GBase 8s 三权分立配置示例

南 大 通 用 数 据 技 术 股 份 有 限 公 司

General Data Technologies Co., Ltd.

天津总公司：天津市高新区华苑产业园区开华道 22 号普天创新园东塔 20-23 层

电　　话：022-58815678

传　　真：022-58815679

北京分公司：北京市朝阳区太阳宫中路 12 号太阳宫大厦 10 层 1008 室

电　　话：010-88866866

传　　真：010-88864556

http://www.gbase.cn

E-mail:info@gbase.cn

南大通用数据库 GBase 8s 三权分立配置示例，南大通用数据技术股份有限公司

作者：
终审者：

通讯方式
南大通用数据技术股份有限公司
中国天津市高新区华苑产业园区开华道 22 号普天创新园东塔 20-23 层(300384)
电话：400-013-9696　　邮箱：info@gbase.cn

目 录

1. 三权分立介绍

数据一旦保存在数据库里就真的安全了吗？事实并非如此简单。因为在数据库中还存在一些所谓的“超级用户”（也称为DBA-数据库管理员的英文文缩写），例如 Oracle 数据库中的 sys 和 system 用户，IBM DB2 数据库的 db2admin 用户，Microsoft SQL Server 或 Sybase 数据库的 sa 用户。只要用这些超级用户登录数据库，就可以看到数据库中所有用户的数据，也可以修改任何用户的数据。

过度集中的权力带来高风险

为什么会存在这些超级用户呢？这些超级用户是数据库创建过程中的缺省用户，可以认为是数据库中的“造物主”，因为所有新的用户都是由他们创建的。他们就象 Unix 系统的 root 用户，Windows 的 Adminstrator 用户，有着至高无上的权力。当然，为了安全，一般这种超级用户的口令都被掌握在极少数人手里。

但是过度集中的权力都会带来问题，当超级用户拥有最高权力的时候，意味着他或她可以做任何想做的事，而且可以不留下任何痕迹。这种诱惑力太大了，如果你也看过科幻电影《透明人(Hollow Man)》，就知道这种诱惑可能会让一个原本善良的人滑向罪恶的深渊。

事实上，我们有过这么一些例子：某大型企业的 DBA 在公司的财务系统数据库中查到老总的工资，晒到了网上；某外包公司的技术人员利用非法获取的 DBA 口令在移动公司的数据库中篡改充值卡数据，为自己牟利了三百多万；爱尔兰的某个政府雇员利用自己的管理员身份把高收入人群的信息偷出来交给自己的弟弟，而他弟弟据此勒索那些富人的钱财；美国一个金融服务公司的 DBA 在五年时间内盗取了八百多万客户的名单，自己开了家公司靠出卖这些信息赢利；而金融危机爆发以后，也有听到被裁员的员工带走公司机密的案例。

举这些例子并不是想说明 DBA 是不可靠的（事实上绝大部分的 DBA 都是称职的数据保护者），而是过于集中的权力给 DBA 这个角色带来了很大的风险。

那么如何防止这些滥用特权的行为呢？有些企业想的办法是把超级用户的密码分成两段，必须由两个人一起输入才能登录，所有操作也必须两人同时在场。这看上去更安全了，但是就象保管金库的两个人可以串通了一起监守自盗一样，这个方法并不能解决本质的问题。

三权分立

现实世界里解决权力过度集中的方式之一就是三权分立（这里的“三”可以泛指为“多”）。我们想象一下，如果有人可以执行管理数据的操作，有人负责控制管理数据的规则，另外还有人监督和审计前两类人的行为，那么权力过度集中的问题就可以通过互相制约被解决。这就和政治学里著名的行政、立法、司法三权分立不谋而合。

以下是数据管理三权分立的详细规划：

第一类用户是**数据库管理员**，他们有数据的管理权（行政权）。他们可以授予和取消普通用户数据访问的权限，执行数据管理的各种操作。他们仍然能做一些特殊的，需要数据库级权限的操作，例如备份整个数据库的数据。但是传统的数据库管理员的“万能”的权力被大大削减，包括创建新用户的权限也会被收回。

第二类用户是**安全管理员**，他们拥有安全规则的制定权（立法权），和之前的由 DBA 管理用户权限不同的是，他们在数据库原有的权限管理之外，对数据的访问控制做更周密和灵活的规则设置。例如指定某些敏感数据的集合只能被指定的用户访问，如果没有被指定，即使是 DBA 也无法访问。又例如，即使是数据的所有者，也可以被安全管理员限制不能删除自己的数据。安全管理员可以规定某些操作只能在某个时间段内执行，或者某些操作只能在指定的 IP 地址上执行。

但是安全管理员不能为用户授予各种权限，也就是说，如果要想让某个用户（包括安全管理员自己）看到另一个用户的数据，还必须由另一个用户自身或者数据库管理员先对该用户授权。

这是一种互相制约的机制。安全管理员可以创建新用户，可以指定新用户为某些敏感数据的允许访问者，这是个必要条件。但是并不意味着这个新用户就可以看到这些敏感数据，他还需要得到 DBA 的授权。而 DBA 也不再能随意查询或修改其他用户的数据。DBA 原来的种种特权也可以被安全管理员根据实际需求通过命令规则进行限制。

第三类用户是**审计管理员**，他们拥有数据操作的审计权（司法权）。他们可以监督前两类用户的操作，如果发现有不符合法规或内部控制要求的活动，他们可以调查这些活动的细节。这些活动可能包括数据库管理员将权限授给不合适的用户，或者安全管理员临时取消某些安全规则，以方便某些用户执行非法操作等

等。

审计管理员和**安全管理员**一样，本身都不能执行对其他用户的具体数据的操作，这是一种平衡。但是审计管理员拥有一套机制，可以保护审计记录数据不会被数据库管理员或者安全管理员删除或者篡改。

对于普通的数据库用户，相当于平民大众，他们的日常操作不会受到任何影响，所有访问数据库的应用程序也不需要做任何修改。但是他们对敏感数据的所有操作，也可以被记录下来，受到审计管理员的审计和监督。

至此，滥用数据库超级用户特权的安全漏洞可以完全被堵住。整个数据管理的安全性也得到了本质的提高。

数据库发展的新方向

这套三权分立的机制看上去比较复杂，而且需要至少三个人才能实现。但是如果被管理的数据确实很重要，泄漏或破坏的后果非常严重的话，那么相信我，建立这么一套机制是必要的。

尤其是设立审计管理员之后，对一些没有事先采取防范措施导致的事故可以做事后的追溯，从而可以清楚地区分事故的责任。

有人要问，我只有一个 DBA，如何做三权分立？其实，只要有一个安全控制和审计软件系统，安全管理员和审计管理员并不需要由专职的懂数据库的技术人员担当，因为他们的操作非常简单，都是通过图形化的界面完成。举个例子，审计管理员就可以由 IT 部门经理自己担任，他只需要通过报表和报警信息就可以完成日常的审计，而且还可以了解自己的下属都在做什么。

也有人要问，三权分立看上去很不错，但是实现起来是不是很困难呢？事实上，数据管理的三权分立已经成为数据库发展新的方向之一。首先，各种主流的数据库都已经提供了数据库审计的功能，而以 Oracle Audit Vault 为代表的数据库审计软件能把企业组织内部所有的数据库（无论是 Oracle, DB2, 还是 SQL Server, Sybase）的审计信息集中管理起来，解决了审计管理员的问题。其次，在安全控制上，各主流的数据库厂商也已经或即将推出相应的解决方案。

当然，目前对基于文件系统的数据管理实现三权分立还有些难度，所以，还是把敏感的数据存放在数据库中吧，这是更好的选择。

以上信息来自《软件世界》2009 年第 4 期 《我的数据真的安全吗》

2. 数据库三权分立配置示例

GBase 8s 数据库的三权分立是以超级管理员权限拆分来实现的。分解为数据库管理员（DBA），安全管理员（SSO）和审计管理员（AAO）。

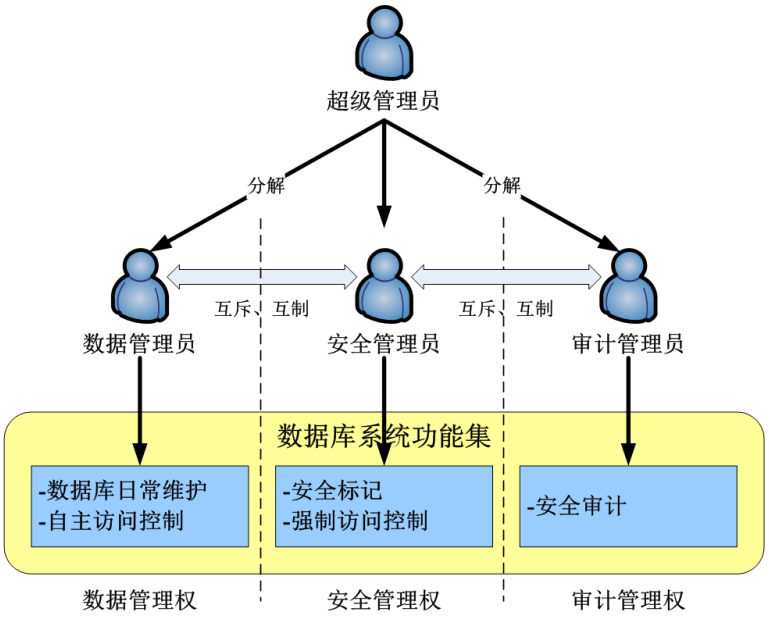

图 1 三权分立示意图

数据库管理员的主要职责：

- 数据库日常维护
- 自主访问控制

安全管理员的主要职责：

- 安全标记
- 强制访问控制

审计管理员的主要职责：

- 安全审计

2.1. 角色和用户

根据三权分立的原则，数据库需要创建三个角色（组）：DBA 组，使用 gbasedbt 组名；SSO 组，使用 dbsso 组名；aao 组，使用 dbaao 组名。

同时创建同组名相同的用户名。

```
# 创建三个组
[root@a01 ~]# groupadd gbasedbt
[root@a01 ~]# groupadd dbsso
```

```
[root@a01 ~]# groupadd dbaao
# 创建三个用户
[root@a01 ~]# useradd -g gbasedbt -d /home/gbase -m -s /bin/bash gbasedbt
[root@a01 ~]# useradd -g dbsso -d /home/dbsso -m -s /bin/bash dbsso
[root@a01 ~]# useradd -g dbaao -d /home/dbaao -m -s /bin/bash dbaao
```

2.2. 数据库软件安装

可以在数据库软件安装时指定开启角色分离，并绑定用户组到角色。以下仅列出关键选项。

```
[root@a01 install]# ./ids_install
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...
……(省略)……

DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y/N): Y      # 接受协议



===============================================================================
Installation Location
---------------------

Choose location for software installation.

  Default Install Folder: /opt/GBASE/gbase

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO ACCEPT THE DEFAULT
      : /opt/gbase                    # 指定目录

INSTALL FOLDER IS: /opt/gbase
   IS THIS CORRECT? (Y/N): Y          # 确认目录

……(省略)……

Custom: Install the database server with specific features and software that
you need.
Optionally install a configured database server instance.
Minimum disk space required: 75 MB (without a server instance)

  ->1- Typical installation
```

```
    2- Custom installation
    3- Extract the product files (-DLEGACY option)

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: 2
    # 选择自定义安装方式

……(省略)……

================================================================================
Get Role Separation choice
--------------------------

Enable role separation for auditing procedures.

If you enable role separation, you can assign existing groups of users to
specific roles.

If you do not enable role separation, the database server administrator
performs all administration tasks.

    1- Enable role separation
  ->2- Do not enable role separation

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: 1
    # 选择启用角色分离

================================================================================
Role Separation groups selection
--------------------------------

Assign a group of users to each of the following roles by specifying group
identifiers (group IDs). The group IDs specified must already exist on your
system.

Group for security-related tasks: (DEFAULT: gbasedbt): dbsso
    # 安全相关的角色（组）
Group for audit-administration tasks: (DEFAULT: gbasedbt): dbaao
    # 审计相关的角色（组）
Group for database users (leave blank to allow all users): (DEFAULT: ): (回车)
    # 数据库用户组，空白是所有的用户，或者指定角色组


================================================================================
Server Instance
```

```
---------------

Type 'back' to go to the previous step or 'quit' to cancel the installation.

Create a database server instance?


    1- Yes - create a server instance
  ->2- No - do not create a server instance

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS <ENTER> TO ACCEPT THE DEFAULT:: (回车)

……(省略)……

================================================================================
Installation Complete
---------------------

Congratulations! GBase Software Bundle installation is complete.

Product install status:
GBase: Successful
GBase Connect: Successful

Main Version: GBase 8s V8.8


For more information about using GBase products, see the GBase Information
Center at http://www.gbase.cn.

PRESS <ENTER> TO EXIT THE INSTALLER: (回车)          # 完成安装
```

软件安装完成后，安装目录/opt/gbase 下 aaodir 的目录及其包含的文件所属组为 dbaao，dbssodir 的目录及其包含的文件所属组为 dbsso。

```
drwxrwxr-x.  2 gbasedbt dbaao        38 9月   8 10:50 aaodir
drwxrwxr-x.  2 gbasedbt dbsso        40 9月   8 10:51 dbssodir
```

dbssodir 目录下的 seccfg 配置文件，IXUSERS 参数决定哪个组（指明组名）或者是所有用户均为数据库用户（值为*）。

```
[gbasedbt@a01 dbssodir]$ more seccfg
IXUSERS=*
```

2.3. 初始化数据库实例

按照通用的数据库初始化方式进行数据库实例初始化操作：修改环境变量、创建配置文件 SQLHOSTS、创建修改配置文件 ONCONFIG、配置磁盘空间和初始化操作。

这里不在详细说明如何进行实例初始化。

2.4. 三权分立-审计配置

角色分离（三权分立）后，DBA 用户将无权使用审计相关的操作，SSO 用户可以设置安全掩码但无权开启审计和查看审计，AAO 用户可以开启审计和查看审计但无权设置安全掩码。

2.4.1. 系统表 sysadtinfo 表赋权

确认 public 用户有访问 sysmaster 库 sysadtinfo 表的权限。

```
[gbasedbt@a01 ~]$ echo 'select tabauth from systabauth where tabid = (select tabid
from systables where tabname = "sysadtinfo");' | dbaccess sysmaster -

Database selected.

tabauth

s--------

1 row(s) retrieved.
```

如果不是's--------',则需要修改为此值，然后必须重启数据库生效。

```
[gbasedbt@a01 ~]$ echo 'update systabauth set tabauth=" s--------" where tabid =
(select tabid from systables where tabname = "sysadtinfo");' | dbaccess sysmaster
-
```

2.4.2. 审计配置的用户

DBA 用户执行查看审计配置命令，被限制；执行数据库管理命令则成功。

```
[gbasedbt@a01 ~]$ onaudit -c
Onaudit -- Audit Subsystem Configuration Utility
```

```
Must be an AAO or DBSSO to run this program.

[gbasedbt@a01 ~]$ onstat -g sql
On-Line -- Up 00:11:14 -- 508696 Kbytes

Sess       SQL            Current            Iso Lock       SQL  ISAM F.E.
Id          Stmt type       Database            Lvl Mode        ERR  ERR  Vers
Explain
31         -              testdb             CR  Not Wait    0    0    9.24  Off
```

dbsso 用户执行查看审计配置命令，被限制；执行数据库管理命令，被限制。

```
[dbsso@a01 ~]$ onaudit -c
Onaudit -- Audit Subsystem Configuration Utility

Must be an AAO to execute this action.

[dbsso@a01 ~]$ onstat -g sql
On-Line -- Up 00:10:25 -- 508696 Kbytes

Must be a DBSA to run this program
```

dbaao 用户执行查看审计配置命令成功，执行数据库管理命令，被限制。

```
[dbaao@a01 ~]$ onaudit -c
Onaudit -- Audit Subsystem Configuration Utility

Current audit system configuration:
    ADTMODE    = 0
    ADTERR     = 0
    ADTPATH    = /usr/gbasedbt/aaodir
    ADTSIZE    = 50000
    Audit file = 0
    ADTROWS    = 0

[dbaao@a01 ~]$ onstat -g sql
On-Line -- Up 00:09:23 -- 508696 Kbytes

Must be a DBSA to run this program
```

2.4.3. 审计配置步骤

2.4.3.1. 使用 dbaao 用户配置审计相关参数以及开启审计

创建目录，设置 ADTPATH，开启审计，查看审计配置文件

```
[dbaao@a01 ~]$ mkdir -p /home/dbaao/aaodir
[dbaao@a01 ~]$ chmod 755 /home/dbaao/aaodir

[dbaao@a01 ~]$ onaudit -p /home/dbaao/aaodir/
Onaudit -- Audit Subsystem Configuration Utility

[dbaao@a01 ~]$ onaudit -l 1
Onaudit -- Audit Subsystem Configuration Utility

[dbaao@a01 ~]$ onaudit -c
Onaudit -- Audit Subsystem Configuration Utility

Current audit system configuration:
    ADTMODE    = 1
    ADTERR     = 0
    ADTPATH    = /home/dbaao/aaodir/
    ADTSIZE    = 50000
    Audit file = 0
    ADTROWS    = 0
```

2.4.3.2. 使用 dbsso 用户设置审计掩码

设置审计掩码，查看审计掩码

```
[dbsso@gbase8s05 ~]$ onaudit -o -y
Onaudit -- Audit Subsystem Configuration Utility

_default                            -

[dbsso@gbase8s05 ~]$ onaudit -m -u _default -e +CRDB,DRDB,CRTB,DRTB,ALTB,CLDB
Onaudit -- Audit Subsystem Configuration Utility


[dbsso@gbase8s05 ~]$ onaudit -o -y
Onaudit -- Audit Subsystem Configuration Utility
```

```
_default                                -    ALTB,CLDB,CRDB,CRTB,DRDB,DRTB
```

2.4.3.3. 数据库用户触发审计事件

数据库用户触发 CRDB 和 CRTB 事件

```
[gbasedbt@a01 ~]$ dbaccess - -
> create database t1db;

Database created.

> create table tab1(col1 int);

Table created.

>
```

2.4.3.4. 使用 dbaao 用户查看审计内容

通过查看审计日志的方式查看审计内容

```
[dbaao@a01 ~]$ more /home/dbaao/aaodir/gbase01.1
ONLN|2021-09-08 12:33:45.000|localhost|24110|gbase01|dbsso|0:CLDB:sysmaster
ONLN|2021-09-08 12:33:48.000|localhost|24113|gbase01|dbsso|0:CLDB:sysmaster
ONLN|2021-09-08 12:35:51.000|localhost|24131|gbase01|gbasedbt|0:CRDB:t1db:-
ONLN|2021-09-08
12:36:03.000|localhost|24131|gbase01|gbasedbt|0:CRTB:t1db:100:tab1:gbasedbt:0:-
```

通过 onshowaudit 查看审计内容

```
[dbaao@a01 ~]$ onshowaudit
ONSHOWAUDIT Secure Audit Utility
GBASE-SQL Version 12.10.FC4G1TL
The directory name specified by the ADTPATH configuration parameter does not
 exist or does not have the necessary permissions.
```

如果出现以上错误，修改$GBASEDBTDIR/aaodir/adtcfg 配置文件中的 ADTPATH 为实际的审计目录，如：/home/dbaao/aaodir。再次执行

```
[dbaao@a01 ~]$ onshowaudit
ONSHOWAUDIT Secure Audit Utility
GBASE-SQL Version 12.10.FC4G1TL
ONLN|2021-09-08 12:33:45.000|localhost|24110|gbase01|dbsso|0:CLDB:sysmaster

ONLN|2021-09-08 12:33:48.000|localhost|24113|gbase01|dbsso|0:CLDB:sysmaster
```

```
ONLN|2021-09-08 12:35:51.000|localhost|24131|gbase01|gbasedbt|0:CRDB:t1db:-

ONLN|2021-09-08
12:36:03.000|localhost|24131|gbase01|gbasedbt|0:CRTB:t1db:100:tab1:gbasedbt:0:-

ONLN|2021-09-08 12:41:37.000|localhost|24131|gbase01|gbasedbt|0:CLDB:t1db


Program Over
```

2.4.3.5. 审计日志安全

审计日志所在的目录为/home/dbaao/aaodir，目录及日志文件的各级权限为

一级目录/home

```
drwxr-xr-x.   6 root     root       60 9月   7 20:35 home
```

二级目录/home/dbaao，仅限 dbaao 用户可进入，同级的有 dbsso 和 gbase

```
drwx------. 6 dbaao    dbaao    158 9月   7 20:43 dbaao
drwx------. 5 dbsso    dbsso    144 9月   7 20:39 dbsso
drwxr-xr-x. 5 gbasedbt gbasedbt 144 9月   8 12:44 gbase
```

三级目录/home/dbaao/aaodir，gbasedbt 用户及 dbaao 组用户可进入

```
drwxr-xr-x. 2 dbaao    dbaao     23 9月   8 12:45 aaodir
```

审计日志文件权限，gbasedbt 用户及 dbaao 组用户可读可写

```
-rw-rw----. 1 gbasedbt dbaao    398 9月   8 12:41 gbase01.1
```

综合以上权限：

DBA 用户 gbasedbt 用户无法进入审计日志所在的目录，则无法删除审计日志；AAO 用户 dbaao 用户可查看审计日志内容。仅操作系统 root 和 dbaao 用户有权限删除审计日志。

2.5. 未开启角色分离的实例启用三权分立配置示例

按照 2.1 创建 SSO 组和 AAO 组，以及对应的用户。

```
# 创建两个组 (DBA 组 gbasedbt 应当已经存在)
[root@a01 ~]# groupadd dbsso
[root@a01 ~]# groupadd dbaao
# 创建两个用户
[root@a01 ~]# useradd -g dbsso -d /home/dbsso -m -s /bin/bash dbsso
```

```
[root@a01 ~]# useradd -g dbaao -d /home/dbaao -m -s /bin/bash dbaao
```

关闭数据库

```
[gbasedbt@a01 ~]$ onmode -ky
```

按 2.2 修改软件安装目录下的 aaodir、dbssodir 目录及含文件的属组

```
[root@a01 gbase]# chgrp -R dbaao aaodir
[root@a01 gbase]# chgrp -R dbsso dbssodir
```

检查软件安装目录下的 dbssodir 目录下的 seccfg 配置文件内容中的 IXUSERS 参数值，如果不是 IXUSERS=*，数据库启动将报错误。

```
[gbasedbt@a01 dbssodir]$ more seccfg
IXUSERS=*
```

重新启动数据库

```
[gbasedbt@a01 ~]$ oninit -vy
```

此时可以按照 2.4 来配置三权分立，唯一需要注意的是 2.4.2.2 使用 dbsso 用户设置审计掩码中，因为无默认的掩码名称_default，故需要创建该掩码。

```
[dbsso@a01 ~]$ onaudit -o -y
Onaudit -- Audit Subsystem Configuration Utility

[dbsso@a01 ~]$ onaudit -a -u _default -e +CRDB,DRDB,CRTB,DRTB,ALTB,CLDB
Onaudit -- Audit Subsystem Configuration Utility

[dbsso@a01 ~]$ onaudit -o -y
Onaudit -- Audit Subsystem Configuration Utility

_default                              -    ALTB,CLDB,CRDB,CRTB,DRDB,DRTB
```