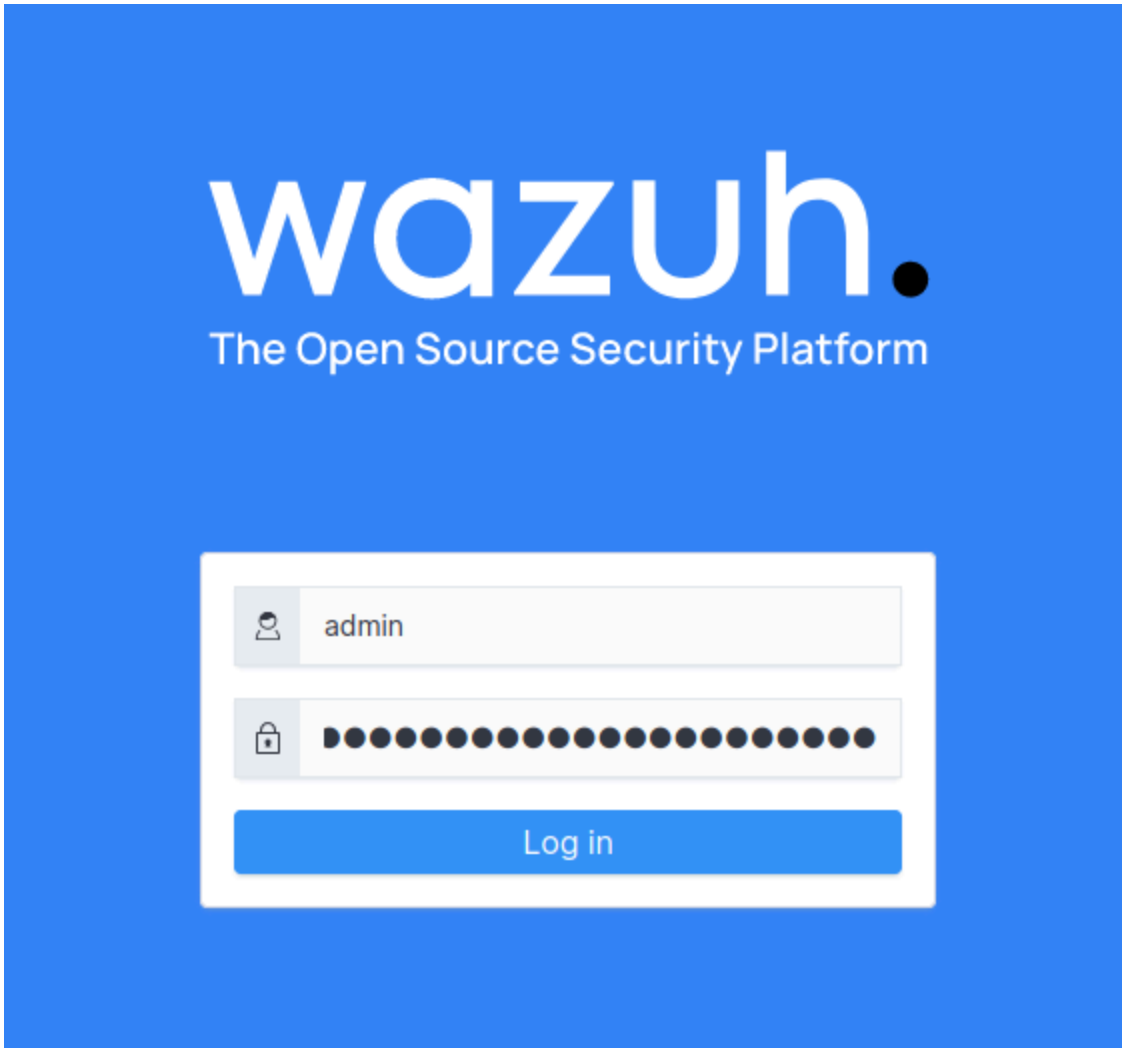


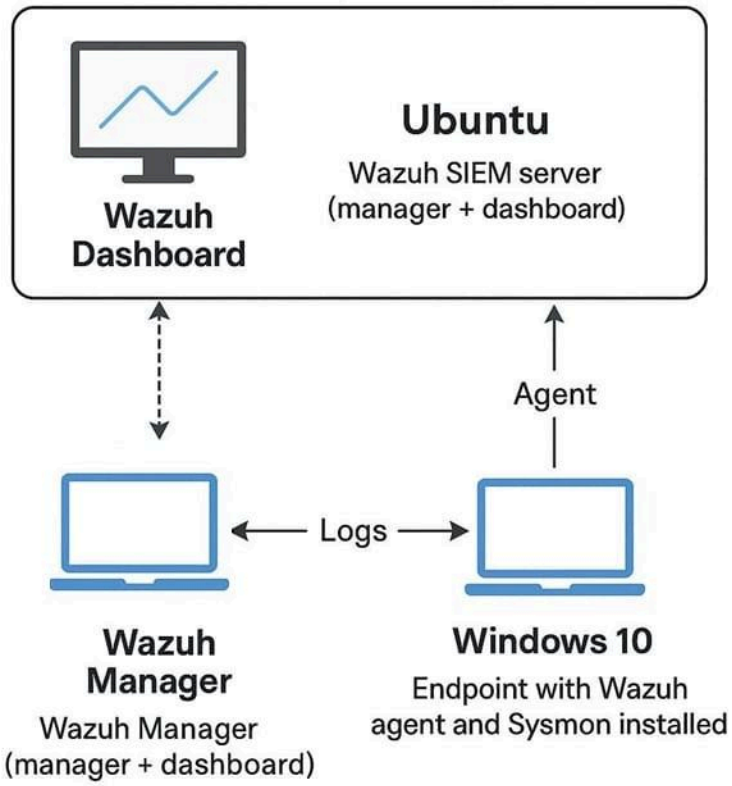
Wazuh is an open-source security monitoring platform used for threat detection, integrity monitoring, and incident response. Setting up a Wazuh home lab environment is an excellent way for SOC (Security Operations Center) analysts to gain hands-on experience in security monitoring, alerting, and response.

In this Homelab tutorial, I'm going to be installing and running an absolutely free and open-source cybersecurity solution, which goes by the name of Wazuh. Wazuh is a SIEM and an XDR, which stands for Extended Detection and Response. And as I stated earlier as well, it's absolutely free. So if you're looking to get into cybersecurity and want to get your hands dirty, this is an absolutely perfect Homelab project for you. We're going to be installing and running our Wazuhmanager on an Ubuntu VM. And we'll also be installing a Wazuh agent on our host Windows machine. And the agent is then going to send different events and logs to our Wazuh manager, which we then view on the Wazuh dashboard. As part of this Homelab, we are also going to be performing file and directory integrity monitoring, which means that we'll choose to monitor a specific directory in our Wazuh agent. And the moment we create a file or we delete a file, those logs are then going to be sent to our Wazuh manager. So we've got complete control over what our endpoint is doing. So it's an amazing lab. And if you want to learn these aspects of cybersecurity, make sure you get your laptop, stick around and follow all the steps.

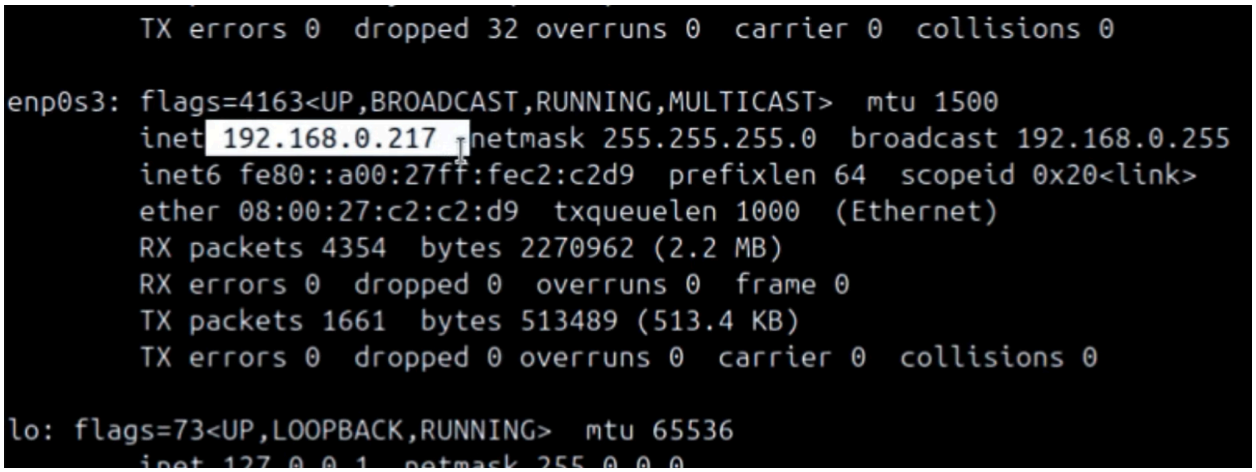
Requirements

Jumping straight into the requirement of what We need for this lab is you need a laptop with at least 8 GB RAM and a hypervisor. I'm going to be running VirtualBox again because it's free and I'm going to be running an Ubuntu VM which is going to host my Wazow manager and the agent will then be installed on my Windows machine.

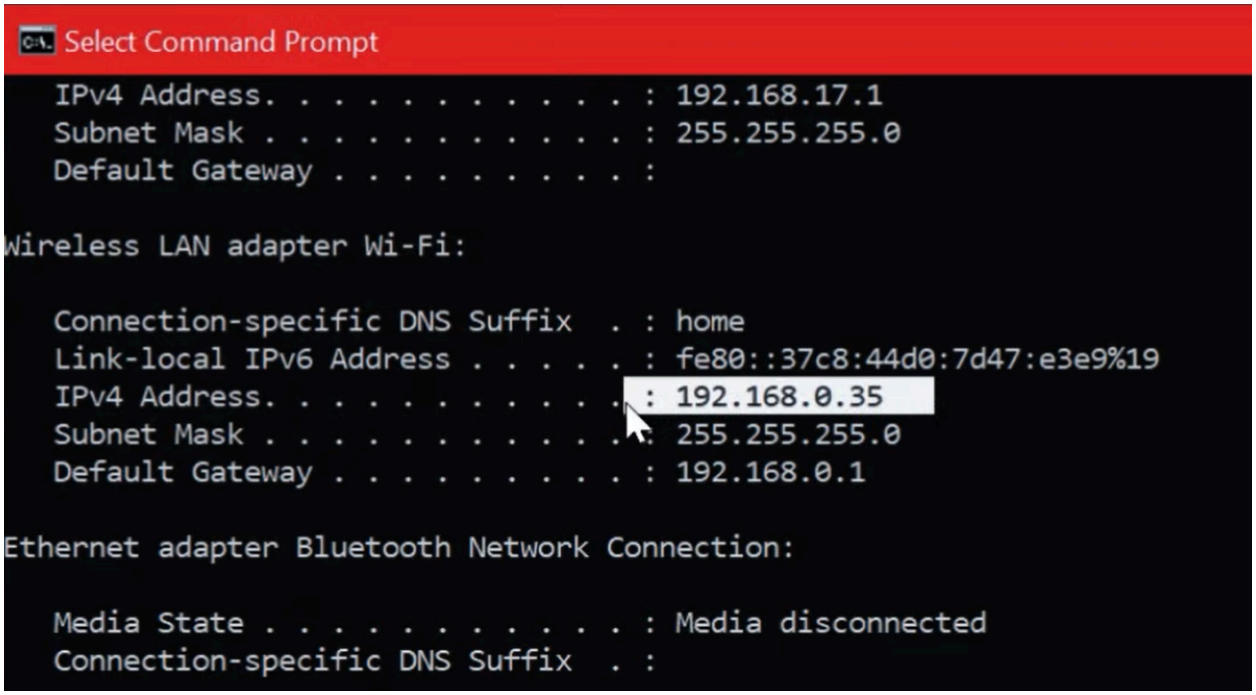
Lab Architecture And IP address configuration.



So if we look at what the diagram will look like, we've got a Ubuntu machine (Wazuh manager) and we've got our Windows machine (Wazow agent). The way we've set it up is that the Ubuntu machine is going to be connected to a bridged network adapter. So it looks like both of these machines are connected on the same network and they get the same IP address from my home router. Not the same IP address but they're pretty much on the same network. So both these devices can easily communicate with each other and you need two-way communication for your whole Wazow agent and Wazow manager system to work accurately. So now let's go into our Ubuntu server and check the IP address.



So this one's currently 192.168.0.217 and let's check our Windows IP address as well.

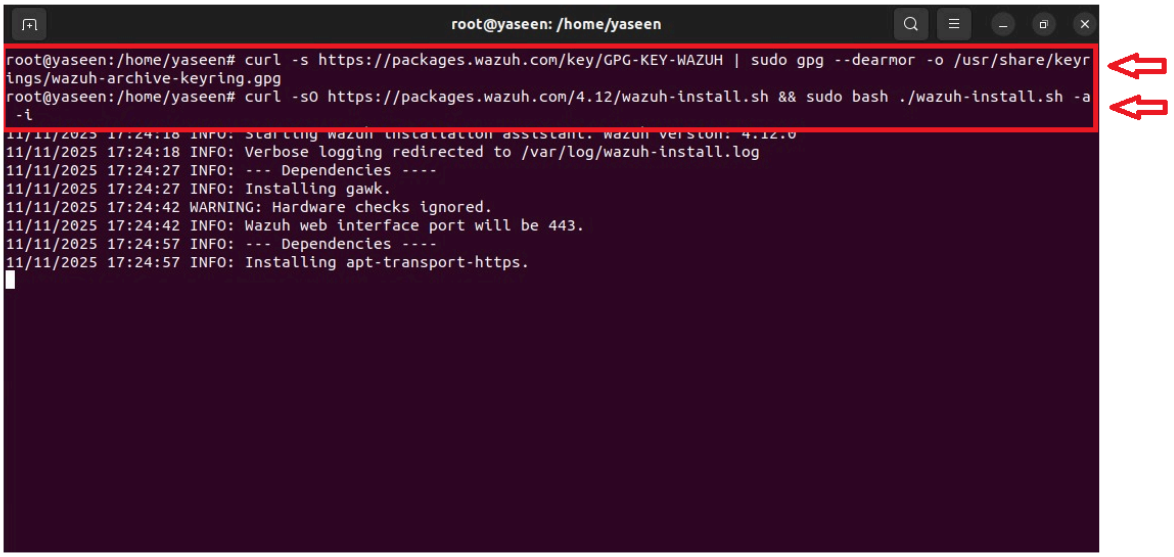


That is 192.168.0.35. So both of these are on the same network which is the 192.168.0.0/24

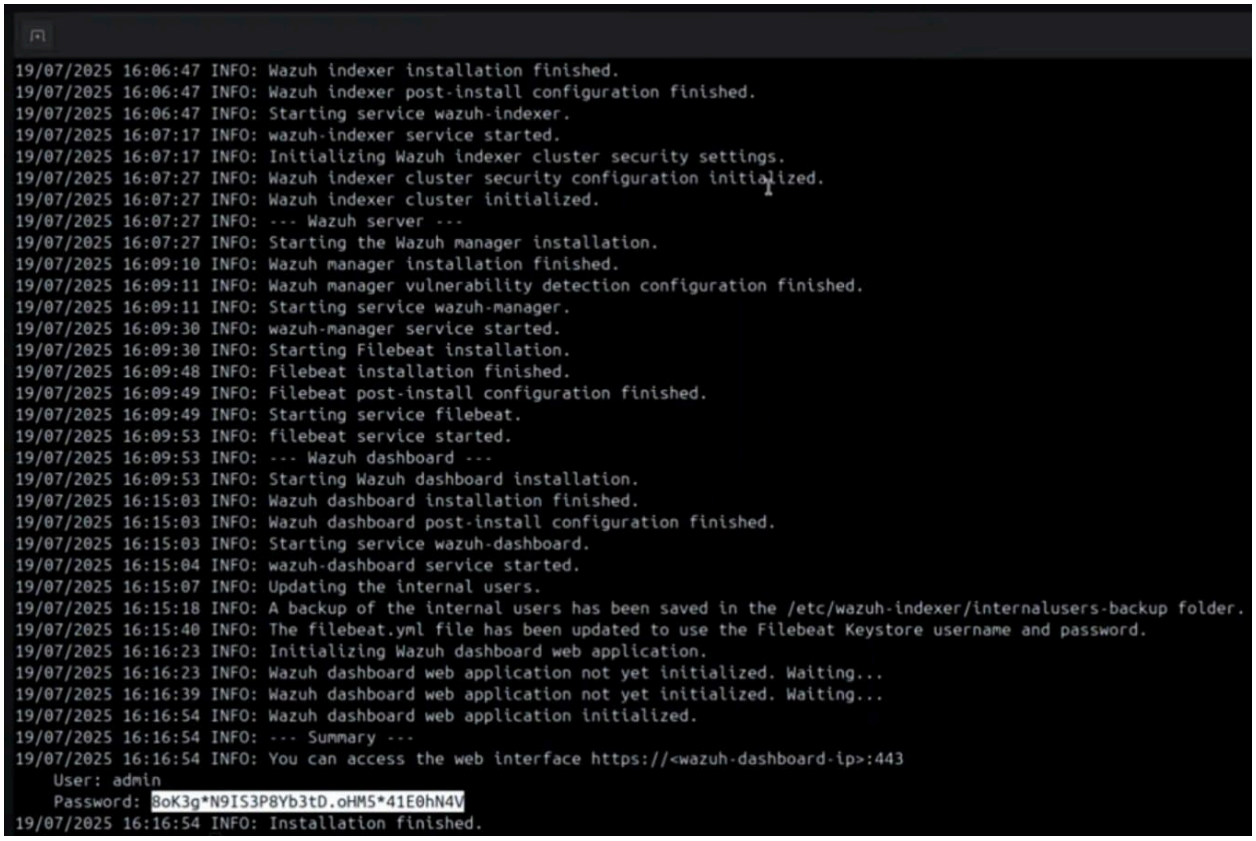
network which is exactly what we want from our lab setup.

Wazuh Manager Installation (Ubuntu)

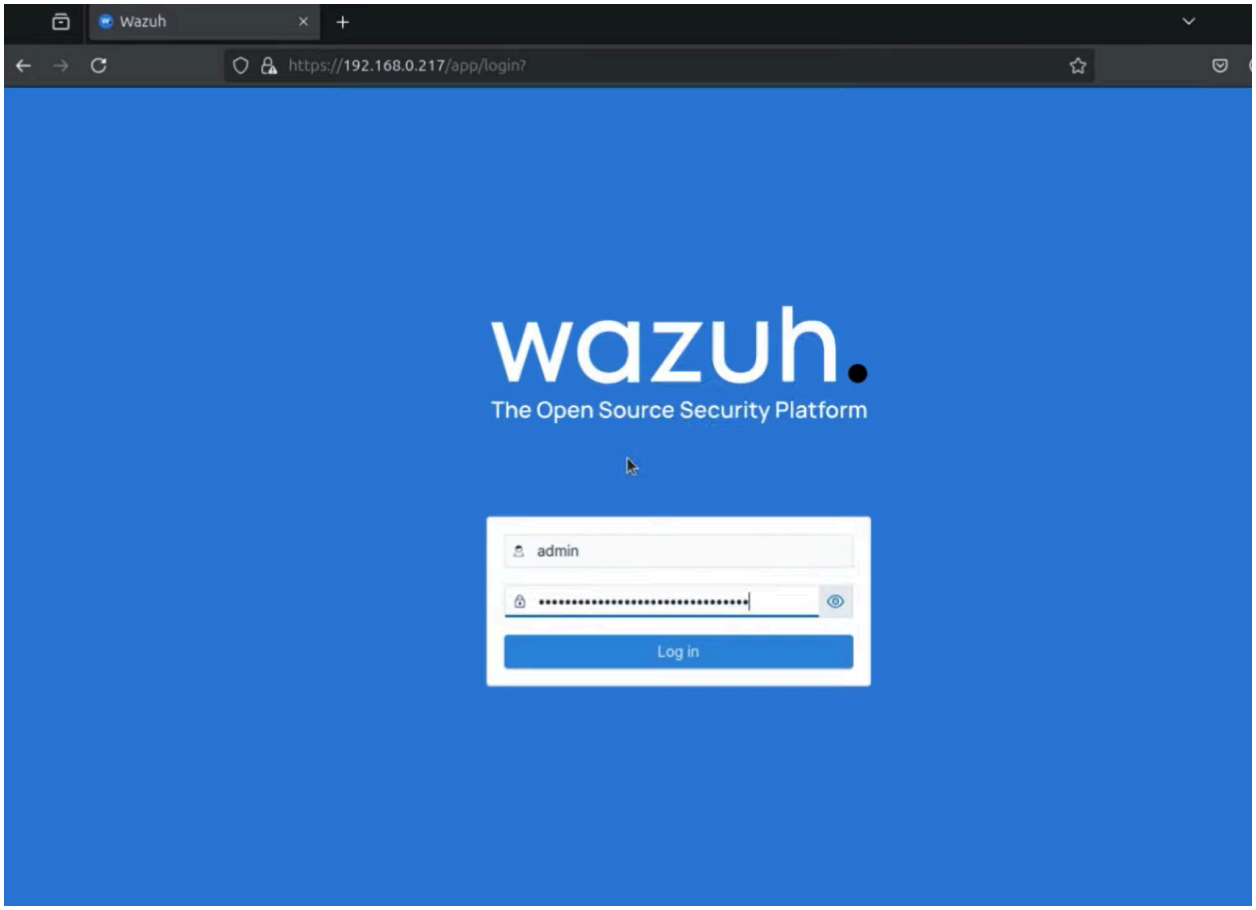
So before we do anything, let's go ahead and install our Wazow keyring for verification when we're installing and setting up our Wazow package. So we're going to use the installation command = curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | sudo gpg --dearmor -o /usr/share/keyrings/wazuh-archive-keyring.gp This will add the GPG for verification and just add the key to the keyring. Once that's done, we will then go ahead and run our installation command which is = curl -sO https://packages.wazuh.com/4.12/wazuh-install.sh && sudo bash ./wazuh-install.sh -a -i. So let's head back to our Ubuntu machine and let's wait for our Wazow installation which is currently going through the different steps.



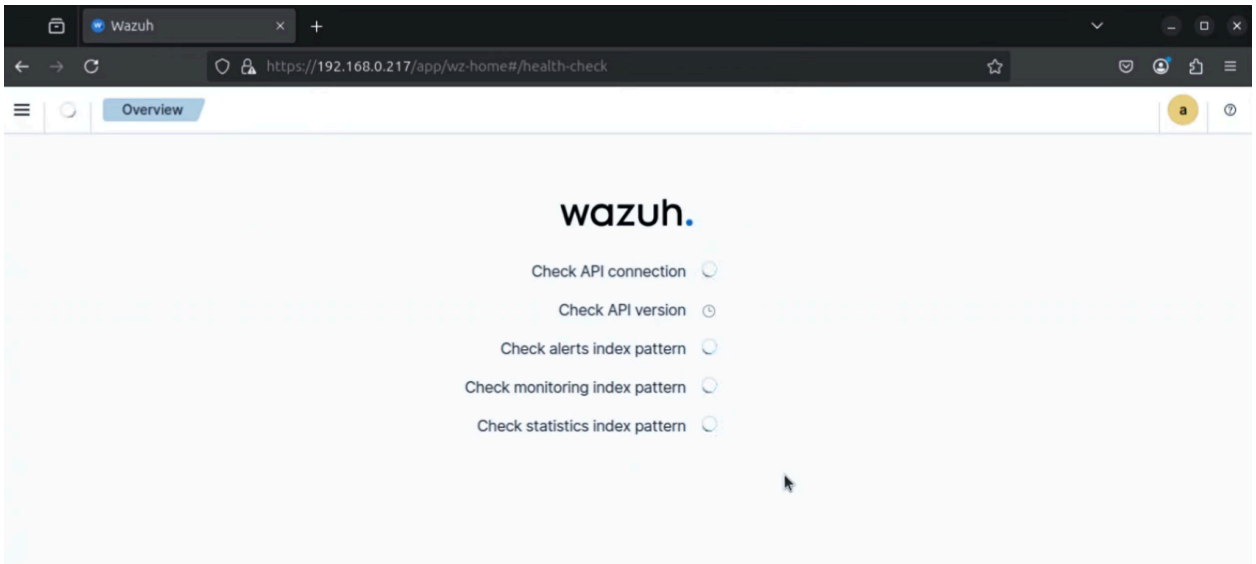
Your Wazuh Installer installs different components as part of its installation process, which includes the Wazuh indexer, the server, the dashboard, file beat, etc. But once the installation is done, which takes roughly about 10 minutes, you'll see that you can now access the web interface message on port 443, and it also gives you a username and a password which you can use to access your Wazuh dashboard.

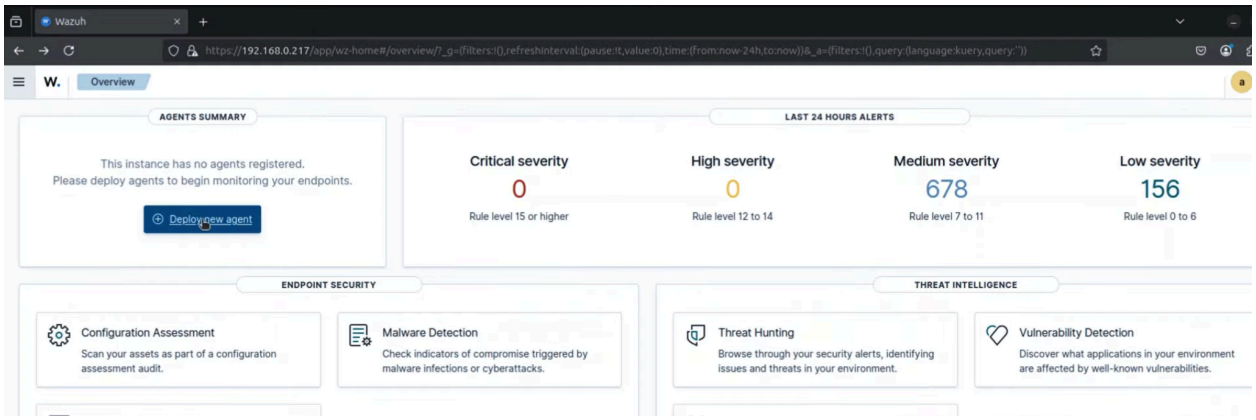


So copy this password. And let's go to our Wazuh dashboard, which is accessible on your machine's IP address. So let's quickly launch a Firefox window and go and check if the install is clean and completed successfully or not. So we'll add the IP address, which is 192.168.0.217.



So this is our Wazuh interface, and we'll add our username and password, which is admin, and the password, which we've just copied from the CLI window. We can see it's doing different checks. And I'm pretty excited and waiting for this to quickly load up so we can see what the user interface exactly looks like.

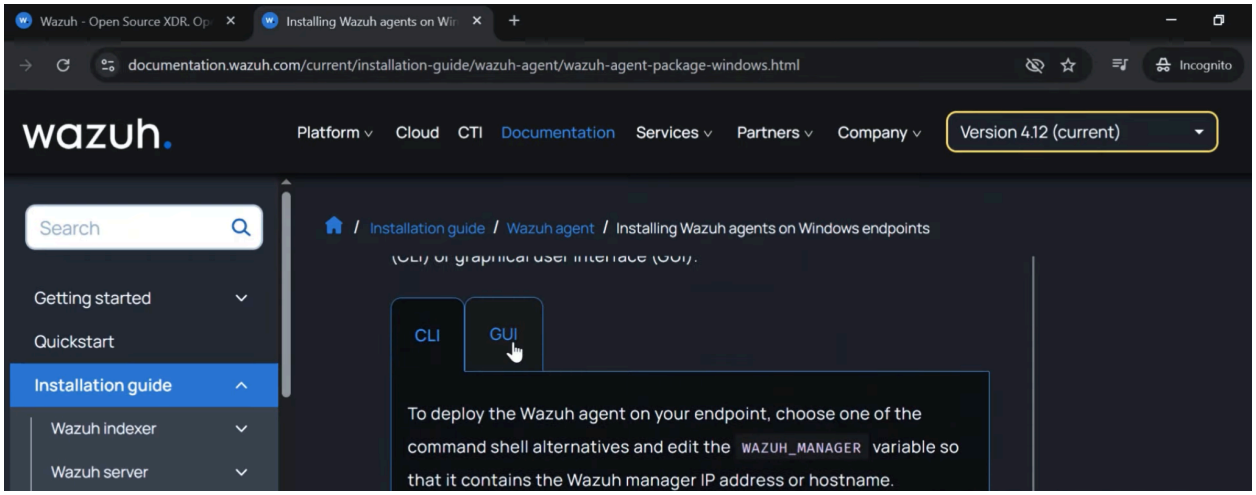




So this is what our Wazuh dashboard looks like. And you can have a play around, look at the different options that you can access within the Wazuh dashboard.

Wazuh Agent Installation (Windows).

Now I'm going to be installing our Wazuh Windows OS agent using this installation link = https://documentation.wazuh.com/current/installation-guide/wazuh-agent/wazuh-agent-package-windows.html. So lets just copy that and go to our Wazuh website so that we can install our Windows agent. So there are two methods.

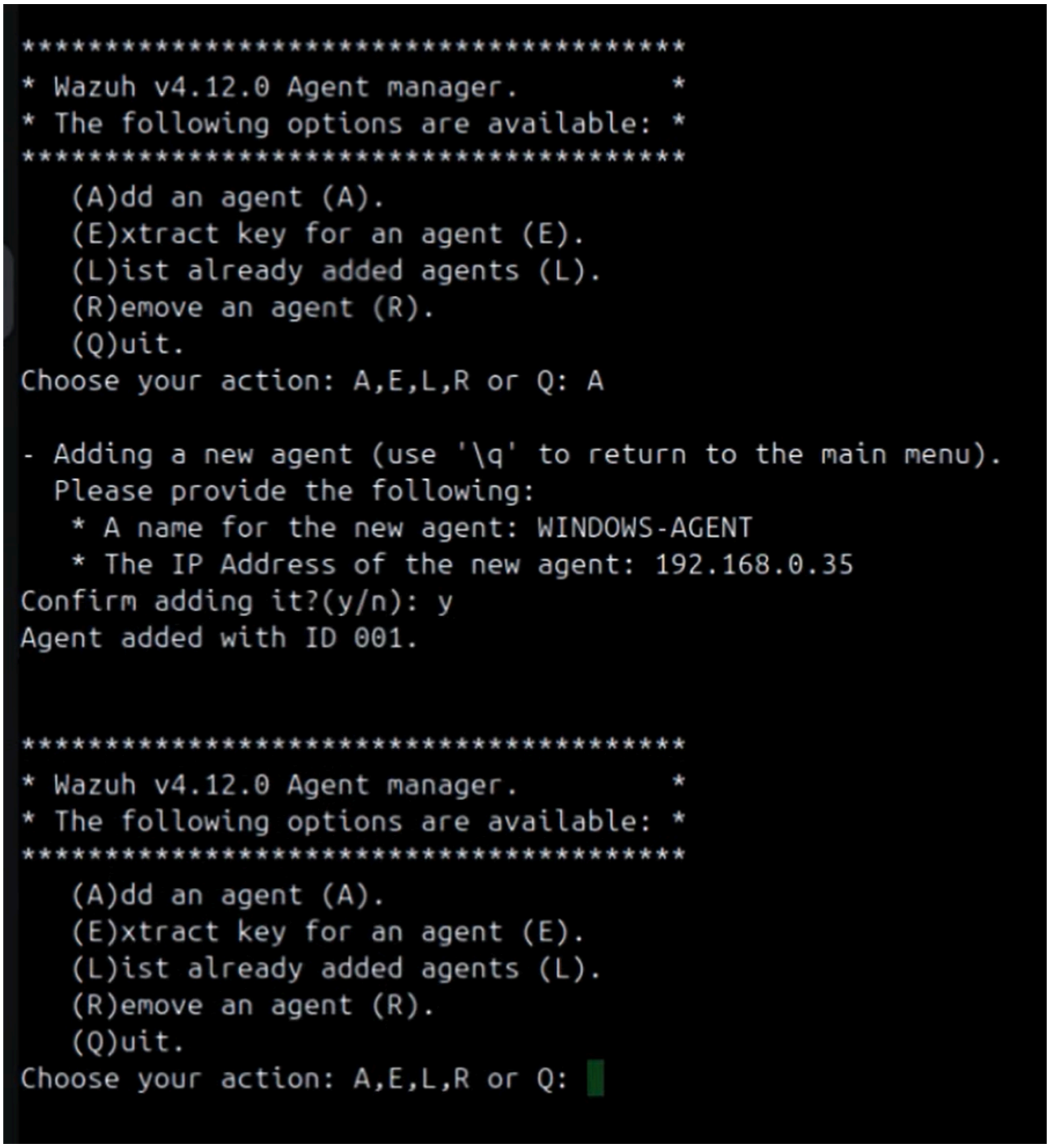


You can either do it using CLI or GUI. First, let's download the Windows installer.

And we'll save that in our computer. And let's run the Windows installer, accept the terms.

And let's go ahead and see what exactly happens while the Wazuh agent is installed. Once the agent installation is complete, you'll see a small window which says the Wazuh agent. And you've got a field to enter the manager's IP address. In our case, our manager is 192.168.0.217. So let's quickly do that.

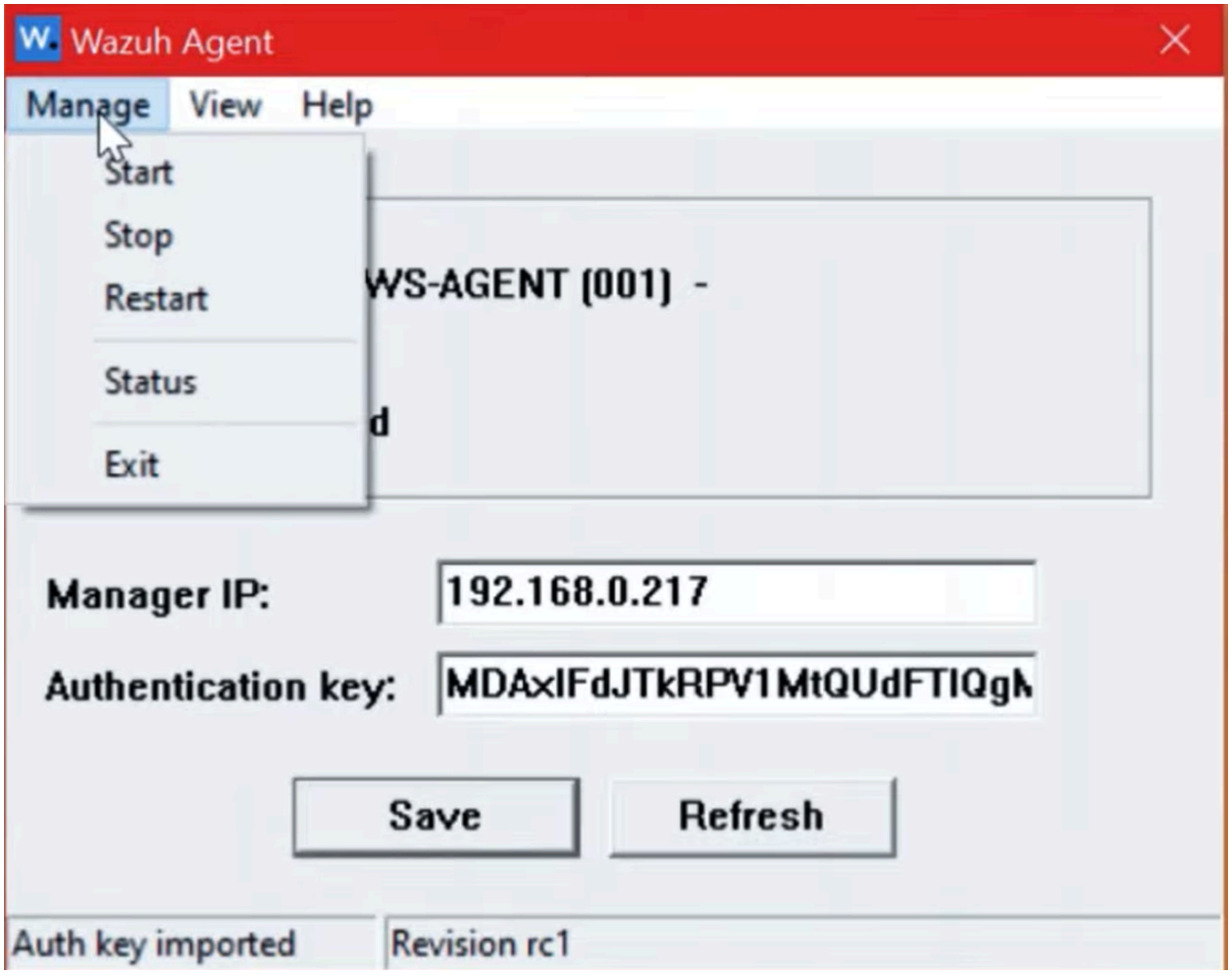
And also it's asking for an authentication key. Now, you need an authentication key so that the agent can then communicate with the server. So to do that, we first also got to add a manual entry of the Wazuh agent on our Wazuh manager (Ubuntu machine). So let's go back to our Ubuntu VM. So on our Ubuntu CLI, we'll run this command = sudo /var/ossec/bin/manage_agents, in order to manage our agents and add a new agent. And let's select one of the following actions. So in our case, we want to add an agent, so let's go A, Add. Let's give a name for the agent, so we'll call it Windows-Agent. And the IP address is 192.168.0.35. That's the IP address of my host Windows machine. All right, so it added an agent with an ID 001.



But other than this, I also want a key so that I can add that key on my Windows agent. So as per the menu options, that's option number E, which is to extract a key for an agent. And we give the ID number, which is 001.

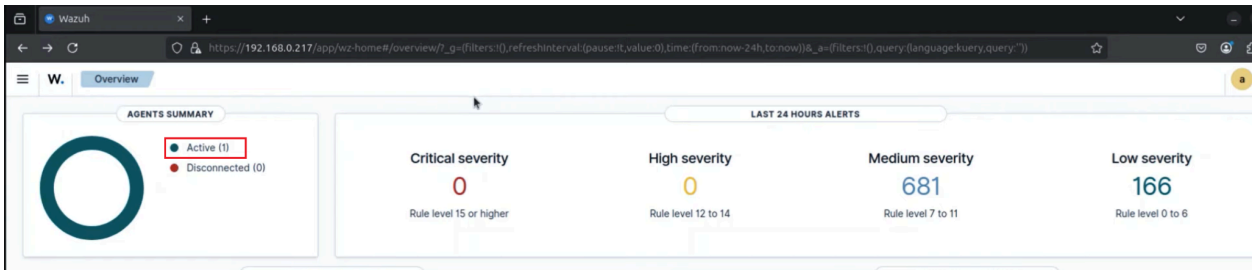
```
****************************************
* Wazuh v4.12.0 Agent manager.         *
* The following options are available: *
****************************************
   (A)dd an agent (A).
   (E)xtract key for an agent (E).
   (L)ist already added agents (L).
   (R)emove an agent (R).
   (Q)uit.
Choose your action: A,E,L,R or Q: E

Available agents:
   ID: 001, Name: WINDOWS-AGENT, IP: 192.168.0.35
Provide the ID of the agent to extract the key (or '\q' to quit): 001

Agent key information for '001' is:
MDAxIFdJTkRPV1MtQUdFTlQgMTkyLjE2OC4wLjM1IDhkZjk5YjM3NWFjMjU0N2QzNjQzNWY1ZjIwYzhlM2ZlMTkyMzAxMDkxMmM3MzYxNDlmYjljYTA1YmExMzk0Mjk=
```

And this is the Windows-Agent key. So let's copy this. And then let's go back to our Windows Wazuhagent and add the authentication key there. And once you do it, let's quickly restart our Wazuh agent server. So you go to Manage and Restart, and it says Agent Restarted.

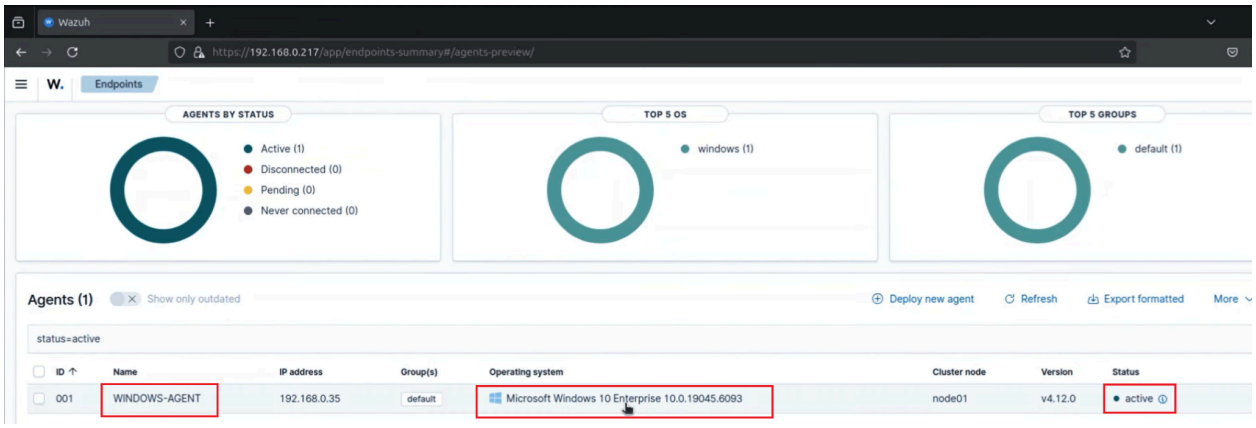


Verifying Agent Connection.

So once it's done, and if you go back to your WazuhUI on your server, we should now be able to see our Windows agent or our Windows machine. So let's quickly go and verify that. So on the Wazuhdashboard earlier, we could see an agent summary which was asking us to deploy a new agent. But now you can see that it says an agent is active.



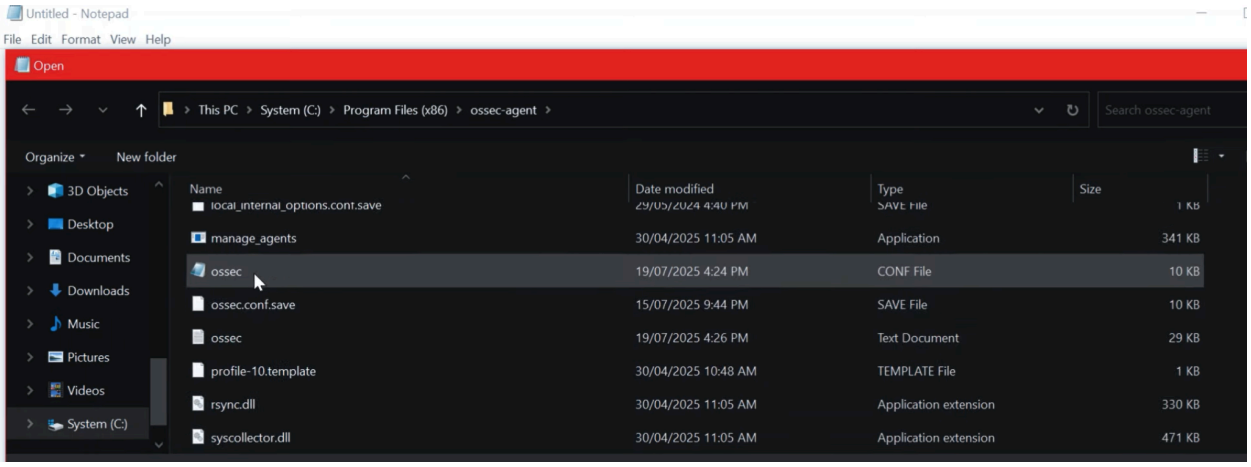
So let's click on it, and this should be our Windows machine which we've just added. So there you go. It's Windows-Agent. That's the agent name which we just added, and it's a Microsoft Windows 10 Enterprise with the number. And it's given it a cluster node of node 01. And the version here which is v.12.0 is the agent version because we're running agent 4.12.



So let's go into our Windows agent, and once we go here, we should be able to see all sorts of events, logs that are sent from our Windows machine which is our Wazuhagent to our Wazuh manager which is the Ubuntu machine. So once we've successfully added our Wazuhagent and we've got communication between the agent and the manager, we now demonstrate file and directory integrity monitoring.

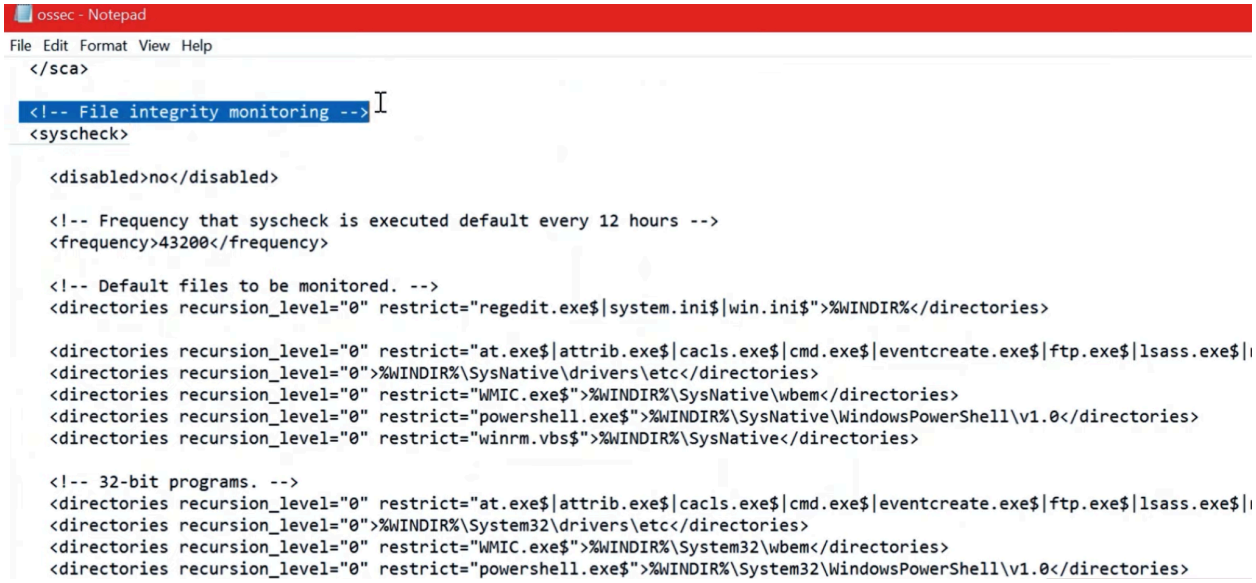
File and Directory Integrity Monitoring (FIM).

So now I will choose a specific directory to be monitored in our Wazuh agent configuration, and any changes such as creation of a new file, deletion of a file, any modifications within that specific directory that we're monitoring will then be visible in the form of logs of our Wazuh manager. That's amazing. You can have different endpoints running different agents, whether Linux, macOS, Windows OS, any types of operating systems you can run as agents, and all of those will send logs to your Wazuhmanager. So it's an amazing cybersecurity tool to set up and practice. So let's go to our agent configuration files, and our Wazuh agent config files are stored in program files and an OSSEC folder. To view the OSSEC config file, you've got to have administrator privileges. So what I'll do is I'll just go to the notepad as an administrator. And once I'm here, I will go in and open our OSSEC config file, which is under Program Files, OSSEC Agent. So this is our OSSEC config file.

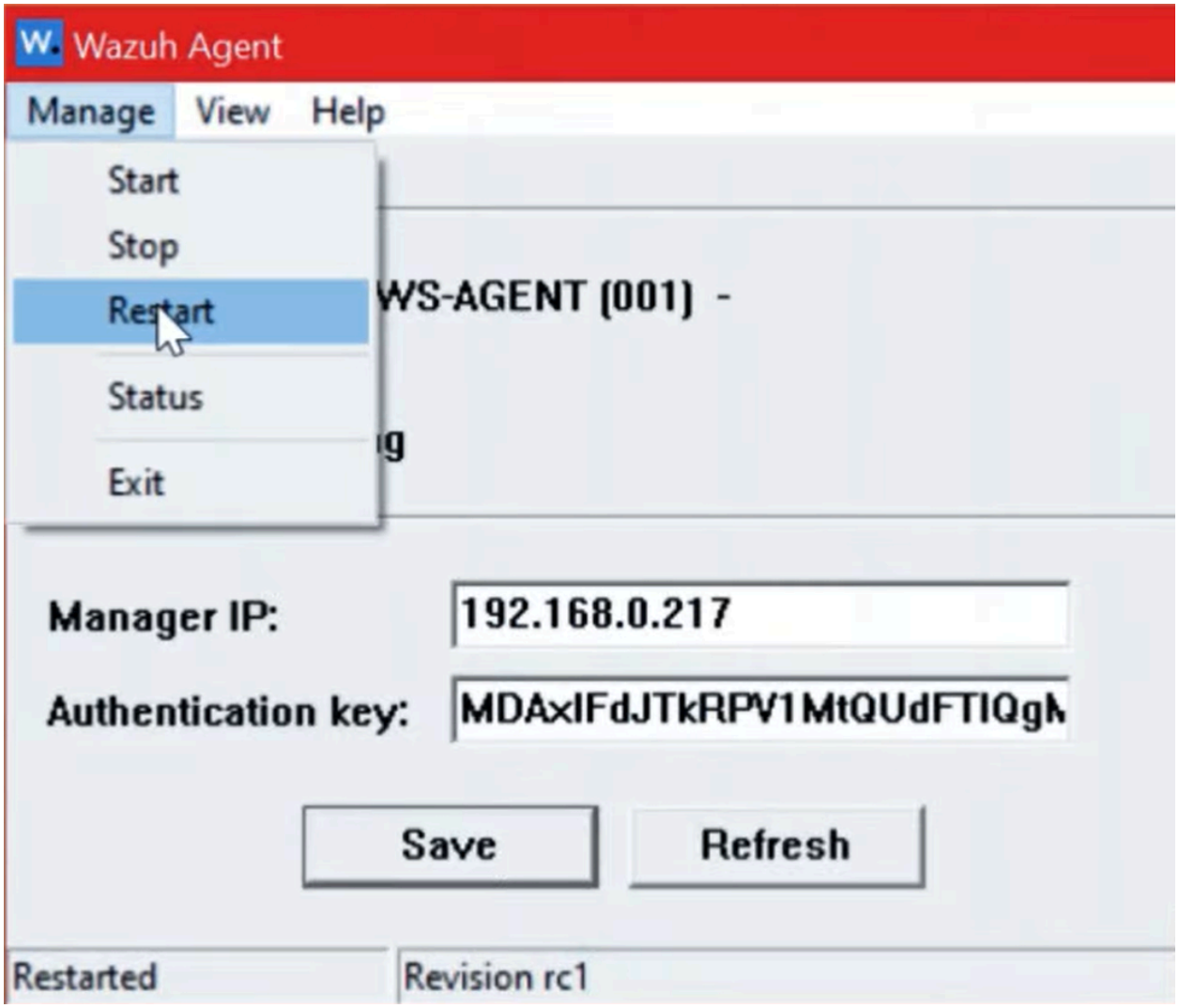


and if you want to see anything related to the WAS or Agent config, this is where you have a look. So as you can see, the manager IP address is here. The port number on which it sends all of these logs, which is 1514, is also listed. You can change whatever you want to change here.

Just make sure that you restart the agent service and also ensure that it's also changed on the manager and others. You'll have incompatibilities and stuff. It's not going to work. So let's quickly go and add a new directory for our file monitoring. So in the config section, you can see there's a portion here which says File Integrity Monitoring

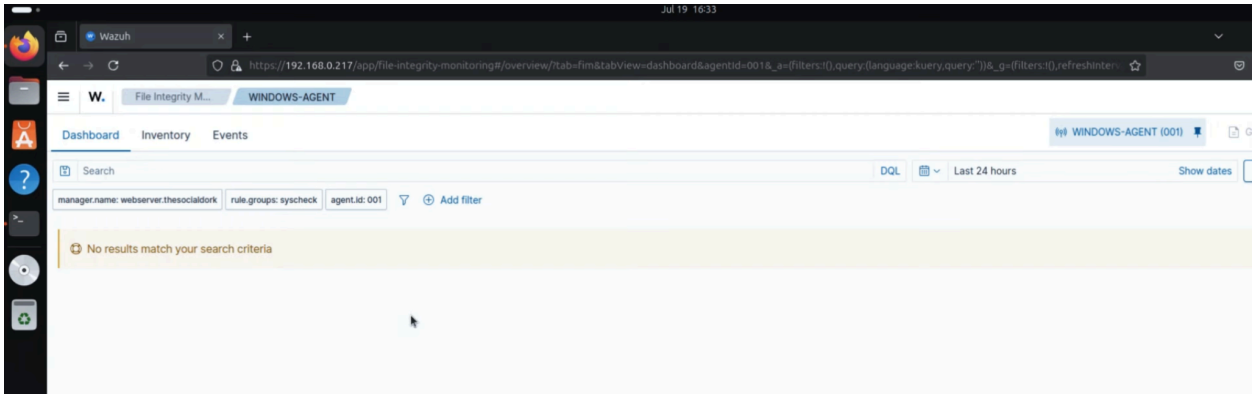


And here there are default files to be monitored with different directories and their paths listed. So I'm going to be adding a new path, which I want to be monitored as well. So I'm copying this file path = <directories realtime="yes">C:\Users\Yaseen\Downloads\WAZUH-TEST</directories>. So I've created a different directory here, which goes by the name of Wazuh Test. So let's copy the directory and paste it in there. We'll save that by Control-S. So once again, you go to File Integrity Monitoring. And in that section, you add the following line. And the path needs to be to the folder that you want to monitor. So that's what I've done. I've saved it. I'm going to close this configuration. And what I'll do is I will restart my agent once again.

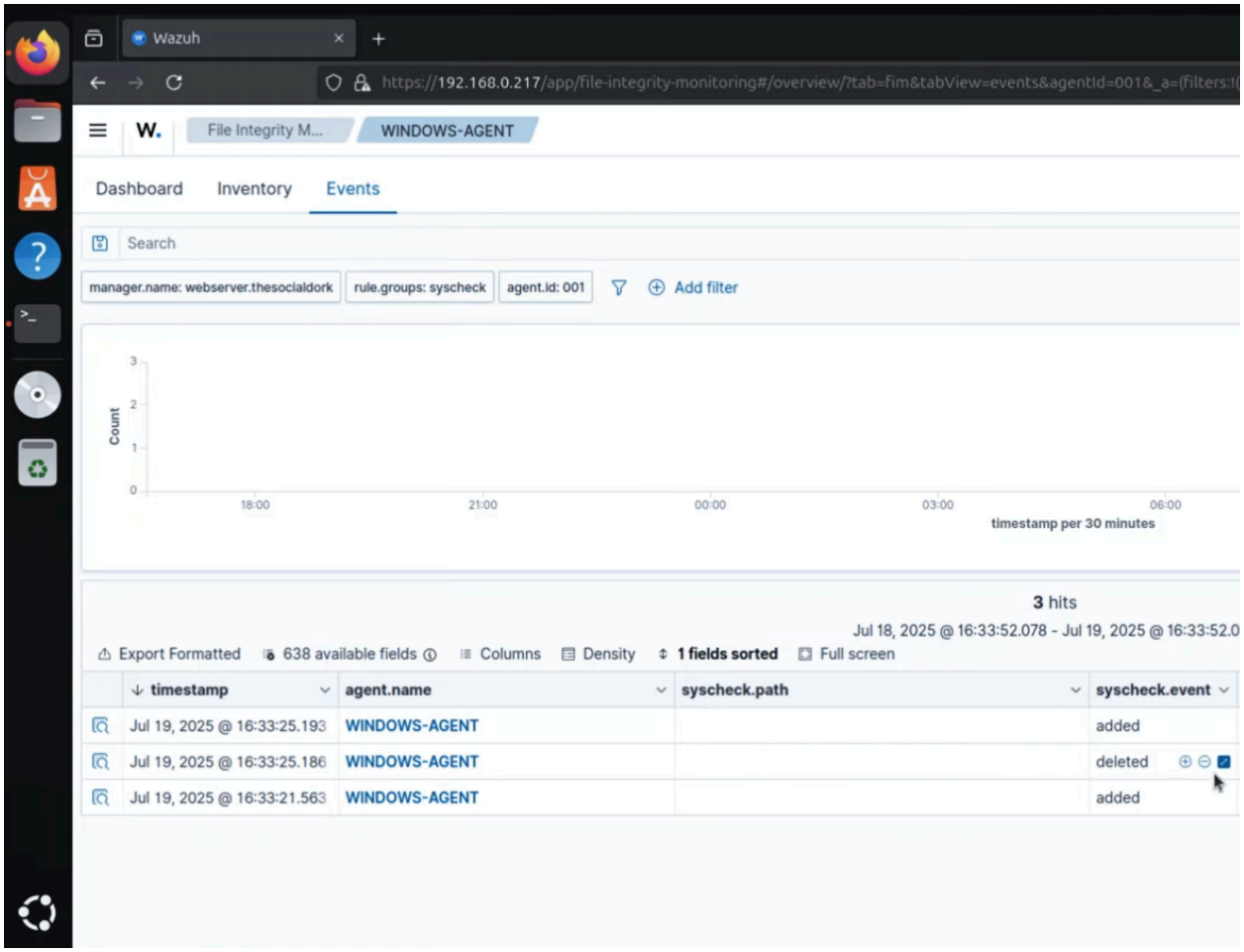


Generating and Monitoring Logs.

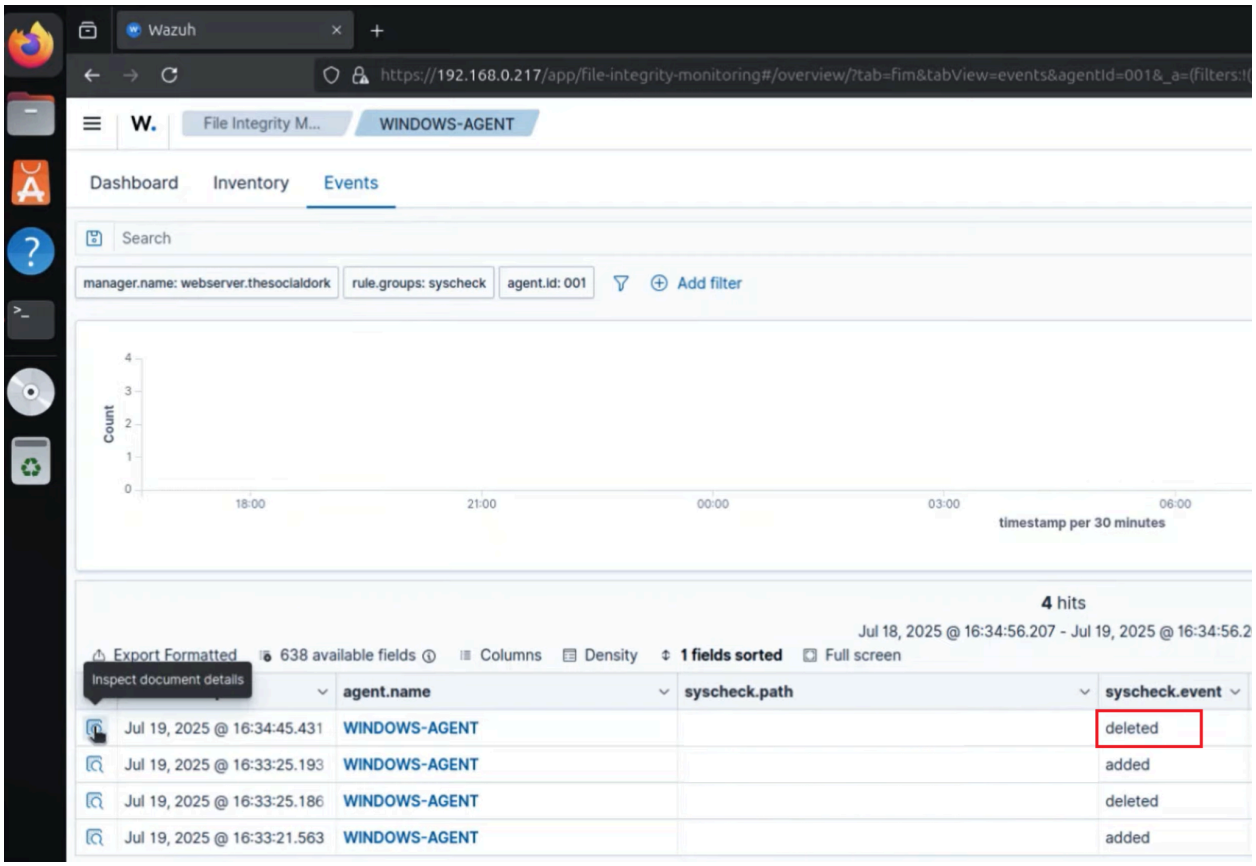
So now I'm going to my Wazuh Manager, I'm going to go to File Integrity Monitoring. And currently, we shouldn't have any events because we haven't generated any events.



So as you can see, it's completely empty right here. So what we'll do is let's quickly go to the windows (Wazuh agent) and in that directory and create a new file. Let's create a New Text Document and call it Test 1. And let's save that here. So once that's done, we go back to our Wazuh Manager, and we should be seeing some logs if we refresh on our Windows agent. So let's quickly have a look and see what exactly shows up.



So here you can see we've got all the details related to the file that's currently added to the system. So let's inspect what the document is. So it says that it shows you the agent IP. It also shows you the file name that you've created. So let's quickly have a look. There you go. This is the full log, which is test1.txt. So that's the exact file that I created in that directory. So one more thing we can do is let's quickly go and delete that specific file now. So let's delete the file which we have created with the name WAZUH-TEST. And once we do this and we get back to our Wazuh Manager, we should then see the deletion of that file as well. So let's refresh once again and give it a couple of seconds. There you go. So we see a file deleted log as well. And upon inspecting, it says test1.txt is deleted.



Practical Outcome.

What we did, what we intended to achieve, we've completely achieved as far as this goes. We performed a Wazuh Manager installation. We performed a Wazuh Agent installation. We then also demonstrated a file integrity monitoring test, which was done by specifying a specific folder in our Wazuh Agent configuration files, which any changes when made to that folder then showed different types of logs on our Wazuh Agent. And this is exactly how real-world systems absolutely function and look like. So if you're looking to be a SOC analyst or a cybersecurity engineer, make sure you practice these home labs.