Documentation › User manual › Wazuh server administration › Configuring email alerts

Configuring email alerts

Wazuh can be configured to send the alerts to an email. You can configure the system to send emails when certain rules are triggered or configure it to send a daily report.

Mail example:

```
From: Wazuh <you@example.com>               5:03 PM (2 minutes ago)
to: me
-----------------------------
Wazuh Notification.
2017 Mar 08 17:03:05

Received From: localhost->/var/log/secure
Rule: 5503 fired (level 5) -> "PAM: User login failed."
Src IP: 192.168.1.37
Portion of the log(s):

Mar  8 17:03:04 localhost sshd[67231]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0
tty=ssh ruser= rhost=192.168.1.37
uid: 0
euid: 0
tty: ssh

 --END OF NOTIFICATION
```

Generic email options

In order to configure Wazuh to send alerts through email, you need to configure the email settings inside the `<global>` section:

```
<ossec_config>
    <global>
        <email_notification>yes</email_notification>
        <email_to>me@test.com</email_to>
        <smtp_server>mail.test.com..</smtp_server>
        <email_from>wazuh@test.com</email_from>
    </global>
    ...
</ossec_config>
```

To see all the available options to configure it, go to global section

After the global configuration, we need to configure the `email_alert_level`. This option establishes the minimum level to send an alert. By default is set to 7.

```
<ossec_config>
  <alerts>
      <email_alert_level>10</email_alert_level>
  </alerts>
  ...
</ossec_config>
```

This example will set the minimum level to 10. More information: alerts section.

When you have configured the `alert_level`, Wazuh needs to be restarted for the change take effect

a) For Systemd:

```
systemctl status wazuh-manager
```

b) For SysV Init:

```
service wazuh-manager status
```

⚠ Warning

Wazuh doesn't handle SMTP authentication. If you want to use an email with it, you need to configure a server relay.

Granular email options

Wazuh also allows a very granular configuration options for your alerts through email. Here you will find some examples of the granular configuration. More info: email_alerts section

⚠ Warning

The minimum level you configured inside `alerts` section, will be also valid here.

So, for example, if you configure your system to send an email when the rule 526 is triggered, if that rule has a level lower than the configured on the previous section the alert will not be sent.

Email alert based on level

The general configuration will be:

```
<email_alerts>
  <email_to>you@example.com</email_to>
  <level>4</level>
  <do_not_delay />
</email_alerts>
```

This will send to `you@example` and email if the any rule with level greater or equal to 10 is triggered. Remember, if the level here is less than the email_alert_level configured on the previous section, this will not be sent.

Email alert based on level and agent

The general configuration will be:

```
<email_alerts>
  <email_to>you@example.com</email_to>
  <event_location>server1</event_location>
  <do_not_delay />
</email_alerts>
```

This will send to `you@example` and email if the for the rules triggered on the `server1`. Also, `event_location` can be configured to monitor a specific log, hostname or network (IP)

Email based on rules ID

```
<email_alerts>
  <email_to>you@example.com</email_to>
  <rule_id>515, 516</rule_id>
  <do_not_delay />
</email_alerts>
```

This will send an email if the rules 515 or 516 are triggered on any agent.

Email based on the group

Each rule can have one or more groups configured. We can use this groups to filter the rules that we want to send through email:

```
<email_alerts>
  <email_to>you@example.com</email_to>
  <group>pci_dss_10.6.1</group>
</email_alerts>
```

This will send an alert if any rule part of the `pci_dss_10.6.1` group is triggered on any machine.

Multiples options and multiples email

This example will show you the real capacity of this capability:

```
<ossec_config>
  <email_alerts>
      <email_to>alice@test.com</email_to>
      <event_location>server1|server2</event_location>
  </email_alerts>
  <email_alerts>
      <email_to>is@test.com</email_to>
      <event_location>/log/secure$</event_location>
  </email_alerts>
  <email_alerts>
      <email_to>bob@test.com</email_to>
      <event_location>192.168.</event_location>
  </email_alerts>
  <email_alerts>
      <email_to>david@test.com</email_to>
      <level>12</level>
  </email_alerts>
 </ossec_config>
```

This configuration will send:

- An email to alice@test.com if any alert on server1 or server2 is triggered
- An email to is@test.com if the alerts came from `/log/secure/`
- An email to bob@test.com if the alerts came from any machine on the `192.168.0.0/24` network
- An email to david@test.com if the alerts have a level equals or higher than 12.

Force forwarding an alert by email

It's also possible to force the mail alert on the rule declaration. In order to do so, you need to use option

The possible values for this option are:

- **alert_by_email**: Always alert by email.
- **no_email_alert**: Never alert by email.
- **no_log**: Do not log this alert.

So for example this rule:

```
<rule id="502" level="3">
  <if_sid>500</if_sid>
  <options>alert_by_email</options>
  <match>Ossec started</match>
  <description>Ossec server started.</description>
</rule>
```

This will send an email every time this rule is triggered. I doesn't matter the level minimum level configured on the `<alerts>` section in `ossec.conf`