

# Database Roles

The **Database Roles** report displays all direct members of Database Roles on all SQL Server, Azure SQL Database, and Amazon RDS for SQL Server instances.

## Getting Started

Follow these steps to create a report:

1. Select the Date, Policy, and Baseline options from the Report Settings box.
2. Select a target instance.
3. Choose the **Level** (User or Member).
4. Select one of the choices of **AD Status** from the drop-down menu (All AD accounts, Active AD accounts, or Disabled AD accounts).
5. Click the **View Report** button to generate your report.



Assess and audit security risks and access rights

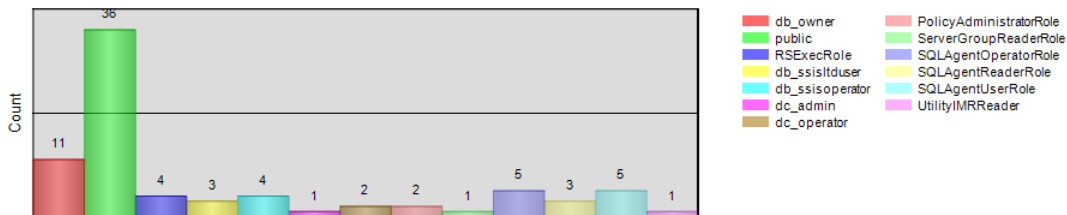
### Database Roles

Most current audit data as of Monday, September 12, 2022

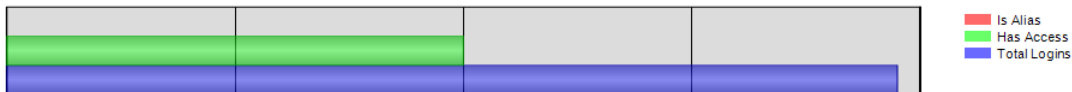
Server: All servers in policy

About: This report shows all direct members of Database Roles on all SQL Server, Azure SQL Database and Amazon RDS for SQL Server instances.

Fixed Role Login Count



Access Counts



Server	Database	Role	Member	Login Type	Access	Is Alias	Has Access
Server 1							
master							
db_owner							
			dbo	SQL Login		No	Yes
public							
			##MS_PolicyEventProcessingLogi	SQL Login		No	Yes
			n##				
			dbo	SQL Login		No	Yes
			guest	SQL Login		No	Yes
			INFORMATION_SCHEMA	SQL Login		No	No
			NT SERVICE\ReportServer	Windows User		No	Yes
			sys	SQL Login		No	No
RExecRole							
			NT SERVICE\ReportServer	Windows User		No	Yes
model							
db_owner							
			dbo	SQL Login		No	Yes
public							
			dbo	SQL Login		No	Yes
			guest	SQL Login		No	No
			INFORMATION_SCHEMA	SQL Login		No	No
			sys	SQL Login		No	No



## Note

Consider that the screenshot above was modified. You can find a complete view on the SQL Secure console.

[IDERA](#) | [Products](#) | [Purchase](#) | [Support](#) | [Community](#) | [Resources](#) | [About Us](#) | [Legal](#)