Track Firewall Changes

Last updated by | Georgeta Gainariu Pache | Mar 22, 2023 at 9:12 AM PDT

Contents

Track Firewall Changes

Issue

Who changed my firewall rules and what are the changes made to my firewall settings.

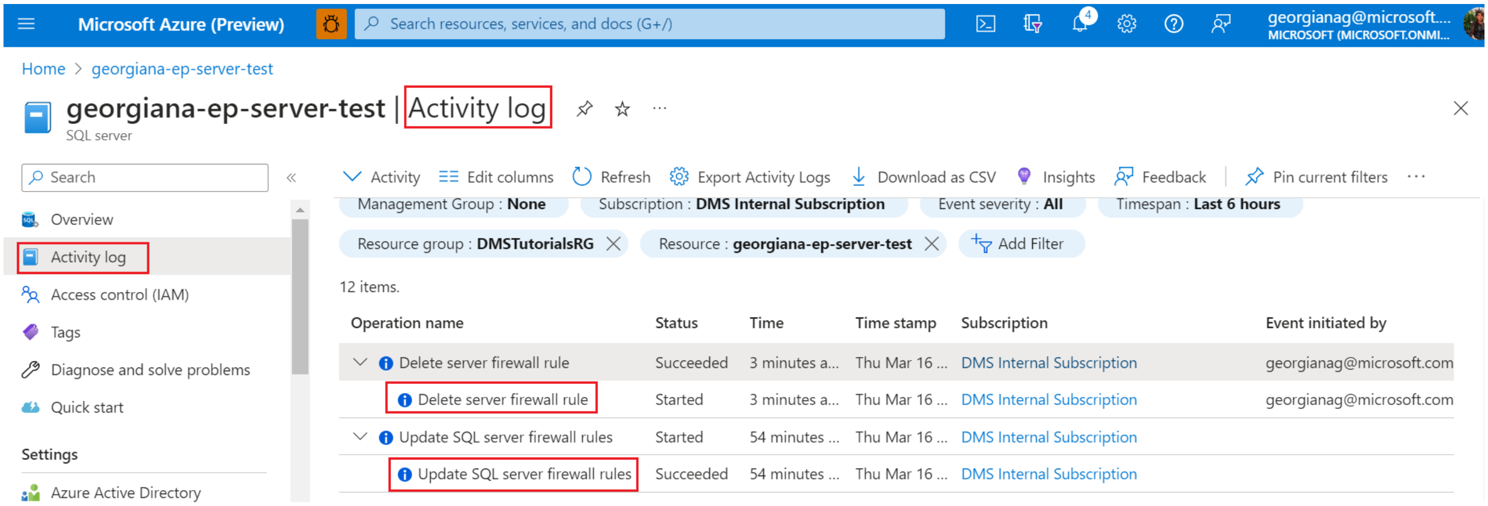
Steps:

1. Activity Log

https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log?tabs=powershell

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

- you need to check for the sub-event, as the original event, will not have complete information:



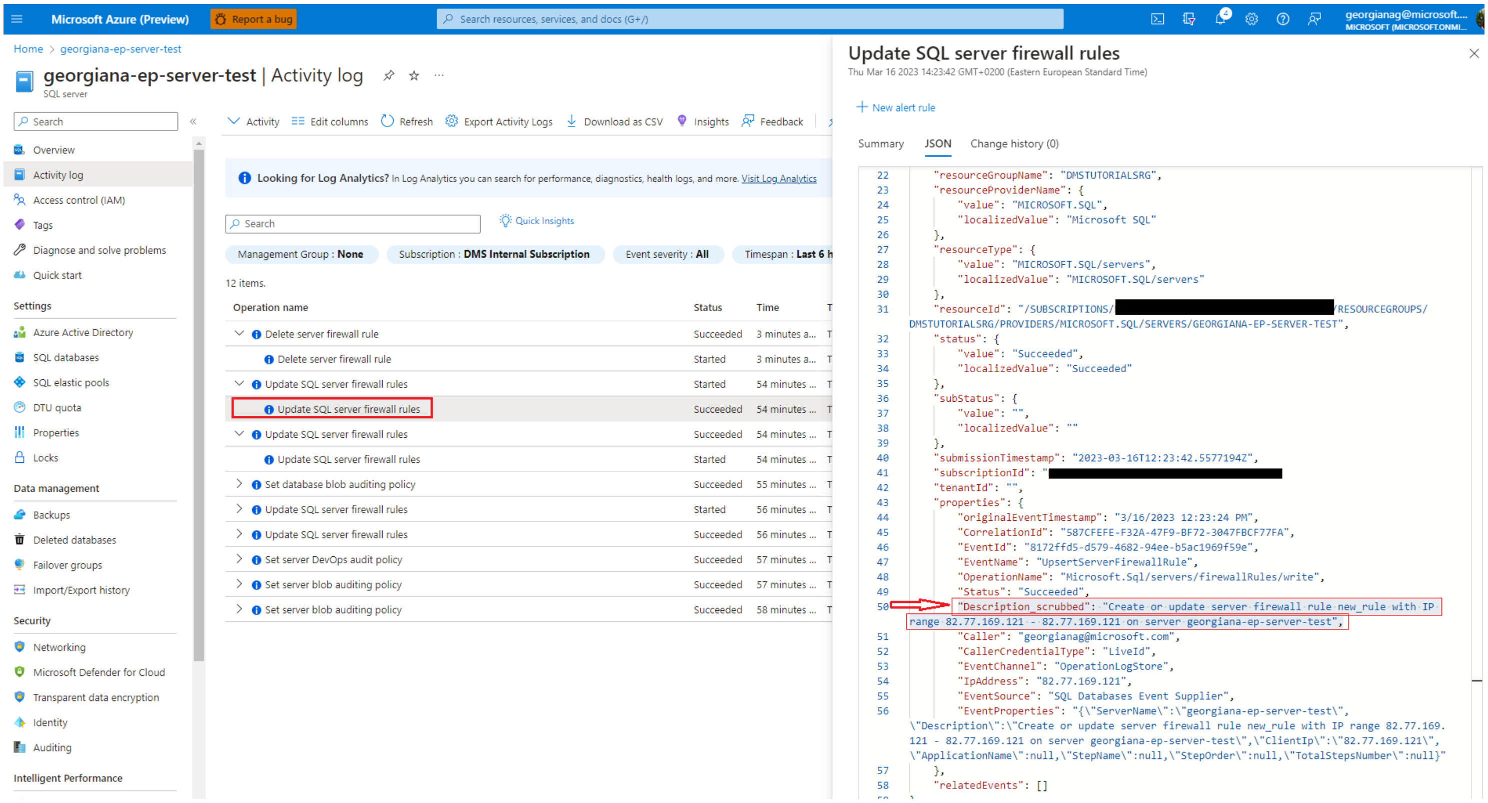
Management Group : **None** Subscription : **DMS Internal Subscription** Event severity : **All** Timespan : **Last 6 hours**

Resource group : **DMSTutorialsRG** Resource : **georgiana-ep-server-test**

12 items.

Operation name	Status	Time	Time stamp	Subscription	Event initiated by
Delete server firewall rule	Succeeded	3 minutes a...	Thu Mar 16 ...	DMS Internal Subscription	georgianag@microsoft.com
Delete server firewall rule	Started	3 minutes a...	Thu Mar 16 ...	DMS Internal Subscription	georgianag@microsoft.com
Update SQL server firewall rules	Started	54 minutes ...	Thu Mar 16 ...	DMS Internal Subscription	
Update SQL server firewall rules	Succeeded	54 minutes ...	Thu Mar 16 ...	DMS Internal Subscription	

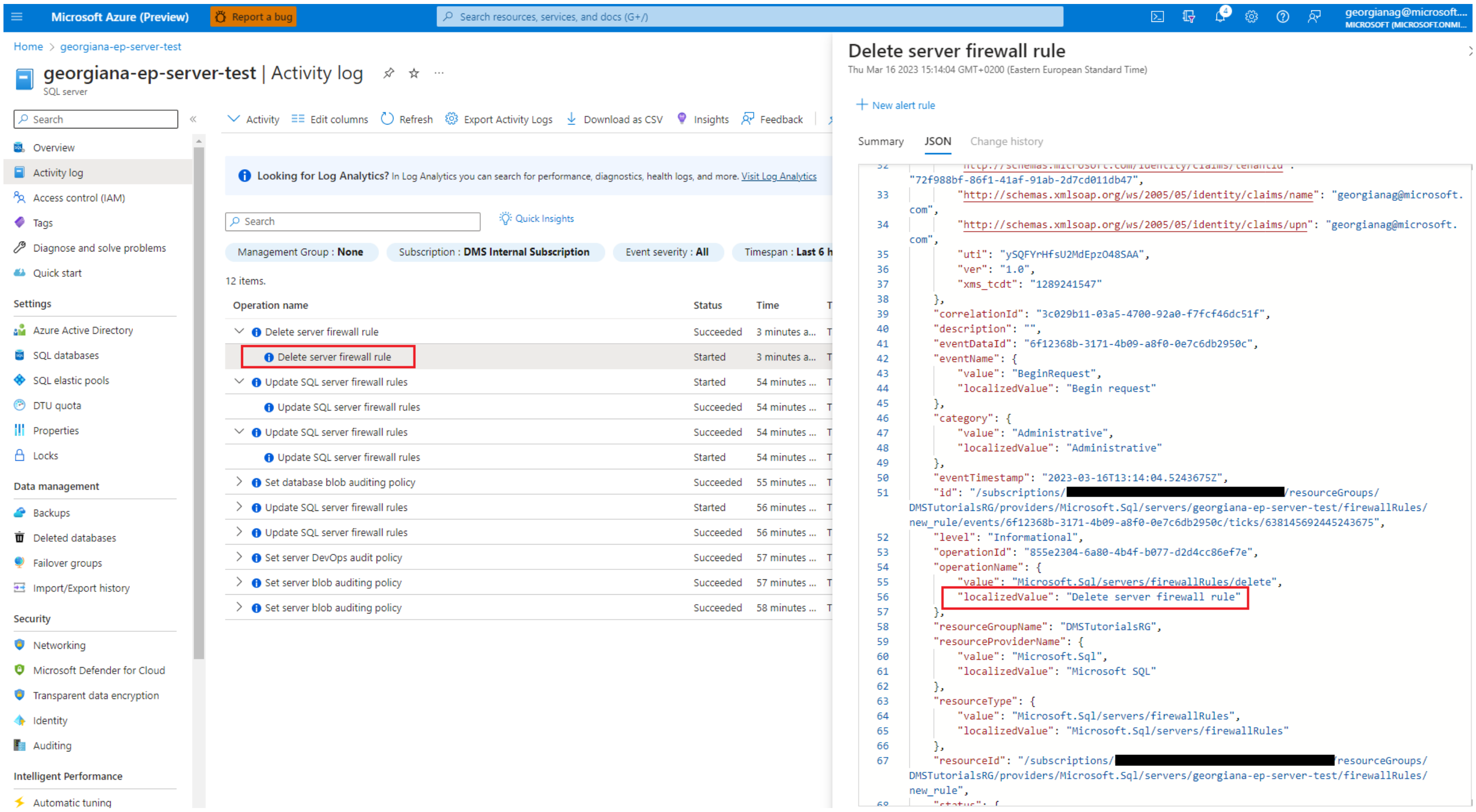
- customer can make several changes, "*Description_scrubbed*" will just have information about the request itself (*Create or update server firewall rule*) for operation name sub-event "*Update SQL server firewall rules*:



Operation name	Status	Time	T
Delete server firewall rule	Succeeded	3 minutes a...	T
Delete server firewall rule	Started	3 minutes a...	T
Update SQL server firewall rules	Started	54 minutes ...	T
Update SQL server firewall rules	Succeeded	54 minutes ...	T
Update SQL server firewall rules	Succeeded	54 minutes ...	T
Update SQL server firewall rules	Started	54 minutes ...	T
Set database blob auditing policy	Succeeded	55 minutes ...	T
Update SQL server firewall rules	Started	56 minutes ...	T
Update SQL server firewall rules	Succeeded	56 minutes ...	T
Set server DevOps audit policy	Succeeded	57 minutes ...	T
Set server blob auditing policy	Succeeded	57 minutes ...	T
Set server blob auditing policy	Succeeded	58 minutes ...	T

```
    "resourceGroupName": "DMSTUTORIALSRG",
    "resourceProviderName": {
        "value": "MICROSOFT.SQL",
        "localizedValue": "Microsoft SQL"
    },
    "resourceType": {
        "value": "MICROSOFT.SQL/servers",
        "localizedValue": "MICROSOFT.SQL/servers"
    },
    "resourceId": "/SUBSCRIPTIONS/[redacted]/RESOURCEGROUPS/
DMSTUTORIALSRG/PROVIDERS/MICROSOFT.SQL/SERVERS/GEORGIANA-EP-SERVER-TEST",
    "status": {
        "value": "Succeeded",
        "localizedValue": "Succeeded"
    },
    "subStatus": {
        "value": "",
        "localizedValue": ""
    },
    "submissionTimestamp": "2023-03-16T12:23:42.5577194Z",
    "subscriptionId": "[redacted]
    "tenantId": "",
    "properties": {
        "originalEventTimestamp": "3/16/2023 12:23:24 PM",
        "CorrelationId": "587CFEFE-F32A-47F9-BF72-3047FBCF77FA",
        "EventId": "8172ffd5-d579-4682-94ee-b5ac1969f59e",
        "EventName": "UpsertServerFirewallRule",
        "OperationName": "Microsoft.Sql/servers/firewallRules/write",
        "Status": "Succeeded",
        "Description_scrubbed": "Create or update server firewall rule new_rule with IP
range 82.77.169.121 - 82.77.169.121 on server georgiana-ep-server-test",
        "Caller": "georgianag@microsoft.com",
        "CallerCredentialType": "LiveId",
        "EventChannel": "OperationLogStore",
        "IpAddress": "82.77.169.121",
        "EventSource": "SQL Databases Event Supplier",
        "EventProperties": "{\"ServerName\":\"georgiana-ep-server-test\",
\"Description\":\"Create or update server firewall rule new_rule with IP range 82.77.169.
121 - 82.77.169.121 on server georgiana-ep-server-test\",\"ClientIp\":\"82.77.169.121\",
\"ApplicationName\":null,\"StepName\":null,\"StepOrder\":null,\"TotalStepsNumber\":null}"
    },
    "relatedEvents": []
```

- when we have a delete operation, we should be able to see this information under operation name sub-event *Delete server firewall rule*:



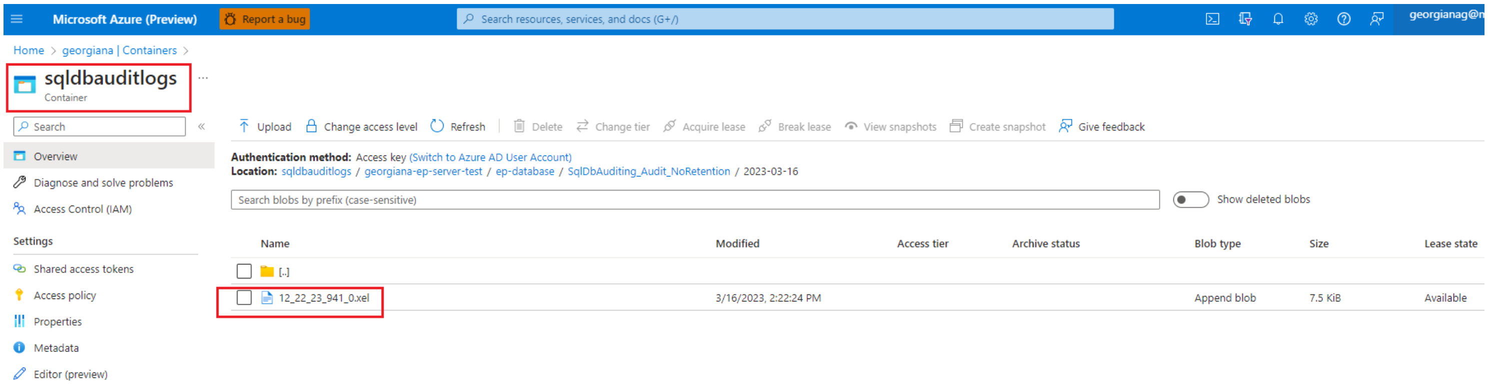
Operation name	Status	Time	T
Delete server firewall rule	Succeeded	3 minutes a...	T
Delete server firewall rule	Started	3 minutes a...	T
Update SQL server firewall rules	Started	54 minutes ...	T
Update SQL server firewall rules	Succeeded	54 minutes ...	T
Update SQL server firewall rules	Succeeded	54 minutes ...	T
Update SQL server firewall rules	Started	54 minutes ...	T
Set database blob auditing policy	Succeeded	55 minutes ...	T
Update SQL server firewall rules	Started	56 minutes ...	T
Update SQL server firewall rules	Succeeded	56 minutes ...	T
Set server DevOps audit policy	Succeeded	57 minutes ...	T
Set server blob auditing policy	Succeeded	57 minutes ...	T
Set server blob auditing policy	Succeeded	58 minutes ...	T

```
        "http://schemas.microsoft.com/identity/claims/tenantid":
"72f988bf-86f1-41af-91ab-2d7cd011db47",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name": "georgianag@microsoft.
com",
        "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn": "georgianag@microsoft.
com",
        "uti": "ySQFYrHfsU2MdEpzO48SAA",
        "ver": "1.0",
        "xms_tcdt": "1289241547"
    },
    "correlationId": "3c029b11-03a5-4700-92a0-f7fcf46dc51f",
    "description": "",
    "eventDataId": "6f12368b-3171-4b09-a8f0-0e7c6db2950c",
    "eventName": {
        "value": "BeginRequest",
        "localizedValue": "Begin request"
    },
    "category": {
        "value": "Administrative",
        "localizedValue": "Administrative"
    },
    "eventTimestamp": "2023-03-16T13:14:04.5243675Z",
    "id": "/subscriptions/[redacted]/resourceGroups/
DMSTutorialsRG/providers/Microsoft.Sql/servers/georgiana-ep-server-test/firewallRules/
new_rule/events/6f12368b-3171-4b09-a8f0-0e7c6db2950c/ticks/638145692445243675",
    "level": "Informational",
    "operationId": "855e2304-6a80-4b4f-b077-d2d4cc86ef7e",
    "operationName": {
        "value": "Microsoft.Sql/servers/firewallRules/delete",
        "localizedValue": "Delete server firewall rule"
    },
    "resourceGroupName": "DMSTutorialsRG",
    "resourceProviderName": {
        "value": "Microsoft.Sql",
        "localizedValue": "Microsoft SQL"
    },
    "resourceType": {
        "value": "Microsoft.Sql/servers/firewallRules",
        "localizedValue": "Microsoft.Sql/servers/firewallRules"
    },
    "resourceId": "/subscriptions/[redacted]/resourceGroups/
DMSTutorialsRG/providers/Microsoft.Sql/servers/georgiana-ep-server-test/firewallRules/
new_rule",
    "status": {
```

2. Auditing

https://learn.microsoft.com/en-us/azure/azure-sql/database/auditing-overview?view=azuresql https://learn.microsoft.com/en-us/azure/azure-sql/database/audit-log-format?view=azuresql

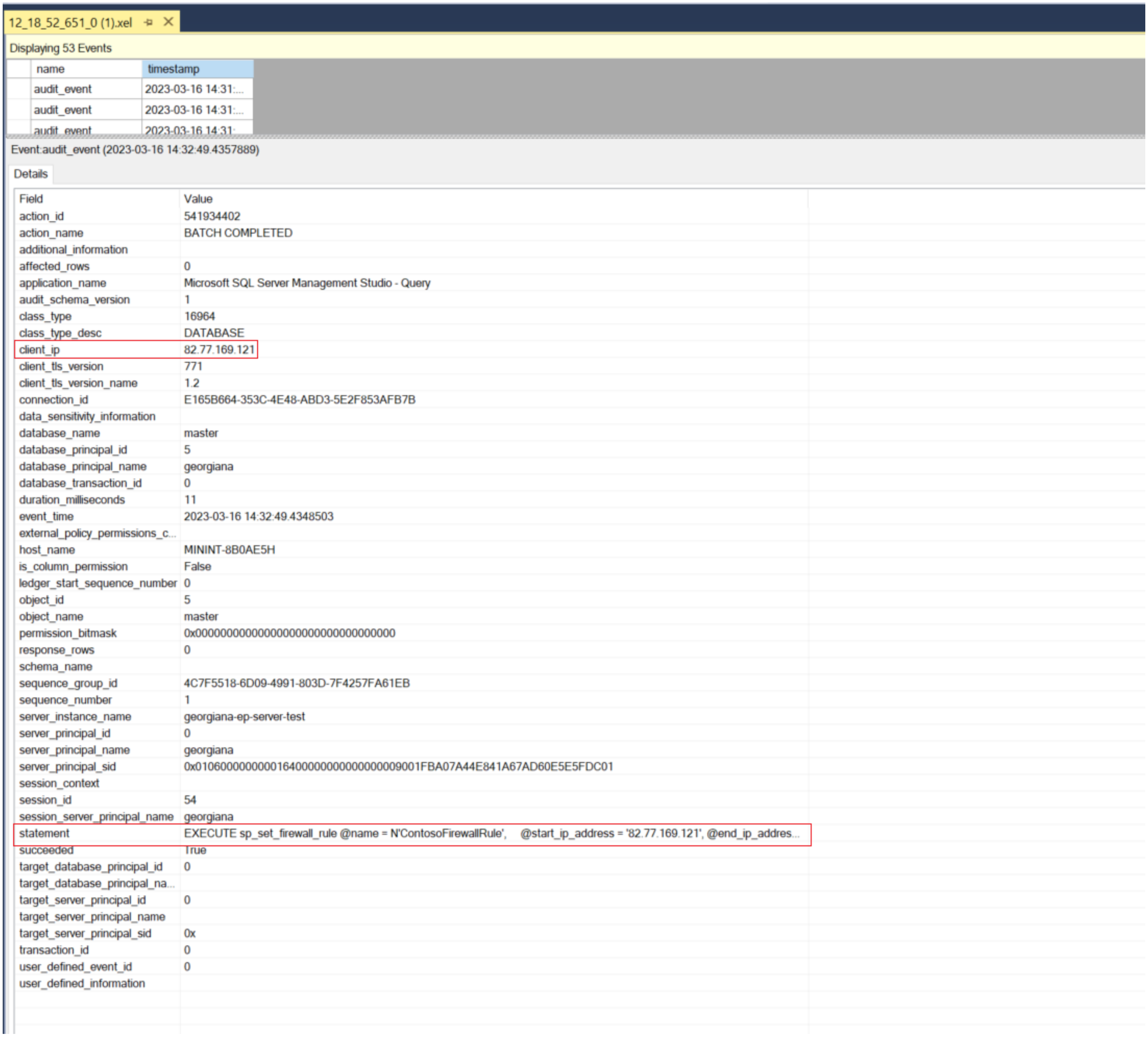
- if auditing is already in place/ set up, you can check for any changes done to the firewall, by accessing the storage where the auditing is synced to:



Authentication method: Access key (Switch to Azure AD User Account)
Location: sqldbauditlogs / georgiana-ep-server-test / ep-database / SqlDbAuditing_Audit_NoRetention / 2023-03-16

	Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
□	[..]						
□	12_22_23_941_0.xel	3/16/2023, 2:22:24 PM			Append blob	7.5 KiB	Available

- we can see how the updated firewall, has been done with a T-SQL query via SSMS, by specific IP user:



12_18_52_651_0 (1).xel

Displaying 53 Events

name	timestamp
audit_event	2023-03-16 14:31:...
audit_event	2023-03-16 14:31:...
audit_event	2023-03-16 14:31:

Event:audit_event (2023-03-16 14:32:49.4357889)

Details

Field	Value
action_id	541934402
action_name	BATCH COMPLETED
additional_information	
affected_rows	0
application_name	Microsoft SQL Server Management Studio - Query
audit_schema_version	1
class_type	16964
class_type_desc	DATABASE
client_ip	82.77.169.121
client_tls_version	771
client_tls_version_name	1.2
connection_id	E165B664-353C-4E48-ABD3-5E2F853AFB7B
data_sensitivity_information	
database_name	master
database_principal_id	5
database_principal_name	georgiana
database_transaction_id	0
duration_milliseconds	11
event_time	2023-03-16 14:32:49.4348503
external_policy_permissions_c...	
host_name	MININT-8B0AE5H
is_column_permission	False
ledger_start_sequence_number	0
object_id	5
object_name	master
permission_bitmask	0x00000000000000000000000000000000
response_rows	0
schema_name	
sequence_group_id	4C7F5518-6D09-4991-803D-7F4257FA61EB
sequence_number	1
server_instance_name	georgiana-ep-server-test
server_principal_id	0
server_principal_name	georgiana
server_principal_sid	0x010600000000016400000000000000009001FBA07A44E841A67AD60E5E5FDC01
session_context	
session_id	54
session_server_principal_name	georgiana
statement	EXECUTE sp_set_firewall_rule @name = N'ContosoFirewallRule', @start_ip_address = '82.77.169.121', @end_ip_addres...
succeeded	True
target_database_principal_id	0
target_database_principal_na...	
target_server_principal_id	0
target_server_principal_name	
target_server_principal_sid	0x
transaction_id	0
user_defined_event_id	0
user_defined_information	

3. Monitor Azure Firewall logs and metrics

https://learn.microsoft.com/en-us/azure/firewall/firewall-diagnostics https://learn.microsoft.com/en-us/azure/firewall/logs-and-metrics

- additional information on Azure Firewall using firewall logs.
- you can also use activity logs to audit operations on Azure Firewall resources. Using metrics, you can view performance counters in the portal.

Classification

Root Cause: Azure SQL DB v2\Connectivity\Login Errors\Firewall errors and misconfigurations

How good have you found this content?

☺ ☹