

安全基线整理

信息系统安全防护



2019-3-14

lY

成都局

目录

[一 安全加固 4](#_Toc3795632)

[1.1 信息主机投运前进行安全加固 4](#_Toc3795633)

[1.2 运维人员每日查看主机报警信息，并及时处理 4](#_Toc3795634)

[二．操作系统-身份鉴别 5](#_Toc3795635)

[2.1对登录操作系统的用户进行身份标识和鉴别 5](#_Toc3795636)

[2.2口令设置应符合公司要求 5](#_Toc3795637)

[2.3启用登录失败处理功能 6](#_Toc3795638)

[2.4 当对服务器进行远程管理时，采取必要措施.防止鉴别信息在网络传输过程中被窃听，可采用SSH等安全的远程管理方式。 6](#_Toc3795639)

[2.5操作系统不同用户分配不同的用户名 7](#_Toc3795640)

[2.6 （补充）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。 7](#_Toc3795641)

[三．操作系统-访问控制 8](#_Toc3795642)

[3.1启用访问控制功能 8](#_Toc3795643)

[3.2如果具有数据库系统，实现操作系统和数据库系统特权用户的权限分离 9](#_Toc3795644)

[3.3限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令 9](#_Toc3795645)

[3.4及时删除多余的，过期的账户 10](#_Toc3795646)

[3.5（补充）默认共享 10](#_Toc3795647)

[3.6（补充）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限 11](#_Toc3795648)

[3.7 （补充）应对重要信息资源设置敏感标记 12](#_Toc3795649)

[3.8应依据安全策略严格控制用户对有敏感标记重要信息资源的操作 12](#_Toc3795650)

[四．操作系统-访问安全 13](#_Toc3795651)

[4.1 能够检测对服务器进行入侵的行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间、并在发生入侵事件时提供报警 13](#_Toc3795652)

[4.2 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施 13](#_Toc3795653)

[4.3仅安装需要的应用程序，关闭业务应用正常运行所不需要的服务和端口 13](#_Toc3795654)

[4.4 在确保系统稳定运行的基础上，保持操作系统补丁及时得到更新，在信息内网通过手动方式导入并进行分发 13](#_Toc3795655)

[五．操作系统-资源控制 14](#_Toc3795656)

[5.1 通过设定终端接入方式、网络地址范围等条件限制终端登录 14](#_Toc3795657)

[5.2 根据安全策略设置登录终端的空闲超时断开会话或锁定 14](#_Toc3795658)

[5.3 应限制单个用户对系统资源的最大或最小使用限度。采用磁盘限额等方式限制单个用户对系统资源的最大使用限度； 14](#_Toc3795659)

[5.4 系统磁盘剩余空间足以满足近一段时间的业务需求 14](#_Toc3795660)

[5.5 对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况； 15](#_Toc3795661)

[5.6 能够对系统的服务水平降低到预先规定的最小值进行检测和报警。 15](#_Toc3795662)

[六．操作系统-安全审计 15](#_Toc3795663)

[6.1 审计范围覆盖到服务器上的每个操作系统用户； 15](#_Toc3795664)

[6.2 审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件； 15](#_Toc3795665)

[6.3 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等； 16](#_Toc3795666)

[6.4 应保护审计记录，避免受到未预期的删除、修改或覆盖等。 16](#_Toc3795667)

[6.5 （补充）应保护审计进程，避免受到未预期的中断； 17](#_Toc3795668)

[七．操作系统-剩余信息保护 17](#_Toc3795669)

[7.1 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中； 17](#_Toc3795670)

[7.2 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用； 18](#_Toc3795671)

[八．漏洞扫描 19](#_Toc3795672)

[8.1 使用web应用安全检查系统扫描WEB应用系统，查看是否存在漏洞； 19](#_Toc3795673)

[8.2 使用漏洞扫描设备开展漏洞扫描，查看是否存在漏洞； 19](#_Toc3795674)

[九．数据库-安全加固 19](#_Toc3795675)

[9.1数据库投运前进行安全加固 19](#_Toc3795676)

[9.2运行人员每日查看数据库报警信息，并及时处理 19](#_Toc3795677)

[十．数据库-身份鉴别 20](#_Toc3795678)

[10.1 对登录数据库系统的用户进行身份标识和鉴别 20](#_Toc3795679)

[10.2 口令必须满足复杂度要求 20](#_Toc3795680)

[10.3 启用登录失败处理功能限制同一用户连续失败登录次数 21](#_Toc3795681)

[10.4 采用强度高于用户名+静态口令的认证机制实现用户身份鉴别 22](#_Toc3795682)

[10.5（补充）应为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性 22](#_Toc3795683)

[十一.数据库-访问控制 22](#_Toc3795684)

[11.1 启用访问控制功能，依据安全策略控制用户对资源的使用 22](#_Toc3795685)

[11.2 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限 23](#_Toc3795686)

[11.3 严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令 24](#_Toc3795687)

[11.4 及时删除多余的、过期的账户，避免共享账户的存在 24](#_Toc3795688)

[十二.数据库-安全审计 25](#_Toc3795689)

[12.1 审计范围覆盖到每个数据库系统的用户 25](#_Toc3795690)

[12.2 审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件 25](#_Toc3795691)

[12.3 审计记录包括事件的日期、时间、类型、主机标识、客体标识和结果等 25](#_Toc3795692)

[12.4 能够根据记录数据进行分析，并生成审计报表 26](#_Toc3795693)

[12.5 保护审计进程，避免受到未预期的中断 26](#_Toc3795694)

[12.6 保护审计记录，避免受到未预期的删除、修改或覆盖等。 26](#_Toc3795695)

[十三.数据库-资源控制 27](#_Toc3795696)

[13.1 通过设定终端接入方式、网络地址范围等条件限制终端登录 27](#_Toc3795697)

[13.2 根据安全策略设置登录终端的操作超时退出 27](#_Toc3795698)

[13.3 检查表空间的利用率和扩展方式，表空间的 29](#_Toc3795699)

[十四.数据库-端口安全 29](#_Toc3795700)

[14.1 在不影响应用的情况下，更改数据库默认端口 29](#_Toc3795701)

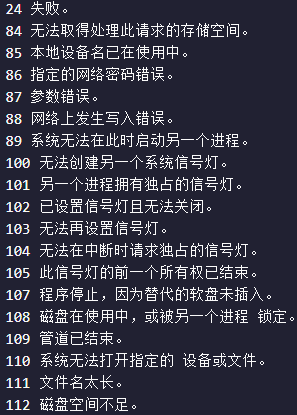
# 一 安全加固

## 信息主机投运前进行安全加固

安全加固根据安全基线规范整理。附上不完全脚本，待完善。

## 运维人员每日查看主机报警信息，并及时处理

查看Windows日志信息，对应用、安全、程序进行监控。对出现的错误信息进行相应处理操作。Windows Error Code具体信息情况见有道云笔记。附上部分代码对应问题：



# 二．操作系统-身份鉴别

## 2.1对登录操作系统的用户进行身份标识和鉴别

访谈管理员，是否为系统用户设置密码，并查看系统账户登录过程中是否使用了密码进行登录验证。

## 2.2口令设置应符合公司要求

检查密码历史记录、密码最长使用期限、最短密码长度、密码复杂性要求等。

检查方法：cmd->secpol.msc

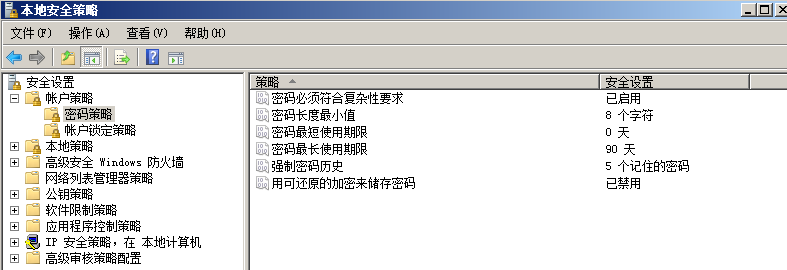
要求：密码必须符合复杂性要求-已启用

密码长度最小值8个字符，为字母，数字和特殊符号混合

每3个月修改一次口令

强制密码历史 5次

可用还原的加密来储存密码：禁用

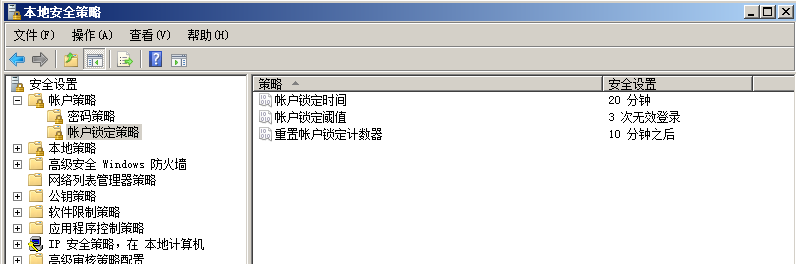


## 2.3启用登录失败处理功能

cmd->secpol.msc查看账户锁定策略：

账户锁定时间：20分钟以上

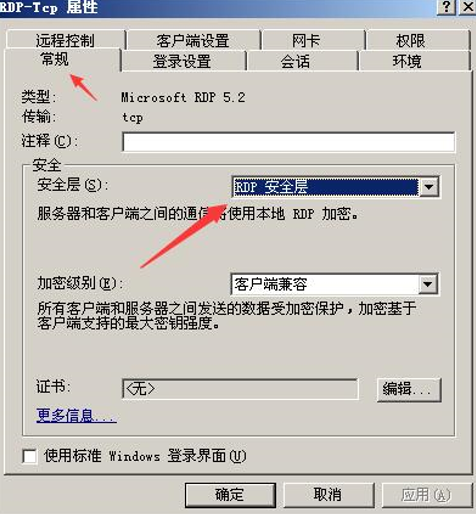
账户锁定阈值：不超过5次



## 2.4 当对服务器进行远程管理时，采取必要措施.防止鉴别信息在网络传输过程中被窃听，可采用SSH等安全的远程管理方式。

确认操作系统必须是Windows Server 2003或者之后的版本；检查终端服务器是否使用了SSL加密，检查安全层参数是否为SSL.

步骤：打开终端服务配置->【连接】→双击右侧【RDP-TCP】，查看【常规】标签，在安全层参数处设置应为【协商】，则会使用TLS1.0的SSL加密方式进行远程连接；

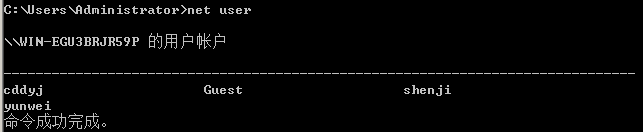
注：安装服务器远程桌面服务后才有终端服务配置选项。

对于MySQL数据库：在数据库中输入show variables；查看“have\_openssl”参数，若为YES则表明使MySQL支持SSL加密协议；

## 2.5操作系统不同用户分配不同的用户名

只需检查Windows系统用户名是否有重复。

检查方法：cmd->net user



## 2.6 （补充）应采用两种或两种以上组合的鉴别技术对管理用户进行身份鉴别。

应询问系统管理员，对系统的登录是否采用双因子身份认证方式进行验证，查看有无CA认证服务器或其他身份认证手段，如存在其他认证方式，尝试进行其他认证方式的身份登录验证，当存在两种或以上身份登录方式为符合；

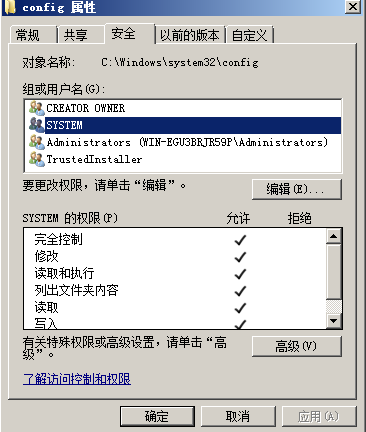
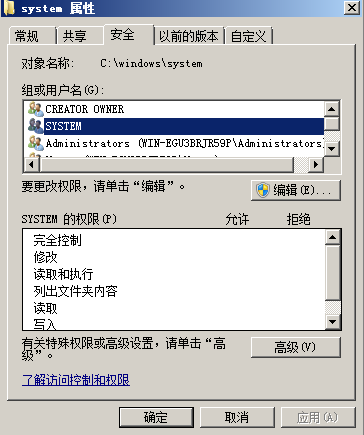
# 三．操作系统-访问控制

## 3.1启用访问控制功能

本项主要涉及两个方面的内容：文件权限、默认共享  
文件权限：

重要目录不能对everyone账户开放。检查%systemdrive%\windows\system、%systemroot%\system32\config两个目录下的各个用户组的权限并记录。

注：个人认为everyone用户不具备所有权限就为正常



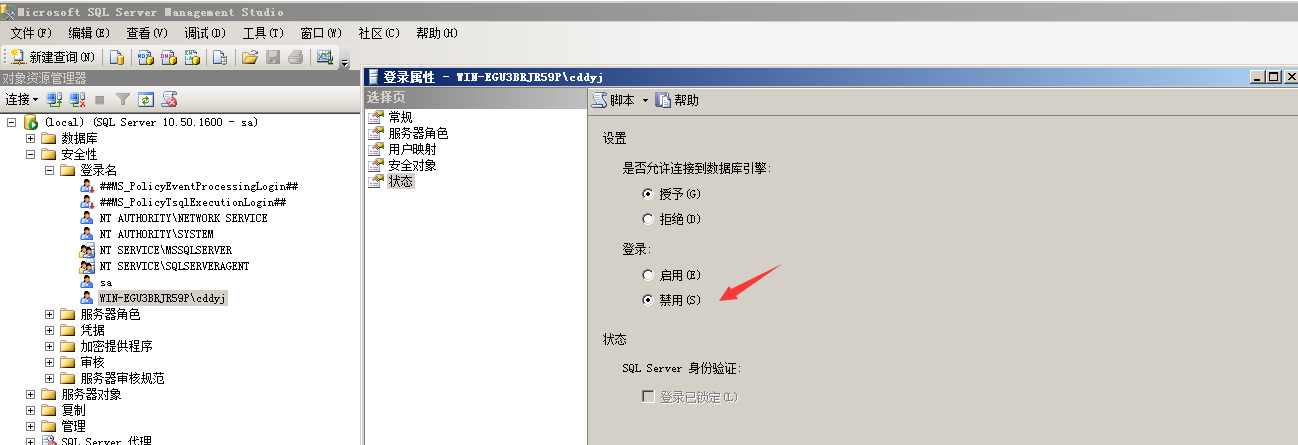
默认共享：

查看注册表  
HLM\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous值是否为0，0表示共享开启，应为1。记录下默认的共享。

## 3.2如果具有数据库系统，实现操作系统和数据库系统特权用户的权限分离

如果主机运行了数据库，询问并记录操作系统管理员和数据库管理员是否为同一人。如果没安装数据库，此项标记为不适用。

打开数据库-安全性-登录名-双击用户名，选择SQL Server身份验证或者禁用账号。将登录方式为windows登陆的全部状态-登陆-禁用（建议超级管理员的windows验证不禁用）。



## 3.3限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令

1.检查默认账户是否重命名；

2.询问是否已经修改默认账户口令；

3.查看是否已经禁用Guest账户；

检查方法：记录未重命名的默认账户，未禁用的默认账户。

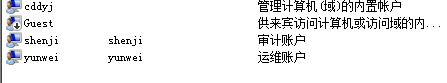
创建如下两个账户:

运维账户：yunwei Cddyj1234!

审计账户：shenji Cddyj1234\*

## 3.4及时删除多余的，过期的账户

保证成都供电公司系统账户为下图4个用户，不存在多余用户。



## 3.5（补充）默认共享

默认共享功能是为了方便网络管理员通过网络对计算机进行远程管理设计的，为了保证系统安全，通常关闭。检查方法：

cmd->net share

netstat -an | find “LISTEN” 查看监听的端口



查看注册表:

HLM\SYSTEM\CurrentControlSet\Control\Lsa\restrictanonymous值是否为0，0表示共享开启，应为1。记录下默认的共享。

## 3.6（补充）应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限

本地策略用户权限分配中查看：

1.“从远端系统强制关机”只指派给Administrators组。

2.“关闭系统”仅指派给Administrators组。

3.“取得文件或其它对象的所有权”仅指派给Administrators。

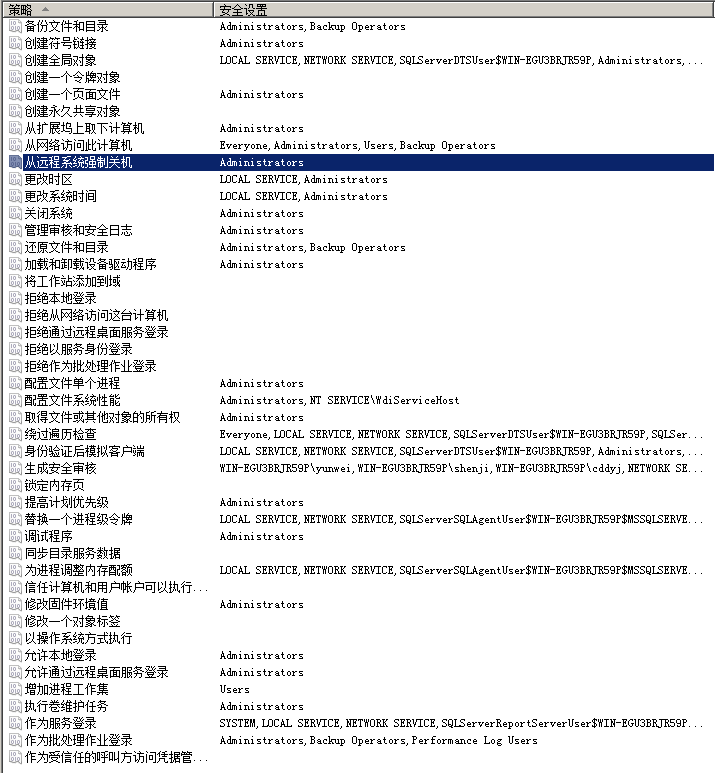
4.“管理审核和安全日志”仅指派给Administrators组。

5.“从本地登录此计算机”指派给指定授权用户。

6.“从网络访问此计算机”指派给Administrators组。

检查方法：cmd->secpol.msc 本地策略->用户权限分配。

说明：所有账户采用最小授权原则（如系统管理员只能对系统进行维护，安全管理员只能进行处理配置和安全设置，安全审计员只能维护审计信息等）；



## 3.7 （补充）应对重要信息资源设置敏感标记

对文件进行安全标记，通常设置权限小于10的用户，没有权利访问。

## 3.8应依据安全策略严格控制用户对有敏感标记重要信息资源的操作

# 四．操作系统-访问安全

## 4.1 能够检测对服务器进行入侵的行为，记录入侵的源IP、攻击的类型、攻击的目的、攻击的时间、并在发生入侵事件时提供报警

针对此条有专门的防火墙（内网行为审计）进行检测。

## 4.2 应能够对重要程序的完整性进行检测，并在检测到完整性受到破坏后具有恢复的措施

对几套重要信息支撑系统拓扑、报表、设备信息、用户信息等功能进行检查，能够正常使用。

## 4.3仅安装需要的应用程序，关闭业务应用正常运行所不需要的服务和端口

Office 2010以下版本具有漏洞，应卸载。其他与业务系统无关软件根据实际情况进行卸载操作。

不需要的服务项有

Alerter、

Computer Browser、

Messenger、

Remote Registry Service、

Routing and Remote、

Access、

Telnet、

Service、

Print Spooler、

Terminal Task Scheduler

不需要的端口 135、139、445等，之前已经进行过端口整改。

## 4.4 在确保系统稳定运行的基础上，保持操作系统补丁及时得到更新，在信息内网通过手动方式导入并进行分发

安装了漏洞补丁服务器，自动分发补丁并进行安装操作。不需要额外的手动下载并进行安装。

# 五．操作系统-资源控制

## 5.1 通过设定终端接入方式、网络地址范围等条件限制终端登录

更改3389端口为13389，查看本地防火墙入站规则和网络防火墙过滤规则是否有做过限制。

## 5.2 根据安全策略设置登录终端的空闲超时断开会话或锁定

限制远程登录空闲断开时间：

本地策略安全选项中查看“Microsoft网络服务器：在挂起会话之前所需的空闲时间”（W2003）是否配置为15分钟。/“Microsoft网络服务器：暂停会话前所需的空闲时间量”（W2008）是否配置为15分钟。

## 5.3 应限制单个用户对系统资源的最大或最小使用限度。采用磁盘限额等方式限制单个用户对系统资源的最大使用限度；

若不限制，一个用户占用的资源过多，很容易造成DoS攻击。磁盘限额是否限制单个用户使用的磁盘大小；远程桌面用户数量同时在线数量是否有限制。

## 5.4 系统磁盘剩余空间足以满足近一段时间的业务需求

查看磁盘容量，主要是C盘容量是否满足最近一段时间业务需要。

## 5.5 对重要服务器进行监视，包括监视服务器的CPU、硬盘、内存、网络等资源的使用情况；

打开“管理工具—性能监视器”查看CPU、内存等使用情况。

## 5.6 能够对系统的服务水平降低到预先规定的最小值进行检测和报警。

问系统管理员如何监控系统服务水平，若有第三方监控程序，询问并查看是否有相关功能。拥有启明星辰日志审计服务器，当主机低于最小值时发生告警。

# 六．操作系统-安全审计

## 6.1 审计范围覆盖到服务器上的每个操作系统用户；

查看系统是否开启了安全审计功能，询问是否有第三方审计工具或者系统，并且记录运行状态。

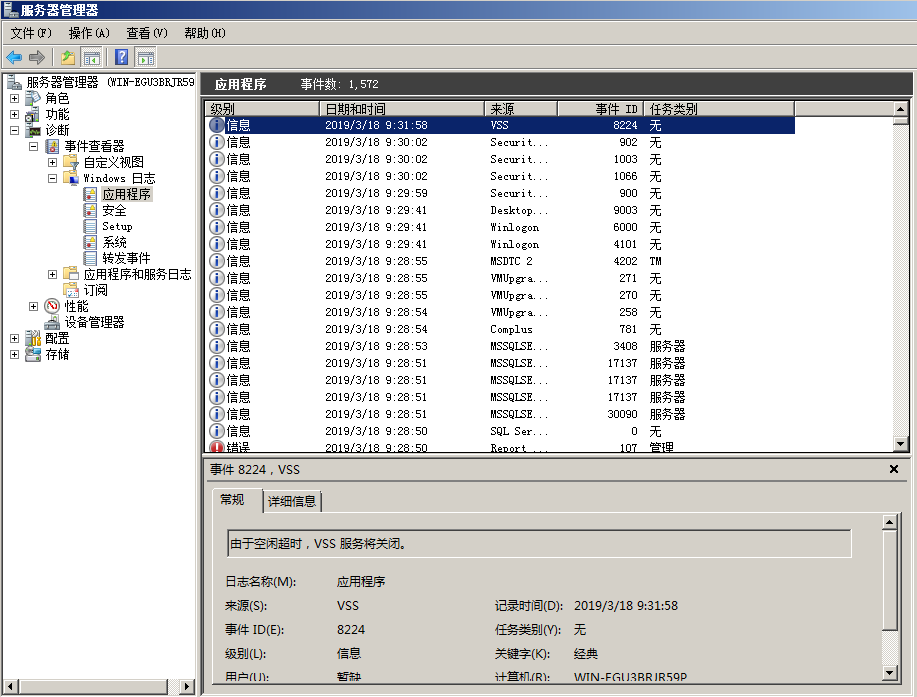
## 6.2 审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

补充6.1，将审计功能的各项成功失败事件都进行记录。



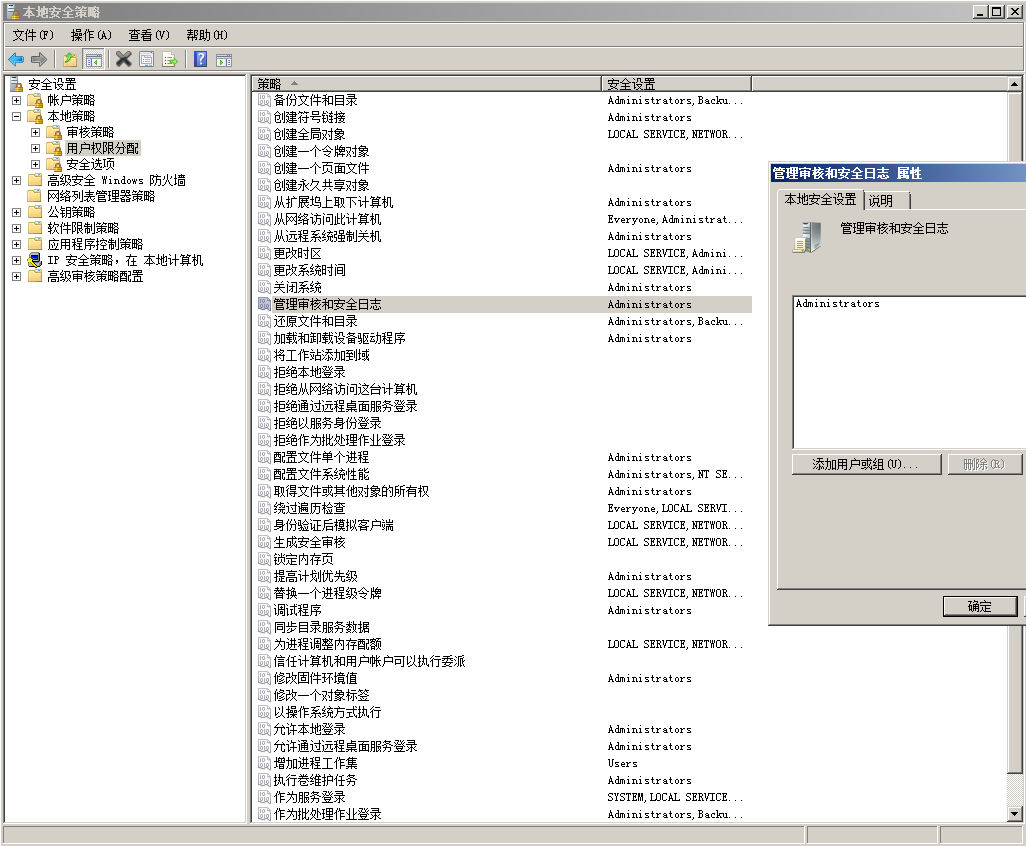
## 6.3 审计记录应包括事件的日期、时间、类型、主体标识、客体标识和结果等；

compmgmt.msc，查看日志文件是否满足要求。



## 6.4 应保护审计记录，避免受到未预期的删除、修改或覆盖等。

访谈审计记录的存储、备份和保护措施，配置有启明星辰日志审计系统。并在策略的安全选项中将对日志的操作仅授权给超级管理员用户。



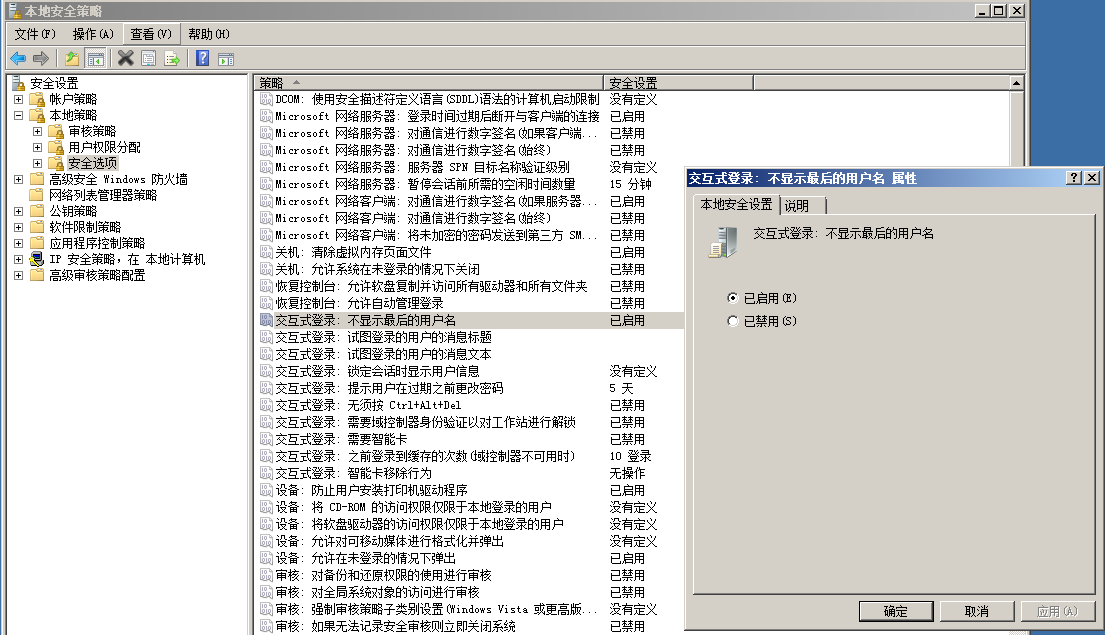
## 6.5 （补充）应保护审计进程，避免受到未预期的中断；

检查审计进程的访问权限是否设置的合理

# 七．操作系统-剩余信息保护

## 7.1 应保证操作系统和数据库系统用户的鉴别信息所在的存储空间，被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

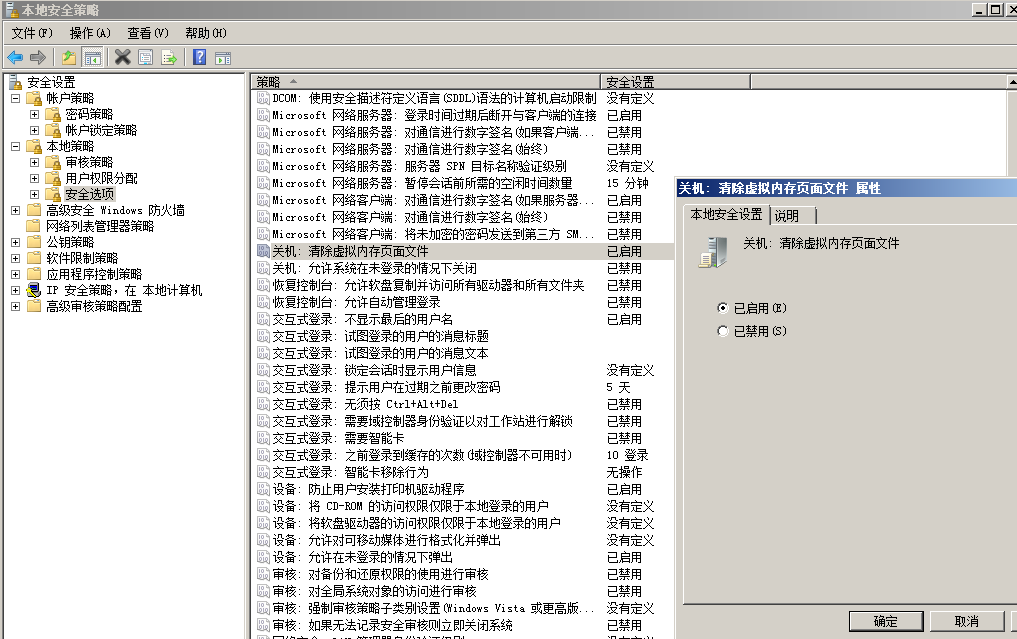
本地策略的安全选项中查看是否启用“不显示上次登录用户名”。



## 7.2 应确保系统内的文件、目录和数据库记录等资源所在的存储空间，被释放或重新分配给其他用；

在密码策略中禁用“用可还原的加密来存储密码”。

“关机：清除虚拟内存页面文件”配置为“已启用”。



# 八．漏洞扫描

## 8.1 使用web应用安全检查系统扫描WEB应用系统，查看是否存在漏洞；

内网使用了专有的漏扫服务器，进行扫描。此条不做。

## 8.2 使用漏洞扫描设备开展漏洞扫描，查看是否存在漏洞；

内网使用了专有的漏扫服务器，进行扫描。此条不做。

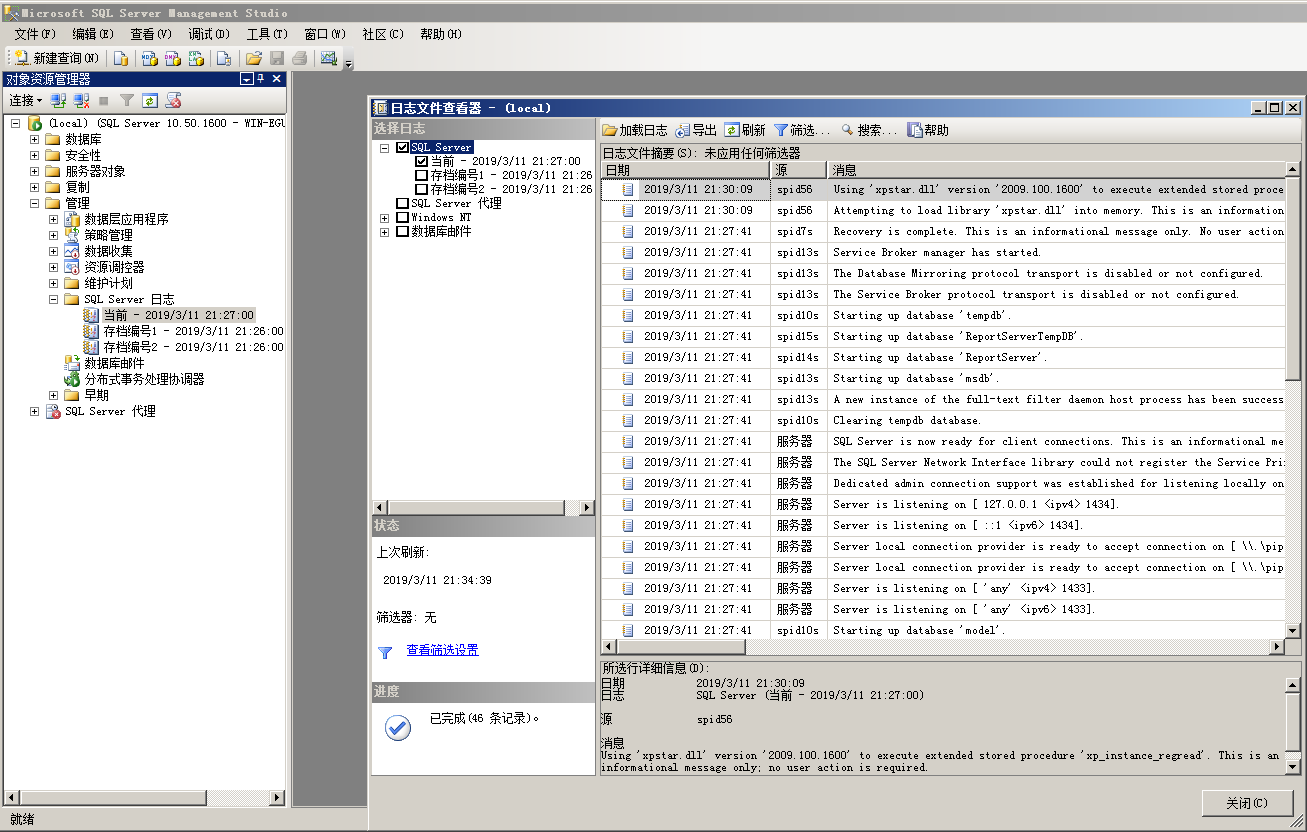
# 九．数据库-安全加固

## 9.1数据库投运前进行安全加固

## 9.2运行人员每日查看数据库报警信息，并及时处理

查看有无异常告警信息，如果有，则解决部分。

对于SQL Server 2008 R2，告警界面如下：



# 十．数据库-身份鉴别

## 10.1 对登录数据库系统的用户进行身份标识和鉴别

对于SQL Server 数据库，

登录数据库时需要输入用户名和密码，则代表进行身份标识

对于MySQL数据库

* 查看MySQL授权主机有那些，是否采用强口令登陆

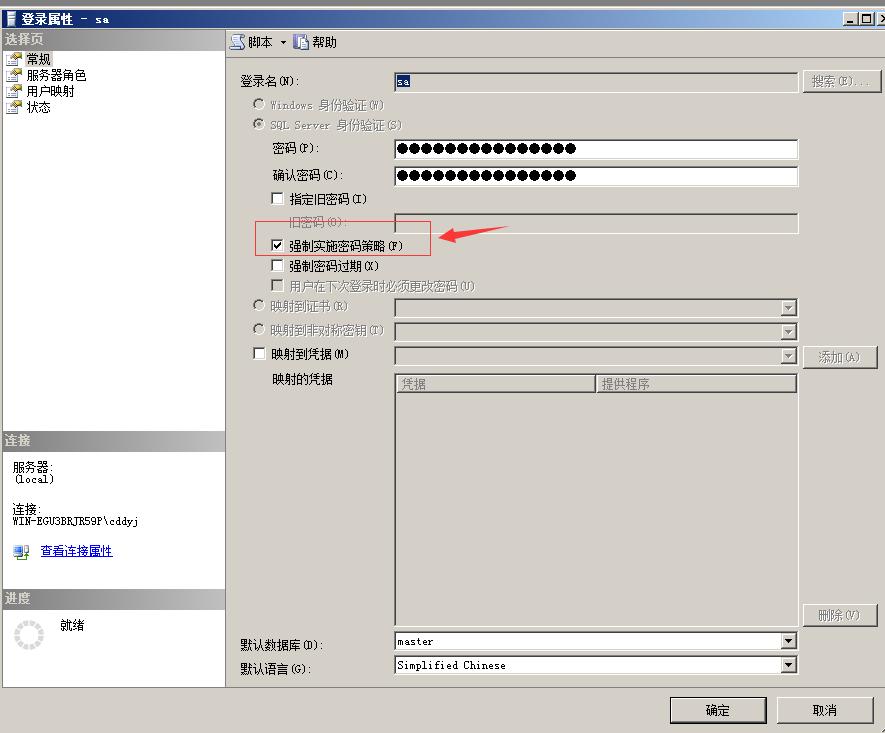
mysql -u root （验证root是否需要口令才能登录）

mysql -uroot@localhost （验证root在本地登录是否需要口令）

* 查看是否存在空口令用户

## 10.2 口令必须满足复杂度要求

对于SQL Server2008数据库，勾选强制密码策略



对于MySQL数据库

mysql本身无法设置密码策略，只能通过第三方软件或公司密码策略制度进行设置并执行。询问管理员是否采用第三方软件或有公司密码策略制度。

## 10.3 启用登录失败处理功能限制同一用户连续失败登录次数

对于SQL Server 数据库

勾选强制密码策略，勾选后默认为和Windows使用一样的密码策略



对于MySQL数据库

需要安装插件实现（**CONNECTION\_CONTROL和CONNECTION\_CONTROL\_FAILED\_LOGIN\_ATTEMPTS**）

## 10.4 采用强度高于用户名+静态口令的认证机制实现用户身份鉴别

此条实现过于复杂，需要动态更改密码。会影响业务系统正常使用，故此条不进行设置。

## 10.5（补充）应为数据库系统的不同用户分配不同的用户名，确保用户名具有唯一性

对于SQL Server 2008数据库：安全性-登录名查看

对于MySQL数据库：mysql>use mysql

# 十一.数据库-访问控制

## 11.1 启用访问控制功能，依据安全策略控制用户对资源的使用

一旦连接到了服务器，一个用户可以使用两种类型的请求:

管理请求(shutdown,reload等)数据库相关的请求(insert，delete，等)。先查看USER表中用户的权限，在查看DB或者HOST表中的权限，以此为对照判断数据库是否进行了访问控制；



Public 公共角色

Sysadmin 用户角色

## 11.2 应根据管理用户的角色分配权限，实现管理用户的权限分离，仅授予管理用户所需的最小权限

对于SQL Server 2008数据库：安全性-登录名查看，有不同用户名对应不同功能

对于MySQL数据库：

登录使用root登录mysql数据库mysql-u root -> 查看数据库show databases； ->选择库 use mysql；-> 查看库中的表 show tables; -> 查看某用户权限show grant for root@localhost \G; 或者select\* from user；

## 11.3 严格限制默认账户的访问权限，重命名系统默认账户，修改这些账户的默认口令

根据需要进行更改

对于SQL Server数据库：



## 11.4 及时删除多余的、过期的账户，避免共享账户的存在

对于SQL Server 2008数据库：安全性-登录名查看

1）show databases;查看是否有测试数据库；

2）查询当前使用的数据库：select database()；

3）查询当前用户：select user()；

4）查看所有用户：SELECT DISTINCTCONCAT('User: ''',user,'''@''',host,''';') AS query FROM mysql.user；

# 十二.数据库-安全审计

## 12.1 审计范围覆盖到每个数据库系统的用户

mysql数据库默认没有安装审计插件，需要修改源代码或者下载审计插件：mysql-[audit](https://cloud.tencent.com/developer/information/audit)。如果安装完成后audit.so和[audit.cn](http://audit.cn/" \t "_blank)f文件中设置参数。

或者开启General\_log，查看日志文件即可；

## 12.2 审计内容包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件

查看日志文件包括重要用户行为、系统资源的异常使用和重要系统命令的使用等系统内重要的安全相关事件；

## 12.3 审计记录包括事件的日期、时间、类型、主机标识、客体标识和结果等

审计内容包括了重要的用户行为，系统资源的异常使用，和重要系统命令的使用等系统内重要的安全相关事件；

## 12.4 能够根据记录数据进行分析，并生成审计报表

询问数据库管理员是否定期对审计数据生成分析报表，或者第三方数据库审计系统是否提供自动生成审核事件的自动生成报表的功能，可查看生成的报表记录。可生成报表时此项满足；

## 12.5 保护审计进程，避免受到未预期的中断

1)以非授权用户登录数据库系统，试图改变审计配置选项，查看是否成功；

2)询问管理员，是否有其他对审核日志文件的保护方式，并在条件允许的情况下尝试进行验证；

3)查看是否定期对日志文件进行备份和转移；

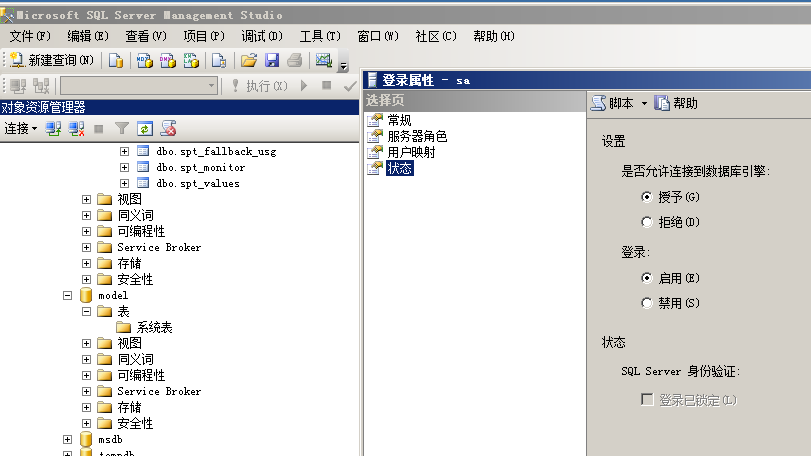
## 12.6 保护审计记录，避免受到未预期的删除、修改或覆盖等。

以普通用户进入数据库系统，查看能否对日志进行非授权操作，询问第三方软件是如何保护数据不被篡改的；

# 十三.数据库-资源控制

## 13.1 通过设定终端接入方式、网络地址范围等条件限制终端登录

SQL Server 状态中设置



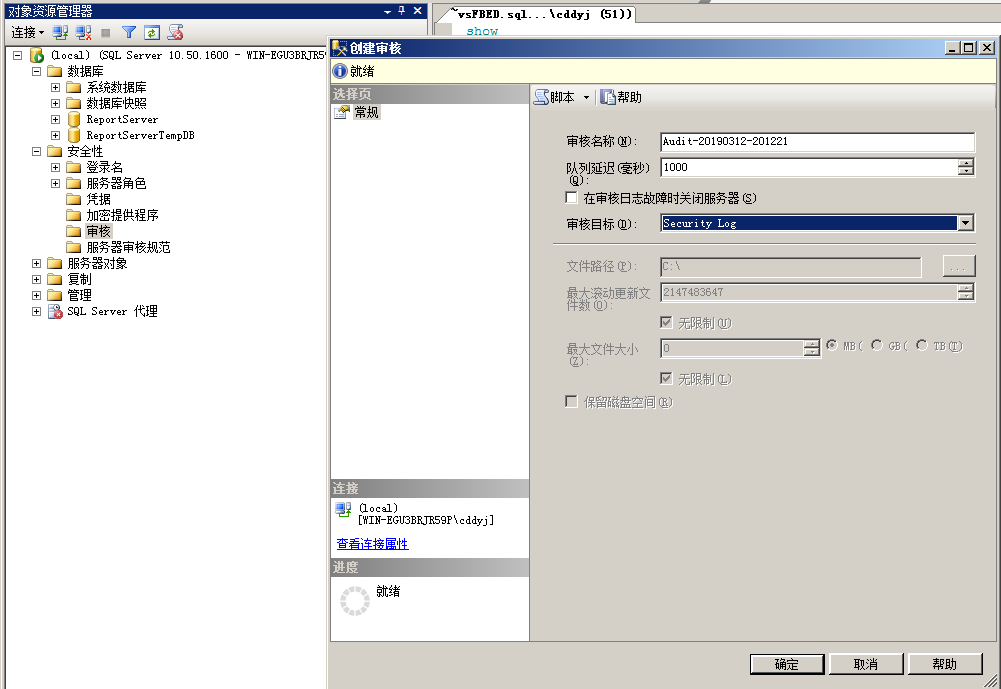
MySQL

1）限制方式 ：grantall on \*.\* to '用户名'@'IP地址'identified by '远程登录密码'

2）无限制方式：grant all on \*.\* to'%'@'localhost' identified by 'password'

## 13.2 根据安全策略设置登录终端的操作超时退出

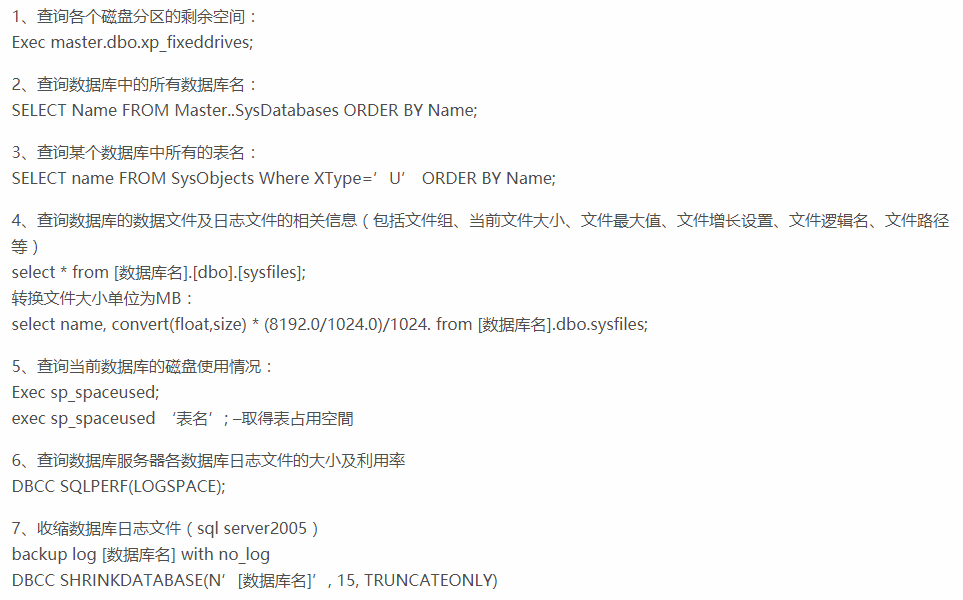
创建审核策略，记录运行日志



在数据块中show variables；或者查看grep -v "^#"/etc/[my.cn](https://cloud.tencent.com/developer/news/my.cn" \t "_blank)f

查看wait\_timeout连接的等待时间默认为28800秒（8小时）

## 13.3 检查表空间的利用率和扩展方式，表空间的



# 十四.数据库-端口安全

## 14.1 在不影响应用的情况下，更改数据库默认端口

默认是将1433端口更改为11433端口。但更改多数会影响业务，故多数不予以更改。

对于SQL Server数据库。

打开SQL Server配置管理器，进入SQL Server网络配置选项，将图示都改为11433.

