# **Database Security Standard**

The intent of this document is to define and describe the SQL Database Role and Permission

**Azure SQL Environment**

|  |  |
| --- | --- |
| **Naming** | **Environments** |
| PROD | PD, TR, DR |
| NP | LT, QA, EU |
| DEV | DV1, IN1,SB, SI |

**Azure SQL Database Roles and Permissions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Role Name** | **Database Permissions** | | |
| GZPDAppDeveloper | None |  |  |
| GZPDValidator | db\_datareader | ViewDefinition DB |  |
| GZPDAppAccount | db\_datareader | db\_datawriter | EXECUTE |
| GZPDSSRS | db\_datareader | EXECUTE |  |
| TDMPDrole | db\_datareader | VIEW ANY DEFINITION on User DB's |  |
| GZNPAppDeveloper | VIEW ANY DEFINITION | Read DB state | db\_datareader |
| GZNPValidator | db\_datareader | VIEW ANY DEFINITION on User DB's |  |
| GZNPAppAccount | db\_datareader | db\_datawriter | EXECUTE |
| GZNPSSRS | db\_datareader | EXECUTE |  |
| GZNpTDM | db\_datareader | db\_datawriter | VIEW ANY DEFINITION |
| GZDevAppDeveloper | db\_owner |  | VIEW ANY DEFINITION |
| GZDevDataValidator | db\_datareader | View Definition |  |
| GZDevAppAccount | db\_datareader | db\_datawriter | EXECUTE |
| GZDevSSRS | db\_datareader | EXECUTE |  |
| GZDevTDM | db\_datareader | db\_datawriter | VIEW ANY DEFINITION on User DB's |
| DBDeploy\_role |  | db\_owner |  |
| SplunkRole | VIEW ANY DEFINITION | read\_sql\_log |  |

# **SQL Server Database Security Standard Roles and Permissions**

The intent of this document is to define and describe the SQL Server Database Role and Permission in Azure IaaS and On-premises

|  |  |
| --- | --- |
| **Naming** | **Environments** |
| PROD | PD, TR, DR, AU |
| NP | USR, FT, FNST, LT, QA, EU, SR, TT |
| DEV | DV1, IN1, ED1, EI1, SB, SI |

* **If the server doesn't have the latest QC, please update Admin database with the latest permission related store procedures. You can update DBAUtil by running the following NP or PD version from the latest QC (QCZNP\_140\_Roles\_Permissions\_StoredProcedures\_on\_DBAUtil, QCZNP\_145\_Roles\_On\_Model\_Database, QCZNP\_150\_Create\_Roles\_On\_USER\_Databases and QCZNP\_155\_Mapping\_Standard\_Login\_To\_All\_Databases\_Except\_SSISDB)**

**Azure SQL Database Roles and Permissions**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Role Name** | **Interactive?** | **Database Permissions** | | |  |
| GZPDAppDeveloper | yes | None |  |  |  |
| GZPDValidator | yes | db\_datareader (DR Only) | ViewDefinition DB (DR Only) |  |  |
| GZPDAppAccount | no | db\_datareader | db\_datawriter | EXECUTE |  |
| GZPDSSRS | no | db\_datareader | EXECUTE |  |  |
| GZPDTDM | no | db\_datareader | VIEW ANY DEFINITION on User DB's |  |  |
| GZNPAppDeveloper | yes | db\_datareader | VIEW ANY DEFINITION on User DB's | Read DB state |  |
| GZNPValidator | yes | db\_datareader | VIEW ANY DEFINITION on User DB's |  |  |
| GZNPAppAccount | no | db\_datareader | db\_datawriter | EXECUTE |  |
| GZNPSSRS | no | db\_datareader | EXECUTE |  |  |
| GZNPTDM | no | db\_datareader | db\_datawriter | VIEW ANY DEFINITION on User DB's |  |
| GZDevAppDeveloper | yes | db\_owner | SSIS deploy | VIEW ANY DEFINITION and View Server State |  |
| GZDevDataValidator | yes | db\_datareader | View Definition |  |  |
| GZDevAppAccount | no | db\_datareader | db\_datawriter | EXECUTE |  |
| GZDevSSRS | no | db\_datareader | EXECUTE |  |  |
| GZDevTDM | no | db\_datareader | db\_datawriter | VIEW ANY DEFINITION on User DB's |  |
| DBDeploy\_role (ICAT) | no | db\_owner | ssis\_admin |  | Created by SQLDBA |
| SplunkRole | no | VIEW ANY DEFINITION | read\_sql\_log |  |  |
| ControlM\_Role | no | ssis\_admin | MSDB\_ownerView | START STOP JOBS | MSDB: db\_reader,  SQLAgentOperatorRole, SQLAgentReaderRole, SQLAgentUserRole SSIS:  ssis\_admin |
| SSIS\_validator\_Role (Dev and NP) | yes | db\_datareader | View catalog objects | Read Job Execution History (Use SSRS for PD) |  |
| SSIS\_Developer\_Role (Dev) | yes | ssis\_admin | db\_datareader |  |  |
| ProxyRole | no | ssis\_admin | MSDB\_admin | DatabaseMailUserRole |  |
| SplunkRole | no | VIEW ANY DEFINITION | read\_sql\_log |  |  |
| FiveTran | no |  |  |  | GZDevValidator    (db\_datareader  and  View Definition on user database), GZDevSSRS  role (db\_datareader  and EXECUTE) on MSDB and View Server State |
| GZDBAMonitoring | yes | VIEW ANY DATABASE  VIEW SERVER STATE  CONNECT ANY DATABASE  VIEW ANY DEFINITION  xp\_readerrorlog  xp\_sqlagent\_enum\_jobs | **DBAUtil:**  db\_owner  **MSDB:** SQLAgentOperatorRole  db\_datareader  **SSISDB:**  ssis\_admin  ssis\_logreader  db\_datareader |  | This role is intended for use by DBA team for system and job monitoring without granting sysadmin access or any access to user data. |