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.

Revision #6
Created 25 December 2024 21:12:20 by Ayşegül Sarıkaya
Updated 25 December 2024 21:44:05 by Ayşegül Sarıkaya