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
```

Revision #2
Created 6 December 2023 18:06:22 by LastGuard
Updated 24 October 2024 08:31:26 by LastGuard