Required accounts and permissions

Required Accounts and Permissions

SQL Enterprise Job Manager connects to registered SQL Server instances and their host computers to collect information. The collection service requires permissions to connect and gather information using SQL connection credentials.

Depending on the level of access and actions you want SQL Enterprise Job Manager to perform on your environment, you should check you have the following permissions in each account:

Account	Action	Permissions required
Windows User Account	To install SQL Enterprise Job Manager components	Windows Administrator permission on the Target computer
	To create and access the SQL Enterprise Job Manager repository databases	• Create Database Rights on the target SQL Server Instance • Read and write privileges on the SQL Enterprise Job Manager Repository Databases
	To start or stop the SQL Server Agent	Windows Administrator permission on the computer running the SQL Server Agent service
SQL Server login account	For most SQL queries	VIEW SERVER STATE VIEW ANY DATABASE VIEW ANY DEFINITION
	To monitor database information	ALTER ANY DATABASE server level permission or CREATE DATABASE in the master database
	To start or stop the SQL Server Agent	sysadmin server roles
	To create and access the SQL Enterprise Job Manager repository databases	• Create Database Rights on the target SQL Server Instance • Read and write privileges on the SQL Enterprise Job Manager Repository Databases

IDERA suggests that you provide SQL connection credentials with "sysadmin" server roles if you want to be able to collect all information from your environment.