Wazuh Server

Wazuh Server, agentlardan alınan verileri analiz ederek tehditler veya anomalileri tespit ederek uyarılar oluşturur. Ayrıca agentların konfigürasyonlarını uzaktan yönetmek ve durumlarını takip etmek için kullanılır. Wazuh serverlarını single-node veya multi-node kurabilirsiniz. Multi-node mimariler yüksek kullabılabilirlik ve gelişmiş performans sağlar. Load balancer ile birlikte kullanıldığında kapasitesinini daha verimli şekilde kullanılması sağlanabilir.

- Wazuh Kurulum Asistanı
- Adım Adım Kurulum
- Wazuh Server Sistem Gereksinimleri

Wazuh Kurulum Asistanı

Asistan aracılığıla single-node veya multi-node olarak kurulum yapabilirsiniz. Bu bileşen wazuh manager ve filebeat içerir.

1. Wazuh asistan kurulumunu indirin.

```
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

2. Wazuh asistan kurulum dosyasını `--wazuh-server` parametresi ve server node adı ile birlikte kurun. Indexer sunucusunda hazırladığınız `config.yml` dosyasında yer alan isim ile parametre olarak verilen isim aynı olmalıdır.

> Indexer'da oluşturduğunuz wazuh-install-files.tar dosyasının bir kopyasının .sh dosyasını çalıştırdığınız dizinde olduğundan emin olun.

```
bash wazuh-install.sh --wazuh-server wazuh-1
```

Wazuh server kurulumu başarıyla tamamlandı. Eğer birden fazla server node'u kuracaksanız bu işlemi diğer node'lara da uygulamalısınız.

Servislerin doğru çalıştığından emin olmak için aşağıdaki iki komutu kullanabilirsiniz.

```
systemctl status wazuh-manager
systemctl status filebeat
```

Adım Adım Kurulum

Wazuh Server Sistem Gereksinimleri

Wazuh server için desteklenen ve önerilen sistem gereksinimleri ve işletim sistemleri aşağıda yer almaktadır. Kurulum sırasında root kullanıcı yetkisine ihtiyacınız olacak. Multi-node veya single-node olarak kurulum gerçekleştirebilirsiniz.

Önerilen işletim sistemleri

Wazuh 64-bit Linux işletim sistemlerine kurulabilir. Aşağıdaki işletim sistemlerini destekler:

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

Donanım Gereksinimleri

	Minimum		Önerilen	
Component	**RAM (GB)**	**CPU (cores)**	**RAM (GB)**	**CPU (cores)**
Wazuh Indexer	2	2	4	8

Veri miktarı, saniye başına oluşturulan uyarılara (APS) bağlıdır. Bu tablo, izlenen uç noktaların türüne bağlı olarak, bir Wazuh server node'unda 90 günlük uyarıları depolamak için aracı başına ihtiyaç duyulan tahmini disk alanının ayrıntılarını verir.

Monitör edilen endpointler	**APS**	**Wazuh Indexer depolama (GB/90 gün)**
Sunucular	0.25	0.1
Workstationlar	0.1	0.04
Ağ cihazları	0.5	0.2

Örneğin, 80 workstation, 10 sunucu ve 10 ağ cihazının bulunduğu bir ortam için Wazuh indeksleyici sunucusunda 90 günlük uyarılar için gereken depolama alanı 6 GB'dir.

Bir Wazuh Server'ın daha fazla kaynak gerektirip gerektirmediğini belirlemek için şu dosyaları izleyin.

- `/var/ossec/var/run/wazuh-analysisd.state` : `events_dropped` değişkeni, olayların kaynak eksikliği nedeniyle bırakılıp bırakılmadığını gösterir.
- `/var/ossec/var/run/wazuh-remoted.state` : `discarded_count` değişkeni, agentlardan gelen mesajların atılıp atılmadığını gösterir.

Ortam düzgün çalışıyorsa bu iki değişkenin sıfır olması gerekir. Aksi takdirde kümeye ek düğümler eklenebilir.