Amazon Makine Görüntüleri (AMI)

Wazuh önceden oluşturulmuş bir Amazon Makine Görüntüsü (AMI) sağlar. Bir AMI, Amazon Elastic Compute Cloud (Amazon EC2) içinde sanal bir bilgi işlem ortamı oluşturmak için kullanıma hazır, önceden yapılandırılmış bir şablondur. En son Wazuh AMI paketleri, Amazon Linux 2'yi Wazuh sunucunuz için aşağıdaki merkezi bileşenlerle bir araya getirir:

- Wazuh yöneticisi 4.9.2
- Filebeat-OSS 7.10.2
- Wazuh dizinleyici 4.9.2
- Wazuh gösterge paneli 4.9.2

Paket Listesi

Dağıtım	Mimarlık	VM Biçimi	Son sürüm	Ürün sayfası
Amazon Linux 2	64 bit	AWS AMI	4.9.2	Wazuh Hepsi Bir Arada Dağıtım

Dağıtım Alternatifleri

Bir Wazuh örneğini dağıtmak için iki alternatif vardır. Wazuh All-In-One Deployment AMI'yi doğrudan AWS Marketplace'ten başlatabilir veya AWS Management Console'u kullanarak bir örneği yapılandırabilir ve dağıtabilirsiniz.

- AWS Marketplace'ten bir örnek başlatın
- AWS Yönetim Konsolu'nu kullanarak bir örneği dağıtın

> Not: Wazuh Danışmanlık Hizmeti AWS Marketplace'te de mevcuttur. Wazuh'un sunduğu Profesyonel Hizmet paketlerini kontrol edin.

AWS Marketplace'ten Bir Örnek Başlatın

1. AWS Marketplace'teki Wazuh All-In-One Dağıtımına gidin ve ardından **Abone Olmaya Devam Et'e** tıklayın .
2. Bilgileri inceleyin ve yazılım için şartları kabul edin. Sunucu ürünümüze aboneliğinizi onaylamak için **Yapılandırmaya Devam Et'e tıklayın.**
3. Bir **Yazılım Sürümü** ve örneğin dağıtılacağı **Bölgeyi seçin. Ardından Başlatmaya Devam Et'e** tıklayın .
4. Yazılımı başlatmadan önce yapılandırmanızı gözden geçirin ve tüm ayarların doğru olduğundan emin olun. Varsayılan yapılandırma değerlerini ihtiyaçlarınıza göre uyarlayın.
    1. **EC2 Örnek Türünü** seçerken bir örnek türü kullanmanızı öneririz `c5a.xlarge`.
    2. **Güvenlik Grubunu** seçerken , doğru işlemi garantilemek için Wazuh örneğiniz için uygun ayarlara sahip olması gerekir . **Satıcı ayarlarına göre yeni oluştur'u** seçerek yeni bir güvenlik grubu oluşturabilirsiniz . Bu yeni grup varsayılan olarak uygun ayarlara sahip olacaktır.
5. Örneği oluşturmak için **Başlat'a** tıklayın .

Örneğiniz başarıyla başlatıldıktan ve birkaç dakika geçtikten sonra Wazuh kontrol paneline erişebilirsiniz .

AWS Yönetim Konsolu'nu Kullanarak Bir Örneği Dağıtın

1. AWS Yönetim Konsolu panonuzdan **Örneği başlat'ı** seçin .
2. Wazuh Inc. tarafından sunulan Wazuh All-In-One Deployment'ı bulun ve abone olmak için **Seç'e** tıklayın .
3. Sunucu ürün özelliklerini inceleyin, ardından **Devam'a** tıklayın . Bu, Sunucu ürünümüze abone olmanızı sağlar.
4. İhtiyaçlarınıza göre örnek türünü seçin ve ardından **İleri: Örnek Ayrıntılarını Yapılandır'a** tıklayın . Bir örnek türü kullanmanızı öneririz `c5a.xlarge`.
5. Örneğinizi gerektiği gibi yapılandırın ve ardından **İleri: Depolama Ekle'ye** tıklayın .
6. Örneğinizin depolama kapasitesini **Boyut (GiB)** sütunu altında ayarlayın ve ardından **İleri: Etiket Ekle'ye** tıklayın . 100 GiB GP3 veya daha fazlasını öneririz.
7. İhtiyacınız kadar etiket ekleyin ve ardından **İleri: Güvenlik Grubunu Yapılandır'a** tıklayın .
8. Portların ve protokollerin Wazuh için portlar ve protokoller olduğunu kontrol edin . Örneğiniz için güvenlik önlemlerini kontrol edin. Bu, Güvenlik Grubunu (SG) kuracaktır. Ardından, **İncele ve Başlat'a** tıklayın .
9. Örnek yapılandırmasını gözden geçirin ve **Başlat'a** tıklayın .
10. Anahtar çifti ayarlarıyla ilgili olarak mevcut üç yapılandırma alternatifinden birini seçin: **Mevcut bir anahtar çifti seçin** , **Yeni bir anahtar çifti oluşturun** , **Anahtar çifti**

olmadan devam edin . Örneğe SSH ile erişmek için mevcut bir anahtar çifti seçmeniz veya yeni bir tane oluşturmanız gerekir.

11. İşlemi tamamlamak ve örneğinizi dağıtmak için **Örnekleri başlat'a** tıklayın .

Örneğiniz tamamen yapılandırılıp lansmandan birkaç dakika sonra hazır hale geldiğinde Wazuh kontrol paneline erişebilirsiniz .

Yapılandırma Dosyaları

Bu AMI'de bulunan tüm bileşenler, herhangi bir ayarı değiştirmeye gerek kalmadan kullanıma hazır şekilde yapılandırılır. 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`

Wazuh'u yapılandırma hakkında daha fazla bilgi edinmek için Kullanım kılavuzuna bakın .

Wazuh Dashboard'a Erişin

Örnek başlatıldığında, kullanıcı parolaları otomatik olarak ilk harfi büyük olan örnek kimliğine değiştirilir. Örneğin: `I-07f25f6afe4789342`. Bu, yalnızca oluşturucunun arayüze erişebilmesini sağlar. Bu işlem, örneğin türüne bağlı olarak ortalama beş dakika sürebilir. Bu süre zarfında, hem SSH erişimi hem de Wazuh panosuna erişim devre dışı bırakılır.

Örnek çalışmaya başladıktan ve parola başlatma işlemi tamamlandıktan sonra kimlik bilgilerinizle Wazuh kontrol paneline erişebilirsiniz.

- URL: *https://<ÖRNEĞİNİZ_IP>*
- **Kullanıcı adı** : *admin*
- **Şifre** : *<YOUR_INSTANCE_ID>*

> Not: Şifre ilk harfi büyük olan örnek kimliğidir. Örneğin: `I-07f25f6afe4789342`.

> Uyarı: Sunucu API kullanıcıları için parola `wazuh`, kullanıcının parolasıyla `wazuh-wui`aynıdır `admin`. İlk SSH erişiminde varsayılan parolaları değiştirmenizi şiddetle öneririz. Bu işlemi gerçekleştirmek için Parola yönetimi bölümüne bakın.

SSH ile İlgili Güvenlik Hususları

- Kullanıcı `root`SSH ile tanımlanamıyor ve örneğe yalnızca şu kullanıcı aracılığıyla erişilebiliyor: `wazuh-user`.
- Parolalar aracılığıyla SSH kimlik doğrulaması devre dışı bırakıldı ve örneğe yalnızca bir anahtar çifti aracılığıyla erişilebilir. Bu, yalnızca anahtar çiftine sahip kullanıcının örneğe erişebileceği anlamına gelir.
- Örneğe bir anahtar çiftiyle erişmek için, AWS'de oluşturulan veya depolanan anahtarı indirmeniz gerekir. Ardından, örneğe bağlanmak için aşağıdaki komutu çalıştırın.

  ```
  ssh -i "<KEY_PAIR_NAME>" wazuh-user@<YOUR_INSTANCE_IP>
  ```

- Olası sorunları önlemek için ilk parola değiştirme işlemi sırasında erişim devre dışı bırakılır. Bu işlemin tamamlanması birkaç dakika sürebilir. Tamamlanmadan önce herhangi bir erişim girişimi gösterilir .`wazuh-user@<INSTANCE_IP>: Permission denied (publickey,gssapi-keyex,gssapi-with-mic)`

Sonraki Adımlar

Wazuh AMI artık hazır ve izlenecek sistemlere Wazuh ajanlarını dağıtmaya başlayabilirsiniz .

AMI'yi Yükseltme

Wazuh merkezi bileşenlerinin nasıl yükseltileceğine ilişkin talimatları izleyin.

> - Wazuh merkezi bileşenlerinin yükseltilmesi

Revision #5
Created 23 December 2024 21:15:14 by Ayşegül Sarıkaya
Updated 23 December 2024 21:28:31 by Ayşegül Sarıkaya