

Complete Wazuh + Filebeat + Elasticsearch OSS + Kibana OSS Setup with Cisco Switch Log Collection

This document outlines a **step-by-step guide** to set up Wazuh (with Filebeat), Elasticsearch OSS, and Kibana OSS to collect and analyze logs from network devices like **Cisco Catalyst 1000**. It includes all successful commands, their outputs, and detailed descriptions.

Why This Stack? (Theory & Purpose) Wazuh

Wazuh is a **Security Information and Event Management (SIEM)** solution used for:

- Log analysis and correlation
- Threat detection
- Compliance monitoring (e.g., PCI-DSS, GDPR)

It reads logs from various sources and matches them against detection rules to generate alerts.

Filebeat

Filebeat is a lightweight log shipper:

- Sends Wazuh alerts or other logs to Elasticsearch
- Acts as a forwarder so Wazuh doesn't directly write into Elasticsearch

Elasticsearch OSS

Elasticsearch is a **distributed search and analytics engine**:

- Stores and indexes logs from Wazuh via Filebeat
- Provides real-time querying capabilities

Kibana OSS

Kibana is a web-based visualization tool:

- Connects to Elasticsearch
- Displays dashboards, search results, and log alerts interactively

Why rsyslog?

rsyslog is used to collect syslog data (e.g., from Cisco switches) and write it to a file Wazuh can read.

Flow Summary

Cisco Switch → rsyslog → /var/log/cisco_switch.log → Wazuh → Filebeat → Elasticsearch → Kibana

Install Elasticsearch OSS 7.10.2

Elasticsearch is the core data store used by Wazuh and visualized via Kibana.

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-oss-  
7.10.2-amd64.deb  
sudo dpkg -i elasticsearch-oss-7.10.2-amd64.deb  
sudo systemctl daemon-reexec  
sudo systemctl enable elasticsearch --now
```

Verify Elasticsearch is Running

curl -XGET

```
'http://localhost:9200/?pretty'
```

Expected output:

```
{  
  "name" : "sundar-  
VMware7-1",  
  "cluster_name" :  
  "elasticsearch", "version"  
  : {  
    "number" : "7.10.2",  
    ...  
  },  
  "tagline" : "You Know, for Search"  
}
```

```
root@sundar-VMware7-1:~# curl -XGET 'http://localhost:9200/?pretty'
{
  "name" : "sundar-VMware7-1",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "srrBDCEaQvS8XLuWYxSbIw",
  "version" : {
    "number" : "7.17.28",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "139cb5a961d8de68b8e02c45cc47f5289a3623af",
    "build_date" : "2025-02-20T09:05:31.349013687Z",
    "build_snapshot" : false,
    "lucene_version" : "8.11.3",
    "minimum_wire_compatibility_version" : "6.8.0",
    "minimum_index_compatibility_version" : "6.0.0-beta1"
  },
  "tagline" : "You Know, for Search"
}
root@sundar-VMware7-1:~#
```

Install Kibana OSS 7.10.2

Kibana is the frontend interface to visualize alerts and logs.

```
wget https://artifacts.elastic.co/downloads/kibana/kibana-oss-
```

```
7.10.2-amd64.deb sudo dpkg -i kibana-oss-7.10.2-amd64.deb
```

Configure Kibana to Connect to Elasticsearch

```
sudo nano
```

```
/etc/kibana/kibana.yml
```

Add the following:

```
server.host: "0.0.0.0"
```

```
elasticsearch.hosts: ["http://localhost:9200"]
```

```
GNU nano 7.2                               Jun 5 14:28
root@sundar-VMware7-1:~                  /etc/kibana/kibana.yml
# Kibana is served by a back end server. This setting specifies the port to use.
#server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "0.0.0.0"

# Enables you to specify a path to mount Kibana at if you are running behind a proxy.
# Use the 'server.rewriteBasePath' setting to tell Kibana if it should remove the basePath
# from requests it receives, and to prevent a deprecation warning at startup.
# This setting cannot end in a slash.
#serverbasePath: ""

# Specifies whether Kibana should rewrite requests that are prefixed with
# 'server.basePath' or require that they are rewritten by your reverse proxy.
# This setting was effectively always 'false' before Kibana 6.3 and will
# default to 'true' starting in Kibana 7.0.
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# 'server.basePath' is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
[ Read 115 lines ]
^C Help      ^O Write Out   ^W Where Is   ^K Cut        ^T Execute    ^C Location   M-U Undo    M-A Set Mark
^X Exit     ^R Read File   ^\ Replace    ^U Paste     ^J Justify    ^I Go To Line M-E Redo    M-G Copy
```

Start Kibana:

```
sudo systemctl enable kibana --now
```

You can access the Kibana web interface at <http://<your-ip>:5601>.

Install Wazuh Manager

Wazuh analyzes and correlates logs for security and

compliance monitoring.

```
curl -sO
```

```
https://packages.wazuh.com/4.7/wazuh-manager-4.7.3.deb
```

```
sudo dpkg -i wazuh-manager-4.7.3.deb
```

```
sudo systemctl enable wazuh-manager --now
```

Configure Wazuh to Parse Cisco Logs

Wazuh needs to know where to read logs from:

```
sudo nano /var/ossec/etc/ossec.conf
```



```
<ossec_config>
<global>
  <jsonout_output>yes</jsonout_output>
  <alerts_log>yes</alerts_log>
  <logall>no</logall>
  <logall_json>no</logall_json>
  <email_notification>no</email_notification>
  <update_check>yes</update_check>
  <agents_disconnection_time>10m</agents_disconnection_time>
  <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  <white_list>127.0.0.1</white_list>
  <white_list>^localhost.localdomain$</white_list>
  <white_list>127.0.0.53</white_list>
</global>

<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>12</email_alert_level>
  <scan_on_start>yes</scan_on_start>

</alerts>

<logging>
  <log_format>plain</log_format>
</logging>

<remote>
  <connection>secure</connection>
  <port>1514</port>
```

```
<protocol>tcp</protocol>
<queue_size>131072</queue_size>
</remote>

<rootcheck>
  <disabled>no</disabled>
  <check_files>yes</check_files>
  <check_trojans>yes</check_trojans>
  <check_dev>yes</check_dev>
  <check_sys>yes</check_sys>
  <check_pids>yes</check_pids>
  <check_ports>yes</check_ports>
  <check_if>yes</check_if>
  <frequency>43200</frequency>
  <rootkit_files>etc/rootcheck/rootkit_files.txt</rootkit_files>
  <rootkit_trojans>etc/rootcheck/rootkit_trojans.txt</rootkit_trojans>
  <skip_nfs>yes</skip_nfs>
  <ignore>/var/lib/containerd</ignore>
  <ignore>/var/lib/docker/overlay2</ignore>
</rootcheck>

<syscheck>
  <disabled>no</disabled>
  <frequency>43200</frequency>

  <alert_new_files>yes</alert_new_files>
  <directories>/etc,/usr/bin,/usr/sbin</directories>
  <directories>/bin,/sbin,/boot</directories>
  <ignore>/etc/mtab</ignore>
  <ignore>/etc/hosts.deny</ignore>
```

```
<ignore>/etc/mail/statistics</ignore>
<ignore>/etc/random-seed</ignore>
<ignore>/etc/random.seed</ignore>
<ignore>/etc/adjtime</ignore>
<ignore>/etc/httpd/logs</ignore>
<ignore>/etc/utmpx</ignore>
<ignore>/etc/wtmpx</ignore>
<ignore>/etc/cups/certs</ignore>
<ignore>/etc/dumpdates</ignore>
<ignore>/etc/svc/volatile</ignore>
<ignore type="sregex">.log$|.swp$</ignore>
<nodiff>/etc/ssl/private.key</nodiff>
<skip_nfs>yes</skip_nfs>
<skip_dev>yes</skip_dev>
<skip_proc>yes</skip_proc>
<skip_sys>yes</skip_sys>
<process_priority>10</process_priority>
<max_eps>50</max_eps>
<synchronization>
  <enabled>yes</enabled>
  <interval>5m</interval>
  <max_eps>10</max_eps>
</synchronization>
</syscheck>
<wodle name="syscollector">
  <disabled>no</disabled>
  <interval>1h</interval>
  <scan_on_start>yes</scan_on_start>
  <hardware>yes</hardware>
  <os>yes</os>
  <network>yes</network>
```

```
<packages>yes</packages>
<ports all="no">yes</ports>
<processes>yes</processes>
<synchronization>
  <max_eps>10</max_eps>
</synchronization>
</wodle>
```

```
<sca>
  <enabled>yes</enabled>
  <scan_on_start>yes</scan_on_start>
  <interval>12h</interval>
  <skip_nfs>yes</skip_nfs>
</sca>
```

```
<vulnerability-detection>
  <enabled>yes</enabled>
  <index-status>yes</index-status>
  <feed-update-interval>60m</feed-update-interval>
</vulnerability-detection>
```

```
<localfile>
  <log_format>command</log_format>
  <command>df -P</command>
  <frequency>360</frequency>
</localfile>
```

```
<localfile>
  <log_format>full_command</log_format>
```

```
<command>last -n 20</command>
<frequency>360</frequency>
</localfile>

<localfile>
<log_format>syslog</log_format>
<location>/var/log/syslog</location>
</localfile>

<localfile>
<log_format>syslog</log_format>
<location>/var/ossec/logs/active-responses.log</location>
</localfile>

<localfile>
<log_format>syslog</log_format>
<location>/var/log/dpkg.log</location>
</localfile>

<ruleset>
<decoder_dir>ruleset/decoders</decoder_dir>
<rule_dir>ruleset/rules</rule_dir>
<rule_exclude>0215-policy_rules.xml</rule_exclude>
<list>etc/lists/audit-keys</list>
<list>etc/lists/amazon/aws-eventnames</list>
<list>etc/lists/security-eventchannel</list>
```

```
<decoder_dir>etc/decoders</decoder_dir>
<rule_dir>etc/rules</rule_dir>
</ruleset>

<rule_test>
  <enabled>yes</enabled>
  <threads>1</threads>
  <max_sessions>64</max_sessions>
  <session_timeout>15m</session_timeout>
</rule_test>

<auth>
  <disabled>no</disabled>
  <port>1515</port>
  <use_source_ip>no</use_source_ip>
  <purge>yes</purge>
  <use_password>no</use_password>
  <ciphers>HIGH:!ADH:!EXP:!MD5:!RC4:!3DES:!CAMELLIA:@STRENGTH
H</ciphers>
  <ssl_verify_host>no</ssl_verify_host>
  <ssl_manager_cert>etc/sslmanager.cert</ssl_manager_cert>
  <ssl_manager_key>etc/sslmanager.key</ssl_manager_key>
  <ssl_auto_negotiate>no</ssl_auto_negotiate>
</auth>

<cluster>
  <name>wazuh</name>
  <node_name>node01</node_name>
  <node_type>master</node_type>
  <key></key>
```

```
<port>1516</port>
<bind_addr>0.0.0.0</bind_addr>

<nodes>
  <node>NODE_IP</node>
</nodes>
<hidden>no</hidden>
<disabled>yes</disabled>
</cluster>
```

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/auth.log</location>
</localfile>
```

```
<remote>
  <connection>syslog</connection>
  <protocol>udp</protocol>
  <port>514</port>
</remote>
```

```
</ossec_config>
```



Inside `<ossec_config>`, add:

```
<localfile>
  <log_format>syslog</log_format>
```

```
<location>/var/log/cisco_switch.log</location>
</localfile>
```

Restart

Wazuh:

```
sudo systemctl restart wazuh-manager
```

This tells Wazuh to read Cisco logs written to /var/log/cisco_switch.log.

Enable rsyslog to Accept Cisco Syslog Messages

Make sure rsyslog is configured to receive logs over

UDP port 514: sudo nano /etc/rsyslog.conf

Uncomment:

```
module(load="imudp")
input(type="imudp" port="514")
```

```
GNU nano 7.2 /etc/rsyslog.conf configuration file for rsyslog
#
# For more information install rsyslog-doc and see
# /usr/share/doc/rsyslog-doc/html/configuration/index.html
#
# Default logging rules can be found in /etc/rsyslog.d/50-default.conf

#####
#### MODULES #####
#####

module(load="imuxsock") # provides support for local system logging
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")
input(type="imudp" port="514")

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

# provides kernel logging support and enable non-kernel klog messages
module(load="imklog" permitnonkernelfacility="on")

#####
## GLOBAL DIRECTIVES ##

[ Read 53 lines ]
```

File menu: Help, Exit, Read File, Replace, Cut, Paste, Execute, Justify, Location, Go To Line, Undo, Redo, Set Mark, Copy.

Create rsyslog Rule for

Cisco Logs sudo nano

/etc/rsyslog.d/cisco.conf Add:

if (\$fromhost-ip == '192.168.1.30') then

/var/log/cisco_switch.log & stop

Restart rsyslog:

sudo systemctl restart rsyslog

This routes incoming logs from Cisco switch (IP 192.168.1.30) to a dedicated file.

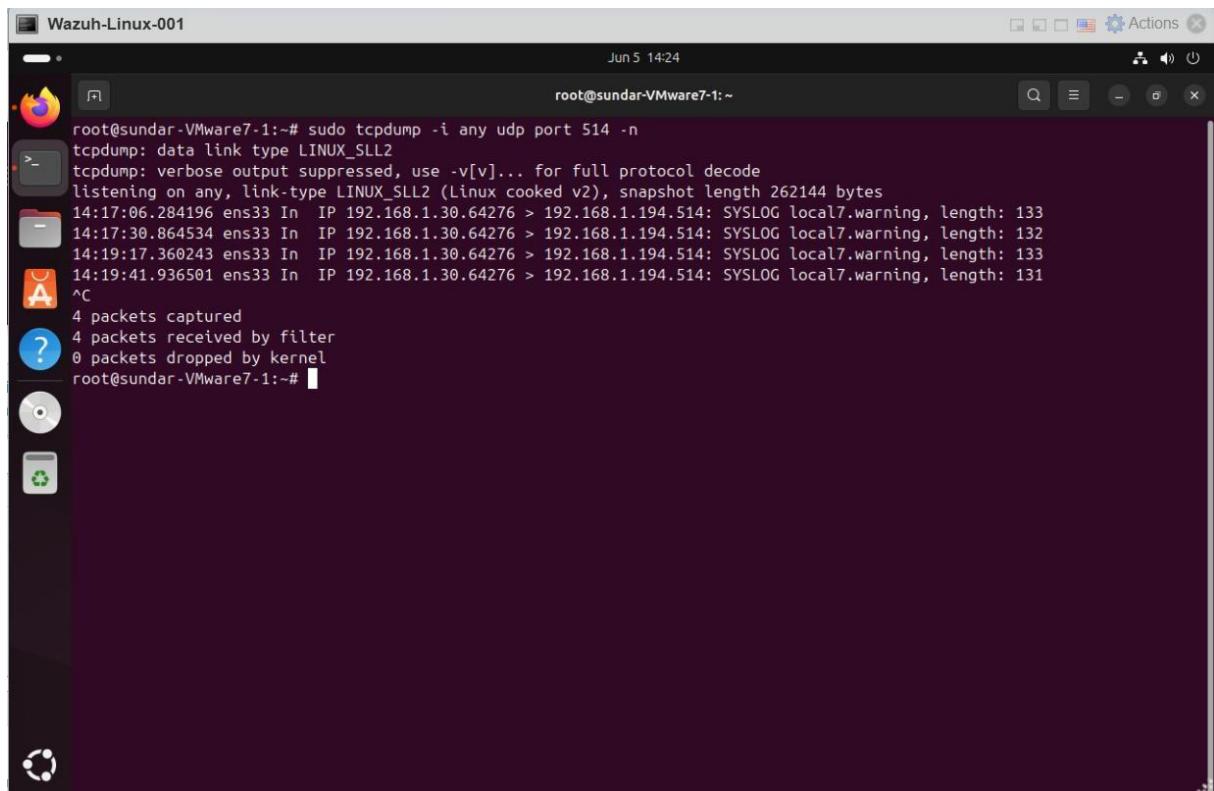
Verify Logs from Cisco Switch

Monitor incoming packets:

```
sudo tcpdump -i any udp port 514
```

-n Example:

```
IP 192.168.1.30.65398 > 192.168.1.194.514: SYSLOG local7.warning
```



```
root@sundar-VMware7-1:~# sudo tcpdump -i any udp port 514 -n
tcpdump: data link type LINUX_SLL2
tcpdump: verbose output suppressed, use -v[v]... for full protocol decode
listening on any, link-type LINUX_SLL2 (Linux cooked v2), snapshot length 262144 bytes
14:17:06.284196 ens33 In  IP 192.168.1.30.64276 > 192.168.1.194.514: SYSLOG local7.warning, length: 133
14:17:30.864534 ens33 In  IP 192.168.1.30.64276 > 192.168.1.194.514: SYSLOG local7.warning, length: 132
14:19:17.360243 ens33 In  IP 192.168.1.30.64276 > 192.168.1.194.514: SYSLOG local7.warning, length: 133
14:19:41.936501 ens33 In  IP 192.168.1.30.64276 > 192.168.1.194.514: SYSLOG local7.warning, length: 131
^C
4 packets captured
4 packets received by filter
0 packets dropped by kernel
root@sundar-VMware7-1:~#
```

Check the log file:

```
sudo tail -f
```

```
/var/log/cisco_switch.log
```

Example logs:

```
%SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://...) failed
```

```
root@sundar-VMware7-1:~# sudo tail -f /var/log/cisco_switch.log
2025-06-05T14:36:47.845620+05:30 192.168.1.30 153: *Jun  5 14:39:47.616: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet1/0/23, changed state to up
2025-06-05T14:36:47.845820+05:30 192.168.1.30 154: *Jun  5 14:39:47.686: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up
2025-06-05T14:36:47.846177+05:30 192.168.1.30 155: *Jun  5 14:39:53.911: %SYS-6-LOGGINGHOST_STARTSTOP: Logging to host 1 92.168.1.194 port 514 started - reconnection
2025-06-05T14:38:45.338411+05:30 192.168.1.30 156: *Jun  5 14:41:51.399: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/network-config) failed
2025-06-05T14:39:09.914497+05:30 192.168.1.30 157: *Jun  5 14:42:15.974: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/cisconet.cfg) failed
2025-06-05T14:40:56.512188+05:30 192.168.1.30 158: *Jun  5 14:44:02.567: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/pyramid.config) failed
2025-06-05T14:41:21.091280+05:30 192.168.1.30 159: *Jun  5 14:44:27.145: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/pyramid.cfg) failed
2025-06-05T14:49:34.454296+05:30 192.168.1.30 160: *Jun  5 14:52:40.486: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/network-config) failed
2025-06-05T14:49:59.031406+05:30 192.168.1.30 161: *Jun  5 14:53:05.062: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/cisconet.cfg) failed
2025-06-05T14:52:11.103441+05:30 192.168.1.30 163: *Jun  5 14:55:17.152: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/pyramid.cfg) failed
```

Confirm Wazuh Alerting on

Switch Logs sudo tail -f

/var/ossec/logs/alerts/alerts.log

Expected:

cisco.facility:

SYS

cisco.severity

: 4

cisco.mnemonic: CONFIG_RESOLVE_FAILURE

This confirms Wazuh is parsing and generating alerts.

```

root@sundar-VMware7-1:~# sudo tail -f /var/ossec/logs/alerts/alerts.log
cisco.facility: SYS
cisco.severity: 4
cisco.mnemonic: CONFIG_RESOLVE_FAILURE

** Alert 1749114741.65139: - pam,syslog,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Jun 05 14:42:21 sundar-VMware7-1->/var/log/auth.log
Rule: 5502 (level 3) -> 'PAM: Login session closed.'
User: root
2025-06-05T14:42:20.350877+05:30 sundar-VMware7-1 sudo: pam_unix(sudo:session): session closed for user root

** Alert 1749114745.65540: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Jun 05 14:42:25 sundar-VMware7-1->/var/log/auth.log
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: root(uid=0)
2025-06-05T14:42:23.777783+05:30 sundar-VMware7-1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by sundar(uid=0)
uid: 0

** Alert 1749114745.66002: - syslog,sudo,pci_dss_10.2.5,pci_dss_10.2.2,gpg13_7.6,gpg13_7.8,gpg13_7.13,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,nist_800_53_AC.6,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Jun 05 14:42:25 sundar-VMware7-1->/var/log/auth.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
User: root
2025-06-05T14:42:23.777012+05:30 sundar-VMware7-1 sudo:      root : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/tail -f /var/ossec/logs/alerts/alerts.log
tty: pts/1
pwd: /root
command: /usr/bin/tail -f /var/ossec/logs/alerts/alerts.log

```

Install Filebeat OSS 7.10.2 for Log Shipping

Filebeat forwards Wazuh logs to Elasticsearch.

```
curl -sO https://packages.wazuh.com/4.7/filebeat-oss-7.10.2-x86_64.deb
sudo dpkg -i filebeat-oss-7.10.2-x86_64.deb
```

Filebeat Configuration

```
sudo nano
```

```
/etc/filebeat/filebeat.yml Set
```

output and Kibana:

output.elasticsearch:

```
hosts: ["http://localhost:9200"]
```

setup.kibana:

host:

"localhost:5601"

Enable Wazuh

module:

sudo filebeat modules enable

wazuh Start Filebeat:

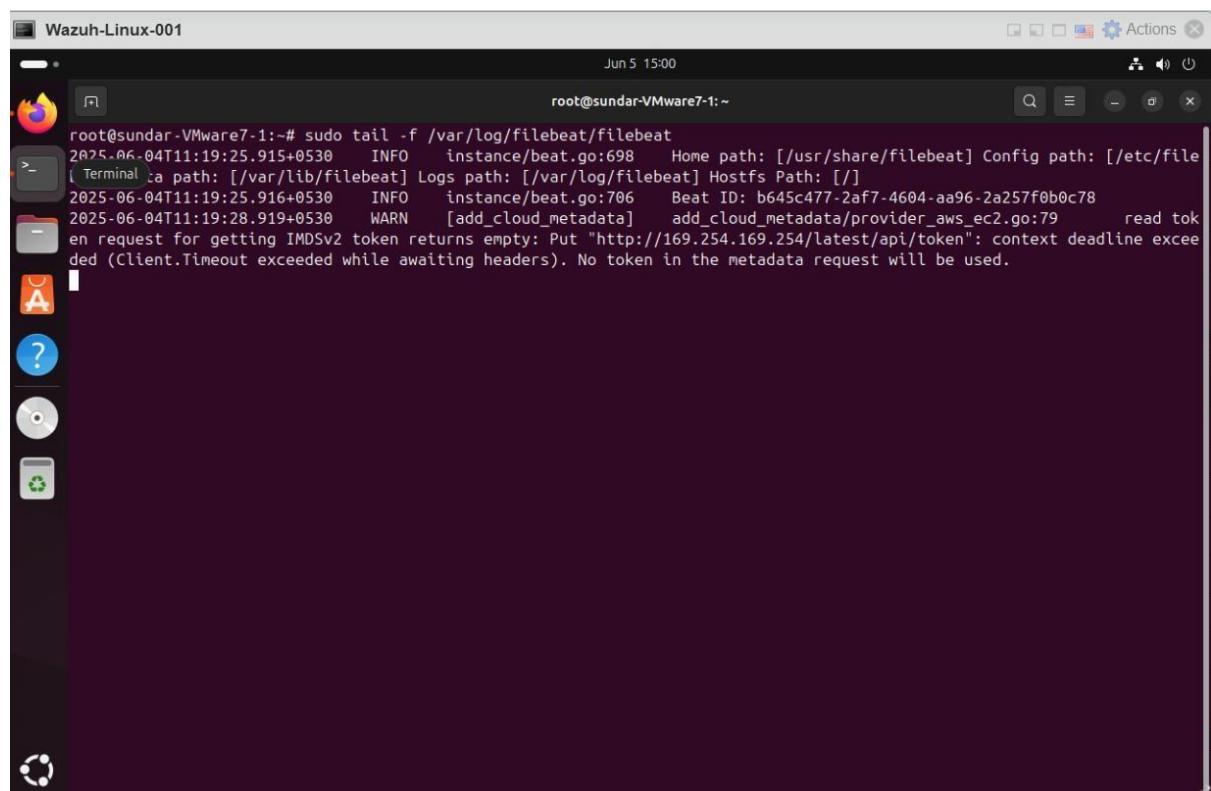
sudo systemctl enable filebeat --now

Verify the Setup

Check each component:

Filebeat logs:

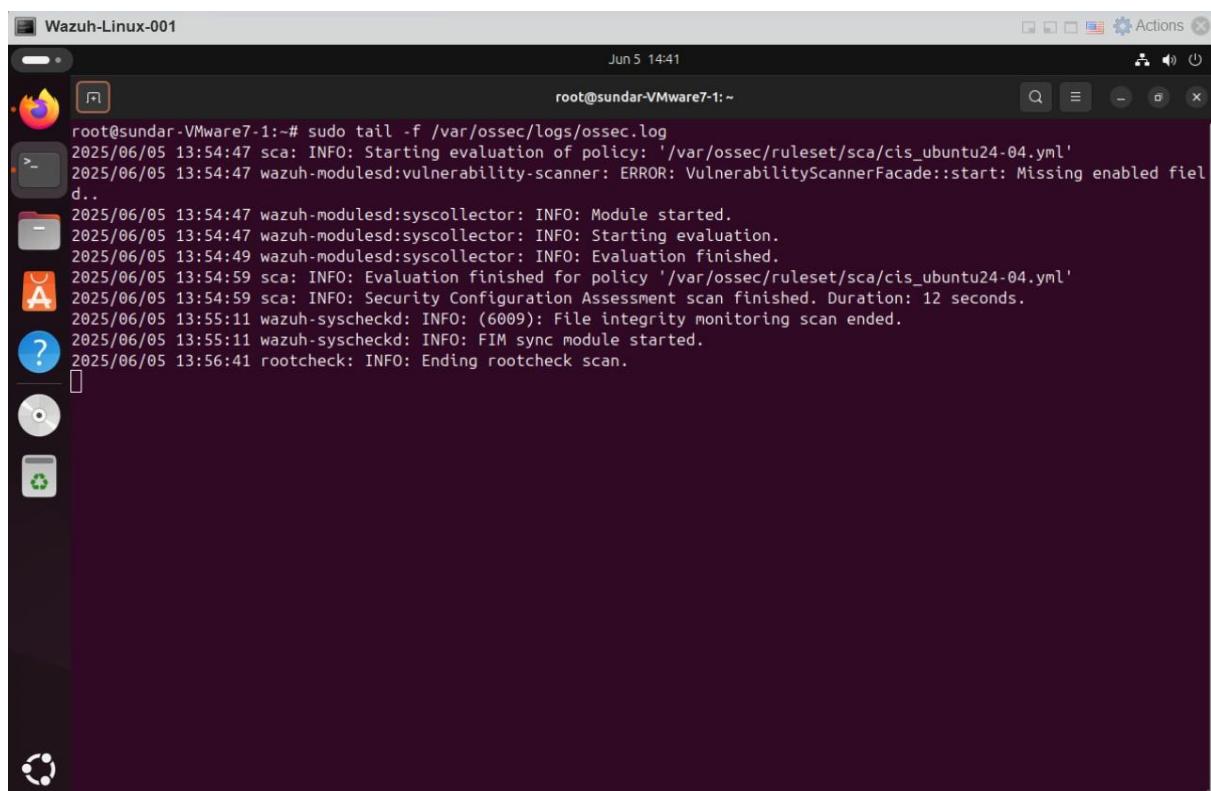
sudo tail -f /var/log/filebeat/filebeat



```
root@sundar-VMware7-1:~# sudo tail -f /var/log/filebeat/filebeat
2025-06-04T11:19:25.915+0530    INFO    instance/beat.go:698   Home path: [/usr/share/filebeat] Config path: [/etc/filebeat]
[ Terminal ]a path: [/var/lib/filebeat] Logs path: [/var/log/filebeat] Hostfs Path: []
2025-06-04T11:19:25.916+0530    INFO    instance/beat.go:706   Beat ID: b645c477-2af7-4604-aa96-2a257f0b0c78
2025-06-04T11:19:28.919+0530    WARN    [add_cloud_metadata]    add_cloud_metadata/provider_aws_ec2.go:79      read token request for getting IMDSv2 token returns empty: Put "http://169.254.169.254/latest/api/token": context deadline exceeded (Client.Timeout exceeded while awaiting headers). No token in the metadata request will be used.
```

Wazuh internal logs:

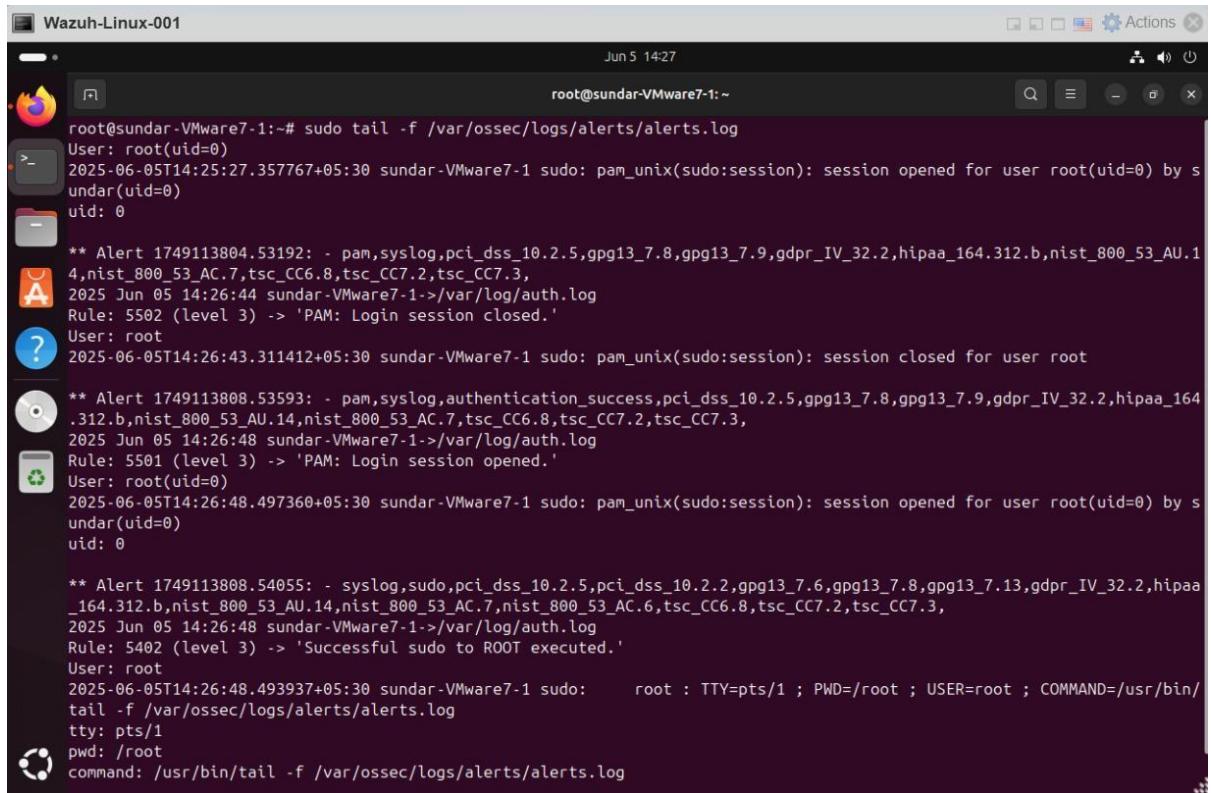
```
sudo tail -f /var/ossec/logs/ossec.log
```



```
root@sundar-VMware7-1:~# sudo tail -f /var/ossec/logs/ossec.log
2025/06/05 13:54:47 sca: INFO: Starting evaluation of policy: '/var/ossec/ruleset/sca/cis_ubuntu24-04.yml'
2025/06/05 13:54:47 wazuh-modulesd:vulnerability-scanner: ERROR: VulnerabilityScannerFacade::start: Missing enabled field...
2025/06/05 13:54:47 wazuh-modulesd:syscollector: INFO: Module started.
2025/06/05 13:54:47 wazuh-modulesd:syscollector: INFO: Starting evaluation.
2025/06/05 13:54:49 wazuh-modulesd:syscollector: INFO: Evaluation finished.
2025/06/05 13:54:59 sca: INFO: Evaluation finished for policy '/var/ossec/ruleset/sca/cis_ubuntu24-04.yml'
2025/06/05 13:54:59 sca: INFO: Security Configuration Assessment scan finished. Duration: 12 seconds.
2025/06/05 13:55:11 wazuh-syscheckd: INFO: (6009): File integrity monitoring scan ended.
2025/06/05 13:55:11 wazuh-syscheckd: INFO: FIM sync module started.
2025/06/05 13:56:41 rootcheck: INFO: Ending rootcheck scan.
```

Wazuh alerts:

```
sudo tail -f /var/ossec/logs/alerts/alerts.log
```



```
root@sundar-VMware7-1:~# sudo tail -f /var/ossec/logs/alerts/alerts.log
User: root(uid=0)
2025-06-05T14:25:27.357767+05:30 sundar-VMware7-1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by s
undar(uid=0)
uid: 0

** Alert 1749113804.53192: - pam,syslog,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_164.312.b,nist_800_53_AU.1
4,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Jun 05 14:26:44 sundar-VMware7-1->/var/log/auth.log
Rule: 5502 (level 3) -> 'PAM: Login session closed.'
User: root
2025-06-05T14:26:43.311412+05:30 sundar-VMware7-1 sudo: pam_unix(sudo:session): session closed for user root

** Alert 1749113808.53593: - pam,syslog,authentication_success,pci_dss_10.2.5,gpg13_7.8,gpg13_7.9,gdpr_IV_32.2,hipaa_
.312.b,nist_800_53_AU.14,nist_800_53_AC.7,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Jun 05 14:26:48 sundar-VMware7-1->/var/log/auth.log
Rule: 5501 (level 3) -> 'PAM: Login session opened.'
User: root(uid=0)
2025-06-05T14:26:48.497360+05:30 sundar-VMware7-1 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by s
undar(uid=0)
uid: 0

** Alert 1749113808.54055: - syslog,sudo,pci_dss_10.2.5,pci_dss_10.2.2,gpg13_7.6,gpg13_7.8,gpg13_7.13,gdpr_IV_32.2,hipaa
_164.312.b,nist_800_53_AU.14,nist_800_53_AC.7,nist_800_53_AC.6,tsc_CC6.8,tsc_CC7.2,tsc_CC7.3,
2025 Jun 05 14:26:48 sundar-VMware7-1->/var/log/auth.log
Rule: 5402 (level 3) -> 'Successful sudo to ROOT executed.'
User: root
2025-06-05T14:26:48.493937+05:30 sundar-VMware7-1 sudo:      root : TTY=pts/1 ; PWD=/root ; USER=root ; COMMAND=/usr/bin/
tail -f /var/ossec/logs/alerts/alerts.log
tty: pts/1
pwd: /root
command: /usr/bin/tail -f /var/ossec/logs/alerts/alerts.log
```

Kibana Discover:

Use Kibana to search logs:

- Navigate to **Discover** tab
- Search syslog, pam, or Cisco messages
- Create visualizations if needed

The screenshot shows the Kibana interface running in a browser window titled "Wazuh-Linux-001". The top navigation bar includes tabs for "Discover", "Dashboard", "Visualize", and "Logs". The "Discover" tab is active, showing a table of log entries. The table has two header rows: "Table" and "JSON". The "Table" row contains columns for "Field" and "Value". The "JSON" row contains the same fields. Below the table, individual log entries are listed as JSON objects. The first few entries are as follows:

Field	Value
_id	60Q-P5cB9x2k-UJpWbLw
_index	wazuh-alerts-4.x-2025.06.05#60Q-P5cB9x2k-UJpWbLw
_score	1
_type	_doc
@timestamp	Jun 5, 2025 @ 14:08:53.820
agent.id	000
agent.name	sundar-VMware7-1
data.cisco.facility	SYS
data.cisco.mnemonic	CONFIG_RESOLVE_FAILURE
data.cisco.severity	4
decoder.name	cisco-10s
full_log	2025-06-05T14:08:52.811799+05:30 192.168.1.38 139: *Jun 5 14:11:58.962: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/pyramid.cfg) failed
id	1749112733.48525

t full_log	2025-06-05T14:08:52.811799+05:30 192.168.1.30 139: *Jun 5 14:11:58.962: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tftp://255.255.255.255/pyramid.cfg) failed
t id	1749112733.48525
t input.type	log
t location	/var/log/syslog
t manager.name	sundar-VMware7-1
t predecoder.program_name	139
t predecoder.timestamp	2025-06-05T14:08:52.811799+05:30
t rule.description	Cisco IOS warning message - CONFIG_RESOLVE_FAILURE
# rule.firedtimes	4
t rule.gpg13	4.12
t rule.groups	syslog, cisco_ios
t rule.id	4714
# rule.level	3
t rule.mail	false
timestamp	Jun 5, 2025 @ 14:08:53.820

Devices Tested

- **Cisco Catalyst 1000 Series (IP: 192.168.1.30)**
- **FORTINET LOGS**

FortiGate Configuration (Syslog Forwarding)

On the FortiGate web interface:

1. Go to Log & Report → Log Settings
2. Under Syslog Servers, configure:
 - o Server: 192.168.1.194 (IP of Wazuh server)
 - o Port: 514
 - o Format: Default
 - o Facility: local7
 - o Enable log types: Traffic, Event, UTM logs, etc.

Firewall CLI

```
config log syslogd setting
  set status enable
  set server <WAZUH_IP>
  set mode udp
  set port 514
```

```
    set facility local7
end

config log syslog filter
    set severity information
    set forward-traffic enable
    set local-traffic enable
    set multicast-traffic enable
    set sniffer-traffic enable
    set anomaly enable
    set voip enable
end
```

Configure rsyslog on Wazuh Server

Edit /etc/rsyslog.conf and ensure these lines are uncommented:

bash

CopyEdit

```
module(load="imudp")
input(type="imudp" port="514")
```

Then create a new rule file:

bash

CopyEdit

```
sudo nano /etc/rsyslog.d/fortigate.conf
```

Add:

bash

CopyEdit

```
if ($fromhost-ip == '192.168.1.1') then /var/log/fortigate.log
& stop
```

Replace 192.168.1.1 with your actual FortiGate IP address.

Restart rsyslog:

bash

CopyEdit

```
sudo systemctl restart rsyslog
```

❖ Configure Wazuh to Parse FortiGate Logs

Edit /var/ossec/etc/ossec.conf and add:

xml

CopyEdit

```
<localfile>
```

```
    <log_format>syslog</log_format>
    <location>/var/log/fortigate.log</location>
</localfile>
```

Then restart Wazuh:

bash

CopyEdit

```
sudo systemctl restart wazuh-manager
```

Validate Logs & Alerts

To check if logs are being received:

bash

CopyEdit

```
sudo tail -f /var/log/fortigate.log
```

To confirm Wazuh is generating alerts:

bash

CopyEdit

```
sudo tail -f /var/ossec/logs/alerts/alerts.log
```

You should see entries like:

makefile

CopyEdit

rule.id: 81633

rule.description: Fortigate: App passed by firewall.

app: Google.Chat

action: pass

srcip: 192.168.1.58

dstip: 142.251.222.142

Kibana Integration

Open Kibana (<http://<wazuh-ip>:5601>), go to Discover, and search:

kql

CopyEdit

```
decoder.name: "fortigate-firewall-v5"
```

Create dashboards or alerts for:

- Allowed/Dropped apps (e.g., Google.Chat)
 - Blocked IPs or ports
 - App usage by department/IP
-

Example FortiGate Log Parsed

json

CopyEdit

{

 "app": "Google.Chat",

 "action": "pass",

 "srcip": "192.168.1.58",

 "dstip": "142.251.222.142",

 "proto": "17",

 "service": "HTTPS",

 "hostname": "chat.google.com",

 "decoder.name": "fortigate-firewall-v5",

 "rule.description": "Fortigate: App passed by firewall."

}

Tested Firewall Device

- FortiGate-40F
 - IP: 192.168.1.1
 - syslog facility: local7
 - Transport: UDP port 514

FortiGate-40F

Global Settings Local Logs Threat Weight

Syslog logging Enable Disable

IP address/FQDN: 192.168.1.194

Log Settings

Event logging: All

Local traffic logging: All

Syslog logging: Enable Disable

Address: 192.168.1.194

GUI Preferences

Resolve hostnames:

Resolve unknown applications:

Additional Information

API Preview

Online Guides Relevant Documentation Video Tutorials

Fortinet Community

No Traffic Logs in FortiADC

Send logs from FortiGate 40F firewall to LimaCharlie with encryption

Fortigate 40F fortiguard-log issue

See More

Security Rating Issues

Show Dismissed

Elastic

Discover

rule.groups: fortigate

Search field names

Filter by type: 0

Available fields: 72

Popular: _index, rule.groups

Time: Jun 11, 2025 @ 15:44:10.864 - Jun 11, 2025 @ 15:59:10.864

Document

5,975 hits

Jun 11, 2025 @ 15:44:10.864 - Jun 11, 2025 @ 15:59:10.864

```
rule.groups: fortigate, syslog @timestamp: Jun 11, 2025 @ 15:59:04.734 agent.id: 000
agent.name: sundar-VMware7-1 data.action: pass data.app: QUIC data.appcat: Network.Service
data.appid: 40169 data.applist: default data.apprisk: low data.devid: FGT40FTK21009350
data.devname: FortiGate-40F data.direction: outgoing data.dstcountry: United States
data.dstintf: wan data.dstintfrole: wan data.dstip: 142.251.220.3 data.dstport: 443
```

```
rule.groups: fortigate, syslog @timestamp: Jun 11, 2025 @ 15:59:04.734 agent.id: 000
agent.name: sundar-VMware7-1 data.action: pass data.app: Google.Services
```

Chart options

Search Elastic

Options New Open Share Inspect Save

Discover

rule.groups: fortigate

Search field names

Filter by type: 0

Available fields: 72

Popular: _index, rule.groups

Time: Jun 11, 2025 @ 15:44:10.864 - Jun 11, 2025 @ 15:59:10.864

Document

5,975 hits

Jun 11, 2025 @ 15:44:10.864 - Jun 11, 2025 @ 15:59:10.864

```
rule.groups: fortigate, syslog @timestamp: Jun 11, 2025 @ 15:59:02.736 agent.id: 000
agent.name: sundar-VMware7-1 data.action: pass data.app: HTTPS.BROWSER data.appcat: Web.Client
data.appid: 40568 data.applist: default data.apprisk: medium data.devid: FGT40FTK21009350
data.devname: FortiGate-40F data.direction: incoming data.dstcountry: United States
data.dstintf: wan data.dstintfrole: wan data.dstip: 13.107.246.58 data.dstport: 443
```

```
rule.groups: fortigate, syslog @timestamp: Jun 11, 2025 @ 15:59:02.734 agent.id: 000
agent.name: sundar-VMware7-1 data.action: pass data.app: SSL data.appcat: Network.Service
data.appid: 15895 data.applist: default data.apprisk: elevated data.devid: FGT40FTK21009350
data.devname: FortiGate-40F data.direction: outgoing data.dstcountry: United States
```

Chart options

Search Elastic

Options New Open Share Inspect Save

The image displays three screenshots of the Elastic Stack interface, specifically the Discover and Visualize features.

Screenshot 1: Discover - Log Details

Field	Value
_id	W6-JXpcB98yC-xmKTF5q
_index	wazuh-alerts-4.x-2025.06.11#W6-JXpcB98yC-xmKTF5q
_score	1
_type	_doc
@timestamp	Jun 11, 2025 @ 15:59:04.734
agent.id	000
agent.name	sundar-VMware7-1
data.action	pass
data.app	QUIC
data.appcat	Network.Service
data.appid	40169
data.applist	default
data.apprisk	low
data.devid	FGT40FTK21009350
data.devname	FortiGate-40F

Screenshot 2: Discover - Field Values

Field	Value
data.appcat	Network.Service
data.appid	40169
data.applist	default
data.apprisk	low
data.devid	FGT40FTK21009350
data.devname	FortiGate-40F
data.direction	outgoing
data.dstcountry	United States
data.dstintf	wan
data.dstintrole	wan
data.dstip	142.251.220.3
data.dstport	443
data.eventtime	1749637743798832379
data.eventtype	signature
data.incidentserialno	22751543
data.level	information

Screenshot 3: Visualize Library - Bar Vertical Stacked

Search: rule.groups: fortigate + Add filter

KQL: Last 15 minutes

Visualizations:

- Bar vertical stacked: wazuh-alerts-* (Top values of rule.groups)

The bar chart shows the count of records for different rule groups. The data is as follows:

rule.group	Count of records
fortigate	~5800
firewall_drop	~100
invalid_login	~10

✓ Now Your Setup Supports:

- Cisco Catalyst Switch Logging
- FortiGate Firewall Logging
- Wazuh Real-Time Alerting Centralized Visualization with Kibana.