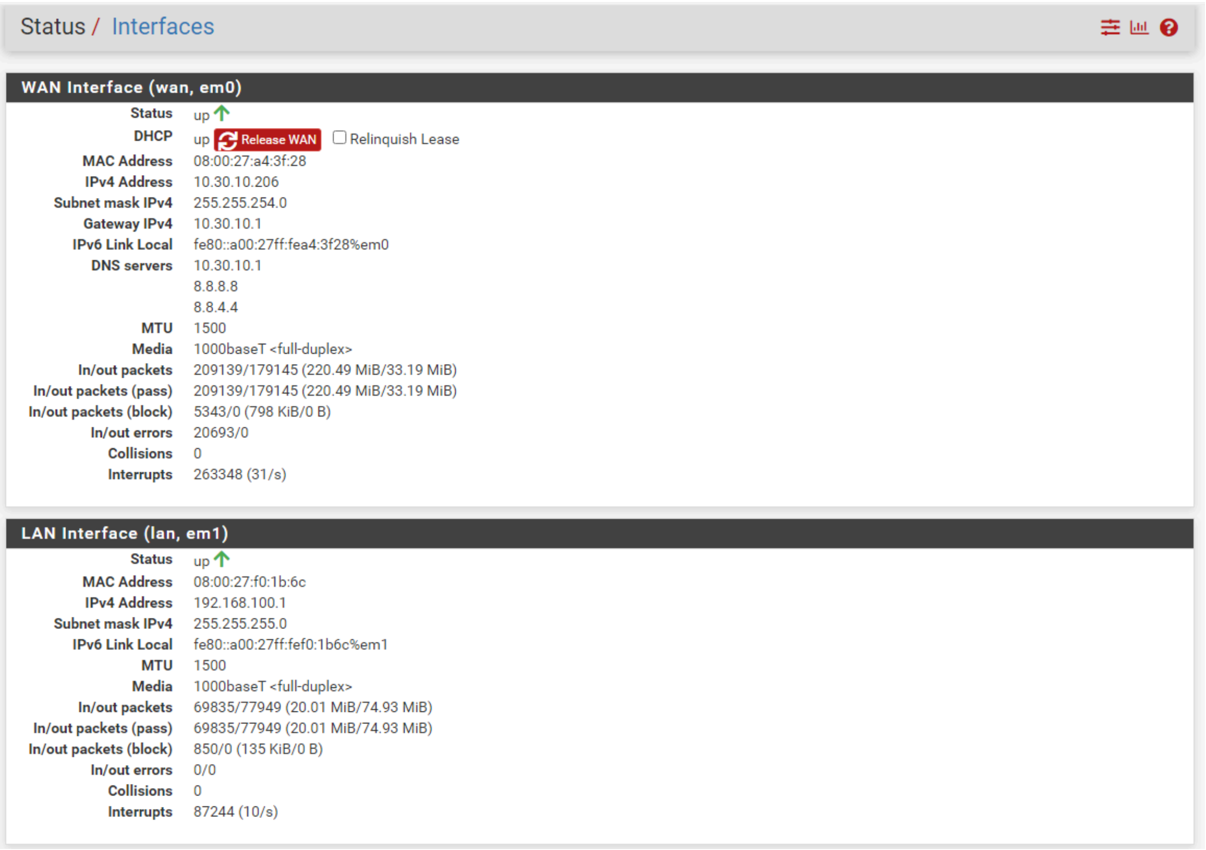
Pfsense

Configuración de la infraestructura de red



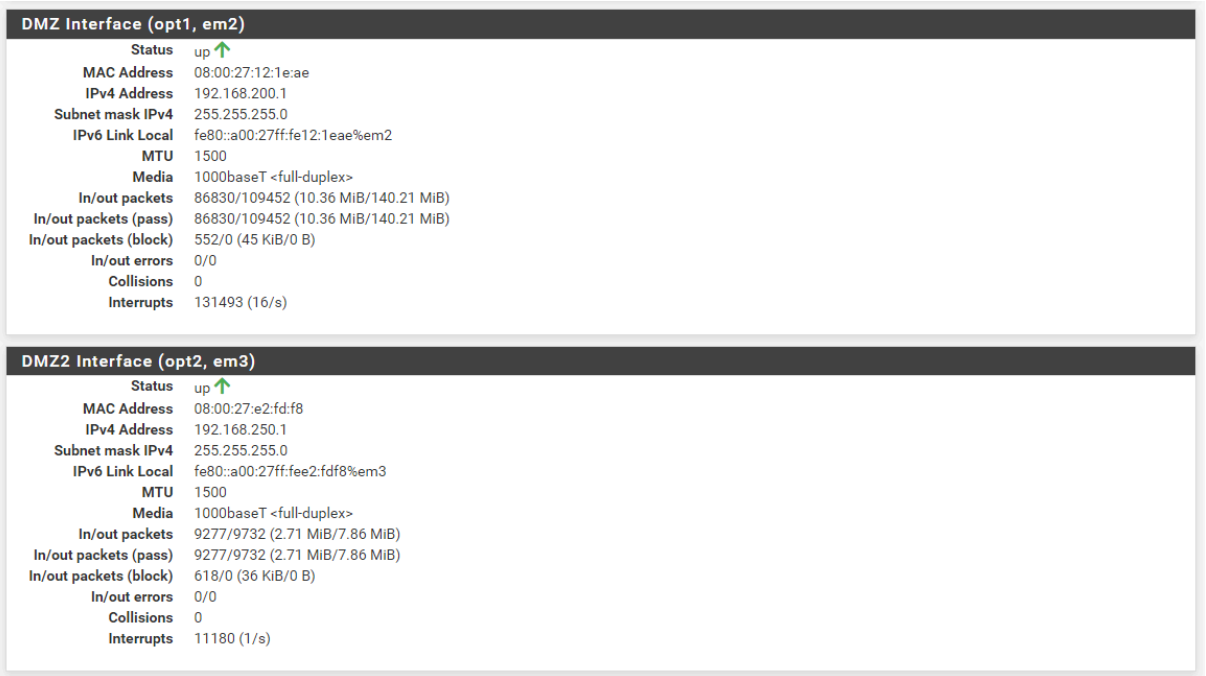
Status / Interfaces

WAN Interface (wan, em0)

Status	up ↑
DHCP	up Release WAN □ Relinquish Lease
MAC Address	08:00:27:a4:3f:28
IPv4 Address	10.30.10.206
Subnet mask IPv4	255.255.254.0
Gateway IPv4	10.30.10.1
IPv6 Link Local	fe80::a00:27ff:fea4:3f28%em0
DNS servers	10.30.10.1 8.8.8.8 8.8.4.4
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	209139/179145 (220.49 MiB/33.19 MiB)
In/out packets (pass)	209139/179145 (220.49 MiB/33.19 MiB)
In/out packets (block)	5343/0 (798 KiB/0 B)
In/out errors	20693/0
Collisions	0
Interrupts	263348 (31/s)

LAN Interface (lan, em1)

Status	up ↑
MAC Address	08:00:27:f0:1b:6c
IPv4 Address	192.168.100.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fef0:1b6c%em1
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	69835/77949 (20.01 MiB/74.93 MiB)
In/out packets (pass)	69835/77949 (20.01 MiB/74.93 MiB)
In/out packets (block)	850/0 (135 KiB/0 B)
In/out errors	0/0
Collisions	0
Interrupts	87244 (10/s)



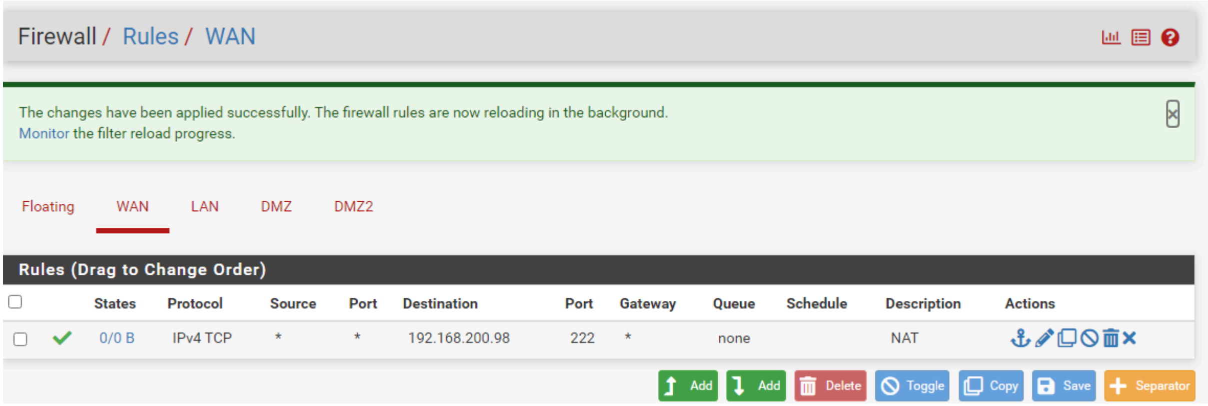
DMZ Interface (opt1, em2)

Status	up ↑
MAC Address	08:00:27:12:1e:ae
IPv4 Address	192.168.200.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fe12:1eae%em2
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	86830/109452 (10.36 MiB/140.21 MiB)
In/out packets (pass)	86830/109452 (10.36 MiB/140.21 MiB)
In/out packets (block)	552/0 (45 KiB/0 B)
In/out errors	0/0
Collisions	0
Interrupts	131493 (16/s)

DMZ2 Interface (opt2, em3)

Status	up ↑
MAC Address	08:00:27:e2:fd:f8
IPv4 Address	192.168.250.1
Subnet mask IPv4	255.255.255.0
IPv6 Link Local	fe80::a00:27ff:fee2:fdf8%em3
MTU	1500
Media	1000baseT <full-duplex>
In/out packets	9277/9732 (2.71 MiB/7.86 MiB)
In/out packets (pass)	9277/9732 (2.71 MiB/7.86 MiB)
In/out packets (block)	618/0 (36 KiB/0 B)
In/out errors	0/0
Collisions	0
Interrupts	11180 (1/s)

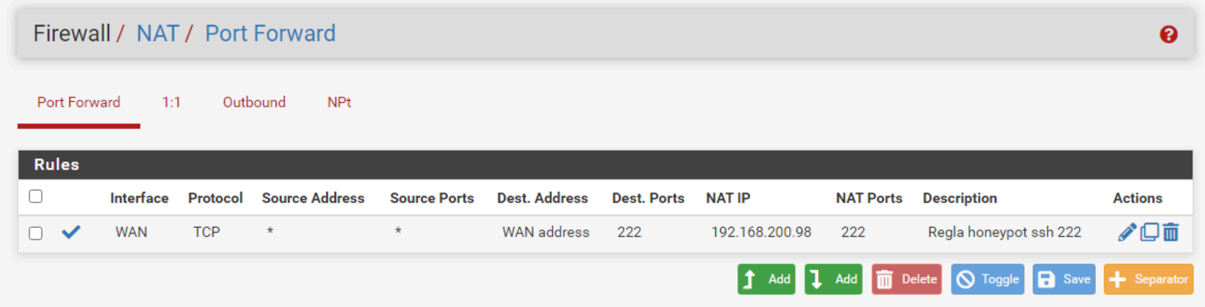
Reglas Honeypot



The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

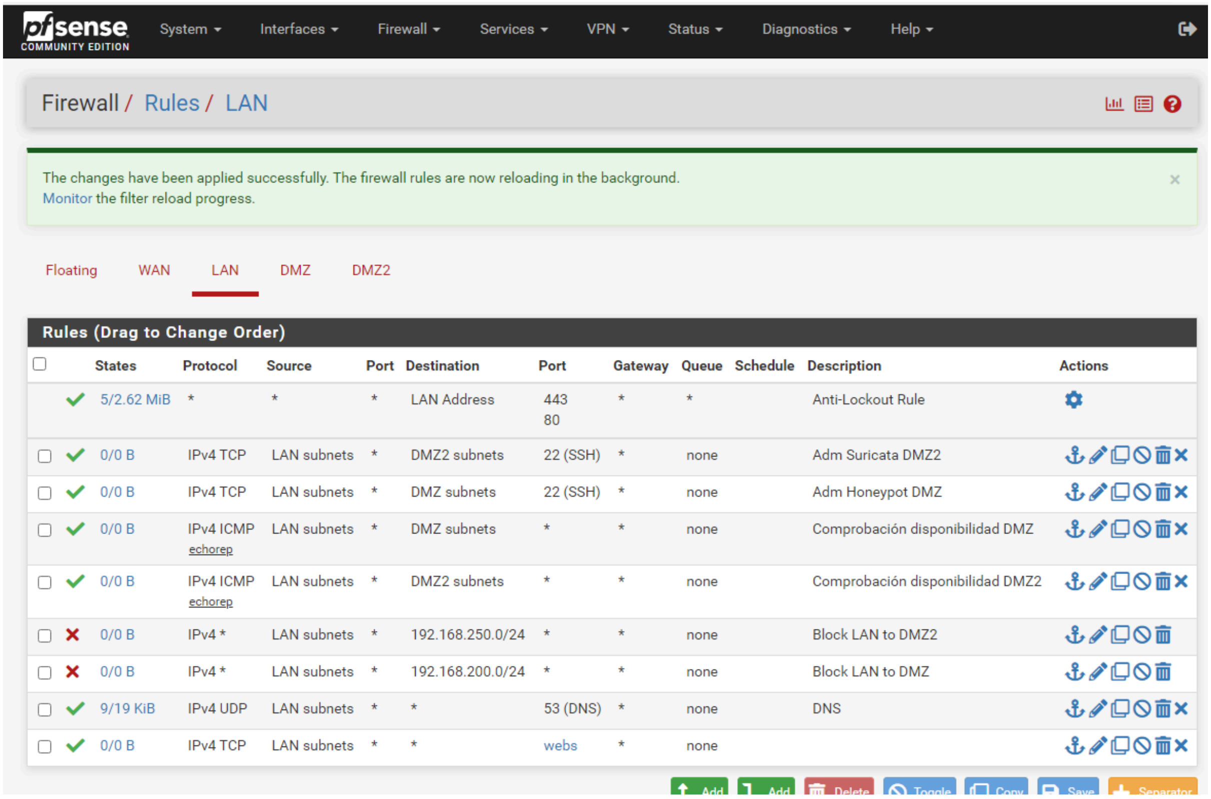
□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✓	0/0 B	IPv4 TCP	*	*	192.168.200.98	222	*	none		NAT	



Rules

□		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
□	✓	WAN	TCP	*	*	WAN address	222	192.168.200.98	222	Regla honeypot ssh 222	

LAN

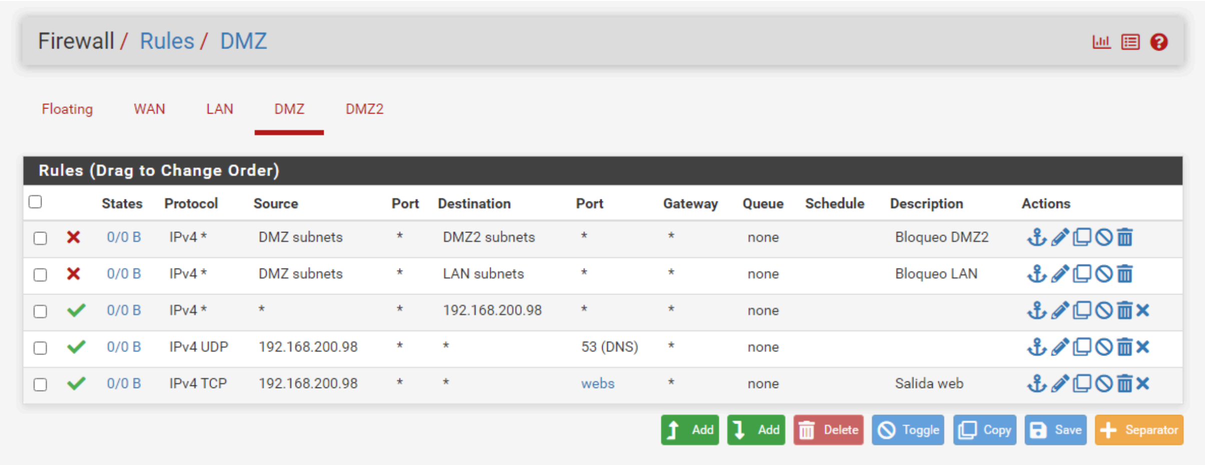


The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
	✓	5/2.62 MiB	*	*	*	LAN Address	443 80	*	*		Anti-Lockout Rule	
□	✓	0/0 B	IPv4 TCP	LAN subnets	*	DMZ2 subnets	22 (SSH)	*	none		Adm Suricata DMZ2	
□	✓	0/0 B	IPv4 TCP	LAN subnets	*	DMZ subnets	22 (SSH)	*	none		Adm Honeypot DMZ	
□	✓	0/0 B	IPv4 ICMP echorep	LAN subnets	*	DMZ subnets	*	*	none		Comprobación disponibilidad DMZ	
□	✓	0/0 B	IPv4 ICMP echorep	LAN subnets	*	DMZ2 subnets	*	*	none		Comprobación disponibilidad DMZ2	
□	✗	0/0 B	IPv4 *	LAN subnets	*	192.168.250.0/24	*	*	none		Block LAN to DMZ2	
□	✗	0/0 B	IPv4 *	LAN subnets	*	192.168.200.0/24	*	*	none		Block LAN to DMZ	
□	✓	9/19 KiB	IPv4 UDP	LAN subnets	*	*	53 (DNS)	*	none		DNS	
□	✓	0/0 B	IPv4 TCP	LAN subnets	*	*	webs	*	none			

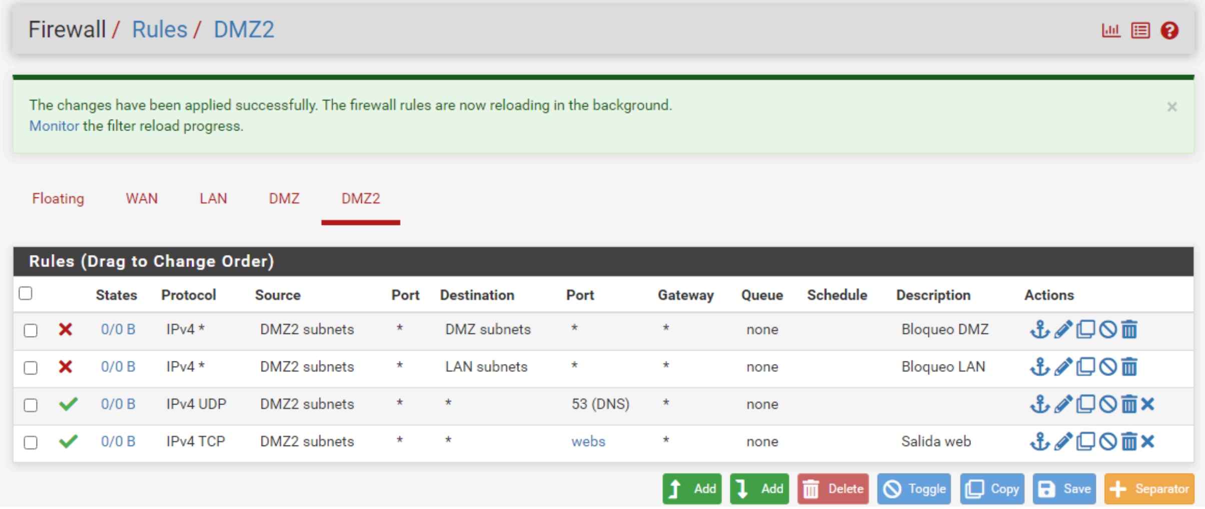
DMZ



Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0/0 B	IPv4 *	DMZ subnets	*	DMZ2 subnets	*	*	none		Bloqueo DMZ2	
□	✗	0/0 B	IPv4 *	DMZ subnets	*	LAN subnets	*	*	none		Bloqueo LAN	
□	✓	0/0 B	IPv4 *	*	*	192.168.200.98	*	*	none			
□	✓	0/0 B	IPv4 UDP	192.168.200.98	*	*	53 (DNS)	*	none			
□	✓	0/0 B	IPv4 TCP	192.168.200.98	*	*	webs	*	none		Salida web	

DMZ2



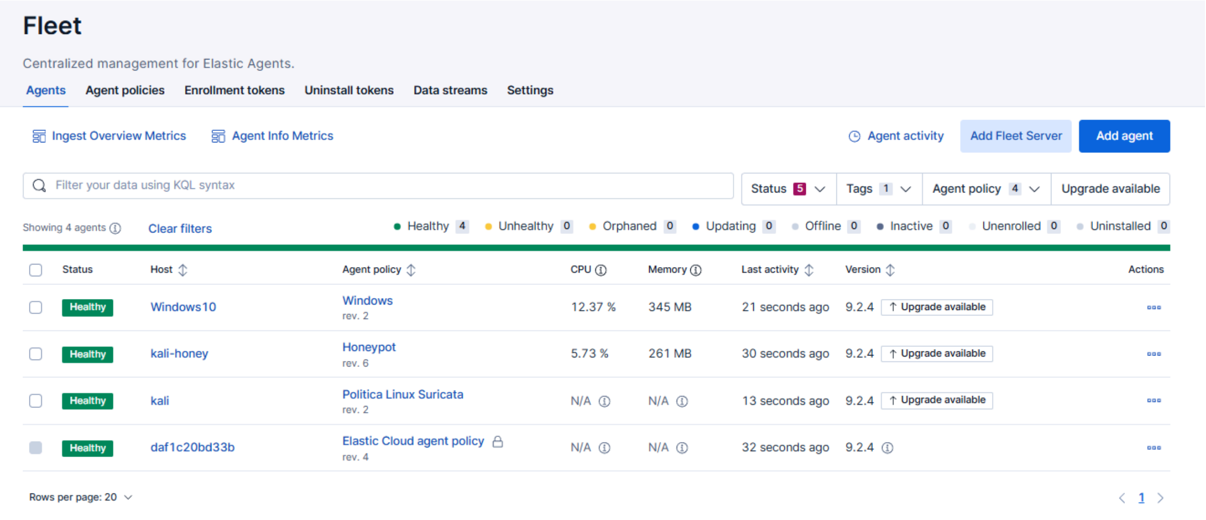
The changes have been applied successfully. The firewall rules are now reloading in the background.
Monitor the filter reload progress.

Rules (Drag to Change Order)

□		States	Protocol	Source	Port	Destination	Port	Gateway	Queue	Schedule	Description	Actions
□	✗	0/0 B	IPv4 *	DMZ2 subnets	*	DMZ subnets	*	*	none		Bloqueo DMZ	
□	✗	0/0 B	IPv4 *	DMZ2 subnets	*	LAN subnets	*	*	none		Bloqueo LAN	
□	✓	0/0 B	IPv4 UDP	DMZ2 subnets	*	*	53 (DNS)	*	none			
□	✓	0/0 B	IPv4 TCP	DMZ2 subnets	*	*	webs	*	none		Salida web	

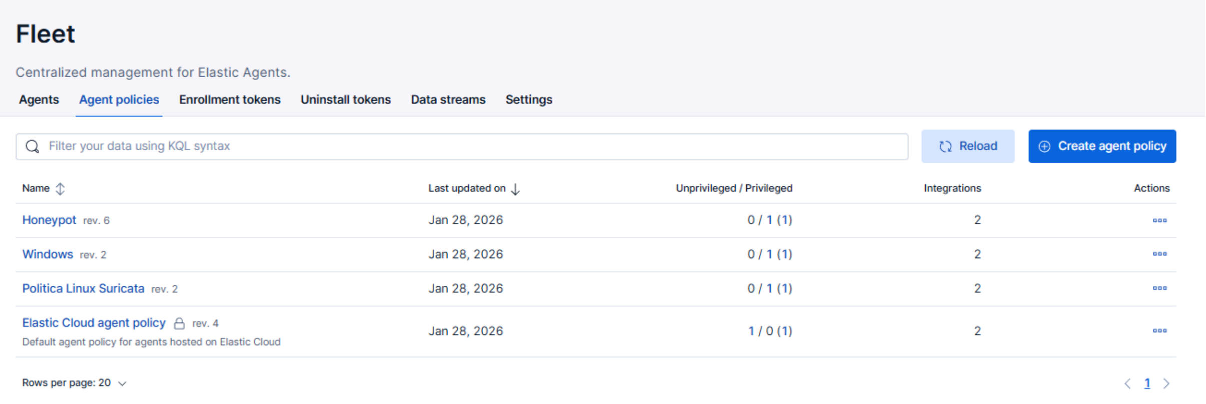
Elastic

Agents

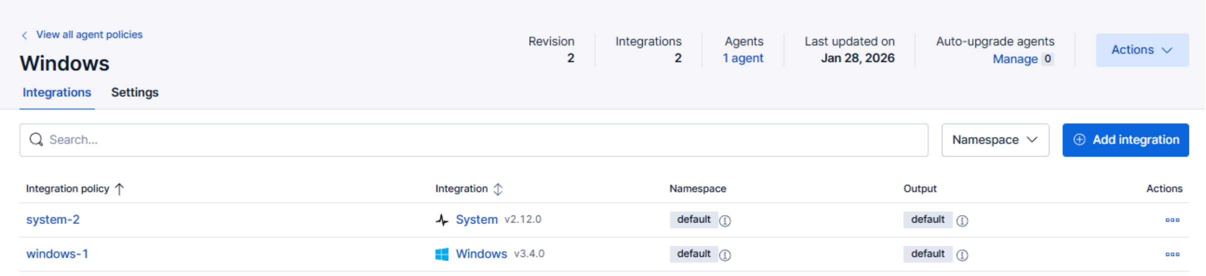


	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
□	Healthy	Windows10	Windows rev. 2	12.37 %	345 MB	21 seconds ago	9.2.4 ↑ Upgrade available	•••
□	Healthy	kali-honey	Honeypot rev. 6	5.73 %	261 MB	30 seconds ago	9.2.4 ↑ Upgrade available	•••
□	Healthy	kali	Politica Linux Suricata rev. 2	N/A	N/A	13 seconds ago	9.2.4 ↑ Upgrade available	•••
□	Healthy	daf1c20bd33b	Elastic Cloud agent policy rev. 4	N/A	N/A	32 seconds ago	9.2.4	•••

Políticas

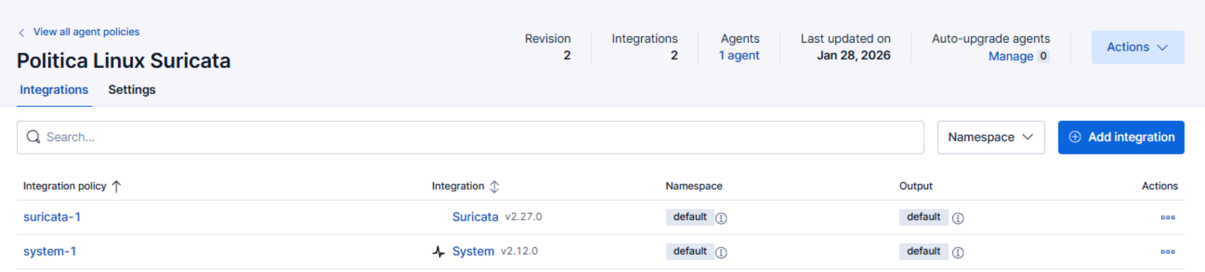


Name	Last updated on	Unprivileged / Privileged	Integrations	Actions
Honeypot rev. 6	Jan 28, 2026	0 / 1 (1)	2	•••
Windows rev. 2	Jan 28, 2026	0 / 1 (1)	2	•••
Politica Linux Suricata rev. 2	Jan 28, 2026	0 / 1 (1)	2	•••
Elastic Cloud agent policy rev. 4 Default agent policy for agents hosted on Elastic Cloud	Jan 28, 2026	1 / 0 (1)	2	•••



Revision 2 | Integrations 2 | Agents 1 agent | Last updated on Jan 28, 2026 | Auto-upgrade agents Manage 0

Integration policy	Integration	Namespace	Output	Actions
system-2	System v2.12.0	default	default	•••
windows-1	Windows v3.4.0	default	default	•••



< View all agent policies

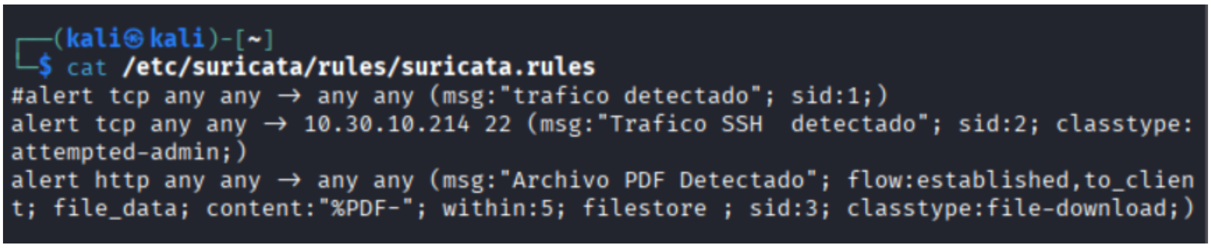
Politica Linux Suricata

Revision 2 · Integrations 2 · Agents 1 agent · Last updated on Jan 28, 2026 · Auto-upgrade agents Manage 0

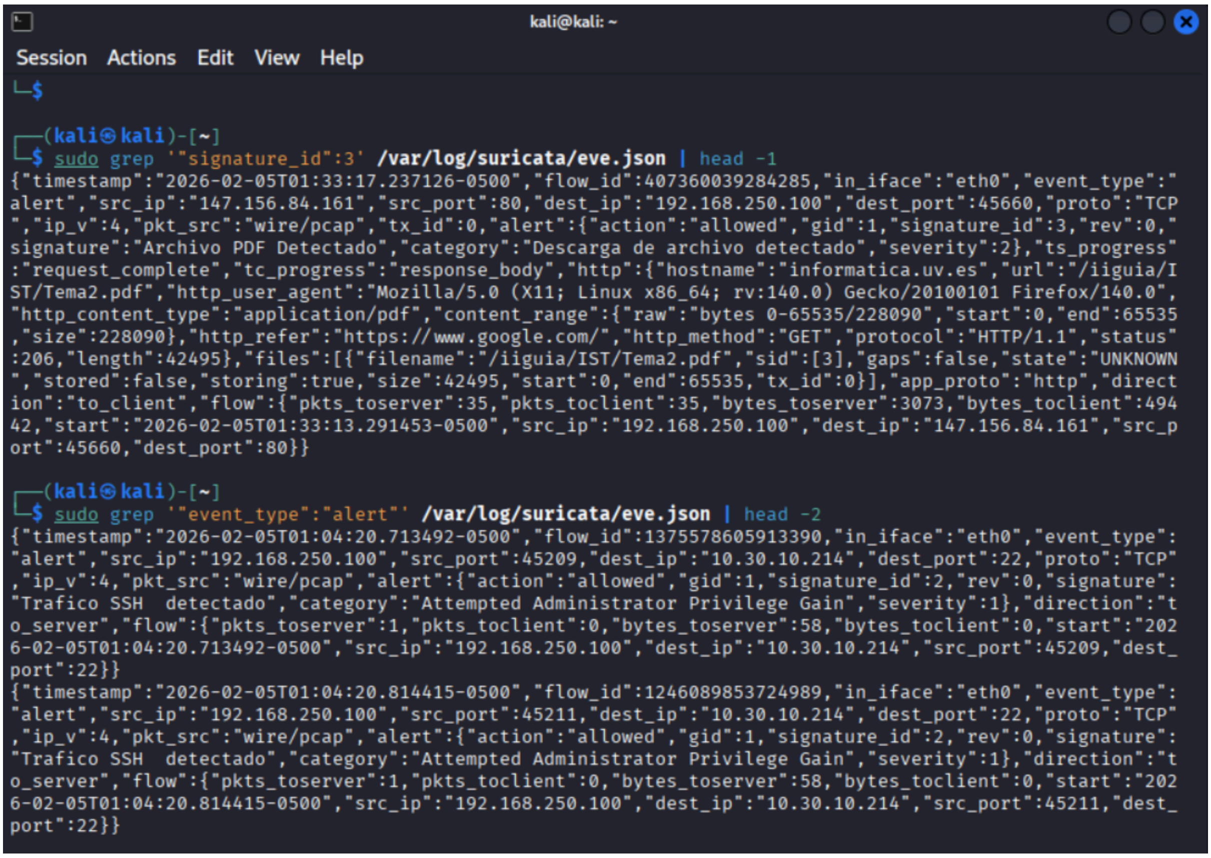
Integration policy	Integration	Namespace	Output	Actions
suricata-1	Suricata v2.27.0	default	default	···
system-1	System v2.12.0	default	default	···

Suricata

Reglas



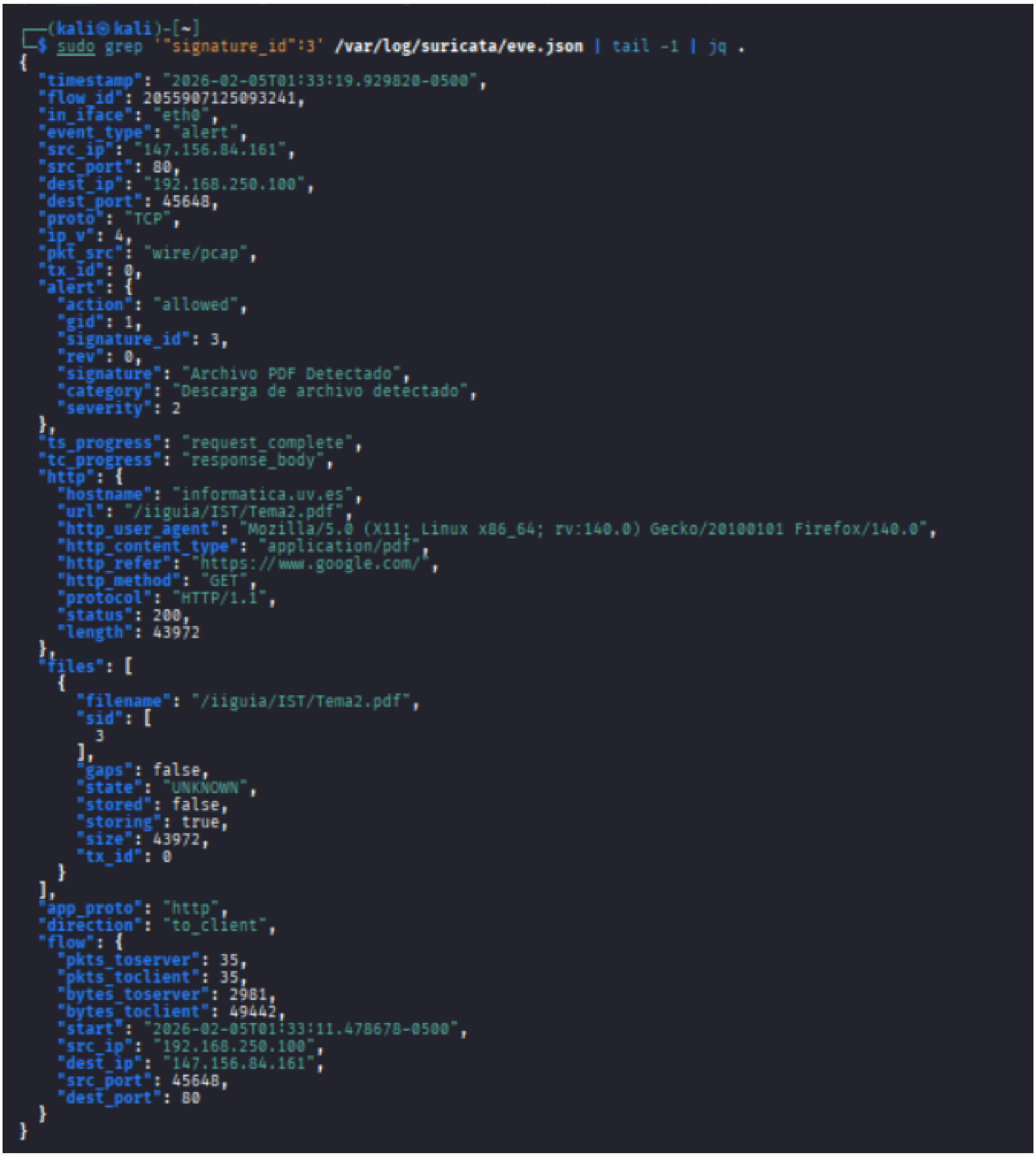
```
┌──(kali㉿kali)-[~]
└─$ cat /etc/suricata/rules/suricata.rules
#alert tcp any any → any any (msg:"trafico detectado"; sid:1;)
alert tcp any any → 10.30.10.214 22 (msg:"Trafico SSH  detectado"; sid:2; classtype:
attempted-admin;)
alert http any any → any any (msg:"Archivo PDF Detectado"; flow:established,to_clien
t; file_data; content:"%PDF-"; within:5; filestore ; sid:3; classtype:file-download;)
```



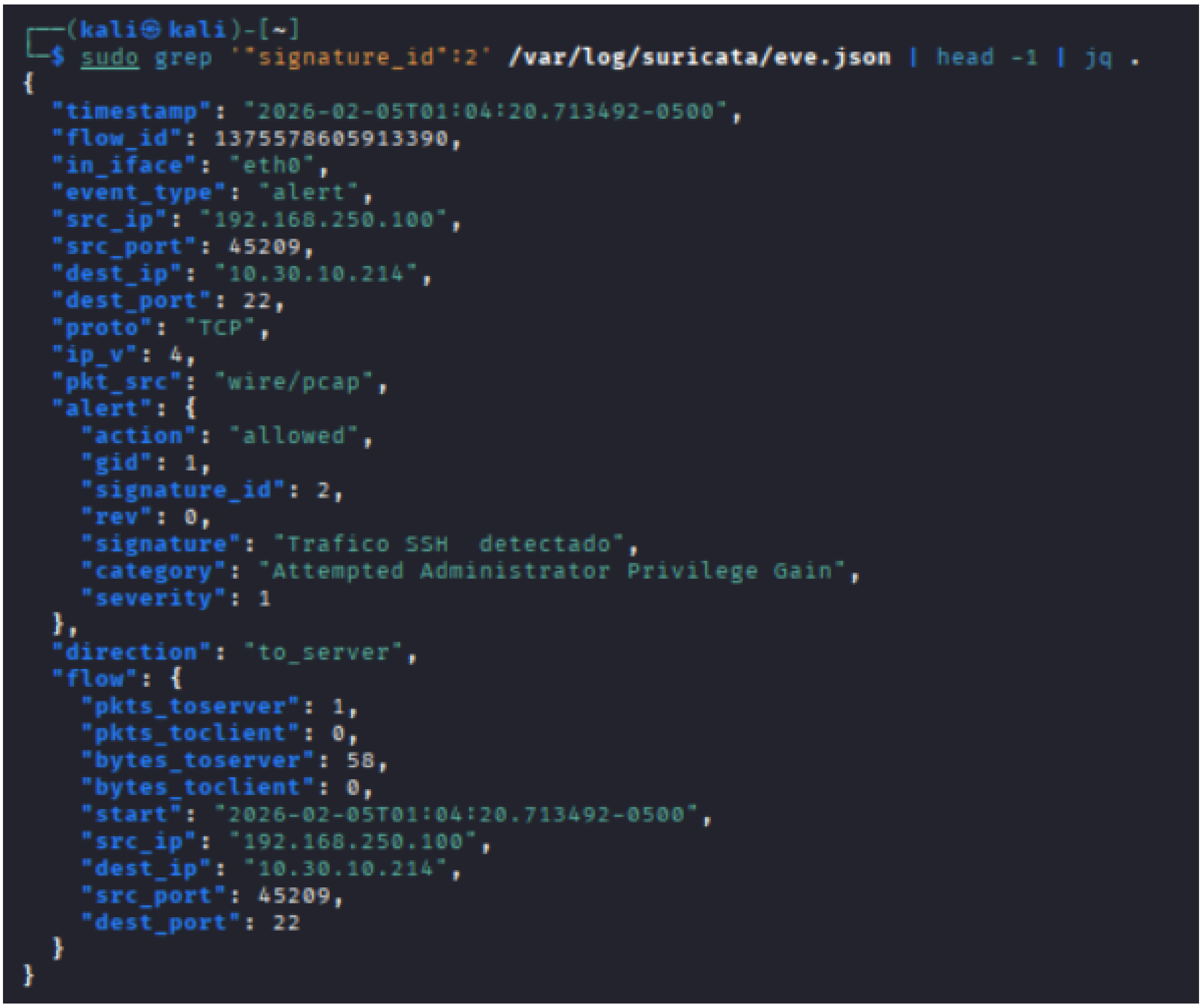
```
└─$

┌──(kali㉿kali)-[~]
└─$ sudo grep '"signature_id":3' /var/log/suricata/eve.json | head -1
{"timestamp":"2026-02-05T01:33:17.237126-0500","flow_id":407360039284285,"in_iface":"eth0","event_type":"
alert","src_ip":"147.156.84.161","src_port":80,"dest_ip":"192.168.250.100","dest_port":45660,"proto":"TCP
","ip_v":4,"pkt_src":"wire/pcap","tx_id":0,"alert":{"action":"allowed","gid":1,"signature_id":3,"rev":0,"
signature":"Archivo PDF Detectado","category":"Descarga de archivo detectado","severity":2},"ts_progress"
:"request_complete","tc_progress":"response_body","http":{"hostname":"informatica.uv.es","url":"/iiguia/I
ST/Tema2.pdf","http_user_agent":"Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0",
"http_content_type":"application/pdf","content_range":{"raw":"bytes 0-65535/228090","start":0,"end":65535
,"size":228090},"http_refer":"https://www.google.com/","http_method":"GET","protocol":"HTTP/1.1","status"
:206,"length":42495},"files":[{"filename":"/iiguia/IST/Tema2.pdf","sid":[3],"gaps":false,"state":"UNKNOWN
","stored":false,"storing":true,"size":42495,"start":0,"end":65535,"tx_id":0}],"app_proto":"http","direct
ion":"to_client","flow":{"pkts_toserver":35,"pkts_toclient":35,"bytes_toserver":3073,"bytes_toclient":494
42,"start":"2026-02-05T01:33:13.291453-0500","src_ip":"192.168.250.100","dest_ip":"147.156.84.161","src_p
ort":45660,"dest_port":80}}

┌──(kali㉿kali)-[~]
└─$ sudo grep '"event_type":"alert"' /var/log/suricata/eve.json | head -2
{"timestamp":"2026-02-05T01:04:20.713492-0500","flow_id":1375578605913390,"in_iface":"eth0","event_type":
"alert","src_ip":"192.168.250.100","src_port":45209,"dest_ip":"10.30.10.214","dest_port":22,"proto":"TCP"
,"ip_v":4,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":2,"rev":0,"signature":
"Trafico SSH  detectado","category":"Attempted Administrator Privilege Gain","severity":1},"direction":"t
o_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":58,"bytes_toclient":0,"start":"202
6-02-05T01:04:20.713492-0500","src_ip":"192.168.250.100","dest_ip":"10.30.10.214","src_port":45209,"dest_
port":22}}
{"timestamp":"2026-02-05T01:04:20.814415-0500","flow_id":1246089853724989,"in_iface":"eth0","event_type":
"alert","src_ip":"192.168.250.100","src_port":45211,"dest_ip":"10.30.10.214","dest_port":22,"proto":"TCP"
,"ip_v":4,"pkt_src":"wire/pcap","alert":{"action":"allowed","gid":1,"signature_id":2,"rev":0,"signature":
"Trafico SSH  detectado","category":"Attempted Administrator Privilege Gain","severity":1},"direction":"t
o_server","flow":{"pkts_toserver":1,"pkts_toclient":0,"bytes_toserver":58,"bytes_toclient":0,"start":"202
6-02-05T01:04:20.814415-0500","src_ip":"192.168.250.100","dest_ip":"10.30.10.214","src_port":45211,"dest_
port":22}}
```

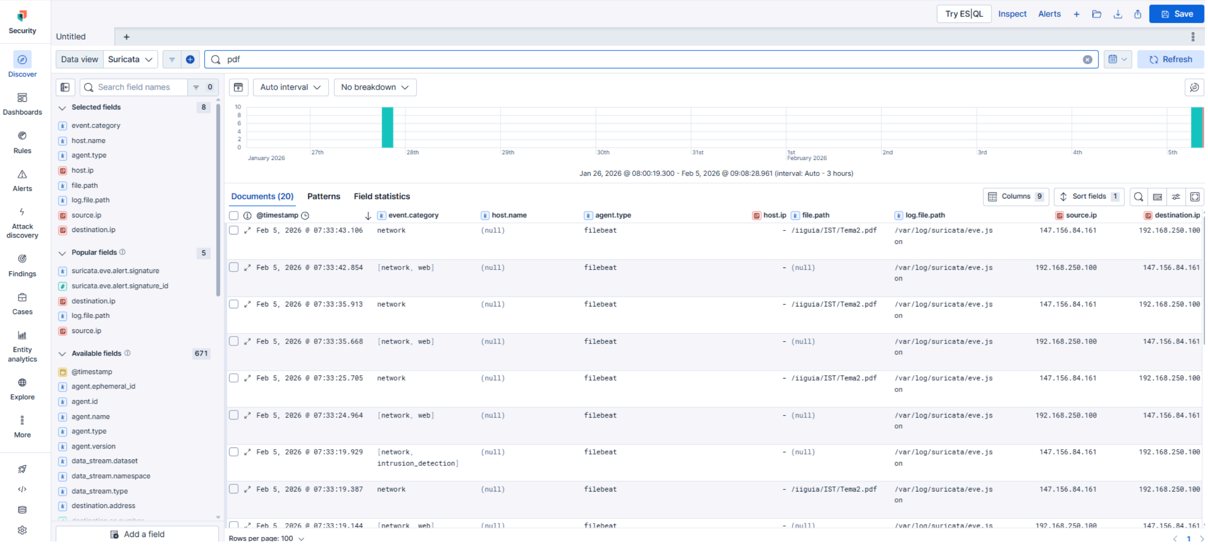


```
┌──(kali㉿kali)-[~]
└─$ sudo grep '"signature_id":3' /var/log/suricata/eve.json | tail -1 | jq .
{
  "timestamp": "2026-02-05T01:33:19.929820-0500",
  "flow_id": 2055907125093241,
  "in_iface": "eth0",
  "event_type": "alert",
  "src_ip": "147.156.84.161",
  "src_port": 80,
  "dest_ip": "192.168.250.100",
  "dest_port": 45648,
  "proto": "TCP",
  "ip_v": 4,
  "pkt_src": "wire/pcap",
  "tx_id": 0,
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 3,
    "rev": 0,
    "signature": "Archivo PDF Detectado",
    "category": "Descarga de archivo detectado",
    "severity": 2
  },
  "ts_progress": "request_complete",
  "tc_progress": "response_body",
  "http": {
    "hostname": "informatica.uv.es",
    "url": "/iiguia/IST/Tema2.pdf",
    "http_user_agent": "Mozilla/5.0 (X11; Linux x86_64; rv:140.0) Gecko/20100101 Firefox/140.0",
    "http_content_type": "application/pdf",
    "http_refer": "https://www.google.com/",
    "http_method": "GET",
    "protocol": "HTTP/1.1",
    "status": 200,
    "length": 43972
  },
  "files": [
    {
      "filename": "/iiguia/IST/Tema2.pdf",
      "sid": [
        3
      ],
      "gaps": false,
      "state": "UNKNOWN",
      "stored": false,
      "storing": true,
      "size": 43972,
      "tx_id": 0
    }
  ],
  "app_proto": "http",
  "direction": "to_client",
  "flow": {
    "pkts_toserver": 35,
    "pkts_toclient": 35,
    "bytes_toserver": 2981,
    "bytes_toclient": 49442,
    "start": "2026-02-05T01:33:11.478678-0500",
    "src_ip": "192.168.250.100",
    "dest_ip": "147.156.84.161",
    "src_port": 45648,
    "dest_port": 80
  }
}
```



```
┌──(kali㉿kali)-[~]
└─$ sudo grep '"signature_id":2' /var/log/suricata/eve.json | head -1 | jq .
{
  "timestamp": "2026-02-05T01:04:20.713492-0500",
  "flow_id": 1375578605913390,
  "in_iface": "eth0",
  "event_type": "alert",
  "src_ip": "192.168.250.100",
  "src_port": 45209,
  "dest_ip": "10.30.10.214",
  "dest_port": 22,
  "proto": "TCP",
  "ip_v": 4,
  "pkt_src": "wire/pcap",
  "alert": {
    "action": "allowed",
    "gid": 1,
    "signature_id": 2,
    "rev": 0,
    "signature": "Trafico SSH  detectado",
    "category": "Attempted Administrator Privilege Gain",
    "severity": 1
  },
  "direction": "to_server",
  "flow": {
    "pkts_toserver": 1,
    "pkts_toclient": 0,
    "bytes_toserver": 58,
    "bytes_toclient": 0,
    "start": "2026-02-05T01:04:20.713492-0500",
    "src_ip": "192.168.250.100",
    "dest_ip": "10.30.10.214",
    "src_port": 45209,
    "dest_port": 22
  }
}
```

Logs



Data view: Suricata — pdf

Selected fields 8: event.category, host.name, agent.type, host.ip, file.path, log.file.path, source.ip, destination.ip

Popular fields 5: suricata.eve.alert.signature, suricata.eve.alert.signature_id, destination.ip, log.file.path, source.ip

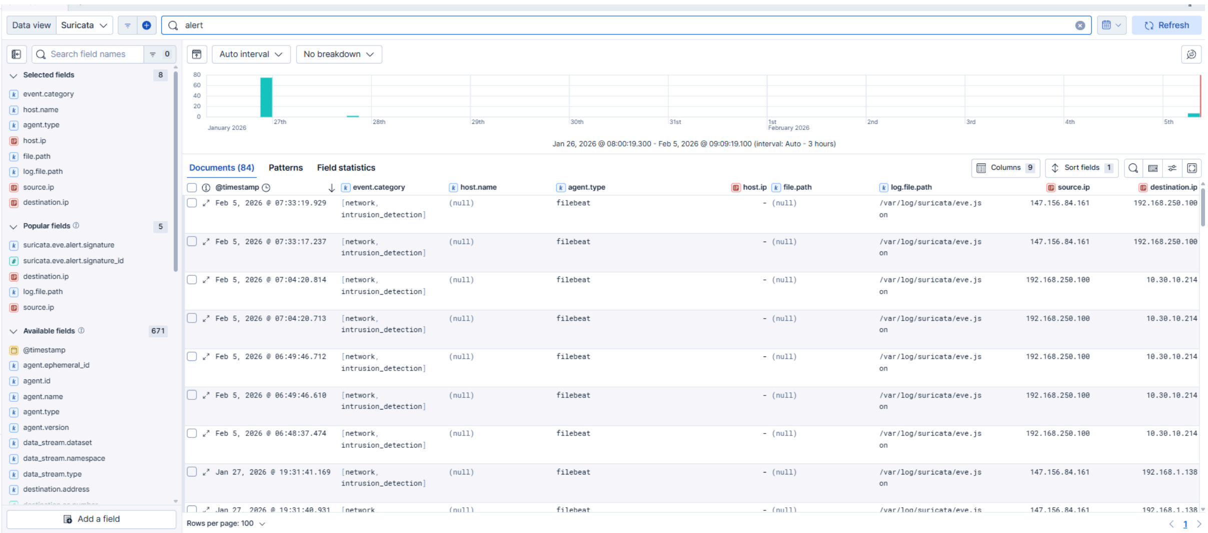
Available fields 671: @timestamp, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, data_stream.dataset, data_stream.namespace, data_stream.type, destination.address

Jan 26, 2026 @ 08:00:19.300 - Feb 5, 2026 @ 09:08:28.961 (interval: Auto - 3 hours)

Documents (20)

@timestamp	event.category	host.name	agent.type	host.ip	file.path	log.file.path	source.ip	destination.ip
Feb 5, 2026 @ 07:33:43.106	network	(null)	filebeat	-	/iiguia/IST/Tema2.pdf	/var/log/suricata/eve.json	147.156.84.161	192.168.250.100
Feb 5, 2026 @ 07:33:42.854	[network, web]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	147.156.84.161
Feb 5, 2026 @ 07:33:35.913	network	(null)	filebeat	-	/iiguia/IST/Tema2.pdf	/var/log/suricata/eve.json	147.156.84.161	192.168.250.100
Feb 5, 2026 @ 07:33:35.668	[network, web]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	147.156.84.161
Feb 5, 2026 @ 07:33:25.705	network	(null)	filebeat	-	/iiguia/IST/Tema2.pdf	/var/log/suricata/eve.json	147.156.84.161	192.168.250.100
Feb 5, 2026 @ 07:33:24.964	[network, web]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	147.156.84.161
Feb 5, 2026 @ 07:33:19.929	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	147.156.84.161	192.168.250.100
Feb 5, 2026 @ 07:33:19.387	network	(null)	filebeat	-	/iiguia/IST/Tema2.pdf	/var/log/suricata/eve.json	147.156.84.161	192.168.250.100
Feb 5, 2026 @ 07:33:19.144	[network, web]	(null)	filebeat	-	(null)	/var/log/suricata/eve.js	192.168.250.100	147.156.84.161

Rows per page: 100



Data view: Suricata — alert

Selected fields 8: event.category, host.name, agent.type, host.ip, file.path, log.file.path, source.ip, destination.ip

Popular fields 5: suricata.eve.alert.signature, suricata.eve.alert.signature_id, destination.ip, log.file.path, source.ip

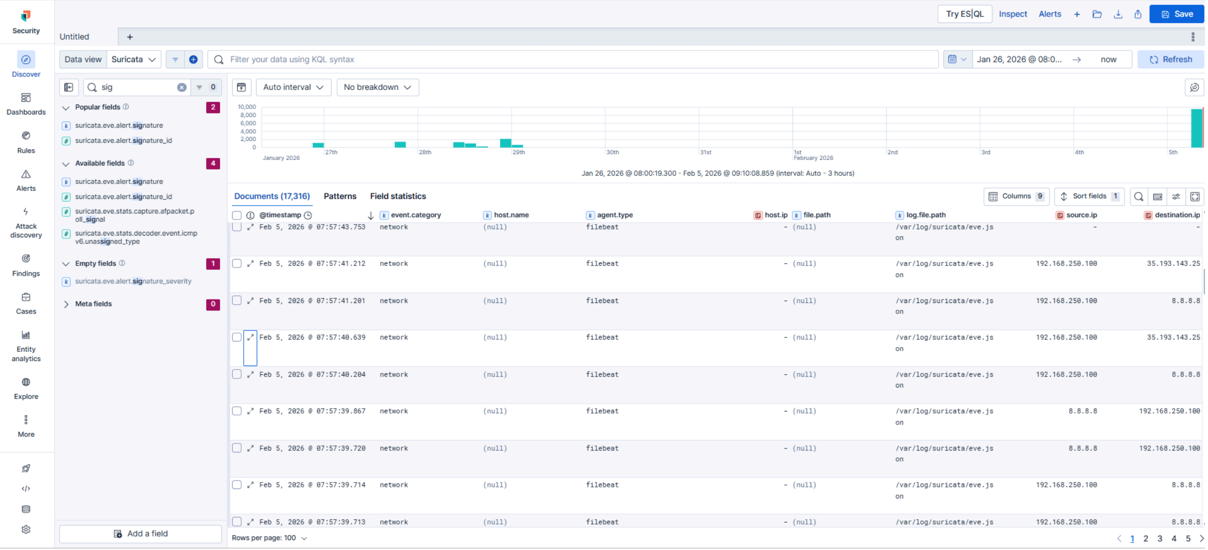
Available fields 671: @timestamp, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, data_stream.dataset, data_stream.namespace, data_stream.type, destination.address

Jan 26, 2026 @ 08:00:19.300 - Feb 5, 2026 @ 09:09:19.100 (interval: Auto - 3 hours)

Documents (84)

@timestamp	event.category	host.name	agent.type	host.ip	file.path	log.file.path	source.ip	destination.ip
Feb 5, 2026 @ 07:33:19.929	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	147.156.84.161	192.168.250.100
Feb 5, 2026 @ 07:33:17.237	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	147.156.84.161	192.168.250.100
Feb 5, 2026 @ 07:04:20.814	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	10.30.10.214
Feb 5, 2026 @ 07:04:20.713	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	10.30.10.214
Feb 5, 2026 @ 06:49:46.712	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	10.30.10.214
Feb 5, 2026 @ 06:49:46.610	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	10.30.10.214
Feb 5, 2026 @ 06:48:37.474	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	10.30.10.214
Jan 27, 2026 @ 19:31:41.169	[network, intrusion_detection]	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	147.156.84.161	192.168.1.138
Jan 27, 2026 @ 19:31:40.931	[network	(null)	filebeat	-	(null)	/var/log/suricata/eve.js	147.156.84.161	192.168.1.138

Rows per page: 100



Data view: Suricata — Jan 26, 2026 @ 08:0... → now

sig

Popular fields 2: suricata.eve.alert.signature, suricata.eve.alert.signature_id

Available fields 4: suricata.eve.alert.signature, suricata.eve.alert.signature_id, suricata.eve.stats.capture.afpacket.poll_signal, suricata.eve.stats.decoder.event.icmpv6.unassigned_type

Empty fields 1: suricata.eve.alert.signature_severity

Meta fields 0

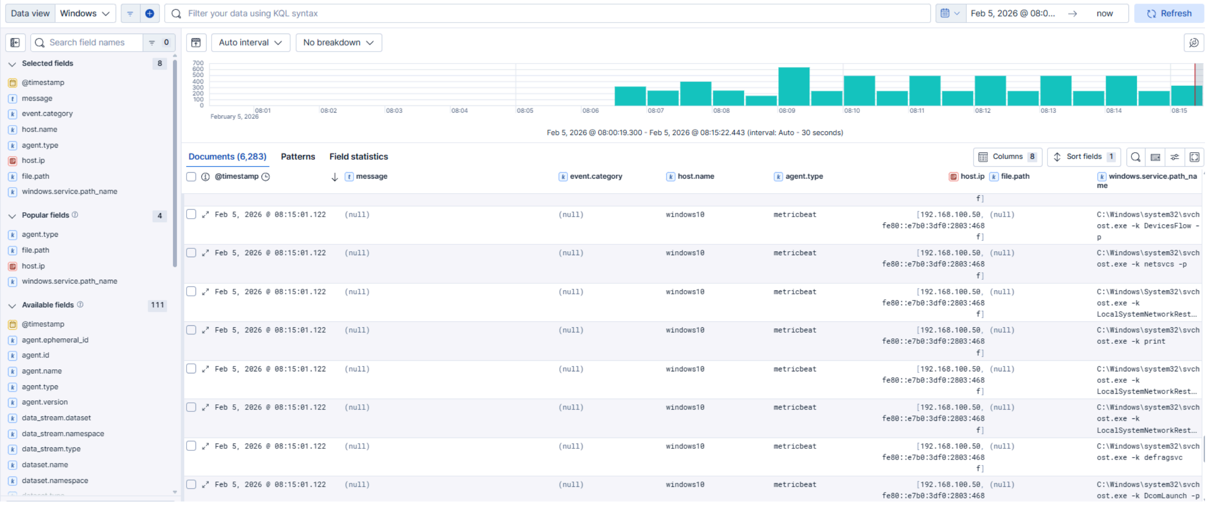
Jan 26, 2026 @ 08:00:19.300 - Feb 5, 2026 @ 09:10:08.859 (interval: Auto - 3 hours)

Documents (17,316)

@timestamp	event.category	host.name	agent.type	host.ip	file.path	log.file.path	source.ip	destination.ip
Feb 5, 2026 @ 07:57:43.753	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	-	-
Feb 5, 2026 @ 07:57:41.212	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	35.193.143.25
Feb 5, 2026 @ 07:57:41.201	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	8.8.8.8
Feb 5, 2026 @ 07:57:40.639	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	35.193.143.25
Feb 5, 2026 @ 07:57:40.204	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	8.8.8.8
Feb 5, 2026 @ 07:57:39.867	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	8.8.8.8	192.168.250.100
Feb 5, 2026 @ 07:57:39.720	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	8.8.8.8	192.168.250.100
Feb 5, 2026 @ 07:57:39.714	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.json	192.168.250.100	8.8.8.8
Feb 5, 2026 @ 07:57:39.713	network	(null)	filebeat	-	(null)	/var/log/suricata/eve.js	192.168.250.100	8.8.8.8

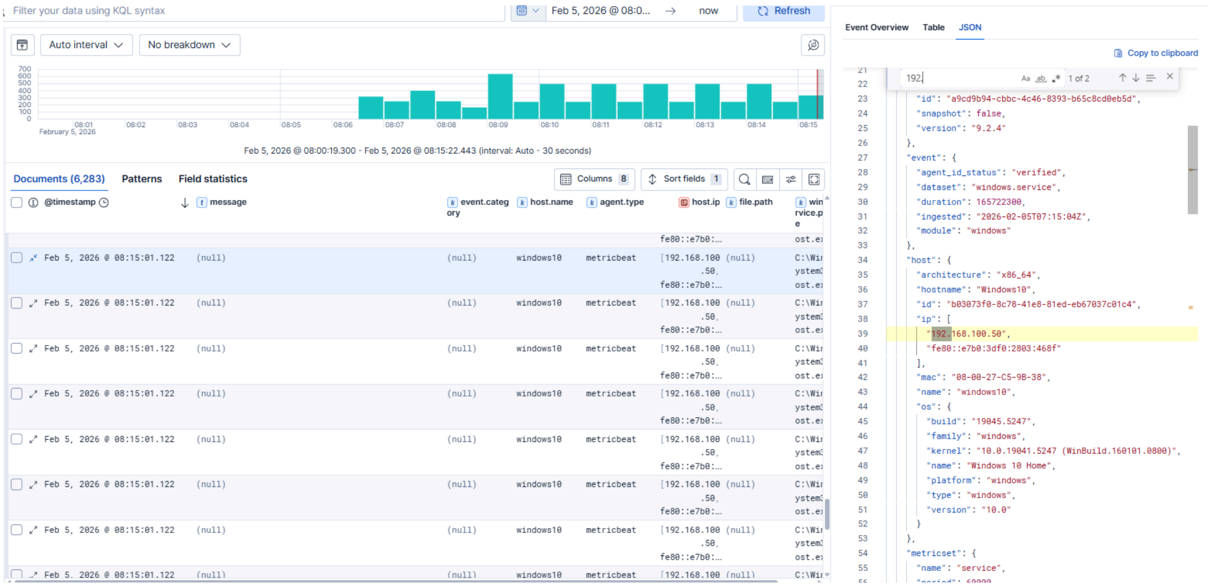
Rows per page: 100 — 1 2 3 4 5

Logs Windows



Feb 5, 2026 @ 08:00:19.300 - Feb 5, 2026 @ 08:15:22.443 (interval: Auto - 30 seconds)

@timestamp	message	event.category	host.name	agent.type	host.ip	file.path	windows.service.path_name
					f]		
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468f]	(null)	C:\Windows\system32\svchost.exe -k DevicesFlow -p
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468f]	(null)	C:\Windows\system32\svchost.exe -k netsvcs -p
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468f]	(null)	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRest…
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468f]	(null)	C:\Windows\system32\svchost.exe -k print
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468f]	(null)	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRest…
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468f]	(null)	C:\Windows\system32\svchost.exe -k LocalSystemNetworkRest…
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468f]	(null)	C:\Windows\system32\svchost.exe -k defragsvc
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:3df0:2803:468	(null)	C:\Windows\system32\svchost.exe -k DcomLaunch -p

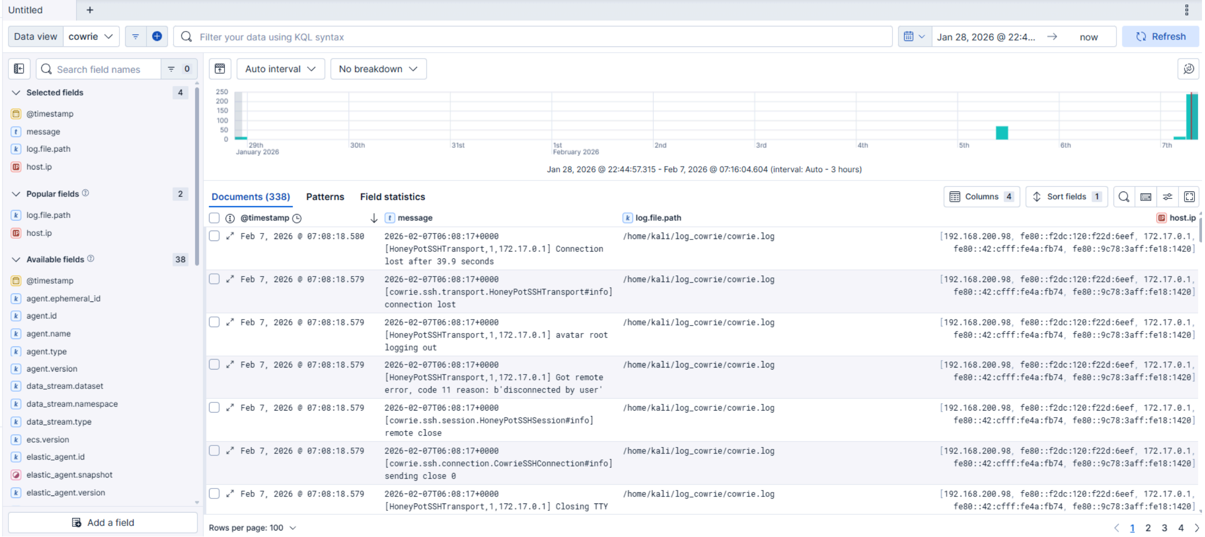


Feb 5, 2026 @ 08:00:19.300 - Feb 5, 2026 @ 08:15:22.443 (interval: Auto - 30 seconds)

@timestamp	message	event.category	host.name	agent.type	host.ip	file.path	windows.service.path_name
					fe80::e7b0:…		ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:…	(null)	C:\Wi ystem ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:…	(null)	C:\Wi ystem ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:…	(null)	C:\Wi ystem ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:…	(null)	C:\Wi ystem ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:…	(null)	C:\Wi ystem ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:…	(null)	C:\Wi ystem ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100.50, fe80::e7b0:…	(null)	C:\Wi ystem ost.e
Feb 5, 2026 @ 08:15:01.122	(null)	(null)	windows10	metricbeat	[192.168.100	(null)	C:\Wi

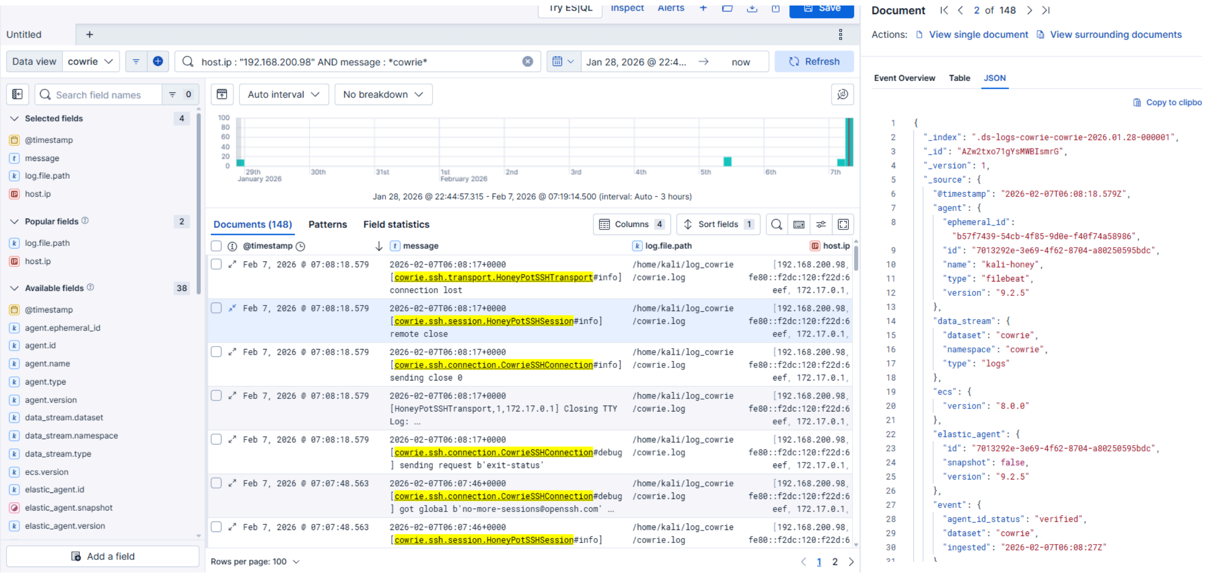
```
      "id": "a9cd9b94-cbbc-4c46-8393-b65c8cd0eb5d",
      "snapshot": false,
      "version": "9.2.4"
    },
    "event": {
      "agent_id_status": "verified",
      "dataset": "windows.service",
      "duration": 165722300,
      "ingested": "2026-02-05T07:15:04Z",
      "module": "windows"
    },
    "host": {
      "architecture": "x86_64",
      "hostname": "Windows10",
      "id": "b03073f0-8c78-41e8-81ed-eb67037c01c4",
      "ip": [
        "192.168.100.50",
        "fe80::e7b0:3df0:2803:468f"
      ],
      "mac": "08-00-27-C5-9B-38",
      "name": "windows10",
      "os": {
        "build": "19045.5247",
        "family": "windows",
        "kernel": "10.0.19041.5247 (WinBuild.160101.0800)",
        "name": "Windows 10 Home",
        "platform": "windows",
        "type": "windows",
        "version": "10.0"
      }
    },
    "metricset": {
      "name": "service",
```

Logs Honeypot



Jan 28, 2026 @ 22:44:57.315 - Feb 7, 2026 @ 07:16:04.604 (interval: Auto - 3 hours)

```
@timestamp                    message                                                  log.file.path                           host.ip
Feb 7, 2026 @ 07:08:18.580    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie/cowrie.log        [192.168.200.98, fe80::f2dc:120:f22d:6eef, 172.17.0.1,
                              [HoneyPotSSHTransport,1,172.17.0.1] Connection                                                     fe80::42:cfff:fe4a:fb74, fe80::9c78:3aff:fe18:1420]
                              lost after 39.9 seconds
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie/cowrie.log        [192.168.200.98, fe80::f2dc:120:f22d:6eef, 172.17.0.1,
                              [cowrie.ssh.transport.HoneyPotSSHTransport#info]                                                   fe80::42:cfff:fe4a:fb74, fe80::9c78:3aff:fe18:1420]
                              connection lost
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie/cowrie.log        [192.168.200.98, fe80::f2dc:120:f22d:6eef, 172.17.0.1,
                              [HoneyPotSSHTransport,1,172.17.0.1] avatar root                                                    fe80::42:cfff:fe4a:fb74, fe80::9c78:3aff:fe18:1420]
                              logging out
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie/cowrie.log        [192.168.200.98, fe80::f2dc:120:f22d:6eef, 172.17.0.1,
                              [HoneyPotSSHTransport,1,172.17.0.1] Got remote                                                     fe80::42:cfff:fe4a:fb74, fe80::9c78:3aff:fe18:1420]
                              error, code 11 reason: b'disconnected by user'
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie/cowrie.log        [192.168.200.98, fe80::f2dc:120:f22d:6eef, 172.17.0.1,
                              [cowrie.ssh.session.HoneyPotSSHSession#info]                                                       fe80::42:cfff:fe4a:fb74, fe80::9c78:3aff:fe18:1420]
                              remote close
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie/cowrie.log        [192.168.200.98, fe80::f2dc:120:f22d:6eef, 172.17.0.1,
                              [cowrie.ssh.connection.CowrieSSHConnection#info]                                                   fe80::42:cfff:fe4a:fb74, fe80::9c78:3aff:fe18:1420]
                              sending close 0
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie/cowrie.log        [192.168.200.98, fe80::f2dc:120:f22d:6eef, 172.17.0.1,
                              [HoneyPotSSHTransport,1,172.17.0.1] Closing TTY                                                    fe80::42:cfff:fe4a:fb74, fe80::9c78:3aff:fe18:1420]
```



host.ip : "192.168.200.98" AND message : *cowrie*

Jan 28, 2026 @ 22:44:57.315 - Feb 7, 2026 @ 07:19:14.500 (interval: Auto - 3 hours)

```
@timestamp                    message                                                  log.file.path            host.ip
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie    [192.168.200.98,
                              [cowrie.ssh.transport.HoneyPotSSHTransport#info]         /cowrie.log              fe80::f2dc:120:f22d:6
                              connection lost                                                                   eef, 172.17.0.1,
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie    [192.168.200.98,
                              [cowrie.ssh.session.HoneyPotSSHSession#info]             /cowrie.log              fe80::f2dc:120:f22d:6
                              remote close                                                                      eef, 172.17.0.1,
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie    [192.168.200.98,
                              [cowrie.ssh.connection.CowrieSSHConnection#info]         /cowrie.log              fe80::f2dc:120:f22d:6
                              sending close 0                                                                   eef, 172.17.0.1,
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie    [192.168.200.98,
                              [HoneyPotSSHTransport,1,172.17.0.1] Closing TTY          /cowrie.log              fe80::f2dc:120:f22d:6
                              Log: ...                                                                          eef, 172.17.0.1,
Feb 7, 2026 @ 07:08:18.579    2026-02-07T06:08:17+0000                                 /home/kali/log_cowrie    [192.168.200.98,
                              [cowrie.ssh.connection.CowrieSSHConnection#debug         /cowrie.log              fe80::f2dc:120:f22d:6
                              ] sending request b'exit-status'                                                  eef, 172.17.0.1,
Feb 7, 2026 @ 07:07:48.563    2026-02-07T06:07:46+0000                                 /home/kali/log_cowrie    [192.168.200.98,
                              [cowrie.ssh.connection.CowrieSSHConnection#debug         /cowrie.log              fe80::f2dc:120:f22d:6
                              ] got global b'no-more-sessions@openssh.com' ...                                  eef, 172.17.0.1,
Feb 7, 2026 @ 07:07:48.563    2026-02-07T06:07:46+0000                                 /home/kali/log_cowrie    [192.168.200.98,
                              [cowrie.ssh.session.HoneyPotSSHSession#info]             /cowrie.log              fe80::f2dc:120:f22d:6
```

```
{
  "_index": ".ds-logs-cowrie-cowrie-2026.01.28-000001",
  "_id": "AZw2txo71gYsMWBIsmrG",
  "_version": 1,
  "_source": {
    "@timestamp": "2026-02-07T06:08:18.579Z",
    "agent": {
      "ephemeral_id":
        "b57f7439-54cb-4f85-9d0e-f40f74a58986",
      "id": "7013292e-3e69-4f62-8704-a80250595bdc",
      "name": "kali-honey",
      "type": "filebeat",
      "version": "9.2.5"
    },
    "data_stream": {
      "dataset": "cowrie",
      "namespace": "cowrie",
      "type": "logs"
    },
    "ecs": {
      "version": "8.0.0"
    },
    "elastic_agent": {
      "id": "7013292e-3e69-4f62-8704-a80250595bdc",
      "snapshot": false,
      "version": "9.2.5"
    },
    "event": {
      "agent_id_status": "verified",
      "dataset": "cowrie",
      "ingested": "2026-02-07T06:08:27Z"
```