

文章

姚鑫 · 十一月 4, 2021 阅读大约需 9 分钟

第六十六章 SQL命令 REVOKE

第六十六章 SQL命令 REVOKE

从用户或角色中删除特权。

大纲

```
REVOKE admin-privilege FROM grantee
```

```
REVOKE role FROM grantee
```

```
REVOKE [GRANT OPTION FOR] object-privilege  
      ON object-list FROM grantee [CASCADE | RESTRICT] [AS grantor]
```

```
REVOKE [GRANT OPTION FOR] SELECT ON CUBE[S] object-list FROM grantee
```

```
REVOKE column-privilege (column-list)  
      ON table FROM grantee [CASCADE | RESTRICT]
```

参数

- admin-privilege - 管理员级特权或以前授予要撤销的管理员级特权的以逗号分隔的列表。
可用的syspriv选项包括16个对象定义权限和4个数据修改权限。对象定义权限为:%CREATEFUNCTION, %DROPFUNCTION, %CREATEMETHOD, %DROPMETHOD, %CREATEPROCEDURE, %DROPPROCEDURE, %CREATEQUERY, %DROPQUERY, %CREATETABLE, %ALTERTABLE, %DROPTABLE, %CREATEVIEW, %ALTERVIEW, %DROPVIEW, %CREATETRIGGER, %DROPTRIGGER。
或者,可以指定%DBOBJECTDEFINITION,这将撤销所有16个对象定义特权。数据修改权限为INSERT、UPDATE、DELETE操作的%NOCHECK、%NOINDEX、%NOLOCK、%NOTRIGGER权限。
- grantee - 拥有SQL系统权限、SQL对象权限或角色的一个或多个用户的列表。
有效值是一个以逗号分隔的用户或角色列表,或“*”。
星号(*)指定当前定义的所有没有%all角色的用户。
- AS grantor - 此子句允许通过指定原始授予者的名称来撤销另一个用户授予的特权。
有效的授予者值是用户名、以逗号分隔的用户名列表或“*”。
星号(*)指定当前定义的所有授予者。
要使用AS授予子句,必须具有%All角色或%AdminSecure资源。
- role - 一个角色或以逗号分隔的角色列表,这些角色的权限将从用户被撤销。
- object-privilege - 基本级别特权或先前授予要撤销的基本级别特权的逗号分隔列表。
该列表可以包含以下一个或多个:%ALTER、DELETE、SELECT、INSERT、UPDATE、EXECUTE和REFERENCES。
要撤销所有特权,可以使用“all [privileges]”或“*”作为此参数的值。
注意,您只能从多维数据集撤销SELECT特权,因为这是惟一可授予的多维数据集特权。
- object-list -
一个以逗号分隔的列表,其中包含一个或多个正在撤销对象特权的表、视图、存储过程或多维数据集。
可以使用SCHEMA关键字指定从指定模式中的所有对象撤销对象特权。
可以使用“*”指定从当前命名空间中的所有对象撤销对象特权。
- column-privilege - 从一个或多个列列表列出的列撤销基本权限。

可用选项有SELECT、INSERT、UPDATE和REFERENCES。

- column-list - 由一个或多个列名组成的列表，用逗号分隔，用括号括起来。
- table - 包含列列表的表或视图的名称。

描述

REVOKE语句撤销允许用户或角色在指定的表、视图、列或其他实体上执行指定任务的权限。

REVOKE还可以撤销用户分配的角色。

REVOKE撤销GRANT命令的操作；

特权只能由授予特权的用户撤销，或者通过CASCADE操作(如下所述)。

可以从指定用户、用户列表或所有用户(使用*语法)撤销角色或特权。

因为REVOKE的准备和执行速度很快，而且通常只运行一次，所以IRIS不会在ODBC、JDBC或动态SQL中为REVOKE创建缓存查询。

即使不能执行实际的撤销(例如，指定的特权从未被授予或已经被撤销)，REVOKE也会成功地完成。

但是，如果在REVOKE操作期间发生错误，SQLCODE将被设置为负数。

撤销的角色

角色可以通过SQL GRANT和REVOKE命令授予或撤销，也可以通过^SECURITY IRIS System SECURITY命令授予或撤销。

可以使用REVOKE命令从某个用户撤销一个角色，也可以从另一个角色撤销一个角色。

不能使用IRIS System Security将角色授予或撤销给其他角色。

特殊变量\$ROLES不显示授予角色的角色。

REVOKE可以指定单个角色，也可以指定要撤销的角色列表，以逗号分隔。

REVOKE可以从指定的用户(或角色)、用户(或角色)列表或所有用户(使用*语法)中撤销一个或多个角色。

GRANT命令可以将一个不存在的角色授予用户。

可以使用REVOKE命令从现有用户撤销不存在的角色。

但是，角色名必须使用与授予角色时相同的字母大小写来指定。

如果试图从不存在的用户或角色撤销现有角色，IRIS将发出SQLCODE -118错误。

如果不是超级用户，并且试图撤销一个不拥有且没有ADMIN OPTION的角色，InterSystems IRIS将发出SQLCODE -112错误。

撤销对象权限

对象特权赋予用户或角色对特定对象的某些权限。

从一个被授予者的对象列表上撤销一个对象特权。

对象列表可以在当前名称空间中指定一个或多个表、视图、存储过程或多维数据集。

通过使用逗号分隔的列表，单个REVOKE语句可以从多个用户和/或角色中撤销多个对象上的多个对象特权。

可以使用星号(*)通配符作为对象列表值，从当前名称空间中的所有对象撤销对象特权。

例如，REVOKE SELECT ON * FROM Deborah将撤销该用户对所有表和视图的SELECT权限。

REVOKE EXECUTE ON * FROM Deborah将撤销该用户对所有非隐藏存储过程的EXECUTE权限。

可以使用SCHEMA SCHEMA

-name作为对象列表值，以撤销指定模式中当前名称空间中的所有表、视图和存储过程的对象特权。

例如，REVOKE SELECT ON SCHEMA Sample FROM

Deborah将撤销该用户对Sample模式中所有对象的SELECT权限。

可以将多个模式指定为逗号分隔的列表；

例如，REVOKE SELECT ON SCHEMA Sample,Cinema FROM

Deborah撤销Sample和Cinema模式中所有对象的SELECT权限。

可以从用户或角色撤消对象特权。

如果从某个角色撤销该权限，则仅通过该角色拥有该权限的用户将不再拥有该权限。

不再拥有特权的用户不能再执行需要该对象特权的现有缓存查询。

当REVOKE撤销对象特权时，它将成功完成并将SQLCODE设置为0。

如果REVOKE没有执行实际的撤销(例如，指定的对象权限从未被授予或已经被撤销)，它将成功完成，并将SQLCODE设置为100(不再有数据)。

如果在REVOKE操作期间发生错误，它将SQLCODE设置为负数。

多维数据集是不受模式名称限制的SQL标识符。

要指定多维数据集对象列表，必须指定CUBE(或cubes)关键字。

因为多维数据集只能有SELECT权限，所以您只能从多维数据集撤销SELECT权限。

对象权限可以通过以下任意方式撤销：

- REVOKE command.

- \$SYSTEM.SQL.Security.RevokePrivilege()方法。

- 通过IRIS系统安全。

转到管理门户，选择系统管理、安全、用户(或系统管理、安全、角色)，为所需的用户或角色选择Edit，然后选择SQL表或SQL视图选项卡。

在下拉列表中选择Namespace。

向下滚动到所需的表，然后单击revoke来撤销权限。

可以通过调用%CHECKPRIV命令来确定当前用户是否具有指定的对象特权。

通过调用\$SYSTEM.SQL.Security.CheckPrivilege()方法，可以确定指定的用户是否具有指定的表级对象特权。

撤销对象所有者特权

如果从对象的所有者那里撤消对SQL对象的特权，那么所有者仍然隐式地拥有对对象的特权。

为了从对象的所有者完全撤销对象上的所有特权，必须更改对象以指定不同的所有者或没有所有者。

撤销表级和列级特权

REVOKE可用于撤销表级特权或列级特权的授予。

表级特权提供对表中所有列的访问。

列级特权提供对表中每个指定列的访问。

向表中的所有列授予列级特权在功能上等同于授予表级特权。

然而，这两者在功能上并不完全相同。

列级REVOKE只能撤销在列级授予的权限。

不能向表授予表级特权，然后在列级为一个或多个列撤销此特权。

在这种情况下，REVOKE语句对已授予的权限没有影响。

CASCADE 或 RESTRICT

IRIS支持可选的CASCADE和Estrict关键字来指定REVOKE对象特权行为。

如果没有指定关键字，则默认为RESTRICT。

可以使用CASCADE或RESTRICT来指定从一个用户撤销对象特权或列特权是否也会从通过WITH GRANT OPTION接收到该特权的任何其他用户撤销该特权。

CASCADE撤销所有这些关联的特权。

当检测到关联的特权时，RESTRICT(默认值)导致REVOKE失败。

相反，它设置SQLCODE -126错误“REVOKE with RESTRICT failed”。

下面的例子展示了这些关键字的使用：

```
--UserA
GRANT Select ON MyTable TO UserB WITH GRANT OPTION

--UserB
GRANT Select ON MyTable TO UserC

--UserA
REVOKE Select ON MyTable FROM UserB
-- This REVOKE fails with SQLCODE -126

--UserA
REVOKE Select ON MyTable FROM UserB CASCADE
-- This REVOKE succeeds
-- It revokes this privilege from UserB and UserC
```

注意，CASCADE和RESTRICT对用户B创建的引用MyTable的视图没有影响。

对缓存查询的影响

当撤销特权或角色时，IRIS将更新系统上所有缓存的查询，以反映特权中的这一更改。但是，当无法访问某个名称空间时——例如，当连接到数据库服务器的ECP连接关闭时——REVOKE会成功完成，但不会对该名称空间中的缓存查询执行任何操作。这是因为REVOKE不能更新不可达名称空间中的缓存查询，以撤销缓存查询级别的特权。没有发出错误。

如果数据库服务器稍后启动，则该名称空间中缓存查询的权限可能不正确。如果某个角色或特权可能在某个名称空间不可访问时被撤销，建议清除该名称空间中的缓存查询。

IRIS Security

REVOKE命令是一个特权操作。在嵌入式SQL中使用REVOKE之前，必须以具有适当特权的用户身份登录。如果不这样做，将导致SQLCODE -99错误(特权冲突)。

使用\$SYSTEM.Security.Login()方法为用户分配适当的权限：

```
DO $SYSTEM.Security.Login("_SYSTEM","SYS")
&sql(      )
```

必须具有%Service_Login:Use权限才能调用\$SYSTEM.Security.登录方法。

示例

下面的嵌入式SQL示例创建两个用户，创建一个角色，并将角色分配给用户。然后，它使用星号(*)语法从所有用户撤销该角色。如果用户或角色已经存在，CREATE语句将发出SQLCODE -118错误。如果用户不存在，GRANT或REVOKE语句将发出SQLCODE -118错误。如果用户存在但角色不存在，则GRANT或REVOKE语句发出SQLCODE 100。

如果用户和角色存在，则GRANT或REVOKE语句发出SQLCODE 0。
即使已经完成了角色的授予或撤销，如果您试图撤销从未被授予的角色，也是如此。

```
ClassMethod Revoke()
{
    d $SYSTEM.Security.Login("_SYSTEM","SYS")
    &sql(
        CREATE USER User1 IDENTIFY BY fredpw
    )
    &sql(
        CREATE USER User2 IDENTIFY BY barneypw
    )
    w !,"CREATE USER error code: ",SQLCODE
    &sql(
        CREATE ROLE workerbee
    )
    w !,"CREATE ROLE error code: ",SQLCODE
    &sql(
        GRANT workerbee TO User1,User2
    )
    w !,"GRANT role error code: ",SQLCODE
    &sql(
        REVOKE workerbee FROM *
    )
    w !,"REVOKE role error code: ",SQLCODE
}
```

在下面的示例中，使用AS授予子句，一个用户(Joe)授予一个特权，另一个用户(John)撤销该特权：

```
/* User Joe */
GRANT SELECT ON Sample.Person TO Michael

/* User John */
REVOKE SELECT ON Sample.Person FROM Michael AS Joe
```

注意，John必须具有%All角色或%AdminSecure资源。

[#SQL #Caché](#)

源

URL:

<https://cn.community.intersystems.com/post/%E7%AC%AC%E5%85%AD%E5%8D%81%E5%85%AD%E7%AB%A0-sql%E5%91%BD%E4%BB%A4-revoke>