文章
姚 鑫 · 十月 16, 2021 阅读大约需 8 分钟

第四十七章 SQL命令 GRANT（一）

第四十七章 SQL命令 GRANT（一）

向用户或角色授予特权。

大纲

```
GRANT admin-privilege TO grantee [WITH ADMIN OPTION]

GRANT role TO grantee [WITH ADMIN OPTION]

GRANT object-privilege ON object-list TO grantee [WITH GRANT OPTION]

GRANT SELECT ON CUBE[S] object-list TO grantee [WITH GRANT OPTION]

GRANT column-privilege (column-list) ON table TO grantee  [WITH GRANT OPTION]
```

参数

- grantee - 一个或多个用户或角色的逗号分隔列表。
  有效值是用户列表、角色列表、“ * ” 或PUBLIC。
  星号(*)指定当前定义的所有没有% all角色的用户。
  PUBLIC关键字指定所有当前定义的和尚未定义的用户。
- admin-privilege - 被授予的管理级别特权或以逗号分隔的管理级别特权列表。
  该列表可由下列一项或多项按任何顺序组成:
  %CREATEMETHOD， %DROPMETHOD， %CREATEFUNCTION， %DROPFUNCTION，%CREATEPROCEDURE， %DROPPROCEDURE， %CREATEQUERY， %DROPQUERY，%CREATETABLE，%ALTERTABLE， %DROPTABLE，%CREATEVIEW，%ALTERVIEW，%DROPVIEW，%CREATETRIGGER，%DROPTRIGGER%DBOBJECTDEFINITION，授予上述所有16个权限。%NOCHECK，%NOINDEX，%NOLOCK，%NOTRIGGER用于INSERT,UPDATE和DELETE操作。
  %BUILDINDEX为BUILD INDEX命令授予特权。
- role - 被授予权限的角色或以逗号分隔的角色列表。
- object-privilege - 被授予的基本级别特权或以逗号分隔的基本级别特权列表。
  该列表可以包含以下一个或多个:%ALTER、DELETE、SELECT、INSERT、UPDATE、EXECUTE和REFERENCES。
  可以使用 “ all [privileges] ” 或 “ * ” 作为参数值授予所有表和视图特权。
  注意，只能授予多维数据集SELECT权限。
- object-list - 为其授予对象特权的一个或多个表、视图、存储过程或多维数据集的逗号分隔列表。
  可以使用SCHEMA关键字指定将对象特权授予指定模式中的所有对象。
  可以使用" * "指定将对象特权授予当前命名空间中的所有表或所有非隐藏的存储过程。
  注意，多维数据集对象列表需要CUBE(或cubes)关键字，并且只能被授予SELECT权限。
- column-privilege - 向一个或多个列出的列授予基本权限。
  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 - 包含列列表列的表或视图的名称。

描述

GRANT命令将对指定的表、视图、列或其他实体执行指定任务的权限授予一个或多个指定的用户或角色。
可以进行以下基本操作:

- 给用户授予特权。
- 为角色授予特权。
- 赋予用户角色。
- 将一个角色赋予另一个角色，创建角色的层次结构。

如果为某个用户赋予特权，则该用户可以立即行使该特权。
如果为角色授予权限，则已被授予该角色的用户可以立即使用该权限。
如果取消特权，用户将立即失去该特权。
一个用户实际上只被授予一次特权。
多个用户可以多次授予一个用户相同的权限，但单个REVOKE会删除该权限。

特权是基于每个名称空间授予的。

SQL特权只能通过ODBC、JDBC和动态SQL (%SQL. statement)强制执行。

因为GRANT准备和执行非常快，而且通常只运行一次，所以
IRIS不会在ODBC、JDBC或动态SQL中为GRANT创建缓存查询。
执行GRANT命令时，会执行*的扩展。

GRANT admin-privilege

SQL管理(admin)权限适用于用户或角色。
任何没有绑定到任何特定对象的特权(因此是该用户或角色的一般权限)都被认为是管理特权。
这些特权是根据当前名称空间的每个名称空间授予的。

%DBOBJECTDEFINITION权限授予所有16个数据定义权限。
它没有授予%BUILDINDEX、%NOCHECK、%NOINDEX、%NOLOCK和%NOTRIGGER权限，这些权限必须显式授予。

%BUILDINDEX特权授予使用BUILD INDEX命令。
%NOCHECK、%NOINDEX、%NOLOCK和%NOTRIGGER权限授予在INSERT、UPDATE、INSERT OR UPDATE或DELETE语句的约束子句中使用这些选项。
它们对使用%NOINDEX关键字作为谓词条件的前言没有影响。
因为TRUNCATE TABLE执行删除具有%NOTRIGGER行为的表中的所有行，所以必须拥有%NOTRIGGER权限才能运行TRUNCATE TABLE。
在准备INSERT、UPDATE、INSERT or UPDATE或DELETE语句时，必须具有适当的%NOCHECK、%NOINDEX、%NOLOCK或%NOTRIGGER权限才能使用该限制。

如果指定的管理特权不是有效的特权名称(例如，由于拼写错误)， IRIS将成功完成，并发出SQLCODE 100(到达数据末尾);
IRIS不检查指定的用户(或角色)是否存在。
如果指定的管理权限有效，但指定的用户(或角色)不存在， IRIS将发出SQLCODE -118错误。

GRANT role

这种形式的GRANT将用户分配给指定的角色。
还可以将一个角色分配给另一个角色。
如果接收分配的指定角色不存在 IRIS将发出SQLCODE 100(到达数据末尾)。
如果分配给角色的指定用户(或角色)不存在 IRIS将发出SQLCODE -118错误。

如果不是超级用户，并且正在尝试授予一个不拥有且没有ADMIN OPTION的角色， IRIS将发出SQLCODE -112错误。

使用CREATE ROLE语句创建角色。
如果角色名是分隔的标识符，则在分配时必须将其括在引号中。

角色可以通过SQL GRANT和REVOKE命令授予或撤销，也可以通 IRIS System Security:
- 进入管理界面，选择“ 系统管理 ”、“ 安全 ”、“ 用户 ”，显示当前用户。
选择所需用户的名称以显示该用户的编辑选项，然后选择Roles选项卡以将用户分配(或取消分配)到一个或多个角色。
- 进入“ 管理门户 ”界面，选择“ 系统管理 ”、“ 安全 ”、“ 角色 ”，显示当前角色。
选择所需角色的名称以显示该角色的编辑选项，然后选择Assigned to选项卡将该角色分配(或取消分配)给一个或多个角色。
注意，ObjectScript $ROLES特殊变量不显示授予角色的角色。

GRANT object-privilege

对象特权赋予用户或角色对特定对象的某些权限。
将对象列表上的对象特权授予被授予者。
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GRANT语句可以将多个对象上的多个对象特权授予多个用户和/或角色。

以下是可用的对象特权值:

- %ALTER和DELETE权限授予对表或视图定义的访问权。
- SELECT、INSERT、UPDATE、DELETE和REFERENCES权限授予对表数据的访问权限。
- EXECUTE特权授予对存储过程的访问权。
  执行存储过程或在查询中调用用户定义的SQL函数需要此特权。
  例如:SELECT Field1,MyFunc() FROM SQLUser。
  MyTable需要SQLUser上的SELECT权限。
  SQLUser上的MyTable和EXECUTE权限。
  MyFunc过程。
- ALL PRIVILEGES授予所有表和视图权限;
  它不授予EXECUTE权限。

可以使用星号(*)通配符作为对象列表值，将对象特权授予当前命名空间中的所有对象。
例如，GRANT SELECT ON * TO Deborah授予该用户对所有表和视图的SELECT权限。
GRANT EXECUTE ON * TO Deborah授予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，将对象特权授予当前命名空间中命名模式中的所有表、视图和存储过程。
例如，GRANT SELECT ON SCHEMA Sample TO Deborah为该用户授予Sample模式中所有对象的SELECT权限。
这包括将来将在该模式中定义的所有对象。
可以将多个模式指定为逗号分隔的列表;
例如，GRANT SELECT ON SCHEMA Sample,Cinema TO Deborah授予Sample和Cinema模式中所有对象的SELECT权限。

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。
只能向多维数据集授予SELECT权限。

下面的示例演示了如何为特定表的特定用户授予SELECT和UPDATE权限:

```
ClassMethod Grant()
{
    d $SYSTEM.Security.Login("_SYSTEM","SYS")
```

```
CreateUser
    s x = $SYSTEM.SQL.UserExists("DeborahTest")
    if x = 0 {
        &sql(
            CREATE USER DeborahTest IDENTIFY BY birdpw
        )
        if SQLCODE '= 0 {
            WRITE "??????: ",SQLCODE,!
            q
        }
    } else {
        w "??DeborahTest??????????",!
        q
    }
GrantPrivsToUser
    &sql(
        GRANT SELECT,UPDATE ON SQLUSER.T1 TO DeborahTest
    )
    w !,"GRANT ????: ",SQLCODE
DropUser
    &sql(
        DROP USER DeborahTest
    )
    if SQLCODE '= 0 {
        w "DROP USER error: ",SQLCODE,!
    }
}
```

权限只能显式授予已经存在的表、视图或存储过程。
如果指定的对象不存在，IRIS将发出SQLCODE -30错误。
但是，可以向一个模式授予特权，该模式将特权授予该模式中所有现有的对象，以及在授予特权时该模式中不存在的所有未来对象。

如果表的所有者是PUBLIC，则用户访问表不需要被授予对象权限。

如果指定的用户不存在， IRIS将发出SQLCODE -118错误。
如果已经授予了指定的对象特权， IRIS将发出SQLCODE 100(到达数据末尾)。

对象权限可以通过以下方式授予或撤销:

- GRANT和REVOKE命令。
- $SYSTEM.SQL.Security.GrantPrivileve()和$SYSTEM.SQL.Security.RevokePrivileve()方法。这些方法返回%Status值并设置SQLCODE变量。与任何方法或函数一样，始终首先测试返回值：
    - 如果%status=1且SQLCODE=0：特权被授予或撤销。
    - 如果%status=1且SQLCODE=100：未授予或撤消任何特权，因为它已被授予或撤消。
    - 如果%status不是1，则不设置SQLCODE并且可能未定义：由于方法错误，未授予或撤消任何特权。%Status包含指示失败类型的SQLCODE：ObjPriv：SQLCODE-60表示无效特权；ObjList：指定对象类型的ObjList对象不存在：SQLCODE-30、-187、-428或-473；类型：SQLCODE-400应为表、视图、多维数据集、架构或存储过程的对象类型；用户：SQLCODE-118未知或非唯一的用户或角色。
- 通过IRIS系统安全。转到管理门户，依次选择System Administration、Security、Users(或System Administration、Security、Roles)，选择所需用户或角色的名称，然后选择SQL Tables或SQL Views选项卡。从下拉列表中选择所需的命名空间。然后选择Add Tables或Add Views按钮。在显示的窗口中，选择方案，选择一个或多个表，然后分配权限。

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权限。可以通过调用$SYSTEM.SQL.Security.CheckPrivileve()方法来确定指定用户是否具有指定的表级对象权限，如下例所示：

```
   WRITE "SELECT privilege? ",$SYSTEM.SQL.Security.CheckPrivilege("DeborahTest","1,SQ
LUSER.TestT1","s"),!
   WRITE "UPDATE privilege? ",$SYSTEM.SQL.Security.CheckPrivilege("DeborahTest","1,SQ
LUSER.TestT1","u"),!
   WRITE "DELETE privilege? ",$SYSTEM.SQL.Security.CheckPrivilege("DeborahTest","1,SQ
LUSER.TestT1","d"),!
```

对象所有者权限

表、视图或过程的所有者始终隐式拥有SQL对象的所有SQL特权。该对象的所有者在该对象映射到的所有名称空间中拥有该对象的特权。

#SQL #Caché

源URL: https://cn.community.intersystems.com/post/%E7%AC%AC%E5%9B%9B%E5%8D%81%E4%B8%83%E7%AB%A0-sql%E5%91%BD%E4%BB%A4-grant%EF%BC%88%E4%B8%80%EF%BC%89