

RED HAT
SUMMIT

BOSTON, MA
JUNE 23-26, 2015

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 open sourced 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"








Service Path	Display Name	Description	Enable Run Levels	Disable Run Levels
etc/passwd				0123456
etc/functions				
etc/iscsi		Starts and stops login and scanning of iSCSI devices.	345	0126
etc/iscsid		Starts and stops login iSCSI daemon.	345	0126
etc/livesys			345	0126
etc/livesys-late			345	0126
etc/netcf-transaction		save/restore network configuration files		
etc/netconsole				0123456
etc/network		Bring up/down networking		0123456

Overview - Relationships

VM and Instance "Fed18-Apache"

Platform Tools	toolsNotInstalled
Operating System	 Fedora release 18 (Spherical Cow)
CPU Affinity	
Snapshots	 None
Advanced Settings	 55
Resources	Available
Management Engine GUID	47b7df46-4839-11e4-b801-005056a9bb70

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	

Relationships	
Infrastructure Provider	 vCntr-London
Cluster	 Production
Host	 bldr15ca03.redhat.com
Resource Pool	 Default for Cluster / Deployment Role Production
Datstores	 cmbu-shared2
Service	 None
Parent VM	 None

Overview – All under one view

Search

VMs and Instances - Filtered by "Demo Level 1" ([clear](#))

<input type="checkbox"/>				1	CentOS-LB
<input type="checkbox"/>				0	CFME_1
<input type="checkbox"/>				0	DemoMaster
<input type="checkbox"/>				0	Demo ...SCVMM
<input type="checkbox"/>				1	DevAI...-John
<input type="checkbox"/>				0	devops-jdoe
<input type="checkbox"/>				0	DevTeam-Bill
<input type="checkbox"/>				0	Domai...imary
<input type="checkbox"/>				0	Fed18-Apache
<input type="checkbox"/>				0	jenkins-opsA
<input type="checkbox"/>				0	produ...rhel6
<input type="checkbox"/>				0	produ...rhel7
<input type="checkbox"/>				0	rhel6
<input type="checkbox"/>				1	RHEL7-LdTst
<input type="checkbox"/>				0	scvmm
<input type="checkbox"/>				0	sql
<input type="checkbox"/>				0	test2
<input type="checkbox"/>				0	WordPress

Overview – Why is this important

- A Cloud Management Platform **should** give you a full picture fo what's going on in your environement.
 - 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

RED HAT SATELLITE Red Hat Access  Richard Jerrido

Default Organization@Default Location Monitor Content Containers Hosts Configure Infrastructure Access Insights Administer

Errata

All Repositories Applicable Installable

Search... Showing 38 of 38 (1206 Total) 0 Selected Apply Errata






<input type="checkbox"/>	Errata ID	Title	Type	Content Host Counts	Updated
<input type="checkbox"/>	RHBA-2015:1018	lvm2 bug fix update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	5/20/15
<input type="checkbox"/>	RHBA-2015:1016	bind bug fix update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	5/19/15
<input type="checkbox"/>	RHBA-2015:1013	yum-rhn-plugin bug fix update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	5/18/15
<input type="checkbox"/>	RHBA-2015:0966	libcrypt bug fix update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0962	util-linux bug fix update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0965	nss, nss-util, and nspr bug fix and enhancement update	🔧 Bug Fix Advisory	8 Applicable, 3 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0984	openssh bug fix update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0975	openssl bug fix update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0978	libcap bug fix update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHEA-2015:0972	systemd enhancement update	🔧 Product Enhancement Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0974	binutils bug fix update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHSA-2015:0987	Important: kernel security and bug fix update	⚠ Security Advisory - Important	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0985	selinux-policy bug fix and enhancement update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0964	ca-certificates bug fix and enhancement update	🔧 Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHSA-2015:0986	Moderate: kexec-tools security, bug fix, and enhancement update	⚠ Security Advisory - Moderate	8 Applicable, 0 Installable	5/12/15
<input type="checkbox"/>	RHBA-2015:0953	selinux-policy bug fix update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	5/11/15
<input type="checkbox"/>	RHBA-2015:0948	ca-certificates bug fix and enhancement update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	5/6/15
<input type="checkbox"/>	RHBA-2015:0950	lvm2 bug fix update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	5/6/15
<input type="checkbox"/>	RHBA-2015:0926	nss, nss-util, and nspr bug fix and enhancement update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	5/5/15
<input type="checkbox"/>	RHBA-2015:0915	dracut bug fix update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	4/29/15
<input type="checkbox"/>	RHEA-2015:0913	tzdata enhancement update	🔧 Product Enhancement Advisory	8 Applicable, 8 Installable	4/28/15
<input type="checkbox"/>	RHBA-2015:0871	dbus bugfix update	🔧 Bug Fix Advisory	2 Applicable, 0 Installable	4/22/15

Errata Management in Satellite 6.1

Errata

All Repositories Applicable Installable

Search... Showing 38 of 38 (1206 Total)

<input type="checkbox"/> Errata ID	Title	Type	Content Host Counts
<input type="checkbox"/> RHBA-2015:1018	lvm2 bug fix update	 Bug Fix Advisory	2 Applicable, 0 Installable
<input type="checkbox"/> RHBA-2015:1016	bind bug fix update	 Bug Fix Advisory	2 Applicable, 0 Installable
<input type="checkbox"/> RHBA-2015:1013	yum-rhn-plugin bug fix update	 Bug Fix Advisory	2 Applicable, 0 Installable
<input type="checkbox"/> RHBA-2015:0966	libcrypt bug fix update	 Bug Fix Advisory	8 Applicable, 0 Installable
<input type="checkbox"/> RHBA-2015:0962	util-linux bug fix update	 Bug Fix Advisory	8 Applicable, 0 Installable

Errata Management in Satellite 6.1

The screenshot displays the Red Hat Satellite web interface for Errata Management. The top navigation bar includes the Red Hat Satellite logo, the current organization and location, and a menu with options like Monitor, Content, Containers, Hosts, Configure, Infrastructure, and Access Insights. The user is identified as Richard Jerrido.

The main content area is titled "Errata" and features a search bar, a dropdown for "All Repositories", and checkboxes for "Applicable" (checked) and "Installable". It shows "Showing 38 of 38 (1206 Total)" and "0 Selected" with an "Apply Errata" button.

On the left, a list of errata is shown, with "RHBA-2015:1018" selected. The right pane displays the details for this errata, titled "lvm2 bug fix update".

Errata Details:

- Advisory:** RHBA-2015:1018
- CVEs:** N/A
- Type:** Bug Fix Advisory
- Severity:** N/A
- Issued:** 5/20/15
- Last Updated On:** 5/20/15
- Reboot Suggested?:** No

Topic: Updated lvm2 packages that fix one bug are now available for Red Hat Enterprise Linux 6.

Description: The lvm2 packages include complete support for handling read and write operations on physical volumes, creating volume groups from one or more physical volumes and creating one or more logical volumes in volume groups.

This update fixes the following bug:

- * Previously, the "lvm pvs" command did not correctly honor the given physical volume clone and therefore failed to scan for a volume group (VG) on the device. As a consequence, running the "vgimportclone" command to import and properly rename VGs on physical volumes (PV) clones failed. An upstream patch has been backported to fix this bug, and "vgimportclone" now imports and renames duplicate VGs successfully. (BZ#1222111)

Users of lvm2 are advised to upgrade to these updated packages, which fix this bug.

Solution:

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

RED HAT SATELLITE Red Hat Access  Richard Jerrido
 Administrator

Default Organization@Default Location Monitor Content Containers Hosts Configure Infrastructure Access Insights

Errata

All Repositories Applicable Installable 0 Selected Apply Errata

Search... Showing 38 of 38 (1206 Total)

Errata ID

- RHBA-2015:1018 ▶
- RHBA-2015:1016
- RHBA-2015:1013
- RHBA-2015:0966
- RHBA-2015:0962
- RHBA-2015:0965
- RHBA-2015:0984
- RHBA-2015:0975
- RHBA-2015:0978
- RHEA-2015:0972
- RHBA-2015:0974
- RHSA-2015:0987
- RHBA-2015:0985
- RHBA-2015:0964
- RHSA-2015:0986
- RHBA-2015:0953
- RHBA-2015:0948
- RHBA-2015:0950
- RHBA-2015:0926
- RHBA-2015:0915
- RHEA-2015:0913
- RHBA-2015:0871

lvm2 bug fix update ✕ Close

Details Content Hosts Repositories

Apply To Content Hosts

Only show content hosts where lvm2 bug fix update is currently installable in the host's Lifecycle Environment.

Filter by Environment Showing 2 of 2 (2 Total)

Search... 1 Selected Apply to Hosts

<input type="checkbox"/> Name	OS	Environment	Content View
<input checked="" type="checkbox"/> devnode-0001.example.com	Red Hat Enterprise Linux Server 6.6	Development	RHEL6_Base_SOE
<input type="checkbox"/> devnode-0002.example.com	Red Hat Enterprise Linux Server 6.6	Development	RHEL6_Base_SOE

Errata Management in Satellite 6.1

The screenshot shows the Red Hat Satellite web interface. At the top, the navigation bar includes 'RED HAT SATELLITE', 'Default Organization@Default Location', and various menu items like 'Monitor', 'Content', 'Containers', 'Hosts', 'Configure', 'Infrastructure', and 'Access Insights'. The user is identified as 'Richard Jerrido' with an 'Administrator' role.

The main content area is titled 'Errata'. It features a search bar, a dropdown for 'All Repositories', and checkboxes for 'Applicable' (checked) and 'Installable'. Below this is a list of errata with 'RHBA-2015:1018' selected. A modal dialog box is open for 'lvm2 bug fix update', showing the 'Content Hosts' tab. The dialog contains the following text and table:

Apply RHBA-2015:1018

These Errata are not installable via your published Content View versions running on the selected hosts. The new Content View Versions (specified below) will be created which will make this Errata Installable in the host's Environment. This new version will replace the current version in your host's Lifecycle Environment. To install these errata immediately on hosts after publishing check the box below.

Content View	Version	Environment	Host Count
RHEL6_Base_SOE	6.4	Development	1

Apply Errata to Content Hosts immediately after publishing.

Buttons: Cancel, Confirm, Close

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.

RED HAT **SUMMIT**

13821 - Hands on with Red Hat CloudForms

**LEARN. NETWORK.
EXPERIENCE OPEN SOURCE.**

HAVE MORE QUESTIONS ON SECURITY?

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

Hall A, First floor