Kubernetes'e Yüklenen Wazuh'u Yükseltin

Hangi Dosyaların Birime Aktarılacağının Kontrol Edilmesi

Kubernetes dağıtımımız Docker'dan Wazuh görüntülerimizi kullanır. Docker kullanarak Wazuh yapılandırmasından çıkarılan aşağıdaki koda bakarsak, yükseltmede hangi dizinlerin ve dosyaların kullanıldığını görebiliriz.

```
/var/ossec/api/configuration
/var/ossec/etc
/var/ossec/logs
/var/ossec/queue
/var/ossec/var/multigroups
/var/ossec/integrations
/var/ossec/active-response/bin
/var/ossec/agentless
/var/ossec/wodles
/etc/filebeat
/var/lib/filebeat
/usr/share/wazuh-dashboard/config/
/usr/share/wazuh-dashboard/certs/
/var/lib/wazuh-indexer
/usr/share/wazuh-indexer/certs/
/usr/share/wazuh-indexer/opensearch.yml
/usr/share/wazuh-indexer/opensearch-security/internal_users.yml
```

Bu dosyalarla ilgili herhangi bir değişiklik ilişkili birimde de yapılacaktır. Replika pod oluşturulduğunda, önceki değişiklikleri koruyarak bu dosyaları birimden alacaktır.

Sertifikaların Yeniden Oluşturulması

v4.8.0'dan önceki bir sürümden yükseltme yapmak SSL sertifikalarını yeniden oluşturmanızı gerektirir. Bunun için SSL sertifikalarını kurun bölümündeki talimatları izleyin.

Yükseltmeyi Yapılandırma

4.9 sürümüne yükseltmek için iki stratejiden birini izleyebilirsiniz.

- Varsayılan manifestoları kullanma : Bu strateji Wazuh 4.9 için varsayılan manifestoları kullanır. Güncel olmayan Wazuh sürümünüzün wazuh-kubernetes manifestolarını değiştirir.
- Özel bildirimleri tutma : Bu strateji, güncel olmayan Wazuh dağıtımınızın wazuh-kubernetes bildirimlerini korur. En son Wazuh sürümünün bildirimlerini yok sayar.

Varsayılan Bildirimleri Kullanma

1. Wazuh-kubernetes'in güncel sürümü için etiketi inceleyin:

   ```
   git checkout v4.9.2
   ```

2. Yeni yapılandırmayı uygula

Özel Beyannamelerin Tutulması

Wazuh 4.4'te bazı yollar önceki sürümlerdekilerden farklıdır. Özel bildirimlerinizi tutuyorsanız eski yolları yenileriyle güncellemelisiniz.

`old-path->new-path`

- `/usr/share/wazuh-dashboard/config/certs/->/usr/share/wazuh-dashboard/certs/`
- `/usr/share/wazuh-indexer/config/certs/->/usr/share/wazuh-indexer/certs/`
- `/usr/share/wazuh-indexer/plugins/opensearch-security/securityconfig/->/usr/share/wazuh-indexer/opensearch-security/`

Özel bildirimlerinizi koruyarak dağıtımınızı yükseltmek için aşağıdakileri yapın.

1. 4.3'ten güncelleme yapıyorsanız, aşağıdaki dosyaları düzenleyin ve 4.4'teki yeni yollarla güncelleyin. Aşağıdaki örneklerde her dosyanın yanında yeni yolları görebilirsiniz.

   - `wazuh/indexer_stack/wazuh-dashboard/dashboard-deploy.yaml`

     ```
     image: 'wazuh/wazuh-dashboard:4.9.2'
     mountPath: /usr/share/wazuh-dashboard/certs/cert.pem
     mountPath: /usr/share/wazuh-dashboard/certs/key.pem
     ```

```
mountPath: /usr/share/wazuh-dashboard/certs/root-ca.pem
value: /usr/share/wazuh-dashboard/certs/cert.pem
value: /usr/share/wazuh-dashboard/certs/key.pem
```

- `wazuh/indexer_stack/wazuh-dashboard/dashboard_conf/opensearch_dashboards.yml`

```
server.ssl.key: "/usr/share/wazuh-dashboard/certs/key.pem"
server.ssl.certificate: "/usr/share/wazuh-dashboard/certs/cert.pem"
opensearch.ssl.certificateAuthorities: ["/usr/share/wazuh-dashboard/certs/root-ca.pem"]
```

- `wazuh/indexer_stack/wazuh-indexer/cluster/indexer-sts.yaml`

```
image: 'wazuh/wazuh-indexer:4.9.2'
mountPath: /usr/share/wazuh-indexer/certs/node-key.pem
mountPath: /usr/share/wazuh-indexer/certs/node.pem
mountPath: /usr/share/wazuh-indexer/certs/root-ca.pem
mountPath: /usr/share/wazuh-indexer/certs/admin.pem
mountPath: /usr/share/wazuh-indexer/certs/admin-key.pem
mountPath: /usr/share/wazuh-indexer/opensearch.yml
mountPath: /usr/share/wazuh-indexer/opensearch-security/internal_users.yml
```

- `wazuh/indexer_stack/wazuh-indexer/indexer_conf/opensearch.yml`

```
plugins.security.ssl.http.pemcert_filepath: /usr/share/wazuh-indexer/certs/node.pem
plugins.security.ssl.http.pemkey_filepath: /usr/share/wazuh-indexer/certs/node-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /usr/share/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /usr/share/wazuh-indexer/certs/node.pem
plugins.security.ssl.transport.pemkey_filepath: /usr/share/wazuh-indexer/certs/node-key.pem
plugins.security.ssl.transport.pemtrustedcas_filepath: /usr/share/wazuh-indexer/certs/root-ca.pem
```

- `wazuh/wazuh_managers/wazuh-master-sts.yaml`

```
image: 'wazuh/wazuh-manager:4.9.2'
```

- `wazuh/wazuh_managers/wazuh-worker-sts.yaml`

```
image: 'wazuh/wazuh-manager:4.9.2'
```

2. Yeni yapılandırmayı uygula

Yeni Yapılandırmayı Uygula

Son adım yeni yapılandırmayı uygulamaktır:

- EKS kümesi

```
kubectl apply -k envs/eks/
```

- Diğer küme türleri

```
kubectl apply -k envs/local-env/
```

Output

```
statefulset.apps "wazuh-manager-master" configured
```

Bu işlem eski pod'u sonlandırırken aynı birime bağlı yeni bir sürümle yeni bir pod yaratacaktır. Pod'lar başlatıldığında güncelleme hazır olacak ve yüklenen yeni Wazuh sürümünü, kümeyi ve birimlerin kullanımıyla korunan değişiklikleri kontrol edebiliriz.

Revision #4
Created 23 December 2024 22:34:15 by Ayşegül Sarıkaya
Updated 23 December 2024 22:43:33 by Ayşegül Sarıkaya