Here is a comprehensive configuration document for the Wahzu Management Server, Wahzu Agents, and Filebeat, specifically focusing on network settings, IP addresses, and connectivity architecture:

Document Title: Wahzu Management Server & Agent Configuration (incl. Filebeat & Network Settings)

Version: 1.0

Date: 2025-07-03

Author: [Your Name or Team]

Confidentiality: Internal Use Only

**1. Overview**

This document outlines the configuration requirements for the Wahzu ecosystem, including the Wahzu Management Server, Wahzu Agents, and Filebeat with respect to network setup, IP addressing, ports, and communication flow. It ensures proper deployment in a secure and performant environment.

**2. Network Topology**

plaintext

Kopieren

Bearbeiten

+----------------------+

| Wahzu Management |

| Server (192.168.10.11)|

+----------+-----------+

|

Port: 1514/udp, 1515/tcp, 55000/tcp

|

+---------------------+----------------------+

| | |

+----+----+ +-----+-----+ +-----+-----+

| Agent 1 | | Agent 2 | ... | Agent N |

|192.168.20.11 |192.168.20.12 |192.168.20.N

+---------+ +-----------+ +-----------+

|

+-- Filebeat (Local)

**3. Wahzu Management Server Configuration**

IP Address: 192.168.10.11

OS: Ubuntu 22.04 LTS (recommended)

Hostname: wahzu-mgmt

Firewall Rules:

Port Protocol Purpose

1514 UDP Syslog reception from agents

1515 TCP Agent registration and communication

55000 TCP Agent-manager API communication

9200 TCP Elasticsearch (if hosted locally)

5601 TCP Kibana interface (if applicable)

NAT / DNS Note:

Ensure agents can resolve the FQDN of the server or access the public IP if behind NAT.

Configuration File: /var/ossec/etc/ossec.conf

xml

Kopieren

Bearbeiten

<remote>

<connection>secure</connection>

<port>1514</port>

<protocol>udp</protocol>

</remote>

<auth>

<port>1515</port>

</auth>

<cluster>

<node\_name>wahzu-mgmt</node\_name>

<node\_type>master</node\_type>

</cluster>

**4. Wahzu Agent Configuration**

Default Agent Configuration Path: /var/ossec/etc/ossec.conf

Required Fields:

xml

Kopieren

Bearbeiten

<client>

<server-ip>192.168.10.11</server-ip>

<port>1515</port>

</client>

Agent Host Configuration:

Each agent must have a static IP or DHCP reservation.

Ensure UDP 1514 and TCP 1515/55000 outbound traffic is allowed.

Hostname should be unique and resolvable for logging clarity.

Firewall Rules on Agents:

Direction Port Protocol Description

Outbound 1514 UDP Send logs to server

Outbound 1515 TCP Agent registration

Outbound 55000 TCP API communication

**5. Filebeat Configuration**

Filebeat is used to forward log files to Elasticsearch or the Wahzu Manager.

YAML Configuration File: /etc/filebeat/filebeat.yml

yaml

Kopieren

Bearbeiten

filebeat.inputs:

- type: log

paths:

- /var/log/syslog

- /var/log/auth.log

output.elasticsearch:

hosts: ["http://192.168.10.11:9200"]

username: "elastic"

password: "changeme"

# Optional: Output to Wahzu Manager via Logstash or custom port

# output.logstash:

# hosts: ["192.168.10.11:5044"]

Network Notes:

Filebeat uses HTTP/HTTPS (TCP 9200) to send logs to Elasticsearch.

Ensure time sync (NTP) for log integrity.

**6. Connectivity Test Checklist**

Component Check Command Example

Agent → Manager UDP 1514 reachability nc -u -zv 192.168.10.11 1514

Agent → Manager TCP 1515 registration port telnet 192.168.10.11 1515

Filebeat → ES Elasticsearch reachability curl -XGET http://192.168.10.11:9200

Manager → Agent Reverse API check (optional) curl https://192.168.20.x:55000

**7. Security Best Practices**

Use TLS for all API and log connections (especially in public or hybrid networks).

Define firewall rules per agent group/subnet.

Enable agent authentication via key pairs.

Monitor log throughput to avoid packet drops on UDP.

**8. Maintenance and Monitoring**

Set up Health checks using Prometheus/Grafana or custom scripts.

Periodically verify agent registration state.

Use wazuh-control and wazuh-agent commands for diagnostics.