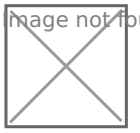
Microsoft Azure Günlük Analizi

Microsoft Azure Log Analytics, Microsoft Azure altyapınızı izleyen ve verilerinize özel gelişmiş aramalar yapmanıza olanak tanıyan sorgu yetenekleri sunan bir hizmettir.

Azure Log Analytics çözümü, tüm Azure aboneliklerinizdeki Azure etkinlik günlüklerini analiz etmenize ve aramanıza yardımcı olur ve aboneliklerinizin kaynaklarıyla gerçekleştirilen işlemler hakkında bilgi sağlar.



Microsoft Entra ID kimlik doğrulama şemasını kullanan Azure Log Analytics REST API'sini kullanarak Log Analytics tarafından toplanan verileri sorgulayabilirsiniz. Azure Log Analytics REST API'sini kullanmak için nitelikli bir uygulamaya veya istemciye ihtiyacınız vardır. Bunu Microsoft Azure portalında manuel olarak yapılandırmanız gerekir. Aşağıdaki bölüm uygulamanın nasıl kurulacağını gösterir ve bir kullanım örneği verir:

- Uygulamanın kurulumu
- Azure Log Analytics kullanım örneği

Yapılandırma

Azure

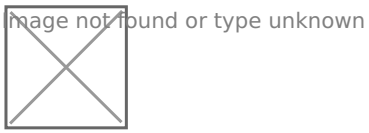
Uygulamanın kurulumu

Aşağıdaki işlem Azure Log Analytics REST API'sini kullanarak bir uygulama oluşturmayı ayrıntılı olarak açıklamaktadır. Mevcut bir uygulamayı yapılandırmak da mümkündür. Zaten mevcut bir uygulamanız varsa lütfen Uygulama oluşturma adımını atlayın.

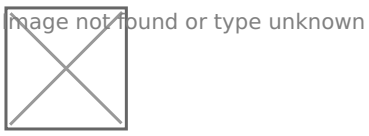
Uygulamanın oluşturulması

Azure Log Analytics için yeni bir uygulama oluşturmak üzere Microsoft Azure portalındaki Microsoft Entra ID paneline gidiyoruz.

1. **Microsoft Entra ID** panelinden **Uygulama kayıtları** seçeneğini seçin . Ardından, **Yeni kayıt** seçeneğini seçin.

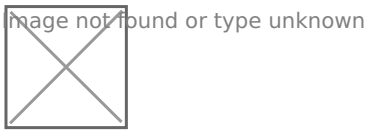


2. Uygulama için kullanıcıya dönük görüntü adını tanımlayın ve **Kaydet'i** seçin .

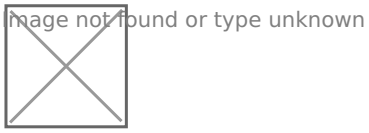


Uygulamaya İzinlerin Verilmesi

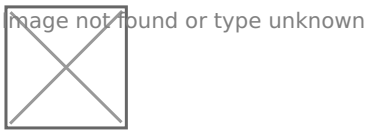
1. **Uygulama kaydından** Tüm **uygulamaları** seçin ve yenileyin. Yeni uygulama görünecektir. Bizim durumumuzda, görünen ad **LogAnalyticsApp'dir**.



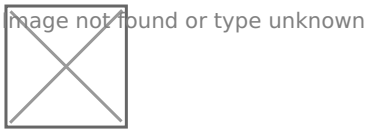
2. **Genel Bakış** bölümüne gidin ve **Uygulama (istemci) kimliğini** daha sonraki kimlik doğrulaması için kaydedin.



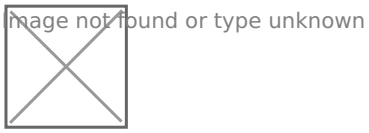
3. **API izinleri** bölümüne gidin ve uygulamaya **Data.Read** iznini ekleyin.



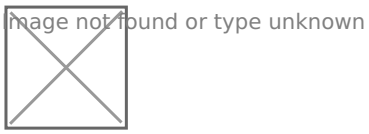
4. **Log Analytics API'yi** arayın .



5. Uygulamalar izinlerinden **Log Analytics verilerini oku iznini** seçin.

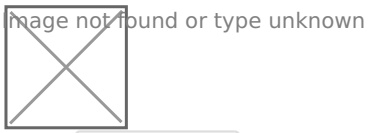


6. Kiracıya **yönetici onayı vermek** için bir yönetici kullanıcısı kullanın.

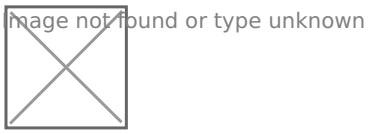


Uygulamaya Azure Log Analytics API'sine Erişim İzni Verme

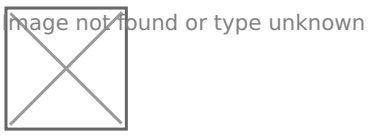
1. **Log Analytics çalışma alanlarına** erişin ve yeni bir çalışma alanı oluşturun veya mevcut bir çalışma alanını seçin.



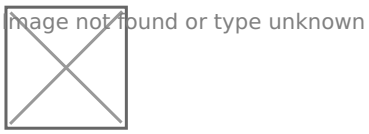
2. **Genel Bakış** bölümünden değeri kopyalayın .Workspace ID



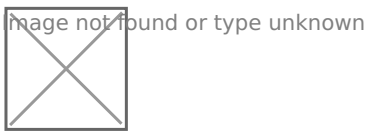
3. **Erişim denetimi (IAM)** bölümüne gidin , **Ekle'ye** tıklayın ve uygulamaya gerekli rolü eklemek için **Rol ataması ekle'yi** seçin .



4. **İş fonksiyonları rol sekmesinden Log Analytics Okuyucu** rolünü seçin.



5. **Üyeler** sekmesinden **Kullanıcı, grup veya hizmet sorumlusunu** seçin . **Üyeleri seç'e** tıklayın ve daha önce oluşturulan Uygulama kaydını bulun.

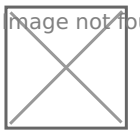


6. Bitirmek için **Gözden Geçir + Ata'ya** tıklayın .

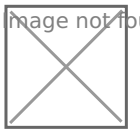
Günlükleri Çalışma Alanına gönderme

Önceki adımlarda oluşturulan Azure Log Analytics Çalışma Alanına günlükleri toplamak ve göndermek için bir tanılama ayarı oluşturmanız gerekir.

1. **Microsoft Entra ID'ye** geri dönün , sol menü çubuğunu aşağı kaydırın ve **Tanılama ayarları** bölümünü seçin.
2. **Tanılama ayarı ekle'ye** tıklayın.



3. **Kategoriler** altında toplamak istediğiniz günlük kategorilerini seçin . **Hedef ayrıntıları** altında **Log Analytics çalışma alanına gönder** seçeneğini işaretleyin. Önceki adımlarda oluşturduğunuz **Log Analytics Çalışma Alanını** seçin .



4. **Kaydet'e** tıklayın .

Azure Log Analytics, seçili kategorileri çalışma alanınıza aktaracaktır.

Wazuh, Azure Log Analytics'ten günlükleri çekmek için geçerli kimlik bilgileri gerektirir. Uygulama kaydına erişmek için bir istemci sırrının nasıl oluşturulacağını öğrenmek için kimlik bilgileri bölümüne bakın.

Wazuh Sunucusu veya Aracısı

Azure Log Analytics'inize erişmek için Wazuh modülünü Azure için yetkilendirmeniz gerekir. Yetkilendirmeyi ayarlama hakkında daha fazla bilgi için Azure kimlik bilgilerini yapılandırma bölümüne bakın.

1. `/var/ossec/etc/ossec.conf`Aşağıdaki yapılandırmayı Wazuh sunucusunun veya aracısının yerel yapılandırma dosyasına uygulayın . Bu, Wazuh modülünü Azure için nerede yapılandırdığınıza bağlı olacaktır:

```
<wodle name="azure-logs">
  <disabled>no</disabled>
  <run_on_start>no</run_on_start>

  <log_analytics>
    <auth_path>/var/ossec/wodles/credentials/log_analytics_credentials</auth_path>
    <tenantdomain>wazuh.com</tenantdomain>

    <request>
      <tag>azure-auditlogs</tag>
      <query>AuditLogs</query>
      <workspace>d6b...efa</workspace>
      <time_offset>1d</time_offset>
    </request>

  </log_analytics>
</wodle>
```

   Nerede:

- `<auth_path>`çalışma alanı gizli anahtarının saklandığı tam yoldur.
- `<tenantdomain>`kiracı etki alanı adıdır. Bunu Microsoft Entra ID'deki Genel Bakış bölümünden edinebilirsiniz.
- `<workspace>`kimlik doğrulaması için ihtiyaç duyduğunuz çalışma alanı kimliğidir.
- `<time_offset>`geriye doğru tarihlenen zaman dilimidir. Bu durumda, 24 saatlik bir zaman dilimi içindeki tüm günlükler indirilecektir.

2. Azure için Wazuh modülünü nerede yapılandırdığınıza bağlı olarak Wazuh sunucunuzu veya aracınızı yeniden başlatın.

   Wazuh temsilcisi:

   ```
   systemctl restart wazuh-agent
   ```

   Wazuh sunucusu:

   ```
   systemctl restart wazuh-manager
   ```

yukarıdaki yapılandırma, Wazuh'un tanımlayıcı olarak `tag` değeri kullanarak herhangi bir sorguyu aramasına olanak tanır .

Azure için Wazuh modülü hakkında daha fazla bilgi için referansı inceleyin .

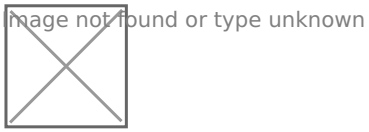
Use Case

Daha önce oluşturulmuş Azure uygulamasını kullanarak altyapı etkinliğinin izlenmesine dair bir örnek aşağıda verilmiştir.

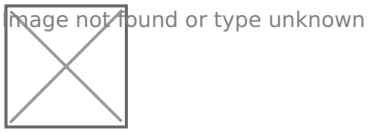
Bir Kullanıcı Oluşturma

Microsoft Entra ID'de kullanıcı oluşturmak için aşağıda belirtilen adımları izleyin:

1. **Entra ID'ye** gidin ve **Tüm kullanıcılar'ı** seçin.
2. **Yeni Kullanıcı'ya** tıklayın.

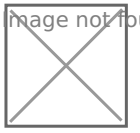


3. **Yeni kullanıcı oluştur** seçeneğini seçin.



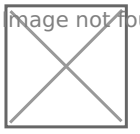
4. Oluşturmak istediğiniz kullanıcı için gerekli bilgileri girin ve ardından **Oluştur** seçeneğini

seçerek oluşturma işlemini tamamlayın.



Wazuh Dashboard Olayların Görselleştirilmesi

Kurulum tamamlandıktan sonra sonuçları Wazuh kontrol panelinden kontrol edebilirsiniz.



Revision #2
Created 31 December 2024 18:48:24 by Ayşegül Sarıkaya
Updated 31 December 2024 19:15:17 by Ayşegül Sarıkaya