

**国家电网公司**

**基于立体巡检体系的无人机装备在智能巡检作业中的综合示范应用项目咨询服务**

**安全加固报告**

天津市万贸科技有限公司

**二〇一六年二月**

**目录**

[第一章 加固基本原则及约定 5](#_Toc514229286)

[1.1加固基本原则及约定 5](#_Toc514229287)

[1.2加固内容综述 5](#_Toc514229288)

[第二章Redhat操作系统安全加固 6](#_Toc514229289)

[2.1账号权限加固 6](#_Toc514229290)

[2.2 网络服务加固 11](#_Toc514229291)

[2.3 数据访问控制加固 15](#_Toc514229292)

[2.4 网络访问控制 19](#_Toc514229293)

[2.5 口令策略加固 23](#_Toc514229294)

[2.6 用户鉴别加固 24](#_Toc514229295)

[2.7 审计策略加固 27](#_Toc514229296)

[第三章Postgres安全加固 34](#_Toc514229297)

[3.1 Postgres数据库补丁集安装 34](#_Toc514229298)

[3.2 postgres数据字典的保护 34](#_Toc514229299)

[3.3 加强访问控制 36](#_Toc514229300)

[3.4 监听程序的管理 37](#_Toc514229301)

[3.5 关闭Extproc功能 38](#_Toc514229302)

[3.6 密码文件管理 38](#_Toc514229303)

[3.7 用户账号管理 39](#_Toc514229304)

[3.8 最小权限使用规则 41](#_Toc514229305)

[3.9 postgres用户 42](#_Toc514229306)

[3.10 密码策略 42](#_Toc514229307)

[3.11 数据库操作审计 43](#_Toc514229308)

[第四章 Weblogic安全加固 45](#_Toc514229309)

[4.1 数据访问控制加固 45](#_Toc514229310)

[4.2 服务加固 45](#_Toc514229311)

[4.3 口令策略加固 46](#_Toc514229312)

[4.4 用户鉴别加固 47](#_Toc514229313)

[4.5 审计策略加固 48](#_Toc514229314)

[4.6 系统补丁及文件配置加固 49](#_Toc514229315)

[第五章 性能调优及安全加固建议 53](#_Toc514229316)

[5.1性能调优建议 53](#_Toc514229317)

[5.1.1操作系统调优 53](#_Toc514229318)

[5.1.2中间件调优 53](#_Toc514229319)

[5.1.3数据库调优 54](#_Toc514229320)

[5.2.安全加固建议 55](#_Toc514229321)

[5.2.1操作系统加固 55](#_Toc514229322)

[5.2.2Weblogic加固 56](#_Toc514229323)

[5.2.3postgres加固 57](#_Toc514229324)

# 第一章 加固基本原则及约定

## 1.1加固基本原则及约定

本加固根据《BZ-30-国家电网公司管理信息系统安全基线要求(Q\_GDW 11445-2015)》的加固原则及要求，对其加固方法与内容的细化。并参考了《BZ-13-国家电网公司应用软件系统通用安全要求(Q\_GDW 1597-2015)》。

## 1.2加固内容综述

无人机巡检系统由内网数据库服务器，内网应用服务器和内网图像处理服务器组成，按照相应加固原则和要求分别进行了系统和应用软件的安全加固，加固信息分别为。

1）内网应用服务器IP地址

操作系统RedHat Enterprise Linux Server 7.4，64位；Web应用为tomcat8。

2）内网数据库服务器IP地址：

操作系统RedHat Enterprise Linux Server 7.4 64位；数据库为Postgresql9.5。

3）内网图像处理服务器IP地址：

操作系统RedHat Enterprise Linux Server 7.4 64位。

# 第二章Redhat操作系统安全加固

## 2.1账号权限加固

对操作系统用户、用户组进行权限设置，应用系统用户和系统普通用户权限的定义遵循最小权限原则，删除系统多余用户，避免使用弱口令。

1. 账户安全

建议锁定系统中多余的自建帐号；对在用的账号设置系统口令策略；限制能够su为root的用户；避免shadow中空口令帐号。

1. 修改帐号口令

确保系统帐号口令长度和复杂度满足安全要求，为空口令用户设置密码。

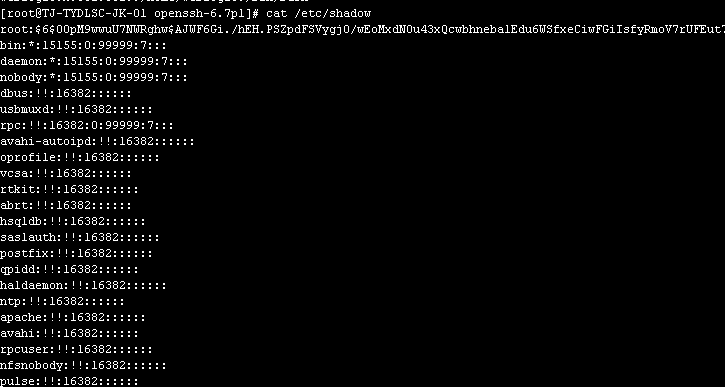
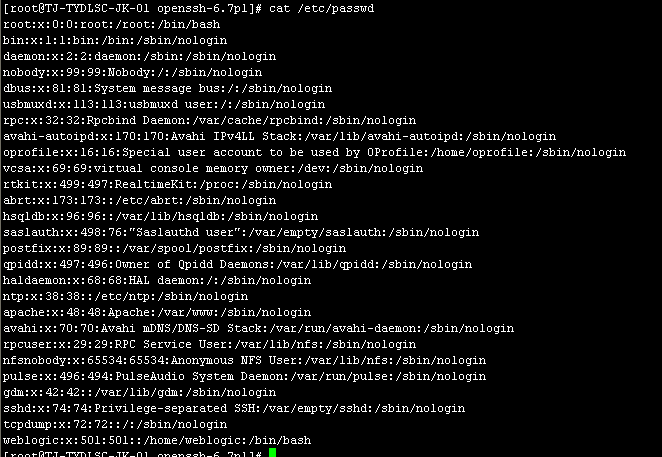
先决条件：查看/etc/passwd文件及/etc/shadow文件，确定是否有空口令用户存在。

实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看/etc/passwd文件及/etc/shadow文件 | #more /etc/passwd | /etc/passwd文件中最后一个字段非”/sbin/nologin”,而/etc/shadow中第二个字段为”!!”的用户为空口令用户 |
| 2 | 记录空口令用户帐号 | 无 |  |
| 3 | 给空口令用户设置密码 | #passwd oracle | 密码复杂度应符合密码策略的要求 |

实施风险：低

实施结果：密码复杂度满足安全要求，未发现空口令用户，加固成功。

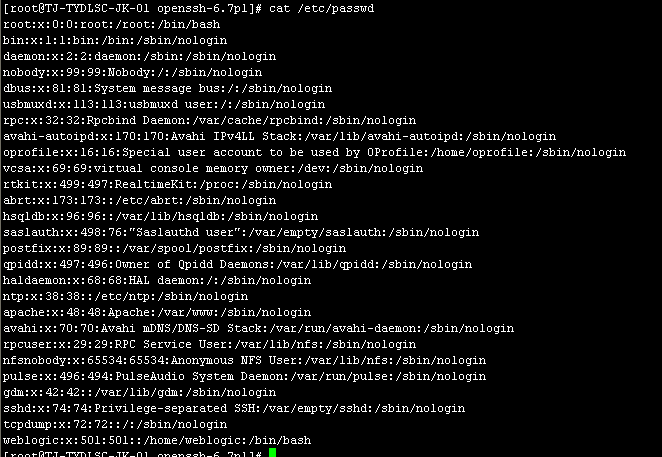


1. 禁用或删除非root的超级用户

* 先决条件：查看/etc/passwd文件，确定是否有非root的超级用户存在。
* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看/etc/passwd文件 | # more /etc/passwd |  |
| 2 | 记录非root的超级用户帐号 | 无 | 非root用户的gid为0 |
| 3 | 禁用或删除非root的超级用户 | 在/etc/passwd中该行前用”#”注释 #userdel username  #usermod –L username | 建议用注释的办法禁用。 |

* 实施风险：低
* 实施结果：未发现非root超级用户，加固成功。



4、禁止系统伪帐户登录

* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看/etc/passwd文件 | # more /etc/passwd |  |
| 2 | 记录伪帐号 | 无 | 登录名不同，uid相同 |
| 3 | 禁用或删除非伪用户 | 在/etc/passwd中该行前用”#”注释 #userdel username  #usermod –L username | 建议用注释的办法禁用。 |

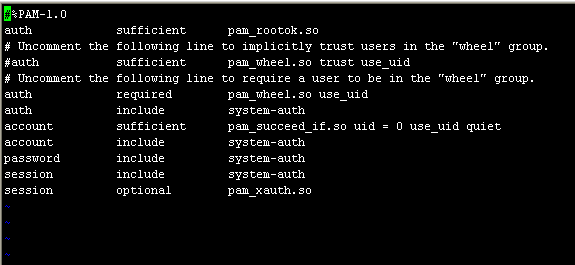
* 实施风险：低
* 实施结果：未发现伪账号，加固成功。

5、限制能够su为root的用户

* 先决条件：确认哪些用户允许su到root。
* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 修改  /etc/pam.d/su配置文件 | #vi /etc/pam.d/su 在  auth required pam\_wheel.so use\_uid  前用”#”注释 | 打开配置文件找到这句话在第六行将其前面的#注释掉 |
| 2 | 修改  /etc/login.defs配置文件 | # echo "SU\_WHEEL\_ONLY yes" >> /etc/login.defs | 在/etc/login.defs文件最后添加"SU\_WHEEL\_ONLY yes" |
| 3 | 将允许su到root的所有用户添加到wheel组中 | # usermod -G wheel <username> | oracle为允许su为root的用户 |

* 实施风险：较高
* 实施结果：将账号oracle设定为唯一能su到root的账号，加固成功。



## 2.2 网络服务加固

关闭系统中不安全的服务，确保操作系统只开启承载业务所必需的网络服务和网络端口。

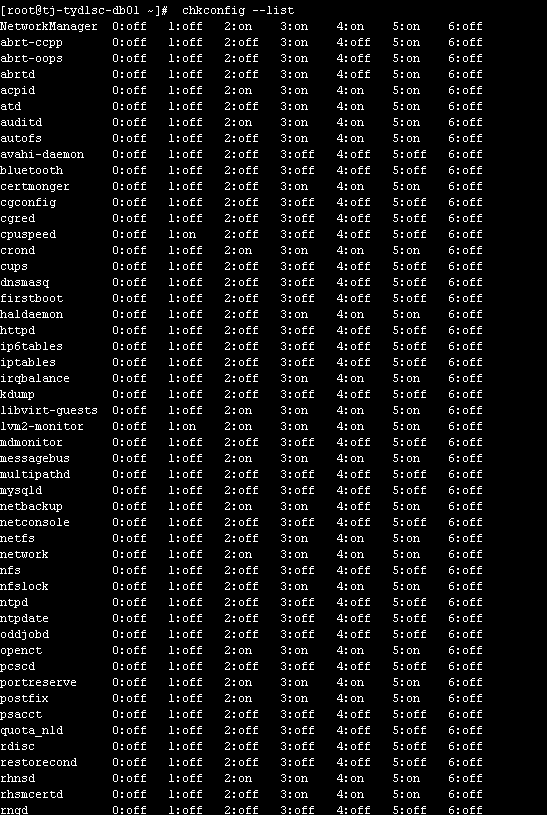
1、在不影响业务系统正常运行情况下，停止或禁用与承载业务无关的服务

* 先决条件：管理员需提供系统实际需要的服务列表，将该列表与当前系统中所启动的服务列表相对比，如果发现与业务应用无关的服务，或不必要的服务和启动项，则关闭掉或禁用。
* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看系统服务启动情况 | # chkconfig --list | 1到6表示linux启动级别，默认启动级别为3 |
| 2 | 关闭不需要的服务 | |  | | --- | | chkconfig avahi-daemon off | | chkconfig bluetooth off | | chkconfig capi off | | chkconfig conman off | | chkconfig cpuspeed off | | chkconfig cups off | | chkconfig dc\_client off | | chkconfig dc\_server off | | chkconfig dnsmasq off | | chkconfig dund off | | chkconfig firstboot off | | chkconfig gpm off | | chkconfig hidd off | | chkconfig hplip off | | chkconfig httpd off | | chkconfig ip6tables off | | chkconfig ipmi off | | chkconfig irda off | | chkconfig isdn off | | chkconfig kdump off | | chkconfig lisa off | | chkconfig mcstrans off | | chkconfig mdmonitor off | | chkconfig mdmpd off | | chkconfig netconsole off | | chkconfig netplugd off | | chkconfig nfs off | | chkconfig nscd off | | chkconfig ntpd off | | chkconfig pand off | | chkconfig pcscd off | | chkconfig psacct off | | chkconfig rdisc off | | chkconfig rpcsvcgssd off | | chkconfig saslauthd off | | chkconfig sendmail off | | chkconfig setroubleshoot off | | chkconfig squid off | | chkconfig tux off | | chkconfig vncserver off | | chkconfig wdaemon off | | chkconfig winbind off | | chkconfig wpa\_supplicant off | | chkconfig ypbind off | | chkconfig yum-updatesd off | | 建议保留  atd crond irqbalance microcode\_ctl network sshd syslog服务，其他服务如果没有特殊要求均可先关闭，有需求时再打开，不指定level时会对所有基本生效 |

实施风险：高

实施结果：关闭了NetworkManager、bluetooth、netfs、cups、ip6tables等没有用到的服务，加固成功。



## 2.3 数据访问控制加固

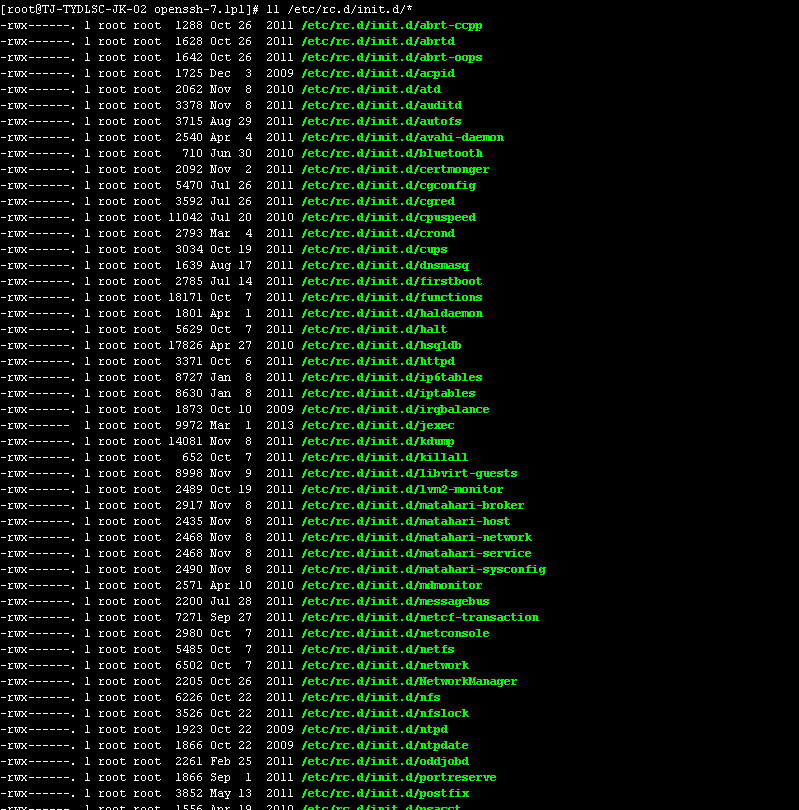
合理设置系统中重要文件的访问权限只授予必要的用户必需的访问权限。

1、配置系统重要文件的访问控制策略，严格限制访问权限（如读、写、执行），避免被普通用户修改和删除

* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看文件访问权限 | # ls -l /etc/passwd  -rw-r--r--. 1 root root 1449 Aug 26 2015 /etc/passwd  # ls -l /etc/shadow  ----------. 1 root root 813 Aug 26 15:33 /etc/shadow  # ls -l /etc/group  -rw-r--r--. 1 root root 764 Aug 26 15:43 /etc/group  # ls -l /etc/gshadow  ----------. 1 root root 627 Aug 26 15:43 /etc/gshadow | ls –l filename |
| 2 | 设置重要文件的权限，不允许任何人修改 | chattr +i /etc/passwd  chattr +i /etc/shadow  chattr +i /etc/group  chattr +i /etc/gshadow | 设置后包括root在内的所有用户均不能修改，所以都无法更改密码也无法新建用户，建议在特殊情况下使用，可以用#chattr -i 命令解除 |
| 3 | 修改重要文件或目录的访问权限 | Chmod -R 700 /etc/rc.d/init.d/\* | /usr/bin、/bin、/sbin目录为可执行文件目录，/etc目录为系统配置目录，包括帐户文件，系统配置，网络配置文件等，这些目录和文件相对重要。确认这些配置文件的权限设置是否安全。 |

* 实施风险：高
* 实施结果：修改了重要文件或目录的访问权限



## 2.4 网络访问控制

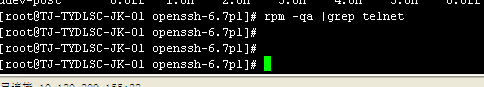
加固远程控制有安全机制保证，限制能够访问本机的用户或IP地址。

1、关闭多余的远程管理方式

* 先决条件：确认多余的远程管理模式。
* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 举例 | 备注 |
| 1 | 关闭telnet服务 | # rpm -qa |grep telnet | 建议关闭telnet服务，使用加密的ssh服务 |
| 2 | 删除telnet服务包 | # rpm -e telnet-server |  |

* 实施风险：高
* 实施结果：未开启telnet服务，加固成功。

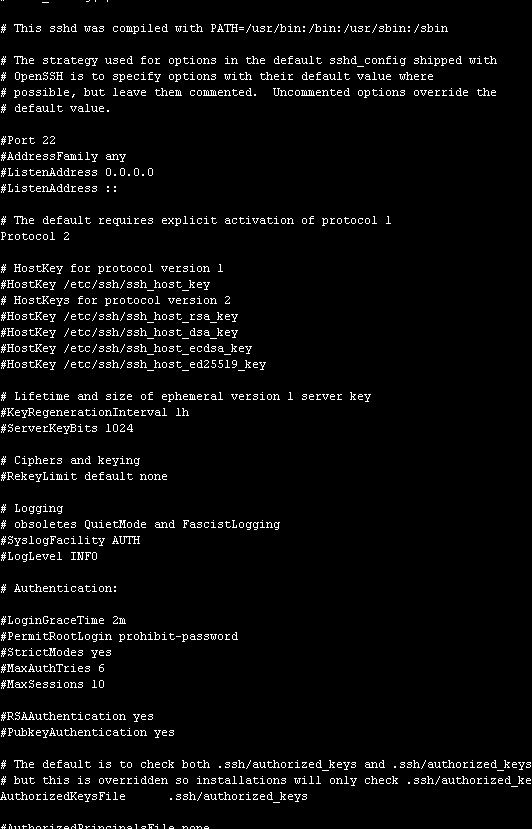
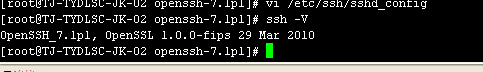


2、使用安全的远程管理方式

* 先决条件：Redhat默认安装时已经安装ssh，如果没有安装需要安装介质。
* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 确认已经安装ssh包 | 升级openssh  [root@TJ-TYDLSC-JK-02 openssh-7.1p1]# ssh -V  OpenSSH\_7.1p1, OpenSSL 1.0.0-fips 29 Mar 2010 | 如果未安装请用安装新版 |
| 2 | 修改相关配置 | vi /etc/ssh/sshd\_config  找到  #Protocol 2,1  将“#”删除，再将行末的“,1”删除；  找到  #PermitEmptyPasswords no  将“#” 删除  找到  #Port 22  将“#” 删除并将22改为50000 | 只允许SSH2方式的连接，　　不允许空密码登录，改变ssh的服务端口为50000（端口号可以根据实际需要修改） |
| 3 |  | #setup | 在Firewall configuration-〉customize-〉  Other ports中添加50000端口 |
| 4 | 重新启动 SSH 服务 | # /etc/rc.d/init.d/sshd restart |  |
| 5 | 进行登录测试 | 用ssh客户端登录服务器查看 | 注意ssh端口改为50000 |

* 实施风险：低
* 实施结果：ssh协议已升级，设置为只允许SSH2方式的连接，不允许空密码登录。加固成功。



## 2.5 口令策略加固

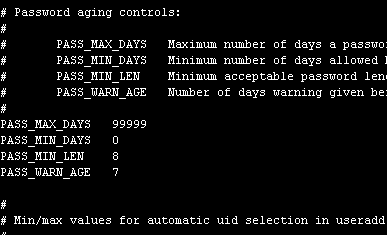
对操作系统设置口令策略，设置口令复杂性要求，为所有用户设置强壮的口令。

1、开启口令复杂性要求，设置口令长度，用户口令长度>8位

* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看密码策略设置 | #more /etc/login.defs|grep PASS |  |
| 2 | 设置口令长度>=8位 | PASS\_MIN\_LEN 8 | 用vi修改/etc/login.defs配置文件相关内容 |
| 3 | 新建用户的密码最长使用天数 | PASS\_MAX\_DAYS 90 | 用vi修改/etc/login.defs配置文件相关内容 |
| 4 | 新建用户的密码最短使用天数 | PASS\_MIN\_DAYS 0 | 用vi修改/etc/login.defs配置文件相关内容 |
| 5 | 新建用户的密码到期提前提醒天数 | PASS\_WARN\_AGE 7 | 用vi修改/etc/login.defs配置文件相关内容 |
| 6 | 重新设置口令 | $passwd | 测试策略修改是否成功 |

* 实施风险：中
* 实施结果：开启了口令复杂性要求，密码长度必须>=8。加固成功。



## 2.6 用户鉴别加固

配置操作系统用户鉴别失败阀值及达到阀值所采取的措施，设置操作系统用户交互登录失败、管理控制台自锁，设置系统超时自动注销功能。

1、设置帐户锁定阀值（登录失败次数）、锁定时间

* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看  /etc/pam.d/system-auth文件有无auth required pam\_tally.so条目的设置 | vim /etc/pam.d/system-auth |  |
| 2 | 设置6次登陆失败后帐户锁定阀值 | 在配置文件中添加一行  auth required pam\_tally.so onerr=fail deny=6 unlock\_time=300 |  |
| 3 | 解除锁定 | # usermod –U username |  |

实施风险：中

实施结果：账户设定为6次登陆失败后自动锁定，锁定时间为300s。加固成功。



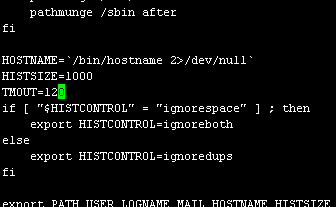
2、修改帐户TMOUT值，设置自动注销时间

* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看/etc/profile文件 | #vi /etc/profile |  |
| 2 | 修改配置 | HISTSIZE= 加入TMOUT=120 | 对于 Bourne, Korn, 和 POSIX shell，修改 /etc/profile文件，添加： export TMOUT=120  对于C shell, 修改 /etc/csh.login文件，添加： set autologout=120 |
| 3 | 登录测试 |  | 连续120s没有输入后会显示  timed out waiting for input: auto-logout，连接丢失。 |

实施风险：中

实施结果：设置客户端120s无操作后，自动注销登录，避免安全隐患。加固成功。



## 2.7 审计策略加固

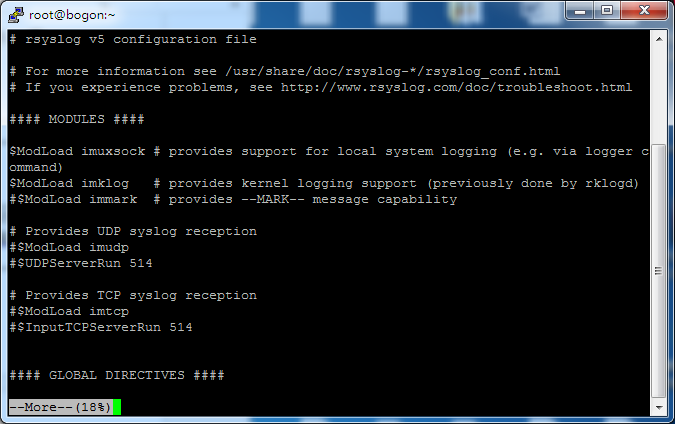
配置操作系统的日志功能，使系统对用户登录、系统管理行为、入侵攻击行为等重要事件进行审计，确保系统在发生安全事件时有日志可供分析。

1、配置系统日志策略配置文件，使系统对鉴权事件、登录事件、重要的系统管理、系统软硬件故障等进行审计。

* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看/var/log/audit/audit.log文件 | # more /var/log/audit/audit.log |  |
| 2 | 查看系统日志服务状态 | #chkconfig –list  chkconfig --add auditd  #ps -aef|grep auditd | 默认该服务是启动的，每次配置修改后需重启该服务 |
| 3 | 启动auditd服务 | # service auditd start |  |
| 4 | 停止auditd服务 | # service auditd stop |  |

* 实施风险：高
* 实施结果：确认开启了日志服务，加固成功。

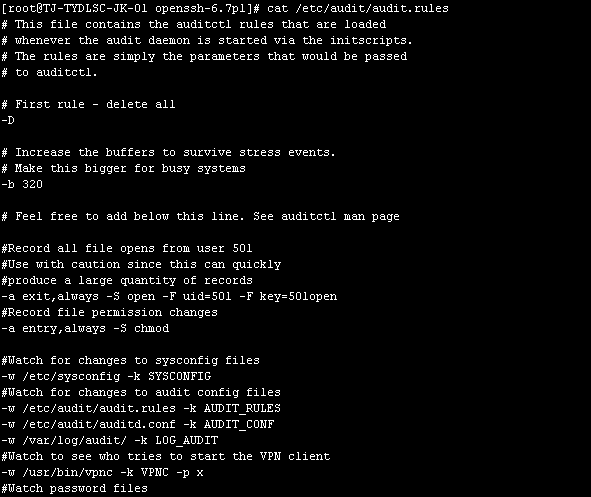
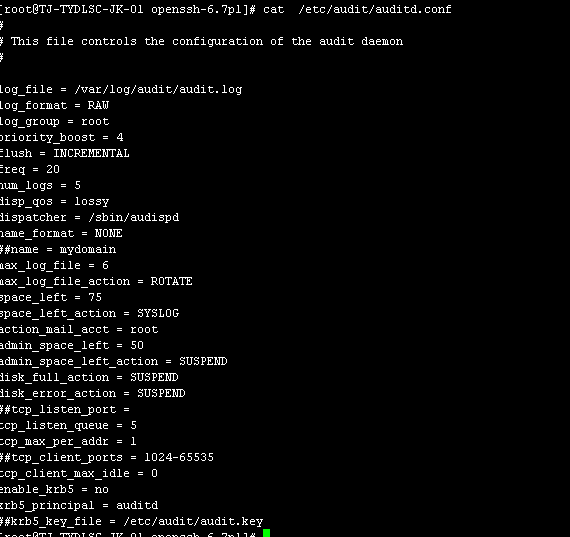


2、开启操作系统审计功能，对审计产生的数据分配合理的存储空间和存储时间

* 实施步骤：

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 工作内容 | 操作内容 | 备注 |
| 1 | 查看audit配置文件并修改 | #more /etc/audit/auditd.conf # This file controls the configuration of the audit daemon #  log\_file = /var/log/audit/audit.log log\_format = RAW priority\_boost = 3 flush = INCREMENTAL freq = 20 num\_logs = 4 dispatcher = /sbin/audispd disp\_qos = lossy max\_log\_file = 5 max\_log\_file\_action = ROTATE space\_left = 75 space\_left\_action = SYSLOG action\_mail\_acct = root admin\_space\_left = 50 admin\_space\_left\_action = SUSPEND disk\_full\_action = SUSPEND disk\_error\_action = SUSPEND |  |
| 2 | 编写审计规则与观察器 | 以下是审计规则：  #Record all file opens from user 501 #Use with caution since this can quickly #produce a large quantity of records -a exit，always -S open -F uid=501 -F key=501open #Record file permission changes -a entry，always -S chmod  以下是观察器：  #Watch for changes to sysconfig files -w /etc/sysconfig -k SYSCONFIG #Watch for changes to audit config files -w /etc/audit/audit.rules -k AUDIT\_RULES -w /etc/audit/auditd.conf -k AUDIT\_CONF -w /var/log/audit/ -k LOG\_AUDIT #Watch to see who tries to start the VPN client -w /usr/bin/vpnc -k VPNC -p x #Watch password files -w /etc/group -k PASSWD -w /etc/passwd -k PASSWD -w /etc/shadow -k PASSWD | 修改配置文件  vi /etc/audit/audit.rules，该配置文件中的每个规则和观察器必须单独在一行中，以#开头的行会被忽略。规则和观察器是auditctl命令行选项，前面没有auditctl命令。它们从上到下阅读文件。如果一个或多个规则或观察器互相冲突，则使用找到的第一个。详见注B：  service auditd restart  chkconfig --add auditd |

* 实施风险：高
* 实施结果：修改了audit配置文件，编写了审计规则和观察器。系统会对文件权限变更、用户密码修改、VPN连接等重要操作进行记录。加固成功。

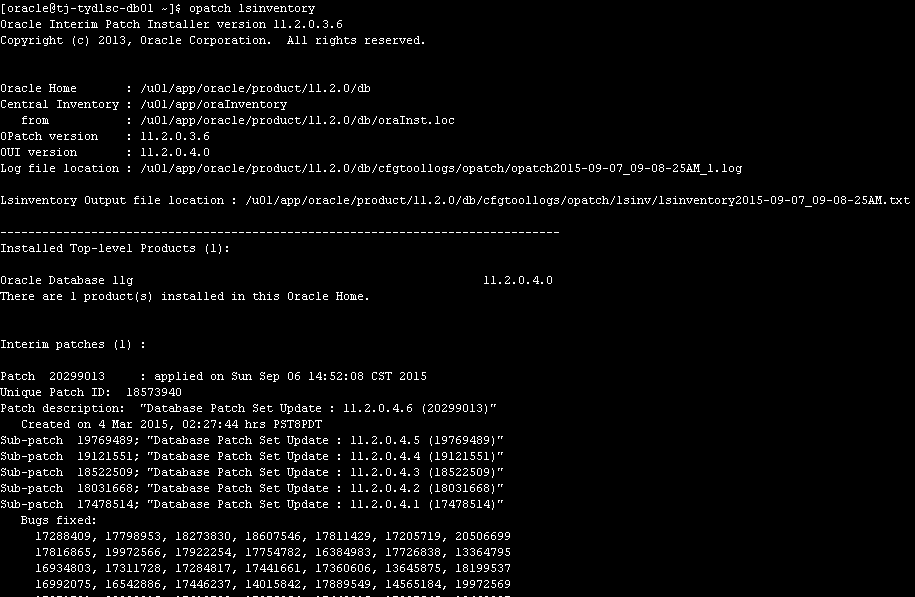


# 第三章Postgres安全加固

## 3.1 Postgres数据库补丁集安装

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | postgres官方补丁集解决BUG和安全问题。 |
| 加固方法 | 运行opatch apply打psu补丁 |

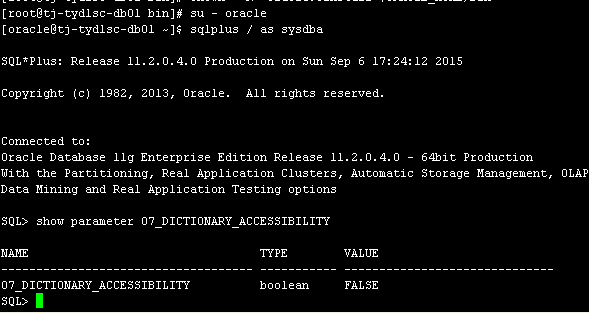
实施结果：经确认补丁安装成功，加固成功。



## 3.2 postgres数据字典的保护

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 设置保护后，可防止其他用户（具有‘ANY’ system privileges）使用数据字典时，具有相同的‘ANY’权限。 |
| 加固方法 | 使用文本方式，打开数据库配置文件init<sid>.ora；更改以下参数O7\_DICTIONARY\_ACCESSIBILITY＝。  1．postgres：缺省值是False  2．postgres：缺省值是True，需要改成False   1. 如果用户必须需要该权限，赋予其权限SELECT ANY DICTIONARY   验证：POSTGRES-#  show parameter O7\_DICTIONARY\_ACCESSIBILITY  NAMETYPEVALUE  ------------------------------------  ---------- ------------------------------  O7\_DICTIONARY\_ACCESSIBILITYbooleanFALSE |

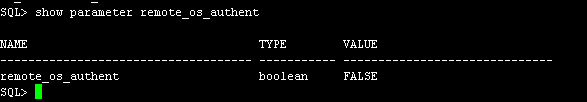
实施结果：经确认O7\_DICTIONARY\_ACCESSIBILITY＝False，加固成功。



## 3.3 加强访问控制

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 设置正确识别客户端用户，并限制操作系统用户数量（包括管理员权限、root权限、普通用户权限等） |
| 加固方法 | 使用文本方式，打开数据库配置文件init<sid>.ora；设置参数REMOTE\_OS\_AUTHENT值为FALSE  在数据库的账户管理中删除不必要的操作系统账号  验证：  POSTGRES-# show parameter remote\_os\_authent |

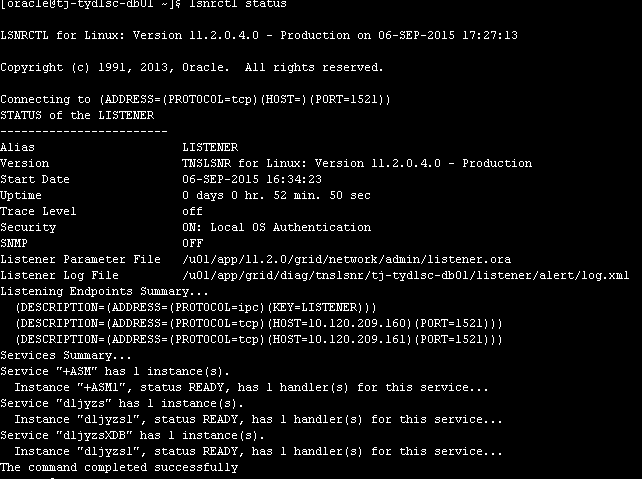
实施结果：禁止采用外部验证的方式登录数据库，加固成功。



## 3.4 监听程序的管理

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 通过设置listener.ora文件中的参数ADMIN\_RESTRICTIONS\_listener\_name来防止远程对监听程序的非授权管理。 |
| 加固方法 | 在listener.ora文件中，设置ADMIN\_RESTRICTIONS\_(listener\_name)=ON。  验证：  lsnrctl  status，查看输出  SecurityON: Local OS Authentication |

实施结果：经确认Security = On，加固成功。



## 3.5 关闭Extproc功能

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 由于extproc存在安全问题允许用户不进行身份认证就可以调用系统函数，因此，如果不需要该功能必须关闭。 |
| 加固方法 | 修改cd /u01/app/postgres删除以下条目：  icache\_extproc  PLSExtproc  Extproc |

实施结果：extproc等已关闭，加固成功。

## 3.6 密码文件管理

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 配置密码文件的使用方式 |
| 加固方法 | 使用文本方式，打开数据库配置文件init<sid>.ora；设置参数REMOTE\_LOGIN\_PASSWORD\_FILE=NONE.  alter  system set remote\_login\_pass[word](http://www.it165.net/edu/ebg/)file=none scope=spfile;  验证：  POSTGRES-# show parameter  remote\_login\_pass[word](http://www.it165.net/edu/ebg/)file |

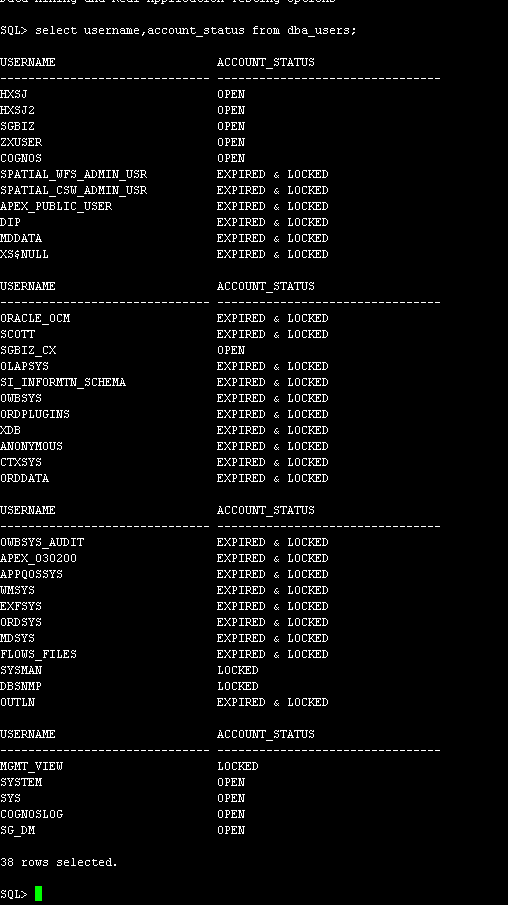
实施结果：密码文件使用方式已修改，加固成功。



## 3.7 用户账号管理

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 为了安全考虑，应用锁定postgres当中不需要的用户；或改变缺省用户的密码。 |
| 加固方法 | 锁定不需要的用户，使用SQL语句：ALTER USER user PASSWORD EXPIRE;  select username,account\_status from dba\_users;  注意锁定emap、mw\_sys、等帐号或修改密码。(如果要使用postgres不能锁定，请修改密码)  DIP、EXFSYS、OUTLN、TSMSYS、WMSYS默认已锁定，请验证。 |

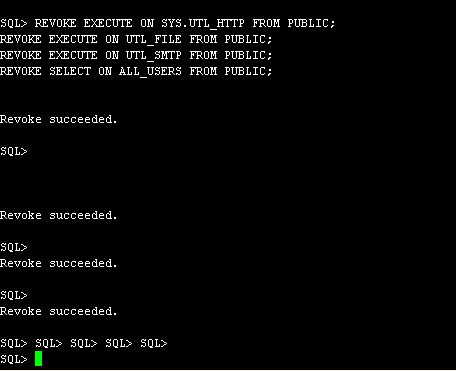
实施结果：锁定了postgres等账户密码，加固成功。



## 3.8 最小权限使用规则

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 应该只提供最小权限给用户  从PUBLIC组中撤回不必要的权限或角色。（如：UTL\_SMTP、UTL\_TCP、UTL\_HTTP、UTL\_FILE、DBMS\_RANDON、DBMS\_SQL、DBMS\_SYS\_SQL、DBMS\_BACKUP\_RESTORE） |
| 加固方法 | 撤销不需要的权限和角色，使用SQL语句  REVOKE EXECUTE ON SYS.UTL\_HTTP FROM PUBLIC;  REVOKE EXECUTE ON UTL\_FILE FROM PUBLIC;  REVOKE EXECUTE ON UTL\_SMTP FROM PUBLIC;  REVOKE SELECT ON ALL\_USERS FROM PUBLIC; |

实施结果：已从PUBLIC组中撤回不必要的权限或角色，加固成功。



## 3.9 postgres用户

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | Postgresql数据库系统安装后，自动创建一个叫做postgres的数据库管理员用户，当该用户连接数据库时，便具有全部系统权限，因而对它的保护尤为重要。 |
| 加固方法 | 更换postgres用户密码；  新建一个DBA用户，作为日常管理使用。 |

实施结果：postgres用户密码已更改，加固成功。

## 3.10 密码策略

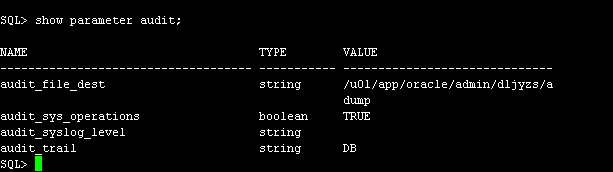
|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 在postgres我们可以通过修改用户概要文件来设置密码的安全策略，可以自定义密码的复杂度。在概要文件中有以下参数是和密码安全有关心的：  FAILED\_LOGIN\_ATTEMPTS:最大错误登录次数  PASSWORD\_GRACE\_TIME:口令失效后锁定时间  PASSWORD\_LIFE\_TIME:口令有效时间  PASSWORD\_LOCK\_TIME:登录超过有效次数锁定时间  PASSWORD\_REUSE\_MAX:口令历史记录保留次数  PASSWORD\_REUSE\_TIME:口令历史记录保留时间  PASSWORD\_VERIFY\_FUNCTION:口令复杂度审计函数 |
| 加固方法 | 在概要文件中设置密码策略，或者执行  POSTGRES-# ALTER PROFILE default  LIMIT FAILED\_LOGIN\_ATTEMPTS 10 |

实施结果：设置密码登录失败次数为10次，加固成功。

## 3.11 数据库操作审计

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | postgres数据库具有对其内部所有发生的活动的审计能力，审计日志一般放在sys.aud$表中，也可以写入操作系统的审计跟踪文件中。可审计的活动有三种类型：登录尝试、数据库活动和对象存取，缺省情况下，数据库不启动审计，要求管理员配置数据库后才能启动审计。 |
| 加固方法 | |  | | --- | |  | | # psql –p 5432 | | POSTGRES-# show parameter audit | | NAME                                 TYPE        VALUE | | ------------------------------------ ----------- ------------------------------ | | audit\_file\_dest                      string      /u01/app/oracle/admin/ORCL/adump | | audit\_sys\_operations                 boolean     FALSE | | audit\_syslog\_level                   string | | audit\_trail                          string      NONE | | POSTGRES-# alter system set audit\_sys\_operations=TRUE scope=spfile;--审计管理用户(以sysdba/sysoper角色登陆) | | POSTGRES-# alter system set audit\_trail=db,extended scope=spfile; | | 重启数据库 | |

实施结果：打开了数据库审计功能，加固成功。

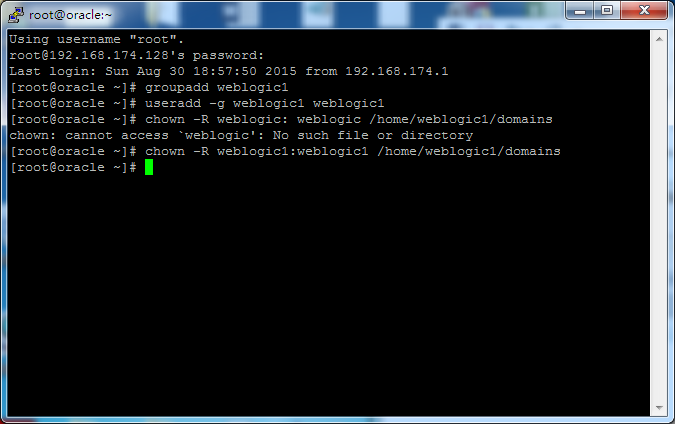


# 第四章 Weblogic安全加固

## 4.1 数据访问控制加固

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 分类设置weblogic中文件写和执行权限，避免未授权的修改和删除 |
| 加固方法 | # groupadd weblogic  # useradd -g weblogic weblogic  # chown -R weblogic: weblogic /home/weblogic/domains |

实施结果：建立weblogic用户和用户组，将域的写权限限定为weblogic用户，加固成功。



## 4.2 服务加固

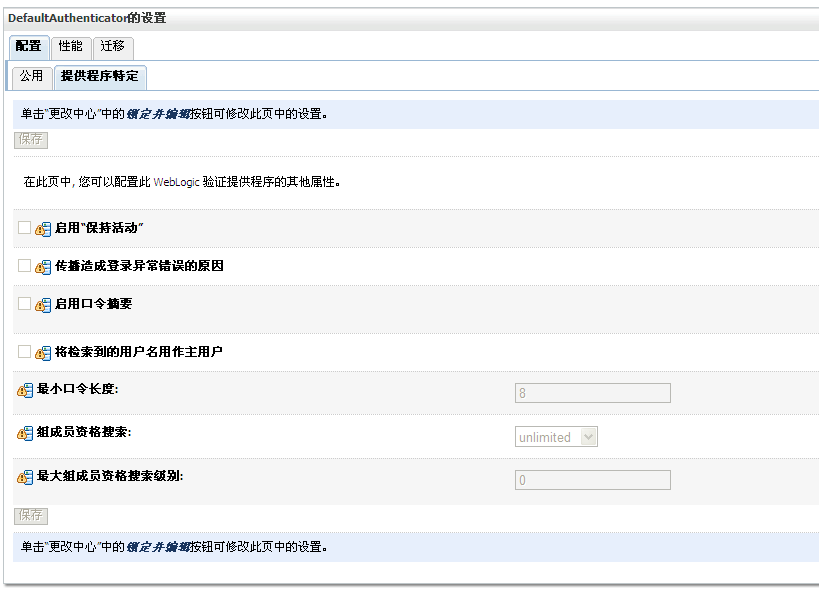
|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 删除系统调试用数据，关闭不需要服务并删除与提供服务无关的应用程序 |
| 加固方法 | 删除weblogic中不必要的组件  删除不必要的examples，samples示例程序 |

实施结果：已确认删除examples，samples示例程序和不必要的组件，加固成功。

## 4.3 口令策略加固

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 对系统设置口令策略，设置口令复杂性要求，为所有用户设置强壮口令 |
| 加固方法 | 1. 设置系统最短口令长度大于8位 2. 禁用Guest用户 3. 为所有用户配置强口令 |

实施结果：已设置密码长度大于8位，未发现Guest用户，加固成功。



## 4.4 用户鉴别加固

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 配置系统用户鉴别失败阀值及达到阀值所采取的措施，设置系统用户交互登录失败、管理控制台自锁，设置系统超时自动注销功能 |
| 加固方法 | 配置weblogic的账户锁定阀值、账户锁定失败登录时间范围、账户锁定持续时间、账户锁定缓存  配置weblogic的console的自动注销功能 |

实施结果：设定账号登录失败次数为5次，锁定时间30分钟，封锁重置持续时间5分钟，console的自动注销功能已设定为6分钟。加固成功。



## 4.5 审计策略加固

|  |  |
| --- | --- |
| **项目** | **说明** |
| 加固目的 | 配置系统日志，设置日志过滤规则，对安全审计范围、日志文件存放位置等进行配置，防止审计数据被非法删除、修改 |
| 加固方法 | 开始审计功能  定制日志的严重度，使weblogic在用户更改域中资源的配置和调用域中资源的管理操作时发出日志消息并生成审核事件 |

实施结果：开启了审计功能，更改了审计类型。设定日志严重度为Info，加固完成。



## 4.6 系统补丁及文件配置加固

1. WebLogic补丁

下载原厂授权的补丁，由原厂工程师指导安装补丁。

1. 账户管理、认证授权；

domain创建之后，会在以下位置创建boot.properties文件（注意：这个位置与weblogic之前的8、9版本有区别）   
weblogic11\user\_projects\domains\example\servers\AdminServer\security   
首先修改boot.properties，如下：

username=weblogic

password=\*\*\*\*\*\*\*\*

这里是明文，但是weblogic启动加载该文件后，会自动通过加密处理。   
 修改完成之后，在控制台中依次进入：安全领域-》myrealm-》用户和组-》weblogic-》口令。输入新的口令即可（需要与boot.properties中配置的一致，如22222222）（如果需要修改账号，需要在用户和组中建立账号，并且赋予管理员权限即可）以上两步完成之后，重启服务即可。

1. 程序目录权限设置；

对启动和环境脚本限制权限为710，确认BEA\_HOME属主为weblogic用户以root 身份执行以下操作：

# chown –R “weblogicuser” $BEA\_HOME

# find $BEA\_HOME/ -name \*.sh |xargs `chmod 710`

1. 日志配置；

默认情况下，weblogic的相关日志的存放位置是：   
weblogic11\user\_projects\domains\example\servers\AdminServer\logs   
这个日志文件夹里面主要包括两种日志   
AdminServer的日志：AdminServer.log（weblogic启动过程中打印出来的日志）   
Http的日志：access.log（http请求的日志）   
web应用的日志存放位置是：   
weblogic11\user\_projects\domains\example\logs   
这里主要就是web应用里面输出的日志文件了   
如果想配置日志，怎么做呢？   
登录domain的console，然后依次选择【环境-》服务器-》AdminServer-》日志】，如下图所示（包括两类日志的配置）：

1. ssl加密；

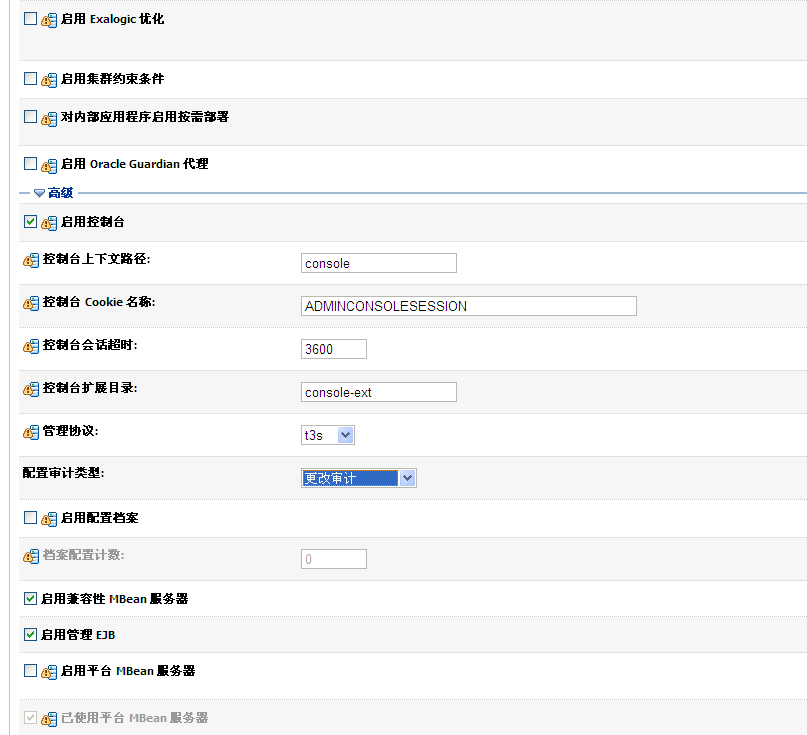
在控制台—服务器中选中server，启用ssl

1. 默认端口更改；

在控制台—服务器中选中server，更改默认端口。

1. 设定默认出错页面。

编辑<Application HOME>/WEB-INF/web.xml ，加入error-page定义



# 第五章 性能调优及安全加固建议

## 5.1性能调优建议

### 5.1.1操作系统调优

1. Linux操作系统安装postgres时需按照官方改出的内核参数建议值修改；
2. 根据每个操作系统安装的应用确任需要启用的后台进程，关闭不是必需的后台守护进程；
3. 建议结合机房网络安全进行操作系统网络优化设置；
4. 系统默认打开的文件数较小，建议调整Linux的最大文件打开数；

### 5.1.2中间件调优

1. 线程池的调整主要视系统的用户访问请求情况，如果短时间内系统并发量大，建议设置线程池；
2. JVM参数优化设置；

经检查当前设置为：

USER\_MEM\_ARGS="-Xms4096m –Xmx4096m -XX:MaxPermSize=512m"

内存没有溢出情况，使用率也不高，当前值设置较大，需注意操作系统内存使用率，如果操作内存使用率太高，此值需从低值开始设置，观察。以免设置太大浪费系统资源。

1. 垃圾回收日志启用设置；

随着业务量不断变化，运维人员启用垃圾回收日志后，平时要多分析日志。运维人员要求有分析日志的能力。

1. Stuck Thread MaxTime的设置；

经检查此选项设置为默认值为600秒，日常运维中注意日志中的提示信息找出慢的业务调优。

1. 连接池大小调整。

经检查当前设置为：

初始容量:1

最大容量:15

最小容量:1

收缩频率:900

建议修改为：

如果数据库压力不大大，建议设置初始容量等于最大容量，都设置为50，以后业务量增长逐步增大。收缩频率修改为0，禁用收缩。

### 5.1.3数据库调优

1. SQL 重用率;

execute to parse% SQL 重用率不高，结合业务监控硬解析的sql语句

1. 表空间大小调整；

system表空间为非自动扩展且使用率超过90%。建议增大表空间大小，平时要注意监控，保证使用率不超过90%。

1. 表的碎片检查；

CO\_CONTRACTBASEINFO表碎片较多，建议对此且做move操作。

1. 分区索引；

结合业务确任是否该建分区索引。

1. 无效对象；

检查无效对象是否程序在用，如不用可以删除。如用检查错误，修改错误后重新编译。

1. 不可用的约束。

检查约束是否表还在用，如不用及时删除。

## 5.2.安全加固建议

### 5.2.1操作系统加固

1. 操作系统补丁

建议联系操作系统原厂商定期根据官方发布的安全补丁，对系统安装补丁。

1. 磁盘分区合理性

根目录（/）、用户目录（/home）、临时目录（/tmp）和/var目录应分开到不同的磁盘分区；  
以上各目录所在分区的磁盘空间大小应充分考虑，避免因某些原因造成分区空间用完而导致系统崩溃；

1. 账户安全

建议锁定系统中多余的自建帐号；对在用的账号设置系统口令策略；限制能够su为root的用户；避免shadow中空口令帐号。

1. 数据访问控制
2. 禁止无用的网络服务
3. 不显示操作系统和版本信息
4. 设置root能登陆的控制台
5. 删除无用的系统用户
6. 禁止使用su命令
7. 禁止 Control-Alt-Delete 重启动机器命令
8. 阻止你的系统响应所有从外部/内部来的ping请求
9. bash\_history设置。

### 5.2.2Weblogic加固

1. WebLogic补丁

安装最新安全相关补丁包，卸载不需要的组件，安全补丁下载需要oracle公司授权，参考WebLogic安全公告

1. 账户管理、认证授权；

建议修改账户密码为复杂密码。

1. 程序目录权限设置；

建议严格控制程序各目录权限。

1. 日志配置；

建议日志单独配置一个目录，注意监控目录大小，定时删除日志，防止日志太大。

1. ssl加密；

建议安全等级高的情况下启用ssl。

1. 默认端口更改；

禁止使用默认端口。

1. 设定默认出错页面。

### 5.2.3postgres加固

1. postgres补丁；

postgres每季度会发布安全补丁集解决产品的bug和安全漏洞，建议及时打补丁

1. 账户安全、角色、密码策略管理；

生产系统要制定严格的账户安全、角色、密码策略制度，保证业务系统的安全。

1. 日志配置；

建议打开审计，在postgres出现安全问题时可以查明原因。

1. 默认端口更改；

默认端口容易被攻击，建议修改默认端口。

1. 登录方式更改；

建议限制具备数据库超级管理员（postgres）权限的用户远程登录

1. 监听安全配置；

建议配置监听密码

1. 连接超时设置。

建议设置连接超时，超时自动退出。