步步高零售系统权限配置手册

作者: IBM

创建日期: 15-May-13

最后更新:

控制号:

版本: V0.2

1. **Title, Subject, Last Updated Date, Reference Number**, **and** **Version** are marked by a Word Bookmark so that they can be easily reproduced in the header and footer of documents. When you change any of these values, be careful not to accidentally delete the bookmark. **You can make bookmarks visible by selecting Tools->Options…View and checking the Bookmarks option in the Show region.**

**审批:**

|  |  |
| --- | --- |
| 公司项目经理 |  |
| 步步高项目经理 |  |

## 文档控制

**变更记录**

1

| 日期 | 作者 | 版本 | 变更索引 |
| --- | --- | --- | --- |
|  |  |  |  |
| 15-May-13 | IBM | 0.1 | 初始版本 |
| 22-May-13 | IBM | 0.2 | 添加权限相关数据库表结构 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**审阅**

| 姓名 | 职务 |
| --- | --- |
|  |  |
|  | 步步高项目经理 |
|  | IBM项目经理 |
|  |  |
|  |  |

**分发**

| 份数.. | 姓名 | 职位 |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

目录

文档控制 ii

RMS 4

权限配置 4

用户创建 6

用户权限赋予 8

用户权限移除 8

删除用户 9

SIM 10

权限配置 10

用户创建 11

用户权限赋予 11

用户权限移除 12

删除用户 12

RPM 13

权限配置 13

用户创建 13

用户权限赋予 14

用户权限移除 14

删除用户 15

BIP/RA 16

权限配置 16

用户创建 17

用户权限赋予 18

用户权限移除 19

删除用户 20

已解决及未解决的问题 21

未解决的问题 21

已解决的问题 21

附录 A 22

## RMS

本文档描述了步步高零售系统中的RMS应用模块中的权限配置，用户创建/删除以及用户权限的赋予与移除。

### 权限配置

#### 创建Functional Role

* **RMS中Functional Role和DB的Role一一匹配**
* **使用下列脚本创建DB Role**

|  |
| --- |
| CREATE ROLE *ROLE\_NAME;* |

*其中ROLE\_NAME代表Functional Role*

#### 分配系统功能到Functional Role

* Form级别
  + Form级别是控制Functional Role能否有权限进入该Form
  + Form级别是在Nav\_element\_mode\_role表中控制的
  + 使用下列脚本给Functional Role赋予进入Form权限

|  |
| --- |
| Insert into nav\_element\_mode\_role values(*ELEMENT,NAV\_MODE,FOLDER,ROLE*); |

*ELEMENT代表Form;*

*NAV\_MODE代表导航模式（查看，编辑或者默认）*

*FOLDER代表文件夹目录ID*

*ROLE代表Functional Role*

* Form Action级别
  + Form Action级别是控制在进入Form之后的操作，所以在Form Action生效之前需要分配对应Form的进入权限。Form Action分为两类：
    - Find Form界面List，控制可以进入主界面的功能，包括：查看，编辑，创建等
    - 主界面的菜单，控制主界面数据的状态，包括：提交，取消，拒绝，审批等
  + Form Acrion级别是在sec\_form\_action\_role表中控制的
  + 使用下列脚本给Functional Role赋予对应的Form Action权限

|  |
| --- |
| Insert into sec\_form\_action\_role values(SEC\_FORM\_ACTION\_ID,ROLD,MERCH\_LVL,ORG\_LVL); |

*其中SEC\_FORM\_ACTION\_ID代表Form Action对应的ID;*

*ROLE代表Functional Role*

*MERCH\_LVL不使用，留空*

*ORG\_LVL不使用，留空*

#### 数据安全组创建

BBG对于组织数据安全性是定义在地点级别，对于商品层级的安全性定义在大类级别。

由于在RMS中不能够配置数据权限到地点，只能够配置到OU级别，所以每一个门店都有其对应的OU（非真实OU，仅仅是给权限控制使用）

在RMS中数据级别的安全控制在OU级别和商品大类级别，需要在用户创建完成之后给用户赋予对应的数据权限。

创建数据安全组脚本：

* OU级别，一个OU对应一个地点
  + SEC\_GROUP为用户数据安全权限组定义表
  + FILTER\_GROUP\_ORG为声明用户组织数据安全权限组筛选级别，以及筛选内容（BBG使用OU，即地点），当某个用户数据安全权限组在此表中无数据代表“所有”。

|  |
| --- |
| Insert into sec\_group values(GROUP\_ID,GROUP\_NAME,ROLE,COMMENTS);  Insert into FILTER\_GROUP\_ORG values(SEC\_GROUP\_ID,FILTER\_ORG\_LEVEL,FILTER\_ORG\_ID); |

*GROUP\_ID代表用户数据安全权限组ID*

*GROUP\_NAME代表用户数据安全权限组名称。地点组使用：“Security Location 120011”*

*ROLE不使用，留空*

*COMMENTS不使用，留空*

*SEC\_GROUP\_ID代表SEC\_GROUP表中的GROUP\_ID*

*FILTER\_ORG\_LEVEL代表筛选组织级别，O代表OU*

*FILTER\_ORG\_ID代表筛选组织ID，为地点对应的OU*

* 大类级别
  + SEC\_GROUP为用户数据安全权限组定义表
  + FILTER\_GROUP\_MERCH为声明用户商品层级数据安全权限组筛选级别，以及筛选内容（BBG使用大类）, 当某个用户数据安全权限组在此表中无数据代表“所有”。

|  |
| --- |
| Insert into sec\_group values(GROUP\_ID,GROUP\_NAME,ROLE,COMMENTS);  Insert into FILTER\_GROUP\_MERCH values(SEC\_GROUP\_ID,FILTER\_MERCH\_LEVEL,FILTER\_MERCH\_ID,FILTER\_MERCH\_ID\_CLASS,FILTER\_MERCH\_ID\_SUBCLASS); |

*GROUP\_ID代表用户数据安全权限组ID*

*GROUP\_NAME代表用户数据安全权限组名称。地点组使用：“Security Department 38”*

*ROLE不使用，留空*

*COMMENTS不使用，留空*

*SEC\_GROUP\_ID代表SEC\_GROUP表中的GROUP\_ID*

*FILTER\_MERCH\_LEVEL代表筛选组织级别，P代表大类*

*FILTER\_MERCH\_ID代表此用户数据安全权限组筛选ID，为大类ID*

*FILTER\_MERCH\_ID\_CLASS由于使用了大类层级，此处留空*

*FILTER\_MERCH\_ID\_SUBCLASS由于使用了大类层级，此处留空*

### 用户创建

#### 创建脚本

RMS用户是与DB用户集成的，需要使用拥有创建用户的DB用户来创建RMS用户，脚本如下：

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  | | --- | | spool create\_user.log | | create user RMS\_USER | | identified by PASSWORD | | default tablespace RETEK\_DATA | | temporary tablespace TEMP | | quota unlimited on RETEK\_DATA | | quota unlimited on RETEK\_INDEX | | / | |  | | grant --developer, | | alter session, | | analyze any, | | create any view, | | create library, | | create procedure, | | create sequence, | | create session, | | create synonym, | | create table, | | create trigger, | | create view, | | create job, | | delete any table, | | drop any procedure, | | drop any view, | | drop any table, | | execute any procedure, | | execute any type, | | insert any table, | | select any sequence, | | select any table, | | update any table, | | select any dictionary | | to RMS\_USER | | / | |  | | grant select on sys.dba\_role\_privs to RMS\_USER | | / | | grant select on sys.dba\_jobs to RMS\_USER | | / | | grant select on sys.dba\_roles to RMS\_USER | | / | | grant execute on dbms\_rls to RMS\_USER | | / | | grant execute on sys.dbms\_crypto to RMS\_USER | | / | | grant select on sys.dba\_sys\_privs to RMS\_USER | | / | | grant execute on sys.dbms\_alert to RMS\_USER | | / | | grant execute on sys.dbms\_lock to RMS\_USER | | / | | grant execute on sys.dbms\_system to RMS\_USER | | / | | grant AQ\_ADMINISTRATOR\_ROLE to RMS\_USER | | / | | grant execute on DBMS\_AQ to RMS\_USER | | / | | grant execute on DBMS\_AQADM to RMS\_USER | | / | |  | | spool off | |

*RMS\_RMS代表RMS用户ID*

*PASSWORD代表RMS用户密码*

#### 用户属性设置

RMS用户的属性在user\_attrib表中维护，使用如下脚本来维护：

|  |
| --- |
| Insert into user\_attrib values(*USER\_ID,USER\_NAME,LANG,STORE\_DEFAULT,USER\_PHONE,USER\_FAX,USER\_PAGER,USER\_EMAIL,DEFAULT\_PRINTER*); |

*USER\_ID代表RMS用户ID*

*USER\_NAME代表RMS用户姓名*

*LANG代表RMS用户使用语言，1代表英语，8代表中文*

*STORE\_DEFUALT代表默认门店，不使用，留空*

*USER\_PHONE代表RMS用户电话*

*USER\_FAX代表RMS用户传真，不使用，留空*

*USER\_PAGER不使用，留空*

*USER\_EMAIL代表RMS用户电子邮件地址*

*DEFAULT\_PRINTER代表RMS用户默认打印机，不使用，留空*

### 用户权限赋予

#### 用户赋予Functional Role

用户的Functional Role赋予，是在DB中给DB用户赋予Functional Role对应的DB Role，脚本如下：

|  |
| --- |
| GRANT ROLE\_NAME TO RMS\_USER; |

*ROLE\_NAME代表Function Role(DB Role)*

*RMS\_USER代表RMS用户ID(DB User)*

#### 用户赋予数据安全

在用户数据安全权限组定义完成后，需要给用户赋予对应的数据安全（包含组织数据安全和商品层次数据安全）：

|  |
| --- |
| Insert into SEC\_USER\_GROUP values(SEC\_GROUP\_ID,USER\_ID); |

*SEC\_GROUP\_ID代表需要给用户赋予的数据安全权限组的ID*

*USER\_ID代表赋予的RMS用户*

### 用户权限移除

#### 移除Function Role

脚本如下：

|  |
| --- |
| REVOKE ROLE FROM RMS\_USER; |

*ROLE代表Functional Role*

*RMS\_USER代表需要移除权限的RMS用户ID*

#### 移除用户数据安全权限组

脚本如下：

|  |
| --- |
| DELETE FROM SEC\_USER\_GROUP WHERE T.GROUP\_ID=REVOKED\_GROUP\_ID AND T.USER\_ID=RMS\_USER |

*REVOKED\_GROUP\_ID代表用户数据安全权限组的ID*

*RMS\_USER代表需要移除用户数据安全权限组的RMS用户ID*

### 删除用户

#### 删除用户

由于RMS用户为DB用户，所以删除RMS用户需要删除DB用户，脚本如下：

|  |
| --- |
| DROP USER RMS\_USER; |

*RMS\_USER代表要删除的RMS用户ID*

## SIM

本文档描述了步步高零售系统中的SIM应用模块中的权限配置，用户创建/删除以及用户权限的赋予与移除。

### 权限配置

#### 创建Functional Role

* **使用下列脚本创建SIM的Functional Role**

|  |
| --- |
| Insert into ac\_role values(ID,NAME,ROLE\_TYPE\_ID,DESCRIPTION,DATE\_REQUIRED); |

*ID代表SIM的Functional Role的ID*

*NAME代表SIM的Functional Role的名称*

*ROLE\_TYPE代表SIM的Functional Role的类型，1代表公司，2代表门店*

*DESCRIPTION代表SIM的Functional Role的描述*

*DATE\_REQUIRED代表SIM的Functional Role的结束日期是否必须，默认为“N”*

* 界面：管理 >> 安全性 >> 角色维护 >> 创建
* LDAP脚本

|  |
| --- |
| dn: roleName=ROLE\_NAME,cn=SIMRoles,cn=SIM,dc=bbg  changetype: add  objectClass: simRole  roleName: ROLE\_NAME  type: STORE  description: ROLE\_NAME |

*ROLE\_NAME代表Functional Role名称，需要和AC\_ROLE表中的NAME相同*

#### 分配系统功能到Functional Role

* 使用下列脚本给Functional Role赋予对应的SIM系统功能

|  |
| --- |
| insert into ac\_role\_permission values(ID,ROLE\_ID,PERMISSION\_ID,PARAMETER\_KEY,PARAMETER\_VALUE) ; |

*ID代表赋权流水号;*

*ROLE\_ID代表SIM的Functional Role ID，在AC\_ROLE中定义*

*PERMISSION\_ID代表SIM系统功能代表的ID*

*PARAMETER\_KEY不使用，留空*

*PARAMETER\_VALUE不使用，留空*

#### 数据安全分配

SIM由于是给门店使用的，所以自己门店的用户只能够看到自己的数据。所以对于SIM系统不控制商品层级的安全性，默认门店用户拥有自己门店所有的商品层级权限。

* 界面：管理 >> 安全性 >> 角色维护 >> 选择角色 >> 数据权限

### 用户创建

#### 创建脚本

SIM用户与LDAP集成，创建用户脚本如下：

|  |
| --- |
| dn: cn=SIM\_USER,cn=Users,dc=bbg  changetype: add  objectclass: top  objectclass: organizationalperson  objectclass: orcluser  objectclass: person  objectclass: orcluserv2  objectclass: inetorgperson  objectclass: simUser  uid: SIM\_USER  cn: SIM\_USER  superUser: TRUE  empStatus: 0  preferredCountry: CN  preferredLanguage: zh  givenname: SIM\_USER  middleName: M1  sn: SIM\_USER  mail: SIM\_USER@bbg.com  telephoneNumber: 800-111-2222  externalId: SIM\_USER  supervisor: X  description: Store 120001 Super User.  startTimestamp: 20071026000000Z  #endTimestamp:  defaultStore: storeId=120001,cn=SIMStores,cn=SIM,dc=bbg  userpassword: PASSWORD |

*SIM\_RMS代表SIM用户ID*

*PASSWORD代表SIM用户密码*

*defaultStore代表用户登录SIM界面默认的门店*

### 用户权限赋予

#### 用户赋予Functional Role

用户的Functional Role赋予，是在LDAP中给LDAP用户赋予Functional Role对应的SIM Functional Role，脚本如下：

|  |
| --- |
| dn: roleName=SIM\_ROLE,cn=SIM\_USER,cn=Users,dc=bbg  changetype: add  objectclass: simUserRole  roleName: SIM\_ROLE  userRole: roleName= SIM\_ROLE,cn=SIMRoles,cn=SIM,dc=bbg  userRoleStores: storeId=120001,cn=SIMStores,cn=SIM,dc=bbg  userRoleStores: storeId=120002,cn=SIMStores,cn=SIM,dc=bbg |

*ROLE\_NAME代表Function Role(DB Role)*

*SIM\_USER代表SIM用户ID*

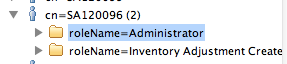
*SIM\_ROLE代表SIM Functional Role*

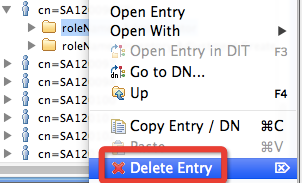
*UserRoleStores代表改Role下改用户能够操作的门店*

### 用户权限移除

#### 移除Function Role

使用LDAP管理工具，查找出需要移除权限的SIM用户：dc=bbg >> cn=Users >> SIM\_USER

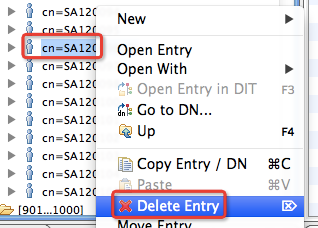




### 删除用户

#### 删除用户

使用LDAP管理工具，查找出需要移除权限的SIM用户：dc=bbg >> cn=Users >> SIM\_USER



## RPM

本文档描述了步步高零售系统中的RPM应用模块中的权限配置，用户创建/删除以及用户权限的赋予与移除。

### 权限配置

#### 创建Functional Role

* **使用下列脚本创建RPM的Functional Role**

|  |
| --- |
| Insert into RSM\_ROLE values(ID,ROLE\_DESCRIPTION); |

*其中ID代表RPM的Functional Role ID*

*ROLE\_DESCRIPTION代表RPM的Functional的描述*

#### 分配系统功能到Functional Role

* 使用下列脚本赋予RPM的Functional Role系统功能

|  |
| --- |
| Insert into RSM\_ROLE\_NAMED\_PERMISSION values(*ID,ROLE\_ID,PERMISSION\_ID,IS\_VIEW,IS\_EDIT,IS\_SUBMIT,IS\_APPROVE,IS\_EMERGENCY*); |

*ID代表流水号*

*ROLE\_ID代表RPM的Functional Role ID*

*PERMISSION\_ID代表RPM的系统功能ID，参考“RSM\_NAMED\_PERMISSION\_DSC”*

*IS\_VIEW代表是否有查看权限，1代表有，0代表没有*

*IS\_EDIT代表是否有编辑权限，1代表有，0代表没有*

*IS\_SUBMIT代表是否有提交权限，1代表有，0代表没有*

*IS\_APPROVE代表是否有审批权限，1代表有，0代表没有*

*IS\_EMERGENCY代表是否有紧急审批权限，1代表有，0代表没有*

***其中（IS\_EMERGENCY>IS\_APPROVE>IS\_SUBMIT>IS\_EDIT>IS\_VIEW）,在最高层的会默认拥有下层权限***

#### 数据安全组

RPM的数据安全组是和Functional Role集成在一起的，及Functional Role包含了系统功能和对应的数据权限。

BBG对于RPM系统的数据安全不做控制，默认每个Role拥有所有所有组织层次和商品层次的权限。

在界面中Functional Role赋数据权限：RSM >> Role Administration >> Edit Data Permissions

### 用户创建

#### 创建脚本

SIM用户与LDAP集成，创建用户脚本如下：

|  |
| --- |
| dn: cn=RPM\_USER,cn=Users,dc=bbg  changetype: add  objectclass: top  objectclass: retailUser  objectclass: person  objectclass: inetorgperson  objectclass: organizationalperson  objectclass: orcluser  objectclass: orcluserv2  uid: RPM\_USER  cn: RPM\_USER  givenname: RPM\_USER  sn: RPM\_USER  userpassword: PASSWORD |

*SIM\_RMS代表RPM用户ID*

*PASSWORD代表RPM用户密码*

### 用户权限赋予

#### 用户赋予Functional Role

脚本如下：

|  |
| --- |
| Insert into RSM\_USER\_ROLE values(ID,USER\_ID,ROLE\_ID,START\_DATE\_TIME,END\_DATE\_TIME); |

*ID代表用户赋权流水号*

*USER\_ID代表RPM用户ID*

*ROLE\_ID代表RPM的Functional Role的ID*

*START\_DATE\_TIME代表用户的有效开始时间*

*END\_DATE\_TIME代表用户的有效结束时间*

### 用户权限移除

#### 移除Function Role

脚本如下：

|  |
| --- |
| DELETE FROM RSM\_USER\_ROLE T WHERE T.USER\_ID=RPM\_USER AND T.ROLE\_ID |

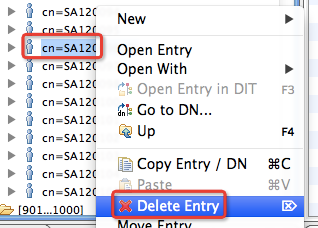
*ROLE\_ID代表RPM的Functional Role的ID*

*RPM\_USER代表需要移除权限的RPM用户ID*

### 删除用户

#### 删除用户

使用LDAP管理工具，查找出需要移除权限的SIM用户：dc=bbg >> cn=Users >> RPM\_USER



## BIP/RA

本文档描述了步步高零售系统中的BIP/RA应用模块中的权限配置，用户创建/删除以及用户权限的赋予与移除。

### 权限配置

#### 创建Functional Role

BIP/RA是一个应用里面的两个组件，它的Functional Role在weblogic中创建，并在weblogic中匹配对应的LDAP Group

* **使用下列脚本创建LDAP Role(Group)**

|  |
| --- |
| dn: cn=BIP\_RA\_ROLE,cn=Groups,dc=bbg  changetype: add  objectclass: groupOfUniqueNames  objectclass: orclGroup  objectclass: orclprivilegegroup  objectclass: top  cn: BIP\_RA\_ROLE |

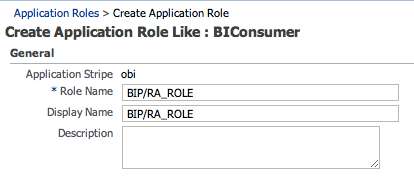
*其中BIP\_RA\_ROLE代表BIP/RA的Functional Role*

#### weblogic匹配LDAP Group

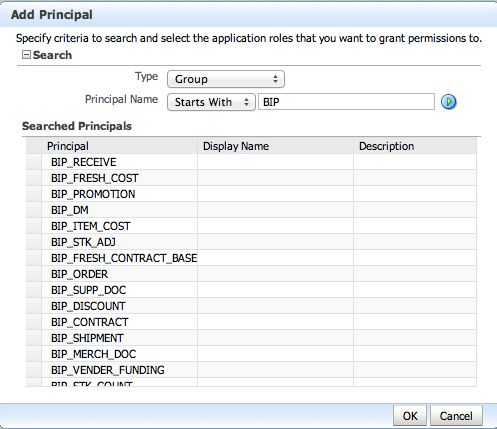
* 登录weblogic的EM：

http://raap2.bbg.com.cn:7001/em

* 创建BIP/RA的Functional Role：Business Intelligence >> coreappliction >> Security >> Application Role >> Create



* 在BIP/RA的Functional Role中添加LDAP Group：Add >> Type: Group >> 查找Group >>确定

**

#### 赋予Functional Role RA权限

使用RA管理员登录RA：

http://raap1.bbg.com.cn:9704/analytics

* 系统功能

管理 >> 管理权限

* 仪表盘

目录 >> 共享文件夹 >> RA报表 >> 仪表盘 >> *选择仪表盘* >> 权限

#### 赋予Functional Role BIP权限

BIP的权限管理是与RA集成的，对于报表的可见性的权限在RA中控制。

使用RA管理员登录RA：

http://raap1.bbg.com.cn:9704/analytics

* BIP报表

目录 >> 共享文件夹 >> BIP报表 >>*选择报表文件夹* >> 权限

### 用户创建

#### 创建脚本

BIP/RA用户与LDAP集成下面是在LDAP中创建用户的脚本：

|  |
| --- |
| dn: cn=BIP\_RA\_USER,cn=Users,dc=bbg  changetype: add  objectclass: inetOrgPerson  objectclass: orclUser  objectclass: orclUserV2  objectclass: organizationalPerson  objectclass: person  objectclass: top  cn: BIP\_RA\_USER  sn: BIP\_RA\_USER  description: BI administrative user.  givenname: BIP\_RA\_USER  mail: BIP\_RA\_USER  uid: BIP\_RA\_USER  userpassword: PASSWORD |

*BIP\_RA\_USER代表BIP/RA用户ID*

*PASSWORD代表RMS用户密码*

#### 用户属性设置

* 用户语言设置，BIP与RA集成，对于BIP的用户语言修改是在RA中进行的
  + RA：我的账户 >> 首选项 >> 区域设置
  + BIP：我的账户 >> BI Publisher首选项 >> 报表区域设置

### 用户权限赋予

#### 用户赋予Functional Role

LDAP脚本如下：

|  |
| --- |
| dn: cn=BIP\_RA\_ROLE,cn=Groups,dc=bbg  changetype: modify  add: uniquemember  uniquemember: cn=BIP\_RA\_USER,cn=users,dc=bbg |

*BIP\_RA\_ROLE代表BIP/RA的Function Role*

*BIP\_RA\_USER代表BIP/RA用户ID*

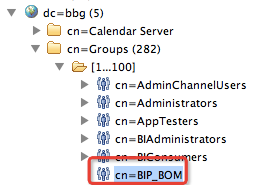
#### 用户赋予数据安全

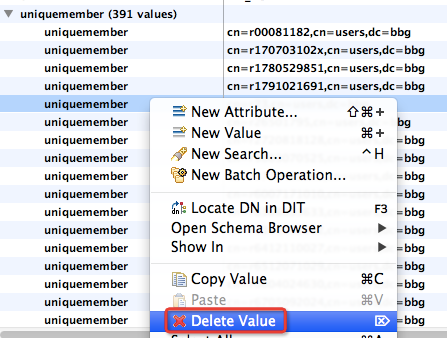
RA用户的数据安全性在数据库表中维护：

RAINY\_USER\_LOC和RAINY\_USER\_LOC

### 用户权限移除

#### 移除Function Role

**

**

#### 移除用户数据安全权限组

删除对应脚本如下：

|  |
| --- |
| DELETE FROM RAINY\_USER\_MERCH T WHERE T.USER\_ID=BIP\_RA\_USER AND T.MERCH=REVOKED\_MERCH;  DELETE FROM RAINY\_USER\_LOC T WHERE T.USER\_ID=BIP\_RA\_USER AND T.LOC=REVOKED\_LOC |

*REVOKED\_MERCH代表大类ID*

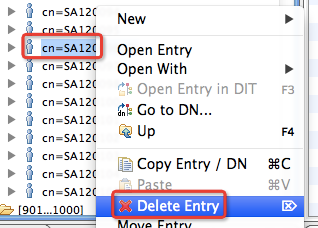
*REVOKED\_LOC代表地点ID*

*BIP\_RA\_USER代表需要移除大类/地点的BIP/RA用户ID*

### 删除用户

#### 删除用户

使用LDAP管理工具，查找出需要移除权限的SIM用户：dc=bbg >> cn=Users >> RPM\_USER



## 已解决及未解决的问题

### 未解决的问题

| 编号 | 说明 | 影响程度 | 负责人 | 计划日期 |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

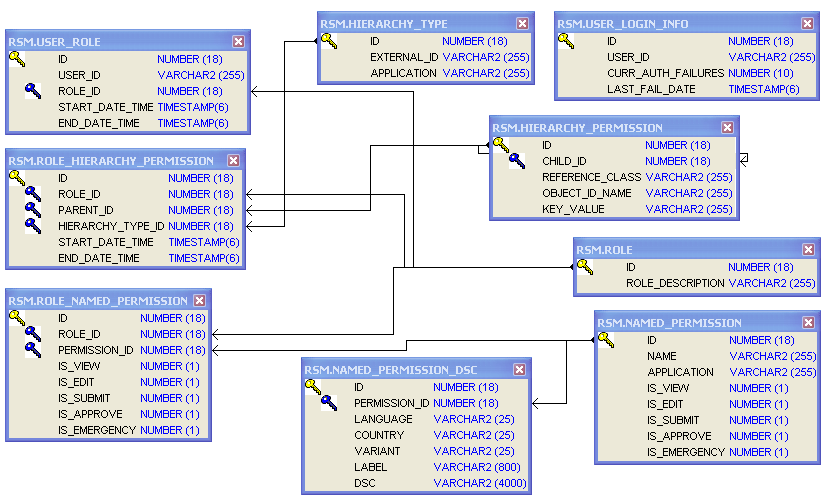
### 已解决的问题

| 编号 | 说明 | 解决方法 | 负责人 | 解决日期 |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## 附录 A

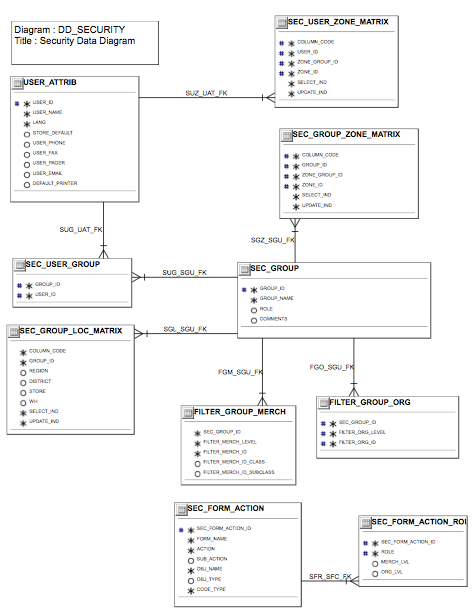
### RPM 权限模型

参考第718-693页，《rpm\_132\_dm.pdf》



### RMS 权限模型

参考《rms-1325-dm.pdf》



### SIM权限模型

参考《sim-1325-dm.pdf》

