## 監控 AWS 基礎架構

這個用例展示了 Wazuh 對 AWS（aws-s3）的模塊如何從不同的 AWS 資源收集日誌數據。

要了解更多關於監控 AWS 資源的信息，請參閱文檔中的 "使用 Wazuh 監控 AWS" 部分。

### 基礎設施

#### 雲服務

描述

Amazon CloudTrail

AWS CloudTrail，就像所有其他支持的 AWS 服務一樣，需要提供有效的身份驗證方法。在這個 PoC 中，我們使用個人檔案認證方法。

### 配置

執行以下步驟來配置 Wazuh 監控 Amazon CloudTrail 服務並識別安全事件。

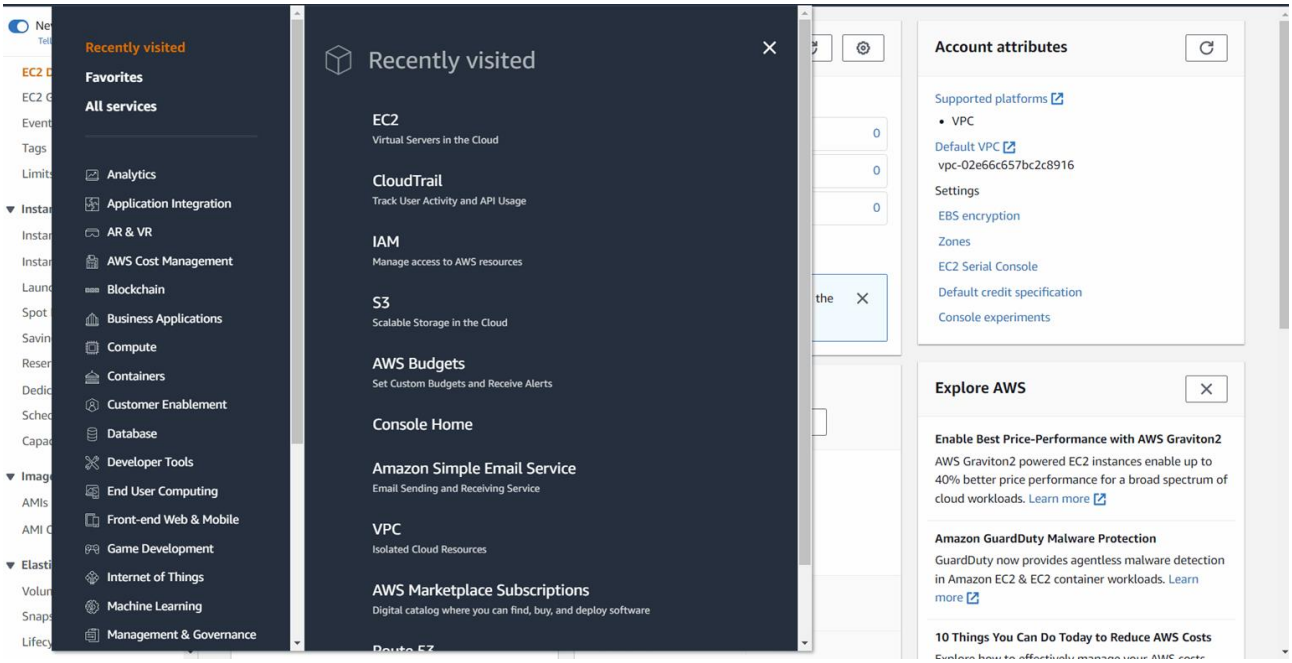
CloudTrail

使用 AWS 控制台訪問 CloudTrail 服務。

創建一個新的日誌跟踪（trail）。

選擇是創建一個新的 S3 存儲桶還是指定一個現有的存儲桶來存儲 CloudTrail 日誌。記下所使用的 S3 存儲桶的名稱，因為需要在 Wazuh 配置中指定它。

下面的圖片展示了如何創建一個新的 CloudTrail 服務並附加一個新的 S3 存儲桶。



## Wazuh 伺服器

從 Wazuh 儀表板，瀏覽到 設定 > 模塊，並啟用 Amazon AWS 模塊儀表板，預設情況下它是禁用的。

在 Wazuh 伺服器的 /var/ossec/etc/ossec.conf 配置文件中啟用 Wazuh AWS 模塊。僅添加感興趣的 AWS 存儲桶。請閱讀我們的指南以了解如何配置 AWS 證書：

```
<wodle name="aws-s3">
  <disabled>no</disabled>
  <interval>30m</interval>
  <run_on_start>yes</run_on_start>
  <skip_on_error>no</skip_on_error>
  <bucket type="cloudtrail">
    <name><AWS_BUCKET_NAME></name>
    <aws_profile><AWS_PROFILE_NAME></aws_profile>
  </bucket>
</wodle>
```

重新啟動 Wazuh 管理器以應用更改：

```
sudo systemctl restart wazuh-manager
```

## 測試配置

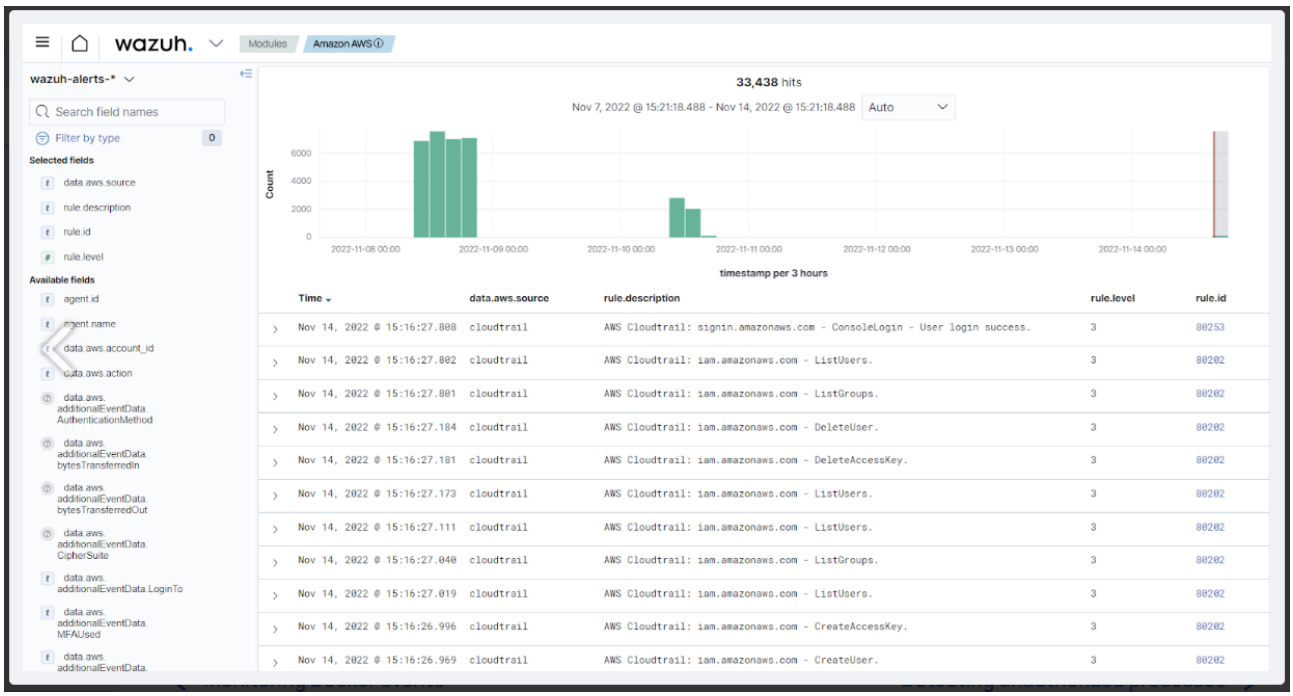
一旦配置 CloudTrail，您可以通過使用 IAM 服務創建新的 IAM 使用者帳戶來生成事件。這會生成 Wazuh 處理的事件。

Wazuh 默認規則集會解析 AWS 日誌並自動生成警報。警報將在 Wazuh 收到 AWS S3 存儲桶的日誌時立即出現。

您也可以在我們的文檔中找到其他 CloudTrail 用例。

## 可視化警報

您可以在 Wazuh 儀表板中可視化警報數據。為此，瀏覽到 模塊 > Amazon AWS 模塊。


wazuh.
Modules
Amazon AWS
wazuh-alerts-*
Search field names
Filter by type
0
Selected fields
data.aws.source
rule.description
rule.id
rule.level
Available fields
agent.id
agent.name
data.aws.account_id
data.aws.action
data.aws.additionalEventData.AuthenticationMethod
data.aws.additionalEventData.bytesTransferredIn
data.aws.additionalEventData.bytesTransferredOut
data.aws.additionalEventData.CipherSuite
data.aws.additionalEventData.LoginTo
data.aws.additionalEventData.MFAUsed
data.aws.additionalEventData.
33,438 hits
Nov 7, 2022 @ 15:21:18.488 - Nov 14, 2022 @ 15:21:18.488
Auto
Count
6000
4000
2000
0
2022-11-08 00:00
2022-11-09 00:00
2022-11-10 00:00
2022-11-11 00:00
2022-11-12 00:00
2022-11-13 00:00
2022-11-14 00:00
timestamp per 3 hours
Time
data.aws.source
rule.description
rule.level
rule.id
Nov 14, 2022 @ 15:16:27.808 cloudtrail AWS Cloudtrail: signin.amazonaws.com - ConsoleLogin - User login success. 3 80253
Nov 14, 2022 @ 15:16:27.802 cloudtrail AWS Cloudtrail: iam.amazonaws.com - ListUsers. 3 80202
Nov 14, 2022 @ 15:16:27.801 cloudtrail AWS Cloudtrail: iam.amazonaws.com - ListGroups. 3 80202
Nov 14, 2022 @ 15:16:27.184 cloudtrail AWS Cloudtrail: iam.amazonaws.com - DeleteUser. 3 80202
Nov 14, 2022 @ 15:16:27.181 cloudtrail AWS Cloudtrail: iam.amazonaws.com - DeleteAccessKey. 3 80202
Nov 14, 2022 @ 15:16:27.173 cloudtrail AWS Cloudtrail: iam.amazonaws.com - ListUsers. 3 80202
Nov 14, 2022 @ 15:16:27.111 cloudtrail AWS Cloudtrail: iam.amazonaws.com - ListUsers. 3 80202
Nov 14, 2022 @ 15:16:27.040 cloudtrail AWS Cloudtrail: iam.amazonaws.com - ListGroups. 3 80202
Nov 14, 2022 @ 15:16:27.019 cloudtrail AWS Cloudtrail: iam.amazonaws.com - ListUsers. 3 80202
Nov 14, 2022 @ 15:16:26.996 cloudtrail AWS Cloudtrail: iam.amazonaws.com - CreateAccessKey. 3 80202
Nov 14, 2022 @ 15:16:26.969 cloudtrail AWS Cloudtrail: iam.amazonaws.com - CreateUser. 3 80202