



Cloud forensics

Mariusz Burdach

05-2024

Agenda

1. Cloud computing types (PaaS/SaaS/IaaS) - what data can be seized?
2. Sizing non-volatile data
 - a. Cloud Logs
 - b. Virtual machines including k8s nodes
 - c. Encrypted disks
3. Forensic environment preparation
 - a. Evidence protection
 - b. Data integrity verification
 - c. Microsoft Azure and Google Cloud Platform reference architectures
4. Common issues

Technical challenges

1. Data volatility and data retention
2. Data location and distributed storage
3. Limited access to data
4. Readiness of incident response teams to investigate cloud environments

Cloud computing types and forensics data types

	On Prem	IaaS	PaaS	SaaS
Application/services logs				
file system data				
logs of operating system				
Images				
physical drives				
Volatile memory*				

 Available by default
 Requires additional tools

*Suspend (GCP) - currently not useful

*Hibernation (Azure) - require additional set up

Examples of cloud computing services

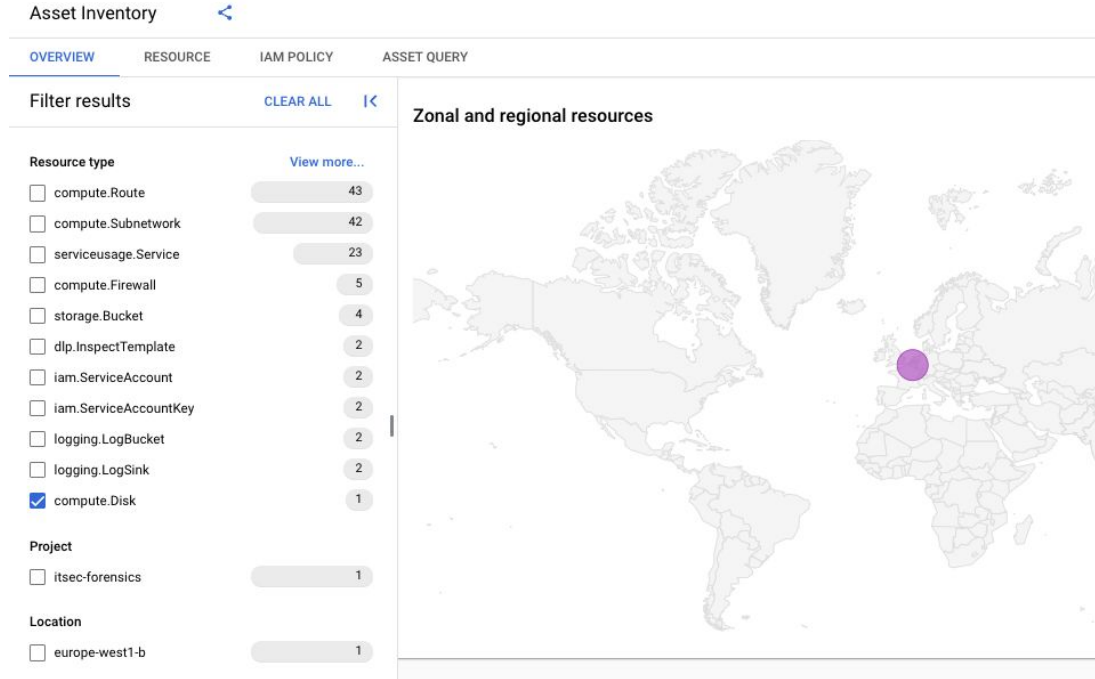
SaaS - GCP IAM, Entra ID, Office365, Google Workspace, GCP KMS, Key Vault, GCP Console, Azure Console

IaaS - GCP Compute Engine, Azure Virtual Machine

PaaS - Azure Web Apps, GCP App Engine

Where is the data?

Regions Zones



Event logs

Audit Logs (Who What Where When)

Enabled audit logs and default retention period

Google GCP

- Admin Activity - 400 days
- Data Access (by default only BigQuery) - 30 days
- System Event - 400 days
- Policy Deny - 30 days

Google Workspace

- Audit logs (Admin, Login, OAuth Token, SAML, Group, Gmail, Drive, Chat, Drive, Device, etc) - 180 days

Microsoft Azure

- Activity Log - 90 days
- Entra ID logs - 30 days

Microsoft 365 / Office 365

- Audit Log (App administration, User administration, Entra administration, Directory administration, Exchange admin, Exchange mailbox, Defender for Endpoint, Teams, Sharing and access request, etc) - 90 days -> 180 days

GCP - Admin Activity

Data contained in audit logs:

- administrative actions that modify the configuration or metadata of GCP resources
- user or service account who modify roles

Examples:

- adding role to user for project, folder or organisation
- removing compute engine

GCP - Data Access

Data contained in audit logs:

- requests that read the configuration or metadata of GCP resources (ADMIN_READ)
- requests that create, modify, delete, read user-provided resource data

Examples:

- read, write, modify or delete user data in BigQuery dataset
- read a cloud storage object

GCP - System Event

Data contained in audit logs:

- actions that modify the configuration of resources (but changes are initialized by Google systems)

Examples:

- automatic backup event or scheduled snapshot
- automatic scaling events

GCP - Policy Deny

Data contained in audit logs:

- denied access to GCP services because of a security policy violation

Examples:

- attempt of adding service account to project
- creation of resource in prohibited region

Azure - Activity (subscription log)

Data contained in audit logs:

- activities related to modify (create/update/delete) all Azure resources
- activities related to RBAC

Examples:

- removing virtual machine
- creating network security group
- adding user to group

Azure - Directory (tenant logs)

Data contained in audit logs:

- records of access to system activity - changes in service configuration, activity related to Azure services, changes in groups and users.
- Sign in Logs - information about sign-ins into Azure, access to application and other resources by users, service principals and managed identities.

Examples:

- history of logins to services
- sign-in locations
- authentication methods used by users
- changes of permissions to service

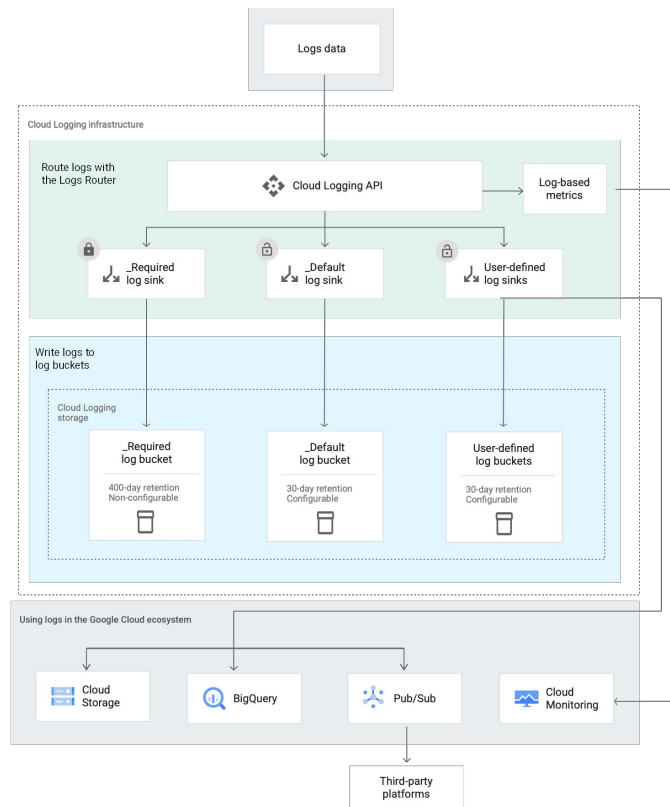
Log management in GCP

- Organizations, Folders and Projects
- Sinks
 - supported destinations
 - filters
- Configuration of additional logs

Data access audit logs configuration

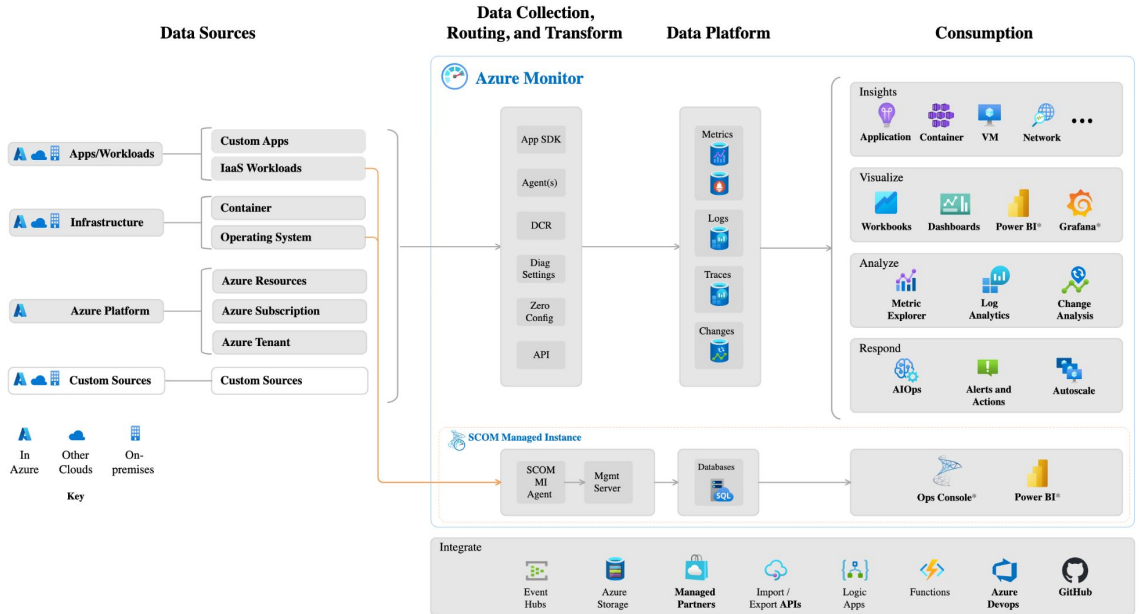
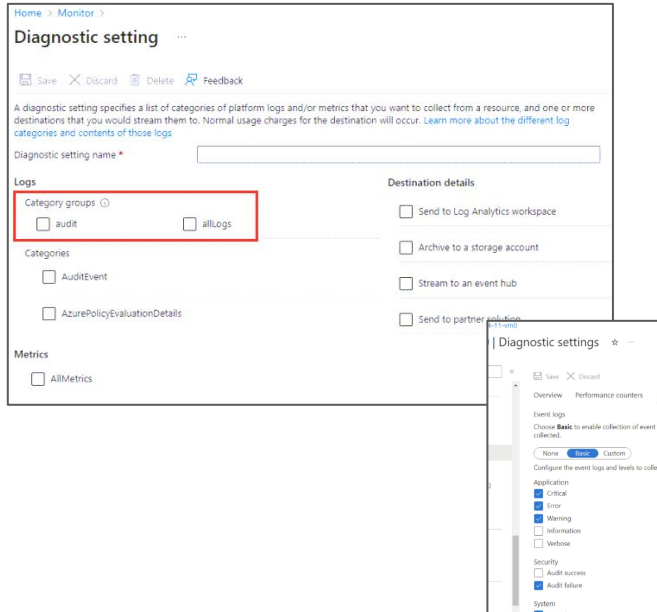
The effective data access configuration below combines the configuration for the currently selected resource and the data access configurations set on all parent resources.

Filter Identity and Access Management (IAM) API Enter property name or value X ? ☰						
<input type="checkbox"/> Service ↑	Admin Read	Data Read	Data Write	Exempted principals	Inherited exempted principals	
<input type="checkbox"/> Identity and Access Management (IAM) API	✓	—	—	0	0	



Log management in Azure

- Resources
- Diagnostics Settings
- Configuration



Export logs from Azure

Supported methods:

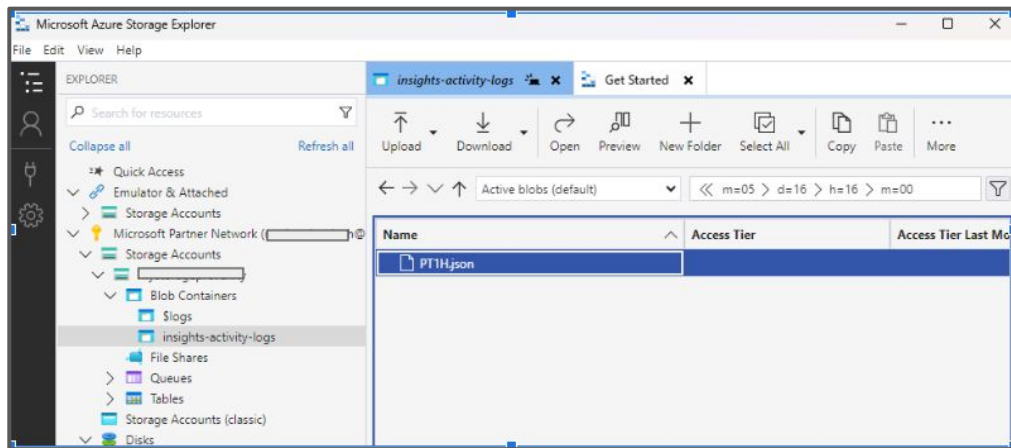
- Portal | Service
- Azure Monitor
- Export Data Settings
- REST API
 - GET

https://auditservice.dev.azure.com/{organization}/_apis/audit/auditlog?api-version=7.1-preview.1

- PowerShell
 - Get-AzLog | Get-AzActivityLog
- Azure CLI
- Microsoft Extractor Suite

Destinations:

- Storage Accounts
- Log Analytics
- Event Hubs



PS - microsoft extractor suite

```
PS /home/mariusz> Get-ActivityLogs -StartDate 2024-02-22 -EndDate 2024-02-25 -OutputDir Evidence
[INFO] Custom directory set to: Evidence
[INFO] Retrieving all subscriptions linked to the logged-in user account
[INFO] Identified Subscription: [REDACTED]
[INFO] Activity logs found in subscription: [REDACTED]
[INFO] Retrieving all Activity Logs for [REDACTED]
[INFO] Connected to Subscription [REDACTED]
[INFO] No Activity Logs found on 2024-02-22. Moving on!
[INFO] No Activity Logs found on 2024-02-23. Moving on!
[INFO] Successfully retrieved 3 Activity logs for 2024-02-24. Moving on!
[INFO] Done all logs are collected for Microsoft Partner Network
PS /home/mariusz>
```

```
[
{
  "EventTimestamp": "2/24/2024 4:06:16 AM",
  "EventName": "End request",
  "EventDataId": "****",
  "TenantId": null,
  "CorrelationId": "****",
  "SubStatus": "OK (HTTP Status Code: 200)",
  "SubscriptionId": "****",
  "SubmissionTimestamp": "2/24/2024 4:09:51 AM",
  "Status": "Succeeded",
  "ResourceType": null,
  "ResourceProviderName": "Microsoft.GuestConfiguration",
  "ResourceId": "/subscriptions/***/providers/Microsoft.GuestConfiguration",
  "ResourceGroupName": "",
  "OperationName": "Registers the feature for Microsoft.GuestConfiguration",
  "OperationId": "****",
  "Level": "Informational",
  "Id": "/subscriptions/***/providers/Microsoft.GuestConfiguration/events/***/ticks/****",
  "Description": "",
  "Category": "Administrative",
  "Caller": "****",
  "...
}
```

Export logs from GCP

Supported methods:

- GCP console
- Cloud Logging service
- API
 - POST
<https://logging.googleapis.com/v2/entries:list>
 - ProjectIDs
 - resourceNames
- CLI
 - `gcloud logging read --format=csv,json`

Destinations:

- Storage
 - `_Default`
 - `_Required` (Admin Activity i System Event)
- BigQuery
- Cloud Pub/Sub

CLI - gcloud

```
gcloud logging read 'timestamp >= "2024-04-09T00:00:00Z" AND timestamp < "2024-04-10T00:00:00Z"' --project=<project> --format=json > exported.log
```

```
[
  {
    "insertId": "-wgmuy5dobky",
    "logName": "projects/***/logs/cloudaudit.googleapis.com%2Factivity",
    "protoPayload": {
      "@type": "type.googleapis.com/google.cloud.audit.AuditLog",
      "authenticationInfo": {
        "principalEmail": "***@***.iam.gserviceaccount.com",
        "principalSubject": "serviceAccount:svc-gcp-permission@t***.iam.gserviceaccount.com",
        "serviceAccountKeyName": "//iam.googleapis.com/projects/***/serviceAccounts/***/***@***.iam.gserviceaccount.com/keys/****"
      },
      "authorizationInfo": [
        {
          "permission": "resourceManager.projects.setIamPolicy",
          "permissionType": "ADMIN_WRITE",
          "resource": "projects/****",
          "resourceAttributes": {
            "name": "projects/****",
            "service": "cloudresourcemanager.googleapis.com",
            "type": "cloudresourcemanager.googleapis.com/Project"
          }
        }
      ],
      {
        "permission": "resourceManager.projects.setIamPolicy",
        "permissionType": "ADMIN_WRITE",
        "resource": "projects/****",
        "resourceAttributes": {
          "name": "projects/c****",
          "service": "cloudresourcemanager.googleapis.com",
          "type": "cloudresourcemanager.googleapis.com/Project"
        }
      }
    ]
  },
  ...
```

Google Workspace - Audit Log Collection

The screenshot displays the Google Admin console's Audit Log interface. On the left, a sidebar lists navigation options: Home, Dashboard, Directory, Chrome browser, Devices, Apps, Security, Overview, Alert centre, Authentication, Access and data control, Security centre, and Reporting. The main content area shows a search bar at the top with the text 'Search for users, groups or settings'. Below it, a breadcrumb trail reads 'Security > Investigation tool > Draft investigation'. The central panel is titled 'Search 1' and includes links for 'Create activity rule', 'Create custom chart', and 'Discard search'. A dropdown menu is set to 'Admin log events', with 'Filter' and 'Condition builder' options. An 'ADD CONDITION' button is present. Below this, the 'GROUP RESULTS' section shows a 'SEARCH' status. A message indicates 'Showing 6101–6200 of many results'. A red rectangle highlights the 'Export all' button, which is part of a row of actions including 'Select results on all pages' and 'Actions'. An export dialog box is open on the right, titled 'Export results from Search 1'. It contains fields for 'Export name' and 'Select format', with 'Comma-separated values (.csv)' selected. A note states: 'The maximum number of exported results depends on the data source and export format. Learn more about export limits'. At the bottom of the dialog are 'CANCEL' and 'EXPORT' buttons.

Admin

Search for users, groups or settings

Security > Investigation tool > Draft investigation

Search 1 Create activity rule Create custom chart Discard search

Admin log events Filter Condition builder

ADD CONDITION

GROUP RESULTS

SEARCH

Showing 6101–6200 of many results Select results on all pages Export all Actions

Date ↓ Event Description Actor

Export results from Search 1

Export name 0/80

Select format

☐ Google Sheets

☒ Comma-separated values (.csv)

i The maximum number of exported results depends on the data source and export format. [Learn more about export limits](#)

CANCEL EXPORT

Google Cloud Platform - Cloud Audit Logs Collection

The screenshot displays the Google Cloud Platform Logs Explorer interface. A query is entered in the top bar: `logName="organizations/*/logs/cloudaudit.googleapis.com%2Factivity"`. The interface shows a timeline view of log entries from April 12 to May 11, 2024. A red box highlights the 'Log fields' section on the left, which includes 'PROJECT ID' and 'RESOURCE TYPE'. Another red box highlights the 'Download logs' dialog box, which is open and shows the 'Maximum log entries' set to 500 and the 'Format' set to CSV. A third red box highlights the 'Select log names' section on the right, where the 'activity' log name is selected. The 'Refine scope' panel on the left shows the 'Scope by storage' option selected, and the 'All logs' checkbox is checked under the 'Filter projects and log views' section.

Logs Explorer

Query

Log fields

Timeline

Download logs

Download logs

Log entries matching your query will be downloaded. If you need over 10,000 logs consider [exporting your logs](#).

Maximum log entries

Format

JSON CSV

View in New Tab Save to Google Drive Download

Select log names

Search log names

CLOUD AUDIT

activity

organizations/*/logs/cloudaudit...

Cancel Apply

Microsoft 365/Office 365 - Audit Log Collection

Audit > Audit search							
Search Query Information: Mon, 13 Feb 2023 00:00:00 GMT to Tue, 14 Feb 2023 00:00:00 GMT ,							
Total Result Count: 416794 items							
<div>↓ Export</div> <div>300 items Filter</div>							
Date (UTC) ↓	IP Address	User	Record type	Activity	Item	Admin Units	Detail
Feb 13, 2023 11:39 PM		app@sharepoint	SharePointFileOperation	Accessed file	WDX_0_80591.txt		Accessed from "IPML_WDX_0_25"
Feb 13, 2023 11:36 PM		app@sharepoint	SharePointFileOperation	Accessed file	WKC_3_4328036_1.txt		Accessed from "IPML_WKC_3_971"
Feb 13, 2023 11:34 PM		app@sharepoint	SharePointFileOperation	Accessed file	WKC_3_2501408_12.txt		Accessed from "IPML_WKC_3_505"
Feb 13, 2023 11:18 PM		app@sharepoint	SharePointFileOperation	Accessed file	WKC_3_1375754_2.txt		Accessed from "IPML_WKC_3_150"
Feb 13, 2023 11:06 PM		app@sharepoint	SharePointFileOperation	Accessed file	WKC_3_850620_13.txt		Accessed from "IPML_WKC_3_1401"
Feb 13, 2023 10:39 PM		app@sharepoint	SharePointFileOperation	Accessed file	WKC_3_4224876_1.txt		Accessed from "IPML_WKC_3_950"
Feb 13, 2023 9:54 PM		app@sharepoint	SharePointFileOperation	Accessed file	WKC_3_853448_2.txt		Accessed from "IPML_WKC_3_1401"
Feb 13, 2023 8:49 PM		app@sharepoint	SharePointFileOperation	Accessed file	WKC_3_3240581_16.txt		Accessed from "IPML_WKC_3_727"

CSV file contains AuditData

Azure - Entra Audit Logs Collection

Microsoft Azure

Search resources, services, and docs (G+/)

Home > [redacted] | Audit logs ...

You can download up to 250,000 records. If you want to download more, use reporting APIs. Click here to learn more.

Your download will be based on the filter selections you have made.

Format
☒ CSV ☐ JSON

File Name
AuditLogs_2024-05-16

Download

Synchronization << Download Export Data Settings Refresh Manage view v Got feedback?

Want to switch back to the legacy audit logs experience? Click here to leave the preview.

Add filter Show dates as: Local Date range: Last 24 hours Service : All Category : All Activity : All Reset filters

Directory Custom Security

Date ↓	Service	Category	Activity	Status	Status Reason
5/16/24, 5:42:17 PM	Core Directory	ApplicationManagement	Add service principal	Failure	Microsoft.Online.Workflows.
5/16/24, 5:42:17 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:17 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:16 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:16 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:16 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:16 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:16 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	
5/16/24, 5:42:15 PM	Core Directory	ApplicationManagement	Add service principal	Success	

Monitoring

Sign-in logs

Audit logs

Provisioning logs

Health

Log Analytics

Diagnostic settings

Workbooks

Usage & insights

Bulk operation results (Preview)

Troubleshooting + Support

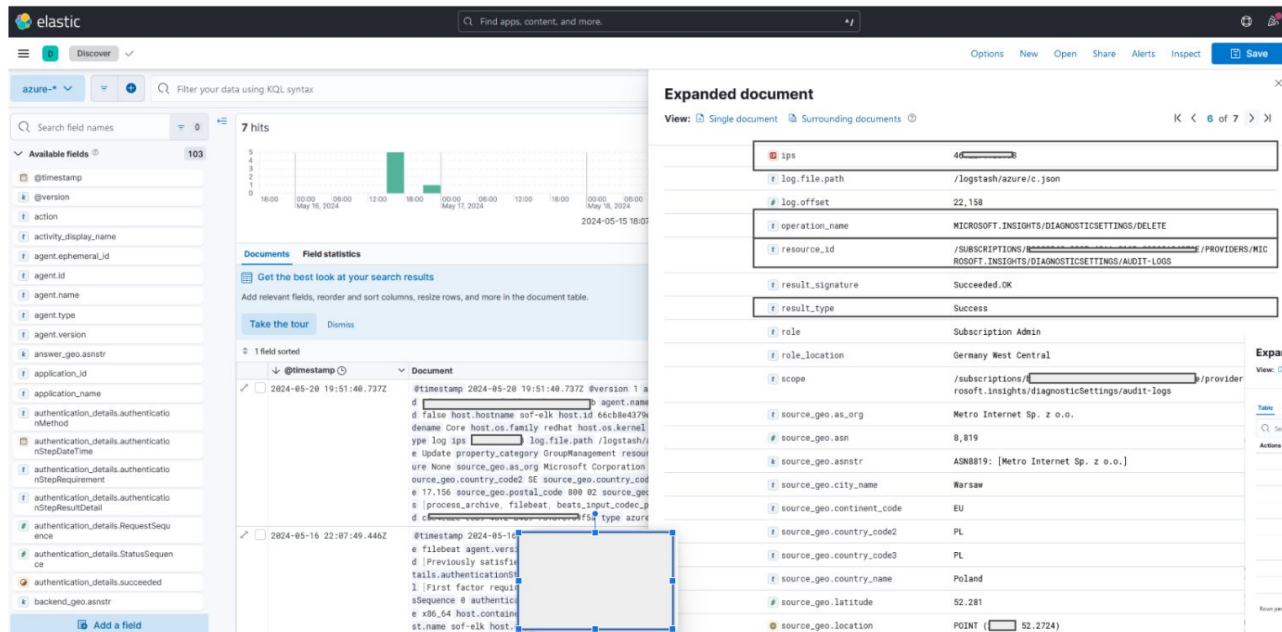
Analysis with SOF-ELK (GCP logs)

The screenshot displays the Elastic Discover interface for analyzing GCP logs. The main search results pane shows 316 hits. The left sidebar lists available fields, including @timestamp, @version, agent.ephemeral_id, agent.id, agent.name, agent.type, agent.version, answer.geo.ipstr, authorization_info.granted, authorization_info.permission, authorization_info.resource, authorization_info.resourceAttribute.s.name, authorization_info.resourceAttribute.s.service, authorization_info.resourceAttribute.s.type, authorization_permissions.cloudtrans.state.translationmemories.delete.granted, authorization_permissions.compute.images.create.granted, and authorization_permissions.compute.i.

The central pane shows a list of documents with the following fields: @timestamp, @version, agent.name, agent.type, agent.version, authorization_info.granted, authorization_info.permission, authorization_info.resource, authorization_permissions.orgpolicy.policies.delete, authorization_permissions.orgpolicy.policies.delete.resource, event.type, gcp_log_id, host.architecture, host.containerized, host.hostname, and host.id.

The right-hand pane shows the expanded document details, including fields like _score, @timestamp, @version, agent.name, agent.type, agent.version, authorization_info.granted, authorization_info.permission, authorization_info.resource, authorization_permissions.orgpolicy.policies.delete, authorization_permissions.orgpolicy.policies.delete.resource, event.type, gcp_log_id, host.architecture, host.containerized, host.hostname, and host.id.

Analysis with SOF-ELK (Azure logs)



Expanded document

View: Single document Surrounding documents

K < 6 of 7 >

Table JSON

Search field names

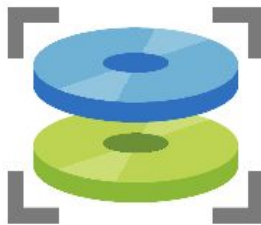
Field	Value
source_geo.postal_code	[redacted]
source_geo.region_code	16
source_geo.region_name	Poland
source_geo.timezone	Europe/Warsaw
source_ip	[redacted]
tags	[process.archive, filebeat, beats, logstash, logstash-input-logstash, logstash-output-logstash]
type	source
source_geo.location	POINT (52.2724)

Rows per page: 10

VMs



Dysk



Snapshot



WORM

Discussed scenario: Shutdown the VM and take a snapshot of each disk, but it is possible to take snapshot while the VM is running.

GCP - Compute Engine - image acquisition

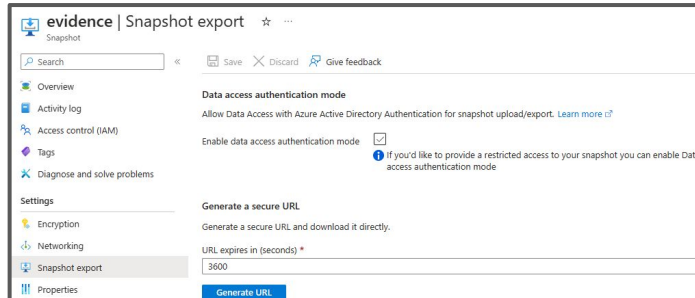
1. Enumerating all VM disks
 - `gcloud compute instances describe <VM_NAME> --format="tabledisks"`
2. Creating snapshot
 - `gcloud compute disks snapshot <DISK_NAME> --snapshot-names=evidence --zone=<ZONE>`
3. Creating image
 - `gcloud compute images create evidence-image --source-snapshot=evidence`
4. Exporting image to bucket
 - `gcloud compute images export --destination-uri=gs://<BUCKET>/<NAME> --image=evidence-image --export-format=vmdk`

GCP - Compute Engine - copy disk to bucket

1. Creating of temp disk (disk will be used to store evidence)
 - `gcloud compute disks create temp-forensic-disk --size 40GB --zone=<ZONE>`
2. Creating of new disk from original snapshot
 - `gcloud compute disks create evidence-disk --source-snapshot=evidence --zone=<ZONE>`
3. Setting up new (temporary) VM
 - `gcloud compute instances create <VM_NAME> --scopes storage-ro --disk name=evidence-disk,device-name=evidence-disk--zone=<ZONE>`
4. Adding disk from step 1(temp-forensic-disk) in RW mode
5. Configuration of temp disk and making copy of new disk
 - `mkfs.ext4 -F /dev/disk/by-id/google-temp-forensic-disk`
 - `mount -o rw /dev/disk/by-id/google-temp-forensic-disk /mnt`
 - `dd if=/dev/<sdx> of=/mnt/<image> conv=sync,noerror`
 - hash calculation (`openssl sha256 <image>`)
 - compression/conversion of evidence
6. Making copy of disk to bucket
 - `gsutil cp <image> gs://<bucket-name>/<image>`
7. Temporary sharing of image with sign-url feature of GCP
 - `gcloud storage sign-url gs://<bucket-name>/<image> --private-key-file=<privkey.json> --duration=20m`

Azure - Virtual Machine - disk acquisition

1. Gathering metadata information about VM and disks (OsDisk and DataDisks)
 - `$vm = Get-AzVM -ResourceGroupName <GROUP-NAME> -Name <VM-NAME>`
 - `$datadisk = Get-AzDisk -ResourceGroupName <GROUP-NAME> -DiskName $vm.StorageProfile.DataDisks.Name` (in this example we will copy an additional data disk)
2. Snapshot configuration
 - `$snapshotconfig = New-AzSnapshotConfig -SourceUri $datadisk.Id -CreateOption Copy -Location $vm.Location`
3. Snapshot creation
 - `New-AzSnapshot -ResourceGroupName <GROUP_NAME> -Snapshot $snapshotconfig -SnapshotName "evidence"`
4. Export from Azure console



Azure - Virtual Machine - copy image to blob

Copying to Storage Account BLOB

1. Gathering Storage Account metadata
 - `$targetstoragecontextblob = (Get-AzStorageAccount -ResourceGroupName <GROUP-NAME> -Name "<STORAGE-NAME>").Context`
2. Gathering snapshot metadata
 - `$snapshot = Get-AzSnapshot -ResourceGroupName <GROUP-NAME> -SnapshotName "evidence"`
3. Temporary sharing of snapshot
 - `$snapshotSasURL = Grant-AzSnapshotAccount -ResourceGroupName <GROUP-NAME> -SnapshotName $snapshot.Name -DurationInSecond 3600 -Access Read`
4. Copying of snapshot to Storage Blob
 - `Start-AzStorageBlobCopy -AbsoluteUri $snapshotSasUrl.AccessSAS -DestContainer <CONTAINER-NAME> -DestContext $targetstoragecontextblob -DestBlob "evidence-snapshot" -Force`

Kubernetes forensics

- Creation of snapshot of disks attached to K8S nodes (as presented on previous slides)
- Mount node image (image contains containers but also logs from pods)
- Use Docker-explorer or Container-explorer (for GCP) in order to mount containers
- Docker-explorer shows image history:

```
de.py -r /mnt/root/var/lib/docker history
003fd5af7dcb0d8f84ecb49dbb5648a6e4626affa6c29417a2cf6cf7351bb2d6

{
  "sha256:7968321274dc6...": {
    "container_cmd": "/bin/sh -c #(nop) CMD [\"sh\"]",
    "created_at": "2024-04-21T18:42:05.712133",
    "size": 0
  }
}
```

Mounting container from GKE node - example

- Attach disk to VM in read only mode
- Identify disk
 - `dmesg | grep sd`
- Listing all partitions on disk
 - `fdisk -l /dev/sdc`

Device	Start	End	Sectors	Size	Type
/dev/sdc1	8704000	104857566	96153567	45.9G	Linux filesystem
...					

- Mounting file system /dev/sdc1 as read only
 - `mount -o ro,noload,noexec /dev/sdc1 /mnt`
- Listing containers with use of container explorer
 - `. /ce -i /mnt/part1/ --support-container-data supportcontainer.yaml list containers`
- Mounting container
 - `. /ce -i /mnt/part1 --support-container-data supportcontainer.yaml -n k8s.io mount 003fd5af7dcb0d8f84ecb49dbb5648a6e4626affa6c29417a2cf6cf7351bb2d6 /mnt/container/`

Encrypted disks

GCP

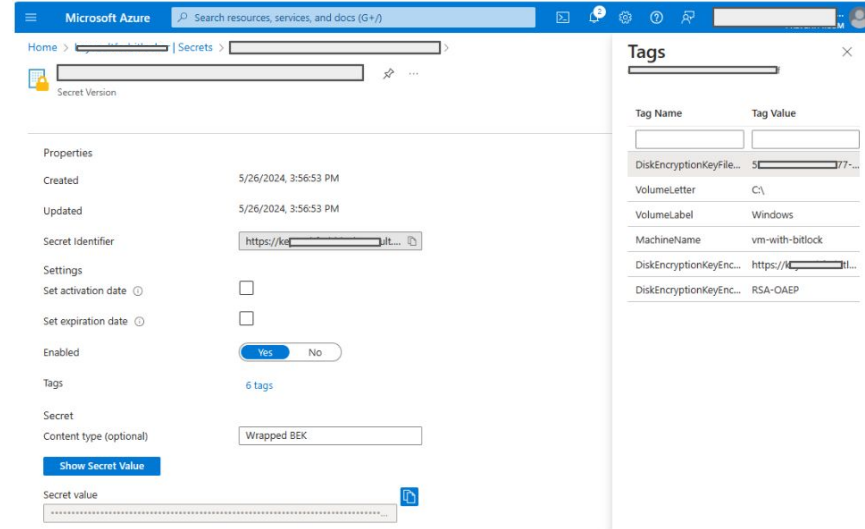
- Google managed encryption (at rest)
- Cloud KMS
 - KEK/DEK
 - CMEK
 - CSEK
- Snapshot points to KMS

Azure

- Azure Disk Storage Server-Side Encryption
 - Disk Encryption Set
- Encryption at host
- Azure Disk Encryption
 - Azure Key Vault stores Bitlocker encryption key (BEK) i DM-Crypt encryption key

BitLocker - decrypting disk

- **Check whether volumes are encrypted**
 - `Get-AzVmDiskEncryptionStatus -ResourceGroupName <NAME> -VMName <NAME>`
- **Collect metadata about encrypted disk**
 - `$disk = Get-AzDisk -ResourceGroupName <GROUP-NAME> -DiskName <DISK-NAME>`
- **Retrieve BitLocker Encryption Key URL**
 - `$BEKurl = echo $disk.EncryptionSettingsCollection.EncryptionSettings.DiskEncryptionKey.SecretUrl`
- **Retrieve Key Encryption Key URL**
 - `$KEKurl = Get-AzKeyVaultKey -VaultName <NAME> -Name <KEYNAME>`
- **Unwrap (decrypt) BitLocker Encryption Key**
 - `*unwrapbek.ps1 $BEKurl $KEKurl $recoverykey (output)`
- **Mount and unlock volume**
 - `manage-bde -unlock <drive> -RecoveryKey <recoverykey>`



Preparation of forensic environment in cloud

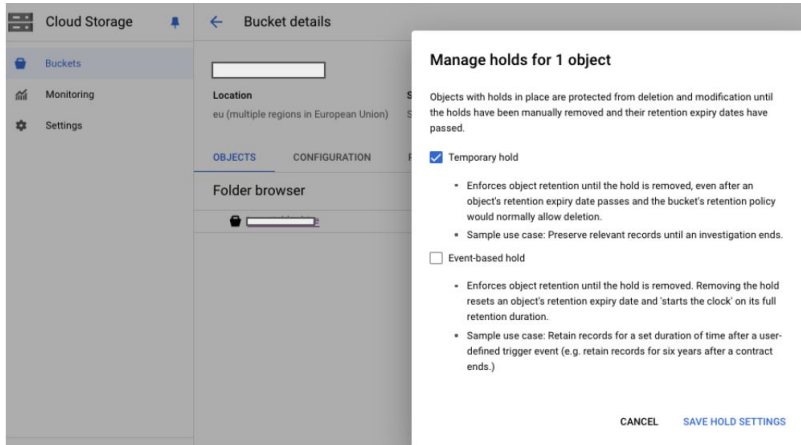
- Evidence protection
- Data integrity verification
- Microsoft Azure and Google Cloud Platform reference architectures

Immutable storage

GCP

Lifecycle Management

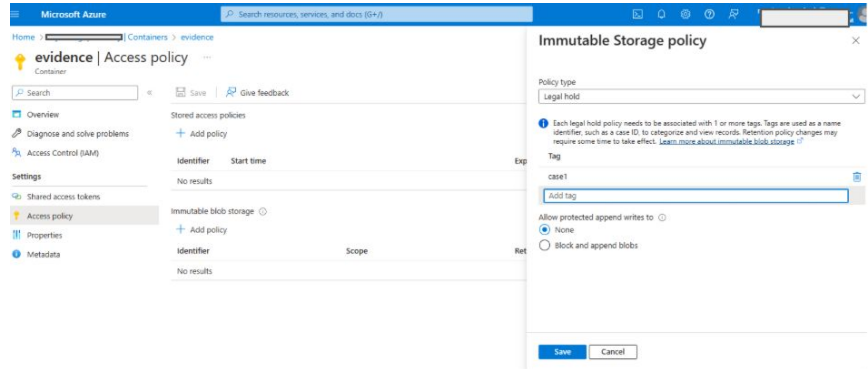
Manage Holds



Azure

Lifecycle Management

Legal Hold



Automation - handling images

Operations which can be performed remotely

- Compression (valuable due to image size)
- hash calculation
- conversion of images - e01, vmdk, vhd, EWF.

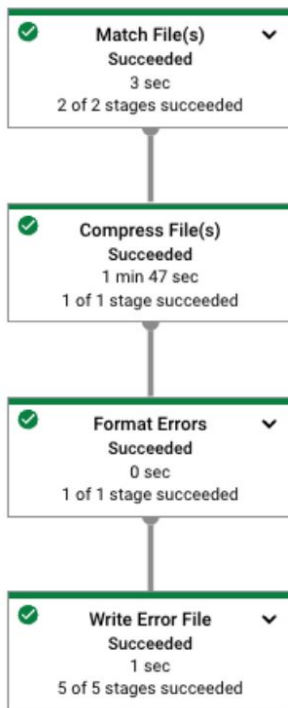
GCP

- Cloud Function
- Cloud Dataflow

Azure

- Azure Function
- Data Factory
- Azure Automation

Cloud Dataflow example - image compression



Pipeline options

appName	BulkCompressor
compression	GZIP
filesToStage	[/home/runner/actions-runner/_work/C ... SEE ALL
gcpTempLocation	gs://[redacted]/temp
inputFilePattern	gs://[redacted]/*.img
jobName	myforeniscjob
labels	{goog-dataflow-provided-template-nam
numWorkers	2
outputDirectory	gs://[redacted]/output/
outputFailureFile	gs://[redacted]
pipelineUrl	gs://dataflow-templates-libraries/2024-
project	[redacted]
region	europe-west1
runner	org.apache.beam.runners.dataflow.Dat
sdkContainerImage	-
serviceAccountEmail	sa-[redacted].iam.gse
stagingLocation	gs://dataflow-templates-libraries/2024-
templateLocation	gs://dataflow-templates-europe-west1/

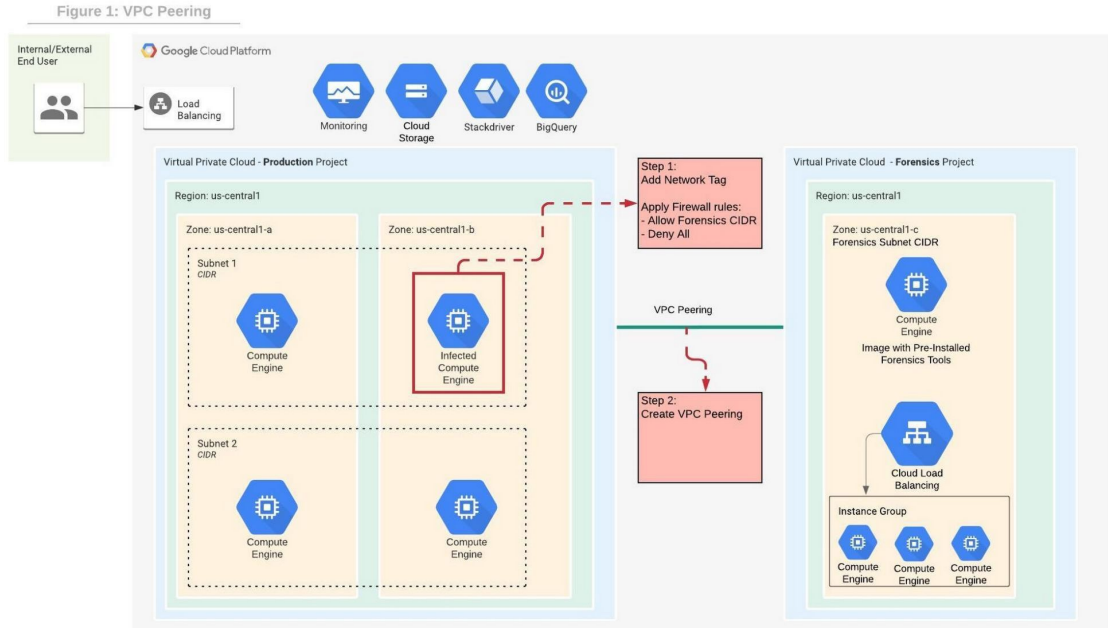
Reference Forensic Architecture for GCP

Incident response process:

Step 1: Isolation of MV

Step 2: enabling access between
forensic VM and infected VM

Step 3: Manual seizing of disks
and RAM (optional)

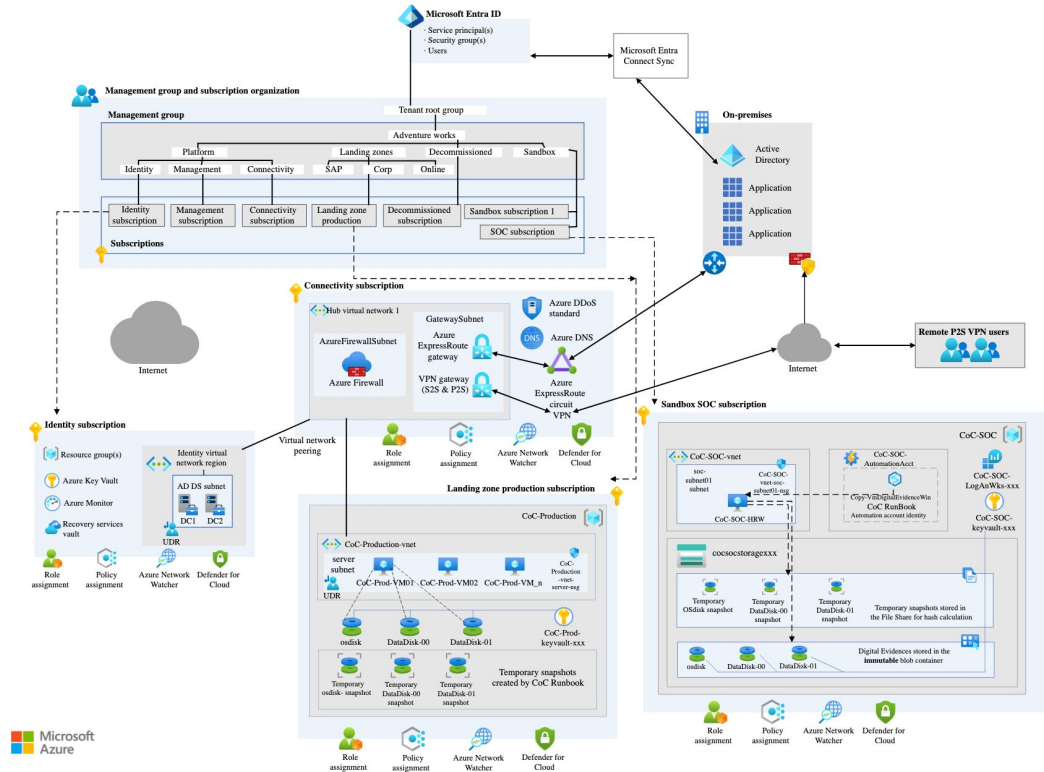


Reference Forensic Architecture for AZURE

Incident response process:

Step 1: Execution of Copy-VmDigitalEvidence runbook with use of Automation - runbook worker (VM). Script is copying BEK key.

Step 2: Manual seizing of RAM (optional)



Cloud Forensics - common issues

- Insufficient permissions
 - GCP -> roles/logging.privateLogViewer
 - Azure -> Key Vault Secrets User
- Constraint Policies
 - GCP -> Organization policy constraints (for example trusted image projects)
- Images/snapshots/disks are stored in different locations
- Limitation related to some cloud features (for example azure functions limits related to size of processed files with powershell)
- Firewall rules blocking access to VMs

References

<https://learn.microsoft.com/en-us/entra/identity/monitoring-health/>

<https://learn.microsoft.com/en-us/entra/identity/monitoring-health/concept-audit-logs>

<https://microsoft-365-extractor-suite.readthedocs.io/en/latest/>

<https://cloud.google.com/logging/docs/routing/overview>

<https://www.sans.org/tools/sof-elk/>

<https://github.com/google/docker-explorer>

<https://github.com/google/container-explorer>

<https://github.com/Prevenity/Azure-Cloud-Security>

<https://cloud.google.com/blog/products/identity-security/how-to-use-live-forensics-to-analyze-a-cyberattack>

<https://learn.microsoft.com/en-us/troubleshoot/azure/virtual-machines/windows/unlock-encrypted-disk-offline>

<https://learn.microsoft.com/en-us/azure/architecture/example-scenario/forensics/>

Thank you.