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.



Revision #2
Created 31 December 2024 18:02:44 by Ayşegül Sarıkaya
Updated 31 December 2024 20:50:13 by Ayşegül Sarıkaya