管理：用户管理和安全

SAP Sybase IQ 16.0 SP03

文档 ID： DC02016-01-1603-01
最后修订日期： 2013 年 12 月

目录

安全管理

SAP® Sybase® IQ 提供一种基于角色的安全模型，用于控制对数据库对象的访问及用于执行特许操作。此模型为要授予用户的特权提供完全控制和细分。数据库中的每项特许操作都要求将一项或多项系统特权或对象级特权分配给用户，以便执行操作。

*系统特权*允许用户执行授权数据库任务。例如，为用户分配 CREATE TABLE 系统特权，以允许其创建自有表。

*对象级特权*允许用户对指定对象执行授权任务。例如，为用户分配 `TableA` 的 ALTER 对象级特权可允许其改动此表，但不允许改动其它表。

*角色*是一个或多个系统特权、对象级特权和其它角色的集合。为用户授予角色等同于为该用户授予该角色的基础系统特权和对象级特权。

所有新用户均自动被授予 PUBLIC 系统角色，该角色会使用户具有以下权限：

- 查看存储在系统视图中的数据
- 执行大多数系统存储过程

一旦创建一个新用户，您可以：

- 向其授予用户定义的角色、系统角色、系统特权和对象级特权。
- 为其指派登录策略。缺省情况下,将向用户指派根登录策略。
- 将其设置为发布者或数据库的远程用户（在 SQL 远程系统中使用）。

在每个新的或迁移的 SAP Sybase IQ 数据库中都包括一组可用于入门的预定义角色。以这些系统角色为起点来实施基于角色的安全性。

注意： 如果您使用的是 16.0 之前版本的 SAP Sybase IQ，SAP 建议您在与您操作系统相对应的《迁移》指南的“Upgrading to Role-Based Security”中查阅有关安全模型是如何从授权/权限/组模型改为角色/特权/用户扩展角色模型的章节。

计划和实施基于角色的安全

用于计划和实施基于角色的安全模型的工作流是一个完全不同的工作流。

设计安全层次

1. 标识用户要执行的各种授权任务。分组密切相关的任务。可根据任意组织结构（部门、职能等）进行分组。您可创建一个与组织层次相匹配的角色层次。为每个分组指派一个名称。这些分组表示您所创建的*角色*。
2. 对执行每个已标识授权任务所需的*系统特权*和*对象级特权*进行标识。

3. 对执行各种授权任务的*用户*进行标识。将这些用户与适当角色或已标识的单个任务相关联。
4. （可选）标识所创建角色的管理员。管理员可向其他用户授予此角色及从其他用户中撤消此角色。
5. （可选）标识不属于所创建角色的系统特权和对象级特权的管理员。

构建安全层次

1. 创建所需角色。请参见角色。
2. 为每个角色授予系统特权。请参见角色和特权。
3. 创建用户。请参见用户。
4. 向每个用户授予适当角色，包括适用时授予管理权限。请参见角色。
5. 向用户授予适当的对象级特权和系统特权（已通过角色间接授予的特权除外），包括适用时授予管理权限。请参见特权。

另请参见

- 角色 （第 2 页）
- 特权 （第 28 页）
- 用户 （第 99 页）

角色

角色是一个容器，其中包含有系统特权、对象级特权和角色。授予和撤消角色特权与授予和撤消用户特权是相同的。角色和用户不能同名。

用户定义的角色

用户定义的角色是系统特权和对象级特权的自定义集合，通常为将与特定任务或一组任务相关的特权集中到一起而创建。

用户定义的角色：

- 可以是没有登录特权但拥有对象的独立角色。
- 可以是能够充当角色（用户扩展角色）的数据库用户。如果现有用户 ID 具有登录特权，则用户扩展角色将保留登录特权。
- 可以授予对其他对象的特权。
- 可以授予对其他角色的特权。
- 名称不区分大小写。

用户定义角色的授权在语义上等同于分别授予每个基础系统特权和对象级特权。

不能将用户定义角色转换为用户扩展角色，反之亦然。

注意： 除非另行说明，否则术语*用户定义角色*既指用户扩展角色又指用户定义角色。

创建用户定义的角色

新建用户定义的角色。

前提条件

MANAGE ROLES 系统特权。

过程

用户定义的角色不能拥有登录口令。创建用户定义的角色时，可以指定角色的管理员，并指明管理员是否也将成为角色成员。如果未指定任何管理员，全局角色管理员(被授予 MANAGE ROLES 系统特权的任何用户）将成为角色的缺省管理员。

但如果在角色创建期间至少指定一个角色管理员，全局角色管理员无法管理角色，因为系统不会自动向角色授予 SYS_MANAGE_ROLES_ROLE 系统特权和管理权限。因此，SAP 强烈建议您在创建角色时不要定义任何角色管理员（而是在创建之后添加），或者在创建过程中显式授予 SYS_MANAGE_ROLES_ROLE 系统特权，同时仅授予管理权限以及任何角色管理员。

可在创建角色后添加和删除角色管理员。如果试图使用现有角色名称创建新角色，该语句将失败。

要新建用户定义的角色，请执行下列语句之一：

创建条件	语句
只有全局角色管理员； 无角色管理员	**CREATE ROLE** *role_name*
角色管理员无角色成员资格； 无全局角色管理员	**CREATE ROLE** *role_name* **WITH ADMIN ONLY** *admin_name [,...]*
角色管理员具有角色成员资格； 无全局角色管理员*	**CREATE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]*
角色管理员无角色成员资格； 有全局角色管理员*	**CREATE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE**, *admin_name [,...]*

*由于无法为全局角色管理员授予角色成员资格，因此，如果在创建角色时为角色管理员授予角色成员资格（使用 WITH ADMIN OPTION 子句），则管理员列表中不能包含 SYS_MANAGE_ROLES_ROLE。但是，如果在创建角色时没有为角色管理员授予角色成员资格（使用 WITH ADMIN ONLY OPTION 子句），则可将其包含在管理员列表中。

示例：

此语句创建角色 Sales，并且未指定任何角色管理员。任何具有 MANAGE ROLES 系统特权的用户都是此角色的缺省管理员。

```
CREATE ROLE Sales
```

此语句创建角色 Marketing，并且 *Jane* 和 *Bob* 充当角色管理员，但未向这些管理员授予角色成员资格。该语句还允许全局角色管理员管理角色。

```
CREATE ROLE Marketing WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE, Jane,
Bob
```

另请参见

- 角色和全局角色管理员 （第 9 页）
- CREATE ROLE 语句 （第 231 页）

将现有用户转换为用户扩展角色

可对现有用户 ID 进行扩展，使其用作角色。如果某个用户被指派有一组系统特权和对象级特权，而您想将这组系统特权和对象级特权授予其他用户，则进行此操作将非常有用。

前提条件

MANAGE ROLES 系统特权。

过程

如果现有 ID 具有登录特权，则用户扩展角色将保留登录特权。

将用户转换为角色时，可以指定角色的管理员，并指明管理员是否也将成为角色成员。如果未指定任何管理员，全局角色管理员（被授予 MANAGE ROLES 系统特权的任何用户）将成为角色的缺省管理员。

但如果在转换期间至少指定一个角色管理员，全局角色管理员无法管理角色，因为系统不会自动向角色授予 SYS_MANAGE_ROLES_ROLE 系统特权和管理权限。因此，SAP 强烈建议您在创建角色时不要定义任何角色管理员（而是在创建之后添加），或者在创建过程中显式授予 SYS_MANAGE_ROLES_ROLE 系统特权，同时仅授予管理权限以及任何角色管理员。

可在转换用户后添加和删除角色管理员。如果您试图用不存在的用户 ID 转换用户，该语句将失败。

要转换现有用户，请执行下列语句之一：

转换条件	语句
只有全局角色管理员； 无角色管理员	**CREATE ROLE FOR USER** *userID*
角色管理员无角色成员资格； 无全局角色管理员	**CREATE ROLE FOR USER** *userID* **WITH ADMIN ONLY** *admin_name [,...]*
角色管理员具有角色成员资格； 无全局角色管理员*	**CREATE ROLE FOR USER** *userID* **WITH ADMIN** *admin_name [,...]*
角色管理员无角色成员资格； 全局角色管理员*	**CREATE ROLE FOR USER** *userID* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE**, *admin_name [,...]*

*由于无法为全局角色管理员授予角色成员资格，因此，如果在创建角色时为角色管理员授予角色成员资格（使用 WITH ADMIN OPTION 子句），则管理员列表中不能包含 SYS_MANAGE_ROLES_ROLE。但是，如果在创建角色时没有为角色管理员授予角色成员资格（使用 WITH ADMIN ONLY OPTION 子句），则可将其包含在管理员列表中。

示例：

以下语句将用户 `Sales1` 扩展为角色。由于未指定任何角色管理员，因此，任何具有 MANAGE ROLES 系统特权的用户都可管理该角色。

```
CREATE ROLE FOR USER Sales1
```

以下语句将用户 `Marketing1` 扩展为角色，其中 *Jane* 和 *Bob* 充当角色管理员。该语句还允许全局角色管理员管理角色。

```
CREATE ROLE FOR USER Marketing1 WITH ADMIN ONLY
SYS_MANAGE_ROLES_ROLE, Jane, Bob
```

另请参见

- 角色和全局角色管理员 （第 9 页）
- CREATE ROLE 语句 （第 231 页）

将用户扩展角色转换回用户

可以将用户扩展角色转换回常规用户。

前提条件

具有对要转换的用户扩展角色的管理权限。

过程

该用户会保留授予用户扩展角色的所有登录特权、系统特权及角色。该用户仍然是其扩展为角色后所创建的对象的所有者。可以立即撤消用户扩展角色的任意成员。

无论何时，都必须分别针对每个角色指定最小数量（由 **MIN_ROLE_ADMINS** 数据库选项定义）的具有登录口令的角色或全局角色管理员。将用户扩展角色转换回用户时，所有用户扩展角色的相关角色都必须继续满足该最低要求，否则转换将失败。

要将用户扩展角色转换回用户，请执行下列语句之一：

转换条件	语句
未将角色 授予任何成员。	**DROP ROLE FROM USER** *role_name*
已将角色 授予成员。	**DROP ROLE FROM USER** *role_name* **WITH REVOKE**

向用户或角色添加用户定义的角色

向用户或角色（被授予者）添加用户定义的角色成员资格，同时授予或不授予管理权限。

前提条件

对所授予角色的管理特权。

过程

可为用户定义角色授予管理权限，也可以不授予管理权限。如果授予管理权限（即使用 WITH ADMIN OPTION 子句），则用户可以管理（授予、撤消和删除）角色，也可以使用该角色的所有基础系统特权和对象级特权。如果仅授予管理权限（使用 WITH ADMIN ONLY OPTION 子句），则用户可以管理该角色，但不能使用该角色的基础系统特权和对象级特权。如果不授予任何管理权限，则用户可以使用该角色的基础系统特权和对象级特权，但不能管理该角色。

向用户授予角色成员资格时，用户将继承该角色的所有基础系统特权和角色，其中包括对表、视图和过程的所有对象级权限。

将角色授予另一角色时，被授予的角色（子角色）的所有成员将自动成为接收角色（父角色）的成员，并继承父角色的所有基础系统特权和角色，其中包括对表、视图和过程的所有权限。父角色的现有成员不会成为子角色的成员，也不会继承其任何基础系统特权和角色。

要向被授予者授予用户定义的角色，请执行下列语句之一：

授予类型	语句
角色成员资格 以及对角色的全部 管理权限	**GRANT ROLE** *role_name* **TO** *grantee [,...]* **WITH ADMIN OPTION**
仅对角色的 管理权限	**GRANT ROLE** *role_name* **TO** *grantee [,...]* **WITH ADMIN ONLY OPTION**
角色成员资格， 但不授予对角色的 管理权限	**GRANT ROLE** *role_name* **TO** *grantee [,...]* **WITH NO ADMIN OPTION**

示例：

- 存在三个用户：User1、User2、User3。
- 存在四个角色：Role1、Role2、Role3、Role4。
- 存在两种系统特权：Priv1、Priv2。
- 向 Role1 授予 Priv1 和 Role3。
- User2 和 User3 是 Role1 的成员。
- 向 Role2 授予 Priv1 和 Role4。
- User3 是 Role2 的成员。

执行以下语句：

```
GRANT ROLE Role1 TO User1 WITH ADMIN OPTION
```

User1 成为 Role1 的成员。

作为 Role1 的成员，User1 继承 Priv1 并从 Role3（间接）继承所有系统特权和角色。

User1 也可以管理 Role1。

执行以下语句：

```
GRANT ROLE Role2 TO Role1 WITH ADMIN OPTION
```

Role1 成为 Role2 的成员。

作为 Role1 的成员，User2、User3 和 User1（来自先前的授予）从 Role2 继承下列内容：Priv2 以及 Role4 的所有系统特权和角色（间接继承）。

作为 Role2 的成员，User3 不会成为 Role1 的成员，不会继承 Role1 的任何系统特权或角色。

User1、User2 和 User3 可以管理 Role2。

另请参见

- GRANT ROLE 语句 （第 247 页）

从用户定义的角色中删除成员

删除作为角色成员的用户或角色。用户或角色无法使用某角色的任何基础系统特权或角色，并且无法管理该角色（如果被授予了管理权限）。

前提条件

对所管理角色的管理特权。

过程

无论何时，都必须分别针对每个角色指定最小数量（由 **MIN_ROLE_ADMINS** 数据库选项定义）的具有登录口令的角色或全局角色管理员。如果该成员是角色的管理员并且删除该成员将违反最低要求，则删除操作将失败。
要删除被授予者的用户定义的角色成员资格，请执行下列语句之一：

撤消类型	语句
角色成员资格和 对角色的所有管理权限	**REVOKE ROLE** *role_name* **FROM** *grantee [,...]*
仅对角色的 管理权限	**REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *grantee [,...]*

另请参见

- REVOKE ROLE 语句 （第 264 页）

删除用户定义的角色

从数据库中删除用户定义的角色，前提是所有相关角色可以保持具有活动口令的管理员用户的最低要求数量。如果未保持该最小值，命令将失败。

前提条件

- 对待删除角色的管理特权。
- 如果待删除角色是用户定义的角色，则该角色没有任何对象。

过程

如果将用户扩展角色转换回用户，则不删除所拥有的对象；转换后的用户仍拥有这些对象。

待删除角色的类型以及该角色是否已被授予用户决定着 DROP 语句所需的子句。

- **FROM USER** – 删除用户扩展角色时需要。
- **WITH REVOKE** – 删除已被授予多个用户和角色的角色时需要。

要删除用户定义的角色，请执行下列语句之一：

删除条件	语句
尚未向用户定义的角色 授予任何成员。	**DROP ROLE** *role_name*
用户扩展的角色 已被授予成员。	**DROP ROLE** *role_name* **WITH REVOKE**
用户扩展的角色 尚未被授予任何成员*。	**DROP ROLE FROM USER** *role_name*
用户扩展的角色 已被授予成员*。	**DROP ROLE FROM USER** *role_name* **WITH REVOKE**

*用户扩展的角色成为常规用户。

另请参见

- DROP ROLE 语句 （第 237 页）

角色和全局角色管理员

角色管理员 和 *全局角色管理员* 可将用户定义角色授予用户和其他角色，还可撤消用户和其他角色的用户定义角色。您可以根据需要添加和删除角色及全局角色管理员。

可以授予单个角色的角色管理员没有最大数目限制。但有最小数目限制，这由可配置的 **MIN_ROLE_ADMINS** 数据库选项指定。首先会校验是否满足此最小数目要求，然后才能撤消角色的角色管理员或全局角色管理员。角色管理员的最小数目可设置为 1（缺省值）到 10 之间的任意值。

角色管理员可以是用户、用户扩展角色或用户定义角色。

全局角色管理员包括被授予 MANAGE ROLES 系统特权的用户。全局角色管理员可以管理被授予 SYS_MANAGE_ROLES_ROLE 系统特权和管理权限的任意角色。

角色和全局角色管理员都可以授予、撤消和删除角色，并且可以向角色添加角色和全局角色管理员或者从角色删除角色和全局角色管理员。角色管理员可以是用户或角色，不需要 MANAGE ROLES 系统特权即可管理角色。

可以在创建角色的过程中或者在创建完成后指定角色管理员，并指明角色管理员是否也将成为角色成员。如果未指定任何管理员，全局角色管理员将在缺省情况下成为该角色的管理员。

如果在角色创建期间至少指定一个角色管理员，全局角色管理员无法管理角色，因为系统不会自动向角色授予 SYS_MANAGE_ROLES_ROLE 系统特权和管理权限。因此，SAP 强烈建议您在创建角色时不要定义任何角色管理员（而是在创建之后添加），或者在创建过程中显式授予 SYS_MANAGE_ROLES_ROLE 系统特权，同时仅授予管理权限以及任何角色管理员。

如果在创建角色时未指定角色管理员，系统将自动向角色授予全局角色管理员（SYS_MANAGE_ROLES_ROLE 系统特权），同时仅授予管理权限。

如果最初创建角色时未指定角色管理员，角色管理员是后添加的，则全局角色管理员（SYS_MANAGE_ROLES_ROLE 系统特权）是否会遭到删除取决于角色管理员的添加方式。如果使用 **GRANT** 语句，仍会向角色授予 SYS_MANAGE_ROLES_ROLE 系统特权。但是，如果使用 **CREATE OR REPLACE** 语句，并且角色管理员的新列表中未显式包含 SYS_MANAGE_ROLES_ROLE 系统特权，则该系统特权将被删除。

注意： 如果从角色中删除 SYS_MANAGE_ROLES_ROLE 系统特权将导致不满足所定义的最小角色管理员数目，则无法从角色中删除此系统特权。

缺省情况下，SYS_MANAGE_ROLES_ROLE 系统特权不会被授予兼容性角色 (SYS_AUTH_*_ROLE)。因此，为了让全局角色管理员能够管理兼容性角色，必须向角色显式授予 SYS_MANAGE_ROLES_ROLE，同时仅授予管理权限。

创建角色时添加角色管理员
新建角色时指定角色管理员。

前提条件
MANAGE ROLES 系统特权。

过程
如果在创建角色时至少指定一个角色管理员，那么除非显式指定，否则全局角色管理员将无法管理该角色。

因此，SAP 强烈建议您始终考虑将全局角色管理员添加到角色管理员列表中。
要在创建过程中添加角色管理员，请执行下列语句之一：

创建类型	语句
只有管理权限； 无角色成员资格	**CREATE ROLE** *role_name* **WITH ADMIN ONLY** *admin_name [,...]*
授予的角色和全局角色管理员 只有管理权限；无角色成员资格*	**CREATE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE,** *admin_name [,...]*

创建类型	语句
管理权限和 角色成员资格	**CREATE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]*

*由于无法为全局角色管理员授予角色成员资格，因此，如果在创建角色时为角色管理员授予角色成员资格（使用 WITH ADMIN OPTION 子句），则管理员列表中不能包含 SYS_MANAGE_ROLES_ROLE。

示例：

执行以下语句可以使 `Joe` 和 `Bob` 成为 `Sales` 角色的角色管理员：

```
CREATE ROLE Sales WITH ADMIN Joe, Bob
```

由于使用 WITH ADMIN 子句，因此 `Joe` 和 `Bob` 都可以授予和撤消角色，也可以使用角色的基础系统特权。如果使用 WITH ADMIN ONLY 子句，则 `Joe` 和 `Bob` 将只能授予和撤消角色。

执行以下语句可以使 `Joe` 和 `Bob` 成为 `Sales` 角色的角色管理员，并且允许全局角色管理员管理该角色：

```
CREATE ROLE Sales WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE, Joe, Bob
```

另请参见

- CREATE ROLE 语句 （第 231 页）

创建角色时添加全局角色管理员

允许全局角色管理员管理新角色。

前提条件

MANAGE ROLES 系统特权。

过程

如果在创建角色时至少指定一个角色管理员，那么除非显式指定，否则全局角色管理员将无法管理该角色。

因此，SAP 强烈建议您始终考虑将全局角色管理员添加到角色管理员列表中。

要在创建过程中添加全局角色管理员，请执行下列语句之一：

创建类型	语句
只有全局角色管理员； 无角色管理员	**CREATE ROLE** *role_name*

创建类型	语句
角色管理员和全局角色管理员*	**CREATE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE**, *admin_name [,...]*

*全局角色管理员只能具有角色的管理权限 (WITH ADMIN ONLY)。因此，如果在创建角色时指定角色管理员和全局角色管理员，只有 WITH ADMIN ONLY 子句有效。

示例：

执行以下语句创建 `Sales` 角色，并只允许全局角色管理员来管理该角色：

```
CREATE ROLE Sales
```

执行以下语句使 `Joe` 和 `Bob` 成为角色 `Sales` 的角色管理员，同时仅授予管理权限，从而也允许全局角色管理员管理该角色：

```
CREATE ROLE Sales WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE, Joe, Bob
```

向现有角色添加角色管理员

向现有角色添加角色管理员。可以授予单个角色的角色管理员没有最大数目限制。

前提条件

如果角色具有全局角色管理员，则需要对角色具有管理特权或具有 MANAGE ROLES 系统特权。

过程

要添加角色管理员，请执行下列语句之一：

授予类型	语句
只有管理特权	**GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN ONLY OPTION**
管理特权 和角色成员资格	**GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN OPTION**

示例：

执行以下语句可以使 `Mary` 和 `Bob` 成为 `Sales` 角色的角色管理员。

```
GRANT ROLE Sales TO Mary, Bob WITH ADMIN ONLY OPTION
```

因为使用 WITH ADMIN ONLY OPTION 子句，任何用户都可以管理该角色，但不能使用该角色的基础系统特权。

执行以下语句可以使 Sarah 成为 Sales 角色的角色管理员，由于使用 WITH ADMIN OPTION 子句，还可以管理该角色并使用该角色的基础系统特权。

```
GRANT ROLE Sales TO Sarah WITH ADMIN OPTION
```

另请参见

- GRANT ROLE 语句 （第 247 页）

向现有角色添加全局角色管理员

向现有角色添加全局角色管理员。

前提条件

对角色的管理特权。

过程

可以向角色授予全局角色管理员，同时仅授予管理权限（WITH ADMIN ONLY OPTION 子句）。

要恢复角色的全局角色管理员，请执行：

```
GRANT ROLE role_name TO SYS_MANAGE_ROLES_ROLE
WITH ADMIN ONLY OPTION
```

另请参见

- GRANT ROLE 语句 （第 247 页）

使用户或角色成为全局角色管理员

允许用户或角色充当全局角色管理员。

前提条件

已授予 MANAGE ROLES 系统特权以及管理权限。

过程

要成为全局角色管理员，必须为您授予 MANAGE ROLES 系统特权。充当全局角色管理员不需要对 MANAGE ROLES 系统特权具有管理权限。如果将 MANAGE ROLES 系统特权授予某角色，该角色的所有成员都将继承此系统特权，因此，可以充当全局角色管理员。

要授予 MANAGE ROLES 系统特权，请执行以下语句：

```
GRANT MANAGE ROLES TO grantee [,...]
```

另请参见

- GRANT 系统特权语句 （第 254 页）

替换角色的现有角色管理员
以新管理员替换现有角色管理员。

前提条件
如果角色具有全局角色管理员，则需要对角色具有管理特权或具有 MANAGE ROLES 系统特权。

过程
替换角色管理员会涉及到更改能够充当管理员的用户和角色及其对角色具有的管理权限级别。根据替换范围的不同，可分别采用以下两种方法。每种方法对角色和全局管理员的实际影响是不同的。第一种方法允许您有选择地替换现有角色的管理员。第二种方法允许您完全替换所有现有角色的管理员。使用第二种方法还包括替换全局角色管理员。

第一种方法分为两个步骤：添加新的角色管理员，然后从角色中移除现有管理员。整个过程中必须始终满足管理员的最低数量要求；因此，SAP 建议您在移除现有管理员之前添加新的管理员。如果角色具有全局角色管理员，将会予以保留，除非将其显式移除。

第二种方法只有一个步骤，但影响范围更大：定义角色管理员的新列表。所有现有角色管理员将被新的角色管理员覆盖。如果需要继续保留任何当前角色管理员，必须将其加入到替换角色管理员列表中。该列表将替换所有现有管理员，具体行为如下：

- 所有被授予 WITH ADMIN OPTION 而未包含在新角色管理员列表中的现有角色管理员将成为没有管理权限的角色的成员。
- 所有被授予 WITH ADMIN ONLY OPTION 而未包含在新角色管理员列表中的现有角色管理员将作为角色的成员被移除。
- 如果新角色管理员列表中包含的某个现有角色管理员的原始管理权限高于替换权限，则保留其原始管理权限。例如，新角色管理员被授予 WITH ADMIN ONLY 权限。最初被授予具有 WITH ADMIN 权限的角色并包括在新列表中的 `User1` 保留较高的 WITH ADMIN 权限。
- 如果角色具有全局角色管理员，那么除非您将其显式包括在新角色管理员列表中，否则会将其从角色中移除。
- 如果为新的角色管理员授予了 WITH ADMIN 权限，那么现有全局角色管理员不能包括在列表中，原因是不能为其授予 WITH ADMIN 权限。全局角色管理员会从角色中移除。

只要替换管理选项大于等于当前级别，便可发出替换角色命令。要降低管理级别，必须从角色中移除（撤消）所有角色管理员，然后再重新授予。

无论何时，都必须分别针对每个角色指定最小数量（由 **MIN_ROLE_ADMINS** 数据库选项定义）的具有登录口令的角色或全局角色管理员。替换角色管理员时，如果替换管理员的数量违反了保留最低数量管理员的要求，替换操作将失败。

要替换角色管理员，请执行下列语句之一：

替换选项	语句
替换所选角色管理员 (只具有管理权限， 无角色成员资格)	• **GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN ONLY OPTION** • **REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *admin_name [,...]*
替换所选角色管理员 (具有管理权限和角色成员资格)	• **GRANT ROLE** *role_name* **TO** *admin_name [,...]* **WITH ADMIN OPTION** • **REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *admin_name [,...]*
替换所有角色管理员 (只具有管理权限，无角色成员资格）。 移除全局角色管理员（如存在）。	**CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN ONLY** *admin_name [,...]*
替换所有角色管理员 (具有管理权限和角色成员资格）。 移除全局角色管理员（如存在）。	**CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]*
替换所有角色管理员 管理权限) 其中包括全局角色管理员。*	**CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN ONLY SYS_MANAGE_ROLES_ROLE**, *admin_name [,...]*
替换所有角色管理员 (具有全部管理权限）。 恢复角色的全局角色管理员*	• **CREATE OR REPLACE ROLE** *role_name* **WITH ADMIN** *admin_name [,...]* • **GRANT ROLE** *role_name* **TO SYS_MANAGE_ROLES_ROLE** **WITH ADMIN ONLY OPTION**

*只能使用 WITH ADMIN ONLY OPTION 子句向角色授予 SYS_MANAGE_ROLES_ROLE。因此，当 CREATE OR REPLACE 语句包括 WITH ADMIN ONLY OPTION 子句时，SYS_MANAGE_ROLES_ROLE 可包括在管理员列表中。当 CREATE OR REPLACE 语句使用 WITH ADMIN OPTION 子句时，必须使用 WITH ADMIN ONLY OPTION 子句发出单独的 grant 语句来向角色授予 SYS_MANAGE_ROLES_ROLE。

示例：

`Sales` 有 `Mary` 和 `Bob` 这两个拥有全部管理权限的角色管理员。`Sales` 还有一个全局角色管理员。

执行以下语句移除 Bob 的角色管理员身份并将其替换为 Sarah 和 Jeff，这二人具有与其相同的管理权限。Bob 仍为 Sales 的成员，但不具有管理权限。

```
GRANT ROLE sales TO Sarah, Jeff WITH ADMIN OPTION
REVOKE ADMIN OPTION FOR ROLE Sales FROM Bob
```

执行以下语句，用具有全部管理权限的 Sarah 和 Jeff，替换现有角色管理员（Mary 和 Bob）。由于全局角色管理员不能包括在列表中（原因是不能为其授予全部管理权限），因此必须在替换角色管理员之后，重新为角色显式授予全局角色管理员。

```
CREATE OR REPLACE ROLE Sales WITH ADMIN Sarah, Jeff
GRANT ROLE sales TO SYS_MANAGE_ROLES_ROLE WITH ADMIN ONLY OPTION
```

执行以下语句，用只具有管理权限的 Bob 和 Sarah 替换现有角色管理员（Mary 和 Bob）。要保留全局角色管理员，必须将其加入到列表中。由于 Bob 仍为角色管理员并且原始管理权限高于新的角色管理员，因此他将保留较高的原始管理权限。

```
CREATE OR REPLACE ROLE Sales WITH ADMIN ONLY Bob, Sarah,
SYS_MANAGE_ROLES_ROLE
```

另请参见

- GRANT ROLE 语句 （第 247 页）
- REVOKE ROLE 语句 （第 264 页）
- CREATE ROLE 语句 （第 231 页）

从角色中删除角色管理员

从角色中删除角色管理员。

前提条件

对角色的管理特权。

过程

无论何时，都必须分别针对每个角色指定最小数量（由 **MIN_ROLE_ADMINS** 数据库选项定义）的具有登录口令的角色或全局角色管理员。只要在删除角色管理员后仍能满足最小数目，便可将其删除。

删除角色管理员时，如果最初是使用 WITH ADMIN OPTION 子句向用户授予角色管理权限，则撤消角色管理权限将仅删除其管理角色（授予、撤消、删除）的权限，而不会删除使用角色基础系统特权的权限（成员资格）。但是，如果最初是使用 WITH ADMIN ONLY OPTION 子句向用户授予角色管理权限，则撤消角色管理权限与完全撤消角色的结果相同，因为不存在与角色关联的成员资格。

要从角色中移除角色管理员，请执行下列语句之一：

移除类型	语句
移除角色管理员， 但保留角色中的成员资格。	**REVOKE ADMIN OPTION FOR ROLE** *role_name* **FROM** *admin_name [,...]*
移除角色管理员 以及角色中的成员资格。	**REVOKE ROLE** *role_name* **FROM** *admin_name [,...]*

示例：

本示例假设 Mary 和 Sarah 当前均为 Sales 角色的角色管理员。Mary 已被授予角色中的成员资格和管理角色的权限。但却仅授予 Sarah 管理角色的权限，并未授予其成员资格。由于授予的管理级别不同，执行此语句撤消 Sales 角色的管理权限对每位管理员的影响也有所区别：

```
REVOKE ADMIN OPTION FOR ROLE Sales FROM Mary, Sarah
```

此语句将导致 Mary's 失去管理 Sales 角色的权限，但保留其角色的成员资格。它将彻底删除 Sarah 的 Sales 角色。

另请参见

- REVOKE ROLE 语句 （第 264 页）

从角色中删除全局角色管理员

从角色中删除全局角色管理员。

前提条件

对角色的管理特权。

过程

无论何时，都必须分别针对每个角色指定最小数量（由 **MIN_ROLE_ADMINS** 数据库选项定义）的具有登录口令的角色或全局角色管理员。只要仍能满足角色的最小数目，便可从角色中删除全局角色管理员。

要从角色中删除全局角色管理员，请执行：

```
REVOKE ROLE role_name
FROM SYS_MANAGE_ROLES_ROLE
```

另请参见

- REVOKE ROLE 语句 （第 264 页）

最小角色管理员数

MIN_ROLE_ADMINS 数据库选项的值是可配置的，该值可确保避免这样一种情况，即剩余的用户或角色都不具有足够的系统特权来管理其余用户和角色。

该值是指每个角色的最小角色管理员数，而不是所有角色的最小角色管理员数；但在以下情况下则视为所有角色的最小角色管理员数：

- 创建或撤消角色
- 删除用户或角色
- 将用户口令更改为空值

注意： 不具有口令的用户或角色不能成为管理员。

尝试更改此值时，系统会验证现有的每个角色是否仍至少具有新值所定义的相同角色管理员数。即使有一个角色不满足此要求，该语句就会失败。同样，在删除用户时，如果剩余管理员数降到指定的最小值以下，该语句将失败。

注意： 计算角色的管理员数量时，不考虑锁定的帐户。

示例 1

MIN_ROLE_ADMINS 值为 2

`Role1` 有两个管理员，而 `Role2` 有三个管理员。

如果将该值减少到 1，则命令成功，因为这两个角色仍具有新指定的最小角色管理员数。但如果将该值增加到 3，则命令失败，因为 `Role1` 具有的管理员数不足，不能满足新的最小值。

示例 2

MIN_ROLE_ADMINS 值为 4

`Role1` 有六个管理员，而 `Role2` 有四个管理员。

如果从 `Role1` 中删除一位用户，则命令成功，因为 `Role1` 具有的管理员数仍满足最小值。但如果从 `Role2` 中删除一位用户，则命令失败，因为 `Role2` 具有的管理员数不足，无法满足最小值。

另请参见

- 用户帐户自动解锁 （第 106 页）
- MIN_ROLE_ADMINS 选项 （第 281 页）

设置最小角色管理员数

设置管理每个角色所需的最小角色管理员数。

前提条件

SET ANY SECURITY OPTION 系统特权。

过程

最小角色管理员数是一个可配置的数据库选项，您可以将其设置为 1（缺省值）到 10 之间的任意整数。您无法更改该值，一旦更改，则任一角色的角色管理员数量将与新的最小值不一致。您也无法临时设置该选项。

该值针对每个角色，而并非所有角色总计。例如，如果有 20 个角色且最小角色管理员数设置为 2，则必须针对 20 个角色中的每个角色分别定义 2 个角色管理员，而不是定义 2 个角色管理员来管理 20 个角色。

要更改最小角色管理员数，请执行：

```
SET OPTION Public.min_role_admins = value
```

另请参见

- 用户帐户自动解锁 （第 106 页）
- MIN_ROLE_ADMINS 选项 （第 281 页）

无法管理角色的 DBA 用户

在某些情况下，DBA 用户可能无法管理（授权、撤消或删除）角色。

这种情况会在满足下列条件时发生：

- 已从角色中删除了全局角色管理员；
- 未将 DBA 用户定义为该角色的角色管理员。

要解决此问题，可将全局角色管理员授予该角色（建议）或添加 DBA 用户作为该角色的角色管理员。

另请参见

- GRANT ROLE 语句 （第 247 页）
- 向现有角色添加角色管理员 （第 12 页）
- 向现有角色添加全局角色管理员 （第 13 页）

系统角色

系统角色是内置角色，在每个新数据库中自动创建。

系统角色：

- 无法删除。
- 无法修改或撤消其缺省基础系统特权。
- 可向其授予（或从中撤消）其它角色和系统特权。
- 无法授予管理权限（使用 WITH ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句）。
- 未指派口令，所以用户无法作为可授予的系统角色连接到数据库。
- 除 SYS、dbo 和 rs_systabgroup 角色外，没有其它对象。

授予 dbo 系统角色

dbo 系统角色拥有许多系统存储过程和视图。

前提条件

MANAGE ROLES 系统特权。

过程

缺省情况下，dbo 系统角色是 SYS 系统角色和 SYS_AUTH_RESOURCE_ROLE 兼容性角色中不具备管理权限的成员。也是 SYS_AUTH_DBA_ROLE 兼容性角色中的成员，且具有全部管理权限。

可将 dbo 系统角色授予其它角色，只是不授予管理权限（使用 WITH NO ADMIN OPTION 子句）。WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对 dbo 系统角色无效。

可将系统特权和角色授予 dbo 系统角色，也可从 dbo 系统角色中撤消系统特权和角色，这其中包括缺省角色。

要授予 dbo 系统角色，请执行：

```
GRANT ROLE dbo TO grantee [,...]
```

另请参见

- GRANT ROLE 语句 （第 247 页）

授予诊断系统角色

诊断系统角色的成员可继承对诊断表和视图的 SELECT、INSERT、UPDATE、DELETE 和 ALTER 特权。

前提条件

MANAGE ROLES 系统特权。

过程

可将诊断系统角色授予其它角色，只是不授予管理权限（使用 WITH NO ADMIN OPTION 子句）。WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对诊断系统角色无效。

可将系统特权和角色授予诊断系统角色，也可从诊断系统角色中撤消系统特权和角色。

要授予诊断系统角色，请执行：

```
GRANT ROLE diagnostics TO grantee [,...]
```

另请参见

- GRANT ROLE 语句 （第 247 页）

授予 PUBLIC 系统角色

PUBLIC 系统角色拥有对一组系统表的 SELECT 特权以及对系统过程的 EXECUTE 特权。

前提条件

MANAGE ROLES 系统特权。

过程

缺省情况下，PUBLIC 系统角色是 dbo 和 SYS 系统角色中不具备管理权限的成员。作为 SYS 角色的成员，它拥有对某些系统表和视图的读取访问权限，因此数据库的任何用户都可以查看有关数据库模式的信息。要限制此访问权限，可撤消 PUBLIC 在 SYS 系统角色中的成员资格。

任何新用户 ID 都自动成为 PUBLIC 系统角色的成员，并继承专门授予该角色的任意特权。虽然可从 PUBLIC 系统角色中移除用户，但 SAP 不建议您这样做，因为这样会影响到用户运行系统存储过程的权限。

可将 PUBLIC 系统角色授予其它角色，只是不授予管理权限（使用 WITH NO ADMIN OPTION 子句）。WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对 PUBLIC 系统角色无效。

可将系统特权和角色授予 PUBLIC 系统角色，也可从 PUBLIC 系统角色中撤消系统特权和角色，这其中包括缺省角色。

要授予 PUBLIC 系统角色，请执行：

```
GRANT ROLE PUBLIC TO grantee [,...]
```

另请参见

- GRANT ROLE 语句 （第 247 页）

授予 rs_systabgroup 系统角色

rs_systabgroup 系统角色拥有 Replication Server 所需的表和系统过程，并授予用户执行 Replication Server 功能的基础系统特权。

前提条件

MANAGE ROLES 系统特权。

过程

可将 rs_systabgroup 系统角色授予其它角色，只是不授予管理权限（使用 WITH NO ADMIN OPTION 子句）。WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对 rs_systabgroup 系统角色无效。

可将系统特权和角色授予 rs_systabgroup 系统角色，也可从 rs_systabgroup 系统角色中撤消系统特权和角色。

要授予 rs_systabgroup 系统角色，请执行：

```
GRANT ROLE rs_systabgroup TO grantee [,...]
```

另请参见

- GRANT ROLE 语句 （第 247 页）

授予 SYS 系统角色

SYS 系统角色拥有数据库的系统表和视图，它们包含了有关数据库模式的完整说明（包括所有数据库对象和用户 ID）。

前提条件

MANAGE ROLES 系统特权。

过程

缺省情况下，授予 SYS 系统角色 dbo 和 PUBLIC 系统角色，而不授予管理权限。但 dbo 和 PUBLIC 系统角色的成员不会继承直接或间接授予 SYS 系统角色的任何系统特权。

可将 SYS 系统角色授予其它角色，只是不授予管理权限（使用 WITH NO ADMIN OPTION 子句）。WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对 SYS 系统角色无效。

不能向 SYS 系统角色授予其它系统特权，也不能从中撤消其它系统特权。

要授予 SYS 系统角色，请执行：

```
GRANT ROLE SYS TO grantee [,...]
```

另请参见

- GRANT ROLE 语句 （第 247 页）

授予 SYS_REPLICATION_ADMIN_ROLE

执行与复制有关的管理任务（如授予复制角色、管理发布、预订、同步用户和配置文件、管理消息类型、设置与复制相关选项等）需要 SYS_RUN_REPLICATION_ADMIN_ROLE 系统角色。

前提条件

MANAGE ROLES 系统特权。

过程

缺省情况下，将授予 SYS_REPLICATION_ADMIN_ROLE 系统角色这些系统特权，但不授予管理权限：

- CREATE ANY PROCEDURE
- CREATE ANY TABLE

- DROP ANY TABLE
- DROP ANY PROCEDURE
- MANAGE ANY OBJECT PRIVILEGE
- MANAGE ANY USER
- MANAGE ANY WEB SERVICE
- MANAGE REPLICATION
- MANAGE ROLES
- SERVER OPERATOR
- SELECT ANY TABLE
- SET ANY SYSTEM OPTION
- SET ANY PUBLIC OPTION
- SET ANY USER DEFINED OPTION

无法撤消 SYS_RUN_REPLICATION_ADMIN_ROLE 系统角色的这组缺省系统特权，但可将其它系统特权和角色授予 SYS_RUN_REPLICATION_ADMIN_ROLE 系统角色，还可从 SYS_RUN_REPLICATION_ADMIN_ROLE 系统角色中撤消其它系统特权和角色。

可将 SYS_RUN_REPLICATION_ADMIN_ROLE 系统角色授予其它角色，只是不能授予管理权限（使用 WITH NO ADMIN OPTION 子句）。WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对 SYS_RUN_REPLICATION_ADMIN_ROLE 系统角色无效。

要授予 SYS_REPLICATION_ADMIN_ROLE 系统角色，请执行：

```
GRANT ROLE SYS_REPLICATION_ADMIN_ROLE TO grantee [,...]
```

另请参见

- GRANT ROLE 语句 （第 247 页）

授予 SYS_RUN_REPLICATION_ROLE

在使用 **dbremote** 执行复制任务以及使用 **dbmlsync** 执行同步任务时需要 SYS_RUN_REPLICATION_ROLE 系统角色。SYS_RUN_REPLICATION_ROLE 系统角色仅对通过这些实用程序连接的用户有效。

前提条件

MANAGE REPLICATION 系统特权。

过程

SYS_RUN_REPLICATION_ROLE 系统角色是 SYS_AUTH_DBA_ROLE 兼容性角色的成员，具有全部管理权限。

该角色还被授予以下系统特权，但没有管理权限：

- SELECT ANY TABLE

- SET ANY USER DEFINED OPTION
- SET ANY SYSTEM OPTION
- BACKUP DATABASE
- MONITOR

无法撤消 SYS_RUN_REPLICATION_ROLE 系统角色的这组缺省系统特权，但可将其它系统特权和角色授予 SYS_RUN_REPLICATION_ROLE 系统角色，还可从 SYS_RUN_REPLICATION_ROLE 系统角色中撤消其它系统特权和角色。

缺省情况下，系统为 SYS_RUN_REPLICATION_ROLE 系统角色授予 SYS_AUTH_DBA_ROLE 兼容性角色，从而满足以下情况下对附加系统特权的任何可能要求：在执行其它与复制相关的已授权任务时所需的附加系统特权高于上述显式授予的系统特权。但 SAP 建议从 SYS_RUN_REPLICATION_ROLE 系统角色撤消 SYS_AUTH_DBA_ROLE 兼容性角色，并将针对其它复制任务标识的特定附加系统特权或角色显式授予 SYS_RUN_REPLICATION_ROLE 系统角色。

可将 SYS_RUN_REPLICATION_ROLE 系统角色授予其它角色，只是不能授予管理权限（使用 WITH NO ADMIN OPTION 子句）。 WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对 SYS_RUN_REPLICATION_ROLE 系统角色无效。

缺省情况下，授予 SYS_RUN_REPLICATION_ROLE 时，接收组成员将继承基础系统特权。要阻止继承，可以仅针对此系统角色包括 WITH NO SYSTEM PRIVILEGE INHERITANCE 子句。

MIN_ROLE_ADMINS 数据库选项可确保指定数目的用户始终存在于数据库中，这些用户可以为其他用户授予和撤消 MANAGE REPLICATION 系统特权。

要授予 SYS_RUN_REPLICATION_ROLE 系统角色，请执行下列语句之一：

继承类型	语句
继承	**GRANT ROLE SYS_RUN_REPLICATION_ROLE TO** *grantee [,...]*
不继承	**GRANT ROLE SYS_RUN_REPLICATION_ROLE TO** *grantee [,...]* **WITH NO SYSTEM PRIVILEGE INHERITANCE**

另请参见

- GRANT ROLE 语句 （第 247 页）

授予 SYS_SPATIAL_ADMIN_ROLE 系统角色

SYS_SPATIAL_ADMIN_ROLE 系统角色授予用户对空间参照系和空间测量单位进行创建、更改、删除或注释的权限。SYS_SPATIAL_ADMIN_ROLE 是全部空间对象的所有者。

前提条件

MANAGE ROLES 系统特权。

过程

缺省情况下，系统为 SYS_SPATIAL_ADMIN_ROLE 系统角色授予 MANAGE ANY SPATIAL OBJECT 系统特权，而不授予管理权限。

可将 SYS_SPATIAL_ADMIN_ROLE 系统角色授予其它角色，只是不授予管理权限（使用 WITH NO ADMIN OPTION 子句）。WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句对 SYS_SPATIAL_ADMIN_ROLE 系统角色无效。

可将系统特权和角色授予 SYS_SPATIAL_ADMIN_ROLE 系统角色，也可从 SYS_SPATIAL_ADMIN_ROLE 系统角色中撤消系统特权和角色，这其中包括缺省特权。

要授予 SYS_SPATIAL_ADMIN_ROLE 系统角色，请执行：

```
GRANT ROLE SYS_SPATIAL_ADMIN_ROLE TO grantee [,...]
```

另请参见

- GRANT ROLE 语句 （第 247 页）

撤消系统角色

撤消用户或角色的系统角色。

前提条件

对要撤消的系统角色具有管理特权。

过程

要撤消系统角色，请执行：

```
REVOKE ROLE role_name FROM grantee [,...]
```

示例：

以下语句完全撤消 Mary 的 dbo 系统角色：

```
REVOKE ROLE dbo FROM Mary
```

另请参见

- REVOKE ROLE 语句 （第 264 页）

兼容性角色

提供兼容性角色是为了实现与 16.0 以前版本的 SAP Sybase IQ（支持基于授权的安全性）的向后兼容。

可以授予或撤消兼容性角色，也可在特定条件下将其删除。无法修改任意基础系统特权。但可将兼容性角色迁移到用户定义角色，然后再修改基础系统特权。迁移兼容性角色时，会自动将用户定义角色授予兼容性角色的所有被授予者。

请在与您操作系统相对应的《迁移》指南中参阅“从 16.0 之前版本升级时的注意事项”>“了解从 15.x 升级后的基于角色的安全性”。

角色拥有的视图、过程和表

与用户拥有的视图、过程和表相比，用户扩展角色拥有的上述对象更加便于管理。

要解除对对象名称的强制限定，可使需要访问表、视图或存储过程的用户成为拥有该对象的角色中的成员。

例如，表 Employees 归角色 Personnel 所有，而 Jeff 是该角色的一位成员。当 Jeff 想引用 Employees 表时，他只需要在 SQL 语句中指定表名称，例如：

```
SELECT * FROM EMPLOYEES
```

但非 Personnel 成员 John 想引用 Employees 表时，他必须使用表的限定名称，例如：

```
SELECT * FROM PERSONNEL.EMPLOYEES
```

注意： 由于数据库对象的所有权与单个用户 ID 相关联，因此当所有者为角色时，该角色的成员不会继承该表的所有权。

不得向拥有对象的角色授予系统特权。可采用以下方式：

- 创建已授予特定系统特权的不同角色
- 为需要特定系统特权成员资格的用户授予合适的角色
- 将每个不同角色授予拥有对象的角色。

这样便可完全控制每个用户执行的任务。通过在与对象关联的相应角色中授予和撤消成员资格来维护授权任务。

例如，表 Sales 属于 Sales1 角色。用户 Mary、Bob、Joe、Laurel 和 Sally 被授予 Sales1 成员资格。创建 Task1_role 并授予其完成特定任务所需的系统特权。将 Task1_role 授予 Mary 和 Bob。创建 Task2_role，授予其特定系统特权，并将其授予 Joe 和 Sally。最后，将 Task1_role 和 Task2_role 授予 Sales1。尽管两个角色都被授予 Sales1，但其他 Sales1 成员不会自动继承 Task1_role 和 Task2_role 的基础系统特权。Mary 和 Bob 所执行的任务与 Joe 和 Sally 不同。由于未向 Laurel 授予 Task1_role 或 Task2_role，且没有直接将系统特权授予 Sales1，因此 Laurel 无法对 Sales 表执行特权性任务。通过此配置可以维护并控制每个用户可执行的任务。

显示授予的角色

sp_displayroles 存储过程返回被授予指定系统特权、系统角色、用户定义角色或用户名的所有角色，或者显示整个角色层次树。

报告包含角色名称、父角色名称、授予类型（是否具有管理特权）和角色层次的级别。

对您自己的用户 ID 执行 **sp_displayroles** 不需要系统特权。对其他用户执行该过程需要具有 MANAGE ROLES 系统特权。要执行角色或系统特权的过程，需要拥有对指定角色或系统特权的管理特权。

示例
下例返回为发出该命令的用户授予的所有角色。

```
CALL sp_displayroles();
```

此示例返回被授予 SYS_SPATIAL_ADMIN_ROLE 系统角色的系统特权列表：

```
CALL sp_displayroles( 'SYS_SPATIAL_ADMIN_ROLE' );
```

role_name	parent_role_name	grant_type	role_level
MANAGE ANY SPATIAL OBJECT	(NULL)	NO ADMIN	1

此示例返回被授予 SYS_SPATIAL_ADMIN_ROLE 的系统特权列表，其中包括角色层次中该角色上面的所有角色：

```
CALL sp_displayroles( 'SYS_SPATIAL_ADMIN_ROLE', 'expand_up');
```

role_name	parent_role_name	grant_type	role_level
SYS_AUTH_DBA_ROLE	dbo	ADMIN	-3
SYS_AUTH_SSO_ROLE	SYS_AUTH_DBA_ROLE	ADMIN	-3
MANAGE ROLES	SYS_AUTH_REMOTE_DBA_ROLE	ADMIN	-2
MANAGE ROLES	SYS_AUTH_SSO_ROLE	ADMIN	-1
MANAGE ROLES	SYS_REPLICATION_ADMIN_ROLE	NO ADMIN	-1
SYS_SPATIAL_ADMIN_ROLE	MANAGE ROLES	ADMIN	0

另请参见

- sp_displayroles 系统过程 （第 297 页）

确定授予用户的角色和特权

sp_has_role 存储函数返回整数值，以表明过程调用者是被授予指定系统特权还是用户定义角色。

执行此函数不需具备系统特权。当用于用户定义存储过程中的权限检查时，该函数会在用户权限检查失败时显示错误消息。

- **1** – 表示已为调用用户授予系统特权或用户定义角色。
- **0 或权限被拒绝：您没有执行此 command/procedure 的权限** – 表示未向调用用户授予系统特权或用户定义角色。throw_error 参数设置为 1 时，将返回错误消息代替值 0。

- **-1** – 表示指定的系统特权或用户定义角色不存在。即使 throw_error 参数设置为 1，也不显示任何错误消息。

另请参见

- SP_HAS_ROLE 函数 [系统] （第 301 页）

特权

特权允许用户在系统中执行已授权的操作。例如，变更表就是一种特许操作，具体取决于您要进行的变更类型。

有两类特权：系统特权和对象级特权。

*系统特权*为您提供执行特许操作的常规权限，而*对象级特权*使您只能对特定对象执行操作。例如，如果具有 ALTER ANY TABLE 系统特权，则可变更系统中的任何表。如果具有 ALTER TABLE 系统特权，只能变更您拥有的表或已为您授予 ALTER 对象级特权的表。对象级特权可以被授予或撤消，但不能创建或删除。

系统特权内置于数据库中，可以被授予或撤消，但不能创建或删除。除 MANAGE ROLES 和 UPGRADE ROLE 特权外，不能修改系统特权。缺省情况下，除 SET USER 系统特权外的每个系统特权都会被授予 SYS_AUTH_SA_ROLE 或 SYS_AUTH_SSO_ROLE 角色，但不能同时授予这两个角色。SET USER 系统特权可以同时授予这两个角色。

使用 **GRANT** 和 **REVOKE** 语句可授予和撤消系统特权和对象级特权。

特权与权限

在基于角色的安全中，权限和特权具有不同的含义。用户可能已被授予执行某项已授权任务所需的特权，但没有对所需对象执行该已授权任务的必要权限。

特权指授予用户或角色执行特定已授权任务的权限。但权限是指在其中执行任务的上下文。

执行某项已授权任务时，如果出现故障，所出现的错误消息通常表示用户没有执行该任务的权限，而不是用户没有执行该任务的特权。在执行某项特许任务或操作之前，系统将验证用户是否具有执行以下操作的正确特权：

- 特许操作
- 对起作用的对象的特许操作
- 在尝试操作的上下文中的特许操作

如果用户在任何级别都没有正确的特权，则可以说该用户没有执行相应任务的权限。操作失败并显示一条错误消息。

示例

用户仅被授予对 `Myconfig.ini` 文本配置对象的 ALTER 特权。

对象特权：用户尝试修改 Myconfig.ini 之外的其它文本配置对象。任务失败，因为授予给用户的 ALTER 特权是特定于 Myconfig.ini Myconfig.ini 文本对象的，而非所有文本对象。

下上文特权：用户尝试删除 Myconfig.ini 的前置过滤器。虽然用户已被授予对 Myconfig.ini 的 ALTER 特权，但要删除文本配置对象的前置过滤器，需要 ALTER ANY TEXT CONFIGURATION 或 ALTER ANY OBJECT 系统特权，而该特权尚未授予用户。

系统特权

系统特权用于控制对已授权系统操作的访问。服务器上的每个特许数据库任务都需要具备特定的系统特权。可向用户或角色逐个授予各个系统特权。

将某个系统特权授予某个角色后，该角色的所有成员都将继承该系统特权。角色的所有新成员会自动继承角色的所有基础系统特权。

缺省情况下，除 SET USER 系统特权外的每个系统特权都会被授予 SYS_AUTH_SA_ROLE 或 SYS_AUTH_SSO_ROLE 角色，但不能同时授予这两个角色。但 SET USER 系统特权可以同时授予这两个角色。

逐个授予某个角色的基础系统特权在语义上等同于授予该角色本身。系统特权可以任意组合形式授予多个用户定义的系统角色，以满足组织的职能安全要求。

除 MANAGE ROLES 和 UPGRADE ROLE 外，不能修改系统特权。系统特权可授予角色和用户，并可以从角色和用户中撤消，但不能将其删除。系统特权不能拥有对象。

按职能范围列出的系统特权

按职能范围划分的系统特权列表。

数据库系统特权

与对数据库执行已授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

ALTER DATABASE 系统特权

变更数据库时需要。

ALTER DATABASE 系统特权允许用户：

- 执行数据库升级
- 执行成本模型校准
- 装载统计信息
- 更改事务日志（另外还需要 SERVER OPERATOR 系统特权）
- 更改数据库所有权（另外还需要 MANAGE ANY MIRROR SERVER 系统特权）

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

BACKUP DATABASE 系统特权
允许用户在一个或多个档案设备上备份数据库。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CHECKPOINT 系统特权
强制数据库服务器执行检查点时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP CONNECTION 系统特权
删除用户与数据库的任意连接时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）

- 列出所有系统特权 （第 64 页）

MANAGE PROFILING 系统特权
启用或禁用应用程序分析的服务器跟踪时需要。充分利用诊断功能向用户提供信息时也需要 DIAGNOSTICS 系统角色。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

MONITOR 系统特权
允许用户执行监控相关任务（例如，访问特许统计信息和运行服务器监控器相关过程等）时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

数据库选项系统特权
与执行用于设置数据库选项的已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

SET ANY PUBLIC OPTION 系统特权
设置任何不需要 SET ANY SECURITY OPTION 或 SET ANY SYSTEM OPTION 系统特权的 PUBLIC 系统数据库选项时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）

- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

SET ANY SECURITY OPTION 系统特权
设置任何 PUBLIC 安全数据库选项时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

SET ANY SYSTEM OPTION 系统特权
设置任何 PUBLIC 系统数据库选项时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

SET ANY USER DEFINED OPTION 系统特权
设置任何用户定义选项时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

数据类型系统特权
与对数据类型执行已授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

ALTER DATATYPE 系统特权
变更数据类型时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE DATATYPE 系统特权
创建数据类型时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP DATATYPE 系统特权
删除数据类型时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

Dbspace 系统特权
与对 dbspace 执行已授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

MANAGE ANY DBSPACE 系统特权
对 dbspace 执行管理相关任务时需要。

MANAGE ANY DBSPACE 系统特权允许用户：

- 针对任何 dbspace 发出 CREATE、ALTER、DROP 或 COMMENT 语句
- 对任何 dbspace 具有 GRANT 或 REVOKE CREATE 对象级特权
- 将数据移动到任何 dbspace
- 对任何 dbspace 发出只读选择性恢复语句
- 运行数据库删除文件函数

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

调试系统特权
与执行调试相关授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

DEBUG ANY PROCEDURE 系统特权
调试任何数据库对象中的所有代码时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

事件系统特权
与事件授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

MANAGE ANY EVENT 系统特权
创建、变更、删除或触发事件时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

外部环境系统特权
与对外部环境执行已授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

CREATE EXTERNAL REFERENCE 系统特权
在数据库中创建外部引用时需要。

创建引用外部对象的数据库对象时，除了所需的任何其他系统特权外，还需要此系统特权。

例如，在创建外部：

- 术语断开器或使用外部术语断开器的自有文本配置时，除了 CREATE EXTERNAL REFERENCE 系统特权外，还需要 CREATE TEXT CONFIGURATION 系统特权。
- 过程或函数时，除了 CREATE EXTERNAL REFERENCE 系统特权外，还需要 CREATE PROCEDURE 系统特权。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

MANAGE ANY EXTERNAL ENVIRONMENT 系统特权
管理外部环境时需要。

MANAGE ANY EXTERNAL ENVIRONMENT 系统特权允许用户对外部环境发出 ALTER、COMMENT、START 或 STOP 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

MANAGE ANY EXTERNAL OBJECT 系统特权
发出 INSTALL、COMMENT ON 或 REMOVE EXTERNAL OBJECT 语句时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

文件系统特权
与文件授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

READ CLIENT FILE 系统特权
读取驻留在客户端计算机上的文件时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）

- 列出所有系统特权 （第 64 页）

READ FILE 系统特权
读取驻留在服务器计算机上的文件时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

WRITE CLIENT FILE 系统特权
写入驻留在客户端计算机上的文件时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

WRITE FILE 系统特权
写入驻留在服务器计算机上的文件时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

索引系统特权
与索引授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

ALTER ANY INDEX 系统特权
变更现有索引时需要。

ALTER ANY INDEX 系统特权允许用户：

- 在任何用户所拥有的任何表中变更索引
- 对任何用户所拥有的任何索引发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY INDEX 系统特权
创建新索引时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

CREATE ANY INDEX 系统特权允许用户：

- 在任何用户所拥有的任何表中创建索引
- 对任何用户所拥有的任何索引发出 COMMENT 语句

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP ANY INDEX 系统特权
在任何用户所拥有的任何表中删除索引时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）

- 列出所有系统特权 （第 64 页）

LDAP 系统特权
与对 LDAP 服务器配置对象执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

MANAGE ANY LDAP SERVER 系统特权
需要该特权才能对 LDAP 服务器配置对象发出 CREATE、ALTER 或 DROP 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

实例化视图系统特权
与对实例化视图执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

CREATE ANY MATERIALIZED VIEW 系统特权
创建任何用户所拥有的实例化视图时需要。该特权还允许用户对任何用户所拥有的实例化视图发出 COMMENT 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE MATERIALIZED VIEW 系统特权
创建自有实例化视图时需要。该特权还允许用户对自有实例化视图发出 COMMENT 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

ALTER ANY MATERIALIZED VIEW 系统特权
变更任何用户所拥有的实例化视图时需要。该特权还允许用户对任何用户所拥有的实例化视图发出 COMMENT 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP ANY MATERIALIZED VIEW 系统特权
删除任何用户所拥有的实例化视图时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

消息系统特权
与对消息执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

CREATE MESSAGE 系统特权
创建消息时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP MESSAGE 系统特权
删除消息时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

杂项系统特权
与执行杂项授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

ALTER ANY OBJECT 系统特权
变更任何人所拥有的对象时需要。

ALTER ANY OBJECT 系统特权允许用户发出下列语句：

- ALTER TABLE
- ALTER INDEX
- ALTER JOIN INDEX
- ALTER VIEW
- ALTER MATERIALIZED VIEW
- ALTER PROCEDURE
- ALTER EVENT

- ALTER SEQUENCE
- ALTER FUNCTION
- ALTER DATATYPE
- ALTER MESSAGE
- ALTER TEXT CONFIGURATION
- ALTER TRIGGER
- ALTER STATISTICS
- 对不同对象的 COMMENT
- ALTER SPATIAL REFERENCE SYSTEM
- ALTER SPATIAL UNIT OF MEASURE

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

ALTER ANY OBJECT OWNER 系统特权
必须具有此特权才能更改任何人所拥有的用户表的所有者。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

注意： 该系统特权仅适用于表对象。无法更改其它对象（如过程、实例化视图等）的所有者。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

COMMENT ANY OBJECT 系统特权
对任何用户所拥有的任何对象进行注释时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）

- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY OBJECT 系统特权
创建任何人所拥有的对象时需要。

CREATE ANY OBJECT 系统特权允许用户发出下列语句：

- 对不同对象的 COMMENT
- CREATE DATATYPE
- CREATE EVENT
- CREATE FUNCTION
- CREATE INDEX
- CREATE JOIN INDEX
- CREATE MATERIALIZED VIEW
- CREATE MESSAGE
- CREATE PROCEDURE
- CREATE SCHEMA
- CREATE SEQUENCE
- CREATE SPATIAL REFERENCE SYSTEM
- CREATE SPATIAL UNIT OF MEASURE
- CREATE STATISTICS
- CREATE TABLE
- CREATE TEXT CONFIGURATION
- CREATE VIEW

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP ANY OBJECT 系统特权
删除任何人所拥有的对象时需要。

DROP ANY OBJECT 系统特权允许用户发出下列语句：

- DROP DATATYPE
- DROP EVENT
- DROP FUNCTION

- DROP INDEX
- DROP JOIN INDEX
- DROP MATERIALIZED VIEW
- DROP MESSAGE
- DROP PROCEDURE
- DROP SEQUENCE
- DROP SPATIAL REFERENCE SYSTEM
- DROP SPATIAL UNIT OF MEASURE
- DROP STATISTICS
- DROP TABLE
- DROP TEXT CONFIGURATION
- DROP TRIGGER
- DROP VIEW

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

MANAGE ANY OBJECT PRIVILEGES 系统特权
管理对象时需要。

MANAGE ANY OBJECT PRIVILEGES 系统特权允许用户执行管理相关的任务，例如：

- 授予对任何用户所拥有的对象的任何对象级特权（INSERT、UPDATE、DELETE、SELECT、ALTER、REFERENCES 或 EXECUTE）
- 撤消对象所有者或具有 MANAGE ANY OBJECT PRIVILEGES 系统特权的其他用户所授予的任何对象级特权

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

REORGANIZE ANY OBJECT 系统特权
针对任何用户所拥有的适用对象发出 REORGANIZE 语句时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

VALIDATE ANY OBJECT 系统特权
在任何用户所拥有的系统存储库中校验或检查表、实例化视图、索引或数据库时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

镜像服务器系统特权
与镜像服务器授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

MANAGE ANY MIRROR SERVER 系统特权
执行高可用性服务器管理任务时需要。

MANAGE ANY MIRROR SERVER 系统特权允许用户：

- 针对镜像服务器发出 CREATE、ALTER 或 DROP 语句
- 更改镜像服务器参数
- 设置镜像服务器选项
- 执行 ALTER 语句来更改数据库所有权

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

Multiplex 系统特权
在 Multiplex 环境中执行授权任务时需具备的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

ACCESS SERVER LS 系统特权
允许使用 SERVER 逻辑服务器上下文进行逻辑服务器连接。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

MANAGE MULTIPLEX 系统特权
允许执行与 Multiplex 服务器管理相关的管理任务。

MANAGE MULTIPLEX 系统特权允许用户：

- 针对逻辑服务器策略发出 Multiplex 相关的 CREATE、ALTER、DROP 或 COMMENT 语句
- 针对逻辑服务器发出 Multiplex 相关的 CREATE、ALTER、DROP 或 COMMENT 语句
- 执行 dbspace 到逻辑服务器的独占分配
- 从逻辑服务器的独占使用释放填充的 dbspace

注意： MANAGE MULTIPLEX 系统特权还管理故障转移配置，手动故障转移时需要该特权。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）

- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

过程系统特权
与执行过程授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

ALTER ANY PROCEDURE 系统特权
变更任何用户所拥有的任何存储过程或函数时需要。

ALTER ANY PROCEDURE 系统特权允许用户：

- 变更任何用户所拥有的存储过程和函数
- 针对任何用户所拥有的过程发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY PROCEDURE 系统特权
创建任何用户所拥有的任何存储过程或函数时需要。

CREATE ANY PROCEDURE 系统特权允许用户：

- 创建任何用户所拥有的存储过程和函数
- 针对任何用户所拥有的过程发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE PROCEDURE 系统特权
创建自有存储过程或函数时需要。

CREATE PROCEDURE 系统特权允许用户:

- 创建自有存储过程和函数
- 针对自有过程发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP ANY PROCEDURE 系统特权
删除任何用户所拥有的任何存储过程或函数时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

EXECUTE ANY PROCEDURE 系统特权
执行任何用户所拥有的任何存储过程或函数时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

MANAGE AUDITING 系统特权
必须具有此特权才能运行 **sa_audit_string** 存储过程。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

复制系统特权
与执行授权复制任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

MANAGE REPLICATION 系统特权
执行复制相关任务时需要。

MANAGE REPLICATION 系统特权允许用户：

- 发出 CREATE、ALTER、DROP 或 COMMENT PUBLICATION 语句
- 发出 CREATE、ALTER、DROP 或 SYNCHRONIZATION SUBSCRIPTION 语句
- 发出 CREATE、ALTER、DROP 或 SYNCHRONIZATION USER 语句
- 发出 CREATE、ALTER、DROP 或 COMMENT SYNCHRONIZATION PROFILE 语句
- 发出 CREATE 或 DROP SUBSCRIPTION 语句
- 发出 CREATE REMOTE MESSAGE TYPE 语句
- 发出 DROP REMOTE MESSAGE TYPE 语句
- 发出 GRANT 或 REVOKE CONSOLIDATE 语句
- 发出 GRANT 或 REVOKE REMOTE 语句
- 发出 GRANT 或 REVOKE PUBLISH 语句
- 发出 LOCK FEATURE 语句
- 发出 START、STOP 或 SYNCHRONIZE SUBSCRIPTION 语句
- 发出 PASSSTHROUGH 语句
- 发出 REMOTE RESET 语句
- 发出 SET REMOTE OPTION 语句
- 发出 START 或 STOP SYNCHRONIZATION SCHEMA CHANGE 语句
- 发出 SYNCHRONIZE PROFILE 语句

- 执行 SA_SETREMOTEUSER 过程
- 执行 SA_SETSUBSCRIPTION 过程

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

角色系统特权
与执行角色授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

MANAGE ROLES 系统特权
创建新角色和充当缺省角色管理员时需要。

MANAGE ROLES 系统特权允许用户创建新的用户定义角色，但不允许删除角色。因此，用户需要对该角色具有管理权限。

被授予 MANAGE ROLES 系统特权的用户充当用户定义角色的缺省全局角色管理员。

如果在角色创建过程中未指定任何角色管理员，系统将自动使用 ADMIN ONLY OPTION 子句向角色授予 MANAGE ROLES 系统特权 (SYS_MANAGE_ROLES_ROLE)，这样全局角色管理员便可管理该角色。如果在角色创建过程中至少指定一个角色管理员，则不会向角色授予 MANAGE ROLES 系统特权，全局角色管理员将无法管理该角色。

MANAGE ROLES 是唯一可被授予对用户定义角色的管理权限的系统特权。

注意： 也可在创建角色的过程中或者在创建完成后向用户直接授予角色管理权限。对用户直接授予角色管理权限时，用户不需要 MANAGE ROLES 系统特权来管理角色。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

UPGRADE ROLE 系统权限
对 16.0 之前版本的 IQ 数据库进行升级时所引入的新系统特权进行管理时需要。

缺省情况下，UPGRADE ROLE 系统特权会被授予 SYS_AUTH_SA_ROLE 角色（前提是该角色存在）。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

序列系统特权
与执行排序授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

ALTER ANY SEQUENCE 系统特权
变更任何序列时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY SEQUENCE 系统特权
创建任何序列时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）

- 列出所有系统特权 （第 64 页）

DROP ANY SEQUENCE 系统特权
删除任何序列时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

USE ANY SEQUENCE 系统特权
使用任何序列时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

服务器操作员系统特权
与执行已授权服务器操作员任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

SERVER OPERATOR 系统特权
执行服务器操作员任务时需要。

SERVER OPERATOR 系统特权允许用户：

- 创建数据库
- 高速缓存管理
- 删除数据库
- 启动或停止数据库
- 启动或停止数据库引擎
- 创建、变更或删除服务器

- 创建加密或解密数据库
- 创建加密或解密文件
- 发出 **ALTER** 语句来更改数据库的事务日志
- 发出 **RESTORE DATABASE** 语句以完全恢复数据库或仅恢复目录

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

空间对象系统特权
与对空间对象执行已授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

MANAGE ANY SPATIAL OBJECT 系统特权
管理任何空间对象时需要。

MANAGE ANY SPATIAL OBJECT 系统特权允许用户发出：

- 针对空间对象的 CREATE、ALTER 或 DROP 语句
- 针对空间测量单位的 CREATE、ALTER 或 DROP 语句
- 针对空间测量单位的 COMMENT 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

统计系统特权
与对统计执行已授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

MANAGE ANY STATISTICS 系统特权
针对任何表的统计信息发出 CREATE、ALTER、DROP 或 UPDATE 语句时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

表系统特权
与对表执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

ALTER ANY TABLE 系统特权
变更任何人所拥有的任何表时需要。

ALTER DATABASE 系统特权允许用户：

- 针对任何用户所拥有的表、表分区或视图发出 ALTER 或 TRUNCATE 语句
- 针对任何用户所拥有的表发出 COMMENT 语句
- 针对任何用户所拥有的表的列发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY TABLE 系统特权
创建任何用户所拥有的表时需要。

CREATE ANY TABLE 系统特权允许用户：

- 创建任何用户所拥有的表，其中包括代理表
- 针对任何用户所拥有的表发出 COMMENT 语句

- 针对任何用户所拥有的表的列发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE PROXY TABLE 系统特权
创建自有代理表时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE TABLE 系统特权
创建自有表时需要。

CREATE TABLE 系统特权允许用户：

- 创建自有表（不包括代理表）
- 针对自有表发出 COMMENT 语句
- 针对自有表的列发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DELETE ANY TABLE 系统特权
删除任何用户所拥有的表、表分区或视图中的行时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP ANY TABLE 系统特权
删除任何用户所拥有的表时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

INSERT ANY TABLE 系统特权
向任何人拥有的表和视图中插入行时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

LOAD ANY TABLE 系统特权
在 **-gl** 服务器开关设置为 DBA 时针对任何表执行 LOAD 命令时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

SELECT ANY TABLE 系统特权
查询任何用户所拥有的表、视图或实例化视图时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

TRUNCATE ANY TABLE 系统特权
针对任何表执行 TRUNCATE 命令时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

UPDATE ANY TABLE 系统特权
更新任何用户所拥有的表和视图中的行时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

文本配置系统特权
与对文本配置执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

ALTER ANY TEXT CONFIGURATION 系统特权
变更任何用户所拥有的文本配置时需要。

ALTER ANY TEXT CONFIGURATION 系统特权允许用户发出：

- 针对任何用户所拥有的文本配置的 ALTER 语句
- 针对任何用户所拥有的文本配置的 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY TEXT CONFIGURATION 系统特权
创建其他用户所拥有的文本配置时需要。

CREATE ANY TEXT CONFIGURATION 系统特权允许用户：

- 创建任何用户所拥有的配置
- 针对任何用户所拥有的文本配置发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE TEXT CONFIGURATION 系统特权
创建自有文本配置时需要。

CREATE TEXT CONFIGURATION 系统特权允许用户：

- 创建自有文本配置
- 针对自有文本配置发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP ANY TEXT CONFIGURATION 系统特权
删除任何用户所拥有的文本配置时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

触发器系统特权
与对触发器执行已授权任务相关的系统特权。

另请参见

- 列出所有系统特权 （第 64 页）

ALTER ANY TRIGGER 系统特权
变更触发器时需要。如果用户对表具有 ALTER 特权，还可以对表发出 COMMENT 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY TRIGGER 系统特权
创建触发器时需要。如果用户对表具有 ALTER 特权，还可以对表发出 COMMENT 语句。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

用户和登录管理系统特权
与对用户和登录策略执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

CHANGE PASSWORD 系统特权
允许用户管理自己及其他用户的口令。

可将此系统特权局限为允许用户管理一组特定用户的口令、管理被授予一组特定角色的任何用户的口令，或者管理任何现有数据库用户的口令。 使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- 口令 （第 84 页）
- GRANT CHANGE PASSWORD 语句 （第 239 页）
- REVOKE CHANGE PASSWORD 语句 （第 258 页）
- 列出所有系统特权 （第 64 页）

MANAGE ANY LOGIN POLICY 系统特权
管理登录策略时需要。

MANAGE ANY LOGIN POLICY 系统特权允许用户发出：

- 针对登录策略的 CREATE、ALTER 或 DROP 语句
- 针对登录策略的 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

MANAGE ANY USER 系统特权
管理用户时需要。

MANAGE ANY USER 系统特权允许用户：

- 针对数据库用户发出 CREATE、ALTER 或 DROP 语句（包括指派初始口令）
- 为用户定义验证机制（Kerberos 登录、集成登录）
- 针对外部登录发出 CREATE 或 DROP 语句
- 强制任何用户在下一次登录时更改口令
- 向任何用户指派登录策略
- 重置任何用户的登录策略
- 针对用户登录、集成登录或 Kerberos 登录发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

SET USER 系统特权
允许用户暂时采用（模仿）其他用户的特定角色和系统特权。

注意： SET USER 系统特权是两个词；而 SETUSER 语句是一个词。

授予 SET USER 系统特权后，可将模仿范围定义为：

- 数据库中的任意用户。
- 指定用户列表中的任意用户 (*target_users_list*)。
- 指定角色中的任意用户 (*target_roles_list*)。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- 模仿 （第 90 页）
- GRANT 系统特权语句 （第 254 页）

- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

视图系统特权
与对视图执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

ALTER ANY VIEW 系统特权
变更任何用户所拥有的视图时需要。

ALTER ANY VIEW 系统特权允许用户：

- 变更任何用户所拥有的视图
- 针对任何用户所拥有的视图发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE ANY VIEW 系统特权
创建任何用户所拥有的视图时需要。

CREATE ANY VIEW 系统特权允许用户：

- 创建任何用户所拥有的视图
- 针对任何用户所拥有的视图发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

CREATE VIEW 系统特权
创建自有视图时需要。

CREATE VIEW 系统特权允许用户：

- 创建自有视图
- 针对自有视图发出 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

DROP ANY VIEW 系统特权
删除任何用户所拥有的视图时需要。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见
- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

Web 服务系统特权
与对 Web 服务执行已授权任务相关的系统特权。

另请参见
- 列出所有系统特权 （第 64 页）

MANAGE ANY WEB SERVICE 系统特权
管理 Web 服务相关任务时需要。

MANAGE ANY WEB SERVICE 系统特权允许用户发出：

- 针对 Web 服务的 CREATE、ALTER 或 DROP 语句
- 针对 Web 服务的 COMMENT 语句

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

另请参见

- GRANT 系统特权语句 （第 254 页）
- REVOKE 系统特权语句 （第 268 页）
- 列出所有系统特权 （第 64 页）

列出所有系统特权

所有系统特权的列表。

系统特权用于控制用户执行授权数据库任务的权限。

另请参见

- ACCESS SERVER LS 系统特权 （第 46 页）
- ALTER ANY INDEX 系统特权 （第 38 页）
- ALTER ANY MATERIALIZED VIEW 系统特权 （第 40 页）
- ALTER ANY OBJECT 系统特权 （第 41 页）
- ALTER ANY OBJECT OWNER 系统特权 （第 42 页）
- ALTER ANY PROCEDURE 系统特权 （第 47 页）
- ALTER ANY SEQUENCE 系统特权 （第 51 页）
- ALTER ANY TABLE 系统特权 （第 54 页）
- ALTER ANY TEXT CONFIGURATION 系统特权 （第 58 页）
- ALTER ANY TRIGGER 系统特权 （第 59 页）
- ALTER ANY VIEW 系统特权 （第 62 页）
- ALTER DATABASE 系统特权 （第 29 页）
- ALTER DATATYPE 系统特权 （第 33 页）
- BACKUP DATABASE 系统特权 （第 30 页）
- CHANGE PASSWORD 系统特权 （第 60 页）
- CHECKPOINT 系统特权 （第 30 页）
- COMMENT ANY OBJECT 系统特权 （第 42 页）
- CREATE ANY INDEX 系统特权 （第 38 页）
- CREATE ANY MATERIALIZED VIEW 系统特权 （第 39 页）
- CREATE ANY OBJECT 系统特权 （第 43 页）
- CREATE ANY PROCEDURE 系统特权 （第 47 页）
- CREATE ANY SEQUENCE 系统特权 （第 51 页）
- CREATE ANY TABLE 系统特权 （第 54 页）
- CREATE ANY TEXT CONFIGURATION 系统特权 （第 58 页）
- CREATE ANY TRIGGER 系统特权 （第 60 页）

- CREATE ANY VIEW 系统特权 （第 62 页）
- CREATE DATATYPE 系统特权 （第 33 页）
- CREATE EXTERNAL REFERENCE 系统特权 （第 35 页）
- CREATE MATERIALIZED VIEW 系统特权 （第 40 页）
- CREATE MESSAGE 系统特权 （第 41 页）
- CREATE PROCEDURE 系统特权 （第 48 页）
- CREATE PROXY TABLE 系统特权 （第 55 页）
- CREATE TABLE 系统特权 （第 55 页）
- CREATE TEXT CONFIGURATION 系统特权 （第 58 页）
- CREATE VIEW 系统特权 （第 63 页）
- DEBUG ANY PROCEDURE 系统特权 （第 34 页）
- DELETE ANY TABLE 系统特权 （第 56 页）
- DROP ANY INDEX 系统特权 （第 38 页）
- DROP ANY MATERIALIZED VIEW 系统特权 （第 40 页）
- DROP ANY OBJECT 系统特权 （第 43 页）
- DROP ANY PROCEDURE 系统特权 （第 48 页）
- DROP ANY SEQUENCE 系统特权 （第 52 页）
- DROP ANY TABLE 系统特权 （第 56 页）
- DROP ANY TEXT CONFIGURATION 系统特权 （第 59 页）
- DROP ANY VIEW 系统特权 （第 63 页）
- DROP CONNECTION 系统特权 （第 30 页）
- DROP DATATYPE 系统特权 （第 33 页）
- DROP MESSAGE 系统特权 （第 41 页）
- EXECUTE ANY PROCEDURE 系统特权 （第 48 页）
- LOAD ANY TABLE 系统特权 （第 56 页）
- INSERT ANY TABLE 系统特权 （第 56 页）
- MANAGE ANY DBSPACE 系统特权 （第 34 页）
- MANAGE ANY EVENT 系统特权 （第 35 页）
- MANAGE ANY EXTERNAL ENVIRONMENT 系统特权 （第 36 页）
- MANAGE ANY EXTERNAL OBJECT 系统特权 （第 36 页）
- MANAGE ANY LDAP SERVER 系统特权 （第 39 页）
- MANAGE ANY LOGIN POLICY 系统特权 （第 60 页）
- MANAGE ANY MIRROR SERVER 系统特权 （第 45 页）
- MANAGE ANY OBJECT PRIVILEGES 系统特权 （第 44 页）
- MANAGE ANY SPATIAL OBJECT 系统特权 （第 53 页）
- MANAGE ANY STATISTICS 系统特权 （第 54 页）
- MANAGE ANY USER 系统特权 （第 61 页）
- MANAGE ANY WEB SERVICE 系统特权 （第 63 页）

- MANAGE AUDITING 系统特权 （第 49 页）
- MANAGE MULTIPLEX 系统特权 （第 46 页）
- MANAGE PROFILING 系统特权 （第 31 页）
- MANAGE REPLICATION 系统特权 （第 49 页）
- MANAGE ROLES 系统特权 （第 50 页）
- MONITOR 系统特权 （第 31 页）
- READ CLIENT FILE 系统特权 （第 36 页）
- READ FILE 系统特权 （第 37 页）
- REORGANIZE ANY OBJECT 系统特权 （第 45 页）
- SELECT ANY TABLE 系统特权 （第 57 页）
- SERVER OPERATOR 系统特权 （第 52 页）
- SET ANY PUBLIC OPTION 系统特权 （第 31 页）
- SET ANY SECURITY OPTION 系统特权 （第 32 页）
- SET ANY SYSTEM OPTION 系统特权 （第 32 页）
- SET ANY USER DEFINED OPTION 系统特权 （第 32 页）
- SET USER 系统特权 （第 61 页）
- TRUNCATE ANY TABLE 系统特权 （第 57 页）
- UPDATE ANY TABLE 系统特权 （第 57 页）
- UPGRADE ROLE 系统权限 （第 51 页）
- USE ANY SEQUENCE 系统特权 （第 52 页）
- VALIDATE ANY OBJECT 系统特权 （第 45 页）
- WRITE CLIENT FILE 系统特权 （第 37 页）
- WRITE FILE 系统特权 （第 37 页）

向用户授予系统特权

允许向特定用户授予特定系统特权，无论用户是否具有管理权限。

前提条件

对要授予的系统特权的管理特权。

过程

警告！ 用于授予系统特权的语法与除 CHANGE PASSWORD 和 SET USER 系统特权之外的所有其它系统特权的语法相同。

使用 WITH ADMIN OPTION、WITH NO ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予此系统特权。如果不指定子句，则缺省情况下，使用 WITH NO ADMIN OPTION。

要向用户授予系统特权，请执行下列语句之一：

管理选项	语句
具有全部管理权限	**GRANT** *system_privilege* **TO** *grantee [,...]* **WITH ADMIN OPTION**
只具有管理权限	**GRANT** *system_privilege* **TO** *grantee [,...]* **WITH ADMIN ONLY OPTION**
不具有管理权限	**GRANT** *system_privilege* **TO** *grantee [,...]* **WITH NO ADMIN OPTION**

另请参见

- GRANT 系统特权语句 （第 254 页）
- GRANT CHANGE PASSWORD 语句 （第 239 页）
- GRANT SET USER 语句 （第 252 页）

撤消用户的系统特权

撤消特定用户的某项特定系统特权以及管理该系统特权的权限。

前提条件

对要撤消的系统特权的管理特权。

过程

警告！ 用于撤消系统特权的语法适用于除 CHANGE PASSWORD 和 SET USER 系统特权之外的所有其它系统特权。

要撤消用户的系统特权，请执行下列语句之一：

管理选项	语句
仅管理权限	**REVOKE ADMIN OPTION FOR** *system_privilege* **FROM** *grantee [,...]*
系统特权和所有管理权限	**REVOKE** *system_privilege* **FROM** *grantee [,...]*

示例：

假设 `Mary` 和 `Joe` 最初被授予 BACKUP DATABASE 系统特权和管理权限，请执行以下语句，仅移除 `Mary's` 对该系统特权的管理权限，但保留其使用该系统特权的权限：

```
REVOKE ADMIN OPTION FOR BACKUP DATABASE FROM Mary
```

执行以下语句从 Joe 中移除系统特权本身以及所有管理权限：

```
REVOKE BACKUP DATABASE FROM Joe
```

另请参见

- REVOKE 系统特权语句 （第 268 页）
- REVOKE CHANGE PASSWORD 语句 （第 258 页）
- REVOKE SET USER 语句 （第 267 页）

授予系统对象的用户和特权

数据库的当前用户及其特权的相关信息存储在数据库系统表中，并可通过系统视图访问。

大多数系统表归 SYS 用户 ID 所有。您无法使用 SYS 用户 ID 进行登录。

DBA 对于所有的系统表都具有 SELECT 访问权限，就像对于数据库中的任何其它表一样。其他用户对某些表的访问会受到限制。例如，只有 DBA 具有访问 SYS.SYSUSERPERM 表的权限，该表中包含所有与数据库用户特权以及每个用户 ID 的口令有关的信息。但 SYS.SYSUSERPERMS 是包含 SYS.SYSUSERPERM 中除口令外的所有信息的视图，并且在缺省情况下，所有用户都有对该视图的 SELECT 访问权限。在新数据库中为 SYS 和 PUBLIC 系统角色自动设置的所有特权和角色成员资格以及 DBA 用户都允许进行完全修改。

系统表中的用户 ID、角色和特权信息

系统表包含有关用户 ID、角色和特权的信息。

所有表和视图都属于 SYS 角色，它们的限定名称为 SYS.ISYSUSERPERM、SYS.ISYSTABLEPERM 等。对这些表执行适当的 SELECT 查询会生成存储在数据库中的所有用户 ID 和特权的信息。

表	缺省值	内容
ISYSUSERPERM	SELECT ANY TABLE 系统特权	各个用户 ID 的数据库级别特权和口令
ISYSTABLEPERM	PUBLIC	由 GRANT 命令授予的对表的所有特权
ISYSCOLPERM	PUBLIC	具有 GRANT 命令所授予的 UPDATE 特权的所有列
ISYSPROCPERM	PUBLIC	每行都保存着一个用户，该用户被授予使用一个过程的特权

系统视图中的用户 ID、角色和特权信息

系统视图包含有关用户 ID、角色和特权的信息。

除该列表以外，还有一些表和视图包含有关数据库中各个对象的信息。

视图	缺省值	内容
SYSUSERAUTH（不建议使用）	SELECT ANY TABLE 系统特权	SYSUSERPERM（不建议使用）中除用户号以外的所有信息
SYSUSERPERMS（不建议使用）	PUBLIC	SYSUSERPERM（不建议使用）中除口令以外的所有信息
SYSUSERLIST（不建议使用）	PUBLIC	SYSUSERAUTH（不建议使用）中除口令以外的所有信息
SYSTABAUTH	PUBLIC	SYSTABLEPERM 中的信息，采用了更加易读的格式
SYSCOLAUTH	PUBLIC	SYSCOLPERM 中的信息，采用了更加易读的格式
SYSPROCAUTH	PUBLIC	SYSPROCPERM 中的信息，采用了更加易读的格式

将系统特权映射到系统角色的存储过程

sp_sys_priv_role_info 存储过程生成用于将每个系统特权角色映射到系统角色的报告。

为每个系统特权生成单独的行。执行此过程不需具备系统特权。

对象级特权

可向用户授予数据库对象级特权以及从用户撤消数据库对象级特权。

数据库对象的所有权特权

拥有数据库对象所有权，即表示具有对该对象执行操作的特权。

数据库对象的创建者不一定是它的所有者。在创建过中可以指定其他用户作为所有者。如果未指定所有者，那么创建者即所有者。

例如，表的*所有者*可以修改表的结构，或者可以向其他数据库用户授予更新表中信息的特权。

注意： 如果表的所有者具有足够特权，或服务器在命令行或配置文件中利用 **-gl all** 开关启动，则该所有者可以装载数据。仅具有所有权或 CREATE ANY OBJECT 系统特权还无法发出 **LOAD TABLE** 命令；还需要对表具有 INSERT 特权。

具有 ALTER ANY OBJECT 系统特权的用户可以修改任何使用 CREATE ANY OBJECT 系统特权创建的数据库对象（无论所有者是谁）。具有 CREATE ANY OBJECT 系统特权的用户可以创建将由其他用户拥有的数据库对象。

数据库特权的继承

可以直接为用户授予数据库特权，用户也可以通过角色成员资格继承特权。

特权名称	支持的数据库对象	允许用户
ALL	表、视图、实例化视图	执行与表、视图和实例化视图相关的全部任务。
ALTER	表	更改表的结构。
CREATE	Dbspace	在 dbspace 上创建对象。所需的附加特权取决于所创建的对象。例如，要创建表，需要 CREATE TABLE、CREATE ANY TABLE 或 CREATE ANT OBJECT 中的其中一种特权。
DELETE	表、视图	从表或视图中删除行。
EXECUTE	过程、用户定义的函数	执行过程或用户定义的函数。
INSERT	表、视图	在表或视图中插入行。
LOAD	表	如果 **-gl** 数据库选项设置为除 NONE 外的任何其它值，则装载表。
REFERENCES	表	在表上创建索引以及创建引用表的外键。
SELECT	表、视图	查看表或视图中的信息。
TRUNCATE	表、实例化视图	截断表或实例化视图。
UPDATE	表、视图	更新表或视图中的行。
USAGE	序列生成器	计算序列中的当前值或下一个值。

在 Multiplex 中，只有写入服务器可以修改由写入服务器拥有的表的表特权。

授予和撤消对象级特权

可以向用户授予或撤消特权组合，以定义其对数据库对象的访问。

授予对表的 ALTER 特权

授予变更表结构的特权。此特权不适用于视图。

前提条件

需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 ALTER 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程
要授予 ALTER 特权，请输入：

```
GRANT ALTER
  ON table_name
  TO userID [,...]
```

另请参见
- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对表和视图的 DELETE 特权
授予该特权以删除指定表或视图中的全部数据。

前提条件

需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 DELETE 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程
要授予 DELETE 特权，请输入：

```
GRANT DELETE
  ON table_name
  TO userID [,...]
```

另请参见
- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对表和视图的 INSERT 特权
授予向表或视图中插入数据的特权。

前提条件

需要满足以下条件之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 INSERT 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程
要授予 INSERT 特权，请输入：

```
GRANT INSERT
   ON table_name
   TO userID [,...]
```

另请参见

- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对表的 LOAD 特权

授予装载指定表的特权。

前提条件

需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 LOAD 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程

要授予 LOAD 特权，请输入：

```
GRANT LOAD
   ON table_name
   TO userID [,...]
```

另请参见

- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对表的 REFERENCES 特权

授予对表中索引和外键的特权。此特权不适用于视图。该特权的范围可以限制为表中的一组列。

前提条件

需要满足以下条件之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 REFERENCES 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程

要授予 REFERENCES 特权，请输入：

```
GRANT REFERENCES column_name
   ON table_name
   TO userID [,...]
```

示例：

以下语句授予用户 Joe 对名为 sales_table 的表中列 Col_1 和 Col_2 的 REFERENCES 特权：

```
GRANT REFERENCES Col_1, Col_2 ON sales_table
TO Joe
```

另请参见

- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对表和视图的 SELECT 特权

授予选择表或视图中数据但不进行变更的特权。该特权的范围可以限制为表中的一组列。

前提条件

需要满足以下条件之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 SELECT 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程

要授予 SELECT 特权，请输入：

```
GRANT SELECT column_name
  ON table_name
  TO userID [,...]
```

示例：

以下语句授予用户 Joe 对名为 sales_table 的表中列 Col_1 和 Col_2 的 SELECT 特权：

```
GRANT SELECT Col_1, Col_2 ON sales_table
TO Joe
```

另请参见

- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对表的 TRUNCATE 特权

授予截断指定表的特权。

前提条件

需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 TRUNCATE 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程

要授予 TRUNCATE 特权，请输入：

```
GRANT TRUNCATE
  ON table_name
  TO userID [,...]
```

另请参见

- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对表和视图的 UPDATE 特权

授予该特权以修改表或视图中的数据。该特权的范围可以限制为表中的一组列。

前提条件

需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 对表的 UPDATE 对象特权（使用 WITH GRANT OPTION 子句），或
- 您拥有该表。

过程

要授予 UPDATE 特权，请输入：

```
GRANT UPDATE column_name
  ON table_name
  TO userID [,...]
```

示例：

下面的语句授予用户 `Joe` 对名为 `sales_table` 的表中列 `Col_1` 和 `Col_2` 的 UPDATE 特权：

```
GRANT UPDATE Col_1, Col_2 ON sales_table
TO Joe
```

另请参见

- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予管理对象级特权的权限
授予该特权可允许用户将特定对象特权传递给其他用户。

前提条件

至少满足以下条件之一：

- 您是表创建者。
- 对表的特权（使用 ADMIN OPTION）。
- LOAD 和 TRUNCATE 对象特权。
- MANAGE ANY OBJECT PRIVILEGE 系统特权。如果使用 WITH GRANT OPTION 子句授予 LOAD 或 TRUNCATE 对象特权，被授予者可以随后将对象特权授予其他用户，但仅限于原始 GRANT 语句中指定的表。在这种情况下，被授予者不必具有 MANAGE ANY OBJECT PRIVILEGE 系统特权。

过程

1. 连接到数据库。
2. 要授予向其他用户授予特权的权限，请输入：

```
GRANT Object_privilege _name
  ON table_name
  TO userID [,...]
  WITH GRANT OPTION
```

示例：

下面的语句授予 Mary 对表 Sales 执行删除的特权：

```
GRANT DELETE ON Sales TO Mary
```

下面的语句授予 Joe 对表 Sales 执行删除的权限，以及将此 DELETE 特权授予其他用户的权限：

```
GRANT DELETE ON Sales TO Joe
WITH GRANT OPTION
```

另请参见

- GRANT 对象级特权语句 （第 245 页）
- 授予管理对象级特权的权限 （第 75 页）

授予对 Dbspace 的 CREATE 特权
授予在指定的 dbspace 中创建数据库对象的特权。

前提条件

需要 MANAGE ANY DBSPACE 系统特权。

过程
要授予 CREATE 特权，请输入：

```
GRANT CREATE
  ON dbspace_name
  TO userID [,...]
```

另请参见
- GRANT CREATE 语句 （第 243 页）

授予对函数和过程的 EXECUTE 特权
授予运行过程或用户定义函数的特权。

前提条件
需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 您拥有该过程。

过程
要授予 EXECUTE 特权，请输入：

```
GRANT EXECUTE
  ON procedure_name
  TO userID [,...]
```

另请参见
- GRANT EXECUTE 语句 （第 244 页）

授予对序列生成器的 USAGE 特权
授予计算序列中当前值或下一个值的特权。

前提条件
需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权，或
- 您拥有序列生成器。

过程
要授予 USAGE 特权，请输入：

```
GRANT USAGE
  ON sequence_name
  TO userID [,...]
```

另请参见
- GRANT USAGE ON SEQUENCE 语句 （第 257 页）

撤消对象级特权
移除用户使用特定对象级特权或将该特权授予其他用户的权限。

前提条件
授予者必须至少满足以下条件之一：

- 为要撤消特权的原始授予者，或
- 具有 MANAGE ANY OBJECT PRIVILEGE 系统特权。

过程

如果撤消已使用 WITH GRANT OPTION 子句为其授予特权的用户的特权，那么也会撤消由该用户授予特权的每个用户的特权。例如，您已通过 WITH GRANT OPTION 子句向 `User1` 授予 SELECT 特权。`User1` 随后将该 SELECT 特权授予 `User2`。如果撤消 `User1` 的 SELECT 特权，也会撤消 `User2` 的此项特权。

REVOKE 命令适用于对象级特权本身，不适用于所授予的对特权的任何管理权限。因此，您无法仅撤消管理权限而使对象级特权保持不变。要以正确方式仅仅移除用户对对象级特权的管理权限，必须先撤消特权，然后在不使用 WITH GRANT OPTION 子句的情况下重新授予该特权。

1. 要撤消对象级特权以及所有管理特权，请执行：

```
REVOKE object_privilege_name
  ON table_name
  FROM userID [,...]
```

2. （可选）要重新授予对象级特权（不包括管理权限），请执行：

```
GRANT object_privilege_name
  ON table_name
  TO userID [,...]
```

示例：

本示例假定已授予 `Joe` 对表 `Sales` 执行删除的权限以及将对该表的 DELETE 对象级特权授予其他用户的权限。

以下语句将撤消对表 `Sales` 的所有 DELETE 对象级特权，其中明确包括所有管理权限：

```
REVOKE DELETE ON Sales FROM Joe
```

以下语句仅重新授予对象级特权，不包括管理权限：

```
GRANT DELETE ON Sales TO Joe
```

另请参见

- REVOKE 对象级特权语句 （第 262 页）
- REVOKE CREATE 语句 （第 261 页）

- REVOKE EXECUTE 语句 （第 262 页）
- REVOKE USAGE ON SEQUENCE 语句 （第 272 页）

管理 Dbspace 中的表对象所需的特权

所需的特权取决于正在执行的任务。

要在 dbspace 中创建新表需要具有对 dbspace 的 CREATE 对象级特权。要将现有表或列移动到 dbspace 需要具有对目标 dbspace 的 MANAGE ANY DBSPACE 系统特权或 CREATE 对象级特权。

除满足 dbspace 的要求之外，还需具有特定任务的系统特权。例如，需要具有 CREATE TABLE 或 CREATE ANY TABLE 系统特权才能创建表，需要具有 ALTER ANY TABLE 系统特权才能更改表，依此类推。

例如，要在 dbspace `test1` 中创建归您所有的 `table1`，需要具有对 `test1` CREATE 对象级特权和 CREATE TABLE 系统特权。然后，要将 `table1` 从 dbspace `test1` 移动到 dbspace `test2`，需要具有对目标 dbspace `test2` 的 MANAGE ANY DBSPACE 系统特权或 CREATE 对象级特权。

可将所需的特权授予用户或角色，也可从用户或角色中撤消所需特权。角色中的任何成员都将从角色继承这些特权。

缺省情况下，会授予 PUBLIC 对 IQ_SYSTEM_MAIN、IQ_SYSTEM_TEMP 和 SYSTEM 的 CREATE 对象级特权。

控制特权的命令行选项

数据库服务器启动命令 **start_iq** 包含一些选项，可用于设置某些数据库和服务器功能的特权级别。

启动和停止数据库的开关

使用 **-gd** 选项，将仅允许在其所连接的数据库中具有以下特定特权的用户在运行的服务器上启动或停止数据库：

- **DBA** – （缺省值）只有具有 SERVER OPERATOR 系统特权的用户才可以启动额外的数据库。
- **ALL** – （**start_iq** 和 `default.cfg` 中的缺省值）任何用户都可启动和停止数据库。此设置表示 DBA 不需要发出 **START DATABASE** 命令。用户仍必须被授予特权才能访问自己启动的特定数据库。
- **NONE** – 任何人都无法通过 Interactive SQL 在运行的服务器上启动或停止数据库。

注意： 如果启动服务器时未设置 **-gd ALL**，则只有具有 SERVER OPERATOR 系统特权的用户才可以启动服务器上的其它数据库。这意味着用户无法连接到在服务器启动时、或随后由具有 SERVER OPERATOR 系统特权的用户启动服务器时未启动的数据库。但是，不具有 SERVER OPERATOR 系统特权的用户也可以停止数据库。因此，建议您将生产数据库上的此设置更改为 DBA。

创建和删除数据库的开关
-gu 选项仅允许在其所连接的数据库中具有特定特权的用户创建和删除数据库。

- **DBA** – 只有具有 SERVER OPERATOR 系统特权的用户才可以创建和删除数据库。
- **ALL**（缺省值） – 任何用户都可以创建和删除数据库。
- **NONE** – 任何用户都不能创建和删除数据库。
- **UTILITY_DB** – 只有能够连接到 `utility_db` 数据库的用户才能创建和删除数据库。

停止服务器开关
使用 **-gk** 选项，可限制能够使用 **dbstop** 实用程序或 **STOP ENGINE** 命令关闭服务器的用户：

- **DBA**（缺省值） – 只有具有 SERVER OPERATOR 系统特权的用户才能停止服务器。
- **ALL** – 任何用户都可以停止服务器。
- **NONE** – 任何用户都不能使用 **dbstop** 实用程序或 **STOP ENGINE** 命令关闭服务器。

装载和卸载数据库的开关
-gl 选项仅允许在数据库中具有特定特权的用户使用 **LOAD TABLE** 装载数据。

- **DBA** – 任何具有 LOAD ANY TABLE、ALTER ANY TABLE 或 ALTER ANY OBJECT 系统特权的用户都可以装载数据。
- **ALL**（**start_iq** 和 `default.cfg` 的缺省值）- 任何用户都可以装载数据。
- **NONE** – 无法装载数据。

另请参见
- -gl iqsrv16 服务器选项 （第 286 页）
- -gu iqsrv16 数据库服务器选项 （第 286 页）
- -gk iqsrv16 数据库服务器选项 （第 285 页）

撤消运行过程的特权
移除执行或调用特定过程的特权。

前提条件
撤消者必须满足以下两个条件之一：

- 为要撤消特权的原始授予者，或
- 具有 MANAGE ANY OBJECT PRIVILEGE 系统特权。

过程
要撤消运行特定过程的 EXECUTE 特权，请执行：

```
REVOKE EXECUTE ON procedure_name
FROM grantee [,...]
```

另请参见

- REVOKE EXECUTE 语句 （第 262 页）

用于显示授予的对象级特权的存储过程

执行 **sp_objectpermission** 存储过程，以生成有关授予指定角色或用户名的对象级特权或授予指定对象或 dbspace 的对象特权的报告。

该报告包含特权授予者和被授予者的用户 ID、对象名称和所有者、授予的特权以及被授予者是否能转而将特权授予其他用户。

对您自己的用户 ID 执行过程不需要系统特权。要对其他用户或 dbspace 执行 **sp_objectpermission**，必须分别拥有 MANAGE ANY OBJECT PRIVILEGE 或 MANAGE ANY DBSPACE 特权。

另请参见

- sp_objectpermission 系统过程 （第 353 页）

系统过程特权

特许系统过程可以两种安全模型运行。每个模型都会授予以不同方式运行系统过程的权限。

注意： 以下信息只适用于 SAP Sybase IQ 特许系统过程，不适合用户定义的存储过程。

第一个模型称为 SYSTEM PROCEDURE DEFINER 模型，以特许系统过程所有者（通常是 dbo）特权来运行该过程。第二个模型称为 SYSTEM PROCEDURE INVOKER 模型，以执行特许系统过程的人员的特权来运行该过程。

要使用 SYSTEM PROCEDURE DEFINER 模型来运行特许系统过程，需要授予对该过程的显式 EXECUTE 对象级特权。运行系统过程的任何基础已授权任务所需的所有系统特权都自动从所有者（系统过程的定义者）继承。

对于使用 SYSTEM PROCEDURE INVOKER 模型的特许系统过程，系统会向 PUBLIC 角色授予 EXECUTE 对象级特权，由于在缺省情况下，每个用户都是 PUBLIC 角色的成员，因此，每个用户都会自动继承 EXECUTE 对象级特权。但是，由于 PUBLIC 角色并不是系统过程的所有者，并且未被授予任何系统特权，因此，必须将运行任何基础已授权任务所需的系统特权直接或间接授予该用户。

缺省情况下，16.0 及更高版本中所创建的数据库使用 SYSTEM PROCEDURE INVOKER 模型来运行所有特许系统过程。16.0 之前版本中以及升级到 16.0 或更高版本的版本中所创建的数据库组合使用 SYSTEM PROCEDURE DEFINER 和 SYSTEM PROCEDURE INVOKER 模型来运行特许系统过程。在组合模型中，所有 16.0 之前版本的特许系统过程都使用 SYSTEM PROCEDURE DEFINER 模型，而在 16.0（或任何之后的版本）中引入的所有特许系统过程都使用 SYSTEM PROCEDURE

INVOKER 模型。在创建或升级数据库期间，可以替换缺省安全模型，也可以在此后的任何时间更改此模型。但 SAP 不建议这么做，因为这可能会造成自定义存储过程和应用程序的功能丢失。

授予运行特许系统过程的权限

授予运行特许系统过程的权限所用的进程取决于该过程以哪种安全模型运行。

对于使用 SYSTEM PROCEDURE DEFINER 模型的特许系统过程，将系统过程的 EXECUTE 对象级特权授予用户：

```
GRANT EXECUTE ON sys_procedure_name
    TO grantee [,...]
```

对于使用 SYSTEM PROCEDURE INVOKER 模型的特许系统过程，将系统过程所需的基础系统特权授予用户。 使用 **sp_proc_priv()** 可标识运行系统过程所需的系统特权。

```
GRANT system_privilege_name
    TO grantee [,...]
```

另请参见

- GRANT EXECUTE 语句 （第 244 页）

撤消运行特许系统过程的权限

撤消运行特许系统过程的权限所用的进程取决于该过程以哪种安全模型运行。

对于使用 SYSTEM PROCEDURE DEFINER 模型的特许系统过程，撤消用户对系统过程的 EXECUTE 对象级特权：

```
REVOKE EXECUTE ON sys_procedure_name
    FROM grantee [,...]
```

对于使用 SYSTEM PROCEDURE INVOKER 模型的特许系统过程，撤消用户具有的系统过程所需的基础系统特权：

```
REVOKE system_privilege_name
    FROM grantee [,...]
```

另请参见

- REVOKE EXECUTE 语句 （第 262 页）

确定数据库所使用的安全模型

有两种安全模型可供数据库使用。

要确定数据库正在使用的安全模型，请执行：

```
select IF ((HEXTOINT(substring(db_property('Capabilities'),
1,length(db_property('Capabilities'))-20)) & 8) = 8)
THEN 1
ELSE 0
END IF
```

1 表示数据库正在使用 SYSTEM PROCEDURE INVOKER 模型。0 表示数据库正在使用组合模型。

在组合模型中，只有 16.0 之前版本的特许系统过程才使用 SYSTEM PROCEDURE DEFINER 来运行。请参考 16.0 之前版本的特许系统过程列表来标识这些系统过程。

无法将新的或升级的 16.0 版本及更高版本的数据库配置为使用 SYSTEM PROCEDURE DEFINER 模型来运行所有系统过程。

16.0 之前版本的特许系统过程

16.0 之前版本的特许系统过程列表。

使用组合安全模型的特许系统过程

对于这些特许系统过程，如果将数据库配置为使用 SYSTEM PROCEDURE DEFINER，您只需要该过程的 EXECUTE 对象级特权便可运行它。如果将数据库配置为使用 SYSTEM PROCEDURE INVOKER，您还需要具有运行每个过程所需的各个系统特权。有关运行各个系统过程所需的系统特权，请参见《参考：构件块、表和过程》指南。

• sa_audit_string • sa_checkpoint_execute • sa_disable_auditing_type • sa_disk_free_space • sa_enable_auditing_type • sa_external_library_unload • sa_flush_cache • sa_list_external_library • sa_server_option • sa_procedure_profile • sa_procedure_profile_summary • sa_table_page_usage • sa_validate • sp_iq_reset_identity • sp_iqaddlogin • sp_iqbackupdetails • sp_iqbackupsummary • sp_iqcardinality_analysis • sp_iqcheckdb • sp_iqcheckoptions • sp_iqclient_lookup • sp_iqcolumn • sp_iqcolumnuse • sp_iqconnection • sp_iqconstraint • sp_iqcontext • sp_iqconstraint • sp_iqcontext • sp_iqcursorinfo • sp_iqdatatype • sp_iqdbsize	• sp_iqdbspace • sp_iqdbspaceinfo • sp_iqdbspaceobjectinfo • sp_iqdbstatistics • sp_iqdroplogin • sp_iqemptyfile • sp_iqestdbspaces • sp_iqestspace • sp_iqevent • sp_iqfile • sp_iqhelp • sp_iqindex • sp_iqindex_alt • sp_iqindexadvice • sp_iqindexfragmentation • sp_iqindexinfo • sp_iqindexmetadata • sp_iqindexsize • sp_iqindexuse • sp_iqlmconfig • sp_iqlocks • sp_iqmodifyadmin • sp_iqmodifylogin • sp_iqmpxcheckdqpconfig • sp_iqmpxdumptlvlog • sp_iqmpxfilestatus • sp_iqmpxincconnpoolinfo • sp_iqmpxincheartbeatinfo • sp_iqcopyloginpolicy • sp_iqmpxincconnpoolinfo • sp_iqmpxincheartbeatinfo	• sp_iqmpxinfo • sp_iqmpxversioninfo • sp_iqobjectinfo • sp_iqpkeys • sp_iqprocedure • sp_iqprocparm • sp_iqrebuildindex • sp_iqrename • sp_iqrestoreaction • sp_iqrowdensity • sp_iqsetcompression • sp_iqsharedtempdistrib • sp_iqshowcompression • sp_iqshowpsexe • sp_iqspaceinfo • sp_iqspaceused • sp_iqstatistics • sp_iqstatus • sp_iqsysmon • sp_iqtable • sp_iqtablesize • sp_iqtableuse • sp_iqtransaction • sp_iqunusedcolumn • sp_iqunusedindex • sp_iqunusedtable • sp_iqversionuse • sp_iqview • sp_iqwho • sp_iqworkmon

使用调用者特权的特许系统过程

16.0 之前版本的这些特许系统过程以运行该过程的用户（而不是过程的所有者）的特权来运行，而不考虑安全模型设置如何。因此，除了需要对系统过程的 EXECUTE 对象级特权（缺省情况下通过 PUBLIC 角色的成员资格授予）之外，还必须为用户授予系统过程所需的其它系统特权。有关运行各个系统过程所需的系统特权，请参见《参考：构件块、表和过程》指南。

- sa_describe_shapefile
- sa_get_user_status
- sa_locks
- sa_performance_diagnostics
- sa_report_deadlocks
- sa_text_index_stats

口令

可为用户授予管理其他用户口令的权限。可将口令管理配置为需要一个或两个用户来完成口令更改。

数据库中的口令

从版本 15.0 开始，SAP Sybase IQ 使用 SHA256 来散列口令。口令以 UTF-8 形式存储。

创建或更改口令时，口令先被转换为 UTF-8，然后再散列并存储在数据库中。如果数据库被卸载和重装到带有不同字符集的数据库，则现有口令将继续有效。如果服务器不能将客户端的字符集转换为 UTF-8，SAP 建议采用由 7 位 ASCII 字符组成的口令，因为其它字符可能会无法正常工作。

向用户授予 CHANGE PASSWORD 系统特权

允许用户管理其他用户的口令。

前提条件

- 已授予 CHANGE PASSWORD 系统特权以及管理权限。
- 每个指定目标用户 (target_users_list) 都是具有登录口令的现有用户角色或用户扩展角色。
- 每个指定目标角色 (target_roles_list) 都必须是现有用户扩展角色或用户定义角色。

过程

可授予用户更改数据库中任意用户口令的权限 (ANY)、仅更改特定用户口令的权限 (*target_users_list*)，或更改特定角色的成员口令的权限 (ANY WITH ROLES *target_roles_list*)。仅当使用 ANY 子句时才能授予 CHANGE PASSWORD 系统特权的管理权限。

如果未指定子句，则缺省使用 ANY 和 WITH NO ADMIN OPTION。

重新授予 CHANGE PASSWORD 系统特权时，授予行为的影响是累积的。例如，如果将仅限于 `User2` 和 `User3` 的特权授予 `User1`，然后重新授予仅限于 `Role1` 的特权，则 `User1` 可以管理 `User2`、`User3` 以及 `Role1` 任意成员的口令。

如果向某位用户授予 CHANGE PASSWORD 系统特权，但权限低于当前已授予的权限，则保留较高权限。例如，如果使用 ANY 子句授予了特权，然后使用 *target_users_list* 子句重新授予特权，则用户会保留使用 ANY 子句授予的权限。

要授予 CHANGE PASSWORD 系统特权，请执行下列语句之一：

授予类型	语句
任意数据库用户（不具有全部管理权限）	**GRANT CHANGE PASSWORD** (**ANY**) **TO** *user_ID* **WITH ADMIN OPTION**
任意数据库用户（不具有管理权限）	**GRANT CHANGE PASSWORD** (**ANY**) **TO** *user_ID* **WITH ADMIN ONLY OPTION**
任意数据库用户（不具有管理权限）	**GRANT CHANGE PASSWORD** (**ANY**) **TO** *user_ID* **WITH NO ADMIN OPTION**
指定用户（不具有管理权限）	**GRANT CHANGE PASSWORD** (*target_users_list*) **TO** *user_ID* **WITH NO ADMIN OPTION**
指定角色的任意成员（不具有管理权限）	**GRANT CHANGE PASSWORD** (**ANY WITH ROLES** *target_roles_list*) **TO** *user_ID* **WITH NO ADMIN OPTION**
指定用户或指定角色的任意成员（不具有管理权限）	**GRANT CHANGE PASSWORD** (*target_users_list*), (**ANY WITH ROLES** *target_roles_list*) **TO** *user_ID* **WITH NO ADMIN OPTION**

示例：

以下语句授予 Sam 更改任意数据库用户口令的权限：

```
GRANT CHANGE PASSWORD (ANY) TO Sam
or
GRANT CHANGE PASSWORD TO Sam
```

以下语句授予 Sally 和 Bob 更改 Jane、*Joe* 和 Laurel（仅限这三者）的口令的权限：

```
GRANT CHANGE PASSWORD (Jane, Joe, Laurel) TO Sally, Bob
```

以下语句授予 Mary 更改 Sales1 角色任意成员的口令的权限：

```
GRANT CHANGE PASSWORD (ANY WITH ROLES Sales1) TO Mary
```

以下语句授予 Sarah 更改 Joe 或 Sue 的口令或更改 Sales2 角色任意成员的口令的权限：

```
GRANT CHANGE PASSWORD (Joe, Sue), (ANY WITH ROLES Sales2) TO Sarah
```

以下语句授予 Joan 更改 Marketing1 或 Marketing2 角色任意成员的口令的权限：

```
GRANT CHANGE PASSWORD (ANY WITH ROLES Marketing1, Marketing2) TO Joan
```

另请参见

- GRANT CHANGE PASSWORD 语句 （第 239 页）

撤消用户的 CHANGE PASSWORD 系统特权

移除用户管理口令和管理系统特权的能力。

前提条件

需要具备所授予的 CHANGE PASSWORD 系统特权以及管理权限。

过程

可使用不同子句向某位用户多次授予 CHANGE PASSWORD 系统特权。例如，使用 ANY 子句为 User1 授予一次 CHANGE PASSWORD 系统特权，然后再使用 *target_users_list* 子句授予一次该特权。在多次授予的情况下，必须使用 **GRANT** 语句所用的同一子句格式来进行撤消。

仍以上例为例，如果使用 ANY 子句撤消 User1 的系统特权，使用 *target_users_list* 子句进行的授予仍生效。实际效果是 User1 现在只能够管理 *target_users_list* 中用户的口令。或者，如果使用 *target_users_list* 子句撤消 User1 的系统特权，使用 ANY 子句进行的授予仍生效。此时的实际效果是 User1 可继续管理数据库中任意用户的口令。

要撤消 CHANGE PASSWORD 系统特权，请执行下列语句之一：

撤消类型	说明
仅系统特权 的管理权限	**REVOKE ADMIN OPTION FOR CHANGE PASSWORD** (**ANY**) **FROM** *user_ID [,...]*

撤消类型	说明
用于管理任意数据库用户的口令的系统特权，包括管理权限	**REVOKE CHANGE PASSWORD** **FROM** *user_ID [,...]*
用于管理指定角色的口令的系统特权	**REVOKE CHANGE PASSWORD** (*target_users_list*) **FROM** *user_ID [,...]*
用于管理指定角色的口令的系统特权	**REVOKE CHANGE PASSWORD** (**ANY WITH ROLES** *target_roles_list*) **FROM** *user_ID [,...]*

示例：

以下两条语句用于移除 Sam 更改任意数据库用户口令的权限：

```
REVOKE CHANGE PASSWORD (ANY) FROM Sam
or
GRANT CHANGE PASSWORD TO Sam
```

假设已通过 ANY 和 WITH ADMIN OPTION 子句为 Frank 授予了 CHANGE PASSWORD 系统特权，以下语句仅移除 Frank 管理系统特权的权限。他可以继续更改数据库中任意用户的口令。

```
REVOKE ADMIN OPTION FOR CHANGE PASSWORD (ANY) FROM Frank
```

以下语句移除 Sally 和 Bob 更改 Jane、Joe 和 Laurel（仅限这三者）的口令的权限：

```
REVOKE CHANGE PASSWORD (Jane, Joe, Laurel) FROM Sally, Bob
```

以下语句移除 Mary 更改 Sales1 角色任意成员的口令的权限：

```
REVOKE CHANGE PASSWORD (ANY WITH ROLES Sales1) FROM Mary
```

以下语句移除 Sarah 更改 Joe 或 Sue 的口令或者更改 Sales2 角色任意成员的口令的权限：

```
REVOKE CHANGE PASSWORD (Joe, Sue), (ANY WITH ROLES Sales2) FROM Sarah
```

以下语句移除 Joan 更改 Marketing1 或 Marketing2 角色任意成员的口令的权限：

```
REVOKE CHANGE PASSWORD (ANY WITH ROLES Marketing1, Markeing2) FROM
Joan
```

另请参见

- REVOKE CHANGE PASSWORD 语句 （第 258 页）

更改口令 – 单一控制

单个用户可管理其他用户的口令。

前提条件

- CHANGE PASSWORD 系统特权。
- 已授予管理用户更改目标用户口令的权限。

过程

在命令提示符处键入：

```
ALTER USER userID
IDENTIFIED BY password
```

另请参见

- 用户 ID 和口令区分大小写 （第 101 页）
- ALTER USER 语句 （第 218 页）

双重控制口令管理选项

双重控制口令选项要求由两位管理用户来更改一位目标用户的口令，从而确保任何一位用户都不知道（或不能控制）该目标用户的口令。

要生成新口令的各个组成部分，需要有两位不同的管理用户。这两部分组成了目标用户的新口令。同一用户无法生成两个口令部分。如果同一用户尝试定义两个口令部分，服务器将显示一条错误消息，并且不会设置第二个口令部分。

如果在指定第一个口令部分之后但在指定第二个口令部分之前重新启动服务器，第一个口令部分不会丢失。由其他用户指定第二个口令部分后，双重口令更改过程即成功完成。之后，目标用户可以使用组合的口令部分进行登录。

启动后，只要为用户授予了 CHANGE PASSWORD 系统特权以及管理目标用户口令的权限，就可以通过将 "NULL" 指定为口令来取消为目标用户生成的双重口令。

每个设置口令部分的管理用户必须将新口令部分通知给目标用户，并指出该部分口令是第一部分还是第二部分。要使用口令，目标用户必须按第一部分、第二部分的顺序输入双重口令。每个部分的长度不得超过 127 个字符。

双重口令更改进程完成后，如果目标用户未登录，则该用户登录即可。系统接受双重口令后，将立即提示用户更改其口令。这提供了最终级别的口令安全性。双重口令更改进程完成后，如果用户已登录，则该用户可以使用 **ALTER USER** 或 **GRANT CONNECT** 语句，或者 **sp_password** 或 **sp_iqpassword** 系统过程来更改口令。在当前口令的提示符下，输入新的双重部分口令，而非最初为当前会话输入的口令。

“更改口令的双重控制”选项在登录策略中已启用。

另请参见

- 用户 ID 和口令区分大小写 （第 101 页）
- ALTER USER 语句 （第 218 页）
- GRANT CONNECT 语句 （第 241 页）
- sp_iqpassword 过程 （第 352 页）

启用更改口令的双重控制

需要由两个管理用户进行输入来更改另一用户的口令。

前提条件

MANAGE ANY LOGIN POLICY OPTION 系统特权。

过程

口令管理的双重控制是登录策略的一个可配置选项。缺省情况下，禁用该选项 (OFF)。

要启用该选项，请执行：

```
ALTER LOGIN POLICY policy-name
CHANGE_PASSWORD_DUAL_CONTROL=ON
```

另请参见

- ALTER LOGIN POLICY 语句 （第 209 页）
- CREATE LOGIN POLICY 语句 （第 224 页）

更改口令 – 双重控制

需要两个用户来管理其他用户的口令。

前提条件

- CHANGE PASSWORD 系统特权。
- 已授予管理用户更改目标用户口令的权限。
- 在管理用户的登录策略中启用 CHANGE_PASSWORD_DUAL_CONTROL 选项。

过程

1. 在命令提示符处，第一个管理用户输入：

   ```
   ALTER USER userID
   IDENTIFIED FIRST BY password_part1
   ```

2. 在命令提示符处，第二个管理用户输入：

   ```
   ALTER USER userID
   IDENTIFIED LAST BY password_part1
   ```

示例

假设登录策略 Sales1 启用了 **CHANGE_PASSWORD_DUAL_CONTROL** 选项，为 User3 指派了 Sales1，并且已为 User1 和 User2 授予了更改 User3 口令的必要特权，以下语句将 User3 的两个口令部分分别设置为 *NewPassPart1* 和 *NewPassPart2*:

User1 键入：

```
ALTER USER user3 IDENTIFIED FIRST BY NewPassPart1
```

User2 键入：

```
ALTER USER user3 IDENTIFIED LAST BY NewPassPart2
```

另请参见

- 用户 ID 和口令区分大小写 （第 101 页）
- ALTER USER 语句 （第 218 页）

模仿

用户可临时采用（模仿）其他用户的特定角色和系统特权来执行操作，前提是该用户已具有执行任务所需的最低特权。

假设 User1 负责执行某个关键任务，但该用户缺席。User2 具有的特权足以完成该任务，但其还具有 User1 不可用的其它特权。如果由 User2 执行该任务，则可能与 User1 执行时完全不同。要避免出现这种情况，User2 临时采用（模仿）User1 特定的角色和系统特权来执行该任务。

先为用户授予 SET USER 系统特权，然后发出 SETUSER 语句来启动模仿，这样便可实现模仿。

注意： SET USER 系统特权是两个词；而 SETUSER 语句是一个词。

授予 SET USER 系统特权后，可将模仿范围定义为：

- 数据库中的任意用户。
- 指定用户列表中的任意用户 (*target_users_list*)。
- 指定角色中的任意用户 (*target_roles_list*)。

要模仿其他用户，必须至少向模仿（被授予）用户授予被模仿（目标）用户的所有角色和系统特权，并授予相同或更高的管理特权。这称为*必要*条件。可向模仿用户授予其它角色、系统特权或更高的管理特权，但不能更少。在模仿其他用户时，只要不违反*必要*条件，就可以进行模仿，也可以向模仿者授予或撤消其它角色和特权。如果授予或撤消操作违反条件，则会出现一条错误消息，且语句将失败。

例如，User1 成功模仿 User2。您将新角色授予 User1，而不是 User2。由于此授予操作不会违反 User1 模仿 User2 时需满足的条件（User1 至少仍具有向 User2

授予的角色和特权），所以此授予将成功。但如果将新角色授予 User2 而不是 User1，此授予语句将失败，因为这会导致授予 User2 的角色多于 User1。

当您模仿其他用户时，被模仿用户的用户 ID（而不是您的用户 ID）将出现在审计日志中。但由于模仿行为（发出 SETUSER 命令）也记录在审计日志中，因此，可以确定任务是由被授予者执行的还是目标用户执行的。

在 Multiplex 配置中，如果模仿在协调器的连接中处于活动状态，而且试图授予或撤消角色和特权将违反必要条件，则包含活动模仿的连接将终止。由于终止连接也会终止模仿，因此，违反必要条件就不再成为问题，**GRANT** 或 **REVOKE** 语句将成功执行。

模仿要求

只有满足一组特定条件（也称为*必要*要求）时，用户才能成功模仿其他用户。

要成功模仿需要满足以下四个条件：

1. 已授予模仿者模仿目标用户的权限。
2. 模仿者至少具有目标用户被授予的所有角色和系统特权。
3. 已授予模仿者具有类似或更高管理权限的角色和系统特权。

   注意： 为了满足管理权限条件，将认为 WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句授予类似的管理权限。此外，还会认为这些子句授予的管理权限比 WITH NO ADMIN OPTION 子句授予的权限要高。例如，使用 WITH ADMIN OPTION 子句向 User1 授予 Role1，使用 WITH ADMIN ONLY 子句向 User2 授予 Role1，使用 WITH NO ADMIN OPTION 子句向 User3 授予 Role1。将授予 User1 和 User2 具有类似管理权限的 Role1。将授予 User1 和 User2 管理权限比 User3 高的 Role1。
4. 如果已授予目标用户支持扩展的系统特权，则用于授予模仿者系统特权的子句是用于目标用户的子句的超集。仅 SET USER 和 CHANGE PASSWORD 系统特权支持扩展。
   - 将 ANY 子句视为 *target_roles_list* 和 *target_users_list* 子句的超集。如果已授予目标用户具有 ANY 授权的 SET USER 系统特权，则模仿者必须也具有 ANY 授权。
   - 如果同时使用 *target_roles_list* 和 *target_users_list* 子句授予目标用户 SET USER 系统特权，则必须同时使用这两个子句授予模仿者系统特权，并且每个子句的目标列表必须与目标用户的相应子句授权列表相同，或是其列表的超集。例如，如果模仿者和目标用户的目标列表分别包含 User1、User2 及 Role1、Role2，则每个子句的目标列表授权将视为相同。或者，如果模仿者的目标列表授权分别包含 User1、User2、Role1 和 Role2，而目标用户的目标列表授权仅包含 User1 和 Role2，则认为模仿者的目标列表授权是目标用户列表的超集。
   - 如果已使用单个目标列表子句授予目标用户 SET USER 系统特权，则模仿者的目标列表必须与目标用户的列表相同，或是其列表的超集。例如，模仿者和目标用户的 *target_user_list* 均包含 User1 和 User2（相同），或模仿者列表包含

User1 和 User2，而目标用户列表包含 User2，则 User1、User2（模仿者列表）是 User2（目标用户列表）的超集。

- 根据定义，用户可以始终模仿其自身。因此，如果授予目标用户模仿模仿者的权限，将不会违反模仿者的“必须相同或为超集”的条件要求。例如，User3 是模仿者，而 User4 是目标用户。User3 的 *target_user_list* 包含 User4 和 User5。User4 的 *target_user_list* 包含 User3 和 User5。如果从目标列表中删除该模仿者，则 User3 的目标列表满足条件要求。

第 1 种情形
假设满足条件 2 和 3，考虑以下情形：

- 共有五个用户：*User1*、*User2*、*User3*、*User4* 和 *User5*。
- 存在两个角色：*Role1* 和 *Role2*。
- 使用 ANY 子句向 *User1* 授予了 SET USER 系统特权。
- 使用针对 *User1* 和 *User4* 的 *target_users_list* 子句向 *User2* 授予了 SET USER 系统特权。
- 使用针对 *User1*、*User2*、*User4* 和 *User5* 的 *target_users_list* 子句以及针对 *Role1* 和 *Role2* 的 ANY WITH ROLES *target_roles_list* 子句向 *User3* 授予了 SET USER 系统特权。
- 使用 ANY 子句以及针对 *Role1* 的 *target_roles_list* 子句向 *User4* 授予了 SET USER 系统特权。
- 使用针对 *User4* 的 *target_users_list* 子句和针对 *Role1* 的 ANY WITH ROLES *target_roles_list* 向 *User5* 授予了 SET USER 系统特权。

由于 *User1* 和 *User4* 均使用 ANY 子句被授予 SET USER 系统特权（条件 4），因此，可成功模仿 *User2*、*User3* 和 *User5*。

由于 *User1* 和 *User4* 均使用 ANY 子句被授予特权，因此，可相互进行模仿（条件 4）。

User2、*User3* 和 *User5* 无法模仿 *User1* 或 *User4*，因为没有使用 ANY 子句授予他们特权（条件 4）。

User2 无法模仿 *User3* 或 *User5*，这是因为：

- 未授予 *User2* 模仿这些用户的权限（条件 1）。
- 未使用 *target_roles_list* 子句向 *User2* 授予 SET USER 系统特权（条件 4）。

User3 可成功模仿 *User2*，这是因为：

- 通过 *target_users_list* 子句为 *User3* 授予模仿 *User2* 的权限（条件 1）。
- 针对 *User3* 的 *target_users_list* 子句是 *User2* 的超集（条件 4）。虽然已使用 *target_role_list* 子句授予 *User3* 权限，但也无需满足模仿 *User2* 的要求，因为没有授予后者相同的权限。

User3 可成功模仿 *User5*，这是因为：

- 通过 *target_users_list* 子句为 *User3* 授予模仿 *User5* 的权限（条件 1）。
- 针对 *User3* 的 *target_users_list* 子句列表是 *User5* 的超集（条件 4）。
- 针对 *User3* 和 *User5* 的 *target_roles_list* 子句列表是等效的（条件 4）。

User5 无法模仿任何其他用户，因为：

- 已使用 ANY 子句向 *User1* 和 *User4* 授权（条件 4）。
- 已使用 *target_users_list* 子句向 *User2* 和 *User3* 授权，该子句不是向 *User5* 授权的子集（条件 4）。
- 使用不是子集的 *target_roles_list* 子句向 *User3* 进行了授权（条件 4）。

第 2 种情形
假设满足条件 1 和 4，考虑以下情形：

- 存在两个用户：*User6* 和 *User7*。
- 存在两个角色：*Role4* 和 *Role5*。
- 已使用 WITH ADMIN OPTION 子句为 *User6* 授予 *Role4*、使用 WITH ADMIN ONLY OPTION 子句授予 *Role5*，并使用 WITH ADMIN OPTION 子句授予 MANAGE ANY USER 系统特权。
- 已使用 WITH ADMIN OPTION 子句为 *User7* 授予 *Role4* 并使用 WITH NO ADMIN OPTION 子句授予 *Role5*。

User6 可成功模仿 *User7*，这是因为：

- *User6* 和 *User7* 都被授予了 *Role4* 和 *Role5*。是否向 *User6* 授予其它特权（MANAGE ANY USER 系统特权）并不重要（条件 2）。
- 为 *User6* 授予 *Role4*，以及与 *User7* 相同的管理权限。为 *User6* 授予 *Role5*，以及比 *User7* 更高的管理权限（条件 3）。

User7 无法模仿 *User6*，这是因为：

- 为 *User7* 授予了 *Role4* 和 *Role5*，但未授予 MANAGE ANY USER 系统特权（条件 2）。
- 为 *User7* 授予了 *Role5*，以及比 *User6* 更低的管理权限（条件 3）。

第 3 种情形
考虑以下情形：

- 存在三个用户：*User8*、*User9* 和 *User10*。
- 存在两个角色：*Role5* 和 *Role6*。
- 已使用 WITH ADMIN OPTION 子句为 *User8* 授予 *Role5*，并使用 WITH ADMIN OPTION 子句授予 MANAGE ANY USER 系统特权。
- 已使用 WITH NO ADMIN OPTION 子句为 *User9* 和 *User10* 授予 *Role5*。
- 已使用 *target_users_list* 子句为 *User8* 授予 SET USER 系统特权来模仿 *User9* 和 *User10*。

- 已使用 *target_users_list* 子句为 *User9* 授予 SET USER 系统特权来模仿 *User10*。

User8 可成功模仿 *User9*，这是因为：

- 通过 *target_users_list* 子句为 *User8* 授予模仿 *User9* 的权限（条件 1）。
- 针对 *User8* 的 *target_users_list* 子句列表是 *User9* 的超集（条件 4）。
- *User8* 和 *User9* 均被授予 *Role5*，但相比 *User9*，向 *User8* 授予的对该角色的管理权限更高（条件 2 和 3）。

User8 可成功模仿 *User10*，这是因为：

- 为 *User8* 授予模仿 *User10* 的权限（条件 1）。
- 由于未向 *User10* 授予 SET USER 系统特权，因此，要求 4 不适用。
- *User8* 和 *User10* 均被授予 *Role5*，以及对该角色相同的管理权限（条件 2 和 3）。

User9 无法模仿 *User8*，这是因为：

- 没有为 *User9* 授予模仿 *User8* 的权限（条件 1）。
- 虽然 *User8* 和 *User9* 均被授予 *Role5*，但相比 *User8*，向 *User9* 授予的对该角色的管理权限较少（条件 3）。

条件验证在执行 SETUSER 语句时进行，而不是在授予 SET USER 系统特权时进行。如果用户在发出 SETUSER 语句时不满足任何条件，则将出现权限被拒绝消息，并且不会开始模仿。

向用户授予 SET USER 系统特权

允许一位用户模仿数据库中的另一位用户。无论是否具有管理权限，均可授予此系统特权。

前提条件

- 已授予 SET USER 系统特权以及管理权限。
- 每个指定目标用户 (target_users_list) 都是具有登录口令的现有用户角色或用户扩展角色。
- 每个指定目标角色 (target_roles_list) 都必须是现有用户扩展角色或用户定义角色。

过程

可授予用户模仿数据库中任意用户的权限 (ANY)、仅模仿特定用户的权限 (*target_users_list*)，或模仿特定角色成员的权限 (ANY WITH ROLES *target_roles_list*)。仅当使用 ANY 子句时才能授予 SET USER 系统特权的管理权限。

如果未指定子句，则缺省情况下使用 ANY。

重新向用户授予 SET USER 系统特权时，授予行为的影响是累积的。

如果使用 ANY 子句时未指定管理子句，则缺省使用 WITH NO ADMIN OPTION。

对于 *target_users_list* 或 *target_roles_list* 子句，WITH NO ADMIN OPTION 是唯一有效的管理子句。

要授予 SET USER 系统特权，请执行下列语句之一：

授予类型	语句
用于模仿任意数据库用户的系统特权 (具有全部管理权限)	**GRANT SET USER** (**ANY**) TO *user_ID [,...]* **WITH ADMIN OPTION**
用于模仿任意数据库用户的系统特权 (只具有管理权限)	**GRANT SET USER** (**ANY**) TO *user_ID [,...]* **WITH ADMIN ONLY OPTION**
用于模仿任意数据库用户的系统特权 (不具有管理权限)	**GRANT SET USER** (**ANY**) TO *user_ID [,...]* **WITH NO ADMIN OPTION**
用于模仿 指定用户的系统特权	**GRANT SET USER** (*target_users_list*) TO *user_ID [,...]*
用于模仿 指定角色中任意成员的系统特权	**GRANT SET USER** (**ANY WITH ROLES** *target_roles_list*) TO *user_ID [,...]*
用于模仿指定用户和指定角色的成员的系统特权	**GRANT SET USER** (*target_users_list*), (**ANY WITH ROLES** *target_roles_list*) TO *user_ID [,...]*

示例：

以下两条语句均授予 *Sam* 模仿任意数据库用户的权限：

```
GRANT SET USER (ANY) TO Sam
or
GRANT SET USER TO Sam
```

以下语句授予 *Bob* 和 *Jeff* 模仿 *Mary*、*Joe* 和 *Sue*（仅限这三者）的权限。

```
GRANT SET USER (Mary, Joe, Sue) TO Bob, Jeff
```

以下语句授予 *Mary* 模仿 *Sales1* 角色的任意成员的能力：

```
GRANT SET USER (ANY WITH ROLES Sales1) TO Mary
```

以下语句授予 *Sarah* 模仿 *Joe* 或 *Sue*，或者模仿 *Sales2* 角色任意成员的权限：

```
GRANT SET USER (Joe, Sue), (ANY WITH ROLES Sales2) TO Sarah
```

以下语句授予 *Joan* 模仿 *Marketing1* 或 *Marketing2* 角色的任意成员的权限：

```
GRANT SET USER (ANY WITH ROLES Marketing1, Marketing2) TO Joan
```

另请参见

- GRANT SET USER 语句 （第 252 页）

开始模仿其他用户

允许某位用户采用其他用户的具体角色和系统特权（模仿）。模仿将一直有效，直到被终止或当前会话结束。

前提条件

模仿者和目标用户满足模仿的全部要求。请参见“了解模仿要求”。

过程

必要条件是在执行 SETUSER 命令时进行验证的，而不是在授予 SET USER 系统特权时验证。执行 SETUSER 命令时，如果模仿用户不能满足所有的必要条件，将显示消息权限被拒绝，而且不会开始模仿。然而，如果在执行后续 SETUSER 时满足所有必要条件，则会开始进行模仿。

发出 SETUSER 语句并开始模仿后，模仿将一直有效，直到您手动终止模仿、开始模仿其他用户或当前会话结束为止。在用户模仿其他用户时，可以向模仿者或被模仿者授予或撤消角色和特权及其相关的管理权限，只要这样做不违反模仿所遵守的必要条件即可。如果授予或撤消操作违反条件，则会出现一条错误消息，且语句将失败。SAP 建议在完成所需任务后立即终止模仿。

在命令提示符处键入：

```
SETUSER userID
```

另请参见

- SETUSER 语句 （第 275 页）
- 模仿要求 （第 91 页）

验证用户的当前模仿状态

成功的模仿将一直有效，直到被手动终止或会话终止。

要验证模仿的当前状态，请在发出 SETUSER 命令的计算机上执行以下命令：

```
SELECT CURRENT USER
```

此命令会返回被计算机识别为当前已登录用户的用户名称。如果它是计算机的预期用户，则在该计算机上不会出现活动的模仿。如果出现意外的用户名，则代表计算机上当前正在被模仿的用户。

示例
在 Joe 登录的连接上，执行：

```
> select current user
> go
current user
------------------------------------------------------------------
------------------------------------------------------------
Joe

(1 row affected)

>setuser mary
>go
>select current user
> go
current user
------------------------------------------------------------------
------------------------------------------------------------
Mary
```

停止模仿其他用户

结束模仿计算机上的其他用户。一旦开始模仿其他用户，便一直有效，直到模仿被终止或当前会话结束。

前提条件

SETUSER 命令是从其启动的同一连接中发出的。

过程

在命令提示符处键入：

```
SETUSER
```

另请参见

- SETUSER 语句 （第 275 页）

撤消用户的 SET USER 系统特权

移除某一用户模仿其他用户和管理 SET USER 系统特权的权限。

前提条件

已授予 SET USER 系统特权以及管理权限。

过程

可使用不同子句向某位用户多次授予 SET USER 系统特权。例如，使用 ANY 子句为 `User1` 授予一次 SET USER 系统特权，然后再使用 target_users_list 子句授予一次该

特权。在多次授予的情况下，必须使用 GRANT 所用的同一子句格式来进行撤消。如果使用 ANY 子句撤消 User1 的系统特权，使用 *target_users_list* 子句进行的授予仍生效。实际效果是 User1 现在只能够模仿 *target_users_list* 中的用户。或者，如果使用 *target_users_list* 子句撤消 User1 的系统特权，使用 ANY 子句进行的授予仍生效。此时的实际效果是 User1 可继续模仿数据库中的任意用户。

注意： 以下示例假定 User1 满足成功模仿所需的所有条件。

要撤消 SET USER 系统特权，请执行下列语句之一：

撤消类型	说明
仅系统特权 的管理权限	**REVOKE ADMIN OPTION FOR SET USER** (**ANY**) **FROM** *user_ID [,...]*
用于模仿任意数据库用户的 系统特权，包括 管理权限	**REVOKE SET USER** FROM**FROM** *user_ID [,...]*
用于模仿指定角色的 系统特权	**REVOKE SET USER** (*target_users_list*) **FROM** *user_ID [,...]*
用于模仿指定角色的 系统特权	**REVOKE SET USER** (**ANY WITH ROLES** *target_roles_list*) **FROM** *user_ID [,...]*

示例：

以下两条语句将移除 *Sam* 模仿任意数据库用户的权限：

```
REVOKE SET USER (ANY) FROM Sam
or
REVOKE SET USER FROM Sam
```

以下语句仅移除 *Frank* 对 SET USER 系统特权的管理权限。*Frank* 可继续模仿数据库中的任意用户。

```
REVOKE ADMIN OPTION FOR SET USER (ANY) FROM Frank
```

以下语句移除 *Bob* 和 *Jeff* 模仿 *Mary*、*Joe* 和 *Sue*（仅限这三者）的能力。

```
REVOKE SET USER (Mary, Joe, Sue) FROM Bob, Jeff
```

以下语句移除 *Mary* 模仿 *Sales1* 角色任意成员的能力：

```
REVOKE SET USER (ANY WITH ROLES Sales1) FROM Mary
```

以下语句移除 *Sarah* 模仿 *Joe* 或 *Sue*，或者模仿 *Sales2* 角色任意成员的能力：

```
REVOKE SET USER (Joe, Sue), (ANY WITH ROLES Sales2) FROM Sarah
```

以下语句移除 *Joan* 模仿 *Marketing1* 或 *Marketing2* 角色任意成员的能力：

```
REVOKE SET USER (ANY WITH ROLES Marketing1, Markeing2) FROM Joan
```

另请参见

- REVOKE SET USER 语句 （第 267 页）

用户

用户管理工作包括创建和删除用户 ID 以及管理口令。

DBA 用户

新建 SAP Sybase IQ 数据库时，DBA 用户是所创建的缺省用户。

最初，DBA 用户的口令设置为 "sql"。要在数据库创建过程中覆盖缺省用户名或口令，请将 **CREATE DATABASE** 语句与 DBA USER 或 DBA PASSWORD 子句一起使用。

注意： 如果选择在数据库创建过程中不覆盖缺省口令，SAP 强烈建议您在此之后尽快执行此操作。

缺省情况下，系统会自动授予 DBA 用户对 SYS_AUTH_DBA_ROLE 角色的管理权限，进而授予对 SYS_AUTH_SA_ROLE 和 SYS_AUTH_SSO_ROLE 角色的管理权限。将所有这些角色合并在一起，便相当于向 DBA 用户授予了他在数据库中的所有系统特权和对象级特权，从而允许 DBA 在数据库中执行任何活动：创建表、更改表结构、创建新用户 ID、撤消用户的特权，等等。

为确保数据库的安全性和责任性，请避免将通用名称（如 "dba"）用作第一个用户 ID。请改为具有强口令的真实用户登录名。

用户授予 SYS_AUTH_DBA_ROLE 角色
某些情况下，可以删除 SYS_AUTH_DBA_ROLE 角色的基础角色，并撤消 SYS_AUTH_SA_ROLE 和 SYS_AUTH_SSO_ROLE 角色的基础系统特权。但 SAP Sybase IQ 文档假定 DBA 用户是数据库管理员，并保留缺省授予的所有基础角色和系统特权。

为防止活动的 DBA 用户丢失口令，请创建一个或多个额外 DBA 帐户（具有随机生成的用户名和口令），并锁定这些证书。如果活动的 DBA 口令丢失，则使用其中一个额外证书登录到该 DBA 帐户，并重置原始帐户口令。

添加新用户
DBA 可向数据库添加新用户。随后为新用户授予对数据库执行已授权任务的特权。虽然可将 DBA 职责移交给其他用户 ID，但由于 DBA 具有 SYS_AUTH_DBA_ROLE 角色，因而仍由它来负责数据库的全面管理。

然后，DBA 可以创建数据库对象并为其它用户 ID 指派这些对象的所有权。

区分大小写数据库中的 DBA 用户 ID
用户 ID 和口令是数据库对象。

更改 DBA 口令
所有数据库的 DBA 用户的缺省口令都是 `sql`。更改此口令以防止对数据库的非授权访问。

前提条件

CHANGE PASSWORD 系统特权。

提示： 如果使用 **dbisql**，可将授予的特权放置在命令文件中以供参考，这样您可以在需要时修改或重新运行，以便重新创建特权。

过程
要更改用户口令，请执行：

```
ALTER USER userID
IDENTIFIED BY password
```

另请参见
- 用户 ID 和口令区分大小写 （第 101 页）
- ALTER USER 语句 （第 218 页）

超级用户
超级用户可以执行任何系统特权和管理任何角色；他们可以在系统中执行任何特许操作。基于角色的安全性不需要超级用户来维护数据库；DBA 用户可能不是超级用户。

缺省情况下，DBA 用户可执行任何系统特权，但由于可能无法管理所有用户定义的角色，不将该用户视为真正的超级用户。SAP Sybase IQ 不会自动为新数据库或迁移的数据库创建超级用户。

要创建超级用户，请创建一个用户，然后将 SYS_AUTH_DBA_ROLE 兼容性角色授予该用户。

注意： 如果迁移了 SYS_AUTH_DBA_ROLE，则必须手动授予 SYS_AUTH_DBA_ROLE 的所有基础缺省系统特权以及管理权限，从而创建超级用户。

要维护超级用户状态，创建超级用户后，必须将所有新用户扩展角色和用户定义角色授予超级用户，同时授予管理权限。

为了使 DBA 用户能够充当超级用户，必须将所有新用户扩展角色和用户定义角色授予 DBA 用户，同时授予管理权限。

可以角色管理员或全局角色管理员的形式来授予管理权限。

提高口令安全性

口令在任何数据库安全系统中都是一个重要部分。有几种方法可以提高口令安全性。

- **实现登录策略** – 控制口令更改的频率、指定锁定帐户之前所允许的登录尝试次数，或者强制执行口令到期。请参见登录策略。
- **实现最小口令长度** – 缺省情况下，对口令的长度没有任何限制。要实现更高的安全性，可以对所有新口令规定最小长度要求，不允许使用短（因而容易被猜到的）口令。建议的最短长度为 6。请参见 MIN_PASSWORD_LENGTH。
- **实现口令规则** – 实现高级口令规则，其中包括要求在口令中使用某些类型的字符、不允许口令重用和为口令设置有效期。创建新用户 ID 或更改口令时，会进行规则校验。请参见 VERIFY_PASSWORD_FUNCTION。

另请参见

- 登录策略 （第 106 页）
- VERIFY_PASSWORD_FUNCTION 选项 （第 282 页）
- MIN_PASSWORD_LENGTH 选项 （第 285 页）

数据库中的口令

从版本 15.0 开始，SAP Sybase IQ 使用 SHA256 来散列口令。口令以 UTF-8 形式存储。

创建或更改口令时，口令先被转换为 UTF-8，然后再散列并存储在数据库中。如果数据库被卸载和重装到带有不同字符集的数据库，则现有口令将继续有效。如果服务器不能将客户端的字符集转换为 UTF-8，SAP 建议采用由 7 位 ASCII 字符组成的口令，因为其它字符可能会无法正常工作。

用户 ID 和口令区分大小写

口令的区分大小写的处理方式与其它标识符有所不同。

在 SAP Sybase IQ 和 SAP Sybase SQL Anywhere® 中，新建数据库中的所有口令均区分大小写，与数据库是否区分大小写无关。缺省用户 ID 为 DBA，该用户的口令为小写的 *sql*。

重建现有数据库时，SAP Sybase IQ 和 SQL Anywhere 按以下条件确定口令的大小写：

- 如果数据库最初是在不区分大小写的数据库中输入的，则口令会依然不区分大小写。
- 如果口令最初是在区分大小写的数据库中输入的，则大写和混合大小写的口令依然区分大小写。如果口令全部以小写输入，则口令不区分大小写。
- 对现有口令和新口令进行的更改均区分大小写。

在 SAP Adaptive Server® Enterprise 中，用户 ID 和口令的区分大小写特性遵循服务器的区分大小写特性。

创建新用户

创建一个新用户 ID。

前提条件

MANAGE ANY USER 系统特权。

过程

要创建新用户，请执行：

```
CREATE USER userID
IDENTIFIED BY password
```

示例：

下面的语句将向数据库中添加口令为 `welcome` 的用户 ID `Joe`：

```
CREATE USER Joe
IDENTIFIED BY welcome
```

另请参见

- CREATE USER 语句 （第 233 页）

删除用户

从数据库中删除用户 ID。

前提条件

- 需要 MANAGE ANY USER 系统特权。
- 待删除的用户不具有任何数据库对象且当前未与数据库连接。

过程

如果待删除的用户定义了任何外部登录，则外部登录将在删除过程中一并删除。但不会删除远程服务器上的任何相关对象。
要删除用户，请执行：

```
DROP USER userID
```

注意：

- 删除用户时，将删除由此用户授予的所有权限。
- 如果待删除的用户在数据库中拥有对象，将出现下列错误消息，并且命令会失败：

```
Cannot drop a user that owns tables in runtime system
SQLCODE=-128, ODBC 3  State="42000"
    Line 1, column 1
```

示例：

此语句从数据库中删除用户 ID `Joe`：

```
DROP USER Joe
```

另请参见

- DROP USER 语句 （第 238 页）

更改用户口令

更改其他用户的口令。

前提条件

需要 CHANGE PASSWORD 系统特权。

过程

您可以设置口令规则（**MIN_PASSWORD_LENGTH** 选项）并验证指派的新口令是否符合这些规则（**VERIFY_PASSWORD_FUNCTION** 选项）。例如，您可能要求口令必须包含一个数字或不能是用户 ID。

要更改用户口令，请执行：

```
ALTER USER user_ID
IDENTIFIED BY password
```

示例：

下面的语句将为用户 M_Smith 指派新口令 P&ssW0rd：

```
ALTER USER M_Smith IDENTIFIED BY P&ssW0rd
```

另请参见

- 用户 ID 和口令区分大小写 （第 101 页）
- ALTER USER 语句 （第 218 页）
- VERIFY_PASSWORD_FUNCTION 选项 （第 282 页）
- MIN_PASSWORD_LENGTH 选项 （第 285 页）

将用户扩展角色转换回用户

可以将用户扩展角色转换回常规用户。

前提条件

具有对要转换的用户扩展角色的管理权限。

过程

该用户会保留授予用户扩展角色的所有登录特权、系统特权及角色。该用户仍然是其扩展为角色后所创建的对象的所有者。可以立即撤消用户扩展角色的任意成员。

无论何时，都必须分别针对每个角色指定最小数量（由 **MIN_ROLE_ADMINS** 数据库选项定义）的具有登录口令的角色或全局角色管理员。将用户扩展角色转换回用户时，所有用户扩展角色的相关角色都必须继续满足该最低要求，否则转换将失败。

要将用户扩展角色转换回用户，请执行下列语句之一：

转换条件	语句
未将角色 授予任何成员。	**DROP ROLE FROM USER** *role_name*
已将角色 授予成员。	**DROP ROLE FROM USER** *role_name* **WITH REVOKE**

另请参见

- DROP ROLE 语句 （第 237 页）

永久锁定用户帐户

要永久锁定用户帐户，必须为帐户指派将 locked 选项设置为 ON 的登录策略。一旦禁用，用户将无法连接到 SAP Sybase IQ 服务器。

前提条件

- 具有 MANAGE ANY LOGIN POLICY 系统特权以便创建或变更登录策略。
- 具有 MANAGE ANY USER 系统特权以便为用户指派登录策略。

过程

1. 创建 LOCKED 选项设置为 ON 的登录策略。
2. 执行 **ALTER USER** 命令将登录策略指派给要禁用的用户帐户。

   注意： 在为用户指派登录策略时，不能在同一 **ALTER USER** 命令中指定多个用户名。

示例:

下面命令将创建名为 `lp_locked_users` 且 `LOCKED` 选项设置为 ON 的新登录策略：

```
CREATE LOGIN POLICY lp_locked_users locked=ON
```

以下命令将 `lp_locked_users` 登录策略指派给用户 `John` 和 `Mary`。`John` 和 `Mary` 无法再次登录。

```
ALTER USER john LOGIN POLICY lp_locked_users
ALTER USER Mary LOGIN POLICY lp_locked_users
```

另请参见

- 用户帐户自动解锁 （第 106 页）
- ALTER USER 语句 （第 218 页）
- CREATE LOGIN POLICY 语句 （第 224 页）

解除用户帐户锁定

解除用户帐户锁定。

前提条件

需要 MANAGE ANY USER 系统特权。

过程

执行下列操作之一：

帐户锁定原因	任务
用户帐户已锁定，因为该用户帐户被指派到 locked 选项设置为 ON 的登录策略	重新将该用户指派到 locked 选项设置为 OFF 的登录策略。
用户帐户已锁定，因为该用户帐户超出了 MAX_FAILED_LOGIN_ATTEMPTS 或 MAX_DAYS_SINCE_LOGIN 的限制，	使用 RESET LOGIN POLICY 选项发出 **ALTER USER** 语句。强制重置登录策略会将用户的登录设置恢复为登录策略中的原始值。这通常会清除因用户超出失败登录次数或超出自上次登录后的最大天数而隐式设置的所有锁。 **注意：** 重置指派给某个用户的登录策略中的值不会重置指派了相同登录策略的所有用户的值。

示例

假设登录策略 `lp` 的 LOCKED 选项设置为 OFF，本示例会将当前指派给 `John` 的登录策略替换为登录策略 `lp`：

```
ALTER USER john LOGIN POLICY lp
```

假设 `John's` 的帐户因超出 MAX_FAILED_LOGIN_ATTEMPTS 或 MAX_DAYS_SINCE_LOGIN 的限制而被锁定，本示例将强制重置当前指派给 `John` 的登录策略的值：

```
ALTER USER john RESET LOGIN POLICY
```

另请参见

- 用户帐户自动解锁 （第 106 页）
- ALTER LOGIN POLICY 语句 （第 209 页）
- ALTER USER 语句 （第 218 页）

用户帐户自动解锁

如果具有 MANAGE ANY USER 系统特权的所有管理用户由于登录尝试失败而被数据库锁定，则部分或全部数据库服务将发生锁定。

如果某个用户尝试登录的次数超出了登录策略中定义的最大失败登录尝试次数限制 (MAX_FAILED_LOGIN_ATTEMPTS) 值，则该用户帐户将被自动锁定。锁定后，用户帐户必须由已被授予 MANAGE ANY USER 系统特权的用户手动解锁。但是，如果具有 MANAGE ANY USER 系统特权的所有用户均由于登录尝试失败而被锁定，则可能会导致部分或全部数据库服务发生锁定。

为避免发生这种情况，可使用以下登录策略选项：

- **ROOT_AUTO_LOCK_TIME** – 为具有 MANAGE ANY USER 系统特权的用户定义自动解锁周期。可以在根登录策略中将 root_auto_lock_time 设置为较小的值（如 15 分钟）。此值具有一个为期几小时的服务器强制上限。
- **AUTO_UNLOCK_TIME** – 为所有其他用户定义自动解锁周期。在任何登录策略（包括根登录策略）中将 AUTO_UNLOCK_TIME 设置为 UNLIMITED（缺省值）。

配置这些值时需要 MANAGE ANY LOGIN POLICY 系统特权。

根据授予用户的权限，解锁时会对其中一个登录策略选项进行验证。自动解锁仅适用于因登录尝试失败而锁定的帐户，不适用于任何其它原因的帐户锁定。将在登录期间验证用户的锁定状态，如果用户被锁定的时间等于或超过指定的自动解锁周期，则将允许该用户进行登录，同时将 FAILED_LOGIN_ATTEMPTS 计数器重置为零。

另请参见

- 最小角色管理员数 （第 18 页）
- 解除用户帐户锁定 （第 105 页）
- 永久锁定用户帐户 （第 104 页）
- ALTER LOGIN POLICY 语句 （第 209 页）
- ALTER USER 语句 （第 218 页）

登录策略

*登录策略*定义了 SAP Sybase IQ 建立用户连接所遵循的规则。每个登录策略与称为登录策略选项的一组选项相关联。

在任何 Multiplex 服务器上执行的登录管理命令都会自动传播到 Multiplex 中的所有服务器。为获得最佳性能，请对协调器执行这些命令或任何 DDL。

修改根登录策略

可以修改根登录策略的选项值，但不能删除该策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

每个新数据库在创建时都使用称为根策略的缺省登录策略。如果在创建用户帐户时未指定登录策略，则该用户将成为根登录策略的一部分。
要修改根登录策略的选项，请执行：

```
ALTER LOGIN POLICY ROOT {login_policy_options}
```

另请参见

- ALTER LOGIN POLICY 语句 （第 209 页）
- 登录策略选项 （第 226 页）
- Multiplex 登录策略配置 （第 215 页）
- LDAP 登录策略选项 （第 214 页）

创建新登录策略

创建登录策略时未显式设置的任何选项都会从根登录策略继承其值。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

登录策略名必须唯一。如果要添加的登录策略名已存在，则会显示错误消息。
要创建新登录策略，请执行：

```
CREATE LOGIN POLICY policy_name {login_policy_options}
```

示例：

此语句创建 `Test1` 登录策略，同时 PASSWORD_LIVE_TIME 选项设置为 60 天：

```
CREATE LOGIN POLICY Test1
password_life_time=60
```

另请参见

- CREATE LOGIN POLICY 语句 （第 224 页）
- 登录策略选项 （第 226 页）
- Multiplex 登录策略配置 （第 215 页）
- LDAP 登录策略选项 （第 214 页）

修改现有登录策略

修改现有登录策略中的选项。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

要更改现有登录策略的选项，请执行：

```
ALTER LOGIN POLICY policy-name {login_policy_options}
```

示例：

此语句更改 `Test1` 登录策略的 LOCKED 和 MAX_CONNECTIONS 选项：

```
ALTER LOGIN POLICY Test1
locked=on
max_connections=5
```

另请参见

- ALTER LOGIN POLICY 语句 （第 209 页）
- 登录策略选项 （第 226 页）
- Multiplex 登录策略配置 （第 215 页）
- LDAP 登录策略选项 （第 214 页）

删除登录策略

无法删除根登录策略或当前指派给用户的登录策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

1. 验证要删除的登录策略当前未指派给任何用户。
2. 执行：

   ```
   DROP LOGIN POLICY policy_name
   ```

另请参见

- DROP LOGIN POLICY 语句 （第 236 页）

创建新用户时指派登录策略

如果创建用户帐户时未指派登录策略，将为此帐户指派根登录策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

创建新用户时指派根登录策略以外的登录策略。每次只能为用户指派一个登录策略。执行：

```
CREATE USER userID
[ IDENTIFIED BY password ]
[ LOGIN POLICY policy-name ]
```

注意： 在将登录策略指派给用户时，不能在同一 **CREATE USER** 命令中指定多个用户 ID。

示例：

此语句创建名为 Joe、口令为 welcome 的用户，并为其指派 Test2 登录策略：

```
CREATE USER Joe
IDENTIFIED BY welcome
LOGIN POLICY Test2
```

另请参见

- CREATE USER 语句 （第 233 页）

为现有用户指派登录策略

向现有 SAP Sybase IQ 用户指派登录策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

1. 执行：

   ```
   ALTER USER userID
   LOGIN POLICY policy_name
   ```

2. 使用户注销后再登录以应用新的登录策略。

另请参见

- ALTER USER 语句 （第 218 页）

用户连接

管理用户连接的方法有若干种。

您可以:

- 限制单个用户的活动登录的数目 - 为用户指派设置 MAX_CONNECTIONS 登录策略选项的登录策略。
- 锁定用户帐户:
  - 显式 – 为用户指派 LOCKED 选项设置为 ON 的登录策略。
  - 隐式 - 为用户指派设置 MAX_FAILED_LOGIN_ATTEMPTS 选项的登录策略。如果用户尝试登录的次数超出设定值，系统将锁定该用户的用户帐户。
- 设置口令到期条件 - 为用户指派设置 PASSWORD_EXPIRY_ON_NEXT_LOGIN 登录策略选项的登录策略。您也可以执行 **CREATE USER** 或 **ALTER USER** 语句，包括 FORCE PASSWORD CHANGE 子句。

为用户指派登录策略或强制更改口令需要 MANAGE ANY USER 系统特权。创建或变更登录策略需要 MANAGE ANY LOGIN POLICY 系统特权。

在失败的登录尝试后阻止连接

在超出登录失败的最大尝试次数后，阻止用户进行连接。

前提条件

- 具有 MANAGE ANY LOGIN POLICY 系统特权以便创建或变更登录策略。
- 具有 MANAGE ANY USER 系统特权以便为用户指派登录策略。

过程

可以将系统设置为：如果用户在尝试输入有效登录证书时超出指定次数，则系统自动锁定帐户。一旦帐户被锁定，用户将无法进行连接，即使随后输入了有效证书，帐户仍保持锁定状态，直到手动解锁为止。MAX_FAILED_LOGIN_ATTEMPTS 登录策略选项控制在用户帐户被锁定前连续失败尝试的次数。您可以在新登录策略或现有登录策略（包括根登录策略）中设置该值，系统随后会将该值应用于指派了该登录策略的所有用户。

1. 要设置 MAX_FAILED_LOGIN_ATTEMPTS 选项，可以创建一个新的登录策略，或修改现有登录策略。
2. 为 MAX_FAILED_LOGIN_ATTEMPTS 选项定义值。
3. 可以根据需要为合适的用户指派登录策略。

示例

以下示例将新建一个名为 `lp` 的登录策略，该策略可以在 5 次失败尝试后自动锁定用户帐户:

```
CREATE LOGIN POLICY lp max_failed_login_attempts=5
```

以下示例将修改名为 exist_lp 的现有登录策略，该策略可以在 5 次失败尝试后自动锁定用户帐户：

```
ALTER LOGIN POLICY lp max_failed_login_attempts=5
```

下面的示例将为用户 John 指派登录策略 lp。为 John 指派 lp 登录策略后，如果连续五次输入无效证书，该用户将无法登录。

```
ALTER USER John LOGIN POLICY lp
```

另请参见

- ALTER LOGIN POLICY 语句 （第 209 页）
- ALTER USER 语句 （第 218 页）
- CREATE LOGIN POLICY 语句 （第 224 页）
- 登录策略选项 （第 211 页）
- LDAP 登录策略选项 （第 214 页）
- Multiplex 登录策略配置 （第 215 页）

创建 DBA 恢复帐户

为生产系统创建一个 DBA 恢复帐户。如果丢失了原始 DBA 帐户口令，DBA 恢复帐户为备份帐户。

1. 使用随机生成的用户名和口令创建一个或多个额外的 DBA 帐户。
2. 在安全位置锁定证书。

另请参见

- CREATE USER 语句 （第 233 页）

使用 DBA 恢复帐户登录

使用 DBA 恢复帐户登录，并重置原始 DBA 帐户口令。

1. 从安全位置检索 DBA 恢复帐户的用户名和口令。
2. 使用恢复帐户登录。
3. 重置原始 DBA 帐户口令。
4. 将 DBA 恢复帐户证书退回到其安全位置。

使用存储过程管理连接

可以使用多种存储过程来管理用户连接。

下表列出了可用于执行各种 SAP Sybase IQ 登录管理功能的过程。

存储过程	作用	所需系统特权
sa_get_user_status	检索所有现有用户的当前状态	MANAGE ANY USER 系统特权才能检索所有现有用户的当前状态。没有 MANAGE ANY USER 系统特权的用户只能检索其当前状态。
sp_expireallpasswords	令所有用户口令立即到期	MANAGE ANY USER 系统特权
sp_iqaddlogin	添加用户，定义其口令，指定登录策略以及下次登录时口令到期	MANAGE ANY USER 系统特权
sp_iqcopyloginpolicy	通过复制现有登录策略创建新登录策略	MANAGE ANY LOGIN POLICY 系统特权
sp_iqdroplogin	删除指定用户	MANAGE ANY USER 系统特权
sp_iqmodifylogin	为给定用户指派登录策略	MANAGE ANY USER 系统特权
sp_iqmodifyadmin	将指定登录策略的某个选项设置为特定值	MANAGE ANY LOGIN POLICY 系统特权
sp_iqpassword	更改自己或其他用户的口令	所有用户都可以运行 **sp_iqpassword** 来更改自己的口令。但是，更改其他用户的口令需要具有 CHANGE PASSWORD 系统特权。

另请参见

- sp_expireallpasswords 系统过程 （第 300 页）
- sp_iqcopyloginpolicy 过程 （第 310 页）
- sp_iqdroplogin 过程 （第 320 页）
- sp_iqmodifyadmin 过程 （第 326 页）
- sp_iqmodifylogin 过程 （第 326 页）
- sp_iqpassword 过程 （第 352 页）
- sp_iqaddlogin 过程 （第 303 页）
- sa_get_user_status 系统过程 （第 295 页）

管理连接使用的资源

通过构建一个由用户和角色组成的集合，您可管理针对数据库的权限。数据库安全与管理的另一方面是对单个用户可以使用的资源进行限制。

例如，您可能想防止因某个连接占用过多可用内存或 CPU 资源而降低其他数据库用户的速度。

控制用户资源的数据库选项

控制资源的数据库选项称为*资源调控器*。使用 **SET OPTION** 语句设置数据库选项。

- **CURSOR_WINDOW_ROWS** – 定义缓冲区中的游标行数。
- **MAX_CARTESIAN_RESULT** – 限制包含笛卡尔连接的查询结果的行数。
- **MAX_IQ_THREADS_PER_CONNECTION** – 设置用于 IQ 操作的连接的可用处理线程数。
- **TEMP_CACHE_MEMORY_MB** – 设置 SAP Sybase IQ 临时存储的高速缓存大小。（建议使用服务器选项 **-iqtc** 设置临时高速缓存大小。）
- **QUERY_TEMP_SPACE_LIMIT** – 限制可用于任何一个查询的临时 dbspace 量。
- **QUERY_ROWS_RETURNED_LIMIT** – 通知查询优化程序拒绝可能消耗过多资源的查询。如果优化程序估计查询结果集将超出此选项的值，优化程序将拒绝该查询并返回错误消息。

以下数据库选项会影响引擎，但对 SAP Sybase IQ 的影响有限：

- **JAVA_HEAP_SIZE** – 基于每个连接设置分配给 Java 应用程序的内存的最大大小（字节）。
- **MAX_CURSOR_COUNT** – 限制一个连接的游标数量。
- **MAX_STATEMENT_COUNT** – 限制一个连接的预准备语句的数量。

数据库选项设置不能通过角色结构继承。

另请参见

- SET OPTION 语句 （第 273 页）

使用视图和过程的安全性

您可以使用视图和存储过程来对特权进行量身定制，以适应企业需要。

对于安全性要求很高的数据库，直接对表定义特权有其局限性。授予用户的对表的任何特权都会应用于整个表。您可能需要更精确地指派特权，而不是逐表进行指派。例如：

- 您不想将 employee 表中所存储的个人信息或敏感信息的访问权授予那些需要访问该表其它部分的用户。
- 您可能想要授予销售代表对包含其销售电话记录说明的表的更新特权，但此特权仅允许更新其自己的电话。

视图提供了定制的安全性

使用视图授予用户对表的一部分的访问权。

您可以按行或列来定义可访问表的哪些部分。例如，您可能想要禁止一组用户查看 Employees 表的 Salary 列，或者可能只想允许用户查看自己创建的表的行。

示例 1

销售经理需要访问数据库中有关该部门员工的信息。但是，该经理没有理由访问有关其它部门员工的信息。

为销售经理创建用户 ID，创建可提供其所需信息的视图，并为此销售经理用户 ID 授予相应特权。

1. 以具有 MANAGE ANY USER 系统特权的用户的身份使用 **GRANT** 语句创建新用户 ID。DBA 是 SQL 关键字，因此需要用引号将其括起来。

```
CONNECT "DBA"
IDENTIFIED by sql;
GRANT CONNECT
TO SalesManager
IDENTIFIED BY sales
```

2. 定义一个只查看销售部门员工的视图。将该表标识为 “DBA”.Employees，并将该表的所有者显式标识出来，以便 SalesManager 用户 ID 能够使用该视图。否则，当 SalesManager 使用该视图时，**SELECT** 语句会引用该用户 ID 不能识别的表。

```
CREATE VIEW emp_sales AS
SELECT EmployeeID, GivenName, Surname
FROM "DBA".Employees
WHERE DepartmentID = 200
```

3. 授予 SalesManager 查看该视图的特权。使用授予对表的特权时使用的命令授予对视图的特权。

```
GRANT SELECT
ON emp_sales
TO SalesManager
```

示例 2

该示例创建一个允许销售经理查看销售订单摘要的视图。定义此视图需要有来自多个表的信息：

1. 创建视图。

```
CREATE VIEW order_summary AS
SELECT OrderDate, Region, SalesRepresentative
FROM "GROUPO".SalesOrders
    KEY JOIN "GROUPO".Customers
```

2. 授予 SalesManager 查看该视图的特权。

```
GRANT SELECT
ON order_summary
TO SalesManager
```

3. 要检查该过程是否正确执行，请连接到 SalesManager 用户 ID，然后查看您创建的视图：

```
CONNECT SalesManager IDENTIFIED BY sales ;
SELECT * FROM "GROUPO".emp_sales ;
SELECT * FROM "GROUPO".order_summary ;
```

未授予 SalesManager 查看基础表的特权。因此，这些命令将生成特权错误：

```
SELECT * FROM "DBA".Employees ;
SELECT * FROM "DBA".SalesOrders;
```

这些示例说明了如何使用视图来定制 SELECT 特权。您可以使用相同的方法授予对视图的 INSERT、DELETE 和 UPDATE 特权。

使用视图的准则

对于用于创建视图的 **SELECT** 语句以及能否在视图中插入数据、从视图中删除数据或更新视图，都存在特定的限制。

对于 SELECT 语句的限制

不能在 **SELECT** 查询中使用 ORDER BY 子句。关系表的一个特性是行或列的顺序没有特殊意义，而使用 ORDER BY 子句将在视图的行上强加顺序。可以在视图定义中使用 GROUP BY 子句、子查询和连接。

只在顶级 **SELECT** 列表中支持标量值子查询（视图、派生表或子查询均不支持）。有时顶级 **SELECT** 的 FROM 子句中使用的视图或派生表非常简单，可以“展平”到顶级 **SELECT**。因此，之前的规则实际仅针对子查询、未展平的视图以及未展平的派生表强制执行。例如：

```
CREATE VIEW test_view AS SELECT testkey,(SELECT COUNT(*) FROM
tagtests WHERE tagtests.testkey = testtrd.testkey ) FROM
testtrd
```

```
SELECT * FROM test_view
Msg 21, Level 14, State 0:
SQL Anywhere Error -1005004: Subqueries are allowed only as arguments
of
comparisons, IN, and EXISTS,
-- (opt_Select.cxx 2101)
```

要规划一个视图，可以调整 **SELECT** 查询本身，直到其以所需格式提供完全符合需要的结果。调整好 **SELECT** 语句之后，即可在查询前面添加一个短语来创建视图。例如：

```
CREATE VIEW viewname AS
```

插入和删除视图的准则

有些视图允许使用 **UPDATE**、**INSERT** 和 **DELETE** 语句，有些视图不允许，具体取决于其关联的 **SELECT** 语句。

不能在包含下面内容的视图中执行更新、插入或删除：

- 集合函数，如 **COUNT(*)**
- **SELECT** 语句中的 GROUP BY 子句
- **UNION** 操作

在所有这些情况中，无法将 **UPDATE**、**INSERT** 或 **DELETE** 转换成对基础表的操作。

警告！ 请不要删除 dbo 用户 ID 拥有的视图，该用户 ID 拥有系统对象。删除此类视图或将它们转化为表可能导致意外的问题。

使用过程以提供定制安全性

过程可以限制用户可执行的操作。

用户可以拥有对过程的 EXECUTE 特权，而无需对过程所作用的表拥有任何特权。

缺省情况下，使用过程所有者的特权来执行过程。对于更新表的过程，如果过程所有者对表具有 UPDATE 特权，该用户就可以执行该过程。过程所有者可以通过为 CREATE/ALTER PROCEDURE 语句指定 SQL SECURITY INVOKER，将过程限制为使用执行该过程的用户的特权来执行。

设置基于任务的安全限制

不允许对基础表进行任何访问，并授予用户或角色执行特定存储过程的特权。该方法严格定义了如何控制数据库修改。

允许具有特定特权的用户使用 SAP Sybase IQ 系统过程管理特定任务：

1. 为要执行的每一组授权任务创建一个角色，然后为该角色授予相应的系统特权。
2. 将上述每个角色授予给一个常见角色。
3. 将执行授权任务 IQ 过程的 EXECUTE 特权授予相应的角色。
4. 当创建一个新用户并准备为其授予授权任务时，可将针对每个授权任务创建的角色授予该用户。

授予用户运行相关存储过程的特权

授予用户运行存储过程所需的系统特权。由于大多数特权都是通过角色成员资格继承的，因此用户可以从角色继承系统特权以及对 IQ 过程的执行特权。

前提条件

MANAGE ANY USER 或 EXECUTE ANY PROCEDURE 系统特权。

过程

授予用户 `user1` MANAGE ANY USER 系统特权和执行与用户管理相关的过程的特权：

1. 创建角色 USER_ADMIN_GRP：

```
CREATE ROLE USER_ADMIN_GRP
```

2. 向 USER_ADMIN_GRP 角色授予 MANAGE ANY USER 系统特权：

```
GRANT MANAGE ANY USER TO USER_ADMIN_GRP
```

3. 向 USER_ADMIN_GRP 授予对 SAP Sybase IQ 用户管理存储过程的 EXECUTE 特权：

```
GRANT EXECUTE on sp_iqaddlogin
to USER_ADMIN_GRP
GRANT EXECUTE on sp_iqcopyloginpolicy
to USER_ADMIN_GRP
GRANT EXECUTE on sp_iqdroplogin
to USER_ADMIN_GRP
GRANT EXECUTE on sp_iqmodifyadmin
to USER_ADMIN_GRP
GRANT EXECUTE on sp_iqmodifylogin
to USER_ADMIN_GRP
```

4. 将 USER_ADMIN_GRP 角色授予 user1。 user1 将继承 MANAGE ANY USER 系统特权和通过 USER_ADMIN_GRP 角色的成员资格执行指派的 IQ 过程的权限。

```
GRANT ROLE USER_ADMIN_GRP TO user1
```

用于角色访问的相关存储过程

您可以创建授予各种相关存储过程特权的角色。

角色名称	授予的系统特权	存储过程
OPERATOR_GRP	BACKUP DATABASE DROP CONNECTION CHECKPOINT MONITOR ACCESS SERVER LS	sp_iqbackupdetails sp_iqbackupsummary sp_iqconnection sp_iqsysmon
SPACEADMIN_GRP	MANAGE ANY DBSPACE ACCESS SERVER LS	sp_iqdbspace sp_iqdbspaceinfo sp_iqdbspaceobjectinfo sp_iqemptyfile sp_iqestdbspaces sp_iqfile sp_iqobjectinfo sp_iqspaceused

另请参见

- sp_iqbackupdetails 过程 （第 304 页）

- sp_iqbackupsummary 过程 （第 306 页）
- sp_iqconnection 过程 （第 307 页）
- sp_iqdbspace 过程 （第 310 页）
- sp_iqdbspaceinfo 过程 （第 314 页）
- sp_iqdbspaceobjectinfo 过程 （第 317 页）
- sp_iqemptyfile 过程 （第 321 页）
- sp_iqestdbspaces 过程 （第 322 页）
- sp_iqfile 过程 （第 323 页）
- sp_iqobjectinfo 过程 （第 327 页）
- sp_iqspaceused 过程 （第 330 页）
- sp_iqsysmon 过程 （第 332 页）

数据保密性

可使用传输层安全 (TLS) 来实现客户端与 SAP Sybase IQ 服务器或 SAP Sybase IQ 客户端与数据库服务器之间的安全通信。

SAP Sybase IQ 允许加密数据库或列。

Kerberos 验证和列加密支持由单独授权的 SAP Sybase IQ“高级安全性”选项提供。

另请参见

- SAP Sybase IQ 中的列加密 （第 170 页）
- SAP Sybase IQ 中的 FIPS 支持 （第 169 页）

数据库加密和解密

可以对数据库加密，以增大他人破译数据库中数据的难度。可以选择使用简单加密或高度加密来保护数据库的安全。

注意： 如果数据库已加密，则使用 WinZip 等工具对其进行压缩不会使文件明显小于原始数据库文件。

简单加密与高度加密

简单加密
简单加密等效于模糊处理，对于通过使用磁盘实用程序查看文件来破译数据库中数据的人而言，它会增大破译的难度。简单加密不要求使用密钥就可以对数据库加密。

高度加密
对数据库使用高度加密技术后，如果没有密钥（口令），就无法对数据库进行操作和访问。加密算法会对数据库和事务日志文件中包含的信息进行编码，以使信息无法被破译。

在 SAP Sybase IQ 中，数据库管理员对高度加密的以下四个方面有控制权：

- 高度加密状态
- 加密密钥
- 加密密钥的保护
- 加密算法

支持的高度加密算法
用于实现 SAP Sybase IQ 高度加密的算法为 AES：它是一种数据块加密算法，美国国家标准与技术协会（National Institute of Standards and Technology，简称 NIST）选择它作为新的数据块编码器高级加密标准（Advanced Encryption Standard，简称 AES）。

也可以使用 AES_FIPS（128 位）或 AES256_FIPS（256 位）类型指定另外一种经 FIPS 认可的 AES 模块来进行高度加密。在以 -fips 选项启动数据库服务器时，可以运行用 AES、AES256、AES_FIPS 或 AES256_FIPS 高度加密方法加密的数据库，但不能运行用简单加密方法加密的数据库。指定 -fips 时，也可以在服务器上启动未加密的数据库。

必须在所有用于运行使用 AES_FIPS 或 AES256_FIPS 加密的数据库的计算机上都安装 SAP Sybase IQ 安全性组件。

并非所有平台上都可以使用 FIPS 认证的加密。有关受支持平台的列表，请参见 http://www.sybase.com/detail?id=1061806。

注意： 需要单独授予许可的组成部分。

FIPS 认证的加密需要单独的许可。所有高度加密技术受出口法规约束。

数据库加密方法

- **创建加密数据库** – 可使用以下方法：
  - 将初始化实用程序 (iqinit) 与各种选项配合使用来启用高度加密。
    iqinit 实用程序 -ep 和 -ek 选项可以创建采用高度加密的数据库，您可以在提示框或命令行中指定加密密钥。iqinit -ea 选项将加密算法设置为 AES 或 AES256 算法（或者，对于 FIPS 认证的模块，设置为 AES_FIPS 或 AES256_FIPS 算法）。
  - CREATE DATABASE 语句。
- **加密现有数据库** – 虽然无法直接在现有数据库中启用或禁用高度加密，但可以使用以下其中一种方法来实现高度加密：
  - 重建（卸载/重装）现有数据库，并在重建时更改加密状态。可以重建数据库以卸载现有数据库的所有数据和模式。这样做会创建一个新数据库（此时可以更改包括高度加密状态在内的各种设置），并将数据重装到新数据库中。需要知道密钥才能卸载高度加密的数据库。使用以下其中一种方法重建（卸载/重装）数据库：

    - 卸载实用程序 (dbunload)
      使用卸载实用程序 (dbunload) 并指定相应选项来创建新的采用高度加密的数据库。-an 选项创建新的数据库。要在提示框或命令行中指定高度加密和加密密钥，请使用 -ep 或 -ek 选项。-ea 选项将加密算法设置为 AES 或 AES256 算法（或者，对于 FIPS 认证的模块，设置为 AES_FIPS 或 AES256_FIPS 算法）。
    - UNLOAD 和 RELOAD 语句
    - **“卸载数据库向导”**。
  - 可以使用 CREATE ENCRYPTED DATABASE 语句或 CREATE ENCRYPTED FILE 语句。
- **加密表、列和实例化视图** – 请参见 Column and table encryption。

另请参见

- 列和表加密 （第 124 页）

比较 CREATE ENCRYPTED DATABASE 和 CREATE ENCRYPTED FILE 语句

当想要对现有的数据库进行加密时，应使用 CREATE ENCRYPTED DATABASE 语句。仅在想要对需要恢复的数据库进行加密时才能使用 CREATE ENCRYPTED FILE 语句。

执行该语句时不能连接到正在加密的数据库。

CREATE ENCRYPTED FILE 和 CREATE ENCRYPTED DATABASE 语句彼此之间的不同点如下：

- CREATE ENCRYPTED FILE 语句必须针对每个与数据库相关的文件（事务日志、事务日志镜像、dbspace，如果有）单独执行，而 CREATE ENCRYPTED DATABASE 语句自动加密所有与数据库相关的文件。
- CREATE ENCRYPTED DATABASE 语句不能在需要恢复的数据库上使用；CREATE ENCRYPTED FILE 语句则可以做到这一点。
- CREATE ENCRYPTED DATABASE 语句不能在过程、触发器或批处理内部使用。CREATE ENCRYPTED FILE 语句则可以做到这一点。
- CREATE ENCRYPTED DATABASE 语句支持 SIMPLE 加密算法，但 CREATE ENCRYPTED FILE 语句则不支持。

创建加密数据库 (SQL)

配合使用 ENCRYPTED 子句和 CREATE DATABASE 语句，可在数据库创建期间对其进行加密。

前提条件

缺省情况下，您必须具有 SERVER OPERATOR 系统特权。使用 -gu 数据库服务器选项可对所需的特权进行更改。

过程

该任务不同于对现有数据库进行加密。要加密现有数据库，请使用 CREATE ENCRYPTED DATABASE 语句。

警告！ 小心

对于高度加密的数据库，请将密钥的副本保存在安全的位置。如果丢失了加密密钥，则无法访问数据—即使有技术支持人员的协助也是如此。此时必须放弃该数据库并创建一个新的数据库。

1. 在 Interactive SQL 中，连接到现有数据库。
2. 执行包含 ENCRYPTED 子句、KEY 以及 ALGORITHM 选项的 CREATE DATABASE 语句。

成功创建加密数据库。

创建加密数据库（iqinit 实用程序）

可以使用 iqinit 实用程序创建加密数据库。

前提条件

执行此任务没有前提条件。

过程

警告！ 小心

对于高度加密的数据库，请将密钥的副本保存在安全的位置。如果丢失了加密密钥，则无法访问数据—即使有技术支持人员的协助也是如此。此时必须放弃该数据库并创建一个新的数据库。

运行 iqinit 实用程序创建一个数据库。

- 要通过简单加密进行数据库加密，需包括 -ea simple 选项。
- 要通过高度加密进行数据库加密，需包括 -ek 或 -ep 选项以指定加密密钥。

成功创建加密数据库。

下一步

启动或连接到数据库时，必须指定加密密钥。

创建现有数据库的加密副本 (SQL)

可以使用 CREATE ENCRYPTED DATABASE 语句为数据库创建一个加密副本。此语句创建文件副本（在本例中以加密形式创建），而不会覆盖原始数据库文件。

前提条件

缺省情况下，您必须具有 SERVER OPERATOR 系统特权才能执行 CREATE ENCRYPTED DATABASE 语句。使用 -gu 数据库服务器选项可对所需的特权进行更改。

正在加密的数据库不得处于运行状态。

过程

警告！ 小心

对于高度加密的数据库，请将密钥的副本保存在安全的位置。如果丢失了加密密钥，则无法访问数据—即使有技术支持人员的协助也是如此。此时必须放弃该数据库并创建一个新的数据库。

1. 在 Interactive SQL 中，连接到现有的数据库，而不是您正在加密的数据库。
2. 使用 CREATE ENCRYPTED DATABASE 语句对数据库加密。

执行 CREATE ENCRYPTED DATABASE 语句时，不会加密（覆盖）原文件，而是为该文件创建一个加密形式副本。如果存在与此数据库关联的事务日志、事务日志镜像或 dbspace，则也会创建这些文件的加密副本。

解密数据库 (SQL)

可以使用 CREATE DECRYPTED DATABASE 语句对数据库进行解密。此语句创建文件副本（以加密形式创建），而不会覆盖原始数据库文件。

前提条件

缺省情况下，您必须具有 SERVER OPERATOR 系统特权才能执行 CREATE DECRYPTED TABLE DATABASE 语句。使用 -gu 数据库服务器选项可对所需的特权进行更改。

正在加密的数据库不得处于运行状态。

过程

如果有一个需要恢复的数据库，想要对其进行解密以便送给技术支持部门，则必须使用 CREATE DECRYPTED FILE 语句。任何与数据库相关的文件（例如事务日志、事务日志镜像以及 dbspace 文件）必须也要使用此语句进行解密。

1. 在 Interactive SQL 中，连接到要解密的数据库以外的其它数据库。
2. 执行 CREATE DECRYPTED DATABASE 语句。

执行 CREATE DECRYPTED DATABASE 语句时，不会解密（覆盖）原文件，而是为该文件创建一个解密形式副本。如果存在与此数据库关联的事务日志、事务日志镜像或 dbspace，则也会创建这些文件的解密副本。

加密密钥

最好选择一个无法被轻易猜到的加密密钥值。对密钥的长度没有任何限制，但通常密钥越长越好，因为与较长的密钥相比，较短的密钥更易于猜测。同样，组合使用数字、字母和特殊字符会减少他人猜中密钥的几率。

加密密钥始终区分大小写，它们不能包含前导空格、尾随空格或分号。

每次想要启动数据库时都必须提供此密钥。丢失或忘记密钥会导致数据库完全无法访问。

可以选择是在命令提示符处（缺省设置）还是在提示框中输入加密密钥。选择在提示框中输入密钥增加了安全性，因为这样人们根本无法看清密钥。每次当客户端启动数据库时，都必须指定密钥。如果数据库管理员启动数据库，则客户端永远都不需要具有访问密钥的权限。

警告！ 对于高度加密的数据库，请将密钥的副本保存在安全的位置。如果丢失了加密密钥，则无法访问数据—即使有技术支持人员的协助也是如此。此时必须放弃该数据库并创建一个新的数据库。

更改数据库的加密密钥

可以使用 CREATE ENCRYPTED DATABASE 语句更改已加密数据库或已启用表加密的数据库的加密密钥。更改加密密钥不会覆盖现有文件，而是为该文件创建一个使用新密钥进行加密的副本。

前提条件

缺省情况下，您必须具有 SERVER OPERATOR 系统特权才能执行 CREATE ENCRYPTED DATABASE 语句。使用 -gu 数据库服务器选项可对所需的特权进行更改。

过程

使用 CREATE ENCRYPTED DATABASE 语句更改已加密数据库的加密密钥。

加密密钥已更改。

安全性与性能问题

数据库加密后，SAP Sybase IQ 的性能会有所下降。对性能的影响取决于从磁盘读取页或向磁盘写入页的频率，可以通过确保服务器使用足够的高速缓存大小来将这种影响降至最低水平。

可以在启动服务器时使用 -c 选项来增加高速缓存的起始大小。对于支持动态调整高速缓存大小的操作系统，所使用的高速缓存大小可能会受到可用内存量的限制；若要增加高速缓存大小，应增加可用内存量。

列和表加密

如果只想要加密数据库的某些部分，则可以选择加密列或表。

列加密可以随时在任意表中的任意列上执行。表加密要求数据库已经启用了表加密。表加密在数据库创建（初始化）时启用。

- **对表进行加密** – 可使用以下方法：
  - 初始化实用程序 (iqinit)。
  - CREATE DATABASE 语句。
  - ALTER DATABASE 语句。
  - CREATE ENCRYPTED TABLE DATABASE 语句。
- **对列进行加密** – ENCRYPT 函数。
- **对实例化视图进行加密** – ALTER MATERIALIZED VIEW 语句。

列加密

要对数据库中的列进行加密，请使用 ENCRYPT 函数。ENCRYPT 函数对传递给它的值进行加密时所用的算法即用于数据库加密的 AES 高度加密算法。

加密的数据可以使用 DECRYPT 函数进行解密。必须使用 ENCRYPT 函数中指定的那个密钥。这两个函数都会返回 LONG BINARY 值。如果需要其它数据类型的值，可以使用 CAST 函数将值转换为所需的数据类型。

ENCRYPT 和 DECRYPT 函数还支持原始加密。可以将数据库服务器内部的数据加密成可导出到服务器外部并进行解密的格式。

如果数据库用户需要访问解密形式的数据，但您不想让他们访问加密密钥，则可以创建一个使用 DECRYPT 函数的视图。这样用户就可以在不知道加密密钥的情况下访问解密数据。创建使用该表的视图或存储过程时，可以使用 ALTER VIEW 和 ALTER PROCEDURE 语句的 SET HIDDEN 参数来确保用户无法通过查看视图或过程定义访问加密密钥。

列加密示例

以下示例使用触发器对名为 user_info 的表中存储口令的列进行加密。user_info 表的定义如下：

```
CREATE TABLE user_info (
   employee_ID INTEGER NOT NULL PRIMARY KEY,
```

```
   user_name CHAR(80),
   user_pwd CHAR(80) );
```

将两个触发器添加到数据库中，以在添加新用户或更新现有用户口令时对 user_pwd 列中的值进行加密。

- 每当在 user_info_table 中添加新行时，都会触发 encrypt_new_user_pwd 触发器：

```
CREATE TRIGGER encrypt_new_user_pwd
BEFORE INSERT
ON user_info
REFERENCING NEW AS new_pwd
FOR EACH ROW
BEGIN
    SET new_pwd.user_pwd=ENCRYPT(new_pwd.user_pwd, '8U3dkA');
END;
```

- 每当在 user_info 表中更新 user_pwd 列时，都会触发 encrypt_updated_pwd 触发器：

```
CREATE TRIGGER encrypt_updated_pwd
BEFORE UPDATE OF user_pwd
ON user_info
REFERENCING NEW AS new_pwd
FOR EACH ROW
BEGIN
    SET new_pwd.user_pwd=ENCRYPT(new_pwd.user_pwd, '8U3dkA');
END;
```

向数据库添加新用户：

```
INSERT INTO user_info
VALUES ( '1', 'd_williamson', 'abc123');
```

如果执行 SELECT 语句以查看 user_info 表中的信息，则可看到 user_pwd 列中的值是二进制数据（口令的加密形式），而不是 INSERT 语句中指定的值 abc123。

如果该用户的口令发生更改，则将触发 encrypt_updated_pwd 触发器，并在 user_pwd 列中显示新口令的加密形式。

```
UPDATE user_info
SET user_pwd='xyz'
WHERE employee_ID='1';
```

通过发出以下 SQL 语句可以检索原始口令。此语句使用 DECRYPT 函数和加密密钥对数据进行解密，并使用 CAST 函数将值从 LONG BINARY 转换为 CHAR 类型：

```
SELECT CAST (
   DECRYPT( user_pwd, '8U3dkA' )
   AS CHAR(100))
   FROM user_info
   WHERE employee_ID = '1';
```

原始加密

原始加密用于将数据库服务器内部的数据加密成可导出到数据库服务器外部并进行解密的格式。这种加密格式被称为**原始**。要对原始格式的数据进行加密，必须指定加密密钥、初始化矢量以及填充格式（可选）。要解密数据，必须指定相同的参数值。

还可以使用 DECRYPT 函数对数据库服务器内部的数据进行解密。

原始加密适用于以下情况：

- **想禁止数据库用户访问数据时** – 如果不希望他人访问敏感数据，即使数据库管理员也不可以访问，则可使用原始加密对这些敏感数据进行加密，然后使用客户端应用程序对数据进行解密，而不使用数据库服务器。当数据只能通过数据库服务器进行加密和解密时，不建议使用原始加密。
- **无法使用 TLS 加密时** – 可以使用原始加密来代替 TLS 加密。与 TLS 加密不同，原始加密无法阻止重放或转接攻击，也无法验证数据库服务器。

示例

您需要将数据从数据库中 SensitiveData 表的 binary_data 列发送到不使用数据库的客户端。由于数据具有敏感性，您使用以下 SQL 语句将数据加密为原始格式：

```
SELECT ENCRYPT( binary_data, 'TheEncryptionKey','AES(FORMAT=RAW)',
'ThisIsTheIV' )FROM SensitiveData;
```

您将加密数据连同可解密其内容的应用程序一起复制到客户端。您还为客户端提供了与应用程序一起使用的加密密钥 (TheEncryptionKey) 和初始化矢量 (ThisIsTheIV)。客户端使用应用程序对数据进行解密和查看。

表加密

表加密可以对包含敏感数据的表或实例化视图进行加密，而且不会造成在对整个数据库加密时可能会导致的性能影响。启用表加密时，会对加密表的表页、相关联的索引页和临时文件页进行加密。还会对包含有关加密表的事务的事务日志页进行加密。

要对数据库中的表加密，必须启用表加密。启用表加密必须在数据库初始化时进行。要查看是否启用了表加密，请使用 DB_PROPERTY 函数查询 EncryptionScope 数据库属性，如下所示：

```
SELECT DB_PROPERTY( 'EncryptionScope' );
```

如果返回值为 TABLE，则表明表加密已启用。

要查看表加密当前使用的加密算法，请使用 DB_PROPERTY 函数查询 Encryption 数据库属性，如下所示：

```
SELECT DB_PROPERTY( 'Encryption' );
```

表加密对性能的影响

对于加密的表，每个表页在写入磁盘时都会进行加密，在从磁盘读入时都会进行解密。此过程对应用程序不可见。不过，从加密的表读出或向其中写入时，可能会对性能产生轻微的负面影响。对现有表进行加密或解密可能会花费很长的时间，时间长短取决于表的大小。

加密表中列索引的索引页也将被加密，包含有关加密表事务的事务日志页及数据库临时文件中的所有页同样会进行加密。所有其它数据库和事务日志页均未加密。

加密表可能包含压缩列。在这种情况下，数据将先进行压缩，再进行加密。

对表加密不会影响存储要求。

启动启用了表加密的数据库
启动启用了表加密的数据库与启动加密数据库的情况相同。例如，如果启动数据库时使用 -ek 选项，则必须指定密钥。如果启动数据库时使用 -ep 选项，则会提示您输入密钥。

启用数据库中的表加密 (SQL)
使用 CREATE DATABASE 语句创建采用表加密的数据库，或使用 CREATE ENCRYPTED TABLE DATABASE 语句在现有数据库中启用表加密。

前提条件

缺省情况下，您必须具有 SERVER OPERATOR 系统特权才能执行 CREATE DATABASE 语句和 CREATE ENCRYPTED TABLE DATABASE 语句。使用 -gu 数据库服务器选项可对所需的特权进行更改。

过程

必须在创建数据库时启用和配置表加密。如果数据库未启用表加密或数据库加密处于有效状态，使用 CREATE ENCRYPTED TABLE DATABASE 语句会为该数据库创建一个启用了表加密的副本，而不会覆盖原始数据库文件。

创建采用表加密的数据库，或对现有数据库启用表加密。

选项	操作
创建采用表加密的数据库	使用 CREATE DATABASE 语句创建数据库，并指定密钥和加密算法。
为现有数据库启用表加密	使用 CREATE ENCRYPTED TABLE DATABASE 语句创建数据库的副本，并指定密钥。

表加密已启用。

下一步

使用 CREATE TABLE 语句创建加密表，或使用 ALTER TABLE 语句将现有表更改为加密状态。对表进行加密时，会使用启用表加密时所指定的密钥和/或算法。

启用数据库中的表加密（iqinit 实用程序）
可以使用命令行在数据库创建期间启用表加密。

前提条件

必须在创建数据库时启用和配置表加密。如果数据库未启用表加密，或当前正在执行数据库加密，则必须重新创建数据库以启用表加密。

过程

使用 iqinit -et 和 -ek 选项创建数据库，并指定密钥和加密算法。

表加密已启用。

加密表

可以使用 CREATE TABLE 语句创建加密表，或使用 ALTER TABLE 语句对现有表进行加密。

前提条件

要使用 CREATE TABLE 语句，必须具有以下一种系统特权：

CREATE TABLE
CREATE ANY TABLE
CREATE ANY OBJECT

要使用 ALTER TABLE 语句，您必须是要更改的表的所有者，或者具有以下一种特权：

表的 ALTER 特权
ALTER ANY TABLE
ALTER ANY OBJECT

要对数据库中的表加密，必须已在数据库中启用表加密。

过程

加密表时，将使用在数据库创建时所指定的加密算法和密钥。

您可以创建一个加密的表，或者对现有表进行加密。

选项	操作
创建加密的表	使用 CREATE TABLE 语句的 ENCRYPTED 子句创建表。
对现有表进行加密	使用 ALTER TABLE 语句的 ENCRYPTED 子句对表加密。

表已加密。

IPv6 支持

SAP Sybase IQ 支持 Internet 协议版本 6 (IPv6)，它包含通过 Internet 发送包的寻址信息和控制信息。

IPv6 支持 2^{128} 个唯一的 IP 地址，与其之前版本 IPv4 支持的地址数相比有了大幅增加。对于任何可在客户端或服务器上指定 IP 地址的环境，SAP Sybase IQ 对 IPv4 和 IPv6 两种地址均支持。

ODBC 类支持将 IPv6 地址用于远程数据访问。 JDBC 类不支持将 IPv6 地址用于远程数据访问。

设置传送层安全

以下步骤概述了设置传送层安全所需的任务。

1. 获取数字证书。
   您需要标识文件和证书文件。服务器标识文件包含服务器的专用密钥，应和数据库安全地保存在一起。将服务器证书文件分发给客户端。
   您可以从证书颁发机构购买证书，也可以使用证书创建实用程序 (createcert)。SAP Sybase IQ 还提供了创建证书的功能，此功能对于开发和测试十分有用。
2. 如果要为 SAP Sybase IQ 客户端/服务器应用程序设置传送层安全，请执行以下步骤：
   - **启动支持传送层安全的 SAP Sybase IQ 数据库服务器** – 使用 -ec 数据库服务器选项指定安全类型、服务器标识文件名以及用以保护服务器专用密钥的口令。

     如果还需要通过共享内存允许非加密的连接，请指定 -es 选项。

     TDS 连接不使用 TLS 协议。为防止未加密连接使用 TDS 协议，需将 tcpip 选项指定为 -x tcpip(TDS=NO)。
   - **配置客户端应用程序以使用传送层安全** – 使用 Encryption 连接参数 [ENC] 指定受信任证书的路径和文件名。
3. 如果要为 SAP Sybase IQ Web 服务设置传送层安全，请执行以下步骤：
   - **启动支持传送层安全的 SAP Sybase IQ 数据库服务器** – 使用 -xs 数据库服务器选项指定安全类型、服务器标识文件名和保护服务器专用密钥的口令。
   - **将浏览器或其它 Web 客户端配置为信任证书** – 加密 SAP Sybase IQ Web 服务。
4. 如果要设置 SAP Sybase IQ 多路复用数据库服务器：

   INC 和 MIPC 连接根据 -ec 服务器选项内容确定要使用的 TLS 连接参数。
   将 TRUSTED_CERTIFICATES_FILE 选项设置为相应的证书颁发机构。

数字证书

设置传送层安全需要数字证书。您可以从证书颁发机构获取证书，也可以使用证书创建实用程序 (createcert) 创建证书。

证书创建实用程序
可利用证书创建实用程序 (createcert) 通过 RSA 生成 X.509 证书文件。

证书查看器实用程序
可利用证书查看器实用程序 viewcert 通过 RSA 读取 X.509 证书。

用于服务器验证的证书
用于服务器验证的证书文件可以遵循相同的过程来创建。在每种情况下，都要创建标识文件和证书文件。

对于服务器验证，需创建服务器标识文件和证书文件以分发给客户端。

证书配置
证书可以是自签名证书，也可以是由商业或企业证书颁发机构签名的证书。

- **自签名证书** – 自签名服务器证书可用于进行简单设置。
- **企业根证书** – 企业根证书可用于签署服务器证书来提高多服务器部署的数据完整性和可扩展性。

  您可以将用于签署服务器证书的专用密钥保存在一个安全的中央位置。对于服务器验证，无需重新配置客户端即可添加数据库服务器。
- **商业证书颁发机构** – 您可以使用第三方证书颁发机构替代企业根证书。商业证书颁发机构拥有用于保存专用密钥和创建高质量服务器证书的专用设施。

自签名根证书
自签名根证书可用于只包含一个数据库服务器的简单设置。

提示： 如果需要多个服务器标识文件，请使用企业级证书链或商业证书颁发机构。证书颁发机构使用专用设施保存根专用密钥，从而实现了可扩展性和更高级别的证书完整性。

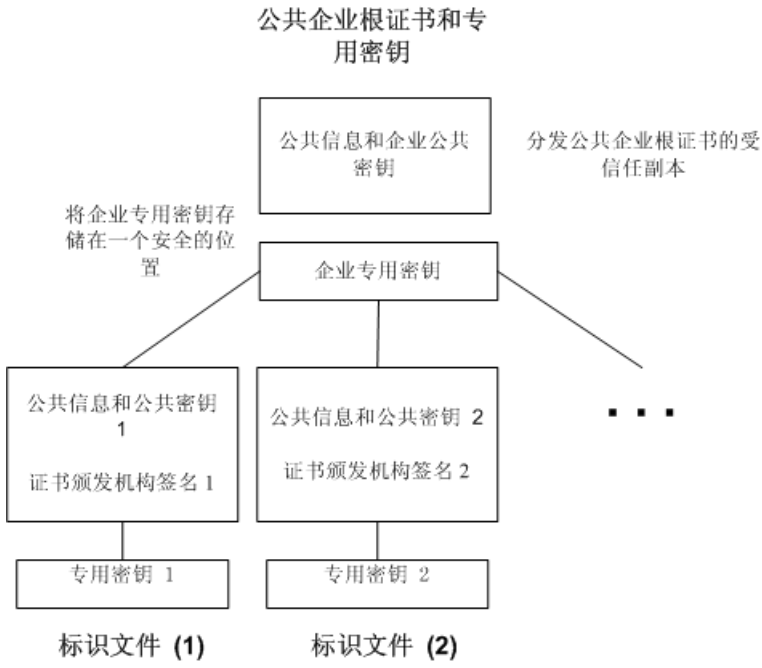
- **证书** – 对于服务器验证证书，自签名证书将分发给客户端。它是一个包含标识信息、服务器的公共密钥和自签名数字签名的电子文档。
- **标识文件** – 对于服务器验证证书，标识文件应和数据库服务器安全地保存在一起。它是自签名证书（分发给客户端）与相应专用密钥的组合。专用密钥使数据库服务器能够解密初始握手中由客户端发送的消息。

证书链
如果需要多个标识文件，您可使用证书链而非自签名证书来提高安全性和可扩展性。证书链需要证书颁发机构或企业根证书来签署标识。

使用证书链的好处
证书链具有以下优点：

- **可扩展性** – 对于服务器验证，可将客户端配置为信任由企业根证书或证书颁发机构签名的任何证书。如果添加了一个新的数据库服务器，客户端不需要新证书的副本。
- **安全** – 企业根证书的专用密钥不存在于标识文件中。请将根证书的专用密钥保存在更安全的位置，或利用能提供专用设施的证书颁发机构，以保护服务器验证的完整性。

下图展示了基本的企业根证书体系结构。



在多服务器环境中使用证书
创建用于多服务器环境的证书：

- 生成一个公共企业根证书和企业专用密钥。
  将企业专用密钥保存在一个安全位置，最好是专用设施中。
  对于服务器验证，公共企业根证书将被分发到客户端。
- 使用企业根证书签署标识。
  使用公共企业根证书和企业专用密钥签署每个标识。对于服务器验证，该标识文件用于服务器。

您也可以利用第三方证书颁发机构来签署您的服务器证书。商业证书颁发机构拥有保存专用密钥和创建高质量服务器证书的专用设施。

企业根证书
企业根证书提高了多服务器部署的数据完整性和可扩展性。

您可将用于创建受信任证书的专用密钥保存在一个专用设施中。
对于服务器验证，您无需重新配置客户端即可添加服务器。

要设置企业根证书，请创建用于签署标识的企业根证书和企业专用密钥。

签名标识文件
可使用企业根证书签署服务器标识文件。

对于服务器验证，为每个服务器生成标识文件。由于这些证书是由企业根证书签署的，所以请使用 createcert -s 选项。

全局签名证书
商业证书颁发机构是从事创建高质量证书并使用这些证书为您的证书请求签名的组织。

全局签名证书有以下优点：

- 对于公司间通信，对公认的外部机构的共同信任将增强对系统安全的信心。证书颁发机构必须保证其签署的所有证书中的标识信息的准确性。
- 证书颁发机构提供生成证书的受控环境和高级方法。
- 根证书的专用密钥必须保持专用。您的组织也许没有合适的位置保存这一至关重要的信息，但证书颁发机构能够设计并维护专用设施，以实现此目的。

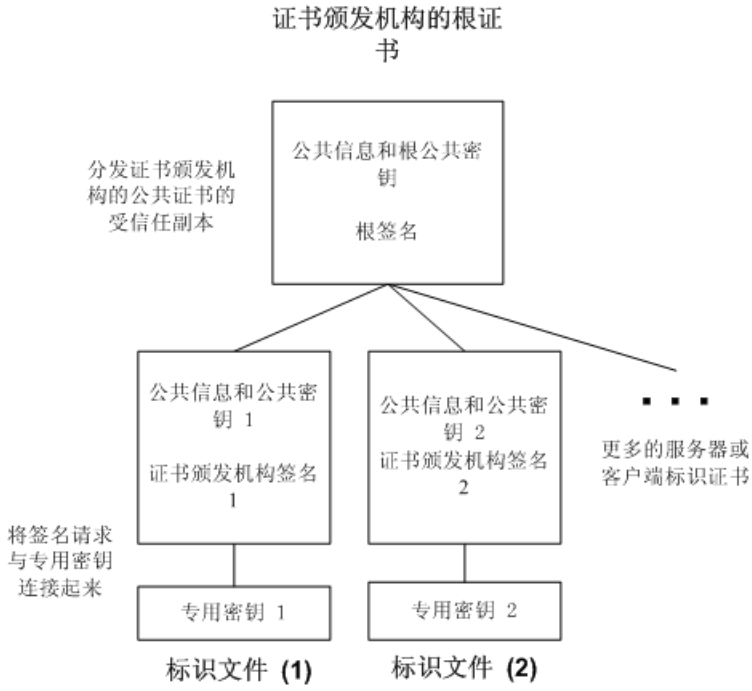
设置全局签名证书
要设置全局签名标识文件，您可以执行以下操作：

- 使用 createcert 实用程序及 -r 选项创建证书请求。
- 利用证书颁发机构签署每个请求。可将签名请求与相应的专用密钥相结合来创建服务器标识文件。

注意： 您可以对企业根证书进行全局签名。只有在证书颁发机构生成了可用于对其它证书进行签名的证书的情况下，您才能这么做。

全局签名标识文件

您可以直接使用全局签名证书作为服务器标识文件。下图显示了多标识文件的配置：



在 iqsrv16 命令行中，引用服务器标识文件和专用密钥的口令。

证书颁发机构的证书的客户端信任设置

对于服务器验证，必须确保与联系服务器的客户端信任链中的根证书。对于全局签名证书，根证书就是证书颁发机构的证书。

注意： 当使用全局签名证书时，每个客户端必须校验字段值以避免信任的证书已被同一证书颁发机构签署给其它客户端。

实用程序数据库服务器安全性

SAP Sybase IQ 包含一个称为*实用程序数据库*的虚拟数据库，该数据库物理上不存在，也不含任何数据。

实用程序数据库可以在任何 SAP Sybase IQ 服务器上运行。在 SAP Control Center 中，此实用程序数据库的服务器称作实用程序服务器。

实用程序数据库允许的专用函数范围较小。这使您不必先连接到物理数据库就可以执行数据库文件操作语句，如 **CREATE DATABASE** 和 **DROP DATABASE** 语句。

您也可以从实用程序数据库检索数据库和连接属性。这些属性在连接到实用程序数据库时应用于您所创建的数据库。

您的配置任务之一是设置实用程序数据库及其服务器的安全性。您必须决定：

- 谁能够连接到实用程序数据库，以及
- 谁能够执行文件管理语句。

在连接时定义实用程序数据库名称

在启动实用程序数据库时，由于没有与该数据库相关联的数据库文件，无法进行指定。必须在连接时指定数据库名称。

连接到实用程序数据库时指定 `utility_db` 作为数据库名称。

例如：

```
dbisqlc -c "uid=dba;pwd=sql;eng=myserver;dbn=utility_db"
```

注意： 当连接到实用程序数据库以创建使用 Windows 原始分区的 IQ 数据库时，IQ PATH 中存在一个语法差异。例如，要在设备 I 上指定 Windows 原始分区：对于实用程序数据库，可以使用格式 “\\.\I:”对于其它 IQ 数据库，则必须使用两对双斜线，因此同一设备的格式为 "\\\\.\\I:"。反斜线字符在 IQ 数据库中被视为转义字符，在实用程序数据库中则被视为常规字符。

定义实用程序数据库口令

定义实用程序数据库的用户 ID `DBA`。

1. 使用文本编辑器打开文件 `util_db.ini`，该文件存储在服务器的可执行文件目录中。

   由于该目录位于服务器上，因此您可以控制对该文件的访问，从而也可控制谁能够访问该口令。
2. 找到下面这一行，将 "password" 替换为要使用的口令：

   ```
   [UTILITY_DB]
   PWD=password
   ```

   由于 `util_db.ini` 文件可通过文本编辑器轻松读取，因此 utility_db 安全级别的使用依赖于托管数据库服务器的计算机的物理安全性。

执行文件管理语句的权限

针对数据库创建和删除单独设置的一个安全级别，为数据库提供了另外一重安全保障。**-gu** 数据库服务器命令行选项用于控制哪些用户可以执行文件管理语句。

文件管理语句的使用权限共有以下四个级别：`all`、`none`、`DBA` 和 `utility_db`。`utility_db` 级别允许能够连接到实用程序数据库的用户使用文件管理语句。

表 1. 角色管理权限

-gu 开关值	效果	适用于
all	任何用户都能够执行文件管理语句	任何数据库（包括实用程序数据库）
无	任何用户都不能执行文件管理语句	任何数据库（包括实用程序数据库）
DBA	只有具有 SERVER OPERATOR 系统特权的用户才能执行文件管理语句	任何数据库（包括实用程序数据库）
utility_db	只有能够连接到实用程序数据库的用户才能执行文件管理语句	仅限实用程序数据库

示例

在 Sun、HP、Linux 和 Windows 平台上，要仅允许知道实用程序数据库口令的用户连接到实用程序数据库并创建或删除数据库，请使用以下命令行启动服务器：

```
start_iq -n testsrv -gu utility_db
```

在 AIX 上，要仅允许知道实用程序数据库口令的用户连接到实用程序数据库并创建或删除数据库，请使用以下命令行启动服务器：

```
start_iq -n testsrv -gu utility_db -iqmt 256
```

假定实用程序数据库口令在安装过程中设置为 `IQ&Mine49`，则下面的命令会将 Interactive SQL 实用程序作为客户端应用程序启动、连接到名为 `testsrv` 的服务器、装载实用程序数据库，然后连接该用户：

```
dbisql -c "uid=DBA;pwd=IQ&Mine49;dbn=utility_db;eng=testsrv"
```

该语句执行成功后便会连接到实用程序数据库，现在即可创建和删除数据库。

注意： 数据库名称、用户 ID 和口令均区分大小写。确保您在 **dbisql** 命令和 `util_db.ini` 文件中指定了相同的大小写。

数据安全

由于数据库可能包含专有、机密或专用信息，因此确保数据库及其中数据采用安全保护设计非常重要。

系统安全功能

可以禁止数据库服务器中所运行的数据库访问系统安全功能。

在功能受到保护（无法访问）后，便无法通过客户端应用程序、数据库定义的存储过程、触发器及事件来使用该功能。安全功能设置适用于所选数据库服务器上运行的所有数据库。当您需要启动可能含有不确定嵌入式逻辑（如病毒）的数据库时，或者当

您想锁定由第三方供应商托管的数据库服务器或数据库时，安全功能将十分有用。使用 **-sf** 数据库服务器选项可以为数据库服务器上运行的数据库指定要保护的功能。

安全功能密钥

`system secure feature key` 是在创建数据库服务器时，通过指定 **-sk** 数据库服务器选项创建而成的。在数据库服务器开始运行后，使用 **sa_server_option** 系统过程来更改是对功能进行保护还是不进行保护。

创建系统安全功能密钥后，可以创建 `customized secure feature keys` 并将其指派到特定用户，从而将这些用户的访问局限于管理员为该密钥保护的功能。

通过指定的系统过程管理定制安全功能密钥。

创建安全功能密钥

使用安全功能数据库服务器选项 (-sf) 来指定数据库服务器上禁止用户访问的功能，以控制用户可使用的数据库功能。-sk 数据库服务器选项用于创建系统安全功能密钥，sp_create_secure_feature_key 系统过程用于创建定制安全功能密钥。

前提条件

您必须具有 SERVER OPERATOR 系统特权和访问 manage_keys 功能的权限。

过程

安全功能设置适用于数据库服务器上运行的所有数据库。

安全功能选项 (-sf) 控制以下类别功能的可用性：

服务器端备份
外部存储过程
远程数据访问
Web 服务

-sk 选项指定用于管理数据库服务器安全功能访问权限的系统安全功能密钥。要在数据库服务器运行后更改受保护功能的列表，请使用 sa_server_option 系统过程。要在数据库服务器运行后更改定制安全功能密钥，请使用 sp_alter_secure_feature_key 系统过程。

1. 在命令提示符处，使用 -sf 和 -sk 选项启动数据库服务器。

   例如，以下命令将启动数据库服务器并保护所有的功能。此命令中所含的密钥稍后可用于访问针对连接的受保护功能。

   ```
   iqsrv16 -n secure_server -sf all -sk someSystemKey c:\mydemo.db
   ```

2. 连接到数据库服务器：

   ```
   dbisql -c
   "UID=DBA;PWD=sql;Host=myhost;Server=secure_server;DBN=mydemo"
   ```

3. 调用 sp_use_secure_feature_key 系统过程以指定针对连接的安全功能密钥。这种情况下，安全功能密钥与通过 -sk 选项指定的密钥相同：

   ```
   CALL sp_use_secure_feature_key ( 'system' , 'someSystemKey' );
   ```

4. 使用 sa_server_option 系统过程更改系统安全功能密钥的安全功能。

   例如：

   ```
   CALL sa_server_option( 'SecureFeatures', '-remote_data_access' );
   ```

5. 为特定用户创建定制安全功能密钥。

   例如，为 Bob 创建允许其发送电子邮件的定制安全功能密钥：

   ```
   CALL sp_create_secure_feature_key ( 'bobsKey' , 'anotherAuthKey' ,
   'sa_send_email' );
   ```

   登录到数据库后，Bob 必须运行以下命令以发送电子邮件：

   ```
   CALL sp_use_secure_feature_key ( 'bobsKey' , 'anotherAuthKey' );
   ```

   禁止数据库服务器 secure_server 上所运行数据库的用户访问除 remote_data_access 功能之外的所有受保护功能。但用户 Bob 还可以访问 sa_send_email 功能。

现在，存在一个数据库服务器的系统安全功能，以及一个已指派给特定用户的定制安全功能。

另请参见

- -sk iqsrv16 数据库服务器选项 （第 288 页）
- -sf iqsrv16 数据库服务器选项 （第 288 页）
- sp_alter_secure_feature_key 系统过程 （第 357 页）
- sp_create_secure_feature_key 系统过程 （第 297 页）
- sp_drop_secure_feature_key 系统过程 （第 359 页）
- sp_list_secure_feature_keys 系统过程 （第 359 页）
- sp_use_secure_feature_key 系统过程 （第 360 页）

外部验证

SAP Sybase IQ 支持 LDAP 和 Kerberos 外部验证方法。

使用 SAP Sybase IQ 的 LDAP 用户验证

您可将 SAP Sybase IQ 集成到所有基于轻型目录访问协议 (LDAP) 这一公认国际标准的现有企业范围的目录访问框架中。

SAP Sybase IQ 与 LDAP 用户验证的集成支持：

- 使用搜索到的可分辨名称 (DN) 的验证
- 到次级 LDAP 服务器的故障转移，以实现高可用性
- 自动故障回复到之前失败的服务器
- 与 OpenLDAP 第三方库的集成
- 与 LDAP 服务器的安全通信
- 频繁短暂连接的有效设计
- 多个域和多个 LDAP 服务器的可扩展性

LDAP 用户验证的许可要求

高级安全性选项 (IQ_SECURITY) 用于保护您的环境，防止进行未经授权的访问，而且，要想通过 SAP Sybase IQ 进行 LDAP 用户验证，必须提供此选项。

关于 LDAP 服务器配置对象

SAP Sybase IQ 使用称为 LDAP 服务器的配置对象来允许执行 LDAP 用户验证。

无论 LDAP 服务器的名称是什么，它始终是驻留在 SAP Sybase IQ 服务器上的一个配置对象，而非实际服务器。它的唯一功能是提供到物理 LDAP 服务器的连接，以允许进行 LDAP 用户验证。LDAP 服务器配置对象的任何配置都仅适用于 LDAP 用户验证等式的 SAP Sybase IQ 端。LDAP 服务器配置对象配置设置从不写入物理 LDAP 服务器。

注意： 在本文档中，为清晰起见，LDAP 服务器配置对象指 SAP Sybase IQ 内部配置对象。LDAP 服务器指外部实体。

使用 LDAP 用户验证时的故障转移功能

为支持故障转移功能，可分别创建一个主 LDAP 服务器配置对象和一个次级 LDAP 服务器配置对象。

每个 LDAP 服务器配置对象都连接到单独的 LDAP 服务器，并可被指定为主服务器或次级服务器。如果指定的主 LDAP 服务器配置对象无法连接到 LDAP 服务器，则使用指定的次级 LDAP 服务器配置对象进行用户验证。可使用 SQL 语句手动管理故

障转移和故障回复，也可由 SAP Sybase IQ 在检测到适用的变化时自动执行故障转移和故障回复。

在登录策略中定义主 LDAP 服务器配置对象和次级 LDAP 服务器配置对象。为了能够实现故障转移，必须同时定义一个主 LDAP 服务器配置对象和一个次级 LDAP 服务器配置对象。如果在登录策略中仅定义主 LDAP 服务器配置对象，则不会发生故障转移。如果定义了次级 LDAP 服务器配置对象，但没有定义主 LDAP 服务器配置对象，则该次级 LDAP 服务器配置对象相当于主 LDAP 服务器配置对象，但不会发生故障转移。

指定次级 LDAP 服务器配置对象时，必须将该 LDAP 服务器配置对象配置为连接到正确的故障转移 LDAP 服务器。在发生故障转移的情况下，如果次级 LDAP 服务器配置对象无法连接到次级 LDAP 服务器，则 SAP Sybase IQ 中的 LDAP 用户验证将不可用。

启用 LDAP 用户验证

配置使用 SAP Sybase IQ 的 LDAP 用户验证。完成配置后，验证用户是否能够使用 LDAP 用户验证进行登录。

1. 将 LDAP 用户验证配置为登录方法
   要启用 LDAP 用户验证，必须将值 LDAPUA 添加到 LOGIN_MODE 数据库选项。
2. 创建 LDAP 服务器配置对象
   创建新的 LDAP 服务器配置对象以允许 LDAP 用户验证。
3. 校验 LDAP 服务器配置对象
   校验新的或现有 LDAP 服务器配置对象的属性。
4. 管理 LDAP 用户验证登录策略选项
   存在多个特定于 LDAP 用户验证的登录策略选项。在指派给使用 LDAP 用户验证的用户的任意登录策略（包括根登录策略）中，必须定义这些选项。
5. 显示 LDAP 服务器配置对象的当前状态
   运行 sa_get_ldapserver_status 存储过程可生成关于 LDAP 服务器配置对象当前状态的报告。

将 LDAP 用户验证配置为登录方法

要启用 LDAP 用户验证，必须将值 `LDAPUA` 添加到 LOGIN_MODE 数据库选项。

前提条件

需要 SET ANY SECURITY OPTION 系统特权。

过程

一旦设置 LDAP 用户验证，便可立即进行使用。
要将 LDAPUA 值添加到 LOGIN_MODE 选项，执行：

```
SET OPTION PUBLIC.login_mode = LDAPUA
```

创建 LDAP 服务器配置对象

创建新的 LDAP 服务器配置对象以允许 LDAP 用户验证。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

LDAP 服务器配置对象提供 SAP Sybase IQ 和物理 LDAP 服务器之间的连接。如果您正在使用多个 LDAP 服务器（尤其是在故障转移期间），请为每个 LDAP 服务器设置一个单独的 LDAP 服务器配置对象。LDAP 服务器配置对象的参数存储在 `ISYSLDAPSERVER`（系统视图 SYSLDAPSERVER）系统表中。要在创建时自动激活到 LDAP 服务器的连接，请使用 WITH ACTIVATE 子句。

1. 确定要为新 LDAP 服务器配置对象定义的各适用 SEARCH DN 属性的值。

表 2. SEARCH DN 属性

属性	有效值
URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
ACCESS ACCOUNT	正在连接到外部 LDAP 服务器的用户的可分辨名称。
IDENTIFIED BY	与 ACCESS ACCOUNT 可分辨名称关联的口令。
IDENTIFIED BY ENCRYPTED	与 ACCESS ACCOUNT 可分辨名称关联的加密口令。

2. 确定适合新 LDAP 服务器配置对象的各 LDAPUA 服务器属性的值。

表 3. LDAPUA 属性

属性	有效值
SEARCH DN	通过 SEARCH DN 属性定义的所有属性（请参见步骤 1）。
AUTHENTI-CATION URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
CONNEC-TION TIME-OUT	为 SAP Sybase IQ 和外部 LDAP 服务器之间的 DN 搜索和验证指定连接超时值。以毫秒为单位指定此值，缺省值为 10 秒。

属性	有效值
CONNECTION RETRIES	指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
TLS	定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。有效设置为 ON 和 OFF（缺省值）。 **注意：** 请参见启用安全 LDAP 和设置 TLS 连接受信任关系。

3. 执行 **CREATE LDAP SERVER** 命令，指定适用属性和子句。例如：

```
CREATE LDAP SERVER secure_primary
SEARCH DN
     URL 'ldaps://my_LDAPserver:636/dc=MyCompany,dc=com??sub?cn=*'
     ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
     IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldaps://my_LDAPserver:636/'
CONNECTION TIMEOUT 3000
CONNECTION RETRIES 3
TLS OFF
WITH ACTIVATE
```

校验 LDAP 服务器配置对象

校验新的或现有 LDAP 服务器配置对象的属性。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

在设置新的 LDAP 服务器配置对象或诊断 SAP Sybase IQ 和 LDAP 服务器之间的连接问题时，**VALIDATE LDAP SERVER** 命令将会对管理员有所帮助。由 VALIDATE LDAP SERVER 语句建立的任何连接均为临时连接，语句执行结束时即关闭。

要验证 LDAP 服务器上是否存在该用户，请加入 **CHECK** 子句。指定 userID 和要比较的 *user-dn-string*。

1. 确定要校验的 LDAP 服务器配置对象的 SEARCH DN 属性。

表 4. SEARCH DN 属性

属性	有效值
URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。

属性	有效值
ACCESS ACCOUNT	正在连接到外部 LDAP 服务器的用户的可分辨名称。
IDENTIFIED BY	与 ACCESS ACCOUNT 可分辨名称关联的口令。
IDENTIFIED BY ENCRYPTED	与 ACCESS ACCOUNT 可分辨名称关联的加密口令。

2. 确定要校验的 LDAP 服务器配置对象的 LDAPUA 属性。

表 5. LDAPUA 属性

属性	有效值
SEARCH DN	通过 SEARCH DN 属性定义的所有属性（请参见步骤 1）。
AUTHENTICATION URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
CONNECTION TIMEOUT	为 SAP Sybase IQ 和外部 LDAP 服务器之间的 DN 搜索和验证指定连接超时值。以毫秒为单位指定此值，缺省值为 10 秒。
CONNECTION RETRIES	指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
TLS	定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。有效设置为 ON 和 OFF（缺省值）。 **注意：** 请参见启用安全 LDAP 和设置 TLS 连接受信任关系。

3. 以适用属性执行 **VALIDATE LDAP SERVER** 命令。

例如，假设已按如下方式创建名为 `apps_primary` 的 LDAP 服务器配置对象，并将 `SET OPTION PUBLIC.login_mode` 设置为 ‘`Standard,LDAPUA`’：

```
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

以下语句通过使用可选的 CHECK 子句将 userID `myusername` 与 LDAP 服务器配置对象 `apps_primary` 上的预期用户可分辨名称（括在引号内）进行比较，从而校验该 userID 是否存在。

```
VALIDATE LDAP SERVER apps_primary
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

管理 LDAP 用户验证登录策略选项

存在多个特定于 LDAP 用户验证的登录策略选项。在指派给使用 LDAP 用户验证的用户的任意登录策略（包括根登录策略）中，必须定义这些选项。

您可以在最初创建登录策略时定义特定于 LDAP 服务器数据库对象的选项，也可以将这些选项添加到现有策略，包括根登录策略。

必须具有 MANAGE ANY LOGIN POLICY 系统特权才能定义登录策略选项。

另请参见

- 显示 LDAP 服务器配置对象的当前状态 （第 146 页）

修改根登录策略

可以修改根登录策略的选项值，但不能删除该策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

每个新数据库在创建时都使用称为根策略的缺省登录策略。如果在创建用户帐户时未指定登录策略，则该用户将成为根登录策略的一部分。

要修改根登录策略的选项，请执行：

```
ALTER LOGIN POLICY ROOT {login_policy_options}
```

另请参见

- 修改现有登录策略 （第 144 页）
- 创建新登录策略 （第 145 页）
- 为现有用户指派登录策略 （第 145 页）

修改现有登录策略

修改现有登录策略中的选项。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

要更改现有登录策略的选项，请执行：

```
ALTER LOGIN POLICY policy-name {login_policy_options}
```

示例：

此语句更改 `Test1` 登录策略的 LOCKED 和 MAX_CONNECTIONS 选项：

```
ALTER LOGIN POLICY Test1
locked=on
max_connections=5
```

另请参见

- 修改根登录策略 （第 144 页）
- 创建新登录策略 （第 145 页）
- 为现有用户指派登录策略 （第 145 页）

创建新登录策略

创建登录策略时未显式设置的任何选项都会从根登录策略继承其值。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

登录策略名必须唯一。如果要添加的登录策略名已存在，则会显示错误消息。

要创建新登录策略，请执行：

```
CREATE LOGIN POLICY policy_name {login_policy_options}
```

示例：

此语句创建 `Test1` 登录策略，同时 PASSWORD_LIVE_TIME 选项设置为 60 天：

```
CREATE LOGIN POLICY Test1
password_life_time=60
```

另请参见

- 修改根登录策略 （第 144 页）
- 修改现有登录策略 （第 144 页）
- 为现有用户指派登录策略 （第 145 页）

为现有用户指派登录策略

向现有 SAP Sybase IQ 用户指派登录策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

1. 执行：

   ```
   ALTER USER userID
   LOGIN POLICY policy_name
   ```

2. 使用户注销后再登录以应用新的登录策略。

另请参见

- 修改根登录策略 （第 144 页）
- 修改现有登录策略 （第 144 页）
- 创建新登录策略 （第 145 页）

显示 LDAP 服务器配置对象的当前状态

运行 **sa_get_ldapserver_status** 存储过程可生成关于 LDAP 服务器配置对象当前状态的报告。

状态信息包括 LDAP 服务器配置对象名称、对象标识符、当前状态以及上次更改状态的日期和时间。配置正确且正在运行的 LDAP 服务器配置对象具有 READY 或 ACTIVE 状态。

运行此存储过程不需具备任何系统特权。

另请参见

- 管理 LDAP 用户验证登录策略选项 （第 144 页）

使用 SAP Sybase IQ 管理 LDAP 服务器配置对象

管理工作包括创建和修改 LDAP 服务器配置对象以及维护其选项，以便实施 LDAP 用户验证。

将 LDAP 用户验证配置为登录方法

要启用 LDAP 用户验证，必须将值 `LDAPUA` 添加到 LOGIN_MODE 数据库选项。

前提条件

需要 SET ANY SECURITY OPTION 系统特权。

过程

一旦设置 LDAP 用户验证，便可立即进行使用。
要将 LDAPUA 值添加到 LOGIN_MODE 选项，执行：

```
SET OPTION PUBLIC.login_mode = LDAPUA
```

另请参见

- LOGIN_MODE 选项 （第 280 页）

允许在仅支持 LDAP 用户验证的环境中进行标准验证

允许特定用户在仅支持 LDAP 用户验证的环境中使用标准验证进行验证。

如果只能通过 LDAP 用户验证这一种方式访问 SAP Sybase IQ 数据库，那么很可能会出现所有用户都无法登录的情况：

- 不存在已启用 LDAP 用户验证的登录策略；

- 没有为任何用户指派已启用 LDAP 用户验证的登录策略；或
- 为所有用户帐户指派的登录策略均已锁定 LDAP 用户验证。

您可能无法阻止这种情况发生，但有一种方法可解决此问题，即允许特定数量的用户使用标准验证登录 SAP Sybase IQ 数据库。当 LOGIN_MODE 配置阻止所有用户连接到数据库时，可采用此方法作为临时解决方案。

当授予选定用户使用标准验证进行访问的权限时，需确保其中至少一个用户具有 SET ANY SECURITY OPTION 或 MANAGE ANY LOGIN POLICY 系统特权，以便能够永久性解决该问题。可能需要以上系统特权中的一项或两项来永久解决该问题，具体取决于所有用户都无法使用 LDAP 用户验证登录的根本原因。最多可指定五个用户 ID，以分号分隔，并用双引号括起来。

仅在发生锁定问题后授予标准验证访问权限；不需要提前进行设置。不需要提前进行设置。要允许选定用户使用标准验证登录，请执行带 **-al** *user-id-list* 命令行开关的 **start_iq** 实用程序。获得授权后，用户可以在出现证书提示后输入其标准验证用户名和口令。

在服务器级别或数据库级别添加 **-al** 开关。在服务器级别，在下次服务器重启前 **-al** 开关一直有效。在数据库级别，在数据库下次停止并重启前 **-al** 开关一直有效。

要允许标准验证，请执行下列命令之一：

级别	语句
服务器	**start_iq -al** *"user1,user2,user3" server_name.cfg database-name.db*
数据库	**start_iq** *servername.cfg database_name.db* **-al** *"user1,user2,user3"*

示例：

该示例假设 login_mode 设置为 "LDAPUA"。下面命令允许用户 `Alice`、`Bob` 和 `Carol` 在 `server1` 的 `database1` 上使用标准验证进行验证：

```
start_iq -al  "alice;bob;carol" server1.cfg database1.db
```

另请参见

- -al iqsrv16 服务器选项 （第 282 页）
- -al iqsrv16 数据库选项 （第 282 页）

设置 TLS 连接受信任关系

定义传送层安全性 (TLS) 与外部 LDAP 服务器连接用户验证所使用的受信任关系所在的位置和文件名。

前提条件

需要 SET ANY SECURITY OPTION 系统特权。

过程

在 LDAP 用户验证期间，SAP Sybase IQ 充当 LDAP 服务器的客户端，且必须有权访问包含签署 TLS 证书的证书颁发机构 (CA) 名称的文件。CA 的路径和文件名存储在仅公用的 TRUSTED_CERTIFICATES_FILE 数据库安全选项中。缺省情况下，该选项设置为 NULL（禁用），表示由于没有受信任的 CA 而无法启动出站连接。设置完成后，该值立即生效。

在 Windows 环境中，签署服务器证书的受信任 CA 列表可能会在本地 C: 驱动器中共享，供此计算机上的所有 SAP Sybase 应用程序使用。

要设置 TRUSTED_CERTIFICATES_FILE 数据库安全选项，请执行：

```
SET OPTION PUBLIC.TRUSTED_CERTIFICATES_FILE = 'path/filename'
```

示例

下面的示例设置了到 `C:\sybase\shared` 下名为 `\trusted.txt` 的受信任证书文件的路径：

```
SET OPTION PUBLIC.TRUSTED_CERTIFICATES_FILE = 'C:\sybase\shared
\trusted.txt'
```

另请参见

- TRUSTED_CERTIFICATES_FILE 选项 （第 281 页）

创建 LDAP 服务器配置对象

创建新的 LDAP 服务器配置对象以允许 LDAP 用户验证。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

LDAP 服务器配置对象提供 SAP Sybase IQ 和物理 LDAP 服务器之间的连接。如果您正在使用多个 LDAP 服务器（尤其是在故障转移期间），请为每个 LDAP 服务器设置一个单独的 LDAP 服务器配置对象。LDAP 服务器配置对象的参数存储在 `ISYSLDAPSERVER`（系统视图 SYSLDAPSERVER）系统表中。要在创建时自动激活到 LDAP 服务器的连接，请使用 WITH ACTIVATE 子句。

1. 确定要为新 LDAP 服务器配置对象定义的各适用 SEARCH DN 属性的值。

表 6. SEARCH DN 属性

属性	有效值
URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
ACCESS ACCOUNT	正在连接到外部 LDAP 服务器的用户的可分辨名称。
IDENTIFIED BY	与 ACCESS ACCOUNT 可分辨名称关联的口令。
IDENTIFIED BY ENCRYPTED	与 ACCESS ACCOUNT 可分辨名称关联的加密口令。

2. 确定适合新 LDAP 服务器配置对象的各 LDAPUA 服务器属性的值。

表 7. LDAPUA 属性

属性	有效值
SEARCH DN	通过 SEARCH DN 属性定义的所有属性（请参见步骤 1）。
AUTHENTICATION URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
CONNECTION TIMEOUT	为 SAP Sybase IQ 和外部 LDAP 服务器之间的 DN 搜索和验证指定连接超时值。以毫秒为单位指定此值，缺省值为 10 秒。
CONNECTION RETRIES	指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
TLS	定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。有效设置为 ON 和 OFF（缺省值）。 **注意：** 请参见启用安全 LDAP 和设置 TLS 连接受信任关系。

3. 执行 **CREATE LDAP SERVER** 命令，指定适用属性和子句。例如：

```
CREATE LDAP SERVER secure_primary
SEARCH DN
     URL 'ldaps://my_LDAPserver:636/dc=MyCompany,dc=com??sub?cn=*'
     ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
     IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldaps://my_LDAPserver:636/'
CONNECTION TIMEOUT 3000
CONNECTION RETRIES 3
```

```
TLS OFF
WITH ACTIVATE
```

另请参见

- LDAP 服务器配置对象 URL 的语法和参数 （第 156 页）
- 启用安全 LDAP （第 156 页）
- CREATE LDAP SERVER 语句 （第 221 页）
- 编辑 LDAP 服务器配置对象属性 （第 152 页）
- 设置 TLS 连接受信任关系 （第 147 页）

校验 LDAP 服务器配置对象

校验新的或现有 LDAP 服务器配置对象的属性。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

在设置新的 LDAP 服务器配置对象或诊断 SAP Sybase IQ 和 LDAP 服务器之间的连接问题时，**VALIDATE LDAP SERVER** 命令将会对管理员有所帮助。由 VALIDATE LDAP SERVER 语句建立的任何连接均为临时连接，语句执行结束时即关闭。

要验证 LDAP 服务器上是否存在该用户，请加入 **CHECK** 子句。指定 userID 和要比较的 *user-dn-string*。

1. 确定要校验的 LDAP 服务器配置对象的 SEARCH DN 属性。

表 8. SEARCH DN 属性

属性	有效值
URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
ACCESS ACCOUNT	正在连接到外部 LDAP 服务器的用户的可分辨名称。
IDENTIFIED BY	与 ACCESS ACCOUNT 可分辨名称关联的口令。
IDENTIFIED BY ENCRYPTED	与 ACCESS ACCOUNT 可分辨名称关联的加密口令。

2. 确定要校验的 LDAP 服务器配置对象的 LDAPUA 属性。

表 9. LDAPUA 属性

属性	有效值
SEARCH DN	通过 SEARCH DN 属性定义的所有属性（请参见步骤 1）。
AUTHENTICATION URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
CONNECTION TIMEOUT	为 SAP Sybase IQ 和外部 LDAP 服务器之间的 DN 搜索和验证指定连接超时值。以毫秒为单位指定此值，缺省值为 10 秒。
CONNECTION RETRIES	指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
TLS	定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。有效设置为 ON 和 OFF（缺省值）。 **注意：** 请参见启用安全 LDAP 和设置 TLS 连接受信任关系。

3. 以适用属性执行 **VALIDATE LDAP SERVER** 命令。

例如，假设已按如下方式创建名为 `apps_primary` 的 LDAP 服务器配置对象，并将 `SET OPTION PUBLIC.login_mode` 设置为 ‘`Standard,LDAPUA`’：

```
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=myadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

以下语句通过使用可选的 CHECK 子句将 userID `myusername` 与 LDAP 服务器配置对象 `apps_primary` 上的预期用户可分辨名称（括在引号内）进行比较，从而校验该 userID 是否存在。

```
VALIDATE LDAP SERVER apps_primary
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

另请参见

- 启用安全 LDAP （第 156 页）
- LDAP 服务器配置对象 URL 的语法和参数 （第 156 页）
- VALIDATE LDAP SERVER 语句 （第 277 页）
- 编辑 LDAP 服务器配置对象属性 （第 152 页）
- 设置 TLS 连接受信任关系 （第 147 页）

激活 LDAP 服务器配置对象

通过将连接状态设置为 READY 来激活 LDAP 服务器配置对象。这将启用 LDAP 用户验证。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

从 ISYSLDAPSERVER 系统表中读取 LDAP 服务器配置对象属性值，并将这些值应用到与 LDAP 服务器之间的新连接和向 SAP Sybase IQ 服务器发送的传入验证请求。成功验证用户后，LDAP 服务器的连接状态将更改为 ACTIVE。
要激活 LDAP 服务器配置对象，请执行：

```
ALTER LDAP SERVER LDAP_server_name
WITH ACTIVATE
```

另请参见

- ALTER LDAP SERVER 语句 （第 207 页）
- LDAP 服务器配置对象状态 （第 155 页）

编辑 LDAP 服务器配置对象属性

修改 LDAP 服务器的现有属性。对属性的所有更改都会应用到后续连接。应用更改时已启动的任何连接都不会立即反映该更改。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

1. 确定待修改的现有 SEARCH DN 属性。

表 10. SEARCH DN 属性

属性	有效值
URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
ACCESS ACCOUNT	正在连接到外部 LDAP 服务器的用户的可分辨名称。
IDENTIFIED BY	与 ACCESS ACCOUNT 可分辨名称关联的口令。

属性	有效值
IDENTIFIED BY ENCRYPTED	与 ACCESS ACCOUNT 可分辨名称关联的加密口令。

2. 确定待修改的现有 LDAPUA 属性。

表 11. LDAPUA 属性

属性	有效值
SEARCH DN	通过 SEARCH DN 属性定义的所有属性（请参见步骤 1）。
AUTHENTICATION URL	指定主机（按名称或 IP 地址）、端口号以及要执行的用于查找给定用户 ID 的 DN 的搜索，或者输入 NULL。 **注意：** 有关受支持的语法，请参见“LDAP 服务器配置对象 URL 的语法和参数”。
CONNECTION TIMEOUT	为 SAP Sybase IQ 和外部 LDAP 服务器之间的 DN 搜索和验证指定连接超时值。以毫秒为单位指定此值，缺省值为 10 秒。
CONNECTION RETRIES	指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
TLS	定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。有效设置为 ON 和 OFF（缺省值）。 **注意：** 请参见启用安全 LDAP 和设置 TLS 连接受信任关系。

3. 确定要使用的服务器子句。

子句	说明
WITH SUSPEND	将 LDAP 服务器置入维护模式
WITH ACTIVATE	将 LDAP 服务器置入 READY 状态并启用 LDAP 验证
WITH REFRESH	重新初始化 LDAP 用户验证

4. 以适用参数和子句执行 **ALTER LDAP SERVER** 命令，例如：

```
ALTER LDAP SERVER apps_primary
AUTHENTICATION URL 'ldap://my_LDAPserver:1066/'
CONNECTION RETRIES 10
WITH ACTIVATE
```

另请参见

- LDAP 服务器配置对象 URL 的语法和参数 （第 156 页）

- 启用安全 LDAP （第 156 页）
- ALTER LDAP SERVER 语句 （第 207 页）
- 设置 TLS 连接受信任关系 （第 147 页）
- 校验 LDAP 服务器配置对象 （第 150 页）

刷新 LDAP 服务器配置对象

重新初始化 LDAP 服务器。如果 LDAP 服务器的连接状态不是 ACTIVE 或 READY，此命令将失败。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

刷新 LDAP 服务器时，将关闭与 LDAP 服务器之间的所有连接并重新从 `ISYSLDAPSERVER` 系统表中读取 LDAP 服务器的选项值。然后将这些值应用到与 LDAP 服务器间的所有新连接以及向 SAP Sybase IQ 服务器发送的所有传入用户验证请求。执行 REFRESH 命令不会更改 LDAP 服务器的连接状态，也不会更改客户端与 SAP Sybase IQ 服务器之间的所有现有连接。

为确保下次用户验证时应用所有更改，建议您在更改 TRUSTED_CERTIFICATES_FILE 数据库选项或更改 TRUSTED_CERTIFICATES_FILE 数据库选项所指定文件的内容后，刷新 LDAP 服务器。

要刷新 LDAP 服务器，请执行：

```
ALTER LDAP SERVER LDAP_server_name
WITH REFRESH
```

另请参见

- ALTER LDAP SERVER 语句 （第 207 页）
- LDAP 服务器配置对象状态 （第 155 页）

暂停 LDAP 服务器配置对象

将 LDAP 服务器置入维护模式。与 LDAP 服务器间的所有连接均将关闭，LDAP 用户验证也不再可用。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

要暂停 LDAP 服务器，请执行：

```
ALTER LDAP SERVER LDAP_server_name
WITH SUSPEND
```

另请参见

- ALTER LDAP SERVER 语句 （第 207 页）
- LDAP 服务器配置对象状态 （第 155 页）

删除 LDAP 服务器配置对象

删除没有处于 READY 或 ACTIVE 状态的 LDAP 服务器配置对象。

前提条件

需要 MANAGE ANY LDAP SERVER 系统特权。

过程

针对状态为 READY 或 ACTIVE 的 LDAP 服务器配置对象发出 DROP 语句时，该语句失败。如果存在引用要删除的 LDAP 服务器配置对象的登录策略，DROP 语句也将失败。为确保在删除 LDAP 服务器配置对象前先从所有登录策略中移除对该 LDAP 服务器配置对象的所有引用，请加入 WITH DROP ALL REFERENCES 子句。为忽略服务器状态检查并将数据库对象置入维护模式（无论其当前状态为何），请在删除 LDAP 服务器配置对象时加入 WITH SUSPEND 子句。

删除 LDAP 服务器配置对象将从 `ISYSLDAPSERVER` 系统表中移除已命名的对象。

要删除 LDAP 服务器配置对象，请执行以下命令（包括适用子句）：

```
DROP LDAP SERVER LDAP_Server_name
WITH SUSPEND
WITH DROP ALL REFERENCES
```

示例：

以下示例删除名为 `ldapserver1` 的 LDAP 服务器配置对象（无论其当前状态为何），并移除所有登录策略中对 `ldapserver1` 的所有引用：

```
DROP LDAP SERVER ldapserver1
WITH DROP ALL REFERENCES
WITH SUSPEND
```

由于未包括 WITH DROP ALL REFERENCES 子句，因此，如果任何登录策略中引用了名为 `ldapserver2` 的 LDAP 服务器配置对象，**DROP LDAP SERVER** 命令将失败：

```
DROP LDAP SERVER ldapserver1
WITH SUSPEND
```

另请参见

- DROP LDAP SERVER 语句 （第 235 页）
- LDAP 服务器配置对象状态 （第 155 页）

LDAP 服务器配置对象状态

LDAP 服务器配置对象的可能状态列表。

LDAP 服务器配置对象的状态持续在可写数据库的 `ISYSLDAPSERVER` 系统表中进行维护，以便管理员能够了解 LDAP 用户验证。如果重新启动 LDAP 服务器配置对象，

将保留关闭时的状态。这使得 LDAP 服务器配置对象的维护在重新启动过程中一直有效。对于只读数据库，状态更改不会永久存储 - 它们仅发生在内存中，并在关闭数据库后丢失。连接状态会在启动时使用只读数据库中的值进行设置，内存中可能会发生瞬时状态更改以提供 LDAP 用户验证。

LDAP 服务器配置对象可能的状态包括：

- **RESET** – 自上次激活后，已输入或修改一个或多个 LDAP 服务器配置对象属性。
- **READY** – LDAP 服务器配置对象已准备好接受连接。
- **ACTIVE** – LDAP 服务器配置对象已成功执行至少一次 LDAP 用户验证。
- **FAILED** – 连接到 LDAP 服务器配置对象时出现问题。
- **SUSPENDED** – LDAP 服务器配置对象处于维护模式，无法用于 LDAP 用户验证。

启用安全 LDAP

安全 LDAP 使用 TLS 证书验证以提供防欺骗保护。

使用 TLS 证书可为到 LDAP 服务器的客户端连接提供证据，证明服务器身份的真实性。

在 LDAP 服务器配置对象上启用安全 LDAP 可采用以下两种方式之一：

- **ldaps://** – 在 LDAP 服务器配置对象上，定义 SEARCH DN URL 或 AUTHENTICATION URL 属性时使用 ldaps://，并将 TLS 属性设置为 OFF。
- **TLS 参数** – 在 LDAP 服务器配置对象上，定义 SEARCH DN URL 属性时使用 ldap://，并将 TLS 属性设置为 ON。

注意： 最新版本的 Active Directory (AD)、Tivoli、SunONE Oracle DS 和 OpenLDAP 同时支持这两种方法。较旧版本可能仅支持其中的一种方法。为与所有版本均兼容，SAP Sybase IQ 支持以上两种方法。

LDAP 服务器配置对象 URL 的语法和参数

URL 用于标识主机（按名称或按 IP 地址）、端口号，以及对 LDAP 服务器执行安全可分辨名称 (DN) 查找时所执行的搜索。

URL 的语法有以下两种形式，您可根据与 LDAP 服务器之间建立安全连接方式的不同，采用其中的一种形式，但对于每种形式来说，URL 的基础参数均相同。

- **ldaps://** – 在 LDAP 服务器配置对象上，定义 SEARCH DN URL 或 AUTHENTICATION URL 属性时使用 ldaps://，并将 TLS 属性设置为 OFF。

```
ldapurl::=ldaps://host:[port]/[node]?[attributes]? [base | one | sub]? [filter]
```

- **TLS 参数** – 在 LDAP 服务器配置对象上，定义 SEARCH DN URL 属性时使用 ldap://，并将 TLS 属性设置为 ON。

```
ldapurl::=ldap://host:[port]/[node]?[attributes]? [base | one |
sub]? [filter]
```

参数	说明
host	LDAP 服务器的主机名。
port	LDAP 服务器的端口号。
node	对象层次中启动搜索所在的节点。
attributes	结果集中返回的属性列表。每个 LDAP 服务器可能支持一种不同的属性，具体取决于 LDAP 服务器所使用的模式。但对于每个 LDAP 服务器，仅使用第一个属性，并应返回用户的可分辨名称 (DN)。
base | one | sub	限定搜索条件。 base – 指定基节点的搜索。 one – 指定节点及一个子级别的搜索。 sub – 指定节点及所有子级别的搜索。
filter	指定用于搜索数据库用户的可分辨名称 (DN) 的属性。过滤器可以是简单过滤器，如 "uid=*"，也可以是复合过滤器，如 "(uid=*)(ou=group)"。过滤器中的属性取决于 LDAP 服务器模式。搜索 DN 时，LDAP 用户验证将用数据库用户 ID 替换每个通配符 (*)。

在创建 LDAP 服务器配置对象时，URL 最初被定义为其中的一个服务器属性，并可随时进行更改。这些参数没有缺省值。创建或修改 LDAP 服务器配置对象需要 MANAGE ANY LDAP SERVER 系统特权。

注意： 最新版本的 Active Directory (AD)、Tivoli、SunONE Oracle DS 和 OpenLDAP 同时支持这两种方法。较旧版本可能仅支持其中的一种方法。为与所有版本均兼容，SAP Sybase IQ 支持以上两种方法。

管理 LDAP 用户验证登录策略选项

存在多个特定于 LDAP 用户验证的登录策略选项。在指派给使用 LDAP 用户验证的用户的任意登录策略（包括根登录策略）中，必须定义这些选项。

您可以在最初创建登录策略时定义特定于 LDAP 服务器数据库对象的选项，也可以将这些选项添加到现有策略，包括根登录策略。

必须具有 MANAGE ANY LOGIN POLICY 系统特权才能定义登录策略选项。

修改根登录策略

可以修改根登录策略的选项值，但不能删除该策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

每个新数据库在创建时都使用称为根策略的缺省登录策略。如果在创建用户帐户时未指定登录策略，则该用户将成为根登录策略的一部分。
要修改根登录策略的选项，请执行：

```
ALTER LOGIN POLICY ROOT {login_policy_options}
```

另请参见

- 修改现有登录策略 （第 158 页）
- 创建新登录策略 （第 158 页）
- 为现有用户指派登录策略 （第 159 页）
- 管理 LDAP 用户验证登录策略选项 （第 157 页）
- ALTER LOGIN POLICY 语句 （第 209 页）

修改现有登录策略

修改现有登录策略中的选项。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

要更改现有登录策略的选项，请执行：

```
ALTER LOGIN POLICY policy-name {login_policy_options}
```

示例：

此语句更改 `Test1` 登录策略的 LOCKED 和 MAX_CONNECTIONS 选项：

```
ALTER LOGIN POLICY Test1
locked=on
max_connections=5
```

另请参见

- 修改根登录策略 （第 157 页）
- 创建新登录策略 （第 158 页）
- 为现有用户指派登录策略 （第 159 页）
- 管理 LDAP 用户验证登录策略选项 （第 157 页）
- ALTER LOGIN POLICY 语句 （第 209 页）

创建新登录策略

创建登录策略时未显式设置的任何选项都会从根登录策略继承其值。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

登录策略名必须唯一。如果要添加的登录策略名已存在，则会显示错误消息。
要创建新登录策略，请执行：

```
CREATE LOGIN POLICY policy_name {login_policy_options}
```

示例：

此语句创建 Test1 登录策略，同时 PASSWORD_LIVE_TIME 选项设置为 60 天：

```
CREATE LOGIN POLICY Test1
password_life_time=60
```

另请参见

- 修改根登录策略 （第 157 页）
- 修改现有登录策略 （第 158 页）
- 为现有用户指派登录策略 （第 159 页）
- 管理 LDAP 用户验证登录策略选项 （第 157 页）
- CREATE LOGIN POLICY 语句 （第 224 页）

为现有用户指派登录策略

向现有 SAP Sybase IQ 用户指派登录策略。

前提条件

MANAGE ANY LOGIN POLICY 系统特权。

过程

1. 执行：

   ```
   ALTER USER userID
   LOGIN POLICY policy_name
   ```

2. 使用户注销后再登录以应用新的登录策略。

另请参见

- 修改根登录策略 （第 157 页）
- 修改现有登录策略 （第 158 页）
- 创建新登录策略 （第 158 页）
- ALTER USER 语句 （第 218 页）

管理 LDAP 用户验证的用户和口令

要使用 LDAP 用户验证登录到 SAP Sybase IQ，每个用户必须在外部 LDAP 服务器上有一个活动的用户 ID 和口令，同时必须在 SAP Sybase IQ 服务器上有一个活动的用户 ID。

在 SAP Sybase IQ 中创建新用户时，并未要求指定口令，但建议您指定一个口令以保障新用户帐户在首次 LDAP 用户验证登录前的安全。

新用户第一次登录或现有用户在更改口令后登录时，SAP Sybase IQ 数据库中的口令会自动被外部 LDAP 服务器中定义的相应用户口令覆盖。因此，必须始终在外部 LDAP 服务器而不是 SAP Sybase IQ 服务器上为使用 LDAP 用户验证的用户执行 SAP Sybase IQ 口令的所有维护操作。

由于系统会自动同步口令，因此对于授予使用标准验证权限的用户来说（口令在 SAP Sybase IQ 数据库中定义），当尝试使用标准验证登录时，应继续使用其 LDAP 服务器证书。

显示用户的当前状态信息

运行 **sa_get_user_status** 存储过程可生成关于用户当前状态的报告。

该信息包含有关连接和失败登录的信息，以及用户是否已被锁定和锁定原因。如果使用 LDAP 用户验证对用户进行验证，则输出将包括该用户的可分辨名称以及该可分辨名称被找到之时的日期和时间。

必须具有 MANAGE ANY USER 系统特权才能运行该存储过程。不具有 MANAGE ANY USER 系统特权的用户可以通过创建和执行具有 MANAGE ANY USER 系统特权的用户所拥有的包装过程来获取用户信息。

另请参见

- sa_get_user_status 系统过程 （第 295 页）

显示 LDAP 服务器配置对象的当前状态

运行 **sa_get_ldapserver_status** 存储过程可生成关于 LDAP 服务器配置对象当前状态的报告。

状态信息包括 LDAP 服务器配置对象名称、对象标识符、当前状态以及上次更改状态的日期和时间。配置正确且正在运行的 LDAP 服务器配置对象具有 READY 或 ACTIVE 状态。

运行此存储过程不需具备任何系统特权。

另请参见

- sa_get_ldapserver_status 系统过程 （第 294 页）

Kerberos 验证

Kerberos 登录功能允许您对数据库连接、操作系统和网络登录维护单个用户 ID 和口令。Kerberos 登录使用户更加方便，且允许数据库和网络安全体系具有统一的安全系统。它的优点包括：

- 用户连接数据库时无需提供用户 ID 或口令。
- 多个用户可映射到单个数据库用户 ID。
- 用于登录到 Kerberos 的名称和口令不必与数据库用户 ID 和口令一致。

Kerberos 是一种网络验证协议，它使用密钥加密算法提供强验证和强加密。已经登录到 Kerberos 的用户无需提供用户 ID 或口令即可连接到数据库。

可使用 Kerberos 进行验证。要将验证委派给 Kerberos，您必须：

- 将服务器和数据库配置为使用 Kerberos 登录。
- 创建登录到计算机或网络的用户 ID 与数据库用户之间的映射。

警告！ 小心

将 Kerberos 登录用作单独的安全解决方案时，需要考虑一些值得引起关注的安全性方面的负效应。

SAP Sybase IQ 中不包含 Kerberos 软件；该软件必须单独获取。Kerberos 软件中包含以下组件：

- **Kerberos 库** – 这些被称作 Kerberos 客户端或 GSS（通用安全服务）-API 运行时库。这些 Kerberos 库可执行明确定义的 GSS-API。每个想要使用 Kerberos 的客户端和服务器计算机上都必须有这些库。如果您使用 Active Directory 作为您的 KDC，则可以使用内置的 Windows SSPI 接口来取代第三方 Kerberos 客户端库。

  SSPI 只能在 Kerberos 连接参数中由 SAP Sybase IQ 客户端使用。SAP Sybase IQ 数据库服务器不能使用 SSPI，它们需要支持的 Kerberos 客户端而不是 SSPI。
- **Kerberos 密钥分发中心 (KDC) 服务器** – KDC 起着用户和服务器的仓库的作用。同时它还能验证用户和服务器的身份标识。KDC 通常安装在不供应用程序或用户登录的服务器计算机上。

SAP Sybase IQ 支持通过 DBLib、ODBC、OLE DB 和 ADO.NET 客户端以及 Sybase Open Client 和 jConnect 客户端进行 Kerberos 验证。Kerberos 验证可以与 SAP Sybase IQ 传送层安全加密配合使用，但 SAP Sybase IQ 不支持网络通信的 Kerberos 加密。

Windows 使用 Kerberos 作为 Windows 域和域帐户。Active Directory Windows 域控制器执行 Kerberos KDC。数据库服务器计算机仍然需要第三方 Kerberos 客户端或运行时库才能在此环境下进行验证，但 Windows 客户端计算机可使用内置的 Windows SSPI 接口来取代第三方 Kerberos 客户端或运行时库。

Kerberos 客户端

Kerberos 验证可用于多个平台。有关经过测试的 Kerberos 客户端的列表，请参见 http://www.sybase.com/detail?id=1061807。

下表列出了所支持的 Kerberos 客户端使用的 keytab 和 GSS-API 文件的缺省名称和位置。

注意： SSPI 只能由 SAP Sybase IQ 客户端在 Kerberos 连接参数中使用。SAP Sybase IQ 数据库服务器不能使用 SSPI，它们需要受支持的 Kerberos 客户端而不是 SSPI。

Kerberos 客户端	缺省 keytab 文件	GSS-API 库文件名	注释
Windows MIT Kerberos 客户端	`C:\WINDOWS\krb5kt`	`gssapi32.dll` 或 `gssapi64.dll`	在启动数据库服务器前，可以设置 KRB5_KTNAME 环境变量，以指定不同的 keytab 文件。
Windows CyberSafe Kerberos 客户端	`C:\Program Files\CyberSafe\v5srvtab`	`gssapi32.dll` 或 `gssapi64.dll`	在启动数据库服务器前，可以设置 CSFC5KTNAME 环境变量，以指定不同的 keytab 文件。
Unix MIT Kerberos 客户端	`/etc/krb5.keytab`	`libgssapi_krb5.so` [1]	在启动数据库服务器前，可以设置 KRB5_KTNAME 环境变量，以指定不同的 keytab 文件。
Unix CyberSafe Kerberos 客户端	`/krb5/v5srvtab`	`libgss.so` [1]	在启动数据库服务器前，可以设置 CSFC5KTNAME 环境变量，以指定不同的 keytab 文件。
Unix Heimdal Kerberos 客户端	`/etc/krb5.keytab`	`libgssapi.so.1` [1]	

[1] 这些文件名可能会有所不同，这取决于您的操作系统和 Kerberos 客户端版本。

将 Kerberos 系统设置为与 SAP Sybase IQ 一同使用

您可以将 Kerberos 验证配置为与 SAP Sybase IQ 一同使用。

前提条件

您必须使用 Kerberos 验证登录到您的计算机。

过程

Kerberos 是一种网络验证协议，它使用密钥加密算法提供强验证和强加密。

1. 必要时，在客户端和服务器上都安装和配置 Kerberos 客户端软件，其中包括 GSS-API 运行时库。

   在使用 Active Directory 密钥分发中心（Key Distribution Center，简称 KDC）的 Windows 客户端计算机上，您可以使用 SSPI，不必安装 Kerberos 客户端。
2. 如有必要，请在 Kerberos KDC 内为每位用户创建一个 Kerberos 主体。

   Kerberos 主体就是一个 Kerberos 用户 ID，其格式为 *user*/*instance*@*REALM*，其中 /*instance* 为可选项。如果您正在使用 Kerberos，则主体应该已经存在，因此不必为每位用户创建一个 Kerberos 主体。

   主体区分大小写，因此必须指定正确的大小写。不支持映射只有大小写存在差异的多个主体（例如，无法同时映射 jjordan@MYREALM.COM 和 JJordan@MYREALM.COM）。
3. 在 SAP Sybase IQ 数据库服务器的 KDC 内创建 Kerberos 主体。

   数据库服务器缺省 Kerberos 主体的格式为 *server-name*@*REALM*，其中 *server-name* 指 SAP Sybase IQ 数据库服务器的名称。要使用不同的服务器主体，请使用 -kp 服务器选项。主体区分大小写，并且 *server-name* 不能包含多字节字符或者 /、\ 或 @。

   因为服务器使用 keytab 文件进行 KDC 验证，所以必须在 KDC 内创建服务器服务主体。keytab 文件是受保护和已加密的。
4. 将主体 *server-name*@*REALM* 的 keytab 从 KDC 安全地提取并复制到运行 SAP Sybase IQ 数据库服务器的计算机上。Keytab 文件的缺省位置取决于 Kerberos 客户端和平台。keytab 文件的权限应设置为 SAP Sybase IQ 服务器能够读取该文件，而其他未授权的用户则没有读取权限。

Kerberos 系统已经过验证并配置为与 SAP Sybase IQ 一同使用。

下一步

将 SAP Sybase IQ 数据库服务器和数据库配置为使用 Kerberos。

配置 SAP Sybase IQ 数据库使用 Kerberos

您可以将 SAP Sybase IQ 数据库配置为使用 Kerberos 登录。

前提条件

您必须拥有 SET ANY PUBLIC OPTION 和 MANAGE ANY USER 系统特权。

您必须事先配置 Kerberos，之后 SAP Sybase IQ 才能使用它。

过程

Kerberos 登录功能允许您针对数据库连接、操作系统和网络登录维护单个用户 ID 和口令。

1. 使用 -krb 或 -kr 选项启动 SAP Sybase IQ 数据库服务器，以启用 Kerberos 验证，或者使用 -kl 选项指定 GSS-API 库的位置并启用 Kerberos。
2. 将公共或临时公共选项 login_mode 更改为包含 Kerberos 的值。因为数据库选项只作用于它们所在的数据库，所以，不同的数据库即使是在同一数据库服务器内装载和运行，也可以有不同的 Kerberos 登录设置。例如：

   ```
   SET OPTION PUBLIC.login_mode = 'Kerberos,Standard';
   ```

   警告！ 小心

   将 login_mode 数据库选项设置为 Kerberos，会使只有被授予了 Kerberos 登录映射的用户才能进行连接。如果用户不具有 SYS_AUTH_DBA_ROLE 系统角色，则尝试使用用户 ID 和口令连接会生成错误。

3. 为客户端用户创建数据库用户 ID。只要现有数据库用户拥有相应的特权，您就可以使用该用户的 ID 进行 Kerberos 登录。例如：

   ```
   CREATE USER "kerberos-user"
   IDENTIFIED BY abc123;
   ```

4. 执行 GRANT KERBEROS LOGIN TO 语句可创建从客户端的 Kerberos 主体到现有数据库用户 ID 的映射。例如：

   ```
   GRANT KERBEROS LOGIN TO "pchin@MYREALM.COM"
   AS USER "kerberos-user";
   ```

   要在使用的 Kerberos 主体没有映射的情况下进行连接，请确保具有 Guest 数据库用户 ID 且拥有口令。

5. 确保客户端用户已经使用其 Kerberos 主体登录（具有有效的 Kerberos 票据授予票据）且客户端的 Kerberos 票据未过期。Windows 用户登录到已拥有票据授予票据的域帐户，使他们可以对服务器进行验证（假设他们的主体拥有足够权限）。

   票据授予票据是一种通过用户口令加密的 Kerberos 票据，票据授予服务使用该票据来验证用户的身份。

6. 从客户端连接，指定 KERBEROS 连接参数（通常为 KERBEROS=YES，但也可以使用 KERBEROS=SSPI 或 KERBEROS=*GSS-API-library-file*）。如果指定了用户 ID 或口令连接参数，则它们将被忽略。例如：

   ```
   dbisql -c "KERBEROS=YES;Server=my_server_princ"
   ```

SAP Sybase IQ 数据库已配置为使用 Kerberos 验证。

下一步

您可以使用 Kerberos 验证从客户端进行连接。另外，您也可以创建 Kerberos 登录映射。

从 Sybase Open Client 或 jConnect 应用程序连接

从 Sybase Open Client 或 jConnect 应用程序连接：

- 设置 Kerberos 验证。
- 将 SAP Sybase IQ 配置为使用 Kerberos。
- 使用 Adaptive Server Enterprise 为 Kerberos 验证设置 Sybase Open Client 或 jConnect（按照您期望的方式）。服务器名称必须是 SAP Sybase IQ 服务器的名称且区分大小写。不能使用备用服务器名称从 Sybase Open Client 或 jConnect 连接。

在 Windows 上使用 SSPI 进行 Kerberos 登录

在 Windows 域中，可以在基于 Windows 的计算机上使用 SSPI 且无需在客户端计算机上安装 Kerberos 客户端。Windows 域帐户已经拥有关联的 Kerberos 主体。

前提条件

您必须事先配置 Kerberos，之后 SAP Sybase IQ 才能使用它。必须已将 SAP Sybase IQ 数据库服务器和数据库配置为使用 Kerberos。

过程

SSPI 只能由 SAP Sybase IQ 客户端在 Kerberos 连接参数中使用。SAP Sybase IQ 数据库服务器不能使用 SSPI，它们需要受支持的 Kerberos 客户端而不是 SSPI。

从客户端计算机连接数据库。例如：

```
dbisql -c "KERBEROS=SSPI;Server=my_server_princ"
```

若连接字符串中指定了 Kerberos=SSPI，则会尝试进行 Kerberos 登录。

如果某个用户已经登录，且登录时使用的用户配置文件名与数据库服务器的缺省数据库中的 Kerberos 登录映射相匹配，那么，使用以下 SQL 语句尝试连接也会成功：

```
CONNECT USING 'KERBEROS=SSPI';
```

可以在 Windows 上使用 SSPI 进行 Kerberos 验证。

疑难解答：Kerberos 连接

如果尝试启用或使用 Kerberos 验证时出现意外错误，建议在数据库服务器和客户端上均启用附加诊断消息。

如果在启动数据库服务器时指定 -z 选项，或者在服务器已经运行时执行 `CALL sa_server_option( 'DebuggingInformation', 'ON' )`，数据库服务器消息日志中将包含附加诊断消息。LogFile 连接参数可使客户端诊断信息写入指定的文件。

您可以使用 -z 参数代替 LogFile 连接参数来运行 Ping 实用程序 (dbping)。-z 参数显示的诊断消息可帮助您判断出现连接问题的原因。

无法启动数据库服务器

症状	常用解决办法
[无法装载 Kerberos GSS-API 库] 消息	• 确保数据库服务器计算机上已经安装 Kerberos 客户端，包括 GSS-API 库。 • 数据库服务器 -z 输出显示正在尝试装载的库名。验证库名是否正确。如有必要，可使用 -kl 选项指定正确的库名。 • 确保目录和所有支持库都列在库路径（在 Windows 上为 %PATH%）中。 • 如果数据库服务器 -z 输出显示 GSS-API 库缺少入口点，则该库不是受支持的第 5 版本 Kerberos GSS-API 库。
[无法获取服务器名 "*server-name*" 的 Kerberos 证书] 消息	• 确保 KDC 中具有 *server-name*@*REALM* 的主体。主体区分大小写，因此请确保数据库服务器名与主体名的用户部分大小写一致。 • 确保 SAP Sybase IQ 服务器的名称是主体的主要/用户部分。 • 确保服务器的主体已被提取到一个 keytab 文件中，并且此 keytab 文件位于 Kerberos 客户端的正确位置。 • 如果数据库服务器计算机上的 Kerberos 客户端的缺省域与服务器主体内的域不同，请使用 -kr 选项指定服务器主体内的域。
[Kerberos 登录失败] 客户端错误	• 检查数据库服务器的诊断消息。服务器所用的 keytab 文件的某些问题在客户端尝试进行验证时才会发现。

Kerberos 客户端连接疑难解答

如果客户端在尝试使用 Kerberos 验证进行连接时出现错误：

症状	常用解决办法
[不支持 Kerberos 登录] 错误，并且 LogFile 内包含消息 [未能装载库 Kerberos GSS-API]	• 确保客户端计算机上已安装了 Kerberos 客户端，包括 GSS-API 库。 • LogFile 所指定的文件列出尝试装载的库的名称。检查库名是否正确，如有必要可使用 Kerberos 连接参数指定正确的库名。 • 确保库路径（在 Windows 上为 %PATH%）中包含所有支持库的目录。 • 如果 LogFile 输出显示 GSS-API 库缺少入口点，则该库不是受支持的第 5 版本 Kerberos GSS-API 库。

症状	常用解决办法
[不支持 Kerberos 登录] 错误	• 确保数据库服务器已经通过指定一个或多个 -krb、-kl 或 -kr 服务器选项启用了 Kerberos 登录。 • 确保客户端和服务器平台上的 SAP Sybase IQ 均支持 Kerberos 登录。
[Kerberos 登录失败] 错误	• 确保用户已经登录到 Kerberos 且拥有尚未过期的有效票据授予票据。 • 确保将客户端计算机和服务器计算机的时间同步到相差不到 5 分钟。
[login_mode 设置不容许登录模式 'Kerberos'] 错误	• login_mode 选项的公共或临时公共数据库选项设置中必须包含值 Kerberos 以允许 Kerberos 登录。
[登录 ID '*client-Kerberos-principal*' 未被映射到任何数据库用户 ID]	• 必须使用 GRANT KERBEROS LOGIN 语句将 Kerberos 主体映射到一个数据库用户 ID。注意，必须将包括域在内的完整客户端主体提供给 GRANT KERBEROS LOGIN 语句，只在实例或域内有差异的主体将被区分对待。 • 或者，如果希望所有尚未明确映射的有效 Kerberos 主体能建立连接，可使用 GRANT CONNECT 创建一个带口令的 Guest 数据库用户 ID。

安全问题：用于增加安全性的临时公共选项

如果使用 SET OPTION 语句为指定数据库设置 login_mode 选项的值以允许标准、集成、Kerberos 和 LDAPUA 登录，该语句将为该数据库永久启用指定类型的登录。例如，以下语句用于永久启用标准登录和集成登录：

```
SET OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

如果关闭并重新启动该数据库，则该选项的值将保持不变，集成登录仍处于启用状态。

使用 SET TEMPORARY OPTION 设置 login_mode 选项仍然允许用户通过集成登录进行访问，但只在数据库未关闭前有效。以下语句可临时更改该选项的值：

```
SET TEMPORARY OPTION PUBLIC.login_mode = 'Standard,Integrated';
```

如果永久选项值为 [标准]，数据库将在关闭时恢复为该值。

设置临时公共选项可为数据库提供附加的安全性。将集成登录、Kerberos 或 LDAPUA 登录添加到数据库后，数据库将依赖于其运行时所在的操作系统的安全性。如果数据库被复制到另一台计算机，则对于数据库的访问将恢复到 SAP Sybase IQ 安全模型。

安全问题：复制的数据库文件

如果可以复制数据库文件，则应为集成登录和 Kerberos 登录使用临时公共 login_mode 选项。如果文件被复制，缺省情况下将不再支持集成登录和 Kerberos 登录。

如果数据库内包含敏感信息，则应防止存储数据库文件的计算机受到未经授权的访问。否则，数据库文件可能会被复制，并且可以在其它计算机上对数据进行未经授权的访问。要增加数据库的安全性：

- 使口令复杂难猜。
- 将 PUBLIC.login_mode 数据库选项设置为 Standard。要启用集成登录或 Kerberos 登录，每次启动服务器时应仅更改临时公共选项。这可确保在数据库被复制时只允许进行标准登录。
- 应使用 AES 加密算法强加密数据库文件。加密密钥应复杂难猜。

Kerberos 的许可要求

高级安全性选项 (IQ_SECURITY) 用于保护您的环境，防止进行未经授权的访问，要将 Kerberos 验证与 SAP Sybase IQ 一起使用，必须提供此选项。

SAP Sybase IQ 中的高级安全性选项

SAP® Sybase® IQ 高级安全性选项支持列加密、经联邦信息处理标准 (FIPS) 认可的网络加密技术，以及针对数据库连接、操作系统登录和网络登录的 LDAP 和 Kerberos 验证。高级安全性选项是单独授权的 SAP Sybase IQ 选项。

SAP Sybase IQ 中的 FIPS 支持

SAP Sybase IQ 支持经联邦信息处理标准 (FIPS) 认可的加密技术。LinuxAMD64 服务器、Solaris Sparc 服务器、Solaris AMD64 服务器、LinuxAMD32 客户端和 Windows32 客户端都支持 FIPS。

SAP Sybase IQ 的 FIPS 支持的主要作用是加密可以是非确定性的，这也是缺省行为。非确定性算法是相同的输入每次都产生不同输出值的算法。这意味着当您使用密钥对字符串加密时，每次产生的加密字符串都不相同。但该算法仍可使用密钥对非确定性结果进行解密。使用这种功能后，加密算法更加难以分析，从而使加密更安全。

并非所有平台上都可以使用 FIPS 认证的加密。有关受支持平台的列表，请参见

SAP Sybase IQ 同时提供 RSA 和 FIPS 安全性。RSA 加密无需单独的库，但 FIPS 需要以下可选库：

- dbfips16.dll、libeay32.dll、msvcr90.dll、ssleay32.dll（32 位 Windows）
- dbfips16.dll、libeay32.dll、msvcr100.dll、ssleay32.dll（64 位 Windows）
- libssl.so 和 libcrypto.so (Linux)

这两种安全模型都需要证书。`rsaserver` 证书命名为 `rsaserver.id`。

FIPS 认证的加密技术

您可以使用经过 FIPS 认可的安全算法加密数据库文件，或加密数据库客户端/服务器通信、Web 服务的通信内容。

联邦信息处理标准 (FIPS) 140-2 规定了对安全算法的要求。FIPS 140-2 是由美国和加拿大政府通过美国国家标准与测试协会（National Institute of Standards and Testing，简称 NIST）和加拿大通信安全机构（Communications Security Establishment，简称 CSE）授予的。

强制使用 FIPS

或者，您也可以在客户端或带有 FIPS 选项的服务器上强制使用 FIPS 认证的加密。将 FIPS 选项设置为 on 时，所有安全通信必须经过 FIPS 认证。如果有人尝试使用非 FIPS RSA 加密，则会自动升级为 FIPS 认证的 RSA 加密。可以在客户端或想要强制执行 FIPS 认证的加密的服务器上设置 FIPS 选项。SAP Sybase IQ 具有 -fips 命令行选项，客户端具有可使用加密连接参数进行设置的 fips 选项。

SAP Sybase IQ 中的列加密

SAP Sybase IQ 支持用户加密的列。

SAP Sybase IQ 数据库文件的强加密使用 128 位算法和安全密钥。如果没有密钥，数据将不可读取，而且基本上无法被破解。在联邦信息处理标准的高级加密标准 (FIPS-197) 中介绍了受支持的算法。

SAP Sybase IQ 支持使用 **AES_ENCRYPT** 和 **AES_DECRYPT** 函数以及 **LOAD TABLE ENCRYPTED** 子句的用户加密列。这些函数允许通过应用程序调用来显式加密和解密列数据。加密和解密的密钥管理由应用程序负责。

某些数据库选项会影响列的加密。

另请参见

- 列加密的数据库选项 （第 195 页）

列加密的许可要求

要将用户加密的列与 SAP Sybase IQ 一起使用，必须提供高级安全性选项 (IQ_SECURITY)。

加密术语定义

描述对存储数据的加密时所用术语的定义。

- 明文 - 以可读懂的原始形式存在的数据。明文并不仅限于字符串数据，而是用来描述任何以原始表示形式存在的数据。
- 密文 - 以难以读懂的形式存在，对明文形式的信息内容起保护作用的数据。
- 加密 - 将数据从明文变为密文的可逆转换。也称为加密。
- 解密 - 将密文变回明文的逆向转换。也称为解密。
- 密钥 - 用于对数据进行加密或解密的数字。对称密钥加密系统使用相同的密钥进行加密和解密。非对称密钥系统使用一个密钥进行加密，使用另一个（但在数学上是相关的）密钥进行解密。SAP Sybase IQ 接口允许将字符串用作密钥。
- Rijndael - 发音为 "reign dahl"。支持各种密钥和块大小的特定加密算法。设计此算法的初衷在于使用简单的整字节操作，因此在软件中这种算法相对容易实现。
- AES - 高级加密标准，是一种经过 FIPS 认可的加密算法，用于保护敏感（但未分类）的电子数据。AES 采用限制块大小和密钥长度的 Rijndael 算法。AES 是 SAP Sybase IQ 支持的算法。

适用于加密列的数据类型

加密列支持的、可与这些加密列配合使用的数据类型。

支持的数据类型

AES_ENCRYPT 函数的第一个参数必须是受支持的数据类型之一。

CHAR	NUMERIC
VARCHAR	FLOAT
TINYINT	REAL
SMALLINT	DOUBLE
INTEGER	DECIMAL
BIGINT	DATE
BIT	TIME
BINARY	DATETIME
VARBINARY	TIMESTAMP
UNSIGNED INT	SMALLDATETIME
UNSIGNED BIGINT	

SAP Sybase IQ 列加密当前不支持 LOB 数据类型。

数据类型保留

SAP Sybase IQ 可确保在解密数据后保留原始数据类型的明文，前提是将该数据类型作为参数提供给 **AES_DECRYPT** 函数，或者此函数位于 **CAST** 函数内。

SAP Sybase IQ 会将 **CAST** 函数的目标数据类型与原始加密数据的数据类型进行比较。如果这两种数据类型不匹配，则会出现 -1001064 错误，其中包括有关原始和目标数据类型的详细信息。

例如，假定有一个经过加密的 VARCHAR(1) 值以及下面这个有效的解密语句：

```
SELECT AES_DECRYPT ( thecolumn, 'theKey',
VARCHAR(1) ) FROM thetable
```

如果尝试使用以下语句对数据进行解密：

```
SELECT AES_DECRYPT ( thecolumn, 'theKey',
SMALLINT ) FROM thetable
```

则返回的错误如下：

```
Decryption error: Incorrect CAST type smallint(5,0)
for decrypt data of type varchar(1,0).
```

只有提供 **CAST** 或数据类型参数时，才进行该数据类型检查。否则，查询将以二进制数据形式返回密码文本。

当对文字常量使用 **AES_ENCRYPT** 函数时（如以下语句中所示）：

```
INSERT INTO t (cipherCol) VALUES (AES_ENCRYPT (1, ‘key’))
```

1 的数据类型不明确；它可以是 TINYINT、SMALLINT、INTEGER、UNSIGNED INT、BIGINT、UNSIGNED BIGINT，也可能是其它数据类型。

您应显式使用 **CAST** 函数来消除任何潜在的不明确性，如以下语句中所示：

```
INSERT INTO t (cipherCol)
VALUES ( AES_ENCRYPT (CAST (1 AS UNSIGNED INTEGER), ‘key’))
```

在加密数据时通过使用 **CAST** 函数以显式方式转换数据类型，可以防止在解密数据时出现与使用 **CAST** 函数有关的问题。

如果要加密的数据来自于列，或加密数据是使用 **LOAD TABLE** 插入的，则不存在不明确性问题。

不同数据类型对密文的影响

要为不同的数据类型生成相同的密码文本，请将 **AES_ENCRYPT** 的输入转换为相同数据类型以生成相同密码文本。

对于两种不同的数据类型，即使指定相同的输入值和密钥，**AES_ENCRYPT** 生成的密码文本也不同。因此，将分别保存两种不同数据类型加密值的两个密码文本列连接后，可能不会返回相同的结果。

例如，假定：

```
CREATE TABLE tablea(c1 int, c2 smallint);
INSERT INTO tablea VALUES (100,100);
```

值 AES_ENCRYPT(c1, 'key') 与 AES_ENCRYPT(c2,'key') 不同，并且值 AES_ENCRYPT(c1,'key') 与 AES_ENCRYPT(100,'key') 也不同。

若要解决此问题，请将 **AES_ENCRYPT** 的输入强制转换为同一数据类型。例如，以下代码段的结果是相同的：

```
AES_ENCRYPT(c1, 'key');
```

```
AES_ENCRYPT(CAST(c2 AS INT), 'key');
```

```
AES_ENCRYPT(CAST(100 AS INT), 'key');
```

另请参见

- AES_ENCRYPT 函数 [String] （第 173 页）

AES_ENCRYPT 函数 [String]

使用所提供的加密密钥对指定值进行加密，并返回 VARBINARY 或 LONG VARBINARY。

语法

```
AES_ENCRYPT( string-expression, key )
```

参数

string-expression - 要加密的数据。也可以将二进制值传递到 **AES_ENCRYPT**。此参数区分大小写，即使是在不区分大小写的数据库中也是如此。

key - 用于对 *string-expression* 进行加密的加密密钥。要获取原始值，请使用同一密钥对值进行解密。此参数区分大小写，即使是在不区分大小写的数据库中也是如此。

与大多数口令一样，应为其选择不容易被猜到的密钥值。请选择满足以下条件的值：长度至少为 16 个字符，混合使用大小写字母并包含数字和特殊字符。每次要对数据进行解密时，都需要使用此密钥。

警告！ 请保护好您的密钥；将密钥副本存储在安全位置。如果丢失了密钥，则加密数据将完全无法访问且无法恢复。

用法

AES_ENCRYPT 返回一个 VARBINARY 值，其长度最多比输入 *string-expression* 长 31 个字节。该函数返回的值为密码文本，人类无法理解。可以使用 **AES_DECRYPT** 函数对用 **AES_ENCRYPT** 函数加密的 *string-expression* 进行解密。要成功解密 *string-expression*，请使用对数据加密时所使用的相同加密密钥和算法。如果指定的加密密钥不正确，将会生成错误。

如果将加密值存储在表中，则列的数据类型应为 VARBINARY 或 VARCHAR 且应大于或等于 32 个字节，以避免对数据执行字符集转换。（字符集转换会阻止数据解密。）如果 VARBINARY 或 VARCHAR 列的长度小于 32 个字节，**AES_DECRYPT** 函数将返回错误。

AES_ENCRYPT 函数的结果数据类型可以是 LONG BINARY。如果在 **SELECT INTO** 语句中使用 **AES_ENCRYPT**，您必须具有“非结构化数据分析选项”许可证，或使用 **CAST** 并将 **AES_ENCRYPT** 设置为正确的数据类型和大小。

标准和兼容性

- SQL - ISO/ANSI SQL 语法的服务商扩充。
- Sybase – Adaptive Server 不支持。

另请参见

- AES_DECRYPT 函数 [String] （第 175 页）
- 加密和解密示例 （第 197 页）

- LOAD TABLE ENCRYPTED 子句 （第 176 页）
- 不同数据类型对密文的影响 （第 172 页）
- 适用于加密列的数据类型 （第 170 页）

REPLACE 函数 [字符串]
用另一个子串替换在各个位置出现的某个子串。

语法

```
REPLACE ( original-string, search-string, replace-string )
```

参数
如果有参数为空值，此函数返回空值。

参数	描述
original-string	待搜索的字符串。此字符串可以为任意长度。
search-string	要搜索并以 *replace-string* 替换的字符串。此字符串的长度不应超过 255 个字节。如果 *search-string* 是空字符串，则按原样返回原始字符串。
replace-string	替代字符串，用于替换 *search-string*。可为任意长度。如果 *replace-string* 为空字符串，则删除出现的所有 *search-string*。

返回
LONG VARCHAR

LONG NVARCHAR

注意： 结果数据类型为 LONG VARCHAR。如果在 **SELECT INTO** 语句中使用 **REPLACE**，您必须具有“非结构化数据分析选项”许可证，或使用 **CAST** 并将 **REPLACE** 设置为正确的数据类型和大小。

注释
REPLACE 函数的结果数据类型为 LONG VARCHAR。如果在 **SELECT INTO** 语句中使用 **REPLACE**，您必须具有“非结构化数据分析选项”许可证，或使用 **CAST** 并将 **REPLACE** 设置为正确的数据类型和大小。

有两种方法可以解决这一问题：

- 声明一个局部临时表，然后执行 **INSERT**：

```
DECLARE local temporary table #mytable
  (name_column char(10)) on commit preserve rows;
INSERT INTO #mytable SELECT REPLACE(name,'0','1')   FROM
dummy_table01;
```

- 使用 **CAST**：

```
SELECT CAST(replace(name, '0', '1') AS Char(10)) into #mytable
from dummy_table01;
```

如果需要在 *replace-string* 宽于 *search-string* 时控制结果列的宽度，可使用 **CAST** 函数。例如：

```
CREATE TABLE aa(a CHAR(5));
INSERT INTO aa VALUES( 'CCCCC' );
COMMIT;
SELECT a, CAST(REPLACE(a,' C' ,' ZZ' ) AS CHAR(5)) FROM aa;
```

标准和兼容性

- SQL - ISO/ANSI SQL 语法的服务商扩充。
- Sybase - 与 Adaptive Server Enterprise 兼容。

示例

以下语句返回值 "xx.def.xx.ghi"：

```
SELECT REPLACE( 'abc.def.abc.ghi', 'abc', 'xx' ) FROM iq_dummy
```

以下语句生成包含 **ALTER PROCEDURE** 语句的结果集，这些语句在执行时会修复那些引用已重命名的表的存储过程。（表名必须唯一才有用。）

```
SELECT REPLACE(
  replace(proc_defn,'OldTableName','NewTableName'),
  'create procedure',
  'alter procedure')
FROM SYS.SYSPROCEDURE
WHERE proc_defn LIKE '%OldTableName%'
```

对于 **LIST** 函数，使用逗号以外的分隔符：

```
SELECT REPLACE( list( table_id ), ',', '--')
FROM  SYS.ISYSTAB
WHERE table_id <= 5
```

AES_DECRYPT 函数 [String]

使用所提供的密钥对字符串解密，并在缺省条件下返回 VARBINARY 或 LONG BINARY，或者返回原始明文类型。

语法

AES_DECRYPT(*string-expression*, *key* [, *data-type*])

参数

string-expression - 要解密的字符串。也可以将二进制值传递到此函数。此参数区分大小写，即使是在不区分大小写的数据库中也是如此。

key - 对 *string-expression* 解密所需的加密密钥。若要获取加密的原始值，密钥必须是用于加密 *string-expression* 的加密密钥。此参数区分大小写，即使在不区分大小写的数据库中也是如此。

警告！ 请保护好您的密钥；将密钥副本存储在安全位置。如果丢失了密钥，则加密数据将完全无法访问且无法恢复。

data-type - 该可选参数指定解密的 *string-expression* 的数据类型，其值必须为原始明文的数据类型。

如果在使用 **AES_ENCRYPT** 函数插入数据时没有使用 **CAST** 语句，则可以通过将 VARCHAR 作为 *data-type* 传递来使用 **AES_DECRYPT** 函数查看相同数据。如果没有将 *data-type* 传递给 **AES_DECRYPT**，则返回 VARBINARY 数据类型。

用法

可以使用 **AES_DECRYPT** 函数对用 **AES_ENCRYPT** 函数加密的 *string-expression* 进行解密。如果未指定数据类型，此函数返回与输入字符串具有相同字节数的 VARBINARY 或 LONG VARBINARY 值。否则，将返回指定的数据类型。

为了成功对 *string-expression* 进行解密，必须使用用于加密数据的加密密钥。使用不正确的加密密钥将导致返回错误。

示例

对 user_info 表中的用户口令解密。

```
SELECT AES_DECRYPT(user_pwd, '8U3dkA', CHAR(100))
FROM user_info;
```

标准和兼容性

- SQL - ISO/ANSI SQL 语法的服务商扩充。
- Sybase - 不受 Adaptive Server 支持。

另请参见

- AES_ENCRYPT 函数 [String] （第 173 页）
- 加密和解密示例 （第 197 页）
- LOAD TABLE ENCRYPTED 子句 （第 176 页）
- 适用于加密列的数据类型 （第 170 页）

LOAD TABLE ENCRYPTED 子句

LOAD TABLE 语句支持 column-spec 关键字 **ENCRYPTED**。

column-specs 必须按以下顺序遵循 **LOAD TABLE** 语句中的列名：

- *format-specs*
- *null-specs*
- *encrypted-specs*

语法

```
| ENCRYPTED(data-type 'key-string' [, 'algorithm-string' ] )
```

参数

- **data-type** – 输入文件字段应转换到的目标数据类型，作为 **AES_ENCRYPT** 函数的输入。*data-type* 应该与 **AES_DECRYPT** 函数的输出数据类型相同。
- **key-string** – 用于对数据进行加密的加密密钥。此密钥必须为字符串。要获取原始值，请使用同一密钥对值进行解密。此参数区分大小写，即使是在不区分大小写的数据库中也是如此。

  与大多数口令一样，应为其选择不容易被猜到的密钥值。请选择满足以下条件的值：长度至少为 16 个字符，混合使用大小写字母并包含数字和特殊字符。每次要对数据进行解密时，都需要使用此密钥。

  警告！ 请保护密钥；将密钥副本存储在一个安全位置。丢失密钥将导致加密数据完全无法访问，而完全无法访问的加密数据是无法进行恢复的。
- **algorithm-string** – 用于对数据进行加密的算法。此参数是可选的，但必须使用相同的算法对数据进行加密和解密。目前，缺省算法为 AES，因为它是唯一受支持的算法。AES 是一种数据块加密算法，美国国家标准与技术协会（National Institute of Standards and Technology，简称 NIST）选择它作为新的数据块编码器高级加密标准（Advanced Encryption Standard，简称 AES）。

用法

ENCRYPTED 列指定允许指定加密密钥和/或用于对载入列中的数据进行加密的算法。这种装载操作的目标列应为 VARBINARY 类型。指定其它数据类型将返回错误。

示例

```
LOAD TABLE table_name
(
plaintext_column_name,
a_ciphertext_column_name
NULL('nil')
ENCRYPTED(varchar(6),'tHefiRstkEy') ,
another_encrypted_column
ENCRYPTED(bigint,'thEseconDkeY','AES')
)
FROM '/path/to/the/input/file'
FORMAT ascii
DELIMITED BY ';'
ROW DELIMITED BY '\0xa'
QUOTES OFF
ESCAPES OFF
```

其中 **LOAD TABLE** 语句的输入文件的格式为：

```
a;b;c;
d;e;f;
g;h;i;
```

另请参见

- AES_ENCRYPT 函数 [String] （第 173 页）

- AES_DECRYPT 函数 [String] （第 175 页）
- 加密和解密示例 （第 197 页）
- 适用于加密列的数据类型 （第 170 页）

LOAD TABLE 语句

将数据从外部文件导入数据库表。

快速链接:

转至参数 （第 179 页）

转至示例 （第 189 页）

转至用法 （第 191 页）

转至标准 （第 194 页）

转至权限 （第 194 页）

语法

```
[ INTO ] TABLE [ owner.]table-name
   ... ( load-specification [, ⋯] )
   ...  { FROM | USING [ CLIENT ] FILE }
   { 'filename-string' | filename-variable } [, ⋯]
   ... [ CHECK CONSTRAINTS { ON | OFF } ]
   ... [ DEFAULTS { ON | OFF } ]
   ... [ QUOTES OFF ]
   ... ESCAPES OFF
   ... [ FORMAT { ascii | binary | bcp } ]
   ... [ DELIMITED BY 'string' ]
   ... [ STRIP { OFF | RTRIM } ]
   ... [ WITH CHECKPOINT { ON | OFF } ]
   ... [ BYTE ORDER { NATIVE | HIGH | LOW } ]
   ... [ LIMIT number-of-rows ]
   ... [ NOTIFY number-of-rows ]
   ... [ ON FILE ERROR { ROLLBACK | FINISH | CONTINUE } ]
   ... [ PREVIEW { ON | OFF } ]
   ... [ ROW DELIMITED BY 'delimiter-string' ]
   ... [ SKIP number-of-rows ]
   ... [ HEADER SKIP number [ HEADER DELIMITED BY 'string' ] ]
   ... [ WORD SKIP number ]
   ... [ ON PARTIAL INPUT ROW { ROLLBACK | CONTINUE } ]
   ... [ IGNORE CONSTRAINT constraint-type [, ⋯] ]
   ... [ MESSAGE LOG 'string' ROW LOG 'string' [ ONLY LOG log-what
[, ⋯] ]
   ... [ LOG DELIMITED BY 'string' ]

load-specification - (back to Syntax)
   { column-name [ column-spec ]
      | FILLER ( filler-type ) }

column-spec - (back to load-specification)
   { ASCII ( input-width )
   | BINARY [ WITH NULL BYTE ]
```

```
    | PREFIX { 1 | 2 | 4 }
    | 'delimiter-string'
    | DATE ( input-date-format )
    | DATETIME ( input-datetime-format )
    | ENCRYPTED ( data-type 'key-string' [, 'algorithm-string' ] )
    | DEFAULT default-value }
    [ NULL ( { BLANKS | ZEROS | 'literal', …} ) ]

filler-type – (back to load-specification)
    { input-width
    | PREFIX { 1 | 2 | 4 }
    | 'delimiter-string'
    }

constraint-type – (back to Syntax)
    { CHECK integer
    | UNIQUE integer
    | NULL integer
    | FOREIGN KEYinteger
    | DATA VALUE integer
    | ALL integer
    }

log-what – (back to Syntax)
    { CHECK
    | ALL
    | NULL
    | UNIQUE
    | DATA VALUE
    | FOREIGN KEY
    | WORD
    }
```

参数

(返回顶部) (第 178 页)

- **FROM** – 标识要从中装载数据的一个或多个文件。要指定多个文件，请使用逗号分隔每个 `filename-string`。*filename-string* 以字符串形式传递到服务器。因此，该字符串遵循的格式要求与其它 SQL 字符串相同。

  要在 Windows 系统中指示目录路径，反斜杠字符 \ 必须用两个反斜杠来表示。因此，要将文件 `c:\temp\input.dat` 中的数据装载到 `Employees` 表的语句是：

  ```
  LOAD TABLE Employees
  FROM 'c:\\temp\\input.dat' ...
  ```

  路径名相对于数据库服务器，而不是客户端应用程序。如果在其它某台计算机的数据库服务器上运行此语句，则目录名是指服务器计算机上的目录，而不是客户端计算机上的目录。装载 Multiplex 数据库时，请在所有文件名中使用绝对（完全限定）路径。请不要使用相对路径名。

  由于受资源限制的影响，SAP Sybase IQ 无法保证能够装载所有数据。如果资源分配失败，整个装载事务将被回退。一次读取一个文件，并按 FROM 子句中指定的

顺序处理这些文件。任何 SKIP 或 LIMIT 值都只在装载开始时应用，而不是针对每个文件应用。

现已不建议使用 LOAD TABLE FROM 子句，但可使用该子句指定服务器上存在的文件。此示例从客户端计算机上的文件 a.inp 装载数据。

```
LOAD TABLE t1(c1,c2,filler(30))
USING CLIENT FILE 'c:\\client-data\\a.inp'
QUOTES OFF ESCAPES OFF
IGNORE CONSTRAINT UNIQUE 0, NULL 0
MESSAGE LOG 'c:\\client-data\\m.log'
ROW LOG 'c:\\client-data\\r.log'
ONLY LOG UNIQUE
```

- **USING** – USING FILE 从服务器装载一个或多个文件。该子句的作用等同于指定 FROM *filename* 子句。USING CLIENT FILE 从客户端批量装载一个或多个文件。客户端上文件的字符集必须与服务器归类相同。SAP Sybase IQ 将依次处理文件列表中的文件。每个文件在处理时将锁定为读取模式，然后解锁。客户端批量装载不会产生任何管理开销，例如额外的磁盘空间以及内存或网络监控守护程序需求，但会强制对每个文件进行单线程处理。

  批量装载大对象时，USING CLIENT FILE 子句同时适用于主文件和辅助文件。

  LOAD TABLE 语句只能装载 gzip 格式的压缩客户端和服务器文件。扩展名为 ".gz" 或 ".gzip" 的所有文件都视为压缩文件。装载压缩文件时不支持命名管道或辅助文件。压缩文件和未压缩文件可以在同一 **LOAD TABLE** 语句中指定。装载中的每个压缩文件都由一个线程进行处理。

  在客户端装载过程中，将在客户端主机上创建 IGNORE CONSTRAINT 日志文件，创建日志文件过程中出现的任何错误都会导致操作回退。

  客户端批量装载受使用命令序列协议的 Interactive SQL 和 ODBC/JDBC 客户端支持。使用 TDS 协议的客户端则不支持。为了确保网络数据安全，请使用“传送层安全性”。要控制谁能够使用客户端批量装载，请使用安全功能 (-sf) 服务器启动开关、**ALLOW_READ_CLIENT_FILE** 数据库选项和/或 READCLIENTFILE 访问控制。

- **CHECK CONSTRAINTS** – 对检查约束进行评估，即，可忽略或记录。CHECK CONSTRAINTS 缺省设置为 ON。

  设置 CHECK CONSTRAINTS OFF 将导致 SAP Sybase IQ 忽略所有检查约束违规。例如，此设置在重建数据库时十分有用。如果表的检查约束调用尚未创建的用户定义函数，则重建将失败，除非此选项设置为 OFF。

  此选项与以下选项互斥。如果在同一装载中指定了以下任何选项，将导致错误：

  - IGNORE CONSTRAINT ALL
  - IGNORE CONSTRAINT CHECK
  - LOG ALL
  - LOG CHECK

- **DEFAULTS** – 使用列缺省值。缺省情况下，此选项为 ON。如果 DEFAULTS 选项为 OFF，则为列列表中未显示的列分配 NULL。

  DEFAULTS 选项的设置适用于所有列 DEFAULT 值，包括 AUTOINCREMENT。

- **QUOTES** – 表示输入字符串用引号字符括起来。QUOTES 是可选参数，且缺省设置为 ON。引号字符是撇号（单引号）或引号（双引号）。字符串中出现的第一个这样的字符将被视为该字符串的引号字符。字符串数据必须以匹配的引号结束。

  在 QUOTES ON 的情况下，可以在列值中包括列或行分隔符。假定前导引号字符和结尾引号字符不是值的一部分并将其从装载的数据值中排除。

  要在使用 QUOTES ON 的值中包括引号字符，必须使用两个引号。例如，此行在第三列中包含一个单引号字符值：

  ```
  ‘123 High Street, Anytown’, ‘(715)398-2354’,’’’’
  ```

  在打开 STRIP 时（缺省情况），首先从值中去除尾随空白，然后再插入这些值。仅去除不带引号的字符串的尾随空白。带引号的字符串保留其尾随空白。仅当设置为 ON 时，才会剪裁前导空白或 TAB 字符。

  数据抽取工具提供多个引号处理选项（**TEMP_EXTRACT_QUOTES**、**TEMP_EXTRACT_QUOTES_ALL** 和 **TEMP_EXTRACT_QUOTE**）。如果您计划通过缺省 ASCII 抽取方式抽取数据以将其装载到 IQ 主存储表中，且字符串字段包含列或行分隔符，请使用 **TEMP_EXTRACT_BINARY** 选项进行抽取并对 **LOAD TABLE** 使用 FORMAT binary 和 QUOTES OFF 选项。

  限制：

  - QUOTES ON 仅适用于列分隔的 ASCII 字段。
  - 在 QUOTES 设置为 ON 的情况下，列分隔符或行终结符的第一个字符不能是单引号或双引号。
  - QUOTES ON 将强制对给定文件进行单线程处理。
  - 无论 QUOTES 选项的设置如何，都不适用于从辅助文件装载二进制大对象 (BLOB) 或字符大对象 (CLOB) 数据。前导或尾随引号将作为 CLOB 数据的一部分来装载。使用 QUOTES ON 选项，位于引号之间的两个连续引号将作为两个连续引号进行装载。
  - Adaptive Server BCP 不支持 QUOTES 选项。拷入或拷出所有字段数据的方式与设置 QUOTES OFF 时的情况相同。由于 QUOTES ON 是 SAP Sybase IQ **LOAD TABLE** 语句的缺省设置，因此将 ASE 数据从 BCP 输出导入至 SAP Sybase IQ 表时，您必须指定 QUOTES OFF。

  例外情况：

  - 如果 **LOAD TABLE** 在引起来的字段的结尾引号字符之后遇到任何非空白字符，则将报告以下错误并回退装载操作：

```
Non-SPACE text found after ending quote character for
an enclosed field.
SQLSTATE: QTA14    SQLCODE: -1005014L
```

- 在 QUOTES 设置为 ON 的情况下，如果将单引号或双引号指定为列分隔符的第一个字符，则将报告错误并且装载操作将失败：

```
Single or double quote mark cannot be the 1st character
of column delimiter or row terminator with QUOTES option
ON.
SQLSTATE: QCA90    SQLCODE: -1013090L
```

- **ESCAPES** – 如果省略输入字段的 *column-spec* 定义，则在 ESCAPES 为 ON（缺省值）的情况下，数据库服务器会识别跟在反斜杠字符后的字符并将其解释为特殊字符。可以以组合形式 \n 添加换行符，以十六进制 ASCII 代码形式添加其它字符，例如，使用 \x09 表示制表符。两个连续的反斜线字符 (\\ ) 被解释为单个反斜线。对于 SAP Sybase IQ，必须设置 ESCAPES OFF。

- **FORMAT** – SAP Sybase IQ 支持 ASCII 和二进制输入字段。此格式通常由上述 *column-spec* 定义。如果省略列的此定义，则在缺省情况下，SAP Sybase IQ 使用此选项定义的格式。假定输入行具有 ascii（缺省值）或 **binary** 字段，每个输入行对应一行，并使用列分隔符来分隔各个值。

  SAP Sybase IQ 也允许将 BCP 字符文件中的数据作为 **LOAD TABLE** 命令的输入。

  - 使用 **LOAD TABLE FORMAT BCP** 语句装载到 SAP Sybase IQ 表中的 BCP 数据文件必须利用 -c 选项以跨平台文件格式进行导出 (BCP OUT)。
  - 对于 FORMAT BCP，**LOAD TABLE** 语句的缺省列分隔符是 <tab>，而缺省行终结符是 <newline>。
  - 对于 FORMAT BCP，行中的最后一列必须以行终结符终止，而不能以列分隔符终止。如果列分隔符位于行终结符之前，则将列分隔符视为数据的一部分。
  - 装载规范中除最后一列以外的所有列中的数据只能以列分隔符进行分隔。对于除最后一列以外的所有列，如果在列分隔符之前先遇到行终结符，则将行终结符视为列数据的一部分。
  - 可通过 DELIMITED BY 子句指定列分隔符。对于 FORMAT BCP，分隔符的长度必须小于或等于 10 个字符。如果分隔符长度大于 10，则返回错误。
  - 对于 FORMAT BCP，装载规范只能包含列名、NULL 和 ENCRYPTED。如果在装载规范中指定了任何其它选项，则返回错误。

    例如，下列即属于有效的 **LOAD TABLE** 装载规范：

```
LOAD TABLE x( c1, c2 null(blanks), c3 )
FROM 'bcp_file.bcp'
FORMAT BCP
...
```

```
LOAD TABLE x( c1 encrypted(bigint,'KEY-ONE','aes'), c2, c3 )
FROM 'bcp_file.bcp'
FORMAT BCP
...
```

- **DELIMITED BY** – 如果在 *column-spec* 定义中省略列分隔符，则缺省的列分隔符为逗号。通过提供单个 ASCII 字符或十六进制字符表示形式可指定其它列分隔符。DELIMITED BY 子句为：

  ```
  ... DELIMITED BY '\x09' ...
  ```

  要将换行符用作分隔符，您可以指定特殊组合 '\n' 或其 ASCII 值 '\x0a'。在 column-spec *delimiter-string* 中最多可指定四个字符，而在 DELIMITED BY 子句中只能指定一个字符。
- **STRIP** – 确定在插入不带引号的值之前是否应去除其尾随空白。**LOAD TABLE** 命令接受以下 STRIP 关键字：
  - **STRIP OFF** – 不去除尾随空白。
  - **STRIP RTRIM** – 去除尾随空白。
  - **STRIP ON** – 不建议使用。使用 STRIP RTRIM。

  在打开 STRIP 时（缺省情况），SAP Sybase IQ 首先将从值中去除尾随空白，然后再插入这些值。此设置仅适用于 VARCHAR 数据。STRIP OFF 会保留尾随空白。

  仅去除不带引号的字符串的尾随空白。带引号的字符串保留其尾随空白。如果不需要区分空白，可以使用 FILLER 选项作为替代选项，以便更确切地指定要去除的字节数，而不是去除所有尾随空格。对于 SAP Sybase IQ，STRIP OFF 会更有效，在处理尾随空白时，它会遵循 ANSI 标准。（CHAR 数据始终会进行填补，因此 STRIP 选项仅影响 VARCHAR 数据。）

  STRIP 选项仅适用于长度可变的非二进制数据，不适用于 ASCII 固定宽度插入。以下列模式为例：

  ```
  CREATE TABLE t( c1 VARCHAR(3) );
  LOAD TABLE t( c1 ',' ) ........ STRIP RTRIM    // trailing blanks
  trimmed

  LOAD TABLE t( c1 ',' ) ........ STRIP OFF      // trailing blanks
  not trimmed

  LOAD TABLE t( c1 ASCII(3) ) ... STRIP RTRIM    // trailing blanks
  not trimmed
  LOAD TABLE t( c1 ASCII(3) ) ... STRIP OFF      // trailing blanks
  trimmed

  LOAD TABLE t( c1 BINARY ) ..... STRIP RTRIM    // trailing blanks
  trimmed
  LOAD TABLE t( c1 BINARY ) ..... STRIP OFF      // trailing blanks
  trimmed
  ```

  始终剪裁二进制数据中的尾随空白。
- **WITH CHECKPOINT** – 确定 SAP Sybase IQ 是否执行检查点。此选项只适用于在 SAP Sybase IQ 数据库中装载 SQL Anywhere 表。

  缺省设置为 OFF。如果将此子句设置为 ON，则会在成功完成并记录语句之后执行检查点操作。如果服务器在提交连接后及下次检查点之前出现故障，则必须具

有用来装载表的数据文件才能成功完成恢复。不过，如果指定了 WITH CHECKPOINT ON，并且此后需要恢复，则在恢复时不需要数据文件。

如果数据库损坏，需要使用备份并应用当前的日志文件，则无论此子句的设置情况如何，都需要数据文件。

警告！ 如果将数据库选项 CONVERSION_ERROR 设置为 OFF，则可能会将错误的数据装载到表中而收不到任何错误报告。如果未指定 WITH CHECKPOINT ON，并且需要恢复数据库，则当恢复过程中 CONVERSION_ERROR 设置为 ON（缺省值）时，恢复可能失败。建议您不要在 CONVERSION_ERROR 设置为 OFF 且未指定 WITH CHECKPOINT ON 的情况下装载表。

另请参见 CONVERSION_ERROR 选项 [TSQL]。

- **BYTE ORDER** – 指定读取时的字节顺序。此选项适用于所有二进制输入字段。如果未定义，则此选项将被忽略。SAP Sybase IQ 始终以其所在计算机的本机格式读取二进制数据（缺省值为 NATIVE）。您还可以指定：
  - HIGH，当多字节数量以高位字节优先时（对于 Sun、IBM AIX 和 HP 等 big endian 平台而言）。
  - LOW，当多字节数量以低位字节优先时（对于 Windows 等 little endian 平台而言）。
- **LIMIT** – 指定要插入表中的最大行数。缺省值为 0，表示无限制。最大值为 $2^{31} - 1$ (2147483647) 行。
- **NOTIFY** – 指定每次在表中成功插入指定行数时将发送消息通知您。缺省值为 0，表示不打印任何通知。此选项的值将覆盖 NOTIFY_MODULUS 数据库选项的值。
- **ON FILE ERROR** – 指定 SAP Sybase IQ 在因输入文件不存在或没有读取该文件的正确权限而无法打开文件时应执行的操作。您可以指定以下其中一个操作：
  - **ROLLBACK** – 中止整个事务（缺省设置）。
  - **FINISH** – 结束已完成的插入操作并终止装载操作。
  - **CONTINUE** – 返回错误，但只是跳过该文件，然后继续执行装载操作。

  只允许有一个 ON FILE ERROR 子句。
- **PREVIEW** – 显示目标表中输入的布局，包括每列的起始位置、名称和数据类型。SAP Sybase IQ 将在装载过程开始时显示此信息。如果写入日志文件，此信息也会包含在日志中。
- **ROW DELIMITED BY delimiter-string** – 指定最大长度 4 字节的字符串，以指示输入记录的结尾。仅当行中的所有字段为以下任意一种情形时才能使用此选项：
  - 由列终结符分隔
  - 通过 DATE 或 DATETIME *column-spec* 选项定义数据
  - ASCII 固定长度字段

始终包含 ROW DELIMITED BY 以确保进行并行装载。从 LOAD 规范中删除此子句可能会导致 SAP Sybase IQ 以串行方式而非并行方式进行装载。

如果任何输入字段包含二进制数据，则无法使用此选项。使用此选项，行终结符将使任何缺失字段设置为 NULL。所有行均必须具有相同的行分隔符，并且必须区别于所有列分隔符。行分隔符字符串和字段分隔符字符串彼此不能为初始子集。例如，不能指定 "*" 作为字段分隔符并指定 "*#" 作为行分隔符，但可以与该行分隔符一起指定 "#" 作为字段分隔符。

如果行缺少分隔符，则 SAP Sybase IQ 会返回错误并回退整个装载事务。唯一一种例外情况是文件的最后一条记录，系统会回退该行并返回警告消息。在 Windows 上，通常由换行符后跟回车符表示行分隔符。对于此选项或 FILLER，您可能需要将此指定为 *delimiter-string*（见以上说明）。

- **SKIP** – 定义此装载要在输入表开头跳过的行数。要跳过的最大行数为 $2^{31} - 1$ (2147483647)。缺省值为 0。SKIP 在读取要跳过的行时以单线程模式运行。
- **HEADER SKIP…HEADER DELIMITED BY** – 指定 **LOAD TABLE** 要在数据文件开头跳过的行数，其中包括标题行。在跳过指定的行数之前，将忽略所有的 **LOAD TABLE** 列规范及其它装载选项。
  - 要跳过的行数大于或等于零。
  - 行由 HEADER DELIMITED BY 子句中指定的长度为 1 到 4 个字符的分隔符字符串确定。缺省的 HEADER DELIMITED BY 字符串为 '\n' 字符。
  - HEADER DELIMITED BY 字符串的最大长度为四个字符。如果字符串长度大于 4 或小于 1，将返回错误。
  - 如果指定了非零 HEADER SKIP 值，则会忽略包含 HEADER DELIMITED BY 分隔符的所有数据，直到分隔符的出现次数达到 HEADER SKIP 子句中指定的次数。
  - 在跳过指定的行数之前，将忽略所有的 **LOAD TABLE** 列规范及其它装载选项。在跳过指定的行数后，**LOAD TABLE** 列规范及其它装载选项将应用于剩余数据。
  - 仅忽略数据开头处的“标题”字节。如果在 USING 子句中指定了多个文件，HEADER SKIP 将只忽略从第一个文件的第一行开始的数据，直到跳过指定的标题行数，即使这些行位于后面的文件中。**LOAD TABLE** 在开始解析实际数据后便不会寻找标题。
  - 如果 **LOAD TABLE** 在跳过 HEADER SKIP 指定的行数之前处理所有输入数据，则不会报告错误。
- **WORD SKIP** – 遇到长度超过创建字索引时所指定限制的数据时，允许装载继续进行。

  如果因字超过最大允许大小而未能装载某一行，则会向 `.iqmsg` 文件写入一条警告。还可以选择将 WORD 大小违规记录到 MESSAGE LOG 文件中，并将被拒绝的行记录到 **LOAD TABLE** 语句中指定的 ROW LOG 文件。

- 如果未指定此选项，则 **LOAD TABLE** 将在第一次遇到长度超过指定限制的字时报告错误并回退。
- *number* 指定忽略“字不能超过允许的最大字长度”错误的次数。
- 0（零）表示没有限制。

- **ON PARTIAL INPUT ROW** – 指定在装载期间遇到部分输入行时执行的操作。您可以指定以下其中一个操作：
  - CONTINUE 发出警告并继续执行装载操作。这是缺省设置。
  - ROLLBACK 中止整个装载操作并报告错误。

    ```
    Partial input record skipped at EOF.
    SQLSTATE: QDC32    SQLSTATE: -1000232L
    ```

- **IGNORE CONSTRAINT** – 指定是否忽略装载期间发生的 CHECK、UNIQUE、NULL、DATA VALUE 和 FOREIGN KEY 完整性约束违规，以及在启动回退之前忽略的最大违规次数。指定每个 *constrainttype* 都具有以下结果：
  - **CHECK limit** – 如果 *limit* 指定为零，则将要忽略的 CHECK 约束违规次数将无限制。如果未指定 CHECK，则首次发生任何 CHECK 约束违规时都将导致 **LOAD** 语句回退。如果 *limit* 为非零，则发生 *limit* +1 次 CHECK 约束违规后将导致装载回退。
  - **UNIQUE *limit*** – 如果 *limit* 指定为零，则要忽略的 UNIQUE 约束违规次数将无限制。如果 *limit* 为非零，则发生 *limit* +1 次 UNIQUE 约束违规后将导致装载回退。
  - **NULL *limit*** – 如果 *limit* 指定为零，则要忽略的 NULL 约束违规次数将无限制。如果 *limit* 为非零，则发生 *limit* +1 次 NULL 约束违规后将导致装载回退。
  - **FOREIGN KEY *limit*** – 如果 *limit* 指定为零，则要忽略的 FOREIGN KEY 约束违规次数将无限制。如果 *limit* 为非零，则发生 *limit* +1 次 FOREIGN KEY 约束违规后将导致装载回退。
  - **DATA VALUE *limit*** – 如果数据库选项 CONVERSION_ERROR 为 ON，则将报告错误并回退语句。如果 *limit* 指定为零，则要忽略的 DATA VALUE 约束违规（数据类型转换错误）次数将无限制。如果 *limit* 为非零，则发生 *limit* +1 次 DATA VALUE 约束违规后将导致装载回退。
  - **ALL *limit*** – 如果数据库选项为 `CONVERSION_ERROR = ON`，则将报告错误并回退语句。如果 *limit* 指定为零，则要忽略的所有完整性约束违规的累计总数将无限制。如果 *limit* 为非零，则在忽略的所有 UNIQUE、NULL、DATA VALUE 和 FOREIGN KEY 完整性约束违规累计总数超过 *limit* 值时，装载将回退。例如，可指定此 IGNORE CONSTRAINT 选项：

    ```
    IGNORE CONSTRAINT NULL 50, UNIQUE 100, ALL 200
    ```

    完整性约束违规的总数不能超过 200，而 NULL 和 UNIQUE 约束违规的总数分别不能超过 50 和 100。只要超出这些限制中的任何一个，LOAD TABLE 语句便会回退。

注意： 单个行可具有多个完整性约束违规。每出现一次完整性约束违规便计一次，直至达到该类违规的限定值。

如果要记录忽略的完整性约束违规，可将 IGNORE CONSTRAINT 选项限制设置为非零值。记录过多的违规数会影响装载性能

如果在 IGNORE CONSTRAINT 子句中未指定 CHECK、UNIQUE、NULL 或 FOREIGN KEY，则在第一次发生上述其中一种完整性约束违规时，装载将回退。

如果未在 IGNORE CONSTRAINT 子句中指定 DATA VALUE，则当首次发生这种类型的完整性约束违规时，将回退装载，但如果数据库选项为 `CONVERSION_ERROR = OFF` 则例外。如果为 `CONVERSION_ERROR = OFF`，则对于任何 DATA VALUE 约束违规，都将发出警告并继续装载。

装载完成时，将在 `.iqmsg` 文件中记录一条与完整性约束违规有关的信息性消息。此消息包含装载时发生的完整性约束违规次数及跳过的行数。

- **MESSAGE LOG** – 指定要在其中记录完整性约束违规和要记录的违规类型信息的文件的名称。表示装载开始和完成的时间戳记录在 MESSAGE LOG 和 ROW LOG 文件中。必须指定 MESSAGE LOG 和 ROW LOG，否则将不记录与完整性违规有关的信息。
  - 如果未指定 ONLY LOG 子句，则不会记录有关完整性约束违规的信息。而是只记录表示装载开始和完成的时间戳。
  - 对于 ONLY LOG 子句中指定的所有完整性约束类型违规，或在指定关键字 WORD 情况下的所有字索引长度违规，将记录相关违规信息。
  - 如果记录约束违规，则每次发生完整性约束违规时，将在 MESSAGE LOG 文件中生成一行信息。

    由于装载是由并行运行的多个线程执行的，MESSAGE LOG 文件中的行数（报告的错误）可能会超出 IGNORE CONSTRAINT 选项限制。可能会有多个线程报告约束违规次数超出指定限值。
  - 如果记录约束违规，则对于某一给定行，将在 ROW LOG 文件中记录一行信息，而不考虑该行发生的完整性约束违规次数。

    MESSAGE LOG 文件中的不同错误数可能与 ROW LOG 文件中的行数不完全匹配。行数差是由于 MESSAGE LOG 的上述并行装载处理造成的。
  - MESSAGE LOG 和 ROW LOG 文件不能为原始分区或命名管道。
  - 如果已存在 MESSAGE LOG 或 ROW LOG 文件，则会将新信息附加到相应文件。
  - 为 MESSAGE LOG 或 ROW LOG 文件指定无效文件名将产生错误。
  - 为 MESSAGE LOG 和 ROW LOG 文件指定相同的文件名将产生错误。

  IGNORE CONSTRAINT 和 MESSAGE LOG 选项的各种组合会导致不同的记录操作。

表 12. LOAD TABLE 记录操作

是否已指定 IGNORE CONSTRAINT？	是否已指定 MESSAGE LOG？	操作
是	是	回退之前，将记录所有被忽略的完整性约束违规（包括用户指定的限制）。
否	是	回退之前，将记录第一次完整性约束违规。
是	否	不记录任何信息。
否	否	不记录任何信息。第一次发生完整性约束违规即会导致回退。

提示： 如果要记录忽略的完整性约束违规，可将 IGNORE CONSTRAINT 选项限制设置为非零值。如果单行出现多次完整性约束违规，则将针对每次违规在 MESSAGE LOG 文件中写入一行。记录过多的违规数会影响装载性能。

- **LOG DELIMITED BY** – 指定 ROW LOG 文件中各数据值之间的分隔符。缺省分隔符为逗号。

  将 FORMAT BCP 指定为 **LOAD TABLE** 子句时，SAP Sybase IQ 不再返回错误消息。此外，会验证以下情况，并返回相应的错误消息

  - 如果指定的装载格式不是 ASCII、BINARY 或 BCP，SAP Sybase IQ 会返回消息“`LOAD 格式仅支持 ASCII、BCP 和 BINARY。`”
  - 如果 **LOAD TABLE** 列规范包含除列名、NULL 或 ENCRYPTED 以外的任何内容，SAP Sybase IQ 会返回错误消息“`LOAD ... FORMAT BCP 的装载说明无效。`”
  - 如果 FORMAT BCP 装载的列分隔符或行终结符的大小超过 10 个字符，SAP Sybase IQ 会返回消息“`分隔符 '%2' 的长度必须为 1 到 %3 个字符。`”(其中 %3 等于 10）。

    对于 FORMAT BCP 和 FORMAT ASCII 出现的错误或警告情况，与这些情况相对应的消息对于两种格式而言都是相同的。
  - 如果指定的装载缺省值为 AUTOINCREMENT、IDENTITY 或 GLOBAL AUTOINCREMENT，SAP Sybase IQ 会返回错误“`缺省值 %2 不能用作 LOAD 缺省值。%1`”
  - 如果 **LOAD TABLE** 规范不包含需要从指定文件装载的任何列，SAP Sybase IQ 会返回错误“`LOAD 语句必须至少包含要从输入文件中装载的 1 列。`”并回退 **LOAD TABLE** 语句。
  - 如果装载超出了具有 TEXT 索引的文本文档的最大词语数限制，SAP Sybase IQ 会返回错误“文本文档超出最大词语数。每个文档最多支持 `4294967295` 个词语。”

示例

(返回顶部) (第 178 页)

- **示例 1** – 将数据从一个文件装载到 Windows 系统上的 `Products` 表中。使用制表符作为列分隔符，后跟 `Description` 和 `Color` 列：

```
LOAD TABLE Products
( ID ASCII(6),
FILLER(1),
Name   ASCII(15),
FILLER(1),
Description   '\x09',
Size   ASCII(2),
FILLER(1),
Color   '\x09',
Quantity   PREFIX 2,
UnitPrice   PREFIX 2,
FILLER(2) )
FROM 'C:\\mydata\\source1.dmp'
QUOTES OFF
ESCAPES OFF
BYTE ORDER LOW
NOTIFY 1000
```

- **示例 2** – 从客户端计算机上的文件 `a.inp` 装载数据：

```
LOAD TABLE t1(c1,c2,filler(30))
USING CLIENT FILE 'c:\\client-data\\a.inp'
QUOTES OFF ESCAPES OFF
IGNORE CONSTRAINT UNIQUE 0, NULL 0
MESSAGE LOG 'c:\\client-data\\m.log'
ROW LOG 'c:\\client-data\\r.log'ONLY LOG UNIQUE
```

- **示例 3** – 将数据从两个文件装载到 UNIX 系统上的 `product_new` 表中（该表允许 NULL 值）。制表符为缺省的列分隔符，并且使用换行符作为行分隔符：

```
LOAD TABLE product_new
( id,
name,
description,
size,
color   '\x09'   NULL( 'null', 'none', 'na' ),
quantity   PREFIX 2,
unit_price   PREFIX 2 )
FROM '/s1/mydata/source2.dump',
'/s1/mydata/source3.dump'
QUOTES OFF
ESCAPES OFF
FORMAT ascii
DELIMITED BY '\x09'
ON FILE ERROR CONTINUE
ROW DELIMITED BY '\n'
```

- **示例 4** – 忽略 10 字长度违规；出现第 11 个字时，配置新错误并回退装载：

```
load table PTAB1(
       ck1         ','  null ('NULL') ,
```

```
       ck3fk2c2    ','  null ('NULL') ,
       ck4         ','  null ('NULL') ,
       ck5         ','  null ('NULL') ,
       ck6c1       ','  null ('NULL') ,
       ck6c2       ','  null ('NULL') ,
       rid         ','  null ('NULL')  )
FROM 'ri_index_selfRI.inp'
       row delimited by '\n'
       LIMIT 14   SKIP 10
       IGNORE CONSTRAINT UNIQUE 2, FOREIGN KEY 8
       word skip 10 quotes off escapes off strip
       off
```

- **示例 5** – 使用 **FORMAT BCP** 装载选项将数据从 **BCP** 字符文件 `bcp_file.bcp` 装载到表 `t1`:

```
LOAD TABLE t1 (c1, c2, c3)
FROM ‘bcp_file.bcp’
FORMAT BCP
...
```

- **示例 6** – 使用 **DEFAULT** 装载选项将缺省值 12345 装载到 `c1`，从 `LoadConst04.dat` 文件向 `c2` 和 `c3` 装载数据:

```
LOAD TABLE t1 (c1 DEFAULT ‘12345 ’ , c2, c3, filler(1))
FROM ‘LoadConst04.dat’
STRIP OFF
QUOTES OFF
ESCAPES OFF
DELIMITED BY ‘,’ ;
```

- **示例 7** – 使用 **FORMAT BCP** 装载选项从文件 `bcp_file.bcp` 向 `c1` 和 `c2` 装载数据，并将 `c3` 的值设置为 10:

```
LOAD TABLE t1 (c1, c2, c3 DEFAULT ‘10’)
FROM ‘bcp_file.bcp’
FORMAT BCP
QUOTES OFF
ESCAPES OFF;
```

- **示例 8** – 以下代码段会忽略数据文件开头处用 '&&' 分隔的一个标题行:

```
LOAD TABLE
...HEADER SKIP 1 HEADER DELIMITED by '&&'
```

- **示例 9** – 以下代码段会忽略数据文件开头处用 '\n' 分隔的 2 个标题行:

```
LOAD TABLE
...HEADER SKIP 2
```

- **示例 10** – 将文件装载到启用 RLV 的表中。

  使用 **FORMAT BCP** 装载选项将数据从 **BCP** 字符文件 `bcp_file.bcp` 装载到启用 RLV 的表 `rvt1` 中:

```
LOAD TABLE rvt1 (c1, c2, c3)
FROM ‘bcp_file.bcp’
```

```
FORMAT BCP
...
```

用法

(返回顶部) (第 178 页)

LOAD TABLE 允许执行从带有 ASCII 或二进制数据的文件到数据库表的高效的大量插入。

使用 **LOAD TABLE** 选项也可以控制违反完整性约束时的装载行为并且记录有关违规的信息。

对临时表可以使用 **LOAD TABLE**，但是该临时表必须是用 **ON COMMIT PRESERVE ROWS** 声明的，否则下一条 **COMMIT** 将删除已装载的行。

LOAD TABLE 支持装载大对象 (LOB) 数据。

SAP Sybase IQ 支持从 ASCII 和二进制数据装载，并且支持固定长度格式和可变长度格式。要处理所有这些格式，您必须提供一个 *load-specification* 来通知 SAP Sybase IQ 需要从源文件中的每个“列”或字段获得何种数据。可通过 *column-spec* 定义下列格式：

- 具有固定字节长度的 ASCII。*input-width* 值是表示每条记录中输入字段的固定宽度的整数（单位为字节）。
- 使用一定数量的 PREFIX 字节（1、2 或 4）指定输入长度的二进制或非二进制字段。

  以下两部分与 **PREFIX** 子句相关：
  - 前缀值 – 始终为二进制值。
  - 关联数据字节 – 始终为字符格式，永远不采用二进制格式。

  如果使用抽取工具卸载数据时将 TEMP_EXTRACT_BINARY 选项设置为 ON，则在装载二进制数据时必须针对每个列使用 **BINARY WITH NULL BYTE** 参数。
- 由分隔符分隔的可变长度字符。可以将终结符指定为十六进制 ASCII 字符。*delimiter-string* 可以是由最多 4 个字符构成的任意字符串，包括可打印字符的任意组合以及表示非打印字符的任意 8 位十六进制 ASCII 代码。例如，指定：
  - '\x09'，以将制表符表示为终结符。
  - '\x00'，表示空终结符（如同 "C" 字符串中一样，没有可见终结符）。
  - '\x0a'，表示作为终结符的换行符。还可以使用特殊字符组合 "\n" 作为换行符。

  注意： 分隔符字符串长度可为 1 到 4 个字符，但在 **DELIMITED BY** 子句中只能指定单个字符。对于 **BCP**，分隔符最多可达 10 个字符。
- ASCII 字符形式的 DATE 或 DATETIME 字符串。必须使用 SAP Sybase IQ 支持的日期数据类型和日期时间数据类型的对应格式之一定义字符串的 *input-date-format* 或 *input-datetime-format*。使用 **DATE** 表示日期值，并使用 **DATETIME** 表示日期时间和时间值。

表 13. 格式化日期和时间

选项	含义
yyyy 或 YYYY yy 或 YY	表示年份数字。缺省值为当前年份。
mm 或 MM	表示月份数字。适当情况下始终在月份数字中使用前导零或空白，例如，"05" 表示 5 月。DATE 值必须包含月份。例如，如果您输入的 **DATE** 值为 1998，则会收到错误提示。如果输入 "03"，则 SAP Sybase IQ 将应用缺省年份和日期，并将其转换为 '1998-03-01'。
dd 或 DD jjj 或 JJJ	表示日期数字。缺省日期为 01。适当情况下始终在日期数字中使用前导零，例如，'01' 表示第一天。J 或 j 表示一年中的儒略日（1 至 366）。
hh HH	表示小时。小时基于 24 小时制。适当情况下始终在小时中使用前导零或空白，例如，'01' 表示凌晨 1 点。'00' 也是有效值，表示中午 12 点。
nn	表示分钟。适当情况下始终在分钟中使用前导零，例如，'08' 表示 8 分钟。
ss[.ssssss]	表示秒和秒的小数部分。
aa	表示 a.m. 或 p.m. 标记。
pp	仅当需要时表示 p.m. 标记。（这与 12.0 之前的 SAP Sybase IQ 版本不兼容；先前 "pp" 与 "aa" 是同义词。）
hh	SAP Sybase IQ 假设分钟和秒钟均为零。例如，如果您输入的 **DATETIME** 值为 '03'，则 SAP Sybase IQ 将该值转换为 '03:00:00.0000'。
hh:nn 或 hh:mm	SAP Sybase IQ 假设秒钟为零。例如，如果您输入的时间值为 '03:25'，则 SAP Sybase IQ 将该值转换为 '03:25:00.0000'。

表 14. 示例 DATE 和 DATETIME 格式选项

输入数据	格式规范
12/31/98	DATE ('MM/DD/YY')
19981231	DATE ('YYYYMMDD')
123198140150	DATETIME ('MMDDYYhhnnss')
14:01:50 12-31-98	DATETIME ('hh:nn:ss MM-DD-YY')
18:27:53	DATETIME ('hh:nn:ss')
12/31/98 02:01:50AM	DATETIME ('MM/DD/YY hh:nn:ssaa')

SAP Sybase IQ 针对常用日期、时间和日期时间格式提供了内置装载优化。如果您要装载的数据与其中一种格式匹配，则使用相应的格式可以显著缩短装载时间。

还可以将日期/时间字段指定为 ASCII 固定宽度字段（如上所述），并使用 FILLER(1) 选项跳过列分隔符。

装载到表列中时，*column-spec* 的 NULL 部分指示如何将某些输入值视为 NULL 值。这些字符可能包括 BLANKS、ZEROS 或您定义的任何其它文字列表。指定 NULL 值或从源文件读取 NULL 值时，目标列必须能够包含 NULL。

ZEROS 含义如下：如果（并且仅当）输入数据（转换前，如果为 ASCII）均为二进制零（而不为字符零），则此单元设置为 NULL。

- 如果输入数据为字符零，则：
  1. NULL (ZEROS) 永远不会导致单元变为 NULL。
  2. NULL ('0') 导致单元变为 NULL。
- 如果输入数据为二进制零（清除所有位），则：
  1. NULL (ZEROS) 导致单元变为 NULL。
  2. NULL ('0') 永远不会导致单元变为 NULL。

例如，如果 **LOAD** 语句包含 `col1 date('yymmdd') null(zeros)` 并且日期为 000000，则会收到错误消息，提示您 000000 无法转换为 `DATE`(4)。若要使 **LOAD TABLE** 在数据为 000000 时在 `col1` 中插入空值，请将 NULL 子句编写为 `null('000000')`，或将数据修改为相同数目的二进制零并使用 NULL(ZEROS)。

如果 `VARCHAR` 单元的长度为零并且该单元不为空值，则将获得一个零长度单元。对于所有其它数据类型来说，如果单元长度为零，SAP Sybase IQ 将插入 NULL。这是 ANSI 行为。对于零长度字符数据的非 ANSI 处理，请设置 **NON_ANSI_NULL_VARCHAR** 数据库选项。

使用 **DEFAULT** 选项指定装载缺省列值。即使列未在表模式中定义缺省值，您仍可以向该列装载缺省值。在装载时，此功能可提供更大的灵活性。

- **LOAD TABLE DEFAULTS** 选项必须为 ON 才能使用 **LOAD TABLE** 语句中指定的缺省值。如果 **DEFAULTS** 选项为 OFF，则不会使用指定的装载缺省值，而会在列中插入 NULL 值。
- **LOAD TABLE** 命令必须包含至少一个需要从 **LOAD TABLE** 命令所指定的文件中装载的列。否则将报告错误，并且不会执行装载。
- 指定的装载缺省值必须符合受支持的列缺省值和缺省值限制。**LOAD TABLE DEFAULT** 选项不支持 **AUTOINCREMENT**、**IDENTITY** 或 **GLOBAL AUTOINCREMENT** 作为装载缺省值。
- **LOAD TABLE DEFAULT** *default-value* 必须属于数据库的字符集。
- 对于在 **LOAD TABLE DEFAULT** 子句中指定的装载缺省值，不支持对缺省值进行加密。
- 对于在表中插入的每行，将计算因评估指定装载缺省值而引起的约束冲突的总数。

load-specification 的另一重要部分是 **FILLER** 选项。此选项指示您希望跳过源输入文件中的指定字段。例如，在输入文件中的行末尾或整个字段可能会存在不希望添加到表中的字符。与 *column-spec* 定义一样，使用 **FILLER** 可以指定 ASCII 固定字节长度、由分隔符分隔的可变长度字符，以及使用 PREFIX 字节的二进制字段。

标准

(返回顶部) (第 178 页)

- SQL - ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - 不适用。

权限

(返回顶部) (第 178 页)

执行 **LOAD TABLE** 语句所需的权限取决于数据库服务器的 **-gl** 命令行选项，如下所示:

- **-gl ALL** – 您必须是表的所有者，对表具有 ALTER 或 LOAD 权限，或者具有 ALTER ANY TABLE、LOAD ANY TALBE 或 ALTER ANY OBJECT 系统特权。
- **-gl DBA** – 您必须具有 ALTER ANY TABLE、LOAD ANY TABLE 或 ALTER ANY OBJECT 系统特权。
- **-gl NONE** – 不允许执行 **LOAD TABLE** 语句。

有关 **-gl** 命令行选项的详细信息，请参阅《实用程序指南》>“start_iq 数据库服务器启动实用程序”>“start_iq 服务器选项”。

LOAD TABLE 还需要对表进行写锁定。

对加密文本进行字符串比较

如果数据不区分大小写，或者使用 ISO_BINENG 以外的归类，则必须对密码文本列进行解密，以便执行字符串比较。

当对字符串执行比较时，对于许多归类而言，等同字符串和相同字符串之间的区别非常重要，并且取决于 **CREATE DATABASE** 的 **CASE** 选项。在设置为 **CASE RESPECT** 且采用 ISO_BINENG 归类的数据库中，将以相同方式解决 SAP Sybase IQ 的缺省值、等同性和相同性问题。

相同字符串始终是等同的，但等同字符串有可能不相同。仅当字符串使用相同字节值表示时，它们才是相同的。当数据不区分大小写或使用必须将多个字符视为等同的归类时，等同性和相同性之间的区别非常重要。ISO1LATIN1 便是这种类型的归类。

例如，字符串 "ABC" 和 "abc" 在不区分大小写的数据库中不相同，但二者等同。在区分大小写的数据库中，上述字符串既不相同也不等同。

Sybase 加密函数创建的密文保留相同性，但不保留等同性。换句话说，"ABC" 和 "abc" 密文永远不会等同。

若要在归类或 **CASE** 设置不允许等同性比较的情况下对密文执行等同性比较，应用程序必须将该列中的值修改为某种规范形式，即任何等同值都是相同值。例如，如果数据库是使用 **CASE IGNORE** 和 ISO_BINENG 归类创建的，且应用程序在将所有输入值放入列中之前向所有输入值应用了 UCASE，则所有等同值都是相同的。

列加密的数据库选项

某些 SAP Sybase IQ 数据库选项设置会影响列的加密和解密；缺省设置对于大多数列加密操作而言都不是最佳设置。

防止密文意外截断

为防止加密函数的密码文本输出被意外截断（或防止任何其它字符或二进制字符串被意外截断），请设置 STRING_RTRUNCATION 数据库选项。

```
SET OPTION STRING_RTRUNCATION = 'ON'
```

当 STRING_RTRUNCATION 设置为 ON（缺省值）时，只要在装载、插入、更新或 **SELECT INTO** 操作期间字符串被截断，引擎就会引发错误。这是 ISO/ANSI SQL 行为，也是推荐做法。

当需要执行显式截断时，请使用诸如 **LEFT**、**SUBSTRING** 或 **CAST** 之类的字符串表达式。

将 STRING_RTRUNCATION 设置为 OFF 会对字符串强制执行无提示截断。

AES_DECRYPT 函数也会检查输入密码文本的有效数据长度，并检查文本输出以验证所得数据的长度以及所提供密钥的正确性。如果提供数据类型参数，那么也会检查数据类型。

保护密文的完整性

设置 ASE_BINARY_DISPLAY 以保留密码文本的完整性。

```
SET OPTION ASE_BINARY_DISPLAY = 'OFF'
```

当 ASE_BINARY_DISPLAY 设置为 OFF（缺省值）时，系统将不修改二进制数据，保持其原始二进制形式不变。

当 ASE_BINARY_DISPLAY 设置为 ON 时，系统会将二进制数据转换为其十六进制字符串显示表示形式。只有需要向最终用户显示数据或者需要将数据导出至另一个外部系统时，才可临时将该选项设置为 ON，在这两种情况下，原始二进制形式在传递过程中可能会发生改变。

防止误用密文

设置 CONVERSION_MODE 以防止对加密数据进行隐式数据类型转换（这种转换可导致在语义上无意义的操作）。

CONVERSION_MODE 数据库选项限制各种操作中二进制数据类型（BINARY、VARBINARY 和 LONG BINARY）与其它非二进制数据类型（BIT、TINYINT、SMALLINT、INT、UNSIGNED INT、BIGINT、UNSIGNED BIGINT、CHAR、VARCHAR 和 LONG VARCHAR）之间的隐式转换：

```
SET TEMPORARY OPTION CONVERSION_MODE = 1
```

将 CONVERSION_MODE 设置为 1，可在执行 **INSERT** 和 **UPDATE** 命令以及执行查询时限制二进制数据类型到任何其它非二进制数据类型的隐式转换。这种限制二进制转换模式还适用于 **LOAD TABLE** 缺省值和 **CHECK** 约束。

CONVERSION_MODE 选项采用缺省值 0 时，可保留 SAP Sybase IQ 12.7 版之前的二进制数据类型隐式转换行为。

CONVERSION_MODE 选项
限制各种操作中二进制数据类型（BINARY、VARBINARY 和 LONG BINARY）与其它非二进制数据类型（BIT、TINYINT、SMALLINT、INT、UNSIGNED INT、BIGINT、UNSIGNED BIGINT、CHAR、VARCHAR 和 LONG VARCHAR）之间的隐式转换。

允许值
0, 1

默认值
0

范围
可在数据库 (PUBLIC) 或用户级别设置选项。在数据库级别进行设置时，值将变为任何新用户的缺省值，但不会对现有用户产生任何影响。在用户级别进行设置时，仅替换该用户的 PUBLIC 值。为自身设置选项无需任何系统特权。在数据库或用户级别为任何其他用户设置选项都需要系统特权。

必须具有 SET ANY PUBLIC OPTION 系统特权才能设置此选项。可针对个别连接或 PUBLIC 角色进行临时设置。设置立即生效。

注释
缺省值 0 将保留 12.7 版之前的隐式转换行为。将 **CONVERSION_MODE** 设置为 1，可在执行 **INSERT**、**UPDATE** 以及查询时限制二进制数据类型到任何其它非二进制数据类型的隐式转换。这种限制二进制转换模式还适用于 **LOAD TABLE** 缺省值和 CHECK 约束。**CONVERSION_MODE 1** 可防止对加密数据进行隐式数据类型转换（这种转换可导致在语义上无意义的操作）。

用户必须获得专门许可，才能使用 SAP Sybase IQ“高级安全性选项”的加密列功能。

隐式转换限制
CONVERSION_MODE 选项限制为二进制模式值 1 (**CONVERSION_MODE** = 1)，将限制以下操作的隐式转换：

- 具有 CHECK 约束或缺省值的 **LOAD TABLE**
- **INSERT...SELECT**、**INSERT...VALUE** 和 **INSERT...LOCATION**
- 特定类型的 **UPDATE**
- 通过可更新游标进行的特定类型的 **INSERT** 和 **UPDATE**

- 一般查询的各个方面

加密和解密示例

使用 **AES_ENCRYPT** 和 **AES_DECRYPT** 函数的示例，该示例是用带注释的 SQL 编写的。

```
--   This example of aes_encrypt and aes_decrypt function use is
presented in three parts:
--
-- Part I: Preliminary description of target tables and users as DDL
-- Part II: Example schema changes motivated by introduction of
encryption
-- Part III: Use of views and stored procedures to protect encryption
keys
--


--   Part I: Define target tables and users

--   Assume two classes of user, represented here by the instances
--   PrivUser and NonPrivUser, assigned to groups reflecting
differing
--   privileges.

--   The initial state reflects the schema prior to the introduction
--   of encryption.

--   Set up the starting context: There are two tables with a common
key.
--   Some columns contain sensitive data, the remaining columns do
not.
--   The usual join column for these tables is sensitiveA.
--   There is a key and a unique index.

    grant connect to PrivUser identified by 'verytrusted' ;
    grant connect to NonPrivUser identified by 'lesstrusted' ;

    grant connect to high_privileges_group ;
    create role high_privileges_group ;
    grant role high_privileges_group to PrivUser ;

    grant connect to low_privileges_group ;
    create role low_privileges_group ;
    grant role low_privileges_group to NonPrivUser ;

    create table DBA.first_table
                    (sensitiveA char(16) primary key
                    ,sensitiveB numeric(10,0)
                    ,publicC    varchar(255)
                    ,publicD    date
                    )  ;


--   There is an implicit unique HG (HighGroup) index enforcing the
```

```
primary key.

    create table second_table
                    (sensitiveA char(16)
                    ,publicP integer
                    ,publicQ tinyint
                    ,publicR varchar(64)
                    )  ;

    create hg index second_A_HG on second_table ( sensitiveA ) ;

--   TRUSTED users can see the sensitive columns.

    grant select ( sensitiveA, sensitiveB, publicC, publicD )
        on DBA.first_table to PrivUser ;
    grant select ( sensitiveA, publicP, publicQ, publicR )
        on DBA.second_table to PrivUser ;

--   Non-TRUSTED users in existing schema need to see sensitiveA to
be
--   able to do joins, even though they should not see sensitiveB.

    grant select ( sensitiveA, publicC, publicD )
        on DBA.first_table to NonPrivUser ;
    grant select ( sensitiveA, publicP, publicQ, publicR )
        on DBA.second_table to NonPrivUser ;

--   Non-TRUSTED users can execute queries such as

    select I.publicC, 3*II.publicQ+1
    from DBA.first_table I, DBA.second_table II
    where I.sensitiveA = II.sensitiveA and I.publicD IN
( '2006-01-11' ) ;

--   and

    select count(*)
    from DBA.first_table I, DBA.second_table II
    where I.sensitiveA = II.sensitiveA and SUBSTR(I.sensitiveA,4,3)
    BETWEEN '345' AND '456' ;

--   But only TRUSTED users can execute the query

    select I.sensitiveB, 3*II.publicQ+1
    from DBA.first_table I, DBA.second_table II
    where I.sensitiveA = II.sensitiveA and I.publicD IN
( '2006-01-11' ) ;


--   Part II: Change the schema in preparation for encryption
--
--    The DBA introduces encryption as follows:
--
--    For applicable tables, the DBA changes the schema, adjusts
access
--    permissions, and updates existing data. The encryption
```

```
--    keys used are hidden in a subsequent step.


--   DataLength comparison for length of varbinary encryption result
--   (units are Bytes):
--
--    PlainText CipherText    Corresponding Numeric Precisions
--
--            0         16
--      1 -  16         32      numeric(1,0)   - numeric(20,0)
--     17 -  32         48      numeric(21,0)  - numeric(52,0)
--     33 -  48         64      numeric(53,0)  - numeric(84,0)
--     49 -  64         80      numeric(85,0)  - numeric(116,0)
--     65 -  80         96      numeric(117,0) - numeric(128,0)
--     81 -  96        112
--     97 - 112        128
--    113 - 128        144
--    129 - 144        160
--    145 - 160        176
--    161 - 176        192
--    177 - 192        208
--    193 - 208        224
--    209 - 224        240

--   The integer data types tinyint, small int, integer, and bigint
--   are varbinary(32) ciphertext.

--   The exact relationship is
--   DATALENGTH(ciphertext) =
--   (((DATALENGTH(plaintext)+ 15) / 16) + 1) * 16

--   For the first table, the DBA chooses to preserve both the
plaintext and
--   ciphertext forms. This is not typical and should only be done if
the
--   database files are also encrypted.

--   Take away NonPrivUser's access to column sensitiveA and transfer
--   access to the ciphertext version.

--   Put a unique index on the ciphertext column. The ciphertext
--   itself is indexed.

--   NonPrivUser can select the ciphertext and use it.

--   PrivUser can still select either form (without paying decrypt
costs).

    revoke select ( sensitiveA ) on DBA.first_table from
NonPrivUser ;
    alter table DBA.first_table add encryptedA varbinary(32) ;
    grant select ( encryptedA ) on DBA.first_table to PrivUser ;
    grant select ( encryptedA ) on DBA.first_table to NonPrivUser ;
    create unique hg index first_A_unique on first_table
( encryptedA ) ;
    update DBA.first_table
```

```
        set encryptedA = aes_encrypt(sensitiveA, 'seCr3t')
        where encryptedA is null ;
    commit

--   Now change column sensitiveB.

    alter table DBA.first_table add encryptedB varbinary(32) ;
    grant select ( encryptedB ) on DBA.first_table to PrivUser ;
    create unique hg index first_B_unique on first_table
( encryptedB ) ;
    update DBA.first_table
        set encryptedB = aes_encrypt(sensitiveB,
        'givethiskeytonoone') where encryptedB is null ;
    commit

--   For the second table, the DBA chooses to keep only the
ciphertext.
--   This is more typical and encrypting the database files is not
required.

    revoke select ( sensitiveA ) on DBA.second_table from
NonPrivUser ;
    revoke select ( sensitiveA ) on DBA.second_table from PrivUser ;
    alter table DBA.second_table add encryptedA varbinary(32) ;
    grant select ( encryptedA ) on DBA.second_table to PrivUser ;
    grant select ( encryptedA ) on DBA.second_table to NonPrivUser ;
    create unique hg index second_A_unique on second_table
( encryptedA ) ;
    update DBA.second_table
        set encryptedA = aes_encrypt(sensitiveA, 'seCr3t')
        where encryptedA is null ;
    commit
    alter table DBA.second_table drop sensitiveA ;

--   The following types of queries are permitted at this point,
before
--   changes are made for key protection:

--   Non-TRUSTED users can equi-join on ciphertext; they can also
select
--   the binary, but have no way to interpret it.

    select I.publicC, 3*II.publicQ+1
    from DBA.first_table I, DBA.second_table II
    where I.encryptedA = II.encryptedA and I.publicD IN
( '2006-01-11' ) ;

--   Ciphertext-only access rules out general predicates and
expressions.
--   The following query does not return meaningful results.
--
--   NOTE: These four predicates can be used on the varbinary
containing
--   ciphertext:
--      = (equality)
--      <> (inequality)
```

```
--      IS NULL
--      IS NOT NULL

    select count(*)
    from DBA.first_table I, DBA.second_table II
    where I.encryptedA = II.encryptedA and SUBSTR(I.encryptedA,4,3)
        BETWEEN '345' AND '456' ;

--   The TRUSTED user still has access to the plaintext columns that
--   were retained. Therefore, this user does not need to call
--   aes_decrypt and does not need the key.

    select count(*)
    from DBA.first_table I, DBA.second_table II
    where I.encryptedA = II.encryptedA and SUBSTR(I.sensitiveA,4,3)
        BETWEEN '345' AND '456' ;


--   Part III: Protect the encryption keys

--   This section illustrates how to grant access to the plaintext,
but
--   still protect the keys.

--   For the first table, the DBA elected to retain the plaintext
columns.
--   Therefore, the following view has the same capabilities as the
trusted
--   user above.
--   Assume group_member is being used for additional access control.

--   NOTE: In this example, NonPrivUser still has access to the
ciphertext
--   encrypted in the base table.

    create view DBA.a_first_view (sensitiveA, publicC, publicD)
        as
            select
            IF group_member('high_privileges_group',user_name()) = 1
                 THEN sensitiveA
                 ELSE NULL
              ENDIF,
              publicC,
              publicD
            from first_table ;

    grant select on DBA.a_first_view to PrivUser ;
    grant select on DBA.a_first_view to NonPrivUser ;

--   For the second table, the DBA did not keep the plaintext.
--   Therefore, aes_decrypt calls must be used in the view.
--   IMPORTANT: Hide the view definition with ALTER VIEW, so that no
one
--   can discover the key.

    create view DBA.a_second_view
```

```
(sensitiveA,publicP,publicQ,publicR)
        as
            select
            IF group_member('high_privileges_group',user_name()) = 1
                 THEN aes_decrypt(encryptedA,'seCr3t', char(16))
                 ELSE NULL
              ENDIF,
              publicP,
              publicQ,
              publicR
            from second_table ;

    alter view DBA.a_second_view set hidden ;
    grant select on DBA.a_second_view to PrivUser ;
    grant select on DBA.a_second_view to NonPrivUser ;

--   Likewise, the key used for loading can be protected in a stored
     procedure.
--   By hiding the procedure (just as the view is hidden), no-one can
see
--   the keys.

    create procedure load_first_proc(@inputFileName varchar(255),
                        @colDelim varchar(4) default '$',
                        @rowDelim varchar(4) default '\n')
        begin
            execute immediate with quotes
                'load table DBA.second_table
                (encryptedA encrypted(char(16),' ||
              '''' || 'seCr3t' || '''' || '),publicP,publicQ,publicR)
' ||
                ' from ' || '''' || @inputFileName || '''' ||
                ' delimited by ' || '''' || @colDelim || '''' ||
                ' row delimited by ' || '''' || @rowDelim || '''' ||
                ' quotes off escapes off' ;
        end
    ;

    alter procedure DBA.load_first_proc set hidden ;

--   Call the load procedure using the following syntax:

    call load_first_proc('/dev/null', '$', '\n') ;

--   Below is a comparison of several techniques for protecting the
--   encryption keys by using user-defined functions (UDFs), other
views,
--   or both. The first and the last alternatives offer maximum
performance.

--   The second_table is secured as defined earlier.


--   Alternative 1:
--   This baseline approach relies on restricting access to the
entire view.
```

```
     create view

DBA.second_baseline_view(sensitiveA,publicP,publicQ,publicR)
        as
            select
            IF group_member('high_privileges_group',user_name()) = 1
                 THEN aes_decrypt(encryptedA,'seCr3t', char(16))
                 ELSE NULL
              ENDIF,
              publicP,
              publicQ,
              publicR
            from DBA.second_table ;

     alter view DBA.second_baseline_view set hidden ;
     grant select on DBA.second_baseline_view to NonPrivUser ;
     grant select on DBA.second_baseline_view to PrivUser ;


--   Alternative 2:
--     Place the encryption function invocation within a user-defined
--   function (UDF).
--    Hide the definition of the UDF. Restrict the UDF permissions.
--   Use the UDF in a view that handles the remainder of the security
--     and business logic.
--    Note: The view itself does not need to be hidden.

     create function DBA.second_decrypt_function(IN datum
varbinary(32))
            RETURNS char(16) DETERMINISTIC
            BEGIN
                RETURN aes_decrypt(datum,'seCr3t', char(16));
            END  ;

     grant execute on DBA.second_decrypt_function to PrivUser ;
     alter function DBA.second_decrypt_function set hidden ;

     create view

DBA.second_decrypt_view(sensitiveA,publicP,publicQ,publicR)
        as
                select
               IF group_member('high_privileges_group',user_name())
= 1
                     THEN second_decrypt_function(encryptedA)
                     ELSE NULL
                  ENDIF,
                  publicP,
                 publicQ,
                 publicR
                from DBA.second_table ;

     grant select on DBA.second_decrypt_view to NonPrivUser ;
     grant select on DBA.second_decrypt_view to PrivUser ;
```

```
--  Alternative 3:
--    Sequester only the key selection in a user-defined function.
--    This function could be extended to support selection of any
--  number of keys.
--    This UDF is also hidden and has restricted execute privileges.
--    Note: Any view that uses this UDF therefore does not compromise
-- the key values.

     create function DBA.second_key_function()
             RETURNS varchar(32) DETERMINISTIC
             BEGIN
               return 'seCr3t' ;
             END

     grant execute on DBA.second_key_function to PrivUser ;
     alter function DBA.second_key_function set hidden ;

     create view
DBA.second_key_view(sensitiveA,publicP,publicQ,publicR)
               as
                   select
                     IF
group_member('high_privileges_group',user_name()) = 1
                        THEN
aes_decrypt(encryptedA,second_key_function(),
                        char(16))
                        ELSE NULL
                     ENDIF,
                     publicP,
                     publicQ,
                     publicR
                   from DBA.second_table ;

     grant select on DBA.second_key_view to NonPrivUser ;
     grant select on DBA.second_key_view to PrivUser ;


--  Alternative 4:
--    The recommended alternative is to separate the security logic
--   from the business logic by dividing the concerns into two views.
--    Only the security logic view needs to be hidden.
--   Note: The performance of this approach is similar to that of the
first
-- alternative.

     create view

DBA.second_SecurityLogic_view(sensitiveA,publicP,publicQ,publicR)
           as
               select
              IF group_member('high_privileges_group',user_name())
= 1
                   THEN aes_decrypt(encryptedA,'seCr3t', char(16))
                   ELSE NULL
                ENDIF,
                publicP,
```

```
                  publicQ,
                  publicR
                from DBA.second_table ;

     alter view DBA.second_SecurityLogic_view set hidden ;

     create view

DBA.second_BusinessLogic_view(sensitiveA,publicP,publicQ,publicR)
            as
                select
                  sensitiveA,
                  publicP,
                  publicQ,
                  publicR
                from DBA.second_SecurityLogic_view ;

     grant select on DBA.second_BusinessLogic_view to NonPrivUser ;
     grant select on DBA.second_BusinessLogic_view to PrivUser ;

-- End of encryption example
```

另请参见

- AES_ENCRYPT 函数 [String] （第 173 页）
- AES_DECRYPT 函数 [String] （第 175 页）
- LOAD TABLE ENCRYPTED 子句 （第 176 页）

SAP Sybase IQ 中的 Kerberos 验证支持

SAP Sybase IQ 支持 Kerberos 验证，它是一种登录功能，允许您对数据库连接以及操作系统登录和网络登录维护单一用户 ID 和口令。

使用 Kerberos 证书，无需指定用户 ID 或口令即可连接到数据库。

Kerberos 验证是单独授权的 SAP Sybase IQ 高级安全性选项的组成部分。

Kerberos 的许可要求

高级安全性选项 (IQ_SECURITY) 用于保护您的环境，防止进行未经授权的访问，要将 Kerberos 验证与 SAP Sybase IQ 一起使用，必须提供此选项。

SAP Sybase IQ 中的 LDAP 用户验证支持

您可将 SAP Sybase IQ 集成到所有基于轻型目录访问协议 (LDAP) 这一公认国际标准的现有企业范围的目录访问框架中。

LDAP 用户验证的许可要求

高级安全性选项 (IQ_SECURITY) 用于保护您的环境，防止进行未经授权的访问，而且，要想通过 SAP Sybase IQ 进行 LDAP 用户验证，必须提供此选项。

附录：SQL 参考

本文档中提及的 SQL 语句、数据库选项、函数及系统过程的参考资料。

SQL 语句

Interactive SQL 语句可以自定义并修改数据库。

ALTER LDAP SERVER 语句

对 LDAP 服务器配置对象的所有更改都会应用到后续连接。应用更改时已启动的任何连接都不会立即反映该更改。

快速链接：

转至参数 （第 207 页）

转至示例 （第 208 页）

转至用法 （第 209 页）

转至标准 （第 209 页）

转至权限 （第 209 页）

语法

```
ALTER LDAP SERVER ldapua-server-name
    { ldapua-server-attribs
    | [ WITH ( SUSPEND | ACTIVATE | REFRESH ) ] }

ldapua-server-attribs - (back to Syntax)
    SEARCH DN
        URL { 'URL_string' | NULL }
        | ACCESS ACCOUNT { 'DN_string' | NULL }
        | IDENTIFIED BY ( 'password' | NULL }
        | IDENTIFIED BY ENCRYPTED { encrypted-password | NULL }
    | AUTHENTICATION URL { 'URL_string' | NULL }
    | CONNECTION TIMEOUT timeout_value
    | CONNECTION RETRIES retry_value
    | TLS { ON | OFF }
```

参数

(返回顶部) （第 207 页）

- **URL** – 标识主机（按名称或按 IP 地址）、端口号以及为查寻给定用户 ID 的 DN 而执行的搜索。系统会先校验此值的 LDAP URL 语法是否正确，然后再将其存储在 ISYSLDAPSERVER 系统表中。此字符串的最大大小为 1024 个字节。
- **ACCESS ACCOUNT** – 在 LDAP 服务器上创建的供 SAP Sybase IQ 使用的用户，而不是 SAP Sybase IQ 中的用户。此用户的可分辨名称 (DN) 用于连接到 LDAP 服务器。此用户在 LDAP 服务器中具有一定权限，可按用户 ID 在 SEARCH DN URL 指定的位置搜索 DN。此字符串的最大大小为 1024 个字节。
- **IDENTIFIED BY** – 提供与 ACCESS ACCOUNT 用户关联的口令。该口令使用对称加密的形式存储在磁盘中。使用值 NULL 可清除该口令并将其设置为无。明文口令的最大大小为 255 个字节。
- **IDENTIFIED BY ENCRYPTED** – 以加密格式配置与 ACCESS ACCOUNT 可分辨名称相关联的口令。二进制值是加密口令并按原样存储在磁盘中。使用值 NULL 可清除该口令并将其设置为无。二进制值的最大大小为 289 个字节。加密密钥应该是有效的 varbinary 值。请勿用引号将加密密钥引起来。
- **AUTHENTICATION URL** – 标识主机（按名称或 IP 地址）以及用于验证用户的 LDAP 服务器的端口号。这是为 URL_string 定义的值，系统会先校验此值的 LDAP URL 语法是否正确，然后再将其存储在 ISYSLDAPSERVER 系统表中。通过之前的 DN 搜索获取的用户的 DN 以及用户口令将新连接绑定到验证 URL。与 LDAP 服务器之间的成功连接将被视为连接用户的身份证明。此字符串的最大大小为 1024 个字节。
- **CONNECTION TIMEOUT** – 指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的连接超时。该值以毫秒为单位，缺省值为 10 秒。
- **CONNECTION RETRIES** – 指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
- **TLS** – 定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。该参数设置为 ON 时使用 TLS 协议，URL 以 "ldap://" 开头。设置为 OFF（或未指定）时使用安全 LDAP 协议，URL 以 "ldaps://" 开头。使用 TLS 协议时，通过包含（签署 LDAP 服务器所用证书的）证书颁发机构 (CA) 证书的文件名指定数据库安全选项 TRUSTED_CERTIFICATES_FILE。
- **WITH ACTIVATE** – 创建时激活 LDAP 服务器配置对象以便立即使用。这样便可在一个语句中定义并激活 LDAP 用户验证。使用 WITH ACTIVATE 时，LDAP 服务器配置对象状态会更改为 READY。

示例

（返回顶部） （第 207 页）

- **示例 1** – 暂停名为 apps_primary 的 LDAP 服务器配置对象：

```
ALTER LDAP SERVER apps_primary SUSPEND
```

- **示例 2** – 将名为 apps_primary 的 LDAP 服务器配置对象更改为使用不同的 URL 在主机 fairfax 上进行验证，将端口号设置为 1066，将连接重试次数设置为 10，最后激活 LDAP 服务器配置对象：

```
ALTER LDAP SERVER apps_primary
AUTHENTICATION URL 'ldap://my_LDAPserver:1066/'
CONNECTION RETRIES 10
WITH ACTIVATE
```

用法

(返回顶部) (第 207 页)

除了重置 LDAP 服务器配置对象属性值外，**ALTER LDAP SERVER** 语句还允许管理员将 LDAP 服务器配置对象置于维护模式，然后从维护模式恢复至服务模式，从而对服务器的状态和行为进行手动调整。

标准

(返回顶部) (第 207 页)

ANSI SQL – 遵从性级别：Transact-SQL® 扩充。

权限

(返回顶部) (第 207 页)

需要 MANAGE ANY LDAP SERVER 系统特权。

ALTER LOGIN POLICY 语句

更改现有登录策略或配置逻辑服务器访问。

快速链接：

转至参数 (第 210 页)

转至示例 (第 211 页)

转至用法 (第 211 页)

转至权限 (第 211 页)

语法

语法 1

```
ALTER LOGIN POLICY policy-name
    { { ADD | DROP | SET } LOGICAL SERVER ls-assignment-list
    [ LOGICAL SERVER ls-override-list ])

ls-assignment-list – (back to Syntax 1)
    { { ls-name, ...}
    | ALL
```

```
    | COORDINATOR
    | SERVER
    | NONE
    | DEFAULT }

ls-override-list - (back to Syntax 1)
    { ls-name, ...}

ls-name - (back to ls-assignment-list) or (back to ls-override-list)
    { OPEN | user-defined-ls-name }
```

语法 2

```
ALTER LOGIN POLICY policy-name policy-option

policy-option - (back to Syntax 2)
    policy-option-name = policy-option-value

policy-option-name - (back to policy-option)
   AUTO_UNLOCK_TIME
    | CHANGE_PASSWORD_DUAL_CONTROL
    | DEFAULT_LOGICAL_SERVER
    | LOCKED
    | MAX_CONNECTIONS
    | MAX_DAYS_SINCE_LOGIN
    | MAX_FAILED_LOGIN_ATTEMPTS
    | MAX_NON_DBA_CONNECTIONS
    | PASSWORD_EXPIRY_ON_NEXT_LOGIN
    | PASSWORD_GRACE_TIME
    | PASSWORD_LIFE_TIME
    | ROOT_AUTO_UNLOCK_TIME
    | LDAP_PRIMARY_SERVER
    | LDAP_SECONDARY_SERVER
    | LDAP_AUTO_FAILBACK_PERIOD
    | LDAP_FAILOVER_TO_STD
    | LDAP_REFRESH_DN

policy-option-value - (back to policy-option)
    { UNLIMITED | DEFAULT | value }
```

参数

（返回顶部） （第 209 页）

- **policy-name** – 登录策略的名称。指定修改根登录策略的根。
- **policy-option-name** – 策略选项的名称。有关每个选项的详细信息，请参见“登录策略选项”和“LDAP 登录策略选项”。
- **policy-option-value** – 指派给登录策略选项的值。如果指定为 UNLIMITED，则未使用限制。如果指定为 DEFAULT，则使用缺省的限制。有关每个选项支持的值，请参见“登录策略选项”和“LDAP 登录策略选项”.

应用于

Simplex 和 Multiplex。

示例

(返回顶部) (第 209 页)

- **示例 1** – 请参见“逻辑服务器访问配置”和“Multiplex 登录策略配置”：
- **示例 2** – 在 Test1 登录策略中，将 password_life_time 值设置为 UNLIMITED，并将 max_failed_login_attempts 值设置为 5。

```
ALTER LOGIN POLICY Test1
password_life_time=UNLIMITED
max_failed_login_attempts=5;
```

用法

(返回顶部) (第 209 页)

如果不指定任何策略选项，则将从根登录策略获得此登录策略值。新策略不继承 MAX_NON_DBA_CONNECTIONS 和 ROOT_AUTO_UNLOCK_TIME 策略选项。

所有新数据库都包含根登录策略。可以修改根登录策略的值，但不能删除该策略。

权限

(返回顶部) (第 209 页)

需要 MANAGE ANY LOGIN POLICY 系统特权。

登录策略选项

可用于根登录策略和用户定义登录策略的选项。

选项	描述
AUTO_UNLOCK_TIME	锁定时间段，此时段过后，未被授予 MANAGE ANY USER 系统特权的锁定帐户将自动解锁。此选项可在任意登录策略（包括根登录策略）中定义。 • **值** – 0 – UNLIMITED • **缺省值** – UNLIMITED • **适用于** – 所有未被授予 MANAGE ANY USER 系统特权的用户。
CHANGE_PASSWORD_ DUAL_CONTROL	需要授予了 CHANGE PASSWORD 系统特权的两位用户的输入，以更改其他用户的口令。 • **值** – ON、OFF • **缺省值** – OFF • **适用于** – 所有用户。

选项	描述

DEFAULT_LOGICAL_SERVER	如果连接字符串未指定逻辑服务器，则用户连接到在用户登录策略中指定的 DEFAULT_LOGICAL_SERVER 选项值。
	• **值** –
	  • 现有用户定义逻辑服务器的名称
	  • ALL – 允许访问所有逻辑服务器。
	  • AUTO – 根登录策略中缺省逻辑服务器的值。
	  • COORDINATOR – 当前协调器节点。
	  • NONE – 拒绝访问任何 Multiplex 服务器。
	  • OPEN – 单独使用或与用户定义逻辑服务器的名称一同使用。允许访问所有非用户定义逻辑服务器成员的 Multiplex 节点。
	  • SERVER - 允许访问所有符合 SERVER 逻辑服务器语义的 Multiplex 节点。
	• **缺省值** – AUTO
	• **适用于** – 所有用户。需要 MANAGE MULTIPLEX 系统特权。

LOCKED	如果设置为 ON，用户无法建立新连接。此设置将临时拒绝对登录策略用户的访问。不允许覆盖逻辑服务器的此选项。 • **值** – ON、OFF • **缺省值** – OFF • **适用于** – 所有不具备 MANAGE ANY USER 系统特权的用户。
MAX_CONNECTIONS	用户允许的最大并发连接数。可为此选项指定“每逻辑服务器”设置。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有不具备 SERVER OPERATOR 或 DROP CONNECTION 系统特权的用户。
MAX_DAYS_SINCE_LOGIN	同一用户在两次连续登录之间可以经过的最大天数。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有不具备 MANAGE ANY USER 系统特权的用户。

选项	描述
MAX_FAILED_LOGIN_ATTEMPTS	自上次成功登录以来，在帐户锁定前尝试登录到用户帐户的最多失败次数。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有用户。
MAX_NON_DBA_CONNECTIONS	不具备 SERVER OPERATOR 或 DROP CONNECTION 系统特权的用户可进行的最大并发连接数。只在根登录策略中支持此选项。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有不具备 SERVER OPERATOR 或 DROP CONNECTION 特权的用户。
PASSWORD_EXPIRY_ON_NEXT_LOGIN	如果设为 ON，用户口令将在下次登录时到期。 • **值** – ON、OFF • **缺省值** – OFF • **适用于** – 所有用户。 **注意：** 登录到 SAP Control Center 时当前未实现此功能。系统不会提示用户更改其口令。但在登录到 SAP Control Center 之外的 SAP Sybase IQ 时（例如，使用 Interactive SQL），则提示用户更改口令。
PASSWORD_GRACE_TIME	口令到期前剩余的天数，在此期间允许登录，但缺省 post_login 过程会发出警告。 • **值** – 0 – 2147483647 • **缺省值** – 0 • **适用于** – 所有用户。
PASSWORD_LIFE_TIME	口令存在的最多天数，此时段后必须更改该口令。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有用户。

选项	描述
ROOT_AUTO_UNLOCK_TIME	锁定时间段，此时段过后，被授予 MANAGE ANY USER 系统特权的锁定帐户将自动解锁。只能在根登录策略中定义此选项。 • **值** – 0 – UNLIMITED • **缺省值** – 15 • **适用于** – 所有被授予 MANAGE ANY USER 系统特权的用户。

LDAP 登录策略选项

LDAP 用户验证的可用登录策略选项

选项	说明
LDAP_PRIMARY_SERVER	指定主 LDAP 服务器的名称。 • **值** – N/A • **缺省值** – 无 • **适用于** – 所有用户。
LDAP_SECONDARY_SERVER	指定次级 LDAP 服务器的名称。 • **值** – N/A • **缺省值** – 无 • **适用于** – 所有用户。
LDAP_AUTO_FAILBACK_PERIOD	指定尝试自动故障回复到主服务器后的时间段（以分钟为单位）。 • **值** – 0 - 2147483647 • **缺省值** – 15 分钟 • **适用于** – 所有用户。
LDAP_FAILOVER_TO_STD	由于系统资源、网络中断、连接超时或类似系统故障而导致 LDAP 服务器验证失败时，允许使用标准验证进行验证。但是，不允许从 LDAP 服务器返回的实际验证失败故障转移到标准验证。 • **值** – ON、OFF • **缺省值** – ON • **适用于** – 所有用户。

选项	说明
LDAP_REFRESH_DN	将 ISYSLOGINPOLICYOPTION 系统表中的 ldap_refresh_dn 值（该值以协调通用时间 (UTC) 形式存储）更新为当前时间。 每次用户使用 LDAP 进行验证时，如果 ISYSLOGINPOLICYOPTION 中的 ldap_refresh_dn 值比 ISYSUSER 中的 user_dn 值更新，则会搜索新用户 DN。然后使用新用户 DN 更新 user_dn 的值，并再次将 user_dn_changed_at 的值更新为当前时间。 • **值** – NOW • **ROOT 策略的初始值** – NULL • **用户定义登录策略的初始值** – 以 UTC 格式存储的当前时间 • **适用于** – 所有用户。

Multiplex 登录策略配置

配置 Multiplex 服务器的登录策略。

示例

本示例将替换某个逻辑服务器的登录策略设置，从而增加逻辑服务器 ls1 上的最大连接数：

```
ALTER LOGIN POLICY lp1 max_connections=20 LOGICAL SERVER ls1;
```

用法

仅适用于 Multiplex。

对任何 Multiplex 服务器执行的任何登录管理命令都会自动传播到 Multiplex 中的所有服务器。为获得最佳性能，请对协调器执行这些命令或任何 DDL。

逻辑服务器级别替换的替换意味着不同的逻辑服务器有不同的特定登录策略选项设置。SYS.ISYSIQLSLOGINPOLICYOPTION 用于存储逻辑服务器替换的登录策略选项值。对于某个登录策略选项的每个逻辑服务器替换，在 ISYSIQLSLOGINPOLICYOPTION 中都存在对应的一行。

逻辑服务器访问配置

配置逻辑服务器访问。

示例 1

假设根登录策略允许访问逻辑服务器 ls4 和 ls5，且登录策略 lp1 存在，但未分配给任何逻辑服务器。以下语句可将登录策略 lp1 有效分配至逻辑服务器 ls4 和 ls5。

将逻辑服务器 ls1 分配给登录策略 lp1：

```
ALTER LOGIN POLICY lp1 ADD LOGICAL SERVER ls1
```

示例 2

该语句允许从登录策略 lp1 访问逻辑服务器 ls2 和 ls3：

```
ALTER LOGIN POLICY lp1 ADD LOGICAL SERVER ls2, ls3
```

示例 3

将登录策略 lp1 修改为仅允许访问 ls3 和 ls4：

```
ALTER LOGIN POLICY lp1 ADD LOGICAL SERVER ls4

ALTER LOGIN POLICY lp1 DROP LOGICAL SERVER ls1, ls2
```

或者：

```
ALTER LOGIN POLICY lp1 SET LOGICAL SERVER ls3, ls4
```

示例 4

将登录策略 lp1 修改为拒绝访问任何逻辑服务器：

```
ALTER LOGIN POLICY lp1 SET LOGICAL SERVER NONE
```

示例 5

删除登录策略 lp1 的当前逻辑服务器分配，并允许其继承根登录策略的逻辑服务器分配：

```
ALTER LOGIN POLICY lp1 SET LOGICAL SERVER DEFAULT
```

用法
ADD、DROP 或 SET 子句可用于配置登录策略的逻辑服务器分配：

- **ADD** – 将新逻辑服务器分配添加到登录策略中。
- **DROP** – 从登录策略删除现有逻辑服务器分配。
- **SET** – 将登录策略的所有逻辑服务器分配替换为一组新逻辑服务器。

只能使用一个 ADD、DROP 或 SET 子句。只能将 SERVER、NONE 和 DEFAULT 子句与 SET 子句一起使用。对于每个 ls-assignment 列表或 ls-override 列表，只能指定一次特定逻辑服务器名称。

出现以下情况时会返回错误：

- 通过 ADD 子句指定的逻辑服务器已分配到登录策略。
- 通过 DROP 子句指定的逻辑服务器当前未分配到登录策略。
- 逻辑服务器分配的更改可能导致已分配逻辑服务器间成员资格重叠。

SYS.ISYSIQLOGINPOLICYLSINFO 用于存储逻辑服务器分配信息。对于某个登录策略选项的每个逻辑服务器替换，在 ISYSIQLOGINPOLICYLSINFO 中都存在对应的一行。

ALTER ROLE 语句

将兼容性角色迁移到用户定义的系统角色，然后自动删除兼容性角色。

注意： 您不能使用 ALTER ROLE 语句迁移 SYS_AUTH_SA_ROLE 或 SYS_AUTH_SSO_ROLE。迁移 SYS_AUTH_DBA_ROLE 时，会自动迁移这两个角色。

快速链接：

转至参数 （第 217 页）

转至示例 （第 217 页）

转至用法 （第 218 页）

转至标准 （第 218 页）

转至权限 （第 218 页）

语法

语法 1 - 迁移 SYS_AUTH_DBA_ROLE

```
ALTER ROLE predefined_sys_role_name
    MIGRATE TO new_role_name [, new_sa_role_name, new_sso_role_name]
```

语法 2 – 迁移所有其他兼容性角色

```
ALTER ROLE predefined_sys_role_name
    MIGRATE TO new_role_name
```

参数

(返回顶部) （第 217 页）

- **predefined_sys_role_name** – 仍存在于数据库中（尚未被删除）的兼容性角色的名称。
- **new_role_name** – 新角色的名称，不能以 SYS_ 作为前缀，也不能以 _ROLE 作为后缀。
- **new_sa_role_name** – 仅在迁移 SYS_AUTH_DBA_ROLE 时需要此参数。要向其迁移 SYS_AUTH_SA_ROLE 的基础系统特权的新角色不能是数据库中已存在的角色，新角色名称也不能以前缀 SYS_ 开头或以后缀 _ROLE 结尾。
- **new_sso_role_name** – 仅在迁移 SYS_AUTH_DBA_ROLE 时需要此参数。要向其迁移 SYS_AUTH_SSO_ROLE 的基础系统特权的新角色不能是数据库中已存在的角色，新角色名称也不能以前缀 SYS_ 开头或以后缀 _ROLE 结尾。

示例

(返回顶部) （第 217 页）

- **示例 1** – 将 SYS_AUTH_DBA_ROLE 分别迁移到新角色 Custom_DBA、Custom_SA 和 Custom_SSO。然后将授予 SYS_AUTH_DBA_ROLE 的所有用户、基础系统特权和角色自动迁移到适用的新角色。最后，删除 SYS_AUTH_DBA_ROLE、SYS_AUTH_SA_ROLE 和 SYS_AUTH_SSO_ROLE。

```
ALTER ROLE SYS_AUTH_DBA_ROLE
MIGRATE TO Custom_DBA, Custom_SA, Custom_SSO
```

- **示例 2** – 将 SYS_AUTH_OPERATOR_ROLE 角色迁移到新角色 Operator_role。然后将授予 SYS_AUTH_OPERATOR_ROLE 的所有用户、基础系统特权和角色自动迁移到新角色并删除 SYS_AUTH_OPERATOR_ROLE。

```
ALTER ROLE SYS_AUTH_OPERATOR_ROLE
MIGRATE TO Operator_role
```

用法

(返回顶部) (第 217 页)

迁移过程中：

- 创建一个新的用户定义角色。
- 当前已授予要迁移的预定义角色的所有系统特权均自动授予该新的用户定义角色。
- 当前已授予要迁移的预定义角色的所有用户和角色均自动授予该新的用户定义角色。
- 删除兼容性角色。

由于在迁移过程中未指定角色管理员，因此只有全局角色管理员能够管理新角色。请使用 CREATE ROLE 语句为该角色添加具有适当管理权限的角色管理员。

标准

(返回顶部) (第 217 页)

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) (第 217 页)

需要具备所授予的 MANAGE ROLES 系统特权以及管理权限。

ALTER USER 语句

更改用户设置。

快速链接：

转至参数 (第 219 页)

转至示例 (第 220 页)

转至用法 (第 220 页)

转至标准 （第 221 页）

转至权限 （第 221 页）

语法

语法 1 - 更改数据库用户的定义

```
ALTER USER user-name
    | [ IDENTIFIED BY password ]
    | [ LOGIN POLICY policy-name ]
    | [ FORCE PASSWORD CHANGE { ON | OFF } ]
```

语法 2 - 为 LDAP 用户刷新可分辨名称 (DN)

```
ALTER USER user-name
    REFRESH DN
```

语法 3 - 将用户的登录策略恢复为原始值

```
ALTER USER user-name
    RESET LOGIN POLICY
```

语法 4 - 启用用户登录策略中的 CHANGE_PASSWORD_DUAL_CONTROL 时更改用户口令。

```
ALTER USER user-name
    IDENTIFIED [ FIRST | LAST ] BY password_part
```

参数

(返回顶部) （第 218 页）

- **user-name** – 用户的名称。
- **IDENTIFIED BY** – 用户的口令。如果在用户登录策略中启用了 CHANGE_PASSWORD_DUAL_CONTROL 选项，不支持子句 (ERROR)。
- **IDENTIFIED[FIRST | LAST] BY** – 如果在目标用户的登录策略中启用了 CHANGE_PASSWORD_DUAL_CONTROL 选项，强制使用子句。FIRST | LAST 关键字指定要定义的双重口令部分。
- **policy-name** – 指派给用户的登录策略的名称。如果未指定登录策略，则不进行任何更改。如果不指定 LOGIN POLICY 子句则不进行任何更改。
- **FORCE PASSWORD CHANGE** – 控制用户登录时是否必须指定新口令。此设置将覆盖用户登录策略中的 PASSWORD_EXPIRY_ON_NEXT_LOGIN 选项设置。

  注意： 登录到 SAP Control Center 时当前未实现此功能。系统不会提示用户更改其口令。但在登录到 SAP Control Center 之外的 SAP Sybase IQ 时（例如，使用 Interactive SQL），则提示用户更改口令。

- **RESET LOGIN POLICY** – 将用户登录设置恢复为登录策略中的原始值。这通常会清除因用户超出失败登录次数或超出自上次登录后的最大天数而隐式设置的所有锁。重置登录策略后，用户就可以访问由于超出登录策略选项的限制（如

MAX_FAILED_LOGIN_ATTEMPTS 或 MAX_DAYS_SINCE_LOGIN）而被锁定的帐户。

- **REFRESH DN** – 清除为用户保存的、在 LDAP 验证期间使用的 DN 和时间戳。

示例

(返回顶部) (第 218 页)

- **示例 1** – 更改名为 SQLTester 的用户。口令设置为 welcome。为 SQLTester 用户指派了 Test1 登录策略，而且下次登录时口令不到期：

```
ALTER USER SQLTester
IDENTIFIED BY welcome
LOGIN POLICY Test1
FORCE PASSWORD CHANGE OFF
```

- **示例 2** – 清除用户 Mary 的用于 LDAP 验证的可分辨名称 (DN) 和时间戳：

```
ALTER USER Mary REFRESH DN
```

- **示例 3** – 将 user3 的口令设置为 PassPart1PassPart2。其中假定 user1 和 user2 具有 CHANGE PASSWORD 系统特权，并且在 user3 的登录策略中启用了 change_password_dual_control 选项 (ON)：

  User1 输入：

```
ALTER USER user3 IDENTIFIED FIRST BY PassPart1
```

  User2 输入：

```
ALTER USER user3 IDENTIFIED LAST BY PassPart2
```

  为 user3 设置口令后，user3 通过输入口令 PassPart1PassPart2 登录。

用法

(返回顶部) (第 218 页)

用户 ID 和口令不能出现以下情况：

- 以空格、单引号或双引号开头
- 以空格结尾
- 含有分号

口令不能超过 255 个字符。

如果将 PASSWORD_EXPIRY_ON_NEXT_LOGIN 值设置为 ON，则指派有此登录策略的所有用户的口令将在其下次登录时立即到期。您可使用 **ALTER USER** 和 **LOGIN POLICY** 子句强制用户在下次登录时更改其口令。

如果在双重口令更改进程中禁用了 CHANGE_PASSWORD_DUAL CONTROL 登录策略选项 (OFF)：

- 目标用户将无法使用已定义的单一口令部分进行登录。必须使用单一口令控制语法重新发出 **ALTER USER** 命令。
- 如果在双重口令更改进程完成之后、目标用户登录之前禁用该选项，则不会对目标用户造成任何影响。目标用户必须使用两个口令部分进行登录。

如果在进行双重口令更改进程时目标用户已登录，则该用户无法在当前会话中更改其口令，一直到新口令的两个部分均设置完毕。双重口令更改进程完成后，目标用户不必先注销即可对口令使用 **GRANT CONNECT**、**ALTER USER**、**sp_password** 或 **sp_iqpassword**。系统随即提示输入当前口令，请使用新的双重控制口令，而非最初为当前会话输入的口令。

在双重口令更改进程中，不支持使用 **GRANT CONNECT** 语句设置任何口令部分。但在双重口令更改进程完成后，目标用户不必先注销即可使用 **GRANT CONNECT** 语句、**ALTER USER**、**sp_password** 或 **sp_iqpassword** 更改其口令。

用户通过 CHANGE PASSWORD 系统特权成功指定口令的两个部分之后，目标用户的口令将自动过期。这将强制目标用户在其下次登录时更改口令。

用于散列用户口令的加密算法是经 FIPS 认证的加密支持：

- 此 DLL 称为 **dbfips10.dll**
- HASH 函数接受以下算法： **SHA1_FIPS SHA256_FIPS**
- 如果指定了 **-fips** 服务器选项并为 HASH 函数提供了非 FIPS 认证算法，则数据库服务器将使用 **SHA1_FIPS** 而不用 **SHA1**，使用 **SHA256_FIPS** 而不用 **SHA256**，并在使用了 **MD5**（**MD5** 不是 FIPS 认证算法）的情况下返回错误。
- 如果指定了 **-fips** 选项，则数据库服务器将使用 SHA256_FIPS 进行口令散列处理。

标准

（返回顶部） （第 218 页）

- SQL - ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - 不受 Adaptive Server 支持。

权限

（返回顶部） （第 218 页）

- 更改自己的口令 – 无需任何权限。
- 更改任意用户的口令 – 需要具有 CHANGE PASSWORD 系统特权。
- 使用 **LOGIN POLICY**、**FORCE PASSWORD CHANGE**、**RESET LOGIN POLICY** 或 **REFRESH DN** 子句需要具有 MANAGE ANY USER 系统特权。

CREATE LDAP SERVER 语句

针对 LDAP 用户验证新建 LDAP 服务器配置对象。创建 LDAP 服务器配置对象期间定义的参数存储在 `ISYSLDAPSERVER`（系统视图 `SYSLDAPSERVER`）系统表中。

快速链接：

转至参数 （第 222 页）

转至示例 （第 223 页）

转至标准 （第 224 页）

转至权限 （第 224 页）

语法

```
CREATE LDAP SERVER ldapua-server-name
    [ ldapua-server-attribs ]
    [ WITH ACTIVATE ]

ldapua-server-attribs
    SEARCH DN
        URL { 'URL_string' | NULL }
        | ACCESS ACCOUNT { 'DN_string' | NULL }
        | IDENTIFIED BY ( 'password' | NULL }
        | IDENTIFIED BY ENCRYPTED { encrypted-password | NULL }
    | AUTHENTICATION URL { 'URL_string' | NULL }
    | CONNECTION TIMEOUT timeout_value
    | CONNECTION RETRIES retry_value
    | TLS { ON | OFF }
```

参数

(返回顶部) （第 221 页）

- **URL** – 标识主机（按名称或按 IP 地址）、端口号以及为查寻给定用户 ID 的 DN 而执行的搜索。系统会先校验此值的 LDAP URL 语法是否正确，然后再将其存储在 ISYSLDAPSERVER 系统表中。此字符串的最大大小为 1024 个字节。
- **ACCESS ACCOUNT** – 在 LDAP 服务器上创建的供 SAP Sybase IQ 使用的用户，而不是 SAP Sybase IQ 中的用户。此用户的可分辨名称 (DN) 用于连接到 LDAP 服务器。此用户在 LDAP 服务器中具有一定权限，可按用户 ID 在 SEARCH DN URL 指定的位置搜索 DN。此字符串的最大大小为 1024 个字节。
- **IDENTIFIED BY** – 提供与 ACCESS ACCOUNT 用户关联的口令。该口令使用对称加密的形式存储在磁盘中。使用值 NULL 可清除该口令并将其设置为无。明文口令的最大大小为 255 个字节。
- **IDENTIFIED BY ENCRYPTED** – 以加密格式配置与 ACCESS ACCOUNT 可分辨名称相关联的口令。二进制值是加密口令并按原样存储在磁盘中。使用值 NULL 可清除该口令并将其设置为无。二进制值的最大大小为 289 个字节。加密密钥应该是有效的 varbinary 值。请勿用引号将加密密钥引起来。
- **AUTHENTICATION URL** – 标识主机（按名称或 IP 地址）以及用于验证用户的 LDAP 服务器的端口号。这是为 URL_string 定义的值，系统会先校验此值的 LDAP URL 语法是否正确，然后再将其存储在 ISYSLDAPSERVER 系统表中。通过之前的 DN 搜索获取的用户的 DN 以及用户口令将新连接绑定到验证 URL。与 LDAP 服

务器之间的成功连接将被视为连接用户的身份证明。此字符串的最大大小为 1024 个字节。

- **CONNECTION TIMEOUT** – 指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的连接超时。该值以毫秒为单位，缺省值为 10 秒。
- **CONNECTION RETRIES** – 指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
- **TLS** – 定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。该参数设置为 ON 时使用 TLS 协议，URL 以 "ldap://" 开头。设置为 OFF（或未指定）时使用安全 LDAP 协议，URL 以 "ldaps://" 开头。使用 TLS 协议时，通过包含（签署 LDAP 服务器所用证书的）证书颁发机构 (CA) 证书的文件名指定数据库安全选项 TRUSTED_CERTIFICATES_FILE。
- **WITH ACTIVATE** – 创建时激活 LDAP 服务器配置对象以便立即使用。这样便可在一个语句中定义并激活 LDAP 用户验证。使用 WITH ACTIVATE 时，LDAP 服务器配置对象状态会更改为 READY。

示例

(返回顶部) (第 221 页)

- **示例 1** – 设置搜索参数、验证 URL、3 秒超时，并激活服务器，使其能够开始验证用户。连接 LDAP 服务器时不使用 TLS 或 SECURE LDAP 协议。

```
SET OPTION PUBLIC.login_mode = 'Standard,LDAPUA'
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

- **示例 2** – 使用与示例 1 相同的搜索参数，但指定的是 "ldaps"，因此，在主机 my_LDAPserver 的端口 636 上与 LDAP 服务器建立安全 LDAP 连接。现在，只有使用安全 LDAP 协议的 LDAP 客户端才能连接到此端口。数据库安全选项 TRUSTED_CERTIFICATE_FILE 必须使用包含（签署 "ldaps://my_LDAPserver:636" 上的 LDAP 服务器所用证书的）证书颁发机构 (CA) 证书的文件名进行设置。在与 LDAP 服务器握手期间，LDAP 服务器所提供的证书将由 SAP Sybase IQ 服务器（LDAP 客户端）进行检查，以确保其由该文件中所列的其中一个证书进行签署。客户端通过证书与服务器建立信任，从而确认服务器自行声明的身份。LDAP 服务器可以通过 ACCESS ACCOUNT 和 IDENTIFIED BY 参数与客户端建立信任，从而确认客户端自行声明的身份。

注意： 使用安全 LDAP 而非 TLS 协议时，TLS 参数必须设为 OFF。

```
SET OPTION PUBLIC.login_mode = 'Standard,LDAPUA'
SET OPTION PUBLIC.trusted_certificates_file = '/mycompany/shared/
```

```
trusted.txt'
CREATE LDAP SERVER secure_primary
SEARCH DN
    URL  'ldaps://my_LDPAserver:636/dc=MyCompany,dc=com??sub?
cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldaps://my_LDAPserver:636/'
CONNECTION TIMEOUT 3000
TLS OFF
WITH ACTIVATE
```

- **示例 3** – 在端口 389 上建立 TLS 协议连接。这也要求数据库安全选项 TRUSTED_CERTIFICATE_FILE 使用文件名进行设置并提供与示例 2 相同的安全类型。在本示例中，TLS 协议设为 ON，有助于 LDAP 服务器供应商提供更广泛的支持。

注意: 确定如何配置 SAP Sybase IQ 服务器的安全 LDAP 或 TLS 时检查所有 LDAP 服务器的要求。

```
SET OPTION PUBLIC.login_mode = 'Standard,LDAPUA'
SET OPTION PUBLIC.trusted_certificates_file = '/mycompany/shared/
trusted.txt'
CREATE LDAP SERVER tls_primary
SEARCH DN
   URL  'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
TLS ON
WITH ACTIVATE
```

标准

(返回顶部) （第 221 页）

ANSI SQL – 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 221 页）

需要 MANAGE ANY LDAP SERVER 系统特权。

CREATE LOGIN POLICY 语句

在数据库中创建登录策略。

快速链接:

转至参数 （第 225 页）

转至示例 （第 225 页）

转至用法 （第 226 页）

转至权限 （第 226 页）

语法

```
CREATE LOGIN POLICY policy-name policy-option

policy-option – (back to Syntax)
    policy-option-name = policy-option-value

policy-option-name – (back to policy-option)
   AUTO_UNLOCK_TIME
     | CHANGE_PASSWORD_DUAL_CONTROL
     | DEFAULT_LOGICAL_SERVER
     | LOCKED
     | MAX_CONNECTIONS
     | MAX_DAYS_SINCE_LOGIN
     | MAX_FAILED_LOGIN_ATTEMPTS
     | MAX_NON_DBA_CONNECTIONS
     | PASSWORD_EXPIRY_ON_NEXT_LOGIN
     | PASSWORD_GRACE_TIME
     | PASSWORD_LIFE_TIME
     | ROOT_AUTO_UNLOCK_TIME
     | LDAP_PRIMARY_SERVER
     | LDAP_SECONDARY_SERVER
     | LDAP_AUTO_FAILBACK_PERIOD
     | LDAP_FAILOVER_TO_STD
     | LDAP_REFRESH_DN

policy-option-value – (back to policy-option)
    { UNLIMITED | DEFAULT | value }
```

参数

(返回顶部) （第 224 页）

- **policy-name** – 登录策略的名称。指定修改根登录策略的根。
- **policy-option-name** – 策略选项的名称。有关每个选项的详细信息，请参见“登录策略选项”和“LDAP 登录策略选项”。
- **policy-option-value** – 指派给登录策略选项的值。如果指定为 UNLIMITED，则未使用限制。如果指定为 DEFAULT，则使用缺省的限制。有关每个选项支持的值，请参见“登录策略选项”和“LDAP 登录策略选项”.

应用于

Simplex 和 Multiplex。

示例

(返回顶部) （第 224 页）

- **示例 1** – 创建 Test1 登录策略。此登录策略规定口令没有有效期限制，输入口令时允许用户最多尝试五次，之后便会锁定帐户。

```
CREATE LOGIN POLICY Test1
password_life_time=UNLIMITED
max_failed_login_attempts=5;
```

用法

(返回顶部) （第 224 页）

如果不指定任何策略选项，则将从根登录策略获得此登录策略值。新策略不继承 MAX_NON_DBA_CONNECTIONS 和 ROOT_AUTO_UNLOCK_TIME 策略选项。

权限

(返回顶部) （第 224 页）

需要 MANAGE ANY LOGIN POLICY 系统特权。

下列系统特权可替换所述登录策略选项：

例外系统特权	登录策略选项
SERVER OPERATOR 或 DROP CONNECTION 系统特权	MAX_NON_DBA_CONNS MAX_CONNECTIONS
MANAGE ANY USER 系统特权	LOCKED MAX_DAYS_SINCE_LOGIN

登录策略选项

可用于根登录策略和用户定义登录策略的选项。

选项	描述
AUTO_UNLOCK_TIME	锁定时间段，此时段过后，未被授予 MANAGE ANY USER 系统特权的锁定帐户将自动解锁。此选项可在任意登录策略（包括根登录策略）中定义。 • **值** – 0 – UNLIMITED • **缺省值** – UNLIMITED • **适用于** – 所有未被授予 MANAGE ANY USER 系统特权的用户。

选项	描述
CHANGE_PASSWORD_DUAL_CONTROL	需要授予了 CHANGE PASSWORD 系统特权的两位用户的输入，以更改其他用户的口令。 • **值** – ON、OFF • **缺省值** – OFF • **适用于** – 所有用户。

DEFAULT_LOGICAL_SERVER	如果连接字符串未指定逻辑服务器，则用户连接到在用户登录策略中指定的 DEFAULT_LOGICAL_SERVER 选项值。
	• **值** –
	  • 现有用户定义逻辑服务器的名称
	  • ALL – 允许访问所有逻辑服务器。
	  • AUTO – 根登录策略中缺省逻辑服务器的值。
	  • COORDINATOR – 当前协调器节点。
	  • NONE – 拒绝访问任何 Multiplex 服务器。
	  • OPEN – 单独使用或与用户定义逻辑服务器的名称一同使用。允许访问所有非用户定义逻辑服务器成员的 Multiplex 节点。
	  • SERVER - 允许访问所有符合 SERVER 逻辑服务器语义的 Multiplex 节点。
	• **缺省值** – AUTO
	• **适用于** – 所有用户。需要 MANAGE MULTIPLEX 系统特权。

LOCKED	如果设置为 ON，用户无法建立新连接。此设置将临时拒绝对登录策略用户的访问。不允许覆盖逻辑服务器的此选项。 • **值** – ON、OFF • **缺省值** – OFF • **适用于** – 所有不具备 MANAGE ANY USER 系统特权的用户。
MAX_CONNECTIONS	用户允许的最大并发连接数。可为此选项指定“每逻辑服务器”设置。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有不具备 SERVER OPERATOR 或 DROP CONNECTION 系统特权的用户。

选项	描述
MAX_DAYS_SINCE_LOGIN	同一用户在两次连续登录之间可以经过的最大天数。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有不具备 MANAGE ANY USER 系统特权的用户。
MAX_FAILED_LOGIN_ATTEMPTS	自上次成功登录以来，在帐户锁定前尝试登录到用户帐户的最多失败次数。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有用户。
MAX_NON_DBA_CONNECTIONS	不具备 SERVER OPERATOR 或 DROP CONNECTION 系统特权的用户可进行的最大并发连接数。只在根登录策略中支持此选项。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有不具备 SERVER OPERATOR 或 DROP CONNECTION 特权的用户。
PASSWORD_EXPIRY_ON_NEXT_LOGIN	如果设为 ON，用户口令将在下次登录时到期。 • **值** – ON、OFF • **缺省值** – OFF • **适用于** – 所有用户。 **注意：** 登录到 SAP Control Center 时当前未实现此功能。系统不会提示用户更改其口令。但在登录到 SAP Control Center 之外的 SAP Sybase IQ 时（例如，使用 Interactive SQL），则提示用户更改口令。
PASSWORD_GRACE_TIME	口令到期前剩余的天数，在此期间允许登录，但缺省 post_login 过程会发出警告。 • **值** – 0 – 2147483647 • **缺省值** – 0 • **适用于** – 所有用户。

选项	描述
PASSWORD_LIFE_TIME	口令存在的最多天数，此时段后必须更改该口令。 • **值** – 0 – 2147483647 • **缺省值** – UNLIMITED • **适用于** – 所有用户。
ROOT_AUTO_UNLOCK_TIME	锁定时间段，此时段过后，被授予 MANAGE ANY USER 系统特权的锁定帐户将自动解锁。只能在根登录策略中定义此选项。 • **值** – 0 – UNLIMITED • **缺省值** – 15 • **适用于** – 所有被授予 MANAGE ANY USER 系统特权的用户。

LDAP 登录策略选项

LDAP 用户验证的可用登录策略选项

选项	说明
LDAP_PRIMARY_SERVER	指定主 LDAP 服务器的名称。 • **值** – N/A • **缺省值** – 无 • **适用于** – 所有用户。
LDAP_SECONDARY_SERVER	指定次级 LDAP 服务器的名称。 • **值** – N/A • **缺省值** – 无 • **适用于** – 所有用户。
LDAP_AUTO_FAILBACK_PERIOD	指定尝试自动故障回复到主服务器后的时间段（以分钟为单位）。 • **值** – 0 - 2147483647 • **缺省值** – 15 分钟 • **适用于** – 所有用户。

选项	说明
LDAP_FAILOVER_TO_STD	由于系统资源、网络中断、连接超时或类似系统故障而导致 LDAP 服务器验证失败时，允许使用标准验证进行验证。但是，不允许从 LDAP 服务器返回的实际验证失败故障转移到标准验证。 • **值** – ON、OFF • **缺省值** – ON • **适用于** – 所有用户。
LDAP_REFRESH_DN	将 ISYSLOGINPOLICYOPTION 系统表中的 ldap_refresh_dn 值（该值以协调通用时间 (UTC) 形式存储）更新为当前时间。 每次用户使用 LDAP 进行验证时，如果 ISYSLOGINPOLICYOPTION 中的 ldap_refresh_dn 值比 ISYSUSER 中的 user_dn 值更新，则会搜索新用户 DN。然后使用新用户 DN 更新 user_dn 的值，并再次将 user_dn_changed_at 的值更新为当前时间。 • **值** – NOW • **ROOT 策略的初始值** – NULL • **用户定义登录策略的初始值** – 以 UTC 格式存储的当前时间 • **适用于** – 所有用户。

Multiplex 登录策略配置

配置 Multiplex 服务器的登录策略。

示例

本示例将替换某个逻辑服务器的登录策略设置，从而增加逻辑服务器 ls1 上的最大连接数：

```
ALTER LOGIN POLICY lp1 max_connections=20 LOGICAL SERVER ls1;
```

用法

仅适用于 Multiplex。

对任何 Multiplex 服务器执行的任何登录管理命令都会自动传播到 Multiplex 中的所有服务器。为获得最佳性能，请对协调器执行这些命令或任何 DDL。

逻辑服务器级别替换的替换意味着不同的逻辑服务器有不同的特定登录策略选项设置。SYS.ISYSIQLSLOGINPOLICYOPTION 用于存储逻辑服务器替换的登录策略选项值。对于某个登录策略选项的每个逻辑服务器替换，在 ISYSIQLSLOGINPOLICYOPTION 中都存在对应的一行。

CREATE ROLE 语句

新建角色、将现有用户扩展为角色，或者管理角色对应的角色管理员。

快速链接：

转至参数 （第 231 页）

转至示例 （第 232 页）

转至用法 （第 232 页）

转至标准 （第 233 页）

转至权限 （第 233 页）

语法

```
CREATE [ OR REPLACE ] ROLE { role_name | FOR USER userID }
   [ WITH ADMIN [ ONLY ] admin_name [...,], [ SYS_MANAGE_ROLES_ROLE ]
```

参数

(返回顶部) （第 231 页）

- **role_name** – 除非使用 OR REPLACE 子句，否则 *role_name* 不能已存在于数据库中。
- **OR REPLACE** – *role_name* 必须已存在于数据库中。如果 *role_name* 尚不存在，将创建一个新的用户定义角色。当前所有管理员将由 *admin_name [..]* 子句中指定的管理员所替换，具体如下所述：
  - 所有被授予 WITH ADMIN OPTION 而未包含在新角色管理员列表中的现有角色管理员将成为没有角色管理权限的角色的成员。
  - 所有被授予 WITH ADMIN ONLY OPTION 而未包含在新角色管理员列表中的现有角色管理员将作为角色的成员被移除。

  使用 OR REPLACE 子句时，如果新角色管理员列表中包含的某个现有角色管理员的原始管理权限高于替换权限，则保留其原始管理权限。例如，用户 A 是一个现有角色管理员，最初被授予对角色的 WITH ADMIN 权限。新角色管理员被授予 WITH ADMIN ONLY 权限。如果该列表中包含用户 A，则用户 A 将保留较高的 WITH ADMIN 权限。
- **FOR USER** – 使用 FOR USER 子句而不使用 OR REPLACE 时，*userID* 必须是当前无法用作角色的现有用户的名称。
- **admin_name** – 要指定为角色管理员的用户的列表。

- **WITH ADMIN** – 除了所有基础系统特权外，指定的每个 *admin_name* 还被授予对角色的管理特权。列表中包含 SYS_MANAGE_ROLES_ROLE 时，WITH ADMIN 子句无效。
- **WITH ADMIN ONLY** – 指定的每个 *admin_name* 仅被授予对角色的管理特权，而不是基础系统特权。
- **SYS_MANAGE_ROLES_ROLE** – 允许全局角色管理员管理角色。可结合 WITH ADMIN ONLY 子句进行指定。

示例

(返回顶部) (第 231 页)

- **示例 1** – 创建角色 `Sales`。只有全局角色管理员可以管理此角色。

```
CREATE ROLE Sales
```

- **示例 2** – 扩展现有用户 `Jane` 以用作角色。

```
CREATE OR REPLACE ROLE FOR USER Jane
```

- **示例 3** – 创建角色 `Finance`，并使 `Mary` 和 `Jeff` 成为具有角色管理权限的角色管理员。全局角色管理员无法管理此角色。

```
CREATE ROLE Finance
WITH ADMIN Mary, Jeff
```

- **示例 3** – 创建角色 `Marketing`，并使 `Mary` 和 `Jeff` 成为角色管理员。全局角色管理员也可以管理此角色。

```
CREATE ROLE Finance
WITH ADMIN ONLY Mary, Jeff, SYS_MANAGE_ROLES_ROLE
```

- **示例 4** – `Finance` 是一个现有角色，`Harry` 和 `Susan` 是具有管理权限的角色管理员。您希望 `Susan` 保留管理员角色，替换 `Harry` 并添加全局角色管理员。新角色管理员将仅具有管理权限。

  此语句保留 `Susan` 的管理员角色，但 `Susan` 保留对角色的管理权限，因为授予的原始管理权限较高。`Harry` 由仅具有管理权限的 `Bob` 和 `Sarah` 替换，系统向该角色添加全局角色管理员。`Harry` 仍是角色成员，但不具有管理权限。

```
CREATE OR REPLACE ROLE Finance
WITH ADMIN ONLY Susan, Bob, Sarah, SYS_MANAGE_ROLE_ROLE
```

用法

(返回顶部) (第 231 页)

如果指定角色管理员 (*admin_name*)，但不包含全局角色管理员 (SYS_MANAGE_ROLES_ROLE)，则全局角色管理员将无法管理新角色。因此，建议您在创建过程中不指定角色管理员。之后使用 OR REPLACE 子句进行添加。

如果未指定 ADMIN 子句，将使用缺省 WITH ADMIN ONLY 子句，且缺省管理员为全局角色管理员 (SYS_MANAGE_ROLES_ROLE)。

替换角色管理员时，如果角色具有全局角色管理员，则必须将全局角色管理员包含在新角色管理员列表中，否则会将其从角色中删除。

但是，使用 WITH ADMIN 子句授予角色管理员时，由于该子句对全局角色管理员无效，您必须使用 **GRANT ROLE** 语句将全局角色管理员 (SYS_MANAGE_RILES_ROLE) 重新添加到角色。执行此授予失败则表示全局角色管理员无法管理该角色。

标准

(返回顶部) (第 231 页)

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) (第 231 页)

- 创建新角色 - 需要 MANAGE ROLES 系统特权。
- OR REPLACE 子句 – 需要 MANAGE ROLES 系统特权，以及对所替换角色的管理权限。

CREATE USER 语句

创建用户。

快速链接:

转至参数 (第 233 页)

转至示例 (第 234 页)

转至用法 (第 234 页)

转至标准 (第 235 页)

转至权限 (第 235 页)

语法

```
CREATE USER  user-name  [ IDENTIFIED BY password ]
[ LOGIN POLICY policy-name ]
[ FORCE PASSWORD CHANGE { ON | OFF } ]
```

参数

(返回顶部) (第 233 页)

- **user-name** – 用户的名称。

- **IDENTIFIED BY** – 用户的口令。
- **policy-name** – 指派给用户的登录策略的名称。如果未指定登录策略，则不进行任何更改。
- **FORCE PASSWORD CHANGE** – 控制用户登录时是否必须指定新口令。此设置将覆盖用户登录策略中的 PASSWORD_EXPIRY_ON_NEXT_LOGIN 选项设置。

  注意： 登录到 SAP Control Center 时当前未实现此功能。系统不会提示用户更改其口令。但在登录到 SAP Control Center 之外的 SAP Sybase IQ 时（例如，使用 Interactive SQL），则提示用户更改口令。

- **password** – 为用户指定口令不是必须的。没有口令的用户不能连接到数据库。如果要创建角色，但不希望任何人使用角色用户 ID 连接到数据库，这将非常有用。用户 ID 必须是有效的标识符。用户 ID 和口令不能出现以下情况：
  - 以空格、单引号或双引号开头
  - 以空格结尾
  - 含有分号

  口令可以是有效的标识符，也可以是以单引号括起来的字符串（最多 255 个字符）。口令区分大小写。口令应由 7 位 ASCII 字符组成，因为如果数据库服务器不能将其从客户端的字符集转换为 UTF-8，则其它字符可能无法正常显示。

  可使用 VERIFY_PASSWORD_FUNCTION 选项来指定函数，以实现口令规则（例如，口令必须至少包含一位）。如果使用口令验证函数，则不能在 **GRANT CONNECT** 语句中指定多个用户 ID 和口令。

  用于散列用户口令的加密算法是经 FIPS 认证的加密支持：
  - 此 DLL 称为 dbfips10.dll
  - HASH 函数接受以下算法：SHA1_FIPS SHA256_FIPS。
  - 如果指定了 -fips 服务器选项并向 HASH 函数提供了一个非 FIPS 认证的算法，则数据库服务器将使用 SHA1_FIPS 而不用 SHA1，使用 SHA256_FIPS 而不用 SHA256，并在使用了 MD5（MD5 不是 FIPS 认证的算法）的情况下返回一个错误。
  - 如果指定了 -fips 选项，则数据库服务器将使用 SHA256_FIPS 进行口令散列处理。

示例

（返回顶部） （第 233 页）

- **示例 1** – 创建一个名为 `SQLTester` 的用户，口令为 welcome。为 `SQLTester` 用户指派 `Test1` 登录策略，且下次登录时口令将到期：

```
CREATE USER SQLTester IDENTIFIED BY welcome
LOGIN POLICY Test1
FORCE PASSWORD CHANGE ON;
```

标准

(返回顶部) (第 233 页)

- SQL - ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - 不受 Adaptive Server 支持。

权限

(返回顶部) (第 233 页)

需要 MANAGE ANY USER 系统特权。

DROP LDAP SERVER 语句

验证 LDAP 服务器配置对象未处于 READY 或 ACTIVE 状态后，从 SYSLDAPSERVER 系统视图中删除命名的 LDAP 服务器配置对象。

快速链接:

转至参数 (第 235 页)

转至示例 (第 235 页)

转至用法 (第 236 页)

转至标准 (第 236 页)

转至权限 (第 236 页)

语法

```
DROP LDAP SERVER ldapua-server-name
   [ WITH DROP ALL REFERENCES ] [ WITH SUSPEND ]
```

参数

(返回顶部) (第 235 页)

- **WITH DROP ALL REFERENCES** – 用于从服务中删除在登录策略中所引用的 LDAP 服务器配置对象。
- **WITH SUSPEND** – 使用该语句，即使 LDAP 服务器配置对象处于 READY 或 ACTIVE 状态，也可以将其删除。

示例

(返回顶部) (第 235 页)

- **示例 1** – 假定已从所有登录策略中删除对 LDAP 服务器配置对象的引用，则以下两组命令等效。使用 WITH DROP ALL REFERENCES 和 WITH SUSPEND 参数就不必在 **DROP LDAP SERVER** 语句之前执行 **ALTER LDAP SERVER** 语句:

```
DROP LDAP SERVER ldapserver1 WITH DROP ALL REFERENCES WITH SUSPEND
```

等效于

```
ALTER LDAP SERVER ldapserver1 WITH SUSPEND DROP LDAP SERVER
ldapserver1 WITH DROP ALL REFERENCES
```

用法

(返回顶部) （第 235 页）

针对状态为 READY 或 ACTIVE 的 LDAP 服务器配置对象发出 **DROP LDAP SERVER** 语句时，该语句失败。这样可确保不会无意删除处于使用状态的 LDAP 服务器配置对象。如果存在引用 LDAP 服务器配置对象的登录策略，**DROP LDAP SERVER** 语句也将失败。

标准

(返回顶部) （第 235 页）

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 235 页）

需要 MANAGE ANY LDAP SERVER 系统特权。

DROP LOGIN POLICY 语句

从数据库中删除登录策略。

快速链接:

转至示例 （第 236 页）

转至用法 （第 237 页）

转至权限 （第 237 页）

语法

DROP LOGIN POLICY *policy-name*

示例

(返回顶部) （第 236 页）

- **示例 1** – 先创建 `Test11` 登录策略，然后将其删除：

```
CREATE LOGIN POLICY Test11;
DROP LOGIN POLICY Test11 ;
```

用法

(返回顶部) (第 236 页)

如果您尝试删除已分配给用户的策略，则 **DROP LOGIN POLICY** 语句会失败。您可以使用 **ALTER USER** 语句更改用户的策略分配，或使用 **DROP USER** 语句删除用户。

权限

(返回顶部) (第 236 页)

需要 MANAGE ANY LOGIN POLICY 系统特权。

DROP ROLE 语句

从数据库中删除用户定义的角色，或者将用户扩展角色转换为常规用户。

快速链接:

转至参数 (第 237 页)

转至示例 (第 238 页)

转至用法 (第 238 页)

转至标准 (第 238 页)

转至权限 (第 238 页)

语法

```
DROP ROLE [ FROM USER ] role_name
    [ WITH REVOKE ]
```

参数

(返回顶部) (第 237 页)

- **role_name** – 必须是数据库中已存在的角色的名称。
- **FROM USER** – 需要该参数才能将用户扩展角色转换为常规用户，而不是将其从数据库中删除。*role_name* 必须存在于数据库中。

  用户保留所有登录特权、系统特权以及向用户扩展角色授予的角色，并将成为用户扩展角色拥有的所有对象的所有者。向用户扩展角色授予的所有用户将立即撤消。
- **WITH REVOKE** – 删除为用户授予了基础系统特权的独立角色或用户扩展角色时需要此参数。既可以使用 WITH ADMIN OPTION 也可以使用 WITH NO ADMIN OPTION 子句进行授权。

示例

(返回顶部) （第 237 页）

- **示例 1** – 将尚未向其他用户或角色授予的名为 Joe 的用户扩展角色转换回常规用户：

```
DROP ROLE FROM USER Joe
```

- **示例 2** – 将尚未向其他用户或角色授予的名为 Jack 的用户扩展角色从数据库中删除：

```
DROP ROLE Jack
```

- **示例 3** – 将尚未向其他用户或角色授予的名为 Sam 的用户扩展角色转换回常规角色：

```
DROP ROLE FROM USER Sam
WITH REVOKE
```

- **示例 4** – 将已向其他用户或角色授予的名为 Sales2 的独立角色从数据库中删除：

```
DROP ROLE Sales2
WITH REVOKE
```

用法

(返回顶部) （第 237 页）

只要所有剩余的相关角色满足具有活动口令的管理用户的最低要求数量，用户定义的角色便可随时从数据库中删除或转换回常规用户。

标准

(返回顶部) （第 237 页）

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 237 页）

- 需要对待删除的角色具有管理权限。
- 如果待删除角色拥有对象，在执行 DROP 语句时，任何用户在任何会话中都未使用这些对象。

DROP USER 语句

删除用户。

快速链接：

转至参数 （第 239 页）

转至示例 （第 239 页）
转至标准 （第 239 页）
转至权限 （第 239 页）

语法

```
DROP USER user-name
```

参数

(返回顶部) （第 238 页）

- **user-name** – 要删除的用户的名称。

示例

(返回顶部) （第 238 页）

- **示例 1** – 从数据库中删除用户 SQLTester：

```
DROP USER SQLTester
```

标准

(返回顶部) （第 238 页）

- SQL - 符合 ISO/ANSI SQL 标准。
- SAP Sybase 数据库产品 - 不受 Adaptive Server 支持。

权限

(返回顶部) （第 238 页）

需要 MANAGE ANY USER 系统特权。

注意： 删除用户时，将一同删除该用户拥有的对象以及授予的权限。

GRANT CHANGE PASSWORD 语句

允许用户管理其他用户的口令并管理 CHANGE PASSWORD 系统特权。

快速链接：

转至参数 （第 240 页）
转至示例 （第 240 页）
转至用法 （第 241 页）
转至标准 （第 241 页）
转至权限 （第 241 页）

语法

```
GRANT CHANGE PASSWORD ( target_user_list | ANY | ANY WITH ROLES
target_role_list )
   TO userID [,...]
   [ WITH ADMIN [ONLY] OPTION | WITH NO ADMIN OPTION]
```

参数

(返回顶部) (第 239 页)

- **target_user_list** – 用户（被授予者）可以进行模仿。此列表必须包含具有登录口令的现有用户或用户扩展角色。列表中的 userID 用逗号分隔。
- **ANY** – 所有具有登录口令的数据库用户都会成为管理每个被授予者口令的潜在目标用户。
- **ANY WITH ROLES *target_role_list*** – 每个被授予者的目标角色列表。被授予任何目标角色的所有用户都会成为每个被授予者的潜在目标用户。*target_role_list* 必须包含现有角色，而被授予上述角色的用户必须包含具有登录口令的数据库用户。多个 userID 使用逗号来分隔。
- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。
- **WITH ADMIN OPTION** – （仅在使用 ANY 子句时有效）用户既可以管理口令，也可以将 CHANGE PASSWORD 系统特权授予其他用户。
- **WITH ADMIN ONLY OPTION** – （仅在使用 ANY 子句时有效）用户可将 CHANGE PASSWORD 系统特权授予其他用户，但不能管理其他用户的口令。
- **WITH NO ADMIN OPTION** – 用户可以管理口令，但不能将 CHANGE PASSWORD 系统特权授予其他用户。

示例

(返回顶部) (第 239 页)

- **示例 1** – 为 `Sally` 和 `Laurel` 授予对 `Bob`、`Sam` 和 `Peter` 的口令进行管理的权限：

  ```
  GRANT CHANGE PASSWORD (Bob, Sam, Peter) TO (Sally, Laurel)
  ```

- **示例 2** – 为 `Mary` 授予将 CHANGE PASSWORD 系统特权授予数据库中任何用户的权限。但是，由于使用 WITH ADMIN ONLY OPTION 子句授予系统特权，因此，`Mary` 无法管理任何其他用户的口令。

  ```
  GRANT CHANGE PASSWORD (ANY) TO Mary WITH ADMIN ONLY OPTION
  ```

- **示例 3** – 为 `Steve` 和 `Joe` 授予对 `Role1` 或 `Role2` 的任何成员的口令进行管理的权限：

```
GRANT CHANGE PASSWORD (ANY WITH ROLES Role1, Role2) TO Steve, Joe
```

用法

(返回顶部) （第 239 页）

可为用户授予管理数据库中任意用户 (ANY) 口令或仅管理特定用户 (*target_users_list*) 口令或特定角色的成员 (ANY WITH ROLES *target_roles_list*) 口令的权限。仅当使用 ANY 子句时才能授予 CHANGE PASSWORD 系统特权的管理权限。

如果未指定子句，则缺省情况下使用 ANY。如果未在授予语句中指定任何管理子句，则使用 WITH NO ADMIN OPTION 子句。

缺省情况下，使用 WITH NO ADMIN OPTION 子句将 CHANGE PASSWORD 系统特权授予 SYS_AUTH_SA_ROLE 兼容性角色，使用 ADMIN ONLY OPTION 子句将该系统特权授予 SYS_AUTH_SSO_ROLE 兼容性角色（前提是存在上述两个角色）。

标准

(返回顶部) （第 239 页）

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 239 页）

- 已授予 CHANGE PASSWORD 系统特权以及管理权限。
- 每个指定目标用户 (target_users_list) 都是具有登录口令的现有用户角色或用户扩展角色。
- 每个指定目标角色 (target_roles_list) 都必须是现有用户扩展角色或用户定义角色。

GRANT CONNECT 语句

向用户授予 CONNECT 特权。

快速链接:

转至参数 （第 242 页）

转至示例 （第 242 页）

转至用法 （第 242 页）

转至标准 （第 243 页）

转至权限 （第 243 页）

语法

```
GRANT CONNECT
   TO userID [,...]
   IDENTIFIED BY password [,...]
```

参数

(返回顶部) (第 241 页)

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

示例

(返回顶部) (第 241 页)

- **示例 1** – 为数据库创建两个新用户，分别名为 `Laurel` 和 `Hardy`：

```
GRANT CONNECT TO Laurel, Hardy
IDENTIFIED BY Stan, Ollie
```

- **示例 2** – 创建没有口令的用户 `Jane`：

```
GRANT CONNECT TO Jane
```

- **示例 3** – 将 `Bob` 的口令更改为 `newpassword`：

```
GRANT CONNECT TO Bob IDENTIFIED BY newpassword
```

用法

(返回顶部) (第 241 页)

GRANT CONNECT 可用于创建新用户，也可供任意用户更改自己的口令。

提示： 要创建用户，请使用 **CREATE USER** 语句，而不是 **GRANT CONNECT** 语句。

如果您在尝试添加新用户时无意间输入了某现有用户的用户 ID，则实际上是在更改现有用户的口令。您不会收到警告，因为这会被视为正常操作。

存储过程 **sp_addlogin** 和 **sp_adduser** 也可用于添加用户。如果尝试添加现有用户 ID，这两个过程将显示一条错误。

注意： 要添加和移除用户 ID，请使用系统过程，而不是 **GRANT** 和 **REVOKE** 语句。

没有口令的用户不能连接到数据库。这在您想要创建组但不希望任何人连接到角色用户 ID 时很有用。要创建没有口令的用户，请不要包括 IDENTIFIED BY 子句。

指定口令时，它必须是有效的标识符。口令的最大长度为 255 个字节。如果 **VERIFY_PASSWORD_FUNCTION** 数据库选项已设置为一个值而不是空字符串，则 **GRANT CONNECT TO** 语句将调用由此选项值标识的函数。该函数将返回 NULL，表明口令符合规则。如果设置了 `VERIFY_PASSWORD_FUNCTION` 选项，则只能使用 **GRANT CONNECT** 语句指定一个 *userid* 和 *password*。

数据库用户 ID 和口令的无效名称包括以下情况：

- 以空格、单引号或双引号开头

- 以空格结尾
- 含有分号

标准

(返回顶部) (第 241 页)

- SQL - 其它语法是 ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - Adaptive Server 和 SAP Sybase IQ 中的安全模型不同，所以其它语法也不同。

权限

(返回顶部) (第 241 页)

- 如果要创建新用户，必须具有 MANAGE ANY USER 系统特权。
- 任何用户均可更改自己的口令。
- 如果要更改其他用户的口令，必须具有 CHANGE PASSWORD 系统特权。

注意： 如果要更改其他用户的口令，该相应用户将无法连接到数据库。

另请参见

- CREATE USER 语句 (第 233 页)

GRANT CREATE 语句

向指定用户和角色授予对指定 dbspace 的 CREATE 特权。

快速链接:

转至参数 (第 243 页)

转至示例 (第 244 页)

转至标准 (第 244 页)

转至权限 (第 244 页)

语法

```
GRANT CREATE
   ON dbspace_name
   TO userID [,...]
```

参数

(返回顶部) (第 243 页)

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

示例

(返回顶部) (第 243 页)

- **示例 1** – 向用户 `Lawrence` 和 `Swift` 授予对 dbspace *DspHist* 的 `CREATE` 特权：

```
GRANT CREATE ON DspHist
TO LAWRENCE, SWIFT
```

- **示例 2** – 向用户 `Fiona` 和 `Ciaran` 授予对 dbspace `DspHist` 的 `CREATE` 特权：

```
GRANT CREATE ON DspHist TO Fiona, Ciaran
```

标准

(返回顶部) (第 243 页)

- SQL - 其它语法是 ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - Adaptive Server 和 SAP Sybase IQ 中的安全模型不同，所以其它语法也不同。

权限

(返回顶部) (第 243 页)

需要 MANAGE ANY DBSPACE 系统特权。

GRANT EXECUTE 语句

授予对过程或用户定义函数的 EXECUTE 特权。

快速链接：

转至参数 (第 244 页)

转至标准 (第 245 页)

转至权限 (第 245 页)

语法

```
GRANT EXECUTE
  ON [ owner.] {procedure-name | user-defined-function-name }
  TO userID [,...]
```

参数

(返回顶部) (第 244 页)

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

标准

(返回顶部) (第 244 页)

- SQL - 语法是持久存储模块特性。
- SAP Sybase 数据库产品 - Adaptive Server 和 SAP Sybase IQ 中的安全模型不同，所以其它语法也不同。

权限

(返回顶部) (第 244 页)

需要以下权限之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权。
- 您拥有该过程。

GRANT 对象级特权语句

向用户或角色授予对单个表或视图的数据库对象级特权。

快速链接：

转至参数 (第 246 页)

转至用法 (第 246 页)

转至标准 (第 246 页)

转至权限 (第 246 页)

语法

```
GRANT  object-level-privilege  [, ⋯]
    ON  [ owner.]object-name
    TO  userID [,...]
    [  WITH GRANT OPTION  ]

object-level-privilege
    ALL  [  PRIVILEGES  ]
    |  ALTER
    |  DELETE
    |  INSERT
    |  LOAD
    |  REFERENCE  [  (  column-name  [, ⋯]  )  ]
    |  SELECT  [  (  column-name  [, ⋯]  )  ]
    |  TRUNCATE
    |  UPDATE  [  (  column-name, ⋯)  ]  }
```

参数

(返回顶部) (第 245 页)

- **userID** – 必须是现有用户或不可变角色的名称。该列表必须包含具有登录口令的现有用户。列表中的 userID 用逗号分隔。
- **ALL** – 将所有特权授予用户
- **ALTER** – 用户可使用 **ALTER TABLE** 语句来变更此表。不允许对视图使用此特权。
- **DELETE** – 用户可从此表或视图中删除行。
- **INSERT** – 用户可向指定的表或视图插入行。
- **LOAD** – 用户可在指定的表或视图中装载数据。
- **REFERENCES** – 用户可在指定的表上创建索引，以及创建引用指定表的外键。如果指定了列名，则用户只能引用指定的这些列。列的 REFERENCES 特权不能授予视图，只能授予表。
- **SELECT** – 用户可查看此视图或表中的信息。如果指定了列名，则用户只能查看指定的这些列。列的 SELECT 权限不能授予视图，只能授予表。.
- **TRUNCATE** – 用户可截断指定的表或视图。
- **UPDATE** – 用户可更新此视图或表中的行。如果指定了列名，则用户只能更新指定的这些列。列的 UPDATE 特权不能授予视图，只能授予表。要更新表，用户必须对表拥有 SELECT 和 UPDATE 特权。
- **WITH GRANT OPTION** – 指定用户 ID 也被授予向其他用户 ID 授予相同特权的特权。

用法

(返回顶部) (第 245 页)

可以列出表特权，也可以指定 ALL 一次性授予所有特权。

标准

(返回顶部) (第 245 页)

- SQL - 语法是入门级特性。
- SAP Sybase 数据库产品 - Adaptive Server 中支持语法。

权限

(返回顶部) (第 245 页)

需要以下权限之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权
- 已使用 WITH GRANT OPTION 子句授予您对表的特定对象特权。
- 您拥有该表。

GRANT ROLE 语句

向用户或其他角色授予角色，无论该用户或角色是否具有管理权限。

快速链接：

转至参数 （第 248 页）

转至示例 （第 248 页）

转至用法 （第 249 页）

转至标准 （第 251 页）

转至权限 （第 251 页）

语法

```
GRANT ROLE  role_name  [, ⋯]
    TO  grantee [, ⋯]
    [ {WITH NO ADMIN  |  WITH ADMIN  [  ONLY  ]  }  OPTION  ]
    [  WITH NO SYSTEM PRIVILEGE INHERITANCE  ]

role_name
    dbo□□□
    |  diagnostics□□□
    |  PUBLIC□□□
    |  rs_systabgroup□□□
    |  SA_DEBUG□□□
    |  SYS□□□
    |  SYS_AUTH_SA_ROLE
    |  SYS_AUTH_SSO_ROLE
    |  SYS_AUTH_DBA_ROLE□□
    |  SYS_AUTH_RESOURCE_ROLE□
    |  SYS_AUTH_BACKUP_ROLE□
    |  SYS_AUTH_VALIDATE_ROLE□
    |  SYS_AUTH_WRITEFILE_ROLE
    |  SYS_AUTH_WRITEFILECLIENT_ROLE
    |  SYS_AUTH_READFILE_ROLE
    |  SYS_AUTH_READFILECLIENT_ROLE
    |  SYS_AUTH_PROFILE_ROLE
    |  SYS_AUTH_USER_ADMIN_ROLE
    |  SYS_AUTH_SPACE_ADMIN_ROLE
    |  SYS_AUTH_MULTIPLEX_ADMIN_ROLE
    |  SYS_AUTH_OPERATOR_ROLE
    |  SYS_AUTH_PERMS_ADMIN_ROLE
    |  SYS_REPLICATE_ADMIN_ROLE□□□
    |  SYS_RUN_REPLICATE_ROLE□□□
    |  SYS_SPATIAL_ADMIN_ROLE□□□
    |  user-defined role name
```

- 向其他角色授予选择兼容性角色时可以使用 WITH NO SYSTEM PRIVILEGE INHERITANCE 子句。它用于防止兼容性角色的成员自动继承该角色的基础系统特权。授予给用户扩展的角色时，WITH NO SYSTEM PRIVILEGE INHERITANCE 子句仅适用于角色成员。充当角色的用户会自动继承基础系统特权，而不考虑子句为何。
- WITH NO ADMIN OPTION WITH NO SYSTEM PRIVILEGE INHERITANCE 和 WITH NO SYSTEM PRIVILEGE INHERITANCE 子句在语义上等效。
- ☒授予 SYS_AUTH_BACKUP_ROLE、SYS_AUTH_RESOURCE_ROLE 或 SYS_AUTH_VALIDATE_ROLE 角色时，不能结合 WITH NO SYSTEM PRIVILEGE INHERITANCE 子句指定 WITH ADMIN OPTION 或 WITH ADMIN ONLY 子句。
- ☒☒授予 SYS_AUTH_DBA_ROLE 或 SYS_RUN_REPLICATION_ROLE 角色时，只能结合 WITH NO SYSTEM PRIVILEGE INHERITANCE 子句来指定 WITH ADMIN OPTION 子句。
- ☒☒☒系统角色不支持 WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句。

参数

(返回顶部) (第 247 页)

- **role_name** – 必须已存在于数据库中。用逗号分隔多个角色名。
- **grantee** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。
- **WITH NO ADMIN OPTION** – 为每个 *grantee* 授予每个 *role_name* 的基础系统特权，但不能向其他用户授予 *role_name*。
- **WITH ADMIN ONLY OPTION** – 为每个 *userID* 授予对各 *role_name* 的管理特权，但不会被授予 *role_name* 的基础系统特权。
- **WITH ADMIN OPTION** – 为每个 userID 授予每个 *role_name* 的基础系统特权以及将 *role_name* 授予其他用户的权限。
- **WITH NO SYSTEM PRIVILEGE INHERITANCE** – 接收角色的成员不会继承授予角色的基础系统特权。但是，如果接收角色是用户扩展角色，则向扩展用户授予基础系统特权。

示例

(返回顶部) (第 247 页)

- **示例 1** – 将 `Sales_Role` 授予 `Sally`，同时授予管理特权，这意味着她可以将 `Sales_Role` 授予其他用户或从其他用户撤消，也可以执行该角色授予的任何已授权任务：

```
GRANT ROLE Sales_Role TO Sally WITH ADMIN OPTION
```

- **示例 2** – 将兼容性角色 SYS_AUTH_PROFILE_ROLE 授予角色 Sales_Admin，但不授予管理权限。Sales_Admin 是独立角色，并且已向 Mary 和 Peter 授予 Sales_Admin。由于 SYS_AUTH_PROFILE_ROLE 是可继承的兼容性角色，因此，向 Mary 和 Peter 授予 Sales_Role 的基础系统特权。由于授予该角色时未授予管理权限，因此，他们无法授予或撤消此角色。

```
GRANT ROLE SYS_AUTH_PROFILE_ROLE TO Sales_Role WITH NO ADMIN
OPTION
```

- **示例 3** – 将兼容性角色 SYS_AUTH_BACKUP_ROLE 授予 Tom，但不授予管理权限。Tom 是用户扩展角色，已为其授予了 Betty 和 Laurel。由于 SYS_AUTH_BACKUP_ROLE 是不可继承的兼容性角色，因此，未向 Betty 和 Laurel 授予该角色的基础系统特权。但是，由于 Tom 是扩展用户，因此，将直接向 Tom 授予基础系统特权。

```
GRANT ROLE SYS_AUTH_BACKUP_ROLE TO Tom
WITH NO SYSTEM PRIVILEGE INHERITANCE
```

用法

(返回顶部) (第 247 页)

使用 WITH ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句可以让被授予者授予或撤消角色，但不允许被授予者删除角色。

缺省情况下，如果未在授予语句中指定任何管理子句，则授予每个兼容性角色时还授予以下缺省管理权限：

WITH ADMIN OPTION	WITH ADMIN ONLY OPTION	WITH NO ADMIN OPTION
SYS_AUTH_SA_ROLE SYS_AUTH_SSO_ROLE	SYS_AUTH_DBA_ROLE	SYS_AUTH_RESOURCE_ROLE SYS_AUTH_BACKUP_ROLE SYS_AUTH_VALIDATE_ROLE SYS_AUTH_WRITEFILE_ROLE SYS_AUTH_WRITEFILECLIENT_ROLE SYS_AUTH_READFILE_ROLE SYS_AUTH_READFILECLIENT_ROLE SYS_AUTH_PROFILE_ROLE SYS_AUTH_USER_ADMIN_ROLE SYS_AUTH_SPACE_ADMIN_ROLE SYS_AUTH_MULTIPLEX_ADMIN_ROLE SYS_AUTH_OPERATOR_ROLE SA_DEBUG SYS_RUN_REPLICATION_ROLE

SYS_AUTH_PERMS_ADMIN_ROLE 角色授予下列基础角色以及缺省管理权限：

WITH ADMIN OPTION	WITH NO ADMIN OPTION
SYS_AUTH_BACKUP_ROLE SYS_AUTH_OPERATOR_ROLE SYS_AUTH_USER_ADMIN_ROLE SYS_AUTH_SPACE_ADMIN_ROLE SYS_AUTH_MULTIPLEX_ADMIN_ROLE SYS_AUTH_RESOURCE_ROLE SYS_AUTH_VALIDATE_ROLE SYS_AUTH_PROFILE_ROLE SYS_AUTH_WRITEFILE_ROLE SYS_AUTH_WRITEFILECLIENT_ROLE SYS_AUTH_READFILE_ROLE SYS_AUTH_READFILECLIENT_ROLE	MANAGE ROLES MANAGE ANY OBJECT PRIVILEGE CHANGE PASSWORD

标准

(返回顶部) (第 247 页)

- SQL - 其它语法是 ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - Adaptive Server 中支持语法。

权限

(返回顶部) (第 247 页)

- 需要 MANAGE ROLES 系统特权才能授予以下系统角色：
  - dbo
  - diagnostics
  - PUBLIC
  - rs_systabgroup
  - SA_DEBUG SYS
  - SYS
  - SYS_REPLICATION_ADMIN_ROLE
  - SYS_RUN_REPLICATION_ROLE
  - SYS_SPATIAL_ADMIN_ROLE
- 需要对角色具有管理特权才能授予以下角色：
  - SYS_AUTH_SA_ROLE
  - SYS_AUTH_SSO_ROLE
  - SYS_AUTH_DBA_ROLE
  - SYS_AUTH_RESOURCE_ROLE
  - SYS_AUTH_BACKUP_ROLE
  - SYS_AUTH_VALIDATE_ROLE
  - SYS_AUTH_WRITEFILE_ROLE
  - SYS_AUTH_WRITEFILECLIENT_ROLE
  - SYS_AUTH_READFILE_ROLE
  - SYS_AUTH_READFILECLIENT_ROLE
  - SYS_AUTH_PROFILE_ROLE
  - SYS_AUTH_USER_ADMIN_ROLE
  - SYS_AUTH_SPACE_ADMIN_ROLE
  - SYS_AUTH_MULTIPLEX_ADMIN_ROLE
  - SYS_AUTH_OPERATOR_ROLE
  - SYS_AUTH_PERMS_ADMIN_ROLE
  - <用户定义的角色名称>

GRANT SET USER 语句

为某一用户授予模仿其他用户和管理 SET USER 系统特权的能力。

快速链接：

转至参数 （第 252 页）

转至示例 （第 253 页）

转至用法 （第 253 页）

转至标准 （第 253 页）

转至权限 （第 253 页）

语法

```
GRANT SET USER ( target_users_list
       | ANY
       | ANY WITH ROLES target_roles_list )
  TO userID [,...]
  [ WITH ADMIN [ ONLY ] OPTION | WITH NO ADMIN OPTION ]
```

参数

（返回顶部） （第 252 页）

- **target_users_list** – 必须包含具有登录口令的现有用户，并且是被授予者用户不可再模仿的潜在目标用户列表。列表中的用户 ID 用逗号分隔。
- **ANY** – 每个被授予者的潜在目标用户的列表中均包含具有登录口令的所有数据库用户。
- **ANY WITH ROLES *target_roles_list*** – *target_role_list* 必须包含现有角色，而每个被授予者的潜在目标用户列表必须包含具有登录口令的数据库用户，这些用户具有 *target_role_list* 中的角色子集。角色列表用逗号分隔。
- **userID** – 每个 *userID* 都必须是现有用户或不可变角色的名称。该列表必须包含具有登录口令的现有用户。列表中的 userID 用逗号分隔。
- **WITH ADMIN OPTION** – （仅在与 ANY 子句结合使用时有效）用户既可以发出 SETUSER 命令来模仿其他用户，也可以将 SET USER 系统特权授予其他用户。
- **WITH ADMIN ONLY OPTION** – （仅在与 ANY 子句结合使用时有效）用户可将 SET USER 系统特权授予其他用户，但不能发出 SETUSER 命令用于模仿其他用户。
- **WITH NO ADMIN OPTION** – 用户可发出 SETUSER 命令用于模仿其他用户，但不能将 SET USER 系统特权授予其他用户。

示例

(返回顶部) (第 252 页)

- **示例 1** – 为 Sally 和 Laurel 授予模仿 Bob、Sam 和 Peter 的能力：

```
GRANT SET USER (Bob, Sam, Peter) TO (Sally, Laurel)
```

- **示例 2** – 为 Mary 授予将 SET USER 系统特权授予数据库中任何用户的权限。但是，由于使用 WITH ADMIN ONLY OPTION 子句授予系统特权，因此，Mary 无法模仿任何其他用户。

```
GRANT SET USER (ANY) TO Mary WITH ADMIN ONLY OPTION
```

- **示例 3** – 为 Steve 和 Joe 授予模仿 Role1 或 Role2 的任意成员的能力：

```
GRANT SET USER (ANY WITH ROLES Role1, Role2) TO Steve, Joe
```

用法

(返回顶部) (第 252 页)

可为某位用户授予模仿数据库中任意用户 (ANY)，或仅模仿特定用户 (*target_users_list*) 或模仿特定角色成员 (ANY WITH ROLES *target_roles_list*) 的权限。仅当使用 ANY 子句时才能授予 SET USER 系统特权的管理权限。

如果未指定子句，则缺省情况下使用 ANY。如果未在授予语句中指定任何管理子句，则使用 WITH NO ADMIN OPTION 子句。

重新向用户授予 SET USER 系统特权时，重新授予行为的影响是累积的。

缺省情况下，使用 WITH NO ADMIN OPTION 子句将 SET USER 系统特权授予 SYS_AUTH_SSO_ROLE 兼容性角色（前提是存在该角色）。

为某用户授予 SET USER 系统特权仅仅是授予其模仿其他用户的权限。在发出 **SETUSER** 语句前，不会对成功模仿其他用户所需的*必要*条件进行校验。

标准

(返回顶部) (第 252 页)

ANSI SQL – 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) (第 252 页)

- 已授予 SET USER 系统特权以及管理权限。
- 每个指定目标用户 (target_users_list) 都是具有登录口令的现有用户角色或用户扩展角色。
- 每个指定目标角色 (target_roles_list) 都必须是现有用户扩展角色或用户定义角色。

GRANT 系统特权语句

向用户或角色授予特定系统特权，无论该用户或角色是否具有管理权限。

快速链接：

转至参数 （第 254 页）

转至示例 （第 254 页）

转至用法 （第 255 页）

转至标准 （第 255 页）

转至权限 （第 255 页）

语法

```
GRANT system_privilege_name [, ⋯]
   TO userID [, ⋯]
   [ { WITH NO ADMIN | WITH ADMIN [ ONLY ] } OPTION ]
```

参数

(返回顶部) （第 254 页）

- **system_privilege_name** – 必须是现有系统特权的名称。
- **userID** – 必须是现有用户或不可变角色的名称。该列表必须包含具有登录口令的现有用户。多个 userID 用逗号分隔。
- **WITH NO ADMIN OPTION** – 用户可以管理系统特权，但不能向其他用户授予系统特权。
- **WITH ADMIN ONLY OPTION** – 如果使用 WITH ADMIN ONLY OPTION 子句，则每个 *userID* 均被授予对每个 *system_privilege* 的管理特权，但不授予 *system_privilege* 本身。
- **WITH ADMIN OPTION** – 除 *system_privilege* 的所有基础系统特权外，每个 *userID* 还被授予对各 *system_privilege* 的管理特权。

示例

(返回顶部) （第 254 页）

- **示例 1** – 向具有管理特权的 `Joe` 授予 DROP CONNECTION 系统特权：

  ```
  GRANT DROP CONNECTION TO Joe WITH ADMIN OPTION
  ```

- **示例 2** – 向不具有管理特权的 `Sally` 授予 CHECKPOINT 系统特权：

  ```
  GRANT CHECKPOINT TO Sally WITH NO ADMIN OPTION
  ```

- **示例 3** – 向仅具有管理特权的 Jane 授予 MONITOR 系统特权：

```
GRANT MONITOR TO Jane WITH ADMIN ONLY OPTION
```

用法

(返回顶部) （第 254 页）

缺省情况下，如果未在授予语句中指定任何管理子句，则使用 WITH NO ADMIN OPTION 子句。

标准

(返回顶部) （第 254 页）

- SQL - 其它语法是 ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - Adaptive Server 中支持语法。

权限

(返回顶部) （第 254 页）

需要具备对要授予的系统特权的管理特权。

所有系统特权的列表

所有系统特权的列表。

系统特权用于控制用户执行授权数据库任务的权限。

下面列出了可用的系统特权：

- ACCESS SERVER LS
- ALTER ANY INDEX
- ALTER ANY MATERIALIZED VIEW
- ALTER ANY OBJECT
- ALTER ANY OBJECT OWNER
- ALTER ANY PROCEDURE
- ALTER ANY SEQUENCE
- ALTER ANY TABLE
- ALTER ANY TEXT CONFIGURATION
- ALTER ANY TRIGGER
- ALTER ANY VIEW
- ALTER DATABASE
- ALTER DATATYPE
- BACKUP DATABASE
- CHANGE PASSWORD

- CHECKPOINT
- COMMENT ANY OBJECT
- CREATE ANY INDEX
- CREATE ANY MATERIALIZED VIEW
- CREATE ANY OBJECT
- CREATE ANY PROCEDURE
- CREATE ANY SEQUENCE
- CREATE ANY TABLE
- CREATE ANY TEXT CONFIGURATION
- CREATE ANY TRIGGER
- CREATE ANY VIEW
- CREATE DATATYPE
- CREATE EXTERNAL REFERENCE
- CREATE MATERIALIZED VIEW
- CREATE MESSAGE
- CREATE PROCEDURE
- CREATE PROXY TABLE
- CREATE TABLE
- CREATE TEXT CONFIGURATION
- CREATE VIEW
- DEBUG ANY PROCEDURE
- DELETE ANY TABLE
- DROP ANY INDEX
- DROP ANY MATERIALIZED VIEW
- DROP ANY OBJECT
- DROP ANY PROCEDURE
- DROP ANY SEQUENCE
- DROP ANY TABLE
- DROP ANY TEXT CONFIGURATION
- DROP ANY VIEW
- DROP CONNECTION
- DROP DATATYPE
- DROP MESSAGE
- EXECUTE ANY PROCEDURE
- LOAD ANY TABLE
- INSERT ANY TABLE
- MANAGE ANY DBSPACE
- MANAGE ANY EVENT
- MANAGE ANY EXTERNAL ENVIRONMENT

- MANAGE ANY EXTERNAL OBJECT
- MANAGE ANY LDAP SERVER
- MANAGE ANY LOGIN POLICY
- MANAGE ANY MIRROR SERVER
- MANAGE ANY OBJECT PRIVILEGES
- MANAGE ANY SPATIAL OBJECT
- MANAGE ANY STATISTICS
- MANAGE ANY USER
- MANAGE ANY WEB SERVICE
- MANAGE AUDITING
- MANAGE MULTIPLEX
- MANAGE PROFILING
- MANAGE REPLICATION
- MANAGE ROLES
- MONITOR
- READ CLIENT FILE
- READ FILE
- REORGANIZE ANY OBJECT
- SELECT ANY TABLE
- SERVER OPERATOR
- SET ANY PUBLIC OPTION
- SET ANY SECURITY OPTION
- SET ANY SYSTEM OPTION
- SET ANY USER DEFINED OPTION
- SET USER（仅授予管理权限）
- TRUNCATE ANY TABLE
- UPDATE ANY TABLE
- UPGRADE ROLE
- USE ANY SEQUENCE
- VALIDATE ANY OBJECT
- WRITE CLIENT FILE
- WRITE FILE

GRANT USAGE ON SEQUENCE 语句

将指定序列的 USAGE 系统特权授予用户或角色。

快速链接：

转至参数 （第 258 页）

转至标准 （第 258 页）

转至权限 （第 258 页）

语法

```
GRANT USAGE ON SEQUENCE sequence-name
   TO userID [,...]
```

参数

(返回顶部) （第 257 页）

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

标准

(返回顶部) （第 257 页）

- SQL - 语法是持久存储模块特性。
- SAP Sybase 数据库产品 - Adaptive Server 和 SAP Sybase IQ 中的安全模型不同，因此其它语法也不同。

权限

(返回顶部) （第 257 页）

需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权。
- 您拥有该序列。

REVOKE CHANGE PASSWORD 语句

使用户无法管理口令和系统特权。

快速链接：

转至参数 （第 259 页）

转至示例 （第 259 页）

转至用法 （第 259 页）

转至标准 （第 260 页）

转至权限 （第 260 页）

语法

```
REVOKE [ ADMIN OPTION FOR ] CHANGE PASSWORD
   [(target_user_list
      | ANY
      | ANY WITH ROLES target_role_list )]
   FROM userID [,...]
```

参数

(返回顶部) (第 258 页)

- **target_user_list** – 用户（被授予者）可以进行模仿。此列表必须包含具有登录口令的现有用户或用户扩展角色。列表中的 userID 用逗号分隔。
- **ANY** – 所有具有登录口令的数据库用户都会成为管理每个被授予者口令的潜在目标用户。
- **ANY WITH ROLES *target_role_list*** – 每个被授予者的目标角色列表。被授予任何目标角色的所有用户都会成为每个被授予者的潜在目标用户。*target_role_list* 必须包含现有角色，而被授予上述角色的用户必须包含具有登录口令的数据库用户。多个 userID 使用逗号来分隔。
- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

示例

(返回顶部) (第 258 页)

- **示例 1** – 使 `Joe` 无法管理 `Sally` 或 `Bob` 的口令：

```
REVOKE CHANGE PASSWORD (Sally, Bob) FROM Joe
```

- **示例 2** – 如果最初使用 WITH ADMIN OPTION 子句将 CHANGE PASSWORD 系统特权授予 `Sam`，本示例将使 `Sam` 无法向其他用户授予 CHANGE PASSWORD 系统特权，但仍允许 `Sam` 管理原始 **GRANT CHANGE PASSWORD** 语句中指定的用户的口令。但是，如果最初使用 WITH ADMIN ONLY OPTION 子句将 CHANGE PASSWORD 系统特权授予 `Sam`，本示例将删除 `Sam` 对系统特权拥有的所有权限。

```
REVOKE ADMIN OPTION FOR CHANGE PASSWORD FROM Sam
```

用法

(返回顶部) (第 258 页)

根据 CHANGE PASSWORD 系统特权的最初授予方式，撤消 CHANGE PASSWORD 系统特权时使用 ADMIN OPTION FOR 子句将产生不同的结果。如果最初使用 WITH ADMIN OPTION 子句授予 CHANGE PASSWORD 系统特权，则在撤消语句中包含 ADMIN OPTION FOR 子句将仅撤消对 CHANGE PASSWORD 系统特权的管理权限（即，向其他用户授予系统特权）。实际管理其他用户口令的权限将会保留。但是，如果最初使用 WITH ADMIN ONLY OPTION 子句授予 CHANGE PASSWORD 系统特权，则在撤消语句中包含 ADMIN OPTION FOR 子句将在语义上等效于撤消全部 CHANGE PASSWORD 系统特权。最后，如果最初使用 WITH NO ADMIN OPTION 子句授予 CHANGE PASSWORD 系统特权，且 ADMIN OPTION FOR 子句包含在撤消语句中，那么将不会撤消任何权限，因为最初没有授予任何管理权限。

可从所授予的用户和角色的任意组合中撤消 CHANGE PASSWORD 系统特权。

标准

（返回顶部） （第 258 页）

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

（返回顶部） （第 258 页）

已授予 CHANGE PASSWORD 系统特权以及管理权限。

REVOKE CONNECT 语句

从数据库中删除用户。

快速链接：

转至参数 （第 260 页）

转至用法 （第 260 页）

转至标准 （第 260 页）

转至权限 （第 261 页）

语法

```
REVOKE CONNECT
    FROM userID [,...]
```

参数

（返回顶部） （第 260 页）

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

用法

（返回顶部） （第 260 页）

使用系统过程或 CREATE USER 和 DROP USER 语句（而非 **GRANT** 和 **REVOKE** 语句）可添加和删除用户 ID。

如果用户拥有数据库对象（例如表），则不能撤消该用户的连接特权。尝试使用 **REVOKE** 语句或者尝试使用 **sp_droplogin** 或 **sp_iqdroplogin** 存储过程来执行此操作将返回错误，如不能删除在运行时系统中拥有表的用户。

标准

（返回顶部） （第 260 页）

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 260 页）

需要 MANAGE ANY USER 系统特权。

注意： 如果正在撤消其他用户的 **CONNECT** 权限或表权限，则目标用户不能连接到数据库。

REVOKE CREATE 语句

删除指定用户 ID 对特定 dbspace 的 CREATE 特权。

快速链接：

转至参数 （第 261 页）

转至示例 （第 261 页）

转至标准 （第 261 页）

转至权限 （第 262 页）

语法

```
REVOKE CREATE ON dbspace-name
   FROM userID [,...]
```

参数

(返回顶部) （第 261 页）

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

示例

(返回顶部) （第 261 页）

- **示例 1** – 撤消用户 `Smith` 对 dbspace `DspHist` 的 CREATE 特权：

```
REVOKE CREATE ON DspHist FROM Smith
```

- **示例 2** – 从数据库中撤消用户 ID `fionat` 对 dbspace `DspHist` 的 CREATE 特权：

```
REVOKE CREATE ON DspHist FROM fionat
```

标准

(返回顶部) （第 261 页）

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 261 页）

需要 MANAGE ANY DBSPACE 系统特权。

REVOKE EXECUTE 语句

删除使用 **GRANT** 语句授予的 EXECUTE 权限。

快速链接：

转至参数 （第 262 页）

转至标准 （第 262 页）

转至权限 （第 262 页）

语法

```
REVOKE  EXECUTE ON [ owner.]procedure-name
    FROM userID [,...]
```

参数

(返回顶部) （第 262 页）

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

标准

(返回顶部) （第 262 页）

- SQL - 语法是持久存储模块特性。
- SAP Sybase 数据库产品 - Adaptive Server 支持语法。Adaptive Server 和 SAP Sybase IQ 的用户管理和安全模型不同。

权限

(返回顶部) （第 262 页）

需要以下特权之一：

- 拥有该过程，或者
- 具有 MANAGE ANY OBJECT PRIVILEGE 系统特权。

REVOKE 对象级特权语句

删除使用 **GRANT** 语句授予的对象级特权。

快速链接：

转至参数 （第 263 页）

转至示例 （第 264 页）

转至标准 （第 264 页）

转至权限 （第 264 页）

语法

```
REVOKE { object-level-privilege [,...]
    [ owner.]table-name
   FROM userID [,...]

object-level-privilege
    ALL [ PRIVILEGES ]
    | ALTER
    | DELETE
    | INSERT
    | LOAD
    | REFERENCE [ ( column-name [, ⋯] ) ]
    | SELECT [ ( column-name [, ⋯] ) ]
    | TRUNCATE
    | UPDATE [ ( column-name, ⋯) ] }
```

参数

(返回顶部) （第 262 页）

- **userID** – 必须是现有用户或不可变角色的名称。该列表必须包含具有登录口令的现有用户。列表中的 userID 用逗号分隔。
- **ALL** – 将所有特权授予用户
- **ALTER** – 用户可使用 **ALTER TABLE** 语句来变更此表。不允许对视图使用此特权。
- **DELETE** – 用户可从此表或视图中删除行。
- **INSERT** – 用户可向指定的表或视图插入行。
- **LOAD** – 用户可在指定的表或视图中装载数据。
- **REFERENCES** – 用户可在指定的表上创建索引，以及创建引用指定表的外键。如果指定了列名，则用户只能引用指定的这些列。列的 REFERENCES 特权不能授予视图，只能授予表。
- **SELECT** – 用户可查看此视图或表中的信息。如果指定了列名，则用户只能查看指定的这些列。列的 SELECT 权限不能授予视图，只能授予表。.
- **TRUNCATE** – 用户可截断指定的表或视图。

- **UPDATE** – 用户可更新此视图或表中的行。如果指定了列名，则用户只能更新指定的这些列。列的 UPDATE 特权不能授予视图，只能授予表。要更新表，用户必须对表拥有 SELECT 和 UPDATE 特权。

示例

(返回顶部) （第 262 页）

- **示例 1** – 阻止用户 Dave 向 Employees 表中插入数据：

```
REVOKE INSERT ON Employees FROM Dave
```

- **示例 2** – 阻止用户 Dave 更新 Employees 表：

```
REVOKE UPDATE ON Employees FROM Dave
```

标准

(返回顶部) （第 262 页）

- SQL - 语法是入门级特性。
- SAP Sybase 数据库产品 - Adaptive Server 中支持语法。

权限

(返回顶部) （第 262 页）

需要以下特权之一：

- 拥有该表，或者
- 拥有通过 GRANT OPTION 子句授予的 MANAGE ANY OBJECT PRIVILEGE 系统特权。

REVOKE ROLE 语句

删除用户的角色成员资格或用户管理该角色的能力。

快速链接：

转至参数 （第 265 页）

转至示例 （第 265 页）

转至标准 （第 266 页）

转至权限 （第 266 页）

语法

```
REVOKE [ ADMIN OPTION FOR ] ROLE role_name [,...]
    FROM grantee [,...]

role_name
```

```
dbo□□□
  | diagnostics□□□
  | PUBLIC□□□
  | rs_systabgroup□□□
  | SA_DEBUG□□□
  | SYS□□□
  | SYS_AUTH_SA_ROLE
  | SYS_AUTH_SSO_ROLE
  | SYS_AUTH_DBA_ROLE
  | SYS_AUTH_RESOURCE_ROLE
  | SYS_AUTH_BACKUP_ROLE
  | SYS_AUTH_VALIDATE_ROLE
  | SYS_AUTH_WRITEFILE_ROLE
  | SYS_AUTH_WRITEFILECLIENT_ROLE
  | SYS_AUTH_READFILE_ROLE
  | SYS_AUTH_READFILECLIENT_ROLE
  | SYS_AUTH_PROFILE_ROLE
  | SYS_AUTH_USER_ADMIN_ROLE
  | SYS_AUTH_SPACE_ADMIN_ROLE
  | SYS_AUTH_MULTIPLEX_ADMIN_ROLE
  | SYS_AUTH_OPERATOR_ROLE
  | SYS_AUTH_PERMS_ADMIN_ROLE
  | SYS_REPLICATE_ADMIN_ROLE□□□
  | SYS_RUN_REPLICATE_ROLE□□□
  | SYS_SPATIAL_ADMIN_ROLE□□□
  | user-defined role name
```

□□□系统角色不支持 ADMIN OPTION FOR 子句。

参数

(返回顶部) (第 264 页)

- **role_name** – 必须已存在于数据库中。用逗号分隔多个角色名。
- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。
- **ADMIN OPTION FOR** – 必须为每个 *userID* 授予对指定 *role_name* 的管理特权。

  注意： 此子句仅撤消角色的管理特权，而不是该角色的成员资格，除非最初使用 WITH ADMIN ONLY OPTION 子句授予此角色。对于使用 WITH ADMIN ONLY OPTION 子句授予的角色而言，ADMIN OPTION FOR 子句是可选的，这是因为其在语义上等效于完全撤消角色的成员资格。

示例

(返回顶部) (第 264 页)

- **示例 1** – 撤消 `User1` 的用户定义（独立）角色 `Role1`：

```
REVOKE ROLE Role1 FROM User1
```

执行此命令后，User1 将无权再使用向 Role1 授予的任何系统特权来执行任何已授权任务。

- **示例 2** – 撤消 User1 管理兼容性角色 SYS_AUTH_WRITEFILE_ROLE 的能力：

```
REVOKE ADMIN OPTION FOR ROLE SYS_AUTH_WRITEFILE_ROLE FROM User1
```

User1 保留执行 SYS_AUTH_WRITEFILE_ROLE 所授予的任何已授权任务的能力。

标准

(返回顶部) (第 264 页)

- SQL - 其它语法是 ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - Adaptive Server 中支持语法。

权限

(返回顶部) (第 264 页)

需要 MANAGE ROLES 系统特权才能撤消以下角色：

- diagnostics
- dbo
- PUBLIC
- rs_systabgroup
- SA_DEBUG
- SYS
- SYS_RUN_REPLICATE_ROLE
- SYS_SPATIAL_ADMIN_ROLE

需要对角色具有管理特权才能撤消以下角色：

- SYS_AUTH_SA_ROLE
- SYS_AUTH_SSO_ROLE
- SYS_AUTH_DBA_ROLE
- SYS_AUTH_RESOURCE_ROLE
- SYS_AUTH_BACKUP_ROLE
- SYS_AUTH_VALIDATE_ROLE
- SYS_AUTH_WRITEFILE_ROLE
- SYS_AUTH_WRITEFILECLIENT_ROLE
- SYS_AUTH_READFILE_ROLE
- SYS_AUTH_READFILECLIENT_ROLE
- SYS_AUTH_PROFILE_ROLE
- SYS_AUTH_USER_ADMIN_ROLE
- SYS_AUTH_SPACE_ADMIN_ROLE

- SYS_AUTH_MULTIPLEX_ADMIN_ROLE
- SYS_AUTH_OPERATOR_ROLE
- SYS_AUTH_PERMS_ADMIN_ROLE
- <用户定义的角色名称>

REVOKE SET USER 语句

删除某一用户模仿其他用户和管理 SET USER 系统特权的能力。

快速链接：

转至参数 （第 267 页）

转至示例 （第 267 页）

转至用法 （第 268 页）

转至标准 （第 268 页）

转至权限 （第 268 页）

语法

```
REVOKE [ ADMIN OPTION FOR ] SETUSER
   (target_user_list
      | ANY
      | ANY WITH ROLES target_role_list ])
 FROM userID [,...]
```

参数

(返回顶部) （第 267 页）

- **target_user_list** – 必须包含具有登录口令的现有用户，并且是被授予者用户不可再模仿的潜在目标用户列表。列表中的用户 ID 用逗号分隔。
- **ANY** – 每个被授予者的潜在目标用户的列表中均包含具有登录口令的所有数据库用户。
- **ANY WITH ROLES *target_role_list*** – *target_role_list* 必须包含现有角色，而每个被授予者的潜在目标用户列表必须包含具有登录口令的数据库用户，这些用户具有 *target_role_list* 中的角色子集。角色列表用逗号分隔。
- **userID** – 每个 *userID* 都必须是现有用户或不可变角色的名称。该列表必须包含具有登录口令的现有用户。列表中的 userID 用逗号分隔。

示例

(返回顶部) （第 267 页）

- **示例 1** – 阻止 `Bob` 模仿 `Sally` 或 `Bob`：

```
REVOKE SET USER (Sally, Bob) FROM Bob
```

- **示例 2** – 如果最初使用 WITH ADMIN OPTION 子句将 SET USER 系统特权授予 Sam，本示例将删除 Sam 向其他用户授予 SET USER 系统特权的能力，但仍允许 Sam 模仿已向其授予的那些用户。但是，如果最初使用 WITH ADMIN ONLY OPTION 子句将 SET USER 系统特权授予 Sam，本示例将删除 Sam 对系统特权拥有的所有权限。

```
REVOKE ADMIN OPTION FOR SET USER FROM Sam
```

用法

(返回顶部) （第 267 页）

根据 SET USER 系统特权的最初授予方式，撤消 SET USER 系统特权时使用 ADMIN OPTION FOR 子句将产生不同的结果。如果最初使用 WITH ADMIN OPTION 子句授予 SET USER 系统特权，则在撤消语句中包含 ADMIN OPTION FOR 子句将仅撤消对 SET USER 系统特权的管理能力（即，向其他用户授予系统特权）。实际模仿其他用户的能力将会保留。但是，如果最初使用 WITH ADMIN ONLY OPTION 子句授予 SET USER 系统特权，则在撤消语句中包含 ADMIN OPTION FOR 子句将在语义上等效于撤消全部 SET USER 系统特权。最后，如果最初使用 WITH NO ADMIN OPTION 子句授予 SET USER 系统特权，且 ADMIN OPTION FOR 子句包含在撤消语句中，那么将不会撤消任何权限，因为最初没有授予任何管理系统特权。

标准

(返回顶部) （第 267 页）

ANSI SQL – 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 267 页）

已授予 SET USER 系统特权以及管理权限。

REVOKE 系统特权语句

删除特定用户的特定系统特权以及管理特权的权限。

快速链接：

转至参数 （第 269 页）

转至示例 （第 269 页）

转至用法 （第 269 页）

转至标准 （第 270 页）

转至权限 （第 270 页）

语法

```
REVOKE [ ADMIN OPTION FOR ] system_privilege_name [,...]
   FROM userID [,...]
```

参数

(返回顶部) (第 268 页)

- **system_privilege_name** – 必须是现有系统特权。
- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。
- **ADMIN OPTION FOR** – 当前必须将每个 *system_privilege* 授予使用管理特权指定的每个 *userID*。

  注意: 此子句仅撤消系统特权的管理特权，仍授予系统特权本身。但是，如果最初使用 WITH ADMIN ONLY OPTION 子句来授予系统特权，则 ADMIN OPTION FOR 子句将完全撤消该系统特权。在这种情况下，不需要使用 ADMIN OPTION FOR 子句便可撤消管理特权。

示例

(返回顶部) (第 268 页)

- **示例 1** – 撤消用户 Jim 的 BACKUP DATABASE 系统特权：

  ```
  REVOKE BACKUP DATABASE FROM Jim
  ```

- **示例 2** – 假设最初使用 WITH ADMIN OPTION 子句将 BACKUP DATABASE 系统特权授予用户 Jim，本示例将撤消用户 Jim 管理 BACKUP DATABASE 系统特权的权限。将保留执行系统特权所授权的任务的权限。但是，如果最初使用 WITH ADMIN ONLY OPTION 子句将 BACKUP DATABASE 系统特权授予用户 Jim，本示例将删除用户 Jim 对系统特权拥有的所有权限。

  ```
  REVOKE ADMIN OPTION FOR BACKUP DATABASE FROM Jim
  ```

用法

(返回顶部) (第 268 页)

根据系统特权的最初授予方式，撤消系统特权时使用 ADMIN OPTION FOR 子句将产生不同的结果。如果最初使用 WITH ADMIN OPTION 子句授予系统特权，则在撤消语句中包含 ADMIN OPTION FOR 子句将仅撤消对系统特权的管理能力（即，向其他用户授予系统特权）。实际使用系统特权的能力将会保留。但是，如果最初使用 WITH ADMIN ONLY OPTION 子句授予系统特权，则在撤消语句中包含 ADMIN OPTION FOR 子句将在语义上等效于撤消全部系统特权。最后，如果最初使用 WITH NO ADMIN OPTION 子句授予系统特权，且 ADMIN OPTION FOR 子句包含在撤消语句中，那么将不会撤消任何权限，因为最初没有授予任何管理系统特权。

标准

(返回顶部) （第 268 页）

- SQL - 其它语法是 ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - Adaptive Server 不支持语法。

权限

(返回顶部) （第 268 页）

需要具备高于要撤消的系统特权的管理特权。

所有系统特权的列表

所有系统特权的列表。

系统特权用于控制用户执行授权数据库任务的权限。

下面列出了可用的系统特权：

- ACCESS SERVER LS
- ALTER ANY INDEX
- ALTER ANY MATERIALIZED VIEW
- ALTER ANY OBJECT
- ALTER ANY OBJECT OWNER
- ALTER ANY PROCEDURE
- ALTER ANY SEQUENCE
- ALTER ANY TABLE
- ALTER ANY TEXT CONFIGURATION
- ALTER ANY TRIGGER
- ALTER ANY VIEW
- ALTER DATABASE
- ALTER DATATYPE
- BACKUP DATABASE
- CHANGE PASSWORD
- CHECKPOINT
- COMMENT ANY OBJECT
- CREATE ANY INDEX
- CREATE ANY MATERIALIZED VIEW
- CREATE ANY OBJECT
- CREATE ANY PROCEDURE
- CREATE ANY SEQUENCE
- CREATE ANY TABLE
- CREATE ANY TEXT CONFIGURATION

- CREATE ANY TRIGGER
- CREATE ANY VIEW
- CREATE DATATYPE
- CREATE EXTERNAL REFERENCE
- CREATE MATERIALIZED VIEW
- CREATE MESSAGE
- CREATE PROCEDURE
- CREATE PROXY TABLE
- CREATE TABLE
- CREATE TEXT CONFIGURATION
- CREATE VIEW
- DEBUG ANY PROCEDURE
- DELETE ANY TABLE
- DROP ANY INDEX
- DROP ANY MATERIALIZED VIEW
- DROP ANY OBJECT
- DROP ANY PROCEDURE
- DROP ANY SEQUENCE
- DROP ANY TABLE
- DROP ANY TEXT CONFIGURATION
- DROP ANY VIEW
- DROP CONNECTION
- DROP DATATYPE
- DROP MESSAGE
- EXECUTE ANY PROCEDURE
- LOAD ANY TABLE
- INSERT ANY TABLE
- MANAGE ANY DBSPACE
- MANAGE ANY EVENT
- MANAGE ANY EXTERNAL ENVIRONMENT
- MANAGE ANY EXTERNAL OBJECT
- MANAGE ANY LDAP SERVER
- MANAGE ANY LOGIN POLICY
- MANAGE ANY MIRROR SERVER
- MANAGE ANY OBJECT PRIVILEGES
- MANAGE ANY SPATIAL OBJECT
- MANAGE ANY STATISTICS
- MANAGE ANY USER
- MANAGE ANY WEB SERVICE

- MANAGE AUDITING
- MANAGE MULTIPLEX
- MANAGE PROFILING
- MANAGE REPLICATION
- MANAGE ROLES
- MONITOR
- READ CLIENT FILE
- READ FILE
- REORGANIZE ANY OBJECT
- SELECT ANY TABLE
- SERVER OPERATOR
- SET ANY PUBLIC OPTION
- SET ANY SECURITY OPTION
- SET ANY SYSTEM OPTION
- SET ANY USER DEFINED OPTION
- SET USER（仅授予管理权限）
- TRUNCATE ANY TABLE
- UPDATE ANY TABLE
- UPGRADE ROLE
- USE ANY SEQUENCE
- VALIDATE ANY OBJECT
- WRITE CLIENT FILE
- WRITE FILE

REVOKE USAGE ON SEQUENCE 语句

删除指定序列的 USAGE 特权。

快速链接：

转至参数 （第 272 页）

转至标准 （第 273 页）

转至权限 （第 273 页）

语法

```
REVOKE  USAGE ON SEQUENCE sequence-name
    FROM userID [,...]
```

参数

（返回顶部） （第 272 页）

- **userID** – 必须是具有登录口令的现有用户或角色的名称。多个 userID 用逗号分隔。

标准

(返回顶部) (第 272 页)

- SQL - 语法是持久存储模块特性。
- SAP Sybase 数据库产品 - Adaptive Server 和 SAP Sybase IQ 中的安全模型不同，因此其它语法也不同。

权限

(返回顶部) (第 272 页)

需要以下特权之一：

- MANAGE ANY OBJECT PRIVILEGE 系统特权。
- 您拥有该序列。

SET OPTION 语句

更改影响数据库行为及数据库与 Transact-SQL 兼容性的选项。设置选项的值可更改所有用户或某个用户的行为，作用域可以是临时的，也可以是永久的。

快速链接：

转至参数 (第 273 页)

转至示例 (第 274 页)

转至用法 (第 274 页)

转至标准 (第 275 页)

转至权限 (第 275 页)

语法

```
SET [ EXISTING ] [ TEMPORARY ] OPTION
   ... [ userid. | PUBLIC.]option-name = [ option-value ]
```

参数

(返回顶部) (第 273 页)

- **option-value** – 主机变量（允许使用指示符）、字符串、标识符或数字。*option-value* 设置为字符串时，其最大长度为 127 个字节。

  如果忽略 *option-value*，将从数据库中删除指定的选项设置。如果它是个人选项设置，则所用的值会恢复为 PUBLIC 设置。

注意： 对于所有接受整数值的数据库选项，SAP Sybase IQ 会将任何小数形式的 *option-value* 设置截断为整数值。例如，值 3.8 将被截断为 3。

- **EXISTING** – 如果某选项没有 PUBLIC 用户 ID 设置，则无法为单个用户 ID 设置此选项的值。
- **TEMPORARY** – 更改选项更改有效性的持续时间。如果没有 TEMPORARY 子句，则对选项的更改将是永久性更改：在使用 **SET OPTION** 进行显式更改之前，它不会发生变化。

  如果使用单个用户 ID 应用 TEMPORARY 子句，则只要用户在数据库中处于登录状态，新选项值就会一直有效。

  如果通过 PUBLIC 用户 ID 使用 TEMPORARY 子句，则更改在数据库运行时间内将一直有效。当数据库关闭时，PUBLIC 用户 ID 的 TEMPORARY 选项恢复为其永久值。

  如果删除一个 TEMPORARY 选项，则选项设置会恢复为永久设置。

示例

(返回顶部) (第 273 页)

- **示例 1** – 设置 DATE_FORMAT 选项：

```
SET OPTION public.date_format = 'Mmm dd yyyy'
```

- **示例 2** – 将 WAIT_FOR_COMMIT 选项设置为 on：

```
SET OPTION wait_for_commit = 'on'
```

- **示例 3** – 嵌入式 SQL 示例：

```
EXEC SQL SET OPTION :user.:option_name = :value;
EXEC SQL SET TEMPORARY OPTION Date_format = 'mm/dd/yyyy';
```

用法

(返回顶部) (第 273 页)

选项的分类如下：

- 常规数据库选项
- Transact-SQL 兼容性数据库选项

指定用户 ID 或 PUBLIC 用户 ID 可确定该选项是为单个用户、为由 *userid* 表示的角色，还是为 PUBLIC 用户 ID（所有用户都属于该角色的成员）设置的。如果选项适用于角色 ID，则角色成员不会继承选项设置，即，仅将更改应用于角色 ID。如果未指定角色，则将所做选项更改应用于发出 **SET OPTION** 语句的当前登录用户 ID。例如，以下语句对 PUBLIC 用户 ID 应用选项更改：

```
SET OPTION Public.login_mode = standard
```

在嵌入式 SQL 中，只有数据库选项可以临时设置。

为 PUBLIC 用户 ID 更改选项的值，相当于为没有设置该值的任意用户设置此选项的值。如果某选项没有 PUBLIC 用户 ID 设置，则无法为单个用户 ID 设置此选项的值。

相对于永久性地设置选项的值，临时设置 PUBLIC 用户 ID 的选项更具安全优势。例如，在启用 **LOGIN_MODE** 选项时，数据库依赖于其所运行的系统的登录安全性。临时启用该选项意味着，对于依赖于 Windows 域的安全性的数据库，如果关闭该数据库并将它复制到本地计算机，它的安全不会受到威胁。在这种情况下，临时启用的 **LOGIN_MODE** 将恢复为它的永久值（可能是“标准”模式，这种模式不允许集成登录）。

警告！ 不支持从游标中读取行时更改选项设置，因为这会导致意外的行为。例如，在从游标中读取时更改 DATE_FORMAT 设置会在结果集的行中返回不同的日期格式。不要在读取行时更改选项设置。

标准

(返回顶部) （第 273 页）

- SQL - ISO/ANSI SQL 语法的服务商扩充。
- SAP Sybase 数据库产品 - 不受 Adaptive Server 支持。SAP Sybase IQ 支持一些使用 **SET** 语句的 Adaptive Server 选项。

权限

(返回顶部) （第 273 页）

设置自身的选项不需要特定系统特权。

必须具有 SET ANY PUBLIC OPTION 系统特权才能为其他用户设置数据库选项。

必须具有 SET ANY SYSTEM OPTION 系统特权才能为 PUBLIC 用户 ID 设置 SYSTEM 选项。

必须具有 SET ANY SECURITY OPTION 系统特权才能为 PUBLIC 用户 ID 设置 SECURITY 选项。

SETUSER 语句

允许用户临时采用其他用户的角色和系统特权（也称为模仿）来执行操作，前提是该用户已具有执行任务所需的最低特权。

注意： SET USER 系统特权是两个词；而 SETUSER 语句是一个词。

快速链接：

转至参数 （第 276 页）

转至用法 （第 276 页）

转至标准 （第 276 页）

转至权限 （第 276 页）

语法

SETUSER *userID*

参数

(返回顶部) （第 275 页）

- **UserID** – 必须是具有登录口令的现有用户或角色的名称。

用法

(返回顶部) （第 275 页）

必要条件验证在执行 SETUSER 语句时进行，而不是在授予 SET USER 系统特权时进行。

要终止成功的模仿，可发出 SETUSER 语句，而不指定 userID。

标准

(返回顶部) （第 275 页）

ANSI SQL – 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 275 页）

需要以下各项：

- 已授予模仿者模仿目标用户的权限。
- 模仿者至少具有目标用户被授予的所有角色和系统特权。
- 已授予模仿者具有类似或更高管理权限的角色和系统特权。

  注意： 为了满足管理权限条件，将认为 WITH ADMIN OPTION 和 WITH ADMIN ONLY OPTION 子句授予类似的管理权限。此外，还会认为这些子句授予的管理权限比 WITH NO ADMIN OPTION 子句授予的权限要高。例如，使用 WITH ADMIN OPTION 子句向 `User1` 授予 `Role1`，使用 WITH ADMIN ONLY 子句向 `User2` 授予 `Role1`，使用 WITH NO ADMIN OPTION 子句向 `User3` 授予 `Role1`。将授予 `User1` 和 `User2` 具有类似管理权限的 `Role1`。将授予 `User1` 和 `User2` 管理权限比 `User3` 高的 `Role1`。
- 如果已授予目标用户支持扩展的系统特权，则用于授予模仿者系统特权的子句是用于目标用户的子句的超集。 仅 SET USER 和 CHANGE PASSWORD 系统特权支持扩展。

- 将 ANY 子句视为 *target_roles_list* 和 *target_users_list* 子句的超集。如果已授予目标用户具有 ANY 授权的 SET USER 系统特权，则模仿者必须也具有 ANY 授权。
- 如果同时使用 *target_roles_list* 和 *target_users_list* 子句授予目标用户 SET USER 系统特权，则必须同时使用这两个子句授予模仿者系统特权，并且每个子句的目标列表必须与目标用户的相应子句授权列表相同，或是其列表的超集。例如，如果模仿者和目标用户的目标列表分别包含 `User1`、`User2` 及 `Role1`、`Role2`，则每个子句的目标列表授权将视为相同。或者，如果模仿者的目标列表授权分别包含 `User1`、`User2`、`Role1` 和 `Role2`，而目标用户的目标列表授权仅包含 `User1` 和 `Role2`，则认为模仿者的目标列表授权是目标用户列表的超集。
- 如果已使用单个目标列表子句授予目标用户 SET USER 系统特权，则模仿者的目标列表必须与目标用户的列表相同，或是其列表的超集。例如，模仿者和目标用户的 *target_user_list* 均包含 `User1` 和 `User2`（相同），或模仿者列表包含 `User1` 和 `User2`，而目标用户列表包含 `User2`，则 `User1`、`User2`（模仿者列表）是 `User2`（目标用户列表）的超集。
- 根据定义，用户可以始终模仿其自身。因此，如果授予目标用户模仿模仿者的权限，将不会违反模仿者的“必须相同或为超集”的条件要求。例如，`User3` 是模仿者，而 `User4` 是目标用户。`User3` 的 *target_user_list* 包含 `User4` 和 `User5`。`User4` 的 *target_user_list* 包含 `User3` 和 `User5`。如果从目标列表中删除该模仿者，则 `User3` 的目标列表满足条件要求。

VALIDATE LDAP SERVER 语句

先验证对现有 LDAP 服务器配置对象的设置更改，然后再应用这些更改。

快速链接：

转至参数 （第 278 页）

转至示例 （第 279 页）

转至用法 （第 279 页）

转至标准 （第 280 页）

转至权限 （第 280 页）

语法

```
VALIDATE LDAP SERVER [ ldapua-server-name | ldapua-server-attribs ]
   [ CHECK userid [ user-dn-string ] ]

ldapua-server-attribs
   SEARCH DN
            URL { 'URL_string' | NULL }
            | ACCESS ACCOUNT { 'DN_string' | NULL }
            | IDENTIFIED BY ( 'password' | NULL }
            | IDENTIFIED BY ENCRYPTED { encrypted-password | NULL }
```

```
   | AUTHENTICATION URL { 'URL_string' | NULL }
   | CONNECTION TIMEOUT timeout_value
   | CONNECTION RETRIES retry_value
   | TLS { ON | OFF }
```

参数

(返回顶部) (第 277 页)

- **ldapua-server-name** – 标识 LDAP 服务器配置对象。
- **URL** – 标识主机（按名称或按 IP 地址）、端口号以及为查寻给定用户 ID 的 DN 而执行的搜索。系统会先校验此值的 LDAP URL 语法是否正确，然后再将其存储在 ISYSLDAPSERVER 系统表中。此字符串的最大大小为 1024 个字节。
- **ACCESS ACCOUNT** – 在 LDAP 服务器上创建的供 SAP Sybase IQ 使用的用户，而不是 SAP Sybase IQ 中的用户。此用户的可分辨名称 (DN) 用于连接到 LDAP 服务器。此用户在 LDAP 服务器中具有一定权限，可按用户 ID 在 SEARCH DN URL 指定的位置搜索 DN。此字符串的最大大小为 1024 个字节。
- **IDENTIFIED BY** – 提供与 ACCESS ACCOUNT 用户关联的口令。该口令使用对称加密的形式存储在磁盘中。使用值 NULL 可清除该口令并将其设置为无。明文口令的最大大小为 255 个字节。
- **IDENTIFIED BY ENCRYPTED** – 以加密格式配置与 ACCESS ACCOUNT 可分辨名称相关联的口令。二进制值是加密口令并按原样存储在磁盘中。使用值 NULL 可清除该口令并将其设置为无。二进制值的最大大小为 289 个字节。
- **AUTHENTICATION URL** – 标识主机（按名称或 IP 地址）以及用于验证用户的 LDAP 服务器的端口号。这是为 <URL_string> 定义的值，系统会先校验此值的 LDAP URL 语法是否正确，然后再将其存储在 ISYSLDAPSERVER 系统表中。通过之前的 DN 搜索获取的用户的 DN 以及用户口令将新连接绑定到验证 URL。与 LDAP 服务器之间的成功连接将被视为连接用户的身份证明。此字符串的最大大小为 1024 个字节。
- **CONNECTION TIMEOUT** – 指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的连接超时。该值以毫秒为单位，缺省值为 10 秒。
- **CONNECTION RETRIES** – 指定从 SAP Sybase IQ 连接到 LDAP 服务器以进行 DN 搜索和验证的重试次数。值的有效范围为 1 - 60，缺省值为 3。
- **TLS** – 定义使用 TLS 协议还是安全 LDAP 协议连接到 LDAP 服务器以进行 DN 搜索和验证。该参数设置为 ON 时使用 TLS 协议，URL 以 "ldap://" 开头。设置为 OFF（或未指定）时使用安全 LDAP 协议，URL 以 "ldaps://" 开头。使用 TLS 协议时，通过包含（签署 LDAP 服务器所用证书的）证书颁发机构 (CA) 证书的文件名指定数据库安全选项 TRUSTED_CERTIFICATES_FILE。
- **CHECK userID** – 在 LDAP 服务器上验证存在性的 userID。

- **user-dn-string** – 将用户的 DN 值与用户 ID 进行比较以进行验证。

示例

(返回顶部) (第 277 页)

- **示例 1** – 假定 apps_primary LDAP 服务器配置对象按如下方式创建而成：

```
SET OPTION PUBLIC.login_mode = 'Standard,LDAPUA'
CREATE LDAP SERVER apps_primary
SEARCH DN
    URL 'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
WITH ACTIVATE
```

  此语句使用可选 CHECK 子句在 apps_primary LDAP 服务器配置对象上比较 userID 和预期用户可分辨名称（扩在引号内），从而验证是否存在 userID myusername。

```
VALIDATE LDAP SERVER apps_primary
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

- **示例 2** – 包含搜索属性时，不必在 **VALIDATE LDAP SERVER** 语句中定义 LDAP 服务器配置对象的名称：

```
VALIDATE LDAP SERVER
SEARCH DN
   URL  'ldap://my_LDAPserver:389/dc=MyCompany,dc=com??sub?cn=*'
    ACCESS ACCOUNT 'cn=aseadmin, cn=Users, dc=mycompany, dc=com'
    IDENTIFIED BY 'Secret99Password'
AUTHENTICATION URL 'ldap://my_LDAPserver:389/'
CONNECTION TIMEOUT 3000
CHECK myusername 'cn=myusername,cn=Users,dc=mycompany,dc=com'
```

用法

(返回顶部) (第 277 页)

此语句特别适合管理员将新服务器设置为使用 LDAP 用户验证以及诊断 LDAP 服务器配置对象与外部 LDAP 服务器之间是否存在问题。**VALIDATE LDAP SERVER** 语句进行的所有连接均为临时连接，并在语句结束时关闭。

按名称校验 LDAP 服务器配置对象时，将使用先前 **CREATE LDAP SERVER** 和 **ALTER LDAP SERVER** 语句中的定义。另外，在指定 *ldapua-server-attributes*（而非 LDAP 服务器配置对象）时，将验证指定的属性。指定 *ldapua-server-attributes* 时，将分析 URL 以标识语法错误，检测到语法错误后，语句处理将停止。

无论使用 LDAP 服务器配置对象名称还是成功分析的一组 *ldapua-server-attributes*，系统都会尝试与外部 LDAP 服务器进行连接。如果指定 ACCESS ACCOUNT 参数和口

令，这些值将用于建立与 SEARCH DN URL 的连接。这包括 SEARCH DN URL、ACCESS ACCOUNT 和 ACCESS ACCOUNT 口令。

使用可选 CHECK 子句时，在搜索中使用 userID 来校验外部 LDAP 服务器中是否存在该用户。如果已知给定用户的预期 DN 值，则可指定此值，并将其与搜索结果进行比较以确定成功还是失败。

标准

(返回顶部) （第 277 页）

ANSI SQL - 遵从性级别：Transact-SQL 扩充。

权限

(返回顶部) （第 277 页）

需要 MANAGE ANY LDAP SERVER 系统特权。

数据库选项

数据库选项可以自定义并修改数据库行为。

LOGIN_MODE 选项

控制对数据库的集成登录的使用。

允许值

- Standard - 缺省设置，不允许集成登录。如果尝试集成登录连接，则会发生错误。
- Mixed - 允许集成登录和标准登录。
- Integrated - 必须使用集成登录执行所有数据库登录操作。
- Kerberos - 必须使用 Kerberos 登录执行所有数据库登录操作。
- LDPAUA - 必须使用 LDAP 登录执行所有数据库登录操作。

注意： Mixed 等效于 "Standard,Integrated"。

默认值
标准

范围
只能在数据库 (PUBLIC) 级别设置选项。

必须具有 SET ANY SECURITY OPTION 系统特权才能设置此选项。设置立即生效。

注释
值不区分大小写：

警告！

- 在混合环境中将 **LOGIN_MODE** 限制为单一模式（例如，仅 Integrated 或仅 LDAPUA），相当于仅允许已被授予相关登录映射的用户进行连接。尝试使用其它方法连接会产生错误。只有具备全部管理权限的用户（SYS_AUTH_DBA_ROLE 或 SYS_AUTH_SSO_ROLE）不受此限制。
- 将 **LOGIN_MODE** 限制为仅 LDAPUA 可能会导致以下配置：当不存在允许 LDAPUA 的用户或登录策略时，所有用户将都无法连接到服务器。使用命令行开关 **-al** *user-id-list* 和 **start_iq** 实用程序可以从该情况中恢复。

MIN_ROLE_ADMINS 选项

为所有角色配置所需的最小管理员数。

允许值
1 – 10

缺省值
1

范围
只能在数据库 (PUBLIC) 级别设置选项。

必须具有 SET ANY SECURITY OPTION 系统特权才能设置此选项。设置立即生效。

注释
该选项为所有角色设置所需的最小管理员数。该值是指每个角色的最小角色管理员数，而不是所有角色的最小角色管理员数。当删除角色或用户时，该值可确保避免这样一种情况，即剩余的用户或角色都不具有足够的系统特权来管理其余用户和角色。

TRUSTED_CERTIFICATES_FILE 选项

指定通过 LDAP 用户验证建立的出站传送层安全性 (TLS) 连接、INC 连接以及 MIPC 连接的信任关系。

允许值
一个有效网络路径，指向列有用于签署服务器证书的受信任证书颁发机构的 TXT 文件的位置。

缺省值
NULL，表示无法启动任何出站 TLS 连接，因为没有受信任证书颁发机构。

范围
只能在数据库 (PUBLIC) 级别设置选项。

必须具有 SET ANY SECURITY OPTION 系统特权才能设置此选项。设置立即生效。

注释
此选项用于标识指向受信任证书颁发机构列表位置的路径。该列表必须存储在 TXT 文件中。该文件可以在本地驱动器上 Windows 环境下的某个位置共享，供该计算机上的所有 SAP Sybase 应用程序使用。

-al iqsrv16 服务器选项

将 LDAPUA LOGIN_MODE 仅扩展到选定数量的使用标准验证的用户

语法

```
-al "user1;user2;user3" server_name.cfg database-name.db
```

注释

- 最多可以指定五个用户 ID，以分号分隔并用双引号括起来。
- 在服务器级别运行时，**-al** 开关将一直有效，直到下次重新启动服务器。

-al iqsrv16 数据库选项

将 LDAPUA LOGIN_MODE 仅扩展到选定数量的使用标准验证的用户。

语法

```
-al "user1;user2;user3" server_name.cfg database_name.db
```

注释

- 最多可以指定五个用户 ID，以分号分隔并用双引号括起来。
- 在数据库级别运行时，此选项将一直有效，直到下次停止/启动数据库。

VERIFY_PASSWORD_FUNCTION 选项

指定可用于实现口令规则的用户提供的验证函数。

允许值
字符串

缺省值
"（空字符串）。（设置口令时不调用函数。）

范围
可在数据库 (PUBLIC) 或用户级别设置选项。在数据库级别进行设置时，值将变为任何新用户的缺省值，但不会对现有用户产生任何影响。在用户级别进行设置时，仅替换该用户的 PUBLIC 值。为自身设置选项无需任何系统特权。在数据库或用户级别为任何其他用户设置选项都需要系统特权。

必须具有 SET ANY SECURITY OPTION 系统特权才能设置此选项。可针对个别连接或 PUBLIC 角色进行临时设置。设置立即生效。

注释

当 **VERIFY_PASSWORD_FUNCTION** 选项值设置为有效字符串时，语句 **GRANT CONNECT TO** *userid* **IDENTIFIED BY** *password* 将调用该选项值所指定的函数。

该选项值需要使用 *owner.function_name* 格式，以防止用户覆盖该函数。

该函数具有两个参数：

- *user_name* VARCHAR(128)
- *new_pwd* VARCHAR(255)

返回值类型为 VARCHAR(255)。

如果设置了 **VERIFY_PASSWORD_FUNCTION**，则无法使用 **GRANT CONNECT** 语句指定多个用户 ID 和口令。

示例

以下示例代码定义表和函数并设置一些登录策略选项。它们共同实现了高级口令规则，其中包括要求在口令中使用某些类型的字符、不允许口令重用和为口令设置有效期。当创建用户 ID 或更改口令时，数据库服务器会通过 verify_password_function 选项调用函数。应用程序可以调用 post_login_procedure 选项指定的过程，以报告口令应在到期前进行更改。

```
-- only DBA should have privileges on this table
CREATE TABLE DBA.t_pwd_history(
        pk          INT         DEFAULT AUTOINCREMENT PRIMARY KEY,
        user_name   CHAR(128),  -- the user whose password is set
        pwd_hash    CHAR(32) ); -- hash of password value to detect
                                -- duplicate passwords

-- called whenever a non-NULL password is set
-- to verify the password conforms to password rules
CREATE FUNCTION DBA.f_verify_pwd( uid     VARCHAR(128),
                                  new_pwd VARCHAR(255) )
RETURNS VARCHAR(255)
BEGIN
    -- enforce password rules
    -- enforce minimum length (can also be done with
    -- min_password_length option)
    IF length( new_pwd ) < 6 THEN
        RETURN 'password must be at least 6 characters long';
    END IF;

    -- number of lowercase characters IN new_pwd
    SELECT count(*) INTO num_lower_chars
       FROM pwd_chars WHERE CAST( c AS BINARY ) BETWEEN 'a' AND 'z';

    -- enforce rules based on characters contained in new_pwd
    IF ( SELECT count(*) FROM pwd_chars WHERE c BETWEEN '0' AND '9' )
           < 1 THEN
        RETURN 'password must contain at least one numeric digit';
    ELSEIF length( pwd_alpha_only ) < 2 THEN
```

```
        RETURN 'password must contain at least two letters';
    ELSEIF num_lower_chars = 0
           OR length( pwd_alpha_only ) - num_lower_chars = 0 THEN
        RETURN 'password must contain both upper- and lowercase
characters';
    END IF;

    -- not the same as any user name
    -- (this could be modified to check against a disallowed words
table)
    IF EXISTS( SELECT * FROM SYS.SYSUSER
                    WHERE lower( user_name ) IN
( lower( pwd_alpha_only ),
                                              lower( new_pwd ) ) ) THEN
       RETURN 'password or only alphabetic characters in password '
||
               'must not match any user name';
    END IF;

    -- not the same as any previous password for this user
    IF EXISTS( SELECT * FROM t_pwd_history
                    WHERE user_name = uid
                   AND pwd_hash = hash( uid || new_pwd, 'md5' ) ) THEN
        RETURN 'previous passwords cannot be reused';
    END IF;

    -- save the new password
    INSERT INTO t_pwd_history( user_name, pwd_hash )
        VALUES( uid, hash( uid || new_pwd, 'md5' ) );

    RETURN( NULL );
END;

ALTER FUNCTION DBA.f_verify_pwd SET HIDDEN;
GRANT EXECUTE ON DBA.f_verify_pwd TO PUBLIC;
SET OPTION PUBLIC.verify_password_function = 'DBA.f_verify_pwd';


-- All passwords expire in 180 days. Expired passwords can be changed
-- by the user using the NewPassword connection parameter.
ALTER LOGIN POLICY DEFAULT password_life_time = 180;

-- If an application calls the procedure specified by the
-- post_login_procedure option, then the procedure can be used to
-- warn the user that their password is about to expire. In
particular,
-- Interactive SQL calls the post_login_procedure.
ALTER LOGIN POLICY DEFAULT password_grace_time = 30;
```

要关闭该选项，请将其设置为空字符串：

```
SET OPTION PUBLIC.VERIFY_PASSWORD_FUNCTION = ''
```

MIN_PASSWORD_LENGTH 选项

设置数据库中新口令的最小长度。

允许值
大于或等于零的整数

值以字节为单位。对于单字节字符集，它与字符数相等。

默认值
3 个字符

范围
只能在数据库 (PUBLIC) 级别设置选项。

必须具有 SET ANY SECURITY OPTION 系统特权才能设置此选项。设置立即生效。

注释
此选项对所有新口令强制使用一个最小长度，以实现更高的安全性。现有口令不受影响。

示例
将新口令的最小长度设置为 6 个字节：

```
SET OPTION PUBLIC.MIN_PASSWORD_LENGTH = 6
```

-gk iqsrv16 数据库服务器选项

设置停止数据库服务器所需的特权。

语法

```
iqsrv16 -gk { DBA | all | none } ...
```

允许值

- **DBA** – 只有具有 SERVER OPERATOR 系统特权的用户才能停止数据库服务器。这是网络服务器的缺省设置。
- **all** – 关闭数据库服务器不需要任何特权。
- **none** – 数据库服务器无法停止。

适用于
所有操作系统和数据库服务器。

注释
-gd 数据库服务器选项应用于 dbstop 实用程序以及以下语句：

- ALTER DATABASE *dbname* FORCE START 语句。
- STOP DATABASE 语句

-gl iqsrv16 服务器选项

设置使用 **LOAD TABLE** 装载数据时所需的权限。

语法

-gl level

Remarks

LOAD TABLE 语句用于从数据库服务器计算机中读取文件。要控制使用这些语句对文件系统进行访问，可使用 **-gl** 命令行开关来控制这些语句所需的数据库权限级别。*level* 是：

- DBA – 只有具有 LOAD ANY TABLE、ALTER ANY TABLE 或 ALTER ANY OBJECT 系统特权的用户才能装载数据。
- ALL – 所有用户都可以装载数据。
- NONE – 无法装载数据。

可以对这些选项使用大写和小写语法。

对于使用 **start_iq** 启动的服务器，缺省设置为 **all**；对于其它服务器，缺省设置为 **dba**。为了与早期版本保持一致，请在所有系统中使用 **all** 值。在 `iqdemo.cfg` 和 `default.cfg` 配置文件中使用 **all** 设置。

-gu iqsrv16 数据库服务器选项

设置执行数据库文件管理语句（例如用于创建或删除数据库）所需的特权。

语法

```
iqsrv16 -gu { all | none | DBA | utility_db } ...
```

允许值

-gu 选项	效果	适用于
`all`	*不建议使用此选项。*任何用户都能够执行文件管理语句。	任何数据库（包括实用程序数据库）
`none`	不允许执行文件管理语句。	任何数据库（包括实用程序数据库）
`DBA`	只有具有 SERVER OPERATOR 系统特权的用户才能执行文件管理语句	任何数据库（包括实用程序数据库）
`utility_db`	只有能够连接到实用程序数据库的用户才能执行文件管理语句	仅限实用程序数据库

缺省值
DBA

适用于
所有操作系统和数据库服务器。

注释
限制可执行以下数据库文件管理语句的用户：

- ALTER DATABASE dbfile ALTER TRANSACTION LOG
- CREATE DATABASE 语句
- CREATE DECRYPTED DATABASE 语句
- CREATE DECRYPTED FILE 语句
- CREATE ENCRYPTED DATABASE 语句
- CREATE ENCRYPTED FILE 语句
- DROP DATABASE 语句
- RESTORE DATABASE 语句。

如果指定 utility_db，则只能从实用程序运行这些语句。如果指定 DBA，则只能由具有 SERVER OPERATOR 系统特权的用户运行这些语句。如果未指定上述两项，则所有用户均无法执行这些语句。

示例

要防止文件管理语句被使用，请使用 -gu 选项的 none 特权级别启动数据库服务器。以下命令启动一个数据库服务器并将其命名为 TestSrv。它装载 `mytestdb.db` 数据库，但禁止任何用户使用该服务器来创建或删除数据库或者执行任何其它文件管理语句，而不管用户是否具有资源创建权限或者能否装载实用程序数据库并连接到该数据库。

```
iqsrv16 -n TestSrv -gu none c:\mytestdb.db
```

要只允许知道实用程序数据库口令的用户执行文件管理语句，通过运行以下命令启动服务器。

```
iqsrv16 -n TestSrv -su secret -gu utility_db
```

以下命令将 Interactive SQL 作为客户端应用程序启动，连接到名为 TestSrv 的服务器、装载实用程序数据库并连接到用户。

```
dbisql -c
"UID=DBA;PWD=secret;DBN=utility_db;Host=host1;Server=TestSrv"
```

在成功执行上述命令之后，用户连接到该实用程序数据库，并能执行文件管理语句。

-sk iqsrv16 数据库服务器选项

指定可用于允许对数据库服务器中受保护的功能进行访问的系统安全功能密钥。

语法

```
iqsrv16 -sk key ...
```

适用于
所有操作系统和数据库服务器。

注释
在使用 -sf 选项确保数据库服务器功能的安全时，也可同时使用 -sk 选项，以指定可与 sp_use_secure_feature_key 系统过程一起使用的密钥，从而允许访问连接的安全功能。连接也可使用 sa_server_option 系统过程以修改对于运行于数据库服务器上的所有数据库而言均受到保护的功能或功能集。

密钥必须为非空字符串，至少长六个字符，而且不能包含双引号、控制字符（任何小于 0x20 的字符）或反斜线。每个数据库的安全功能密钥不能超过 1000 个。

将 sp_use_secure_feature_key 系统过程的 authorization_key 参数值设置为任何不同于 -sk 所指定的值时，将不会给出任何错误，由 -sf 指定的功能对该连接而言仍受到保护。

如果仅指定 -sk 而未指定 -sf，则只会启用缺省的安全功能，但您可在数据库服务器运行时使用系统安全功能密钥以更改安全功能设置。

示例

以下命令将启动一个名为 secure_server 的数据库服务器，并保护备份功能。可随后使用由 -sk 选项指定的密钥以允许访问特定连接的上述功能。

```
iqsrv16 -n secure_server -sf backup -sk j978kls12
```

对于与运行于 secure_server 数据库服务器上的数据库的连接而言，将 authorization_key 参数设置为由 -sk 指定的值将允许该连接执行备份或更改在 secure_server 数据库服务器上受保护的功能：

```
CALL sp_use_secure_feature_key ( 'MyKey' , 'j978kls12' );
```

然后，用户即可执行以下语句，以保护 secure_server 上所运行的数据库的所有功能：

```
CALL sa_server_option( 'SecureFeatures', 'all' );
```

-sf iqsrv16 数据库服务器选项

控制用户是否能够访问当前数据库服务器上所运行的数据库的功能。只有具有相应特权的用户才能访问受保护的功能，所有用户均可访问未受保护的功能。

语法

```
iqsrv16 -sf feature-list ...
```

```
feature-list :
feature-name | feature-set [ ,feature-name | feature-set ] ...
```

Feature set	Included features (feature sets in bold)
none	All features are unsecured except manage_features, manage_keys, and disk_sandbox.
manage_server	processor_affinity
manage_security	manage_features manage_keys manage_disk_sandbox
server_security	disk_sandbox trace_system_event

Feature set	Included features (feature sets in bold)
all	**client** – read_client_file write_client_file **remote** – remote_data_access send_udp send_email web_service_client **local** – • **local_call** – cmdshell external_procedure java • **local_db** – backup restore database dbspace • **local_env** – getenv • **local_io** – create_trace_file read_file write_file directory sp_list_directory sp_create_directory sp_copy_directory sp_move_directory sp_delete_directory sp_copy_file sp_move_file

Feature set	Included features (feature sets in bold)
	sp_delete_file • **local_log** – request_log console_log webclient_log

参数

- **none** – 指定未保护任何功能。
- **manage_server** – 禁止用户访问所有与数据库服务器相关的功能。该功能集由以下功能组成：
  - **processor_affinity** – 禁止用户更改数据库服务器的处理器相似性（所使用的逻辑处理器的数量）。
- **manage_security** – 禁止用户访问用于管理数据库服务器安全的功能。缺省情况下，这些功能是受保护的。
  - **manage_features** – 禁止用户修改可在数据库服务器上受保护的功能的列表。
  - **manage_keys** – 禁止创建、修改、删除或列出安全功能密钥。

    能访问 manage_keys 功能但不能访问 manage_features 功能的用户只能使用为其指派的安全功能来定义密钥。
  - **manage_disk_sandbox** – 禁止用户使用 sa_server_option 系统过程或 sa_db_option 系统过程临时更改磁盘沙箱设置。不能为所有数据库或用户关闭 manage_disk_sandbox 安全功能—只能使用 sp_use_secure_feature_key 系统过程为各个连接关闭此安全功能。
- **server_security** – 禁止用户访问可临时跳过安全设置的功能。缺省情况下，这些功能是受保护的。
  - **disk_sandbox** – 禁止用户在位于主数据库文件所在目录之外的数据库上执行读写文件操作。
  - **trace_system_event** – 禁止用户创建用户定义的跟踪事件。
- **all** – 禁止用户访问以下组：
  - **client** – 禁止用户访问所有允许访问客户端相关输入和输出的功能。此功能控制对客户端计算环境的访问。该功能集由以下功能组成：
    - **read_client_file** – 禁止使用能够读取客户端文件的语句。例如，READ_CLIENT_FILE 函数和 LOAD TABLE 语句。
    - **write_client_file** – 禁止使用能够写入客户端文件的所有语句。例如，UNLOAD 语句和 WRITE_CLIENT_FILE 函数。

- **remote** – 禁止用户访问所有允许远程访问或与远程进程通信的功能。该功能集由以下功能组成：
  - **remote_data_access** – 禁止使用任何远程数据访问服务，例如代理表。
  - **send_udp** – 禁止使用 sa_send_udp 系统过程向指定地址发送 UDP 包的功能。
  - **send_email** – 禁止使用电子邮件系统过程，例如 xp_sendmail。
  - **web_service_client** – 禁止使用 Web 服务客户端存储过程调用（发出 HTTP 请求的存储过程）。
- **local** – 禁止用户访问所有本地相关功能。此功能控制对服务器计算环境的访问。该功能集由 `local_call`、`local_db`、`local_io` 和 `local_log` 功能子集组成。
  - **local_call** – 禁止用户访问所有能够执行不直接属于数据库服务器且不受该数据库服务器控制的代码的功能。该功能集由以下功能组成：
    - **cmdshell** – 禁止使用 xp_cmdshell 过程。
    - **external_procedure** – 禁止使用外部存储过程。此设置不会禁用内置于数据库服务器中的 xp_* 系统过程（例如 xp_cmdshell、xp_readfile 等）。为这些系统过程提供了单独的功能控制选项。
    - **external_procedure_v3** – 请参阅《用户定义函数》指南。
    - **java** – 禁止使用 Java 相关的功能，例如，Java 过程。
  - **local_db** – 禁止用户访问所有与数据库文件相关的功能。该功能集由以下功能组成：
    - **backup** – 禁止使用 BACKUP 语句，从而禁止使用执行服务器端备份的功能。您仍可使用 dbbackup 实用程序执行客户端备份。
    - **restore** – 禁止使用 RESTORE DATABASE 语句。
    - **database** – 禁止使用 CREATE DATABASE、ALTER DATABASE、DROP DATABASE、CREATE ENCRYPTED FILE、CREATE DECRYPTED FILE、CREATE ENCRYPTED DATABASE 和 CREATE DECRYPTED DATABASE 语句。
    - **dbspace** – 禁止使用 CREATE DBSPACE、ALTER DBSPACE 和 DROP DBSPACE 语句。
  - **local_env** – 禁止用户访问所有与环境变量相关的功能。该功能集由以下功能组成：
    - **getenv** – 禁止用户读取任何环境变量值。
  - **local_io** – 禁止用户访问所有允许直接访问文件及其内容的功能。该功能集由以下功能组成：
    - **create_trace_file** – 禁止使用可创建事件跟踪目标的语句。

- **read_file** – 禁止使用能够读取本地文件的语句。例如，xp_read_file 系统过程、LOAD TABLE 语句以及 OPENSTRING(FILE...) 的使用。). 不建议使用替代名 load_table 和 xp_read_file。
- **write_file** – 禁止使用能够写入本地文件的所有语句。例如，UNLOAD 语句和 xp_write_file 系统过程。不建议使用替代名 unload_table 和 xp_write_file。
- **delete_file** – 禁止使用能够删除本地文件的所有语句。例如，如果指定 -x 或 -xo 选项，则保护此功能将导致 dbbackup 实用程序运行失败。
- **directory** – 禁止使用目录类代理表。该功能在禁用 remote_data_access 时将被禁用。
- **sp_list_directory** – 禁止使用 sp_list_directory 系统过程。
- **sp_create_directory** – 禁止使用 sp_create_directory 系统过程。
- **sp_copy_directory** – 禁止使用 sp_copy_directory 系统过程。
- **sp_move_directory** – 禁止使用 sp_move_directory 系统过程。
- **sp_delete_directory** – 禁止使用 sp_delete_directory 系统过程。
- **sp_copy_file** – 禁止使用 sp_copy_file 系统过程。
- **sp_move_file** – 禁止使用 sp_move_file 系统过程。
- **sp_delete_file** – 禁止使用 sp_delete_file 系统过程。

- **local_log** – 禁止用户访问所有导致创建或直接向磁盘上某个文件写入数据的记录功能。该功能集由以下功能组成：
  - **request_log** – 禁止使用更改请求日志文件名的功能，同时禁止使用增加请求日志文件大小或文件数量限制的功能。可在启动数据库服务器的命令中指定请求日志文件以及对此文件的限制；但在数据库服务器启动之后将无法进行更改。禁用请求日志功能时，仍可打开和关闭请求记录功能，并可减少请求记录文件的最大文件大小和数量。
  - **console_log** – 禁止使用 sa_server_option 系统过程的 ConsoleLogFile 选项更改数据库服务器消息日志文件名的功能。保护此功能同时将禁止使用 sa_server_option 系统过程的 ConsoleLogMaxSize 选项增加日志文件最大大小的功能。可在启动数据库服务器时指定服务器日志文件及其大小。
  - **webclient_log** – 禁止使用 sa_server_option 系统过程的 WebClientLogFile 选项更改 Web 服务客户端日志文件名的功能。可在启动数据库服务器时指定 Web 服务客户端日志文件。

适用于
所有操作系统和数据库服务器。

注释
此选项允许数据库服务器所有者控制用户是否能够访问数据库服务器上所运行数据库的功能。-sk 选项允许数据库服务器的所有者创建一个系统安全功能密钥，此系统安全功能密钥可禁止用户访问由 -sf 选项指定的功能。

如果在启动数据库时没有指定系统安全功能密钥，则缺省的安全功能将受到保护，所以您无法对数据库服务器或其上运行的任何数据库的安全功能设置进行更改。您无法

在稍后创建系统安全功能密钥—必须关闭数据库服务器，并在重新启动时指定系统安全功能密钥。

feature-list 是针对数据库服务器的、要加以保护的功能名称或功能集逗号分隔列表。如果对某一功能进行保护，则除管理员之外的所有数据库用户将无法访问该功能。如果指定某一功能集，则该功能集中包含的所有功能均将受到保护。要对功能集中的一个或多个功能进行保护，但并不保护所有功能，请指定各个功能的名称。

注意： 在缺省情况下受到保护的功能集中，其子功能所受的保护无法通过命令行取消。也就是说，以下命令无效：

```
-sf manage_security, -manage_keys
```

使用 *feature-name* 指示功能应受到保护（无法访问），使用 *–feature-name* 或 *feature-name–* 指示应取消对功能的保护（所有数据库用户均可访问）。例如，以下命令指示只有 dbspace 功能可供所有用户访问：

```
iqsrv16 -n secure_server -sf all,-dbspace
```

示例

以下命令启动一个名为 secure_server 的数据库服务器，启动时将保护对请求日志的访问权限，并保护所有远程数据访问功能。由 -sk 选项指定的密钥稍后可与 sp_use_secure_feature_key 系统过程一起使用，从而使这些功能可供当前连接上的所有用户访问。

```
iqsrv16 -n secure_server -sf remote,-request_log -sk j978kls12
```

如果连接到 secure_server 数据库服务器上所运行的数据库的用户使用 sp_use_secure_feature_key 系统过程，并将 authorization_key 参数设置为由 -sk 指定的值，则该连接能够访问远程数据访问功能：

```
CALL sp_use_secure_feature_key ( 'MyKey' , 'j978kls12' );
```

以下命令将保护所有功能，但本地数据库功能除外：

```
iqsrv16 -n secure_server -sf all,-local_db
```

过程和函数

在 SAP Sybase IQ 数据库中使用系统提供的存储函数和过程来检索系统信息。

sa_get_ldapserver_status 系统过程

确定 LDAP 服务器配置对象的当前状态。

语法

sa_get_ldapserver_status()

特权
您必须具有系统过程的 EXECUTE 特权。

注释

列名	数据类型	说明
ldsrv_id	UNSIGNED BIGINT	LDAP 服务器配置对象的唯一标识符，同时也是主键，由登录策略用来引用 LDAP 服务器。
ldsrv_name	CHAR(128)	指派给 LDAP 服务器配置对象的名称。
ldsrv_state	CHAR(9)	LDAP 服务器的只读状态： 1 – RESET 2 – READY 3 – ACTIVE 4 – FAILED 5 – SUSPENDED 数字值存储在系统表中；相应的文本值在系统视图中显示。
ldsrv_last_ state_change	TIMESTAMP	表示上一次更改状态的时间。无论 LDAP 服务器的本地时区是多少，该值都以协调通用时间 (UTC) 形式存储。

在执行检查点操作并且内存中的内容写入磁盘目录之前，查看 SYSLDAPSERVER 列的值。在对 LDAP 服务器对象执行检查点操作期间，因存在导致 LDAP 服务器对象状态发生更改的事件（如由于访问 LDAP 目录服务器失败而导致连接失败），目录列 ldsrv_state 和 ldsrv_last_state_change 的更新以异步方式执行。LDAP 服务器对象的状态反映了 LDAP 目录服务器的状态。

sa_get_user_status 系统过程

用于确定用户的当前状态。

语法

```
sa_get_user_status( )
```

结果集

列名	数据类型	说明
user_id	UNSIGNED INTEGER	标识用户的唯一编号。

列名	数据类型	说明
user_name	CHAR(128)	用户的名称。
connections	INTEGER	该用户当前建立的连接数。
failed_logins	UNSIGNED INTEGER	用户进行的登录失败重试次数。
last_login_time	TIMESTAMP	用户上次登录时的本地时间。
locked	TINYINT	指示用户帐户是否锁定。
reason_locked	LONG VARCHAR	帐户被锁定的原因。
user_dn	CHAR(1024)	正在连接到 LDAP 服务器的用户 ID 的可分辨名称（Distinguished Name，简称 DN）。
user_dn_cached_at	TIMESTAMP	存储 DN 时的本地时间。
password_change_state	BIT	用于指示是否正在对双重口令进行更改的值（0 = 否，1 = 是）。缺省值为 0。
password_change_first_user	UNSIGNED INTEGER	如果用户设置了双重口令的第一部分，则为该用户的 user_id；否则为 NULL。
password_change_second_user	UNSIGNED INTEGER	如果用户设置了双重口令的第二部分，则为该用户的 user_id；否则为 NULL。
user_dn	CHAR(1024)	用户的可分辨名称 (DN)。
user_dn_cached_at	TIMESTAMP	找到可分辨名称时的日期和时间。

注释
此过程返回一个显示用户当前状态的结果集。除了基本用户信息外，该过程还包括两列，分别指示用户是否被锁定以及锁定原因。用户可能由于以下几种原因而被锁定：由于策略、口令到期或失败重试次数过多而被锁定。

如果使用 LDAP 用户验证对用户进行验证，则输出将包括该用户的可分辨名称以及该可分辨名称被找到之时的日期和时间。

特权
您可以查看有关您自己的信息，不需要任何特权。要查看有关其他用户的信息，则必须具有 MANAGE ANY USER 系统特权。

副作用
无

示例

以下示例使用 sa_get_user_status 系统过程返回数据库用户的状态。

```
CALL sa_get_user_status;
```

sp_create_secure_feature_key 系统过程

创建新的安全功能密钥。

语法

```
sp_create_secure_feature_key （
    name,
    auth_key,
    features )
```

参数

- **name** – 新安全功能密钥的 VARCHAR (128) 名称。此参数不能为 NULL 或空字符串。
- **auth_key** – 安全功能密钥的 CHAR (128) 验证密钥。验证密钥必须为至少六个字符的非空字符串。
- **features** – 安全功能的 LONG VARCHAR 列表，以逗号分隔，可由新密钥启用。在功能之前指定 "-" 表示该功能在设置安全功能密钥时不重新启用。

特权

您必须具有系统过程的 EXECUTE 特权。此外，您必须是数据库服务器的所有者，并且已为连接启用 manage_keys 功能。

注释

此过程创建的新安全功能密钥可授予任何用户。系统安全功能密钥使用 -sk 数据库服务器选项进行创建。

sp_displayroles 系统过程

显示授予用户定义角色或用户的所有角色，或显示整个角色层次树。

语法

```
sp_displayroles (
   [ user_role_name ],
   [ display_mode ],
   [ grant_type ] )
```

参数

- **user_role_name** – 有效值包括：
  - 有效的系统特权名称或系统特权角色名称

  - 有效的用户定义角色名称
  - 有效的用户名

  在缺省情况下，如果未指定参数，则使用当前登录用户。
- **display_mode** – 有效值包括：
  - **EXPAND_UP** – 显示授予输入角色或系统特权的所有角色；即父级的角色层次树。
  - **EXPAND_DOWN** – 显示授予输入角色或用户的所有角色或系统特权；即子级的角色层次树。

  如果未指定参数（缺省值），则仅显示直接授予的角色或系统特权。
- **grant_type** – 有效值包括：
  - **ALL** – 显示授予的所有角色或系统特权。
  - **NO_ADMIN** – 显示使用 WITH NO ADMIN OPTION 或 WITH ADMIN OPTION 子句授予的所有角色或系统特权。
  - **ADMIN** – 显示使用 WITH ADMIN OPTION 或 WITH ADMIN ONLY OPTION 子句授予的所有角色或系统特权。

  如果未指定参数，则使用 **“ALL”**。

特权
您必须具有系统过程的 EXECUTE 特权。要对其他用户执行此过程，您必须具有 MANAGE ROLES 系统特权。要对角色或系统特权执行此过程，您必须是角色管理员或对系统特权具有管理权限。

注释

列名	数据类型	说明
role_name	char(128)	列出角色/系统特权名称。
parent_role_name	char(128)	列出父项的角色名称。
grant_type	char(10)	列出授予类型。
role_level	smallint	对于 `Expand_down` 模式，1 表示直接授予的角色，2 表示其下面的下一个层次级别，依此类推。对于 `Expand_up` 模式，0 表示为指定角色授予的角色，-1 表示其上面的下一个层次级别，依此类推。

使用系统特权名称作为名称时，其结果将显示系统特权名称而不是系统特权角色名称。

使用 Expand_down 模式时，级别 1（直接授予的角色）的 parent_role_name 为 NULL。如果未指定模式（缺省设置），则 role_level 为 1，parent_role_name 为 NULL，因为只显示直接授予的角色。

如果使用用户名作为名称，且模式为 expand_up，则不返回任何结果，因为用户位于任意角色层次中的顶级。同样，如果使用不可变系统特权名称作为名称，且模式为 expand_down，也不会返回任何结果，因为不可变系统特权位于任意角色层次中的底层。

使用缺省模式时，parent_role_name 列为 NULL 且 role_level 为 1。

示例

该示例假设已执行下面的 GRANT 语句：

```
GRANT SERVER OPERATOR TO r4;
GRANT BACKUP DATABASE TO r3 WITH ADMIN OPTION;
GRANT DROP CONNECTION TO r3 WITH ADMIN ONLY OPTION;
GRANT MONITOR TO r2;GRANT CHECKPOINT TO r1;
GRANT ROLE r2 TO r1 WITH ADMIN OPTION;
GRANT ROLE r3 TO r2 WITH NO ADMIN OPTION;
GRANT ROLE r4 TO r3 WITH ADMIN ONLY OPTION;
GRANT ROLE r1 TO user1;
GRANT ROLE r1 TO r7;
GRANT ROLE r7 TO user2 WITH ADMIN OPTION;
GRANT BACKUP DATABASE TO user2 WITH ADMIN ONLY OPTION;
```

`sp_displayroles( 'user2', 'expand_down', 'ALL' )` 产生的输出如下所示：

role_name	parent_role_name	grant_type	role_level
r7	NULL	ADMIN	1
PUBLIC	NULL	NO ADMIN	1
BACKUP DATABASE	NULL	ADMIN ONLY	1
dbo	PUBLIC	NO ADMIN	2
r1	r7	NO ADMIN	2
r2	r1	ADMIN	3
CHECKPOINT	r1	NO ADMIN	3
r3	r2	NO ADMIN	4
MONITOR	r2	NO ADMIN	4
r4	r3	ADMIN ONLY	5
BACKUP DATABASE	r3	ADMIN	5
DROP CONNECTION	r3	ADMIN ONLY	5

`sp_displayroles( 'user2', 'expand_down', 'NO_ADMIN' )` 产生的输出如下所示：

role_name	parent_role_name	grant_type	role_level
r7	NULL	ADMIN	1
PUBLIC	NULL	NO ADMIN	1
dbo	PUBLIC	NO ADMIN	2
r1	r7	NO ADMIN	2
r2	r1	ADMIN	3
CHECKPOINT	r1	NO ADMIN	3
r3	r2	NO ADMIN	4
MONITOR	r2	NO ADMIN	4
BACKUP DATABASE	r3	ADMIN	5

`sp_displayroles( 'r3', 'expand_up', 'NO_ADMIN' )` 产生的输出如下所示：

role_name	parent_role_name	grant_type	role_level
r1	r7	NO ADMIN	-2
r2	r1	ADMIN	-1
r3	r2	NO ADMIN	0

`sp_displayroles( 'r1', 'NO_ADMIN', 'expand_up')` 产生的输出如下所示：

role_name	parent_role_name	grant_type	role_level
r1	r7	NO ADMIN	0

sp_expireallpasswords 系统过程

让所有用户口令立即到期。

语法 1

```
call sp_expireallpasswords
```

语法 2

```
sp_expireallpasswords
```

特权

您必须具有系统过程的 EXECUTE 特权，以及 MANAGE ANY USER 系统特权。

SP_HAS_ROLE 函数 [系统]

返回一个整数值，表示是为调用用户授予了指定系统特权还是用户定义的角色。当用于对用户定义的存储过程执行特权检查时，**SP_HAS_ROLE** 会在用户特权检查失败时返回一条错误消息。

语法

dbo.sp_has_role(*[rolename], [grant_type], [throw_error]*)

参数

参数	描述
rolename	系统特权或用户定义角色的名称。
grant_type	有效值包括：ADMIN 和 NO ADMIN。如果为 NULL 或未指定，则缺省使用 NO ADMIN。
throw_error	有效值包括： • **“1”** – 如果没有为调用用户授予指定系统特权或用户定义角色，则显示错误消息。 • **“0”** –（缺省值）如果没有为调用用户授予指定系统特权或用户定义角色，将不显示错误消息。

返回值

值	描述
1	已为调用用户授予系统特权或用户定义角色。
0 或权限被拒绝：您没有执行此命令/过程的权限。	没有为调用用户授予系统特权或用户定义角色。`throw_error` 参数设置为 1 时，将返回错误消息以代替值 0。
-1	指定的系统特权或用户定义角色不存在。即使 `throw_error` 参数设置为 1，也不显示任何错误消息。

注释

如果 `grant_type` 参数的值为 ADMIN，该函数将检查调用用户是否具有系统特权的管理特权。如果 `grant_type` 参数的值为 NO ADMIN，该函数将检查调用用户是否具有对系统特权或角色的使用特权。

如果未指定 `grant_type` 参数，则缺省使用 NO ADMIN，且输出仅指示是为调用用户授予（直接或间接）了指定的系统特权还是用户定义角色。

如果 rolename 和 grant_type 参数都为 NULL，且 throw_error 参数为 1，则显示错误消息。对于从目录表读取特定值而不是检查是否存在调用用户的系统特权之后出现错误消息的存储过程来说，此功能非常有用。

注意： 如果参数 rolename 和 grant_type 设置为 NULL 且 throw_error 设置为 1，或三个参数全部设置为 NULL，则返回权限被拒绝的错误消息。

示例
假定以下情形：

- 已使用 WITH NO ADMIN OPTION 子句授予 u1 CREATE ANY PROCEDURE 系统特权。
- 已授予 u1 CREATE ANY TABLE 系统特权。
- 已使用 WITH ADMIN ONLY OPTION 子句授予 u1 用户定义角色 Role_A。
- Role_B 存在，但未被授予 u1
- 角色 Role_C 不存在。

基于以上情形，以下命令

- `sp_has_role 'create any procedure'`

  返回值 1，表示已授予 u1 CREATE ANY PROCEDURE 系统特权。
- `sp_has_role 'create any table'`

  返回值 0，表示未授予 u1 CREATE ANY TABLE 系统特权。未返回错误消息，因为未指定 throw_error 参数。
- `sp_has_role 'create any procedure','admin',1`

  返回 Permission denied 错误消息 (throw_error=1)。即使已授予 u1 CREATE ANY PROCEDURE 系统特权，但未授予 u1 对系统特权的管理权限。
- `sp_has_role 'Role_A'`

  返回值 1，表示已授予 u1 角色 Role_A。
- `sp_has_role 'Role_A','admin',1`

  返回值 1，表示已授予 u1 具有管理权限的角色 Role_A。
- `sp_has_role 'Role_B'`

  返回值 0，表示未授予 u1 角色 ROLE_B。未返回错误消息，因为未指定 throw_error 参数。
- `sp_has_role 'Role_C'`

  返回值 -1，表示角色 ROLE_C 不存在。
- `sp_has_role 'Role_C',NULL,1`

  返回值 -1，表示角色 ROLE_C 不存在。

sp_iqaddlogin 过程

向指定的登录策略添加一个新的 SAP Sybase IQ 用户帐户。

语法 1

```
call sp_iqaddlogin ( 'username_in', 'pwd',
[ 'password_expiry_on_next_login' ] [ , 'policy_name' ] )
```

语法 2

```
sp_iqaddlogin 'username_in', 'pwd',
[ 'password_expiry_on_next_login' ] [ , 'policy_name' ]
```

语法 3

```
sp_iqaddlogin username_in, pwd, [ password_expiry_on_next_login ] [ ,
policy_name ]
```

参数

- **username_in** – 用户的登录名。登录名必须符合标识符的规则。
- **pwd** – 用户的口令。口令必须符合口令规则，即它们必须是有效标识符。
- **password_expiry_on_next_login** – （可选）指定是否在创建用户登录后该用户的口令立即到期。缺省设置为 OFF（口令不到期）。
- **policy_name** – （可选）按照命名登录策略创建用户。如果未指定，则按照根登录策略创建用户。

使用 **sp_iqaddlogin** 创建、并设置为一天后到期的 *username_in/pwd* 第二天全天有效，随后一天无效。换言之，今天创建并设置为 *n* 天后到期的登录在日期变为第 *(n+1)* 天时将不再可用。

特权
您必须具有系统过程的 EXECUTE 特权，以及 MANAGE ANY USER 系统特权。

注释
添加新的 SAP Sybase IQ 用户帐户，为该用户分配登录策略，并将该用户添加到 ISYSUSER 系统表中。如果此用户已经拥有针对数据库的用户 ID，但不在 `ISYSUSER` 中（例如，如果是使用 **GRANT CONNECT** 语句或 SAP Control Center 添加的），则 **sp_iqaddlogin** 会将该用户添加到此表中。

如果在调用过程时未指定登录策略名，SAP Sybase IQ 会为用户分配根登录策略。

注意： 如果登录策略的最大登录数没有限制，则属于该登录策略的用户可以有无限数目的连接。

第一次用户登录将强制更改口令，并为新创建的用户分配登录策略。使用 **CREATE USER** 创建新用户，但为了能够向后兼容，仍支持 **sp_iqaddlogin**。

示例
以下调用将按照 expired_password 登录策略添加用户 rose，口令为 irk324。本示例假设 expired_password 登录策略已存在。

```
call sp_iqaddlogin('rose', 'irk324', 'ON', 'expired_password')
```

```
sp_iqaddlogin 'rose','irk324', 'ON', 'expired_password'
```

sp_iqbackupdetails 过程

显示特定备份中包括的所有 dbfile。

语法

```
sp_iqbackupdetails  backup_id
```

参数

- **backup_id** – 指定备份操作的事务标识符。

注意： 通过执行以下查询可获得 SYSIQBACKUPHISTORY 表中的 backup_id 值：

```
select * from sysiqbackuphistory
```

特权
您必须具有系统过程的 EXECUTE 特权。

注释
sp_iqbackupdetails 返回：

表 15. sp_iqbackupdetails 列

列名	描述
backup_id	备份事务的标识符。
backup_time	备份的时间。
backup_type	备份的类型："full"、"Incremental since incremental" 或 "Incremental since full"。
selective_type	备份的子类型："All inclusive"、"All RW files in RW dbspaces"、"Set of RO dbspace/file"。
depends_on_id	备份所依赖的上次备份的标识符。
dbspace_id	正在备份的 dbspace 的标识符。

列名	描述
dbspace_name	如果 dbspace 名与给定 dbspace_id 的 SYSDBSPACE 中的 dbspace 名相匹配，则为 SYSIQBACKUPHISTORYDETAIL 的 dbspace 名。否则为 "null"。
dbspace_rwstatus	"ReadWrite" 或 "Read Only"。
dbspace_createid	Dbspace 创建的事务标识符。
dbspace_alterid	变更 DBSPACE 读写模式的事务标识符。
dbspace_online	状态 "Online" 或 "Offline"。
dbspace_size	备份时 dbspace 的大小 (KB)。
dbspace_backup_size	在 dbspace 中备份的数据的大小 (KB)。
dbfile_id	要备份的 dbfile 的标识符。
dbfile_name	如果备份操作后未重命名，则为逻辑文件名。如果重命名，则为 "null"。
dbfile_rwstatus	"ReadWrite" 或 "Read Only"。
dbfile_createid	Dbfile 创建的事务标识符。
dbfile_alterid	变更 FILE 读写模式的变更 DBSPACE 的事务标识符。
dbfile_size in MB	dbfile 的大小 (MB)。
dbfile_backup_size	dbfile 备份的大小 (KB)。
dbfile_path	SYSBACKUPDETAIL 的 dbfile 路径，如果路径与给定 dbspace_id 和 dbfile_id 的 SYSDBFILE 中的物理文件路径 ("file_name") 相匹配，则为 SYSBACKUPDETAIL 的 dbfile 路径。否则为 "null"。

示例

sp_iqbackupdetails 的输出样本：

```
backup_id   backup_time              backup_type   selective_type   d
epends_on_id
      883   2008-09-23 13:58:49.0   Full          All
inclusive                0

dbspace_id   dbspace_name   dbspace_rwstatus   dbspace_createid
         0   system         ReadWrite                         0

dbspace_alterid   dbspace_online dbspace_size dbspace_backup_size
dbfile_id
              0              0        2884              2884        0

dbfile_name dbfile_rwstatus dbfile_createid dbfile_alterid
```

```
dbfile_size
     system        ReadWrite                0              0       2884
```

```
dbfile_backup_size dbfile_path
              2884  C:\\Documents and Settings\\All Users\\SybaseIQ\
\demo\\iqdemo.db
```

sp_iqbackupsummary 过程

总结执行的备份操作。

语法

```
sp_iqbackupsummary [ timestamp or backup_id ]
```

参数

- **timestamp 或 backup_id** – 指定报告备份操作的间隔。如果指定时间戳或备份 ID，则只返回 backup_time 大于或等于输入时间的那些记录。如果不指定时间戳，该过程返回 ISYSIQBACKUPHISTORY 中的所有备份记录。

特权

您必须具有系统过程的 EXECUTE 特权。

注释

表 16. sp_iqbackupsummary 列

列名	描述
backup_id	备份事务的标识符
backup_time	备份的时间
backup_type	备份的类型：“Full”、“Incremental since incremental”或“Incremental since full”
selective_type	备份的子类型："All Inclusive"、"All RW files in RW dbspaces"、"Set of RO dbspace/file"
virtual_type	虚拟备份的类型：“Non-virtual”、“Decoupled”或“Encapsulated”
depends_on_id	备份所依赖的备份的标识符
creator	备份的创建者
backup_size	备份的大小 (KB)
user_comment	用户注释
backup_command	发出的备份语句（减去注释）

示例

sp_iqbackupsummary 的输出样本：

```
backup_id   backup_time             backup_type   selective_type   v
irtual_type
     883   2008-09-23 13:58:49.0   Full          All inclusive    Non
virtual

depends_on_id   creator   backup_size   user_comment   backup_command
           0   DBA              10864              backup database to
                                                          'c:\\\\temp
\\\\b1'
```

sp_iqconnection 过程

显示有关连接和版本的信息，包括哪些用户正在使用临时 dbspace、哪些用户正在使版本保持活动状态、连接在 SAP Sybase IQ 内部执行哪些操作、连接状态、数据库版本状态，等等。

语法

sp_iqconnection [*connhandle*]

适用于

Simplex 和 Multiplex。

特权

您必须具有系统过程的 EXECUTE 特权。 必须具有以下一种系统特权：

- DROP CONNECTION
- MONITOR
- SERVER OPERATOR

注释

connhandle 相当于 `Number` 连接属性，是连接的 ID 编号。**connection_property** 系统函数返回连接 ID：

```
SELECT connection_property ( 'Number' )
```

当使用有效的 *connhandle* 的输入参数进行调用时，**sp_iqconnection** 仅对该连接返回一行。

sp_iqconnection 为每个活动连接都返回一行。列 ConnHandle、Name、Userid、LastReqTime、ReqType、CommLink、NodeAddr 和 LastIdle 分别是连接属性 Number、Name、Userid、LastReqTime、ReqType、CommLink、NodeAddr 和 LastIdle，并返回与系统函数 **sa_conn_info** 相同的值。其它列返回来自 SAP Sybase IQ 引擎的 SAP Sybase IQ 端的连接数据。各行按 ConnCreateTime 排序。

MPXServerName 列存储与节点间通信 (INC) 有关的信息，如下所示：

运行服务器	MPXServerName 列内容
Simplex 服务器	NULL（所有连接均为本地/用户连接）
Multiplex 协调器	• NULL 用于本地/用户连接。 • 包含每个 INC 连接（根据需要或专用活动连接）的辅助节点服务器名称（连接源）。
Multiplex 辅助服务器	• NULL 用于本地/用户连接。 • 包含协调器服务器名的值（连接源）。

在 Java 应用程序中，请在 "RemotePWD" 字段中指定来自 TDS 客户端的特定于 SAP Sybase IQ 的连接属性。以下示例显示如何指定 IQ 特定连接参数，其中的 **myconnection** 为 IQ 连接名：

```
p.put("RemotePWD",",,CON=myconnection");
```

列名	描述
ConnHandle	连接的 ID 号。
名称	服务器的名称。
Userid	连接的用户 ID。
LastReqTime	指定连接的上次请求开始的时间。
ReqType	表示上次请求类型的字符串。
IQCmdType	在 SAP Sybase IQ 端执行的当前命令（如果有）。该命令类型反映在引擎的实现级别定义的命令。这些命令由事务命令、用于处理 IQ 存储库中的数据的 DDL 和 DML 命令、内部 IQ 游标命令和特殊控制命令（如 **OPEN** 和 **CLOSE**、**BACKUP DATABASE**、**RESTORE DATABASE**）以及其它命令组成。
LastIQCmdTime	此连接上最后一个 IQ 命令在 SAP Sybase IQ 引擎 IQ 端上的启动或完成时间。
IQCursors	此连接上在 IQ 存储库中打开的游标数。
LowestIQCursorState	IQ 游标状态（如果有）。如果连接上存在多个游标，则显示的状态是所有游标中位置最靠下游标的状态，即距离完成时间最远的那个游标的状态。游标状态反映 SAP Sybase IQ 内部实现的详细信息，并可能在未来发生更改。对于此版本，游标状态包括：NONE、INITIALIZED、PARSED、DESCRIBED、COSTED、PREPARED、EXECUTED、FETCHING、END_OF_DATA、CLOSED 和 COMPLETED。就像名称所暗示的那样，游标状态在操作结束时发生更改。例如，PREPARED 状态指示游标正在执行。

列名	描述
IQthreads	当前分配给连接的 SAP Sybase IQ 线程数。某些线程可能已分配，但仍处于空闲状态。此列可以帮助您确定哪些连接使用了最多的资源。
TxnID	连接上当前事务的事务 ID。该事务 ID 与 `.iqmsg` 文件中 BeginTxn、CmtTxn 和 PostCmtTxn 消息显示的事务 ID 以及打开数据库时所记录的 Txn ID Seq 相同。
ConnCreateTime	连接的创建时间。
TempTableSpaceKB	此连接在处理 IQ 临时表中存储的数据时所用的 IQ 临时存储空间的字节数 (KB)。
TempWorkSpaceKB	此连接在处理诸如排序、散列和临时位图时所用的 IQ 临时存储空间的字节数 (KB)。由位图或由属于 SAP Sybase IQ 临时表索引一部分的其它对象所使用的空间将反映在 TempTableSpaceKB 中。
IQConnID	作为 `.iqmsg` 文件中所有消息的一部分显示的十位连接 ID。它是一个单调递增整数，在整个服务器会话内唯一。
satoiq_count	内部计数器，用于显示从 SAP Sybase IQ 引擎的 SQL Anywhere 端到 IQ 端的相交数。这在确定连接活动时有可能会用到。结果集将在行缓冲区中返回，但不会每行都增加一次 satoiq_count 或 iqtosa_count。
iqtosa_count	内部计数器，用于显示从 SAP Sybase IQ 引擎的 IQ 端到 SQL Anywhere 端的相交数。这在确定连接活动时有可能会用到。
CommLink	连接的通信链接。这是 SAP Sybase IQ 所支持的网络协议之一，如果为相同计算机连接，则为 local。
NodeAddr	客户端/服务器连接中客户端的节点。
LastIdle	请求间隔时间数。
MPXServerName	如果是 INC 连接，则 varchar(128) 值包含发起 INC 连接的 Multiplex 服务器的名称。如果不是 INC 连接，则为 NULL。
LSName	连接的逻辑服务器名。如果逻辑服务器上下文未知或不适用，则为 NULL。
INCConnName	某个用户连接的基础 INC 连接的名称。此列的数据类型为 varchar(255)。如果 **sp_iqconnection** 显示某个已挂起用户连接的 INC 连接名，则该用户连接将有一个同样挂起的关联 INC 连接。
INCConnSuspended	此列中的 "Y" 值表示某个用户连接的基础 INC 连接处于挂起状态。"N" 值则表示该连接未挂起。

示例

sp_iqconnection

```
ConnHandle      Name    Userid                 LastReqTime   ReqType
=== ================== ======  =========================   =======
 1  'SQL_DBC_100525210' 'DBA'   '2011-03-28  09:29:24.466'  'OPEN'


           IQCmdType    LastIQCmdTime      IQCursors  LowestIQCursorState
====================    ==============     =========  ===================
'IQUTILITYOPENCURSOR'  2011-03-28 09:29:24.0       0             'NONE'


IQthreads   TxnID          ConnCreateTime TempTableSpaceKB TempWorkSpaceKB
=========  =======  =====================  =============== ===============
        0  3352568  2011-03-28 09:29:20.0                0           0


IQconnID satoiq_count iqtosa_count CommLink NodeAdd LastIdle MPXServerName
======== ============ ============ ======== ======= ======== ============
      34           43           2  'local'      ''      244  (NULL)

LSName      INCConnName                  INCConnSuspended
==========  ===================          ================
Finance_LS  'IQ_MPX_SERVER_P54'          'Y'
```

sp_iqcopyloginpolicy 过程

通过复制现有登录策略创建新的登录策略。

语法 1

```
call sp_iqcopyloginpolicy ( 'existing-policy-name', 'new-policy-name' )
```

语法 2

```
sp_iqcopyloginpolicy 'existing-policy-name', 'new-policy-name'
```

参数

- **existing-policy-name** – 要复制的登录策略。
- **new-policy-name** – 要创建的新登录策略的名称 (CHAR(128))。

特权

您必须具有系统过程的 EXECUTE 特权，以及 MANAGE ANY LOGIN POLICY 系统特权。

示例

从现有登录策略 *root* 中复制登录策略选项值，新建一个登录策略 *lockeduser*:

```
call sp_iqcopyloginpolicy ('root','lockeduser')
```

sp_iqdbspace 过程

显示每个 SAP Sybase IQ dbspace 的详细信息。

语法

```
sp_iqdbspace [ dbspace-name ]
```

适用于
Simplex 和 Multiplex。

特权
您必须具有系统过程的 EXECUTE 特权，以及 MANAGE ANY DBSPACE 系统特权。

注释
利用 **sp_iqdbspace** 中的信息确定是否必须移动数据，以及对于已移动的数据是否已释放旧版本。

列名	描述
DBSpaceName	在 **CREATE DBSPACE** 语句中指定的 dbspace 的名称。无论是指定 **CREATE DATABASE...CASE IGNORE** 还是指定 **CASE RESPECT**，Dbspace 名称始终不区分大小写。
DBSpaceType	dbspace 的类型（MAIN、SHARED_TEMP、TEMPORARY、RLV 或 CACHE）。
Writable	T（可写）或 F（不可写）。
Online	T（联机）或 F（脱机）。
Usage	所有文件当前使用的 dbspace 占整个 dbspace 的百分比。
TotalSize	dbspace 中所有文件的总大小，以 B（字节）、K（千字节）、M（兆字节）、G（千兆字节）、T（千吉字节）或 P（千万亿字节）为单位。
Reserve	dbspace 中可以添加到所有文件的保留空间总大小。
NumFiles	dbspace 中的文件数。
NumRWFiles	dbspace 中的读/写文件数。
Stripingon	F（关闭）。
StripeSize	如果磁盘条带化已开启，则始终为 1。
BlkTypes	用户数据和内部系统结构占用的空间。
OkToDrop	"Y" 表示可删除 dbspace；否则为 "N"。

BlkTypes 块类型标识符的值：

标识符	块类型
A	活动版本
B	备份结构

标识符	块类型
C	检查点日志
D	数据库标识
F	空闲列表
G	全局空闲列表管理器
H	空闲列表的头块
I	索引建议存储
M	Multiplex CM*
O	旧版本
R	RLV 空闲列表管理器
T	表使用
U	索引使用
N	列使用
X	在检查点处删除

*Multiplex 提交标识块（实际 128 块）存在于所有 IQ 数据库中，即使 Simplex 数据库不使用它也不例外。

示例
显示有关 dbspace 的信息：

```
sp_iqdbspace;
```

注意： 以下示例显示 `iqdemo` 数据库中的对象，以便更好地阐释输出。`iqdemo` 包括一个名为 `iq_main` 的示例用户 dbspace，您自己的数据库中可能不包括此 dbspace。

DBSpaceName	DBSpaceType	Writable
IQ_MAIN	MAIN	T
IQ__ SYSTEM_ MAIN	MAIN	T
IQ_SYSTEM_ TEMP	TEMPORARY	T
myDas	CACHE	T

（继续）Online	Usage	DBSpaceName
T	55	IQ_MAIN
T	21	IQ__ SYSTEM_ MAIN
T	1	IQ_SYSTEM_ TEMP
T	1	myDas

（继续）Reserve	NumFiles	NumRWFiles
200M	1	1
50M	1	1
50M	1	1
0B	5	5

（继续）DBSpaceName	Stripingon	Stripe Size
IQ_MAIN	T	1K
IQ__ SYSTEM_ MAIN	F	8K
IQ_SYSTEM_ TEMP	F	8K
myDas	T	1K

（继续）Blk Types	OkTo Drop
1H，5169A，190	N
1H，7648F，32D，128M	N
1H，64F，32A	N
5，192FH	Y

sp_iqdbspaceinfo 过程

显示在指定表中使用的每个对象和子对象的大小。这不受 RLV dbspace 支持。

语法

```
sp_iqdbspaceinfo [ dbspace-name ] [ , owner_name ] [ ,
object_name ] [ , object-type  ]
```

参数
所有参数均为可选参数，并且任何参数的提供均不受其它参数值的影响。

- **dbspace_name** – 如果已指定，则 **sp_iqdbspaceinfo** 会为指定 dbspace 中具备组件的每个表显示一行。否则，该过程显示数据库中所有 dbspace 的信息。
- **owner_name** – 对象的所有者。如果指定，**sp_iqdbspaceinfo** 将仅显示包含指定所有者的那些表的输出。如果未指定，**sp_iqdbspaceinfo** 显示数据库中所有用户的表的相关信息。
- **object_name** – 表的名称。如果未指定，**sp_iqdbspaceinfo** 显示数据库中所有表的相关信息。
- **object_type** – 有效的 **table** 对象。

sp_iqdbspaceinfo 存储过程支持用于解释 *dbspace_name*、*object_name* 和 *owner_name* 的通配符。它以 **LIKE** 子句匹配查询内部模式的方式显示匹配指定模式的所有 dbspace 的信息。

适用于
Simplex 和 Multiplex。

特权
您必须具有系统过程的 EXECUTE 特权。 必须具有以下一种系统特权：

- BACKUP DATABASE
- SERVER OPERATOR
- MANAGE ANY DBSPACE

注释
如果指定 RLV dbspace，该过程将不返回任何结果。

sp_iqdbspaceinfo 向 DBA 显示各个 dbspace 中驻留的对象所占用的空间大小。DBA 可利用这些信息确定必须先重新定位哪些对象，然后才能删除 dbspace。子对象列以整数后跟后缀 B、K、M、G、T 或 P（分别表示字节、千字节、兆字节、千兆字节、千吉字节和千万亿字节）的形式显示报告的大小。

对于表，**sp_iqdbspaceinfo** 显示所有子对象的大小信息（以整数加上后缀 B、K、M、G、T 或 P 的形式表示），按 *dbspace_name*、*object_name* 和 *owner_name* 排序。

表 17. sp_iqdbspaceinfo 列

列名	描述
dbspace_name	dbspace 的名称。
object_type	对象的类型（仅限于 **table** 或 **joinindex**）
owner	对象所有者的名称。
object_name	dbspace 中对象的名称。
object_id	对象的全局对象 ID。
id	对象的表 ID。
columns	给定 dbspace 上的列存储空间大小。
indexes	给定 dbspace 上的索引存储空间大小。不要使用系统生成的索引（例如，唯一约束中的 HG 索引或 FP 索引）。
metadata	给定 dbspace 上元数据对象的存储空间大小。
primary_key	给定 dbspace 上主键相关对象的存储空间大小。
unique_constraint	给定 dbspace 上唯一约束相关对象的存储空间大小。
foreign_key	给定 dbspace 上外键相关对象的存储空间大小。
dbspace_online	表示 dbspace 是处于联机状态 (**Y**) 还是脱机状态 (**N**)。

如果对使用 -r 开关（只读）启动的服务器运行 sp_iqdbspaceinfo，将显示错误 `Msg 13768, Level 14, State 0: SQL Anywhere Error -757: Modifications not permitted for read-only database`。此行为是预期行为。其它存储过程（如 `sp_iqdbspace`、`sp_iqfile`、`sp_iqdbspaceobjectinfo` 或 `sp_iqobjectinfo`）则不会发生此错误。

示例

注意： 以下示例显示 `iqdemo` 数据库中的对象，以便更好地阐释输出。`iqdemo` 包括一个名为 `iq_main` 的示例用户 dbspace，您自己的数据库中可能不包括此 dbspace。

显示数据库所有 dbspace 内的所有表中的所有对象和子对象的大小：

```
sp_iqdbspaceinfo
```

```
dbspace_name    object_type  owner   object_name     object_id  id
  columns
iq_main         table        DBA     emp1            3689     741   96K
iq_main         table        DBA     iq_dummy        3686     740   24K
iq_main         table        DBA     sale            3698     742   96K
iq_main          table         GROUPO  Contacts          3538     732
```

```
   288K
iq_main         table        GROUPO  Customers         3515     731
   240K
iq_main        table       GROUPO  Departments      3632    738   72K
iq_main         table        GROUPO  Employees         3641     739
   408K
iq_main         table        GROUPO  FinancialCodes    3612     736
   72K
iq_main        table       GROUPO  FinancialData    3621    737   96K
iq_main         table        GROUPO  Products
 3593     735   272K
iq_main         table        GROUPO  SalesOrderItems   3580     734
   120K
iq_main         table        GROUPO  SalesOrders       3565     733
   144K

indexes  metadata  primary_key  unique_constraint  foreign_key  dbsp
ace_online
0B       1.37M     0B           0B                 0B           Y
0B       464K      0B           0B                 0B           Y
0B       1.22M     0B           0B                 0B           Y
0B       5.45M     24K          0B                 48K          Y
48K      4.63M     24K          0B                 0B           Y
0B       1.78M     24K          0B                 48K          Y
0B       8.03M     24K          0B                 48K          Y
0B       1.53M     24K          0B                 0B           Y
0B       2.19M     24K          0B                 48K          Y
192K     4.67M     24K          0B                 0B           Y
0B       2.7M      24K          0B                 104K         Y
0B       3.35M     24K          0B                 144K         Y
```

显示数据库指定 dbspace 内由指定用户拥有的所有对象和子对象的大小：

```
sp_iqdbspaceinfo iq_main,GROUPO
```

```
dbspace_name    object_type  owner   object_name     object_id  id
  columns
iq_main         table        GROUPO  Contacts          3538     732
   288K
iq_main         table        GROUPO  Customers         3515     731
   240K
iq_main        table       GROUPO  Departments      3632    738   72K
iq_main         table        GROUPO  Employees         3641     739
   408K
iq_main         table        GROUPO  FinancialCodes    3612     736
   72K
iq_main        table       GROUPO  FinancialData    3621    737   96K
iq_main         table        GROUPO  Products          3593     735
   272K
iq_main         table        GROUPO  SalesOrderItems   3580     734
   120K
iq_main         table        GROUPO  SalesOrders       3565     733
   144K

indexes  metadata  primary_key  unique_constraint  foreign_key  dbsp
ace_online
```

```
0B        5.45M     24K          0B                  48K          Y
48K       4.63M     24K          0B                  0B           Y
0B        1.78M     24K          0B                  48K          Y
0B        8.03M     24K          0B                  48K          Y
0B        1.53M     24K          0B                  0B           Y
0B        2.19M     24K          0B                  48K          Y
192K      4.67M     24K          0B                  0B           Y
0B        2.7M      24K          0B                  104K         Y
0B        3.35M     24K          0B                  144K         Y
```

显示数据库中指定的 dbspace 内由指定用户拥有的指定对象及其子对象的大小：

```
sp_iqdbspaceinfo iq_main,GROUPO,Departments
```

```
dbspace_name    object_type  owner   object_name     object_id  id
  columns
iq_main        table       GROUPO  Departments      3632    738   72K

indexes  metadata  primary_key  unique_constraint  foreign_key  dbsp
ace_online
0B       1.78M     24K          0B                  48K          Y
```

sp_iqdbspaceobjectinfo 过程

列出给定 dbspace 中表类型的对象和子对象（包括列、索引、元数据、主键、唯一约束、外键和分区）。这不受 RLV dbspace 支持。

语法

sp_iqdbspaceobjectinfo [*dbspace-name*] [, *owner_name*] [, *object_name*] [, *object-type*]

参数
所有参数都是可选的，并且任何参数的提供均不受其它参数值的影响。

- **dbspace-name** – 如果已指定，**sp_iqdbspaceobjectinfo** 将仅显示指定 dbspace 的输出。否则，将显示数据库中所有 dbspace 的信息。
- **owner-name** – 对象的所有者。如果指定，**sp_iqdbspaceobjectinfo** 将仅显示包含指定所有者的那些表的输出。如果未指定，**sp_iqdbspaceobjectinfo** 显示数据库中所有用户的表的相关信息。
- **object-name** – 表的名称。如果未指定，**sp_iqdbspaceobjectinfo** 显示数据库中所有表的相关信息。
- **object-type** – **table** 对象的有效对象类型。

sp_iqdbspaceobjectinfo 存储过程支持用于解释 *dbspace_name*、*object_name* 和 *owner_name* 的通配符。它以 **LIKE** 子句匹配查询内部的模式的方式显示匹配指定模式的所有 dbspace 的信息。

特权
您必须具有系统过程的 EXECUTE 特权。

注释
如果指定 RLV dbspace，该过程将不返回任何结果。

对于表，**sp_iqdbspaceobjectinfo** 将为所有关联子对象显示汇总信息，按 dbspace_name、owner 和 object_name 排序。

sp_iqdbspaceobjectinfo 根据输入参数值显示以下信息：

表 18. sp_iqdbspaceobjectinfo 列

列名	描述
dbspace_name	dbspace 的名称。
dbspace_id	dbspace 的标识符。
object_type	表。
owner	对象所有者的名称。
object_name	dbspace 中表对象的名称。
object_id	对象的全局对象 ID。
id	对象的表 ID。
列	位于给定 dbspace 中的表列数。如果某一列或其中一个列分区位于某个 dbspace 上，则认为该列或该列分区位于该 dbspace 上。结果以 n/N 形式显示（总计 N 列的表中有 n 列位于给定 dbspace 上）。
indexes	位于给定 dbspace 上的用户定义表索引数。以 n/N 形式显示（总计 N 个表索引中有 n 个位于给定 dbspace 上）。如果是唯一约束，则不包含系统生成的索引，如 FP 索引和 HG 索引。
metadata	布尔字段 (Y/N)，表示子对象的元数据信息是否也位于此 dbspace 上。
primary_key	布尔字段 (1/0)，表示表的主键（如果有）是否也位于此 dbspace 上。
unique_constraint	位于给定 dbspace 上的唯一表约束数。以 n/N 形式显示（总计 N 个唯一表约束中有 n 个位于给定 dbspace 上）。
foreign_key	位于给定 dbspace 上的表外键数。以 n/N 形式显示（总计 N 个表外键中有 n 个位于给定 dbspace 上）。
partitions	位于给定 dbspace 上的表分区数。以 n/N 形式显示（总计 N 个表分区中有 n 个位于给定 dbspace 上）。

示例
以下示例显示 `iqdemo` 数据库中的对象，以便更好地阐释输出。`iqdemo` 包括一个名为 `iq_main` 的示例用户 dbspace，您自己的数据库中可能不包括此 dbspace。

显示数据库中某特定 dbspace 的相关信息：

```
sp_iqdbspaceobjectinfo iq_main
```

```
dbspace_name  dbspace_id object_type  owner   object_name  object_i
d  id  columns
iq_main       16387      table        DBA     emp1           3689
   741  4/4
iq_main       16387      table        DBA     iq_dummy       3686
   740  1/1
iq_main       16387      table        DBA     sale           3698
   742  4/4
iq_main       16387      table        GROUPO  Contacts       3538
   732  12/12
iq_main       16387      table        GROUPO  Customers      3515
   731  10/10
iq_main       16387      table        GROUPO  Departments    3632
   738  3/3
iq_main       16387      table        GROUPO  Employees      3641
   739  21/21
iq_main       16387      table        GROUPO  FinancialCodes 3612
   736  3/3
iq_main       16387      table        GROUPO  FinancialData  3621
   737  4/4
iq_main       16387      table        GROUPO  Products       3593
   735  8/8
iq_main       16387      table        GROUPO  SalesOrderItems3580
   734  5/5
iq_main       16387      table        GROUPO  SalesOrders    3565
   733  6/6

indexes  metadata  primary_key  unique_constraint  foreign_key  part
itions
0/0      Y                   0  0/0                0/0          0/0
0/0      Y                   0  0/0                0/0          0/0
0/0      Y                   0  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
1/1      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
4/4      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                2/2          0/0
0/0      Y                   1  0/0                3/3          0/0
```

显示数据库中某特定 dbspace 中指定用户拥有的对象的相关信息：

```
sp_iqdbspaceobjectinfo iq_main,GROUPO
```

```
dbspace_name  dbspace_id object_type  owner   object_name    object_
id  id  columns
iq_main       16387      table        GROUPO  Contacts       3538
     732 2/12
iq_main       16387      table        GROUPO  Customers      3515
     731 10/10
```

```
iq_main       16387      table        GROUPO  Departments    3632
     738 3/3
iq_main       16387      table        GROUPO  Employees      3641
     739 21/21
iq_main       16387      table        GROUPO  FinancialCodes 3612
     736 3/3
iq_main       16387      table        GROUPO  FinancialData  3621
     737 4/4
iq_main       16387      table        GROUPO  Products       3593
     735 8/8
iq_main       16387      table        GROUPO  SalesOrderItems3580
     734 5/5
iq_main       16387      table        GROUPO  SalesOrders    3565
     733 6/6

indexes  metadata  primary_key  unique_constraint  foreign_key  part
itions
0/0      Y                   1  0/0                1/1          0/0
1/1      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                1/1          0/0
0/0      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                1/1          0/0
4/4      Y                   1  0/0                0/0          0/0
0/0      Y                   1  0/0                2/2          0/0
0/0      Y                   1  0/0                3/3          0/0
```

在本示例中，命令将 dbspace_x 上的所有表移动到 dbspace_y。

```
SELECT 'ALTER TABLE ' || owner || '.' ||
object_name || ' MOVE TO dbspace_y;'
FROM sp_iqdbspaceobjectinfo()
WHERE object_type = 'table' AND
dbspace_name = 'dbspace_x';
```

结果为以下 **ALTER TABLE** 命令：

```
ALTER TABLE DBA.dt1 MOVE TO dbspace_y;
ALTER TABLE DBA.dt2 MOVE TO dbspace_y;
ALTER TABLE DBA.dt3 MOVE TO dbspace_y;
```

sp_iqdroplogin 过程

删除 SAP Sybase IQ 用户帐户。

语法 1

call sp_iqdroplogin ('*userid*')

语法 2

sp_iqdroplogin '*userid*'

语法 3

sp_iqdroplogin *userid*

语法 4

```
sp_iqdroplogin ( 'userid' )
```

参数

- **userid** – 要删除用户的 ID。

特权
您必须具有系统过程的 EXECUTE 特权。

注释
sp_iqdroplogin 删除指定的用户。

示例
以下命令全部用于移除用户 `rose`：

```
sp_iqdroplogin 'rose'
```

```
sp_iqdroplogin rose
```

```
call sp_iqdroplogin ('rose')
```

sp_iqemptyfile 过程

清空某个 dbfile 并将该 dbfile 中的对象移动到同一个 dbspace 中的另外一个可用读写 dbfile。这不适用于 RLV dbspace 中的文件。

语法

```
sp_iqemptyfile ( logical-file--name )
```

特权
您必须具有系统过程的 EXECUTE 特权。 必须具有以下一种系统特权：

- BACKUP DATABASE
- SERVER OPERATOR
- ALTER DATABASE

此外，您必须还要至少拥有以下系统特权之一：

- INSERT ANY TABLE
- UPDATE ANY TABLE
- DELETE ANY TABLE
- ALTER ANY TABLE
- LOAD ANY TABLE
- TRUNCATE ANY TABLE
- ALTER ANY OBJECT

注释

sp_iqemptyfile 清空某个 dbfile。dbspace 必须是只读 dbspace 才能执行 **sp_iqemptyfile** 过程。此过程将该文件中的对象移动到同一个 dbspace 中的另外一个可用读写 dbfile。如果没有其它读写 dbfile 可用，SAP Sybase IQ 会显示一条错误消息。

注意： 在 Multiplex 环境中，只能在协调器上运行 **sp_iqemptyfile**。必须有一个读写 dbspace 可用才能成功执行该过程。

如果 dbfile 位于 RLV dbspace 中，此错误消息将显示：

```
Cannot empty files in an rlv store dbspace.
```

示例

清空 dbfile **dbfile1**：

```
sp_iqemptyfile 'dbfile1'
```

sp_iqestdbspaces 过程

估计给定索引总大小所需的 dbspace 的数量和大小。

语法

```
sp_iqestdbspaces ( db_size_in_bytes, iq_page_size,
min_#_of_bytes, max_#_of_bytes )
```

特权

您必须具有系统过程的 EXECUTE 特权。 必须具有以下一种 系统特权：

- MANAGE ANY DBSPACE
- ALTER DATABASE

注释

sp_iqestdbspaces 根据数据的唯一程度提出多项建议：

建议	描述
min	如果数据几乎没有变化，可以选择只创建建议大小为 **min** 的 dbspace 段。这些建议反映在最少改变数据的情况下可能的最佳数据压缩。
avg	如果数据的变化量为平均水平，则可以创建建议大小为 **min** 的 dbspace 段，以及建议大小为 **avg** 的其它段。
max	如果数据变化度较高（有许多唯一值），则可以创建建议大小为 **min**、**avg** 和 **max** 的 dbspace 段。
spare	如果不确定数据中唯一值的数量，可以创建建议大小为 **min**、**avg**、**max** 和 **spare** 的 dbspace 段。装载数据后，可以随时删除不使用的段，但是创建的段过少可能会花费一些时间。

根据数据库的大小、IQ 页大小和每个 dbspace 段的字节数范围，显示有关 dbspace 段数量和大小的信息。此过程假定数据库是使用指定 IQ 页大小的缺省块大小创建的（否则，返回的估计值将不正确）。

表 19. sp_iqestdbspaces 参数

Name	数据类型	描述
db_size_in_bytes	decimal(16)	数据库的大小（以字节为单位）。
iq_page_size	smallint	为数据库的 IQ 段定义的页大小（必须是 2 的幂且介于 65536 和 524288 之间；缺省值为 131072）。
min_#_of_bytes	int	每个 dbspace 段的最小字节数。缺省值为 20,000,000 (20MB)。
max_#_of_bytes	int	每个 dbspace 段的最大字节数。缺省值为 2,146,304,000 (2.146GB)。

sp_iqfile 过程

显示有关 dbspace 中每个 dbfile 的详细信息。

语法

```
sp_iqfile [ dbspace-name ]
```

适用于

Simplex 和 Multiplex。

特权

您必须具有系统过程的 EXECUTE 特权，以及 MANAGE ANY DBSPACE 系统特权。

注释

sp_iqfile 显示 dbspace 中每个 dbfile 中的数据的用法、属性和类型。可以使用这些信息确定是否必须移动数据，以及对于已移动的数据是否已释放旧版本。

列名	描述
DBSpaceName	在 **CREATE DBSPACE** 语句中指定的 dbspace 的名称。无论是指定 **CREATE DATABASE...CASE IGNORE** 还是指定 **CASE RESPECT**，Dbspace 名称始终不区分大小写。
DBFileName	逻辑文件名。
Path	物理文件或原始分区的位置。
SegmentType	dbspace 的类型（MAIN、TEMPORARY、RLV 或 CACHE）。
RWMode	dbspace 的模式：始终为读写 (RW)。

列名	描述
Online	T（联机）或 F（脱机）。
Usage	此文件当前使用的 dbspace 占整个 dbspace 的百分比。在 Multiplex 配置中针对辅助节点运行时，此列将显示 NA。
DBFileSize	文件或原始分区的当前大小。对于原始分区来说，此大小值可以小于实际大小。
Reserve	dbspace 中可添加到此文件的保留空间。
StripeSize	如果磁盘条带化已开启，则始终为 1。
BlkTypes	用户数据和内部系统结构占用的空间。
FirstBlk	分配给文件的第一个 IQ 块号。
LastBlk	分配给文件的最后一个 IQ 块号。
OkToDrop	"Y" 表示可删除文件；否则为 "N"。

标识符	块类型
A	活动版本
B	备份结构
C	检查点日志
D	数据库标识
F	空闲列表
G	全局空闲列表管理器
H	空闲列表的标头块
I	索引建议存储
M	Multiplex CM*
O	旧版本
R	RLV 空闲列表管理器
T	表使用
U	索引使用
N	列使用
X	在检查点处删除

*Multiplex 提交标识块（实际 128 块）存在于所有 IQ 数据库中，即使 Simplex 数据库不使用也不例外。

示例
显示有关 dbspace 中文件的信息：

```
sp_iqfile;
```

```
sp_iqfile;
DBSpaceName,DBFileName,Path,SegmentType,RWMode,Online,
Usage,DBFileSize,Reserve,StripeSize,BlkTypes,FirstBlk,
LastBlk,OkToDrop

'IQ_SYSTEM_MAIN','IQ_SYSTEM_MAIN','/sun1-c1/users/smith/mpx/m/
mpx_db.iq','MAIN','RW','T','21','
2.92G','0B','1K','1H,76768F,32D,19A,185O,128M,34B,32C'
,1,384000,'N'

'mpx_main1','mpx_main1','/sun1-c1/users/smith/mpx/m/
mpx_main1.iq','MAIN','RW','T','1'
,'100M','0B','1K','1H',1045440,1058239,'N'

'IQ_SHARED_TEMP','sharedfile1_bcp','/sun1-c1/users/smith/mpx/m/
f1','SHARED_TEMP','RO','T','0',
'50M','0B','1K','1H',1,6400,'N'

'IQ_SHARED_TEMP','sharedfile2_bcp','/sun1-c1/users/smith/mpx/m/
f2','SHARED_TEMP','RO','T','0',
'50M','0B','1K','1H',1045440,1051839,'N'

'myDAS', 'ssd_dev_1', '/dev/raw/ssd_dev_1', 'CACHE', 'RW', 'T', '2',
'20M', '0B', '1K', '1H', '64F', '1', '5120', 'N'
'myDAS', 'ssd_dev_2', '/dev/raw/ssd_dev_2', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '522208', '527327', 'N'
'myDAS', 'ssd_dev_3', '/dev/raw/ssd_dev_3', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '1044416', '1049535', 'N'
'myDAS', 'ssd_dev_4', '/dev/raw/ssd_dev_4', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '1566624', '1571743', 'N'
'myDAS', 'ssd_dev_5', '/dev/raw/ssd_dev_5', 'CACHE', 'RW', 'T', '1',
'20M', '0B', '1K', '1H', '32F', '2088832', '2093951', 'N'

'IQ_SYSTEM_TEMP','IQ_SYSTEM_TEMP','/sun1-c1/users/smithmpx/m/
mpx_db.iqtmp','TEMPORARY','RW',
'T','1','2.92G','0B','1K','1H,64F,33A',1,384000,'N'
```

sp_iqmodifyadmin 过程

将指定登录策略中的某个选项设为一个特定值。如果未指定登录策略，则在根策略上设置该选项。在 Multiplex 中，**sp_iqmodifyadmin** 将采用可选参数，即 Multiplex 服务器名称。

语法 1

```
call sp_iqmodifyadmin ( 'policy_option_name', 'value_in' ,
['login_policy_name'] )
```

语法 2

```
sp_iqmodifyadmin 'policy_option_name',
'value_in' ,' login_policy_name '
```

语法 3

```
sp_iqmodifyadmin  policy_option_name, value_in, ,login_policy_name
```

语法 4

```
sp_iqmodifyadmin 'policy_option_name',
'value_in' ,' login_policy_name ' ,' server_name '
```

参数

- **policy_option_name** – 要更改的登录策略选项。
- **value_in** – 登录策略选项的新值。
- **login_policy_name** – 要更改其登录策略选项的策略。

特权

您必须具有系统过程的 EXECUTE 特权，以及 MANAGE ANY LOGIN POLICY 系统特权。

示例

对于 *lockeduser* 策略，将登录选项 `locked` 设置为 ON：

```
call sp_iqmodifyadmin ('locked','on','lockeduser')
```

对于 `Writer1` Multiplex 服务器上的 *lockeduser* 策略，将登录选项 `locked` 设置为 ON：

```
call sp_iqmodifyadmin ('locked','on','lockeduser','Writer1')
```

sp_iqmodifylogin 过程

为用户分配登录策略。

语法 1

```
call sp_iqmodifylogin 'userid', ['login_policy_name']
```

语法 2

```
sp_iqmodifylogin 'userid', ['login_policy_name']
```

参数

- **userid** – 存放待修改的帐户名的变量。
- **login_policy_name** – （可选）指定将分配给用户的登录策略的名称。如果未指定任何登录策略名，则向用户分配根登录策略。

特权
您必须具有系统过程的 EXECUTE 特权，以及 MANAGE ANY USER 系统特权。

示例
将用户 joe 分配给登录策略 expired_password:

```
sp_iqmodifylogin 'joe', 'expired_password'
```

将用户 joe 分配给根登录策略:

```
call sp_iqmodifylogin ('joe')
```

sp_iqobjectinfo 过程

返回数据库对象和子对象的分区和 dbspace 分配。

语法

```
sp_iqobjectinfo [ owner_name ]  [ , object_name ] [ , object-type ]
```

参数

- **owner_name** – 对象的所有者。如果指定，**sp_iqobjectinfo** 将仅显示包含指定所有者的那些表的输出。如果未指定，**sp_iqobjectinfo** 显示数据库中所有用户的表的相关信息。
- **object_name** – 表的名称。如果未指定，**sp_iqobjectinfo** 显示数据库中所有表的相关信息。
- **object-type** – 有效的 **table** 对象类型。

  如果 object-type 是表，则必须用引号引起。

所有参数都是可选的，并且任何参数的提供均不受其它参数值的影响。

特权
您必须具有系统过程的 EXECUTE 特权。

注释
将输入参数与 **sp_iqobjectinfo** 一起使用；您可以查询 **sp_iqobjectinfo** 的结果，如果使用输入参数，而不是在查询的 **WHERE** 子句中使用谓词，执行效果会更好。例如，将查询 A 编写为：

```
SELECT COUNT(*) FROM sp_iqobjectinfo()
WHERE owner = 'DBA'
AND object_name = 'tab_case510'
AND object_type = 'table'
AND sub_object_name is NULL
AND dbspace_name = 'iqmain7'
AND partition_name = 'P1'
```

查询 B 对查询 A 进行了重新编写，改为使用 **sp_iqobjectinfo** 输入参数：

```
SELECT COUNT(*) FROM sp_iqobjectinfo('DBA','tab_case510','table')
WHERE sub_object_name is NULL
AND dbspace_name = 'iqmain7'
AND PARTITION_NAME = 'P1'
```

查询 B 返回结果的速度要快于查询 A。将输入参数传递到 **sp_iqobjectinfo** 后，该过程将进行比较，然后连接系统表中的少量记录，因此与查询 A 相比，工作量较少。在查询 B 中，过程本身使用了谓词，它返回的结果集较小，因此查询中使用的谓词数较少。

sp_iqobjectinfo 存储过程支持用于解释 *owner_name*、*object_name* 和 *object_type* 的通配符。它以 **LIKE** 子句匹配查询内部模式的方式显示匹配指定模式的所有 dbspace 的信息。

返回（表类型中）特定或所有数据库对象及其子对象的所有分区和 dbspace 分配。子对象为列、索引、主键、唯一约束和外键。

表 20. sp_iqobjectinfo 列

列名	描述
owner	对象所有者的名称。
object_name	位于 dbspace 上的（表类型）对象的名称。
sub_object_name	dbspace 中对象的名称。
object_type	对象的类型（列、索引、主键、唯一约束、外键、分区或表）。
object_id	对象的全局对象 ID。
id	对象的表 ID。
dbspace_name	对象所在的 dbspace 的名称。在已分区对象的特殊元行中显示字符串 "[multiple]"。[multiple] 行表示输出中存在多个描述表或列的行。
partition_name	给定对象的分区的名称。

示例

注意： 以下示例显示 iqdemo 数据库中的对象，以便更好地阐释输出。iqdemo 包括一个名为 iq_main 的示例用户 dbspace，您自己的数据库中可能不包括此 dbspace。

显示某特定用户拥有的特定数据库对象及子对象的分区和 dbspace 分配的相关信息：

```
sp_iqobjectinfo GROUPO,Departments
```

```
owner   object_name  sub_object_name                object_type  obj
ect_id  id
GROUPO  Departments  (NULL)                          table         3
632     738
GROUPO  Departments  DepartmentID                    column        3
633     738
GROUPO  Departments  DepartmentName                  column        3
634     738
GROUPO  Departments  DepartmentHeadID                column        3
635     738
GROUPO  Departments  DepartmentsKey                  primary
key   83       738
GROUPO  Departments  FK_DepartmentHeadID_EmployeeID  foreign
key   92       738

dbspace_name     partition_name
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
iq_main          (NULL)
```

显示 *object-type* **table** 的某特定用户拥有的特定数据库对象及子对象的分区和 dbspace 分配的相关信息：

```
sp_iqobjectinfo DBA,sale,'table'
```

```
owner  object_name  sub_object_name  object_type  object_id  id
DBA    sale         (NULL)           table        3698       742
DBA    sale         prod_id          column       3699       742
DBA    sale         month_num        column       3700       742
DBA    sale         rep_id           column       3701       742
DBA    sale         sales            column       3702       742

dbspace_name      partition_name
iq_main           (NULL)
iq_main           (NULL)
iq_main           (NULL)
iq_main           (NULL)
iq_main           (NULL)
```

sp_iqspaceused 过程

显示 IQ 存储库、IQ 临时存储库、RLV 存储库以及 IQ 全局和局部共享临时存储库中可用空间和已用空间的相关信息。

语法

```
sp_iqspaceused(out mainKB             unsigned bigint,
               out mainKBUsed         unsigned bigint,
               out tempKB             unsigned bigint,
               out tempKBUsed         unsigned bigint,
               out shTempTotalKB      unsigned bigint,
               out shTempTotalKBUsed  unsigned bigint,
               out shTempLocalKB      unsigned bigint,
               out shTempLocalKBUsed  unsigned bigint,
               out rlvLogKB           unsigned bigint,
               out rlvLogKBUsed       unsigned bigint)
```

适用于
Simplex 和 Multiplex。

特权
您必须具有系统过程的 EXECUTE 特权。 必须具有以下一种系统特权：

- ALTER DATABASE
- MANAGE ANY DBSPACE
- MONITOR

注释
sp_iqspaceused 以 unsigned bigint 输出参数形式返回多个值。该系统存储过程可由用户定义的存储过程调用，以确定正在使用的主存储空间、临时存储空间和 RLV 存储空间的大小。

sp_iqspaceused 返回 **sp_iqstatus** 提供的信息的部分内容，但允许用户以 SQL 变量返回信息以在计算中使用。

如果在 Multiplex 数据库上运行，该过程将应用于在其上运行该过程的服务器。另外还返回 IQ_SHARED_TEMP 的已用空间。

列名	描述
mainKB	IQ 主存储空间的总大小 (KB)。
mainKBUsed	数据库使用的 IQ 主存储空间的大小 (KB)。辅助 Multiplex 节点返回 '(Null)'。
tempKB	IQ 临时存储空间的总大小 (KB)。

列名	描述
tempKBUsed	数据库使用的 IQ 临时存储空间的总大小 (KB)。
shTempTotalKB	IQ 全局共享临时存储空间的总大小 (KB)。
shTempLocalKB	IQ 局部共享临时存储空间的总大小 (KB)。
shTempLocalKBUsed	数据库使用的 IQ 局部共享临时存储空间的大小 (KB)。
rlvLogKB	RLV 存储空间的总大小 (KB)。
rlvLogKBUsed	数据库使用的 RLV 存储空间的大小 (KB)。

示例

sp_iqspaceused 需要 7 个输出参数。创建一个用于声明 7 个输出参数的用户定义存储过程 **myspace**，然后调用 **sp_iqspaceused**：

```
  create or replace procedure dbo.myspace()
begin
     declare mt unsigned bigint;
     declare mu unsigned bigint;
     declare tt unsigned bigint;
     declare tu unsigned bigint;
     declare gt unsigned bigint;
     declare gu unsigned bigint;
     declare lt unsigned bigint;
     declare lu unsigned bigint;
     declare tt_t unsigned bigint;
     declare mt_t unsigned bigint;
     declare gt_t unsigned bigint;
     declare lt_t unsigned bigint;
     call sp_iqspaceused(mt,mu,tt,tu,gt,gu,lt,lu);
     if (tt = 0) then
        set tt_t = 0;
     else
        set tt_t = tu*100/tt;
     end if;
     if (mt = 0) then
        set mt_t = 0;
     else
        set mt_t = mu*100/mt;
     end if;
     if (gt = 0) then
        set gt_t = 0;
     else
        set gt_t = gu*100/gt;
     end if;
     if (lt = 0) then
        set lt_t = 0;
     else
        set lt_t = lu*100/lt;
     end if;
  select cast(mt/1024 as unsigned bigint) as mainMB,
```

```
         cast(mu/1024 as unsigned bigint) as mainusedMB, mt_t as
mainPerCent,
         cast(tt/1024 as unsigned bigint) as tempMB,
         cast(tu/1024 as unsigned bigint) as tempusedMB, tt_t as
tempPerCent,
         cast(gt/1024 as unsigned bigint) as shTempTotalKB,
        cast(gu/1024 as unsigned bigint) as shTempTotalKBUsed, gt_t
as globalshtempPerCent,
         cast(lt/1024 as unsigned bigint) as shTempLocalMB,
        cast(lu/1024 as unsigned bigint) as shTempLocalKBUsed, lt_t
as localshtempPerCent;
end
```

要显示 **sp_iqspaceused** 的输出，请执行 **myspace**：

```
myspace
```

sp_iqsysmon 过程

监控 SAP Sybase IQ 的多个组件，其中包括管理缓冲区高速缓存、内存、线程、锁、I/O 功能和 CPU 利用率。

批处理模式语法

```
sp_iqsysmon start_monitor
sp_iqsysmon stop_monitor [, 'section(s)' ]
or
sp_iqsysmon 'time-period' [, 'section(s)' ]
```

文件模式语法

```
sp_iqsysmon start_monitor, 'filemode' [, 'monitor-options' ]
sp_iqsysmon stop_monitor
```

批处理模式参数

- **start_monitor** – 开始监控。
- **stop_monitor** – 停止监控并显示报告。
- **time-period** – 监控时间段，采用 HH:MM:SS 格式。
- **section(s)** – 要由 **sp_iqsysmon** 显示的一个或多个部分的缩写。

  请参见“注释 （第 0 页）”部分了解有关缩写的完整列表的信息。

  如果指定多个部分，请使用空格分隔各个部分缩写，并将列表括在单引号或双引号中。缺省情况下显示所有部分。

  对于与 IQ 主存储库相关的部分，可通过分别在部分缩写前面添加前缀 'm' 或 't' 来指定主存储库或临时存储库。如果不添加前缀，则会监控这两个存储库。例如，如果指定 'mbufman'，则仅监控 IQ 主存储库缓冲区管理器。如果指定 'mbufman tbufman' 或 'bufman'，则会同时监控主存储库缓冲区管理器和临时存储库缓冲区管理器。

注意： **sp_iqsysmon** 当前不支持 SAP Sybase IQ 组件磁盘 I/O 和锁管理器。

文件模式参数

- **start_monitor** – 开始监控。
- **stop_monitor** – 停止监控并将剩余输出写入日志文件。
- **filemode** – 指定 **sp_iqsysmon** 在文件模式下运行。在文件模式下，将在监控周期的每个间隔显示统计信息样本。缺省情况下，输出写入到名为 *dbname.connid-iqmon* 的日志文件中。使用 **file_suffix** 选项可更改输出文件的后缀。有关 **file_suffix** 选项的说明，请参见 *monitor_options* 参数。
- **monitor_options** – monitor _options 字符串可以包含一个或多个选项：
  - **-interval seconds** – 指定报告间隔（秒）。每一间隔后，将监控器示例统计信息输出到日志文件中。如果未指定 -interval 选项，则缺省设置为每 60 秒输出一次。最小报告间隔为 2 秒。如果为该选项指定的间隔无效或小于 2 秒，则会将间隔设置为 2 秒。

    初次显示时，显示自服务器启动以来的计数器信息。后续显示则显示与先前显示的不同之处。在运行有关性能问题的查询期间或在通常会出现性能问题的那一天中的某个时间，以 60 秒的缺省间隔运行监控器通常可以获得有用的结果。非常短的间隔可能不会提供有意义的结果。间隔应与作业时间成比例；60 秒通常已足够。
  - **-file_suffix suffix** – 创建一个名为 `dbname.connid-suffix` 的监控器输出文件。如果未指定 -file_suffix 选项，则后缀缺省为 `iqmon`。如果指定 -file_suffix 选项，但是未提供后缀或提供空字符串作为后缀，则不使用后缀。
  - **-append 或 -truncate** – 分别指示 **sp_iqsysmon** 向现有输出文件附加内容或截断现有输出文件。截断是缺省设置。如果同时指定这两个选项，则在字符串中较晚指定的那个选项有效。
  - **-section section(s)** – 指定要写入监控器日志文件的一个或多个部分的缩写。

    请参见“注释 （第 0 页）”部分了解有关缩写的完整列表的信息。

    缺省情况下写入所有部分。文件模式下在部分列表中指定的缩写与批处理模式下使用的缩写相同。如果指定多个部分，则必须以空格分隔各个部分的缩写。

    如果指定 -section 选项时没有指定任何部分，则不会对任何部分进行监控。无效部分缩写将被忽略，并向 IQ 消息文件中写入一条警告。

特权

您必须具有系统过程的 EXECUTE 特权，以及 MONITOR 系统特权。

注释

要报告的报告部分或 IQ 组件	要输入的缩写
缓冲区分配	（主） – mbufalloc （临时） – tbufalloc

要报告的报告部分或 IQ 组件	要输入的缩写
缓冲区管理器	（主） – mbufman （临时） – tbufman
缓冲池	（主） – mbufpool （临时） – tbufpool
目录统计信息	目录
CPU 利用率	cpu
空闲列表管理	（主） – mfreelist （临时） – tfreelist
内存管理	memory
预取管理	（主） – mprefetch （临时） – tprefetch
IQ RLV 内存存储库统计信息	rlv
大容量内存分配器 (LMA) 统计信息	lma
服务器上下文统计信息	server
线程管理	threads
事务管理	txn

sp_iqsysmon 存储过程监控 SAP Sybase IQ 的多个组件，其中包括管理缓冲区高速缓存、内存、线程、锁、I/O 功能和 CPU 利用率。

sp_iqsysmon 过程支持两种监控模式：

- **批处理模式** – **sp_iqsysmon** 收集在监控器启动到停止期间或 *time-period* 参数指定的期间内监控器的统计信息。监控期间结束时，**sp_iqsysmon** 显示合并统计信息的列表。

  批处理模式下的 **sp_iqsysmon** 与 SAP Adaptive Server® Enterprise 过程 **sp_sysmon** 相似。
- **文件模式** – **sp_iqsysmon** 将监控器启动到停止期间的每个时间间隔的示例统计信息写入日志文件。

  在文件模式下初次显示时，将显示自服务器启动以来的计数器信息。后续显示则显示与先前显示的不同之处。

  文件模式下的 **sp_iqsysmon** 与 **IQ UTILITIES** 命令 **START MONITOR** 和 **STOP MONITOR** 接口相似。

批处理模式语法示例

示例 1：

在批处理模式下启动监控器，并显示主存储库和临时存储库的所有部分：

```
sp_iqsysmon start_monitor
sp_iqsysmon stop_monitor
```

示例 2：

在批处理模式下启动监控器，并显示主存储库的缓冲区管理器和缓冲池统计信息。

```
sp_iqsysmon start_monitor
sp_iqsysmon stop_monitor 'mbufman mbufpool'
```

示例 3：

在 10 分钟后输出监控信息：

```
sp_iqsysmon '00:10:00'
```

示例 4：

5 分钟之后，仅输出 **sp_iqsysmon** 报告的内存管理器部分：

```
sp_iqsysmon '00:05:00', memory
```

示例 5：

启动监控器，执行两个过程和一个查询，停止监控器，然后仅输出报告的缓冲区管理器部分：

```
sp_iqsysmon start_monitor
     go
     execute proc1
     go
     execute proc2
     go
     select sum(total_sales) from titles
     go
     sp_iqsysmon stop_monitor, bufman
     go
```

示例 6：

2 分钟后仅输出报告的主缓冲区管理器和主缓冲池部分：

```
sp_iqsysmon '00:02:00', 'mbufman mbufpool'
```

示例 7：

1 小时后仅输出报告的 RLV 部分：

```
sp_iqsysmon '01:00:00','rlv'
```

示例 8：

5 秒后仅输出报告的 LMA 部分：

```
sp_iqsysmon '00:00:05', 'lma'
```

示例 9：

在批处理模式下运行监控器 10 秒钟，并在该时间段结束时显示合并统计信息：

```
sp_iqsysmon '00:00:10', 'mbufpool memory'
```

文件模式语法示例
示例 1：

在监控器启动到停止期间，每 2 秒截断信息一次并将其写入日志文件中：

```
sp_iqsysmon start_monitor, 'filemode', '-interval 2'
     .
     .
     .
     sp_iqsysmon stop_monitor
```

示例 2：

仅将主缓冲区管理器和内存管理器部分的输出附加到名为 dbname.connid-testmon 的 ASCII 文件。对于数据库 iqdemo，将结果写入文件 iqdemo.2-testmon 中：

```
sp_iqsysmon start_monitor, 'filemode',
     '-file_suffix testmon -append -section mbufman memory'
     .
     .
     .
     sp_iqsysmon stop_monitor
```

示例 3：

仅输出报告的 RLV 和 LMA 部分：

```
sp_iqsysmon start_monitor,'filemode','-section rlv lma'
     sp_iqsysmon stop_monitor
```

示例 4：

在文件模式下启动监控器，并将主缓冲池和内存管理器的统计信息写入日志文件（每 5 秒写入一次）：

```
sp_iqsysmon start_monitor, ‘filemode’, '-interval 5 -section
mbufpool memory'
sp_iqsysmon stop_monitor
```

sp_iqsysmon 过程示例

sp_iqsysmon 输出示例。

示例 1：

在 20 分钟后显示缓冲区分配（主存储和临时存储）的输出。

```
sp_iqsysmon '00:20:00', 'mbufalloc tbufalloc'

==============================
Buffer Allocator (Main)"
==============================

STATS-NAME                   VALUE
NActiveCommands                  2
BufAllocMaxBufs               2275( 81.6% )
BufAllocAvailBufs             2115( 93.0% )
BufAllocReserved               160( 7.0% )
BufAllocAvailPF                750( 33.0% )
BufAllocSlots                  100
BufAllocNPinUsers                0
BufAllocNPFUsers                 2
BufAllocNPostedUsrs              0
BufAllocNUnpostUsrs              0
BufAllocPinQuota                 0
BufAllocNPostEst                 0
BufAllocNUnPostEst               0
BufAllocMutexLocks               0
BufAllocMutexWaits               0( 0.0% )

STATS-NAME                   VALUE
NActiveCommands                  2
BufAllocMaxBufs               2275( 81.6% )
BufAllocAvailBufs             2115( 93.0% )
BufAllocReserved               160( 7.0% )
BufAllocAvailPF                750( 33.0% )
BufAllocSlots                  100
BufAllocNPinUsers                0
BufAllocNPFUsers                 2
BufAllocNPostedUsrs              0
BufAllocNUnpostUsrs              0
BufAllocPinQuota                 0
BufAllocNPostEst                 0
BufAllocNUnPostEst               0
BufAllocMutexLocks               0
BufAllocMutexWaits               0( 0.0% )


STATS-NAME                 TOTAL  UNKNWN    HASH        CSORT     ROW
ROWCOL      FP  GARRAY     LOB   BTREE      BM      BV   STORE     TEST
NumClients                   2       0       0           0       2
0       0       0       0       0       0       0       0       0
PinUserQuota                 0       0       0           0       0
0       0       0       0       0       0       0       0       0
PrefetchUserQuota          160       0       0           0     160
0       0       0       0       0       0       0       0       0
PinUserRegisters             2       2       0           0       0
0       0       0       0       0       0       0       0       0
PfUserRegisters           4697       0       0           0     382
2621     377     182       0       2       0       0       0       0

ClientCountOfPinners         0       1       3           6      10
33      66     100     333     666    1000    3333    6666   10000
```

```
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Hash                            0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Sort                            0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Row                             2       0       0           0       0
0       0       0       0       0       0       0       0       0       0
RowColumn                       0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
FP                              0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Garray                          0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
LOB                             0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
BTree                           0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
BM                              0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
BV                              0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Store                           0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Test                            0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
DBCC                            0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Run                             0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
QCPRun                          0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
TextDoc                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Unknown                         0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
VDO                             0       0       0           0       0
0       0       0       0       0       0       0       0       0       0
Load                          Pass      2       0           0       0
0       0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)            DBCC   BLKMAP   IQUTIL
NumClients                      0       0       0           0       0
0       0       0       0       0
PinUserQuota                    0       0       0           0       0
0       0       0       0       0
PrefetchUserQuota               0       0       0           0       0
0       0       0       0       0
PinUserRegisters                0       0       0           0       0
0       0       0       0       0
```

```
PfUserRegisters                0      0      0          0      0
0       0       0    1133       0

ClientCountOfPinners         33333   66666  100000   4294967295
Unknown                          0       0       0            0
Hash                             0       0       0            0
Sort                             0       0       0            0
Row                              0       0       0            0
RowColumn                        0       0       0            0
FP                               0       0       0            0
Garray                           0       0       0            0
LOB                              0       0       0            0
BTree                            0       0       0            0
BM                               0       0       0            0
BV                               0       0       0            0
Store                            0       0       0            0
Test                             0       0       0            0
DBCC                             0       0       0            0
Unknown                          0       0       0            0
Unknown                          0       0       0            0
Run                              0       0       0            0
QCPRun                           0       0       0            0
TextDoc                          0       0       0            0
Unknown                          0       0       0            0
Unknown                          0       0       0            0
VDO                              0       0       0            0
Load                         0      0      0          0      0      0


================================
Buffer Allocator (Temporary)
================================

STATS-NAME                   VALUE
NActiveCommands                  2
BufAllocMaxBufs               2275( 81.6% )
BufAllocAvailBufs             2263( 99.5% )
BufAllocReserved                12( 0.5% )
BufAllocAvailPF                908( 39.9% )
BufAllocSlots                  100
BufAllocNPinUsers                2
BufAllocNPFUsers                 2
BufAllocNPostedUsrs              0
BufAllocNUnpostUsrs              0
BufAllocPinQuota               175
BufAllocNPostEst                 2
BufAllocNUnPostEst               2
BufAllocMutexLocks               0
BufAllocMutexWaits               0( 0.0% )

STATS-NAME                 TOTAL  UNKNWN    HASH       CSORT     ROW
ROWCOL      FP  GARRAY     LOB   BTREE      BM      BV   STORE     TEST
NumClients                   4       0       0           4       0
0       0       0       0       0       0       0       0       0
PinUserQuota                10       0       0          10       0
0       0       0       0       0       0       0       0       0
```

```
PrefetchUserQuota              2       0       0           2       0
0       0       0       0       0       0       0       0       0
PinUserRegisters               668         0       300           247
0       0       0       0       0       0       0       0       0       0
PfUserRegisters              675       0       0         295       0
0       0       0       0       0       0       0       1       0

ClientCountOfPinners           0       1       3           6       10
33      66      100     333     666     1000    3333    6666    10000
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Hash                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
Sort                           2       0       1           0       1
0       0       0       0       0       0       0       0       0
Row                            0       0       0           0       0
0       0       0       0       0       0       0       0       0
RowColumn                       0       0       0           0       0
0       0       0       0       0       0       0       0       0
FP                             0       0       0           0       0
0       0       0       0       0       0       0       0       0
Garray                         0       0       0           0       0
0       0       0       0       0       0       0       0       0
LOB                            0       0       0           0       0
0       0       0       0       0       0       0       0       0
BTree                          0       0       0           0       0
0       0       0       0       0       0       0       0       0
BM                             0       0       0           0       0
0       0       0       0       0       0       0       0       0
BV                             0       0       0           0       0
0       0       0       0       0       0       0       0       0
Store                          0       0       0           0       0
0       0       0       0       0       0       0       0       0
Test                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
DBCC                           0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Run                            0       0       0           0       0
0       0       0       0       0       0       0       0       0
QCPRun                         `       0       0           0       0
0       0       0       0       0       0       0       0       0
TextDoc                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
Unknown                        0       0       0           0       0
0       0       0       0       0       0       0       0       0
VDO                            0       0       0           0       0
0       0       0       0       0       0       0       0       0
Load                         Pass      2       0           0       0
0       0       0       0       0       0       0       0       0
```

```
STATS-NAME (cont'd)           DBCC   BLKMAP   IQUTIL
NumClients                    0      0       0           0       0
0       0       0       0       0
PinUserQuota                  0      0       0           0       0
0       0       0       0       0
PrefetchUserQuota             0      0       0           0       0
0       0       0       0       0
PinUserRegisters              0      0       0         110       2
0       0       0       0       9
PfUserRegisters               0      0       0         378       0
0       0       1       0       0

ClientCountOfPinners         33333   66666  100000   4294967295
Unknown                          0       0       0            0
Hash                             0       0       0            0
Sort                             0       0       0            0
Row                              0       0       0            0
RowColumn                        0       0       0            0
FP                               0       0       0            0
Garray                           0       0       0            0
LOB                              0       0       0            0
BTree                            0       0       0            0
BM                               0       0       0            0
BV                               0       0       0            0
Store                            0       0       0            0
Test                             0       0       0            0
DBCC                             0       0       0            0
Unknown                          0       0       0            0
Unknown                          0       0       0            0
Run                              0       0       0            0
QCPRun                           0       0       0            0
TextDoc                          0       0       0            0
Unknown                          0       0       0            0
Unknown                          0       0       0            0
VDO                              0       0       0            0
Load                         0       0       0           0       0
0
```

示例 2:

在 20 分钟后显示缓冲区管理器（主存储和临时存储）的输出。

```
sp_iqsysmon '00:20:00', 'mbufman tbufman'


================================
Buffer Manager (Main)
================================

STATS-NAME                   TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
Finds                     80137       0       0       0       0    9046
3307       0   20829       0       0       0       0     275
Hits                      80090       0       0       0       0    9015
3291       0   20829       0       0       0       0     275
Hit%                       99.9       0       0       0       0    99.7
```

```
99.5       0     100        0        0        0        0     100
FalseMiss                   26469       0        0        0        0
63       40        0     1097        0        0        0        0        0
UnOwnRR                        48       0        0       0        0      31
16        0        1        0        0        0        0        0
Cloned                                0        0        0        0        0
0        0        0        0        0        0        0        0        0
Creates                      1557       0        0        0        0       60
179       0     256        0        0        0        0       58
Destroys                      546       0        0        0        0        0
12       21        0        6        0        0        0        0       29
Dirties                      7554       0        0        0        0     1578
585       0        0        0        0        0        0        0
RealDirties                  2254       0        0        0        0        0
117     180        0      542        0        0        0        0        0       58
PrefetchReqs                   80       0        0        0        0        0
0        0        0       74        0        0        0        0        0        0
PrefetchNotInMem               1        0        0        0        0        0
0        0        0        1        0        0        0        0        0        0
PrefetchInMem                1466       0        0        0        0        0
0        0        0     1466        0        0        0        0        0        0
Reads                          48       0        0        0        0       31
16        0        1        0        0        0        0        0
PReadBlks                     114       0        0        0        0        0
80       32        0        2        0        0        0        0        0        0
PReadKB                                0        0        0        0        0
0        0        0        0        0        0        0        0        0        0
ReReads                                0        0        0        0        0
0        0        0        0        0        0        0        0        0        0
Writes                        2002       0        0        0        0      104
163       0      538        0        0        0        0       29
PWriteBlks                    6506       0        0        0        0      210
326       0     1115        0        0        0        0       58
PWriteKB                               0        0        0        0        0
0        0        0        0        0        0        0        0        0        0
GrabbedDirty                           0        0        0        0        0
0        0        0        0        0        0        0        0        0        0
ReadRemoteRpc                          0        0        0        0        0
0        0        0        0        0        0        0        0        0        0
ReadRemotePhyIO                        0        0        0        0        0
0        0        0        0        0        0        0        0        0        0

STATS-NAME (cont'd)          BARRAY  BLKMAP    HASH    CKPT      BM
TEST     CMID    RIDCA       LOB  LVCRID    FILE  RIDMAP    RVLOG
Finds                         2681    8329       0       0    35670
0        0        0        0        0        0        0        0
Hits                          2681    8329       0       0    35670
0        0        0        0        0        0        0        0
Hit%                           100     100       0       0      100
0        0        0        0        0        0        0        0
FalseMiss                       84    8329       0       0    16856
0        0        0        0        0        0        0        0
UnOwnRR                                0        0        0        0        0
0        0        0        0        0        0        0        0
Cloned                                 0        0        0        0        0
0        0        0        0        0        0        0        0
```

```
Creates                        108     358       0       0     538
0       0       0       0       0       0       0       0
Destroys                         0     126       0       0      59
0       0       0       0       0       0       0       0
Dirties                        512     235       0       0    4644
0       0       0       0       0       0       0       0
RealDirties                    128     593       0       0     636
0       0       0       0       0       0       0       0
PrefetchReqs                     6       0       0       0       0
0       0       0       0       0       0       0       0
PrefetchNotInMem                 0       0       0       0       0
0       0       0       0       0       0       0       0
PrefetchInMem                    0       0       0       0       0
0       0       0       0       0       0       0       0
Reads                          0       0       0       0       0       0
0       0       0       0       0       0       0
PReadBlks                        0       0       0       0       0
0       0       0       0       0       0       0       0
PReadKB                          0       0       0       0       0
0       0       0       0       0       0       0       0
ReReads                          0       0       0       0       0
0       0       0       0       0       0       0       0
Writes                         128     466       0       0     574
0       0       0       0       0       0       0       0
PWriteBlks                     239    3728       0       0     830
0       0       0       0       0       0       0       0
PWriteKB                         0       0       0       0       0
0       0       0       0       0       0       0       0
GrabbedDirty                     0       0       0       0       0
0       0       0       0       0       0       0       0
ReadRemoteRpc                    0       0       0       0       0
0       0       0       0       0       0       0       0
ReadRemotePhyIO                  0       0       0       0       0
0       0       0       0       0       0       0       0

STATS-NAME                    VALUE
BusyWaits                        98
LRUNumLocks                  401784
LRUNumSpinsWoTO                   0      0%
LRUNumSpinLoops                4315
LRUNumTimeOuts                 4315  -1.10%
BmapHTNumLocks                    0
BmapHTNumWaits                    0      0%
CacheTeamTimesWoken             182
CacheTeamNumAsleep               10
BmapHTMaxEntries               4096
BmapHTNEntries                   27
BmapHTNInserts                31954
BmapHTNCollisn                  203
BmapHTNFinds                  51419
BmapHTNHits                   19576
BmapHTNHits1                  19550
BmapHTNHits2                     26
BmapHTNClears                 31933
BmapHTNLChain                     1
BmapHTNRehash                     0
```

```
BlockmapMutexsNLocks              0
BlockmapMutexsNWaits              0
BlockmapUID                    3659
BlockmapUIDnallocs             3652
BlockmapRegEver               31851
BlockmapRegisters             31844
BufHTNBuckets                  4608
BufHTNEntries                  1208
BufHTNw2orMore                  158
BufHTMaxBucketSize               19
BufHTNFoiledOps                   0
IONumLocks                        0
IONumWaits                        0      0%

================================
Buffer Manager (Temporary)
================================

STATS-NAME                     TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
Finds                         31656       0       0       0       0
0       0       0       0       0       0    1022       0       0
Hits                          31655       0       0       0       0
0       0       0       0       0       0    1022       0       0
Hit%                            100       0       0       0       0
0       0       0       0       0       0     100       0       0
FalseMiss                     23898       0       0       0       0
0       0       0       0       0       0       0       0       0
UnOwnRR                           0       0       0       0       0
0       0       0       0       0       0       0       0       0
Cloned                            0       0       0       0       0
0       0       0       0       0       0       0       0       0
Creates                        5682       0       0       0       0
0       0       0       0       0       0    1048     716       0
Destroys                       5670       0       0       0       0
0       0       0       0       0       0     821      17       0
Dirties                        6702       0       0       0       0
0       0       0       0       0       0     379       0       0
RealDirties                    5692       0       0       0       0
0       0       0       0       0       0    1048     716       0
PrefetchReqs                      1       0       0       0       0
0       0       0       0       0       0       0       0       0
PrefetchNotInMem                  1       0       0       0       0
0       0       0       0       0       0       0       0       0
PrefetchInMem                   446       0       0       0       0
0       0       0       0       0       0     446       0       0
Reads                             2       0       0       0       0       0
0       0       0       0       0       0       0       0
PReadBlks                      4096       0       0       0       0
0       0       0       0       0       0       0       0       0
PReadKB                           0       0       0       0       0
0       0       0       0       0       0       0       0       0
ReReads                           2       0       0       0       0
0       0       0       0       0       0       0       0       0
Writes                           10       0       0       0       0
0       0       0       0       0       0       0       0       0
```

```
PWriteBlks                      80       0       0       0       0
0       0       0       0       0       0       0       0       0
PWriteKB                         0       0       0       0       0
0       0       0       0       0       0       0       0       0
GrabbedDirty                     0       0       0       0       0
0       0       0       0       0       0       0       0       0
ReadRemoteRpc                    0       0       0       0       0
0       0       0       0       0       0       0       0       0
ReadRemotePhyIO                  0       0       0       0       0
0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)        BARRAY  BLKMAP    HASH    CKPT      BM
TEST    CMID    RIDCA     LOB  LVCRID    FILE  RIDMAP   RVLOG
Finds                            0    8569     124       0   21939
0       0       0       0       0       2       0       0
Hits                             0    8569     124       0   21939
0       0       0       0       0       1       0       0
Hit%                             0     100     100       0     100
0       0       0       0       0      50       0       0
FalseMiss                        0    8569       0       0   15328
0       0       0       0       0       1       0       0
UnOwnRR                          0       0       0       0       0
0       0       0       0       0       0       0       0
Cloned                           0       0       0       0       0
0       0       0       0       0       0       0       0
Creates                          0    1440     777       0    1041
0       0       0       0       0       0     660       0
Destroys                         0    1434     777       0     123
0       0       0       0       0       0     660       0
Dirties                          0       0       0       0    6323
0       0       0       0       0       0       0       0
RealDirties                      0    1440     777       0    1051
0       0       0       0       0       0     660       0
PrefetchReqs                     0       0       0       0       0
0       0       0       0       0       1       0       0
PrefetchNotInMem                 0       0       0       0       0
0       0       0       0       0       1       0       0
PrefetchInMem                    0       0       0       0       0
0       0       0       0       0       0       0       0
Reads                          0       0       0       0       0       0
0       0       0       0       2       0       0
PReadBlks                        0       0       0       0       0
0       0       0       0       0    4096       0       0
PReadKB                          0       0       0       0       0
0       0       0       0       0       0       0       0
ReReads                          0       0       0       0       0
0       0       0       0       0       2       0       0
Writes                           0       0       0       0      10
0       0       0       0       0       0       0       0
PWriteBlks                       0       0       0       0      80
0       0       0       0       0       0       0       0
PWriteKB                         0       0       0       0       0
0       0       0       0       0       0       0       0
GrabbedDirty                     0       0       0       0       0
0       0       0       0       0       0       0       0
ReadRemoteRpc                    0       0       0       0       0
```

```
0       0       0       0       0       0       0       0
ReadRemotePhyIO                 0       0       0       0       0
0       0       0       0       0       0       0       0

STATS-NAME                    VALUE
BusyWaits                         0
LRUNumLocks                  136253
LRUNumSpinsWoTO                   0      0%
LRUNumSpinLoops                2780
LRUNumTimeOuts                 2780  -0.02%
BmapHTNumLocks                    0
BmapHTNumWaits                    0      0%
CacheTeamTimesWoken               1
CacheTeamNumAsleep               10
BmapHTMaxEntries               4096
BmapHTNEntries                   17
BmapHTNInserts                 2334
BmapHTNCollisn                    0
BmapHTNFinds                    183
BmapHTNHits                       0
BmapHTNHits1                      0
BmapHTNHits2                      0
BmapHTNClears                  2327
BmapHTNLChain                     0
BmapHTNRehash                     0
BlockmapMutexsNLocks              0
BlockmapMutexsNWaits              0
BlockmapUID                    2380
BlockmapUIDnallocs             2335
BlockmapRegEver                2344
BlockmapRegisters              2334
BufHTNBuckets                  4608
BufHTNEntries                    24
BufHTNw2orMore                    0
BufHTMaxBucketSize                3
BufHTNFoiledOps                   0
IONumLocks                        0
IONumWaits                        0      0%
```

示例 3:

在 20 分钟后显示缓冲池（主存储和临时存储）的输出。

```
sp_iqsysmon '00:20:00', 'mbufpool tbufpool'

==============================
Buffer Pool (Main)
==============================

STATS-NAME                    TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
MovedToMRU                 68731       0       0       0       0    9094
2767       0   21083        0       0       0       0     303
MovedToWash                    0       0       0       0       0
0       0       0       0       0       0       0       0       0
RemovedFromLRU             67564       0       0       0       0
```

```
9020    2597       0   20830       0       0       0       0     274
RemovedFromWash             11457       0       0       0       0
1559     356       0    2189       0       0       0       0      68
RemovedInScanMode               0       0       0       0       0
0       0       0       0       0       0       0       0       0
MovedToPSList                   0       0       0       0       0
0       0       0       0       0       0       0       0       0
RemovedFromPSList               0       0       0       0       0
0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)        BARRAY  BLKMAP    HASH    CKPT      BM
TEST    CMID   RIDCA     LOB  LVCRID    FILE  RIDMAP   RVLOG
MovedToMRU                   2169    8561       0       0   24754
0       0       0       0       0       0       0       0
MovedToWash                     0       0       0       0       0
0       0       0       0       0       0       0       0
RemovedFromLRU               2065    8330       0       0   24448
0       0       0       0       0       0       0       0
RemovedFromWash               233    1437       0       0    5615
0       0       0       0       0       0       0       0
RemovedInScanMode               0       0       0       0       0
0       0       0       0       0       0       0       0
MovedToPSList                   0       0       0       0       0
0       0       0       0       0       0       0       0
RemovedFromPSList               0       0       0       0       0
0       0       0       0       0       0       0       0

STATS-NAME                  VALUE
Pages                        2787
InUse                        1208 ( 43.3% )
Dirty                          11 ( 0.4% )
Pinned                         19 ( 0.7% )
Flushes                         0
FlushedBufferCount              0
GetPageFrame                 1605
GetPageFrameFailure             0
GotEmptyFrame                1605
Washed                          0
TimesSweepersWoken              0
PriorityWashed                  0
NPrioritySweepersWoken          0
washTeamSize                   10
WashMaxSize                   455 ( 16.3% )
washNBuffers                  455 ( 16.3% )
washNDirtyBuffers               0 ( 0.0% )
washSignalThreshold            46 ( 1.7% )
washNActiveSweepers             0
NPriorityWashBuffers            0
NActivePrioritySweepers         0
washIntensity                   0
FlushAndEmpties                 0
EmptiedBufferCount              0
EmptiedSkippedCount             0
EmptiedWriteCount               0
EmptiedErrorCount               0
nAffinityTotal                  0 ( 0.0% )
```

```
nAffinityArea                    0 ( 0.0% )

==============================
Buffer Pool (Temporary)
==============================

STATS-NAME                    TOTAL    NONE  TXTPOS  TXTDOC  CMPACT
BTREEV  BTREEF      BV     VDO   DBEXT    DBID    SORT   STORE  GARRAY
MovedToMRU                   30514       0       0       0       0
0       0       0       0       0       0    1218     696       0
MovedToWash                    258       0       0       0       0
0       0       0       0       0       0       0     256       0
RemovedFromLRU               30506       0       0       0       0
0       0       0       0       0       0    1218     694       0
RemovedFromWash              30503       0       0       0       0
0       0       0       0       0       0    1218     694       0
RemovedInScanMode                0       0       0       0       0
0       0       0       0       0       0       0       0       0
MovedToPSList                    0       0       0       0       0
0       0       0       0       0       0       0       0       0
RemovedFromPSList                0       0       0       0       0
0       0       0       0       0       0       0       0       0

STATS-NAME (cont'd)         BARRAY  BLKMAP    HASH    CKPT      BM
TEST    CMID    RIDCA      LOB  LVCRID    FILE  RIDMAP   RVLOG
MovedToMRU                       0    8575     124       0   19898
0       0       0       0       0       3       0       0
MovedToWash                      0       0       0       0       0
0       0       0       0       0       2       0       0
RemovedFromLRU                   0    8569     124       0   19898
0       0       0       0       0       3       0       0
RemovedFromWash                  0    8569     124       0   19898
0       0       0       0       0       0       0       0
RemovedInScanMode                0       0       0       0       0
0       0       0       0       0       0       0       0
MovedToPSList                    0       0       0       0       0
0       0       0       0       0       0       0       0
RemovedFromPSList                0       0       0       0       0
0       0       0       0       0       0       0       0

STATS-NAME                   VALUE
Pages                         2787
InUse                           24 ( 0.9% )
Dirty                           17 ( 0.6% )
Pinned                           4 ( 0.1% )
Flushes                          0
FlushedBufferCount               0
GetPageFrame                  5684
GetPageFrameFailure              0
GotEmptyFrame                 5684
Washed                           0
TimesSweepersWoken               0
PriorityWashed                   0
NPrioritySweepersWoken           0
washTeamSize                    10
WashMaxSize                    455 ( 16.3% )
```

```
washNBuffers                    20 ( 0.7% )
washNDirtyBuffers               13 ( 0.5% )
washSignalThreshold             46 ( 1.7% )
washNActiveSweepers              0
NPriorityWashBuffers             0
NActivePrioritySweepers          0
washIntensity                    0
FlushAndEmpties                  0
EmptiedBufferCount               0
EmptiedSkippedCount              0
EmptiedWriteCount                0
EmptiedErrorCount                0
nAffinityTotal                   0 ( 0.0% )
nAffinityArea                    0 ( 0.0% )
```

示例 4：

在 20 分钟后显示预取管理器（主存储和临时存储）的输出。

```
sp_iqsysmon '00:20:00', 'mprefetch tprefetch'

==============================
Prefetch Manager (Main)
==============================

STATS-NAME                   VALUE
PFMgrNThreads                   10
PFMgrNSubmitted                 81
PFMgrNDropped                    0
PFMgrNValid                      0
PFMgrNRead                       1
PFMgrNReading                    0
PFMgrCondVar              Locks  0  Lock-Waits 0 ( 0.0% )  Signals 0
Broadcasts  2  Waits  2

==============================
Prefetch Manager (Temporary)
==============================

STATS-NAME                   VALUE
PFMgrNThreads                   10
PFMgrNSubmitted                  1
PFMgrNDropped                    0
PFMgrNValid                      0
PFMgrNRead                       1
PFMgrNReading                    0
PFMgrCondVar              Locks  0  Lock-Waits 0 ( 0.0% )  Signals 0
Broadcasts  2  Waits  2
```

示例 5：

在 20 分钟后显示 IQ 存储库空闲列表（主存储和临时存储）的输出。

```
sp_iqsysmon '00:20:00', 'mfreelist tfreelist'

==============================
IQ Store (Main) Free List
```

```
==============================

STATS-NAME                   VALUE
FLBitCount                   74036
FLIsOutOfSpace                 NO
FLMutexLocks                    0
FLMutexWaits                    0 ( 0.0% )

==============================
IQ Store (Temporary) Free List
==============================

STATS-NAME                   VALUE
FLBitCount                    4784
FLIsOutOfSpace                 NO
FLMutexLocks                    0
FLMutexWaits                    0 ( 0.0% )
```

示例 6:

在 20 分钟后显示内存管理器、线程管理器、CPU 利用率以及事务管理器的输出。

```
sp_iqsysmon '00:20:00', 'memory threads cpu txn'

==============================
Memory Manager
==============================

STATS-NAME                       VALUE
MemAllocated                  67599536  ( 66015 KB )
MemAllocatedMax              160044816 ( 156293 KB )
MemAllocatedEver            1009672456 ( 986008 KB )
MemNAllocated                    77309
MemNAllocatedEver               914028
MemNTimesLocked                      0
MemNTimesWaited                      0      ( 0.0 %)

==============================
Thread Manager
==============================

STATS-NAME                       VALUE
ThrNumOfCpus                         4
ThreadLimit                         99
ThrNumThreads                       98     ( 99.0 %)
ThrReserved                         15     ( 15.2 %)
ThrNumFree                          55     ( 55.6 %)
NumThrUsed                          44     ( 44.4 %)
UsedPerActiveCmd                    22
ThrNTeamsInUse                       5
ThrMaxTeams                          7
NumTeamsAlloc                      238
TeamThrAlloc                       421
SingleThrAlloc                     492
ThrMutexLocks                        0
ThrMutexWaits                        0      ( 0.0 %)
```

```
==============================
CPU time statistics
==============================

STATS-NAME                      VALUE
Elapsed Seconds                 59.65     ( 25.0 %)
CPU User Seconds                37.79     ( 15.8 %)
CPU Sys Seconds                  1.89      ( 0.8 %)
CPU Total Seconds               39.68     ( 16.6 %)

==============================
Transaction Manager
==============================

STATS-NAME                      VALUE
TxnMgrNPending                      0
TxnMgrNBlocked                      2
TxnMgrNWaiting                      0
TxnMgrPCcondvar               Locks     0      Lock-Wait 0 ( 0.0 %)
Signals 0  Broadcasts 2 Waits 2
TxnMgrTxnIDseq                    407
TxnMgrtxncblock                Locks     0       Lock-Wait 0 ( 0.0 %)
TxnMgrVersionID                     0
TxnMgrOAVI                          0
TxnMgrVersionLock             Locks     0      Lock-Wait 0 ( 0.0 %)
Signals 0  Broadcasts 0 Waits 0
```

示例 7:

在 20 分钟后显示服务器上下文和目录统计信息的输出。

```
sp_iqsysmon '00:20:00', 'context catalog'

==============================
Context Server statistics
==============================

STATS-NAME                  VALUE
StCntxNumConns                  1
StCntxNResource                16
StCntxNOrigResource            18
StCntxNWaiting                  0
StCntxNWaited                   0
StCntxNAdmitted              1116
StCntxLock                  Locks  0 Lock-Waits  0 ( 0.0 %)
StCntxCondVar               Locks  0 Lock-Waits  0 ( 0.0 %)

==============================
Catalog, DB Log, and Repository statistics
==============================

STATS-NAME                  VALUE
CatalogLock             RdLocks  0   RdWaits  0 ( 0.0 %)  RdTryFails
0  WrLocks  30037  WrWaits  0 ( 0.0 %)  WrTryFail 0
DbLogMLock                  Locks  0 Lock-Waits  0 ( 0.0 %)
```

```
DbLogSLock                    Locks  0 Lock-Waits  0 ( 0.0 %)
RepositoryNList                   0
RepositoryLock              Locks  1  SpinsWoTO  0 ( 0.0 %)     Spins
0  TimeOuts     0 ( 0.0 %)
```

示例 8：

在 20 分钟后显示 IQ RLV 内存存储库和大容量内存分配器 (LMA) 统计信息的输出。

```
sp_iqsysmon '00:20:00', 'rlv lma'

==============================
IQ In-Memory Store
==============================

STATS-NAME               VALUE
RLV Memory Limit       2048 MB
RLV Memory Used           0 MB
RLV Chunks Used              0

==============================
Large Memory Allocator
==============================

STATS-NAME               VALUE
Large Memory Space     2048 MB
Large Memory Max Fle    512 MB
Large Memory Num Fle          0
Large Memory Flexibl        0.5
Large Memory Flexibl      0 MB
Large Memory Inflexi        0.9
Large Memory Inflexi      0 MB
Large Memory Anti-St        0.5
Large Memory Num Con          0
```

sp_iqpassword 过程

更改用户口令。

语法 1

```
call sp_iqpassword ( 'caller_password' , 'new_password' [,
'user_name' ])
```

语法 2

```
sp_iqpassword 'caller_password' , 'new_password' [, 'user_ name' ]
```

参数

- **caller_password** – 您的口令。在您更改自己的口令时，该口令是您的旧口令。如果具有 CHANGE PASSWORD 系统特权的用户要更改其他用户的口令，caller_password 则为执行更改的用户口令。
- **new_password** – 用户的新口令或 *loginname* 的新口令。

- **user_name** – 要由具有 CHANGE PASSWORD 系统特权的另一用户更改口令的用户的登录名。更改自己的口令时，请勿指定 user_name。

特权

您必须具有系统过程的 EXECUTE 特权。设置自己的口令不需要具备其它系统特权。设置其他用户的口令需具备 CHANGE PASSWORD 系统特权。

注释

用户口令是一个标识符。任何用户均可使用 **sp_iqpassword** 来更改自己的口令。更改任何现有用户的口令需具备 CHANGE PASSWORD 系统特权。

标识符的最大长度是 128 个字节。当以下任一条件成立时，标识符必须用双引号引起来或用中括号括起来：

- 标识符包含空格。
- 标识符的首字符不是字母字符（定义将在后面提供）。
- 标识符包含保留字。
- 标识符包含字母和数字以外的其它字符。

  *字母字符*包括字母表中的字母，以及下划线 (_)、at 符号 (@)、井号 (#) 和美元符号 ($)。数据库归类序列指出了哪些字符被视为字母字符或数字字符。

示例

将已登录用户的口令从 irk103 更改为 exP984：

```
sp_iqpassword 'irk103', 'exP984'
```

如果已登录用户具有 CHANGE PASSWORD 系统特权或该用户为用户 `joe`，将用户 `joe` 的口令从 `eprr45` 更改为 `pdi032`：

```
call sp_iqpassword ('eprr45', 'pdi932', 'joe')
```

sp_objectpermission 系统过程

生成有关授予指定角色或用户名的对象特权或者授予指定对象或 dbspace 的对象特权的报告。

语法

sp_objectpermission ([*object_name*], [*object_owner*], [*object_type*])

参数

- **object_name** – 对象、dbspace、用户或角色的名称。如果未指定，则报告当前用户的对象特权。缺省值为 NULL。
- **object_owner** – 指定对象名称的对象所有者的名称。显示由指定对象所有者拥有的指定对象的对象特权。必须指定该参数以获取由另一用户或角色所拥有的对象的对象特权。缺省值为 NULL。
- **object_type** – 有效值包括：

- TABLE*
- VIEW
- MATERIALIZED VIEW
- SEQUENCE
- PROCEDURE
- FUNCTION
- DBSPACE
- USER

注意： *同时显示列级别的对象特权。

如果未指定任何值，则返回所有对象类型的特权。缺省值为 NULL。

特权

您必须具有系统过程的 EXECUTE 特权。 任何用户都可以执行 **sp_objectpermission** 以获取授予自己的所有对象特权。对象所有者也可以执行此过程来获取其自身拥有的对象的对象特权。要获取以下对象特权，还需具备其它系统特权：

- **授予其它用户或授权其它用户拥有的对象的对象特权** – 您还要必须具有 MANAGE ANY OBJECT PRIVILEGE 系统特权
- **授予角色拥有的对象或授予角色的对象特权** – 您还要必须具有 MANAGE ANY OBJECT PRIVILEGE 系统特权或成为角色的角色管理员
- **dbspace 的对象特权** – 您必须具有 MANAGE ANY DBSPACE 系统特权

注释

列名	数据类型	说明
授予者	char(128)	授予者的用户 ID
grantee	char(128)	被授予者的用户 ID
object_name	char(128)	对象的名称
owner	char(128)	对象所有者的名称
object_type	char(20)	对象的类型
column_name	char(128)	列的名称
permission	char(20)	特权名称
grantable	char(1)	特权是否可授予

所有参数均为可选，并可生成以下报告：

- 如果输入为对象（表、视图、过程、函数、序列等），该过程将列出对该对象具有不同对象特权的所有角色和用户。

- 如果输入为角色或用户，该过程将列出授予该角色或输入的所有对象特权。通过执行 **sp_objectpermission** 来显示用户或角色的对象特权时，也将显示通过角色授予继承而来的对象特权。
- 如果输入为 dbspace 名称，该过程将列出对指定 dbspace 具有 CREATE 特权的所有用户或角色。
- 缺省情况下，对象类型为 NULL，并将显示与指定对象名称匹配的所有现有对象类型的对象特权。

示例

执行下面的 GRANT 语句：

```
GRANT SERVER OPERATOR TO r4;
GRANT BACKUP DATABASE TO r3 WITH ADMIN OPTION;
GRANT DROP CONNECTION TO r3 WITH ADMIN ONLY OPTION;
GRANT MONITOR TO r2;GRANT CHECKPOINT TO r1;
GRANT ROLE r2 TO r1 WITH ADMIN OPTION;
GRANT ROLE r3 TO r2 WITH NO ADMIN OPTION;
GRANT ROLE r4 TO r3 WITH ADMIN ONLY OPTION;
```

假设具有以下对象特权：

- `r5` 在数据库中拥有一个名为 `test_tab` 的表和一个名为 `test_proc` 的过程。
- 对 `r5` 拥有管理权限的 `u5` 授予以下特权：
  - GRANT SELECT ON r5.test_tab TO r2 WITH GRANT OPTION;
  - GRANT SELECT (c1), UPDATE (c1) ON r5.test_tab TO r6 WITH GRANT OPTION;
  - GRANT EXECUTE ON r5.test_proc TO r3;
- 对 `r6` 拥有管理权限的 `u6` 授予以下特权：
  - GRANT SELECT (c1), REFERENCES (c1) ON r5.test_tab TO r3;

如果执行 `sp_objectpermission( 'r1' )`，输出将如下所示：

表 21. 示例 sp_objectpermission('r1') 输出

授予者	grantee	object_name
u5	r2	test_tab
u6	r3	test_tab
u6	r3	test_tab
u6	r3	test_proc

（继续）owner	object_type	授予者
r5	TABLE	u5
r5	COLUMN	u6
r5	COLUMN	u6
r5	PROCEDURE	u6

（继续）可授予	column_name	privilege
Y	NULL	SELECT
N	c1	SELECT
Y	c1	REFERENCES
N	NULL	EXECUTE

如果执行 `sp_objectpermission( ‘test_tab’, ‘r5’, ‘table’ )`，输出将如下所示：

表 22. 示例 sp_objectpermission(‘test_tab’, ‘r5’, ‘table’) 输出

授予者	grantee	object_name
u5	r2	test_tab
u5	r6	test_tab
u5	r6	test_tab
u6	r3	test_tab
u6	r3	test_tab

（继续）owner	object_type	授予者
r5	TABLE	u5
r5	COLUMN	u5
r5	COLUMN	u5

（继续）owner	object_type	授予者
r5	COLUMN	u6
r5	COLUMN	u6

（继续）column_name	privilege	可授予
NULL	SELECT	Y
c1	SELECT	Y
c1	UPDATE	Y
c1	SELECT	N
c1	REFERENCES	N

sp_sys_priv_role_info 系统过程

生成系统特权到相应系统角色的映射报告。为每个系统特权返回单独的行。

语法

sp_sys_priv_role_info()

特权

您必须具有系统过程的 EXECUTE 特权。

注释

列名	数据类型	说明
sys_priv_name	char(128)	系统特权的名称。
sys_priv_role_name	char(128)	与系统特权对应的角色名称。
sys_priv_id	unsigned int	系统特权的 ID。

sp_alter_secure_feature_key 系统过程

通过修改验证密钥和/或功能列表更改以前定义的安全功能密钥。

语法

```
sp_alter_secure_feature_key （
    name,
    auth_key,
    features )
```

参数

- **name** – 要变更的安全功能密钥的 VARCHAR (128) 名称。必须已经存在具有给定名称的密钥。
- **auth_key** – 安全功能密钥的 CHAR (128) 验证密钥。验证密钥必须为至少六个字符的非空字符串，或者为 NULL，NULL 表示不更改现有的验证密钥。
- **features** – 安全功能的 LONG VARCHAR 列表，以逗号分隔，可由密钥启用。feature_list 可为 NULL，表示不更改现有 feature_list。

特权
您必须具有系统过程的 EXECUTE 特权。此外，您必须是数据库服务器的所有者，并且已为连接启用 manage_keys 功能。

注释
此过程允许您变更现有安全功能密钥的验证密钥或功能列表。

sp_create_secure_feature_key 系统过程

创建新的安全功能密钥。

语法

```
sp_create_secure_feature_key （
    name,
    auth_key,
    features )
```

参数

- **name** – 新安全功能密钥的 VARCHAR (128) 名称。此参数不能为 NULL 或空字符串。
- **auth_key** – 安全功能密钥的 CHAR (128) 验证密钥。验证密钥必须为至少六个字符的非空字符串。
- **features** – 安全功能的 LONG VARCHAR 列表，以逗号分隔，可由新密钥启用。在功能之前指定 "-" 表示该功能在设置安全功能密钥时不重新启用。

特权
您必须具有系统过程的 EXECUTE 特权。此外，您必须是数据库服务器的所有者，并且已为连接启用 manage_keys 功能。

注释
此过程创建的新安全功能密钥可授予任何用户。系统安全功能密钥使用 -sk 数据库服务器选项进行创建。

sp_drop_secure_feature_key 系统过程

删除安全功能密钥。

语法

```
sp_drop_secure_feature_key ( name )
```

参数

- **name** – 要删除的安全功能密钥的 VARCHAR (128) 名称。

特权
您必须具有系统过程的 EXECUTE 特权。此外，您必须是数据库服务器的所有者，并且已为连接启用 manage_keys 功能。

注释
如果指定的密钥不存在，则返回一条错误。如果指定的密钥存在，只要它不是允许管理安全功能和安全功能密钥的最后一个安全功能密钥，就会将其删除。例如，不能删除系统安全功能密钥，除非有另一个密钥已启用 manage_features 和 manage_keys 安全功能。

sp_list_secure_feature_keys 系统过程

返回有关目录内容的信息。

语法

```
sp_list_secure_feature_keys ( )
```

特权
您必须具有系统过程的 EXECUTE 特权。此外，您必须是数据库服务器的所有者，并且已为连接启用 manage_keys 功能。

注释

列名	数据类型	说明
name	VARCHAR(128)	安全功能密钥的名称。
features	LONG VARCHAR	通过安全功能密钥启用的安全功能。

此过程返回现有安全功能密钥的名称，以及可通过每个密钥启用的安全功能集。

如果用户已启用 manage_features 和 manage_keys 安全功能，则该过程将返回所有安全功能密钥的列表。

如果用户仅启用了 manage_keys 安全功能，则该过程返回功能或功能子集与当前用户所启用功能相同的密钥。

sp_use_secure_feature_key 系统过程

启用现有安全功能密钥。

语法

```
sp_use_secure_feature_key ( name, sfkey)
```

参数

- **name** – 要启用的安全功能密钥的 VARCHAR (128) 名称。
- **sfkey** – 要启用的安全功能密钥的 CHAR (128) 验证密钥。验证密钥必须至少六个字符。

特权
您必须具有系统过程的 EXECUTE 特权。

注释
该过程将启用由指定安全功能密钥启动的安全功能密钥。

附录：启动和连接参数

start_iq 实用程序的启动选项和连接参数的参考资料。

-ec iqsrv16 数据库服务器选项

使用传送层安全或简单加密对往来于所有客户端的所有命令序列通信协议包（例如 DBLib 和 ODBC）进行加密。不加密 TDS 包。

语法

```
iqsrv16 -ec encryption-options ...
```

```
encryption-options :
```

```
{ NONE |
   SIMPLE |
   TLS ( [ FIPS={ Y | N }; ]
   IDENTITY=server-identity-filename;
   IDENTITY_PASSWORD=password ) }, ...
```

允许值

- **NONE** – 接受未加密的连接。
- **SIMPLE** – 接受使用简单加密技术加密的连接。所有平台以及以前版本的数据库服务器和客户端都支持此类加密。简单加密不提供服务器验证、RSA 加密或其它传送层安全性功能。
- **TLS** – 接受使用 RSA 加密技术加密的连接。TLS 参数接受以下参数：
  - **FIPS** – 对于 FIPS 认证的 RSA 加密，请指定 `FIPS=Y`。RSA FIPS 认证的加密使用单独的认证库，但是与指定 RSA 的 9.0.2 或更高版本的客户端兼容。

    有关 FIPS 认证组件的列表，请参见 http://www.sybase.com/detail?id=1061806。

    算法必须与用于创建证书的加密匹配。
  - ***server-identity-filename*** – 是服务器身份证书的路径和文件名。如果使用 FIPS 认证的 RSA 加密，必须使用 RSA 算法生成证书。
  - ***password*** – 是服务器专用密钥的口令。在创建服务器证书时指定此口令。

适用于

NONE 和 SIMPLE 适用于所有服务器和操作系统。

TLS 适用于所有服务器和操作系统。

有关支持 FIPS 认证的加密的信息，请参见 http://www.sybase.com/detail?id=1061806。

注释
您可以使用此选项，利用传送层安全功能来保护客户端应用程序和数据库服务器之间传输的通信包的安全。

-ec 选项指示数据库服务器只接受使用一种指定类型进行加密的连接。必须指定至少一个逗号分隔的列表中的受支持的参数。无论是否使用 -ec 选项，将始终接受通过 TDS 协议建立的连接（包括使用 jConnect 的 Java 应用程序），并从不对其进行加密。如果将 TDS 协议选项设置为 NO，则不允许建立这些未加密的 TDS 连接。

缺省情况下，通信包是不加密的，但这样可能会引起潜在的安全风险。如果您注重网络包的安全性，可使用 -ec 选项。加密对于性能只有很轻微的影响。

如果数据库服务器接受简单加密，但不接受未加密的连接，则所有未使用加密的非 TDS 连接尝试会自动使用简单加密。

使用 `-ec SIMPLE` 启动数据库服务器将通知数据库服务器仅接受使用简单加密的连接。TLS 连接（RSA 和 FIPS 认证的 RSA 加密）将失败，无加密要求的连接会使用简单加密。

如果想要数据库服务器接受通过 TCP/IP 的加密连接，但还希望能够从本地计算机上通过共享内存连接到数据库，则可在启动数据库服务器时指定 -es 选项以及 -ec 选项。

`dbrsa16.dll` 文件中包含用于加密和解密的 RSA 代码。文件 `dbfips16.dll` 含有用于 FIPS 认证的 RSA 算法的代码。连接数据库服务器时，如果找不到合适的文件或者发生错误，则会在数据库服务器消息窗口中显示一条消息。如果无法启动指定类型的加密，则该服务器不启动。

客户端和服务器的加密设置必须匹配，否则连接将失败，但以下情况除外：

- 如果在数据库服务器上指定了 -ec SIMPLE，但未指定 -ec NONE，则不要求加密的连接可以连接并自动使用简单加密。
- 如果数据库服务器指定了 RSA，客户端指定了 FIPS 认证的加密，或者相反，则连接将成功。这些情况下，[Encryption] 连接属性将返回数据库服务器所指定的值。

注意： 所有高度加密技术受出口法规约束。

示例

以下示例显示允许不使用加密的连接和使用简单加密的连接。

```
iqsrv16 -ec NONE,SIMPLE -x tcpip c:\mydemo.db
```

以下示例启动一个使用 RSA 服务器证书 `rsaserver.id` 的数据库服务器。

```
iqsrv16 -ec TLS(IDENTITY=rsaserver.id;IDENTITY_PASSWORD=test) -x
tcpip c:\mydemo.db
```

以下示例启动一个使用 FIPS 认可的 RSA 服务器证书 `rsaserver.id` 的数据库服务器。

```
iqsrv16 -ec TLS(FIPS=Y;IDENTITY=rsaserver.id;IDENTITY_PASSWORD=test)
-x tcpip c:\mydemo.db
```

-es iqsrv16 数据库服务器选项

允许在共享内存上进行未加密的连接。

语法

```
iqsrv16 -ec encryption-options -es ...
```

适用于
所有服务器和操作系统。

注释
仅当使用 -ec 选项指定时，此选项才有效。-es 选项指示数据库服务器通过共享内存允许未加密的连接。通过 TCP/IP 的连接必须使用 -ec 选项指定的加密类型。此选项对于想要远程客户端使用加密连接的情况非常有用，但出于性能方面的原因，最好从本地计算机使用未加密的连接访问数据库。

示例

以下示例指定允许使用简单加密的连接以及未加密的共享内存连接。

```
iqsrv16 -ec SIMPLE -es -x tcpip c:\mydemo.db
```

TDS 通信参数

控制服务器是否允许 TDS 连接。

用法
TCP/IP，NamedPipes（仅限服务器端）

值
YES, NO

缺省值
YES

描述
要禁止与数据库服务器建立 TDS 连接，请将 TDS 设置为 NO。如果希望确保仅与服务器建立加密连接，则这些端口选项是禁止建立 TDS 连接的唯一方法。

示例

以下命令使用 TCP/IP 协议启动数据库服务器，但是禁止从 Open Client 或 jConnect 应用程序连接。

```
start_iq -x tcpip(TDS=NO) ...
```

索引

符号

A

B

C

D

E

F

G

H

I

J

K

L

M

T

U

V

W

X

Y

Z