Wazuh Sunucu API'sini Güvence Altına Alma

Wazuh panosu ile Wazuh sunucu API'si arasındaki iletişim varsayılan olarak HTTPS ile şifrelenir. Wazuh sunucu API'si, kullanıcılar bunları sağlamazsa ilk çalıştırma sırasında kendi özel anahtarını ve sertifikasını oluşturur. Ek olarak, Wazuh sunucu API'si OVA kurulumuyla birlikte kurulduğunda aşağıdaki kullanıcı adı-şifre çiftini otomatik olarak oluşturur:

- `wazuh:wazuh`
- `wazuh-wui:wazuh-wui`

Wazuh dağıtımı kurulum yardımcısı betiği kullanılarak gerçekleştirildiyse, Wazuh API kullanıcı adı şudur `wazuh`ve aşağıdaki komutu çalıştırarak parolayı çıkarabilirsiniz:

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "\'wazuh\'" -A 1
```

Bu nedenle Wazuh yöneticisini kurduktan sonra Wazuh sunucu API'sinin güvenliğini sağlamak büyük önem taşımaktadır.

> Uyarı: Wazuh sunucu API'si tarafından oluşturulan sertifikanın kendi imzalı olması nedeniyle varsayılan şifreleri değiştirmenizi ve kendi sertifikanızı kullanmanızı şiddetle öneririz.

Wazuh Sunucu API'sini Güvence Altına Almak İçin Önerilen Değişiklikler

1. HTTPS Parametrelerini Değiştirin

Wazuh sunucu API'si varsayılan olarak HTTPS'yi etkinleştirmiştir. Eğer içinde kullanılabilir bir sertifika yoksa `/var/ossec/api/configuration/ssl/`, Wazuh sunucusu başlatıldığında özel anahtarı ve kendi kendine imzalanmış bir sertifikayı üretecektir. Eğer durum buysa ve API günlük biçimi olarak ayarlanmışsa `plain`, aşağıdaki satırlar görünecektir `/var/ossec/logs/api.log`:

```
INFO: HTTPS is enabled but cannot find the private key and/or certificate. Attempting to generate them.
INFO: Generated private key file in WAZUH_PATH/api/configuration/ssl/server.key.
INFO: Generated certificate file in WAZUH_PATH/api/configuration/ssl/server.crt.
```

Bu HTTPS seçeneklerini, durumlarını veya sertifika yolunu da içerecek şekilde, şu adreste bulunan Wazuh sunucu API yapılandırma dosyasını düzenleyerek değiştirebilirsiniz `/var/ossec/api/configuration/api.yaml`:

```
https:
  enabled: yes
  key: "server.key"
  cert: "server.crt"
  use_ca: False
  ca: "ca.crt"
  ssl_protocol: "auto"
  ssl_ciphers: ""
```

Değişiklikleri uygulamak için Wazuh yönetici hizmetini kullanarak Wazuh sunucu API'sini yeniden başlatın:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

2. Yönetici Kullanıcıları İçin Varsayılan Parolayı Değiştirin

Yönetici kullanıcıları için varsayılan şifreyi değiştirmek için `wazuh`aşağıdaki `wazuh-wui`Wazuh sunucu API isteğini kullanabilirsiniz: PUT /security/users/{user_id} .

> Not: Kullanıcıların şifresi 8 ile 64 karakter arasında olmalıdır. En az bir büyük harf, küçük harf, rakam ve sembol içermelidir.

Aşağıda curl kullanarak şifre değiştirmenin bir örneğini gösteriyoruz :

1. Kullanıcıların kullanıcı kimlikleriyle birlikte bir listesini alın:

```
curl -k -X GET "https://localhost:55000/security/users?pretty=true" -H  "Authorization: Bearer $TOKEN"
```

2. İstenilen kullanıcının şifresini değiştirin:

```
curl -k -X PUT "https://localhost:55000/security/users/<USER_ID>" -H "Authorization: Bearer $TOKEN"
-H "Content-Type: application/json" -d '{"password": "<NEW_PASSWORD>"}'
```

`<USER_ID>`Kullanıcının ID'si ve `<NEW_PASSWORD>`yeni şifre ile değiştirin.

> Uyarı: `wazuh-wui` kullanıcı parolasını değiştirmek Wazuh panosunu etkileyecektir. Yeni kimlik bilgileriyle `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml` yapılandırma dosyasını uygun şekilde güncellemeniz gerekecektir. Daha fazla bilgi edinmek için Wazuh gösterge tablosu yapılandırma dosyası belgesine bakın.

3. Varsayılan Host ve Portu Değiştirin

Varsayılan olarak, `host`olarak ayarlanır ve Wazuh sunucu API'sinin tüm kullanılabilir ağ arayüzlerinde gelen bağlantıları kabul etmesine olanak tanır. Erişimi kısıtlamak için, Wazuh sunucu API yapılandırmasını şurada düzenleyin :`['0.0.0.0', '::']`/var/ossec/api/configuration/api.yaml

```
host: ['0.0.0.0', '::']
```

Varsayılan portu da değiştirebilirsiniz:

```
port: 55000
```

Bu parametreleri yapılandırdıktan sonra, Systemd veya SysV init ile Wazuh yönetici servisini kullanarak Wazuh sunucu API'sini yeniden başlatın:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

4. Dakika Başına Maksimum İstek Sayısını Ayarlayın

Wazuh sunucu API'sinin aşırı yüklenmesini önlemek için, API'nin dakikada işleyebileceği maksimum istek sayısını belirlemek için hız sınırlaması uygulayabilirsiniz. Bu sınır aşılırsa, API geri kalan süre boyunca herhangi bir kullanıcıdan gelen diğer istekleri reddeder.

`max_request_per_minute`Varsayılan sınır dakikada 300 istektir. Bunu, içindeki ayarı değiştirerek ayarlayın `/var/ossec/api/configuration/api.yaml`.

> Not: Hız sınırlamasını devre dışı bırakmak için değerini 0 olarak ayarlayın.

5. Maksimum Oturum Açma Girişimi Sayısını Ayarlayın

Kaba kuvvet saldırılarına karşı korunmak için, belirli bir zaman dilimi içinde aynı IP adresinden gelen oturum açma girişimlerini sınırlayabilirsiniz. Bu sınırın aşılması, IP adresini o süre boyunca engeller.

Varsayılan olarak, 300 saniyelik periyotta 50 oturum açma girişimine izin verilir. Bu sınırları ayarlamak için `max_login_attempts` ve/veya `block_time` ayarlarını `/var/ossec/api/configuration/api.yaml`'da düzenleyin.

Revision #5
Created 25 December 2024 23:07:10 by Ayşegül Sarıkaya
Updated 31 December 2024 13:26:28 by Ayşegül Sarıkaya