**SQL DATABASE SECURITY**

**Advanced data security:**

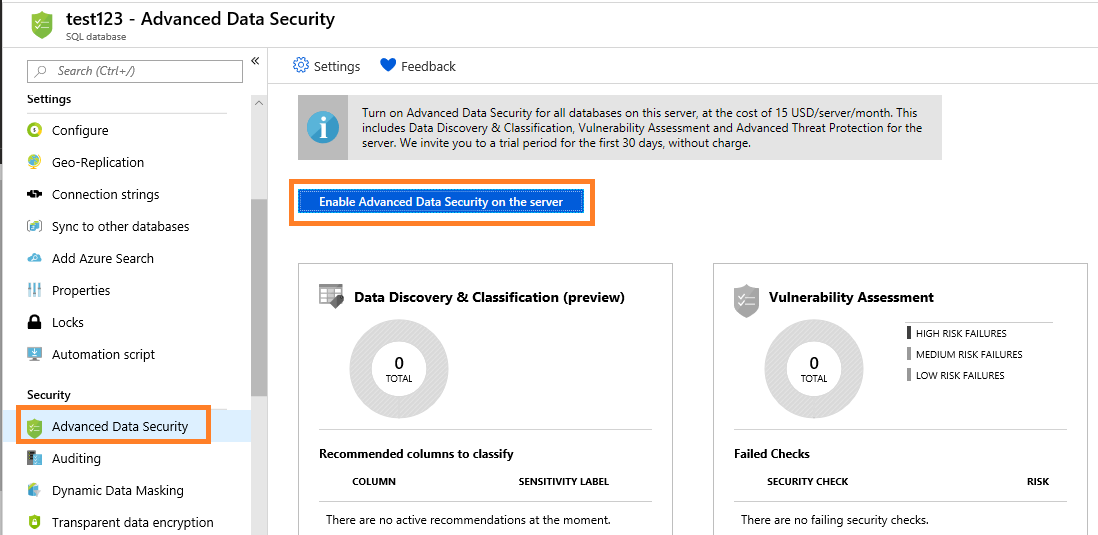
Advanced data security (ADS) provides a set of advanced SQL security capabilities, including data discovery & classification, vulnerability assessment, and threat detection.

**vulnerability assessment**

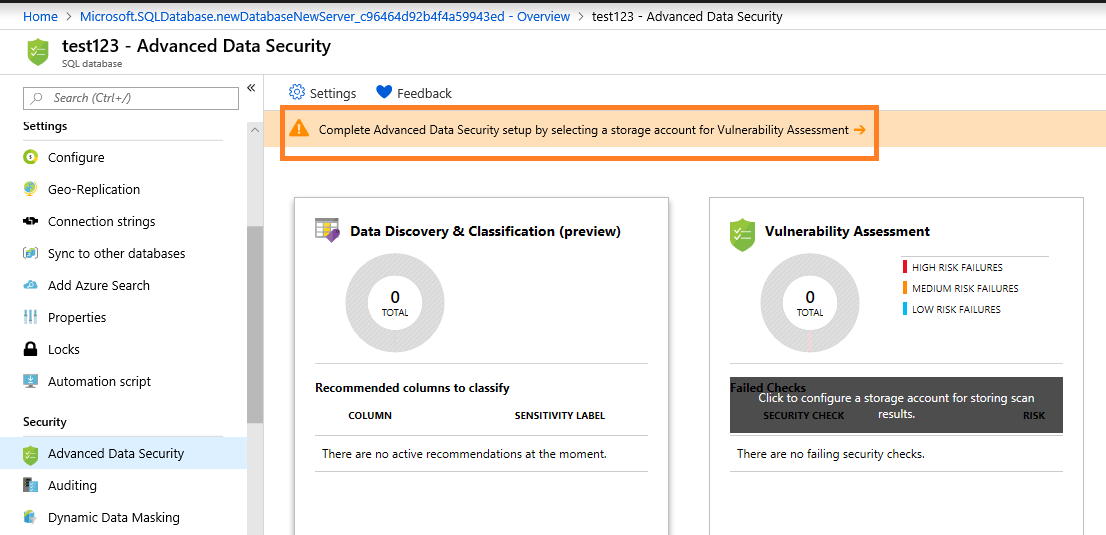
* It helps to Assess, track, and improve the security of SQL databases, in Azure and on-prem.

**Configure vulnerability assessment:**

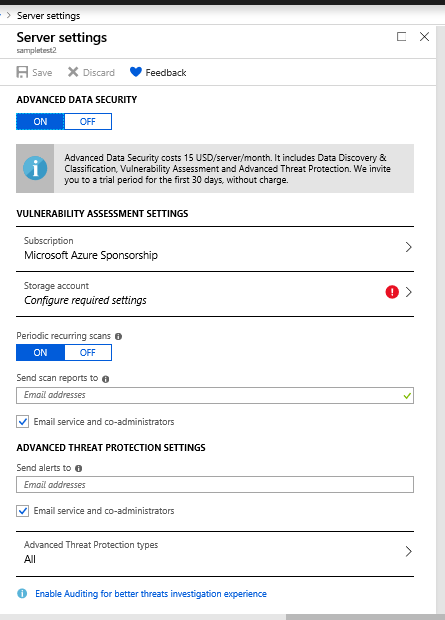
1. Click on the Advanced Security and to enable ADS for all databases on the database server or managed instance, click **Enable Advanced Data Security on the server**.



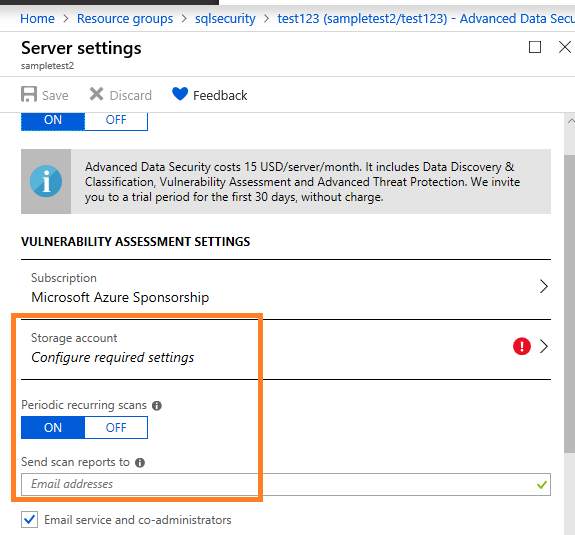
1. Click on the Vulnerability Assessment



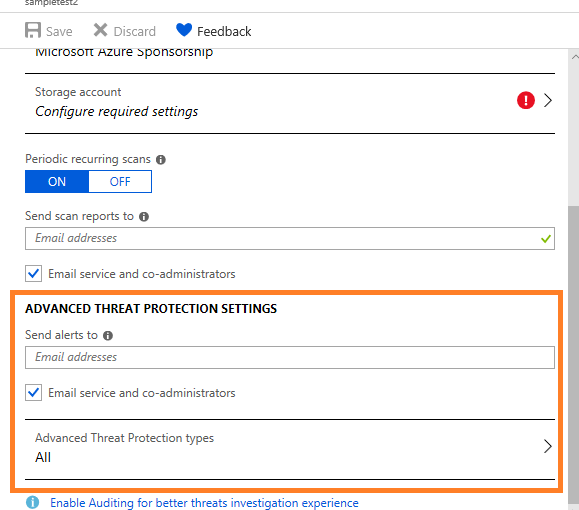
1. To start using vulnerability assessment, you need to configure a storage account where scan results are saved.



1. Select or create a storage account for saving scan results. You can also turn on periodic recurring scans to configure vulnerability assessment to run automatic scans once per week. A scan result summary is sent to the email address(es) you provide.



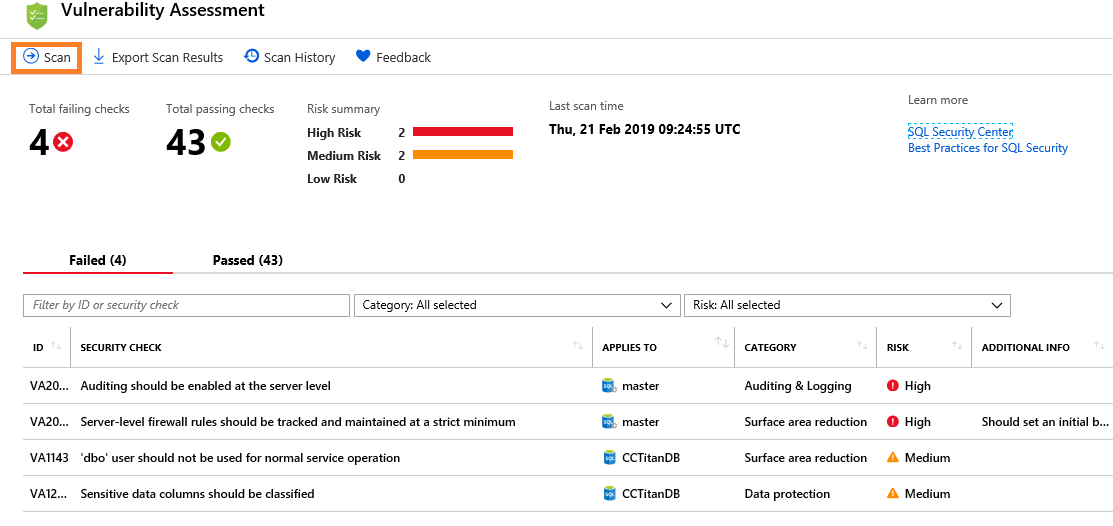
1. Threat protection provides a new layer of security, which enables customers to detect and respond to potential threats as they occur by providing security alerts on anomalous activities.



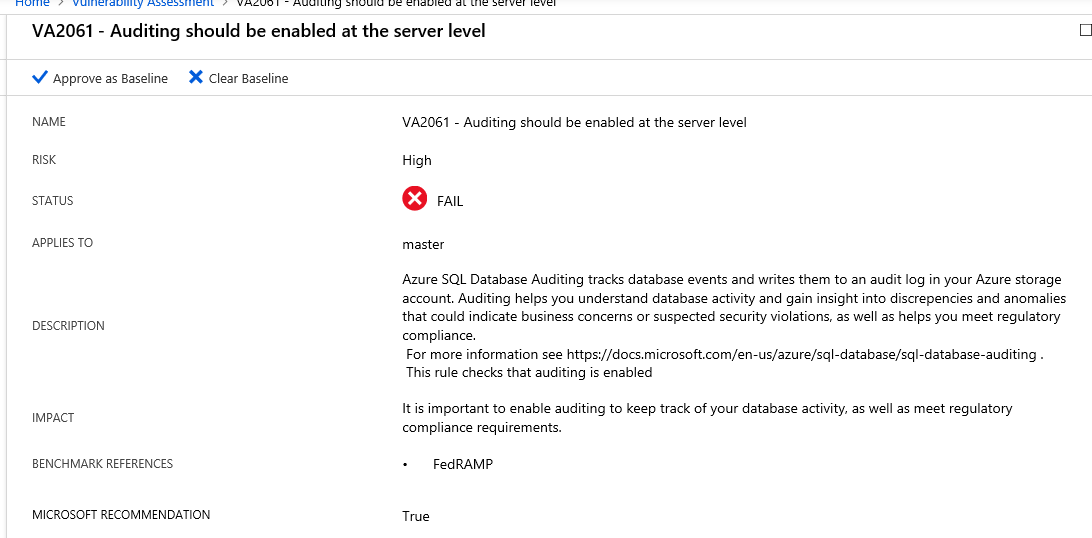
If we configured vulnerability assessment and Threat protection, now we can go and check Scan.

Click on the Scan and View the report

* 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 and a snapshot of your security-related settings, such as database principals and roles and their associated permissions.

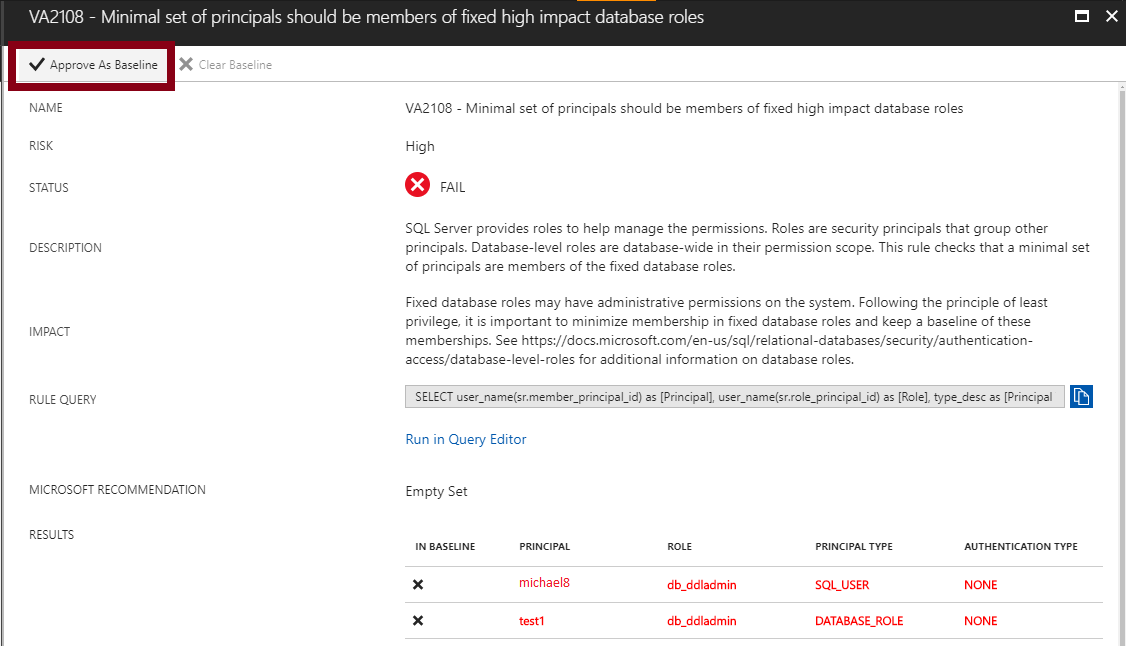


Analyze the results and resolve issues



Set your baseline

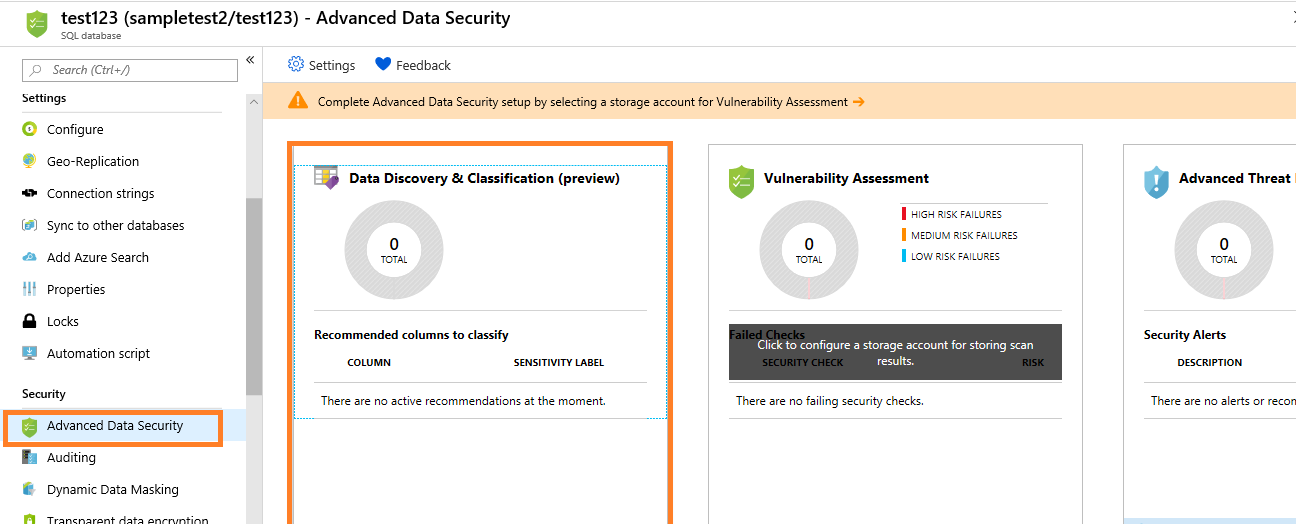
Once you have established your baseline security state, VA only reports on deviations from the baseline and you can focus your attention on the relevant issues.



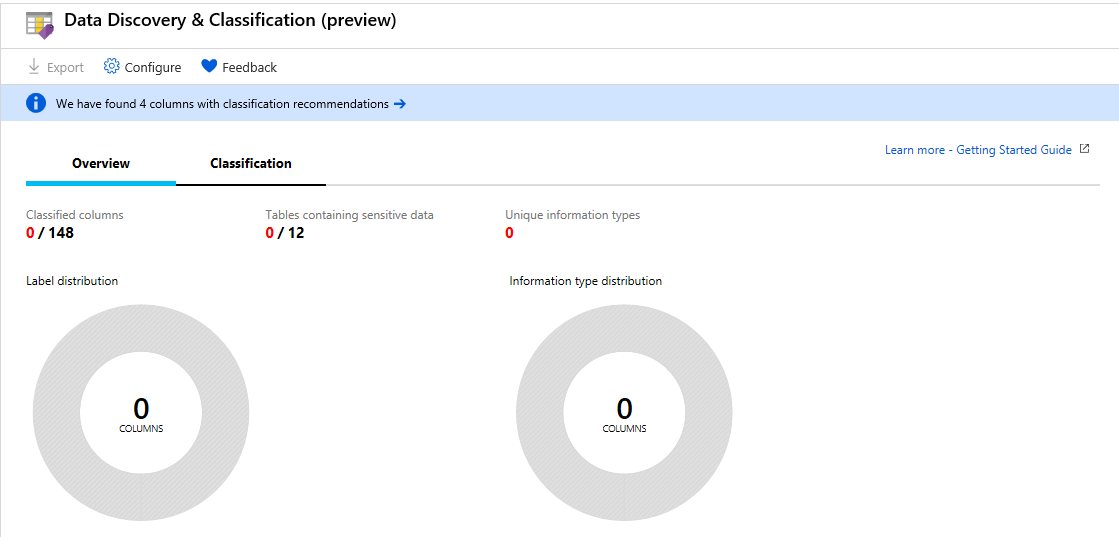
**Azure SQL Database data discovery & classification:**

* Discovering and classifying your most sensitive data (business, financial, healthcare, personally identifiable data.
* The **Overview**tab includes a summary of the current classification state of the database, including a detailed list of all classified columns, which you can also filter to view only specific schema parts, information types and labels. If you haven’t yet classified any columns.

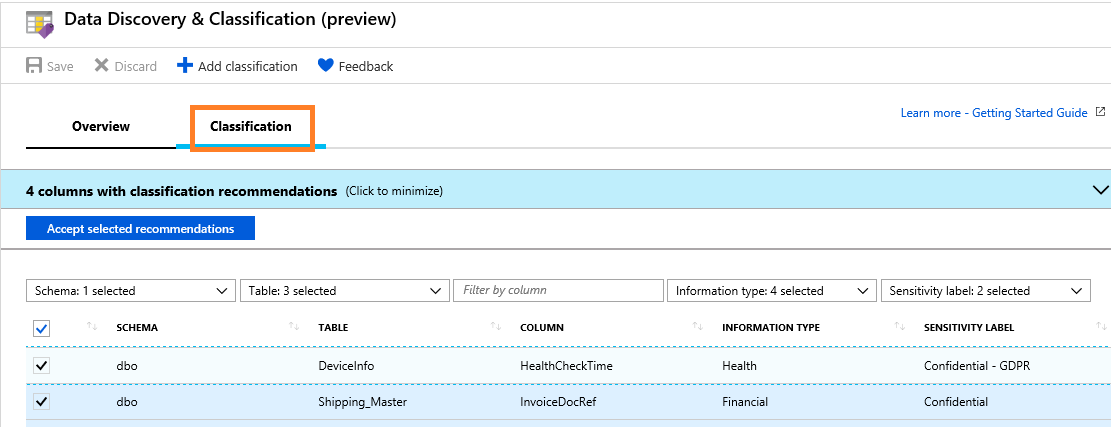
1. Navigate to**Advanced Data Security** under the Security heading in your Azure SQL Database pane. Click to enable advanced data security, and then click on the **Data discovery & classification (preview)** card.



1. The **Overview** tab includes a summary of the current classification state of the database, including a detailed list of all classified columns, which you can also filter to view only specific schema parts, information types and labels.

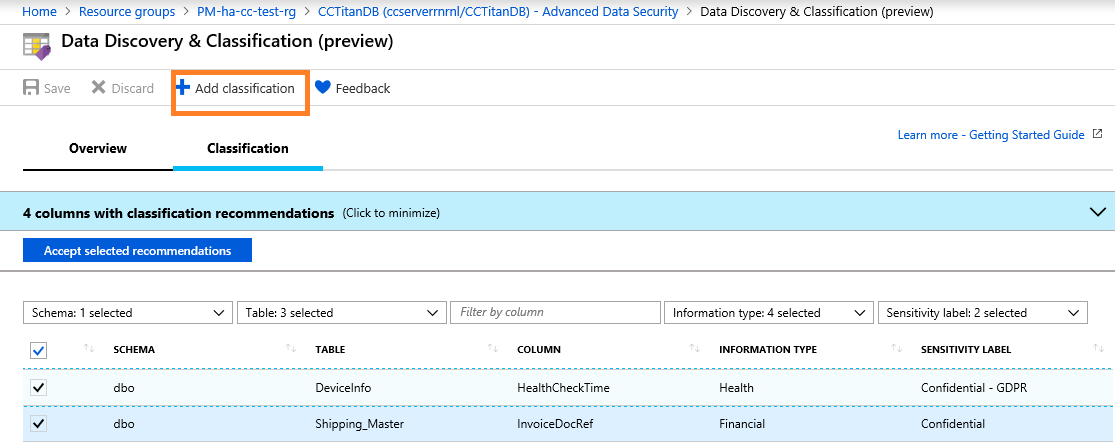


1. To begin classifying your data, click on the **Classification tab** at the top of the window.



1. You can also **manually classify** columns as an alternative, or in addition, to the recommendation-based classification:

* Click on **Add classification** in the top menu of the window.

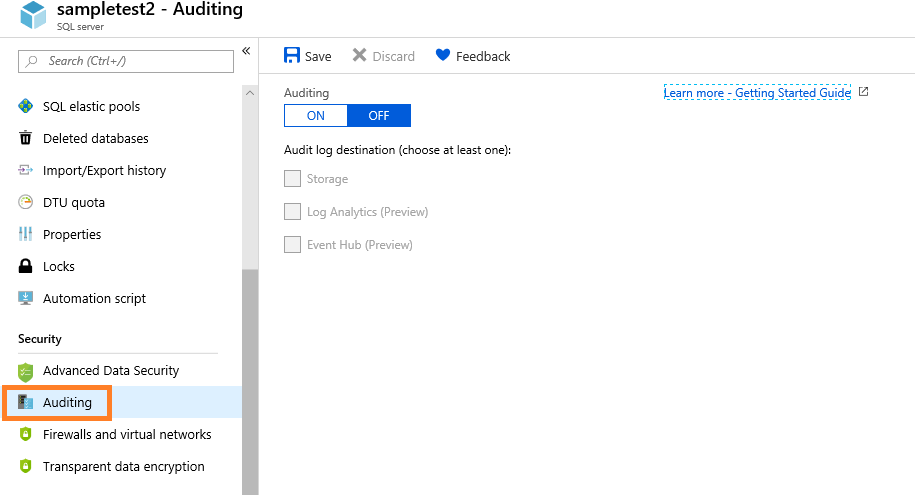


**Auditing:**

 Audit logs helps monitor data and keep track of potential security breaches or internal misuses of information.

**Set up auditing for your database**

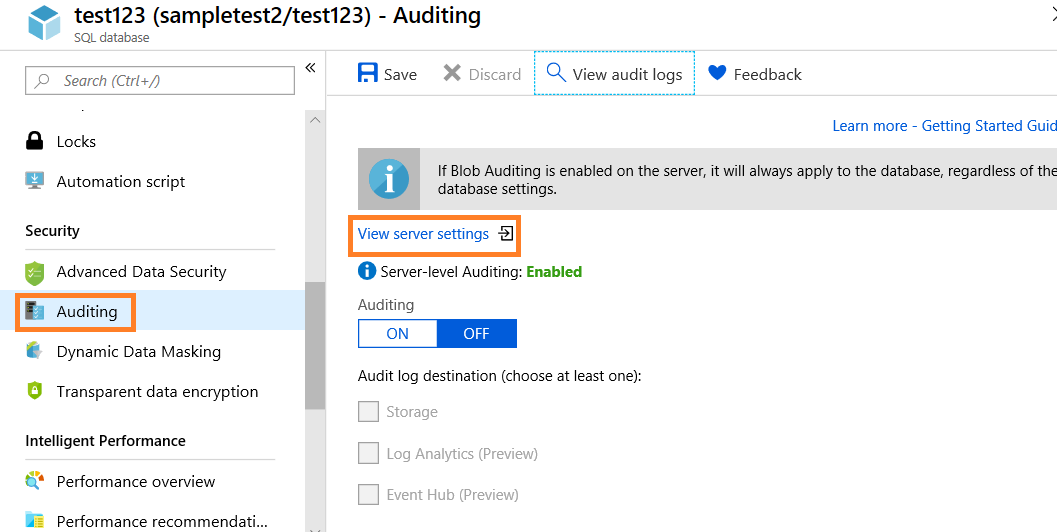
1. Navigate to **Auditing** under the Security heading in your SQL database/server pane.



1. Switch auditing ON and You now have multiple options for configuring where audit logs will be written.

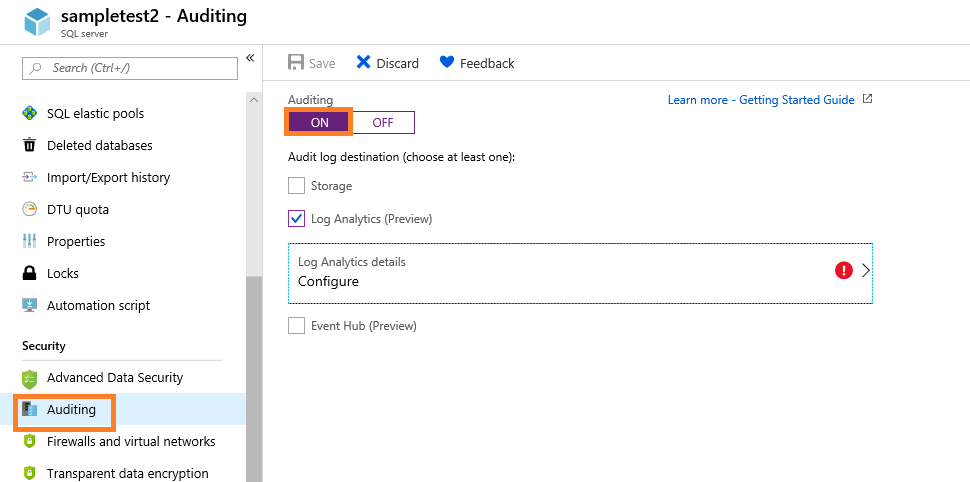
* You now have multiple options for configuring where audit logs will be written. You can write logs to an Azure storage account, to a Log Analytics workspace for consumption by Log Analytics, or to event hub for consumption using event hub. You can configure any combination of these options, and audit logs will be written to each.

If you prefer to enable auditing on the Server level, switch **Auditing** to **OFF**.

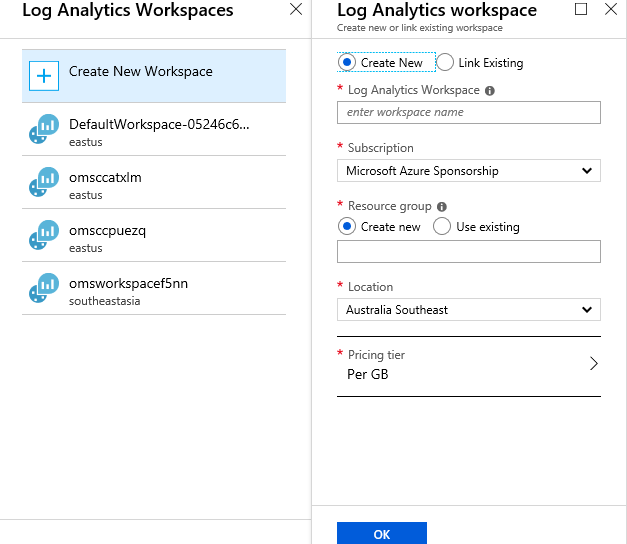


(Or)

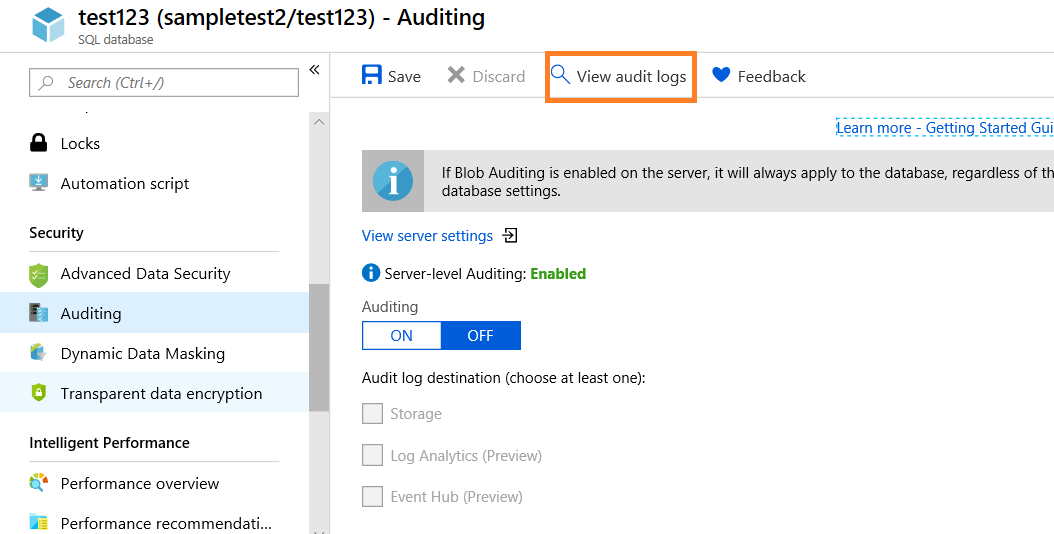
If you prefer to enable auditing on the database level, switch **Auditing** to **ON**.

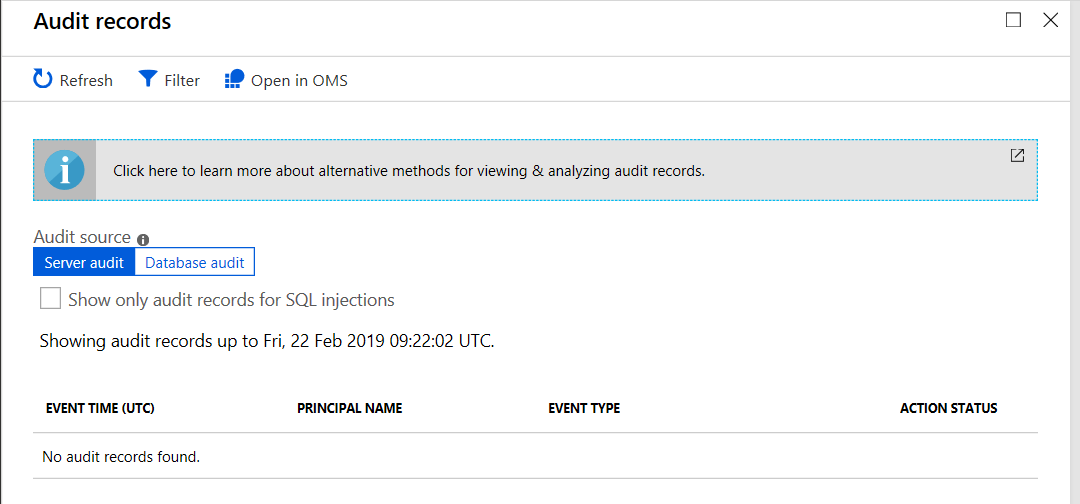


1. Fill all the details and Click Save.



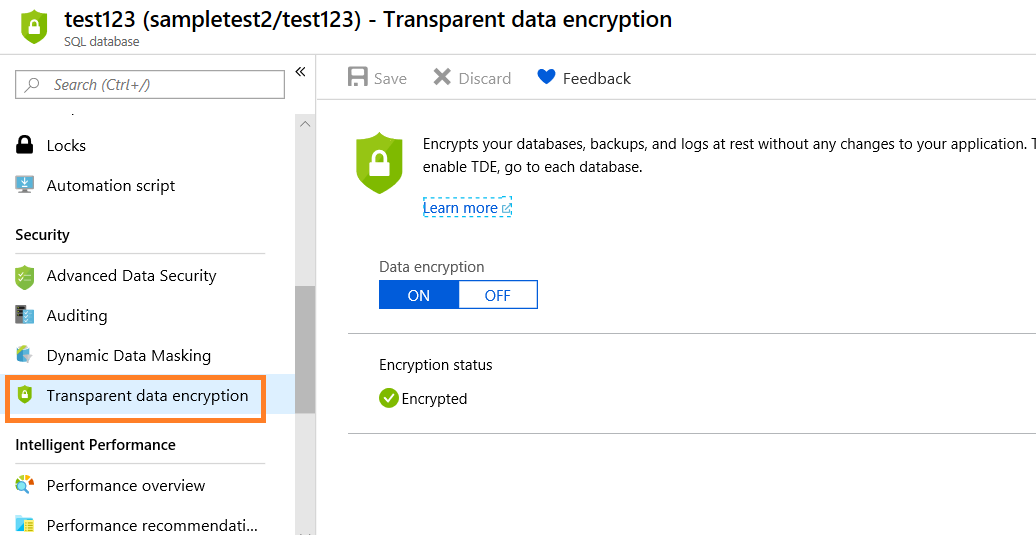
1. Clicking on **Open in OMS** at the top of the **Audit records** page will open the Logs view in Log Analytics, where you can customize the time range and the search query.



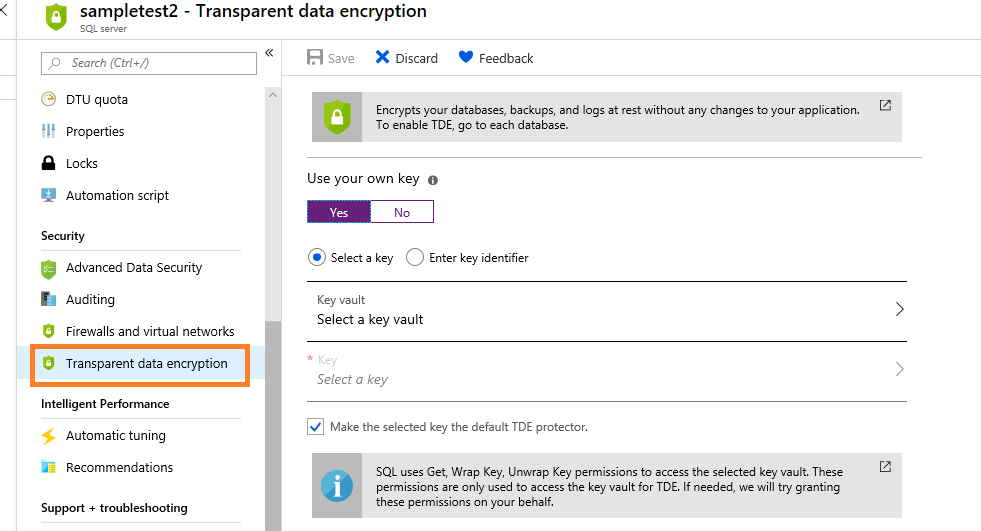


**Transparent data encryption for SQL Database and Data Warehouse:**

* Transparent data encryption (TDE) helps protect Azure SQL Database, Azure SQL Managed Instance, and Azure Data Warehouse against the threat of malicious activity.
* It performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.
* Transparent data encryption encrypts the storage of an entire database by using a symmetric key called the database encryption key.
* This database encryption key is protected by the transparent data encryption protector.
* The protector is either a service-managed certificate (service-managed transparent data encryption) or an asymmetric key stored in Azure Key Vault (Bring Your Own Key).

1. You turn transparent data encryption on and off on the database level. 
2. You set the transparent data encryption master key, also known as the transparent data encryption protector, on the server level.

* To use transparent data encryption with Bring Your Own Key support and protect your databases with a key from Key Vault, open the transparent data encryption settings under your server.



**SQL Database dynamic data masking:**

Dynamic data masking helps prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer. It’s a policy-based security feature that hides the sensitive data in the result set of a query over designated database fields, while the data in the database is not changed.

**Examples**

| **Masking Function** | **Masking Logic** |
| --- | --- |
| Credit card | Masking method, which exposes the last four digits of the designated fields and adds a constant string as a prefix in the form of a credit card.  XXXX-XXXX-XXXX-1234 |
| Email | Masking method, which exposes the first letter and replaces the domain with XXX.com using a constant string prefix in the form of an email address.  aXX@XXXX.com |

