SQL Server 伺服器角色與資料庫角色類型說明

伺服器角色 (Server Roles)

角色名稱	說明	主要權限
sysadmin	系統管理員	可在 SQL Server 執行個體上執行任何活動，最高權限角色
serveradmin	伺服器管理員	可變更伺服器範圍組態選項和關閉伺服器
securityadmin	安全性管理員	管理登入帳戶、密碼政策和讀取錯誤記錄
processadmin	處理程序管理員	可結束 SQL Server 執行個體中執行的處理程序
setupadmin	安裝管理員	可新增和移除連結的伺服器及執行某些系統預存程序
bulkadmin	大量匯入管理員	可執行 BULK INSERT 陳述式
diskadmin	磁碟管理員	管理磁碟檔案
dbcreator	資料庫建立者	可建立、修改、刪除和還原任何資料庫
public	公用角色	每個 SQL Server 登入都屬於 public 角色，無法移除

資料庫角色 (Database Roles)

角色名稱	說明	主要權限
db_owner	資料庫擁有者	可執行資料庫內的所有組態與維護活動
db_securityadmin	安全性管理員	可管理資料庫中的角色成員資格和權限
db_accessadmin	存取管理員	可新增或移除使用者對資料庫的存取權
db_backupoperator	備份操作員	可備份資料庫
db_ddladmin	DDL 管理員	可在資料庫中執行任何 DDL 操作
db_datawriter	資料寫入者	可在所有使用者資料表中新增、刪除或變更資料
db_datareader	資料讀取者	可從所有使用者資料表讀取資料
db_denydatawriter	拒絕資料寫入者	不能新增、修改或刪除資料表中的資料
db_denydatareader	拒絕資料讀取者	不能讀取使用者資料表中的資料
public	資料庫公用角色	每個資料庫使用者都屬於此角色，無法移除

特殊用途的資料庫角色

角色名稱	資料庫	說明
db_ssisadmin	msdb	管理 SSIS 套件
db_ssisltduser	msdb	可檢視和執行 SSIS 套件但不能修改
db_ssisoperator	msdb	可列出和執行 SSIS 套件
db_dlcadmin	msdb	數據收集集管理員
db_dlcuser	msdb	數據收集集使用者
db_dlcreader	msdb	數據收集集讀取者
dbm_monitor	msdb	資料庫鏡像監視器
SQLAgentOperatorRole	msdb	SQL Server Agent 操作員角色
SQLAgentReaderRole	msdb	SQL Server Agent 讀取者角色
SQLAgentUserRole	msdb	SQL Server Agent 使用者角色
TargetServersRole	msdb	可管理主伺服器和目標伺服器
PolicyAdministratorRole	msdb	原則型管理管理員

使用者自訂角色 (User-Defined Roles)

角色類型	說明	建立方式
伺服器層級自訂角色	SQL Server 2014 及更新版本支援	`CREATE SERVER ROLE role_name [AUTHORIZATION server_principal]`
資料庫層級自訂角色	可根據業務需求自訂	`CREATE ROLE role_name [AUTHORIZATION database_principal]`
應用程式角色	提供應用程式特定的權限	`CREATE APPLICATION ROLE role_name WITH PASSWORD = 'password' [, DEFAULT_SCHEMA = schema_name]`

角色繼承與關係

角色關係	說明	範例
巢狀角色	角色可以是其他角色的成員	開發團隊角色可包含在專案管理角色中
權限衝突	DENY 權限優先於 GRANT 權限	若 DENY SELECT 給角色 A，即使 GRANT SELECT 給角色 B，且使用者同時屬於這兩個角色，使用者也無法執行 SELECT

角色關係	說明	範例
角色繼承	加入角色的成員繼承該角色的所有權限	加入 db_datareader 的使用者自動擁有所有表的讀取權限

角色管理最佳實踐

最佳實踐	說明	範例
最小權限原則	僅授與完成工作所需的最小權限	為報表使用者僅提供 db_datareader 角色
使用自訂角色	為特定業務需求建立自訂角色	`CREATE ROLE Sales_Manager`
避免直接授與權限	優先通過角色管理權限而非直接授與使用者	將使用者加入適當角色，而非直接授與表格權限
定期審核	定期檢查角色成員和權限	使用系統視圖如 `sys.server_role_members` 審核角色成員
分離權責	避免單一角色擁有過多權限	將資料修改和管理權限分配給不同角色