Cloudy with a Chance of Bad Logs: Cloud Platform Log Configurations to Consider in Investigations | Mandiant

By Mandiant

Published: 2023-05-03 · Archived: 2026-04-05 14:57:37 UTC

Written by: David Pany, Caitlin Hanley

More and more organizations utilize cloud technology for applications, file storage, and more. However, if an attacker compromises a cloud environment, organizations may not know how to investigate those technologies, or may not even be logging the evidence that could allow the organization to identify what an attacker did.

This blog post describes a hypothetical scenario of a cloud platform compromise with multiple components that would require investigation. Each component is an example of a real intrusion tactic that Mandiant has investigated across various cloud platforms, sometimes with logs available and sometimes without logs available.

Cloud Technology Themes

For each part of the compromise, we provide recommended logging configurations and investigation processes organized into cloud technology "themes" that group cloud services from Google Cloud Platform (GCP), Amazon Web Services (AWS), and Microsoft Azure together:

- Cloud Virtual Machines
  - GCP Compute Engine Virtual Machines, AWS EC2 Instance, Azure Virtual Machine
- Cloud Applications or Cloud Containers
  - GCP Kubernetes Engine, AWS Elastic Kubernetes Service, Azure Kubernetes Service
- Cloud Serverless Functions
  - GCP Cloud Functions,AWS Lambda, Azure Functions
- Cloud Database Services
  - GCP Datastore, GCP Cloud Bigtable, GCP Cloud SQL, AWS DynamoDB, AWS Aurora, AWS Relational Database Service, Azure Database, Azure SQL Database
- Cloud Authentication Services
  - GCP Cloud Identity, Azure Active Directory, AWS Directory Service
- Cloud Management Console
  - GCP Console, Azure Portal, AWS Console,
- Cloud Email
  - Google Workspace, Microsoft 365, Amazon Simple Email Service
- Cloud Code Repositories
  - GCP Cloud Source, AWS CodeCommit, Azure Repos
- Cloud Logging Platforms

    - GCP Logs Explorer, AWS Athena, Azure Monitor, Microsoft Sentinel, Azure Log Analytics
- Cloud Log Analysis Formats
    - GCP Audit Logs, GCP VPC Flow Logs, AWS CloudTrail, AWS VPC Flow Logs, Azure AD Audit Logs, Azure AD Sign In Logs, Azure Resource Logs, Azure Activity Logs, Azure NSG Flow Logs
- Cloud Networking
    - GCP Virtual Private Cloud, AWS Virtual Private Cloud, Azure Virtual Network
- Cloud File Storage
    - GCP Cloud Storage, AWS Simple Storage Solution (S3), Azure Blob Storage

Main Takeaways

After reading through this scenario, you should be able to:

1. Understand an example attack technique that targets each cloud technology theme
2. Identify event log configurations that should be reviewed in your cloud platform to facilitate an investigation
3. Develop and test incident response playbooks using the investigation recommendations
4. Utilize the event log checklists to review logging configurations and create logging standards

Areas to Research Further

While we review many concepts, there are some limitations to be aware of in the scope of this post:

1. These logging and investigation themes are just starting points to be aware of as you design cloud platforms unique to your environment. Not all of the logs discussed may be available or feasible, but if implemented they would assist in helping investigators identify malicious activity that may have only been recorded in the logs. This improves the timeliness and accuracy of the investigation
2. Since this blog post discusses a wide variety of cloud platforms, and configurations are frequently changing, we do not provide log implementation steps. Please work with your cloud administration team and cloud vendors to identify the considerations, configurations, and costs associated with the logs discussed here.
3. There are many hardening and configuration practices available to mitigate the malicious actions that occur in the post that are not covered here.

The Attack Path

1. Credential Stuffing

The attacker gained access to the Cloud Email platform through a credential stuffing attack against a cloud administrator account. Once the attacker found a valid password, the attacker authenticated with those credentials and the Cloud Email platform asked them which type of multi-factor authentication (MFA) process they preferred. The attacker chose the “push” option, which sent an approval request to the legitimate user. The administrator user deals with push authentication requests throughout the day for various services and mistakenly accepted the authentication request, which provided initial access to the attacker.

Investigation Theme: Cloud Authentication Services and Cloud Email

1. Analyze logins for the cloud administrator account.
2. Analyze Cloud Authentication Service alerts for risk-based patterns such as credential stuffing or authentications from unexpected locations.
3. Identify if IP addresses associated with failed logons have any successful logons.
4. Identify user accounts logging in from multiple IP addresses in multiple locations, particularly if the IP addresses are unexpected based on previous legitimate user activity.
5. Utilize threat intelligence to enrich context for suspicious IP addresses identified.
6. Review emails received by users for possible credential harvesting phishing links, particularly if the user reported the email as phishing.
7. Review Cloud Email alerts for suspicious emails identified by Cloud Email provider and users.
8. Review logs from Cloud Authentication Service risk-based detections for user sign-ins.

Logging Theme: Cloud Authentication Services

1. Log user authentication with timestamp, username, and source IP address.
2. Log multi-factor authentication details.
3. Turn on risk-based detections, if available.

2. Reconnaissance

Once the attacker identified the cloud administrator credentials and authenticated, they logged in to the Cloud Management Console to identify other applications that the user could access.

Investigation Theme: Cloud Authentication Services

1. Analyze the Cloud Management Console authentication logs for the previously identified suspicious source IP addresses and compromised user account.
2. Analyze the Cloud Management Console application access logs to identify unusual application access activity.

Logging Theme: Cloud Authentication Service

1. Log user authentication with timestamp, username, and source IP address.

3. Reconfiguring Privileges

The attacker identified that the cloud administrator account had access to the Cloud Authentication Services application and authenticated to it. In the Cloud Authentication Services application, the attacker changed the privileges of the cloud administrator to the highest global administrator account privileges available and removed the multi-factor requirement.

Investigation Theme: Cloud Authentication Services

1. Analyze changes to user accounts, including password, permissions, and contact information such as phone numbers for MFA or password reset.
2. Analyze accounts that have weak security controls such as disabled MFA requirements.
3. Analyze applications that have weak security controls such as disabled MFA requirements or access to unexpected user accounts.
4. Analyze MFA settings per account for anomalies such as disabled MFA, multiple MFA methods registered, recent MFA configuration changes, or configuration changes outside of policy.

Logging Theme: Cloud Authentication Services

1. Log access to all cloud services for authenticated users.
2. Log user authentication with timestamp, username, and source IP address.
3. Log changes to user permissions and configurations.

4. Identifying Hard-coded Credentials in Code

While in the Cloud Management Console, the attacker identified that the organization uses a custom Cloud Application. The attacker accessed the Cloud Code Repository with the global administrator account and identified the Cloud Application source code hosted there. The attacker accessed the code and identified plain-text hard-coded credentials for an application service account.

Investigation Theme: Cloud Applications or Containers, Cloud Code Repositories

1. Analyze user access to application source code.
2. Analyze creation and modification of application source code.
3. Review accessed code to identify impact of exposed data, such as credentials.
4. Review logs related to application-related files and code download, if available.

Logging Themes: Cloud Authentication Services, Cloud Applications and Containers, and Cloud Code Repositories

1. Log access to all cloud services for authenticated users.
2. Log creation, modification, and access to application code.
3. Log download of files and code related to application.
4. Log web-based code views, downloads, and edits.
5. Log code management access and modification through tools such as git.
6. Log user authentication with timestamp, username, and source IP address.

5. Identifying Hard-coded Credentials in Logs

While in the Cloud Authentication Services application, the attacker identified that the Administrator had access to the Cloud Logging platform. The attacker authenticated to the Cloud Logging platform and searched logs for keywords related to plain-text credentials. The attacker exported logs that contained those keywords, particularly database user credentials.

Investigation Theme: Cloud Logging

1. Analyze access to cloud log aggregation platforms.
2. Analyze log queries performed.
3. Analyze exported logs.
4. Analyze log modification and deletion.

Logging Theme: Cloud Logging

1. Log authentication to logging services.
2. Log queries executed for log data.
3. Log data exports.
4. Log modification/deletion of log data.

6. Environment Enumeration

The attacker returned to the cloud Authentication Service application and performed reconnaissance on systems and users. The attacker exported all environment objects including systems and accounts.

Investigation Theme: Cloud Authentication Services

1. Analyze access to Authentication Service queries and configurations viewed.
2. Analyze exported Authentication Service and domain data.
3. Analyze Authentication Service modifications for permissions and security parameters.

Logging Theme: Cloud Authentication Services

1. Log access to all cloud services for authenticated users.
2. Log changes to user permissions and configurations.
3. Log exported domain data.
4. Log created user accounts.

7. Infrastructure Creation

Next, the attacker pivoted to the Cloud Virtual Machine infrastructure and created a templated virtual machine. The attacker assigned the virtual machine to the application service account previously identified in the application source code. The attacker configured the Cloud Networking rules to allow remote desktop protocol (RDP) access from the internet. The application service account did not require MFA for any authentication activity because of its intended use. The attacker logged on to the virtual machine through RDP from their command and control (C2) server.

Investigation Theme: Virtual Machines

1. Analyze virtual machine creation and modification events.
2. Analyze virtual IP address actions such as create, delete, and modify.

3. Analyze changes made to network configurations.
4. Analyze modifications to network controls.
5. Analyze Authentication Service authentications for systems.

Logging Themes: Virtual Machines and Cloud Networking

1. Configure system event logs to follow standard endpoint logging policies for authentication, user activity, and privileged account use.
2. Log virtual machine management actions such as start, pause, backup, snapshot, Create, Delete, and Command executions.
3. Log changes made to network configurations.
4. Log virtual IP address management actions such as create, delete, and modify.
5. Log network flow metadata.

8. Database Access

While logged on to the newly created virtual machine, the attacker identified a database server based on the hostname SQLDB01. The attacker moved laterally from the virtual machine they created to the database server via RDP using the application service account.

The attacker connected to the database, which utilized a Cloud Database Service backend, using the database user credentials previously identified in logs and explored the data by enumerating the table schema and running “select *” queries.

Investigation Theme: Cloud Database Services

1. Analyze database authentication logs to identify unexpected authentications based on account name, timeframe, or source of authentication.
2. Analyze queries for reconnaissance activity such as “select *” or access to unexpected data.
3. Analyze queries for modification and deletion activity.

Logging Theme: Cloud Database Services

1. Log database user authentication and source network address.
2. Log data access including source network address and user.
3. Log data modification and deletion including source network address and user.
4. Log errors and long running queries, which could be indicative of data transfer or reconnaissance.

9. Network Scanning

While logged on to the attacker-created virtual machine, the attacker also performed internal reconnaissance to identify other systems of interest. The attacker scanned the network for other systems using custom port scanning utilities that searched for open SSH, RPD, and SMB ports.

Investigation Themes: Cloud Virtual Machines and Cloud Networking

1. Analyze endpoint artifacts on virtual machines based on endpoint forensic processes.
2. Review internal network log data for patterns of network scanning.

Logging Themes: Cloud Virtual Machines and Cloud Networking

1. Configure system event logs to follow standard endpoint logging policies for authentication, user activity, and privileged account use.
2. Forward system logs to a log management platform or SIEM as part of standard polices and processes.
3. Log network flow metadata.

10. File Theft

The attacker identified a network-shared file server that hosted files on a Cloud File Storage solution. After enumerating files stored on the network share, the attacker copied files to their C2 system using a bulk network file transfer utility.

Investigation Theme: Cloud File Storage

1. Analyze files accessed by user accounts and source IP addresses.
2. Analyze users with a large number of file downloads during the timeframe.
3. Analyze users with a large number of file deletions during the timeframe.

Logging Themes: Cloud File Storage and Cloud Networking

1. Log file download events with user account, source IP address, and timestamp.
2. Log network flow metadata.
3. Log file creation, modification, upload, and deletion events with user account, IP address, and timestamp.
4. Log API access to file storage locations, folders, and files.
5. Log file and directory listing metadata view.

11. Placing Malware

While accessing the file server, the attacker also decided to stage further backdoors in trojanized files that are likely to be opened by users.

Investigation Theme: File Storage

1. Analyze file uploads, creations, modifications, and deletions, particularly from compromised accounts and IP addresses.
2. Analyze access to trojanized files to identify users whose systems need further investigation.
3. Scan files with anti-virus.
4. Analyze quarantined files.

Logging Theme: File Storage

1. Log user authentication.
2. Log file creation, upload, modification, and deletion events, including IP addresses.
3. Log file download events with user account, source IP address, and timestamp.
4. Turn on alerts for suspicious activity, including malware and mass downloads, if available.

12. Email Theft

While logged on to cloud email for the administrator account, the attacker browsed through the last several days of messages. The attacker looked at email folders named “finance” and “hr” and downloaded attachments from sent messages.

Investigation Theme: Collaboration — Cloud Email

1. Analyze messages viewed in a mailbox, particularly by compromised accounts and IP addresses.
2. Analyze attachments downloaded in a mailbox.
3. Analyze searches performed in a mailbox.

Logging Theme: Collaboration — Cloud Email

1. Log authentication to mailboxes.
2. Log access and views of email messages.
3. Log download and access of email attachments.
4. Log searches of mailboxes.

13. Spreading Malware

The attacker shared the uploaded trojanized backdoor file through the collaboration platform’s file sharing service with 20 users.

Investigation Theme: Collaboration — Cloud File Sharing

1. Analyze known bad files to see what accounts shared them and with whom.
2. Analyze known bad file downloads.

Logging Theme: Collaboration — Cloud File Sharing

1. Log authentication of user account and source IP address.
2. Log file creation, modification, upload, and deletion events with user account, IP address, and timestamp.
3. Log file download events with user account, source IP address, and timestamp.
4. Log location, folder, and file permission changes.
5. Log API access to file storage locations, folders, and files.

14. Impersonating Users

Several users messaged the administrator's account and asked questions about errors opening the new document they downloaded through the collaboration platform based on an automated file shared email link. The attacker replied to tell the users the document is legitimate.

Investigation Theme: Collaboration — Cloud Chat

1. Analyze chat message logs sent by compromised accounts.
2. Analyze chat message logs sent from users logged in from known malicious IP addresses.

Logging Theme: Collaboration — Cloud Chat

1. Log authentication of user account and source IP address.
2. Log messages sent, received, edited, and deleted.
3. Log files transferred and store content for review.

15. Anti-forensics

Finally, in an attempt to delay detection, the attacker created a mailbox rule to automatically delete replies to the compromised file share email.

Investigation Steps

1. Analyze current mailbox rule configurations to identify active mailbox rules.
2. Analyze mailbox rule logs to identify if the attacker modified existing rules or deleted rules they no longer needed.
3. Analyze messages currently in "Deleted" folders.
4. Analyze logs of messages permanently deleted.
5. Analyze other email message storage locations such as security tools or e-discovery retention platforms.

Logging theme: Collaboration — Email

1. Log mailbox rule creation, modification, and deletion.
2. Log message deletion.

Detection and Response

The aforementioned hypothetical scenario took place in a matter of several days, reflecting how quickly the threat actors moved in the real scenarios this one is based on. In these cases, information security teams commonly have only a few medium priority alerts fire that go unnoticed due to the abundance of alerts feeding from their tools.

In this scenario, suspicion started when several helpdesk team members realized they had separate reports of users who had suspicious files shared with them. The helpdesk team escalated to Information Security per their documented processes and the Incident Response (IR) team started an investigation into the cloud file sharing platform associated with the file sharing.

The IR team quickly realized that the default logging available with their lowest cost license subscription recorded many useful logs such as:

1. Failed and successful logons associated with credential stuffing and initial compromise
2. File sharing activity
3. Mailbox rules created
4. Files accessed in the cloud file sharing platform

Unfortunately, the investigation could not answer the question “did the attacker access any email messages or synchronize any mailboxes?” due to the default logging levels. The IR team also realized they were lucky the incident was detected relatively quickly because the default license subscription only stored logs for 90 days with their Cloud Logging platform.

After a post-mortem review several months later, the organization realized the IR team only reviewed collaboration platform authentications and did not cross reference against domain authentication logs. This meant that the internal team never identified that the attacker compromised the cloud infrastructure platform and performed follow-on activities such as creating and accessing a VM, elevating to domain administrator privileges, and interacting with file servers. They focused only the collaboration platform because the initial incident identification occurred after the sharing of files on the Collaboration Cloud File Sharing platform. The investigation had to be reopened several months later when evidence had started to disappear from Cloud Logging sources.

Conclusion

As the scenario demonstrates, attackers have a wider surface area to persist and steal data because of the adoption of cloud infrastructure and collaboration platforms. The move to these cloud platforms brings useful functionality and security features, but configuring everything correctly can be overwhelming for a team that is new to the technology.

Not only are there many access, permission, and protection configurations to consider, but teams should also make sure that they would be able to fully investigate various attacks that could happen by storing the correct logs.

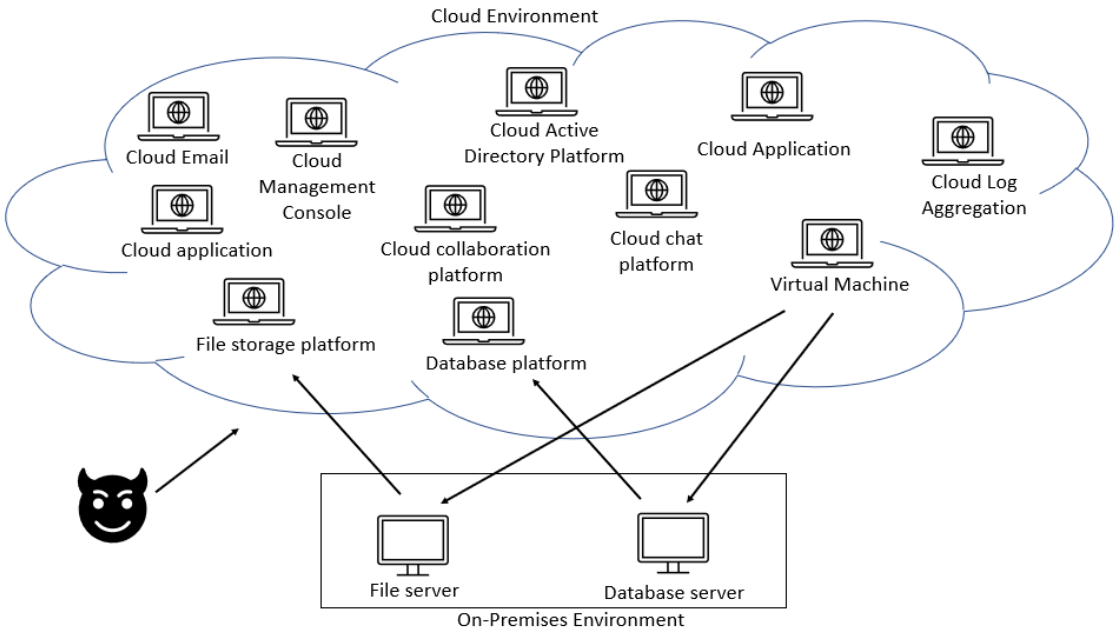
Understanding what technologies your organization uses and performing threat modeling is one way to make sure you have these logs and investigative processes set up should you need to investigate.

For details on how Mandiant can assist with your cloud security, please check out the following resources:

- Security Assessment for Microsoft 365
- Cloud Architecture and Security Assessment

Critical Attack Path

The following attack path diagram visualizes how the actor accessed a wide range of cloud platforms from outside a standard perimeter in this scenario. The actor also used cloud technologies to interact with systems in the non-cloud environment as well through connections and integrations.



Infrastructure Logging Checklist

The following checklist is designed to be copied or printed for your cloud infrastructure logging review efforts. The provided logs are example categories of commonly utilized event logs for forensic investigations.

Reference Number	Technology	Log Type
1.1.1	Cloud Virtual Machines	Configure system event logs to follow standard endpoint logging policies for authentication, user activity, and privileged account use.
1.1.2	Cloud Virtual Machines	Log virtual machine management actions such as Start, pause, backup, snapshot, create, delete, and command executions etc.
1.1.3	Cloud Virtual Machines	Forward system logs to a log management platform or SEIM as part of standard polices and processes.
1.2.1	Applications or Functions	Log web server access to application including source IP address, protocol used, request parameters, response status, user agent, referrer, and response size. Ensure that source IP address is not overwritten by proxy or load balancer technology.
1.2.2	Cloud Applications, Containers, and Functions	Log creation, modification, and access to application code.

1.2.3	Cloud Applications, Containers, and Functions	Record successful and failed authentication activity including source IP address.
1.2.4	Cloud Applications, Containers, and Functions	Log application user activity including user account, information viewed, actions performed, and sensitive data accessed.
1.2.5	Cloud Applications, Containers, and Functions	Forward system logs to a log management platform or SEIM as part of standard polices and processes.
1.3.1	Cloud Database Services	Log database user authentication and source network address.
1.3.2	Cloud Database Services	Log data access including source network address and user.
1.3.3	Cloud Database Services	Log data modification and deletion including source network address and user.
1.3.4	Cloud Database Services	Forward system logs to a log management platform or SEIM as part of standard polices and processes.
1.3.5	Cloud Database Services	Log errors and long running queries, which could be indicative of data transfer or reconnaissance.
1.4.1	Cloud File Storage	Log user authentication.
1.4.2	Cloud File Storage	Log file creation, modification, upload, and deletion events with user account, IP address, and timestamp.
1.4.3	Cloud File Storage	Log file download events with user account, source IP address, and timestamp
1.4.4	Cloud File Storage	Log location, folder, and file permission changes.
1.4.5	Cloud File Storage	Log API access to file storage locations, folders, and files.
1.4.6	Cloud File Storage	Log file and directory listing metadata view.
1.4.7	Cloud File Storage	Turn on alerts for suspicious activity, including malware and mass downloads, if available.
1.5.1	Cloud Authentication Services	Log user authentication with timestamp, username, and source IP address.

1.5.2	Cloud Authentication Services	Log changes to user permissions and configurations.
1.5.3	Cloud Authentication Services	Log created user accounts.
1.5.4	Cloud Authentication Services	Log all successful and failed authentications to cloud management platform
1.5.5	Cloud Authentication Services	Log access to all cloud services for authenticated users.
1.5.6	Cloud Authentication Services	Log exported domain data.
1.5.6	Cloud Authentication Services	Turn on risk-based detections, if available.
1.5.7	Cloud Authentication Services	Log user authentication with timestamp, username, and source IP address.
1.6.1	Cloud Code Repositories	Log web-based code views, downloads, and edits.
1.6.2	Cloud Code Repositories	Log code management access and modification through tools such as git.
1.7.1	Cloud Logging	Log authentication to logging services.
1.7.2	Cloud Logging	Log queries executed for log data.
1.7.3	Cloud Logging	Log data exports.
1.7.4	Cloud Logging	Log modification and deletion of log data.
1.8.1	Cloud Networking	Log network flow metadata.
1.8.2	Cloud Networking	Log changes made to network configurations.
1.8.3	Cloud Networking	Log virtual IP address management actions such as create, delete, and modify.

Collaboration Platform Logging Checklist

Reference Number	Technology	Log Type

2.1.1	Cloud Email	Log inbound and outbound email metadata. Minimum details should include: 1. Timestamp sent/received 2. Sender 3. Recipient(s) 4. Attachment name 5. Sender mail server address
2.1.2	Cloud Email	Log authentication to mailboxes.
2.1.3	Cloud Email	Log access and views of email messages.
2.1.4	Cloud Email	Log download and access of email attachments.
2.1.5	Cloud Email	Log creation and deletion of mailbox rules.
2.1.6	Cloud Email	Log deletion of messages.
2.1.7	Cloud Email	Log permission and access configuration changes to mailboxes.
2.1.8	Cloud Email	Log searches of mailboxes.
2.2.1	Cloud Chat	Log authentication of user account and source IP address.
2.2.2	Cloud Chat	Log messages sent, received, edited, and deleted.
2.2.3	Cloud Chat	Log files transferred and store content for review.
2.2.4	Cloud Chat	Log relevant data for applications connected to chat platforms.
2.3.1	Cloud File Sharing	Log user authentication.
2.3.2	Cloud File Sharing	Log file creation, modification, upload, and deletion events with user account, IP address, and timestamp.
2.3.3	Cloud File Sharing	Log file download events with user account, source IP address, and timestamp
2.3.4	Cloud File Sharing	Log location, folder, and file permission changes.
2.3.5	Cloud File Sharing	Log API access to file storage locations, folders, and files.

Posted in

- Threat Intelligence

- Security & Identity
