

Wazuh Indexer Endeksleri

Bir dizin, birbirleriyle ilişkili belgelerin bir koleksiyonudur. Wazuh dizinleyicisi, hızlı erişim için güvenlik verilerini depolamak ve düzenlemek için dizinleri kullanır. Wazuh, bu verileri depolamak için aşağıdaki dizin desenlerini kullanır:

- `wazuh-alerts-*` : Bu, Wazuh sunucusu tarafından oluşturulan uyarılar için dizin desenidir.
- `wazuh-archives-*` : Bu, Wazuh sunucusuna gönderilen tüm olaylar için dizin desenidir.
- `wazuh-monitoring-*` : Bu, Wazuh araçlarının durumu için endeks desenidir.
- `wazuh-statistics-*` : Bu, Wazuh sunucusunun istatistiksel bilgilerine ait dizin desenidir.
- `wazuh-states-vulnerabilities-*` : - Bu, izlenen uç noktalarda tespit edilen güvenlik açıkları hakkındaki bilgilere yönelik dizin desenidir.

Uyarılar için dizin desenini daha da özelleştirmek için özel bir dizin deseni oluşturabilirsiniz.

Özel İzin Deseni Oluşturma

`my-custom-alerts-*` Bu bölümde , varsayılan desen olan . ile birlikte örneğin . gibi özel bir dizin deseninin nasıl oluşturulacağı açıklanmaktadır. `wazuh-alerts-*` Kök kullanıcıya geçin ve aşağıdaki adımları uygulayın.

1. Filebeat hizmetini durdurun:

```
systemctl stop filebeat
```

2. Wazuh şablonunu indirin ve bir dosyaya kaydedin (örneğin, `template.json`):

```
curl -so template.json
https://raw.githubusercontent.com/wazuh/wazuh/v4.9.2/extensions/elasticsearch/7.x/wazuh-
template.json
```

3. Şablon dosyasını açın ve dosyanın başında şu satırı bulun:

```
"index_patterns": [
  "wazuh-alerts-4.x-*",
  "wazuh-archives-4.x-*"
],
```

Özel deseninizi şu şekilde görünecek şekilde ekleyin:

```
"index_patterns": [  
  "wazuh-alerts-4.x-*",  
  "wazuh-archives-4.x-*",  
  "my-custom-alerts-*"  
],
```

Dizin desenlerindeki yıldız karakteri (*) önemlidir çünkü Filebeat, Wazuh panosundaki uyarıları görselleştirmek için doğru formatı uygulamak için gerekli olan bu deseni izleyen bir ad kullanarak dizinler oluşturacaktır.

4. Değişiklikleri kaydedin ve yeni şablonu Wazuh indeksleyicisine ekleyin. Bu, mevcut şablonu değiştirecektir:

```
curl -XPUT -k -u <INDEXER_USERNAME>:<INDEXER_PASSWORD>  
'https://<INDEXER_IP_ADDRESS>:9200/_template/wazuh' -H 'Content-Type: application/json' -d  
@template.json
```

Yer değiştirmek:

- <INDEXER_IP_ADDRESS> Wazuh dizinleyicinizin IP adresiyle
- <INDEXER_USERNAME> ve <INDEXER_PASSWORD> Wazuh dizinleyici kullanıcı adı ve parolasıyla. Yeni dağıtımlar için Wazuh dizinleyici kimlik bilgilerini şu komutu kullanarak alabilirsiniz:

Not: Wazuh OVA kullanıyorsanız varsayılan kimlik bilgilerini kullanın veya [parola yönetimi](#) admin:admin bölümüne bakın .

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "'admin\'" -A 1
```

Output

```
{"acknowledged":true}
```

Not: {"acknowledged":true} şablonun doğru şekilde eklendiğini gösterir.

Uyarı: wazuh-alerts-* 5. adımı yalnızca varsayılan uyarı dizini modelini ve/veya varsayılan arşiv dizini modelini . wazuh-archives-* ile değiştirmek istiyorsanız uygulayın my-custom-alerts-*

5. Wazuh uyarı yapılandırma dosyasını `/usr/share/filebeat/module/wazuh/alerts/manifest.yml` ve isteğe bağlı olarak arşiv dosyasını açın `/usr/share/filebeat/module/wazuh/archives/manifest.yml` ve dizin adını değiştirin.

Örneğin, şuradan:

```
- name: index_prefix  
  default: wazuh-alerts-
```

Buna:

```
- name: index_prefix  
  default: my-custom-alerts-
```

Not: Dizin adı `#`, `\`, `/`, `*`, `?`, `"`, `<`, `>`, `|`, karakterlerini içermemeli ve `,`, `.` veya `_` ile başlamamalıdır. Ayrıca, tüm harfler küçük harf olmalıdır. `-` ve `+`

6. (İsteğe bağlı) Yeni dizin desenini varsayılan olarak kullanmak istiyorsanız, dosyayı açın `/usr/share/wazuh-dashboard/data/wazuh/config/wazuh.yml` ve aşağıdaki yapılandırmayı ekleyin:

```
pattern: my-custom-alerts-*
```

Bu, Wazuh sunucusunun yeni endeks desenini otomatik olarak oluşturmasını ve/veya seçmesini sağlayacaktır.

7. Filebeat'i ve Wazuh sunucu bileşenlerini yeniden başlatın:

```
systemctl restart filebeat  
systemctl restart wazuh-manager  
systemctl restart wazuh-indexer  
systemctl restart wazuh-dashboard
```

Uyarı: Önceki adla oluşturulmuş dizinleriniz varsa, bunlar değiştirilmeyecektir. Bunları görmek için yine de önceki dizin düzenine geçebilir veya mevcut dizinleri yeniden adlandırmak için yeniden dizinleme yapabilirsiniz.

Endeks Bilgilerinin Kontrol Edilmesi

Wazuh endeksleri hakkında bilgiye iki şekilde ulaşabilirsiniz.

- Web kullanıcı arayüzünü kullanma.
- Wazuh indeksleyici API'sine bir istekte bulunuluyor.

Web Kullanıcı Arayüzünü Kullanma

1. Wazuh kontrol panelinin sol üst menüsünde ☰ , **Dizin Yönetimi** > **Dizin Yönetimi**'ne gidin.

Endeks yönetimi menü seçeneği

2. **Endekslere** tıklayın.

Endeks yönetimi endeksleri seçeneği

Desen Wazuh panosunda mevcut değilse, my-custom-alerts-* şablonunda kullanılan dizin desenini kullanarak yeni bir tane oluşturun ve **Zaman Filtresi** alan adı olarak timestamp kullandığınızdan emin olun .

Özel uyarı dizini deseni oluşturma

Wazuh Indexer API'sini Kullanma

Wazuh gösterge panelinden veya Wazuh sunucusundan Wazuh indeksleyici API'sini kullanarak endeks bilgilerini sorgulayabilirsiniz.

Wazuh Dashboard

1. ☰ > **Dizinleyici yönetimi** > **Geliştirme Araçları**'na gidin :

```
GET /_cat/indices/wazuh-*?v
```

Dev Tools endeksleri listesi

Komut Satırı Arayüzü

1. Aşağıdaki komutu kullanarak yeni dağıtımlar için Wazuh dizinleyici kullanıcı adı ve parolasını edinin:

```
tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "'admin\'" -A 1
```

Not: Wazuh OVA kullanıyorsanız varsayılan kimlik bilgilerini admin:admin olarak kullanın veya [parola yönetimi](#) bölümüne bakın.

2. Dizin durumunuzu sorgulamak için aşağıdaki komutu çalıştırın. ve'yi elde edilen kullanıcı adı ve parola ile değiştirin. Wazuh dizinleyici IP adresiniz veya FQDN'nizle değiştirin `<INDEXER_USERNAME>`. Sorgunuz için daha belirli bir desenle değiştirebilirsiniz, örneğin .

`<INDEXER_PASSWORD><INDEXER_IP_ADDRESS>wazuh-*wazuh-alerts-*`

```
curl -k -u <INDEXER_USERNAME>:<INDEXER_PASSWORD>
https://<INDEXER_IP_ADDRESS>:9200/_cat/indices/wazuh-*?v
```

Output

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size
green	open	wazuh-statistics-2023.30w	xtHZtGqBR0WNJWbs5sjrnQ	1	0	2394	0	1.2mb	
green	open	wazuh-alerts-4.x-2023.07.28	VbBfAasJTsiqw3lwRhY5sg	3	0	513	0	1.9mb	
green	open	wazuh-alerts-4.x-2023.07.27	7s2x8lNqRVmtz5uqMDuA7Q	3	0	515	0	2mb	
green	open	wazuh-alerts-4.x-2023.07.05	0h4cyLjoQYiMvMnqyLDnag	3	0	49	0	370.4kb	
green	open	wazuh-alerts-4.x-2023.07.07	kp_N4c7RRuOE91KkuqPuAw	3	0	98	0	397.7kb	
green	open	wazuh-alerts-4.x-2023.07.29	rbAC4bef57epxOjiSzFRQQ	3	0	1717	0	3.9mb	
green	open	wazuh-monitoring-2023.31w	1WwxSGQHRfG1_DOIZD-Lag	1	0	954	0	771.9kb	
green	open	wazuh-alerts-4.x-2023.07.20	SQbaQC24SgO9eWO_AsBI_w	3	0	1181	0	2.8mb	
green	open	wazuh-statistics-2023.28w	jO52bS6eRamtB2YNmfGzIA	1	0	676	0	501.1kb	

wazuh-alerts-* Endeksleri

Wazuh sunucusu izlenen uç noktalardan alınan olayları analiz eder ve olaylar bir algılama kuralıyla eşleştğinde uyarılar üretir. Bu uyarılar dizinler kullanılarak kaydedilir `wazuh-alerts-*`.

Wazuh sunucusu uyarı verilerini varsayılan olarak `/var/ossec/logs/alerts/alerts.json`ve dosyalarına kaydeder. Dosyaya kaydedildikten sonra, JSON uyarı belgesini indeksleme için Wazuh indeksleyici API'sine iletir. İndekslenen dosyalar Wazuh indeksleyicisinin dizininde saklanır.

`/var/ossec/logs/alerts/alerts.log/var/ossec/logs/alerts/alerts.json/var/lib/wazuh-indexer/nodes/0/indices`

Wazuh dizinleyicisine uyarıları iletirken, Wazuh sunucusu geçerli tarihi bir dizin adına biçimlendirir. Örneğin, Wazuh sunucusu dizin adlarını `wazuh-alerts-4.x-2023.03.17`ve `wazuh-alerts-4.x-2023.03.18`sırasıyla 17 ve 18 Mart uyarılarını tanımlar. Wazuh dizinleyicisi daha sonra tanımlanan `wazuh-alerts-*`dizin adlarını kullanarak uyarı dizinleri oluşturur.

`/usr/share/filebeat/module/wazuh/alerts/ingest/pipeline.json`Wazuh sunucusunun dosyasındaki varsayılan dizin adını değiştirebilirsiniz . Bunu yapmak için, dosyadaki varsayılan dizin adı biçimlendirmesini değiştirmek için `date_index_name`alanına ve anahtara gidin :`date_rounding`

`/usr/share/filebeat/module/wazuh/alerts/ingest/pipeline.json`

```
{
  "description": "Wazuh alerts pipeline",
  "processors": [
    { "json" : { "field" : "message", "add_to_root": true } },
    {
      "geoip": {
        "field": "data.srcip",
        "target_field": "GeoLocation",
        "properties": ["city_name", "country_name", "region_name", "location"],
        "ignore_missing": true,
        "ignore_failure": true
      }
    },
    {
      "geoip": {
        "field": "data.win.eventdata.ipAddress",
        "target_field": "GeoLocation",
        "properties": ["city_name", "country_name", "region_name", "location"],
        "ignore_missing": true,
        "ignore_failure": true
      }
    },
    {
      "geoip": {
        "field": "data.aws.sourceIPAddress",
        "target_field": "GeoLocation",
        "properties": ["city_name", "country_name", "region_name", "location"],
        "ignore_missing": true,
        "ignore_failure": true
      }
    },
    {
      "geoip": {
        "field": "data.gcp.jsonPayload.sourceIP",
        "target_field": "GeoLocation",
        "properties": ["city_name", "country_name", "region_name", "location"],
        "ignore_missing": true,
        "ignore_failure": true
      }
    },
    {
      "geoip": {
        "field": "data.office365.ClientIP",
        "target_field": "GeoLocation",
        "properties": ["city_name", "country_name", "region_name", "location"],
        "ignore_missing": true,
        "ignore_failure": true
      }
    },
    {
      "date": {
        "field": "timestamp",
        "target_field": "@timestamp",
```

```
"formats": ["ISO8601"],
"ignore_failure": false
},
{
  "date_index_name": {
    "field": "timestamp",
    "date_rounding": "d",
    "index_name_prefix": "{{fields.index_prefix}}",
    "index_name_format": "yyyy.MM.dd",
    "ignore_failure": false
  },
  { "remove": { "field": "message", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "ecs", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "beat", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "input_type", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "tags", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "count", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "@version", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "log", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "offset", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "type", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "host", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "fields", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "event", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "fileset", "ignore_missing": true, "ignore_failure": true } },
  { "remove": { "field": "service", "ignore_missing": true, "ignore_failure": true } }
],
"on_failure" : [{
  "drop" : { }
}]
}
```

Değerlerin olduğu yer:

- ☐ M- ay anlamına gelir
- ☐ w- hafta anlamına gelir
- ☐ d- günü temsil eder

wazuh-archives-* Endeksleri

`/var/ossec/logs/alerts/alerts.json` ve dosyalarına uyarıları kaydetmenin yanı sıra `/var/ossec/logs/alerts/alerts.log`, Wazuh arşivlerini Wazuh sunucusunun aldığı tüm olayları kaydetmesi ve dizine eklemesi için etkinleştirebilirsiniz. Bu, Wazuh tarafından analiz edilen olayları ve uyarıları tetiklemeyen olayları içerir.

Tüm olayları depolamak ve dinlemek daha sonraki analiz ve uyumluluk gereksinimleri için yararlı olabilir. Ancak, tüm olayların günlüğe kaydedilmesini ve dinlenmesini etkinleştirmenin Wazuh sunucusundaki depolama gereksinimini artıracakını göz önünde bulundurmalısınız.

/usr/share/filebeat/module/wazuh/archives/ingest/pipeline.json Varsayılan olarak, Wazuh dizinleyici her benzersiz gün için olay dizinleri oluşturur. Wazuh sunucusunun dosyasındaki varsayılan dizin adını değiştirebilirsiniz . Bunu yapmak için:

1. Alana gidin `date_index_name`.
2. Anahtarı bulun `date_rounding` ve dosyadaki varsayılan dizin adı biçimlendirmesini değiştirin `/usr/share/filebeat/module/wazuh/archives/ingest/pipeline.json`.

Aşağıdaki bölümlerde wazuh arşivlerinin nasıl etkinleştirileceği ve endekslerin nasıl ayarlanacağı hakkında ayrıntılar verilmektedir `wazuh-archives-*`.

Wazuh Arşivlerini Etkinleştirme

1. `/var/ossec/etc/ossec.conf` Wazuh sunucusunda düzenleme yapın ve `<logall_json>` satırı . olarak ayarlayın. Bu, tüm olayların `archives.json` dosyasına kaydedilmesini sağlar . Wazuh dizinleyicisine iletmek, tüm olayların JSON formatında kaydedilmesini gerektirir.

```
<logall_json>yes</logall_json>
```

2. Değişikliğin etkili olması için Wazuh yöneticisini yeniden başlatın.

```
systemctl restart wazuh-manager
```

veya

```
service wazuh-manager restart
```

3. Arşiv eşlemesinde düzenleme yapın `/etc/filebeat/filebeat.yml` ve değiştirin `enabled: true` Bu, olayların Wazuh dizinleyicisine iletilmesini sağlar.

```
filebeat.modules:  
- module: wazuh  
  alerts:  
    enabled: true  
  archives:  
    enabled: true
```

4. Değişikliği uygulamak için Filebeat hizmetini yeniden başlatın:

```
systemctl restart filebeat
```

5. Filebeat hizmetinin düzgün çalıştığını test edin:

filebeat test output

Output

```
elasticsearch: https://127.0.0.1:9200...
parse url... OK
connection...
parse host... OK
dns lookup... OK
addresses: 127.0.0.1
dial up... OK
TLS...
security: server's certificate chain verification is enabled
handshake... OK
TLS version: TLSv1.2
dial up... OK
talk to server... OK
version: 7.10.2
```

Endeks Pattern Tanımlama

1. Wazuh kontrol panelinin sol üst menüsünde **≡** , **Kontrol Paneli yönetimi > Kontrol Paneli Yönetimi**'ne gidin ve **Endeks Desenleri**'ne tıklayın .
2. **Dizin deseni oluştur**'a tıklayın .
3. **Dizin desen adı** `wazuh-archives-*` olarak ayarlayın . Bu, iletilen ve dizine eklenen olaylarla eşleşecek dizin deseni tanımlar. **Sonraki adım**'a tıklayın .
4. **Zaman** alanı için **zaman damgasını** seçin.
5. **Dizin deseni oluştur**'a tıklayın.

Not: `@timestamp` yerine `timestamp` seçeneğini seçmeye dikkat edin .

Endeks Pattern Görüntüleme

1. Sol üst menüde **Keşfet**'e **≡** tıklayın ve ardından **Keşfet**'e tıklayın .
2. Etkinlikleri görüntülemek için **wazuh-archives-*** öğesini seçin .

Wazuh arşiv etkinlikleri

wazuh-monitoring-* Endeksleri

Kayıtlı bir Wazuh temsilcisinin herhangi bir andaki bağlantı durumu aşağıdakilerden biridir:

- **Aktif**
- **Bağlantısı kesildi**
- **Askıda olması**
- **Hiç bağlanmadı**

Wazuh, tüm araçlarının bağlantı durumlarının geçmişini depolar. Varsayılan olarak, aracı bağlantı durumunu `wazuh-monitoring-*` dizinleri kullanarak dizinler. Wazuh dizinleyicisi varsayılan olarak haftada bir bu dizinlerden birini oluşturur. [Özel oluşturma aralıkları](#) hakkındaki belgeleri kontrol edin . Bu dizinler varsayılan olarak tüm araçların bağlantı durumunu her 15 dakikada bir depolar. [API isteklerinin sıklığı](#) hakkındaki belgeleri kontrol edin .

Wazuh panosu, aracı durumu hakkında bilgi görüntülemek için bu endekslere ihtiyaç duyar. Örneğin, **☰ > Sunucu yönetimi > Uç Nokta Özeti**'ne tıklayarak , Wazuh aracısının bağlantı durumu ve belirlenen zaman dilimlerindeki geçmiş evrimi gibi bilgileri görebilirsiniz.

Temsilciler panosundaki durum ve evrim

[Wazuh panosu yapılandırma dosyasında](#) , aşağıdakileri yapmak için ayarları değiştirebilirsiniz:

- Aracılar için bağlantı durumu verilerinin eklenmesini ve gösterilmesini devre dışı bırakın. Bunu başarmak için `wazuh.monitoring.enabled`'ı değiştirin.
- Aracılar için bağlantı durumu verilerinin ekleme sıklığını değiştirin. Bunu başarmak için `wazuh.monitoring.frequency`'yi değiştirin.

Wazuh-istatistik-* Endeksleri

Wazuh panosu, `wazuh-statistics-*` Wazuh sunucu kullanımı ve performansı hakkında istatistikleri görüntülemek için endeksleri kullanır. Görüntülenen bilgiler arasında kod çözülen olay sayısı, alınan baytlar ve TCP oturumları bulunur.

Wazuh panosu, kullanımla ilgili bilgileri sorgulamak için Wazuh yönetici API'sine istekler çalıştırır. `wazuh-statistics-*` Toplanan bilgilerden endekslere veri ekler. Wazuh endeksleyicisi `wazuh-statistics-*` varsayılan olarak haftada bir endeks oluşturur. [İstatistik oluşturma aralığı hakkındaki belgeleri kontrol edin](#). Bu endeksler varsayılan olarak Wazuh sunucusu istatistiklerini her 5 dakikada bir **depolar**. Görev yürütme sıklığı hakkındaki belgeleri kontrol edin .

Bu bilgileri Wazuh panosunda görüntülemek için **Sunucu yönetimi > İstatistikler** bölümüne gidin.

İstatistik analiz motoru panosu

wazuh-states-vulnerabilities-* Endeksleri

Dizin deseni, wazuh-states-vulnerabilities-* izlenen varlıkların güvenlik açığı durumuyla ilgili verileri depolamak için Wazuh'ta kullanılır. Bu dizin genellikle izlenen sistemlerde tespit edilen güvenlik açıkları hakkında bilgi içerir; bu bilgiler arasında ciddiyet, durum, etkilenen yazılım ve güvenlik açığı referansı gibi ayrıntılar bulunur. *Dizin deseninin sonunda, benzer adlara sahip, zamana veya diğer faktörlere göre bölümlere ayrılmış birden fazla dizinin oluşturulmasına olanak tanır. Bu, güvenlik açığı verilerinin zaman içinde verimli bir şekilde depolanmasını ve alınmasını sağlar.

Bu bilgileri Wazuh panosunda görüntülemek için Wazuh panosu ana sayfasından **Güvenlik Açığı Tespiti'ne tıklayın**.

Wazuh güvenlik açıkları endekslerini belirtiyor
Wazuh güvenlik açıkları endekslerini belirtiyor

Revision #4
Created 31 December 2024 18:01:41 by Ayşegül Sarıkaya
Updated 31 December 2024 20:38:52 by Ayşegül Sarıkaya