

Risk Assessment

The **Risk Assessment** report shows all policy and risk assessment results.

In this report, you can find a Risk Assessment summary detailing the following information:

- The **SQL Server** instance you are analyzing.
- The performed **Security Check**.
- The Risk Assessment **Findings**.
- The **Ref #**.
- The **Threshold** for each security check.

Getting Started

Follow these steps to create a report:

1. Select the Date, Policy, and Baseline options from the Report Settings box.
2. Select an assessment.
3. Select a target instance.
4. Check **Show Risks Only** to only show risks.
5. Click the **View Report** button to generate your report.



Assess and audit security risks and access rights

Risk Assessment

Policy Information

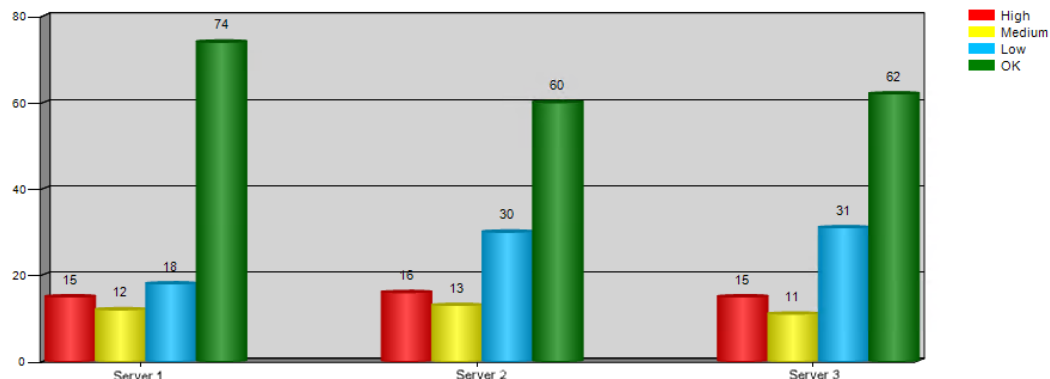
All Servers - Current

Global security checks that should be performed on all SQL Servers; based on the Idera Level 2 Balanced Protection policy.

Assessment Date: Most current audit data as of Tuesday, September 27, 2022

Assessment Results

Risk Assessment Summary



Severity Level: OK OK, low explained OK, medium explained OK, high explained Low Medium High

Assessment Information

SQL Server	Security Check	Finding	Category	Ref #	Threshold
Server 1					
	Was the most recent snapshot collected within an acceptable timeframe?	Audit data is within the selected date range.	Data Integrity	-	Audit data is acceptable if within 30 days of the selected date.
	Is SQL Server below the minimum acceptable version?	Current version is 15.0.2095.3	Configuration	CIS 1.1	Acceptable levels for each SQL Server version are '15.0.4138.2','14.0.3401.7','13.0.5888.11','12.0.6433.1','11.0.7507.2','10.50.6560','10.00.6556' and above.
Server 2					
	Was the most recent snapshot collected within an acceptable timeframe?	Audit data is within the selected date range.	Data Integrity	-	Audit data is acceptable if within 30 days of the selected date.
	Is SQL Server below the minimum acceptable version?	Current version is 14.0.3356.20	Configuration	CIS 1.1	Acceptable levels for each SQL Server version are '15.0.4138.2','14.0.3401.7','13.0.5888.11','12.0.6433.1','11.0.7507.2','10.50.6560','10.00.6556' and above.
	Is SQL Authentication enabled on the SQL Server?	SQL Server and Windows Authentication Mode	Login	-	Server is vulnerable if 'SQL Server and Windows Authentication Mode' is enabled.
Server 3					
	Was the most recent snapshot collected within an acceptable timeframe?	Audit data is within the selected date range.	Data Integrity	-	Audit data is acceptable if within 30 days of the selected date.
	Is SQL Server below the minimum acceptable version?	Current version is 14.0.3356.20	Configuration	CIS 1.1	Acceptable levels for each SQL Server version are '15.0.4138.2','14.0.3401.7','13.0.5888.11','12.0.6433.1','11.0.7507.2','10.50.6560','10.00.6556' and above.
	Is SQL Authentication enabled on the SQL Server?	SQL Server and Windows Authentication Mode	Login	-	Server is vulnerable if 'SQL Server and Windows Authentication Mode' is enabled.



Note

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

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