Wazuh Indexer

Wazuh Indexer, yüksek ölçeklenebilir, full-text search ve analiz motorudur. Bu bileşen, Wazuh server tarafından oluşturulan uyarıları indeksler ve saklar. Neredeyse gerçek zamanlı veri arama ve analiz yetenekleri sağlar.

- Wazuh Kurulum Asistanı
- Adım Adım Kurulum
- Wazuh Indexer Sistem Gereksinimleri

Wazuh Kurulum Asistanı

Kurulum asistanı yöntemini kullanarak Wazuh Indexer'ı single-node veya multi-node şeklinde kurabilirsiniz. Bu yöntem manuel yapılacak bazı işlemlerin .sh dosyasına çevrilerek kolaylaştırılmasını sağlamaktadır.

Bu kurulum üç aşamaya ayrılmıştır:

1. İlk konfigürasyon
2. Wazuh indexer nodelarının kurulumu
3. Cluster başlatma

> Tüm komutları çalıştırırken root kullanıcı yetkisine ihtiyacınız olacak. "sudo su" ile root üzerinden kurulumu gerçekleştirmeniz önerilmektedir.

1.Initial configuration

Deployment konfigürasyonunuzu hazırlayın, Wazuh bileşenleri arasındaki iletişimi şifrelemek için SSL sertifikalarını oluşturun ve kurulum sırasında rastgele parolalar oluşturun. Tüm bunlar için aşağıdaki adımları izleyebilirsiniz.

1. Wazuh kurulum asistanı ve konfigürasyon dosyasını indirin.

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

2. `./config.yml` dosyasını düzenleyin. Node isimleri ve IP değerlerini kurulumunuza göre düzenleyin. Eğer tek node kuracaksanız yorum satırlarınızı kaldırmanıza gerek yok. Ancak birden fazla indexer veya manager sunucusu kuracaksanız yorum satırı alanlarına name ve IP değerlerini girmeniz gerekiyor.

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "<indexer-node-ip>"
    #- name: node-2
    #  ip: "<indexer-node-ip>"
```

```
  #- name: node-3
  #  ip: "<indexer-node-ip>"

# Wazuh server nodes
# If there is more than one Wazuh server
# node, each one must have a node_type
server:
  - name: wazuh-1
    ip: "<wazuh-manager-ip>"
  #  node_type: master
  #- name: wazuh-2
  #  ip: "<wazuh-manager-ip>"
  #  node_type: worker
  #- name: wazuh-3
  #  ip: "<wazuh-manager-ip>"
  #  node_type: worker

# Wazuh dashboard nodes
dashboard:
  - name: dashboard
    ip: "<dashboard-node-ip>"
```

3. Kurulum için gerekli Wazuh cluster key, sertifikalar ve parolaları oluşturmak için Wazuh kurulum asistanını `--generate-config-files` parametresi ile birlikte çalıştırın. Bu komut size `./wazuh-install-files.tar` dosyalarını oluşturacak. Diğer sunucuların kurulumunda da bu dosyalara ihtiyacınız olacak. Kurulum boyunca bu dosyaları saklayın ve diğer sunuculara aktarın. Tüm Wazuh kurulumu tamamlandığında bu .tar dosyasını silmeniz faydalı olacaktır.

```
bash wazuh-install.sh --generate-config-files
```

4. `wazuh-install-files.tar` dosyasını diğer wazuh server, wazuh indexer ve wazuh dashboard nodelarına kopyalayın. Bu aşamada `scp` veya farklı yöntemler kullanabilirsiniz.

2. Wazuh Indexer Nodelarının Kurulumu

Daha önce indirdiğiniz `wazuh-install.sh` dosyasını `--wazuh-indexer` parametresi ve node adı ile çalıştırın. Node adı `config.yml` dosyasındaki ile aynı olmalıdır.

```
bash wazuh-install.sh --wazuh-indexer node-1
```

Eğer multi-node bir kurulum planladıysanız, yani birden fazla indexer node'u planlıyorsanız diğer nodelara da aynı işlemi uygulayın.

3. Cluster Başlatma

Kurulumun son aşamasında sertifika bilgilerini yüklemek ve clusterı başlatmak için herhangi bir indexer node'unda kurulum asistanı dosyanızı --start-cluster parametresi ile başlatın.

```
bash wazuh-install.sh --start-cluster
```

> Bu işlemi yalnızca bir indexer node'unda yapmanız yeterlidir. Birden fazla node üzerinde veya tüm node'larda bu işlemi yapmanıza gerek yok.

Kurulumun test edilmesi

Aşağıdaki komutu çalıştırın ve admin parolasını alın.

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

Ardından kurulumun sorunsuz tamamlandığını teyit etmek için aşağıdaki komutu çalıştırın. Önceki komut çıktısından elde ettiğiniz parolayı aşağıdaki <ADMIN_PASSWORD> alanıyla değiştirin. Aynı zamanda wazuh indexer IP adresini de <WAZUH_INDEXER_IP> alanıyla değiştirin.

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200
```

Örnek çıktı aşağıdaki gibiyse kurulumun gerçekleştiğini kabul edebiliriz.

```
{
  "name" : "node-1",
  "cluster_name" : "wazuh-cluster",
  "cluster_uuid" : "095jEW-oRJSFKLz5wmo5PA",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "rpm",
    "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
    "build_date" : "2023-06-03T06:24:25.112415503Z",
```

```
    "build_snapshot" : false,
    "lucene_version" : "9.6.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
```

Parola ve IP değerini tekrar değiştirerek aşağıdaki komutla nodelarınızı test edebilirsiniz.

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200/_cat/nodes?v
```

Adım Adım Kurulum

Wazuh dizinleyicisini adım adım talimatları izleyerek tek düğümlü veya çok düğümlü küme olarak kurun ve yapılandırın. Wazuh dizinleyicisi son derece ölçeklenebilir bir tam metin arama motorudur ve gelişmiş güvenlik, uyarı, dizin yönetimi, derin performans analizi ve diğer birçok özelliği sunar.

Kurulum süreci üç aşamaya ayrılıyor.

1. Sertifika oluşturma
2. Düğüm kurulumu
3. Küme başlatma

> **Not:** Aşağıda açıklanan tüm komutları çalıştırabilmek için root kullanıcı ayrıcalıklarına sahip olmanız gerekir.
> 1. Sertifika Oluşturma

SSL Sertifikalarının Oluşturulması

1. `wazuh-certs-tool.sh`Komut dosyasını ve yapılandırma dosyasını indirin `config.yml`. Bu, Wazuh merkezi bileşenleri arasındaki iletişimleri şifreleyen sertifikaları oluşturur.

   ```
   curl -sO https://packages.wazuh.com/4.9/wazuh-certs-tool.sh
   curl -sO https://packages.wazuh.com/4.9/config.yml
   ```

2. Düğüm adlarını ve IP değerlerini düzenleyin `./config.yml`ve karşılık gelen adlar ve IP adresleriyle değiştirin. Bunu tüm Wazuh sunucusu, Wazuh dizinleyicisi ve Wazuh panosu düğümleri için yapmanız gerekir. Gerektiği kadar düğüm alanı ekleyin.

   ```
   nodes:
     # Wazuh indexer nodes
     indexer:
       - name: node-1
         ip: "<indexer-node-ip>"
       #- name: node-2
       #  ip: "<indexer-node-ip>"
       #- name: node-3
       #  ip: "<indexer-node-ip>"

     # Wazuh server nodes
   ```

```
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
    - name: wazuh-1
      ip: "<wazuh-manager-ip>"
    #  node_type: master
    #- name: wazuh-2
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker
    #- name: wazuh-3
    #  ip: "<wazuh-manager-ip>"
    #  node_type: worker

  # Wazuh dashboard nodes
  dashboard:
    - name: dashboard
      ip: "<dashboard-node-ip>"
```

3. Sertifikaları oluşturmak için çalıştırın `./wazuh-certs-tool.sh`. Çok düğümlü bir küme için, bu sertifikaların daha sonra kümenizdeki tüm Wazuh örneklerine dağıtılması gerekir.

```
bash ./wazuh-certs-tool.sh -A
```

4. Gerekli tüm dosyaları sıkıştırın.

```
tar -cvf ./wazuh-certificates.tar -C ./wazuh-certificates/ .
rm -rf ./wazuh-certificates
```

5. `wazuh-certificates.tar`Dosyayı Wazuh dizinleyicisi, Wazuh sunucusu ve Wazuh panosu düğümleri dahil tüm düğümlere kopyalayın . Bu `scp`, yardımcı programı kullanarak yapılabilir.

2. Düğümlerin Kurulumu

Paket Bağımlılıklarını Yükleme

1. Eksikse aşağıdaki paketleri yükleyin:

   Yum:

```
yum install coreutils
```

APT:

```
apt-get install debconf adduser procps
```

Wazuh Deposunu Ekleme

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 dizinleyicisini yükleme

1. Wazuh indexer paketini yükleyin.

   Yum:

   ```
   # yum -y install wazuh-indexer
   ```

   APT:

   ```
   apt-get -y install wazuh-indexer
   ```

Wazuh dizinleyicisini yapılandırma

1. Edit the `/etc/wazuh-indexer/opensearch.yml` configuration file and replace the following values:

   a. `network.host`: Sets the address of this node for both HTTP and transport traffic. The node will bind to this address and use it as its publish address. Accepts an IP address or a hostname.

Use the same node address set in `config.yml` to create the SSL certificates.

   b. `node.name`: Name of the Wazuh indexer node as defined in the `config.yml` file. For example, `node-1`.

   c. `cluster.initial_master_nodes`: List of the names of the master-eligible nodes. These names are defined in the `config.yml` file. Uncomment the `node-2` and `node-3` lines, change the names, or add more lines, according to your `config.yml` definitions.

```
cluster.initial_master_nodes:
- "node-1"
- "node-2"
- "node-3"
```

d. `discovery.seed_hosts:`Ana uygun düğümlerin adreslerinin listesi. Her bir öğe bir IP adresi veya bir ana bilgisayar adı olabilir. Wazuh dizinleyicisini tek bir düğüm olarak yapılandırıyorsanız bu ayarı yorumlanmış olarak bırakabilirsiniz. Çoklu düğüm yapılandırmaları için bu ayarı yorumlanmamış olarak bırakın ve her ana uygun düğümün IP adreslerini ayarlayın.

```
discovery.seed_hosts:
- "10.0.0.1"
- "10.0.0.2"
- "10.0.0.3"
```

e. `plugins.security.nodes_dn`: List of the Distinguished Names of the certificates of all the Wazuh indexer cluster nodes. Uncomment the lines for `node-2` and `node-3` and change the common names (CN) and values according to your settings and your `config.yml` definitions.

```
plugins.security.nodes_dn:
- "CN=node-1, OU=Wazuh, L=California, C=US"
- "CN=node-2, OU=Wazuh, L=California, C=US"
- "CN=node-3, OU=Wazuh, L=California, C=US"
```

Sertifikaların dağıtımı

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

1. Run the following commands replacing `<indexer-node-name>` with the name of the Wazuh indexer node you are configuring as defined in `config.yml`. For example, `node-1`. This deploys the SSL certificates to encrypt communications between the Wazuh central components.

   ```
   NODE_NAME=<indexer-node-name>
   ```

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

2. **Önerilen eylem** : Bu düğüme başka Wazuh bileşeni yüklenmeyecekse, güvenliği artırmak için `wazuh-certificates.tar` dosyayı çalıştırarak kaldırın. `rm -f ./wazuh-certificates.tar`

Hizmet başlatılıyor

1. Wazuh dizinleyici hizmetini etkinleştirin ve başlatın.

Systemd:

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

SysV Init:

Kullanılan işletim sistemine göre bir seçenek seçin.

1. RPM tabanlı işletim sistemi:

```
chkconfig --add wazuh-indexer
service wazuh-indexer start
```

2. Debian tabanlı işletim sistemi:

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

Kurulum sürecinin bu aşamasını kümenizdeki her Wazuh dizinleyici düğümü için tekrarlayın. Ardından bir sonraki aşamada tek düğümlü veya çok düğümlü kümenizi başlatmaya devam edin.

3. Küme başlatma

1. Yeni sertifika bilgilerini yüklemek ve tek düğümlü veya çok düğümlü kümeyi başlatmak için *herhangi bir* Wazuh dizinleyici düğümünde Wazuh dizinleyici `indexer-security-init.sh` betiğini çalıştırın.

   ```
   # /usr/share/wazuh-indexer/bin/indexer-security-init.sh
   ```

   Not: *Kümeyi yalnızca bir kez* başlatmanız yeterlidir , bu komutu her düğümde çalıştırmanıza gerek yoktur.

Küme Kurulumunu Test Etme

1. `<WAZUH_INDEXER_IP_ADDRESS>`Kurulumun başarılı olduğunu doğrulamak için aşağıdaki komutları değiştirin ve çalıştırın.

   ```
   curl -k -u admin:admin https://<WAZUH_INDEXER_IP_ADRESS>:9200
   ```

   Output

   ```
   {
     "name" : "node-1",
     "cluster_name" : "wazuh-cluster",
     "cluster_uuid" : "095jEW-oRJSFKLz5wmo5PA",
     "version" : {
       "number" : "7.10.2",
       "build_type" : "rpm",
       "build_hash" : "db90a415ff2fd428b4f7b3f800a51dc229287cb4",
       "build_date" : "2023-06-03T06:24:25.112415503Z",
       "build_snapshot" : false,
       "lucene_version" : "9.6.0",
       "minimum_wire_compatibility_version" : "7.10.0",
       "minimum_index_compatibility_version" : "7.0.0"
     },
     "tagline" : "The OpenSearch Project: https://opensearch.org/"
   }
   ```

2. `<WAZUH_INDEXER_IP_ADDRESS>`Tek düğümlü veya çok düğümlü kümenin doğru çalışıp çalışmadığını kontrol etmek için aşağıdaki komutu değiştirin ve çalıştırın.

   ```
   curl -k -u admin:admin https://<WAZUH_INDEXER_IP_ADDRESS>:9200/_cat/nodes?v
   ```

Sonraki adımlar

Wazuh dizinleyicisi artık tek düğümlü veya çok düğümlü kümenize başarıyla yüklendi ve Wazuh sunucusunu yüklemeye devam edebilirsiniz. Bu işlemi gerçekleştirmek için Wazuh sunucusunu adım adım yükleme bölümüne bakın.

Wazuh dizinleyicisini kaldırmak istiyorsanız Wazuh dizinleyicisini kaldırma bölümüne bakın .

Wazuh Indexer Sistem Gereksinimleri

Wazuh indexer 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	4	2	16	8

Veri miktarı, saniye başına oluşturulan uyarılara (APS) bağlıdır. Bu tablo, izlenen uç noktaların türüne bağlı olarak, bir Wazuh indeksleyici sunucusunda 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	3.7
Workstationlar	0.1	1.5
Ağ cihazları	0.5	7.4

Örneğin, 80 workstation, 10 sunucu ve 10 ağ cihazının bulunduğu bir ortam için Wazuh indeksleyici sunucusunda 90 günlük uyarılar için gereken depolama alanı 230 GB'dir.