

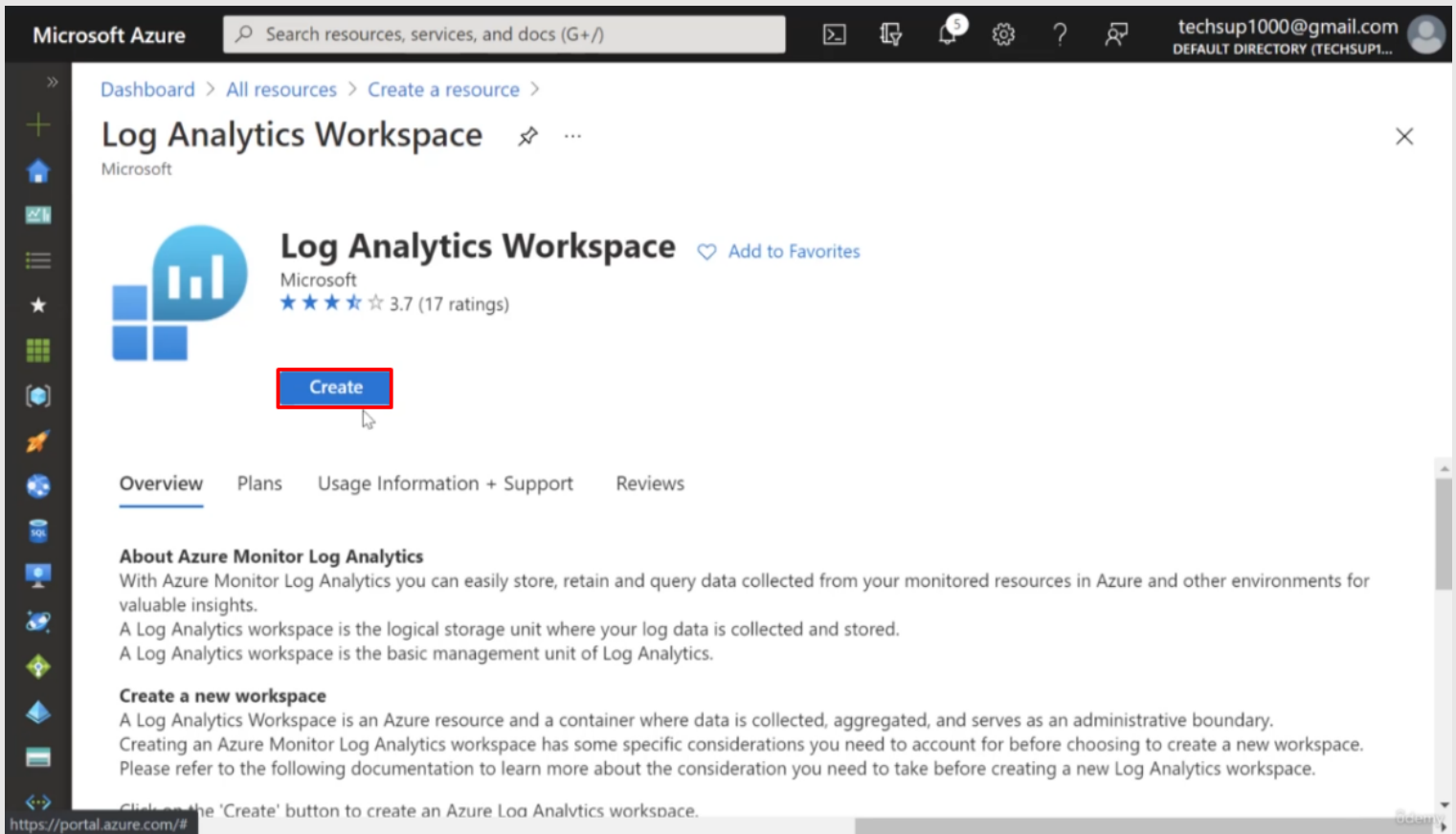
# Azure Synapse Auditing

---

- Puede habilitar la auditoría para un Azure SQL Pool en Azure Synapse Analytics.
- Esta función se puede utilizar para realizar un seguimiento de los eventos de la base de datos y escribirlos en un audit log.
- Los logs pueden almacenarse en una cuenta de Azure Storage, en un workspace de Log Analytics y en Azure Event Hubs.
- Esto ayuda en el cumplimiento normativo. Ayuda a obtener información sobre cualquier anomalía en las actividades de la base de datos.
- La auditoría puede activarse a nivel de data warehouse o a nivel de servidor
- Si se aplica a nivel de servidor, se aplicará a todos los data warehouses que residan en el servidor.

Ahora, les mostrare como habilitar la auditoria para sus SQL Pools en Azure Synapse. Ahora, vamos a crear un nuevo recurso. Vamos a crear un Log Analytics workspace para que todos los logs puedan ser dirigidos a ese workspace. Ahora, un Log Analytics workspace es una característica que está disponible con Azure Monitor. Esto realmente le da un lugar central de logging en el que puede dirigir los logs de varios recursos en Azure. A continuación, puede utilizar el lenguaje de consulta personalizado para consultar los datos en el Log Analytics workspace. También puede crear alertas basadas en los datos que se acumulan en ese workspace. Así que eso es sólo una breve reseña sobre el Log Analytics workspace.

Comenzaremos creando un Log Analytics Workspace



Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > All resources > Create a resource >

# Log Analytics Workspace

Microsoft

★★★★☆ 3.7 (17 ratings)

**Create**

Overview Plans Usage Information + Support Reviews

**About Azure Monitor Log Analytics**

With Azure Monitor Log Analytics you can easily store, retain and query data collected from your monitored resources in Azure and other environments for valuable insights.

A Log Analytics workspace is the logical storage unit where your log data is collected and stored.

A Log Analytics workspace is the basic management unit of Log Analytics.

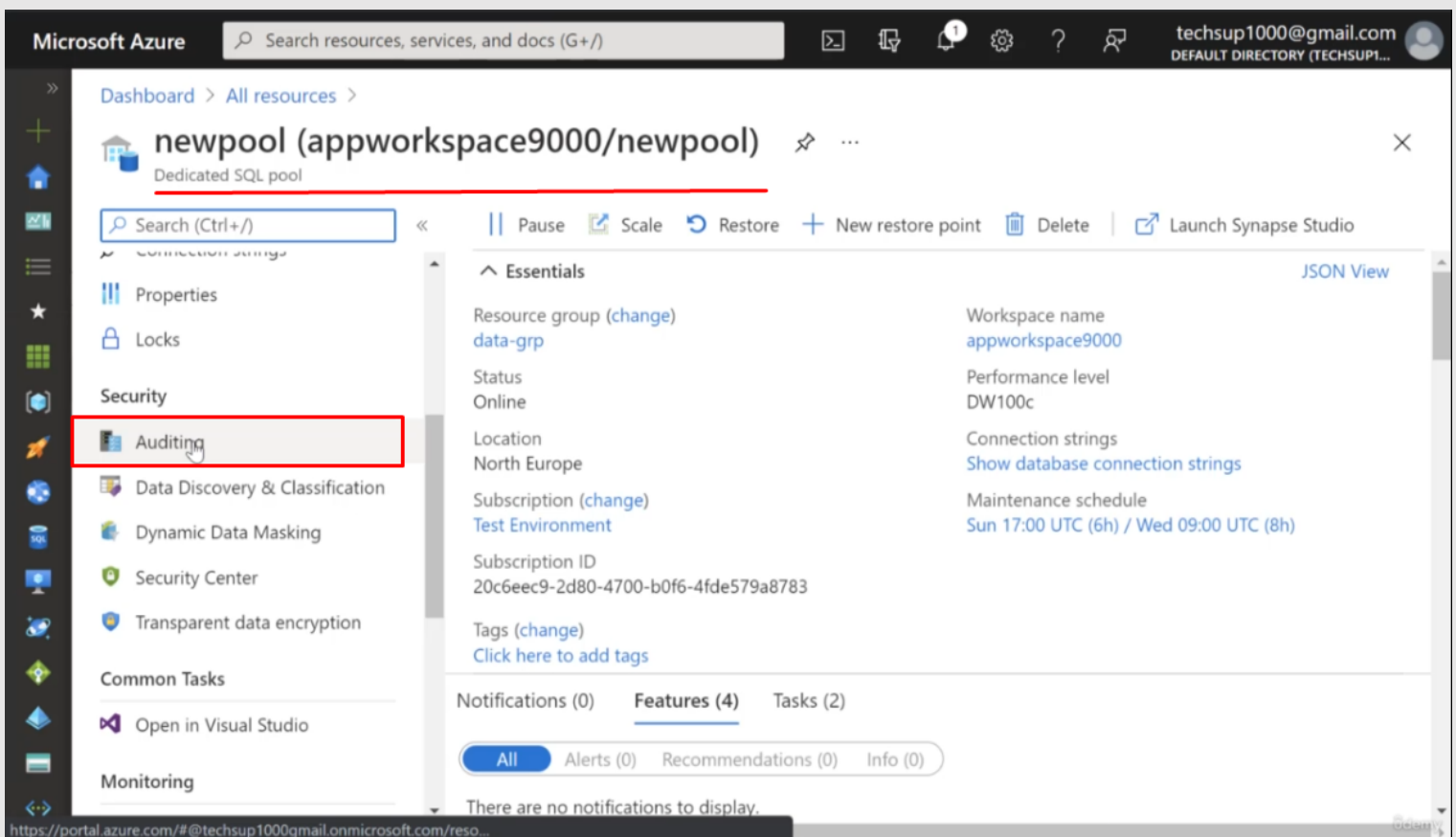
**Create a new workspace**

A Log Analytics Workspace is an Azure resource and a container where data is collected, aggregated, and serves as an administrative boundary. Creating an Azure Monitor Log Analytics workspace has some specific considerations you need to account for before choosing to create a new workspace. Please refer to the following documentation to learn more about the consideration you need to take before creating a new Log Analytics workspace.

Click on the 'Create' button to create an Azure Log Analytics workspace.

https://portal.azure.com/#

Desde el workspace de nuestra base de datos del Dedicated SQL Pool



Microsoft Azure

Search resources, services, and docs (G+/)

Dashboard > All resources >

# newpool (appworkspace9000/newpool)

Dedicated SQL pool

Search (Ctrl+/) Pause Scale Restore + New restore point Delete Launch Synapse Studio

Connection strings

Properties Locks Security Auditing Data Discovery & Classification Dynamic Data Masking Security Center Transparent data encryption Common Tasks Open in Visual Studio Monitoring

**Essentials**

Resource group (change) data-grp

Status Online

Location North Europe

Subscription (change) Test Environment

Subscription ID 20c6eec9-2d80-4700-b0f6-4fde579a8783

Tags (change) Click here to add tags

Workspace name appworkspace9000

Performance level DW100c

Connection strings Show database connection strings

Maintenance schedule Sun 17:00 UTC (6h) / Wed 09:00 UTC (8h)

Notifications (0) Features (4) Tasks (2)

All Alerts (0) Recommendations (0) Info (0)

There are no notifications to display.

https://portal.azure.com/#@techsup1000gmail.onmicrosoft.com/reso...

Microsoft Azure Search resources, services, and docs (G+)

Dashboard > All resources > newpool (appworkspace9000/newpool)

## newpool (appworkspace9000/newpool) | Auditing

Dedicated SQL pool

Search (Ctrl+/) Save Discard View audit logs Feedback

If Azure SQL Auditing is enabled on the workspace, it will always apply to the SQL Pool, regardless of the SQL Pool settings.

View workspace settings

Workspace-level Auditing: **Disabled**

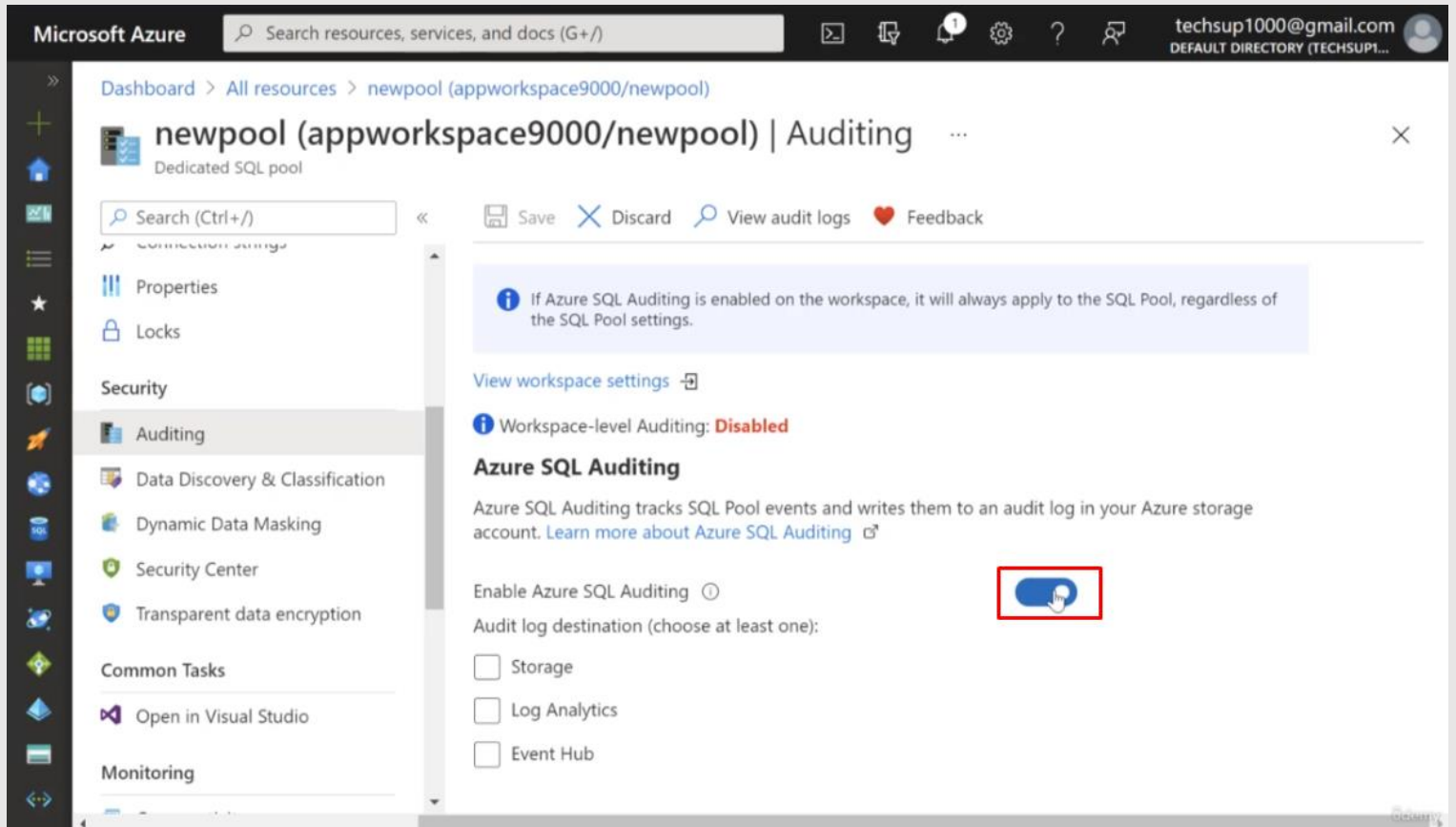
### Azure SQL Auditing

Azure SQL Auditing tracks SQL Pool events and writes them to an audit log in your Azure storage account. [Learn more about Azure SQL Auditing](#)

Enable Azure SQL Auditing

Audit log destination (choose at least one):

- ☐ Storage
- ☐ Log Analytics
- ☐ Event Hub



Desde Azure Synapse workspace

Microsoft Azure Search resources, services, and docs (G+)

Dashboard > All resources >

## appworkspace9000

Synapse workspace

Search (Ctrl+/) + New dedicated SQL pool + New Apache Spark pool Refresh Reset SQL admin password

Apache Spark pools

Security

- Encryption
- Firewalls
- Managed identities
- Private endpoint connections
- Approved Azure AD tenants
- Azure SQL Auditing**
- Azure Defender for SQL

Monitoring

- Alerts
- Metrics

Resource group (change) data-grp

Status Succeeded

Location North Europe

Subscription (change) Test Environment

Subscription ID 20c6eec9-2d80-4700-b0f6-4fde579a8783

Managed virtual network No

Managed Identity object ID e9951814-9161-4347-997f-6c970554a175

Workspace web URL <https://web.azuresynapse.net?workspace=%2fs...>

Tags (change) [Click here to add tags](#)

Firewalls [Show firewall settings](#)

Primary ADLS Gen2 account URL <https://synapsedatalake10001.dfs.core.windows...>

Primary ADLS Gen2 file system data

SQL admin username sqladminuser

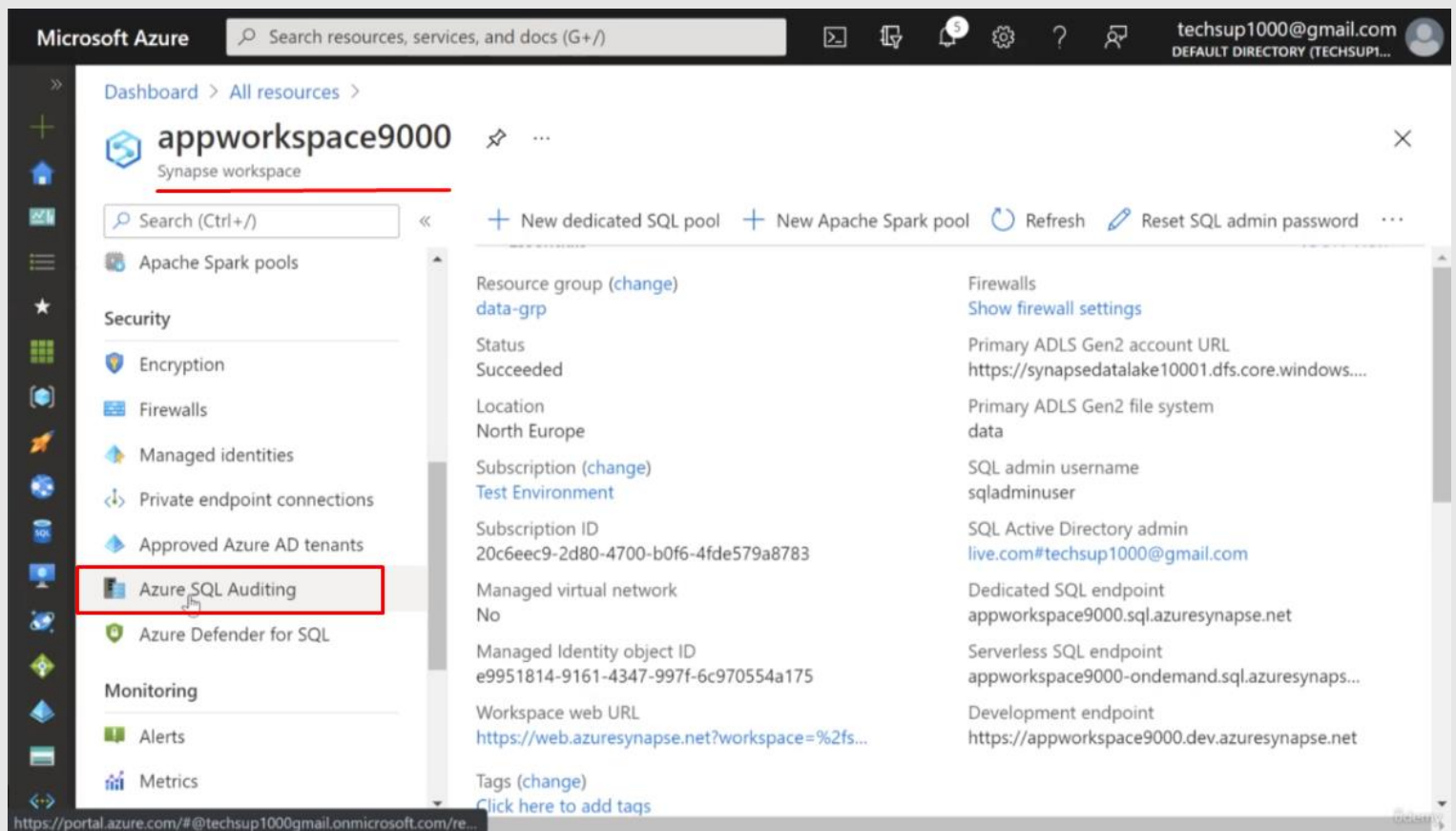
SQL Active Directory admin [live.com#techsup1000@gmail.com](mailto:live.com#techsup1000@gmail.com)

Dedicated SQL endpoint appworkspace9000.sql.azuresynapse.net

Serverless SQL endpoint appworkspace9000-ondemand.sql.azuresynaps...

Development endpoint <https://appworkspace9000.dev.azuresynapse.net>

<https://portal.azure.com/#@techsup1000gmail.onmicrosoft.com/re...>



Microsoft Azure Search resources, services, and docs (G+ /)

Dashboard > All resources > appworkspace9000

## appworkspace9000 | Azure SQL Auditing

Synapse workspace

Search (Ctrl+ /)

Apache Spark pools

Security

- Encryption
- Firewalls
- Managed identities
- Private endpoint connections
- Approved Azure AD tenants
- Azure SQL Auditing**
- Azure Defender for SQL

Monitoring

- Alerts
- Metrics

Save Discard Feedback

⚠ Azure SQL auditing settings apply only to dedicated SQL pools in this workspace.

Enable Azure SQL Auditing ⓘ ☒

Audit log destination (choose at least one):

- ☐ Storage
- ☒ Log Analytics

Subscription \*  
Test Environment

Log Analytics \*  
dbworkspace1000(northeurope)

☐ Event Hub

ⓘ Turn on Azure Defender for SQL to receive security alerts upon suspicious events.

Microsoft Azure Search resources, services, and docs (G+ /)

Dashboard > Microsoft.LogAnalyticsOMS > dbworkspace1000

## dbworkspace1000 | Logs

Log Analytics workspace

Search (Ctrl+ /)

Advanced settings

General

- Workspace summary
- Workbooks
- Logs**
- Solutions
- Usage and estimated costs
- Properties
- Service Map

Workspace Data Sources

- Virtual machines
- Storage accounts logs

### Welcome to Log Analytics

Azure Monitor Log Analytics is a tool used to produce insights from Azure Monitor logs.

Microsoft Azure Search resources, services, and docs (G+/)

Dashboard > Microsoft.LogAnalyticsOMS > dbworkspace1000

## dbworkspace1000 | Logs

Log Analytics workspace

New Query 1 x + Feedback Queries Query explorer

dbworkspace1000 Select scope hours Save Share New alert rule Export

1 Type your query here or click one of the queries to start

Tables Queries Functions

Search

Filter Group by: Solution

Collapse all

**Favorites**

You can add favorites by clicking on the ☆ icon

LogManagement

SQLSecurityAuditEvents

**SQLSecurityAuditEvents** ☆

Use in editor

**Description**

Azure Synapse SQL Audit Log.

Tags

Useful links

Microsoft Azure Search resources, services, and docs (G+/)

Dashboard > Microsoft.LogAnalyticsOMS > dbworkspace1000

## dbworkspace1000 | Logs

Log Analytics workspace

New Query 1\* x + Feedback Queries Query explorer

Run Time range: Last 24 hours Save Share New alert rule Export

1 SQLSecurityAuditEvents

Results Chart Columns Display time (UTC+00:00) Group columns

Completed. Showing results from the last 24 hours. 00:00.6 22 records

TimeGenerated [UTC]	LogicalServerName	ResourceGroup
> 7/13/2021, 10:30:50.903 AM	appworkspace9000	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e...
> 7/13/2021, 10:30:50.903 AM	appworkspace9000	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e...
> 7/13/2021, 10:30:51.903 AM	appworkspace9000	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e...
> 7/13/2021, 10:35:25.993 AM	appworkspace9000	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e...
> 7/13/2021, 10:35:25.993 AM	appworkspace9000	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e...



Microsoft Azure Search resources, services, and docs (G+/)

Dashboard > Microsoft.LogAnalyticsOMS > dbworkspace1000

### dbworkspace1000 | Logs

Log Analytics workspace

New Query 1\* Run Time range: Last 24 hours Save Share New alert rule Export

1 SQLSecurityAuditEvents

Results Chart Columns Display time (UTC+00:00) Group columns

Completed. Showing results from the last 24 hours. 00:00.6 22 records

TimeGenerated [UTC]	LogicalServerName	ResourceGroup
7/13/2021, 10:30:50.903 AM	appworkspace9000	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e...
...		
TenantId	ddcc3a4d-50f6-4ef0-824e-30bf4ce30734	
LogicalServerName	appworkspace9000	
ResourceGroup	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e7624a250	

Schema and Filter

https://logextension.hosting.portal.azure.net/logextension/az/#

Microsoft Azure Search resources, services, and docs (G+/)

Dashboard > Microsoft.LogAnalyticsOMS > dbworkspace1000

### dbworkspace1000 | Logs

Log Analytics workspace

New Query 1\* Run Time range: Last 24 hours Save Share New alert rule Export

1 SQLSecurityAuditEvents

Results Chart Columns Display time (UTC+00:00) Group columns

Completed. Showing results from the last 24 hours. 00:00.6 22 records

TimeGenerated [UTC]	LogicalServerName	ResourceGroup
...		
ResourceGroup	synapseworkspace-managedrg-54eb0e30-984f-4d75-baf3-1f3e7624a250	
TimeGenerated [UTC]	2021-07-13T10:30:50.903323Z	
Category	SQLSecurityAuditEvents	
AuditSchemaVersion	1	
EventTime [UTC]	2021-07-13T10:30:50.34Z	

Schema and Filter

https://logextension.hosting.portal.azure.net/logextension/az/#