وَقُل رَّبِّ زِدْنِي عِلْمًا

Full Enterprise Linux Environment Deployment for Company

Supervised by ENG: Sondos Alsafy

System Administrator Track

Made by ENG: Mahmoud Hamed

Project Introduction

This project demonstrates how to deploy and configure a secure, organized, and automated Linux server environment for a mid-sized company.

I utilized **Bash scripting** throughout each phase to automate tasks such as user creation, permission setup, storage provisioning, and security hardening, thereby making the setup faster, repeatable, and reliable.

🛠️ The setup includes:

- 👥 Group-based access and user management
- 🗂️ File system permissions and ACLs
- 💽 LVM storage with disk quotas
- ⚙️ Automation using shell scripts, cron, and at
- 🌐 Web server configuration (Apache)
- 🔐 Security hardening using sudo rules, SSH keys, SELinux, and firewalld

The project is split into **7 logical phases** to simulate real-world system admin tasks.

👨‍💻 Phase 1: System Preparation & User Environment

- 🖥️ Change hostname : (intranet.technova.local)

🌐 Assign static IP : (192.168.153.10/24)

- 👥 Create groups: (dev_team, hr_team, it_team, sales_team)
- 👨‍💼 Add users and assign them to groups
- 🐚 Set default shell to /bin/bash & assign secure passwords
- 🔑 Force password change on first login

Change hostname && Assign static IP

```
[root@intranet ~]# hostname
intranet.technova.local
[root@intranet ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qle
n 1000
    link/ether 00:0c:29:66:11:1c brd ff:ff:ff:ff:ff:ff
    altname enp3s0
    inet 192.168.153.10/24 brd 192.168.153.255 scope global noprefixroute ens160
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe66:111c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
[root@intranet ~]#
```

Static ip for the server

👥 Create groups && 👨 Add users

```
[root@intranet ~]# tail -n 5 /etc/group
dev_team:x:1001:
hr_team:x:1002:
it_team:x:1003:
sales_team:x:1004:
apache:x:48:
[root@intranet ~]#
[root@intranet ~]# id alice bob carol dave erin frank
uid=1001(alice) gid=1001(dev_team) groups=1001(dev_team)
uid=1002(bob) gid=1002(hr_team) groups=1002(hr_team)
uid=1005(carol) gid=1003(it_team) groups=1003(it_team)
uid=1006(dave) gid=1004(sales_team) groups=1004(sales_team)
uid=1003(erin) gid=1001(dev_team) groups=1001(dev_team)
uid=1004(frank) gid=1003(it_team) groups=1003(it_team)
[root@intranet ~]#
[root@intranet ~]#
```

Creating groups to assign users to

Assigning users to their groups

🔑 Force password change on first login

```
[frank@intranet ~]$ su - dave
Password:
You are required to change your password immediately (administrator enforced).
Current password:
New password:
Retype new password:
[dave@intranet ~]$
[dave@intranet ~]$
[dave@intranet ~]$ su - erin
Password:
You are required to change your password immediately (administrator enforced).
Current password:
New password:
Retype new password:
[erin@intranet ~]$
[erin@intranet ~]$
```

Change Pass is required at the first login

Setting a new password

📁 Phase 2: Directory & Permission Setup

📂 Create shared folders in /srv/

👨‍🔧 Set ownership

🔒 Apply permissions: chmod 2770

📄 Use ACLs:

- 🛡️ frank: full access to all department folders
- 👀 bob: read-only access to /srv/sales

🗃️ Create /srv/public_temp with sticky bit

📁 Create folders && 👷 Set ownership && 🔒 Set Gid

```
[root@intranet ~]# ls -l /srv/
total 0
drwxrws---+ 2 root dev_team    6 Jun 24 15:44 dev
drwxrws---+ 2 root hr_team    35 Jun 24 15:44 hr
drwxrws---+ 2 root it_team     6 Jun 24 15:44 it
drwxrwxrwt. 2 root root        6 Jun 24 08:54 public_temp
drwxrws---+ 2 root sales_team 22 Jun 24 15:44 sales
[root@intranet ~]#
```

Set Gid 2770

Creating folders

Set ownership for each team to its folder

dev_team → dev

Use ACLs

```
[root@intranet ~]# getfacl /srv/dev/
getfacl: Removing leading '/' from absolute path names
# file: srv/dev/
# owner: root
# group: dev_team
# flags: -s-
user::rwx
user:frank:rwx
group::rwx
mask::rwx
other::---
```

```
[root@intranet ~]# getfacl /srv/hr
getfacl: Removing leading '/' from absolute path names
# file: srv/hr
# owner: root
# group: dev_team
# flags: -s-
user::rwx
user:frank:rwx
group::rwx
mask::rwx
other::---
```

```
[root@intranet ~]# getfacl /srv/it
getfacl: Removing leading '/' from absolute path names
# file: srv/it
# owner: root
# group: dev_team
# flags: -s-
user::rwx
user:frank:rwx
group::rwx
mask::rwx
other::---
```

```
[root@intranet ~]# getfacl /srv/sales
getfacl: Removing leading '/' from absolute path names
# file: srv/sales
# owner: root
# group: dev_team
# flags: -s-
user::rwx
user:bob:r-x
user:frank:rwx
group::rwx
mask::rwx
other::---
```

frank(IT Manger): Access to all folder

bob(HR auditing)

💽 Phase 3: Storage & LVM Setup

- 🧱 Use /dev/sda to create: PV → VG → 4 LVs
- 🪵 Mount each LV to /srv/DEPT
- 📄 Format with XFS and configure /etc/fstab
- 📏 Enable disk quotas on /srv/hr and /srv/sales

Use /dev/sda to create: PV → VG → 4 LVs

```
[root@intranet ~]# pvs
  PV             VG          Fmt  Attr PSize    PFree
  /dev/nvme0n1p2 rl          lvm2 a--   <99.00g
  /dev/sda       vg_deptdata lvm2 a--  <100.00g <96.5
[root@intranet ~]#
[root@intranet ~]# vgs
  VG          #PV #LV #SN Attr   VSize    VFree
  rl            1   3   0 wz--n-  <99.00g       0
  vg_deptdata   1   4   0 wz--n- <100.00g <96.51g
[root@intranet ~]#
[root@intranet ~]# lvs
  LV       VG          Attr       LSize   Pool Origin Data%  Meta%  Move Log Cpy%Sync Convert
  home     rl          -wi-ao---- <31.52g
  root     rl          -wi-ao----  64.55g
  swap     rl          -wi-ao----  <2.93g
  lv_dev   vg_deptdata -wi-ao----   1.00g
  lv_hr    vg_deptdata -wi-ao---- 500.00m
  lv_it    vg_deptdata -wi-ao----   1.00g
  lv_sales vg_deptdata -wi-ao----   1.00g
```

I make /dev/sda as my Physical Volume

The name of the Volume Group

The logical volumes I make from the vg

Mount each LV to /srv/Dept

```
[root@intranet ~]# df -hT
Filesystem                      Type      Size  Used Avail Use% Mounted on
devtmpfs                        devtmpfs  4.0M     0  4.0M   0% /dev
tmpfs                           tmpfs     1.8G     0  1.8G   0% /dev/shm
tmpfs                           tmpfs     725M  9.7M  715M   2% /run
/dev/mapper/rl-root             xfs        65G  5.2G   60G   9% /
/dev/nvme0n1p1                  xfs       960M  464M  497M  49% /boot
/dev/mapper/rl-home             xfs        32G  258M   32G   1% /home
/dev/mapper/vg_deptdata-lv_dev  xfs       960M   39M  922M   5% /srv/dev
/dev/mapper/vg_deptdata-lv_it   xfs       960M   39M  922M   5% /srv/it
/dev/mapper/vg_deptdata-lv_hr   xfs       436M   29M  408M   7% /srv/hr
/dev/mapper/vg_deptdata-lv_sales xfs      960M   39M  922M   5% /srv/sales
tmpfs                           tmpfs     363M   92K  363M   1% /run/user/0
[root@intranet ~]#
```

I mount each logical volume to its related /srv/dept name like:

/dev/vg_deptdata/lv_dev → /srv/dev

Format with XFS and configure /etc/fstab

```
# /etc/fstab
# Created by anaconda on Thu May  8 14:41:10 2025
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/rl-root     /                       xfs     defaults        0 0
UUID=fa512dd3-5be4-4fe0-9cbf-581ab67a644c /boot                   xfs     defaults        0 0
/dev/mapper/rl-home     /home                   xfs     defaults        0 0
/dev/mapper/rl-swap     none                    swap    defaults        0 0
/dev/vg_deptdata/lv_dev   /srv/dev   xfs   defaults                  0 0
/dev/vg_deptdata/lv_it    /srv/it    xfs   defaults                  0 0
/dev/vg_deptdata/lv_hr    /srv/hr    xfs   defaults,uquota           0 2
/dev/vg_deptdata/lv_sales /srv/sales xfs   defaults,uquota           0 2
                                                                    19,71
```

To ensure that the mounted LVs remain accessible after a reboot, add them to the /etc/fstab file.

Enable disk quotas on /srv/hr and /srv/sales

```
[root@intranet ~]# xfs_quota -x -c 'report -h' /srv/hr
User quota on /srv/hr (/dev/mapper/vg_deptdata-lv_hr)
                        Blocks
User ID       Used   Soft   Hard Warn/Grace
---------- --------------------------------
root            4K      0      0  00 [------]
bob             4K    100M   150M  00 [------]

[root@intranet ~]# xfs_quota -x -c 'report -h' /srv/sales
User quota on /srv/sales (/dev/mapper/vg_deptdata-lv_sales)
                        Blocks
User ID       Used   Soft   Hard Warn/Grace
---------- --------------------------------
root            0      0      0  00 [------]
dave            0    100M   150M  00 [------]

[root@intranet ~]#
```

Disk quotas were set for HR and Sales users using xfs_quota, with a 100 MB soft limit (temporary overuse allowed) and a 150 MB hard limit (strict maximum), to control disk space usage.

🔐 Phase 4: Security Hardening

- ⚙️ Sudo access for frank via /etc/sudoers.d/
- 🛡️ SSH Configuration:
  - 👥 Allow only it_team
  - ⛔ Disable root login
  - 🔑 Set up SSH key for frank
- 🔒 SELinux: enforce + allow Apache access
- 🌐 Open the firewall for:

  SSH (22), HTTP (80), ICMP (ping)

⚙️ Sudo access for frank via /etc/sudoers.d/

```
[root@intranet ~]# cat /etc/sudoers.d/frank
frank ALL=(ALL) NOPASSWD:/usr/sbin/useradd, /usr/sbin/userdel,/usr/sbin/usermod, /usr/bin/yum, /usr/bin/dnf
[root@intranet ~]#
[root@intranet ~]#
```

Sudo access was configured for frank to manage users and services, using a secure custom rule in /etc/sudoers.d/frank

👥 Allow only it_team && ⛔ Disable root login

```
[root@intranet ~]# tail -n 2 /etc/ssh/sshd_config
AllowGroups it_team
PermitRootLogin no
[root@intranet ~]#
[root@intranet ~]#
```

Allowing only the it_team to access SSH and disable root login

🔑 Set up SSH key for frank

```
[root@intranet ~]# ssh frank@192.168.153.10
Last login: Wed Jun 25 15:10:34 2025 from 192.168.153.10
[frank@intranet ~]$
[frank@intranet ~]$
[frank@intranet ~]$
```

User (frank) can access the server (SSH) without a password.

🔑 Firewall Configuration

```
[root@intranet ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: ens160
  sources:
  services: cockpit dhcpv6-client http ssh
  ports:
  protocols:
  forward: yes
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
[root@intranet ~]#
```

Permit services (ssh) && (http) && (ping)

🌐 Phase 5: Internal Web Portal

- 🧰 Install and enable Apache (httpd)
- 🖼️ Getting HTML page
- 🔗 Set correct SELinux context for web files
- ✅ Ensure accessible from browser at http://192.168.100.10

🧰 Install and enable Apache (httpd)

```
[root@intranet ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
     Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; preset: disabled)
     Active: active (running) since Wed 2025-06-25 08:46:56 EEST; 6h ago
       Docs: man:httpd.service(8)
   Main PID: 1163 (httpd)
     Status: "Total requests: 0; Idle/Busy workers
      Tasks: 177 (limit: 22782)
     Memory: 42.3M
        CPU: 17.217s
```

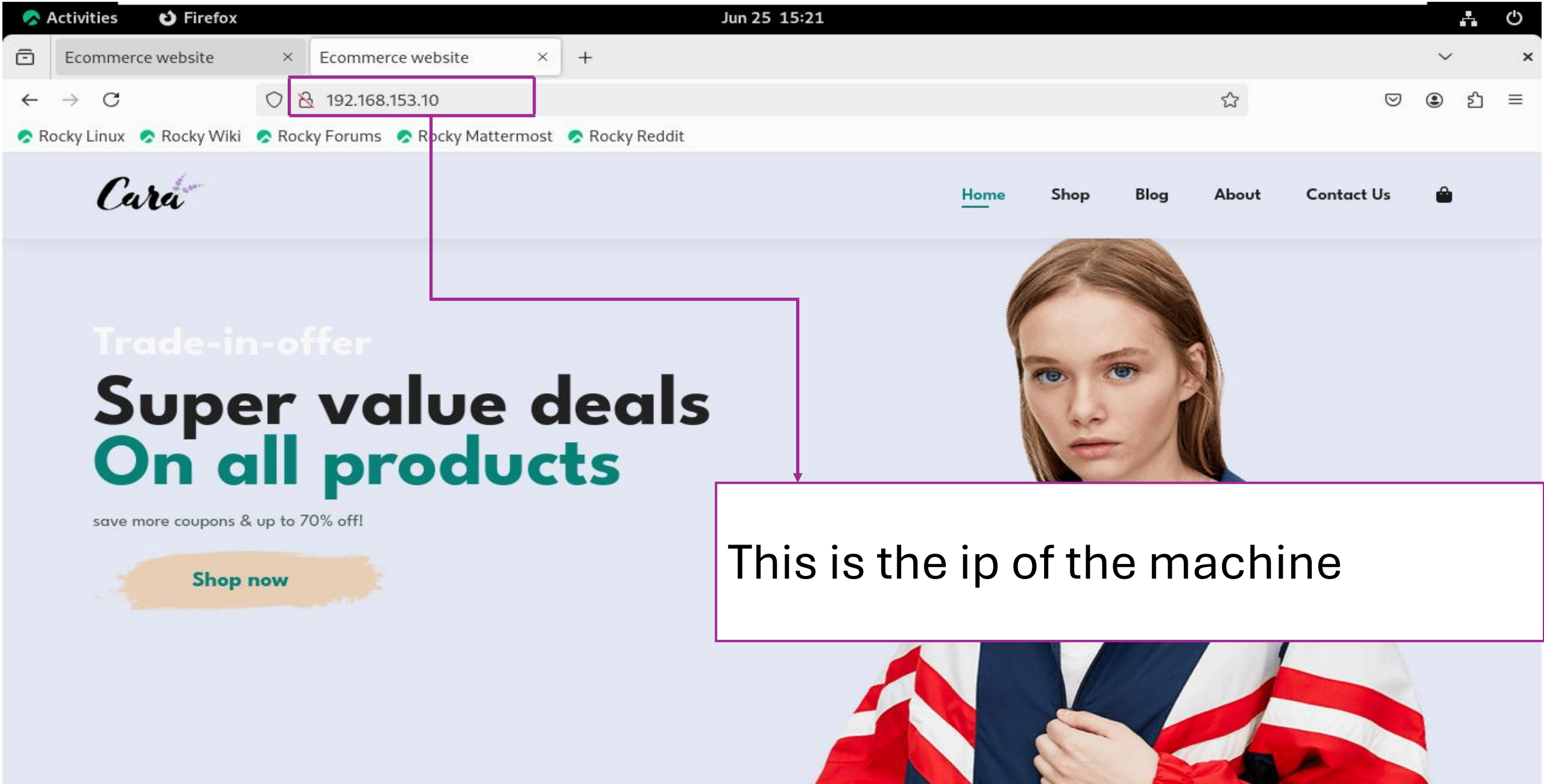
This means (httpd) is running, and with every reboot, it will run too

🔗 Set correct SELinux context for web files

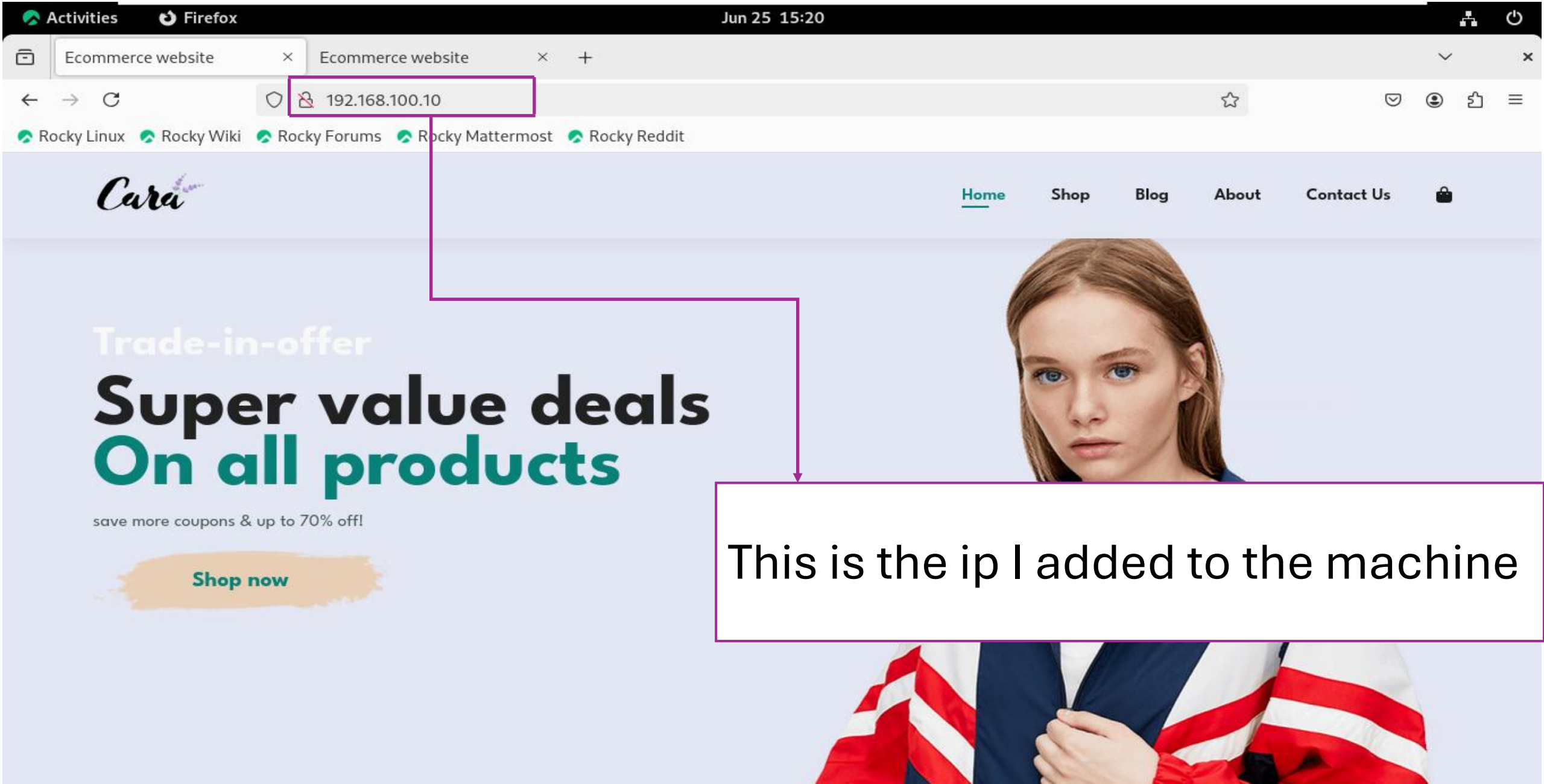
```
[root@intranet ~]# ls -lZ /var/www/html/website/
total 36
drwxr-xr-x. 9 root root unconfined_u:object_r:httpd_sys_content_t:s0   153 Jun 24 19:31 images
-rwxr-xr-x. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0 16193 Jun 24 19:40 index.html
-rwxr-xr-x. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0   417 Jun 24 19:40 README.md
-rwxr-xr-x. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0   160 Jun 24 19:40 script.js
-rwxr-xr-x. 1 root root unconfined_u:object_r:httpd_sys_content_t:s0  8422 Jun 24 19:40 style.css
[root@intranet ~]#
```

This is the SELinux type (context) required by httpd to access files

Getting HTML page



✅ Ensure accessible from browser at http://192.168.100.10



⚙️ Phase 6: Automation & Scripting

- 📜 Write backup script: /usr/local/bin/backup_dept.sh
- 🕐 Schedule daily with cron (1:00 AM)
- 🗒️ Log success/failure with logger
- 📢 Use at job to broadcast a message at 5 PM

Write backup script && Log success/failure with logger

root@intranet:~ — /usr/bin/vim /usr/local/bin/backup_dept.sh

```
#!/bin/bash
set -e
mkdir -p /backups
Today=$(date +%F)
for Dept in dev hr it sales; do
    Source="/srv/$Dept"
    Dest="/backups/${Dept}_${Today}.tar.gz"

    tar -czf "$Dest" "$Source" 2>/dev/null && \
    logger "Backup complete for $Dept" || \
    logger "Backup failed for $Dept"
done
~
```

The backup_script path

Using a logger to log the successful backup and the failed one

🕐 Schedule cron && 📢 Use at job

```
[root@intranet ~]# crontab -l
0 1 * * * /usr/local/bin/backup_dept.sh
[root@intranet ~]#
[root@intranet ~]#
[root@intranet ~]# atq
1       Wed Jun 25 17:00:00 2025 a root
[root@intranet ~]#
[root@intranet ~]#
[root@intranet ~]#
```

Cron job daily at 1:00 AM

```
[root@intranet ~]# at -c 1 | tail -n 3
wall "System maintenance will occur tonight at 1:00 AM. Save your work!!"


marcinDELIMITER75a613e1
[root@intranet ~]#
```

at job, to tell everyone to save their work at 17:00

🪛 Phase 7: Troubleshooting & Logs

- ❌ Introduce /etc/fstab error
- ✅ Recover using GRUB or single-user mode
- 🚫 Check SSH failures in /var/log/secure
- ✅ Backup success messages in /var/log/messages

❌ Introduce /etc/fstab error

```
/dev/mapper/rl-root     /                       xfs     defaults        0
UUID=fa512dd3-5be4-4fe0-9cbf-581ab67a644c /boot                   xfs
/dev/mapper/rl-home     /home                   xfs     defaults        0
/dev/mapper/rl-swap     none                    swap    defaults        0
/dev/vg_deptdata/lv_dev   /srv/dev    xfs    defaults                    0 0
/dev/vg_deptdata/lv_it    /srv/it     xfs    defaults                    0 0
/dev/vg_deptdata/lv_hr    /srv/hr     xfs    defaults,uquota             0 2
/de/vg_deptdata/lv_sales /srv/sales xfs    defaults,uquota             0 2
                                                                      19,3
```

Making syntax wrong in the /etc/fstab and reboot the machine

✅ Recover using GRUB or single-user mode

```
#
# /etc/fstab
# Created by anaconda on Thu May  8 14:41:10 2025
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/rl-root     /                       xfs     defaults        0 0
UUID=fa512dd3-5be4-4fe0-9cbf-581ab67a644c /boot                   xfs     defaults        0 0
/dev/mapper/rl-home     /home                   xfs     defaults        0 0
/dev/mapper/rl-swap     none                    swap    defaults        0 0
/dev/vg_deptdata/lv_dev   /srv/dev    xfs    defaults                    0 0
/dev/vg_deptdata/lv_it    /srv/it     xfs    defaults                    0 0
/dev/vg_deptdata/lv_hr    /srv/hr     xfs    defaults,uquota             0 2
/dev/vg_deptdata/lv_sales /srv/sales xfs    defaults,uquota             0 2
~
~
~
~
```

Correct the wrong to make the machine start successfully

Check SSH failures in /var/log/secure

```
[root@intranet ~]# ssh bob@192.168.153.10
bob@192.168.153.10's password:
Permission denied, please try again.
bob@192.168.153.10's password:
Permission denied, please try again.
bob@192.168.153.10's password:
bob@192.168.153.10: Permission denied (publickey,gssapi-keyex,gssapi-with-mic,password).
[root@intranet ~]#
```

The (it_team). Can only access the server with SSH. bob is not in

```
[root@intranet ~]# cat /var/log/secure | tail -n 2
Jun 25 15:38:21 intranet sshd[6640]: Connection closed by invalid user bob 192.168.153.10 port
54912 [preauth]
Jun 25 15:38:21 intranet sshd[6640]: PAM 2 more authentication failures; logname= uid=0 euid=0
tty=ssh ruser= rhost=192.168.153.10  user=bob
[root@intranet ~]#
```

The attempt to log in by bob had been reported

🎉 Thanks for Watching!

I hope you enjoyed this project demonstration and found it informative.

Your feedback is always welcome!