

全站跨平台系统补丁自动化部署实践

梅岑恺 高级运维经理

目录



1

背景介绍

2

问题分析

3

系统架构

4

未来展望

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

24*7

业务类型

Windows
&
Linux

系统类型

十万
级

系统数量

数千
个

应用数量

目录

1 背景介绍

➔ **2** 问题分析

3 系统架构

4 未来展望

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

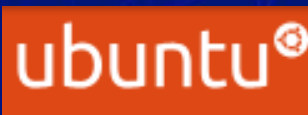
1. 漏洞定位
 - 哪些机器有哪些漏洞
 - 怎么从应用角度看漏洞
2. 补丁部署
 - 怎样跨平台
 - 怎样补才安全
 - 怎么验证结果
3. 关于打补丁的其他问题

漏洞发现

主动扫描



厂商通告



业界通告



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)

漏洞修补策略

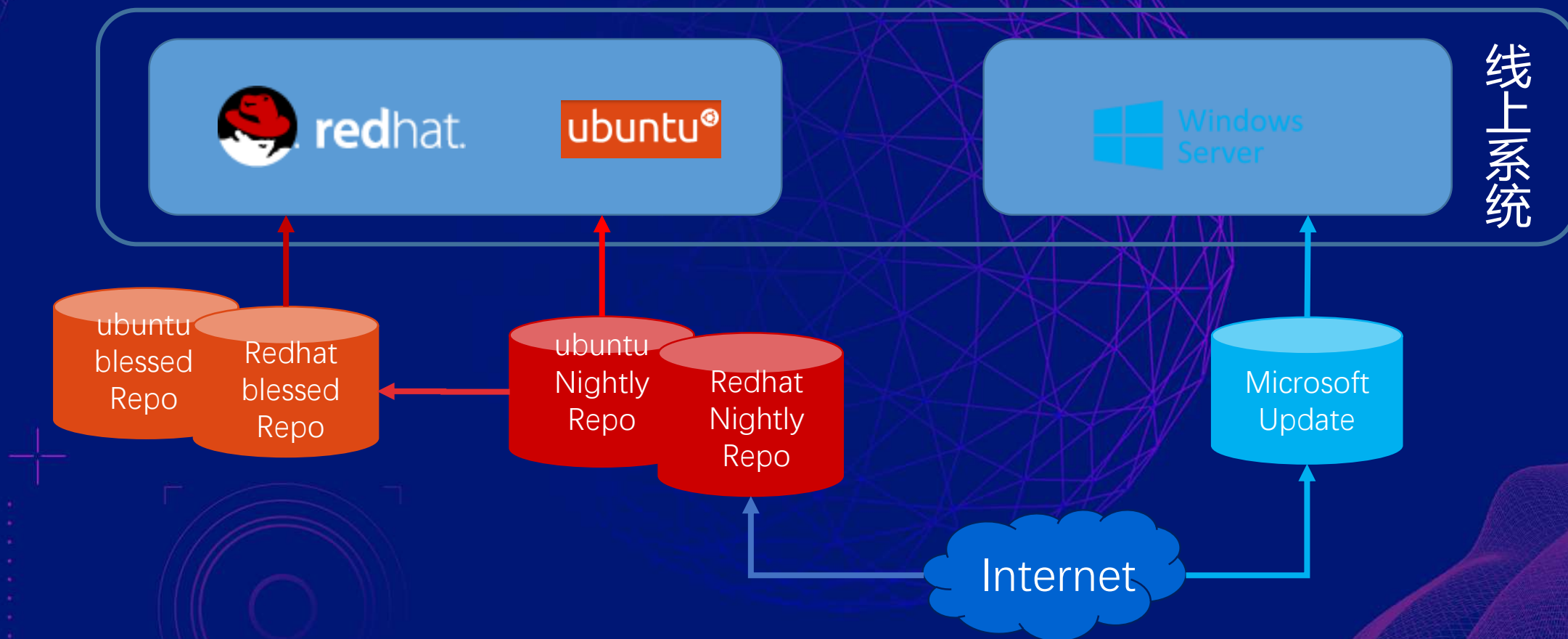
常规补丁

系统补丁



应用补丁

基础架构



补丁部署安全

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

容量问题

补丁部署和代码部署分开

监控问题

补丁部署时标志

权限管理

基于AD或者LDAP分组

目录

1 背景介绍

2 问题分析



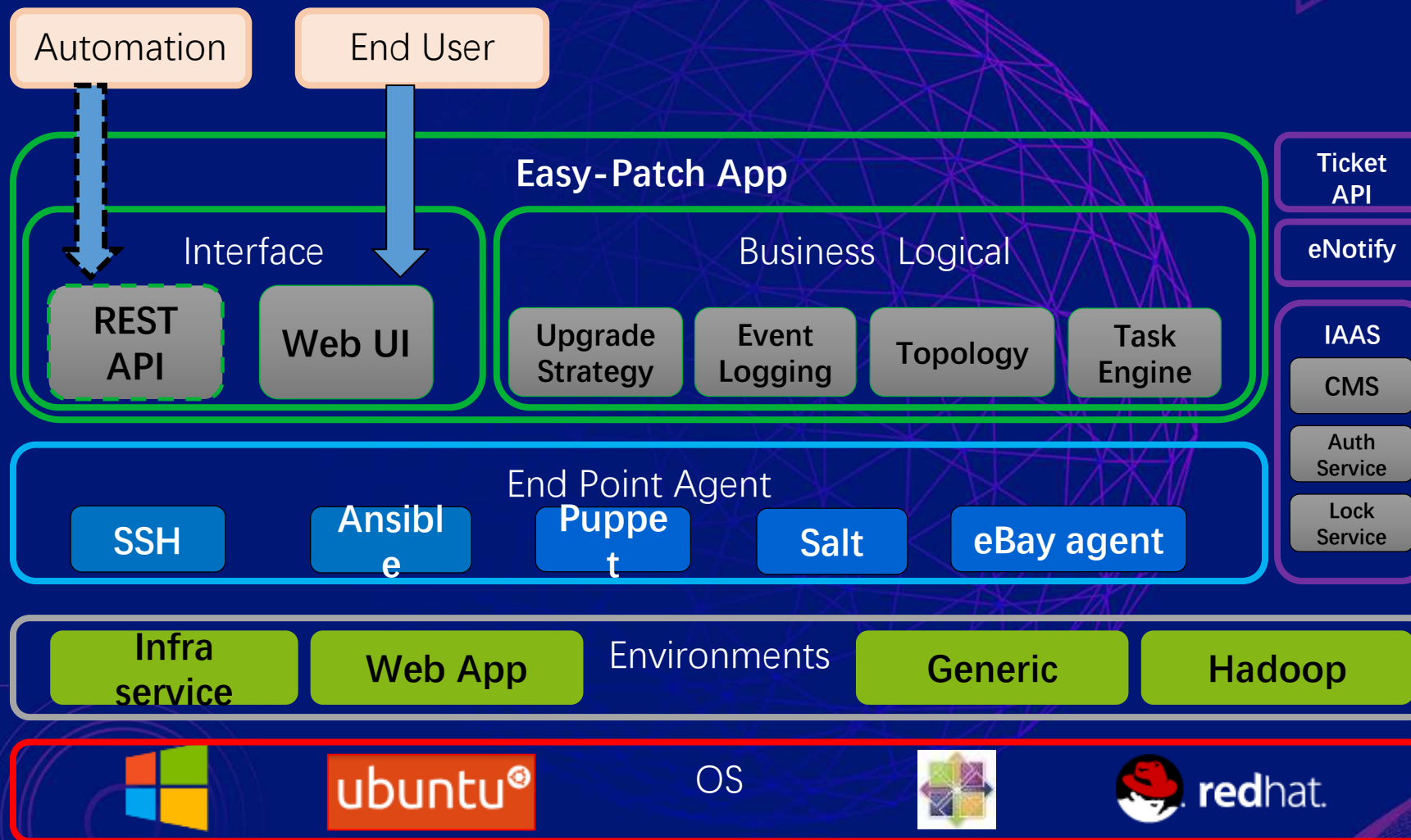
3 系统架构

4 未来展望

持续系统补丁平台



部署系统架构



自助式服务

补丁可以让
各团队可以
集中式自助
完成



HISTORY

- My Patch Tasks
- All Patch Tasks
- Search Tasks

CREATE SELF-SERVICE TASK BY TEAM

- FrontEnd
- Hadoop-Zoom
- Search
- Others

There are 7 tasks to run, please click "Actions" button to start the task.

5 records per page

Job ID	Actions	Task Name	Status	Current Phase
600		check connection	Finished	Common Phase 100% Con
599		Connection to Caty DB	Finished	Common Phase 100% Con
598		Connection to Caty DB	Finished	Common Phase 100% Con
596		Connection to Caty DB	Finished	Common Phase 100% Con
589			Cancelled	

Showing 1 to 5 of 54 entries

Summary Details

导览式任务创建

Create a General Task

Patch By

☒ Pool
☐ Servers

Pools

ops:tool

Search Pools

COS
☒ Pre-Production
☒ Production

Search: String or regex

Show / hide columns

☐ Label
☐ ops:tool-app

COS

Pre-Production

Production

ENV-Label

Pre-Production-1

Production

Alias

ENVh...

gentool

Status

PREP

LIVE

ENV

ENVh...

ENV...

Task Name

fix puppet

Production Strategy

SpotTest-1%-50%-100%

Agent Type

SSH

Username

root or LDAP account, root accept multiple pa

Run as sudo

☐

Password(s)

.....

Ticket Type

☒ CHNGE

Workflow

Default

Action

☐ CommandLine
☒ Script
☐ ShrimpPatch

Script Location:

http://lvs2b01c-.../tmp/ezpatch/tes
t.sh

Advanced Options

Notification recipients

Add emails, hit any to add

Concurrency

0

server(s) a time

100

threshold(

Submit

可视化任务状态

任务提醒

任务列表

Actions	Task Name	Status	Current Phase	By	Task Type	Start Time
	Upgrade rubygems	Finished	Common Phase 100% Completed	16014781	General	Mar 20, 2018 11:28
	Upgrade ruby	Finished	Common Phase 100% Completed	16014781	General	Mar 20, 2018 10:40
	patch script01	Finished	Common Phase 100% Completed	16014781	General	Mar 14, 2018 00:55
	MCP5-12524-upgrade1	Finished	Common Phase 100% Completed	518120	General	Mar 8, 2018 21:18
	MCP5-12524-upgrade2	Finished	Common Phase 100% Completed	518120	General	Mar 8, 2018 19:49

Showing 5 to 10 of 55 entries (filtered from 200 total entries)

任务状态

Task Name: Upgrade Ruby Job Type: CommandLine (yum -y upgrade ruby)
Agent Type: SSH (Username jgarpatel) Reboot: No
Teams: Others / Others

Servers in This Task

Completed Running Suspend Canceled Failed

Init -> Spec Test -> Common Phase 1% -> Common Phase 50% -> Common Phase 100% -> Done

定制 workflow

Easy Patch

DashboardPatch TasksSwitch COSMiscUser GuidePuppet 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

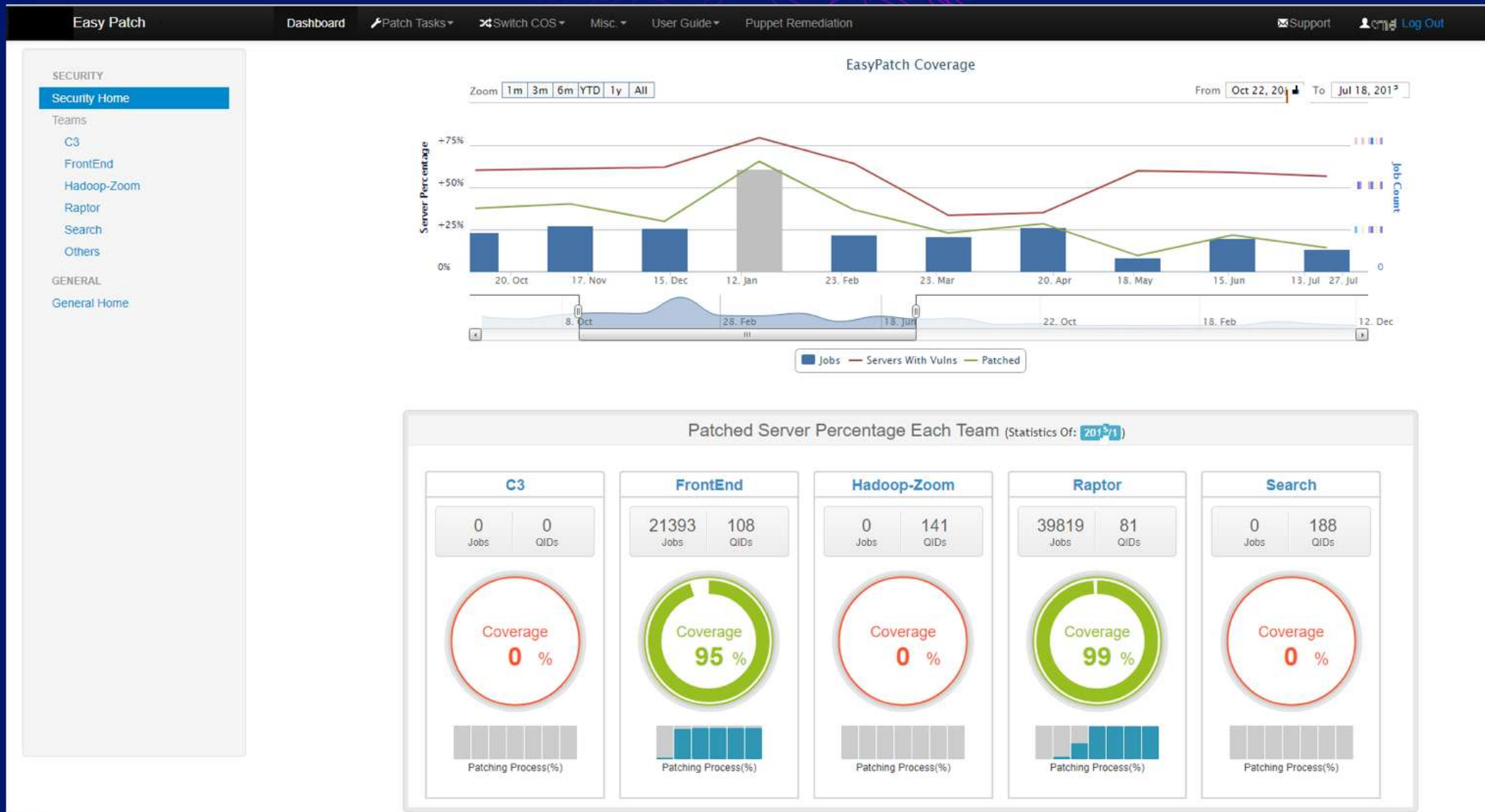
3. Post-check

Reboot Server

Post Check

Make this Public

整体部署情况



目录

1 背景介绍

2 问题分析

3 系统架构

 **4** 未来展望

A person stands on a rocky shore, looking out at the ocean during a sunset. The sun is low on the horizon, casting a long, bright reflection on the water. The sky is filled with colorful clouds, and the overall scene is serene and contemplative.

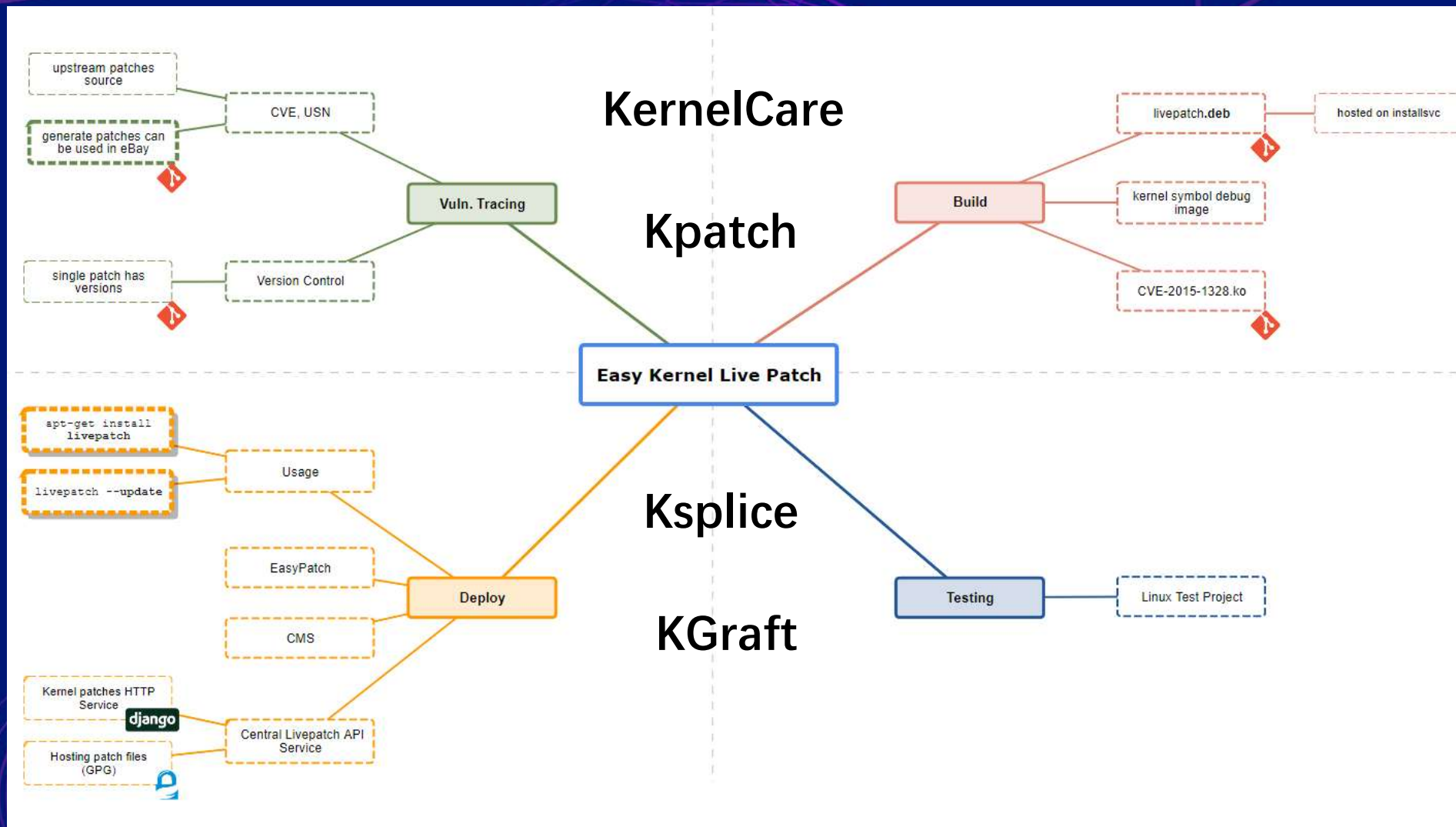
未来展望

内核热补丁

容器和重装 替代补丁

内核补丁

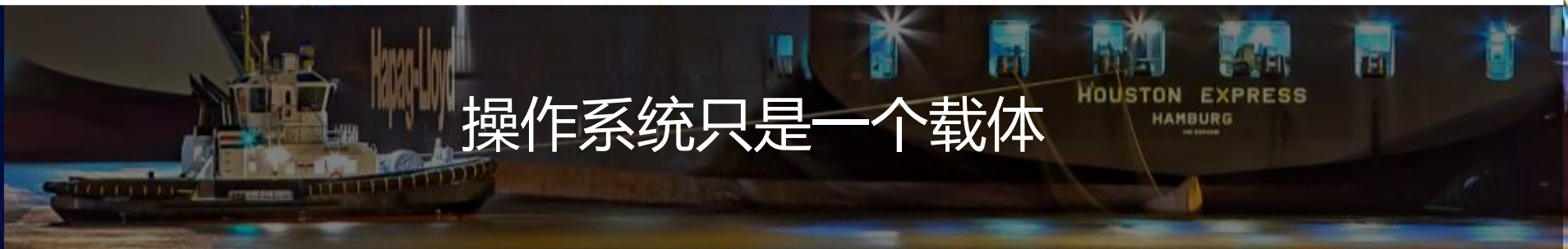
免重启，
无宕机
热补
Linux
内核



容器和重装代替补丁



应用和数据都在容器里



操作系统只是一个载体

A man with a surprised expression, wearing a white headband and a dark grey jersey with "Brooklyn" written on it, is holding a basketball. He is standing on an outdoor basketball court with trees in the background.

打个补丁就这么溜

本PPT来自2018携程技术峰会
更多技术干货，请关注“携程技术中心”微信公众号

