Envío de alertas por correo Wazuh manager

Para configurar Wazuh para enviar alertas por correo electrónico, los ajustes de correo electrónico deben configurarse en la sección del archivo principal de configuración ossec.conf.

```
sudo nano /var/ossec/etc/ossec.conf
```

```
<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>
```

Una vez configurado el apartado anterior, se debe establecer en el nivel de alerta mínimo que activará un correo electrónico. De forma predeterminada, este nivel se establece en 12.email_alert_level.

```
<ossec_config>
  <alerts>
      <email_alert_level>12</email_alert_level>
  </alerts>
</ossec_config>
```

Para aplicar los cambios se debe reiniciar el servidor de Wazuh:

```
systemctl restart wazuh-manager
```

Para que los cambios surtan efecto se debe realizar la **configuración SMTP.** Las alertas de correo electrónico de Wazuh no admiten servidores SMTP con autenticación como Gmail. Sin embargo, puede usar una retransmisión de servidor, como Postfix, para enviar estos correos electrónicos. Para configurar Postfix con Gmail seguimos los pasos a continuación:

El tipo de configuración del servidor de correo se establece en: *sin configuración*.

```
sudo apt-get update && apt-get install postfix mailutils libsasl2-2 ca-certificates libsasl2-modules
```

Para configurar Postfix se debe crear el archivo main de configuración.

```
sudo nano /etc/postfix/main.cf
```

```
relayhost = [smtp-mail.outlook.com]:587
smtp_sasl_auth_enable = yes
smtp_sasl_password_maps = hash:/etc/postfix/sasl_passwd
smtp_sasl_security_options = noanonymous
smtp_tls_CAfile = /etc/ssl/certs/ca-certificates.crt
smtp_use_tls = yes
smtpd_relay_restrictions = permit_mynetworks, permit_sasl_authenticated, defer_unauth_destination
```

Establezca la dirección de correo electrónico y la contraseña del remitente reemplazando *USERNAME* y *PASSWORD* con datos reales.
Para este paso se tiene que crear una contraseña de aplicación para que no se solicite la autenticación en 2 pasos y se pueda utilizar para las notificaciones.

```
echo [smtp-mail.outlook.com]:587 correo@outlook.com:******** > /etc/postfix/sasl_passwd
postmap /etc/postfix/sasl_passwd
chmod 400 /etc/postfix/sasl_passwd
```

Cambiamos los permisos de base de datos de contraseña para que solo usuario root pueda verla.

```
chown root:root /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
chmod 0600 /etc/postfix/sasl_passwd /etc/postfix/sasl_passwd.db
```

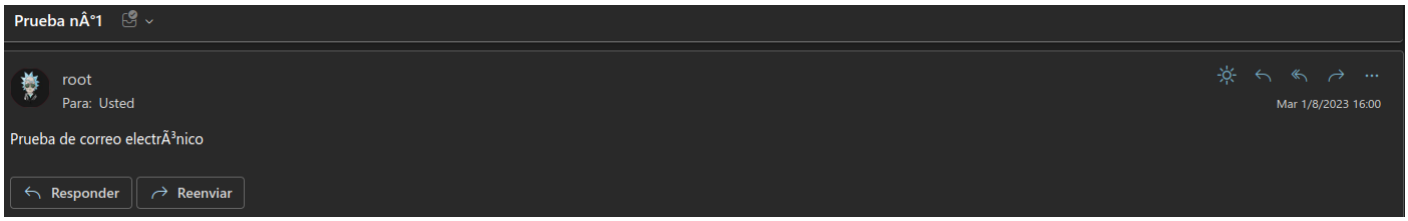
Se debe reiniciar Postfix para aplicar los cambios:

```
systemctl restart postfix
```

Prueba de configuración:
Reemplazando los datos de dirección de correo electrónico. Verificamos que se reciba este correo electrónico de prueba.you@example.com:

```
echo "Prueba de correo electrónico" | mail -s "Prueba n°1" -r "correo_que_envia@outlook.com"
 correo_que_recibe@outlook.com
```

En la bandeja de entrada tenemos:



Con la prueba realizada se configuran las notificaciones por correo electrónico en el archivo de configuración de Wazuh.

```
sudo nano /var/ossec/etc/ossec.conf
```

```
<global>
  <email_notification>yes</email_notification>
  <smtp_server>localhost</smtp_server>
  <email_from>USERNAME@gmail.com</email_from>
  <email_to>you@example.com</email_to>
</global>
```

```
<ossec_config>
  <global>
    <jsonout_output>yes</jsonout_output>
    <alerts_log>yes</alerts_log>
    <logall>no</logall>
    <logall_json>no</logall_json>
    <email_notification>yes</email_notification>
    <smtp_server>localhost</smtp_server>
    <email_from>[redacted]@outlook.com</email_from>
    <email_to>noxatrubaudi-8034@yopmail.com</email_to>
    <email_maxperhour>12</email_maxperhour>
    <email_log_source>alerts.log</email_log_source>
    <agents_disconnection_time>10m</agents_disconnection_time>
    <agents_disconnection_alert_time>0</agents_disconnection_alert_time>
  </global>

  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>7</email_alert_level>
  </alerts>
```

Para este ejemplo modificamos el nivel de alerta de correo a nivel 7 para ver distintos tipos de alertas enviados al correo electrónico, sin embargo en un entorno de producción es recomendable que sean

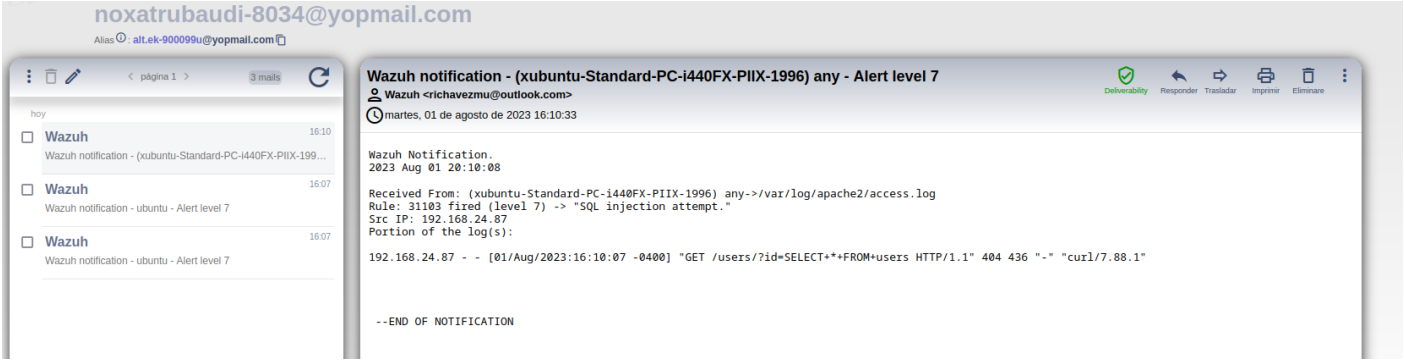
alertas de nivel máximo.

Reiniciamos el servidor para aplicar los cambios:

```
systemctl restart wazuh-manager
```

El correo de prueba es un e-mail temporal al cual nos llega la prueba de eventos, se puede configurar el mismo destinatario y origen con el mismo correo pero para probar la funcionalidad de reenvío se realizó la prueba con 2 correos diferentes.

Alerta en el correo de prueba ***noxatrubaudi-8034@yopmail.com***.



Revision #5
Created 9 abril 2024 09:46:10 by Ricardo Alberto
Updated 10 abril 2024 12:16:47 by Ricardo Alberto