Updated Jan 28, 2023

Lab 3.2 - Wazuh

> 💡You've seen what a centralized syslog server can do in terms of receipt and organization of log files from across the enterprise. In this new lab, we are going to experiment with a far more modern logging system called Wazuh. Wazuh is one of several ELK based SIEMs. We are using this one because of the relatively ease of installation as well as functionality. Unlike a traditionally syslog client and server, Wazuh allows us to install agents on supported systems. Agents can refine that information sent to their SIEM for streamlined analysis.

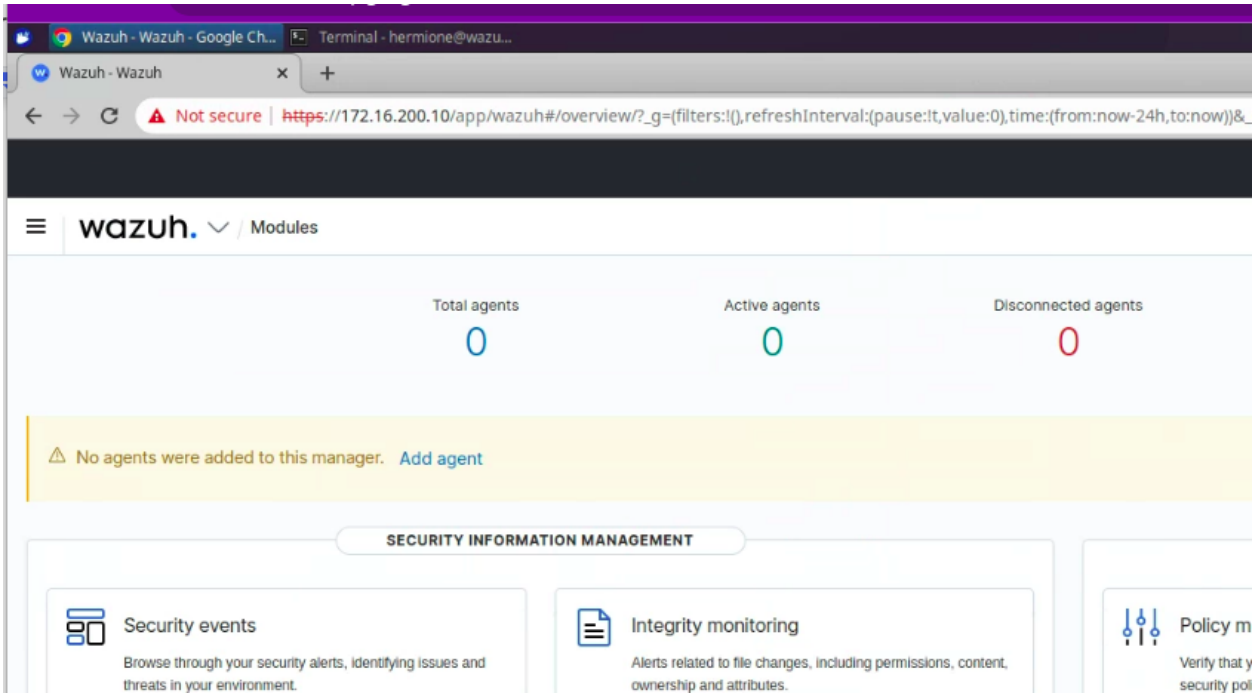
Installation

For a single node installation on wazuh, run the following command.

```
curl -sO https://packages.wazuh.com/4.3/wazuh-install.sh && sudo bash
./wazuh-install.sh -a
```

> 💡It's a good idea to look at these remote installers before blindly run them through sudo. Take note of your admin password, put it in a password manager for now. It is read only and will require modifications to the configuration later to change it. Don't complain if you lose it.

`Deliverable 1. A screenshot that clearly shows your wazuh server as accessed via mgmt01 similar to the one below`



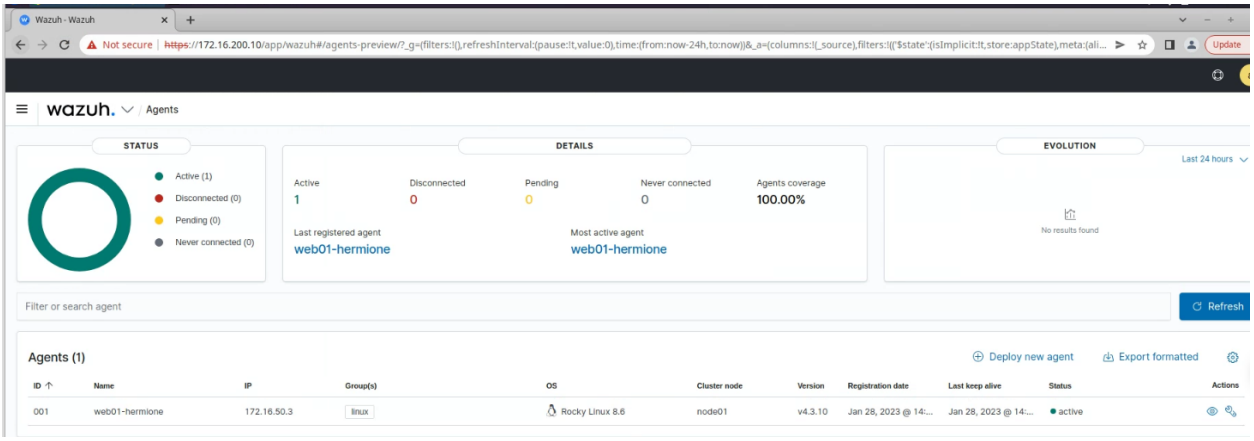
Updated Jan 28, 2023

Wazuh/OSSEC Agent on web01

Find the groups screen in Wazuh, create a new group called linux
Find the agents screen in Wazuh, Deploy a new agent with the following configuration.

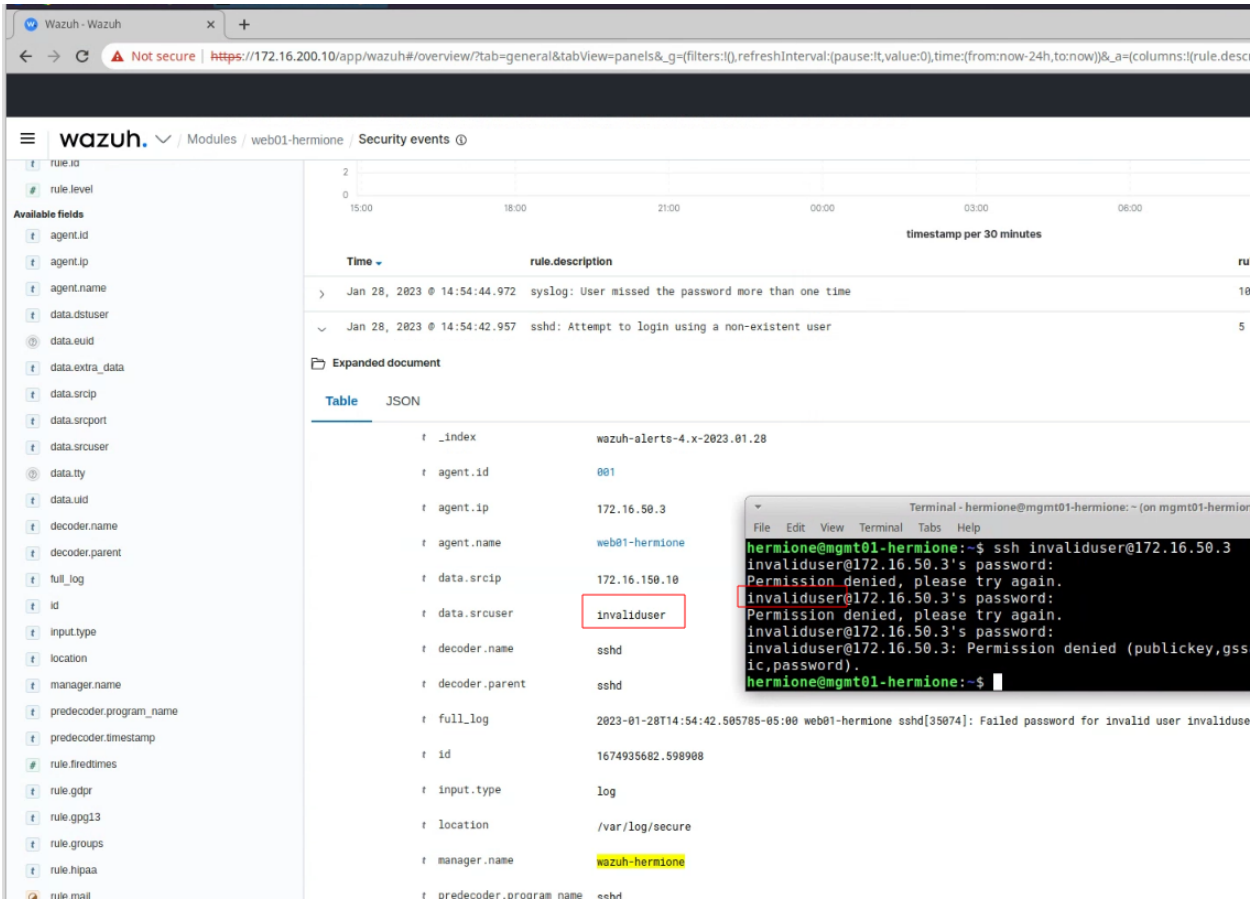
1. Redhat/CentoS
2. CentOS 6 or higher (Note, it will work on rocky 8)
3. x86_64
4. 172.16.200.10
5. linux
6. Run this command on your web01 server
7. Start the Wazuh agent on web01

`Deliverable 2.  Provide a wazuh screenshot that shows the registered agent on web01`



Updated Jan 28, 2023

Deliverable 3. Attempt an ssh login using an invalid user on web01 similar to the screenshot below. Search web01's wazuh security events until you find the associated event.



💡You may be asking yourself about the usefulness of syslog data. The content above suggests that agent based reporting is far more useful. That said, there are network devices and applications that don't natively support the installation of agents. SYSLOG is usually a common denominator on these devices and can be leveraged to gain visibility into remote events. We will be using a combination of wazuh agents and syslog to accomplish this.

Deliverable 4.
Create a wazuh article in your tech journal. Cover the installation of the server, including the firewall commands required as well as agent installation. Find out where the agent files are located and peruse that directory structure.