# sql-server安全基线检查

## 删除不必要的账号

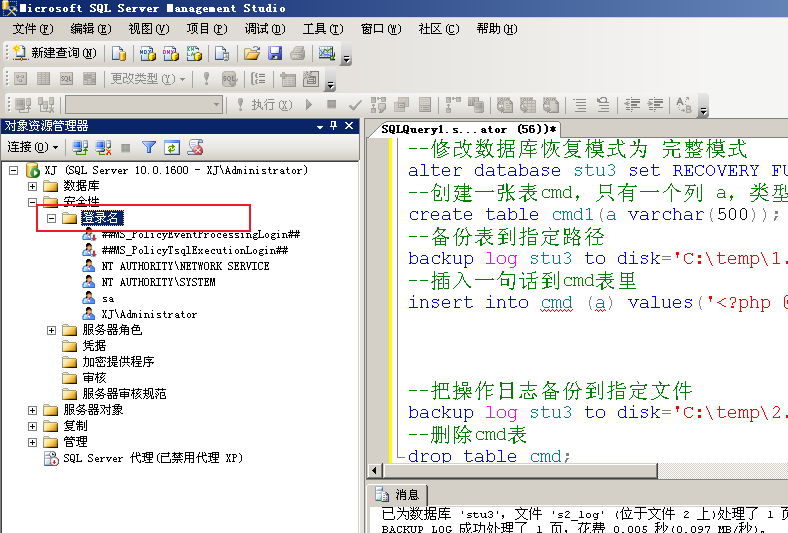
* 安全基线项目名称∶数据库管理系统SQLServer用户安全基线要求项
* 安全基线项说明∶应删除与数据库运行、维护等工作无关的帐号。
* 检测操作步骤∶

SQL SERVER企业管理器->安全性->登陆中删除无关帐号;

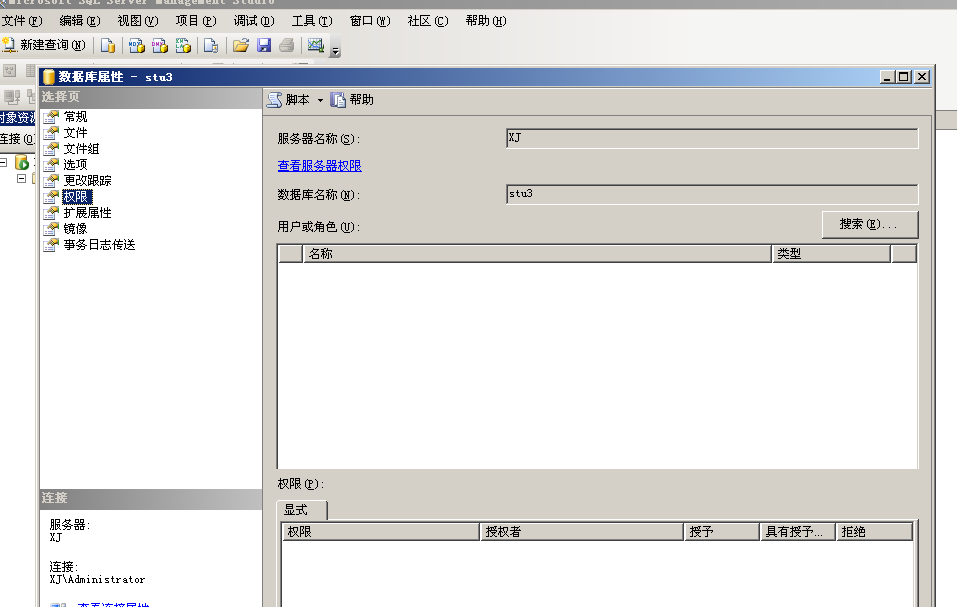
SQL SERVER企业管理器->数据库->对应数据库->用户中删除无关帐号;

■ 基线符合性判定依据∶首先删除不需要的用户，已删除数据库不能登陆使用在MS SQL SERVER查询分析器的登陆界面中使用已删除帐号登陆

SQL SERVER企业管理器->安全性->登陆中删除无关帐号;



SQL SERVER企业管理器->数据库->对应数据库->用户中删除无关帐号;



## 用户口令安全

■安全基线项目名称∶数据库管理系统SQLServer用户口令安全基线要求项

■安全基线项说明∶对用户的属性进行安全检查，包括空密码、密码更新时间等。修改

目前所有帐号的口令，确认为强口令。特别是sa 帐号，口令长度至少8位，并包括数字、小写字母、大写字母和特殊符号四类中至少两类。且5次以内不得设置相同的口令。密码应至少每90天进行更换。

■ 检测操作步骤∶

1. 检查passWord字段是否为null。
2. 参考配置操作查看用户状态

运行查询分析器，执行

select \* from sysusers

*select name, password from sys.syslogins where password is null order by name #查看口令为空的用户*

■基线符合性判定依据∶用户登录账号的password字段不为null。

## 3、根据用户分配帐号避免帐号共享

■ 安全基线项目名称∶数据库管理系统SQLServer共享帐号安全基线要求项

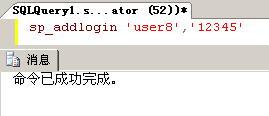
■安全基线项说明∶应按照用户分配帐号，避免不同用户间共享帐号。

■检测操作步骤∶

1.参考配置操作

sp\_addlogin 'user\_name\_1','password1'

sp\_addlogin 'user\_name\_2','password2'



或在企业管理器中直接添加远程登陆用户

建立角色，并给角色授权，把角色赋给不同的用户或修改用户属性中的角色和权限

2.检测方法∶

在查询分析器中用user\_name\_1/password1连接数据库成功

3.补充操作说明

user\_name\_1和user\_name\_2 是两个不同的帐号名称，可根据不同用户，取不同的名称;

■ 基线符合性判定依据∶不同名称的用户可以连接数据库

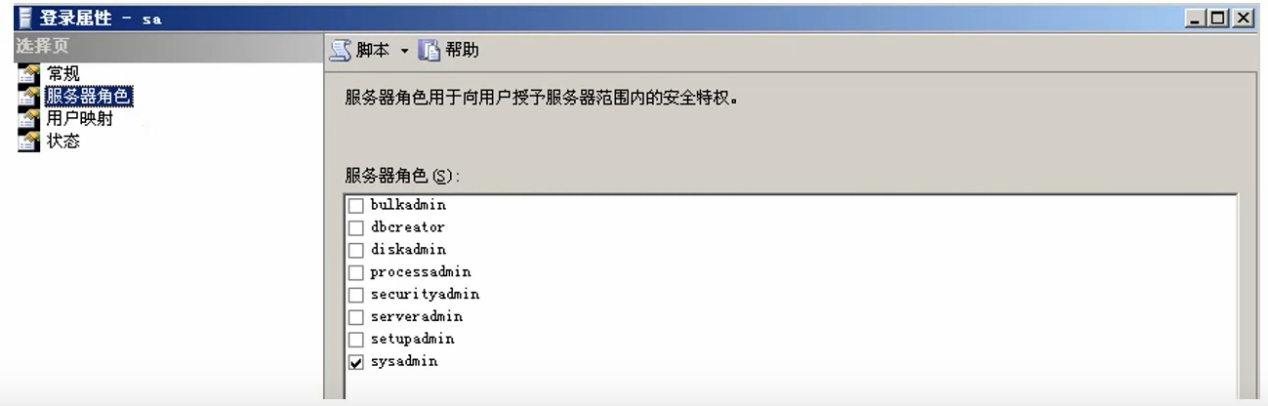
## 4、分配数据库用户所需的最小权限

■ 安全基线项目名称∶数据库管理系统SQLServer共享帐号安全基线要求项

■安全基线项说明∶在数据库权限配置能力内，根据用户的业务需要，配置其所需的最小权限。

■ 检测操作步骤∶

1. 更改数据库属性，取消业务数据库帐号不需要的服务器角色;





2.更改数据库属性，取消业务数据库帐号不需要的"数据库访问许可"和"数据库角色中允许”中不需要的角色。





## 网络访问限制

■安全基线项目名称∶数据库管理系统SQLServer共享帐号安全基线要求项

■安全基线项说明∶通过数据库所在操作系统或防火墙限制，只有信任的IP 地址才能通过监听器访问数据库。

■检测操作步骤∶

在防火墙中做限制，只允许与指定的IP地址建立1433的通讯。当然，从更为安全的角度来考虑，应该把1433端口改成其他的端口。

1. 在"Windows 防火墙"对话框中，单击"例外"选项卡。
2. 单击"添加端口"。
3. 键入您要允许的端口名称，键入端口号，然后单击"TCP"或"UDP"以提示这是TCP还是 UDP端口。
4. 单击"更改范围"。
5. 指定要为其阻止此端口的一系列计算机，然后单击"确定"。

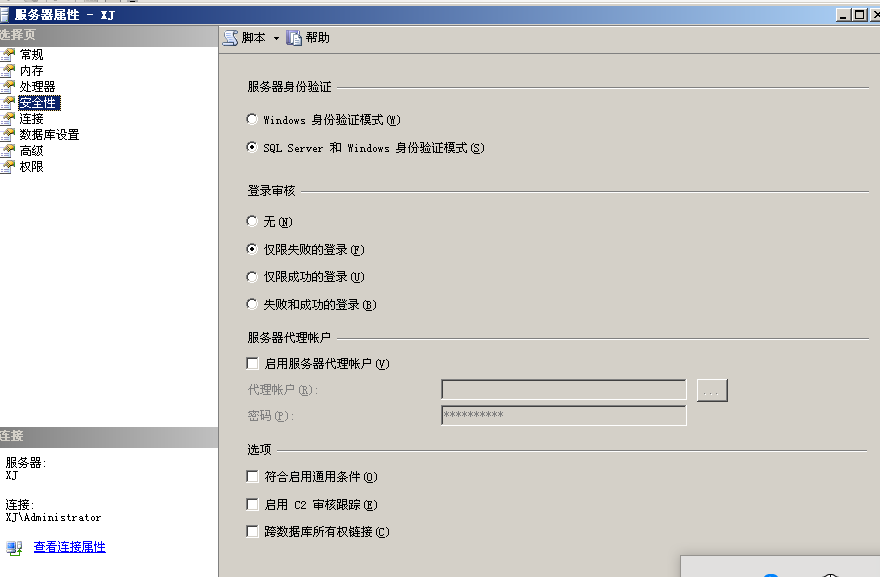
■基线符合性判定依据∶无关IP不允许连接1433端口

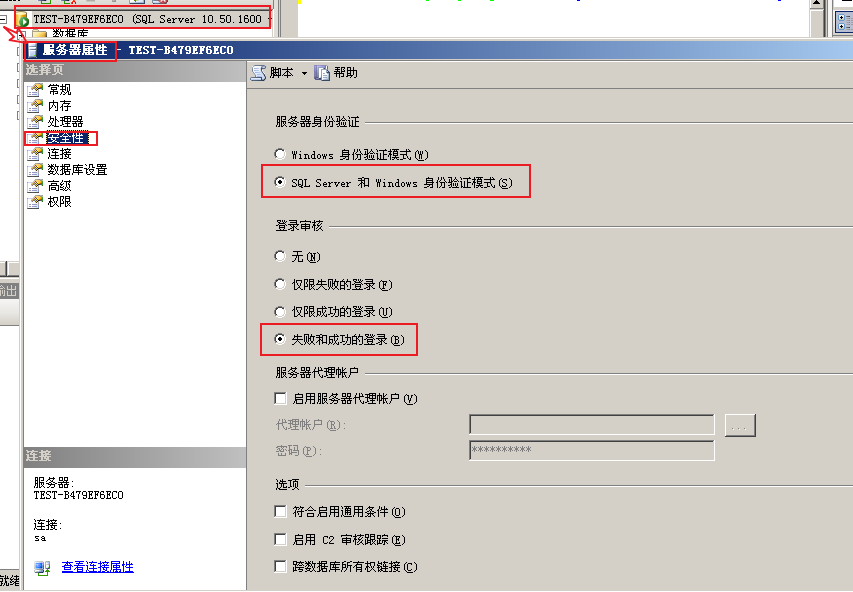
## Sql-server审计登陆

■ 安全基线项目名称.数据库管理系统SQLServer登录审计安全基线要求项

■ 安全基线项说明∶数据库应配置日志功能，对用户登录进行记录，记录内容包括用户登录使用的帐号、登录是否成功、登录时间。

■ 检测操作步骤∶打开数据库属性，选择安全性，将安全性中的审计级别调整为"全部

■基线符合性判定依据∶ 登录成功和失败测试，检查相关信息是否被记录



## Sql-server安全事件审计

■安全基线项目名称∶ 数据库管理系统SQLServer安全事件审计安全基线要求项

■安全基线项说明∶数据库应配置日志功能，记录对与数据库相关的安全事件。

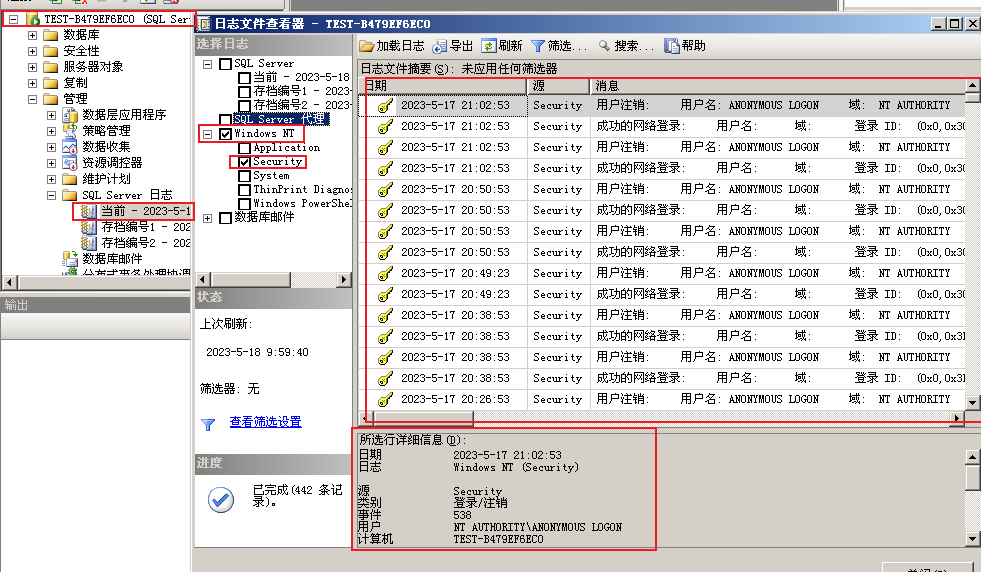
■检测操作步骤∶

打开企业管理器，查看数据库"管理"中的"SQL Server日志"，查看当前的日志记录和存档的日志记录是否包含相关数据库安全事件

1. 参考配置操作数据库默认开启日志记录
2. 补充操作说明

增加帐号登陆审计∶打开数据库属性，选择安全性，将安全性中的审计级别调整为"全部"。

■基线符合性判定依据∶SQL Server日志中是否存在数据库相关事件日志信息。



## 数据库的补丁要求

■安全基线项目名称∶数据库管理系统SQLServer补丁安全基线要求项

■安全基线项说明∶ 为系统打最新的补丁包。

■检测操作步骤∶

检查当前所有已安装的数据库产品的版本信息，运行SQL查询分析器，执行∶select @@version

