Wazuh Docker Yardımcı Programları

Wazuh-Docker konteynerlerini kurduktan sonra, Wazuh kurulumunuzdan en iyi şekilde yararlanmak için yapabileceğiniz birkaç görev vardır.

Hizmetlere ve Konteynerlere Erişim

1. Docker ana bilgisayar IP adresini kullanarak Wazuh panosuna erişin. Örneğin, `https://localhost`Docker ana bilgisayarındaysanız.

   > Not: Kendinden imzalı bir sertifika kullanmanız durumunda tarayıcınız sertifikanın gerçekliğini doğrulayamadığına dair bir uyarı verecektir.

2. Standart kayıt sürecini izleyerek ve Docker ana bilgisayar adresini yönetici adresi olarak kullanarak aracıları kaydedin. Daha fazla bilgi için Wazuh aracı kayıt belgelerine bakın.
3. Wazuh dosyasının bulunduğu dizindeki kapsayıcıları listeleyin `docker-compose.yml`:

   ```
   docker-compose ps
   ```

   Output

   ```
   NAME                        COMMAND                  SERVICE           STATUS          PORTS
   single-node-wazuh.dashboard-1   "/entrypoint.sh"         wazuh.dashboard   running         443/tcp, 0.0.0.0:443->5601/tcp
   single-node-wazuh.indexer-1     "/entrypoint.sh open…"   wazuh.indexer     running         0.0.0.0:9200->9200/tcp
   single-node-wazuh.manager-1     "/init"                  wazuh.manager     running         0.0.0.0:1514-1515->1514-1515/tcp, 0.0.0.0:514->514/udp, 0.0.0.0:55000->55000/tcp, 1516/tcp
   ```

4. `docker-compose.yml`Her bir konteynerin komut satırına erişmek için dosyanın bulunduğu dizinden aşağıdaki komutu çalıştırın:

   ```
   docker-compose exec <SERVICE> bash
   ```

Wazuh Servis Veri Hacimleri

Wazuh yapılandırma ve günlük dosyalarının kapsayıcılarının dışında var olmasını ayarlayabilirsiniz. Bu, dosyaların kapsayıcıları kaldırdıktan sonra da kalıcı olmasını sağlar ve kapsayıcılarınıza özel yapılandırma dosyaları sağlayabilirsiniz.

Bir Wazuh konteynerinde kalıcılığı garantilemek için birden fazla birime ihtiyacınız var. Aşağıda `docker-compose.yml`kalıcı birimlere sahip bir örnek verilmiştir:

```
services:
  wazuh:
    . . .
    volumes:
      - wazuh_api_configuration:/var/ossec/api/configuration


volumes:
  wazuh_api_configuration:
```

Kalıcı birimleri şu şekilde listeleyebilirsiniz : `docker volume ls`

Output

```
DRIVER              VOLUME NAME
local               single-node_wazuh_api_configuration
```

Wazuh Indexer ve Dashboard İçin Depolama Hacmi

Wazuh dizinleyici verilerinin depolanması için bir birim eklemek de mümkündür. Varsayılan olarak, tek düğümlü ve çok düğümlü dağıtımlar zaten yapılandırılmış birimlere sahiptir. Tek düğümlü bir wazuh dizinleyici biriminin bir örneği aşağıda gösterilmiştir `docker-compose.yml`:

```
wazuh.indexer:
    . . .
    volumes:
      - wazuh-indexer-data:/var/lib/wazuh-indexer


    . . .
```

```
volumes:
  wazuh-indexer-data
```

Özel Komutlar ve Scriptler

Wazuh yönetici kabında komutları çalıştırmak için bir kabuk çalıştırabilirsiniz:

```
docker exec -it single-node-wazuh.manager-1 bash
```

Bu kabukta yapılan her değişiklik, veri birimleri doğru şekilde yapılandırıldığı sürece kalıcı olur.

Revision #5
Created 23 December 2024 22:17:25 by Ayşegül Sarıkaya
Updated 23 December 2024 22:25:38 by Ayşegül Sarıkaya