# Wazuh Puppet module

This module has been authored by Nicolas Zin and updated by Jonathan Gazeley and Michael Porter. Wazuh has forked it with the purpose of maintaining it. Thank you to the authors for the contribution.

## Install Wazuh module

Download and install the Wazuh module from Puppet Forge:

```
$ sudo puppet module install wazuh-wazuh
Notice: Preparing to install into /etc/puppet/modules ...
Notice: Downloading from https://forgeapi.puppetlabs.com ...
Notice: Installing -- do not interrupt ...
/etc/puppet/modules
└─┬ wazuh-wazuh (v2.0.21)
  ├── puppet-selinux (v0.8.0)
  ├── puppetlabs-apt (v2.2.0)
  ├── puppetlabs-concat (v1.2.4)
  ├── puppetlabs-stdlib (v4.9.0)
  └── stahnma-epel (v1.1.1)
```

This module installs and configures Wazuh agent and manager.

## Install manager via Puppet

The manager is configured by installing the `wazuh::server` class, and optionally using:

- `wazuh::command`: to define active response command (like `firewall-drop.sh`).
- `wazuh::activeresponse`: to link rules to active response commands.
- `wazuh::addlog`: to define additional log files to monitor.

Here is an example of a manifest `wazuh-manager.pp`:

```
node "server.yourhost.com" {
   class { 'wazuh::server':
     smtp_server => 'localhost',
     ossec_emailto => ['user@mycompany.com'],
   }

   wazuh::command { 'firewallblock':
     command_name       => 'firewall-drop',
     command_executable => 'firewall-drop.sh',
     command_expect     => 'srcip'
   }

   wazuh::activeresponse { 'blockWebattack':
      command_name => 'firewall-drop',
      ar_level     => 9,
      ar_agent_id  => 123,
      ar_rules_id  => [31153,31151],
      ar_repeated_offenders => '30,60,120'
   }

   wazuh::addlog { 'monitorLogFile':
     logfile => '/var/log/secure',
     logtype => 'syslog'
   }
}
```

Place the file at */etc/puppetlabs/code/environments/production/manifests/* in your Puppet master and it will be executed in the specified node after the *runinterval* time set in puppet.conf.

## Install agent via Puppet

The agent is configured by installing the `wazuh::client` class.

Here is an example of a manifest `wazuh-agent.pp` (please replace with your IP address):

```
node "client.yourhost.com" {

class { "wazuh::client":
  ossec_server_ip => "192.168.209.166"
}

}
```

Place the file at */etc/puppetlabs/code/environments/production/manifests/* in your Puppet master and it will be executed in the specified node after the *runinterval* time set in puppet.conf.

## Reference Wazuh puppet

| Sections | Functions |
| --- | --- |
| Wazuh server class | email_alert<br>command<br>activeresponse<br>addlog |
| Wazuh agent class | addlog |
| ossec_scanpaths configuration | |

### Contents