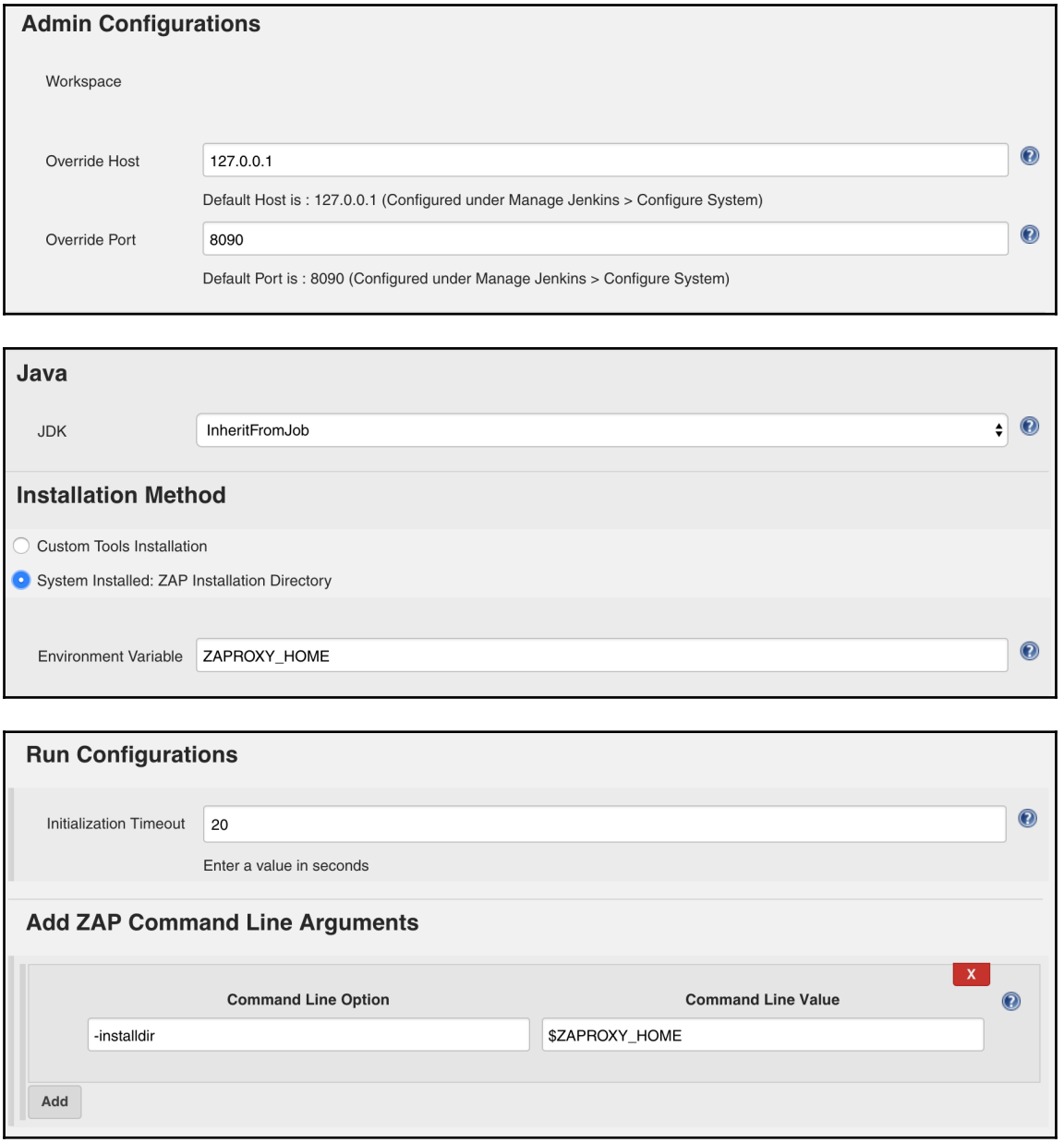
High (Medium)	Anti CSRF Tokens Scanner
Description	A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim. The underlying cause is application functionality using predictable URL/form actions in a repeatable way. The nature of the attack is that CSRF exploits the trust that a web site has for a user. By contrast, cross-site scripting (XSS) exploits the trust that a user has for a web site. Like XSS, CSRF attacks are not necessarily cross-site, but they can be. Cross-site request forgery is also known as CSRF, XSRF, one-click attack, session riding, confused deputy, and sea surf. CSRF attacks are effective in a number of situations, including: * The victim has an active session on the target site. * The victim is authenticated via HTTP auth on the target site. * The victim is on the same local network as the target site. CSRF has primarily been used to perform an action against a target site using the victim's privileges, but recent techniques have been discovered to disclose information by gaining access to the response. The risk of information disclosure is dramatically increased when the target site is vulnerable to XSS, because XSS can be used as a platform for CSRF, allowing the attack to operate within the bounds of the same-origin policy.
URL	http://192.168.33.111/dvws/vulnerabilities/jwt/api.php
Method	POST
Evidence	<form method="post" action="">
URL	http://192.168.33.111/dvws/vulnerabilities/jwt/login.php
Method	GET

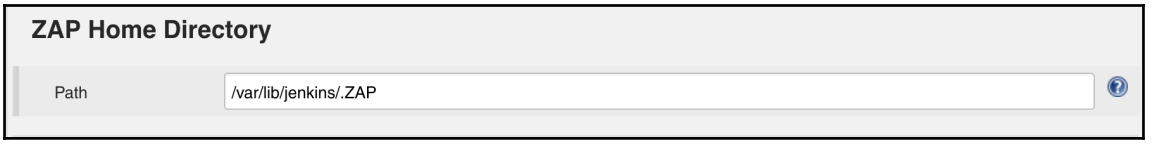

Jenkins
DemoProject
General
Source Code Management
Build Triggers
Build Environment
Build
Post-build Actions
Build
Invoke Ansible Playbook
X
Playbook path
${WORKSPACE}/zap-baseline-scan.yml
Inventory
Do not specify Inventory
File or host list
Inline content
Dynamic inventory
Content
[zap]
localhost ansible_ssh_host=192.168.33.111
Host subset
Credentials
root/******
Add
sudo
Advanced...
Add build step


Jenkins
DemoProject
#14
Back to Project
Status
Changes
Console Output
View as plain text
Edit Build Information
Previous Build
Console Output
Progress:
Started by user hodor
Building in workspace /var/lib/jenkins/workspace/DemoProject
[DemoProject] $ sshpass ******** ansible-playbook /var/lib/jenkins/workspace/DemoProject/zap-baseline-scan.yml -i /tmp/inventory4430787531958624888.ini -f 5 -u root -k
PLAY [Running OWASP ZAP Baseline Scan] ***********
TASK [adding write permissions to reports directory] ***********
ok: [localhost]
TASK [running owasp zap baseline scan container against "192.168.33.111"] ***
changed: [localhost]
TASK [getting raw output of the scan] ***********
changed: [localhost]
TASK [debug]
ok: [localhost] => {
"msg": {
"changed": true,
"failed": false,
"rc": 0,
"stderr": "Shared connection to 127.0.0.1 closed.\r\n",
"stdout": "_XSERVTransmkdir: ERROR: euid != 0,directory
/tmp/.X11-unix will not be created.\r\nOct 15, 2017 1:36:22 PM
java.util.prefs.FileSystemPreferences$1 run\r\nINFO: Created user
preferences directory.\r\nTotal of 20 URLs\r\nPASS: Cookie Without
Secure Flag [10011]\r\nPASS: Password Autocomplete in Browser
[10012]\r\nPASS: Incomplete or No Cache-control and Pragma HTTP Header
Set [10015]\r\nPASS: Cross-Domain JavaScript Source File Inclusion
[10017]\r\nPASS: Content-Type Header Missing [10019]\r\nPASS:
Information Disclosure - Sensitive Informations in URL [10024]\r\nPASS:

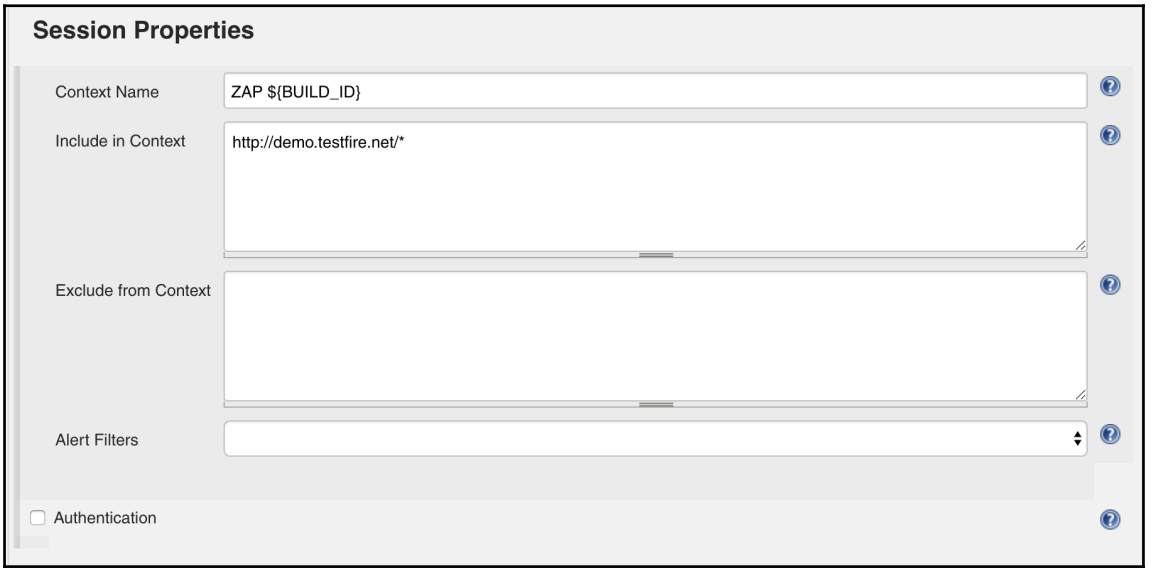

Enter an item name
ZAP-Jenkins
» Required field
Freestyle project
This is the central feature of Jenkins. Jenkins will build your project, combining any SCM with any build system, and this can be even used for something other than software build.
Multi-configuration project
Suitable for projects that need a large number of different configurations, such as testing on multiple environments, platform-specific builds, etc.
if you want to create a new item from other existing, you can use this option:
Copy from
Type to autocomplete
OK

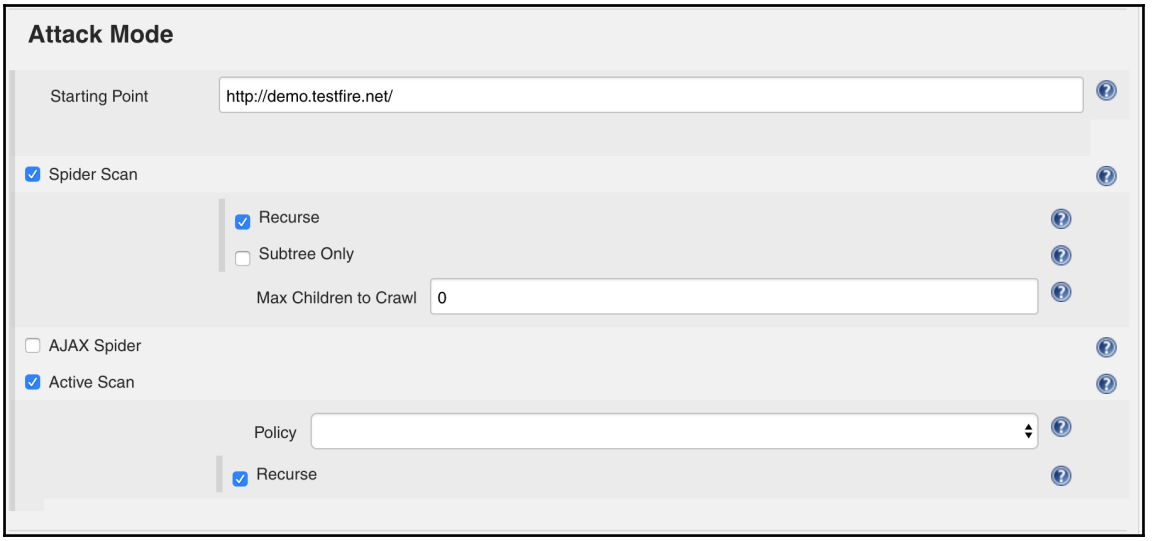

Build
Add build step
Execute Windows batch command
Execute ZAP
Execute shell
Inject environment variables
Invoke top-level Maven targets
Save
Apply

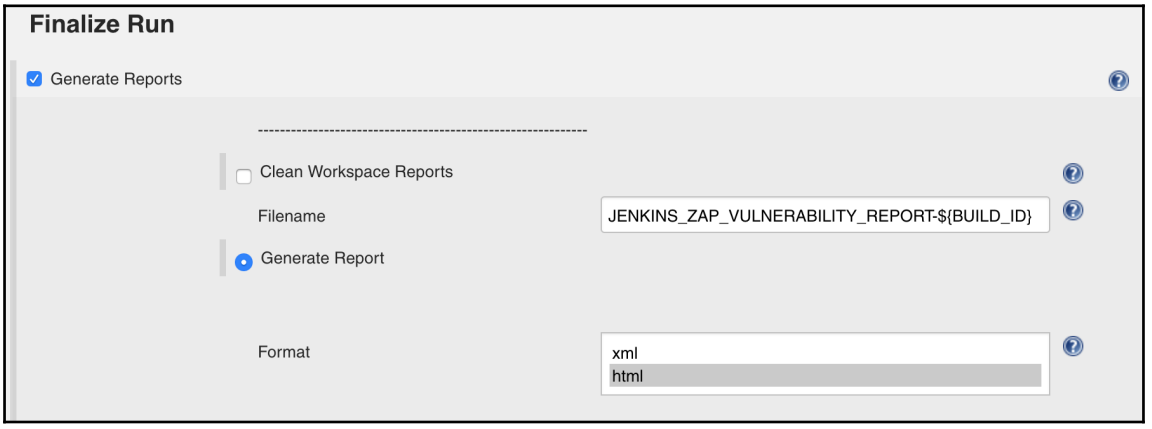

Admin Configurations
Workspace
Override Host
127.0.0.1
Default Host is : 127.0.0.1 (Configured under Manage Jenkins > Configure System)
Override Port
8090
Default Port is : 8090 (Configured under Manage Jenkins > Configure System)
Java
JDK
InheritFromJob
Installation Method
Custom Tools Installation
System Installed: ZAP Installation Directory
Environment Variable
ZAPROXY_HOME
Run Configurations
Initialization Timeout
20
Enter a value in seconds
Add ZAP Command Line Arguments
X
Command Line Option
Command Line Value
-installdir
$ZAPROXY_HOME
Add


ZAP Home Directory
Path
/var/lib/jenkins/.ZAP

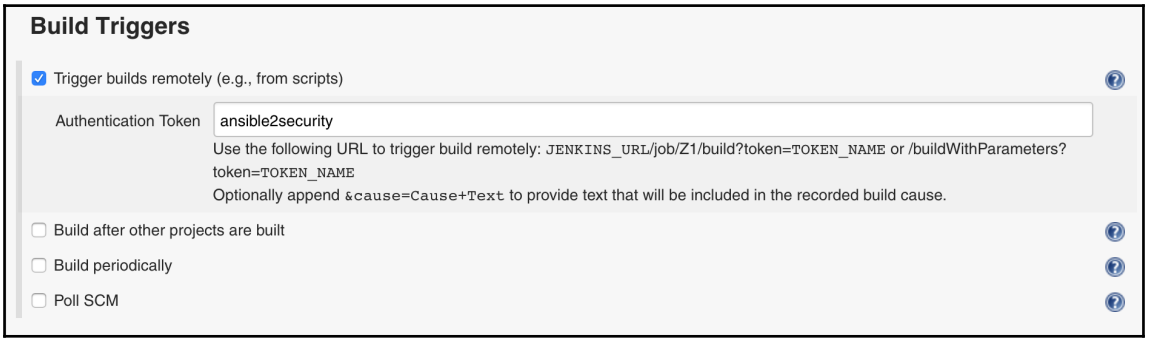

Session Management
Load Session
Path
/var/lib/jenkins/workspace/Z1/attack.session
Persist Session

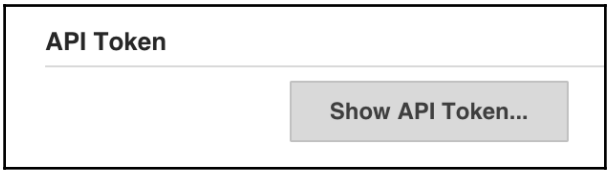

Session Properties
Context Name
ZAP ${BUILD_ID}
Include in Context
http://demo.testfire.net/*
Exclude from Context
Alert Filters
Authentication

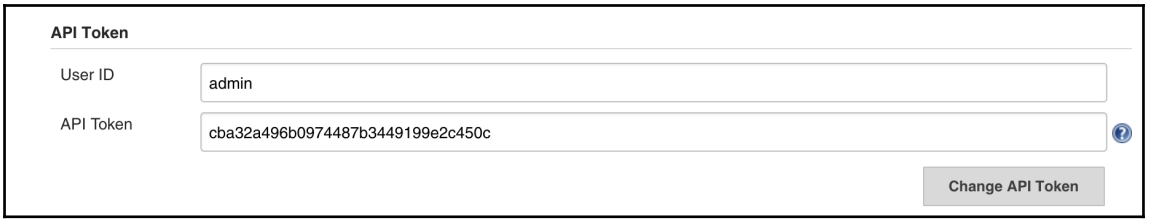

Attack Mode
Starting Point
http://demo.testfire.net/
Spider Scan
Recurse
Subtree Only
Max Children to Crawl
0
AJAX Spider
Active Scan
Policy
Recurse


Finalize Run
Generate Reports
Clean Workspace Reports
Filename
JENKINS_ZAP_VULNERABILITY_REPORT-${BUILD_ID}
Generate Report
Format
xml
html

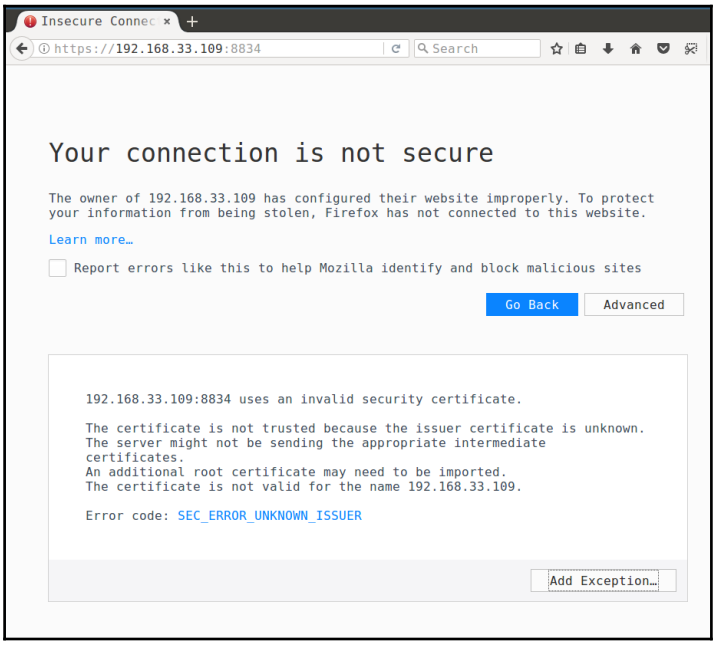

This project is parameterized
String Parameter
Name
TARGET
Default Value
http://demo.testfire.net
Description
[Plain text] Preview
Add Parameter

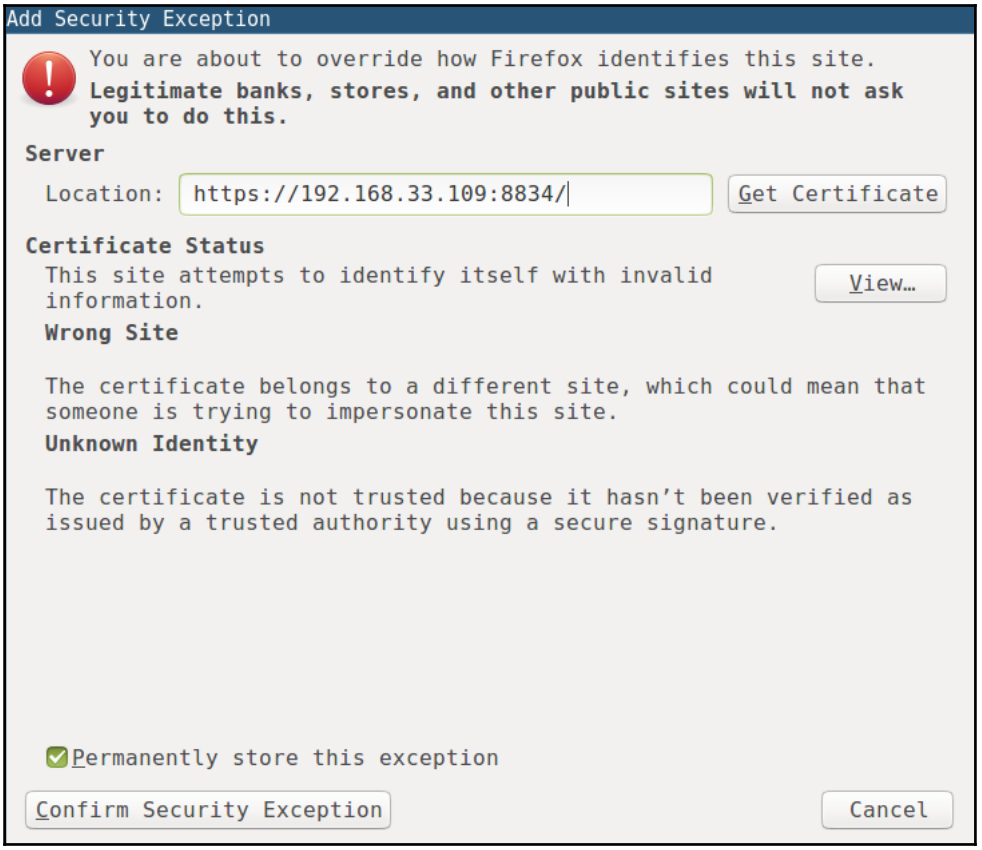

Build Triggers
Trigger builds remotely (e.g., from scripts)
Authentication Token
ansible2security
Use the following URL to trigger build remotely: JENKINS_URL/job/Z1/build?token=TOKEN_NAME or /buildWithParameters?token=TOKEN_NAME
Optionally append &cause=Cause+Text to provide text that will be included in the recorded build cause.
Build after other projects are built
Build periodically
Poll SCM

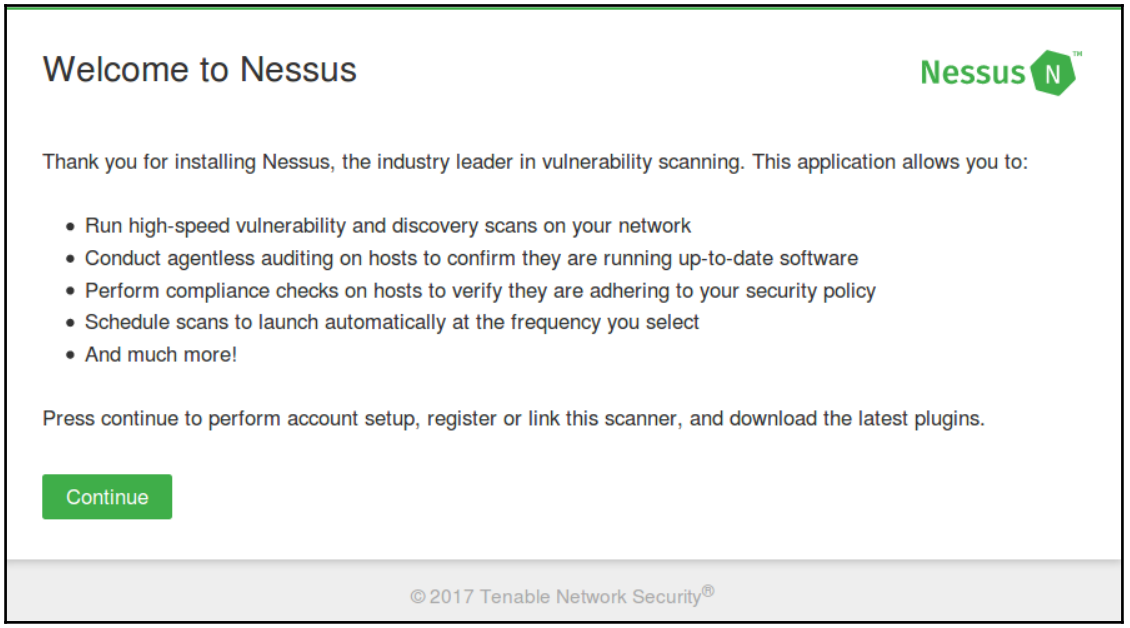

API Token
Show API Token...

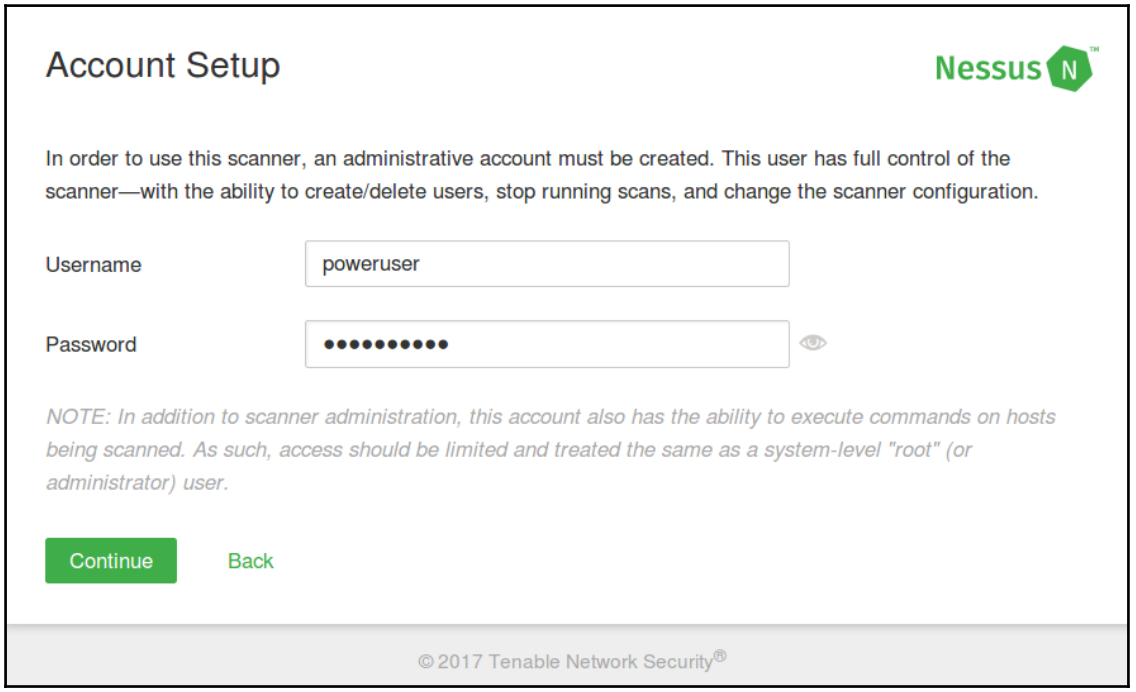

API Token
User ID
admin
API Token
cba32a496b0974487b3449199e2c450c
Change API Token

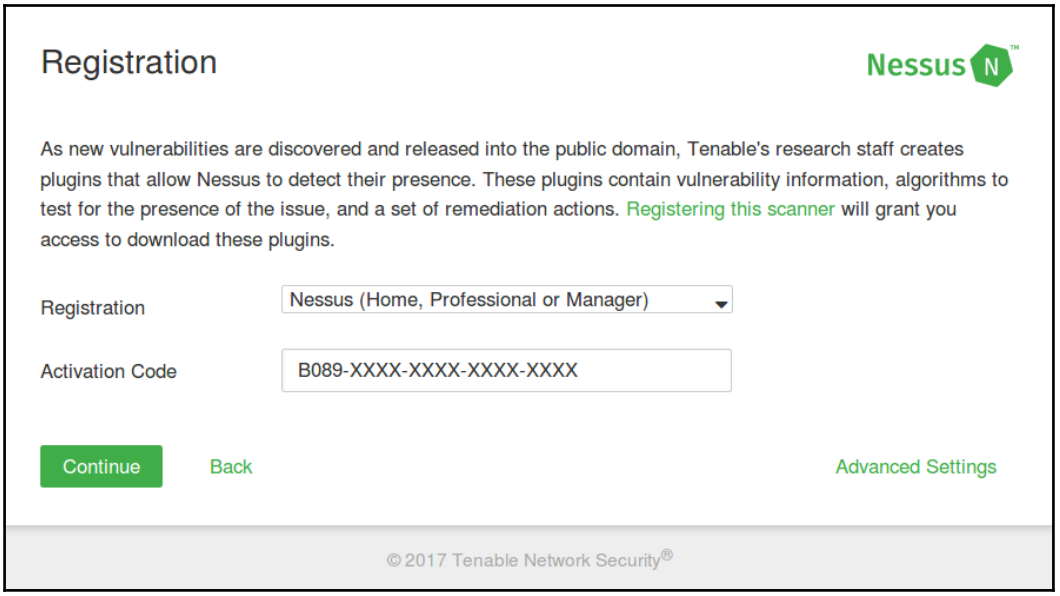
Chapter 06: Vulnerability Scanning with Nessus

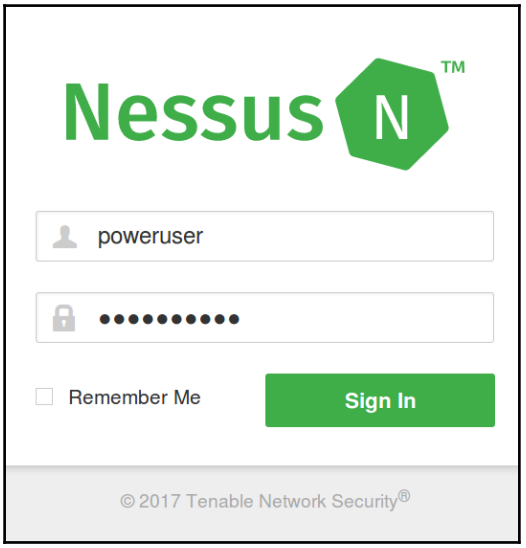


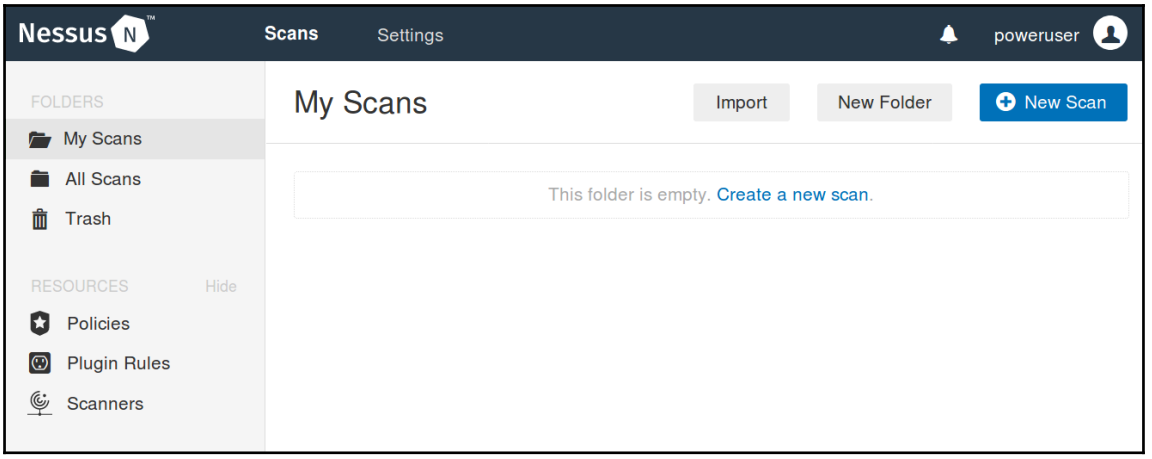

Add Security Exception
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Server
Location: https://192.168.33.109:8834/
Get Certificate
Certificate Status
This site attempts to identify itself with invalid information.
View…
Wrong Site
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.
Unknown Identity
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
Permanently store this exception
Confirm Security Exception
Cancel

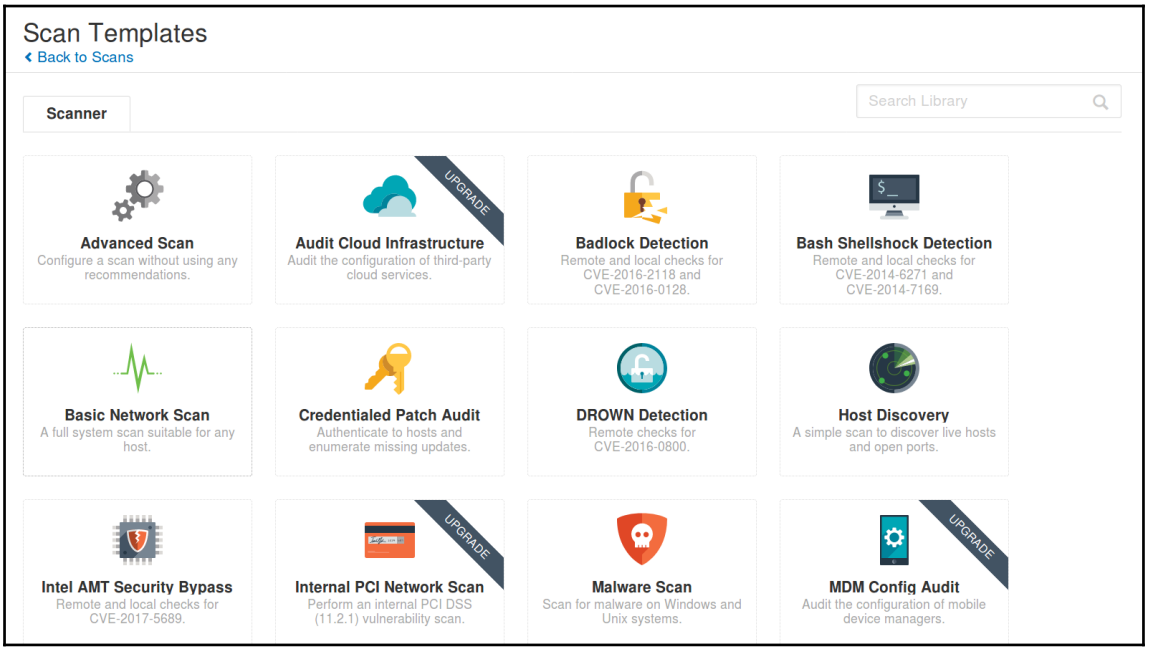

Welcome to Nessus
Nessus
Thank you for installing Nessus, the industry leader in vulnerability scanning. This application allows you to:
Run high-speed vulnerability and discovery scans on your network
Conduct agentless auditing on hosts to confirm they are running up-to-date software
Perform compliance checks on hosts to verify they are adhering to your security policy
Schedule scans to launch automatically at the frequency you select
And much more!
Press continue to perform account setup, register or link this scanner, and download the latest plugins.
Continue
© 2017 Tenable Network Security®

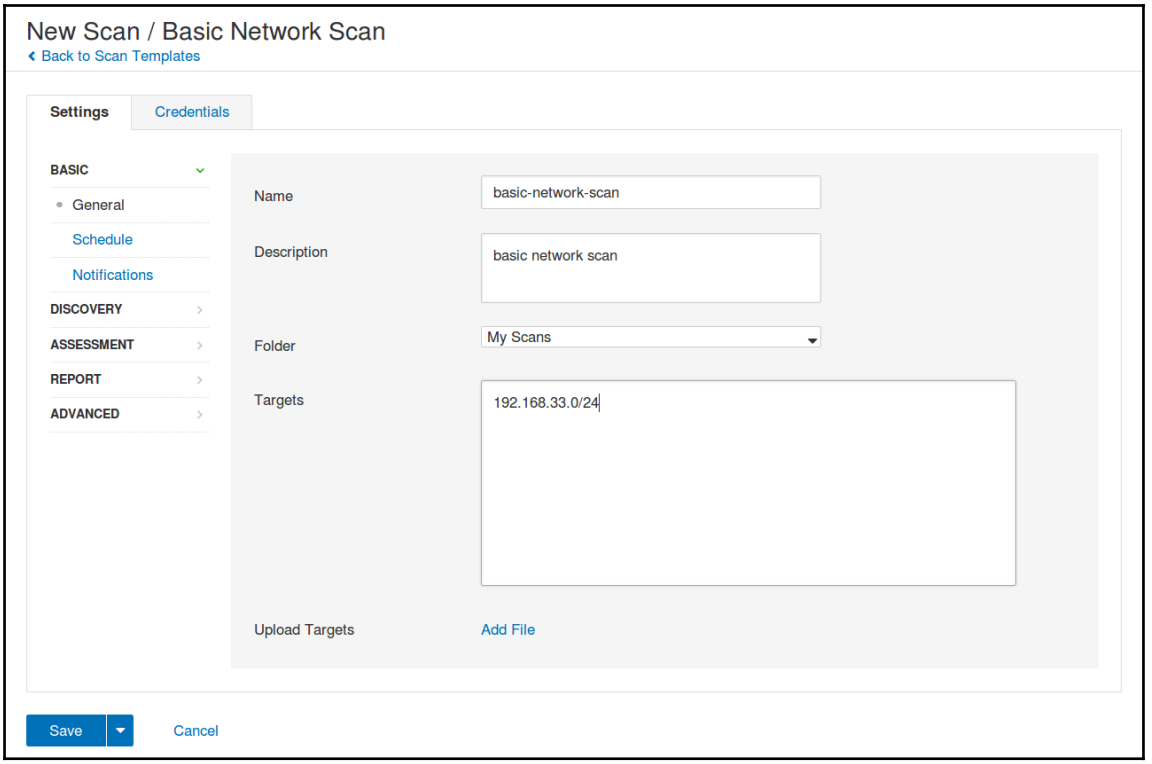

Account Setup
Nessus
In order to use this scanner, an administrative account must be created. This user has full control of the scanner—with the ability to create/delete users, stop running scans, and change the scanner configuration.
Username
poweruser
Password
NOTE: In addition to scanner administration, this account also has the ability to execute commands on hosts being scanned. As such, access should be limited and treated the same as a system-level "root" (or administrator) user.
Continue
Back
© 2017 Tenable Network Security®

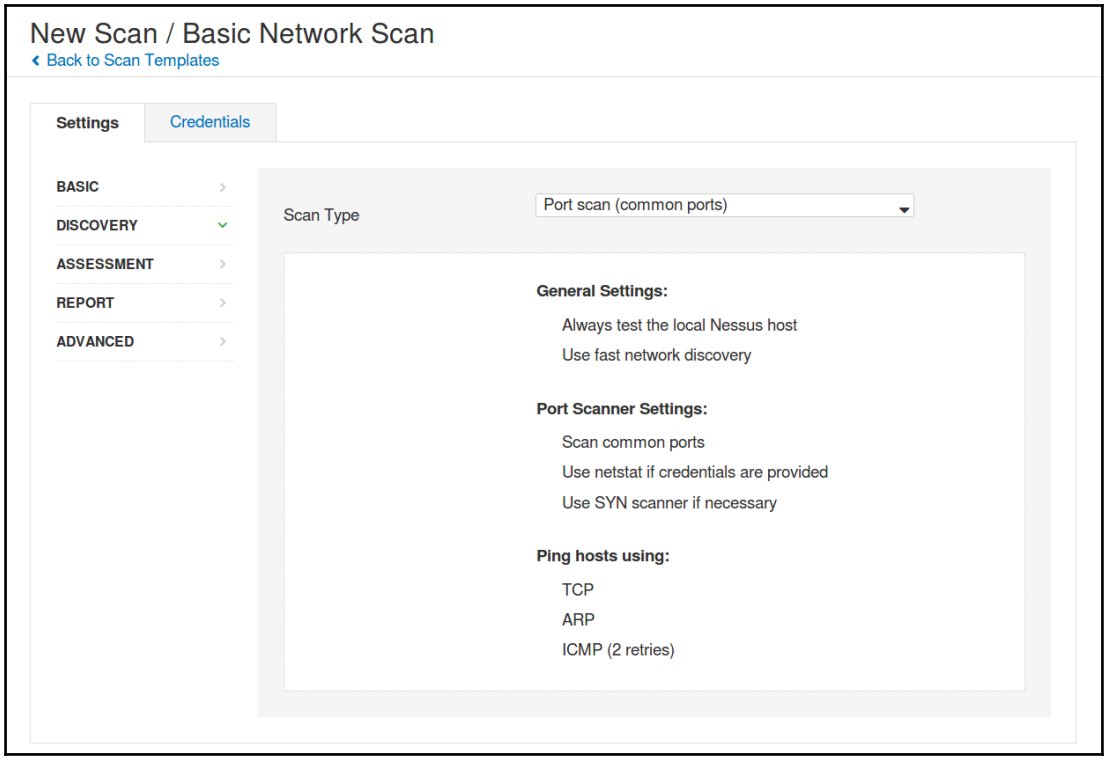

Registration
Nessus
As new vulnerabilities are discovered and released into the public domain, Tenable's research staff creates plugins that allow Nessus to detect their presence. These plugins contain vulnerability information, algorithms to test for the presence of the issue, and a set of remediation actions. Registering this scanner will grant you access to download these plugins.
Registration
Nessus (Home, Professional or Manager)
Activation Code
B089-XXXX-XXXX-XXXX-XXXX
Continue
Back
Advanced Settings
© 2017 Tenable Network Security®

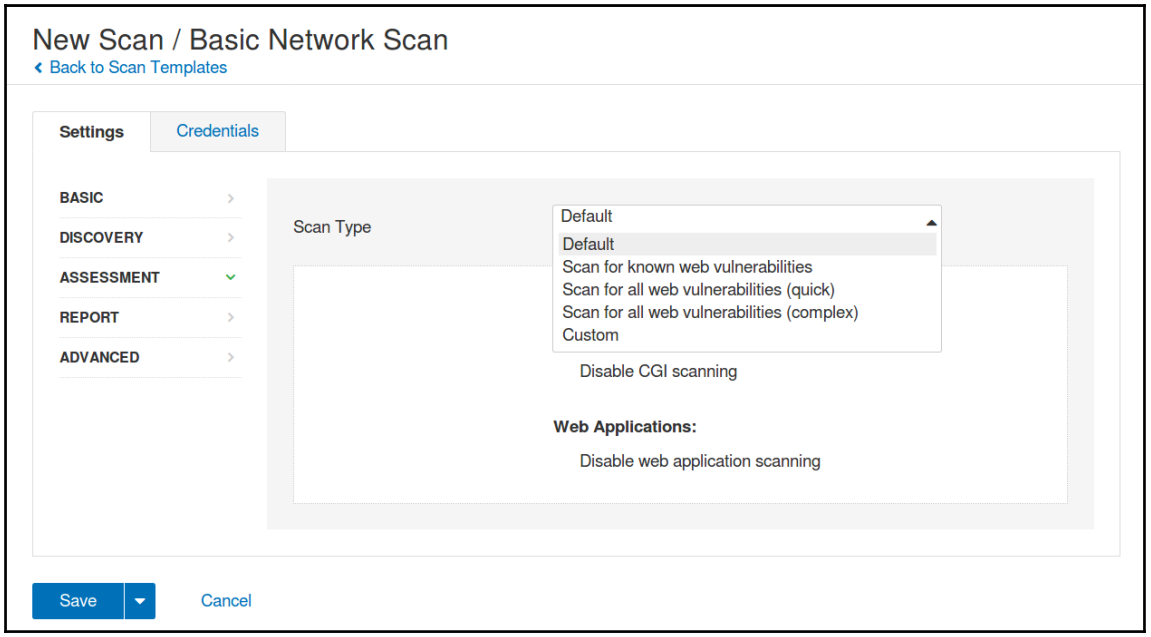

Nessus
poweruser
Remember Me
Sign In
© 2017 Tenable Network Security®

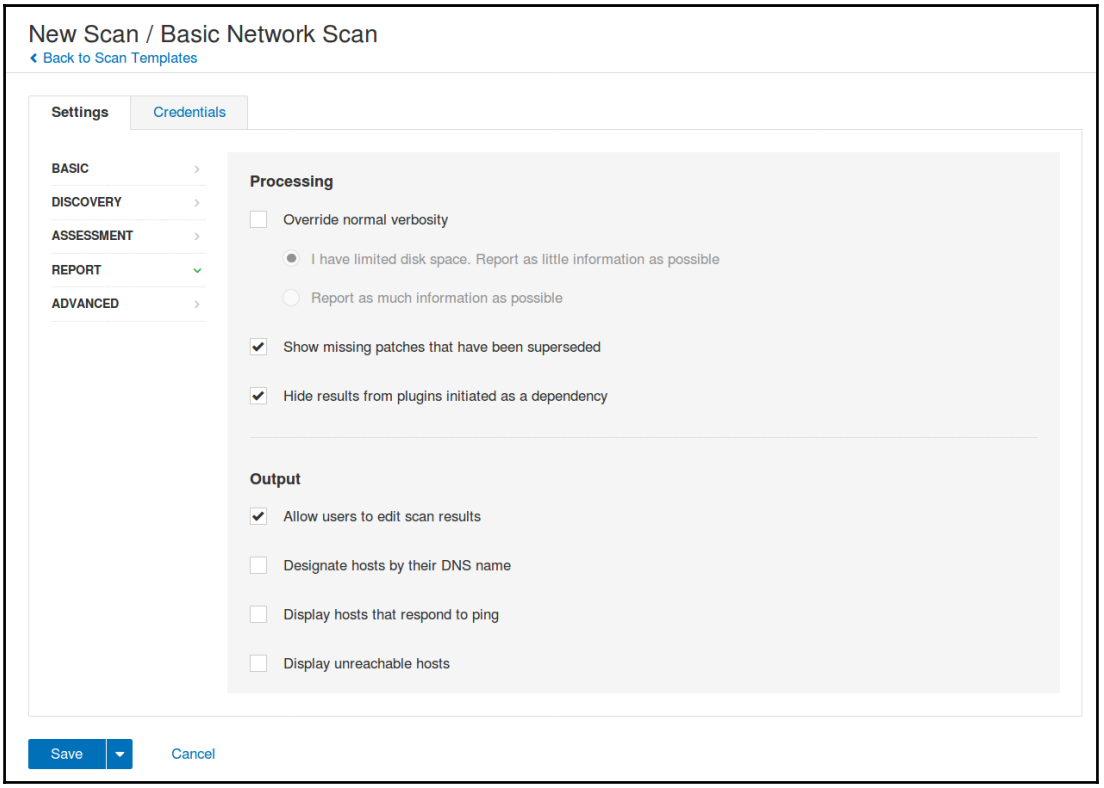

Nessus
Scans
Settings
poweruser
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Hide
Policies
Plugin Rules
Scanners
My Scans
Import
New Folder
New Scan
This folder is empty. Create a new scan.

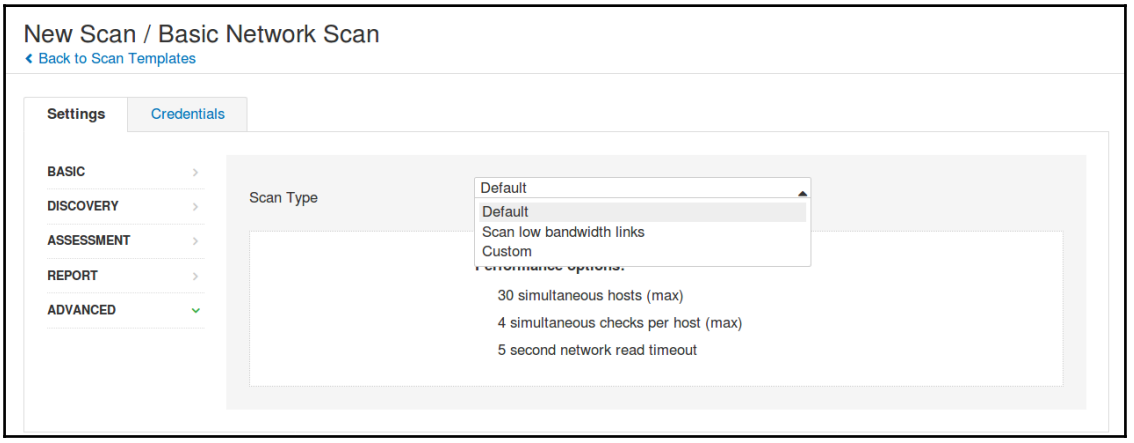

Scan Templates
Back to Scans
Scanner
Search Library
Advanced Scan
Configure a scan without using any recommendations.
Audit Cloud Infrastructure
Audit the configuration of third-party cloud services.
UPGRADE
Badlock Detection
Remote and local checks for CVE-2016-2118 and CVE-2016-0128.
Bash Shellshock Detection
Remote and local checks for CVE-2014-6271 and CVE-2014-7169.
Basic Network Scan
A full system scan suitable for any host.
Credentialed Patch Audit
Authenticate to hosts and enumerate missing updates.
DROWN Detection
Remote checks for CVE-2016-0800.
Host Discovery
A simple scan to discover live hosts and open ports.
Intel AMT Security Bypass
Remote and local checks for CVE-2017-5689.
Internal PCI Network Scan
Perform an internal PCI DSS (11.2.1) vulnerability scan.
UPGRADE
Malware Scan
Scan for malware on Windows and Unix systems.
MDM Config Audit
Audit the configuration of mobile device managers.
UPGRADE

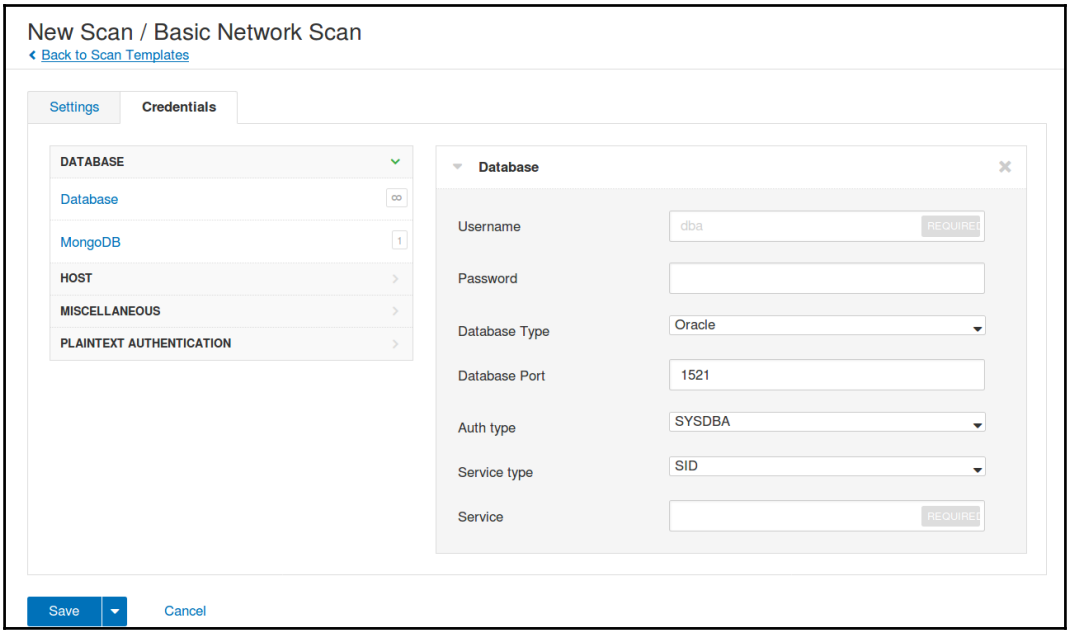

New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
BASIC
General
Schedule
Notifications
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Name
basic-network-scan
Description
basic network scan
Folder
My Scans
Targets
192.168.33.0/24
Upload Targets
Add File
Save
Cancel

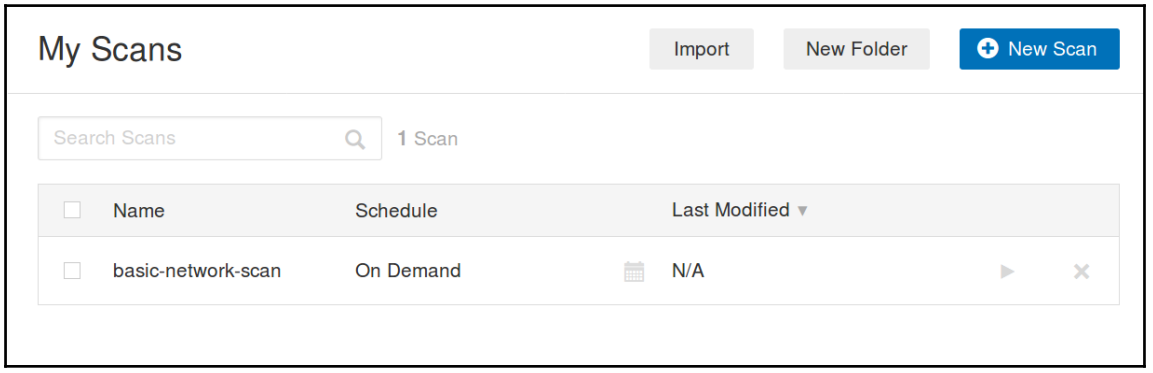

New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Port scan (common ports)
General Settings:
Always test the local Nessus host
Use fast network discovery
Port Scanner Settings:
Scan common ports
Use netstat if credentials are provided
Use SYN scanner if necessary
Ping hosts using:
TCP
ARP
ICMP (2 retries)

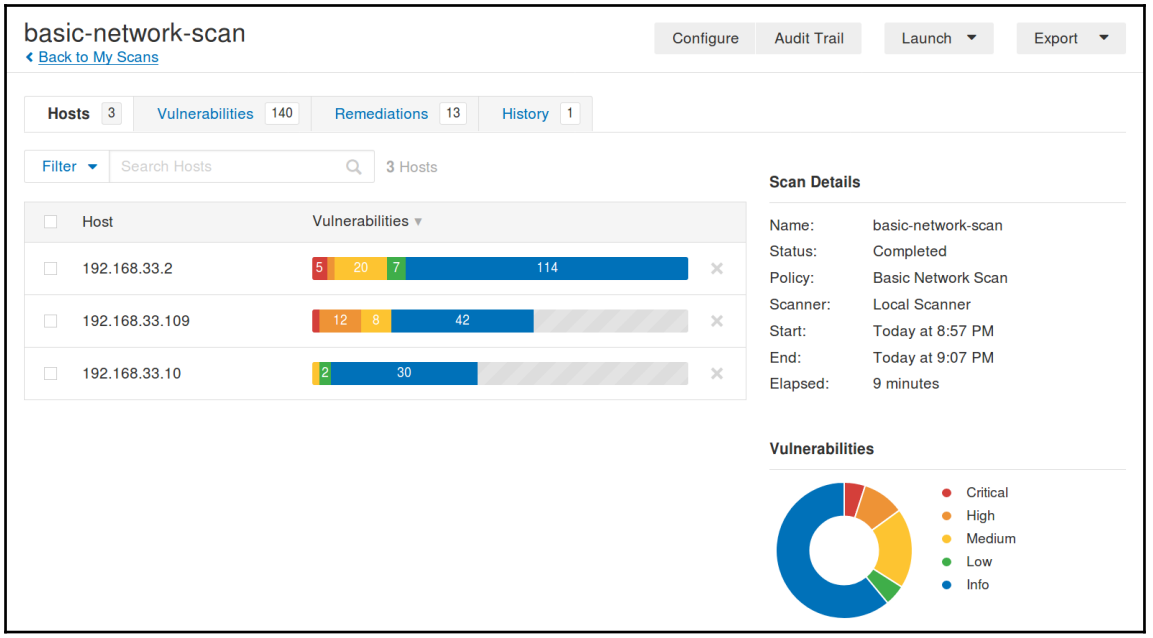

New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Default
Default
Scan for known web vulnerabilities
Scan for all web vulnerabilities (quick)
Scan for all web vulnerabilities (complex)
Custom
Disable CGI scanning
Web Applications:
Disable web application scanning
Save
Cancel

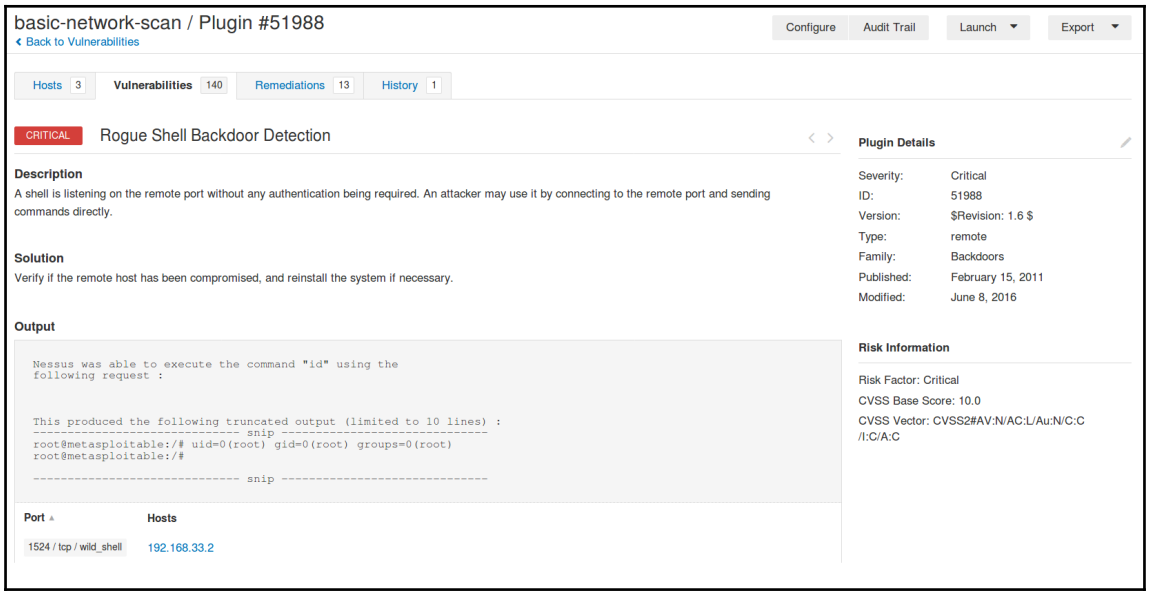

New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Processing
Override normal verbosity
I have limited disk space. Report as little information as possible
Report as much information as possible
Show missing patches that have been superseded
Hide results from plugins initiated as a dependency
Output
Allow users to edit scan results
Designate hosts by their DNS name
Display hosts that respond to ping
Display unreachable hosts
Save
Cancel


New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
BASIC
DISCOVERY
ASSESSMENT
REPORT
ADVANCED
Scan Type
Default
Default
Scan low bandwidth links
Custom
30 simultaneous hosts (max)
4 simultaneous checks per host (max)
5 second network read timeout


New Scan / Basic Network Scan
Back to Scan Templates
Settings
Credentials
DATABASE
Database
MongoDB
HOST
MISCELLANEOUS
PLAINTEXT AUTHENTICATION
Database
Username
dba
REQUIRED
Password
Database Type
Oracle
Database Port
1521
Auth type
SYSDBA
Service type
SID
Service
REQUIRED
Save
Cancel

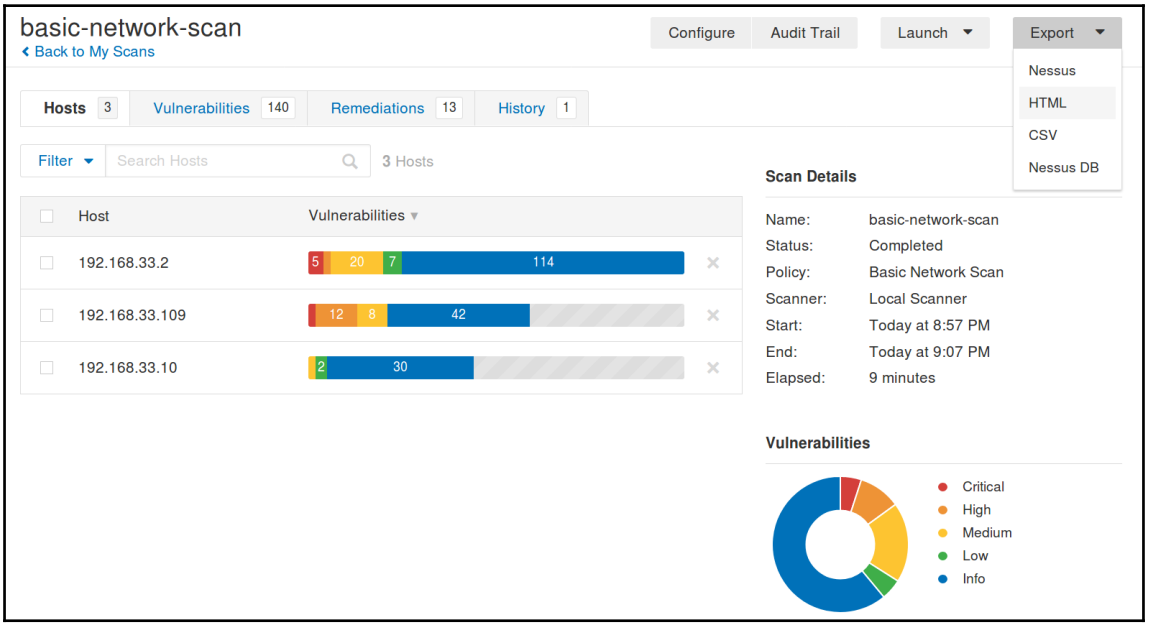

My Scans
Import
New Folder
New Scan
Search Scans
1 Scan
Name
Schedule
Last Modified
basic-network-scan
On Demand
N/A

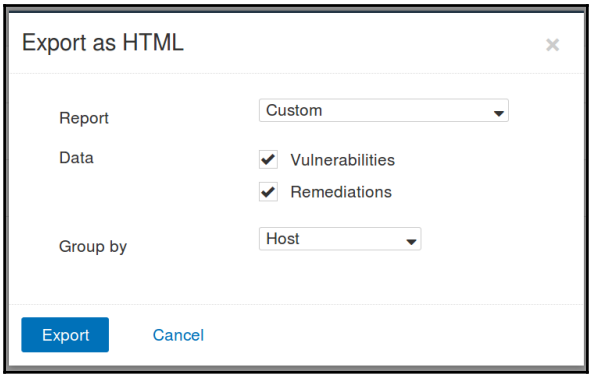

basic-network-scan
Back to My Scans
Configure
Audit Trail
Launch
Export
Hosts 3
Vulnerabilities 140
Remediations 13
History 1
Filter
Search Hosts
3 Hosts
Host
Vulnerabilities
192.168.33.2
5 20 7 114
192.168.33.109
12 8 42
192.168.33.10
2 30
Scan Details
Name: basic-network-scan
Status: Completed
Policy: Basic Network Scan
Scanner: Local Scanner
Start: Today at 8:57 PM
End: Today at 9:07 PM
Elapsed: 9 minutes
Vulnerabilities
Critical
High
Medium
Low
Info

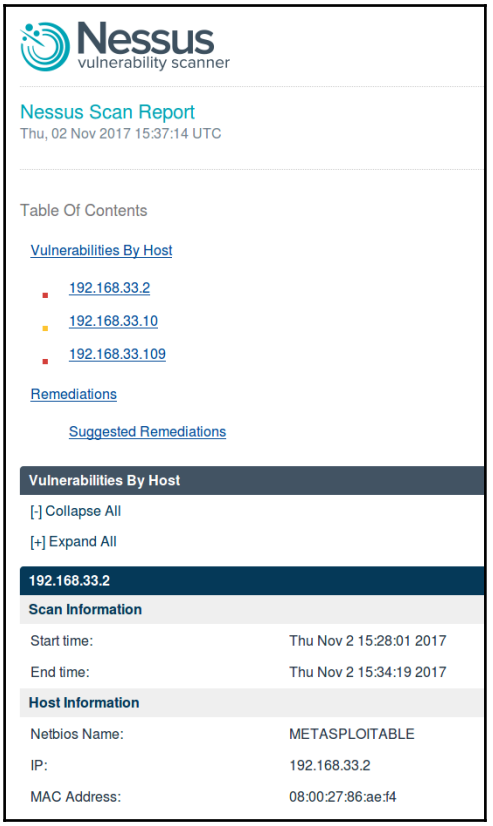

basic-network-scan / Plugin #51988
Back to Vulnerabilities
Configure
Audit Trail
Launch
Export
Hosts 3
Vulnerabilities 140
Remediations 13
History 1
CRITICAL
Rogue Shell Backdoor Detection
Description
A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
Solution
Verify if the remote host has been compromised, and reinstall the system if necessary.
Output
Nessus was able to execute the command "id" using the following request :
This produced the following truncated output (limited to 10 lines) :
snip
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#
snip
Port
Hosts
1524 / tcp / wild_shell
192.168.33.2
Plugin Details
Severity: Critical
ID: 51988
Version: $Revision: 1.6 $
Type: remote
Family: Backdoors
Published: February 15, 2011
Modified: June 8, 2016
Risk Information
Risk Factor: Critical
CVSS Base Score: 10.0
CVSS Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

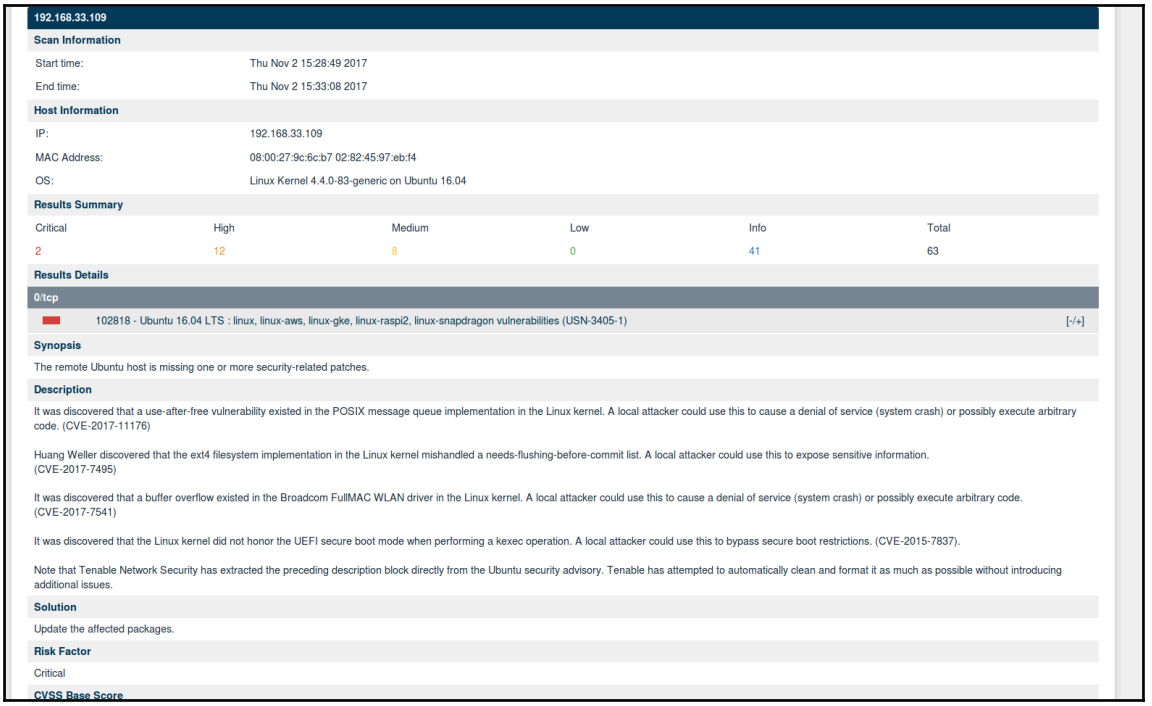
```
TASK [listscans : list current scans and IDs using autoNessus] *****************************************************************************************
changed: [192.168.33.109]

TASK [listscans : debug] *******************************************************************************************************************************
ok: [192.168.33.109] => {
    "msg": [
        "Script started: 11-06-17 @ 17:48:24",
        "Logging in...",
        "Logged in!",
        "",
        "",
        "Scan Name                Status            ID",
        "-----------------------------------------",
        "webapp                :    paused        :    17",
        "basic-network-scan    :    completed     :    6"
    ]
}
```

```
TASK [startscan : starting nessus scan "17" using autoNessus] ******************************************************************************************
changed: [192.168.33.109]

TASK [startscan : debug] *******************************************************************************************************************************
ok: [192.168.33.109] => {
    "msg": [
        "Script started: 11-06-17 @ 17:52:34",
        "Logging in...",
        "Logged in!",
        "",
        "",
        "Launching Scan 17",
        "",
        "Scan Name           Status  ",
        "-------------------------------------",
        "webapp           :  running"
    ]
}
```




Export as HTML
Report
Custom
Data
Vulnerabilities
Remediations
Group by
Host
Export
Cancel


Nessus
vulnerability scanner
Nessus Scan Report
Thu, 02 Nov 2017 15:37:14 UTC
Table Of Contents
Vulnerabilities By Host
192.168.33.2
192.168.33.10
192.168.33.109
Remediations
Suggested Remediations
Vulnerabilities By Host
[-] Collapse All
[+] Expand All
192.168.33.2
Scan Information
Start time: Thu Nov 2 15:28:01 2017
End time: Thu Nov 2 15:34:19 2017
Host Information
Netbios Name: METASPLOITABLE
IP: 192.168.33.2
MAC Address: 08:00:27:86:ae:f4



192.168.33.109

Scan Information

Start time:	Thu Nov 2 15:28:49 2017
End time:	Thu Nov 2 15:33:08 2017

Host Information

IP:	192.168.33.109
MAC Address:	08:00:27:9c:6c:b7 02:82:45:97:eb:f4
OS:	Linux Kernel 4.4.0-83-generic on Ubuntu 16.04

Results Summary

Critical	High	Medium	Low	Info	Total
2	12	8	0	41	63

Results Details

0/tcp

102818 - Ubuntu 16.04 LTS : linux, linux-aws, linux-gke, linux-raspi2, linux-snapdragon vulnerabilities (USN-3405-1) [-/+]

Synopsis

The remote Ubuntu host is missing one or more security-related patches.

Description

It was discovered that a use-after-free vulnerability existed in the POSIX message queue implementation in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-11176)

Huang Weller discovered that the ext4 filesystem implementation in the Linux kernel mishandled a needs-flushing-before-commit list. A local attacker could use this to expose sensitive information. (CVE-2017-7495)

It was discovered that a buffer overflow existed in the Broadcom FullMAC WLAN driver in the Linux kernel. A local attacker could use this to cause a denial of service (system crash) or possibly execute arbitrary code. (CVE-2017-7541)

It was discovered that the Linux kernel did not honor the UEFI secure boot mode when performing a kexec operation. A local attacker could use this to bypass secure boot restrictions. (CVE-2015-7837).

Note that Tenable Network Security has extracted the preceding description block directly from the Ubuntu security advisory. Tenable has attempted to automatically clean and format it as much as possible without introducing additional issues.

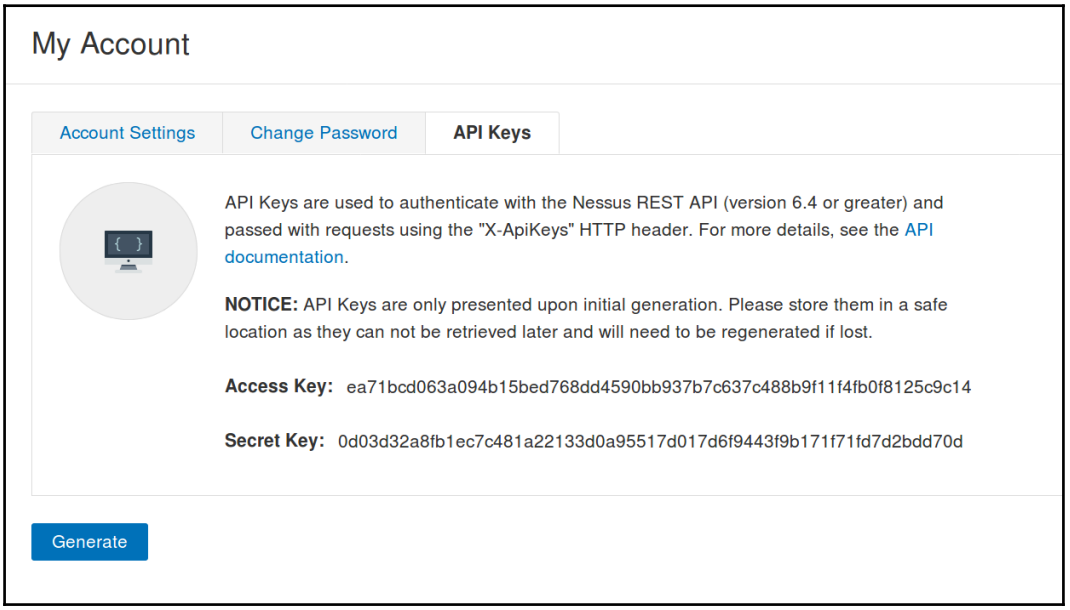
Solution

Update the affected packages.

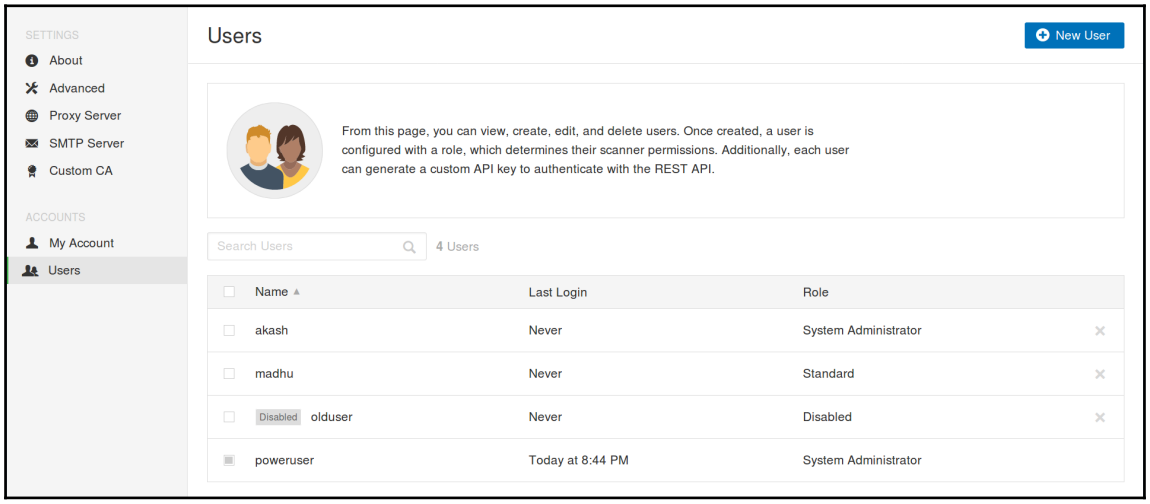
Risk Factor

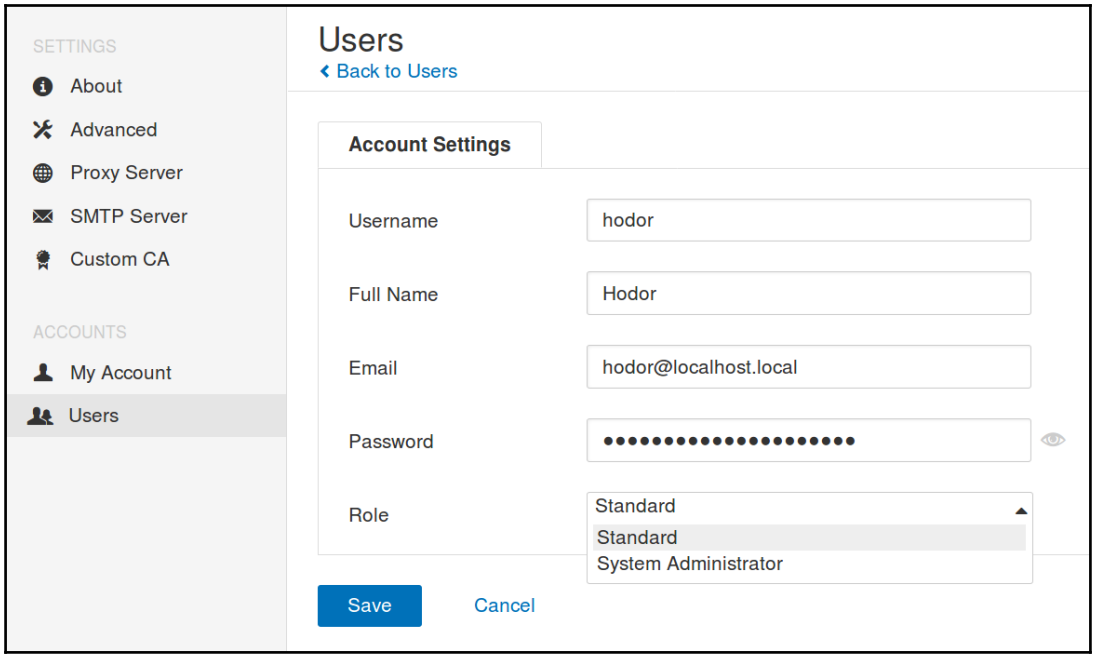
Critical

CVSS Base Score



```
$ ansible-playbook site.yml
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available


PLAY [working with nessus rest api] ********************************************************************************************************************************************************

TASK [download_report : export the report for given scan "17"] *****************************************************************************************************************************
ok: [localhost]

TASK [download_report : debug] *************************************************************************************************************************************************************
ok: [localhost] => {
    "msg": "File id is 834426329 and scan id is 17"
}

TASK [download_report : check the report status for "834426329"] ***************************************************************************************************************************
ok: [localhost]

TASK [download_report : debug] *************************************************************************************************************************************************************
ok: [localhost] => {
    "msg": "Report status is ready"
}

TASK [download_report : downloading the report locally] ************************************************************************************************************************************
changed: [localhost]

TASK [download_report : debug] *************************************************************************************************************************************************************
ok: [localhost] => {
    "msg": "Report can be found at ./17_834426329.html"
}

PLAY RECAP *********************************************************************************************************************************************************************************
localhost                  : ok=6    changed=1    unreachable=0    failed=0
```

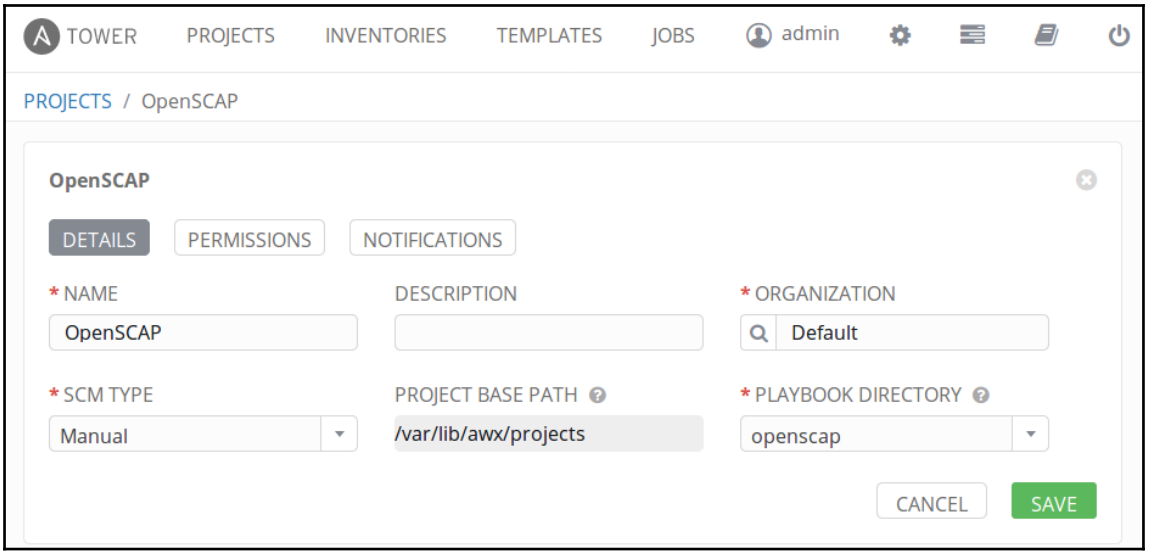


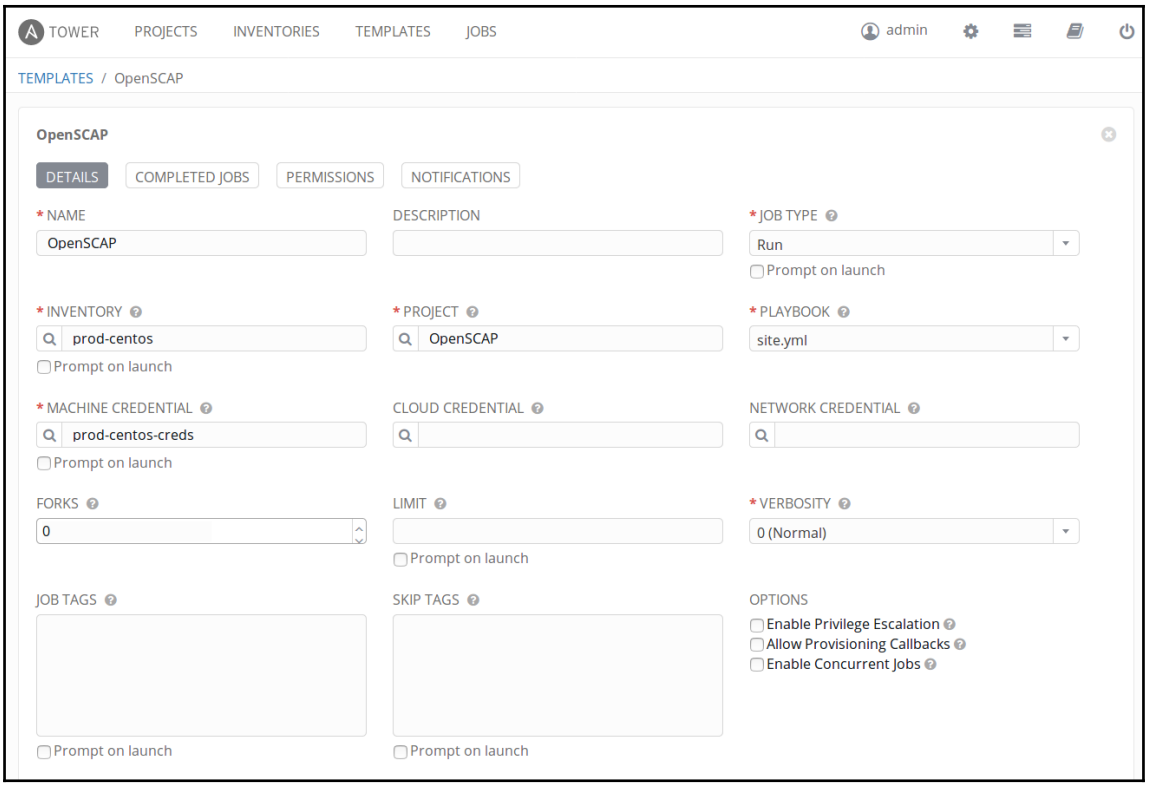

SETTINGS
About
Advanced
Proxy Server
SMTP Server
Custom CA
ACCOUNTS
My Account
Users
Users
Back to Users
Account Settings
Username
hodor
Full Name
Hodor
Email
hodor@localhost.local
Password
Role
Standard
Standard
System Administrator
Save
Cancel

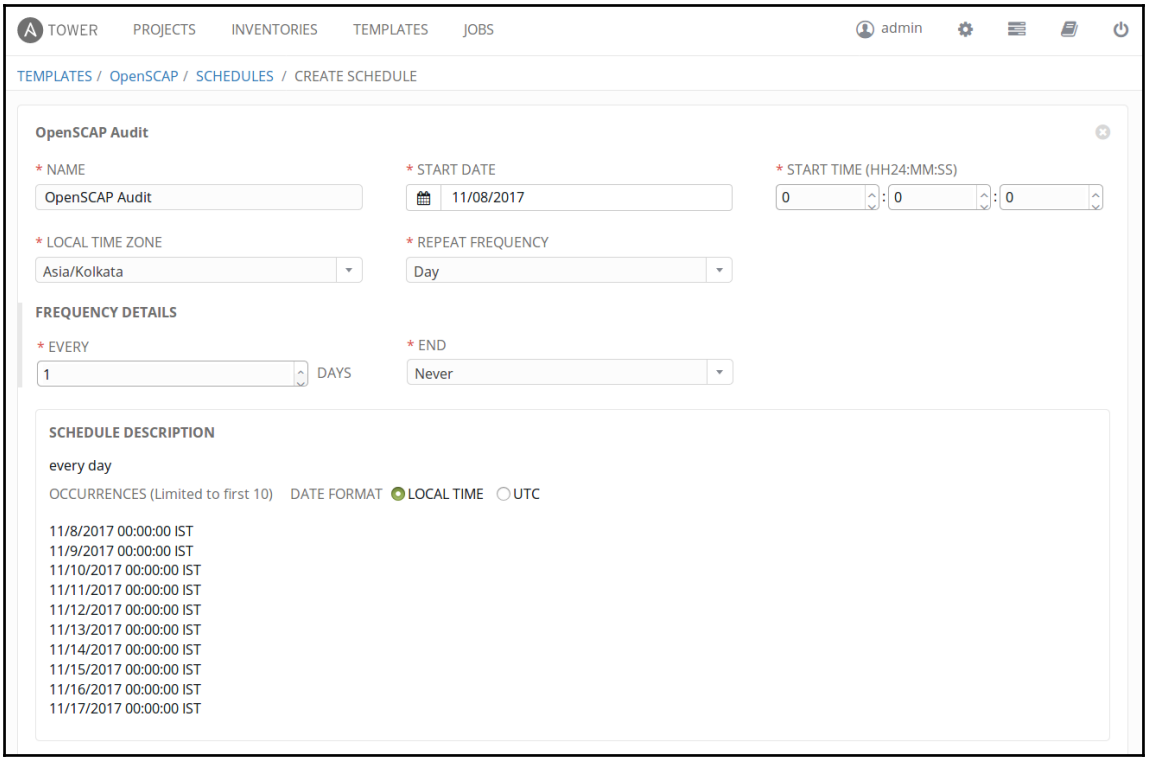
Chapter 07: Security Hardening for Applications and Networks

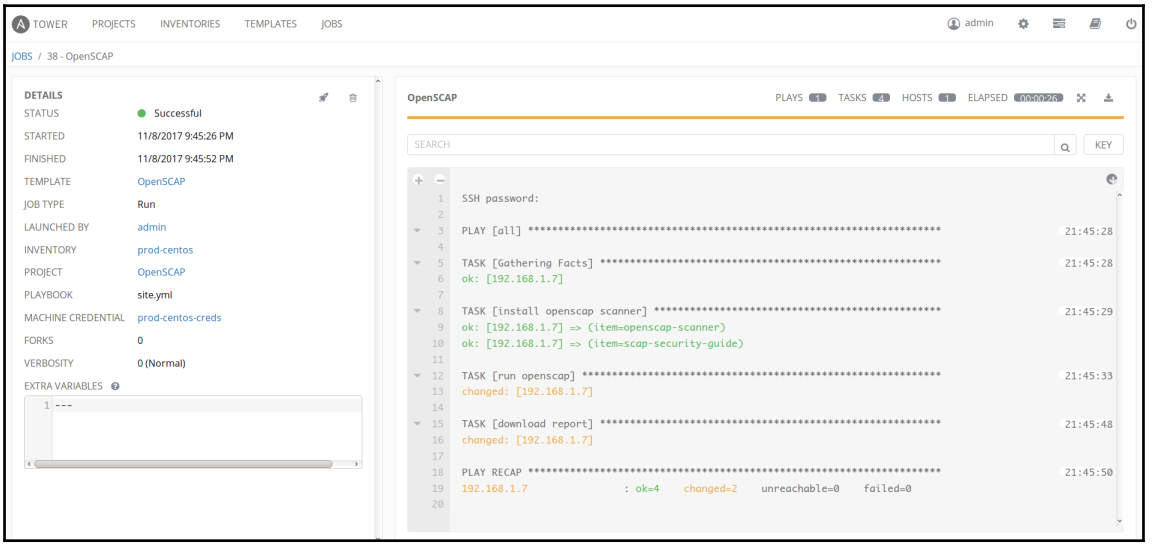
```
$ ansible-playbook site.yml
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available

[DEPRECATION WARNING]: The use of 'include' for tasks has been deprecated. Use 'import_tasks' for static inclusions or 'include_tasks' for dynamic inclusions. This feature
will be removed in a future release. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[DEPRECATION WARNING]: include is kept for backwards compatibility but usage is discouraged. The module documentation details page may explain more about this rationale..
This feature will be removed in a future release. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.

PLAY [localhost] ***************************************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************
ok: [localhost]

TASK [dev-sec.os-hardening : Set OS family dependent variables] ****************************************************************************************************
ok: [localhost]

TASK [dev-sec.os-hardening : Set OS dependent variables] ***********************************************************************************************************

TASK [dev-sec.os-hardening : create limits.d-directory if it does not exist | sysctl-31a, sysctl-31b] *************************************************************
skipping: [localhost]

TASK [dev-sec.os-hardening : create sane limits.conf | sysctl-31a, sysctl-31b] *************************************************************************************
skipping: [localhost]

TASK [dev-sec.os-hardening : create login.defs | os-05, os-05b] ****************************************************************************************************
changed: [localhost]

TASK [dev-sec.os-hardening : find directories for minimizing access] ***********************************************************************************************
ok: [localhost] => (item=/usr/local/sbin)
ok: [localhost] => (item=/usr/local/bin)
ok: [localhost] => (item=/usr/sbin)
ok: [localhost] => (item=/usr/bin)
ok: [localhost] => (item=/sbin)
ok: [localhost] => (item=/bin)

TASK [dev-sec.os-hardening : minimize access] **********************************************************************************************************************
ok: [localhost] => (item={'_ansible_parsed': True, u'stat': {u'isuid': False, u'uid': 0, u'exists': True, u'attr_flags': u'e', u'woth': False, u'isreg': False, u'device_type'
: 0, u'mtime': 1500647698.7412262, u'block_size': 4096, u'inode': 66669, u'isgid': False, u'size': 4096, u'executable': True, u'charset': u'binary', u'readable': True, u'vers
ion': u'1546678241', u'pw_name': u'root', u'gid': 0, u'ischr': False, u'wusr': True, u'writeable': True, u'mimetype': u'inode/directory', u'blocks': 8, u'xoth': True, u'islnk
': False, u'nlink': 2, u'issock': False, u'rgrp': True, u'gr_name': u'root', u'path': u'/usr/local/sbin', u'xusr': True, u'atime': 1510075677.0864868, u'isdir': True, u'ctime
': 1500648230.5338638, u'isblk': False, u'wgrp': False, u'xgrp': True, u'dev': 2049, u'roth': True, u'isfifo': False, u'mode': u'0755', u'rusr': True, u'attributes': [u'exten
```

```
$ ansible-playbook -i inventory.ini main.yml --ask-pass
SSH password:
[DEPRECATION WARNING]: The use of 'include' for tasks has been deprecated. Use 'import_tasks' for static inclusions or 'include_tasks' for dynamic inclusions. This feature
will be removed in a future release. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[DEPRECATION WARNING]: include is kept for backwards compatibility but usage is discouraged. The module documentation details page may explain more about this rationale..
This feature will be removed in a future release. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.

PLAY [STIGs ansible-hardening for automated security hardening] ****************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : Gather variables for each operating system] **********************************************************************************************
ok: [192.168.1.7] => (item=/home/ubuntu/.ansible/roles/ansible-hardening/vars/redhat.yml)

TASK [ansible-hardening : Check for check/audit mode] **************************************************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : Check to see if we are booting with EFI or UEFI] *****************************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : Set facts] *******************************************************************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : Check if grub is present on the remote node] *********************************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : include] *********************************************************************************************************************************
included: /home/ubuntu/.ansible/roles/ansible-hardening/tasks/rhel7stig/main.yml for 192.168.1.7

TASK [ansible-hardening : Create temporary directory to hold any temporary files] **********************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : Set a fact for the temporary directory] **************************************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : include] *********************************************************************************************************************************
included: /home/ubuntu/.ansible/roles/ansible-hardening/tasks/rhel7stig/async_tasks.yml for 192.168.1.7

TASK [ansible-hardening : Verify all installed RPM packages] *******************************************************************************************************
ok: [192.168.1.7]

TASK [ansible-hardening : Check for .shosts or shosts.equiv files] *************************************************************************************************
skipping: [192.168.1.7]
```

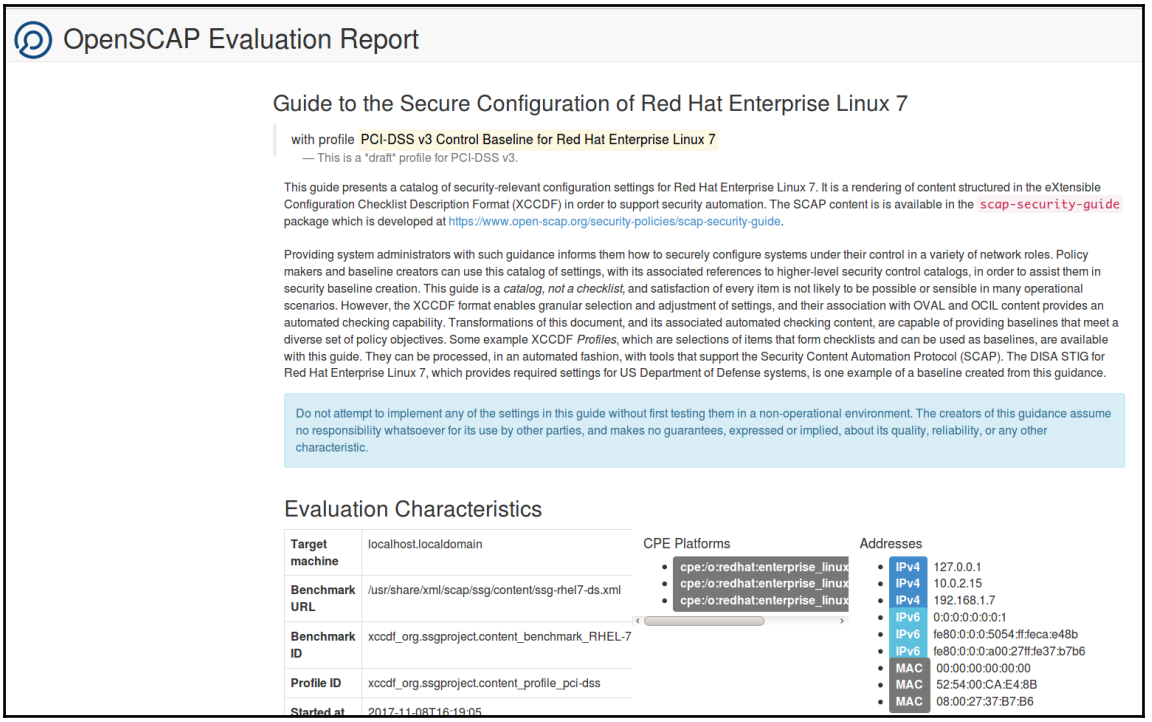

TOWER
PROJECTS
INVENTORIES
TEMPLATES
JOBS
admin
PROJECTS / OpenSCAP
OpenSCAP
DETAILS
PERMISSIONS
NOTIFICATIONS
* NAME
OpenSCAP
DESCRIPTION
* ORGANIZATION
Default
* SCM TYPE
Manual
PROJECT BASE PATH
/var/lib/awx/projects
* PLAYBOOK DIRECTORY
openscap
CANCEL
SAVE

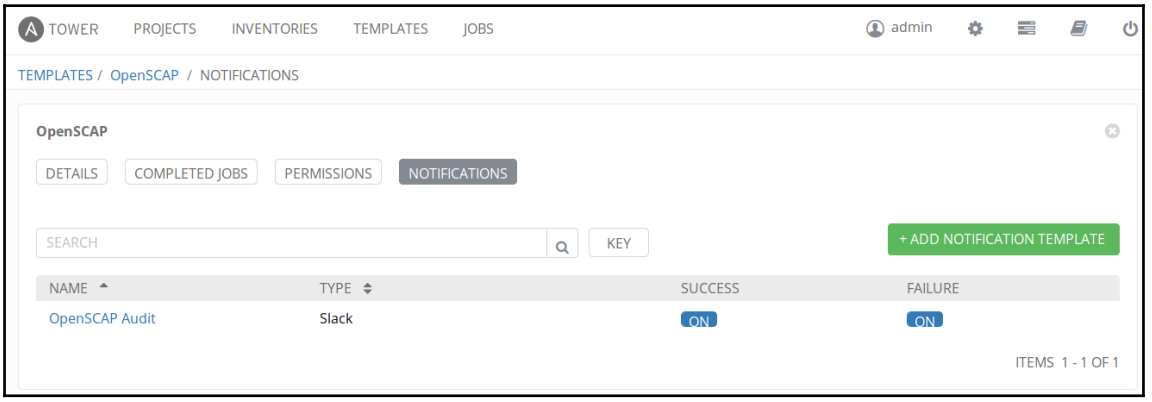

TOWER
PROJECTS
INVENTORIES
TEMPLATES
JOBS
admin
TEMPLATES / OpenSCAP
OpenSCAP
DETAILS
COMPLETED JOBS
PERMISSIONS
NOTIFICATIONS
* NAME
OpenSCAP
DESCRIPTION
* JOB TYPE
Run
Prompt on launch
* INVENTORY
prod-centos
Prompt on launch
* PROJECT
OpenSCAP
* PLAYBOOK
site.yml
* MACHINE CREDENTIAL
prod-centos-creds
Prompt on launch
CLOUD CREDENTIAL
NETWORK CREDENTIAL
FORKS
0
LIMIT
Prompt on launch
* VERBOSITY
0 (Normal)
JOB TAGS
Prompt on launch
SKIP TAGS
Prompt on launch
OPTIONS
Enable Privilege Escalation
Allow Provisioning Callbacks
Enable Concurrent Jobs


TOWER
PROJECTS
INVENTORIES
TEMPLATES
JOBS
admin
TEMPLATES / OpenSCAP / SCHEDULES / CREATE SCHEDULE
OpenSCAP Audit
* NAME
OpenSCAP Audit
* START DATE
11/08/2017
* START TIME (HH24:MM:SS)
0 : 0 : 0
* LOCAL TIME ZONE
Asia/Kolkata
* REPEAT FREQUENCY
Day
FREQUENCY DETAILS
* EVERY
1
DAYS
* END
Never
SCHEDULE DESCRIPTION
every day
OCCURRENCES (Limited to first 10)
DATE FORMAT
LOCAL TIME
UTC
11/8/2017 00:00:00 IST
11/9/2017 00:00:00 IST
11/10/2017 00:00:00 IST
11/11/2017 00:00:00 IST
11/12/2017 00:00:00 IST
11/13/2017 00:00:00 IST
11/14/2017 00:00:00 IST
11/15/2017 00:00:00 IST
11/16/2017 00:00:00 IST
11/17/2017 00:00:00 IST

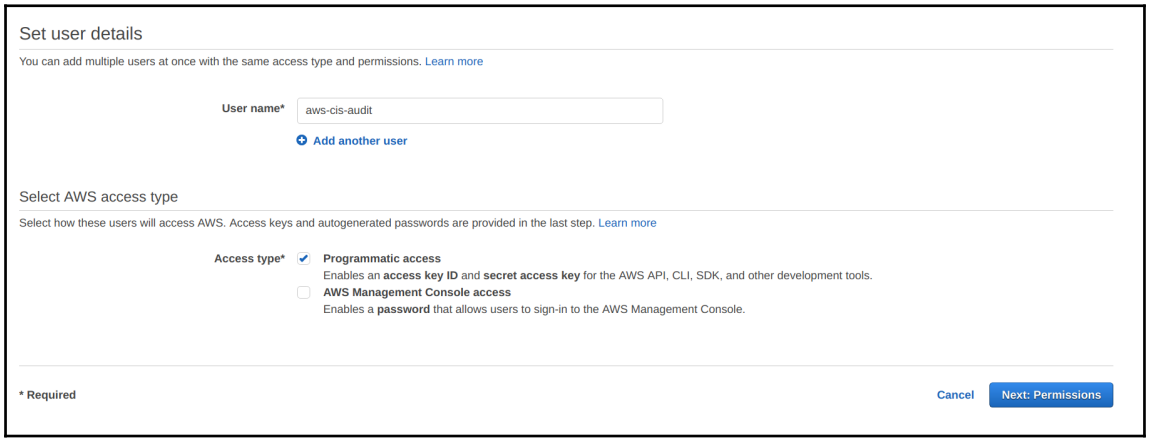

TOWER
PROJECTS
INVENTORIES
TEMPLATES
JOBS
admin
JOBS / 38 - OpenSCAP
DETAILS
STATUS
Successful
STARTED
11/8/2017 9:45:26 PM
FINISHED
11/8/2017 9:45:52 PM
TEMPLATE
OpenSCAP
JOB TYPE
Run
LAUNCHED BY
admin
INVENTORY
prod-centos
PROJECT
OpenSCAP
PLAYBOOK
site.yml
MACHINE CREDENTIAL
prod-centos-creds
FORKS
0
VERBOSITY
0 (Normal)
EXTRA VARIABLES

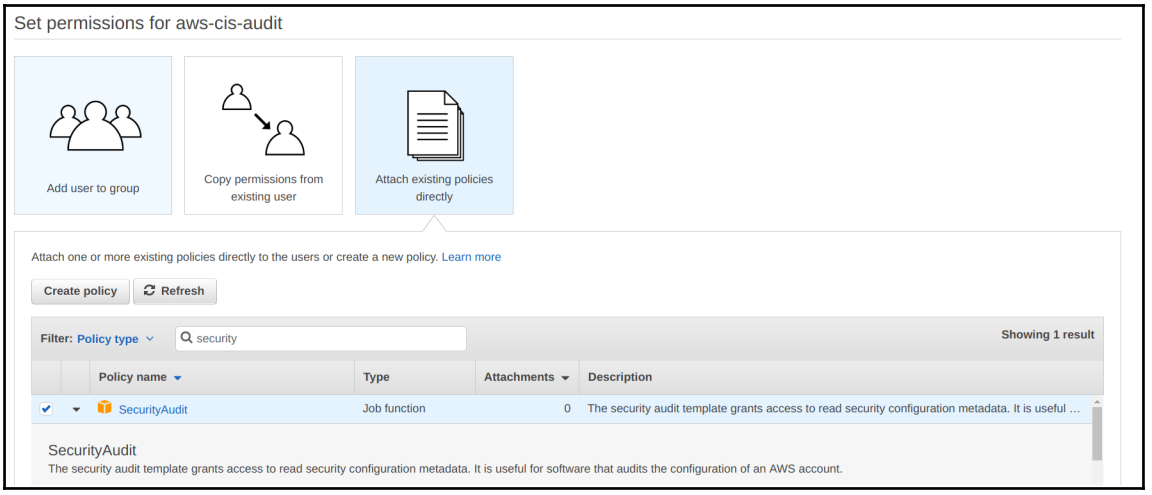
OpenSCAP
PLAYS 1
TASKS 4
HOSTS 1
ELAPSED 00:00:27
SEARCH
KEY
SSH password:
PLAY [all] ********** 21:45:28
TASK [Gathering Facts] ********** 21:45:28
ok: [192.168.1.7]
TASK [install openscap scanner] ********** 21:45:29
ok: [192.168.1.7] => (item=openscap-scanner)
ok: [192.168.1.7] => (item=scap-security-guide)
TASK [run openscap] ********** 21:45:33
changed: [192.168.1.7]
TASK [download report] ********** 21:45:48
changed: [192.168.1.7]
PLAY RECAP ********** 21:45:50
192.168.1.7 : ok=4 changed=2 unreachable=0 failed=0

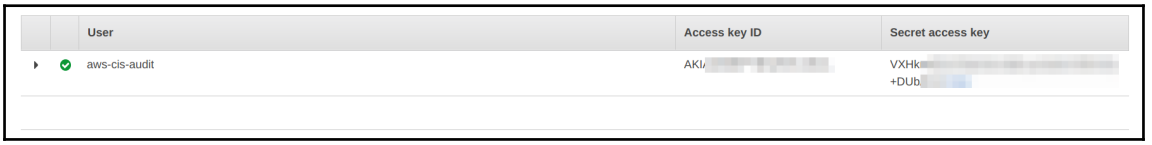

OpenSCAP Evaluation Report
Guide to the Secure Configuration of Red Hat Enterprise Linux 7
with profile PCI-DSS v3 Control Baseline for Red Hat Enterprise Linux 7
— This is a *draft* profile for PCI-DSS v3.
This guide presents a catalog of security-relevant configuration settings for Red Hat Enterprise Linux 7. It is a rendering of content structured in the eXtensible Configuration Checklist Description Format (XCCDF) in order to support security automation. The SCAP content is is available in the scap-security-guide package which is developed at https://www.open-scap.org/security-policies/scap-security-guide.
Providing system administrators with such guidance informs them how to securely configure systems under their control in a variety of network roles. Policy makers and baseline creators can use this catalog of settings, with its associated references to higher-level security control catalogs, in order to assist them in security baseline creation. This guide is a catalog, not a checklist, and satisfaction of every item is not likely to be possible or sensible in many operational scenarios. However, the XCCDF format enables granular selection and adjustment of settings, and their association with OVAL and OCIL content provides an automated checking capability. Transformations of this document, and its associated automated checking content, are capable of providing baselines that meet a diverse set of policy objectives. Some example XCCDF Profiles, which are selections of items that form checklists and can be used as baselines, are available with this guide. They can be processed, in an automated fashion, with tools that support the Security Content Automation Protocol (SCAP). The DISA STIG for Red Hat Enterprise Linux 7, which provides required settings for US Department of Defense systems, is one example of a baseline created from this guidance.
Do not attempt to implement any of the settings in this guide without first testing them in a non-operational environment. The creators of this guidance assume no responsibility whatsoever for its use by other parties, and makes no guarantees, expressed or implied, about its quality, reliability, or any other characteristic.
Evaluation Characteristics
Target machine
localhost.localdomain
Benchmark URL
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
Benchmark ID
xccdf_org.ssgproject.content_benchmark_RHEL-7
Profile ID
xccdf_org.ssgproject.content_profile_pci-dss
Started at
2017-11-08T16:19:05
CPE Platforms
cpe:/o:redhat:enterprise_linux
cpe:/o:redhat:enterprise_linux
cpe:/o:redhat:enterprise_linux
Addresses
IPv4 127.0.0.1
IPv4 10.0.2.15
IPv4 192.168.1.7
IPv6 0:0:0:0:0:0:0:1
IPv6 fe80:0:0:0:5054:ff:feca:e48b
IPv6 fe80:0:0:0:a00:27ff:fe37:b7b6
MAC 00:00:00:00:00:00
MAC 52:54:00:CA:E4:8B
MAC 08:00:27:37:B7:B6


TOWER
PROJECTS
INVENTORIES
TEMPLATES
JOBS
admin
TEMPLATES / OpenSCAP / NOTIFICATIONS
OpenSCAP
DETAILS
COMPLETED JOBS
PERMISSIONS
NOTIFICATIONS
SEARCH
KEY
+ ADD NOTIFICATION TEMPLATE
NAME
TYPE
SUCCESS
FAILURE
OpenSCAP Audit
Slack
ON
ON
ITEMS 1 - 1 OF 1

```
$ ansible-playbook cis.yml
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available

[DEPRECATION WARNING]: The use of 'include' for tasks has been deprecated. Use 'import_tasks' for static inclusions or 'include_tasks' for dynamic inclusions. This feature
will be removed in a future release. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.
[DEPRECATION WARNING]: include is kept for backwards compatibility but usage is discouraged. The module documentation details page may explain more about this rationale..
This feature will be removed in a future release. Deprecation warnings can be disabled by setting deprecation_warnings=False in ansible.cfg.

PLAY [localhost] ***************************************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************
ok: [localhost]

TASK [cis : 1.1 Install Updates, Patches and Additional Security Software (Not Scored)] ****************************************************************************

changed: [localhost]

TASK [cis : Check if reboot is required] ***************************************************************************************************************************
changed: [localhost]

TASK [cis : Reboot host to apply updates] **************************************************************************************************************************
skipping: [localhost]

TASK [cis : Wait for the host to finish rebooting] ******************************************************************************************************************
skipping: [localhost]

TASK [cis : 2.1 Create Separate Partition for /tmp (Scored)] *******************************************************************************************************
ok: [localhost] => {
    "msg": "*** Manually create separate partition for /tmp"
}

TASK [cis : 2.2 - 2.4 Set nodev,nosuid,noexec option for /tmp Partition (Scored)] **********************************************************************************
skipping: [localhost] => (item={u'block_used': 338415, u'uuid': u'3e13556e-d28d-407b-bcc6-97160eafebe1', u'size_total': 10340831232, u'block_total': 2524617, u'inode_availabl
e': 1184043, u'block_available': 2186202, u'size_available': 8954683392, u'fstype': u'ext4', u'inode_total': 1280000, u'mount': u'/', u'device': u'/dev/sda1', u'inode_used':
95957, u'block_size': 4096, u'options': u'rw,relatime,data=ordered'})

TASK [cis : 2.5 Create Separate Partition for /var (Scored)] *******************************************************************************************************
ok: [localhost] => {
    "msg": "*** Manually create separate partition for /var"
}
```








```
$ ansible-playbook main.yml
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available


PLAY [AWS CIS Benchmarks playbook] *********************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [localhost]

TASK [installing python2] ******************************************************************************************
changed: [localhost]

TASK [installing pip] **********************************************************************************************
ok: [localhost]

TASK [installing aws cli and ansi2html] ****************************************************************************
ok: [localhost] => (item=awscli)
ok: [localhost] => (item=ansi2html)

TASK [downloading and setting up prowler] **************************************************************************
ok: [localhost]

TASK [running prowler full scan] ***********************************************************************************
changed: [localhost]

TASK [AWS CIS Benchmarks report downloaded] ************************************************************************
ok: [localhost] => {
    "msg": "Report can be found at ./aws-cis-report-1510253857.html"
}

PLAY RECAP *********************************************************************************************************
localhost                  : ok=7    changed=2    unreachable=0    failed=0
```

```
 _ __ _ __ _____      _| | ___ _ __
| '_ \| '__/ _ \ \ /\ / / |/ _ \ '__|
| |_) | | | (_) \ V  V /| |  __/ |
| .__/|_|  \___/ \_/\_/ |_|\___|_|
|_| CIS based AWS Account Hardening Tool

 Date: Thu Nov  9 18:57:46 UTC 2017

Colors Code for results:  INFORMATIVE, OK (RECOMMENDED VALUE),  WARNING (FIX REQUIRED)


This report is being generated using credentials below:

AWS-CLI Profile: [ENV] AWS API Region: [us-east-1] AWS Filter Region: [all]

Caller Identity:
-----------------------------------------------------------------
|                       GetCallerIdentity                       |
+---------+-----------------------------------------------------+
|  Account|  [redacted]                                         |
|  Arn    |  arn:aws:iam::[redacted]:user/aws-cis-audit         |
|  UserId |  [redacted]                                         |
+---------+-----------------------------------------------------+


 0.1  Generating AWS IAM Credential Report...

 1  Identity and Access Management ***************************************

 1.1  Avoid the use of the root account (Scored).
       INFO! Root account last accessed (password key_1 key_2): 2017-11-09T18:28:52+00:00 N/A N/A

 1.2  Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a console password (Scored)
       OK!  No users found with Password enabled and MFA disabled

 1.3  Ensure credentials unused for 90 days or greater are disabled (Scored)
       OK!  No users found with password enabled

 1.4  Ensure access keys are rotated every 90 days or less (Scored)
       WARNING!  stack has not rotated access key1 in over 90 days
       OK!  No users with access key 2.

 1.5  Ensure IAM password policy requires at least one uppercase letter (Scored)
       WARNING! Password Policy missing upper-case requirement

 1.6  Ensure IAM password policy require at least one lowercase letter (Scored)
       WARNING! Password Policy missing lower-case requirement
```

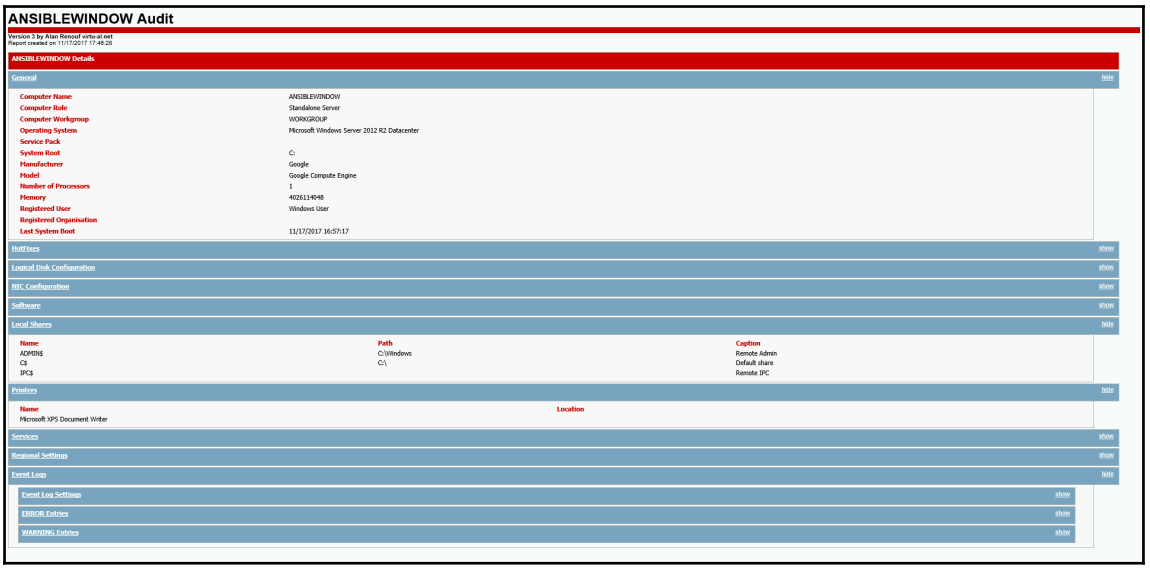
```
$ ansible-playbook -i inventory main.yml --ask-pass
SSH password:

PLAY [Lynis security audit playbook] ***************************************

TASK [Gathering Facts] *****************************************************
ok: [192.168.1.5]

TASK [adding lynis repo key] ***********************************************
ok: [192.168.1.5]

TASK [installing apt-transport-https] **************************************
ok: [192.168.1.5]

TASK [adding repo] *********************************************************
ok: [192.168.1.5]

TASK [installing lynis] ****************************************************
ok: [192.168.1.5]

TASK [audit scan the system] ***********************************************
changed: [192.168.1.5]

TASK [downloading report locally] ******************************************
changed: [192.168.1.5]

TASK [report location] *****************************************************
ok: [192.168.1.5] => {
    "msg": "Report can be found at ./192.168.1.5-lynis-report-2017-11-13.log"
}

PLAY RECAP *****************************************************************
192.168.1.5                : ok=8    changed=2    unreachable=0    failed=0
```

```
$ cat ./192.168.1.5-lynis-report-2017-11-13.log

[ Lynis 2.5.7 ]

################################################################################
  Lynis comes with ABSOLUTELY NO WARRANTY. This is free software, and you are
  welcome to redistribute it under the terms of the GNU General Public License.
  See the LICENSE file for details about using this software.

  2007-2017, CISOfy - https://cisofy.com/lynis/
  Enterprise support available (compliance, plugins, interface and tools)
################################################################################


[+] Initializing program
------------------------------------
  - Detecting OS...                                           [ DONE ]
  - Checking profiles...                                      [ DONE ]

  ---------------------------------------------------
  Program version:           2.5.7
  Operating system:          Linux
  Operating system name:     Ubuntu Linux
  Operating system version:  16.04
  Kernel version:            4.4.0
  Hardware platform:         x86_64
  Hostname:                  ubuntu-xenial
  ---------------------------------------------------
  Profiles:                  /etc/lynis/default.prf
  Log file:                  /var/log/lynis.log
  Report file:               /var/log/lynis-report.dat
  Report version:            1.0
  Plugin directory:          /usr/share/lynis/plugins
  ---------------------------------------------------
  Auditor:                   [Not Specified]
  Language:                  en
  Test category:             all
  Test group:                all
  ---------------------------------------------------
  - Program update status...                                  [ NO UPDATE ]

[+] System Tools
------------------------------------
  - Scanning available tools...
  - Checking system binaries...
```

```
[+] Initializing program
------------------------------------


  Usage: lynis command [options]


  Command:

    audit
        audit system                  : Perform local security scan
        audit system remote <host>    : Remote security scan
        audit dockerfile <file>       : Analyze Dockerfile

    show
        show                          : Show all commands
        show version                  : Show Lynis version
        show help                     : Show help

    update
        update info                   : Show update details


  Options:

    --no-log                          : Don't create a log file
    --pentest                         : Non-privileged scan (useful for pentest)
    --profile <profile>               : Scan the system with the given profile file
    --quick (-Q)                      : Quick mode, don't wait for user input

    Layout options
    --no-colors                       : Don't use colors in output
    --quiet (-q)                      : No output
    --reverse-colors                  : Optimize color display for light backgrounds

    Misc options
    --debug                           : Debug logging to screen
    --view-manpage (--man)            : View man page
    --verbose                         : Show more details on screen
    --version (-V)                    : Display version number and quit

    Enterprise options
    --plugin-dir "<path>"             : Define path of available plugins
    --upload                          : Upload data to central node

    More options available. Run '/usr/sbin/lynis show options', or use the man page.
```

```
$ ansible-playbook -i inventory windows-security-updates.yml
[DEPRECATION WARNING]: [defaults]hostfile option, The key is misleading as it c
be removed in version 2.8. Deprecation warnings can be disabled by setting depr

PLAY [Windows Security Updates] ************************************************

TASK [Gathering Facts] *********************************************************
ok: [redacted]

TASK [install all critical and security updates] ********************************
changed: [redacted]

TASK [reboot host if required] *************************************************
changed: [redacted]

PLAY RECAP *********************************************************************
[redacted]                 : ok=3    changed=2    unreachable=0    failed=0
```

```
$ ansible-playbook -i inventory windows-security-audit.yml

PLAY [Windows Audit Playbook] ***************************************************

TASK [Gathering Facts] **********************************************************
ok: [redacted]

TASK [download audit script] ****************************************************
changed: [redacted]

TASK [running windows audit script] *********************************************
changed: [redacted]

PLAY RECAP **********************************************************************
[redacted]                 : ok=3    changed=2    unreachable=0    failed=0
```



ANSIBLEWINDOW Audit

Version 3 by Alan Renouf virtu-al.net
Report created on 11/17/2017 17:48:28

ANSIBLEWINDOW Details

General — hide

Computer Name	ANSIBLEWINDOW
Computer Role	Standalone Server
Computer Workgroup	WORKGROUP
Operating System	Microsoft Windows Server 2012 R2 Datacenter
Service Pack	
System Root	C:
Manufacturer	Google
Model	Google Compute Engine
Number of Processors	1
Memory	4026114048
Registered User	Windows User
Registered Organisation	
Last System Boot	11/17/2017 16:57:17

HotFixes — show

Logical Disk Configuration — show

NIC Configuration — show

Software — show

Local Shares — hide

Name	Path	Caption
ADMIN$	C:\Windows	Remote Admin
C$	C:\	Default share
IPC$		Remote IPC

Printers — hide

Name	Location
Microsoft XPS Document Writer	

Services — show

Regional Settings — show

Event Logs — hide

- Event Log Settings — show
- ERROR Entries — show
- WARNING Entries — show

```
$ ansible-playbook main.yml --ask-sudo-pass
[DEPRECATION WARNING]: The sudo command line option has been deprecated in favor
Deprecation warnings can be disabled by setting deprecation_warnings=False in an
SUDO password:
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available


PLAY [Basic NMAP Scan Playbook] ************************************************

TASK [check if nmap installed and install] *************************************
ok: [localhost]

TASK [top ports scan] **********************************************************
changed: [localhost]

PLAY RECAP *********************************************************************
localhost                  : ok=2    changed=1    unreachable=0    failed=0
```

```
$ ls -l
total 52
-rw-rw-r-- 1 madhuakula madhuakula  556 Nov 14 21:10 main.yml
-rw-rw-r-- 1 madhuakula madhuakula  472 Nov 14 21:10 nmap-scan-2017-11-14.gnmap
-rw-rw-r-- 1 madhuakula madhuakula  591 Nov 14 21:10 nmap-scan-2017-11-14.nmap
-rw-rw-r-- 1 madhuakula madhuakula 5992 Nov 14 21:10 nmap-scan-2017-11-14.xml
```

```
$ cat nmap-scan-2017-11-14.nmap
# Nmap 7.01 scan initiated Tue Nov 14 21:19:32 2017 as: nmap --top-ports 1000 -Pn -oA nmap-scan-%Y-%m-%d 192.168.1.1 scanme.nmap.org 127.0.0.1
Nmap scan report for 192.168.1.1
Host is up (0.013s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
53/tcp   open  domain
80/tcp   open  http

Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 986 closed ports
PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
554/tcp   filtered rtsp
1022/tcp  filtered exp2
1023/tcp  filtered netvenuechat
1026/tcp  filtered LSA-or-nterm
1720/tcp  filtered h323q931
1863/tcp  filtered msnp
5190/tcp  filtered aol
9898/tcp  filtered monkeycom
31337/tcp open     Elite

Nmap scan report for localhost (127.0.0.1)
Host is up (0.00011s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE
53/tcp  open  domain

# Nmap done at Tue Nov 14 21:20:05 2017 -- 3 IP addresses (3 hosts up) scanned in 32.50 seconds
```

```
$ ansible-playbook main.yml
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available


PLAY [Advanced NMAP Scan using NSE] ********************************************

TASK [Gathering Facts] *********************************************************
ok: [localhost]

TASK [Running Nmap NSE scan] ***************************************************
changed: [localhost] => (item=http-methods)
changed: [localhost] => (item=http-enum)

PLAY RECAP *********************************************************************
localhost                  : ok=2    changed=1    unreachable=0    failed=0
```

```
$ cat nmap-http-*.nmap
# Nmap 7.01 scan initiated Tue Nov 14 22:49:33 2017 as: nmap -Pn -p 80,443 --script http-enum -oA nmap-http-enum-results-%Y-%m-%d scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.23s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT    STATE  SERVICE
80/tcp  open   http
| http-enum:
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
|_  /shared/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'
443/tcp closed https

# Nmap done at Tue Nov 14 22:50:01 2017 -- 1 IP address (1 host up) scanned in 28.03 seconds
# Nmap 7.01 scan initiated Tue Nov 14 22:49:30 2017 as: nmap -Pn -p 80,443 --script http-methods -oA nmap-http-methods-results-%Y-%m-%d scanme.nmap.org
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.24s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
PORT    STATE  SERVICE
80/tcp  open   http
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
443/tcp closed https

# Nmap done at Tue Nov 14 22:49:33 2017 -- 1 IP address (1 host up) scanned in 2.28 seconds
```

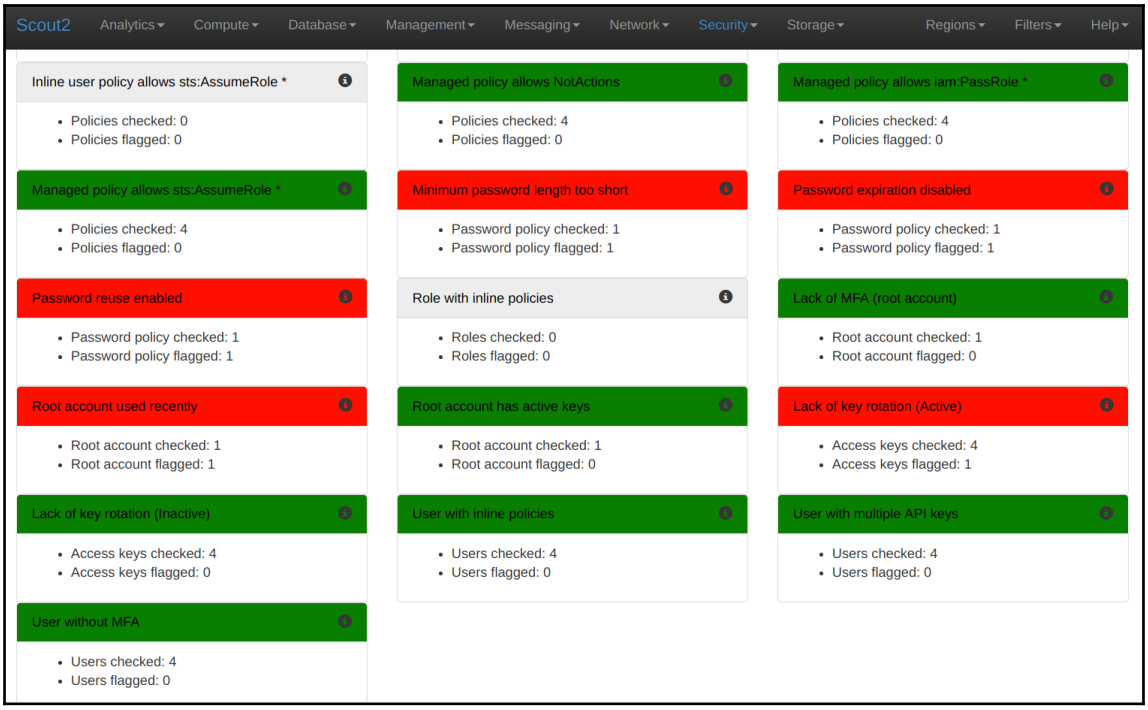
Scout2 Analytics Compute Database Management Messaging Network Security Storage Regions Filters Help

Account ID: [redacted]

Dashboard

Summary:

Service	# of Resources	# of Rules	# of Findings	# of Checks
Cloudformation	1	1	0	1
CloudTrail	0	5	15	16
CloudWatch	1	1	0	1
Directconnect	0	0	0	0
EC2	38	22	93	1258
EFS	0	0	0	0
Elasticache	0	0	0	0
Elb	0	1	0	0


Scout2
Analytics
Compute
Database
Management
Messaging
Network
Security
Storage
Regions
Filters
Help
Inline user policy allows sts:AssumeRole *
Policies checked: 0
Policies flagged: 0
Managed policy allows sts:AssumeRole *
Policies checked: 4
Policies flagged: 0
Password reuse enabled
Password policy checked: 1
Password policy flagged: 1
Root account used recently
Root account checked: 1
Root account flagged: 1
Lack of key rotation (Inactive)
Access keys checked: 4
Access keys flagged: 0
User without MFA
Users checked: 4
Users flagged: 0
Managed policy allows NotActions
Policies checked: 4
Policies flagged: 0
Minimum password length too short
Password policy checked: 1
Password policy flagged: 1
Role with inline policies
Roles checked: 0
Roles flagged: 0
Root account has active keys
Root account checked: 1
Root account flagged: 0
User with inline policies
Users checked: 4
Users flagged: 0
Managed policy allows iam:PassRole *
Policies checked: 4
Policies flagged: 0
Password expiration disabled
Password policy checked: 1
Password policy flagged: 1
Lack of MFA (root account)
Root account checked: 1
Root account flagged: 0
Lack of key rotation (Active)
Access keys checked: 4
Access keys flagged: 1
User with multiple API keys
Users checked: 4
Users flagged: 0

```
$ ansible-playbook -i inventory main.yml --ask-pass
SSH password:

PLAY [Brakeman Scanning Playbook] ***********************************************

TASK [installing ruby and git] **************************************************
ok: [192.168.1.5] => (item=[u'ruby-full', u'git'])

TASK [installing brakeman gem] **************************************************
ok: [192.168.1.5]

TASK [cloning the https://github.com/OWASP/railsgoat.git] ***********************
changed: [192.168.1.5]

TASK [Brakeman scanning in action] **********************************************
changed: [192.168.1.5]

TASK [Downloading the report] ***************************************************
changed: [192.168.1.5]

TASK [debug] ********************************************************************
ok: [192.168.1.5] => {
    "msg": "Report can be found at ./report.html"
}

PLAY RECAP **********************************************************************
192.168.1.5                : ok=6    changed=3    unreachable=0    failed=0
```

Brakeman Report

Application Path	Rails Version	Brakeman Version	Report Time	Checks Performed
/tmp/railsgoat	5.1.4	4.0.1	2017-11-15 17:48:12 +0000 0.596077956 seconds	BasicAuth, BasicAuthTimingAttack, ContentTag, CreateWith, CrossSiteScripting, DefaultRoutes, Deserialize, DetailedExceptions, DigestDoS, DynamicFinders, EscapeFunction, Evaluation, Execute, FileAccess, FileDisclosure, FilterSkipping, ForgerySetting, HeaderDoS, I18nXSS, JRubyXML, JSONEncoding, JSONParsing, LinkTo, LinkToHref, MailTo, MassAssignment, MimeTypeDoS, ModelAttrAccessible, ModelAttributes, ModelSerialize, NestedAttributes, NestedAttributesBypass, NumberToCurrency, QuoteTableName, Redirect, RegexDoS, Render, RenderDoS, RenderInline, ResponseSplitting, RouteDoS, SQL, SQLCVEs, SSLVerify, SafeBufferManipulation, SanitizeMethods, SelectTag, SelectVulnerability, Send, SendFile, SessionManipulation, SessionSettings, SimpleFormat, SingleQuotes, SkipBeforeFilter, StripTags, SymbolDoSCVE, TranslateBug, UnsafeReflection, ValidationRegex, WithoutProtection, XMLDoS, YAMLParsing

Summary

Scanned/Reported	Total
Controllers	17
Errors	0
Ignored Warnings	0
Models	12
Security Warnings	16 (12)
Templates	27

Warning Type	Total
Command Injection	1
Cross-Site Request Forgery	1
Cross-Site Scripting	1
Dangerous Send	1
File Access	1
Format Validation	1
Mass Assignment	1
Remote Code Execution	4
Session Setting	3
SQL Injection	2

Security Warnings

Confidence	Class	Method	Warning Type	Message
High	DashboardController	change_graph	Dangerous Send	User controlled method execution near line 14: self.try(params[:graph])
High	BenefitFormsController	download	File Access	Parameter value used in file name near line 11: send_file(params[:type].constantize.new(params[:name]...
High	Api::V1::MobileController	show	Remote Code Execution	Unsafe reflection method constantize called with parameter value near line 9: params[:class].classify.constantize app/controllers/api/v1/mobile_controller.rb 5 respond_to :json 7 def show 8 if params[:class] 9 model = params[:class].classify.constantize 10 respond_with model.find(params[:id]).to_json 11 end 12 end 14 def index
High	Api::V1::MobileController	index	Remote Code Execution	Unsafe reflection method constantize called with parameter value near line 16: params[:class].classif...
High	BenefitFormsController	download	Remote Code Execution	Unsafe reflection method constantize called with parameter value near line 10: params[:type].constant...
High			Session Setting	Session cookies should be set to HTTP only near line 3
High			Session Setting	Session secret should not be included in version control near line 7
High			Session Setting	Session secret should not be included in version control near line 8
High	UsersController	update	SQL Injection	Possible SQL injection near line 28: User.where("user_id = '#{params[:user][:user_id]}'")
Medium	Benefits	Benefits.make_backup	Command Injection	Possible command injection near line 14: system("cp #{full_file_name} #{data_path}/bak#{Time.zone.now...
Medium	UsersController	user_params	Mass Assignment	Parameters should be whitelisted for mass assignment near line 50: params.require(:user).permit!
Medium	Analytics	hits_by_ip	SQL Injection	Possible SQL injection near line 2: select("#{col}")
Medium	PasswordResetsController	reset_password	Remote Code Execution	Marshal.load called with parameter value near line 5: Marshal.load(Base64.decode64(params[:user]))

```
$ ansible-playbook -i inventory main.yml

PLAY [OWASP Dependency Check Playbook] *****************************************************************

TASK [Gathering Facts] *********************************************************************************
ok: [192.168.1.10]

TASK [installing pre requisuites] **********************************************************************
ok: [192.168.1.10] => (item=[u'git', u'unzip', u'mono-runtime', u'mono-devel', u'default-jre'])

TASK [downloading owasp dependency-check] **************************************************************
changed: [192.168.1.10]

TASK [adding symlink to the system] ********************************************************************
changed: [192.168.1.10]

TASK [cloning the https://github.com/psiinon/bodgeit.git] **********************************************
changed: [192.168.1.10]

TASK [updating CVE database] ***************************************************************************
changed: [192.168.1.10]

TASK [OWASP dependency-check scanning in action] *******************************************************
changed: [192.168.1.10]

TASK [Downloading the report] **************************************************************************
changed: [192.168.1.10]

TASK [debug] *******************************************************************************************
ok: [192.168.1.10] => {
    "msg": "Report can be found at ./report.html"
}

PLAY RECAP *********************************************************************************************
192.168.1.10               : ok=9    changed=6    unreachable=0    failed=0
```

DEPENDENCY-CHECK

How to read the report | Suppressing false positives | **Getting Help:** google group | github issues

Project: bodgeit

Scan Information (show all):

- *dependency-check version*: 3.0.2
- *Report Generated On*: Nov 16, 2017 at 19:46:09 +00:00
- *Dependencies Scanned*: 52 (49 unique)
- *Vulnerable Dependencies*: 19
- *Vulnerabilities Found*: 108
- *Vulnerabilities Suppressed*: 0
- ...

Display: Showing Vulnerable Dependencies (click to show all)

Dependency	CPE	GAV	Highest Severity	CVE Count	CPE Confidence	Evidence Count
servlet-api.jar	cpe:/a:apache_tomcat:apache_tomcat:6.0.13 cpe:/a:apache:tomcat:6.0.13 cpe:/a:apache_software_foundation:tomcat:6.0.13	org.apache.tomcat:servlet-api:6.0.13 ✓	High	75	Highest	15
selenium-server-standalone-2.43.0.jar/META-INF/maven/org.apache.httpcomponents/httpclient/pom.xml	cpe:/a:apache:httpclient:4.3.4	org.apache.httpcomponents:httpclient:4.3.4	Medium	2	Highest	15
selenium-server-standalone-2.43.0.jar/META-INF/maven/org.apache.httpcomponents/httpmime/pom.xml	cpe:/a:apache:httpclient:4.3.4	org.apache.httpcomponents:httpmime:4.3.4	Medium	2	Highest	15
selenium-server-standalone-2.43.0.jar/META-INF/maven/commons-collections/commons-collections/pom.xml	cpe:/a:apache:commons_collections:3.2.1	commons-collections:commons-collections:3.2.1	High	1	Highest	16
selenium-server-standalone-2.43.0.jar/META-INF/maven/com.google.protobuf/protobuf-java/pom.xml	cpe:/a:google:protobuf:2.4.1	com.google.protobuf:protobuf-java:2.4.1	Medium	1	Low	16

selenium-server-standalone-2.43.0.jar/META-INF/maven/commons-collections/commons-collections/pom.xml

Description: Types that extend and augment the Java Collections Framework.

File Path: /tmp/bodgeit/lib/selenium-server-standalone-2.43.0.jar/META-INF/maven/commons-collections/commons-collections/pom.xml
MD5: 602190bb9bd6a1ff3c9b47b58e4ce76a
SHA1: c812635cfb96cd2431ee315e73418eed86aeb5e4

Evidence

Identifiers

- **cpe:** cpe:/a:apache:commons_collections:3.2.1 *Confidence*:Highest suppress
- **maven:** commons-collections:commons-collections:3.2.1 *Confidence*:High

Published Vulnerabilities

CVE-2015-6420 suppress

Severity: High
CVSS Score: 7.5 (AV:N/AC:L/Au:N/C:P/I:P/A:P)

Serialized-object interfaces in certain Cisco Collaboration and Social Media; Endpoint Clients and Client Software; Network Application, Service, and Acceleration; Network and Content Security Devices; Network Management and Provisioning; Routing and Switching - Enterprise and Service Provider; Unified Computing; Voice and Unified Communications Devices; Video, Streaming, TelePresence, and Transcoding Devices; Wireless; and Cisco Hosted Services products allow remote attackers to execute arbitrary commands via a crafted serialized Java object, related to the Apache Commons Collections (ACC) library.

- BID - 78872
- CISCO - 20151209 Vulnerability in Java Deserialization Affecting Cisco Products
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05376917
- CONFIRM - https://h20566.www2.hpe.com/portal/site/hpsc/public/kb/docDisplay?docId=emr_na-c05390722
- MISC - https://www.tenable.com/security/research/tra-2017-14
- MISC - https://www.tenable.com/security/research/tra-2017-23

Vulnerable Software & Versions: (show all)

- cpe:/a:apache:commons_collections:3.2.1 and all previous versions
- ...

```
$ ansible-playbook -i inventory main.yml

PLAY [Nikto Playbook] *********************************************************************************************************************************************

TASK [Gathering Facts] ********************************************************************************************************************************************
ok: [192.168.1.10]

TASK [installing pre requisuites] *********************************************************************************************************************************
ok: [192.168.1.10] => (item=[u'git', u'perl', u'libnet-ssleay-perl', u'openssl', u'libauthen-pam-perl', u'libio-pty-perl', u'libmd-dev'])

TASK [downloading nikto] ******************************************************************************************************************************************
ok: [192.168.1.10]

TASK [Nikto scanning in action] ***********************************************************************************************************************************
changed: [192.168.1.10]

TASK [downloading the report] *************************************************************************************************************************************
changed: [192.168.1.10]

TASK [debug] ******************************************************************************************************************************************************
ok: [192.168.1.10] => {
    "msg": "Report can be found at ./report.html"
}

PLAY RECAP ********************************************************************************************************************************************************
192.168.1.10               : ok=6    changed=2    unreachable=0    failed=0
```

idontexistdomainnamewebsite.com / idontexistdomainnamewebsite.com port 80	
Target IP	idontexistdomainnamewebsite.com
Target hostname	idontexistdomainnamewebsite.com
Target Port	80
HTTP Server	Apache/2.4.7 (Ubuntu)
Site Link (Name)	http://idontexistdomainnamewebsite.com:80/
Site Link (IP)	http://idontexistdomainnamewebsite.com:80/

URI	/
HTTP Method	GET
Description	Retrieved x-powered-by header: PHP/5.5.9-1ubuntu4.20
Test Links	http://idontexistdomainnamewebsite.com:80/ http://idontexistdomainnamewebsite.com:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The anti-clickjacking X-Frame-Options header is not present.
Test Links	http://idontexistdomainnamewebsite.com:80/ http://idontexistdomainnamewebsite.com:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
Test Links	http://idontexistdomainnamewebsite.com:80/ http://idontexistdomainnamewebsite.com:80/
OSVDB Entries	OSVDB-0
URI	/
HTTP Method	GET
Description	The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a different fashion to the MIME type
Test Links	http://idontexistdomainnamewebsite.com:80/ http://idontexistdomainnamewebsite.com:80/
OSVDB Entries	OSVDB-0

```
$ ansible-playbook main.yml
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available


PLAY [WPScan Playbook] *********************************************************************

TASK [Gathering Facts] *********************************************************************
ok: [localhost]

TASK [Downloading wpscanteam/wpscan docker container] **************************************
ok: [localhost]

TASK [creating output report file] **********************************************************
changed: [localhost]

TASK [Scanning www.idontexistdomainnamewebsite.com website using WPScan] *******************
changed: [localhost]

TASK [WPScan report downloaded] ************************************************************
ok: [localhost] => {
    "msg": "The report can be found at /tmp/www.idontexistdomainnamewebsite.com.txt"
}

PLAY RECAP *********************************************************************************
localhost                  : ok=5    changed=2    unreachable=0    failed=0
```

```
$ cat /tmp/www.idontexistdomainnamewebsite.com.txt
_______________________________________________________________
        __          _______   _____
        \ \        / /  __ \ / ____|
         \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
          \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
           \  /\  /  | |     ____) | (__| (_| | | | |
            \/  \/   |_|    |_____/ \___|\__,_|_| |_|

       WordPress Security Scanner by the WPScan Team
                      Version 2.9.4-dev
          Sponsored by Sucuri - https://sucuri.net
      @_WPScan_, @ethicalhack3r, @erwan_lr, @_FireFart_
_______________________________________________________________

[i] Updating the Database ...
[i] Update completed.
Following redirection https://www.idontexistdomainnamewebsite.com/
[+] URL: https://www.idontexistdomainnamewebsite.com/
[+] Started: Wed Nov 15 16:20:25 2017

[+] robots.txt available under: 'https://www.idontexistdomainnamewebsite.com/robots.txt'
[+] Interesting entry from robots.txt: https://www.idontexistdomainnamewebsite.com/out/
[+] Interesting entry from robots.txt: https://www.idontexistdomainnamewebsite.com/wp/out/
[+] Interesting header: LINK: <https://www.idontexistdomainnamewebsite.com/wp-json/>; rel="https://api.w.org/"
[+] Interesting header: LINK: <https://www.idontexistdomainnamewebsite.com/>; rel=shortlink
[+] Interesting header: SERVER: nginx
[+] Interesting header: X-CONTENT-TYPE-OPTIONS: nosniff
[+] Interesting header: X-POWERED-BY: PHP/7.1.11

[+] WordPress version 4.8.3 (Released on 2017-10-31) identified from links opml
[!] 1 vulnerability identified from the version number

[!] Title: WordPress 2.3-4.8.3 - Host Header Injection in Password Reset
    Reference: https://wpvulndb.com/vulnerabilities/8807
    Reference: https://exploitbox.io/vuln/WordPress-Exploit-4-7-Unauth-Password-Reset-0day-CVE-2017-8295.html
    Reference: http://blog.dewhurstsecurity.com/2017/05/04/exploitbox-wordpress-security-advisories.html
    Reference: https://core.trac.wordpress.org/ticket/25239
    Reference: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-8295
```

```
$ ansible-playbook -i inventory main.yml

PLAY [running common role] *****************************************************************************

TASK [common : installing python if not installed] *****************************************************
changed: [blueserver]
changed: [greenserver]
changed: [proxy]

TASK [common : updating and installing git, curl] ******************************************************
ok: [greenserver] => (item=[u'git', u'curl'])
ok: [blueserver] => (item=[u'git', u'curl'])
ok: [proxy] => (item=[u'git', u'curl'])

PLAY [running haproxy role] ****************************************************************************

TASK [Gathering Facts] *********************************************************************************
ok: [proxy]

TASK [haproxy : adding haproxy repo] *******************************************************************
ok: [proxy]

TASK [haproxy : updating and installing haproxy] *******************************************************
ok: [proxy]

TASK [haproxy : updating the haproxy configuration] ****************************************************
ok: [proxy]

TASK [haproxy : starting the haproxy service] **********************************************************
ok: [proxy]

PLAY [running webserver role] **************************************************************************

TASK [Gathering Facts] *********************************************************************************
ok: [blueserver]
ok: [greenserver]

TASK [nginx : installing nginx] ************************************************************************
ok: [greenserver]
ok: [blueserver]

TASK [nginx : starting the nginx service] **************************************************************
ok: [blueserver]
ok: [greenserver]
```

```
$ ansible-playbook -i inventory main.yml

PLAY [Updating to GREEN deployment] ********************************************

TASK [Gathering Facts] *********************************************************
ok: [proxy]

TASK [updating proxy configuration] ********************************************
changed: [proxy]

TASK [updating the service] ****************************************************
changed: [proxy]

TASK [debug] *******************************************************************
ok: [proxy] => {
    "msg": "GREEN deployment successful. Please check your server :)"
}

PLAY RECAP *********************************************************************
proxy                      : ok=4    changed=2    unreachable=0    failed=0
```

Chapter 08: Continuous Security Scanning for Docker Containers

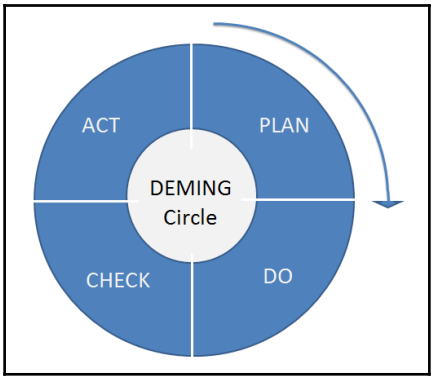
```
$ ansible-playbook -i inventory main.yml --ask-pass
SSH password:

PLAY [Docker bench security playbook] ******************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.1.9]

TASK [make sure git installed] *************************************************
ok: [192.168.1.9]

TASK [download the docker bench security] **************************************
ok: [192.168.1.9]

TASK [running docker-bench-security scan] **************************************
changed: [192.168.1.9]

TASK [downloading report locally] **********************************************
changed: [192.168.1.9]

TASK [report location] *********************************************************
ok: [192.168.1.9] => {
    "msg": "Report can be found at ./192.168.1.9-docker-report-2017-11-09.log"
}

PLAY RECAP *********************************************************************
192.168.1.9                : ok=6    changed=2    unreachable=0    failed=0
```

```
$ cat ./192.168.1.9-docker-report-2017-11-09.log
Initializing Thu Nov  9 20:31:12 UTC 2017


[INFO] 1 - Host Configuration
[WARN] 1.1  - Ensure a separate partition for containers has been created
[NOTE] 1.2  - Ensure the container host has been Hardened
[INFO] 1.3  - Ensure Docker is up to date
[INFO]      * Using 17.09.0, verify is it up to date as deemed necessary
[INFO]      * Your operating system vendor may provide support and security maintenance for Docker
[INFO] 1.4  - Ensure only trusted users are allowed to control Docker daemon
[INFO]      * docker:x:999:
[WARN] 1.5  - Ensure auditing is configured for the Docker daemon
[WARN] 1.6  - Ensure auditing is configured for Docker files and directories - /var/lib/docker
[WARN] 1.7  - Ensure auditing is configured for Docker files and directories - /etc/docker
[INFO] 1.8  - Ensure auditing is configured for Docker files and directories - docker.service
[INFO]      * File not found
[INFO] 1.9  - Ensure auditing is configured for Docker files and directories - docker.socket
[INFO]      * File not found
[WARN] 1.10 - Ensure auditing is configured for Docker files and directories - /etc/default/docker
[INFO] 1.11 - Ensure auditing is configured for Docker files and directories - /etc/docker/daemon.json
[INFO]      * File not found
[WARN] 1.12 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-containerd
[WARN] 1.13 - Ensure auditing is configured for Docker files and directories - /usr/bin/docker-runc


[INFO] 2 - Docker daemon configuration
[WARN] 2.1  - Ensure network traffic is restricted between containers on the default bridge
[PASS] 2.2  - Ensure the logging level is set to 'info'
[PASS] 2.3  - Ensure Docker is allowed to make changes to iptables
[PASS] 2.4  - Ensure insecure registries are not used
[WARN] 2.5  - Ensure aufs storage driver is not used
[INFO] 2.6  - Ensure TLS authentication for Docker daemon is configured
[INFO]      * Docker daemon not listening on TCP
[INFO] 2.7  - Ensure the default ulimit is configured appropriately
[INFO]      * Default ulimit doesn't appear to be set
[WARN] 2.8  - Enable user namespace support
[PASS] 2.9  - Ensure the default cgroup usage has been confirmed
[PASS] 2.10 - Ensure base device size is not changed until needed
[WARN] 2.11 - Ensure that authorization for Docker client commands is enabled
[WARN] 2.12 - Ensure centralized and remote logging is configured
[WARN] 2.13 - Ensure operations on legacy registry (v1) are Disabled
[WARN] 2.14 - Ensure live restore is Enabled
[WARN] 2.15 - Ensure Userland Proxy is Disabled
[INFO] 2.16 - Ensure daemon-wide custom seccomp profile is applied, if needed
[PASS] 2.17 - Ensure experimental features are avoided in production
[PASS] 2.18 - Ensure containers are restricted from acquiring new privileges
```

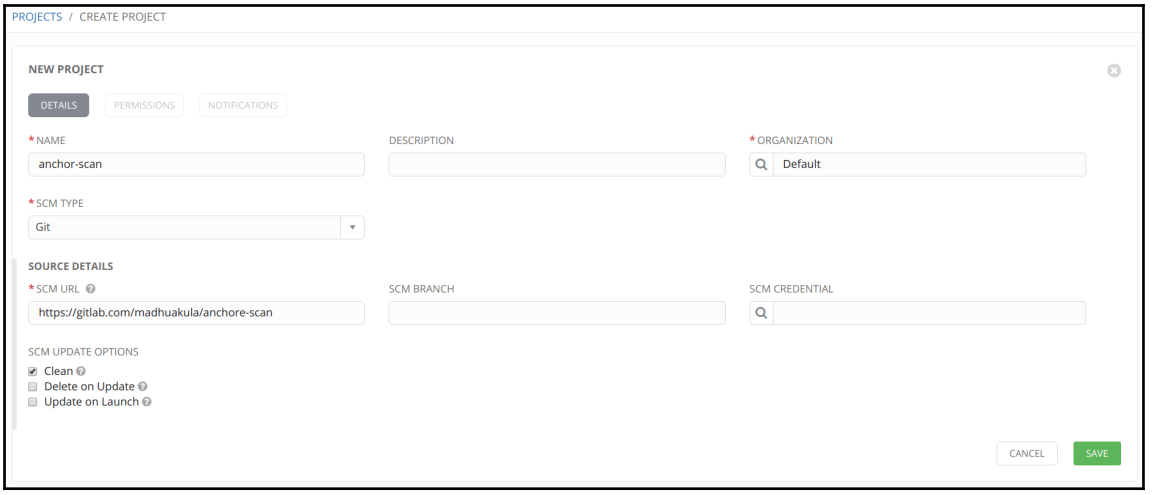
```
$ ansible-playbook -i inventory main.yaml

PLAY [Clair Scanner Server Setup] **********************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.1.10]

TASK [setting up clair-db] *****************************************************
changed: [192.168.1.10]

TASK [setting up clair-local-scan] *********************************************
changed: [192.168.1.10]

PLAY RECAP *********************************************************************
192.168.1.10               : ok=3    changed=2    unreachable=0    failed=0

$
```

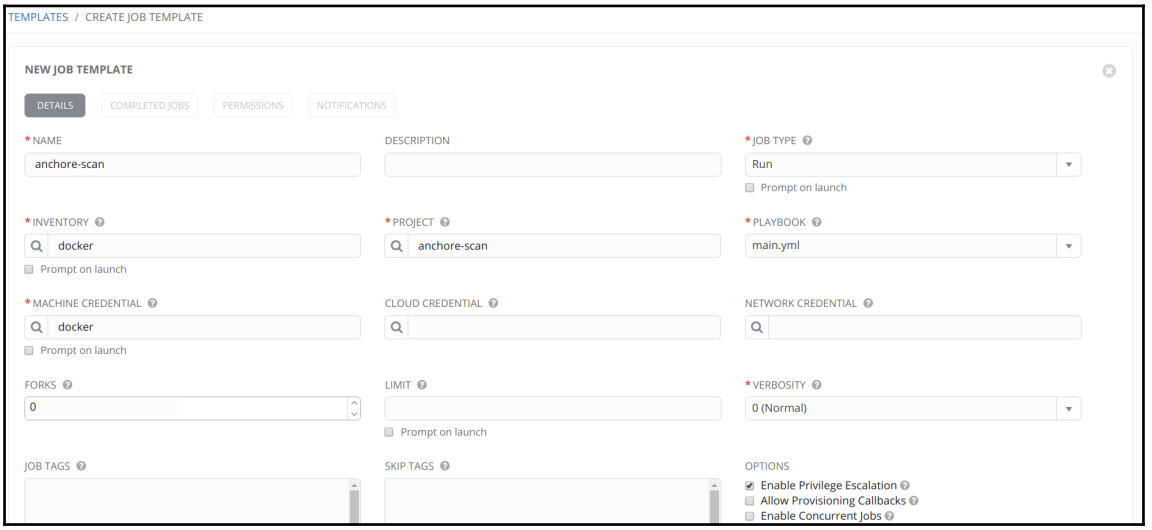
```
$ ansible-playbook -i inventory main.yaml

PLAY [Scanning containers using clair-scanner] *********************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.1.10]

TASK [downloading and setting up clair-scanner binary] *************************
ok: [192.168.1.10]

TASK [scanning debian:sid container for vulnerabilities] ***********************
fatal: [192.168.1.10]: FAILED! => {"changed": true, "cmd": ["clair-scanner", "
bian:sid"], "delta": "0:00:02.100922", "end": "2017-11-20 19:32:17.243730", "f
derr": "2017/11/20 19:32:15 \u001b[0;32m[INFO] ▶ Start clair-scanner\u001b[0m\
32:17 \u001b[0;32m[INFO] ▶ Analyzing cc1a9442a61f5792fb7d3fbccbe210cbbbc577383
ities [[CVE-2012-3878 CVE-2011-4116 CVE-2016-2781 CVE-2011-3374 CVE-2010-4756
0-4051 CVE-2017-8804 CVE-2010-4052 CVE-2016-2779 CVE-2013-4235 CVE-2007-5686 C
7245 CVE-2017-16231 CVE-2017-11164]]\u001b[0m", "stderr_lines": ["2017/11/20 1
F0] ▶ Server listening on port 9279\u001b[0m", "2017/11/20 19:32:17 \u001b[0;3
 "2017/11/20 19:32:17 \u001b[0;32m[INFO] ▶ Unapproved vulnerabilities [[CVE-20
-2017-12132 CVE-2017-15804 CVE-2017-15670 CVE-2016-10228 CVE-2010-4051 CVE-201
017-1000082 CVE-2017-15908 CVE-2005-2541 CVE-2017-7246 CVE-2017-7245 CVE-2017-
...ignoring

TASK [downloading the report locally] ******************************************
changed: [192.168.1.10]

PLAY RECAP *********************************************************************
192.168.1.10               : ok=4    changed=2    unreachable=0    failed=0
```

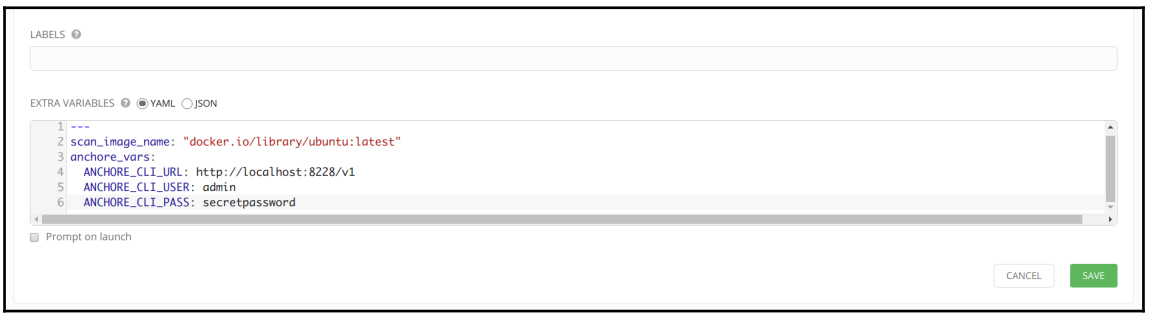
```
$ cat debian\:sid-scan-report.json
{
    "image": "debian:sid",
    "unaproved": [
        "CVE-2011-3374",
        "CVE-2007-5686",
        "CVE-2017-12424",
        "CVE-2013-4235",
        "CVE-2013-4392",
        "CVE-2017-1000082",
        "CVE-2017-7245",
        "CVE-2017-7246",
        "CVE-2017-11164",
        "CVE-2010-4052",
        "CVE-2010-4051",
        "CVE-2015-8985",
        "CVE-2017-12132",
        "CVE-2010-4756",
        "CVE-2016-10228",
        "CVE-2017-8804",
        "CVE-2016-2779",
        "CVE-2012-3878",
        "CVE-2011-4116",
        "CVE-2016-2781",
        "CVE-2011-3389",
        "CVE-2005-2541"
    ],
    "vulnerabilities": [
        {
            "vulnerability": "CVE-2011-3374",
            "namespace": "debian:unstable",
            "severity": "Negligible"
        },
        {
            "vulnerability": "CVE-2007-5686",
            "namespace": "debian:unstable",
            "severity": "Negligible"
        },
        {
            "vulnerability": "CVE-2017-12424",
            "namespace": "debian:unstable",
            "severity": "High"
        },
        {
            "vulnerability": "CVE-2013-4235",
            "namespace": "debian:unstable",
            "severity": "Negligible"
        },
```

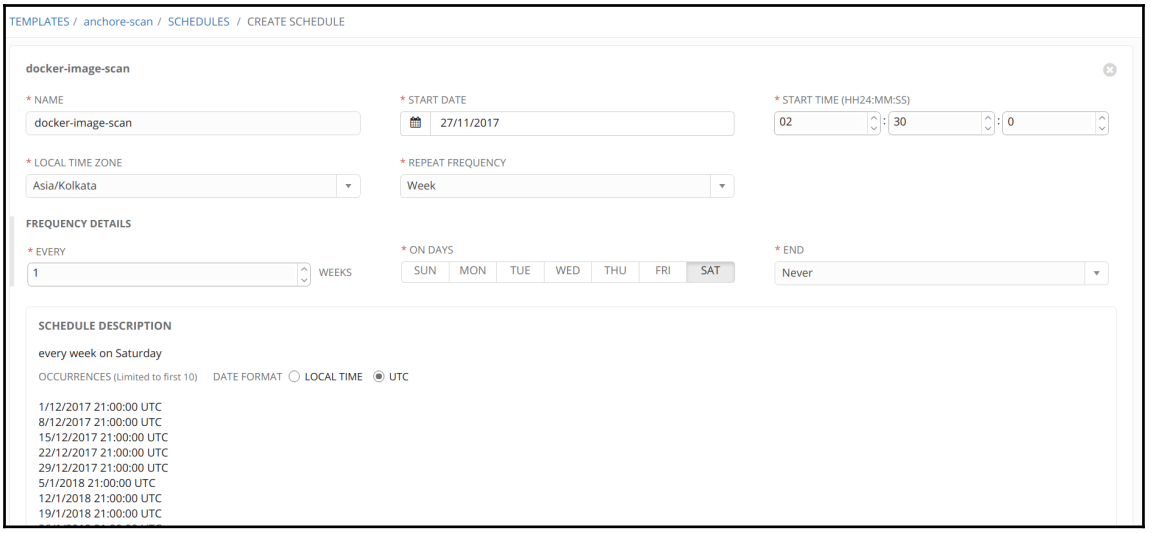


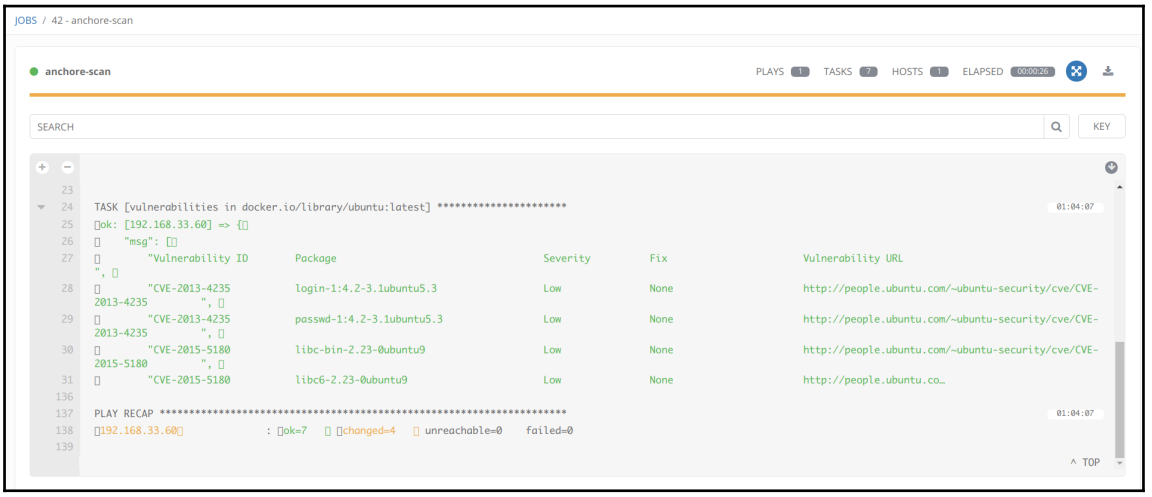

```
$ ansible-playbook -i inventory main.yml

PLAY [anchore server setup] ****************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.33.60]

TASK [creating volumes] ********************************************************
changed: [192.168.33.60] => (item=/root/aevolume/db)
changed: [192.168.33.60] => (item=/root/aevolume/config)

TASK [copying anchore-engine configuration] ************************************
changed: [192.168.33.60]

TASK [starting anchore-db container] *******************************************
changed: [192.168.33.60]

TASK [starting anchore-engine container] ***************************************
changed: [192.168.33.60]

PLAY RECAP *********************************************************************
192.168.33.60              : ok=5    changed=4    unreachable=0    failed=0
```


PROJECTS / CREATE PROJECT
NEW PROJECT
DETAILS
PERMISSIONS
NOTIFICATIONS
* NAME
anchor-scan
DESCRIPTION
* ORGANIZATION
Default
* SCM TYPE
Git
SOURCE DETAILS
* SCM URL
https://gitlab.com/madhuakula/anchore-scan
SCM BRANCH
SCM CREDENTIAL
SCM UPDATE OPTIONS
Clean
Delete on Update
Update on Launch
CANCEL
SAVE


TEMPLATES / CREATE JOB TEMPLATE
NEW JOB TEMPLATE
DETAILS
COMPLETED JOBS
PERMISSIONS
NOTIFICATIONS
* NAME
anchore-scan
DESCRIPTION
* JOB TYPE
Run
Prompt on launch
* INVENTORY
docker
Prompt on launch
* PROJECT
anchore-scan
* PLAYBOOK
main.yml
* MACHINE CREDENTIAL
docker
Prompt on launch
CLOUD CREDENTIAL
NETWORK CREDENTIAL
FORKS
0
LIMIT
Prompt on launch
* VERBOSITY
0 (Normal)
JOB TAGS
SKIP TAGS
OPTIONS
Enable Privilege Escalation
Allow Provisioning Callbacks
Enable Concurrent Jobs


LABELS
EXTRA VARIABLES
YAML
JSON
---
scan_image_name: "docker.io/library/ubuntu:latest"
anchore_vars:
ANCHORE_CLI_URL: http://localhost:8228/v1
ANCHORE_CLI_USER: admin
ANCHORE_CLI_PASS: secretpassword
Prompt on launch
CANCEL
SAVE


TEMPLATES / anchore-scan / SCHEDULES / CREATE SCHEDULE
docker-image-scan
* NAME
docker-image-scan
* START DATE
27/11/2017
* START TIME (HH24:MM:SS)
02
30
0
* LOCAL TIME ZONE
Asia/Kolkata
* REPEAT FREQUENCY
Week
FREQUENCY DETAILS
* EVERY
1
WEEKS
* ON DAYS
SUN
MON
TUE
WED
THU
FRI
SAT
* END
Never
SCHEDULE DESCRIPTION
every week on Saturday
OCCURRENCES (Limited to first 10)
DATE FORMAT
LOCAL TIME
UTC
1/12/2017 21:00:00 UTC
8/12/2017 21:00:00 UTC
15/12/2017 21:00:00 UTC
22/12/2017 21:00:00 UTC
29/12/2017 21:00:00 UTC
5/1/2018 21:00:00 UTC
12/1/2018 21:00:00 UTC
19/1/2018 21:00:00 UTC


JOBS / 42 - anchore-scan
anchore-scan
PLAYS 1
TASKS 7
HOSTS 1
ELAPSED 00:00:26
SEARCH
KEY
TASK [vulnerabilities in docker.io/library/ubuntu:latest] **********
01:04:07
ok: [192.168.33.60] => {
"msg": [
"Vulnerability ID Package Severity Fix Vulnerability URL",
"CVE-2013-4235 login-1:4.2-3.1ubuntu5.3 Low None http://people.ubuntu.com/~ubuntu-security/cve/CVE-2013-4235",
"CVE-2013-4235 passwd-1:4.2-3.1ubuntu5.3 Low None http://people.ubuntu.com/~ubuntu-security/cve/CVE-2013-4235",
"CVE-2015-5180 libc-bin-2.23-0ubuntu9 Low None http://people.ubuntu.com/~ubuntu-security/cve/CVE-2015-5180",
"CVE-2015-5180 libc6-2.23-0ubuntu9 Low None http://people.ubuntu.co…
PLAY RECAP **********
01:04:07
192.168.33.60 : ok=7 changed=4 unreachable=0 failed=0
^ TOP

```
$ ansible-playbook -i inventory main.yml

PLAY [setting up vuls using docker containers] ****************************

TASK [Gathering Facts] ****************************************************
ok: [192.168.33.60]

TASK [vuls_containers_download : pulling containers locally] **************
ok: [192.168.33.60] => (item=vuls/go-cve-dictionary)
ok: [192.168.33.60] => (item=vuls/goval-dictionary)
ok: [192.168.33.60] => (item=vuls/vuls)

TASK [vuls_database_download : fetching NVD database locally] *************
changed: [192.168.33.60] => (item=2002)
changed: [192.168.33.60] => (item=2003)
changed: [192.168.33.60] => (item=2004)
changed: [192.168.33.60] => (item=2005)
changed: [192.168.33.60] => (item=2006)
changed: [192.168.33.60] => (item=2007)
changed: [192.168.33.60] => (item=2008)
changed: [192.168.33.60] => (item=2009)
changed: [192.168.33.60] => (item=2010)
changed: [192.168.33.60] => (item=2011)
changed: [192.168.33.60] => (item=2012)
changed: [192.168.33.60] => (item=2013)
changed: [192.168.33.60] => (item=2014)
changed: [192.168.33.60] => (item=2015)
changed: [192.168.33.60] => (item=2016)
changed: [192.168.33.60] => (item=2017)

TASK [vuls_database_download : fetching redhat oval data] *****************
changed: [192.168.33.60] => (item=6)
changed: [192.168.33.60] => (item=7)

TASK [vuls_database_download : fetching ubuntu oval data] *****************
changed: [192.168.33.60] => (item=12)
changed: [192.168.33.60] => (item=14)
changed: [192.168.33.60] => (item=16)

PLAY RECAP ****************************************************************
192.168.33.60              : ok=5    changed=3    unreachable=0    failed=0
```

```
$ ansible-playbook -i inventory main.yml

PLAY [scanning and reporting using vuls] ***************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.33.60]

TASK [copying configuraiton file and ssh keys] *********************************
ok: [192.168.33.60] => (item={u'src': u'config.toml', u'dst': u'/root/config.toml'})
ok: [192.168.33.60] => (item={u'src': u'192-168-33-80', u'dst': u'/root/.ssh/192-168-33-80'})

TASK [running config test] *****************************************************
changed: [192.168.33.60]

TASK [running vuls scanner] ****************************************************
changed: [192.168.33.60]

TASK [sending slack report] *****************************************************
changed: [192.168.33.60]

TASK [vuls webui report] ********************************************************
changed: [192.168.33.60]

PLAY RECAP *********************************************************************
192.168.33.60              : ok=6    changed=4    unreachable=0    failed=0
```

192-168-33-80 (ubuntu14.04)

Total: 10 (High:10 Medium:0 Low:0 ?:0)

CVE-2017-1000111
8.9 (HIGH)

Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the

Show more...

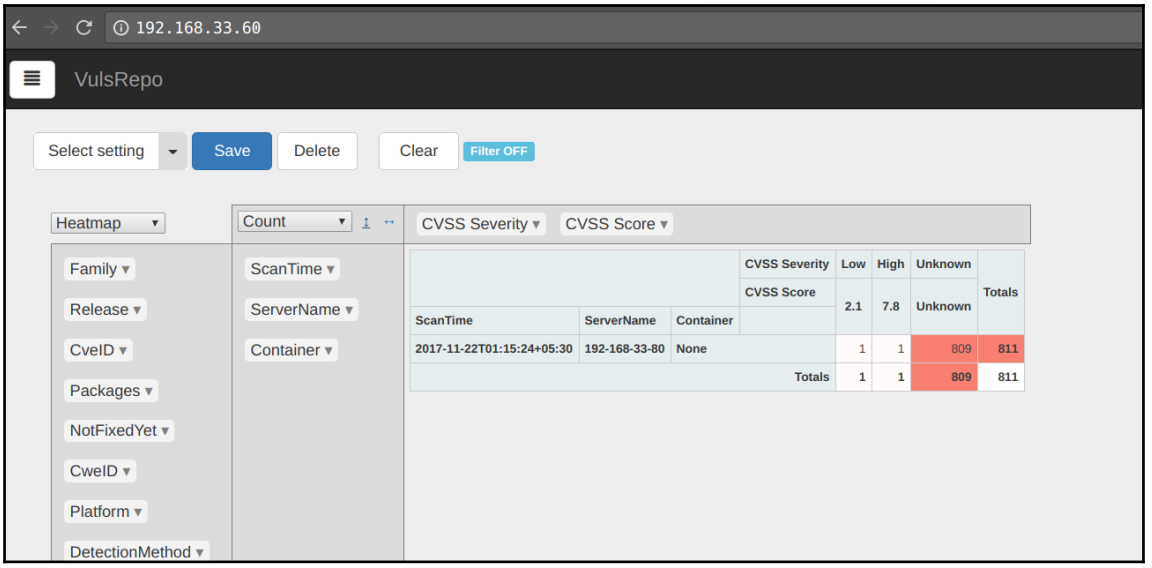
Installed	Candidate
linux-image-3.13.0-125-generic-3.13.0-125.174	Not Fixed Yet

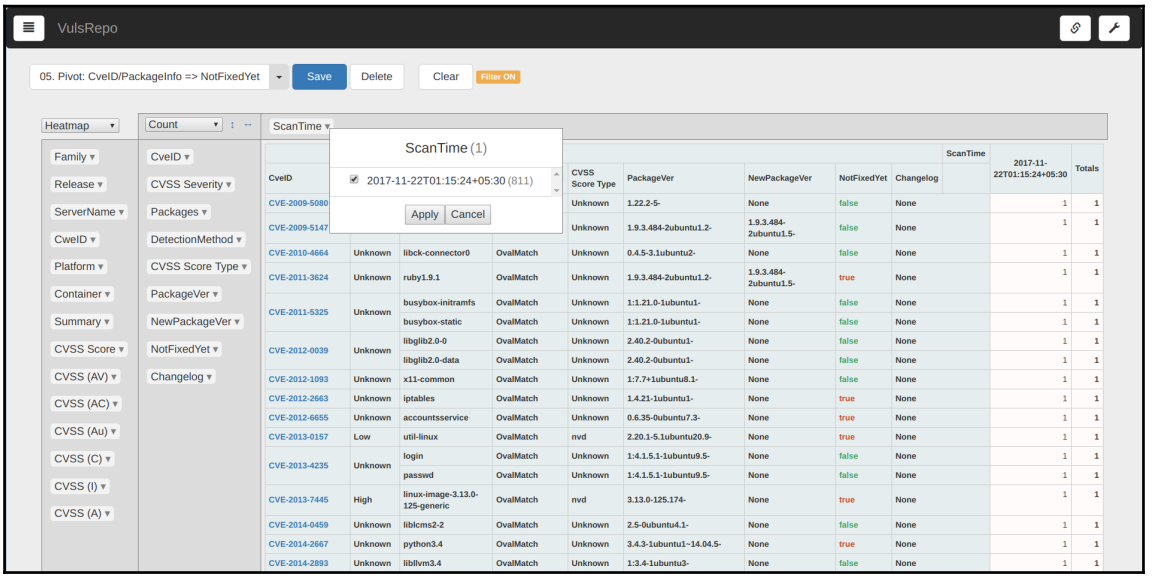
CVE-2017-1000112
8.9 (HIGH)

Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_MORE __ip_append_data() calls ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen - skb->len becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation

Show more...

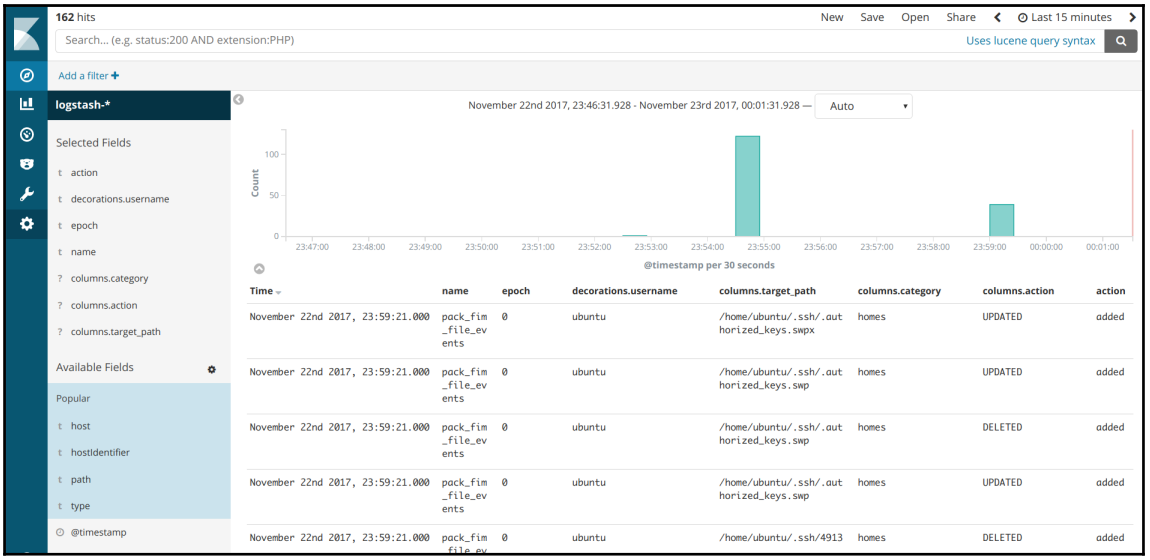
Installed	Candidate
linux-image-3.13.0-125-generic-3.13.0-125.174	Not Fixed Yet


192.168.33.60
VulsRepo
Select setting
Save
Delete
Clear
Filter OFF
Heatmap
Count
CVSS Severity
CVSS Score
Family
Release
CveID
Packages
NotFixedYet
CweID
Platform
DetectionMethod
ScanTime
ServerName
Container
CVSS Severity
CVSS Score
Low
High
Unknown
Totals
2.1
7.8
Unknown
ScanTime
ServerName
Container
2017-11-22T01:15:24+05:30
192-168-33-80
None
1
1
809
811
Totals
1
1
809
811


VulsRepo
05. Pivot: CveID/PackageInfo => NotFixedYet
Save
Delete
Clear
Filter ON
Heatmap
Count
ScanTime
Family
Release
ServerName
CweID
Platform
Container
Summary
CVSS Score
CVSS (AV)
CVSS (AC)
CVSS (Au)
CVSS (C)
CVSS (I)
CVSS (A)
CveID
CVSS Severity
Packages
DetectionMethod
CVSS Score Type
PackageVer
NewPackageVer
NotFixedYet
Changelog
ScanTime (1)
2017-11-22T01:15:24+05:30 (811)
Apply
Cancel
CveID
CVSS Score Type
PackageVer
NewPackageVer
NotFixedYet
Changelog
ScanTime
2017-11-22T01:15:24+05:30
Totals

```
osquery> SELECT * FROM users;
+------+------+-----------+------------+-----------+-----------------------------------+-------------------+-----------------+-------+
| uid  | gid  | uid_signed | gid_signed | username  | description                       | directory         | shell           | uuid  |
+------+------+-----------+------------+-----------+-----------------------------------+-------------------+-----------------+-------+
| 0    | 0    | 0         | 0          | root      | root                              | /root             | /bin/bash       |       |
| 1    | 1    | 1         | 1          | daemon    | daemon                            | /usr/sbin         | /usr/sbin/nologin |       |
| 2    | 2    | 2         | 2          | bin       | bin                               | /bin              | /usr/sbin/nologin |       |
| 3    | 3    | 3         | 3          | sys       | sys                               | /dev              | /usr/sbin/nologin |       |
| 4    | 65534 | 4         | 65534      | sync      | sync                              | /bin              | /bin/sync       |       |
| 5    | 60   | 5         | 60         | games     | games                             | /usr/games        | /usr/sbin/nologin |       |
| 6    | 12   | 6         | 12         | man       | man                               | /var/cache/man    | /usr/sbin/nologin |       |
| 7    | 7    | 7         | 7          | lp        | lp                                | /var/spool/lpd    | /usr/sbin/nologin |       |
| 8    | 8    | 8         | 8          | mail      | mail                              | /var/mail         | /usr/sbin/nologin |       |
| 9    | 9    | 9         | 9          | news      | news                              | /var/spool/news   | /usr/sbin/nologin |       |
| 10   | 10   | 10        | 10         | uucp      | uucp                              | /var/spool/uucp   | /usr/sbin/nologin |       |
| 13   | 13   | 13        | 13         | proxy     | proxy                             | /bin              | /usr/sbin/nologin |       |
| 33   | 33   | 33        | 33         | www-data  | www-data                          | /var/www          | /usr/sbin/nologin |       |
| 34   | 34   | 34        | 34         | backup    | backup                            | /var/backups      | /usr/sbin/nologin |       |
| 38   | 38   | 38        | 38         | list      | Mailing List Manager              | /var/list         | /usr/sbin/nologin |       |
| 39   | 39   | 39        | 39         | irc       | ircd                              | /var/run/ircd     | /usr/sbin/nologin |       |
| 41   | 41   | 41        | 41         | gnats     | Gnats Bug-Reporting System (admin) | /var/lib/gnats    | /usr/sbin/nologin |       |
| 65534 | 65534 | 65534     | 65534      | nobody    | nobody                            | /nonexistent      | /usr/sbin/nologin |       |
| 100  | 101  | 100       | 101        | libuuid   |                                   | /var/lib/libuuid  |                 |       |
| 101  | 104  | 101       | 104        | syslog    |                                   | /home/syslog      | /bin/false      |       |
| 102  | 106  | 102       | 106        | messagebus |                                  | /var/run/dbus     | /bin/false      |       |
| 103  | 109  | 103       | 109        | landscape |                                   | /var/lib/landscape | /bin/false      |       |
| 104  | 65534 | 104       | 65534      | sshd      |                                   | /var/run/sshd     | /usr/sbin/nologin |       |
| 105  | 1    | 105       | 1          | pollinate |                                   | /var/cache/pollinate | /bin/false      |       |
| 1000 | 1000 | 1000      | 1000       | vagrant   |                                   | /home/vagrant     | /bin/bash       |       |
| 106  | 112  | 106       | 112        | colord    | colord colour management daemon,,, | /var/lib/colord   | /bin/false      |       |
| 107  | 65534 | 107       | 65534      | statd     |                                   | /var/lib/nfs      | /bin/false      |       |
| 108  | 114  | 108       | 114        | puppet    | Puppet configuration management daemon,,, | /var/lib/puppet | /bin/false      |       |
| 1001 | 1001 | 1001      | 1001       | ubuntu    | Ubuntu                            | /home/ubuntu      | /bin/bash       |       |
| 109  | 116  | 109       | 116        | mysql     | MySQL Server,,,                   | /nonexistent      | /bin/false      |       |
+------+------+-----------+------------+-----------+-----------------------------------+-------------------+-----------------+-------+
```

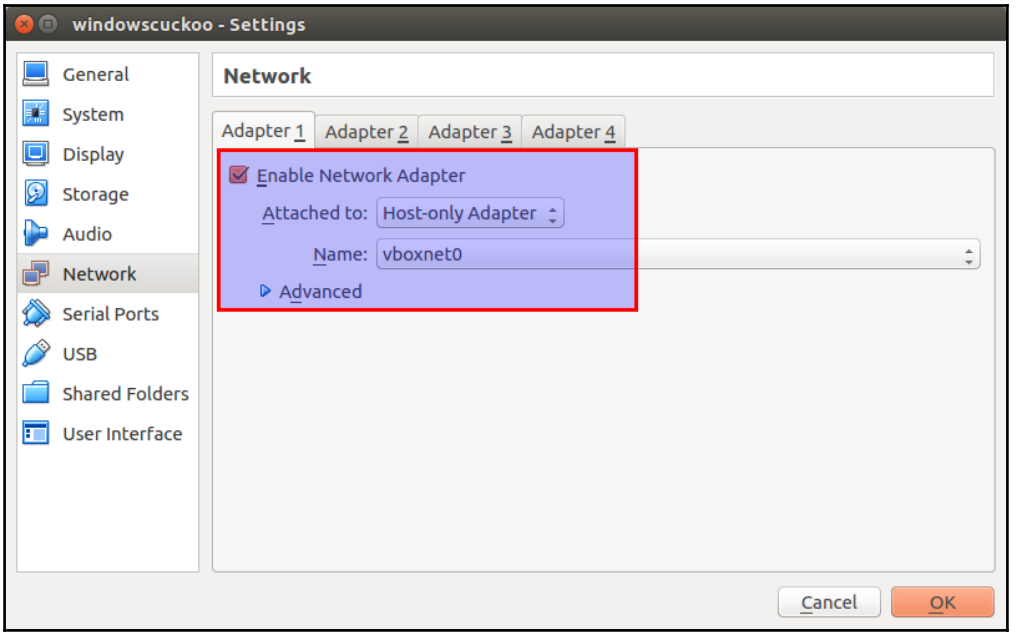
```
$ ansible-playbook -i inventory main.yml

PLAY [setting up osquery] ******************************************************************************

TASK [Gathering Facts] *********************************************************************************
ok: [192.168.33.60]

TASK [installing osquery] ******************************************************************************
changed: [192.168.33.60]

TASK [adding osquery configuration] ********************************************************************
changed: [192.168.33.60] => (item={u'src': u'fim.conf', u'dst': u'/usr/share/osquery/packs/fim.conf'})
changed: [192.168.33.60] => (item={u'src': u'osquery.conf', u'dst': u'/etc/osquery/osquery.conf'})

TASK [starting and enabling osquery service] ***********************************************************
changed: [192.168.33.60]

PLAY RECAP *********************************************************************************************
192.168.33.60              : ok=4    changed=3    unreachable=0    failed=0

$
```

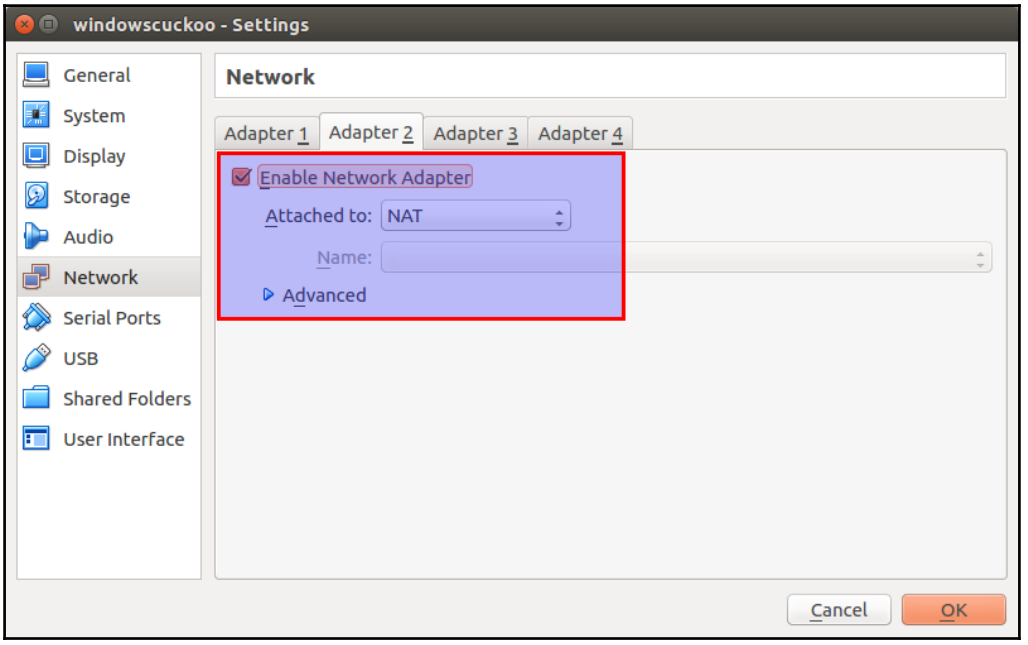

162 hits
New
Save
Open
Share
Last 15 minutes
Search... (e.g. status:200 AND extension:PHP)
Uses lucene query syntax
Add a filter +
logstash-*
Selected Fields
t action
t decorations.username
t epoch
t name
? columns.category
? columns.action
? columns.target_path
Available Fields
Popular
t host
t hostIdentifier
t path
t type
@timestamp
November 22nd 2017, 23:46:31.928 - November 23rd 2017, 00:01:31.928 —
Auto
Count
100
50
0
23:47:00
23:48:00
23:49:00
23:50:00
23:51:00
23:52:00
23:53:00
23:54:00
23:55:00
23:56:00
23:57:00
23:58:00
23:59:00
00:00:00
00:01:00
@timestamp per 30 seconds
Time
name
epoch
decorations.username
columns.target_path
columns.category
columns.action
action
November 22nd 2017, 23:59:21.000 pack_fim_file_events 0 ubuntu /home/ubuntu/.ssh/.authorized_keys.swpx homes UPDATED added
November 22nd 2017, 23:59:21.000 pack_fim_file_events 0 ubuntu /home/ubuntu/.ssh/.authorized_keys.swp homes UPDATED added
November 22nd 2017, 23:59:21.000 pack_fim_file_events 0 ubuntu /home/ubuntu/.ssh/.authorized_keys.swp homes DELETED added
November 22nd 2017, 23:59:21.000 pack_fim_file_events 0 ubuntu /home/ubuntu/.ssh/.authorized_keys.swp homes UPDATED added
November 22nd 2017, 23:59:21.000 pack_fim_file_ev 0 ubuntu /home/ubuntu/.ssh/4913 homes DELETED added

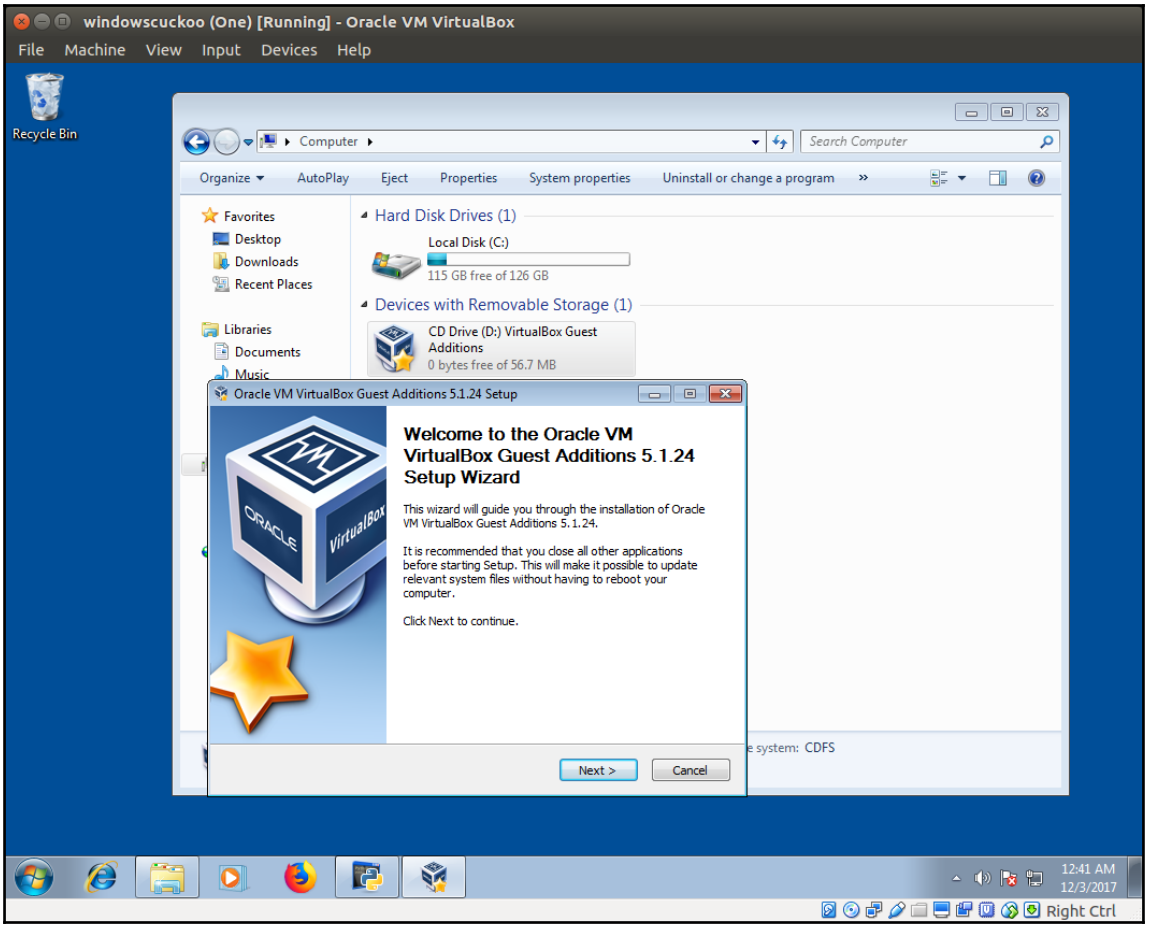
Chapter 09: Automating Lab Setups for Forensics Collection and Malware Analysis

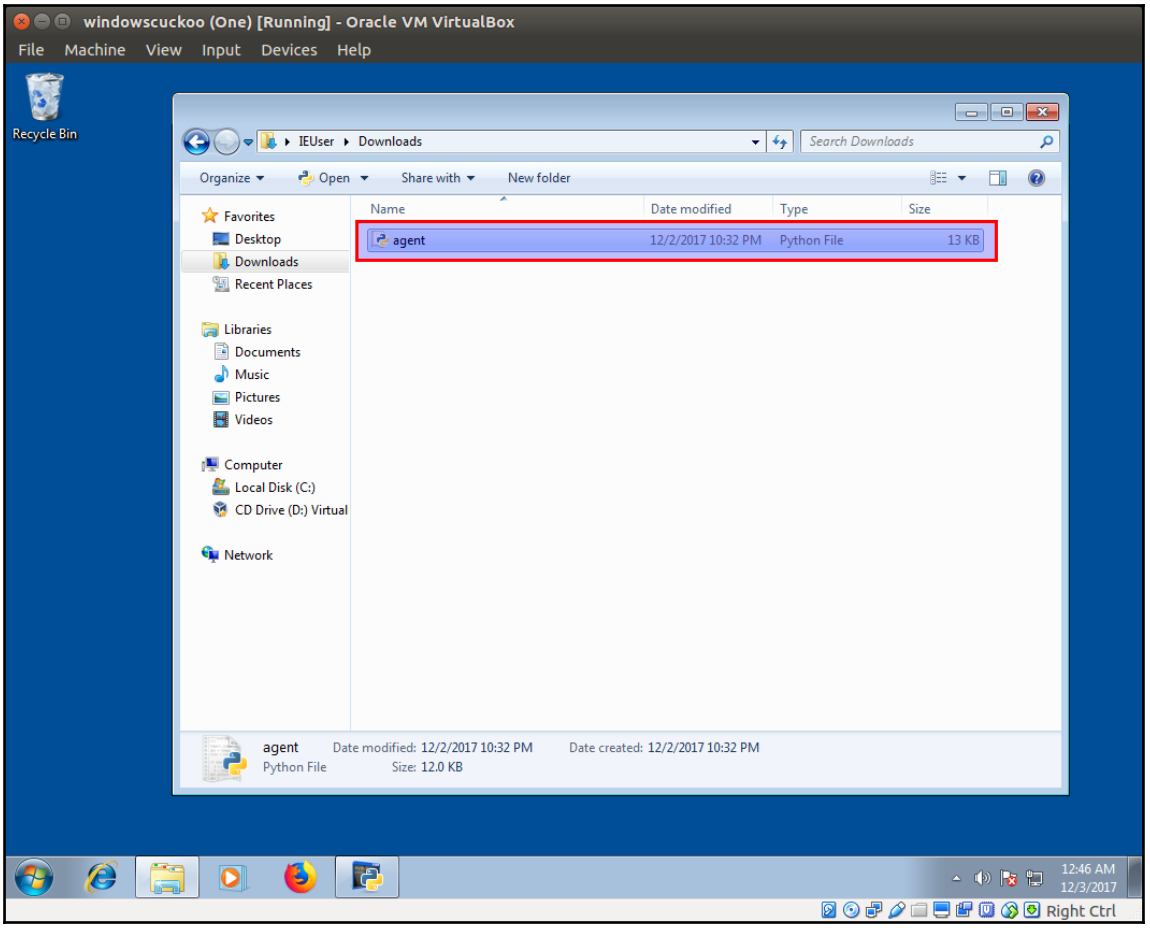
```
$ ansible-playbook -i inventory main.yml

PLAY [setting up VirusTotal] ***************************************************

TASK [Gathering Facts] *********************************************************
ok: [192.168.33.21]

TASK [installing pip] **********************************************************
ok: [192.168.33.21] => (item=[u'python-pip', u'unzip'])

TASK [checking if vt already exists] *******************************************
ok: [192.168.33.21]

TASK [downloading VirusTotal api tool repo] ************************************
changed: [192.168.33.21]

TASK [installing the dependencies] *********************************************
changed: [192.168.33.21]

TASK [installing vt] ***********************************************************
changed: [192.168.33.21]

PLAY RECAP *********************************************************************
192.168.33.21              : ok=6    changed=3    unreachable=0    failed=0
```

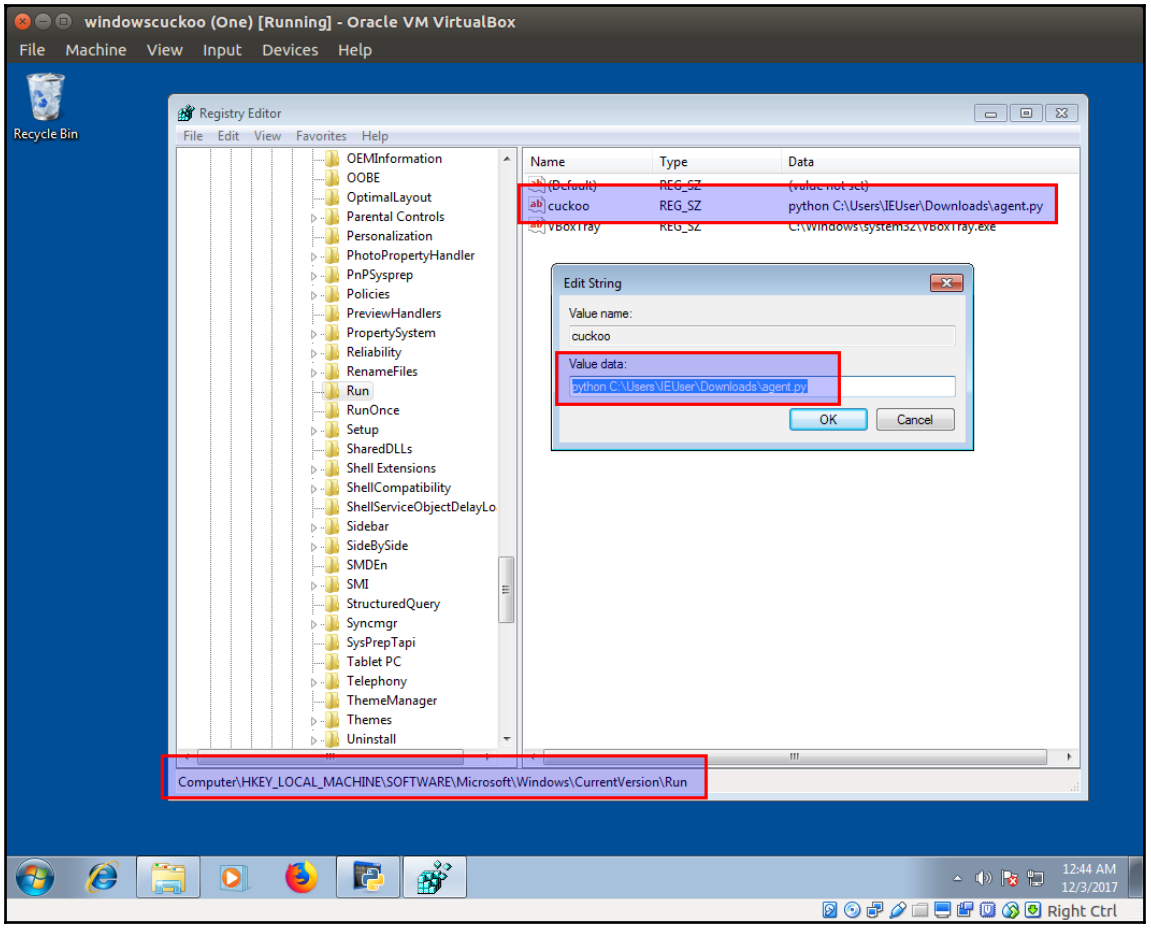
```
TASK [virus total scan results] ************************************************************************************************************************
ok: [192.168.33.21] => {
    "msg": [
        "",
        "Calculating hash for: /tmp/sample-file/random",
        "",
        "Scanned on : ",
        "\t2017-11-29 17:57:33",
        "",
        "Detections:",
        "\t 0/59 Positives/Total",
        "",
        "\tResults for MD5    : 04a9a0cadce634da6e3e83dd324c264c",
        "\tResults for SHA1   : aa3b2783e55cfd9d2eb687d607d7b8afd3fa83d3",
        "\tResults for SHA256 : cc1d5297f2904dec59294cc1bb34915a44fc7d17c00267e24040cc71bca6e67a",
        "",
        "\tPermanent Link : https://www.virustotal.com/file/cc1d5297f2904dec59294cc1bb34915a44fc7d17c00267e24040cc71bca6e67a/analysis/1511978253/",
        "",
        "",
        "Calculating hash for: /tmp/sample-file/rootkit.ex1",
        "",
        "Scanned on : ",
        "\t2017-11-29 16:48:46",
        "",
        "Detections:",
        "\t 60/68 Positives/Total",
        "",
        "\tResults for MD5    : 9219e2cfcc64ccde2d8de507538b9991",
        "\tResults for SHA1   : 181e59600d057dc6b31a3b19d7f4f75301a3425e",
        "\tResults for SHA256 : 5af3fd53aea5e008d8725c720ea0290e2e0cd485d8a953053ccf02e5e81a94a0",
        "",
        "\tPermanent Link : https://www.virustotal.com/file/5af3fd53aea5e008d8725c720ea0290e2e0cd485d8a953053ccf02e5e81a94a0/analysis/1511974126/"
    ]
}
```

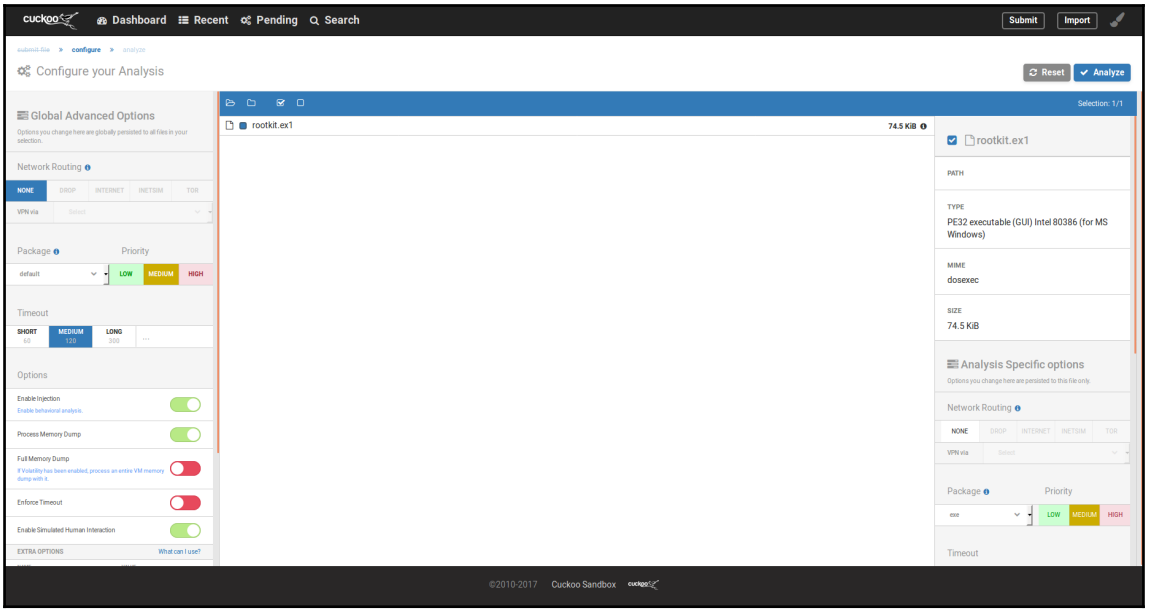

windowscuckoo - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
Host-only Adapter
Name:
vboxnet0
Advanced
Cancel
OK

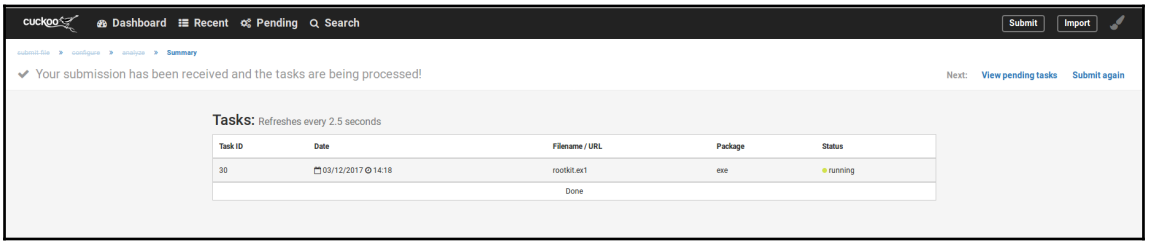

windowscuckoo - Settings
General
System
Display
Storage
Audio
Network
Serial Ports
USB
Shared Folders
User Interface
Network
Adapter 1
Adapter 2
Adapter 3
Adapter 4
Enable Network Adapter
Attached to:
NAT
Name:
Advanced
Cancel
OK

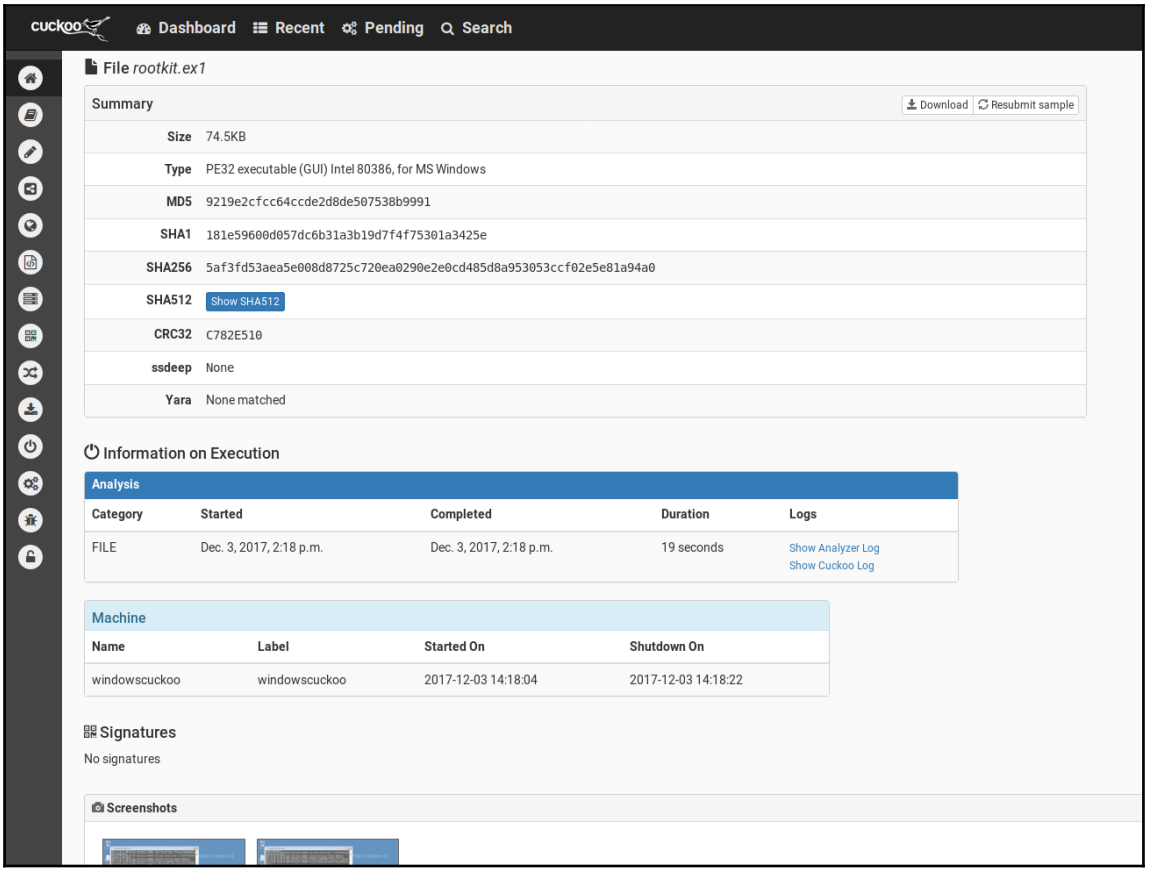

windowscuckoo (One) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Computer
Search Computer
Organize AutoPlay Eject Properties System properties Uninstall or change a program
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Hard Disk Drives (1)
Local Disk (C:)
115 GB free of 126 GB
Devices with Removable Storage (1)
CD Drive (D:) VirtualBox Guest Additions
0 bytes free of 56.7 MB
Oracle VM VirtualBox Guest Additions 5.1.24 Setup
Welcome to the Oracle VM VirtualBox Guest Additions 5.1.24 Setup Wizard
This wizard will guide you through the installation of Oracle VM VirtualBox Guest Additions 5.1.24.
It is recommended that you close all other applications before starting Setup. This will make it possible to update relevant system files without having to reboot your computer.
Click Next to continue.
Next >
Cancel
e system: CDFS
12:41 AM
12/3/2017
Right Ctrl

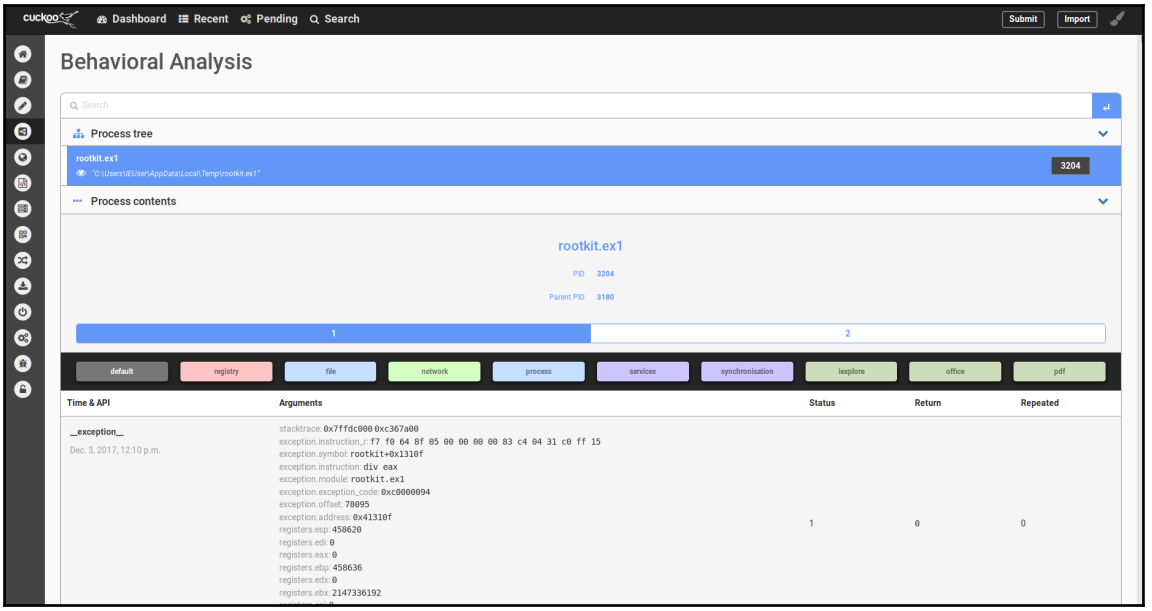

windowscuckoo (One) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
IEUser ▸ Downloads
Search Downloads
Organize
Open
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Local Disk (C:)
CD Drive (D:) Virtual
Network
Name
Date modified
Type
Size
agent
12/2/2017 10:32 PM
Python File
13 KB
agent
Python File
Date modified: 12/2/2017 10:32 PM
Size: 12.0 KB
Date created: 12/2/2017 10:32 PM
12:46 AM
12/3/2017
Right Ctrl


windowscuckoo (One) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Recycle Bin
Registry Editor
File Edit View Favorites Help
OEMInformation
OOBE
OptimalLayout
Parental Controls
Personalization
PhotoPropertyHandler
PnPSysprep
Policies
PreviewHandlers
PropertySystem
Reliability
RenameFiles
Run
RunOnce
Setup
SharedDLLs
Shell Extensions
ShellCompatibility
ShellServiceObjectDelayLo
Sidebar
SideBySide
SMDEn
SMI
StructuredQuery
Syncmgr
SysPrepTapi
Tablet PC
Telephony
ThemeManager
Themes
Uninstall
Name Type Data
(Default) REG_SZ (value not set)
cuckoo REG_SZ python C:\Users\IEUser\Downloads\agent.py
VBoxTray REG_SZ C:\Windows\system32\VBoxTray.exe
Edit String
Value name:
cuckoo
Value data:
python C:\Users\IEUser\Downloads\agent.py
OK
Cancel
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
12:44 AM
12/3/2017
Right Ctrl

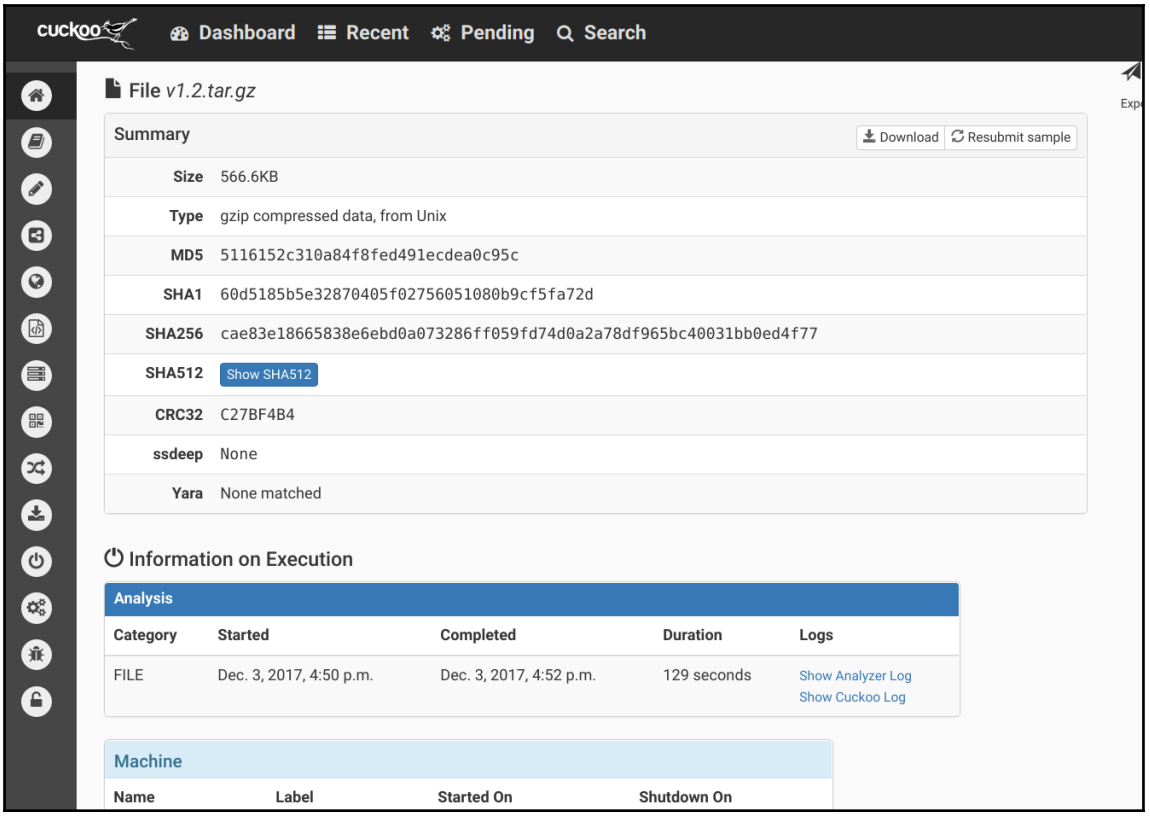

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
configure
Configure your Analysis
Reset
Analyze
Global Advanced Options
Options you change here are globally persisted to all files in your selection.
Network Routing
NONE
DROP
INTERNET
INETSIM
TOR
VPN via
Package
Priority
default
LOW
MEDIUM
HIGH
Timeout
SHORT
60
MEDIUM
120
LONG
300
Options
Enable Injection
Enable behavioral analysis.
Process Memory Dump
Full Memory Dump
If Volatility has been enabled, process an entire VM memory dump with it.
Enforce Timeout
Enable Simulated Human Interaction
EXTRA OPTIONS
What can I use?
Selection: 1/1
rootkit.ex1
74.5 KiB
PATH
TYPE
PE32 executable (GUI) Intel 80386 (for MS Windows)
MIME
dosexec
SIZE
74.5 KiB
Analysis Specific options
Options you change here are persisted to this file only.
exe
©2010-2017 Cuckoo Sandbox

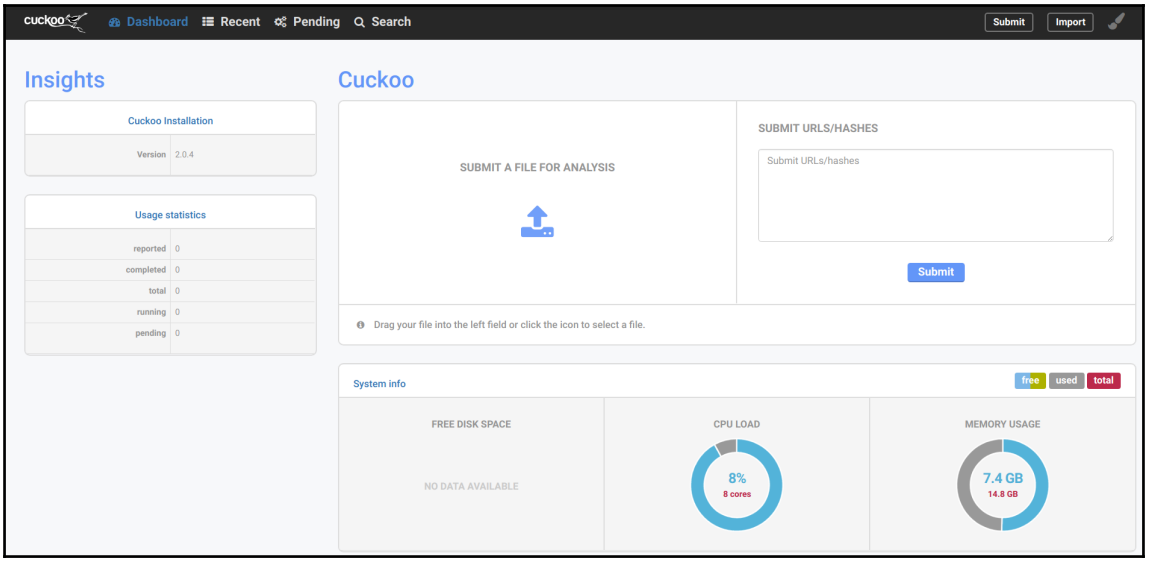

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
submit file
configure
analyze
Summary
Your submission has been received and the tasks are being processed!
Next:
View pending tasks
Submit again
Tasks: Refreshes every 2.5 seconds
Task ID
Date
Filename / URL
Package
Status
30
03/12/2017 14:18
rootkit.ex1
exe
running
Done


cuckoo
Dashboard
Recent
Pending
Search
File rootkit.ex1
Summary
Download
Resubmit sample
Size 74.5KB
Type PE32 executable (GUI) Intel 80386, for MS Windows
MD5 9219e2cfcc64ccde2d8de507538b9991
SHA1 181e59600d057dc6b31a3b19d7f4f75301a3425e
SHA256 5af3fd53aea5e008d8725c720ea0290e2e0cd485d8a953053ccf02e5e81a94a0
SHA512 Show SHA512
CRC32 C782E510
ssdeep None
Yara None matched
Information on Execution
Analysis
Category Started Completed Duration Logs
FILE Dec. 3, 2017, 2:18 p.m. Dec. 3, 2017, 2:18 p.m. 19 seconds Show Analyzer Log Show Cuckoo Log
Machine
Name Label Started On Shutdown On
windowscuckoo windowscuckoo 2017-12-03 14:18:04 2017-12-03 14:18:22
Signatures
No signatures
Screenshots

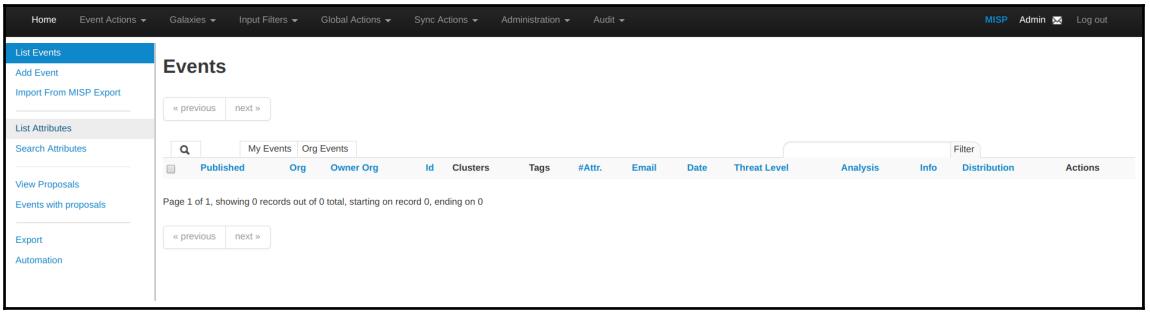



```
$ ansible-playbook -i inventory main.yml

PLAY [Cuckoo malware sample analysis] ******************************************

TASK [Gathering Facts] *********************************************************
ok: [172.16.1.119]

TASK [copying malware sample to cuckoo for analysis] ***************************
changed: [172.16.1.119]

TASK [submitting the files to cuckoo for analysis] *****************************
changed: [172.16.1.119]

PLAY RECAP *********************************************************************
172.16.1.119               : ok=3    changed=2    unreachable=0    failed=0
```

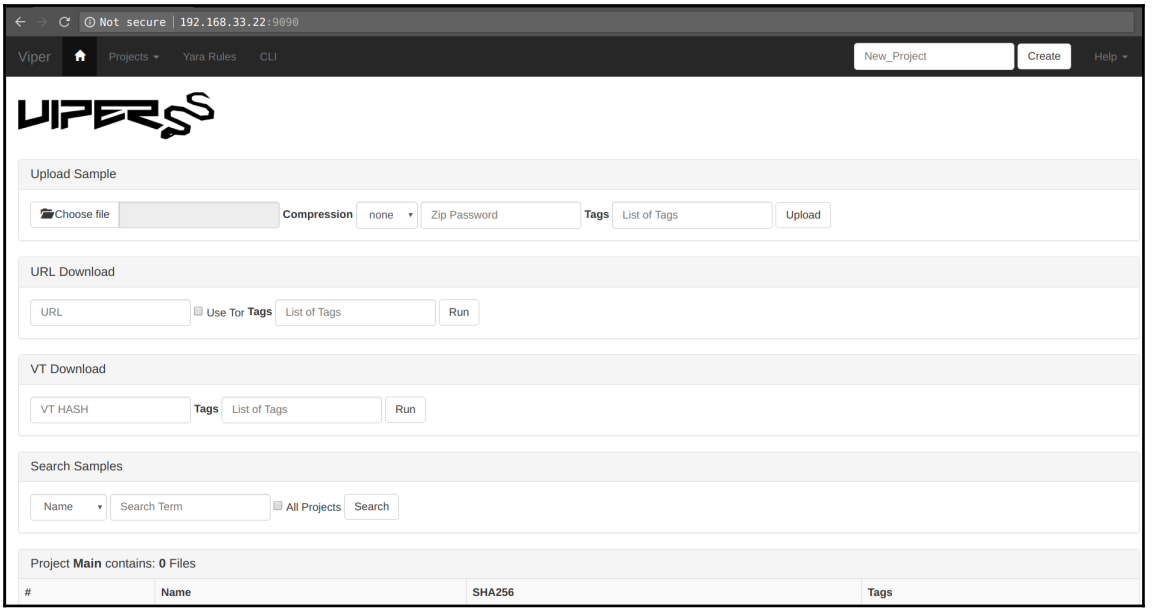

cuckoo
Dashboard
Recent
Pending
Search
File v1.2.tar.gz
Summary
Download
Resubmit sample
Size 566.6KB
Type gzip compressed data, from Unix
MD5 5116152c310a84f8fed491ecdea0c95c
SHA1 60d5185b5e32870405f02756051080b9cf5fa72d
SHA256 cae83e18665838e6ebd0a073286ff059fd74d0a2a78df965bc40031bb0ed4f77
SHA512 Show SHA512
CRC32 C27BF4B4
ssdeep None
Yara None matched
Information on Execution
Analysis
Category Started Completed Duration Logs
FILE Dec. 3, 2017, 4:50 p.m. Dec. 3, 2017, 4:52 p.m. 129 seconds Show Analyzer Log Show Cuckoo Log
Machine
Name Label Started On Shutdown On

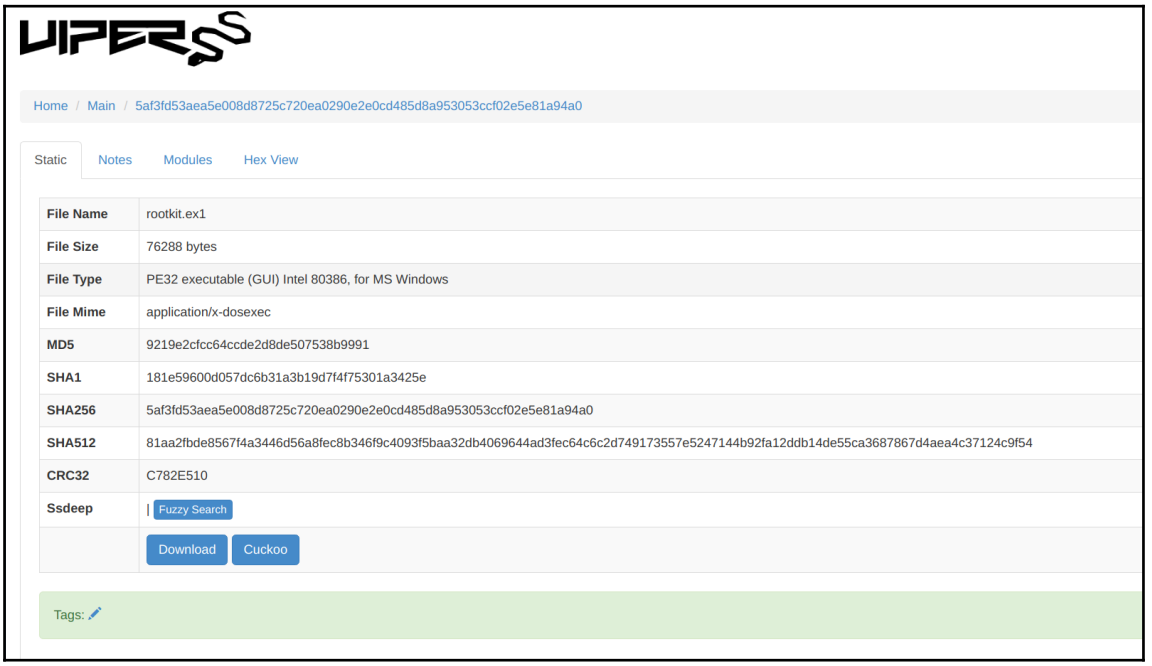

cuckoo
Dashboard
Recent
Pending
Search
Submit
Import
Insights
Cuckoo Installation
Version
2.0.4
Usage statistics
reported
0
completed
0
total
0
running
0
pending
0
Cuckoo
SUBMIT A FILE FOR ANALYSIS
SUBMIT URLS/HASHES
Submit URLs/hashes
Submit
Drag your file into the left field or click the icon to select a file.
System info
free
used
total
FREE DISK SPACE
NO DATA AVAILABLE
CPU LOAD
8%
8 cores
MEMORY USAGE
7.4 GB
14.8 GB


MISP
Threat Sharing
Login
Email
admin@admin.test
Password
Login



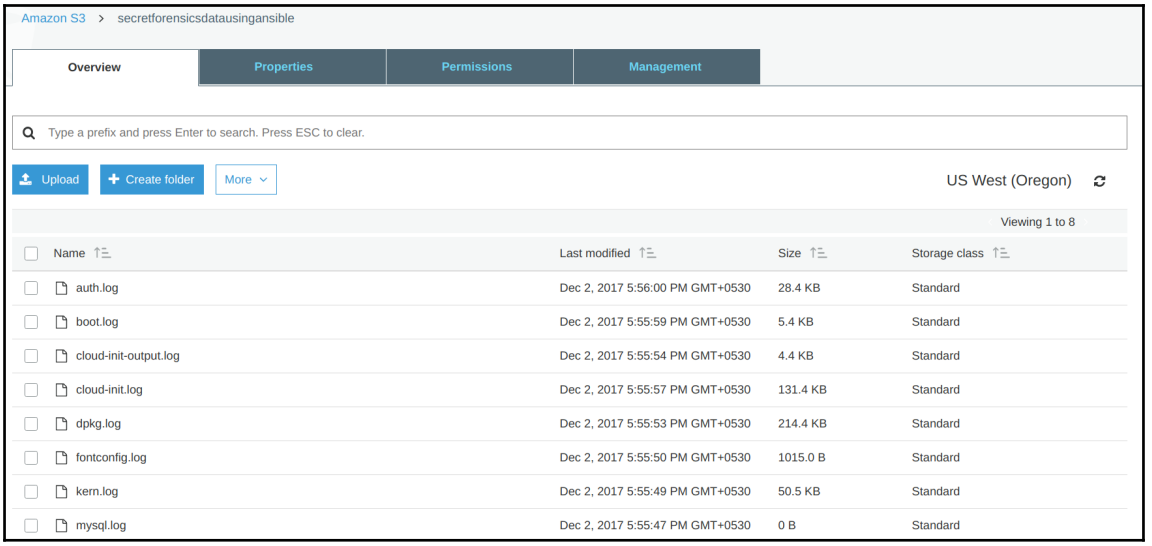

```
$ ansible-playbook -i inventory main.yml

PLAY [Setting up Viper - binary management and analysis framework] ********************************

TASK [Gathering Facts] ****************************************************************************
ok: [192.168.33.22]

TASK [dependencies : installing required packages] ************************************************
changed: [192.168.33.22] => (item=[u'gcc', u'python-dev', u'python-pip', u'libssl-dev', u'swig'])

TASK [dependencies : downloading ssdeep release] **************************************************
changed: [192.168.33.22]

TASK [dependencies : copy ssdeep setup script] ****************************************************
changed: [192.168.33.22]

TASK [dependencies : installing ssdeep] ***********************************************************
changed: [192.168.33.22]

TASK [dependencies : installing core dependencies] ************************************************
changed: [192.168.33.22] => (item=SQLAlchemy)
changed: [192.168.33.22] => (item=PrettyTable)
changed: [192.168.33.22] => (item=python-magic)
changed: [192.168.33.22] => (item=pydeep)

TASK [setup : downloading the release] ************************************************************
changed: [192.168.33.22]

TASK [setup : installing pip dependencies] ********************************************************
changed: [192.168.33.22]

TASK [setup : starting viper webinterface] ********************************************************
changed: [192.168.33.22]

TASK [setup : debug] ******************************************************************************
ok: [192.168.33.22] => {
    "msg": "Viper web interface is running at http://192.168.33.22:9090"
}

PLAY RECAP ****************************************************************************************
192.168.33.22              : ok=10   changed=8    unreachable=0    failed=0
```


Not secure 192.168.33.22:9090
Viper
Projects
Yara Rules
CLI
New_Project
Create
Help
Upload Sample
Choose file
Compression
none
Zip Password
Tags
List of Tags
Upload
URL Download
URL
Use Tor
Tags
List of Tags
Run
VT Download
VT HASH
Tags
List of Tags
Run
Search Samples
Name
Search Term
All Projects
Search
Project Main contains: 0 Files
#
Name
SHA256
Tags


Home / Main / 5af3fd53aea5e008d8725c720ea0290e2e0cd485d8a953053ccf02e5e81a94a0
Static
Notes
Modules
Hex View
File Name
rootkit.ex1
File Size
76288 bytes
File Type
PE32 executable (GUI) Intel 80386, for MS Windows
File Mime
application/x-dosexec
MD5
9219e2cfcc64ccde2d8de507538b9991
SHA1
181e59600d057dc6b31a3b19d7f4f75301a3425e
SHA256
5af3fd53aea5e008d8725c720ea0290e2e0cd485d8a953053ccf02e5e81a94a0
SHA512
81aa2fbde8567f4a3446d56a8fec8b346f9c4093f5baa32db4069644ad3fec64c6c2d749173557e5247144b92fa12ddb14de55ca3687867d4aea4c37124c9f54
CRC32
C782E510
Ssdeep
Fuzzy Search
Download
Cuckoo
Tags:

```
$ tree /tmp/LOGS_*
/tmp/LOGS_blue-server
└── 192.168.100.10
    └── var
        └── log
            ├── apt
            │   ├── history.log
            │   └── term.log
            ├── auth.log
            ├── cloud-init.log
            ├── cloud-init-output.log
            ├── dpkg.log
            ├── kern.log
            └── nginx
                ├── access.log
                └── error.log
/tmp/LOGS_green-server
└── 192.168.100.20
    └── var
        └── log
            ├── apt
            │   ├── history.log
            │   └── term.log
            ├── auth.log
            ├── cloud-init.log
            ├── cloud-init-output.log
            ├── dpkg.log
            ├── kern.log
            └── nginx
                ├── access.log
                └── error.log

10 directories, 18 files
```

```
$ ansible-playbook main.yml
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available


PLAY [backing up the log data] *************************************************

TASK [installing s3cmd if not installed] ***************************************
changed: [localhost] => (item=[u'python-magic', u'python-dateutil', u's3cmd'])

TASK [create s3cmd config file] ************************************************
changed: [localhost]

TASK [make sure "secretforensicsdatausingansible" is avilable] *****************
changed: [localhost]

TASK [running the s3 backup to "secretforensicsdatausingansible"] **************
changed: [localhost]

PLAY RECAP *********************************************************************
localhost                  : ok=4    changed=4    unreachable=0    failed=0
```


Amazon S3 > secretforensicsdatausingansible
Overview
Properties
Permissions
Management
Type a prefix and press Enter to search. Press ESC to clear.
Upload
Create folder
More
US West (Oregon)
Viewing 1 to 8
Name
Last modified
Size
Storage class
auth.log
Dec 2, 2017 5:56:00 PM GMT+0530
28.4 KB
Standard
boot.log
Dec 2, 2017 5:55:59 PM GMT+0530
5.4 KB
Standard
cloud-init-output.log
Dec 2, 2017 5:55:54 PM GMT+0530
4.4 KB
Standard
cloud-init.log
Dec 2, 2017 5:55:57 PM GMT+0530
131.4 KB
Standard
dpkg.log
Dec 2, 2017 5:55:53 PM GMT+0530
214.4 KB
Standard
fontconfig.log
Dec 2, 2017 5:55:50 PM GMT+0530
1015.0 B
Standard
kern.log
Dec 2, 2017 5:55:49 PM GMT+0530
50.5 KB
Standard
mysql.log
Dec 2, 2017 5:55:47 PM GMT+0530
0 B
Standard

Chapter 10: Writing an Ansible Module for Security Testing

```
PLAY [Setting Developer Environment] *******************************************

TASK [Gathering Facts] *********************************************************
ok: [172.16.1.119]

TASK [installing prerequirements if not installed] *****************************
ok: [172.16.1.119] => (item=[u'git', u'virtualenv', u'python-pip'])

TASK [downloading ansible repo locally] ****************************************
ok: [172.16.1.119]

TASK [creating virtual environment] ********************************************
changed: [172.16.1.119]

PLAY RECAP *********************************************************************
172.16.1.119               : ok=4    changed=1    unreachable=0    failed=0
```

```
2594 [ZAP-daemon] INFO org.parosproxy.paros.extension.ExtensionLoader  - Initializing Easy way to
 replace strings in requests and responses
2689 [ZAP-daemon] INFO org.zaproxy.zap.extension.callback.ExtensionCallback  - Started callback s
erver on 0.0.0.0:40083
2689 [ZAP-daemon] INFO org.zaproxy.zap.extension.dynssl.ExtensionDynSSL  - Creating new root CA c
ertificate
3089 [ZAP-daemon] INFO org.zaproxy.zap.extension.dynssl.ExtensionDynSSL  - New root CA certificat
e created
3091 [ZAP-daemon] INFO org.zaproxy.zap.DaemonBootstrap  - ZAP is now listening on 0.0.0.0:8080
```

```
localhost | FAILED! => {
    "changed": false,
    "module_stderr": "",
    "module_stdout": "",
    "msg": "MODULE FAILURE",
    "rc": 0
}
```

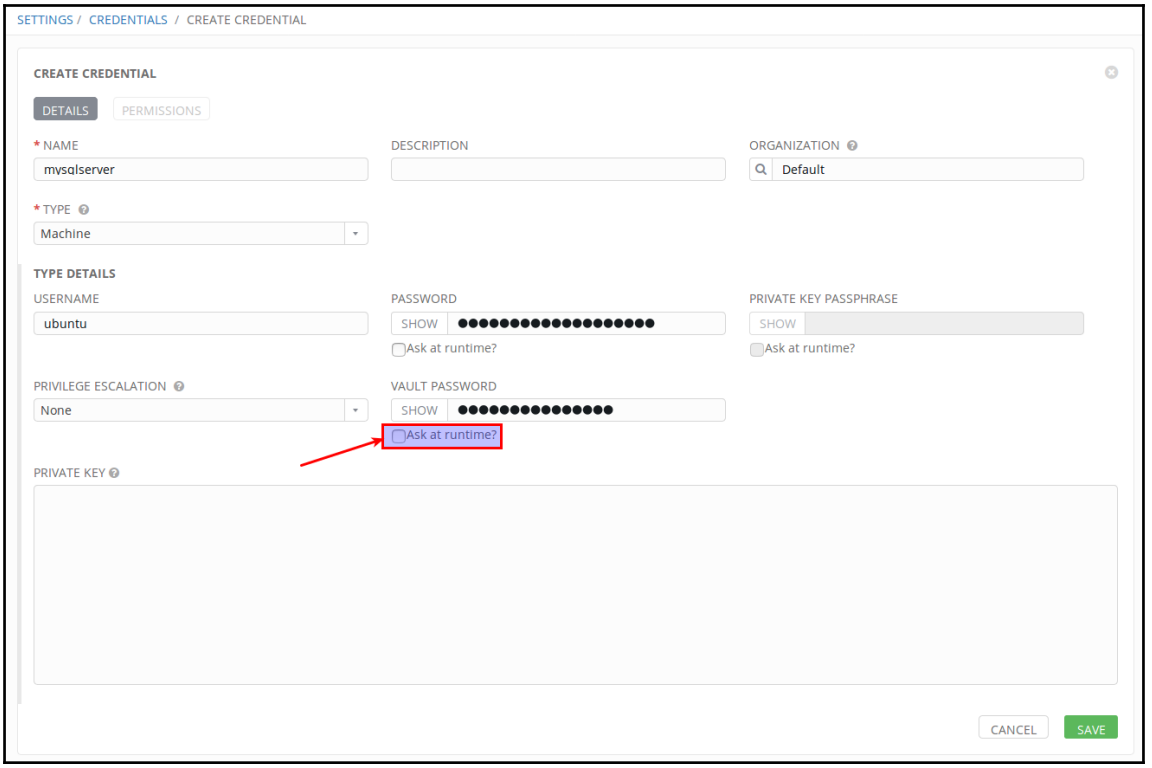
```
PLAY [Testing OWASP ZAP Test Module] ********************************************************

TASK [Gathering Facts] **********************************************************************
ok: [localhost]

TASK [Scan a website] ***********************************************************************
ok: [localhost]

PLAY RECAP **********************************************************************************
localhost                  : ok=2    changed=0    unreachable=0    failed=0
```

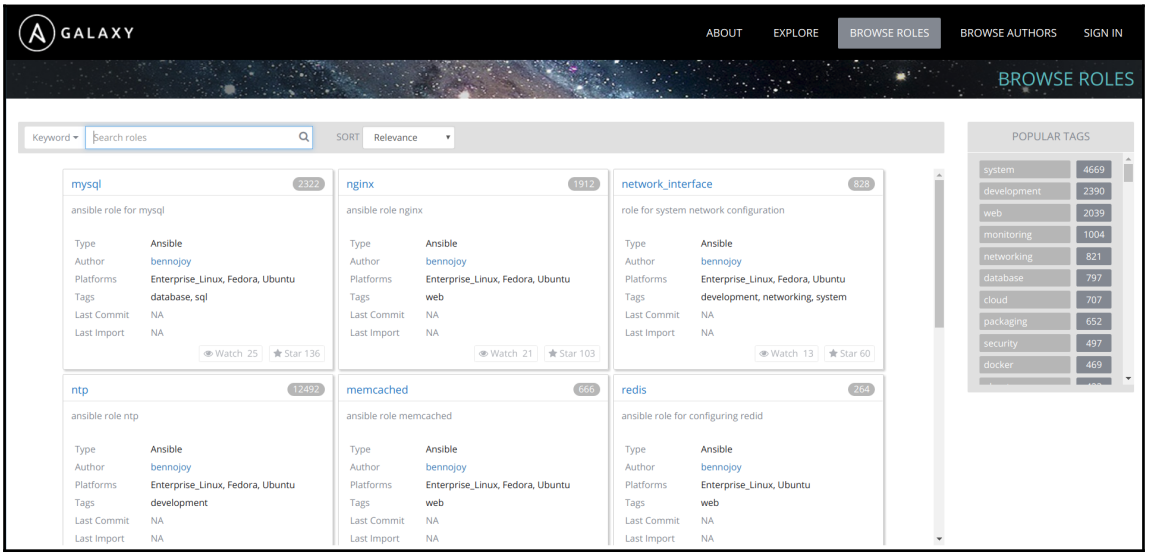
Chapter 11: Ansible Security Best Practices, References, and Further Reading

```
$ ansible-playbook --ask-vault -i hosts main.yml
Vault password:

PLAY [Installing MySQL server] *********************************************

TASK [mysqlsetup : set mysql root password] ********************************
changed: [192.168.33.22]

TASK [mysqlsetup : confirm mysql root password] ****************************
changed: [192.168.33.22]

TASK [mysqlsetup : install mysqlserver] ************************************
changed: [192.168.33.22] => (item=[u'mysql-server', u'mysql-client'])

PLAY RECAP *****************************************************************
192.168.33.22              : ok=3    changed=3    unreachable=0    failed=0
```

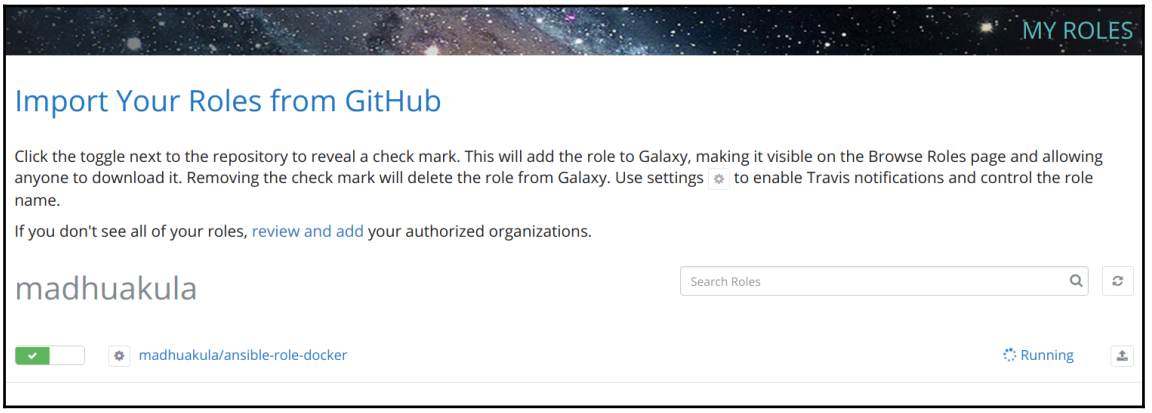
```
$ echo -n '53ff4ad63849e6977cb652763g7b7c64e2fa42a' | ansible-vault encrypt_string --stdin-name 'api_key'
New Vault password:
Confirm New Vault password:
Reading plaintext input from stdin. (ctrl-d to end input)
api_key: !vault |
          $ANSIBLE_VAULT;1.1;AES256
          30623561633236303231353061353365326136346165303662333762363730663561613136316133
          34343935316231653239343333313962386162626166340a643337396333663836633634656537
          66303633666337653266646365613533333264353235616634633433653737323532646261633939
          38636264373937303 20a663737663036663332396435323962313632343639383132393766666439
          33663735363464663461353138313339336264623338393863363065663530666262646466643563
          66366536396637323633236333386133346635626234303165
Encryption successful
```

```
$ ansible-playbook --ask-vault-pass main.yml
Vault password:
 [WARNING]: Could not match supplied host pattern, ignoring: all

 [WARNING]: provided hosts list is empty, only localhost is available


PLAY [ViewDNS domain information] ***********************************************

TASK [Gathering Facts] **********************************************************
ok: [localhost]

TASK [getting google.com server info] *******************************************
ok: [localhost]

TASK [debug] ********************************************************************
ok: [localhost] => {
    "msg": {
        "query": {
            "host": "google.com",
            "tool": "reverseip_PRO"
        },
        "response": {
            "domain_count": "3",
            "domains": [
                {
                    "last_resolved": "2017-12-01",
                    "name": "epinoybills.com"
                },
                {
                    "last_resolved": "2017-12-01",
                    "name": "google.com"
                },
                {
                    "last_resolved": "2017-12-01",
                    "name": "youtube.com"
                }
            ]
        }
    }
}

PLAY RECAP **********************************************************************
localhost                  : ok=3    changed=0    unreachable=0    failed=0
```

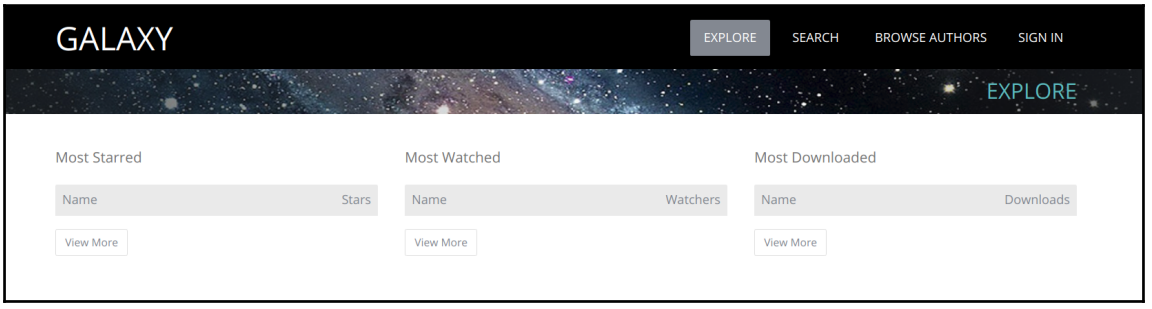

SETTINGS / CREDENTIALS / CREATE CREDENTIAL
CREATE CREDENTIAL
DETAILS
PERMISSIONS
* NAME
mysqlserver
DESCRIPTION
ORGANIZATION
Default
* TYPE
Machine
TYPE DETAILS
USERNAME
ubuntu
PASSWORD
SHOW
Ask at runtime?
PRIVATE KEY PASSPHRASE
SHOW
Ask at runtime?
PRIVILEGE ESCALATION
None
VAULT PASSWORD
SHOW
Ask at runtime?
PRIVATE KEY
CANCEL
SAVE


GALAXY
ABOUT
EXPLORE
BROWSE ROLES
BROWSE AUTHORS
SIGN IN
BROWSE ROLES
Keyword
Search roles
SORT
Relevance
POPULAR TAGS
mysql
2322
ansible role for mysql
nginx
1912
ansible role nginx
network_interface
828
role for system network configuration
ntp
12492
ansible role ntp
memcached
666
ansible role memcached
redis
264
ansible role for configuring redid

```
$ ansible-galaxy --help
Usage: ansible-galaxy [delete|import|info|init|install|list|login|remove|search|setup] [--help] [options] ...

Options:
  -h, --help            show this help message and exit
  -c, --ignore-certs    Ignore SSL certificate validation errors.
  -s API_SERVER, --server=API_SERVER
                        The API server destination
  -v, --verbose         verbose mode (-vvv for more, -vvvv to enable
                        connection debugging)
  --version             show program's version number and exit

 See 'ansible-galaxy <command> --help' for more information on a specific
command.
```




```
$ docker ps
CONTAINER ID        IMAGE                          COMMAND                  CREATED             STATUS              PORTS                                  NAMES
090c984666ef        ansible/galaxy:develop         "/entrypoint.sh /b..."   8 seconds ago       Up 7 seconds        8000/tcp                               galaxy_worker_1
cf0c23f9b173        ansible/galaxy:develop         "/entrypoint.sh /b..."   8 seconds ago       Up 8 seconds        0.0.0.0:80->8000/tcp                   galaxy_web_1
c3bf8f05ebc5        rabbitmq:latest                "docker-entrypoint..."   10 seconds ago      Up 9 seconds        4369/tcp, 5671-5672/tcp, 25672/tcp     galaxy_rabbitmq_1
09fb10beca2c        memcached:latest               "docker-entrypoint..."   10 seconds ago      Up 9 seconds        11211/tcp                              galaxy_memcache_1
5cbf8ee6ed80        postgres:9.5.4                 "/docker-entrypoin..."   10 seconds ago      Up 8 seconds        5432/tcp                               galaxy_postgres_1
4b684ab656e7        elasticsearch:2.4.1            "/docker-entrypoin..."   10 seconds ago      Up 9 seconds        9200/tcp, 9300/tcp                     galaxy_elastic_1
$
```



```
$ ansible-galaxy install dev-sec.os-hardening
- downloading role 'os-hardening', owned by dev-sec
- downloading role from https://github.com/dev-sec/ansible-os-hardening/archive/4.2.0.tar.gz
- extracting dev-sec.os-hardening to /home/ubuntu/.ansible/roles/dev-sec.os-hardening
- dev-sec.os-hardening (4.2.0) was installed successfully
$
```

```
PLAY [localhost] ***************************************************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************************************
ok: [localhost]

TASK [dev-sec.os-hardening : Set OS family dependent variables] ****************************************************************************************************************
ok: [localhost]

TASK [dev-sec.os-hardening : Set OS dependent variables] ***********************************************************************************************************************

TASK [dev-sec.os-hardening : create limits.d-directory if it does not exist | sysctl-31a, sysctl-31b] *************************************************************************
skipping: [localhost]

TASK [dev-sec.os-hardening : create sane limits.conf | sysctl-31a, sysctl-31b] *************************************************************************************************
skipping: [localhost]

TASK [dev-sec.os-hardening : create login.defs | os-05, os-05b] ****************************************************************************************************************
changed: [localhost]

TASK [dev-sec.os-hardening : find directories for minimizing access] ***********************************************************************************************************
ok: [localhost] => (item=/usr/local/sbin)
ok: [localhost] => (item=/usr/local/bin)
ok: [localhost] => (item=/usr/sbin)
ok: [localhost] => (item=/usr/bin)
ok: [localhost] => (item=/sbin)
ok: [localhost] => (item=/bin)
```

```
TASK [dev-sec.os-hardening : minimize access] **********************************************************************************************************************************
ok: [localhost] => (item={'_ansible_parsed': True, u'stat': {u'isuid': False, u'uid': 0, u'exists': True, u'attr_flags': u'e', u'woth': False, u'isreg': False, u'device_type'
: 0, u'mtime': 1500647698.7412262, u'block_size': 4096, u'inode': 66669, u'isgid': False, u'size': 4096, u'executable': True, u'roth': True, u'charset': u'binary', u'readable
': True, u'version': u'1546678241', u'pw_name': u'root', u'gid': 0, u'ischr': False, u'wusr': True, u'writeable': True, u'isdir': True, u'blocks': 8, u'xoth': True, u'rusr':
True, u'nlink': 2, u'issock': False, u'rgrp': True, u'gr_name': u'root', u'path': u'/usr/local/sbin', u'xusr': True, u'atime': 1512286775.327596, u'mimetype': u'inode/directo
ry', u'ctime': 1500648230.5338638, u'isblk': False, u'xgrp': True, u'dev': 2049, u'wgrp': False, u'isfifo': False, u'mode': u'0755', u'islnk': False, u'attributes': [u'extent
s']}, u'changed': False, '_ansible_no_log': False, 'item': u'/usr/local/sbin', '_ansible_item_result': True, 'failed': False, u'invocation': {u'module_args': {u'checksum_algo
rithm': u'sha1', u'get_checksum': True, u'follow': False, u'path': u'/usr/local/sbin', u'get_md5': True, u'get_mime': True, u'get_attributes': True}}, '_ansible_ignore_errors
': None})
ok: [localhost] => (item={'_ansible_parsed': True, u'stat': {u'isuid': False, u'uid': 0, u'exists': True, u'attr_flags': u'e', u'woth': False, u'isreg': False, u'device_type'
: 0, u'mtime': 1500647698.7412262, u'block_size': 4096, u'inode': 66663, u'isgid': False, u'size': 4096, u'executable': True, u'roth': True, u'charset': u'binary', u'readable
': True, u'version': u'1546678235', u'pw_name': u'root', u'gid': 0, u'ischr': False, u'wusr': True, u'writeable': True, u'isdir': True, u'blocks': 8, u'xoth': True, u'rusr':
True, u'nlink': 2, u'issock': False, u'rgrp': True, u'gr_name': u'root', u'path': u'/usr/local/bin', u'xusr': True, u'atime': 1512286775.327596, u'mimetype': u'inode/director
y', u'ctime': 1500648230.5338638, u'isblk': False, u'xgrp': True, u'dev': 2049, u'wgrp': False, u'isfifo': False, u'mode': u'0755', u'islnk': False, u'attributes': [u'extents
']}, u'changed': False, '_ansible_no_log': False, 'item': u'/usr/local/bin', '_ansible_item_result': True, 'failed': False, u'invocation': {u'module_args': {u'checksum_algori
thm': u'sha1', u'get_checksum': True, u'follow': False, u'path': u'/usr/local/bin', u'get_md5': True, u'get_mime': True, u'get_attributes': True}}, '_ansible_ignore_errors':
None})
ok: [localhost] => (item={'_ansible_parsed': True, u'stat': {u'isuid': False, u'uid': 0, u'exists': True, u'attr_flags': u'e', u'woth': False, u'isreg': False, u'device_type'
: 0, u'mtime': 1500648593.766223, u'block_size': 4096, u'inode': 32318, u'isgid': False, u'size': 4096, u'executable': True, u'roth': True, u'charset': u'binary', u'readable'
: True, u'version': u'1546644977', u'pw_name': u'root', u'gid': 0, u'ischr': False, u'wusr': True, u'writeable': True, u'isdir': True, u'blocks': 8, u'xoth': True, u'rusr': T
rue, u'nlink': 2, u'issock': False, u'rgrp': True, u'gr_name': u'root', u'path': u'/usr/sbin', u'xusr': True, u'atime': 1512286775.327596, u'mimetype': u'inode/directory', u'
ctime': 1500648593.766223, u'isblk': False, u'xgrp': True, u'dev': 2049, u'wgrp': False, u'isfifo': False, u'mode': u'0755', u'islnk': False, u'attributes': [u'extents']}, u'
changed': False, '_ansible_no_log': False, 'item': u'/usr/sbin', '_ansible_item_result': True, 'failed': False, u'invocation': {u'module_args': {u'checksum_algorithm': u'sha1
', u'get_checksum': True, u'follow': False, u'path': u'/usr/sbin', u'get_md5': True, u'get_mime': True, u'get_attributes': True}}, '_ansible_ignore_errors': None})
ok: [localhost] => (item={'_ansible_parsed': True, u'stat': {u'isuid': False, u'uid': 0, u'exists': True, u'attr_flags': u'Ie', u'woth': False, u'isreg': False, u'device_type
': 0, u'mtime': 1512287010.753355, u'block_size': 4096, u'inode': 32319, u'isgid': False, u'size': 20480, u'executable': True, u'roth': True, u'charset': u'binary', u'readabl
e': True, u'version': u'1546645124', u'pw_name': u'root', u'gid': 0, u'ischr': False, u'wusr': True, u'writeable': True, u'isdir': True, u'blocks': 40, u'xoth': True, u'rusr'
: True, u'nlink': 2, u'issock': False, u'rgrp': True, u'gr_name': u'root', u'path': u'/usr/bin', u'xusr': True, u'atime': 1512287014.543249, u'mimetype': u'inode/directory',
u'ctime': 1512287010.753355, u'isblk': False, u'xgrp': True, u'dev': 2049, u'wgrp': False, u'isfifo': False, u'mode': u'0755', u'islnk': False, u'attributes': [u'indexed', u'
extents']}, u'changed': False, '_ansible_no_log': False, 'item': u'/usr/bin', '_ansible_item_result': True, 'failed': False, u'invocation': {u'module_args': {u'checksum_algor
ithm': u'sha1', u'get_checksum': True, u'follow': False, u'path': u'/usr/bin', u'get_md5': True, u'get_mime': True, u'get_attributes': True}}, '_ansible_ignore_errors': None}
)
ok: [localhost] => (item={'_ansible_parsed': True, u'stat': {u'isuid': False, u'uid': 0, u'exists': True, u'attr_flags': u'e', u'woth': False, u'isreg': False, u'device_type'
: 0, u'mtime': 1500648591.2542205, u'block_size': 4096, u'inode': 4217, u'isgid': False, u'size': 4096, u'executable': True, u'roth': True, u'charset': u'binary', u'readable'
: True, u'version': u'1546624967', u'pw_name': u'root', u'gid': 0, u'ischr': False, u'wusr': True, u'writeable': True, u'isdir': True, u'blocks': 8, u'xoth': True, u'rusr': T
rue, u'nlink': 2, u'issock': False, u'rgrp': True, u'gr_name': u'root', u'path': u'/sbin', u'xusr': True, u'atime': 1512286775.327596, u'mimetype': u'inode/directory', u'ctim
e': 1500648591.2542205, u'isblk': False, u'xgrp': True, u'dev': 2049, u'wgrp': False, u'isfifo': False, u'mode': u'0755', u'islnk': False, u'attributes': [u'extents']}, u'cha
nged': False, '_ansible_no_log': False, 'item': u'/sbin', '_ansible_item_result': True, 'failed': False, u'invocation': {u'module_args': {u'checksum_algorithm': u'sha1', u'ge
t_checksum': True, u'follow': False, u'path': u'/sbin', u'get_md5': True, u'get_mime': True, u'get_attributes': True}}, '_ansible_ignore_errors': None})
ok: [localhost] => (item={'_ansible_parsed': True, u'stat': {u'isuid': False, u'uid': 0, u'exists': True, u'attr_flags': u'e', u'woth': False, u'isreg': False, u'device_type'
: 0, u'mtime': 1500647870.1534083, u'block_size': 4096, u'inode': 12, u'isgid': False, u'size': 4096, u'executable': True, u'roth': True, u'charset': u'binary', u'readable':
True, u'version': u'1546620762', u'pw_name': u'root', u'gid': 0, u'ischr': False, u'wusr': True, u'writeable': True, u'isdir': True, u'blocks': 8, u'xoth': True, u'rusr': Tru
e, u'nlink': 2, u'issock': False, u'rgrp': True, u'gr_name': u'root', u'path': u'/bin', u'xusr': True, u'atime': 1512286775.327596, u'mimetype': u'inode/directory', u'ctime':
 1500648227.6818607, u'isblk': False, u'xgrp': True, u'dev': 2049, u'wgrp': False, u'isfifo': False, u'mode': u'0755', u'islnk': False, u'attributes': [u'extents']}, u'change
d': False, '_ansible_no_log': False, 'item': u'/bin', '_ansible_item_result': True, 'failed': False, u'invocation': {u'module_args': {u'checksum_algorithm': u'sha1', u'get_ch
ecksum': True, u'follow': False, u'path': u'/bin', u'get_md5': True, u'get_mime': True, u'get_attributes': True}}, '_ansible_ignore_errors': None})
```

```
TASK [dev-sec.os-hardening : NSA 2.3.3.5 Upgrade Password Hashing Algorithm to SHA-512] ***********************************************************************
changed: [localhost]

TASK [dev-sec.os-hardening : create profile.conf] ******************************************************************************************************
changed: [localhost]

TASK [dev-sec.os-hardening : create securetty] **********************************************************************************************************
changed: [localhost]

TASK [dev-sec.os-hardening : remove suid/sgid bit from binaries in blacklist | os-06] ***********************************************************************
ok: [localhost] => (item=/usr/bin/rcp)
ok: [localhost] => (item=/usr/bin/rlogin)
ok: [localhost] => (item=/usr/bin/rsh)
ok: [localhost] => (item=/usr/libexec/openssh/ssh-keysign)
changed: [localhost] => (item=/usr/lib/openssh/ssh-keysign)
ok: [localhost] => (item=/sbin/netreport)
ok: [localhost] => (item=/usr/sbin/usernetctl)
ok: [localhost] => (item=/usr/sbin/userisdnctl)
ok: [localhost] => (item=/usr/sbin/pppd)
ok: [localhost] => (item=/usr/bin/lockfile)
ok: [localhost] => (item=/usr/bin/mail-lock)
ok: [localhost] => (item=/usr/bin/mail-unlock)
ok: [localhost] => (item=/usr/bin/mail-touchlock)
ok: [localhost] => (item=/usr/bin/dotlockfile)
ok: [localhost] => (item=/usr/bin/arping)
ok: [localhost] => (item=/usr/sbin/uuidd)
ok: [localhost] => (item=/usr/bin/mtr)
ok: [localhost] => (item=/usr/lib/evolution/camel-lock-helper-1.2)
ok: [localhost] => (item=/usr/lib/pt_chown)
changed: [localhost] => (item=/usr/lib/eject/dmcrypt-get-device)
ok: [localhost] => (item=/usr/lib/mc/cons.saver)
```

Here are a few services that are available

Fully loaded ready to go applications

GitLab | GitLabCI | Etherpad | DokuWiki | ownCloud | phpIPAM | Mailman

Databases

PostgreSQL | MariaDB | Redis | Memcached | Elasticsearch

Programming languages

Ruby | Golang | Java | NodeJS | PHP

Web application deployment

nginx | Apache | RubyOnRails

Service monitoring and logging

LibreNMS | monit | rsyslog

Networking

dnsmasq | DHCP | Radvd | ferm | postfix | SMS | SSH | NFS | Samba | Tinc

Virtualization

LXC | Docker | libvirt

Backup and encryption

Safekeep | BoxBackup | encFS | cryptsetup | SKS | Monkeysphere

Security

PKI | dhparam | slapd