Check Firewall changes in Activity Log

Last updated by | Charlene Wang | Jan 3, 2023 at 12:30 AM PST

Contents

Issue Summary

Customer asking “who changed my firewall rules”, “what changed as made”

Troubleshooting

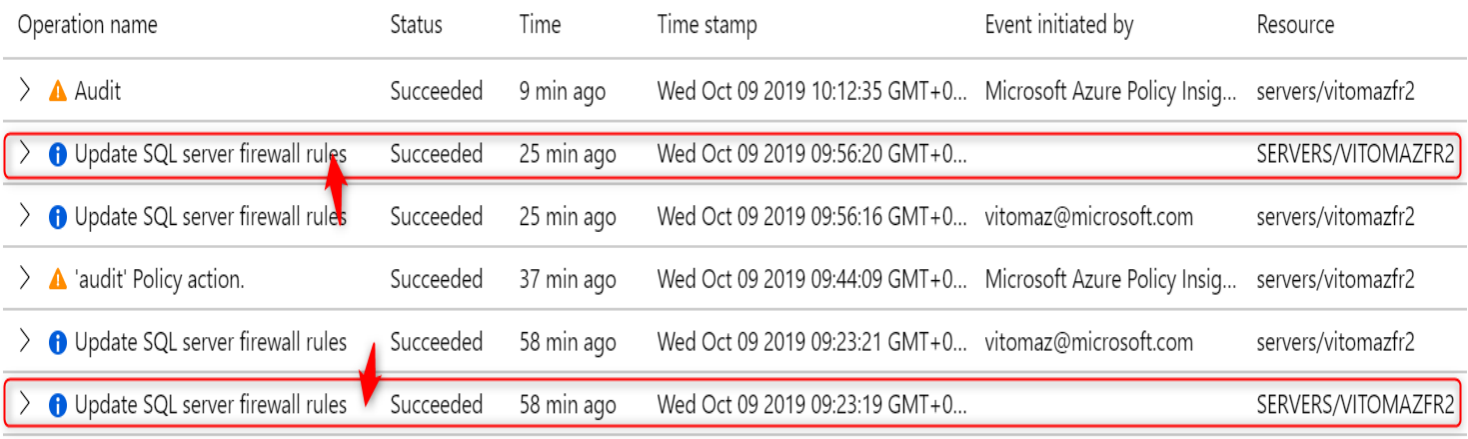
We actually expose information about the firewall change request (Description_scrubbed) in Activity Log but there are some notes:

- You need to check for another event, the original event and all sub-events will not have this information. A new event is inserted, with a new correlationId, check for the same/similar datetime and same resource.

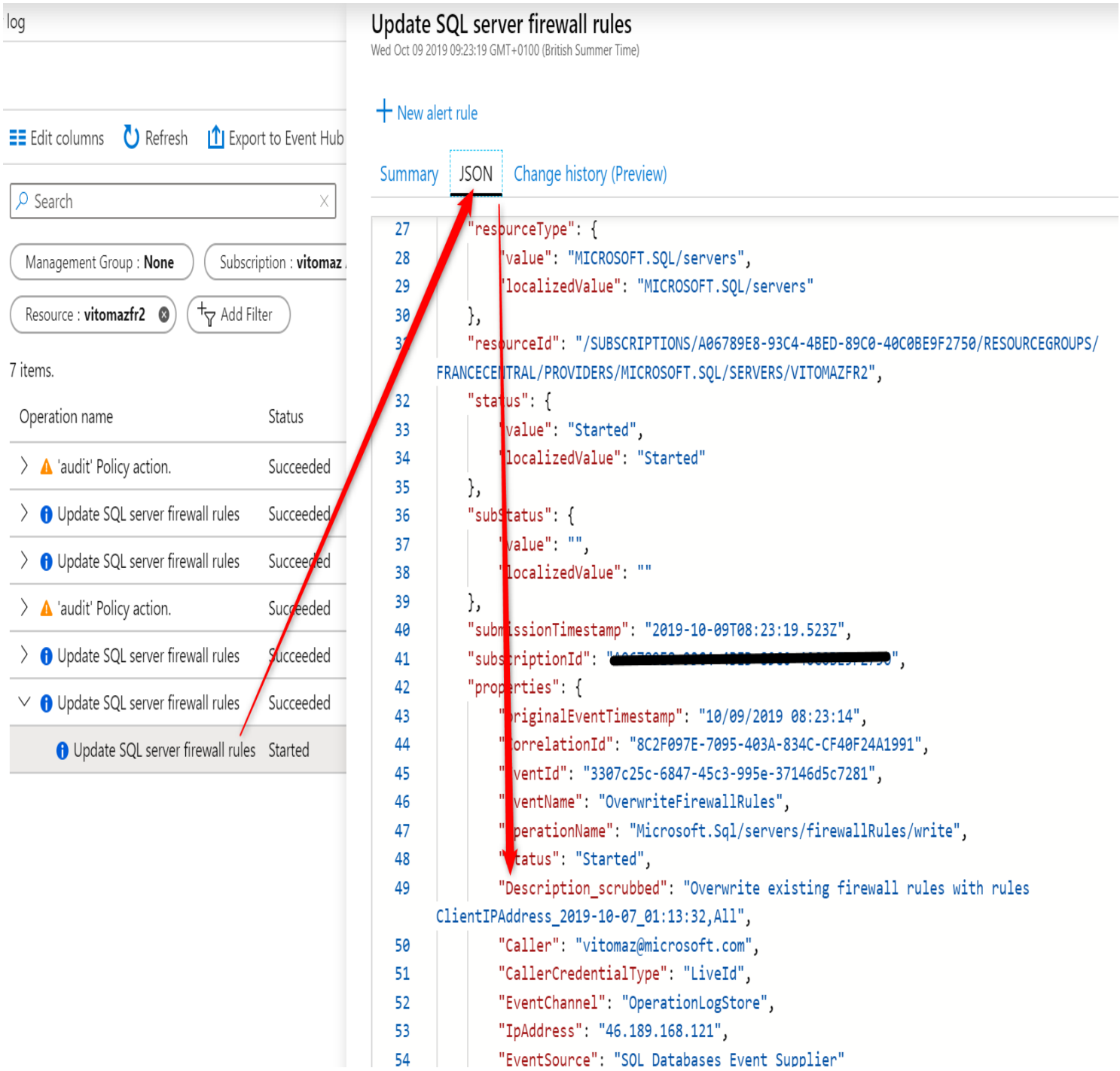
- Customer can make several changes, "Description_scrubbed" will just have info about the requested state submitted (can't clearly see what was removed).

- The second entry on event log with this information can take a large number of minutes to show up (more than 10).

- (tip) At the moment, these entries seems to have the 'Resource' column in caps and nothing on 'Event initiated by', helps identify them.



Operation name	Status	Time	Time stamp	Event initiated by	Resource
Audit	Succeeded	9 min ago	Wed Oct 09 2019 10:12:35 GMT+0...	Microsoft Azure Policy Insig...	servers/vitomazfr2
Update SQL server firewall rules	Succeeded	25 min ago	Wed Oct 09 2019 09:56:20 GMT+0...		SERVERS/VITOMAZFR2
Update SQL server firewall rules	Succeeded	25 min ago	Wed Oct 09 2019 09:56:16 GMT+0...	vitomaz@microsoft.com	servers/vitomazfr2
'audit' Policy action.	Succeeded	37 min ago	Wed Oct 09 2019 09:44:09 GMT+0...	Microsoft Azure Policy Insig...	servers/vitomazfr2
Update SQL server firewall rules	Succeeded	58 min ago	Wed Oct 09 2019 09:23:21 GMT+0...	vitomaz@microsoft.com	servers/vitomazfr2
Update SQL server firewall rules	Succeeded	58 min ago	Wed Oct 09 2019 09:23:19 GMT+0...		SERVERS/VITOMAZFR2



Classification

Root cause path - CRUD/User request/Who created/dropped/changed my resource

How good have you found this content?