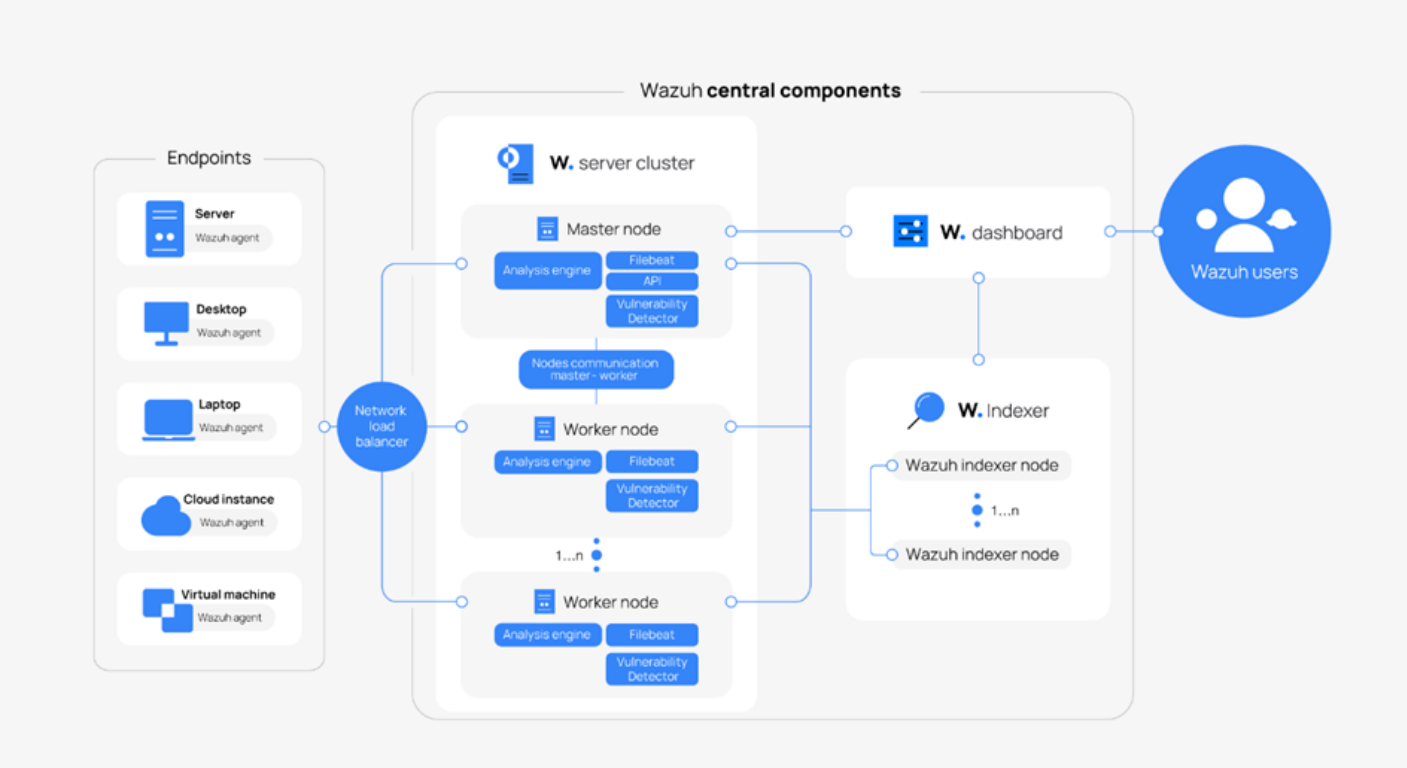
Mimari

Wazuh mimarisi, uç noktalardaki güvenlik olaylarını analiz etmek amacıyla merkezi bir sunucuya veri ileten ajanlar (agents) ile çalışır. Güvenlik duvarları, switchler, routerlar ve erişim noktaları gibi aracısız cihazlardan gelen log verileri **Syslog**, **SSH** veya **API** entegrasyonları aracılığıyla aktarılabilir. Merkezi sunucu, gelen verileri çözümleyerek analiz eder ve sonuçları dizinleme ve depolama işlemleri için **Wazuh Dizinleyici (Indexer)** bileşenine gönderir.

Wazuh dizinleyici kümesi, dizinler üzerinde okuma ve yazma işlemleri gerçekleştirmek için birbirleriyle iletişim kuran bir veya daha fazla düğümden oluşan bir koleksiyondur. Büyük miktarda veri işlemeyi gerektirmeyen küçük Wazuh dağıtımları, tek düğümlü bir küme tarafından kolayca işlenebilir. Çok sayıda izlenen uç nokta olduğunda, büyük miktarda veri beklendiğinde veya yüksek kullanılabilirlik gerektiğinde çok düğümlü kümeler önerilir.

Üretim ortamları için, Wazuh sunucusunu ve Wazuh dizinleyicisini farklı ana bilgisayarlara dağıtmanız önerilir. Bu senaryoda, Filebeat, TLS şifrelemesi kullanarak Wazuh uyarılarını ve arşivlenmiş olayları Wazuh dizinleyici kümesine (tek düğümlü veya çok düğümlü) güvenli bir şekilde iletmek için kullanılır.

Aşağıdaki diyagram bir Wazuh dağıtım mimarisini temsil eder. Çözüm bileşenlerine ve Wazuh server ve Wazuh indexer düğümlerinin yük dengeleme ve yüksek kullanılabilirlik sağlayarak kümeler olarak nasıl yapılandırılabileceğini gösterir.



Wazuh Agent - Wazuh Server İletişimi

Wazuh aracısı, analiz ve tehdit tespiti için sürekli olarak Wazuh sunucusuna olaylar gönderir. Bu verileri göndermeye başlamak için, aracı, varsayılan olarak 1514 numaralı bağlantı noktasını dinleyen aracı bağlantısı için sunucu hizmetiyle bir bağlantı kurar (bu yapılandırılabilir). Wazuh sunucusu daha sonra analiz motorunu kullanarak alınan olayları çözer ve kural denetimi yapar. Bir kuralı tetikleyen olaylar, kural kimliği ve kural adı gibi uyarı verileriyle zenginleştirilir. Olaylar, bir kuralın tetiklenip tetiklenmediğine bağlı olarak aşağıdaki dosyalardan birine veya her ikisine de kaydedilebilir:

- Dosya, /var/ossec/logs/archives/archives.json bir kuralı tetikleyip tetiklemediğine bakılmaksızın tüm olayları içerir.
- Dosya /var/ossec/logs/alerts/alerts.json yalnızca yüksek önceliğe sahip bir kuralı tetikleyen olayları içerir (eşik yapılandırılabilir).

Wazuh mesaj protokolü varsayılan olarak blok başına 128 bit ve 256 bit anahtarlarla AES şifrelemesini kullanır. Alternatif olarak Blowfish şifreleme seçeneği de mevcuttur.

Wazuh Server - Wazuh Indexer İletişimi

Wazuh sunucusu, uyarı ve olay verilerini TLS şifrelemesi aracılığıyla güvenli bir şekilde Wazuh dizinleyicisine iletmek için Filebeat'i kullanır. Filebeat, Wazuh sunucusundan gelen çıktı verilerini izler ve varsayılan olarak 9200/TCP portunu dinleyen Wazuh dizinleyicisine iletir. Dizinlendikten sonra, verileri Wazuh dashboard aracılığıyla analiz edebilir ve görselleştirebilirsiniz.

Güvenlik Açığı Tespiti modülü güvenlik açığı envanterini günceller. Ayrıca uyarılar üreterek sistem güvenlik açıklarına ilişkin içgörüler sağlar.

Wazuh panosu, Wazuh sunucusunun ve aracılarının yapılandırma ve durumla ilgili bilgilerini görüntülemek için Wazuh RESTful API'sini (varsayılan olarak Wazuh sunucusunda 55000/TCP portunu dinler) sorgular. Ayrıca API çağrıları aracılığıyla aracıları veya sunucu yapılandırma ayarlarını değiştirebilir. Bu iletişim TLS ile şifrelenir ve bir kullanıcı adı ve parola ile doğrulanır.

Gerekli Portlar

Wazuh bileşenlerinin iletişimi için çeşitli hizmetler kullanılır. Aşağıda bu hizmetler tarafından kullanılan varsayılan portların listesi bulunmaktadır. Kullanıcılar gerektiğinde bu port numaralarını değiştirebilirler.

Bileşen	Liman	Protokol	Amaç

Wazuh sunucusu	1514	TCP (varsayılan)	Ajan bağlantı hizmeti
	1514	UDP (isteğe bağlı)	Aracı bağlantı hizmeti (varsayılan olarak devre dışıdır)
	1515	Tpg	Acente kayıt hizmeti
	1516	Tpg	Wazuh kümeleme arka plan programı
	514	UDP (varsayılan)	Wazuh Syslog toplayıcısı (varsayılan olarak devre dışıdır)
	514	TCP (isteğe bağlı)	Wazuh Syslog toplayıcısı (varsayılan olarak devre dışıdır)
	55000	Tpg	Wazuh sunucusu RESTful API
Wazuh dizinleyici	9200	Tpg	Wazuh dizinleyici RESTful API
	9300-9400	Tpg	Wazuh dizinleyici küme iletişimi
Wazuh gösterge paneli	443	Tpg	Wazuh web kullanıcı arayüzü

Arşiv Veri Depolama

Hem uyarılar hem de uyarı olmayan olaylar Wazuh sunucusundaki dosyalarda saklanır ve ayrıca Wazuh dizinleyicisine gönderilir. Bu dosyalar JSON biçiminde (. json) veya düz metin biçiminde (.log) yazılabilir. Bu dosyalar günlük olarak sıkıştırılır ve MD5, SHA1 ve SHA256 toplam kontrolleri kullanılarak imzalanır. Dizin ve dosya adı yapısı aşağıdaki gibidir:

```
root@wazuh-manager:/var/ossec/logs/archives/2022/Jan# ls -l
```

Output

```
total 176
-rw-r----- 1 wazuh wazuh 234350 Jan  2 00:00 ossec-archive-01.json.gz
-rw-r----- 1 wazuh wazuh    350 Jan  2 00:00 ossec-archive-01.json.sum
-rw-r----- 1 wazuh wazuh 176221 Jan  2 00:00 ossec-archive-01.log.gz
-rw-r----- 1 wazuh wazuh    346 Jan  2 00:00 ossec-archive-01.log.sum
-rw-r----- 1 wazuh wazuh 224320 Jan  2 00:00 ossec-archive-02.json.gz
-rw-r----- 1 wazuh wazuh    350 Jan  2 00:00 ossec-archive-02.json.sum
-rw-r----- 1 wazuh wazuh 151642 Jan  2 00:00 ossec-archive-02.log.gz
-rw-r----- 1 wazuh wazuh    346 Jan  2 00:00 ossec-archive-02.log.sum
-rw-r----- 1 wazuh wazuh 315251 Jan  2 00:00 ossec-archive-03.json.gz
-rw-r----- 1 wazuh wazuh    350 Jan  2 00:00 ossec-archive-03.json.sum
-rw-r----- 1 wazuh wazuh 156296 Jan  2 00:00 ossec-archive-03.log.gz
-rw-r----- 1 wazuh wazuh    346 Jan  2 00:00 ossec-archive-03.log.sum
```

Arşiv dosyalarının rotasyonu ve yedeklenmesi Wazuh sunucusunun depolama kapasitesine göre önerilir. Cron işlerini kullanarak, arşiv dosyalarının yalnızca belirli bir zaman aralığını, örneğin geçen yıl veya son üç ayı, sunucuda yerel olarak tutmayı kolayca başarabilirsiniz.

Öte yandan, arşiv dosyalarını depolamayı bırakıp arşiv depolaması için Wazuh dizinleyicisine güvenmeyi seçebilirsiniz. Periyodik Wazuh dizinleyici anlık görüntü yedeklemeleri çalıştırıyorsanız ve/veya yüksek kullanılabilirlik için parça replikaları olan çok düğümlü bir Wazuh dizinleyici kümeniz varsa bu alternatif tercih edilebilir. Anlık görüntülenmiş dizinleri son veri depolama sunucusuna taşımak ve bunları MD5, SHA1 ve SHA256 karma algoritmalarını kullanarak imzalamak için bir cron işi bile kullanabilirsiniz.

Revision #7
Created 6 December 2023 17:36:23 by LastGuard
Updated 11 December 2024 15:23:55 by Ayşegül Sarıkaya