Hızlı Başlangıç

Wazuh, endpoint (uç noktalar) ve cloud (bulut) iş yüklerinin korunması için geliştirilmiş, birleşik bir XDR (Extended Detection and Response) ve SIEM (Security Information and Event Management) platformudur. Bu kapsamlı çözüm, güvenlik operasyonlarının merkezi bir yapı üzerinde yürütülmesini sağlamak amacıyla üç temel bileşenden oluşur: **Wazuh server (sunucu)**, **Wazuh indexer (dizinleyici)** ve **Wazuh dashboard (pano)**. Platform, evrensel bir ajan tarafından desteklenerek uç noktalardan veri toplar ve merkezi bileşenlerde korelasyon, analiz ve görselleştirme süreçlerini gerçekleştirir. Daha fazla bilgi için "Başlangıç" dökümantasyonuna göz atabilirsiniz.

Wazuh, **özgür ve açık kaynaklı** bir güvenlik çözümüdür. Platform bileşenleri, **GNU Genel Kamu Lisansı Sürüm 2** ve **Apache Lisansı Sürüm 2.0 (ALv2)** kapsamında lisanslanmıştır. Bu da güvenlik ekiplerine esneklik ve özelleştirme imkânı sunar.

Bu hızlı başlangıç rehberi, **Wazuh merkezi bileşenlerini** (Wazuh Indexer, Server ve Dashboard) tek bir ana bilgisayarda hızlı ve kolay bir şekilde nasıl kurabileceğinizi gösterir. Daha gelişmiş kurulum seçenekleri ve detaylar için "Kurulum Rehberi" belgesine başvurabilirsiniz.

Sistem Gereksinimleri

Donanım

Wazuh'un donanım gereksinimleri, ağı izleyen uç noktaların ve bulut iş yüklerinin sayısına bağlı olarak değişkenlik gösterir. İzlenecek sistemlerin sayısı, analiz edilecek veri miktarını ve depolanacak güvenlik uyarılarının hacmini belirlemekte önemli bir etkendir.

Hızlı başlangıç dağıtımı, **Wazuh Sunucusunu, Dizinleyiciyi ve Panoyu tek bir ana bilgisayara kurmayı hedefler.** Bu yapılandırma, genellikle 100 uç noktaya kadar izleme kapasitesi ve 90 günlük güvenlik uyarı verilerinin sorgulanabilir/dizinlenebilir biçimde saklanması için yeterlidir. Aşağıdaki tablo, önerilen donanım gereksinimlerini özetler:

Acenteler	İşlemci	Veri deposu	Depolama (90 gün)
1–25	4 sanal işlemci	8 GiB	50 GB
25–50	8 sanal işlemci	8 GiB	100 GB
50–100	8 sanal işlemci	8 GiB	200 GB

Daha büyük ortamlar için dağıtılmış bir dağıtım öneriyoruz. Çok düğümlü küme yapılandırması, Wazuh sunucusu ve Wazuh dizinleyicisi için kullanılabilir ve yüksek kullanılabilirlik ve yük dengelemesi sağlar.

İşletim Sistemi

Wazuh merkezi bileşenleri 64-bit Linux işletim sistemine kurulabilir. Wazuh aşağıdaki işletim sistemi sürümlerinden herhangi birini önerir:

Amazon Linux 2, Amazon Linux 2023	CentOS 7, 8
Red Hat Enterprise Linux 7, 8, 9	Ubuntu 16.04, 18.04, 20.04, 22.04, 24.04

Wazuh'u Kurmak

1. Wazuh kurulum yardımcısını indirin ve çalıştırın.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh && sudo bash ./wazuh-install.sh -a
```

Yardımcı kurulumu tamamladığında, çıktı erişim kimlik bilgilerini ve kurulumun başarılı olduğunu doğrulayan bir mesajı gösterir.

```
INFO: --- Summary ---
INFO: You can access the web interface https://<wazuh-dashboard-ip>
    User: admin
    Password: <ADMIN_PASSWORD>
INFO: Installation finished.
```

Artık Wazuh'u kurdunuz ve yapılandırdınız.

2. Wazuh web arayüzüne aşağıdaki https://<wazuh-dashboard-ip>bilgileri ve kimlik bilgilerinizi kullanarak erişin:

- Kullanıcı adı: admin
- Şifre: <ADMIN_PASSWORD>

Wazuh panosuna ilk kez eriştiğinizde, tarayıcı sertifikanın güvenilir bir otorite tarafından verilmediğini belirten bir uyarı mesajı gösterir. Bu beklenen bir durumdur ve kullanıcı sertifikayı bir istisna olarak kabul etme veya alternatif olarak sistemi güvenilir bir otoritenin sertifikasını kullanacak şekilde yapılandırma seçeneğine sahiptir.

> **Not:** Wazuh indeksleyicisinin ve Wazuh API kullanıcılarının tüm şifrelerini wazuh-install-files.tar içindeki wazuh-passwords.txt dosyasında bulabilirsiniz. Bunları yazdırmak için aşağıdaki komutu çalıştırın:

Wazuh indeksleyicisinin ve Wazuh API kullanıcılarının tüm şifrelerini wazuh-install-files.tar içindeki wazuh-passwords.txt dosyasında bulabilirsiniz. Bunları yazdırmak için aşağıdaki komutu çalıştırın:

```
sudo tar -O -xvf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt
```

Wazuh Central bileşenlerini kaldırmak istiyorsanız, -u veya –-uninstall seçeneğini kullanarak Wazuh kurulum yardımcısını çalıştırın.

Sonraki Adımlar

Artık Wazuh kurulumunuz hazır olduğuna göre, Wazuh aracısını dağıtmaya başlayabilirsiniz. Bu, dizüstü bilgisayarları, masaüstü bilgisayarları, sunucuları, bulut örneklerini, kapsayıcıları veya sanal makineleri korumak için kullanılabilir. Aracı hafif ve çok amaçlıdır ve çeşitli güvenlik yetenekleri sağlar.

Wazuh aracısının nasıl dağıtılacağına ilişkin talimatları dokümanlarımızda veya aşağıdaki linklerden bulabilirsiniz:

Linux için tıklayınız.

Windows için tıklayınız.

macOS için tıklayınız.

Solaris için tıklayınız.

AIX için tıklayınız.

HP-UX için tıklayınız.

Revision #16
Created 6 December 2023 18:05:34 by LastGuard
Updated 11 December 2024 16:06:19 by Ayşegül Sarıkaya