

Custom Rule İçin Alert Oluşturma

Amaç

Yeni oluşturduğumuz custom rule için alert tipi tanımlama.

Adımlar

/var/ossec/etc nano ossec.conf ile gir. email_alert_level 10 yap.

```
<alerts>
  <log_alert_level>3</log_alert_level>
  <email_alert_level>10</email_alert_level>
</alerts>
```

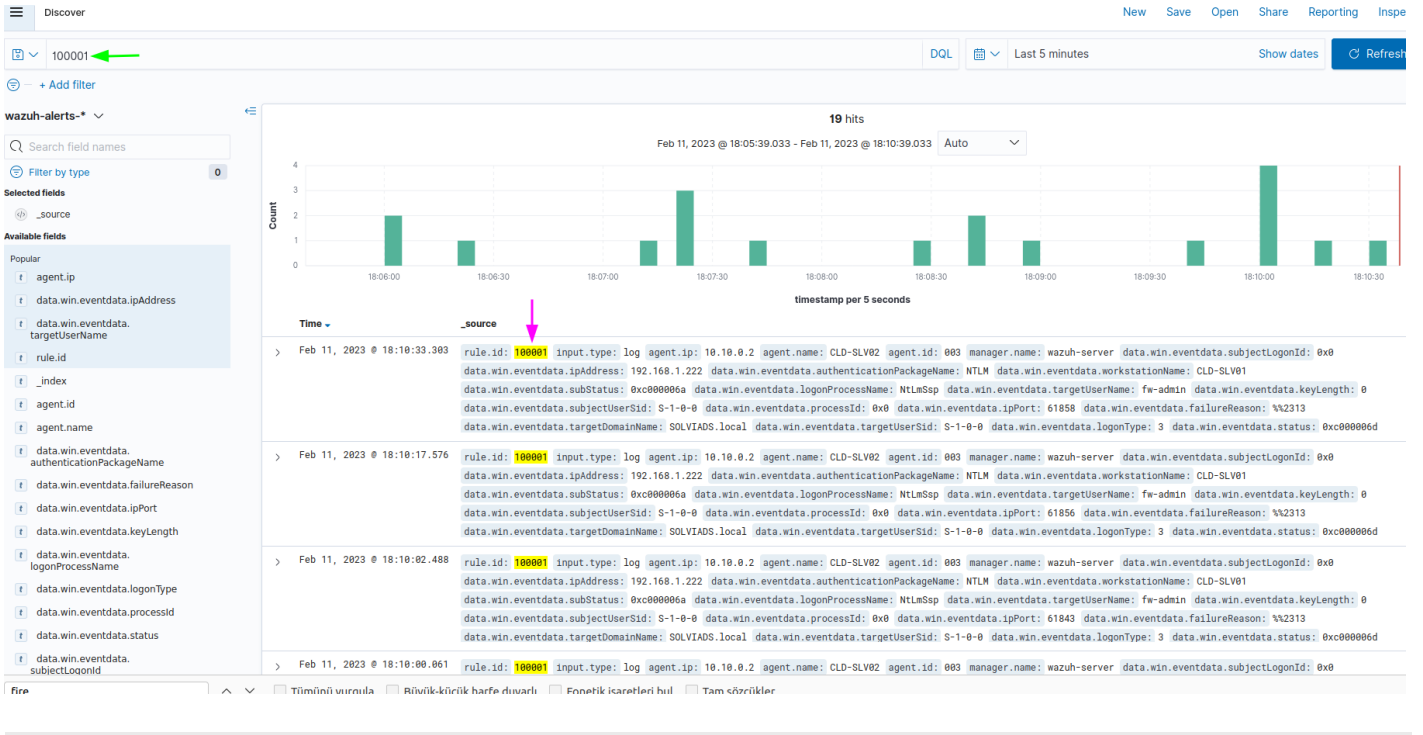
Mail gönderilecek adresi yaz. rule_id'yi custom rule'a verdiğin ID yap.

```
<email_alerts>
  <email_to>it-helpdesk@solviads.com</email_to>
  <rule_id>100001</rule_id>
  <do_not_delay />
</email_alerts>
```

^x ile çık ve çıkarken kaydetmeyi unutma.

sudo systemctl restart wazuh-manager servisi yeniden başlat.

wazuh discover a gir. Custom ID filtrele sonucu gör.



Revision #2

Created 11 February 2023 14:57:55 by Hüseyin Günaydın

Updated 11 February 2023 15:13:28 by Hüseyin Günaydın