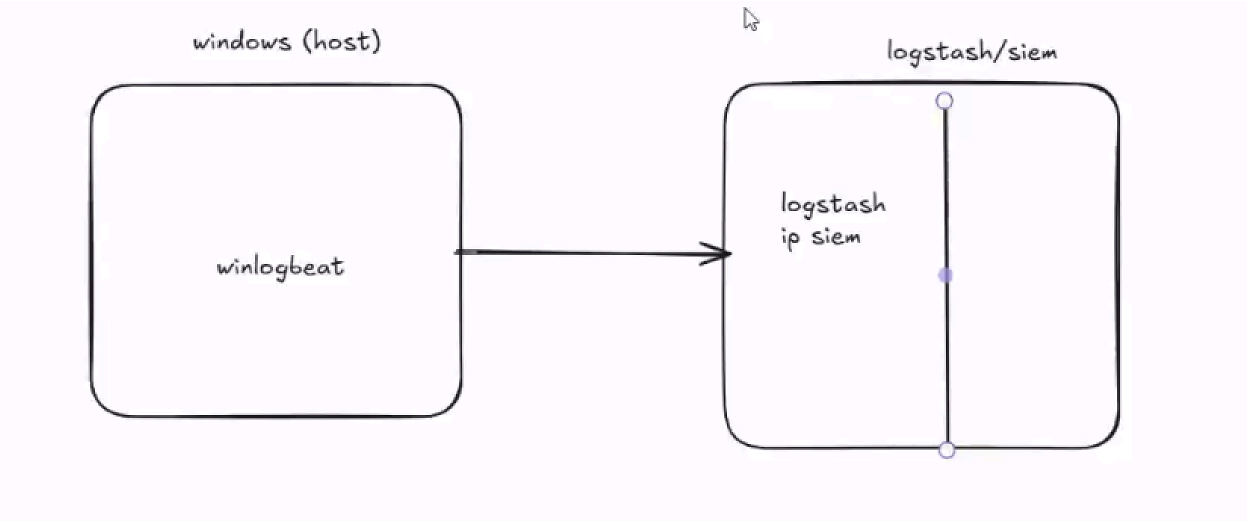
Winlogbeat_Logstash_Elastic_Setup

Yehia A. Mostafa

Winlogbeat + Logstash Setup Task Description



- Requirements

1. install winlogbeat in windows (host) and configure it to send logs to logstash
2. install logstash in linux (siem machine) and send logs to elastic

   Why add Logstash in the middle?

   1. **Parsing & Enrichment**
      - Raw Windows logs can be messy.
      - Logstash pipelines let you extract fields, apply filters, add geoIP, lookup data, normalize timestamps, etc.
   2. **Centralized Processing**
      - If you have multiple log sources (Winlogbeat, Filebeat, Syslog, etc.), Logstash acts as a hub to unify and normalize data before sending to Elasticsearch.
   3. **Flexibility**
      - You can route logs to multiple outputs (Elasticsearch, Kafka, S3, SIEM, etc.).
      - Winlogbeat alone can't do complex routing.

    4. **Reliability**
        - Logstash can buffer, retry, and handle backpressure better than sending directly from the endpoint.
3. screenshots of conf OK and from running logstash and success kibana

Remove Elastic Agent from Windows

Open **PowerShell** as Administrator and run:

```
& "C:\Program Files\Elastic\Agent\elastic-agent.exe" uninstall
```

- Removes the installed Elastic Agent service and files from your Windows host.
- Confirm the service is no longer listed `Get-Service | findstr Elastic`

Install Logstash on Linux SIEM Machine

Download & Install

```
sudo apt update
sudo apt install apt-transport-https default-jre -y
# 1. Download Elastic's GPG key and save it to /etc/apt/trusted.gpg.d/
curl -fsSL https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /etc/apt/trusted.gpg.d/elastic.gpg
# 2. Add Elastic's repository
echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
# 3. Update package lists
sudo apt update
# 4. Install Logstash
sudo apt install logstash -y
```

Configure Logstash for Winlogbeat

Create a new file:

```
sudo nano /etc/logstash/conf.d/winlogbeat.conf
```

Add:

```
input {
  beats {
    port => 5044
  }
}

output {
  elasticsearch {
    hosts => ["https://localhost:9200"]
    user => "elastic"
    password => "Yehia5050"
    ssl_enabled => true
    ssl_verification_mode => "none"
    index => "winlogbeat-%{+yyyy.MM.dd}"
  }
}
```

- Ensure **port 5044** is open on the SIEM machine:

```
sudo ufw allow 5044
```

Enable & Start Logstash

```
sudo systemctl enable logstash
sudo systemctl start logstash
sudo systemctl status logstash
```

Install Winlogbeat on Windows

Download Winlogbeat

1. Go to Elastic Downloads and download the `.zip` package for Windows.
2. Extract it to:

   ```
   C:\Program Files\Winlogbeat\winlogbeat-9.1.2-windows-x86_64
   ```

Configure Winlogbeat to send logs to Logstash

Important precautions:

- Always edit `winlogbeat.yml` **as Administrator**.
- If you keep both `output.elasticsearch` and `output.logstash` enabled, Winlogbeat will fail to start.
- You **must** comment out (disable) the Elasticsearch section if using Logstash.

Configuration (`winlogbeat.yml`)

```
#=========================== Winlogbeat inputs =====================
=========
winlogbeat.event_logs:
  - name: Security
  - name: System
  - name: Application

#=========================== Output configuration ===================
=======

# Comment out Elasticsearch output to prevent conflicts:
#output.elasticsearch:
  # Array of hosts to connect to.
 # hosts: ["localhost:9200"]

  # Protocol - either `http` (default) or `https`.
  #protocol: "https"

  # Authentication credentials - either API key or username/password.
  #api_key: "id:api_key"
  #username: "elastic"
  #password: "changeme"

  # Pipeline to route events to security, sysmon, or powershell pipelines.
  #pipeline: "winlogbeat-%{[agent.version]}-routing"

# Enable Logstash output:
output.logstash:
  hosts: ["<Logstash_Server_IP>:5044"]  # Linux SIEM machine's IP

#=========================== Logging ============================
=
logging.level: info
logging.to_files: true
logging.files:
  path: C:\Program Files\Winlogbeat\winlogbeat-9.1.2-windows-x86_64\logs
  name: winlogbeat
  keepfiles: 7
  permissions:0644
```

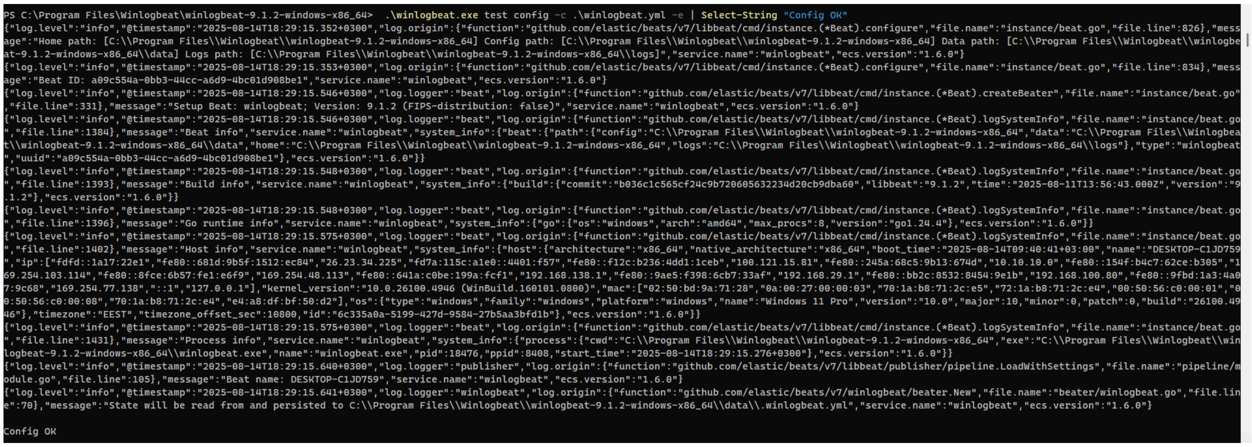
- `<Logstash_Server_IP>` is left blank in the documentation on purpose for future reference and understanding.

Test Configuration Before Installing Service

Before creating the service, run:

```
cd "C:\Program Files\Winlogbeat\winlogbeat-9.1.2-windows-x86_64"
.\winlogbeat.exe test config -c .\winlogbeat.yml -e
```

- Config is OK, you will see:



```
PS C:\Program Files\Winlogbeat\winlogbeat-9.1.2-windows-x86_64>  .\winlogbeat.exe test config -c .\winlogbeat.yml -e | Select-String "Config OK"
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.352+0300","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":826},"mess
age":"Home path: [C:\\Program Files\\Winlogbeat\\winlogbeat-9.1.2-windows-x86_64] Config path: [C:\\Program Files\\Winlogbeat\\winlogbeat-9.1.2-windows-x86_64] Data path: [C:\\Program Files\\Winlogbeat\\winlogbe
at-9.1.2-windows-x86_64\\data] Logs path: [C:\\Program Files\\Winlogbeat\\winlogbeat-9.1.2-windows-x86_64\\logs]","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.353+0300","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).configure","file.name":"instance/beat.go","file.line":834},"mess
age":"Beat ID: a09c554a-0bb3-44cc-a6d9-4bc01d908be1","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.546+0300","log.logger":"beat","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).createBeater","file.name":"instance/beat.go"
,"file.line":331},"message":"Setup Beat: winlogbeat; Version: 9.1.2 (FIPS-distribution: false)","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.546+0300","log.logger":"beat","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/cmd/instance.(*Beat).logSystemInfo","file.name":"instance/beat.go
","file.line":1384},"message":"Beat info","service.name":"winlogbeat","system_info":{"beat":{"path":{"config":"C:\\Program Files\\Winlogbeat\\winlogbeat-9.1.2-windows-x86_64","data":"C:\\Program Files\\Winlogbea
t\\winlogbeat-9.1.2-windows-x86_64\\data","home":"C:\\Program Files\\Winlogbeat\\winlogbeat-9.1.2-windows-x86_64","logs":"C:\\Program Files\\Winlogbeat\\winlogbeat-9.1.2-windows-x86_64\\logs"},"type":"winlogbeat
","uuid":"a09c554a-0bb3-44cc-a6d9-4bc01d908be1"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.548+0300","log.logger":"beat","log.origin":{"function":"github.com/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":"2025-08-14T18:29:15.548+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":"2025-08-14T18:29:15.575+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":"2025-08-14T09:40:41+03:00","name":"DESKTOP-C1JD759
","ip":["fdfd::1a17:22e1","fe80::681d:9b5f:1512:ec84","26.23.34.225","fd7a:115c:a1e0::4401:f57","fe80::f12c:b236:4dd1:1ceb","100.121.15.81","fe80::245a:68c5:9b13:674d","10.10.10.0","fe80::154f:b4c7:62ce:b305","1
69.254.103.114","fe80::8fce:6b57:fe1:e6f9","169.254.48.113","fe80::641a:c0be:199a:fcf1","192.168.138.1","fe80::9ae5:f398:6cb7:33af","192.168.29.1","fe80::bb2c:8532:8454:9e1b","192.168.100.80","fe80::9fbd:1a3:4a0
7:9c68","169.254.77.138","::1","127.0.0.1"],"kernel_version":"10.0.26100.4946 (WinBuild.160101.0800)","mac":["02:50:bd:9a:71:28","0a:00:27:00:00:03","70:1a:b8:71:2c:e5","72:1a:b8:71:2c:e4","00:50:56:c0:00:01","0
0:50:56:c0:00:08","70:1a:b8:71:2c:e4","e4:a8:df:bf:50:d2"],"os":{"type":"windows","family":"windows","platform":"windows","name":"Windows 11 Pro","version":"10.0","major":10,"minor":0,"patch":0,"build":"26100.49
46"},"timezone":"EEST","timezone_offset_sec":10800,"id":"6c335a0a-5199-427d-9584-27b5aa3bfd1b"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.575+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\\winlogbeat-9.1.2-windows-x86_64","exe":"C:\\Program Files\\Winlogbeat\\win
logbeat-9.1.2-windows-x86_64\\winlogbeat.exe","name":"winlogbeat.exe","pid":18476,"ppid":8408,"start_time":"2025-08-14T18:29:15.276+0300"},"ecs.version":"1.6.0"}}
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.640+0300","log.logger":"publisher","log.origin":{"function":"github.com/elastic/beats/v7/libbeat/publisher/pipeline.LoadWithSettings","file.name":"pipeline/m
odule.go","file.line":105},"message":"Beat name: DESKTOP-C1JD759","service.name":"winlogbeat","ecs.version":"1.6.0"}
{"log.level":"info","@timestamp":"2025-08-14T18:29:15.641+0300","log.logger":"winlogbeat","log.origin":{"function":"github.com/elastic/beats/v7/winlogbeat/beater.New","file.name":"beater/winlogbeat.go","file.lin
e":70},"message":"State will be read from and persisted to C:\\Program Files\\Winlogbeat\\winlogbeat-9.1.2-windows-x86_64\\data\\.winlogbeat.yml","service.name":"winlogbeat","ecs.version":"1.6.0"}

Config OK
```

- If you see YAML parsing errors, fix **indentation** or comment mistakes first.

Install Winlogbeat as a Windows Service

```
cd "C:\Program Files\Winlogbeat\winlogbeat-9.1.2-windows-x86_64"
Set-ExecutionPolicy Bypass -Scope Process
```

```
.\install-service-winlogbeat.ps1
```

Start Winlogbeat Service

```
Start-Service winlogbeat
```

If you get:

```
Cannot start service winlogbeat on computer '.'
```

Check:

1. Config is correct (`.\winlogbeat.exe test config ...`).
2. Elasticsearch output is **commented out** if using Logstash.
3. The Logstash server is reachable on port **5044**.

Verify Winlogbeat Service Status

```
Get-Service winlogbeat
```

```
Status   Name               DisplayName
------   ----               -----------
Running  winlogbeat         winlogbeat
```

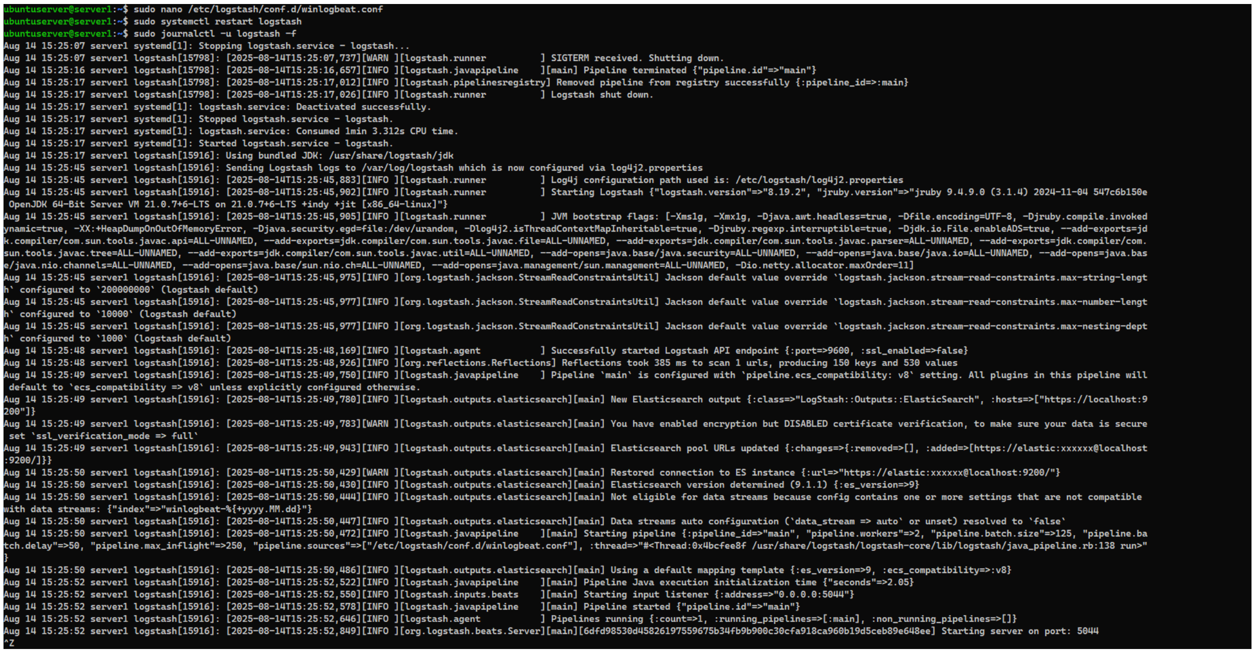
Test Data Flow

On Windows:

```
Restart-Service winlogbeat
```

On Linux:

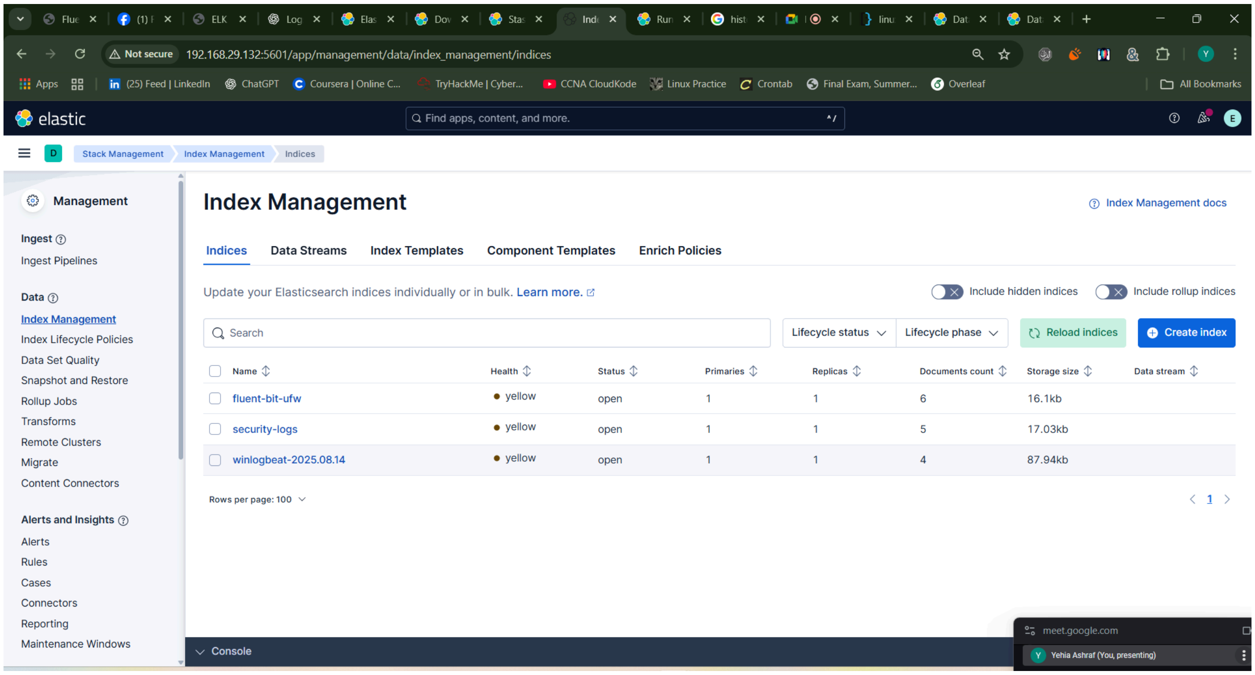
```
sudo systemctl restart logstash
sudo journalctl -u logstash -f
```



```
ubuntuserver@server1:~$ sudo nano /etc/logstash/conf.d/winlogbeat.conf
ubuntuserver@server1:~$ sudo systemctl restart logstash
ubuntuserver@server1:~$ sudo journalctl -u logstash -f
Aug 14 15:25:07 server1 systemd[1]: Stopping logstash.service - logstash...
Aug 14 15:25:07 server1 logstash[15798]: [2025-08-14T15:25:07,737][WARN ][logstash.runner          ] SIGTERM received. Shutting down.
Aug 14 15:25:16 server1 logstash[15798]: [2025-08-14T15:25:16,657][INFO ][logstash.javapipeline    ][main] Pipeline terminated {"pipeline.id"=>"main"}
Aug 14 15:25:17 server1 logstash[15798]: [2025-08-14T15:25:17,012][INFO ][logstash.pipelinesregistry] Removed pipeline from registry successfully {:pipeline_id=>:main}
Aug 14 15:25:17 server1 logstash[15798]: [2025-08-14T15:25:17,026][INFO ][logstash.runner          ] Logstash shut down.
Aug 14 15:25:17 server1 systemd[1]: logstash.service: Deactivated successfully.
Aug 14 15:25:17 server1 systemd[1]: Stopped logstash.service - logstash.
Aug 14 15:25:17 server1 systemd[1]: logstash.service: Consumed 1min 3.312s CPU time.
Aug 14 15:25:17 server1 systemd[1]: Started logstash.service - logstash.
Aug 14 15:25:17 server1 logstash[15916]: Using bundled JDK: /usr/share/logstash/jdk
Aug 14 15:25:45 server1 logstash[15916]: Sending Logstash logs to /var/log/logstash which is now configured via log4j2.properties
Aug 14 15:25:45 server1 logstash[15916]: [2025-08-14T15:25:45,883][INFO ][logstash.runner          ] Log4j configuration path used is: /etc/logstash/log4j2.properties
Aug 14 15:25:45 server1 logstash[15916]: [2025-08-14T15:25:45,902][INFO ][logstash.runner          ] Starting Logstash {"logstash.version"=>"8.19.2", "jruby.version"=>"jruby 9.4.9.0 (3.1.4) 2024-11-04 547c6b150e
 OpenJDK 64-Bit Server VM 21.0.7+6-LTS on 21.0.7+6-LTS +indy +jit [x86_64-linux]"}
Aug 14 15:25:45 server1 logstash[15916]: [2025-08-14T15:25:45,905][INFO ][logstash.runner          ] JVM bootstrap flags: [-Xms1g, -Xmx1g, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djruby.compile.invoked
ynamic=true, -XX:+HeapDumpOnOutOfMemoryError, -Djava.security.egd=file:/dev/urandom, -Dlog4j2.isThreadContextMapInheritable=true, -Djruby.regexp.interruptible=true, -Djdk.io.File.enableADS=true, --add-exports=jd
k.compiler/com.sun.tools.javac.api=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.file=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.parser=ALL-UNNAMED, --add-exports=jdk.compiler/com.
sun.tools.javac.tree=ALL-UNNAMED, --add-exports=jdk.compiler/com.sun.tools.javac.util=ALL-UNNAMED, --add-opens=java.base/java.security=ALL-UNNAMED, --add-opens=java.base/java.io=ALL-UNNAMED, --add-opens=java.bas
e/java.nio.channels=ALL-UNNAMED, --add-opens=java.base/sun.nio.ch=ALL-UNNAMED, --add-opens=java.management/sun.management=ALL-UNNAMED, -Dio.netty.allocator.maxOrder=11]
Aug 14 15:25:45 server1 logstash[15916]: [2025-08-14T15:25:45,975][INFO ][org.logstash.jackson.StreamReadConstraintsUtil] Jackson default value override `logstash.jackson.stream-read-constraints.max-string-lengt
h` configured to `200000000` (logstash default)
Aug 14 15:25:45 server1 logstash[15916]: [2025-08-14T15:25:45,977][INFO ][org.logstash.jackson.StreamReadConstraintsUtil] Jackson default value override `logstash.jackson.stream-read-constraints.max-number-lengt
h` configured to `10000` (logstash default)
Aug 14 15:25:45 server1 logstash[15916]: [2025-08-14T15:25:45,977][INFO ][org.logstash.jackson.StreamReadConstraintsUtil] Jackson default value override `logstash.jackson.stream-read-constraints.max-nesting-dept
h` configured to `1000` (logstash default)
Aug 14 15:25:48 server1 logstash[15916]: [2025-08-14T15:25:48,169][INFO ][logstash.agent           ] Successfully started Logstash API endpoint {:port=>9600, :ssl_enabled=>false}
Aug 14 15:25:48 server1 logstash[15916]: [2025-08-14T15:25:48,926][INFO ][org.reflections.Reflections] Reflections took 385 ms to scan 1 urls, producing 150 keys and 530 values
Aug 14 15:25:49 server1 logstash[15916]: [2025-08-14T15:25:49,750][INFO ][logstash.javapipeline    ] Pipeline `main` is configured with `pipeline.ecs_compatibility: v8` setting. All plugins in this pipeline will
 default to `ecs_compatibility => v8` unless explicitly configured otherwise.
Aug 14 15:25:49 server1 logstash[15916]: [2025-08-14T15:25:49,780][INFO ][logstash.outputs.elasticsearch][main] New Elasticsearch output {:class=>"LogStash::Outputs::ElasticSearch", :hosts=>["https://localhost:9
200"]}
Aug 14 15:25:49 server1 logstash[15916]: [2025-08-14T15:25:49,783][WARN ][logstash.outputs.elasticsearch][main] You have enabled encryption but DISABLED certificate verification, to make sure your data is secure
 set `ssl_verification_mode => full`
Aug 14 15:25:49 server1 logstash[15916]: [2025-08-14T15:25:49,943][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch pool URLs updated {:changes=>{:removed=>[], :added=>[https://elastic:xxxxxx@localhost
:9200/]}}
Aug 14 15:25:50 server1 logstash[15916]: [2025-08-14T15:25:50,429][WARN ][logstash.outputs.elasticsearch][main] Restored connection to ES instance {:url=>"https://elastic:xxxxxx@localhost:9200/"}
Aug 14 15:25:50 server1 logstash[15916]: [2025-08-14T15:25:50,430][INFO ][logstash.outputs.elasticsearch][main] Elasticsearch version determined (9.1.1) {:es_version=>9}
Aug 14 15:25:50 server1 logstash[15916]: [2025-08-14T15:25:50,444][INFO ][logstash.outputs.elasticsearch][main] Not eligible for data streams because config contains one or more settings that are not compatible
with data streams: {"index"=>"winlogbeat-%{+yyyy.MM.dd}"}
Aug 14 15:25:50 server1 logstash[15916]: [2025-08-14T15:25:50,447][INFO ][logstash.outputs.elasticsearch][main] Data streams auto configuration (`data_stream => auto` or unset) resolved to `false`
Aug 14 15:25:50 server1 logstash[15916]: [2025-08-14T15:25:50,472][INFO ][logstash.javapipeline    ][main] Starting pipeline {:pipeline_id=>"main", "pipeline.workers"=>2, "pipeline.batch.size"=>125, "pipeline.ba
tch.delay"=>50, "pipeline.max_inflight"=>250, "pipeline.sources"=>["/etc/logstash/conf.d/winlogbeat.conf"], :thread=>"#<Thread:0x4bcfee8f /usr/share/logstash/logstash-core/lib/logstash/java_pipeline.rb:138 run>"
}
Aug 14 15:25:50 server1 logstash[15916]: [2025-08-14T15:25:50,486][INFO ][logstash.outputs.elasticsearch][main] Using a default mapping template {:es_version=>9, :ecs_compatibility=>:v8}
Aug 14 15:25:52 server1 logstash[15916]: [2025-08-14T15:25:52,522][INFO ][logstash.javapipeline    ][main] Pipeline Java execution initialization time {"seconds"=>2.05}
Aug 14 15:25:52 server1 logstash[15916]: [2025-08-14T15:25:52,550][INFO ][logstash.inputs.beats    ][main] Starting input listener {:address=>"0.0.0.0:5044"}
Aug 14 15:25:52 server1 logstash[15916]: [2025-08-14T15:25:52,578][INFO ][logstash.javapipeline    ][main] Pipeline started {"pipeline.id"=>"main"}
Aug 14 15:25:52 server1 logstash[15916]: [2025-08-14T15:25:52,646][INFO ][logstash.agent           ] Pipelines running {:count=>1, :running_pipelines=>[:main], :non_running_pipelines=>[]}
Aug 14 15:25:52 server1 logstash[15916]: [2025-08-14T15:25:52,849][INFO ][org.logstash.beats.Server][main][6dfd98530d45826197559675b34fb9b900c30cfa918ca960b19d5ceb89e648ee] Starting server on port: 5044
^Z
```

Look for incoming beats connection.

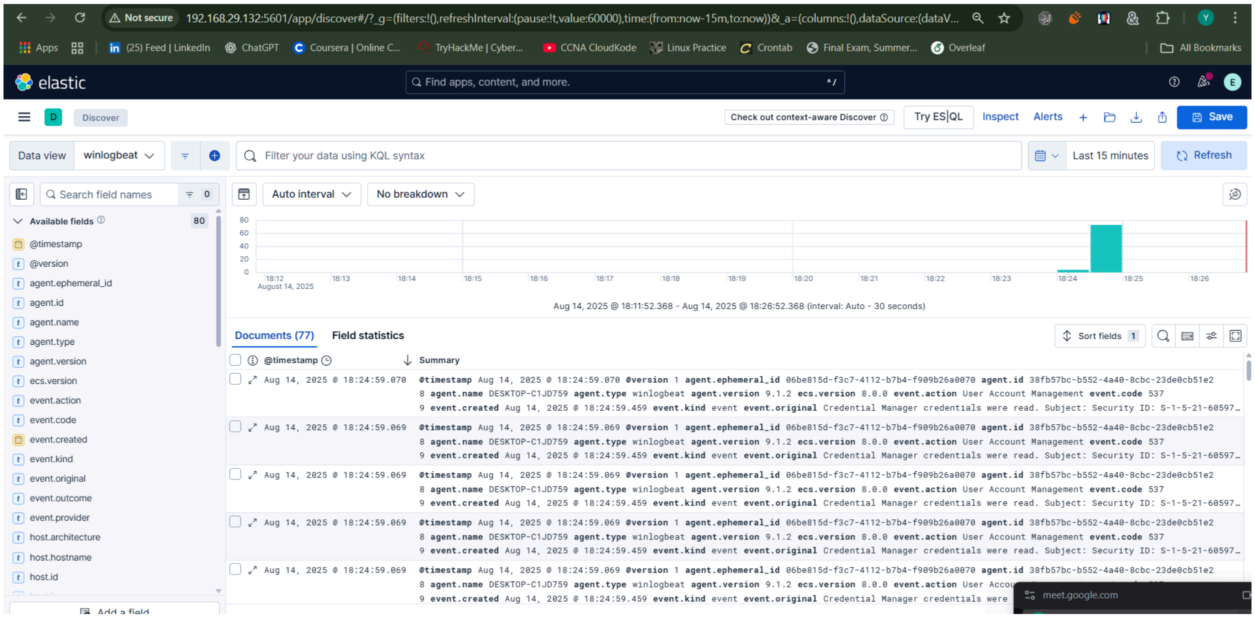
- In **Kibana** → **Stack Management → Index Management (should appear).** → To access the logs **Discover Index**



Index Management

Update your Elasticsearch indices individually or in bulk. Learn more.

Name	Health	Status	Primaries	Replicas	Documents count	Storage size	Data stream
fluent-bit-ufw	● yellow	open	1	1	6	16.1kb	
security-logs	● yellow	open	1	1	5	17.03kb	
winlogbeat-2025.08.14	● yellow	open	1	1	4	87.94kb	



```
Aug 14, 2025 @ 18:24:59.070  @timestamp Aug 14, 2025 @ 18:24:59.070 @version 1 agent.ephemeral_id 06be815d-f3c7-4112-b7b4-f909b26a0070 agent.id 38fb57bc-b552-4a40-8cbc-23de0cb51e2
                             8 agent.name DESKTOP-C1JD759 agent.type winlogbeat agent.version 9.1.2 ecs.version 8.0.0 event.action User Account Management event.code 537
                             9 event.created Aug 14, 2025 @ 18:24:59.459 event.kind event event.original Credential Manager credentials were read. Subject: Security ID: S-1-5-21-60597…
Aug 14, 2025 @ 18:24:59.069  @timestamp Aug 14, 2025 @ 18:24:59.069 @version 1 agent.ephemeral_id 06be815d-f3c7-4112-b7b4-f909b26a0070 agent.id 38fb57bc-b552-4a40-8cbc-23de0cb51e2
                             8 agent.name DESKTOP-C1JD759 agent.type winlogbeat agent.version 9.1.2 ecs.version 8.0.0 event.action User Account Management event.code 537
                             9 event.created Aug 14, 2025 @ 18:24:59.459 event.kind event event.original Credential Manager credentials were read. Subject: Security ID: S-1-5-21-60597…
Aug 14, 2025 @ 18:24:59.069  @timestamp Aug 14, 2025 @ 18:24:59.069 @version 1 agent.ephemeral_id 06be815d-f3c7-4112-b7b4-f909b26a0070 agent.id 38fb57bc-b552-4a40-8cbc-23de0cb51e2
                             8 agent.name DESKTOP-C1JD759 agent.type winlogbeat agent.version 9.1.2 ecs.version 8.0.0 event.action User Account Management event.code 537
                             9 event.created Aug 14, 2025 @ 18:24:59.459 event.kind event event.original Credential Manager credentials were read. Subject: Security ID: S-1-5-21-60597…
Aug 14, 2025 @ 18:24:59.069  @timestamp Aug 14, 2025 @ 18:24:59.069 @version 1 agent.ephemeral_id 06be815d-f3c7-4112-b7b4-f909b26a0070 agent.id 38fb57bc-b552-4a40-8cbc-23de0cb51e2
                             8 agent.name DESKTOP-C1JD759 agent.type winlogbeat agent.version 9.1.2 ecs.version 8.0.0 event.action User Account Management event.code 537
                             9 event.created Aug 14, 2025 @ 18:24:59.459 event.kind event event.original Credential Manager credentials were read. Subject: Security ID: S-1-5-21-60597…
Aug 14, 2025 @ 18:24:59.069  @timestamp Aug 14, 2025 @ 18:24:59.069 @version 1 agent.ephemeral_id 06be815d-f3c7-4112-b7b4-f909b26a0070 agent.id 38fb57bc-b552-4a40-8cbc-23de0cb51e2
                             8 agent.name DESKTOP-C1JD759 agent.type winlogbeat agent.version 9.1.2 ecs.version 8.0.0 event.action User Accou
                             9 event.created Aug 14, 2025 @ 18:24:59.459 event.kind event event.original Credential Manager credentials were
```

success.