Wazuh Indexer

Wazuh dizinleyicisi, güvenlik verileri için gerçek zamanlı, tam metin arama ve analiz motorudur. Wazuh sunucusuna alınan günlük verileri analiz edilir ve dizinleme ve depolama için dizinleyiciye iletilir. Bu olaylar daha sonra Wazuh panosunda sorgulanır. Wazuh dizinleyicisi verileri JSON belgeleri olarak depolar. Her belge, bir dizi anahtarı, alan adını veya özniteliği, karakterler, sayılar, boole değerleri, tarihler, değer dizileri, coğrafi konumlar veya diğer veri türleri olabilen karşılık gelen değerleriyle ilişkilendirir. Wazuh dizinleyicisi, ölçeklenebilirlik ve yüksek kullanılabilirlik sağlayan tek düğümlü veya çok düğümlü bir küme olarak yapılandırılabilir. Belgeleri, shard olarak bilinen farklı kapsayıcılara dağıtır. Sırayla, bu shard'ları küme düğümlerine dağıtır. Belgeleri birden fazla shard'a ve bu shard'ları birden fazla düğüme dağıtarak, Wazuh dizinleyicisi yedekliliği garanti eder. Yedeklilik, bir arıza durumunda Wazuh dizinleyicisinin kullanılabilirliğini garanti eder ve küme düğümleri arasında sorgu kapasitesini artırır.

- Wazuh Indexer Endeksleri
- Yeniden İndeksleme
- Index Yaşam Döngüsü Yönetimi
- Wazuh Indexer Ayarı
- Wazuh Endekslerinin Taşınması

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 aracılarının 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.`_-+`

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-*` şablonda 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          1.2mb
green  open   wazuh-alerts-4.x-2023.07.28 VbBfAasJTsiqw3lwRhY5sg   3   0       513            0      1.9mb          1.9mb
green  open   wazuh-alerts-4.x-2023.07.27 7s2x8INqRVmtz5uqMDuA7Q   3   0       515            0        2mb            2mb
green  open   wazuh-alerts-4.x-2023.07.05 0h4cyLJoQYiMvMnqyLDnag   3   0        49            0    370.4kb        370.4kb
green  open   wazuh-alerts-4.x-2023.07.07 kp_N4c7RRuOE91KkuqPuAw   3   0        98            0    397.7kb        397.7kb
green  open   wazuh-alerts-4.x-2023.07.29 rbAC4befS7epxOjiSzFRQQ   3   0      1717            0      3.9mb          3.9mb
green  open   wazuh-monitoring-2023.31w   1WwxsGQHRfG1_DOIZD-Lag   1   0       954            0    771.9kb        771.9kb
green  open   wazuh-alerts-4.x-2023.07.20 SQbaQC24SgO9eWO_AsBI_w   3   0      1181            0      2.8mb          2.8mb
green  open   wazuh-statistics-2023.28w   jO52bS6eRamtB2YNmfGzIA   1   0       676            0    501.1kb        501.1kb
```

wazuh-alerts-* Endeksleri

Wazuh sunucusu izlenen uç noktalardan alınan olayları analiz eder ve olaylar bir algılama kuralıyla eşleştiğinde 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` alana 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 dizinlemek daha sonraki analiz ve uyumluluk gereksinimleri için yararlı olabilir. Ancak, tüm olayların günlüğe kaydedilmesini ve dizinlenmesini etkinleştirmenin Wazuh

sunucusundaki depolama gereksinimini artıracağını 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`yes` 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 desenini 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

Image not found or type unknown

wazuh-monitoring-* Endeksleri

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

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

Wazuh, tüm aracılarının 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 aracıların 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 .

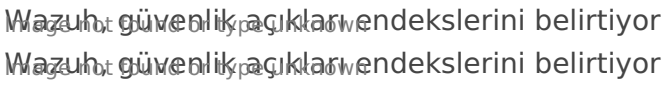
Bu bilgileri Wazuh panosunda görüntülemek için **Sunucu yönetimi** > **İstatistikler** bölümüne gidin.



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

Yeniden İndeksleme

Dizinin veri şemasında değişiklikler yapıldığında, bu değişiklikleri yansıtmak için verileri yeniden dizinlemek gerekir. Mevcut veriler yeniden dizinleme yapılmadan güncellenen şemayla eşleşmeyebilir ve bu da sorgular sırasında veri tutarsızlıklarına veya hatalara yol açabilir. Yeniden dizinleme, verilerinizin tamamını veya bir alt kümesini bir kaynak dizinden hedef dizine kopyalamanıza olanak tanır.

Mevcut bir dizini yeniden dizinlemek için Wazuh panosunda veya Wazuh sunucusunda aşağıdaki adımları uygulayın.

Wazuh Dashboard

1. **Sol üst menüye** ☰ tıklayın ve **Indexer yönetimine,** ardından da **Dev Tools'a** gidin .
2. Aşağıdaki API çağrısını, `my-source-index`kaynak dizin deseniyle ve `my-destination-index`hedef dizin deseniyle değiştirerek girin.

```
POST /_reindex
{
  "source":{
    "index":"my-source-index"
  },
  "dest":{
    "index":"my-destination-index"
  }
}
```

Örneğin:

```
POST /_reindex
{
  "source":{
    "index":"wazuh-alerts-*"
  },
  "dest":{
    "index":"example-alerts"
  }
}
```

Output

```
{
  "took": 23655,
```

```
  "timed_out": false,
  "total": 26849,
  "updated": 0,
  "created": 26849,
  "deleted": 0,
  "batches": 27,
  "version_conflicts": 0,
  "noops": 0,
  "retries": {
    "bulk": 0,
    "search": 0
  },
  "throttled_millis": 0,
  "requests_per_second": -1,
  "throttled_until_millis": 0,
  "failures": []
}
```


Komut Satırı Arayüzü

Wazuh API'sine kimlik doğrulaması yapmasına izin verilen herhangi bir Wazuh merkezi bileşeninde aşağıdaki komutu çalıştırın. `<INDEXER_USERNAME>`ve'yi `<INDEXER_PASSWORD>`dizinleyici kullanıcı adı ve parolasıyla değiştirin:

```
curl -k -u "<INDEXER_USERNAME>:<INDEXER_PASSWORD>" -XPOST "https://<INDEXER_IP_ADDRESS>:9200/_rein
{
  "source":{
    "index":"my-source-index"
  },
  "dest":{
    "index":"my-destination-index"
  }
}'
```

Örneğin:

```
root@wazuh-server:~$ curl -k -u "INDEXER_USERNAME:INDEXER_PASSWORD" -XPOST "https://<INDEXER_IP_ADDR
{
  "source":{
    "index":"wazuh-alerts-*"
  },
  "dest":{
    "index":"example-alerts"
  }
}'
```

Output

{"took":18025,"timed_out":false,"total":26854,"updated":26854,"created":0,"deleted":0,"batches":27,"version_cor

Index Yaşam Döngüsü Yönetimi

Dizin yaşam döngüsü yönetimi, bir dizinin yaşam döngüsünü kontrol ederek Wazuh dizinleyici kümesi performansını optimize etmeye yardımcı olur. Dizin devretme ve silme gibi periyodik işlemler gerçekleştirebilirsiniz. Bu periyodik işlemler Dizin Durumu Yönetimi (ISM) politikaları kullanılarak yapılandırılır.

Dizin Durumu Yönetimi (ISM), bu operasyonel görevleri otomatikleştirmenizi sağlar. ISM kullanarak verileriniz için saklama politikaları gibi yaşam döngüsü politikalarını uygulayabilirsiniz. ISM, politikalarınıza ve dizin yaşı, boyutu ve belge sayısında algılanan değişikliklere göre dizin işlemlerini otomatik olarak tetikler.

Bu bölümde, Wazuh dizinleyici depolama alanının optimizasyonu için dizin yaşam döngüsünü yönetmek üzere bazı yapılandırma seçenekleri ele alınmaktadır.

Index Tutma

Güvenlik standartları, verilerin denetimler için asgari bir süre boyunca erişilebilir tutulmasını gerektirir. Bu saklama süresinden daha eski veriler için, depolama alanından tasarruf etmek amacıyla verileri silmek isteyebilirsiniz.

Silme işlemlerini otomatik olarak işlemek için belirli politikalar tanımlayabilirsiniz. Bu politikaları dizin geçişleri için de yararlı bulabilirsiniz.

Bir Saklama Politikası Oluşturma

Görsel Düzenleyiciyi Kullanma

1. Sol üst menüye tıklayın ☰ **, Indexer yönetimine** gidin ve **Index Yönetimi'ni seçin. Durum yönetimi politikalarını** seçin ve **Politika oluştur'a** tıklayın . **Görsel düzenleyiciyi** seçin ve **Devam'a** tıklayın.

Devlet yönetim politikaları
Image not found or type unknown

Görsel düzenleyici yapılandırma yöntemi

Image not found or type unknown

2. **Politika bilgisi** bölümüne benzersiz bir **Politika Kimliği** girin . Örneğin, `wazuh-alert-retention-policy`. İsteğe bağlı olarak politikayı **Açıklama** alanında tanımlayabilirsiniz .

Politika oluştur

Image not found or type unknown

3. **ISM şablonları** altında **Şablon ekle'ye** tıklayın ve bu politikayı gelecekteki uyarı dizinlerine otomatik olarak uygulamak gibi bir dizin deseni girin . Öncelik varsayılan değerine ayarlanır ve başka herhangi bir değere ayarlanabilir. Öncelik değeri daha yüksek olan dizin önce işlenir.`wazuh-alerts-*1`
4. **Dizin silme için bir durum oluşturmak üzere Durum ekle'ye** tıklayın . . gibi bir ad girin `delete_alerts`.
5. **Eylem ekle'ye** tıklayın ve **Eylem türünde** Sil'i **seçin** . **Eylem ekle'ye** tıklayın . Ardından **Durumu kaydet'e** tıklayın .
6. **Başlangıç durumunu oluşturmak için tekrar Durum ekle'ye** tıklayın . . gibi bir ad girin `initial`.
7. **Sipariş** sekmesinden **Önce Ekle'yi** seçin ve **delete_alerts** seçeneğini seçin .
8. **Geçiş ekle'ye** tıklayın ve **Hedef durumu** olarak **delete_alerts'i** seçin .
9. Condition'da **Minimum Endeks Yaşını** seçin . **Minimum Endeks Yaşına** örneğin 90 gün için **90d gibi** tutma değerini girin .
10. **Geçiş Ekle'ye** tıklayın . **Durumu Kaydet'e tıklayın. Oluştur'a** tıklayın .
11. **Başlangıç Durumunu Başlangıç** olarak değiştirin.

ISM Politika Devletleri

Image not found or type unknown

JSON Editor Kullanma

1. Sol üst menüye tıklayın ☰ **, Indexer yönetimine** gidin ve **Index Yönetimi'ni seçin. Durum yönetimi politikalarını** seçin ve **Politika oluştur'a** tıklayın . **JSON düzenleyicisini** seçin ve **Devam'a** tıklayın.

JSON düzenleyici yapılandırma yöntemi

Image not found or type unknown

2. **Politika bilgisi** bölümüne benzersiz bir **Politika Kimliği** girin . Örneğin, `wazuh-alert-retention-policy` . İsteğe bağlı olarak JSON politika tanımınıza bir açıklama girebilirsiniz.

JSON politika tanımı

Image not found or type unknown

3. **Define policy** bölümünde , içeriği JSON policy tanımınızla değiştirin. Tanımınız buna benzer görünmelidir.

```
{
  "policy": {
    "policy_id": "wazuh-alert-retention-policy",
    "description": "Wazuh alerts retention policy",
    "schema_version": 17,
    "error_notification": null,
    "default_state": "retention_state",
    "states": [
```

```
        {
          "name": "retention_state",
          "actions": [],
          "transitions": [
            {
              "state_name": "delete_alerts",
              "conditions": {
                "min_index_age": "90d"
              }
            }
          ]
        },
        {
          "name": "delete_alerts",
          "actions": [
            {
              "retry": {
                "count": 3,
                "backoff": "exponential",
                "delay": "1m"
              },
              "delete": {}
            }
          ],
          "transitions": []
        }
      ],
      "ism_template": [
        {
          "index_patterns": [
            "wazuh-alerts-*"
          ],
          "priority": 1
        }
      ]
    }
}
```

Minimum endeks tutma için tercih ettiğiniz gün sayısına göre `“min_index_age”:`ayarlayın . `“90d”`

4. **Oluştur'a** tıklayın .

Saklama Politikasının Uyarı Dizinine Uygulanması

1. Sol üst menüye tıklayın ☰ **, Indexer yönetimine** gidin ve **Index Yönetimi'ni** seçin . **Indexes'i** seçin .
2. Politikayı eklemek istediğiniz endeksi veya endeksleri seçin.
3. **Eylemler** > **Politikayı uygula'ya** tıklayın.

Politikayı endekslere uygula

Image not found or type unknown

4. Önceki adımlarda oluşturulan politikayı **Politika Kimliği menüsünden seçin. Uygula'ya** tıklayın .

Sıcak-ılık Mimarisini Kurun

Bu bölüm, sıcak ve ılık düğümlerde depolanacak dizinlerin nasıl yapılandırılacağını gösterir. Sıcak-ılık bir mimari, aşağıdaki özelliklere sahip sıcak ve ılık düğümlerden oluşur:

- Sıcak düğümler, yüksek bilgi işlem kaynaklarına sahip olmaları nedeniyle genellikle hızlı ve pahalıdır.
- Sıcak bir düğüm, daha düşük bilgi işlem kaynaklarına ihtiyaç duyması nedeniyle daha yavaş ve daha ucuzdur.

Verilerinizi önce sıcak düğümlere dizinlediğiniz ve belirli bir süre sonra sıcak düğümlere taşıdığınız sıcak-ılık bir mimari tasarlayabilirsiniz. Bu mimari, sık sık sorgulamadığınız eski verileriniz varsa sizin için uygundur. Eski veriler, daha yavaş ve daha az maliyetli bir donanımda depolanmak üzere taşınır. Bu mimari, bilgi işlem maliyetlerinden tasarruf etmenize yardımcı olur.

Sıcak düğüm sayısını artırmak yerine, sık erişmediğiniz veriler için sıcak düğümler ekleyebilirsiniz.

Sıcak-ılık depolama mimarisini yapılandırmak için `temp`ilgili düğümlere nitelikler ekleyin.

> Not: Tüm sıcak ve ılık düğümleriniz için tutarlı olduğu sürece, öznitelik adını ve değerini istediğiniz şekilde ayarlayabilirsiniz.

Sıcak (Hot) Bir Düğüm Yapılandırın

Sıcak bir düğümü yapılandırmak için dosyaya aşağıdaki yapılandırmayı ekleyin `/etc/wazuh-indexer/opensearch.yml`:

```
node.attr.temp: hot
```

Wazuh dizinleyici hizmetini yeniden başlatın:

```
# systemctl restart wazuh-indexer
```

Sıcak (Worm) Bir Düğüm Yapılandırın

Sıcak bir düğüm yapılandırmak için dosyaya aşağıdaki yapılandırmayı ekleyin `/etc/wazuh-indexer/opensearch.yml`:

```
node.attr.temp: warm
```

Wazuh dizinleyici hizmetini yeniden başlatın:

```
systemctl restart wazuh-indexer
```

Dizinleyici Durum Yönetimi Politikası Oluştur

Wazuh gösterge paneli konsolunda aşağıdaki adımları uygulayın.

1. `temp`Daha önce atanan niteliklerin uygulandığını onaylayın :

   ```
   GET _cat/nodeattrs?v&h=node,attr,value
   ```

2. `wazuh-alerts-4.x-*`Sıcak düğümlere dizin örüntüsünü kullanarak dizinler atamak ve belirli bir süre sonra bunları sıcak düğümlere taşımak için bir ISM politikası oluşturun :

   ```
   PUT _plugins/_ism/policies/hot_warm
   {
     "policy": {
       "description": "Send shards from hot to warm nodes",
       "schema_version": 17,
       "error_notification": null,
       "default_state": "hot",
       "states": [
         {
           "name": "hot",
           "actions": [],
           "transitions": [
             {
               "state_name": "warm",
               "conditions": {
                 "min_index_age": "30d"
               }
             }
           ]
         },
         {
           "name": "warm",
           "actions": [
             {
               "retry": {
                 "count": 3,
                 "backoff": "exponential",
                 "delay": "1m"
               },
               "replica_count": {
                 "number_of_replicas": 0
               }
   ```

```
            },
            {
              "retry": {
                "count": 3,
                "backoff": "exponential",
                "delay": "1m"
              },
              "allocation": {
                "require": {
                  "temp": "warm"
                },
                "include": {},
                "exclude": {},
                "wait_for": false
              }
            }
          ],
          "transitions": []
        }
      ],
      "ism_template": [
        {
          "index_patterns": [
            "wazuh-alerts-*"
          ],
          "priority": 1
        }
      ]
    }
}
```

Sıcak düğümde endeksleri depolamak için minimum gün sayısını tanımlamak için, tercih ettiğiniz gün sayısına `min_index_age` ayarlayın .`30d`

Artık dizin deseni kullanılarak oluşturulan tüm gelecekteki dizinler `wazuh-alerts-4.x-*` sıcak bir düğüme tahsis edilecektir. `min_index_age` Koşul karşılandıktan sonra, dizinler sıcak bir düğüme taşınır ve tüm kopyalar kaldırılır. Kopyaların kaldırılması, veriler sık sık sorgulanmayacağı için depolamanın sıcak düğümde yönetilmesini sağlar.

ISM Politikasını Mevcut Endekslere Uygulayın

1. **Endeks** Yönetimi'nde **Endeksleri** seçin .
2. Politikayı eklemek istediğiniz endeksi veya endeksleri seçin.
3. **Eylemler** > **Politikayı uygula'ya** tıklayın .
4. `hot-warm` Politika Kimliği'nde politikayı seçin .
5. Politikayı seçili endekslere eklemek için **Uygula'ya** tıklayın.

ISM politikasını endekslere uygulayın

Image not found or type unknown

Wazuh Indexer Ayarı

Bu kılavuz, Wazuh dizinleyici performansını optimize etmek için ayarların nasıl değiştirileceğini gösterir. Wazuh dizinleyici parolasını değiştirmek için Parola yönetimi bölümüne bakın.

- Bellek kilitleme
- Parçalar ve kopyalar
- Parça tahsis farkındalığını veya zorunlu farkındalığı yapılandırın
- Bir kümedeki her düğüm için düğüm niteliklerini ayarlayın

Bellek Kilitleme

Sistem belleği takas ederken, Wazuh dizinleyicisi beklendiği gibi çalışmayabilir. Bu nedenle, Wazuh dizinleyici düğümünün sağlığı için Java Sanal Makinesi'nin (JVM) hiçbir zaman diske takas edilmemesi önemlidir. Herhangi bir Wazuh dizinleyici belleğinin takas edilmesini önlemek için, Wazuh dizinleyicisini işlem adres alanını RAM'e kilitlemek üzere aşağıdaki gibi yapılandırın.

> Not: Aşağıda açıklanan komutları çalıştırmak için kök kullanıcı ayrıcalıklarına ihtiyacınız var.

1. `/etc/wazuh-indexer/opensearch.yml`Bellek kilitlemeyi etkinleştirmek için Wazuh indeksleyicisindeki yapılandırma dosyasına aşağıdaki satırı ekleyin :

   ```
   bootstrap.memory_lock: true
   ```

2. Sistem kaynaklarının sınırını değiştirin. Sistem ayarlarını yapılandırmak Wazuh dizinleyici kurulumunun işletim sistemine bağlıdır.

   Systemd

   1. Sistem sınırlarını belirten dosya için yeni bir dizin oluşturun:

      ```
      mkdir -p /etc/systemd/system/wazuh-indexer.service.d/
      ```

   2. Yeni sistem sınırı eklenerek yeni oluşturulan dizinde `wazuh-indexer.conf` dosyayı oluşturmak için aşağıdaki komutu çalıştırın :

      ```
      # cat > /etc/systemd/system/wazuh-indexer.service.d/wazuh-indexer.conf << EOF
      [Service]
      ```

```
LimitMEMLOCK=infinity
EOF
```

SysV Başlatma

1. Sistem sınırlarını belirten dosya için yeni bir dizin oluşturun:

```
mkdir -p /etc/init.d/wazuh-indexer.service.d/
```

2. Yeni sistem sınırı eklenerek yeni oluşturulan dizinde `wazuh-indexer.conf` dosyayı oluşturmak için aşağıdaki komutu çalıştırın :

```
# cat > /etc/init.d/wazuh-indexer.service.d/wazuh-indexer.conf << EOF
[Service]
LimitMEMLOCK=infinity
EOF
```

3. Dosyayı düzenleyin `/etc/wazuh-indexer/jvm.options`ve JVM bayraklarını değiştirin. Bellek kullanımını sınırlamak için bir Wazuh dizinleyici yığın boyutu değeri ayarlayın. JVM yığın sınırları, `OutOfMemory`Wazuh dizinleyicisi önceki adımdaki yapılandırma nedeniyle kullanılabilir olandan daha fazla bellek ayırmaya çalışırsa istisnayı önler. Önerilen değer sistem RAM'inin yarısıdır. Örneğin, 8 GB RAM'li bir sistem için boyutu aşağıdaki gibi ayarlayın.

```
-Xms4g
-Xmx4g
```

Toplam yığın alanı:
- `-Xms4g`- Başlangıç boyutu 4Gb RAM olarak ayarlandı.
- `-Xmx4g`- Maksimum boyut 4Gb RAM'dir.

> Uyarı: Çalışma zamanında JVM yığın yeniden boyutlandırması nedeniyle performans düşüşünü önlemek için, minimum (Xms) ve maksimum (Xmx) boyut değerlerinin aynı olması gerekir.

4. Wazuh dizinleyici hizmetini yeniden başlatın:

```
systemctl daemon-reload
systemctl restart wazuh-indexer
```

5. Ayarın başarıyla değiştirildiğini doğrulamak için aşağıdaki komutu çalıştırarak `mlockall` değerin şu şekilde ayarlandığını kontrol edin `true`:

```
curl -k -u <INDEXER_USERNAME>:<INDEXER_PASSWORD>
"https://<INDEXER_IP_ADDRESS>:9200/_nodes?filter_path=**.mlockall&pretty"
```

Output

```
{
  "nodes" : {
    "sRuGbIQRRfC54wzwIHjJWQ" : {
      "process" : {
        "mlockall" : true
      }
    }
  }
}
```

Çıktı ise `false`, istek başarısız olmuş ve dosyada aşağıdaki satır görünür `/var/log/wazuh-indexer/wazuh-indexer.log`:

```
Unable to lock JVM Memory
```

Parçalar ve Kopyalar

Wazuh dizinleyicisi, bir dizini shard adı verilen birden fazla parçaya bölme olanağı sunar. Her shard, Wazuh dizinleyici kümesindeki herhangi bir düğümde barındırılabilen tamamen işlevsel ve bağımsız bir "indekstir". Bölme iki ana nedenden dolayı önemlidir:

- Yatay ölçekleme.
- Parçalar arası dağıtım ve paralelleştirme işlemleri, performans ve verimi artırır.

Ayrıca, Wazuh dizinleyicisi kullanıcıların dizin parçacıklarının bir veya daha fazla kopyasını, kısaca replikalar veya replikalar olarak adlandırılan şekilde oluşturmasına olanak tanır. Replikasyon iki nedenden dolayı önemlidir:

- Bir parçanın veya düğümün arızalanması durumunda yüksek erişilebilirlik sağlar.
- Aramalar tüm replikalarda paralel olarak yürütülebildiğinden arama hacminin ve veriminin ölçeklenmesine olanak tanır.

Bir Index İçin Parça Sayısı

İlk dizini oluşturmadan önce, kaç tane parçaya ihtiyaç duyulacağını dikkatlice düşünün. Parça sayısını yeniden dizinlemeden değiştirmek mümkün değildir.

Optimum performans için gereken parça sayısı, Wazuh dizinleyici kümesindeki düğüm sayısına bağlıdır. Genel bir kural olarak, parça sayısı düğüm sayısıyla aynı olmalıdır. Örneğin, üç düğümü olan bir kümenin üç parçası olmalı, yalnızca bir düğümü olan bir kümenin ise yalnızca bir parçaya ihtiyacı olacaktır.

Bir Index İçin Kopya Sayısı

Kopyaların sayısı, dizinler için kullanılabilir depolama alanına bağlıdır. İşte üç düğüm ve üç parçadan oluşan bir Wazuh dizinleyici kümesinin nasıl kurulabileceğine dair bir örnek.

- **Kopya yok** : Her düğümün bir parçası vardır. Bir düğüm çökerse, yalnızca iki parçadan oluşan eksik bir dizin kullanılabilir.
- **Bir kopya** : Her düğümün bir parçası ve bir kopyası vardır. Bir düğüm çökerse, tam bir dizin hala kullanılabilir.
- **İki replika** : Her düğümün bir parça ve iki replika ile tam dizini vardır. Bu kurulumla, iki düğüm çökse bile küme çalışmaya devam eder. Bu en iyi çözüm gibi görünse de depolama gereksinimlerini artırır.

Aşağıdaki görüntü, her biri birincil parça ve iki kopya parça içeren üç düğümden oluşan bir Wazuh dizinleyici kümesini göstermektedir.



Parçalar ve kopyalar diyagramıyla Wazuh dizinleyici kümesi

Parça Sayısını Ayarlama

> Uyarı: Parça ve replika sayısı, dizin oluşturma sırasında dizin başına tanımlanır. Dizin oluşturulduktan sonra, replika sayısı dinamik olarak değiştirilebilse de, parça sayısı yeniden dizinleme yapılmadan değiştirilemez .

Wazuh dizinleyici düğümünün varsayılan kurulumu her dizini üç birincil parça ve hiçbir kopya olmadan oluşturur. Wazuh API'sini kullanarak yeni bir şablon yükleyerek birincil parça ve kopya sayısını değiştirebilirsiniz.

Aşağıdaki örnekte, tek düğümlü bir Wazuh dizinleyicisi için parçacık sayısını 1 olarak ayarladık. Wazuh API'sini kullanarak kimlik doğrulaması yapmasına izin verilen Wazuh dizinleyici düğümünde veya herhangi bir merkezi bileşende aşağıdaki adımları uygulayın.

1. Wazuh indeksleyici şablonunu indirin:

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

2. `index.number_of_shards` öğesini `1` olarak ayarlamak için `w-indexer-template.json` dosyasını düzenleyin. Filebeat'in mevcut şablonun üzerine yazmasını önlemek için sırayı 1 olarak ayarlayın. Aynı sırada birden fazla eşleşen şablon, deterministik olmayan bir birleştirme sırasına neden olur.

```
{
  "order": 1,
  "index_patterns": [
    "wazuh-alerts-4.x-*",
    "wazuh-archives-4.x-*"
  ],
  "settings": {
    "index.refresh_interval": "5s",
    "index.number_of_shards": "1",
    "index.number_of_replicas": "0",
    "index.auto_expand_replicas": "0-1",
    "index.mapping.total_fields.limit": 10000,
    ...
```

3. Yeni ayarları yükleyin.

```
curl -X PUT "https://<INDEXER_IP_ADDRESS>:9200/_template/wazuh-custom" -H 'Content-Type: application/json' -d @w-indexer-template.json -k -u <INDEXER_USERNAME>:<INDEXER_PASSWORD>
```

Output

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

4. Yapılandırmanın başarıyla güncellendiğini onaylayın.

```
curl "https://<INDEXER_IP_ADDRESS>:9200/_template/wazuh-custom?pretty&filter_path=wazuh-custom.settings" -k -u <INDEXER_USERNAME>:<INDEXER_PASSWORD>
```

Output

```
{
  "wazuh-custom" : {
    "settings" : {
      "index" : {
        "mapping" : {
          "total_fields" : {
            "limit" : "10000"
```

```
      }
    },
    "refresh_interval" : "5s",
    "number_of_shards" : "1",
    "auto_expand_replicas" : "0-1",
    "number_of_replicas" : "0",
    ...
```

Eğer indeks daha önceden oluşturulmuşsa yeniden indekslenmesi gerekir .

Kopyaların Sayısını Ayarlama

Kopya sayısı, Wazuh dizinleyici API'si kullanılarak dinamik olarak değiştirilebilir. Tek düğümlü bir kümede, kopya sayısı sıfıra ayarlanmalıdır. Bu, Wazuh dizinleyici düğümünde veya Wazuh API'si kullanılarak kimlik doğrulaması yapılmasına izin verilen herhangi bir merkezi bileşende aşağıdaki komutu çalıştırarak gerçekleştirilir:

```
curl -k -u "<INDEXER_USERNAME>:<INDEXER_PASSWORD>" -XPUT "https://<INDEXER_IP_ADDRESS>:9200/wazuh
{
  "settings": {
    "index": {
      "number_of_replicas": 0
    }
  }
}'
```

Parça Tahsis Farkındalığını veya Zorunlu Farkındalığı Yapılandırın

Bu, Wazuh indeksleyici düğümlerinin coğrafi olarak dağınık bölgelere yayıldığı durumlarda en çok uygulanabilir.

Farkındalığı yapılandırmak için, `/etc/wazuh-indexer/opensearch.yml`farklı bölgeler için Wazuh dizinleyici düğümlerindeki dosyaya bölge niteliklerini ekleyin.

`/etc/wazuh-indexer/opensearch.yml`Örneğin: A ve B bölgesi adında iki bölgeniz var. Aşağıdaki yapılandırmayı sırasıyla A ve B bölgesindeki her Wazuh dizinleyici düğümüne dosyaya ekleyeceksiniz :

```
node.attr.zone: zoneA
```

```
node.attr.zone: zoneB
```

Tahsis farkındalığı, A ve B bölgesindeki Wazuh dizinleyici düğümlerindeki depolama %50'den az kullanılıyorsa en iyi şekilde kullanılır. Bu, bölgedeki replikaları tahsis etmek için yeterli depolama kapasitesi sağlar.

Hem A hem de B bölgesindeki Wazuh dizinleyici düğümlerinin tüm birincil ve kopya parçacıklarını depolamak için yeterli kapasitesi yoksa, zorunlu farkındalık bir seçenektir. Bu, bir bölge arızası olması durumunda Wazuh dizinleyicisinin kalan bölgenizi aşırı yüklememesini ve kümenizin depolama yetersizliği nedeniyle kilitlenmesini önler.

Tahsis farkındalığı veya zorunlu farkındalığı seçmek, birincil ve kopya parçalarınızı dengelemek için her bölgede ne kadar alanınız olduğuna bağlıdır.

Parça Tahsisi Farkındalığı

Parça tahsisi farkındalığı, birincil ve replika parçaları birden fazla bölgeye yaymaya çalışır. Bir replika parçayı birincil bölgesinden farklı bir bölgeye tahsis etmek için kullanılır.

Bir bölge içinde düğüm arızası durumunda, replika parçalarınızın kalan bölgeleriniz arasında dağıtıldığından emin olabilirsiniz. Bu, hata toleransını artırarak verilerinizi bölge arızalarına ve bireysel düğüm arızalarına karşı korur.

Parça tahsis farkındalığını yapılandırmak için küme ayarlarını güncelleyin:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.routing.allocation.awareness.attributes": "zone"
  }
}
```

`persistent`ya da ayarlarını kullanabilirsiniz `transient`. Ayarı kullanmanızı öneririz `persistent`çünkü küme yeniden başlatma sırasında kalıcıdır. `transient`Ayar küme yeniden başlatma sırasında kalıcı değildir.

> Not: Yalnızca bir bölge mevcutsa (örneğin bölge arızalarından sonra), Wazuh dizinleyicisi çoğaltma parçalarını yalnızca kalan bölgeye tahsis eder.

Zorla Farkındalık

Zorunlu farkındalığın kullanılması, birincil ve kopya parçaların asla aynı bölgeye tahsis edilmediği anlamına gelir.

Zorunlu farkındalığı yapılandırmak için bölge nitelikleriniz için tüm olası değerleri belirtin:

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.routing.allocation.awareness.attributes": "zone",
    "cluster.routing.allocation.awareness.force.zone.values":["zoneA", "zoneB"]
  }
}
```

Başka bölgeler varsa, diğer bölgeleri `cluster.routing.allocation.awareness.force.zone.values` alanına ekleyin .

> Uyarı: Bir düğüm başarısız olursa, zorunlu farkındalık replikaları aynı bölgedeki başka bir düğüme tahsis etmez. Bunun yerine, küme sarı bir duruma girer ve yalnızca diğer bölgedeki(bölgelerdeki) düğümler çevrimiçi olduğunda replikaları tahsis eder.

Tahsis Filtreleme

Bu, bir düğümün parça tahsisinden hariç tutulmasına olanak tanır. Yaygın bir kullanım durumu, bir bölge içindeki bir düğümü devre dışı bırakmak istediğiniz zamandır.

Bir düğümü devre dışı bırakmadan önce parçaları taşımak için, düğümü IP adresini kullanarak hariç tutan bir filtre oluşturun. Bu, kapatılmadan önce o düğüme tahsis edilen tüm parçaları taşıyacaktır. Ayrıca, `*`bir IP aralığında devre dışı bırakılacak birden fazla düğümün olduğu bir durumda joker karakter kullanabilirsiniz.

```
PUT _cluster/settings
{
  "persistent": {
    "cluster.routing.allocation.exclude._ip": "192.168.0.*"
  }
}
```

Bir Kümedeki Her Düğüm İçin Düğüm Niteliklerini Ayarlayın

Varsayılan olarak, her Wazuh dizinleyici düğümü bir ana uygun, veri, alım ve koordinasyon düğümüdür. Düğüm sayısına karar vermek, düğüm türlerini atamak ve her düğüm türü için donanımı seçmek kullanım durumunuza bağlıdır.

Küme Yöneticisi Düğümleri

Küme yöneticisi düğümleri, düğümlere parça ekleme, kaldırma ve tahsis etme, ayrıca dizin ve alan oluşturma ve silme dahil olmak üzere küme genelindeki tüm yapılandırmaları ve değişiklikleri yönetir.

Dağıtılmış bir fikir birliği tekniği, küme yöneticisi uygun düğümleri arasından tek bir küme yöneticisi düğümü seçmek için kullanılır. Bu küme yöneticisi düğümü, mevcut düğüm başarısız olursa yeniden seçilir.

Varsayılan olarak zaten yapılmış olsa da, bir Wazuh dizinleyici düğümünün küme yöneticisi düğümü olduğunu belirtebilirsiniz.

`cluster_manager`Aşağıdaki yapılandırmayı dosyaya ekleyerek bir Wazuh dizinleyici düğümü rolü ayarlayın `/etc/wazuh-indexer/opensearch.yml`:

```
node.roles: [ cluster_manager ]
```

Veri Düğümleri

Veri düğümü, verileri depolamak ve aramaktan sorumludur. Yerel parçalarda tüm veriyle ilgili işlemleri (indeksleme, arama, toplama) gerçekleştirir. Bunlar Wazuh dizinleyici kümenizin çalışan düğümleridir ve diğer tüm düğüm türlerinden daha fazla disk alanına ihtiyaç duyarlar.

Aşağıdaki yapılandırmayı dosyaya ekleyerek bir Wazuh dizinleyici düğümü rolünü veri düğümü olarak ayarlayın `/etc/wazuh-indexer/opensearch.yml`:

```
node.roles: [ data, ingest ]
```

Veri düğümleri eklerken bunları bölgeler arasında dengeli tutmak önemlidir. Örneğin, üç bölgeniz varsa, her bölge için bir veri düğümü ekleyin. Depolama ve RAM ağırlıklı düğümler kullanmanızı öneririz.

Koordinasyon Düğümleri

Koordinasyon düğümü, istemci isteklerini veri düğümlerindeki parçalara devreder, sonuçları toplar ve tek bir nihai sonuçta birleştirir ve bunu Wazuh panosuna geri gönderir.

Her düğüm varsayılan olarak bir koordinasyon düğümüdür, ancak bir düğümü özel bir koordinasyon düğümü yapmak için `node.roles`boş bir liste ayarlayın:

```
node.roles: []
```

Wazuh Endekslerinin Taşınması

Bu bölümde, anlık görüntüleri kullanarak Wazuh dizinlerini taşımaya odaklanıyoruz. Bu, orijinal zaman damgasını kaybetmeden uyarıları bir Wazuh dizinleyici kümesinden diğerine geri yüklemeye yardımcı olur.

Paylaşımlı Dosya Sistemini Kurun

Anlık görüntü deposu için paylaşımlı bir dosya sistemi oluşturmak amacıyla bir Ağ Dosya Sistemi (NFS) kullanılmasını öneririz.

NFS Sunucusu

Adanmış bir sunucuda NFS'yi kurmak için aşağıdaki adımları uygulayın:

1. Anlık görüntü deposu için şu dizinde bir hedef `/mnt` dizinİ oluşturun :

   ```
   mkdir /mnt/snapshots
   ```

2. Aşağıdaki komutları çalıştırarak NFS'yi yükleyin:

   Yum

   ```
   yum update
   yum install -y nfs-utils
   yum install exportfs
   systemctl enable nfs-server
   systemctl start nfs-server
   ```

   APT

   ```
   apt -y install nfs-kernel-server
   systemctl start nfs-kernel-server.service
   ```

3. Aşağıdaki komutu kullanarak `/mnt/snapshots` dizinini `/etc/exports` dosyasına ekleyin. `<NETWORK_ADDRESS/CIDR>` değişkenini ağ adresinizle değiştirin.

```
echo "/mnt/snapshots     <NETWORK_ADDRESS/CIDR>(rw,sync,no_root_squash,no_subtree_check)" |
sudo tee -a /etc/exports
```

   Nerede:
   - `rw`- Paylaşılan dizine hem okuma hem de yazma erişimi sağlar.
   - `sync`- NFS sunucusunun değişiklikleri hemen diske yazmasını zorlar ve dosya sistemini senkron hale getirir.
   - `no_root_squash`- NFS istemci sistemindeki "root" kullanıcısının NFS sunucusundaki dosyalara tam ve kısıtlanmamış erişime sahip olmasını sağlar.
   - `no_subtree_check`- Büyük dizin ağaçları için performansı artırabilen alt ağaç denetimini devre dışı bırakır.

4. NFS yapılandırmasını uygulayın:

```
exportfs -a
```

Wazuh Indexer

Paylaşımlı dosya sistemi kurulumunu tamamlamak için Wazuh dizinleyici düğümünde (düğümlerinde) aşağıdaki adımları gerçekleştirin.

1. Anlık görüntü deposu için şu dizinde bir hedef `/mnt` dizin oluşturun :

```
mkdir /mnt/snapshots
```

2. NFS istemcisini yükleyin:

   Yum

```
yum -y install nfs-utils
```

   APT

```
apt -y install nfs-common
```

3. Paylaşılan dizini `/mnt/snapshots`Wazuh dizinleyici düğümüne(düğümlerine) bağlayın. `<NFS_SERVER_IP>`

Değişkeni NFS sunucusunun IP adresiyle değiştirin:

```
mount -t nfs <NFS_SERVER_IP>:/mnt/snapshots /mnt/snapshots
```

4. `wazuh-indexer`Kullanıcıya dizinin sahipliğini verin `/mnt/snapshots`:

```
chown wazuh-indexer:wazuh-indexer /mnt/snapshots
```

5. Yapılandırmayı ekleyin: `path.repo:/mnt/snapshots` depo yolunu belirtmek için `/etc/wazuh-indexer/opensearch.yml` dosyasına:

```
network.host: "127.0.0.1"
node.name: "node-1"
cluster.initial_master_nodes:
- "node-1"
cluster.name: "wazuh-cluster"

node.max_local_storage_nodes: "3"
path.data: /var/lib/wazuh-indexer
path.logs: /var/log/wazuh-indexer
path.repo: /mnt/snapshots

plugins.security.ssl.http.pemcert_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.http.pemkey_filepath: /etc/wazuh-indexer/certs/wazuh-indexer-key.pem
plugins.security.ssl.http.pemtrustedcas_filepath: /etc/wazuh-indexer/certs/root-ca.pem
plugins.security.ssl.transport.pemcert_filepath: /etc/wazuh-indexer/certs/wazuh-indexer.pem
plugins.security.ssl.transport.pemkey_filepath: /etc/wazuh-indexer/certs/wazuh-indexer-key.>plugins.security
plugins.security.ssl.http.enabled: true
plugins.security.ssl.transport.enforce_hostname_verification: false
plugins.security.ssl.transport.resolve_hostname: false
plugins.security.ssl.http.enabled_ciphers:
  - "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256"
  - "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384"
  - "TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256"
  - "TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384"
plugins.security.ssl.http.enabled_protocols:
  - "TLSv1.2"
plugins.security.authcz.admin_dn:
- "CN=admin,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.check_snapshot_restore_write_privileges: true
plugins.security.enable_snapshot_restore_privilege: true
plugins.security.nodes_dn:
- "CN=indexer,OU=Wazuh,O=Wazuh,L=California,C=US"
plugins.security.restapi.roles_enabled:
- "all_access"
- "security_rest_api_access"
```

```
plugins.security.system_indices.enabled: true
plugins.security.system_indices.indices: [".opendistro-alerting-config", ".opendistro-alert>
### Option to allow Filebeat-oss 7.10.2 to work ###
compatibility.override_main_response_version: true
```

6. Yapılandırma değişikliklerini uygulamak için Wazuh dizinleyicisini yeniden başlatın:

```
systemctl restart wazuh-indexer
```

Uyarı: `ll` yardımcı programını kullanarak `/mnt/snapshots` dizininin Wazuh dizinleyici düğümlerinde `wazuh-indexer:wazuh-indexer` sahipliğine sahip olduğunu doğruladığınızdan emin olun.

NFS paylaşım dizini `/mnt/snapshots`'ı anlık görüntü deposu olarak kullanmak için hedef Wazuh dizinleyici(ler)de Paylaşılan dosya sistemini kur > Wazuh dizinleyici adımlarını tekrarlayın.

Anlık Görüntü Deposunu Kurun

Wazuh kontrol panelinde aşağıdaki adımları uygulayın:

1. **Sol üst menüye** ☰ tıklayın , **Indexer yönetimi** > **Anlık Görüntü Yönetimi** > **Depolar'a** gidin ve yeni bir anlık görüntü deposu oluşturmak için **Depo oluştur'u seçin.**
2. Bir depo adı girin, depo türünü **Paylaşılan dosya sistemi** olarak seçin , depo konumunu girin `/mnt/snapshots`ve yeni deponun kaydını yapmak için **Ekle'yi seçin.**



Anlık görüntü deposu oluştur

Benzer bir anlık görüntü deposu kurmak için yukarıdaki adımları hedef Wazuh kümesinde tekrarlayın.

Anlık Görüntüler Alın

1. **Sol üst menüye** ☰ tıklayın ve **Indexer yönetimi** > **Anlık Görüntü Yönetimi** > **Anlık Görüntüler** bölümüne gidin .
2. **Anlık görüntü al'ı** seçin ve bir Anlık Görüntü adı girin.
3. Kaynak dizin desenlerini seçin veya girin.
4. Anlık görüntüleri depolamak için daha önce oluşturulan depoları seçin.
5. **Gelişmiş seçenekleri** seçin ve **Anlık görüntülere küme durumunu dahil et** seçeneğini işaretleyin.



Anlık görüntülere küme durumunu dahil et seçeneği

6. Yeni bir anlık görüntü oluşturmak için **Ekle'yi** seçin .

Anlık görüntü dosyaları `/mnt/snapshots` depolama konumuna kaydedilir .

Anlık görüntü dosyası kaydedildi



Anlık Görüntüleri Geri Yükle

Wazuh dizin geçiş adımlarını tamamlamak için eski Wazuh dizinleyicilerinden alınan anlık görüntüleri hedef Wazuh dizinleyicilerine geri yükleyin. Hedef Wazuh dizinleyicisinde aşağıdaki adımları gerçekleştirin.

Not

Anlık görüntüleri geri yükleme işlemine geçmeden önce hedef Wazuh kümesinde Paylaşımlı dosya sistemini kur ve Anlık görüntü deposunu kur bölümlerindeki adımların gerçekleştirilmesi gerekir .

1. Anlık görüntü dosyalarını yüklemek için hedef Wazuh kümesindeki Wazuh dizinleyici düğümlerini şu komutu kullanarak yeniden başlatın:

   ```
   systemctl restart wazuh-indexer
   ```

2. **Sol üst menüye** ☰ tıklayın , **Indexer yönetimi** > **Anlık Görüntü Yönetimi** > **Anlık Görüntüler'e** gidin ve Anlık Görüntüler sayfasını yenileyin. Depo konumundaki anlık görüntüler `/mnt/snapshots`hedef Wazuh kümesinin panosunda gösterilecektir.
3. Anlık görüntüyü seçin ve **Geri Yükle'ye**`restored_` tıklayın. Dizinleri orijinal adlarına geri yüklemek için öneki silin . `restored_`Önek, çakışan dizin adlarını önlemek için vardır.
4. **Gelişmiş seçenekleri** seçin ve tüm seçeneklerin işaretli olmadığından emin olun.

   Anlık görüntü gelismis seçeneklerini geri yükle

5. Göç sürecini tamamlamak için **Anlık görüntüyü geri yükle'yi** seçin.

   Anlık görüntüyü geri yükle