<!-- Slide number: 1 -->
# Ansible Alliance

![](Picture4.jpg)
Securing IaaS in the cloud
Lake Laberge, Yukon Territory, Canada. Shutterstock
Greg Cormier, Kevin Dutton, Alex Imray-Papineau

<!-- Slide number: 2 -->
# Background
DFO started their cloud journey in 2017
By volume of data, mostly unclassified data related to science
A number of systems at the Protected B level
DFO’s cloud strategy is multi-cloud
DFO chose Azure as their first cloud service provider to focus efforts, and AWS is the second rolling out in 2019

2

<!-- Slide number: 3 -->
# The Problem
Cloud requires skills in various domains which are generally maintained by other teams (SSC)
Some of these areas are well known to Cloud Service Providers
As a result, they offer tailored solutions specific to their cloud offering
Infrastructure as a Service (IaaS) has the biggest burden of responsibility for the customer

How do we handle IaaS management?
3

### Notes:
- Networking, Storage, Backups, Patching, automation

<!-- Slide number: 4 -->
# Our first attempt at a solution…
Provider specific tools
Azure Update Management
Azure Automation DSC (Desired State Config)
Fairly good integration into the Azure ecosystem
Portal integration was good

4

<!-- Slide number: 5 -->
# … reality sets in
We had to deal with powered-off VM’s
Failed updates often caused issues and broke things
The solution didn’t feel production ready
All of the efforts, and any of the attempted problem solving or customization would take more work

Were we ready to do this all over again in AWS?

5

<!-- Slide number: 6 -->
# Problem Redefined
How do we handle IaaS management, in a cloud service provider agnostic manner?

How do we get, at a glance, the status of all our infrastructure in the cloud?

6

<!-- Slide number: 7 -->

![File:Ansible logo.svg](Picture2.jpg)
“Ansible is an open-source software provisioning, configuration management, and application-deployment tool.”
7

<!-- Slide number: 8 -->
# Ansible
Lets us maintain the state of a VM
Ansible is agent-less – it talks directly to an operating system (whether it is on the cloud or not)
Linux - SSH to talk to the target
Windows - WinRM (SSH under development)

Playbooks are a YAML file that describes what to do
Ansible handles multiple executions of the same playbook against hosts for most modules
Ansible provides a simple way to enforce common software installations, or common settings, across multiple hosts
8

<!-- Slide number: 9 -->
# Example Windows Playbooks
- name: Install all security, critical, and rollup updates
  win_updates:
    category_names:
      - SecurityUpdates
      - CriticalUpdates
      - UpdateRollups
- name: Restart a service
  win_service:
    name: spooler
    state: restarted

9

<!-- Slide number: 10 -->
# Example Linux Playbooks
- name: Upgrade all Linux packages to the latest version
  apt:
    name: "*"
    state: latest
- name: Ensure the httpd service is running
  service:
    name: httpd
    state: started
  become: true
10

<!-- Slide number: 11 -->
# Example Execution
- name: This is a hello-world example
  hosts: 127.0.0.1
  tasks:
    - name: Create a file called '/tmp/testfile.txt' with the content 'hello world'.
      copy:
        content: hello world
        dest: /tmp/testfile.txt

![](Picture6.jpg)
11

<!-- Slide number: 12 -->

![](Picture5.jpg)
12

<!-- Slide number: 13 -->

![](Picture6.jpg)
AWX adds a web-based user interface, job scheduling, inventory management, reporting, workflow automation, credential sharing, and tooling to enable delegation.

AWX is the open source project behind Red Hat Ansible Tower.
13

### Notes:

<!-- Slide number: 14 -->
# AWX
AWX lets us take simple Ansible playbooks, and apply the management at a much larger scale
It supports various sources for the inventory, including Azure, AWS, GCP, VMWare vCenter
It can use code repositories as the source for the playbooks, to allow simple updates and deployments
We can define schedules to run different playbooks as required

14

### Notes:
- Best of all, it’s the GUI!

<!-- Slide number: 15 -->

![](Picture4.jpg)
15

<!-- Slide number: 16 -->
# AWX at DFO
Hourly compliance playbooks based on the ULL profile
Nightly patching playbooks, with Azure Automation integration for powering on shutdown VM’s

We can apply this to any VM, whether it’s on Azure or on AWS, and have a single pane to view the status of our security and patching tasks.

16

<!-- Slide number: 17 -->
# Back to Security
Ansible let’s us easily define the blueprints on what configurations or changes an OS needs
We decided to use this to define our security blueprint
Using an existing list of settings from TBS, we converted these to Ansible Playbooks
17

<!-- Slide number: 18 -->

![Image result for we need you](Picture2.jpg)
18

<!-- Slide number: 19 -->
# Ansible Alliance
https://github.com/dfocloud/ansible-alliance

We’re looking for departments to help contribute towards a PBMM hardening profile

We can change the implementation of various controls over time as the OS matures
For security, the more eyes, the better!
Combine our IT expertise for various aspects of hardening

19

<!-- Slide number: 20 -->
# Demo and Questions
Greg.Cormier@dfo-mpo.gc.ca
Alex.ImrayPapineau@dfo-mpo.gc.ca
Kevin.Dutton@dfo-mpo.gc.ca

20

### Notes: