Sıraya Girme Mekanizmaları

Wazuh sunucusu, izlenen uç noktalardan olay toplanmasını kolaylaştıran bir kuyruk mekanizması içerir. Wazuh ajanlarından, syslog uç noktalarından ve ajansız cihazlardan Wazuh sunucusuna sürekli veri akışı sağlayarak olay taşmasını önler. Wazuh sunucu kuyruğu İlk Giren İlk Çıkar (FIFO) metodolojisini kullanır; bu nedenle, ilk kuyruğa alınan olay kuyruktan ilk kaldırılan ve işlenen olaydır. Dağıtılmış işleme dayalıdır ve günlük analiz görevlerinin paralel hale getirilmesine olanak tanır. Bu, günlük işleme hattının ölçeklenebilirliğini ve performansını iyileştirerek Wazuh'un büyük hacimli günlük verilerini etkili bir şekilde işlemesini sağlar.

Wazuh sunucusunda olay akışlarını yönetmek için iki yerel kuyruk bulunur:

- Wazuh aracı iletişim kuyruğu (queue_rd)
- Wazuh analiz motoru kuyruğu (queue_and)

Wazuh aracısı, olay tıkanıklığını önlemek için Wazuh aracı kuyruğunu (queue_ad) kullanır . Bu kuyruk, Wazuh aracısının Wazuh sunucusunun işleyebileceğinden daha hızlı olay göndermemesini sağlar.

Wazuh Agent İletişim Kuyruğu (queue_rd)

Kuyruk `queue_rd`, sunucu tarafı aracı iletişim hizmetinde bulunur . Wazuh aracılarından olayları alır ve olay kod çözme ve kural eşleştirme için Wazuh analiz motoruna gönderir .

Wazuh Agent İletişim Kuyruğu Nasıl Yapılandırılır

1. Wazuh sunucusundaki `/var/ossec/etc/ossec.conf` dosyasının `<queue_size>`uzak bölümünde düzenleme yaparak Wazuh aracı iletişim kuyruğunu yapılandırın:

```
<remote>
  <connection>secure</connection>
  <port>1514</port>
  <protocol>tcp,udp</protocol>
  <queue_size>131072</queue_size>
  <rids_closing_time>5m</rids_closing_time>
  <connection_overtake_time>600</connection_overtake_time>
  <agents>
    <allow_higher_versions>no</allow_higher_versions>
```

```
  </agents>
</remote>
```

Değişken `<queue_size>`, Wazuh aracı iletişim kuyruğunun kuyruk kapasitesini ayarlar. Aşağıdaki tablo `<queue_size>` değişkenin yapılandırmasını gösterir.

Varsayılan değer	İzin verilen değerler
131072	1 ile 262144 arasında herhangi bir sayı.

> Not: Wazuh aracı iletişim kuyruğu (`queue_rd`) yalnızca Wazuh aracı olayları için kullanılabilir, uzak syslog olayları için kullanılamaz. Bu seçenek yalnızca bağlantı olarak ayarlandığında çalışır `secure`.

2. Değişiklikleri uygulamak için Wazuh yönetici hizmetini yeniden başlatın.

```
systemctl restart wazuh-manager
```

Olay düşüşleri gözlemlendiğinde `/var/ossec/etc/ossec.conf` dosyasının `<remote>` bloğundaki `queue_size` değerini ve `/var/ossec/etc/internal_options.conf` dosyasındaki `worker_pool` boyutunu artırabilirsiniz.

`worker_pool`Aşağıdaki tablo Wazuh sunucusundaki boyut yapılandırmasını göstermektedir .

uzaktan.çalışan_havuzu	Tanım	Yük alımını işleyen iş parçacığı sayısı
	Varsayılan değer	4
	İzin verilen değer	1 ile 16 arasında herhangi bir tam sayı

Wazuh sunucu API'sini `wazuh-remoted` sorgulayarak veya daemon istatistiksel durum dosyasını okuyarak olay düşüşlerini izleyebilirsiniz .

Wazuh Sunucu API'sini Sorgulama

`wazuh-remoted`Aşağıdaki adımları izleyerek istatistiksel bilgileri sorgulayabilirsiniz :

1. Wazuh panosunda **Araçlar'a** ve ardından **API Konsolu'na** gidin .
2. API konsoluna aşağıdakileri ekleyin ve Wazuh sunucusu API'sine sorgu göndermek için yeşil oka tıklayın:

```
GET /manager/daemons/stats
```

3. Sorgu sonucu aşağıdaki ekran görüntüsünün sol tarafında gösterilmektedir. Wazuh uzaktan istatistiklerini gösteren Wazuh daemon'larının istatistiksel sorgusu.

Sorgu, kuyruk boyutu değerini, tarafından işlenen olay sayısını `wazuh-remoted`ve atılan olay sayısını döndürür.

Aracı İletişim İstatistiksel Durum Dosyası

Bu istatistiksel dosya, `wazuh-remoted`kuyruk boyutu, atılan mesajlar, uzak bağlantı sayısı ve diğer önemli bilgiler gibi uzak daemon ile ilgili verileri sunar.

Dosyayı okumak için Wazuh sunucusunda aşağıdaki komutu çalıştırın:

```
cat /var/ossec/var/run/wazuh-remoted.state
```

Aşağıda dosyanın içeriğine dair bir örnek verilmiştir `wazuh-remoted.state`:

```
# State file for wazuh-remoted
# THIS FILE WILL BE DEPRECATED IN FUTURE VERSIONS
# Updated every 5 seconds.

# Queue size
queue_size='0'

# Total queue size
total_queue_size='131072'

# TCP sessions
tcp_sessions='1'

# Events sent to Analysisd
evt_count='126714'

# Control messages received
ctrl_msg_count='2637'

# Discarded messages
discarded_count='0'

# Total number of bytes sent
sent_bytes='4434745'

# Total number of bytes received
recv_bytes='93866086'

# Messages dequeued after the agent closes the connection
dequeued_after_close='0'
```

Wazuh Analiz Motoru Kuyruğu (queue_and)

Sıra Wazuh analiz motorunda `queue_and` bulunur ve olayların alınmasını kolaylaştırır. Wazuh analiz motoru daha sonra alınan günlükleri Wazuh sunucusundaki kurallarla eşleştirir.

Wazuh Analiz Motoru Kuyruğu Nasıl Yapılandırılır

Wazuh analiz motoru kuyruğu, `queue_and` kuyruğu kullanarak analiz için Wazuh ajanlarından günlükleri alır. Gelen tüm günlük mesajları kategorilere ayrılır ve aşağıdaki kategorilerde sıraya alınır:

- Dosya bütünlüğü izleme olayı kod çözücü kuyruğu.
- Syscollector olay kod çözücü kuyruğu.
- Kök denetimi olayı kod çözücü kuyruğu.
- Ana bilgisayar bilgisi olay kod çözücü kuyruğu.
- Olay kod çözücü kuyruğu.
- Windows olay kod çözücü kuyruğu.

Her kuyruk kategorisinin İlk Giren İlk Çıkar (FIFO) olay yönetiminden sorumlu bir dizi iş parçacığı vardır. İş parçacığı sayısı, `/var/ossec/etc/internal_options.conf` Wazuh sunucusundaki dosya aracılığıyla olay türüne göre ayrı ayrı yapılandırılabilir.

> Not: Yükseltmelerin kuyruk yapılandırmalarını geçersiz kılmamasını sağlamak için `/var/ossec/etc/local_internal_options.conf` dosyası yerine `/var/ossec/etc/internal_options.conf` dosyasını kullanın.

Aşağıdaki tabloda Wazuh analiz motoru kuyruğu (`queue_and`) için kullanılabilen yapılandırma seçenekleri gösterilmektedir.

Kuyruklar (wazuh-analysisd.state)	Ayar (local_internal_options.conf)	Varsayılan	Dakika	Maksimum
syscheck_queue_kullanımı	analizd.decode_syscheck_queue_size	16384	128	2000000
syscollector_kuyruğu_kullanımı	analizd.decode_syscollector_queue_size	16384	128	2000000
kök_kontrolu_kuyruk_kullanımı	analizd.decode_rootcheck_queue_size	16384	128	2000000

Kuyruklar (wazuh-analysisd.state)	Ayar (local_internal_options.conf)	Varsayılan	Dakika	Maksimum
sca_queue_kullanımı	analizd.decode_sca_queue_size	16384	128	2000000
hostinfo_kuyruk_kullanımı	analiz.decode_hostinfo_queue_size	16384	128	2000000
winevt_kuyruk_kullanımı	analizd.decode_winevt_kuyruk_boyutu	16384	128	2000000
dbsync_kuyruk_kullanımı	analizd.dbsync_queue_size	16384	128	2000000
yükseltme_kuyruğu_kullanımı	analizd.yükseltme_kuyruğu_boyutu	16384	128	2000000
olay_kuyruğu_kullanımı	analizd.decode_event_queue_size	16384	128	2000000
kural_eşleşen_kuyruk_kullanımı	analizd.decode_output_queue_size	16384	128	2000000
uyarılar_kuyruğu_kullanımı	analizd.uyarılar_kuyruk_boyutu	16384	128	2000000
güvenlik_kuyruğu_kullanımı	analizd.firewall_queue_size	16384	128	2000000
istatistiksel_kuyruk_kullanımı	analizd.istatistiksel_kuyruk_boyutu	16384	128	2000000
arşiv_kuyruğu_kullanımı	analizd.arşivler_kuyruğu_boyutu	16384	128	2000000
	analizd.fts_kuyruk_boyutu	16384	128	2000000
	analizd.fts_liste_boyutu	32	12	512
	analysisd.fts_min_size_for_str	14	6	128
	analizd.decoder_order_size	256	32	1024

Wazuh analiz motorunda "olay düşüşleri" gözlemlendiğinde kuyruk ayarları ayarlanmalıdır. Wazuh sunucu API'sini sorgulayarak veya daemon istatistiksel durum dosyasını okuyarak wazuh-analysisd'deki olay düşüşlerini izleyebilirsiniz .

Wazuh Sunucu API'sini Sorgulama

Wazuh analiz motorundan istatistiksel bilgileri kontrol etmek için günlük kategorisi durumu Wazuh sunucu API'si kullanılarak sorgulanabilir. Yeni istatistikler, alınan veya düşürülen olayların olay türüne göre dökümünü gösterir. Bu, yalnızca düşürmeyi gösteren kuyruk boyutlarını ayarlamak için hayati önem taşır.

Aşağıdaki adımları izleyerek Wazuh analiz motorunun istatistiksel bilgilerini sorgulayabilirsiniz:

1. Wazuh panosunda **Araçlar'a** ve ardından **API Konsolu'na** gidin .
2. Konsola aşağıdakileri ekleyin ve Wazuh sunucu API'sine sorgu göndermek için yeşil oka tıklayın:

```
GET /manager/daemons/stats
```

3. `wazuh-analysisd` Aşağıdaki ekran görüntüsünde sağ tarafta gösterilen sorgu sonucunun bulunduğu bölüme doğru aşağı kaydırın .
Wazuh-analysisd istatistiklerini gösteren Wazuh daemon'larının istatistiksel sorgusu

Sorgu, kuyruk boyutu değerini, Wazuh analiz motoru tarafından işlenen olay sayısını ve atılan olay sayısını döndürür.

`/var/ossec/etc/internal_options.conf` Wazuh analiz motoru kuyruğu , Wazuh sunucusundaki dosya aracılığıyla olay türüne göre yapılandırılabilir .

> Not: Yükseltmelerin kuyruk yapılandırmalarını geçersiz kılmamasını sağlamak için `/var/ossec/etc/local_internal_options.conf` dosyası yerine `/var/ossec/etc/internal_options.conf` dosyasını kullanın.

Wazuh Analiz Motoru İstatistiksel Durum Dosyası

Wazuh analiz motoru için istatistiksel dosya şu adreste bulunur `/var/ossec/var/run/wazuh-analysisd.state`. Dosya, Wazuh sunucusundaki olay işleme sorunlarını araştırırken yararlı olabilir.

Dosyayı okumak için Wazuh sunucusunda aşağıdaki komutu çalıştırın:

```
cat /var/ossec/var/run/wazuh-analysisd.state
```

Aşağıda wazuh-remoted.state dosyasının içeriğine dair bir örnek verilmiştir:

```
# State file for wazuh-analysisd
# THIS FILE WILL BE DEPRECATED IN FUTURE VERSIONS

# Total events decoded
total_events_decoded='137726'

# Syscheck events decoded
```

```
syscheck_events_decoded='3935'

# Syscollector events decoded
syscollector_events_decoded='2590'

# Rootcheck events decoded
rootcheck_events_decoded='37'

# Security configuration assessment events decoded
sca_events_decoded='8991'

# Winevt events decoded
winevt_events_decoded='87993'

# Database synchronization messages dispatched
dbsync_messages_dispatched='26004'

# Other events decoded
other_events_decoded='8176'

# Events processed (Rule matching)
events_processed='112252'

# Events received
events_received='138283'

# Events dropped
events_dropped='0'

# Alerts written to disk
alerts_written='6707'

# Firewall alerts written to disk
firewall_written='0'

# FTS alerts written to disk
fts_written='0'

# Syscheck queue
syscheck_queue_usage='0.00'

# Syscheck queue size
syscheck_queue_size='16384'

# Syscollector queue
syscollector_queue_usage='0.00'

# Syscollector queue size
syscollector_queue_size='16384'

# Rootcheck queue
rootcheck_queue_usage='0.00'
```

```
# Rootcheck queue size
rootcheck_queue_size='16384'

# Security configuration assessment queue
sca_queue_usage='0.00'

# Security configuration assessment queue size
sca_queue_size='16384'

# Hostinfo queue
hostinfo_queue_usage='0.00'

# Hostinfo queue size
hostinfo_queue_size='16384'

# Winevt queue
winevt_queue_usage='0.00'

# Winevt queue size
winevt_queue_size='16384'

# Database synchronization message queue
dbsync_queue_usage='0.00'

# Database synchronization message queue size
dbsync_queue_size='16384'

# Upgrade module message queue
upgrade_queue_usage='0.00'

# Upgrade module message queue size
upgrade_queue_size='16384'

# Event queue
event_queue_usage='0.00'

# Event queue size
event_queue_size='16384'

# Rule matching queue
rule_matching_queue_usage='0.00'

# Rule matching queue size
rule_matching_queue_size='16384'

# Alerts log queue
alerts_queue_usage='0.00'

# Alerts log queue size
alerts_queue_size='16384'

# Firewall log queue
firewall_queue_usage='0.00'
```

```
# Firewall log queue size
firewall_queue_size='16384'

# Statistical log queue
statistical_queue_usage='0.00'

# Statistical log queue size
statistical_queue_size='16384'

# Archives log queue
archives_queue_usage='0.00'

# Archives log queue size
archives_queue_size='16384'
```

Wazuh Agent Kuyruğu (queue_ad)

Sıra `queue_ad`, aracı tarafı aracı bağlantı hizmetinde bulunur ve Wazuh aracısından Wazuh sunucusuna olay iletimini yönetir. Sıra, Wazuh sunucusuna iletmeden önce sistem olayları ve güvenlik yapılandırması değerlendirme çıktıları gibi günlükleri toplar. Ayrıca, yapılandırılabilir parametrelere göre olay iletimini kısıtlayan ve Wazuh sunucusunun işleme kapasitesini aşma riskini azaltan bir anti-flooding mekanizması içerir.

Wazuh Kuyruk Çözücü ve Kuralları

Wazuh, olay sel çıkışını analiz etmek ve Wazuh panosunda uyarılar oluşturmak için kullanıma hazır bir kod çözücü ve kurallar sağlar.

Decoder

Kod çözücü Wazuh sunucusundaki dosyada mevcuttur `/var/ossec/ruleset/decoders/0005-wazuh_decoders.xml`. Kod çözücü Wazuh sunucusundaki flood olaylarını analiz etmekten sorumludur.

```
<decoder name="agent-buffer">
  <parent>wazuh</parent>
  <prematch offset="after_parent">^Agent buffer:</prematch>
  <regex offset="after_prematch">^ '(\S+)'.</regex>
  <order>level</order>
</decoder>
```

Kurallar

Aşağıda görüldüğü gibi kurallar, `201`ile arasındaki ID'lerle tanımlanmış olup Wazuh sunucusundaki dosyada `205`mevcuttur .`/var/ossec/ruleset/rules/0016-wazuh_rules.xml`

```
<!-- Agent buffer rules -->
<rule id="201" level="0">
  <if_sid>200</if_sid>
  <match>^wazuh: Agent buffer: </match>
  <description>Agent event queue rule</description>
  <group>agent_flooding,</group>
</rule>

<rule id="202" level="7">
  <if_sid>201</if_sid>
  <field name="level">%</field>
  <description>Agent event queue is $(level) full.</description>
  <group>agent_flooding,pci_dss_10.6.1,gdpr_IV_35.7.d,</group>
</rule>

<rule id="203" level="9">
  <if_sid>201</if_sid>
  <field name="level">full</field>
  <description>Agent event queue is full. Events may be lost.</description>
  <group>agent_flooding,pci_dss_10.6.1,gdpr_IV_35.7.d,</group>
</rule>

<rule id="204" level="12">
  <if_sid>201</if_sid>
  <field name="level">flooded</field>
  <description>Agent event queue is flooded. Check the agent configuration.</description>
  <group>agent_flooding,pci_dss_10.6.1,gdpr_IV_35.7.d,</group>
</rule>

<rule id="205" level="3">
  <if_sid>201</if_sid>
  <field name="level">normal</field>
  <description>Agent event queue is back to normal load.</description>
  <group>agent_flooding,</group>
</rule>
```

Nerede:

- Kural Kimliği, `201`olay kuyruğu için temel kuraldır.
- Kural Kimliği, `202`olay kuyruğu seviyesi %90'a ulaştığında tetiklenir.
- Kural kimliği, `203`olay kuyruğu dolduğunda tetiklenir.
- `204`Olay kuyruğu dolduğunda kural kimliği tetiklenir.
- Kural Kimliği, `205`bir su baskını olayından sonra olay kuyruğu normale döndüğünde tetiklenir.

Revision #6
Created 28 December 2024 00:34:38 by Ayşegül Sarıkaya
Updated 31 December 2024 13:26:28 by Ayşegül Sarıkaya