**目 录**

[第1章 概述 1](#_Toc345422533)

[1.1 目的 1](#_Toc345422534)

[1.2 适用范围 1](#_Toc345422535)

[1.3 适用版本 1](#_Toc345422536)

[1.4 实施 1](#_Toc345422537)

[1.5 例外条款 1](#_Toc345422538)

[第2章 安装规划 2](#_Toc345422539)

[2.1 操作系统版本 2](#_Toc345422540)

[2.2 主机命名 2](#_Toc345422541)

[2.3 服务器信息搜集 2](#_Toc345422542)

[第3章 安装过程 2](#_Toc345422543)

[3.1 语言的选择 2](#_Toc345422544)

[3.2 文件系统划分 2](#_Toc345422545)

[3.3 网络配置 3](#_Toc345422546)

[3.4 时间配置 3](#_Toc345422547)

[3.4.1 时区配置 3](#_Toc345422548)

[3.4.2 配置NTP 4](#_Toc345422549)

[3.5 软件包定制 4](#_Toc345422550)

[3.5.1 桌面环境 4](#_Toc345422551)

[3.5.2 应用程序 5](#_Toc345422552)

[3.5.3 开发环境 5](#_Toc345422553)

[3.5.4 服务器 5](#_Toc345422554)

[3.5.5 基础系统 5](#_Toc345422555)

[3.5.6 虚拟化 5](#_Toc345422556)

[3.5.7 语言 5](#_Toc345422557)

[3.6 防火墙设置 5](#_Toc345422558)

[3.7 SELinux设置 6](#_Toc345422559)

[第4章 系统配置 6](#_Toc345422560)

[4.1 文字界面启动 6](#_Toc345422561)

[4.2 关闭Root用户远程登陆 6](#_Toc345422562)

[4.3 取消不用的服务 6](#_Toc345422563)

[4.4 备份操作系统关键文件 7](#_Toc345422564)

[第5章 针对ORACLE的系统配置 7](#_Toc345422565)

[5.1 补丁的检查及安装 7](#_Toc345422566)

[第6章 评审与修订 8](#_Toc345422567)

# 概述

## 目的

为了规范安装Linux操作系统，减少系统运行中出现的问题，统一服务器设备的系统安装、基本配置、磁盘划分、基础软件安装、系统安全等操作，同时方便管理与维护；体现公司运维规范、专业化，特制定Linux安装部署规范文档。

本文详细规划了在常见环境中Linux的一些规划、设置；并对安全设置提出了一些要求，同时对磁盘分区格式进行统一制定。

## 适用范围

本配置标准的使用者包括：服务器系统管理员、应用管理员、网络安全管理员。

本配置标准适用的范围包括：安邦保险总部和各省公司信息化部门维护管理的LINUX 服务器系统。

## 适用版本

LINUX系列服务器；

## 实施

本标准的解释权和修改权属于安邦保险集团IT部，在本标准的执行过程中若有任何疑问或建议，应及时反馈。

本标准发布之日起生效。

## 例外条款

欲申请本标准的例外条款，申请人必须准备书面申请文件，说明业务需求和原因，送交金诚财富集团公司IT部进行审批备案。

# 安装规划

## 操作系统版本

操作系统的版本应根据各应用的兼容列表选择操作系统的版本。如果没有特殊要求，则统一安装Linux RedHat AS5 Update3版本。安装前应获取物理机器的CPU架构，根椐CPU位数（32位或64位）选择相应的安装介质。

## 主机命名

《主机名命名规范》

地区简拼-服务器用途简称-T/M/B/F/M/V

地区简拼-工号-T

注：T=台式机

         N=笔记本

         B=刀片机

         F=机架服务器

         M=小型机

         V=虚拟机

如：HZZB-DCHP1-V     \杭州总部DHCP1号虚拟机

         ZTIDC-virtulsrv-F    \转塘IDC..

         GDIDC-CWDB-M    \古荡IDC..

## 服务器信息搜集

* 服务器的内存大小
* 分区的特殊需求
* IP地址的规划，是否使用IPV6
* 软件包的特殊需求
* 防火墙和SELinux的特殊要求

# 安装过程

## 语言的选择

安装语言决定了使用的默认语言包，所以安装语言应根据最终使用的默认语言决定。在没有特殊情况下，使用英文进行安装。

## 文件系统划分

首先划分/boot分区和swap分区，其它所有空间都划分在LVM中。其中/boot分区大小为100M，swap分区的大小根据下表确定：

|  |  |  |  |
| --- | --- | --- | --- |
| 物理内存大小 | 小于4GB | 大于4GB小于8GB | 大于8GB |
| Swap空间值 | 物理内存\*2 | 物理内存\*1.5 | 物理内存\*1 |

其它文件系统在LVM中进行划分，初始大小设置如下：

/ 4G

/tmp 4G

/home 4G

/opt 4G

/usr 4G

/var 4G

以下为应用所需文件系统及目录

/app 此目录用来存放应用程序所需的中间件，大小为10G，请将中间件安装在/app目录下的子目录中，如/app/weblogic或/app/oracle

/applog 此目录用来存放应用程序所需的日志文件，大小为10G，优先放在外部存储上，请将应用日志定义到此目录，将来由应用需求部门进行内容的维护

/appdata 此目录用来存放应用程序所需的文件或数据文件，大小默认20G，优先放在外部存储上，应用需求部门可以申请调整大小，将来由应用需求部门进行内容的维护

*注：禁止将应用所需文件安装在操作系统的/home、/usr、/var等目录下，应用需求部门对目录和空间大小有特殊要求的请在提交的变更中注明。*

## 网络配置

在没有特殊要求的情况下，应关闭IPV6的支持，并且填上规划好的IP地址和网关、DNS信息。系统的IP地址将根据应用需求部门所要求的应用类型由网络组统一分配。如果对系统的网络有特殊要求，例如防火墙限制或多网段同时接入等，请在安装需求中说明。

## 时间配置

### 时区配置

在配置系统时间前，首先请设置时区为东8区。在有些操作系统上东8区有2类，实行夏时制(daylight saving)和不实现夏时制的，请选择不实行夏时制的。操作系统通常处理UTC时间，然后根据时区设置进行换算。

### 配置NTP

测试Linux/Unix系统是否能访问“公司ntp 服务器”：ntpdate –d “ntp server IP”

保证Linux/Unix系统时间差距不超过1000秒：ntpdate –d “ntp server IP”

如果输出的offset超过1000秒，请先手动更新，命令是ntpdate “ntp server IP”。

在Linux环境配置NTP客户端要做3件事情，修改ntp.conf的文件、修改ntpd文件和设定自动启动xntp服务器。

1、修改/etc/ntp.conf

/etc/ntp.conf文件内容如下，注释调所有其他的内容。并且创建1个空文件 /var/lib/ntp/drift。

restrict default ignore

restrict 127.0.0.1

restrict $NTPSVR1 mask 255.255.255.255 nomodify notrap noquery

restrict $NTPSVR2 mask 255.255.255.255 nomodify notrap noquery

server $NTPSVR1

server $NTPSVR2

driftfile /var/lib/ntp/drift

注：此处$NTPSVR1和$NTPSVR2请用真实的ntp服务器地址代替

2、修改/etc/sysconfig/ntpd，添加“-x”参数，文件内容如下：

# Drop root to id 'ntp:ntp' by default.

OPTIONS="-x -u ntp:ntp -p /var/run/ntpd.pid" 

# Set to 'yes' to sync hw clock after successful ntpdate

SYNC\_HWCLOCK=no

# Additional options for ntpdate

NTPDATE\_OPTIONS=""

注：其中“-x”为追加项，主要为了解决时间回溯问题。

3、设定自动启动xntp服务器

命令“chkconfig --list ntpd”检查是否配置和自动启动，如果没有，则运行命令：

“chkconfig ntpd on & service ntpd start”

## 软件包定制

软件包选择的原则应遵循精简服务器内存占用、完全选择开发软件包。

### 桌面环境

为了方便日后有应用需要X图形界面的安装，选择一个GNOME桌面环境即可。

### 应用程序

在没有特殊要求的情况下，只要勾选Editors（编辑器）即可。

### 开发环境

开发环境需要完全安装，把所有开发组件全部选上。特别注意的是在开发工具需要在自定义包中把gcc包全部勾选。

### 服务器

没有特殊需求的情况下，需要勾选FTP服务器、Windows Server服务器，并且去掉打印服务器。

### 基础系统

在此需要把所有的都勾选上。

### 虚拟化

除非特殊需求，否则虚拟化不需要安装

### 语言

在英文语言安装中，应把中文支持安装上。

如果是在中文语言安装环境中，应把英语支持安装上。

## 防火墙设置

因为防火墙会阻挡应用程序中的很多端口，在给应用程序部署时带来不可预测的一些错误发生。所以在没有特别要求的情况下，应关闭防火墙设置。

## SELinux设置

SELinux带来安全性的同时,也对应用程序的部署带来一定的影响，在没有特殊要求的情况下页应该对其关闭。

# 系统配置

系统安全配置要求符合《安邦保险环境安全基线》的要求。

## 用户管理

在使用部门没有特殊要求的情况下，Oracle数据库服务器建立dba组和oracle用户，gid与uid都设置为700。Weblogic应用中间件服务器建立bea组及beaadmin、bea1用户，gid与uid都设置为700。

## 文字界面启动

默认安装完成后，会启动图形界面，这样会占用系统一定的资源，并且系统多使用一个X服务后，会多一个程序崩溃的可能性。

vi /etc/inittab

id:3:initdefault: //修改此行中的数字为3

## 关闭Root用户远程登陆

多数被攻击的服务器都是因为root用户开放了远程登录的权限。所以要求在安装完毕后关闭root用户登录的权限。

vi /etc/ssh/sshd\_config

PermitRootLogin no //修改此行如左

*注意：如果是远程安装，做完此操作后，root用户将不能再登录系统，请先建立临时用户再做此操作。*

## 取消不用的服务

系统默认会启动很多不用的服务，这些服务会占用系统的资源，并且带来安全的隐患。

# setup

如果没有特殊要求，在选项中去掉yum-updatesd、bluetooth、ekrb5-telnet、gssftp、krb5-telnet、vsftpd、sendmail。

## 备份操作系统关键文件

系统安装完成后，要求对操作系统关键配置文件进行备份，避免对这些文件的误操作、误删除。

# cp /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-eth0.bak

# cp /etc/fstab /etc/fstab.bak

# cp /etc/system /etc/system.bak

# cp /etc/rc.d/rc.sysinit /etc/rc.d/rc.sysinit.bak

# 针对ORACLE的系统配置

## 补丁的检查及安装

基于oracle服务器的操作系统安装完成后，应检查oracle依赖的补丁包是否存在。

# rpm -q gcc gcc-c++ glibc make openmotif setarch compat-db compat-gcc compat-gcc-c++ compat-libstdc++ compat-libstdc++-devel

在测试环境中，Linux AS5.4 64位操作系统在安装完成后，缺失如下包：

openmotif is not installed

package compat-db is not installed

package compat-gcc is not installed

package compat-gcc-c++ is not installed

package compat-libstdc++ is not installed

package compat-libstdc++-devel is not installed

openmotif包在安装光盘内就能找到，该包需要依赖libXp.so.6()(64bit)包

安装方法如下：

# mount /dev/cdrom /mnt

# cd /mnt/server

# rpm -ivh libXp-1.0.0-8.1.el5.x86\_64.rpm

warning: libXp-1.0.0-8.1.el5.x86\_64.rpm: Header V3 DSA signature: NOKEY, key ID 37017186

Preparing... ########################################### [100%]

1:libXp ########################################### [100%]

# rpm -ivh openmotif-2.3.1-2.el5.x86\_64.rpm

warning: openmotif-2.3.1-2.el5.x86\_64.rpm: Header V3 DSA signature: NOKEY, key ID 37017186

Preparing... ########################################### [100%]

1:openmotif ########################################### [100%]

# rpm -q openmotif

openmotif-2.3.1-2.el5

compat-db包在光盘里也可以找到，安装方法如下：

# rpm -ivh compat-db-4.2.52-5.1.x86\_64.rpm

warning: compat-db-4.2.52-5.1.x86\_64.rpm: Header V3 DSA signature: NOKEY, key ID 37017186

Preparing... ########################################### [100%]

1:compat-db ########################################### [100%]

# rpm -q compat-db

其他的gcc包可以从服务台领取到，安装方法如下：

# rpm -ivh compat-gcc-7.3-2.96.128.i386.rpm

warning: compat-gcc-7.3-2.96.128.i386.rpm: Header V3 DSA signature: NOKEY, key ID 025e513b

Preparing... ########################################### [100%]

1:compat-gcc ########################################### [100%]

# rpm -e compat-libstdc++-296-2.96-138.i386

# rpm -ivh compat-libstdc++-7.3-2.96.128.i386.rpm

warning: compat-libstdc++-7.3-2.96.128.i386.rpm: Header V3 DSA signature: NOKEY, key ID 025e513b

Preparing... ########################################### [100%]

1:compat-libstdc++ ########################################### [100%]

# rpm -ivh compat-libstdc++-devel-7.3-2.96.128.i386.rpm

warning: compat-libstdc++-devel-7.3-2.96.128.i386.rpm: Header V3 DSA signature: NOKEY, key ID 025e513b

Preparing... ########################################### [100%]

1:compat-libstdc++-devel ########################################### [100%]

# rpm -ivh compat-gcc-c++-7.3-2.96.128.i386.rpm

warning: compat-gcc-c++-7.3-2.96.128.i386.rpm: Header V3 DSA signature: NOKEY, key ID 025e513b

Preparing... ########################################### [100%]

# 评审与修订

本标准由安邦保险IT部定期进行审查，根据审视结果修订标准，并颁发执行。

# 附件1：系统检查列表

|  |  |  |  |
| --- | --- | --- | --- |
| **1. 补丁和安装情况** | |  |  |
|  |  |  |  |
| **编号** | **检查选项** | **风险等级** | **适用**  **类型** |
|
| 1 | 系统是厂商（Redhat）支持的版本 | I |  |
| *使用uname -a命令检查系统的版本 目前，Redhat Linux9以及之前的版本，Redhat均已不再提供支持。* |
| 2 | 系统的内核不存在本地缓冲区溢出漏洞 | I |  |
| *Linux内核2.4.22之前的版本存在多个可以导致恶意用户获得root权限的漏洞。* |
| 3 | 系统已经安装了最新的安全补丁 | I |  |
| *如果版本是Redhat Linux 9以及之前的版本，则此项为不符合。* |
|  |  |  |  |
| **2. xinetd启动的网络服务** | |  |  |
| **操作**：chkconfig --list命令，检查**xinetd based services:**部分的内容，相关的服务是否为**off**状态，或者不存在 | | | |
| **编号** | **检查选项** | **风险等级** | **适用**  **类型** |
|
| 1 | chargen/chargen-udp、daytime/daytime-udp、echo/echo-udp、time/time-udp等小服务已被禁用 | III |  |
| 2 | cups-lpd服务已被禁用 | III |  |
| 3 | finger服务已被禁用 | III |  |
| 4 | rexec服务已被禁用 | III |  |
| 5 | rlogin服务已被禁用 | III |  |
| 6 | rsh服务已被禁用 | III |  |
| 7 | rsync服务已被禁用 | II |  |
| 8 | ntalk服务已被禁用 | III |  |
| 9 | talk服务已被禁用 | III |  |
| 10 | wu-ftpd服务已被禁用 | II |  |
| 11 | tftp服务已被禁用 | III |  |
| 12 | ipop2服务已被禁用 | III |  |
| 13 | ipop3服务已被禁用 | III |  |
| 14 | telnet服务已被禁用 | III |  |
| 15 | xinetd服务已被禁用 | IV |  |
|  |  |  |  |
| **3. 不必要服务** | |  |  |
| **操作**：执行chkconfig --list命令，检查相关的服务是否不存在，或者在3、5两个运行级别中为off状态，例如：portmap 0:off 1:off 2:off **3:off** 4:on **5:off** 6:off | | | |
| **编号** | **检查选项** | **风险等级** | **适用**  **类型** |
|
| 1 | sendmail服务已被禁用 | II |  |
| 2 | xfs服务已被禁用 | IV |  |
| 3 | apmd服务已被禁用 | III |  |
| 4 | canna服务已被禁用 | IV |  |
| 5 | FreeWnn服务已被禁用 | IV |  |
| 6 | gpm服务已被禁用 | III |  |
| 7 | innd服务已被禁用 | III |  |
| 8 | irda服务已被禁用 | IV |  |
| 9 | isdn服务已被禁用 | IV |  |
| 10 | kdcrotate服务已被禁用 | IV |  |
| 11 | lvs服务已被禁用 | IV |  |
| 12 | mars-nwe服务已被禁用 | IV |  |
| 13 | oki4daemon服务已被禁用 | IV |  |
| 9 | rstatd服务已被禁用 | III |  |
| 10 | rusersd服务已被禁用 | III |  |
| 11 | rwalld服务已被禁用 | III |  |
| 12 | rwhod服务已被禁用 | III |  |
| 13 | wine服务已被禁用 | IV |  |
| 10 | smb服务已被禁用 | III |  |
| 11 | nfs服务已被禁用 | III |  |
| 12 | autofs/nfslock服务已被禁用 | III |  |
| 13 | ypbind服务已被禁用 | III |  |
| 10 | ypserv/yppasswdd服务已被禁用 | III |  |
| 11 | portmap服务已被禁用 | III |  |
| 12 | netfs服务已被禁用 | III |  |
| 13 | cups服务已被禁用 | III |  |
| 13 | lpd服务已被禁用 | III |  |
| 13 | snmpd服务已被禁用 | III |  |
| 13 | named服务已被禁用 | III |  |
| 13 | postgresql服务已被禁用 | III |  |
| 13 | mysql服务已被禁用 | III |  |
| 13 | webmin服务已被禁用 | II |  |
| 13 | squid服务已被禁用 | II |  |
| 13 | kudzu服务已被禁用 | IV |  |
| 4 | 系统已禁用X-Window系统 | IV |  |
| *检查/etc/inittab文件是否存在id:5:initdefault* |
|  |  |  |  |
| **4. 文件／目录控制** | |  |  |
|  |  |  |  |
| **编号** | **检查选项** | **风险等级** | **适用**  **类型** |
|
| 1 | 移动介质（软盘、光盘）使用nosuid选项挂载 | IV |  |
| *检查/etc/fstab文件/dev/floppy和/dev/cdrom相关的条目* |
| 2 | /tmp和/var/tmp目录具有粘滞位 | II |  |
| *例如：# ls -al / | grep tmp drwxrwxrwt 7 root 4096 May 11 20:07 tmp/* |
|  |  |  |  |
| **5. 帐户及环境** | |  |  |
|  |  |  |  |
| **编号** | **检查选项** | **风险等级** | **适用**  **类型** |
|
| 1 | 帐户密码的最小长度为8 | IV |  |
| *cat /etc/login.defs | grep PASS\_MIN\_LEN* |
| 2 | root PATH环境变量，不包含当前目录“.” | II |  |
| *echo $PATH* |
|  |  |  |  |
| **6. 系统信任关系** | |  |  |
|  |  |  |  |
| **编号** | **检查选项** | **风险等级** | **适用**  **类型** |
|
| 1. | 系统与其它主机不存在信任关系 | II |  |
| *检查系统中是否存在.rhosts，.netrc，hosts.equiv文件，以及内容是否为空。* |
|  |  |  |  |
| **7. 其它安全配置** | |  |  |
|  |  |  |  |
| **编号** | **检查选项** | **风险等级** | **适用**  **类型** |
|
| 1. | 系统已经加固了TCP/IP协议栈 | IV |  |
| *检查/etc/sysctl.conf是否存在以下内容： net.ipv4.tcp\_max\_syn\_backlog = 4096 net.ipv4.conf.all.rp\_filter = 1 net.ipv4.conf.all.accept\_source\_route = 0 net.ipv4.conf.all.accept\_redirects = 0 net.ipv4.conf.all.secure\_redirects = 0 net.ipv4.conf.default.rp\_filter = 1 net.ipv4.conf.default.accept\_source\_route = 0 net.ipv4.conf.default.accept\_redirects = 0 net.ipv4.conf.default.secure\_redirects = 0* |

**8.标准化安装**

**附件2：Linux操作系统安装报告**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **一、服务器信息** | | | | | |
| 服务器型号 | |  | 序列号 |  | |
| IP地址 | |  | 用途 |  | |
| 机房 | |  | 机柜 |  | |
| 申请人 | |  | 申请日期 |  | |
| **二、系统安装情检查** | | | | | |
| 1 | 操作系统版本（Linux RedHat AS5 Update3 以上版本） | | | |  |
| 2 | 按《主机名命名规范》修改主机名 | | | |  |
| 3 | 配置LVM逻辑卷管理 | | | |  |
| 4 | Boot 分区（100M） | | | |  |
| 5 | /、/opt、/usr、/home、/tmp、/var分区（4G） | | | |  |
| 6 | /app分区（安装应用软件，初始10G） | | | |  |
| 7 | /applog分区（放置应用日志，初始10G） | | | |  |
| 8 | /appdata分区（放置应用数据，初始10G） | | | |  |
| 9 | 双网卡绑定（互备模式）测试 | | | |  |
| 10 | 时钟同步设置（设置“-x”参数） | | | |  |
| 11 | 根据使用要求建立相应用户及组 | | | |  |
| 12 | 取消不用的服务：yum-updatesd、bluetooth、ekrb5-telnet、gssftp、krb5-telnet、vsftpd、sendmail | | | |  |
| **三、其它补充说明** | | | | | |
|  | | | | | |