Cloud Connector, instalación y uso

Cloud Connector: Instalación en AWS y uso

Documentación Cloud Connector

- Documentación oficial: https://docs.sysdig.com/en/aws-cloud-auditing-with-sysdig-cloud-connector.html

- Documentación proyecto: https://sysdiglabs.github.io/cloud-connector/
  - Instalación: https://sysdiglabs.github.io/cloud-connector/deployment-cloudformation.html
  - Listado de reglas incluidas: https://sysdiglabs.github.io/cloud-connector/rules/cloudtrail.html
- Artículo de Blog https://sysdig.com/blog/aws-threat-detection-cloudtrail/

Instalación de Cloud Connector en AWS

1. Usar cuenta administrador que NO sea ROOT
2. Instalar y configurar AWS CLI si queremos usar bash scripts
3. Activar AWS Security Hub (tiene cierto coste) https://console.aws.amazon.com/securityhub/home
4. Desplegar plantilla CloudFormation: https://console.aws.amazon.com/cloudformation/home#/stacks/create/template?stackName=CloudConnector&templateURL=https://cf-templates-cloud-connector.s3.amazonaws.com/cloud-connector.template

   - No olvidar **marcar consentimiento crear recursos IAM**
   - Los recursos que utiliza tienen cierto coste (ECS/Fargate)

5. AWS puede tardar hasta 10 minutos aproximadamente en activar CloudTrail y comenzar a enviar eventos

Workshops en vivo de AWS

- Durante Enero 2021, AWS organizará 3 workshop gratuitos en remoto
- Se realizan en tiempo real durante cada evento, con explicación inicial y soporte durante su realización
- Se publicarán en https://www.awsworkshop.io
  - Sysdig automatic scan con Amazon ECR
  - Sysdig automatic scan con Amazon ECS/Fargate
  - **Sysdig Cloud Connector para cloud security**

Algunas reglas incluidas

- AWS Command Executed on Unused Region
- CloudTrail Trail Deleted
- Allocate New Elastic IP Address to AWS Account
- Logged in without Using MFA
- Root User Executing AWS Command
- Attach Administrator Policy
- Create AWS user
- Create Customer Master Key (for KMS with rotation disabled)

Lista completa: https://sysdiglabs.github.io/cloud-connector/rules/cloudtrail.html

Pruebas, reglas incluidas

- Si inicias sesión como *Root account* o sin usar MFA, hazlo de nuevo y aparecerá una advertencia
- Creamos un EC2 para luego borrarlo

Comprobar resultados:

- AWS Security Finds
  - Filtrar Product=Default
- Cloud Connector, CloudWatch logs

Sobre eventos de Cloudtrail

- https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitor-with-cloudtrail.html

- Formato JSON
- Campos importantes:
  - eventName : Tipo de evento
  - requestParameters : Parámetros del evento
  - sourceIPAddress : IP del solicitante
  - awsRegion : Región AWS
  - userIdentity / arn : Id del solicitante

Creación y modificación de reglas

- Reglas basadas en procesar eventos CloudTrail en formato JSON
- Subir fichero con reglas a bucket S3 y reiniciar Cloud Connector
- Ejemplos:
  - Actualizar lista: Establecer regiones no utilizadas
  - Detectar parar o iniciar instancia EC2 https://aws.amazon.com/premiumsupport/knowledge-center/cloudtrail-search-api-calls/

Regla existente: region no permitida

```
- list: disallowed_aws_regions
  items: []

- rule: AWS command executed on unused region
  desc: Detect AWS command execution on unused regions
  condition: >
    not jevt.value[/errorCode] exists and
    jevt.value[/awsRegion] in (disallowed_aws_regions)
  output: >
    An AWS command has been executed on an unused region
    (requesting user=%jevt.value[/userIdentity/arn],
    requesting IP=%jevt.value[/sourceIPAddress],
    AWS region=%jevt.value[/awsRegion]
  priority: CRITICAL
  tags: [cloud, source=cloudtrail, aws]
  source: k8s_audit
```

Actualizamos lista de regiones no permitidas

```
- list: disallowed_aws_regions
  items: [us-east-2, us-west-1, us-west-2, af-south-1, ap-east-1, ap-south-1,
ap-northeast-3, ap-northeast-2, ap-southeast-1, ap-southeast-2, ap-northeast-
1, ca-central-1, eu-central-1, eu-west-1, eu-west-2, eu-south-1, eu-west-3,
eu-north-1, me-south-1, sa-east-1]
  append: true

- rule: AWS Command Executed on Unused Region
  condition: and not jevt.value[/sourceIPAddress]="autoscaling.amazonaws.com"
  append: true
```

Aquí están todas menos us-east-1

Regiones disponibles:
https://docs.aws.amazon.com/es_es/AWSEC2/latest/UserGuide/using-regions-availability-zones.html#concepts-available-regions

Nueva regla existente: terminate EC2

```
- rule: Terminate AWS Instances
  desc: Detect terminating AWS instances.
  condition:
    jevt.value[/eventName]="TerminateInstances" and not jevt.value[/errorCode] exists
  output:
    A number of AWS EC2 instances have been terminated.
    (requesting user=%jevt.value[/userIdentity/arn],
     requesting IP=%jevt.value[/sourceIPAddress],
     AWS region=%jevt.value[/awsRegion])
  priority: WARNING
  tags:
    - cloud
    - source=cloudtrail
    - aws
    - aws_ec2
  source: k8s_audit
```

QUANTIKA 14

```
# Subimos la carpeta con el archivo
cc_bucket=$(aws cloudformation list-stack-resources --stack-name CloudConnector --
output json | jq '.StackResourceSummaries[] |
select(.LogicalResourceId=="CloudConnectorCloudTrailBucket").PhysicalResourceId' |
xargs) echo $cc_bucket

aws s3 sync "./rules/" s3://$cc_bucket/rules --delete


# Reiniciamos Cloud Connector para que lea fichero de reglas
task_id=$(aws ecs list-tasks --cluster CloudConnector --output json | jq
'.taskArns[0]' | xargs | sed -E 's/.*\/(.+)/\1/')
echo $task_id
AWS_PAGER="" aws ecs stop-task --cluster CloudConnector --task $task_id
```

```
# Consultamos cuál es el nuevo log stream tras reiniciar Cloud Connector
cc_log_stream=$(aws logs describe-log-streams --log-group-name cloud-connector --
order-by LastEventTime --descending | grep -m1 "ecs/CloudConnector/" | sed 's/"\
(.*\)".*"\(.*\)",/\2/' | xargs)
echo $cc_log_stream

# Comprobamos que se han cargado los nuevos ficheros de reglas
aws logs filter-log-events --log-group-name cloud-connector --log-stream-names
$cc_log_stream --filter-patter "-http-server -console-notifier"

# Consultamos los últimos eventos de seguridad
aws logs get-log-events --log-group-name cloud-connector --log-stream-name alerts --
no-start-from-head --limit 5
```