

ANSIBLE

## SECURITY AUTOMATION WITH ANSIBLE

Faz Sadeghi  
Specialist Solution Architect

# WHY SECURITY AUTOMATION

ANSIBLE



Application Security  
Network Security  
Forensics  
Incident Response  
Penetration Testing  
Fraud Detection and Prevention  
Governance, Risk, Compliance

# STORY OF MARKO

ANSIBLE



## WALL OF SEPARATION

**SECurity**



Wants to ensure Information Assurance

**OPerations**



Wants to ensure System Availability

**Rule Title:** The SSH daemon must not allow authentication using an empty password Linux servers.

**Rule Title:** Anonymous enumeration of shares must be restricted on Windows servers.

**Rule Title:** The network element must only allow management connections for administrative access from hosts residing in to the management network.

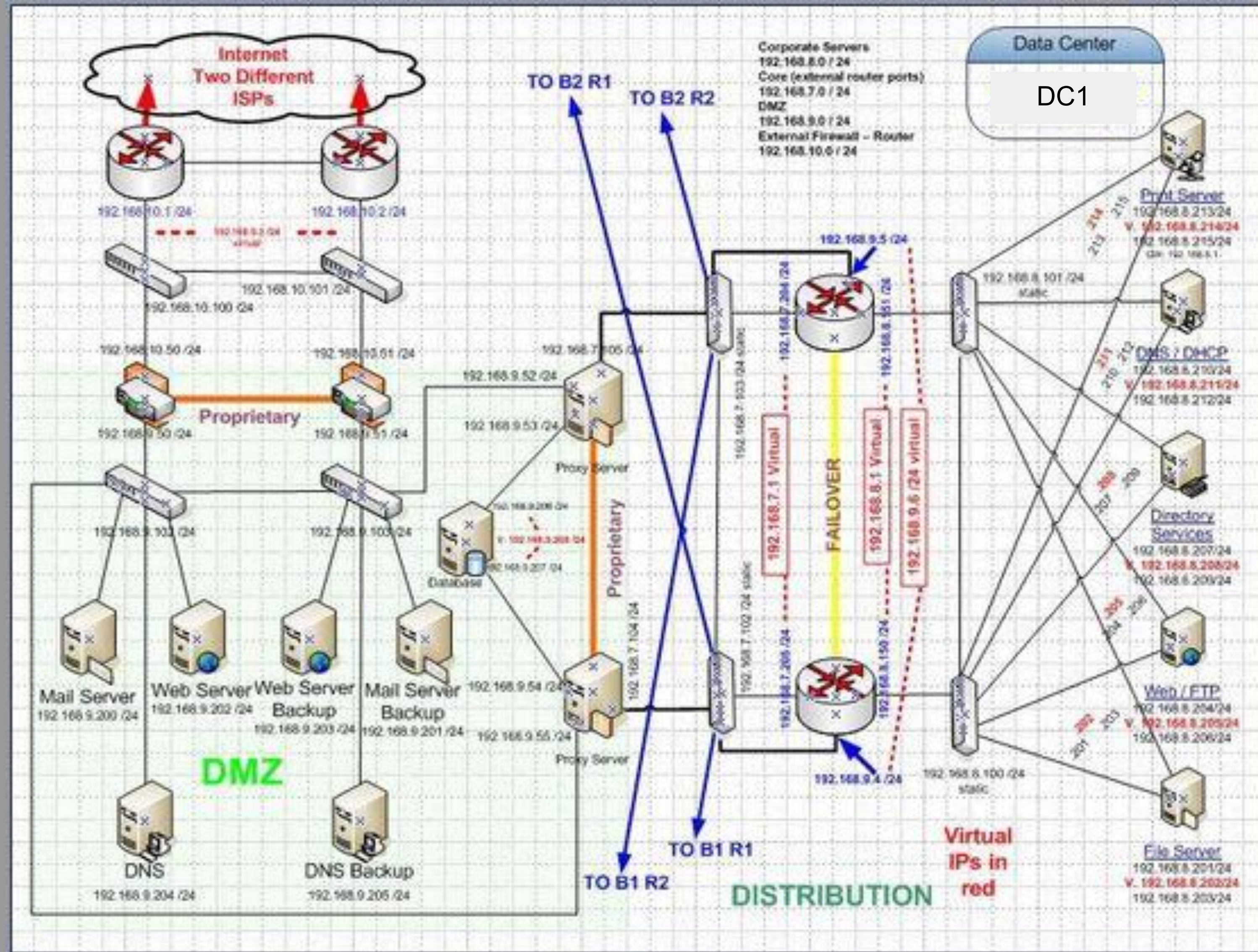
**Rule Title:** Change root password on all servers, according to policy every 60 days.

**Rule Title:** Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release.

**Rule Title:** Protect against CVE-2016-5696.

**Rule Title:** Fix and test shellshock.

# PLANNING THE IMPLEMENTATION









# SYSTEM MELTDOWN

ANSIBLE



**Something has to change**

# WE NEED A SOLUTION

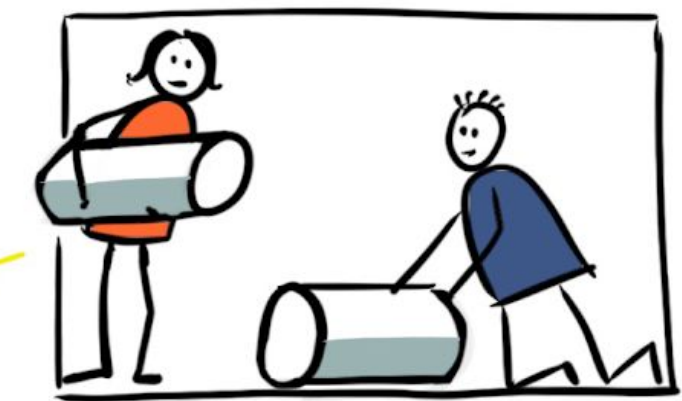
ANSIBLE



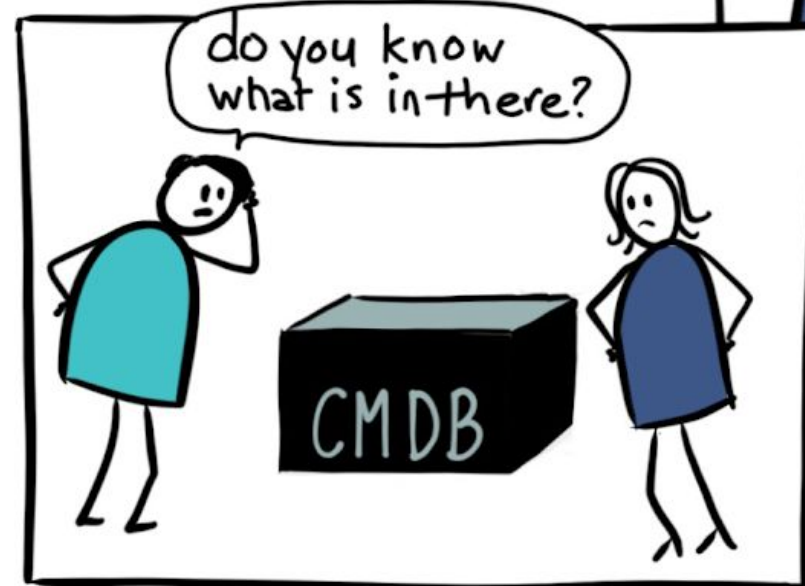
BETTER, FASTER,  
SMARTER WITH  
DEVOPS

## DEVOPS & AUTOMATION

### HOW TO START



BUILD A PIPELINE



do you know  
what is in there?

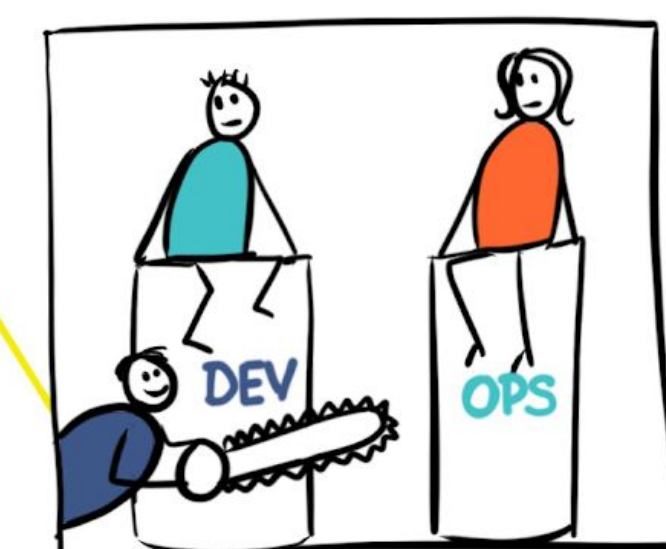


TODAY'S REALITY

Look, I found  
Ansible!



FIND THE  
BOTTLENECKS

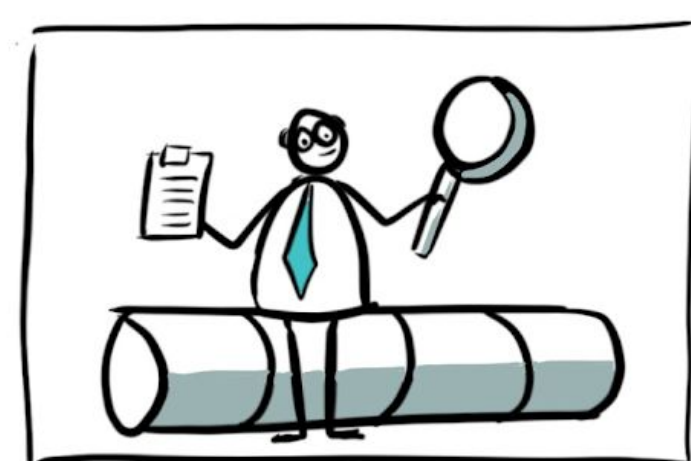


GET RID OF SILOS



WHERE  
IS THE  
WASTE

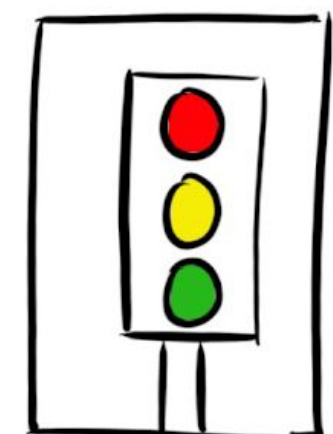
Automate security



COMPLIANCE SHOULD  
BE CONTINUOUS TOO

PERIODIC TABLE OF DEVOPS TOOLS (V2)									
Gh									
Gt	Dm								
Bb	Lb								
Gl	Rg	Mv	Gr	At	Fn	Se	Ga	Dh	Jn
Sv	Dt	Gt	Gp	Br	Cu	Cj	Qu	Npm	Cs
Hg	Dp	Sb	Mk	Ck	Ju	Jm	Th	Ay	Tc
Cw	ld	Msb	Rk	Pk	Mc	Xltv	Jm	Nx	Co
Xlr	Ur	Bm	Hp	Au	Pi	Sr	Tfs	Tr	Jr
Ki	Nr	Ni	Zb	Dd	Ei	Ss	Sp	Le	Sl

FIND THE RIGHT TOOLS



CREATE  
VISIBILITY  
&  
CONTROL

Thea Schukken

- **Agentless**
- **SSH/WinRM**
- **Desired State**
- **Idempotent**
- **Easy to learn**
- **Extensible and modular**
- **Push-based architecture**
- **Easy targeting based on facts**



The screenshot displays the Ansible Tower dashboard interface. At the top, navigation tabs include TOWER, PROJECTS, INVENTORIES, JOB TEMPLATES, and JOBS. The user is logged in as 'admin'. The dashboard features a 'DASHBOARD' section with six summary cards: 524 HOSTS, 63 FAILED HOSTS, 48 INVENTORIES, 2 INVENTORY SYNC FAILURES, 29 PROJECTS, and 1 PROJECT SYNC FAILURES. Below this is a 'JOB STATUS' line chart showing the number of jobs over time from May 10 to June 10. The chart has two data series: a green line for total jobs and a red line for failed jobs. A significant peak in total jobs is visible around June 4th. At the bottom, there are two sections: 'RECENTLY USED JOB TEMPLATES' and 'RECENT JOB RUNS'. The first section shows a template titled 'Deploy Software' with a full activity status and action icons. The second section shows a recent job run titled 'Terminate AWS instances' that completed at 3:01:01 AM.

**Summary Metrics:**

- 524 HOSTS
- 63 FAILED HOSTS
- 48 INVENTORIES
- 2 INVENTORY SYNC FAILURES
- 29 PROJECTS
- 1 PROJECT SYNC FAILURES

**JOB STATUS**

PERIOD: PAST MONTH | JOB TYPE: ALL | VIEW: ALL

**RECENTLY USED JOB TEMPLATES**

TITLE	ACTIVITY	ACTIONS
Deploy Software	●●●●●●●●●●	

**RECENT JOB RUNS**

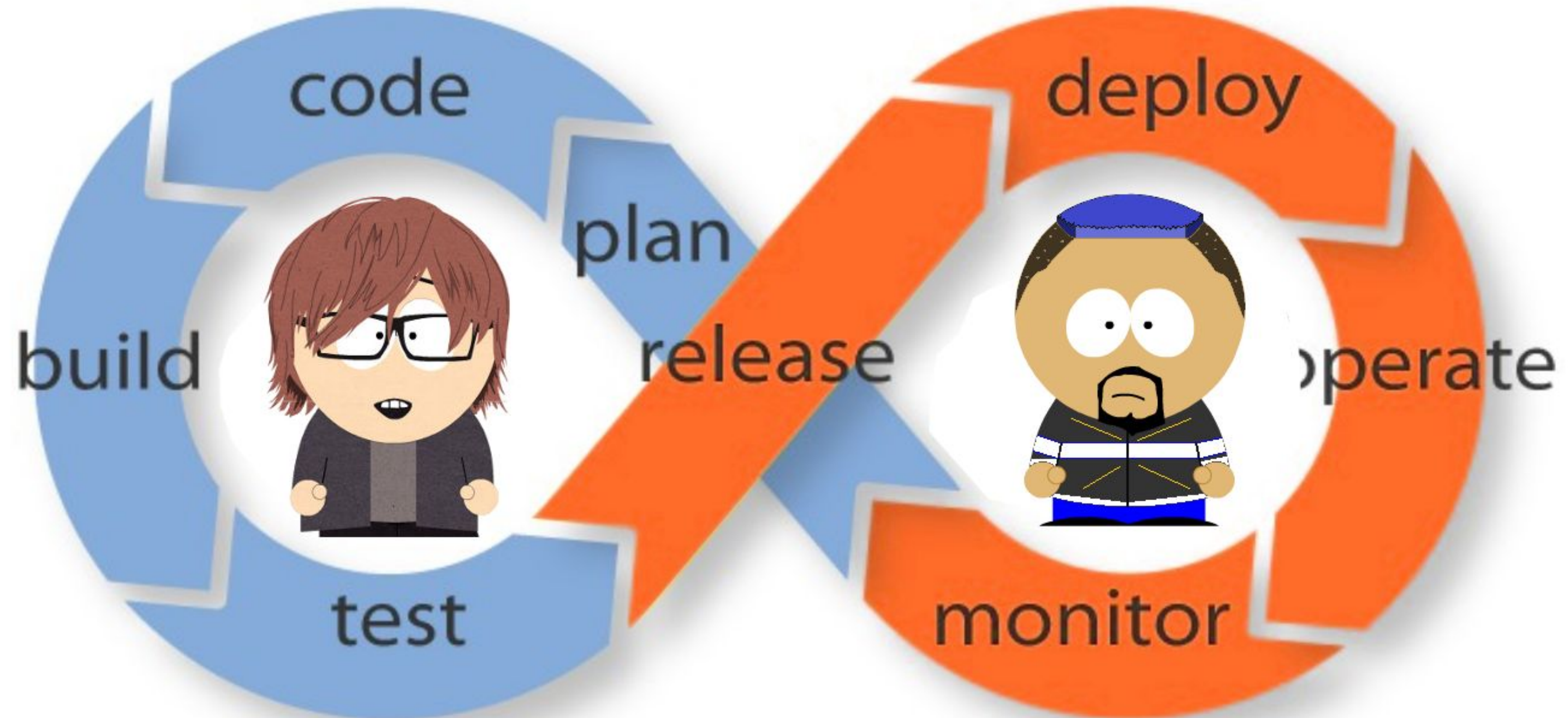
TITLE	TIME
● Terminate AWS instances	3:01:01 AM



LET'S GET AUTOMATING

ANSIBLE





<https://www.niceideas.ch/roller2/badtrash/entry/devops-explained>

**Rule Title:** The SSH daemon must not allow authentication using an empty password.

**Fix Text:** To explicitly disallow remote logon from accounts with empty passwords, add or correct the following line in

"/etc/ssh/sshd\_config" **line** /etc/ssh/sshd\_config

PermitEmptyPasswords no

PermitEmptyPasswords no

- name: "HIGH | RHEL-07-010270 | PATCH | The SSH daemon must not allow authentication using an empty password."

**lineinfile:**

state: present

dest: /etc/ssh/sshd\_config

regexp: ^#?PermitEmptyPasswords

line: PermitEmptyPasswords no

validate: sshd -tf %s

notify: restart sshd

**Rule Title:** The network element must only allow management connections for administrative access from hosts residing in to the management network.

**Fix Text:** Configure an **ACL or filter** to restrict management access to **management network** from only the management network

- hosts: ios  
connection: local
  
- tasks:
  - name: Create management ACL  
**ios\_config:**
    - parents: ip access-list mgmnt
    - before: no ip access-list mgmnt
    - lines:
      - 10 permit ip host 192.168.1.99 log
      - 20 permit ip host 192.168.1.121 log
  
  - name: Harden VTY lines  
**ios\_config:**
    - parents: line vty 0 15
    - lines:
      - exec-timeout 15
      - transport input ssh
      - access mgmnt in

**Rule Title:** Anonymous enumeration of shares must be restricted.

**Fix Text:** Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Do not allow anonymous enumeration of SAM accounts and shares" to "Enabled".

- **hosts:** windows

**tasks:**

- **name:** Restrict enumeration of shares

**win\_regedit:**

**key:**

'HKLM:\System\CurrentControlSet\Control\Lsa'

**value:** RestrictAnonymous

**data:** 1

**datatype:** dword

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.

- name: RHEL | Install updates

**yum:**

name: "\*"

state: latest

exclude: "mysql\* httpd\* nginx\*"

when: "ansible\_os\_family == 'RedHat'"

- name: DEBIAN | Install updates

**apt:**

update\_cache: yes

cache\_valid\_time: 7200

name: "\*"

state: latest

when: "ansible\_os\_family == 'Debian'"

Change root password every 60 days

---

```
- name: Change root password
hosts: all
become: yes
vars:
  root_password: "{{ vault_root_password }}"
  root_password_salt: "{{ vault_root_password_salt }}"
tasks:
  - name: Change root password
    user:
      name: root
      password: "{{ root_password |
password_hash(salt=root_password_salt) }}"
```

## Protect against CVE-2016-5696

---

```
- name: Protect against CVE-2016-5696
  hosts: all
  become: yes
  become_user: root

  tasks:
    - name: CVE-2016-5696 | Limit TCP challenge ACK limit
      sysctl:
        name: net.ipv4.tcp_challenge_ack_limit
        value: 999999999
        sysctl_set: yes
```



## Fix and test shellshock

---

```
- name: Fix and test shellshock
hosts: all
tasks:
  - name: Update bash
    yum:
      name: bash
      state: latest
      update_cache: yes

  - name: Test vulnerability 1
    shell: 'env x='' () { :; }; echo vulnerable' bash -c "echo
this is a test"
    executable: /bin/bash
    register: vulntest1
    failed_when: vulntest1.stdout | search('vulnerable')
    ignore_errors: yes
    changed_when: no
```

## Fix and test shellshock - continued

---

- name: Test vulnerability 2
  - shell: `'env X='' () { (a)=>' bash -c ''echo date'';'`
  - executable: `/bin/bash`
  - register: `vulntest2`
  - failed\_when:
    - `not vulntest2.stderr | search('error importing function definition')`
  - ignore\_errors: `yes`
  - changed\_when: `no`
- name: Cleanup after vulnerability test 2
  - file:
    - path: `~/echo`
    - state: `absent`

THE END

ANSIBLE



Ansible Lockdown

Ansible Hardening

Mailing List

Ansible Galaxy

<https://github.com/samdoran/demo-playbooks>