OSSEC Ubuntu Server

OSSEC is a useful tool in monitoring for malicious activity across various servers. It's lightweight, and easy to install an agent and have it reporting to the master server within minutes. Unfortunately, there is no automated solution to configuring agents remotely via Ansible or other tools that I am aware of.

OSSEC Server Configuration

Its important to note that we are installing the server in these instructions, and not an agent manager. An Agent manager is a much lighter installation from the same tarball that allows connecting to this server and reporting alerts through one host.

Creating OSSEC User

Once you are logged in to the host you wish to act as the server sending email alerts and recieving reports from agents and create a new user to manage OSSEC -

```
admin@host:~$ git clone https://github.com/shaunrd0/klips


Cloning into 'klips'...
remote: Enumerating objects: 295, done.
remote: Counting objects: 100% (295/295), done.
remote: Compressing objects: 100% (187/187), done.
remote: Total 295 (delta 109), reused 255 (delta 72), pack-reused 0
Receiving objects: 100% (295/295), 47.48 KiB | 3.96 MiB/s, done.
Resolving deltas: 100% (109/109), done.
admin@host:~$ cp klips/scripts/adduser.sh .
admin@host:~$ sudo ./adduser.sh ossec 5555
Adding user `ossec' ...
Adding new group `ossec' (5555) ...
Adding new user `ossec' (5555) with group `ossec' ...
Creating home directory `/home/ossec' ...
Copying files from `/etc/skel' ...


Enter 1 if ossec should have sudo privileges. Any other value will continue and make no changes
1
Configuring sudo for ossec...
```

```
Enter 1 to set a password for ossec, any other value will exit with no password set
1
Changing password for ossec...
New password:
Retype new password:
passwd: password updated successfully
```

Dependencies / Installation Files

Now that we have our user created, lets become them and prepare to install the OSSEC server

```
admin@host:~$ sudo -iu ossec

To run a command as administrator (user "root"), use "sudo <command>".
see "man sudo_root" for details.
```

OSSEC Official Downloads provides the official download sources, and after selecting one the file can be downloaded right to your working directory using `wget` -

```
# Download the tar for linux server / agent installation
wget https://github.com/ossec/ossec-hids/archive/3.3.0.tar.gz
# Extract it
tar xf 3.3.0.tar.gz
```

Now, we have created the below directory -

```
ossec-hids-3.3.0/
BUGS       CONFIG        INSTALL  README.md   active-response  doc  install.sh
CHANGELOG  CONTRIBUTORS  LICENSE  SUPPORT.md  contrib          etc  src
```

We should prepare to start installing by grabbing basic OSSEC dependencies -

```
sudo apt install build-essential gcc make
```

> Below we will cover the several error cases I've encountered installing OSSEC on Ubuntu servers 18.04 and later. If you just want to get through the install, feel free to skip below and install / extract all the dependencies that fixed the many errors I've encountered during the installation process. Otherwise, only install or correct the packages which give you errors during installation

Installing OSSEC Server

> During installation, OSSEC will ask for a server hostname / IP address. Using anything other than a direct IP has always given me issues. If you install and want to change the IP of your OSSEC server, edit the `/var/ossec/etc/agent.conf` file.

Now we have our user created, permissions granted, and dependencies / files we need to install OSSEC. Navigate within the `ossec-hids-3.3.0/` directory and run `sudo ./install.sh`. You will be prompted to select preferred settings for this installation. Pay attention to the prompts and respond accordingly, this is where the difference is seen in installing an Agent vs installing the OSSEC Monitoring Server.

You may see the below error for a missing dependency - pcre2.

```
5- Installing the system
 - Running the Makefile
cd external/pcre2-10.32/ && \
./configure \
        --prefix=/home/kossec/ossec-hids-3.3.0/src/external/pcre2-10.32//install \
        --enable-jit \
        --disable-shared \
        --enable-static && \
make install-libLTLIBRARIES install-nodist_includeHEADERS
/bin/sh: 1: cd: can't cd to external/pcre2-10.32/
Makefile:770: recipe for target 'external/pcre2-10.32//install/lib/libpcre2-8.a' failed
make: *** [external/pcre2-10.32//install/lib/libpcre2-8.a] Error 2

 Error 0x5.
 Building error. Unable to finish the installation.
```

Continue on by running the below commands, which will add the required files to your extracted `ossec-hids-3.3.0/` directory -

```
# Error - build fails because of missing pcre2
# Run these commands within the installation directory
cd ossec-hids-3.3.0
wget https://ftp.pcre.org/pub/pcre/pcre2-10.32.tar.gz
tar xzf pcre2-10.32.tar.gz -C src/external
```

Now run `sudo PCRE2_SYSTEM=no ./install` to start the installation, and keep in mind should you need to restart the install later for any reason you will need to run `sudo PCRE2_SYSTEM=no ./install` and NOT `sudo ./install`.

After fixing the above error, you may see another when attempting to install again. The error below is due to the missing `libz-dev` dependency -

```
os_zlib/os_zlib.c:13:10: fatal error: zlib.h: No such file or directory
 #include <zlib.h>
          ^~~~~~~~
compilation terminated.
Makefile:727: recipe for target 'os_zlib/os_zlib.o' failed
make: *** [os_zlib/os_zlib.o] Error 1

 Error 0x5.
 Building error. Unable to finish the installation.
```

If you see *this* error, you'll need to install zlib using the below command

```
# Error Making os_auth
sudo apt install -y libz-dev
```

Now we may see yet another error -

```
client-agent/start_agent.c:15:10: fatal error: event.h: No such file or directory
 #include <event.h>
          ^~~~~~~~~
compilation terminated.
Makefile:1014: recipe for target 'client-agent/start_agent.o' failed
make: *** [client-agent/start_agent.o] Error 1
 Error 0x5.
 Building error. Unable to finish the installation.
```

To correct this problem, we can run `sudo apt install libevent-dev` but it doesn't end there..

We might see the problem below -

```
#include <openssl/opensslv.h> /* For OPENSSL_VERSION_NUMBER */
          ^~~~~~~~~~~~~~~~~~~
compilation terminated.
Makefile:1017: recipe for target 'ossec-agentd' failed
make: *** [ossec-agentd] Error 1
 Error 0x5.
 Building error. Unable to finish the installation
```

To fix this problem, we run `sudo apt install libssl-dev`

That's it! :)

Enable EMail Notifications

To enable email alerting from the OSSEC server and the remote agents it monitors, follow the instructions on Configuring Postfix and then make the appropriate changes to the mail settings in `/var/ossec/etc/ossec.conf` below -

```
<ossec_config>
  <global>
    <email_notification>yes</email_notification>
    <email_to>someone@somedomain.com</email_to>
    <smtp_server>127.0.0.1</smtp_server>
    <email_from>ossec@host</email_from>
  </global>
```

There is no need to point `smtp_server` to a mail server directly, handling mail this way simply bounces the messages off the localhost's configuration we already have setup and validated working from Configuring Postfix.

If you can send mail with the below command, chances are the issue is within OSSEC and not your servers postifx configuration or gmail authentication.

```
echo "This email confirms that Postfix is working" | mail -s "Testing Posfix" emailuser@example.com
```

If this command fails, go back and check that you've configured Postfix correctly with GMail, and once you have that verified come back here to finish up with OSSEC.

Managing Agents

> I haven't had much luck with using domain names or floating IPs with OSSEC agents or servers, so in general I'd recommend just using a direct IP address. If there is a way around this, I'm not aware of it.

To use the manage_agent utility that comes with OSSEC, run `/var/ossec/bin/manage_agents` either as root or with sudo (`sudo /var/ossec/bin/manage_agents`)

If you are running the manage_agents utility on an OSSEC Server -

```
****************************************
* OSSEC HIDS v3.3.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: q
```

If you are running the manage_agents utility on an OSSEC Agent -

```
****************************************
* OSSEC HIDS v3.3.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q:
```

This tool is used to define an agent on the server, export its key, then import the server's key within the ossec-agent on the remote host, allowing the connection. Its important to follow these steps carefully, as any discrepency in IP or `client.keys` will result in a connection failing.

Defining Agents

To start, on the OSSEC Server, run the manage_agents utility and add an agent -

```
****************************************
* OSSEC HIDS v3.3.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: a


- Adding a new agent (use '\q' to return to the main menu).
```

```
  Please provide the following:
   * A name for the new agent: test
   * The IP Address of the new agent: 0.0.0.0
   * An ID for the new agent[007]: 007
Agent information:
   ID:007
   Name:test
   IP Address:0.0.0.0

Confirm adding it?(y/n): y
Agent added.
```

Extracting Server Keys (Server)

We've define our agent with the local OSSEC Server, and prepared it for the connection. Now we need to continue through the prompts and extract the key for the agent to copy over onto our remote host -

```
****************************************
* OSSEC HIDS v3.3.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: e

Provide the ID of the agent to extract the key (or '\q' to quit): 007

Agent key information for '007' is:
MDA2Ig4LjQzIDkxZDYmRlZGN5mOG5NzY5Nd325dmFmMTU0NzZkddaDM1ND456431MWY1ODhhMDyjukuMDYzg
4MzA5MmM=
** Press ENTER to return to the main menu.
```

Exit the prompts, and copy this key or temporarily store it in the text file. We will need it to register the agent with its remote server.

Importing Server Keys (Agent)

Open a terminal on the host you have installed the OSSEC Agent on, and run the manage_agents utility just as we did on the last host (`sudo /var/ossec/bin/manage_agents`) -

```
****************************************
* OSSEC HIDS v3.3.0 Agent manager.     *
* The following options are available: *
****************************************
   (I)mport key from the server (I).
   (Q)uit.
Choose your action: I or Q: i



* Provide the Key generated by the server.
* The best approach is to cut and paste it.
*** OBS: Do not include spaces or new lines.

Paste it here (or '\q' to quit):
MDA2Ig4LjQzIDkxZDYmRlZGN5mOG5NzY5Nd325dmFmMTU0NzZkddaDM1ND456431MWY1ODhhMDyjukuMDYzg
4MzA5MmM

Agent information:
   ID:007
   Name:test
   IP Address:0.0.0.0

Confirm adding it?(y/n): y
Added.
** Press ENTER to return to the main menu.
```

Starting OSSEC Agent

That's it! Press enter and exit through the prompts, then just `sudo /var/ossec/bin/ossec-control restart` to apply our changes on both the server and the agent.

Sometimes, when initially starting an agent on a new host you will get like the below -

```
ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf': XMLERR: File
'/var/ossec/etc/shared/agent.conf' not found. (line 99).
ossec-syscheckd(1226): ERROR: Error reading XML file '/var/ossec/etc/shared/agent.conf': XMLERR: File
'/var/ossec/etc/shared/agent.conf' not found. (line 99).
```

Just `touch /var/ossec/etc/shared/agent.conf` and `sudo /var/ossec/bin/ossec-control restart` / `sudo /var/ossec/bin/ossec-control start` again. The services should start normally. This is an old bug I came across in this GitHub issue.

Troubleshooting Agent Connections

If an agent isnt connecting, try the following commands to check for common problems -

Verify Agent Server Configuration

When attempting to start the OSSEC agent, you may see errors like the following -

```
Deleting PID file '/var/ossec/var/run/ossec-logcollector-23324.pid' not used...
Deleting PID file '/var/ossec/var/run/ossec-agentd-23320.pid' not used...
ossec-logcollector not running ..
ossec-syscheckd not running ..
ossec-agentd not running ..
Killing ossec-execd ..
OSSEC HIDS v2.9.0 Stopped
Starting OSSEC HIDS v2.9.0 (by Trend Micro Inc.)...
Started ossec-execd...
2019/11/04 17:17:16 ossec-agentd: INFO: Using notify time: 600 and max time to reconnect: 1800
Started ossec-agentd...
Started ossec-logcollector...
2019/11/04 17:17:19 ossec-syscheckd(1210): ERROR: Queue '/var/ossec/queue/ossec/queue' not accessible:
'Connection r
efused'.
2019/11/04 17:17:19 rootcheck(1210): ERROR: Queue '/var/ossec/queue/ossec/queue' not accessible:
'Connection refused
'.
```

Checking the logs within `/var/ossec/logs/ossec.log` reveals that no there is no valid OSSEC server configuration. To resolve this, ensure that you used the correct IP during installation for your OSSEC Server, then use the `/var/ossec/bin/manage_agents` tool on both the server and the agent to Add / Export Agent Keys and then run `sudo /var/ossec/bin/ossec-control restart` to restart the agent.

Check Agent Status on Server

There are many ways to check the agent status on the OSSEC Server host itself. One of which is within the manage_agents utility used to register new agents. Simply run `sudo /var/ossec/bin/manage_agents` and select L to list added agents and their current status with the server.

```
****************************************
* OSSEC HIDS v3.3.0 Agent manager.     *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: l

Available agents:
   ID: 001, Name: host, IP: 100.200.300.400
   ID: 002, Name: host2, IP: 200.200.300.400
   ID: 003, Name: host3, IP: 300.200.300.400
   ID: 004, Name: host4, IP: 400.200.300.400

** Press ENTER to return to the main menu.
```

We can also list all agents with the built in OSSEC utility list_agents, run the following command to list all agents, even if they are disconnected or have never been connected in the first place -

```
admin@host:~# /var/ossec/bin/list_agents -a
host-100.200.300.400 is active.
host2-200.200.300.400 is active.
host3-300.200.300.400 is active.
host4-400.200.300.400 is active.
```

Check OSSEC Logs

OSSEC is an HIDS, which means it takes a ton of logs. Use them to your advantage, in this care we can easily check for general OSSEC errors within the `/var/ossec/logs/ossec.log`

Logs such as the below could indicate an incorrect `client.key`, which is configured when adding the agent to the OSSEC server, and again on the remote host when importing the generated key. If you see errors like this, try going back and removing the agent from the OSSEC server, create a new one and be sure you are using the correct IP for your agent.

```
2019/08/31 18:14:05 ossec-remoted(1213): WARN: Message from '100.200.300.400' not allowed.
2019/08/31 18:14:43 ossec-remoted(1213): WARN: Message from '100.200.300.400' not allowed.
2019/08/31 18:14:49 ossec-remoted(1213): WARN: Message from '100.200.300.400' not allowed.
```

```
2019/08/31 18:14:53 ossec-remoted(1213): WARN: Message from '100.200.300.400' not allowed.
2019/08/31 18:14:58 ossec-remoted(1213): WARN: Message from '100.200.300.400' not allowed
```

It's important to note that when installing the agent on the remote host you wish to monitor, you are prompted to input the Server IP - this is an important step and if done incorrectly just re-run the installation as if you were starting on a fresh host, and when prompted to update OSSEC input NO. Follow the prompts and install in the same location you did previously, and OSSEC will prompt you to remove the previous installation before reinstalling. Do so, and input the correct IP of the host running your OSSEC Server.

A useful trick when debugging mail issues with `ossec-maild` -

```
tail -f /var/ossec/logs/ossec.log | grep ossec-maild
```

For a live feed, filtered log on `ossec-maild` within the base OSSEC server logs.

Check IPTables

You may need to allow traffic on ports used by OSSEC with `iptables`, to do so, run the following commands. If you make any changes to iptables, be sure to `sudo apt install iptables-persistent`, which will enable iptables to carry over your settings if your host is restarted.

View current iptables -

```
iptables -nL
```

Allow the Agent to connect to our OSSEC Server host on the specified port, run -

```
iptables -A INPUT -p UDP --dport 1514 -s your_agent_ip -j ACCEPT
```

Allow the OSSEC Server to connect to our agent on the specified port, run -

```
iptables -A INPUT -p UDP --dport 1514 -s your_server_ip -j ACCEPT
```

Allow all outbound traffic, assuming no malicious activity will come from within -

```
iptables -A OUTPUT -j ACCEPT
```

Check Network Traffic

Still not sure why your agent isn't connecting? Try to monitor network traffic on the ports you're running OSSEC across - this could give you some idea of if there is traffic moving on one host and not the other, and lead you to where it is being stopped.

The output below is healthy traffic from my OSSEC server monitoring a few hosts -

```
tcpdump -i eth0 port 1514
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
21:48:48.984246 IP 100.200.300.400.53359 > monitor.1514: UDP, length 265
21:48:48.984314 IP 100.200.300.400.53359 > monitor.1514: UDP, length 265
21:48:49.991446 IP 100.200.300.400.53359 > monitor.1514: UDP, length 233
21:48:49.992233 IP monitor.1514 > 159.65.224.81.53359: UDP, length 73
21:48:53.914955 IP 100.200.300.400.48049 > monitor.1514: UDP, length 265
21:48:54.990058 IP 200.200.300.400.53359 > monitor.1514: UDP, length 249
```

Duplicate Counter Errors

Sometimes, when attempting an update or reinstall / reconfiguration of the OSSEC server or agents you may see the errors below within your `/var/ossec/logs/ossec.log` -

```
2019/11/05 01:58:16 ossec-remoted: WARN: Duplicate error:  global: 0, local: 7316, saved global: 0, saved local:7317
2019/11/05 01:58:16 ossec-remoted(1407): ERROR: Duplicated counter for 'box1'.
2019/11/05 01:59:20 ossec-remoted: WARN: Duplicate error:  global: 0, local: 5910, saved global: 0, saved local:5911
2019/11/05 01:59:20 ossec-remoted(1407): ERROR: Duplicated counter for 'box2'.
```

OSSEC uses a counter system to avoid repeat alerts on the same attacks. If you recently refactored your monitoring, it is easy to get your wires crossed in the process and knock the OSSEC server out of sync with its agents. This can happen any number of ways, but a resolution can be found in the OSSEC FAQ Docs. The process is detailed below.

```
    On every agent:


        stop ossec
        go to: .../ossec/queue/rids (or ossec-agent/rids on Windows) and remove every file in there.


    Go to the server:


        Stop ossec
        Remove the rids file with the same name as the agent id that is reporting errors.


    Restart the server
    Restart the agents.
```

In my case, the error above was exactly as stated - I had left the previous ossec agent running while installing the newer version, so there were two agents trying to report to the same IP. The agents were running on the same box, and therefore had the same source IP which was allowed, so OSSEC was confused and sending groups of the errors below

```
2019/11/05 02:44:38 ossec-remoted: WARN: Duplicate error:  global: 0, local: 6997, saved global: 0, saved local:6999
2019/11/05 02:44:38 ossec-remoted(1407): ERROR: Duplicated counter for 'kapps'.
2019/11/05 02:46:17 ossec-remoted(1403): ERROR: Incorrectly formatted message from '1.2.3.4'.
2019/11/05 02:46:23 ossec-remoted(1403): ERROR: Incorrectly formatted message from '1.2.3.4'.
```

To fix this, I just opened `htop` and hit <F3> to type `ossec` and search for any running agents. After finding them, I killed them with <F9> within `htop`

If you can't seem to chase down what is causing these errors but notice that your OSSEC server and agents are running normally despite noisy alerts, you can disable this feature. This is not reconmmended as it removes a security feature of OSSEC but it can be done by viewing the settings within `/var/ossec/etc/internal_options.conf`. Note that you should not edit this file, but copy any settings you wish to modify or override to `/var/ossec/etc/local_internal_options.conf` and set the values to your liking.

For these errors, to stop monitoring for duplicated messages, we add the following line to `/var/ossec/etc/local_internal_options.conf`, save the file and then restart the OSSEC agent.

```
# Default value is set to 1
# Verify msg id (set to 0 to disable it)
remoted.verify_msg_id=0
```

Disconnected Agents

I have been neglecting server maintenance for a few months recently, and came to find out that all of my OSSEC agents had crashed.. A few months ago.

On my OSSEC server, `/var/ossec/logs/ossec.log` shows the following logs

```
2022/06/09 00:01:55 INFO: Connected to 127.0.0.1 at address 127.0.0.1, port 25
2022/06/09 03:56:52 rootcheck: INFO: Starting rootcheck scan.
2022/06/09 03:59:48 rootcheck: INFO: Ending rootcheck scan.
2022/06/09 17:44:48 ossec-syscheckd: INFO: Starting syscheck scan.
2022/06/09 18:32:39 ossec-syscheckd: INFO: Ending syscheck scan.
2022/06/09 23:55:01 ossec-reportd: INFO: Started (pid: 1143516).
```

```
2022/06/09 23:55:06 ossec-reportd: INFO: Report completed. Creating output...
2022/06/09 23:55:06 ossec-reportd: INFO: Started (pid: 1143527).
2022/06/09 23:55:11 ossec-reportd: INFO: Report completed. Creating output...
2022/06/10 00:00:20 ossec-monitord: INFO: Starting daily reporting for 'Daily report: OSSEC Summary'
2022/06/10 00:00:25 ossec-monitord: INFO: Report 'Daily report: OSSEC Summary' completed. Creating output...
2022/06/10 00:00:25 INFO: Connected to 127.0.0.1 at address 127.0.0.1, port 25
2022/06/10 00:02:39 rootcheck: INFO: Starting rootcheck scan.
2022/06/10 00:05:35 rootcheck: INFO: Ending rootcheck scan.
2022/06/10 16:35:35 ossec-syscheckd: INFO: Starting syscheck scan.
2022/06/10 17:23:32 ossec-syscheckd: INFO: Ending syscheck scan.
2022/06/10 20:08:32 rootcheck: INFO: Starting rootcheck scan.
2022/06/10 20:11:28 rootcheck: INFO: Ending rootcheck scan.
2022/06/10 23:55:01 ossec-reportd: INFO: Started (pid: 1155364).
2022/06/10 23:55:06 ossec-reportd: INFO: Report completed. Creating output...
2022/06/10 23:55:06 ossec-reportd: INFO: Started (pid: 1155375).
2022/06/10 23:55:11 ossec-reportd: INFO: Report completed. Creating output...
2022/06/11 00:00:50 ossec-monitord: INFO: Starting daily reporting for 'Daily report: OSSEC Summary'
2022/06/11 00:00:55 ossec-monitord: INFO: Report 'Daily report: OSSEC Summary' completed. Creating output...
# NOTE: Above this line is normal activity

2022/06/11 00:00:55 INFO: Connected to 127.0.0.1 at address 127.0.0.1, port 25
2022/06/11 01:00:39 ossec-logcollector: socketerr (not available).
2022/06/11 01:00:39 ossec-logcollector(1224): ERROR: Error sending message to queue.
2022/06/11 01:00:42 ossec-logcollector(1210): ERROR: Queue '/var/ossec/queue/ossec/queue' not accessible: 'Connection refused'.
2022/06/11 01:00:42 ossec-logcollector(1211): ERROR: Unable to access queue: '/var/ossec/queue/ossec/queue'. Giving up..
2022/06/11 01:00:59 ossec-remoted: socketerr (not available).
2022/06/11 01:00:59 ossec-remoted(1210): ERROR: Queue '/queue/ossec/queue' not accessible: 'Connection refused'.
2022/06/11 01:01:02 ossec-remoted(1210): ERROR: Queue '/queue/ossec/queue' not accessible: 'Connection refused'.
2022/06/11 01:01:02 ossec-remoted(1211): ERROR: Unable to access queue: '/queue/ossec/queue'. Giving up..
2022/06/11 01:31:20 ossec-monitord: socketerr (not available).
2022/06/11 01:31:20 ossec-monitord(1224): ERROR: Error sending message to queue.
2022/06/11 15:26:28 ossec-syscheckd: INFO: Starting syscheck scan.
2022/06/11 15:26:28 ossec-syscheckd: socketerr (not available).
2022/06/11 15:26:28 ossec-syscheckd(1224): ERROR: Error sending message to queue.
2022/06/11 15:26:31 ossec-syscheckd(1210): ERROR: Queue '/var/ossec/queue/ossec/queue' not accessible: 'Connection refused'.
```

```
2022/06/11 15:26:31 ossec-syscheckd(1211): ERROR: Unable to access queue: '/var/ossec/queue/ossec/queue'. Giving up..
2022/06/11 23:01:04 agent_control(1210): ERROR: Queue '/queue/alerts/ar' not accessible: 'Connection refused'.
2022/06/11 23:01:04 agent_control(1301): ERROR: Unable to connect to active response queue.
2022/06/11 23:55:01 ossec-reportd: INFO: Started (pid: 1157527).
2022/06/11 23:55:06 ossec-reportd: INFO: Report completed. Creating output...
2022/06/11 23:55:06 ossec-reportd: INFO: Started (pid: 1157538).
2022/06/11 23:55:11 ossec-reportd: INFO: Report completed. Creating output...
2022/06/12 00:01:21 ossec-monitord: INFO: Starting daily reporting for 'Daily report: OSSEC Summary'
2022/06/12 00:01:26 ossec-monitord: INFO: Report 'Daily report: OSSEC Summary' completed and zero alerts post-filter.
2022/06/12 00:01:26 ossec-monitord: INFO: Report 'Daily report: OSSEC Summary' empty.
2022/06/12 23:01:04 agent_control(1210): ERROR: Queue '/queue/alerts/ar' not accessible: 'Connection refused'.
2022/06/12 23:01:04 agent_control(1301): ERROR: Unable to connect to active response queue.
2022/06/12 23:55:01 ossec-reportd: INFO: Started (pid: 1159635).
2022/06/12 23:55:06 ossec-reportd: INFO: Report completed. Creating output...
2022/06/12 23:55:06 ossec-reportd: INFO: Started (pid: 1159646).
2022/06/12 23:55:11 ossec-reportd: INFO: Report completed. Creating output...
2022/06/13 00:01:51 ossec-monitord: INFO: Starting daily reporting for 'Daily report: OSSEC Summary'
2022/06/13 00:01:51 ossec-monitord: ERROR: Unable to open alerts file to generate report.
2022/06/13 00:01:51 ossec-monitord: INFO: Report 'Daily report: OSSEC Summary' empty.
2022/06/13 00:02:21 ossec-monitord: File '/logs/alerts/2022/Jun/ossec-alerts-12.log' not found. MD5 checksum skipped.
2022/06/13 00:02:21 ossec-monitord: File '/logs/alerts/2022/Jun/ossec-alerts-12.log' not found. SHA1 checksum skipped.
2022/06/13 23:01:04 agent_control(1210): ERROR: Queue '/queue/alerts/ar' not accessible: 'Connection refused'.
```

On my OSSEC agents, `/var/ossec/logs/ossec.log` shows the following logs

```
2022/06/09 23:08:48 ossec-syscheckd: INFO: Starting syscheck scan.
2022/06/09 23:24:21 ossec-syscheckd: INFO: Ending syscheck scan.
2022/06/10 19:09:21 rootcheck: INFO: Starting rootcheck scan.
2022/06/10 19:12:12 rootcheck: INFO: Ending rootcheck scan.
2022/06/10 21:27:12 ossec-syscheckd: INFO: Starting syscheck scan.
2022/06/10 21:42:46 ossec-syscheckd: INFO: Ending syscheck scan.
2022/06/10 23:02:46 rootcheck: INFO: Starting rootcheck scan.
2022/06/10 23:05:37 rootcheck: INFO: Ending rootcheck scan.
2022/06/10 23:05:37 ossec-syscheckd: INFO: Starting syscheck scan.
2022/06/10 23:21:12 ossec-syscheckd: INFO: Ending syscheck scan.
# NOTE: Above this line is normal activity
```

```
2022/06/11 01:03:33 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:03:34 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:09:36 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:09:37 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:09:38 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:09:39 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:09:40 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:09:41 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:15:36 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:15:37 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:15:38 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:21:38 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:21:39 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:21:40 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:27:41 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:27:42 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:27:43 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:29:36 ossec-agentd: WARN: Server unavailable. Setting lock.
2022/06/11 01:29:46 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:29:58 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:29:59 ossec-agentd(4101): WARN: Waiting for server reply (not started). Tried: '159.203.190.63'.
2022/06/11 01:30:01 ossec-agentd: INFO: Trying to connect to server 159.203.190.63, port 1514.
2022/06/11 01:30:01 INFO: Connected to 159.203.190.63 at address 159.203.190.63, port 1514
2022/06/11 01:30:11 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:30:21 ossec-logcollector: WARN: Process locked. Waiting for permission...
2022/06/11 01:30:23 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:30:24 ossec-agentd(4101): WARN: Waiting for server reply (not started). Tried: '159.203.190.63'.
2022/06/11 01:30:44 ossec-agentd: INFO: Trying to connect to server 159.203.190.63, port 1514.
2022/06/11 01:30:44 INFO: Connected to 159.203.190.63 at address 159.203.190.63, port 1514
2022/06/11 01:30:54 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:31:06 ossec-agentd(1218): ERROR: Unable to send message to 'server'.
2022/06/11 01:31:07 ossec-agentd(4101): WARN: Waiting for server reply (not started). Tried: '159.203.190.63'.
# ... Literally 3 months of logs like this; try, fail
```

Fixed with the following commands

On the OSSEC server -

```
sudo su
cd /var/ossec/bin/
./agent_control -l

OSSEC HIDS agent_control. List of available agents:
   ID: 000, Name: not (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: real, IP: 1.1.1.1, Disconnected
   ID: 002, Name: agent, IP: 2.2.2.2, Disconnected
   ID: 003, Name: names, IP: 3.3.3.3, Disconnected
```

These agents are all normally connected. My email logs are showing only reports for the OSSEC server for the last 3 months. Nice.

My server runs this command every day at a certain time, and if it fails I get an email alert. I've been ignoring them, but I guess the alerting has done its job here. I knew there was a problem, I just didn't care.

```
./agent_control -r -a
2022/09/12 23:17:08 agent_control(1210): ERROR: Queue '/queue/alerts/ar' not accessible: 'Connection ref
used'.
2022/09/12 23:17:08 agent_control(1301): ERROR: Unable to connect to active response queue.

** Unable to connect to remoted.
```

To fix this all I had to do was restart the agents. On my server *and* the remote agents. OSSEC makes this simple, and it's just a single command that is the same for the server and agents.

```
cd /var/ossec/bin
./ossec-control restart
```

The worst part of fixing this was logging into all the servers and resetting them manually. I feel they're decently secure for what they are, but I have not made authenticating as root a simple process, even for myself. Anyhow - after running the command above on all your servers things should be fine.

```
cd /var/ossec/bin/
./agent_control -l

OSSEC HIDS agent_control. List of available agents:
   ID: 000, Name: not (server), IP: 127.0.0.1, Active/Local
   ID: 001, Name: real, IP: 1.1.1.1, Active
   ID: 002, Name: agent, IP: 2.2.2.2, Active
   ID: 003, Name: names, IP: 3.3.3.3, Active
```

Links

More links:

OSSEC Installation Tutorial

Revision #18
Created 31 August 2019 18:58:09 by Shaun Reed
Updated 12 September 2022 23:56:43 by Shaun Reed