Adım Adım Kurulum

Adım adım talimatları izleyerek Wazuh panosunu kurun ve yapılandırın. Wazuh panosu, Wazuh sunucu uyarılarını ve arşivlenmiş olayları çıkarmak ve görselleştirmek için bir web arayüzüdür.

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

Wazuh Gösterge Paneli Kurulumu

Paket Bağımlılıklarını Yükleme

1. Eğer eksikse aşağıdaki paketleri kurun.
   Yum:

   ```
   yum install libcap
   ```

   APT:

   ```
   apt-get install debhelper tar curl libcap2-bin #debhelper version 9 or later
   ```

Wazuh Deposunu Ekleme

> **Not:** Wazuh panosunu Wazuh indeksleyicisi veya Wazuh sunucusuyla aynı ana bilgisayara yüklüyorsanız, Wazuh deposunu zaten 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 Panosunun Kurulumu

1. Wazuh gösterge paneli paketini yükleyin.

Yum:

```
yum -y install wazuh-dashboard
```

APT:

```
apt-get -y install wazuh-dashboard
```

Wazuh Panosunu Yapılandırma

1. Dosyayı düzenleyin `/etc/wazuh-dashboard/opensearch_dashboards.yml`ve aşağıdaki değerleri değiştirin:

   a. `server.host`: Bu ayar, Wazuh gösterge paneli sunucusunun ana bilgisayarını belirtir. Uzak kullanıcıların bağlanmasına izin vermek için, değeri Wazuh gösterge paneli sunucusunun IP adresine veya DNS adına ayarlayın. Değer, `0.0.0.0`ana bilgisayarın tüm kullanılabilir IP adreslerini kabul edecektir.

   b. `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://localhost:9200
opensearch.ssl.verificationMode: certificate
```

Sertifikaların Dağıtımı

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

1. `<DASHBOARD_NODE_NAME>`Sertifikaları oluşturmak için kullandığınız aynı adla Wazuh kontrol paneli düğümünüzün adını değiştirin `config.yml`ve sertifikaları ilgili konumlarına taşıyın.

1.
```
NODE_NAME=<DASHBOARD_NODE_NAME>
```

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

Wazuh Panosu Hizmeti Başlatılıyor

1. Wazuh gösterge paneli hizmetini etkinleştirin ve başlatın.

   Systemd:

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

   SysV Başlatma:

   İşletim sisteminize göre bir seçenek seçin:

   - RPM tabanlı işletim sistemi:

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

   - Debian tabanlı işletim sistemi:

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

2. 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
```

3. Kimlik bilgilerinizle Wazuh web arayüzüne erişin.
    - URL: *https://<WAZUH_DASHBOARD_IP_ADRESİ>*
    - **Kullanıcı adı** : *admin*
    - **Şifre** : *admin*

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 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 kullanıcıların 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* , Wazuh parolaları aracını indirin ve bunu kullanarak Wazuh API kullanıcılarının parolalarını değiştirin.

   ```
   curl -sO https://packages.wazuh.com/4.9/wazuh-passwords-tool.sh
   bash wazuh-passwords-tool.sh --api --change-all --admin-user wazuh --admin-password wazuh
   ```

   Output

   ```
   INFO: The password for Wazuh API user wazuh is ivLOfmj7.jL6*7Ev?UJoFjrkGy9t6Je.
   INFO: The password for Wazuh API user wazuh-wui is fL+f?sFRPEv5pYRE559rqy9b6G4Z5pVi
   ```

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 merkezi bileşenlerinin tamamı başarıyla kuruldu ve sabitlendi.

Wazuh ortamı artık hazır ve izlenecek uç noktalara Wazuh aracısını yüklemeye devam edebilirsiniz. Bu eylemi gerçekleştirmek için Wazuh aracısı bölümüne bakın.

Wazuh panosunu kaldırmak istiyorsanız Wazuh panosunu kaldırma bölümüne bakın .

Revision #7
Created 6 December 2023 18:07:43 by LastGuard
Updated 23 December 2024 17:52:42 by Ayşegül Sarıkaya