Jacob Brown

cloud mx crew llc | jacksonville, fl

Locked LAMP

cloud mx crew llc

Jacksonville, fl

**Table of Contents**

[**Project Overview** 2](#_Toc78545365)

[**Project Goals & Objectives (Benefits)** 3](#_Toc78545366)

[**Network Infrastructure Requirement** 4](#_Toc78545367)

[**Assumptions & Risks** 4](#_Toc78545368)

[**Work Breakdown Structure (WBS)** 5](#_Toc78545369)

[**Network Topology Diagram with IP Addresses** 9](#_Toc78545370)

[**Appendices** 9](#_Toc78545371)

[**Gantt Chart** 9](#_Toc78545372)

[**Ansible Script** 10](#_Toc78545373)

[**DISA STIGs** 22](#_Toc78545374)

**Scope of Work**

**Project Title**

Locked Linux, Apache, MySQL, PHP (LAMP)

# **Project Overview**

The purpose of this project is to automate the pre-deployment of Rapid Digital Marketing LLC.’s (Rapid-DM) promotional marketing content to the internet. Rapid-DM focuses on one-time, limited-time flash sales and only while supplies last type marketing strategies. This project enhances the Command and Control Web Script project completed in June of this year. Project Locked LAMP will enable security and consistency with droplet creations for high-traffic regions, allowing Rapid-DM to add clients to existing droplets. The Content Management System (CMS) application Ansible will serve as the scripting and automation tool used for deploying multiple web servers into multilabel regions. Ansible will create pre-configured secured servers for Rapid-DM to deploy content from their GitHub repositories. The Ansible script will procure two (2) Digital Ocean servers, called droplets, and configure both droplets with twenty (20) Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIGS). The Ansible script will automate the two (2) deployments using only the Application Programming Interface (API) token and no secondary input for completion.

The project completion date is August 1, 2021, with four (4) milestones. Milestone 1 consists of Researching Digital Ocean and Ansible modules, Creating the CentOS 8 Virtual Machine (VM) for the Ansible automation tool, and creating a basic Ansible Playbook for connection to Digital Ocean. Milestone 2 consists of creating a Playbook to update the Operational System (OS) and configure twenty-one (21) DISA STIGs, the LAMP stack, and firewall ports. Milestone 3 consists of finalizing and validating the Ansible script for full functionality, Prevising from nothing but the API Token to two (2) full functional LAMP stacks with DISA STIGs. Finally, milestone 4 is the validation of the project with Rapid-DM for reliability and functionality of the Ansible script and desired project outcome.

Milestone completion dates:

Milestone I – July 4, 2021

Milestone II – July 18, 2021

Milestone III – July 25, 2021

Milestone IV – August 1, 2021

# **Project Goals & Objectives (Benefits)**

Upon completion of this project, Rapid-DM should benefit from the following:

* **Administration** - By using an API access token that can be created and used for each client project. Easy to build stand-alone servers, without extensive startup needs of resource groups, separate security groups, and internal virtual networks to maintain.
* **Security** - Login into Digital Ocean requires a username, password, and multifactor authentication or an API token that can be revoked or created at any time. Logging into a droplet requires a registered Secure SHell (SSH) key. DISA STIGs provides OS hardening to droplets, making it harder for a malicious actor to steal data or deface websites.
* **Scalability** - Quick pre-deployment of new hardened droplets for Rapid-DM’s CI/CD process from their private GitHub repository. Adding servers to the same or new region can happen in minutes and not hours or days.
* **Reliability** - Digital Ocean boasts a 99.99% uptime placing Digital Ocean’s reliability with Azure, Amazon Web Services (AWS), and Google Cloud Services (GCS).
* **Automation** - With Ansible’s Immutable modules delivering the same results with multiple uses of the same script. Ansible creates the droplets and is the Content Management System (CMS) for the droplets. Make changes as a part of your CI/CD rerun the script for it to be updated.
* **Cost** - Basic server with 1 CPU, 1 GB RAM, 25 GB storage, and 1 TB transfer it’s $5 month at Digital Ocean, but it’s $85 to $100 a month for AWS, Google, and Azure. By hardening, the OS Rapid-DM can leave servers up to add multiple clients to each droplet.  
  Calculator: <https://www.digitalocean.com/pricing/calculator/>

# **Network Infrastructure Requirement**

Rapid-DM’s infrastructure requirements are as follows:

* Virtual Machine
  + Operating System - CentOS 8.2.2004-x86\_64-dvd1.iso
  + Processor - 2 cores
  + Memory - 2048 MB
  + Hard disk storage - 20 GB
  + Application - Ansible version 2.9.21
* Digital Ocean droplets
  + Operating System - CentOS 8.3-x86\_64
  + Processor - 1 core
  + Memory - 1 GB
  + Hard disk storage - 25 GB
  + Applications:
    - Apache - 2.4.37
    - MariaDB - 10.3.28
    - PHP version - 7.4.20

# **Assumptions & Risks**

The following assumptions are included as part of this project:

* Rapid-DM will have internet access and network bandwidth.
* Rapid-DM is responsible for the web content and its security.
* Rapid-DM will assume responsibility for testing and validation for project acceptance.
* Rapid-DM will maintain support for internal employees for help and questions with the new process.
* Rapid-DM will manage security and the updating of application dependencies as needed for continued use.
* Digital Ocean will provide the physical security and hardware updates and maintenance as a part of their Service Level Agreement (SLA) to Rapid-DM.

The following risks are included as part of this project:

* Rapid-DM will accept the role of implementation of organizational change as well as initial and ongoing training needs.
* Rapid-DM’s commitment and support for the go-live date.

# **Work Breakdown Structure (WBS)**

1. Locked LAMP
   1. Milestone 1 Start
      1. Research
         1. Digital Ocean
         2. Ansible Modules
         3. API Communications
         4. DISA STIGs
         5. Phase Complete
      2. Digital Ocean Account
         1. Create Account
         2. Create API Token
         3. Phase Complete
      3. CentOS Virtual Machine
         1. Download CentOS ISO file
         2. Create CentOS VM
            1. Static IP Address
            2. Create Client Folder
            3. Create an SSH key
            4. Sub-Phase Complete
         3. Ansible
            1. Update CentOS
            2. Install EPEL-release
            3. Install Ansible
            4. Create Ansible Host File
            5. Modify Ansible Configuration File
            6. Create Ansible Vault

Secure API Token

Secure SSH Key

Sub-Tasks Complete

* + - * 1. Sub-Phase Complete
      1. Phase Complete
    1. Project Administration
       1. Status Report Upload
       2. Time Sheet Upload
       3. Create Work Breakdown Structure Upload
       4. Phase Complete
    2. Milestone 1 Complete
  1. Milestone 2 Start
     1. Communicate with Digital Ocean
        1. Create Basic Ansible Playbook
        2. Upload SSH Keys
        3. Create Droplet
        4. Add Droplet Public IP Address to Memory
        5. Phase Complete
     2. DISA STIGs Playbook
        1. Update and Upgrade OS
        2. Install Packages
           1. Install EPEL RPM
           2. Install REMI RPM
           3. Install PHP 7.4
           4. Install MariaDB 10.3
           5. Install Apache 2.4
           6. Install php-mysqlnd
           7. Install php-fpm
           8. Install git
           9. Install Firewalld
           10. Install pymysql with pip
           11. Sub-Phase Complete
        3. MariaDB
           1. Start MariaDB Service
           2. Create Root Password
           3. Remove Anonymous DB Users
           4. Remove Test Databases
           5. Sub-Phase Complete
        4. Configure Firewall Ports
           1. Start Firewall Service
           2. Open Port 80 for HTTP
           3. Open Port 22 for SSH
           4. Sub-Phase Complete
        5. Apache
           1. Start Apache
           2. Sub-Phase Complete
        6. Configure Cat 1 STIGs
           1. Enforce Local Packages Certificate Signature - ID: V-230265
           2. Remove All “shosts.equiv” files - ID: V-230283
           3. Remove All “.shosts” files - ID: V-230284
           4. Remove Telnet-Server Packages - ID: V-230487
           5. Remove RSH-Server Package - ID: V-230492
           6. Block “ctrl-alt-del” Reboot - ID: V-230529
           7. Block “ctrl-alt-del” Burst Reboot - ID: V-230531
           8. Remove TFTP server - ID: V-230533
           9. Remove FTP server - ID: V-230558
           10. Sub-Phase Complete
        7. Configure Cat 2 STIGs
           1. Install rsyslog Remote System Log - ID: V-230228
           2. Encrypt All Stored Passwords - ID: V-230231
           3. Valid Root Authentication for Rescue/Emergency Mode - ID: V-230236
           4. Enable and Enforce Secure Enhanced Linux (SELinux) - ID: V-230240
           5. SSH Connection Timeout - ID: V-230244
           6. Force The Use of TLSv1.2 - ID: V-230255
           7. Change System Commands Permissions - ID: V-230257
           8. Change System Commands Owner - ID: V-230258
           9. Change System Commands Group - ID: V-230259
           10. Change Library File Permissions - ID: V-230260
           11. Change Library File Owner - ID: V-230261
           12. Change Library File Group - ID: V-230262
           13. Sub-Phase Complete
        8. Phase Complete
     3. Project Administration
        1. Status Report Upload
        2. Time Sheet Upload
        3. Prep Gantt Chart Upload
        4. Ansible Script Upload
        5. Phase Complete
     4. Milestone 2 Complete
  2. Milestone 3 Start
     1. Validation
        1. Validate Security Integrity
        2. Validate Ansible Playbook
        3. Phase Complete
     2. Project Administration
        1. Status Report Upload
        2. Time Sheet Upload
        3. Prep Training
        4. Prep Presentation
        5. Prep Project Report
        6. Finalize Gantt Chart
        7. Phase Complete
     3. Milestone 3 Complete
  3. Milestone 4 Start
     1. Finalize Project with Client
        1. Project Presentation
        2. Project Report
        3. Ansible Playbook and Files
        4. Client Acceptance
        5. Provide Training
        6. Phase Complete
     2. Project Administration
        1. Status Report Upload
        2. Time Sheet Upload
        3. Phase Complete
     3. Milestone 4 Complete

# **Network Topology Diagram with IP Addresses**

Diagram

Description automatically generated

# **Appendices**

## **Gantt Chart**

See Attachment: GanntChart.gan.zip

## **Ansible Script**

---

#####################################################

# This playbook is designed for: #

# Host: CentOS-8 #

# Ansible Version: 2.9.23 #

# Playbook with Vault Command: #

# ansible-playbook Locked\_LAMP.yml --ask-vault-pass #

#####################################################

- hosts: digitalocean

gather\_facts: false

vars:

do\_token: "{{ lookup('file', '~/DO\_Token.txt') }}"

ssh\_key\_name: Jacob-Brown-2107

my\_ssh\_key: "{{ lookup('file', '~/.ssh/id\_rsa.pub') }}"

tag\_name:

- Client\_Name

- Client\_Ref\_Num

droplet\_name:

- BrownJ-2107-STIG1

- BrownJ-2107-STIG2

## 1.2. Milestone 2 Start

tasks:

- name: |

Task - 1.2.1.2

Upload SSH Key

digital\_ocean\_sshkey:

oauth\_token: "{{ do\_token }}"

name: "{{ ssh\_key\_name }}"

ssh\_pub\_key: "{{ my\_ssh\_key }}"

state: present

register: mysshkey

- name: |

Task - 1.2.1.3

Create Two DO Droplets

digital\_ocean\_droplet:

state: present

name: "{{ item }}"

oauth\_token: "{{ do\_token }}"

size: s-1vcpu-1gb

region: nyc1

unique\_name: yes

image: centos-8-x64

tags: "{{ tag\_name }}"

ssh\_keys: ["{{ mysshkey.data.ssh\_key.id }}"]

with\_items: "{{ droplet\_name }}"

register: droplet\_details

- name: |

Task - 1.2.1.4.

Add The Droplets' Public IP Addresses to Memory

add\_host:

name: "{{ item.data.ip\_address }}"

groups: droplets

with\_items: ["{{ droplet\_details.results }}"]

- hosts: droplets

remote\_user: root

gather\_facts: false

vars:

db\_pswd: Fullsail11!!

mysql\_root\_password: Fullsail11!!

vaulted\_raw\_password: Fullsail11!!

ssh\_passphrase: Fullsail11!!

tasks:

- name: Wait for Port 22 to Become Available

wait\_for:

host: "{{ inventory\_hostname }}"

port: 22

delegate\_to: localhost

## 1.2.2. DISA STIGs Playbook

- name: |

Task - 1.2.2.1.

Update and Upgrade OS

dnf:

name: "\*"

state: latest

## 1.2.2.2. Install Packages

######### These 3 steps are needed for PHP 7.4 not available in EPEL

- name: |

Task - 1.2.2.2.1.

Install EPEL RPM

command: dnf install -y https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm

- name: |

Tast - 1.2.2.2.2.

Install REMI RPM

command: dnf install -y https://rpms.remirepo.net/enterprise/remi-release-8.rpm

- name: |

Task - 1.2.2.2.3.

Install PHP 7.4 from REMI

command: dnf module install -y php:remi-7.4

######### Remove previous 3 steps when PHP 7.4 is available in EPEL

- name: |

Tasks - 1.2.2.2.5. - 1.2.2.2.9.

Installing LAMP Stack

dnf:

name:

- epel-release

- firewalld

- httpd

- mariadb-server

- mariadb

# - php #Use this when EPEL repo is updated with version 7.4 or higher

- php-mysqlnd

- php-fpm

- python2

- python3

- tar

- curl

- git

update\_cache: yes

state: latest

- name: |

Task - 1.2.2.2.10.

Install PyMySQL With PIP

become: true

pip:

name: pymysql

state: present

## Task - 1.2.2.3. MariaDB

- name: |

Task - 1.2.2.3.1

Start MariaDB and Enable it on Boot

service:

name: mariadb

state: started

enabled: yes

- name: |

Task - 1.2.2.3.2.

Create MariaDB Root Password

mysql\_user:

login\_host: localhost

login\_user: root

login\_password: ''

name: root

password: "{{ mysql\_root\_password }}"

state: present

ignore\_errors: yes

- name: |

Task - 1.2.2.3.3.

Remove Anonymous DB Users

mysql\_user:

login\_host: localhost

login\_user: root

login\_password: "{{ mysql\_root\_password }}"

name: ""

host: localhost

state: absent

no\_log: true

- name: |

Task - 1.2.2.3.4.

Remove Test Databases

mysql\_db:

login\_host: localhost

login\_user: root

login\_password: "{{ mysql\_root\_password }}"

name: test

state: absent

no\_log: true

## Task - 1.2.2.4. Configure Firewall Ports

- name: |

Task - 1.2.2.4.1.

Start Firewall and Enable it on Boot

service:

name: firewalld

state: started

enabled: yes

- name: |

Task - 1.2.2.4.2.

Open Port 80 for HTTP

firewalld:

zone: public

service: http

permanent: yes

state: enabled

- name: |

Task - 1.2.2.4.3.

Open Port 22 for SSH

firewalld:

zone: public

service: ssh

permanent: yes

state: enabled

## 1.2.2.5. Apache

- name: |

Task - 1.2.2.5.1.

Start Apache and Enable it on Boot.

service:

name: httpd

state: started

enabled: yes

## 1.2.2.6. Configure Cat 1 STIGs

- name: |

Task - 1.2.2.6.1.

Enforce Local Packages Certificate Signature - ID V-230265

lineinfile:

path: /etc/dnf/dnf.conf

regexp: '^gpgcheck='

line: 'gpgcheck=1'

state: present

- name: |

Task - 1.2.2.6.2. PART 1

Find All “shosts.equiv” files - ID V-230283

find:

path: "/"

recurse: yes

patterns: "shosts.equiv"

register: shosts

- name: |

Task - 1.2.2.6.2. PART 2

Remove All “shosts.equiv” files - ID V-230283

file:

path: "{{ item.path }}"

state: absent

with\_items: "{{ shosts.files }}"

- name: |

Task - 1.2.2.6.3. PART 1

Find All “.shosts” files - ID V-230284

find:

path: "/"

recurse: yes

patterns: "\*.shosts"

register: anyshosts

- name: |

Task - 1.2.2.6.3. PART 2

Remove All “.shosts” files - ID V-230284

file:

path: "{{ item.path }}"

state: absent

with\_items: "{{ anyshosts.files }}"

- name: |

Task - 1.2.2.6.4.

Remove Telnet-Server Packages - ID V-230487

dnf:

name: telnet-server

state: absent

- name: |

Task - 1.2.2.6.5.

Remove RSH-Server Package - ID V-230492

dnf:

name: rsh-server

state: absent

- name: |

Task - 1.2.2.6.6.

Mask “ctrl-alt-del” Reboot - ID V-230529

systemd:

name: ctrl-alt-del.target

masked: yes

- name: |

Task - 1.2.2.6.7.

Block “ctrl-alt-del” Burst Reboot - ID V-230531

lineinfile:

path: /etc/systemd/system.conf

regexp: '^CtrlAltDelBurstAction'

line: 'CtrlAltDelBurstAction=none'

state: present

- name: |

Task - 1.2.2.6.8.

Remove TFTP server - ID V-230533

dnf:

name: tftp-server

state: absent

- name: |

Task - 1.2.2.6.9.

Remove FTP server - ID V-230558

dnf:

name: vsftpd

state: absent

## 1.2.2.7. Configure Cat 2 STIGs

- name: |

Task - 1.2.2.7.1. PART 1

Install rsyslog Remote System Log - ID V-230228

dnf:

name: rsyslog

state: latest

- name: |

Task - 1.2.2.7.1. PART 2

Configure rsyslog Remote System Log - ID V-230228

lineinfile:

path: /etc/rsyslog.conf

regexp: '^authpriv.\*'

line: 'auth.\*;authpriv.\*;daemon.\* /var/log/secure'

state: present

- name: |

Task - 1.2.2.7.2.

Encrypt All Stored Passwords - ID V-230231

lineinfile:

path: /etc/login.defs

regexp: '^ENCRYPT\_METHOD'

line: 'ENCRYPT\_METHOD SHA512'

state: present

- name: |

Task - 1.2.2.7.3.

Valid Root Authentication for Rescue/Emergency Mode - ID V-230236

lineinfile:

path: /usr/lib/systemd/system/rescue.service

regexp: '^ExecStart'

line: 'ExecStart=-/usr/lib/systemd/systemd-sulogin-shell rescue'

state: present

- name: |

Task - 1.2.2.7.4.

Enable and Enforce Secure Enhanced Linux (SELinux) - ID V-230240

command: chcon -t httpd\_sys\_rw\_content\_t /var/www/html -R

- name: |

Task - 1.2.2.7.5. PART 1

SSH Connection Interval - ID V-230244

lineinfile:

path: /etc/ssh/sshd\_config

regexp: '^#ClientAliveInterval'

line: 'ClientAliveInterval 600'

state: present

- name: |

Task - 1.2.2.7.5. PART 2

SSH Connection Max - ID V-230244

lineinfile:

path: /etc/ssh/sshd\_config

regexp: '^#ClientAliveCountMax'

line: 'ClientAliveCountMax 0'

state: present

- name: |

Task - 1.2.2.7.6.

Force The Use of TLSv1.2 - ID V-230255

lineinfile:

path: /etc/crypto-policies/back-ends/opensslcnf.config

regexp: '^MinProtocol = TLSv1.2'

line: 'MinProtocol = TLSv1.2'

state: present

- name: |

Tasks - 1.2.2.7.7. - 1.2.2.7.9.

Change System Directory/File Command Permissions, Owner, and Group

ID V-230257 - ID: V-230258 - ID: V-230259

file:

path: "{{ item }}"

owner: root

group: root

mode: 0755

state: directory

recurse: yes

with\_items:

- /bin

- /sbin

- /usr/bin

- /usr/sbin

- /usr/local/bin

- /usr/local/sbin

- name: |

Task - 1.2.2.7.10. - 1.2.2.7.12.

Change Library Directory/File Permissions, Owner, and Group

ID: V-230260 - ID: V-230261 - ID: V-230262

file:

path: "{{ item }}"

owner: root

group: root

mode: 0755

state: directory

recurse: yes

with\_items:

- /lib

- /lib64

- /usr/lib

- /usr/lib64

- name: Reboot Droplet for Configuration Changes

reboot:

reboot\_timeout: 600

...

## **DISA STIGs**

|  |  |  |  |
| --- | --- | --- | --- |
| **Cat 1 High Vulnerability** | | | |
| **Task #** | **Activity** | **Vulnerability ID** | **Description** |
| 1.2.2.6.1. | Enforce Local Packages Certificate Signature | ID: V-230265 | Checks the locally installed packages certificates for validity before using. |
| 1.2.2.6.2. | Remove All “shosts.equiv” files | ID: V-230283 | The “shosts.equiv” is used for SSH authentication but does not require interactive identification and authentication of a connection request. Two parts in script find and remove. |
| 1.2.2.6.3. | Remove All “.shosts” files | ID: V-230284 | The “.shosts” is also used for SSH authentication but does not require interactive identification and authentication of a connection request. Two parts in script find and remove. |
| 1.2.2.6.4. | Remove Telnet-Server Packages | ID: V-230487 | Not installed by default; however, it could be added to the base image by a cloud provider. |
| 1.2.2.6.5. | Remove RSH-Server Package | ID: V-230492 | Not installed by default; however, it could be added to the base image by a cloud provider. |
| 1.2.2.6.6. | Block “ctrl-alt-del” Reboot | ID: V-230529 | From the Command Line Interface (CLI), you can reboot a server using “ctrl-alt-del” and then access safe mode with administrator access. |
| 1.2.2.6.7. | Block “ctrl-alt-del” Burst Reboot | ID: V-230531 | From the CLI, you can reboot a server using “ctrl-alt-del” seven times in two seconds and then access safe mode with administrator access. |
| 1.2.2.6.8. | Remove TFTP server | ID: V-230533 | The Trivial File Transfer Protocol (TFTP) can transmit files to and from a remote server; however, there are no login or access control measures. |
| 1.2.2.6.9. | Remove FTP server | ID: V-230558 | The File Transfer Protocol (FTP) is used to transmit files to and from remote servers. It does have a username and password for authentication; however, it transmits all data without encryption. |
| **Cat 2 Medium Vulnerability** | | | |
| **Task #** | **Activity** | **Vulnerability ID** | **Description** |
| 1.2.2.7.1. | Install rsyslog Remote System Log | ID: V-230228 | This remote system log logs the security events and can be configured to send the security and system logs to a remote server. |
| 1.2.2.7.2. | Encrypt All Stored Passwords | ID: V-230231 | Ensures all passwords are encrypted with SHA512. |
| 1.2.2.7.3. | Valid Root Authentication for Rescue/Emergency Mode | ID: V-230236 | Request authentication for accessing the safe or recovery mode. |
| 1.2.2.7.4. | Enable and Enforce Secure Enhanced Linux (SELinux) | ID: V-230240 | SELinux isolates permissions for a process. Here we allowed Apache to edit all the subdirectories in the /var/www/html and serve web content. |
| 1.2.2.7.5. | SSH Connection Timeout | ID: V-230244 | We programmed to terminate the SSH connection after 10 minutes and only one connection to the server at a time. |
| 1.2.2.7.6. | Force The Use of TLSv1.2 | ID: V-230255 | The encryption most trusted is the Transport Layer Security (TLS) version 1.2 or higher. All previous encryption versions have been deemed insecure. |
| 1.2.2.7.7. | Change System Commands Permissions | ID: V-230257 | This blocks the ability of groups and other users to modify the system commands. Root only edit. |
| 1.2.2.7.8. | Change System Commands Owner | ID: V-230258 | Changes system command owner to root. |
| 1.2.2.7.9. | Change System Commands Group | ID: V-230259 | Changes system command group to root. |
| 1.2.2.7.10. | Change Library File Permissions | ID: V-230260 | This blocks the ability of groups and other users from modifying the system library. Root only edit. |
| 1.2.2.7.11. | Change Library File Owner | ID: V-230261 | Changes library file owner to root. |
| 1.2.2.7.12. | Change Library File Group | ID: V-230262 | Changes library file group to root. |