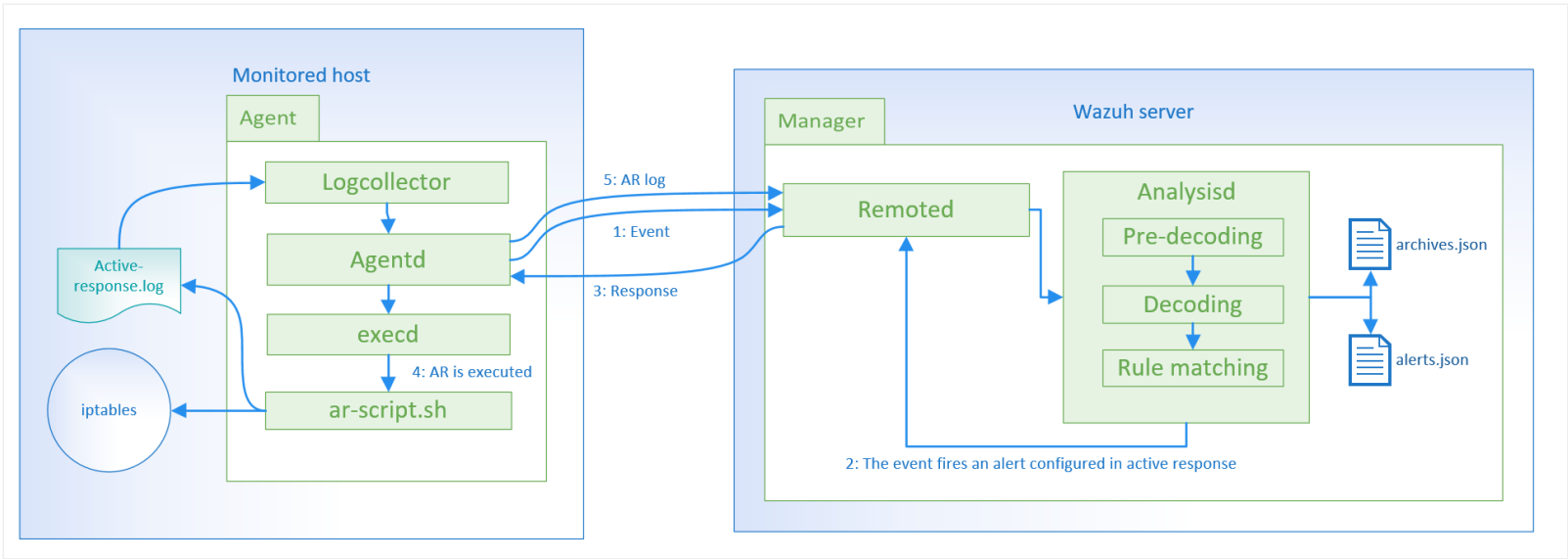


How it works



When is an active response triggered?

An active response can be triggered by a specific alert, alert level or rule group as configured in the `ossec.conf` file, where a script is configured to execute with a certain rule/group. **Active responses** are either stateful or stateless responses. Stateful responses will undo the action after a specified period of time while stateless responses are one-time actions.

Where are active response actions executed?

Active response specifies where their associated command will be executed: on the agent that triggered the alert, on the manager, on another specified agent, or on all agents plus the manager.

Active response configuration

An active response is configured in `ossec.conf` as follows:

1. Create a command

In order to configure an active response, a **command** must be defined that will initiate a certain script in response to a trigger.

To configure the active response, define the name of a **command** using the pattern below and then reference the script to be initiated. Next, define what data element(s) will be passed to the script.

Custom scripts that have the ability to receive parameters from the command line may also be used for an active response.

Example:

```
<command>
  <name>host-deny</name>
  <executable>host-deny.sh</executable>
  <expect>srcip</expect>
  <timeout_allowed>yes</timeout_allowed>
</command>
```

In this example, the command is called `host-deny` which initiates the `host-deny.sh` script. The data element is defined as `srcip` and this command is configured with a specified period of time, making it a stateful response.

Note

More information about options for creating a [command](#)


2. Define the active response

The active response configuration defines when and where a command is going to be executed. A command will be triggered when a specific rule with a specific id, severity level or source matches the active response criteria. This configuration will further define where the action of the command will be initiated, meaning in which environment (Agent, Manager, Local, or everywhere).

Example:

```
<active-response>
  <command>host-deny</command>
  <location>local</location>
  <level>7</level>
  <timeout>600</timeout>
</active-response>
```

In this example, the active response is configured to execute the command that was defined in the previous step. The where of the action is defined as the local host and the when is defined as any time the rule has a level higher than 6. The timeout that was allowed in the command configuration is also defined in the above example.

 **Note**

More information about all the options you can define for the [Active response](#)

You can view the active response log at `/var/ossec/logs/active-response.log`.

Default Active response scripts

Wazuh is preconfigured with the following scripts:

Script name	Description
disable-account.sh	disables an account by setting <code>passwd-l</code>
firewall-drop.sh	adds an IP to the iptables deny list
firewalld-drop.sh	adds an IP to firewalld drop list
host-deny.sh	adds an IP to the /etc/hosts.deny file
ip-customblock.sh	Custom OSSEC block, easily modifiable for custom response
ipfw_mac.sh	Firewall-drop response script created for the Mac OS
ipfw.sh	Firewall-drop response script created for ipfw
npf.sh	Firewall-drop response script created for npf
ossec-slack.sh	in order to post modifications
ossec-tweeter.sh	in order to post modifications
pf.sh	Firewall-drop response script created for pf
restart-ossec.sh	Automatically restarts Wazuh when ossec.conf has been changed
route-null.sh	Adds an IP to null route