

509.4 Google Cloud Platform

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.

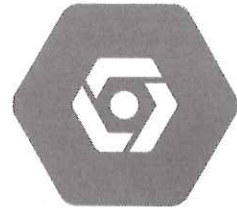
SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

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.



Google Cloud Platform



© 2021 Josh Lemon | All Rights Reserved | Version G01_01

This page intentionally left blank.

SANS DFIR

DIGITAL FORENSICS & INCIDENT RESPONSE

f 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
GCTA



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
GCHH

This page intentionally left blank.

FOR509.4 – Google Cloud Platform (GCP)

Section 4.1: Understanding GCP

Section 4.3: Log Sources, Collection & Log Routing

Section 4.2: VM & Storage Investigations

Section 4.4: GCP Network Forensics

This page intentionally left blank.

Purpose of this Section

- The purpose of this section is to gain a basic understanding of key Google Cloud Platform (GCP) resources and logs to facilitate incident response and digital forensics
- Become familiar with evidence available for virtual machines, networking, and storage
- Understand how platform logs are generated, routed, and stored within GCP
- Understand Log Explorer and importing logs into SOF-ELK
- Discuss various attacks on GCP

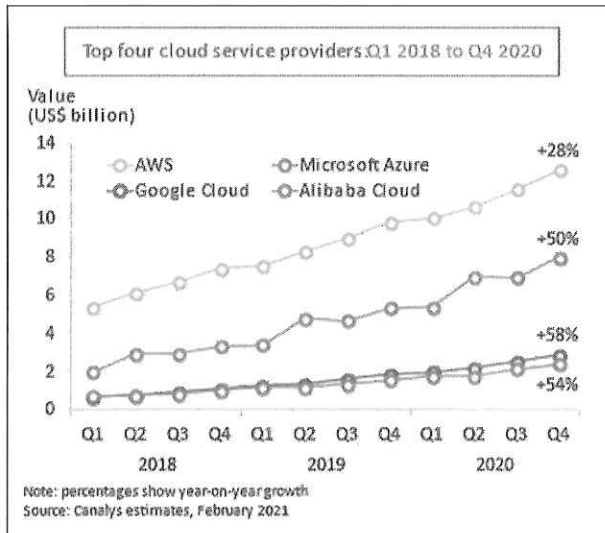
GCP is very similar to the other three main Cloud platforms that have been shown already. However, as you have seen with the other Cloud platforms each of them have slightly different terminologies and services that are useful from an investigation perspective. In this section we will examine the logs and services available to investigators. We will also review how logs work in general within GCP and how to alter what is logged and how to forward, or ship, those logs to other locations.

This section will again focus on extracting logs out of the Google Cloud Platform and moving them into SOF-ELK for analysis. While there are many different scenarios this could work in practice, we'll continue to use SOF-ELK to show the overall principals which would allow investigators in the field to adapt these techniques as needed for their environment.

Additionally, we will also look at some common attacks that can occur in GCP. While this will not be an extensive list, it is intended to again show you techniques for leveraging GCP's infrastructure and services so you can adapt this as needed in the field.

By the end of this section, you will have a strong understanding of the logging capabilities in GCP. This will provide you a solid foundation to conduct incident response and forensics in your environment.

Why We're Covering What We're Covering



- GCP is the third largest cloud provider after AWS and Azure
- While the third largest cloud is has seen the largest growth in the past year compared to AWS or Azure.
- As with other Cloud platforms organizations are forecast to grow their cloud spend by 18.4% in 2021
- This sets up Cloud infrastructure to be in the cross-hairs of threat actors

GCP is currently seen as the third most used cloud platform as of Q4 in 2020^[1], behind AWS and Azure. However, it is the cloud platform that is seeing the fastest increase in customers making the fastest growing platform as well^[1].

Cloud platforms as a whole are seeing an increase growth, with end-users forecast to grow their use of the cloud by 18.4% in 2021^[2]. Although SaaS (Software as a Service) is the largest growing area within the cloud, other services such as PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) as followed closely behind^[2]. It is due to this we try to cover a cross sections of these platforms within this section with a focus on the areas that Enterprises are most focused on from an incident response perspective.

References:

[1] <https://for509.com/xr0ai>

[2] <https://for509.com/yx381>

Google Cloud Platform Roadmap

4.1: Understanding GCP

4.2: Log Sources, Collection & Log Routing

4.3: VM & Storage Investigations

4.4: GCP Network Forensics

- Google Cloud
- Global Footprint
- Organizations
- GCP Resources
- Pricing Structure
- GCP Identity and Access Management
- Challenges with IAM
- **Lab 3.1: GCP IAM and Access Tracking**

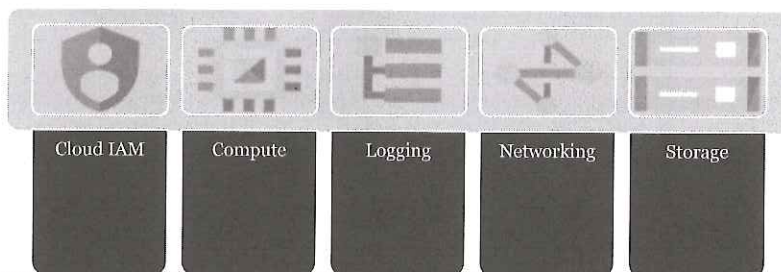
This page intentionally left blank.

Google Cloud

“Today, most of the world's enterprise computing still happens on-premise. It hasn't moved to the cloud yet, because the path forward is complex and daunting, and full of difficult decisions. How do you modernize in-place without having to jump completely to the cloud? How do you bridge incompatible architectures while you transition? And how do you maintain flexibility and avoid lock-in?”

Sundar Pichai, Google's CEO (2019)

Key services for
incident response
and forensics:



Before we can deep dive into digital forensics in GCP we need to discuss some of the fundamentals to GCP to ensure everyone understands the terms and language used to describe different items and objects within GCP. Once we have some of these fundamentals covered, we're going to focus on the five services that offer the most useful digital forensics value when an incident has occurred within GCP, this will include;

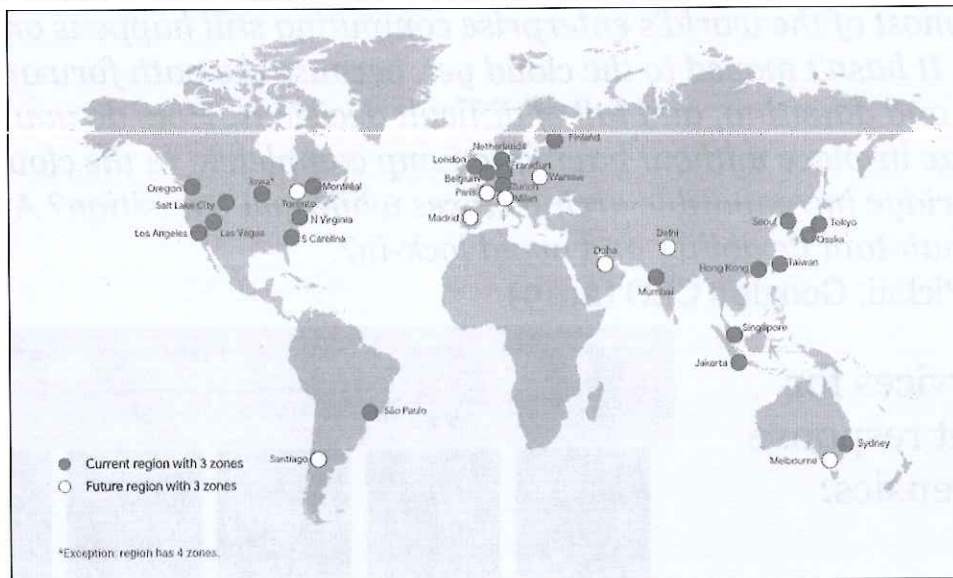
- GPC Identify and Access Management
- GCP Compute or also known as Virtual Machines
- GCP's Logging Platform
- GCP Networking and the Services within Networking, and
- GCP Storage Buckets

To start with, let's go back to 2019 when the current Google CEO, Sundar Pichai, addressed the Google Cloud Next 2019 Conference. During this address Sundar presented to the attendees a challenge with cloud computing as a whole – how do you produce a cloud platform without locking in customers and making it continually flexible to be used. It is this challenge that Sundar presented that you will see appear within the GCP platform to ensuing services are flexible to the end-user, this will become obvious when we start to look at host OS logging that does not even need to exist within GCP for the GCP Logging Platform to use it.

References:

- [1] Sundar Pichai, Google's CEO, Google Cloud Next 2019 Conference in April 2019

GCP Global Footprint (I)



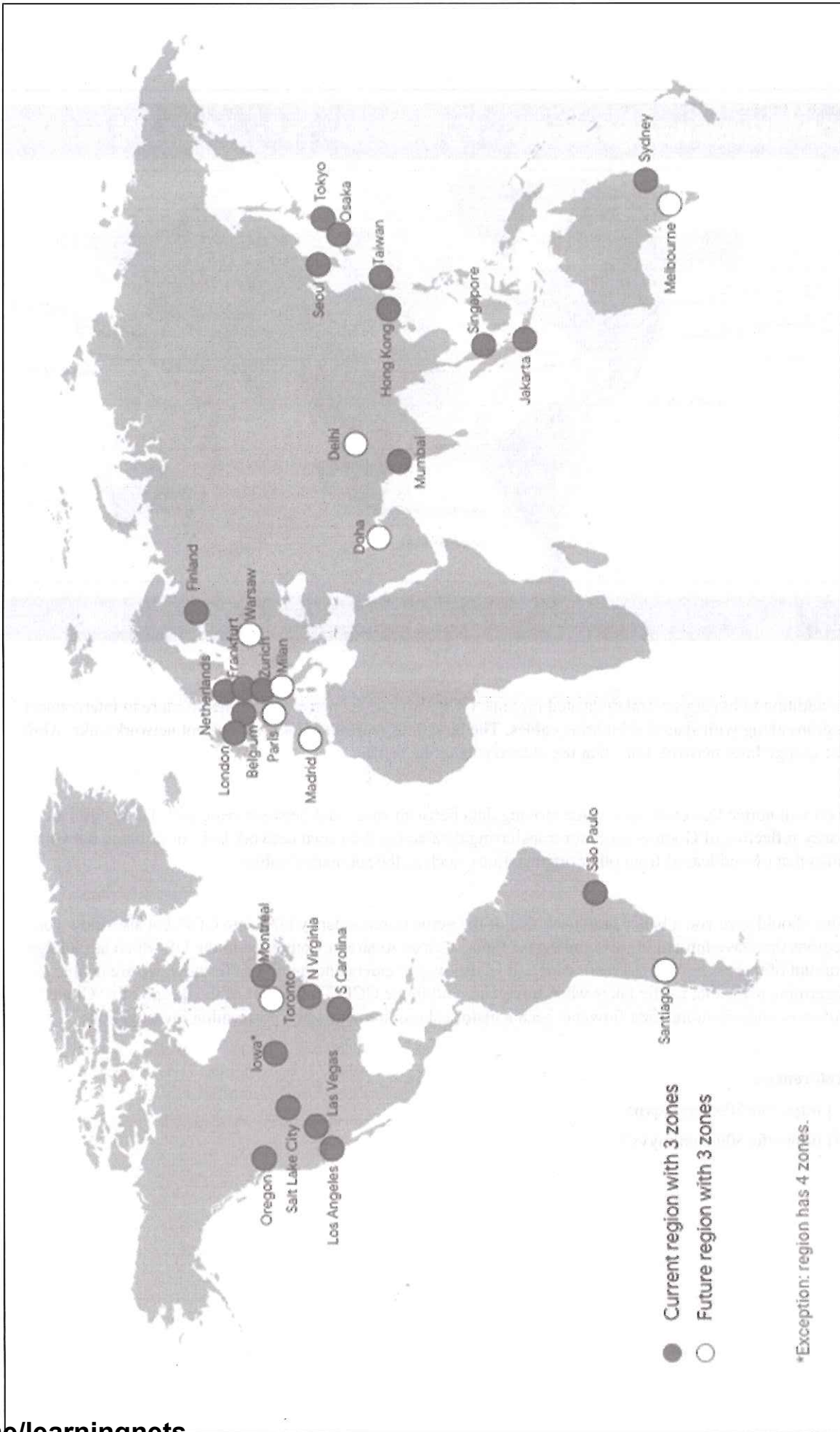
As for GCP's overall global footprint, at the time of publishing, GCP had 25 different regions which included 76 zones. Even at the time of publishing this course, GCP currently has listed additional countries and regions which will likely be in production by the time you are reading this.

While the majority of core services are in each zone and region, some specific services aren't included in every region. This can be for a variety of reasons, including licensing issues within a region, physical space to introduce additional equipment to cater for more specialized services.

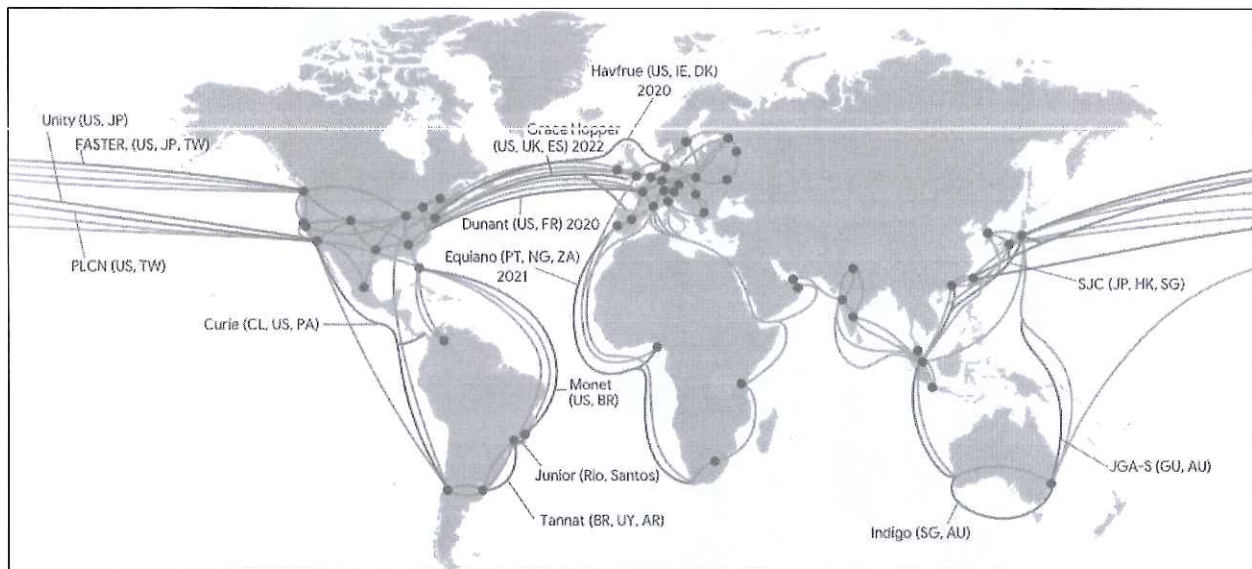
While GCP's overall platform will seem relatively transparent when you're looking at the console, to be mindful of any data residency issues or regulation issues with where you are storing and processing data. This in particular is important when you're moving data around for digital forensics or evidence processing.

Reference:

[1] <https://for509.com/hqvn5>



GCP Global Footprint (2)



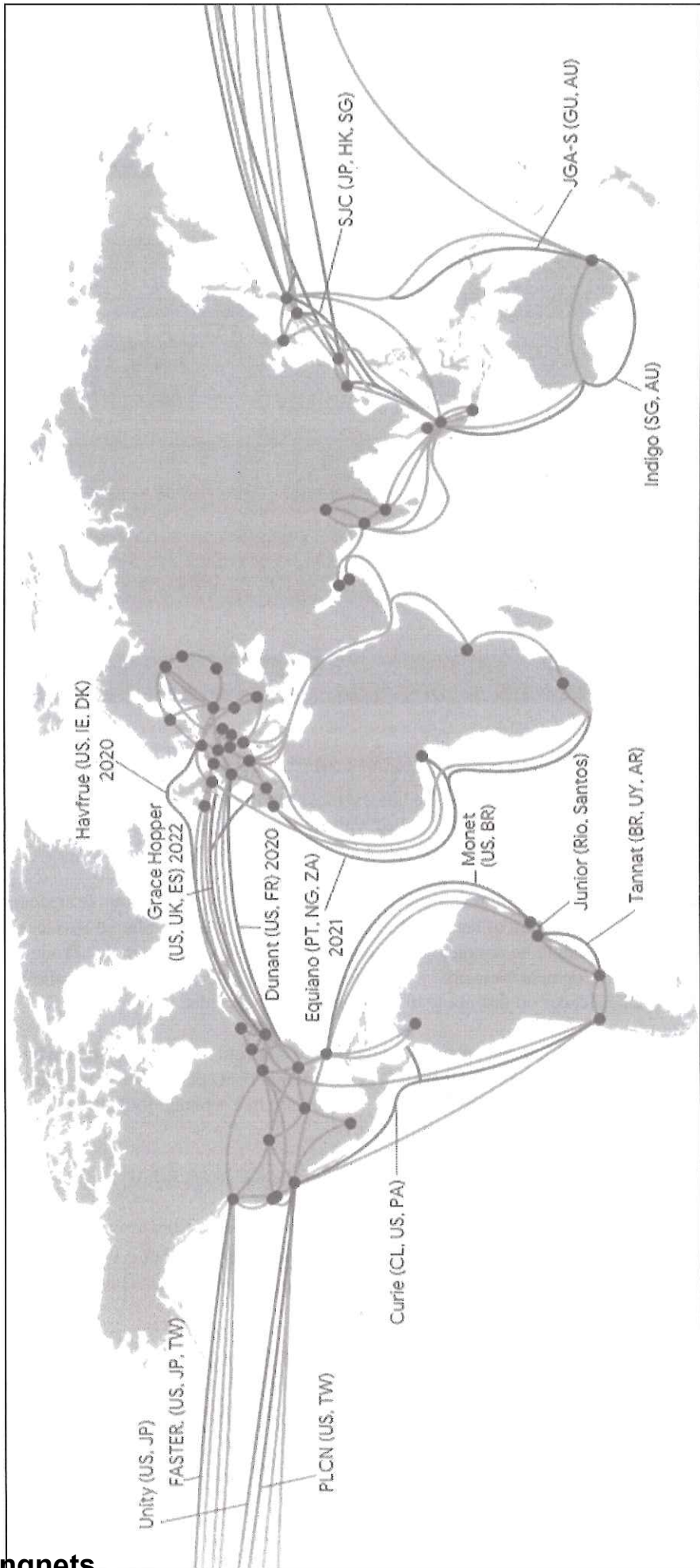
In addition to having several dedicated regions, GCP also uses its networking infrastructure to interconnect regions along with shared submarine cables. The blue lines represent Google's current network links, while the orange lines network links that use shared submarine cables.

You will notice that costs vary when moving data between zones and between regions^[2]. These costs are partly reflective of Google's costs for transferring data across their own network links or utilizing network links that owned/leased from other organizations, such as the submarine cables.

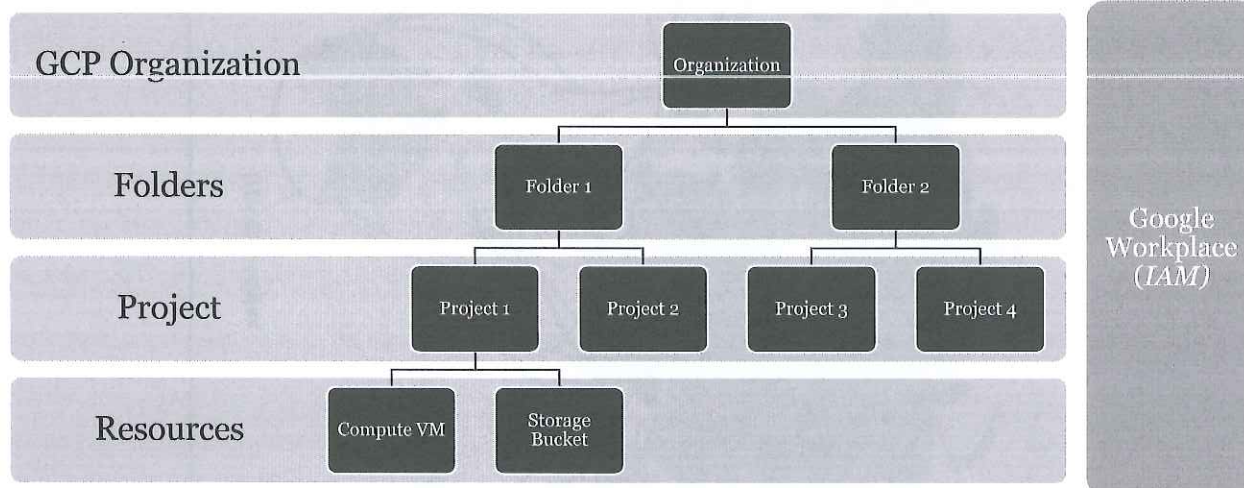
This should give you a better graphical idea of the network redundancy built into GCP, but also show you regions that have limited ingress and egress links, such as Australia, compared to the US which has a large amount of ingress and egress redundancy. It is also worth understanding that as for now, we are unable to determine paths that traffic takes when traversing within the GCP. This is part of the design of a "Cloud" however understanding data flow has been a historical requirement when performing investigations.

References:

- [1] <https://for509.com/hqvn5>
- [2] <https://for509.com/myvs2>



GCP Organizations Overview



The GPC Organization is the root of how objects and services are assigned and ordered within a GCP instance. The “**Organization**” is considered the highest most parent in the overall structure. This object is usually a domain main (example.com), and if linked with Google Workspace, would also be the primary domain that is used in your Google Workspace.

Underneath an Organization are “**Folders**”, these are used to logically order or group teams/departments together. These could be in the form of teams, for example an “R&D Team”, “Shared Services”, and “Customer Services”. Or it could be arranged based on logical boundary, for example “Production Network”, “Staging Network”, “Development Network”. The grouping of folders is significant as it allows an Organization to set policies later on that apply to everything within a folder.

For a digital forensics and incident response team, you would expect to have your evidence processing services within a folder separate from all other folders. Additional concepts on this will be discussed further into this section, however, understand that if your DFIR team are in a separate folder they can have policies separated from other teams which maybe more restrictive.

You can have multiple layers of folders to also give you sub-folders, or sub-teams, if you need to further break down the structure of teams within GCP.

“**Projects**” are logical groups of services within GCP that are run by a team that is within a Folder. Projects are the item you group your running services within GCP to. Projects are also used for billing purposes to track spend on the services consumed within GCP.

The lowest level of objects within an Organization are the GCP “**Resources**”, these are the services that you use within GCP and generally have a cost associated with them. Resources inherit permissions from policies that are applied to Folders and Projects. The use of Resources are billed against a Project.

References:

[1] <https://for509.com/gt8s9>

GCP Organizations In Practice

Organization

Folder (Level 1)

Sub-Folder (Level 2)

Project

Name	ID
longconsecurity.com	1021459341713
Futures Lab	543351784754
Bio Testing Lab	773148157163
Yellow Jacket	632199294359
Flight-Control-Nav	flight-control-nav
Suite-AI-Processing	suite-ai-processing

SANS DFIR

FOR509 | Enterprise Cloud Forensics & Incident Response 13

This example shows what a GCP Organization would look like within the GCP console. Conceptually the hierarchy is similar to what we have just discussed in the previous page. However, this example also shows you sub-folders as well. You can see from this example:

Organization – *longconsecurity.com*

Folder (Level 1 – *Futures Lab*

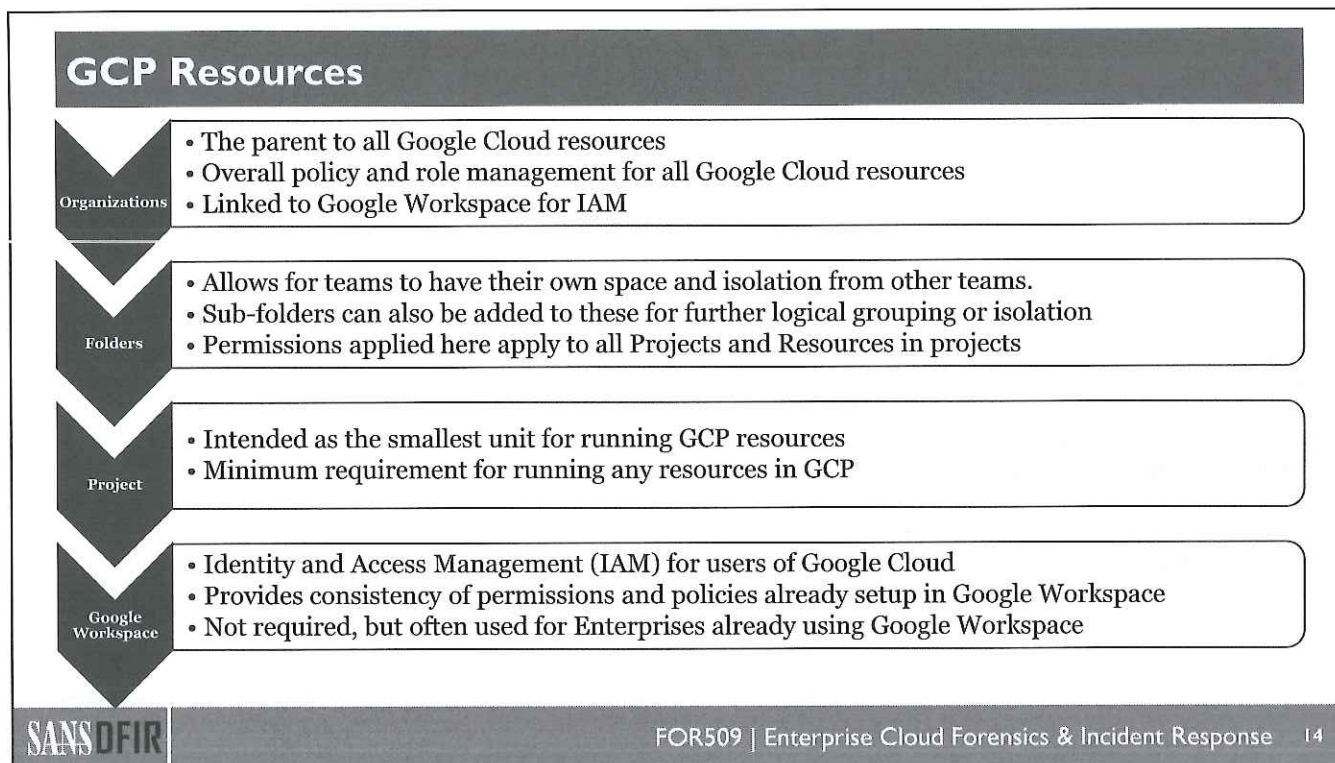
Folder (Level 2) – *Bio Testing Lab* and *Yellow Jacket*

Projects (under Yellow Jacket Folder) – *Flight-Control-Nav* and *Suite-AI-Processing*

Within the Organization view you can create new projects under folders. The Resources, discussed on the previous page, are not shown in the Organization view, however, when you select different Folders or Projects it will change the Resources visible in the GCP Console.

References:

[1] <https://for509.com/gt8s9>



The hierarchy of the GCP resources is intended to not only make organizing your GCP resources easier, but also aid in setting policies or exclusions for different teams or resources.

Policies that are applied higher up the organization roll down to resources and objects under them. Additionally, exclusions can be applied to objects further down the organization tree to open up policy restrictions for specific groups.

The use of Folders in an Organization also allows for isolation away from other teams. While it doesn't restrict one team in a Folder sharing information with other team in a Folder, it does provide for initial isolation of Projects and Resources.

As we'll discuss in future pages, Identity and Access Management (IAM) form the basis for setting up individual user permissions. At this point it's worth understanding that Google Workspace, and the groups within Google Workspace, can also provide a level of grouping users to allow managing resources and permissions. We'll cover IAM in more details, for now, understand that grouping of Resources, Users, or sub-grouping will provide stronger resource management overall.

References:

[1] <https://for509.com/ahcm1>

GCP Organization Benefits for DFIR

- Apply Constraints to EVERYTHING
 - Determining what VM templates users are allowed to create
- Apply Permissions to EVERYTHING
 - Allow your DFIR team to see all permissions on all objects EVERYWHERE
 - Restrict or grant visibility based on Google Workspace groups
- Restrict Actions on ANYTHING
 - Only allow resources to be created in specific regions
 - Prevent users from turning off logging ;)
 - Use “constraints” to set accepted configurations on resources

One of the strong benefits of GCP for incident response and digital forensics investigators is the ability to quickly implement policies that can take control of compromised resources or objects within an organization's GCP instance^{[1][3]}.

As mentioned in the previous pages, logically grouping resources with Folders and Projects allows you to set restrictions or open executions. However, the level of detail that can be applied varies all the way from restricting specific VM templates users can access, through to enforcing logging standards for specific resources.

When it comes to using policies for incident response, they can allow a response team to set policies for access to all resources within a folder, sub-folder, or project^[3]. This can enable a response team to quickly obtain evidence or access to systems for preservation.

It is important to understand that policies allow for setting permissions on “what” an object can and cannot do, whereas IAM is used to determine “who” can and cannot access objects. All policies flow from top down within an organization and IAM access applies per object. If you want to add exceptions for policies, they are applied per object.

References:

[1] <https://for509.com/5m3il>

[2] <https://for509.com/7ldt3>

[3] <https://cloud.google.com/resource-manager/docs/organization-policy/defining-locations>

Key Resources for DFIR



Within GCP there is an ever growing list of resources and services that can be used by Organizations. When new resources are added by Google they are often automatically pushed into a customer's GCP console ready to use. This means there is an ever growing list of resources that incident responders and digital forensics professionals need to stop on top of.

For this section of the course, we have highlighted the key resources that you should focus on first. This list is developed from the author's experience of assisting victims that have had their GCP resources compromised. While this is not an exhaustive list, it covers the large majority of resources when leveraged by threat actors.

During this section of the course, we will focus on most of these resources and how you can obtain and analyze evidence from them. The principles we will teach you for each of these resources can be transposed to similar resources. For example, the logging analysis you will learn with Storage will be applicable to Filestore.

As a starting point, it is important to understand the categories each of these resources are grouped under. These categories directly relate to the categories within GCP, although they will contain a much larger list of resources. This will help you navigate the GCP console, along with understanding conceptually what evidence may be available to you within each category.

Pricing - Overview

All actions in GCP work on a per-consumption model. Except for a few critical actions, everything has a cost.

Temporary Costs



Compute Engine

- Virtual Machines are priced based on the number of CPUs and amount of memory
- They only accrue cost when running
- You can make sure to shut them down when not in use



BigQuery

- Queries against BigQuery are priced on the analysis (actions) against data.



Persistent Disk

Persistent Costs

- Disks and snapshots are priced based on performance and quantity
- They accrue cost all the time until deleted



Cloud SQL

- Storage of data in BigQuery

Before we can drive right in and start to enable logs, store evidence in a Bucket, or spin up a Virtual Machine, you need to have an understanding of what doing these tasks may cost you^[1].

Being able to use the GCP to not only extract evidence, but also analyze it, will significantly speed up your analysis time and evidence processing time. Additionally, it will enable you to keep data within specific geographies if needed, or even within specific network segments if you run into restrictions with moving evidence.

Within GCP there are two concepts to how resources and use of the platform are billed to a customer. These are **temporary costs** and **persistent costs**.

Temporary Costs

Resources that are used on an “as needed” basis are generally billed for as long as you required them to be available. The simplest version of this is a Virtual Machines CPU processing. While ever you need the CPU for a Virtual Machine to be processing your data you will be billed a fee for this. Once you have finished using the CPU for a Virtual Machine and you release your CPU usage, you’re no longer billed for that resource.

Persistent Costs

In contrast to the above, resources that you want to hold for a long period of time or that are required for GCP to be held for an ongoing period of time, are considered persistent costs. These type of resources are billed on a quality basis, instead of a “as needed” basis. Using the example above, the storage disk of a Virtual Machine is considered a resource that will need to exist regardless if the Virtual Machine is using the CPU. In fact, the storage disk is expected to be persistent even if I reboot or temporarily suspend my Virtual Machine. The storage disk is considered a persistent cost that is billed based on the space it is consuming within GCP.

Mixing of Costs

The concept of temporary and persistent storage are intended to be simple concepts to aid in understanding how resources are billed. However, you should be aware that some services mix these concepts together when

they bill a GCP customers. An example of this would be the BigQuery resource. As a customer you are billed for the storage size you consume for holding data, you'd like to be able to query with BigQuery, this is your persistent costs. You are also billed for any queries or "actions" you make against the data you are storing; this is considered a temporary cost.

It is important to understand both these cost models as they can be useful to help decrease your GCP costs, as an analyst. They can also be cause significant billing costs if you aren't aware of the services you're enabling and the resources you leave running.

To get a complete overview on the costs associated with GCP, as they are subject to change, you should review GCP's online costing for their resources^[1]. One final note on costs, there are a small number of items within GCP that have no billing cost associated with them, they include;

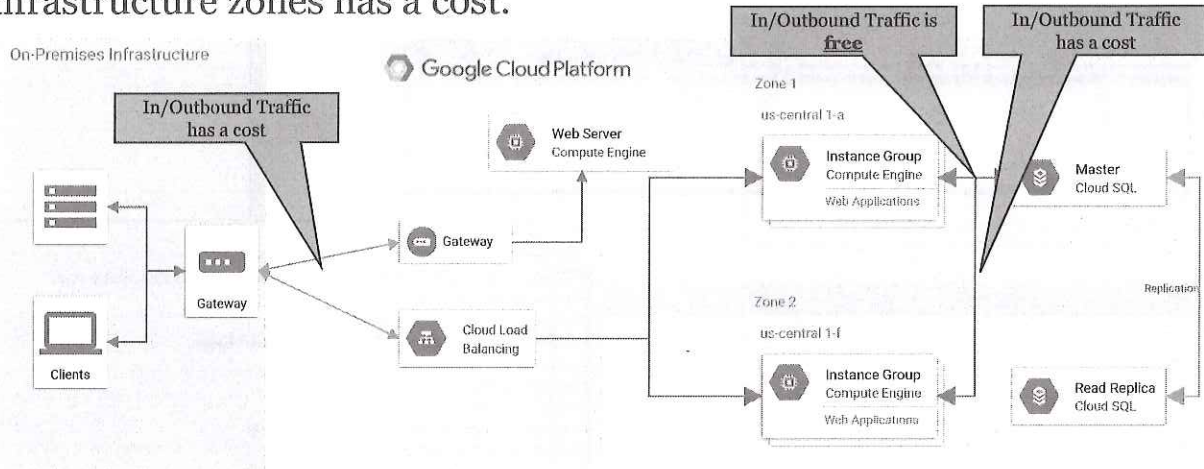
- Using GCP's console via a web browser – which is shown extensively throughout this section of the class.
- Cloud Shell – which is really used within the web browser while you're accessing the GCP Console.
- Logs in the "_Required" log bucket that Organizations cannot change

References:

[1] <https://for509.com/rvkbh>

Pricing – Data Transfer

Data transferred to/from the internet and within the GCP infrastructure zones has a cost.



When it comes to moving data to and from your GCP instance you will also attract ingress and egress fees^[1]. These fees vary depending on the region you are moving data into or out of the GCP.

The costs assigned to both ingress and egress are often based on each resource that you use. For example, if you are sending data from on VM (VM-A) to another VM (VM-B) in a different region you will incur both ingress and egress costs at both locations. This is because if “VM-A” sends traffic, you will incur an egress fee, but you will also incur an ingress fee for traffic the is going back to “VM-A” as part of any TCP communications that respond to the traffic being transferred to “VM-B”.

At the time of publishing this class GCP was not chagrining for ingress traffic going into a GCP resource, however, be aware this is subject to change and should always be checked using GCP’s pricing pages^[1].

Traffic that moves between GCP resources within the same region and zone, while using GCP’s internal assigned IP addresses, do not attract any traffic charges. Because of this you should always try and use GCP’s internal IP addresses and put systems that will communicate a lot in the same zone. This applies to any of your forensic processing tools that will access other systems via GCP’s network.

If you move traffic between GCP zones within a region, or between GCP regions, this will incur a fee, however, again if you use GCP’s internal IP addresses you will use Google’s network backbone which assists in keeping network traffic costs lower.

Traffic costs can quickly get out of hand when you’re using GCP for processing evidence. Especially if you are moving large amount of data to any forensic tools within VM’s. Always try to keep forensic processing VM’s in the same region and zone that your evidence is originating from and try to always using GCP’s internal network IP addresses. In addition to keeping costs lower, it will also keep the speed of traffic transfers over the network quick.

[1] <https://for509.com/yamvd>

Pricing – GCP Cost Calculator (I)

GCP allows you to estimate resources costs

Google Cloud Pricing Calculator

COMPUTE ENGINE GKE STANDARD GKE AUTOPILOT CLOUD RUN VMWARE ENGINE APP ENGINE CLOUD STORAGE NETWORKING EGRESS CLO BAL

Estimate

Search for a product you are interested in.

Operating System / Software

- Free: Debian, CentOS, CoreOS, Ubuntu, or other User Provided OS
- Paid: Windows Server 2008r2, Windows Server 2012r2, Windows Server 2016, Windows Core
- Paid: Red Hat Enterprise Linux
- Paid: Red Hat Enterprise Linux for SAP Applications
- Paid: Red Hat Enterprise Linux for SAP with HA and Update Services
- Paid: SLES
- Paid: SLES 12 for SAP
- Paid: SLES 15 for SAP
- Paid: SQL Server Standard (2012, 2014, 2016, 2017, 2019)
- Paid: SQL Server Web (2012, 2014, 2016, 2017, 2019)
- Paid: SQL Server Enterprise (2012, 2014, 2016, 2017, 2019)

GCP provides a simple online cost calculator to estimate resources you intend to use^[1]. This will allow you to select the resource, the region, the amount of data, and the length of time you intend to use GCP resources. Remember this calculator is only as accurate as the data you provide it, so ensure your estimations are realistic.

You should also be aware that some resources within GCP have additional running costs that maybe not listed on GCP's resource pricing page. An example of this could be the host operation system you are using within a VM. GCP will clearly give you details about the resource cost of using the VM, but you need to also be aware that the licensing costs for the host operating system will be charged to you.

GCP has provided useful licensing when it comes to host operating system licensing. They will provide you a license on an "on-demand" basis. So, if you create a VM running Windows Server 2016 Standard, you will be charged for this as the VM is created. Additionally, users can also use their existing Window VM licensing but adding it into the GCP console^[2]. GCP's Cost Calculator will take operating system licensing into account when you are estimating you running costs.

References:

[1] <https://for509.com/zqrk4>

[2] <https://for509.com/5u6rw>

Pricing – GCP Cost Calculator (2)

The screenshot shows the GCP Cost Calculator interface. It is titled "Estimate" and contains two main sections: "Compute Engine" and "Persistent Disk".

Compute Engine:

- 1 x (with edit and delete icons)
- 20 total hours per month
- VM class: regular
- Instance type: e2-standard-2
- Region: Iowa
- Estimated Component Cost: USD 1.34 per 1 month

Persistent Disk:

- Iowa (with edit and delete icons)
- Zonal standard PD: 128 GiB
- USD 5.12

Total Estimated Cost: USD 6.46 per 1 month

At the bottom, there are two buttons: "ENABLE ESTIMATE" and "SAVE ESTIMATE".

Virtual Machine Estimate:

- 2 vCPUs
 - 8GB RAM
 - 128GB for OS drive
 - 20 hours uptime for the investigation
-
- Higher performance machine may be required depending on the investigation

The GCP cost calculator is perfect for estimating your running costs for a forensic analysis system within the cloud^[1]. In the example above we have chosen a typical VM that would be suitable of accessing other systems in the cloud and for processing disk evidence attached to the VM. The size and requirements for an analysis system can vary significantly depending on scale and it's intended job.

Often when using GCP VM's for forensics analysis processing, you may setup a VM very similar to the example show, then for processing timeline data you could increase the resources for the VM so it can perform the data processing much quicker, then revert the VM back to the example shown for review once timeline processing is completed.

In the example shown we have selected "Iowa (US-Central1)", additionally the pricing was generated with a price list that was last update on 24th of March 2021.

References:

[1] <https://for509.com/zqrk4>

Estimate

Compute Engine

1 x



20 total hours per month

VM class: regular

Instance type: e2-standard-2

Region: iowa

Estimated Component Cost: USD 1.34 per 1 month

Persistent Disk

iowa



Zonal standard PD: 128 GiB

USD 5.12

Total Estimated Cost: USD 6.46 per 1 month

Estimate Currency

USD - US Dollar



EMAIL ESTIMATE

SAVE ESTIMATE

Pricing – GCP Cost Calculator (3)

The screenshot shows the 'Estimate' section of the GCP Cost Calculator. It is titled 'Persistent Disk' and shows the following configuration and pricing:

- Region: Iowa
- Zonal SSD PD: 1,024 GiB
- Snapshot storage: 1,024 GiB
- USD 200.70
- Total Estimated Cost: USD 200.70 per 1 month
- Estimate Currency: USD - US Dollar

Buttons for 'EMAIL ESTIMATE' and 'SAVE ESTIMATE' are visible at the bottom.

- The 1st storage cost is to apply the snapshot to and mount on the forensic VM. Performance is key, so Premium SSD is selected
- The 2nd storage cost is for holding the snapshot.

Snapshot storage is priced differently to a running disk

When performing analysis with a VM in GCP you are most often going to be access snapshots of other system when it comes to disk analysis, as mentioned earlier in this class. Because of this, you have to include the cost of hold the snapshot image as part of your disk analysis. However, you don't need to hold this snapshot on expensive storage given you will mainly be querying or extracting individual items from the image. This allows you to the snapshot on cheaper storage^[1], as show in this example.

References:

[1] <https://for509.com/ijn48>

Pricing – GCP Cost Calculator (4)

The screenshot shows the GCP Cost Calculator interface. It is divided into two main sections: 'Compute Engine' and 'Persistent Disk'.
Under 'Compute Engine', the configuration includes:
- 1 x instance
- 20 total hours per month
- VM class: regular
- Instance type: e2-standard-2
- Region: Iowa
- Estimated Component Cost: USD 1.34 per 1 month
Under 'Persistent Disk', the configuration includes:
- Zone: S5D PD: 1,152 GiB
- Snapshot storage: 1,024 GiB
- USD 222.46
At the bottom, the 'Total Estimated Cost' is shown as USD 223.80 per 1 month. There are also buttons for 'EMAIL ESTIMATE' and 'SAVE ESTIMATE'.

- This is a typical monthly cost for a “small” investigation where all DFIR work is performed within GCP.
- GCP’s cost calculator does not break out the individual disks, it bundles them together.

Taking into consideration the size of the analysis VM we have showed so far, running that VM for approximately 20hrs to conduct analysis, along with holding 1Tb of snapshot data, it will cost you (as at the 24th of March 2021) approximately USD \$222.

In terms of maintaining your own hardware, or the task of procuring hardware and setting it up, this cost is relatively inexpensive. At the time of writing this section, GCP is also the cheapest cloud, out of AWS and Azure, to run an analysis system of this size.

Estimate

Compute Engine

1 x



20 total hours per month

VM class: regular

Instance type: e2-standard-2

Region: iowa

Estimated Component Cost: USD 1.34 per 1 month

Persistent Disk

iowa



Zonal SSD PD: 1,152 GiB

Snapshot storage: 1,024 GiB

USD 222.46

Total Estimated Cost: USD 223.80 per 1 month

Estimate Currency

USD - US Dollar



EMAIL ESTIMATE

SAVE ESTIMATE

Pricing – Cost Reduction Options

There are options available to assist with keeping costs lower in GCP.

- **Preemptible VM Instance**

- CPU is variable and changes pending demand within GCP
- Ideal when you have multiple VMs and you don't require dedicated CPU
- Not ideal for single system evidence processing (i.e., Plaso)

- **Data Movement within GCP**

- Moving data within a single zone doesn't cost money – if you use an internal IP address
- Put your DFIR Analysis VM in the same zone as your evidence source

- **Queries Against Data**

- Queries are charged based on bytes processed
- Holding data in smaller data sets can save on the cost of each query

There are some useful cost reduction options that the GCP provides customers. One of these, that's extremely useful for VM's, is a "Preemptible" VM instance^[1]. This type of instance won't provide customers with dedicated CPU processing, but instead will provide customers with excess CPU processing that isn't being used by other customers that have paid for dedicated VM instances. The concept is that a "Preemptible" VM will flux within its CPU utilization based on CPU resources that aren't being used within the overall GCP. This is a particularly good way to reduce VM costs, however, it does mean you don't get dedicated CPU resources for processing. Where these instance maybe useful to customers and investigators, is when you have multiple VM's that are load balancing requests or computation, so they have redundancy built in. These type of VM's would not be suitable if you have an evidence process that has to reside within a single VM, for example Plaso.

When you conduct investigations within GCP ensure you get your evidence processing VM's in the same region and zone as the majority of your target systems/evidence. As discussed previously, moving data within the same region and zone has no ingress or egress costs provided you use the GCP internal IP address to communicate between systems.

Lastly, be careful of how you use data analysis tools within GCP. Most common for investigators is the use of resources like BigQuery. As mentioned previously BigQuery is billed based on holding data and also querying of data. While there is not a lot that can be done to reduce the cost of holding the data, you can reduce the cost of querying data. BigQuery is billed based on compute time used to perform a query^[2]. If you can reduce the number of queries you need to make it will aid in keeping costs lower, along with ensuring you document the output of a query so you, or other investigators, don't need to run it a second time. If you have team members that have strong SQL skills, use them to help craft queries that perform sub-queries or cross-correlate data in a single query.

References:

[1] <https://for509.com/5xbh3>

[2] <https://for509.com/ei73s>

GCP Identity and Access Management (IAM)



This page intentionally left blank.

GCP IAM Overview (I)

Member	Role	Policy
<ul style="list-style-type: none">• Google Accounts• Service Accounts• Google Groups• Google Workspace Domains• Cloud Identity Domains• All authenticated users• All users	<ul style="list-style-type: none">• Basic Roles<ul style="list-style-type: none">• Owner• Editor• Viewer• Predefined Roles• Custom Roles	<ul style="list-style-type: none">• Member(s) + Role = Binding• Assigned to Resources<ul style="list-style-type: none">• Folders• Projects• Objects/Services

Identity and Access Management (IAM) is a key resource that all investigators will heavily use in GCP^[1]. Because of this, it's important that you have a strong understanding of how IAM works and how it's setup within GCP. This section will cover the fundamentals of IAM and provide you with the building blocks to understand IAM in more depth. While IAM is the main backbone to identity and access management within GCP, you should be aware that some large enterprises may use other third-party tools to aid with their IAM management, however, the basis for what resources have access to will still be bound by the concepts we'll present in this section.

GCP defines IAM objects into "Members", "Roles", and "Policies"

Member

A member is an individual user, group, or service account that is treated as an object that can have permissions assigned. Members are not limited to only users within GCP, it can also be users or groups within Google Workspace, or users and service accounts in other GCP organizations. An email address is the primary identifier for members including service accounts and groups, however, this can also be extended to a domain when you are defining a very large group of members together.

Roles

Roles represent a collection of permissions assigned to a common group that grant or restrict access to Members. Within Roles there are three common categories, there are; Basic Roles, Predefined Roles and Custom Roles.

Basic Roles have existed since GCP was first developed by Google and consist of three sub-groups; Owner, Editor, and Viewer. These types of Roles were really developed as a simple and easy way to get started with GCP; however, they can present challenges with securing a GCP instance that we will look at later in this section.

Predefined Roles are similar to Basic Roles; however, they provide a much more fine-grained approach to permissions allow you to be a more specific with the types of permissions you may want to assign a Member. These role types, as the name suggests, are predefined by GCP. In terms of securing your GCP these are the types of Roles you should be assigning Members.

Custom Roles[2] allow you to create your own role types using the thousands of permissions available in GCP. These are ideal when you need to create custom roles that are within the Predefined Roles offered in GCP.

Policy

Policies are a way to tie together a number of Members, assign them a Role and bind it to a resource within GCP. A Policy is assigned to resources within GCP and are used to check permissions when a member attempts to accesses a resource.

References:

- [1] <https://for509.com/nrdg0>
- [2] <https://for509.com/g0kqa>

Google Cloud Identity Setup



SETTING UP GCP Identity

GCP allows Organizations to use either:

- Cloud Identity, or
- Google Workspace (previously GSuite)

Cloud Identity can be used as IDaaS (Identity as a Service) with no link to Google Workspace

The GCP Organization will be associated with your Domain.

When using Google Workspace you should create Groups to Manage GCP User Accounts

When you setup GCP you will need to determine how authentication and Members are managed. GCP provides you with two standard options being either the IAM service within GCP referred to as “Cloud Identity” or through the use of “Google Workspace”^[1]. There are other IAM services, outside of GCP and Google Workspace, that make it possible to create members and authenticate within GCP, however, these usually use a connector into one of the two options mentioned above. Authentication and Member management outside of the two options mentioned here are beyond the details of this course. However, the principals will be similar.

When you link your Google Workspace to GCP you also link your primary domain, within Google Workspace, to GCP. This results in your GCP Organization being your Google Workspace’s primary domain.

As you’ll see shortly, using Google Workspace can become a simple way to managing users and groups for GCP access.

References:

[1] <https://for509.com/o8za4>

Google Cloud IAM Recommended Groups

`gcp-organization-admins`

- This group is required to link Google Workspace to Google Cloud
- Used to organizing your GCP resource structure

`gcp-network-admins`

- Commonly used for creating and managing networking infrastructure within GCP

`gcp-security-admins`

- Commonly used to maintain security policies across the whole organization.
- Also used for implementing organization wide IAM constrain policies

`gcp-billing-admins`

- Commonly used to monitoring billing and resource use across the organization
- Responsible for implementing billing for projects within an organization

`gcp-devops`

- Similar to "gcp-developers" except they would manage the overall pipeline of application development and data manipulation.

`gcp-developers`

- Used by developers that construct code, design applications and implement application testing.

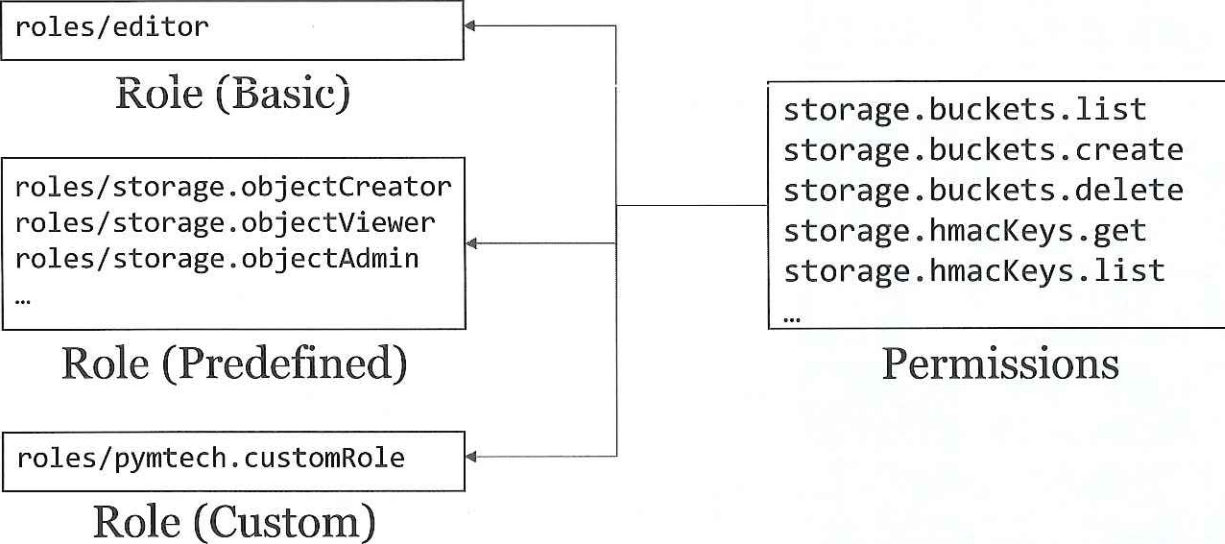
When setting up Google Workspace to work alongside of GCP IAM, you have to create the "gcp-organization-admins" group and put your Organizational admins within that group. Without this group GCP will not link to Google Workspace.

The rest of the groups presented in this page are intended as best practice groups for your Google Workspace and your users^[1]. These groups will help you better define the users and allow you to assign Roles to Google Workspace groups for a better structure of permissions. You can of course put a single member/user within multiple groups; however, you should avoid this as part of best practice with separating permissions.

References:

[1] <https://for509.com/x6h3g>

GCP IAM - Roles



To better understand how permissions are defined and how Roles link with permissions, consider a Role a group of permissions. The permissions within GCP are preset granular permissions for each resource one permissions on its own is not overly useful, however, it's when you cluster or group these permissions together you can define a set of permissions as a Role for a Member.

As mentioned previously, Basic Roles are predefined roles with a predefined set of permissions that cannot be changed. However, they do offer the greatest flexibility for quickly building within GCP. Although, they are very broad sets of permissions that may provide more permissions than you initially need or intend Members to have.

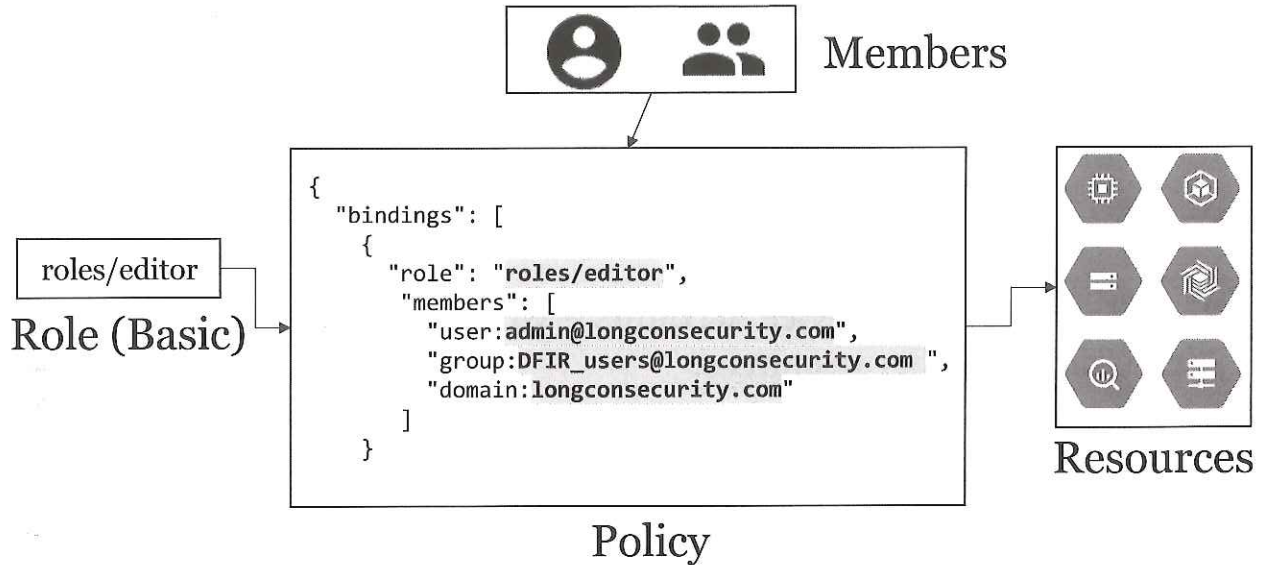
Predefined Roles are pre-made groups of permissions from GCP. They group permissions together for a more narrow defined Role^[1]. These are well documented within GCP's documentation to allow Organizations to better define what each Member is allowed to do within GCP^[1].

Custom Roles allow Organizations to make their own permissions and assign them to Custom Roles. Along with creating your own permissions, you can use the existing permissions within GCP and mix them together with any custom permissions you decide to make. They allow an organization to specify exactly what permissions are assigned to a Role, however, there are hundreds of permissions, and this can be an extremely long task to get right.

Reference:

[1] <https://for509.com/0mors>

GCP IAM – How Policies Work



A Policy is made up for the binding together of Roles, which are groupings of permissions, and Members into a single Policy object. This Policy is then applied to one or many resources within GCP.

Policies are not applied to members! This is one of the fundamental differences to GCP compared to what you've learnt so far with AWS and Azure. You cannot query a Member and determine all the permissions that a member may have. You can only query a Resource to determine who has permissions for that Resource, this is because a Resource has the Policy applied to it.

To complicate further an administrator's ability to determine what permissions a Member has, you can have resources in a completely different Organization grant access to a member in another unrelated Organization. This means one of the Members in your Organization may have high level permissions to a Resource in another Organization and you would be unable to determine this from within your own Organization.

GCP IAM Challenges

- Policies are bound to Resources, not Members.
- You cannot view a Member and see all the permissions it has.
- You can query a resource and see all the permissions it has allowed.
- Resources can have Service Accounts – which can also have permissions to other resources.

The challenge with how GCP applies permissions to Resources, instead of Members, is a change in the model of how most people expect identity management to work. This means you can't simply query a Member to understand all the permissions they may have, or all the Resources they could possibly have access to. This is often a challenge when it comes to incident response if an account with GCP is being misused. It results in investigators having to rely on logging a lot more than they would to determine a Member's permissions. In the world of Microsoft Active Directory, as mentioned previously in the course, you could query a user and see all their groups and each group's permissions. That's no longer the case within GCP.

To understand the permissions a Member may have, you have to query the Resource. This can have some benefits from an investigation perspective. It means if you know a certain Resource was abused you can simply query the permissions that Resource has assigned and see all the Members that can access it and what their permission level is on that Resource.

As mentioned in the previous pages, this can be challenging as you could have Members with access to Resources in another GCP Organization, that you have no control over, but your Members could have access to it. To extend this challenge further, if a Member within your GCP Organization accessed a Resource within another GCP Organization the logging for that access would be in the *other* Organization, not yours.

To extend out the permissions model a little further, Resources can have their own Service Accounts if they need to access other Resources. For example, if you have a VM Resource that needed to access a Storage Bucket for reading and/or writing data, it will require a Service Account for the VM Resource with that Service Account given permissions on the Storage Bucket via a Policy applied to the Storage Bucket. Service Accounts work in the same way we have discussed Member accounts, in fact that are considered Member accounts. This means the same permission challenge mentioned above also applies to Service Accounts.

GCP IAM – Service Accounts

The screenshot displays the 'Create an instance' wizard in the Google Cloud Platform console. The 'Identity and API access' section is highlighted, showing the 'Service account' dropdown set to 'Compute Engine default service account'. A callout box points to this section with the text 'Permissions set against the Service Account used.' The 'Access scopes' section is also visible, showing 'Allow default access' selected.

In most cases Service Accounts are created as you create new Resources within GCP that may be used to access other Resources within GCP. When you created a new VM a Service Account is created and assigned to that VM at the time it is created^[1]. This is shown in the example above where a new VM is being created and a Service Account for the resource is created at the same time. This Service Account will also appear in IAM and allow you to manage the account the same way you would any other Member in IAM.

You could delete this account in IAM; however, it will likely cause access issues if you're attempting have your VM interact with other GCP Resources. You can also control the permissions this account has on other Resources, which is usually the best way to keep your Service Accounts under control in terms of their level of permissions.

References:

[1] <https://for509.com/w5ykm>

← Create an instance



New VM instance

Create a single VM instance from scratch



New VM instance from template

Create a single VM instance from an existing template



New VM instance from machine image

Create a single VM instance from

instance-1

Labels [?](#) (Optional)

+ Add label

Region [?](#)

Region is permanent

us-west1 (Oregon)

Zone [?](#)

Zone is permanent

us-west1-b

Machine configuration

Machine family

General-purpose

Compute-optimized

Memory-optimized

Machine types for common workloads, optimized for cost and flexibility

Learn more about Microsoft license mobility requirements

Identity and API access [?](#)

Service account [?](#)

Compute Engine default service account

Access scopes [?](#)

- Allow default access
- Allow full access to all Cloud APIs
- Set access for each API

Firewall [?](#)

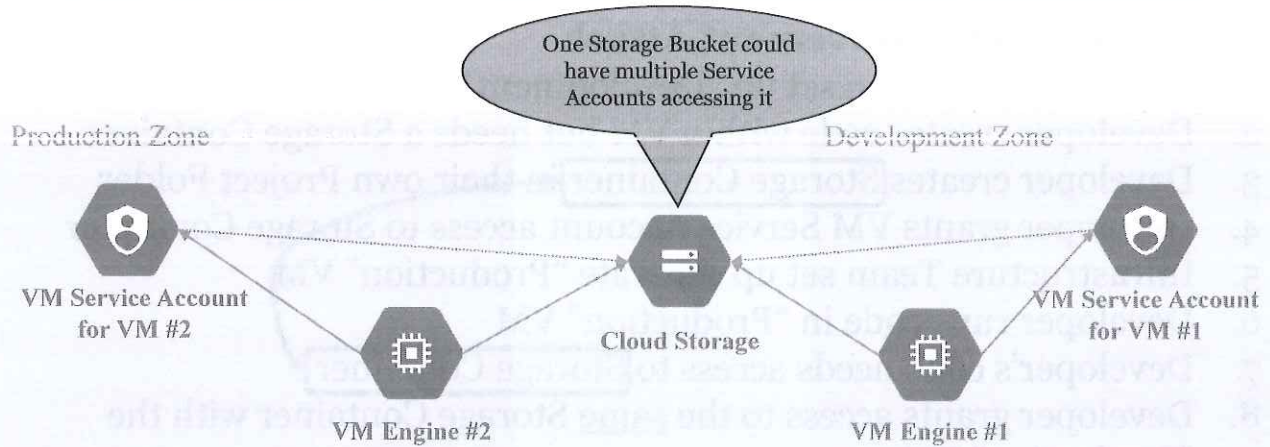
GCP IAM Challenges

Common Lateral Movement Attack

1. Infrastructure Team set up “Development” VM for testing
2. Developer creates code within VM but needs a Storage Container
3. Developer creates **Storage Container** ~~in their own Project Folder~~
4. Developer grants VM Service Account access to Storage Container
5. Infrastructure Team set up separate “Production” VM
6. Developer runs code in “Production” VM
7. Developer’s code needs access to **Storage Container**
8. Developer grants access to the same Storage Container with the “Production” VM

This page intentionally left blank.

GCP IAM – Service Accounts



Service accounts are used to access other resources within GCP. The resource you want to access has to allow the service account permission to access it. You would assign a policy to the resource that allows the Service Account permission.

This also means it's hard to control what Service Accounts have access to if a developer grants access to a resource that they control.

GCP IAM Challenges

Common Lateral Movement Attack

- Shared Services Accounts (with “Editor” permissions) allow the compromise of a resource to laterally move to other resources
- This can occur across Projects and across Organizations!
- If a resource is compromised and it has other high permissioned Service Accounts you can “actAs” and escalate privilege
- Plus.....someone automated this with a tool called **gcploit**

gcploit is written by Dylan Ayrey^[1] and then presented by Dylan and Alison D as part of Blackhat/Defcon 2020^[2].

References:

[1] <https://for509.com/wqfoe>

[2] <https://for509.com/4quy0>

elastic Discover

service_name:iam.googleapis.com x + Add filter

gcp-*

Filter by type 0

Selected fields: 4

- ips
- method_name
- resource_name
- username

Available fields: 39

- Popular
- event_type
- log_name
- service_name
- _id
- _index
- _score
- _type
- @timestamp
- @version
- agent.ephermal_id
- agent.hostname
- agent.id
- agent.name
- agent.type
- agent.version
- ecs.version

2021-01-27 13:46:20.497 +00:00 - 2021-04-27 13:46:20.497 +00:00 Auto

69 hits

Count	IP	Method Name	Resource Name	Username	Timestamp	Service Name	Path
15	2021-03-29 12:09:03.395 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.QueryGrantableRoles	2401:d802	google.iam.admin.v1.QueryGrantableRoles	//cloudresourcemanager.googleapis.com/projects/suit-ai
10	2021-03-29 12:09:03.394 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.QueryGrantableRoles	2401:d802	google.iam.admin.v1.QueryGrantableRoles	//cloudresourcemanager.googleapis.com/projects/suit-ai
5	2021-03-29 12:09:02.546 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.GetPolicyDetails	2401:d802	google.iam.admin.v1.GetPolicyDetails	//cloudresourcemanager.googleapis.com/projects/suit-ai
0	2021-03-29 12:07:36.608 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.QueryGrantableRoles	2401:d802	google.iam.admin.v1.QueryGrantableRoles	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1
	2021-03-29 12:07:35.247 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.GetPolicyDetails	2401:d802	google.iam.admin.v1.GetPolicyDetails	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/instances/instance-1
	2021-03-29 11:59:25.515 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.QueryGrantableRoles	2401:d802	google.iam.admin.v1.QueryGrantableRoles	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/disks/inst
	2021-03-29 11:59:24.637 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.GetPolicyDetails	2401:d802	google.iam.admin.v1.GetPolicyDetails	//compute.googleapis.com/projects/suit-ai/zones/us-west1-b/disks/inst
	2021-03-29 11:33:26.951 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.GetPolicyDetails	2401:d802	google.iam.admin.v1.GetPolicyDetails	//storage.googleapis.com/projects/_/buckets/light-maps
	2021-03-29 11:30:21.013 +00:00	admin@longconsecurity.c	admin@longconsecurity.c	admin.v1.GetPolicyDetails	2401:d802	google.iam.admin.v1.GetPolicyDetails	//storage.googleapis.com/projects/_/buckets/log_bucket_for_logs

Hide chart

Lab 4.1

GCP IAM and Access Tracking

This page intentionally left blank.

FOR509.4 – Google Cloud Platform (GCP)

Section 4.1: Understanding GCP

Section 4.3: Log Sources, Collection & Log Routing

Section 4.2: VM & Storage Investigations

Section 4.4: GCP Network Forensics

This page intentionally left blank.

Google Cloud Platform Roadmap

4.1: Understanding GCP

4.2: Log Sources, Collection & Log Routing

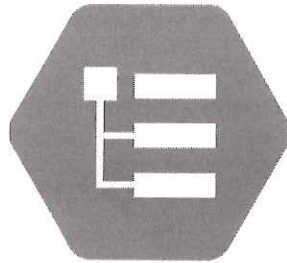
4.3: VM & Storage Investigations

4.4: GCP Network Forensics

- GCP Log Explorer
- Log Explorer Queries
- Log Routing
- Log Storage
- Logging Pipelines
- Logging Exporting

This page intentionally left blank.

Google Cloud Logging



This page intentionally left blank.

Enabling Auditing & Logging (I)

The screenshot shows the Google Cloud Platform IAM & Admin console. The 'Audit Logs' section is active, displaying a table of audit logs. The table has the following columns: Title, Admin Read, Data Read, Data Write, and Exemptions. The 'Audit Logs' menu item is highlighted with a '2'.

<input checked="" type="checkbox"/>	Title ↑	Admin Read	Data Read	Data Write	Exemptions
<input type="checkbox"/>	Access Approval	--	--	--	0
<input type="checkbox"/>	AI Platform Notebooks	--	--	--	0
<input type="checkbox"/>	Apigee	--	--	--	0
<input type="checkbox"/>	Apigee Connect API	--	--	--	0
<input type="checkbox"/>	Assured Workloads API	--	--	--	0
<input type="checkbox"/>	Binary Authorization	--	--	--	0
<input type="checkbox"/>	Certificate Authority Service	--	--	--	0
<input type="checkbox"/>	Cloud AI Platform API	--	--	--	0
<input type="checkbox"/>	Cloud AI Gateway	--	--	--	0

NOTE

Getting Logging inside of GCP works in two ways, either;

- **Audit Logs** from the Platform, or

- You ship logs from another application / system / service

This page intentionally left blank.

Enabling Auditing & Logging (2)

longconsecurity.com Audit Logs

← Default audit config

Default audit configuration

Set a default audit logging configuration for all Google Cloud Platform services. Default configurations set at the organization level are inherited to all projects in that organization.

LOG TYPE EXEMPTED USERS

Turn on/off audit logging for selected services.

- Admin Read
- Admin Write
- Data Read
- Data Write

SAVE

NOTE

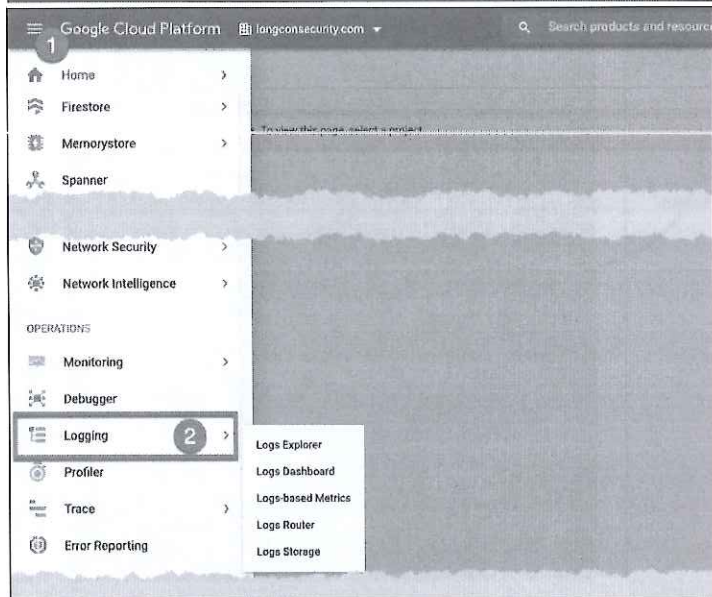
By default, GCP only audits/logs “Admin Write” commands on all modules in.

Defaults are relative to the Organization object you are looking at. You should set a minimum base audit level at the top organization object.

You can increase logging for more sensitive projects (i.e., R&D or Production project)

This page intentionally left blank.

Accessing Logging



NOTE

GCP has recently taken significant steps to upgrade the production, collection and searching available for logs.

Accessing and Searching Logs requires Permission

Logs are Stored and Accessed per Project

This page intentionally left blank.

GCP Log Explorer

The screenshot displays the GCP Log Explorer interface. At the top, there are navigation options like 'SHARE LINK', 'LAST HOUR', 'PAGE LAYOUT', and 'LEARN'. Below this, a 'Query Builder' section allows users to filter logs by resource, log name, and severity. A 'Results Histogram' shows a bar chart of log counts over time. The 'Query Results' section displays a table of log entries with columns for severity, timestamp, and message. The interface is annotated with callouts pointing to these key features.

Scope of Logs

Query Builder

Results Histogram

Query Results

This page intentionally left blank.

GCP Log Explorer - Search Query

The screenshot displays the GCP Log Explorer interface. The top section is the 'Query builder' with tabs for 'Recent (7)', 'Saved (0)', and 'Suggested (0)'. It features a 'Resource' dropdown (1) and a 'Severity' dropdown. Below this is a 'Select resource' panel (2) with a search bar and a list of resource types including GCE SSL Certificate, GCE Target HTTP Proxy, GCE Target HTTPS Proxy, GCE Target SSL Proxy, GCE URL Map, GCS Bucket, Global, and Google Project. A 'GCS Bucket' resource is selected, leading to a table with columns for 'All bucket_name' and 'All location'. The table contains two rows: 'flight-maps' (3) and 'log_bucket_for_logs'. The 'flight-maps' row is selected, and its location 'us-east1' (4) is highlighted. A 'Cancel' (5) and 'Add' button are at the bottom. To the right, a 'Select time range' panel is shown with options: 30 seconds, 15 minutes, 24 hours, 7 days, Enter custom range, and Jump to time. The '24 hours' option is selected. Below the query builder is the 'Logs Explorer' section with 'OPTIONS', 'REFINE SCOPE', 'SHARE LINK', 'LAST 1 DAY', and 'PAGE LAYOUT' controls. It shows a 'Query builder' with 'Log name' and 'Severity' dropdowns, and a 'Run query' button. The query text is: 'resource.type="gcs_bucket" resource.labels.bucket_name="flight-maps" resource.labels.location="us-east1"'. The results table is currently empty.

This page intentionally left blank.

GCP Log Explorer - Search Query

Query preview
resource.type="gcs_bucket" resource.labels.bucket_name="flight-maps" resource.labels.location="us-east1" Save Stream logs Run query

Query results Jump to now Actions Configure

SEVERITY	TIMESTAMP	GMT	SUMMARY
	Showing logs for last 5 hours starting at 3/29/21, 8:07 AM. Extend time by: 1 hour Edit time		
	2021-03-29 11:32:48.527 GMT	IAM	storage.googleapis.com storage.buckets.create projects/_/buckets/flight-maps admin@longconsecurity.com audit_log, method: "storage.buckets...
	Showing logs for last 5 hours ending at 3/29/21, 1:05 PM. Extend time by: 1 hour Edit time		

This page intentionally left blank.

GCP Log Explorer - Search Query

```
2021-03-29 11:32:48.527 GMT IAM storage.googleapis.com storage.buckets.create projects/_/buckets/flight-maps admin@longconsecurity.com audit_log_method:
"storage.buckets.create", principal_email: "admin@longconsecurity.com"

protoPayload: {
  @type: "type.googleapis.com/google.cloud.audit.AuditLog"
  status: (0)
  authenticationInfo: {
    principalEmail: "admin@longconsecurity.com"
  }
  requestMetadata: {
    callerIp: "2481:9902:"
    callerSuppliedUserAgent: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.48 Safari/537.36,gzip(gfe),gzip(gfe)"
    requestAttributes: (2)
    destinationAttributes: (0)
  }
  serviceName: "storage.googleapis.com"
  methodName: "storage.buckets.create"
  authorizationInfo: (1)
  serviceData: (2)
  request: (1)
  resourceLocation: (1)
}

resource: (2)
timestamp: "2021-03-29T11:32:48.527942758Z"
severity: "NOTICE"
logName: "projects/eust-ai/logs/cloudaudit.googleapis.com%2Factivity"
receiveTimestamp: "2021-03-29T11:32:49.764491837Z"
```

This page intentionally left blank.

GCP Log Explorer - Search Query

The screenshot displays the GCP Log Explorer interface. At the top, it shows 'Query results' with a search bar and filters. The main area displays a log entry for 'storage.googleapis.com' with a 'storage.buckets.create' method. The log entry is expanded to show the 'protoPayload' field, which contains details about the request, including the principal email 'admin@longconsecurity.com'. A red box highlights the 'principalEmail' field in the log entry, and an arrow points to it. Below the log entry, a 'Query builder' section shows a list of recent queries. The second query is highlighted with a red box and an arrow, showing the search query: 'protoPayload.authenticationInfo.principalEmail="admin@longconsecurity.com"'. The query builder also shows filters for 'Resource', 'Log name', and 'Severity'.

This page intentionally left blank.

Query results

SEVERITY TIMESTAMP

Showing logs for last 5 hours starting at 3/29/21, 8:07 AM.

2021-03-29 11:32:48.527 GMT IAM storage.googleapis.com storage.buckets.create projects/_/buckets/flight-maps admin@longconsecrity.com audit_log, method: "storage.buckets.create", principal_email: "admin@longconsecrity.com"

Hide log summary Expand nested fields Copy to clipboard Copy link

```

{
  protoPayload: {
    @type: "type.googleapis.com/google.cloud.audit.AuditLog"
    status: {}
    authenticationInfo: {
      principalEmail: "admin@longconsecrity.com"
    }
    requestMetadata: {
      callerIp: "248...
      callerSupplied...
      requestAttribu...
      destinationAtt...
    }
    serviceName: "storage.googleapis.com"
    methodName: "storage.buckets.create"
    authorizationInfo: [1]
    resourceName: "projects/_/buckets/flight-maps"
    serviceData: {2}
    request: {1}
    resourceLocation: {1}
  }
  insertId: "pjcw1ehm4w"
  resource: {2}
  timestamp: "2021-03-29T11:32:48.527942759Z"
  severity: "NOTICE"
  logName: "projects/suit-21/logs/cloudaudit.googleapis.com%2Factivity"
  receiverTimestamp: "2021-03-29T11:32:49.764491037Z"
}

```

Query builder Recent (7) Saved (0) Suggested (0)

Resource v Log name v Severity v

- resource.type="gs_bucket" resource.labels.bucket.name="flight-maps" resource.labels.location="us-east1"
- protoPayload.authenticationInfo.principalEmail="admin@longconsecrity.com"

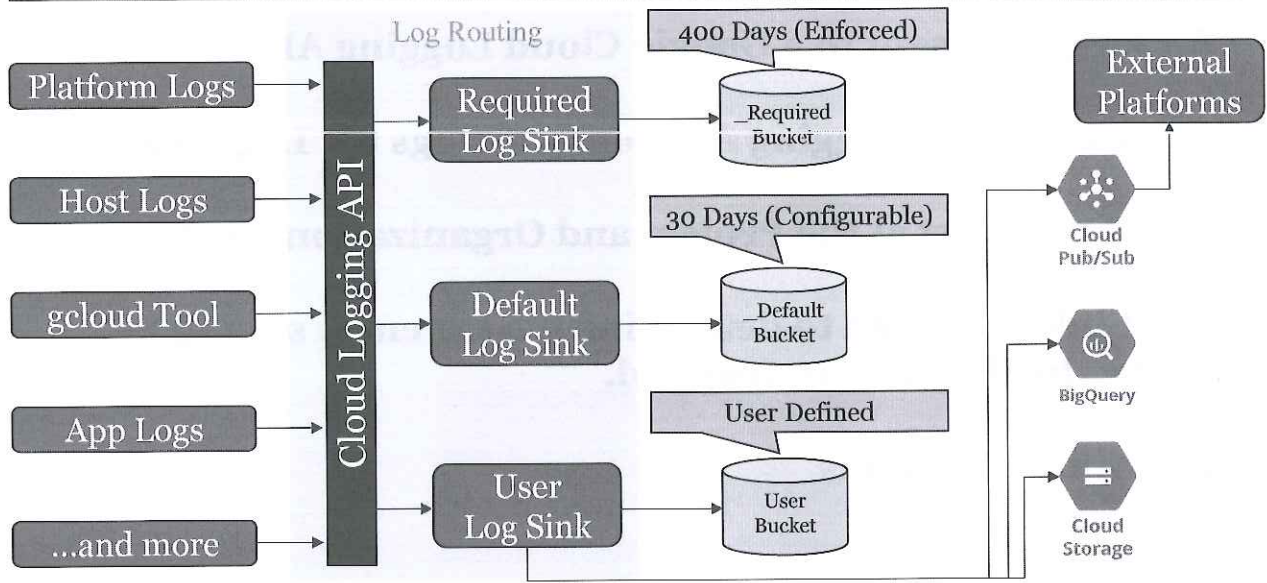
GCP Logging Principals

- **All logging is sent to a Google Cloud Logging API**
- **Google’s Cloud Logging API sends all logs to “Log Sinks”**
- **Log Sinks exist at the Project and Organization level**
- **Log Sinks are used to determine if a log entry should be routed by the Sink or dropped.**
- **Log Sink “Exclusions**

References:

[1] <https://for509.com/tm3b0>

GCP Log Routing Overview



References:

[1] <https://for509.com/tm3b0>

GCP Logging Storage

- The “*_Required Bucket*” and “*_Required Sink*” cannot be modified.
 - This does not count towards the costs in your GCP Billing
- The “*_Default Bucket*” and “*_Default Sink*” can be modified.
 - This does count towards the costs in your GCP Billing
- Logging Buckets can hold logs between 1 and 3650 days
 - Yes – that’s over 9 years!
- Log Routing and Storage can be encrypted using your own keys (CMEK)

References:

[1] <https://for509.com/8yt5o>

[2] <https://for509.com/4unh8>

GCP Log Routing Sinks

The screenshot shows the GCP Logs Router interface. At the top, there are buttons for 'CREATE SINK' and 'DELETE', and a 'LEARN' link. The main content area is titled 'Logs Router Sinks' and contains a table with the following data:

Enabled	Type	Name	Description	Destination	Created	Last Updated	
<input type="checkbox"/>	Cloud Logging bucket	_Default		logging.googleapis.com/projects/suit-ai/locations/global/buckets/_Default	1/1/70, 12:00 AM	1/1/70, 12:00 AM	⋮
<input checked="" type="checkbox"/>	Cloud Logging bucket	_Required		logging.googleapis.com/projects/suit-ai/locations/global/buckets/_Required	1/1/70, 12:00 AM	1/1/70, 12:00 AM	⋮

_Default Log Sink

_Required Log Sink

This page intentionally left blank.

Operations **Logging**

- Logs Explorer
- Logs Dashboard
- Logs-based Metrics
- Logs Router
- Logs Storage

Logs Router [CREATE SINK](#) [DELETE](#) [LEARN](#)

Logs Router Sinks

Filter Filter

<input type="checkbox"/> Enabled	Type	Name ↑	Description	Destination	Created	Last Updated
<input type="checkbox"/>	Cloud Logging bucket	_Default		logging.googleapis.com/projects/suit-ai/locations/global/buckets/_Default	1/1/70, 12:00 AM	1/1/70, 12:00 AM
<input checked="" type="checkbox"/>	Cloud Logging bucket	_Required		logging.googleapis.com/projects/suit-ai/locations/global/buckets/_Required	1/1/70, 12:00 AM	1/1/70, 12:00 AM

GCP Log Storage (I)

Operations
Logging

Logs Explorer
Logs Dashboard
Logs-based Metrics
Logs Router
Logs Storage

Logs Storage

CREATE LOGS BUCKET CREATE USAGE ALERT DELETE

Current total volume
Previous month volume
Projected volume by EOM

Since the first of this month. See total usage by resource type
Total for month of February. See bill
By end of the month

Logs buckets

Filter Filter

<input type="checkbox"/>	Name ↑	Description	Retention period	Region	Status	
<input type="checkbox"/>	_Default	Default bucket	30 days	global	Unlocked	⋮
<input type="checkbox"/>	_Required	Audit bucket	400 days	global	Locked	⋮

_Default Log Sink

_Required Log Sink

This page intentionally left blank.

Operations
Logging

- Logs Explorer
- Logs Dashboard
- Logs-based Metrics
- Logs Router
- Logs Storage

Logs Storage
CREATE LOGS BUCKET
CREATE USAGE ALERT
DELETE

Current total volume

Since the first of this month. See [total usage by resource type](#)

Previous month volume

Total for month of February. See [bill](#)

Projected volume by EOM

By end of the month

Logs buckets

Filter Filter

<input type="checkbox"/>	Name ↑	Description	Retention period	Region	Status
<input type="checkbox"/>	_Default	Default bucket	30 days	global	Unlocked
<input type="checkbox"/>	_Required	Audit bucket	400 days	global	Locked

GCP Log Storage (2)

Logs buckets

Filter Filter

<input type="checkbox"/>	Name ↑	Description	Retention period	Region	Status	
<input type="checkbox"/>	_Default	Default bucket	30 days	global	Unlocked	1
<input type="checkbox"/>	_Required	Audit bucket	400 days	global	Locked	2

View bucket details

Edit bucket

Delete bucket

View logs in this bucket

View usage data for this bucket

- **Retention time and Name can be changed after creation.**
- **Bucket Location is fixed after initial creation.**

Edit logs bucket

Bucket details

Provide a name and description for the logs bucket.

Name (required)
_Default
8/100

Description
Default bucket

Select logs bucket region
global
Logs bucket regions can't be changed later

DONE

Set the retention period

Choose the duration that logs are stored in the bucket. Setting a longer retention period impacts billing.

Retention *
30 Day(s)

UPDATE BUCKET CANCEL

This page intentionally left blank.

Create a Log Sink

1 Sink details
Provide a name and description for logs routing sink

Name: DFIR_Flow_Logs
Description: Network Flow Logs for whole Project

2 Sink destination
Select the service type and destination for logs routing sink

Service: Cloud Logging bucket
Destination: logging.googleapis.com/projects/sl...

3 Choose logs to include in sink
Create an inclusion filter to determine which logs are included in logs routing sink

Build inclusion filter: PREVIEW LOGS

1 resource.type="gce_subnetwork" AND
2 log_id("compute.googleapis.com/vpc_flows")

4 Choose logs to filter out of sink (optional)
Create exclusion filters to determine which logs are excluded from logs routing sink

CREATE SINK CANCEL

Current Sink Destination options

2 Sink destination
Select the service type and destination for log

Select sink service *

- Cloud Logging bucket
- BigQuery dataset
- Cloud Storage bucket
- Cloud Pub/Sub topic
- Splunk
- Other project

Create a unique (within the Project) Sink name

Determine where you are going to send the logs collected

Use a search query to determine what is captured by the Sink

Use a search query to determine any exclusions

SANS DFIR
FOR509 | Enterprise Cloud Forensics & Incident Response
63

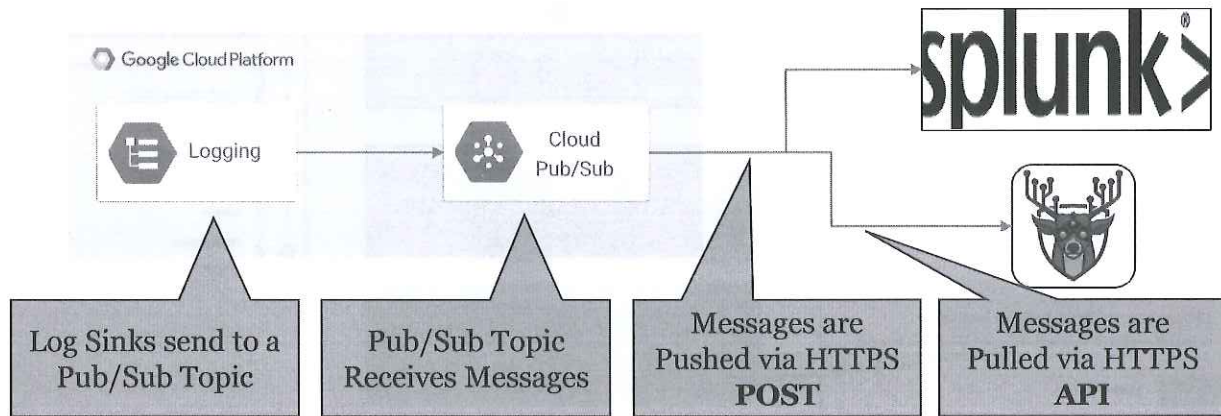
Query Used: `resource.type="gce_subnetwork" AND log_id("compute.googleapis.com/vpc_flows")`

Reference:

[1] <https://for509.com/gsuok>

Exporting Logs Outside of GCP

- So far we've looked at storing logs within GCP
- What happens when we want to get logs into SOF-ELK/Splunk



References:

- [1] <https://for509.com/bp54a>
- [2] <https://for509.com/r12cx>
- [3] <https://for509.com/knxcj>
- [4] <https://for509.com/1slyv>

Using Pub/Sub to Export Logs (I)

Create a topic

A topic forwards messages from publishers to subscribers.

Topic ID *

SOF-ELK-Forwarder

Topic name: projects/suit-ai/topics/SOF-ELK-Forwarder

Add a default subscription

Use a schema

Use a customer-managed encryption key (CMEK)

CANCEL CREATE TOPIC

Subscription name & Topic that is it subscribed to

Message delivery, ideally Push for external Logging

NOTE

The "Topic" creation is straight forward and will produce a "Subscription" already paired with it

Messages will be retained if they cannot be delivered

Edit subscription DELETE

Subscription name

projects/suit-ai/subscriptions/SOF-ELK-Forwarder-sub

Topic name

projects/suit-ai/topics/SOF-ELK-Forwarder

Delivery type

Pull

Push

Endpoint URL *

Enable authentication [Learn more](#)

Message retention duration

Duration is from 10 minutes to 7 days

Days: 7 Hours: 0 Minutes: 0

Retain acknowledged messages

When enabled, acknowledged messages are retained for the message retention duration specified above. This increases message storage fees. [Learn more](#)

This page intentionally left blank.

Using Pub/Sub to Export Logs (2)

- **Messages** can also be **Retained** even if they are delivered successfully, this has a cost associated with it.
 - This will follow the time set by the **Message Retention Duration** for undelivered messages
- **Subscriptions** can also be set with an **Expiration Period** if you want them removed after receiving no messages.
- **Subscriptions** can auto-forward messages that cannot be delivered using **Dead Lettering**

This page intentionally left blank.

Pub/Sub Push Message Type - Example

- **Pushed** messages over HTTP use the below data structure in a POST request from Pub/Sub.

```
{
  "message": {
    "attributes": {
      "key": "value"
    },
    "data": "SGVsbG8gQ2xvdWQgUHVhL1N1YiEgSGVyZSBpcyBteSBtZXNzYWdlIQ==",
    "messageId": "2070443601311540",
    "message_id": "2070443601311540",
    "publishTime": "2021-02-26T19:13:55.749Z",
    "publish_time": "2021-02-26T19:13:55.749Z",
  },
  "subscription": "projects/myproject/subscriptions/mysubscription"
}
```

References:

[1] <https://for509.com/r12cx>

FOR509.4 – Google Cloud Platform (GCP)

Section 4.1: Understanding GCP

Section 4.3: Log Sources, Collection & Log Routing

Section 4.2: VM & Storage Investigations

Section 4.4: GCP Network Forensics

This page intentionally left blank.

Google Cloud Platform Roadmap

4.1: Understanding GCP

4.2: Log Sources, Collection & Log Routing

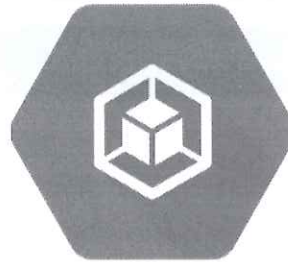
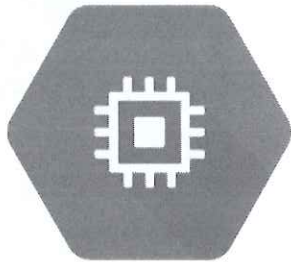
4.3: VM & Storage Investigations

4.4: GCP Network Forensics

- Compute Overview
- VM Snapshotting
- Google Logging Agent
- Logging Agent in AWS
- **Lab 3.2: Google VM Logging Agent - Agent Log Analysis**
- GCP Storage Buckets
- **Lab 3.3: Storage Exfil Abuse**

This page intentionally left blank.

Google Cloud Compute



This page intentionally left blank.

GCP Compute Overview (I)

Google Clouds Compute functionality includes anything within GCP that consists of CPU processing, either dedicated or on-demand.

IaaS	PaaS	FaaS
<ul style="list-style-type: none">• Virtual Machines• Shielded VMs• Cloud GPUs	<ul style="list-style-type: none">• App Engine• Google Kubernetes Engine (GKE)• Cloud Run	<ul style="list-style-type: none">• Cloud Functions• Cloud Workflows

This page intentionally left blank.

GCP Compute Overview (2)

Google Cloud Platform



Compute
Engine



Cloud
Functions

NOTE

There is an ever-growing number of **compute type resources** in GCP

For the purpose of this class, we're going to **only focus on two.**

The principals for these **will apply to many of the others.**

This page intentionally left blank.

Virtual Machine Types - Predefined

E2

- General Purpose
- Up to 32 vCPU's & 128GB RAM

N2

- General Purpose
- Up to 80 vCPUs & 8GB RAM per CPU

N2D

- General Purpose
- Up to 224 vCPUs & 8GB RAM per CPU

N1

- General Purpose
- Up to 96 vCPUs & 6.5GB RAM per CPU

M2/1

- Extremely high memory workloads
- Up to 12TB of RAM

C2

- Extremely high compute workloads
- Up to 3.8Ghz sustained on all cores

A2

- High performance compute workloads
- Parallelized compute workloads (i.e., ML)

NOTE

- GCP has a number of predefined VM types
- VMs can run public OS or private custom images
- VMs can run Docker Containers on suitable OS images
- GCP also has the ability to create custom machine types

References:

- [1] <https://for509.com/r9pb8>

Virtual Machine Types - Others

GPUs

- Can be added to an existing VM
- Ideal for graphic intensive processing
- Only in specific zones

Preemptible

- Must be defined at time of creation
- Ideal for cost reduction
- Do not run all the time, they use excess CPU capacity in a GCP zone

Shielded VMs

- Uses Secure Boot and integrity monitoring
- Can provide DRM with vTPM shielding/sealing

NOTE

GCP also has other types and configurations to VMs

The three listed are most relevant to DFIR work, however, understand there are more outside of this list

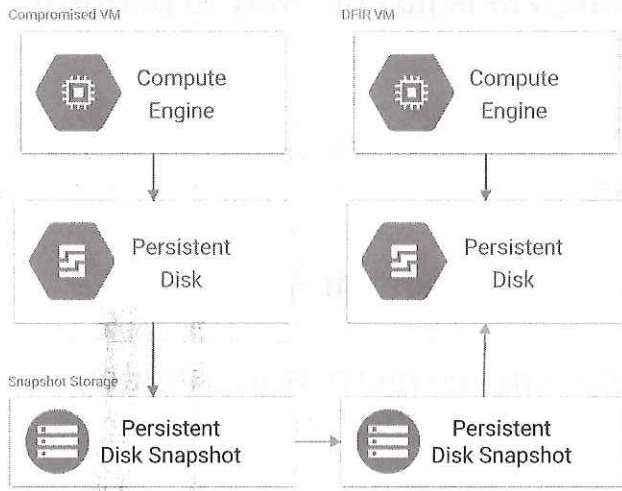
References:

[1] <https://for509.com/w9prz>

[2] <https://for509.com/5xbh3>

[3] <https://for509.com/oarxb>

Virtual Machine – Storage & Snapshots (I)



Capturing a VM Disk Image

- Requires the Compromised VM to have its Disk "Snapshot"
- The snapshot needs to be shared with the user/project/org that has your DFIR VM
- Once shared it can be copied
- The copy can be converted back to a Disk
- The Disk can be mounted as a "read only" drive to your DFIR analysis VM
- From here, normal Disk Forensics would occur (i.e., FOR508)

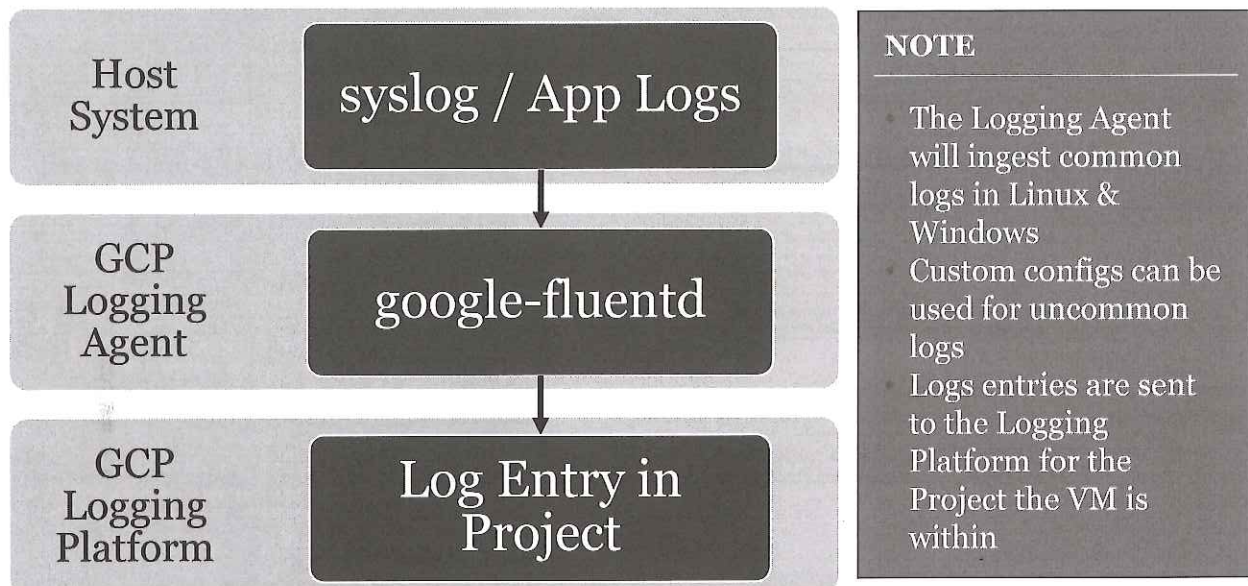
This page intentionally left blank.

Virtual Machine – Storage & Snapshots (2)

- The method of snapshotting a running VM is just one way to perform forensics on a running VM.
- This method has been available since a lot of the IaaS platforms first enabled the ability to snapshot disks.
- It also has one large draw back – it’s a single point in time.
- GCP has built out the concept of collecting telemetry from running VMs and applications on those VMs, known as “**Cloud Logging Agent**”

This page intentionally left blank.

GCP Logging Agent Overview



NOTE

- The Logging Agent will ingest common logs in Linux & Windows
- Custom configs can be used for uncommon logs
- Logs entries are sent to the Logging Platform for the Project the VM is within

References:

- [1] <https://for509.com/st7qb>
- [2] <https://for509.com/kvzui>

GCP Logging Agent Logs

The screenshot displays the GCP Logging Agent logs interface. At the top, a query preview shows the filter: `logName="projects/suit-ai/logs/syslog" AND labels."compute.googleapis.com/resource_name"="instance-1"`. Below this, a table of streaming logs is visible, with one entry highlighted: `projects/suit-ai/logs/syslog "Started Session 3 of user noname."`. A detailed view of this log entry is shown below, including the `resource` and `labels` fields. The `labels` field contains: `instance_id: "6315291702291668", project_id: "suit-ai", zone: "us-west1-b"`. The `resource` field contains: `type: "gce_instance"`. The `insertId` is `"2206487bf0f5"` and the `timestamp` is `"2021-04-10T14:09:50Z"`.

NOTE

Once the Logging Agent is installed it will stream logs to the Logging Platform

Logs are located by "logName" using "projects/[ProjectName]/logs/[LogType]"

To look at specific systems use the "resource_name" label

References:

- [1] <https://for509.com/m5x2c>
- [2] <https://for509.com/v39uh>

Query preview
 logName="projects/suit-ai/logs/syslog" AND labels."compute.googleapis.com/resource_name"="instance-1"

Run query

Configure

SEVERITY	TIMESTAMP	GMT	SUMMARY
Streaming logs...			
>	2021-04-10 14:00:29.000	GMT	projects/suit-ai/logs/syslog "Reloading."
>	2021-04-10 14:00:29.000	GMT	projects/suit-ai/logs/syslog "Condition check resulted in Authentication service fr being skipp...
>	2021-04-10 14:00:34.000	GMT	projects/suit-ai/logs/syslog "[system] Reloaded configuration"
>	2021-04-10 14:00:54.000	GMT	projects/suit-ai/logs/syslog "systemd-hostnamed.service: Succeeded."
>	2021-04-10 14:05:42.000	GMT	projects/suit-ai/logs/syslog "Selected source 169.254.169.254"
>	2021-04-10 14:05:50.000	GMT	projects/suit-ai/logs/syslog "daemon quit"
>	2021-04-10 14:05:50.000	GMT	projects/suit-ai/logs/syslog "packagekit.service: Succeeded."
>	2021-04-10 14:09:25.000	GMT	projects/suit-ai/logs/syslog "Starting Cleanup of Temporary Directories..."
>	2021-04-10 14:09:26.000	GMT	projects/suit-ai/logs/syslog "systemd-tmpfiles-clean.service: Succeeded."
>	2021-04-10 14:09:26.000	GMT	projects/suit-ai/logs/syslog "Finished Cleanup of Temporary Directories."
>	2021-04-10 14:09:42.000	GMT	projects/suit-ai/logs/avxlog "session-1 scope: Succeeded."
>	2021-04-10 14:09:50.000	GMT	projects/suit-ai/logs/syslog "Started Session 3 of user noname."

```
{
  insertId: "z2xpb65rthnfq5z"
  jsonPayload: {4}
  resource: {
    type: "gce_instance"
    labels: {
      instance_id: "651533120232493845"
      project_id: "suit-ai"
      zone: "us-west1-b"
    }
  }
  timestamp: "2021-04-10T14:09:50Z"
  labels: {
    compute.googleapis.com/resource_name: "instance-1"
  }
  logName: "projects/suit-ai/logs/syslog"
  receiveTimestamp: "2021-04-10T14:09:55.11708874Z"
}
```

Hide log summary

Copy link

GCP Logging Agent Monitoring

← VM INSTANCES ▾ 🔍 ⚙️ 🗺️ 🔄 OFF TIME 1H 6H 1D 1W 1M 6W CUSTOM ☆ + 3 RECOMMENDED ALERTS

Filter...

INVENTORY OVERVIEW CPU MEMORY DISK NETWORK EXPLORE

Name ^	Zone	Monitoring agent status	Logging agent status	Public IP	Private IP	Size	Connect
instance-1	us-west1-b	● Install Agent	● Latest	35.197.	10.138.0.6	e2-medium	SSH ▾
instance-2	us-west1-b	● Install Agent	● Install Agent	34.105.	10.138.0.7	e2-medium	SSH ▾

Items per page: 25 1 - 2 of 2 < >

NOTE

GCP Monitoring gives you the ability to see which VM's have the Logging Agent installed and running.

You can also install the Logging Agent from the Console using `gcloud` commands

References:

[1] <https://for509.com/3sjlx>

Install the Logging Agent

Use the Cloud Logging agent to gather logging metrics from VM instances and send them to Cloud Monitoring. [Learn more](#)

Confirm VM operating system

Review VM details and select the relevant OS.

[View additional details.](#)

Name	instance-2
Boot disk image	ubuntu-2004-lts

Operating System *

Ubuntu

Select the VM OS to install the appropriate agent

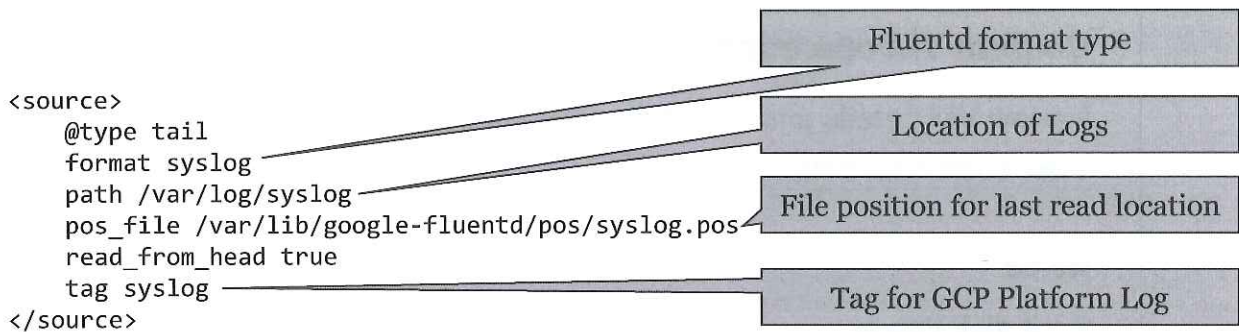
```
$ gcloud beta compute ssh instance-2 --proj
```

INSTALL AGENT

CANCEL

GCP Logging Agent – Structured and Unstructured (I)

- Logging Agent is based on “**fluentd**”
- **Fluentd** has a number of support parsers that **google-fluentd** can use to transform data to JSON when configured



References:

- [1] <https://for509.com/0g215>
- [2] <https://for509.com/5pftw>

GCP Logging Agent – Structured and Unstructured (2)

- **Fluentd** existing parsers can transform syslog data into JSON

```
<1> Apr 10 14:09:50 instance-1 system: Started Session 3 of user noname.
```

```
jsonPayload: {  
  pid: "1"  
  message: "Started Session 3 of user noname."  
  ident: "systemd"  
  host: "instance-1"  
}  
timestamp: "2021-04-10T14:09:50Z"
```

References:

[1] <https://for509.com/0g215>

[2] <https://for509.com/5pftw>

GCP Logging Agent with AWS and Ops Agent

- **The GCP Logging Agent is also compatible with AWS Linux and Windows VM's**
 - **This requires an AWS Connector – usually a separate Project within your Organization**
- **There is also an “Ops Agent” in GCP**
 - **This is used for VMs with very high log throughput or resource utilization**
 - **This agent is also used for performance monitoring of VMs (i.e., CPU, Memory, Disk, etc.)**

References:

[1] <https://for509.com/5k1zv>

[2] <https://for509.com/dwntc>

VM Agent Log Lab Example (I)

Limit your data set
log_name is
*/GCEGuestAgent

Make sure you are
looking at the gcp-*
index

elastic Discover

log_name:*/GCEGuestAgent Add filter

gcp-*

1,036 hits

2021-01-27 12:38:27.785 +00:00 - 2021-04-27 12:38:27.785 +00:00 Auto

Count

Time

system_message

2021-03-15 12:55:25.830 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.

2021-03-15 12:55:25.826 +00:00 Creating user admin.

2021-03-15 12:55:19.665 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.

2021-03-15 12:55:19.661 +00:00 Creating user admin.

2021-03-15 12:55:14.042 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.

2021-03-15 12:55:14.037 +00:00 Creating user admin.

2021-03-15 12:55:08.495 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.

The example above shows you SOF-ELK with the VM Agent logs extracted from GCP in JSON format and loaded into SOF-ELK. In the Lab, that is coming up, your data set will already be limited to only the GCP VM Agent logs, however, if you have loaded other data into SOF-ELK you will need to limit your data set.

The data set under the “gcp-*” index will hold all the GCP data, except for Flow Logs. When you’re viewing this index, you will see all GCP data loaded in SOF-ELK. Using the “Available fields” section locate the “log_name” field, once you click on this field it will show you the other services that are also loaded into SOF-ELK from previous GCP data you may have been working with. Select the one of the entries that end with “GCEGuestAgent”, once selected you will need to modify this search slightly, click on the filter you just created at the top and alter the Value to be “*/GCEGuestAgent”. For this example in the course, we are going to expose all the VM Agent logs, however, in practice you may want to limit this to specific projects or folders. You can still use this technique to limit your logs to a specific project or folder.

Remember, you can always click on the filter you’ve just put in place and select “Temporarily disable” if you want to see all GCP data related to your search in the search bar at the top.

log_name: */GCEGuestAgent X + Add filter

gcp-*

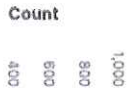
Search field names

Filter by type 0

- resource.location
- resource_name
- resource_type
- severity
- source_ip
- tags
- type
- useragent
- useragentinfo.build
- useragentinfo.device
- useragentinfo.major
- useragentinfo.minor
- useragentinfo.name
- useragentinfo.os
- useragentinfo.os_major
- useragentinfo.os_minor

1,036 hits

2021-01-27 12:38:27.785 +00:00 - 2021-04-27 12:38:27.785 +00:00 Auto



system_message

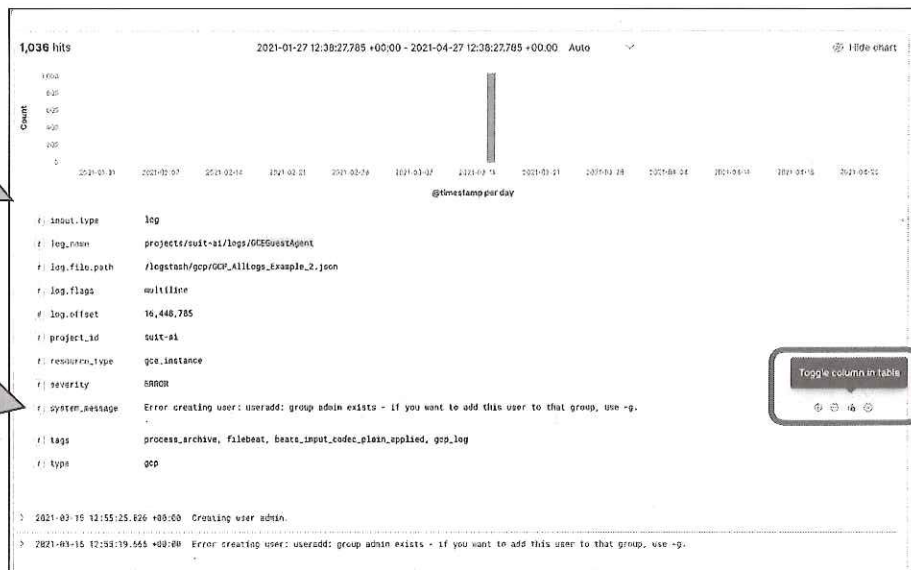
@timestamp per day

- 2021-03-15 12:55:25.830 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.
- 2021-03-15 12:55:25.826 +00:00 Creating user admin.
- 2021-03-15 12:55:19.665 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.
- 2021-03-15 12:55:19.661 +00:00 Creating user admin.
- 2021-03-15 12:55:14.842 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.
- 2021-03-15 12:55:14.837 +00:00 Creating user admin.
- 2021-03-15 12:55:08.485 +00:00 Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.

VM Agent Log Lab Example (2)

Expand one of the log entries so reveal all the fields.

Hover over the highlight buttons on the right and select "Toggle column in table"



You may want to get a better view of the data that has been capture by the VM Agent. You can do this by adding in a field of data to the non-expanded data view. If you want to see System Messages in you unexpanded explorer view, you can expand one of the records and find the "system_message" field. If you hover of the right-hand side of the field, you will see an icon that represents "Toggle column in table", if you select this it will put this field in the unexpanded view of the record making it easier to see data in the Explorer view.

log_name: */GCEquestAgent x + Add filter

gcp-*

Search field names

Filter by type 0

- log.file.path
- log.flags
- log.offset
- ports
- projectId
- resource.location
- resource.name
- resource.type
- severity
- source_ip
- tags
- type
- useragent
- useragentinfo.build
- useragentinfo.device
- useragentinfo.major
- useragentinfo.minor
- useragentinfo.name
- useragentinfo.os
- useragentinfo.os.major
- useragentinfo.os.minor
- useragentinfo.os.name
- useragentinfo.patch
- username

1,036 hits

2021-01-27 12:38:27.785 +00:00 - 2021-04-27 12:38:27.785 +00:00 Auto



#	log.offset	ports	projectId	resource.location	resource.name	resource.type	severity	source_ip	tags	type	useragent	useragentinfo.build	useragentinfo.device	useragentinfo.major	useragentinfo.minor	useragentinfo.name	useragentinfo.os	useragentinfo.os.major	useragentinfo.os.minor	useragentinfo.os.name	useragentinfo.patch	username	
							log		projects/suit-ai/logs/GCEquestAgent														
							/logstash/gcp/GCP_AllLogs_Example_2.json		multiline														
							16,448,785																
							suit-ai																
							gce_instance																
							ERROR																
							Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.																
							process_archive, filebeat, beats_input_codec_plain_applied, gcp_log																
							gcp																
							Creating user admin.																
							Error creating user: useradd: group admin exists - if you want to add this user to that group, use -g.																
							Creation user admin																

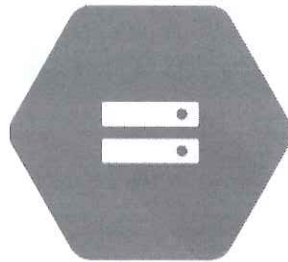
Toggle column in table

Lab 4.2

Google VM Logging Agent - Agent Log Analysis

This page intentionally left blank.

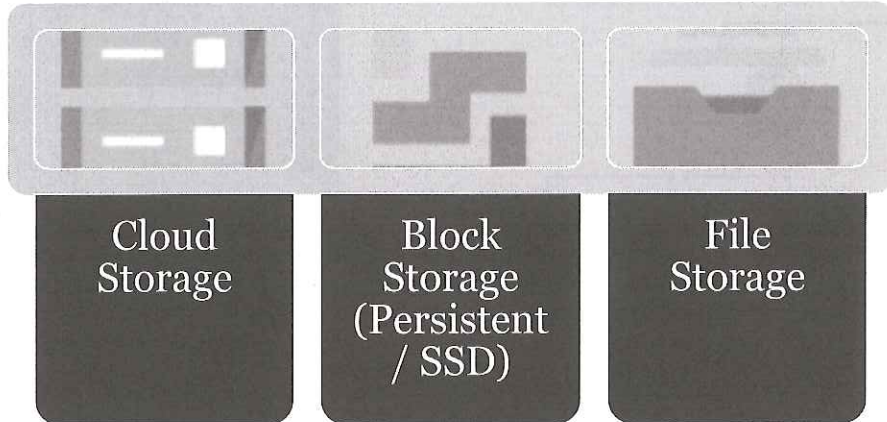
Google Cloud Storage



This page intentionally left blank.

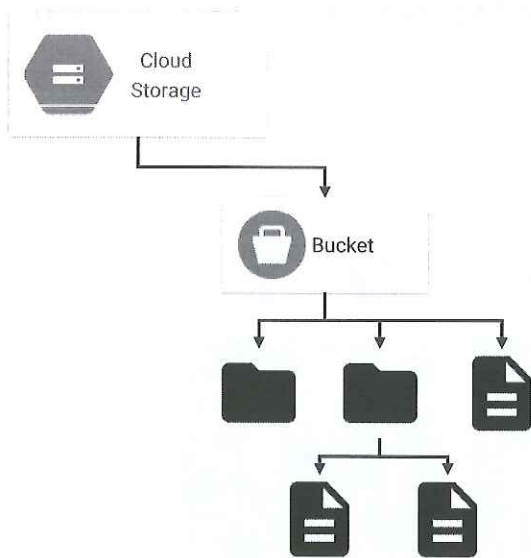
GCP Storage Overview

There are several different Storage types in GCP along with features that can be used on the different storage types. For DFIR, we're going to focus on "Cloud Storage" (Buckets)



This page intentionally left blank.

GCP Buckets Overview



NOTE

Cloud Storage allows you to create “Buckets” within “Projects” to store data.

Within in a Bucket you can have folders, sub-folders and files.

All the contents within the Bucket follow the permissions and polices of the parent Bucket.

This page intentionally left blank.

GCP Bucket Permissions Uniform

← Bucket details

flight-maps

OBJECTS CONFIGURATION PERMISSIONS PERMISSIONS

Overview

Created	March 29, 2021 at 10:32:48 PM GMT+11
Updated	March 29, 2021 at 10:32:48 PM GMT+11
Location type	Region
Location	us-east1 (South Carolina)
Default storage class	Standard
Requester pays	<input type="radio"/> OFF
Labels	None
Cloud Console URL	https://console.cloud.google.com/storage/buckets/flight-maps
gsutil URI	gs://flight-maps

Permissions

Access control	Uniform
Public access	Not public

Protection

Encryption type	Google-managed key
-----------------	--------------------

Bucket Name

Bucket Configuration Panel

Access Control set to "Uniform" by default

NOTE

These are the default settings for Google Bucket permissions, to prevent you from exposing the Bucket's data by default

References:

[1] <https://for509.com/phmxg>

GCP Bucket Permissions Fine-Grained

Edit the ACLs on an object

Access type as **Reader or **Owner**.**

Domain: Shares with another Organization
Group: Shared to a Workspace Group
User: Individual users
Project: Shares entirely with another project
Public: Open to the Internet.

References:

[1] <https://for509.com/48hrz>

GCP Bucket Attacks

Recon

- Attacker scans all GCP for possible Buckets based on key words

Orientate

- Determine if the ability to list Objects is available

Steal

- Attacker downloads open access Objects

Escalate

- Check permissions to perform other actions (write/delete), or escalate permission to Storage Admin

NOTE

The most common attack against Buckets is accessing data/files stored in buckets due to misconfiguration.

GCPBucketBrute automates this attack on GCP Buckets.

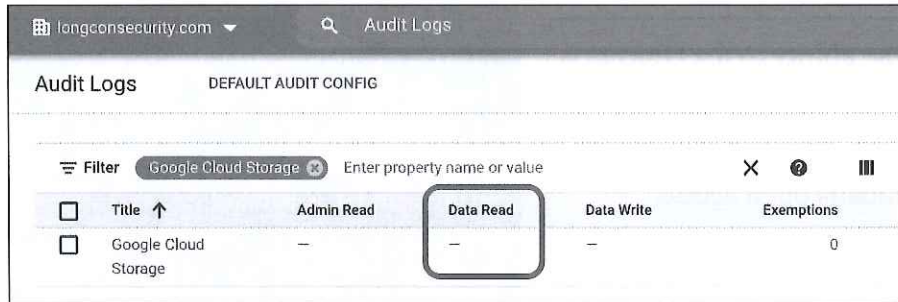
Resources:

[1] <https://for509.com/afj2q>

[2] <https://for509.com/95h84>

Cloud Storage – Enabling Object Logging

WARNING: Object logging is not turned on by default
This mean no object access logging to detect DLP 🙄



The screenshot shows the Google Cloud Audit Logs interface. At the top, there's a search bar with 'Audit Logs' and a filter set to 'Google Cloud Storage'. Below the filter is a table with columns: Title, Admin Read, Data Read, Data Write, and Exemptions. The 'Data Read' column is highlighted with a red box. The table shows one entry for 'Google Cloud Storage' with dashes in the 'Admin Read', 'Data Read', and 'Data Write' columns, and '0' in the 'Exemptions' column.

<input type="checkbox"/>	Title ↑	Admin Read	Data Read	Data Write	Exemptions
<input type="checkbox"/>	Google Cloud Storage	-	-	-	0

NOTE

You need to enable “**Data Read**” if you want to see access to Objects in Buckets.

Only do this on sensitive data – it will produce a *LOT* of logs.

This page intentionally left blank.

Cloud Storage – Detecting Exfil in Logs

Query preview
resource.type="gcs_bucket" resource.labels.bucket_name="flight-maps"

Save Stream logs Run query

Query results Jump to now Actions Configure

SEVERITY	TIMESTAMP	GMT	SUMMARY
	> 2021-04-13 04:28:30.260	GMT	IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
			IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
			IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
			IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
	> 2021-04-13 04:28:31.216	GMT	IAH storage.googleapis.com storage.objects.get -
			IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
			IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
			IAH storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
	> 2021-04-13 04:28:33.543	GMT	IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
	> 2021-04-13 04:28:33.560	GMT	IAH storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
			IAH storage.googleapis.com storage.getIamPermissions projects/_/buckets/flight-maps admin@longconsecurity.com audi...
			IAH storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
			IAH storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...
	> 2021-04-13 04:28:34.443	GMT	IAH storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...

Unauthenticated download of object

Authenticated download of object

Authenticated File listing of objects

This page intentionally left blank.

Query preview
resource.type="gcs_bucket" resource.labels.bucket_name="flight-maps"

Save Stream logs Run query

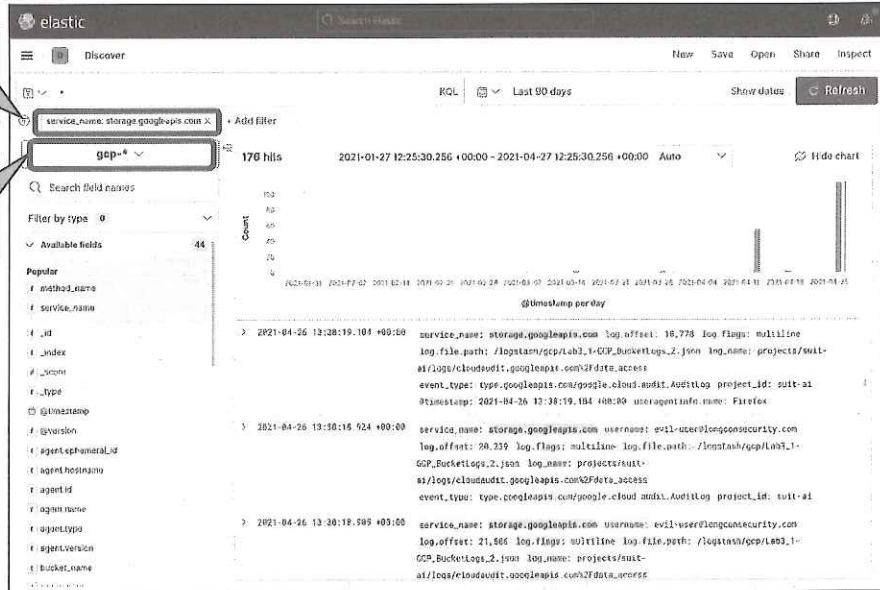
Query results [1]

SEVERITY	TIMESTAMP	GMT	SUMMARY	Jump to now	Actions	Configure
> i	2021-04-13 04:28:30.268 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:30.291 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:30.295 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:31.371 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:31.216 GMT	GMT	IAM storage.googleapis.com storage.objects.get ...			
> i	2021-04-13 04:28:31.268 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:33.480 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:33.541 GMT	GMT	IAM storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:33.545 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:33.560 GMT	GMT	IAM storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:33.580 GMT	GMT	IAM storage.googleapis.com storage.getiampermissions projects/_/buckets/flight-maps admin@longconsecurity.com audi...			
> i	2021-04-13 04:28:33.518 GMT	GMT	IAM storage.googleapis.com storage.buckets.get projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:34.423 GMT	GMT	IAM storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			
> i	2021-04-13 04:28:34.443 GMT	GMT	IAM storage.googleapis.com storage.objects.list projects/_/buckets/flight-maps admin@longconsecurity.com audit_log...			

Cloud Storage Lab Example

Limit your data set to **storage.googleapis.com**

Make sure you are looking at the **gcp-*** index



The example above shows you SOF-ELK with the Bucket Storage logs extracted from GCP in JSON format and loaded into SOF-ELK. In the Lab this incoming data set will already be limited to only the Bucket Storage logs, however, if you have loaded other data into SOF-ELK you will need to limit your data set.

The data set under the “gcp-*” index will hold all of the GCP data, except for Flow Logs. So, when you’re viewing this index you will see all GCP data loaded in SOF-ELK. Using the “Available fields” section locate the “service_name” field, once you click on this field it will show you the other services that are also loaded into SOF-ELK from previous GCP data you may have been working with. Select the “storage.googleapis.com” “service_name” to limit your data to only logs related to GCP Storage data. This will aid in ensuring searches you run in the search bar are limited to GCP Storage data. You can always click on the limit you’ve just put in place and select “Temporarily disable” if you want to see all GCP data related to your search in the search bar at the top.

service_name: storage.googleapis.com X

+ Add filter

KQL Last 90 days

Show dates

Refresh

gcp-*

Search field names

Filter by type 0

Available fields 44

- Popular
- method_name
- service_name
- _id
- _index
- _score
- _type
- @timestamp
- @version
- agentephemeral_id
- agenthostname
- agent_id
- agent_name
- agent_type
- agent_version
- bucket_name

176 hits

2021-01-27 12:25:30.256 +00:00 - 2021-04-27 12:25:30.256 +00:00

Auto

Hide chart



> 2021-04-26 13:38:19.104 +00:00

```

service_name: storage.googleapis.com log.offset: 18.778 log.flags: multiline
log.file.path: /logstash/gcp/lab3_1-GCP_Bucketlogs_2.json log_name: projects/suit-ai/logs/cloudaudit.googleapis.com%2Fdata_access
event_type: type.googleapis.com/google.cloud.audit.Auditlog project_id: suit-ai
timestamp: 2021-04-26 13:38:19.104 +00:00 useragentinfo.name: Firefox

```

> 2021-04-26 13:38:18.924 +00:00

```

service_name: storage.googleapis.com username: evil-user@longconsecurity.com
log.offset: 20.239 log.flags: multiline log.file.path: /logstash/gcp/lab3_1-GCP_Bucketlogs_2.json log_name: projects/suit-ai/logs/cloudaudit.googleapis.com%2Fdata_access
event_type: type.googleapis.com/google.cloud.audit.Auditlog project_id: suit-ai

```

> 2021-04-26 13:38:18.905 +00:00

```

service_name: storage.googleapis.com username: evil-user@longconsecurity.com
log.offset: 21.586 log.flags: multiline log.file.path: /logstash/gcp/lab3_1-GCP_Bucketlogs_2.json log_name: projects/suit-ai/logs/cloudaudit.googleapis.com%2Fdata_access

```

Lab 4.3

Storage Abuse and Exfil

This page intentionally left blank.

FOR509.4 – Google Cloud Platform (GCP)

Section 4.1: Understanding GCP

Section 4.3: Log Sources, Collection & Log Routing

Section 4.2: VM & Storage Investigations

Section 4.4: GCP Network Forensics

This page intentionally left blank.

Google Cloud Platform Roadmap

4.1: Understanding GCP

4.2: Log Sources, Collection & Log Routing

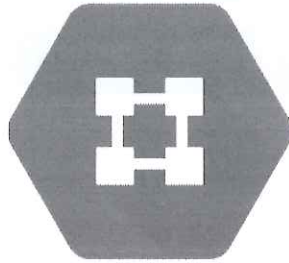
4.3: VM & Storage Investigations

4.4: GCP Network Forensics

- GCP Network DFIR Services Overview
- GCP VPC Overview
- VPC Networking
- VPC Flow Logs
- Firewall Rules & Logging
- GCP Packet Mirroring
- **Lab 3.4: GCP Network Forensics**

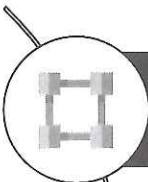
This page intentionally left blank.

Google Cloud Virtual Network

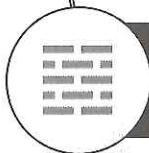


This page intentionally left blank.

GCP Network DFIR Services Overview



VPC Flow Logs – provides sampled flow data from network subnets within a VPC



Cloud Firewall - used to apply on individual hosts or on VPCs



Packet Mirroring - allows capture of network packet from specific VMs

Cloud Firewalls

- Can be defined as a policy at the Folder and Organization level.

GCP VPC Overview

- **Google Cloud's VPC provides network connectivity between compute instances, other VPCs, and VPN tunnels or cloud interconnects.**
- **Andromeda is the technology that support traffic switching and routing for VPCs**
- **Subnets are considered regional, all other VPC resources are considered global (i.e., Firewalls, NAT, Routing)**
- **VPCs only support IPv4 unicast. There is no IPv6, broadcast or multicast traffic within a VPC.**

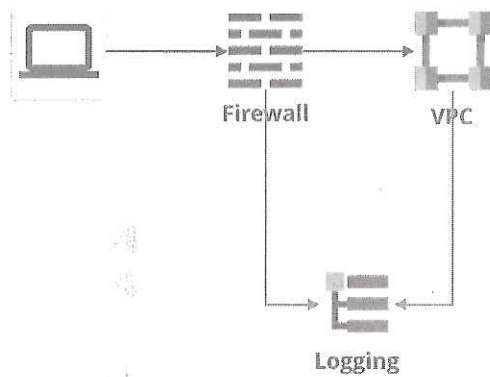
IPv6 can be achieved by using a global load balancer for public facing services.

References:

[1] <https://for509.com/h2k1g>

[2] <https://for509.com/6ctfx>

GCP Networking – VPC Network (I)



VPC LOGGING

VPC's usually have Firewall rules applied/attached to a VPC – this occurs across all subnets within a VPC.

Firewalls can produce logs per rule, this applies to success or failure. This logging is disabled by default.

VPC's allow provide “sampled” Flow Logging per subnet within a VPC. This is disabled by default.

This page intentionally left blank.

GCP Networking – VPC Network (2)

The screenshot shows the 'VPC network details' page for a network named 'yellow-jacket-prod-network'. The page has a top navigation bar with 'EDIT' and 'DELETE VPC NETWORK' buttons. Below the network name, there are tabs for 'SUBNETS', 'STATIC INTERNAL IP ADDRESSES', 'FIREWALL POLICIES', 'FIREWALL RULES', 'ROUTES', 'VPC NETWORK PEERING', and 'PRIVATE SERVICE CONNECTION'. The 'FIREWALL RULES' tab is highlighted, and a callout box points to it with the text 'Access the Firewall Rules for the VPC to add/remove rules'. Below the tabs, there is a 'FLOW LOGS' dropdown menu, and a callout box points to it with the text 'Access Flow Log configuration that is applied to selected subnets within the VPC'. Below the dropdown is a table of subnets.

<input type="checkbox"/>	Name ↑	Region	IP address ranges	Gateway	Private Google Access	Flow logs	
<input type="checkbox"/>	yellow-jacket-prod-network	us-central1	10.128.0.0/20	10.128.0.1	Off	Off	🗑️
<input type="checkbox"/>	yellow-jacket-prod-network	eu-west1	10.132.0.0/20	10.132.0.1	Off	Off	🗑️
<input type="checkbox"/>	yellow-jacket-prod-network	us-west1	10.138.0.0/20	10.138.0.1	Off	Off	🗑️
<input type="checkbox"/>	yellow-jacket-prod-network	asia-east1	10.140.0.0/20	10.140.0.1	Off	Off	🗑️
<input type="checkbox"/>	yellow-jacket-prod-network	us-east1	10.142.0.0/20	10.142.0.1	Off	Off	🗑️
<input type="checkbox"/>	yellow-jacket-prod-network	asia-southeast1	10.146.0.0/20	10.146.0.1	Off	Off	🗑️

This page intentionally left blank.

VPC Flow Log Configuration

VPC flow logs can increase costs

Turning on VPC flow logs won't affect performance, but some systems generate a large number of logs. This can increase costs in Stackdriver as well as log export destinations such as BigQuery and Cloud Pub/Sub. [Learn more](#)

Manage these logs and resulting costs by adjusting the settings below, or in [Cloud Logging](#)

Aggregation Interval

5 SEC 30 SEC 1 MIN 5 MIN 10 MIN 15 MIN

Additional fields

Include metadata

Sample rate

50

Estimated logs generated per day: 0 B

CANCEL SAVE

FLOW LOG CONFIGURATION

VPC Flow Logs are only sampled, they **are not 100%** of all flows that occur within a subnet.

Flow Logs are really intended for performance monitoring and summarized data.

They can prove useful for log running incidents with sustained C2 communications, or DDoS type incidents.

Disabling "Includes metadata" will reduce the overall log storage size.

References:

[1] <https://for509.com/knzmq>

[2] <https://for509.com/aoprn>

VPC Flow Log Capture and Store

TCP and UDP traffic is sampled at the VM

Filtering for Flows is applied

Flows are aggregated to produce a "Flow Log Entry"

Flows are sampled again based on "Sample Rate"

Metadata for the Flows can be dropped if needed

Flows are written into Cloud Logging

Logs are forwarded with Pub/Sub if enabled

References:

[1] <https://for509.com/knzmq>

VPC Firewall Rules (1)

The screenshot shows the 'Create a firewall rule' interface in the AWS VPC console. The form is divided into several sections, with callouts pointing to specific fields:

- Firewall Rule Name:** Points to the 'Name' field, which contains 'allow-https'.
- Source / Destination Rule:** Points to the 'Source IP ranges' field, which contains '0.0.0.0/0'.
- Enabled/Disable Logging:** Points to the 'Logs' section, where 'On' is selected.
- Protocols and Ports:** Points to the 'Protocols and ports' section, where 'tcp: 443' and 'udp: 443' are selected.
- Priority to determine order:** Points to the 'Priority' field, which is set to '1000'.
- Traffic Direction:** Points to the 'Direction of traffic' section, where 'Ingress' is selected.

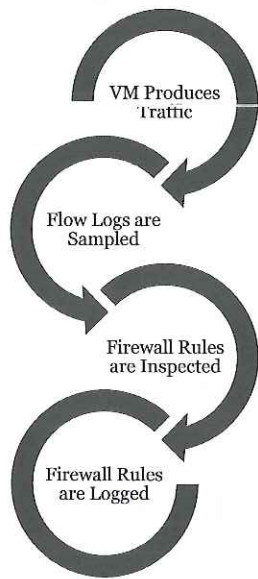
Other visible fields include 'Additional fields' (with 'Include metadata' checked), 'Network' (set to 'yellow-jacket-prod-network'), and 'Action on match' (set to 'Allow').

Disabling “Includes metadata” will reduce the overall log storage size.

References:

[1] <https://for509.com/798su>

VPC Firewall Rules (2)



LOGGING ANALYSIS

Firewall rules are assessed after Flow Logs are generated.

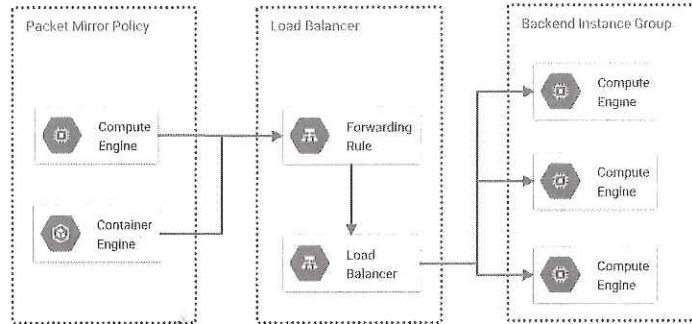
You could see Flow Logs indicating traffic occurred, however, Firewall Rules may prevent the traffic ever leaving the VPC.

Review Firewall Logs and Flow Logs together to determine if traffic ever made it out of your VPC.

References:

[1] <https://for509.com/knzmq>

GCP Packet Mirroring



A Mirror Policy defines which system(s) to capture traffic from

A Load Balancer determines where the capture packets are sent

The Backend Instances are where the Mirrored traffic is sent for capture/processing

MIRRORING PRINCIPALS

Packet Mirroring is defined per VM instance or per GKE Cluster.

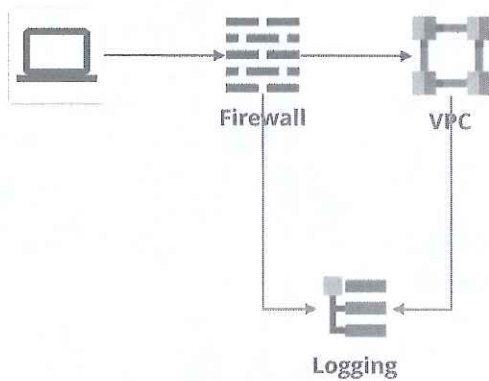
GCP does not currently enable you to store a PCAP file in a Bucket. It has to be processed by a system you defined.

For DFIR purposes, we could setup our Backend Instances to be Moloch or NSM devices to capture and analysis.

References:

- [1] <https://for509.com/fp614>
- [2] <https://for509.com/jaq42>

GCP Networking – VPC Network (3)



VPC LOGGING

VPC's usually have Firewall rules applied/attached to a VPC – this occurs across all subnets within a VPC.

Firewalls can produce logs per rule, this applies to success or failure. This logging is disabled by default.

VPC's allow provide “sampled” Flow Logging per subnet within a VPC. This is disabled by default.

This page intentionally left blank.

+ Add filter

netflow-*

Search field names

Filter by type 0

Selected fields 6

- aprotocol
- destination_ip
- destination_port
- source_ip
- source_port
- source_vrn_name

Available fields 64

- _id
- _index
- _score
- _type
- @timestamp
- @version
- agent_ephemeral_id
- agent_hostname
- agent_id
- agent_name
- agent_type
- agent_version
- destination_as

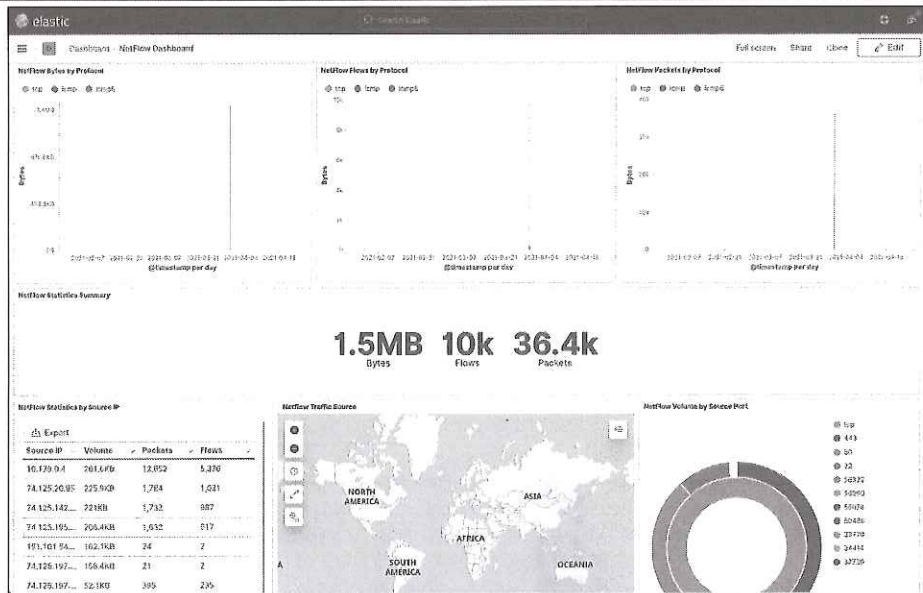
9,999 hits

2021-01-27 14:04:24:102 +00:00 - 2021-04-27 14:04:24:103 +00:00 Auto



Time	source_ip	source_port	destination_ip	destination_port	aprotocol	source_vrn_name
> 2021-03-31 10:51:42.145Z	10.138.0.4	49210	142.250.107.95	443	tcp	Instance-1
> 2021-03-31 10:51:42.144Z	10.138.0.4	49210	142.250.107.95	443	tcp	Instance-1
> 2021-03-31 10:51:30.715Z	173.194.203.95	443	10.138.0.4	35804	tcp	-
> 2021-03-31 10:51:30.714Z	173.194.203.95	443	10.138.0.4	35804	tcp	-
> 2021-03-31 10:51:30.712Z	10.138.0.4	35804	173.194.203.95	443	tcp	Instance-1
> 2021-03-31 10:51:30.704Z	10.138.0.4	58824	74.125.142.95	443	tcp	Instance-1
> 2021-03-31 10:51:30.704Z	74.125.142.95	443	10.138.0.4	58824	tcp	-
> 2021-03-31 10:51:30.704Z	74.125.142.95	443	10.138.0.4	58824	tcp	-
> 2021-03-31 10:51:30.691Z	142.250.107.95	443	10.138.0.4	49210	tcp	-
> 2021-03-31 10:51:30.690Z	10.138.0.4	49210	142.250.107.95	443	tcp	Instance-1
> 2021-03-31 10:51:30.681Z	74.125.20.95	443	10.138.0.4	45790	tcp	-
> 2021-03-31 10:51:17.184Z	10.138.0.4	45790	74.125.20.95	443	tcp	Instance-1
> 2021-03-31 10:51:17.184Z	74.125.142.95	443	10.138.0.4	58824	tcp	-
> 2021-03-31 10:51:17.184Z	74.125.20.95	443	10.138.0.4	45790	tcp	-

Cloud Network Forensics Lab Example (2)

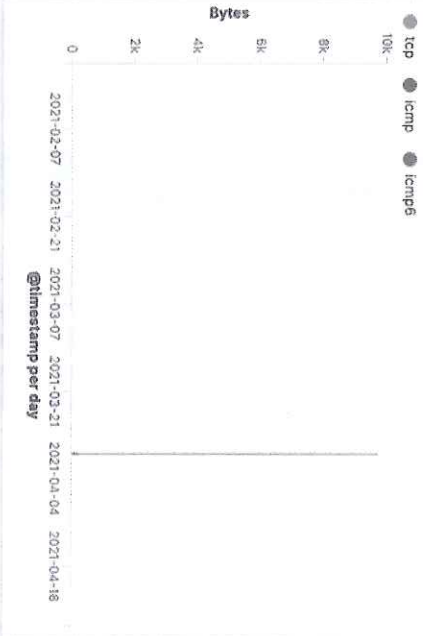


The example shows the pre-made flow data dashboard with the same data you were viewing on the previous page. This uses the power of SOF-ELK to arrange and group flow data. Additionally, this dashboard would also allow you to see flow data information from any other flow data source you loaded into SOF-ELK at the same time. This is simply an example of the same data presented graphically.

NetFlow Bytes by Protocol



NetFlow Flows by Protocol



NetFlow Packets by Protocol



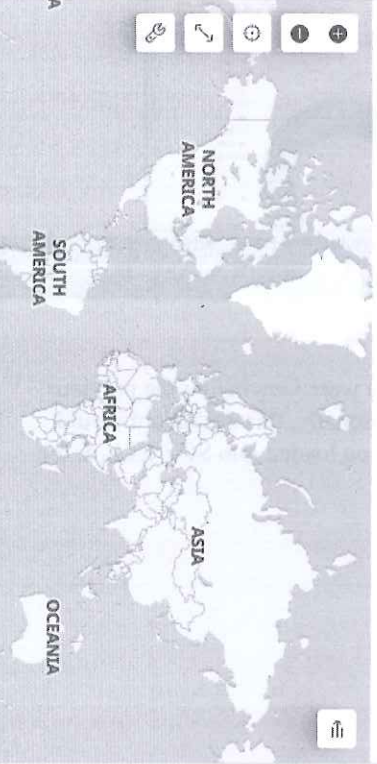
NetFlow Statistics Summary

1.5MB Bytes
10k Flows
36.4k Packets

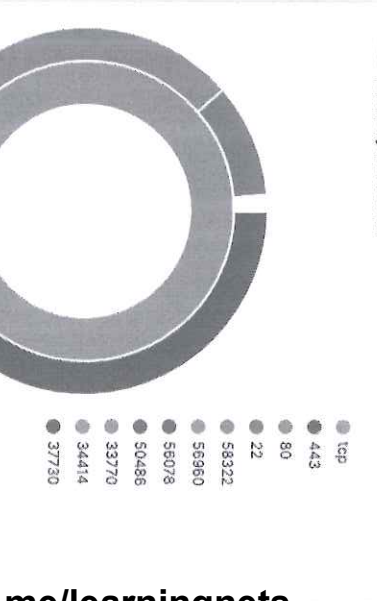
NetFlow Statistics by Source IP

Source IP	Volume	Packets	Flows
10.138.0.4	261.6KB	12,652	5,336
74.125.20.95	225.9KB	1,784	1,031
74.125.142....	221KB	1,732	987
74.125.195....	206.4KB	1,632	917
151.101.54....	162.1KB	24	2
74.125.197....	158.4KB	21	2
74.125.197....	52.1KB	395	235

Netflow Traffic Source



NetFlow Volume by Source Port



Lab 4.4

Google Cloud – Network Forensics

This page intentionally left blank.

SANS DFIR

DIGITAL FORENSICS | INCIDENT RESPONSE

f 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

Josh Lemon
josh@joshlemon.com.au
Twitter: @joshlemon



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: Josh Lemon

Email: josh@joshlemon.com.au

Twitter: @joshlemon

"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](https://www.sansinstitute.com)

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>