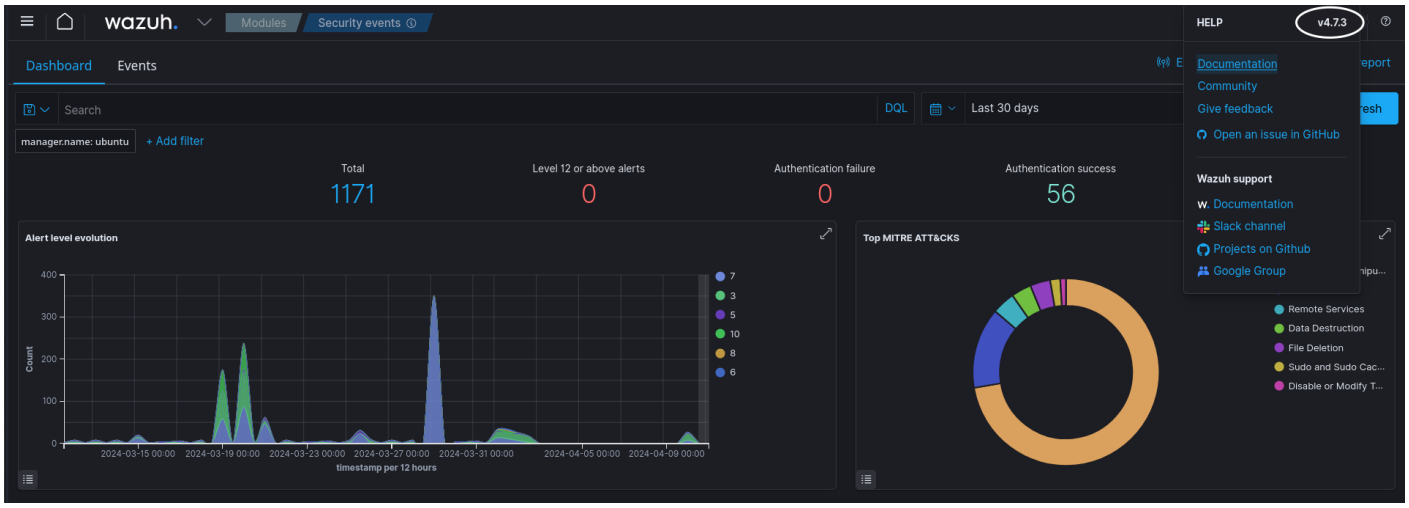
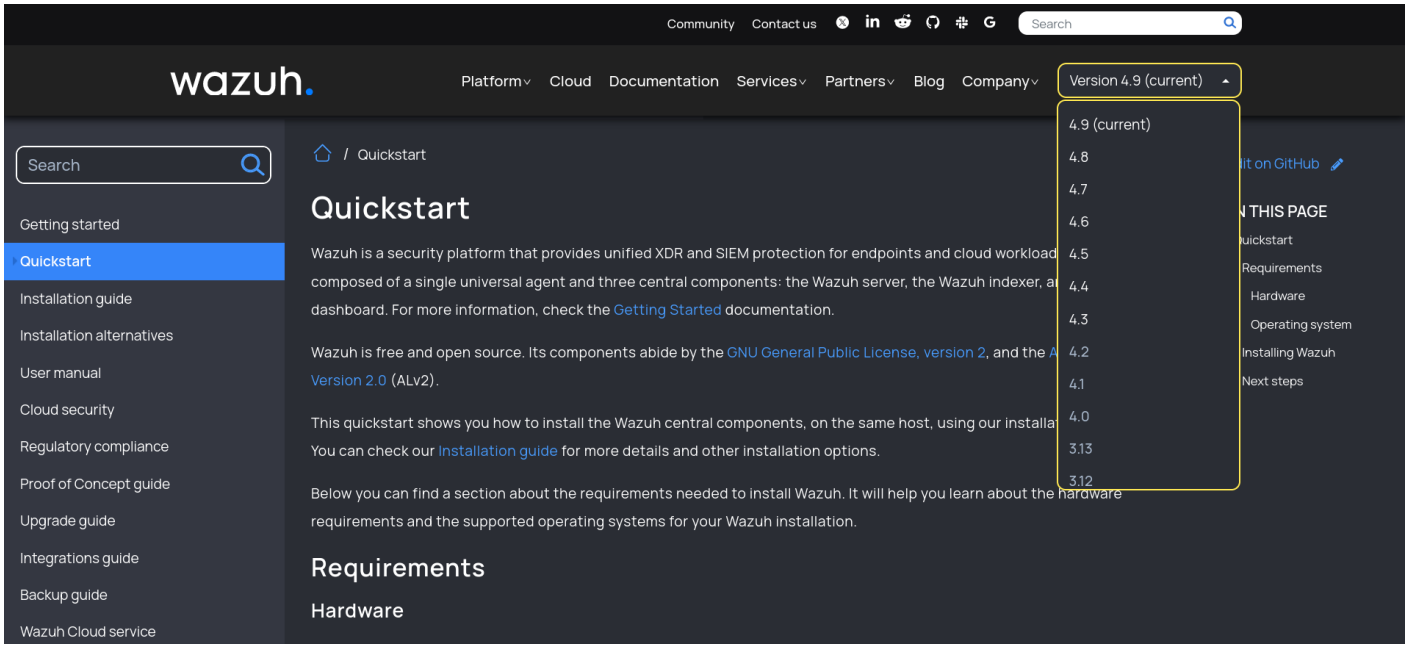
Actualización Wazuh Manager

Para realizar la actualización del servidor de Wazuh procedemos a identificar la versión que tenemos. Se puede identificar desde el Dashboard haciendo clic en la parte superior derecha. Identificamos que tenemos la versión v 4.7.3.



En la página oficial de Wazuh se encuentra la documentación donde nos indican cuál es la versión actual en la esquina superior derecha, por lo que procedemos a verificar la última versión.



Se deben verificar las características de hardware necesarias para que no se tengan problemas de espacio en disco y cantidad de memoria RAM requerida.

Como los servicios de Indexador, Dashboard y Manager de Wazuh se encuentran en el mismo equipo, poseen la misma dirección IP y no se tiene configuración de cluster, se procede a detener estos servicios de Wazuh, con la respectiva verificación.

```
sudo systemctl stop wazuh-manager
sudo systemctl stop wazuh-dashboard
sudo systemctl stop wazuh-indexer
```

```
sudo systemctl status wazuh-manager
```

```
○ wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: inactive (dead) since Tue 2024-04-02 17:12:49 -04; 22s ago
    Process: 403935 ExecStop=/usr/bin/env /var/ossec/bin/wazuh-control stop (code=exited, status=0/SUCCESS)
        CPU: 16h 6min 36.683s

abr 02 17:12:47 ubuntu env[403935]: Killing wazuh-authd...
abr 02 17:12:48 ubuntu env[403935]: wazuh-agentlessd not running...
abr 02 17:12:48 ubuntu env[403935]: Killing wazuh-integratord...
abr 02 17:12:48 ubuntu env[403935]: wazuh-dbd not running...
abr 02 17:12:48 ubuntu env[403935]: wazuh-csyslogd not running...
abr 02 17:12:48 ubuntu env[403935]: Killing wazuh-apid...
abr 02 17:12:49 ubuntu env[403935]: Wazuh v4.5.1 Stopped
abr 02 17:12:49 ubuntu systemd[1]: wazuh-manager.service: Deactivated successfully.
abr 02 17:12:49 ubuntu systemd[1]: Stopped Wazuh manager.
abr 02 17:12:49 ubuntu systemd[1]: wazuh-manager.service: Consumed 16h 6min 36.683s CPU time.
```

```
sudo systemctl status wazuh-dashboard
```

```
○ wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
     Active: inactive (dead) since Tue 2024-04-02 17:12:41 -04; 2min 1s ago
    Process: 678 ExecStart=/usr/share/wazuh-dashboard/bin/opensearch-dashboards -c /etc/wazuh-dashboard/opensearch_dashboards.yml (code=exited, status=0/SUCCESS)
   Main PID: 678 (code=exited, status=0/SUCCESS)
        CPU: 32min 42.884s

abr 02 17:06:00 ubuntu opensearch-dashboards[678]: {"type":"response","@timestamp":"2024-04-02T21:06:00Z","tags":[],"pid":678,"method":"get","statusCode":200,"req":{"url":"/45103/bundles/plugin/visTypeVislib/visTypeV
abr 02 17:06:00 ubuntu opensearch-dashboards[678]: {"type":"response","@timestamp":"2024-04-02T21:06:00Z","tags":[],"pid":678,"method":"post","statusCode":200,"req":{"url":"/elastic/alerts","method":"post","headers":
abr 02 17:06:00 ubuntu opensearch-dashboards[678]: {"type":"response","@timestamp":"2024-04-02T21:06:00Z","tags":[],"pid":678,"method":"post","statusCode":200,"req":{"url":"/elastic/alerts","method":"post","headers":
abr 02 17:06:00 ubuntu opensearch-dashboards[678]: {"type":"response","@timestamp":"2024-04-02T21:06:00Z","tags":[],"pid":678,"method":"post","statusCode":200,"req":{"url":"/elastic/alerts","method":"post","headers":
abr 02 17:06:00 ubuntu opensearch-dashboards[678]: {"type":"response","@timestamp":"2024-04-02T21:06:00Z","tags":[],"pid":678,"method":"post","statusCode":200,"req":{"url":"/elastic/alerts","method":"post","headers":
abr 02 17:12:41 ubuntu systemd[1]: Stopping wazuh-dashboard...
abr 02 17:12:41 ubuntu opensearch-dashboards[678]: {"type":"log","@timestamp":"2024-04-02T21:12:41Z","tags":["info","plugins-system"],"pid":678,"message":"Stopping all plugins."}
abr 02 17:12:41 ubuntu systemd[1]: wazuh-dashboard.service: Deactivated successfully.
abr 02 17:12:41 ubuntu systemd[1]: Stopped wazuh-dashboard.
abr 02 17:12:41 ubuntu systemd[1]: wazuh-dashboard.service: Consumed 32min 42.884s CPU time.
```

```
sudo systemctl status wazuh-indexer
```

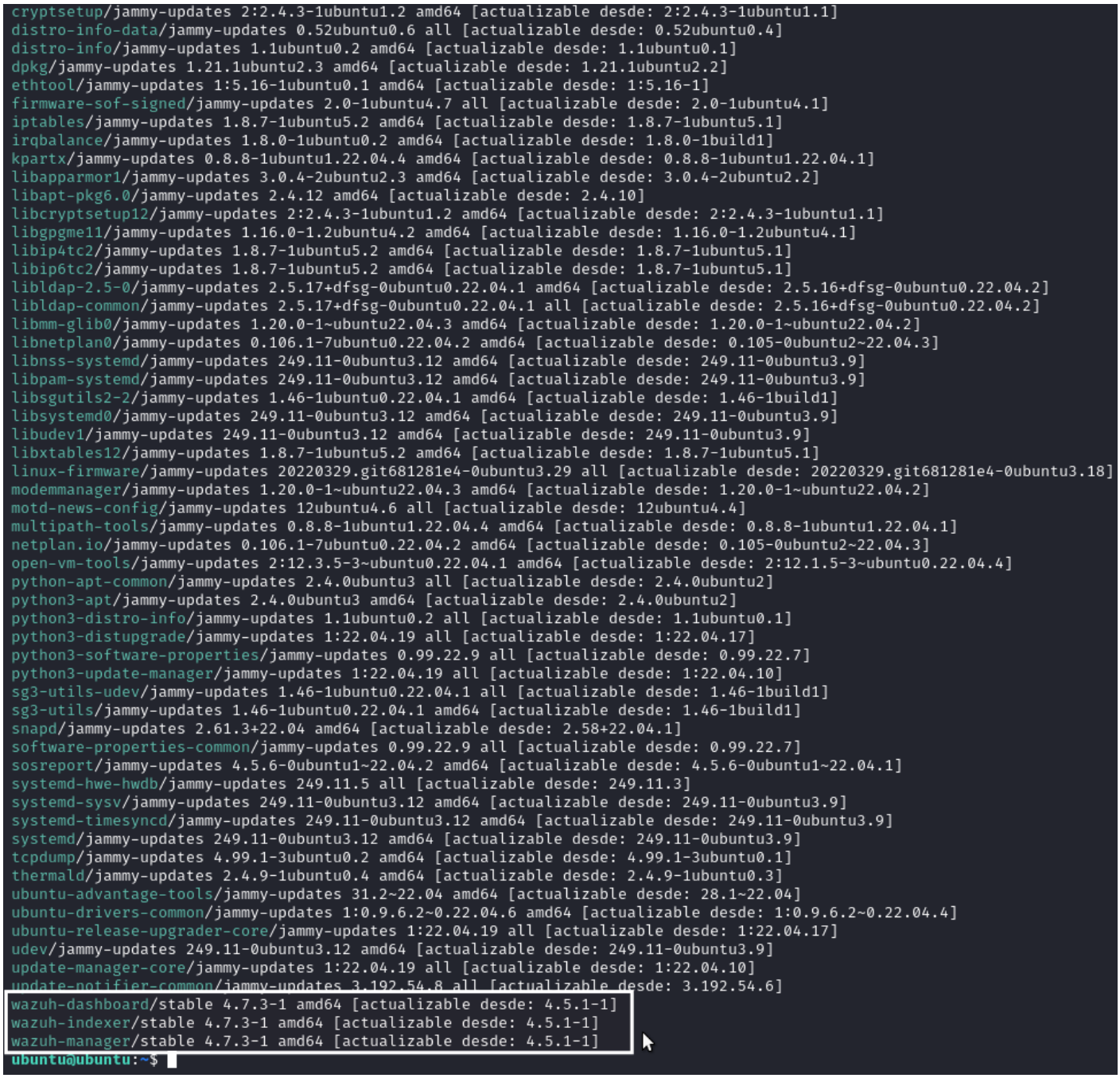
```
○ wazuh-indexer.service - Wazuh-indexer
     Loaded: loaded (/lib/systemd/system/wazuh-indexer.service; enabled; vendor preset: enabled)
     Active: inactive (dead) since Tue 2024-04-02 17:12:50 -04; 2min 35s ago
       Docs: https://documentation.wazuh.com
    Process: 679 ExecStart=/usr/share/wazuh-indexer/bin/systemd-entrypoint -p ${PID_DIR}/wazuh-indexer.pid --quiet (code=exited, status=143)
   Main PID: 679 (code=exited, status=143)
        CPU: 6h 34min 8.220s

abr 02 00:00:00 ubuntu systemd-entrypoint[679]:         at org.opensearch.common.util.concurrent.ThreadContext$ContextPreservingRunnable.run(ThreadContext.java:747)
abr 02 00:00:00 ubuntu systemd-entrypoint[679]:         at org.opensearch.common.util.concurrent.PrioritizedOpenSearchThreadPoolExecutor$TieBreakingPrioritizedRunnable.runAndClean(PrioritizedOpenSearchThreadPoolExecutor.java:282)
abr 02 00:00:00 ubuntu systemd-entrypoint[679]:         at org.opensearch.common.util.concurrent.PrioritizedOpenSearchThreadPoolExecutor$TieBreakingPrioritizedRunnable.run(PrioritizedOpenSearchThreadPoolExecutor.java:245)
abr 02 00:00:00 ubuntu systemd-entrypoint[679]:         at java.base/java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1136)
abr 02 00:00:00 ubuntu systemd-entrypoint[679]:         at java.base/java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:635)
abr 02 00:00:00 ubuntu systemd-entrypoint[679]:         at java.base/java.lang.Thread.run(Thread.java:833)
abr 02 17:12:49 ubuntu systemd[1]: Stopping Wazuh-indexer...
abr 02 17:12:50 ubuntu systemd[1]: wazuh-indexer.service: Deactivated successfully.
abr 02 17:12:50 ubuntu systemd[1]: Stopped Wazuh-indexer.
abr 02 17:12:50 ubuntu systemd[1]: wazuh-indexer.service: Consumed 6h 34min 8.220s CPU time.
```

Posteriormente realizamos una actualización de los repositorios.

```
sudo apt-get update
```

Listamos los paquetes que pueden actualizarse para encontrar wazuh-dashboard, wazuh-indexer y wazuh-manager en la lista.

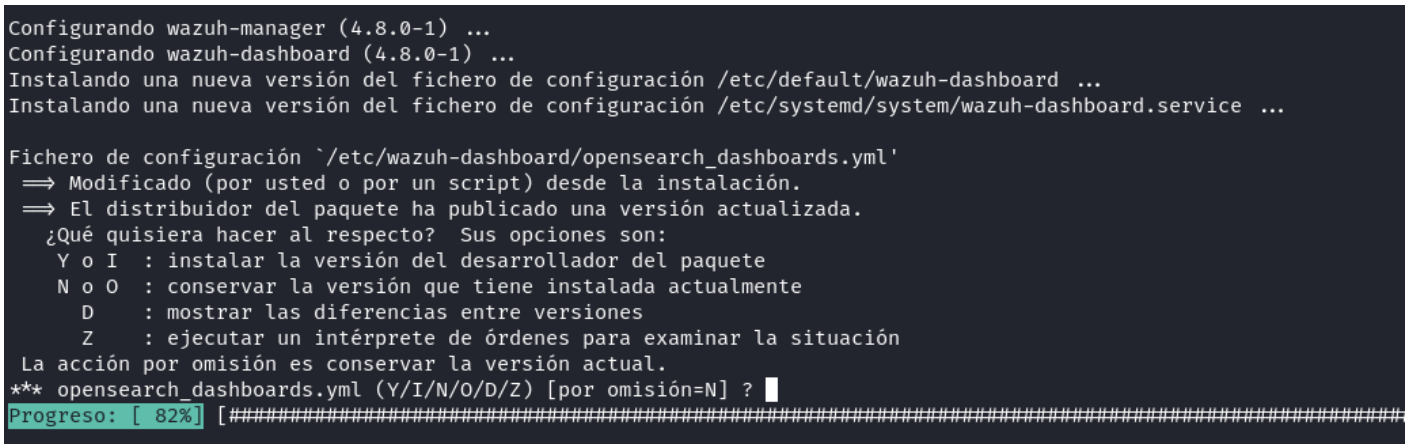
```
sudo apt list --upgradable
```



Por ultimo realizamos la actualización de paquetes con el comando upgrade.

```
sudo apt upgrade
```

Durante la actualización de los componentes del sistema, se nos proporciona la opción de reemplazar archivos en la funcionalidad del dashboard con la siguiente consulta, en la cual debemos seleccionar la opción "D" para revisar los cambios implementados en los archivos de configuración.



Fichero de configuración /etc/wazuh-dashboard/opensearch_dashboards.yml'

==> Modificado (por usted o por un script) desde la instalación.

==> El distribuidor del paquete ha publicado una versión actualizada.

¿Qué quisiera hacer al respecto? Sus opciones son:

Y o I : instalar la versión del desarrollador del paquete

N o O : conservar la versión que tiene instalada actualmente

D : mostrar las diferencias entre versiones

Z : ejecutar un intérprete de órdenes para examinar la situación

La acción por omisión es conservar la versión actual.

*** opensearch_dashboards.yml (Y/I/N/O/D/Z) [por omisión=N] ? D

--- /etc/wazuh-dashboard/opensearch_dashboards.yml 2024-08-01 20:39:58.576766390 +0000

+++ /etc/wazuh-dashboard/opensearch_dashboards.yml.dpkg-new 2023-05-05 12:31:50.000000000 +0000

@@ -1,15 +1,14 @@

server.host: 0.0.0.0

-opensearch.hosts: https://127.0.0.1:9200

server.port: 443

+opensearch.hosts: https://localhost:9200

opensearch.ssl.verificationMode: certificate

-# opensearch.username: kibanaserver

-# opensearch.password: kibanaserver

+#opensearch.username:

+#opensearch.password:

opensearch.requestHeadersAllowlist: ["securitytenant","Authorization"]

opensearch_security.multitenancy.enabled: false

```
 opensearch_security.readonly_mode.roles: ["kibana_read_only"]
 server.ssl.enabled: true
-server.ssl.key: "/etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem"
-server.ssl.certificate: "/etc/wazuh-dashboard/certs/wazuh-dashboard.pem"
+server.ssl.key: "/etc/wazuh-dashboard/certs/dashboard-key.pem"
+server.ssl.certificate: "/etc/wazuh-dashboard/certs/dashboard.pem"
 opensearch.ssl.certificateAuthorities: ["/etc/wazuh-dashboard/certs/root-ca.pem"]
-uiSettings.overrides.defaultRoute: /app/wazuh
-opensearch_security.cookie.secure: true
+uiSettings.overrides.defaultRoute: /app/wz-home
```

El mismo caso se presenta multiples veces en la instalación de Wazuh Indexer por lo que seleccionamos la misma opción "D" para revisar los cambios que se realizan en nuestros archivos de configuración:

```
--- /etc/init.d/wazuh-indexer   1970-01-01 00:00:00.000000000 +0000
+++ /etc/init.d/wazuh-indexer.dpkg-new  2024-08-30 10:12:22.000000000 +0000
@@ -0,0 +1,168 @@
+#!/usr/bin/env bash
+#
+# /etc/init.d/wazuh-indexer -- startup script for Wazuh indexer
+#
+### BEGIN INIT INFO
+# Provides:          wazuh-indexer
+# Required-Start:    $network $remote_fs $named
+# Required-Stop:     $network $remote_fs $named
+# Default-Start:     2 3 4 5
+# Default-Stop:      0 1 6
+# Short-Description: Starts wazuh-indexer
+# Description:       Starts wazuh-indexer using start-stop-daemon
+### END INIT INFO
+set -e -o pipefail
+PATH=/bin:/usr/bin:/sbin:/usr/sbin
+NAME=wazuh-indexer
+DESC=$NAME
+DEFAULT=/etc/default/$NAME
+
+if [ `id -u` -ne 0 ]; then
```

```
+       echo "You need root privileges to run this script"
+       exit 1
+fi
+
+. /lib/lsb/init-functions
+
+if [ -r /etc/default/rcS ]; then
+       . /etc/default/rcS
+fi
+
+# The following variables can be overwritten in $DEFAULT
+
+# Directory where the OpenSearch binary distribution resides
+OPENSEARCH_HOME=/usr/share/$NAME
+
+# Additional Java OPTS
+#OPENSEARCH_JAVA_OPTS=
+
+# Maximum number of open files
+MAX_OPEN_FILES=65535
+
+# Maximum amount of locked memory
+#MAX_LOCKED_MEMORY=
+
+# OpenSearch configuration directory
+OPENSEARCH_PATH_CONF=/etc/$NAME
+
+# Maximum number of VMA (Virtual Memory Areas) a process can own
+MAX_MAP_COUNT=262144
+
+# OpenSearch PID file directory
+PID_DIR="/var/run/$NAME"
+
+# End of variables that can be overwritten in $DEFAULT
+
+# overwrite settings from default file
+if [ -f "$DEFAULT" ]; then
```

```
+       . "$DEFAULT"
+fi
+
+# Define other required variables
+PID_FILE="$PID_DIR/$NAME.pid"
+DAEMON=$OPENSEARCH_HOME/bin/opensearch
+DAEMON_OPTS="-d -p $PID_FILE"
+
+export OPENSEARCH_JAVA_OPTS
+export OPENSEARCH_PATH_CONF
+export JAVA_HOME
+export OPENSEARCH_JAVA_HOME
+
+if [ ! -x "$DAEMON" ]; then
+       echo "The wazuh-indexer startup script does not exists or it is not executable, tried: $DAEMON"
+       exit 1
+fi
+
+case "$1" in
+  start)
+
+       log_daemon_msg "Starting $DESC"
+
+       pid=`pidofproc -p $PID_FILE wazuh-indexer`
+       if [ -n "$pid" ] ; then
+               log_begin_msg "Already running."
+               log_end_msg 0
+               exit 0
+       fi
+
+       # Ensure that the PID_DIR exists (it is cleaned at OS startup time)
+       if [ -n "$PID_DIR" ] && [ ! -e "$PID_DIR" ]; then
+               mkdir -p "$PID_DIR" && chown wazuh-indexer:wazuh-indexer "$PID_DIR"
+       fi
+       if [ -n "$PID_FILE" ] && [ ! -e "$PID_FILE" ]; then
+               touch "$PID_FILE" && chown wazuh-indexer:wazuh-indexer "$PID_FILE"
+       fi
```

```
+
+       if [ -n "$MAX_OPEN_FILES" ]; then
+               ulimit -n $MAX_OPEN_FILES
+       fi
+
+       if [ -n "$MAX_LOCKED_MEMORY" ]; then
+               ulimit -l $MAX_LOCKED_MEMORY
+       fi
+
+       if [ -n "$MAX_MAP_COUNT" -a -f /proc/sys/vm/max_map_count ] && [ "$MAX_MAP_COUNT" -gt $(cat
/proc/sys/vm/m>
+               sysctl -q -w vm.max_map_count=$MAX_MAP_COUNT
+       fi
+
+       # Start Daemon
+       start-stop-daemon -d $OPENSEARCH_HOME --start --user wazuh-indexer -c wazuh-indexer --pidfile "$PID_FILE"
>
+       return=$?
+       if [ $return -eq 0 ]; then
+               i=0
+               timeout=10
+               # Wait for the process to be properly started before exiting
+               until { kill -0 `cat "$PID_FILE"`; } >/dev/null 2>&1
+               do
+                       sleep 1
+                       i=$(($i + 1))
+                       if [ $i -gt $timeout ]; then
+                               log_end_msg 1
+                               exit 1
+                       fi
+               done
+       fi
+       log_end_msg $return
+       exit $return
+       ;;
+  stop)
+       log_daemon_msg "Stopping $DESC"
```

```
+
+      if [ -f "$PID_FILE" ]; then
+              start-stop-daemon --stop --pidfile "$PID_FILE" \
+                      --user wazuh-indexer \
+                      --quiet \
+                      --retry forever/TERM/20 > /dev/null
+              if [ $? -eq 1 ]; then
+                      log_progress_msg "$DESC is not running but pid file exists, cleaning up"
+              elif [ $? -eq 3 ]; then
+                      PID="`cat $PID_FILE`"
+                      log_failure_msg "Failed to stop $DESC (pid $PID)"
+                      exit 1
+              fi
+              rm -f "$PID_FILE"
+      else
+              log_progress_msg "(not running)"
+      fi
+      log_end_msg 0
+      ;;
+  status)
+      status_of_proc -p $PID_FILE wazuh-indexer wazuh-indexer && exit 0 || exit $?
+      ;;
+  restart|force-reload)
+      if [ -f "$PID_FILE" ]; then
+              $0 stop
+      fi
+      $0 start
+      ;;
+  *)
+      log_success_msg "Usage: $0 {start|stop|restart|force-reload|status}"
+      exit 1
+      ;;
+esac
+
+exit 0
```

```
--- /etc/wazuh-indexer/jvm.options      2024-08-01 20:37:13.516578584 +0000
+++ /etc/wazuh-indexer/jvm.options.dpkg-new     2024-08-30 10:14:23.000000000 +0000
@@ -19,8 +19,8 @@
 # Xms represents the initial size of total heap space
 # Xmx represents the maximum size of total heap space

--Xms1955m
--Xmx1955m
+-Xms1g
+-Xmx1g

 ################################################################
 ## Expert settings
@@ -79,13 +79,15 @@
 # Explicitly allow security manager (https://bugs.openjdk.java.net/browse/JDK-8270380)
 18-:-Djava.security.manager=allow

+# JDK 20+ Incubating Vector Module for SIMD optimizations;
+# disabling may reduce performance on vector optimized lucene
+20:--add-modules=jdk.incubator.vector
+
+# HDFS ForkJoinPool.common() support by SecurityManager
+-
Djava.util.concurrent.ForkJoinPool.common.threadFactory=org.opensearch.secure_sm.SecuredForkJoinWorkerThrea
dFact>
+
 ## OpenSearch Performance Analyzer
 -Dclk.tck=100
 -Djdk.attach.allowAttachSelf=true
 -Djava.security.policy=file:///etc/wazuh-indexer/opensearch-performance-analyzer/opensearch_security.policy
---add-opens=jdk.attach/sun.tools.attach=ALL-UNNAMED
-
-## OpenDistro Performance Analyzer
--Dclk.tck=100
--Djdk.attach.allowAttachSelf=true
--Djava.security.policy=file:///usr/share/wazuh-indexer/plugins/opendistro-performance-
analyzer/pa_config/es_secur>
```

```
+--add-opens=jdk.attach/sun.tools.attach=ALL-UNNAMED
\ No newline at end of file
```

```
--- /etc/wazuh-indexer/opensearch-security/internal_users.yml   2024-08-01 20:40:06.324974273 +0000
+++ /etc/wazuh-indexer/opensearch-security/internal_users.yml.dpkg-new  2024-08-30 10:14:23.000000000 +0000
@@ -1,19 +1,36 @@
 ---
+# This is the internal user database
+# The hash value is a bcrypt hash and can be generated with plugin/tools/hash.sh
+
 _meta:
   type: "internalusers"
   config_version: 2
+
+# Define your internal users here
+
+## Demo users
+
 admin:
-  hash: $2y$12$Cu8jP7gd1mJlSClvW82kCO69/S7Yf74IGdY9bPWcTeHjwoH0uYr6q
+  hash: "$2a$12$VcCDgh2NDk07JGN0rjGbM.Ad41qVR/YFJcgHp0UGns5JDymv..TOG"
   reserved: true
   backend_roles:
   - "admin"
   description: "Demo admin user"
+
+anomalyadmin:
+  hash: "$2y$12$TRwAAJgnNo67w3rVUz4FIeLx9Dy/llB79zf9I15CKJ9vkM4ZzAd3."
+  reserved: false
+  opendistro_security_roles:
+  - "anomaly_full_access"
+  description: "Demo anomaly admin user, using internal role"
+
 kibanaserver:
-  hash: $2y$12$kr4ikvWjGejjmlMnz6wTJ.slYy6lR9uEy1ljW1l3w8eJMBrNwFd7S
+  hash: "$2a$12$4AcgAt3xwOWadA5s5blL6ev39OXDNhmOesEoo33eZtrq2N0YrU3H."
   reserved: true
```

```
-  description: "Demo kibanaserver user"
+  description: "Demo OpenSearch Dashboards user"
+
 kibanaro:
-  hash: $2y$12$/nkeD10mgx3qKoD7W6kWwO7WCMPmsS/pgHj0S3GhiYhzgeCS5JJHu
+  hash: "$2a$12$JJSXNfTowz7Uu5ttXfeYpeYE0arACvcwlPBStB1F.MI7f0U9Z4DGC"
   reserved: false
   backend_roles:
   - "kibanauser"
@@ -22,22 +39,25 @@
     attribute1: "value1"
     attribute2: "value2"
     attribute3: "value3"
-  description: "Demo kibanaro user"
+  description: "Demo read only user, using external role mapping"
+
 logstash:
-  hash: $2y$12$Z7sPb.rL8/MGxz7jtXdbFOoURmtGIW/G4vLjA.96M8wH8y.4FLTUu
+  hash: "$2a$12$u1ShR4l4uBS3Uv59Pa2y5.1uQuZBrZtmNfqB3iM/.jL0XoV9sghS2"
   reserved: false
   backend_roles:
   - "logstash"
-  description: "Demo logstash user"
+  description: "Demo logstash user, using external role mapping"
+
 readall:
-  hash: $2y$12$T0fcXbC8L/fut/BLGV5/7uSleSxKlrX53LjWEX4mZ9XNlaYhWzSkC
+  hash: "$2a$12$ae4ycwzwvLtZxwZ82RmiEunBbIPiAmGZduBAjKN0TXdwQFtCwARz2"
   reserved: false
   backend_roles:
   - "readall"
-  description: "Demo readall user"
+  description: "Demo readall user, using external role mapping"
+
 snapshotrestore:
-  hash: $2y$12$sS6Ecv.XpRDuB6Xw1N7OCu8ubT1xB5uKnIMtqzi32ZyD98IotSqXW
+  hash: "$2y$12$DpwmetHKwgYnorbgdvORCenv4NAK8cPUg8AI6pxLCuWf/ALc0.v7W"
```

```
  reserved: false
  backend_roles:
  - "snapshotrestore"
-  description: "Demo snapshotrestore user"
+  description: "Demo snapshotrestore user, using external role mapping"
```

Modificamos el nombre de los certificados de Wazuh dashboard para que estén de acuerdo a la nueva configuración.

```
sudo mv /etc/wazuh-dashboard/certs/wazuh-dashboard-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
sudo mv /etc/wazuh-dashboard/certs/wazuh-dashboard.pem /etc/wazuh-dashboard/certs/dashboard.pem
```

Cambiamos la lista de permisos.

```
sudo chown wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs/*.pem
sudo chmod 600 /etc/wazuh-dashboard/certs/*.pem
```

Verificamos la configuración de la API por el puerto "55000".

```
sudo nano /usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml
```

```
hosts:
  - default:
      url: https://127.0.0.1
      port: 55000
      username: wazuh-wui
      password: "Contraseña Wazuh-Wui"
      run_as: false
```

Por último para la cantidad de memoria RAM asignada para los procesos modificamos el archivo:

```
sudo nano /etc/wazuh-indexer/jvm.options
```

Dentro del archivo cambiamos "Xms1g" por "Xms2g"

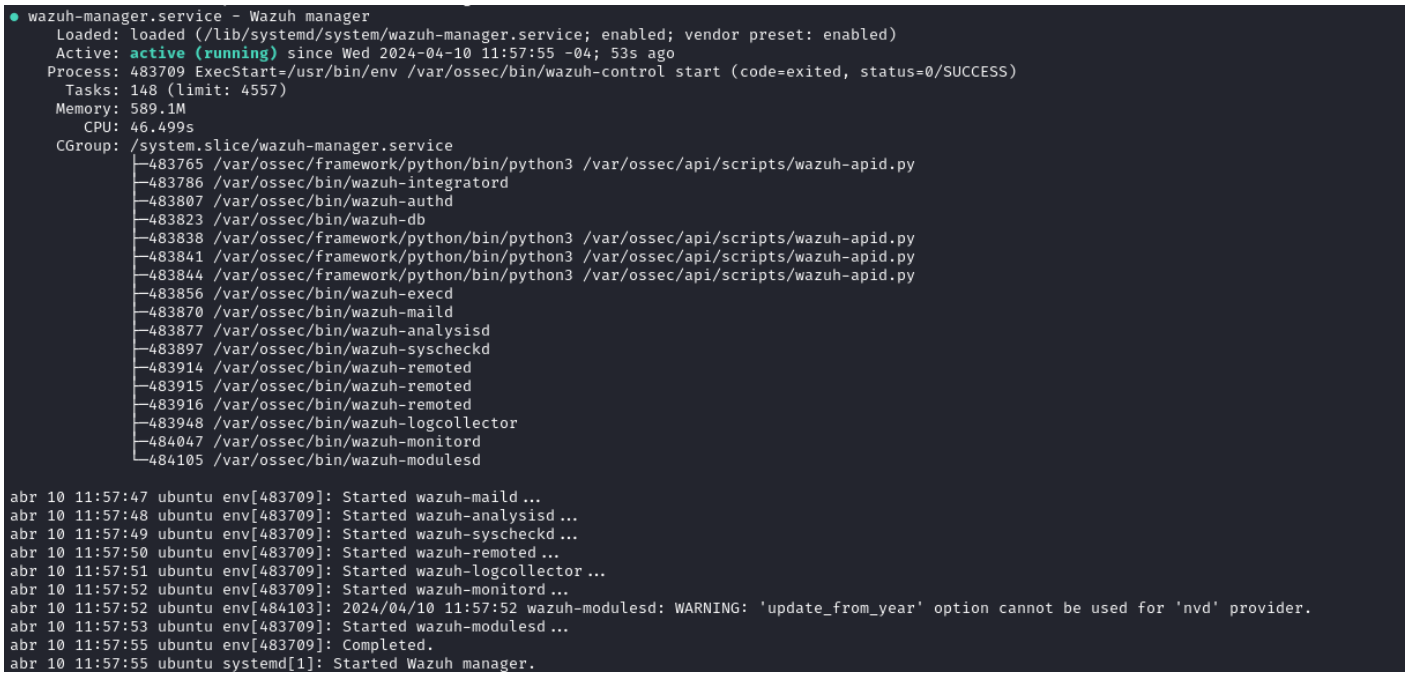
En el caso de la modificación de permisos por actualizar desde una versión inferior a 4.5.7 se vuelve a modificar el cambio de directorio del indexador.

```
sudo chmod -R 755 /usr/share/wazuh-indexer
sudo chown -R wazuh-indexer:wazuh-indexer /usr/share/wazuh-indexer
```

Realizamos un "**restart**" a cada uno de los componentes de Wazuh para aplicar los cambios y esperamos aproximadamente 2 minutos para utilizar los servicios.

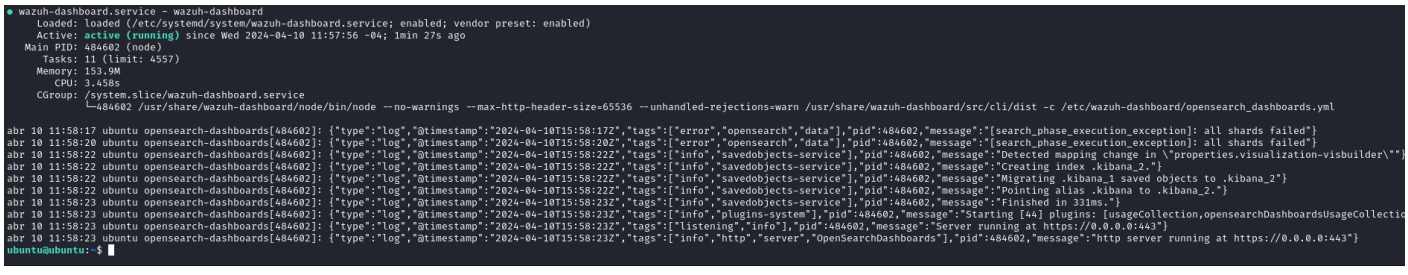
```
sudo systemctl daemon-reload
sudo systemctl restart wazuh-manager
sudo systemctl restart wazuh-dashboard
sudo systemctl restart wazuh-indexer
```

```
sudo systemctl status wazuh-manager
```



```
● wazuh-manager.service - Wazuh manager
     Loaded: loaded (/lib/systemd/system/wazuh-manager.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-04-10 11:57:55 -04; 53s ago
    Process: 483709 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=exited, status=0/SUCCESS)
      Tasks: 148 (limit: 4557)
     Memory: 589.1M
        CPU: 46.499s
     CGroup: /system.slice/wazuh-manager.service
             ├─483765 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─483786 /var/ossec/bin/wazuh-integratord
             ├─483807 /var/ossec/bin/wazuh-authd
             ├─483823 /var/ossec/bin/wazuh-db
             ├─483838 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─483841 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─483844 /var/ossec/framework/python/bin/python3 /var/ossec/api/scripts/wazuh-apid.py
             ├─483856 /var/ossec/bin/wazuh-execd
             ├─483870 /var/ossec/bin/wazuh-maild
             ├─483877 /var/ossec/bin/wazuh-analysisd
             ├─483897 /var/ossec/bin/wazuh-syscheckd
             ├─483914 /var/ossec/bin/wazuh-remoted
             ├─483915 /var/ossec/bin/wazuh-remoted
             ├─483916 /var/ossec/bin/wazuh-remoted
             ├─483948 /var/ossec/bin/wazuh-logcollector
             ├─484047 /var/ossec/bin/wazuh-monitord
             └─484105 /var/ossec/bin/wazuh-modulesd

abr 10 11:57:47 ubuntu env[483709]: Started wazuh-maild...
abr 10 11:57:48 ubuntu env[483709]: Started wazuh-analysisd...
abr 10 11:57:49 ubuntu env[483709]: Started wazuh-syscheckd...
abr 10 11:57:50 ubuntu env[483709]: Started wazuh-remoted...
abr 10 11:57:51 ubuntu env[483709]: Started wazuh-logcollector...
abr 10 11:57:52 ubuntu env[483709]: Started wazuh-monitord...
abr 10 11:57:52 ubuntu env[484103]: 2024/04/10 11:57:52 wazuh-modulesd: WARNING: 'update_from_year' option cannot be used for 'nvd' provider.
abr 10 11:57:53 ubuntu env[483709]: Started wazuh-modulesd...
abr 10 11:57:55 ubuntu env[483709]: Completed.
abr 10 11:57:55 ubuntu systemd[1]: Started Wazuh manager.
```

```
sudo systemctl status wazuh-dashboard
```



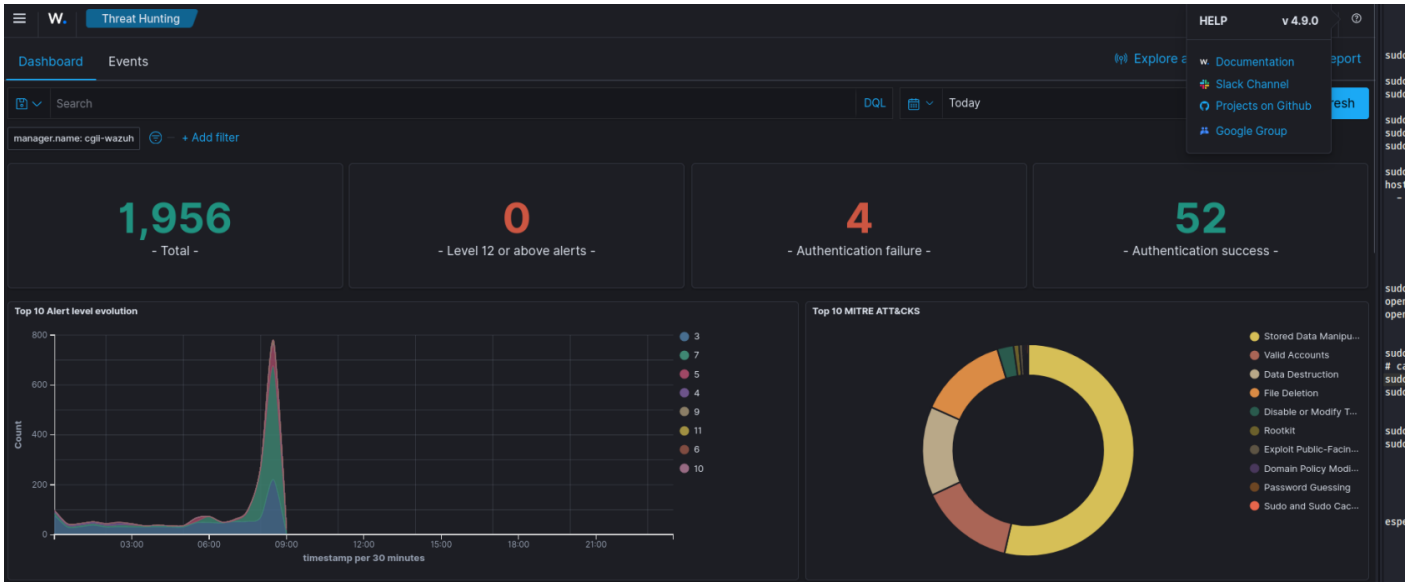
```
● wazuh-dashboard.service - wazuh-dashboard
     Loaded: loaded (/etc/systemd/system/wazuh-dashboard.service; enabled; vendor preset: enabled)
     Active: active (running) since Wed 2024-04-10 11:57:56 -04; 1min 27s ago
   Main PID: 484602 (node)
      Tasks: 11 (limit: 4557)
     Memory: 153.9M
        CPU: 3.458s
     CGroup: /system.slice/wazuh-dashboard.service
             └─484602 /usr/share/wazuh-dashboard/node/bin/node --no-warnings --max-http-header-size=65536 --unhandled-rejections=warn /usr/share/wazuh-dashboard/src/cli/dist -c /etc/wazuh-dashboard/opensearch_dashboards.yml

abr 10 11:58:17 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:17Z","tags":["error","opensearch","data"],"pid":484602,"message":"[search_phase_execution_exception]: all shards failed"}
abr 10 11:58:20 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:20Z","tags":["error","opensearch","data"],"pid":484602,"message":"[search_phase_execution_exception]: all shards failed"}
abr 10 11:58:22 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:22Z","tags":["info","savedobjects-service"],"pid":484602,"message":"Detected mapping change in \"properties.visualization-visbuilder\""}
abr 10 11:58:22 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:22Z","tags":["info","savedobjects-service"],"pid":484602,"message":"Creating index .kibana_2."}
abr 10 11:58:22 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:22Z","tags":["info","savedobjects-service"],"pid":484602,"message":"Migrating .kibana_1 saved objects to .kibana_2"}
abr 10 11:58:22 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:22Z","tags":["info","savedobjects-service"],"pid":484602,"message":"Pointing alias .kibana to .kibana_2."}
abr 10 11:58:23 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:23Z","tags":["info","savedobjects-service"],"pid":484602,"message":"Finished in 331ms."}
abr 10 11:58:23 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:23Z","tags":["info","plugins-system"],"pid":484602,"message":"Starting [44] plugins: [usageCollection,opensearchDashboardsUsageCollectio
abr 10 11:58:23 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:23Z","tags":["listening","info"],"pid":484602,"message":"Server running at https://0.0.0.0:443"}
abr 10 11:58:23 ubuntu opensearch-dashboards[484602]: {"type":"log","@timestamp":"2024-04-10T15:58:23Z","tags":["info","http","server","OpenSearchDashboards"],"pid":484602,"message":"http server running at https://0.0.0.0:443"}
ubuntu@ubuntu:~$
```

```
sudo systemctl status wazuh-indexer
```

En el caso del sistema Ubuntu server 22.04 en fecha 03-10-2024, se normalizó la utilización de la herramienta después de un reinicio y una espera de 5 minutos.

```
sudo reboot
```

Ingresamos al dashboard y verificamos que la versión de Wazuh se actualizó con éxito.



Consideraciones a tomar en cuenta en caso de más de 50 agentes de Wazuh.

```
nano /etc/wazuh-indexer/jvm.options
```

Expandir la cantidad de recursos que se pueden utilizar en caso de exceso de eventos e incrementar según consumo de recursos Ej. a 2GB para indexación de elementos.

```
# Xms represents the initial size of total heap space
# Xmx represents the maximum size of total heap space
-Xms2048m
-Xmx2048m
```

Revision #6
Created 10 abril 2024 11:31:53 by Ricardo Alberto
Updated 24 abril 2025 15:40:19 by Ricardo Alberto