

🔧 Cybersecurity Lab: Day 2 — Setting Up Wazuh Agent on Red Hat Server

✅ Objectives Completed:

1. Prepared Red Hat Server for Wazuh Agent

- Verified internet connection.
- Confirmed basic server readiness (Apache and SSH running).

Chose to install wazuh agent on redhat remotely using ssh

2. Added Wazuh Repository on Red Hat Server

- Logged into the Red Hat server via SSH from the Kali machine.

Ssh username@<ip>

```
(kali@kali)-[~]
└─$ ssh ilya@10.0.2.4
ilya@10.0.2.4's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Thu May  8 19:20:34 2025
[ilya@localhost ~]$
[ilya@localhost ~]$
[ilya@localhost ~]$
[ilya@localhost ~]$ sudo rpm --import https://packages.wazuh.com/key/GPG-KEY-
WAZUH
[sudo] password for ilya:
```

- Added the Wazuh repository to the Red Hat server:

sudo rpm --import https://packages.wazuh.com/key/GPG-KEY-

```
[ilya@localhost ~]$ sudo rpm --import https://packages.wazuh.com/key/GPG-KEY-
WAZUH
[sudo] password for ilya:
[ilya@localhost ~]$ cat << EOF | sudo tee /etc/yum.repos.d/wazuh.repo
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
EOF
[wazuh]
gpgcheck=1
gpgkey=https://packages.wazuh.com/key/GPG-KEY-WAZUH
enabled=1
name=EL-$releasever - Wazuh
baseurl=https://packages.wazuh.com/4.x/yum/
protect=1
[ilya@localhost ~]$ sudo yum clean all
```

3. Installed Wazuh Agent on Red Hat Server Remotely via SSH

`sudo yum install wazuh-agent -y`

```
Metadata cache created.
[ilya@localhost ~]$ sudo yum install wazuh-agent -y
Updating Subscription Management repositories.
Last metadata expiration check: 0:01:25 ago on Thu 08 May 2025 08:00:59 PM EDT.
Dependencies resolved.

Package                Architecture Version      Repository    Size
Installing:
wazuh-agent            x86_64      4.12.0-1    wazuh         9.6 M

Transaction Summary
Install 1 Package
```

4. Configured Agent to Connect to Wazuh Server

- Edited the `ossec.conf` file on the Red Hat server:

`sudo nano /var/ossec/etc/ossec.conf`

- Set the Wazuh manager IP (10.0.2.6): edit this part only

```
<server>

<address>10.0.2.6</address>

<protocol>tcp</protocol>

</server>
```

5. Started Wazuh Agent and Verified Status

- Started and enabled the agent service on the Red Hat server:

```
[ilya@localhost ~]$ sudo systemctl status wazuh-agent
● wazuh-agent.service - Wazuh agent
   Loaded: loaded (/usr/lib/systemd/system/wazuh-agent.service; disabled; vendor preset: enabled)
   Active: active (running) since Thu 2025-05-08 20:10:52 EDT; 13s ago
     Process: 10418 ExecStart=/usr/bin/env /var/ossec/bin/wazuh-control start (code=0)
    Tasks: 28 (limit: 23006)
   Memory: 49.2M
      CPU: 8.123s
   CGroup: /system.slice/wazuh-agent.service
           └─10446 /var/ossec/bin/wazuh-execd
             └─10458 /var/ossec/bin/wazuh-agentd
               └─10472 /var/ossec/bin/wazuh-syscheckd
                 └─10486 /var/ossec/bin/wazuh-logcollector
                   └─10504 /var/ossec/bin/wazuh-modulesd

May 08 20:10:43 localhost.localdomain systemd[1]: Starting Wazuh agent ...
May 08 20:10:43 localhost.localdomain env[10418]: Starting Wazuh v4.12.0 ...
May 08 20:10:45 localhost.localdomain env[10418]: Started wazuh-execd ...
May 08 20:10:46 localhost.localdomain env[10418]: Started wazuh-agentd ...
```

6. Verified Agent Connection from Wazuh Manager

- From the Wazuh server, confirmed the agent connection:

```
valid_lft forever preferred_lft forever
wazuh-user@wazuh-server ~]$ sudo /var/ossec/bin/agent_control -l

wazuh agent_control. List of available agents:
  ID: 000, Name: wazuh-server (server), IP: 127.0.0.1, Active/Local
  ID: 001, Name: localhost.localdomain, IP: any, Active

List of agentless devices:

wazuh-user@wazuh-server ~]$ sudo systemctl enable wazuh-manager
wazuh-user@wazuh-server ~]$
```

Troubleshooting steps done: The Wazuh agent on the RedHat server was not connecting to the Wazuh Manager, and the following steps were done

1. Allow connection through the ports chosen

```
[ilya@localhost ~]$ sudo firewall-cmd --permanent --add-port=1514/udp
sudo firewall-cmd --permanent --add-port=1515/tcp
sudo firewall-cmd --reload
[sudo] password for ilya:
success
success
success
[ilya@localhost ~]$
```

Outcome: Did not solve the problem but useful.

2. Check the config files for correct ip address to server

- `sudo nano /var/ossec/etc/ossec.conf`

finding :the ip address was correctly set

3. checked the log files

sudo tail -f /var.....

finding: an error the agent and server were of different version

correction: re installed the current version of wazuh server

```
[ilya@localhost ~]$ sudo tail -f /var/ossec/logs/ossec.log
2025/05/08 21:19:55 wazuh-agentd: INFO: Using agent name as: localhost.localdomain
2025/05/08 21:19:55 wazuh-agentd: INFO: Waiting for server reply
2025/05/08 21:19:55 wazuh-agentd: ERROR: Agent version must be lower or equal to manager version (from manager)
2025/05/08 21:19:55 wazuh-agentd: ERROR: Unable to add agent (from manager)
2025/05/08 21:20:20 wazuh-agentd: INFO: Requesting a key from server: 10.0.2.6
2025/05/08 21:20:20 wazuh-agentd: INFO: No authentication password provided
2025/05/08 21:20:20 wazuh-agentd: INFO: Using agent name as: localhost.localdomain
2025/05/08 21:20:20 wazuh-agentd: INFO: Waiting for server reply
2025/05/08 21:20:20 wazuh-agentd: ERROR: Agent version must be lower or equal to manager version (from manager)
2025/05/08 21:20:20 wazuh-agentd: ERROR: Unable to add agent (from manager)
2025/05/08 21:20:50 wazuh-agentd: INFO: Requesting a key from server: 10.0.2.6
2025/05/08 21:20:50 wazuh-agentd: INFO: No authentication password provided
2025/05/08 21:20:50 wazuh-agentd: INFO: Using agent name as: localhost.localdomain
```

⚠ Troubleshooting Summary Issue Fix Agent service failed to start Version mismatch error – upgraded Wazuh Manager Yum could not find package Used RPM manual installation Agent not listed in manager Use correct restarted services, and verified port connectivity

📝 Notes Ensure both agent and manager are running compatible Wazuh versions.

After configuration changes, always restart the services.

Use journalctl, ossec.log, and telnet for debugging.

