Dağıtım

Gerekli servisleri ve pod'ları dağıtmak için bu deponun klonunu oluşturun.

```
git clone https://github.com/wazuh/wazuh-kubernetes.git -b v4.9.2 --depth=1
cd wazuh-kubernetes
```

SSL Sertifikalarını Kurun

Wazuh dizinleyici kümesi için kendi kendine imzalı sertifikaları adresindeki betiği kullanarak üretebilir `wazuh/certs/indexer_cluster/generate_certs.sh` veya kendi betiğinizi sağlayabilirsiniz.

Wazuh panosu kümesi için kendi imzalı sertifikaları adresindeki betiği kullanarak üretebilir `wazuh/certs/dashboard_http/generate_certs.sh` veya kendi betiğinizi sağlayabilirsiniz.

Gerekli sertifikalar secretGenerator aracılığıyla şu dosyaya aktarılır `kustomization.yml`:

```
secretGenerator:
  - name: indexer-certs
    files:
      - certs/indexer_cluster/root-ca.pem
      - certs/indexer_cluster/node.pem
      - certs/indexer_cluster/node-key.pem
      - certs/indexer_cluster/dashboard.pem
      - certs/indexer_cluster/dashboard-key.pem
      - certs/indexer_cluster/admin.pem
      - certs/indexer_cluster/admin-key.pem
      - certs/indexer_cluster/filebeat.pem
      - certs/indexer_cluster/filebeat-key.pem
  - name: dashboard-certs
    files:
      - certs/dashboard_http/cert.pem
      - certs/dashboard_http/key.pem
      - certs/indexer_cluster/root-ca.pem
```

Depolama Sınıfını Ayarlayın (EKS Olmayan Küme İçin İsteğe Bağlı)

Çalıştırdığınız kümenin türüne bağlı olarak, Depolama Sınıfı farklı bir sağlayıcıya sahip olabilir.

Sizinkini çalıştırarak kontrol edebilirsiniz . Şuna benzer bir şey göreceksiniz:`kubectl get sc`

```
kubectl get sc
NAME                      PROVISIONER          RECLAIMPOLICY   VOLUMEBINDINGMODE
ALLOWVOLUMEEXPANSION   AGE
elk-gp2                   microk8s.io/hostpath   Delete          Immediate          false                  67d
microk8s-hostpath (default)   microk8s.io/hostpath   Delete          Immediate          false                  54d
```

Provizyonlayıcı sütunu microk8s.io/hostpath'i gösteriyor, dosyayı düzenlemeli `envs/local-env/storage-class.yaml` ve bu provizyonlayıcıyı ayarlamalısınız.

Tüm Bildirimleri Kustomize Kullanarak Uygulayın

Manifest'in iki çeşidi vardır: `eks`ve `local-env`. EKS kümesini kullanıyorsanız eks manifest'i kullanılmalıdır, diğer küme türleri için ise local-env manifest'i kullanılmalıdır.

Hangi bildirimi dağıtmak istediğinize bağlı olarak, yamaları düzenleyerek küme için kaynakları ayarlamak mümkündür. Her küme nesnesinin kalıcı birimleri için CPU, bellek ve depolamayı ayarlayabilirsiniz. Bu, bu yamaları kaldırarak `envs/eks/`veya yamaların kendilerini farklı değerlerle değiştirerek geri alınabilir.`envs/local-env/kustomization.yaml`

Özelleştirme dosyasını kullanarak kümeyi tek bir komutla dağıtabiliriz:

- EKS kümesi

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

- Diğer küme türleri

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

Dağıtımın Doğrulanması

Ad alanı

```
kubectl get namespaces | grep wazuh
```

Output

```
wazuh        Active    12m
```

Hizmetler

```
kubectl get services -n wazuh
```

Output

```
NAME              TYPE          CLUSTER-IP       EXTERNAL-IP       PORT(S)                    AGE
indexer           ClusterIP     xxx.yy.zzz.24    <none>            9200/TCP                   12m
dashboard         ClusterIP     xxx.yy.zzz.76    <none>            5601/TCP                   11m
wazuh             LoadBalancer  xxx.yy.zzz.209   internal-a7a8...  1515:32623/TCP,55000:30283/TCP  9m
wazuh-cluster     ClusterIP     None             <none>            1516/TCP                   9m
Wazuh-indexer     ClusterIP     None             <none>            9300/TCP                   12m
wazuh-workers     LoadBalancer  xxx.yy.zzz.26    internal-a7f9...  1514:31593/TCP             9m
```

Dağıtımlar

```
kubectl get deployments -n wazuh
```

Output

```
NAME           DESIRED   CURRENT   UP-TO-DATE   AVAILABLE   AGE
wazuh-dashboard  1       1         1            1           11m
```

Durum Kümesi

```
kubectl get statefulsets -n wazuh
```

Output

```
NAME              READY   AGE
wazuh-indexer     3/3     15m
```

```
wazuh-manager-master   1/1     15m
wazuh-manager-worker   2/2     15m
```

Baklalar

```
kubectl get pods -n wazuh
```

Output

```
NAME                          READY     STATUS    RESTARTS   AGE
wazuh-indexer-0               1/1       Running   0          15m
wazuh-dashboard-f4d9c7944-httsd   1/1       Running   0          14m
wazuh-manager-master-0          1/1       Running   0          12m
wazuh-manager-worker-0-0        1/1       Running   0          11m
wazuh-manager-worker-1-0        1/1       Running   0          11m
```

Wazuh panosuna erişim

Hizmetler için alan adları oluşturduysanız, önerilen alan adını kullanarak panoya erişebilmelisiniz: `https://wazuh.your-domain.com`. Bulut sağlayıcıları genellikle panoya doğrudan erişim için harici bir IP adresi veya ana bilgisayar adı sağlar. Bu, hizmetleri kontrol ederek görüntülenebilir:

```
kubectl get services -o wide -n wazuh
```

Output

```
 NAME              TYPE          CLUSTER-IP       EXTERNAL-IP                PORT(S)                      AGE
SELECTOR
 dashboard         LoadBalancer   xxx.xx.xxx.xxx   xxx.xx.xxx.xxx             80:31831/TCP,443:30974/TCP
15m       app=wazuh-dashboard
```

İsteğe bağlı : Harici IP adresine erişilemeyen yerel bir küme dağıtımında şunları kullanabilirsiniz `port-forward`:

```
kubectl -n wazuh port-forward --address <INTERFACE_IP_ADDRESS> service/dashboard 8443:443
```

`<INTERFACE_IP_ADDRESS>`Kubernetes ana bilgisayarının IP adresi nerede ?

Wazuh kontrol paneline şu adresten ulaşabilirsiniz `https://<INTERFACE_IP_ADDRESS>:8443`: .

Varsayılan kimlik bilgileri şunlardır `admin:SecretPassword`: .

Wazuh Kullanıcılarının Şifresini Değiştirin

Güvenliği artırmak için Wazuh kullanıcılarının varsayılan şifresini değiştirebilirsiniz. İki tür Wazuh kullanıcısı vardır:

- Wazuh dizinleyici kullanıcıları
- Wazuh API kullanıcıları

Wazuh Dizinleyici Kullanıcıları

Varsayılan `admin` ve `kibanaserver` kullanıcıların şifrelerini değiştirmek için aşağıdakileri yapın.

> Uyarı: Özel kullanıcılarınız varsa, bunları `internal_users.yml` dosyaya ekleyin. Aksi takdirde, bu prosedürü yürütmek onları siler.

Wazuh Dashboard Oturumunuzu Kapatma

Şifre değiştirme işlemine başlamadan önce Wazuh kontrol paneli oturumunuzdan çıkış yapmanızı öneririz.

Çıkış yapmadığınız takdirde, kalıcı oturum çerezleri kullanıcı şifrelerini değiştirdikten sonra Wazuh'a erişirken hatalara neden olabilir.

Yeni Bir Hash Ayarlama

1. `wazuh-indexer-0`'de bir Bash kabuğu başlatın.

   ```
   kubectl exec -it wazuh-indexer-0 -n wazuh -- /bin/bash
   ```

2. Yeni parolanızın karmasını oluşturmak için bu komutları çalıştırın. İstendiğinde, yeni parolayı girin ve **Enter'a** basın.

   ```
   wazuh-indexer@wazuh-indexer-0:~$ export JAVA_HOME=/usr/share/wazuh-indexer/jdk
   wazuh-indexer@wazuh-indexer-0:~$ bash /usr/share/wazuh-indexer/plugins/opensearch-security/tools/hash.sh
   ```

3. Oluşturulan hash'i kopyalayın ve Bash kabuğundan çıkın.
4. Dosyayı açın `wazuh/indexer_stack/wazuh-indexer/indexer_conf/internal_users.yml`. Şifresini değiştirdiğiniz kullanıcıya ait bloğu bulun.

5. Karmayı değiştirin.
   - `admin`kullanıcı

     ```
     ...
     admin:
       hash: "$2y$12$K/SpwjtB.wOHJ/Nc6GVRDuc1h0rM1DfvziFRNPtk27P.c4yDr9njO"
       reserved: true
       backend_roles:
       - "admin"
       description: "Demo admin user"

     ...
     ```

   - `kibanaserver`kullanıcı

     ```
     ...
     kibanaserver:
       hash: "$2a$12$4AcgAt3xwOWadA5s5blL6ev39OXDNhmOesEoo33eZtrq2N0YrU3H."
       reserved: true
       description: "Demo kibanaserver user"

     ...
     ```

Yeni Şifreyi Ayarlama

> Uyarı: Yeni şifrenizde `$`veya `&` karakterlerini kullanmayın . Bu karakterler dağıtım sırasında hatalara neden olabilir.

1. Yeni parolanızı base64 biçiminde kodlayın. Karma değerini korumak için son satır karakteri eklemekten kaçının. Örneğin, seçeneği `-n`komutla `echo`aşağıdaki gibi kullanın.

   ```
   echo -n "NewPassword" | base64
   ```

2. Dizinleyici veya pano sırları yapılandırma dosyasını aşağıdaki gibi düzenleyin. Alanın değerini `password`yeni kodlanmış parolanızla değiştirin.
   - Kullanıcı şifresini değiştirmek için dosyayı `admin`düzenleyin `wazuh/secrets/indexer-cred-secret.yaml`.

     ```
     ...
     apiVersion: v1
     kind: Secret
     metadata:
       name: indexer-cred
     data:
       username: YWRtaW4=              # string "admin" base64 encoded
       password: U2VjcmV0UGFzc3dvcmQ=  # string "SecretPassword" base64 encoded
     ```

```
...
```

- Kullanıcı şifresini değiştirmek için dosyayı `kibanaserver`düzenleyin `wazuh/secrets/dashboard-cred-secret.yaml`.

```
...
apiVersion: v1
kind: Secret
metadata:
    name: dashboard-cred
data:
    username: a2liYW5hc2VydmVy  # string "kibanaserver" base64 encoded
    password: a2liYW5hc2VydmVy  # string "kibanaserver" base64 encoded
...
```

Değişiklikleri Uygulama

1. Bildirim değişikliklerini uygulayın

   - EKS kümesi

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

   - Diğer küme türleri

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

2. Bir kez daha bash kabuğunu başlatın `wazuh-indexer-0`.

   ```
   kubectl exec -it wazuh-indexer-0 -n wazuh -- /bin/bash
   ```

3. Aşağıdaki değişkenleri ayarlayın:

   ```
   export INSTALLATION_DIR=/usr/share/wazuh-indexer
   CACERT=$INSTALLATION_DIR/certs/root-ca.pem
   KEY=$INSTALLATION_DIR/certs/admin-key.pem
   CERT=$INSTALLATION_DIR/certs/admin.pem
   export JAVA_HOME=/usr/share/wazuh-indexer/jdk
   ```

4. Wazuh dizinleyicisinin düzgün bir şekilde başlatılmasını bekleyin. Bekleme süresi iki ila beş dakika arasında değişebilir. Kümenin boyutuna, atanan kaynaklara ve ağın hızına bağlıdır. Ardından, `securityadmin.sh`tüm değişiklikleri uygulamak için scripti çalıştırın.

```
bash /usr/share/wazuh-indexer/plugins/opensearch-security/tools/securityadmin.sh -cd /usr/share/wazuh-indexer/opensearch-security/ -nhnv -cacert  $CACERT -cert $CERT -key $KEY -p 9200 -icl -h $NODE_NAME
```

5. Bileşen kimlik bilgilerini güncellemek için tüm Wazuh yönetici bölmelerini silin.

```
kubectl delete -n wazuh pod/wazuh-manager-master-0 pod/wazuh-manager-worker-0 pod/wazuh-manager-worker-1
```

6. Wazuh kontrol panelinde yeni kimlik bilgilerinizle giriş yapın.

Wazuh API Kullanıcıları

Kullanıcı `wazuh-wui`, varsayılan olarak Wazuh API'sine bağlanacak kullanıcıdır. Parolayı değiştirmek için şu adımları izleyin.

> Not: Wazuh API kullanıcıları için parola 8 ila 64 karakter uzunluğunda olmalıdır. En az bir büyük harf ve bir küçük harf, bir sayı ve bir sembol içermelidir.

1. Yeni parolanızı base64 biçiminde kodlayın. Karma değerini korumak için son satır karakteri eklemekten kaçının. Örneğin, seçeneği `-n`komutla `echo`aşağıdaki gibi kullanın.

```
echo -n "NewPassword" | base64
```

2. `wazuh/secrets/wazuh-api-cred-secret.yaml` dosyayı düzenleyin ve `password` alanın değerini değiştirin .

```
apiVersion: v1
kind: Secret
metadata:
  name: wazuh-api-cred
  namespace: wazuh
data:
  username: d2F6dWgtd3Vp          # string "wazuh-wui" base64 encoded
  password: UGFzc3dvcmQxMjM0LmE=  # string "MyS3cr37P450r.*-" base64 encoded
```

3. Manifest değişikliklerini uygulayın.

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

4. Wazuh panosu ve Wazuh yöneticisi ana bilgisayarı için pod'ları yeniden başlatın.

Agentlar

Wazuh ajanları ana bilgisayarları izlemek için tasarlanmıştır. Bunları kullanmaya başlamak için:

1. Ajanı yükleyin .
2. Dosyayı değiştirerek aracı kaydedin `/var/ossec/etc/ossec.conf`. "Taşıma protokolünü" TCP olarak değiştirin ve 'yi `MANAGER_IP`1514 numaralı bağlantı noktasına işaret eden hizmetin harici IP adresiyle veya bulut sağlayıcısı tarafından sağlanan ana bilgisayar adıyla değiştirin

Acentelerin kaydedilmesi hakkında daha fazla bilgi edinmek için dokümantasyonun Wazuh acente kaydı bölümüne bakın.

Revision #12
Created 23 December 2024 22:36:10 by Ayşegül Sarıkaya
Updated 23 December 2024 23:12:59 by Ayşegül Sarıkaya