Here’s a **Wazuh (SIEM) Configuration Cheat Sheet** for quick reference. It covers essential paths, ports, services, commands, and best practices for configuring and managing Wazuh.

**🧠 WAZUH CONFIGURATION CHEAT SHEET**

**📁 Key File Locations**

| **Component** | **File/Directory** |
| --- | --- |
| Main config | /var/ossec/etc/ossec.conf |
| Agent keys | /var/ossec/etc/client.keys |
| Agent auth tool | /var/ossec/bin/manage\_agents |
| Logs (Manager) | /var/ossec/logs/ossec.log |
| Rules | /var/ossec/rules or /var/ossec/etc/rules |
| Decoders | /var/ossec/decoders |
| Alerts | /var/ossec/logs/alerts/alerts.json |
| Wazuh Dashboard | /usr/share/wazuh-dashboard |
| Filebeat config | /etc/filebeat/filebeat.yml |
| API config | /var/ossec/api/configuration/config.js |

**🔐 Default Ports**

| **Purpose** | **Port** | **Protocol** |
| --- | --- | --- |
| Wazuh Agent to Manager | 1514 | UDP |
| Agent Registration | 1515 | TCP |
| Wazuh API | 55000 | TCP |
| Wazuh Dashboard (UI) | 443 | TCP (HTTPS) |
| Elasticsearch / OpenSearch | 9200 | TCP |

**⚙️ Essential Commands**

**🔧 Wazuh Manager**

bash

KopierenBearbeiten

# Restart Manager

systemctl restart wazuh-manager

# Check Manager status

systemctl status wazuh-manager

# Show agent list

/var/ossec/bin/agent\_control -l

# Restart Filebeat

systemctl restart filebeat

# Restart Wazuh API

systemctl restart wazuh-api

**🧩 Agent Management**

bash

KopierenBearbeiten

# Interactive agent tool

/var/ossec/bin/manage\_agents

# Add new agent key manually

/var/ossec/bin/agent-auth -m <manager-ip>

# Remove agent

/var/ossec/bin/agent\_control -r <agent-id>

**📝 Key Configuration Snippets**

**ossec.conf – Agent Registration**

xml

KopierenBearbeiten

<auth>

<disabled>no</disabled>

<port>1515</port>

<use\_source\_ip>yes</use\_source\_ip>

</auth>

**ossec.conf – Log Collection (Syslog Example)**

xml

KopierenBearbeiten

<localfile>

<log\_format>syslog</log\_format>

<location>/var/log/auth.log</location>

</localfile>

**Filebeat Output to Wazuh**

yaml

KopierenBearbeiten

# filebeat.yml

output.elasticsearch:

hosts: ["https://localhost:9200"]

username: "admin"

password: "yourpassword"

ssl.verification\_mode: none

**📡 Wazuh API Example Calls**

bash

KopierenBearbeiten

# Get list of agents

curl -u user:password -k https://localhost:55000/agents

# Get agent status

curl -u user:password -k https://localhost:55000/agents/<agent-id>/status

**🛡️ Security Best Practices**

* Change default credentials for Dashboard and API.
* Enable TLS between agents and manager.
* Restrict API and dashboard access to trusted IPs.
* Regularly update Wazuh and dependencies.
* Use role-based access control (RBAC) on Dashboard/API.

**🧪 Troubleshooting Tips**

| **Symptom** | **Fix/Check** |
| --- | --- |
| Agent not showing | Check firewall, run agent-auth, verify port 1514/1515 |
| No logs in Dashboard | Check Filebeat status/logs |
| API 401 errors | Check credentials, RBAC configuration |
| High CPU on Wazuh Manager | Tune ossec.conf active response and rules |

**📘 Useful Logs**

| **Log File** | **Description** |
| --- | --- |
| /var/ossec/logs/ossec.log | Core Wazuh Manager log |
| /var/log/filebeat/filebeat | Filebeat ingestion errors |
| /var/log/syslog / messages | OS-level issues |
| /var/ossec/logs/alerts/alerts.json | Alert output |