Wazuh Server

Wazuh Server, agentlardan alınan verileri analiz ederek tehditler veya anomalileri tespit ederek uyarılar oluşturur. Ayrıca agentların konfigürasyonlarını uzaktan yönetmek ve durumlarını takip etmek için kullanılır. Wazuh serverlarını single-node veya multi-node kurabilirsiniz. Multi-node mimariler yüksek kullabılabilirlik ve gelişmiş performans sağlar. Load balancer ile birlikte kullanıldığında kapasitesinini daha verimli şekilde kullanılması sağlanabilir.

- Wazuh Kurulum Asistanı
- Adım Adım Kurulum
- Wazuh Server Sistem Gereksinimleri

Wazuh Kurulum Asistanı

Asistan aracılığıla single-node veya multi-node olarak kurulum yapabilirsiniz. Bu bileşen wazuh manager ve filebeat içerir.

1. Wazuh asistan kurulumunu indirin.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

2. Wazuh asistan kurulum dosyasını `--wazuh-server` parametresi ve server node adı ile birlikte kurun. Indexer sunucusunda hazırladığınız `config.yml` dosyasında yer alan isim ile parametre olarak verilen isim aynı olmalıdır.

> Indexer'da oluşturduğunuz wazuh-install-files.tar dosyasının bir kopyasının .sh dosyasını çalıştırdığınız dizinde olduğundan emin olun.

```
bash wazuh-install.sh --wazuh-server wazuh-1
```

Wazuh server kurulumu başarıyla tamamlandı. Eğer birden fazla server node'u kuracaksanız bu işlemi diğer node'lara da uygulamalısınız.

Servislerin doğru çalıştığından emin olmak için aşağıdaki iki komutu kullanabilirsiniz.

```
systemctl status wazuh-manager
systemctl status filebeat
```

Adım Adım Kurulum

Adım adım talimatları izleyerek Wazuh sunucusunu tek düğümlü veya çok düğümlü küme olarak kurun ve yapılandırın. Wazuh sunucusu, Wazuh yöneticisi ve Filebeat'i içeren merkezi bir bileşendir. Wazuh yöneticisi, dağıtılan Wazuh aracılarından veri toplar ve analiz eder. Tehditler veya anormallikler algılandığında uyarıları tetikler. Filebeat, uyarıları ve arşivlenmiş olayları güvenli bir şekilde Wazuh dizinleyicisine iletir.

Kurulum süreci iki aşamaya ayrılıyor.

1. Wazuh sunucu düğümü kurulumu
2. Çoklu düğüm dağıtımı için küme yapılandırması

> **Not:** Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.

1. Wazuh Sunucu Düğümü Kurulumu

Wazuh Deposunu Ekleme

> **Not:** Wazuh sunucusunu Wazuh indeksleyicisinin bulunduğu ana bilgisayara kuruyorsanız, Wazuh deposunu daha önce eklemiş olabileceğiniz için bu adımları atlayabilirsiniz.

Yum:

1. GPG anahtarını içe aktarın.

```
rpm --import https://packages.wazuh.com/key/GPG-KEY-WAZUH
```

2. Depoyu ekleyin.

```
echo -e '[wazuh]\ngpgcheck=1\ngpgkey=https://packages.wazuh.com/key/GPG-KEY-
WAZUH\nenabled=1\nname=EL-$releasever -
Wazuh\nbaseurl=https://packages.wazuh.com/4.x/yum/\nprotect=1' | tee
```

```
/etc/yum.repos.d/wazuh.repo
```

APT:

1. Eğer eksikse aşağıdaki paketleri kurun.

```
apt-get install gnupg apt-transport-https
```

2. GPG anahtarını yükleyin.

```
curl -s https://packages.wazuh.com/key/GPG-KEY-WAZUH | gpg --no-default-keyring --keyring gnupg-ring:/usr/share/keyrings/wazuh.gpg --import && chmod 644 /usr/share/keyrings/wazuh.gpg
```

3. Depoyu ekleyin.

```
echo "deb [signed-by=/usr/share/keyrings/wazuh.gpg] https://packages.wazuh.com/4.x/apt/ stable main" | tee -a /etc/apt/sources.list.d/wazuh.list
```

4. Paket bilgilerini güncelleyin.

```
apt-get update
```

Wazuh yöneticisinin kurulumu

1. Wazuh yönetici paketini yükleyin.

   Yum:

   ```
   yum -y install wazuh-manager
   ```

   APT:

   ```
   apt-get update
   ```

Filebeat'i yükleme

Yum:

```
yum -y install filebeat
```

APT:

```
apt-get -y install filebeat
```

Filebeat'i yapılandırma

1. Önceden yapılandırılmış Filebeat yapılandırma dosyasını indirin.

2. Yapılandırma dosyasını düzenleyin `/etc/filebeat/filebeat.yml`ve aşağıdaki değeri değiştirin:
   a. `hosts`: Bağlanılacak Wazuh dizinleyici düğümlerinin listesi. IP adreslerini veya ana bilgisayar adlarını kullanabilirsiniz. Varsayılan olarak, ana bilgisayar localhost olarak ayarlanmıştır . Bunu uygun şekilde Wazuh dizinleyici adresinizle d in.`hosts: ["127.0.0.1:9200"]`
   b. Birden fazla Wazuh dizinleyici düğümünüz varsa, adresleri virgül kullanarak ayırabilirsiniz. Örneğin,`hosts: ["10.0.0.1:9200", "10.0.0.2:9200", "10.0.0.3:9200"]`

   ```
   # Wazuh - Filebeat configuration file
   output.elasticsearch:
   hosts: ["10.0.0.1:9200"]
   protocol: https
   username: ${username}
   password: ${password}
   ```

3. Kimlik doğrulama bilgilerini güvenli bir şekilde depolamak için bir Filebeat anahtar deposu oluşturun.

   ```
   filebeat keystore create
   ```

4. Varsayılan kullanıcı adı ve parolayı `admin`: `admin`gizli anahtar deposuna ekleyin.

   ```
   echo admin | filebeat keystore add username --stdin --force
   echo admin | filebeat keystore add password --stdin --force
   ```

5. Wazuh indeksleyicisi için uyarı şablonunu indirin.

```
curl -so /etc/filebeat/wazuh-template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.9.2/extensions/elasticsearch/7.x/wazuh-template.json
chmod go+r /etc/filebeat/wazuh-template.json
```

6. Filebeat için Wazuh modülünü yükleyin.

```
curl -s https://packages.wazuh.com/4.x/filebeat/wazuh-filebeat-0.4.tar.gz | tar -xvz -C /usr/share/filebeat/module
```

Sertifikaların Dağıtımı

> **Not:** `wazuh-certificates.tar` İlk yapılandırma adımında oluşturulan dosyanın bir kopyasının çalışma dizininize yerleştirildiğinden emin olun .

1. `<SERVER_NODE_NAME>` Wazuh sunucu düğüm sertifika adınızla değiştirin , `config.yml` sertifikaları oluştururken kullanılanla aynı. Ardından, sertifikaları karşılık gelen konumlarına taşıyın.

```
NODE_NAME=<SERVER_NODE_NAME>
```

```
mkdir /etc/filebeat/certs
tar -xf ./wazuh-certificates.tar -C /etc/filebeat/certs/ ./$NODE_NAME.pem ./$NODE_NAME-key.pem ./root-ca.pem
mv -n /etc/filebeat/certs/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem
mv -n /etc/filebeat/certs/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem
chmod 500 /etc/filebeat/certs
chmod 400 /etc/filebeat/certs/*
chown -R root:root /etc/filebeat/certs
```

Wazuh Indexer Bağlantısını Yapılandırma

> Not: Eğer güvenlik açığı tespit özelliğini kullanmayacaksanız bu adımı atlayabilirsiniz.

> Not: Varsayılan adım adım kurulum kimlik bilgileri şunlardır `admin`:`admin`

1. Wazuh dizinleyici kullanıcı adını ve parolasını wazuh-keystore aracını kullanarak Wazuh yöneticisi anahtar deposuna kaydedin:

```
echo '<INDEXER_USERNAME>' | /var/ossec/bin/wazuh-keystore -f indexer -k username
echo '<INDEXER_PASSWORD>' | /var/ossec/bin/wazuh-keystore -f indexer -k password
```

2. `/var/ossec/etc/ossec.conf`Dizinleyici bağlantısını yapılandırmak için düzenleyin . Varsayılan olarak, dizinleyici ayarları bir ana bilgisayara yapılandırılmıştır. Aşağıda vurgulandığı gibi ayarlanmıştır `0.0.0.0`.

```
<indexer>
  <enabled>yes</enabled>
  <hosts>
    <host>https://0.0.0.0:9200</host>
  </hosts>
  <ssl>
    <certificate_authorities>
      <ca>/etc/filebeat/certs/root-ca.pem</ca>
    </certificate_authorities>
    <certificate>/etc/filebeat/certs/filebeat.pem</certificate>
    <key>/etc/filebeat/certs/filebeat-key.pem</key>
  </ssl>
</indexer>
```

   Wazuh dizinleyici düğüm IP adresiniz veya ana bilgisayar adınızla değiştirin `0.0.0.0`. Bu değeri Filebeat yapılandırma dosyasında bulabilirsiniz `/etc/filebeat/filebeat.yml`.

   Filebeat sertifikasının ve anahtar adının `/etc/filebeat/certs`.

   Bir Wazuh dizinleyici kümeniz varsa, `<host>`düğümlerinizin her biri için bir giriş ekleyin. Örneğin, iki düğümlü bir yapılandırmada:

```
<hosts>
  <host>https://10.0.0.1:9200</host>
  <host>https://10.0.0.2:9200</host>
</hosts>
```

   Güvenlik açığı tespiti, listedeki ilk düğüme raporlamayı önceliklendirir. Kullanılabilir olmadığında bir sonraki düğüme geçer.

Wazuh yöneticisinin başlatılması

1. Wazuh yönetici servisini etkinleştirin ve başlatın.

   SysV Başlatma:

   İşletim sisteminize göre bir seçenek seçin:

   1. RPM tabanlı işletim sistemi:

   ```
   chkconfig --add wazuh-manager
   service wazuh-manager start
   ```

   2. Debian tabanlı işletim sistemi:

   ```
   # update-rc.d wazuh-manager defaults 95 10
   # service wazuh-manager start
   ```

   Systemd:

   ```
   systemctl daemon-reload
   systemctl enable wazuh-manager
   systemctl start wazuh-manager
   ```

2. Wazuh yöneticisinin durumunu doğrulamak için aşağıdaki komutu çalıştırın.

   SysV Başlatma:

   ```
   service wazuh-manager status
   ```

   Systemd:

   ```
   systemctl status wazuh-manager
   ```

Filebeat hizmetini başlatma

1. Filebeat servisini etkinleştirin ve başlatın.

   SysV Başlatma:

   Kullanılan işletim sistemine göre bir seçenek seçin.
   a. RPM tabanlı işletim sistemi:

   ```
   chkconfig --add filebeat
   service filebeat start
   ```

   b. Debian tabanlı işletim sistemi:

   ```
   update-rc.d filebeat defaults 95 10
   service filebeat start
   ```

   Systemd:

   ```
   systemctl daemon-reload
   systemctl enable filebeat
   systemctl start filebeat
   ```

2. Filebeat'in başarıyla yüklendiğini doğrulamak için aşağıdaki komutu çalıştırın.

   ```
   filebeat test output
   ```

   Örnek yanıtı görmek için çıktıyı genişletin.

   Output

   ```
   elasticsearch: https://127.0.0.1:9200...
     parse url... OK
     connection...
       parse host... OK
       dns lookup... OK
       addresses: 127.0.0.1
       dial up... OK
     TLS...
       security: server's certificate chain verification is enabled
       handshake... OK
       TLS version: TLSv1.3
       dial up... OK
     talk to server... OK
     version: 7.10.2
   ```

Wazuh sunucu düğümünüz artık başarıyla kuruldu. Kurulum sürecinin bu aşamasını Wazuh kümenizdeki her Wazuh sunucu düğümü için tekrarlayın, ardından Wazuh kümesini yapılandırmaya devam edin. Wazuh sunucusu tek düğümlü bir küme istiyorsanız, her şey ayarlanmıştır ve doğrudan Wazuh panosunu adım adım yükleme ile devam edebilirsiniz .

2. Çoklu düğüm dağıtımı için küme yapılandırması

Sonraki adımlar

Wazuh sunucu kurulumu artık tamamlandı ve adım adım Wazuh dashboard yüklemeye geçebilirsiniz .

Wazuh sunucusunu kaldırmak istiyorsanız Wazuh sunucusunu kaldırma bölümüne bakın .

Wazuh Server Sistem Gereksinimleri

Wazuh server için desteklenen ve önerilen sistem gereksinimleri ve işletim sistemleri aşağıda yer almaktadır. Kurulum sırasında root kullanıcı yetkisine ihtiyacınız olacak. Multi-node veya single-node olarak kurulum gerçekleştirebilirsiniz.

Önerilen işletim sistemleri

Wazuh 64-bit Linux işletim sistemlerine kurulabilir. Aşağıdaki işletim sistemlerini destekler:

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Donanım Gereksinimleri

	Minimum		Önerilen	
Component	**RAM (GB)**	**CPU (cores)**	**RAM (GB)**	**CPU (cores)**
Wazuh Indexer	2	2	4	8

Veri miktarı, saniye başına oluşturulan uyarılara (APS) bağlıdır. Bu tablo, izlenen uç noktaların türüne bağlı olarak, bir Wazuh server node'unda 90 günlük uyarıları depolamak için aracı başına ihtiyaç duyulan tahmini disk alanının ayrıntılarını verir.

Monitör edilen endpointler	**APS**	**Wazuh Indexer depolama (GB/90 gün)**
Sunucular	0.25	0.1
Workstationlar	0.1	0.04
Ağ cihazları	0.5	0.2

Örneğin, 80 workstation, 10 sunucu ve 10 ağ cihazının bulunduğu bir ortam için Wazuh indeksleyici sunucusunda 90 günlük uyarılar için gereken depolama alanı 6 GB'dir.

Bir Wazuh Server'ın daha fazla kaynak gerektirip gerektirmediğini belirlemek için şu dosyaları izleyin.

- `/var/ossec/var/run/wazuh-analysisd.state` : `events_dropped` değişkeni, olayların kaynak eksikliği nedeniyle bırakılıp bırakılmadığını gösterir.
- `/var/ossec/var/run/wazuh-remoted.state` : `discarded_count` değişkeni, agentlardan gelen mesajların atılıp atılmadığını gösterir.

Ortam düzgün çalışıyorsa bu iki değişkenin sıfır olması gerekir. Aksi takdirde kümeye ek düğümler eklenebilir.