Our Cool Automation

-Or -

Our experience with Ansible and Redhat Ansible Automation Platform
for rapid and widespread monitoring agent deployments

Who we are

- Patrick Spinler
  - IT Architect in Monitoring Solutions group
  - Started using linux in 1992 – SLS, then Yggdrasil
    - Had scsi drivers BSD didn't!
  - First use at work for a 1993 project needing X-Terms to access and program a HP unix system
  - Have been developer, dba, sysadmin, ...
- Mayo Clinic
  - Only here as myself, not representing views of Mayo Clinic

What We Do

- Infrastructure and Log Monitoring using Splunk
  - Our OnPrem infrastructure
  - Some cloud APM and logs, but not applicable to this topic
- APM Monitoring using AppDynamics
  - Java, php, python, apache, dotNet core
- ~2500 linux and AIX systems
  - 99% of systems have splunk agents
  - ~500 have appdynamics agents

Problem of the day

- How to get agents to servers
- Started with custom scripts, bash and perl
- Included in build process for splunk agent, log in and run it for appdynamics
- Scripts large and complex, hard to maintain
- 'log in and run it' process doesn't scale

But Ansible !

- Really really like declarative and idempotent nature of a properly constructed playbook
  - No writing tests in shell / perl "if not this way, then … "
  - Perl / bash 714 lines, ansible 218 lines
- Mass installs in parallel
- Our system build process includes our playbooks

And also Tower, now RHAAP

- For manual installs, our less technical team members can just use a web page
- Less required sudo privs
- Central system logging and tracking, makes admins happy(er)

Some successes

- Twice – upgrade all splunk agents on all VM's
  - Less than a day!
- Modified every systemd unit file to include restart on fail
- Large batch upgrades / installs of AppDynamics agents
- Entire team now doing agent installs

But we still have problems

- Fiefdoms
  - We have multiple admin groups, several smaller groups want our agents but won't allow tower / ansible to run on their systems.
  - Still having to maintain old scripts so we have something to give to them
  - Also, getting the "main" sysadmin team to initally share tower/rhapp access ...

But we still have problems

- Security and access for Agents
  - Separate security realms / directory services for different groups of servers.
    - Does this daemon account exist in this realm ?
  - Sudo rules and ACL's needed for support team to actually support the agent
    - Not all admin groups allow, not all systems support

But we still have problems

- Some install steps can't be scripted
  - Particularly APM agents
    - Java requires modifying the startup parameters. Which params, and where to find them? JBOSS config, websphere config, systemd unit file, tomcat setenv.sh, basic shell script, cron jobs …
    - Php requires fiddly exact locations, limited support for older runtimes
    - Node.js requires code changes
    - c/c++ requires recompile + code changes
    - Etc etc etc

But we still have problems

- Vendor agent installs suck
  - No-one has selinux labels and/or policies. Always have to hand craft these
    - Testing sucks, 'cause running something interactively works more often than not, but then fails as a systemd unit file. Always takes me a second to go "d'oh! Selinux!"
  - Few people think about running agents as non-root, or more so, multiple non-root for different users on a shared big machine
  - When the vendor does supply a systemd unit file, almost always have to edit it post running the vendor install script

Show off some ansible

Where do we go from here

- Sadly – projecting less use of ansible for our onprem agent installs as we move to containerized onprem, as well as cloud and kubernetes
- But! -- ansible playbooks to install and upgrade some of our own infrastructure
- Non ansible future topics
  - Moving away from vendor specific monitoring agents, and towards OTEL and MELT

Offtopic – Splunk and/or AppDynamics demos