RED HAT FORUM
Europe, Middle East & Africa
SYSTEM MANAGEMENT UPDATE

Fred van Zwieten
Solution Architect Platform & Cloud
10-10-2017
RED HAT INSIGHTS
MANAGING INFRASTRUCTURE RISK

Automated remediation

ANALYZE
IDENTIFY
PRIORITIZE
RESOLVE
RED HAT INSIGHTS
ARCHITECTURE

INFRASCTRUCTURE

SERVER DATA ANONYMIZATION

MINIMAL NETWORK IMPACT

RESULTS TAILORED TO EACH HOST

REMEDICATION STEPS

PLAYBOOKS
ALREADY A RED HAT® ENTERPRISE LINUX® CUSTOMER?
Try Insights at no cost:
https://access.redhat.com/insights/getting-started

INTERESTED IN A MANAGEMENT SUITE?
Insights is included in:
Red Hat Cloud Infrastructure + Red Hat Cloud Suite

WOULD YOU LIKE TO LEARN MORE ABOUT INSIGHTS?
For more info, visit: https://access.redhat.com/insights/info
Run an Insights assessment for 30 days:
1. Work with your account team to get an Insights eval subscription.
2. Install the Red Hat Insights RPM.
3. Register 50+ systems for best view.
4. See results immediately.
5. Schedule a best practices workshop.

See valuable insights in minutes:

QUESTIONS?
insights@redhat.com
RED HAT ENTERPRISE LINUX

EASE OF MANAGEMENT

Using WEB GUI
COCKPIT

Using ANSIBLE
SYSTEM ROLES
CURRENT ROLES

- email (postfix)
- kdump (kernel crash dump)
- network
- selinux
- timesync

FUTURE ROLES

- Subscription Management
- firewall
- system logging
- storage
- kerberos authentication
- bootloader
- tuned (power management)
- etc
Roles and Ansible CLI delivered with RHEL
Extras channel, upstream on git and galaxy
# yum --enablerepo=rhel-7-server-extras-rpms install rhel-system-roles ansible

From RHEL 6.9+
Abstraction, RHEL version agnostic

Support on System Roles included
Ansible CLI support only in system role use-cases

Control Node on RHEL 7.4+
Managed Nodes RHEL 6.9+
Choice:
- Now: Puppet Inside or Puppet Enterprise and/or Ansible Tower
- V6.3: Puppet v3 and/or Puppet v4 and/or Ansible Tower
- V6.4: Puppet and/or Ansible Inside and/or Ansible Tower

For Configuration Management use-cases

Integration with Insights
- V6.4: Including Ansible remediation playbook support

Integration with CloudForms
- Bare metal insights, utilize Satellite from Ansible Inside CloudForms

Integration with Ansible Tower
- Satellite as Inventory Source and Ansible Callbacks
RED HAT ANSIBLE TOWER
Scale + operationalize your automation
CONTROL KNOWLEDGE DELEGATION

RED HAT ANSIBLE ENGINE
Support for your Ansible automation
SIMPLE POWERFUL AGENTLESS

FUELED BY AN INNOVATIVE OPEN SOURCE COMMUNITY
NEW PRODUCT OFFERING!
Support for Ansible CLI & Core Modules

SUPPORT FOR NETWORK MODULES
Add-on to Red Hat Engine *

OVER 1250 MODULES INCLUDED
Core, Networking, Certified & Community

*Premium support only
RED HAT ANSIBLE ENGINE
HOW IT WORKS

CLOUD
OpenStack, VMware, EC2, Rackspace, GCE, Azure, Spacewalk, Hanlon, Cobbler

CUSTOM CMDB

PUBLIC / PRIVATE CLOUD

CMDB

PUBLIC / PRIVATE CLOUD

ANSIBLE'S AUTOMATION ENGINE

INVENTORY

API

MODULES

PLUGINS

HOSTS

NETWORK DEVICES

ANSIBLE PLAYBOOK

USERS
- name: install and start apache
  hosts: web
  become: yes
  vars:
    http_port: 80

  tasks:
  - name: httpd package is present
    yum:
      name: httpd
      state: latest

  - name: latest index.html file is present
    copy:
      src: files/index.html
      dest: /var/www/html/

  - name: httpd is started
    service:
      name: httpd
      state: started
Use Ansible to manage, validate, and continuously track heterogeneous network device configurations and deployments.

Network modules are included as part of the Ansible distribution.

33+ Networking platforms

460+ Networking Modules

ansible.com/networking
- name: configure ios interface
  hosts: ios01
  tasks:
    - name: collect device running-config
      ios_command:
        commands: show running-config interface GigabitEthernet0/2
        register: config

    - name: verify operational status
      ios_command:
        commands:
          - show interfaces GigabitEthernet0/2
          - show cdp neighbors GigabitEthernet0/2 detail
        waitfor:
          - result[0] contains 'line protocol is up'
          - result[1] contains 'iosxr03'
          - result[1] contains '10.0.0.42'

        provider: "{{ cli }}"
Use Ansible to deploy and manage Windows systems and applications.

70+ Windows Modules

350+ Powershell DSC resources
- hosts: new_servers
  tasks:
  - name: ensure common OS updates are current
    win_updates:
    register: update_result

  - name: ensure domain membership
    win_domain_membership:
      dns_domain_name: contoso.corp
      domain_admin_user: '{{ domain_admin_username }}'
      domain_admin_password: '{{ domain_admin_password }}'
      state: domain
    register: domain_result

  - name: ensure common tools are installed
    win_chocolatey:
      name: '{{ item }}'
    with_items: ['sysinternals', 'googlechrome']
### Red Hat Ansible Engine

**Supported Platforms**

<table>
<thead>
<tr>
<th>Control nodes</th>
<th>Managed Nodes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Hat Enterprise Linux 7.2 and later (x86_64 only)</td>
<td>Red Hat Enterprise Linux 6.3 and later (x86_64 only)</td>
</tr>
<tr>
<td>Ubuntu 14.04 LTS (x86_64 only)</td>
<td>Red Hat Enterprise Linux 7.2 and later (x86_64 only)</td>
</tr>
<tr>
<td>Ubuntu 16.04 LTS (x86_64 only)</td>
<td>Ubuntu 14.04 * 16.04 LTS (x86_64 only)</td>
</tr>
<tr>
<td>Network Devices</td>
<td>Others - unlisted RHEL variants, SuSE, Solaris, AIX, etc.</td>
</tr>
<tr>
<td>(Arista EOS, Cisco IOS, IOS-XE, IOS-XR, NX-OS, Juniper Junos OS, VyOS)</td>
<td>Commercially reasonable support only</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RED HAT ANSIBLE TOWER

WHAT IS NEW?

- **BUILT-IN FACT CACHING**
  Facts stored in Tower database

- **SMART INVENTORIES**
  Dynamic fact based grouping

- **INVENTORY FROM SOURCE CONTROL**
  Version controlled inventories
RED HAT ANSIBLE TOWER

WHAT IS NEW?

- CUSTOM CREDENTIALLY
  Define your own credential types

- INSTANCE GROUPS
  Dynamic fact based grouping

- ISOLATED NODES
  Offload execution to remote control nodes
RED HAT ANSIBLE TOWER

WHAT IS NEW?

- Remote Office
- Isolated Nodes
- Public Cloud
- DMZ
- ssh
- Cluster
- Instance Group
- ssh
- cold standby
RED HAT ANSIBLE TOWER

WHAT IS NEW?

ISSUE: Decreased security in system logging permissions
Issues related to system logging and auditing were detected on your system. Important services are disabled or log file permissions are not secure.
dddddd (33649)

ISSUE: Kernel key management subsystem vulnerable to local privilege escalation (CVE-2016-0728)
A vulnerability in the Linux kernel allowing local privilege escalation was discovered. The issue was reported as [CVE-2016-0728] (https://access.redhat.com/security/cve/cve-2016-0728).
dddddd (33649)

ISSUE: Kernel vulnerable to privilege escalation via permission bypass (CVE-2016-5195)
A flaw was found in the Linux kernel’s memory subsystem. An unprivileged local user could use this flaw to write to files they would normally only have read-only access to and thus increase their privileges on the system.
dddddd (33649)

ISSUE: Kernel vulnerable to man-in-the-middle via payload injection
A flaw in the Linux kernel’s TCP/IP networking subsystem implementation of the [RFC 5961] (https://tools.ietf.org/html/rfc5961) challenge ACK rate limiting was found that could allow an attacker located on different subnet to inject or take over a TCP connection between a server and client without needing to use a traditional man-in-the-middle (MITM) attack.
CLOUDFORMS
AN EVOLUTIONARY PATH TO HYBRID CLOUD

CONTAINERS
Red Hat® OpenShift Container Platform

VIRTUALIZATION
VMware®, Microsoft® Hyper-V, Red Hat Virtualization

PRIVATE CLOUD
Red Hat Openstack® Platform

PUBLIC CLOUD
Amazon® Web Services, Microsoft Azure, Google® Cloud Platform

SOFTWARE DEFINED NETWORKING
Self Service Playbooks

Playbook as a Service

- Order
- Modify (roadmap)
- Retire
Policy State Management

Playbook as a Policy Action
See events, Conditionally Process and run a Playbook

Event - Condition - Playbook
VM Powers On - Is Database Server - Connect extra Disk
Software Scan - Is Vulnerable - Update Software
Alerts

Playbook as a Alert Action
React to

- Alert
  Out of Disk Space
  High CPU Long Duration

- Playbook
  Expand Disk
  Add More CPU
Call Ansible Playbooks as methods in a state machine
Allows for Hybrid Ruby and Ansible Orchestration

Compute Resource Linking to CloudForms Services
Provides visibility of Compute items that Ansible deployed.

More credentials supported
OpenStack, (RHV), Azure, Google, Satellite, Subversion, GitLab
Networking

More CloudForms modules
Including secure authentication van Ansible callbacks into CloudForms

Self Service Portal Languages
In het Nederlands!
Q & A