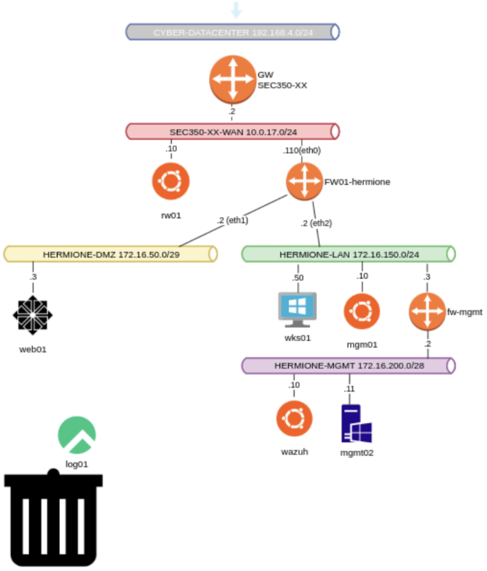
Updated Sep 8, 2023

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.


CYBER-DATACENTER 192.168.4.0/24
GW
SEC350-XX
.2
SEC350-XX-WAN 10.0.17.0/24
.10
rw01
.110(eth0)
FW01-hermione
.2 (eth1)
.2 (eth2)
HERMIONE-DMZ 172.16.50.0/29
.3
web01
HERMIONE-LAN 172.16.150.0/24
.50
wks01
.10
mgm01
.3
fw-mgmt
.2
HERMIONE-MGMT 172.16.200.0/28
.10
wazuh
.11
mgmt02
log01

Installation

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

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

(NOTE: added -i to ignore minimum requirements of 2CPU and 4 GB RAM

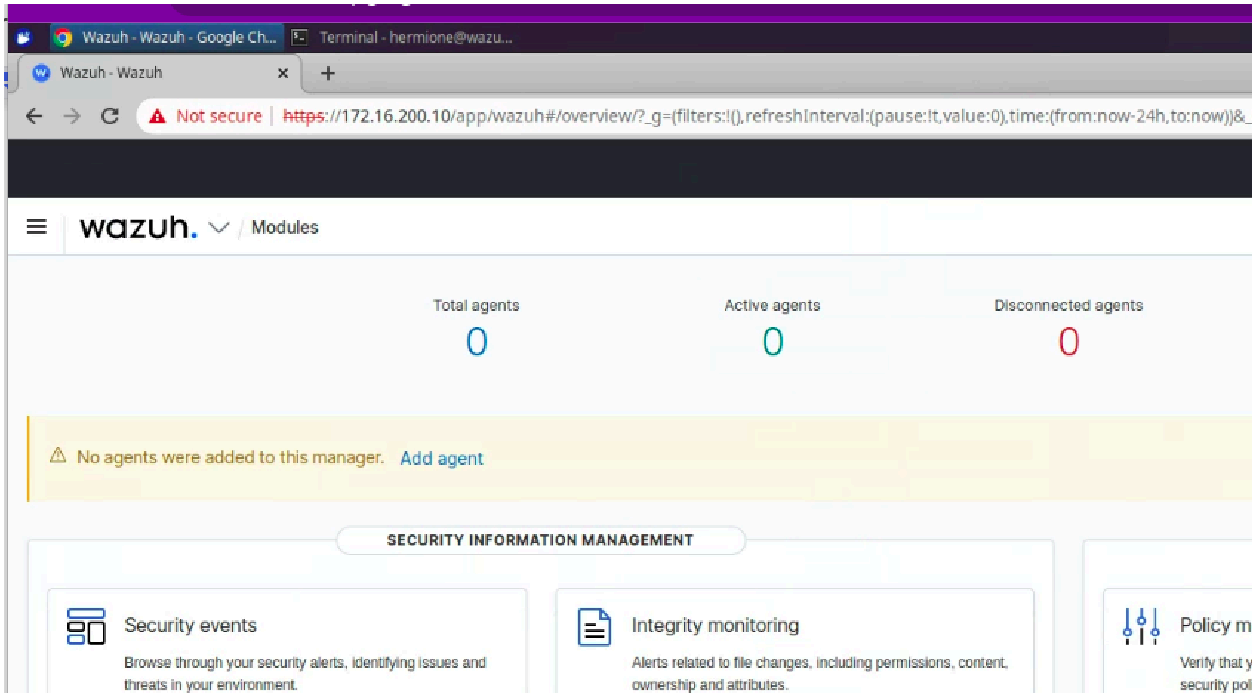
> 💡It's a good idea to look at these remote installers before blindly run them through sudo. **Take note of your admin password, put it in a password manager for now. It is read only and will require modifications to the configuration later to change it. Don't complain if you lose it.**

NOTE: Takes a while for the server to run - at the end you should see something like:

Updated Sep 8, 2023

“You can access the web interface https://<wazuh-dashboard-ip>
User: admin
Password: <a longish random password> **Make note of this!**

You can then log into the Wazuh web dashboard from a browser tab on mgmt01
Deliverable 1. A screenshot that clearly shows your wazuh server as accessed via mgmt01 similar to the one below



Not secure | ~~https~~://172.16.200.10/app/wazuh#/overview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_

Total agents 0

Active agents 0

Disconnected agents 0

⚠ No agents were added to this manager. Add agent

SECURITY INFORMATION MANAGEMENT

Security events
Browse through your security alerts, identifying issues and threats in your environment.

Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.

Policy m
Verify that y
security poli

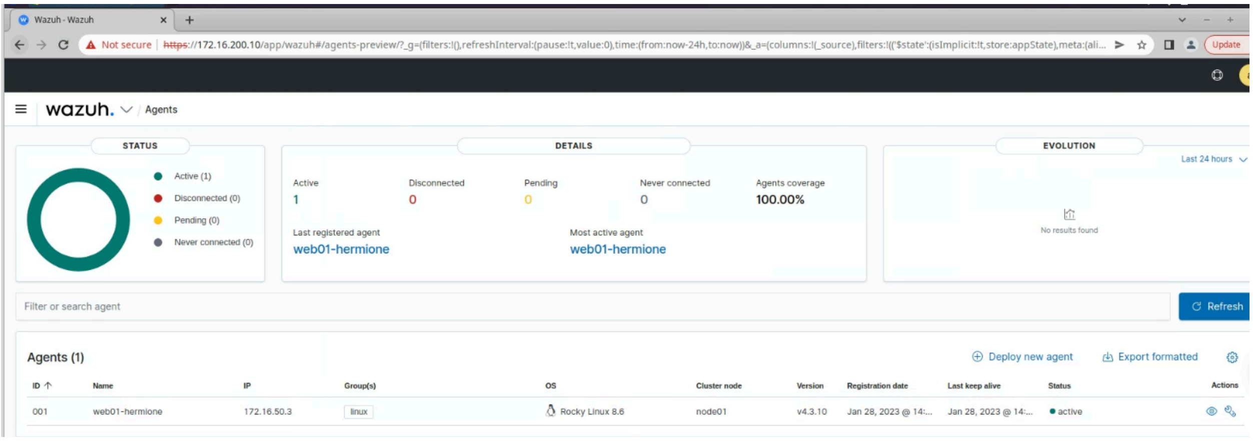
Wazuh/OSSEC Agent on web01

1. Find the groups screen in Wazuh, create a new group called linux
2. 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. This will give you the syntax for a command that you can run on Web01 to install the agent

    7. Run the command on your web01 server
    8. Use the systemctl commands provided by Wazuh to Start the Wazuh agent on web01

Updated Sep 8, 2023

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


Wazuh - Wazuh
Not secure
https://172.16.200.10/app/wazuh#/agents-preview/?_g=(filters:!(),refreshInterval:(pause:!t,value:0),time:(from:now-24h,to:now))&_a=(columns:!(_source),filters:!(('$state':(isImplicit:!t,store:appState),meta:(ali...
Update
wazuh.
Agents
STATUS
Active (1)
Disconnected (0)
Pending (0)
Never connected (0)
DETAILS
EVOLUTION
Last 24 hours
No results found
Filter or search agent
Refresh
Deploy new agent
Export formatted

Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	0	100.00%

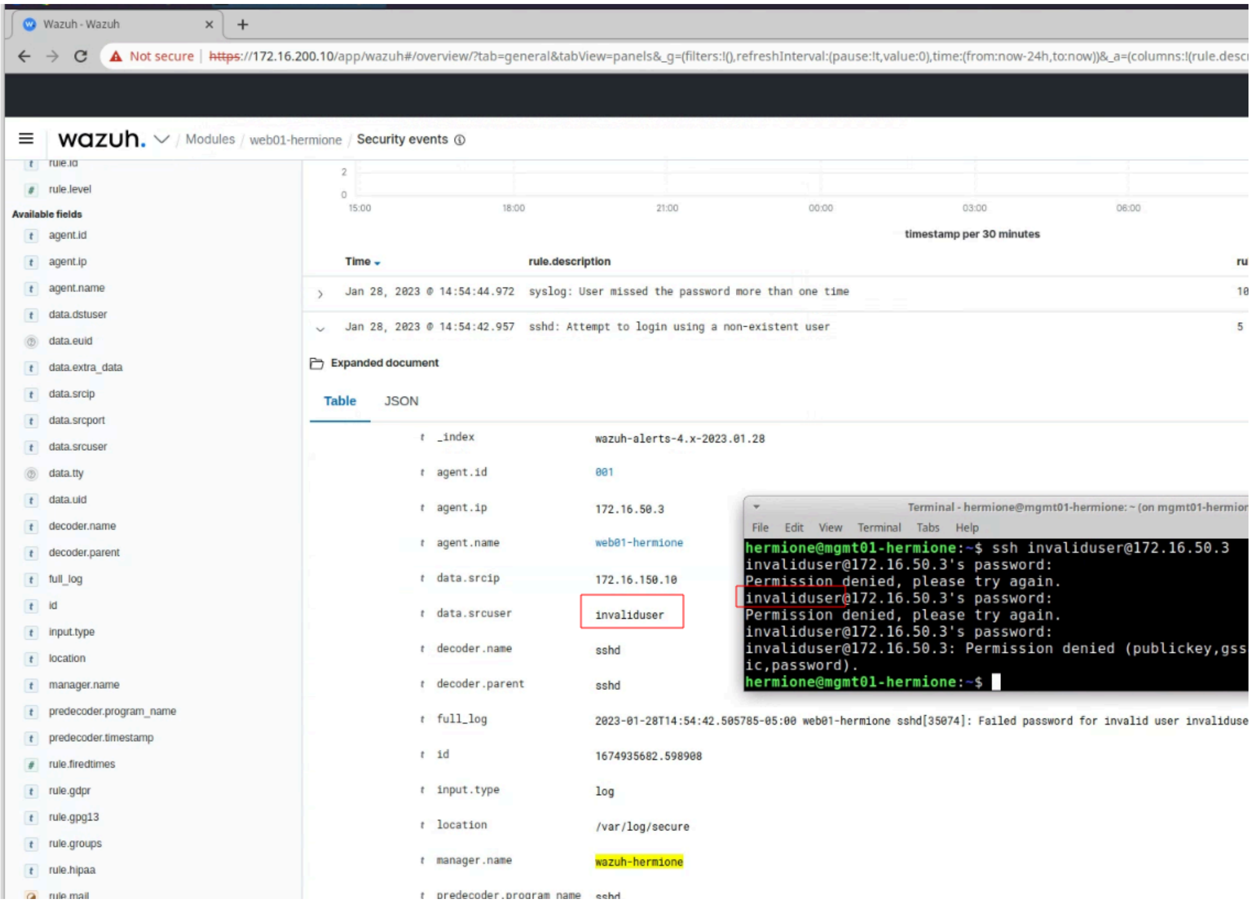
Last registered agent web01-hermione

Most active agent web01-hermione

Agents (1)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	web01-hermione	172.16.50.3	linux	Rocky Linux 8.6	node01	v4.3.10	Jan 28, 2023 @ 14:...	Jan 28, 2023 @ 14:...	● active	

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.



```
Time          rule.description                                              ru
Jan 28, 2023 @ 14:54:44.972  syslog: User missed the password more than one time   10
Jan 28, 2023 @ 14:54:42.957  sshd: Attempt to login using a non-existent user      5
```

```
t _index                    wazuh-alerts-4.x-2023.01.28
t agent.id                  001
t agent.ip                  172.16.50.3
t agent.name                web01-hermione
t data.srcip                172.16.150.10
t data.srcuser              invaliduser
t decoder.name              sshd
t decoder.parent            sshd
t full_log                  2023-01-28T14:54:42.505785-05:00 web01-hermione sshd[35074]: Failed password for invalid user invaliduse
t id                        1674935682.598908
t input.type                log
t location                  /var/log/secure
t manager.name              wazuh-hermione
t predecoder.program_name   sshd
```

Terminal - hermione@mgmt01-hermione: ~ (on mgmt01-hermion

File Edit View Terminal Tabs Help

```
hermione@mgmt01-hermione:~$ ssh invaliduser@172.16.50.3
invaliduser@172.16.50.3's password:
Permission denied, please try again.
invaliduser@172.16.50.3's password:
Permission denied, please try again.
invaliduser@172.16.50.3's password:
invaliduser@172.16.50.3: Permission denied (publickey,gss
ic,password).
hermione@mgmt01-hermione:~$
```

Updated Sep 8, 2023

💡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 agent installation.  Find out where the
agent files are located and peruse that directory structure.
```