GOPS2018
Shenzhen

GOPS

全球运维大会 2018

2018.4.13-4.14 中国·广东·深圳·南山区 圣淘沙大酒店（翡翠店）

GOPS2018
Shenzhen

全站跨平台系统补丁自动化部署实践

梅岑恺 运维经理

目录

背景介绍 – 外部安全形势

2017年是全球漏洞攻击异常活跃的一年：

5月中旬WannaCry勒索病毒利用“永恒之蓝”漏洞洗劫全球150多个国家；12月底CPU特性漏洞曝光，几乎影响所有Windows、Linux等操作系统和相关软件

背景介绍 – 内部运行状况

业务类型

系统类型

系统数量

应用数量

目录

谈谈打补丁

发展历程

支持单一OS，
脚本化运行，
重复劳动多

支持单一OS，
将流程自动化，
降低重复劳动

支持多种OS，
可视化操作，
平台化管理

打补丁的问题

1. 漏洞定位
   - 哪些机器有哪些漏洞
   - 怎么从应用角度看漏洞
2. 补丁部署
   - 怎样跨平台
   - 怎样补才安全
   - 怎么验证结果
3. 关于打补丁的其他问题

漏洞发现

主动扫描

厂商通告

业界通告

Nessus Professional

Windows Server

CVE

QUALYS ON DEMAND SECURITY

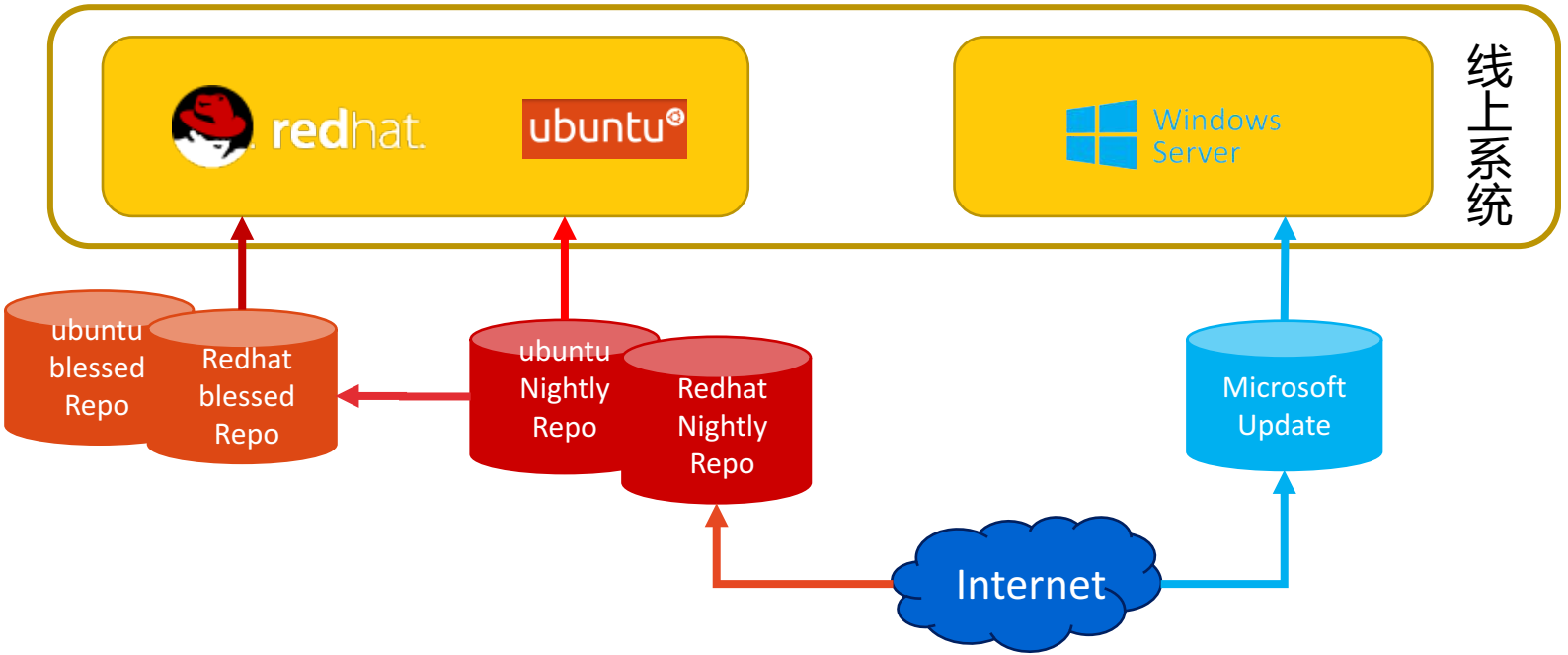
redhat

ubuntu

漏洞评估


IP-漏洞列表
配置管理系统
应用
漏洞列表
漏洞评估分级
紧急补丁(0day)
常规补丁
漏洞修补策略
系统补丁
应用补丁

基础架构


redhat
ubuntu
Windows Server
线上系统
ubuntu blessed Repo
Redhat blessed Repo
ubuntu Nightly Repo
Redhat Nightly Repo
Microsoft Update
Internet

补丁部署安全

GOPS2018
Shenzhen

补丁测试

测试环境中进行 兼容性，稳定性，LnP测试

异常防护

补丁前检测，软件包排除列表，只读文件系统检测，系统版本检查，等

抽样测试

生产环境中抽样，基于每个应用集群的每种OS，

灰度发布

多种灰度发布策略，3阶段，5阶段，定制等

补丁回滚

补丁部署后，如发现应用异常，回滚软件包到最初版本

结果验证

测试阶段

假阳性和假阴性

系统崩溃

软件包依赖性关系

系统性能变化

补丁生效依赖性

部署阶段

补丁部署覆盖率

Agent失效补全

增量新系统发现

补丁部署结果统计

其他问题

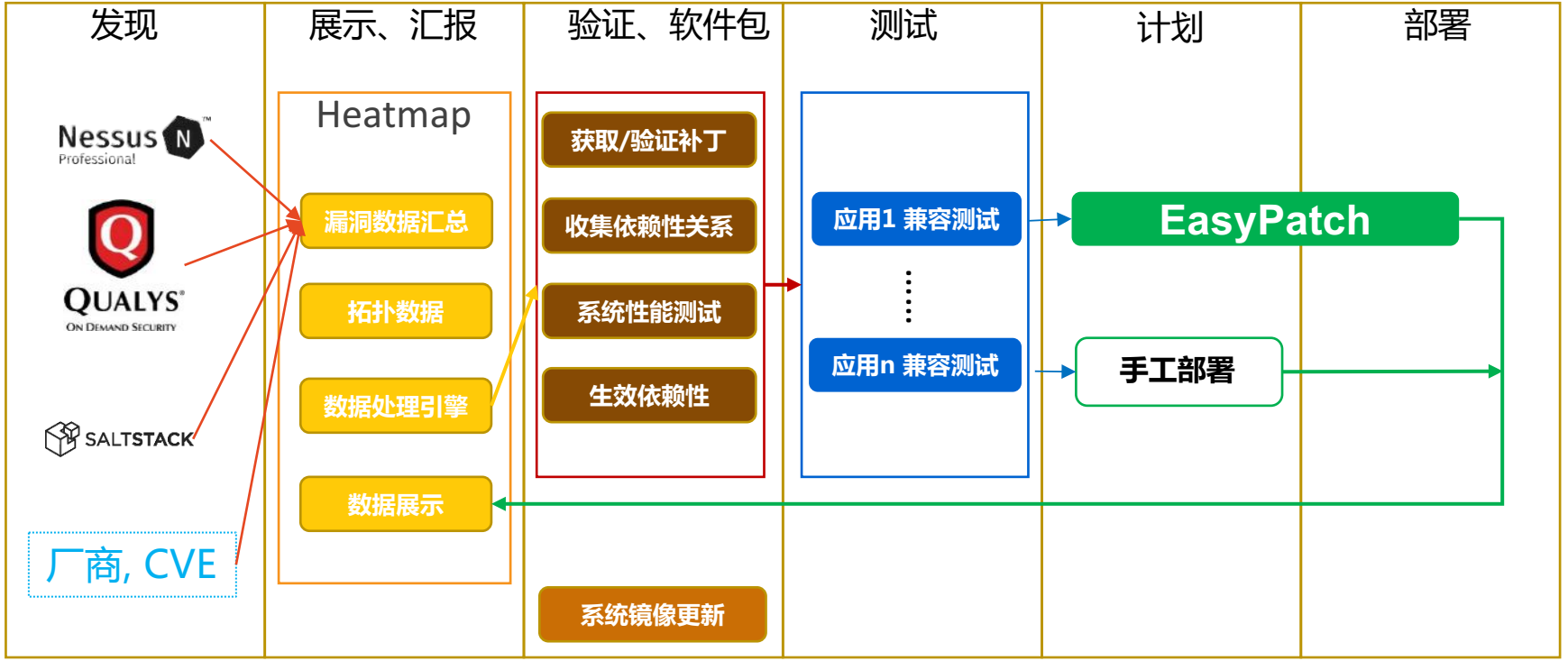
补丁部署和代码部署分开

补丁部署时标志

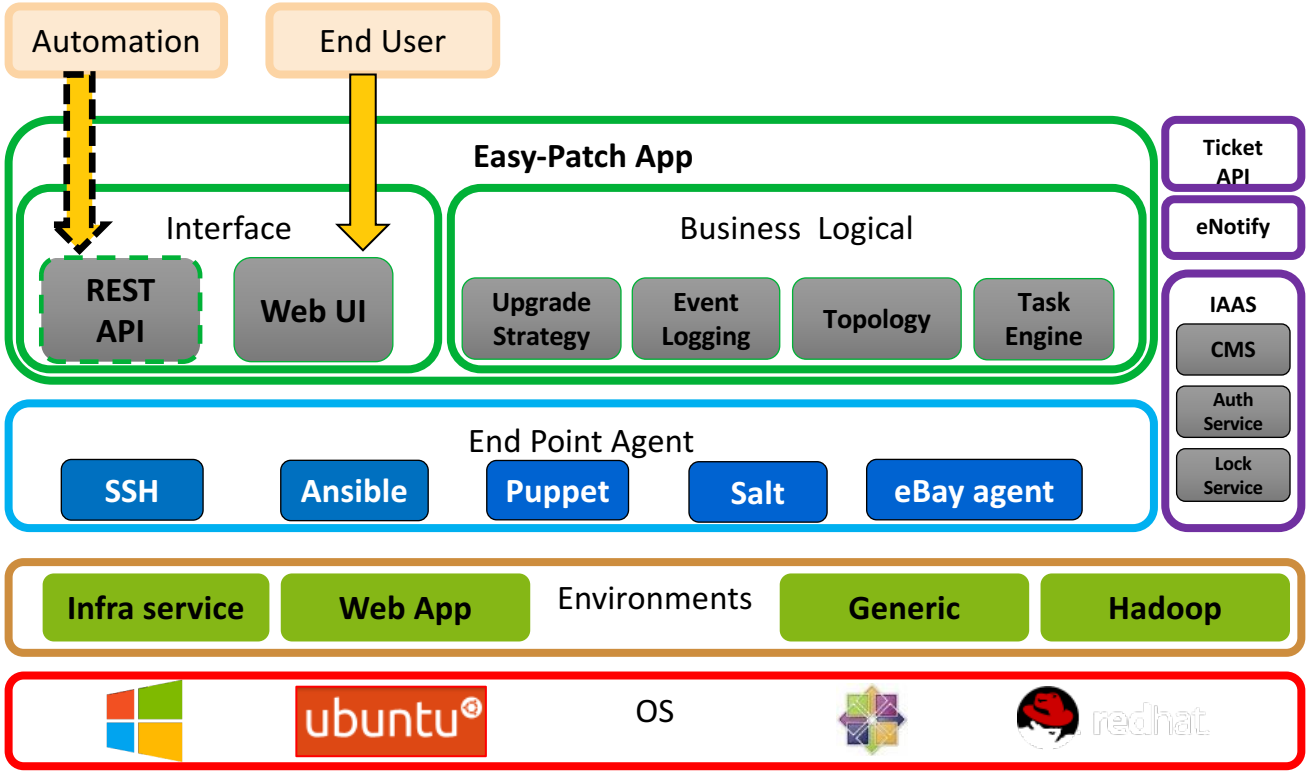
基于AD或者LDAP分组

目录

持续系统补丁平台


发现
展示、汇报
验证、软件包
测试
计划
部署
Nessus Professional
QUALYS ON DEMAND SECURITY
SALTSTACK
厂商, CVE
Heatmap
漏洞数据汇总
拓扑数据
数据处理引擎
数据展示
获取/验证补丁
收集依赖性关系
系统性能测试
生效依赖性
系统镜像更新
应用1 兼容测试
应用n 兼容测试
EasyPatch
手工部署

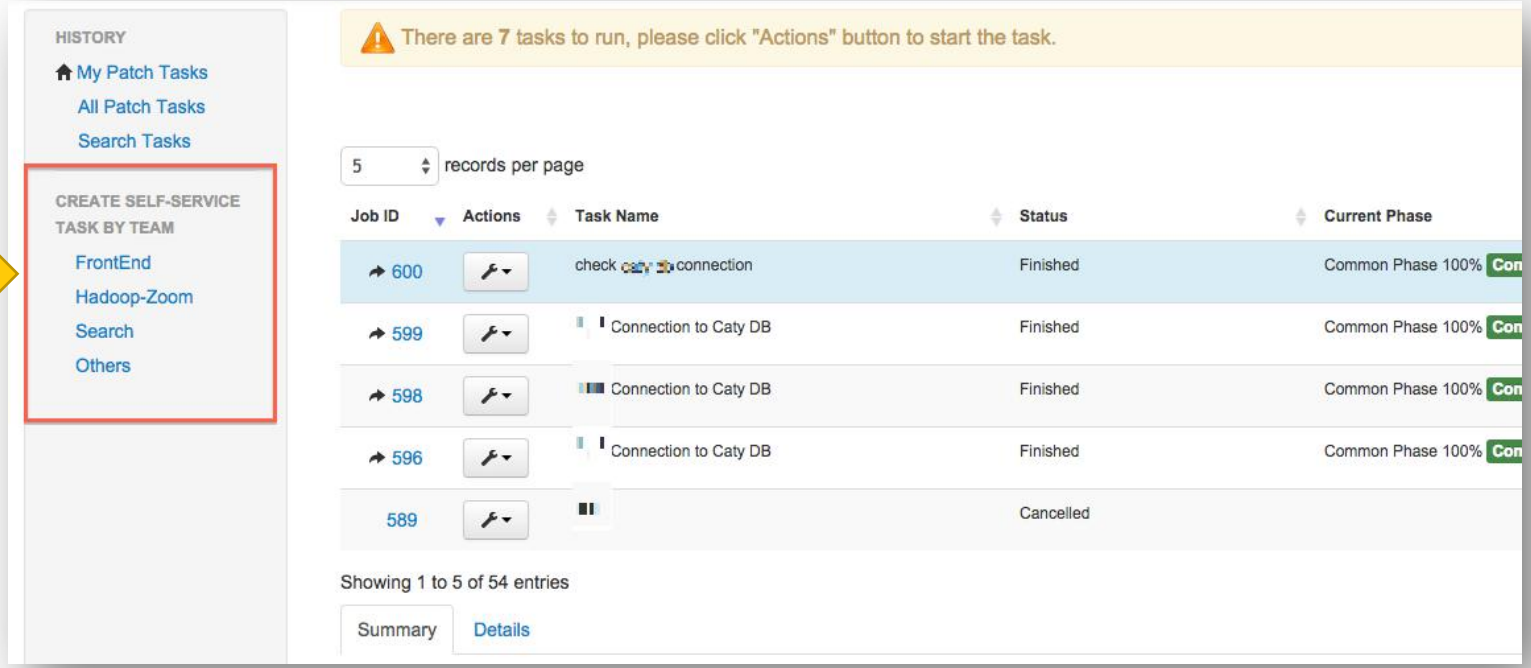
部署系统架构


Automation
End User
Easy-Patch App
Interface
REST API
Web UI
Business Logical
Upgrade Strategy
Event Logging
Topology
Task Engine
Ticket API
eNotify
IAAS
CMS
Auth Service
Lock Service
End Point Agent
SSH
Ansible
Puppet
Salt
eBay agent
Infra service
Web App
Environments
Generic
Hadoop
ubuntu
OS
redhat

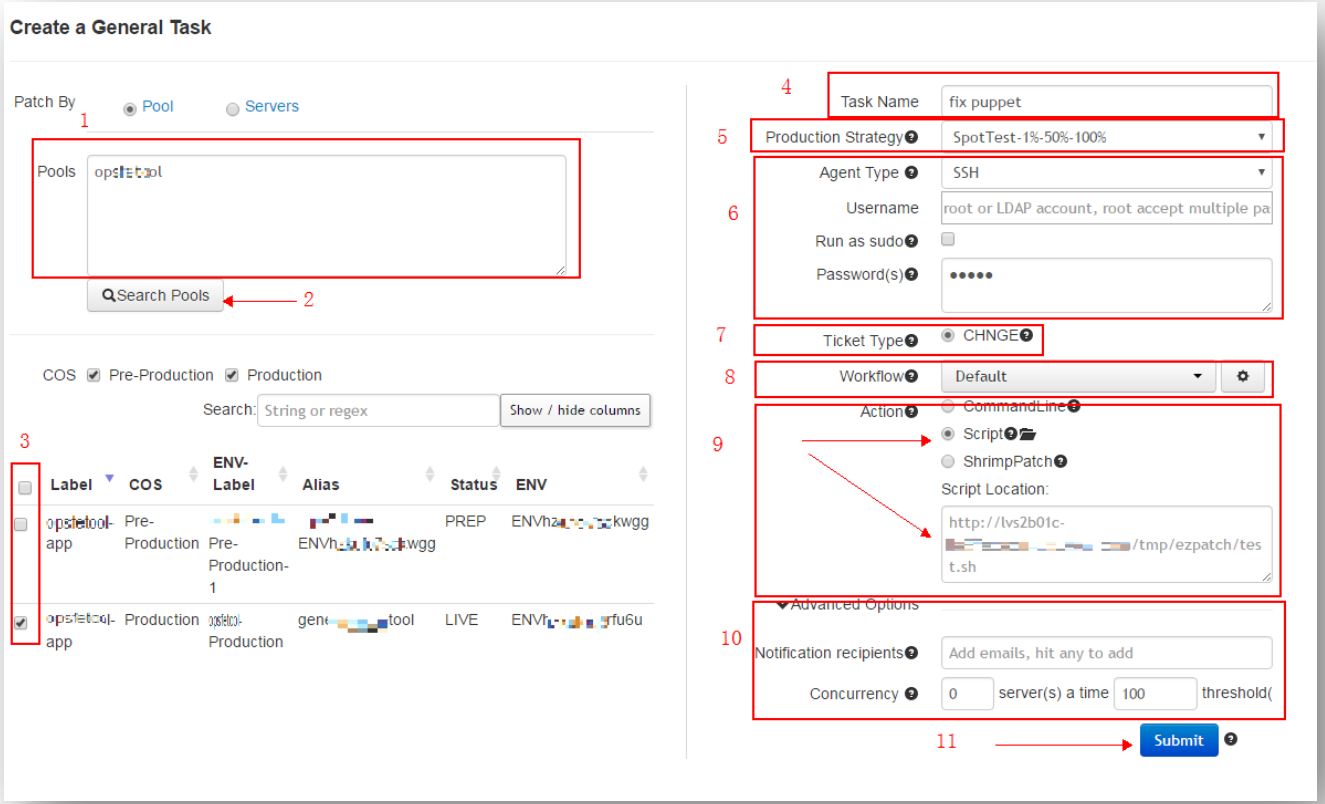
自助式服务

GOPS2018
Shenzhen

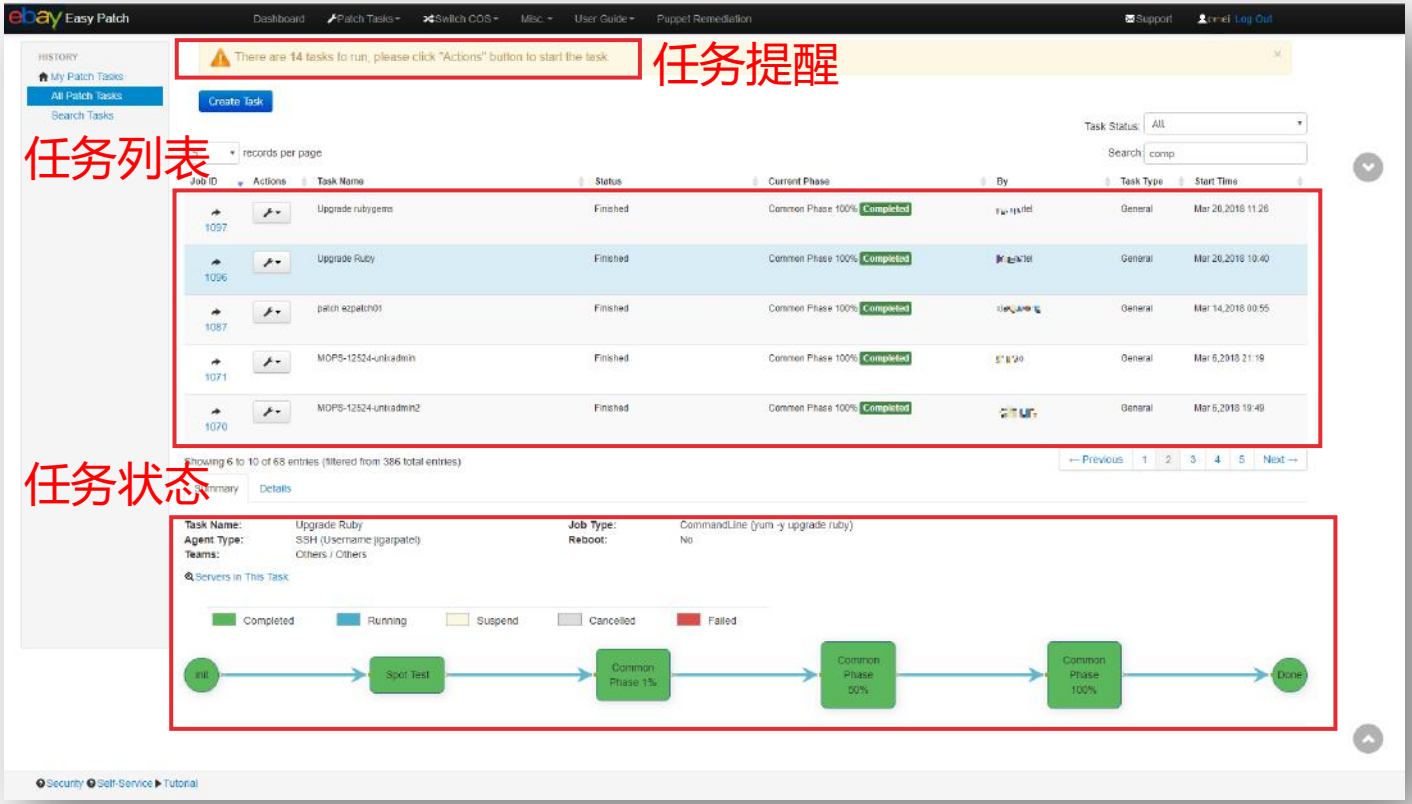
补丁可以让各团队可以集中式自助完成



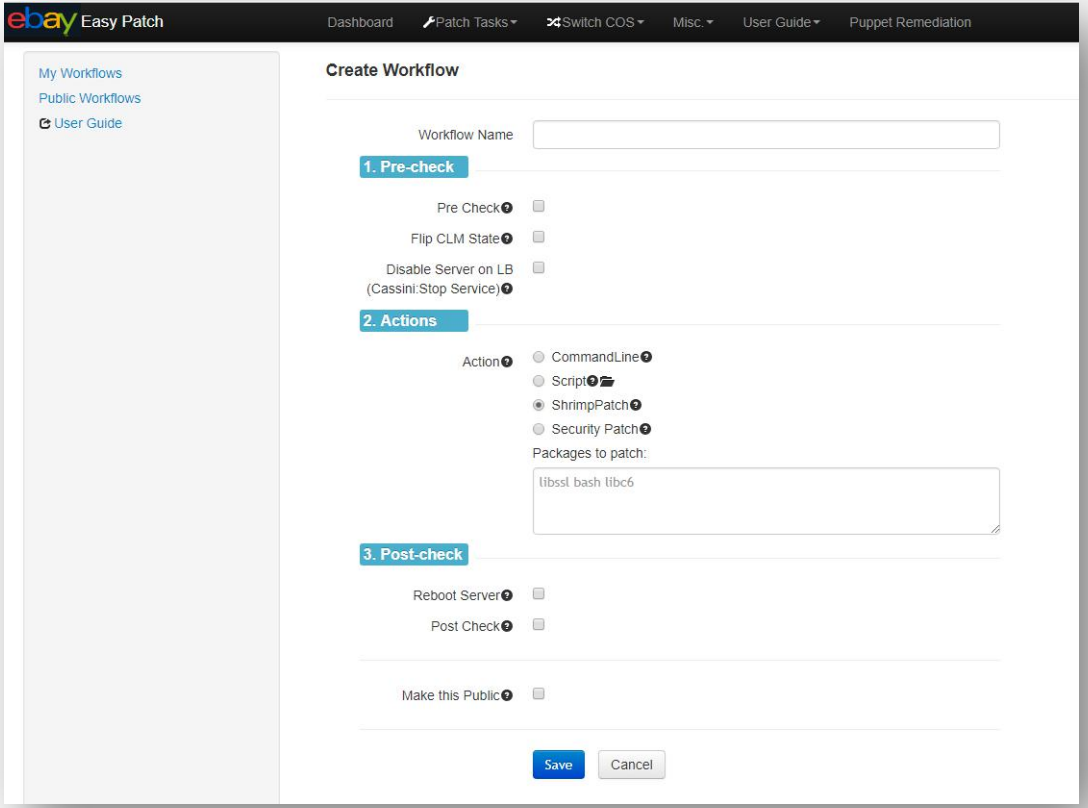
导览式任务创建


Create a General Task
Patch By
Pool
Servers
1
Pools
opsletool
Search Pools
2
COS
Pre-Production
Production
Search:
String or regex
Show / hide columns
3
Label
COS
ENV-Label
Alias
Status
ENV
opsletool-app
Pre-Production
Pre-Production-1
PREP
opsletool-app
Production
LIVE
4
Task Name
fix puppet
5
Production Strategy
SpotTest-1%-50%-100%
6
Agent Type
SSH
Username
root or LDAP account, root accept multiple pa
Run as sudo
Password(s)
7
Ticket Type
CHNGE
8
Workflow
Default
Action
CommandLine
9
Script
ShrimpPatch
Script Location:
http://lvs2b01c-
/tmp/ezpatch/test.sh
Advanced Options
10
Notification recipients
Add emails, hit any to add
Concurrency
0
server(s) a time
100
threshold(
11
Submit

可视化任务状态


Easy Patch
Dashboard
Patch Tasks
Switch COS
Misc
User Guide
Puppet Remediation
Support
Log Out
HISTORY
My Patch Tasks
All Patch Tasks
Search Tasks
There are 14 tasks to run, please click "Actions" button to start the task
任务提醒
Create Task
任务列表
records per page
Task Status: All
Search: comp
Job ID
Actions
Task Name
Status
Current Phase
By
Task Type
Start Time
1097 Upgrade rubygems Finished Common Phase 100% Completed General Mar 26,2018 11:26
1096 Upgrade Ruby Finished Common Phase 100% Completed General Mar 26,2018 10:40
1087 patch ezpatch01 Finished Common Phase 100% Completed General Mar 14,2018 00:55
1071 MOPS-12524-unixadmin Finished Common Phase 100% Completed General Mar 6,2018 21:19
1070 MOPS-12524-unixadmin2 Finished Common Phase 100% Completed General Mar 6,2018 19:49
Showing 6 to 10 of 68 entries (filtered from 386 total entries)
← Previous 1 2 3 4 5 Next →
任务状态
Summary
Details
Task Name: Upgrade Ruby
Agent Type: SSH (Username:jgarpatel)
Teams: Others / Others
Job Type: CommandLine (yum -y upgrade ruby)
Reboot: No
Servers in This Task
Completed
Running
Suspend
Cancelled
Failed
Init
Spot Test
Common Phase 1%
Common Phase 50%
Common Phase 100%
Done
Security
Self-Service
Tutorial

定制工作流


ebay Easy Patch
Dashboard
Patch Tasks
Switch COS
Misc.
User Guide
Puppet Remediation
My Workflows
Public Workflows
User Guide
Create Workflow
Workflow Name
1. Pre-check
Pre Check
Flip CLM State
Disable Server on LB (Cassini:Stop Service)
2. Actions
Action
CommandLine
Script
ShrimpPatch
Security Patch
Packages to patch:
libssl bash libc6
3. Post-check
Reboot Server
Post Check
Make this Public
Save
Cancel

整体部署情况


ebay Easy Patch
Dashboard
Patch Tasks
Switch COS
Misc
User Guide
Puppet Remediation
Support
Log Out
SECURITY
Security Home
Teams
C3
FrontEnd
Hadoop-Zoom
Raptor
Search
Others
GENERAL
General Home
EasyPatch Coverage
Zoom 1m 3m 6m YTD 1y All
From Oct 22, 201
To Jul 18, 201
Server Percentage
Job Count
75%
50%
25%
0%
20. Oct
17. Nov
15. Dec
12. Jan
23. Feb
25. Mar
20. Apr
18. May
15. Jun
13. Jul
27. Jul
Jobs
Servers With Vulns
Patched
Patched Server Percentage Each Team (Statistics Of: 201
C3
0 Jobs
0 QIDs
Coverage 0 %
Patching Process(%)
FrontEnd
21393 Jobs
108 QIDs
Coverage 95 %
Patching Process(%)
Hadoop-Zoom
0 Jobs
141 QIDs
Coverage 0 %
Patching Process(%)
Raptor
39819 Jobs
81 QIDs
Coverage 99 %
Patching Process(%)
Search
0 Jobs
188 QIDs
Coverage 0 %
Patching Process(%)

目录

未来展望

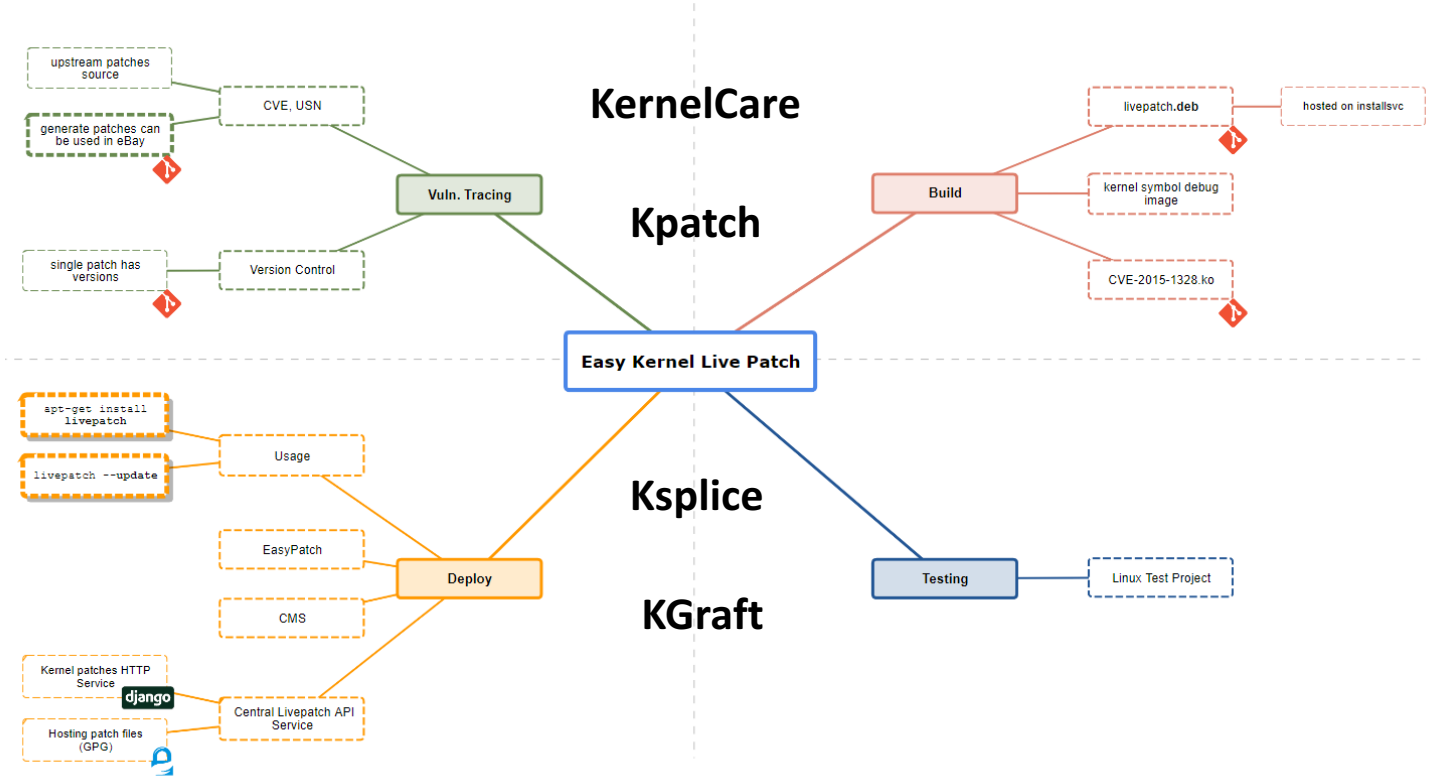
内核热补丁

容器和重装替代补丁

内核补丁

GOPS2018
Shenzhen

免重启，无宕机
热补
Linux内核



容器和重装代替补丁


TERMINAL BURCHARDKAI
应用和数据都在容器里
操作系统只是一个载体
HOUSTON EXPRESS
HAMBURG

打个补丁就这么溜

GOPS2018 Shenzhen

GOPS2018
Shenzhen

Thanks

高效运维社区

开放运维联盟

荣誉出品

想第一时间看到高效运维社区的新动态吗？

高维在线