Utilizing Red Hat Management Solutions to Enable PCI Compliance: A Customer Perspective

Daniel Kinon, RHCE . Choice Hotels International
Akash Chandrashekar, RHCE . Red Hat

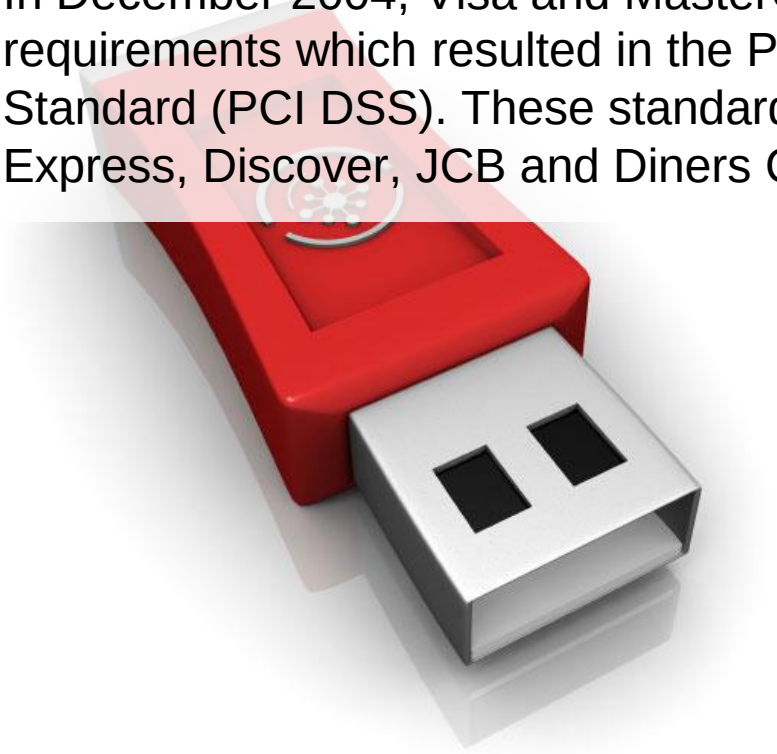
Agenda

- Understanding PCI Compliance
- How Red Hat Meets Your Compliance Needs
- Choice Hotel's Compliance Challenge
- How RHN Satellite Makes Achieving Compliance Easy

Understanding PCI Compliance

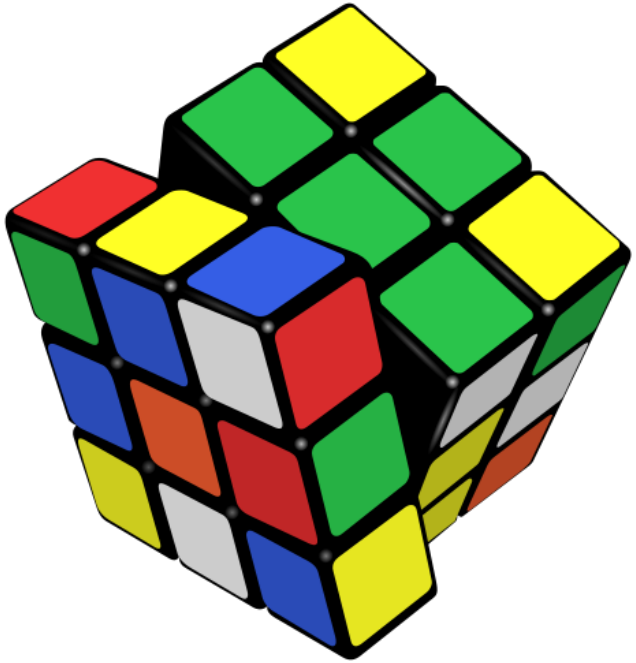
PCI Compliance Basics

- One the most important security concerns in computing is around data breach incidents of cardholder information.
- The incidents are have become more common, prevalent and sophisticated.
- In an effort to thwart such threats, the payment card industry has worked on developing and implementing security standards to help protect cardholder data.
- In December 2004, Visa and MasterCard defined a common set of data security requirements which resulted in the Payment Card Industry Data Security Standard (PCI DSS). These standards were then endorsed by American Express, Discover, JCB and Diners Club.



PCI Compliance Requirements

- PCI identifies 12 requirements which MUST be met by any merchant or service provider that stores, processes or transmits credit card information.
- These 12 requirements are further subdivided into over 250 granular audit points which collectively focus on the establishment of strong end-user access controls, activity monitoring and logging, and the need to regularly test security systems and processes.
- These requirements require organizations have strong end- user access controls and activity monitoring and logging need to regularly test security systems and processes.



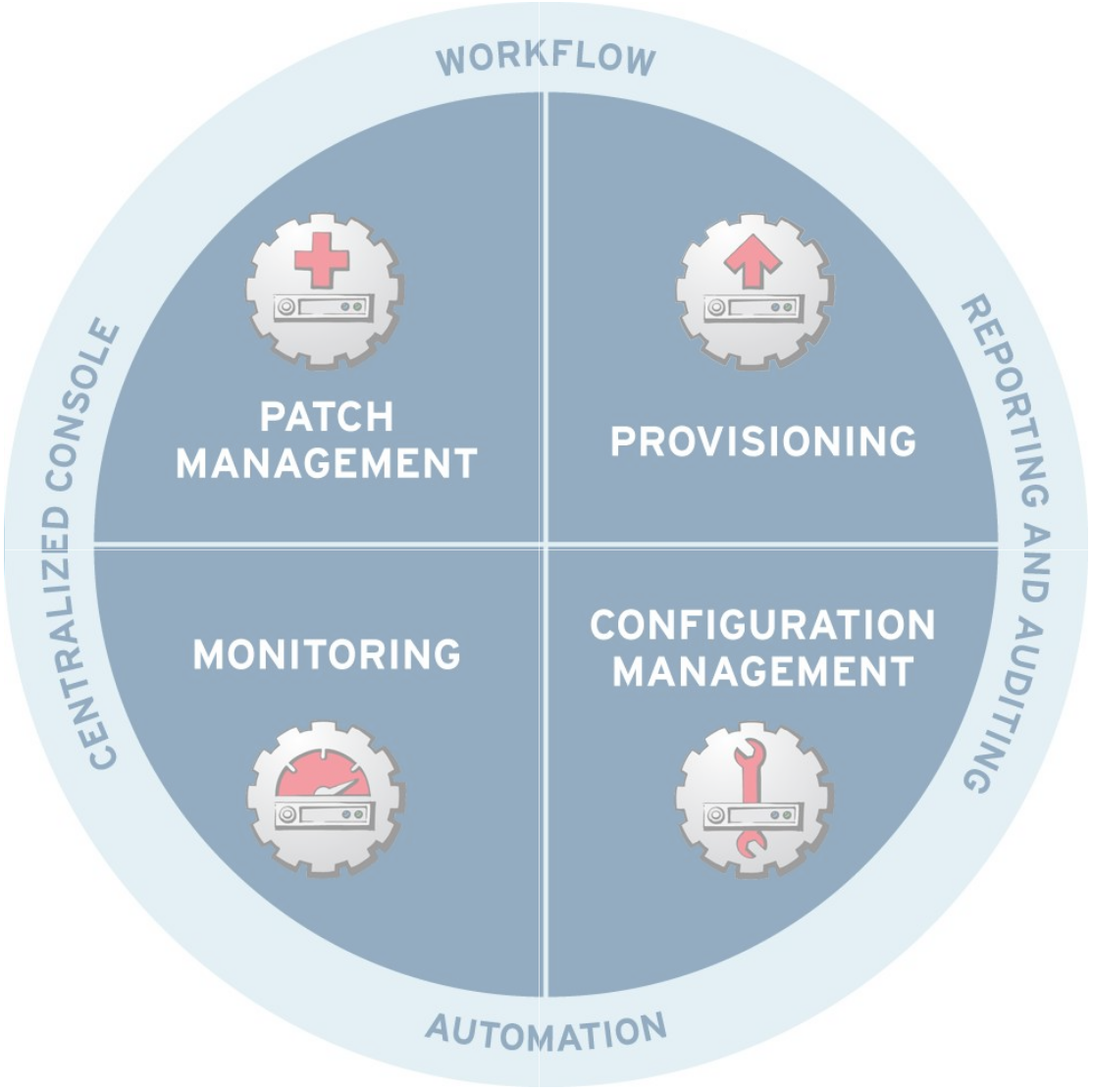
What??? More Requirements?

The PCI program also set forth standards for the security of all system that are connected to the overall payment network. These components include:

- Firewalls, Intrusion Detection Systems, Switches and Routers
- Network Appliances
- Web Servers, Applications, Databases, DNS, Mail Servers
- Authentication Systems
- POS Systems
- Card Scanners
- E-commerce Web Sites

How Red Hat Meets Your Compliance Needs

Red Hat Systems Management



RHSA-2010:0457 - Security Advisory

Details Packages Affected Systems

Synopsis

Moderate: perl security update

Issued:	6/7/10
Updated:	6/7/10

Topic

Updated perl packages that fix two security issues are now available for Red Hat Enterprise Linux 3 and 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Description

Perl is a high-level programming language commonly used for system administration utilities and web programming. The Safe extension module allows users to compile and execute Perl code in restricted compartments.

The Safe module did not properly restrict the code of implicitly called methods (such as DESTROY and AUTOLOAD) on implicitly blessed objects returned as a result of unsafe code evaluation. These methods could have been executed unrestricted by Safe when such objects were accessed or destroyed. A specially-crafted Perl script executed inside of a Safe

Vulnerability/Threat Assessment

Critical

This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms.

Important

This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.

Moderate

This rating is given to flaws that may be harder or more unlikely to be exploitable but given the right circumstances could still lead to some compromise of the confidentiality, integrity, or availability of resources.

Low

This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.

redhat

Security Response Team
2010 CVE
CVE-2010-1168
2009 CVE
2008 CVE
2007 CVE
2006 CVE
2005 CVE
2004 CVE
2003 CVE
2002 CVE
2001 CVE
2000 CVE
1999 CVE

CVE-2010-1168

Impact: Moderate (classification)

Public: May 20 2010

Bugzilla: 576508: CVE-2010-1168 perl Safe: Intended restriction bypass via object references

Details

The MITRE CVE dictionary describes this issue as:

> ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

Find out more about CVE-2010-1168 from the MITRE CVE dictionary and NIST NVD.

CVSS v2 metrics

NOTE: The following CVSS v2 metrics and score provided are preliminary and subject to review.

Base Score:	5.8	Base Metrics:	AV:N/AC:M/Au:N/C:P/I:P/A:N
Access Vector:	Network	Confidentiality Impact:	Partial
Access Complexity:	Medium	Integrity Impact:	Partial
Authentication:	None	Availability Impact:	None

Find out more about Red Hat support for the Common Vulnerability Scoring System (CVSS).

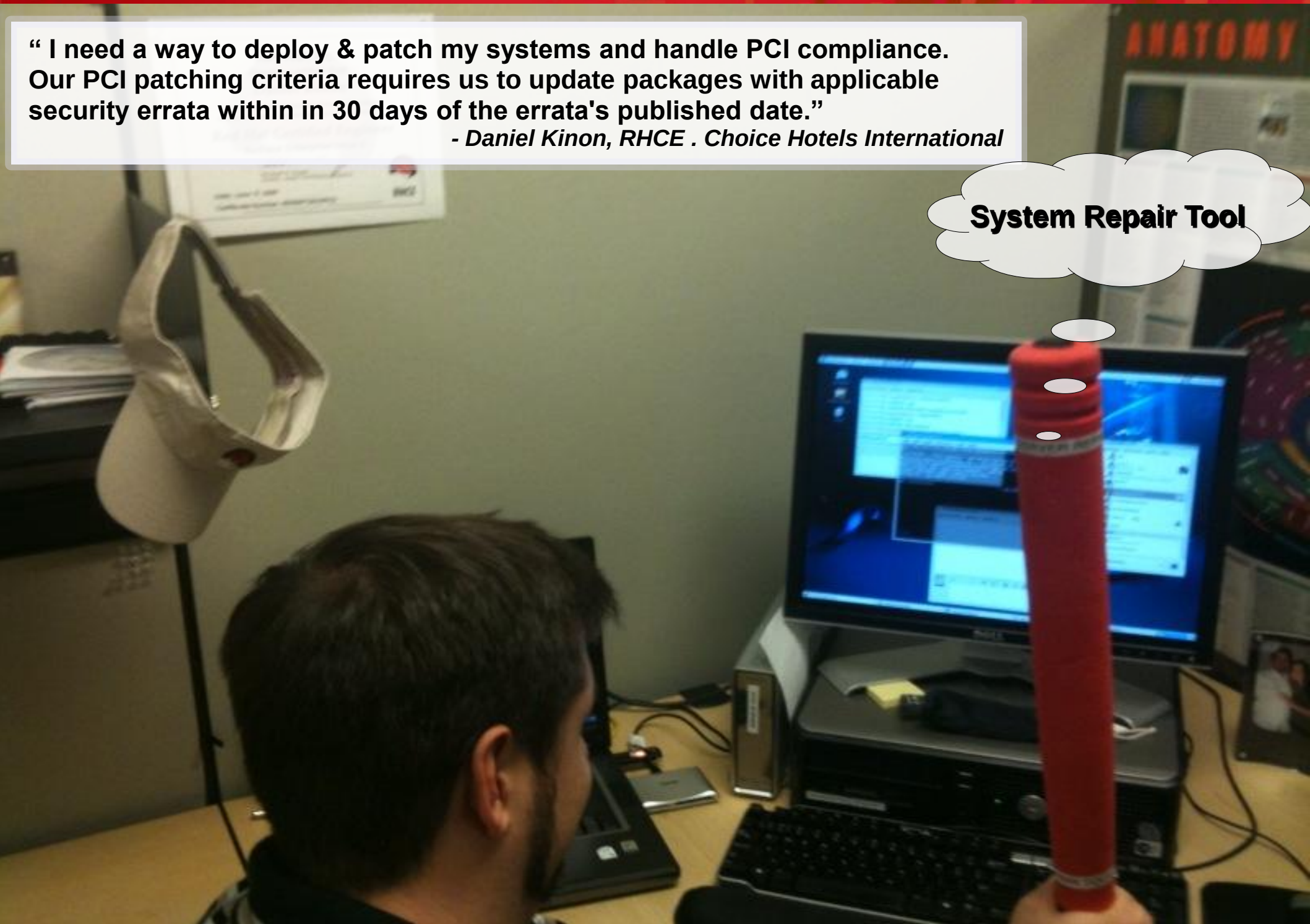
http://www.redhat.com/security/data/cve

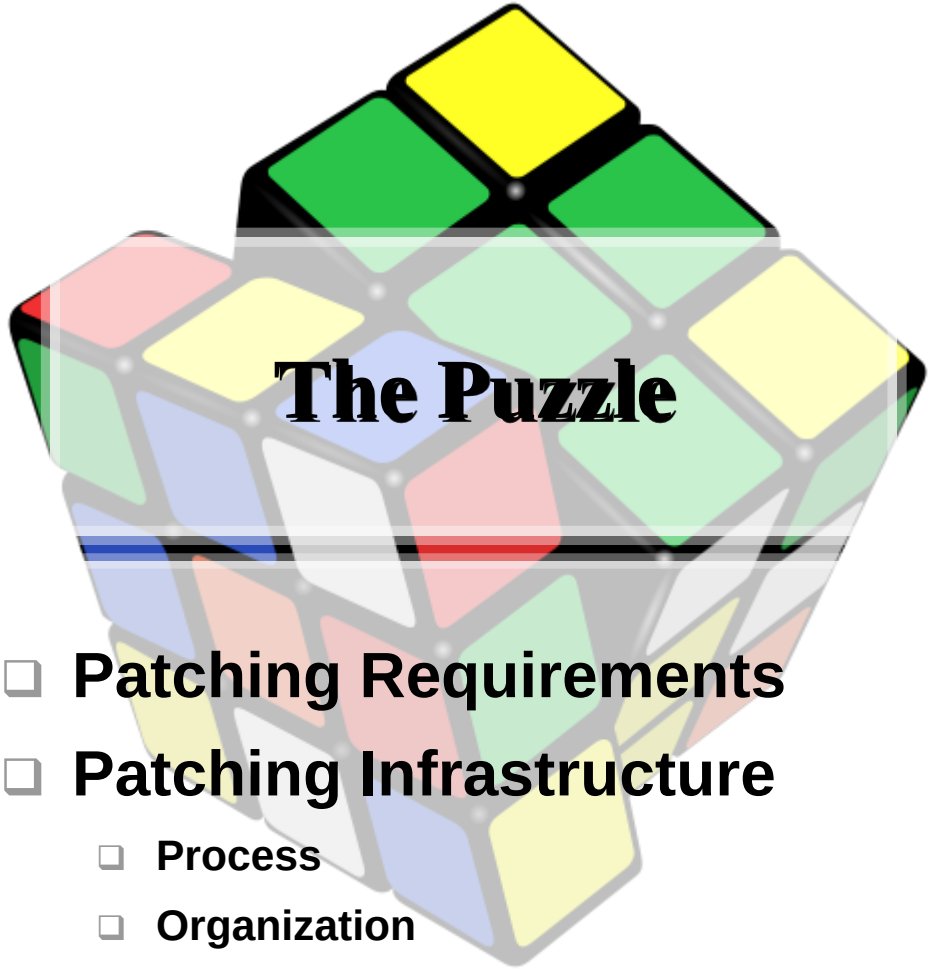
Choice Hotel's Compliance Challenge

- The Puzzle
- The Pieces
- The Tools
- The Solution

“ I need a way to deploy & patch my systems and handle PCI compliance. Our PCI patching criteria requires us to update packages with applicable security errata within in 30 days of the errata's published date.”

- Daniel Kinon, RHCE . Choice Hotels International





The Puzzle

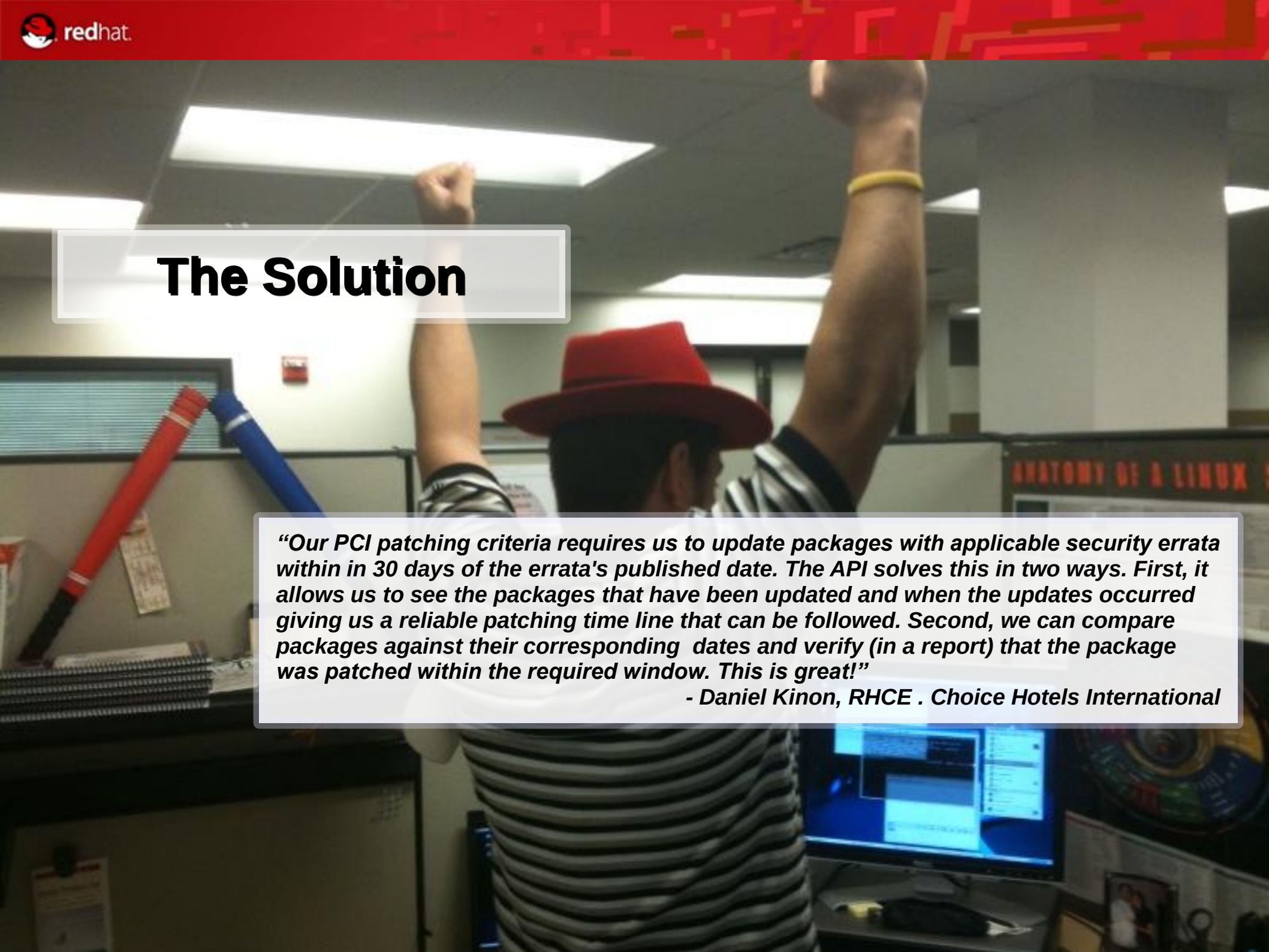
- Patching Requirements
- Patching Infrastructure
  - Process
  - Organization
  - Delegation
- Audit Reporting

The Pieces

- List of Servers w/ Applicable Errata
- Errata Type (RHSA vs. RHBA)
- Errata Published Date
- Server Patching Process
- Patch Application Date
- Final Compliance Report

The Tools

- **Red Hat Satellite**
  - **Package Management**
  - **Configuration Management**
  - **Channel Management**
  - **Satellite API & Reporting**
- **Satellite Reporting Package**
- **Third Party APIs *(Optional)***

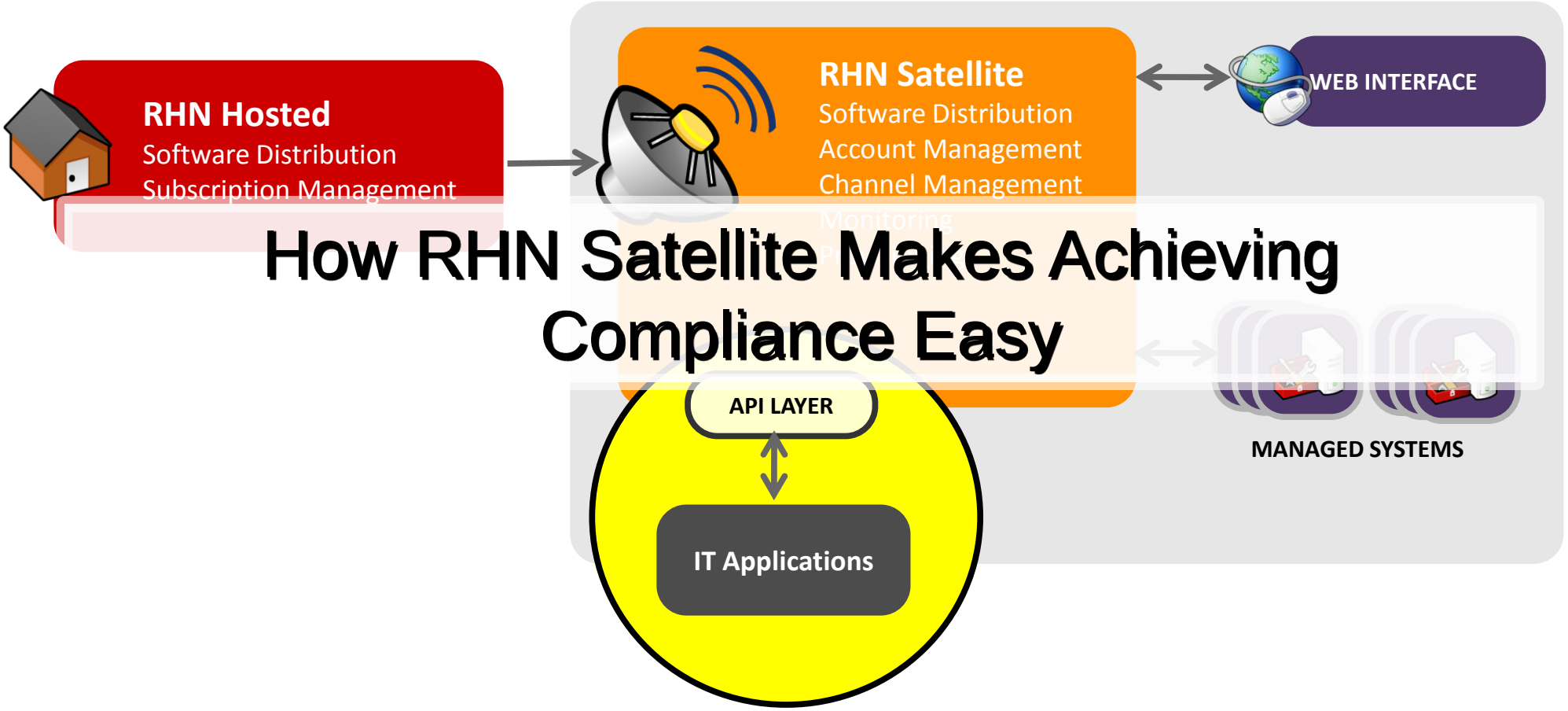


The Solution

“Our PCI patching criteria requires us to update packages with applicable security errata within in 30 days of the errata's published date. The API solves this in two ways. First, it allows us to see the packages that have been updated and when the updates occurred giving us a reliable patching time line that can be followed. Second, we can compare packages against their corresponding dates and verify (in a report) that the package was patched within the required window. This is great!”

- Daniel Kinon, RHCE . Choice Hotels International

How RHN Satellite Makes Achieving Compliance Easy



Why use Red Hat Network Satellite?

Red Hat Network Satellite makes Linux:

Deployable

Provision thousands of machines at once without touching them

Scalable

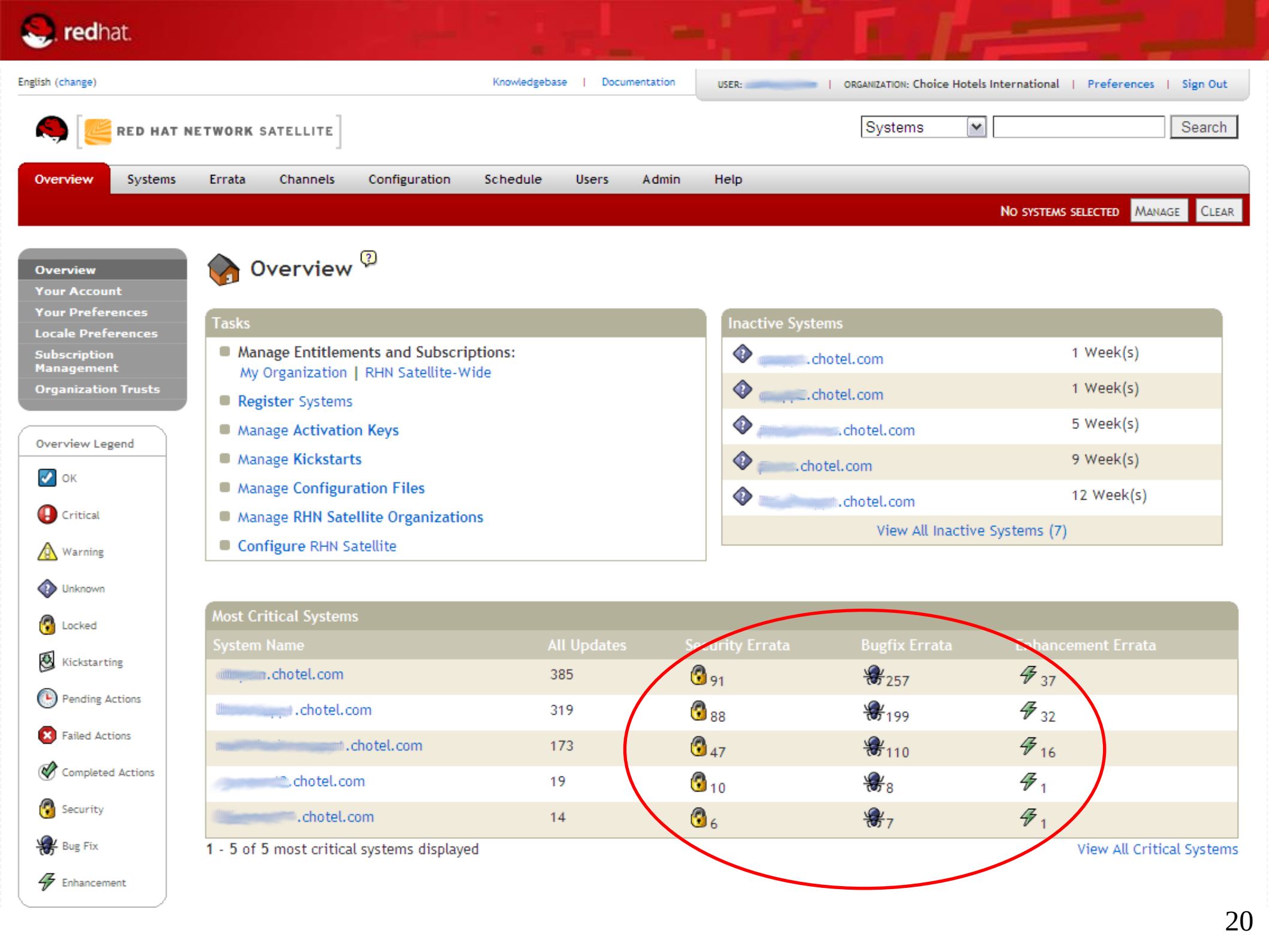
Expand IS/IT capabilities without expanding resources

Manageable

Update 1,000 systems as easily as 1

Consistent

Ensure that security fixes and configuration changes are applied across your organization


redhat
English (change)
Knowledgebase | Documentation
USER: [redacted] | ORGANIZATION: Choice Hotels International | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview
Systems
Errata
Channels
Configuration
Schedule
Users
Admin
Help
NO SYSTEMS SELECTED
MANAGE
CLEAR
Overview
Your Account
Your Preferences
Locale Preferences
Subscription Management
Organization Trusts
Overview
Tasks
Manage Entitlements and Subscriptions:
My Organization | RHN Satellite-Wide
Register Systems
Manage Activation Keys
Manage Kickstarts
Manage Configuration Files
Manage RHN Satellite Organizations
Configure RHN Satellite
Inactive Systems
[redacted].chotel.com 1 Week(s)
[redacted].chotel.com 1 Week(s)
[redacted].chotel.com 5 Week(s)
[redacted].chotel.com 9 Week(s)
[redacted].chotel.com 12 Week(s)
View All Inactive Systems (7)
Overview Legend
OK
Critical
Warning
Unknown
Locked
Kickstarting
Pending Actions
Failed Actions
Completed Actions
Security
Bug Fix
Enhancement
Most Critical Systems
System Name
All Updates
Security Errata
Bugfix Errata
Enhancement Errata
[redacted].chotel.com 385 91 257 37
[redacted].chotel.com 319 88 199 32
[redacted].chotel.com 173 47 110 16
[redacted].chotel.com 19 10 8 1
[redacted].chotel.com 14 6 7 1
1 - 5 of 5 most critical systems displayed
View All Critical Systems

Errata
Relevant
All
Advanced Search
Manage Errata
Clone Errata

RHSA-2010:0457 - Security Advisory

Details Packages Affected Systems

Synopsis

Moderate: perl security update

Issued:	6/7/10
Updated:	6/7/10

Topic

Updated perl packages that fix two security issues are now available for Red Hat Enterprise Linux 3 and 4.

The Red Hat Security Response Team has rated this update as having moderate security impact. Common Vulnerability Scoring System (CVSS) base scores, which give detailed severity ratings, are available for each vulnerability from the CVE links in the References section.

Description

Perl is a high-level programming language commonly used for system administration utilities and web programming. The Safe extension module allows users to compile and execute Perl code in restricted compartments.

The Safe module did not properly restrict the code of implicitly called methods (such as DESTROY and AUTOLOAD) on implicitly blessed objects returned as a result of unsafe code evaluation. These methods could have been executed unrestricted by Safe when such objects were accessed or destroyed. A specially-crafted Perl script executed inside of a Safe

Vulnerability/Threat Assessment

Critical

This rating is given to flaws that could be easily exploited by a remote unauthenticated attacker and lead to system compromise (arbitrary code execution) without requiring user interaction. These are the types of vulnerabilities that can be exploited by worms.

Important

This rating is given to flaws that can easily compromise the confidentiality, integrity, or availability of resources. These are the types of vulnerabilities that allow local users to gain privileges, allow unauthenticated remote users to view resources that should otherwise be protected by authentication, allow authenticated remote users to execute arbitrary code, or allow local or remote users to easily cause a denial of service.

Moderate

This rating is given to flaws that may be harder or more unlikely to be exploitable but given the right circumstances could still lead to some compromise of the confidentiality, integrity, or availability of resources.

Low

This rating is given to all other issues that have a security impact. These are the types of vulnerabilities that are believed to require unlikely circumstances to be able to be exploited, or where a successful exploit would give minimal consequences.

Solution

Before applying this update, make sure all previously-released errata relevant to your system have been applied.

This update is available via the Red Hat Network. Details on how to use the Red Hat Network to apply this update are available at
http://kbase.redhat.com/faq/docs/DOC-11259

Affected Channels

Red Hat Enterprise Linux AS (v. 4 for 32-bit x86)
Red Hat Enterprise Linux AS (v. 4 for 64-bit AMD64/Intel EM64T)
Red Hat Enterprise Linux AS (v. 4 for 64-bit Intel Itanium)
Red Hat Enterprise Linux ES (v. 4 for 32-bit x86)

Fixes

['CVE-2010-1168 perl Safe: Intended restriction bypass via object references']
['CVE-2010-1447 perl: Safe restriction bypass when reference to subroutine in compartment is called from outside']

Keywords

(none)

CVEs

CVE-2010-1168
CVE-2010-1447

OVAL

(none)

References

http://www.redhat.com/security/updates/classification/#moderate
http://cpansearch.perl.org/src/RGARCIA/Safe-2.27/Changes

Notes

(none)

Celebrating 10 Years

Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names

TOTAL CVEs: 42067

About CVE
Terminology
Documents
FAQs
CVE List
About CVE Identifiers
Obtain a CVE Identifier
Search CVE
Search NVD
CVE In Use
CVE Adoption
CVE-Compatible Products
NVD for CVE Fix Information
More . . .
News & Events
Calendar
Free Newsletter
Community
CVE Editorial Board
Sponsor
Contact Us
Search the Site

Printer-Friendly View

CVE-ID

CVE-2010-1168
(under review)

Learn more at National Vulnerability Database (NVD)
• Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Status

Candidate

This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.

Phase

Assigned (20100329)

Votes

Comments

Candidate assigned on 20100329 and proposed on N/A

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

FOR MORE INFORMATION: cve@mitre.org

BACK TO TOP

CVE List
Data Updates & RSS Feeds
Reference Key/Maps
Data Sources
Versions
Search Tips
Editor's Commentary
Obtain a CVE Identifier
Editorial Policies
About CVE Identifiers

ITEMS OF INTEREST
Terminology
NVD

redhat

Security Response Team
2010 CVE
CVE-2010-1168
2009 CVE
2008 CVE
2007 CVE
2006 CVE
2005 CVE
2004 CVE
2003 CVE
2002 CVE
2001 CVE
2000 CVE
1999 CVE

CVE-2010-1168

Impact: Moderate (classification)

Public: May 20 2010

Bugzilla: 576508: CVE-2010-1168 perl Safe: Intended restriction bypass via object references

Details

The MITRE CVE dictionary describes this issue as:

> ** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

Find out more about CVE-2010-1168 from the MITRE CVE dictionary and NIST NVD.

CVSS v2 metrics

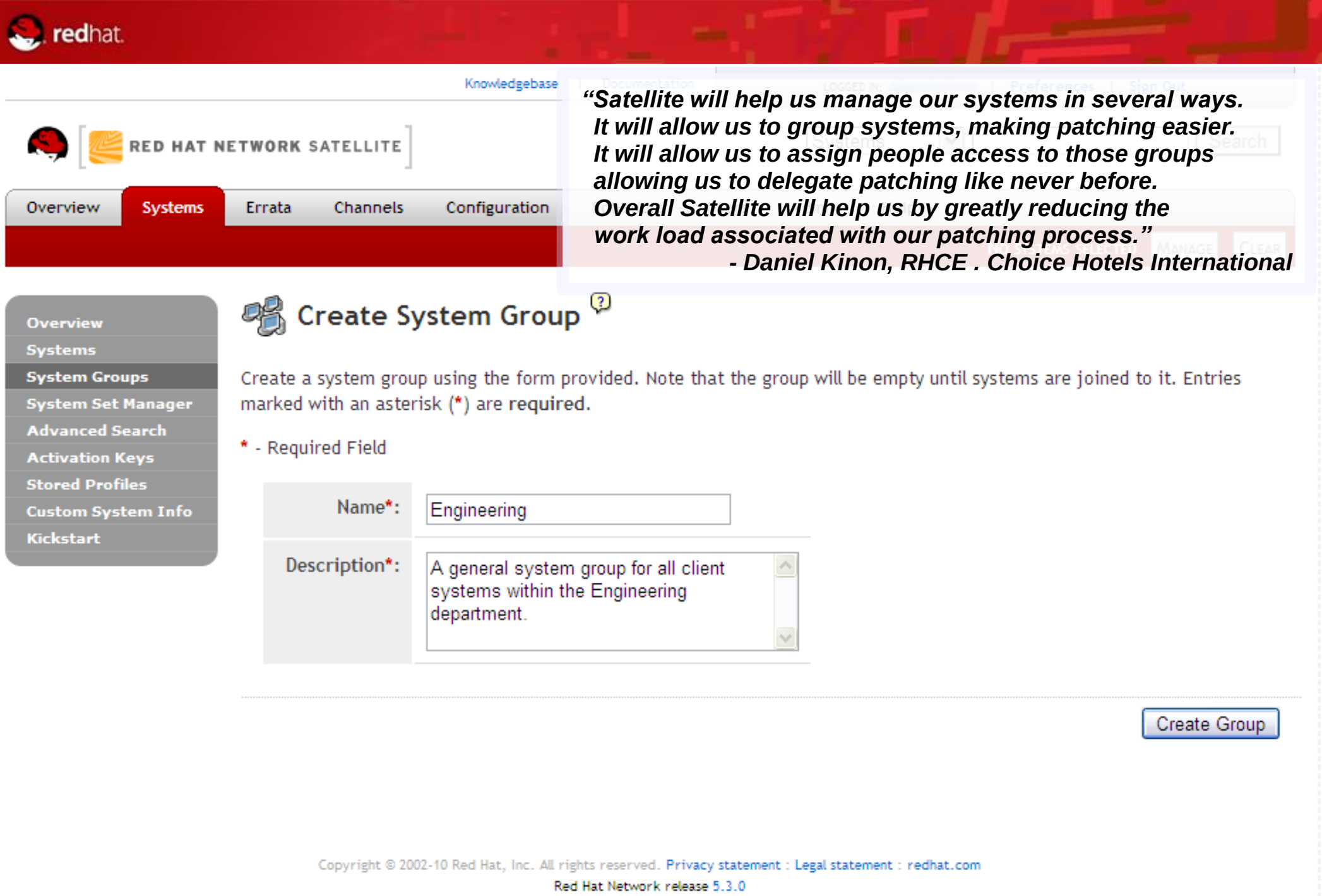
NOTE: The following CVSS v2 metrics and score provided are preliminary and subject to review.

Base Score:	5.8	Base Metrics:	AV:N/AC:M/Au:N/C:P/I:P/A:N
Access Vector:	Network	Confidentiality Impact:	Partial
Access Complexity:	Medium	Integrity Impact:	Partial
Authentication:	None	Availability Impact:	None

Find out more about Red Hat support for the Common Vulnerability Scoring System (CVSS).

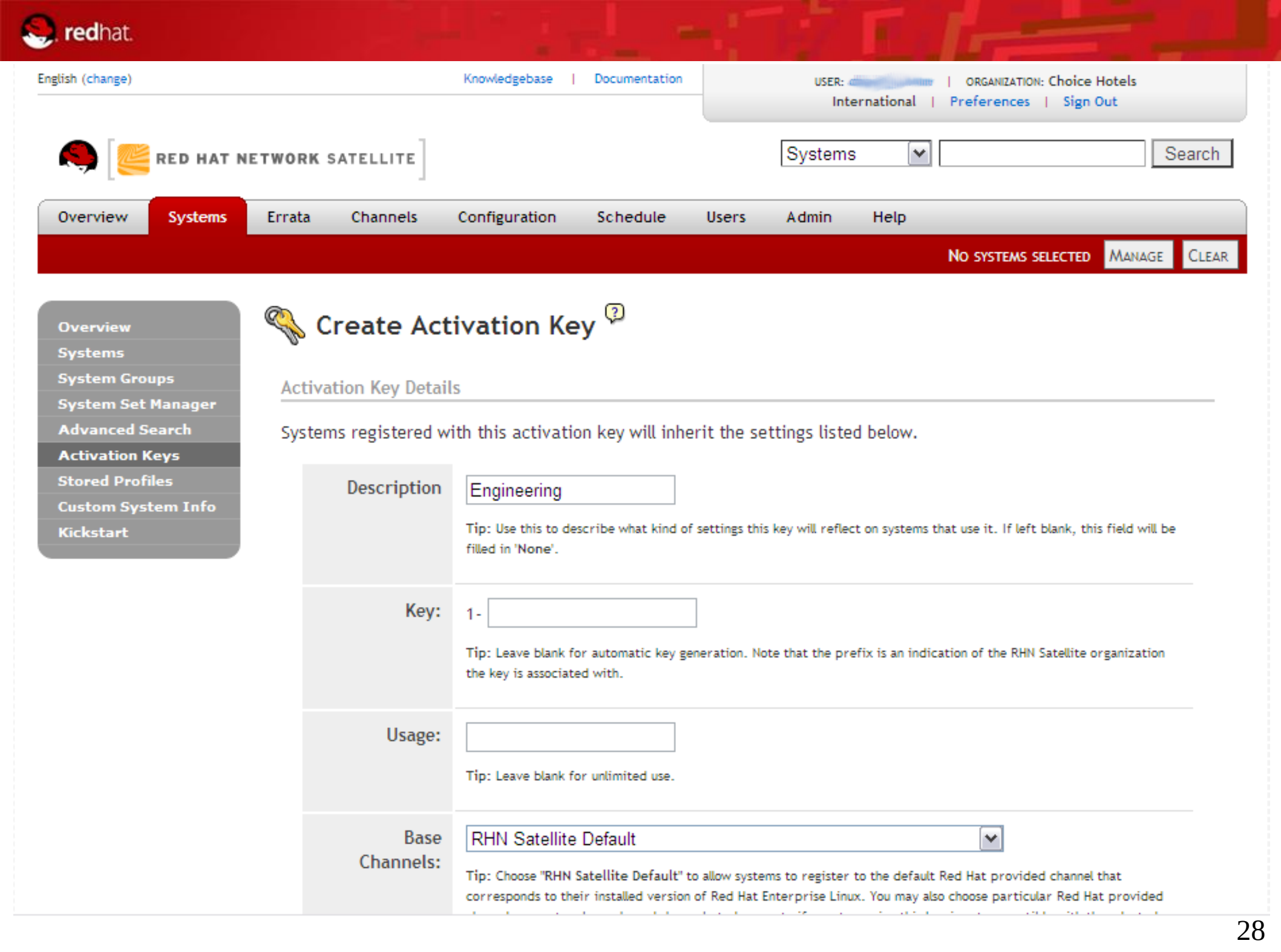
http://www.redhat.com/security/data/cve

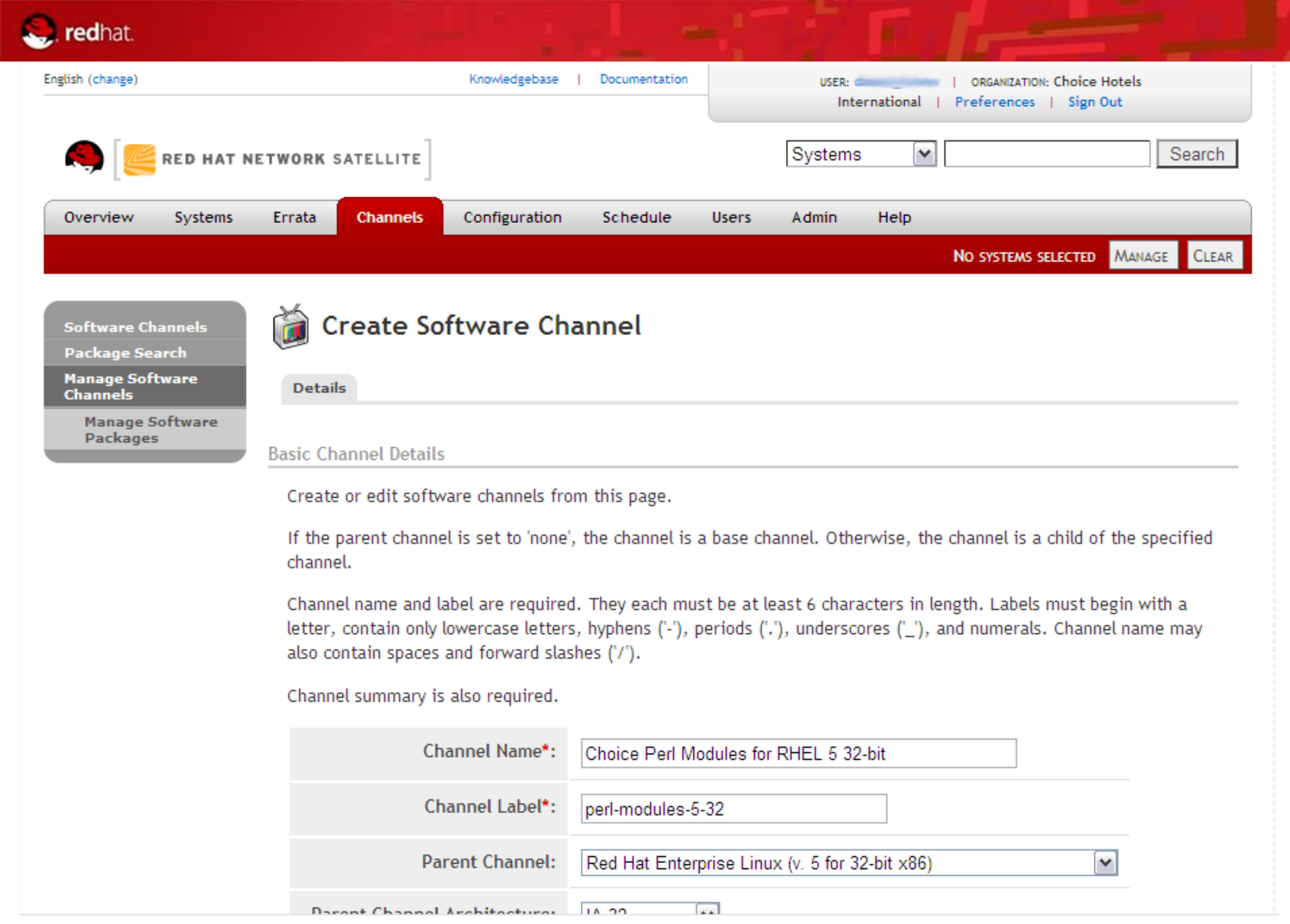
Poor Planning?

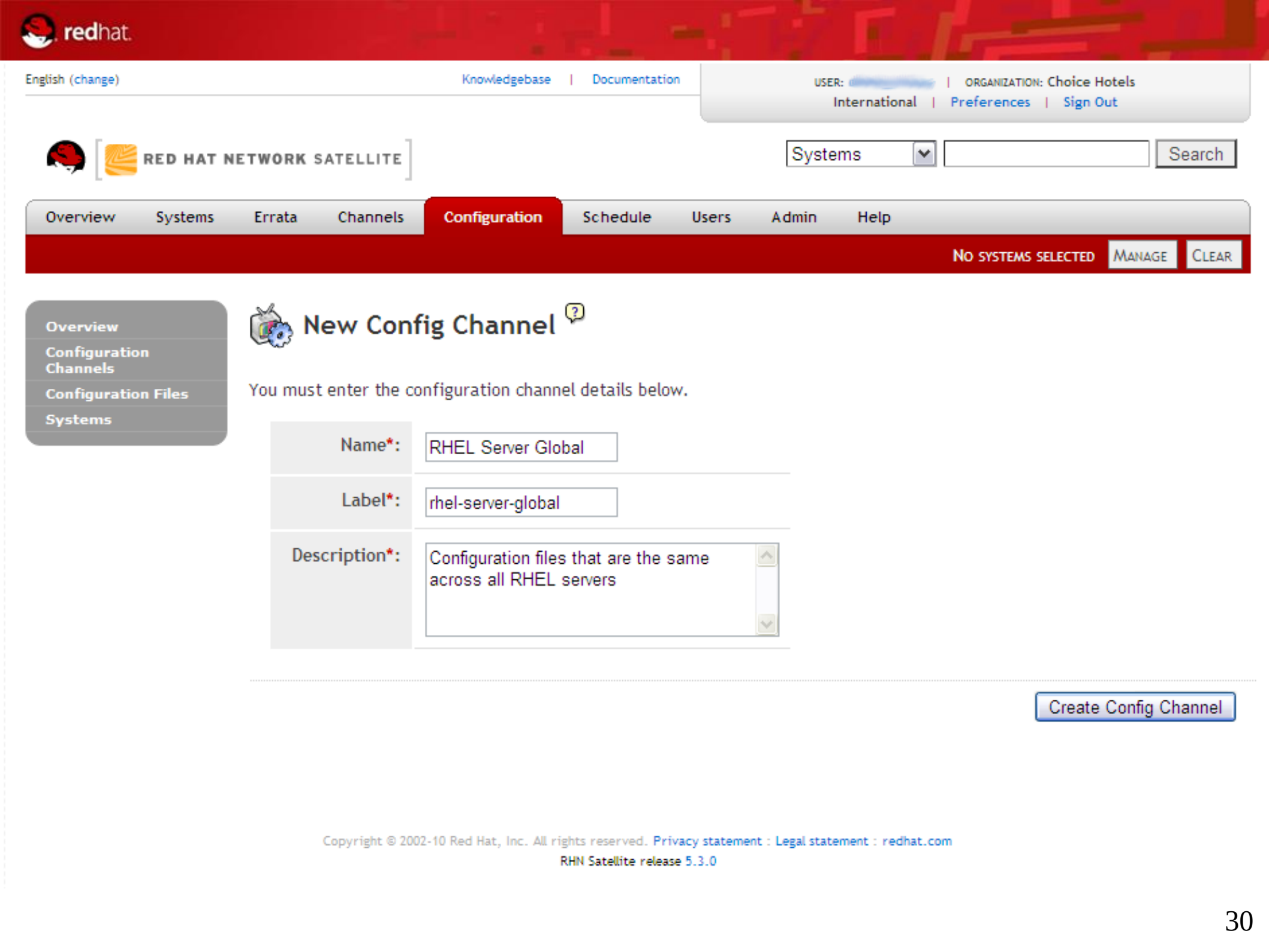


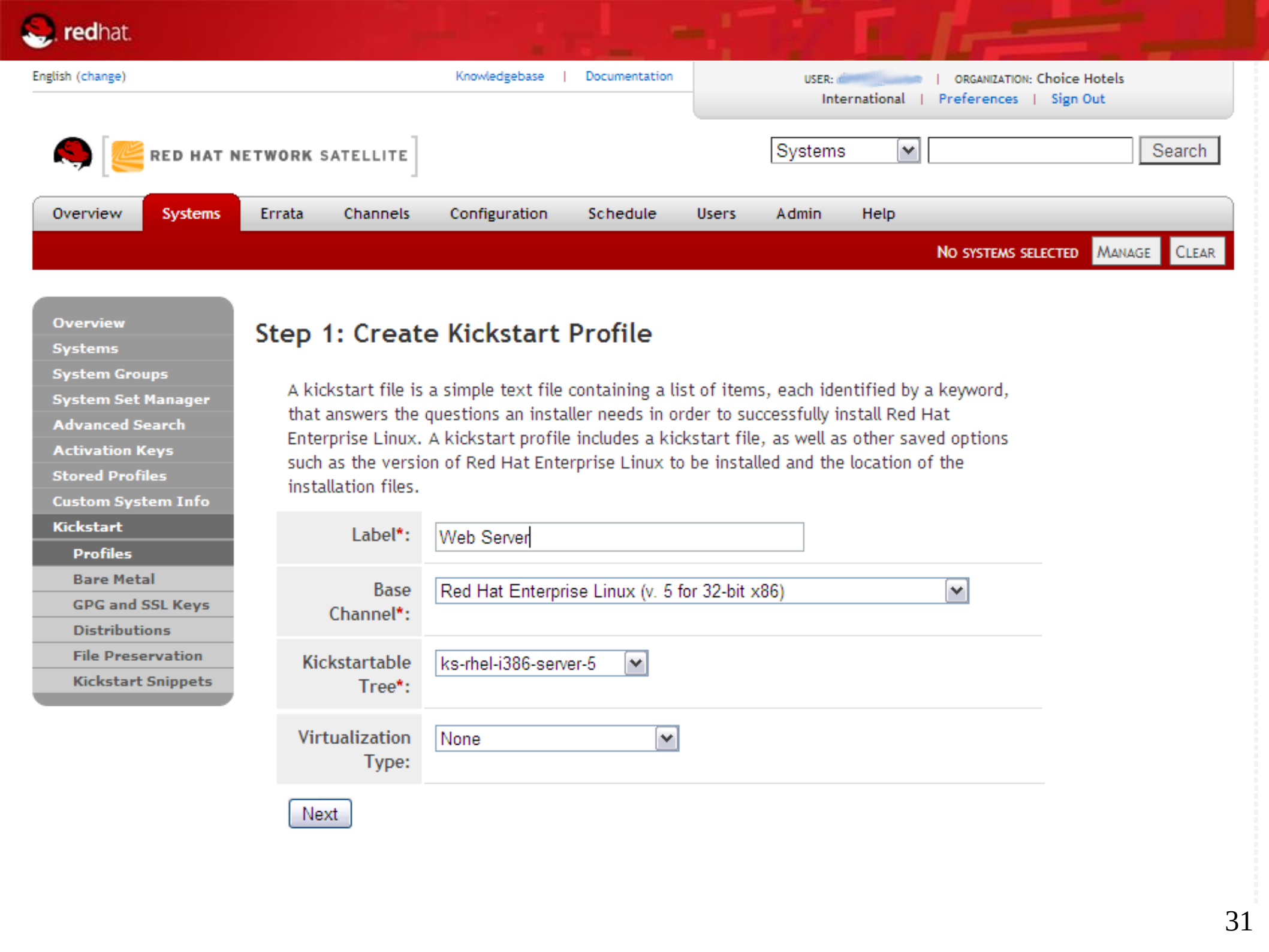
"Satellite will help us manage our systems in several ways. It will allow us to group systems, making patching easier. It will allow us to assign people access to those groups allowing us to delegate patching like never before. Overall Satellite will help us by greatly reducing the work load associated with our patching process."

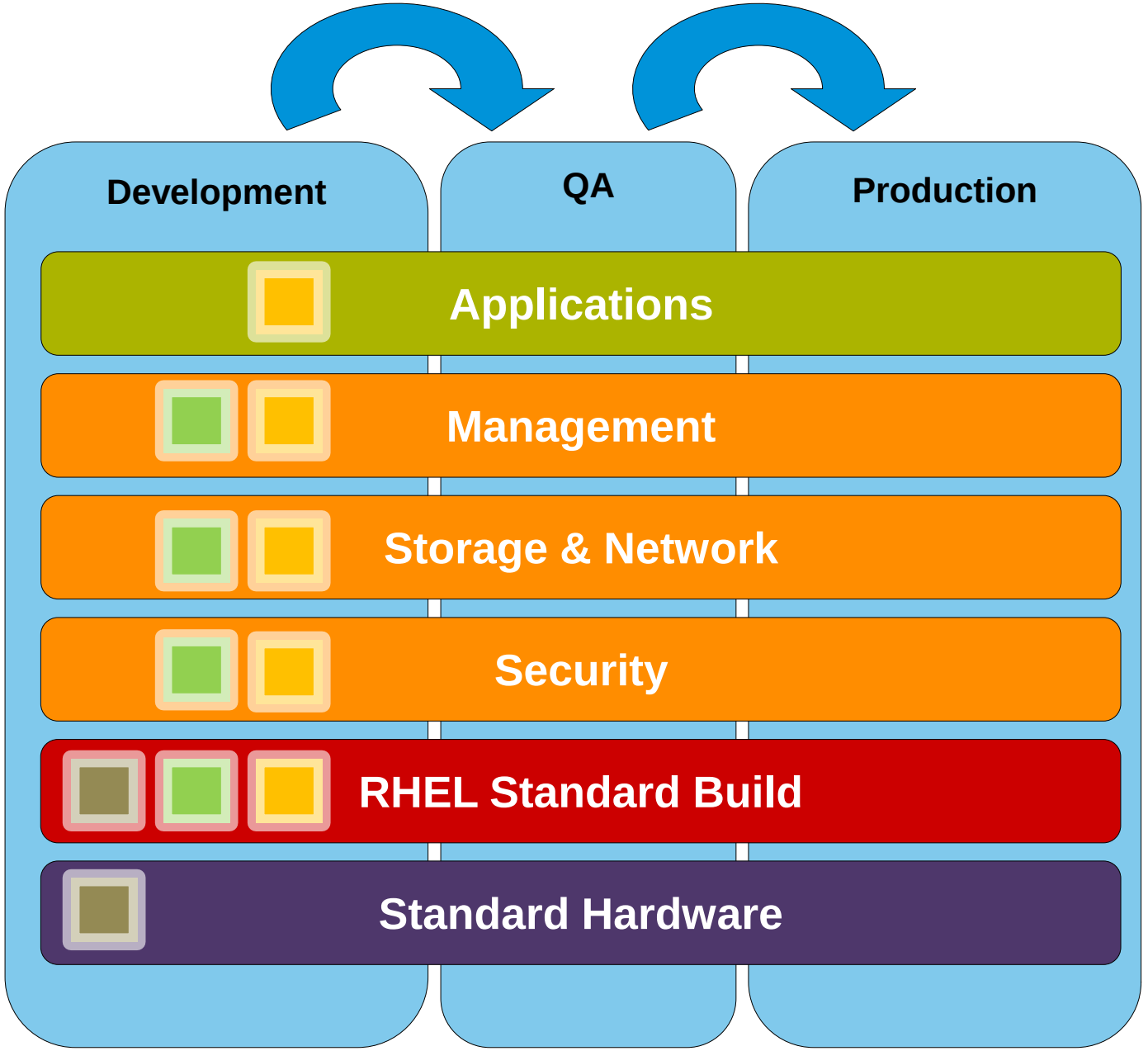
- Daniel Kinon, RHCE . Choice Hotels International


redhat
English (change)
Knowledgebase | Documentation
USER: | ORGANIZATION: Choice Hotels
International | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview
Systems
Errata
Channels
Configuration
Schedule
Users
Admin
Help
NO SYSTEMS SELECTED
MANAGE
CLEAR
Overview
Systems
System Groups
System Set Manager
Advanced Search
Activation Keys
Stored Profiles
Custom System Info
Kickstart
Create Activation Key
Activation Key Details
Systems registered with this activation key will inherit the settings listed below.
Description
Engineering
Tip: Use this to describe what kind of settings this key will reflect on systems that use it. If left blank, this field will be filled in 'None'.
Key:
1-
Tip: Leave blank for automatic key generation. Note that the prefix is an indication of the RHN Satellite organization the key is associated with.
Usage:
Tip: Leave blank for unlimited use.
Base Channels:
RHN Satellite Default
Tip: Choose "RHN Satellite Default" to allow systems to register to the default Red Hat provided channel that corresponds to their installed version of Red Hat Enterprise Linux. You may also choose particular Red Hat provided


redhat
English (change)
Knowledgebase | Documentation
USER: [redacted] | ORGANIZATION: Choice Hotels
International | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview
Systems
Errata
Channels
Configuration
Schedule
Users
Admin
Help
NO SYSTEMS SELECTED
MANAGE
CLEAR
Software Channels
Package Search
Manage Software Channels
Manage Software Packages
Create Software Channel
Details
Basic Channel Details
Create or edit software channels from this page.
If the parent channel is set to 'none', the channel is a base channel. Otherwise, the channel is a child of the specified channel.
Channel name and label are required. They each must be at least 6 characters in length. Labels must begin with a letter, contain only lowercase letters, hyphens ('-'), periods ('.'), underscores ('_'), and numerals. Channel name may also contain spaces and forward slashes ('/').
Channel summary is also required.
Channel Name*:
Choice Perl Modules for RHEL 5 32-bit
Channel Label*:
perl-modules-5-32
Parent Channel:
Red Hat Enterprise Linux (v. 5 for 32-bit x86)


redhat
English (change)
Knowledgebase | Documentation
USER: | ORGANIZATION: Choice Hotels
International | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview Systems Errata Channels Configuration Schedule Users Admin Help
NO SYSTEMS SELECTED
MANAGE
CLEAR
Overview
Configuration Channels
Configuration Files
Systems
New Config Channel
You must enter the configuration channel details below.
Name*:
RHEL Server Global
Label*:
rhel-server-global
Description*:
Configuration files that are the same across all RHEL servers
Create Config Channel
Copyright © 2002-10 Red Hat, Inc. All rights reserved. Privacy statement : Legal statement : redhat.com
RHN Satellite release 5.3.0


redhat
English (change)
Knowledgebase | Documentation
USER: [redacted] | ORGANIZATION: Choice Hotels
International | Preferences | Sign Out
RED HAT NETWORK SATELLITE
Systems
Search
Overview
Systems
Errata
Channels
Configuration
Schedule
Users
Admin
Help
NO SYSTEMS SELECTED
MANAGE
CLEAR
Overview
Systems
System Groups
System Set Manager
Advanced Search
Activation Keys
Stored Profiles
Custom System Info
Kickstart
Profiles
Bare Metal
GPG and SSL Keys
Distributions
File Preservation
Kickstart Snippets
Step 1: Create Kickstart Profile
A kickstart file is a simple text file containing a list of items, each identified by a keyword, that answers the questions an installer needs in order to successfully install Red Hat Enterprise Linux. A kickstart profile includes a kickstart file, as well as other saved options such as the version of Red Hat Enterprise Linux to be installed and the location of the installation files.
Label*:
Web Server
Base Channel*:
Red Hat Enterprise Linux (v. 5 for 32-bit x86)
Kickstartable Tree*:
ks-rhel-i386-server-5
Virtualization Type:
None
Next



Package Management

Configuration Management

Provisioning (Cobbler)

How can your business benefit from Red Hat Network Satellite?

Lower system administration costs

Management tools let you maximize your hardware investment

Customize configurations for various types of environments

Increase productivity

4-10X system admin productivity, easily allowing 150+ systems/system admin

Flexible architecture allows use of GUI, API, or CLI (scripted) interface

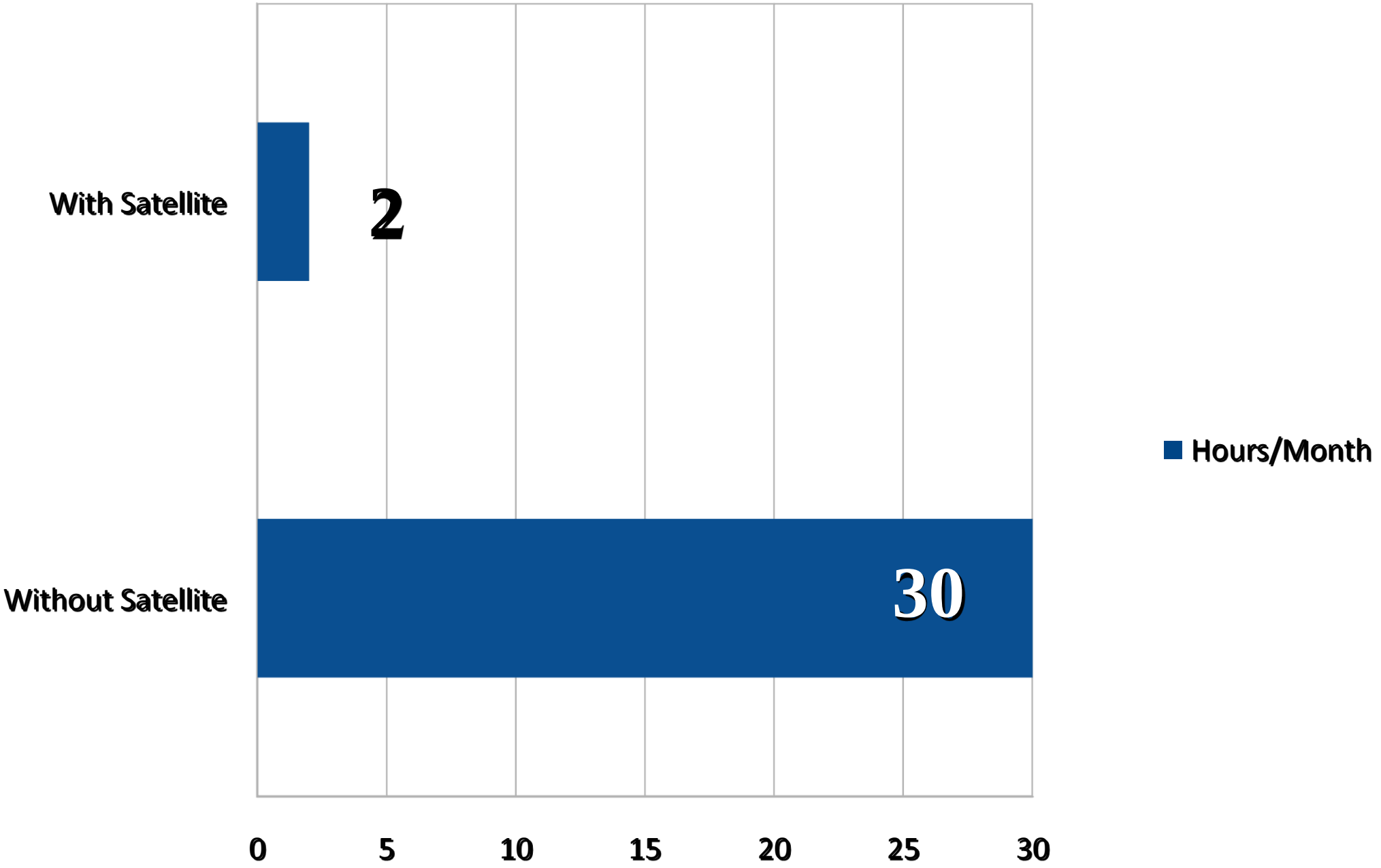
All tasks automated - allowing you to move beyond “guru bottleneck”

Improve security

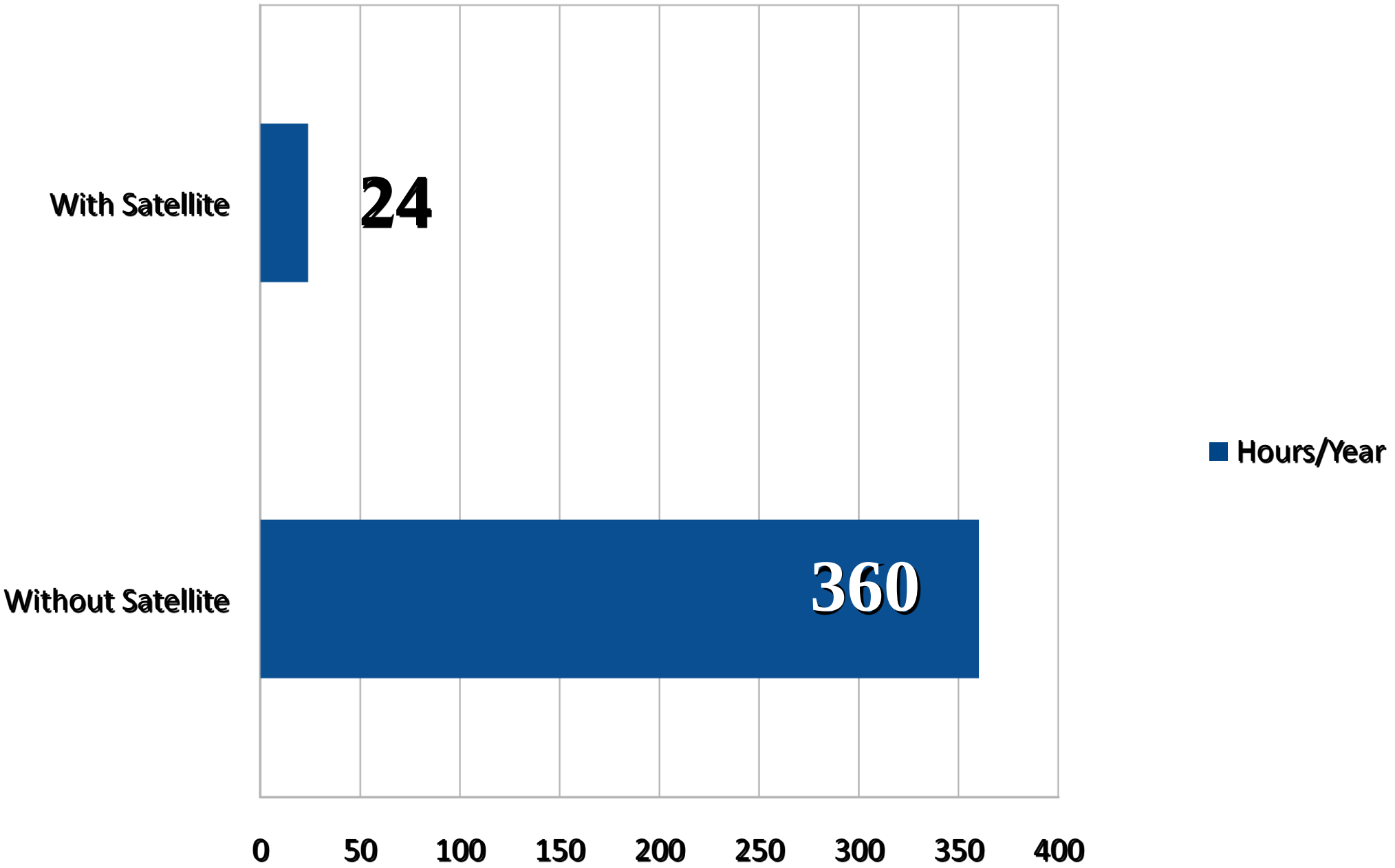
Content stream comes directly & immediately from Red Hat

Complete audit trail and various pre-defined reports

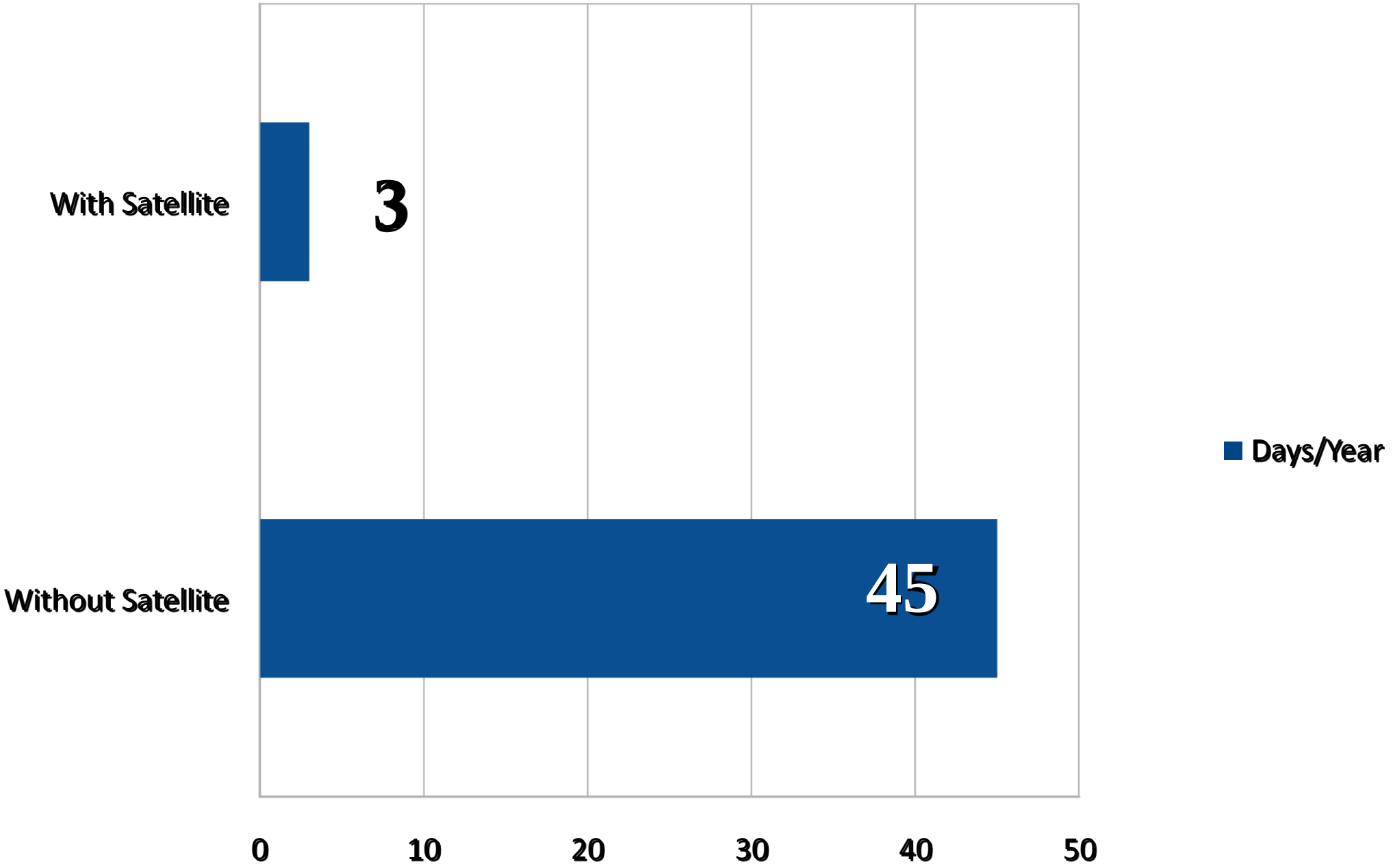
Policies and permissions provide centrally managed role-based administration



* data based on patching 200 servers

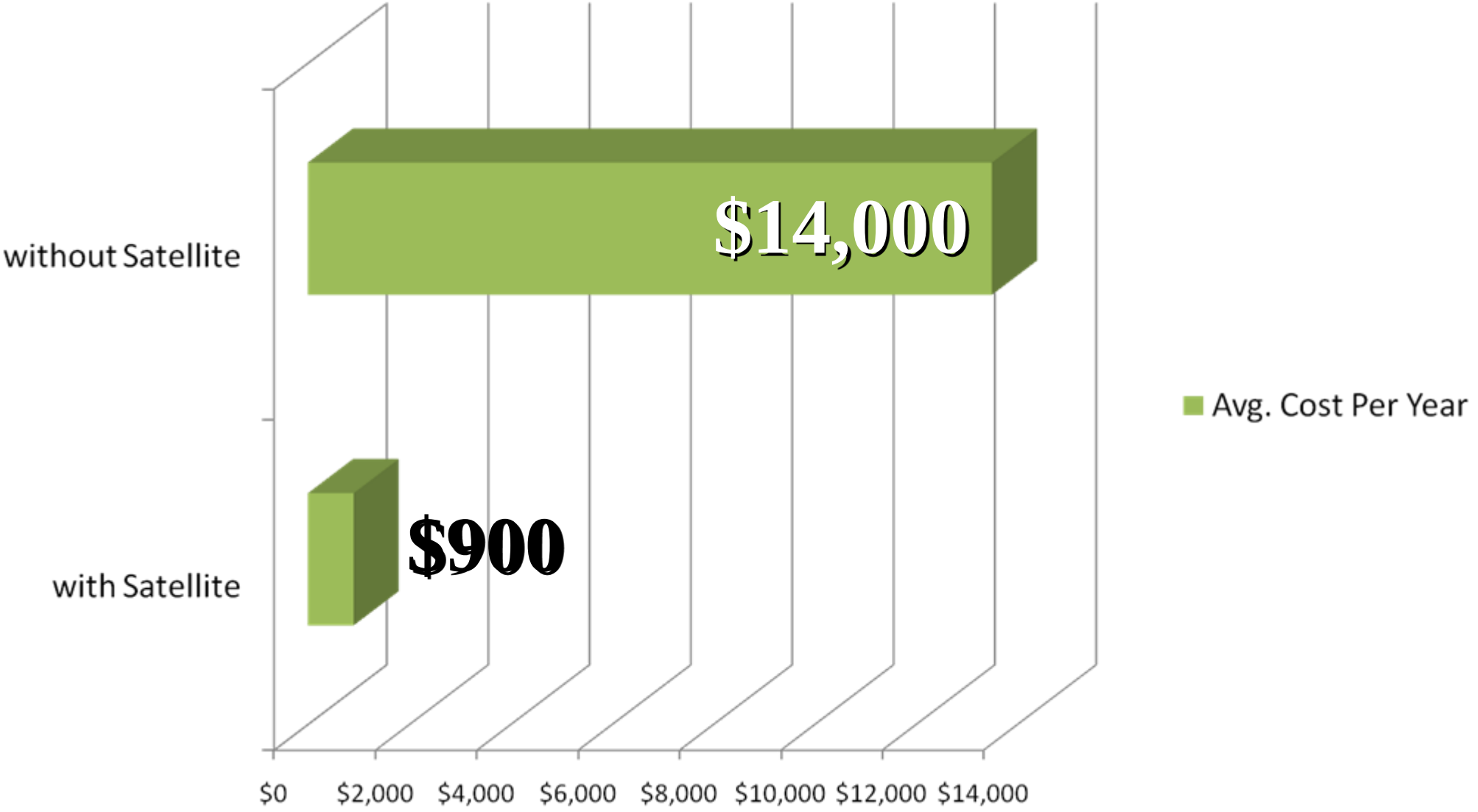


* data based on patching 200 servers



* data based on patching 200 servers

According to indeed.com (http://www.indeed.com/salary/Linux-Administrator.html) the average Linux Administrators salary is about $80k, ~ $300 per day.



*** data based on patching 200 servers**

Supported Programming Languages

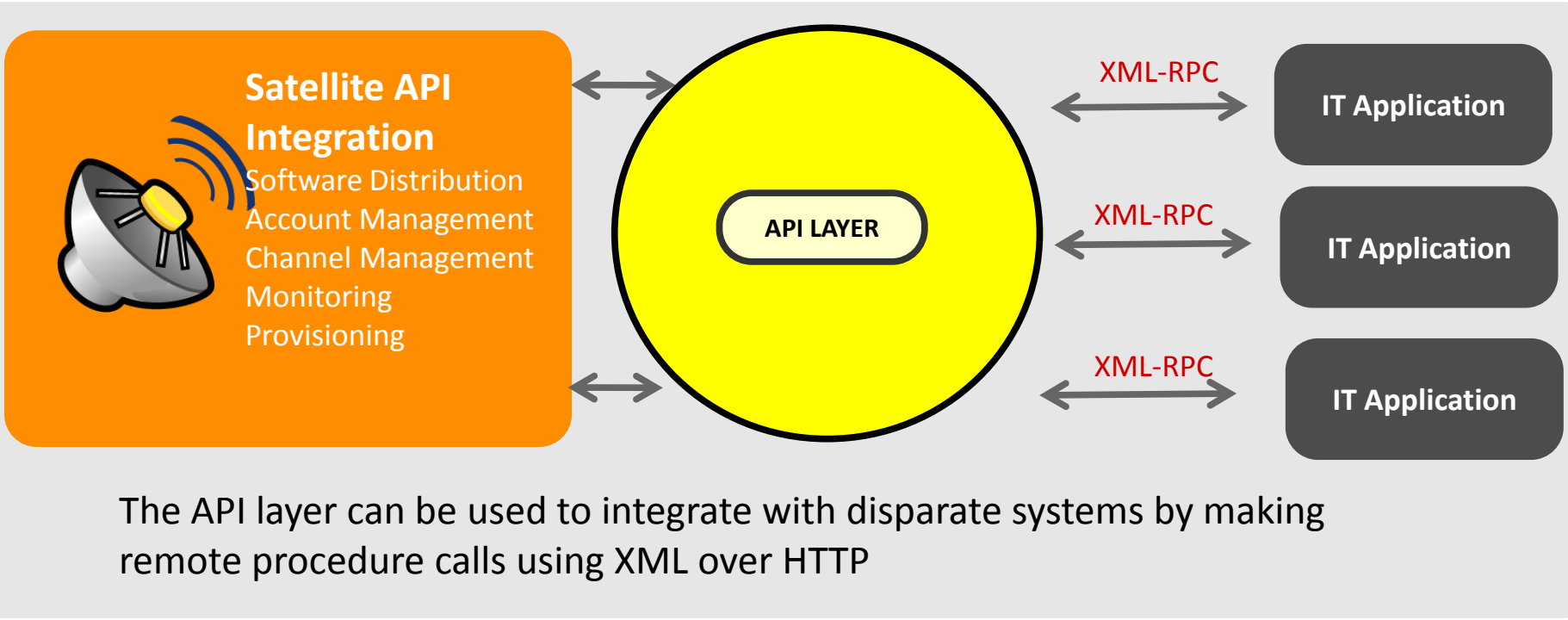
XML-RPC

XML-RPC is a client/server remote procedure call communications protocol that uses XML tags to encode its messages. It uses the HTTP protocol as its transport mechanism.

Works with languages with XML-RPC client support

Most common languages used are Perl and Python
Python in Red Hat Enterprise Linux works out of the box
Perl requires perl-Frontier-RPC package, included with Satellite.

Integration of Third Party Tools



The API layer can be used to integrate with disparate systems by making remote procedure calls using XML over HTTP

- CMDB
- Asset Tracking / Management
- Ticketing Systems
- Monitoring

API Example

```
#!/usr/bin/perl –w
use Frontier::Client;
Use strict;

# Login and create session
my $client = new Frontier::Client(url => ”http://<satellite server hostname>/rpc/api”);
my $session = $client->call('auth.login',<username>,<password>);

#List Software Channels: returns an array (arrayref) of structs (hashrefs)
my $channels = $client->call('channel.listSoftwareChannels', $session);

# List Systems: returns an array (arrayref) of structs (hashrefs)
my $systems = $client->call('system.listUserSystems', $session);
foreach my $system (@$systems) {
    My $id = $system->{id};
    # Get Event History per System: returns an array (arrayref) of structs (hashrefs)
    my $sysEvents = $client->call('system.getEventHistory', $session, $id);
}

# Logout
$client->call('auth.login', $session);
```

1) Set API URL

2) Auth and get Session Key

3) Execute a remote call using your Session Key

4) Iterate over the resulting Data Structure

5) When you are done, Logout

Satellite Reporting

Red Hat Satellite 5.3.0
API v.10.8

server.example.com

System Information

- **RHN ID:** 1000010028
- **Reg Date:** 2009-06-24 T00:59:45
- **Last Check-in:** 2009-08-28 T22:18:28
- **Vendor:** Dell Computer Corporation
- **System:** PowerEdge 1850
- **Asset Tag:** 3VCRJ91
- **Bios Version:** A04

System Events

Package Install 2009-07-06 23:41:33.0
Result: Failed: Some of the packages specified were on a skip list
- kernel-2.6.9-89.EL
- kernel-smp-2.6.9-89.EL
- kernel-utils-2.4-18.el4:1

Package Removal 2009-06-30 13:27:12.0
Result: [['cscope', '15.5', '10.RHEL4.3', '', 'i386']] removed successfully
- cscope-15.5-10.RHEL4.3

Package Removal 2009-07-07 04:08:12.0
Result: cairo-1.2.4-5.el5 failed because of package not installed cdparanoia-libs-alpha9.8-27.2 failed because of package not installed boost-devel-1.32.0-7.rhel4 failed because of package not installed boost-1.32.0-7.rhel4 failed because of package not installed
- boost-1.32.0-7.rhel4
- boost-devel-1.32.0-7.rhel4
- cadaver-0.22.1-3
- cairo-1.2.4-5.el5
- Canna-3.7p3-9.el4
- Canna-libs-3.7p3-9.el4
- cdparanoia-alpha9.8-24
- cdparanoia-libs-alpha9.8-24
- cdparanoia-libs-alpha9.8-27.2

Package Install 2009-07-06 23:40:13.0
Result: Packages were installed successfully
- audit-1.0.16-4.el4
- audit-libs-1.0.16-4.el4
- file-4.10-8.el4
- kernel-2.6.9-89.EL
- kernel-smp-2.6.9-89.EL
- kernel-utils-2.4-18.el4:1
- krb5-libs-1.3.4-62.el4
- mkinitrd-4.2.1.13-4

Reporting from Satellite without the API

Satellite Reporting Tool

- A command-line tool that produces a handful of CSV reports with information found in the RHN Satellite server database.
- Produces stock CSV reports:
  - Entitlements and subscriptions
  - System inventory
  - Software and errata
  - Users and groups

Where can I get the tool?

The spacewalk-reports package is provided by the redhat-rhn-satellite software channel and can be installed after a Satellite server is installed and registered with Red Hat Network.

Useful Links

- https://rhn.redhat.com/rhn/apidoc/index.jsp
- https://fedorahosted.org/spacewalk/wiki/SpacewalkApiPerlGuide
- http://www.redhat.com/security/data/cve
- http://cve.mitre.org


Q & A