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 .

Revision #9
Created 6 December 2023 18:06:43 by LastGuard
Updated 23 December 2024 17:50:12 by Ayşegül Sarıkaya