Azure Platformunu ve Hizmetlerini İzleme

Azure Monitor Logs, Azure hizmetleri, sanal makineler ve uygulamalar dahil olmak üzere izlenen kaynaklardan günlükleri ve performans verilerini toplar ve düzenler. Bu içgörü, Azure Log Analytics REST API'sini kullanarak veya doğrudan bir Microsoft Azure Storage hesabının içeriklerine erişerek Wazuh'a gönderilir. Azure için Wazuh modülü, Wazuh dağıtımınızdan Microsoft Azure ortamlarınızın merkezi günlük kaydını, tehdit algılamasını ve uyumluluk yönetimini sağlar.

Azure için Wazuh modülü, Microsoft Azure günlüklerinize erişmek için bağımlılıklar ve kimlik bilgileri gerektirir. Bu bağımlılıklar varsayılan olarak Wazuh yöneticisinde mevcuttur, ancak entegrasyon için bir Wazuh aracısı kullandığınızda bunları yüklemeniz gerekir. Devam etmeden önce Önkoşullar bölümüne bir göz atın.

Ön koşullar

Bağımlılıkları Yükleme

Wazuh modülünü Azure için Wazuh yöneticisinde veya bir Wazuh aracısında yapılandırabilirsiniz. Bu seçim tamamen ortamınızda Azure altyapınıza nasıl eriştiğinize bağlıdır.

Azure ile entegrasyonu bir Wazuh aracısında yapılandırırken yalnızca bağımlılıkları yüklemeniz gerekir. Wazuh yöneticisi zaten gerekli tüm bağımlılıkları içerir.

Python

Azure için Wazuh modülü Python 3.8–3.12 ile uyumludur. Daha sonraki Python sürümleri de çalışmalı ancak uyumlu olduklarını garanti edemeyiz. Python 3 zaten yüklü değilse, izlenen uç noktanızda aşağıdaki komutu çalıştırın.

Yum

```
yum update && yum install python3
```

APT

```
apt-get update && apt-get install python3
```

Gerekli modülleri Python paket yöneticisi Pip ile kurabilirsiniz. Çoğu UNIX dağıtımının yazılım depolarında bu araç mevcuttur. Zaten kurulu değilse, uç noktanıza pip'i kurmak için aşağıdaki komutu çalıştırın.

Yum

```
yum update && yum install python3-pip
```

APT

```
apt-get update && apt-get install python3-pip
```

Bağımlılıkların kurulumunu kolaylaştırmak için Pip 19.3 veya üzerini kullanmanızı öneririz. Pip sürümünüzü kontrol etmek için bu komutu çalıştırın.

```
pip3 --version
```

Örnek çıktı aşağıdaki gibidir.

Output

```
pip 22.0.2 from /usr/lib/python3/dist-packages/pip (python 3.10)
```

Eğer pip versiyonunuz 19.3'ten düşükse, versiyonu yükseltmek için aşağıdaki komutu çalıştırın.

Python 3.8–3.10

```
pip3 install --upgrade pip
```

Python 3.11–3.12

```
pip3 install --upgrade pip --break-system-packages
```

> Not: Bu komut, varsayılan harici olarak yönetilen Python ortamını değiştirir. Daha fazla bilgi için PEP 668 açıklamasına bakın.
>
> Değişikliği önlemek için sanal bir ortamda çalışabilirsiniz . Python betiğinin shebang'ini

> sanal ortamınızdaki yorumlayıcıyla güncellemelisiniz . Örneğin, .`pip3 install --upgrade pip` `/var/ossec/wodles/azure/azure-logs#!/path/to/your/virtual/environment/bin/python3`

Python İçin Azure Storage İstemci Kitaplığı

Wazuh aracı uç noktanızı kurmak ve Microsoft Azure platformunuzu ve hizmetlerinizi izlemek için aşağıdaki komuttaki kütüphanelere ihtiyacınız var.

Python 3.8–3.10

```
pip3 install azure-storage-blob==12.20.0 azure-storage-common==2.1.0 azure-common==1.1.25 cryptography==3.3.2 cffi==1.14.4 pycparser==2.20 six==1.14.0 python-dateutil==2.8.1 requests==2.25.1 certifi==2022.12.07 chardet==3.0.4 idna==2.9 urllib3==1.26.18 SQLAlchemy==2.0.23 pytz==2020.1
```

Python 3.11–3.12

```
pip3 install --break-system-packages azure-storage-blob==12.20.0 azure-storage-common==2.1.0 azure-common==1.1.25 cryptography==3.3.2 cffi==1.14.4 pycparser==2.20 six==1.14.0 python-dateutil==2.8.1 requests==2.25.1 certifi==2022.12.07 chardet==3.0.4 idna==2.9 urllib3==1.26.18 SQLAlchemy==2.0.23 pytz==2020.1
```

> Not: Eğer sanal ortam kullanıyorsanız `--break-system-packages`yukarıdaki komuttan parametreyi kaldırın.

Azure Kimlik Bilgilerini Yapılandırma

Azure için Wazuh modülünün Azure'a başarılı bir şekilde bağlanabilmesi için erişim kimlik bilgilerine sahip olması gerekir. Gereken kimlik bilgileri izleme türüne göre değişir. Bunlar şunları içerir:

- Microsoft Graph ve Azure Log Analytics için erişim kimlik bilgileri
- Microsoft Azure Storage için erişim kimlik bilgileri

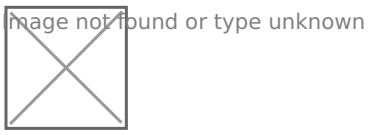
Aşağıdaki bölümlerde bu kimlik bilgilerini nasıl oluşturabileceğinize dair genel bir bakış sunulmaktadır.

Microsoft Graph ve Azure Log Analytics İçin Erişim Kimlik Bilgilerini Alma

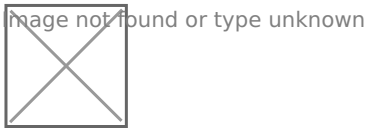
Azure için Wazuh modülünden gelen bağlantıyı doğrulamak için geçerli application_id ve application_key değerlerine ihtiyacınız var.

`application_id`ve elde etmek için aşağıdaki adımları izleyin `application_key`:

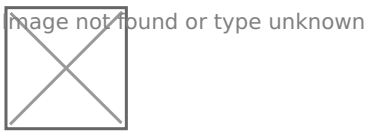
1. Microsoft Entra ID'ye gidin ve kayıtlı uygulamaya gidin.



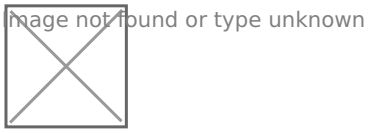
2. **Seçtiğiniz uygulamanın Sertifikalar ve sırlar** bölümüne gidin , ardından **Yeni istemci sırrı'nı** seçerek bir gizli anahtar oluşturun .



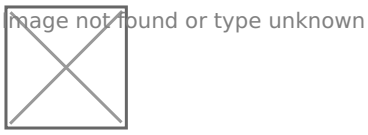
3. Anahtara açıklayıcı bir ad verin ve anahtarın etkin kalacağı süreyi belirtin, ardından **Ekle'yi** seçin.



4. `Value`ve 'yi kopyalayın . Bu değerleri güvenli bir şekilde sakladığınızdan emin olun, çünkü bunları yalnızca bir kez görüntüleyebilirsiniz. ' dir .`Secret ID``Value``application_key`



5. `application_id`Kayıtlı uygulamanızın değerini **Genel Bakış** bölümünden kopyalayın.



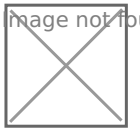
Microsoft Azure Storage İçin Erişim Kimlik Bilgilerini Alma

Microsoft Azure Storage geçerli `account_name`ve değerleri gerektirir. Bunları Azure ortamınızdaki **Storage hesaplarının Erişim anahtarları** bölümünden `account_key`edinebilirsiniz . Bir depolama hesabı oluşturmak için Microsoft kılavuzunu izleyin .

Aşağıdaki bölüm Microsoft Azure Depolama hesabı anahtarının alınmasına ilişkin adımları göstermektedir.

1. Microsoft Azure ortamınızın **Depolama hesapları** bölümüne gidin ve ilgilendiğiniz hesabı

seçin.



2. ve değerlerine erişmek için sol bölmede bulunan **Erişim tuşlarına** gidin .`account_name` `account_key`



Wazuh Azure Kimlik Doğrulama Dosyası

Microsoft Azure ortamınızı Wazuh'ta kimlik doğrulamak için kimlik bilgilerinizi biçimini kullanarak bir dosyada saklamanız gerekir .`field = value`

Kimlik bilgileri dosyasında bulunması beklenen alanlar, izlediğiniz hizmet veya etkinliğin türüne bağlıdır.

Microsoft Azure Log Analitiği ve Grafiği

Dosya sadece iki satırdan oluşmalıdır, biri için `application_id`, diğeri ise `application_key`daha önce elde edilenler için:

```
application_id = <YOUR_APPLICATION_ID>
application_key = <YOUR_APPLICATION_KEY>
```

Microsoft Azure Depolama

Dosya sadece iki satırdan oluşmalıdır, biri için `account_name`ve diğeri `account_key`daha önce elde edilen için:

```
account_name = <YOUR_ACCOUNT_NAME>
account_key = <YOUR_ACCOUNT_KEY>
```

İzlediğiniz hizmet veya etkinlikten bağımsız olarak, yapılandırma dosyasında kimlik doğrulama dosyasını etiketi `/var/ossec/etc/ossec.conf`kullanarak belirtin. Aşağıdaki örneğe bir göz atın:`<auth_path>`

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

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

```
    <request>
      <query>AzureActivity</query>
      <workspace>12345678-90ab-cdef-1234-567890abcdef</workspace>
      <time_offset>1d</time_offset>
    </request>
  </log_analytics>

  <graph>
    <auth_path>/var/ossec/wodles/credentials/graph_credentials</auth_path>
    <tenantdomain>wazuh.com</tenantdomain>
    <request>
      <query>auditLogs/directoryAudits</query>
      <time_offset>1d</time_offset>
    </request>
  </graph>

<storage>
    <auth_path>/var/ossec/wodles/credentials/storage_credentials</auth_path>
    <container name="insights-activity-logs">
      <blobs>.json</blobs>
      <content_type>json_inline</content_type>
      <time_offset>24h</time_offset>
    </container>
  </storage>
</wodle>
```

`request`Aynı yapılandırmada aynı anda birden fazla blok eklemek mümkündür. Azure için Wazuh modülü her isteği sırayla işler. Yukarıdaki yapılandırma bir örnektir. Microsoft Azure Log Analytics, Graph ve Storage yapılandırma bloklarını içerir.

Yeniden Çözümlemek

> Uyarı: Bu `reparse`seçenek başlangıç tarihinden bugüne kadar tüm günlükleri getirecek ve işleyecektir. Bu işlem yinelenen uyarılar üretebilir.

Daha eski Azure günlüklerini getirmek ve işlemek için, seçeneğini kullanarak Azure için Wazuh modülünü çalıştırmanız gerekir `--reparse`.
Değer `la_time_offset`, başlangıç noktası için bir ofset olarak zamanı ayarlar. Bir değer sağlamazsanız `la_time_offset`, Azure için Wazuh modülü ilk dosyayı işlediği tarihe döner.

Aşağıdaki kod bloğu, Wazuh yöneticisinde Azure için Wazuh modülünün şu `--reparse`seçenek kullanılarak çalıştırılmasına ilişkin bir örneği göstermektedir:

```
/var/ossec/wodles/azure/azure-logs --log_analytics --la_auth_path credentials_example --la_tenant_domain 'wazuh.example.domain' --la_tag azure-activity --la_query "AzureActivity" --workspace example-workspace --la_time_offset 50d --debug 2 --reparse
```

Parametre ayrıntılı bir çıktı alır. Bu çıktı, özellikle büyük miktarda veri işlenirken betiğin çalıştığını göstermek için yararlıdır.`--debug 2`

Revision #7
Created 30 December 2024 21:22:53 by Ayşegül Sarıkaya
Updated 30 December 2024 21:41:29 by Ayşegül Sarıkaya