GIVING POWER TO THE PEOPLE With ANSIBLE @ General Mills

Ops | Devs | Net

Ashley Nelson
DevOps Engineer - General Mills

Mike Dahlgren
Sr. Cloud Solution Architect - Red Hat

WHO ARE WE?

ASHLEY NELSON
DEVOPS @ GEN MILLS

MIKE DAHLGREN
CLOUD SA @ REDHAT

AGENDA!

- History of Automation at General Mills
- Use Case #1: Operations
- Use Case #2: Networking
- Use Case #3: Application Management
- Operationalizing Ansible and Tower

GMI'S HISTORY OF AUTOMATION

C

Large File Copy Script

Perl

SAN Zoning Script

Bash

VM Storage Script

Python

Linux Group Mapping Script

Ruby

Server Provisioning Scripts

Puppet

Server Config Deployment

Room for Improvement

Portability

Supportability

Integration

Locality

Knowledge Sharing

Permissions

WHY ANSIBLE?

No Setup

RPM Installation

Use existing SSH

Python-based

On Linux by default

Familiar with language

Intuitive

YAML – markup language

Sequentially executed

Integration

No need to change environment

Works alongside Puppet

Glues automation together

Ecosystem

Modules for a variety of use cases

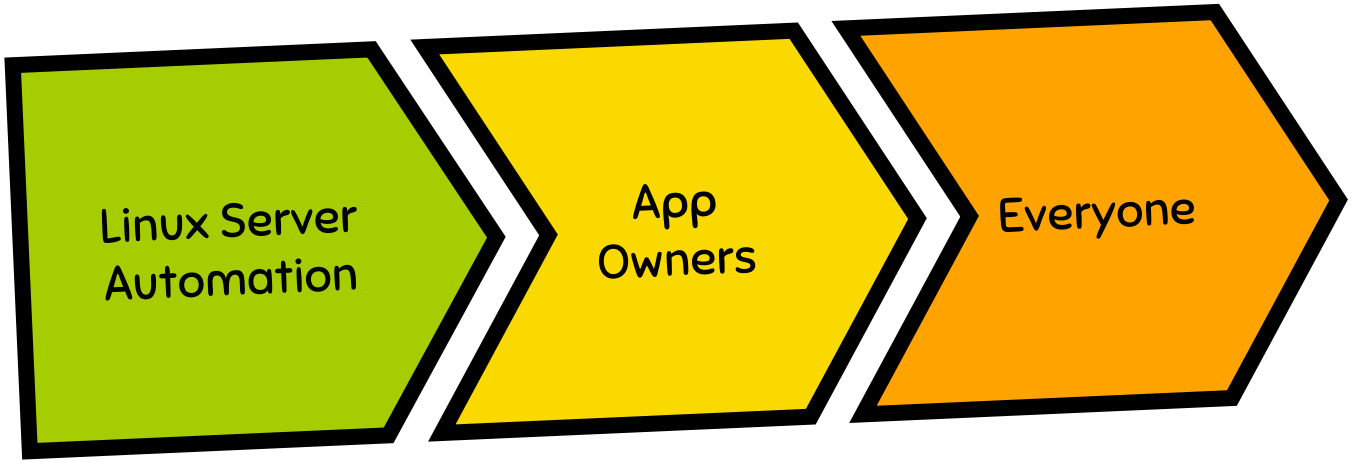
Most of our vendors have modules

Ad-hoc Tasks

Runs automation just once

Don't always need to worry about idempotence

ANSIBLE @ GENERAL MILLS



WHY TOWER?

PRIVILEGED ACCESS

Non-server admins can execute privileged automation

No access to playbook or credentials

USER INTERFACE

Easier for people that are unfamiliar with Linux and the command line

API

Enables end to end automation when Ansible is not at the beginning of the pipeline

#1

USE CASE: OPERATIONS

Integrate Everything

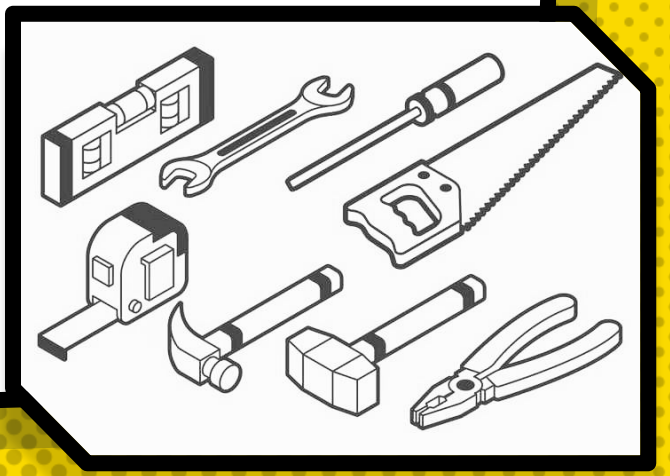
EVERYONE LOVES

SERVER PATCHING

RIGHT?

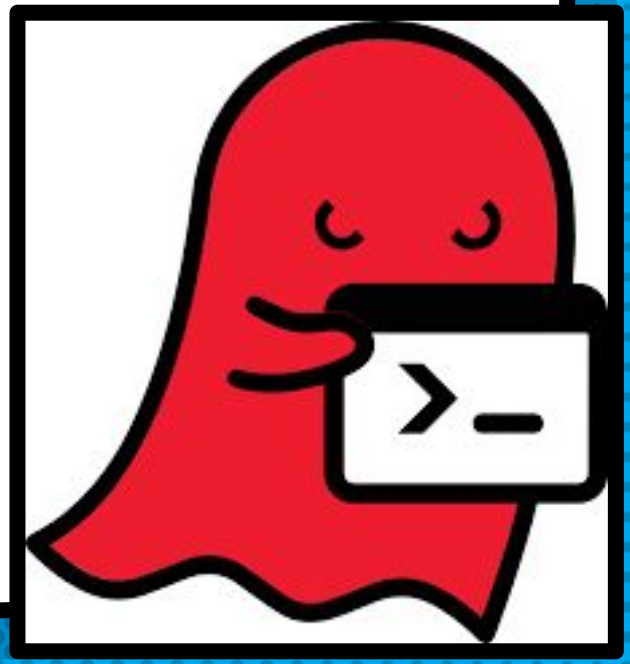
THE OLD WAY

- Whole team in a room together
- Divide up servers among everyone
- Manually run commands
  - Stop services
  - Update packages
  - Reboot
  - Verify new kernel



GLIBC GHOST VULNERABILITY

Critical buffer overflow vulnerability that required immediate patching



```
- assert: { that: "ansible_os_family == 'RedHat'" }

- name: update RHEL 7 channel
  command: /opt/gmi/tools/satellite/channels update {{ inventory_hostname }}
  delegate_to: job_server
  when: ansible_distribution_version == '7.1'

- name: upgrade all packages
  yum: name=* state=latest
  notify:
    - reboot machine

handlers:
 - name: reboot machine
   shell: sleep 2 && shutdown -r now "Ansible updates triggered"
   async: 1
   poll: 0
   ignore_errors: true
```

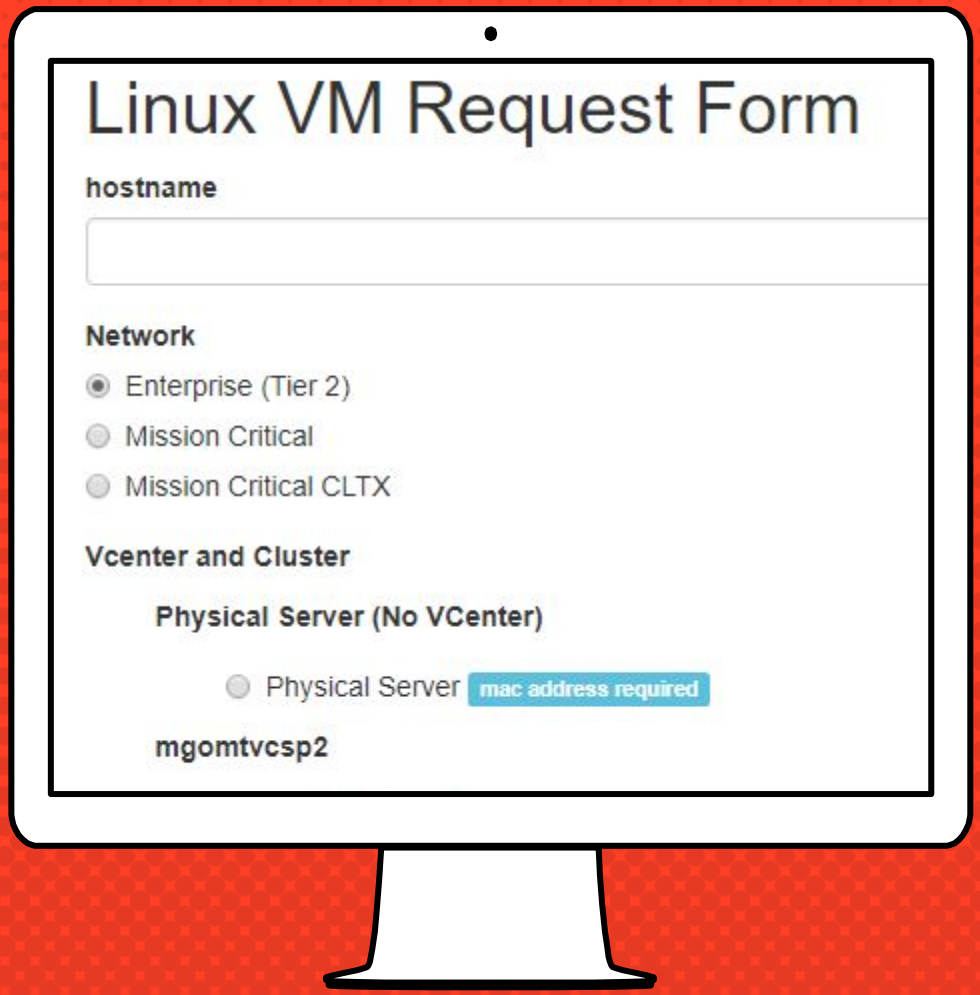
MY FIRST PLAYBOOK

9 PEOPLE
In a cramped room

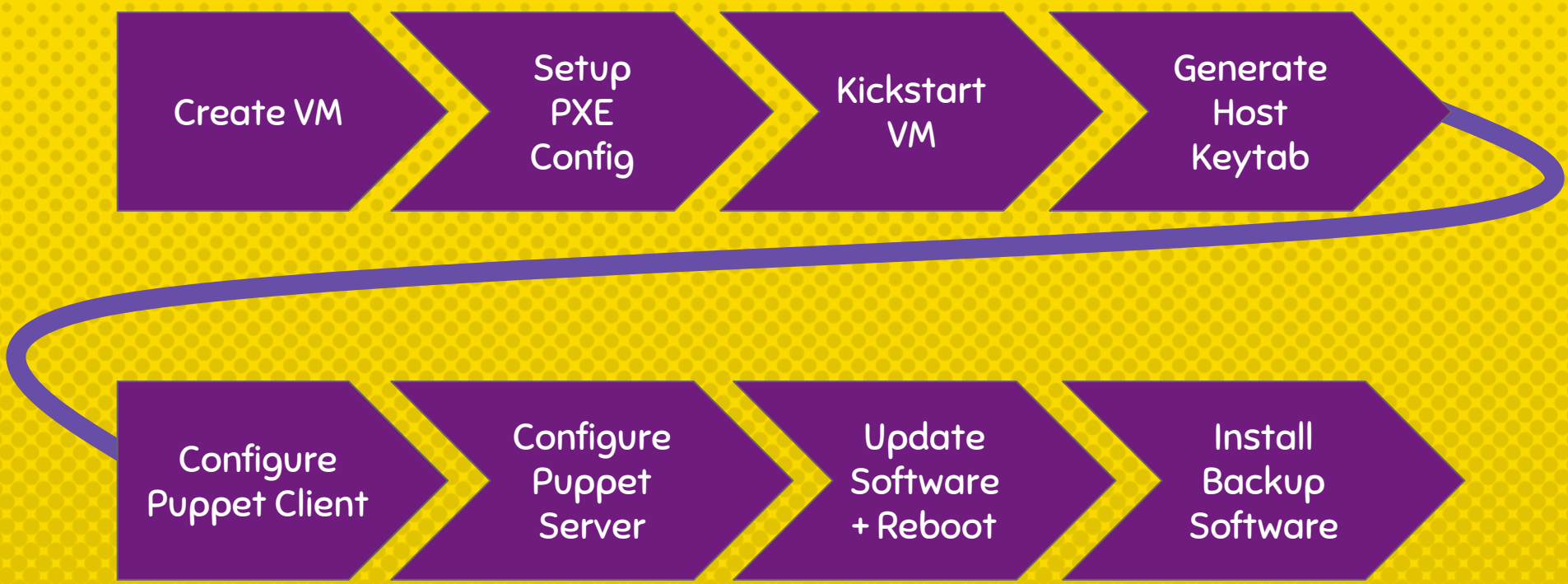
1 PERSON
In their pajamas

89%
Labor savings

WHERE DO SERVERS COME FROM?


Linux VM Request Form
hostname
Network
Enterprise (Tier 2)
Mission Critical
Mission Critical CLTX
Vcenter and Cluster
Physical Server (No VCenter)
Physical Server
mac address required
mgomtvcsp2

ANSIBLE ROLES



CONFIG MAPPING

```
vm_compute_map:
    clustorr1:
        vcenter: xmvcsq1
        datacenter: QA1
        cluster: Cluster1
        network_type: standard
vm_network_map:
    mission_critical:
        template: rhel_tier1net
    enterprise:
        template: rhel_tier2net
kickstart_map:
    rhel68_virtual:
        kickstart_profile: rhel68-rhel-x86_64-server6
        pxe_provider: satellite
```

PLAY FROM SERVER BUILD PLAYBOOK

```yaml
- name: Set up PXE boot
  hosts: new_hosts
  gather_facts: false
  serial: 1
  vars_files:
      - build_config_maps.yaml
  tags:
      - before_kickstart
  vars:
    kickstart_profile: "{{kickstart_map[kickstart].kickstart_profile}}"
    vcenter: "{{vm_compute_map[vm_compute].vcenter}}"
    vmware_datacenter: "{{vm_compute_map[vm_compute].datacenter}}"
  roles:
      - pxe_config
```

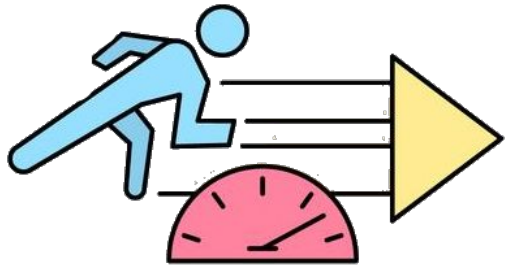
PHYSICAL SERVER BUILDS

```
- name: get HP ILO MAC address
  hpilo_facts:
    host: "{{inventory_hostname}}-ilo"
    login: admin
    password: "{{ lookup('ini', 'password section=ilo file=' + ilo_pw) }}"
  delegate_to: localhost
  connection: local
  register: ilo_facts

- name: set boot interface mac address fact
  vars:
    interface: "{{interface_map[hp_model]}}"
  set_fact:
    boot_mac_addr: "{{ilo_facts.ansible_facts[interface].macaddress | lower()}}"
    boot_mac_addr_dash: "{{ilo_facts.ansible_facts[interface].macaddress_dash}}"
```

RESULTS

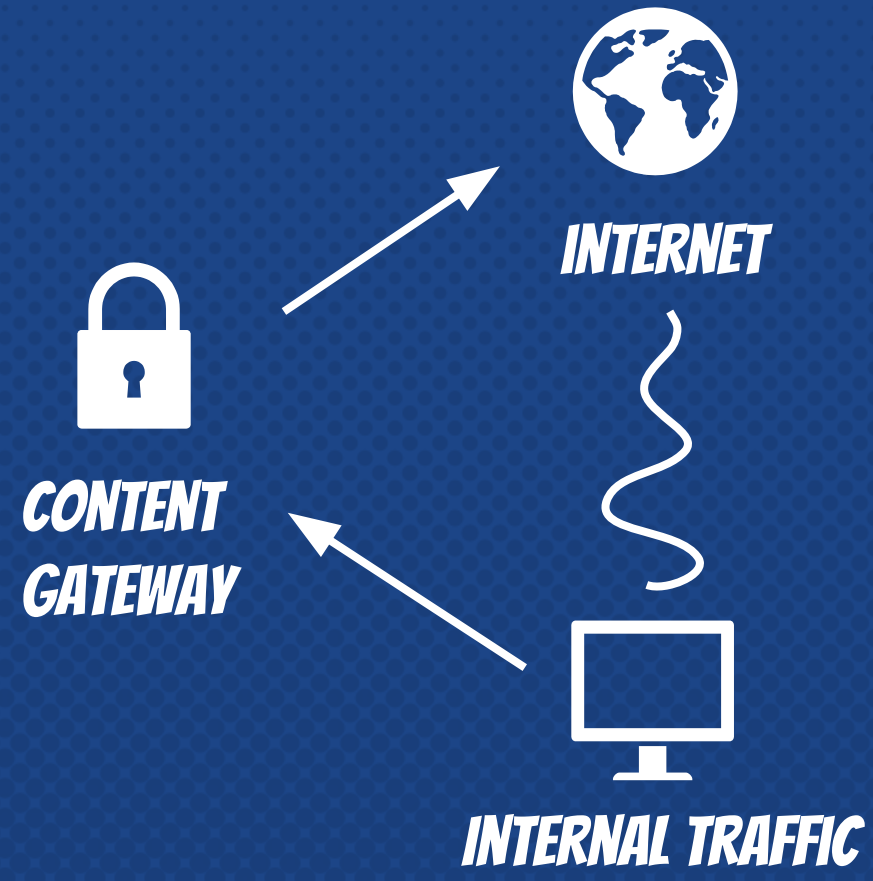
- Fully automated server provisioning
- 30 minutes of manual work to 1 minute
- Easier to automate for change
  - vCenters
  - OS versions
  - Networks



#2

USE CASE: NETWORKING

Router ACL's & The Cloud



OFFICE 365, MICROSOFT EXCHANGE, AND SKYPE DON'T APPRECIATE GOING THROUGH THE REDIRECT

PROCESS OF MANUALLY CREATING WHITELIST WAS 10+ HOURS OF WORK 🤯

THE ANSIBLE APPROACH !

PLAYBOOK #1

Detect whether Microsoft has updated their IP address list

PLAYBOOK #2

Retrieve new list and generate config to deploy to all routers

PLAYBOOK SAMPLE

```
- name: GET MICROSOFT PRODUCT IP ADDRESSES
  shell: /mnt/data1/network/scripts/get_microsoft_product_ip_addrs.py
  delegate_to: localhost
  run_once: true
  tags: always

- name: GENERATE INTERNET-WCCP ACCESS-LIST FILE
  template: src=internet_wccp.j2 dest={{acl_dir}}/internet-wccp.txt
  tags: generate_acl_file
...
- name: DEPLOY {{ inventory_hostname }} INTERNET-WCCP ACCESS-LIST
  napalm_install_config:
    provider: "{{ creds['conn'] }}"
    dev_os: "{{ dev_os }}"
    config_file: "{{acl_dir}}/internet-wccp.txt"
    commit_changes: True
    replace_config: False
    diff_file: "/tmp/{{ inventory_hostname }}.diff"
  tags: deploy_acl
```

NETWORKING RESULTS

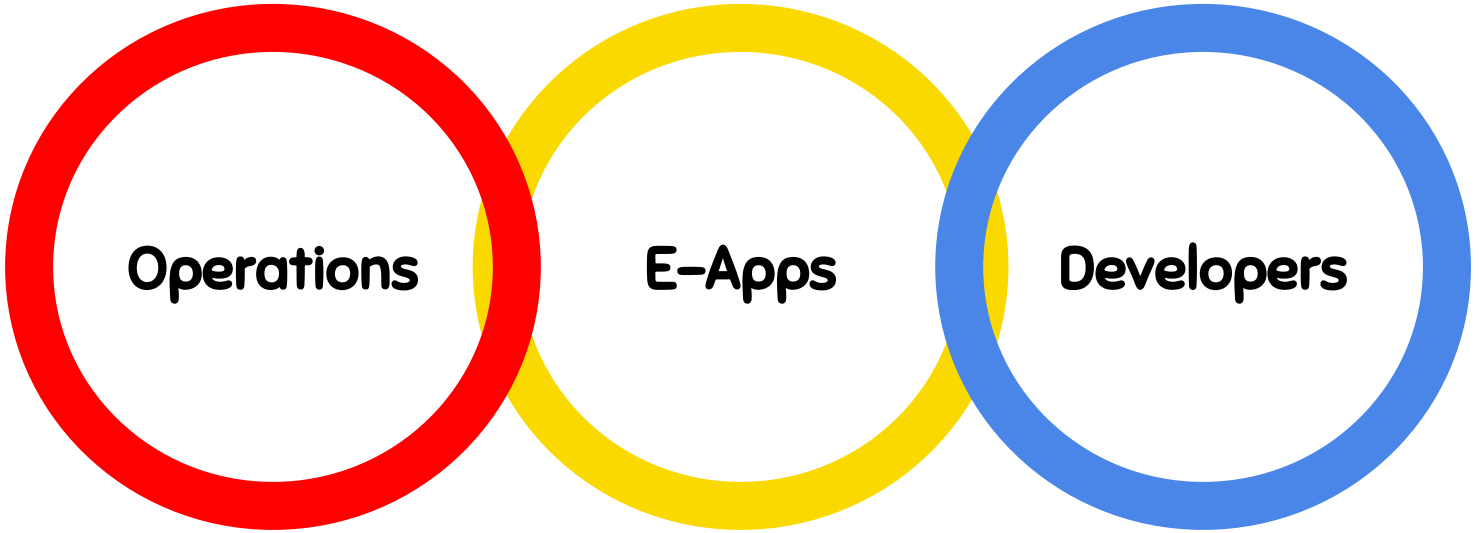
- Fully automated 10+ hours of tedious work
- Removed human error from equation
- Now updating router ACLs weekly
- For the end user the Cloud just works!

#3

USE CASE: APP MANAGEMENT

Empower the user!

WHAT'S BETWEEN DEVOPS?



THE SITUATION . . .

The E-Apps Team

11 PEOPLE
150+ APPS

- Responsible for Start/Stop/Deploy etc.
- Provided self-service for Win applications
  - SharePoint > Word Doc > watching process > JSON > PowerShell > 🤯
- Tasked with owning Linux applications
- Most of team not automation experts

THE APPROACH - ANSIBLE TOWER!

- Put everything in GIT
- Create a template of a template
  - Allows E-Apps team to quickly build services for new apps
- Used Tower Survey vs Word docs
- Allow users to schedule actions

ALL IN ONE ANSIBLE PLAYBOOK

THE USER

THE JOB TEMPLATE TEMPLATE

(ALL Options)

(ALL Servers)

THE JOB TEMPLATE (NEW SURVEY)

(LIMITED Options)

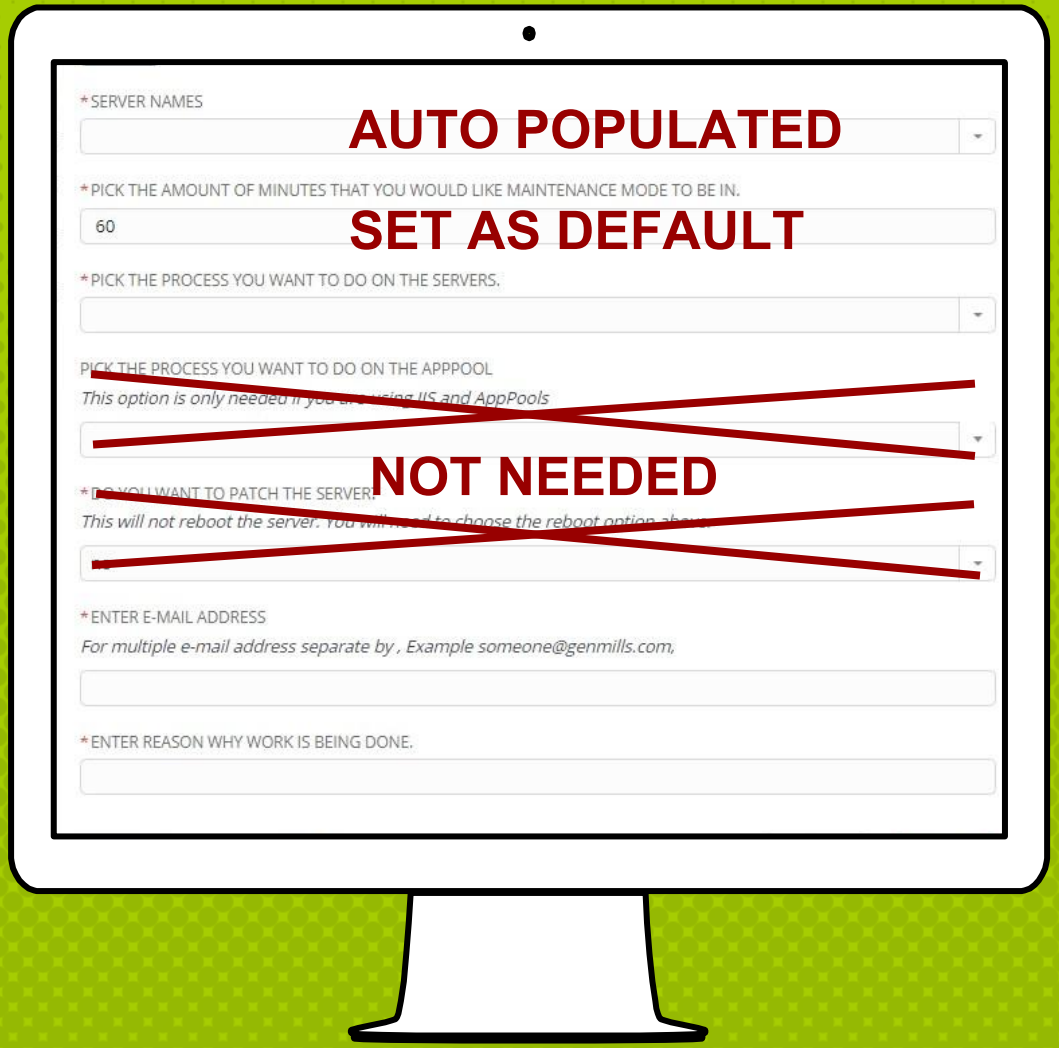
(LIMITED Servers)

THE ANSIBLE JOB

THE JOB TEMPLATE TEMPLATE!

Has all the options

CUSTOMIZE WHAT YOU DON'T WANT!



THE END USER EXPERIENCE!

Everything you need
– nothing you don't!

PLAYBOOK SAMPLE

```yaml
- include_tasks: "Windows_services_stop.yml sname={{ item }}"
  name: "Stopping {{stop_service_name}}"
  with_items: "{{stop_service_name}}"
  when: (win_command == "stop") or (win_command == "reboot")

- name: "Pause before stopping AppPool"
  pause:
    seconds: 60
  when: (AppPool_state == "stopped") or (AppPool_state == "restarted")

- name: "stop an application pool"
  win_iis_webapppool:
    name: "{{AppPool}}"
    state: "{{AppPool_state}}"
  when: (AppPool_state == "stopped") or (AppPool_state == "restarted")
```

ADVANTAGES

- Global changes can be made in one place
- Still allows for isolation
- Easily create Job templates
- Even without Ansible knowledge!

CHALLENGES

#1 WinRM

- Ansible wants to use HTTPS everywhere
- No GPO for certificate deployment
- Currently leveraging powershell script

#2 Plan the organization first!

- Split out the middleware group
- Required moving 100's of templates
- Give people access to multiple orgs

RESULTS

- Simpler interface for end users
- 90% of team workload now automated by Ansible
- Single automation platform for Windows + Linux
- Changes the role of the E-app team
- Can now focus on big picture projects

OPERATIONALIZING ANSIBLE

Introducing Teams to Ansible

- Meet with teams to go over Ansible architecture
- Linux –> Ansible Core server
- Windows –> Ansible Tower
- Segment teams by organization in Tower

Sharing Roles and Modules

- Open repositories in TFS
- Enforce best practices
- Required vs. optional variables documentation
- Import roles with Ansible Galaxy CLI or git submodules

Challenges

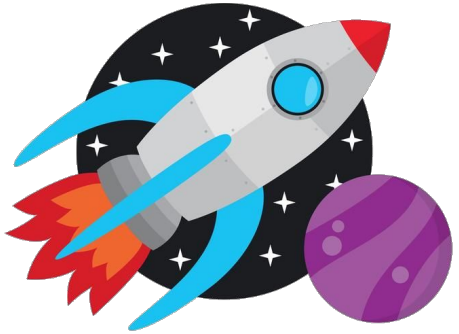
- × Python dependencies
- × Jump host with Windows
- × Integration with TFS
- × Job isolation

YOU'RE NOT ALONE!

Red Hat has support for Tower, Networking, and Engine.

Join your local Ansible meetups and RHUG's (Red Hat User Group).

FUTURE PLANS



- Replace scripts with Ansible
- Eliminate manual infrastructure changes
- Setup Tower Isolated Nodes
- Isolated Python environments for teams

CREDITS

Special thanks to everyone who made this possible:

- Application story by Richard Zuraff
- Network story by Warren Welford
- Presentation template by SlidesCarnival
- Photographs from Vecteezy.com

THANK YOU


plus.google.com/+RedHat


facebook.com/redhatinc


linkedin.com/company/red-hat


twitter.com/RedHat

youtube.com/user/RedHatVideos