Çevrimdışı Kurulum

İnternet bağlantısı olmasa bile Wazuh'u yükleyebilirsiniz. Çözümü çevrimdışı olarak yüklemek, Wazuh merkezi bileşenlerini indirip daha sonra İnternet bağlantısı olmayan bir sisteme yüklemeyi içerir. Wazuh sunucusu, Wazuh dizinleyicisi ve Wazuh panosu, hepsi bir arada bir dağıtımda aynı ana bilgisayara yüklenebilir ve yapılandırılabilir veya her bileşen, ortam ihtiyaçlarınıza bağlı olarak dağıtılmış bir dağıtım olarak ayrı bir ana bilgisayara yüklenebilir.

- Yardımcıyı Kullanarak Wazuh Bileşenlerini Yükleyin
- Wazuh Bileşenlerini Adım Adım Yükleyin

Yardımcıyı Kullanarak Wazuh Bileşenlerini Yükleyin

Wazuh kurulum asistanının yardımıyla farklı Wazuh bileşenlerini kurun ve yapılandırın.

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

Lütfen ilk yapılandırma adımında oluşturulan `wazuh-install-files.tar`ve `wazuh-offline.tar.gz`dosyalarının bir kopyasının çalışma dizininize yerleştirildiğinden emin olun.

Wazuh Indexer Yükleme

Wazuh dizinleyici düğümlerini kurun ve yapılandırın.

RPM

Wazuh indeksleyici düğümlerine aşağıdaki bağımlılıkların yüklenmesi gerekir.

- coreutils

DEB

Wazuh indeksleyici düğümlerine aşağıdaki bağımlılıkların yüklenmesi gerekir.

- debconf
- adduser
- procps

1. Çevrimdışı bir kurulum gerçekleştirmek için asistanı ile çalıştırın `--offline-installation`. Wazuh dizinleyicisini kurmak ve yapılandırmak için seçeneği `--wazuh-indexer`ve düğüm adını kullanın. Düğüm adı, ilk yapılandırma için kullanılanla aynı olmalıdır `config.yml`, örneğin, `node-1`.

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

Bu adımı kümenizdeki her Wazuh dizinleyici düğümü için tekrarlayın. Ardından bir sonraki adımda tek düğümlü veya çok düğümlü kümenizi başlatmaya devam edin.

2. `--start-cluster` Yeni sertifika bilgilerini yüklemek ve kümeyi başlatmak için herhangi bir Wazuh dizinleyici düğümünde Wazuh kurulum yardımcısını seçeneğiyle çalıştırın.

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

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

Küme Kurulumunu Test Etme

1. *Yönetici* parolasını almak için aşağıdaki komutu çalıştırın :

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

2. Kurulumun başarılı olduğunu doğrulamak için aşağıdaki komutu çalıştırın. `<ADMIN_PASSWORD>` Önceki komutun çıktısından alınan parola ile değiştirin. `<WAZUH_INDEXER_IP>` Yapılandırılmış Wazuh dizinleyici IP adresi ile değiştirin:

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

```
}
```

3. `<WAZUH_INDEXER_IP>`ve ile değiştirin `<ADMIN_PASSWORD>`ve kümenin düzgün çalışıp çalışmadığını kontrol etmek için aşağıdaki komutu çalıştırın:

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

Wazuh Sunucusunun Kurulumu

DEB

Paket yöneticisi olarak apt kullanılan sistemlerde Wazuh sunucu düğümlerine aşağıdaki bağımlılıkların yüklenmesi gerekmektedir.

- gnupg
- apt-transport-https

1. Çevrimdışı bir kurulum gerçekleştirmek için asistanı ile çalıştırın `--offline-installation`. Wazuh sunucusunu kurmak için düğüm adının ardından gelen seçeneği kullanın `--wazuh-server`. Düğüm adı, ilk yapılandırma için kullanılanla aynı olmalıdır `config.yml`, örneğin, `wazuh-1`.

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

Wazuh sunucunuz artık başarıyla kuruldu.

- Eğer bir Wazuh sunucusu çok düğümlü kümesi istiyorsanız, bu adımı her Wazuh sunucusu düğümünde tekrarlayın.
- Eğer Wazuh sunucusunda tek node kümesi istiyorsanız her şey hazır ve doğrudan bir sonraki aşamaya geçebilirsiniz.

Wazuh Dashboard Kurulumu

RPM
Wazuh panosu düğümüne aşağıdaki bağımlılıkların yüklenmesi gerekir.

- libcap

DEB
Wazuh panosu düğümüne aşağıdaki bağımlılıkların yüklenmesi gerekir.

- debhelper sürüm 9 veya üzeri
- tar
- curl
- libcap2-bin

1. Çevrimdışı bir kurulum gerçekleştirmek için asistanı ile çalıştırın `--offline-installation`. Wazuh panosunu kurmak ve yapılandırmak için seçeneği `--wazuh-dashboard`ve düğüm adını kullanın. Düğüm adı, ilk yapılandırma için kullanılanla aynı olmalıdır `config.yml`, örneğin, `dashboard`.

```
bash wazuh-install.sh --offline-installation --wazuh-dashboard dashboard
```

Varsayılan Wazuh web kullanıcı arayüzü portu, Wazuh panosu tarafından kullanılan 443'tür. Bu portu isteğe bağlı parametreyi kullanarak değiştirebilirsiniz . Önerilen bazı portlar 8443, 8444, 8080, 8888 ve 9000'dir.`-p|--port <port_number>`
Yardımcı kurulumu tamamladığında, çıktı erişim kimlik bilgilerini ve kurulumun başarılı olduğunu doğrulayan bir mesajı gösterir.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
  User: admin
  Password: <ADMIN_PASSWORD>

INFO: Installation finished.
```

`wazuh-passwords.txt`Artık Wazuh'u kurdunuz ve yapılandırdınız. Wazuh kurulum asistanı tarafından oluşturulan tüm parolalar arşivin içindeki dosyada bulunabilir `wazuh-install-files.tar` . Bunları yazdırmak için aşağıdaki komutu çalıştırın:

```
tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

2. Kimlik bilgilerinizle Wazuh web arayüzüne erişin.
   - URL: *https://<wazuh-dashboard-ip>*
   - **Kullanıcı adı** : *admin*
   - **Şifre** : *<ADMIN_PASSWORD>*

Wazuh panosuna ilk kez eriştiğinizde, tarayıcı sertifikanın güvenilir bir otorite tarafından verilmediğini belirten bir uyarı mesajı gösterir. Web tarayıcısının gelişmiş seçeneklerine bir istisna eklenebilir. Daha fazla güvenlik için, `root-ca.pem`daha önce oluşturulan dosya bunun

yerine tarayıcının sertifika yöneticisine aktarılabilir. Alternatif olarak, güvenilir bir otoritenin sertifikası yapılandırılabilir.

Wazuh Bileşenlerini Adım Adım Yükleyin

1. `wazuh-offline.tar.gz`ve dosyalarını yerleştirdiğiniz çalışma dizininde `wazuh-install-files.tar`, kurulum dosyalarını açmak için aşağıdaki komutu çalıştırın.

   ```
   tar xf wazuh-offline.tar.gz
   tar xf wazuh-install-files.tar
   ```

   Sıkıştırılmış paket dosyalarının SHA512'sini . adresinden kontrol edebilirsiniz `wazuh-offline/wazuh-packages/`. SHA512 toplam kontrol değerlerini Paketler listesinde bulabilirsiniz.

Wazuh Indexer Yükleme

RPM
Wazuh indeksleyici düğümlerine aşağıdaki bağımlılıkların yüklenmesi gerekir.

- coreutils

DEB
Wazuh indeksleyici düğümlerine aşağıdaki bağımlılıkların yüklenmesi gerekir.

- debconf
- adduser
- procps

1. Wazuh indeksleyicisini yüklemek için aşağıdaki komutları çalıştırın.

   RPM

   ```
   rpm --import ./wazuh-offline/wazuh-files/GPG-KEY-WAZUH
   rpm -ivh ./wazuh-offline/wazuh-packages/wazuh-indexer*.rpm
   ```

   DEB

```
dpkg -i ./wazuh-offline/wazuh-packages/wazuh-indexer*.deb
```

2. Aşağıdaki komutları, `<indexer-node-name>`yapılandırdığınız Wazuh dizinleyici düğümünün adını 'de tanımlandığı gibi değiştirerek çalıştırın `config.yml`. Örneğin, `node-1`. Bu, Wazuh merkezi bileşenleri arasındaki iletişimleri şifrelemek için SSL sertifikalarını dağıtır.

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

```
mkdir /etc/wazuh-indexer/certs
mv -n wazuh-install-files/$NODE_NAME.pem /etc/wazuh-indexer/certs/indexer.pem
mv -n wazuh-install-files/$NODE_NAME-key.pem /etc/wazuh-indexer/certs/indexer-key.pem
mv wazuh-install-files/admin-key.pem /etc/wazuh-indexer/certs/
mv wazuh-install-files/admin.pem /etc/wazuh-indexer/certs/
cp wazuh-install-files/root-ca.pem /etc/wazuh-indexer/certs/
chmod 500 /etc/wazuh-indexer/certs
chmod 400 /etc/wazuh-indexer/certs/*
chown -R wazuh-indexer:wazuh-indexer /etc/wazuh-indexer/certs
```

Burada node-1.pem ve *node-1-key.pem* gibi düğüm sertifikasını ve anahtar dosyalarını ilgili *certs* klasörüne taşırsınız. Bunlar düğüme özgüdür ve diğer düğümlerde gerekli değildir. Ancak, *root-ca.pem* sertifikasının taşınmadığını, *certs* klasörüne kopyalandığını unutmayın. Bu şekilde, sonraki adımlarda diğer bileşen klasörlerine dağıtmaya devam edebilirsiniz.

3. `/etc/wazuh-indexer/opensearch.yml`Aşağıdaki değerleri düzenleyin ve değiştirin:

    1. `network.host`: Bu düğümün adresini hem HTTP hem de taşıma trafiği için ayarlar. Düğüm bu adrese bağlanacak ve ayrıca bunu yayın adresi olarak kullanacaktır. Bir IP adresi veya ana bilgisayar adını kabul eder.
    `config.yml`SSL sertifikalarını oluşturmak için ayarlanan aynı düğüm adresini kullanın .
    2. `node.name`: Dosyada tanımlandığı gibi Wazuh dizinleyici düğümünün adı `config.yml`. Örneğin, `node-1`.
    3. `cluster.initial_master_nodes`: Ana-uygun düğümlerin adlarının listesi. Bu adlar dosyada tanımlanmıştır `config.yml`. `node-2`ve `node-3`satırlarının yorumunu kaldırın, adları değiştirin veya tanımlarınıza göre daha fazla satır ekleyin `config.yml`.

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

4. `discovery.seed_hosts:`Ana uygun düğümlerin adreslerinin listesi. Her bir öğe bir IP adresi veya bir ana bilgisayar adı olabilir. Wazuh dizinleyicisini tek düğüm olarak yapılandırıyorsanız bu ayarı yorumlanmış olarak bırakabilirsiniz. Çok düğümlü yapılandırmalar için bu ayarın yorumunu kaldırın ve ana uygun düğümlerinizin adreslerini ayarlayın.

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

5. `plugins.security.nodes_dn`: Tüm Wazuh dizinleyici küme düğümlerinin sertifikalarının Ayrıcalıklı Adlarının listesi. ve satırlarının yorumunu kaldırın `node-2`ve `node-3`ortak adları (CN) ve değerleri ayarlarınıza ve `config.yml`tanımlarınıza göre değiştirin.

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

4. Wazuh dizinleyici hizmetini etkinleştirin ve başlatın.

- **Systemd**

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

SysV Başlatma
Kullanılan işletim sistemine göre bir seçenek seçin.

- RPM tabanlı işletim sistemi:

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

- Debian tabanlı işletim sistemi:

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

5. Çok düğümlü kümeler için, önceki adımları her Wazuh dizinleyici düğümünde tekrarlayın.

6. Tüm Wazuh dizinleyici düğümleri çalıştığında, yeni sertifika bilgilerini yüklemek ve kümeyi başlatmak için *herhangi bir Wazuh dizinleyici*`indexer-security-init.sh` düğümünde Wazuh dizinleyici

betiğini çalıştırın.

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

7. Kurulumun başarılı olup olmadığını kontrol etmek için aşağıdaki komutu çalıştırın. Bu komutun kullandığını unutmayın `127.0.0.1`, gerekirse Wazuh dizinleyici adresinizi ayarlayın.

```
curl -XGET https://127.0.0.1:9200 -u admin:admin -k
```

Örnek yanıtı görmek için çıktıya göz atın.

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/"
}
```

Wazuh Sunucusunun Kurulumu

DEB
Paket yöneticisi olarak apt kullanılan sistemlerde Wazuh sunucu düğümlerine aşağıdaki bağımlılıkların yüklenmesi gerekmektedir.

- gnupg
- apt-transport-https

1. Wazuh anahtarını içe aktarmak ve Wazuh yöneticisini yüklemek için aşağıdaki komutları çalıştırın.

RPM

```
rpm --import ./wazuh-offline/wazuh-files/GPG-KEY-WAZUH
rpm -ivh ./wazuh-offline/wazuh-packages/wazuh-manager*.rpm
```

DEB

```
dpkg -i ./wazuh-offline/wazuh-packages/wazuh-manager*.deb
```

2. 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
```

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

3. Wazuh yönetici servisini etkinleştirin ve başlatın.

Systemd

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

SysV Başlatma

Kullanılan işletim sistemine göre bir seçenek seçin.

- RPM tabanlı işletim sistemi:

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

- Debian tabanlı işletim sistemi:

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

4. Wazuh yöneticisi durumunun etkin olduğunu doğrulamak için aşağıdaki komutu çalıştırın.

Systemd

```
# systemctl status wazuh-manager
```

SysV Başlatma

```
service wazuh-manager status
```

Filebeat'i Yükleme

Filebeat, Wazuh yöneticisinin kurulu olduğu sunucuda kurulu ve yapılandırılmış olmalıdır.

1. Filebeat'i yüklemek için aşağıdaki komutu çalıştırın.
   RPM

   ```
   rpm -ivh ./wazuh-offline/wazuh-packages/filebeat*.rpm
   ```

   DEB

   ```
   dpkg -i ./wazuh-offline/wazuh-packages/filebeat*.deb
   ```

2. Yapılandırma dosyalarının bir kopyasını uygun konuma taşıyın. Üzerine yazmak için istemde "evet" yazdığınızdan emin olun `/etc/filebeat/filebeat.yml`.

   ```
   cp ./wazuh-offline/wazuh-files/filebeat.yml /etc/filebeat/ &&\
   cp ./wazuh-offline/wazuh-files/wazuh-template.json /etc/filebeat/ &&\
   chmod go+r /etc/filebeat/wazuh-template.json
   ```

3. Yapılandırma dosyasını düzenleyin `/etc/filebeat/filebeat.yml`ve aşağıdaki değeri değiştirin:

   1. `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 değiştirin.`hosts: ["127.0.0.1:9200"]`
      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}
      ```

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

oluşturun.

```
filebeat keystore create
```

5. Kullanıcı adı ve şifreyi `admin`: `admin`gizli anahtar deposuna ekleyin.

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

6. Filebeat için Wazuh modülünü yükleyin.

```
tar -xzf ./wazuh-offline/wazuh-files/wazuh-filebeat-0.4.tar.gz -C /usr/share/filebeat/module
```

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

```
NODE_NAME=<SERVER_NODE_NAME>
```

```
mkdir /etc/filebeat/certs
mv -n wazuh-install-files/$NODE_NAME.pem /etc/filebeat/certs/filebeat.pem
mv -n wazuh-install-files/$NODE_NAME-key.pem /etc/filebeat/certs/filebeat-key.pem
cp wazuh-install-files/root-ca.pem /etc/filebeat/certs/
chmod 500 /etc/filebeat/certs
chmod 400 /etc/filebeat/certs/*
chown -R root:root /etc/filebeat/certs
```

8. Filebeat servisini etkinleştirin ve başlatın.

Systemd

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

SysV Başlatma

Kullanılan işletim sistemine göre bir seçenek seçin.

1. RPM tabanlı işletim sistemi:

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

2. Debian tabanlı işletim sistemi:

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

9. Filebeat'in başarıyla yüklendiğinden emin olmak 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. Kümenizdeki her Wazuh sunucu düğümü için bu kurulum süreci aşamasının adımlarını tekrarlayın, aşağıdaki **çoklu düğüm dağıtımı için Wazuh küme yapılandırmasını** genişletin ve ardından Wazuh kümesini yapılandırmaya devam edin. Wazuh sunucu tek düğümlü bir küme istiyorsanız, her şey ayarlanmıştır ve doğrudan Wazuh panosu kurulumuna geçebilirsiniz.

Çoklu Düğüm Dağıtımı İçin Wazuh Küme Yapılandırması

```
NAME         TYPE    VERSION  ADDRESS
master-node  master  4.9.2    10.0.0.3
worker-node1 worker  4.9.2    10.0.0.4
worker-node2 worker  4.9.2    10.0.0.5
```

Wazuh sunucusunun her node'a kurulumunu tamamladıktan sonra, yalnızca bir sunucu node'unu master olarak, geri kalanını ise workers olarak yapılandırmanız gerekiyor.

Wazuh sunucu ana düğümünü yapılandırma

1. Yapılandırma dosyasında aşağıdaki ayarları düzenleyin `/var/ossec/etc/ossec.conf`.

```
<cluster>
  <name>wazuh</name>
  <node_name>master-node</node_name>
  <node_type>master</node_type>
  <key>c98b62a9b6169ac5f67dae55ae4a9088</key>
  <port>1516</port>
  <bind_addr>0.0.0.0</bind_addr>
  <nodes>
    <node>WAZUH-MASTER-ADDRESS</node>
  </nodes>
  <hidden>no</hidden>
  <disabled>no</disabled>
</cluster>
```

Yapılandırılacak parametreler:

isim	Kümenin adını belirtir.
düğüm_adı	Mevcut düğümün adını belirtir.
düğüm_türü	Düğümün rolünü belirtir. Olarak ayarlanması gerekir `master`.
anahtar	Küme düğümleri arasındaki iletişimi şifrelemek için kullanılan anahtar. Anahtar 32 karakter uzunluğunda olmalı ve kümedeki tüm düğümler için aynı olmalıdır. Aşağıdaki komut rastgele bir anahtar oluşturmak için kullanılabilir: .`openssl rand -hex 16`
liman	Küme iletişimi için hedef portunu belirtir.
bağ_adresi	Düğümün gelen istekleri dinlemek için bağlandığı ağ IP'sidir (herhangi bir IP için 0.0.0.0).
düğümler	Bu, adresidir ve bir IP veya DNS olabilir. Bu parametre, ana bilgisayarın kendisi de dahil olmak üzere tüm düğümlerde belirtilmelidir.`master node`
gizlenmiş	Oluşturulan uyarılarda küme bilgilerinin gösterilmesini veya gizlenmesini sağlar.
engelli	Düğümün kümede etkin mi yoksa devre dışı mı olduğunu gösterir. Bu seçenek olarak ayarlanmalıdır `no`.

2. Wazuh yöneticisini yeniden başlatın.

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
service wazuh-manager restart
```

Wazuh Sunucusu Çalışan Düğümlerini Yapılandırma

1. Dosyadaki aşağıdaki ayarları düzenleyerek küme düğümünü yapılandırın `/var/ossec/etc/ossec.conf`.

```
<cluster>
  <name>wazuh</name>
  <node_name>worker-node</node_name>
  <node_type>worker</node_type>
  <key>c98b62a9b6169ac5f67dae55ae4a9088</key>
  <port>1516</port>
  <bind_addr>0.0.0.0</bind_addr>
  <nodes>
    <node>WAZUH-MASTER-ADDRESS</node>
  </nodes>
  <hidden>no</hidden>
  <disabled>no</disabled>
</cluster>
```

Yapılandırılacak parametreler:

isim	Kümenin adını belirtir.
düğüm_adı	Geçerli düğümün adını belirtir. Kümenin her düğümünün benzersiz bir adı olmalıdır.
düğüm_türü	Düğümün rolünü belirtir. Olarak ayarlanması gerekir `worker`.
anahtar	Düğüm için daha önce oluşturulan anahtar `master`. Tüm düğümler için aynı olması gerekir.
düğümler	Adresini içermesi gerekir ve bir IP veya DNS olabilir. `master node`
engelli	Düğümün kümede etkin mi yoksa devre dışı mı olduğunu gösterir. olarak ayarlanması gerekir `no`.

2. Wazuh yöneticisini yeniden başlatın.

Systemd

```
systemctl restart wazuh-manager
```

SysV Başlatma

```
systemctl restart wazuh-manager
```

Kümenizdeki her Wazuh sunucu çalışan düğümü için bu yapılandırma adımlarını tekrarlayın.

Wazuh sunucu kümesini test etme

Wazuh kümesinin etkinleştirildiğini ve tüm düğümlerin bağlı olduğunu doğrulamak için aşağıdaki komutu yürütün:

```
/var/ossec/bin/cluster_control -l
```

Komutun örnek çıktısı aşağıdaki gibidir:

Output

`10.0.0.3`, `10.0.0.4`, örnek `10.0.0.5`IP'lerdir.

Wazuh Dashboard Kurulumu

RPM

Wazuh panosu düğümüne aşağıdaki bağımlılıkların yüklenmesi gerekir.

- libcap

DEB

Wazuh panosu düğümüne aşağıdaki bağımlılıkların yüklenmesi gerekir.

- debhelper sürüm 9 veya üzeri
- tar
- curl
- libcap2-bin

1. Wazuh panosunu yüklemek için aşağıdaki komutları çalıştırın.

RPM

```
rpm --import ./wazuh-offline/wazuh-files/GPG-KEY-WAZUH
rpm -ivh ./wazuh-offline/wazuh-packages/wazuh-dashboard*.rpm
```

DEB

```
dpkg -i ./wazuh-offline/wazuh-packages/wazuh-dashboard*.deb
```

2. `<DASHBOARD_NODE_NAME>>`Wazuh panonuzun düğüm adıyla değiştirin , `config.yml` sertifikaları oluşturmak için kullanılanla aynı. Örneğin, `dashboard`. Ardından, sertifikaları karşılık gelen konumlarına taşıyın.

```
NODE_NAME=<DASHBOARD_NODE_NAME>>
```

```
mkdir /etc/wazuh-dashboard/certs
mv -n wazuh-install-files/$NODE_NAME.pem /etc/wazuh-dashboard/certs/dashboard.pem
mv -n wazuh-install-files/$NODE_NAME-key.pem /etc/wazuh-dashboard/certs/dashboard-key.pem
cp wazuh-install-files/root-ca.pem /etc/wazuh-dashboard/certs/
chmod 500 /etc/wazuh-dashboard/certs
chmod 400 /etc/wazuh-dashboard/certs/*
chown -R wazuh-dashboard:wazuh-dashboard /etc/wazuh-dashboard/certs
```

3. Dosyayı düzenleyin `/etc/wazuh-dashboard/opensearch_dashboards.yml`ve aşağıdaki değerleri değiştirin:
   1. `server.host`: Bu ayar, arka uç sunucusunun ana bilgisayarını belirtir. Uzak kullanıcıların bağlanmasına izin vermek için, değeri Wazuh panosunun IP adresine veya DNS adına ayarlayın. Değer, `0.0.0.0`ana bilgisayarın tüm kullanılabilir IP adreslerini kabul edecektir.
   2. `opensearch.hosts`: Tüm sorgularınız için kullanılacak Wazuh dizinleyici örneklerinin URL'leri. Wazuh panosu, aynı kümedeki birden fazla Wazuh dizinleyici düğümüne bağlanacak şekilde yapılandırılabilir. Düğümlerin adresleri virgülle ayrılabilir. Örneğin, `["https://10.0.0.2:9200", "https://10.0.0.3:9200","https://10.0.0.4:9200"]`

      ```
      server.host: 0.0.0.0
      server.port: 443
      opensearch.hosts: https://127.0.0.1:9200
      opensearch.ssl.verificationMode: certificate
      ```

4. Wazuh panosunu etkinleştirin ve başlatın.

Systemd

```
systemctl daemon-reload
systemctl enable wazuh-dashboard
```

```
systemctl start wazuh-dashboard
```

SysV Başlatma
İşletim sisteminize göre bir seçenek seçin:

1. RPM tabanlı işletim sistemi:

```
chkconfig --add wazuh-dashboard
service wazuh-dashboard start
```

2. Debian tabanlı işletim sistemi:

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

5. Dosyayı düzenleyin `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml` ve `url` değeri Wazuh sunucusu ana düğümünün IP adresi veya ana bilgisayar adıyla değiştirin.

```
hosts:
  - default:
      url: https://<WAZUH_SERVER_IP_ADDRESS>
      port: 55000
      username: wazuh-wui
      password: wazuh-wui
      run_as: false
```

6. Wazuh panosu hizmetinin etkin olduğunu doğrulamak için aşağıdaki komutu çalıştırın.

Systemd

```
systemctl status wazuh-dashboard
```

SysV Başlatma

```
service wazuh-dashboard status
```

7. Web arayüzüne erişin.
   - URL: *https://<WAZUH_DASHBOARD_IP_ADRESİ>*
   - **Kullanıcı adı** : admin
   - **Şifre** : admin

Wazuh panosuna ilk erişimde, tarayıcı sertifikanın güvenilir bir otorite tarafından verilmediğini belirten bir uyarı mesajı gösterir. Web tarayıcısının gelişmiş seçeneklerinde bir istisna eklenebilir veya daha fazla güvenlik için `root-ca.pem` daha önce oluşturulan dosya tarayıcının sertifika yöneticisine aktarılabilir. Alternatif olarak, güvenilir bir otoritenin sertifikası yapılandırılabilir.

Wazuh Kurulumunuzun Güvenliğini Sağlama

Artık tüm Wazuh merkezi bileşenlerini yüklediniz ve yapılandırdınız. Altyapınızı olası saldırılardan korumak için varsayılan kimlik bilgilerini değiştirmenizi öneririz.

Dağıtım türünüzü seçin ve hem Wazuh API'si hem de Wazuh dizinleyici kullanıcıları için varsayılan parolaları değiştirmek üzere talimatları izleyin.

Hepsi Bir Arada Dağıtım

1. Tüm dahili kullanıcılarınızın şifrelerini değiştirmek için Wazuh şifre aracını kullanın.

```
/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --api --change-all --admin-user wazuh --admin-password wazuh
```

Output

```
INFO: The password for user admin is yWOzmNA.?Aoc+rQfDBcF71KZp?1xd7IO
INFO: The password for user kibanaserver is nUa+66zY.eDF*2rRl5GKdgLxvgYQA+wo
INFO: The password for user kibanaro is 0jHq.4i*VAgclnqFiXvZ5gtQq1D5LCcL
INFO: The password for user logstash is hWW6U45rPoCT?oR.r.Baw2qaWz2iH8Ml
INFO: The password for user readall is PNt5K+FpKDMO2TlxJ6Opb2D0mYl*I7FQ
INFO: The password for user snapshotrestore is +GGz2noZZr2qVUK7xbtqjUup049tvLq.
WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard a
INFO: The password for Wazuh API user wazuh is JYWz5Zdb3Yq+uOzOPyUU4oat0n60VmWI
INFO: The password for Wazuh API user wazuh-wui is +fLddaCiZePxh24*?jC0nyNmgMGCKE+2
INFO: Updated wazuh-wui user password in wazuh dashboard. Remember to restart the service.
```

Dağıtılmış Dağıtım

1. *Herhangi bir Wazuh dizinleyici* düğümünde , Wazuh dizinleyici kullanıcılarının parolalarını değiştirmek için Wazuh parolaları aracını kullanın.

```
/usr/share/wazuh-indexer/plugins/opensearch-security/tools/wazuh-passwords-tool.sh --change-all
```

Output

```
INFO: Wazuh API admin credentials not provided, Wazuh API passwords not changed.
INFO: The password for user admin is wcAny.XUwOVWHFy.+7tW9l8gUW1L8N3j
INFO: The password for user kibanaserver is qy6fBrNOI4fD9yR9.Oj03?pihN6Ejfpp
INFO: The password for user kibanaro is Nj*sSXSxwntrx3O7m8ehrgdHkxCc0dna
```

```
INFO: The password for user logstash is nQg1Qw0nIQFZXUJc8r8+zHVrkelch33h
INFO: The password for user readall is s0iWAei?RXObSDdibBfzSgXdhZCD9kH4
INFO: The password for user snapshotrestore is Mb2EHw8SIc1d.oz.nM?dHiPBGk7s?UZB
WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard a
```

2. Wazuh sunucunuzun *ana* düğümünde , yönetici kullanıcılarının varsayılan parolasını değiştirin: *wazuh* ve *wazuh-wui* . Aşağıdaki komutların 127.0.0.1 kullandığını unutmayın, gerekirse Wazuh yöneticinizin IP adresini ayarlayın.

    1. Yetkilendirme TOKEN'ı alın.

    ```
    TOKEN=$(curl -u wazuh-wui:wazuh-wui -k -X GET
    "https://127.0.0.1:55000/security/user/authenticate?raw=true")
    ```

    2. *Wazuh* kullanıcı kimlik bilgilerini (ID 1) değiştirin . 8 ila 64 karakter uzunluğunda bir parola seçin, en az bir büyük harf ve bir küçük harf, bir sayı ve bir sembol içermelidir. Daha fazla bilgi edinmek için PUT /security/users/{user_id} bölümüne bakın .

    ```
    curl -k -X PUT "https://127.0.0.1:55000/security/users/1" -H "Authorization: Bearer $TOKEN" -H 'Content-Ty
    {
      "password": "SuperS3cretPassword!"
    }'
    ```

    Output

    ```
    {"data": {"affected_items": [{"id": 1, "username": "wazuh", "allow_run_as": true, "roles": [1]}], "total_affe
    ```

    3. *Wazuh-wui* kullanıcı kimlik bilgilerini (ID 2) değiştirin .

    ```
    curl -k -X PUT "https://127.0.0.1:55000/security/users/2" -H "Authorization: Bearer $TOKEN" -H 'Content-Ty
    {
      "password": "SuperS3cretPassword!"
    }'
    ```

    Output

    ```
    {"data": {"affected_items": [{"id": 2, "username": "wazuh-wui", "allow_run_as": true, "roles": [1]}], "total_
    ```

    Ek güvenlik yapılandırmaları için Wazuh API'sini Güvence Altına Alma bölümüne bakın.

    > Not: Bu şifreleri güvenli bir yerde saklamayı unutmayın.

3. *Tüm Wazuh sunucu düğümlerinizde* , Filebeat anahtar deposundaki *yönetici* parolasını güncellemek için aşağıdaki komutu çalıştırın . `<ADMIN_PASSWORD>`İlk adımda oluşturulan rastgele parola ile değiştirin.

```
echo <ADMIN_PASSWORD> | filebeat keystore add password --stdin --force
```

4. Değişikliği uygulamak için Filebeat'i yeniden başlatın.

Systemd

```
systemctl restart filebeat
```

SysV Başlatma

```
service filebeat restart
```

> Not: 3. ve 4. adımları *her Wazuh sunucu düğümünde* tekrarlayın.

5. *Wazuh kontrol paneli* düğümünüzde , Wazuh kontrol paneli anahtar deposundaki *kibanaserver* parolasını güncellemek için aşağıdaki komutu çalıştırın . `<KIBANASERVER_PASSWORD>`İlk adımda oluşturulan rastgele parola ile değiştirin.

```
echo <KIBANASERVER_PASSWORD> | /usr/share/wazuh-dashboard/bin/opensearch-dashboards-keystore --allow-root add -f --stdin opensearch.password
```

6. İkinci adımda oluşturulan `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml`yeni *wazuh-wui* şifresi ile yapılandırma dosyasını güncelleyin.

```
hosts:
  - default:
      url: https://127.0.0.1
      port: 55000
      username: wazuh-wui
      password: "<wazuh-wui-password>"
      run_as: false
```

7. Değişiklikleri uygulamak için Wazuh panosunu yeniden başlatın.

Systemd

```
systemctl restart wazuh-dashboard
```

SysV Başlatma

```
service wazuh-dashboard restart
```

Sonraki Adımlar

Wazuh ortamı hazır olduğunda, izlenecek her uç noktaya Wazuh aracıları yüklenebilir. Wazuh aracılarını yüklemek ve uç noktaları izlemeye başlamak için Wazuh aracı yükleme bölümüne bakın. Bunları çevrimdışı yüklemeniz gerekiyorsa, izlenen sisteminiz için indirilecek uygun aracı paketini Wazuh aracı paketleri listesi bölümünden kontrol edebilirsiniz.

Tüm Wazuh Central bileşenlerini kaldırmak için Wazuh Central bileşenlerini kaldırma bölümüne bakın.