Audit logs are not getting logged for specific event - SQL Security Audit Event

Last updated by | Vitor Tomaz | Feb 24, 2023 at 3:32 AM PST

Contents

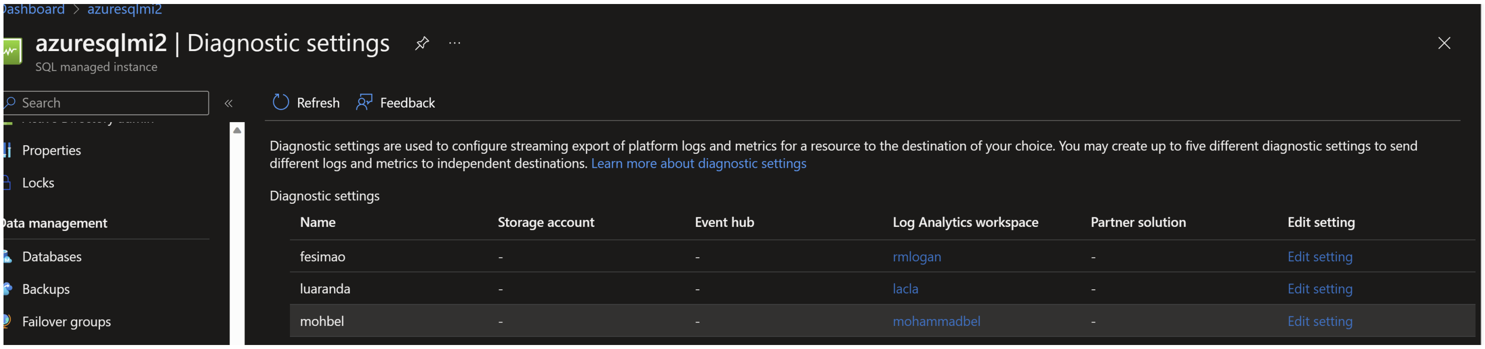
Issue

Audit setup with Diagnostic settings setup to send audit logs to Log Analytics.

Audit log records are not being written on Log Analytics.

Investigation/Analysis

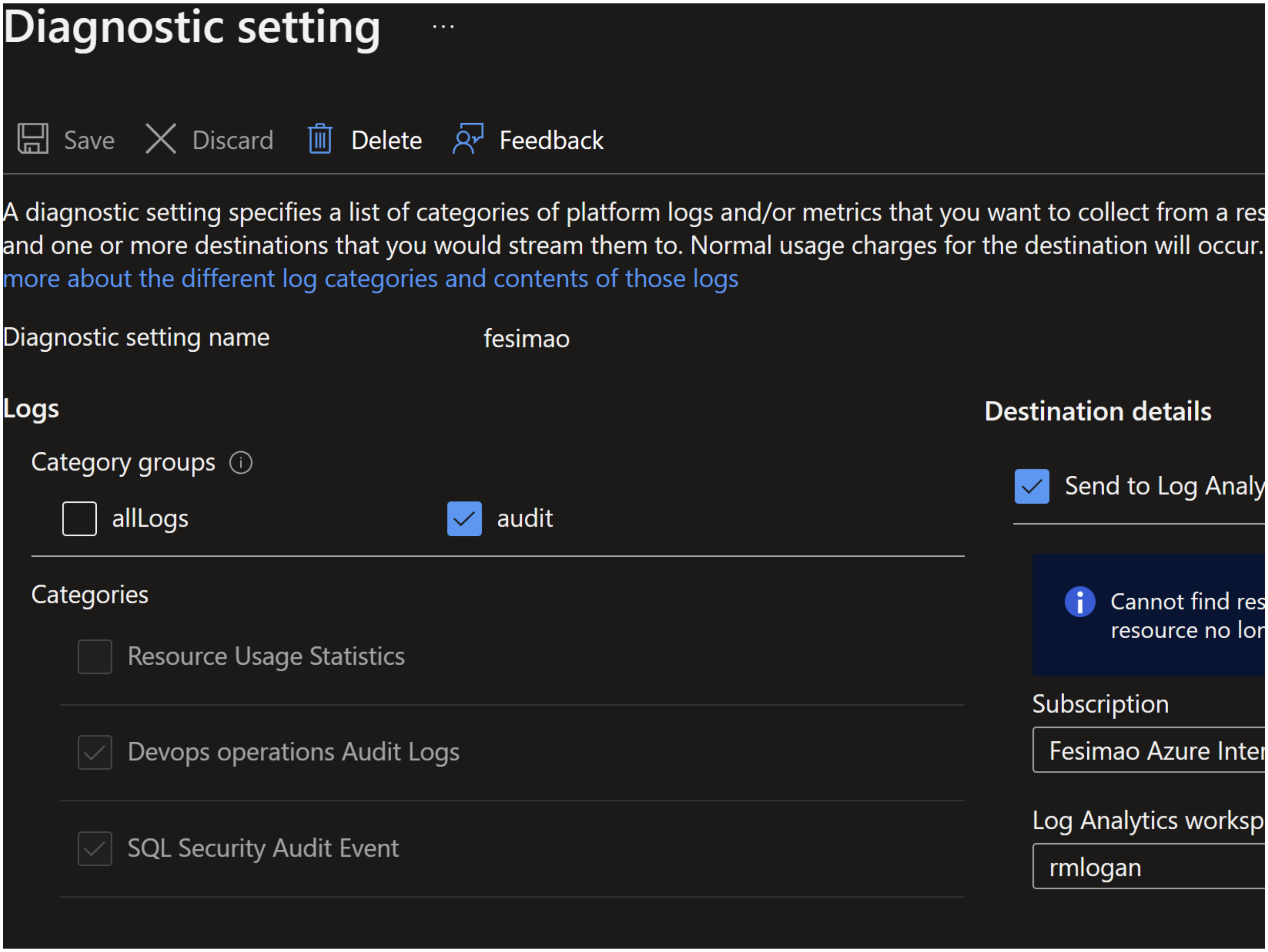
First verify if Diagnostic Settings are being sent log analytics. For example:



Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. Learn more about diagnostic settings

Diagnostic settings

Name	Storage account	Event hub	Log Analytics workspace	Partner solution	Edit setting
fesimao	-	-	rmlogan	-	Edit setting
luaranda	-	-	lacla	-	Edit setting
mohbel	-	-	mohammadbel	-	Edit setting



A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a res
and one or more destinations that you would stream them to. Normal usage charges for the destination will occur.
more about the different log categories and contents of those logs

Diagnostic setting name fesimao

Logs

Category groups

□ allLogs ☑ audit

Categories

□ Resource Usage Statistics

☑ Devops operations Audit Logs

☑ SQL Security Audit Event

Destination details

☑ Send to Log Analy

Cannot find res
resource no lon

Subscription

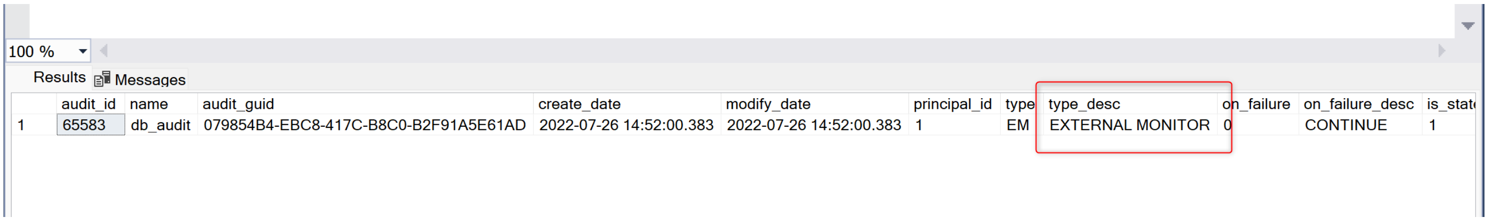
Fesimao Azure Inter

Log Analytics worksp

rmlogan

From SSMS, confirm that the audit is being sent to external_monitor

```
select * from sys.server_audits
where name = '<audit_name>'
```



	audit_id	name	audit_guid	create_date	modify_date	principal_id	type	type_desc	on_failure	on_failure_desc	is_stat
1	65583	db_audit	079854B4-EBC8-417C-B8C0-B2F91A5E61AD	2022-07-26 14:52:00.383	2022-07-26 14:52:00.383	1	EM	EXTERNAL MONITOR	0	CONTINUE	1

Confirm the order that was used to setup. The order should be always:

- diagnostic settings
- create audit

Mitigation

Diagnostic setting have to be setup before Audit.

Follow this public document

Internal reference

361036646

How good have you found this content?

🙂 🙁