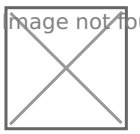
Microsoft Azure Depolama

Microsoft Azure Storage, Microsoft Azure bulut depolama çözümünü ifade eder. Bu hizmet, veri nesneleri için büyük ölçüde ölçeklenebilir bir nesne deposu, güvenilir mesajlaşma için bir mesajlaşma deposu, bulut için bir dosya sistemi hizmeti ve bir NoSQL deposu sağlar.



Azure Log Analytics REST API'sine alternatif olarak Wazuh, bir Microsoft Azure Depolama hesabına erişim sunar. Microsoft Azure altyapısının etkinlik günlüklerini depolama hesaplarına aktarabilirsiniz.

Bu bölümde, Microsoft Azure etkinlik günlüklerinizi bir depolama hesabında arşivlemek için Azure portalının nasıl kullanılacağı açıklanmaktadır.

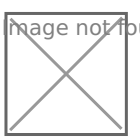
Yapılandırma

Azure

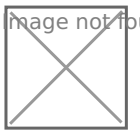
Etkinlik Günlüğü Dışa Aktarımını Yapılandırma

1. **Microsoft Entra ID** içerisindeki **İzleme bölümünden Denetim Günlükleri** seçeneğini seçin ve **Veri Ayarlarını Dışa Aktar'a** tıklayın.

2. **Tanılama ayarı ekle'ye** tıklayın.

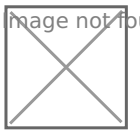


3. **Denetim Günlükleri'ni** seçin ve **Depolama hesabına arşivleyin** onay kutusunu seçin , ardından açılır menüden günlükleri dışa aktarmak istediğiniz aboneliği ve Depolama hesabını seçin.



Wazuh Sunucusu veya Agent

`account_name`Depolama hesabının ve'sini kimlik doğrulaması için ayarlamak önemlidir `account_key`. Aşağıdaki görüntü önceden yapılandırılmış bir depolama hesabını gösterir.



Microsoft Azure Depolama kimlik bilgilerini yapılandırma konusunda rehberlik için kimlik bilgileri bölümünü kontrol edin .

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>
    <interval>1d</interval>
    <run_on_start>yes</run_on_start>

    <storage>

        <auth_path>/home/manager/Azure/storage_auth.txt</auth_path>
        <tag>azure-activity</tag>

        <container name="insights-activity-logs">
            <blobs>.json</blobs>
            <content_type>json_inline</content_type>
            <time_offset>24h</time_offset>
            <path>info-logs</path>
        </container>

    </storage>
</wodle>
```

Nerede

- `<auth_path>`çalışma alanı gizli anahtarının saklandığı tam yoldur.
- `<container>`blog depolama içeriklerini getirirken yararlı parametreler içerir.
- `<container name="insights-activity-logs">`Akışı yapılacak günlük kabı.
- `<blobs>.json</blobs>`indirilecek blob formatıdır.
- `<time_offset>`geriye doğru tarihlenen zaman dilimidir. Bu durumda, 24 saatlik bir zaman dilimi içindeki tüm günlükler indirilecektir.

- `<content_type>`blob'ların içeriğinin depolanması için kullanılan formattır.

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
   ```

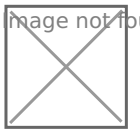
Kullanım Durumu

Yukarıdaki yapılandırmayı kullanarak Microsoft Entra ID etkinlik izleme örneğini aşağıda bulabilirsiniz.

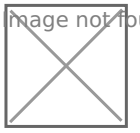
Yeni Bir Kullanıcı Oluştur

Microsoft Entra ID kullanarak Microsoft Azure ortamınızda yeni bir kullanıcı oluşturun. Kullanıcıyı oluşturduktan birkaç dakika sonra, `insights-activity-logs`Activity log export'u yapılandırılırken belirtilen Storage hesabının içinde adlandırılan bir kapsayıcıda yeni bir günlük kullanılabilir olacaktır.

Lütfen Azure Log Analytics kullanım örneği altında kullanıcı oluşturma bölümüne bakın .



Sonuçları Wazuh panelinden kontrol edebilirsiniz.



Revision #1
Created 31 December 2024 19:23:45 by Ayşegül Sarıkaya
Updated 31 December 2024 19:29:52 by Ayşegül Sarıkaya