Yapılandırma

> Not: Wazuh sunucu API'sini nasıl koruyacağınız hakkında daha fazla bilgi için lütfen Wazuh sunucu API'sini güvence altına alma bölümünü inceleyin.

Wazuh Sunucu API Yapılandırma Dosyası

`/var/ossec/api/configuration/api.yaml`Wazuh sunucusu API yapılandırması Wazuh sunucusundaki dosyada bulunur . Varsayılan olarak, tüm ayarlar yorum satırına alınır. Farklı bir yapılandırma uygulamak için, yorum satırını kaldırın ve istediğiniz satırı düzenleyin.

Yapılandırma dosyası için tüm kullanılabilir ayarlar şunlardır `/var/ossec/api/configuration/api.yaml`. Her bir ayar hakkında daha fazla bilgi için yapılandırma seçeneklerini kontrol edin:

```
host: ['0.0.0.0', '::']
port: 55000

drop_privileges: yes
experimental_features: no
max_upload_size: 10485760

intervals:
  request_timeout: 10

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

logs:
  level: "info"
  format: "plain"
  max_size:
   enabled: false

cors:
  enabled: no
```

```
    source_route: "*"
    expose_headers: "*"
    allow_headers: "*"
    allow_credentials: no

  access:
    max_login_attempts: 50
    block_time: 300
    max_request_per_minute: 300

  upload_configuration:
    remote_commands:
      localfile:
        allow: yes
        exceptions: []
      wodle_command:
        allow: yes
        exceptions: []
    limits:
      eps:
        allow: yes
     agents:
      allow_higher_versions:
        allow: yes
     indexer:
      allow: yes
     integrations:
      virustotal:
        public_key:
          allow: yes
          minimum_quota: 240
```

> Uyarı: Bir Wazuh sunucu kümesi çalıştırıldığında, ana düğüm yerel Wazuh sunucu API yapılandırma dosyasını otomatik olarak çalışan düğümlere göndermez. Her düğüm kendi Wazuh sunucu API yapılandırmasını korur. Bu nedenle, ana düğümdeki yapılandırma dosyasında herhangi bir değişiklik yapılırsa, tutarlılığı sağlamak için her çalışan düğümünde yapılandırmayı manuel olarak güncellemelisiniz. Her çalışanın yerel yapılandırmasında IP adresinin ve bağlantı noktasının üzerine yazılmadığından emin olun.

Yapılandırma dosyasını düzenledikten sonra Wazuh yönetici servisini kullanarak Wazuh sunucu API'sini yeniden başlattığınızdan emin olun:

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

API Yapılandırma Seçenekleri

home

İzin verilen değerler	Varsayılan değer	Tanım
Geçerli IP adresleri veya ana bilgisayar adlarının listesi	['0.0.0.0', '::']	Wazuh sunucu API'sinin çalıştığı Wazuh yöneticisinin IP adresleri veya ana bilgisayar adları.

port

İzin verilen değerler	Varsayılan değer	Tanım
1 ile 65535 arasındaki herhangi bir değer	55000	Wazuh sunucu API'sinin dinleyeceği port.

use_only_authd

> 4.3.0 sürümünden itibaren kullanımdan kaldırılmıştır.

İzin verilen değerler	Varsayılan değer	Tanım
evet, doğru, hayır, yanlış	YANLIŞ	Ajanları kaydederken ve kaldırırken wazuh-authd kullanımını zorunlu kılın.

drop_privileges

İzin verilen değerler	Varsayılan değer	Tanım
evet, doğru, hayır, yanlış	doğru	Wazuh-api işlemini kullanıcı olarak çalıştırın `wazuh`.

experimental_features

İzin verilen değerler	Varsayılan değer	Tanım
evet, doğru, hayır, yanlış	YANLIŞ	Geliştirme aşamasındaki özellikleri etkinleştirin

max_upload_size

İzin verilen değerler	Varsayılan değer	Tanım
Herhangi bir pozitif tam sayı	10485760	API'nin kabul edebileceği maksimum gövde boyutunu bayt cinsinden ayarlayın (0 -> sınırsız)

intervals (aralıklar)

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
request_timeout		10	Her API isteği için maksimum yanıt süresini (saniye cinsinden) ayarlayın

https

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
enabled	evet, doğru, hayır, yanlış	doğru	Wazuh sunucu API'sinde SSL'yi (https) etkinleştirin veya devre dışı bırakın.
key	Herhangi bir metin dizesi	sunucu.anahtar	Özel anahtarın adı. İçinde saklanır `/var/ossec/api/configuration/ssl`.
sertifika	Herhangi bir metin dizesi	sunucu.crt	Sertifikanın adı. Şurada saklanır `/var/ossec/api/configuration/ssl`: .
use_ca	evet, doğru, hayır, yanlış	YANLIŞ	Bir Sertifika Yetkilisinden alınan sertifikanın kullanılıp kullanılmayacağı.
ca	Herhangi bir metin dizesi	yaklaşık.krt	Sertifika Yetkilisinin (CA) sertifikasının adı. İçinde saklanır `/var/ossec/api/configuration/ssl`.
ssl_protocol	TLS, TLSv1, TLSv1.1, TLSv1.2, otomatik	4.8.0 sürümündeki yenilikler. otomatik	SSL protokolüne izin vermek için. Değeri büyük/küçük harfe duyarlı değildir.
ssl_ciphers	Herhangi bir metin dizesi	Hiçbiri	SSL şifrelerine izin verilir. Değeri büyük/küçük harfe duyarlı değildir.

logs

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
level	devre dışı, bilgi, uyarı, hata, hata ayıklama, debug2 (her seviye bir önceki seviyeyi içerir)	bilgi	Wazuh sunucusu API günlüklerinin ayrıntı düzeyini ayarlayın.
path	Herhangi bir metin dizesi.	günlükler/api.log	4.3.0 sürümünden itibaren kullanımdan kaldırılmıştır. Wazuh sunucusu API kayıtlarının kaydedileceği yol.
format		ova	4.4.0 sürümündeki yenilikler. Wazuh sunucusu API günlüklerinin biçimini ayarlayın.

max_size

> 4.6.0 sürümündeki yenilikler.

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
enabled	evet, doğru, hayır, yanlış	YANLIŞ	Zaman tabanlı ve boyut tabanlı Wazuh API günlük döndürme arasında geçiş yapın. Bu seçeneği etkinleştirmek zaman tabanlı döndürmeyi devre dışı bırakır ve bunun yerine dosya boyutuna dayalı döndürmeyi etkinleştirir.
size	Geçerli bir birimden sonra gelen herhangi bir pozitif sayı. Kilobayt için K/k, megabayt için M/m.	1M	Boyut tabanlı günlük döndürmeyi tetiklemeyecek şekilde maksimum dosya boyutunu ayarlayın. 1 M'den düşük değerler 1 M olarak kabul edilir.

cors

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
enabled		YANLIŞ	Wazuh sunucu API'sinde CORS kullanımını etkinleştirin veya devre dışı bırakın.
source_route	Herhangi bir metin dizesi	`*`	Kaynakların mevcut olacağı kaynaklar. Örneğin `http://client.example.org`.
expose_headers	Herhangi bir metin dizesi	`*`	Hangi başlıkların yanıtın bir parçası olarak açığa çıkarılabileceği.

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
allow_headers		`*`	Gerçek istek sırasında hangi HTTP başlıklarının kullanılabileceği.
allow_credentials	evet, doğru, hayır, yanlış	YANLIŞ	Tarayıcılara yanıtın ön uç JavaScript'e açılıp açılmayacağını söyleyin.

access (erişim)

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
max_login_attempts	Herhangi bir pozitif tam sayı	50	Belirtilen saniye sayısı içerisinde yapılabilecek maksimum oturum açma girişimi sayısını ayarlayın `block_time`.
block_time		300	Oturum açma isteklerini denemek için belirlenen zaman aralığı (saniye cinsinden). Belirlenen istek sayısı (`max_login_attempts`) bu zaman sınırı içinde aşılırsa, IP adresi blok zaman aralığının sonuna kadar engellenir.
max_request_per_minute	Herhangi bir pozitif tam sayı	300	Dakikada izin verilen maksimum istek sayısı. Kimlik doğrulama istekleri hariç tüm Wazuh sunucu API uç noktaları için geçerlidir. Bu sınıra bir dakikadan kısa sürede ulaşılması, kalan süre boyunca herhangi bir kullanıcıdan gelen tüm istekleri engeller. Bir değeri `0`bu özelliği devre dışı bırakır. İstekler için, etkili değer 30'dan büyük değerler içindir.`POST /events30`

upload_configuration

> 4.4.0 sürümündeki yenilikler.

remote_commands (yerel_dosya ve wodle "komut")

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
allow	evet, doğru, hayır, yanlış	doğru	Wazuh sunucu API'si aracılığıyla uzaktan komutlarla yapılandırmaların yüklenmesine izin verin. Bu seçeneğin ayarlanması, wodle "command" seçeneğini veya localfile etiketi içindeki seçeneği içeren dosyaların `false` yüklenmesini engeller .`ossec.conf<command>`

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
exceptions	komut listesi	[ ]	API aracılığıyla yüklenmesine izin verilen komutların bir listesini ayarlayın. Bu istisnalar yapılandırmadan bağımsız olarak her zaman yüklenebilir `allow`.

sınırlar

eps

> 4.4.0 sürümündeki yenilikler.

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
allow	evet, doğru, hayır, yanlış	doğru	Wazuh sunucu API'si aracılığıyla değiştirilmiş EPS limitleriyle yapılandırmaların yüklenmesine izin verin. Bu seçeneğin ayarlanması, genel etiketin içindeki bölüm değiştiyse dosyaların `false` yüklenmesini engeller. `ossec.conf<limits><eps>`

agents

allow_higher_versions

> 4.6.0 sürümündeki yenilikler.

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
allow	evet, doğru, hayır, yanlış	doğru	Wazuh sunucu API'si aracılığıyla daha yüksek aracı sürümlerini kabul eden yapılandırmaların yüklenmesine izin verin. Bu seçeneğin ayarlanması, auth veya remote etiketleri içindeki değere sahip bölümü içeren dosyaların `false`yüklenmesini engeller .`ossec.conf` `<allow_higher_versions>yes`

indexer

> 4.8.0 sürümündeki yenilikler.

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım

allow	evet, doğru, hayır, yanlış	doğru	Wazuh sunucu API'si aracılığıyla güncellenmiş bir dizinleyici yapılandırma bölümünün yüklenmesine izin verir . Bu seçeneğin ayarlanması `false`, yükleme sırasında dizinleyici yapılandırmasının güncellenmesini önler `ossec.conf`.

entegrasyonlar

> 4.8.0 sürümündeki yenilikler.

virüstotal (public_key)

Alt alanlar	İzin verilen değerler	Varsayılan değer	Tanım
allow	evet, doğru, hayır, yanlış	doğru	Wazuh sunucu API'si aracılığıyla genel bir API anahtarı kullanılarak güncellenmiş bir Virus Total entegrasyon yapılandırma bölümünün yüklenmesine izin verir . Bu seçeneğin ayarlanması `false`, yükleme sırasında entegrasyonların Virus Total yapılandırmasının güncellenmesini önler `ossec.conf`.
minimum_quota	Herhangi bir pozitif tam sayı	240	Virus Total genel API anahtarı için minimum kota değeri.

Wazuh Sunucu API Güvenlik Yapılandırması

`auth_token_exp_timeout`Güvenlik yapılandırmasını ve `rbac_mode`ayarlarını yalnızca Wazuh sunucu API uç noktaları aracılığıyla sorgulayabilir ve değiştirebilirsiniz : GET /security/config , PUT /security/config ve DELETE /security/config . `auth_token_exp_timeout`Bir kimlik doğrulama belirtecinin süresi dolmadan ve yenilenmesi gerekmeden önceki saniye cinsinden süreyi tanımlar. `rbac_mode`Kullanıcı rollerine ve izinlerine göre kaynaklara ve uç noktalara erişimi genel olarak izin vermek veya kısıtlamak üzere yapılandırılabilen Rol Tabanlı Erişim Kontrol sisteminin genel davranışını belirler. Daha fazla ayrıntı için Rol Tabanlı Erişim Kontrol belgelerine bakın. Yapılandırma, geçerliyse bir kümedeki her Wazuh sunucu API'sine uygulanır.

Her bir ayar hakkında daha fazla bilgi için lütfen güvenlik yapılandırma seçeneklerini kontrol edin .

```
auth_token_exp_timeout: 900
rbac_mode: white
```

> Uyarı: Güvenlik nedenleriyle, güvenlik yapılandırmasını değiştirmek tüm JWT'leri iptal eder. Değişiklikten sonra oturum açmanız ve yeni bir token edinmeniz gerekecektir.

Güvenlik Yapılandırma Seçenekleri

auth_token_exp_timeout

İzin verilen değerler	Varsayılan değer	Tanım
Herhangi bir pozitif tam sayı	900	JWT token'larının süresinin dolmasının kaç saniye süreceğini ayarlayın.

rbac_mode

İzin verilen değerler	Varsayılan değer	Tanım
siyah, beyaz	beyaz	RBAC davranışını ayarlayın. Varsayılan olarak, siyah modda her şeye izin verilirken beyaz modda her şey reddedilir. İstenen RBAC altyapısına daha uygun olan rbac_mode'u seçin. Siyah modda, sadece bazı politikalarla birkaç belirli eylem-kaynak çiftini reddetmek çok kolaydır, beyaz mod ise daha güvenlidir ve sıfırdan oluşturulmasını gerektirir.

Yapılandırma Endpoints

Wazuh sunucu API'sinin geçerli yapılandırmasını sorgulamaya izin veren birkaç uç noktası vardır.

Genel API yapılandırmasını değiştirmek için dosyayı Wazuh sunucu API yapılandırma dosyası `/var/ossec/api/configuration/api.yaml` bölümünde ayrıntılı olarak açıklandığı şekilde düzenleyin .

Yapılandırmayı Al

- GET /manager/api/config : Yerel Wazuh sunucusunun API yapılandırmasının tamamını alın.
- GET /cluster/api/config : Tüm küme düğümlerinin (veya bir listesinin) Wazuh sunucusu API yapılandırmasının tamamını alın.
- GET /security/config : Mevcut güvenlik yapılandırmasını alın.

Yapılandırmayı Değiştir

- PUT /security/config : Güvenlik yapılandırmasını değiştirin.

Yapılandırmayı Geri Yükle

- DELETE /security/config : Varsayılan güvenlik yapılandırmasını geri yükler.

SSL sertifikası

> Not: Bu işlem Wazuh sunucu API'si ilk kez çalıştırıldığında otomatik olarak gerçekleştirilir.

SSL sertifikası, Wazuh sunucu API'si ile istemcileri arasında güvenli iletişimi sağlar. Sertifika dosyaları dizinde saklanır `/var/ossec/api/configuration/ssl/`.

Wazuh sunucu API'si için yeni sertifikalar oluşturmak üzere aşağıdaki adımları izleyin:

1. Anahtar ve sertifika isteğini oluşturun (`openssl`paket gereklidir):

   ```
   cd /var/ossec/api/configuration/ssl
   openssl req -newkey rsa:2048 -new -nodes -x509 -days 365 -keyout server.key -out server.crt
   ```

   Varsayılan olarak, anahtarın parolası sunucu her çalıştırıldığında girilmelidir. Anahtar Wazuh sunucu API'si veya yukarıdaki komut tarafından üretilmişse, parolası olmazdı.
2. (İsteğe bağlı) Anahtarı bir parola ile güvenceye alın:

   ```
   ssh-keygen -p -f server.key
   ```

   Yeni şifreyi girmeniz ve onaylamanız istenecektir.

Revision #10
Created 31 December 2024 12:20:10 by Ayşegül Sarıkaya
Updated 31 December 2024 13:26:28 by Ayşegül Sarıkaya