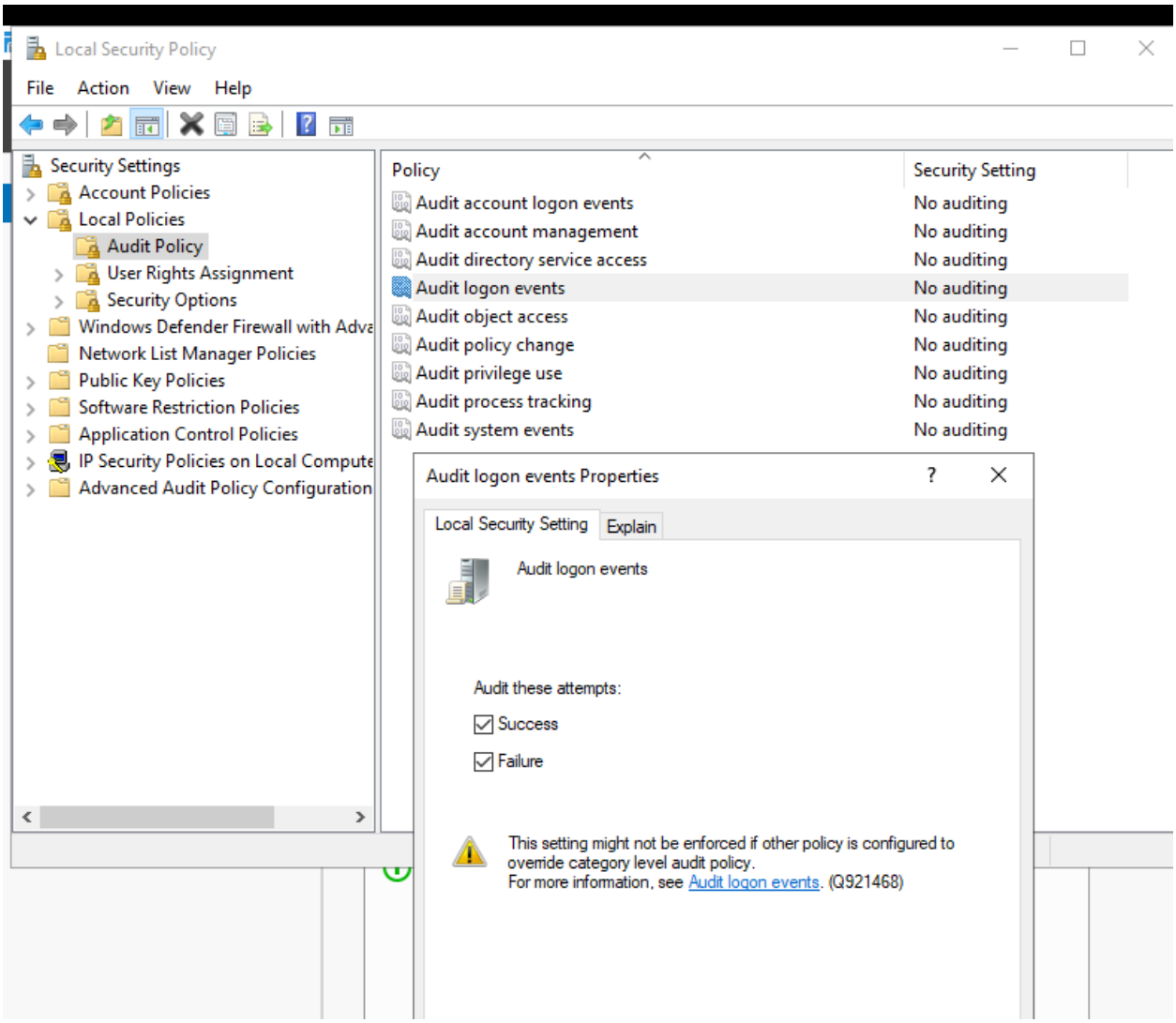
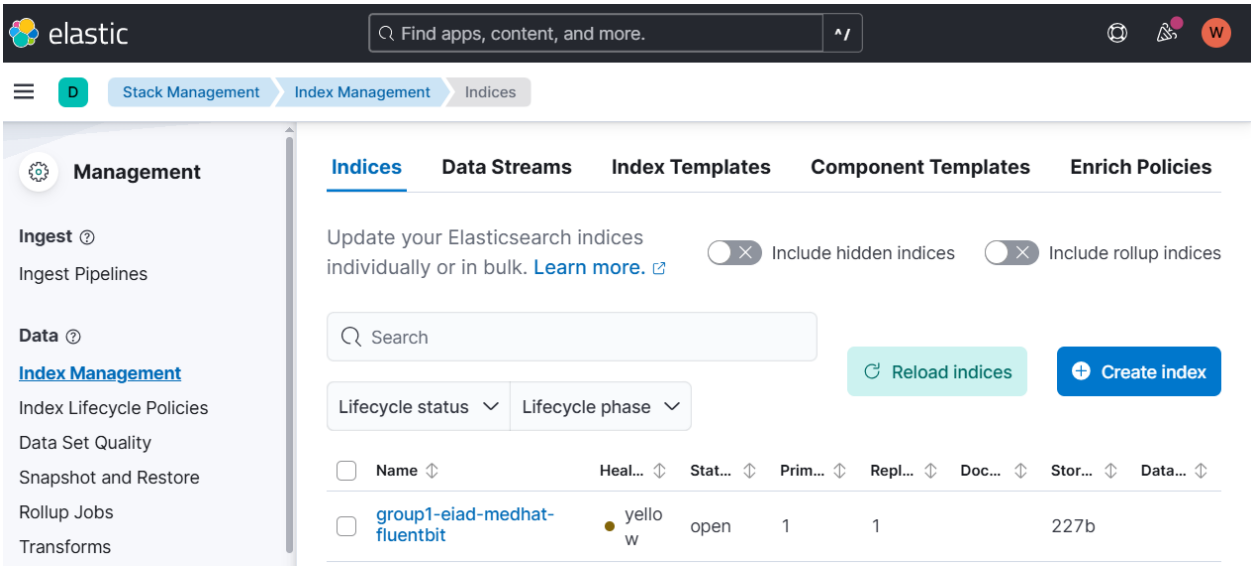

Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
Policy
Security Setting
Audit account logon events
No auditing
Audit account management
No auditing
Audit directory service access
No auditing
Audit logon events
No auditing
Audit object access
No auditing
Audit policy change
No auditing
Audit privilege use
No auditing
Audit process tracking
No auditing
Audit system events
No auditing
Audit logon events Properties
Local Security Setting
Explain
Audit logon events
Audit these attempts:
Success
Failure
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)

@timestamp	Document
Aug 28, 2025 @ 11:27:08.578	**@timestamp** Aug 28, 2025 @ 11:27:08.578 **agent.ephemeral_id** 739b5fc1-6061-4eab-8e6a-b2c202d3bd4c **agent.id** 568bf57c-d07d-46db-9202-3d1b72d70476 **agent.name** Group-Eiad-Medhat **agent.type** filebeat **agent.version** 8.15.2 **data_stream.dataset** system.securit y **data_stream.namespace** default **data_stream.type** logs **destination.ip** 198.96.95.202 **destination.port** 9,200 **ecs.version** 8.11.…
Aug 28, 2025 @ 11:27:08.578	**@timestamp** Aug 28, 2025 @ 11:27:08.578 **agent.ephemeral_id** 739b5fc1-6061-4eab-8e6a-b2c202d3bd4c **agent.id** 568bf57c-d07d-46db-9202-3d1b72d70476 **agent.name** Group-Eiad-Medhat **agent.type** filebeat **agent.version** 8.15.2 **data_stream.dataset** winlog.winlo g **data_stream.namespace** default **data_stream.type** logs **ecs.version** 8.0.0 **elastic_agent.id** 568bf57c-d07d-46db-9202-3d1b72d7047…
Aug 28, 2025 @ 11:27:08.577	**@timestamp** Aug 28, 2025 @ 11:27:08.577 **agent.ephemeral_id** 739b5fc1-6061-4eab-8e6a-b2c202d3bd4c **agent.id** 568bf57c-d07d-46db-9202-3d

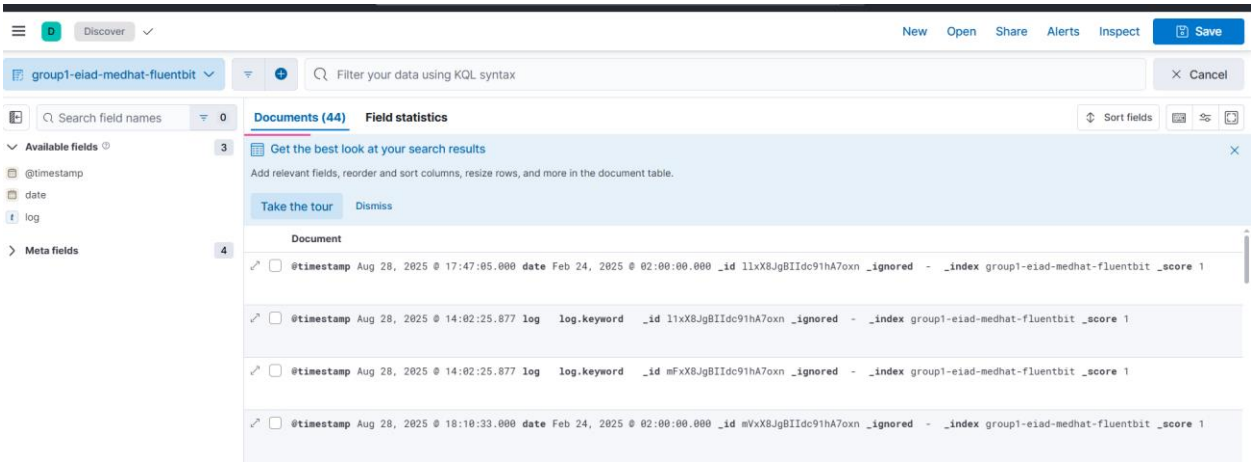
Select Administrator: Windows PowerShell

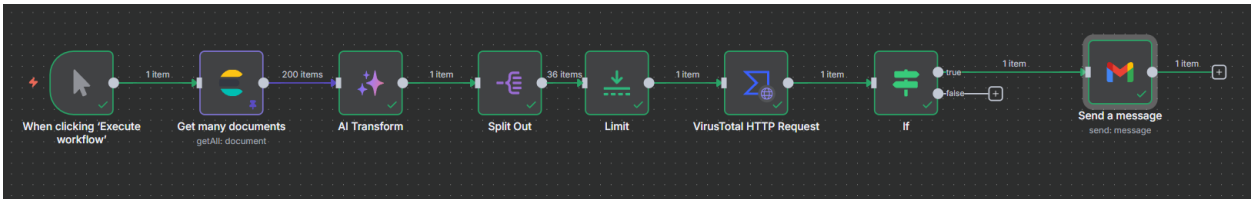
/elastic/beats/v7/libbeat/cmd/instance.(*Beat).logSystemInfo","file.name":"instance/beat.go","file.line":1393},"message":"Build info","service.name":"winlogbeat","system_info":{"build":{"commit":"b036c1c565cf24c9b720605632234d20cb9dba60","libbeat":"9.1.2","time":"2025-08-11T13:56:43.000Z","version":"9.1.2"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2025-08-28T11:27:14.761+0300","log.logger":"beat","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).logSystemInfo","file.name":"instance/beat.go","file.line":1396},"message":"Go runtime info","service.name":"winlogbeat","system_info":{"go":{"os":"windows","arch":"amd64","max_procs":8,"version":"go1.24.4"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2025-08-28T11:27:14.787+0300","log.logger":"beat","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).logSystemInfo","file.name":"instance/beat.go","file.line":1402},"message":"Host info","service.name":"winlogbeat","system_info":{"host":{"architecture":"x86_64","native_architecture":"x86_64","boot_time":"2025-08-28T11:15:54+03:00","name":"Group-Eiad-Medhat","ip":["fe80::437:b8e8:b66c:bfcf","169.254.80.200","fe80::fbbb:b161:242e:10bd","192.168.56.1","fe80::7fde:26e1:d439:a91c","169.254.43.135","fe80::e1c9:33f7:853f:8e7a","169.254.187.203","fe80::b0dd:f730:ee14:f3ec","192.168.133.1","fe80::3190:8873:d7d0:c6af","192.168.153.1","fe80::cbbb:795d:c02a:b560","10.151.1.252","::1","127.0.0.1"],"kernel_version":"10.0.19041.6216 (WinBuild.160101.0800)","mac":["84:a9:3e:b6:c7:ff","0a:00:27:00:00:13","b4:69:21:77:51:ce","b6:69:21:77:51:cd","00:50:56:c0:00:01","00:50:56:c0:00:08","b4:69:21:77:51:cd"],"os":{"type":"windows","family":"windows","platform":"windows","name":"Windows 10 Pro","version":"10.0","major":10,"minor":0,"patch":0,"build":"19045.6216"},"timezone":"EEST","timezone_offset_sec":10800,"id":"6dd4950c-bd9f-4426-be05-c8666af998e2"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2025-08-28T11:27:14.788+0300","log.logger":"beat","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).logSystemInfo","file.name":"instance/beat.go","file.line":1431},"message":"Process info","service.name":"winlogbeat","system_info":{"process":{"cwd":"C:\\Program Files\\Winlogbeat","exe":"C:\\Program Files\\winlogbeat\\winlogbeat.exe","name":"winlogbeat.exe","pid":12860,"ppid":16136,"start_time":"2025-08-28T11:27:14.448+0300"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2025-08-28T11:27:14.838+0300","log.logger":"elasticsearch.esclientleg","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/esleg/eslegclient.NewConnection","file.name":"eslegclient/connection.go","file.line":132},"message":"elasticsearch url: http://198.96.95.202:9200","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-08-28T11:27:14.838+0300","log.logger":"publisher","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/publisher/pipeline.LoadWithSettings","file.name":"pipeline/module.go","file.line":105},"message":"Beat name: Group-Eiad-Medhat","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-08-28T11:27:14.839+0300","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.New","file.name":"beater/winlogbeat.go","file.line":70},"message":"State will be read from and persisted to C:\\Program Files\\Winlogbeat\\data\\.winlogbeat.yml","service.name":"winlogbeat","ecs.version":"1.6.0"}

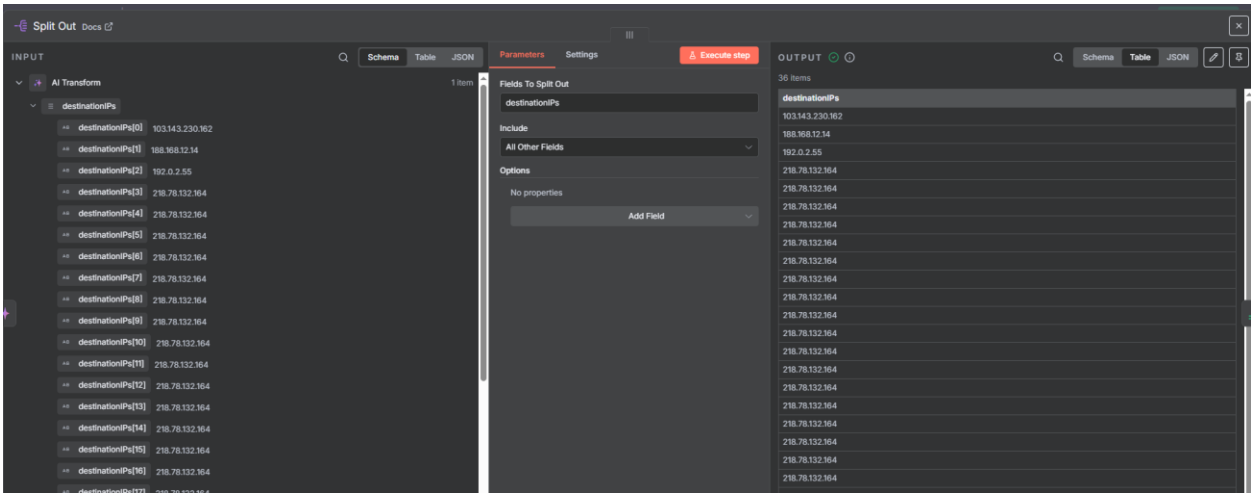
Config OK
PS C:\Program Files\Winlogbeat> .\winlogbeat.exe test output
>>
elasticsearch: http://198.96.95.202:9200...
  parse url... OK
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 198.96.95.202
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... ERROR Get "http://198.96.95.202:9200": EOF




```
eiadmedhat@Group1-Eiad-Medhat:~$ sudo systemctl restart fluent-bit
eiadmedhat@Group1-Eiad-Medhat:~$ sudo journalctl -u fluent-bit -f
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [simd    ] SSE2
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [cmetrics] version=1.0.5
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [ctraces ] version=0.6.6
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [input:tail:tail.0] initializing
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [input:tail:tail.0] storage_strategy='memory' (memory only)
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [sp] stream processor started
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [engine] Shutdown Grace Period=5, Shutdown Input Grace Period=2
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [output:es:es.0] worker #0 started
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [input:tail:tail.0] inotify_fs_add(): inode=1179732 watch_fd=1 name=/home/ei
admedhat/Desktop/firewall.log
Aug 28 13:37:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:08] [ in
fo] [output:es:es.0] worker #1 started
Aug 28 13:37:25 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:37:25] [ in
fo] [input:tail:tail.0] inotify_fs_remove(): inode=1179732 watch_fd=1
Aug 28 13:38:08 Group1-Eiad-Medhat fluent-bit[10978]: [2025/08/28 13:38:08] [ in
fo] [input:tail:tail.0] inotify_fs_add(): inode=1179752 watch_fd=2 name=/home/ei
admedhat/Desktop/firewall.log
```







eiadmedhat337@gmail.com

This Ip 103.143.230.162 Is Malicious By Virustotal
