ShellShock, HeartBleed--What's the next headache for compliance?

Brad Ascar
Field Product Manager - CloudForms
24 June 2015
Brad Ascar is Field Product Manager for CloudForms at Red Hat.

He has worked as a developer/architect in Enterprise IT, IT Operations, R&D, medium and small startups in his 30+ year career.
Rich Jerrido has worked with Linux since 1999 and with virtualization since 2000. Rich is the Technical Product Marketing Manager for Red Hat Satellite, assisting customers in efficiently deploying their infrastructures in support of their business objectives. Particularly, he focuses on lifecycle management, content management and governance of all things Red Hat: servers, content, configuration and subscriptions.
A little history

Q: Why this title?
A: Why are you sitting in this session?

Q: Are you responsible for the security and/or compliance of your compute landscape?
A: You are in the right place.
How do Red Hat CloudForms and Red Hat Satellite help?
A little CloudForms history

- CloudForms is on version 3.2
- History is from an acquisition of ManageIQ in late 2012
- Red Hat opensourced it like we do we do everything else
- Now is the ManageIQ community at ManageIQ.org
- It is numbered at 3.2 but is actually the 8th major release
- Customers in every major sector including government, telecom, financials, banking, cloud providers, advertising, aerospace
A little walk through CloudForms
Red Hat's award winning CMP
Overview - Inventory

Security
- Users: 42
- Groups: 61

Configuration
- Packages: 1253
- Init Processes: 9
- Files: 0

Datastore Allocation Summary
- Number of Disks: 2
- Disks Aligned: True
- Thin Provisioning Used: True
- Disks: 10 GB

Virtual Machine "Fed18-Apache"

<table>
<thead>
<tr>
<th>Entry Path</th>
<th>Display Name</th>
<th>Description</th>
<th>Enable Run Levels</th>
<th>Disable Run Levels</th>
</tr>
</thead>
<tbody>
<tr>
<td>/etc/init.d/iscsid</td>
<td>iscsid</td>
<td>Starts and stops login and scanning of iSCSI devices.</td>
<td>0123456</td>
<td>0126</td>
</tr>
<tr>
<td>/etc/init.d/livesys</td>
<td>livesys</td>
<td>Starts and stops login iSCSI daemon.</td>
<td>345</td>
<td>0128</td>
</tr>
<tr>
<td>/etc/init.d/livesys-late</td>
<td>livesys-late</td>
<td></td>
<td>345</td>
<td>0128</td>
</tr>
<tr>
<td>/etc/init.d/netif-transaction</td>
<td>netif-transaction</td>
<td>save/restore network configuration files.</td>
<td>345</td>
<td>0126</td>
</tr>
<tr>
<td>/etc/init.d/netconsole</td>
<td>netconsole</td>
<td></td>
<td>345</td>
<td>0126</td>
</tr>
<tr>
<td>/etc/init.d/network</td>
<td>network</td>
<td>Bring up/down networking</td>
<td>0123456</td>
<td>0123456</td>
</tr>
</tbody>
</table>
## Overview - Relationships

### VM and Instance "Fed18-Apache"

<table>
<thead>
<tr>
<th>Platform Tools</th>
<th>toolsNotInstalled</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Fedora release 18 (Spherical Cow)</td>
</tr>
<tr>
<td>CPU Affinity</td>
<td>None</td>
</tr>
<tr>
<td>Snapshots</td>
<td>None</td>
</tr>
<tr>
<td>Advanced Settings</td>
<td>55</td>
</tr>
<tr>
<td>Resources</td>
<td>Available</td>
</tr>
<tr>
<td>Management Engine GUID</td>
<td>47b7df16-4839-11e4-b801-0050568b70</td>
</tr>
</tbody>
</table>

### Lifecycle

- **Discovered**: Tue Sep 30 00:32:38 UTC 2014
- **Last Analyzed**: Sat Jun 13 20:01:44 UTC 2015
- **Retirement Date**: Never
- **Retirement State**: None

### Relationships

- **Infrastructure Provider**: vCtri-London
- **Cluster**: Production
- **Host**: bid156a03.redhat.com
- **Resource Pool**: Default for Cluster / Deployment Role Production
- **Datastores**: cmbu-shared2
- **Service**: None
- **Parent VM**: None
Overview – All under one view
Overview – Why is this important

• A Cloud Management Platform **should** give you a full picture of what’s going on in your environment.
  – What is inside the container is important
    • Sometimes more important than where or when
    • Being able to detect problems is crucial
Challenges CloudForms helps with

- Hosts configuration
- VM / Instance configuration
- Standards
  - Company
  - Best Practices
  - Industry
  - Regulatory
Why is this important?

• Assets under your control can have many implications
  – Security
    • Prevention
    • Remediation
    • Reporting
  – Fiscal
    • Do you have fiduciary responsibilities in your role?
      – Then it really does matter
Smart State Analysis
Smart State Analysis

- Part of the technology and patent portfolio from ManageIQ
- Allows collection of a deep level of information about what is INSIDE your workloads
  - Why is that important?
  - What kind of data?
    - Application and file versions
    - File contents
    - System settings
    - Init processes
    - Registry keys
  - Metadata stored in the CloudForms database
    - Versioned
    - Comparable
Smart State Analysis – Platform support

- Current
  - Red Hat Enterprise Virtualization (RHEV) via RHEV-M (RHEV Manager)
  - VMware
  - OpenStack

- Future roadmap
  - Microsoft SCVMM
  - Amazon AWS
  - Containers
Wait, I do this in my Configuration Management system...

• Some of this, yes, in many cases
• BUT.....
  – What if the system hasn't phoned home in a while?
  – The system is sitting in an isolated network compartment?
  – What if it's NIC is:
    • Disconnected
    • Misconfigured
    • Unreachable
  – System hasn't been turned on in months?
  – It can't currently boot
  – Is a virtual appliance and you don't normally patch or care for?
• These are valid exception cases
  – So what do you do when one of these use cases apply?
I bet you are going to say CloudForms

• Why yes, I am going to say CloudForms
  – Combination of the following can help in these situations
  – Smart State analysis
  – Compliance
  – Policy
  – Automation
  – Tagging
  – Reporting
Policy & Profiles

- Policy by design breaks down into small concrete items in CloudForms
- Then applied to policy profiles, which are assigned to all or portions of your cloud
- Example of a policy chaining
  - Let’s start with
    - Move
    - Change
    - SmartState
    - Compliance
    - Fails compliance
    - Remediation
ShellShock example

- Very shortly after the vulnerability was reported
  - Someone asked in the ManageIQ community how to check in MIQ and CloudForms
  - Someone created the filter to find in environments
  - Customers quickly ran scans
    - Identified the impact
    - Started appropriate remediation
    - Provided reporting to show compliance
    - Found issue in old shutdown systems
    - Found issue in generic appliances
CloudForms and Satellite

- Power of the combined solutions
  - New features in CloudForms 3.2 uses Satellite hosts and hosts groups
  - Can now do bare metal provisioning via Satellite
  - Satellite can do remediation
  - CloudForms can install agents into systems without the agents
Red Hat Satellite
Errata Management in Satellite 6.1

- Satellite 6.1 has new capabilities to:
  - Quickly address 0-day vulnerabilities such as Heartbleed, ShellShock and GHOST
  - Easily report on Errata required by systems prior to promotion / release
  - Provide detailed email reporting on Errata as it is promoted through its lifecycle
Errata Management in Satellite 6.1

- Errata Has two classifications
  - Applicable – The RPMs in this errata can update RPMs installed on systems in your environment
  - Installable – The RPMs are promoted to an environment/content view where they can be installed.
## Errata Management in Satellite 6.1

<table>
<thead>
<tr>
<th>ID</th>
<th>Title</th>
<th>Type</th>
<th>Current Host Counts</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHEL-202108</td>
<td>firmware bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 applicable, 2 unavailable</td>
<td>5/20/15</td>
</tr>
<tr>
<td>RHEL-2021011</td>
<td>firmware bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 applicable, 2 unavailable</td>
<td>5/19/15</td>
</tr>
<tr>
<td>RHEL-2021013</td>
<td>yum rpm plugin bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 applicable, 2 unavailable</td>
<td>5/18/15</td>
</tr>
<tr>
<td>RHEL-2021006</td>
<td>libgpg-error bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/17/15</td>
</tr>
<tr>
<td>RHEL-2021062</td>
<td>unif Linux bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 applicable, 2 unavailable</td>
<td>5/16/15</td>
</tr>
<tr>
<td>RHEL-2021000</td>
<td>net, network, and ntp bug fix enhancement update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>openstack bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021007</td>
<td>openssl bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021015</td>
<td>libform bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021007</td>
<td>systemd bug fix update</td>
<td>Product Enhancement Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021007</td>
<td>brend bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021007</td>
<td>software bug fix update</td>
<td>Security Advisory, Important</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>software bug fix and enhancement update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>ca-certificates bug fix and enhancement update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>middleware, security, and enhancement update</td>
<td>Security Advisory, Moderate</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>package, security, and enhancement update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>ca-certificates bug fix and enhancement update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>bug fix updated</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
<tr>
<td>RHEL-2021004</td>
<td>bug fix update</td>
<td>Bug Fix Advisory</td>
<td>0 applicable, 2 unavailable</td>
<td>5/15/15</td>
</tr>
</tbody>
</table>

#redhat #rhsummit
## Errata Management in Satellite 6.1

<table>
<thead>
<tr>
<th>Errata ID</th>
<th>Title</th>
<th>Type</th>
<th>Content Host Counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>RHBA-2015:1018</td>
<td>lvm2 bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 Applicable, 0 Installable</td>
</tr>
<tr>
<td>RHBA-2015:1016</td>
<td>bind bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 Applicable, 0 Installable</td>
</tr>
<tr>
<td>RHBA-2015:1013</td>
<td>yum-rhn-plugin bug fix update</td>
<td>Bug Fix Advisory</td>
<td>2 Applicable, 0 Installable</td>
</tr>
<tr>
<td>RHBA-2015:0966</td>
<td>libgcrypt bug fix update</td>
<td>Bug Fix Advisory</td>
<td>8 Applicable, 0 Installable</td>
</tr>
<tr>
<td>RHBA-2015:0962</td>
<td>util-linux bug fix update</td>
<td>Bug Fix Advisory</td>
<td>8 Applicable, 0 Installable</td>
</tr>
</tbody>
</table>
Errata Management in Satellite 6.1

Ivrn2 bug fix update

Details

- Advisory: B-RP-2015-0016
- CVE:
- Type: Bug Fix Advisory
- Security:
- Issued: 5/26/15
- Last Updated On: 5/26/15
- Redhat Suggested:

Description

The ivrn2 package includes complete support for handling read and write operations on physical volumes, cloning volume groups from one or more physical volumes and cloning one or more logical volumes in volume groups.

This update fixes the following bug:

* Previously, the "lvs pv" command did not correctly honor the given physical volume name and the entire list of volume groups on the device. As a consequence, executing the "lvdisplay" command to inspect and properly reissue lvs on physical volumes (PVs) does not work. An upstream patch has been backported to fix this bug, and "lvdisplay" now imports and reissues lvs successfully (RHEL-2015-3211).

Users of ivrn2 are advised to upgrade to these updated packages, which fix this bug.

Solutions
Errata Management in Satellite 6.1

- Incremental Updates
  - A method for releasing a fix (and just that fix) for a critical flaw (either bugfix or security)
  - Versioned just like any other promotion (with a minor release number)
Errata Management in Satellite 6.1

- Example:
  - Version 7 of My_Content_View in Dev
  - Version 4 of My_Content_View in QA
  - Version 2 of My_Content_View in Prod

- Heartbleed hits. What do you do?
Errata Management in Satellite 6.1

- Satellite 6.0
  - Update My_Content_View to version 8 (including the fix for Heartbleed)
  - Promote version 8 to Dev, then QA, then Production
  - We've addressed Heartbleed!!
  - But we've also released content way ahead of schedule
Errata Management in Satellite 6.1

- Satellite 6.1
  - Update each Content View with the fixes for Heartbleed
    - Update Dev to 7.1
    - Update QA to 4.1
    - Update Prod to 2.1
  - We call this an 'incremental update'
How can CloudForms leverage this

• Given a hostname, from CloudForms we'll
  – Make an API call to Satellite to see if the identified errata is available in a content view that a host has access to:
    • If yes, then install it.
    • If no, then create an incremental update.
      – Publish incremental update
      – (optionally) apply the update
Errata Management in Satellite 6.1
Errata Management in Satellite 6.1
Q & A

Please move to the microphones so that all may hear and the recordings will catch your questions.
More Talks:

Thu, 2:30pm, Room 206 - Red Hat CloudForms roadmap

Fri, 11:00am, Room 313 - Cloud automation: Migrating 1000+ servers from vCloud to OpenStack

Other:

Tue-Thu, Exhibition Floor - CloudForms and Hybrid Cloud Management Pods

Thu, 4:00pm, Sheraton Boston - ManageIQ birds of a feather Session
More questions?

The presenters will be available after this session just outside this room.

We also have people at the CloudForms and Satellite booths on the show floor.
HAVE MORE QUESTIONS ON SECURITY?

Speak one-on-one with Red Hat Product Security experts in Customer Central

Hall A, First floor