Sanal Makine (OVA)

Wazuh, Open Virtual Appliance (OVA) formatında önceden oluşturulmuş bir sanal makine görüntüsü sağlar. Bu, doğrudan VirtualBox'a veya diğer OVA uyumlu sanallaştırma sistemlerine aktarılabilir. Bu VM'nin yalnızca 64 bit sistemlerde çalıştığını unutmayın. Kutudan çıktığı anda yüksek kullanılabilirlik ve ölçeklenebilirlik sağlamaz. Ancak bunlar dağıtılmış dağıtım kullanılarak uygulanabilir .

Aşağıdaki bileşenleri içeren sanal cihazı (OVA) indirin :

- Amazon Linux 2
- Wazuh yöneticisi 4.9.2
- Wazuh dizinleyici 4.9.2
- Filebeat-OSS 7.10.2
- Wazuh gösterge paneli 4.9.2

Paket Listesi

Dağıtım	Mimarlık	VM Biçimi	Sürüm	Paket
Amazon Linux 2	64 bit	OVA	4.9.2	wazuh-4.9.2.ova (sha512)

Donanım Gereksinimleri

Wazuh VM'nin bir ana işletim sistemine aktarılabilmesi için aşağıdaki gereksinimlerin karşılanması gerekir:

- Ana bilgisayar işletim sisteminin 64-bit olması gerekiyor.
- Donanım sanallaştırmanın, ana bilgisayarın donanım yazılımında etkinleştirilmesi gerekir.
- Ana bilgisayara VirtualBox gibi bir sanallaştırma platformu kurulmalıdır.

Wazuh VM, kutudan çıktığı haliyle aşağıdaki özelliklerle yapılandırılmıştır:

Bileşen	CPU (çekirdekler)	RAM (GB)	Depolama (GB)
Wazuh v4.9.2 OVA	4	8	50

Ancak bu donanım yapılandırması, korunan uç nokta sayısına ve dizinlenmiş uyarı verilerine bağlı olarak değiştirilebilir. Gereksinimler hakkında daha fazla bilgi burada bulunabilir .

Sanal Makineyi İçe Aktarın ve Erişin

1. OVA'yı sanallaştırma platformuna aktarın.
2. VirtualBox kullanıyorsanız, `VMSVGA`grafik denetleyicisini ayarlayın. Başka bir grafik denetleyicisi ayarlamak VM penceresini dondurur.
   1. İçeri aktarılan VM'yi seçin.
   2. **Ayarlar** > **Görüntüle'ye** tıklayın
   3. **Grafik denetleyicide** seçeneğini seçin `VMSVGA`.
3. Makineyi çalıştırın.
4. Aşağıdaki kullanıcı adı ve parolayı kullanarak sanal makineye erişin. Sanallaştırma platformunu kullanabilir veya SSH üzerinden erişebilirsiniz.

   ```
   user: wazuh-user
   password: wazuh
   ```

   SSH `root`kullanıcı girişi devre dışı bırakıldı; ancak `wazuh-user`sudo ayrıcalıkları korunuyor. Kök ayrıcalık yükseltmesi aşağıdaki komutu çalıştırarak gerçekleştirilebilir:

   ```
   sudo -i
   ```

Wazuh Dashboard'a Erişin

VM başlatıldıktan kısa bir süre sonra, Wazuh panosuna aşağıdaki kimlik bilgilerini kullanarak web arayüzünden erişilebilir:

```
URL: https://<wazuh_server_ip>
user: admin
password: admin
```

`<wazuh_server_ip>` Aşağıdaki komutu VM'de yazarak bulabilirsiniz :

```
ip a
```

Yapılandırma Dosyaları

Bu sanal görüntüde bulunan tüm bileşenler, herhangi bir ayarı değiştirmeye gerek kalmadan, kutudan çıktığı gibi çalışacak şekilde yapılandırılmıştır. Ancak, tüm bileşenler tamamen özelleştirilebilir. Yapılandırma dosyalarının konumları şunlardır:

- Wazuh yöneticisi:`/var/ossec/etc/ossec.conf`
- Wazuh indeksleyici:`/etc/wazuh-indexer/opensearch.yml`
- Filebeat-OSS:`/etc/filebeat/filebeat.yml`
- Wazuh gösterge paneli:
  - `/etc/wazuh-dashboard/opensearch_dashboards.yml`
  - `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml`

VirtualBox Zaman Yapılandırması

VirtualBox kullanılması durumunda, sanal makine içe aktarıldığında, VirtualBox konuk makinenin saatini senkronize ettiğinde zaman kaymasından kaynaklanan sorunlarla karşılaşılabilir. Bu durumdan kaçınmak için, sanal makine yapılandırmasının sekmesindeki seçeneği etkinleştirin. `Hardware Clock in UTC TimeSystem`

> Not: Varsayılan olarak, ağ arabirimi türü Bridged Adapter olarak ayarlanır. VM, ağ DHCP sunucusundan bir IP adresi almaya çalışır. Alternatif olarak, VM'nin dayandığı Amazon Linux işletim sistemindeki uygun ağ dosyalarını yapılandırarak statik bir IP adresi ayarlanabilir.

Sanal makine içe aktarılıp çalıştırıldıktan sonraki adım, izlenecek sistemlere Wazuh aracılarını dağıtmaktır .

VM'yi Yükseltme

Sanal makine geleneksel kurulum gibi yükseltilebilir:

- Wazuh merkezi bileşenlerinin yükseltilmesi

Revision #1
Created 23 December 2024 20:53:01 by Ayşegül Sarıkaya

Updated 23 December 2024 21:12:00 by Ayşegül Sarıkaya