Indexer Entegrasyonu

Dizinleyici entegrasyonu, verileri Wazuh yöneticisinden Wazuh dizinleyicisine veya üçüncü taraf dizinleyicilere ileten veri ileticilerini tanımlar.

Wazuh Indexer

Bu entegrasyon, Wazuh yöneticisi ile Wazuh dizinleyicisi arasında bir köprü sağlar. Verileri dizinleme için Wazuh yöneticisinden Wazuh dizinleyicisine iletir. Wazuh dizinleyici entegrasyonu iki ileticiden oluşur: Filebeat ve Wazuh dizinleyici bağlayıcısı .

Filebeat

Bu bileşen, Wazuh yöneticisi tarafından işlenen uyarıları ve arşivlenmiş olayları indeksleme ve depolama için Wazuh indeksleyicisine güvenli bir şekilde iletmek üzere tasarlanmış hafif bir veri taşıyıcısıdır. Wazuh analiz motorunun çıktısını okur ve olayları gerçek zamanlı olarak gönderir.

Yapılandırma

Aşağıdaki kod bloğu, Wazuh sunucu dosyasındaki varsayılan Filebeat yapılandırmasını gösterir `/etc/filebeat/filebeat.yml`. Bu yapılandırma dosyası, adım adım Wazuh sunucu kurulumu gerçekleştirilirken indirilir. Filebeat'i nasıl indireceğinizi, yapılandıracağınızı ve yükleyeceğinizi öğrenmek için, belgelerdeki Filebeat'i yapılandırma bölümüne bakın.

```
# Wazuh - Filebeat configuration file
output.elasticsearch.hosts:
        - 127.0.0.1:9200
#       - <elasticsearch_ip_node_2>:9200
#       - <elasticsearch_ip_node_3>:9200

output.elasticsearch:
  protocol: https
  username: ${username}
  password: ${password}
  ssl.certificate_authorities:
    - /etc/filebeat/certs/root-ca.pem
  ssl.certificate: "/etc/filebeat/certs/wazuh-server.pem"
  ssl.key: "/etc/filebeat/certs/wazuh-server-key.pem"
setup.template.json.enabled: true
```

```
setup.template.json.path: '/etc/filebeat/wazuh-template.json'
setup.template.json.name: 'wazuh'
setup.ilm.overwrite: true
setup.ilm.enabled: false

filebeat.modules:
  - module: wazuh
    alerts:
      enabled: true
    Archives:

logging.level: info
logging.to_files: true
logging.files:
  path: /var/log/filebeat
  name: filebeat
  keepfiles: 7
  permissions: 0644

logging.metrics.enabled: false

seccomp:
  default_action: allow
  syscalls:
  - action: allow
    names:
    - rseq
```

Nerede:

- `<output.elasticsearch.hosts>`bağlanılacak Wazuh dizinleyici düğümlerinin listesini belirtir. IP adreslerini veya ana bilgisayar adlarını kullanabilirsiniz. Varsayılan olarak, ana bilgisayar localhost, olarak ayarlanmıştır `127.0.0.1:9200`. Bunu uygun şekilde Wazuh dizinleyici adresinizle değiştirin. Birden fazla Wazuh dizinleyici düğümünüz varsa adresleri virgül kullanarak ayırabilirsiniz.
- `<protocol>`bağlantı için kullanılacak protokolü belirtir. Varsayılan değer 'dir `https`. İzin verilen değerler `http`ve 'dir `https`.
- `<username>`ve `<password>`Wazuh indeksleyicisine güvenli bir şekilde kimlik doğrulaması yapmak için kullanılan ortam değişkenini belirtir.
- `<ssl.certificate_authorities>`HTTPS sunucu doğrulamaları için kök sertifikalarına giden yolu belirtir. Varsayılan değer 'dir `/etc/filebeat/certs/root-ca.pem`. Olası değer herhangi bir geçerli yoldur
- `<ssl.certificate>`Filebeat SSL sertifikasına giden yolu belirtir. Varsayılan değer 'dir `/etc/filebeat/certs/wazuh-server.pem`. Olası değer herhangi bir geçerli yoldur.
- `<ssl.key>`Filebeat tarafından kullanılan SSL anahtarının yolunu belirtir. Varsayılan değer 'dir `/etc/filebeat/certs/wazuh-server-key.pem`. Olası değer herhangi bir geçerli yoldur.
- `<setup.template.json.enabled>`özel şablonların kullanımını etkinleştirir veya devre dışı bırakır. Varsayılan değer `true`.
- `<setup.template.json.path>`şablon JSON dosyasına giden dosya yolunu belirtir. Varsayılan değer 'dir `/etc/filebeat/wazuh-template.json`. Olası değer herhangi bir geçerli yoldur.

- `<setup.template.json.name>`şablonun adını tanımlar. Varsayılan değer `wazuh`.
- `<setup.ilm.overwrite>`olarak ayarlandığında `true`, yaşam döngüsü ilkesi başlangıçta üzerine yazılır. Varsayılan değer 'dir `true`.
- `<setup.ilm.enabled>`oluşturulan herhangi bir yeni endekste endeks yaşam döngüsü yönetimini etkinleştirir veya devre dışı bırakır. Varsayılan değer 'dir `false`. Olası geçerli değerler `true`ve ' dir `false`.
- `<filebeat.modules>`Filebeat'in kullanacağı modülleri belirtir.
- `<module>`kullanılacak modülü tanımlar. Varsayılan değer `wazuh`.
- `<alerts>`uyarıların Wazuh dizinleyicisine iletilmesini etkinleştirir veya devre dışı bırakır. Yapılandırma seçeneği olarak ayarlandığında `<enabled>`, `true`uyarılar Wazuh dizinleyicisine iletilir.
- `<archives>`Arşiv günlüklerinin işlenip işlenmeyeceğini ve iletileceğini belirleyen yapılandırmaları belirtir.
- `<logging.level>`günlük düzeyini tanımlar. Varsayılan değer, `info`bilgi günlüklerini temsil eder. Diğer günlük düzeyleri `debug`, `error`, ve 'dir `warning`.
- `<logging.to_files>`dosyalara günlük kaydını etkinleştirir veya devre dışı bırakır. Varsayılan değer 'dir `true`. olarak ayarlandığında `true`, filebeat tüm günlükleri bir dosyaya yazar.
- `<logging.files.path>`günlük dosyalarının saklanacağı dizini belirtir. Varsayılan günlük yolu `/var/log/filebeat`.
- `<logging.files.name>`günlüklerin depolandığı dosyanın adını belirtir. Varsayılan ad `filebeat`.
- `<logging.files.keepfiles>`saklanacak yakın zamanda döndürülen günlük dosyalarının sayısını belirtir. Varsayılan değer 'dir . İzin verilen değer ve `7`arasında bir tam sayıdır .`1`1`0`2`4`
- `<logging.files.permissions>`günlük dosyaları için dosya izinlerini ayarlar. Varsayılan değer 'dir `0644`, bu da günlük dosyalarının sahibinin bunları okuyabileceği ve yazabileceği, diğerlerinin ise yalnızca okuyabileceği anlamına gelir.
- `<logging.metrics.enabled>`dahili ölçümlerin günlüğe kaydedilmesini etkinleştirir veya devre dışı bırakır. Varsayılan değer 'dir `true`. Olası değerler `true`ve ' dir `false`.
- `<seccomp>`filebeat işleminin yapabileceği sistem çağrılarının sayısını kısıtlayan bir secomp (güvenli bilgi işlem modu) politikası belirtir.
- `<default_action>`sistem çağrıları için varsayılan eylemi izin verecek şekilde ayarlar. Bu, syscalls listesinde açıkça belirtilmeyen herhangi bir sistem çağrısına varsayılan olarak izin verileceği anlamına gelir.
- `<syscalls>`sistem çağrısı adlarının ve karşılık gelen eylemlerin bir listesini tanımlar.
- `<action>`listelenen sistem çağrılarından herhangi biri `names`yürütüldüğünde gerçekleştirilecek eylemi belirtir. Varsayılan değer 'dir `allow`. Diğer değerler `errno`, `trace`, `trap`, `kill_thread`, `kill_process`, ve 'dir `log`.
- `<names>`sistem çağrısı adlarının bir listesini tanımlar. Listede en az bir sistem çağrısı tanımlanmalıdır. `rseq`(yeniden başlatılabilir diziler) sistem çağrısı, birden fazla iş parçacığında paylaşılan bellekte kullanıcı alanı işlemlerini hızlandırmak için kullanılır. `rseq` Sistem çağrısına bu yapılandırmada izin verilir.

Wazuh Indeksleyici Bağlayıcısı

Wazuh dizinleyici bağlayıcısı şu anda Wazuh yöneticisinden güvenlik açığı verilerini alıyor ve güvenli bir şekilde Wazuh dizinleyicisine iletiyor. Güvenlik açığı verilerini Elastic Common Schema'yı (ECS) takip eden JSON formatında alıyor ve veri tutarlılığı ve güvenilirliğini sağlamak için durumunu Wazuh dizinleyicisiyle senkronize ediyor. Wazuh dizinleyici bağlayıcısı Wazuh yöneticisiyle birlikte gönderilir.

`/var/ossec/etc/ossec.conf`İndeksleyici bağlayıcısı için standart yapılandırma , Wazuh sunucusundaki dosyada aşağıda gösterildiği gibi belirtilmiştir :

```
<ossec_config>
 <indexer>
   <enabled>yes</enabled>
   <hosts>
    <host>https://127.0.0.1:9200</host>
   </hosts>
   <ssl>
    <certificate_authorities>
     <ca>/etc/filebeat/certs/root-ca.pem</ca>
    </certificate_authorities>
    <certificate>/etc/filebeat/certs/filebeat.pem</certificate>
    <key>/etc/filebeat/certs/filebeat-key.pem</key>
   </ssl>
 </indexer>
</ossec_config>
```

Nerede:

- `<indexer>`Wazuh indeksleyici bağlayıcısı için yapılandırma seçeneklerini belirtir.
- `<enabled>`Wazuh dizinleyici bağlayıcısını etkinleştirir veya devre dışı bırakır. Bu seçenek için izin verilen değerler ve'dir `yes`. `no`Değer, `yes`Wazuh dizinleyici bağlayıcısını etkinleştirir ve `no`devre dışı bırakır. Varsayılan değer 'dir `yes`.
- `<hosts>`bağlanılacak Wazuh dizinleyici düğümlerinin bir listesini belirtir. `host`Her düğüm bağlantısını ayarlamak için seçeneği kullanın.
- `<host>`bağlanılacak Wazuh dizinleyici düğüm URL'sini veya IP adresini belirtir. Örneğin, `http://172.16.1.11`veya `192.168.3.2:9230`. Varsayılan olarak, değer localhost ana bilgisayarına ayarlanır: `https://127.0.0.1:9200`.
- `<ssl>`SSL parametreleri için yapılandırma seçeneklerini belirtir.
- `<certificate_authorities>`doğrulama için kök sertifika dosya yollarının bir listesini belirtir. `ca`Her CA sertifika dosya yolunu ayarlamak için seçeneği kullanın.
- `<ca>`HTTPS sunucu doğrulamaları için kök CA sertifikasını belirtir. Varsayılan değer 'dir `/etc/filebeat/certs/root-ca.pem`. Olası değer herhangi bir geçerli CA sertifikasıdır.
- `<certificate>`Filebeat SSL sertifikasına giden yolu belirtir. Varsayılan değer 'dir `/etc/filebeat/certs/filebeat-key.pem`. Olası değer herhangi bir geçerli anahtardır.
- `<key>`kimlik doğrulama için kullanılan sertifika anahtarını belirtir. Varsayılan değer 'dir `/etc/filebeat/certs/filebeat-key.pem`. Olası değer herhangi bir geçerli anahtardır.

Referans kılavuzunun dizinleyici bölümünde mevcut yapılandırma seçenekleri hakkında daha fazla bilgi edinebilirsiniz .

Üçüncü Taraf Indexer

Wazuh yöneticisi uyarıları üçüncü taraf dizinleyicilere iletebilir. Wazuh yöneticilerini yalnızca günlük analizi için kullanıyorsanız ve uyarıları dizinleme ve depolama için üçüncü taraf çözümlere iletmek istiyorsanız, alternatif seçenekler mevcuttur. Wazuh, uyarıları istediğiniz çözüme aktarmak için her Wazuh yönetici düğümüne istediğiniz veri ileticisini yüklemenize olanak tanır. Şu anda Wazuh, aşağıdaki üçüncü taraf çözümler için belgeler sunmaktadır:

Çözüm	Tanım
ELK Stack	Wazuh yöneticisi uyarılarını Logstash kullanarak ELK Stack'e iletme.
OpenSearch	Wazuh yöneticisi uyarılarını Logstash kullanarak OpenSearch'e iletme.
Splunk	Wazuh yöneticisi uyarılarını Logstash kullanarak Splunk'a iletme.
	Splunk Evrensel Yönlendiriciyi kullanarak Wazuh sunucu uyarılarını Splunk'a iletme.

Bu seçenekler, Wazuh'u mevcut izleme ve analiz altyapınızla entegre etmede esneklik sağlar.

Revision #4
Created 28 December 2024 00:33:31 by Ayşegül Sarıkaya
Updated 31 December 2024 13:26:28 by Ayşegül Sarıkaya