DevOps在重大活动网站安全保障中的应用

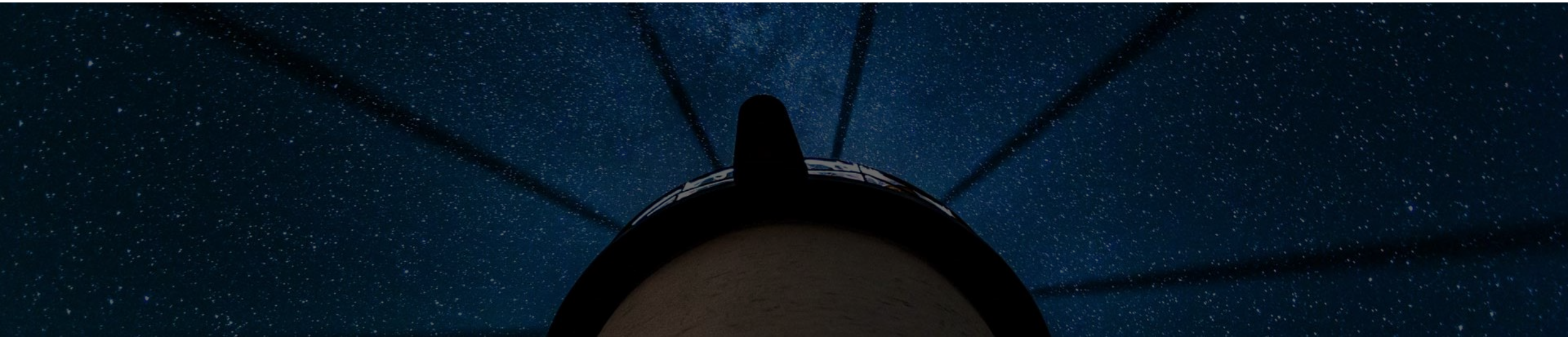
厦门大学 郑海山 https://dog.xmu.edu.cn

2017/11/24 武汉大学

CONTENT

01 静态网站安全性

SECURITY OF STATIC WEBSITES



相关信息

- 在金砖会晤和十九大期间，我们整个保障措施可以看许卓斌月初在安全工作组会议分享的《重点服务保障期间的安全实践》http://sec2017.eventdove.com/
- 静态网页安全防护可看《中国教育网络》2017年11月 P55页。电子版暂缺。
- DNS 安全：https://dog.xmu.edu.cn/images/paper/dns-query-log-analysis-system-based-on-open-source-software.pdf


网络安全：挑战·策略·应急

厦门大学

重大活动时期网站安全防护手册

姜开达：网络安全的特点是攻防高度不对称，黑客可以一点突破引发目标全线奔溃。作为防护的一方，全局体系任何一处都不能存在短板。

用户端浏览器 -> hosts文件 -> DNS -> 浏览器缓存 -> Safe Browsing -> 证书检查 ->网关/无线/路由器 -> 代理 -> CDN -> 防火墙 -> IPS/IDS -> WAF -> 负载均衡 -> 虚拟化宿主机 -> 虚拟机 -> 操作系统 -> HTTP服务器 -> HTTP服务器 WAF -> URL重写 -> 文件载入 -> 脚本解析 -> URL路由分发 -> Cache -> 数据库 -> 渲染结果 -> 压缩 -> HTTPS加包 -> 浏览器接收 -> 浏览器插件 -> JS渲染

《Westworld》 Teddy

简单和冗余的平衡

漏洞扫描
/FW/WAF/IPS/IDS/DDOS/Lynis/OpenScap/nmap/ClamAV/chkrookit/RootKit Hunter/Fail2ban/mod_evasive/mod_reqtimeout/mod_qos/OSSEC/mod_security

纵深防御

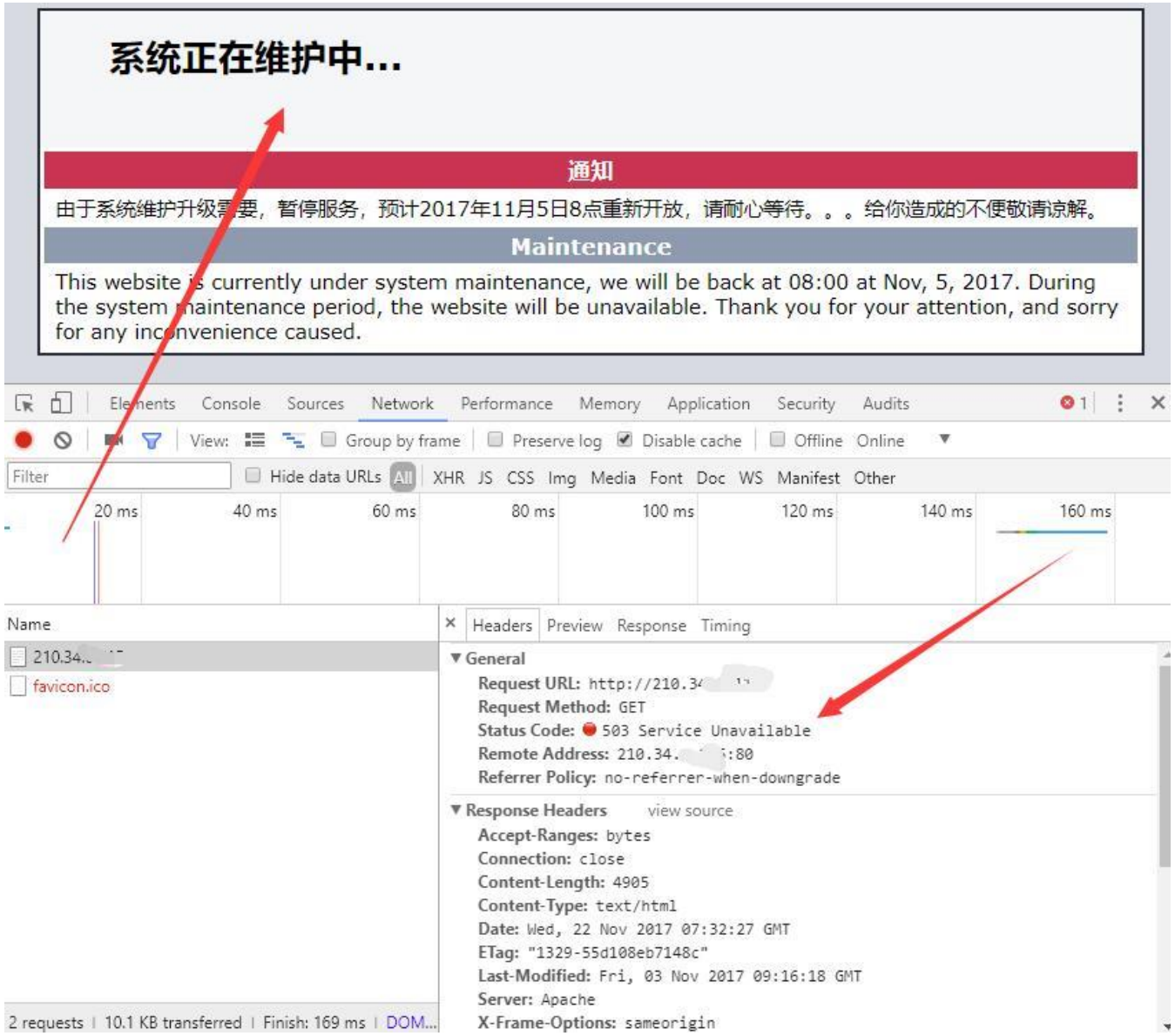
奥卡姆剃刀原则：若无必要，勿增实体
KISS（Keep It Simple, Stupid）

怼用户：你的问题，不是我的问题

云DNS投毒、CDN投毒、客户端本身ARP攻击、客户端接入商随意插入广告甚至被人截图后PS修改等。如发现应当及时下线，并执行检查，如果确定非自身因素则应当及时上线，并在页面上显著位置公布以消除不良影响。

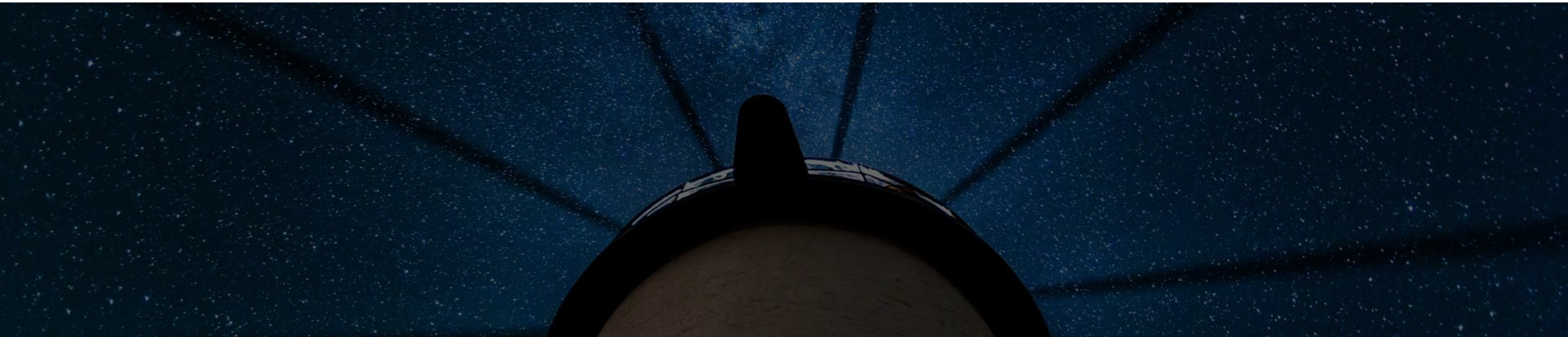
通知页面的技巧

- 对于一些存在安全隐患而被暂时性下线的网站，可使用应用交付设备或者把DNS导入到一个特定的通知页面，以减少突然关闭对网站管理员和浏览者带来的不便。
- 为避免临时性替换网站页面内容导致搜索引擎删除原有网站信息，通知页面应当返回503 HTTP状态码，也可根据恢复时间指定Retry-After返回值。



02 DevOps介绍

INTRODUCTION

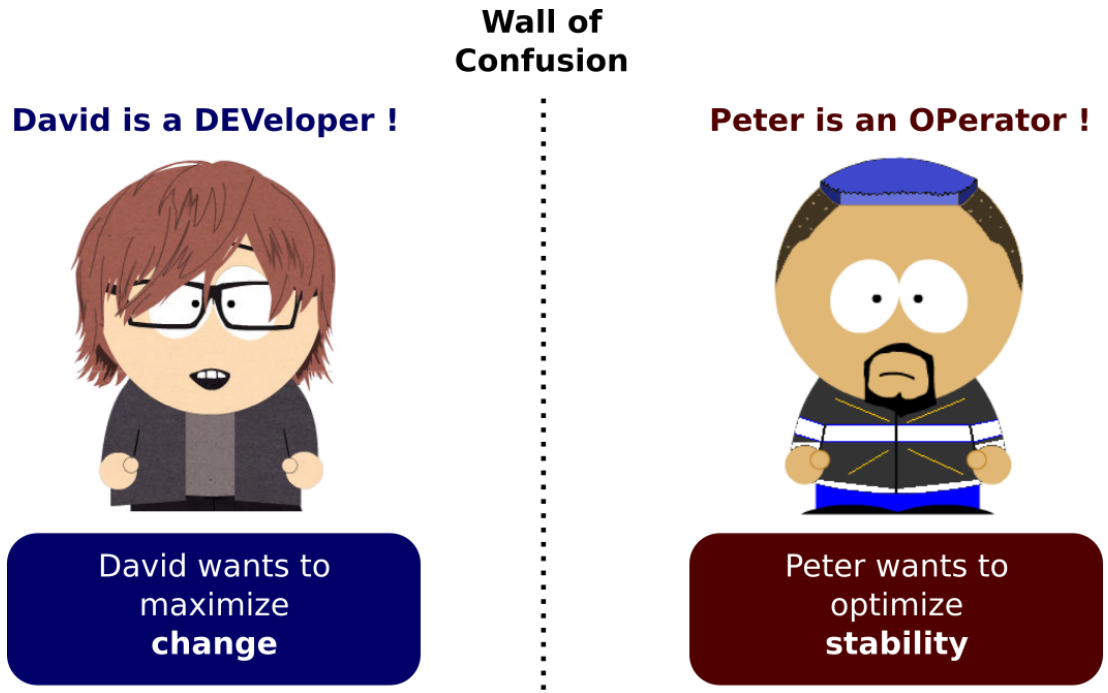


DevOps介绍

DevOps（Development和Operations的组合词）是一种重视“软件开发人员（Dev）”和“IT运维技术人员（Ops）”之间沟通合作的文化、运动或惯例。透过自动化“软件交付”和“架构变更”的流程，来使得构建、测试、发布软件能够更加地快捷、频繁和可靠。 wikipedia.org

DevOps是一种方法论，其中包含一系列基本原则和实践。
http://www.infoq.com/cn/articles/detail-analysis-of-devops

宽以待己，严以律人的开发



话说天下大势，分久必合，合久必分

开发和运营之间的矛盾：

开发不希望产品经理频繁变更需求，运营不希望开发随意变更软件运行环境。

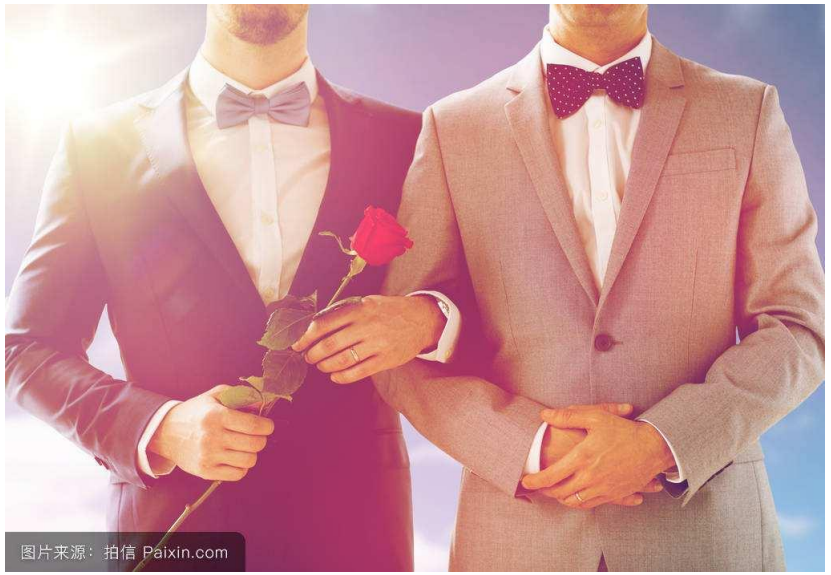
“在我的电脑上运行得好好的”

开发只关注实现功能，性能让运维处理。

分层，关注点分离

Dev和Ops结合，Dev不能只搞开发，也要去蹚运维的浑水。运维要把触角伸到开发。

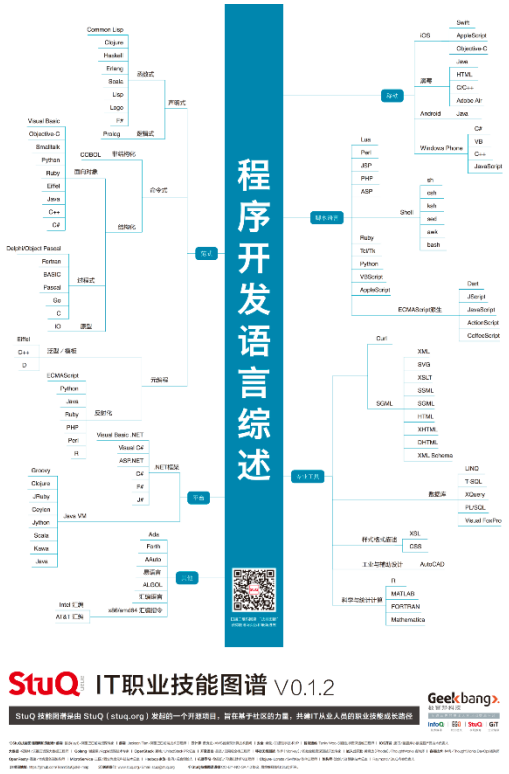
新名词：DevSecOps



带来新的问题

技能点要求不同：前端工程师、后端工程师、iOS工程师、Android工程师、架构师、DBA、网络工程师、基础架构工程师、发布经理。

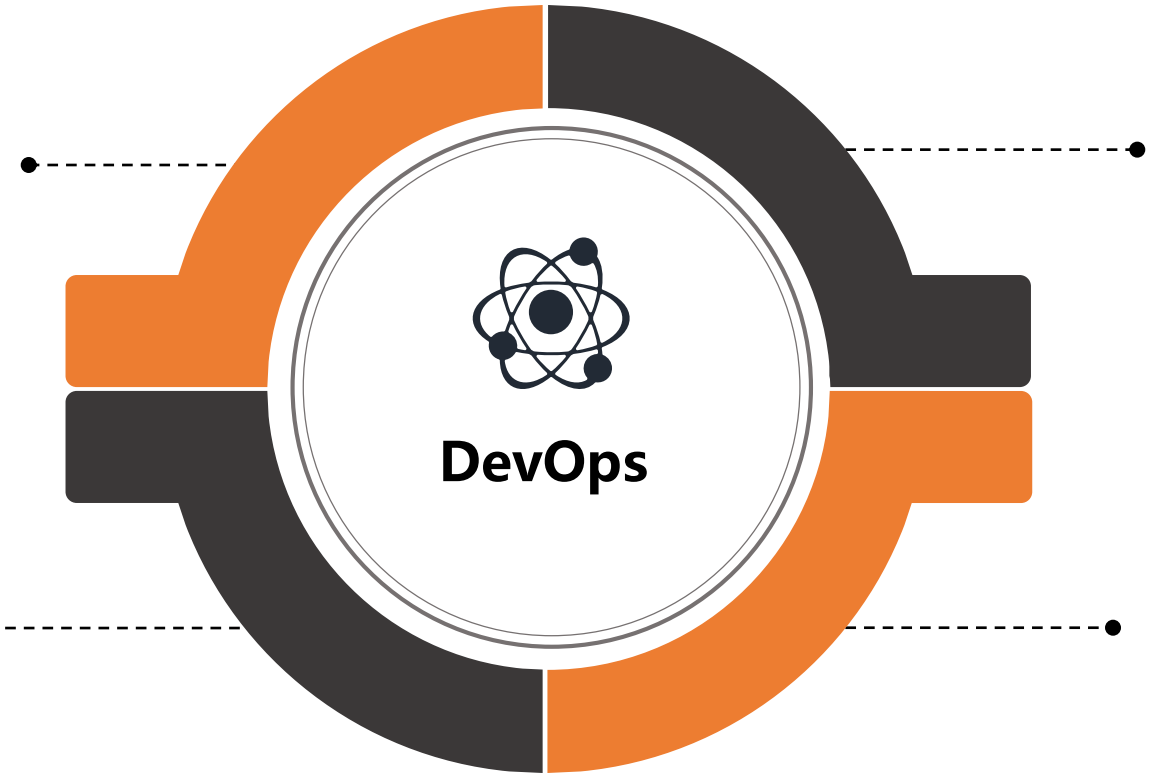
成本不同。



https://github.com/TeamStuQ/skill-map

基础架构代码化

- 解放效率，可复制。
- 可重复运行，幂等 1^n。
- 减少人为出错，执行人员可替换。
- 代码就是文档，方便审计。
- 版本控制，变更记录。



不可变服务器

- 改变部署的方法，原先替换一个文件，现在可以替换整个服务器。
- 打补丁更安全。
- 蓝绿部署。
- 金丝雀发布。

反馈快

走太快容易扯着X，小步快跑
每天部署几百次
编译测试要快

部署流水线

管道，链式调用，部署流水线，Gulp或者Grunt

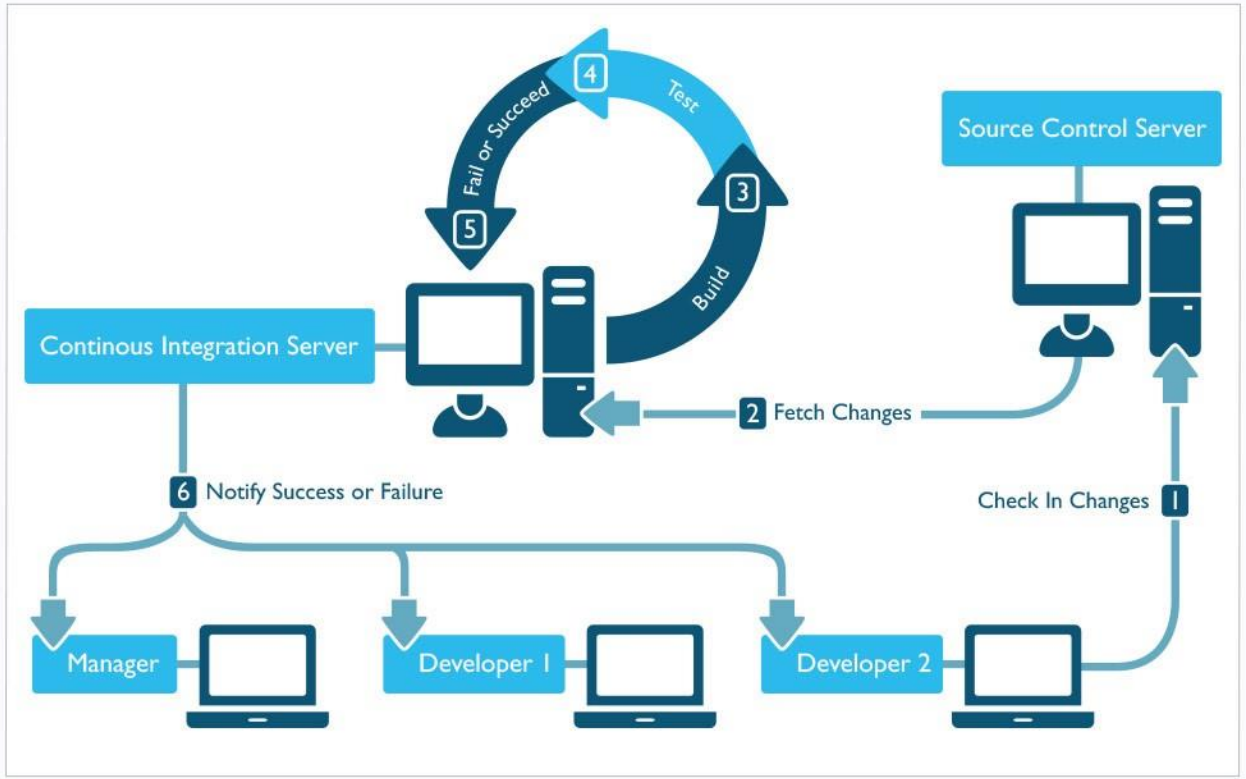
管道示例：

```
cat dog.txt | sort | uniq -c | sort -n -r -k 1 -t ' ' | awk -F '//' '{print $2}' | head -5
```

JavaScript链接调用示例：

```
d3.select("#wordcloud_topN_by_post")
    .append("svg")
    .style("width", "100%")
    .attr("preserveAspectRatio", "xMidYMin meet")
    .append("g")
    .attr("transform", "translate(100, 100)")
    .selectAll("text")
    .data(words).enter().append("text")
    .style("font-size", function(d) { return d.size + "px"; })
    .style("font-family", "Impact")
    .style("fill", function(d, i) { return color(i); })
    .attr("text-anchor", "middle")
    .text(function(d) { return d.text; })
```

部署流水线：开发 -> 单元测试 -> 提交Git -> Pull代码 -> 编译 -> 测试 -> JavaScript混淆整合最小化版本化 -> 图片优化整合 -> 打包编译Docker -> 自动化集成测试 -> 正式环境配置 -> 数据库Migrate -> 蓝绿发布 -> 正式发布 -> 监控



http://insights.sei.cmu.edu

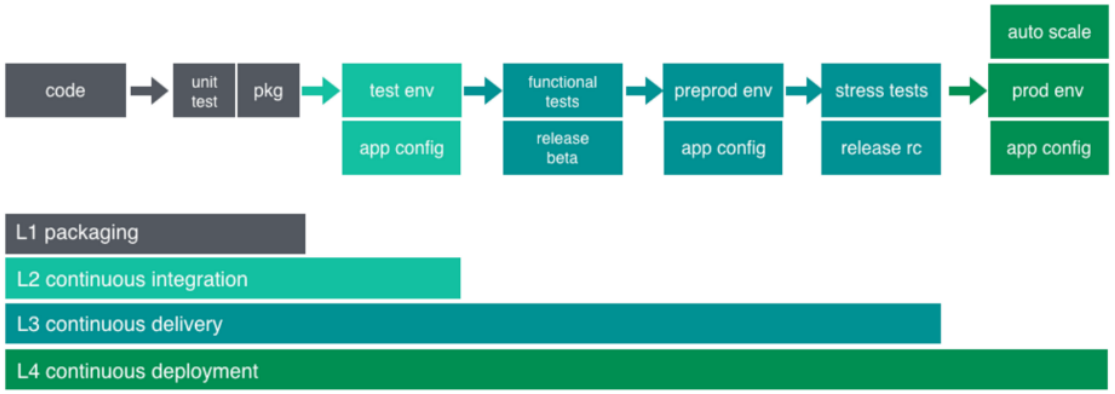


Figure: Continuous deployment maturity model

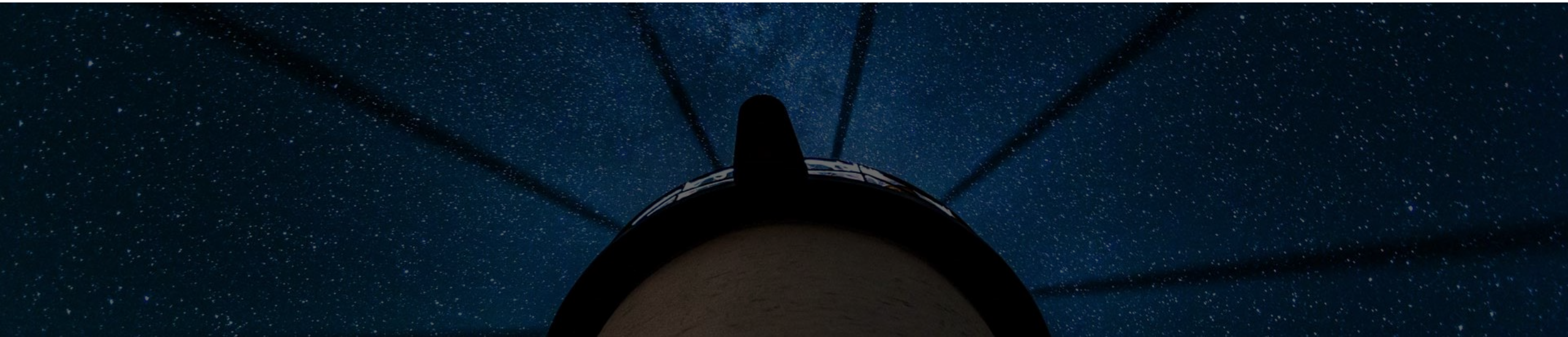
https://dzone.com

Why Ansible

Ansible，主控模式，依赖小，通过SSH，基于Python，YAML语法。顺序执行。
Puppet，Pull模式。Ruby，DSL语法。执行顺序必须显式写出依赖。
Chef
SaltStack
CFEngine

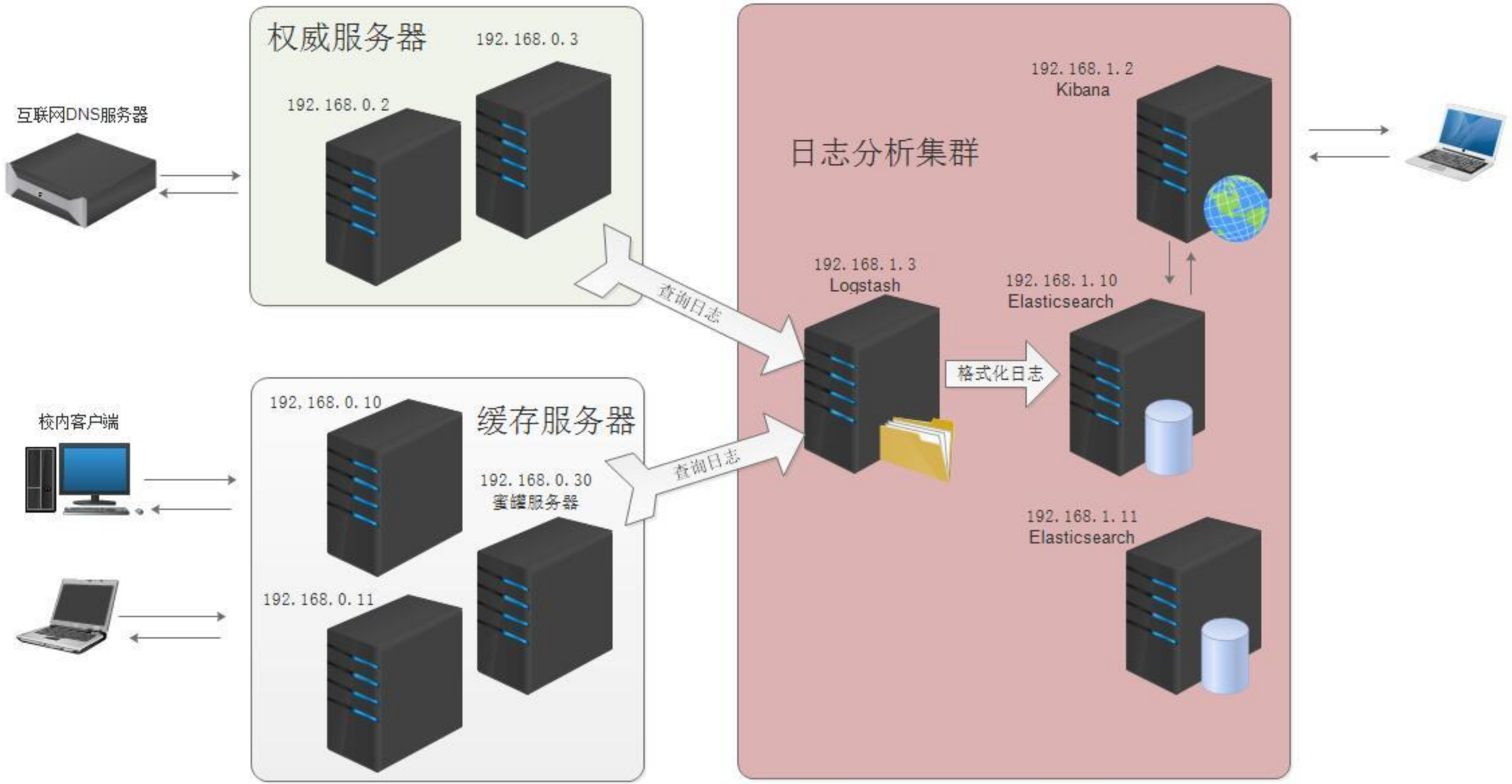
03 应用和落地

PRACTICE



厦门大学主页安全保障中应用

- 基础架构代码化
- 静态网站生成自动化：wget下来，Python脚本更改链接地址，PhantomJS截图
- DNS自动化：更改条目后，跑一个命令reload.sh，自动比对所有DNS条目是否有备案，没有备案劫持到通知页面，域名指向校外IP直接忽略。Master/Master 架构复制，更新缓存服务器的.xmu.edu.cn域，dig测试view和4台服务器解析是否正确。
- 巡检自动化：Ansible获取Facts，比对。


权威服务器
192.168.0.3
192.168.0.2
互联网DNS服务器
查询日志
日志分析集群
192.168.1.2
Kibana
192.168.1.3
Logstash
192.168.1.10
Elasticsearch
格式化日志
192.168.1.11
Elasticsearch
校内客户端
192.168.0.10
缓存服务器
192.168.0.30
蜜罐服务器
192.168.0.11
查询日志

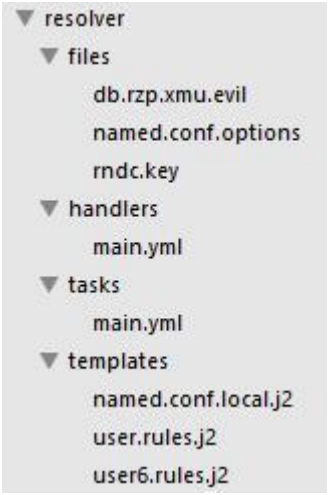
ansible-playbook site.yml -i hosts.production


```
[master-server]
210.34.0.    is_controller=true
210.34.0.    is_controller=false

[resolver-server]
210.34.0.
210.34.0.

[elasticsearch-server]
172.27.64.    jvm_memory_minmax=26

[logstash-server]
172.27.77.

[kibana-server]
172.27.77.
```

hosts.production定义IP和服务器名

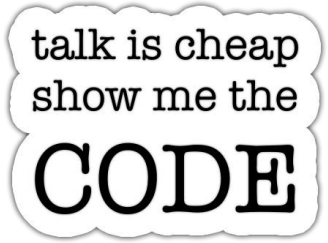
```
---
- name: master
  hosts: master-server
  roles:
    - common
    - master
    - { role: filebeat, document_type: 'nslog' }

- name: resolver
  hosts: resolver-server
  roles:
    - common
    - resolver
    - { role: filebeat, document_type: 'dnslog' }
  tags:
    - debug

- hosts: elasticsearch-server
  roles:
    - common
    - elasticsearch

- hosts: logstash-server
  roles:
    - common
    - logstash

- hosts: kibana-server
  roles:
    - common
    - kibana
```

site.yml定义服务器的角色



- task/main.yml定义角色的具体操作内容
- 我需要安装什么软件
- 我的软件如何配置（修改配置文件）

```
- name: Update all packages to the latest version
  apt:
    update_cache: yes
    cache_valid_time: 864000  # 86400 1 day
    upgrade: dist
    autoclean: yes
    autoremove: yes
    purge: yes
  become: true

- name: install apache2
  package:
    pkg: apache2
    state: installed
  become: true

- name: install php7.0-xml
  package:
    pkg: php7.0-xml
    state: installed
  become: true
  notify: restart apache2

- file: path=/var/www/cache/ state=directory owner=www-data group=www-data
  become: true

- name: copy www.conf
  template: src=www.conf.j2 dest=/etc/apache2/sites-available/www.conf owner=root group=root mode="a+r"
  vars:
    conf_type: http
  become: true
  notify: restart apache2

- apache2_module:
    state: absent
    name: "{{ item }}"
    force: true
  become: true
  with_items:
    - autoindex
    - alias
  notify: restart apache2

- apache2_module:
    state: present
    name: "{{ item }}"
  become: true
  with_items:
      - ssl
      - rewrite
      - headers
  notify: restart apache2
```



```
- ufw:
    state: reset
  become: true

- ufw:
    state: enabled
    policy: deny
  become: true

- ufw:
    rule: allow
    port: 22
  with_items:
    - {{host}}

- ufw:
    rule: allow
    port: 5044
  with_items:
    - {{host}}
```

```
TASK [kibana : start kibana] ***************************************************
ok: [172.27.

TASK [kibana : lineinfile] *****************************************************
ok: [172.27.

TASK [kibana : lineinfile] *****************************************************
ok: [172.27

PLAY RECAP *********************************************************************
172.27.                    : ok=31   changed=0    unreachable=0    failed=0
172.27.                    : ok=17   changed=0    unreachable=0    failed=0
172.27.                    : ok=18   changed=0    unreachable=0    failed=0
210.34.                    : ok=28   changed=0    unreachable=0    failed=0
210.34.                    : ok=36   changed=0    unreachable=0    failed=0
210.34.                    : ok=35   changed=0    unreachable=0    failed=0
210.34.                    : ok=28   changed=0    unreachable=0    failed=0
```

```
- ufw:
    state: enabled
    policy: deny
  become: true
  tags: testufw

- name: copy user.rules
  template: src=user.rules.j2 dest=/etc/ufw/user.rules owner=root group=root
  become: true
  notify: restart ufw
```

user.rules.j2

```
{% for host in groups['master-server'] %}
    {% if hostvars[host].is_controller == 'true' %}
### tuple ### allow tcp 22 0.0.0.0/0 any {{host}} in
-A ufw-user-input -p tcp --dport 22 -s {{host}} -j ACCEPT
    {% endif %}
{% endfor %}

{% for host in groups['master-server'] + groups['resolver-server'] %}
### tuple ### allow tcp 5044 0.0.0.0/0 any {{host}} in
-A ufw-user-input -p tcp --dport 5044 -s {{host}} -j ACCEPT
{% endfor %}
```

conf.d目录

apache: /etc/apache2/conf-enabled

crontab: /etc/cron.daily

included local_setting.conf

```
- lineinfile:
    path: /etc/apache2/conf-enabled/security.conf
    regexp: '^ServerTokens'
    line: 'ServerTokens Prod'
  become: true
  notify: restart apache2

- lineinfile:
    path: /etc/apache2/conf-enabled/security.conf
    regexp: '^ServerSignature'
    line: 'ServerSignature Off'
  become: true
  notify: restart apache2

- lineinfile:
    path: /etc/apache2/conf-enabled/security.conf
    regexp: '#?Header set X-Frame-Options: "sameorigin"'
    line: 'Header set X-Frame-Options: "sameorigin"'
  become: true
  notify: restart apache2

- blockinfile:
    path: /etc/elasticsearch/elasticsearch.yml
    block: |
        indices.breaker.fielddata.limit: 9gb
        http.cors.enabled: true
        http.cors.allow-origin: "*"
  become: true
  notify: restart Elasticsearch
```

谢谢

厦门大学 郑海山
https://dog.xmu.edu.cn

标注

字体使用	英文 微软雅黑
	中文 微软雅黑
行距	正文 1.3
背景图片出处	OfficePLUS Pexels
模板作者	Healthyyang2

OfficePLUS