Alarm Yönetimi

`/var/ossec/logs/alerts/alerts.log`Uyarılar, Wazuh aracılarından ve aracısız aygıtlardan alınan olayları işledikten sonra Wazuh yöneticisi tarafından oluşturulan bildirimlerdir. Varsayılan olarak, uyarılar ve dosyalarında saklanır `/var/ossec/logs/alerts/alerts.json`.

Varsayılan olarak, Wazuh sunucusu, oluşturulan uyarıları dizinleme için Wazuh dizinleyicisine iletmek için Filebeat'i kullanır. Ek olarak, Wazuh yöneticisini syslog sunucuları, e-posta sistemleri ve veritabanlarını içeren diğer sistemlere uyarıları iletecek şekilde yapılandırabilirsiniz.

Uyarı Eşiği

Uyarı eşiği, bir uyarının tetiklenmesi için aşılması gereken en düşük önem seviyesidir. Wazuh yöneticisi, kurallar kümesindeki eşleşen kurala göre izlenen uç noktalardan gelen her olaya bir önem seviyesi atar. Varsayılan olarak, yalnızca önem seviyesi `3`veya daha yüksek olan uyarıları tetikler.

Yapılandırma

`/var/ossec/etc/ossec.conf`Uyarı eşiği , Wazuh sunucusundaki yapılandırma dosyasında XML etiketi içerisinde yapılandırılır `<alerts>`.

Aşağıdaki kod bloğu, olaylar ve uyarıların e-posta yoluyla iletilmesi için varsayılan uyarı eşiği yapılandırmasını gösterir:

```
<ossec_config>
  <alerts>
    <log_alert_level>3</log_alert_level>
    <email_alert_level>12</email_alert_level>
  </alerts>
</ossec_config>
```

Nerede:

- `<log_alert_level>` etiket , `/var/ossec/logs/alerts/alerts.log` ve/veya `/var/ossec/logs/alerts/alerts.json` dosyada depolanan uyarıları tetiklemek için minimum önem seviyesini ayarlar . Varsayılan değer `3`'dür . İzin verilen değer, kurallar sınıflandırma kılavuzunda belirtildiği gibi `1` ila `16` arasında herhangi bir tam sayıdır

- Etiket `<email_alert_level>`, bir uyarının e-posta bildirimi oluşturması için minimum önem seviyesini ayarlar. Varsayılan değer 'dir `12`. İzin verilen değer, `1`'den 'e kadar herhangi bir tam sayıdır `16`. Bu ayar, ayrıntılı e-posta uyarısı yapılandırmasını geçersiz kılar. Ancak, bireysel kurallar içindeki `alert_by_email` seçenek , bir e-posta uyarısını tetiklemek için hem genel hem de ayrıntılı uyarı düzeyi eşiklerini geçersiz kılabilir.

Uyarı eşiği yapılandırma hakkında ayrıntılı bilgi için uyarı başvuru kılavuzuna bakın.

> Not: Yapılandırma dosyasında herhangi bir değişiklik yaptığınızda Wazuh yöneticisini yeniden başlatın. Bu eylem değişikliklerin etkili olmasını sağlar.

Aşağıdaki komutla komut satırı arayüzü üzerinden Wazuh yöneticisini yeniden başlatın:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

Uyarıları İletme

Wazuh yöneticisi, dizinleme ve analiz yetenekleri için uyarıları varsayılan olarak Wazuh dizinleyicisine iletir. Ayrıca, Wazuh yöneticisi, analiz ve yedekleme için uyarıları yapılandırma ve diğer sistemlere iletme yeteneği sağlar.

Syslog Çıktısını Yapılandırma

Syslog_output seçeneğini kullanarak Wazuh sunucusunu bir syslog sunucusuna uyarılar gönderecek şekilde yapılandırabilirsiniz . Uyarıları bir syslog sunucusuna iletmek, merkezi izleme ve özel raporlama için yararlı olabilir.

Yapılandırma

`/var/ossec/etc/ossec.conf`Syslog çıktısı, blok içindeki Wazuh sunucu yapılandırma dosyasında yapılandırılır . Varsayılan olarak, Wazuh yöneticisi uyarıları UDP protokolü üzerinden `<ossec_config>` port kullanarak syslog sunucularına iletir .`514`

Aşağıdaki kod bloğu, uyarıları bir syslog sunucusuna iletmek için örnek bir yapılandırmayı göstermektedir:

```
<ossec_config>
  <syslog_output>
    <level>9</level>
    <server>192.168.1.241</server>
  </syslog_output>
</ossec_config>
```

Yapılandırma seçenekleri aşağıdaki şekilde tanımlanmıştır:

- Etiket `<level>`, syslog sunucusuna iletilecek uyarıların minimum önem seviyesini ayarlar. Örnek değer, `9`Wazuh sunucusunun uyarıları yalnızca uyarı seviyesi 'den yüksekse syslog sunucusuna ilettiğini gösterir `9`. Bu seçenek tanımlanmamışsa, Wazuh sunucusu tüm uyarıları syslog sunucusuna iletir.
- Etiket `<server>`, uyarıları iletmek için syslog sunucusunun IP adresini veya ana bilgisayar adını ayarlar. `192.168.1.241`Yapılandırmadaki IP adresi bir örnek olarak kullanılır.

Değişikliklerin her yapılandırmadan sonra uygulanması için Wazuh yönetici hizmetini yeniden başlatın:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

Yapılandırma dosyasında blok `<syslog_output>`içerisinde birden fazla blok tanımlayarak uyarıları birden fazla syslog sunucusuna iletebilirsiniz .`<ossec_config>`/var/ossec/etc/ossec.conf

```
<ossec_config>
  <syslog_output>
    <server>192.168.1.240</server>
  </syslog_output>

  <syslog_output>
    <level>9</level>
    <server>192.168.1.241</server>
  </syslog_output>
</ossec_config>
```

Yukarıdaki yapılandırmada,

- İlk `<syslog_output>`blok tüm uyarıları filtrelemeden IP adresine sahip syslog sunucusuna gönderir `192.168.1.240`.
- İkinci blok , yalnızca uyarı seviyesi 'den yüksekse `<syslog_output>`syslog sunucusuna uyarılar gönderir .`192.168.1.2419`

E-posta Uyarılarını Yapılandırma

Wazuh, bir Wazuh sunucusunda oluşturulduğunda e-posta sistemlerine uyarılar göndermek için bir özellik sunar. Kurallar tetiklendiğinde veya özelleştirilmiş ayarlara göre bir veya daha fazla e-posta adresine e-posta uyarıları göndermek üzere yapılandırabilirsiniz. Bu yapılandırma günlük olay raporları ve daha fazlası için size yardımcı olabilir.

Kural kimliği `553`tetiklendiğinde Wazuh tarafından gönderilen örnek bir e-posta aşağıda gösterilmektedir:

```
Wazuh Notification.
2024 Apr 29 08:58:30

Received From: wazuh-server->syscheck
Rule: 553 fired (level 7) -> "File deleted."
Portion of the log(s):

File '/var/ossec/test_dir/somefile.
txt' deleted
Mode: realtime

Attributes:
 - Size: 0
 - Permissions: rw-r--r--
 - Date: Mon Apr 29 08:46:12 2024
 - Inode: 841858
 - User: root (0)
 - Group: root (0)
 - MD5: d41d8cd98f00b204e9800998ecf8427e
 - SHA1: da39a3ee5e6b4b0d3255bfef95601890afd80709
 - SHA256: e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855


--END OF NOTIFICATION
```

Genel E-posta Seçenekleri

Wazuh'un e-posta uyarıları göndermesini yapılandırmak için `/var/ossec/etc/ossec.conf` dosyanın `<global>` bölümündeki e-posta seçeneklerini yapılandırıyoruz .

E-posta adresine uyarı göndermek için örnek bir e-posta yapılandırması `me@test.com` aşağıda gösterilmektedir:

```
<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>
```

Yukarıdakiler yapılandırıldıktan sonra, `email_alert_level`bir e-postayı tetiklemek için seçeneğin minimum uyarı seviyesine ayarlanması gerekir. Varsayılan olarak, bu seviye olarak ayarlanır `12`.

Aşağıdaki örnek yapılandırma, e-posta uyarılarının gönderileceği minimum seviyeyi belirler `10`:

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

Değişikliklerin her yapılandırmadan sonra uygulanması için Wazuh yönetici hizmetini yeniden başlatın:

Systemd

```
systemctl restart wazuh-manager
```

SysV İnit

```
service wazuh-manager restart
```

> Uyarı: Wazuh SMTP kimlik doğrulamasını işlemez. E-posta servisiniz bunu kullanıyorsa, bir sunucu rölesi yapılandırmanız gerekir .

Ayrıntılı E-posta Seçenekleri

Wazuh, e-posta uyarıları için ayrıntılı yapılandırma seçeneklerine izin verir. Bu ayar, dosyanın bölümünde yapılandırılan genel e-posta seçeneklerini genişletir. Ayrıntılı e-posta yapılandırmaları, dosyanın etiketi içinde tanımlanır .<global>/var/ossec/etc/ossec.conf<email_alerts>/var/ossec/etc/ossec.conf

> Uyarı: Bölümde yapılandırılan minimum önem düzeyi <alerts>bu ayrıntılı e-posta yapılandırmalarına uygulanır ve bunları geçersiz kılar. Örneğin, Wazuh yöneticisini kural tetiklendiğinde bir e-posta gönderecek şekilde yapılandırırsanız 526ancak kuralın düzeyi bölümde belirtilen minimum düzeyden düşükse <alerts>uyarı gönderilmez.

Seviyeye Göre E-posta Uyarısı

Bu seçenek, Wazuh yöneticisini, önem düzeyi ayarlanan değere eşit veya daha büyük olduğunda e-posta uyarıları gönderecek şekilde yapılandırır. Bu seçenek aşağıdaki şekilde yapılandırılır:

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

you@example.comBu yapılandırma, Wazuh yöneticisinin , seviyesi eşit veya daha büyük olan herhangi bir kural tetiklendiğinde bir e-posta göndermesine olanak tanır 4.

> Not: Buradaki önem seviyesi <alerts> bölümde yapılandırılan email_alert_level önem seviyesinden daha düşükse , e-posta gönderilmeyecektir.

Etkinlik Lokasyonuna Göre E-posta Uyarısı

Bu event_locationseçenek, olayın kaynaklandığı konuma göre e-posta uyarıları göndermeyi içerir. Oluşturulan uyarı, e-posta yoluyla iletilmek üzere olay konumuyla eşleşmelidir. Bu seçenek için izin verilen değerler Wazuh aracı adı, ana bilgisayar adı, IP adresi veya günlük dosyasıdır.

Bu seçenek aşağıdaki şekilde yapılandırılır:

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

you@example.comBu yapılandırma, Wazuh yöneticisinin uyarıları oluşturan olayların Wazuh adlı aracıda kaynaklandığı zaman adresine bir e-posta göndermesine olanak tanır server1.

Kural Kimliğine Dayalı E-posta

Bu rule_idseçenek, kural kimliklerine dayalı uyarı e-postaları göndermek için kullanılır. Bu seçenek, yalnızca belirli tanımlanmış kurallar tetiklendiğinde e-postaların gönderilmesini sınırlar.

Bu seçenek aşağıdaki şekilde yapılandırılır:

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

Bu yapılandırma , Wazuh yöneticisinin you@example.comkurallar tetiklendiğinde bir e-posta göndermesine olanak tanır .515516

Kural Grubuna Dayalı E-posta

Seçenek group, uyarıların ait olduğu bir veya daha fazla kural grubuna göre e-posta göndermek üzere yapılandırılabilir.

Bu seçenek aşağıdaki şekilde yapılandırılır:

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

you@example.comBu yapılandırma, Wazuh yöneticisinin, grubun parçası olan herhangi bir kural pci_dss_10.6.1herhangi bir Wazuh izlenen uç noktasında tetiklendiğinde bir e-posta göndermesine olanak tanır.

Birden Fazla Seçenek ve Birden Fazla E-posta

E-posta uyarıları, her biri benzersiz kriterlere sahip birden fazla e-posta adresine gönderilebilir.

Aşağıdaki örnek yapılandırma, birden fazla kritere sahip e-posta uyarılarının birden fazla e-posta adresine nasıl gönderileceğini gösterir:

```
<ossec_config>
  <email_alerts>
    <email_to>alice@test.com</email_to>
    <event_location>endpoint1|endpoint2</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>
```

Bu yapılandırma şunları gönderir:

- `alice@test.com`Herhangi bir uyarı tetiklendiğinde `endpoint1`e -posta adresinize gönderilecek `endpoint2`.
- `is@test.com`Uyarıların dosyadan gelip gelmediğine dair bir e-posta `/log/secure`.
- `bob@test.com`Uyarıların ağdaki herhangi bir uç noktadan gelip gelmediğine dair bir e-posta `192.168.0.0/24`.
- `david@test.com`Uyarıların seviyesi eşit veya daha yüksekse e-posta gönderilecektir `12`.

Bir Uyarıyı E-postayla İletmeyi Zorla

E-posta yoluyla uyarı göndermek için minimum önem seviyesi `12`varsayılan olarak. Wazuh yöneticisini yapılandırılmış minimum önem seviyesinin altında bir e-posta uyarısı göndermek üzere yapılandırabilirsiniz. Bunu yapmak için aşağıdaki kural seçeneklerinden birini kullanmanız gerekir:

- `alert_by_email`her zaman e-posta ile uyarmak.
- `no_email_alert`asla e-posta yoluyla uyarıda bulunmayın.
- `no_log`Bu uyarının kaydedilmemesi için.

Örneğin, aşağıdaki kural tanımı, `502`minimum önem düzeyi ne olarak ayarlanmış olursa olsun, kural her tetiklendiğinde bir e-posta gönderir:

```
<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>
```

Kimlik Doğrulamalı SMTP Sunucusu

Wazuh e-posta uyarıları, Gmail gibi kimlik doğrulaması olan SMTP sunucularını desteklemez. Ancak, bu e-postaları Postfix gibi bir sunucu rölesi aracılığıyla gönderebilirsiniz.

Postfix'i Gmail ile yapılandırmak için aşağıdaki adımları röle sunucunuzda gerçekleştirin.

1. Gerekli paketleri yüklemek için bu komutu çalıştırın. Posta sunucusu yapılandırma türü hakkında sorulursa *Yapılandırma yok'u seçin.*

   CentOS

   ```
   yum update && yum install postfix mailx cyrus-sasl cyrus-sasl-plain
   ```

   Ubuntu

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

2. Postfix'i yapılandırmak için bu satırları dosyaya ekleyin `/etc/postfix/main.cf`. Eksikse dosyayı oluşturun.

   CentOS

   ```
   relayhost = [smtp.gmail.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-bundle.crt
   smtp_use_tls = yes
   ```

   Ubuntu

   ```
   relayhost = [smtp.gmail.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
```

3. Gönderenin kimlik bilgilerini dosyaya ayarlayın `/etc/postfix/sasl_passwd`ve Postfix için bir veritabanı dosyası oluşturun. `<USERNAME>`ve `<PASSWORD>`değişkenlerini sırasıyla gönderenin e-posta adresi kullanıcı adı ve parolasıyla değiştirin.

```
echo [smtp.gmail.com]:587 <USERNAME>@gmail.com:<PASSWORD> > /etc/postfix/sasl_passwd
postmap /etc/postfix/sasl_passwd
```

> Not: Şifre bir Uygulama Şifresi olmalıdır . Uygulama Şifreleri yalnızca 2 Adımlı Doğrulama özelliği açık olan hesaplarda kullanılabilir.

4. Parola DB dosyanızı yalnızca `root`kullanıcının tam okuma ve yazma erişimine sahip olması için güvenceye alın. Bunun nedeni `/etc/postfix/sasl_passwd`ve `/etc/postfix/sasl_passwd.db` dosyalarının düz metin kimlik bilgilerine sahip olmasıdır.

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

5. Yapılandırma değişikliklerini gerçekleştirmek için Postfix'i yeniden başlatın:

   Systemd

```
systemctl restart postfix
```

   SysV Başlatma

```
service postfix restart
```

6. Yapılandırmayı test etmek için aşağıdaki komutu çalıştırın:

```
echo "Test mail from postfix" | mail -s "Test Postfix" -r "<CONFIGURED_EMAIL>" <RECEIVER_EMAIL>
```

Yer değiştirmek:

- `<CONFIGURED_EMAIL>`Yapılandırılmış e-posta adresinizle.
- `<RECEIVER_EMAIL>`Alıcının e-posta adresiyle birlikte.

Komut, alıcının e-postasına `Test Postfix` konu ve `Test mail from postfix` gövdeyi içeren bir e-posta gönderir.

If you get the error message `fatal: tls_fprint: error computing md5 message digest` in the `/var/log/maillog` file, run the following commands to switch Postfix from the default `MD5` hashing function to `SHA-256`:

```
#
```

`/var/log/maillog` dosyasında `fatal: tls_fprint: error computing md5 message digest` hata mesajı alırsanız , Postfix'i varsayılan `MD5` karma işlevinden `SHA-256`'ya geçirmek için aşağıdaki komutları çalıştırın :

```
postconf -e smtp_tls_fingerprint_digest=sha256
postconf -e smtpd_tls_fingerprint_digest=sha256
```

7. `<global>`Wazuh sunucusunun `/var/ossec/etc/ossec.conf`dosyasının etiketi içerisinde e-posta bildirimlerini aşağıdaki şekilde yapılandırın:

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

Nerede:

- `<email_notification>`e-posta uyarılarının kullanımını değiştirir.
- `<smtp_server>`uyarıları iletmek için kullanılacak SMTP sunucusunu tanımlar.
- `<email_from>`yapılandırılmış gönderenin e-posta adresini belirtir. `<USERNAME>`E-posta adresinizin yapılandırılmış kullanıcı adınızla değiştirin.
- `<email_to>`uyarıların alıcısının e-posta adresini belirtir. `<RECEIVER_EMAIL>`Alıcının e-posta adresiyle değiştirin.

8. Değişiklikleri uygulamak için Wazuh yöneticisini yeniden başlatın:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

Veritabanı Çıktısını Yapılandırma

Wazuh, uyarıları veritabanı sistemlerine iletmeyi destekler. Wazuh yöneticisini, oluşturulan uyarıları bir veritabanına çıktı olarak verecek şekilde yapılandırabilirsiniz. Bu yapılandırmayı elde etmek için, Wazuh yöneticisini kullanmak istediğiniz veritabanı türündeki kaynaklardan derlemelisiniz. Wazuh şu anda MySQL ve PostgreSQL veritabanlarını destekler.

> Not: Bu kılavuz, MySQL veya PostgreSQL'i zaten kurduğunuzu ve kullanıcıları ve veritabanlarını nasıl oluşturacağınızı bildiğinizi varsayar.

Ön Koşullar

Yapılandırmak istediğiniz veritabanı sistemine ait geliştirme kütüphanelerini kurmanız ve Wazuh yöneticisini gerekli veritabanı sistemini kullanacak şekilde derlemeniz gerekmektedir.

1. Veritabanı sistemi için geliştirme kütüphanelerini yükleyin:

   - **MySQL için** :

     Yum

     ```
     yum install mysql-devel
     ```

     APT

     ```
     apt-get install libmysqlclient-dev
     ```

   - **PostgreSQL için** :

     Yum

     ```
     yum install postgresql-devel
     ```

     APT

     ```
     apt-get install libpq-dev
     ```

2. Bağımlılıkları, bağımlılıkları yükleme bölümünde açıklandığı şekilde yükleyin.

3. Wazuh'un son sürümünü indirin ve çıkarın:

```
curl -Ls https://github.com/wazuh/wazuh/archive/v4.9.2.tar.gz | tar zx
```

4. Wazuh dizinine geçmek için aşağıdaki komutları çalıştırın ve kullanılacak veritabanı türünü belirtin, `<DATABASE_TYPE>` değişkeni `mysql` veya `pgsql` ile değiştirin :

```
cd wazuh-4.9.2/src
make deps && make TARGET=server DATABASE=<DATABASE_TYPE>
```

> Not: Sistem özelliklerinize bağlı olarak derleme işlemi biraz zaman alabilir.

5. Betiği çalıştırın `install.sh`. Wazuh kaynaklarını kullanarak kurulum sürecinde size rehberlik edecek bir sihirbaz görüntüler:

```
cd ..
./install.sh
```

6. Script size ne tür bir kurulum istediğinizi sorduğunda `manager`Wazuh yöneticisini kurmak için şunu yazın:

```
1- What kind of installation do you want (manager, agent, local, hybrid, or help)? manager
```

> Not: Kurulum sırasında kurulum yoluna karar verebilirsiniz. `install.sh` dosyasını çalıştırın ve dili seçin, kurulum modunu `manager` olarak ayarlayın, ardından kurulum yolunu ayarlayın (`Choose where to install Wazuh [/var/ossec]`/var/ossec). Varsayılan kurulum yolu /var/ossec'tir. Yaygın olarak kullanılan özel bir yol `/opt` olabilir.

> Uyarı: Varsayılandan farklı bir yol seçerseniz kritik bir kurulum dizini seçmemeye son derece dikkat edin. Dizin zaten mevcutsa, yükleyici dizini silmenizi veya Wazuh'u içine kurarak devam etmenizi isteyecektir.

7. Kurulum programı kurulumun sonunda Wazuh'u başlatmak isteyip istemediğinizi sorar. Eğer istemezseniz, aşağıdaki komutla daha sonra başlatabilirsiniz:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

Veritabanı Yapılandırması

Veritabanı sisteminize göre yeni bir veritabanı oluşturun, veritabanı kullanıcısını ayarlayın ve `src/os_dbd`kaynak kodun bulunduğu dizinde bulunan şemayı aşağıdaki komutlarla ekleyin:

- **MySQL için** :

```
mysql -u root -p
```

```
mysql> CREATE DATABASE Alerts_DB;
Query OK, 1 row affected (2.34 sec)

mysql> CREATE USER '<DATABASE_USER>'@'<DATABASE_SERVER_IP>' IDENTIFIED BY '<DATABASE_USER_
Query OK, 0 rows affected (0.00 sec)

mysql> GRANT INSERT,SELECT,UPDATE,CREATE,DELETE,EXECUTE on Alerts_DB.* to '<DATABASE_USER>'@'
Query OK, 0 rows affected (0.00 sec)

mysql> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.00 sec)

mysql> quit;
```

Yukarıdaki komutlarda aşağıdaki değişkenleri değiştirin:

- `<DATABASE_USER>`Veritabanı sunucusu için oluşturmak istediğiniz kullanıcıyla.
- `<DATABASE_SERVER_IP>`veritabanı sunucusunun IP adresi ile.
- `<DATABASE_USER_PASSWORD>`veritabanı sunucusuna erişmek için kullanıcı şifresi ile.

```
mysql -u root -p Alerts_DB < src/os_dbd/mysql.schema
```

- **PostgreSQL için** :

```
sudo -u postgres createuser -P <DATABASE_USER>
sudo -u postgres createdb -O <DATABASE_USER> Alerts_DB
psql -U <DATABASE_USER> -d Alerts_DB -f src/os_dbd/postgresql.schema
```

`<DATABASE_USER>`Veritabanı sunucusu için oluşturmak istediğiniz kullanıcıyla değiştirin .

> Not: Kullanıcıyı oluştururken iki kez parola girmeniz istenecektir. Wazuh yöneticisini yapılandırırken gerekli olduğundan bu parolayı not edin.

Wazuh Yöneticisi Yapılandırması

Wazuh yöneticisini veritabanı sistemine uyarılar ve diğer verileri gönderecek şekilde yapılandırmak için aşağıdaki adımları izleyin.

1. Wazuh sunucusundaki dosya `<ossec_config>`bloğunun içine aşağıdaki kod bloğunu ekleyin : `/var/ossec/etc/ossec.conf`

   - **MySQL için** :

     ```
     <database_output>
       <hostname><DATABASE_SERVER_IP></hostname>
       <username><DATABASE_USER></username>
       <password><DATABASE_USER_PASSWORD></password>
       <database>Alerts_DB</database>
       <type>mysql</type>
     </database_output>
     ```

   - **PostgreSQL için** :

     ```
     <database_output>
       <hostname><DATABASE_SERVER_IP></hostname>
       <username><DATABASE_USER></username>
       <password><DATABASE_USER_PASSWORD></password>
       <database>Alerts_DB</database>
       <type>postgresql</type>
     </database_output>
     ```

   Nerede:
   - `<hostname>`veritabanı sunucusunun IP adresini belirtir. `<DATABASE_SERVER_IP>` Veritabanı sunucusunun IP adresini değiştirin.
   - `<username>`veritabanına erişecek kullanıcıyı belirtir. `<DATABASE_USER>`Yukarıda oluşturulan veritabanı kullanıcısıyla değiştirin.
   - `<password>`veritabanına erişmek için kullanıcı parolasını belirtir. `<DATABASE_USER_PASSWORD>`Yukarıda oluşturulan kullanıcı parolasıyla değiştirin.
   - `<database>`uyarıların depolanacağı veritabanının adını belirtir. Örneğin, `Alerts_DB` yukarıdaki yapılandırmada belirtildiği gibi.
   - `<type>`veritabanının türünü belirtir (MySQL veya PostgreSQL). İzin verilen değerler `mysql`veya `pgsql`.

2. Değişiklikleri uygulamak için Wazuh yönetici hizmetini yeniden başlatın:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

3. Wazuh yöneticisinin veritabanına bağlı olduğunu doğrulamak için aşağıdaki komutu çalıştırın:

```
grep wazuh-dbd /var/ossec/logs/ossec.log
```

Output

```
2024/06/24 14:49:11 wazuh-dbd: INFO: Connected to database 'Alerts_DB' at '127.0.0.1'.
```

Veritabanı artık Wazuh yöneticisinden veri almaya başlayacaktır.

Revision #3
Created 11 December 2024 16:25:02 by Ayşegül Sarıkaya
Updated 31 December 2024 13:26:28 by Ayşegül Sarıkaya