Microsoft Azure'u Wazuh ile İzleme

Microsoft Azure, Microsoft'un bilgi işlem gücü, depolama seçenekleri ve ağ yetenekleri gibi çok çeşitli hizmetler sunan bir bulut bilişim platformudur. Sanal bilgi işlem, analiz, depolama ve ağ gibi çeşitli uygulamalar için çözümler sunar ve işletmelerin ve geliştiricilerin çeşitli ihtiyaçlarını karşılar. Bulut örneğinizi güvence altına almak, Microsoft Azure gibi bulut sağlayıcıları tarafından sunulan bulut hizmetlerini kullanan şirketler için önemli bir husustur. Açık kaynaklı bir güvenlik izleme platformu olan Wazuh, Microsoft Azure ortamlarında güvenlik ve çalışma zamanı olayları tarafından oluşturulan verileri toplamak ve analiz etmek için çözümler sunar. Wazuh'u Microsoft Azure ile entegre etmek, Azure dağıtımlarının güvenlik duruşunu iyileştirir ve düzenleyici standartlara ve operasyonel bütünlüğe uyumu sağlar.

- İzleme Örnekleri
- Azure Platformunu ve Hizmetlerini İzleme
- Microsoft Azure Günlük Analizi
- Microsoft Graph Servislerini Wazuh İle İzleme
- Microsoft Azure Depolama
- Microsoft Grafiği

İzleme Örnekleri

Wazuh aracısı platformlar arası uyumludur, yani Windows, Linux, Solaris, BSD ve macOS dahil olmak üzere çeşitli işletim sistemlerinde çalışabilir. Farklı sistemler ve uygulamalar hakkında veri toplar ve örneğin Dosya Bütünlüğü İzleme (FIM) ve Güvenlik Yapılandırma Değerlendirmesi (SCA) gibi diğer Wazuh yeteneklerinden yararlanmasını sağlar. Bu veriler şifrelenmiş ve kimliği doğrulanmış bir kanal aracılığıyla Wazuh sunucusuna gönderilir. Benzersiz önceden paylaşılmış anahtar kayıt işlemi bu güvenli kanalı oluşturur.

Microsoft Azure ortamınızdaki sanal makinelere Wazuh aracısını yükleyebilirsiniz. Wazuh aracısını kullanarak bulut sanal makinelerini izlemek faydalıdır çünkü kapsamlı güvenlik ve performans denetimi sağlayarak dinamik bulut ortamlarında olası tehditlerin ve operasyonel sorunların erken tespitini sağlar.

Wazuh aracıları hakkında daha fazla bilgi edinmek için Wazuh agent kurulum ve kayıt belgelerini inceleyin . Ayrıca, Wazuh SIEM ve XDR yetenekleri ve bunların yapılandırması hakkında yetenekler belgelerimizde okuyun.

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

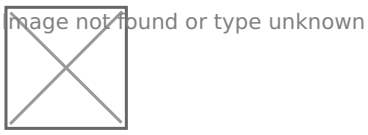
Aşağıdaki bölümlerde bu kimlik bilgilerini nasıl oluşturabileceğinize dair genel bir bakış sunulmaktadır.

Microsoft Graph ve Azure Log Analytics İçin Erişim Kimlik Bilgilerini Alma

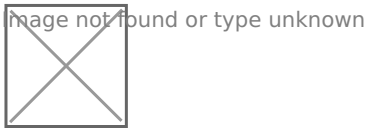
Azure için Wazuh modülünden gelen bağlantıyı doğrulamak için geçerli application_id ve application_key değerlerine ihtiyacınız var.

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

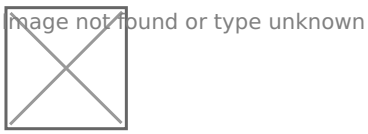
1. Microsoft Entra ID'ye gidin ve kayıtlı uygulamaya gidin.



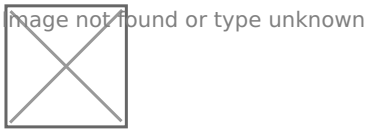
2. **Seçtiğiniz uygulamanın Sertifikalar ve sırlar** bölümüne gidin , ardından **Yeni istemci sırrı'nı** seçerek bir gizli anahtar oluşturun .



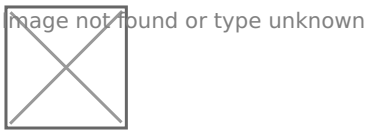
3. Anahtara açıklayıcı bir ad verin ve anahtarın etkin kalacağı süreyi belirtin, ardından **Ekle'yi** seçin.



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.

Image not found or type unknown

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

Image not found or type unknown

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:

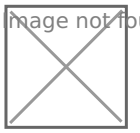
```
/var/ossec/wodles/azure/azure-logs --log_analytics --la_auth_path credentials_example --la_tenant_domain 'wazuh.example.domain' --la_tag azure-activity --la_query "AzureActivity" --workspace example-workspace --la_time_offset 50d --debug 2 --reparse
```

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

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

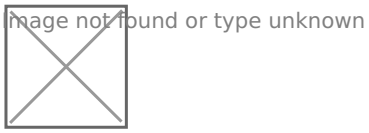
Uygulamanın kurulumu

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.

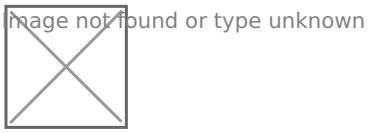
Uygulamanın oluşturulması

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.

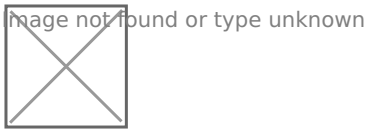


2. Uygulama için kullanıcıya dönük görüntü adını tanımlayın ve **Kaydet'i** seçin .

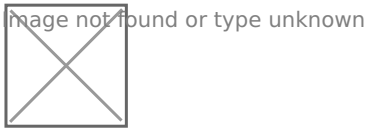


Uygulamaya İzinlerin Verilmesi

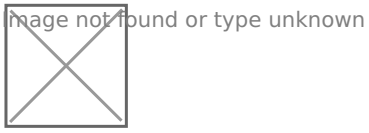
1. **Uygulama kaydından** Tüm **uygulamaları** seçin ve yenileyin. Yeni uygulama görünecektir. Bizim durumumuzda, görünen ad **LogAnalyticsApp'dir**.



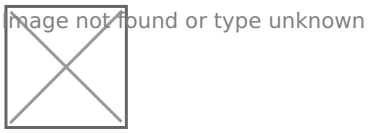
2. **Genel Bakış** bölümüne gidin ve **Uygulama (istemci) kimliğini** daha sonraki kimlik doğrulaması için kaydedin.



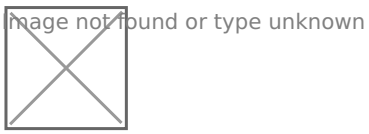
3. **API izinleri** bölümüne gidin ve uygulamaya **Data.Read** iznini ekleyin.



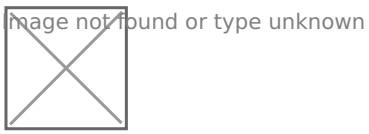
4. **Log Analytics API'yi** arayın .



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

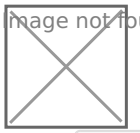


6. Kiracıya **yönetici onayı vermek** için bir yönetici kullanıcısı kullanın.

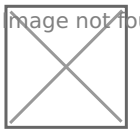


Uygulamaya Azure Log Analytics API'sine Erişim İzni Verme

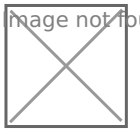
1. **Log Analytics çalışma alanlarına** erişin ve yeni bir çalışma alanı oluşturun veya mevcut bir çalışma alanını seçin.



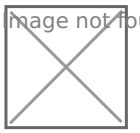
2. **Genel Bakış** bölümünden değeri kopyalayın .Workspace ID



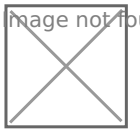
3. **Erişim denetimi (IAM)** bölümüne gidin , **Ekle'ye** tıklayın ve uygulamaya gerekli rolü eklemek için **Rol ataması ekle'yi** seçin .



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.

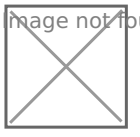


6. Bitirmek için **Gözden Geçir + Ata'ya** tıklayın .

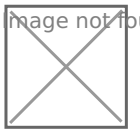
Günlükleri Çalışma Alanına gönderme

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 .

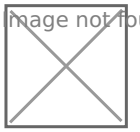
Use Case

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.

Image not found or type unknown

Wazuh Dashboard Olayların Görselleştirilmesi

Kurulum tamamlandıktan sonra sonuçları Wazuh kontrol panelinden kontrol edebilirsiniz.

Image not found or type unknown

Microsoft Graph Servislerini Wazuh İle İzleme

Microsoft Graph API, Microsoft 365, Azure, Dynamics 365 ve diğer çeşitli Microsoft bulut bileşenleri dahil ancak bunlarla sınırlı olmamak üzere Microsoft bulut hizmetlerinin tüm paketindeki verilere erişim sağlayan kapsamlı bir API sistemidir. Microsoft Bulut ekosisteminden yapılandırılmış verilere, içgörülere ve zengin ilişkilere erişim için bir uç noktadır.

Bu bölümde, Microsoft Graph için Wazuh modülünü kullanarak kuruluşunuzun Microsoft Graph API kaynaklarını ve ilişkilerini izlemeye yönelik talimatlar verilmektedir.

Şu anda Microsoft Graph için Wazuh modülü Wazuh ile aşağıdakileri izlemenize olanak sağlıyor:

- Microsoft Entra Kimlik Koruması
- Microsoft 365 Savunucusu
- Bulut Uygulamaları için Microsoft Defender
- Microsoft Defender Uç Nokta İçin
- Kimlik için Microsoft Defender
- Office 365 için Microsoft Defender
- Microsoft Kapsamı eKeşif
- Microsoft Kapsamı Veri Kaybını Önleme (DLP)

Bunlar güvenlik kaynağı için temel olsa da, Microsoft Graph API'sini kullanarak birçok ek kaynağı izleyebilirsiniz. Daha fazla bilgi edinmek için Microsoft Graph belgelerine Genel Bakış'a bakın.

> Not: Güvenlik kaynağı, önceden oluşturulmuş kurallarla test edildiği için olgun olarak kabul edilebilir. Ancak, kuruluşunuz günlükleri diğer kaynaklardan Wazuh dağıtımınıza alabilir.

İçerik alınıyor

Microsoft Graph'tan bir dizi günlük almak için `GET`aşağıdaki URL'yi kullanarak bir istekte bulunun:

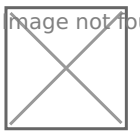
```
GET https://graph.microsoft.com/{version}/{resource}/{relationship}?{query-parameters}
```

Microsoft Graph API'nin mevcut üretim sürümünün açıklaması Microsoft Graph'a Genel Bakış'ta bulunabilir .

Alternatif olarak, API doğrudan Microsoft Graph Explorer aracılığıyla denenebilir .

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

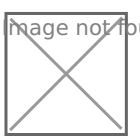
Azure

Etkinlik Günlüğü Dışa Aktarımını Yapılandırma

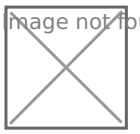
1. **Microsoft Entra ID** içerisindeki **İzleme bölümünden Denetim Günlükleri** seçeneğini seçin ve **Veri Ayarlarını Dışa Aktar'a** tıklayın.



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

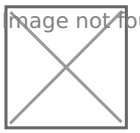


3. **Denetim Günlükleri'ni** seçin ve **Depolama hesabına arşivleyin** onay kutusunu seçin , ardından açılır menüden günlükleri dışa aktarmak istediğiniz aboneliği ve Depolama hesabını seçin.



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
   ```

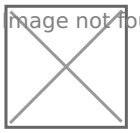
Kullanım Durumu

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

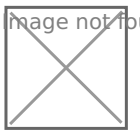
Yeni Bir Kullanıcı Oluştur

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.



Microsoft Grafiği

Bu bölümde, Microsoft Graph REST API'yi kullanarak Microsoft Entra ID etkinliğinizi nasıl izleyeceğinizi öğreneceksiniz. Bu bölüm şunları içerir:

- Azure yapılandırması
- Wazuh yapılandırması
- Microsoft Entra ID kullanım örneği

Aşağıda Microsoft Entra ID'deki denetim ve izleme faaliyetleriyle ilgili Microsoft Graph REST API'sindeki uç noktalar yer almaktadır.

Rapor türü	**Sorgu**
Dizin denetimleri	`auditLogs/directoryaudits`
Oturum açmalar	`auditLogs/signIns`
Tedarik	`auditLogs/provisioning`

Bu uç noktalar, yöneticilerin ve geliştiricilerin güvenlik, uyumluluk ve operasyonel amaçlar doğrultusunda Microsoft Entra ID içindeki etkinlikleri izlemesine ve denetlemesine olanak tanır.

Wazuh, yukarıdaki uç noktaları kullanarak Microsoft Entra ID etkinlik raporlarını işleyebilir. Her biri farklı bir sorgu yürütmenizi gerektirir. Bu sorguları Azure yapılandırması için Wazuh modülünüzün komut bloğuna yerleştireceksiniz .

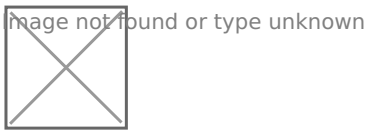
Yapılandırma

Azure

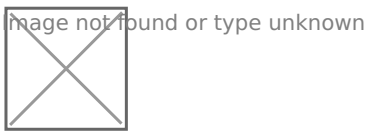
Uygulamanın Oluşturulması

Bu bölüm Azure Log Analytics REST API'sini kullanarak bir uygulama oluşturmayı açıklar. Ancak, mevcut bir uygulamayı yapılandırmak da mümkündür. Bu durumda, bu adımı atlayın.

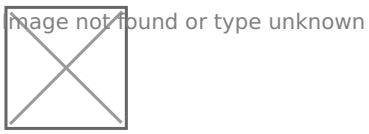
1. **Microsoft Entra ID** panelinde , **Uygulama kayıtları'nı** seçin . Ardından, **Yeni kayıt'ı** seçin.



2. Uygulamaya açıklayıcı bir ad verin, uygun **hesap türünü** seçin ve **Kaydol'a** tıklayın.

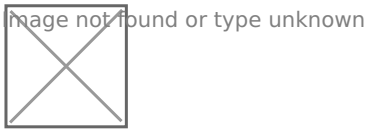


Uygulama artık kayıtlı.

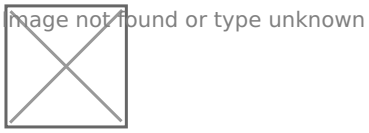


Uygulamaya İzinlerin Verilmesi

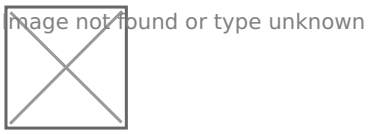
1. Uygulamaya tıklayın, **Genel Bakış** bölümüne gidin ve daha sonraki kimlik doğrulaması için **Uygulama (istemci) Kimliğini** kaydedin.



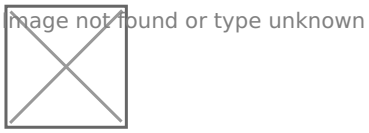
2. **API izinleri** bölümünde **İzin ekle** seçeneğini belirleyin.



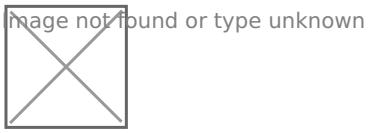
3. "*Microsoft Graph*"ı arayın ve API'yi seçin.



4. **Uygulamalar** izinlerinde altyapınızla uyumlu izinleri seçin . Bu durumda `AuditLog.Read.All` izinler verilecektir. Ardından **İzinleri ekle'ye** tıklayın.



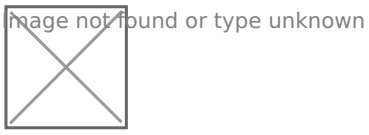
5. Kiracıya **yönetici onayı vermek** için bir yönetici kullanıcısı kullanın.



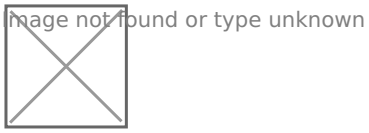
Kimlik Doğrulama İçin Uygulama Anahtarının Alınması

Log Analytics API'yi günlükleri almak için kullanmak üzere, Log Analytics API'yi doğrulamak için bir uygulama anahtarı üretmeliyiz. Uygulama anahtarını üretmek için aşağıdaki adımları izleyin.

1. **Sertifikalar ve sırlar'ı** seçin , ardından bir anahtar oluşturmak için **Yeni istemci sırrı'nı seçin.**

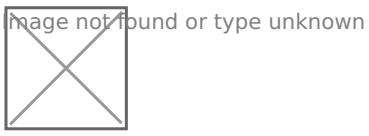


2. Uygun bir **açıklama** girin , anahtar için tercih edilen süreyi ayarlayın ve ardından **Ekle'ye** tıklayın.



3. Anahtar **değerini** kopyalayın . Bu daha sonra kimlik doğrulama için kullanılacaktır.

> Not: Bu sayfadan çıkmadan önce anahtarı kopyalayın, çünkü yalnızca bir kez görüntülenecektir. Sayfadan çıkmadan önce kopyalamazsanız, yeni bir anahtar oluşturmanız gerekecektir.



Wazuh Sunucusu veya Agent

Burada önceki adımlarda kaydedilen uygulamanın ve'sini `key`kullanacaksınız . Bu durumda, her iki alan da kimlik doğrulama için bir dosyaya kaydedildi. Bu konu hakkında daha fazla bilgi için Azure kimlik bilgilerini yapılandırma bölümüne bakın.`ID`

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>
  <wday>Monday</wday>
```

```
  <time>2:00</time>
  <run_on_start>no</run_on_start>

  <graph>
    <auth_path>/var/ossec/wodles/azure/credentials</auth_path>
    <tenantdomain>wazuh.com</tenantdomain>
    <request>
       <tag>microsoft-entra_id</tag>
       <query>auditLogs/directoryAudits</query>
       <time_offset>1d</time_offset>
    </request>
  </graph>

</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
- `<wday>`tarama için planlanan haftanın günü nedir
- `<query>`Denetim günlüklerinin saklandığı yoldur.
- `<time>`tarama için planlanan zamandır.
- `<time_offset>`' a ayarlandığında `1d`, yalnızca son güne ait günlük verileri ayrıştırılır.

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
   ```

Farklı kullanılabilir parametreleri kullanma hakkında daha fazla bilgi için Azure referansı için Wazuh modülünü kontrol edin . Microsoft Entra kimliğinizi izlemek için kimlik bilgilerini nasıl ayarlayacağınıza dair rehberlik için lütfen Wazuh Azure kimlik doğrulama dosyası bölümüne bakın.

> Uyarı: Alan zorunludur. Bunu **Microsoft Entra ID'deki Genel Bakış** bölümünden `tenantdomain`edinebilirsiniz .

Kullanım Durumu

Microsoft Entra ID'yi İzleme

Microsoft Entra ID, temel dizin hizmetlerini, uygulama erişim yönetimini ve kimlik korumasını tek bir çözümde birleştiren kimlik ve dizin yönetim hizmetidir.

Wazuh, Microsoft Graph REST API tarafından sağlanan etkinlik raporlarını kullanarak Microsoft Entra ID (ME-ID) hizmetini izleyebilir . Microsoft Graph API, Microsoft Entra ID uygulamalarındaki dizin verileri ve nesneler üzerinde okuma işlemleri gerçekleştirebilir.

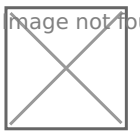


Yukarıdaki yapılandırmayı kullanarak Microsoft Entra ID etkinlik izleme örneğini aşağıda bulabilirsiniz.

Yeni Bir Kullanıcı Oluştur

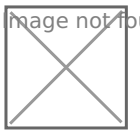
Azure'da yeni bir kullanıcı oluşturun. Başarılı bir kullanıcı oluşturma etkinliği bunu yansıtacak bir günlük üretecektir. Bu günlüğü auditLogs/directoryAudits sorgusunu kullanarak alabilirsiniz.

1. **Kullanıcılar** > **Tüm kullanıcılar'a** gidin , **Yeni kullanıcı** > **Yeni kullanıcı oluştur'u** seçin.



2. Gerekli bilgileri girin ve **İncele + oluştur'a** tıklayın . Kullanıcı artık oluşturuldu.

Başarılı kullanıcı oluşturma sonucunu **Microsoft Entra ID'nin Denetim günlükleri** bölümünden kontrol edebilirsiniz .



Entegrasyon çalışmaya başladığında, sonuçlar **Wazuh panosunun** Güvenlik **Olayları** sekmesinde mevcut olacaktır.

