

509.2

Amazon AWS

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

<https://t.me/learningnets>

509.2

Amazon AWS

SANS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

<https://t.me/learningnets>

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With the CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, YOU AGREE TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, YOU AGREE THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If you do not agree, you may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP and PMBOK are registered marks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

FOR509.2

Enterprise Cloud Forensics and Incident Response



Amazon AWS

© 2021 David Cowen | All Rights Reserved | Version G01_01

Authors:

David Cowen – dlcowen@gmail.com

<https://twitter.com/HECFBlog>

<https://www.hecfblog.com/>

Pierre Lidome – plidome@gmail.com

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

f SANSForensics

▶ dfr.to/DFIRCast

🐦 @SANSForensics



OPERATING SYSTEM & DEVICE IN-DEPTH



FOR308
Digital Forensics Essentials



FOR498
Battlefield Forensics
& Data Acquisition
GBFA



FOR500
Windows Forensic Analysis
GCPE



FOR518
Mac and iOS Forensic Analysis
& Incident Response



FOR585
Smartphone Forensic
Analysis In-Depth
GASF

INCIDENT RESPONSE & THREAT HUNTING



FOR508
Advanced Incident
Response, Threat Hunting,
& Digital Forensics
GCFA



FOR572
Advanced Network Forensics:
Threat Hunting, Analysis,
& Incident Response
GNFA



FOR578
Cyber Threat Intelligence
GCTI



FOR610
REM: Malware Analysis
Tools & Techniques
GREM



SEC504
Hacker Tools,
Techniques, Exploits,
& Incident Handling
GCIH

This page intentionally left blank.

Sample Incident: Pymtechlabs

- For the purpose of learning AWS logs, this incident is limited to a few steps
- Focus on understanding the uniqueness of AWS logs
- Question to take back after this class: are AWS logs configured correctly and available to me in my environment?
- Logs can be reviewed in different ways inside the AWS console, but most companies will use a SIEM
- Labs leverage SOF-ELK, and all relevant data has extracted to the VM

To further the educational experience, we have created a simple scenario that will facilitate learning about the different logs. All the data has been imported into SOF-ELK to facilitate your analysis.

AWS Global Datacenter Map



Credit: Amazon AWS

Picture as of 4/17/21

Source: <https://aws.amazon.com/about-aws/global-infrastructure/>

FOR509.2 – Amazon AWS (I)

Section 2.1: Understanding IR in AWS

Section 2.2: Networking, VMs and Storage

Section 2.3: Log Sources for IR

Section 2.4: Event Driven Response

Section 2.5: In Cloud IR

This page intentionally left blank.

FOR509.2 – Amazon AWS



English to AWS Translation



A quick language primer so you can speak AWS natively

This section will introduce you to the language of AWS. The major services that are involved with most environments as well as the forensic data we can expect to receive from them. This course is not meant to teach how to configure, maintain or deploy AWS services but how to investigate and respond to breaches within them.

When talking to AWS professionals having the ability to speak their language will go a long way in their ability to assist you in your investigation.

For instance here are several questions that result in good forensic data:

“Where do you store CloudTrail logs?”

“Do you have flow logs for this VPC?”

“Can this AKS cluster reach the metadata service?”

Don't understand what all these things mean? No problem that's what this section will help you understand while making sure those in the AWS world can understand you!

Amazon AWS Roadmap

2.1: Understanding IR in AWS

2.2: Networking, VM and Storage

2.3: Log Sources for IR

2.4: Event Drive Response

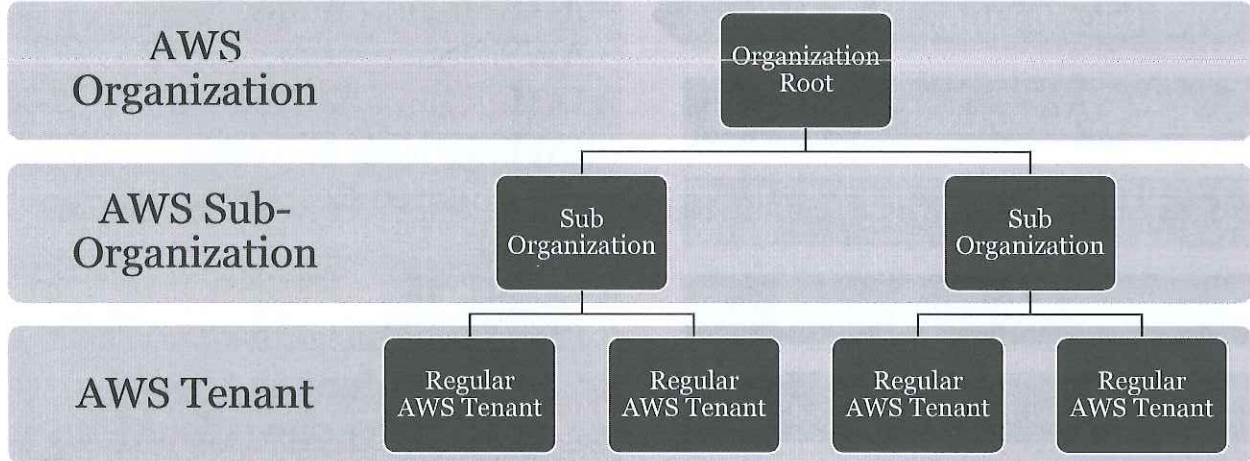
2.5: In-cloud IR

- AWS Organizations
- AWS Organizations for IR
- IAM
- IAM Methods of Access
- AWS Shared Responsibility Model
- CloudTrail
- CloudTrail Insights
- CloudTrail Hunting
- **Lab 2.1: Reviewing CloudTrail logs**

This page intentionally left blank.

AWS Organizations

One Tenant to Rule Them All



AWS Organizations are a way to group all your companies AWS Tenants into one tree so that you can:

- Manage access between AWS Tenants
- Establish single sign on across your AWS Tenants
- Recognize cost savings by allowing you usage to be accumulated across all Tenants for volume discounts

You can learn more about them here: <https://aws.amazon.com/organizations/>

AWS Organizations

AWS Tenant

- A single AWS billing entity
- A company may have 100s to 1000s of these

AWS Organization

- A group of AWS Tenants linked to a single entity

AWS Sub Organization

- A distinct group of AWS Tenants that are given different policies than other sub orgs

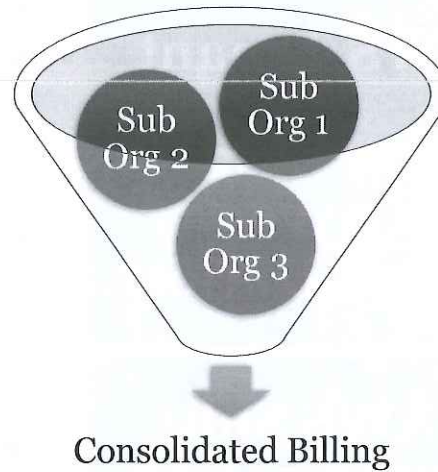
AWS Tenant – A single AWS tenant that you’ve created with Amazon Web services. If you’ve just started with AWS, then you likely have one of these. In large organizations each department could have an AWS Tenant per project, per group or per department. It’s not unusual as cloud adoption grows to find over 100 AWS tenants operating for one company.

AWS Organization – A group of AWS Tenants with one tenant serving as the master.

AWS Sub Organization -

Why use Organizations? (1)

- Consolidated Billing
 - Discounts for bulk usage
 - AWS Provides discounts the more of it you use
 - Consolidated billing allows all of the Tenants in your Organization to add up all their usage for a larger discount



This page intentionally left blank.

Why use Organizations? (2)

Master
Tenant

- Root of Trust, the master Tenant
- A role defined here can access all AWS Tenants below it

Sub
Organization

- Sub Root, like a top Tenant for a specific department
- A role here can access all Sub Org AWS Tenants but not any adjacent Tenants or the master Tenant

AWS Tenant

- The bottom of the trust stack
- A role here can access resources within the single AWS Tenant but not any adjacent or above it in the Org tree

This page intentionally left blank.

IR Roles in Organizations



Automatic Write Blocking!



**You can define read only
global access too:**

- S3 Buckets
- EC2 Virtual Machines
- EBS Data Stores
- Databases
- Containers
- And More!

This page intentionally left blank.

IAM – Identity and Access Management



Cornerstone of AWS



Roles, rules and responsibilities



Can be cross-AWS Tenants with organizations



It's like Active Directory for AWS

This page intentionally left blank.

Ways of Accessing AWS



Username and password = Tired



API Key = The New Normal



SAML Token = Cool Kids Club



IAM Roles Assigned = Robot Uprising

This page intentionally left blank.

Accessing AWS

Username and Password

- Good:
 - Good for using the web console, but shouldn't be hardcoded anywhere else
 - Make sure to turn on MFA
- Bad:
 - Static credentials that allow full access
 - Keeping track of multiple Tenants for multiple roles

API Key

- Good:
 - Defining role based access with specific permissions
 - Allows access without exposing passwords
- Bad:
 - Bad guys and bug bounty hunters are already searching the world for API Keys
 - Typically don't expire and can easily continue to exist when someone leaves

SAML Token

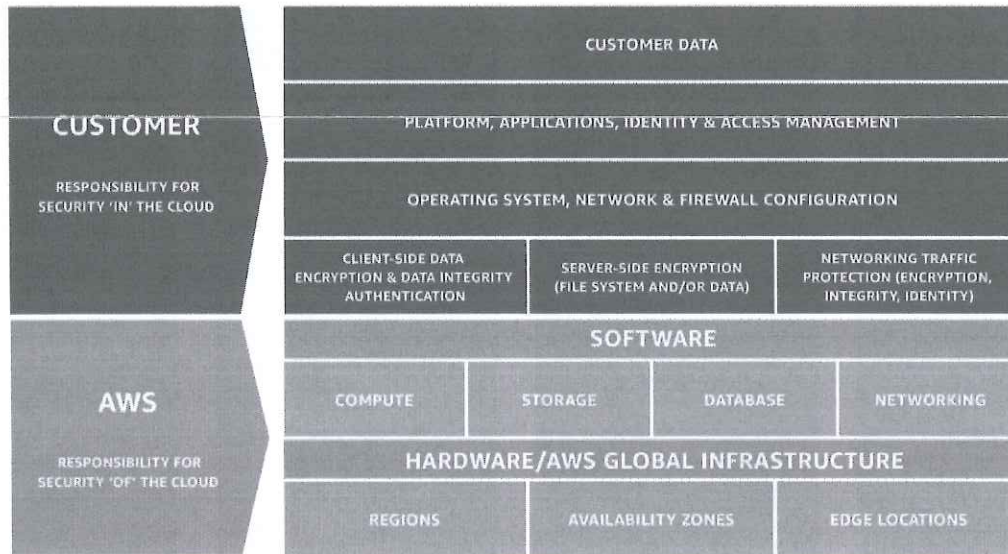
- Good:
 - Allows for one time usage of an AWS Resource
 - Allows access to resources outside of your organization
- Bad:
 - Requires someone with Admin permissions to

IAM Roles Assigned to Resources

- Good:
 - Allows access without credentials
- Bad:
 - Once compromised provides those roles without credentials

This page intentionally left blank.

AWS Shared Responsibility Model



This page intentionally left blank.

What do you maintain the security of?

You are responsible to secure, maintain and monitor

- Operating system you choose to run and manage
- Firewall you configure
- S3 Bucket you provision
- Web applications you decide to run

Amazon will help with monitoring, for a fee

This page intentionally left blank.

What does AWS maintain?

Amazon provided hypervisor (EC2)

Amazon provided share storage space (S3)

Amazon maintained web application

Amazon maintained database

If Amazon maintains it, they secure it

This page intentionally left blank.

What is CloudTrail



Like Event Logs for your cloud tenant



Created by default



You have to pay to retain them longer than 90 days

This page intentionally left blank.

CloudTrail



Records are committed at a maximum of 15 minutes after the action by SLA



Some records will be available in less than 5 minutes, AWS does not maintain a list of which get this SLA



Logs can be retained in S3 if configured



You can search them within AWS provided services

- CloudTrail portal
- Athena
- Security Hub



Can also be shipped to other platforms or exported

This page intentionally left blank.

CloudTrail Pricing

Free Tier

- The built in CloudTrail portal and the 90 days it stores is searchable at no cost
- You can create one 'trail' in S3 for free and retain data longer than 90 days
- Does not include CloudTrail Insights

Paid Tier

- After the first 'trail' second copies of management events are \$2 per 100k events
- Data events are \$.10 per 100k events sent to S3
- CloudTrail Insights is \$.35 per 100k events

This page intentionally left blank.

CloudTrail Insights

CloudTrail > Insights

Insights (18) Info



Download events ▼

Select a lookup ... ▼

Enter a lookup value

30m

1h

3h

12h

Custom




1





| Event name | Event start time | Event source | Baseline ... | Insight a... | API call rate cha... |
|-------------------------|------------------------------------|----------------------|--------------|--------------|----------------------|
| AuthorizeSecurityGro... | April 03, 2021, 17:07:00 (UTC-0... | ec2.amazonaws.com | 0.0002 | 0.8000 | 456180% ↑ |
| CreateSecurityGroup | April 03, 2021, 17:04:00 (UTC-0... | ec2.amazonaws.com | 0.0000 | 0.6000 | 60% ↑ |
| ModifyNetworkInterf... | April 03, 2021, 17:04:00 (UTC-0... | ec2.amazonaws.com | 0.0000 | 1.2000 | 120% ↑ |
| CreateGrant | April 03, 2021, 17:03:00 (UTC-0... | kms.amazonaws.com | 0.0000 | 0.6000 | 60% ↑ |
| CreateNetworkInterf... | April 03, 2021, 17:03:00 (UTC-0... | ec2.amazonaws.com | 0.0000 | 2.4000 | 240% ↑ |
| ConsoleLogin | March 21, 2021, 13:51:00 (UTC-... | signin.amazonaws.com | 0.0002 | 0.8000 | 448340% ↑ |


This page intentionally left blank.


CloudTrail Fields for IR (I)


 **eventTime:** The time of the event in UTC, generated by the regional service by sync'd with NTP


 **userIdentity:** Details on how and who triggered the event

 **eventSource:** The AWS service that is creating the event

 **eventName:** The action that occurred

 **awsRegion:** In what region the action occurred

 **sourceIPAddress:** Where the action originated from

 **ARN:** The full name of the AWS resource that was used to authenticate

This page intentionally left blank.

CloudTrail Fields for IR (2)



userAgent : How the request was made



requestParameters/responseElements : What was requested/what was returned



eventID : Unique event number in CloudTrail



eventType : What type of event occurred



resources : What was accessed during the event



sessionCredentialFromConsole : did this event occur from the AWS console

This page intentionally left blank.

CloudTrail userIdentity Types

Root – The event was triggered by someone with the root identity account

IAMUser – The event was triggered by someone using IAM user credentials

AssumedRole - The event was triggered by an account that got credentials by IAM role or cross-account access

FederatedUser – The event was triggered via a temporary security token issued through federated authentication

AWSAccount – The event was triggered by an AWS account outside of your organization

AWSService – An AWS service triggered the event

This page intentionally left blank.

CloudTrail IAM Investigation Examples



Tracking access to the console



Finding API key creations



Finding exposed API keys



Threat Hunting in CloudTrail

This page intentionally left blank.

CloudTrail: Tracking access to the console

✓ Important fields



ARN

What account was logging in



eventTime

When they logged in



userAgent

What browser they used to login



sourceIPAddress

Where did they come from?



responseElements

Was it successful?



MFAUsed

Did they use MFA to login?

This page intentionally left blank.

CloudTrail Console Login

```
"eventVersion": "1.08",
"userIdentity": {
  "type": "Root",
  "principalId": "305681518678",
  "arn": "arn:aws:iam::305681518678:root",
  "accountId": "305681518678",
  "accessKeyId": ""
},
"eventTime": "2021-03-27T20:58:55Z",
"eventSource": "signin.amazonaws.com",
"eventName": "ConsoleLogin",
"awsRegion": "us-east-1",
"sourceIPAddress": "47.185.244.137",
"userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101 Firefox/87.0",
"requestParameters": null,
"responseElements": {
  "ConsoleLogin": "Success"
},
"additionalEventData": {
  "LoginTo": "https://console.aws.amazon.com/console/home?state=hashArgs%23&isauthcode=true",
  "MobileVersion": "No",
  "MFAUsed": "Yes"
}
```

What account logged in

When they logged in (UTC)

Login from web console

Source IP Address from browser

Browser used to login

It was successful

MFA was used to login

This page intentionally left blank.

CloudTrail: Tracking new API keys

ARN

- What account created the Key

eventTime

- When they created the key

userAgent

- What service (API/CLI/Console) did they use to do it?

sourceIPAddress

- Where did they come from?

responseElements

- What key was created?

This page intentionally left blank.

CloudTrail: New API Key Created from Console (1)

```
"userIdentity": {  
  "type": "Root",  
  "principalId": "305681518678",  
  "arn": "arn:aws:iam::305681518678:root",  
  "accountId": "305681518678",  
  "accessKeyId": "ASIAUOLAJ2BLAIKUWJ7S",  
  "userName": "pymtechlabs",  
  ...  
  "eventTime": "2021-03-27T21:00:43Z",  
  "eventSource": "iam.amazonaws.com",  
  "eventName": "CreateAccessKey",  
  "awsRegion": "us-east-1",  
  "sourceIPAddress": "47.185.244.137",  
  "userAgent": "console.amazonaws.com",  
  "requestParameters": {  
    "userName": "hpym"  }  
}
```

What account created the API Key

When did the key get created

Source IP of the browser

Console creation

This page intentionally left blank.

CloudTrail: New API Key Created from Console (2)

```
"responseElements": {
```

```
  "accessKey": {
```

```
    "userName": "hpym",
```

IAM user that corresponds with the key

```
    "accessKeyId": "AKIAUOLAJ2BLOJUMYJZM",
```

API Access Key

```
    "status": "Active"
```

Active or Disabled

```
    "createDate": "Mar 27, 2021 9:00:43 PM"
```

When the key was created

This page intentionally left blank.

CloudTrail User Agents

Examples

`signin.amazonaws.com`

`console.amazonaws.com`

`lambda.amazonaws.com`

`aws-cli`

Web Browser User Agents

This page intentionally left blank.

CloudTrail: Finding Exposed API Keys

Role Enumeration

| eventTime | eventSource | eventName | sourceipaddress | useragent | requestparameters | eventType |
|----------------------|-------------------|---------------------------|-----------------|---|---|------------|
| 2021-04-03T18:36:36Z | iam.amazonaws.com | ListRoles | 47.185.244.137 | aws-cli/2.1.32 Python/3.8.8 Windows/10 exe/AMD64 prompt/off onull | | AwsApiCall |
| 2021-04-03T18:43:36Z | iam.amazonaws.com | ListGroupsForUser | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |
| 2021-04-03T18:43:36Z | iam.amazonaws.com | GetUser | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | null | AwsApiCall |
| 2021-04-03T18:43:37Z | iam.amazonaws.com | GetPolicy | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/AdministratorAccess"} | AwsApiCall |
| 2021-04-03T18:43:37Z | iam.amazonaws.com | GetPolicyVersion | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/IAMUserChangePassword", "versionId": "v2"} | AwsApiCall |
| 2021-04-03T18:43:37Z | iam.amazonaws.com | ListUserPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |
| 2021-04-03T18:43:37Z | iam.amazonaws.com | ListAttachedGroupPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"groupName": "admin-access"} | AwsApiCall |
| 2021-04-03T18:43:37Z | iam.amazonaws.com | ListAttachedUserPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |
| 2021-04-03T18:43:37Z | iam.amazonaws.com | GetPolicyVersion | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/AdministratorAccess", "versionId": "v1"} | AwsApiCall |
| 2021-04-03T18:43:37Z | iam.amazonaws.com | ListGroupPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"groupName": "admin-access"} | AwsApiCall |
| 2021-04-03T18:44:25Z | iam.amazonaws.com | GetPolicy | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/IAMUserChangePassword"} | AwsApiCall |
| 2021-04-03T18:44:25Z | iam.amazonaws.com | ListAttachedGroupPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"groupName": "admin-access"} | AwsApiCall |
| 2021-04-03T18:44:25Z | iam.amazonaws.com | ListGroupsForUser | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |

This page intentionally left blank.

| eventtime | eventsource | eventname | sourceaddress | useragent | requestparameters | eventtype |
|----------------------|-------------------|---------------------------|----------------|--|---|------------|
| 2021-04-08T18:43:36Z | iam.amazonaws.com | ListRoles | 47.185.244.137 | aws-cli/2.1.32 Python/3.8.8 Windows/10 exe/AMD64 prompt/off curl | | AwsApiCall |
| 2021-04-08T18:43:36Z | iam.amazonaws.com | ListGroupsForUser | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |
| 2021-04-08T18:43:36Z | iam.amazonaws.com | GetUser | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | null | AwsApiCall |
| 2021-04-08T18:43:37Z | iam.amazonaws.com | GetPolicy | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/AdministratorAccess"} | AwsApiCall |
| 2021-04-08T18:43:37Z | iam.amazonaws.com | GetPolicyVersion | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/AdministratorAccess", "versionId": "v2"} | AwsApiCall |
| 2021-04-08T18:43:37Z | iam.amazonaws.com | ListUserPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |
| 2021-04-08T18:43:37Z | iam.amazonaws.com | ListAttachedGroupPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"groupName": "admin-access"} | AwsApiCall |
| 2021-04-08T18:43:37Z | iam.amazonaws.com | ListAttachedUserPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |
| 2021-04-08T18:43:37Z | iam.amazonaws.com | GetPolicyVersion | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/AdministratorAccess", "versionId": "v1"} | AwsApiCall |
| 2021-04-08T18:43:37Z | iam.amazonaws.com | ListGroupPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"groupName": "admin-access"} | AwsApiCall |
| 2021-04-08T18:44:25Z | iam.amazonaws.com | GetPolicy | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"policyArn": "arn:aws:iam::aws:policy/AdministratorAccess", "versionId": "v2"} | AwsApiCall |
| 2021-04-08T18:44:25Z | iam.amazonaws.com | ListAttachedGroupPolicies | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"groupName": "admin-access"} | AwsApiCall |
| 2021-04-08T18:44:25Z | iam.amazonaws.com | ListGroupsForUser | 47.185.244.137 | Boto3/1.17.44 Python/3.9.1 Windows/10 Botocore/1.20.44 | {"userName": "hpym"} | AwsApiCall |

CloudTrail:Threat Hunting

Impossible travel

- Console logins
- API Keys

IAM Roles testing permissions

New Source Ips accessing accounts

Keys and Roles querying the console

New account creations

Groups of VMs being created

This page intentionally left blank.

Lab 2.1

Reviewing CloudTrail Logs

This page intentionally left blank.

Guard Duty (I)



Now that you've learned how to manually review CloudTrail logs, don't you wish there was an easier way to find that likely threat?



Enter Guard Duty!

This page intentionally left blank.

Guard Duty (2)

Findings Info U Info

Info Saved rules *No saved rules*

Current ▼ Add filter criteria

| <input type="checkbox"/> | Finding type | Resource | Last seen | Count |
|--------------------------|--------------------------------------|-----------------------------------|----------------|-------|
| <input type="checkbox"/> | Policy:IAMUser/RootCredentialUsage | pyntechlabs: ASIAUOLAJ2ILCBCEXHXF | 12 minutes ago | 435 |
| <input type="checkbox"/> | UnauthorizedAccess:EC2/SSHBruteForce | Instance: i-0ca74a97b591310b2 | 4 days ago | 7 |
| <input type="checkbox"/> | UnauthorizedAccess:EC2/SSHBruteForce | Instance: i-07d9890b7ac8cd616 | 24 days ago | 20 |
| <input type="checkbox"/> | UnauthorizedAccess:EC2/SSHBruteForce | Instance: i-06960469a17634ccf | 2 months ago | 41 |
| <input type="checkbox"/> | UnauthorizedAccess:EC2/SSHBruteForce | Instance: i-0f594aa417b5daa4b | 3 months ago | 26 |

This page intentionally left blank.

FOR509.2 – Amazon AWS (2)

Section 2.1: Understanding AWS

Section 2.2: Networking, VMs and Storage

Section 2.3: Log Sources for IR

Section 2.4: Event Driven Response

Section 2.5: In Cloud IR

This page intentionally left blank.

Amazon AWS Roadmap

2.1: Understanding IR in AWS

2.2: Networking, VMs and Storage

2.3: Log Sources for IR

2.4: Event Drive Response

2.5: In-cloud IR

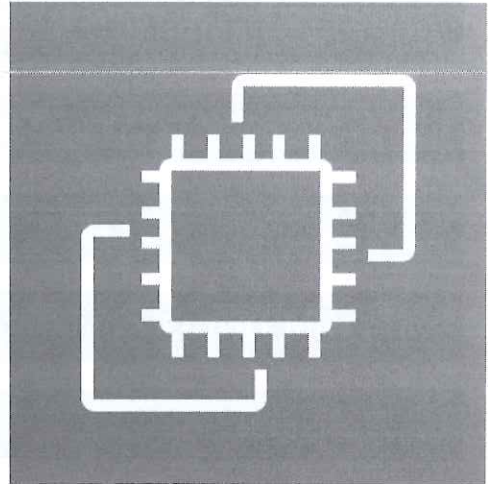
- EC2 Types
- CloudTrail: EC2
- EBS Types
- CloudTrail: EBS
- Snapshots
- CloudTrail: Snapshots
- EFS
- CloudTrail: EFS
- **Lab 2.2: Finding Rogue VMs**

This page intentionally left blank.

EC2 – Elastic Compute Cloud

This is the cloud version of a virtual machine

- AWS Provides
 - Initial Tenant creation
 - IP Address assignment
- You choose
 - When you want it to run
 - CPUs, Memory, Storage
 - How you will maintain it
 - How you will access it
 - How you will secure it



This page intentionally left blank.

EC2 Types

General Purpose Prefixes

- MAC – Bare metal Macs
- T - Burstable
- M – Most Scenarios
- A – ARM Based

Compute Optimized Prefix

- C – One CPU for every 2gb of ram

Memory Optimized

- R - RAM
- X – Extra Large Memory
- Z – High Frequency

Accelerated Computing

- P – GPU
- G - GPU
- F - FPGA

Storage Optimized

- I – IO Focused
- D – Dense Storage
- H – Large local storage

This page intentionally left blank.

Regions Matter!



In the IAM section we didn't have to talk much about Regions as accounts are valid across all regions.



However, many resources like EC2 VMs and EBS storage are region based meaning you have to know the region to access them.



Additionally, if you are going to transfer data it is faster to do it within the same Region.

This page intentionally left blank.

CloudTrail: Creating an EC2 Instance (I)

"userIdentity": {

IAM user that corresponds
with the key

"type": "Root",

"principalId": "305681518678",

"arn": "arn:aws:iam::305681518678:root",

"accountId": "305681518678",

API Key provided

"accessKeyId": "ASIAUOLAJ2BLL4OVFFHG",

"userName": "pymtechlabs",

This page intentionally left blank.

CloudTrail: Creating an EC2 Instance (2)

```
"eventTime": "2021-04-03T22:07:07Z"
```

What AWS Service generated the event

```
"eventSource": "ec2.amazonaws.com"
```

```
"eventName": "RunInstances",
```

What event occurred

```
"awsRegion": "us-east-1"
```

In what Region

```
"sourceIPAddress": "47.185.244.137",
```

```
"userAgent": "console.ec2.amazonaws.com"
```

```
"requestParameters": {
```

```
  "instancesSet": {
```

```
    "items": [
```

```
    {
```

```
      "imageId": "ami-037ce2fddcbf52",
```

```
      "minCount": 1,
```

```
      "maxCount": 1,
```

```
      "keyName": "NewEC2"
```

What was used to send the request

SSH Private Key Pair assigned

ImageID for VM Deployed

This page intentionally left blank.

CloudTrail: Creating an EC2 Instance (3)

```
"attributes": {
  "mfaAuthenticated": "true",
  "creationDate": "2021-04-01T12:03:50Z"
  "groupSet": {
    "items": [
      {
        "groupId": "sg-00b98f2f5d3339900"
      },
      {
        "groupId": "sg-044c410b2327cc21f"
      }
    ]
  },
  "userData": "<sensitiveDataRemoved>",
  "instanceType": "t2.micro",
}
```

The type of EC2 VM that was created

This page intentionally left blank.

CloudTrail: Creating an EC2 Instance with GPU

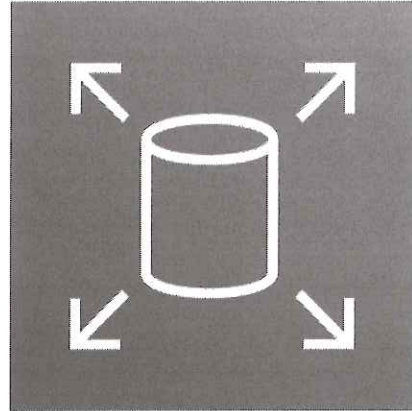
```
"attributes": {  
    "mfaAuthenticated": "true",  
    "creationDate": "2021-04-03T18:03:51Z"  
},  
"groupSet": {  
    "items": [  
        {  
            "groupId": "sg-00b98f2f5d3339900"  
        },  
        {  
            "groupId": "sg-044c410b2327cc21f"  
        }  
    ]  
},  
"userData": "<sensitiveDataRemoved>",  
"instanceType": "g4ad.4xlarge",
```

A GPU Enabled VM was created

This page intentionally left blank.

EBS – Elastic Block Store

- Virtual Storage for EC2
 - In virtual machine terms – VMDKs, VDIs, VHDs
- You can have as many virtual storage devices as you need



This page intentionally left blank.

EBS Types



General Purpose
Cheaper SSD

Gp3

Gp2



Provisioned IOPS
High throughput

Io2

io1

This page intentionally left blank.

CloudTrail: Creation of EBS

```
"instanceType": "t2.micro",
  "blockDeviceMapping": {
    "items": [
      {
        "deviceName": "/dev/xvda",
        "ebs": {
          "volumeSize": 8,
          "deleteOnTermination": true,
          "volumeType": "gp2"
        }
      }
    ]
  }
```

Mounted device path to EC2 VM

EBS Volume Type

This page intentionally left blank.

Snapshots

- Creates a disk image of the current state of the disk through the hypervisor
- First snapshot contains all data
- Subsequent snapshots only contain differences on a per block basis
- Copying snapshots between regions will get hit with a data transfer charge (\$.01 - \$.02 per GC)



This page intentionally left blank.

Snapshot Pricing

- **Storage** – Storage is charged on total space allocated, free space is not included
 - Free Tier
 - 1GB of snapshot storage
 - Paid Tier
 - \$.05 GB/month of data stored
- **Fast Snapshot Restoration**
 - \$.75 per 1 DSU hour (Data Service Hours)
- **Direct Block Access**
 - List Blocks - \$.0006 per thousand requests
 - Get Blocks - \$.003 per thousand units
 - Put Blocks - \$.006 per thousand units

This page intentionally left blank.

Making a snapshot with the CLI

```
aws ec2 create-snapshot --volume-id <volumeid>
  --description "Making a snapshot"
{
  "Description": "Making a snapshot",
  "Encrypted": false,
  "OwnerId": "305681518678",
  "Progress": "",
  "SnapshotId": "snap-096a35e714244ea98",
  "StartTime": "2021-04-17T21:22:48+00:00",
  "State": "pending",
  "VolumeId": "<volumeid>",
  "VolumeSize": 8,
  "Tags": []
}
```

This page intentionally left blank.

CloudTrail: Creation of Snapshot (I)

| | | |
|---------------------|--|-------------------------------------|
| useridentity | <code>{type=IAMUser, principalid=AIDAUOLAJ2BLHPNEMTP2X, arn=arn:aws:iam::305681518678:user/hpym, accountid=305681518678, invokedby=null, accesskeyid=AKIAUOLAJ2BLOJUMYJZM, username=hpym}</code> | Who requested the snapshot |
| eventtime | <code>2021-04-17T21:22:48Z</code> | When it was created |
| eventsource | <code>ec2.amazonaws.com</code> | EC2 generated the event |
| eventname | <code>CreateSnapshot</code> | Event is named CreateSnapshot |
| awsregion | <code>us-east-2</code> | Region where the snapshot is stored |

This page intentionally left blank.

CloudTrail: Creation of Snapshot (2)

Requested from a Windows 10 pc using AWS CLI

useragent

aws-cli/2.1.32 Python/3.8.8 Windows/10 exe/AMD64 prompt/off command/ec2.create-snapshot

CLI Command executed

EBS Volume Snaphotted

requestparameters {"volumeId": "vol-086eb487a26893eff" "description": "Making a snapshot"}

Snapshot ID

Not Encrypted

{ "...", "snapshotId": "snap-096a35e714244ea98", "volumeId": "vol-086eb487a26893eff", "...", "volumeSize": "8" "encrypted": false, "description": "Making a snapshot", "...

responseelements

This page intentionally left blank.

EFS – Elastic File Store



An AWS Hosted NFS Share



Allows scalable file shares for systems that support NFS



Can be mounted at boot



Great for containers and elastic host configurations

This page intentionally left blank.

CloudTrail: Mounting EFS (I)

```
"type": "AssumedRole",  
"principalId": "AROAUOLAJ2BLEGMUX2J52:523670242123",  
  "arn": "arn:aws:sts::305681518678:assumed-role/AWSServiceRoleForAmazonElasticFileSystem/523670242123",  
"accountId": "305681518678",  
  ...  
"attributes": {  
  "mfaAuthenticated": "false",  
  "creationDate": "2021-04-03T22:03:52Z"  
},  
"invokedBy": "elasticfilesystem.amazonaws.com"
```

This page intentionally left blank.

CloudTrail: Mounting EFS (2)

```
},  
  "eventTime": "2021-04-03T22:03:53Z",  
  "eventSource": "ec2.amazonaws.com",  
  "eventName": "CreateNetworkInterface",  
  "awsRegion": "us-east-1",  
  "sourceIPAddress": "elasticfilesystem.amazonaws.com",  
  "userAgent": "elasticfilesystem.amazonaws.com",  
  "requestParameters": {  
    "subnetId": "subnet-0fecba79524beb4ed",  
    "description": "EFS mount target for fs-747766c1 (fsmt-7bd116ce)",  
    "groupSet": {},  
    "privateIpAddressesSet": {}  
  }  
},
```

This page intentionally left blank.

CloudTrail: Mounting EFS (3)

```
"responseElements": {  
  "requestId": "cfcf5ado-8855-4e27-936d-c4bf6abda234",  
  "networkInterface": {  
    "networkInterfaceId": "eni-0bb4b98b581305086",  
    "subnetId": "subnet-0feebea79524beb4ed",  
    "vpcId": "vpc-09edf30a76f46ad91",  
    "availabilityZone": "us-east-1e",  
    "description": "EFS mount target for fs-747766c1 (fsmt-7bd116ce)",  
    ...  
    "macAddress": "06:62:de:b6:ca:15",  
    "privateIpAddress": "172.31.54.64",  
    "privateDnsName": "ip-172-31-54-64.ec2.internal",  
    "sourceDestCheck": true,  
  }  
}
```

This page intentionally left blank.

Lab 2.2

Finding Rogue VMs

This page intentionally left blank.

Amazon AWS Roadmap

2.1: Understanding IR in AWS

2.2: Networking, VMs and Storage

2.3: Log Sources for IR

2.4: Event Drive Response

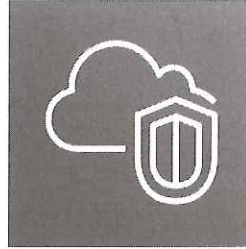
2.5: In-cloud IR

- VPC
- VPC Subnets
- Internet Gateways
- Load Balances
- VPC Flow Logs
- VPC Flow Log examples
- VPC Flow Log storage
- VPC Flow Log pricing
- **Lab 2.3: VPC Flow Logs**

This page intentionally left blank.

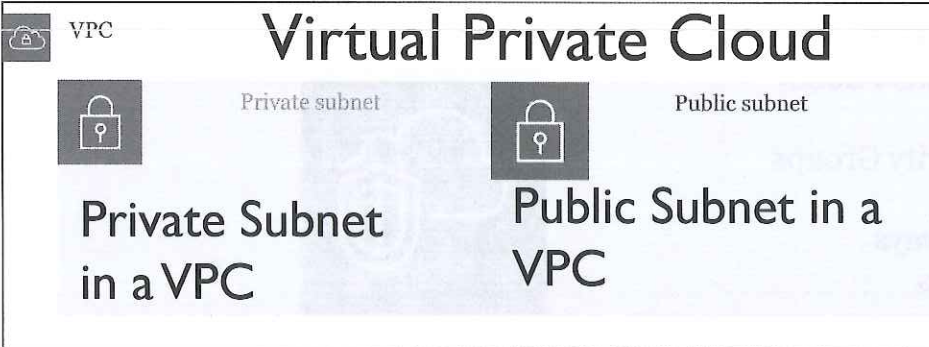
Virtual Private Cloud

- A collection of resources grouped into a group
- A VPC can contain
 - Subnets (Private/Public)
 - EC2 VMs
 - Network Security Groups
 - Proxy Servers
 - Internet Gateways
 - Load Balancers



This page intentionally left blank.

FOR509.2 – Amazon AWS cont'd.



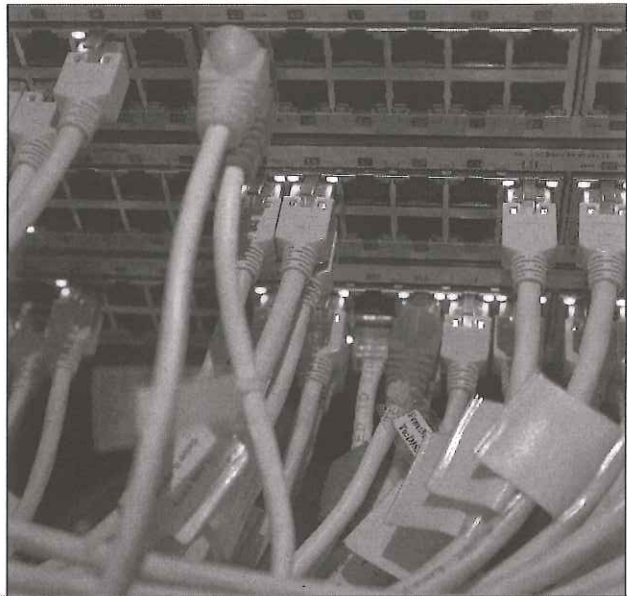
NOTE

VPCs are like a single network switch. Without any gateways they have no network access outside of the subnet.

This page intentionally left blank.

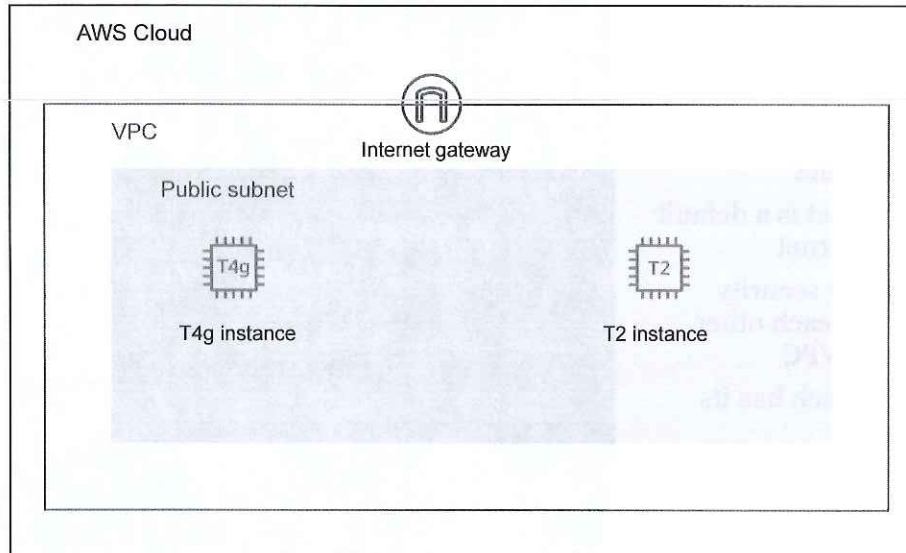
VPC Subnets

- Subnets within VPCs
 - Within a VPC you can have both public and private subnets
 - What makes a private subnet is no direct routing ability to the internet
 - What makes a public subnet is a default route that leads to the internet
 - Subnets can have different security policies and features than each other than still live in the same VPC
 - Subnets are like VLANs, each has its own IP address space
 - You can create routes between subnets, by default they are isolated



This page intentionally left blank.

Internet Gateways



NOTE

Internet gateways are what all your VPC public subnets to route to the internet. It also allows internet addresses assigned to be able to route the VPC.

This page intentionally left blank.

AWS Load Balancers

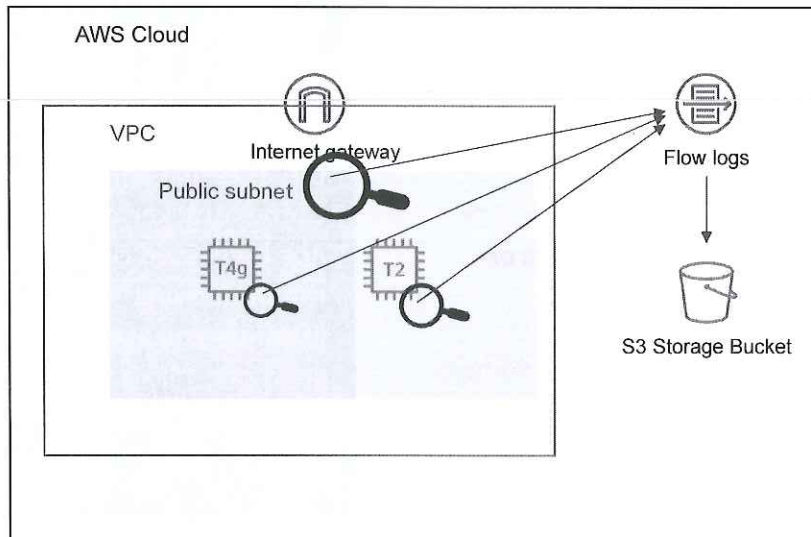
- AWS load balancers work one of four ways:
 - Application load balancer
 - Understands HTTP and can route requests between sets of web servers
 - Classic load balancer
 - Balances traffic by routing traffic based on weights or rotation
 - Network load balancer
 - Balances loads across multiple VPCs

NOTE

If a AWS load balancer is in place the external address of the attacker may not be passed on to the underlying instance you are analyzing. Make sure to get load balancer logs!

This page intentionally left blank.

VPC Flow Logs



NOTE

Flow logs can be enabled at the:

- VPC
- Subnet
- Network interface

They put no load on your network and are collected out of band.

You can enable them at any time.

This page intentionally left blank.

VPC Flow Log Examples

| | | |
|---------------------|-----------------------|---|
| version | 2 | The version of AWS Flow Log |
| account-id | 305681518678.00 | The AWS Account that this was generated in |
| interface-id | eni-06fa0119bda73bdc5 | The virtual network interface that was contacted |
| srcaddr | 209.17.96.130 | The system that sent the connection |
| dstaddr | 10.0.2.99 | The system the connection was sent to |
| dstport | 61087 | The port that was on the destination |
| sreport | 990 | The port used by the sending system |
| protocol | 6 | The protocol number in use |
| packets | 1 | The number of packets in this connection |
| bytes | 44 | The number of bytes in this connection |
| start | 1618617647 | A unix time stamp of when this connection started |
| end | 1618617703 | A unix time stamp of when this connection ended |
| action | ACCEPT | What action the network security group took |
| log-status | OK | OK |

NOTE
Flow logs record sessions every 10 minutes by default

This page intentionally left blank.

VPC Flow Log Pricing



Stored in S3 Buckets

Up to 50TB \$.023/GB



Shipped to CloudWatch

\$.50/GB up to 10TB
Scales up to 50TB at \$.05/GB

This page intentionally left blank.

Lab 2.3

VPC Flow Logs

This page intentionally left blank.

Amazon AWS Roadmap

2.1: Understanding IR in AWS

2.2: Networking, VMs and Storage

2.3: Log Sources for IR

2.4: Event Drive Response

2.5: In-cloud IR

- S3 Buckets
- S3 Buckets for Log Storage
- S3 Bucket Access Logs
- S3 Bucket Pricing
- Route 53
- **Lab 2.4: S3 Analysis**

This page intentionally left blank.

S3 Buckets

Those things you keep reading about in the news

A file share you can upload to with a web browser

S3 Names are Universal

- That means only one customer can have a s3 bucket name in all of amazon

This page intentionally left blank.

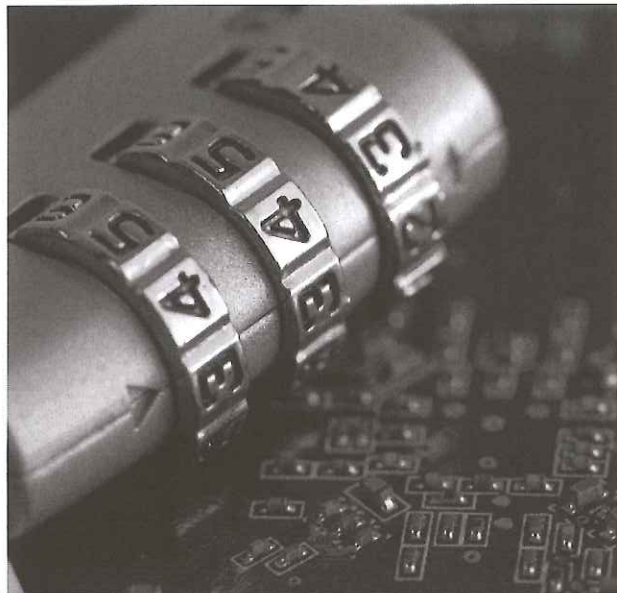
S3 Buckets – Restrictions of access

- Public
 - Anyone can access the contents
- AWS User
 - Any AWS user can access
- Org User
 - A specified user(s) can access the contents
- IAM Roles
 - Specific roles can access the contents
- Tokens in URL strings
 - Anyone with the correct link, in the specified time, can access the contents

This page intentionally left blank.

S3 Buckets – Cornerstone of AWS IR

- S3 Buckets can store
 - Snapshots
 - NetFlow logs
 - Load balancer logs
 - CloudTrail logs
 - S3 audit logs
 - Anything!



This page intentionally left blank.

S3 Buckets – Methods of DFIR Usage



Accelerated Upload with Acceleration



Searching logs with Glue and Athena



Remote Triage with Lambda Triggers

This page intentionally left blank.

S3 Bucket Access Log

| | |
|-------------------|--|
| field | Who downloaded the file |
| useridentity | {type=LAMUser, principalid=AIDAUOLAJ2B... arn=arn:aws:iam::305681518678:user/hpym, accountid=305681518678, invokedby=null, accesskeyid=AKIAUOLAJ2BLOJUMYJZM, username=hpym sessioncontext=null} |
| eventtime | The s3 operation executed |
| eventsource | s3.amazonaws.com |
| eventname | GetObject |
| awsregion | us-east-2 |
| sourceipaddress | 47.185.244.137 |
| useragent | aws-cli/2.1.32 Python/3.8.8 Windows/10 exe/AMD64 |
| requestparameters | bucketName=s3security.pymtech.com Host:s3.us-east-2.amazonaws.com, key:AWSLogs/305681518678/CloudTrail-Digest/af-south-1/2020/04/22/305681518678_CloudTrail-Digest_af-south-1_Test_us-east-1_20200422T170000Z.json.gz |
| | What was downloaded |

This page intentionally left blank.

S3 Access Log Storage Pricing

| S3 Intelligent Tiering | Cost per GB |
|---|------------------|
| Frequent Access Tier, First 50 TB / Month | \$0.023 per GB |
| Frequent Access Tier, Next 450 TB / Month | \$0.022 per GB |
| Frequent Access Tier, Over 500 TB / Month | \$0.021 per GB |
| Infrequent Access Tier, All Storage / Month | \$0.0125 per GB |
| Archive Access Tier, All Storage / Month | \$0.004 per GB |
| Deep Archive Access Tier, All Storage / Month | \$0.00099 per GB |

NOTE

S3 data access logs won't appear in the CloudTrail console.

You have to parse the CloudTrail logs in a tool like Athena to view data/object logs. API Events will appear in the CloudTrail console.

This page intentionally left blank.

Route 53 – AWS DNS

- Amazon's Hosted DNS Service
- DNS Zone Query Logging
 - Log queries made to your hosted DNS Domains
- Route 53 Resolver Query Logs
 - Log all DNS queries made within your VPC



This page intentionally left blank.

Lab 2.4

S3 Analysis

This page intentionally left blank.

FOR509.2 – Amazon AWS (3)

Section 2.1: Understanding AWS

Section 2.2: Networking, VMs and Storage

Section 2.3: Log Sources for IR

Section 2.4: Event Driven Response

Section 2.5: In Cloud IR

This page intentionally left blank.

Amazon AWS Roadmap

2.1: Understanding IR in AWS

2.2: Networking, VM and Storage

2.3: Log Sources for IR

2.4: Event Drive Response

2.5: In-cloud IR

- AWS Log Sources
- AWS Athena
- AWS Glue
- AWS Glue Syntax
- AWS/Glue Pricing
- AWS Security Hub
- AWS Detective
- **Lab 2.5: Tracking Lateral Movement**

This page intentionally left blank.

AWS Logs Sources

CloudTrail

- Tenant Audit Logs

CloudWatch Logs

- Forwarded Logs from applications and endpoints

CloudWatch Logs Insights

- Metrics and patterns

Guard Duty

- Anomaly detection within CloudTrail

VPC Flow Logs

- NetFlow logs from your virtual private clouds

S3 Logs

- Logs from data storage access

1. Tenant logs
2. Network logs
3. Storage logs

Can I do it in one slide for all three clouds???

AWS Athena

The screenshot displays the AWS Athena console interface. On the left, the 'Data source' is set to 'AwsDataCatalog' and the 'Database' is 'default'. Below this, a list of tables is shown, including 'cloudtrail_logs_for50993116'. The main area contains a query editor with the following SQL query: `select * from cloudtrail_logs_for50993116 where eventName like '%GetObject%' and userAgent not like '%SANS Ince...'`. The query has been executed, with a run time of 1 minute 43 seconds and 4.45 GB of data scanned. The results are displayed in a table with columns 'eventversion' and 'useridentity'. Three rows of data are visible, all with 'eventversion' set to 1.00 and 'useridentity' containing detailed AWS IAM information.

| eventversion | useridentity |
|--------------|---|
| 1.00 | {type=Root, principalId=305681618676, iam=arn:aws:iam::305681618676:root, accountId=305681618676, invokedBy=athena.amazonaws.com, accessKeyId=ASIAJEWELY2ZVTRUJYDA, username=pyntech} |
| 1.00 | {type=Root, principalId=305681618676, iam=arn:aws:iam::305681618676:root, accountId=305681618676, invokedBy=athena.amazonaws.com, accessKeyId=ASIAJIC3JCSIKCIJCH8Q, username=pyntech} |
| 1.00 | {type=Root, principalId=305681618676, iam=arn:aws:iam::305681618676:root, accountId=305681618676, invokedBy=athena.amazonaws.com, accessKeyId=ASIAJIC3JCSIKCIJCH8Q, username=pyntech} |

This page intentionally left blank.

AWS Glue Interface

Tables > cloudtrail Last updated 17 Apr 2021 04:32 PM **Table** Version (Current version) ▾

Edit table Delete table Partitions and indices View partitions Compare versions Edit schema

| | |
|-------------------------|---|
| Name | cloudtrail |
| Description | |
| Database | cloudtraillogs |
| Classification | cloudtrail |
| Location | s3://for509trais/AWSLogs/305681518678/CloudTrail/ |
| Connection | |
| Deprecated | No |
| Last updated | Sat Apr 17 16:32:37 GMT-500 2021 |
| serde parameters | - |

Table properties

| | | | | | |
|----------------------------------|------------|--------------------------------|--------|------------|---------------|
| sizeKey | 4109757944 | objectCount | 128793 | | |
| UPDATED_BY_CRAWLER | TrailGlue | CrawlerSchemaSerializerVersion | 1.0 | | |
| recordCount | 1786914 | averageRecordSize | 1221 | jsonPath | \$.Records[*] |
| CrawlerSchemaDeserializerVersion | 1.0 | compressionType | gzip | typeOfData | file |

SANS DFIR FOR509 | Enterprise Cloud Forensics & Incident Response 85

This page intentionally left blank.

AWS Glue Syntax

```
CREATE EXTERNAL TABLE  
[TABLE_NAME] (  
  eventVersion STRING,  
  userIdentity STRUCT<  
    type: STRING,  
    principalId: STRING,  
    arn: STRING,  
    accountId: STRING,  
    invokedBy: STRING,  
    accessKeyId: STRING,  
    userName: STRING,  
  ...
```

Glue allows you to format, convert, enrich and combine data sources for Athena to search

Glue creates the tables/partitions that Athena will search across

Glue can define schemas like date and time against specific log fields

CloudTrail has a predefined Glue data set

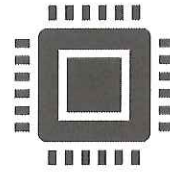
This page intentionally left blank.

AWS Athena/Glue Pricing



Athena Searching

\$5 per TB scanned while searching
Failed queries are not charged



Glue Crawling

\$0.44 per DPU (Data Process Unit) hour
DPUs have 4 CPUs and 16GB of memory.
10 minute minimum billed

This page intentionally left blank.

Security Hub

The screenshot shows the AWS Security Hub console. On the left is a navigation sidebar with options: Summary, Security standards, Insights, Findings, Integrations, Settings, and What's new. The main content area is titled 'Summary' and is divided into two columns. The left column, 'Insights', lists five items with a 'Results' column showing zero findings for each. The right column, 'Latest findings from AWS integrations', lists several AWS services with a 'No findings' status for each.

| Insights | Results |
|---|---------|
| 1. AWS resources with the most findings | 0 |
| 2. S3 buckets with public write or read permissions | 0 |
| 3. AMIs that are generating the most findings | 0 |
| 4. EC2 instances involved in known Tactics, Techniques, and Procedures (TTPs) | 0 |
| 5. AWS principals with suspicious access key activity | 0 |

| Latest findings from AWS integrations | Results |
|--|-------------|
| Amazon GuardDuty Open the GuardDuty console ↗ | No findings |
| Amazon Inspector Open the Inspector console ↗ | No findings |
| Amazon Macie Open the Macie console ↗ | No findings |
| AWS IAM Access Analyzer Open the IAM Access Analyzer console ↗ | No findings |
| AWS Systems Manager Patch Manager Open the Systems Manager Patch Manager console ↗ | No findings |
| AWS Firewall Manager Open the Firewall Manager console ↗ | No findings |

This page intentionally left blank.

Security Hub Pricing

- Security Checks
 - First 100,000 \$.0010/check
 - $\geq 500,000$ \$.0008/check
 - $>500,000$ \$.0005/check
- Ingestion Events
 - First 10,000 Free
 - $>10,000$ \$.00003/finding

This page intentionally left blank.

AWS Detective

Detective ×

Summary
Search

▼ Settings

Account management
General
Preferences
Usage

What's new 11
Getting started
Video tutorials

Detective > Summary

Summary Info

The Detective Summary page helps you to identify entities that you might want to view additional details for. It provides another starting point for an investigation.

Roles and users with the most API call volume in the past 24 hours Info

| Principal (role or user) | AWS account | Trend (7 days) | Success ▼ | Failure ▼ | Total |
|--------------------------|-------------|----------------|------------------------|------------------------|-------|
| No results to display | | | | | |

EC2 instances with the most traffic volume in the past 24 hours Info

| EC2 instance | AWS account | Trend (7 days) | Bytes in ▼ | Bytes out ▼ | Total |
|-----------------------|-------------|----------------|-------------------------|--------------------------|-------|
| No results to display | | | | | |

Newly observed geolocations in the past 24 hours Info

This page intentionally left blank.

AWS Detective Pricing

- Ingested Logs per GB
 - $\leq 1,000$ GB \$2/GB
 - $\leq 5,000$ GB \$1/GB
 - $\leq 10,000$ GB \$.50/GB
 - $>10,000$ GB \$.25/GB

This page intentionally left blank.

Lab 2.5

Tracking Lateral Movement

This page intentionally left blank.

FOR509.2 – Amazon AWS (4)

Section 2.1: Understanding AWS

Section 2.2: Networking, VMs and Storage

Section 2.3: Log Sources for IR

Section 2.4: Event Driven Response

Section 2.5: In Cloud IR

This page intentionally left blank.

Amazon AWS Roadmap

2.1: Understanding IR in AWS

2.2: Networking, VM and Storage

2.3: Log Sources for IR

2.4: Event Drive Response

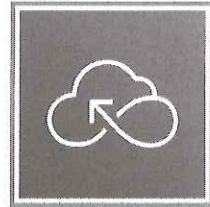
2.5: In-cloud IR

- Lambda Functions
- Lambda Pricing
- Step Functions
- Step Functions Pricing
- Event Triggers
- Event Driven DFIR Automation

This page intentionally left blank.

Lambda Functions

- Lambda is AWS's version of Serverless functions
- Lambda functions can be written in several languages
 - Java
 - Go
 - PowerShell
 - Node.js
 - C#
 - Python
 - and Ruby



This page intentionally left blank.

Lambda Pricing



\$.20 per 1 Million Requests

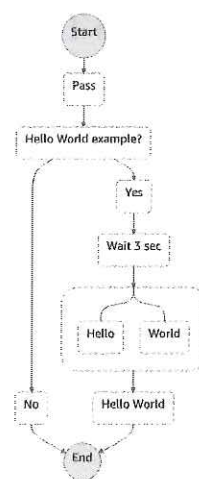


Also charged \$0.0000166667 for every GB of ram used per second the function runs

This page intentionally left blank.

Step Functions

- Step functions allows you to chain lambda functions into a workflow where the prior output is the input for the next step.
- This allows you to divide your workflow into fast and cheap running lambda functions and build a larger IR automation tool.



This page intentionally left blank.

Step Functions Pricing

- 4,000 State Transitions are Free per month
- More than 4,000 state transactions are \$.025 per 1,000 state transactions

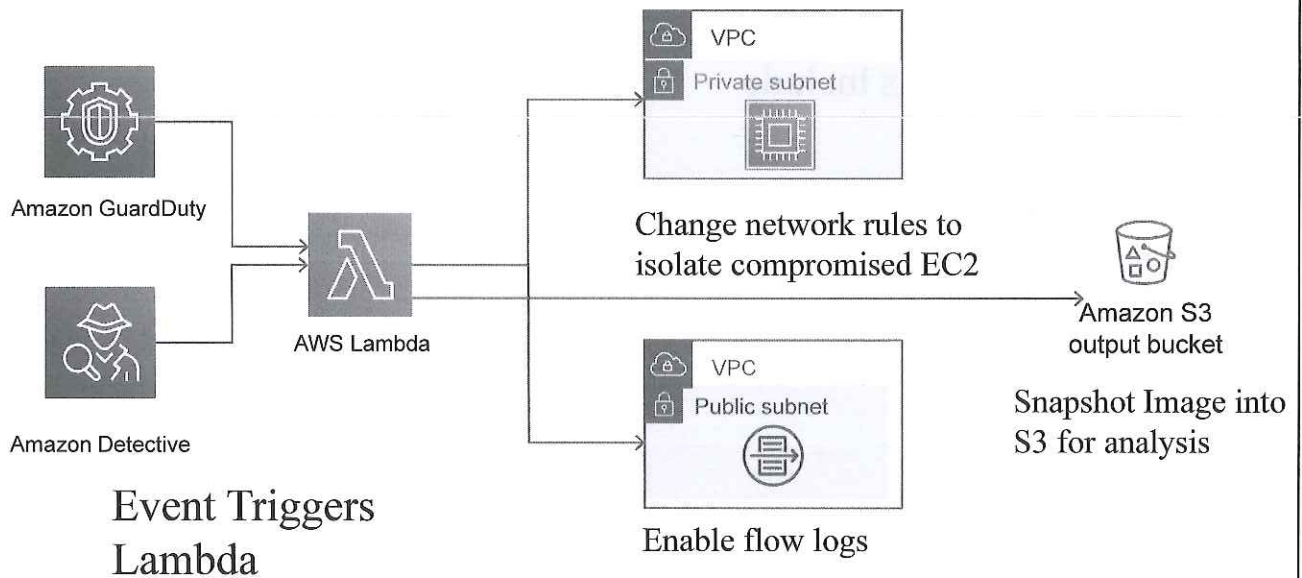
This page intentionally left blank.

Event Triggers

- Lambda functions can be triggered with AWS events
- Examples of Events include
 - S3 Uploads
 - CloudTrail events
 - EC2 Changes
 - EFS Changes
 - Amazon Config changes

This page intentionally left blank.

Event Driven DFIR Automation



This page intentionally left blank.

FOR509.2 – Amazon AWS (5)

Section 2.1: Understanding AWS

Section 2.2: Networking, VMs and Storage

Section 2.3: Log Sources for IR

Section 2.4: Event Driven Response

Section 2.5: In Cloud IR

This page intentionally left blank.

Amazon AWS Roadmap

2.1: Understanding IR in AWS

2.2: Networking, VM and Storage

2.3: Log Sources for IR

2.4: Event Drive Response

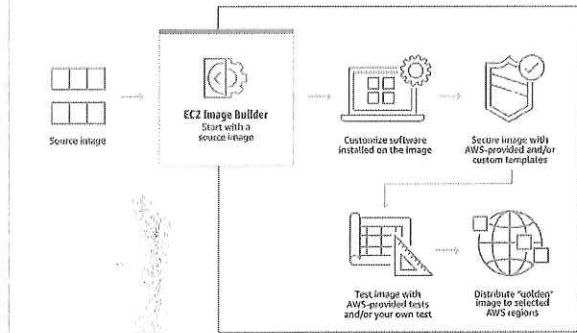
2.5: In-cloud IR

- Creating IR VMs
- AMI and IR
- In cloud vs On Prem
- Downloading AMIs
- AWS Systems Manager
- Capturing Linux Memory
- Capturing Windows Memory
- Accessing Snapshots
- Isolating compromised hosts
- ECS, EKS, ECR
- **Lab 2.6: Container Investigations**

This page intentionally left blank.

Creating IR VMs

How it works



Amazon makes it easy to create a custom IR VM

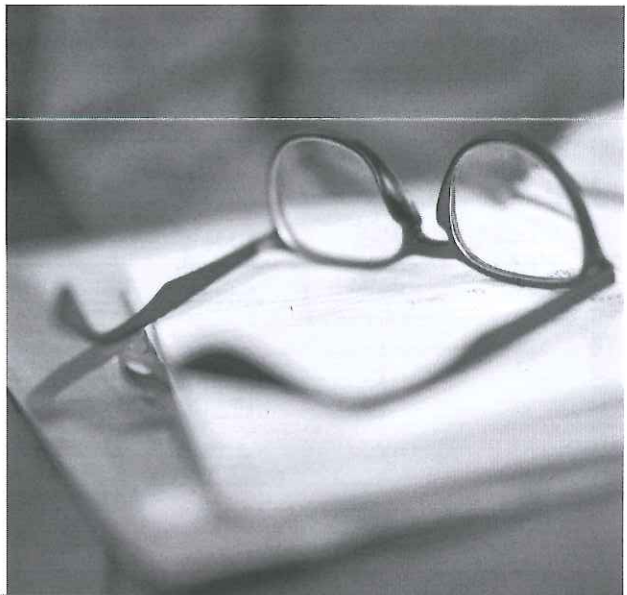
The EC2 Image Builder lets you pick a base image (Windows, Linux, etc..)

You can then configure the base system and then upload them as a template for your organization to deploy on demand anywhere in the world.

This page intentionally left blank.

AMIs and IR

- AMIs can be examined in two ways
 - Within AWS
 - You can snapshot the running system and attach it to a DFIR AMI that is running
 - Run all of your tools against the Snapshots
 - Snapshots are basically raw disks that can be accessed like a DD Image
 - Outside of AWS
 - You can snapshot the running system and then download the data
 - You can power off the running system and download the AMI
 - The time to download could be longer than it takes to do the examination within AWS



This page intentionally left blank.

In cloud vs. On Prem AMI examination

In Cloud

- Pros
 - Fastest time to access data
 - Able to process and load data using Amazon provided services:
 - Elastic auto scaling clusters
 - Athena for log searching
 - Containers for scalable processing
 - On demand DFIR lab anywhere in the world
- Cons
 - Cost for every examination
 - If the entire organization is compromised your DFIR account may be too

On Prem

- Pros
 - After initial investment in hardware, software and people there is no cost per incident to run the DFIR systems.
 - Isolated labs can be outside of compromised cloud environment
- Cons
 - Time to download cloud data
 - Time to process data
 - Data speeds can be slower on international transfers
 - Infrastructure maintenance costs

This page intentionally left blank.

Downloading AMIs

- Requires an S3 bucket to write to
- Requires the AWS CLI
- Exporting an Instance

```
aws ec2 create-instance-export-task --instance-id instance-id --target-environment vmware --export-to-s3-task file://C:\file.json
```

- Exporting an AMI

```
aws ec2 export-image --image-id ami-id --disk-image-format VMDK --s3-export-location S3Bucket=my-export-bucket,S3Prefix=exports/
```

This page intentionally left blank.

AWS Systems Manager

AWS Systems Manager

Quick Setup

Operations Management

Explorer

OpsCenter

CloudWatch Dashboard

PHD

Application Management

Application Manager ^{New}

AppConfig

AWS Systems Manager > Run Command > Run a command

Run a command

Command document

Select the type of command that you want to run.

Search by keyword or filter by tag or attributes

| Name | Owner | Platform types |
|--|--------|----------------|
| <input checked="" type="radio"/> AWS-ApplyAnsiblePlaybooks | Amazon | Linux |
| <input type="radio"/> AWS-ApplyChefRecipes | Amazon | Windows, Linux |

This page intentionally left blank.

Capturing Linux Memory

Margarita Shotgun

- <https://github.com/ThreatResponse/margaritashotgun>
- Logs into a running EC2 instance via SSH and runs LiME to capture memory

AVML and AWS Systems Manager

- AWS Systems Manager allows you to execute commands across instances that have the system manager agent installed
- AVML can be statically compiled meaning it does not require compromised systems have kernel headers

This page intentionally left blank.

Capturing Windows Memory

AWS Systems Manager

- Deploy your favorite tool to capture ram, write out to a mounted share

Endpoint Tools

- Many endpoint agents will allow remote memory capture, if installed

PSEXec

- Push out your favorite memory capture tool, if there is no AWS Systems Manager agent installed

This page intentionally left blank.

Accessing Snapshots from DFIR AMIs

- First you need to create a volume out of the snapshot

```
aws ec2 create-volume --availability-zone <zone where your DFIR AMI is running> --snapshot-id <snapshot-id>
```

- Second you have to attach it to your running EC2 instance

```
aws ec2 attach-volume --volume-id <volume id returned from prior command> --instance-id <your DFIR EC2 instance> --device </dev/sdX>
```

This page intentionally left blank.

Isolating Compromised Hosts

- Need to isolate a compromised host?
 - Virtual firewalls can be configured on demand
 - Lambda to change ec2 security group

```
def modifyInstanceAttribute(instanceId,securityGroupId):  
    response = ec2Client.modify_instance_attribute(  
        Groups=[securityGroupId], InstanceId=instanceId)
```

- Lambda to place it in the isolated security group

```
def createSecurityGroup(groupName, descriptionString, vpcId):  
    resource = boto3.resource('ec2')  
    securityGroupId = resource.create_security_group(GroupName=groupName,  
        Description=descriptionString, VpcId=vpcId)  
    securityGroupId.revoke_egress(IpPermissions= [{'IpProtocol': '-  
1', 'IpRanges':    [{'CidrIp': '0.0.0.0/0'}], 'Ipv6Ranges':  
[], 'PrefixListIds': [], 'UserIdGroupPairs': []}])  
    return securityGroupId.
```

Reference: <https://aws.amazon.com/blogs/security/automate-amazon-ec2-instance-isolation-by-using-tags/>

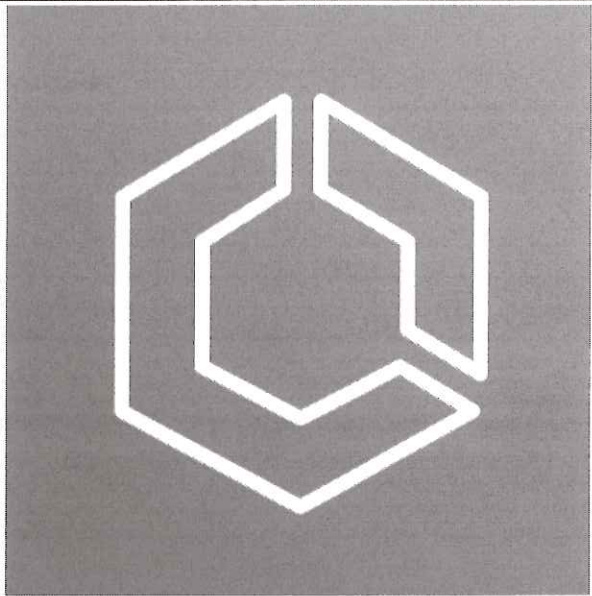
Regions and Response

- Regions Matter!
- Every region is physically resident in the country it's named after
- Transferring data between regions:
 - Takes time
 - Costs money
- Consider spinning up your DFIR AMIs in the region where you want to analyze the data

This page intentionally left blank.

ECS - Elastic Container Service

- Amazon's version of Kubernetes
- Allows for a lower overhead container cluster
- Runs docker containers at scale and manages spinning up more as needed.



This page intentionally left blank.

Container Registry

Amazon Container Services



Amazon ECS

Clusters

Task definitions

Amazon EKS

Clusters

ECR > Repositories

Private

Public

Private repositories (1)

Find repositories

Repository name

URI



dfir-containers



305681518678.dkr.ecr.us-east-1.amazonaws.com/dfir-containers

This page intentionally left blank.

EKS – Elastic Kubernetes Service

- The real Kubernetes
 - Requires more administration than ECS
 - Can spin up any number of containers from the container registry



This page intentionally left blank.

Most Common Container Investigations

Vulnerable applications from the AWS Marketplace

- Many developers will launch preconfigured container applications from the AWS Marketplace
- Many of these preconfigured applications are out of date and can be launched with known exploitable services

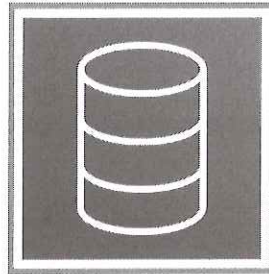
Stolen IAM roles through the Metadata service

- Once an attacker has access to the container environment, they can reach the Metadata service unless the NSG prevents it
- Always available at <http://169.254.169.254/latest/meta-data/>
- Once accessed IAM roles and credentials applied to the instance can be stolen

This page intentionally left blank.

Amazon Hosted Databases

- Rather than running a database in EC2 Amazon provides hosted databases where you only must manage the data within them.
- Databases supported:
 - Amazon Aurora
 - PostgreSQL
 - MySQL
 - MariaDB
 - Oracle Database
 - MS SQL Server



This page intentionally left blank.

Lab 2.6


Container Investigations

This page intentionally left blank.

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

 SANSForensics

 dfir.to/DFIRCast


 @SANSForensics



OPERATING SYSTEM & DEVICE IN-DEPTH

 FOR308
Digital Forensics Essentials


 FOR498
Battlefield Forensics
& Data Acquisition
GBFA


 FOR500
Windows Forensic Analysis
GCFA


 FOR518
Mac and iOS Forensic Analysis
& Incident Response

 FOR585
Smartphone Forensic
Analysis In-Depth
GASF

INCIDENT RESPONSE & THREAT HUNTING

 FOR508
Advanced Incident
Response, Threat Hunting,
& Digital Forensics
GCFA

 FOR572
Advanced Network Forensics:
Threat Hunting, Analysis,
& Incident Response
GNFA

 FOR578
Cyber Threat Intelligence
GCTI

 FOR610
REM: Malware Analysis
Tools & Techniques
GREM

 SEC504
Hacker Tools,
Techniques, Exploits,
& Incident Handling
GCIH

This page intentionally left blank.

Course Resources and Contact Information

Here is my lens. You know my methods. —Sherlock Holmes



AUTHOR CONTACT

David Cowen
dlcowen@gmail.com
Twitter: @hecfblog



SANS INSTITUTE

11200 Rockville Pike, Suite 200
North Bethesda, MD 20852
301.654.SANS(7267)



DFIR RESOURCES

digital-forensics.sans.org
Twitter: @sansforensics



SANS EMAIL

GENERAL INQUIRIES: info@sans.org
REGISTRATION: registration@sans.org
TUITION: tuition@sans.org
PRESS/PR: press@sans.org

Author: David Cowen

Email: dlcowen@gmail.com

Twitter: @hecfblog

"As usual, SANS courses pay for themselves by Day 2. By Day 3, you are itching to get back to the office to use what you've learned."

Ken Evans, Hewlett Packard Enterprise - Digital Investigation Services

SANS Programs sans.org/programs

GIAC Certifications
Graduate Degree Programs
NetWars & CyberCity Ranges
Cyber Guardian
Security Awareness Training
CyberTalent Management
Group/Enterprise Purchase Arrangements
DoDD 8140
Community of Interest for NetSec
Cybersecurity Innovation Awards



Search SANSInstitute

SANS Free Resources sans.org/security-resources

- E-Newsletters
 - NewsBites*: Bi-weekly digest of top news
 - OUCH!*: Monthly security awareness newsletter
 - @RISK*: Weekly summary of threats & mitigations
- Internet Storm Center
- CIS Critical Security Controls
- Blogs
- Security Posters
- Webcasts
- InfoSec Reading Room
- Top 25 Software Errors
- Security Policies
- Intrusion Detection FAQ
- Tip of the Day
- 20 Coolest Careers
- Security Glossary

SANS Institute

8120 Woodmont Avenue | Suite 310

Bethesda, MD 20814

301.654.SANS(7267)

info@sans.org

<https://t.me/learningnets>