OS选型

- 推荐使用CentOS 7.4 （kernel 3.10.0-693.el7.x86_64)。
- 推荐（次要）使用CentOS 6.9（kernel 2.6.32-696.el6.x86_64)。
- 如有其他需求，请需求方说明原因。

基础设定 Base

- hostname 命名规则

> 系统名称-应用名称-编号
> 如：SCRM-Redis-01

- lvm 命名规则

> --vg_name--lv_mountpoint

- 时区

> Asia/Shanghai

- 语言

> UTF-8

文件系统 Filesystem

- LinuxOS使用的文件系统大小为100G
- boot

> 创建Standard Partition挂载至/boot，大小为1024Mib，格式为：xfs(centos7)/ext4(centos6)

- vg_os

> 将该块硬盘上的剩余空间全部以pv的形式提供给vg_os，该空间将用于创建/、swap以及将直接安装至/下的software。

- lv_root

> 于vg_os下创建lv_root，大小为50Gib，并以xfs(centos7)/ext4(centos6)格式挂载于/

- swap

> 于vg_os下创建lv_swap，swap空间大小原则如下：

- 针对项目组需求对应创建相应的卷组和逻辑卷，并挂载至相应mountpoint

> 如：/dev/mapper/vg_data-lv_data -> /data`
> 格式为：xfs(centos7)/ext4(centos6)

网络Network

- VirtualMachine 网络配置

> 通过/etc/udev/rules.d/70-persistent-net.rules(CentOS6)60-net.rules(CentOS7)进行指定网卡MAC、网卡名称及网络接口文件，确定均使用eth0作为生产网络。

- 在网卡配置文件中配置DNS

> DNS1=10.8.6.10
> DNS2=172.17.0.10

- Hosts

> 添加本地IP与hostname的解析记录
> *例如*:
> 127.0.0.1 zabbix-server localhost localhost.localdomain
> 10.8.6.16 zabbix-server

系统服务 System-Service

- 关闭firewalld（centos7）iptables(centos6)
- 关闭selinux
- 关闭kdump
- 关闭NetworkManager(centos6)
- 关闭postfix
- 配置时间同步chrony(centos7)/ntp(centos6)

> ntpserver 10.8.6.11

- 升级并统一openssl与openssh版本

> openssh 7.4p1 prefix=/usr/local/openssh
> openssl 1.0.2k prefix=/usr/local/openssl

预安装包 Pre-install-package

- lrzsz
- net-tools
- vim
- bash-completion
- nc
- iotop
- iftop
- ipmitool
- bind-libs
- bind-utils

- libselinux-python
- python-devel
- tcpdump
- dstat
- iptraf

管理服务 Management-Service

- 安装监控zabbix-agent
- 配置账户管理ldap
- 安装CMDB gse-agent

用户权限

- 锁定无效用户
- 建立sauser,uid=2048，权限同root用户
- 建立devuser，uid=2047

> 前期权限较大，后期逐步裁剪权限 同root权限，ALL=ALL(NOPASSWORD)除下列权限：
>
> - 禁止vim(vi) /etc/sudoers
> - 禁止su
> - 禁止passwd root
> - 禁止 vim(vi) /etc/passwd /etc/shadow homedir: /home/devuser/

内核参数

- /etc/security/limits.conf

> 关闭CoreDump
> * soft core 0
> * hard core 0
> 修改用户打开最大文件描述符限制 - '* - nofile 165535'
> - '* soft nofile 165535'
> - '* hard nofile 165535'
> - '* soft nproc 165535'
> - '* hard nproc 165535'

- /etc/sysctl.conf

```
  - 'net.ipv4.tcp_syncookies = 1'
    - 'kernel.core_uses_pid=1'
    - 'kernel.core_pattern=/tmp/core-%e-%p'
    - 'fs.suid_dumpable=2'
    - 'net.ipv4.tcp_tw_reuse=1'
    - 'net.ipv4.tcp_tw_recycle=0'
```

```
    - 'net.ipv4.tcp_timestamps=1'
    - 'vm.max_map_count=655360'
```

环境变量

- 命令历史记录

> - 修改历史命令输出格式
>   修改/etc/bashrc文件，在末行添加如下行：
>   export HISTTIMEFORMAT="%F %T `who -u am i|awk '{print $1,$7}'|sed -e 's/[()]//g'`"
> - 修改历史命令保存数量
>   修改/etc/profile文件，修改：
>   HISTSIZE=1000
>   为：
>   HISTSIZE=10000
>   HISTFILESIZE=10000

- 登陆超时锁定

> TMOUT=600

安全性

- 禁root用户远程登录
- 密码复杂度

> 大写、小写、数字、特殊符号、至少8位
> pam_tally2.so

- 登陆策略

> 密码错误6次，锁定10分钟

- 关键文件权限

> chmod 644 /etc/passwd
> chmod 400 /etc/shadow
> chmod 644 /etc/group
> chmod 644 /etc/services
> chmod 600 /etc/xinetd.conf
> chmod 600 /etc/security

- 禁用ctrl-alt-del

> rm -rf /etc/systemd/system/ctrl-alt-del.target