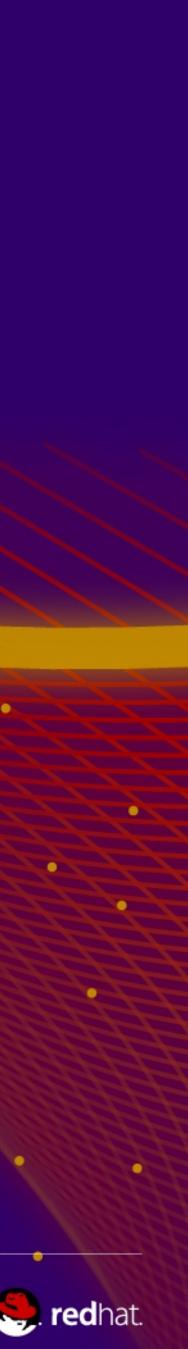


BOSTON, MA JUNE 23-26, 2015

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

Brad Ascar Field Product Manager - CloudForms 24 June 2015





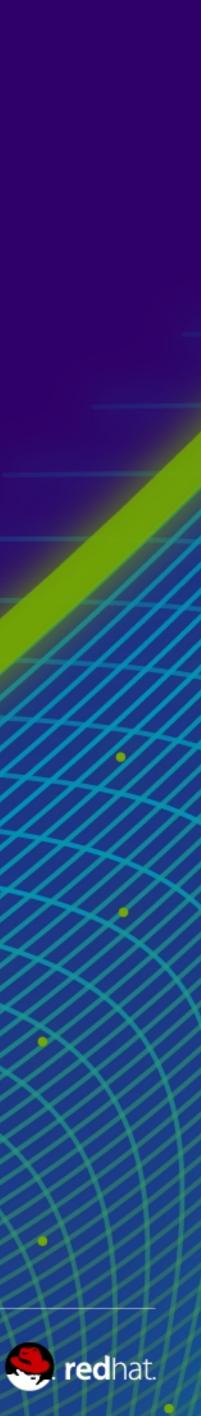
Brad Ascar is Field Product Manager for CloudForms at Red Hat.



#redhat #rhsummit

He has worked as a developer/architect in Enterprise IT, IT Operations, R&D, medium and small startups in his 30+ year career.

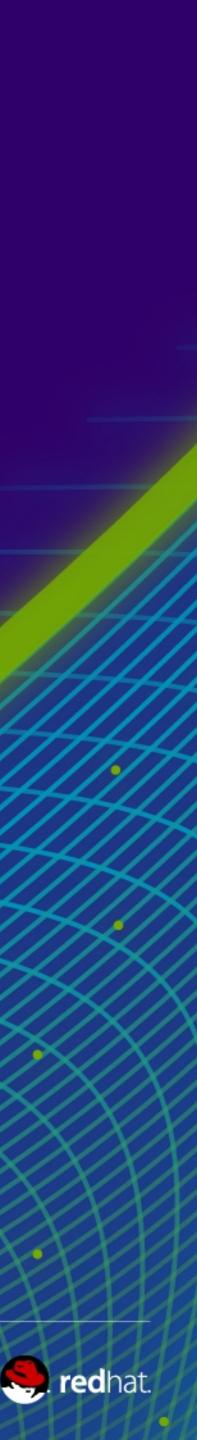




Rich Jerrido has worked with Linux since 1999 and with virtualization since 2000. Rich is the Technical Product Marketing Manager for Red Hat Satellite, assisting customers in efficiently deploying their infrastructures in support of their business objectives. Particularly, he focuses on lifecycle management, content management and governance of all things Red Hat: servers,

content, configuration and subscriptions



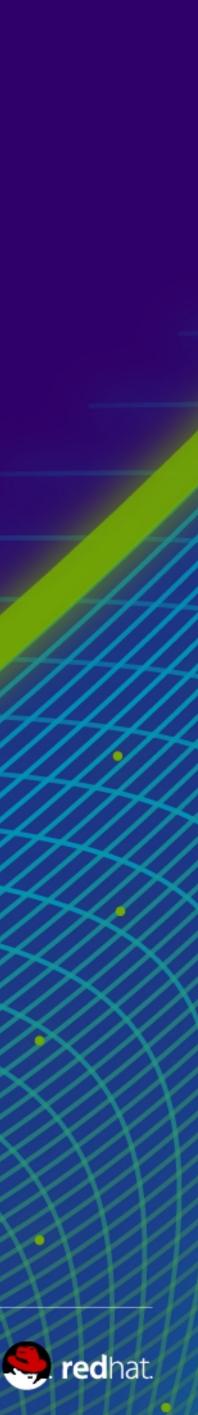


A little history

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?

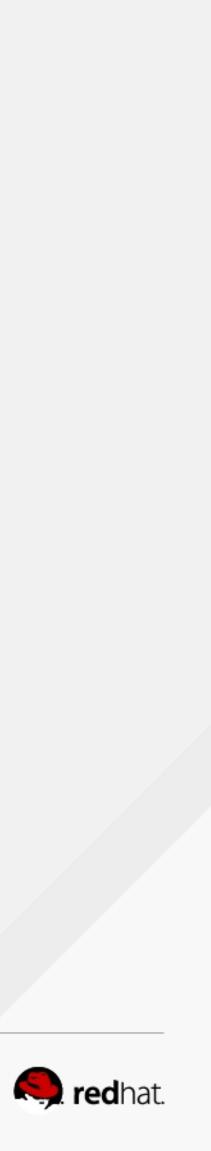




A little CloudForms history

- CloudForms is on version 3.2
- telecom, financials, banking, cloud providers, advertising,

- History is from an acquisition of ManagelQ in late 2012 Red Hat opensourced it like we do we do everything else Now is the ManagelQ community at ManagelQ.org • It is numbered at 3.2 but is actually the 8th major release •Customers in every major sector including government, aerospace



A little walk through CloudForms Red Hat's award winning CMP

#redhat #rhsummit

.

.

. . .



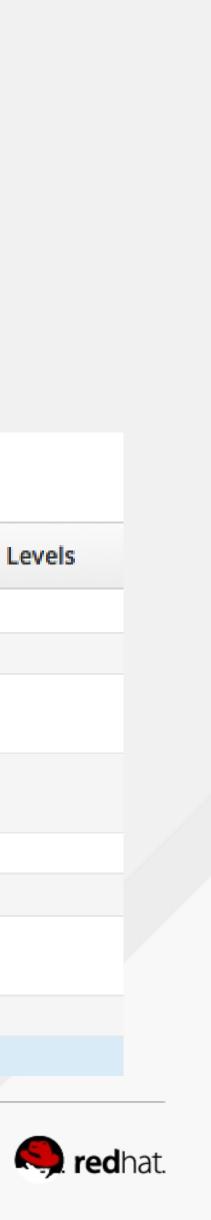


Overview - Inventory

Security		
Users	1 42	
Groups	<u>\$</u> 61	

Configuration	
Packages	1253 Jun
Init Processes	* 9
Files	► 0

					ual Mach	ine "Fed18-A	Apache"		
Datastore Allocation Summary							1		
Number of Disks	<u></u> 2				age Path	Display Name	Description	Enable Run Levels	Disble Run Levels
Disks Aligned	True				t.d/ebtables				0123456
Thin Provisioning Used	True				t.d/functions				
Disks	10 GB		t.d/iscsi		Starts and stops login and scanning of iSCSI devices.	345	0126		
		Ф	iscsid	/etc/rc.d/	'init.d/iscsid		Starts and stops login iSCSI daemon.	345	0126
		\$	livesys	/etc/rc.d/	init.d/livesys			345	0126
		\$	livesys-late	/etc/rc.d/	init.d/livesys-late			345	0126
		•	netcf-transaction	/etc/rc.d/	init.d/netcf-		save/restore network		
		*	neto-transaction	transacti	on		configuration files		
		\$	netconsole	/etc/rc.d/	init.d/netconsole				0123456
			network	/etc/rc.d/	init.d/network		Bring up/down networking		0123456



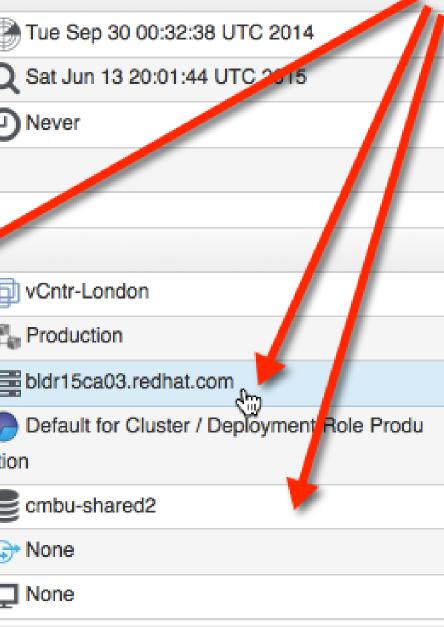
Overview - Relationships

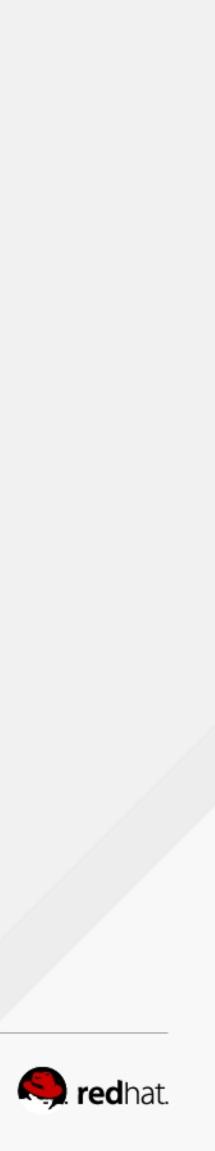
VM and Instance "Fed18-Apache"

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
Lifecvcle	

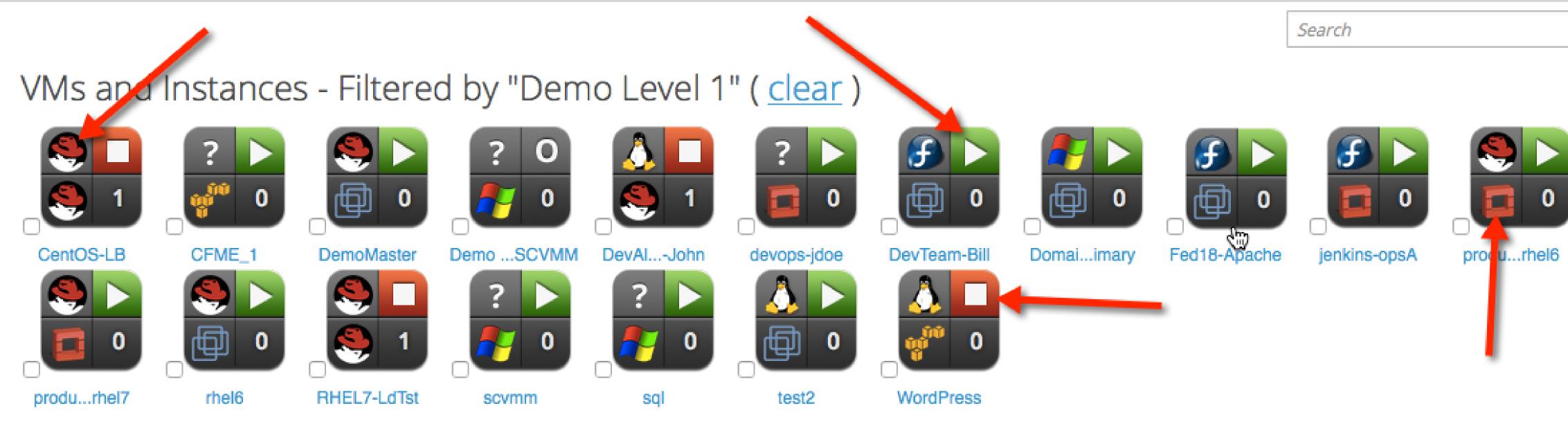
Lifecycle	
Discovered	Ē
Last Analyzed	Q
Retirement Date	Θ
Retirement State	

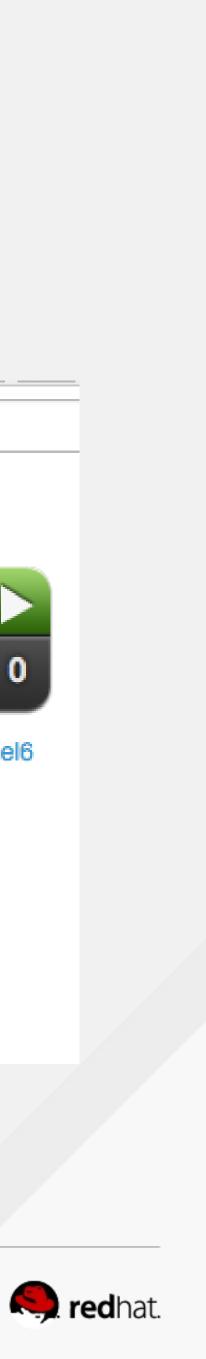
Relationships	
Infrastructure Provider	þ
Cluster	84
Host	
Resource Pool	ctic
Datastores	
Service	Ð
Parent VM	Ţ





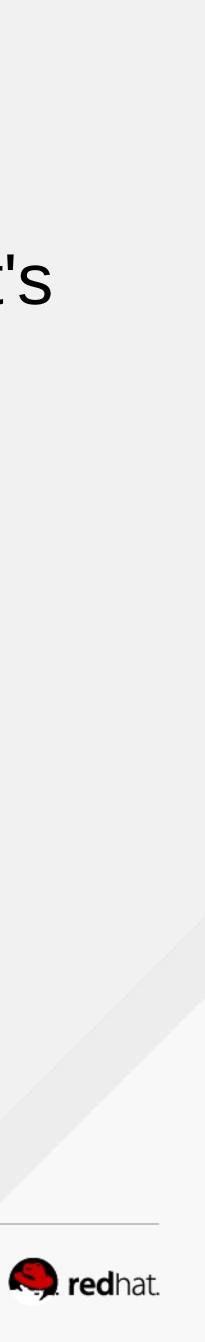
Overview – All under one view





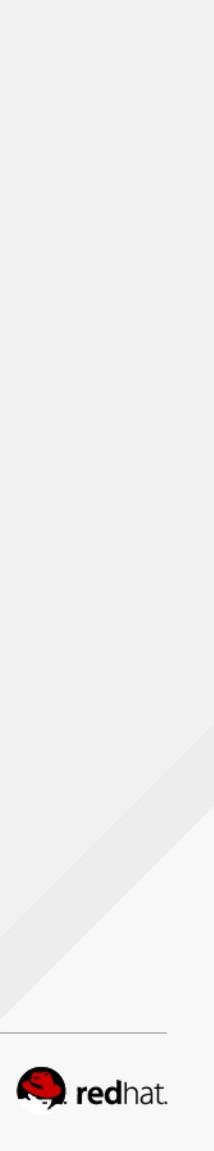
Overview – Why is this important

- 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

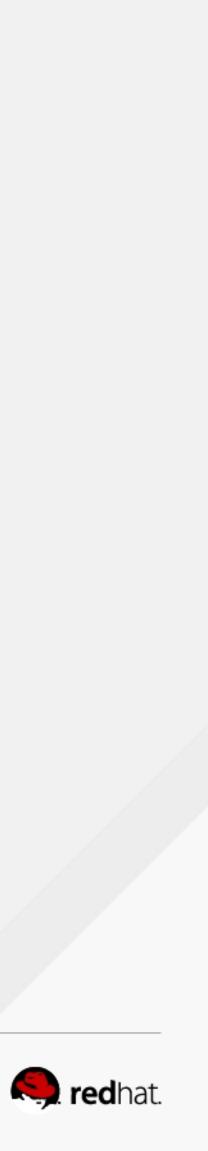


Why is this important?

- - -Security
 - Prevention
 - Remediation
 - •Reporting

-Fiscal Do you have fudiciary responsibilities in your role? -Then it really does matter

Assets under your control can have many implications



Smart State Analysis

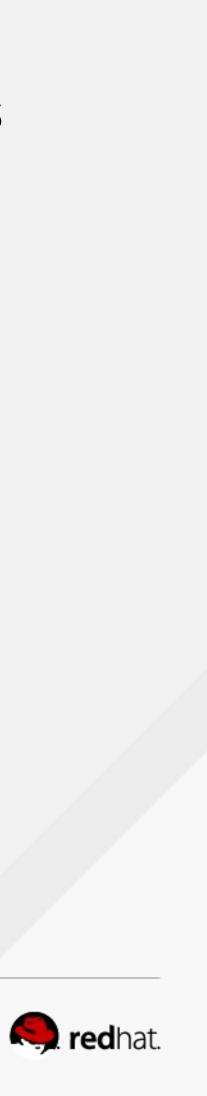






Smart State Analysis

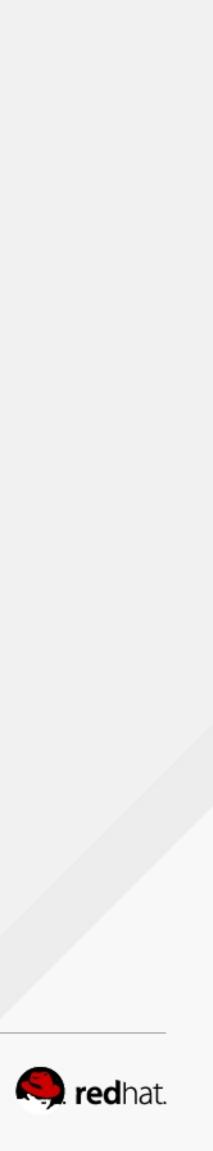
- Part of the technology and patent portfolio from ManagelQ
- Allows collection of a deep level of information about what is INSIDE your workloads
 - -Why is that important?
 - -What kind of data?
 - Application and file versions
 - File contents
 - System settings
 - Init processes
 - Registry keys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



Smart State Analysis – Platform support

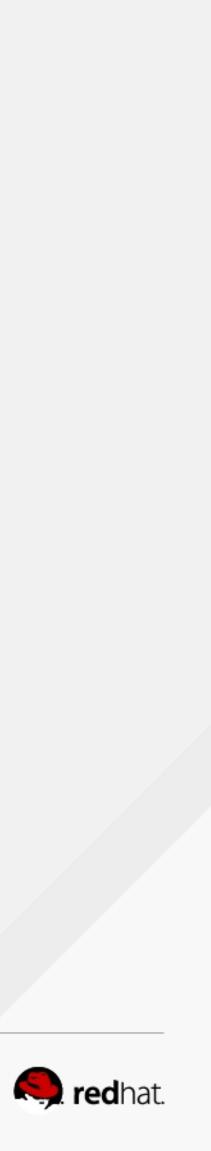
• Current

- -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...

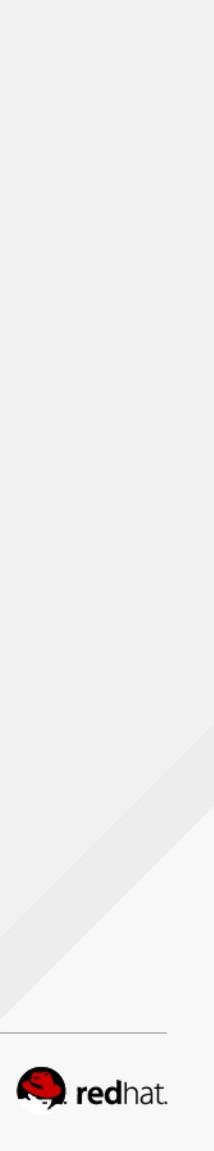
- Some of this, yes, in many cases
- BUT.....
 - -What if the system hasn't phoned home in a while?
 - The system is sitting in an isolated network compartment?
 - -What if it's NIC is:
 - Disconnected
 - Misconfigured
 - Unreachable
 - System hasn't been turned on in months?
 - It can't currently boot
 - 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

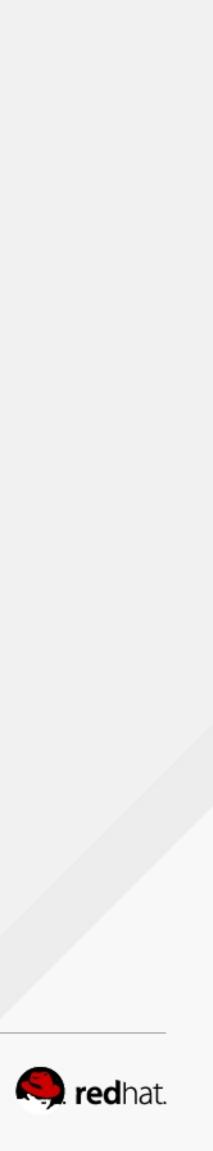
- Why yes, I am going to say CloudForms
 - -Combination of the following can help in these situations
 - -Smart State analysis
 - -Compliance
 - -Policy
 - -Automation
 - -Tagging
 - -Reporting

dForms an help in these situations



- 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

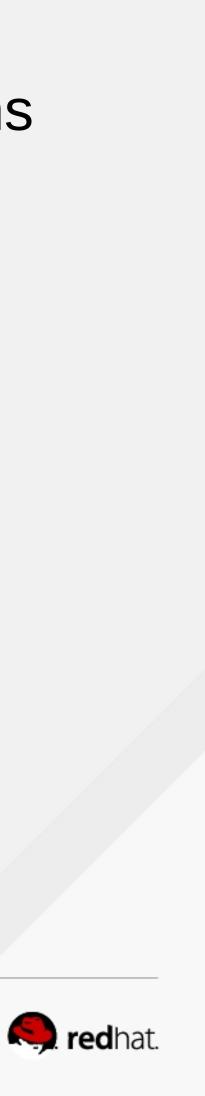
Policy & Profiles



ShellShock example

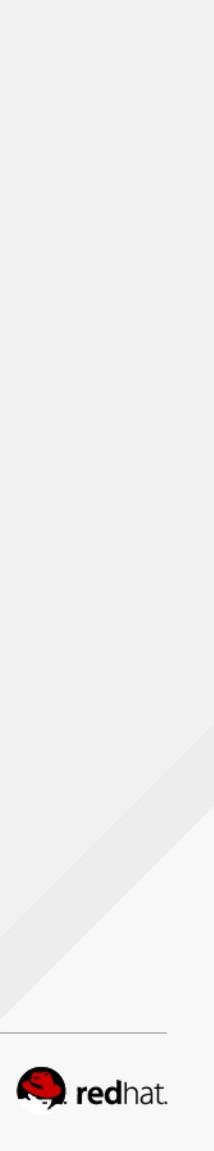
- Very shortly after the vulnerability was reported
 - -Someone asked in the ManagelQ community how to check in MIQ and CloudForms - Someone created the filter to find in environments

 - -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

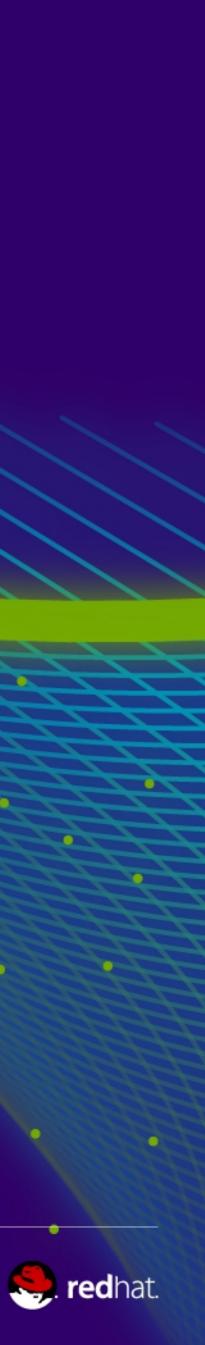
- Power of the combined solutions
 - -New features in CloudForms 3.2 uses Satellite hosts and hosts groups
 - Can now do bare metal provisioning via Satellite
 - Satellite can do remediation
 - CloudForms can install agents into systems without the agents



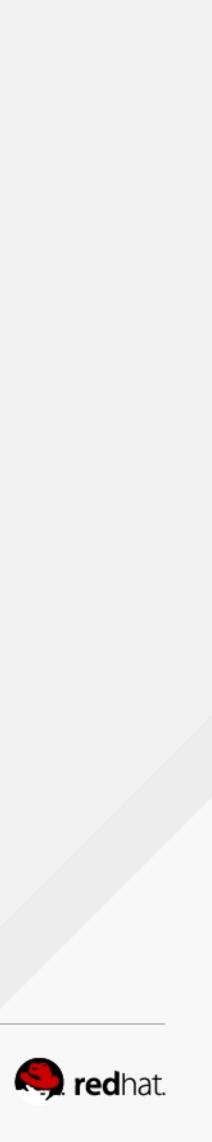
Red Hat Satellite

#redhat #rhsummit

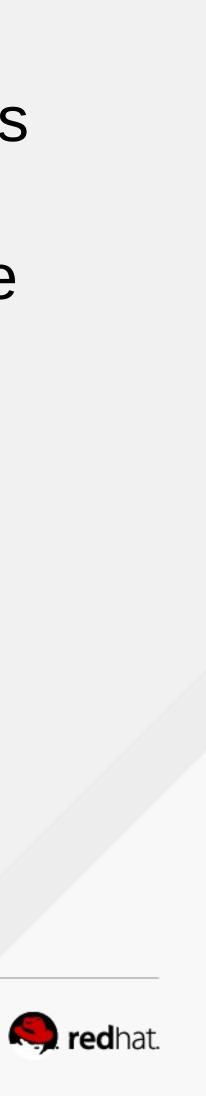




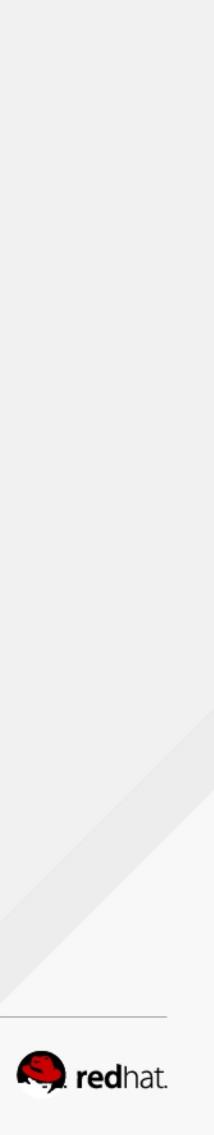
- Satellite 6.1 has new capabilities to:
 - -Quickly address 0-day vulnerabilities such as Heartbleed, ShellShock and GHOST
 - Easily report on Errata required by systems prior to promotion / release
 Provide detailed email reporting on Errata as it is promoted through its
 - Provide detailed email reporting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



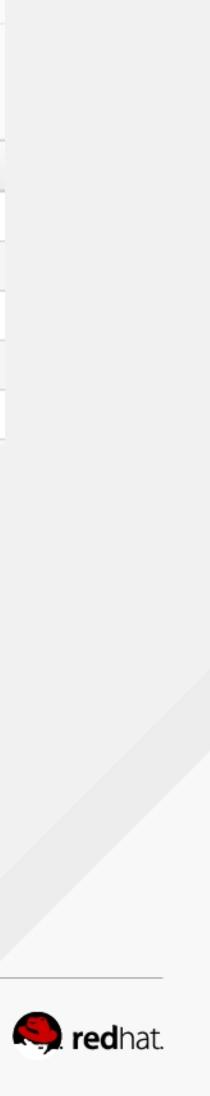
- Errata Has two classifications
 - Applicable The RPMs in this errata can update RPMs installed on systems in your environment
 - Installable The RPMs are promoted to an environment/content view where they can be installed.



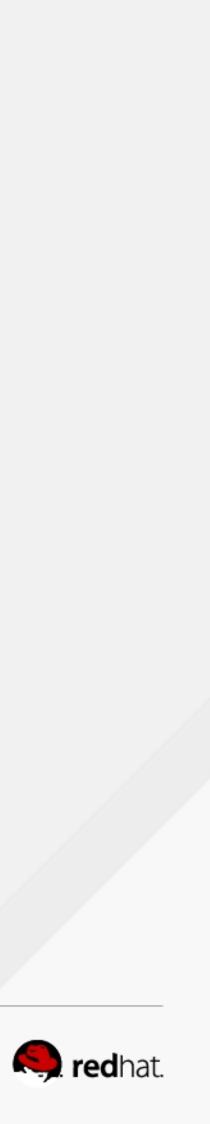
R	RED HAT SATELLITE Red Hat Access × Richard Jerrido × Default Organization@Default Location × Monitor × Containers × Hosts × Configure × Infrastructure × Access Insights × Administer × Administer × Access Insights × Access Insights × Access Insights × Administer ×						
Er	Errata						
	All Repositories Installable Search Q Showing 38 of 38 (1206 Total)						
	Errata ID	Title	Туре	Content Host Counts	Updated		
	RHBA-2015:1018	lvm2 bug fix update	I Bug Fix Advisory	2 Applicable, 0 Installable	5/20/15		
	RHBA-2015:1016	bind bug fix update	I Bug Fix Advisory	2 Applicable, 0 Installable	5/19/15		
	RHBA-2015:1013	yum-rhn-plugin bug fix update	I Bug Fix Advisory	2 Applicable, 0 Installable	5/18/15		
	RHBA-2015:0966	libgcrypt bug fix update	I Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0962	util-linux bug fix update	I Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0965	nss, nss-util, and nspr bug fix and enhancement update	n Bug Fix Advisory	8 Applicable, 3 Installable	5/12/15		
	RHBA-2015:0984	openssh bug fix update	n Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0975	openssl bug fix update	n Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0978	libpcap bug fix update	n Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHEA-2015:0972	systemd enhancement update	Product Enhancement Advisory	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0974	binutils bug fix update	n Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHSA-2015:0987	Important: kernel security and bug fix update	A Security Advisory - Important	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0985	selinux-policy bug fix and enhancement update	n Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0964	ca-certificates bug fix and enhancement update	n Bug Fix Advisory	8 Applicable, 0 Installable	5/12/15		
	RHSA-2015:0986	Moderate: kexec-tools security, bug fix, and enhancement update	A Security Advisory - Moderate	8 Applicable, 0 Installable	5/12/15		
	RHBA-2015:0953	selinux-policy bug fix update	n Bug Fix Advisory	2 Applicable, 0 Installable	5/11/15		
	RHBA-2015:0948	ca-certificates bug fix and enhancement update	I Bug Fix Advisory	2 Applicable, 0 Installable	5/6/15		
	RHBA-2015:0950	lvm2 bug fix update	I Bug Fix Advisory	2 Applicable, 0 Installable	5/6/15		
	RHBA-2015:0926	nss, nss-util, and nspr bug fix and enhancement update	I Bug Fix Advisory	2 Applicable, 0 Installable	5/5/15		
	RHBA-2015:0915	dracut bug fix update	I Bug Fix Advisory	2 Applicable, 0 Installable	4/29/15		
	RHEA-2015:0913	tzdata enhancement update	Product Enhancement Advisory	8 Applicable, 8 Installable	4/28/15		
	RHBA-2015:0871	dbus bugfix update	I Bug Fix Advisory	2 Applicable, 0 Installable	4/22/15		



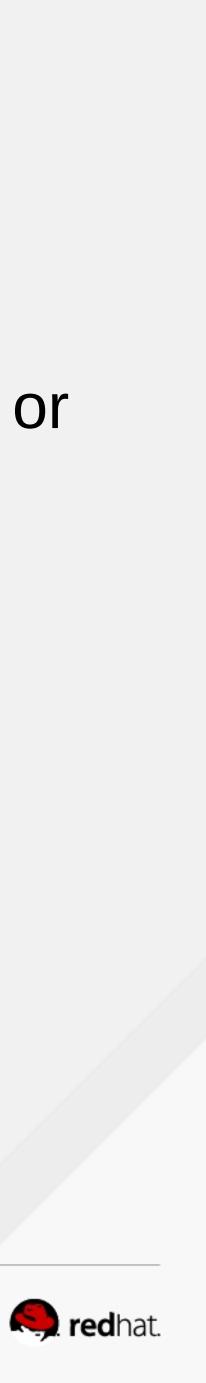
Errata						
All RepositoriesApplicableSearchInstallableShowing 38 of 38 (1206 Total)						
Errata ID	Title	Туре	Content Host Counts			
RHBA-2015:1018	lvm2 bug fix update	₩ Bug Fix Advisory	2 Applicable, 0 Installable			
RHBA-2015:1016	bind bug fix update	₩ Bug Fix Advisory	2 Applicable, 0 Installable			
RHBA-2015:1013	yum-rhn-plugin bug fix update	₩ Bug Fix Advisory	2 Applicable, 0 Installable			
RHBA-2015:0966	libgcrypt bug fix update	🕂 Bug Fix Advisory	8 Applicable, 0 Installable			
RHBA-2015:0962	util-linux bug fix update	₩ Bug Fix Advisory	8 Applicable, 0 Installable			



cata			
rata			
Repositories	🚽 🔽 Applicable 🗌 Installable		
arch	Q Showing 38 of 38 (1206 Total)		0 Selected App
Errata ID			
RHBA-2015:1018 >	Ivm2 bug fix update		×
RHBA-2015:1016	Details Content Hosts Reposi	ories	
RHBA-2015:1013			
HBA-2015:0966	Advisory	RHBA-2015:1018	
HBA-2015:0962	CVEs	N/A	
	Type	Bug Fix Advisory	
HBA-2015:0965	Severity	N/A 5/20/15	
HBA-2015:0984	Last Updated On	5/20/15	
HBA-2015:0975	Reboot Suggested?	No	
HBA-2015:0978	Торіс		
HEA-2015:0972	Updated lvm2 packages that fix one bug are now a	ailable for Red Hat Enterprise	
HBA-2015:0974	Linux 6.		
HSA-2015:0987	Description		
HBA-2015:0985	The lvm2 packages include complete support for ha	ndling read and write	
HBA-2015:0964	operations on physical volumes, creating volume g		
HSA-2015:0986	volumes and creating one or more logical volumes	a volume groups.	
	This update fixes the following bug:		
HBA-2015:0953	* Previously, the "lvm pvs" command did not correc	y honor the given physical	
HBA-2015:0948	volume clone and therefore failed to scan for a volu	ne group (VG) on the device.	
IBA-2015:0950	As a consequence, running the "vgimportclone" con rename VGs on physical volumes (PV) clones failed		
HBA-2015:0926	backported to fix this bug, and "vgimportclone" nov		
HBA-2015:0915	duplicate VGs successfully. (BZ#1222111)		
HEA-2015:0913	Users of lvm2 are advised to upgrade to these upd	ed packages, which fix this	
HBA-2015:0871	bug.		
	Solution		

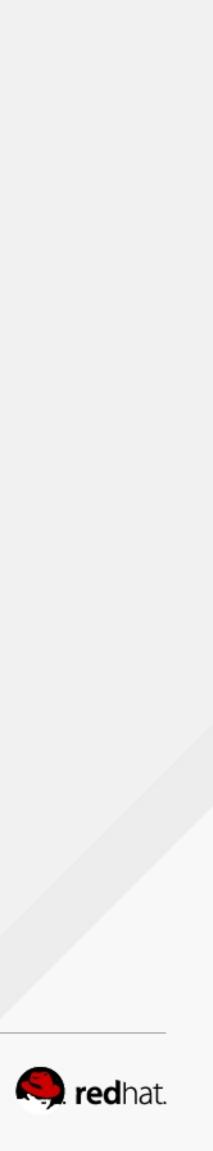


- Incremental Updates
 - A method for releasing a fix (and just that fix) for a critical flaw (either bugfix or security)
 - -Versioned just like any other promotion (with a minor release number)



- 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?

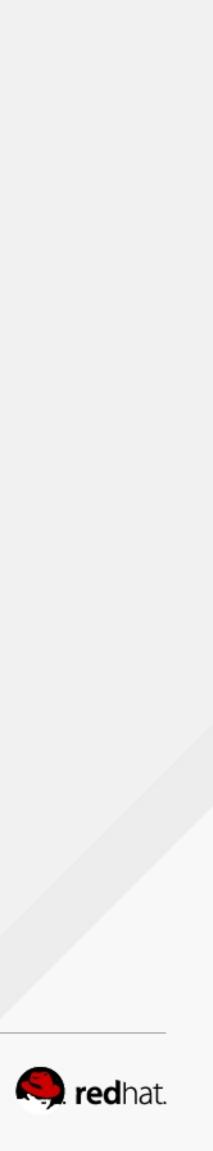
Dev QA Prod



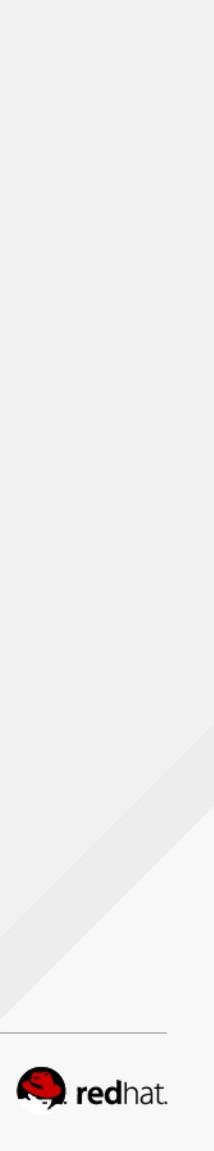
- Satellite 6.0

 - -Promote version 8 to Dev, then QA, then Production
 - -We've addressed Heartbleed!!
 - But we've also released content way ahead of schedule

-Update My_Content_View to version 8 (including the fix for Heartbleed)

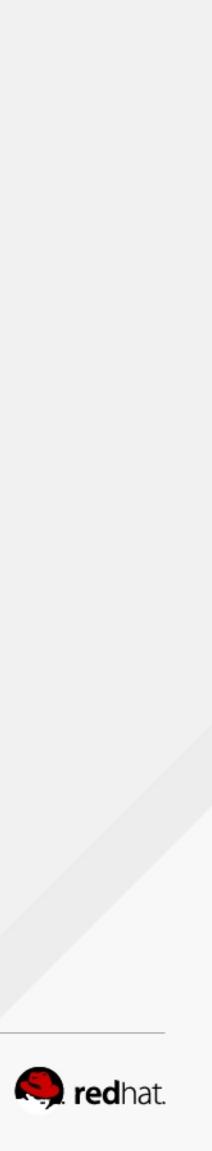


- Satellite 6.1
 - -Update each Content View with the fixes for Heartbleed
 - Update Dev to 7.1
 - Update QA to 4.1
 - Update Prod to 2.1
 - We call this an 'incremental update'

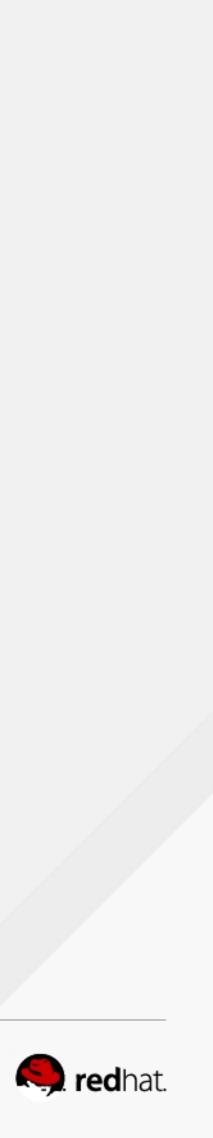


How can CloudForms leverage this

- 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

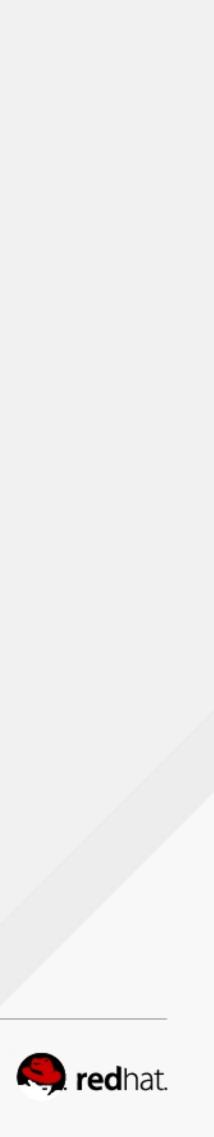


RED HAT SATELLITE				Red Hat Access 👻 📃 Richard Jerrido 🗠
Default Organization@Default Location ~ Mor	nitor 🗸 Content 🗸 Containers 🗸 Hosts 🗸	∽ Configure ∽ Infrastructure ∽ Access Insights ∽		Administer 🗸
Errata				
All Repositories	- Applicable Installable			
Search	Q Showing 38 of 38 (1206 Total)			0 Selected Apply Errata
Errata ID				
RHBA-2015:1018 >	lvm2 bug fix update			* Close
RHBA-2015:1016	Details Content Hosts Repositor	ies		
RHBA-2015:1013				
RHBA-2015:0966	Apply To Content Hosts			
RHBA-2015:0962		is currently installable in the host's Lifecycle Environment.		
RHBA-2015:0965	Filter by Environment	_		
RHBA-2015:0984	Search	Q Showing 2 of 2 (2 Total)		1 Selected Apply to Hosts
RHBA-2015:0975	Name	OS	Environment	Content View
RHBA-2015:0978	devnode-0001.example.com	Red Hat Enterprise Linux Server 6.6	Development	RHEL6_Base_SOE
RHEA-2015:0972	devnode-0002.example.com	Red Hat Enterprise Linux Server 6.6	Development	RHEL6_Base_SOE
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				



RED HAT SATELLITE				Red Hat Access 👻 🔝 Richard Jerrido 🗡	
Default Organization@Default Location ~ Mon	nitor ∽ Content ∽ Containers ∽ Hosts ∽ Configur	∙e ∨ Infrastructure ∨ Access Insights ∨		Administer 🗸	
Errata					
All Repositories	- Applicable Installable				
Search	Q Showing 38 of 38 (1206 Total)			0 Selected Apply Errata	
Errata ID					
RHBA-2015:1018 >	lvm2 bug fix update			× Close	
RHBA-2015:1016	Details Content Hosts Repositories				
RHBA-2015:1013					
RHBA-2015:0966	Errata List » Select Content Hosts » Confirm				
RHBA-2015:0962					
RHBA-2015:0965	Apply RHBA-2015:1018				
RHBA-2015:0984	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 your host's Lifecycle Environment. To install these errata immediately on hosts after publishing check the box below.				
RHBA-2015:0975					
RHBA-2015:0978	Content View	Version	Environment	Host Count	
RHEA-2015:0972	RHEL6_Base_SOE	6.4	Development	1	
RHBA-2015:0974	Apply Errata to Content Hosts immediately after publishing.				
RHSA-2015:0987	Cancel Confirm				
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					

Environment	Host Count
Development	1



#redhat #rhsummit

•

. . .

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 - ManagelQ birds of a feather Session





Nore 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.

#redhat #rhsummit

.



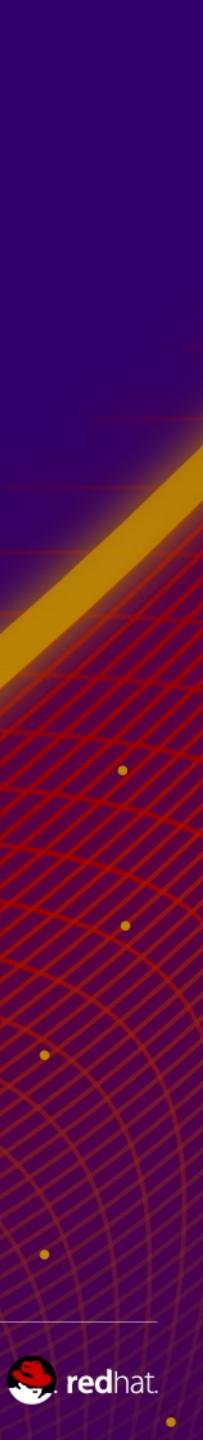




13821 - Hands on with Red Hat CloudForms LEARN. NETWORK. **EXPERIENCE OPEN SOURCE.**

#redhat #rhsummit

RED HAT SUMMIT



• •

.

HAVE MORE QUESTIONS ON SECURITY?

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

#redhat #rhsummit

Hall A, First floor

