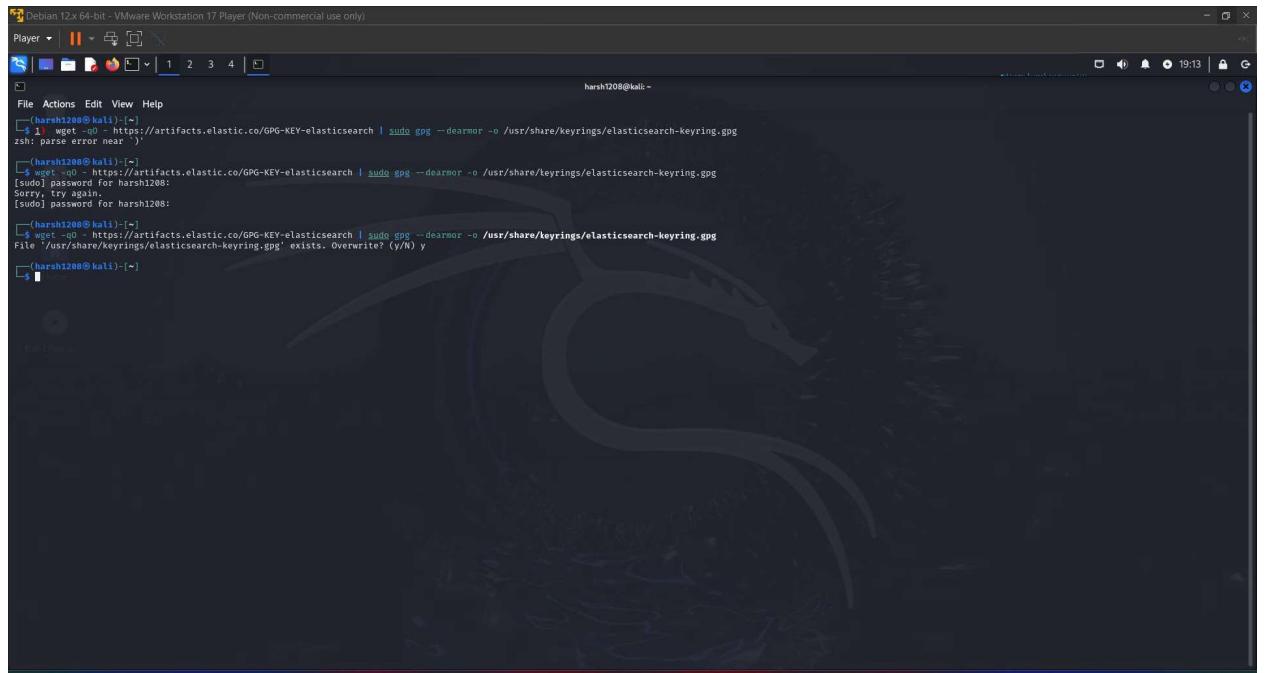


1. Install ElasticSearch (and Kibana), and install Nifi on a KALI VM

INSTALL ELASTICSEARCH

Import the Elasticsearch PGP Key

- 1) wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg



The screenshot shows a terminal window titled "Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)". The terminal session is for user "harsh1208" on a Kali Linux system. The command entered is:

```
harsh1208@kali:~$ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
```

The terminal shows the command being run and the resulting output. There is a parse error message, followed by a password prompt for "harsh1208". The user is prompted to overwrite an existing file, and the command is run again successfully.

Installing from the APT repository

- 1) sudo apt-get install apt-transport-https

```

Debian 12x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | [ ] + [ ] 
File Actions Edit View Help
harsh1208@kali:~$ zsh: parse error near `)'
harsh1208@kali:~[ -] $ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
[sudo] password for harsh1208:
Sorry, try again.
[sudo] password for harsh1208:
[harsh1208@kali:~[ -] $ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
File '/usr/share/keyrings/elasticsearch-keyring.gpg' exists. Overwrite? (y/N) y
[harsh1208@kali:~[ -] $ 1] sudo apt-get install apt-transport-https
zsh: parse error near `)'
[harsh1208@kali:~[ -] $ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
libbadawita-1-0 liblatoi libappstream5 libbatk-adaptor libboost-dev libopenblas-dev libopenblas-pthread-dev libopenblas80 libpython3-all-dev libpython3.12 libpython3.12-dev libstemmer0d libxml2 libxsimd-dev
python3-all-dev python3-anyjson python3-beniget python3-gast python3-pyatspi python3-pygments python3-pyppeteer python3-persistent python3-pythran python3.12-dev x11-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 24.3 kB of archives.
After this operation, 34.8 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 apt-transport-https all 2.7.12+kali1 [24.3 kB]
Fetched 24.3 kB in 0s (74.0 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 444721 files and directories currently installed.)
Preparing to unpack /apt-transport-https_2.7.12+kali1_all.deb ...
Unpacking apt-transport-https (2.7.12+kali1) ...
Setting up apt-transport-https (2.7.12+kali1) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
[harsh1208@kali:~[ -] $ 

```

- 2) echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list

```

Debian 12x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | [ ] + [ ] 
File Actions Edit View Help
harsh1208@kali:~$ [sudo] password for harsh1208:
Sorry, try again.
[sudo] password for harsh1208:
[harsh1208@kali:~[ -] $ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
File '/usr/share/keyrings/elasticsearch-keyring.gpg' exists. Overwrite? (y/N) y
[harsh1208@kali:~[ -] $ 1] sudo apt-get install apt-transport-https
zsh: parse error near `)'
[harsh1208@kali:~[ -] $ sudo apt-get install apt-transport-https
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
libbadawita-1-0 liblatoi libappstream5 libbatk-adaptor libboost-dev libopenblas-dev libopenblas-pthread-dev libopenblas80 libpython3-all-dev libpython3.12 libpython3.12-dev libstemmer0d libxml2 libxsimd-dev
python3-all-dev python3-anyjson python3-beniget python3-gast python3-pyatspi python3-pygments python3-pyppeteer python3-persistent python3-pythran python3.12-dev x11-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 24.3 kB of archives.
After this operation, 34.8 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 apt-transport-https all 2.7.12+kali1 [24.3 kB]
Fetched 24.3 kB in 0s (74.0 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 444721 files and directories currently installed.)
Preparing to unpack /apt-transport-https_2.7.12+kali1_all.deb ...
Unpacking apt-transport-https (2.7.12+kali1) ...
Setting up apt-transport-https (2.7.12+kali1) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
[harsh1208@kali:~[ -] $ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elastic-8.x.list
[harsh1208@kali:~[ -] $ 

```

- 3) sudo apt-get update && sudo apt-get install elasticsearch

```

Debian 12x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | || = 1 2 3 4 | 🔍
File Actions Edit View Help
Fetched 24.3 kB in 0s (74.0 kB/s)
Selecting previously unselected package apt-transport-https.
(Reading database ... 444/721 files and directories currently installed.)
Unpacking apt-transport-https (2.7.12+ kali) ...
Setting up apt-transport-https (2.7.12+ kali) ...
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.

[harsh1208@kali:~] [-]
$ echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee /etc/apt/sources.list.d/elasticsearch-8.x.list
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main

[harsh1208@kali:~] [-]
$ sudo apt-get update && sudo apt-get install elasticsearch
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease [10.4 kB]
Get:2 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [97.6 kB]
Get:3 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 Packages [19.1 MB]
Get:4 http://kali.download/kali kali-rolling/main amd64 Packages [3012 kB]
Get:5 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [44.6 MB]
Get:6 http://kali.download/kali kali-rolling/main amd64 Contrib (deb) [101 kB]
Get:7 http://kali.download/kali kali-rolling/contrib amd64 Packages [219 kB]
Get:8 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [202 kB]
Get:9 http://kali.download/kali kali-rolling/non-free amd64 Packages [863 kB]
Get:10 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [33.0 kB]
Get:11 http://kali.download/kali kali-rolling/non-free firmware amd64 Packages [32.0 kB]
Fetched 68.3 MB in 0s (12.0 MB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
libbadwolf-i-0 libdaniel-libappstream5 libdatk-adaptor libhoobt-dev libboost1.83-dev libopenblas-dev libopenblas libpython3-all-dev libpython3.12-dev libpython3.12 libstemmer0d libxmlb2 libxsimd-dev
python3-all-dev python3-anyjson python3-beniget python3-gast python3-pyatspi python3-pypdf2 python3-pyspeter python3-persistent python3-pythrond 12-dev xt1-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
elasticsearch
0 upgraded, 1 newly installed, 0 to remove and 221 not upgraded.
Need to get 576 MB.
After this operation, 1137 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 elasticsearch amd64 8.13.4 [576 MB]
58% [1 elasticsearch 417 MB/576 MB 72%]
27.6 MB/s 5s

```

Running Elasticsearch with systemd

`sudo /bin/systemctl daemon-reload`

`sudo /bin/systemctl enable elasticsearch.service`

Elasticsearch can be started and stopped as follows:

`sudo systemctl start elasticsearch.service`

`sudo systemctl stop elasticsearch.service`

```

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
harsh1208@kali: ~
File Actions Edit View Help
Generate an enrollment token for Elasticsearch nodes with
'/usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token -s node'.

#### NOT starting on installation, please execute the following statements to configure elasticsearch service to start automatically using systemd
sudo systemctl daemon-reload
sudo systemctl enable elasticsearch.service
tar -xzf /usr/share/elasticsearch/service by executing
sudo systemctl start elasticsearch.service
Scanning processes ...
Scanning linux images ...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

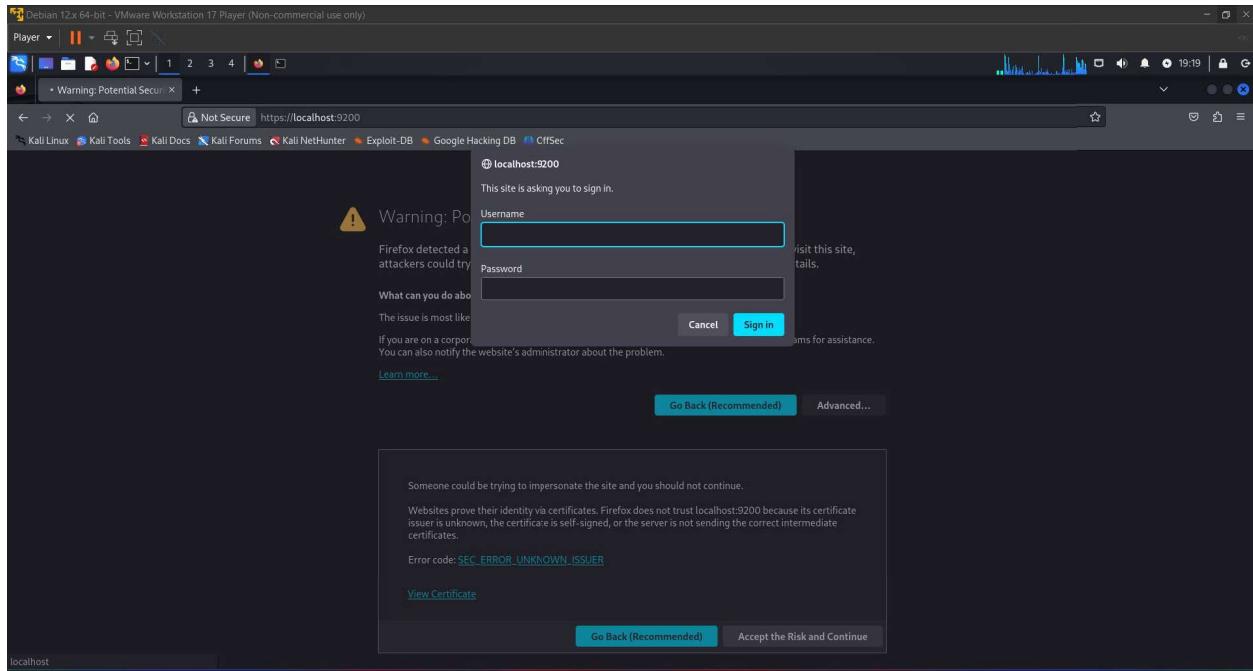
No VM guests are running outdated hypervisor (qemu) binaries on this host.

[harsh1208@kali: ~]
$ sudo /bin/systemctl daemon-reload
[harsh1208@kali: ~]
$ sudo /bin/systemctl enable elasticsearch.service
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.

[harsh1208@kali: ~]
$ sudo systemctl start elasticsearch.service
[harsh1208@kali: ~]
$ systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
   Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
     Active: active (running) since Fri 2024-05-10 19:18:16 EDT; 28s ago
       Main PID: 6087 (java)
          Tasks: 84 (limit: 4567)
         Memory: 2.4G (peak: 2.4G)
            CPU: 0.000 CPU(s)
           CGroup: /system.slice/elasticsearch.service
                   ├─6087 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/_Dcli.libs=lib/tools/server-cli -Des.path.home=/usr/share/elasticsearch
                   ├─6183 /usr/share/elasticsearch/jdk/bin/java -Des.networkAddress.cache.ttl=10 -Djava.security.manager=allow -XX:AlwaysPreTouch -Xss1m -Djava.awt.headless=true -Dfile.encoding=UTF-8
                   └─6189 /usr/share/elasticsearch/modules/x-pack/ml/platform/linux-x64_64/bin/controller

May 10 19:17:57 Kali systemd[1]: Starting elasticsearch.service - Elasticsearch...
May 10 19:18:00 Kali systemd-enterpoint[6087]: May 10, 2024 7:18:00 AM sun.util.locale.LocaleProviderAdapter <clinit>
May 10 19:18:00 Kali systemd-enterpoint[6087]: WARNING: COMPAR locale provider will be removed in a future release
May 10 19:18:16 Kali systemd[1]: Started elasticsearch.service - Elasticsearch.
[lines 1-17/17 (END)]

```



Start Elasticsearch without username and password (disable security settings):

```

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| ☰
File Actions Edit View Help
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt opt proc root run sbin srv sys usr var vmlinuz vmlinuz.old
(harsh1208@kali):~/etc]
$ cd etc
(harsh1208@kali):~/etc]
ls
cifs-utils dns2tcpd.conf grub.d java-21-openjdk logrotate.d nginx profile.d samba subgid updateddb.conf
cloud doc-base gshadow john nikto.conf protocols sambd subgid usb_modeswitch.conf
colord docker kali-menu machine-id nsisconf.nsh proxychains4.conf scalpel subuid usb_modeswitch.d
colorful dhcpcd gpg kismet magic nsswitch.conf pulse screencapture subuid vcconsole.conf
OpenPower kernel-img.conf gtk-2.0 nmap.mime odbc.ini python2.7 subversion vdpa(wrapper).cfg
UPower containerd eas keyutils manpath.config odbcinst.ini python3.7 sudo.conf vim
X11 cracklib elasticsearch guyuager kismet matplotlib.opencl openapi python3.11 security sudo_logsrvd.conf vmware-tools
adduser.conf credstore gsm libcurl curl curl-ca-bundle.pem python3.12 samba_sudoers vulkan
alternatives cron.d environment.conf grub.d-21 openrtsp pythondbus12 sensors3d.conf
apache2 cron.daily ethertypes host.conf id so.conf rcsd profile.sensors_d
apparmor cron.hourly atexec host.conf idso.conf rcsd0 profile.usb_vulkan
apparmor.d cron.monthly firebird hosts.allow libliao.conf modprobe.d opt services_sv_wireshark
apt cron.weekly firefox-esr hosts.deny libaudiotil modules os-release rc4d shadow
apt-get cron.yearly fonts idmandp.conf libaudiotil modules-load.d pam.conf rc5d shadow
apt- scan cron.yearly freeds iplplug libblkdevs.conf motd papersize rc5s shells
avahi crontab issue.net login.defs nfs.conf powershell-empire rut systemd
bash bash_completion cryptsetup-nuke-password fstab inetsim libibus.conf ssh terminfo_xfce4
bash_completion.d crypttab gai.conf ipmi.conf mysql passwd reaver.conf smartmontools
bindsentry.blacklist cryptstore gal.conf initramfs-tools libpaper.d netconfig redsocks.conf speech-dispatcher
cron.d cron-deps gecue inputrc minicom request-key.conf sqmrap ts.conf
bluez dconf ipredconf locale.alias netconfig Plymouth request-key.conf
ca-certificates.conf debconf.conf ipredconf locales.conf netstiff mg polkit-1 resolv.conf ssh udev
ca-certificates.conf.d default gopher.rc ipsec.secrets localtime networks postgresql-common responder
ca-certificates.conf.dpkg-old deluser.conf ipsec.d locale.gen network postresql Empire
chatscripts dhcpcd group issue.net login.defs nfs.conf ppp rpc strongswan.conf ufw
chromium group- libcid_info.plist libcurl libblockdev.conf modules-load.d pam.conf profile runit strongswan_d unicornsanc
chromium.d dictionaries-common libcurlidInfo.plist libcurlid_info.plist libcurlid_info.p
(jarhsh1208@kali):~/etc]
$ cd elasticsearch
cd: permission denied: elasticsearch
(harsh1208@kali):~/etc]
$ cd elasticsearch
(harsh1208@kali):~/etc/elasticsearch]
ls
certs elasticsearch-plugins.example.yml elasticsearch.keystore elasticsearch.yml jvm.options jvm.options.d log4j2.properties role_mapping.yml roles.yml users users_roles
(harsh1208@kali):~/etc/elasticsearch]
$ 

```

```

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| ☰
File Actions Edit View Help
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt opt proc root run sbin srv sys usr var vmlinuz vmlinuz.old
(harsh1208@kali):~/etc]
$ cd etc
(harsh1208@kali):~/etc]
ls
cifs-utils dns2tcpd.conf grub.d java-21-openjdk logrotate.d nginx profile.d samba subgid updateddb.conf
cloud doc-base gshadow john nikto.conf protocols sambd subgid usb_modeswitch.conf
colord docker kali-menu machine-id nsisconf.nsh proxychains4.conf scalpel subuid usb_modeswitch.d
colorful dhcpcd gpg kismet magic nsswitch.conf pulse screencapture subuid vcconsole.conf
OpenPower kernel-img.conf gtk-2.0 nmap.mime odbc.ini python2.7 subversion vdpa(wrapper).cfg
UPower containerd eas keyutils manpath.config odbcinst.ini python3.7 sudo.conf vim
X11 cracklib elasticsearch guyuager kismet matplotlib.opencl openapi python3.11 security sudo_logsrvd.conf vmware-tools
adduser.conf credstore gsm libcurl curl curl-ca-bundle.pem python3.12 samba_sudoers vulkan
alternatives cron.d environment.conf grub.d-21 openrtsp pythondbus12 sensors3d.conf
apache2 cron.daily ethertypes host.conf id so.conf rcsd profile.sensors_d
apparmor cron.hourly atexec host.conf idso.conf rcsd0 profile.usb_vulkan
apparmor.d cron.monthly firebird hosts.allow libliao.conf modprobe.d opt services_sv_wireshark
apt cron.weekly firefox-esr hosts.deny libaudiotil modules os-release rc4d shadow
apt- scan cron.yearly fonts idmandp.conf libaudiotil modules-load.d pam.conf rc5d shadow
avahi crontab issue.net login.defs nfs.conf powershell-empire rut systemd
bash bash_completion cryptsetup-nuke-password fstab inetsim libibus.conf ssh terminfo_xfce4
bash_completion.d crypttab gai.conf ipmi.conf mysql passwd reaver.conf smartmontools
bindsentry.blacklist cryptstore gal.conf initramfs-tools libpaper.d netconfig redsocks.conf speech-dispatcher
cron.d cron-deps gecue inputrc minicom request-key.conf sqmrap ts.conf
bluez dconf ipredconf locale.alias netconfig Plymouth request-key.conf
ca-certificates.conf debconf.conf ipredconf locales.conf netstiff mg polkit-1 resolv.conf ssh udev
ca-certificates.conf.d default gopher.rc ipsec.secrets localtime networks postgresql-common responder
ca-certificates.conf.dPKG-old deluser.conf ipsec.d locale.gen network postresql Empire
chatscripts dhcpcd group issue.net login.defs nfs.conf ppp rpc strongswan.conf ufw
chromium group- libcid_info.plist libcurl libblockdev.conf modules-load.d pam.conf profile runit strongswan_d unicornsanc
chromium.d dictionaries-common libcurlidInfo.plist libcurlid_info.p
(jarhsh1208@kali):~/etc]
$ cd elasticsearch
cd: permission denied: elasticsearch
(harsh1208@kali):~/etc]
$ sudo chmod 777 elasticsearch/
(harsh1208@kali):~/etc]
$ cd elasticsearch
(harsh1208@kali):~/etc/elasticsearch]
ls
certs elasticsearch-plugins.example.yml elasticsearch.keystore elasticsearch.yml jvm.options jvm.options.d log4j2.properties role_mapping.yml roles.yml users users_roles
(harsh1208@kali):~/etc/elasticsearch]
$ 

```

Open yml file

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

File Actions Edit View Help

GNU nano 7.2 Elasticsearch Configuration elasticsearch.yml

```
# NOTE! Elasticsearch comes with reasonable defaults for most settings.
# Before you set out to tweak and tune the configuration, make sure you
# understand what are you trying to accomplish and the consequences.
#
# The primary way of configuring a node is via this file. This template lists
# the most important settings you may want to configure for a production cluster.
#
# Please consult the documentation for further information on configuration options:
# https://www.elastic.co/guide/en/elasticsearch/reference/index.html
#
# -----
# Cluster
# It's a descriptive name for your cluster.
# cluster.name: my-application
#
# -----
# Node
# Use a descriptive name for the node:
# node.name: node-1
#
# Add custom attributes to the node:
# node.attr.rack: r1
#
# -----
# Paths
# Path to directory where to store the data (separate multiple locations by comma):
# path.data: /var/lib/elasticsearch
# Path to log files:
# path.logs: /var/log/elasticsearch
#
# Memory
# Lock the memory on startup:
# bootstrap.memory_lock: true
#
# Make sure that the heap size is set to about half the memory available
# on the system and that the owner of the process is allowed to use this
# limit.
#
# -----
# Help      Write Out      Where Is      Cut      Replace      Execute      Location      Undo      Set Mark      To Bracket      Previous      Redo      Copy      Where Was      Next      Back      Forward      Prev Word      Next Word      Home      End
```

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

File Actions Edit View Help

GNU nano 7.2 elasticsearch.yml

```
# http.port: 9200
# For more information, consult the network module documentation.
#
# -----
# Discovery
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", {"name": "host1"}]
# discovery.seed_hosts: ["host1", "host2"]
#
# Bootstrap the cluster using an initial set of master-eligible nodes:
# cluster.initial_master_nodes: ["node-1", "node-2"]
#
# For more information, consult the discovery and cluster formation module documentation.
#
# -----
# Various
# Allow wildcard deletion of indices:
# action.destructive_requires_name: false
#
# -----
# BEGIN SECURITY AUTO CONFIGURATION
# The following settings, TLS certificates, and keys have been automatically
# generated to configure Elasticsearch security features on 16-05-2024 23:18:48
#
# -----
# Enable security features
xpack.security.enabled: false
xpack.security.enrollment.enabled: False
#
# Enable encryption for HTTP API client connections, such as Kibana, Logstash, and Agents
xpack.security.http.ssl:
  enabled: true
  keyStore.path: certs/http.p12
#
# Enable encryption and mutual authentication between cluster nodes
xpack.security.transport.ssl:
  enabled: true
  verification_mode: certificate
  keyStore.path: certs/transport.p12
  trustStore.path: certs/transport.p12
#
# Create a new cluster with the current node only
# Additional nodes can still join the cluster later
#
# -----
# Help      Write Out      Where Is      Cut      Replace      Execute      Location      Undo      Set Mark      To Bracket      Previous      Redo      Copy      Where Was      Next      Back      Forward      Prev Word      Next Word      Home      End
```

```

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File Actions Edit View Help
ca-certificates.conf      debian_version      gophish          ipsec.d        locale.gen      network          postgresql      resolv.conf      ssl           udev
ca-certificates.conf.dpkg-old default      gprofng.rc      ipsec.secrets  localtime       networks         postgresql-common responder    ss裂          udisks2
chatscripts               deluser.conf       groff           issue          logcheck       nfs.conf        powershell-empire  rmt           strongswan.conf      ufw
chromium                  dhclient.conf     group          iis             logstash      nftables.conf    powershell      runit          strongswan.d       unicorese
chromium.d                dictionaries-common group-          iis             logstash.conf  nftables        profile          runit          strongswan.d       update-motd.d
(harsh1208㉿kali):~/etc]
└── elasticsearch
  cd: permission denied: elasticsearch
(harsh1208㉿kali):~/etc]
$ sudo chmod 777 elasticsearch/
(harsh1208㉿kali):~/etc]
⇒ cd elasticsearch
(harsh1208㉿kali):~/etc/elasticsearch]
ls                                elasticsearch-plugins.example.yml  elasticsearch.keystore  elasticsearch.yml  jvm.options  jvm.options.d  log4j2.properties  role_mapping.yml  roles.yml  users  users_roles
└── etc
  └── elasticsearch
    └── elasticsearch
      └── elasticsearch
        └── elasticsearch
          └── elasticsearch
            └── elasticsearch
              └── elasticsearch
                └── elasticsearch
                  └── elasticsearch
                    └── elasticsearch
                      └── elasticsearch
                        └── elasticsearch
                          └── elasticsearch
                            └── elasticsearch
                              └── elasticsearch
                                └── elasticsearch
                                  └── elasticsearch
                                    └── elasticsearch
                                      └── elasticsearch
                                        └── elasticsearch
                                          └── elasticsearch
                                            └── elasticsearch
                                              └── elasticsearch
                                                └── elasticsearch
                                                  └── elasticsearch
                                                    └── elasticsearch
                                                      └── elasticsearch
                                                        └── elasticsearch
                                                          └── elasticsearch
                                                            └── elasticsearch
                                                              └── elasticsearch
                                                                └── elasticsearch
                                                                  └── elasticsearch
                                                                    └── elasticsearch
                                                                      └── elasticsearch
                                                                        └── elasticsearch
                                                                          └── elasticsearch
                                                                            └── elasticsearch
                                                                              └── elasticsearch
                                                                                └── elasticsearch
                      ↵
(harsh1208㉿kali):~/etc/elasticsearch]
$ sudo systemctl restart elasticsearch.service
(harsh1208㉿kali):~/etc/elasticsearch]
└── elasticsearch.service - Elasticsearch
  ⚡ Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; preset: disabled)
  Active: active (running) since Fri 2024-05-10 19:27:06 EDT; 38s ago
    Main PID: 11801 (java)
      Tasks: 74 (limit: 4567)
        Memory: 2.3G (peak: 2.3G)
       CPU: 0.1% since 19:27:06
      CGroup: /system.slice/elasticsearch.service
          └─11801 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+UseSerialGC -Dcli.name=server -Dcli.script=/usr/share/elasticsearch/bin/elasticsearch -Dcl.lib=lib/tools/server-cli -Des.path.home=/usr/share/elasticsearch -Des.pidfile=/var/run/elasticsearch/elasticsearch.pid -Des.logstash=/usr/share/elasticsearch/bin/logstash -Des.logstash.inputs=junit -Des.logstash.outputs=junit -Des.logstash.proces...
      ↵
May 10 19:26:49 kali systemd[1]: Starting elasticsearch.service - Elasticsearch...
May 10 19:26:50 kali systemd[1]: [11801] May 10, 2024 7:26:52 PM sun.util.locale.provider.LocaleProviderAdapter <clinit>
May 10 19:26:52 kali systemd[1]: [11801] WARNING: COMPAT locale provider will be removed in a future release
May 10 19:27:06 kali systemd[1]: Started elasticsearch.service - Elasticsearch.
[lines 1-17/17 (END)]

```

```

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
File | Player | || | ⊞ | 1 2 3 4 | ☰ | ✎ |
localhost:9200/  https://localhost:9200
← → 🔍 https://localhost:9200
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB ClfSec
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
error:
  root_cause:
    type: "security_exception"
    reason: "missing authentication credentials for REST request [/]"
    header:
      WWW-Authenticate:
        0: ".Basic realm="security" charset="UTF-8""
        1: ".Bearer realm="security""
        2: ".ApiKey"
    type: "security_exception"
    reason: "missing authentication credentials for REST request [/]"
    header:
      WWW-Authenticate:
        0: ".Basic realm="security" charset="UTF-8""
        1: ".Bearer realm="security""
        2: ".ApiKey"
status: 401

```

INSTALL KIBINA

Download Kibana at:

Import the Elastic PGP key

- 1) wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg

Install from the APT repository

```
1)sudo apt-get install apt-transport-https  
2)echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg]  
https://artifacts.elastic.co/packages/8.x/apt stable main" | sudo tee  
/etc/apt/sources.list.d/elastic-8.x.list
```

You can install the Kibana Debian package with:

```
sudo apt-get update && sudo apt-get install kibana
```

The screenshot shows a terminal window titled "Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)". The user is in the directory "/etc/elasticsearch". They run the command "wget -q https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg" to download and import the GPG key. Then, they run "sudo apt update" followed by "sudo apt install kibana". The output shows several dependencies being installed, including libatk-bridge0.0, libatk-bridge0.0-dev, libatk-adopter, libboost-dev, libboost1.83-dev, libopenblas-dev, libopenblas-pthread-dev, libopenblas0, libpython3.12-dev, libpython3.12, libstemmer0, libxml2, libxsimd-dev, python3-all-dev, python3-anyjson, python3-benignet, python3-gast, python3-pypdf2, python3-pypyteer, python3-persistent, python3-pythran, python3.12-dev, xt1-dev, zenity, and zenity-common. The user also runs "zenity --info" to show a message about OpenSSL providers. Finally, they run "kibana" to start the application.

```
harsh1208@kali:~/etc/elasticsearch$ wget -q https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
[sudo] password for harsh1208:
File '/usr/share/keyrings/elasticsearch-keyring.gpg' exists. Overwrite? (y/N)
Enter new filename:
gpg: no valid OpenPGP data found.
gpg: dearmoring failed: file exists
[harsh1208@kali:~/etc/elasticsearch]$ sudo apt update
Hit:1 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Hit:2 http://http.kali.org/kali kali-rolling InRelease
Reading package lists...
Reading package lists... Done
Resolving dependencies...
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer required:
libatk-bridge0.0 libatk-bridge0.0-dev libatk-adopter libboost-dev libboost1.83-dev libopenblas-dev libopenblas-pthread-dev libopenblas0 libpython3.12-dev libpython3.12 libstemmer0 libxml2 libxsimd-dev python3-all-dev python3-anyjson python3-benignet python3-gast python3-pypdf2 python3-pypyteer python3-persistent python3-pythran python3.12-dev xt1-dev zenity zenity-common
Use 'sudo apt autoremove' to remove them.
The following NEW packages will be installed:
kibana
0 upgraded, 1 newly installed, 0 to remove and 221 not upgraded.
Need to get 321 MB of archives.
After this operation, 938 MB of additional disk space will be used.
Get:1 https://artifacts.elastic.co/packages/8.x/apt stable/main amd64 kibana amd64 8.13.4 [321 MB]
Fetched 321 MB in 11s (29.2 MB/s)
Selecting previously unselected package kibana.
(Reading database ... 446006 files and directories currently installed.)
Preparing to unpack .../kibana_8.13.4_amd64.deb ...
Unpacking kibana (8.13.4) ...
Setting up kibana (8.13.4) ...
Creating kibana group... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.13/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
[harsh1208@kali:~/etc/elasticsearch]$
```

Run Kibana with system

```
sudo /bin/systemctl daemon-reload
```

```
sudo /bin/systemctl enable kibana.service
```

```
sudo systemctl start kibana.service
```

```
sudo systemctl stop kibana.service
```

```

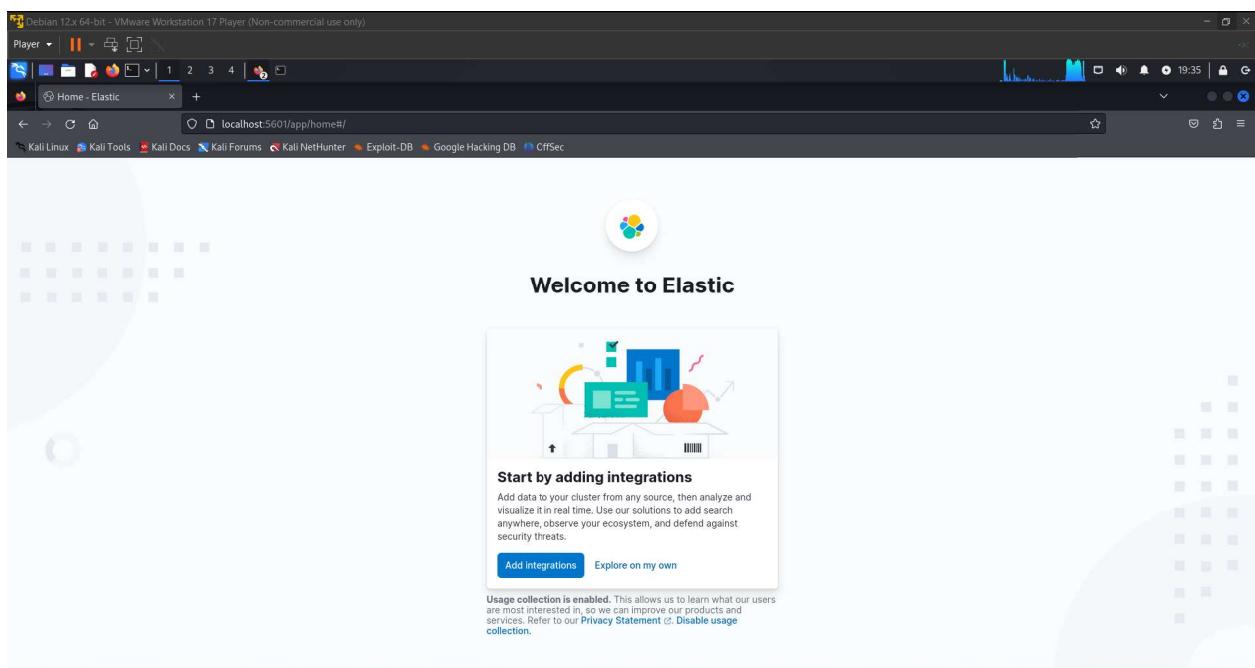
Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)
Player | ||| 1 2 3 4 | 19:34 | Lock

File Actions Edit View Help
harsh1208@kali:/etc/elasticsearch x harsh1208@kali:/etc/elasticsearch x
Creating Kibana user... ok
Kibana is currently running with legacy OpenSSL providers enabled! For details on how to disable see https://www.elastic.co/guide/en/kibana/8.13/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
Scanning processes...
Scanning linux images...
Running kernel seems to be up-to-date.
No services need to be restarted.
No containers need to be restarted.
No user sessions are running outdated binaries.
No VM guests are running outdated hypervisor (qemu) binaries on this host.
[harsh1208@kali]:/etc/elasticsearch]
└─$ sudo /bin/systemctl daemon-reload
[harsh1208@kali]:/etc/elasticsearch]
└─$ sudo /bin/systemctl enable kibana.service
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.service.

[harsh1208@kali]:/etc/elasticsearch]
└─$ sudo systemctl start kibana.service
[harsh1208@kali]:/etc/elasticsearch]
└─$ kibana.service - Kibana
● kibana.service - Kibana
  └─ loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: disabled)
    Active: active (running) since Fri 2024-05-10 19:34:31 EDT; 11s ago
      Main PID: 15402 (node)
        Tasks: 11 (limit: 4567)
       Memory: 356.8M (peak 357.2M)
        CPU: 0ms
       CGroup: /system.slice/kibana.service
              └─ 15402 /usr/share/kibana/bin/../node/bin/node /usr/share/kibana/bin/.../src/cli/dist

May 10 19:34:32 kali kibana[15402]: {"log.level": "info", "@timestamp": "2024-05-10T23:34:32.229Z", "log.logger": "elasticsearch-apm-node", "ecs.version": "8.10.0", "agentVersion": "4.4.0", "env": {"pid": 15402, "proctitle": "/usr/share/kibana/bin/.../node"}, "filebeat": {"version": "8.10.0"}, "filebeat.inputs": [{"type": "log", "log_type": "raw"}], "http": {"method": "GET", "path": "/"}, "kibana": {"version": "8.10.0"}, "logstash": {"version": "8.10.0"}, "node": {"os": "Debian 12.0 (x64)", "version": "v12.0.0-kali1-amd64"}, "process": {"name": "kibana", "pid": 15402, "ppid": 15389, "user": "root", "version": "8.10.0"}, "system": {"cpu": "Intel(R) Core(TM) i7-13650U CPU @ 2.00GHz", "mem_free": 356.809M, "mem_total": 357.209M}, "time": "2024-05-10T23:34:32.229Z"}, "type": "elasticsearch_apm_node"}, "[INFO] [root] Kibana is starting
May 10 19:34:33 kali kibana[15402]: [2024-05-10T19:34:33.719+04:00][INFO][root] Kibana version is 8.10.0. The following plugins are disabled: "cloudChat,cloudExperiments,cloudFullStory,profilingDataAccess,profiling,securitySolutionServerless,server"
May 10 19:34:34 kali kibana[15402]: [2024-05-10T19:34:34.782+04:00][INFO][root] Kibana version is 8.10.0. The following plugins are disabled: "cloudChat,cloudExperiments,cloudFullStory,profilingDataAccess,profiling,securitySolutionServerless,server"
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.587+04:00][INFO][http.server.Preboot] http server running at http://localhost:5601
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.721+04:00][INFO][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.747+04:00][INFO][preboot] "interactiveSetup" plugin is loading setup.. Validating Elasticsearch connection configuration...
May 10 19:34:41 kali kibana[15402]: [2024-05-10T19:34:41.767+04:00][INFO][preboot] "interactiveSetup" plugin is loading setup.. Validating Elasticsearch connection configuration...
May 10 19:34:42 kali kibana[15402]: [2024-05-10T19:34:42.032+04:00][WARN] [config.deprecation] The default mechanism for reporting privileges will work differently in future versions, which will affect the behavior of this cluster. Set [lines 1-21 (END)]

```



Create Index

The screenshot shows the Elasticsearch Index Management interface. On the left, there's a sidebar with sections for Management (Ingest Pipelines, Index Management, Alerts and Insights, Kibana), Data (Index Lifecycle Policies, Snapshot and Restore, Rollup Jobs, Transformations, Remote Clusters, Migrate), and Kibana (Data Views, Plugins). The main area is titled 'Index Management' and has tabs for Indices, Data Streams, Index Templates, Component Templates, and Enrich Policies. The 'Indices' tab is selected. It displays a table with one row for the index 'cybersift'. The table columns include Name, Health, Status, Primaries, Replicas, Docs count, Storage size, and Data stream. The 'cybersift' index is shown with a yellow health status, open status, 1 primary, 1 replica, 227 documents, and 227b storage size. There are also buttons for 'Create index', 'Reload indices', and filters for 'Lifecycle status' and 'Lifecycle phase'.

Install Apache Nifi

Install java:

The screenshot shows a terminal window and a web browser window. The terminal window is running on a Kali Linux VM and shows the user navigating to the /etc/elasticsearch directory and listing files. The output includes commands like 'cd ..', 'cd /etc', and 'java -version'. The Java version is OpenJDK 21.0.2+9-0~2242~a1-16. The web browser window shows the 'Welcome to Elastic' page, which includes a 'Start by adding integrations' section and a 'Using Elasticsearch' link.

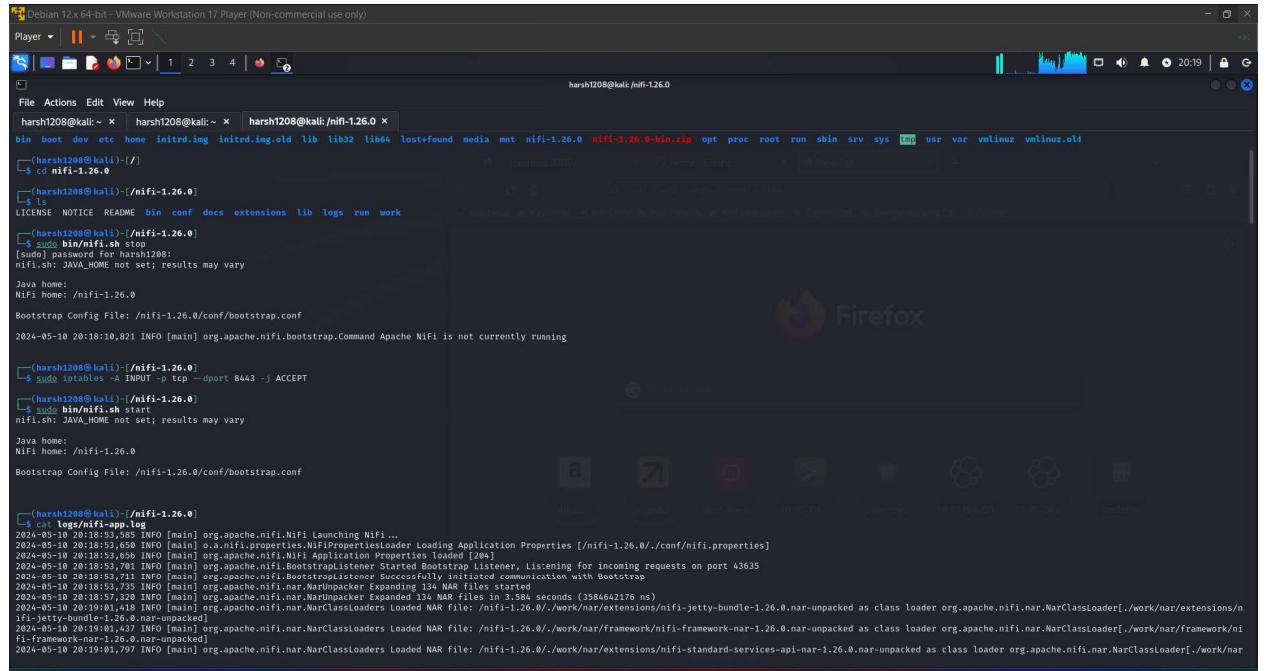
WGET NIFI

```
harsh1208@kali: /etc/elasticsearch x harsh1208@kali: / 
[harsh1208@kali ~]$ cd .. 
[harsh1208@kali ~]$ cd .. 
[harsh1208@kali ~]$ cd .. 
[harsh1208@kali ~]$ java -version 
java version "11.0.10" 2020-10-14 LTS 
Java(TM) SE Runtime Environment (build 11.0.10+11-Debian) 
OpenJDK 64-Bit Server VM (build 11.0.10+11-Debian, mixed mode, sharing) 
[harsh1208@kali ~]$ wget https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip 
[sudo] password for harsh1208: 
Resolving dlcdn.apache.org (dlcdn.apache.org) ... 151.101.2.132, 2a04:4e42::644 
Connecting to dlcdn.apache.org (dlcdn.apache.org)|151.101.2.132|:443... connected. 
HTTP request sent, awaiting response... 
^C 
[harsh1208@kali ~]$ ls 
[nifi-1.26.0-bin.zip] 
[harsh1208@kali ~]$ curl -I https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip 
HTTP/2 200 OK 
Date: Mon, 10 May 2021 19:43:45 GMT 
Content-Type: application/zip 
Content-Length: 328098960 
Last-Modified: Mon, 10 May 2021 19:43:45 GMT 
[harsh1208@kali ~]$ curl -O https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip 
[harsh1208@kali ~]$ ls 
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt nifi-1.26.0-bin.zip opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old 
[harsh1208@kali ~]$ sudo unzip nifi-1.26.0-bin.zip
```

```
harsh1208@kali: /etc/elasticsearch x harsh1208@kali: /nifi-1.26.0/conf x 
[harsh1208@kali ~]$ ls 
[nifi-1.26.0-bin.zip] 
[harsh1208@kali ~]$ curl -I https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip 
HTTP/2 200 OK 
Date: Mon, 10 May 2021 19:43:45 GMT 
Content-Type: application/zip 
Content-Length: 328098960 
Last-Modified: Mon, 10 May 2021 19:43:45 GMT 
[harsh1208@kali ~]$ curl -O https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip 
[harsh1208@kali ~]$ ls 
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt nifi-1.26.0 nifi-1.26.0-bin.zip opt proc root run sbin srv sys tmp usr var vmlinuz vmlinuz.old 
[harsh1208@kali ~]$ sudo unzip nifi-1.26.0-bin.zip 
[harsh1208@kali ~]$ ls 
[nifi-1.26.0] 
[harsh1208@kali ~]$ cd nifi-1.26.0 
[harsh1208@kali ~]$ ls 
LICENSE NOTICE README bin conf docs extensions lib 
[harsh1208@kali ~]$ cd conf 
[harsh1208@kali ~]$ ls 
[nifi-1.26.0] 
[harsh1208@kali ~]$ curl -I https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip 
HTTP/2 200 OK 
Date: Mon, 10 May 2021 19:43:45 GMT 
Content-Type: application/zip 
Content-Length: 328098960 
Last-Modified: Mon, 10 May 2021 19:43:45 GMT 
[harsh1208@kali ~]$ curl -O https://dlcdn.apache.org/nifi/1.26.0/nifi-1.26.0-bin.zip 
[harsh1208@kali ~]$ ls 
[nifi-1.26.0] 
[harsh1208@kali ~]$ sudo nano nifi.properties
```

```
sudo bin/nifi.sh start
```

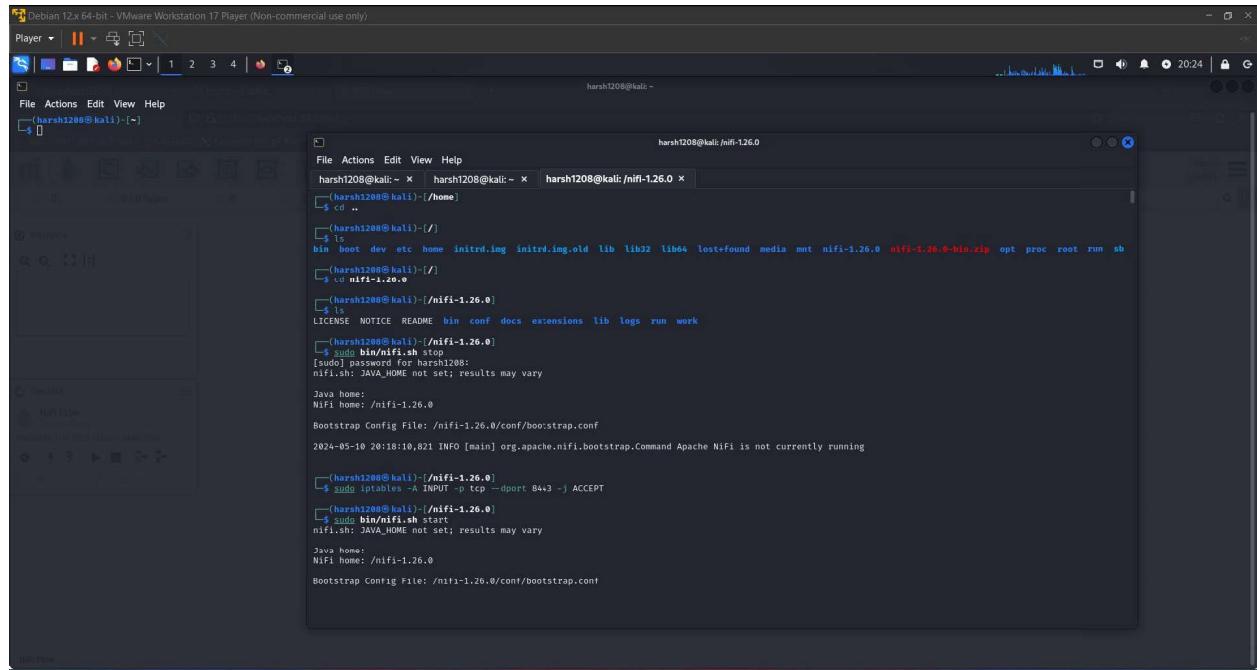
```
cat logs/nifi-app.log
```



```
harsh1208@kali:~ % sudo bin/nifi.sh start
[sudo] password for harsh1208:
nifi.sh: JAVA_HOME not set; results may vary
Java home:
Nifi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf
2024-05-10 20:18:10,821 INFO [main] org.apache.nifi.bootstrap.Command Apache NiFi is not currently running

(harsh1208@kali)~/nifi-1.26.0 %
$ sudo iptables -A INPUT -p tcp --dport 8443 -j ACCEPT
(harsh1208@kali)~/nifi-1.26.0 %
$ sudo bin/nifi.sh start
nifi.sh: JAVA_HOME not set; results may vary
Java home:
Nifi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf

(harsh1208@kali)~/nifi-1.26.0 %
cat logs/nifi-app.log
2024-05-10 20:18:53,088 INFO [main] org.apache.nifi.NiFi Launching NiFi...
2024-05-10 20:18:53,088 INFO [main] o.a.nifi.PropertiesLoader Loading Application Properties [/nifi-1.26.0/.conf/nifi.properties]
2024-05-10 20:18:53,056 INFO [main] org.apache.nifi.NiFi Application Properties loaded [204]
2024-05-10 20:18:53,701 INFO [main] org.apache.nifi.BootstrapListener Started Bootstrap Listener, Listening for incoming requests on port 43635
2024-05-10 20:18:53,712 INFO [main] org.apache.nifi.BootstrapListener Successfully listening for communication with Bootstrap
2024-05-10 20:18:53,712 INFO [main] org.apache.nifi.NarUnpacker Expanded 114 NAR files started
2024-05-10 20:18:57,320 INFO [main] org.apache.nifi.NarUnpacker Expanded 114 NAR files in 3.584 seconds (3584642176 ns)
2024-05-10 20:19:01,418 INFO [main] org.apache.nifi.nar.NarClassLoaders Loaded NAR file: /nifi-1.26.0//work/nar/extensions/nifi-jetty-bundle-1.26.0.nar-unpacked as class loader org.apache.nifi.nar.NarClassLoader[./work/nar/extensions/nifi-jetty-bundle-1.26.0.nar-unpacked]
2024-05-10 20:19:01,431 INFO [main] org.apache.nifi.nar.NarClassLoaders Loaded NAR File: /nifi-1.26.0//work/nar/framework/nifi-framework-nar-1.26.0.nar-unpacked as class loader org.apache.nifi.nar.NarClassLoader[./work/nar/framework/nifi-framework-nar-1.26.0.nar-unpacked]
2024-05-10 20:19:01,797 INFO [main] org.apache.nifi.nar.NarClassLoaders Loaded NAR file: /nifi-1.26.0//work/nar/extensions/nifi-standard-services-api-nar-1.26.0.nar-unpacked as class loader org.apache.nifi.nar.NarClassLoader[./work/nar/extensions/nifi-standard-services-api-nar-1.26.0.nar-unpacked]
```



```
harsh1208@kali:~ % sudo bin/nifi.sh start
[sudo] password for harsh1208:
nifi.sh: JAVA_HOME not set; results may vary
Java home:
Nifi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf
2024-05-10 20:18:10,821 INFO [main] org.apache.nifi.bootstrap.Command Apache NiFi is not currently running

(harsh1208@kali)~/nifi-1.26.0 %
$ cd ..
(harsh1208@kali)~
$ ls
bin boot dev etc home initrd.img initrd.img.old lib lib32 lib64 lost+found media mnt nifi-1.26.0 nifi-1.26.0-bin.zip opt proc root run sb
(harsh1208@kali)~/nifi-1.26.0 %
$ ls
(harsh1208@kali)~/nifi-1.26.0 %
$ sudo bin/nifi.sh start
nifi.sh: JAVA_HOME not set; results may vary
Java home:
Nifi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf

(harsh1208@kali)~/nifi-1.26.0 %
$ sudo iptables -A INPUT -p tcp --dport 8443 -j ACCEPT
(harsh1208@kali)~/nifi-1.26.0 %
$ sudo bin/nifi.sh start
nifi.sh: JAVA_HOME not set; results may vary
Java home:
Nifi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf
```

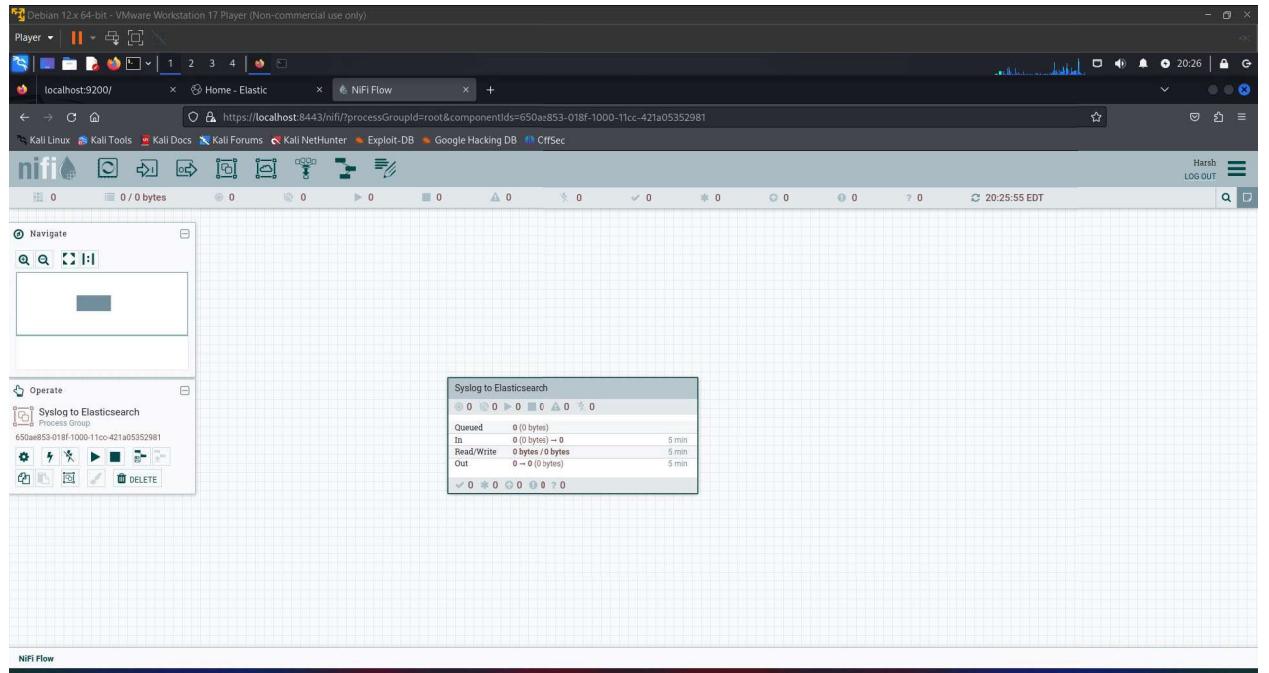
```
[root@kali ~]# ./nifi-1.26.0/nifi.sh set-single-user-credentials Harsh "Ms0123456789"
nifi.sh: JAVA_HOME not set; results may vary
Java home:
NiFi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf
Login Identity Providers Processed [/nifi-1.26.0./conf/login-identity-providers.xml]

[root@kali ~]# ./nifi-1.26.0/nifi.sh stop
nifi.sh: JAVA_HOME not set; results may vary
Java home:
NiFi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf
Login Identity Providers Processed [/nifi-1.26.0./conf/login-identity-providers.xml]

[root@kali ~]# ./nifi-1.26.0/nifi.sh start
nifi.sh: JAVA_HOME not set; results may vary
Java home:
NiFi home: /nifi-1.26.0
Bootstrap Config File: /nifi-1.26.0/conf/bootstrap.conf
Login Identity Providers Processed [/nifi-1.26.0./conf/login-identity-providers.xml]
```

2. Build a simple NiFi pipeline which accept syslog on local port UDP 514 and send it on to ElasticSearch

Create a Process Group name Syslog to Elasticsearch:



1. Set Up Syslog UDP Source

First, you need a processor to receive syslog messages:

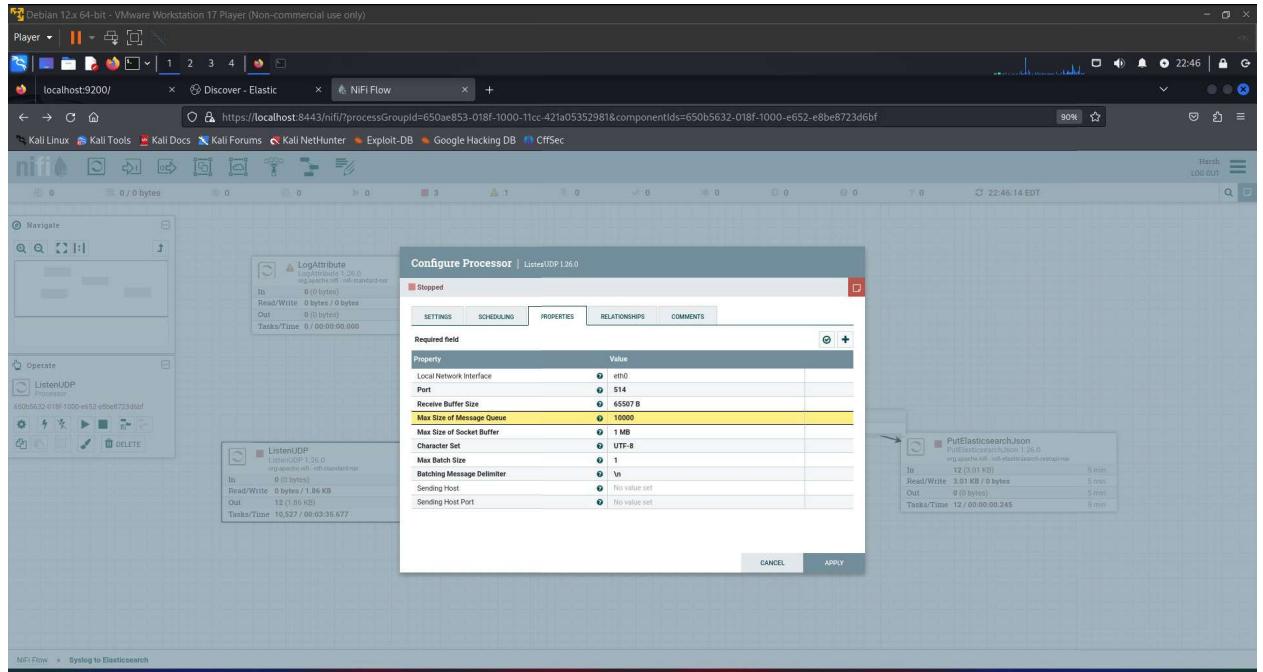
Processor: ListenUDP

Properties:

Local Network Interface: Set to the local network interface IP or keep it blank for all interfaces.

Port: 514

Max Size of Message Queue: Depending on your expected traffic (e.g., 10000).



2. Convert Syslog to JSON

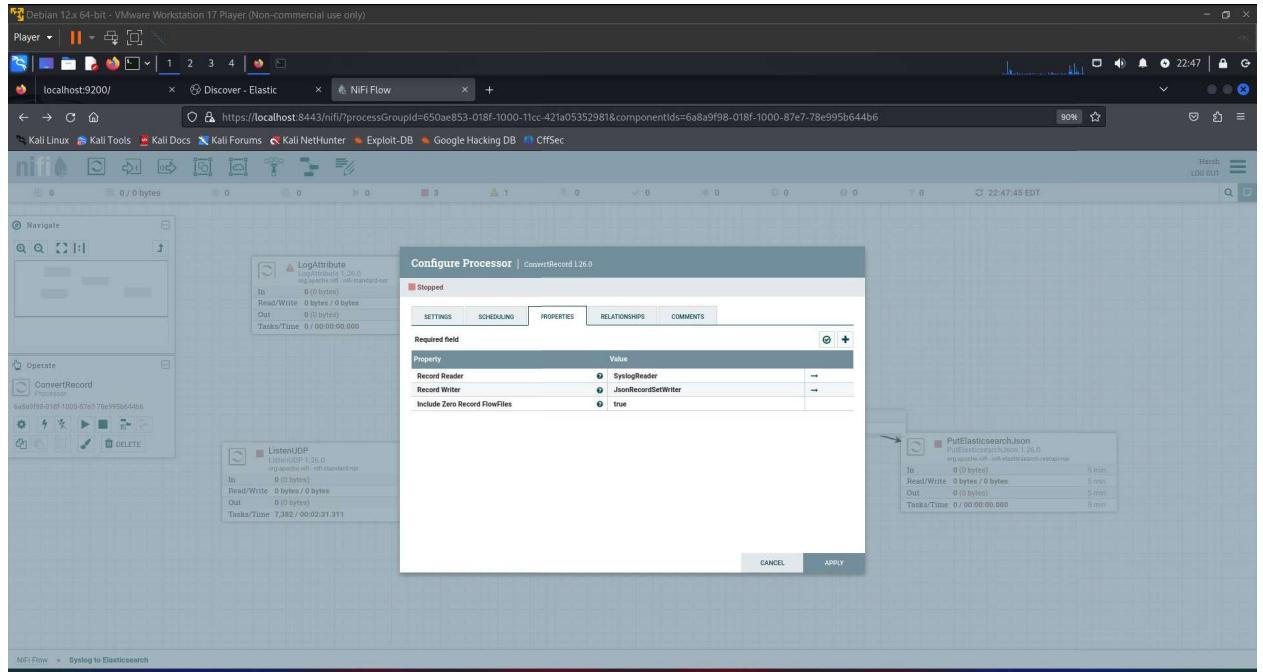
Syslog messages are generally not in JSON format, so you might want to convert them before sending to Elasticsearch:

Processor: ConvertRecord

Properties:

Record Reader: Use SyslogReader to parse syslog messages.

Record Writer: Use JsonRecordSetWriter to convert records to JSON.



3. Send Data to Elasticsearch

Finally, use the PutElasticsearchJson processor to send the formatted syslog messages to your Elasticsearch cluster:

Processor: PutElasticsearchJson

Properties:

Elasticsearch Hosts: URL of the Elasticsearch host (e.g., `http://localhost:9200`).

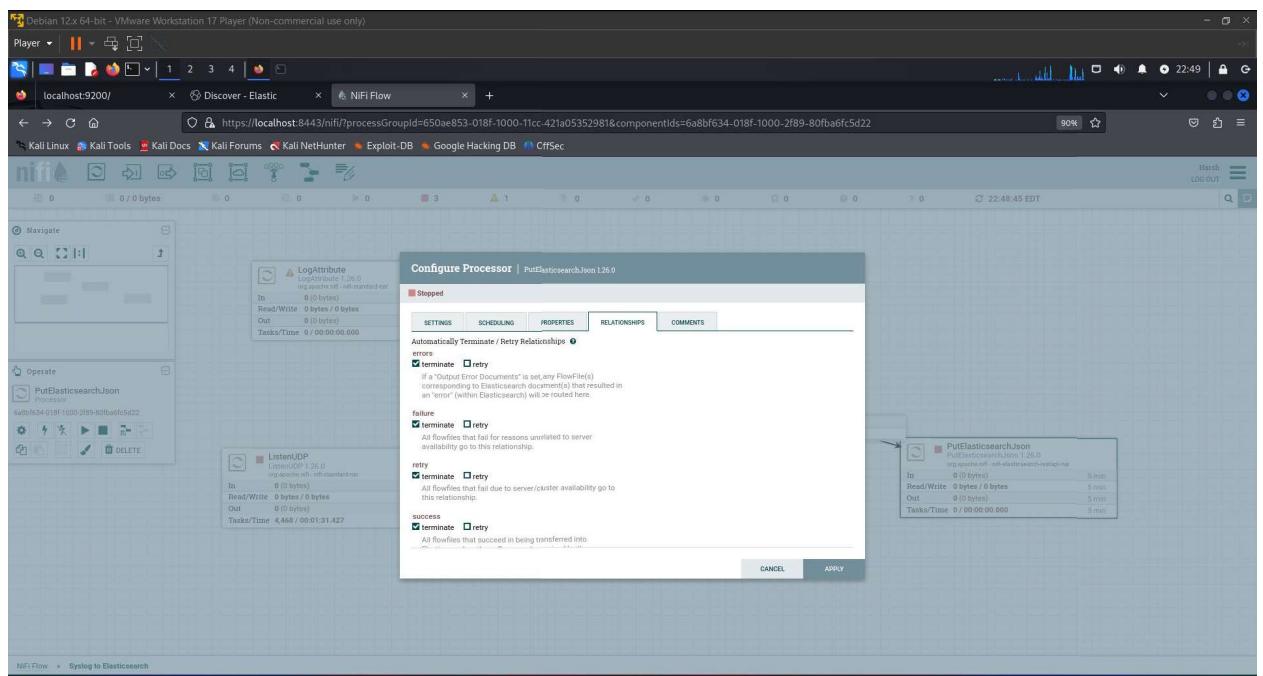
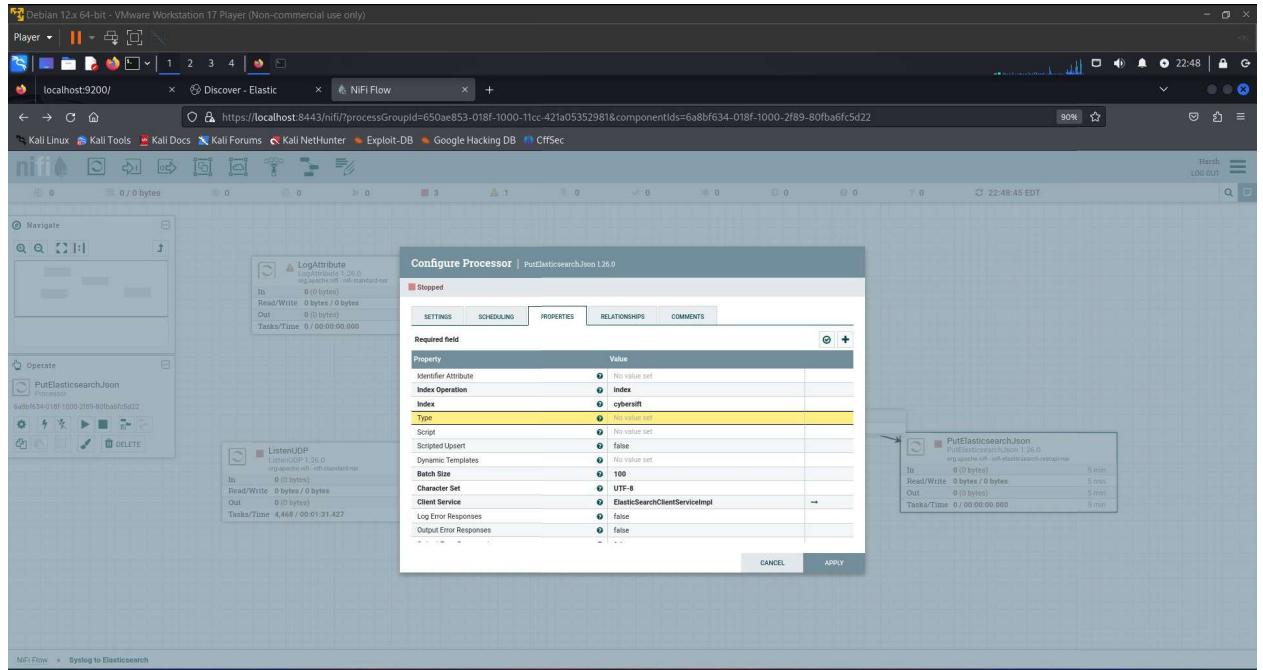
Cluster Name: Name of your Elasticsearch cluster (if applicable).

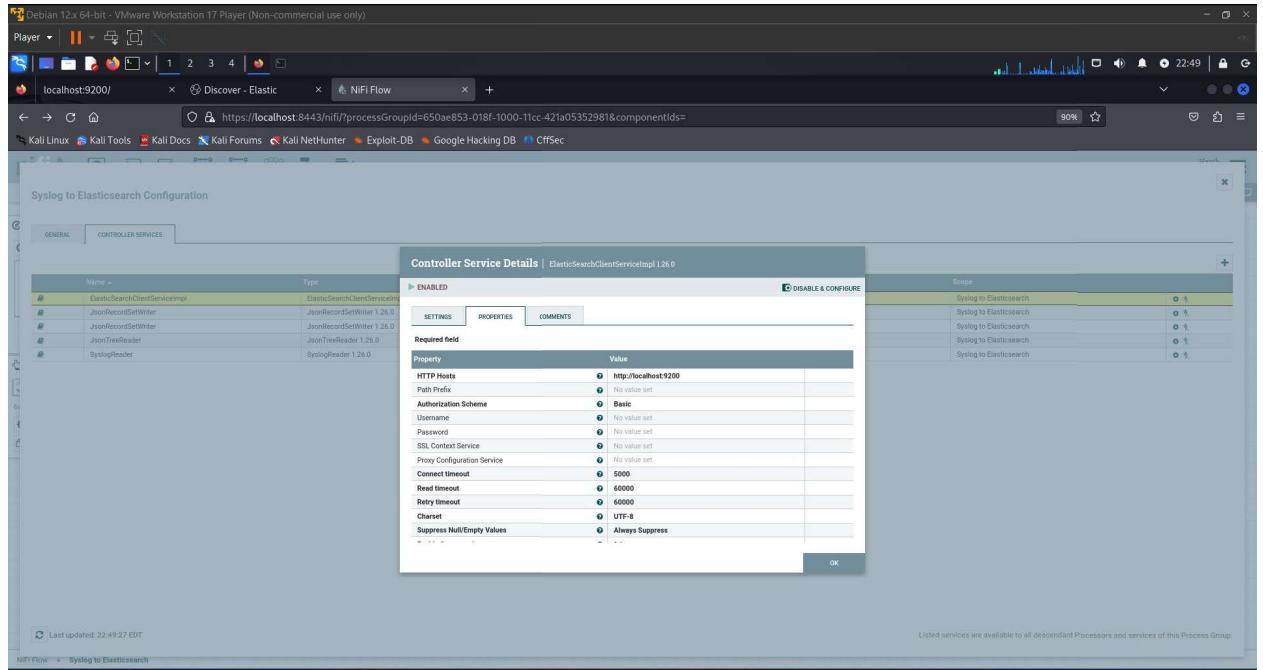
Index: The name of the Elasticsearch index where data will be stored.

Type: The type of the index (as per Elasticsearch version).

Batch Size: Number of records to send in a batch.

ID Attribute: If you want Elasticsearch to use a specific attribute from the record as the document ID.





Connecting the Processors

Connect all processors:

Connect ListenUDP to ConvertRecord with a success relationship.

Connect ConvertRecord to PutElasticsearchJson with a success relationship.

Handle failure relationships according to your error-handling strategy (e.g., connect to a LogMessage processor for debugging).

Error Handling

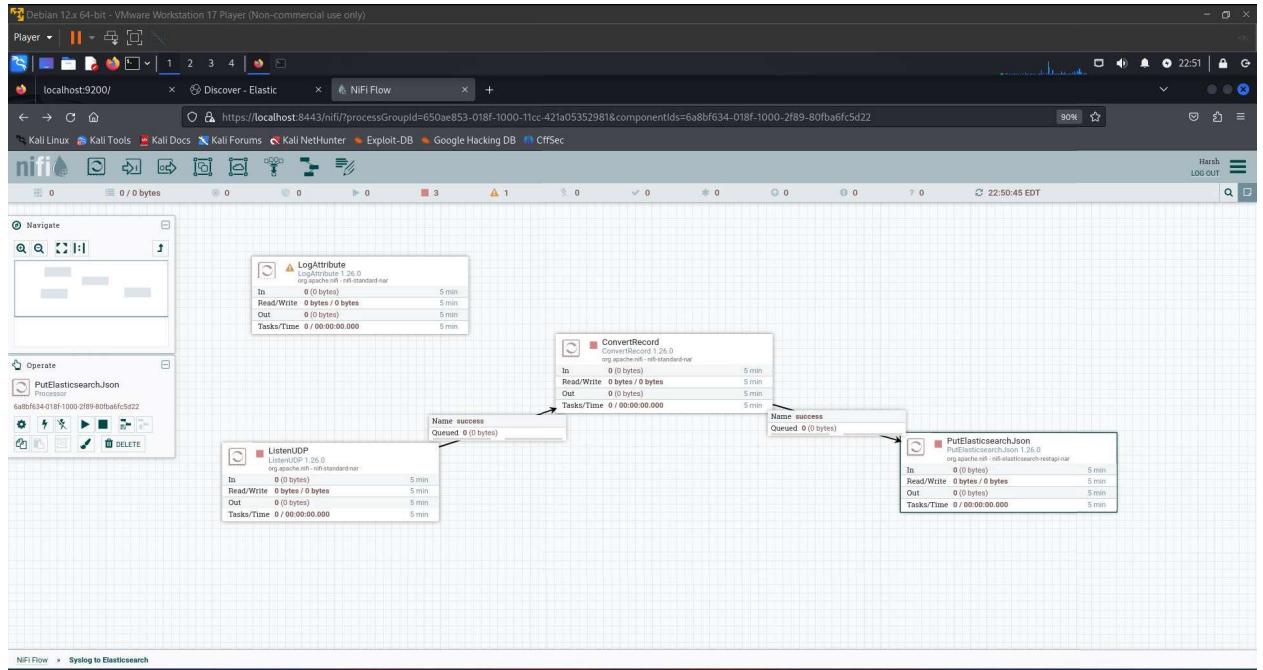
It's good practice to add processors for handling possible errors or failed processing:

Processor: PutFile or LogMessage for debugging purposes.

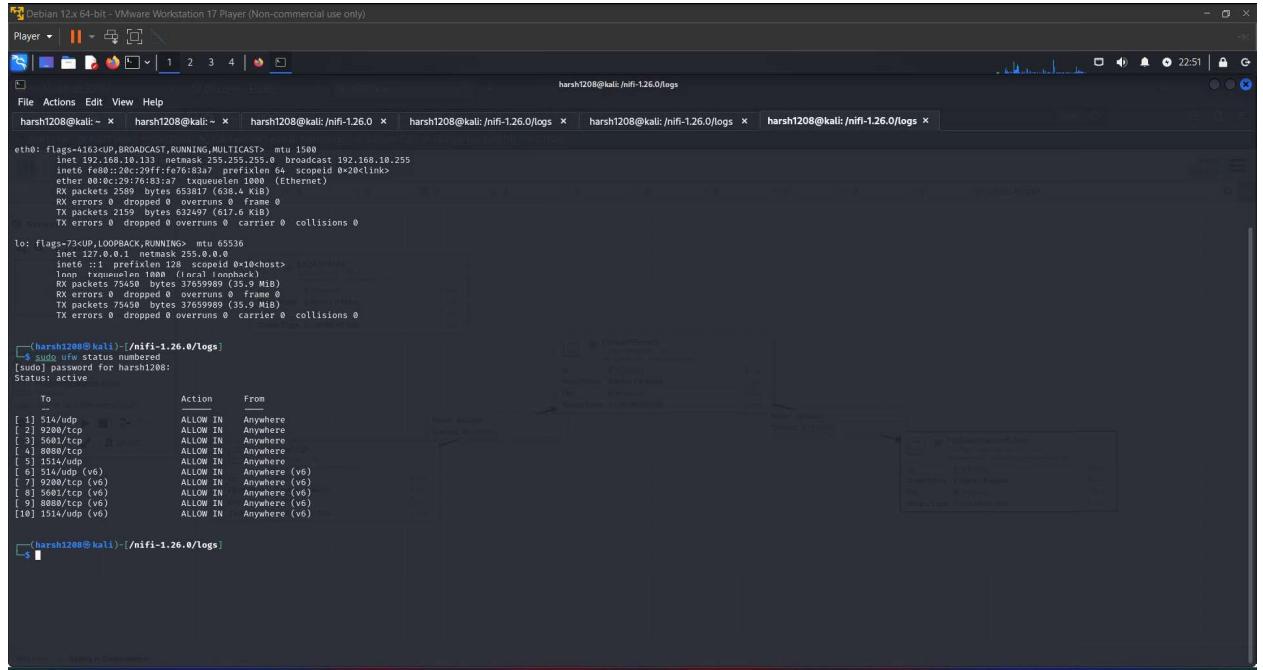
Final Steps

Start the Processors: Once all configurations are done, start all the processors.

Monitor the Flow: Use NiFi's built-in data provenance and logging to monitor the data flow and troubleshoot any issues.

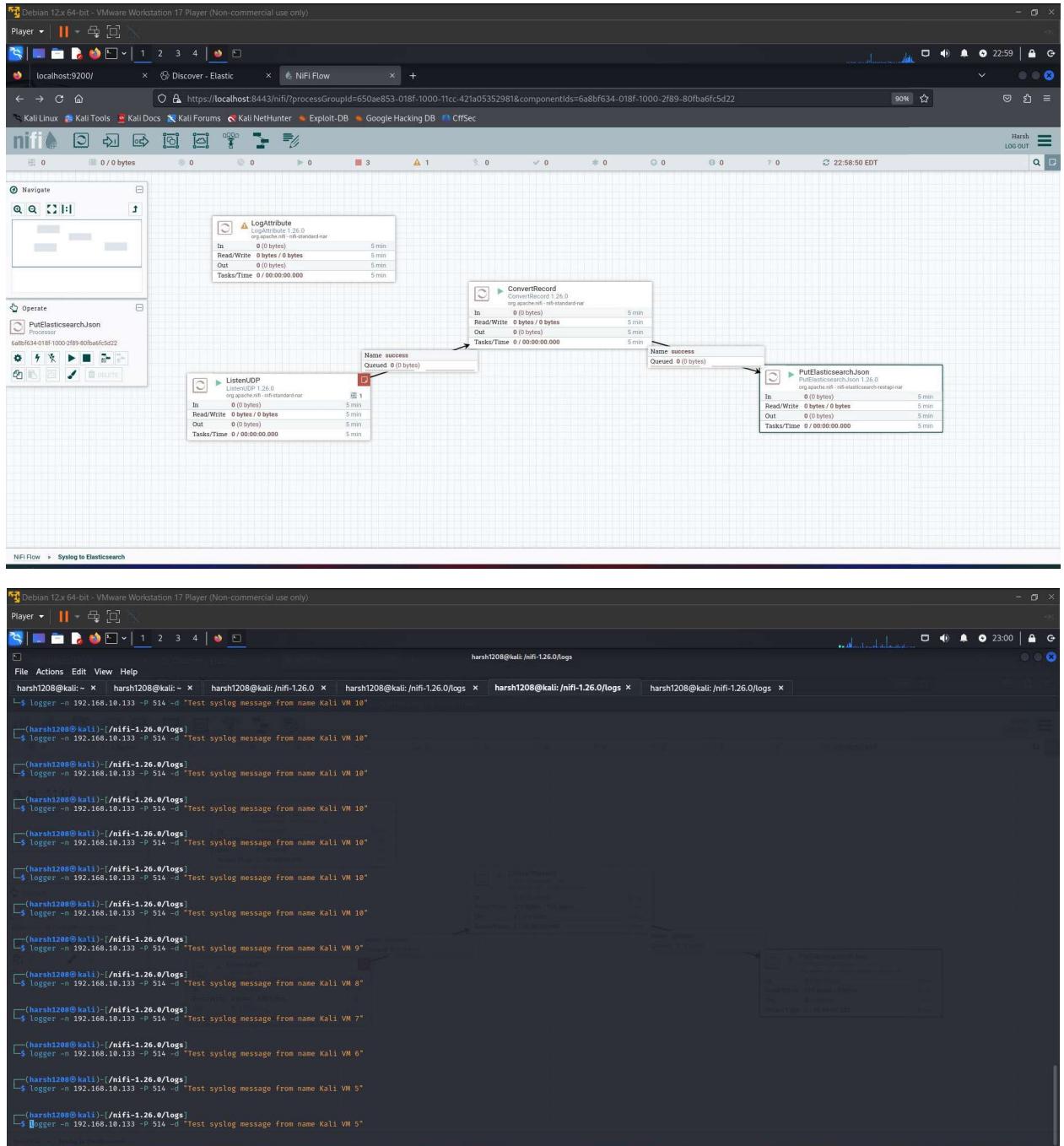


Firewall and Network Settings:



Next, Start all the Processors in NiFi and then send/generate multiple syslog messages like:

- logger -n 192.168.10.133 -P 514 -d "Test syslog message from name Kali VM"



Open logs in nifi.logs and see for any errors:

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | || | WriteAheadFlowFileRepository

File Actions Edit View Help

harsh1208@kali:~/nifi-1.26.0/logs

```
2024-05-11 22:41:40,726 INFO [pool-7-thread-1] o.a.n.c.r.WriteAheadFlowFileRepository Initiating checkpoint of Flowfile Repository
2024-05-11 22:41:40,726 INFO [pool-7-thread-1] o.a.n.c.r.WriteAheadFlowFileRepository Successfully checkpointed Flowfile Repository with 0 records in 0 milliseconds
2024-05-11 22:41:40,948 INFO [Nifi Web Server-138] o.a.n.c.s.StandardProcessScheduler Starting ListenDP[id=650a8532-018f-1000-e652-e8b0e723d6b]
2024-05-11 22:41:40,948 INFO [Nifi Web Server-138] o.a.n.c.r.StandardProcessorNode Starting ListenDP[id=650a8532-018f-1000-e652-e8b0e723d6b]
2024-05-11 22:41:40,948 INFO [Timer-Driven Process Thread-0] o.a.n.c.s.TimerDrivenSchedulingAgent Scheduled ListenDP[id=650a8532-018f-1000-e652-e8b0e723d6b] Attempted to set Socket Buffer Size to 1048576 bytes but could only set to 1029920 bytes. You may want to consider changing the Operating system's maximum receive buffer
2024-05-11 22:41:40,948 INFO [Timer-Driven Process Thread-0] o.a.n.c.s.TimerDrivenSchedulingAgent Scheduled ListenDP[id=650a8532-018f-1000-e652-e8b0e723d6b] to run with 1 threads
2024-05-11 22:41:40,971 INFO [Flow Service Tasks Thread-1] o.a.nifi.controller.StandardFlowService Saved flow controller org.apache.nifi.controller.FlowController@994ef8c // Another save pending = false
2024-05-11 22:41:40,971 INFO [Flow Service Tasks Thread-1] o.a.nifi.controller.StandardFlowService Starting Consumer[id=a68a9f98-018f-1000-e77-78e995614bc]
2024-05-11 22:41:41,045 INFO [Nifi Web Server-147] o.a.n.c.r.StandardProcessorNode Starting Consumer[id=a68a9f98-018f-1000-e77-78e995614bc]
2024-05-11 22:41:41,046 INFO [Timer-Driven Process Thread-0] o.a.n.c.s.TimerDrivenSchedulingAgent Scheduled ConvertRecord[id=6a8a9f98-018f-1000-e877-78e995614bc] with 1 threads
644be542-11-22-41:41:41,046 INFO [Flow Service Tasks Thread-1] o.a.nifi.controller.StandardFlowService Saved flow controller org.apache.nifi.controller.FlowController@994ef8c // Another save pending = false
2024-05-11 22:41:41,060 INFO [Nifi Web Server-138] o.a.n.c.s.StandardProcessScheduler Starting PutLasticsearchJson[id=6a8bf634-018f-1000-2f89-80fbaf6f5d22]
2024-05-11 22:41:41,060 INFO [Nifi Web Server-138] o.a.n.c.r.StandardProcessorNode Starting PutLasticsearchSearchJson[id=a68a9f98-018f-1000-e2f89-80fbaf6f5d22]
2024-05-11 22:41:41,062 INFO [Timer-Driven Process Thread-8] o.a.n.c.s.TimerDrivenSchedulingAgent Scheduled PutLasticsearchJson[id=6a8bf634-018f-1000-2f89-80fbaf6f5d22] with 1 threads
2024-05-11 22:41:41,062 INFO [Timer-Driven Process Thread-8] o.a.nifi.controller.StandardFlowService Saved flow controller org.apache.nifi.controller.FlowController@994ef8c // Another save pending = false
2024-05-11 22:41:41,071 INFO [Flow Service Tasks Thread-2] o.a.nifi.controller.StandardFlowService Saved flow controller org.apache.nifi.controller.FlowController@994ef8c // Another save pending = false
2024-05-11 22:41:41,071 INFO [Flow Service Tasks Thread-2] o.a.n.c.r.WriteAheadFlowFileRepository Initiating checkpoint of Flowfile Repository
2024-05-11 22:41:40,975 INFO [pool-7-thread-1] o.a.n.c.r.SequentialAccessWriteAheadLog Checkpointed Write-Ahead Log with 0 Records and 0 Swap Files in 4 milliseconds (Stop-the-world time = 0 milliseconds), max Transaction ID 319
2024-05-11 22:41:40,975 INFO [pool-7-thread-1] o.a.n.c.r.SequentialAccessWriteAheadLog Checkpointed Write-Ahead Log with 0 Records and 0 Swap Files in 4 milliseconds (Stop-the-world time = 0 milliseconds), max Transaction ID 319
2024-05-11 22:42:02,471 INFO [Write-Ahead Local State Provider Maintenance] org.wali.MinimalLockingWriteAheadLog.org.wali.MinimalLockingWriteAheadLog@524945e2 checkpointed with 9 Records and 0 Swap Files in 17 milliseconds (Stop-the-world time = 4 milliseconds), Clear Edit Logs time = 5 millis
2024-05-11 22:42:02,471 INFO [Write-Ahead Local State Provider Maintenance] org.wali.MinimalLockingWriteAheadLog.org.wali.MinimalLockingWriteAheadLog@524945e2 checkpointed with 9 Records and 0 Swap Files in 17 milliseconds (Stop-the-world time = 4 milliseconds), Clear Edit Logs time = 5 millis
2024-05-11 22:42:02,981 INFO [Cleanup Archive for default] o.a.n.c.repository.FileSystemRepository Successfully deleted 0 files (0 bytes) from archive
2024-05-11 22:42:02,981 INFO [Cleanup Archive for default] o.a.n.c.repository.FileSystemRepository Archive cleanup completed for container default; will now allow writing to this container.
Bytes used = 23.44 GB, bytes free = 14.7 GB, capacity = 38.14 GB
```

(harsh1208@kali:~/nifi-1.26.0/logs)

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Player | || | WriteAheadFlowFileRepository

File Actions Edit View Help

localhost:9200

Discover - Elasticsearch

Nifi Flow

```
https://localhost:8443/nifi/processGroupID=650a853-018f-1000-2f89-80fbaf6f5d22
```

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB Cffsec

Harsh LOG OUT

23:00:51 EDT

NIFI Flow

Syslog to Elasticsearch

Open Kibana interface for data logs review.

The screenshot shows the Elasticsearch interface with the URL `localhost:9200/_search`. The search query is `from cybersift`. The results table has 18 rows. The first row is expanded, showing the following JSON data:

```
body: "harsh1288 - [timeQuality tzKnown='1' isSynced='1' syncAccuracy='938508'] Test syslog # message from name Kali VM 9",  
body.keyword: "harsh1288 - [timeQuality tzKnown='1' isSynced='1' syncAccuracy='938508'] Test syslog # message from name Kali VM 9",  
facility: 1,  
facility.keyword: 1,  
hostname: "kali",  
hostname.keyword: "kali",  
priority: 13,  
priority.keyword: 13,  
severity: 5,  
severity.keyword: 5,  
timestamp: "2024-05-12T02:59:44.964Z",  
version: 1,  
version.keyword: 1
```

This screenshot shows a detailed view of the first search result from the previous interface. The result is displayed as a table with two columns: **Actions** and **Field**. The **Actions** column contains checkboxes, and the **Field** column contains the field names and their corresponding values.

Actions	Field
<input type="checkbox"/>	body
<input type="checkbox"/>	body.keyword
<input type="checkbox"/>	facility
<input type="checkbox"/>	facility.keyword
<input type="checkbox"/>	hostname
<input type="checkbox"/>	hostname.keyword
<input type="checkbox"/>	priority
<input type="checkbox"/>	priority.keyword
<input type="checkbox"/>	severity
<input type="checkbox"/>	severity.keyword
<input type="checkbox"/>	timestamp
<input type="checkbox"/>	version
<input type="checkbox"/>	version.keyword

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Discover - Elastic

localhost:9200/_app/discover#/?_a=[columns:l(),filters:l(),index:e0f827d4ae70e29246fb647b62b8fc01802a5efdb3fb53a03527ae3f0af72,interval:auto,query:{esql:'from cybersift'},sort:l(),90%]

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB CtfSec

elastic

Discover

ES|SQL from cybersift

18 results

Document

Available fields:

- body
- body.keyword
- facility
- facility.keyword
- hostname
- hostname.keyword
- priority
- priority.keyword
- severity
- severity.keyword
- timestamp
- version
- version.keyword

ES|SQL is currently in technical preview. Find more information in the documentation.

Table JSON

Search field names

Actions	Field	Value
<input type="checkbox"/>	body	harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="932500"] Test syslog message from name Kali VM 8
<input type="checkbox"/>	body.keyword	harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="932500"] Test syslog message from name Kali VM 8
<input type="checkbox"/>	facility	1
<input type="checkbox"/>	facility.keyword	1
<input type="checkbox"/>	hostname	kali
<input type="checkbox"/>	hostname.keyword	kali
<input type="checkbox"/>	priority	13
<input type="checkbox"/>	priority.keyword	13
<input type="checkbox"/>	severity	5
<input type="checkbox"/>	severity.keyword	5
<input type="checkbox"/>	timestamp	2024-05-12T02:59:48.891Z
<input type="checkbox"/>	version	1
<input type="checkbox"/>	version.keyword	1

Rows per page: 25 < 1 >

Debian 12.x 64-bit - VMware Workstation 17 Player (Non-commercial use only)

Discover - Elastic

localhost:9200/_app/discover#/?_a=[columns:l(),filters:l(),index:e0f827d4ae70e29246fb647b62b8fc01802a5efdb3fb53a03527ae3f0af72,interval:auto,query:{esql:'from cybersift'},limit:1,80%,

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB CtfSec

elastic

Discover

ES|SQL from cybersift | limit 10

10 results

Document

Available fields:

- body
- body.keyword
- facility
- facility.keyword
- hostname
- hostname.keyword
- priority
- priority.keyword
- severity
- severity.keyword
- timestamp
- version
- version.keyword

ES|SQL is currently in technical preview. Find more information in the documentation.

Time All time Refresh

Actions	Field	Value
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="392500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:40.455 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="393500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:49.907 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="393500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:50.858 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="394000"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:51.819 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="394500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:52.648 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="395500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:54.021 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="395500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:54.992 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="396500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:56.398 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="397000"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:57.087 version 1
<input type="checkbox"/>	body	body harsh1288 - [timeQuality tzKnown="1" isSynced="1" syncAccuracy="397500"] Test syslog message from name Kali VM 10 facility 1 hostname kali priority 13 severity 5 timestamp May 11, 2024 0:22:41:58.026 version 1

