Wazuh server class

`class wazuh::server`

$smtp_server

SMTP mail server.

$ossec_emailto

Email to address. `['user1@mycompany.com','user2@mycompany.com']`

$ossec_emailfrom

Email from address.

Default ossec@${domain}

$ossec_active_response

Enable or disable active-response.

Default true

$ossec_rootcheck

Enable rootcheck.

Default true

$ossec_rootcheck_frequency

Frequency that the rootcheck is going to be executed (in seconds).

Default 36000

$ossec_rootcheck_checkports

Look for the presence of hidden ports.

Default true

$ossec_rootcheck_checkfiles

Scan the whole filesystem looking for unusual files and permission problems.

Default true

$ossec_global_host_information_level

Alerting level for the events generated by the host change monitor (from 0 to 16).

Default 8

$ossec_global_stat_level

Alerting level for the events generated by the statistical analysis (from 0 to 16).

Default 8

$ossec_email_alert_level

Threshold defining minimum severity for a rule to fire an email alert. Some rules circumvent this threshold (`alert_email` option).

Default 7

$ossec_ignorepaths

Specify paths to ignore ossec scan

Default []

$ossec_scanpaths

Define paths to ossec scan

$ossec_white_list

Allow white listing of IP addresses.

Default []

$ossec_extra_rules_config

Using it, after enabling the Wazuh ruleset (either manually or via the automated script), take a look at the changes made to the ossec.conf file. You will need to put these same changes into the “$ossec_extra_rules_config” array parameter when calling the wazuh::server class.

Default []

$ossec_local_files

Define path log files to scan with ossec

$ossec_emailnotification

Whether or not to send email notifications.

Default yes

$ossec_email_maxperhour

Global Configuration with maximum number of emails per hour.

Default 12

$ossec_email_idsname

Define email ID name

Default undef

$ossec_syscheck_frequency

Frequency that syscheck is executed default every 22 hours

Default 79200

$ossec_auto_ignore

Specifies if syscheck will ignore files that change too often (after the third change)

Default yes

$ossec_prefilter

Command to run to prevent prelinking from creating false positives.

> Note
>
> This option can potentially impact performance negatively. The configured command will be run for each and every file checked.

Default false

$ossec_service_provider

Set service provider to Redhat on Redhat systems.

Default $::ossec::params::ossec_service_provide

$ossec_server_port

Port to allow communication between manager and agents.

Default: ‘1514’

$server_package_version

Modified client.pp and server.pp to accept package versions as a parameter.

Default installed

$manage_repos

Install Wazuh through Wazuh repositories.

Default true

$manage_epel_repo

Install epel repo and inotify-tools

Default true

$manage_client_keys

Manage client keys option.

Default true

$agent_auth_password

Define password for agent-auth

Default undef

$ar_repeated_offenders

A comma separated list of increasing timeouts in minutes for repeat offenders.

There can be a maximum of 5 entries.

Default empty

$syslog_output

Allows a Wazuh manager to send the OSSEC alerts to one or more syslog servers

Default false

$syslog_output_server

The IP Address of the syslog server.

Default undef

$syslog_output_format

Format of alert output.

Default undef

$enable_wodle_openscap

Enable openscap configuration in ossec.conf

Default false

$local_decoder_template

Allow to use a custom local_decoder.xml in the manager.

Default wazuh/local_decoder.xml.erb

$local_rules_template

Allow to use a custom local_rules.xml in the manager.

Default wazuh/local_rules.xml.erb

$shared_agent_template

Enable the configuration to deploy through agent.conf

Default `wazuh/ossec_shared_agent.conf.erb

$manage_paths

Follow the instructions on ossec-scanpaths.

Default [{'path' => '/etc,/usr/bin,/usr/sbin', 'report_changes' => 'no', 'realtime' => 'no'}, {'path' => '/bin,/sbin', 'report_changes' => 'yes', 'realtime' => 'yes'}]

> Note
>
> Consequently, if you add or remove any of the Wazuh rules later on, you'll need to ensure you add/remove the appropriate bits in the $ossec_extra_rules_config array parameter as well.

`function wazuh::email_alert`

$alert_email

Email to send to.

$alert_group

An array of rule group names.

Default false

Note

No email will be sent for alerts with a severity below the global `$ossec_email_alert_level`, unless the rule has alert_email set.

`function wazuh::command`

$command_name

Human readable name for wazuh::activeresponse usage.

$command_executable

Name of the executable. OSSEC comes preloaded with disable-account.sh, host-deny.sh, ipfw.sh, pf.sh, route-null.sh, firewall-drop.sh, ipfw_mac.sh, ossec-tweeter.sh, restart-ossec.sh.

$command_expect

Default srcip

$timeout_allowed

Default true

`function wazuh::activeresponse`

$command_name

Human readable name for wazuh::activeresponse usage.

$ar_location

It can be set to local, server, defined-agent, all.

Default local

$ar_level

Can take values between 0 and 16.

Default 7

$ar_rules_id

List of rule IDs.

Default []

$ar_timeout

Usually active response blocks for a certain amount of time.

Default 300

$ar_repeated_offenders

A comma separated list of increasing timeouts in minutes for repeat offenders. There can be a maximum of 5 entries.

Default empty

`function wazuh::addlog`

$log_name

Configure Wazuh log name

$agent_log

Path to log file.

Default false

$logfile

Path to log file.

$logtype

The OSSEC log_format of the file.

Default syslog