

SQL Vulnerability Assessment for Azure SQL Database AND on-premises SQL Server

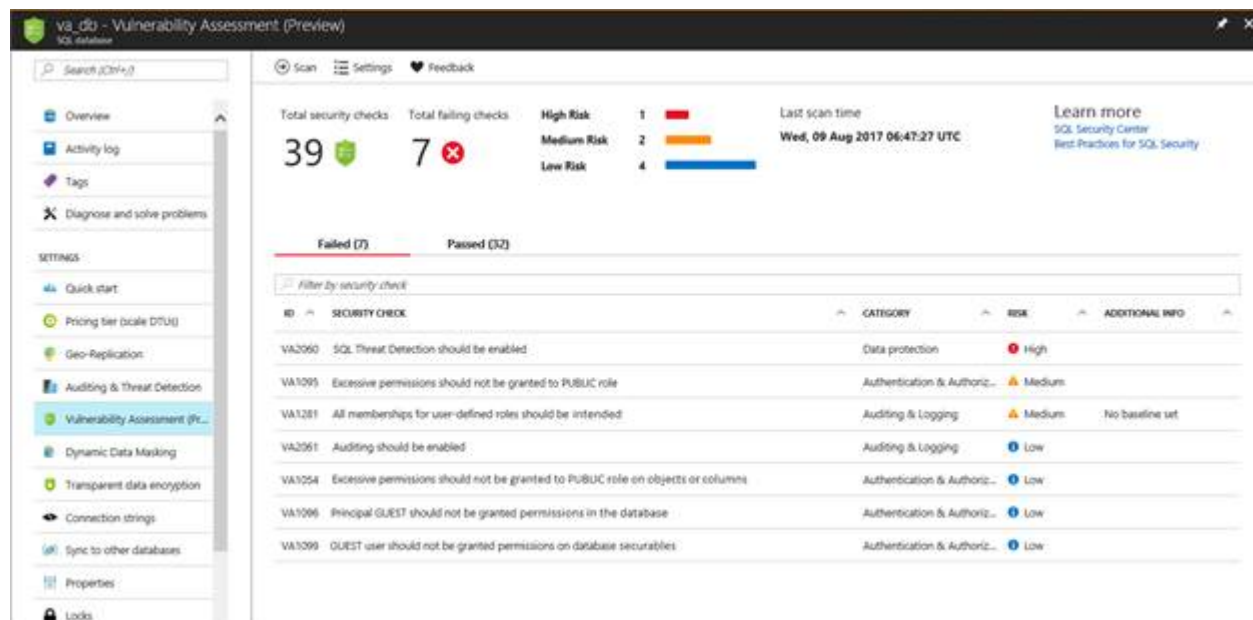
Last updated by | Soma Jagadeesh | Jan 11, 2021 at 11:20 AM PST

Contents

- [What is VA?](#)
 - [How does VA work?](#)
 - [Get Started Today!](#)
 - [SQL Vulnerability Assessment - Preview](#)
 - [Implementing VA](#)
 - [Classification](#)

What is VA?

SQL Vulnerability Assessment (VA) is a new service that provides you with visibility into your security state, and includes actionable steps to investigate, manage and resolve security issues and enhance your database fortifications. It is designed to be usable for non-security-experts – getting started and seeing an initial actionable report takes only a few seconds.



Vulnerability Assessment report in the Azure portal

This service truly enables you to focus your attention on the highest impact actions you can take to proactively improve your database security stature! In addition, if you have data privacy requirements, or need to comply with data protection regulations like the EU GDPR – then VA is your built-in solution to simplify these processes and monitor your database protection status. For dynamic database environments where changes are frequent and hard to track, VA is invaluable in detecting the settings that can leave your database vulnerable to attack.

VA offers a scanning service built into the Azure SQL Database service itself, and is also available via SQL Server Management Studio (SSMS) for scanning SQL Server databases. The service employs a knowledge base of rules that flag security vulnerabilities and deviations from best practices, such as misconfigurations, excessive permissions, and exposed sensitive data. The rule base is founded on intelligence accrued from analyzing millions of databases, and extracting the security issues that present the biggest risks to your database and its valuable data. These rules also represent a set of requirements from various regulatory bodies to meet their compliance standards, which can contribute to compliance efforts. The rule base grows and evolves over time, to reflect the latest security best practices recommended by Microsoft.

Results of the assessment include actionable steps to resolve each issue and provide customized remediation scripts where applicable. An assessment report can be customized for each customer environment and tailored to specific requirements. This process is managed by defining a security **Baseline** for the assessment results, such that only deviations from the custom Baseline are reported.

How does VA work?

We designed VA with simplicity in mind. All you need to do is to run a **Scan**, which will scan your database for vulnerabilities.

*The scan is lightweight and safe. It takes a few seconds to run, and is entirely read-only. It does not make *any* changes to your database!*

When your scan is complete, your scan report will be automatically displayed in the Azure Portal or in the SSMS pane:



Vulnerability Assessment report in SSMS. Currently available in Limited Preview.

The scan results include an overview of your security state, and details about each security issue found. You will find warnings on deviations from security best practices, as well as a snapshot of your security-related settings, such as database principals and roles and their associated permissions. In addition, scan results provide a map of sensitive data discovered in your database with recommendations of the built-in methods available to protect it.

For all the issues found, you can view details on the impact of the finding, and you will find actionable remediation information to directly resolve the issue. VA will focus your attention on security issues relevant to *you*, as your security baseline ensures that you are seeing relevant results customized to your environment. See [Getting Started with Vulnerability Assessment](#) for more details.

You can now use VA to monitor that your database maintains a high level of security at all times, and that your organizational policies are met. In addition, if your organization needs to meet regulatory requirements, VA reports can be helpful to facilitate the compliance process.

Get Started Today!

We encourage you to try out Vulnerability Assessment today, and start proactively improving your database security stature. Track and monitor your database security settings, so that you never again lose visibility and control of potential risks to the safety of your data.

Check out [Getting Started with Vulnerability Assessment](#) for more details on how to run and manage your assessment.

SQL Vulnerability Assessment - Preview

SQL Vulnerability Assessment (currently in preview) is an easy to configure tool, that can discover, track, and remediate potential database vulnerabilities. Use it to proactively improve your database security.

- Meet compliance requirements that require database scan reports.
- Meet data privacy standards.
- Monitor a dynamic database environment where changes are difficult to track.

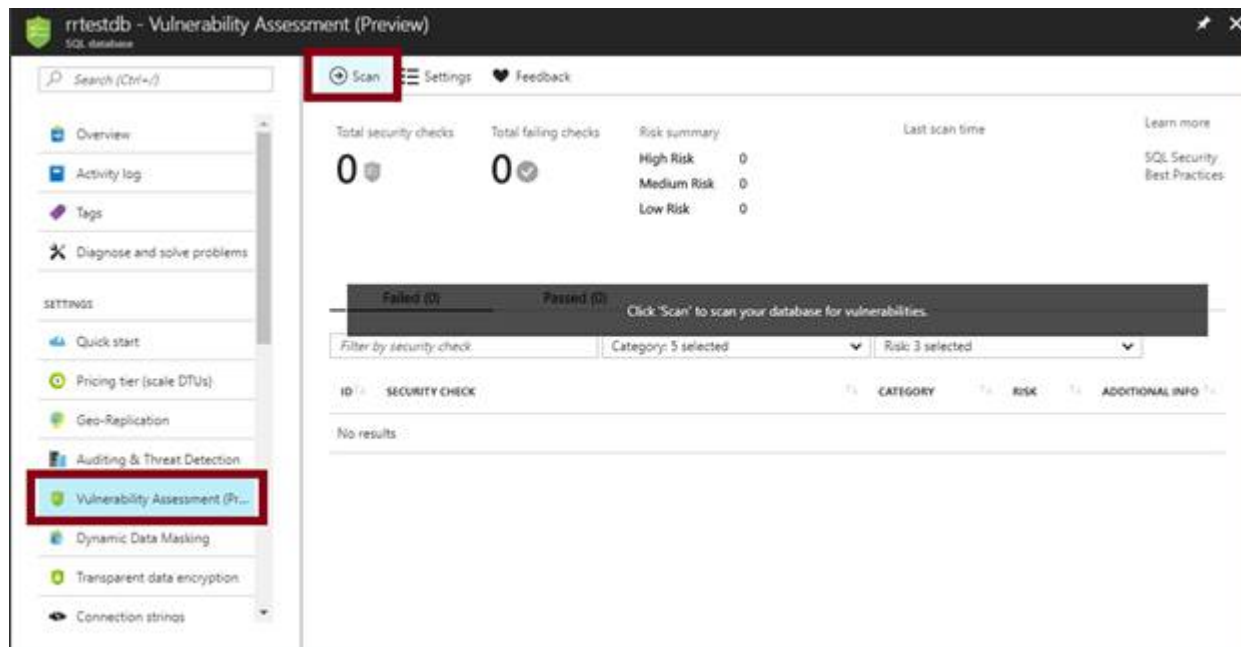
VA is a scanning service built into the Azure SQL Database service. The service employs a knowledge base of rules that flag security vulnerabilities and highlight deviations from best practices, such as misconfigurations, excessive permissions, and unprotected sensitive data. The rules are based on Microsoft's best practices, and focuses on the security issues that present the biggest risks to your database and its valuable data. These rules also represent many of the requirements from various regulatory bodies to meet their compliance standards.

Results of the scan include actionable steps to resolve each issue and provide customized remediation scripts where applicable. An assessment report can be customized for your environment, by setting an acceptable baseline for permission configurations, feature configurations and database settings.

Implementing VA

1. *Run a Scan*

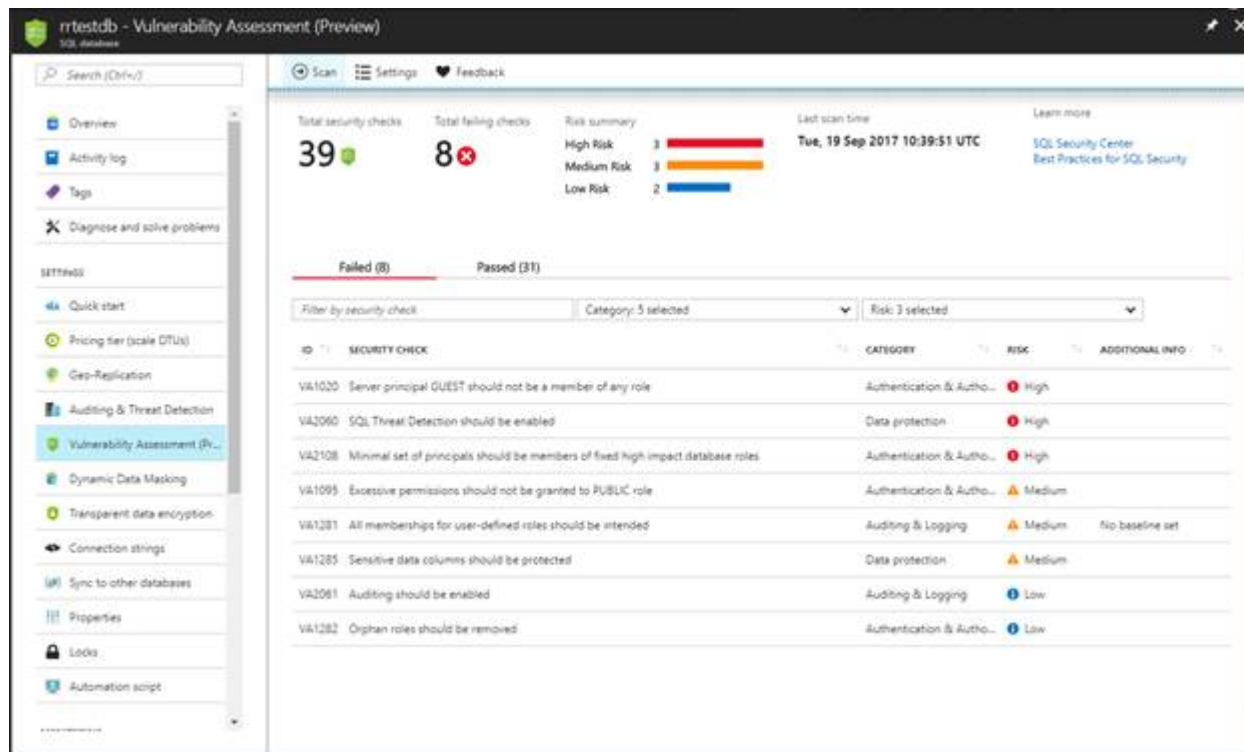
Get started with VA by navigating to Vulnerability Assessment (Preview) setting in your Azure SQL Database pane. You'll start by configuring a storage account where your scan results will be stored. For information about storage accounts, see [About Azure storage accounts](#). [RB1] [RR2] Once storage is configured, click **Scan** to scan your database for vulnerabilities.

**NOTE:**

The scan is lightweight and safe. It takes a few seconds to run, and is entirely read-only. It does not make any changes to your database.

2. View the report

When your scan is complete, your scan report is automatically displayed in the Azure Portal. The report presents an overview of your security state; how many issues were found, and their respective severities. Results include warnings on deviations from best practices, as well as a snapshot of your security-related settings, such as database principals and roles and their associated permissions. The scan report also provides a map of sensitive data discovered in your database, and includes recommendations of the built-in methods available to protect it.



3. Analyze the results and resolve issues

Review your results, and determine which findings in the report are true security issues in your environment. Drill-down to each failed result to understand the impact of the finding, and why each security check failed. Use the actionable remediation information provided by the report, to resolve the issue.

VA2108 - Minimal set of principals should be members of fixed high impact database roles

✓ Approve As Baseline ✕ Clear Baseline

NAME: VA2108 - Minimal set of principals should be members of fixed high impact database roles

RISK: High

STATUS: FAIL

DESCRIPTION: SQL Server provides roles to help manage the permissions. Roles are security principals that group other principals. Database-level roles are database-wide in their permission scope. This rule checks that a minimal set of principals are members of the fixed database roles.

IMPACT: Fixed database roles may have administrative permissions on the system. Following the principle of least privilege, it is important to minimize membership in fixed database roles and keep a baseline of these memberships. See <https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles> for additional information on database roles.

RULE QUERY:

```
SELECT user_name(sr.member_principal_id) as [Principal], user_name(sr.role_principal_id) as [Role], type_desc as [Principal]
```

Run in Query Editor

MICROSOFT RECOMMENDATION: Empty Set

RESULTS:

IN BASELINE	PRINCIPAL	ROLE	PRINCIPAL TYPE	AUTHENTICATION TYPE
✕	chikolulu	db_ddladmin	SQL_USER	NONE
✕	test1	db_ddladmin	DATABASE_ROLE	NONE

REMEDATION: Remove members who should not have access to the database role

REMEDATION SCRIPT:

```
ALTER ROLE [db_ddladmin] DROP MEMBER [chikolulu]
ALTER ROLE [db_ddladmin] DROP MEMBER [test1]
```

Run in Query Editor

4. Set your Baseline

As you review your assessment results, you can mark specific results as being an acceptable *Baseline* in your environment. The baseline is essentially a customization of how the results are reported. Results which match the baseline will be considered as passing in subsequent scans. Once you have established your baseline security state, VA will only report on deviations from the baseline, and you can focus your attention on the relevant issues.

VA2108 - Minimal set of principals should be members of fixed high impact database roles

✓ Approve As Baseline ✕ Clear Baseline

NAME: VA2108 - Minimal set of principals should be members of fixed high impact database roles

RISK: High

STATUS: ✕ FAIL

DESCRIPTION: SQL Server provides roles to help manage the permissions. Roles are security principals that group other principals. Database-level roles are database-wide in their permission scope. This rule checks that a minimal set of principals are members of the fixed database roles.

IMPACT: Fixed database roles may have administrative permissions on the system. Following the principle of least privilege, it is important to minimize membership in fixed database roles and keep a baseline of these memberships. See <https://docs.microsoft.com/en-us/sql/relational-databases/security/authentication-access/database-level-roles> for additional information on database roles.

RULE QUERY: `SELECT user_name(sr.member_principal_id) as [Principal], user_name(sr.role_principal_id) as [Role], type_desc as [Principal]`

Run in Query Editor

MICROSOFT RECOMMENDATION: Empty Set

RESULTS:

IN BASELINE	PRINCIPAL	ROLE	PRINCIPAL TYPE	AUTHENTICATION TYPE
✕	chikoluku	db_ddladmin	SQL_USER	NONE
✕	test1	db_ddladmin	DATABASE_ROLE	NONE

5. Run a new scan to see your customized tracking report

After you complete setting up your **Rule Baselines**, run a new scan to view the customized report. VA now reports only security issues that deviate from your approved baseline state.

rrtestdb - Vulnerability Assessment (Preview)

SQL Database

Scan Settings Feedback

Total security checks: 39 ✓ Total failing checks: 4 ✕

Risk summary: High Risk: 1 ■ Medium Risk: 1 ■ Low Risk: 2 ■

Last scan time: Tue, 19 Sep 2017 10:29:56 UTC

Learn more: [SQL Security Center](#) [Best Practices for SQL Security](#)

Failed (4) Passed (35)

Filter by security check: Category: 5 selected Status: 2 selected

ID	SECURITY CHECK	CATEGORY	STATUS
VA1020	Server principal GUEST should not be a member of any role	Authentication & Author...	✓ PASS (per custom baseline)
VA1054	Excessive permissions should not be granted to PUBLIC role on objects or columns	Authentication & Author...	✓ PASS
VA1095	Excessive permissions should not be granted to PUBLIC role	Authentication & Author...	✓ PASS (per custom baseline)
VA1096	Principal GUEST should not be granted permissions in the database	Authentication & Author...	✓ PASS
VA1097	Principal GUEST should not be granted permissions on objects or columns	Authentication & Author...	✓ PASS
VA1099	GUEST user should not be granted permissions on database securables	Authentication & Author...	✓ PASS
VA1143	'dbo' user should not be used for normal service operation	Surface area reduction	✓ PASS
VA1223	Certificate keys should use at least 2048 bits	Data protection	✓ PASS
VA1246	Application roles should not be used	Authentication & Author...	✓ PASS
VA1248	User-defined database roles should not be members of fixed roles	Authentication & Author...	✓ PASS (per custom baseline)

VA can now be used to monitor that your database maintains a high level of security at all times, and that your organizational policies are met. If compliance reports are required, VA reports can be helpful to facilitate the compliance process.

Classification

Root cause Tree - Security/User Request/How-to/advisory

How good have you found this content?

