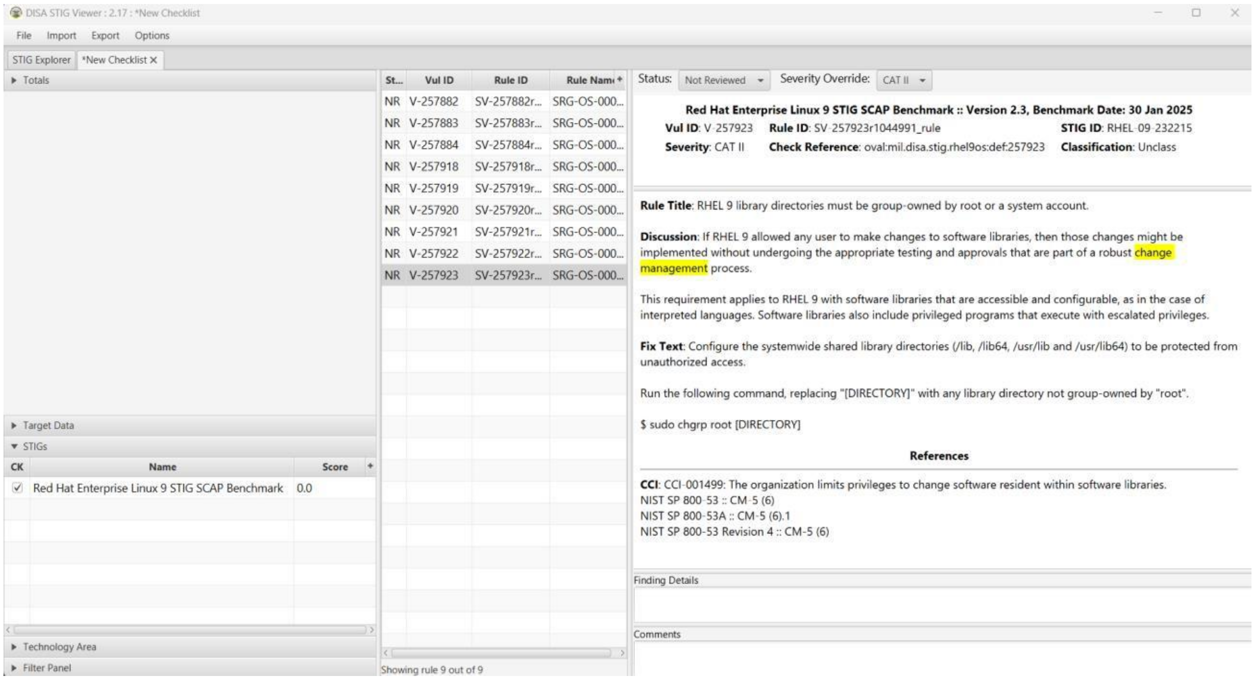
Unit 8 Lab - Configuration Drift and Remediation

Operational Activities



St...	Vul ID	Rule ID	Rule Nam
NR	V-257882	SV-257882r...	SRG-OS-000...
NR	V-257883	SV-257883r...	SRG-OS-000...
NR	V-257884	SV-257884r...	SRG-OS-000...
NR	V-257918	SV-257918r...	SRG-OS-000...
NR	V-257919	SV-257919r...	SRG-OS-000...
NR	V-257920	SV-257920r...	SRG-OS-000...
NR	V-257921	SV-257921r...	SRG-OS-000...
NR	V-257922	SV-257922r...	SRG-OS-000...
NR	V-257923	SV-257923r...	SRG-OS-000...

Showing rule 9 out of 9

CK	Name	Score
☑	Red Hat Enterprise Linux 9 STIG SCAP Benchmark	0.0

Status: Not Reviewed   Severity Override: CAT II

Red Hat Enterprise Linux 9 STIG SCAP Benchmark :: Version 2.3, Benchmark Date: 30 Jan 2025

Vul ID: V-257923   **Rule ID**: SV-257923r1044991_rule   **STIG ID**: RHEL-09-232215

Severity: CAT II   **Check Reference**: oval:mil.disa.stig.rhel9os:def:257923   **Classification**: Unclass

Rule Title: RHEL 9 library directories must be group-owned by root or a system account.

Discussion: If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Fix Text: Configure the systemwide shared library directories (/lib, /lib64, /usr/lib and /usr/lib64) to be protected from unauthorized access.

Run the following command, replacing "[DIRECTORY]" with any library directory not group-owned by "root".

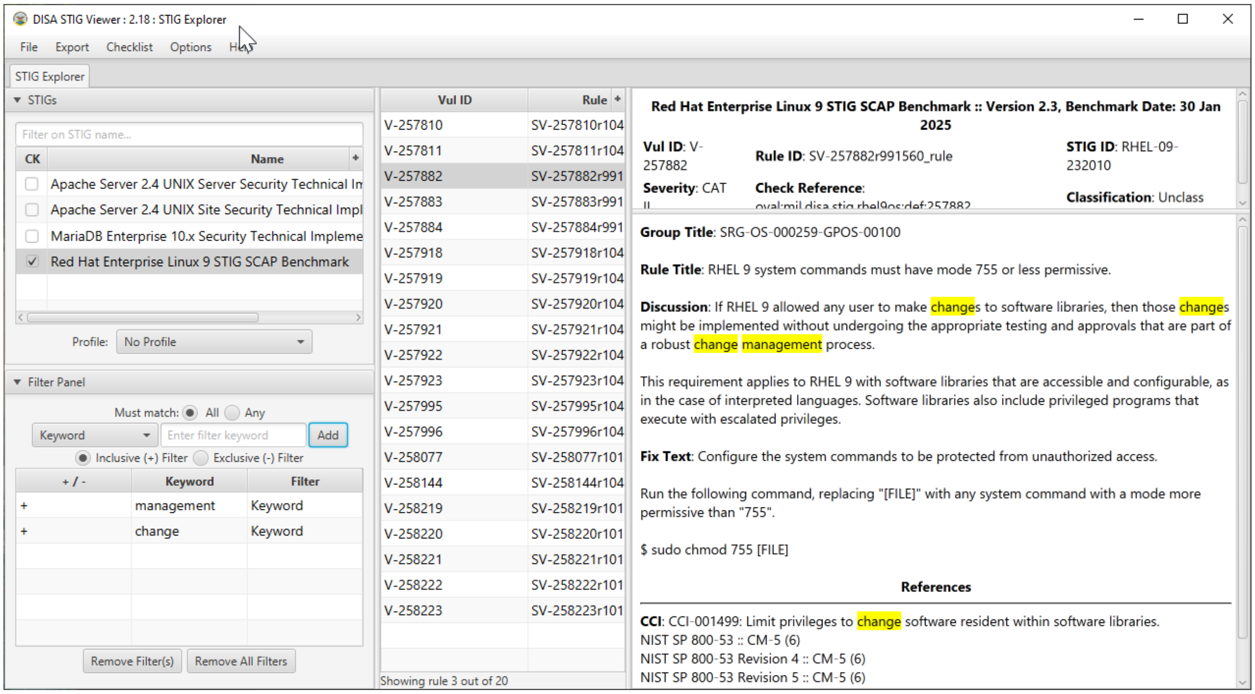
```
$ sudo chgrp root [DIRECTORY]
```

References

CCI: CCI-001499: The organization limits privileges to change software resident within software libraries.
NIST SP 800-53 :: CM-5 (6)
NIST SP 800-53A :: CM-5 (6).1
NIST SP 800-53 Revision 4 :: CM-5 (6)

Check your stig viewer and go to RHEL 9 stigs.

Set a filter for “change management”.



CK	Name
☐	Apache Server 2.4 UNIX Server Security Technical Im
☐	Apache Server 2.4 UNIX Site Security Technical Impl
☐	MariaDB Enterprise 10.x Security Technical Impleme
☑	Red Hat Enterprise Linux 9 STIG SCAP Benchmark

Profile: No Profile

Must match: ● All ○ Any

Keyword | Enter filter keyword | Add

● Inclusive (+) Filter ○ Exclusive (-) Filter

+ / -	Keyword	Filter
+	management	Keyword
+	change	Keyword

Vul ID	Rule
V-257810	SV-257810r104
V-257811	SV-257811r104
V-257882	SV-257882r991
V-257883	SV-257883r991
V-257884	SV-257884r991
V-257918	SV-257918r104
V-257919	SV-257919r104
V-257920	SV-257920r104
V-257921	SV-257921r104
V-257922	SV-257922r104
V-257923	SV-257923r104
V-257995	SV-257995r104
V-257996	SV-257996r104
V-258077	SV-258077r101
V-258144	SV-258144r104
V-258219	SV-258219r101
V-258220	SV-258220r101
V-258221	SV-258221r101
V-258222	SV-258222r101
V-258223	SV-258223r101

Showing rule 3 out of 20

Red Hat Enterprise Linux 9 STIG SCAP Benchmark :: Version 2.3, Benchmark Date: 30 Jan 2025

Vul ID: V-257882

Rule ID: SV-257882r991560_rule

STIG ID: RHEL-09-232010

Severity: CAT II

Check Reference: oval:mil.disa.stig.rhel9os:def:257882

Classification: Unclass

Group Title: SRG-OS-000259-GPOS-00100

Rule Title: RHEL 9 system commands must have mode 755 or less permissive.

Discussion: If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and configurable, as in the case of interpreted languages. Software libraries also include privileged programs that execute with escalated privileges.

Fix Text: Configure the system commands to be protected from unauthorized access.

Run the following command, replacing "[FILE]" with any system command with a mode more permissive than "755".

```
$ sudo chmod 755 [FILE]
```

References

CCI: CCI-001499: Limit privileges to change software resident within software libraries.
NIST SP 800-53 :: CM-5 (6)
NIST SP 800-53 Revision 4 :: CM-5 (6)
NIST SP 800-53 Revision 5 :: CM-5 (6)

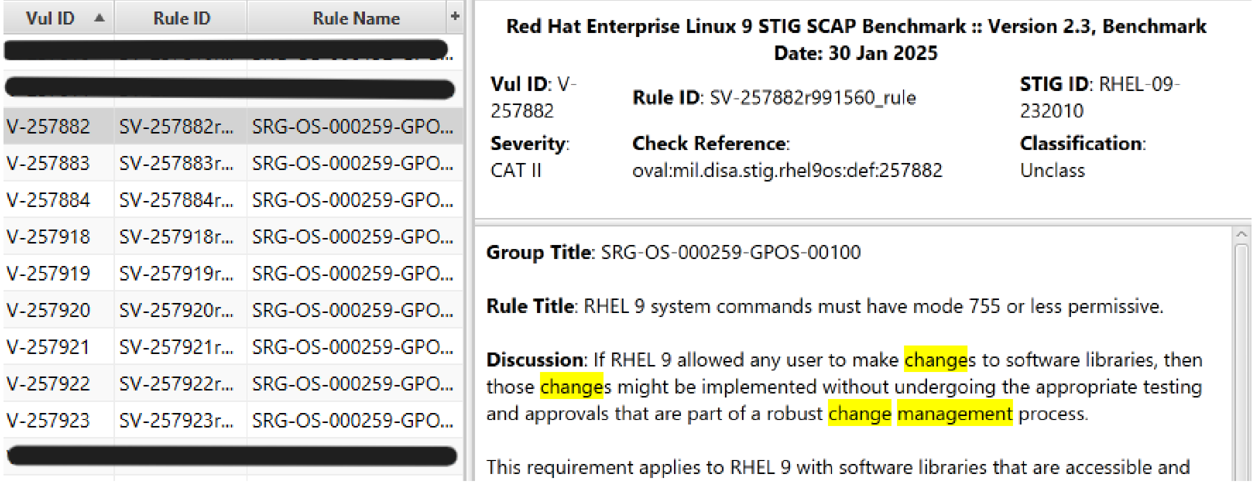
How many STIGs do you see?

The STIG VIEWER did not find anything using the two words together

-so I filtered for management , then for change

-this produced 20 STIGS

-nine (9) had the exact phrase "change management"



Vul ID ▲	Rule ID	Rule Name
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
V-257882	SV-257882r...	SRG-OS-000259-GPO...
V-257883	SV-257883r...	SRG-OS-000259-GPO...
V-257884	SV-257884r...	SRG-OS-000259-GPO...
V-257918	SV-257918r...	SRG-OS-000259-GPO...
V-257919	SV-257919r...	SRG-OS-000259-GPO...
V-257920	SV-257920r...	SRG-OS-000259-GPO...
V-257921	SV-257921r...	SRG-OS-000259-GPO...
V-257922	SV-257922r...	SRG-OS-000259-GPO...
V-257923	SV-257923r...	SRG-OS-000259-GPO...
[redacted]	[redacted]	[redacted]

Red Hat Enterprise Linux 9 STIG SCAP Benchmark :: Version 2.3, Benchmark Date: 30 Jan 2025

Vul ID: V-257882

Rule ID: SV-257882r991560_rule

STIG ID: RHEL-09-232010

Severity: CAT II

Check Reference: oval:mil.disa.stig.rhel9os:def:257882

Classification: Unclass

Group Title: SRG-OS-000259-GPOS-00100

Rule Title: RHEL 9 system commands must have mode 755 or less permissive.

Discussion: If RHEL 9 allowed any user to make changes to software libraries, then those changes might be implemented without undergoing the appropriate testing and approvals that are part of a robust change management process.

This requirement applies to RHEL 9 with software libraries that are accessible and

Review the wording, what is meant by a robust change management process?

To my understanding, using a tool such as ServiceNow ensures a robust process.

To explain it in my own words, was difficult at first glance, so I looked up the below online.

According to a blog

1. **Create templates for every change type**
2. **Document all details of the change**
3. **Define and assign tasks to the right people**
4. **Establish pre-defined approval policies**
5. **Communicate proactively with stakeholders and employees**
   a. **Set up a dedicated channel in your communication tool so that everyone is on the same page with the change implementation.**
6. **… change calendar …**
   a. **Maintain a change management calendar to schedule and track all change requests in one place.**
7. **Implement changes gradually and establish freeze periods**
8. **Prepare a contingency plan to roll back changes**
9. **Conduct post-change reviews**
   a. **In my experience – a client user / app support needs to perform checkouts after some changes**

Do you think this can be applied in just one STIG? Why or why not?

No in large organizations – many of these 9 require architecture/ engineering review in a large organization

Yes in small shops- but to avoid config drift these need to be part of the build stage for every machine.

What type of control is being implemented with change management in these STIGS?

Technical Preventative

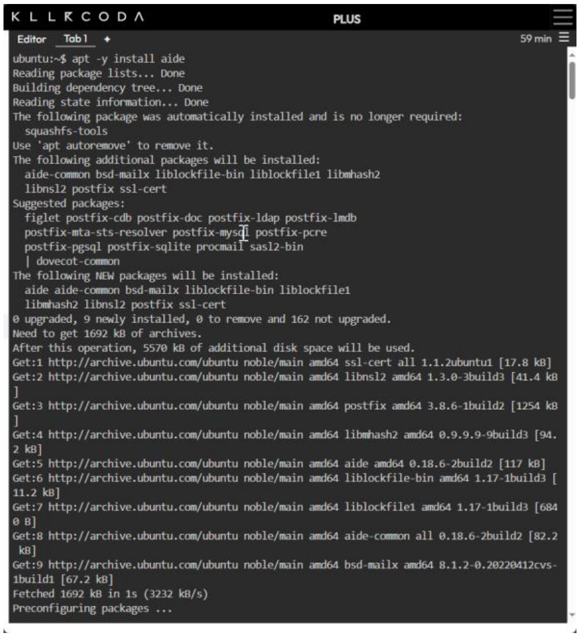
Is it different across the STIGs or all the same?

All the same - the either refer to file/group ownership or permissions

Monitoring configuration drift with Aide

Go into the sandbox lab: https://killercoda.com/playgrounds/scenario/ubuntu

Install aide and watch the installation happen.



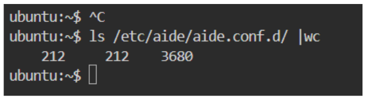
```
ubuntu:~$ apt -y install aide
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  squashfs-tools
Use 'apt autoremove' to remove it.
The following additional packages will be installed:
  aide-common bsd-mailx liblockfile-bin liblockfile1 libmhash2
  libnsl2 postfix ssl-cert
Suggested packages:
  figlet postfix-cdb postfix-doc postfix-ldap postfix-lmdb
  postfix-mta-sts-resolver postfix-mysql postfix-pcre
  postfix-pgsql postfix-sqlite procmail sasl2-bin
  | dovecot-common
The following NEW packages will be installed:
  aide aide-common bsd-mailx liblockfile-bin liblockfile1
  libmhash2 libnsl2 postfix ssl-cert
0 upgraded, 9 newly installed, 0 to remove and 162 not upgraded.
Need to get 1692 kB of archives.
After this operation, 5570 kB of additional disk space will be used.
Get:1 http://archive.ubuntu.com/ubuntu noble/main amd64 ssl-cert all 1.1.2ubuntu1 [17.8 kB]
Get:2 http://archive.ubuntu.com/ubuntu noble/main amd64 libnsl2 amd64 1.3.0-3build3 [41.4 kB
]
Get:3 http://archive.ubuntu.com/ubuntu noble/main amd64 postfix amd64 3.8.6-1build2 [1254 kB
]
Get:4 http://archive.ubuntu.com/ubuntu noble/main amd64 libmhash2 amd64 0.9.9.9-9build3 [94.
2 kB]
Get:5 http://archive.ubuntu.com/ubuntu noble/main amd64 aide amd64 0.18.6-2build2 [117 kB]
Get:6 http://archive.ubuntu.com/ubuntu noble/main amd64 liblockfile-bin amd64 1.17-1build3 [
11.2 kB]
Get:7 http://archive.ubuntu.com/ubuntu noble/main amd64 liblockfile1 amd64 1.17-1build3 [684
0 B]
Get:8 http://archive.ubuntu.com/ubuntu noble/main amd64 aide-common all 0.18.6-2build2 [82.2
 kB]
Get:9 http://archive.ubuntu.com/ubuntu noble/main amd64 bsd-mailx amd64 8.1.2-0.20220412cvs-
1build1 [67.2 kB]
Fetched 1692 kB in 1s (3232 kB/s)
Preconfiguring packages ...
```

apt -y install aide

What is being put in the path /etc/aide/aide.conf.d/?

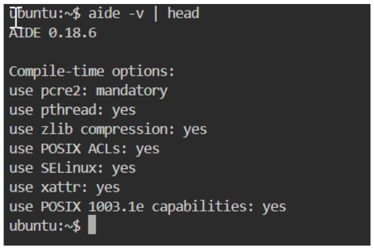
How many files are in there?

212



```
ubuntu:~$ ^C
ubuntu:~$ ls /etc/aide/aide.conf.d/ |wc
    212     212    3680
ubuntu:~$ 
```

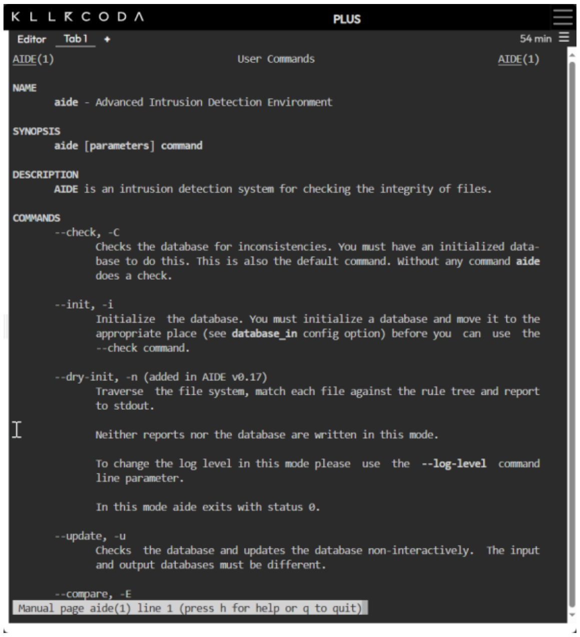
Check your version of aide



```
ubuntu:~$ aide -v | head
AIDE 0.18.6

Compile-time options:
use pcre2: mandatory
use pthread: yes
use zlib compression: yes
use POSIX ACLs: yes
use SELinux: yes
use xattr: yes
use POSIX 1003.1e capabilities: yes
ubuntu:~$
```

aide -v

Read the man page (first page).



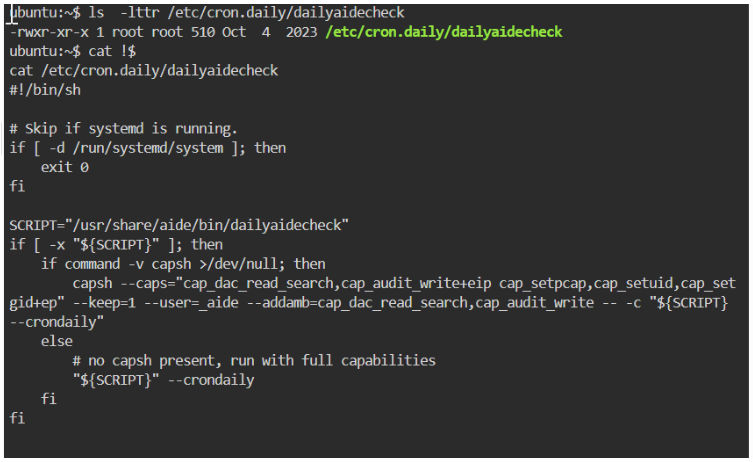
```
AIDE(1)                          User Commands                          AIDE(1)

NAME
       aide - Advanced Intrusion Detection Environment

SYNOPSIS
       aide [parameters] command

DESCRIPTION
       AIDE is an intrusion detection system for checking the integrity of files.

COMMANDS
       --check, -C
              Checks the database for inconsistencies. You must have an initialized data-
              base to do this. This is also the default command. Without any command aide
              does a check.

       --init, -i
              Initialize  the database. You must initialize a database and move it to the
              appropriate place (see database_in config option) before you  can  use  the
              --check command.

       --dry-init, -n (added in AIDE v0.17)
              Traverse  the file system, match each file against the rule tree and report
              to stdout.

              Neither reports nor the database are written in this mode.

              To change the log level in this mode please  use  the  --log-level  command
              line parameter.

              In this mode aide exits with status 0.

       --update, -u
              Checks  the database and updates the database non-interactively.  The input
              and output databases must be different.

       --compare, -E
 Manual page aide(1) line 1 (press h for help or q to quit)
```

man aide

What does aide try to do, and how does it do it?

AIDE is an IDS – intrusion detection system. It monitors all files for changes.

What is the configuration of cron found in /etc/cron.daily/dailyaidecheck?



```
ubuntu:~$ ls  -lttr /etc/cron.daily/dailyaidecheck
-rwxr-xr-x 1 root root 510 Oct  4  2023 /etc/cron.daily/dailyaidecheck
ubuntu:~$ cat !$
cat /etc/cron.daily/dailyaidecheck
#!/bin/sh

# Skip if systemd is running.
if [ -d /run/systemd/system ]; then
    exit 0
fi

SCRIPT="/usr/share/aide/bin/dailyaidecheck"
if [ -x "${SCRIPT}" ]; then
    if command -v capsh >/dev/null; then
        capsh --caps="cap_dac_read_search,cap_audit_write+eip cap_setpcap,cap_setuid,cap_set
gid+ep" --keep=1 --user=_aide --addamb=cap_dac_read_search,cap_audit_write -- -c "${SCRIPT}
--crondaily"
    else
        # no capsh present, run with full capabilities
        "${SCRIPT}" --crondaily
    fi
fi
```

What does this attempt to do?

It runs the dailyaidecheck

What checks are there before execution?

If capsh exists then it dailyaidecheck is run using capsh as a wrapper

If system is running then it quits.

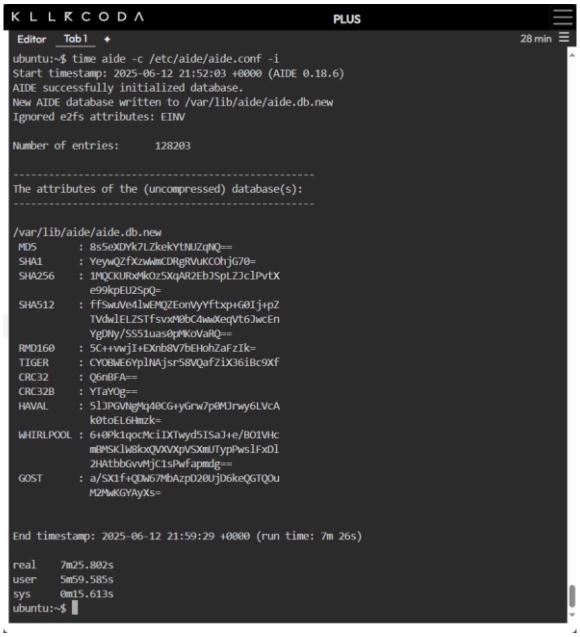
Read the man for capsh, what is it used for?

It is used for gathering extra information about a command by running it withing a sheel wrapper. It can also limit or expand the rights the command has while running.

Set up aide according to the default configuration style

How long did that take?

7.5 minutes



```
ubuntu:~$ time aide -c /etc/aide/aide.conf -i
Start timestamp: 2025-06-12 21:52:03 +0000 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new
Ignored e2fs attributes: EINV

Number of entries:      128203

---------------------------------------------------
The attributes of the (uncompressed) database(s):
---------------------------------------------------

/var/lib/aide/aide.db.new
 MD5       : 8s5eXDYk7LZkekYtNUZqNQ==
 SHA1      : YeywQZfXzwWmCDRgRVuKCOhjG70=
 SHA256    : 1MQCKURxMkOz5XqAR2EbJSpLZJclPvtX
             e99kpEU2SpQ=
 SHA512    : ffSwuVe4lwEMQZEonVyYftxp+G0Ij+pZ
             TVdwlELZSTfsvxM0bC4wwXeqVt6JwcEn
             YgDNy/SS51uas0pMKoVaRQ==
 RMD160    : 5C++vwjI+EXnb8V7bEHohZaFzIk=
 TIGER     : CYOBWE6YplNAjsr58VQafZiX36iBc9Xf
 CRC32     : Q6nBFA==
 CRC32B    : YTaYOg==
 HAVAL     : 5lJPGVNgMq40CG+yGrw7p0MJrwy6LVcA
             k0toEL6Hmzk=
 WHIRLPOOL : 6+0Pk1qocMciIXTwyd5ISaJ+e/BO1VHc
             mBMSKlW8kxQVXVXpVSXmUTypPwslFxDl
             2HAtbbGvvMjC1sPwfapmdg==
 GOST      : a/SX1f+QDW67MbAzpD20UjD6keQGTQOu
             M2MwKGYAyXs=


End timestamp: 2025-06-12 21:59:29 +0000 (run time: 7m 26s)

real    7m25.802s
user    5m59.585s
sys     0m15.613s
ubuntu:~$ 
```

How much time was wall clock v. system/user time?

real 7m25.802s

user 5m59.585s

sys 0m15.613s

Why might you want to know this on your systems?

What do you notice about the output?

It found 128k files to track.

It generated checksums to verify the status of the new database.

What do you need to go read about?

A lot –

1st based on the output I should learn more about these

2nd ....

Set the database up properly

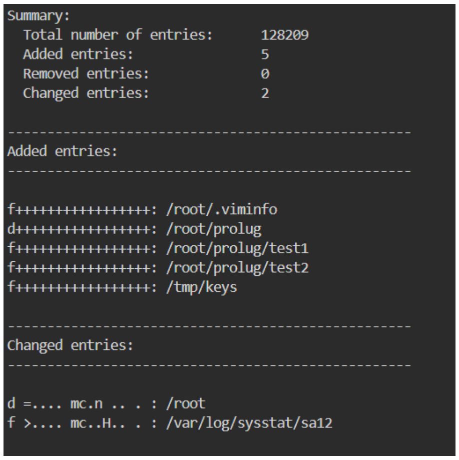
```
cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

Test aide by making files in a tracked directory

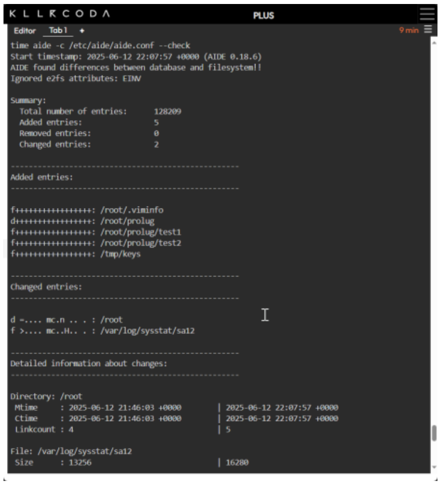
```
mkdir /root/prolug

touch /root/prolug/test1

touch /root/prolug/test2

time aide -c /etc/aide/aide.conf --check
```

Did you see your new files created?

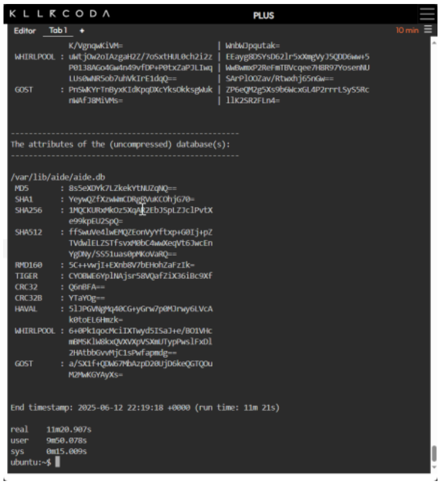
YES



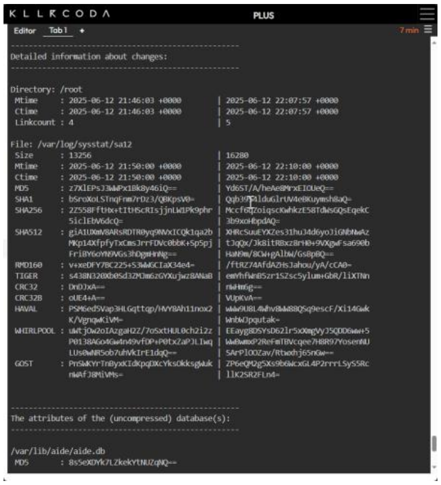
```
Summary:
  Total number of entries:      128209
  Added entries:                5
  Removed entries:              0
  Changed entries:              2

---------------------------------------------------
Added entries:
---------------------------------------------------

f+++++++++++++++++: /root/.viminfo
d+++++++++++++++++: /root/prolug
f+++++++++++++++++: /root/prolug/test1
f+++++++++++++++++: /root/prolug/test2
f+++++++++++++++++: /tmp/keys

---------------------------------------------------
Changed entries:
---------------------------------------------------

d =.... mc.n .. . : /root
f >.... mc..H.. . : /var/log/sysstat/sa12
```



```
time aide -c /etc/aide/aide.conf --check
Start timestamp: 2025-06-12 22:07:57 +0000 (AIDE 0.18.6)
AIDE found differences between database and filesystem!!
Ignored e2fs attributes: EINV

Summary:
  Total number of entries:      128209
  Added entries:                5
  Removed entries:              0
  Changed entries:              2

---------------------------------------------------
Added entries:
---------------------------------------------------

f++++++++++++++++: /root/.viminfo
d++++++++++++++++: /root/prolug
f++++++++++++++++: /root/prolug/test1
f++++++++++++++++: /root/prolug/test2
f++++++++++++++++: /tmp/keys

---------------------------------------------------
Changed entries:
---------------------------------------------------

d =.... mc.n .. . : /root
f >.... mc..H.. . : /var/log/sysstat/sa12

---------------------------------------------------
Detailed information about changes:
---------------------------------------------------

Directory: /root
 Mtime     : 2025-06-12 21:46:03 +0000        | 2025-06-12 22:07:57 +0000
 Ctime     : 2025-06-12 21:46:03 +0000        | 2025-06-12 22:07:57 +0000
 Linkcount : 4                                | 5

File: /var/log/sysstat/sa12
 Size      : 13256                            | 16280
```



```
            K/VgnqwKiVM=                     | WnbWJpqutak=
 WHIRLPOOL : uWtjOw2oIAzgaH2Z/7oSxtHUL0ch2i2z | EEayg8DSYsD62lr5xXmgVyJ5QDD6ww+5
             P0138AGo4Gw4n49vfDP+P0txZaPJLIwq | WwBwmxP2ReFmTBVcqee7H8R97YosenNU
             LUs0wNR5ob7uhVkIrE1dqQ==         | SArPlOOZav/Rtwxhj65nGw==
 GOST      : PnSWKYrTnByxKIdKpqDXcYksOkksgWuk | ZP6eQM2g5Xs9b6WcxGL4P2rrrLSyS5Rc
             nWAfJ8MiVMs=                     | 1lK2SR2FLn4=


---------------------------------------------------
The attributes of the (uncompressed) database(s):
---------------------------------------------------

/var/lib/aide/aide.db
 MD5       : 8s5eXDYk7LZkekYtNUZqNQ==
 SHA1      : YeywQZfXzwWmCDRgRVuKCOhjG70=
 SHA256    : 1MQCKURxMkOz5XqAR2EbJSpLZJclPvtX
             e99kpEU2SpQ=
 SHA512    : ffSwuVe4lwEMQZEonVyYftxp+G0Ij+pZ
             TVdwlELZSTfsvxM0bC4wwXeqVt6JwcEn
             YgDNy/SS51uas0pMKoVaRQ==
 RMD160    : 5C++vwjI+EXnb8V7bEHohZaFzIk=
 TIGER     : CYOBWE6YplNAjsr58VQafZiX36iBc9Xf
 CRC32     : Q6nBFA==
 CRC32B    : YTaYOg==
 HAVAL     : 5lJPGVNgMq40CG+yGrw7p0MJrwy6LVcA
             k0toEL6Hmzk=
 WHIRLPOOL : 6+0Pk1qocMciIXTwyd5ISaJ+e/BO1VHc
             mBMSKlW8kxQVXVXpVSXmUTypPwslFxDl
             2HAtbbGvvMjC1sPwfapmdg==
 GOST      : a/SX1f+QDW67MbAzpD20UjD6keQGTQOu
             M2MwKGYAyXs=


End timestamp: 2025-06-12 22:19:18 +0000 (run time: 11m 21s)

real    11m20.907s
user    9m50.078s
sys     0m15.009s
ubuntu:~$ 
```

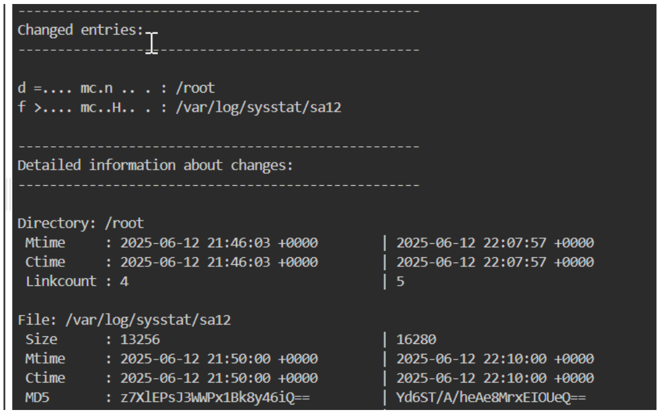


```
---------------------------------------------------
Detailed information about changes:
---------------------------------------------------

Directory: /root
 Mtime     : 2025-06-12 21:46:03 +0000        | 2025-06-12 22:07:57 +0000
 Ctime     : 2025-06-12 21:46:03 +0000        | 2025-06-12 22:07:57 +0000
 Linkcount : 4                                | 5

File: /var/log/sysstat/sa12
 Size      : 13256                            | 16280
 Mtime     : 2025-06-12 21:50:00 +0000        | 2025-06-12 22:10:00 +0000
 Ctime     : 2025-06-12 21:50:00 +0000        | 2025-06-12 22:10:00 +0000
 MD5       : z7XlEPsJ3WWPx1Bk8y46iQ==         | Yd6ST/A/heAe8MrxEIOUeQ==
 SHA1      : bSroXoLSTnqFnm7rDz3/QBKpsV0=     | Qqb39P1duGlrUV4eBKuymsh8aQ=
 SHA256    : 2Z558FftHx+tItHScRIsjjnLW1Pk9phr | MccfGqZoiqscKwhkzE58TdWsGQsEqekC
             5iclEbV6dcQ=                     | 3b9xoHbpdAQ=
 SHA512    : giA1UXmV8ARsRDTR0yq9NVxICQk1qa2b | XHRcSuuEYXZes31huJ4d6yoJiGNbNwAz
             MKp14XfpfyTxCmsJrrFDVc0bbK+Sp5pj | tJqQx/Jk8itRBxz8rH0+9VXgwFsa690b
             Fri8Y6oYN9VGs3hDgmHnNg==         | HaN9m/8CW+gAlbW/Gs8pBQ==
 RMD160    : v+xeDFY7BC225+S3WWGCIaX34e4=     | /ftRZ74AfdAZHsJahou/yA/cCA0=
 TIGER     : s438N320Xb0Sd3ZMJm6zGYXujwz8ANaB | emYhfWnB5zr1SZsc5ylum+GbR/liXTNn
 CRC32     : DnDJxA==                         | nwHm6g==
 CRC32B    : oUE4+A==                         | VUpKvA==
 HAVAL     : PSM6ed5Vap3HLGqttqp/HVY8Ah11nox2 | wWw9U8L4Whv8WW88QSq9escF/Xi14Gwk
             K/VgnqwKiVM=                     | WnbWJpqutak=
 WHIRLPOOL : uWtjOw2oIAzgaH2Z/7oSxtHUL0ch2i2z | EEayg8DSYsD62lr5xXmgVyJ5QDD6ww+5
             P0138AGo4Gw4n49vfDP+P0txZaPJLIwq | WwBwmxP2ReFmTBVcqee7H8R97YosenNU
             LUs0wNR5ob7uhVkIrE1dqQ==         | SArPlOOZav/Rtwxhj65nGw==
 GOST      : PnSWKYrTnByxKIdKpqDXcYksOkksgWuk | ZP6eQM2g5Xs9b6WcxGL4P2rrrLSyS5Rc
             nWAfJ8MiVMs=                     | 1lK2SR2FLn4=


---------------------------------------------------
The attributes of the (uncompressed) database(s):
---------------------------------------------------

/var/lib/aide/aide.db
 MD5       : 8s5eXDYk7LZkekYtNUZqNQ==
```

What type of usage do you see against user/system space?

user   9m50.078s

sys 0m15.009s



```
--------------------------------------------------
Changed entries:
--------------------------------------------------

d =.... mc.n .. . : /root
f >.... mc..H.. . : /var/log/sysstat/sa12

--------------------------------------------------
Detailed information about changes:
--------------------------------------------------

Directory: /root
 Mtime     : 2025-06-12 21:46:03 +0000        | 2025-06-12 22:07:57 +0000
 Ctime     : 2025-06-12 21:46:03 +0000        | 2025-06-12 22:07:57 +0000
 Linkcount : 4                                | 5

File: /var/log/sysstat/sa12
 Size      : 13256                            | 16280
 Mtime     : 2025-06-12 21:50:00 +0000        | 2025-06-12 22:10:00 +0000
 Ctime     : 2025-06-12 21:50:00 +0000        | 2025-06-12 22:10:00 +0000
 MD5       : z7XlEPsJ3WWPx1Bk8y46iQ==         | Yd6ST/A/heAe8MrxEIOUeQ==
```

How long did this take to run?

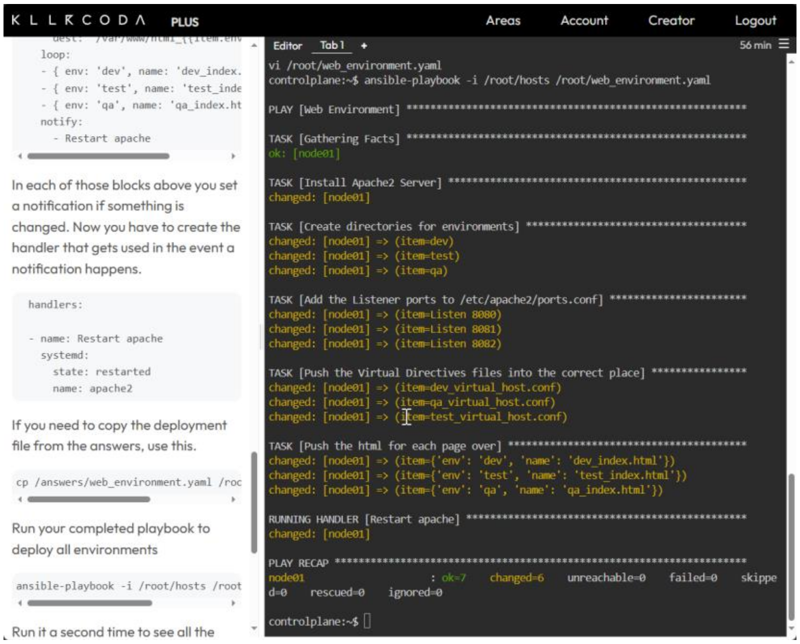
real 11m20.907s

user 9m50.078s

sys 0m15.009s

Using Ansible to fix drift 1 of

Complete the lab here: https://killercoda.com/het-tanis/course/Ansible-Labs/16-Ansible-Web-Server-Env-Deploy



```
      dest: /var/www/html_{{item.env
    loop:
    - { env: 'dev', name: 'dev_index.
    - { env: 'test', name: 'test_inde
    - { env: 'qa', name: 'qa_index.ht
    notify:
      - Restart apache
```

In each of those blocks above you set a notification if something is changed. Now you have to create the handler that gets used in the event a notification happens.

```
handlers:

- name: Restart apache
  systemd:
    state: restarted
    name: apache2
```

If you need to copy the deployment file from the answers, use this.

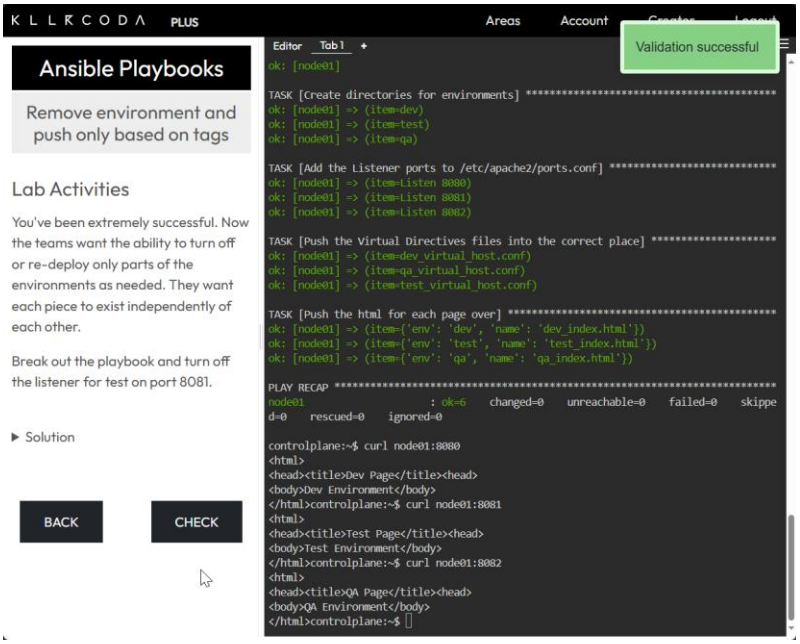
```
cp /answers/web_environment.yaml /roo
```

Run your completed playbook to deploy all environments

```
ansible-playbook -i /root/hosts /root
```

Run it a second time to see all the

```
vi /root/web_environment.yaml
controlplane:~$ ansible-playbook -i /root/hosts /root/web_environment.yaml

PLAY [Web Environment] ***************************************************************

TASK [Gathering Facts] ***************************************************************
ok: [node01]

TASK [Install Apache2 Server] ********************************************************
changed: [node01]

TASK [Create directories for environments] *******************************************
changed: [node01] => (item=dev)
changed: [node01] => (item=test)
changed: [node01] => (item=qa)

TASK [Add the Listener ports to /etc/apache2/ports.conf] *****************************
changed: [node01] => (item=Listen 8080)
changed: [node01] => (item=Listen 8081)
changed: [node01] => (item=Listen 8082)

TASK [Push the Virtual Directives files into the correct place] **********************
changed: [node01] => (item=dev_virtual_host.conf)
changed: [node01] => (item=qa_virtual_host.conf)
changed: [node01] => (item=test_virtual_host.conf)

TASK [Push the html for each page over] **********************************************
changed: [node01] => (item={'env': 'dev', 'name': 'dev_index.html'})
changed: [node01] => (item={'env': 'test', 'name': 'test_index.html'})
changed: [node01] => (item={'env': 'qa', 'name': 'qa_index.html'})

RUNNING HANDLER [Restart apache] *****************************************************
changed: [node01]

PLAY RECAP ***************************************************************************
node01                     : ok=7    changed=6    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0

controlplane:~$
```



Ansible Playbooks

Remove environment and push only based on tags

Lab Activities

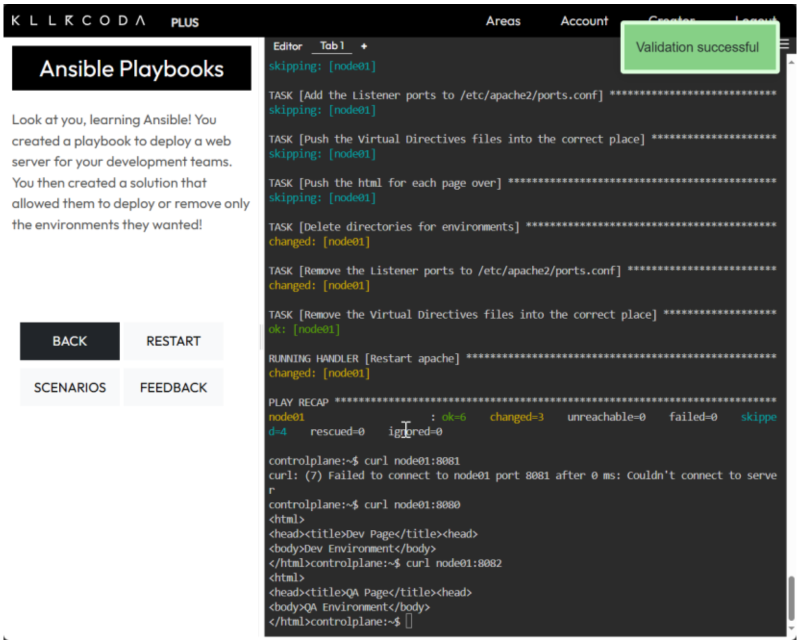
You've been extremely successful. Now the teams want the ability to turn off or re-deploy only parts of the environments as needed. They want each piece to exist independently of each other.

Break out the playbook and turn off the listener for test on port 8081.

▶ Solution

```
ok: [node01]

TASK [Create directories for environments] *******************************************
ok: [node01] => (item=dev)
ok: [node01] => (item=test)
ok: [node01] => (item=qa)

TASK [Add the Listener ports to /etc/apache2/ports.conf] *****************************
ok: [node01] => (item=Listen 8080)
ok: [node01] => (item=Listen 8081)
ok: [node01] => (item=Listen 8082)

TASK [Push the Virtual Directives files into the correct place] **********************
ok: [node01] => (item=dev_virtual_host.conf)
ok: [node01] => (item=qa_virtual_host.conf)
ok: [node01] => (item=test_virtual_host.conf)

TASK [Push the html for each page over] **********************************************
ok: [node01] => (item={'env': 'dev', 'name': 'dev_index.html'})
ok: [node01] => (item={'env': 'test', 'name': 'test_index.html'})
ok: [node01] => (item={'env': 'qa', 'name': 'qa_index.html'})

PLAY RECAP ***************************************************************************
node01                     : ok=6    changed=0    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0

controlplane:~$ curl node01:8080
<html>
<head><title>Dev Page</title><head>
<body>Dev Environment</body>
</html>controlplane:~$ curl node01:8081
<html>
<head><title>Test Page</title><head>
<body>Test Environment</body>
</html>controlplane:~$ curl node01:8082
<html>
<head><title>QA Page</title><head>
<body>QA Environment</body>
</html>controlplane:~$
```

When you finish ensure that you see broken output for 8081, as required.



Ansible Playbooks

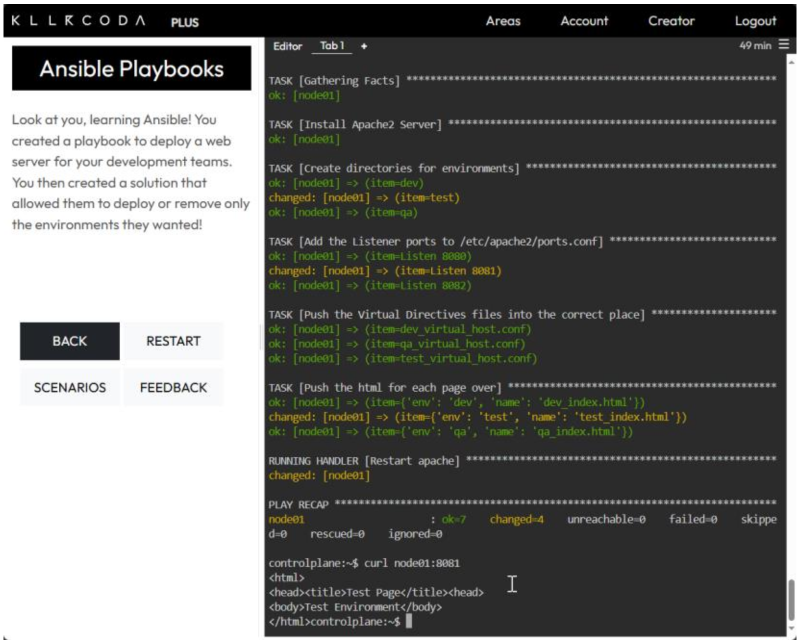
Look at you, learning Ansible! You created a playbook to deploy a web server for your development teams. You then created a solution that allowed them to deploy or remove only the environments they wanted!

```
skipping: [node01]

TASK [Add the Listener ports to /etc/apache2/ports.conf] *****************************
skipping: [node01]

TASK [Push the Virtual Directives files into the correct place] *********************
skipping: [node01]

TASK [Push the html for each page over] *********************************************
skipping: [node01]

TASK [Delete directories for environments] ******************************************
changed: [node01]

TASK [Remove the Listener ports to /etc/apache2/ports.conf] *************************
changed: [node01]

TASK [Remove the Virtual Directives files into the correct place] *******************
ok: [node01]

RUNNING HANDLER [Restart apache] ****************************************************
changed: [node01]

PLAY RECAP **************************************************************************
node01                     : ok=6    changed=3    unreachable=0    failed=0    skippe
d=4    rescued=0    ignored=0

controlplane:~$ curl node01:8081
curl: (7) Failed to connect to node01 port 8081 after 0 ms: Couldn't connect to serve
r
controlplane:~$ curl node01:8080
<html>
<head><title>Dev Page</title><head>
<body>Dev Environment</body>
</html>controlplane:~$ curl node01:8082
<html>
<head><title>QA Page</title><head>
<body>QA Environment</body>
</html>controlplane:~$ 
```

curl node01:8081

One of the dev teams figured out they could modify the test and qa environments because a previous engineer left them in the sudoers file. You can address that separately with the security team, but for now you need to get those environments back to working. Run your original deployment command to see if it sets the environment back properly.

ansible-playbook -i /root/hosts /root/web_environment.yaml



Ansible Playbooks

Look at you, learning Ansible! You created a playbook to deploy a web server for your development teams. You then created a solution that allowed them to deploy or remove only the environments they wanted!

```
TASK [Gathering Facts] *************************************************************
ok: [node01]

TASK [Install Apache2 Server] ******************************************************
ok: [node01]

TASK [Create directories for environments] *****************************************
ok: [node01] => (item=dev)
changed: [node01] => (item=test)
ok: [node01] => (item=qa)

TASK [Add the Listener ports to /etc/apache2/ports.conf] ***************************
ok: [node01] => (item=Listen 8080)
changed: [node01] => (item=Listen 8081)
ok: [node01] => (item=Listen 8082)

TASK [Push the Virtual Directives files into the correct place] ********************
ok: [node01] => (item=dev_virtual_host.conf)
ok: [node01] => (item=qa_virtual_host.conf)
ok: [node01] => (item=test_virtual_host.conf)

TASK [Push the html for each page over] ********************************************
ok: [node01] => (item={'env': 'dev', 'name': 'dev_index.html'})
changed: [node01] => (item={'env': 'test', 'name': 'test_index.html'})
ok: [node01] => (item={'env': 'qa', 'name': 'qa_index.html'})

RUNNING HANDLER [Restart apache] ***************************************************

changed: [node01]

PLAY RECAP *************************************************************************
node01                     : ok=7    changed=4    unreachable=0    failed=0    skippe
d=0    rescued=0    ignored=0

controlplane:~$ curl node01:8081
<html>
<head><title>Test Page</title><head>
<body>Test Environment</body>
</html>controlplane:~$ 
```

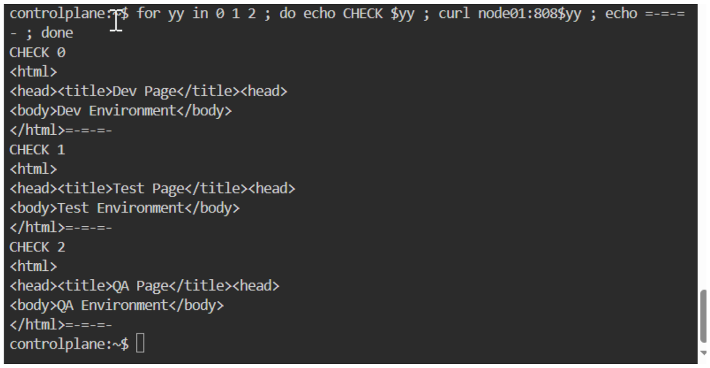
Did this force the system back into a working configuration?

YES

If it worked, would it always work, or would they (the systems) need to be manually intervened?

ALWAYS

What is your test? (hint: curl the ports 8080, 8081, and 8082 from previous commands)



```
controlplane:~$ for yy in 0 1 2 ; do echo CHECK $yy ; curl node01:808$yy ; echo =-=-=
- ; done
CHECK 0
<html>
<head><title>Dev Page</title><head>
<body>Dev Environment</body>
</html>=-=-=-
CHECK 1
<html>
<head><title>Test Page</title><head>
<body>Test Environment</body>
</html>=-=-=-
CHECK 2
<html>
<head><title>QA Page</title><head>
<body>QA Environment</body>
</html>=-=-=-
controlplane:~$ 
```

Could this cause potential problems in the environment?

Accidentally running the incorrect playbook can wipe out manual configurations

If so, is that problem based on technology or operational practices? Why?

Operational practices- running a playbook needs to be under robust change management procedures